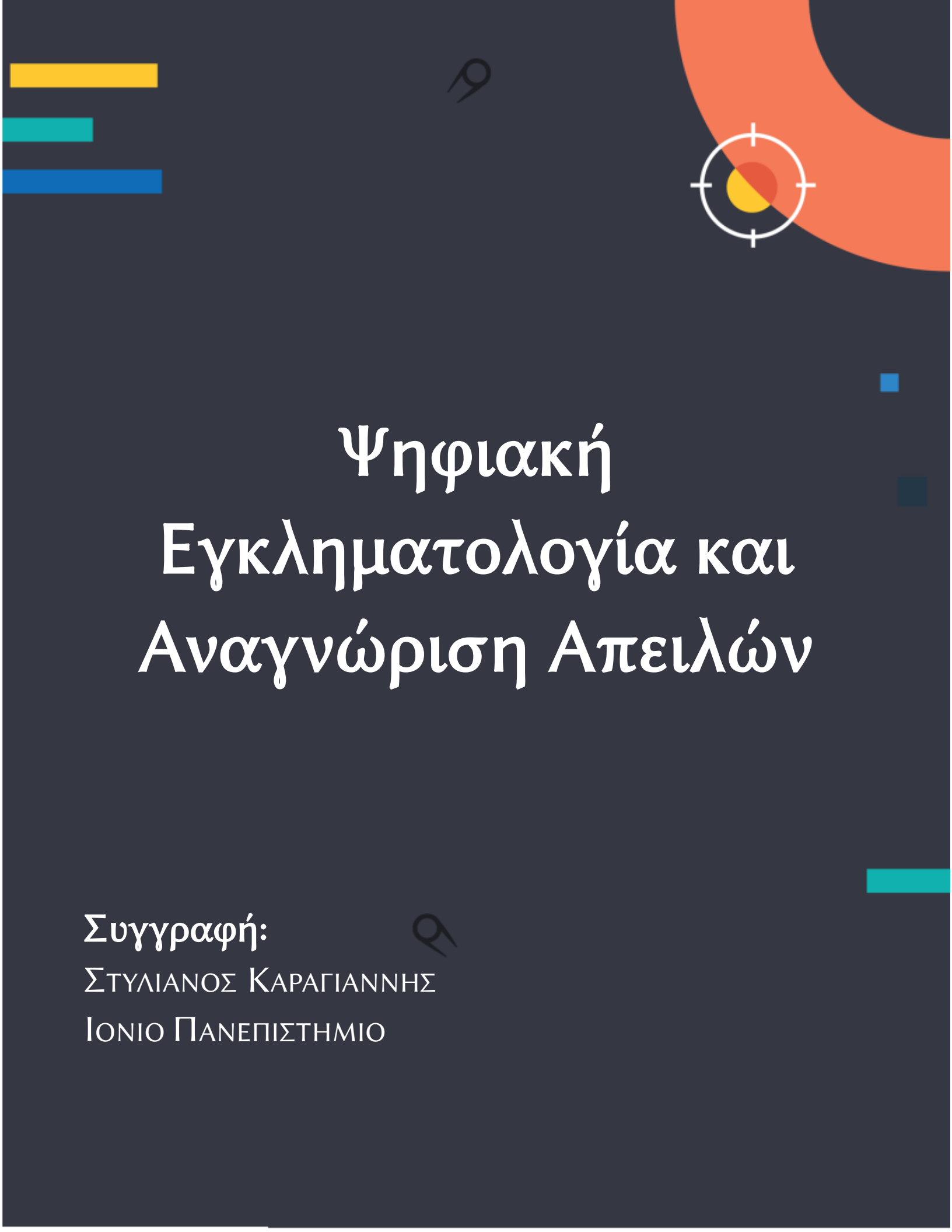




Ψηφιακή Εγκληματολογία και Αναγνώριση Απειλών

Συγγραφή:

ΣΤΥΛΙΑΝΟΣ ΚΑΡΑΓΙΑΝΝΗΣ

ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

1

Ανταπόκριση σε Περιστατικά

Όταν εξετάζονται οι απειλές για τη σύγχρονη τεχνολογία πληροφοριών, η εικόνα μπορεί να φαίνεται αποθαρρυντική. Από απλούς *script kiddies* που χρησιμοποιούν έτοιμο κώδικα έως εργαλεία κρατικών αντιπάλων, είναι κρίσιμο να υπάρχει κατάλληλη προετοιμασία. Για παράδειγμα, ένας εσωτερικός υπάλληλος μπορεί να κατεβάσει ένα και μόνο δείγμα **ransomware**, το οποίο να προκαλέσει σημαντικές επιπτώσεις σε έναν οργανισμό. Ακόμη πιο σύνθετες επιθέσεις, όπως μια προσπάθεια εκμετάλλευσης δικτύου ή μια στοχευμένη παραβίαση δεδομένων, αυξάνουν το χάος που δημιουργεί ένα περιστατικό ασφαλείας. Το τεχνικό προσωπικό θα έχει τα χέρια του γεμάτα, προσπαθώντας να καθορίσει ποια συστήματα έχουν επηρεαστεί και πώς αυτά χειραγωγούνται. Παράλληλα, θα πρέπει να αντιμετωπίσει την πιθανή απώλεια δεδομένων μέσω συμβιβασμένων συστημάτων. Στην ήδη χαοτική αυτή κατάσταση, προστίθενται τα ανώτερα στελέχη, τα οποία απαιτούν συνεχείς ενημερώσεις και απαντήσεις στις καίριες ερωτήσεις: «Πώς συνέβη αυτό;» και «Πόσο σοβαρό είναι;».

Η ικανότητα ορθής αντιμετώπισης περιστατικών ασφαλείας με έναν τακτικό και αποτελεσματικό τρόπο επιτρέπει στους οργανισμούς τόσο να περιορίζουν τη ζημιά μιας πιθανής κυβερνοεπίθεσης όσο και να ανακάμπτουν από τις επιπτώσεις της. Για να διευκολυνθεί αυτή η οργανωμένη αντίδραση, οργανισμοί κάθε μεγέθους έχουν στραφεί στην ενσωμάτωση δυνατότητας **ανταπόκρισης σε περιστατικά** στις υφιστάμενες πολιτικές, διαδικασίες και διεργασίες τους.

Για την οικοδόμηση αυτής της δυνατότητας εντός του οργανισμού, πρέπει να αντιμετωπιστούν αρκετά βασικά στοιχεία. Πρώτον, οι οργανισμοί χρειάζεται να διαθέτουν λειτουργική γνώση της **διαδικασίας ανταπόκρισης σε περιστατικά**. Η διαδικασία αυτή περιγράφει τη γενική ροή ενός περιστατικού και τις γενικές ενέργειες που εκτελούνται σε κάθε στάδιο. Δεύτερον, οι οργανισμοί πρέπει να έχουν πρόσβαση σε προσωπικό που θα αποτελέσει τον πυρήνα κάθε δυνατότητας ανταπόκρισης σε περιστατικά. Αφού συγκροτηθεί η ομάδα, απαιτείται η δημιουργία ενός επίσημου σχεδίου και των σχετικών διαδικασιών. Το γραπτό αυτό σχέδιο και οι διαδικασίες αποτελούν την οργανωμένη δομή που μπορεί να ακολουθηθεί κατά τη διάρκεια ενός περιστατικού. Τέλος, με αυτό το πλαίσιο σε εφαρμογή, το σχέδιο πρέπει να αξιολογείται, να δοκιμάζεται και να βελτιώνεται συνεχώς καθώς αναδύονται νέες απειλές. Η αξιοποίηση αυτού του πλαισίου τοποθετεί τους οργανισμούς σε πλεονεκτική θέση ώστε να είναι έτοιμοι για τη δυσάρεστη πραγματικότητα που πολλοί έχουν ήδη βιώσει: ένα περιστατικό που θέτει σε κίνδυνο την ασφάλειά τους.

Σε αυτό το κεφάλαιο θα καλυφθούν τα εξής θέματα:

- Η διαδικασία ανταπόκρισης σε περιστατικά

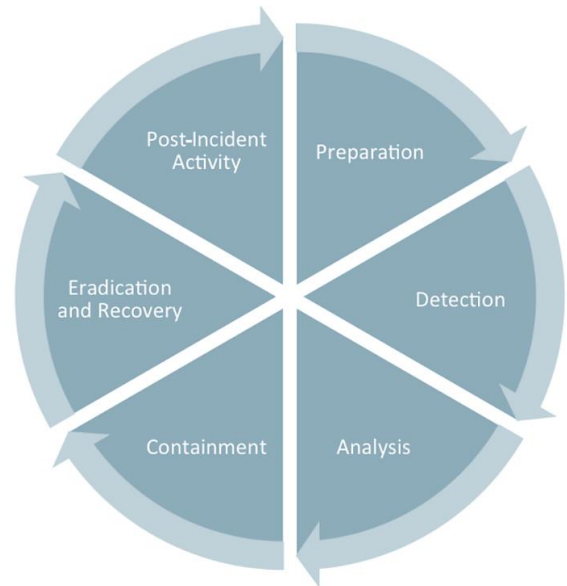
- Το πλαίσιο ανταπόκρισης σε περιστατικά
- Το σχέδιο ανταπόκρισης σε περιστατικά
- Το εγχειρίδιο ενεργειών (*playbook*) ανταπόκρισης σε περιστατικά
- Ο έλεγχος του πλαισίου ανταπόκρισης σε περιστατικά

1.1. Η διαδικασία ανταπόκρισης σε περιστατικά

Υπάρχει μια γενική πορεία που ακολουθούν τα περιστατικά κυβερνοασφάλειας κατά τη διάρκεια του κύκλου ζωής τους. Εάν ένας οργανισμός διαθέτει ώριμη ικανότητα ανταπόκρισης σε περιστατικά, θα έχει λάβει μέτρα ώστε να είναι έτοιμος να αντιμετωπίσει ένα περιστατικό σε κάθε στάδιο της διαδικασίας. Κάθε περιστατικό ξεκινά από τη στιγμή που ο οργανισμός αντιλαμβάνεται για πρώτη φορά ένα γεγονός ή μια σειρά γεγονότων που υποδεικνύουν κακόβουλη δραστηριότητα.

Η ανίχνευση αυτή μπορεί να προέλθει είτε από ειδοποίηση ενός μηχανισμού ασφαλείας είτε από ενημέρωση που παρέχεται από κάποιον εξωτερικό φορέα για ένα πιθανό ζήτημα ασφαλείας. Αφού ενεργοποιηθεί ο συναγερμός, ο οργανισμός προχωρά στην ανάλυση του περιστατικού, εφαρμόζει μέτρα περιορισμού και στη συνέχεια επιδιώκει να επαναφέρει το πληροφοριακό σύστημα σε κανονική λειτουργία.

Το παρακάτω διάγραμμα απεικονίζει τη ροή αυτής της διαδικασίας ως έναν κύκλο, με την **Προετοιμασία** ως αφετηρία. Με πιο προσεκτική εξέταση διαπιστώνεται ότι κάθε περιστατικό συμβάλλει στο να βελτιωθεί περαιτέρω η προετοιμασία του οργανισμού για μελλοντικά περιστατικά. Αυτό επιτυγχάνεται μέσω της φάσης της **Μετα-Περιστασιακής Δραστηριότητας**, η οποία αξιοποιείται εκ νέου στην προετοιμασία.



1.2. Η διαδικασία ανταπόκρισης σε περιστατικά

Η διαδικασία ανταπόκρισης σε περιστατικά μπορεί να χωριστεί σε έξι διακριτές φάσεις, καθεμία από τις οποίες περιλαμβάνει ενέργειες που μπορεί να εκτελέσει ένας οργανισμός για την αντιμετώπιση του περιστατικού:

1. Προετοιμασία (Preparation): Χωρίς σωστή προετοιμασία, οποιαδήποτε επόμενη προσπάθεια ανταπόκρισης θα είναι ανοργάνωτη και μπορεί να επιδεινώσει την κατάσταση. Ένα από τα πιο κρίσιμα στοιχεία είναι η δημιουργία ενός **σχεδίου ανταπόκρισης σε περιστατικά**. Αφού αυτό τεθεί σε

εφαρμογή με το κατάλληλο προσωπικό, πρέπει να διασφαλιστεί ότι οι υπεύθυνοι για την ανταπόκριση έχουν λάβει την κατάλληλη εκπαίδευση. Αυτό περιλαμβάνει διαδικασίες, πρωτόκολλα και επιπλέον εργαλεία απαραίτητα για τη διερεύνηση ενός περιστατικού. Επιπλέον, πρέπει να αποκτηθεί και να ενσωματωθεί υλικό και λογισμικό ψηφιακής εγκληματολογίας. Τέλος, τακτικές ασκήσεις είναι αναγκαίες ώστε ο οργανισμός να είναι εξοικειωμένος με τη διαδικασία.

2. Ανίχνευση (Detection): Η ανίχνευση πιθανών περιστατικών είναι μια σύνθετη διαδικασία. Ανάλογα με το μέγεθος του οργανισμού, μπορεί να καταγράφονται πάνω από 100 εκατομμύρια γεγονότα ημερησίως. Αυτά μπορεί να είναι είτε νόμιμες ενέργειες στο πλαίσιο της επιχειρησιακής λειτουργίας είτε ενδείξεις κακόβουλης δραστηριότητας. Σε αυτόν τον τεράστιο όγκο δεδομένων προστίθενται οι συνεχείς ειδοποιήσεις από μηχανισμούς ασφαλείας, με αποτέλεσμα οι αναλυτές να κατακλύζονται από πληροφορίες και να πρέπει να διαχωρίσουν τα πραγματικά σημαντικά στοιχεία από τον «θόρυβο». Ακόμη και τα πιο σύγχρονα εργαλεία **SIEM (Security Incident and Event Management)** χάνουν την αποτελεσματικότητά τους αν δεν ενημερώνονται τακτικά με νέους κανόνες ανίχνευσης. Στη φάση της ανίχνευσης ο οργανισμός αντιλαμβάνεται για πρώτη φορά ένα ή περισσότερα γεγονότα που ενδέχεται να υποδηλώνουν κακόβουλη δραστηριότητα, τα οποία στη συνέχεια χαρακτηρίζονται ως περιστατικό. Για παράδειγμα, ένας αναλυτής μπορεί να λάβει ειδοποίηση ότι χρησιμοποιήθηκε λογαριασμός διαχειριστή την ώρα που ο διαχειριστής βρισκόταν σε άδεια. Η ανίχνευση μπορεί επίσης να προέλθει από εξωτερικές πηγές, όπως ένας ISP ή μια υπηρεσία επιβολής νόμου. Ακόμη και απλοί χρήστες μπορεί να είναι οι πρώτοι που θα αναφέρουν πρόβλημα, όπως ένας υπάλληλος που ανοίγει αρχείο Excel από άγνωστη πηγή και διαπιστώνει ότι τα αρχεία του κρυπτογραφούνται. Σε κάθε περίπτωση, τέτοια γεγονότα πρέπει να αναβαθμίζονται σε περιστατικά και να ξεκινά η διερεύνηση.

3. Ανάλυση (Analysis): Μόλις ανιχνευθεί ένα περιστατικό, το προσωπικό του οργανισμού ή μια έμπιστη τρίτη οντότητα ξεκινά τη φάση της ανάλυσης. Σε αυτήν, συλλέγονται αποδεικτικά στοιχεία από μνήμη RAM, αρχεία καταγραφής, δικτυακές συνδέσεις και εκτελούμενες διεργασίες. Ανάλογα με το περιστατικό, η συλλογή μπορεί να διαρκέσει ώρες ή και ημέρες. Στη συνέχεια τα δεδομένα εξετάζονται με εργαλεία ανάλυσης ώστε να διαπιστωθεί τι συνέβη, ποια συστήματα επηρεάστηκαν, αν εμπλέκονται και άλλα συστήματα και αν έχουν αποσπαστεί ευαίσθητα δεδομένα. Στόχος είναι ο εντοπισμός της **αιτίας ρίζας (root cause)** και η ανακατασκευή των ενεργειών του επιτιθέμενου από την αρχική παραβίαση έως την ανίχνευση.

4. Περιορισμός (Containment): Αφού καθοριστεί τι ακριβώς συμβαίνει και ποια συστήματα εμπλέκονται, ο οργανισμός προχωρά σε μέτρα περιορισμού. Σε αυτή τη φάση λαμβάνονται δράσεις για να εμποδιστεί ο επιτιθέμενος να συνεχίσει την παραβίαση, να επικοινωνεί με υποδομές *command and control* ή να εξάγει δεδομένα. Οι στρατηγικές περιορισμού μπορεί να περιλαμβάνουν τον αποκλεισμό θυρών και IP διευθύνσεων στο firewall ή ακόμη και την αποσύνδεση ενός μολυσμένου μηχανήματος από το δίκτυο. Κάθε είδος περιστατικού απαιτεί διαφορετική τακτική περιορισμού, αλλά η ύπαρξη πολλών επιλογών αυξάνει τις πιθανότητες επιτυχίας.

5. Εξάλειψη και αποκατάσταση (Eradication and Recovery): Στη φάση εξάλειψης, ο οργανισμός απομακρύνει τον επιτιθέμενο από το δίκτυο. Σε περίπτωση μόλυνσης με κακόβουλο λογισμικό, μπορεί

να χρησιμοποιηθεί ενισχυμένη λύση anti-malware ή να γίνει επανεγκατάσταση συστημάτων. Μπορεί επίσης να απαιτηθεί απενεργοποίηση ή αλλαγή συμβιβασμένων λογαριασμών χρηστών. Αν η επίθεση εκμεταλλεύτηκε κάποια ευπάθεια, εγκαθίστανται τα σχετικά patches ή ενημερώσεις λογισμικού. Η αποκατάσταση ευθυγραμμίζεται με τα σχέδια **συνέχειας λειτουργίας (Business Continuity)** ή **ανάκαμψης από καταστροφή (Disaster Recovery)** του οργανισμού. Σε αυτό το στάδιο, γίνεται επανεγκατάσταση λειτουργικών συστημάτων και εφαρμογών, επαναφορά δεδομένων από backup και έλεγχος λογαριασμών χρηστών/διαχειριστών ώστε να μην παραμένουν «ανοικτές πόρτες» που δημιούργησαν οι επιτιθέμενοι. Τέλος, πραγματοποιείται εκτενής έλεγχος ευπαθειών για να διασφαλιστεί ότι δεν παραμένει κάτι αξιοποιήσιμο.

6. Μετα-περιστασιακή δραστηριότητα (Post-incident activity): Στο τέλος της διαδικασίας πραγματοποιείται πλήρης ανασκόπηση του περιστατικού με όλους τους βασικούς εμπλεκόμενους. Αυτό περιλαμβάνει αξιολόγηση των ενεργειών που έγιναν: τι λειτούργησε σωστά και, πιο σημαντικό, τι δεν λειτούργησε. Οι συζητήσεις αυτές αναδεικνύουν στοιχεία που επηρέασαν θετικά ή αρνητικά την ανταπόκριση. Σε αυτό το στάδιο συντάσσεται αναλυτική γραπτή αναφορά, η οποία καταγράφει με σαφήνεια την αλληλουχία των γεγονότων και την αιτία ρίζας, εφόσον βρέθηκε. Η αναφορά πρέπει να είναι κατανοητή και από άτομα εκτός του τμήματος πληροφορικής, αποφεύγοντας υπερβολική τεχνική ορολογία. Τέλος, ο οργανισμός οφείλει να ενημερώσει τις διαδικασίες ανταπόκρισης με τα **διδάγματα που αντλήθηκαν**, ώστε οι μελλοντικές ανταποκρίσεις να είναι πιο αποτελεσματικές.

2

Ο ρόλος της ψηφιακής εγκληματολογίας

Υπάρχει μια παρανόηση που συχνά διατηρούν άτομα τα οποία δεν είναι εξοικειωμένα με τον χώρο της ανταπόκρισης σε περιστατικά. Η παρανόηση αυτή είναι ότι η ανταπόκριση σε περιστατικά αφορά αποκλειστικά την ψηφιακή εγκληματολογία (*digital forensics*). Ως αποτέλεσμα, συχνά συγχέουν τους δύο όρους. Παρόλο που η ψηφιακή εγκληματολογία αποτελεί κρίσιμο συστατικό στοιχείο της διαδικασίας ανταπόκρισης (και γι' αυτόν τον λόγο περιλαμβάνονται αρκετά κεφάλαια στο παρόν βιβλίο σχετικά με αυτήν), η αντιμετώπιση ενός περιστατικού δεν περιορίζεται μόνο στην εξέταση σκληρών δίσκων.

Είναι προτιμότερο να θεωρείται η εγκληματολογία ως **υποστηρικτική λειτουργία** της συνολικής διαδικασίας ανταπόκρισης. Η ψηφιακή εγκληματολογία λειτουργεί ως ο μηχανισμός για την κατανόηση των τεχνικών πτυχών του περιστατικού, τον πιθανό εντοπισμό της βασικής αιτίας, καθώς και την ανακάλυψη μη εξουσιοδοτημένων προσβάσεων ή άλλων κακόβουλων ενεργειών. Για παράδειγμα, κάποια περιστατικά, όπως οι επιθέσεις **άρνησης υπηρεσίας (DoS)**, απαιτούν ελάχιστη ή και καθόλου εγκληματολογική ανάλυση. Αντίθετα, μια παραβίαση δικτύου που περιλαμβάνει τον συμβιβασμό ενός εσωτερικού διακομιστή και **κίνηση Command and Control (C2)** προς το εξωτερικό θα απαιτήσει εκτενή εξέταση αρχείων καταγραφής, ανάλυση δικτυακής κίνησης και διερεύνηση της μνήμης συστήματος. Από μια τέτοια ανάλυση μπορεί να εξαχθεί η αιτία ρίζας. Και στις δύο περιπτώσεις, ο οργανισμός επηρεάζεται από το περιστατικό, αλλά η εγκληματολογία παίζει σαφώς σημαντικότερο ρόλο στη δεύτερη.

Η ανταπόκριση σε περιστατικά αποτελεί μια λειτουργία ασφάλειας πληροφοριών που αξιοποιεί τις μεθοδολογίες, τα εργαλεία και τις τεχνικές της ψηφιακής εγκληματολογίας, αλλά προχωρά πέρα από αυτά, αντιμετωπίζοντας πρόσθετα στοιχεία. Αυτά περιλαμβάνουν τον περιορισμό πιθανών κακόβουλων λογισμικών ή άλλων εκμεταλλεύσεων, τον εντοπισμό και τη διόρθωση ευπαθειών, καθώς και τη διαχείριση τεχνικού και μη τεχνικού προσωπικού. Ορισμένα περιστατικά μπορεί να απαιτούν ανάλυση δεδομένων μνήμης ή αποδεικτικών στοιχείων από hosts, ενώ άλλα να χρειάζονται απλώς ανασκόπηση καταγραφών firewall. Σε κάθε περίπτωση, οι υπεύθυνοι ακολουθούν τη διαδικασία ανταπόκρισης σε περιστατικά.

2.1. Το πλαίσιο ανταπόκρισης σε περιστατικά

Η ανταπόκριση σε μια παραβίαση δεδομένων, μια επίθεση ransomware ή οποιοδήποτε άλλο περιστατικό ασφαλείας **δεν πρέπει ποτέ να είναι μια αποσπασματική διαδικασία**. Η έλλειψη καθορισμένων διαδικασιών αφήνει τον οργανισμό ανίκανο να προσδιορίσει την έκταση του περιστατικού και να το περιορίσει έγκαιρα ώστε να μειώσει τη ζημιά. Επιπλέον, η προσπάθεια δημιουργίας σχεδίου δράσης την ώρα του περιστατικού ενδέχεται να καταστρέψει κρίσιμα αποδεικτικά στοιχεία ή, ακόμη χειρότερα, να δημιουργήσει περισσότερα προβλήματα.

Η κατανόηση της διαδικασίας απόκρισης σε περιστατικά αποτελεί μόνο το πρώτο βήμα για την οικοδόμηση αυτής της ικανότητας μέσα σε έναν οργανισμό. Αυτό που χρειάζονται οι οργανισμοί είναι ένα πλαίσιο που να αξιοποιεί τις διαθέσιμες πηγές του οργανισμού και να θέτει σε εφαρμογή τις διαδικασίες αυτές. Το πλαίσιο απόκρισης σε περιστατικά περιγράφει τα συστατικά μιας λειτουργικής ικανότητας απόκρισης σε περιστατικά εντός του οργανισμού. Το πλαίσιο αυτό αποτελείται από στοιχεία όπως το προσωπικό, οι πολιτικές και οι διαδικασίες. Μέσω αυτών των στοιχείων, ο οργανισμός χτίζει την ικανότητά του να ανταποκρίνεται σε περιστατικά.

2.2. Ο Χάρτης Απόκρισης σε Περιστατικά

Το πρώτο βήμα για την ανάπτυξη αυτής της ικανότητας είναι η απόφαση της ανώτερης διοίκησης ότι ο κίνδυνος για τον οργανισμό είναι υπερβολικά σημαντικός ώστε να αγνοηθεί η πιθανότητα ενός ενδεχόμενου περιστατικού ασφάλειας. Όταν ληφθεί αυτή η απόφαση, ένα ανώτερο στέλεχος του οργανισμού θα αναλάβει ρόλο χορηγού έργου και θα εκπονήσει τον χάρτη απόκρισης σε περιστατικά. Ο χάρτης αυτός περιλαμβάνει βασικά στοιχεία που θα οδηγήσουν στη δημιουργία μιας Ομάδας Απόκρισης σε Περιστατικά Ασφάλειας Υπολογιστών (Computer Security Incident Response Team - CSIRT).

Παρόλο που υπάρχουν διάφορες ονομασίες για τις ομάδες απόκρισης σε περιστατικά, ο όρος **CERT** συχνά συνδέεται με την **US-CERT** του Υπουργείου Εσωτερικής Ασφάλειας των Ηνωμένων Πολιτειών ή με το **CERT/CC** του Ινστιτούτου Μηχανικής Λογισμικού του Carnegie Mellon. Για τους σκοπούς μας, θα χρησιμοποιήσουμε τον πιο γενικό όρο **CSIRT**.

Ο χάρτης απόκρισης σε περιστατικά πρέπει να είναι ένα γραπτό έγγραφο που να καλύπτει τα εξής:

- **Εξασφάλιση υποστήριξης από την ανώτερη διοίκηση:** Για να αποτελέσει βιώσιμο μέρος του οργανισμού, το CSIRT απαιτεί την υποστήριξη της ανώτερης διοίκησης. Σε έναν ιδιωτικό οργανισμό, μπορεί να είναι δύσκολη η εξασφάλιση της απαραίτητης στήριξης και χρηματοδότησης, καθώς το CSIRT δεν αποφέρει άμεσα έσοδα με τον ίδιο τρόπο που το κάνει το μάρκετινγκ ή οι πωλήσεις. Αυτό που πρέπει να γίνει κατανοητό είναι ότι το CSIRT λειτουργεί ως «ασφαλιστήριο συμβόλαιο» σε περίπτωση που συμβεί το χειρότερο. Με αυτόν τον τρόπο, το CSIRT μπορεί να δικαιολογήσει την ύπαρξή του μειώνοντας τον αντίκτυπο των περιστατικών και συνεπώς το κόστος που συνδέεται με μια παραβίαση ασφαλείας ή άλλη κακόβουλη δραστηριότητα.

- **Ορισμός του πεδίου ευθύνης (constituency):** Το πεδίο ευθύνης καθορίζει σαφώς ποια τμήματα και τομείς του οργανισμού υπάγονται στο CSIRT. Ορισμένοι οργανισμοί διαθέτουν διάφορες διευθύνσεις ή θυγατρικές που, για οποιονδήποτε λόγο, μπορεί να μην αποτελούν μέρος της ευθύνης του CSIRT. Το πεδίο ευθύνης μπορεί να οριστεί είτε ως ένας τομέας (domain), όπως π.χ. local.example.com, είτε ως το όνομα του οργανισμού, π.χ. **ACME Inc.**, μαζί με τις συνδεδεμένες θυγατρικές του.
- **Διαμόρφωση δήλωσης αποστολής (mission statement):** Η σταδιακή επέκταση των ευθυνών του CSIRT (mission creep) μπορεί να συμβεί χωρίς σαφή καθορισμό του σκοπού του. Για να αποφευχθεί αυτό, μια σαφώς διατυπωμένη δήλωση αποστολής θα πρέπει να ενταχθεί στο γραπτό σχέδιο ασφάλειας πληροφοριών. Για παράδειγμα: *Η αποστολή του CSIRT της ACME Inc. είναι να παρέχει έγκαιρη ανάλυση και δράσεις για περιστατικά ασφάλειας που επηρεάζουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριακών συστημάτων και του προσωπικού της ACME Inc.*
- **Καθορισμός υπηρεσιών (service delivery):** Εκτός από τη δήλωση αποστολής, μια σαφώς ορισμένη λίστα υπηρεσιών μπορεί επίσης να μειώσει τον κίνδυνο σταδιακής επέκτασης του ρόλου του CSIRT. Οι υπηρεσίες διακρίνονται συνήθως σε δύο κατηγορίες:
 - ο **Προληπτικές υπηρεσίες (Proactive services):** Περιλαμβάνουν την εκπαίδευση προσωπικού εκτός CSIRT, την παροχή ενημερώσεων για αναδυόμενες απειλές, τη δοκιμή και την ανάπτυξη εργαλείων ασφαλείας όπως EDR, καθώς και τη στήριξη λειτουργιών ασφαλείας με τη δημιουργία κανόνων IDS/IPS.
 - ο **Αντιδραστικές υπηρεσίες (Reactive services):** Επικεντρώνονται κυρίως στην απόκριση σε περιστατικά καθώς αυτά λαμβάνουν χώρα. Αυτό περιλαμβάνει τη συλλογή και ανάλυση αποδεικτικών στοιχείων, τη συνδρομή στη φάση περιορισμού, εξάλειψης και αποκατάστασης, καθώς και την τελική τεκμηρίωση του περιστατικού.

Ένα ακόμη κρίσιμο όφελος ενός ρητά διατυπωμένου χάρτη είναι η **κοινωνικοποίηση του CSIRT εντός του οργανισμού**. Αυτό γίνεται για να εξαλειφθούν φήμες ή εικασίες σχετικά με τον σκοπό της ομάδας. Οι εργαζόμενοι μπορεί να ακούσουν όρους όπως «ψηφιακές έρευνες» ή «ομάδα απόκρισης σε περιστατικά» και να πιστέψουν ότι ο οργανισμός δημιουργεί μια «μυστική αστυνομία» που θα εντοπίζει παραπτώματα εργαζομένων. Για να αποφευχθεί αυτό, μια σύντομη δήλωση που θα περιλαμβάνει την αποστολή του CSIRT μπορεί να κοινοποιείται σε όλους τους εργαζόμενους. Επιπλέον, το CSIRT μπορεί να παρέχει περιοδικές ενημερώσεις στην ανώτερη διοίκηση σχετικά με τα περιστατικά που έχουν αντιμετωπιστεί, προκειμένου να καταδεικνύεται ο σκοπός της ομάδας.

2.3. Στελέχωση CSIRT

Μόλις ολοκληρωθεί ο χάρτης αποστολής της απόκρισης σε περιστατικά (incident response charter), το επόμενο στάδιο είναι η στελέχωση του CSIRT. Οι μεγαλύτεροι οργανισμοί με επαρκείς πόρους

ενδέχεται να είναι σε θέση να αναθέσουν στα άτομα καθήκοντα απόκρισης σε περιστατικά με πλήρη απασχόληση. Ωστόσο, συχνότερα, οι οργανισμοί χρειάζεται να αξιοποιούν προσωπικό που έχει και άλλες υποχρεώσεις πέρα από την απόκριση σε περιστατικά. Το εσωτερικό προσωπικό που απαρτίζει το CSIRT μπορεί να χωριστεί σε τρεις κατηγορίες:

- **βασική ομάδα (core team)**
- **τεχνική υποστήριξη (technical support)**
- **οργανωτική υποστήριξη (organizational support)**

Κάθε άτομο εντός του CSIRT αναλαμβάνει έναν συγκεκριμένο ρόλο. Η δημιουργία αυτής της δυνατότητας σε έναν οργανισμό απαιτεί περισσότερα από την απλή ανάθεση προσωπικού και τη σύνταξη εγγράφων πολιτικής και διαδικασιών. Όπως σε κάθε μεγάλο έργο, απαιτείται σημαντική προσπάθεια ώστε να δημιουργηθεί ένα λειτουργικό CSIRT.

Για κάθε κατηγορία του CSIRT υπάρχουν συγκεκριμένοι ρόλοι και ευθύνες. Το ευρύ αυτό φάσμα στελεχών έχει σχεδιαστεί ώστε να παρέχει καθοδήγηση και υποστήριξη σε περιστατικά που κυμαίνονται από μικρής έως καταστροφικής κλίμακας.

2.4. Βασική Ομάδα CSIRT (CSIRT core team)

Η βασική ομάδα του CSIRT αποτελείται από προσωπικό που έχει καθήκοντα απόκρισης σε περιστατικά ως πλήρη απασχόληση ή αναλαμβάνει τις σχετικές δραστηριότητες όταν απαιτείται. Σε πολλές περιπτώσεις, η βασική ομάδα αποτελείται από μέλη της ομάδας ασφάλειας πληροφοριών. Άλλοι οργανισμοί μπορούν να αξιοποιήσουν προσωπικό με εξειδίκευση στην απόκριση σε περιστατικά.

Συντονιστής απόκρισης σε περιστατικά (Incident Response Coordinator): Αποτελεί κρίσιμο στοιχείο κάθε CSIRT. Χωρίς σαφή ηγεσία, η απόκριση σε ένα πιθανό περιστατικό μπορεί να είναι ανοργάνωτη ή να επικρατεί χάος λόγω διαφορετικών ατόμων που διεκδικούν τον έλεγχο, κάτι που μπορεί να επιδεινώσει την κατάσταση. Συχνά, ο ρόλος αυτός αναλαμβάνεται από τον Chief Security Officer (CSO), τον Chief Information Security Officer (CISO) ή τον Information Security Officer (ISO), καθώς το συγκεκριμένο άτομο έχει συνήθως τη συνολική ευθύνη για την ασφάλεια των πληροφοριών του οργανισμού.

Ο συντονιστής απόκρισης:

- Διαχειρίζεται το CSIRT πριν, κατά τη διάρκεια και μετά από ένα περιστατικό.
- Εξασφαλίζει ότι τα σχέδια και οι πολιτικές του CSIRT επανεξετάζονται και επικαιροποιούνται.
- Διασφαλίζει ότι η ομάδα έχει την κατάλληλη εκπαίδευση, οργανώνει δοκιμές και ασκήσεις.

- Κατά τη διάρκεια ενός περιστατικού, καθοδηγεί την ομάδα στη διαδικασία απόκρισης και αποκατάστασης, διασφαλίζοντας τη συνεργασία με την ανώτερη διοίκηση (π.χ. CEO).
- Μεταφράζει την τεχνική ορολογία σε γλώσσα κατανοητή από μη τεχνικά στελέχη.
- Μετά την ολοκλήρωση του περιστατικού, μεριμνά για την κατάλληλη τεκμηρίωση, την αποστολή αναφορών στους εσωτερικούς και εξωτερικούς εμπλεκόμενους και την ενσωμάτωση των διδαγμάτων στο σχέδιο CSIRT.

Ανώτεροι αναλυτές CSIRT (CSIRT senior analysts): Διαθέτουν εκτενή εκπαίδευση και εμπειρία στην απόκριση σε περιστατικά, στη ψηφιακή εγκληματολογία (digital forensics) και στην ανάλυση δεδομένων δικτύου. Συνήθως έχουν πολυετή εμπειρία είτε ως σύμβουλοι είτε ως μέλη ενός εταιρικού CSIRT.

Καθήκοντα:

- Διασφαλίζουν την κατάρτιση και τις δεξιότητές τους.
- Συμμετέχουν στη διαμόρφωση και την αναθεώρηση του σχεδίου απόκρισης.
- Εκπαιδεύουν νεότερα μέλη της ομάδας.
- Κατά τη διάρκεια ενός περιστατικού, συλλέγουν και αναλύουν αποδεικτικά στοιχεία, κατευθύνουν δραστηριότητες περιορισμού (containment), και υποστηρίζουν στην αποκατάσταση.
- Μετά το περιστατικό, τεκμηριώνουν τις ενέργειες, ετοιμάζουν αναφορές και διαχειρίζονται τα αποδεικτικά στοιχεία.

Αναλυτές CSIRT (CSIRT analysts): Διαθέτουν μικρότερη εμπειρία (1–2 χρόνια) και εργάζονται υπό καθοδήγηση ανώτερων αναλυτών.

Καθήκοντα:

- Εξελίσσουν τις δεξιότητές τους μέσω εκπαίδευσης και ασκήσεων.
- Συμμετέχουν σε αναθεωρήσεις σχεδίων απόκρισης.
- Συλλέγουν δεδομένα από πιθανά επηρεασμένα συστήματα, δικτυακές συσκευές ή αρχεία καταγραφής (logs).
- Συμμετέχουν στην ανάλυση στοιχείων και στη διαδικασία αποκατάστασης.

Αναλυτές Κέντρου Επιχειρήσεων Ασφάλειας (SOC analysts): Μεγάλες επιχειρήσεις διαθέτουν 24/7 Κέντρο Επιχειρήσεων Ασφάλειας (SOC). Οι αναλυτές αυτοί εντοπίζουν και ειδοποιούν για περιστατικά και αποτελούν την «πρώτη γραμμή» στην ανίχνευση και αρχική απόκριση.

Μηχανικοί/Αναλυτές Ασφάλειας Πληροφοριακών Συστημάτων (IT security engineers/analysts): Αναλαμβάνουν την ανάπτυξη, συντήρηση και παρακολούθηση εργαλείων και συσκευών ασφαλείας (antivirus, firewalls, SIEM).

Καθήκοντα:

- Διασφαλίζουν ότι τα συστήματα ασφαλείας είναι σωστά ρυθμισμένα ώστε να εντοπίζουν πιθανά περιστατικά και να καταγράφουν γεγονότα.
- Κατά τη διάρκεια ενός περιστατικού, παρακολουθούν τα συστήματα ασφαλείας για ενδείξεις κακόβουλης δραστηριότητας και συλλέγουν σχετικά στοιχεία.
- Μετά το περιστατικό, ρυθμίζουν τα συστήματα ώστε να παρακολουθούν πιθανές επαναλήψεις της κακόβουλης δραστηριότητας.

2.5. Τεχνικό Προσωπικό Υποστήριξης (Technical support personnel)

Το τεχνικό προσωπικό υποστήριξης αποτελείται από άτομα εντός του οργανισμού που δεν έχουν δραστηριότητες CSIRT ως μέρος των καθημερινών τους αρμοδιοτήτων, αλλά διαθέτουν εξειδίκευση ή πρόσβαση σε συστήματα και διαδικασίες που ενδέχεται να επηρεαστούν από ένα περιστατικό.

Για παράδειγμα, το CSIRT μπορεί να χρειαστεί να συνεργαστεί με έναν διαχειριστή διακομιστών (server administrator) ώστε να βοηθήσει τη βασική ομάδα στην απόκτηση αποδεικτικών στοιχείων από διακομιστές, όπως λήψη μνήμης (memory captures), εξαγωγή εικονικών συστημάτων ή αντιγραφή αρχείων καταγραφής (log files). Μόλις ολοκληρωθεί αυτή η διαδικασία, ο ρόλος του διαχειριστή διακομιστών τερματίζεται και ενδέχεται να μην έχει περαιτέρω εμπλοκή με το περιστατικό. Τα παρακάτω είναι παραδείγματα προσωπικού που μπορεί να υποστηρίξει το CSIRT κατά τη διάρκεια ενός περιστατικού:

Αρχιτέκτονας/Διαχειριστής Δικτύου (Network architect/administrator): Τα περιστατικά συχνά αφορούν την υποδομή δικτύου, όπως επιθέσεις σε δρομολογητές (routers), μεταγωγείς (switches) και άλλο δικτυακό υλικό και λογισμικό. Ο αρχιτέκτονας ή διαχειριστής δικτύου είναι ζωτικής σημασίας για την κατανόηση του φυσιολογικού και μη φυσιολογικού τρόπου λειτουργίας αυτών των συσκευών, καθώς και για τον εντοπισμό ανώμαλης δικτυακής κίνησης. Σε περιστατικά που σχετίζονται με την υποδομή δικτύου, το προσωπικό αυτό μπορεί να βοηθήσει στην απόκτηση αποδεικτικών στοιχείων, όπως αρχεία πρόσβασης (access logs) ή καταγραφές πακέτων (packet captures).

Διαχειριστής Διακομιστών (Server administrator): Οι επιτιθέμενοι συχνά στοχεύουν συστήματα του δικτύου όπου αποθηκεύονται κρίσιμα ή ευαίσθητα δεδομένα. Οι διακομιστές υψηλής αξίας συχνά περιλαμβάνουν domain controllers, file servers ή database servers. Οι διαχειριστές διακομιστών μπορούν να βοηθήσουν στην απόκτηση αρχείων καταγραφής (logs) από αυτά τα συστήματα. Εάν είναι επίσης υπεύθυνοι για τη συντήρηση της δομής του Active Directory, μπορούν να βοηθήσουν

στον εντοπισμό νέων λογαριασμών χρηστών ή αλλαγών σε υπάρχοντες λογαριασμούς χρηστών ή διαχειριστών.

Υποστήριξη Εφαρμογών (Application support): Οι διαδικτυακές εφαρμογές αποτελούν βασικό στόχο για επιτιθέμενους. Αδυναμίες στον κώδικα που επιτρέπουν επιθέσεις όπως SQL injection ή λανθασμένες ρυθμίσεις ασφαλείας είναι υπεύθυνες για σημαντικές παραβιάσεις. Η συμμετοχή προσωπικού υποστήριξης εφαρμογών στο CSIRT διευκολύνει την απόκτηση πληροφοριών άμεσα σχετιζόμενων με επιθέσεις σε εφαρμογές. Τα άτομα αυτά μπορούν να αναγνωρίσουν αλλαγές στον κώδικα ή να επιβεβαιώσουν ευπάθειες που εντοπίστηκαν κατά τη διερεύνηση μιας πιθανής επίθεσης.

Υποστήριξη Επιτραπέζιων Συστημάτων (Desktop support): Το προσωπικό υποστήριξης επιτραπέζιων συστημάτων συχνά είναι υπεύθυνο για τη συντήρηση ελέγχων όπως η πρόληψη απώλειας δεδομένων (Data Loss Prevention – DLP) και το antivirus σε επιτραπέζιους υπολογιστές. Σε περίπτωση περιστατικού, μπορούν να παρέχουν στο CSIRT αρχεία καταγραφής και άλλα αποδεικτικά στοιχεία. Επίσης, μπορεί να είναι υπεύθυνοι για τον καθαρισμό μολυσμένων συστημάτων κατά τη φάση αποκατάστασης.

Γραφείο Υποστήριξης (Help desk): Ανάλογα με τον οργανισμό, το προσωπικό του help desk συχνά αποτελεί τον «προειδοποιητικό δείκτη» (canary in the coal mine) για τον εντοπισμό περιστατικών. Είναι συχνά τα πρώτα άτομα που ειδοποιούνται όταν ένας χρήστης παρατηρεί σημάδια μόλυνσης από κακόβουλο λογισμικό ή άλλης κακόβουλης δραστηριότητας. Επομένως, το προσωπικό του help desk θα πρέπει να εκπαιδεύεται σε διαδικασίες απόκρισης του CSIRT και να γνωρίζει τον ρόλο του στον εντοπισμό και την κλιμάκωση περιστατικών. Επιπλέον, μπορούν να βοηθήσουν στον εντοπισμό επιπλέον επηρεασμένων χρηστών σε περίπτωση εκτεταμένου περιστατικού.

2.6. Οργανωτικό Προσωπικό Υποστήριξης (Organizational support personnel)

Εκτός από τον τεχνικό τομέα, υπάρχουν και άλλα μέλη του οργανισμού που θα πρέπει να περιλαμβάνονται στο CSIRT. Το οργανωτικό προσωπικό μπορεί να συνδράμει σε ποικιλία μη τεχνικών θεμάτων που δεν καλύπτονται από τη βασική ομάδα και το τεχνικό προσωπικό υποστήριξης του CSIRT. Αυτά περιλαμβάνουν τη διαχείριση του εσωτερικού και εξωτερικού νομικού πλαισίου, την υποστήριξη επικοινωνίας με πελάτες ή την παροχή υποστήριξης στο προσωπικό του CSIRT κατά τη διάρκεια επιτόπιων ενεργειών. Παρακάτω παρουσιάζονται μερικές από τις κατηγορίες οργανωτικού προσωπικού που πρέπει να περιλαμβάνονται στο σχέδιο του CSIRT:

Νομική Υπηρεσία (Legal): Οι παραβιάσεις δεδομένων και άλλα περιστατικά συνεπάγονται μια σειρά από νομικά ζητήματα. Σε πολλές χώρες ισχύουν νόμοι περί ειδοποίησης παραβίασης, οι οποίοι υποχρεώνουν τους οργανισμούς να ενημερώνουν τους πελάτες τους ότι τα δεδομένα τους τέθηκαν σε κίνδυνο. Επιπλέον, κανονιστικές απαιτήσεις όπως το HIPAA ή το PCI DSS υποχρεώνουν τον επηρεαζόμενο οργανισμό να επικοινωνήσει με διάφορους εξωτερικούς φορείς και να τους ειδοποιήσει για πιθανή παραβίαση. Η ένταξη νομικής εκπροσώπησης από τα πρώτα στάδια της διαδικασίας απόκρισης διασφαλίζει ότι οι ειδοποιήσεις και άλλες νομικές απαιτήσεις ικανοποιούνται έγκαιρα. Σε

περίπτωση που η παραβίαση προήλθε από εσωτερική πηγή (π.χ. υπάλληλο ή εξωτερικό συνεργάτη), ο οργανισμός ενδέχεται να επιδιώξει αποζημίωση μέσω αστικών διαδικασιών. Η συμμετοχή της νομικής υπηρεσίας από νωρίς επιτρέπει πιο τεκμηριωμένη λήψη αποφάσεων σχετικά με τα επόμενα νομικά βήματα.

Ανθρώπινοι Πόροι (Human resources): Ένα σημαντικό ποσοστό περιστατικών στους οργανισμούς διαπράττεται από υπαλλήλους ή εξωτερικούς συνεργάτες. Η διερεύνηση ενεργειών που κυμαίνονται από απάτη έως μαζική κλοπή δεδομένων ενδέχεται να πρέπει να διεξαχθεί από το CSIRT. Σε περίπτωση που το αντικείμενο της διερεύνησης είναι υπάλληλος ή συνεργάτης, το τμήμα ανθρωπίνων πόρων μπορεί να διασφαλίσει ότι οι ενέργειες του CSIRT συμμορφώνονται με την εργατική νομοθεσία και τις πολιτικές της εταιρείας. Αν πρόκειται να τερματιστεί η συνεργασία με υπάλληλο ή εργολάβο, το CSIRT μπορεί να συντονιστεί με το HR ώστε να ολοκληρωθεί όλη η απαραίτητη τεκμηρίωση, μειώνοντας τον κίνδυνο αγωγής για άδικη απόλυση.

Μάρκετινγκ / Επικοινωνία (Marketing/communications): Εάν εξωτερικοί πελάτες ή συνεργάτες ενδέχεται να επηρεαστούν από ένα περιστατικό, όπως μια επίθεση DoS ή παραβίαση δεδομένων, το τμήμα επικοινωνίας μπορεί να συμβάλει στη διαμόρφωση κατάλληλου μηνύματος για την καθυσύχηση των ανησυχιών και την παροχή έγκυρης πληροφόρησης. Η ιστορία έχει δείξει ότι όταν οργανισμοί προσπάθησαν να αποκρύψουν λεπτομέρειες από πελάτες σε περιπτώσεις παραβίασης, δέχτηκαν σοβαρή αρνητική αντίδραση. Ένα σταθερό πλάνο επικοινωνίας, που ενεργοποιείται από νωρίς, μπορεί να μετριάσει σημαντικά τις πιθανές αρνητικές αντιδράσεις πελατών και συνεργατών.

Διεύθυνση Εγκαταστάσεων (Facilities): Το CSIRT μπορεί να χρειάζεται πρόσβαση σε εγκαταστάσεις εκτός ωραρίου ή για παρατεταμένες περιόδους. Το τμήμα εγκαταστάσεων μπορεί να βοηθήσει στην έγκαιρη παροχή πρόσβασης. Μπορεί επίσης να διαθέτει επιπλέον χώρους για χρήση από το CSIRT σε περίπτωση παρατεταμένου περιστατικού που απαιτεί ειδικό χώρο εργασίας και υποδομές.

Εταιρική Ασφάλεια (Corporate security): Το CSIRT ενδέχεται να κληθεί να αντιμετωπίσει περιστατικά κλοπής πόρων δικτύου ή άλλης τεχνολογίας του οργανισμού. Η κλοπή φορητών υπολογιστών ή ψηφιακών μέσων είναι συχνή. Η εταιρική ασφάλεια διαθέτει συχνά πρόσβαση σε υλικό παρακολούθησης από εισόδους και εξόδους, καθώς και σε αρχεία πρόσβασης (access badges) και καταγραφές επισκεπτών. Αυτό επιτρέπει στο CSIRT να ανασυνθέσει τα γεγονότα που οδήγησαν σε μια κλοπή ή σε άλλες καταστάσεις που σχετίζονται με το περιστατικό.

2.7. Εξωτερικοί Πόροι

Πολλοί κλάδοι διαθέτουν επαγγελματικούς οργανισμούς όπου οι επαγγελματίες, ανεξαρτήτως εργοδότη, μπορούν να συναντώνται για να μοιράζονται πληροφορίες. Το προσωπικό του CSIRT μπορεί επίσης να αναλάβει την επικοινωνία με τις αρχές επιβολής του νόμου και κυβερνητικούς φορείς, ειδικά όταν αποτελούν στόχο ως μέρος μιας ευρύτερης επίθεσης που έχει επηρεάσει πολλές παρόμοιες οργανώσεις. Η ύπαρξη σχέσεων με εξωτερικούς οργανισμούς και φορείς μπορεί να

βοηθήσει το CSIRT στην ανταλλαγή πληροφοριών και στην πρόσβαση σε πόρους σε περίπτωση συμβάντος. Αυτοί οι πόροι περιλαμβάνουν:

1. **High Technology Crime Investigation Association (HTCIA):** Το HTCIA είναι μια διεθνής ομάδα επαγγελματιών και φοιτητών με επίκεντρο το υψηλής τεχνολογίας έγκλημα. Οι πόροι περιλαμβάνουν τα πάντα, από τεχνικές ψηφιακής εγκληματολογίας μέχρι πληροφορίες σε επίπεδο επιχειρήσεων που μπορούν να βοηθήσουν το προσωπικό του CSIRT με νέες τεχνικές και μεθόδους. Περισσότερες πληροφορίες: <https://htcia.org/>
2. **InfraGard:** Για τα μέλη του CSIRT και τους επαγγελματίες ασφάλειας πληροφοριών στις Η.Π.Α., το FBI έχει δημιουργήσει μια ιδιωτικο-δημόσια συνεργασία για δικτύωση και ανταλλαγή πληροφοριών. Αυτή η συνεργασία επιτρέπει στα μέλη του CSIRT να μοιράζονται πληροφορίες σχετικά με τάσεις ή να συζητούν προηγούμενες έρευνες. Περισσότερες πληροφορίες: <https://www.infragard.org/>
3. **Αρχές Επιβολής του Νόμου:** Οι αρχές έχουν δει εκρηκτική αύξηση των εγκλημάτων στον κυβερνοχώρο. Ως αντίδραση, πολλές υπηρεσίες επιβολής του νόμου έχουν αυξήσει την ικανότητά τους να διερευνούν εγκλήματα στον κυβερνοχώρο. Η ηγεσία του CSIRT θα πρέπει να καλλιεργήσει σχέσεις με φορείς που διαθέτουν δυνατότητες έρευνας κυβερνοεγκλήματος. Οι αρχές μπορούν να παρέχουν πληροφορίες για συγκεκριμένες απειλές ή εγκλήματα και να δώσουν στο CSIRT οποιεσδήποτε σχετικές πληροφορίες.
4. **Προμηθευτές (Vendors):** Οι εξωτερικοί προμηθευτές μπορούν να αξιοποιηθούν σε περίπτωση συμβάντος, και αυτό που μπορούν να παρέχουν εξαρτάται συχνά από το συγκεκριμένο επιχειρησιακό αντικείμενο. Για παράδειγμα, ο πάροχος λύσης IPS/IDS μιας οργάνωσης μπορεί να βοηθήσει στη δημιουργία προσαρμοσμένων κανόνων ειδοποίησης και αποκλεισμού για την ανίχνευση και περιορισμό κακόβουλης δραστηριότητας. Οι προμηθευτές με δυνατότητες ανάλυσης απειλών μπορούν επίσης να παρέχουν καθοδήγηση σχετικά με δείκτες κακόβουλης δραστηριότητας. Τέλος, ορισμένες οργανώσεις θα χρειαστεί να συνεργαστούν με προμηθευτές ειδικών σε ανταπόκριση σε περιστατικά, όπως η ανάλυση κακόβουλου λογισμικού, όταν αυτές οι δεξιότητες δεν καλύπτονται εσωτερικά.

Ανάλογα με το μέγεθος της οργάνωσης, γίνεται εύκολα αντιληπτό πώς το CSIRT μπορεί να περιλαμβάνει αρκετά άτομα. Είναι κρίσιμο, κατά τη συγκρότηση ολόκληρου του CSIRT, κάθε μέλος να γνωρίζει τους ρόλους και τις ευθύνες του. Κάθε μέλος θα πρέπει επίσης να παρέχει συγκεκριμένες πληροφορίες σχετικά με την εμπειρογνωμοσύνη που μπορεί να αξιοποιηθεί σε όλη τη διαδικασία ανταπόκρισης σε περιστατικά. Αυτό γίνεται ακόμα πιο σημαντικό στο επόμενο μέρος του πλαισίου ανταπόκρισης σε περιστατικά, που είναι η δημιουργία ενός σχεδίου ανταπόκρισης σε περιστατικά.

2.8. Σχέδιο Αντιμετώπισης Περιστατικών

Μετά τη σύνταξη του καταστατικού αντιμετώπισης περιστατικών και τη συγκρότηση της ομάδας CSIRT, το επόμενο βήμα είναι η δημιουργία του σχεδίου αντιμετώπισης περιστατικών. Το σχέδιο αντιμετώπισης περιστατικών είναι το έγγραφο που περιγράφει τη δομή υψηλού επιπέδου της δυνατότητας αντίδρασης ενός οργανισμού. Πρόκειται για ένα έγγραφο υψηλού επιπέδου που λειτουργεί ως θεμέλιο της ομάδας CSIRT. Τα κύρια στοιχεία του σχεδίου αντιμετώπισης περιστατικών είναι τα εξής:

Καταστατικό Αντιμετώπισης Περιστατικών: Το σχέδιο αντιμετώπισης περιστατικών θα πρέπει να περιλαμβάνει τη δήλωση αποστολής και το κοινό-στόχο από το καταστατικό αντιμετώπισης περιστατικών. Αυτό παρέχει συνέχεια μεταξύ της έναρξης της δυνατότητας αντιμετώπισης περιστατικών και του σχεδίου.

Εκτεταμένος κατάλογος υπηρεσιών: Το αρχικό καταστατικό αντιμετώπισης περιστατικών περιλάμβανε γενικές κατηγορίες υπηρεσιών χωρίς λεπτομέρειες. Το σχέδιο αντιμετώπισης περιστατικών πρέπει να περιλαμβάνει συγκεκριμένες λεπτομέρειες για τις υπηρεσίες που θα προσφέρει η ομάδα CSIRT. Για παράδειγμα, αν οι υπηρεσίες εγκληματολογικής ανάλυσης αναφέρονται ως μέρος των προσφερόμενων υπηρεσιών, το σχέδιο μπορεί να δηλώνει ότι αυτές περιλαμβάνουν ανάκτηση στοιχείων από σκληρούς δίσκους, ανάλυση μνήμης και αντίστροφη μηχανική δυνητικά κακόβουλου κώδικα για την υποστήριξη ενός περιστατικού. Αυτό επιτρέπει στην CSIRT να διαχωρίζει σαφώς ένα κανονικό αίτημα, π.χ. για αναζήτηση ενός σκληρού δίσκου για τυχαία διαγραμμένο έγγραφο μη σχετιζόμενο με περιστατικό, από την απεικόνιση ενός σκληρού δίσκου σε συνάρτηση με δηλωμένο περιστατικό.

Προσωπικό CSIRT: Όπως αναφέρθηκε προηγουμένως, πολλά άτομα απαρτίζουν την ομάδα CSIRT. Το σχέδιο αντιμετώπισης περιστατικών θα καθορίζει σαφώς αυτούς τους ρόλους και τις ευθύνες. Οι οργανισμοί θα πρέπει να επεκταθούν πέρα από ένα όνομα και τίτλο και να ορίσουν ακριβώς τους ρόλους και τις ευθύνες κάθε μέλους. Δεν είναι επιθυμητό να υπάρξει «σύγκρουση αρμοδιοτήτων» κατά τη διάρκεια ενός περιστατικού, και η σαφής οριοθέτηση των ρόλων μειώνει σημαντικά αυτή την πιθανότητα.

Κατάλογος επαφών: Ένας ενημερωμένος κατάλογος επαφών πρέπει να αποτελεί μέρος του σχεδίου αντιμετώπισης περιστατικών. Ανάλογα με τον οργανισμό, η CSIRT μπορεί να χρειαστεί να ανταποκριθεί σε περιστατικά 24 ώρες το 24ωρο. Σε αυτή την περίπτωση, το σχέδιο πρέπει να περιλαμβάνει πρωτεύουσες και δευτερεύουσες πληροφορίες επικοινωνίας. Οι οργανισμοί μπορούν επίσης να χρησιμοποιούν ένα εναλλασσόμενο μέλος της CSIRT σε κατάσταση ετοιμότητας, το οποίο θα λειτουργεί ως πρώτη επαφή σε περίπτωση περιστατικού.

Σχέδιο εσωτερικής επικοινωνίας: Τα περιστατικά μπορεί να δημιουργήσουν χάος καθώς το προσωπικό προσπαθεί να κατανοήσει τι συμβαίνει, ποιους πόρους χρειάζεται και ποιον να εμπλέξει για την αντιμετώπιση του περιστατικού. Ο οδηγός εσωτερικής επικοινωνίας του σχεδίου μπορεί να διαχειριστεί αυτό το χάος. Αυτή η ενότητα καθορίζει τη ροή πληροφοριών προς τα πάνω και προς τα κάτω μεταξύ ανώτατης διοίκησης και της CSIRT. Η πλευρική επικοινωνία μεταξύ της βασικής ομάδας

CSIRT και του υποστηρικτικού προσωπικού πρέπει επίσης να καλύπτεται. Αυτό περιορίζει τα άτομα που επικοινωνούν μεταξύ τους και μειώνει τις πιθανές αντικρουόμενες οδηγίες.

Εκπαίδευση: Το σχέδιο αντιμετώπισης περιστατικών πρέπει επίσης να υποδεικνύει τη συχνότητα εκπαίδευσης για το προσωπικό της CSIRT. Τουλάχιστον, όλη η ομάδα θα πρέπει να συμμετέχει σε μια «επιτραπέζια άσκηση» τουλάχιστον μία φορά ετησίως. Εάν η ανάλυση μετά το περιστατικό δείξει κενά στην εκπαίδευση, αυτά πρέπει να καλυφθούν μέσα σε εύλογο χρόνο μετά την ολοκλήρωση του περιστατικού.

Συντήρηση: Οι οργανισμοί όλων των μεγεθών αλλάζουν συνεχώς, περιλαμβάνοντας αλλαγές σε υποδομές, απειλές και προσωπικό. Το σχέδιο αντιμετώπισης περιστατικών πρέπει να καθορίζει τη συχνότητα αναθεώρησης και ενημέρωσής του. Για παράδειγμα, αν ο οργανισμός εξαγοράσει έναν άλλο οργανισμό, η CSIRT μπορεί να χρειαστεί να προσαρμόσει τις υπηρεσίες ή να ενσωματώσει συγκεκριμένα άτομα και τους ρόλους τους. Τουλάχιστον, το σχέδιο πρέπει να ενημερώνεται ετησίως. Τα μέλη της ομάδας πρέπει επίσης να βελτιώνουν τις δεξιότητές τους μέσω ατομικής εκπαίδευσης και πιστοποιήσεων από οργανισμούς όπως το SANS ή σε συγκεκριμένα εργαλεία ψηφιακής εγκληματολογίας. Οι οργανισμοί μπορούν να ενσωματώνουν τα διδάγματα από τις ασκήσεις σε αυτή την ενημέρωση.

2.9. Σχέδιο Αντιμετώπισης Περιστατικών

Μετά τη σύνταξη του καταστατικού αντιμετώπισης περιστατικών και τη συγκρότηση της ομάδας CSIRT, το επόμενο βήμα είναι η δημιουργία του σχεδίου αντιμετώπισης περιστατικών. Το σχέδιο αντιμετώπισης περιστατικών αποτελεί το έγγραφο που περιγράφει τη δομή υψηλού επιπέδου της δυνατότητας αντίδρασης ενός οργανισμού. Πρόκειται για ένα έγγραφο υψηλού επιπέδου που λειτουργεί ως θεμέλιο για την ομάδα CSIRT. Τα κύρια στοιχεία του σχεδίου αντιμετώπισης περιστατικών είναι τα εξής:

1. **Καταστατικό Αντιμετώπισης Περιστατικών:** Το σχέδιο αντιμετώπισης περιστατικών πρέπει να περιλαμβάνει τη δήλωση αποστολής και το κοινό-στόχο που αναφέρονται στο καταστατικό αντιμετώπισης περιστατικών. Αυτό διασφαλίζει συνέχεια μεταξύ της έναρξης της δυνατότητας αντιμετώπισης περιστατικών και του σχεδίου.
2. **Εκτεταμένος κατάλογος υπηρεσιών:** Το αρχικό καταστατικό περιλάμβανε γενικές κατηγορίες υπηρεσιών χωρίς λεπτομέρειες. Το σχέδιο αντιμετώπισης περιστατικών πρέπει να παρέχει συγκεκριμένες λεπτομέρειες για τις υπηρεσίες που θα προσφέρει η CSIRT. Για παράδειγμα, αν οι υπηρεσίες ψηφιακής εγκληματολογίας περιλαμβάνονται στις προσφερόμενες υπηρεσίες, το σχέδιο μπορεί να αναφέρει ότι αυτές περιλαμβάνουν ανάκτηση στοιχείων από σκληρούς δίσκους, ανάλυση μνήμης και αντίστροφη μηχανική δυνητικά κακόβουλου κώδικα. Αυτό επιτρέπει στη CSIRT να διαχωρίζει σαφώς ένα κανονικό αίτημα από μια ενέργεια που σχετίζεται με περιστατικό.

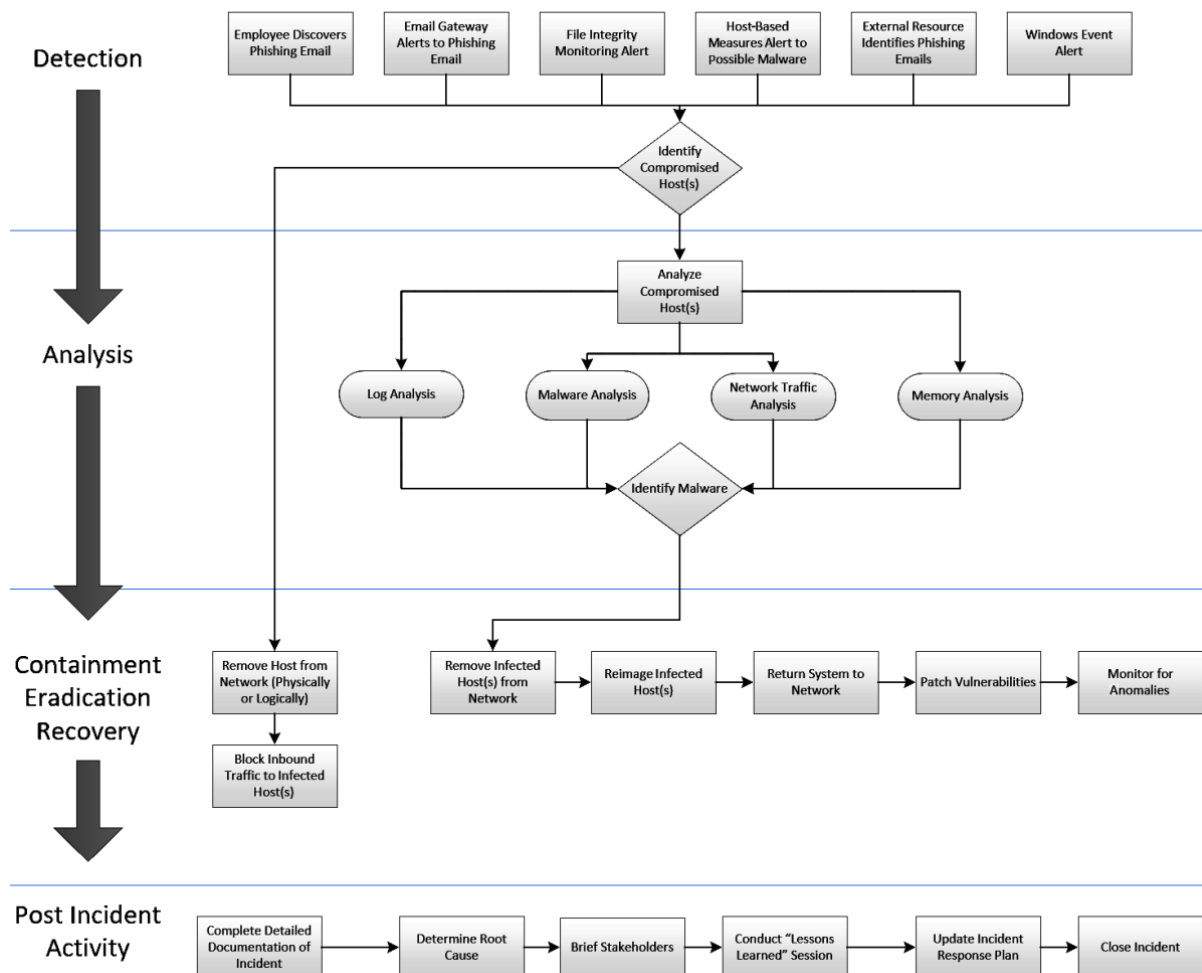
3. **Προσωπικό CSIRT:** Το σχέδιο πρέπει να καθορίζει σαφώς τους ρόλους και τις ευθύνες όλων των μελών της ομάδας CSIRT. Οι οργανισμοί πρέπει να ορίζουν ακριβώς τους ρόλους και τις αρμοδιότητες κάθε μέλους, ώστε να αποφεύγεται η «σύγκρουση αρμοδιοτήτων» κατά τη διάρκεια ενός περιστατικού.
4. **Κατάλογος επαφών:** Ένας ενημερωμένος κατάλογος επαφών πρέπει να αποτελεί μέρος του σχεδίου. Ανάλογα με τις ανάγκες, η CSIRT μπορεί να χρειάζεται να ανταποκρίνεται σε περιστατικά 24/7. Σε αυτή την περίπτωση, το σχέδιο πρέπει να περιλαμβάνει πρωτεύουσες και δευτερεύουσες πληροφορίες επικοινωνίας και να προβλέπει εναλλασσόμενα μέλη σε κατάσταση ετοιμότητας.
5. **Σχέδιο εσωτερικής επικοινωνίας:** Τα περιστατικά μπορεί να δημιουργήσουν χάος καθώς το προσωπικό προσπαθεί να κατανοήσει την κατάσταση, τους πόρους και τα εμπλεκόμενα άτομα. Το σχέδιο εσωτερικής επικοινωνίας καθορίζει τη ροή πληροφοριών προς τα πάνω και προς τα κάτω μεταξύ της διοίκησης και της CSIRT, καθώς και την πλευρική επικοινωνία με το υποστηρικτικό προσωπικό, περιορίζοντας τις πιθανές αντικρουόμενες οδηγίες.
6. **Εκπαίδευση:** Το σχέδιο πρέπει να καθορίζει τη συχνότητα εκπαίδευσης του προσωπικού της CSIRT. Τουλάχιστον, όλη η ομάδα πρέπει να συμμετέχει σε μία «επιτραπέζια άσκηση» ετησίως. Εάν η ανάλυση μετά το περιστατικό εντοπίσει κενά στην εκπαίδευση, αυτά πρέπει να καλυφθούν άμεσα.
7. **Συντήρηση:** Οι οργανισμοί αλλάζουν συνεχώς, με αλλαγές σε υποδομές, απειλές και προσωπικό. Το σχέδιο πρέπει να καθορίζει τη συχνότητα αναθεώρησης και ενημέρωσής του. Τουλάχιστον, πρέπει να αναθεωρείται ετησίως. Τα μέλη της ομάδας πρέπει επίσης να βελτιώνουν τις δεξιότητές τους μέσω ατομικής εκπαίδευσης και πιστοποιήσεων (π.χ. SANS ή σε εργαλεία ψηφιακής εγκληματολογίας). Τα διδάγματα από ασκήσεις μπορούν να ενσωματωθούν στις ενημερώσεις.

2.10. Το εγχειρίδιο αντιμετώπισης περιστατικών (Incident Response Playbook)

Ένα βασικό στοιχείο του σχεδίου αντιμετώπισης περιστατικών είναι η χρήση εγχειριδίων (playbooks). Ένα εγχειρίδιο αντιμετώπισης περιστατικών αποτελεί ένα σύνολο οδηγιών και ενεργειών που πρέπει να εκτελούνται σε κάθε βήμα της διαδικασίας αντιμετώπισης περιστατικών. Τα εγχειρίδια δημιουργούνται για να παρέχουν στους οργανισμούς μια σαφή πορεία μέσα στη διαδικασία, αλλά με έναν βαθμό ευελιξίας σε περίπτωση που το περιστατικό που διερευνάται δεν ταιριάζει ακριβώς σε ένα προκαθορισμένο σενάριο.

Ένας καλός δείκτης για το ποια εγχειρίδια είναι κρίσιμα είναι η αξιολόγηση κινδύνου του οργανισμού. Η εξέταση της αξιολόγησης κινδύνου για οποιαδήποτε απειλή που χαρακτηρίζεται ως κρίσιμη ή υψηλή θα υποδείξει ποια σενάρια πρέπει να αντιμετωπιστούν μέσω εγχειριδίου αντιμετώπισης περιστατικών. Οι περισσότεροι οργανισμοί θα εντοπίσουν αρκετές απειλές, όπως εισβολή στο δίκτυο μέσω εκμετάλλευσης zero-day, ransomware ή phishing, ως κρίσιμες, απαιτώντας προληπτικούς και

ανιχνευτικούς ελέγχους. Δεδομένου ότι η αξιολόγηση κινδύνου έχει εντοπίσει αυτές ως κρίσιμους κινδύνους, είναι καλύτερο να ξεκινήσουν τα εγχειρίδια με αυτές τις απειλές.



Για παράδειγμα, ας εξετάσουμε το διάγραμμα ενός εγχειριδίου για μια κοινή απειλή, την κοινωνική μηχανική (social engineering). Για αυτό το εγχειρίδιο, θα χωρίσουμε τη διαδικασία σύμφωνα με τη διαδικασία αντιμετώπισης περιστατικών που συζητήθηκε προηγουμένως:

- **Προετοιμασία:** Σε αυτή την ενότητα, ο οργανισμός επισημαίνει την προετοιμασία που έχει γίνει. Στην περίπτωση του phishing, αυτό μπορεί να περιλαμβάνει ευαισθητοποίηση των εργαζομένων για την αναγνώριση πιθανών phishing μηνυμάτων ή τη χρήση συσκευής email που σαρώσει τα επισυναπτόμενα αρχεία για κακόβουλο λογισμικό.
- **Ανίχνευση:** Για επιθέσεις phishing, οι οργανισμοί συχνά ειδοποιούνται από ενημερωμένους υπαλλήλους ή μέσω ελέγχων ασφαλείας email. Οι οργανισμοί πρέπει επίσης να προβλέπουν την λήψη ειδοποιήσεων μέσω μέτρων πρόληψης malware ή συστημάτων Host Intrusion Prevention (HIPS).

- **Ανάλυση:** Αν εντοπιστεί ένα γεγονός, η ανάλυση των διαθέσιμων αποδεικτικών στοιχείων είναι κρίσιμη για την ταξινόμηση και την κατάλληλη ανταπόκριση στο περιστατικό. Στην περίπτωση αυτή, η ανάλυση μπορεί να περιλαμβάνει εξέταση της μνήμης του συμβιβασμένου υπολογιστή, έλεγχο των αρχείων καταγραφής (logs) για ύποπτες εγγραφές και ανάλυση της δικτυακής κίνησης που σχετίζεται με τον υπολογιστή.
- **Περιορισμός (Containment):** Αν ένας υπολογιστής έχει ταυτοποιηθεί ως συμβιβασμένος, πρέπει να απομονωθεί από το δίκτυο.
- **Εξάλειψη (Eradication):** Αν έχει εντοπιστεί malware, πρέπει να αφαιρεθεί. Αν όχι, το εγχειρίδιο πρέπει να προβλέπει εναλλακτική, όπως η επανεγκατάσταση του συστήματος με γνωστή καλή εικόνα (reimaging).
- **Ανάκτηση (Recovery):** Η φάση ανάκαμψης περιλαμβάνει σάρωση του υπολογιστή για πιθανές ευπάθειες και παρακολούθηση του συστήματος για ανώμαλη κίνηση.
- **Μετά το περιστατικό (Post-incident activity):** Το εγχειρίδιο πρέπει επίσης να παρέχει οδηγίες για τις ενέργειες που πρέπει να γίνουν μετά από ένα περιστατικό. Πολλές από αυτές τις ενέργειες θα είναι κοινές σε όλα τα εγχειρίδια, αλλά είναι σημαντικό να περιλαμβάνονται για να διασφαλιστεί ότι ολοκληρώνονται πλήρως.

Το παραπάνω διάγραμμα αποτελεί ένα δείγμα εγχειριδίου για επίθεση phishing. Σημειώστε ότι κάθε φάση του κύκλου αντιμετώπισης περιστατικών καλύπτεται, καθώς και οι συγκεκριμένες ενέργειες που πρέπει να γίνουν ως μέρος της ανταπόκρισης. Επιπλέον, οι οργανισμοί μπορούν να αναλύσουν περαιτέρω τις συγκεκριμένες ενέργειες, όπως μέσω ανάλυσης logs για ένα συγκεκριμένο εγχειρίδιο, για μεγαλύτερη λεπτομέρεια.

Τα εγχειρίδια (playbooks) έχουν σχεδιαστεί για να παρέχουν στην ομάδα CSIRT και σε οποιοδήποτε άλλο προσωπικό ένα σύνολο οδηγιών που πρέπει να ακολουθήσουν κατά τη διάρκεια ενός περιστατικού. Αυτό επιτρέπει να χάνεται λιγότερος χρόνος, καθώς υπάρχει προκαθορισμένη πορεία δράσης. Τα εγχειρίδια λειτουργούν ως οδηγός και θα πρέπει να ενημερώνονται τακτικά, ειδικά όταν χρησιμοποιούνται σε κάποιο περιστατικό και εντοπίζονται σημαντικά στοιχεία ή βήματα. Αξίζει να σημειωθεί ότι τα εγχειρίδια δεν είναι «χαραγμένα σε πέτρα» και δεν αποτελούν απλώς μια λίστα ελέγχου. Το προσωπικό του CSIRT δεν δεσμεύεται αυστηρά από το εγχειρίδιο όσον αφορά τις ενέργειες και πρέπει να έχει την ελευθερία να αναλαμβάνει πρόσθετες ενέργειες, εάν το περιστατικό το απαιτεί.

2.11. Διαδικασίες Κλιμάκωσης

Ένα κρίσιμο στοιχείο του σχεδίου αντιμετώπισης περιστατικών είναι οι διαδικασίες κλιμάκωσης. Οι διαδικασίες κλιμάκωσης καθορίζουν ποιος είναι υπεύθυνος για τη μετατροπή ενός γεγονότος ή σειράς γεγονότων από απλές ανωμαλίες στο πληροφοριακό σύστημα σε ένα περιστατικό. Η ομάδα CSIRT θα εξαντληθεί εάν καλείται να ερευνήσει πάρα πολλά ψευδή θετικά. Οι διαδικασίες κλιμάκωσης

διασφαλίζουν ότι η ομάδα CSIRT αξιοποιείται αποτελεσματικά και ότι το προσωπικό καλείται μόνο όταν η εξειδίκευσή του είναι απαραίτητη.

Οι διαδικασίες ξεκινούν με τα άτομα που είναι πιο πιθανό να παρατηρήσουν ανωμαλίες ή γεγονότα στο σύστημα, τα οποία μπορεί να υποδεικνύουν ένα μεγαλύτερο περιστατικό. Για παράδειγμα, το help desk μπορεί να λάβει αρκετές κλήσεις που υποδηλώνουν πιθανή μόλυνση από κακόβουλο λογισμικό. Οι διαδικασίες κλιμάκωσης μπορεί να ορίζουν ότι, αν εντοπιστεί κακόβουλο λογισμικό και δεν μπορεί να αφαιρεθεί μέσω των ελέγχων πρόληψης, πρέπει να επικοινωνήσουν με τον εκάστοτε υπεύθυνο μέλος της ομάδας CSIRT. Το μέλος της CSIRT αναλαμβάνει τότε τον έλεγχο. Εάν καταφέρει να περιορίσει το κακόβουλο λογισμικό σε αυτό το σύστημα και να εντοπίσει τον τρόπο μόλυνσης, θα προσπαθήσει να αφαιρέσει το κακόβουλο λογισμικό και, εάν αυτό δεν είναι δυνατό, θα γίνει επανεγκατάσταση και επαναφορά του συστήματος. Σε αυτό το σημείο, το περιστατικό έχει επιτυχώς ολοκληρωθεί. Το μέλος της CSIRT μπορεί να τεκμηριώσει το περιστατικό και να το κλείσει χωρίς να χρειαστεί να εμπλέξει άλλους πόρους.

Ένα άλλο παράδειγμα, όπου η κλιμάκωση προχωρά σε πλήρη αντίδραση της CSIRT, μπορεί να ξεκινήσει πολύ απλά με έναν έλεγχο των διαπιστευτηρίων του Active Directory. Σε αυτή την περίπτωση, ένας διαχειριστής διακομιστή με αρμοδιότητες διαχείρισης πρόσβασης διεξάγει έναν μηνιαίο έλεγχο των διαπιστευτηρίων διαχειριστών. Κατά τον έλεγχο, εντοπίζει τρεις νέους λογαριασμούς διαχειριστή που δεν συνδέονται με γνωστά δικαιώματα πρόσβασης. Μετά από περαιτέρω διερεύνηση, διαπιστώνει ότι αυτοί οι λογαριασμοί δημιουργήθηκαν μέσα σε λίγες ώρες ο ένας από τον άλλο και κατά τη διάρκεια του Σαββατοκύριακου. Ο διαχειριστής διακομιστή επικοινωνεί με την CSIRT για διερεύνηση.

Ο αναλυτής της CSIRT εξετάζει την κατάσταση και καθορίζει ότι πιθανόν έχει συμβεί παραβίαση. Το μέλος της CSIRT καθοδηγεί τον διαχειριστή διακομιστή να ελέγξει τα αρχεία καταγραφής για τυχόν συνδέσεις χρησιμοποιώντας αυτούς τους λογαριασμούς διαχειριστή. Ο διαχειριστής διακομιστή εντοπίζει δύο συνδέσεις, μία σε διακομιστή βάσης δεδομένων και μία σε web server στο DMZ. Ο αναλυτής της CSIRT καθοδηγεί στη συνέχεια τον διαχειριστή δικτύου που ανήκει στην ομάδα CSIRT να εξετάσει την κίνηση μεταξύ της βάσης SQL και του web server. Επιπλέον, βάσει των συνθηκών, ο αναλυτής της CSIRT κλιμακώνει την υπόθεση στον συντονιστή CSIRT και τον ενημερώνει για την κατάσταση. Ο συντονιστής CSIRT ξεκινά τότε τη διαδικασία εμπλοκής άλλων μελών της κύριας ομάδας CSIRT και τεχνικής υποστήριξης για βοήθεια.

Μετά την εξέταση της δικτυακής κίνησης, διαπιστώνεται ότι ένας εξωτερικός κακόβουλος παράγοντας έχει παραβιάσει και τα δύο συστήματα και βρίσκεται στη διαδικασία εξαγωγής της βάσης δεδομένων πελατών από το εσωτερικό δίκτυο. Σε αυτό το σημείο, ο συντονιστής CSIRT χαρακτηρίζει το περιστατικό ως υψηλής σοβαρότητας και ξεκινά τη διαδικασία εμπλοκής προσωπικού υποστήριξης σε ενημέρωση. Δεδομένου ότι το περιστατικό αφορά παραβίαση δεδομένων πελατών, το προσωπικό υποστήριξης της CSIRT, όπως οι ομάδες μάρκετινγκ, επικοινωνίας και νομικών, πρέπει να εμπλακεί. Εάν απαιτηθούν περισσότεροι πόροι, ο συντονιστής CSIRT θα αναλάβει την πρωτοβουλία για τη λήψη της σχετικής απόφασης.

Οι διαδικασίες κλιμάκωσης δημιουργούνται για να διασφαλίσουν ότι τα κατάλληλα άτομα διαθέτουν την απαραίτητη εξουσιοδότηση και εκπαίδευση ώστε να ζητούν πόρους όταν χρειάζεται. Οι διαδικασίες κλιμάκωσης θα πρέπει επίσης να καλύπτουν τη συμμετοχή άλλου προσωπικού εκτός των βασικών μελών της CSIRT, ανάλογα με τη σοβαρότητα του περιστατικού. Μία από τις κρίσιμες λειτουργίες των διαδικασιών κλιμάκωσης είναι να καθορίζουν με σαφήνεια ποια άτομα έχουν την εξουσιοδότηση να χαρακτηρίζουν μια ανώμαλη δραστηριότητα ως περιστατικό. Οι διαδικασίες κλιμάκωσης θα πρέπει επίσης να ρυθμίζουν τη συμμετοχή άλλου προσωπικού εκτός των βασικών μελών της CSIRT, βάσει της σοβαρότητας του περιστατικού.

2.12. Δοκιμή του πλαισίου ανταπόκρισης σε περιστατικά

Μέχρι στιγμής, έχουν καλυφθεί αρκετοί τομείς όσον αφορά την προετοιμασία για ένα περιστατικό. Από την αρχική κατανόηση της διαδικασίας ανταπόκρισης σε περιστατικά, προχωρήσαμε στη δημιουργία ενός σχεδίου ανταπόκρισης σε περιστατικά και των αντίστοιχων playbooks.

Μόλις δημιουργηθεί η δυνατότητα, θα πρέπει να δοκιμαστεί μέσω μιας **table-top άσκησης** για να εντοπιστούν τυχόν κενά ή ελλείψεις. Αυτή η άσκηση θα πρέπει να περιλαμβάνει ένα σενάριο περιστατικού υψηλού επιπέδου που εμπλέκει ολόκληρη την ομάδα και ένα από τα αντίστοιχα playbooks. Πρέπει επίσης να ετοιμαστεί μια αναφορά που να περιγράφει τα αποτελέσματα της table-top άσκησης, τυχόν κενά, διορθώσεις ή τροποποιήσεις, και να προωθηθεί στη ανώτατη διοίκηση. Μόλις η διοίκηση ενημερωθεί και αναγνωρίσει ότι η CSIRT είναι έτοιμη για ανάπτυξη, θεωρείται πλέον επιχειρησιακή.

Καθώς η CSIRT αποκτά εμπειρία στην εκτέλεση του σχεδίου σε ένα δομημένο σενάριο, μπορεί να επιλέξει πιο σύνθετες δοκιμές. Μια άλλη επιλογή είναι η **Red/Blue ή Purple Team άσκηση**, όπου η CSIRT καλείται να ανταποκριθεί σε μια εξουσιοδοτημένη δοκιμή διείσδυσης (penetration test). Σε αυτή την περίπτωση, η ομάδα μπορεί να δράσει απέναντι σε έναν ζωντανό αντίπαλο και να δοκιμάσει τα σχέδια και τα playbooks της, αυξάνοντας σημαντικά την αξία της δοκιμής διείσδυσης, καθώς παρέχει πληροφορίες τόσο για την ασφάλεια της υποδομής όσο και για την ικανότητα του οργανισμού να ανταποκριθεί κατάλληλα.

Ανεξάρτητα από τη σύνθεση της ομάδας, ένα άλλο βασικό στοιχείο της ανάπτυξης της CSIRT είναι η **τακτική εκπαίδευση**. Τα βασικά μέλη της CSIRT πρέπει να λαμβάνουν συνεχή εκπαίδευση σε θέματα αναδυόμενων απειλών, τεχνικών εγκληματολογίας και εργαλείων. Αυτό μπορεί να πραγματοποιείται μέσω εξωτερικών παρόχων εκπαίδευσης ή, αν υπάρχει δυνατότητα, μέσω εσωτερικής εκπαίδευσης. Τα τεχνικά υποστηρικτικά μέλη της CSIRT πρέπει επίσης να εκπαιδεύονται τακτικά στις διαθέσιμες τεχνικές και εργαλεία, κάτι ιδιαίτερα σημαντικό αν καλούνται να βοηθήσουν στη συλλογή στοιχείων ή στις δραστηριότητες αποκατάστασης κατά τη διάρκεια ενός περιστατικού. Τέλος, τα υπόλοιπα υποστηρικτικά μέλη πρέπει να συμμετέχουν στην **ετήσια δοκιμή του σχεδίου ανταπόκρισης σε περιστατικά**, χρησιμοποιώντας μια table-top άσκηση με σενάριο υψηλού επιπέδου. Μια άλλη επιλογή είναι ο συνδυασμός της δοκιμής του σχεδίου με μια δοκιμή διείσδυσης, ώστε αν ο οργανισμός

εντοπίσει την παρουσία της δοκιμής, να μπορέσει να περάσει από τις πρώτες φάσεις του περιστατικού και να δημιουργήσει ένα table-top για τις υπόλοιπες φάσεις.

Ένα τελευταίο στοιχείο της συνεχούς συντήρησης του σχεδίου ανταπόκρισης σε περιστατικά είναι η **ετήσια πλήρης αναθεώρηση**. Αυτή διεξάγεται για να διασφαλιστεί ότι οποιεσδήποτε αλλαγές σε προσωπικό, οργανωτική δομή ή αποστολή που μπορεί να επηρεάσουν άλλα μέρη του σχεδίου αντιμετωπίζονται κατάλληλα. Επιπλέον, γίνεται πλήρης ανασκόπηση των playbooks. Καθώς οι απειλές αλλάζουν, μπορεί να χρειαστεί να τροποποιηθούν υπάρχοντα playbooks ή να προστεθούν νέα. Το προσωπικό της CSIRT θα πρέπει επίσης να έχει τη δυνατότητα να δημιουργήσει νέο playbook σε περίπτωση εμφάνισης νέας απειλής. Με αυτόν τον τρόπο, η CSIRT θα είναι καλύτερα προετοιμασμένη να αντιμετωπίσει περιστατικά που μπορεί να επηρεάσουν τον οργανισμό. Οποιοσδήποτε σημαντικές αλλαγές ή προσθήκες θα πρέπει επίσης να οδηγήσουν σε νέα table-top άσκηση για την επικύρωση των πρόσθετων σχεδίων και playbooks.

3

Διαχείριση Κυβερνοεπιθέσεων

Το πλαίσιο αντιμετώπισης περιστατικών που περιγράφηκε στο προηγούμενο κεφάλαιο προσέφερε τη συγκεκριμένη δομή μιας Ομάδας Αντιμετώπισης Περιστατικών Ασφάλειας Υπολογιστών (CSIRT) και πώς η CSIRT θα συνεργάζεται με άλλες επιχειρησιακές μονάδες. Το κεφάλαιο επεκτάθηκε περαιτέρω στον απαραίτητο σχεδιασμό και την προετοιμασία που πρέπει να πραγματοποιήσει ένας οργανισμός για την αντιμετώπιση κυβερνοεπιθέσεων. Δυστυχώς, ο σχεδιασμός και η προετοιμασία δεν μπορούν να καλύψουν όλες τις μεταβλητές και τις αβεβαιότητες που υπάρχουν σε περιστατικά κυβερνοασφάλειας.

Όπως είπε ο πυγμάχος Mike Tyson: «Όλοι έχουν ένα σχέδιο μέχρι να φάνε ένα χαστούκι στο πρόσωπο.»

Μια σταθερή βάση και κατανόηση της διαχείρισης κυβερνοεπιθέσεων επιτρέπει στους οργανισμούς να εφαρμόζουν τα σχέδιά τους πιο αποτελεσματικά, να επικοινωνούν έγκαιρα με βασικούς ενδιαφερόμενους και, το πιο σημαντικό, να μειώνουν τη δυνατότητα ζημιάς ή διακοπής λειτουργίας λόγω ενός κυβερνοπεριστατικού.

Το κεφάλαιο αυτό θα καλύψει το πώς να διαχειριστούμε ένα κυβερνοπεριστατικό, εξετάζοντας τα εξής θέματα:

- Συνεργασία με την ομάδα αντιμετώπισης περιστατικών
- Ενσωμάτωση επικοινωνίας κρίσεων
- Διερεύνηση περιστατικών
- Ενσωμάτωση στρατηγικών περιορισμού
- Επανόρθωση και ανάκτηση για επιστροφή στην κανονικότητα

3.1. Συνεργασία με την ομάδα αντιμετώπισης περιστατικών

Η CSIRT λειτουργεί με τρόπο παρόμοιο με μια αστική ή αγροτική πυροσβεστική υπηρεσία. Μια πυροσβεστική υπηρεσία διαθέτει εξειδικευμένους επαγγελματίες που είναι αρμόδιοι να ανταποκρίνονται σε επείγουσες καταστάσεις με εξειδικευμένο εξοπλισμό για τον περιορισμό και την

εξάλειψη μιας πυρκαγιάς. Για να κινητοποιηθεί η πυροσβεστική, ένας πολίτης πρέπει να επικοινωνήσει με τις υπηρεσίες έκτακτης ανάγκης και να παρέχει βασικές πληροφορίες, όπως η φύση του περιστατικού, η τοποθεσία και αν υπάρχουν άνθρωποι σε κίνδυνο. Στη συνέχεια, αυτές οι πληροφορίες μεταβιβάζονται στην πυροσβεστική, η οποία στέλνει τους κατάλληλους πόρους στο συμβάν.

Η διαδικασία ενεργοποίησης μιας CSIRT είναι πολύ παρόμοια με την ενεργοποίηση μιας πυροσβεστικής. Εσωτερικό ή εξωτερικό προσωπικό πρέπει να κλιμακώσει ενδείξεις ενός περιστατικού κυβερνοασφάλειας στο κατάλληλο προσωπικό. Στη συνέχεια, οι πόροι αποστέλλονται στην κατάλληλη τοποθεσία/ες, όπου οι παρευρισκόμενοι αναλαμβάνουν την πρωτοβουλία για τον περιορισμό του περιστατικού και την εξάλειψη ή τον περιορισμό πιθανής διακοπής λειτουργίας ή απώλειας δεδομένων.

Για να γίνει αυτή η διαδικασία όσο το δυνατόν πιο αποδοτική, τα ακόλουθα είναι κρίσιμα στοιχεία της διαδικασίας ενεργοποίησης:

- Τα μοντέλα CSIRT παρέχουν ένα πλαίσιο που τοποθετεί την CSIRT και τις σχετικές διαδικασίες κλιμάκωσης μέσα στη δομή του οργανισμού.
- Ένα **war room** περιγράφει την τοποθεσία από την οποία η CSIRT διαχειρίζεται το περιστατικό.
- Οι επικοινωνίες αφορούν την ικανότητα της CSIRT να επικοινωνεί σωστά.
- Η **περιστροφή προσωπικού** εξετάζει την ανάγκη ανάπαυσης του προσωπικού κατά τη διάρκεια παρατεταμένου περιστατικού.

Η ενεργοποίηση μιας CSIRT, όπως και μια πυροσβεστική, απαιτεί καθορισμένη πορεία κλιμάκωσης. Στις επόμενες ενότητες παρουσιάζονται τρία μοντέλα CSIRT που περιγράφουν κάποιες επιλογές σχετικά με την ορθή κλιμάκωση.

3.2. Εμπλοκή της ομάδας αντιμετώπισης περιστατικών (CSIRT)

Μια ομάδα CSIRT λειτουργεί με τρόπο πολύ παρόμοιο με μια αστική ή αγροτική πυροσβεστική υπηρεσία. Μια πυροσβεστική υπηρεσία διαθέτει ειδικά εκπαιδευμένους επαγγελματίες που έχουν αναλάβει την αντιμετώπιση έκτακτων καταστάσεων με εξειδικευμένο εξοπλισμό για τον περιορισμό και την εξάλειψη μιας πυρκαγιάς. Για να εμπλακεί η πυροσβεστική, ένας πολίτης πρέπει να επικοινωνήσει με τις υπηρεσίες έκτακτης ανάγκης και να παράσχει βασικές πληροφορίες, όπως η φύση της έκτακτης ανάγκης, η τοποθεσία και αν υπάρχουν άνθρωποι σε κίνδυνο. Από εκεί, οι πληροφορίες αυτές διαβιβάζονται στην πυροσβεστική, η οποία στέλνει τους πόρους στην περιοχή της έκτακτης ανάγκης.

Η διαδικασία εμπλοκής μιας ομάδας CSIRT είναι πολύ παρόμοια με την εμπλοκή μιας πυροσβεστικής. Εσωτερικό ή εξωτερικό προσωπικό πρέπει να αναφέρει ενδείξεις ενός περιστατικού κυβερνοασφάλειας στο κατάλληλο προσωπικό. Στη συνέχεια, οι πόροι αποστέλλονται στην

αντίστοιχη τοποθεσία/ες, όπου οι υπεύθυνοι επιτόπου αναλαμβάνουν τον έλεγχο του περιστατικού και την εξάλειψη ή τον περιορισμό ενδεχόμενου χρόνου διακοπής λειτουργίας ή απώλειας δεδομένων. Για να είναι η διαδικασία όσο το δυνατόν πιο αποδοτική, τα παρακάτω αποτελούν κρίσιμα στοιχεία της διαδικασίας εμπλοκής:

- Τα μοντέλα CSIRT παρέχουν ένα πλαίσιο που εντάσσει την ομάδα CSIRT και τις σχετικές διαδικασίες κλιμάκωσης μέσα στη δομή της οργάνωσης.
- Ένα «war room» (αίθουσα επιχειρήσεων) περιγράφει την τοποθεσία από την οποία η CSIRT διαχειρίζεται το περιστατικό.
- Η επικοινωνία αφορά την ικανότητα της CSIRT να επικοινωνεί σωστά.
- Η εναλλαγή προσωπικού εξετάζει την ανάγκη ξεκούρασης του προσωπικού κατά τη διάρκεια παρατεταμένων περιστατικών.

Η εμπλοκή μιας CSIRT, όπως και μιας πυροσβεστικής, απαιτεί μια καθορισμένη πορεία κλιμάκωσης. Στις επόμενες ενότητες παρουσιάζονται τρία μοντέλα CSIRT που περιγράφουν ορισμένες επιλογές για την κατάλληλη διαδικασία κλιμάκωσης.

Μοντέλα CSIRT: Ο τρόπος με τον οποίο μια οργάνωση κλιμακώνει τα περιστατικά προς μια CSIRT εξαρτάται σε μεγάλο βαθμό από τη δομή της. Οι οργανισμοί διαμορφώνουν την ατομική τους CSIRT ώστε να ταιριάζει καλύτερα στη δομή και τους πόρους τους. Οι τρεις βασικές δομές που ακολουθούν μπορούν να χρησιμεύσουν ως οδηγός για την τοποθέτηση της CSIRT στο κατάλληλο τμήμα της οργάνωσης, ώστε να διευκολύνεται η ταχεία κλιμάκωση και να καταγράφονται όσο το δυνατόν περισσότερες λεπτομέρειες του περιστατικού για τη σωστή διερεύνηση.

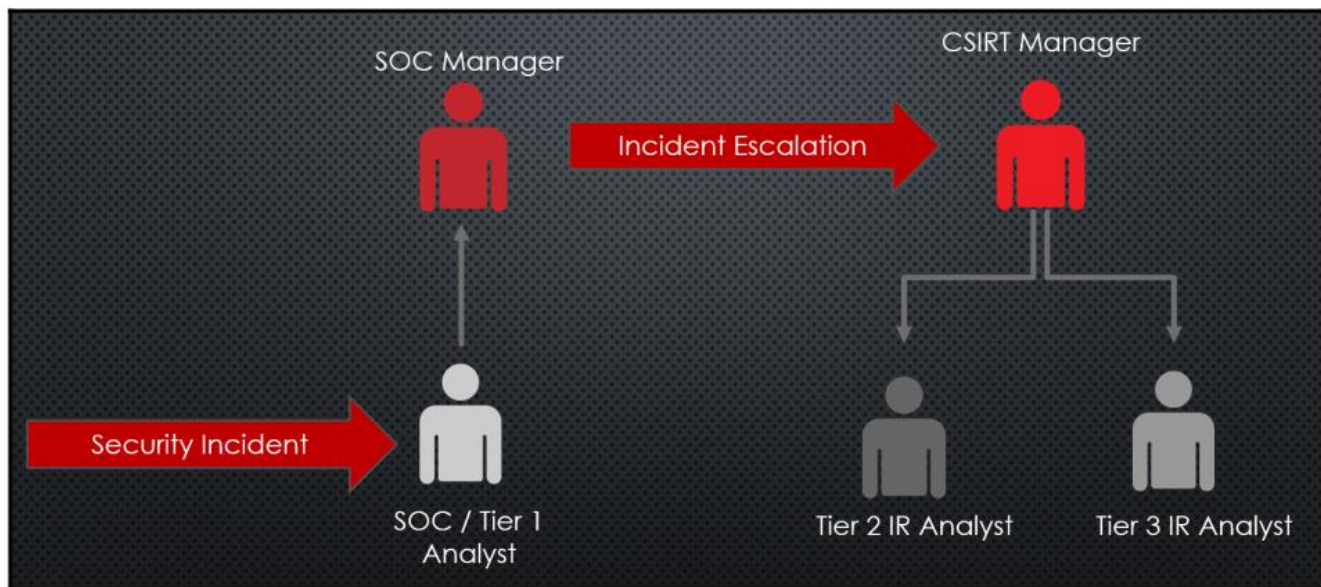
Κλιμάκωση μέσω Κέντρου Λειτουργιών Ασφάλειας (SOC): Σε αυτό το οργανωτικό μοντέλο, το Κέντρο Λειτουργιών Ασφάλειας (SOC) είναι υπεύθυνο για την αρχική ανίχνευση ή διερεύνηση του περιστατικού. Γενικά, το SOC διαχειρίζεται τα εργαλεία ασφαλείας που παρακολουθούν την υποδομή δικτύου. Έχει άμεση πρόσβαση σε συστήματα διαχείρισης συμβάντων, πρόληψης και ανίχνευσης εισβολών, καθώς και σε συστήματα antivirus. Από εκεί, μπορεί να παρακολουθεί συμβάντα, να λαμβάνει και να αξιολογεί ειδοποιήσεις και να επεξεργάζεται άλλα δεδομένα που σχετίζονται με την ασφάλεια.

Η κλιμάκωση μέσω SOC είναι ένα κοινό μοντέλο σε οργανισμούς που διαθέτουν αφιερωμένο SOC, είτε με εσωτερικό προσωπικό είτε μέσω τρίτου παρόχου υπηρεσιών ασφαλείας (MSSP). Σε αυτό το μοντέλο, υπάρχουν σαφώς καθορισμένα βήματα, από την αρχική ειδοποίηση έως την κλιμάκωση, ως εξής:

1. Λαμβάνεται μια ειδοποίηση από τον αναλυτή SOC ή Tier 1.
2. Ο αναλυτής SOC ή Tier 1 καθορίζει εάν η ειδοποίηση πληροί τα κριτήρια για να θεωρηθεί περιστατικό.
3. Όταν εντοπιστεί πιθανό περιστατικό, ο αναλυτής πραγματοποιεί μια αρχική διερεύνηση.

4. Εάν απαιτείται, ο αναλυτής προωθεί το περιστατικό στον υπεύθυνο SOC.
5. Μετά από αξιολόγηση από τον υπεύθυνο SOC, το περιστατικό κλιμακώνεται στον υπεύθυνο CSIRT για την αντιμετώπιση του περιστατικού.

Το ακόλουθο διάγραμμα δείχνει τη ροή της κλιμάκωσης του περιστατικού από τον υπεύθυνο SOC προς τον υπεύθυνο CSIRT.



Στο συγκεκριμένο μοντέλο, υπάρχουν αρκετά ζητήματα που πρέπει να αντιμετωπιστούν από το προσωπικό του CSIRT και του SOC, τα εξής: Πρώτον, η εμπλοκή του CSIRT με αυτόν τον τρόπο δημιουργεί μια κατάσταση όπου πολλοί διαφορετικοί άνθρωποι χειρίζονται ένα περιστατικό πριν το CSIRT αναλάβει πλήρως. Δεύτερον, αν η κλιμάκωση του περιστατικού δεν τεκμηριώνεται σωστά, ο υπεύθυνος του CSIRT θα πρέπει να επικοινωνήσει με τον υπεύθυνο του SOC για διευκρινίσεις ή επιπλέον πληροφορίες, γεγονός που αυξάνει τον χρόνο αντιμετώπισης του περιστατικού. Τρίτον, το προσωπικό του SOC χρειάζεται εκπαίδευση ώστε να καθορίζει ποια παρατηρούμενα γεγονότα συνιστούν πραγματικό περιστατικό και ποια μπορεί να είναι ψευδώς θετικά. Το CSIRT μπορεί να εμφανίσει κόπωση ή απογοήτευση από την ανάγκη να διαχειρίζεται συνεχώς ψευδή περιστατικά που αναφέρουν οι αναλυτές του SOC.

Τέλος, η επικοινωνία μεταξύ του SOC και του CSIRT πρέπει να είναι σαφής και περιεκτική. Οποιοδήποτε κενό στην ικανότητά τους να μοιράζονται πληροφορίες σε πραγματικό χρόνο θα προκαλέσει περαιτέρω σύγχυση.

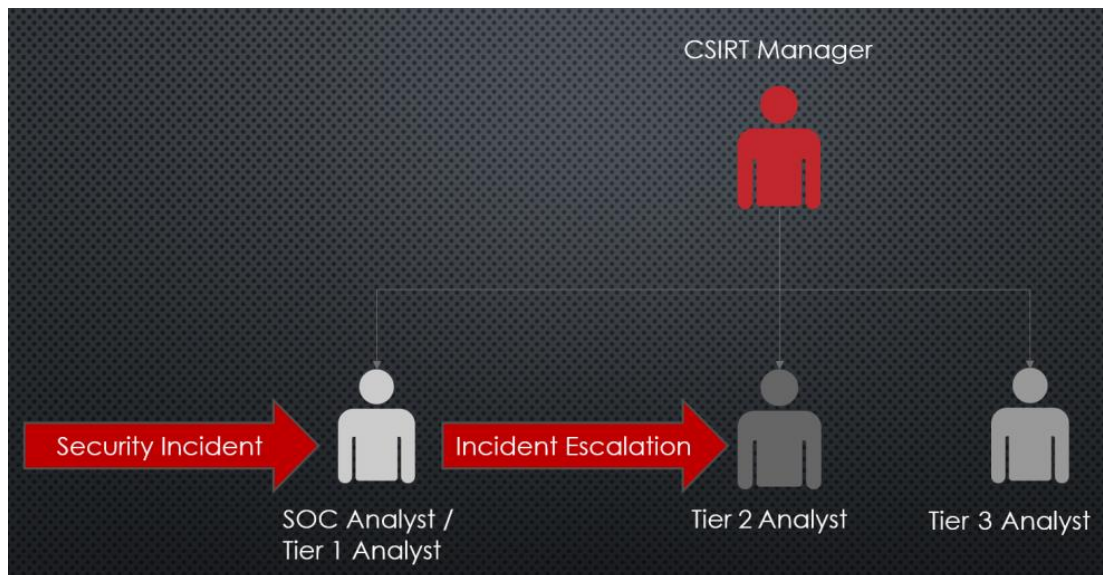
Μια άλλη παραλλαγή αυτού του μοντέλου, κοινή σε οργανισμούς χωρίς αποκλειστικό SOC, είναι όταν ένα αρχικό περιστατικό ασφάλειας λαμβάνεται είτε από ένα helpdesk είτε από ένα κέντρο λειτουργίας δικτύου (NOC). Αυτό προσθέτει επιπλέον πολυπλοκότητα στην έγκαιρη εμπλοκή του CSIRT, καθώς τέτοιο προσωπικό συχνά δεν έχει εκπαίδευση για την αντιμετώπιση περιστατικών αυτής της φύσης. Καλύτερη πρακτική σε αυτή την περίπτωση είναι να εκπαιδεύουν αρκετά μέλη αυτών των ομάδων

στην ανάλυση κυβερνοασφάλειας, ώστε να μπορούν να διεκπεραιώνουν τον αρχικό έλεγχο (triage) και να πραγματοποιούν σωστή κλιμάκωση των περιστατικών.

3.3. Συνδυασμός SOC και CSIRT

Για να περιοριστούν ορισμένα από τα μειονεκτήματα του μοντέλου κλιμάκωσης μέσω SOC, ορισμένοι οργανισμοί ενσωματώνουν το SOC στην ευρύτερη ομάδα του CSIRT. Η τοποθέτηση του SOC σε μια τέτοια δομή μπορεί να αποδειχθεί πιο αποδοτική, δεδομένου ότι το SOC έχει την ευθύνη για την αρχική ειδοποίηση και την αξιολόγηση (triage) των περιστατικών, που συνδέεται άμεσα με το CSIRT.

Σε αυτό το μοντέλο, ο αναλυτής του SOC λειτουργεί ως πρώτη βαθμίδα (Tier 1). Όπως έχει ήδη συζητηθεί, έχει την πρώτη εικόνα των συμβάντων ασφάλειας ή των ειδοποιήσεων των συστημάτων ελέγχου ασφάλειας. Μετά την επεξεργασία και την αξιολόγηση της ειδοποίησης, έχει τη δυνατότητα να κλιμακώσει άμεσα το περιστατικό στον αναλυτή Tier 2, χωρίς να χρειαστεί να εμπλέξει έναν υπεύθυνο, ο οποίος στη συνέχεια θα το προωθούσε στον υπεύθυνο του CSIRT. Αυτή η διαδικασία απεικονίζεται στο παρακάτω διάγραμμα:

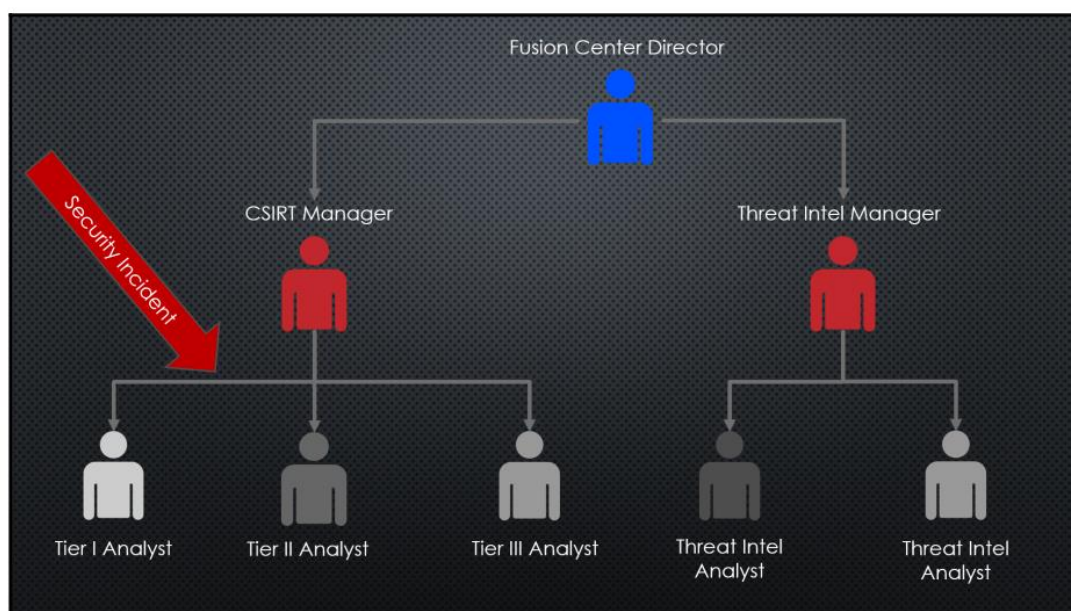


Αυτό το μοντέλο παρουσιάζει ορισμένα σαφή πλεονεκτήματα σε σχέση με το προηγούμενο. Πρώτον, το CSIRT έχει μεγαλύτερη ορατότητα σε όσα βλέπει και κάνει το SOC. Επιπλέον, η ενσωμάτωση του SOC στο CSIRT επιτρέπει στον υπεύθυνο του CSIRT και την ομάδα του να διαμορφώνουν πιο αποτελεσματικές πολιτικές και διαδικασίες που σχετίζονται με τα περιστατικά. Ένα δεύτερο, σαφές πλεονέκτημα αυτής της προσέγγισης είναι ότι η κλιμάκωση των περιστατικών ολοκληρώνεται πολύ ταχύτερα και, κατά κανόνα, με μεγαλύτερη ακρίβεια. Με τον αναλυτή του SOC να διαθέτει άμεση πρόσβαση για κλιμάκωση στην επόμενη βαθμίδα του CSIRT, ολόκληρη η διαδικασία είναι ταχύτερη και επιτρέπει πιο λεπτομερή ανάλυση.

Αυτή η προσέγγιση λειτουργεί καλά σε οργανισμούς με αποκλειστικό, εσωτερικό SOC και όχι εξωτερικευμένο. Για οργανισμούς που χρησιμοποιούν κέντρο λειτουργίας δικτύου (NOC) ή helpdesk, χωρίς αποκλειστικό SOC, αυτή η προσέγγιση δεν είναι ρεαλιστική, καθώς αυτές οι λειτουργίες συχνά διαχειρίζονται εκτός του CSIRT ή ακόμη και των ομάδων ασφάλειας δικτύου. Ένα άλλο ζήτημα είναι ότι, ανάλογα με το μέγεθος των ομάδων SOC και CSIRT, μπορεί να απαιτούνται επιπλέον υπεύθυνοι CSIRT για να διαχειρίζονται τον καθημερινό φόρτο εργασίας και των δύο ομάδων.

3.4. CSIRT Fusion Center

Καθώς η συλλογή και ανάλυση πληροφοριών απειλών (threat intelligence) γίνεται όλο και πιο σημαντικό μέρος των καθημερινών λειτουργιών ασφάλειας, μια οργανωτική δομή που ανταποκρίνεται σε αυτή την τάση είναι το **CSIRT Fusion Center**.



Σε αυτή την περίπτωση, οι αναλυτές του CSIRT, οι αναλυτές του SOC και οι αναλυτές threat intelligence συνεργάζονται σε μία ενιαία ομάδα. Αυτό συνδυάζει τα στοιχεία της δομής **SOC-και-CSIRT** με την προσθήκη εξειδικευμένων αναλυτών threat intelligence.

Σε ένα τέτοιο σενάριο:

- Οι αναλυτές threat intelligence είναι υπεύθυνοι για την υποστήριξη των διερευνήσεων περιστατικών, αξιοποιώντας εσωτερικούς και εξωτερικούς πόρους σχετικούς με το περιστατικό.
- Μπορούν επίσης να χρησιμοποιηθούν για λεπτομερή ανάλυση σε άλλους τομείς που σχετίζονται με το περιστατικό.

Ωστόσο, το CSIRT Fusion Center δεν είναι ευρέως διαδεδομένο, κυρίως επειδή η ενσωμάτωση threat intelligence είναι σχετικά νέα μεθοδολογία και απαιτεί σημαντικούς πόρους. Λίγοι οργανισμοί διαθέτουν τόσο τεχνολογικούς όσο και ανθρώπινους πόρους για να κάνουν αποτελεσματική αυτή τη δομή. Η πρόσληψη αναλυτών threat intelligence πλήρους απασχόλησης, μαζί με διάφορες επί πληρωμή ή ανοιχτές πηγές δεδομένων (και την τεχνολογία για την υποστήριξή τους), συχνά είναι οικονομικά δυσβάσταχτη. Ως αποτέλεσμα, λίγοι οργανισμοί μπορούν να εντάξουν έναν αναλυτή threat intelligence πλήρους απασχόλησης ως μέρος των δυνατοτήτων του CSIRT τους.

3.5. Το “War Room”

Ένας ακόμη παράγοντας που πρέπει να ληφθεί υπόψη κατά την εμπλοκή ενός CSIRT είναι η ανάγκη ύπαρξης ενός **ενιαίου χώρου** από τον οποίο θα μπορεί να λειτουργεί η ομάδα. Υπάρχουν διάφοροι όροι που χρησιμοποιούνται για τον φυσικό χώρο λειτουργίας ενός CSIRT, όπως SOC ή crisis suite, αλλά ένας απλός όρος είναι η **war room** (αίθουσα επιχειρήσεων).

Ένα war room μπορεί να δημιουργηθεί ανάλογα με τις ανάγκες, ή, σε ορισμένες περιπτώσεις, να υπάρχει μια **αφιερωμένη αίθουσα war room**. Στην πρώτη περίπτωση, μια υπάρχουσα αίθουσα συνεδριάσεων χρησιμοποιείται ως war room για όλη τη διάρκεια ενός περιστατικού. Αυτή είναι συχνά η προτιμώμενη επιλογή για οργανισμούς που δεν αντιμετωπίζουν αρκετά περιστατικά ώστε να απαιτείται μόνιμη war room.

Για οργανισμούς που αντιμετωπίζουν μεγαλύτερο αριθμό ή πιο σύνθετα περιστατικά, μπορεί να υπάρχει ανάγκη δημιουργίας μόνιμου war room. Το war room θα πρέπει να διαθέτει τις παρακάτω δυνατότητες για να διευκολύνει μια πιο οργανωμένη αντιμετώπιση των περιστατικών:

- **Χώροι εργασίας:** Κάθε μέλος της βασικής ομάδας CSIRT πρέπει να διαθέτει έναν προσωπικό χώρο εργασίας για την εκτέλεση αναλύσεων, με σύνδεση στο δίκτυο, τροφοδοσία ρεύματος και οθόνες.
- **Οθόνες για την ομάδα:** Ένα από τα προβλήματα που μπορεί να αντιμετωπίσουν τα μέλη του CSIRT είναι η αδυναμία κοινής χρήσης των αποτελεσμάτων της ανάλυσης. Ένας προβολέας ή μια μεγάλη οθόνη διευκολύνει την καλύτερη ανταλλαγή δεδομένων σε όλη την ομάδα.
- **Κοινοποίηση σημειώσεων:** Παρόμοια με την ανταλλαγή δεδομένων μέσω οθονών, μπορεί να υπάρχει ανάγκη κοινοποίησης πληροφοριών σε ομάδες που βρίσκονται σε διαφορετικές γεωγραφικές περιοχές. Αυτό μπορεί να γίνει μέσω εργαλείων συνεργασίας, όπως OneNote, SharePoint ή ένα wiki ειδικά δημιουργημένο για το περιστατικό.
- **Whiteboards:** Μεγάλος όγκος πληροφοριών διακινείται μέσα και έξω από μια war room. Δεδομένα σχετικά με αναθέσεις εργασιών ή λίστες παραβιασμένων συστημάτων είναι καλύτερα να εμφανίζονται σε whiteboard ώστε να είναι ορατά σε όλους.

- **Περιορισμένη πρόσβαση:** Η πρόσβαση στη war room πρέπει να περιορίζεται μόνο στο προσωπικό που έχει νόμιμη ανάγκη να εισέλθει. Ο περιορισμός αυτός αποτρέπει την πτώση ευαίσθητων πληροφοριών σε λάθος χέρια.
-

3.6. Επικοινωνίες

Ένας τομέας που συχνά παραβλέπεται από τους οργανισμούς είναι το πώς θα επικοινωνούν εντός ενός μεγαλύτερου οργανισμού κατά τη διάρκεια ενός περιστατικού. Με το ηλεκτρονικό ταχυδρομείο, τα άμεσα μηνύματα και τις τηλεφωνικές κλήσεις, μπορεί να φαίνεται ότι οι οργανισμοί διαθέτουν ήδη τα απαραίτητα εργαλεία για την κατάλληλη εσωτερική επικοινωνία. Ωστόσο, αυτές οι πλατφόρμες επικοινωνίας ενδέχεται να χρειαστεί να παρακαμφθούν σε περίπτωση περιστατικού που επηρεάζει διαπιστευτήρια χρηστών, συστήματα ηλεκτρονικού ταχυδρομείου ή άλλες cloud-based πλατφόρμες συνεργασίας.

Για παράδειγμα, μια κοινή επίθεση που παρατηρείται είναι ο παραβιασμός του cloud-based email του Office 365. Εάν οι επιτιθέμενοι έχουν αποκτήσει πρόσβαση στο σύστημα email, ενδέχεται να έχουν παραβιάσει και τις σχετικές εφαρμογές άμεσων μηνυμάτων, όπως το Skype. Δεδομένου αυτού, η εξάρτηση από τέτοιες εφαρμογές κατά τη διάρκεια ενός περιστατικού μπορεί στην πραγματικότητα να παρέχει στους επιτιθέμενους πληροφόρηση για τις ενέργειες του CSIRT.

Εάν υπάρχει υποψία ότι αυτές οι εφαρμογές έχουν παραβιαστεί, είναι κρίσιμο να υπάρχει μια δευτερεύουσα – και ακόμη και τριτογενής – επιλογή επικοινωνίας. Τα εμπορικά αποκτηθέντα κινητά τηλέφωνα συχνά αποτελούν ασφαλή εναλλακτική. Επιπλέον, τα μέλη του CSIRT μπορούν να χρησιμοποιήσουν δωρεάν ή χαμηλού κόστους εργαλεία συνεργασίας για περιορισμένο χρονικό διάστημα. Αυτά μπορούν να χρησιμοποιηθούν μέχρι να θεωρηθεί ασφαλές ξανά η χρήση των συνήθων πλατφορμών επικοινωνίας.

3.7. Εναλλαγή προσωπικού

Οι παρατεταμένες έρευνες περιστατικών μπορούν να επηρεάσουν το προσωπικό του CSIRT, τόσο σωματικά όσο και ψυχικά. Παρόλο που μπορεί να φαίνεται σκόπιμο να παραμείνει μια ομάδα μέχρι να αντιμετωπιστεί ένα περιστατικό, αυτό μπορεί να έχει αρνητικές συνέπειες στη λειτουργικότητα της ομάδας. Μελέτες έχουν δείξει τις αρνητικές γνωστικές επιπτώσεις της παρατεταμένης εργασίας με λίγες ώρες ανάπαυσης. Ως εκ τούτου, είναι απαραίτητο ο υπεύθυνος περιστατικού (Incident Commander, IC) να θέτει τους απαντητές σε βάρδιες μετά από μια ορισμένη χρονική περίοδο.

Για παράδειγμα, περίπου 24 ώρες μετά την έναρξη μιας έρευνας περιστατικού, θα είναι απαραίτητο να αρχίσει η εναλλαγή προσωπικού ώστε να έχουν περίοδο ανάπαυσης 8 ωρών. Αυτό περιλαμβάνει και τον IC. Κατά τη διάρκεια ενός παρατεταμένου περιστατικού, θα πρέπει να οριστεί εναλλακτικός IC, για να εξασφαλιστεί η συνέχεια και ότι κάθε IC λαμβάνει τον κατάλληλο χρόνο ανάπαυσης.

Μια άλλη στρατηγική είναι η ενεργοποίηση υποστηρικτικών στοιχείων κατά τις περιόδους αδράνειας σε ένα περιστατικό. Αυτές οι περίοδοι αδράνειας εμφανίζονται γενικά όταν ένα περιστατικό έχει περιοριστεί και η πιθανή κυκλοφορία εντολών και ελέγχου (C2) έχει αντιμετωπιστεί. Το υποστηρικτικό προσωπικό μπορεί να χρησιμοποιηθεί για την παρακολούθηση του δικτύου για τυχόν αλλαγές, δίνοντας στο CSIRT χρόνο για ανάπαυση.

3.8. Διερεύνηση περιστατικών

Το μεγαλύτερο μέρος αυτού του κεφαλαίου αναφέρεται στις διάφορες μεθόδους που μπορούν να χρησιμοποιηθούν κατά τη διερεύνηση ενός περιστατικού. Ο κύριος στόχος του CSIRT είναι να αξιοποιεί μεθόδους που ακολουθούν μια συστημική ανάλυση για να αντιμετωπίσουν τα ακόλουθα βασικά στοιχεία ενός περιστατικού:

Καθορισμός του εύρους: Σε ορισμένα περιστατικά, το πραγματικό εύρος ενδέχεται να μην είναι σαφώς καθορισμένο στο αρχικό στάδιο ανίχνευσης. Για παράδειγμα, ένας οργανισμός μπορεί να λάβει επικοινωνία από μια υπηρεσία επιβολής του νόμου, η οποία έχει αναφέρει ότι ένας διακομιστής C2 έχει απενεργοποιηθεί. Κατά την ανάλυση αυτού του συστήματος, έχει εντοπιστεί η εξωτερική IP του οργανισμού. Από αυτό το σημείο δεδομένων, το εύρος καθορίζεται αρχικά ως ολόκληρο το δίκτυο. Στη συνέχεια, το CSIRT θα αναλύσει δεδομένα από το firewall ή τον web proxy, για να προσδιορίσει τα εσωτερικά συστήματα που επικοινωνούσαν με τον διακομιστή C2. Με βάση αυτά τα δεδομένα, θα περιοριστεί το αρχικό εύρος του περιστατικού σε αυτά τα συστήματα που επηρεάστηκαν.

Κατά την προσπάθεια προσδιορισμού του εύρους του περιστατικού, υπάρχει συχνά η ανάγκη να βρεθεί το «**patient zero**» ή το πρώτο σύστημα που παραβιάστηκε. Σε ορισμένα περιστατικά, αυτό μπορεί να είναι εύκολο να εντοπιστεί, π.χ., ένα phishing email που περιέχει ένα PDF αρχείο που, όταν ανοίγεται, εκτελεί κακόβουλο λογισμικό, μπορεί εύκολα να εντοπιστεί από τον χρήστη ή τον έλεγχο ασφαλείας. Άλλες επιθέσεις μπορεί να μην είναι τόσο προφανείς. Ενώ η ανακάλυψη του patient zero παρέχει πολύτιμα δεδομένα για την ανάλυση της ρίζας του προβλήματος, είναι πιο σημαντικό να προσδιοριστεί πρώτα το εύρος του περιστατικού, παρά να εστιάσουμε σε ένα μόνο σύστημα.

Καθορισμός του αντίκτυπου: Ένας ακόμη κρίσιμος παράγοντας είναι η εκτίμηση του αντίκτυπου του περιστατικού. Όσοι είναι εξοικειωμένοι με τις βασικές έννοιες της ασφάλειας πληροφοριών γνωρίζουν καλά την τριάδα CIA (Confidentiality, Integrity, Availability – Ακεραιότητα, Διαθεσιμότητα, Εμπιστευτικότητα). Κάθε παραβίαση ή παραβίαση ασφάλειας επηρεάζει ένα ή περισσότερα από αυτά τα στοιχεία. Για παράδειγμα, ένα περιστατικό ransomware που επηρεάζει 15 παραγωγικούς διακομιστές επηρεάζει τη **διαθεσιμότητα** των δεδομένων αυτών των συστημάτων. Οι επιπτώσεις στη διαθεσιμότητα, είτε άμεσα είτε μέσω ενεργειών του επιτιθέμενου ή του χρόνου που απαιτείται για απόκριση και αποκατάσταση, είναι σημαντικοί παράγοντες για τον προσδιορισμό του αντίκτυπου του περιστατικού. Άλλα περιστατικά, όπως η κλοπή πνευματικής ιδιοκτησίας, επηρεάζουν την **εμπιστευτικότητα** των δεδομένων. Τέλος, περιστατικά που περιλαμβάνουν μη

εξουσιοδοτημένη τροποποίηση κώδικα ή άλλων δεδομένων επηρεάζουν την **ακεραιότητα** των δεδομένων.

Η κατανόηση του πιθανών επιπτώσεων ενός περιστατικού είναι σημαντική για τη λήψη αποφάσεων σχετικά με τους πόρους που θα διατεθούν για την απόκριση. Μια **επίθεση DDoS** σε μη κρίσιμη υπηρεσία στο διαδίκτυο δεν απαιτεί τον ίδιο τύπο απόκρισης με ένα malware που συλλέγει δεδομένα πιστωτικών καρτών σε υποδομή λιανικών πληρωμών. Ο αντίκτυπος επηρεάζει επίσης τη συμμόρφωση με νόμους και κανονισμούς, και η κατανόηση του αντίκτυπου είναι κρίσιμη για την ορθή αντιμετώπιση του περιστατικού.

Καθορισμός της ρίζας του προβλήματος: Η βασική ερώτηση που θα θέσουν οι IT επαγγελματίες και οι διαχειριστές κατά τη διάρκεια και ειδικά μετά από ένα περιστατικό είναι: «**Πώς συνέβη αυτό;**» Οι οργανισμοί επενδύουν σημαντικούς πόρους για να προστατεύσουν την υποδομή τους. Αν συμβεί ένα περιστατικό που προκαλεί αντίκτυπο, υπάρχει ανάγκη κατανόησης της αιτίας. Στόχος μιας έρευνας περιστατικού είναι να προσδιοριστεί η αλληλουχία γεγονότων, ευπαθειών ή άλλων συνθηκών που οδήγησαν στο περιστατικό και στον αντίκτυπο. Συχνά, η ρίζα του προβλήματος δεν είναι μια απλή ευπάθεια, αλλά μια αλληλουχία γεγονότων και συνθηκών που επέτρεψαν σε έναν επιτιθέμενο να παραβιάσει τα συστήματα ασφάλειας και να πραγματοποιήσει την επίθεσή του. Μέσω της έρευνας, αυτά τα γεγονότα και οι συνθήκες μπορούν να εντοπιστούν ώστε να διορθωθούν ή να ελεγχθούν κατάλληλα.

Ανάθεση ευθυνών περιστατικού: Ένας τομέας συζήτησης κατά τη διερεύνηση ενός περιστατικού είναι η ανάθεση ευθυνών (attribution). Με την ανάθεση, το CSIRT ή το ερευνητικό σώμα προσπαθεί να καθορίσει ποιος οργανισμός βρίσκεται πίσω από την επίθεση. Τα περιστατικά μπορεί να αποδοθούν σε **κρατικούς φορείς, εγκληματικές ομάδες** ή άλλους κυβερνο-αντιπάλους. Αν και η ανάθεση έχει κάποια σημασία από την οπτική της **πληροφοριακής απειλής**, οι πόροι είναι καλύτερα να αφιερωθούν στην έρευνα ή την περιχαράκωση ενός περιστατικού. Η προσπάθεια προσδιορισμού της ομάδας που ευθύνεται είναι χρονοβόρα και σπάνια αποφέρει θετικά αποτελέσματα. Αν η ηγεσία του οργανισμού επιμένει στην ανάθεση, η καλύτερη προσέγγιση είναι η πλήρης τεκμηρίωση του περιστατικού και η παράδοση των δεδομένων σε τρίτο μέρος που ειδικεύεται στην ανάθεση. Τέτοιοι οργανισμοί συνήθως συνδυάζουν δεδομένα από πολλές έρευνες περιστατικών για να δημιουργήσουν φάκελο για ομάδες. Αν τα δεδομένα ταιριάζουν, μπορούν να παρέχουν κάποιο πλαίσιο όσον αφορά την ανάθεση.

3.9. Ενσωμάτωση στρατηγικών περιορισμού (containment strategies)

Οι στρατηγικές περιορισμού είναι οι ενέργειες που λαμβάνονται κατά τη διάρκεια ενός περιστατικού για να περιοριστεί η ζημιά σε συγκεκριμένα συστήματα ή περιοχές του δικτύου. Είναι κρίσιμο για τους οργανισμούς να έχουν προετοιμάσει αυτές τις στρατηγικές σε περίπτωση περιστατικού. Η αύξηση του ransomware, το οποίο συνδυάζει στοιχεία ιών και worms που μπορούν να εξαπλωθούν γρήγορα σε έναν οργανισμό, τονίζει την ανάγκη για ταχεία περιορισμό μιας μόλυνσης πριν επηρεάσει πολλά συστήματα.

Προσθέτοντας στην πρόκληση του περιορισμού είναι το γεγονός ότι πολλά επιχειρησιακά συστήματα πληροφορικής χρησιμοποιούν μια «flat» τοπολογία, όπου η πλειονότητα των συστημάτων μπορεί να επικοινωνεί μεταξύ τους. Σε αυτού του είδους το περιβάλλον, το ransomware και άλλα worms μπορούν να εξαπλωθούν γρήγορα μέσω νόμιμων πρωτοκόλλων, όπως οι Remote Desktop Services (RDS) ή το Server Message Block (SMB), όπως έγινε δημοφιλές κατά την εκστρατεία του ransomware WannaCry, που εκμεταλλεύτηκε την ευπάθεια EternalBlue στο SMB των Windows. Για περισσότερες πληροφορίες, επισκεφθείτε: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144>.

Για να αντιμετωπιστεί ο περιορισμός, ένας οργανισμός πρέπει να έχει σαφή εικόνα της τοπολογίας του δικτύου. Αυτός ο τύπος επίγνωσης του δικτύου μπορεί να επιτευχθεί μέσω των αποτελεσμάτων εργαλείων ανακάλυψης δικτύου, ενημερωμένων διαγραμμάτων δικτύου, καταλόγων συστημάτων και σαρώσεων ευπαθειών. Αυτά τα δεδομένα πρέπει να κοινοποιούνται στην CSIRT, ώστε να επιτευχθεί μια συνολική εικόνα του δικτύου. Από εκεί, η CSIRT πρέπει να συντονίζει τα σχέδια περιορισμού με το προσωπικό λειτουργίας δικτύου, ώστε να δημιουργηθεί μια συνολική στρατηγική περιορισμού και να περιοριστεί η πιθανή ζημιά από ένα περιστατικό. Η συμμετοχή του προσωπικού λειτουργίας δικτύου ως μέρος της τεχνικής υποστήριξης διευκολύνει τη διαδικασία και εξασφαλίζει ότι ο περιορισμός επιτυγχάνεται όσο το δυνατόν πιο γρήγορα.

Ένας άλλος παράγοντας που επηρεάζει άμεσα τη διαχείριση περιστατικών είναι η διαχείριση αλλαγών. Οι ώριμες υποδομές πληροφορικής συνήθως έχουν καλά τεκμηριωμένη και ελεγχόμενη διαδικασία διαχείρισης αλλαγών. Ωστόσο, κατά τη διάρκεια ενός περιστατικού, η CSIRT και το υποστηρικτικό προσωπικό δεν μπορούν να περιμένουν την εξουσιοδότηση αλλαγών και το κατάλληλο παράθυρο για αλλαγές. Όταν εφαρμόζονται στρατηγικές περιορισμού, η ηγεσία της IT και του οργανισμού πρέπει να κατανοεί πλήρως ότι οι αλλαγές θα γίνουν βάσει του περιστατικού. Αυτό δεν απαλλάσσει την CSIRT και το προσωπικό IT από την υποχρέωση προσοχής και τεκμηρίωσης των αλλαγών.

Σε ό,τι αφορά τον περιορισμό ενός περιστατικού malware, όπως επίθεσης ransomware, υπάρχουν διάφορες στρατηγικές που μπορούν να εφαρμοστούν. Ιδανικά, οι οργανισμοί θα πρέπει να έχουν τη δυνατότητα απομόνωσης τμημάτων του δικτύου μεταξύ τους. Αν αυτό δεν είναι δυνατό, η CSIRT και το προσωπικό IT μπορούν να λάβουν ένα ή περισσότερα από τα ακόλουθα μέτρα:

Φυσικός περιορισμός (Physical containment): Σε αυτήν την περίπτωση, η φυσική σύνδεση στο δίκτυο αφαιρείται από το σύστημα. Αυτό μπορεί να είναι τόσο απλό όσο η αποσύνδεση του καλωδίου δικτύου, η απενεργοποίηση της ασύρματης πρόσβασης ή η απενεργοποίηση της σύνδεσης μέσω του λειτουργικού συστήματος. Παρά την απλότητά του, υπάρχουν παράγοντες που καθιστούν αυτή τη στρατηγική δύσκολη ακόμα και για μικρούς οργανισμούς. Πρώτον, η ικανότητα εντοπισμού των επηρεασμένων συστημάτων. Σε ένα data center, αυτό μπορεί να είναι απλό, αλλά σε ένα μεγάλο εταιρικό περιβάλλον η φυσική εντόπιση 20-30 υπολογιστών απαιτεί μεγάλη προσπάθεια. Στο διάστημα που αφαιρούνται τα συστήματα από το δίκτυο, το malware μπορεί να έχει ήδη εξαπλωθεί σε άλλα συστήματα. Επιπλέον, η γεωγραφική διασπορά των συστημάτων δυσκολεύει περαιτέρω τον περιορισμό. Ο φυσικός περιορισμός πρέπει να χρησιμοποιείται μόνο σε περιστατικά περιορισμένου εύρους όπου η CSIRT μπορεί άμεσα να αποσυνδέσει τα συστήματα από το δίκτυο.

Περιορισμός δικτύου (Network containment): Η στρατηγική περιορισμού δικτύου βασίζεται στην εμπειρογνωμοσύνη δικτυακών μηχανικών ή αρχιτεκτόνων. Για αυτόν τον λόγο, συχνά συμμετέχουν στην CSIRT και εμπλέκονται στον σχεδιασμό στρατηγικών περιορισμού. Ο διαχειριστής δικτύου αναλαμβάνει την τροποποίηση ρυθμίσεων switch για να περιοριστεί η κυκλοφορία από μολυσμένα συστήματα σε άλλα μέρη του δικτύου. Αυτό μπορεί να απαιτεί τροποποιήσεις σε μεμονωμένα switches ή μέσω της κονσόλας διαχείρισης. Πρέπει να ληφθεί υπόψη η διαδικασία ελέγχου αλλαγών, ώστε να υπάρχει εξαίρεση για γρήγορη εφαρμογή αλλαγών κατά τη διάρκεια περιστατικών. Οι αλλαγές πρέπει να τεκμηριώνονται για πιθανή αναστροφή κατά τη φάση αποκατάστασης.

Περιορισμός περιμέτρου (Perimeter containment): Το firewall περιμέτρου μπορεί να χρησιμοποιηθεί αποτελεσματικά για περιορισμό. Σε ορισμένες περιπτώσεις, μπορεί να χρησιμοποιηθεί σε συνδυασμό με τον περιορισμό δικτύου, με προσέγγιση «ρώσικης κούκλας», όπου η CSIRT περιορίζει την κυκλοφορία στο firewall και προχωρά προς τα επιμέρους υποδίκτυα με τα επηρεασμένα συστήματα. Για παράδειγμα, αν το malware κατεβάζει επιπλέον κώδικα μέσω PowerShell, η εξωτερική IP που χρησιμοποιείται μπορεί να αποκλειστεί στο firewall για να αποτραπεί περαιτέρω ζημιά. Οι κανόνες μπορούν να παραμείνουν έως ότου κριθεί ότι δεν χρειάζονται πλέον. Οι αλλαγές στο firewall πρέπει επίσης να τεκμηριώνονται και να λαμβάνεται υπόψη η διαδικασία ελέγχου αλλαγών.

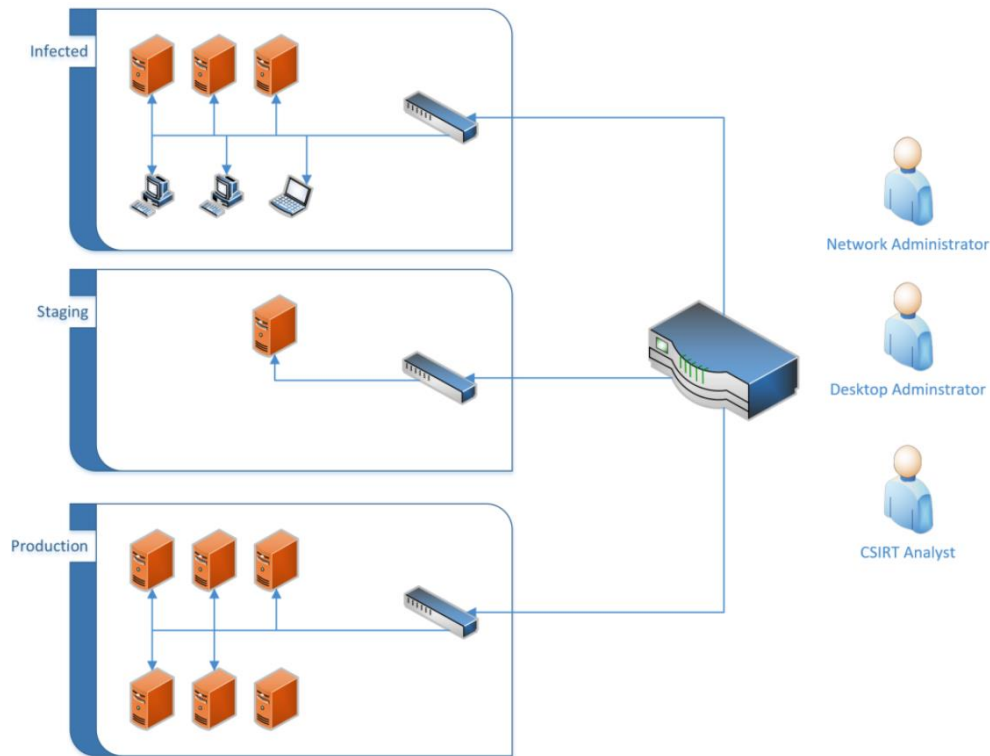
Εικονικός περιορισμός (Virtual containment): Με την άνοδο του cloud computing και της εικονικοποίησης, πολλά συστήματα, όπως servers, έχουν μεταφερθεί μερικώς ή πλήρως σε εικονικά περιβάλλοντα. Η εικονικοποίηση προσφέρει ευελιξία και επιτρέπει την αποσύνδεση πολλαπλών συστημάτων από το δίκτυο ταυτόχρονα μέσω του hypervisor (π.χ., VMware ESXi). Μπορεί επίσης να χρησιμοποιηθεί εικονικός διακόπτης για περιορισμό, όπως με τα φυσικά switches, ή να «παγώσουν» τα εικονικά συστήματα κατά τη διάρκεια του περιστατικού, διατηρώντας στοιχεία που μπορούν να εξεταστούν αργότερα.

3.10. Στρατηγικές Εκρίζωσης

Η δυσάρεστη πραγματικότητα με το σύγχρονο κακόβουλο λογισμικό είναι ότι δεν υπάρχει ασφαλής τρόπος να είμαστε 100% βέβαιοι ότι όλος ο κακόβουλος κώδικας έχει αφαιρεθεί. Στο παρελθόν, οι οργανισμοί μπορούσαν απλώς να σαρώσουν το σύστημα με ένα πρόγραμμα αντι-ιών για να εντοπίσουν τον επιβλαβή κώδικα. Τώρα, με τεχνικές κακόβουλου λογισμικού όπως η έγχυση διεργασιών (process injection) ή η κατάληψη DLL (DLL hijacking), ακόμη και αν αφαιρεθεί ο αρχικός κώδικας, υπάρχει πιθανότητα το σύστημα να παραμένει μολυσμένο. Υπάρχει επίσης η πιθανότητα πρόσθετος κώδικας που έχει κατεβεί να έχει εγκατασταθεί και να μην ανιχνεύεται. Ως αποτέλεσμα, οι περισσότερες στρατηγικές εκρίζωσης βασίζονται στη λήψη των μολυσμένων μηχανών και την επανεγκατάστασή τους με μια γνωστή καλή εικόνα (known good image) ή την επαναφορά από ένα γνωστό καλό αντίγραφο ασφαλείας (backup).

Μια στρατηγική που χρησιμοποιείται συχνά σε περιπτώσεις κακόβουλου λογισμικού και ransomware είναι η χρήση τριών ξεχωριστών εικονικών LAN (VLAN) και η επανεγκατάσταση των μολυσμένων

μηχανών. Αρχικά, όλες οι μολυσμένες μηχανές τοποθετούνται σε ένα ξεχωριστό VLAN. Στη συνέχεια, το CSIRT ή ο διαχειριστής συστήματος μεταφέρει μία από τις μολυσμένες συσκευές σε ένα δευτερεύον VLAN σταδίου (staging VLAN). Το σύστημα επανεγκαθίσταται με μια γνωστή καλή εικόνα ή χρησιμοποιείται ένα γνωστό καλό αντίγραφο ασφαλείας. Αφού ολοκληρωθεί η επανεγκατάσταση ή η εγκατάσταση του backup, το σύστημα μεταφέρεται σε ένα παραγωγικό VLAN (production VLAN), όπου πραγματοποιείται επιπλέον παρακολούθηση για να διασφαλιστεί ότι δεν υπάρχει υπολειπόμενη μόλυνση ή παραβίαση.



Αν και αυτή η μέθοδος μπορεί να είναι χρονοβόρα, αποτελεί έναν εξαιρετικό τρόπο για να διασφαλιστεί ότι όλα τα συστήματα που επηρεάστηκαν έχουν αντιμετωπιστεί.

Στην περίπτωση εικονικών συστημάτων, αν έχει εφαρμοστεί η στρατηγική περιορισμού (containment) που συζητήθηκε προηγουμένως, τα μολυσμένα εικονικά συστήματα δεν έχουν συνδεσιμότητα δικτύου. Σε αυτή την περίπτωση, η πιο απλή στρατηγική εκρίζωσης είναι η επαναφορά των συστημάτων στην τελευταία γνωστή καλή στιγμιότυπη κατάσταση (last-known good snapshot). Μόλις το σύστημα επανεκκινηθεί, πρέπει να συνδεθεί στο VLAN με ενισχυμένη παρακολούθηση. Είναι σημαντικό ότι στην περίπτωση επαναφοράς από στιγμιότυπα, το CSIRT πρέπει να έχει υψηλή εμπιστοσύνη στη χρονική σειρά των γεγονότων. Αν το CSIRT δεν είναι σίγουρο για τη χρονική ακολουθία της επίθεσης, υπάρχει πιθανότητα το στιγμιότυπο να έχει επίσης υποστεί παραβίαση. Αυτό ισχύει ιδιαίτερα σε οργανισμούς που πραγματοποιούν τακτικά λήψεις στιγμιότυπων.

3.11. Στρατηγικές Ανάκαμψης

Στο πλαίσιο της ανάκαμψης, υπάρχουν αρκετές ενέργειες που πρέπει να διαχειριστεί το CSIRT για να επαναφέρει τις λειτουργίες σε κανονική κατάσταση. Η πρώτη από αυτές είναι να διασφαλιστεί ότι όλα τα συστήματα—όχι μόνο αυτά που πέρασαν από τη φάση εκρίζωσης, αλλά όλα τα συστήματα—έχουν εγκαταστήσει σωστά τις πιο πρόσφατες ενημερώσεις ασφαλείας (patches). Αυτό είναι κρίσιμο σε περιπτώσεις όπου ο επιτιθέμενος έχει εκμεταλλευτεί μια ευπάθεια μηδενικής ημέρας (zero-day exploit) ή μια σχετικά νέα ευπάθεια. Σε περιπτώσεις όπου δεν υπάρχει διαθέσιμο patch από τον κατασκευαστή, το CSIRT θα πρέπει να προτείνει επιπλέον μέτρα ασφαλείας για να μειώσει τυχόν υπολειπόμενο κίνδυνο.

Δεύτερον, στη φάση ανάκαμψης, το CSIRT θα πρέπει να συνεργαστεί με το προσωπικό IT και ασφάλειας πληροφοριών για τη δημιουργία επιπλέον ειδοποιήσεων ανίχνευσης και πρόληψης. Κατά την εξέταση των αποδεικτικών στοιχείων για τον εντοπισμό της βασικής αιτίας ή κατά τη φάση περιορισμού, το CSIRT μπορεί να έχει παρέχει δεδομένα για τους ελέγχους ανίχνευσης και πρόληψης. Το CSIRT πρέπει να συνεργαστεί με το υπόλοιπο προσωπικό για να ενισχύσει αυτούς τους ελέγχους με επιπλέον κανόνες ανίχνευσης και πρόληψης, οι οποίοι μπορεί να σχετίζονται ειδικά με το περιστατικό ή με συγκεκριμένες εντοπισμένες ευπάθειες.

Τρίτον, οποιεσδήποτε αλλαγές έγιναν στην υποδομή θα πρέπει να εξεταστούν. Αυτές οι αλλαγές μπορούν αρχικά να αναθεωρηθούν από το CSIRT και το προσωπικό IT, για να καθοριστεί αν εξακολουθούν να είναι απαραίτητες ή μπορούν να αφαιρεθούν. Εάν οι αλλαγές είναι απαραίτητες μακροπρόθεσμα, θα πρέπει να αξιολογηθούν από τη διαδικασία ελέγχου αλλαγών του οργανισμού και να εγκριθούν σύμφωνα με αυτήν.

Τέταρτον, πριν κλείσει ένα περιστατικό, είναι καλό να διεξαχθεί πλήρης σάρωση ευπαθειών σε όλα τα συστήματα. Αυτό είναι κρίσιμο για να διασφαλιστεί ότι όλα τα συστήματα που έχουν παραβιαστεί έχουν αντιμετωπιστεί. Επιπλέον, αυτό το βήμα διασφαλίζει ότι και άλλα συστήματα, τα οποία δεν επηρεάστηκαν από το περιστατικό ασφαλείας, έχουν εγκαταστήσει τα απαραίτητα patches για οποιεσδήποτε ευπάθειες.

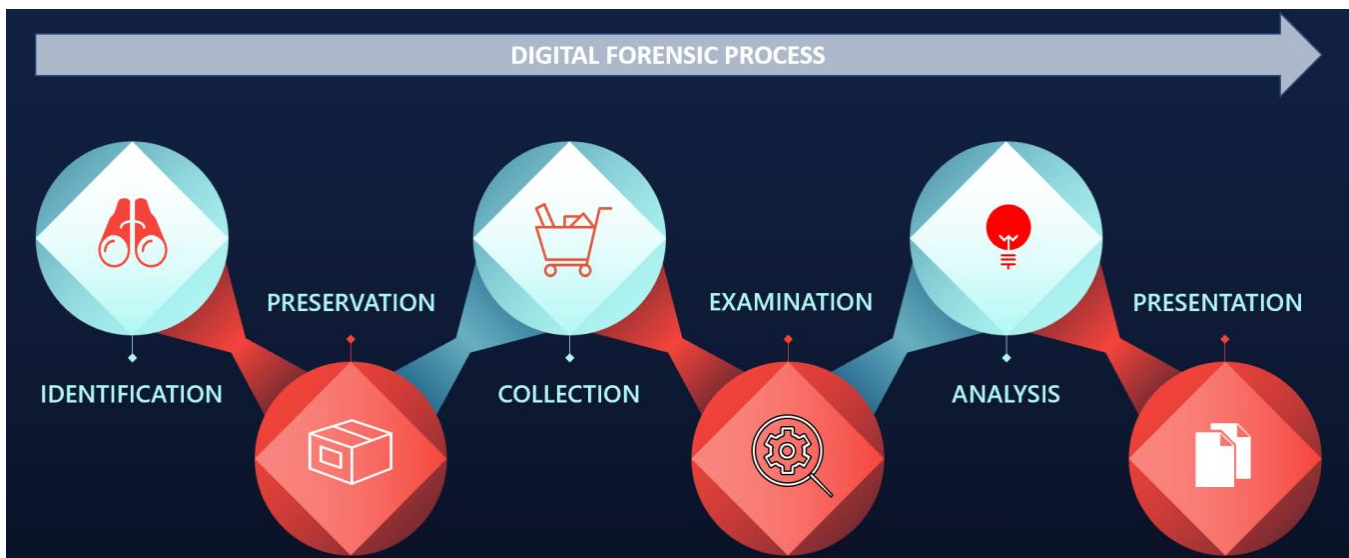
Τέλος, μετά την ολοκλήρωση ενός περιστατικού, είναι σημαντικό να διεξαχθεί μια ανασκόπηση μετά την ενέργεια (after-action review). Αυτή η ανασκόπηση καλύπτει ολόκληρο το περιστατικό, από την αρχή μέχρι το τέλος. Εξετάζονται όλες οι ενέργειες που ανέλαβε το προσωπικό του CSIRT, καθώς και τα σχέδια και τα playbooks που χρησιμοποιήθηκαν με βάση τις ενέργειες του περιστατικού. Οποιοσδήποτε ελλείψεις, όπως η έλλειψη συγκεκριμένων εργαλείων, εκπαίδευσης ή διαδικασιών, πρέπει να εντοπιστούν ώστε να διορθωθούν. Το αποτέλεσμα αυτής της ανασκόπησης θα πρέπει να τεκμηριώνεται ως μέρος της συνολικής τεκμηρίωσης του περιστατικού.

4

Βασικά Στοιχεία Digital Forensics

Όπως αναφέρθηκε στο προηγούμενο κεφάλαιο, η ψηφιακή διερμηνεία αποτελεί σημαντικό στοιχείο της αντίδρασης σε περιστατικά (incident response). Συχνά, η εφαρμογή μεθόδων ψηφιακής διερμηνείας επιτρέπει στους αναλυτές περιστατικών να κατανοήσουν σαφώς την αλληλουχία γεγονότων που οδήγησαν σε κακόβουλη ενέργεια, όπως ένας παραβιασμένος διακομιστής ή διαρροή δεδομένων. Σε άλλα περιστατικά, όπως η εσωτερική απάτη ή η κακόβουλη δραστηριότητα εσωτερικών χρηστών, η ψηφιακή διερμηνεία μπορεί να παρέχει το «καπνιστό όπλο» που υποδεικνύει τον υπεύθυνο.

Πριν από την ανάλυση των εργαλείων και τεχνικών που χρησιμοποιούν οι αναλυτές περιστατικών, είναι κρίσιμο να εξεταστούν τα θεμελιώδη στοιχεία της ψηφιακής διερμηνείας. Αυτά τα στοιχεία παρέχουν όχι μόνο το πλαίσιο για συγκεκριμένες ενέργειες, αλλά και μια μεθοδολογία για να διασφαλιστεί ότι τα αποδεικτικά στοιχεία που εντάσσονται σε μια έρευνα περιστατικού είναι έγκυρα και χρησιμοποιήσιμα.



Διαδικασία Ψηφιακής Διερμηνείας: Όπως και η διαδικασία αντίδρασης σε περιστατικά, η διαδικασία ψηφιακής διερμηνείας ορίζει τη ροή των ψηφιακών αποδεικτικών στοιχείων που σχετίζονται με ένα περιστατικό — από τη στιγμή που αυτά εντοπίζονται για πρώτη φορά έως τη στιγμή που παρουσιάζονται σε ανώτερα στελέχη ή σε αρμόδια αρχή, όπως πολιτικό ή ποινικό δικαστήριο. Υπάρχουν αρκετά σχήματα που καθορίζουν αυτή τη διαδικασία, και για το μεγαλύτερο μέρος τους

ακολουθούν παρόμοια πορεία. Στο παρόν πλαίσιο, χρησιμοποιούμε το **Digital Forensics Research Workshop (DFRWS) digital investigation framework**, το οποίο απεικονίζει τη διαδικασία διερεύνησης ψηφιακών αποδεικτικών στοιχείων με συστηματικό τρόπο.

Το πλαίσιο περιλαμβάνει έξι στοιχεία:

1. Ταυτοποίηση (Identification)
2. Διατήρηση (Preservation)
3. Συλλογή (Collection)
4. Εξέταση (Examination)
5. Ανάλυση (Analysis)
6. Παρουσίαση (Presentation)

Από την οπτική της αντίδρασης σε περιστατικά, το προσωπικό συνήθως δεν κατασχέσει δίκτυα ή κρίσιμα συστήματα και δεν τα θέτει εκτός λειτουργίας, εκτός εάν υπάρχει επαρκής λόγος. Αυτό αποτελεί μία από τις ισορροπίες που είναι εγγενείς στην ψηφιακή διερμηνεία και την αντίδραση σε περιστατικά.

Μια καθαρά ψηφιακή διερμηνευτική προσέγγιση θα συλλέξει όλα τα σχετικά αποδεικτικά στοιχεία, θα τα ασφαλίσει και θα τα επεξεργαστεί. Αυτή η διαδικασία μπορεί να διαρκέσει μήνες, ανάλογα με τον τύπο του περιστατικού. Αν και αυτή η προσέγγιση είναι λεπτομερής και εκτενής, μπορεί να αφήσει έναν οργανισμό χωρίς κρίσιμα συστατικά για κάποιο διάστημα. Οι αναλυτές που ανατίθενται σε ένα CSIRT πρέπει να είναι έτοιμοι να ισορροπήσουν την ανάγκη για λεπτομερή διερεύνηση με την ανάγκη επανέναρξης ή συνέχισης των κανονικών λειτουργιών.

4.1. Ταυτοποίηση

Ένα από τα βασικά αρχές που συζητούνται συχνά στην εγκληματολογία είναι η αρχή ανταλλαγής του Locard. Αυτή η αρχή υποστηρίζει ότι, όταν δύο αντικείμενα έρχονται σε επαφή, αφήνουν ίχνη το ένα πάνω στο άλλο. Για παράδειγμα, αν περπατήσετε σε ένα σπίτι με χαλί, η βρωμιά από τα παπούτσια σας θα μείνει στο χαλί και το χαλί θα αφήσει ίνες στις σόλες των παπουτσιών σας.

Αυτά τα ίχνη που ανταλλάσσονται αποτελούν τη βάση αυτού που ονομάζεται **ίχνη αποδεικτικών στοιχείων** στον φυσικό κόσμο της εγκληματολογίας. Στον ψηφιακό κόσμο, συχνά παρατηρούνται πολύ παρόμοια ίχνη όταν δύο συστήματα έρχονται σε επαφή μεταξύ τους. Για παράδειγμα, αν ένα άτομο επισκεφτεί έναν ιστότοπο, ο web server ή το firewall της εφαρμογής μπορεί να καταγράψει τη διεύθυνση IP του ατόμου σε ένα αρχείο καταγραφής. Ο ιστότοπος μπορεί επίσης να τοποθετήσει ένα cookie στο laptop του ατόμου. Όπως και στον φυσικό κόσμο, τα στοιχεία που ανταλλάσσονται με αυτόν τον τρόπο μπορεί να είναι προσωρινά και η δυνατότητά μας να τα παρατηρήσουμε περιορίζεται στα εργαλεία και τις γνώσεις που διαθέτουμε εκείνη τη στιγμή.

Αυτή η αρχή μπορεί να καθοδηγήσει την **ταυτοποίηση πιθανών πηγών αποδεικτικών στοιχείων** κατά τη διάρκεια ενός περιστατικού. Για παράδειγμα, αν μια ομάδα CSIRT προσπαθεί να προσδιορίσει την αιτία μιας μόλυνσης από malware σε ένα σύστημα, θα ξεκινήσει αναλύοντας το μολυσμένο σύστημα. Καθώς ορισμένο malware απαιτεί πρόσβαση σε C2 server, οι αναλυτές μπορούν να ελέγξουν τα logs του firewall ή του proxy για οποιαδήποτε εξερχόμενη κίνηση από το μολυσμένο σύστημα προς εξωτερικές διευθύνσεις IP. Η ανασκόπηση αυτών των IP διευθύνσεων μπορεί να αποκαλύψει τον C2 server και ενδεχομένως περισσότερες λεπτομέρειες για την συγκεκριμένη παραλλαγή του malware που μολύνει το σύστημα.

Πρέπει να σημειωθεί ότι οι δράστες απειλών μπορούν πολύ εύκολα να παραποιήσουν ψηφιακά στοιχεία, οπότε η εμπιστοσύνη σε ένα μόνο ψηφιακό αποδεικτικό στοιχείο χωρίς άλλα επαληθευμένα στοιχεία πρέπει να αντιμετωπίζεται με προσοχή. Πρέπει να επιβεβαιώνεται πριν θεωρηθεί αξιόπιστο.

4.2. Διατήρηση

Μόλις τα αποδεικτικά στοιχεία εντοπιστούν, είναι σημαντικό να προστατευτούν από οποιοδήποτε είδος τροποποίησης ή διαγραφής. Για στοιχεία όπως αρχεία καταγραφής (log files), μπορεί να χρειαστεί να ενεργοποιηθούν μέτρα ελέγχου που τα προστατεύουν από αφαίρεση ή τροποποίηση. Σε ό,τι αφορά τα συστήματα υπολογιστών όπως desktops, μπορεί να είναι απαραίτητο να απομονωθεί το σύστημα από το υπόλοιπο δίκτυο, είτε με φυσικούς είτε με λογικούς ελέγχους, ελέγχους πρόσβασης στο δίκτυο ή περιμετρικούς ελέγχους. Είναι επίσης κρίσιμο να μην επιτρέπεται σε χρήστες να έχουν πρόσβαση σε ένα ύποπτο σύστημα, ώστε να αποφευχθεί η εκ προθέσεως ή ακούσια αλλοίωση των στοιχείων.

Μια άλλη διάσταση των μέτρων διατήρησης είναι η αυξημένη χρήση **εικονικών πλατφορμών**. Η διατήρηση αυτών των συστημάτων μπορεί να επιτευχθεί μέσω της δημιουργίας **snapshots** και της αποθήκευσης των εικονικών μηχανών σε μη πτητικά μέσα αποθήκευσης.

4.3. Συλλογή

Το στάδιο της συλλογής είναι εκεί που οι εξεταστές ψηφιακής εγκληματολογίας ξεκινούν τη διαδικασία απόκτησης ψηφιακών στοιχείων. Όταν εξετάζονται ψηφιακά στοιχεία, είναι σημαντικό να κατανοήσουμε τη **μεταβλητότητα** ορισμένων αποδεικτικών στοιχείων που θέλει να ελέγξει ο εξεταστής.

Μεταβλητά στοιχεία είναι αυτά που μπορούν να χαθούν όταν ένα σύστημα απενεργοποιηθεί. Για εξοπλισμό δικτύου, αυτά μπορεί να περιλαμβάνουν ενεργές συνδέσεις ή δεδομένα καταγραφής που αποθηκεύονται στη συσκευή. Για laptops και desktops, μεταβλητά δεδομένα περιλαμβάνουν τη μνήμη RAM που χρησιμοποιείται και την cache του **Address Resolution Protocol (ARP)**.

Η **Internet Engineering Task Force (IETF)** δημιούργησε ένα έγγραφο με τίτλο *Guidelines for Evidence Collection and Archiving (RFC 3227)*, το οποίο περιγράφει τη σειρά μεταβλητότητας των ψηφιακών στοιχείων ως εξής:

- **Καταχωρητές και cache:** Πίνακας δρομολόγησης, ARP cache, πίνακας διεργασιών, στατιστικά πυρήνα, μνήμη RAM
- **Προσωρινά συστήματα αρχείων**
- **Δίσκος**
- **Απομακρυσμένα logs και δεδομένα παρακολούθησης**
- **Φυσική διαμόρφωση, τοπολογία δικτύου**
- **Αρχειακά μέσα**

Είναι απαραίτητο οι εξεταστές ψηφιακής εγκληματολογίας να λάβουν υπόψη αυτή τη μεταβλητότητα όταν ξεκινούν τη συλλογή στοιχείων. Πρέπει να χρησιμοποιούνται μέθοδοι που επιτρέπουν τη συλλογή των μεταβλητών στοιχείων και τη μεταφορά τους σε **μη πτητικά μέσα**, όπως ένας εξωτερικός σκληρός δίσκος.

4.4. Σωστή διαχείριση αποδεικτικών στοιχείων

Η σωστή διαχείριση και ασφάλιση των αποδεικτικών στοιχείων είναι κρίσιμη. Λάθη στον τρόπο απόκτησης των αποδεικτικών στοιχείων μπορεί να οδηγήσουν σε αλλοίωσή τους και, κατ' επέκταση, να μην είναι εγκληματολογικά αξιόπιστα. Επιπλέον, αν ένα περιστατικό περιλαμβάνει πιθανές νομικές συνέπειες, κρίσιμα στοιχεία μπορούν να αποκλειστούν από τη διαδικασία σε ποινική ή αστική δίκη. Υπάρχουν ορισμένες βασικές αρχές για τη διαχείριση των αποδεικτικών στοιχείων που πρέπει να ακολουθούνται, όπως αναφέρονται παρακάτω:

Αλλοίωση των αρχικών στοιχείων: Οι ενέργειες των εξεταστών ψηφιακών αποδεικτικών στοιχείων δεν πρέπει να αλλοιώνουν τα αρχικά στοιχεία. Για παράδειγμα, ένας αναλυτής εγκληματολογικών στοιχείων δεν πρέπει να έχει πρόσβαση σε ένα σύστημα που λειτουργεί αν δεν είναι απαραίτητο. Πρέπει να σημειωθεί ότι ορισμένες από τις διαδικασίες που θα εξεταστούν έχουν τη δυνατότητα να αλλοιώσουν κάποια στοιχεία. Ενσωματώνοντας σωστή τεκμηρίωση και έχοντας δικαιολογημένο λόγο, οι εξεταστές μπορούν να μειώσουν την πιθανότητα τα στοιχεία να θεωρηθούν αλλοιωμένα.

Τεκμηρίωση: Ένα βασικό θέμα που συχνά ακούγεται στις δυνάμεις επιβολής του νόμου είναι η φράση: «Αν δεν το έγραψες, δεν συνέβη». Αυτό ισχύει ιδιαίτερα στη ψηφιακή εγκληματολογία. Κάθε ενέργεια που πραγματοποιείται πρέπει να τεκμηριώνεται με κάποιο τρόπο, συμπεριλαμβανομένων λεπτομερών σημειώσεων και διαγραμμάτων. Ένας άλλος τρόπος τεκμηρίωσης είναι μέσω φωτογραφιών. Η σωστή τεκμηρίωση επιτρέπει στους εξεταστές να ανακατασκευάσουν την αλληλουχία γεγονότων εάν ποτέ τεθεί υπό αμφισβήτηση η ακεραιότητα των στοιχείων.

Υπάρχει ευρύ φάσμα πόρων από διάφορες υπηρεσίες επιβολής του νόμου σχετικά με τη σωστή διαχείριση αποδεικτικών στοιχείων στο πεδίο. Είναι σημαντικό να εξοικειωθείτε με αυτές τις διαδικασίες. Οι παρακάτω οδηγίες χρησιμοποιούνται από υπηρεσίες επιβολής του νόμου:

- <http://www.crime-scene-investigator.net/SeizingElectronicEvidence.pdf>
- <https://www.ncjrs.gov/pdffiles1/nij/219941.pdf>
- <https://www.iacpcybercenter.org/wp-content/uploads/2015/04/digitalevidence-booklet-051215.pdf>

4.5. Αλυσίδα Κηδεμονίας (Chain of Custody)

Η αλυσίδα κηδεμονίας περιγράφει την τεκμηρίωση ενός αποδεικτικού στοιχείου καθ' όλη τη διάρκεια ζωής του. Αυτή η διάρκεια ζωής ξεκινά από τη στιγμή που ένα άτομο αναλαμβάνει για πρώτη φορά την κατοχή του αποδεικτικού στοιχείου και συνεχίζεται μέχρι την τελική διαχείριση του περιστατικού, όπου το στοιχείο μπορεί είτε να επιστραφεί είτε να καταστραφεί.



Computer Security Incident Response Chain of Custody Form

Incident Information

CSIRT Intake ID:	Analyst	Submission #:
--	-------------------------------------	---

Electronic Media Details

Item Number: 	Description: 		
Manufacturer: 	Model# 	Serial Number: 	

Image or File Details

Date / Time Acquired: 	Created By: 	Method: 	Storage Drive:
File/Image Name: 		Hash: 	

Chain of Custody

Tracking No:	Date/Time:	FROM:	TO:	Reason:
	Date:	Name/Org:	Name/Org:	
	Time:	Signature:	Signature:	
	Date:	Name/Org:	Name/Org:	

Η διατήρηση σωστής αλυσίδας κηδεμονίας είναι κρίσιμη. Σε περίπτωση που ένα αποδεικτικό στοιχείο πρέπει να παρουσιαστεί σε δικαστήριο, οποιοδήποτε κενό στην αλυσίδα κηδεμονίας μπορεί να οδηγήσει στο να αποκλειστεί το στοιχείο από τη διαδικασία. Είναι, επομένως, ζωτικής σημασίας να διασφαλιστεί ότι όλη η διάρκεια ζωής του αποδεικτικού στοιχείου καταγράφεται επακριβώς.

Υπάρχουν δύο κύριοι τρόποι με τους οποίους μια ομάδα CSIRT μπορεί να καταγράψει και να διατηρήσει την αλυσίδα κηδεμονίας ενός αποδεικτικού στοιχείου:

1. **Ηλεκτρονικά:** Υπάρχουν κατασκευαστές που παρέχουν σε οργανισμούς, όπως εργαστήρια εγκληματολογίας ή υπηρεσίες επιβολής του νόμου, υλικό και λογισμικό που αυτοματοποιεί τη διαδικασία αλυσίδας κηδεμονίας. Αυτά τα συστήματα χρησιμοποιούν μοναδικά αυτοκόλλητα με γραμμωτούς κώδικες για κάθε αποδεικτικό στοιχείο. Ένας σαρωτής δημιουργεί στη συνέχεια ένα ηλεκτρονικό ίχνος καθώς διαβάζει αυτούς τους γραμμωτούς κώδικες.
2. **Μέθοδος χαρτιού και στυλό:** Αυτή η μέθοδος χρησιμοποιεί έντυπα που περιέχουν τις απαραίτητες πληροφορίες για να ξεκινήσει και να διατηρηθεί η αλυσίδα κηδεμονίας. Παρόλο που η μέθοδος χαρτιού και στυλού μπορεί να είναι πιο χρονοβόρα και απαιτεί μεγαλύτερη προσοχή για να διασφαλιστεί ότι το έντυπο προστατεύεται από καταστροφή ή χειραγώγηση, αποτελεί μια πολύ πιο οικονομική λύση για μικρότερες ομάδες CSIRT που δεν διαθέτουν τους πόρους για να υλοποιήσουν μια αυτοματοποιημένη λύση.

Όσον αφορά τα στοιχεία που περιέχει ένα σωστό έντυπο αλυσίδας κηδεμονίας, υπάρχουν πολλές ενότητες, η κάθε μία με λεπτομέρειες που πρέπει να καταγραφούν. Παρακάτω υπάρχει ένα παράδειγμα πρότυπου εντύπου αλυσίδας κηδεμονίας (ένα επεξεργάσιμο έντυπο αλυσίδας κηδεμονίας είναι διαθέσιμο από το NIST στο: <https://www.nist.gov/document/sample-chain-custody-formdocx>).

Η πρώτη από αυτές τις ενότητες είναι μια λεπτομερής περιγραφή του αντικειμένου. Μπορεί να φαίνεται περιττό να περιλαμβάνονται πολλά διαφορετικά στοιχεία, αλλά η ψηφιακή εγκληματολογία βασίζεται στις λεπτομέρειες. Η καταγραφή των πληροφοριών αφαιρεί κάθε αμφιβολία σχετικά με την αυθεντικότητα του αντικειμένου. Αυτή η περιγραφή θα πρέπει να περιέχει τα ακόλουθα στοιχεία:

- **Αριθμός Αντικειμένου (Item Number):** Ένας μοναδικός αριθμός αντικειμένου πρέπει να συμπεριληφθεί στο έντυπο. Εάν υπάρχουν πολλαπλά αποδεικτικά στοιχεία, θα συμπληρωθεί ξεχωριστό έντυπο αλυσίδας κηδεμονίας για το καθένα.
- **Περιγραφή (Description):** Πρόκειται για μια γενική περιγραφή του αντικειμένου. Μπορεί να είναι μια απλή δήλωση, όπως «500 GB SATA HDD».
- **Κατασκευαστής (Manufacturer):** Αυτή η λεπτομέρεια βοηθά στην περίπτωση πολλαπλών αποδεικτικών στοιχείων που μπορεί να έχουν διαφορετικούς κατασκευαστές.
- **Μοντέλο (Model):** Δεδομένου ότι υπάρχει μεγάλη ποικιλία αριθμών μοντέλου για τα εξαρτήματα, η καταγραφή τους παρέχει περαιτέρω λεπτομέρειες για το αντικείμενο.

- **Σειριακός Αριθμός (Serial Number):** Αυτό είναι κρίσιμο σε περίπτωση που ένα περιστατικό αφορά πολλά συστήματα με ακριβώς την ίδια διαμόρφωση. Φανταστείτε την προσπάθεια να ανακατασκευαστεί ποια αλυσίδα κηδεμονίας αντιστοιχεί σε ποιο HDD, αν π.χ. κατασχέθηκαν έξι μαζί και είχαν τον ίδιο κατασκευαστή και αριθμό μοντέλου.

Ένα ολοκληρωμένο παράδειγμα της πρώτης ενότητας του έντυπου αλυσίδας κηδεμονίας θα μπορούσε να έχει την εξής μορφή:

Electronic Media Details		
Item Number: 1	Description: Western Digital WD01EURS Hard Drive	
Manufacturer: Western Digital	Model# WD01EURS	Serial Number: WMAV1234567

Μια εναλλακτική ενότητα μπορεί να χρησιμοποιηθεί σε περιπτώσεις όπου τα αποδεικτικά στοιχεία είναι αρχεία καταγραφής (log files) ή εικόνες που έχουν ληφθεί κατά τη διάρκεια της έρευνας. Αυτή περιλαμβάνει τα ακόλουθα στοιχεία:

- **Ημερομηνία/Ωρα Απόκτησης (Date/Time Acquired):** Είναι σημαντικό να καθορίζεται με ακρίβεια η ημερομηνία και η ώρα κατά την οποία αποκτήθηκαν τα συγκεκριμένα αρχεία.
- **Περιγραφή (Description):** Μια σύντομη περιγραφή του μέσου που αποκτήθηκε είναι χρήσιμη.
- **Μέθοδος (Method):** Αν χρησιμοποιήθηκε κάποιο λογισμικό ή εργαλείο ψηφιακής εγκληματολογίας για την απόκτηση των στοιχείων, πρέπει να αναφερθεί. Σε άλλες περιπτώσεις, όπως με αρχεία καταγραφής, μπορεί απλώς να έγινε αντιγραφή σε εξωτερικό σκληρό δίσκο.
- **Μονάδα Αποθήκευσης (Storage Drive):** Σε μια επόμενη ενότητα θα συζητηθεί η σημασία της διαθεσιμότητας εξωτερικών μέσων για την αποθήκευση αρχείων. Η ακριβής μονάδα που χρησιμοποιήθηκε πρέπει να καταγράφεται στο έντυπο αλυσίδας κηδεμονίας.
- **Όνομα Αρχείου/Εικόνας (File/Image Name):** Εδώ καταχωρείται το μοναδικό όνομα του αρχείου ή της εικόνας.
- **Αλυσίδα Ελέγχου (Hash):** Για κάθε ξεχωριστό αρχείο που αποκτάται, πρέπει να υπολογίζεται μια μοναδική τιμή hash.

Ένα ολοκληρωμένο παράδειγμα της ενότητας «Λεπτομέρειες Αρχείου ή Εικόνας» στο έντυπο αλυσίδας κηδεμονίας θα μπορούσε να έχει την εξής μορφή:

Image or File Details			
Date / Time Acquired: 5/30/19 1224 UTC	Created By: Gerard Johansen	Method: Wireshark	Storage Drive: USB Drive 1
File/Image Name: EdgeFirewallCapture.PCAP / Packet Capture		Hash: 1ceaa2393357d2ed88f81bec1e647af0	

Η επόμενη ενότητα περιγράφει τα συγκεκριμένα βήματα που ακολούθησε το αποδεικτικό στοιχείο κατά τη διάρκεια του κύκλου ζωής του. Για κάθε στάδιο πρέπει να καταγράφονται τα ακόλουθα στοιχεία:

- **Αριθμός Παρακολούθησης (Tracking No):** Αυτός ο αριθμός υποδεικνύει το βήμα στον κύκλο ζωής που ακολούθησε το αποδεικτικό στοιχείο.
- **Ημερομηνία/Ωρα (Date/Time):** Πρόκειται για κρίσιμη πληροφορία σε κάθε αλυσίδα κηδεμονίας και εφαρμόζεται σε κάθε βήμα που πραγματοποιείται. Αυτό επιτρέπει σε οποιονδήποτε δει την αλυσίδα κηδεμονίας να ανακατασκευάσει, λεπτό προς λεπτό, κάθε στάδιο του κύκλου ζωής του αποδεικτικού στοιχείου.
- **ΑΠΟ και ΠΡΟΣ (FROM and TO):** Αυτά τα πεδία μπορεί να αναφέρονται είτε σε άτομο είτε σε χώρο αποθήκευσης. Για παράδειγμα, αν ένας αναλυτής κατάσχει έναν σκληρό δίσκο και τον μεταφέρει σε ασφαλή θήκη αποθήκευσης, η «προς» τοποθεσία θα καταγραφεί ως ο ασφαλής χώρος. Είναι κρίσιμο τα άτομα που εμφανίζονται στην αλυσίδα κηδεμονίας να υπογράφουν το έντυπο (όταν απαιτείται), για να διασφαλιστεί η υπευθυνότητα.
- **Λόγος (Reason):** Η μεταφορά ενός αποδεικτικού στοιχείου δεν πρέπει να γίνεται χωρίς αιτιολόγηση. Σε αυτό το τμήμα της αλυσίδας κηδεμονίας περιγράφεται ο λόγος για τη μετακίνηση.

Η ακόλουθη εικόνα δείχνει ένα παράδειγμα καταγραφής της μετακίνησης του σκληρού δίσκου από το προηγούμενο παράδειγμα.

Chain of Custody				
Tracking No:	Date/Time:	FROM:	TO:	Reason:
1	Date: 5/30/19	Name/Org: Carol Davies Global Services Corp.	Name/Org: Gerard Johansen IRProactive	Evidence Acquisition
	Time: 1224 UTC	Signature: <i>Carol Davies</i>	Signature: <i>Gerard T Johansen</i>	
2	Date: 5/30/19	Name/Org: G Johansen IRProactive	Name/Org: David Michell ACME Forensics	Analysis
	Time: 1305 UTC	Signature: <i>Gerard T Johansen</i>	Signature: <i>David Michell</i>	

Κάθε μετακίνηση για κάθε αποδεικτικό στοιχείο καταγράφεται εδώ. Η πρώτη μετακίνηση είναι η κατάσχεση του δίσκου από το σύστημα. Σε αυτή την περίπτωση, δεν υπάρχει συγκεκριμένος φύλακας,

καθώς ο δίσκος έχει ληφθεί από το data center. Το κρίσιμο σημείο είναι ότι ο συγγραφέας είναι ο υπεύθυνος για τον δίσκο μέχρι να τον μεταβιβάσει στον David Michell της ACME Forensics για ανάλυση. Οι λεπτομέρειες είναι οι εξής:

Η αλυσίδα κηδεμονίας διατηρείται καθ' όλη τη διάρκεια ζωής του αποδεικτικού στοιχείου. Ακόμη και όταν το αποδεικτικό στοιχείο καταστραφεί ή επιστραφεί, γίνεται μία εγγραφή στο έντυπο αλυσίδας κηδεμονίας. Αυτά τα έντυπα πρέπει να φυλάσσονται μαζί με οποιοδήποτε άλλο υλικό έχει παραχθεί κατά το περιστατικό και να ενσωματώνονται σε οποιαδήποτε επόμενη αναφορά δημιουργηθεί.

4.6. Εξέταση (Examination)

Η φάση της εξέτασης περιγράφει τα συγκεκριμένα εργαλεία και τις εγκληματολογικές τεχνικές που χρησιμοποιούνται για την ανακάλυψη και εξαγωγή δεδομένων από τα αποδεικτικά στοιχεία που κατασχέθηκαν κατά τη διάρκεια ενός περιστατικού. Για παράδειγμα, σε μια υπόθεση όπου υπάρχει υποψία ότι κακόβουλο λογισμικό έχει μολύνει ένα desktop σύστημα ως μέρος μιας μεγαλύτερης επίθεσης, η εξαγωγή συγκεκριμένων πληροφοριών από μια εικόνα μνήμης που έχει αποκτηθεί πραγματοποιείται σε αυτό το στάδιο. Σε άλλες περιπτώσεις, οι αναλυτές ψηφιακής εγκληματολογίας μπορεί να χρειαστεί να εξάγουν κίνηση Secure Shell (SSH) από μια καταγραφή δικτύου.

Η εξέταση των ψηφιακών αποδεικτικών στοιχείων συνεχίζει επίσης τη διαδικασία σωστής διατήρησης, καθώς οι αναλυτές χειρίζονται με τη μέγιστη προσοχή τα στοιχεία κατά τη διάρκεια της εξέτασης. Εάν ο αναλυτής ψηφιακής εγκληματολογίας δεν λάβει τα κατάλληλα μέτρα διατήρησης σε αυτό το στάδιο, υπάρχει η πιθανότητα μόλυνσης, η οποία θα μπορούσε να καταστήσει το αποδεικτικό στοιχείο αναξιόπιστο ή μη χρησιμοποιήσιμο.

4.7. Ανάλυση (Analysis)

Μόλις η φάση της εξέτασης εξάγει πιθανά σχετικά δεδομένα, ο αναλυτής ψηφιακής εγκληματολογίας αναλύει τα δεδομένα αυτά σε συνδυασμό με οποιαδήποτε άλλα σχετικά δεδομένα έχουν συλλεχθεί. Για παράδειγμα, αν ο αναλυτής ανακαλύψει ότι ένας παραβιασμένος υπολογιστής έχει ανοιχτή σύνδεση με μια εξωτερική διεύθυνση IP, θα συσχετίσει αυτή την πληροφορία με την ανάλυση μιας καταγραφής πακέτων από το δίκτυο. Χρησιμοποιώντας τη διεύθυνση IP ως σημείο εκκίνησης, ο αναλυτής μπορεί να απομονώσει την αντίστοιχη κίνηση. Στη συνέχεια, μπορεί να προσδιορίσει ότι ο παραβιασμένος υπολογιστής στέλνει ένα beacon προς έναν C2 server. Με τη χρήση επιπλέον πηγών, ο αναλυτής μπορεί να καθορίσει ποιος συγκεκριμένος τρόπος επίθεσης συνδέεται με αυτή τη διεύθυνση IP.

4.8. Παρουσίαση (Presentation)

Η αναφορά γεγονότων που σχετίζονται με την ψηφιακή εγκληματολογία πρέπει να είναι σαφής, περιεκτική και χωρίς προκατάληψη. Σχεδόν πάντα, ο αναλυτής πρέπει να ετοιμάσει μια λεπτομερή γραπτή αναφορά που περιγράφει κάθε ενέργεια και καταγράφει τα κρίσιμα δεδομένα. Η αναφορά αυτή πρέπει να είναι πλήρης, ακριβής και χωρίς προσωπικές απόψεις ή προκαταλήψεις. Συχνά αποτελεί μέρος μιας ευρύτερης έρευνας περιστατικού και βοηθά στον καθορισμό της βασικής αιτίας του περιστατικού.

Ένας ακόμη ρόλος παρουσίασης είναι η συμμετοχή του αναλυτή σε ποινικές ή αστικές διαδικασίες. Μπορεί να απαιτηθεί κατάθεση σε δικαστήριο αν το περιστατικό έχει οδηγήσει σε ύποπτο ή άλλο υπεύθυνο άτομο. Κατά τη διάρκεια της κατάθεσης, ο αναλυτής πρέπει να παρουσιάσει τα γεγονότα της εξέτασης με αντικειμενικότητα, όπως ακριβώς στην αναφορά. Οι αναλυτές παρουσιάζουν γεγονότα και συμπεράσματα χωρίς προκατάληψη και μπορεί να περιορίζονται στις γνώμες που μπορούν να εκφέρουν, ανάλογα με την εκπαίδευση και την εμπειρία τους. Ορισμένοι μπορεί να περιορίζονται στην παρουσίαση των γεγονότων, ενώ άλλοι, ως έμπειροι μάρτυρες-ειδικοί, μπορούν να παρέχουν και γνώμη.

4.9. Εργαστήριο ψηφιακής εγκληματολογίας (Digital Forensics Lab)

Η ψηφιακή εγκληματολογία είναι μια αυστηρή διαδικασία που απαιτεί σωστά εργαλεία, τεχνικές και γνώση για την εξαγωγή αποδεικτικών στοιχείων από συστήματα. Είναι σημαντικό οι αναλυτές να διαθέτουν χώρο ξεχωριστό από τις κανονικές επιχειρησιακές δραστηριότητες. Ο καλύτερος τρόπος για αυτό είναι να παρέχεται στα μέλη της ομάδας CSIRT, που συμμετέχουν άμεσα στην εξέταση ψηφιακών αποδεικτικών, ένας χώρος πλήρως ανεξάρτητος από την υπόλοιπη οργάνωση.

Ένα εργαστήριο ψηφιακής εγκληματολογίας πρέπει να έχει βασικά χαρακτηριστικά για να εξασφαλίζεται η ιδιωτικότητα των αναλυτών και η ακεραιότητα των αποδεικτικών κατά την εξέταση.

4.10. Φυσική ασφάλεια (Physical Security)

Η πρόσβαση στο εργαστήριο πρέπει να ελέγχεται αυστηρά. Για τη διατήρηση της αλυσίδας κηδεμονίας, μόνο άτομα με νόμιμη ανάγκη πρέπει να έχουν πρόσβαση. Ο χώρος πρέπει να κλειδώνεται συνεχώς και η πρόσβαση να γίνεται ιδανικά μέσω καρτών ή fobs, με κεντρικό σύστημα διαχείρισης, ώστε να μπορεί να ανακατασκευαστεί πλήρως ποιοι είχαν πρόσβαση σε συγκεκριμένο χρόνο. Το εργαστήριο πρέπει επίσης να διαθέτει ντουλάπες αποθήκευσης αποδεικτικών στοιχείων για σωστή φύλαξη όταν δεν εξετάζονται. Οι ντουλάπες πρέπει να είναι κλειδωμένες (με κλειδί ή συνδυασμό), και η πρόσβαση να δίνεται μόνο στους αναλυτές. Αν οι πόροι της οργάνωσης το επιτρέπουν, κάθε περιστατικό πρέπει να έχει τη δική του ντουλάπα για να αποφεύγεται η ανάμιξη ψηφιακών στοιχείων.

4.11. Εργαλεία (Tools)

Ανάλογα με τις συγκεκριμένες εξετάσεις που πρέπει να πραγματοποιηθούν, μπορεί να χρειαστεί η αφαίρεση βιδών ή το κόψιμο καλωδίων. Η ύπαρξη ενός μικρού σετ χειροκίνητων εργαλείων θα είναι βολική για τους εξεταστές. Το εργαστήριο θα πρέπει επίσης να διαθέτει κουτιά για την ασφαλή φύλαξη των αποδεικτικών στοιχείων. Εάν οι εξεταστές χρειάζεται να επεξεργαστούν smartphones ή tablets, θα πρέπει να υπάρχουν διαθέσιμες σακούλες Faraday. Αυτές οι σακούλες επιτρέπουν στους εξεταστές να απομονώσουν ένα smartphone ή tablet από το κινητό δίκτυο, ενώ ταυτόχρονα διατηρείται η τροφοδοσία ρεύματος.

4.12. Υλικό (Hardware)

Το εργαστήριο θα πρέπει να διαθέτει επαρκείς υπολογιστές και άλλο υλικό για την εκτέλεση μιας ποικιλίας απαραίτητων λειτουργιών. Οι εξεταστές θα κληθούν να δημιουργούν εικόνες (imaging) σκληρών δίσκων και να επεξεργάζονται gigabytes δεδομένων. Ως αποτέλεσμα, είναι απαραίτητος ένας δικτυακός υπολογιστής (forensic computer) με επαρκή μνήμη RAM. Αν και υπάρχουν προσωπικές προτιμήσεις ως προς τη μνήμη, συνιστάται τουλάχιστον 32 GB RAM. Επιπλέον της μνήμης και της επεξεργαστικής ισχύος, οι εξεταστές συχνά θα εξετάζουν μεγάλο όγκο δεδομένων. Οι forensic workstations θα πρέπει να διαθέτουν έναν κύριο δίσκο για το λειτουργικό σύστημα και το λογισμικό εγκληματολογίας και έναν δευτερεύοντα δίσκο για την αποθήκευση αποδεικτικών στοιχείων, με χωρητικότητα τουλάχιστον 2 TB.

Εκτός από τη forensic workstation, ο εξεταστής θα πρέπει να διαθέτει έναν υπολογιστή συνδεδεμένο στο διαδίκτυο. Η forensic workstation δεν θα πρέπει να έχει σύνδεση στο διαδίκτυο, για λόγους ασφαλείας και για την αποφυγή πιθανής αλλοίωσης των αποδεικτικών στοιχείων κατά τη διάρκεια της εξέτασης. Ο δευτερεύων υπολογιστής θα χρησιμοποιείται για έρευνα ή για τη σύνταξη αναφορών.

Ένα ακόμη κρίσιμο εργαλείο είναι ο φυσικός write blocker. Αυτή η συσκευή επιτρέπει τη σύνδεση ενός σκληρού δίσκου που κατασχέθηκε ως αποδεικτικό με τη μηχανή δημιουργίας εικόνας (imaging). Η ουσιαστική διαφορά μεταξύ ενός φυσικού write blocker και μιας απλής σύνδεσης USB ή Thunderbolt είναι ότι ο εξεταστής ψηφιακής εγκληματολογίας μπορεί να είναι σίγουρος ότι δεν γράφονται δεδομένα στον δίσκο αποδεικτικών στοιχείων.

Για εργαστήρια ψηφιακής εγκληματολογίας που πραγματοποιούν μεγάλο αριθμό εργασιών imaging, υπάρχει η επιλογή εγκατάστασης μιας αποκλειστικής σταθμού για forensic imaging, που επιτρέπει ταχύτερη δημιουργία εικόνων αποδεικτικών δίσκων χωρίς να δεσμεύεται η forensic workstation. Το μειονέκτημά του είναι το κόστος.

Το CSIRT θα πρέπει επίσης να επενδύσει σε μεγάλο αριθμό εξωτερικών USB δίσκων υψηλής χωρητικότητας, οι οποίοι είναι πιο εύκολοι στη χρήση για τη διαδικασία imaging από τους παραδοσιακούς δίσκους SATA ή IDE. Αυτοί οι δίσκοι χρησιμοποιούνται για την αποθήκευση εικόνων δίσκων για περαιτέρω ανάλυση. Καλό είναι να υπάρχουν τουλάχιστον έξι τέτοιοι δίσκοι υψηλής

χωρητικότητας, με χωρητικότητα 2–3 TB, για την αποθήκευση πολλαπλών εικόνων ταυτόχρονα. Μικρότεροι USB δίσκοι είναι επίσης χρήσιμοι για τη συλλογή αρχείων καταγραφής (log files) και εικόνων μνήμης για μετέπειτα επεξεργασία. Οι USB 3.0 εκδόσεις προσφέρουν ταχύτερη επεξεργασία.

Τέλος, οι εξεταστές ψηφιακής εγκληματολογίας που υποστηρίζουν ένα CSIRT θα πρέπει να διαθέτουν ανθεκτική θήκη για τη μεταφορά του εξοπλισμού, σε περίπτωση που χρειαστεί να πραγματοποιήσουν εξέταση εκτός εργαστηρίου. Πολλά από τα εργαλεία αυτά είναι εύθραυστα. Συνιστώνται τουλάχιστον δύο σκληρές θήκες, μία για εξωτερικούς σκληρούς δίσκους και μία για φορητό υπολογιστή forensic, για την προστασία από πιθανή ζημιά κατά τη μεταφορά.

3.13. Λογισμικό (Software)

Υπάρχουν πολλά εργαλεία λογισμικού στην αγορά, εμπορικά ή δωρεάν. Το εργαστήριο ψηφιακής εγκληματολογίας θα πρέπει να έχει πρόσβαση σε αρκετά εργαλεία για να εκτελεί παρόμοιες λειτουργίες. Τουλάχιστον, θα πρέπει να υπάρχει λογισμικό για:

- Δημιουργία εικόνων αποδεικτικών δίσκων (imaging)
- Ανάλυση εικόνων
- Ανάλυση μνήμης (memory captures)
- Σύνταξη αναφορών

Κύριες εφαρμογές ψηφιακής εγκληματολογίας:

- **Autopsy:** Λογισμικό ανοιχτού κώδικα από τον Brian Carrier, με πολλά αυτοματοποιημένα εργαλεία ψηφιακής εγκληματολογίας.
- **EnCase:** Εμπορικό λογισμικό της OpenText για πλήρη ανάλυση ψηφιακών αποδεικτικών, με δυνατότητες αναφορών. Το κόστος μπορεί να είναι σημαντικό.
- **Forensic Toolkit (FTK):** Πλήρης εφαρμογή, εναλλακτική του EnCase, ευρέως χρησιμοποιούμενη.
- **X-Ways Forensics:** Λογισμικό με παρόμοιες δυνατότητες, χαμηλότερου κόστους, χωρίς ανάγκη για δίκτυο ή απομακρυσμένη πρόσβαση.

Εργαλεία Linux: Υπάρχουν διανομές Linux για ψηφιακή εγκληματολογία, συχνά δωρεάν, που διευκολύνουν την εξέταση αποδεικτικών στοιχείων.

- **DEFT Zero:** Βασίζεται στο GNU Linux, boot από USB ή CD/DVD, για ασφαλή απόκτηση δεδομένων χωρίς αλλοίωση.
- **Paladin:** Βασισμένο στο Ubuntu, με εργαλεία για ανάλυση malware, hashing και imaging.

- **SIFT (SANS Investigate Forensic Toolkit):** Βασισμένο στο Ubuntu 16.04, για imaging, ανάλυση μνήμης, δημιουργία timeline και άλλα. Διατίθεται δωρεάν ως VM ή εγκατάσταση σε Ubuntu.
- **CAINE (Computer Aided INvestigative Environment):** Ακόμη μια διανομή για forensic χρήσεις.

3.14. Επισκόπηση των δικτυακών αποδεικτικών στοιχείων

Υπάρχουν πηγές καταγραφής δικτύου που μπορούν να παρέχουν στο προσωπικό CSIRT και στους αναλυτές περιστατικών καλές πληροφορίες. Κάθε συσκευή δικτύου παρέχει διαφορετικά αποδεικτικά στοιχεία ανάλογα με τον κατασκευαστή και το μοντέλο της. Ως μέρος της προετοιμασίας, το προσωπικό CSIRT θα πρέπει να εξοικειωθεί με τον τρόπο πρόσβασης σε αυτές τις συσκευές για τη συλλογή των απαραίτητων στοιχείων ή να έχει ήδη καθιερωμένες διαδικασίες επικοινωνίας με το προσωπικό IT για την υποστήριξη των κατάλληλων τεχνικών ανταπόκρισης κατά τη διάρκεια ενός περιστατικού.

Συσκευές δικτύου όπως switches, routers και firewalls διαθέτουν επίσης εσωτερικά logs που διατηρούν δεδομένα για το ποιος προσέβαλε τη συσκευή και έκανε αλλαγές. Οι αναλυτές περιστατικών θα πρέπει να γνωρίζουν τους τύπους των συσκευών δικτύου στο δίκτυο του οργανισμού τους και να μπορούν να έχουν πρόσβαση σε αυτά τα logs σε περίπτωση περιστατικού:

- **Switches:** Κατανέμονται σε όλο το δίκτυο μέσω ενός συνδυασμού core switches, που διαχειρίζονται την κυκλοφορία από διάφορα τμήματα δικτύου, και edge switches, που χειρίζονται την κυκλοφορία μεμονωμένων τμημάτων. Κατά συνέπεια, η κυκλοφορία που ξεκινά από έναν υπολογιστή και εξέρχεται από το εσωτερικό δίκτυο θα διασχίσει αρκετά switches. Τα switches παρέχουν δύο σημαντικά αποδεικτικά στοιχεία για τους αναλυτές περιστατικών:
 - **Πίνακας CAM (Content Addressable Memory):** Χαρτογραφεί τις φυσικές θύρες του switch με την κάρτα δικτύου (NIC) κάθε συνδεδεμένης συσκευής. Αυτό βοηθά στον εντοπισμό πιθανών μη εξουσιοδοτημένων συσκευών όπως ασύρματα access points ή συστήματα που συνδέονται από έναν επιτιθέμενο.
 - **Καταγραφή κυκλοφορίας δικτύου:** Επιτρέπει τη συλλογή δεδομένων κυκλοφορίας για διερεύνηση περιστατικών.
- **Routers:** Επιτρέπουν τη σύνδεση πολλαπλών LAN σε ένα MAN ή WAN και διαχειρίζονται μεγάλη ποσότητα κυκλοφορίας. Τα σημαντικά αποδεικτικά στοιχεία περιλαμβάνουν:
 - **Πίνακα δρομολόγησης (routing table)** για φυσικές θύρες που αντιστοιχούν σε δίκτυα.
 - Δυνατότητα άρνησης συγκεκριμένης κυκλοφορίας και καταγραφή των επιτρεπόμενων ροών δεδομένων.
 - **Δεδομένα NetFlow:** Παρέχουν πληροφορίες για διευθύνσεις IP, θύρες και πρωτόκολλα της κυκλοφορίας, βοηθώντας στον εντοπισμό της ροής δεδομένων ανά τμήμα δικτύου.
- **Firewalls:** Οι σύγχρονοι firewalls περιλαμβάνουν λειτουργίες όπως ανίχνευση και πρόληψη εισβολών, φιλτράρισμα web, πρόληψη απώλειας δεδομένων και λεπτομερή logs για την

επιτρεπόμενη και αποκλεισμένη κυκλοφορία. Συχνά λειτουργούν ως μηχανισμός ανίχνευσης, ειδοποιώντας το προσωπικό ασφαλείας για πιθανά περιστατικά.

- **Συστήματα ανίχνευσης και πρόληψης εισβολών (IDS/IPS):** Παρέχουν πληροφορίες για πιθανή κακόβουλη δραστηριότητα, χρησιμοποιώντας παρακολούθηση δικτύου και σύνολα κανόνων. Το IDS ειδοποιεί για συγκεκριμένη κακόβουλη δραστηριότητα, ενώ το IPS μπορεί να την ανιχνεύσει και να την μπλοκάρει.
- **Web proxy servers:** Χρησιμοποιούνται για τον έλεγχο της πρόσβασης σε ιστότοπους και παρέχουν συνολική εικόνα της κυκλοφορίας web σε όλο τον οργανισμό. Μπορούν επίσης να ειδοποιούν για συνδέσεις με γνωστούς C2 servers ή κακόβουλους ιστότοπους.
- **Domain controllers / Authentication servers:** Παρέχουν πληροφορίες για επιτυχημένες ή ανεπιτυχείς συνδέσεις, παραβίαση διαπιστευτηρίων ή άλλες χρήσεις διαπιστευτηρίων.
- **DHCP servers:** Καταγράφουν την εκχώρηση δυναμικών IP σε υπολογιστές και μπορούν να βοηθήσουν στον εντοπισμό συγκεκριμένων συσκευών σε συγκεκριμένο χρόνο.
- **Application servers:** Διατηρούν logs ανάλογα με την εφαρμογή και μπορούν να παρέχουν πληροφορίες για απομακρυσμένες συνδέσεις, κάτι χρήσιμο όταν ένας επιτιθέμενος προσπαθεί να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα.

3.15. Προετοιμασία

Η ικανότητα απόκτησης στοιχείων δικτύου εξαρτάται σε μεγάλο βαθμό από την προετοιμασία που πραγματοποιείται από έναν οργανισμό πριν από ένα περιστατικό. Χωρίς βασικά στοιχεία ενός σωστού προγράμματος ασφάλειας υποδομών, κρίσιμα στοιχεία δεν θα είναι διαθέσιμα στους ανακριτές περιστατικών (CSIRT) εγκαίρως. Το αποτέλεσμα είναι ότι στοιχεία μπορεί να χαθούν, ενώ τα μέλη της ομάδας CSIRT αναζητούν κρίσιμες πληροφορίες.

Όσον αφορά την προετοιμασία, οι οργανισμοί μπορούν να βοηθήσουν την ομάδα CSIRT διασφαλίζοντας:

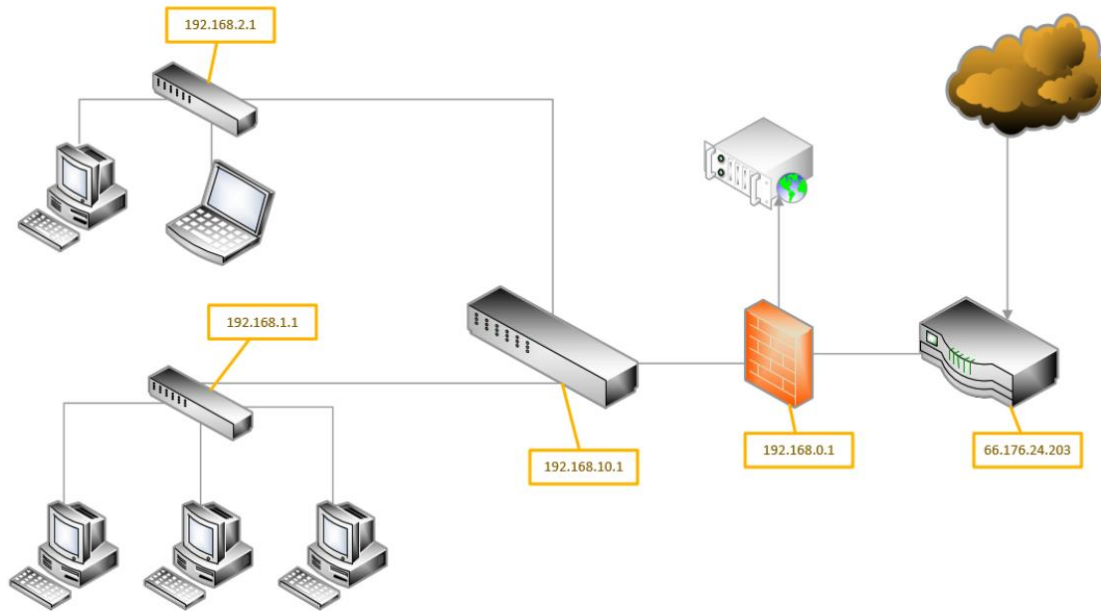
- Τεκμηρίωση του δικτύου (network documentation).
- Ενημερωμένες ρυθμίσεις των συσκευών δικτύου.
- Κεντρική λύση διαχείρισης αρχείων καταγραφής (central log management solution).

Πέρα από την τεχνική προετοιμασία για συλλογή στοιχείων δικτύου, τα μέλη του CSIRT πρέπει να είναι ενήμερα για νομικά ή κανονιστικά ζητήματα σχετικά με τη συλλογή στοιχείων δικτύου. Επιπλέον, πρέπει να γνωρίζουν ότι η καταγραφή της κυκλοφορίας δικτύου μπορεί να θεωρηθεί παραβίαση της ιδιωτικότητας, εάν δεν υπάρχει πολιτική που να δηλώνει σαφώς ότι πραγματοποιείται παρακολούθηση του δικτύου. Συνεπώς, ο νομικός εκπρόσωπος της ομάδας CSIRT πρέπει να διασφαλίσει ότι όλοι οι υπάλληλοι του οργανισμού κατανοούν ότι η χρήση του πληροφοριακού

συστήματος θα παρακολουθείται. Αυτό πρέπει να δηλώνεται ρητά σε πολιτικές πριν από οποιαδήποτε συλλογή στοιχείων.

3.16. Διάγραμμα δικτύου

Για να εντοπίσουν πιθανούς πόρους στοιχείων, οι ανακριτές περιστατικών πρέπει να έχουν σαφή κατανόηση της εσωτερικής δομής του δικτύου.



Μία μέθοδος που μπορούν να χρησιμοποιήσουν οι οργανισμοί είναι η δημιουργία και διατήρηση ενός ενημερωμένου διαγράμματος δικτύου (network diagram). Το διάγραμμα αυτό πρέπει να είναι αρκετά λεπτομερές ώστε οι ανακριτές να μπορούν να αναγνωρίζουν τα επιμέρους στοιχεία του δικτύου, όπως:

- Switches
- Routers
- Wireless access points

Επιπλέον, το διάγραμμα πρέπει να περιλαμβάνει τις εσωτερικές διευθύνσεις IP, ώστε οι ανακριτές να έχουν άμεση πρόσβαση σε αυτά τα συστήματα μέσω απομακρυσμένων μεθόδων.

Αυτό το διάγραμμα επιτρέπει την γρήγορη αναγνώριση πιθανών πηγών αποδεικτικών στοιχείων. Για παράδειγμα, υποθέστε ότι ο φορητός υπολογιστής που είναι συνδεδεμένος στο switch στη διεύθυνση 192.168.2.1 ταυτοποιείται ότι επικοινωνεί με έναν γνωστό C2 server κακόβουλου λογισμικού. Ένας αναλυτής CSIRT θα μπορούσε να εξετάσει το διάγραμμα δικτύου και να διαπιστώσει ότι η κυκλοφορία C2 θα πρέπει να διασχίσει αρκετά δίκτυα υλικό κατά τη διαδρομή προς τα έξω από το εσωτερικό δίκτυο. Για παράδειγμα, η κυκλοφορία θα περάσει από το switch στη διεύθυνση 192.168.10.1, μέσα από το firewall στη διεύθυνση 192.168.0.1 και, τελικά, από τον δρομολογητή προς το διαδίκτυο.

Διαμόρφωση: Ο καθορισμός εάν ένας επιτιθέμενος έχει κάνει τροποποιήσεις σε μια συσκευή δικτύου, όπως ένα switch ή έναν δρομολογητή, μπορεί να γίνει ευκολότερος εάν η ομάδα CSIRT έχει διαθέσιμη μια τυπική διαμόρφωση. Οι οργανισμοί θα πρέπει ήδη να διαθέτουν αποθηκευμένες διαμορφώσεις για συσκευές δικτύου για σκοπούς ανάκτησης από καταστροφή, αλλά θα πρέπει να είναι διαθέσιμες και στα μέλη της CSIRT σε περίπτωση περιστατικού.

3.17. Συλλογή Δικτυακών Αποδεικτικών Στοιχείων

Firewalls και logs proxy: Δύο κύριες πηγές αποδεικτικών στοιχείων κατά την διερεύνηση ενός περιστατικού είναι τα σημεία εισόδου/εξόδου του δικτύου από το διαδίκτυο. Το σύγχρονο κακόβουλο λογισμικό και άλλες εκμεταλλεύσεις συχνά απαιτούν πρόσβαση σε πόρους του διαδικτύου. Αυτό μπορεί να είναι για τη λήψη επιπλέον κακόβουλου λογισμικού ή για εκμετάλλευση κώδικα. Άλλες επιθέσεις που περιλαμβάνουν εξαγωγή δεδομένων απαιτούν πρόσβαση στο διαδίκτυο. Τέλος, οι επιτιθέμενοι συχνά πρέπει να εγκαθιδρύσουν C2 (Command and Control) μέσω των μολυσμένων συστημάτων. Σε όλες αυτές τις περιπτώσεις, η κυκλοφορία από διάφορα πρωτόκολλα θα διασχίσει το περίγραμμα του δικτύου του θύματος. Ανάλογα με τον θύμα, αυτή η κυκλοφορία θα περάσει από firewall, internet proxy ή και τα δύο. Ως αποτέλεσμα, και οι δύο αυτές τεχνολογίες παρέχουν στο προσωπικό απόκρισης σε περιστατικά σημαντική πηγή αποδεικτικών στοιχείων.

Firewalls: Τα firewalls εξελίχθηκαν από μια απλή τεχνολογία δρομολόγησης και αποκλεισμού σε πλατφόρμες που παρέχουν σημαντική εικόνα της κυκλοφορίας που εισέρχεται και εξέρχεται από το δίκτυο. Τα firewalls επόμενης γενιάς συχνά συνδυάζουν κανόνες allow/deny με IDS ή IPS, καθώς και τον έλεγχο πρόσβασης σε εφαρμογές. Αυτό δημιουργεί μια σημαντική πηγή αποδεικτικών στοιχείων που μπορεί να αξιοποιηθεί κατά τη διάρκεια ενός περιστατικού.

Η απόκτηση αποδεικτικών στοιχείων από firewalls εξαρτάται κυρίως από τον κατασκευαστή και το συγκεκριμένο μοντέλο που χρησιμοποιείται. Οι αναλυτές περιστατικών θα πρέπει να κατανοούν πλήρως τα χαρακτηριστικά και τα δεδομένα που μπορούν να ληφθούν ως μέρος της προετοιμασίας τους. Αν και τα χαρακτηριστικά διαφέρουν ανάμεσα σε προμηθευτές και μοντέλα, υπάρχουν κάποια βασικά στοιχεία αποδεικτικών που είναι σχεδόν καθολικά:

- **Αρχείο καταγραφής συνδέσεων (Connection log):** Παρέχει τις διευθύνσεις IP προέλευσης και προορισμού και τα πρωτόκολλα των συνδέσεων μεταξύ εσωτερικών και εξωτερικών συστημάτων. Αυτό είναι κρίσιμο για τον καθορισμό εάν κάποιο εσωτερικό σύστημα ενδέχεται να έχει επικοινωνήσει με ένα σύστημα υπό έλεγχο επιτιθέμενου ή ενδεχομένως να ελέγχεται. Εκτός από τις επιτρεπόμενες συνδέσεις, τα logs μπορεί να παρέχουν πληροφορίες και για τις συνδέσεις που απορρίφθηκαν. Μια τεχνική που χρησιμοποιείται συχνά από τους επιτιθέμενους είναι η χρήση εργαλείων για προσπάθεια σύνδεσης σε γνωστές θύρες που χρησιμοποιούνται συχνά. Αν αυτές οι θύρες είναι κλειστές σε εξωτερικές συνδέσεις, θα υπάρχει καταχώρηση απόρριψης στα logs. Διαδοχικές απορρίψεις σε μια σειρά θυρών υποδηλώνουν δραστηριότητα αναγνώρισης.

- **Αρχεία καταγραφής απομακρυσμένης πρόσβασης (Remote access logs):** Τα firewalls συχνά λειτουργούν ως VPN concentrator για απομακρυσμένη πρόσβαση. Εάν ένας απομακρυσμένος χρήστης μολυνθεί μέσω κακόβουλου λογισμικού, μπορεί να εισαγάγει τη μόλυνση στο εσωτερικό δίκτυο μέσω του VPN. Τα αρχεία καταγραφής απομακρυσμένης πρόσβασης θα δείξουν ποια συστήματα είναι συνδεδεμένα και πότε συνδέθηκαν, επιτρέποντας τη συσχέτιση δραστηριοτήτων και τον καθορισμό της πηγής μόλυνσης.

Ροές Δικτύου (Netflow): Οι ροές δικτύου (Netflow) αναφέρονται σε **μεταδεδομένα ροών κίνησης**. Δεν αποθηκεύεται το πλήρες περιεχόμενο των πακέτων, αλλά πληροφορίες όπως η πηγή, ο προορισμός, ο όγκος και η διαδρομή της κίνησης. Η ανάλυση Netflow βοηθά στη δημιουργία μιας εικόνας της συνολικής δραστηριότητας στο δίκτυο.

- **Χρήση:** Ανάλυση της κίνησης για αναγνώριση προέλευσης/προορισμού, όγκου και διαδρομών.
- **Εργαλεία:** Silk, Nfsen & Nfdump.

Σύλληψη Πακέτων (Packet Capture): Η σύλληψη πακέτων είναι η διαδικασία **παγίδευσης πακέτων δεδομένων** που περνούν από ένα συγκεκριμένο σημείο του δικτύου. Τα πακέτα καταγράφονται σε πραγματικό χρόνο, αποθηκεύονται προσωρινά και στη συνέχεια μπορούν να αναλυθούν ή να αρχειοθετηθούν.

- **Χρήση:** Ανάλυση περιεχομένου επικοινωνιών, troubleshooting, εντοπισμός επιθέσεων.
- **Εργαλεία:** Arkime (Moloch), Tcpdump, Wireshark, Tshark.

Σύστημα Ανίχνευσης Εισβολών Δικτύου (Network IDS – NIDS): Τα NIDS παρακολουθούν την κίνηση του δικτύου και εντοπίζουν κακόβουλη δραστηριότητα. Συνήθως απαιτούν **πρόσβαση σε λειτουργία “promiscuous mode”**, ώστε να μπορούν να βλέπουν όλη την κίνηση.

- **Χρήση:** Ανίχνευση επιθέσεων, malware επικοινωνιών, ανώμαλων μοτίβων.
- **Εργαλεία:** Snort, Suricata, Bro (Zeek), Εμπορικά NIDS προϊόντα.

Καταγραφές Proxy (Proxy Logs)

Ένας proxy server καταγράφει όλα τα **αιτήματα που γίνονται μέσω αυτού**. Αυτά τα logs περιλαμβάνουν όχι μόνο ιστοσελίδες που επισκέπτονται οι χρήστες, αλλά και αιτήματα εφαρμογών ή υπηρεσιών προς το διαδίκτυο (π.χ. ενημερώσεις εφαρμογών).

- **Χρήση:** Έλεγχος χρήσης διαδικτύου, ανίχνευση ύποπτων αιτημάτων εφαρμογών, έλεγχος πολιτικών πρόσβασης.
- **Εργαλεία:** Squid, Εμπορικά Proxy προϊόντα.

Καταγραφές DNS (DNS Logs): Το DNS (Domain Name System) χρησιμοποιείται συχνά σε επιθέσεις, είτε για **εξαγωγή δεδομένων (exfiltration)**, είτε για **επικοινωνία Command and Control (C2)**. Παρά την κρισιμότητά του, πολλές εταιρείες δεν ενεργοποιούν επαρκή καταγραφή DNS, χάνοντας έτσι σημαντικούς κανόνες ανίχνευσης.

- **Δεδομένα που συλλέγονται:**
 - Από DNS Servers.
 - Από το ίδιο το δίκτυο (network collected).
 - Από endpoints (π.χ. Sysmon 10).
 - Passive DNS Logs.
 - **Χρήση:** Ανίχνευση DNS tunneling, ανίχνευση ύποπτων domains, εντοπισμός blind spots.
-

Με λίγα λόγια:

- **Netflow** → Εικόνα της ροής κίνησης.
 - **Packet Capture** → Ανάλυση περιεχομένου πακέτων.
 - **NIDS** → Ανίχνευση εισβολών.
 - **Proxy Logs** → Έλεγχος αιτημάτων χρηστών/εφαρμογών.
 - **DNS Logs** → Ανίχνευση επιθέσεων βασισμένων σε DNS.
-

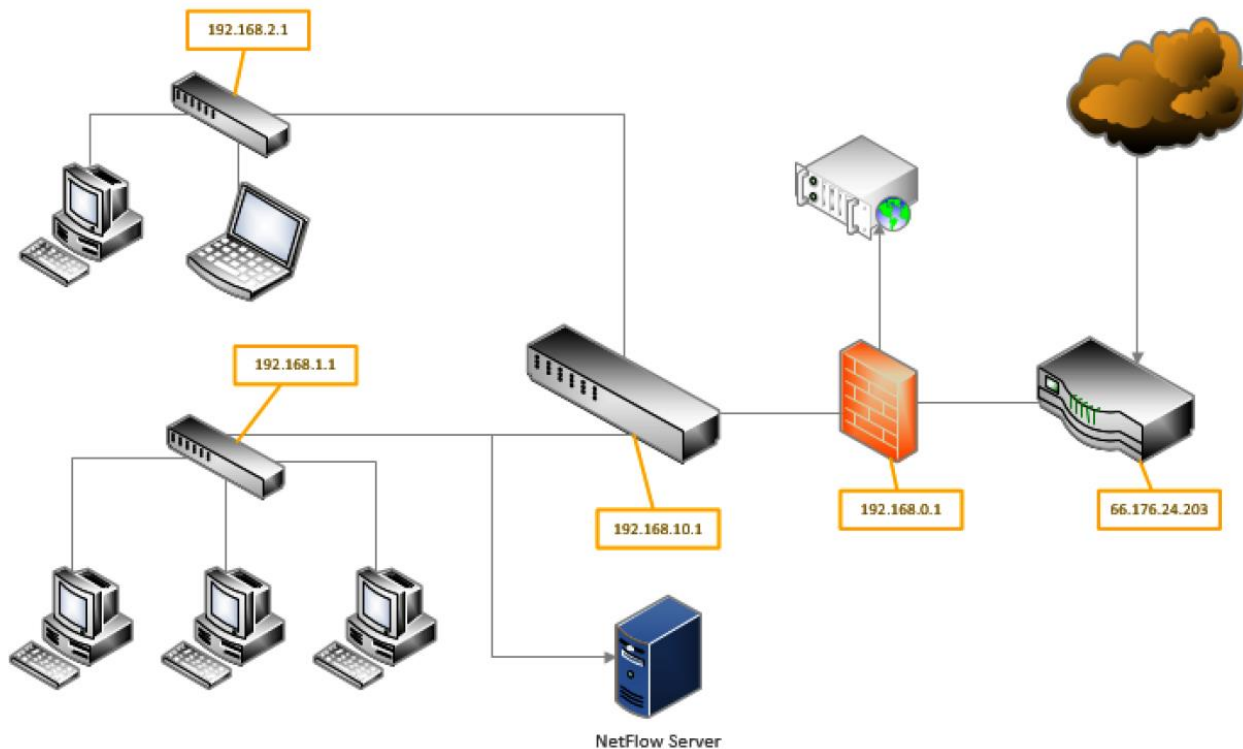
Web proxy server: Οι επιτιθέμενοι συχνά χρησιμοποιούν scripting, όπως Microsoft Visual Basic ή PowerShell, για να κατεβάσουν δευτερεύοντα πακέτα εκμετάλλευσης ή κακόβουλο λογισμικό. Αυτά τα scripts περιέχουν συνήθως μια URL που δείχνει στο exploit ή στο malware. Οι επιτιθέμενοι χρησιμοποιούν URL αντί για IP, καθώς οι διευθύνσεις IP μπορούν εύκολα να αλλάξουν μέσω της εγγραφής domain, επιτρέποντάς τους να αλλάξουν την υποδομή τους χωρίς να τροποποιήσουν τα scripts. Οργανισμοί που χρησιμοποιούν web proxy servers για αιτήματα HTTP και HTTPS θα έχουν αρχείο καταγραφής για οποιοδήποτε σύστημα στο εσωτερικό δίκτυο που προσέγγισε εξωτερικό site. Από αυτά τα δεδομένα μπορούν να εντοπίσουν τη θέση και πιθανώς το κακόβουλο λογισμικό ή το exploit που κατέβηκε. Επιπλέον, η κυκλοφορία C2 που χρησιμοποιεί παρόμοιες τεχνικές μπορεί να δώσει περαιτέρω πληροφορίες. Καθώς η ανίχνευση επιθέσεων συχνά διαρκεί μήνες, είναι κρίσιμο οι αναλυτές να μπορούν να εξετάσουν ιστορικά δεδομένα δραστηριοτήτων που εκτείνονται σε εβδομάδες ή μήνες. Ακόμη και μόνο οι ημερομηνίες, οι ώρες, τα συστήματα που αιτήθηκαν και οι URLs που επισκέφθηκαν μπορούν να παρέχουν σημαντικά αποδεικτικά στοιχεία που αλλιώς δεν θα ήταν διαθέσιμα.

NetFlow: Το NetFlow σχεδιάστηκε αρχικά από την Cisco Systems το 1996 και αποτελεί λειτουργία που υπάρχει σε συσκευές δικτύου όπως switches και routers, επιτρέποντας στους διαχειριστές δικτύου να παρακολουθούν την κυκλοφορία εντός του δικτύου. Το NetFlow δεν είναι αυστηρά εργαλείο ασφαλείας, αλλά παρέχει σημαντικά δεδομένα στους αναλυτές περιστατικών σε περίπτωση συμβάντος. Τα δεδομένα NetFlow αποστέλλονται μέσω του πρωτοκόλλου UDP σε ένα κεντρικό σημείο συλλογής, συχνά ονομάζεται NetFlow Collector

Σε ένα περιβάλλον ασφαλείας, το NetFlow παρέχει βαθιά εικόνα της εσωτερικής κυκλοφορίας μεταξύ συστημάτων (east-west traffic), σε αντίθεση με την κυκλοφορία μεταξύ εσωτερικών και εξωτερικών συστημάτων μέσω του perimeter firewall (north-south traffic). Για παράδειγμα, σε ένα δίκτυο όπου ένα σύστημα στην υποδίκτυο 10.10.2.0/24 έχει μολυνθεί, ο επιτιθέμενος μπορεί να προσπαθήσει να μετακινηθεί σε ένα file server στο 10.10.1.0/24, να αποκτήσει ευαίσθητα δεδομένα και να τα μεταφέρει πίσω στο μολυσμένο σύστημα για εξαγωγή. Τα switches προωθούν τα δεδομένα NetFlow στον συλλέκτη, τα οποία περιλαμβάνουν διευθύνσεις IP, πρωτόκολλα και μέγεθος δεδομένων, κρίσιμα για την παροχή λεπτομερειών στους αναλυτές περιστατικών που αλλιώς δεν θα αποκτούσαν.

Η διαμόρφωση του NetFlow εξαρτάται από τον τύπο και τον κατασκευαστή των στοιχείων του δικτύου. Επιπλέον, υπάρχει μια μεγάλη γκάμα συλλεκτών και εργαλείων ανάλυσης που μπορούν να χρησιμοποιηθούν ανάλογα με τον προϋπολογισμό και άλλους διαθέσιμους πόρους. Ένα από τα πλεονεκτήματα της ενσωμάτωσης της ανάλυσης NetFlow στις συνολικές λειτουργίες του δικτύου είναι ότι παρέχει δεδομένα όχι μόνο στην ομάδα ανταπόκρισης σε περιστατικά, αλλά είναι επίσης

ιδιαίτερα χρήσιμη για τις καθημερινές λειτουργίες του δικτύου, όσον αφορά την ανίχνευση καθυστερήσεων ή άλλων προβλημάτων επικοινωνίας. Αυτή η διπλή χρήση καθιστά την ενσωμάτωσή της στις συνολικές λειτουργίες του δικτύου πιο εύκολα δικαιολογήσιμη.



Καταγραφές Πακέτων (Packet Captures): Η καταγραφή της κυκλοφορίας του δικτύου είναι κρίσιμη για την πλήρη κατανόηση ενός περιστατικού. Η δυνατότητα αναγνώρισης πιθανής κυκλοφορίας προς διευθύνσεις IP C2 μπορεί να παρέχει περαιτέρω πληροφορίες σχετικά με τον τύπο του κακόβουλου λογισμικού που μπορεί να έχει μολύνει έναν υπολογιστή. Σε άλλου τύπου περιστατικά, τα μέλη της ομάδας CSIRT μπορεί να μπορέσουν να εντοπίσουν πιθανούς τρόπους εξαγωγής δεδομένων (exfiltration) που χρησιμοποιεί ένας εξωτερικός επιτιθέμενος. Ένας τρόπος είναι η εγκατάσταση ενός **network tap**. Ένα network tap είναι ένα σύστημα που τοποθετείται στη γραμμή επικοινωνίας μεταξύ του μολυσμένου υπολογιστή και του switch. Για παράδειγμα, στο διάγραμμα δικτύου, αν ο υπολογιστής που έχει μολυνθεί βρίσκεται στο υποδίκτυο 192.168.1.0/24, το tap πρέπει να τοποθετηθεί ανάμεσα στον υπολογιστή και το switch. Αυτό συχνά απαιτεί την τοποθέτηση ενός συστήματος μεταξύ του υπολογιστή και του switch. Μια άλλη επιλογή είναι η διαμόρφωση μιας **θύρας Switched Port Analyzer (SPAN)**. Σε αυτή τη διαμόρφωση, το switch που βρίσκεται πλησιέστερα στον μολυσμένο υπολογιστή θα έχει ενεργοποιημένο το port mirroring. Αυτό στέλνει την κυκλοφορία από ολόκληρο το τμήμα του switch στο σύστημα που βρίσκεται στη θύρα καθρέφτη (mirrored port).

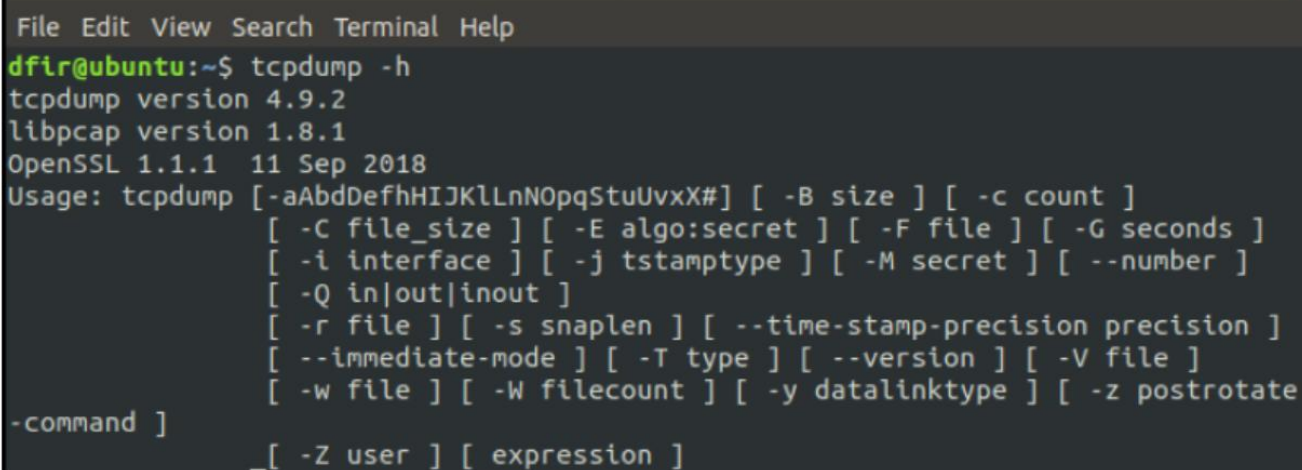
Τέλος, ορισμένες συσκευές δικτύου διαθέτουν ενσωματωμένες εφαρμογές, όπως το **tcpdump**, οι οποίες μπορούν να χρησιμοποιηθούν για την καταγραφή της κυκλοφορίας για περαιτέρω ανάλυση. Αυτή μπορεί να είναι η ταχύτερη επιλογή, καθώς δεν απαιτεί φυσική πρόσβαση στο δίκτυο ή στο switch και μπορεί να διαμορφωθεί απομακρυσμένα. Το μειονέκτημα αυτής της μεθόδου είναι ότι η

αποθήκευση στο switch ενδέχεται να μην υποστηρίζει μεγάλο αρχείο καταγραφής και η επιπλέον φόρτιση μπορεί να αυξήσει τις πιθανότητες να μην καταγραφούν κάποια πακέτα.

Tcpdump: Το **tcpdump** είναι ένα εργαλείο γραμμής εντολών που έχει σχεδιαστεί ειδικά για **packet capture**. Το tcpdump περιλαμβάνεται συχνά σε διανομές Linux και βρίσκεται σε πολλές συσκευές δικτύου. Για πολλές από αυτές τις συσκευές, το tcpdump πρέπει να εκτελείται ως root χρήστης ή με προνόμια root, καθώς παρακολουθεί την κυκλοφορία του δικτύου. Η τεκμηρίωση είναι διαθέσιμη στη διεύθυνση: <http://www.tcpdump.org/>.

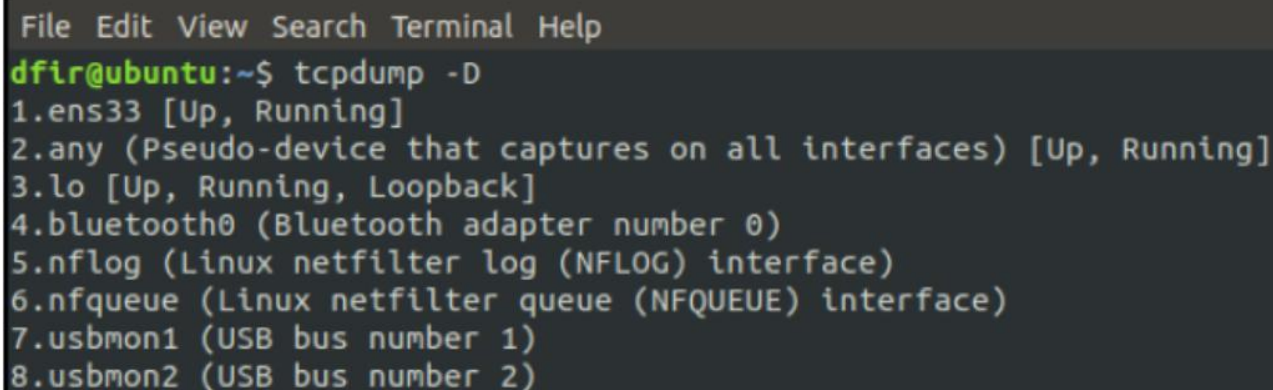
Για να εκτελέσετε ένα **packet capture** με το tcpdump, μπορεί να χρησιμοποιηθεί η ακόλουθη διαδικασία: Για πρόσβαση στο βασικό μενού βοήθειας, πληκτρολογήστε το εξής στο Command Prompt:

```
dfir@ubuntu:~$ tcpdump -h
```



```
File Edit View Search Terminal Help
dfir@ubuntu:~$ tcpdump -h
tcpdump version 4.9.2
libpcap version 1.8.1
OpenSSL 1.1.1 11 Sep 2018
Usage: tcpdump [-aAbdDefhHIJKLlnNOpqStuUvXx#] [-B size] [-c count]
               [-C file_size] [-E algo:secret] [-F file] [-G seconds]
               [-i interface] [-j tstamptype] [-M secret] [--number]
               [-Q in|out|inout]
               [-r file] [-s snaplen] [--time-stamp-precision precision]
               [--immediate-mode] [-T type] [--version] [-V file]
               [-w file] [-W filecount] [-y datalinktype] [-z postrotate
-command ]
               _[-Z user] [ expression ]
```

Η προεπιλεγμένη ρύθμιση του tcpdump είναι να καταγράφει την κυκλοφορία σε όλες τις διαθέσιμες διεπαφές. Εκτελώντας την παρακάτω εντολή παράγεται μια λίστα με όλες τις διεπαφές στις οποίες μπορεί το tcpdump να καταγράψει κυκλοφορία:

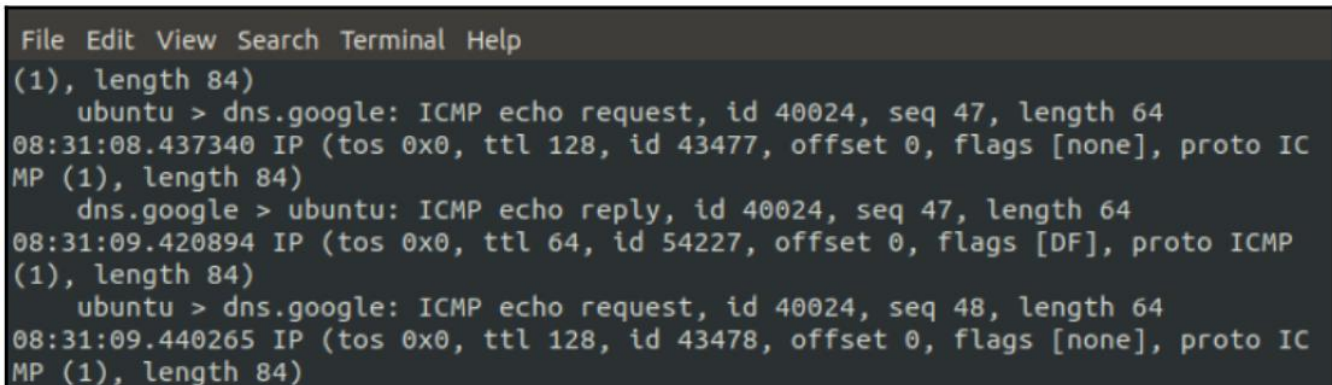


```
File Edit View Search Terminal Help
dfir@ubuntu:~$ tcpdump -D
1.ens33 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.bluetooth0 (Bluetooth adapter number 0)
5.nflog (Linux netfilter log (NFLOG) interface)
6.nfqueue (Linux netfilter queue (NFQUEUE) interface)
7.usbmon1 (USB bus number 1)
8.usbmon2 (USB bus number 2)
```

Για να διαμορφώσετε μια βασική καταγραφή στην Ethernet διεπαφή **ens33** με κανονική λεπτομέρεια, πληκτρολογήστε την ακόλουθη εντολή:

```
dfir@ubuntu:~$ sudo tcpdump -i ens33 -v
```

Η παράμετρος **-i** υποδεικνύει στο tcpdump σε ποια διεπαφή θα πραγματοποιηθεί η καταγραφή πακέτων. Σε αυτή την περίπτωση, είναι η Ethernet διεπαφή **ens33**. Η παράμετρος **-v** καθορίζει τη λεπτομέρεια (verbosity) της καταγραφής πακέτων. Εδώ, η λεπτομέρεια είναι σχετικά χαμηλή. Για περισσότερα δεδομένα, η παράμετρος μπορεί να οριστεί σε **-vvv** για μια πιο λεπτομερή προβολή των πακέτων.



```
File Edit View Search Terminal Help
(1), length 84)
  ubuntu > dns.google: ICMP echo request, id 40024, seq 47, length 64
08:31:08.437340 IP (tos 0x0, ttl 128, id 43477, offset 0, flags [none], proto IC
MP (1), length 84)
  dns.google > ubuntu: ICMP echo reply, id 40024, seq 47, length 64
08:31:09.420894 IP (tos 0x0, ttl 64, id 54227, offset 0, flags [DF], proto ICMP
(1), length 84)
  ubuntu > dns.google: ICMP echo request, id 40024, seq 48, length 64
08:31:09.440265 IP (tos 0x0, ttl 128, id 43478, offset 0, flags [none], proto IC
MP (1), length 84)
```

Αν και αυτή η μέθοδος δείχνει αν η κυκλοφορία διέρχεται από τη διεπαφή, οι πληροφορίες για τα μεμονωμένα πακέτα είναι σχεδόν άχρηστες για έναν αναλυτή λόγω της ταχύτητας με την οποία εμφανίζονται στην οθόνη. Για να είναι χρήσιμη η καταγραφή, συνιστάται η εξαγωγή της σε αρχείο ώστε να μπορεί να γίνει αργότερα ανάλυση με ένα εργαλείο ανάλυσης πακέτων όπως το **Wireshark**.

Το tcpdump μπορεί επίσης να διαμορφωθεί ώστε να επικεντρώνεται σε συγκεκριμένες πηγές ή προορισμούς IP και θύρες. Για παράδειγμα, αν ένας αναλυτής αντιμετώπισης περιστατικών χρειάζεται να συλλέξει πακέτα που φεύγουν από έναν συγκεκριμένο host με διεύθυνση IP **192.168.10.54**, η παρακάτω εντολή tcpdump θα παράγει το επιθυμητό αποτέλεσμα:

```
dfir@ubuntu:~$ sudo tcpdump -i ens33 src host 192.168.10.54
```

Πακέτα που πηγαίνουν σε έναν προορισμό, όπως ένας γνωστός C2 server, μπορούν επίσης να διαχωριστούν από την υπόλοιπη κυκλοφορία με την εντολή:

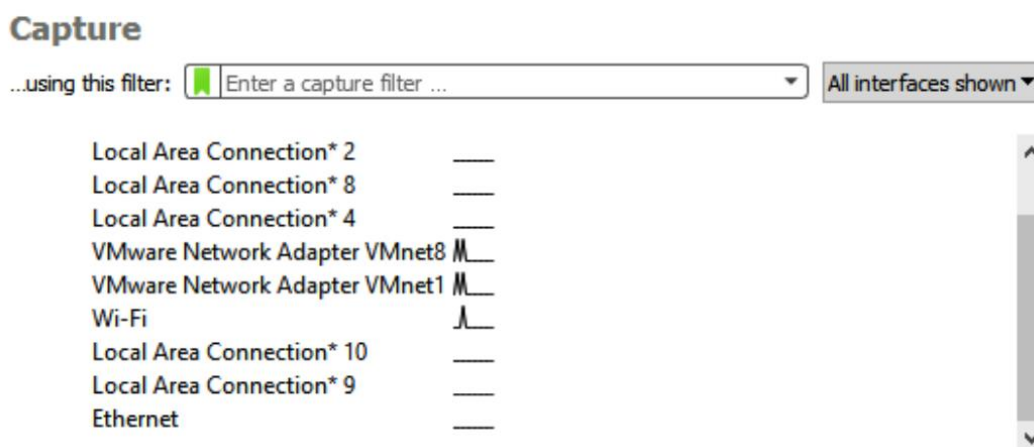
```
dfir@ubuntu:~$ sudo tcpdump -i ens33 dst host 162.4.5.23
```

Wireshark: Το Wireshark είναι ένα εργαλείο καταγραφής και ανάλυσης πακέτων για Unix ή Windows. Σε αντίθεση με το tcpdump ή εργαλεία όπως το RawCap, το Wireshark είναι εργαλείο με γραφικό περιβάλλον (GUI) και διαθέτει πλήθος λειτουργιών όχι μόνο για την καταγραφή, αλλά και για την ανάλυση πακέτων. Ως αποτέλεσμα, το Wireshark μπορεί να είναι δύσκολο να αναπτυχθεί γρήγορα κατά τη διάρκεια ενός περιστατικού, καθώς το πρόγραμμα πρέπει να εγκατασταθεί. Επιπλέον, το

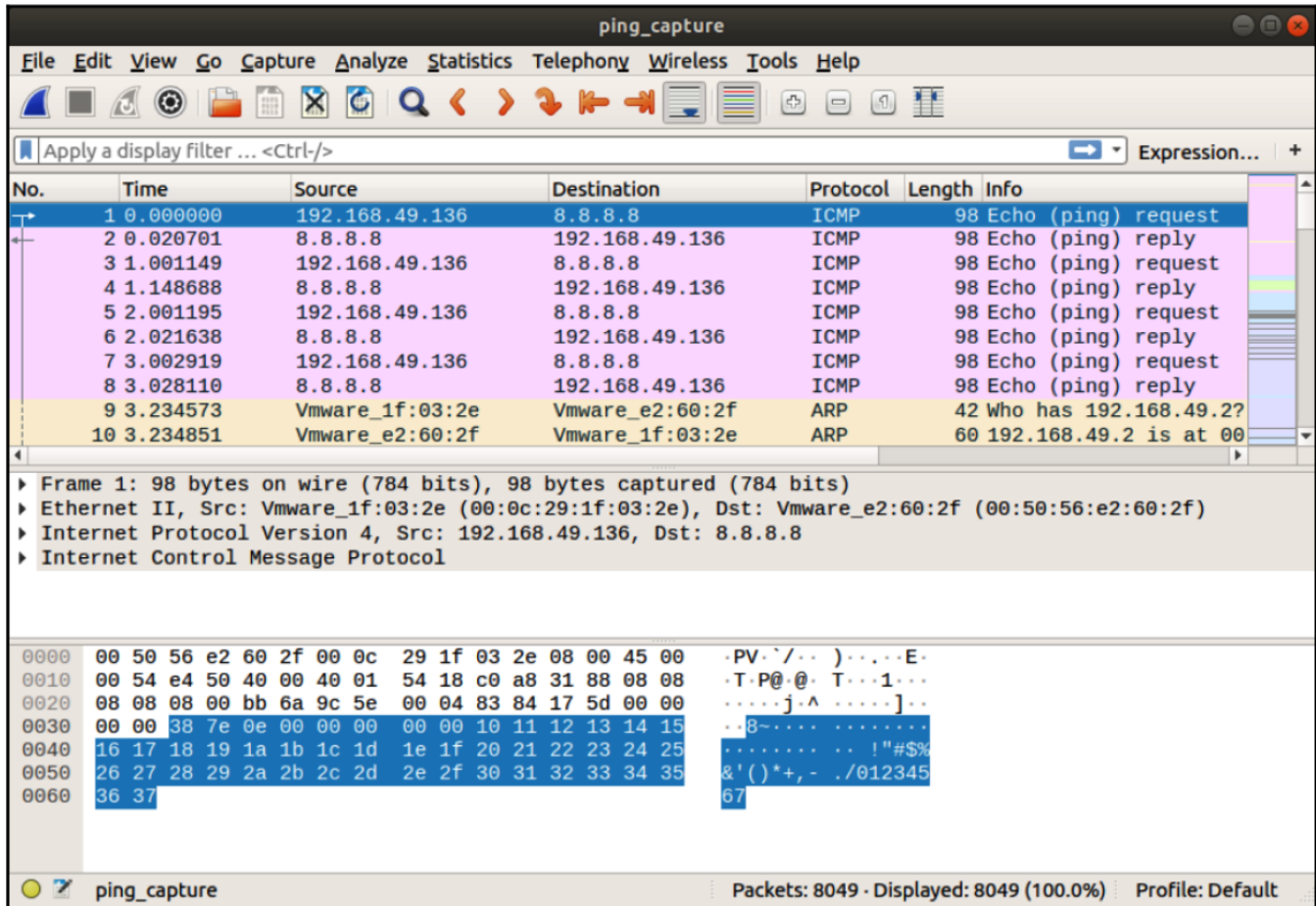
εργαλείο υποστηρίζεται μόνο σε Windows ή macOS. Η εγκατάσταση του Wireshark σε σύστημα Linux απαιτεί λίγο περισσότερη προσπάθεια. Το μοναδικό πλεονέκτημα του Wireshark σε σχέση με τις επιλογές γραμμής εντολών είναι ότι οι αναλυτές αντίδρασης σε περιστατικά μπορούν να πραγματοποιήσουν λεπτομερή έλεγχο της κυκλοφορίας καθώς αυτή καταγράφεται. Το Wireshark μπορεί να εκτελεστεί στο ίδιο το σύστημα ή από ένα USB drive. Αφού εγκατασταθεί, πρέπει να εκτελείται ως διαχειριστής.

Για να πραγματοποιηθεί καταγραφή πακέτων με το Wireshark, ακολουθείται η εξής διαδικασία:

1. Το πρώτο βήμα είναι η επιλογή μιας διεπαφής στην οποία το Wireshark θα καταγράψει την κυκλοφορία:



2. Στην προηγούμενη οθόνη, εμφανίζονται τρεις διεπαφές που φαίνεται να διαχειρίζονται κυκλοφορία. Αυτή στην οποία θα εστιάσουμε είναι η διεπαφή Wi-Fi.
3. Κάνοντας διπλό κλικ στη διεπαφή, θα ξεκινήσει η καταγραφή πακέτων η καταγραφή εμφανίζεται στην οθόνη για άμεση ανάλυση:



Για να σταματήσετε την καταγραφή, πατήστε το κόκκινο κουμπί στην πάνω αριστερή γωνία του παραθύρου. Στη συνέχεια, το αρχείο μπορεί να αποθηκευτεί για περαιτέρω ανάλυση.

Ένα άλλο εργαλείο που περιλαμβάνεται με το Wireshark και είναι χρήσιμο κατά την απόκτηση αποδεικτικών στοιχείων, είναι το **mergcap**. Το mergcap είναι ένα εργαλείο γραμμής εντολών που επιτρέπει στους αναλυτές ανταπόκρισης σε περιστατικά να συνδυάζουν πολλαπλά αρχεία καταγραφής πακέτων από το Wireshark, το tcpdump ή το RawCap. Αυτό είναι ιδιαίτερα χρήσιμο σε περιπτώσεις όπου οι αναλυτές έχουν συλλέξει καταγραφές πακέτων από πολλές πηγές αλλά θέλουν να ελέγξουν την κυκλοφορία προς έναν συγκεκριμένο υπολογιστή.

Για να ανοίξετε το μενού του **mergcap**, πληκτρολογήστε τα εξής σε ένα Command Prompt:

```
dfir@ubuntu:~$mergcap -help
```

```
File Edit View Search Terminal Help
dfir@ubuntu:~$ mergecap -help
Mergcap (Wireshark) 2.6.8 (Git v2.6.8 packaged as 2.6.8-1~ubuntu18.04.0)
Merge two or more capture files into one.
See https://www.wireshark.org for more information.

Usage: mergcap [options] -w <outfile>|- <infile> [<infile> ...]

Output:
  -a          concatenate rather than merge files.
              default is to merge based on frame timestamps.
  -s <snaplen> truncate packets to <snaplen> bytes of data.
  -w <outfile>|- set the output filename to <outfile> or '-' for stdout.
  -F <capture type> set the output file type; default is pcapng.
                  an empty "-F" option will list the file types.
  -I <IDB merge mode> set the merge mode for Interface Description Blocks; default is 'all'.
                  an empty "-I" option will list the merge modes.

Miscellaneous:
  -h          display this help and exit.
  -v          verbose output.
```

Για να συγχωνεύσετε πολλά αρχεία καταγραφής πακέτων, χρησιμοποιείται η εξής εντολή:

```
dfir@ubuntu:~$ mergecap -w switches.pcap switch1.pcap switch2.pcap switch3.pcap
```

Συνδυάζοντας την έξοδο τριών καταγραφών πακέτων σε ένα αρχείο, ο αναλυτής ανταπόκρισης σε περιστατικά μπορεί να εξετάσει ένα ευρύτερο φάσμα δραστηριοτήτων σε πολλαπλές διαδρομές δικτύου. Για παράδειγμα, αν ο αναλυτής αναζητά κυκλοφορία από άγνωστο υπολογιστή προς έναν εξωτερικό C2 server, θα μπορεί να συνδυάσει τις καταγραφές σε όλο το δίκτυο και στη συνέχεια να αναζητήσει τη συγκεκριμένη IP, αντί να ψάχνει χειροκίνητα σε κάθε αρχείο καταγραφής πακέτων.

Συλλογή αποδεικτικών στοιχείων: Για να διεξαχθεί μια σωστή ανάλυση αρχείων καταγραφής και άλλων δεδομένων δικτύου, όπως οι καταγραφές πακέτων, συχνά χρειάζεται να μετακινηθούν από την πηγή τους και να εξεταστούν εκτός σύνδεσης. Όπως με κάθε πηγή αποδεικτικών στοιχείων, τα αρχεία καταγραφής ή οι καταγραφές πακέτων πρέπει να χειρίζονται με προσοχή ώστε να διασφαλιστεί ότι δεν θα καταστραφούν ή τροποποιηθούν κατά τη μεταφορά. Μια απλή λύση είναι η άμεση μεταφορά των αποδεικτικών στοιχείων σε USB drive ή άλλο φορητό μέσο. Από εκεί, μπορεί να δημιουργηθεί ένα hash για τα αποδεικτικά στοιχεία πριν από οποιαδήποτε ανάλυση.

Η απόκτηση αποδεικτικών στοιχείων δικτύου, όπως μια καταγραφή πακέτων ή ένα αρχείο καταγραφής, θα πρέπει να τεκμηριώνεται με ακρίβεια. Το προσωπικό ανταπόκρισης σε περιστατικά μπορεί να συλλέγει αρχεία καταγραφής και καταγραφές πακέτων από πολλές πηγές σε ολόκληρο το δίκτυο. Ως εκ τούτου, θα πρέπει να διασφαλίζεται ότι κάθε ξεχωριστό αποδεικτικό στοιχείο μπορεί να αναχθεί στην πηγή του, καθώς και στην ημερομηνία και ώρα συλλογής του.

File Name	Description	Location	Date	Time	Collected By	MD5 Hash
Ping_capture	Packet Capture of Ping activity	192.168.2.1	6/26/19	1642	GTJ	7e559dc8eeeb66115566d93f96e7dfb8

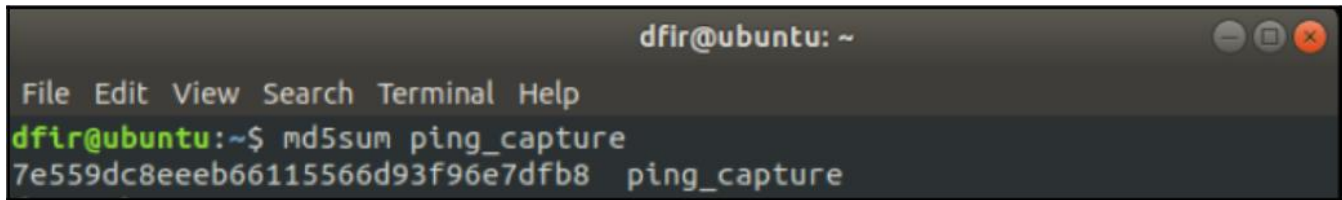
Αυτό μπορεί να καταγραφεί σε ένα φύλλο καταγραφής αποδεικτικών στοιχείων δικτύου, όπου μπορούν να γίνονται εγγραφές για κάθε στοιχείο. Για παράδειγμα, το ακόλουθο είναι ένα δείγμα φύλλου με μία εγγραφή: Η εγγραφή καταγράφει τις εξής απαραίτητες πληροφορίες:

- **Όνομα αρχείου (File Name):** Κάθε αρχείο καταγραφής ή καταγραφή πακέτων πρέπει να έχει μοναδικό όνομα. Στις διαδικασίες που χρησιμοποιεί η CSIRT, θα πρέπει να υπάρχει σύμβαση ονοματοδοσίας για διαφορετικούς τύπους αρχείων αποδεικτικών στοιχείων.
- **Περιγραφή (Description):** Μια σύντομη περιγραφή του αρχείου. Δεν χρειάζεται υπερβολική λεπτομέρεια, εκτός αν πρόκειται για μοναδικό αρχείο που απαιτεί λεπτομερή περιγραφή.
- **Τοποθεσία (Location):** Η τοποθεσία είναι σημαντική. Στην περίπτωση αυτή, η καταγραφή πακέτων αποκτήθηκε από τον switch στη διεύθυνση 192.168.2.1.
- **Ημερομηνία και Ώρα (Date and Time):** Καταγράψτε την ημερομηνία και την ώρα που το αρχείο μεταφέρθηκε στο μέσο αποθήκευσης. Πριν από ένα περιστατικό, είναι σημαντικό να προσδιοριστεί ποια ζώνη ώρας θα χρησιμοποιηθεί. Από αποδεικτική σκοπιά, η ζώνη ώρας δεν έχει ουσιαστική σημασία, αρκεί να είναι συνεπής σε όλη την έρευνα.
- **Συλλέχθηκε από (Collected By):** Τα αρχικά του ατόμου είναι επαρκή για το αρχείο καταγραφής.
- **MD5 Hash:** Μια λεπτομερής παρουσίαση της διαδικασίας hashing θα καλυφθεί σε επόμενα κεφάλαια. Προς το παρόν, αρκεί να σημειωθεί ότι το hash είναι ένας αλγόριθμος μιας κατεύθυνσης που χρησιμοποιείται για να παρέχει ένα ψηφιακό αποτύπωμα για ένα αρχείο. Το hash θα καταγραφεί τόσο κατά τη φάση συλλογής όσο και μετά την ανάλυση, για να αποδειχθεί ότι το αρχείο δεν τροποποιήθηκε κατά τη διάρκεια της ανάλυσης. Υπάρχουν διάφοροι τρόποι υπολογισμού του hash. Στην περίπτωση αυτή, το MD5 hash μπορεί να υπολογιστεί χρησιμοποιώντας το εγκατεστημένο πρόγραμμα hashing md5sum στο Ubuntu. Το md5sum διαθέτει διάφορες επιλογές που είναι προσβάσιμες μέσω της γραμμής εντολών. Για να εμφανιστεί το μενού βοήθειας, πληκτρολογήστε:

```
dfir@ubuntu:~$md5sum --help
```

Το MD5 hash για την καταγραφή πακέτων από τον switch μπορεί να υπολογιστεί απλά με την εκτέλεση της ακόλουθης εντολής:

```
dfir@ubuntu:~$ md5sum ping_capture
```

A terminal window titled 'dfir@ubuntu: ~' with standard window controls. The menu bar includes 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The command prompt shows 'dfir@ubuntu:~\$ md5sum ping_capture' and the output is '7e559dc8eeeb66115566d93f96e7dfb8 ping_capture'.

```
dfir@ubuntu: ~  
File Edit View Search Terminal Help  
dfir@ubuntu:~$ md5sum ping_capture  
7e559dc8eeeb66115566d93f96e7dfb8 ping_capture
```

Αυτό παράγει την αντίστοιχη έξοδο με το hash του αρχείου. Τα αρχεία καταγραφής και οι καταγραφές πακέτων θα πρέπει να μεταφέρονται σε συσκευή αποθήκευσης όσο το δυνατόν συντομότερα. Μόλις ολοκληρωθεί η συλλογή, θα πρέπει επίσης να συμπληρωθεί μια φόρμα αλυσίδας φύλαξης (chain of custody) για το εξωτερικό μέσο που περιέχει τα αρχεία αποδεικτικών στοιχείων. Από εκεί και πέρα, τα αρχεία μπορούν να υποβληθούν σε ανάλυση.

Τα στοιχεία που είναι σχετικά για τους αναλυτές αντιμετώπισης περιστατικών δεν εντοπίζονται μόνο στον σκληρό δίσκο ενός συμβιβασμένου υπολογιστή. Υπάρχει ένας μεγάλος όγκος πληροφοριών διαθέσιμος από τις δικτυακές συσκευές που βρίσκονται διάσπαρτες στο περιβάλλον. Με την κατάλληλη προετοιμασία, ένα CSIRT μπορεί να αξιοποιήσει τα στοιχεία που παρέχουν αυτές οι συσκευές μέσω λύσεων όπως ένα SIEM. Τα μέλη του CSIRT έχουν επίσης τη δυνατότητα να καταγράφουν την κυκλοφορία δικτύου για μετέπειτα ανάλυση μέσω διαφόρων μεθόδων και εργαλείων. Πίσω από όλες αυτές τις τεχνικές, όμως, υπάρχουν νομικές και πολιτικές πτυχές που τα μέλη του CSIRT και ο οργανισμός συνολικά πρέπει να διαχειριστούν. Με την προετοιμασία για τις νομικές και τεχνικές προκλήσεις της συλλογής δικτυακών αποδεικτικών στοιχείων, τα μέλη του CSIRT μπορούν να αξιοποιήσουν αυτά τα στοιχεία και να προχωρήσουν προς τον στόχο της ανεύρεσης της βασικής αιτίας ενός περιστατικού και της επαναφοράς του οργανισμού σε πλήρη λειτουργία.

Το κεφάλαιο αυτό ανέλυσε διάφορες πηγές αποδεικτικών στοιχείων διαθέσιμες στους αναλυτές αντιμετώπισης περιστατικών. Τα αρχεία καταγραφής από δικτυακές συσκευές, είτε αναφέρονται σε ένα SIEM είτε μέσω άλλων μεθόδων, μπορούν να παρέχουν εικόνα για το τι έχει συμβεί στο δίκτυο. Οι καταγραφές πακέτων παρέχουν λεπτομέρειες σχετικά με τη φύση της δικτυακής κυκλοφορίας. Τέλος, οι αναλυτές πρέπει να είναι έτοιμοι να αποκτήσουν αυτές τις πηγές αποδεικτικών στοιχείων με τρόπο εγκληματολογικά ασφαλή.

5

Απόκτηση Αποδεικτικών Στοιχείων από Συστήματα Υπολογιστών

Τα συστήματα υπολογιστών αποτελούν στόχους κακόβουλων ενεργειών πολύ συχνά. Μπορεί να χρησιμοποιηθούν ως αρχικός στόχος, ώστε κάποιος να αποκτήσει σημείο πρόσβασης στο δίκτυο ή να λειτουργήσουν ως σημείο αναπήδησης (pivot point) για περαιτέρω επιθέσεις, αλλά και ως τελικός στόχος των επιτιθέμενων. Ως εκ τούτου, οι αναλυτές απόκρισης σε περιστατικά (incident response analysts) πρέπει να είναι προετοιμασμένοι να διερευνήσουν αυτά τα συστήματα.

Τα σύγχρονα λειτουργικά συστήματα, όπως τα Microsoft Windows, δημιουργούν μια ποικιλία αποδεικτικών τεκμηρίων κατά την εκτέλεση μιας εφαρμογής, όταν γίνονται αλλαγές σε αρχεία ή όταν προστίθενται λογαριασμοί χρηστών. Όλες αυτές οι αλλαγές αφήνουν ίχνη δραστηριότητας που μπορούν να αξιολογηθούν από τους αναλυτές. Ο όγκος των διαθέσιμων δεδομένων για την απόκριση σε περιστατικά αυξάνεται, καθώς η μνήμη και ο αποθηκευτικός χώρος ακόμη και των οικονομικότερων συστημάτων συνεχώς επεκτείνονται. Σήμερα, συνηθισμένα συστήματα διατίθενται με μεγάλη μνήμη και αποθήκευση σε terabytes· άρα υπάρχει πληθώρα δεδομένων που μπορεί να βοηθήσει τους αναλυτές να εντοπίσουν την αιτία ενός περιστατικού. Για τον λόγο αυτό, οι αναλυτές πρέπει να είναι έτοιμοι να αποκτήσουν διαφορετικούς τύπους αποδεικτικών στοιχείων από τα συστήματα προς περαιτέρω ανάλυση.

Σε αυτό το κεφάλαιο θα καλυφθούν τα εξής θέματα:

- Προετοιμασία
- Σειρά πτητικότητας (Order of Volatility)
- Απόκτηση αποδεικτικών στοιχείων
- Απόκτηση πτητικής μνήμης
- Απόκτηση μη πτητικών αποδεικτικών στοιχείων

5.1. Προετοιμασία

Όσον αφορά την προετοιμασία, οι αναλυτές απόκρισης σε περιστατικά πρέπει να διαθέτουν τα απαραίτητα εργαλεία για την απόκτηση αποδεικτικών στοιχείων από τα συστήματα. Οι τεχνικές που

θα συζητηθούν σε αυτό το κεφάλαιο δεν βασίζονται σε εξειδικευμένη τεχνολογία, αλλά σε εργαλεία που μπορούν να αποκτηθούν με μικρό ή μηδενικό κόστος. Είναι κρίσιμο τα εργαλεία που επιλέγονται να προέρχονται από αξιόπιστες πηγές, να έχουν αποδειχθεί αποτελεσματικά από άλλους υπαλλήλους ομάδων CSIRT, και να έχουν επικυρωθεί πριν από τη χρήση τους.

Πέρα από το λογισμικό, ο μοναδικός επιπλέον εξοπλισμός που απαιτείται είναι εξωτερικοί σκληροί δίσκοι και συνηθισμένοι επιτραπέζιοι υπολογιστές.

Σε ένα εταιρικό περιβάλλον, είναι καλή πρακτική οι υπεύθυνοι απόκρισης να γνωρίζουν τους τύπους συστημάτων που χρησιμοποιούνται συνήθως. Για παράδειγμα, σε έναν οργανισμό που χρησιμοποιεί αποκλειστικά λειτουργικά Microsoft, τα εργαλεία πρέπει να υποστηρίζουν πολλές εκδόσεις του λειτουργικού. Σε άλλες περιπτώσεις, μπορεί να υπάρχει αναλογία 80/20 μεταξύ Microsoft και Linux· συνεπώς, οι υπεύθυνοι πρέπει να είναι εξοπλισμένοι με εργαλεία και τεχνικές που καλύπτουν και τα δύο περιβάλλοντα.

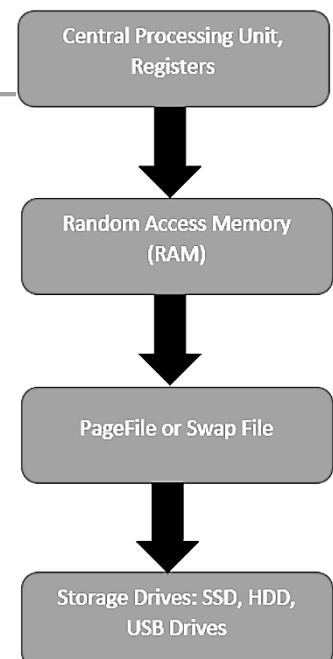
Πολλά από τα εργαλεία και τις τεχνικές που θα συζητηθούν απαιτούν δικαιώματα διαχειριστή. Οι αναλυτές πρέπει να διαθέτουν τα κατάλληλα διαπιστευτήρια για την εκτέλεση αυτών των ενεργειών. Πρέπει να σημειωθεί ότι πρέπει να χρησιμοποιούνται μόνο υπάρχοντες λογαριασμοί, καθώς η προσθήκη νέων σε ένα πιθανώς παραβιασμένο σύστημα μπορεί να καταστήσει τα αποδεικτικά στοιχεία μη αποδεκτά σε δικαστικές διαδικασίες.

Μία τεχνική είναι οι αναλυτές να διαθέτουν ατομικά διαπιστευτήρια που ενεργοποιούνται μόνο κατά τη διάρκεια ενός περιστατικού. Αυτό επιτρέπει στον οργανισμό να διαχωρίζει τη νόμιμη χρήση διαπιστευτηρίων από κακόβουλη χρήση, ενώ διευκολύνει και την αναπαραγωγή των ενεργειών της ομάδας απόκρισης. Αξίζει να σημειωθεί ότι τεχνικά προηγμένοι αντίπαλοι συχνά παρακολουθούν το δίκτυο κατά τη διάρκεια μιας επίθεσης, προκειμένου να διαπιστώσουν αν έχουν εντοπιστεί. Συνεπώς, τα διαπιστευτήρια αυτά δεν πρέπει να αποκαλύπτουν ότι συνδέονται με αναλυτές ή άλλο προσωπικό που ερευνά την παραβίαση.

5.2. Σειρά Πτητικότητας (Order of Volatility)

Δεν έχουν όλα τα αποδεικτικά στοιχεία σε ένα σύστημα την ίδια αξία. Ο όρος **πτητικότητα (volatility)** περιγράφει το πόσο διατηρούνται τα δεδομένα σε ένα σύστημα μετά από ενέργειες όπως αποσύνδεση χρηστών ή τερματισμό λειτουργίας.

- **Πτητικά δεδομένα** είναι εκείνα που χάνονται εάν το σύστημα απενεργοποιηθεί. Σε αυτά περιλαμβάνονται δεδομένα στη CPU, οι πίνακες δρομολόγησης, ή η ARP cache. Ένα από τα πιο κρίσιμα κομμάτια πτητικών αποδεικτικών στοιχείων είναι η μνήμη RAM. Σε περιστατικά όπως μολύνσεις από κακόβουλο λογισμικό, η μνήμη ενός ενεργού συστήματος είναι υψίστης σημασίας, καθώς το κακόβουλο



λογισμικό αφήνει εκεί κρίσιμα ίχνη (π.χ. δεδομένα μητρώου, ιστορικό εντολών, δικτυακές συνδέσεις). Αν χαθούν, ο αναλυτής μπορεί να βρεθεί με ελάχιστα ή καθόλου δεδομένα για διερεύνηση.

- **Μη πτητικά δεδομένα** είναι εκείνα που αποθηκεύονται σε σκληρό δίσκο και διατηρούνται μετά τον τερματισμό του συστήματος. Σε αυτά περιλαμβάνονται καταχωρίσεις του Master File Table (MFT), δεδομένα μητρώου και τα ίδια τα αρχεία. Αν και το κακόβουλο λογισμικό αφήνει αποδείξεις στη μνήμη, εξακολουθούν να υπάρχουν στοιχεία αξίας και στη μη πτητική μνήμη.

Το διάγραμμα απεικονίζει τα διαφορετικά επίπεδα πτητικότητας των ψηφιακών αποδεικτικών στοιχείων, τα οποία πρέπει να λαμβάνονται υπόψη κατά τον καθορισμό της σειράς απόκτησης.

5.3. Απόκτηση Αποδεικτικών Στοιχείων (Evidence Acquisition)

Υπάρχουν διάφορες μέθοδοι που χρησιμοποιούνται όχι μόνο για την πρόσβαση σε μια πιθανή πηγή αποδεικτικών στοιχείων αλλά και για τον καθορισμό του τύπου της απόκτησης που μπορεί να πραγματοποιηθεί. Για τον ορισμό αυτών των μεθόδων, είναι σημαντικό να υπάρχει σαφής κατανόηση του τρόπου και του είδους της απόκτησης που μπορεί να αξιοποιηθεί:

- **Τοπική (Local):** Η πρόσβαση στο υπό διερεύνηση σύστημα αποτελεί συχνά πολυτέλεια για τους περισσότερους οργανισμούς. Ωστόσο, υπάρχουν πολλές περιπτώσεις όπου οι αναλυτές απόκρισης ή άλλο προσωπικό έχουν άμεση φυσική πρόσβαση στο σύστημα.
- **Απομακρυσμένη (Remote):** Στην απομακρυσμένη απόκτηση, οι αναλυτές αξιοποιούν εργαλεία και δικτυακές συνδέσεις για τη συλλογή αποδεικτικών στοιχείων. Η μέθοδος αυτή αποτελεί προφανή επιλογή όταν υπάρχουν γεωγραφικοί περιορισμοί ή όταν οι αναλυτές δεν μπορούν να βρεθούν επιτόπου άμεσα.
- **Ζωντανή (Live acquisition):** Η ζωντανή απόκτηση συμβαίνει όταν τα αποδεικτικά στοιχεία συλλέγονται από ένα σύστημα που είναι ενεργό και σε λειτουργία. Ορισμένες τεχνικές που θα παρουσιαστούν σε αυτό το κεφάλαιο απαιτούν να εφαρμοστούν σε ζωντανό σύστημα (π.χ. απόκτηση μνήμης RAM). Η πλήρης απόκτηση αποδεικτικών στοιχείων από ζωντανό σύστημα είναι απαραίτητη σε περιβάλλοντα υψηλής διαθεσιμότητας όπου δεν είναι δυνατή η διακοπή λειτουργίας. Έτσι, οι αναλυτές μπορούν να αποκτήσουν και να αναλύσουν τα δεδομένα ώστε να διαπιστώσουν αν το σύστημα έχει παραβιαστεί.
- **Εκτός σύνδεσης (Offline acquisition):** Χρησιμοποιείται συχνά από τις διωκτικές αρχές για τη διατήρηση ψηφιακών αποδεικτικών στοιχείων από τον σκληρό δίσκο. Το σύστημα τερματίζεται, αφαιρείται ο δίσκος και εξειδικευμένα εργαλεία χρησιμοποιούνται για την απόκτησή του. Τα μειονεκτήματα αυτής της μεθόδου είναι: (α) η απώλεια πτητικών δεδομένων, (β) η μεγάλη χρονική καθυστέρηση για την απόκτηση, απεικόνιση και ανάλυση του δίσκου, κάτι που μπορεί να οδηγήσει σε καθυστέρηση άνω των 24 ωρών.

Ανάλογα με το είδος του περιστατικού και τους χρονικούς ή γεωγραφικούς περιορισμούς, οι αναλυτές πρέπει να είναι έτοιμοι να εφαρμόσουν οποιαδήποτε από αυτές τις μεθόδους. Το ιδανικό σενάριο για μια ομάδα CSIRT είναι να μπορεί να πραγματοποιεί τόσο ζωντανή όσο και εκτός σύνδεσης απόκτηση, ώστε να εξασφαλίζεται ο μέγιστος όγκος αποδεικτικών στοιχείων προς ανάλυση. Για τον σκοπό αυτό, οι αναλυτές πρέπει να διαθέτουν τα απαραίτητα εργαλεία και εμπειρία.

Για την τοπική απόκτηση, απαιτείται εξωτερικός σκληρός δίσκος ή USB με επαρκή χώρο για τη μνήμη RAM του συστήματος και τυχόν άλλα αρχεία. Για τη διασφάλιση της ακεραιότητας των δεδομένων, συνιστάται ο χωρισμός του USB σε δύο κατατμήσεις: η πρώτη με τα εργαλεία απόκτησης και η δεύτερη ως αποθετήριο αποδεικτικών στοιχείων. Αυτό επιτρέπει τη μετέπειτα μεταφορά των στοιχείων σε μόνιμη αποθήκευση και την εκκαθάριση της κατάτμησης χωρίς απώλεια εργαλείων.

5.4. Διαδικασίες Συλλογής Αποδεικτικών Στοιχείων

Υπάρχουν πολλές ομοιότητες ανάμεσα στη **ψηφιακή εγκληματολογία** και σε άλλες εγκληματολογικές επιστήμες, όπως η ανάλυση ιχνών. Η βασική ομοιότητα είναι ότι οι οργανισμοί πρέπει να διαθέτουν διαδικασίες ορθές, επαναλήψιμες και τεκμηριωμένες. Οι βασικές κατευθυντήριες οδηγίες είναι:

1. **Φωτογράφιση συστήματος και σκηνής:** Ένα μικρό ψηφιακό φωτογραφικό μηχάνημα μπορεί να εξοικονομήσει χρόνο. Οι φωτογραφίες επιτρέπουν ανακατασκευή των γεγονότων σε περίπτωση δικαστικής διαδικασίας. Πρέπει να αποφεύγεται η χρήση κινητών τηλεφώνων, καθώς ενδέχεται να ζητηθεί η κατάσχεσή τους.
2. **Έλεγχος κατάστασης συστήματος:** Αν το σύστημα είναι ενεργό, παραμένει ενεργό. Αν είναι απενεργοποιημένο, δεν ενεργοποιείται. Η ενεργοποίηση ή απενεργοποίηση προκαλεί αλλαγές που μπορεί να αλλοιώσουν τα δεδομένα. Σε συστήματα με πλήρη κρυπτογράφηση δίσκου, η διατήρηση της λειτουργίας επιτρέπει την απόκτηση των λογικών τόμων. Αν υπάρχει κίνδυνος για άλλα συστήματα, αποσυνδέεται από το δίκτυο.
3. **Απόκτηση μνήμης RAM:** Κρίσιμο στοιχείο που περιέχει πληροφορίες για διεργασίες, DLLs και δικτυακές συνδέσεις.
4. **Απόκτηση αρχείων μητρώου και log:** Αν και μη πτητικά, η άμεση πρόσβαση σε αυτά βοηθά στην έρευνα κακόβουλου λογισμικού.
5. **Αποσύνδεση παροχής ρεύματος:** Σε φορητούς υπολογιστές αφαιρείται και η μπαταρία. Φωτογραφίζεται το πίσω μέρος με μοντέλο και σειριακό αριθμό.
6. **Φωτογράφιση σκληρού δίσκου:** Με το κάλυμμα ανοιχτό, φωτογραφίζονται μοντέλο και σειριακός αριθμός.
7. **Αφαίρεση σκληρού δίσκου:** Τοποθέτηση σε αντιστατικό σακουλάκι, σφραγισμένο φάκελο/κουτί. Ο αναλυτής υπογράφει τη σφράγιση και σημειώνονται αριθμός περιστατικού, αποδεικτικού, ημερομηνία, ώρα και υπεύθυνος κατάσχεσης.

8. **Τεκμηρίωση ενεργειών:** Καταγραφή ημερομηνιών, ωρών και υπευθύνων. Οι σημειώσεις και φωτογραφίες κατά την κατάσχεση είναι πολύτιμες για την ανακατασκευή γεγονότων.

5.5. Απόκτηση Πτητικής Μνήμης (Acquiring Volatile Memory)

Η παραδοσιακή ψηφιακή εγκληματολογία (**dead box forensics**) επικεντρώνεται στον σκληρό δίσκο από απενεργοποιημένο σύστημα. Αυτή η προσέγγιση είναι κατάλληλη για εγκλήματα όπως απάτη ή παιδική εκμετάλλευση, όπου αναζητούνται αρχεία εικόνας, έγγραφα, ή υπολογιστικά φύλλα. Όμως, απαιτεί τερματισμό του συστήματος, γεγονός που καταστρέφει κάθε αποδεικτικό στοιχείο που υπήρχε στη μνήμη RAM.

Σε περιστατικά ασφάλειας, μεγάλο μέρος των αποδεικτικών στοιχείων βρίσκεται στη μνήμη ενός παραβιασμένου συστήματος — ειδικά σε περιπτώσεις μόλυνσης από κακόβουλο λογισμικό ή εκμετάλλευσης με εργαλεία όπως το Metasploit. Η μνήμη περιέχει ίχνη που είναι κρίσιμα για την ανάλυση. Επομένως, πριν τερματιστεί το σύστημα και αφαιρεθεί ο σκληρός δίσκος, είναι απαραίτητο να αποκτηθεί η ενεργή μνήμη.

Υπάρχουν τόσο δωρεάν όσο και εμπορικά εργαλεία που χρησιμοποιούνται για την απόκτηση μνήμης. Η επιλογή εξαρτάται από τα εργαλεία ανάλυσης που θα χρησιμοποιηθούν στη συνέχεια. Δύο δημοφιλή πλαίσια για ανάλυση μνήμης είναι τα **Rekall** και **Volatility**.

Η μνήμη μπορεί να αποκτηθεί με δύο τρόπους:

1. **Τοπικά:** μέσω USB ή άλλου αποθηκευτικού μέσου συνδεδεμένου απευθείας στο ύποπτο σύστημα.
2. **Απομακρυσμένα:** με εξειδικευμένο λογισμικό που πραγματοποιεί την απόκτηση μέσω δικτύου.

5.6. Τοπική Απόκτηση (Local Acquisition)

Όταν υπάρχει φυσική πρόσβαση, ο αναλυτής μπορεί να αποκτήσει μνήμη και άλλα δεδομένα τοπικά. Αυτό επιτυγχάνεται με εργαλεία που εκτελούνται από USB ή άλλο αφαιρούμενο μέσο. Η διαδικασία αυτή συνήθως συνοδεύεται και από κατάσχεση του σκληρού δίσκου. Τρία εργαλεία που χρησιμοποιούνται συχνά:

- **FTK Imager (Access Data)**
- **WinPmem (Google)**
- **RamCapturer (Belkasoft)**

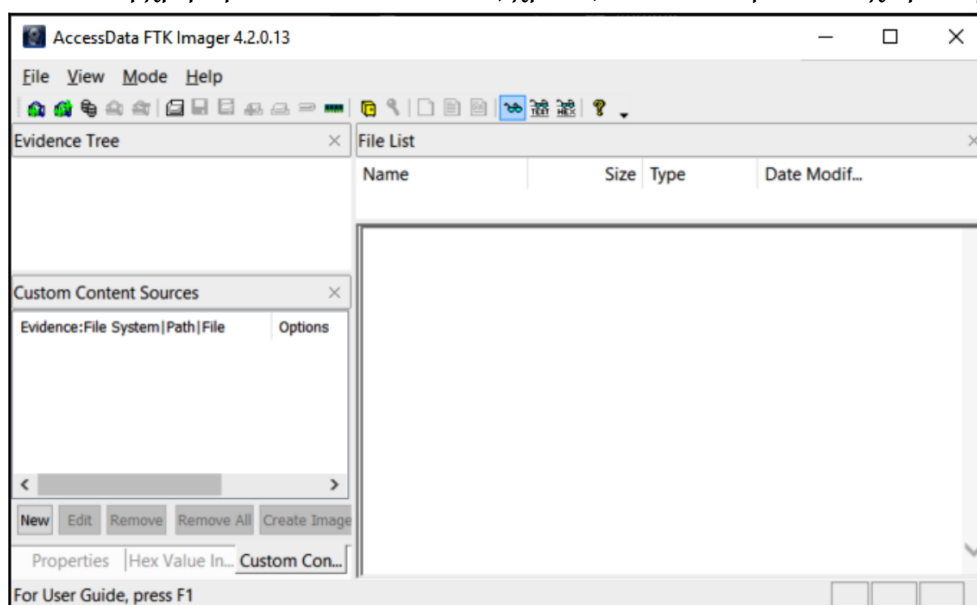
Συνιστάται η χρήση εξωτερικού δίσκου με δύο κατατμήσεις: μία με τα εργαλεία απόκτησης και μία για τα αποδεικτικά αρχεία. Έτσι αποφεύγεται η ανάμειξη αποδεικτικών στοιχείων με τα εργαλεία.

5.7. FTK Imager

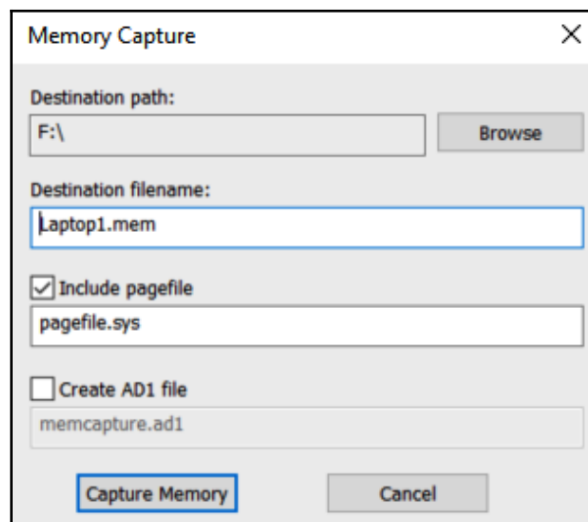
Το **FTK Imager** της Access Data είναι μία πλατφόρμα λογισμικού για Windows, η οποία εκτελεί ποικιλία εργασιών απεικόνισης (imaging), συμπεριλαμβανομένης και της απόκτησης της τρέχουσας μνήμης (running memory) ενός συστήματος. Το λογισμικό μπορεί να ληφθεί από τη διεύθυνση: <https://accessdata.com/product-download>

Ας δούμε τα βήματα χρήσης της πλατφόρμας:

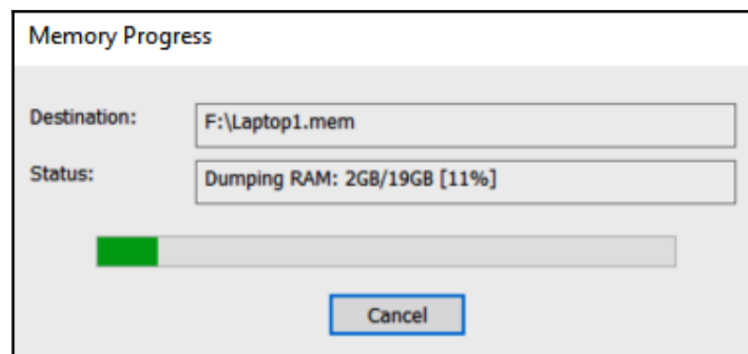
1. Αφού πραγματοποιηθεί η λήψη, εγκατέστησε το εκτελέσιμο αρχείο στην κατάτμηση **Tools** του USB drive.
2. Άνοιξε τον φάκελο του FTK Imager και εκτέλεσε το πρόγραμμα ως **διαχειριστής**. (Το FTK Imager απαιτεί τη χρήση drivers και συνεπώς χρειάζεται δικαιώματα διαχειριστή.)



3. Θα εμφανιστεί το παράθυρο **Capture Memory**, στο οποίο μπορείς να καθορίσεις:



- **Destination path:** Τη διαδρομή στον εξωτερικό δίσκο/USB όπου θα αποθηκευτεί το αρχείο μνήμης.
 - **Include pagefile:** Αν επιθυμείς να συμπεριληφθεί και το αρχείο pagefile.sys (το οποίο μπορεί να περιέχει ίχνη διεργασιών και δεδομένων που δεν χωρούσαν στη RAM).
 - **Create AD1 file:** Επιλογή για αποθήκευση της εικόνας μνήμης σε format AD1 (ειδική μορφή του FTK).
4. Αφού ρυθμίσεις τις επιλογές, πάτησε **Capture Memory**. Θα ξεκινήσει η διαδικασία λήψης της μνήμης. Η πρόοδος θα εμφανίζεται σε γραμμή προόδου (progress bar).
5. Όταν ολοκληρωθεί η διαδικασία, θα δημιουργηθεί ένα αρχείο εικόνας μνήμης (.mem ή .ad1, ανάλογα με τις επιλογές σου). Αυτό το αρχείο μπορεί να χρησιμοποιηθεί στη συνέχεια για ανάλυση με εργαλεία όπως **Rekall** ή **Volatility**.



6. Συνιστάται να καταγράψεις:
- Την ημερομηνία και ώρα απόκτησης.
 - Την ακριβή διαδρομή αποθήκευσης του αρχείου.
 - Τυχόν πρόσθετες επιλογές που ενεργοποιήθηκαν (π.χ. pagefile inclusion).

Με αυτόν τον τρόπο εξασφαλίζεται ότι η διαδικασία είναι **αναπαραγώγιμη** και τα αποδεικτικά στοιχεία διατηρούνται σε **αλυσίδα φύλαξης (chain of custody)**.

5.8. WinPmem

Όπως αναφέρθηκε προηγουμένως, ορισμένα εργαλεία απόκτησης μνήμης συνεργάζονται καλύτερα με συγκεκριμένα εργαλεία ανάλυσης μνήμης. Στην περίπτωση του εργαλείου ανάλυσης μνήμης **Rekall**, παρέχονται αρκετά εργαλεία απόκτησης μνήμης από τον ίδιο οργανισμό που το ανέπτυξε.

Τα εργαλεία **PMEM** που διατίθενται, χρησιμοποιούνται για την απόκτηση ακατέργαστης μνήμης (raw memory) από συστήματα **Linux**, **macOS** και **Windows**. Τα εργαλεία αυτά μπορούν να ληφθούν από την ιστοσελίδα του Rekall: <http://releases.rekallforensic.com/>

Στην παρακάτω επίδειξη, το σύστημα-στόχος είναι το ίδιο που χρησιμοποιήθηκε και στην παρουσίαση του **FTK Imager**. Για τον λόγο αυτό, θα χρησιμοποιηθεί το εργαλείο **WinPmem**, το οποίο έχει σχεδιαστεί ειδικά για την απόκτηση μνήμης από συστήματα Windows.

Από την έκδοση **2.0.1** και μετά, η προεπιλεγμένη έξοδος του εργαλείου WinPmem είναι η μορφή αρχείου **Advanced Forensic Framework 4 (AFF4)**. Η μορφή αυτή δημιουργήθηκε για να επιτρέπει την οργάνωση πολλαπλών πηγών δεδομένων και ροών εργασίας. Πρόκειται για **ανοιχτού κώδικα** μορφή, η οποία χρησιμοποιείται για αποδεικτικά στοιχεία στην ψηφιακή εγκληματολογία, καθώς και για σχετικά δεδομένα.

Ας ξεκινήσουμε:

1. Για να αποκτηθεί η φυσική μνήμη του συστήματος-στόχου, άνοιξε τη γραμμή εντολών **Windows Command Prompt** με δικαιώματα διαχειριστή.

```
D:\>winpmem-2.1.exe -h

USAGE:

winpmem-2.1.exe [-l] [-u] [--write-mode] [--mode <MmMapIoSpace,
PhysicalMemory, PTERemapping>] [--driver <Path to
driver.>] [--format <map, elf, raw>] [-m] [-p
</path/to/pagefile>] ... [-V] [-d] [-v] [-t] [-i
</path/to/file/or/device>] ... [-e <string>] [-o
</path/to/file>] [-c <zlib, snappy, none>] [--]
[--version] [-h] </path/to/aff4/volume> ...
```

Στη συνέχεια, ρύθμισε το **WinPmem** ώστε να αποκτήσει τη μνήμη του συστήματος πληκτρολογώντας:

```
D:\>winpmem-2.1.exe --format raw -o e:\Laptop1
```

Η εντολή αυτή λέει στο WinPmem να αποκτήσει τη μνήμη σε **raw format** και να την αποθηκεύσει σε έναν φάκελο που θα δημιουργηθεί στο **evidence partition** του USB drive που χρησιμοποιείται. Η παραπάνω εντολή θα παραγάγει την εξής έξοδο:

```
D:\>winpmem-2.1.exe --format raw -o e:\Laptop1
Driver Unloaded.
CR3: 0x00001AA000
 7 memory ranges:
Start 0x00001000 - Length 0x0009C000
Start 0x00100000 - Length 0x00002000
Start 0x00103000 - Length 0xBE2FE000
Start 0xBE889000 - Length 0x1BD7E000
Start 0xDA770000 - Length 0x00775000
Start 0xDBAFF000 - Length 0x00001000
Start 0x100000000 - Length 0x31E800000
```

Το WinPmem στη συνέχεια σαρώνει ολόκληρη τη δομή της μνήμης. Κατά τη διάρκεια της διαδικασίας αυτής, θα εμφανιστεί η ακόλουθη έξοδος:

```
Creating output AFF4 Directory structure.
Dumping Range 0 (Starts at 1000, length 9c000)
Dumping Range 1 (Starts at 100000, length 2000)
Dumping Range 2 (Starts at 103000, length be2fe000)
Dumping Range 3 (Starts at be89000, length 1bd7e000)
Dumping Range 4 (Starts at da770000, length 775000)
Dumping Range 5 (Starts at dbaff000, length 1000)
Dumping Range 6 (Starts at 100000000, length 31e800000)
Reading 0x8000 0MiB / 16272MiB 0MiB/s
Reading 0x4398000 67MiB / 16272MiB 255MiB/s
Reading 0x89b0000 137MiB / 16272MiB 275MiB/s
```

Συμπερασματικά, μια επισκόπηση του αρχείου εξόδου δείχνει ότι **ολόκληρη η φυσική μνήμη** περιέχεται μέσα σε ένα μόνο αρχείο, μαζί με άλλα αρχεία ως μέρος του **AFF4 file container**. Το WinPmem είναι ένα εύκολο εργαλείο στη χρήση, αλλά ένα από τα μεγαλύτερα πλεονεκτήματά του είναι ότι υπάρχουν εκδόσεις για **Linux**, **macOS** και **Windows**. Αυτό επιτρέπει στους αναλυτές περιστατικών να εξοικειωθούν με **ένα εργαλείο για όλα τα λειτουργικά συστήματα** που μπορεί να συναντήσουν στον οργανισμό τους.

Το μοναδικό μειονέκτημα της χρήσης του WinPmem είναι ότι το **AFF4 format** πρέπει να μετατραπεί σε **raw memory image**, εάν ο αναλυτής ή ο incident responder επιθυμεί να εξετάσει τη μνήμη με το **Volatility**.

Για να μετατραπεί ένα αρχείο **AFF4** σε **RAW format**, πρέπει να εκτελεστεί η παρακάτω εντολή με το WinPmem:

```
D:\winpmem-2.1.exe D:\Laptop1.aff4 -e PhysicalMemory -o Laptop1.raw
```

5.9. Απομακρυσμένη Απόκτηση (Remote acquisition)

Η προτιμώμενη μέθοδος για την απόκτηση μνήμης είναι μέσω άμεσης επαφής με το ύποπτο σύστημα. Αυτό επιτρέπει στους αναλυτές αντιμετώπισης περιστατικών να προσαρμόζονται σε περίπτωση που κάποιο εργαλείο ή τεχνική δεν λειτουργεί. Επίσης, η μέθοδος αυτή είναι ταχύτερη στην απόκτηση των απαραίτητων αρχείων, καθώς δεν εξαρτάται από σταθερή δικτυακή σύνδεση. Αν και είναι η προτιμώμενη μέθοδος, μπορεί να υπάρχουν γεωγραφικοί περιορισμοί, ειδικά σε μεγάλους οργανισμούς όπου οι αναλυτές βρίσκονται αρκετά μακριά (π.χ. απαιτείται πτήση για να φτάσουν στο σημείο με το αποδεικτικό υλικό).

Στην περίπτωση απομακρυσμένης απόκτησης, οι αναλυτές μπορούν να αξιοποιήσουν τα ίδια εργαλεία που χρησιμοποιούνται και στην τοπική απόκτηση. Η διαφορά είναι ότι απαιτείται η χρήση

απομακρυσμένης τεχνολογίας ώστε να έχουν πρόσβαση στα ύποπτα συστήματα και να εκτελέσουν τη συλλογή δεδομένων. Όπως με κάθε μέθοδο, οι αναλυτές πρέπει να καταγράφουν τη χρήση απομακρυσμένης τεχνολογίας, ώστε αργότερα να είναι δυνατός ο διαχωρισμός των νόμιμων από τις ύποπτες συνδέσεις.

WinPmem: Το WinPmem μπορεί να εγκατασταθεί σε απομακρυσμένα συστήματα μέσω εφαρμογών όπως το **Remote Desktop** ή το **PsExec**. Αφού εγκατασταθεί στο απομακρυσμένο σύστημα, η έξοδος του μπορεί να διοχετευθεί (ripped) σε άλλο σύστημα με τη χρήση του **NetCat**.

Παράδειγμα: Αν ο αναλυτής χρησιμοποιεί ένα σύστημα με διεύθυνση **192.168.0.56** και έχει πρόσβαση στο παραβιασμένο σύστημα μέσω PsExec ή RDS, μπορεί να δημιουργήσει μια σύνδεση με το NetCat πίσω στο δικό του μηχάνημα με την ακόλουθη εντολή:

```
C:/winpmem-2.1.exe - | nc 192.168.0.56 4455
```

Η παραπάνω εντολή λέει στο σύστημα να εκτελέσει τη συλλογή και να στείλει την έξοδο μέσω NetCat στον σταθμό εργασίας του αναλυτή στη θύρα 4455. Το μειονέκτημα αυτής της τεχνικής είναι ότι απαιτεί πρόσβαση στη Γραμμή Εντολών (Command Prompt), καθώς και την εγκατάσταση και των δύο εργαλείων (NetCat και WinPmem). Αυτό μπορεί να μην είναι η καλύτερη επιλογή αν το σύστημα θεωρείται ήδη παραβιασμένο.

5.10. Εικονικές Μηχανές (Virtual machines)

Οι αναλυτές πρέπει επίσης να είναι προετοιμασμένοι να εξετάσουν εικονικές μηχανές. Το σημαντικό πλεονέκτημα των εικονικών συστημάτων έναντι των φυσικών είναι η δυνατότητα διατήρησης της τρέχουσας κατάστασης είτε με τη λήψη **snapshot** είτε με την **παύση (pause)** του συστήματος. Έτσι, οι αναλυτές μπορούν απλώς να αντιγράψουν ολόκληρο το αρχείο σε ένα αποθηκευτικό μέσο (π.χ. USB) για μετέπειτα ανάλυση.

Συνίσταται να υπολογίζεται **hash** για κάθε αρχείο της εικονικής μηχανής πριν και μετά την αντιγραφή, ώστε να διασφαλιστεί η ακεραιότητα του αποδεικτικού υλικού.

Στο **VMware**, η εικονική μηχανή χρησιμοποιεί δύο βασικά αρχεία για τη μνήμη σε εκτέλεση:

- **VMEM:** Το αρχείο φυσικής μνήμης (RAM) της εικονικής μηχανής.
- **VMSS:** Το αρχείο που αποθηκεύει την κατάσταση του συστήματος σε λειτουργία **suspended**.

Για την απόκτηση της μνήμης:

1. Παύση (pause) του συστήματος.
2. Μεταφορά των αρχείων **VMSS** και **VMEM** σε φορητό μέσο (π.χ. USB).

- ο Το VMware περιλαμβάνει συνήθως το εργαλείο **Vmss2Core.exe**, το οποίο συνδυάζει τα δύο αρχεία σε ένα αρχείο **.dmp** για ανάλυση.

3. Εκτέλεση της εντολής

```
C:\Program Files (x86)\VMware\VMware Workstation>vmss2core.exe suspect.vmss suspect.vmem
```

Με αυτόν τον τρόπο δημιουργείται το απαραίτητο **.dmp** αρχείο για περαιτέρω ανάλυση.

5.11. Απόκτηση μη πτητικών δεδομένων (Acquiring non-volatile evidence)

Παρότι πολλά δεδομένα βρίσκονται στη μνήμη, είναι εξίσου σημαντική η απόκτηση του **σκληρού δίσκου** ενός πιθανώς παραβιασμένου συστήματος. Σε τέτοιες συσκευές υπάρχει πλούσιο αποδεικτικό υλικό, ακόμα και σε περιπτώσεις κακόβουλου λογισμικού ή εκμετάλλευσης. Το αποδεικτικό υλικό του δίσκου είναι ακόμα πιο κρίσιμο όταν πρόκειται για περιστατικά όπως εσωτερικές κακόβουλες ενέργειες ή απώλεια δεδομένων. Για να είναι αποδεκτό σε δικαστήριο, οι αναλυτές πρέπει να είναι εξοικειωμένοι με τις σωστές διαδικασίες απόκτησης.

Σε ορισμένες περιπτώσεις, είναι χρήσιμο να αποκτηθούν **δύο βασικά αρχεία** πριν το κλείσιμο του συστήματος:

- Τα **registry keys**
- Τα **event logs**

Αν και δεν είναι πτητικά δεδομένα, βοηθούν πολύ στην ανάλυση. Η απόκτησή τους μέσω πλήρους imaging εξαρτάται από τον χρόνο που απαιτείται για τη διαδικασία. Γι' αυτό, υπάρχουν τεχνικές για γρηγορότερη απόκτηση.

Παράδειγμα: Με πρόσβαση στο σύστημα, οι αναλυτές μπορούν να χρησιμοποιήσουν την παρακάτω εντολή για την εξαγωγή των αρχείων καταγραφής (logs):

```
C:\wevtutil ep1 <Log Type> E:\<FileName>.evtx
```

Αυτή η εντολή μπορεί να εκτελεστεί για τα **security**, **application**, και **system logs**. Επιπλέον, το **FTK Imager** επιτρέπει την απόκτηση **registry key settings** και άλλων πληροφοριών χρήσιμων στην ανάλυση:

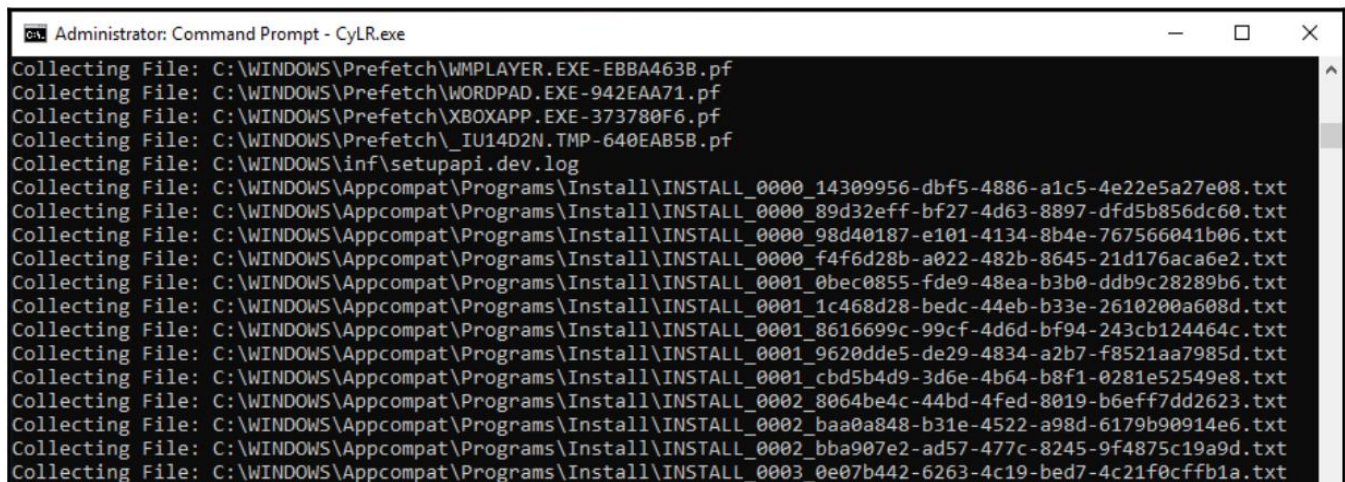
1. Άνοιγμα του FTK Imager και μετάβαση στην καρτέλα **File**.
2. Επιλογή **Obtain Protected Files**.
3. Επιλογή τοποθεσίας αποθήκευσης.
4. Επιλογή **Password recovery and all registry files** → OK.

Το εργαλείο αποθηκεύει τα αρχεία registry και τους κωδικούς στον φάκελο αποδεικτικών στοιχείων, συμπεριλαμβανομένων των: **user, system, SAM, NTUSER.DAT**. Έτσι, μπορεί να ξεκινήσει η ανάλυση πριν ολοκληρωθεί το imaging, επιταχύνοντας την απόκριση σε ένα περιστατικό.

CyLR.exe: Ένα εργαλείο ανοικτού κώδικα που βοηθά τους αναλυτές στην απόκτηση αυτού του είδους δεδομένων είναι η εφαρμογή **CyLR.exe**. Το αυτόνομο εκτελέσιμο, διαθέσιμο στο <https://github.com/orlikoski/CyLR/releases>, μπορεί να εκτελεστεί είτε από USB είτε απευθείας στο σύστημα. Πρόκειται για μια μικρή εφαρμογή, αλλά μπορεί να αποκτήσει μεγάλο όγκο αποδεικτικών στοιχείων που μπορούν να αξιοποιηθούν κατά το αρχικό στάδιο της διερεύνησης ή για σκοπούς **προτεραιοποίησης (triage)**. Ένα ακόμη βασικό χαρακτηριστικό του **CyLR.exe** είναι η δυνατότητά του να αποστέλλει τα αποκτηθέντα δεδομένα σε απομακρυσμένο σύστημα είτε για αποθήκευση είτε για περαιτέρω επεξεργασία.

Για την απόκτηση **μη πτητικών αρχείων καταγραφής (log files)** και άλλων προστατευμένων αρχείων, ο αναλυτής πρέπει να μεταβεί στο εκτελέσιμο **CyLR.exe** μέσω του Command Prompt και να το εκτελέσει ως **διαχειριστής (administrator)**. Ο φάκελος εξόδου που θα περιέχει τα αποδεικτικά στοιχεία θα δημιουργηθεί στον ίδιο φάκελο με το **CyLR.exe**. Αυτό είναι ιδιαίτερα χρήσιμο αν η εκτέλεση γίνεται από USB, καθώς η έξοδος θα αποθηκευτεί απευθείας στη συσκευή.

Κατά την εκτέλεση του **CyLR.exe**, ο αναλυτής θα μπορεί να βλέπει τα αρχεία που αποκτώνται ένα-ένα. Ανάλογα με τον επεξεργαστή και τη διαθέσιμη μνήμη RAM, το **CyLR.exe** αναμένεται να εκτελεστεί για μερικά λεπτά. Μετά την ολοκλήρωση, εμφανίζεται το αντίστοιχο μήνυμα επιτυχίας.



```
Administrator: Command Prompt - CyLR.exe
Collecting File: C:\WINDOWS\Prefetch\WMPLAYER.EXE-EBBA463B.pf
Collecting File: C:\WINDOWS\Prefetch\WORDPAD.EXE-942EAA71.pf
Collecting File: C:\WINDOWS\Prefetch\XBOXAPP.EXE-373780F6.pf
Collecting File: C:\WINDOWS\Prefetch\IU14D2N.TMP-640EAB5B.pf
Collecting File: C:\WINDOWS\inf\setupapi.dev.log
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0000_14309956-dbf5-4886-a1c5-4e22e5a27e08.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0000_89d32eff-bf27-4d63-8897-dfd5b856dc60.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0000_98d40187-e101-4134-8b4e-767566041b06.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0000_f4f6d28b-a022-482b-8645-21d176aca6e2.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0001_0bec0855-fde9-48ea-b3b0-ddb9c28289b6.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0001_1c468d28-bedc-44eb-b33e-2610200a608d.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0001_8616699c-99cf-4d6d-bf94-243cb124464c.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0001_9620dde5-de29-4834-a2b7-f8521aa7985d.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0001_cbd5b4d9-3d6e-4b64-b8f1-0281e52549e8.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0002_8064be4c-44bd-4fed-8019-b6eff7dd2623.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0002_baa0a848-b31e-4522-a98d-6179b90914e6.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0002_bba907e2-ad57-477c-8245-9f4875c19a9d.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0003_0e07b442-6263-4c19-bed7-4c21f0cfff1a.txt
```

Τέλος, ένας έλεγχος στον φάκελο από όπου εκτελέστηκε το **CyLR.exe** θα αποκαλύψει ένα **συμπίεσμένο αρχείο (compressed file)** με όνομα ίδιο με το όνομα του συστήματος. Αποσυμπιέζοντας το αρχείο, αποκαλύπτονται τα εκτενή αποδεικτικά στοιχεία που συλλέχθηκαν.

Η έξοδος περιλαμβάνει:

- αρχεία καταγραφής (log files),
- αρχεία μητρώου (registry files),

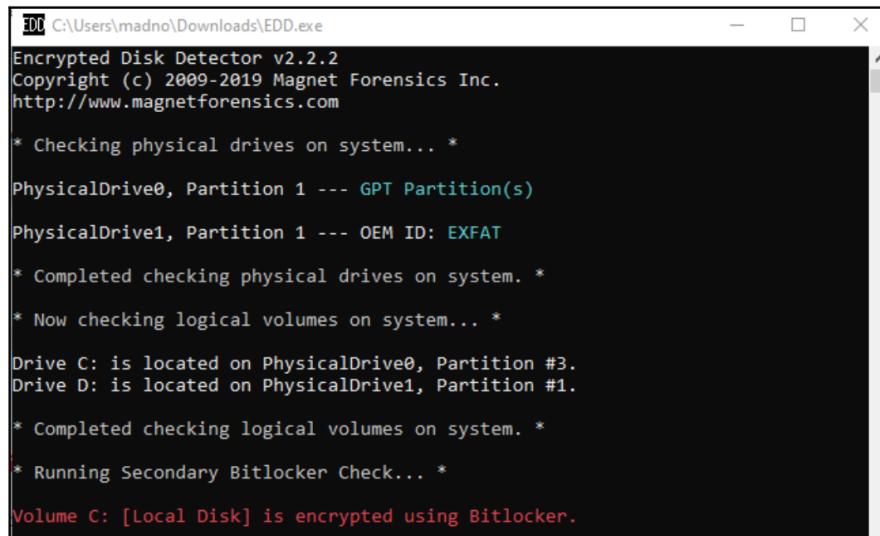
- τον **Master File Table (MFT)**.

Αυτά θα αποδειχθούν ιδιαίτερα σημαντικά σε επόμενα κεφάλαια. Η δυνατότητα απόκτησης όλων αυτών των δεδομένων μέσω ενός απλού εργαλείου αποτελεί σημαντικό πλεονέκτημα της χρήσης του **CyLR.exe** πριν την απενεργοποίηση ενός συστήματος.

5.12. Έλεγχος για κρυπτογράφηση

Ένας τομέας ανησυχίας για τους αναλυτές είναι η χρήση **πλήρους κρυπτογράφησης δίσκου (Full Disk Encryption – FDE)**. Οι διαχειριστές συστημάτων Windows είναι πιθανό να είναι εξοικειωμένοι με εργαλεία FDE όπως το **BitLocker**, το οποίο πλέον αποτελεί μέρος του λειτουργικού συστήματος Windows. Εκτός αυτού, υπάρχουν και άλλα εργαλεία, όπως το **VeraCrypt**, που επιτρέπουν την κρυπτογράφηση είτε μεμονωμένων αρχείων είτε ολόκληρων τόμων. Στο πλαίσιο της διαδικασίας απόκτησης, οι αναλυτές θα πρέπει να ελέγχουν για τυχόν κρυπτογράφηση.

Εργαλεία όπως το **Endpoint Disk Detector** της **Magnet Forensics** μπορούν να προσδιορίσουν εάν υπάρχουν κρυπτογραφημένοι τόμοι. Το εργαλείο αυτό, διαθέσιμο δωρεάν στο <https://www.magnetforensics.com/resources/encrypted-disk-detector/>, μπορεί να εντοπίσει ποια, αν υπάρχουν, μέτρα κρυπτογράφησης χρησιμοποιούνται. Αρκεί η εκτέλεση του εκτελέσιμου ως **διαχειριστής (administrator)** για να ξεκινήσει η εφαρμογή. Στη συνέχεια, εμφανίζονται τα παρακάτω δεδομένα:



```
Encrypted Disk Detector v2.2.2
Copyright (c) 2009-2019 Magnet Forensics Inc.
http://www.magnetforensics.com

* Checking physical drives on system... *
PhysicalDrive0, Partition 1 --- GPT Partition(s)
PhysicalDrive1, Partition 1 --- OEM ID: EXFAT
* Completed checking physical drives on system. *
* Now checking logical volumes on system... *
Drive C: is located on PhysicalDrive0, Partition #3.
Drive D: is located on PhysicalDrive1, Partition #1.
* Completed checking logical volumes on system. *
* Running Secondary Bitlocker Check... *
Volume C: [Local Disk] is encrypted using Bitlocker.
```

Με αυτόν τον τρόπο, ο αναλυτής μπορεί να διαπιστώσει, για παράδειγμα, ότι ο **τόμος C** είναι κρυπτογραφημένος με χρήση **BitLocker**. Ως επιπλέον έλεγχος, ο αναλυτής θα πρέπει να διασφαλίσει ότι το αντίστοιχο κλειδί BitLocker είναι διαθέσιμο, εφόσον χρειαστεί. Εάν δεν είναι δυνατόν να αποκτηθεί το κλειδί κρυπτογράφησης, τότε ο αναλυτής θα πρέπει να προχωρήσει στην απόκτηση του **λογικού τόμου** όσο το σύστημα παραμένει σε λειτουργία.

Η σωστή διαχείριση αποδεικτικών στοιχείων αποτελεί την απαρχή της συνολικής διαδικασίας που στοχεύει στον καθορισμό της **ρίζας ενός περιστατικού** και, ενδεχομένως, στον εντοπισμό του υπεύθυνου. Για να έχει αξία το αποδεικτικό υλικό σε μια έρευνα περιστατικού, πρέπει να αποκτηθεί με **ορθό και αξιόπιστο τρόπο**. Οι **αναλυτές περιστατικών** θα πρέπει να διαθέτουν ισχυρή βάση κατανόησης σχετικά με τους διάφορους τύπους απόκτησης, καθώς και τα εργαλεία και τις τεχνικές που είναι διαθέσιμα, και να εφαρμόζουν αυτά τα εργαλεία και τις τεχνικές στις διαφορετικές καταστάσεις που μπορεί να προκύψουν. Με την εφαρμογή ορθών τεχνικών και την **κατάλληλη τεκμηρίωση** των ενεργειών τους, οι αναλυτές περιστατικών θα βρίσκονται σε θέση να αξιοποιήσουν το αποδεικτικό υλικό όχι μόνο για να καθορίσουν τη **βασική αιτία** ενός περιστατικού, αλλά και για να στηρίξουν τις ενέργειές τους σε μια **δικαστική διαδικασία**, εφόσον αυτό απαιτηθεί.

5.13. Εγκληματολογική Εικόνα (Forensic Imaging)

Μία κρίσιμη εργασία που συχνά καλούνται να εκτελέσουν οι αναλυτές αντιμετώπισης περιστατικών είναι η **δημιουργία εγκληματολογικής εικόνας** (imaging) αποδεικτικών στοιχείων. Όπως αναφέρθηκε σε προηγούμενα κεφάλαια, μεγάλο μέρος στοιχείων που σχετίζονται με ένα περιστατικό μπορεί να βρεθεί μέσα σε **αρχεία καταγραφής (logs)**, **μνήμη** και σε άλλες περιοχές που μπορούν να αποκτηθούν σχετικά γρήγορα.

Ωστόσο, σε ορισμένα περιστατικά, όπως σε περιπτώσεις **κακόβουλης εσωτερικής δραστηριότητας** (π.χ. απάτη, βιομηχανική κατασκοπεία ή διαρροή δεδομένων), μπορεί να απαιτείται πιο λεπτομερής αναζήτηση αποδεικτικών στοιχείων. Αυτά περιλαμβάνουν **καταχωρίσεις στον Master File Table (MFT)**, **αρχεία**, καθώς και **συγκεκριμένα δεδομένα χρήστη** που βρίσκονται στον σκληρό δίσκο ενός υποππου συστήματος. Σε τέτοιες περιπτώσεις, οι αναλυτές καλούνται να αποκτήσουν **εικόνα του δίσκου**.

Όπως σε κάθε πτυχή της ψηφιακής εγκληματολογίας, η απόκτηση μίας χρήσιμης και **νομικά αποδεκτής εικόνας** εξαρτάται από τη χρήση κατάλληλων εργαλείων, τεχνικών και τεκμηρίωσης.

Αυτό το κεφάλαιο εξερευνά τις θεμελιώδεις έννοιες της **ψηφιακής απεικόνισης** (digital imaging), την προετοιμασία και τα εργαλεία που απαιτούνται για την απόκτηση μίας εγκληματολογικά αξιόπιστης εικόνας ενός **φυσικού δίσκου** ή άλλου **λογικού τόμου**. Συγκεκριμένα, καλύπτονται τα εξής θέματα:

- **Κατανόηση της ψηφιακής απεικόνισης:** Η απεικόνιση μιας συσκευής αποθήκευσης είναι διαδικασία όπου οι λεπτομέρειες έχουν σημασία. Εξετάζονται οι βασικές αρχές, οι διαφορετικοί τύποι διαδικασιών απεικόνισης και οι ιδιόκτητοι τύποι αρχείων.
- **Εργαλεία απεικόνισης:** Υπάρχουν πολλά διαθέσιμα εργαλεία για τους αναλυτές. Η κατανόηση αυτών επιτρέπει την επιλογή του κατάλληλου εργαλείου ανά περιστατικό.
- **Προετοιμασία δίσκου-σκηνής (stage drive):** Εξίσου σημαντικό με τον χειρισμό του αποδεικτικού δίσκου είναι η ύπαρξη ενός **εγκληματολογικά καθαρού δίσκου** στον οποίο θα μεταφερθεί η εικόνα.

- **Αποκλειστές εγγραφής (Write blockers):** Απαραίτητα εργαλεία που διασφαλίζουν ότι το αποδεικτικό στοιχείο δεν αλλοιώνεται κατά την απεικόνιση. Εξετάζονται τόσο υλικοί (hardware) όσο και λογισμικοί (software) αποκλειστές.
- **Τεχνικές απεικόνισης:** Το βασικό μέρος του κεφαλαίου επικεντρώνεται στις διαθέσιμες τεχνικές για τη δημιουργία εικόνας αποδεικτικών δίσκων.

Παρότι το κεφάλαιο περιέχει τεχνικό και διαδικαστικό υλικό, είναι κρίσιμο οι αναλυτές να κατανοούν την απεικόνιση, καθώς αυτή αποτελεί θεμέλιο για **ανάλυση αιτίων** και πιθανή χρήση σε **δικαστικό πλαίσιο**.

6

Εγκληματολογική απεικόνιση

Μία κρίσιμη εργασία που συχνά καλούνται να εκτελέσουν οι αναλυτές αντιμετώπισης περιστατικών είναι η δημιουργία **εγκληματολογικής εικόνας** (imaging) αποδεικτικών στοιχείων. Όπως αναφέρθηκε σε προηγούμενα κεφάλαια, μεγάλο μέρος στοιχείων που σχετίζονται με ένα περιστατικό μπορεί να βρεθεί μέσα σε **αρχεία καταγραφής (logs)**, **μνήμη** και σε άλλες περιοχές που μπορούν να αποκτηθούν σχετικά γρήγορα.

Ωστόσο, σε ορισμένα περιστατικά, όπως σε περιπτώσεις **κακόβουλης εσωτερικής δραστηριότητας** (π.χ. απάτη, βιομηχανική κατασκοπεία ή διαρροή δεδομένων), μπορεί να απαιτείται πιο λεπτομερής αναζήτηση αποδεικτικών στοιχείων. Αυτά περιλαμβάνουν **καταχωρίσεις στον Master File Table (MFT)**, **αρχεία**, καθώς και **συγκεκριμένα δεδομένα χρήστη** που βρίσκονται στον σκληρό δίσκο ενός ύποπτου συστήματος. Σε τέτοιες περιπτώσεις, οι αναλυτές καλούνται να αποκτήσουν **εικόνα του δίσκου**.

Όπως σε κάθε πτυχή της ψηφιακής εγκληματολογίας, η απόκτηση μίας χρήσιμης και **νομικά αποδεκτής εικόνας** εξαρτάται από τη χρήση κατάλληλων εργαλείων, τεχνικών και τεκμηρίωσης.

Αυτό το κεφάλαιο εξερευνά τις θεμελιώδεις έννοιες της **ψηφιακής απεικόνισης** (digital imaging), την προετοιμασία και τα εργαλεία που απαιτούνται για την απόκτηση μίας εγκληματολογικά αξιόπιστης εικόνας ενός **φυσικού δίσκου** ή άλλου **λογικού τόμου**. Συγκεκριμένα, καλύπτονται τα εξής θέματα:

- **Κατανόηση της ψηφιακής απεικόνισης:** Η απεικόνιση μιας συσκευής αποθήκευσης είναι διαδικασία όπου οι λεπτομέρειες έχουν σημασία. Εξετάζονται οι βασικές αρχές, οι διαφορετικοί τύποι διαδικασιών απεικόνισης και οι ιδιόκτητοι τύποι αρχείων.
- **Εργαλεία απεικόνισης:** Υπάρχουν πολλά διαθέσιμα εργαλεία για τους αναλυτές. Η κατανόηση αυτών επιτρέπει την επιλογή του κατάλληλου εργαλείου ανά περιστατικό.
- **Προετοιμασία δίσκου-σκηνής (stage drive):** Εξίσου σημαντικό με τον χειρισμό του αποδεικτικού δίσκου είναι η ύπαρξη ενός **εγκληματολογικά καθαρού δίσκου** στον οποίο θα μεταφερθεί η εικόνα.
- **Αποκλειστές εγγραφής (Write blockers):** Απαραίτητα εργαλεία που διασφαλίζουν ότι το αποδεικτικό στοιχείο δεν αλλοιώνεται κατά την απεικόνιση. Εξετάζονται τόσο υλικοί (hardware) όσο και λογισμικοί (software) αποκλειστές.

- **Τεχνικές απεικόνισης:** Το βασικό μέρος του κεφαλαίου επικεντρώνεται στις διαθέσιμες τεχνικές για τη δημιουργία εικόνας αποδεικτικών δίσκων.

Παρότι το κεφάλαιο περιέχει τεχνικό και διαδικαστικό υλικό, είναι κρίσιμο οι αναλυτές να κατανοούν την απεικόνιση, καθώς αυτή αποτελεί θεμέλιο για **ανάλυση αιτίων** και πιθανή χρήση σε **δικαστικό πλαίσιο**.

Η κατανόηση των πτυχών της εγκληματολογικής απεικόνισης είναι σημαντική για τους αναλυτές περιστατικών. Η γνώση των εργαλείων, τεχνικών και διαδικασιών διασφαλίζει ότι το αποδεικτικό υλικό χειρίζεται σωστά και ότι οι αναλυτές έχουν εμπιστοσύνη στα στοιχεία που απέκτησαν. Επιπλέον, η κατανόηση της ορολογίας επιτρέπει την ακριβή σύνταξη αναφορών και την **κατάθεση σε δικαστήριο** εάν χρειαστεί.

Ένα από τα πρώτα σημεία που πρέπει να γίνει κατανοητό είναι η **διαφορά μεταξύ απεικόνισης (imaging) και απλής αντιγραφής (copying)**:

- Η **αντιγραφή** αρχείων από έναν ύποπτο δίσκο παρέχει μόνο τα δεδομένα του αρχείου.
- Η **απεικόνιση** καταγράφει **ολόκληρο τον δίσκο**, περιλαμβάνοντας περιοχές όπως το **slack space**, **unallocated space** και ενδεχομένως αρχεία που έχουν διαγραφεί. Επίσης, διατηρεί **μεταδεδομένα** (π.χ. χρονικές σημάνσεις αρχείων), κάτι που είναι κρίσιμο σε αναλύσεις χρονογραμμής (timeline analysis).

Συχνά, οι όροι **cloning** και **imaging** χρησιμοποιούνται λανθασμένα ως συνώνυμα στην πληροφορική.

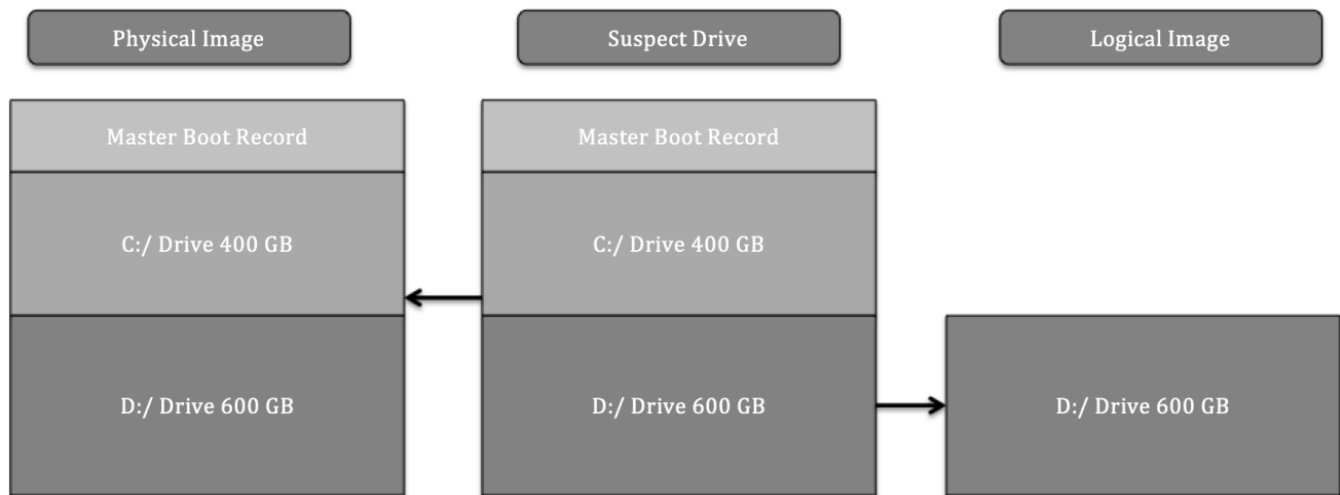
- Το **cloning** είναι **1:1 αντιγραφή** δίσκου που μπορεί να χρησιμοποιηθεί απευθείας για εκκίνηση συστήματος, κυρίως για δημιουργία λειτουργικού αντιγράφου ασφαλείας.
- Η **απεικόνιση** δημιουργεί ένα **αρχείο εικόνας** που περιέχει όλα τα δεδομένα και είναι πιο πρακτική για ανάλυση με εγκληματολογικά εργαλεία.

Το δεύτερο σημείο που πρέπει να γίνει κατανοητό είναι οι **τύποι τόμων** που μπορούν να απεικονιστούν:

- **Φυσικοί τόμοι (physical volumes):** περιλαμβάνουν ολόκληρο τον σκληρό δίσκο, όλες τις κατατμήσεις και το master boot record.
- **Λογικοί τόμοι (logical volumes):** αποτελούν τμήμα του σκληρού δίσκου (π.χ. ένας συγκεκριμένος partition όπως το D drive). Στην απεικόνιση ενός λογικού τόμου, καταγράφονται μόνο τα δεδομένα που περιέχονται σε αυτόν.

Το παρακάτω διάγραμμα απεικονίζει δεδομένα που καταγράφονται κατά την απεικόνιση είτε ενός φυσικού είτε ενός λογικού τόμου. Ο τύπος του περιστατικού που ερευνάται καθορίζει σε μεγάλο βαθμό τον τύπο της απεικόνισης που θα πραγματοποιηθεί. Για παράδειγμα, αν ένας αναλυτής είναι σε θέση να εντοπίσει ένα ενδεχομένως κακόβουλο αρχείο που εκτελείται από τον δίσκο D και επιθυμεί να αποτυπώσει μόνο αυτά τα δεδομένα, μπορεί να είναι ταχύτερο να αποκτήσει μια λογική εικόνα μόνο αυτού του τόμου. Επιπλέον, η λογική απόκτηση μπορεί να είναι αναγκαία σε περιπτώσεις όπου

χρησιμοποιείται Κρυπτογράφηση Δίσκου (Full Disk Encryption – FDE). Χωρίς το κλειδί κρυπτογράφησης, η λογική απόκτηση αρχείων ενώ το σύστημα είναι ενεργό είναι συχνά η μόνη διαθέσιμη επιλογή.



Το βασικό μειονέκτημα μιας λογικής εικόνας είναι ότι δεν θα καταγράψει μη εκχωρημένα δεδομένα ή δεδομένα που δεν αποτελούν μέρος του συστήματος αρχείων. Διαγραμμένα αρχεία και άλλα ίχνη δεν θα συμπεριλαμβάνονται στη λογική εικόνα. Σε περιπτώσεις όπου υπάρχουν υποψίες για δραστηριότητες όπως παραπτώματα εργαζομένων, ο αναλυτής θα χρειαστεί να ιχνηλατήσει όσο το δυνατόν περισσότερη δραστηριότητα, οπότε θα πραγματοποιηθεί πλήρης απεικόνιση του φυσικού τόμου. Εδώ ο χρόνος δεν αποτελεί απαραίτητο παράγοντα.

Στο Κεφάλαιο 4, με την *Συλλογή Αποδείξεων Δικτύου*, συζητήθηκε η απόκτηση αποδεικτικών στοιχείων, όπως αρχείων καταγραφής και ενεργής μνήμης, από ένα σύστημα που βρίσκεται σε λειτουργία. Με παρόμοιο τρόπο, οι αναλυτές αντιμετώπισης περιστατικών έχουν τη δυνατότητα να αποκτήσουν έναν λογικό τόμο από ένα σύστημα που λειτουργεί. Αυτή η τεχνική αναφέρεται ως *ζωντανή απεικόνιση* (live imaging). Η ζωντανή απεικόνιση μπορεί να είναι η καλύτερη επιλογή εάν ένα πιθανώς παραβιασμένο σύστημα δεν μπορεί να τεθεί εκτός λειτουργίας, όπως συμβαίνει σε έναν εξυπηρετητή υψηλής διαθεσιμότητας, και τα πιθανά αποδεικτικά στοιχεία βρίσκονται μέσα σε έναν λογικό τόμο.

Η *νεκρή απεικόνιση* (dead imaging) εκτελείται σε ένα σύστημα που έχει απενεργοποιηθεί και του οποίου ο σκληρός δίσκος έχει αφαιρεθεί. Σε αυτόν τον τύπο απεικόνισης, ο αναλυτής είναι σε θέση να καταγράψει ολόκληρο τον δίσκο, συμπεριλαμβανομένων όλων των τόμων και του master boot record. Αυτό μπορεί να καταστεί αναγκαίο σε περιστατικά όπου οι αναλυτές θέλουν να διασφαλίσουν ότι θα αποτυπωθεί το σύνολο των πρωτογενών αποδεικτικών στοιχείων, ώστε να μην υπάρχει τμήμα που να μην έχει εξεταστεί.

Ένα τελευταίο στοιχείο της εγκληματολογικής απεικόνισης που πρέπει να γνωρίζει ο αναλυτής είναι οι τύποι αρχείων εικόνας που μπορούν να δημιουργηθούν και να αξιοποιηθούν κατά τη διάρκεια μιας έρευνας. Υπάρχουν αρκετοί τύποι αρχείων εικόνας, μερικοί εκ των οποίων είναι εξειδικευμένοι, αλλά

για τους σκοπούς του παρόντος βιβλίου θα επικεντρωθούμε στους δύο πιο κοινούς τύπους αρχείων αποδεικτικών στοιχείων με τους οποίους είναι πιθανότερο να εργαστούν οι αναλυτές:

- **Ακατέργαστες εικόνες (Raw images):** Ένα αρχείο ακατέργαστης εικόνας περιέχει μόνο τα δεδομένα από τον απεικονισμένο τόμο. Δεν παρέχονται πρόσθετα δεδομένα σε αυτόν τον τύπο εικόνας, αν και κάποια εργαλεία απεικόνισης, όπως το FTK Imager, περιλαμβάνουν ξεχωριστό αρχείο με πληροφορίες απεικόνισης. Οι μορφές εξόδου ακατέργαστης εικόνας περιλαμβάνουν τις επεκτάσεις .raw, .img και .dd. Λογισμικό όπως η εντολή *dd* στο Linux προσφέρει ευελιξία όταν η ταχύτητα και η συμβατότητα με εργαλεία εγκληματολογικής ανάλυσης είναι κρίσιμο ζήτημα.
- **Αρχεία αποδεικτικών στοιχείων EnCase:** Το αρχείο αποδεικτικών στοιχείων EnCase (E01 ή EX01) είναι μια ιδιόκτητη μορφή αρχείου που αναπτύχθηκε από την OpenText ως μέρος των εργαλείων EnCase το 1998. Η μορφή αυτή βασίστηκε στο *Expert Witness Format (EWF)*, που συναντάται στη μορφή συμπίεσης Expert Witness της ASR Data. Το αρχείο E01 περιέχει μεταδεδομένα για την εικόνα. Τα μεταδεδομένα που βρίσκονται τόσο στην κεφαλίδα όσο και στο υποσέλιδο καταγράφουν και αποθηκεύουν πληροφορίες σχετικά με τον τύπο του δίσκου, το λειτουργικό σύστημα και τις χρονικές σημάνσεις. Ένα άλλο βασικό χαρακτηριστικό του αρχείου E01 είναι η συμπερίληψη ενός *Cyclical Redundancy Check (CRC)*. Το CRC αυτό αποτελεί έναν μηχανισμό επαλήθευσης ακεραιότητας αρχείων, που εκτελείται μετά από κάθε 64 KB δεδομένων που γράφονται στο αρχείο εικόνας. Αυτό διασφαλίζει την ακεραιότητα του προηγούμενου τμήματος δεδομένων σε όλο το αρχείο εικόνας. Τέλος, το αρχείο E01 περιέχει το hash MD5 στο υποσέλιδο του αρχείου.

File Header	64 KB Data	CRC	64 KB Data	CRC	64 KB Data	CRC	64 KB Data	CRC	MD5
-------------	------------	-----	------------	-----	------------	-----	------------	-----	-----

Ένα αρχείο E01 προτιμάται από τις αρχές επιβολής του νόμου και τις νομικές οντότητες καθώς συνδυάζει την ικανότητα επαλήθευσης της ακεραιότητας των αποδεικτικών στοιχείων με δυνατότητες λογισμικού, όπως η συμπίεση. Επίσης, το E01 υποστηρίζεται από πληθώρα εργαλείων εγκληματολογικής ανάλυσης.

Οι πληροφορίες που παρουσιάστηκαν εδώ αποτελούν μια γενική επισκόπηση κάποιων βασικών εννοιών της απεικόνισης. Ως εκ τούτου, υπάρχουν πολλές λεπτομέρειες σχετικά με την εγκληματολογική απεικόνιση που δεν μπόρεσαν να συμπεριληφθούν στο βιβλίο. Μια λεπτομερής κατανόηση της εγκληματολογικής απεικόνισης θα επιτρέψει σε έναν αναλυτή αντιμετώπισης περιστατικών να ετοιμάσει μια ακριβή αναφορά, ενώ ταυτόχρονα θα είναι σε θέση να περιγράψει με ποιον τρόπο οι ενέργειές του παρήγαγαν τα αποτελέσματα που αποτέλεσαν τη βάση της ανάλυσής του.

Παρόλο που το βιβλίο εστιάζει στις μορφές αρχείων RAW και EnCase, υπάρχουν και δύο άλλες κοινές μορφές αρχείων που οι αναλυτές μπορεί να συναντήσουν, ιδιαίτερα όταν συνεργάζονται με άλλους οργανισμούς:

- **Advanced Forensic File Format (AFF4):** Η μορφή αρχείου εικόνας AFF4 είναι ένα έργο ανοιχτού κώδικα που αναπτύχθηκε για την αποθήκευση ψηφιακών αποδεικτικών στοιχείων και άλλων δεδομένων. Η μορφή αυτή χρησιμοποιείται κυρίως με το εργαλείο απόκτησης πτητικής μνήμης *Pmem*.
- **Access Data Evidence File (AD1):** Στην περίπτωση αυτή, ο κάτοχος της σουίτας εργαλείων *Forensic Tool Kit (FTK)* χρησιμοποιεί το AD1 ως ιδιόκτητο αρχείο αποδεικτικών στοιχείων.

Με την κάλυψη της γενικής έννοιας της εγκληματολογικής απεικόνισης, το επόμενο βήμα είναι η εξέταση των διαθέσιμων εργαλείων για την απόκτηση μιας εγκληματολογικά έγκυρης εικόνας.

6.1. Εργαλεία Απεικόνισης (Imaging tools)

Αν και δεν υπάρχει κάποιο δικαστήριο ή νομικό σώμα που να πιστοποιεί τα εργαλεία απεικόνισης της ψηφιακής εγκληματολογίας, υπάρχουν αρκετές μέθοδοι και σχετικά εργαλεία που θεωρούνται βέλτιστες πρακτικές κατά την απόκτηση αποδεικτικών στοιχείων από δίσκους. Ας τα δούμε:

FTK Imager: Το FTK Imager παρέχεται δωρεάν από την Access Data. Πρόκειται για μια εφαρμογή με γραφικό περιβάλλον (GUI) που επιτρέπει την εγκληματολογικά ορθή απόκτηση λογικών και φυσικών τόμων, μνήμης και άλλων προστατευμένων αρχείων, εξάγοντας τα σε διάφορα μορφή. Επιπλέον, το FTK Imager Lite είναι μια αυτόνομη εφαρμογή που μπορεί να τρέξει από αφαιρούμενο μέσο για την απόκτηση ψηφιακών αποδεικτικών στοιχείων από συστήματα που βρίσκονται σε λειτουργία (αυτό θα αναλυθεί λεπτομερώς αργότερα στο κεφάλαιο).

EnCase Imager: Παρέχεται από την Guidance Software και αποτελεί ένα ακόμα εγκληματολογικό εργαλείο που επιτρέπει στους αναλυτές να αποκτούν ψηφιακά αποδεικτικά στοιχεία από ποικιλία συστημάτων. Παρόμοια με το FTK Imager, το EnCase Imager μπορεί επίσης να εκτελείται από εξωτερικό δίσκο για την απόκτηση δεδομένων από ενεργά συστήματα.

AFF4 Imager: Το AFF4 Imager είναι ένα εκτελέσιμο εργαλείο γραμμής εντολών που αποτελεί τη βάση για εργαλεία όπως το WinPmem. Μπορεί να χρησιμοποιηθεί για την απόκτηση λογικών και φυσικών δίσκων, παρόμοια με τα EnCase ή FTK Imager. Ένα πλεονέκτημα του AFF4 Imager είναι ότι μπορεί να απομονώνει αρχεία με βάση τον χρόνο δημιουργίας και να διαχωρίζει τόμους, μειώνοντας έτσι τον χρόνο απεικόνισης με χρήση συμπίεσης.

dd: Ένα κλασικό εργαλείο του Linux. Σε ορισμένες περιπτώσεις, η εντολή dd του Linux, η οποία χρησιμοποιείται για την αντιγραφή αρχείων και τόμων, μπορεί να χρησιμοποιηθεί και για την απεικόνιση δίσκων ή τόμων. Οι αναλυτές πιθανότατα θα χρησιμοποιήσουν την dd σε πλατφόρμες εγκληματολογίας βασισμένες σε Linux για την απόκτηση αποδεικτικών στοιχείων.

Εργαλεία Εικονικοποίησης (Virtualization tools): Με την ευρεία χρήση της εικονικοποίησης, είναι πιθανό οι αναλυτές να χρειαστεί να αποκτήσουν τουλάχιστον μέρος των αποδεικτικών στοιχείων από εικονικά συστήματα. Αυτό παρουσιάζει πλεονέκτημα, καθώς ολόκληρο το σύστημα μπορεί να εξαχθεί

για ανάλυση. Ανάλογα με το λογισμικό εικονικοποίησης, η απόκτηση μπορεί να επιτευχθεί με παύση του συστήματος και εξαγωγή ολόκληρου του φακέλου που το περιέχει. Αυτό μπορεί επίσης να πραγματοποιηθεί μέσω της λειτουργίας snapshot που προσφέρουν πολλές πλατφόρμες εικονικοποίησης.

Η επιλογή του εργαλείου απεικόνισης εξαρτάται από τον οργανισμό, την εκπαίδευση και την εμπειρία του αναλυτή, καθώς και από τα υπόλοιπα εγκληματολογικά εργαλεία που χρησιμοποιούνται. Για παράδειγμα, αν ένας οργανισμός χρησιμοποιεί το Forensic Tool Kit για ανάλυση, είναι καλύτερο να χρησιμοποιείται το FTK Imager ως μέρος της διαδικασίας.

Με οποιοδήποτε εργαλείο απεικόνισης, είναι καλή πρακτική να εξασφαλίζεται ότι το εργαλείο λειτουργεί σωστά και ότι οι αναλυτές έχουν εκπαιδευτεί επαρκώς στη χρήση του.

Μόλις επιλεγεί το εργαλείο, το επόμενο βήμα είναι να διασφαλιστεί ότι το υπόλοιπο υλικό είναι έτοιμο. Αυτό περιλαμβάνει και την ορθή προετοιμασία του μέσου προορισμού όπου θα αποθηκευτεί η απεικόνιση.

6.2. Προετοιμασία δίσκου αποθήκευσης (stage drive)

Πέρα από την κατοχή του απαραίτητου υλικού και λογισμικού για την εκτέλεση μιας δικανικής απεικόνισης (forensic imaging), είναι κρίσιμο να προετοιμαστεί εκ των προτέρων μια τοποθεσία για την αποθήκευση της εικόνας ή του αρχείου αποδεικτικού υλικού. Για τις ομάδες απόκρισης σε περιστατικά, η καλύτερη επιλογή για αποθήκευση αποδεικτικών στοιχείων είναι ένας εξωτερικός δίσκος USB ή FireWire. Αυτό παρέχει ένα βαθμό φορητότητας, καθώς οι αναλυτές ενδέχεται να χρειαστεί να διερευνήσουν ένα περιστατικό εκτός έδρας ή σε διαφορετικές τοποθεσίες χωρίς την υποδομή ενός εργαστηρίου ψηφιακής εγκληματολογίας.

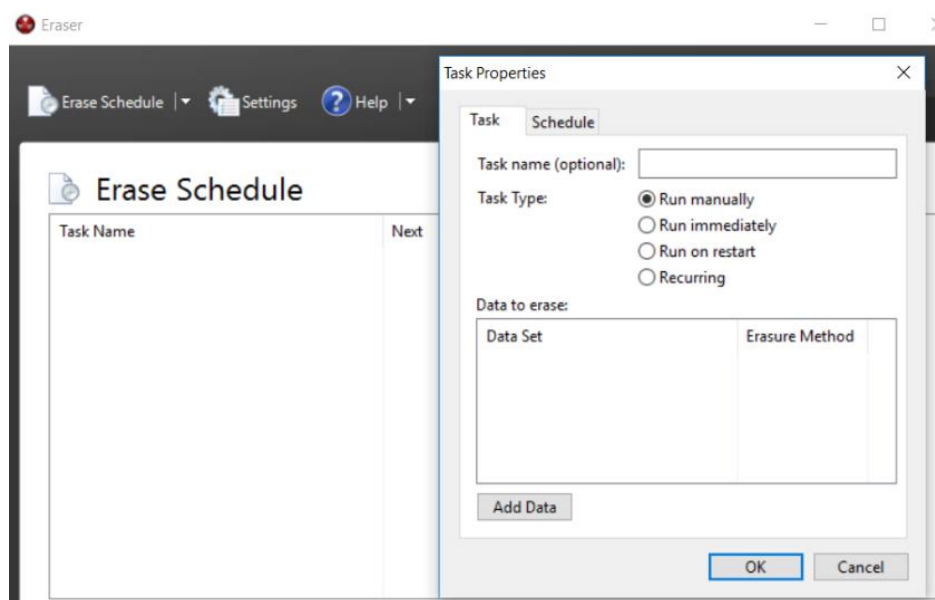
Υπάρχουν δύο εργασίες που πρέπει να εκτελούνται στους δίσκους αποδεικτικών στοιχείων πριν από τη χρήση τους. Η πρώτη είναι η διασφάλιση ότι το αποθετήριο δεν περιέχει δεδομένα. Οι ομάδες αντιμετώπισης περιστατικών πρέπει να διαθέτουν πολιτική και διαδικασία που να επιβάλλουν τον καθαρισμό (wipe) ενός δίσκου αποδεικτικών στοιχείων πριν από κάθε χρήση. Αυτό ισχύει ακόμη και για καινούργιους δίσκους στη συσκευασία τους, καθώς αρκετοί κατασκευαστές αποστέλλουν δίσκους με προεγκατεστημένο λογισμικό δημιουργίας αντιγράφων ασφαλείας ή άλλα δεδομένα που πρέπει να αφαιρεθούν πριν από τη χρήση. Ο καθαρισμός εξασφαλίζει επίσης ότι δίσκοι που έχουν χρησιμοποιηθεί ξανά δεν περιέχουν ίχνη δεδομένων από άλλο περιστατικό. Με αυτόν τον τρόπο διασφαλίζεται ότι τα συλλεγμένα αποδεικτικά στοιχεία σε έναν σωστά καθαρισμένο δίσκο δεν θα επιμολυνθούν με άσχετα δεδομένα.

Η διαδικασία αυτή μπορεί να πραγματοποιηθεί εύκολα με τη χρήση ενός προγράμματος καθαρισμού. Υπάρχει πληθώρα δωρεάν και εμπορικών εργαλείων που μπορούν να χρησιμοποιηθούν. Για παράδειγμα, το πρόγραμμα **Eraser** της Heidi Computers αποτελεί μια δωρεάν εφαρμογή που

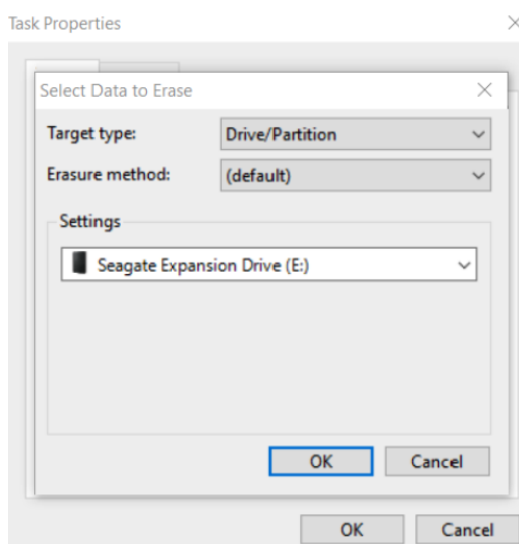
υποστηρίζει καθαρισμό τόσο σε αρχεία όσο και σε ολόκληρους τόμους (διαθέσιμο στο <https://eraser.heidi.ie/>).

Παράδειγμα: Σε αυτήν την περίπτωση, ένας εξωτερικός σκληρός δίσκος 2 TB θα διαγραφεί και θα προετοιμαστεί για χρήση ως δίσκος αποδεικτικών στοιχείων. Η παρακάτω ακολουθία βημάτων πρέπει να επαναλαμβάνεται κάθε φορά που ένας δίσκος πρόκειται να τεθεί σε κατάσταση κατάλληλη για εγκληματολογική διερεύνηση:

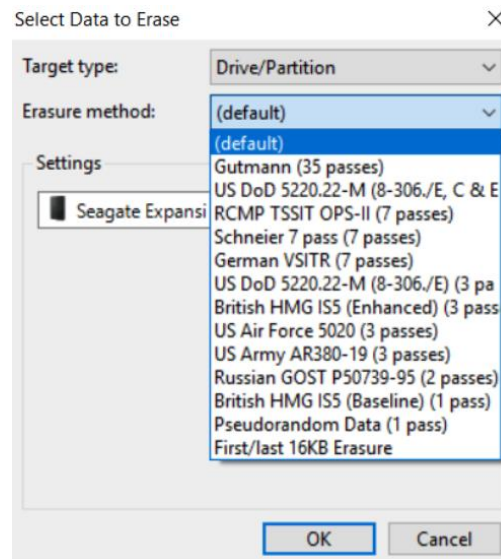
1. Εκκινήστε την εφαρμογή **Eraser**. Στο γραφικό περιβάλλον, επιλέξτε *Erase Schedule* και στη συνέχεια *New Task*.



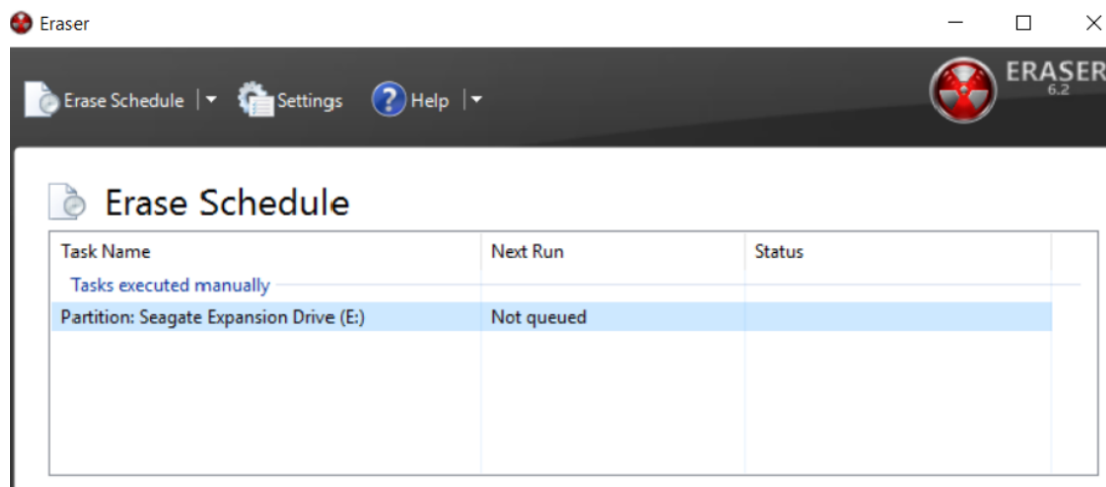
2. Ορίστε ένα όνομα για το έργο. Αυτό βοηθά στην κατάλληλη τεκμηρίωση της διαγραφής του δίσκου αποδεικτικών στοιχείων. Επιλέξτε το κουμπί *Add Data*. Θα ανοίξει νέο παράθυρο.



3. Στο πεδίο *Target type*, επιλέξτε *Drive/Partition*. Στην περιοχή *Settings* θα εμφανιστεί μια λίστα με κατατμήσεις και γράμματα δίσκου. Δώστε ιδιαίτερη προσοχή στα γράμματα δίσκου και βεβαιωθείτε ότι έχει επιλεγεί ο σωστός εξωτερικός δίσκος που πρέπει να καθαριστεί. Σε αυτό το παράδειγμα, χρησιμοποιείται ένας νέος εξωτερικός δίσκος Seagate. Στη συνέχεια, επιλέξτε μια μέθοδο διαγραφής. Υπάρχουν αρκετές διαθέσιμες επιλογές· εδώ επιλέγεται η μέθοδος **US DoD 5220.22-M (8-306./E) (3 Pass)**.



4. Κάντε κλικ στο *OK*. Η εργασία διαγραφής θα εμφανιστεί στο *Erase Schedule*.



5. Κάντε δεξί κλικ στην εργασία (*Partition: Seagate Expansion Drive (E:)*) και επιλέξτε *Run Now*. Αυτό θα ξεκινήσει τη διαδικασία διαγραφής. Όπως αναφέρθηκε, είναι κρίσιμο να διασφαλιστεί ότι καθαρίζεται ο σωστός δίσκος αποδεικτικών στοιχείων.

Ανάλογα με το μέγεθος του δίσκου και το σύστημα που εκτελεί τον καθαρισμό, η διαδικασία μπορεί να διαρκέσει ώρες ή ακόμη και ημέρες. Μόλις ολοκληρωθεί, ο αναλυτής περιστατικών πρέπει να καταγράψει τα στοιχεία που πιστοποιούν ότι ο δίσκος αποδεικτικών στοιχείων καθαρίστηκε σωστά.

Αυτές οι πληροφορίες είναι σημαντικές για την ένταξή τους σε μια γραπτή εγκληματολογική αναφορά, καθώς αποδεικνύουν ότι ελήφθησαν τα κατάλληλα μέτρα ώστε τα αποδεικτικά αρχεία να είναι απαλλαγμένα από αλλοιώσεις ή ανάμειξη με ξένα δεδομένα.

Συνιστάται οι αναλυτές περιστατικών να διαθέτουν αρκετούς δίσκους έτοιμους και προκαθαρισμένους πριν από οποιοδήποτε περιστατικό. Έτσι, μπορούν να χρησιμοποιήσουν άμεσα έναν καθαρισμένο δίσκο αντί να σπαταλούν χρόνο για καθαρισμό επί τόπου, χρόνος που είναι πιο χρήσιμος για δραστηριότητες σχετικές με το περιστατικό.

Μια δεύτερη προετοιμασία που μπορεί να πραγματοποιηθεί είναι η **κρυπτογράφηση του δίσκου αποδεικτικών στοιχείων**. Λογισμικά όπως το **VeraCrypt** ή άλλες πλατφόρμες κρυπτογράφησης μπορούν να χρησιμοποιηθούν για την κρυπτογράφηση της κατάτμησης που περιέχει τα αρχεία αποδεικτικών στοιχείων. Οι αναλυτές περιστατικών που χειρίζονται εμπιστευτικές πληροφορίες, όπως στοιχεία πιστωτικών καρτών ή ιατρικά δεδομένα, πρέπει να κρυπτογραφούν τον δίσκο, ανεξαρτήτως αν αυτός απομακρύνεται από την εγκατάσταση ή όχι.

Υπάρχουν δύο μέθοδοι κρυπτογράφησης που μπορούν να αξιοποιηθούν:

1. Η χρήση λογισμικού κρυπτογράφησης στον εγκληματολογικό σταθμό εργασίας που εκτελεί τη διαδικασία απεικόνισης. Αυτή η προσέγγιση περιορίζεται σε δίσκους που έχουν αφαιρεθεί από το σύστημα και απεικονίζονται σε ειδικά συστήματα με εγκατεστημένο λογισμικό κρυπτογράφησης.
2. Η εγκατάσταση του λογισμικού κρυπτογράφησης απευθείας στον δίσκο αποδεικτικών στοιχείων. Στο προηγούμενο σενάριο, ο δίσκος χωρίστηκε σε δύο κατατμήσεις: μία για τα αρχεία αποδεικτικών στοιχείων και μία για τα εργαλεία (π.χ. λογισμικό λήψης μνήμης ή απεικόνισης). Σε αυτήν την περίπτωση, το λογισμικό κρυπτογράφησης μπορεί να τοποθετηθεί στην κατάτμηση εργαλείων και η κρυπτογράφηση να εφαρμοστεί κατά τη διάρκεια της διαδικασίας απεικόνισης. Αυτό περιορίζει τις αλλαγές που γίνονται στο προς διερεύνηση σύστημα.

Μόλις ο δίσκος προετοιμαστεί, απαιτείται ένα ακόμη επίπεδο προστασίας για να διασφαλιστεί ότι δεν θα πραγματοποιηθούν αλλαγές στο ύποπτο σύστημα κατά την απεικόνιση. Για να διασφαλιστεί αυτό, οι αναλυτές πρέπει να είναι εξοικειωμένοι με τη χρήση **write blockers**.

6.3. Χρήση write blockers

Βασική αρχή της ψηφιακής εγκληματολογίας είναι η διασφάλιση ότι δεν πραγματοποιούνται αλλαγές στα ψηφιακά αποδεικτικά στοιχεία κατά την επεξεργασία και την εξέτασή τους. Οποιαδήποτε αλλαγή, όσο μικρή και αν είναι, έχει τη δυνατότητα να αμφισβητήσει ολόκληρη τη διαδικασία εξέτασης. Υπάρχει μάλιστα το ενδεχόμενο τα αποδεικτικά στοιχεία να αποκλειστούν από νομικές διαδικασίες εάν ο αναλυτής δεν είναι σε θέση να τεκμηριώσει τον τρόπο με τον οποίο εξασφάλισε ότι τα στοιχεία δεν αλλοιώθηκαν κατά την εξέταση. Ως εκ τούτου, είναι σημαντικό να γίνει κατανοητό

πώς οι **write blockers** διατηρούν την ακεραιότητα των ψηφιακών αποδεικτικών στοιχείων. Οι write blockers διακρίνονται σε δύο τύπους. Ο πρώτος είναι οι **λογισμικοί write blockers**. Πρόκειται για λογισμικό που παρεμβάλλεται ανάμεσα στο λειτουργικό σύστημα και τα αποδεικτικά στοιχεία. Συχνά αποτελούν μέρος των εγκληματολογικών εργαλείων που χρησιμοποιούνται κατά τη φάση της εξέτασης. Εξασφαλίζουν πρόσβαση μόνο για ανάγνωση στα αποδεικτικά αρχεία και διασφαλίζουν ότι, κατά την εξέταση, δεν πραγματοποιούνται αλλαγές. Για παράδειγμα, το εργαλείο **FTK Imager**, το οποίο θα παρουσιαστεί εκτενώς σε αυτό το κεφάλαιο, εξασφαλίζει ότι η απόκτηση ψηφιακών αποδεικτικών στοιχείων πραγματοποιείται χωρίς εγγραφή στον δίσκο.

Ο δεύτερος τύπος είναι οι **φυσικοί ή υλικοί (hardware) write blockers**. Όπως υποδηλώνει το όνομα, πρόκειται για φυσικές συσκευές που παρεμβάλλονται ανάμεσα στον δίσκο αποδεικτικών στοιχείων και το σύστημα που πραγματοποιεί την απόκτηση. Τα δεδομένα επιτρέπεται να περάσουν από τον δίσκο προς το σύστημα ανάλυσης, αλλά όχι αντίστροφα. Η χρήση μιας τέτοιας συσκευής επιτρέπει στους αναλυτές να αποδείξουν με σαφήνεια ότι τα αποδεικτικά στοιχεία δεν αλλοιώθηκαν κατά τη φάση της απόκτησης.

Ο τύπος του write blocker που θα χρησιμοποιηθεί εξαρτάται σε μεγάλο βαθμό από το είδος της απόκτησης που διεξάγεται. Ιδανικά, οι αναλυτές πρέπει να επιλέγουν εργαλεία και τεχνικές που αποδεικνύουν ξεκάθαρα ότι έλαβαν κάθε εύλογο μέτρο για να εξασφαλίσουν ότι τα αποδεικτικά στοιχεία δεν αλλοιώθηκαν. Η ενέργεια αυτή μειώνει σημαντικά τον κίνδυνο αποκλεισμού των στοιχείων από νομικές διαδικασίες, ενώ παράλληλα προσφέρει στον αναλυτή τη δυνατότητα να βασιστεί στα στοιχεία για τον εντοπισμό της ρίζας του προβλήματος (root-cause determination).

Με έναν σωστά προετοιμασμένο δίσκο και έναν write blocker σε λειτουργία, οι αναλυτές μπορούν πλέον να προχωρήσουν στην απεικόνιση (imaging) των δίσκων αποδεικτικών στοιχείων.

6.4. Τεχνικές απεικόνισης (Imaging techniques)

Μόλις έχει ρυθμιστεί κατάλληλα ένα αποθετήριο για το αρχείο εικόνας, ο αναλυτής αντιμετώπισης περιστατικών είναι έτοιμος να αποκτήσει τα απαραίτητα αποδεικτικά στοιχεία. Οι αναλυτές θα συναντήσουν ύποπτα συστήματα είτε σε κατάσταση λειτουργίας είτε απενεργοποιημένα. Ανάλογα με την κατάσταση στην οποία θα βρεθεί το ύποπτο σύστημα, θα χρειαστεί να εφαρμοστεί μία από τις ακόλουθες τεχνικές. Σε κάθε περίπτωση περιστατικού, ανεξάρτητα από την τεχνική που θα χρησιμοποιηθεί, οι αναλυτές πρέπει να είναι έτοιμοι να τεκμηριώσουν σωστά τις ενέργειές τους για να συμπεριληφθούν στη μελλοντική εγκληματολογική αναφορά.

6.5. Dead imaging

Το **dead imaging** εκτελείται σε μέσα που δεν είναι ενεργοποιημένα και, στην περίπτωση σκληρών δίσκων, έχουν αφαιρεθεί από το ενδεχομένως παραβιασμένο σύστημα. Από την άποψη προετοιμασίας αποδεικτικών στοιχείων, η μέθοδος αυτή είναι η πιο ολοκληρωμένη, καθώς επιτρέπει την πλήρη

διατήρηση και ανάλυση ενός φυσικού τόμου. Υπάρχουν διάφορες μέθοδοι και εργαλεία, εμπορικά και δωρεάν, που επιτρέπουν τη σωστή απεικόνιση. Εκτός από το λογισμικό, οι αναλυτές περιστατικών χρησιμοποιούν συχνά και υλικούς write blockers, οι οποίοι εξασφαλίζουν ότι δεν θα πραγματοποιηθούν αλλαγές στο ύποπτο μέσο. Όπως αναφέρθηκε και στο Κεφάλαιο 1 (*Κατανόηση της Αντιμετώπισης Περιστατικών*), είναι κρίσιμο να αποδεικνύεται στο δικαστήριο ότι δεν έγιναν αλλαγές στα πρωτότυπα αποδεικτικά στοιχεία.

Ένα πλεονέκτημα της απεικόνισης σκληρού δίσκου ή άλλου ψηφιακού μέσου με αυτήν τη μέθοδο είναι ότι η διαδικασία μπορεί να είναι προτυποποιημένη και επαναλήψιμη. Η ύπαρξη μιας προδιαγεγραμμένης διαδικασίας, ενσωματωμένης στον σχεδιασμό αντιμετώπισης περιστατικών, διασφαλίζει ότι τα αποδεικτικά στοιχεία χειρίζονται με εγκληματολογικά ορθή μέθοδο.

Ένα ιδιαίτερα χρήσιμο εργαλείο για το dead imaging είναι το **FTK Imager**. Το εργαλείο αυτό, που παρέχεται από την AccessData, αποτελεί εγκληματολογικά αξιόπιστη πλατφόρμα για την απόκτηση εικόνας δίσκου.

6.6. Απεικόνιση με χρήση του FTK Imager

Η παρακάτω διαδικασία χρησιμοποιεί έναν σκληρό δίσκο και το FTK Imager για τη δημιουργία μιας εγκληματολογικά αξιόπιστης εικόνας (image) για ανάλυση. Η βιασύνη ή η παρέκκλιση από αυτά τα βήματα μπορεί να δημιουργήσει μια κατάσταση όπου ο αναλυτής δεν θα μπορεί να βασιστεί στην ακεραιότητα των στοιχείων, καθιστώντας τυχόν αποδεικτικά στοιχεία αναξιόπιστα:

1. Το πρώτο βήμα είναι η φυσική επιθεώρηση των στοιχείων. Υπάρχουν δύο κύρια σημεία εστίασης που πρέπει να ελεγχθούν. Το πρώτο είναι η φόρμα αλυσίδας διαχείρισης στοιχείων (chain of custody). Κάθε φορά που παραλαμβάνετε στοιχεία, πρέπει να έχετε πρόσβαση στη φόρμα, να βεβαιωθείτε ότι όλα τα βήματα έχουν καταγραφεί σωστά και να ολοκληρώσετε την εγγραφή με τα δικά σας στοιχεία.



2. Στη συνέχεια, πρέπει να ελέγξετε τη συσκευασία των στοιχείων για να διασφαλίσετε ότι δεν έχουν παραβιαστεί οι σφραγίδες. Ένας γρήγορος τρόπος για να τεκμηριώσετε αυτό είναι να τραβήξετε φωτογραφία των στοιχείων μέσα στην αρχική συσκευασία.
3. Στην προηγούμενη φωτογραφία, έχουμε καταγράψει όλες τις πληροφορίες σχετικά με τα στοιχεία και έχουμε αποδείξει ότι, πριν από την απεικόνιση, η ακεραιότητα των στοιχείων έχει διατηρηθεί. Αφού σπάσει η σφραγίδα, πρέπει να τραβήξετε άλλη φωτογραφία των περιεχομένων της συσκευασίας.



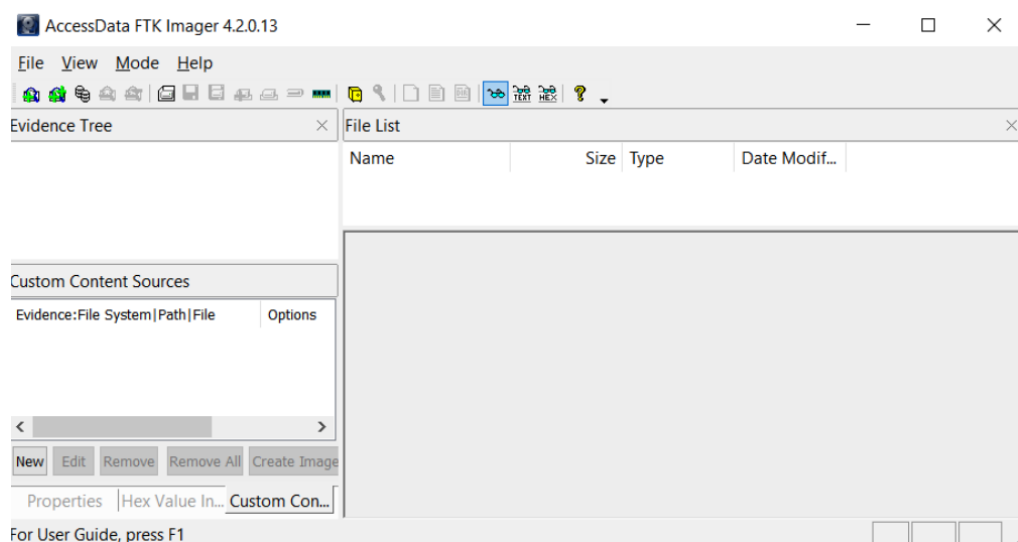
4. Αφού τραβηχτεί η φωτογραφία του στοιχείου, πρέπει να βεβαιωθείτε ότι ταιριάζει με τη φόρμα αλυσίδας διαχείρισης. Σφάλματα μπορεί να προκύψουν σε ένα περιστατικό, και αυτός είναι ένας τρόπος να διορθωθούν όσο το δυνατόν νωρίτερα. Επιβεβαιώνοντας την αλυσίδα διαχείρισης, τυχόν μπερδέματα μπορούν να διορθωθούν.



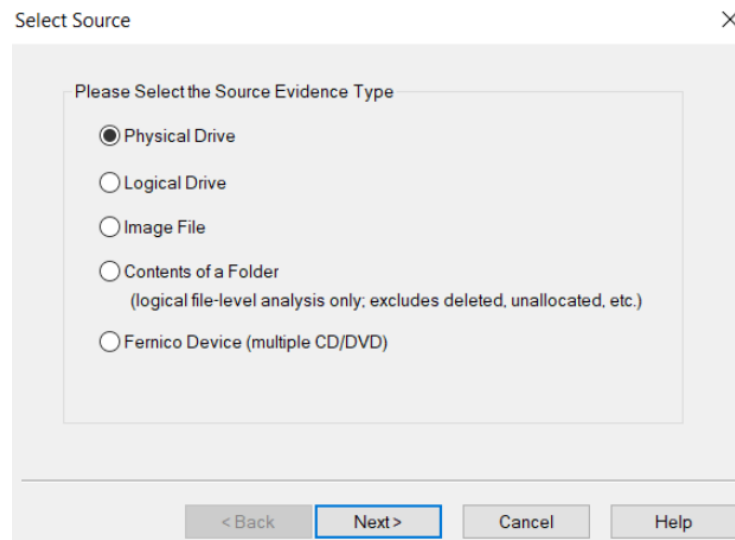
5. Το επόμενο βήμα είναι η ρύθμιση του φυσικού write blocker. Σε αυτήν την περίπτωση, χρησιμοποιείται το **Tableau TK35u USB 3.0 Forensic IDE/SATA Bridge Kit** ως φυσικός write blocker. Ο ύποπτος δίσκος συνδέεται μέσω του παρεχόμενου SATA adapter και γίνεται σύνδεση

FireWire με τον υπολογιστή απεικόνισης. Όταν χρησιμοποιείται φυσικός write blocker, βεβαιωθείτε ότι η συσκευή λειτουργεί σωστά.

6. Με τον φυσικό write blocker στη θέση του, ο ύποπτος δίσκος είναι έτοιμος για απεικόνιση. Στο παράδειγμα αυτό, θα χρησιμοποιηθεί η δωρεάν εφαρμογή **FTK Imager**. Το FTK Imager απαιτεί δικαιώματα διαχειριστή για να τρέξει. Ανοίξτε το εκτελέσιμο αρχείο και θα εμφανιστεί η παρακάτω οθόνη:

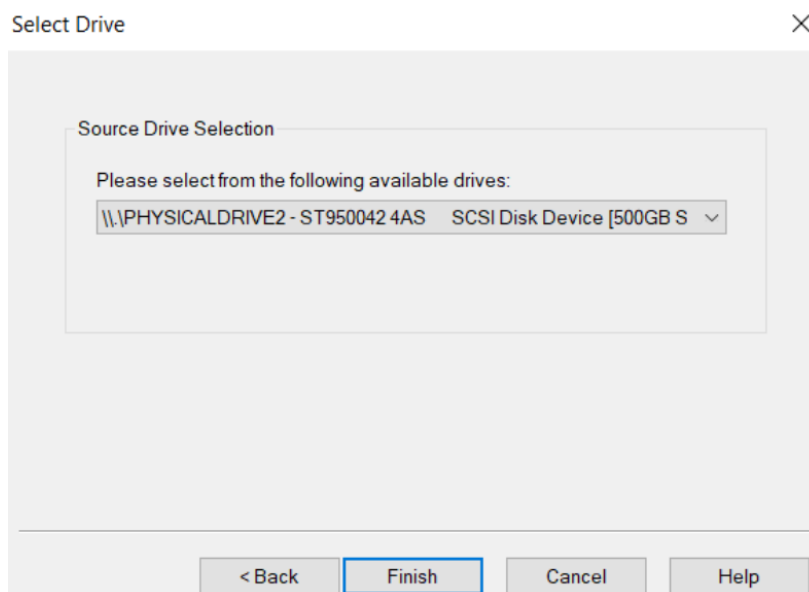


7. Κάντε κλικ στο **File** και μετά στο **Create Disk Image**. Θα ανοίξει ένα παράθυρο όπου μπορείτε να επιλέξετε την πηγή μέσου. Σε αυτήν την περίπτωση, επιλέξτε **Physical Drive**, ώστε να καταγραφεί ολόκληρος ο δίσκος, συμπεριλαμβανομένου του master boot record, για περαιτέρω ανάλυση. Στη συνέχεια, κάντε κλικ στο **Next**.

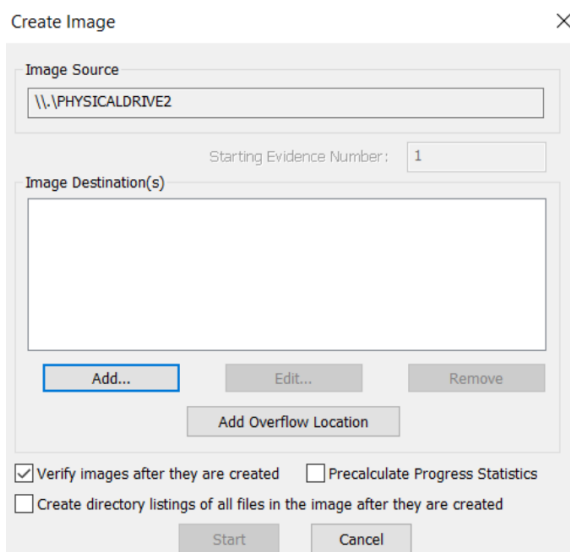


8. Το επόμενο παράθυρο επιτρέπει στον αναλυτή να επιλέξει ποιος δίσκος θα απεικονιστεί. Οι αναλυτές incident response πρέπει να δώσουν προσοχή ώστε να απεικονίσουν τη σωστή

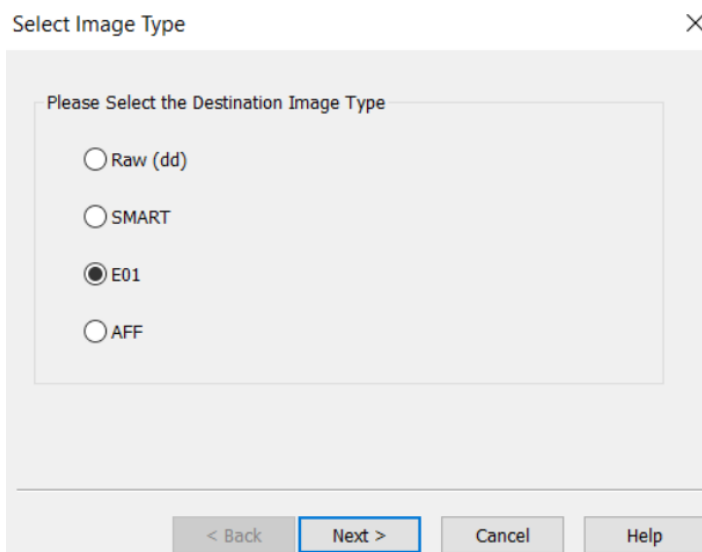
συσκευή, καθώς εμφανίζονται όλες οι συσκευές που είναι ορατές στο λειτουργικό σύστημα. Πρέπει να προσέξετε τον αποθηκευτικό χώρο των δίσκων για να διαχωρίσετε τον ύποπτο δίσκο από τον δίσκο προορισμού. Στο παράδειγμα, εμφανίζονται τέσσερις δίσκοι: δύο στον υπολογιστή απεικόνισης, ένας προορισμός και ένας ύποπτος. Ο ύποπτος δίσκος είναι ο τρίτος, με την ένδειξη \\.\PHYSICALDRIVE2. Επιλέξτε τον και κάντε κλικ στο **Finish**.



9. Μόλις επιλεγεί ο ύποπτος δίσκος, ορίστε τον δίσκο προορισμού κάνοντας κλικ στο **Add...**



10. Στη συνέχεια, επιλέξτε τον τύπο αρχείου εικόνας που θέλετε να δημιουργήσετε. Υπάρχουν τέσσερις επιλογές. Σε αυτήν την περίπτωση, επιλέξτε **E01** και κάντε κλικ στο **Next**.



Select Image Type

Please Select the Destination Image Type

☐ Raw (dd)

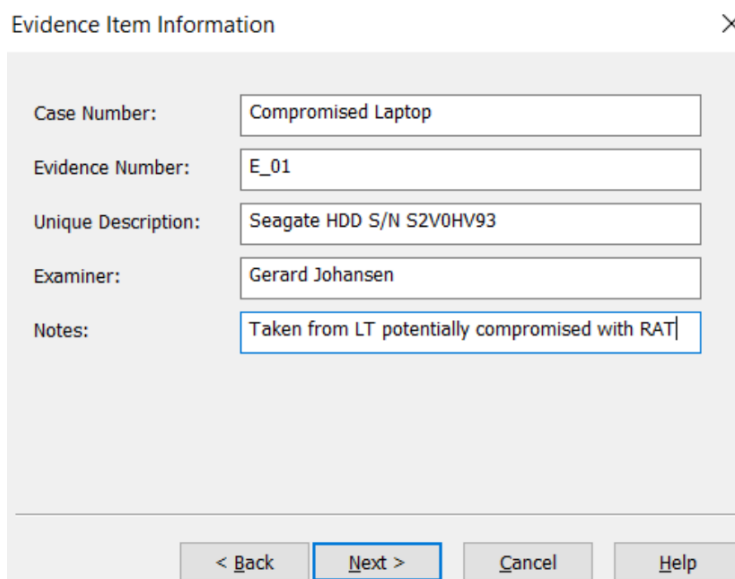
☐ SMART

☒ E01

☐ AFF

< Back Next > Cancel Help

11. Στο επόμενο παράθυρο, εισάγετε πληροφορίες ειδικές για την εικόνα. Ο αναλυτής θα πρέπει να συμπληρώσει τα πεδία με όσο το δυνατόν περισσότερες λεπτομέρειες, καθώς αυτές οι πληροφορίες θα συμπεριληφθούν στην εγκληματολογική αναφορά. Στη συνέχεια, κάντε κλικ στο **Next**.



Evidence Item Information

Case Number: Compromised Laptop

Evidence Number: E_01

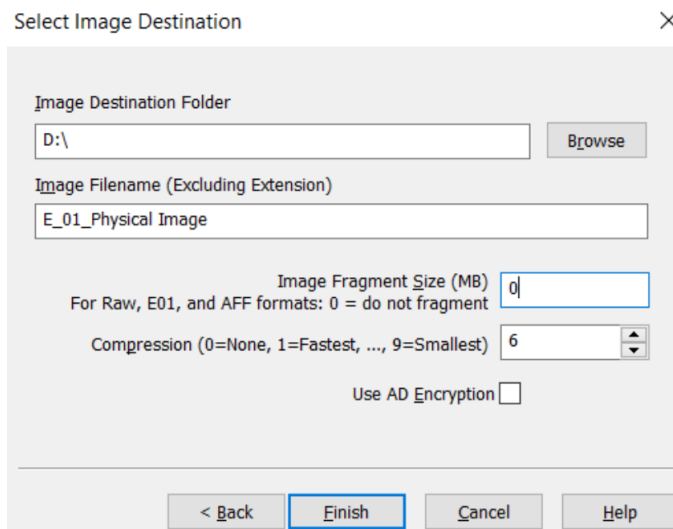
Unique Description: Seagate HDD S/N S2V0HV93

Examiner: Gerard Johansen

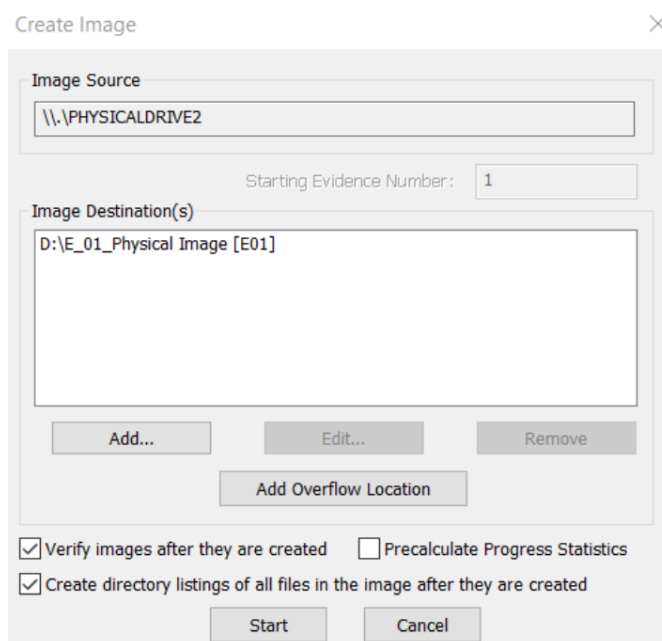
Notes: Taken from LT potentially compromised with RAT

< Back Next > Cancel Help

12. Στο επόμενο παράθυρο, επιβεβαιώστε ότι ο δίσκος προορισμού και τα ονόματα αρχείων είναι σωστά. Εδώ μπορείτε επίσης να ορίσετε το μέγεθος τεμαχισμού (fragmentation) και τη συμπίεση της εικόνας. Το μέγεθος τεμαχισμού μπορεί να οριστεί σε 0, ώστε ολόκληρη η εικόνα να περιέχεται σε ένα αρχείο. Για τώρα, χρησιμοποιούμε τις προεπιλογές. Μόλις επιβεβαιωθούν οι ρυθμίσεις, κάντε κλικ στο **Finish**.

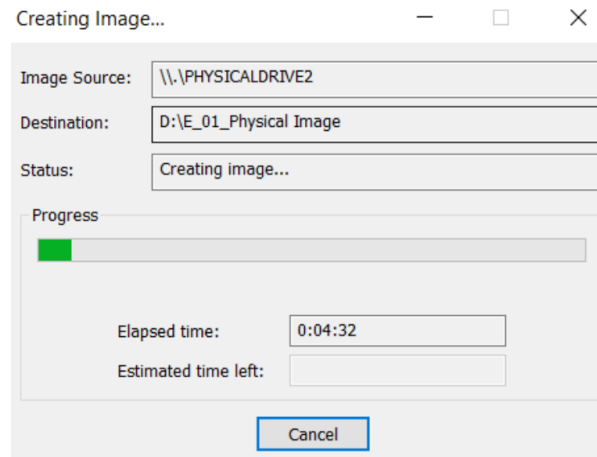


13. Τώρα ανοίγει το παράθυρο **Create Image**. Εδώ μπορείτε να ακυρώσετε τη δημιουργία της εικόνας. Υπάρχουν δύο χρήσιμες επιλογές: η πρώτη είναι να ελέγξει το FTK Imager την εικόνα μετά τη δημιουργία της, για να διασφαλιστεί ότι δεν έγιναν αλλαγές και ότι η εικόνα είναι πλήρης και χωρίς σφάλματα. Η δεύτερη είναι να δημιουργηθεί λίστα όλων των αρχείων στην εικόνα, χρήσιμη εάν κάποια αρχεία έχουν αποδεικτική αξία. Αφού ελεγχθούν οι ρυθμίσεις, κάντε κλικ στο **Start**.

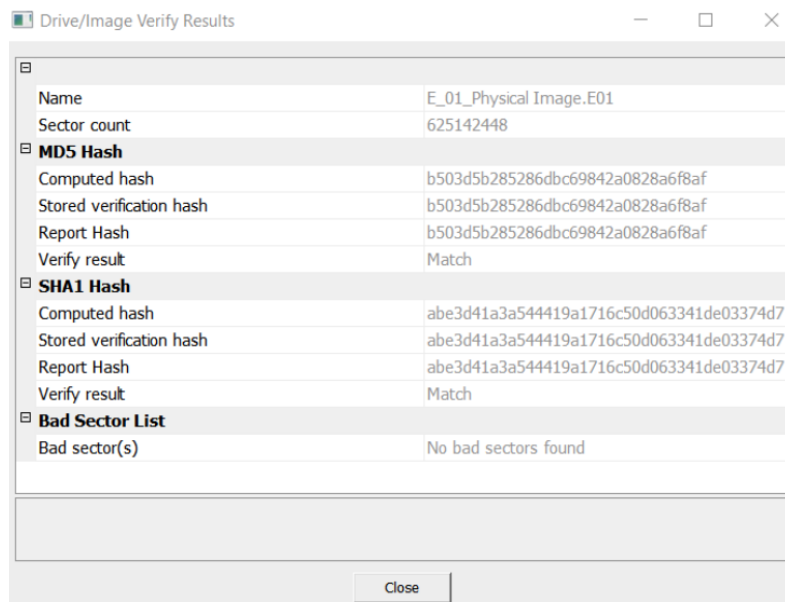


14. Το FTK Imager ξεκινά τη διαδικασία απεικόνισης. Αυτό μπορεί να διαρκέσει ώρες ή και μέρες, ανάλογα με το μέγεθος του δίσκου, την ταχύτητα του συστήματος και τον τύπο σύνδεσης (FireWire, USB κ.λπ.).

15. Μόλις ολοκληρωθεί η απεικόνιση, ανοίγει ένα παράθυρο με λεπτομερείς πληροφορίες. Σημαντικό είναι να ελεγχθούν οι υπολογισμένοι κατακερματισμοί (hashes) για τον δίσκο και την εικόνα. Εάν οι MD5 και SHA1 ταιριάζουν, η διαδικασία απεικόνισης ήταν σωστή και δεν υπήρξαν αλλαγές στα στοιχεία. Είναι καλή πρακτική να περιλαμβάνονται αυτά τα στοιχεία στην αναφορά.



Πλοηγηθείτε στον δίσκο στοιχείων. Εδώ βρίσκεται η πλήρης εικόνα. Ανάλογα με τις ρυθμίσεις τεμαχισμού, μπορεί να υπάρχουν ένα ή περισσότερα αρχεία εικόνας. Το FTK Imager παρέχει επίσης πλήρη λίστα όλων των αρχείων του δίσκου και ένα αρχείο κειμένου με λεπτομέρειες της διαδικασίας, που πρέπει να συμπεριληφθεί σε οποιαδήποτε εγκληματολογική αναφορά. Η διαδικασία απεικόνισης ολοκληρώνεται και ο δίσκος επιστρέφεται στην ασφαλή αποθήκευση.

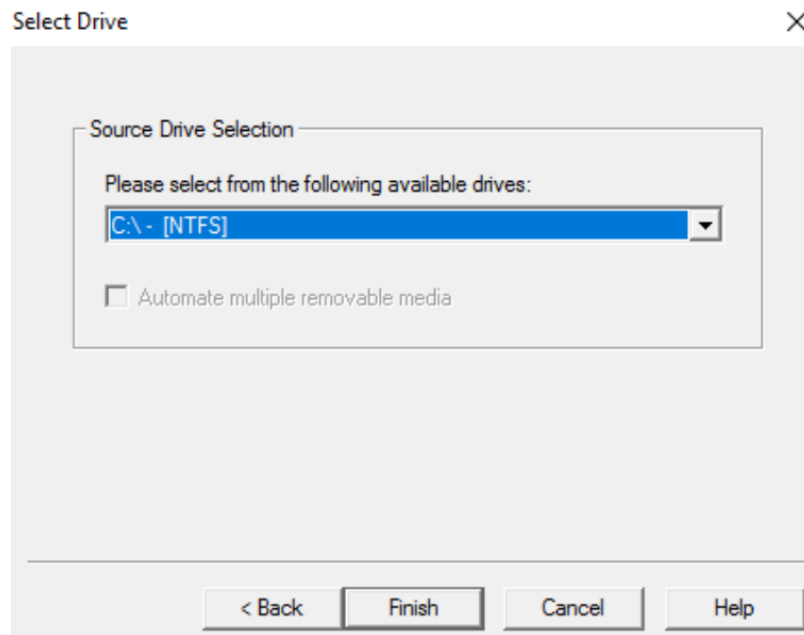


Η **dead imaging** παρέχει την εγκληματολογικά πιο αξιόπιστη καταγραφή. Υπάρχουν όμως περιπτώσεις που ο αναλυτής πρέπει να απεικονίσει ένα σύστημα που είναι ενεργό, οπότε απαιτείται **live imaging**.

6.7. Ζωντανή Απόκτηση Εικόνας (Live imaging)

Μια ζωντανή εικόνα μπορεί να ληφθεί από ένα σύστημα που λειτουργεί χρησιμοποιώντας το FTK Imager με πολύ παρόμοιο τρόπο όπως θα κάνατε για την απόκτηση «νεκρής» εικόνας (dead imaging). Σε αυτή την περίπτωση, η κύρια διαφορά είναι ότι το FTK Imager θα τρέχει από μια συσκευή USB που είναι συνδεδεμένη στο σύστημα. Αυτό επιτρέπει στον αναλυτή απόκρισης σε περιστατικά να δημιουργήσει εικόνα του δίσκου χωρίς να αλλάξει το σύστημα. Αν και ορισμένα αρχεία και ρυθμίσεις μητρώου θα ενημερωθούν, η απόκτηση εικόνας με αυτόν τον τρόπο δεν θα αλλάξει τα αρχεία του συστήματος με τον ίδιο τρόπο όπως θα έκανε η εγκατάσταση του FTK Imager σε ένα ενδεχομένως μολυσμένο σύστημα.

Όσον αφορά την προετοιμασία, ο αναλυτής θα πρέπει να έχει μια προδιαμορφωμένη συσκευή USB με ξεχωριστά partitions για εργαλεία και για τα στοιχεία απόδειξης (evidence). Όπως αναφέραμε προηγουμένως, το partition για τα στοιχεία απόδειξης θα πρέπει να διαγραφεί πριν από οποιαδήποτε χρήση. Επίσης, η πλήρης έκδοση του FTK Imager συχνά αντιμετωπίζει προβλήματα με αρχεία DLL που δεν βρίσκονται στη σωστή θέση όταν προσπαθεί να τρέξει από USB. Για να αντιμετωπιστεί αυτό, η Access Data παρέχει μια ελαφριά έκδοση που ονομάζεται FTK Imager Lite, η οποία μπορεί να κατέβει από: <http://marketing.accessdata.com/ftkimagerlite3.1.1>.



Για να ληφθεί εικόνα ενός δίσκου, συνδέστε τη συσκευή USB στον υπολογιστή στόχο και ξεκινήστε απλά το FTK Imager Lite. Ακολουθήστε την ίδια διαδικασία που περιγράφηκε προηγουμένως. Ο imager θα δημιουργήσει την εικόνα με τον ίδιο τρόπο. Σε αντίθεση με το προηγούμενο παράδειγμα, όπου ολόκληρος ο δίσκος εικονιζόταν, η ζωντανή απόκτηση εικόνας μπορεί να εστιάσει απευθείας σε ένα partition του δίσκου. Για παράδειγμα, σε αυτή την περίπτωση, ο αναλυτής απόκρισης σε

περιστατικά ενδιαφέρεται μόνο για την απόκτηση της μονάδας C: του συστήματος στόχου. Όταν γίνει η επιλογή της πηγής (Source Drive Selection), ο αναλυτής θα πρέπει να επιλέξει: C:\ - [NTFS].

Τα υπόλοιπα βήματα είναι ίδια με αυτά της απόκτησης νεκρής εικόνας, καθώς ο αναλυτής θα επιλέξει τον προορισμό (destination drive) που έχει προδιαμορφωθεί προηγουμένως για τα στοιχεία απόδειξης. Μόλις ολοκληρωθεί η διαδικασία απόκτησης εικόνας, ο αναλυτής θα έχει στη διάθεσή του τις ίδιες πληροφορίες που παρέχονταν και στην προηγούμενη διαδικασία.

6.8. Απόκτηση μνήμης εξ αποστάσεως (Remote memory acquisition)

Η προτιμώμενη μέθοδος για την απόκτηση μνήμης είναι μέσω άμεσης επαφής με το σύστημα του υπόπτου. Αυτό επιτρέπει στους αναλυτές απόκρισης σε περιστατικά να προσαρμόζονται σε περίπτωση που ένα εργαλείο ή μια τεχνική δεν λειτουργήσει. Αυτή η μέθοδος είναι επίσης ταχύτερη για τη λήψη των απαραίτητων αρχείων, καθώς δεν εξαρτάται από σταθερή σύνδεση δικτύου. Αν και αυτή είναι η προτιμώμενη μέθοδος, μπορεί να υπάρχουν γεωγραφικοί περιορισμοί, ειδικά σε μεγάλες οργανώσεις όπου οι αναλυτές απόκρισης σε περιστατικά βρίσκονται σε άλλη πόλη ή χώρα σε σχέση με την τοποθεσία που περιέχει τα στοιχεία απόδειξης.

Στην περίπτωση εξ αποστάσεως απόκτησης, οι αναλυτές απόκρισης μπορούν να χρησιμοποιήσουν τα ίδια εργαλεία που χρησιμοποιούνται και στην τοπική απόκτηση. Η μόνη αλλαγή είναι ότι οι αναλυτές πρέπει να χρησιμοποιήσουν τεχνολογία εξ αποστάσεως για να αποκτήσουν πρόσβαση στα συστήματα υπόπτου και να πραγματοποιήσουν τη λήψη. Στις επόμενες ενότητες θα συζητηθούν δύο επιλογές: το open source εργαλείο WinPmem και η εμπορική επιλογή F-Response. Όπως και με οποιαδήποτε άλλη μέθοδο, οι αναλυτές απόκρισης θα πρέπει να διασφαλίζουν ότι καταγράφουν κάθε χρήση τεχνολογίας εξ αποστάσεως. Αυτό θα επιτρέψει τη σωστή αναγνώριση νόμιμων σε σχέση με ύποπτες συνδέσεις αργότερα.

6.9. WinPmem

Το WinPmem μπορεί να εγκατασταθεί σε απομακρυσμένα συστήματα μέσω εγγενών εφαρμογών όπως το Remote Desktop ή το PSEXEC. Μόλις εγκατασταθεί στο απομακρυσμένο σύστημα, η έξοδος του WinPmem μπορεί να προωθηθεί (ripped) σε άλλο σύστημα χρησιμοποιώντας το NetCat.

Για παράδειγμα, υποθέτουμε ότι ο αναλυτής απόκρισης σε περιστατικά χρησιμοποιεί ένα σύστημα που βρίσκεται στη διεύθυνση 192.168.0.56. Αν ο αναλυτής μπορεί να έχει πρόσβαση στο μολυσμένο σύστημα μέσω PSEXEC ή RDS, μπορεί να δημιουργήσει μια σύνδεση NetCat πίσω στη δική του μηχανή χρησιμοποιώντας την ακόλουθη εντολή:

```
C:/winpmem-2.1.exe - | nc 192.168.0.56 4455
```

Η παραπάνω εντολή λέει στο σύστημα να πραγματοποιήσει τη λήψη μνήμης και να στείλει την έξοδο μέσω NetCat στον σταθμό εργασίας του αναλυτή απόκρισης σε περιστατικά μέσω της θύρας 4455.

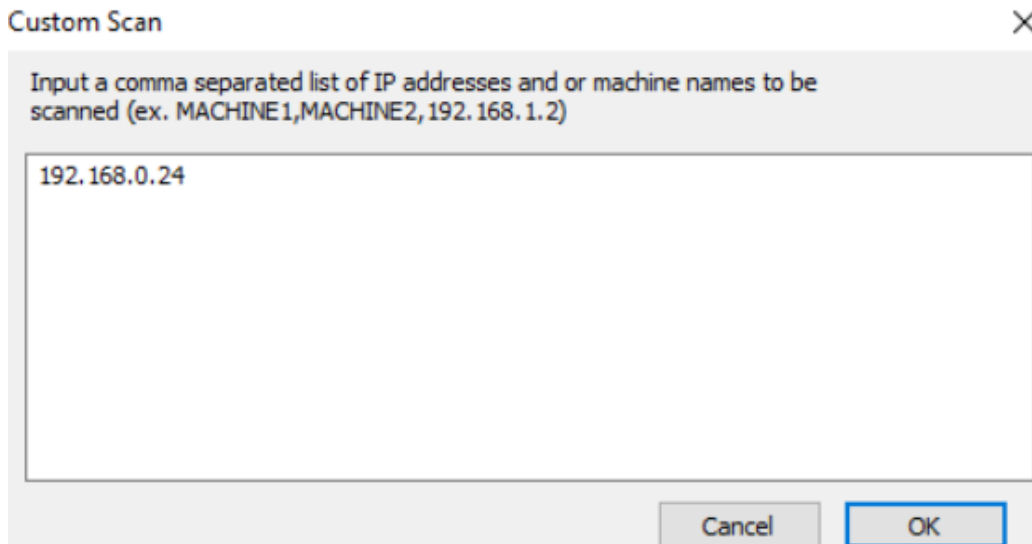
Το μειονέκτημα αυτής της τεχνικής είναι ότι απαιτεί πρόσβαση στη γραμμή εντολών, καθώς και την εγκατάσταση τόσο του NetCat όσο και του WinPmem. Αυτό μπορεί να μην είναι η καλύτερη επιλογή αν ο αναλυτής απόκρισης διαχειρίζεται ένα σύστημα που ήδη θεωρείται ύποπτο για παραβίαση.

6.10. F-Response

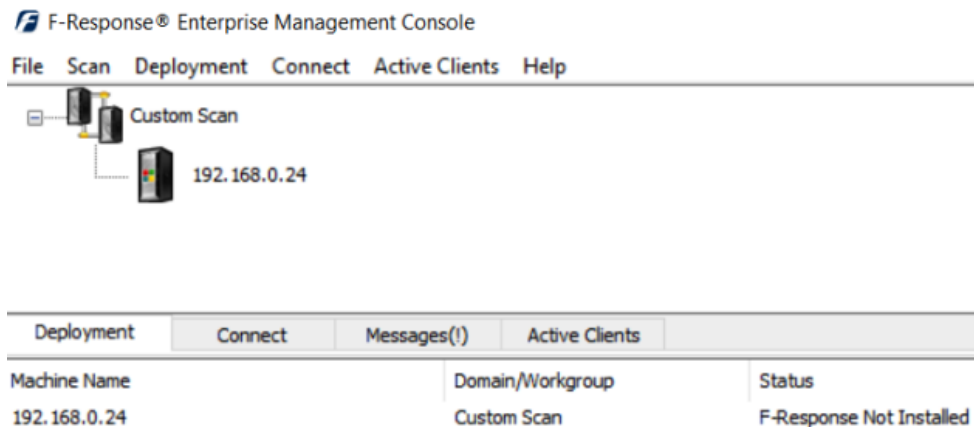
Μια ακόμη επιλογή που διατίθεται στους αναλυτές απόκρισης σε περιστατικά είναι η χρήση του εργαλείου **F-Response**. Το F-Response είναι μια πλατφόρμα λογισμικού που επιτρέπει στους αναλυτές απόκρισης να πραγματοποιούν **απομακρυσμένη απόκτηση αποδεικτικών στοιχείων μέσω δικτύου**. Ένα πλεονέκτημα της χρήσης του F-Response είναι ότι **δεν απαιτεί άμεση πρόσβαση στο απομακρυσμένο σύστημα μέσω SSH ή RDS**. Ένα ακόμη σημαντικό χαρακτηριστικό είναι ότι το εργαλείο έχει σχεδιαστεί για να δημιουργεί σύνδεση ενώ επιτρέπει στον αναλυτή να χρησιμοποιεί τα **προτιμώμενα εργαλεία του** για την απόκτηση των δεδομένων. Πληροφορίες για το προϊόν F-Response είναι διαθέσιμες στη διεύθυνση: <https://www.f-response.com/buyfresponse/software>

Στο παρακάτω παράδειγμα, το F-Response χρησιμοποιείται για να συνδεθεί σε ένα σύστημα που θεωρείται ύποπτο ότι έχει υποστεί παραβίαση μέσω δικτύου, επιτρέποντας στον αναλυτή να χρησιμοποιήσει το **FTK Imager** για να αποκτήσει τη μνήμη του ύποπτου συστήματος. Ακολουθούν τα βήματα που πρέπει να ακολουθηθούν:

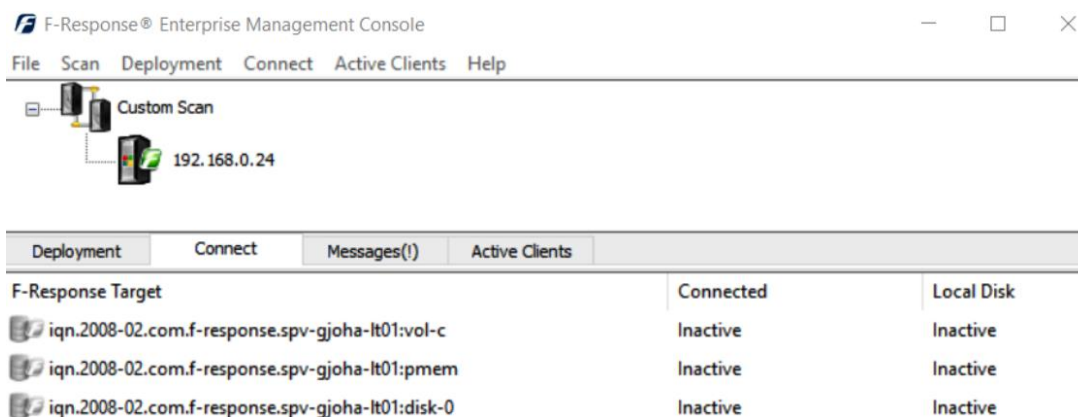
1. Αφού εγκατασταθεί το **F-Response Enterprise**, μεταβείτε στο μενού **Scan** και κάντε κλικ στο **Custom Scan**. Εκεί μπορείτε να εισάγετε τη διεύθυνση IP του ύποπτου συστήματος. Στο παράδειγμα αυτό, το F-Response θα χρησιμοποιηθεί για να καταγράψει τη μνήμη ενός συστήματος στο τοπικό δίκτυο με τη διεύθυνση IP: **192.168.0.24**.



- Μετά την εισαγωγή της IP, κάντε κλικ στο **OK**. Σε αυτό το σημείο, το F-Response προσπαθεί να συνδεθεί με το σύστημα-στόχο. Αν η σύνδεση είναι επιτυχής, το σύστημα θα εμφανιστεί στο πάνω πλαίσιο ως ένα εικονίδιο, συχνά με το λογότυπο των Windows. Στο κάτω πλαίσιο, το σύστημα-στόχος θα υποδεικνύει ότι **δεν έχει εγκατασταθεί το F-Response**.



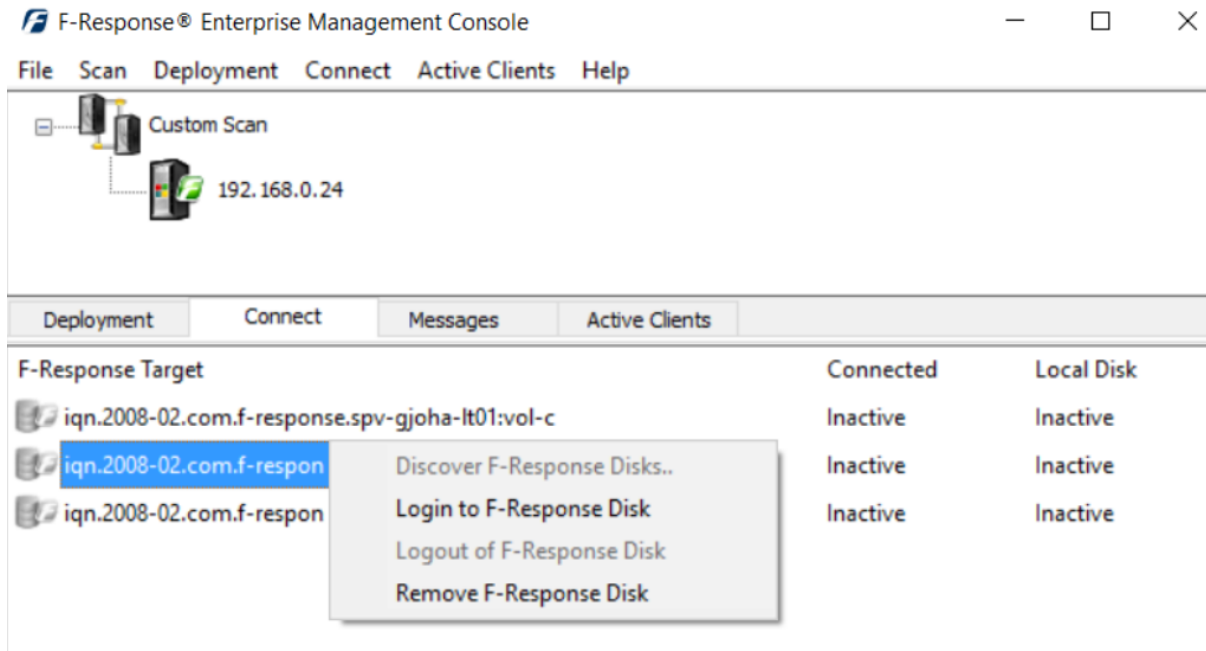
- Για να αποκτήσει το F-Response τα απαιτούμενα στοιχεία, πρέπει να εγκατασταθεί ένας **agent**. Αυτό γίνεται με δεξί κλικ στο σύστημα και επιλογή **Install/Start F-Response**.
- Μόλις εγκατασταθεί το F-Response στο απομακρυσμένο σύστημα, θα εμφανιστούν δύο δείκτες:
 - Ένα πράσινο εικονίδιο F-Response πάνω στο εικονίδιο του συστήματος στο πάνω πλαίσιο.
 - Στο κάτω πλαίσιο, λίστα με τους διαθέσιμους στόχους του συστήματος.



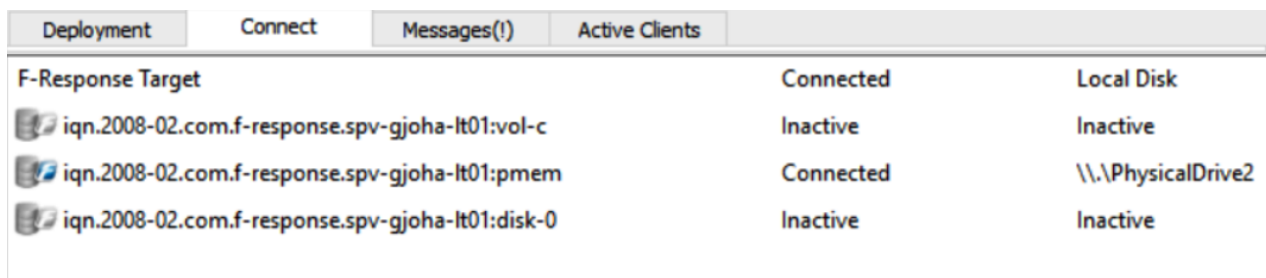
Στο παράδειγμα, το F-Response υποδεικνύει ότι το σύστημα έχει:

- Φυσικό δίσκο (disk-0)
- Λογικό δίσκο (vol-c)

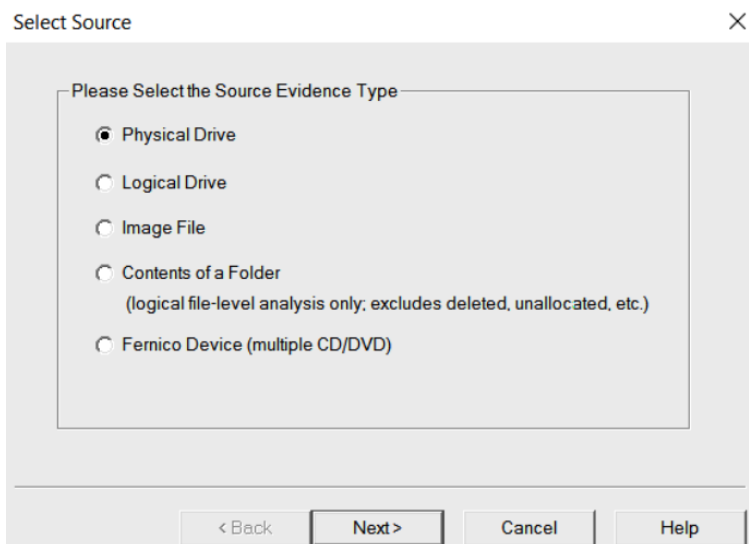
- ο **Μνήμη** (pmem), που είναι και ο στόχος μας.
5. Για να αποκτηθεί η μνήμη, πρέπει να ρυθμιστεί το F-Response ώστε να μπορεί να **mountάρει τον στόχο**. Κάντε δεξί κλικ στον στόχο και επιλέξτε **Login to F-Response Disk**.



6. Μόλις γίνει login, το κάτω πλαίσιο θα δείξει ποιος δίσκος είναι ενεργός. Στο παράδειγμα, η μνήμη έχει ενεργοποιηθεί και μπορεί να mountαριστεί ως φυσικός δίσκος (\\.\PhysicalDrive2 υπό Local Disk). Από εδώ, η μνήμη μπορεί να αποκτηθεί με διάφορα εργαλεία. Στην προκειμένη περίπτωση, χρησιμοποιείται το **FTK Imager** για να αποκτηθεί η μνήμη σε μορφή RAW.



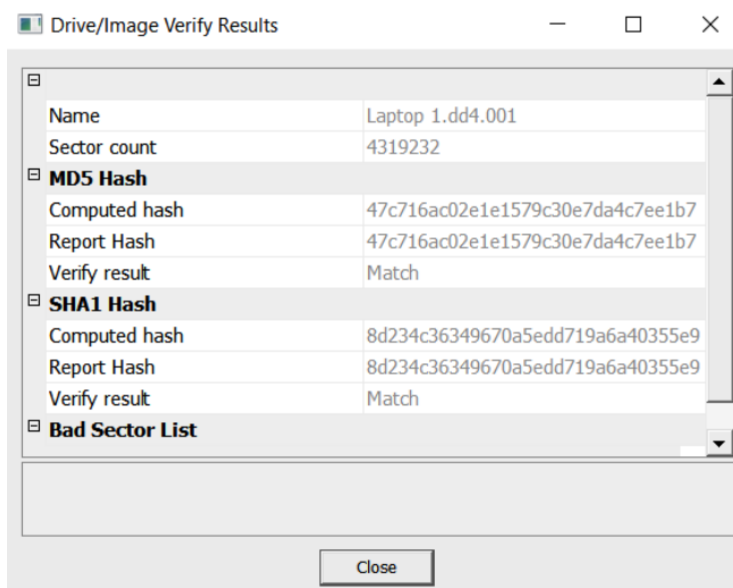
7. Ανοίξτε το **FTK Imager**, μεταβείτε στο **File** και επιλέξτε **Create Disk Image** (προσέξτε να μην επιλέξετε **Capture Memory**, γιατί αυτό θα καταγράψει τη μνήμη στο σύστημα που τρέχει το FTK Imager). Στο νέο παράθυρο, επιλέξτε **Physical Drive** ως τύπο πηγής.
8. Κάντε κλικ στο **Next** και επιλέξτε τον δίσκο που υποδεικνύει το F-Response. Στο παράδειγμα, είναι ο **\\.\PHYSICALDRIVE2**.



Η συνέχεια της διαδικασίας είναι ίδια με αυτή της ανάλυσης Dead Box. Το F-Response παρέχει έναν μηχανισμό ώστε το FTK Imager να αναγνωρίζει τον απομακρυσμένο δίσκο ως πηγή για imaging. Για το FTK δεν έχει σημασία αν ο δίσκος είναι τοπικός ή απομακρυσμένος, αρκεί να



αναγνωρίζεται για δημιουργία εικόνας. Στο τέλος, το FTK Imager παρέχει όλα τα δεδομένα που πρέπει να συμπεριληφθούν στην **αυτοψία/forensic αναφορά**.



6.11. Εικονικές μηχανές (Virtual Machines)

Οι αναλυτές περιστατικών συχνά θα αντιμετωπίσουν εικονικούς διακομιστές και ακόμη και σταθμούς εργασίας στο πλαίσιο μιας έρευνας. Τα εικονικοποιημένα συστήματα μπορούν να αποκτηθούν απλά με την εξαγωγή μιας παγωμένης εικονικής μηχανής σε έναν αφαιρούμενο δίσκο. Σε άλλες περιπτώσεις, οι ανακριτές μπορούν να χρησιμοποιήσουν τη δυνατότητα λήψης στιγμιότυπων (snapshot) ενός εικονικού συστήματος. Αυτό δημιουργεί ένα ξεχωριστό αρχείο που μπορεί να αναλυθεί την ημερομηνία και ώρα που λήφθηκε το στιγμιότυπο. Σε κάθε περίπτωση, οι ανακριτές θα πρέπει να βεβαιωθούν ότι ο δίσκος έχει καθαριστεί σωστά και ότι η σωστή τεκμηρίωση έχει ολοκληρωθεί.

Για να αποκτηθεί η εικονική μηχανή, απλά παγώστε το σύστημα και μετακινήστε ολόκληρο τον κατάλογο στα εξωτερικά μέσα. (Σε ορισμένες περιπτώσεις, αυτό μπορεί να γίνει ακόμη και απομακρυσμένα.) Σε πλατφόρμες εικονικοποίησης των Windows, όπως το VMware, υπάρχουν πολλά αρχεία που αποτελούν την εικονική εικόνα:

- **.vmdk:** Αυτό είναι το αρχείο εικόνας του εικονικού δίσκου. Πρόκειται για τον λογικό τόμο όπου βρίσκεται το εικονικό λειτουργικό σύστημα και τα αρχεία. Η απόκτηση αυτού του αρχείου μοιάζει πολύ με τη δημιουργία εικόνας του δίσκου C σε ένα φυσικό σύστημα.
- **.vmem:** Το αρχείο .vmem είναι το αρχείο εικονικής μνήμης. Πρόκειται για τον χώρο αποθήκευσης της εικονικής RAM ή της φυσικής μνήμης. Αυτό το αρχείο μπορεί να εξαχθεί και να συνδυαστεί με ένα επιπλέον αρχείο για ανάλυση, χρησιμοποιώντας τις μεθόδους που θα συζητηθούν στο Κεφάλαιο 8, «Ανάλυση Μνήμης Συστήματος».
- **.vmss:** Το αρχείο καταστάσεων αναστολής (suspended state) του VMware αποθηκεύει τη ρυθμιζόμενη κατάσταση μιας ανασταλμένης εικονικής μηχανής. Περιλαμβάνει δεδομένα διεργασιών και δικτυακών συνδέσεων. Αυτό το αρχείο συνδυάζεται με το .vmem για να παρέχει τη μνήμη του συστήματος.
- **.vmsn:** Το αρχείο καταστάσεων στιγμιότυπου (snapshot state) περιέχει την κατάσταση του συστήματος όταν λήφθηκαν τα στιγμιότυπα.

Οι ανακριτές μπορούν να χρησιμοποιήσουν αυτά τα αρχεία με διάφορους τρόπους. Πρώτον, το αρχείο .vmdk μπορεί να προσαρτηθεί (mount) όπως ένα αρχείο εικόνας σε διάφορες πλατφόρμες ψηφιακής εγκληματολογίας. Αυτό θα συζητηθεί στο Κεφάλαιο 9, «Ανάλυση Αποθήκευσης Συστήματος». Δεύτερον, το αρχείο .vmsn μπορεί να χρησιμοποιηθεί για την ανακατασκευή του συστήματος απλά αντιγράφοντας το αρχείο και δουλεύοντας με το αντίγραφο. Από εκεί, οι ανακριτές μπορούν να εξετάσουν τη συμπεριφορά του συστήματος ή να εξάγουν στοιχεία χωρίς να επηρεαστεί το αρχικό αρχείο .vmsn.

Τέλος, η τρέχουσα μνήμη που καταγράφεται μέσω των αρχείων .vmem και .vmss μπορεί να αναλυθεί με τον ίδιο τρόπο όπως και άλλες καταγραφές μνήμης. Για να ληφθούν τα κατάλληλα εγκληματολογικά δεδομένα, τα δύο αρχεία πρέπει να συνδυαστούν. Αυτό μπορεί να γίνει χρησιμοποιώντας το εργαλείο **vmss2core.exe**, το οποίο περιλαμβάνεται στο πακέτο εργαλείων του VMware. Για να συνδυαστούν αυτά τα αρχεία, χρησιμοποιείται η εξής σύνταξη εντολής:

```
C:\VirtualTools\vmss2core.exe -W "InfectedServer.vms" "InfectedServer.vmem"
```

Η παραπάνω εντολή θα παράγει ένα memory dump στον κατάλογο που περιέχει τα δύο αρχεία. Αν και η εικονικοποίηση είναι κοινή σε μεγάλες επιχειρήσεις, δεν θα πρέπει να αποτελεί σημαντική πρόκληση. Με κάποιους τρόπους, η δυνατότητα απλά να παγώσει κανείς ένα σύστημα και να εξαγάγει όλα τα απαραίτητα αρχεία καθιστά ταχύτερη την απόκτηση των απαραίτητων αποδεικτικών στοιχείων.

Μέχρι τώρα, η εστίαση ήταν σε εργαλεία των Windows για δημιουργία εικόνων. Μια άλλη επιλογή διαθέσιμη στους ανακριτές είναι η χρήση εργαλείων Linux για imaging. Υπάρχει ποικιλία εργαλείων που παρέχουν δυνατότητες write-blocking και δημιουργίας εικόνων, συχνά ανοιχτού κώδικα.

6.12. Linux Imaging

Ο συνδυασμός μιας διανομής Linux και μιας εκκινήσιμης (bootable) συσκευής USB αποτελεί μια επιλογή που μπορεί να χρησιμοποιηθεί για τη δικαστική αποτύπωση δίσκων συστημάτων που μπορεί να έχουν παραβιαστεί. Οι αναλυτές αντιμετώπισης περιστατικών μπορεί να βρεθούν σε μια κατάσταση όπου χρειάζεται να αποτυπώσουν πολλαπλά συστήματα, ενώ διαθέτουν μόνο έναν *write blocker*. Θα χαθεί πολύς χρόνος αν ο αναλυτής πρέπει να αποτυπώσει καθένα από αυτά τα συστήματα με σειρά. Σε αυτή την περίπτωση, ο αναλυτής μπορεί να το αποφύγει δημιουργώντας μια εκκινήσιμη USB συσκευή για κάθε σύστημα και αποτυπώνοντας ταυτόχρονα όλα τα συστήματα. Το μόνο που χρειάζεται είναι ένας δίσκος αποθήκευσης αποδεικτικών στοιχείων και μια εκκινήσιμη USB για κάθε πηγή αποδεικτικών στοιχείων. Χρησιμοποιώντας αυτή την τεχνική, ο αναλυτής μπορεί να αποτυπώσει τα συστήματα ταυτόχρονα, εξοικονομώντας χρόνο που μπορεί να αξιοποιηθεί σε άλλες δραστηριότητες.

Σε αυτό το σενάριο, η διανομή Linux **CAINE (Computer Aided INvestigative Environment Live)** θα χρησιμοποιηθεί για την αποτύπωση του σκληρού δίσκου ενός ενδεχομένως παραβιασμένου συστήματος. Αρχικά, το σύστημα τερματίζεται και τοποθετείται η εκκινήσιμη USB συσκευή που περιέχει το λειτουργικό CAINE. Στη συνέχεια, το ύποπτο σύστημα ενεργοποιείται. Οι αναλυτές αντιμετώπισης περιστατικών πρέπει να γνωρίζουν πώς να αλλάξουν τη σειρά εκκίνησης ενός συστήματος ώστε να εκκινήσει από την USB συσκευή. Επίσης, πρέπει να είναι έτοιμοι να απενεργοποιήσουν αμέσως το σύστημα αν προσπαθήσει να εκκινήσει το εγγενές OS και όχι την USB συσκευή. Ας ξεκινήσουμε:

1. Τερματίστε το ύποπτο σύστημα και ενεργοποιήστε το ξανά. Μόλις εκκινήσει η συσκευή, τοποθετήστε τον δίσκο αποδεικτικών στοιχείων σε μια άλλη διαθέσιμη θύρα USB. Αν ο δίσκος αποδεικτικών στοιχείων δεν διαθέτει εκκινήσιμο λειτουργικό σύστημα, μπορεί να προκύψουν προβλήματα καθώς η ακολουθία εκκίνησης μπορεί να προσπαθήσει να βρει έγκυρο OS σε αυτόν τον δίσκο. Για αυτό είναι απαραίτητο να περιμένετε μέχρι να εκκινήσει το Linux OS που χρησιμοποιείται.

2. Αφού εισαχθεί ο δίσκος αποδεικτικών στοιχείων, ανοίξτε ένα Terminal και πληκτρολογήστε

```
:# fdisk -l
```

Η εντολή `fdisk -l` εμφανίζει όλες τις κατατμήσεις που είναι ορατές στο CAINE OS. Η συνοπτική έξοδος θα μοιάζει με την εξής:

Σε αυτό το παράδειγμα, υπάρχουν τρεις ξεχωριστοί δίσκοι, ο καθένας με τις δικές του κατατμήσεις. Ο δίσκος με ετικέτα `/dev/sdc` είναι η USB συσκευή που περιέχει το CAINE OS και από την οποία έχει εκκινηθεί το σύστημα. Ο δίσκος `/dev/sdd` είναι ο δίσκος αποδεικτικών στοιχείων στον οποίο θα γίνει η αποτύπωση. Τέλος, το σύστημα-στόχος αναγνωρίζεται ως `/dev/sdb`. Είναι σημαντικό να αναγνωρίζονται οι ξεχωριστοί δίσκοι για να βεβαιωθείτε ότι ο σωστός δίσκος αποτυπώνεται. Εξετάζοντας πιο προσεκτικά το `/dev/sdb`, ο αναλυτής μπορεί να δει τις τρεις ξεχωριστές κατατμήσεις που αποτελούν τον φυσικό όγκο. Το CAINE υποδεικνύει τον εκκινήσιμο τόμο `/dev/sdb1` με αστερίσκο. Αυτή η πληροφορία είναι χρήσιμη καθώς το CAINE μπορεί να χρησιμοποιηθεί είτε για την αποτύπωση ολόκληρου του φυσικού δίσκου, όπως στο παράδειγμα, είτε συγκεκριμένων λογικών τόμων.

```
Disk /dev/sdb: 465.8 GiB, 500107862016 bytes, 976773168 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disklabel type: dos
Disk identifier: 0x345601e6

Device      Boot      Start        End    Sectors    Size Id Type
/dev/sdb1   *            2048    1026047    1024000    500M  7 HPFS/NTFS/exFAT
/dev/sdb2             1026048  975847423  974821376  464.9G  7 HPFS/NTFS/exFAT
/dev/sdb3             975847424  976769023    921600    450M 27 Hidden NTFS WinRE

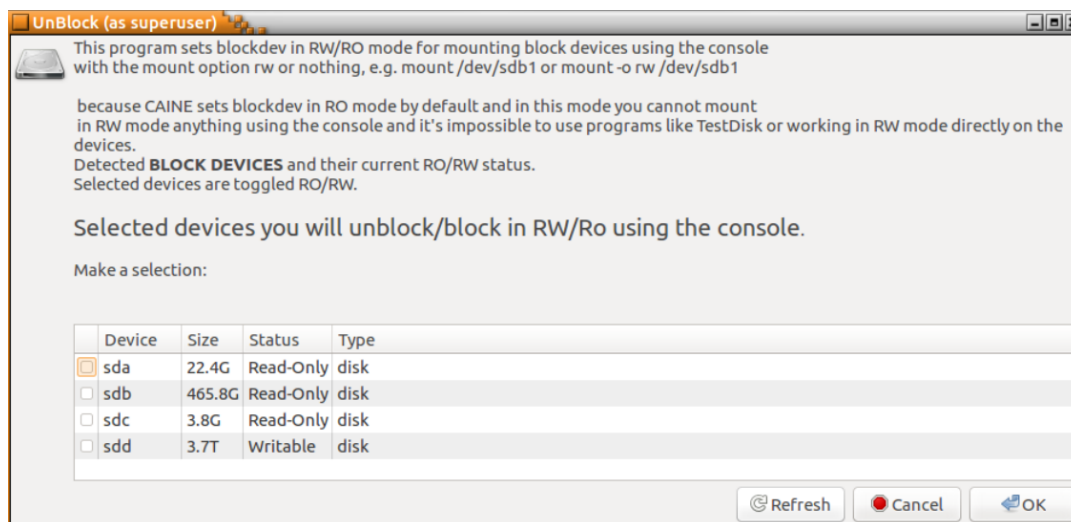
Disk /dev/sdc: 3.8 GiB, 4060086272 bytes, 7929856 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x000f1d04

Device      Boot      Start        End    Sectors    Size Id Type
/dev/sdc1   *            2048  7929855  7927808    3.8G  c W95 FAT32 (LBA)

Disk /dev/sdd: 3.7 TiB, 4000787029504 bytes, 7814037167 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 33553920 bytes
Disklabel type: gpt
Disk identifier: 30B0BF34-42D8-41E5-A90C-E5735893CFB6

Device      Start        End    Sectors    Size Type
/dev/sdd1     34      262177    262144    128M Microsoft reserved
/dev/sdd2  264192  7814035455  7813771264  3.7T Microsoft basic data
```

3. Αφού εντοπιστεί ο σωστός δίσκος-στόχος, είναι κρίσιμο η διαδικασία αποτύπωσης να μην τροποποιήσει δεδομένα του συστήματος-στόχου. Το CAINE OS διαθέτει ενσωματωμένο λογισμικό *write blocker*. Στην επιφάνεια εργασίας θα βρείτε το "Block on/off", που ανοίγει τον λογισμικό write blocker που θα χρησιμοποιηθεί.



Εξετάζοντας τη λίστα των συσκευών, θα δείτε ότι η μόνη εγγράψιμη συσκευή είναι η sdd, που έχουμε προσδιορίσει ως δίσκο αποδεικτικών στοιχείων. Οι άλλοι δίσκοι έχουν οριστεί ως μόνο για ανάγνωση (read-only). Αυτό διασφαλίζει ότι η διαδικασία αποτύπωσης δεν θα τροποποιήσει τον δίσκο-στόχο. Συνιστάται οι αναλυτές να τραβήξουν ένα στιγμιότυπο οθόνης αυτής της πληροφορίας για μελλοντική αναφορά.

- Αφού βεβαιωθείτε ότι ο δίσκος αποδεικτικών στοιχείων είναι στη θέση του και το σύστημα-στόχος έχει οριστεί σε read-only, ο αναλυτής πρέπει να ρυθμίσει τον δίσκο αποδεικτικών ώστε να είναι σωστά προσαρτημένος (mounted). Πρώτα, δημιουργήστε έναν κατάλογο EvidenceDrive1 ως κατάλογο mnt:

```
:# sudo mkdir /mnt/EvidenceDrive1
```

- Στη συνέχεια, προσαρτήστε τον δίσκο sdd σε αυτόν τον κατάλογο:

```
:# sudo mount /dev/sdd2 /mnt/EvidenceDrive1/
```

Τώρα ο δίσκος αποδεικτικών στοιχείων είναι προσαρτημένος στο σημείο mount που δημιουργήθηκε.

- Αλλάξτε κατάλογο στον δίσκο αποδεικτικών:

```
:# cd /mnt/EvidenceDrive1/
```

- Δημιουργήστε έναν κατάλογο που θα περιέχει το αρχείο εικόνας. Στο παράδειγμα, ο κατάλογος θα ονομαστεί με τον αριθμό υπόθεσης, π.χ. Case2017-01:

```
:# mnt/EvidenceDrive1$ mkdir Case2017-01
```

- Μεταβείτε στον νέο κατάλογο:

```
:# mnt/EvidenceDrive1$ cd Case2017-01/
```

9. Τώρα είστε έτοιμοι να αποτυπώσετε το δίσκο-στόχο. Υπάρχουν πολλά εργαλεία για αυτό. Στο παράδειγμα χρησιμοποιείται το **Dc3dd**, που αναπτύχθηκε από τον Jesse Kornblum του Department of Defense Cyber Crime Center. Παρέχει επιπλέον δυνατότητες σε σχέση με την εντολή dd, όπως αναφορές σφαλμάτων και πολλαπλούς αλγόριθμους κατακερματισμού (hash) που μπορούν να χρησιμοποιηθούν on-the-fly. Η εντολή είναι:

```
:# mnt/EvidenceDrive1/Case2017-01$ dc3dd if=/dev/sdb of=ideapad.img hash=md5 log=dc3ddlog.txt
```

```
caine@caine:/mnt/EvidenceDrive1/Case2017-01$ sudo dc3dd if=/dev/sdb of=ideapad.img hash=md5 log=dc3ddlog.txt

dc3dd 7.2.641 started at 2017-04-02 19:18:35 +0100
compiled options:
command line: dc3dd if=/dev/sdb of=ideapad.img hash=md5 log=dc3ddlog.txt
device size: 976773168 sectors (probed), 500,107,862,016 bytes
sector size: 512 bytes (probed)
■ 6376849408 bytes ( 5.9 G ) copied ( 1% ), 58 s, 105 M/s
```

Αυτή η εντολή αποτυπώνει το δίσκο sdb στον δίσκο αποδεικτικών ideapad.img, υπολογίζει το hash MD5 και δημιουργεί ένα αρχείο log dc3ddlog.txt για αναφορά.

10. Ανάλογα με το μέγεθος του δίσκου, η διαδικασία μπορεί να διαρκέσει ώρες. Κατά τη διάρκεια αυτής, ο αναλυτής μπορεί να παρακολουθεί την πρόοδο. Στο τέλος, εμφανίζεται η έξοδος με τους τομείς που χρησιμοποιήθηκαν και το MD5 hash της εικόνας.

```
dc3dd 7.2.641 started at 2017-04-02 19:18:35 +0100
compiled options:
command line: dc3dd if=/dev/sdb of=ideapad.img hash=md5 log=dc3ddlog.txt
device size: 976773168 sectors (probed), 500,107,862,016 bytes
sector size: 512 bytes (probed)
500107862016 bytes ( 466 G ) copied ( 100% ), 5854 s, 81 M/s

input results for device `/dev/sdb':
976773168 sectors in
0 bad sectors replaced by zeros
d48a7ccafae6fab7d284b4be300bd8 (md5)

output results for file `ideapad.img':
976773168 sectors out

dc3dd completed at 2017-04-02 20:56:09 +0100
```

11. Εξετάζοντας το δίσκο αποδεικτικών σε ένα σύστημα Windows, φαίνονται τα δημιουργημένα αρχεία εικόνας και log.

★	dc3ddlog	4/2/2017 12:56 PM	Text Document	2 KB
★	ideapad	4/2/2017 12:56 PM	Disc Image File	488,386,58...

12. Το αρχείο log περιέχει πληροφορίες που πρέπει να συμπεριληφθούν σε οποιαδήποτε αναφορά.

```
dc3dd 7.2.641 started at 2017-04-02 19:18:35 +0100
compiled options:
```

```
command line: dc3dd if=/dev/sdb of=ideapad.img hash=md5
log=dc3ddlog.txt
device size: 976773168 sectors (probed), 500,107,862,016 bytes
sector size: 512 bytes (probed)
500107862016 bytes ( 466 G ) copied ( 100% ), 5854.43 s, 81 M/s
input results for device `/dev/sdb': 976773168 sectors in
0 bad sectors replaced by zeros d48a7ccafaeadd6fab7d284b4be300bd8
(md5)
output results for file `ideapad.img': 976773168 sectors out
dc3dd completed at 2017-04-02 20:56:09 +0100
```

Το Linux αποτελεί μια βιώσιμη επιλογή όσον αφορά την απόκτηση αποδεικτικών στοιχείων από δίσκους. Ένα σημαντικό πλεονέκτημά του είναι ότι είναι εύκολο στη κλιμάκωση. Σε περίπτωση που χρειάζεται να αποκτηθούν δεδομένα από πολλαπλά συστήματα, οι υπεύθυνοι μπορούν να χρησιμοποιήσουν πολλαπλές USB μονάδες αποθήκευσης και συσκευές USB με Linux και να τις αποκτήσουν παράλληλα, αντί να περιμένουν να είναι διαθέσιμο κάποιο λογισμικό. Το CAINE αποτελεί εξαιρετική επιλογή για αυτό, καθώς ο ενσωματωμένος write blocker προσφέρει επίσης ένα επίπεδο ακεραιότητας των αποδεικτικών στοιχείων κατά τη διαδικασία.

Η δημιουργία εικόνας δίσκου (imaging) είναι μια κρίσιμη διαδικασία που πρέπει να κατανοούν οι υπεύθυνοι. Το περιστατικό θα καθορίσει συχνά ποια τεχνική πρέπει να χρησιμοποιηθεί. Σε κάθε περίπτωση όμως, οι υπεύθυνοι πρέπει να διασφαλίζουν ότι η διαδικασία διεξάγεται με σωστό τρόπο, καθώς οι μελλοντικές έρευνες συχνά βασίζονται στα δεδομένα που αποκτήθηκαν από αυτά τα συστήματα.

Δεν θα απαιτεί κάθε περιστατικό τη λήψη εικόνας από έναν πιθανώς παραβιασμένο σκληρό δίσκο ή άλλο όγκο δεδομένων. Παρ' όλα αυτά, οι αναλυτές αντιμετώπισης περιστατικών πρέπει να είναι εξοικειωμένοι με αυτή τη διαδικασία και ικανοί να την εκτελέσουν όταν χρειαστεί. Τα αποδεικτικά στοιχεία που βρίσκονται σε έναν σκληρό δίσκο μπορεί να είναι κρίσιμα για τον καθορισμό μιας αλληλουχίας γεγονότων ή για την απόκτηση αρχείων που μπορούν να βοηθήσουν στον εντοπισμό της βασικής αιτίας ενός περιστατικού. Αυτός είναι ο βασικός λόγος για τον οποίο οι υπεύθυνοι πρέπει να κατανοούν τα θεμελιώδη στοιχεία της δημιουργίας εικόνας δίσκου, καθώς και τα εργαλεία και τις διαδικασίες που εμπλέκονται: πώς να δημιουργούν μια staging drive, πώς να χρησιμοποιούν write blockers και πώς να εκτελούν οποιαδήποτε από τις τεχνικές imaging που αναφέρθηκαν σε αυτό το κεφάλαιο. Όπως σε κάθε διαδικασία που εκτελείται σε ένα εγκληματολογικό πλαίσιο, η δημιουργία εικόνας δίσκου πρέπει να γίνεται με συστηματικό τρόπο, ακολουθώντας όλα τα βήματα και καταγράφοντας σωστά τη διαδικασία. Αυτό διασφαλίζει ότι οποιαδήποτε αποδεικτικά στοιχεία αποκτηθούν θα είναι έγκυρα και αποδεκτά στο δικαστήριο.

7

Ανάλυση Δικτυακών Αποδεικτικών Στοιχείων

Το Κεφάλαιο 4, *Συλλογή Δικτυακών Αποδεικτικών Στοιχείων*, ανέλυσε πώς οι αναλυτές ασφαλείας και οι διαχειριστές περιστατικών μπορούν να αποκτήσουν αποδεικτικά στοιχεία που βασίζονται σε δίκτυα για μετέπειτα αξιολόγηση. Το κεφάλαιο αυτό επικεντρώθηκε σε δύο κύριες πηγές αυτών των στοιχείων: τα αρχεία καταγραφής δικτύου και τις καταγραφές πακέτων (packet captures). Στο παρόν κεφάλαιο θα παρουσιαστούν τα εργαλεία και οι τεχνικές που είναι διαθέσιμες για την εξέταση των συλλεγμένων αποδεικτικών στοιχείων. Η ενσωμάτωση αυτών των τεχνικών σε μια έρευνα αντιμετώπισης περιστατικού μπορεί να παρέχει στους αναλυτές σημαντική εικόνα σχετικά με τη δραστηριότητα στο δίκτυο από πιθανούς απειλητικούς παράγοντες. Στο κεφάλαιο αυτό θα καλυφθούν τα ακόλουθα κύρια θέματα:

- **Επισκόπηση δικτυακών αποδεικτικών στοιχείων:** Οι αντίπαλοι (adversaries) δεσμεύονται από τα ίδια πρωτόκολλα δικτύου που διέπουν την κανονική δικτυακή κίνηση. Αντιμετωπίζονται τεχνικές που μπορούν να εντοπιστούν μέσω της σωστής ανάλυσης των δικτυακών δεδομένων.
- **Ανάλυση αρχείων καταγραφής firewall και proxy:** Οι αντίπαλοι χρειάζονται αρχική και συνεχή σύνδεση με την υποδομή τους. Συσκευές δικτύου όπως firewalls και proxies μπορούν να παρέχουν αποδεικτικά στοιχεία από τα αρχεία καταγραφής.
- **NetFlow:** Το NetFlow περιγράφει δεδομένα για τις συνδέσεις μεταξύ συσκευών στο δίκτυο. Χρησιμοποιείται κυρίως για την επίλυση προβλημάτων σύνδεσης και εύρους ζώνης, αλλά μπορεί επίσης να προσφέρει στους αναλυτές εικόνα σχετικά με τη ροή δεδομένων κατά τη διάρκεια ενός περιστατικού.
- **Καταγραφές πακέτων (packet captures):** Μία από τις καλύτερες πηγές αποδεικτικών στοιχείων κατά τη διάρκεια ενός περιστατικού είναι οι καταγραφές πακέτων. Η ανάλυσή τους μπορεί να αποκαλύψει εξαγωγή δεδομένων, εκμεταλλεύσεις (exploits) και εντολές και έλεγχο (command and control).

7.1. Επισκόπηση δικτυακών αποδεικτικών στοιχείων

Στο Κεφάλαιο 4, υπήρξε εστίαση στις διάφορες πηγές αποδεικτικών στοιχείων που παράγουν οι δικτυακές συσκευές. Τα περισσότερα αποδεικτικά στοιχεία περιέχονται σε διάφορα αρχεία καταγραφής που παράγονται από switches, routers και firewalls. Ανάλογα με το είδος του

περιβάλλοντος, αυτά τα στοιχεία μπορούν να ενισχυθούν με δεδομένα NetFlow και πλήρεις καταγραφές πακέτων.

Μόλις κατανοηθούν οι διάφορες πηγές, είναι σημαντικό να εξεταστεί τι μπορούν να αποκαλύψουν τα αρχεία καταγραφής, το NetFlow και οι καταγραφές πακέτων σχετικά με ένα περιστατικό. Μερικές περιοχές εστίασης περιλαμβάνουν:

- **Συμπεριφορά αναγνώρισης και σάρωσης:** Υπάρχει πληθώρα εργαλείων που χρησιμοποιούν οι αντίπαλοι για αυτοματοποιημένη σάρωση συσκευών περιμέτρου όπως firewalls και routers. Αυτές οι σαρώσεις αφήνουν ίχνη, καθώς απαιτούν συνδέσεις με τις συσκευές. Ανάλογα με το επίπεδο καταγραφής και την περίοδο διατήρησης, οι αναλυτές μπορούν να εντοπίσουν την εξωτερική υποδομή που προσπαθεί να παραβιάσει τα συστήματα περιμέτρου.
- **Αρχική μόλυνση:** Οι αντίπαλοι χρησιμοποιούν συχνά πολυσταδιακές εκμεταλλεύσεις και κακόβουλο λογισμικό. Το πρώτο στάδιο συνδέεται με εξωτερική υποδομή μέσω URL και κατεβάζει επιπλέον εκμεταλλεύσεις. Οι web proxies και τα firewalls μπορεί να περιέχουν στοιχεία σύνδεσης στα αρχεία καταγραφής τους.
- **Πλευρική κίνηση (Lateral movement):** Μόλις εισέλθουν στο δίκτυο, οι αντίπαλοι προσπαθούν να διεξάγουν reconnaissance, να εκμεταλλευτούν άλλα συστήματα και να μεταφέρουν δεδομένα. Τα αρχεία NetFlow παρέχουν εικόνα για αυτή τη συμπεριφορά.
- **Command and control:** Αφού εγκατασταθεί πρόσβαση στο δίκτυο, οι αντίπαλοι χρειάζονται τη δυνατότητα να διατηρούν έλεγχο στα συστήματα. Αρχεία καταγραφής, καταγραφές πακέτων και δεδομένα NetFlow μπορούν να χρησιμοποιηθούν για τον εντοπισμό αυτής της συμπεριφοράς.
- **Εξαγωγή δεδομένων (Data exfiltration):** Ένας στόχος των αντιπάλων μπορεί να είναι η εξαγωγή δεδομένων. Τα αρχεία proxy μπορούν να δείξουν τον προορισμό αυτών των δεδομένων. Το NetFlow μπορεί να δείξει τη ροή δεδομένων από τα εσωτερικά σε εξωτερικά συστήματα. Οι καταγραφές πακέτων μπορούν να χρησιμοποιηθούν για να προσδιοριστούν τα αρχεία, η προέλευση και ο προορισμός τους.

Ανάλυση αρχείων καταγραφής firewall και proxy

Στο Κεφάλαιο 4 περιγράφηκε η συλλογή δικτυακών αποδεικτικών στοιχείων και τα αρχεία καταγραφής που είναι σημαντικά για έναν αναλυτή ασφαλείας. Εκτός από τις καταγραφές πακέτων, μεγάλη έμφαση δόθηκε στη συλλογή αρχείων καταγραφής από διάφορες πηγές, τα οποία μπορούν να παρέχουν ενδείξεις συμβάντων που βοηθούν σε μια έρευνα. Η κύρια πρόκληση για τους αναλυτές είναι η διάκριση των σημαντικών αρχείων καταγραφής ανάμεσα σε μεγάλο όγκο άσχετων δεδομένων.

Μερικές μέθοδοι ανάλυσης περιλαμβάνουν:

- **Χειροκίνητη ανασκόπηση αρχείων καταγραφής:** Τα αρχεία καταγραφής φορτώνονται σε ένα εργαλείο όπως ένας επεξεργαστής κειμένου και εξετάζονται γραμμή προς γραμμή. Χαμηλού κόστους μέθοδος, χρήσιμη μόνο για περιορισμένα δεδομένα.
- **Φιλτραρισμένη ανασκόπηση:** Τα εργαλεία ανάλυσης καταγραφών επιτρέπουν φιλτράρισμα με βάση συγκεκριμένες παραμέτρους, όπως γνωστή κακόβουλη δραστηριότητα. Ωστόσο, τα αρχεία καταγραφής δεν εμφανίζουν πάντα άμεσα τις κακόβουλες ενέργειες.
- **Αναζήτηση αρχείων καταγραφής:** Τα περισσότερα εργαλεία επιτρέπουν αναζήτηση με εκφράσεις regex ή Boolean για συγκεκριμένο χρονικό διάστημα, διεύθυνση IP ή άλλη συνθήκη.
- **Συσχέτιση αρχείων καταγραφής:** Διαχωρισμένες δραστηριότητες μπορούν να συσχετιστούν με άλλα logs μέσω προκαθορισμένων κανόνων ή αλγορίθμων, συνήθως ενσωματωμένων σε πλατφόρμες SIEM.
- **Εξόρυξη δεδομένων (Data mining) από αρχεία καταγραφής:** Εξαγωγή νοήματος και μεγαλύτερου πλαισίου για συγκεκριμένες δραστηριότητες. Υπάρχουν εργαλεία όπως Elasticsearch και Logstash που παρέχουν πλατφόρμες για χρήσιμες πληροφορίες.

Ο όγκος των αρχείων καταγραφής σε ένα μήνα μπορεί να είναι τεράστιος, ειδικά με την προσθήκη νέων πηγών. Η χειροκίνητη επεξεργασία είναι σχεδόν αδύνατη, γι' αυτό η χρήση εργαλείων αυτοματοποίησης, ακόμη και σε μικρά δίκτυα, είναι κρίσιμη για τον εντοπισμό των κρίσιμων στοιχείων.

7.2. DNS Blacklists

Μία τεχνική που συνδυάζει φιλτράρισμα και χειροκίνητη ανασκόπηση αρχείων καταγραφής είναι η χρήση γλωσσών scripting όπως η Python. Αυτά τα scripts μπορούν να επεξεργαστούν αρχεία καταγραφής firewall ή άλλες εισόδους, ώστε να επισημάνουν συγκεκριμένα σημεία ενδιαφέροντος για τον αναλυτή. Ένα τέτοιο script είναι το **DNS blacklists**, διαθέσιμο στη διεύθυνση: <https://bitbucket.org/ethanr/dns-blacklists/>.

Αυτό το script παίρνει ένα αρχείο κειμένου που δημιουργείται από την πηγή των αρχείων καταγραφής ή από τον αναλυτή και το συγκρίνει με λίστες IP διευθύνσεων και domains που έχουν προστεθεί σε blacklists.

Ο φάκελος που περιέχει το script περιέχει επίσης δύο άλλους φακέλους που συγκρίνονται μεταξύ τους. Ένας φάκελος περιέχει τα αρχεία κειμένου με blacklists από IP και domains. Αυτές οι blacklists μπορούν να προέρχονται από ανοιχτές πηγές ή από παρόχους πληροφοριών απειλών (threat intelligence). (Το Κεφάλαιο 13, **Leveraging Threat Intelligence**, εξηγεί πώς μπορούν να αξιοποιηθούν οι πηγές threat intelligence για incident response.) Το script εκτελεί τους ύποπτους καταγραφόμενους φακέλους ή IP διευθύνσεις ενάντια στις blacklists για να διαπιστωθεί αν υπάρχουν ταιριάσματα.

Στο παρακάτω παράδειγμα, μία λίστα με γνωστές διευθύνσεις URL και IP του Emotet πρόκειται να συγκριθεί με ένα αρχείο καταγραφής firewall που έχει ληφθεί. Μόλις τοποθετηθούν τα δεδομένα στους κατάλληλους φακέλους, εισάγεται η παρακάτω εντολή στο Terminal:

```
:# python dns_blacklists.py bad_lists/ traffic_directory/
```

Αυτή η εντολή εκτελεί το script χρησιμοποιώντας τις blacklists του Emotet που περιέχονται στον φάκελο **Bad Lists** ενάντια στα αρχεία καταγραφής ή στις IP διευθύνσεις που βρίσκονται στο φάκελο **Traffic Directory**. Η εντολή παράγει την εξής έξοδο:

```
Note: DNS resolution and reverse resolution is currently not supported.
Parsing blacklist files...
-----
EmotetIOC_01_17_19.txt
EmotetIOC_04_2019.txt
EmotetIOC_08_2019.txt

Parsing check files...
-----
Firewall Logs.txt

=====
The following hostnames were found in the blacklists:
=====
rozhan-hse.com
=====
The following IPs were found in the blacklists:
=====
```

Η έξοδος υποδεικνύει ότι το URL **rozhan-hse.com** βρέθηκε σε μία από τις blacklists IOC του Emotet. Το **DNS_Blacklists** είναι ένα χρήσιμο εργαλείο για αρχική αξιολόγηση αρχείων καταγραφής. Η αποτελεσματικότητα των αποτελεσμάτων εξαρτάται σε μεγάλο βαθμό από τα δεδομένα που περιέχονται στον φάκελο **Blacklist**. Όσο πιο ενημερωμένα και ακριβή είναι αυτά, τόσο καλύτερα θα είναι τα αποτελέσματα. Θετικά αποτελέσματα θα πρέπει να ακολουθούνται από περαιτέρω έρευνα.

7.3. SIEM tools

Στο Κεφάλαιο 4, **Συλλογή Δικτυακών Αποδεικτικών Στοιχείων**, έγινε επίσης αναφορά στη χρήση των πλατφορμών SIEM. Αυτές οι πλατφόρμες δεν χρησιμεύουν μόνο ως σημείο συγκέντρωσης των αρχείων καταγραφής από τις δικτυακές συσκευές, αλλά επιτρέπουν επίσης στους αναλυτές να εκτελούν ερωτήματα στα αρχεία που έχουν συγκεντρωθεί.

Για παράδειγμα, υπήρχαν IP διευθύνσεις που σχετίζονταν με πιθανή κακόβουλη δραστηριότητα, οι οποίες εντοπίστηκαν κατά την ανάλυση ενός αρχείου packet capture. Αυτό το αρχείο περιοριζόταν σε έναν μόνο υπολογιστή στο εσωτερικό δίκτυο. Ένα ερώτημα που θα ήθελαν να απαντήσουν οι αναλυτές είναι: πόσοι άλλοι υπολογιστές θα μπορούσαν πιθανώς να έχουν μολυνθεί; Εάν το SIEM συγκεντρώνει αρχεία καταγραφής συνδέσεων από συσκευές όπως το firewall που βλέπει προς το

εξωτερικό ή τον web proxy, ο αναλυτής θα μπορεί να προσδιορίσει εάν άλλοι εσωτερικοί υπολογιστές συνδέθηκαν σε αυτές τις ύποπτες IP διευθύνσεις.

Υπάρχει μεγάλη ποικιλία πλατφορμών SIEM, από δωρεάν λύσεις έως επιχειρησιακές πλατφόρμες διαχείρισης ασφάλειας. Οι περισσότερες από αυτές επιτρέπουν στους αναλυτές να πραγματοποιούν φιλτραρισμένες αναζητήσεις και συσχετίσεις στα αρχεία καταγραφής. Πολλές από τις πιο εξελιγμένες εμπορικές πλατφόρμες παρέχουν έτοιμα **rulesets** για την ανίχνευση συγκεκριμένων τύπων επιθέσεων και ενημερώσεις αυτών των κανόνων καθώς γίνονται γνωστές νέες επιθέσεις. Οι αναλυτές μπορούν επίσης να ερωτήσουν το SIEM για αρχεία καταγραφής συνδέσεων της IP διεύθυνσης ενός υπολογιστή προς οποιοδήποτε άλλο σύστημα. Αυτή η διαδικασία είναι συνήθης σε περιστατικά όπου ένα malware έχει μολύνει ένα μηχάνημα και ο επιτιθέμενος προσπαθεί να μολύνει άλλα μηχανήματα.

Σε οργανισμούς όπου το προσωπικό incident response είναι ξεχωριστό από εκείνους που έχουν την ευθύνη για τη συντήρηση του SIEM, είναι καλή πρακτική να αναθεωρηθεί η δομή επικοινωνίας, ώστε οι αναλυτές incident response να έχουν πρόσβαση σε αυτές τις πλατφόρμες. Ο πλούτος πληροφοριών και δεδομένων που είναι διαθέσιμος μπορεί να αξιοποιηθεί για να προσδιοριστεί ποια δραστηριότητα στο εσωτερικό δίκτυο συνδέεται με πιθανό περιστατικό, καθώς και ποια στοιχεία μπορούν να χρησιμοποιηθούν για τον προσδιορισμό της βασικής αιτίας.

7.3. Το Elastic Stack

Παράλληλα με την τεχνολογία SIEM, οι αναλυτές incident response μπορούν να αξιοποιήσουν ένα πακέτο εφαρμογών για ανάλυση αρχείων καταγραφής, γνωστό ως **Elastic Stack**. Το πακέτο αυτό συνδυάζει τρία εργαλεία που επιτρέπουν την ανάλυση μεγάλων συνόλων δεδομένων:

1. **Elasticsearch**: Είναι ένα εργαλείο αναζήτησης αρχείων καταγραφής που επιτρέπει σχεδόν σε πραγματικό χρόνο αναζητήσεις σε δεδομένα καταγραφής. Αυτό επιτυγχάνεται μέσω αναζήτησης πλήρους κειμένου (full-text search) με χρήση της Lucene. Επιτρέπει στους αναλυτές να κάνουν ερωτήματα σε αρχεία καταγραφής για στοιχεία όπως user IDs, IP διευθύνσεις ή αριθμούς καταγραφών. Ένα ακόμη σημαντικό χαρακτηριστικό του Elasticsearch είναι η δυνατότητα επέκτασης της λύσης καθώς η επιχείρηση μεγαλώνει και αποκτά περισσότερες πηγές δεδομένων.
2. **Logstash**: Αντιμετωπίζει την εισαγωγή αρχείων καταγραφής από διάφορες πηγές στο δίκτυο, επεξεργάζεται τις καταγραφές και επιτρέπει την εξαγωγή τους μέσω μιας πλατφόρμας οπτικοποίησης. Το Logstash μπορεί να ρυθμιστεί και να αναπτυχθεί εύκολα. Η ενσωμάτωσή του με το Elasticsearch παρέχει στους αναλυτές incident response τη δυνατότητα να πραγματοποιούν γρήγορα ερωτήματα σε μεγάλα σύνολα δεδομένων καταγραφής.
3. **Kibana**: Αποτελεί το οπτικό περιβάλλον ή dashboard του Elastic Stack. Επιτρέπει στους αναλυτές να αποκτούν εικόνα των δεδομένων μέσω dashboards και να εμβαθύνουν σε

συγκεκριμένα κρίσιμα δεδομένα για λεπτομερή ανάλυση. Οι αναλυτές μπορούν να προσαρμόσουν τα dashboards ώστε οι πιο κρίσιμες πληροφορίες, όπως logs ανίχνευσης εισβολών ή αρχεία καταγραφής συνδέσεων, να είναι άμεσα διαθέσιμες. Για παράδειγμα, το dashboard του Kibana χρησιμοποιεί κυκλικά διαγράμματα για να εμφανίζει δραστηριότητα αρχείων καταγραφής, προσφέροντας μια συνολική εικόνα στον αναλυτή.

Το Elastic Stack έχει καταστεί ένα ισχυρό εργαλείο για επαγγελματίες ασφάλειας και incident responders. Συνιστάται οι αναλυτές και οι επαγγελματίες incident response να μελετήσουν περισσότερους πόρους για να εξοικειωθούν με αυτή την τεχνολογία, καθώς είναι πολύ πιθανό να την συναντήσουν ξανά.

7.4. NetFlow

Το **NetFlow** είναι μια δυνατότητα που εισήγαγε πρώτη η Cisco Systems τη δεκαετία του 1990. Το NetFlow συλλέγει συγκεκριμένα δεδομένα σχετικά με τα πακέτα καθώς εισέρχονται ή εξέρχονται από μια διεπαφή ενός δρομολογητή ή ενός switch. Αυτά τα δεδομένα αποστέλλονται στη συνέχεια σε έναν **NetFlow Collector** μέσω ενός **NetFlow Exporter**, που συχνά αποτελεί μέρος των switches ή των δρομολογητών. Ο NetFlow Collector συγκεντρώνει και αποθηκεύει τα δεδομένα ροής για ανάλυση. Αυτά τα δεδομένα χρησιμοποιούνται συχνά από διαχειριστές δικτύων και συστημάτων για την αντιμετώπιση προβλημάτων εύρους ζώνης, την αναγνώριση συμφόρησης στο δίκτυο και την παρακολούθηση της ροής δεδομένων.

Στο επόμενο παράδειγμα περιλαμβάνεται μια δειγματική έξοδος NetFlow. Τα δεδομένα που περιλαμβάνονται σε κάθε ροή μπορεί να διαφέρουν ανάλογα με τον κατασκευαστή της συσκευής δικτύου, καθώς υπάρχουν διάφορες εκδόσεις στην αγορά. Η παρακάτω εικόνα δείχνει κάποιες από τις βασικές πληροφορίες που καταγράφονται σε ένα σύνολο δεδομένων NetFlow:

Src Addr	Dst Addr	Sport	Dport	Proto	Packets	Bytes	Flows
192.168.1.7	192.168.2.56	5734	22	tcp	42	3028	1
192.168.1.5	192.168.2.45	3687	22	tcp	52	2564	1
192.168.1.7	192.168.2.55	4675	22	tcp	1	1240	1
192.168.1.6	192.168.2.34	6897	22	tcp	46	4056	1
192.168.1.6	192.168.2.56	3657	445	tcp	325	56798	1

Στοιχεία μιας εγγραφής NetFlow που εμφανίζονται στο παράδειγμα:

- **Src Addr (Διεύθυνση Πηγής):** Η διεύθυνση που ξεκίνησε τη σύνδεση ή στέλνει την κυκλοφορία.
- **Dst Addr (Διεύθυνση Προορισμού):** Η διεύθυνση προορισμού για τη σύνδεση.
- **Sport (Θύρα Πηγής):** Η θύρα της πηγής.

- **Dport (Θύρα Προορισμού):** Η θύρα προορισμού. Στην ανάλυση NetFlow ως μέρος διερεύνησης περιστατικού, αυτό αποτελεί ένα από τα βασικά σημεία δεδομένων, καθώς δείχνει σε ποια υπηρεσία συνδέεται η διεύθυνση πηγής.
- **Proto (Πρωτόκολλο):** Το πρωτόκολλο που χρησιμοποιείται.
- **Packets (Πακέτα):** Ο αριθμός των πακέτων που αποτελούν τη ροή.
- **Bytes (Bytes):** Το συνολικό μέγεθος σε bytes.
- **Flows (Ροές):** Δείχνει πόσες ροές έχουν καταγραφεί.

Κατά την εξέταση των δεδομένων NetFlow στο παράδειγμα, δύο σημεία είναι ιδιαίτερα σημαντικά. Το πρώτο είναι ο αριθμός των **SSH συνδέσεων** μεταξύ συσκευών. Το Secure Shell είναι ένας συνηθισμένος τρόπος επικοινωνίας μεταξύ συστημάτων, αλλά αν αυτές οι συνδέσεις υπερβαίνουν τα όρια της κανονικής συμπεριφοράς του δικτύου, απαιτείται περαιτέρω διερεύνηση. Επιπλέον, οι συνδέσεις μέσω **SMB (Θύρα 445)** χρησιμοποιούνται συχνά από επιτιθέμενους για πρόσβαση σε άλλα συστήματα, παράδοση ransomware ή πρόσβαση σε κοινόχρηστους φακέλους. Ακόμη και σε αυτό το σύντομο παράδειγμα, γίνεται σαφές ότι οι αναλυτές αποκτούν σημαντική εικόνα απλώς παρακολουθώντας τις συνδέσεις στο εσωτερικό δίκτυο.

Υπάρχει μεγάλη ποικιλία εμπορικών εργαλείων για την προβολή των δεδομένων NetFlow. Η χρήση των δεδομένων NetFlow εξαρτάται σε μεγάλο βαθμό από τον οργανισμό. Η ρύθμιση του NetFlow δεν είναι κάτι που μπορεί να πραγματοποιηθεί εύκολα κατά τη διάρκεια ενός περιστατικού χωρίς πρόσβαση σε σημαντικούς πόρους από εμπορικούς παρόχους και προσωπικό εσωτερικών λειτουργιών. Παρ' όλα αυτά, οι αναλυτές που έχουν πρόσβαση σε NetFlow θα εξυπηρετηθούν σημαντικά αν εξοικειωθούν με την τεχνολογία, καθώς παρέχει πολύτιμη εικόνα για το πώς κινείται η κυκλοφορία στο δίκτυο.

7.5. Ανάλυση πακέτων δεδομένων (packet captures)

Μεγάλο μέρος του Κεφαλαίου 4, *Συλλογή Δικτυακών Αποδεικτικών Στοιχείων*, καλύπτει τις διάφορες μεθόδους απόκτησης πακέτων δεδομένων από πολλαπλές πηγές και τοποθεσίες. Τα πακέτα δεδομένων περιέχουν πολλές πληροφορίες που είναι δυνητικά πολύτιμες για τους αναλυτές αντίδρασης σε περιστατικά. Μερικές από αυτές τις πληροφορίες περιλαμβάνουν τις διευθύνσεις IP προέλευσης και προορισμού, τους τομείς (domains) και τις θύρες (ports), καθώς και το περιεχόμενο των επικοινωνιών μεταξύ των hosts. Σε ορισμένες περιπτώσεις, οι αναλυτές μπορούν να ανακατασκευάσουν πραγματικά αρχεία, όπως έγγραφα κειμένου και εικόνες, από αυτά τα πακέτα δεδομένων.

Το κεφάλαιο αναφέρεται σε διάφορα προκαθορισμένα πακέτα δεδομένων που εξετάζονται. Αυτά τα πακέτα έχουν ληφθεί απευθείας από το malware-traffic-analysis.net με την άδεια του συγγραφέα. Ο ιστότοπος διαθέτει αρκετές ασκήσεις με πακέτα δεδομένων, όπου οι αναλυτές αντίδρασης μπορούν

να εξασκηθούν στον εντοπισμό δεικτών συμβιβασμού (indicators of compromise). Θα πρέπει, όμως, να σημειωθεί ότι αυτά τα captures μπορεί να περιέχουν κακόβουλο λογισμικό. Οι αναγνώστες θα πρέπει να εξετάζουν τα ζωντανά captures μόνο σε σωστά διαμορφωμένο sandbox (βλ. Κεφάλαιο 12, Ανάλυση Κακόβουλου Λογισμικού για Αντίδραση σε Περιστατικά) ή σε άλλο σύστημα που δεν είναι συνδεδεμένο σε παραγωγικό περιβάλλον.

7.6. Εργαλεία γραμμής εντολών (Command-line tools)

Υπάρχουν διάφορα εργαλεία γραμμής εντολών που μπορούν να χρησιμοποιηθούν κατά την ανάλυση πακέτων δεδομένων. Σε πιο εκτεταμένες ή μακροχρόνιες περιπτώσεις αντίδρασης σε περιστατικά, οι αναλυτές μπορεί να συγκεντρώσουν πολλά αρχεία packet captures. Μπορεί να είναι χρήσιμο να συνδυάσουν αυτά τα captures σε ένα ενιαίο αρχείο για ευκολότερη ανάλυση. Η εφαρμογή *Mergecap* κάνει ακριβώς αυτό, συνδυάζοντας πολλά αρχεία packet captures. Το *Mergecap* παρέχεται ως μέρος του λειτουργικού CAINE και εκτελείται με την εξής εντολή:

```
:# mergecap -w mergedpacketcapture.pcap packetcapture1.pcap packetcapture2.pcap
```

Ένα άλλο εργαλείο γραμμής εντολών που είναι χρήσιμο για την ανάλυση packet captures είναι το *Editcap*. Το *Editcap* επιτρέπει στους αναλυτές να χειρίζονται τα αρχεία captures σε μικρότερα τμήματα για ευκολότερη εξέταση. Για παράδειγμα, ένας αναλυτής μπορεί να θέλει να δει captures χωρισμένα σε τμήματα των 50.000 πακέτων. Αυτό είναι χρήσιμο όταν το αρχείο είναι μεγάλο και η διαίρεση διευκολύνει την αναζήτηση. Η εντολή για αυτό είναι η εξής:

```
:# editcap -F pcap -c evidence.pcap split.pcap
```

Στην παραπάνω εντολή, το *Editcap* πήρε το αρχείο *evidence.pcap* και το διαιρεί σε τμήματα των 50.000 πακέτων. Μια άλλη δυνατότητα του *Editcap* είναι η διαίρεση ενός μεγάλου capture σε χρονικά τμήματα. Για παράδειγμα, αν οι αναλυτές θέλουν να χωρίσουν το capture σε διαστήματα 10 λεπτών, χρησιμοποιούν:

```
:# editcap -F pcap -t+600 evidence.pcap split.pcap
```

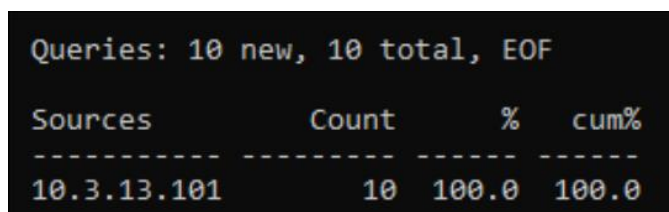
7.7. Ανάλυση κυκλοφορίας DNS

Σε ορισμένες περιπτώσεις, οι αναλυτές μπορεί να θέλουν να απομονώσουν την κυκλοφορία εγγραφής ονομάτων τομέων (domain name registration traffic). Αυτό είναι σημαντικό λόγω ποικίλων επιθετικών ενεργειών, όπως κυκλοφορία C2, εξαγωγή δεδομένων ή ανακατεύθυνση σε κατεστραμμένους ιστότοπους, συχνά εκμεταλλευόμενοι τρωτά σημεία στο DNS. Η εφαρμογή *dnstop* αναλύει αρχεία packet capture και προσδιορίζει τις πηγές και τον αριθμό των DNS queries από εσωτερικούς hosts. Για εγκατάσταση σε σύστημα Linux, χρησιμοποιείται η εντολή:

```
dfir@ubuntu:~$ sudo apt-get install dnstop
```

Αν ένας αναλυτής θέλει να δει αν κάποια IP διεύθυνση στέλνει εξερχόμενα DNS queries, εκτελεί:

```
dfir@ubuntu:~/Documents/Packet Captures$ dnstop 2019-03-13-Emotet-withTrickbot.pcap
```



```
Queries: 10 new, 10 total, EOF
```

Sources	Count	%	cum%
10.3.13.101	10	100.0	100.0

Η έξοδος δείχνει ότι μόνο ένας host είναι η πηγή των DNS queries, με σύνολο 10 queries. Αν και είναι ένα απλό παράδειγμα, οι αναλυτές μπορούν να συνδυάσουν πολλά αρχεία packet capture και να χρησιμοποιήσουν το dnstop για να κατανοήσουν καλύτερα ποια DNS κίνηση αφήνει το εσωτερικό δίκτυο και αν χρειάζεται περαιτέρω διερεύνηση.

7.8. Arkime

Το Arkime (παλιότερα Moloch) προσφέρει εκτεταμένες δυνατότητες καταγραφής και ανάλυσης δικτυακών δεδομένων, επιτρέποντας στους χρήστες να παρακολουθούν και να διερευνούν την κυκλοφορία του δικτύου σε πραγματικό χρόνο. Κύρια χαρακτηριστικά περιλαμβάνουν πλήρη καταγραφή πακέτων, ευρετηριασμένη αναζήτηση και εργαλεία οπτικοποίησης δεδομένων. Το Arkime καταγράφει την κυκλοφορία του δικτύου και την αποθηκεύει για λεπτομερή ανάλυση, δίνοντας στους χρήστες τη δυνατότητα να αναζητούν και να φιλτράρουν μεγάλους όγκους δεδομένων μέσω μιας διαδικτυακής διεπαφής.

Το εργαλείο παρέχει ισχυρές δυνατότητες οπτικοποίησης, παρουσιάζοντας τα δεδομένα σε διάφορες μορφές, όπως γραφήματα, πίνακες και χρονοδιαγράμματα. Αυτό βοηθά τους χρήστες να εντοπίζουν γρήγορα πρότυπα, ανωμαλίες και τάσεις στην κυκλοφορία του δικτύου. Επιπλέον, το Arkime υποστηρίζει tagging και ανακατασκευή συνεδριών, επιτρέποντας λεπτομερή ανάλυση και εγκληματολογικές έρευνες.

Το Arkime χρησιμοποιείται σε διάφορα σενάρια κυβερνοασφάλειας, όπως παρακολούθηση δικτύου, αντιμετώπιση περιστατικών και ανίχνευση απειλών. Επιτρέπει στους οργανισμούς να ανιχνεύουν και να αντιδρούν σε απειλές ασφάλειας σε πραγματικό χρόνο, να εντοπίζουν μη εξουσιοδοτημένη πρόσβαση και να παρακολουθούν ύποπτες δραστηριότητες.

Στην αντιμετώπιση περιστατικών, το Arkime μπορεί να χρησιμοποιηθεί για τη γρήγορη συλλογή και ανάλυση σχετικής κυκλοφορίας δικτύου, βοηθώντας τις ομάδες να κατανοήσουν την έκταση και τον αντίκτυπο ενός περιστατικού.

Επιπλέον, το Arkime είναι χρήσιμο για το threat hunting, επιτρέποντας στους αναλυτές να αναζητούν προληπτικά δείκτες συμβιβασμού και κακόβουλες δραστηριότητες στο δίκτυο. Οι εκτεταμένες

δυνατότητες διατήρησης και αναζήτησης δεδομένων το καθιστούν απαραίτητο εργαλείο για τον εντοπισμό και την έρευνα πιθανών απειλών ασφάλειας πριν κλιμακωθούν.

Παρόλο που το Arkime προσφέρει εκτεταμένα χαρακτηριστικά, έχει και περιορισμούς. Το εργαλείο απαιτεί σημαντικό χώρο αποθήκευσης για την πλήρη καταγραφή πακέτων, κάτι που μπορεί να είναι δαπανηρό και δύσκολο στη διαχείριση. Η απόδοση μπορεί να επηρεαστεί σε περιβάλλοντα με υψηλή κυκλοφορία, απαιτώντας σωστή ρύθμιση και βελτιστοποίηση του υλικού.

Η αποτελεσματικότητα του Arkime εξαρτάται επίσης από τις γνώσεις και την εμπειρία του χρήστη. Η κατανόηση πολύπλοκων πρωτοκόλλων δικτύου και η αναγνώριση κακόβουλων δραστηριοτήτων απαιτούν προηγμένες δεξιότητες. Επιπλέον, ενώ το Arkime παρέχει δυνατότητες καταγραφής και ανάλυσης δεδομένων, δεν περιλαμβάνει αυτοματοποιημένη ανίχνευση ή απόκριση απειλών, καθιστώντας απαραίτητη την ενσωμάτωση με άλλα εργαλεία ασφάλειας για μια ολοκληρωμένη στρατηγική.

Τα προηγμένα χαρακτηριστικά του Arkime περιλαμβάνουν ανάλυση κρυπτογραφημένης κυκλοφορίας, προσαρμοσμένα scripts parsing και ενσωμάτωση API. Οι χρήστες μπορούν να αναλύουν κρυπτογραφημένη κυκλοφορία ενσωματώνοντας το Arkime με εργαλεία αποκρυπτογράφησης SSL/TLS, επιτρέποντας την επιθεώρηση περιεχομένων πακέτων που κανονικά θα ήταν κρυφά.

Μπορούν επίσης να αναπτυχθούν προσαρμοσμένα scripts parsing για την επέκταση των δυνατοτήτων του Arkime, επιτρέποντας την εξαγωγή και ανάλυση δεδομένων από ιδιόκτητα ή ασυνήθιστα πρωτόκολλα.

Επιπλέον, το RESTful API του Arkime επιτρέπει αυτοματοποίηση και ενσωμάτωση με άλλα συστήματα, δίνοντας τη δυνατότητα στους χρήστες να κάνουν προγραμματισμένες αναζητήσεις δεδομένων, να δημιουργούν ειδοποιήσεις και να ξεκινούν καταγραφές. Αυτό αυξάνει την ευελιξία του Arkime και επιτρέπει προσαρμοσμένες λύσεις ασφάλειας.

Για τη μέγιστη αποτελεσματικότητα του Arkime, συνιστάται η τήρηση βέλτιστων πρακτικών, όπως τακτικές ενημερώσεις, διαχωρισμός δικτύου και έλεγχος πρόσβασης. Η διατήρηση του Arkime και των συστατικών του ενημερωμένων εξασφαλίζει προστασία από τις πιο πρόσφατες απειλές και πρόσβαση σε νέες δυνατότητες. Ο διαχωρισμός δικτύου μειώνει τον όγκο της κυκλοφορίας προς καταγραφή και ανάλυση, καθιστώντας τη διαδικασία πιο διαχειρίσιμη και αποτελεσματική.

Η σωστή διαμόρφωση ελέγχου πρόσβασης είναι κρίσιμη για την προστασία ευαίσθητων δεδομένων και τη διατήρηση της ακεραιότητας της ανάλυσης δικτυακής κυκλοφορίας. Περιορίστε την πρόσβαση στη διεπαφή και τα δεδομένα του Arkime μόνο σε εξουσιοδοτημένο προσωπικό και χρησιμοποιήστε ισχυρές μεθόδους πιστοποίησης για την ασφάλεια των λογαριασμών χρηστών.

Η ενσωμάτωση του Arkime με άλλα εργαλεία ασφάλειας ενισχύει τις δυνατότητές του και παρέχει πιο ολοκληρωμένη προσέγγιση στην ασφάλεια δικτύου. Συνδυάστε το Arkime με συστήματα ανίχνευσης εισβολών (IDS), συστήματα διαχείρισης πληροφοριών και συμβάντων ασφάλειας (SIEM)

και πλατφόρμες threat intelligence για συσχέτιση δεδομένων και βελτίωση της ανίχνευσης και απόκρισης απειλών.

Χρησιμοποιώντας το API του Arkime, ενσωματώστε το με εργαλεία αυτοματοποιημένης απόκρισης και συστήματα ticketing για να απλοποιήσετε τη διαδικασία αντιμετώπισης περιστατικών. Συνδυάζοντας τις λεπτομερείς πληροφορίες δικτύου του Arkime με άλλα εργαλεία ασφαλείας, οι οργανισμοί μπορούν να υιοθετήσουν μια στρατηγική πολυεπίπεδης άμυνας, βελτιώνοντας συνολικά την ασφάλειά τους.

Συχνές ερωτήσεις (Q&A):

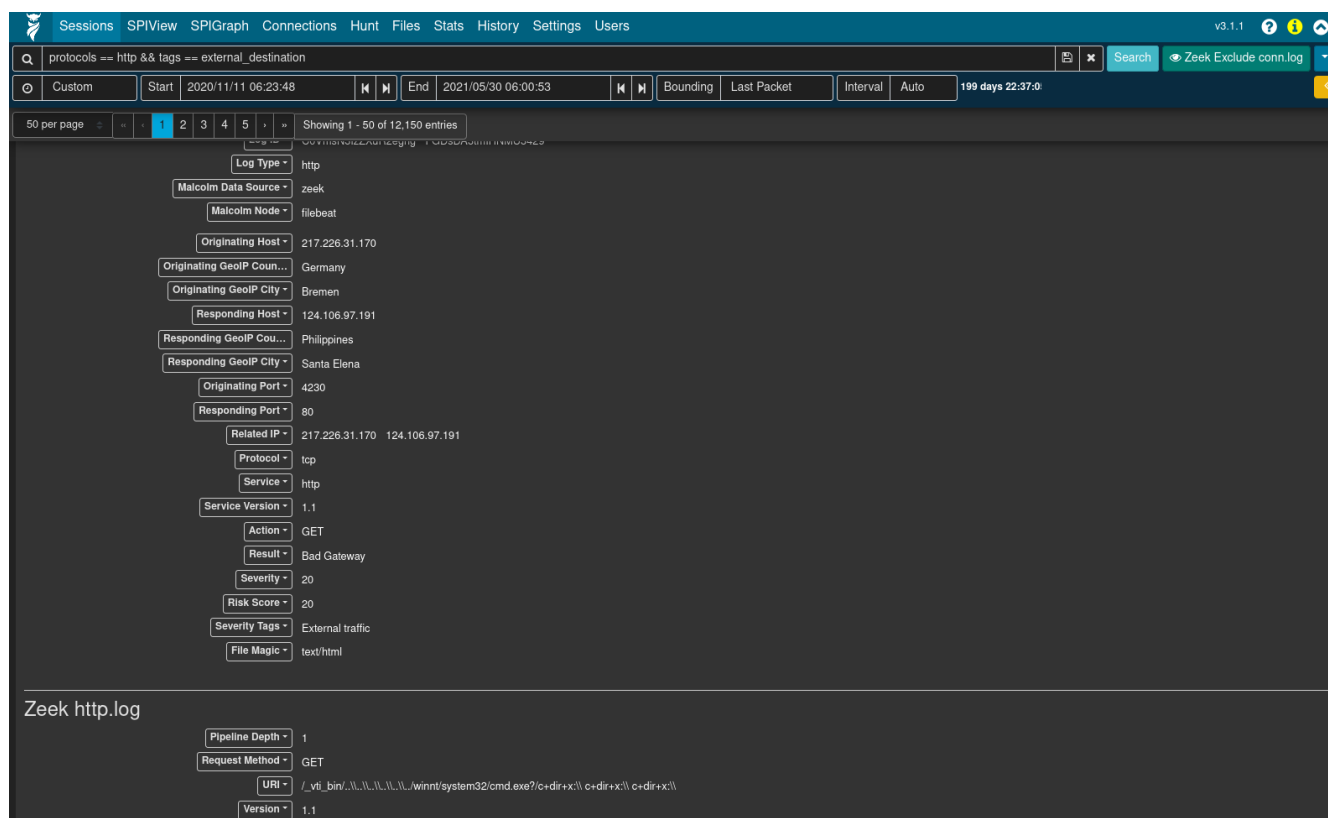
- **Μπορεί το Arkime να αναλύει κρυπτογραφημένη κυκλοφορία;** Ναι, το Arkime μπορεί να αναλύει κρυπτογραφημένη κυκλοφορία όταν ενσωματώνεται με εργαλεία αποκρυπτογράφησης SSL/TLS, επιτρέποντας την επιθεώρηση των περιεχομένων των πακέτων.
- **Πώς διαχειρίζεται το Arkime μεγάλους όγκους δεδομένων;** Το Arkime αποθηκεύει τα καταγεγραμμένα δεδομένα αποδοτικά και παρέχει εργαλεία διαχείρισης, όπως aging και συμπίεση δεδομένων. Ωστόσο, η διαχείριση μεγάλων όγκων δεδομένων απαιτεί επαρκή χώρο αποθήκευσης και σωστή διαμόρφωση.
- **Είναι το Arkime κατάλληλο για μικρές επιχειρήσεις;** Ναι, το Arkime μπορεί να προσαρμοστεί στις ανάγκες μικρών επιχειρήσεων, αν και απαιτεί σωστή εγκατάσταση και συντήρηση. Οι μικρές επιχειρήσεις θα πρέπει να αξιολογήσουν τον όγκο της κυκλοφορίας και τις δυνατότητες αποθήκευσης πριν την υλοποίηση.
- **Μπορεί το Arkime να ενσωματωθεί με άλλα εργαλεία κυβερνοασφάλειας;** Ναι, το Arkime μπορεί να ενσωματωθεί με πλήθος εργαλείων, όπως IDS, SIEM και πλατφόρμες threat intelligence, ενισχύοντας τις δυνατότητές του και προσφέροντας ολοκληρωμένη λύση ασφαλείας.
- **Πώς βελτιώνεται η απόδοση του Arkime σε περιβάλλοντα υψηλής κυκλοφορίας;** Η βελτίωση της απόδοσης περιλαμβάνει βελτιστοποίηση του υλικού, σωστή ρύθμιση των παραμέτρων του Arkime και εφαρμογή διαχωρισμού δικτύου για μείωση της καταγραφής περιττής κυκλοφορίας.

Μύθοι και αλήθειες:

- **M1:** Το Arkime είναι πλήρης λύση ασφαλείας → Λάθος. Είναι εργαλείο ανάλυσης δικτυακής κυκλοφορίας και πρέπει να ενσωματώνεται σε πολυεπίπεδη στρατηγική ασφαλείας.
- **M2:** Το Arkime μπορεί να αντικαταστήσει firewall → Λάθος. Δεν παρέχει φιλτράρισμα ή έλεγχο πρόσβασης, είναι για παρακολούθηση και ανάλυση κυκλοφορίας.
- **M3:** Το Arkime δεν χρειάζεται συντήρηση → Λάθος. Απαιτούνται τακτικές ενημερώσεις και ρυθμίσεις για βέλτιστη απόδοση.

- **M4:** Το Arkime προορίζεται μόνο για μεγάλες επιχειρήσεις → Λάθος. Μπορεί να προσαρμοστεί σε οργανισμούς οποιουδήποτε μεγέθους.
- **M5:** Η καταγραφή και αποθήκευση δεδομένων του Arkime είναι απεριόριστη → Λάθος. Περιορίζεται από τον φυσικό χώρο αποθήκευσης και τους πόρους του συστήματος.

Μια τυπική εγκατάσταση του Arkime εξάγει όλα τα μεταδεδομένα των δικτυακών συνδέσεων («συνεδρίες») («SPI» ή «Session Profile Information») από τα πλήρη αρχεία καταγραφής πακέτων (PCAP). Το Zeek παράγει παρόμοια μεταδεδομένα συνεδριών, συνδέοντας τα γεγονότα δικτύου με τις συνεδρίες μέσω ενός connection UID.



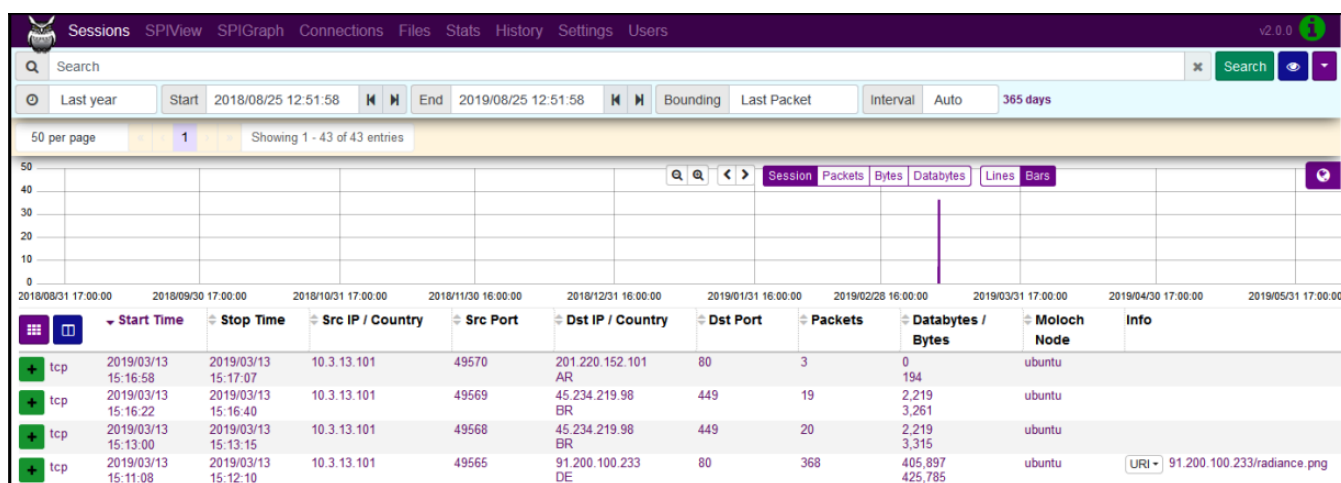
Το Moloch μπορεί να χρησιμοποιηθεί ως σύστημα παρακολούθησης δικτύου μέσω εισαγωγής πακέτων στην υποδομή **Elasticsearch**. Από εκεί, οι αναλυτές μπορούν να εξετάζουν τη δραστηριότητα του δικτύου σχεδόν σε πραγματικό χρόνο. Μία άλλη δυνατότητα του Moloch είναι η φόρτωση καταγραφών πακέτων εκτός σύνδεσης για ευρετηρίαση.

Οι οδηγίες εγκατάστασης του Moloch είναι διαθέσιμες στο <https://molo.ch/#download>. Το Moloch μπορεί να εγκατασταθεί σε διάφορες πλατφόρμες Linux, είτε σε desktop είτε σε server. Η επιλογή του server επιτρέπει σε μεγαλύτερες ομάδες να μοιράζονται δεδομένα σχετικά με τις καταγραφές πακέτων και να αξιολογούν καταγραφές που τρέχουν σε πραγματικό χρόνο. Οι εγκαταστάσεις σε desktop αποτελούν επιλογή για αναλυτές που διαχειρίζονται δεδομένα εκτός σύνδεσης και δεν χρειάζεται να μοιράζονται τα αποτελέσματα.

Για τις ανάγκες αυτού του κεφαλαίου, το Moloch θα χρησιμοποιηθεί για την εξέταση μιας καταγραφής πακέτων εκτός σύνδεσης, που λήφθηκε από το **Malware Traffic Analysis** στο <https://www.malware-traffic-analysis.net/2019/07/22/index.html>. Αρχικά, η καταγραφή πακέτων πρέπει να μεταφερθεί στο σύστημα Moloch. Αυτό μπορεί να γίνει μέσω οποιουδήποτε πελάτη **Secure File Transfer Protocol (SFTP)** απευθείας στον κατάλογο του Moloch: `/data/moloch/raw`. Στη συνέχεια, εκτελέστε την παρακάτω εντολή για να εισάγει το Moloch την καταγραφή:

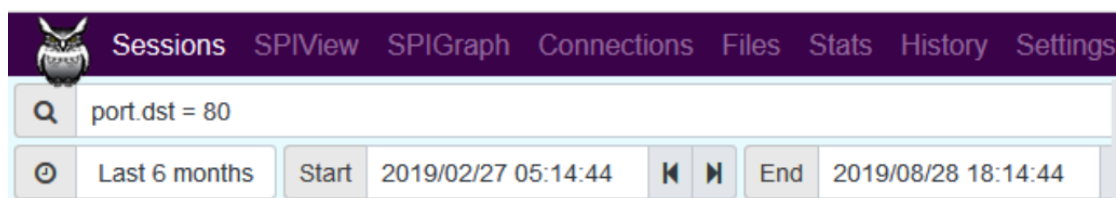
```
dfir@ubuntu:~/data/moloch/bi/moloch-capture -r /data/moloch/raw/2019-07-22-Amadey-infection-with-Pony-and-Ursnif-and-Cobalt-Strike.pcap
```

Αυτό θα επεξεργαστεί την καταγραφή εκτός σύνδεσης. Αφού ολοκληρωθεί, ανοίξτε ένα πρόγραμμα περιήγησης και πλοηγηθείτε στη διεύθυνση IP του server ή workstation στη θύρα 8005. Αυτό θα ανοίξει το περιβάλλον του Arkime.



Το Moloch είναι μια πλατφόρμα με πολλές δυνατότητες. Τα επόμενα βήματα παρέχουν μια επισκόπηση ορισμένων λειτουργιών για την εξέταση καταγραφών πακέτων εκτός σύνδεσης:

1. Από το dashboard, η εξέταση της καταγραφής πακέτων δείχνει διάφορες συνεδρίες όπου το εσωτερικό σύστημα με IP 10.3.13.101 επικοινωνεί με εξωτερικές διευθύνσεις IP. Για να περιοριστούν τα αποτελέσματα μόνο σε κίνηση HTTP στο διαδίκτυο, εισάγετε την αντίστοιχη αναζήτηση στη γραμμή αναζήτησης.



2. Ένας καλός τρόπος για να εντοπιστούν αρχεία μέσα σε μια καταγραφή πακέτων είναι να προσδιοριστεί ο αριθμός των πακέτων ανά συνεδρία. Κάντε κλικ στο βέλος κάτω από την κεφαλίδα της στήλης **Packets** για να ταξινομηθούν από τον μεγαλύτερο προς τον μικρότερο αριθμό πακέτων.

Dst IP / Country	Dst Port	Packets	Databytes / Bytes
83.220.141.232 DE	80	524	506,630 534,942
129.226.63.136 SG	80	291	246,151 261,881
31.44.184.33 RU	80	230	211,253 223,689
129.226.63.136 SG	80	221	195,452 207,402
31.44.184.33 RU	80	218	211,265 223,053

3. Στην δεξιά πλευρά του dashboard εμφανίζονται URLs και σχετικές πληροφορίες για τις συνεδρίες. Η ανάλυση των queries μέχρι τώρα δείχνει ότι αρκετά εκτελέσιμα αρχεία, συμπεριλαμβανομένου του αρχείου a22, φαίνεται να έχουν προσπελαστεί από το σύστημα υπό ανάλυση.

```

URI ▾ neu.x-sait.de/wp-content/plugins/mce-table-buttons/pp.exe
neu.x-sait.de/wp-content/plugins/mce-table-buttons/4.exe
URI ▾
cd.pranahat.at/webstore/zSR1Z6AnDI0PpsiGN_2F9W/7oYFSY47cH/9hfkJMvimgZEx3TIC/hR5_2BF3YKL1/WqZUwlQoia
O/9WGtTrqojm1Fpc/w4JGS_2BqOVVP9F5qP_2B/QcnCwcoZRFssnyQ8/6pxNROtgxS0JSSG/j_2B9TBJ5hwNSZU9f7/1ud
mNsp5a/TjPoAB3gEFw2yvZBcgGC/o1Z1ifT9HbS1Dg4Stts/AFZuGjnzHJzwDKC84R_2Fu/ZcUMga13Z/eNW1ffKY/VxS
URI ▾ 31.44.184.33/uDaB
URI ▾
x1.narutik.at/webstore/Wlpdq7f64iZDVkDP/nNIPLUwRF2LoqfY/E5R_2FJjib_2Ba2k97/bclDnPA_2/BkBxN61i7f8UEj0rGwAa
/dPKTXIMVsft1EHFq3EY/G9gCfV7T5wEjN4HML4X7pG/NOM985YvHHdzP/5Lcb8zEq/NMGJwwOWXxbU6a6_2FuMdbR/V
av0v2m3j2/4GXc_2FXtmWGU6mJ_/2Fn_2BLwcjuW/sYrlBoHcbMb/Xpu043fmlxCp/Uay
URI ▾ 31.44.184.33/H7mp
URI ▾ cd.pranahat.at/jvassets/o1/s64.dat
URI ▾ 31.44.184.33/visit.js
URI ▾ ectcnepal.org/wp-includes/customize/a22.exe

```

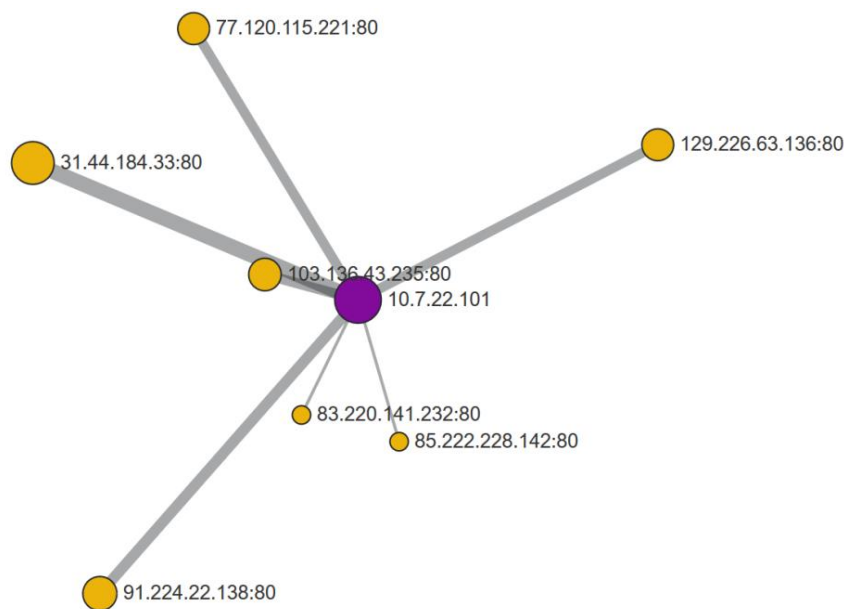
4. Το Moloch παρέχει επιπλέον πληροφορίες για κάθε συνεδρία. Στην ίδια σειρά με το info URL ectcnepal[.]org/wp-includes/customize/a22.exe, κάντε κλικ στο πράσινο πλαίσιο αριστερά για να ανοίξει η αντίστοιχη λεπτομέρεια.

The screenshot displays the Moloch interface for a specific network flow. The top section shows the flow ID as 190722-LQ3wf_0vl_5ETpOliuwvnp8 and the community ID as 1:gkyHOSZKMLAR+92SulX3WgCWxYaY=. The time range is 2019/07/22 09:18:57 - 2019/07/22 09:18:58. The node is ubuntu. The protocols are http and tcp. The IP protocol is tcp. The source and destination statistics are: Src (Packets 36, Bytes 2,285, Databytes 329) and Dst (Packets 90, Bytes 123,905, Databytes 119,041). The Ethernet section shows Src Mac 00:08:02:1c:47:ae (OUI Hewlett Packard) and Dst Mac 20:e5:2a:b6:93:f1 (OUI Netgear). The Src IP/Port is 10.7.22.101 : 49183 and the Dst IP/Port is 85.222.228.142 : 80 (NL) [AS35470 CloudVPS B.V.] {RIPE}. The Payload8 section shows Src 474554202f77702d (GET /wp-) and Dst 485454502f312e31 (HTTP/1.1). The Tags section shows a blue plus icon. The Files section shows /data/moloch/raw/2019-07-22-Amadey-infection-with-Pony-and-Ursnif-and-Cobalt-Strike.pcap. The TCP Flags section shows SYN 1, SYN-ACK 1, ACK 81, PSH 42, RST 0, FIN 2, and URG 0.

5. Κάτω από την επικεφαλίδα **HTTP**, υπάρχουν σημαντικά δεδομένα σχετικά με τη σύνδεση. Η ανάλυση αυτών των πληροφοριών δείχνει ότι το αρχείο a22.exe κατεβράστηκε από τον συγκεκριμένο ιστότοπο. Από εδώ, ο αναλυτής μπορεί να χρησιμοποιήσει επιπλέον εργαλεία για εξαγωγή του αρχείου και περαιτέρω ανάλυση.

The screenshot displays the Moloch interface for a specific HTTP connection. The top section shows the Method as GET. The Status code is 200. The Hosts section shows ectcnepal.org. The User Agents section shows Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW. The Request Headers section shows accept, accept-encoding, connection, host, and user-agent. The Client Versions section shows 1.1. The Response Headers section shows accept-ranges, connection, content-length, and content-type. The Server Versions section shows 1.1. The Body MD5s section shows a607dd7bc894b22328770f4f70ca3fa4. The libfile content type section shows application/x-dosexec. The content-type Header section shows application/x-msdownload. The server Header section shows Apache.

Μία ακόμη χρήσιμη λειτουργία του Moloch είναι η δυνατότητα απεικόνισης των συνδέσεων. Στην κορυφή της web εφαρμογής υπάρχει η επιλογή **Connections**. Κάνοντας κλικ εκεί, εμφανίζεται η αντίστοιχη απεικόνιση.



7.9. Wireshark

Το Wireshark είναι ένα από τα πιο δημοφιλή εργαλεία ανάλυσης πακέτων (packet capture) που χρησιμοποιούν οι αναλυτές αντιμετώπισης περιστατικών (incident response). Εκτός από τη δυνατότητα σύλληψης πακέτων, διαθέτει πολλές άλλες λειτουργίες. Δεδομένου ότι υπάρχουν ολόκληροι τόμοι και εκπαιδευτικά μαθήματα αφιερωμένα στην πλατφόρμα αυτή, είναι αδύνατο να αναλυθεί κάθε χαρακτηριστικό της. Επομένως, αυτό το κεφάλαιο θα επικεντρωθεί σε ορισμένες βασικές λειτουργίες του Wireshark που είναι πιο χρήσιμες σε μια διερεύνηση περιστατικού.

Αναμφισβήτητα, το Wireshark θεωρείται ο προτιμώμενος αναλυτής πακέτων για επαγγελματίες IT και ασφάλειας. Λόγω της ευρείας χρήσης του, υπάρχουν πολλές πηγές διαθέσιμες για επιπλέον εκπαίδευση στο Wireshark και τις δυνατότητές του. Ο ιστότοπος του Wireshark στο <https://www.wireshark.org/> περιέχει πολλές πληροφορίες. Επιπλέον, ο ιστότοπος <https://www.chappelluniversity.com/> προσφέρει ασκήσεις και εκπαιδευτικά packet captures για εξάσκηση στην ανάλυση.

Δεδομένου ότι το Wireshark είναι ένα εργαλείο πλούσιο σε λειτουργίες, ορισμένες ρυθμίσεις ταιριάζουν περισσότερο στην ανάλυση δικτυακής κυκλοφορίας εκτός των δραστηριοτήτων αντιμετώπισης περιστατικών. Ως αποτέλεσμα, προτείνονται ορισμένες αλλαγές ώστε να διευκολυνθεί ο αναλυτής περιστατικών στην ανάλυση πακέτων σχετικά με μια έρευνα περιστατικού:

Χρόνος (Time): Η ρύθμιση χρόνου στο Wireshark προσφέρει διάφορες επιλογές, όπως η ώρα του πακέτου από την 1/1/1970 ή από την έναρξη της σύλληψης. Μια χρήσιμη επιλογή για διερεύνηση περιστατικών είναι η ημερομηνία και ώρα κατά την οποία τα πακέτα καταγράφηκαν. Αυτό επιτρέπει στους αναλυτές να συσχετίσουν ημερομηνίες και ώρες ύποπτης ή κακόβουλης δραστηριότητας με την κυκλοφορία στα συγκεκριμένα πακέτα. Για να ενεργοποιηθεί, πηγαίνουμε στο **View → Time**

Display Format και επιλέγουμε μια επιλογή όπως **Date and Time of Day** ή **Time of Day**. Μια άλλη χρήσιμη επιλογή είναι η χρήση της UTC, ιδιαίτερα αν το εσωτερικό δίκτυο χρησιμοποιεί UTC αντί για τοπική ώρα. Ο χρόνος μπορεί να εμφανίζεται μέχρι και σε νανοδευτερόλεπτα.

No.	Time	Source	Destination	Protocol
1	0.000000	10.3.13.101	10.3.13.1	DNS
2	0.030692	10.3.13.1	10.3.13.101	DNS
3	0.556303	10.3.13.101	88.198.14.102	TCP
4	0.739115	88.198.14.102	10.3.13.101	TCP
5	0.739762	10.3.13.101	88.198.14.102	TCP
6	0.739961	10.3.13.101	88.198.14.102	HTTP
7	0.740053	88.198.14.102	10.3.13.101	TCP
8	2.084099	88.198.14.102	10.3.13.101	TCP
9	2.084368	88.198.14.102	10.3.13.101	TCP
10	2.084401	88.198.14.102	10.3.13.101	TCP

Ανάλυση ονομάτων (Name resolution): Αυτή η ρύθμιση επιτρέπει στους αναλυτές να εναλλάσσονται μεταξύ εμφάνισης διευθύνσεων IP και ονομάτων υπολογιστών. Είναι χρήσιμη για τον εντοπισμό ύποπτων ονομάτων. Για παράδειγμα, για να εμφανιστούν τα hostnames, πηγαίνουμε στο **View → Name Resolution → Resolve Network Addresses**, και το Wireshark θα εμφανίσει τα ονόματα αντί για τις IP.

No.	Time	Source	Destination	Protocol
1	0.000000	10.3.13.101	10.3.13.1	DNS
2	0.030692	10.3.13.1	10.3.13.101	DNS
3	0.556303	10.3.13.101	rozhan-hse.com	TCP
4	0.739115	rozhan-hse.com	10.3.13.101	TCP
5	0.739762	10.3.13.101	rozhan-hse.com	TCP
6	0.739961	10.3.13.101	rozhan-hse.com	HTTP
7	0.740053	rozhan-hse.com	10.3.13.101	TCP
8	2.084099	rozhan-hse.com	10.3.13.101	TCP
9	2.084368	rozhan-hse.com	10.3.13.101	TCP
10	2.084401	rozhan-hse.com	10.3.13.101	TCP

Χρωματισμός λίστας πακέτων (Colorize packet list): Επιτρέπει στους αναλυτές να επιλέγουν αν η λίστα πακέτων θα είναι με κενό φόντο ή αν το Wireshark θα χρωματίζει τα πακέτα.

Επεξήγηση των Κανόνων Χρώματος: Οι κανόνες αυτοί εφαρμόζονται με σειρά προτεραιότητας (από πάνω προς τα κάτω) μέχρι να βρεθεί ο πρώτος που ταιριάζει. Κάθε κανόνας αποτελείται από:

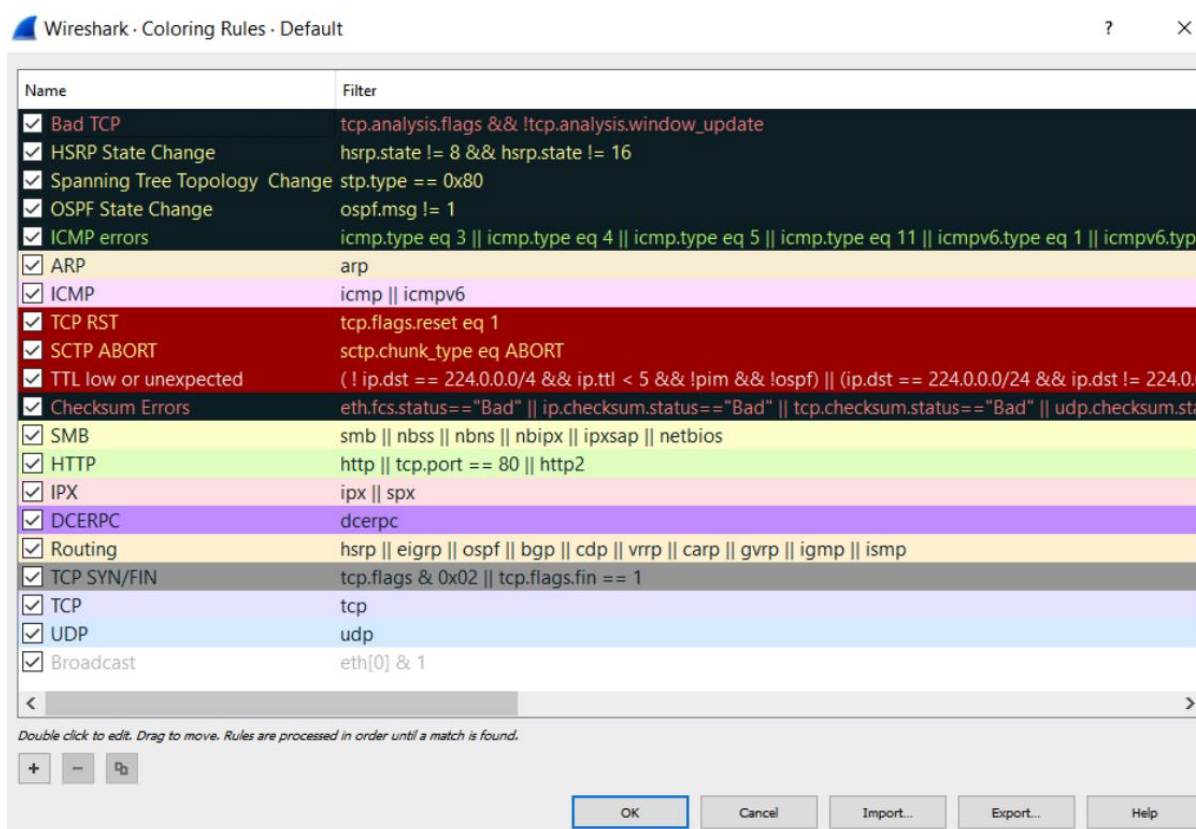
- **Όνομα:** Περιγραφή του κανόνα (π.χ. "Bad TCP", "ICMP").
- **Φίλτρο:** Μια έκφραση που καθορίζει ποιες συνθήκες πρέπει να ικανοποιούνται για να εφαρμοστεί το χρώμα (π.χ. `tcp.analysis.flags && !tcp.analysis.window_update` για "Bad TCP").

Παραδείγματα από την Εικόνα:

1. **Bad TCP:** Εμφανίζει κόκκινο χρώμα σε πακέτα TCP που έχουν προβλήματα ανάλυσης, εκτός από ενημερώσεις παραθύρου.

2. **TCP RST:** Εμφανίζει κόκκινο χρώμα σε πακέτα TCP με κωδικό επαναφοράς (reset) που ισούται με 1.
3. **ICMP:** Εμφανίζει πράσινο χρώμα σε πακέτα ICMP ή ICMPv6.
4. **UDP:** Εμφανίζει ανοιχτό μπλε χρώμα σε πακέτα UDP.
5. **Broadcast:** Εμφανίζει γκρι χρώμα σε πακέτα που προορίζονται για όλους (broadcast) σε διασυνδέσεις eth0 ή eth1.

Χρήση: Οι κανόνες βοηθούν να εντοπίσετε γρήγορα προβλήματα (π.χ. σφάλματα checksum, απορρίψεις TCP) ή συγκεκριμένους τύπους κίνησης (π.χ. SMB, HTTP). Μπορείτε να επεξεργαστείτε, να προσθέσετε ή να μετακινήσετε κανόνες με διπλό κλικ ή drag-and-drop.



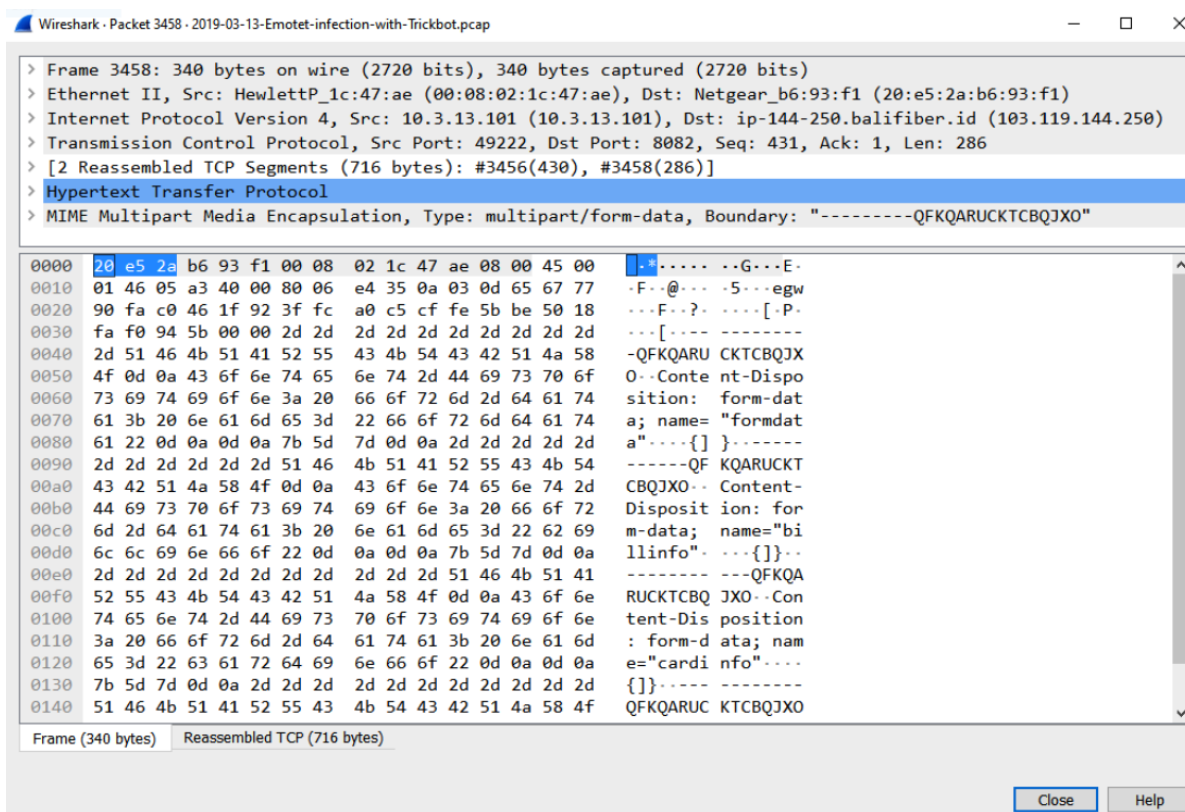
Για τις ανάγκες αυτού του κεφαλαίου, θα εξεταστεί ένα packet capture από το **Malware Traffic Analysis** (<https://www.malware-traffic-analysis.net/2019/03/13/index.html>), σε ένα σενάριο όπου ένας χρήστης κατεβάζει κακόβουλο λογισμικό τύπου crypto locker μέσω εγγράφου Word. Πριν την ανάλυση, το Wireshark διαμορφώθηκε ώστε να εμφανίζει ημερομηνία, ώρα και ονόματα υπολογιστών.

Βασικά χαρακτηριστικά Wireshark για ανάλυση:

Φίλτρα εμφάνισης (Display filters): Δυνατότητα φιλτραρίσματος πακέτων με βάση υπηρεσίες, ports, ή IP διευθύνσεις. Για παράδειγμα, για φιλτράρισμα της κυκλοφορίας από IP 10.3.13.101, κάνουμε δεξί κλικ → **Apply as Filter** → **Selected**.

ip.src==10.3.13.101				
No.	Time	Source	Destination	Protocol
1	0.000000	10.3.13.101	10.3.13.1	DNS
3	0.556303	10.3.13.101	rozhan-hse.com	TCP
5	0.739762	10.3.13.101	rozhan-hse.com	TCP
6	0.739961	10.3.13.101	rozhan-hse.com	HTTP

Αναγνώριση host (Host identification): Σημαντικό για την αναγνώριση του localhost. Από κάθε πακέτο μπορούμε να δούμε hostname, IP και MAC.



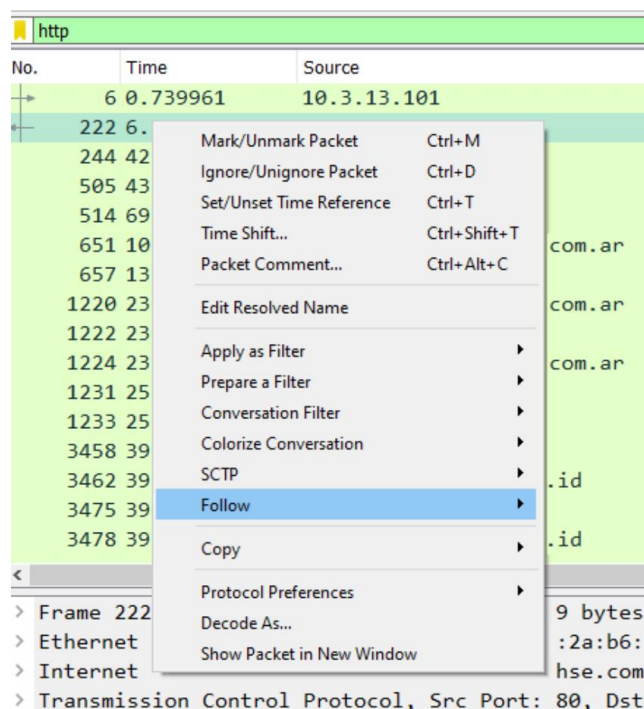
Αναγνώριση φυσικής σύνδεσης (Physical connection identification): Το πακέτο εμφανίζει πηγές και προορισμούς μέσω γραμμών Ethernet II και IPv4, π.χ., από τη συσκευή Hewlett Packard (10.3.13.101) προς 103.119.144.250. Το συγκεκριμένο HTTP πακέτο χρησιμοποιεί μη τυπική θύρα (8082).

Αναγνώριση πρωτοκόλλου (Protocol identification): Ανάλυση HTTP συνδέσεων για εντοπισμό μετάδοσης κακόβουλου λογισμικού. Μπορούμε να φιλτράρουμε με το φίλτρο http.

No.	Time	Source	Destination	Protocol
6	0.739961	10.3.13.101	rozhan-hse.com	HTTP
222	6.111115	rozhan-hse.com	10.3.13.101	HTTP
244	42.716145	10.3.13.101	aliyev.org	HTTP
505	43.744089	aliyev.org	10.3.13.101	HTTP
514	69.467806	10.3.13.101	101.152.220.201.itc.com.ar	HTTP

Αναγνώριση ύποπτων hostnames (Hostname identification): Εντοπισμός ύποπτων ονομάτων, π.χ., rozhan-hse.com. Το Wireshark επιτρέπει την παρακολούθηση TCP ή HTTP streams.

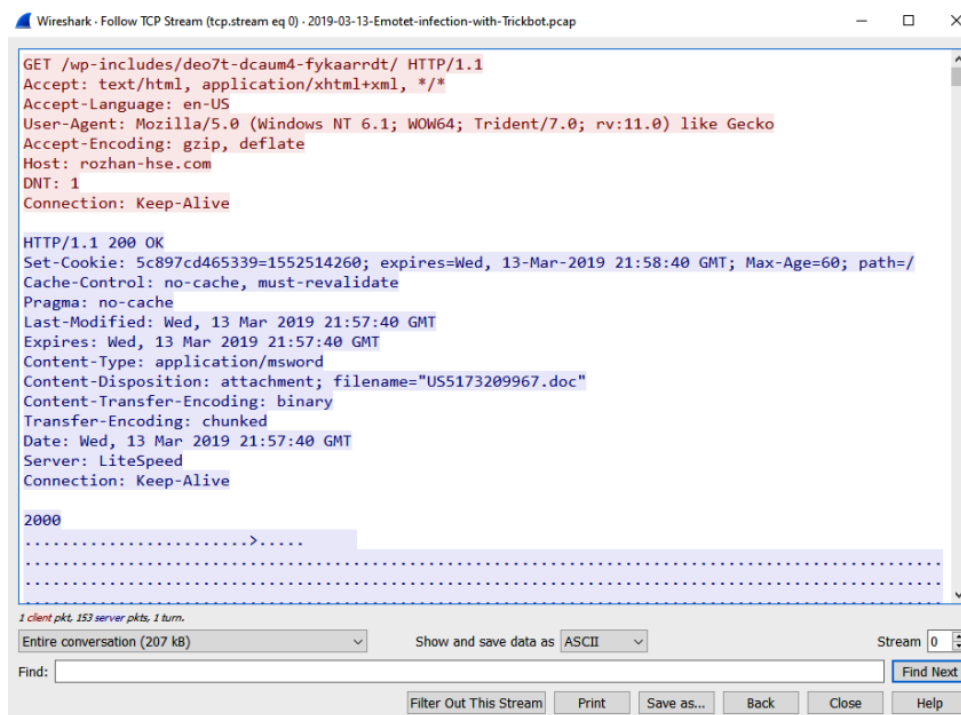
Εξέταση ροής πακέτων (Packet stream examination): Μέσω **Follow TCP Stream**, μπορούμε να εντοπίσουμε HTTP GET αιτήματα, να εξάγουμε αρχεία (File → Export Objects → HTTP) και να τα αποθηκεύσουμε για περαιτέρω ανάλυση.



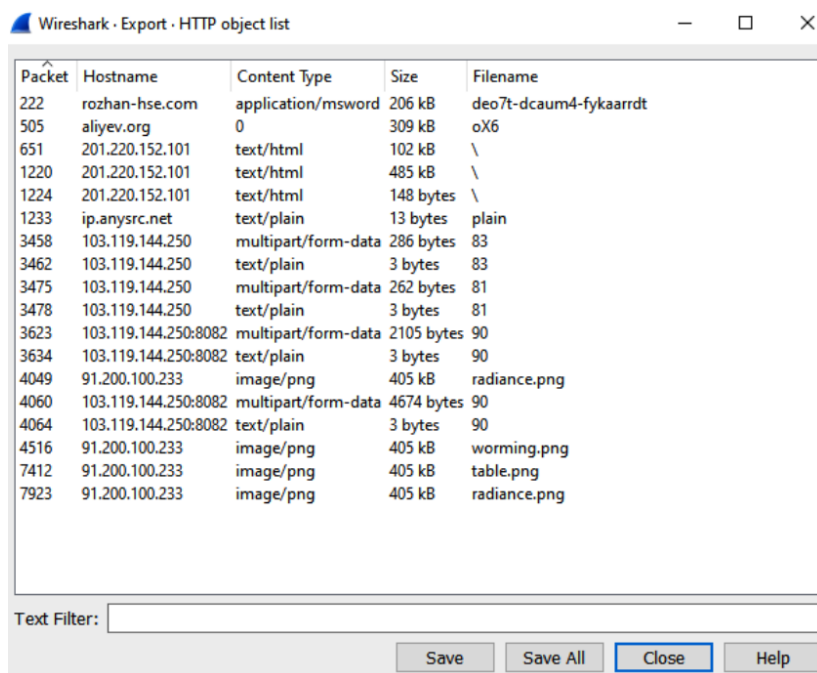
Η εικόνα δείχνει ένα παράθυρο του Wireshark που ακολουθεί μια ροή TCP (TCP Stream) από ένα αρχείο καταγραφής με την ονομασία "Emotet-infection-with-Trickbot.pcap". Αυτό το παράθυρο εμφανίζει την αμφίδρομη επικοινωνία μεταξύ ενός πελάτη (client) και ενός διακομιστή (server), με λεπτομέρειες από την κεφαλίδα HTTP και τα δεδομένα που ανταλλάσσονται. Η ροή περιλαμβάνει 153 πακέτα από τον πελάτη και 1 πακέτο από τον διακομιστή, με συνολικό μέγεθος 207 KB.

Η επικεφαλίδα του αιτήματος (GET) δείχνει ότι ο πελάτης ζητά ένα αρχείο με URL /wp-includes/de07t-dcaum4-fykaarrdt/ HTTP/1.1, το οποίο μπορεί να σχετίζεται με κακόβουλο λογισμικό, όπως υποδηλώνει το όνομα του αρχείου. Ο πελάτης χρησιμοποιεί το πρόγραμμα περιήγησης Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko, υποδεικνύοντας ένα παλαιότερο Windows με τον Internet Explorer. Το αίτημα περιλαμβάνει αποδεκτές μορφές (text/html, application/xhtml+xml), κωδικοποίηση (gzip, deflate) και διατηρεί τη σύνδεση ανοιχτή (Keep-Alive).

Η απάντηση του διακομιστή είναι HTTP/1.1 200 OK, υποδεικνύοντας επιτυχή αίτημα. Η απάντηση περιλαμβάνει ένα cookie με ημερομηνία λήξης 13 Μαρτίου 2019, καθώς και εντολές no-cache και must-revalidate για την ενημέρωση του περιεχομένου. Το αρχείο που επιστρέφεται έχει τύπο application/msexcel, όνομα "US517320967.doc" και μεταφέρεται σε τμήματα (chunked) με κωδικοποίηση binary. Η ημερομηνία τροποποίησης και διακομιστή είναι 13 Μαρτίου 2019, που ταιριάζει με την ώρα της καταγραφής.



Η οπτική αναπαράσταση της ροής δείχνει τα δεδομένα που ανταλλάσσονται, με το "2000" να υποδηλώνει πιθανώς το μέγεθος ενός τμήματος δεδομένων. Αυτή η ροή μπορεί να χρησιμοποιηθεί για να αναλυθεί η επικοινωνία, πιθανώς για την ανίχνευση κακόβουλης δραστηριότητας, όπως λοίμωξη από Emotet ή Trickbot, όπως υποδηλώνει το όνομα του αρχείου.



Η εικόνα δείχνει το παράθυρο "Export HTTP object list" του Wireshark, το οποίο απαριθμεί αντικείμενα HTTP που έχουν εξαχθεί από ένα αρχείο καταγραφής. Κάθε γραμμή περιλαμβάνει πληροφορίες όπως

τον αριθμό πακέτου, το hostname, τον τύπο περιεχομένου, το μέγεθος και το όνομα αρχείου. Αυτή η λίστα επιτρέπει στους χρήστες να εξάγουν συγκεκριμένα αντικείμενα, όπως αρχεία ή εικόνες, που μεταφέρθηκαν μέσω HTTP.

Η λίστα περιλαμβάνει ποικιλία τύπων περιεχομένου, όπως αρχεία Microsoft Word (application/msword), HTML (text/html), απλό κείμενο (text/plain) και εικόνες PNG (image/png). Για παράδειγμα, το πακέτο 222 από το hostname "rozhan-hse.com" περιέχει ένα αρχείο 206 KB με τύπο application/msword και όνομα "de07t-dcaum4-fykaarrdt". Επιπλέον, υπάρχουν πολλά πακέτα από IPs όπως "103.119.144.250" και "91.200.100.233" που περιέχουν μικρά τμήματα δεδομένων (3 bytes) ή εικόνες μεγέθους 405 KB, όπως "radiance.png" και "worming.png".

Ορισμένα hostname, όπως "aliyeen.org" και "201.220.152.101", φαίνονται να συνδέονται με διαφορετικά αντικείμενα, υποδεικνύοντας πιθανή ποικιλία πηγών δεδομένων. Η παρουσία αρχείων όπως "US517320967.doc" και εικόνων με ονόματα όπως "radiance.png" μπορεί να υποδηλώνει κανονική δικτυακή κίνηση ή πιθανή κακόβουλη δραστηριότητα, ανάλογα με το πλαίσιο. Το παράθυρο προσφέρει επιλογές για αποθήκευση επιλεγμένων αντικειμένων ("Save") ή όλων ("Save All"), με τη δυνατότητα φιλτραρίσματος κειμένου για ευκολότερη αναζήτηση.

Το Wireshark είναι ένα ισχυρό εργαλείο για λεπτομερή ανάλυση πακέτων. Η δυνατότητα διάσπασης σε μεμονωμένα πακέτα δίνει στους αναλυτές πλήρη εικόνα της επικοινωνίας μεταξύ εσωτερικών και εξωτερικών hosts, αποκαλύπτοντας πιθανές μολύνσεις και επιτρέποντας την ανίχνευση άλλων ενδεχομένων μολυσμένων hosts.

Τα περιστατικά ασφαλείας δεν αφήνουν μόνο ίχνη στα συστήματα των υπολογιστών, αλλά δημιουργούν επίσης ενδείξεις σε όλες τις συσκευές και τις ροές κυκλοφορίας μέσα σε ένα δίκτυο. Η ικανότητα ανάλυσης αυτών των ιχνών επιτρέπει στους αναλυτές αντιμετώπισης περιστατικών να κατανοούν καλύτερα τον τύπο του περιστατικού που διερευνούν, καθώς και τις πιθανές ενέργειες που μπορούν να αναληφθούν. Αυτό το κεφάλαιο αναφέρθηκε στον τρόπο αξιολόγησης αρχείων καταγραφής (log files), είτε μέσω της γρήγορης διαδικασίας σύγκρισης με μαύρες λίστες ή ανάλυσης DNS, είτε μέσω ανάλυσης αρχείων καταγραφής χρησιμοποιώντας το Elastic Stack ή άλλα συστήματα SIEM. Συμπληρωματικά σε αυτήν την κύρια μέθοδο αξιολόγησης δικτυακών στοιχείων, περιλήφθηκε η ανάλυση NetFlow και η εξέταση των πακέτων δικτύου με εργαλεία όπως τα Moloch και Wireshark. Τα δικτυακά στοιχεία αποτελούν κρίσιμο συστατικό της διερεύνησης περιστατικών. Αυτά τα ίχνη, σε συνδυασμό με στοιχεία που συλλέγονται από πιθανώς παραβιασμένους ιστότοπους, συμβάλλουν σημαντικά στην ικανότητα των αναλυτών να ανασυνθέσουν τα γεγονότα ενός περιστατικού.

8

Ανάλυση Μνήμης Συστήματος

Για μεγάλο χρονικό διάστημα, οι υπηρεσίες επιβολής του νόμου και άλλοι οργανισμοί που πραγματοποιούν ψηφιακές εγκληματολογικές εργασίες, σχετικές με την διερεύνηση περιστατικών, βασίζονταν συχνά σε μεθοδολογίες που επικεντρώνονταν σε στοιχεία που βρίσκονται στον σκληρό δίσκο ενός υπολογιστή. Οι διαδικασίες υπαγόρευαν ότι το σύστημα θα έπρεπε να απενεργοποιηθεί και ο σκληρός δίσκος να αφαιρεθεί για τη δημιουργία εικόνας (imaging). Αν και αυτή η μεθοδολογία και οι συναφείς διαδικασίες ήταν αποτελεσματικές για τη διασφάλιση της ακεραιότητας των στοιχείων, αγνοούσαν τον πλούτο πληροφοριών που περιέχεται στη μνήμη τυχαίας προσπέλασης (RAM) ή απλώς στη μνήμη του στοχευόμενου συστήματος.

Ως αποτέλεσμα, οι αναλυτές απόκρισης περιστατικών άρχισαν να εστιάζουν σημαντικά στην εξασφάλιση κατάλληλων μεθόδων που διατηρούν την ακεραιότητα αυτών των στοιχείων, ενώ ταυτόχρονα τους παρέχουν πλατφόρμα για την απόκτηση πληροφοριών με αποδεικτική αξία.

Αυτό το κεφάλαιο επικεντρώνεται στους τύπους στοιχείων που μπορούν να βρεθούν στη μνήμη ενός συστήματος, στα εργαλεία και στις τεχνικές που έχουν στη διάθεσή τους οι αναλυτές απόκρισης περιστατικών και, τέλος, στο πώς να αναλυθούν αυτές οι πληροφορίες για να κατανοηθεί πλήρως πώς παραβιάστηκε το σύστημα. Επιπλέον, αυτές οι τεχνικές μπορούν να ενσωματωθούν στην ανάλυση άλλων στοιχείων, όπως τα αρχεία καταγραφής δικτύου και τα αρχεία που βρίσκονται στο στοχευόμενο σύστημα.

Στο κεφάλαιο αυτό θα καλυφθούν οι εξής κύριες θεματικές ενότητες:

- **Επισκόπηση ανάλυσης μνήμης:** Η ενότητα αυτή αναλύει τα κρίσιμα δεδομένα που μπορούν να ανακαλυφθούν μέσω σωστής ανάλυσης μνήμης.
- **Μεθοδολογία ανάλυσης μνήμης:** Μια δομημένη προσέγγιση είναι σημαντική ώστε οι αναλυτές να μπορούν να εξάγουν τα απαραίτητα δεδομένα.
- **Ανάλυση μνήμης με Redline:** Το πρώτο εργαλείο που θα εξεταστεί είναι το Mandiant Redline, ένα εργαλείο με GUI που επιτρέπει στους αναλυτές να εξετάζουν λήψεις μνήμης.
- **Ανάλυση μνήμης με Volatility:** Θεωρείται το «χρυσό πρότυπο» για την ανάλυση μνήμης και διαθέτει εκτεταμένες δυνατότητες για συλλογή και ανάλυση δεδομένων.

- **Ανάλυση μνήμης με Strings:** Ένα απλό αλλά αποτελεσματικό εργαλείο που επιτρέπει στους αναλυτές να εξάγουν δεδομένα από περιοχές της μνήμης που μπορεί να παραλείπουν άλλα εργαλεία.

Στο τέλος του κεφαλαίου, ο αναγνώστης θα έχει κατανοήσει τόσο τη μεθοδολογία όσο και τα εργαλεία που απαιτούνται για τον εντοπισμό, την ανάλυση και την εξαγωγή στοιχείων για περαιτέρω διερεύνηση.

8.1. Επισκόπηση Ανάλυσης Μνήμης

Όταν συζητάμε την ανάλυση της μνήμης ενός συστήματος, δύο όροι χρησιμοποιούνται εναλλακτικά: RAM και μνήμη. Οι όροι αυτοί περιγράφουν το τμήμα του υπολογιστή όπου το λειτουργικό σύστημα αποθηκεύει δεδομένα που χρησιμοποιούνται από εφαρμογές και το υλικό του συστήματος ενώ αυτά είναι σε χρήση. Η RAM ή μνήμη διαφέρει από την αποθήκευση λόγω της ευμετάβλητης φύσης των δεδομένων – αν το σύστημα κλείσει, τα δεδομένα συχνά χάνονται.

Μια σημαντική αλλαγή στα λειτουργικά συστήματα που επηρεάζει άμεσα την ανάλυση μνήμης είναι η εισαγωγή των 64-bit λειτουργικών συστημάτων. Η χρήση ενός 64-bit καταχωρητή επιτρέπει στο λειτουργικό σύστημα να αναφερθεί σε έως 17,179,869,184 GB μνήμης, πολύ μεγαλύτερη ποσότητα από ό,τι σε ένα 32-bit OS. Ως αποτέλεσμα, υπάρχει σημαντική ποσότητα δεδομένων στη RAM κατά τη λειτουργία ενός συστήματος που είναι πολύτιμη για τη διερεύνηση περιστατικών. Αυτά περιλαμβάνουν:

- Τρέχουσες διεργασίες
- Φορτωμένες Dynamic Link Libraries (DLL)
- Φορτωμένοι οδηγοί συσκευών (device drivers)
- Ανοιχτά κλειδιά μητρώου (registry keys)
- Συνδέσεις δικτύου
- Ιστορικό εντολών

Καθώς η ανάγκη ανάλυσης μνήμης συστημάτων αυξάνεται, οι αναλυτές έχουν στη διάθεσή τους διάφορα εργαλεία. Το κεφάλαιο αυτό επικεντρώνεται σε τρία εργαλεία, όλα ανοιχτού κώδικα ή δωρεάν, που μπορούν να αναπτυχθούν εύκολα και παρέχουν κρίσιμες πληροφορίες για δραστηριότητες εκμετάλλευσης και κακόβουλου λογισμικού που έχουν επηρεάσει ένα σύστημα.

Δύο λήψεις μνήμης θα χρησιμοποιηθούν: η πρώτη από ένα σύστημα Windows μολυσμένο με τον ιό Stuxnet και η δεύτερη από ένα σύστημα Windows με τον τρωικό Cridex. Αν και οι λοιμώξεις αυτές είναι σχετικά παλιές, είναι χρήσιμες για την επισήμανση χαρακτηριστικών των εργαλείων που θα εξεταστούν.

8.2. Μεθοδολογία Ανάλυσης Μνήμης

Κατά την εξέταση της μνήμης συστήματος, συνιστάται οι αναλυτές να ακολουθούν μια μεθοδολογία για να διασφαλίσουν ότι όλα τα πιθανά στοιχεία θα ανακαλυφθούν και θα αξιοποιηθούν στη διερεύνηση ενός περιστατικού. Η συγκεκριμένη μεθοδολογία μπορεί να εξαρτάται από τον τύπο περιστατικού. Για παράδειγμα, μια προσέγγιση που επικεντρώνεται στον εντοπισμό δεικτών παραβίασης λόγω κακόβουλου λογισμικού μπορεί να αποδώσει πολλές πληροφορίες αλλά να μην είναι κατάλληλη αν υπάρχουν στοιχεία από άλλες πηγές δικτύου σχετικά με ύποπτη IP.

Ένας από τους κύριους στόχους της ανάλυσης μνήμης είναι ο εντοπισμός πιθανώς κακόβουλων διεργασιών ή εκτελέσιμων αρχείων για περαιτέρω εξέταση. Αυτά τα δεδομένα θα επαναχρησιμοποιηθούν και στο Κεφάλαιο 12, «Ανάλυση Κακόβουλου Λογισμικού για Απόκριση Περιστατικών».

8.3. Μεθοδολογία έξι βημάτων του SANS

Το ίδρυμα SANS χρησιμοποιεί μια μεθοδολογία έξι βημάτων για την ανάλυση εικόνων μνήμης:

1. **Αναγνώριση κακόβουλων διεργασιών:** Εντοπισμός διεργασιών που φαίνονται νόμιμες αλλά κρύβουν κακόβουλη δραστηριότητα.
2. **Ανάλυση DLLs και χειριστών διεργασιών:** Εξέταση των DLL και άλλων στοιχείων της διεργασίας για πιθανή παραβίαση.
3. **Ανασκόπηση στοιχείων δικτύου:** Εντοπισμός ενεργών συνδέσεων και διευθύνσεων IP για κατανόηση του τύπου παραβίασης.
4. **Αναζήτηση ενδείξεων εισαγωγής κώδικα:** Εντοπισμός τεχνικών όπως process hollowing και unmapped memory sections.
5. **Έλεγχος για rootkit:** Εντοπισμός malware που επιτρέπει συνεχόμενη και αυξημένη πρόσβαση στο σύστημα.
6. **Απόρριψη ύποπτων διεργασιών και οδηγών:** Απόκτηση για περαιτέρω ανάλυση με άλλα εργαλεία.

8.4. Μεθοδολογία Δικτυακών Συνδέσεων

Σε πολλά περιστατικά, η πρώτη ένδειξη ότι ένα σύστημα έχει παραβιαστεί είναι οι προσπάθειες ή οι επιτυχημένες συνδέσεις με εξωτερικούς hosts. Οι μηχανισμοί ανίχνευσης, όπως τα firewalls ή οι web proxies, μπορεί να υποδεικνύουν ότι ένα ή περισσότερα συστήματα προσπαθούν να επικοινωνήσουν

με ύποπτους εξωτερικούς hosts. Από αυτό το σημείο εκκίνησης, μπορεί να είναι δυνατός ο εντοπισμός πιθανού κακόβουλου λογισμικού στο σύστημα:

- **Ύποπτες δικτυακές συνδέσεις:** Η ανασκόπηση των δικτυακών συνδέσεων στους hosts που έχουν συνδεθεί με εξωτερικούς hosts συχνά αποκαλύπτει τη διεργασία που προσπαθεί να επικοινωνήσει.
- **Όνομα διεργασίας:** Η εξέταση της διεργασίας που συνδέεται με το δίκτυο επιτρέπει στους αναλυτές να εκτελέσουν ενέργειες παρόμοιες με αυτές που περιγράφονται στη μεθοδολογία SANS. Συνιστάται να καθοριστεί επίσης αν η συγκεκριμένη διεργασία συνήθως απαιτεί δικτυακή σύνδεση.
- **ID γονικής διεργασίας (Parent Process ID):** Η επιπλέον εξέταση της γονικής διεργασίας είναι χρήσιμη για να διαπιστωθεί αν η διεργασία είναι νόμιμη και έχει πραγματική ανάγκη να επικοινωνεί μέσω δικτύου.
- **Σχετιζόμενες οντότητες:** Τέλος, η εξέταση των συνδεδεμένων DLL και άλλων artifacts οδηγεί στο στάδιο όπου μπορούν να αποκτηθούν και να αναλυθούν.

8.5. Εργαλεία ανάλυσης μνήμης

Υπάρχουν διάφορα εργαλεία διαθέσιμα στους αναλυτές για την ανασκόπηση εικόνων μνήμης. Ορισμένα παρέχουν γραφικό περιβάλλον (GUI) για ευκολία χρήσης, ενώ άλλα λειτουργούν μέσω γραμμής εντολών, καθιστώντας τα χρήσιμα για scripting. Για τις ανάγκες αυτού του κεφαλαίου, θα εξεταστούν τρία εργαλεία:

1. **Mandiant Redline:** Πρόκειται για ένα εργαλείο ανάλυσης μνήμης με GUI, το οποίο εξετάζει εικόνες μνήμης για σημάδια ύποπτων διεργασιών και τις βαθμολογεί με βάση διάφορους παράγοντες.
2. **Volatility:** Ένα εργαλείο γραμμής εντολών που επιτρέπει στους αναλυτές να εμβαθύνουν στις λεπτομέρειες της εικόνας μνήμης και να εντοπίσουν πιθανώς κακόβουλο κώδικα.
3. **Strings (Linux):** Το Strings επιτρέπει αναζήτηση λέξεων-κλειδιών μέσω GREP, δίνοντας τη δυνατότητα στον αναλυτή να εντοπίσει δείκτες συμβάντων (IOCs) που μπορεί να μην είναι άμεσα ορατοί με τα άλλα εργαλεία.

8.6. Ανάλυση Μνήμης με το Redline

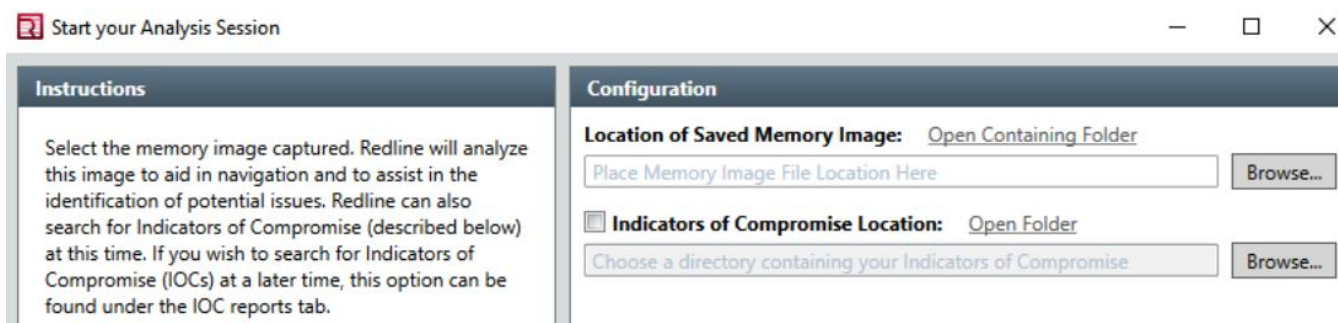
Ένα ισχυρό εργαλείο που οι αναλυτές θα πρέπει να έχουν στη διάθεσή τους είναι το **Mandiant Redline**. Αυτή η εφαρμογή για **Microsoft Windows** παρέχει μια πλατφόρμα πλούσια σε δυνατότητες για την ανάλυση εικόνων μνήμης. Οι δυνατότητες αυτές περιλαμβάνουν τη δυνατότητα δημιουργίας ενός **memory collector**, αν και το εργαλείο μπορεί να λειτουργήσει και με εικόνες μνήμης που έχουν ληφθεί

μέσω των εργαλείων που συζητήθηκαν προηγουμένως. Υπάρχει επίσης η δυνατότητα χρήσης προηγουμένως εντοπισμένων Δεικτών Συμβάντων (IOCs) για την υποβοήθηση της ανάλυσης. Το εργαλείο μπορεί να ληφθεί από τη διεύθυνση: <https://www.fireeye.com/services/freeware/redline.html>. Το πακέτο λήψης περιλαμβάνει έναν **Microsoft self-installer**.

Διαδικασία ανάλυσης με Redline

Για να παρουσιαστούν μερικά από τα βασικά χαρακτηριστικά του Redline, θα χρησιμοποιηθεί η **Stuxnet memory capture**. Για την εκτέλεση της ανάλυσης, ακολουθήστε τα εξής βήματα:

1. **Εγκατάσταση του Redline** μέσω του Microsoft Self Installer.
2. Μετά την εγκατάσταση, κάντε διπλό κλικ στο εικονίδιο και θα εμφανιστεί η κύρια οθόνη. Υπάρχουν πολλές επιλογές χωρισμένες σε δύο κατηγορίες: **Collect Data** και **Analyze Data**. Σε αυτήν την περίπτωση, θα αναλυθεί η μνήμη της Stuxnet.
3. Κάντε κλικ στο **From a Saved Memory File** στην κατηγορία **Analyze Data**. Αυτό θα ανοίξει ένα δεύτερο παράθυρο. Στο **Location of Saved Memory Image**, πλοηγηθείτε στη θέση του αρχείου μνήμης και επιλέξτε το. Στη συνέχεια, κάντε κλικ στο **Next**.



4. Μόλις φορτωθεί το αρχείο μνήμης, η επόμενη οθόνη θα ζητήσει ένα όνομα για το **session file** που θα δημιουργηθεί από το Redline



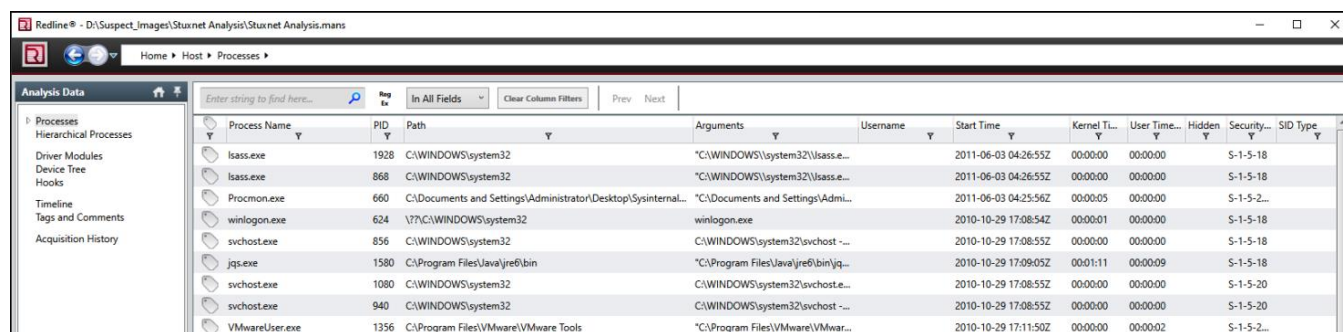
Σε αυτήν την περίπτωση, χρησιμοποιείται το όνομα **Stuxnet Analysis**. Επιπλέον, επιλέξτε έναν φάκελο που θα περιέχει όλα τα δεδομένα αυτής της ανάλυσης. Είναι καλή πρακτική να έχετε ξεχωριστούς φακέλους για κάθε συνεδρία ανάλυσης, ώστε να διασφαλίζεται η απομόνωση των στοιχείων. Σε

περίπτωση που εξετάζονται πολλά συστήματα, αυτό μειώνει τον κίνδυνο ανάμειξης αποδεικτικών στοιχείων. Αφού οριστούν αυτές οι παραμέτροι, κάντε κλικ στο **OK**.

- Το Redline θα ξεκινήσει τότε τη διαδικασία μετατροπής των δεδομένων σε μορφή κατάλληλη για ανάλυση. Ανάλογα με το μέγεθος της εικόνας, αυτό μπορεί να διαρκέσει αρκετά λεπτά.



- Αφού δημιουργηθεί η συνεδρία ανάλυσης, θα εμφανιστεί το επόμενο παράθυρο. Για εικόνες μνήμης που δεν περιέχουν επιπλέον πληροφορίες, κάντε κλικ στο τμήμα **I am Investigating a Host Based on an External Investigative Lead**.
- Στη συνέχεια θα εμφανιστεί το παράθυρο που παρουσιάζει τα αποτελέσματα της ανάλυσης.



Στην κύρια περιοχή της οθόνης, φαίνονται διάφορες διαδικασίες που τρέχουν στο σύστημα, όπως το "lsass.exe", "winlogon.exe", "svchost.exe" και "VMwareUser.exe". Αυτές οι διαδικασίες περιλαμβάνουν κρίσιμες συστημικές λειτουργίες του Windows (π.χ. "lsass.exe" για τη διαχείριση πιστοποιήσεων ασφαλείας) καθώς και εφαρμογές τρίτων, όπως το VMware. Οι πληροφορίες δίπλα σε κάθε διαδικασία δείχνουν την ημερομηνία και ώρα εκκίνησης, που κυμαίνονται από το 2010 έως το 2011.

lsass.exe	1928	C:\WINDOWS\system32	"C:\WINDOWS\system32\lsass.exe"
lsass.exe	868	C:\WINDOWS\system32	"C:\WINDOWS\system32\lsass.exe"
Procmon.exe	660	C:\Documents and Settings\Administrator\Desktop\Sysinternal...	"C:\Documents and Settings\Administrator\Desкто...
winlogon.exe	624	\\?\C:\WINDOWS\system32	winlogon.exe
svchost.exe	856	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost -k DcomLaunch
jqs.exe	1580	C:\Program Files\Java\jre6\bin	"C:\Program Files\Java\jre6\bin\jqs.exe" -service -c...
svchost.exe	1080	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost.exe -k NetworkSe...
svchost.exe	940	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost -k rpcss
VMwareUser.exe	1356	C:\Program Files\VMware\VMware Tools	"C:\Program Files\VMware\VMware Tools\VMware...
lsass.exe	680	C:\WINDOWS\system32	C:\WINDOWS\system32\lsass.exe

Μόλις ολοκληρωθεί η επεξεργασία της εικόνας μνήμης, η κύρια σελίδα παρέχει μια **αναλυτική λίστα των διεργασιών** που εκτελούνταν τη στιγμή της λήψης. Αυτή περιλαμβάνει τη **διαδρομή του αρχείου της διεργασίας**, το **όνομα της διεργασίας** και τον **αριθμό αναγνώρισης διεργασίας (PID)**. Μια επισκόπηση των τρεχουσών διεργασιών δείχνει ότι υπάρχουν **τρεις διεργασίες lsass.exe** με PID 1928, 868 και 680. Αυτό είναι **ύποπτο**, καθώς η ύπαρξη πολλαπλών καταχωρήσεων του lsass.exe υποδηλώνει **κακόβουλη συμπεριφορά**.

Μια ακόμα δυνατότητα του Redline είναι η ικανότητα των αναλυτών να εξετάζουν τις διεργασίες σε σχέση με τις **γονικές τους διεργασίες**. Η **ιεραρχική προβολή διεργασιών** παρέχει μια εικόνα για τη διαδρομή μέσω της οποίας εκτελέστηκαν οι διεργασίες. Αυτό είναι ιδιαίτερα χρήσιμο κατά την εξέταση της μνήμης για στοιχεία **παράνομων ή ύποπτων διεργασιών**. Κάντε κλικ στο **Hierarchical Processes** στο αριστερό πάνελ, κάτω από το **Analysis Data**. Αυτό θα αλλάξει την προβολή ώστε να εμφανίζονται οι διεργασίες σε σχέση με τις γονικές τους διεργασίες.

The screenshot displays the Redline interface with the 'Hierarchical Processes' view selected. The left sidebar shows the navigation menu with 'Hierarchical Processes' highlighted. The main pane shows a tree structure of processes. The 'System' process (PID 4) is expanded, showing its children: 'smss.exe' (PID 376), 'csrss.exe' (PID 600), 'winlogon.exe' (PID 624), 'services.exe' (PID 668), 'alg.exe' (PID 188), 'imapi.exe' (PID 756), 'vmacthlp.exe' (PID 844), 'svchost.exe' (PID 856), 'wmiprvse.exe' (PID 1872), 'lsass.exe' (PID 868), 'svchost.exe' (PID 940), 'svchost.exe' (PID 1032), 'wuauclt.exe' (PID 976), 'wscntfy.exe' (PID 2040), 'svchost.exe' (PID 1080), 'svchost.exe' (PID 1200), 'spoolsv.exe' (PID 1412), 'jqs.exe' (PID 1580), 'vmtoolsd.exe' (PID 1664), 'VMUpgradeHelper.exe' (PID 1816), 'lsass.exe' (PID 1928), 'lsass.exe' (PID 680), 'Explorer.EXE' (PID 1196), and 'TSVNCache.exe' (PID 324). The 'lsass.exe' processes are highlighted in blue, indicating they are the focus of the analysis.

Process Name	PID	Path	Arguments	Username
System	4			
smss.exe	376	\SystemRoot\System32	\SystemRoot\System32\smss.exe	
csrss.exe	600	\??\C:\WINDOWS\system32	C:\WINDOWS\system32\csrss.exe...	
winlogon.exe	624	\??\C:\WINDOWS\system32	winlogon.exe	
services.exe	668	C:\WINDOWS\system32	C:\WINDOWS\system32\services.e...	
alg.exe	188	C:\WINDOWS\system32	C:\WINDOWS\system32\alg.exe	
imapi.exe	756	C:\WINDOWS\system32	C:\WINDOWS\system32\imapi.exe	
vmacthlp.exe	844	C:\Program Files\VMware\VMware Tools	"C:\Program Files\VMware\VMwar...	
svchost.exe	856	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost -...	
wmiprvse.exe	1872	C:\WINDOWS\system32\wbem		
lsass.exe	868	C:\WINDOWS\system32	"C:\WINDOWS\system32\lsass.e...	
svchost.exe	940	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost -...	
svchost.exe	1032	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost.e...	
wuauclt.exe	976	C:\WINDOWS\system32	"C:\WINDOWS\system32\wuauclt...	
wscntfy.exe	2040	C:\WINDOWS\system32	C:\WINDOWS\system32\wscntfy.exe	
svchost.exe	1080	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost.e...	
svchost.exe	1200	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost.e...	
spoolsv.exe	1412	C:\WINDOWS\system32	C:\WINDOWS\system32\spoolsv.e...	
jqs.exe	1580	C:\Program Files\Java\jre6\bin	"C:\Program Files\Java\jre6\bin\jq...	
vmtoolsd.exe	1664	C:\Program Files\VMware\VMware Tools	"C:\Program Files\VMware\VMwar...	
VMUpgradeHelper.exe	1816	C:\Program Files\VMware\VMware Tools	"C:\Program Files\VMware\VMwar...	
lsass.exe	1928	C:\WINDOWS\system32	"C:\WINDOWS\system32\lsass.e...	
lsass.exe	680	C:\WINDOWS\system32	C:\WINDOWS\system32\lsass.exe	
Explorer.EXE	1196	C:\WINDOWS	C:\WINDOWS\Explorer.EXE	
TSVNCache.exe	324	C:\Program Files\TortoiseSVN\bin	"C:\Program Files\TortoiseSVN\bin...	

Process Information

Process: lsass.exe (680)
Parent: winlogon.exe (624)
Path: C:\WINDOWS\system32
Arguments: C:\WINDOWS\system32\lsass.exe
Start Time: 2010-10-29 17:08:54Z
Kernel Time Elapsed: 00:01:04
User Time Elapsed: 00:00:02
Hidden: Not Available

User Information

Username: Not Available
Security ID: S-1-5-18
Security Type: Not Available

Μια εξέταση των διεργασιών δείχνει **τρεις περιπτώσεις του lsass.exe** με τους αριθμούς PID **680, 868 και 1928**. Η ύπαρξη ενός μόνο **lsass.exe** είναι το αναμενόμενο, αλλά η ύπαρξη τριών είναι **ύποπτη**, καθώς το lsass.exe μπορεί να **πλαστογραφηθεί** και συχνά χρησιμοποιείται από προγραμματιστές κακόβουλου λογισμικού.

Από εδώ, η διεργασία **lsass.exe με PID 680** μπορεί να εξεταστεί περαιτέρω. Αν διπλοκλικάρετε στη διεργασία, εμφανίζεται το ακόλουθο παράθυρο:

Αυτές οι **διευρυμένες πληροφορίες της διεργασίας** δείχνουν ότι αυτή η διεργασία δημιουργήθηκε από τη διεργασία **winlogon.exe** από τον φάκελο System32. Αυτό μπορεί να μην είναι ύποπτη συμπεριφορά, καθώς θεωρείται φυσιολογικό. Επειδή θα έπρεπε να υπάρχει μόνο μία διεργασία lsass.exe, οι άλλες δύο πρέπει να εξεταστούν περαιτέρω. Η διεργασία **lsass.exe με PID 868** φαίνεται να έχει εκτελεστεί με γονική διεργασία την **services.exe**.

Process Information

Process: lsass.exe (868)
Parent: services.exe (668)
Path: C:\WINDOWS\system32
Arguments: "C:\WINDOWS\system32\lsass.exe"
Start Time: 2011-06-03 04:26:55Z
Kernel Time Elapsed: 00:00:00
User Time Elapsed: 00:00:00
Hidden: Not Available

User Information

Username: Not Available
Security ID: S-1-5-18
Security Type: Not Available

Τα ίδια αποτελέσματα βρίσκονται και για το **lsass.exe με PID 1928**.

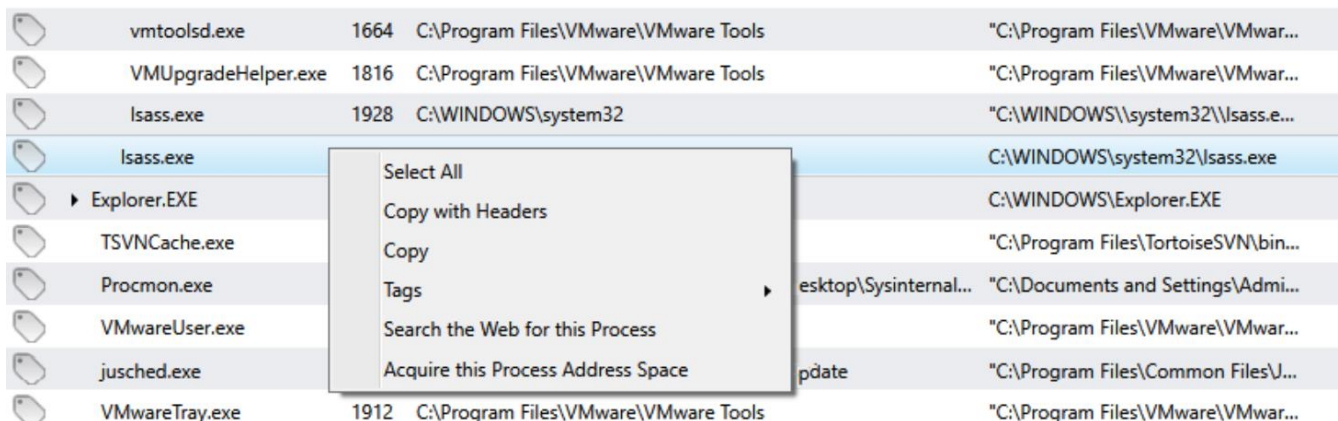
Process Information

Process: lsass.exe (1928)
Parent: services.exe (668)
Path: C:\WINDOWS\system32
Arguments: "C:\WINDOWS\system32\lsass.exe"
Start Time: 2011-06-03 04:26:55Z
Kernel Time Elapsed: 00:00:00
User Time Elapsed: 00:00:00
Hidden: Not Available

User Information

Username: Not Available
Security ID: S-1-5-18
Security Type: Not Available

Σε αυτό το στάδιο, φαίνεται ότι το σύστημα έχει **πολλαπλές διεργασίες Isass.exe**, κάτι που από μόνο του είναι ύποπτο. Το επόμενο βήμα είναι να **αποθηκευτεί ο χώρος διευθύνσεων (address space) και των τριών διεργασιών** για περαιτέρω ανάλυση. Για να γίνει αυτό, κάντε δεξί κλικ στη διεργασία και θα ανοίξει το ακόλουθο παράθυρο:



Κάντε κλικ στο **Acquire this Process Address Space**. Από εδώ, το Redline θα αποκτήσει και θα αποθηκεύσει τα αρχεία που συνδέονται με τη διεργασία σε έναν ξεχωριστό φάκελο zip στον φάκελο που περιέχει τα δεδομένα ανάλυσης.

AcquiredFiles	9/8/2019 9:00 AM	Compressed (zipp...	5,321 KB
ReadMe (ContainsSafeAcquisitionZipPas...	9/8/2019 9:00 AM	Text Document	1 KB

Καθώς και οι τρεις διεργασίες Isass.exe είναι **ύποπτες**, πρέπει να αποκτηθούν όλες. Από εκεί και πέρα, τα αρχεία που συνδέονται με τους χώρους διευθύνσεων μπορούν να εξεταστούν. Αυτό θα καλυφθεί στο Κεφάλαιο 12, **Ανάλυση Κακόβουλου Λογισμικού για Αντιμετώπιση Περιστατικών**, όπου τα αρχεία θα εξεταστούν λεπτομερώς.

Το Redline θα στείλει τα αποκτηθέντα αρχεία σε ένα **τοπικό φάκελο του συστήματος**. Υπάρχει πιθανότητα τα αρχεία να περιέχουν κακόβουλο λογισμικό, οπότε πρέπει να **ρυθμιστεί εξαίρεση για αυτόν τον φάκελο στο antivirus** ώστε τα αρχεία να μην τεθούν σε καραντίνα. Επιπλέον, επειδή υπάρχει πιθανότητα να τοποθετηθούν κακόβουλα αρχεία στο σύστημα, πρέπει να δίνεται **μεγάλη προσοχή** κατά τη χρήση αυτής της διαδικασίας για να μην μολυνθεί το σύστημα.

Αυτό το κεφάλαιο μπόρεσε να καλύψει μόνο την **επιφανειακή λειτουργικότητα του Redline**. Εκτός από τη δυνατότητα αναγνώρισης διεργασιών και εξαγωγής των δεδομένων τους, το Redline μπορεί επίσης να **εντοπίζει άλλα σημαντικά σημεία δεδομένων**, όπως συνδέσεις δικτύου, αρχεία DLL που σχετίζονται με διεργασίες και να εμφανίζει τις διεργασίες σε **προβολή χρονικής γραμμής**.

Η επόμενη ενότητα θα δείξει πώς να εξαγάγετε μερικά από αυτά τα δεδομένα χρησιμοποιώντας το ανοιχτού κώδικα εργαλείο γραμμής εντολών Volatility.

8.7. Ανάλυση Μνήμης με το Volatility

Το Volatility είναι ένα προηγμένο πλαίσιο ψηφιακής εγκληματολογίας μνήμης (memory forensics) ανοιχτού κώδικα. Το βασικό εργαλείο μέσα στο πλαίσιο είναι το σενάριο Python Volatility, το οποίο χρησιμοποιεί μια μεγάλη ποικιλία plugins για την ανάλυση εικόνων μνήμης. Ως αποτέλεσμα, το Volatility μπορεί να τρέξει σε οποιοδήποτε λειτουργικό σύστημα υποστηρίζει Python. Επιπλέον, μπορεί να χρησιμοποιηθεί για αρχεία εικόνων μνήμης από τα περισσότερα κοινώς διαδεδομένα λειτουργικά συστήματα, όπως Windows (από XP έως Windows Server 2016), macOS και κοινές διανομές Linux.

Υπάρχει μια σειρά από διαθέσιμα plugins για το Volatility, με περισσότερα να αναπτύσσονται συνεχώς. Για την ανάλυση της μνήμης του συστήματος, θα εξεταστούν διάφορα plugins ώστε ο αναλυτής να έχει επαρκείς πληροφορίες για να πραγματοποιήσει σωστή ανάλυση. Συνιστάται, πριν από τη χρήση του Volatility, ο αναλυτής να βεβαιωθεί ότι το λογισμικό είναι ενημερωμένο και ότι έχουν εξεταστεί νέα plugins για να προσδιοριστεί η εφαρμοσιμότητά τους στη συγκεκριμένη έρευνα.

Εγκατάσταση Volatility

Το Volatility είναι διαθέσιμο για Linux, Windows και macOS. Πληροφορίες σχετικά με την εγκατάσταση σε διάφορα λειτουργικά συστήματα είναι διαθέσιμες στη διεύθυνση: <https://www.volatilityfoundation.org/releases>. Η ακόλουθη εντολή εγκαθιστά το Volatility στο υποσύστημα Ubuntu καθώς και σε άλλα Linux OS:

```
dfir@Desktop-SFARF6G~$ sudo apt-get install volatility
```

```
Volatility Foundation Volatility Framework 2.6
INFO      : volatility.debug      : Determining profile based on KDBG search...
           Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
           AS Layer1            : IA32PagedMemoryPae (Kernel AS)
           AS Layer2            : FileAddressSpace (/mnt/d/Suspect_Images/cridex_laptop.mem)
           PAE type             : PAE
           DTB                  : 0x2fe000L
           KDBG                 : 0x80545ae0L
           Number of Processors : 1
           Image Type (Service Pack) : 3
           KPCR for CPU 0       : 0xffdf000L
           KUSER_SHARED_DATA    : 0xffdf000L
           Image date and time  : 2012-07-22 02:45:08 UTC+0000
           Image local date and time : 2012-07-21 22:45:08 -0400
```

Μετά την εγκατάσταση, η εφαρμογή Volatility μπορεί να τρέξει από οποιοδήποτε σημείο.

Χρήση του Volatility

Το Volatility έχει βασική σύνταξη με ξεχωριστές εντολές. Το πρώτο μέρος της εντολής είναι η εικόνα μνήμης που θα αναλυθεί. Το δεύτερο είναι το προφίλ της εικόνων μνήμης. Κάθε λειτουργικό σύστημα έχει δικούς του τρόπους διεύθυνσης μνήμης. Το προφίλ καθοδηγεί το Volatility στις συγκεκριμένες

περιοχές μνήμης για την εύρεση των δεδομένων. Το τρίτο μέρος της σύνταξης είναι το plugin που καθορίζει τις πληροφορίες που θέλει να ανακτήσει ο αναλυτής.

```
dfir@Desktop-SFARF6G~$ volatility -f memoryimage.mem -profile=Win7SP1x64 plugin
```

Υπάρχουν και άλλες επιλογές, όπως η αναφορά ενός PID ή η εξαγωγή των αποτελεσμάτων σε αρχείο κειμένου. Πληροφορίες για τα διάφορα plugins είναι διαθέσιμες στη σελίδα GitHub του Volatility: <https://github.com/volatilityfoundation/volatility/wiki/CommandReference>

Η ανάλυση εδώ θα γίνει με την εικόνα μνήμης Cridex που συζητήθηκε προηγουμένως. Αν και πρόκειται για γνωστά μολυσμένη εικόνα, παρέχει ένα γνωστό πλαίσιο για την κατανόηση των δεδομένων που μπορούν να ληφθούν με το Volatility. Για ευκολία, η εικόνα μετονομάστηκε σε `cridex_laptop.mem`.

Πληροφορίες εικόνας Volatility

Ένα από τα βασικά προπαρασκευαστικά βήματα πριν την ανάλυση της μνήμης του συστήματος είναι να προσδιοριστεί το ακριβές λειτουργικό σύστημα. Ακόμη και αν ο αναλυτής είναι σίγουρος για το OS, είναι καλή πρακτική να τρέξει το plugin `imageinfo` του Volatility. Η έξοδος του plugin δείχνει το πιθανό προφίλ της εικόνας μνήμης, κρίσιμο για τη χρήση των άλλων plugins.

```
dfir@Desktop-SFARF6G~$ volatility -f cridex_laptop.mem imageinfo
```

Η έξοδος δείχνει ότι το προφίλ που πιθανότατα θα δώσει τα καλύτερα αποτελέσματα είναι WinXPSP2x86.

Ανάλυση διεργασιών Volatility

Όπως έγινε και στην ενότητα Redline, τα πρώτα plugins που θα συζητηθούν είναι αυτά που παρέχουν δεδομένα για τις διεργασίες που εκτελούνταν κατά τη λήψη της μνήμης. Στόχος είναι να εντοπιστούν ύποπτες διεργασίες και τα σχετικά δεδομένα τους.

Λίστα διεργασιών (pslist)

Το plugin `pslist` εμφανίζει τις τρέχουσες διεργασίες στη μνήμη, μαζί με το offset, το όνομα διεργασίας, PID, αριθμό threads και handles, καθώς και ημερομηνία/ώρα εκκίνησης και τερματισμού. Καθώς το `pslist` περπατάει τη διπλά συνδεδεμένη λίστα `PsActiveProcessHead`, δεν μπορεί να εντοπίσει κρυφές ή αποσυνδεδεμένες διεργασίες.

```
dfir@Desktop-SFARF6G~$ volatility -f cridex_laptop.mem -profile=WinXPSP2x86 pslist
```

Volatility Foundation Volatility Framework 2.6									
Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	
0x823c89c8	System	4	0	53	240	-----	0		
0x822f1020	smss.exe	368	4	3	19	-----	0	2012-07-22 02:42:31	UTC+0000
0x822a0598	csrss.exe	584	368	9	326	0	0	2012-07-22 02:42:32	UTC+0000
0x82298700	winlogon.exe	608	368	23	519	0	0	2012-07-22 02:42:32	UTC+0000
0x81e2ab28	services.exe	652	608	16	243	0	0	2012-07-22 02:42:32	UTC+0000
0x81e2a3b8	lsass.exe	664	608	24	330	0	0	2012-07-22 02:42:32	UTC+0000
0x82311360	svchost.exe	824	652	20	194	0	0	2012-07-22 02:42:33	UTC+0000
0x81e29ab8	svchost.exe	908	652	9	226	0	0	2012-07-22 02:42:33	UTC+0000
0x823001d0	svchost.exe	1004	652	64	1118	0	0	2012-07-22 02:42:33	UTC+0000
0x821dfda0	svchost.exe	1056	652	5	60	0	0	2012-07-22 02:42:33	UTC+0000
0x82295650	svchost.exe	1220	652	15	197	0	0	2012-07-22 02:42:35	UTC+0000
0x821dea70	explorer.exe	1484	1464	17	415	0	0	2012-07-22 02:42:36	UTC+0000
0x81eb17b8	spoolsv.exe	1512	652	14	113	0	0	2012-07-22 02:42:36	UTC+0000
0x81e7bda0	reader_sl.exe	1640	1484	5	39	0	0	2012-07-22 02:42:36	UTC+0000
0x820e8da0	alg.exe	788	652	7	104	0	0	2012-07-22 02:43:01	UTC+0000
0x821fcda0	wuauclt.exe	1136	1004	8	173	0	0	2012-07-22 02:43:46	UTC+0000
0x8205bda0	wuauclt.exe	1588	1004	5	132	0	0	2012-07-22 02:44:01	UTC+0000

Από την έξοδο, δεν φαίνεται κάτι ύποπτο άμεσα, εκτός από το εκτελέσιμο reader_sl.exe, που έχει διαφορετική ονομασία από τις άλλες διεργασίες και ενδέχεται να χρειαστεί περαιτέρω έρευνα.

Σάρωση διεργασιών (psscan)

Το psscan επιτρέπει τον έλεγχο διεργασιών που έχουν τερματιστεί. Αντίθετα με το pslist, μπορεί να εντοπίσει rootkits μέσω διεργασιών που είναι κρυφές ή αποσυνδεδεμένες.

Εντολή:

```
dfir@Desktop-SFARF6G~$ volatility -f cridex_laptop.mem -profile=WinXPSP2x86 psscan
```

Volatility Foundation Volatility Framework 2.6									
Offset(P)	Name	PID	PPID	PDB		Time created			
0x0000000002029ab8	svchost.exe	908	652	0x079400e0	2012-07-22 02:42:33	UTC+0000			
0x000000000202a3b8	lsass.exe	664	608	0x079400a0	2012-07-22 02:42:32	UTC+0000			
0x000000000202ab28	services.exe	652	608	0x07940080	2012-07-22 02:42:32	UTC+0000			
0x000000000207bda0	reader_sl.exe	1640	1484	0x079401e0	2012-07-22 02:42:36	UTC+0000			
0x00000000020b17b8	spoolsv.exe	1512	652	0x079401c0	2012-07-22 02:42:36	UTC+0000			
0x000000000225bda0	wuauclt.exe	1588	1004	0x07940200	2012-07-22 02:44:01	UTC+0000			
0x00000000022e8da0	alg.exe	788	652	0x07940140	2012-07-22 02:43:01	UTC+0000			
0x00000000023dea70	explorer.exe	1484	1464	0x079401a0	2012-07-22 02:42:36	UTC+0000			
0x00000000023dfda0	svchost.exe	1056	652	0x07940120	2012-07-22 02:42:33	UTC+0000			
0x00000000023fcda0	wuauclt.exe	1136	1004	0x07940180	2012-07-22 02:43:46	UTC+0000			
0x0000000002495650	svchost.exe	1220	652	0x07940160	2012-07-22 02:42:35	UTC+0000			
0x0000000002498700	winlogon.exe	608	368	0x07940060	2012-07-22 02:42:32	UTC+0000			
0x00000000024a0598	csrss.exe	584	368	0x07940040	2012-07-22 02:42:32	UTC+0000			
0x00000000024f1020	smss.exe	368	4	0x07940020	2012-07-22 02:42:31	UTC+0000			
0x00000000025001d0	svchost.exe	1004	652	0x07940100	2012-07-22 02:42:33	UTC+0000			
0x0000000002511360	svchost.exe	824	652	0x079400c0	2012-07-22 02:42:33	UTC+0000			
0x00000000025c89c8	System	4	0	0x002fe000					

Η έξοδος δείχνει ότι δεν υπάρχουν πρόσθετες τερματισμένες διεργασίες, και ο αναλυτής μπορεί να εξετάσει τις υπάρχουσες για πιθανή κακόβουλη συμπεριφορά.

Δέντρο διεργασιών (pstree)

Το pstree εμφανίζει τη δομή πατρικών και θυγατρικών διεργασιών. Ένας δείκτης συμβιβασμού του συστήματος είναι η εκτέλεση διεργασίας εκτός των συνηθισμένων γονικών διεργασιών.

```
dfir@Desktop-SFARF6G~$ volatility -f cridex_laptop.mem -profile=WinXPSP2x86 pstree
```

Volatility Foundation Volatility Framework 2.6						
Name	Pid	PPid	Thds	Hnds	Time	
0x823c89c8:system	4	0	53	240	1970-01-01 00:00:00 UTC+0000	
. 0x822f1020:smss.exe	368	4	3	19	2012-07-22 02:42:31 UTC+0000	
.. 0x82298700:winlogon.exe	608	368	23	519	2012-07-22 02:42:32 UTC+0000	
... 0x81e2ab28:services.exe	652	608	16	243	2012-07-22 02:42:32 UTC+0000	
.... 0x821dfda0:svchost.exe	1056	652	5	60	2012-07-22 02:42:33 UTC+0000	
.... 0x81eb17b8:spoolsv.exe	1512	652	14	113	2012-07-22 02:42:36 UTC+0000	
.... 0x81e29ab8:svchost.exe	908	652	9	226	2012-07-22 02:42:33 UTC+0000	
.... 0x823001d0:svchost.exe	1004	652	64	1118	2012-07-22 02:42:33 UTC+0000	
..... 0x8205bda0:wuauc1t.exe	1588	1004	5	132	2012-07-22 02:44:01 UTC+0000	
..... 0x821fcda0:wuauc1t.exe	1136	1004	8	173	2012-07-22 02:43:46 UTC+0000	
.... 0x82311360:svchost.exe	824	652	20	194	2012-07-22 02:42:33 UTC+0000	
.... 0x820e8da0:alg.exe	788	652	7	104	2012-07-22 02:43:01 UTC+0000	
.... 0x82295650:svchost.exe	1220	652	15	197	2012-07-22 02:42:35 UTC+0000	
... 0x81e2a3b8:lsass.exe	664	608	24	330	2012-07-22 02:42:32 UTC+0000	
.. 0x822a0598:csrss.exe	584	368	9	326	2012-07-22 02:42:32 UTC+0000	
0x821dea70:explorer.exe	1484	1464	17	415	2012-07-22 02:42:36 UTC+0000	
. 0x81e7bda0:reader_sl.exe	1640	1484	5	39	2012-07-22 02:42:36 UTC+0000	

Ανάλυση των τριών προηγούμενων plugins δείχνει ότι το PID 1640 συνδέεται με το reader_sl.exe, που εκτελέστηκε μέσω του Windows Explorer.

Λίστα DLLs (dlllist)

Ο αναλυτής μπορεί να ελέγξει τα φορτωμένα DLLs μιας διεργασίας για να δει ποια αρχεία χρησιμοποίησε. Για το PID 1640:

```
dfir@Desktop-SFARF6G~$ volatility -f cridex_laptop.mem -profile=WinXPSP2x86 -p 1640 dlllist
```

Volatility Foundation Volatility Framework 2.6				

reader_sl.exe pid: 1640				
Command line : "C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe"				
Service Pack 3				
Base	Size	LoadCount	LoadTime	Path
0x00400000	0xa000	0xffff		C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe
0x7c900000	0xaf000	0xffff		C:\WINDOWS\system32\ntdll.dll
0x7c800000	0xf6000	0xffff		C:\WINDOWS\system32\kernel32.dll
0x7e410000	0x91000	0xffff		C:\WINDOWS\system32\USER32.dll
0x77f10000	0x49000	0xffff		C:\WINDOWS\system32\GDI32.dll
0x77dd0000	0x9b000	0xffff		C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000	0x92000	0xffff		C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000	0x11000	0xffff		C:\WINDOWS\system32\Secur32.dll
0x7c9c0000	0x817000	0xffff		C:\WINDOWS\system32\SHELL32.dll
0x77c10000	0x58000	0xffff		C:\WINDOWS\system32\msvcrt.dll
0x77f60000	0x76000	0xffff		C:\WINDOWS\system32\SHLWAPI.dll
0x7c420000	0x87000	0xffff		C:\WINDOWS\WinSxS\x86_Microsoft_VC800_CRT_1fc8b3b9a1e18a3b_8.0.50727.762_x-ww_6b128700\WSVCP80.dll
0x78130000	0x9b000	0xffff		C:\WINDOWS\WinSxS\x86_Microsoft_VC800_CRT_1fc8b3b9a1e18a3b_8.0.50727.762_x-ww_6b128700\WSVCR80.dll
0x773d0000	0x103000	0x1		C:\WINDOWS\WinSxS\x86_Microsoft_Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
0x5d090000	0x9a000	0x1		C:\WINDOWS\system32\comctl32.dll
0x5ad70000	0x38000	0x2		C:\WINDOWS\system32\uxtheme.dll
0x71ab0000	0x17000	0x1		C:\WINDOWS\system32\WS2_32.dll
0x71aa0000	0x8000	0x1		C:\WINDOWS\system32\WS2HELP.dll

Η έξοδος δείχνει διάφορα DLLs που φόρτωσε η διεργασία, τα οποία θα εξεταστούν περαιτέρω.

Handles

Το plugin handles δείχνει τους τύπους handles που είναι ανοιχτοί σε μια διεργασία, όπως αρχεία ή κλειδιά μητρώου. Για το PID 1640:

```
dfir@Desktop-SFARF6G~$ volatility -f cridex_laptop.mem -profile=WinXPSP2x86 -p 1640 handles
```

Offset(V)	Pid	Handle	Access Type	Details
0xe10096e0	1640	0x4	0xf0003 KeyedEvent	CritSecOutOfMemoryEvent
0xe159c978	1640	0x8	0x3 Directory	KnownDlls
0x82211678	1640	0xc	0x100020 File	\Device\HarddiskVolume1\Documents and Settings\Robert
0x82210208	1640	0x10	0x100020 File	\Device\HarddiskVolume1\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.762_x-ww_6b128700
0xe14916d0	1640	0x14	0xf000f Directory	Windows
0xe1c6a588	1640	0x18	0x21f0001 Port	
0x82319610	1640	0x1c	0x21f0003 Event	
0x8205a2a0	1640	0x20	0xf037f WindowStation	WinSta0
0x822f8168	1640	0x24	0xf01ff Desktop	Default
0x8205a2a0	1640	0x28	0xf037f WindowStation	WinSta0
0x82311280	1640	0x2c	0x100003 Semaphore	
0x82234dd0	1640	0x30	0x100003 Semaphore	
0xe1c042d0	1640	0x34	0x20f003f Key	MACHINE
0xe1c6c308	1640	0x38	0x2000f Directory	BaseNamedObjects
0x8213d0e0	1640	0x3c	0x1f0003 Semaphore	shell.{A48F1A32-A340-11D1-BC68-00A0C90312E1}
0xe1835648	1640	0x40	0x20f003f Key	USER\5-1-5-21-789336058-261478967-1417001333-1003
0x820d2f28	1640	0x44	0x100020 File	\Device\HarddiskVolume1\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
0xe1c72300	1640	0x48	0x1f0001 Port	
0xe17d3938	1640	0x4c	0x4 Section	
0x81de10c8	1640	0x50	0x1f0003 Event	
0x822924c8	1640	0x54	0xf03ff Thread	TID 1648 PID 1640
0x821dd728	1640	0x58	0x1f0003 Event	
0x82196418	1640	0x5c	0x1f0003 Event	
0x820022e0	1640	0x60	0x1f0003 Event	
0x82002218	1640	0x64	0x1f0003 Event	
0x822924c8	1640	0x68	0xf03ff Thread	TID 1648 PID 1640
0x821dc270	1640	0x6c	0x100001 File	\Device\KsecDD
0xe1c5cfb8	1640	0x70	0x10 Key	USER\5-1-5-21-789336058-261478967-1417001333-1003\SOFTWARE\MICROSOFT\WSH\8149A9A8
0xe1c6c030	1640	0x74	0x18 Token	
0x81de1e68	1640	0x78	0x1f0003 Event	
0x81dd2e08	1640	0x7c	0x1f0003 IoCompletion	
0x81de3c70	1640	0x80	0x1f0003 IoCompletion	
0x81dd2e08	1640	0x84	0x1f0003 IoCompletion	
0x822fdb00	1640	0x88	0x1f0001 Mutant	XMM00000668
0x822d0d98	1640	0x8c	0x1f0003 Event	XME00000668
0xe154db20	1640	0x90	0x10 Key	USER\5-1-5-21-789336058-261478967-1417001333-1003\SOFTWARE\MICROSOFT\WSH\9DBBCFAD
0x820fd260	1640	0x94	0x1f0003 Semaphore	shell.{210A4BA0-JAEA-1069-A2D9-08002B30309D}
0x81e9d708	1640	0x98	0x1f0001 Mutant	XMR8149A9A8
0x81e1d3c0	1640	0x9c	0x1f0003 Event	

Η έξοδος δείχνει ανοιχτές διεργασίες, threads και registry keys, σημαντικά για την κατανόηση της συμπεριφοράς του reader_sl.exe.

LDR modules

Μια κοινή πρακτική των δημιουργών κακόβουλου λογισμικού είναι η προσπάθεια απόκρυψης των δραστηριοτήτων του malware. Μια τεχνική είναι η προσπάθεια απόκρυψης των DLL αρχείων που σχετίζονται με τον κακόβουλο κώδικα. Αυτό μπορεί να επιτευχθεί αποσυνδέοντας (unlinking) τη ύποπτη DLL από το **Process Environment Block (PEB)**. Παρόλο που αυτό μπορεί να προσφέρει κάποια επιφανειακή συγκαλυμμένη λειτουργία, εξακολουθούν να υπάρχουν ίχνη της ύπαρξης της DLL μέσα στο **Virtual Address Descriptor (VAD)**. Το VAD είναι ένας μηχανισμός που εντοπίζει τη βασική διεύθυνση και το πλήρες μονοπάτι της DLL.

Το plugin **ldrmodules** συγκρίνει τη λίστα των διεργασιών και ελέγχει αν βρίσκονται στο PEB. Η παρακάτω εντολή εκτελεί το ldrmodules στο Cridex image file:

```
dfir@Desktop-SFARF6G~$ volatility -f cridex_laptop.mem -profile=WinXPSP2x86 -p 1640 ldrmodules
```

Volatility Foundation Volatility Framework 2.6						
Pid	Process	Base	InLoad	InInit	InMem	MappedPath
1640	reader_sl.exe	0x00400000	True	False	True	\Program Files\Adobe\Reader 9.0\Reader\reader_sl.exe
1640	reader_sl.exe	0x7c800000	True	True	True	\WINDOWS\system32\kernel32.dll
1640	reader_sl.exe	0x773d0000	True	True	True	\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6
1640	reader_sl.exe	0x7c420000	True	True	True	\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b
1640	reader_sl.exe	0x5d090000	True	True	True	\WINDOWS\system32\comctl32.dll
1640	reader_sl.exe	0x77f60000	True	True	True	\WINDOWS\system32\shlwapi.dll
1640	reader_sl.exe	0x77f10000	True	True	True	\WINDOWS\system32\gdi32.dll
1640	reader_sl.exe	0x78130000	True	True	True	\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b
1640	reader_sl.exe	0x71aa0000	True	True	True	\WINDOWS\system32\ws2help.dll
1640	reader_sl.exe	0x77e70000	True	True	True	\WINDOWS\system32\rpcrt4.dll
1640	reader_sl.exe	0x71ab0000	True	True	True	\WINDOWS\system32\ws2_32.dll
1640	reader_sl.exe	0x7c9c0000	True	True	True	\WINDOWS\system32\shell32.dll
1640	reader_sl.exe	0x77dd0000	True	True	True	\WINDOWS\system32\advapi32.dll
1640	reader_sl.exe	0x77fe0000	True	True	True	\WINDOWS\system32\securl32.dll
1640	reader_sl.exe	0x7e410000	True	True	True	\WINDOWS\system32\user32.dll
1640	reader_sl.exe	0x7c900000	True	True	True	\WINDOWS\system32\ntdll.dll
1640	reader_sl.exe	0x77c10000	True	True	True	\WINDOWS\system32\msvcrt.dll
1640	reader_sl.exe	0x5ad70000	True	True	True	\WINDOWS\system32\uxtheme.dll

Μια ανασκόπηση της εξόδου αποκαλύπτει μια ενδιαφέρουσα εγγραφή στην πρώτη γραμμή: Από αυτήν την έξοδο, η διεργασία **reader_sl.exe** φαίνεται να έχει πρόβλημα που σχετίζεται με το DLL αρχείο. Ο δείκτης (Pid 1640) ότι η διαδικασία είναι ύποπτη είναι το **False** στην στήλη **InInit** για την πρώτη εγγραφή. Αυτό υποδεικνύει ότι το εκτελέσιμο έχει αποσυνδέσει τα DLL αρχεία και το αρχείο **reader_sl.exe** χρήζει περαιτέρω έρευνας.

Process xview

Ένα ακόμη χρήσιμο plugin για την ανίχνευση κρυφών διεργασιών είναι το **psxview**. Το plugin αυτό συγκρίνει τις ενεργές διεργασίες που υποδεικνύονται από το **psActiveProcessHead** με οποιεσδήποτε άλλες πιθανές πηγές μέσα στην εικόνα μνήμης. Για να εκτελέσετε το plugin, πληκτρολογήστε την παρακάτω εντολή:

```
dfir@Desktop-SFARF6G~$ volatility -f cridex_laptop.mem -profile=WinXPSP2x86 psxview
```

Volatility Foundation Volatility Framework 2.6										
Offset(P)	Name	PID	pslist	psscan	thrdproc	pspcid	csrss	session	deskthrd	ExitTime
0x02498700	winlogon.exe	608	True	True	True	True	True	True	True	
0x02511360	svchost.exe	824	True	True	True	True	True	True	True	
0x022e8da0	alg.exe	788	True	True	True	True	True	True	True	
0x020b17b8	spoolsv.exe	1512	True	True	True	True	True	True	True	
0x0202ab28	services.exe	652	True	True	True	True	True	True	True	
0x02495650	svchost.exe	1220	True	True	True	True	True	True	True	
0x0207bda0	reader_sl.exe	1640	True	True	True	True	True	True	True	
0x025001d0	svchost.exe	1004	True	True	True	True	True	True	True	
0x02029ab8	svchost.exe	908	True	True	True	True	True	True	True	
0x023fcd00	wuauclt.exe	1136	True	True	True	True	True	True	True	
0x0225bda0	wuauclt.exe	1588	True	True	True	True	True	True	True	
0x0202a3b8	lsass.exe	664	True	True	True	True	True	True	True	
0x023dea70	explorer.exe	1484	True	True	True	True	True	True	True	
0x023dfd00	svchost.exe	1056	True	True	True	True	True	True	True	
0x024f1020	smss.exe	368	True	True	True	True	False	False	False	
0x025c89c8	System	4	True	True	True	True	False	False	False	
0x024a0598	csrss.exe	584	True	True	True	True	False	True	True	

Ένα **False** στη στήλη υποδηλώνει ότι η διαδικασία δεν βρέθηκε σε αυτήν την περιοχή. Αυτό επιτρέπει στον αναλυτή να εξετάσει τη λίστα και να καθορίσει αν υπάρχει νόμιμος λόγος για τον οποίο η διαδικασία δεν εμφανίζεται εκεί ή αν πρόκειται για απόπειρα απόκρυψης της διαδικασίας.

Volatility network analysis

Στην ενότητα **Network connections methodology**, συζητήθηκε η έναρξη της ανάλυσης από ένα URL ή μια IP διεύθυνση που σχετίζεται με κακόβουλη δραστηριότητα. Το Volatility μπορεί να εξάγει από την εικόνα μνήμης υφιστάμενες και ακόμη και τερματισμένες συνδέσεις δικτύου που ήταν ενεργές τη στιγμή της λήψης της μνήμης. Το plugin **netscan** σαρώνει την εικόνα μνήμης για δικτυακά στοιχεία. Το plugin εντοπίζει TCP και UDP endpoints και listeners, παρέχοντας τις τοπικές και απομακρυσμένες IP διευθύνσεις. Το **netscan** λειτουργεί μόνο με 32-bit και 64-bit Windows Vista, Windows 7, Windows 10 και Windows 2008 Server ή νεότερα. Μια βασική δυνατότητα που βοηθά τους αναλυτές είναι ότι η ιδιοκτησία της διαδικασίας εμφανίζεται στην έξοδο για κάθε σύνδεση, κάτι που είναι χρήσιμο για να καθοριστεί αν μια σύνδεση χρησιμοποιεί Internet Explorer ή άλλη διαδικασία, όπως Remote Desktop Services ή SMB.

connscan

Για παλαιότερες εκδόσεις των Windows, όπως τα Windows XP και παλαιότερα, το plugin **connscan** εκτελεί την ίδια λειτουργία με το netscan. Το connscan εντοπίζει το **_TCPT_OBJECT** και μπορεί να βρει τόσο υπάρχουσες όσο και τερματισμένες συνδέσεις. Αυτό παρέχει στους αναλυτές δεδομένα σχετικά με τις συνδέσεις σε σχέση με τις διεργασίες που εκτελούνταν. Για να προσδιοριστούν οι συνδέσεις δικτύου, εκτελέστε την ακόλουθη εντολή για την εικόνα Cridex:

```
dfir@Desktop-SFARF6G~$ volatility -f cridex_laptop.mem -profile=WinXPSP2x86 connscan
```

Volatility Foundation Volatility Framework 2.6			
Offset(P)	Local Address	Remote Address	Pid
0x02087620	172.16.112.128:1038	41.168.5.140:8080	1484
0x023a8008	172.16.112.128:1037	125.19.103.198:8080	1484

Η έξοδος δείχνει ότι το PID 1484, δηλαδή το **Explorer.exe**, γονική διαδικασία της **Reader_sl.exe**, επικοινωνούσε με δύο εξωτερικές IP διευθύνσεις. Μια ανασκόπηση της βάσης απειλής **VirusTotal** έδειξε ότι η IP διεύθυνση **41.168.5.140** σχετίζονταν με αρκετά URLs που επικοινωνούσαν με κακόβουλα εκτελέσιμα.

Λαμβάνοντας υπόψη τα δεδομένα από την ανάλυση διεργασιών μαζί με την IP διεύθυνση από τις συνδέσεις δικτύου, υπάρχει επαρκής λόγος

Communicating Files ⓘ			
Scanned	Detections	Type	Name
2019-07-26	54 / 70	Win32 EXE	MFC100JPN.DLL
2017-12-06	61 / 66	Win32 EXE	kb01445398.exe
2018-02-11	60 / 67	Win32 EXE	kb00113312.exe
2016-01-18	48 / 54	Win32 EXE	kb01397018.exe
2015-10-20	51 / 57	Win32 EXE	kb00591945.exe
2017-12-06	58 / 67	Win32 EXE	kb00421819.exe
2016-01-13	50 / 56	Win32 EXE	kb01382314.exe
2017-12-06	56 / 65	Win32 EXE	kb00578763.exe
2016-01-29	49 / 54	Win32 EXE	kb01300184.exe

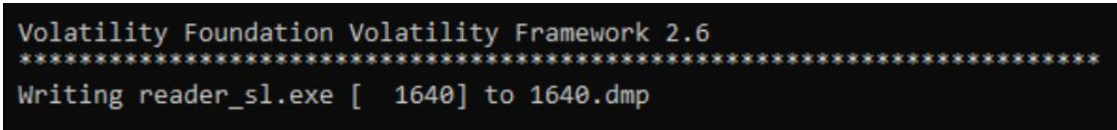
να πιστέψουμε ότι μία ή και οι δύο διεργασίες **Explorer.exe** και **Reader_sl.exe** σχετίζονται με κακόβουλο κώδικα. Στην επόμενη ενότητα, το **Reader_sl.exe** θα εξαχθεί μαζί με τα συσχετιζόμενα DLL αρχεία για περαιτέρω ανάλυση.

8.8. Εξαγωγή αποδεικτικών στοιχείων με το Volatility

Όπως αναφέρθηκε προηγουμένως, ένας από τους βασικούς στόχους της ανάλυσης μνήμης είναι να διαπιστωθεί εάν υπάρχουν ύποπτα δεδομένα που υποδεικνύουν την παρουσία κακόβουλου λογισμικού. Σε περίπτωση που εντοπιστούν τέτοια δεδομένα, όπως στην περίπτωση της εικόνας μνήμης Cridex, μπορούν να αποκτηθούν για περαιτέρω ανάλυση.

Αποθήκευση μνήμης (Memory dump): Κατά τη διάρκεια της ανάλυσης, μπορεί να γίνει απαραίτητο να εξαχθούν οι σελίδες της μνήμης που σχετίζονται με μια διεργασία. Σε αυτή την περίπτωση, χρησιμοποιείται το plugin **memdump** στη μνήμη, με την έξοδο να κατευθύνεται σε έναν φάκελο, με την εξής εντολή:

```
dfir@Desktop-SFARF6G~$ volatility -f cridex_laptop.mem -profile=WinXPSP2x86 -p 1640 memdump --dump-dir /mnt/d/Suspicious_Process_PID_1640
```



```
Volatility Foundation Volatility Framework 2.6
*****
Writing reader_sl.exe [ 1640] to 1640.dmp
```

Η εντολή παράγει ένα αρχείο DMP στο επιλεγμένο σημείο αποθήκευσης. Είναι καλή πρακτική να αναπτύσσεται μια **συμβατική ονοματοδοσία** για τους φακέλους που σχετίζονται με την ανάλυση μνήμης, ώστε τα αρχεία να παραμένουν οργανωμένα. Στην περίπτωση αυτή, χρησιμοποιείται το όνομα φακέλου **Suspect_Process_PID_1640**. Σημειώνεται ότι η εξαγωγή μπορεί να περιέχει κακόβουλο λογισμικό και πρέπει να πραγματοποιείται σε κατάλληλο σύστημα.

Αποθήκευση αρχείων DLL (DLL file dump): Εάν ο αναλυτής εντοπίσει μια ύποπτη διεργασία στη μνήμη, μπορεί να χρησιμοποιήσει το plugin **dlldump** για να εξαχθούν τα περιεχόμενα των αρχείων DLL στον τοπικό υπολογιστή. Αυτό επιτρέπει την εξέταση των DLL και τη σύγκρισή τους με νόμιμα αρχεία, για να διαπιστωθεί αν είναι κακόβουλα. Για παράδειγμα, η διεργασία **Reader_sl.exe** με PID 1640 έχει εντοπιστεί ως πιθανώς κακόβουλη. Για να εξαχθούν τα DLL αρχεία:

```
dfir@Desktop-SFARF6G~$ volatility -f cridex_laptop.mem --profile=WinXPSP2x86 -p 1640 dlldump --dump-dir /mnt/d/Suspicious_Process_PID_1640/
```

Volatility Foundation Volatility Framework 2.6				
Process(V)	Name	Module Base	Module Name	Result
0x81e7bda0	reader_sl.exe	0x00040000	Reader_sl.exe	OK: module.1640.207bda0.400000.dll
0x81e7bda0	reader_sl.exe	0x07c90000	ntdll.dll	OK: module.1640.207bda0.7c900000.dll
0x81e7bda0	reader_sl.exe	0x07813000	MSVCR80.dll	OK: module.1640.207bda0.78130000.dll
0x81e7bda0	reader_sl.exe	0x07c42000	MSVCP80.dll	OK: module.1640.207bda0.7c420000.dll
0x81e7bda0	reader_sl.exe	0x077f1000	GDI32.dll	OK: module.1640.207bda0.77f10000.dll
0x81e7bda0	reader_sl.exe	0x077f6000	SHLWAPI.dll	OK: module.1640.207bda0.77f60000.dll
0x81e7bda0	reader_sl.exe	0x05ad7000	uxtheme.dll	OK: module.1640.207bda0.5ad70000.dll
0x81e7bda0	reader_sl.exe	0x077e7000	RPCRT4.dll	OK: module.1640.207bda0.77e70000.dll
0x81e7bda0	reader_sl.exe	0x05d09000	comctl32.dll	OK: module.1640.207bda0.5d090000.dll
0x81e7bda0	reader_sl.exe	0x071aa000	WS2HELP.dll	OK: module.1640.207bda0.71aa0000.dll

Αποθήκευση εκτελέσιμου αρχείου (Executable dump): Από την ανασκόπηση των αποτελεσμάτων, η διεργασία 1640 και το εκτελέσιμο **Reader_sl.exe** θεωρούνται ύποπτα για παρουσία κακόβουλου λογισμικού. Παρόλο που τα δεδομένα που συλλέχθηκαν είναι χρήσιμα, συχνά χρειάζεται επιβεβαίωση από εξωτερικές πηγές, όπως:

- Έλεγχος του hash του εκτελέσιμου σε τρίτες βάσεις δεδομένων.
- Αποστολή του εκτελέσιμου σε ομάδα ανάλυσης κακόβουλου λογισμικού.

Για να εξαχθεί το εκτελέσιμο από τη μνήμη, χρησιμοποιείται το plugin **procdump**:

```
volatility -f cridex_laptop.mem --profile=WinXPSP2x86 -p 1640 procdump --dump-dir /mnt/d/Suspicious_Process_PID_1640/
```

Volatility Foundation Volatility Framework 2.6			
Process(V)	ImageBase	Name	Result
0x81e7bda0	0x00040000	reader_sl.exe	OK: executable.1640.exe

Η εξέταση του φακέλου επιβεβαιώνει ότι το εκτελέσιμο, η μνήμη της διεργασίας και τα DLL αρχεία έχουν εξαχθεί με επιτυχία. Αφού αποκτηθούν, τα αρχεία μπορούν να αναλυθούν για κακόβουλο λογισμικό είτε από την ομάδα αντίδρασης σε περιστατικά είτε από ξεχωριστή ομάδα ανάλυσης malware.

	1640.dmp	9/8/2019 2:43 PM	DMP File	75,396 KB
	executable.1640	9/8/2019 2:48 PM	Application	29 KB
	module.1640.207bda0.5ad70000.dll	9/8/2019 2:46 PM	Application exten...	214 KB
	module.1640.207bda0.5d090000.dll	9/8/2019 2:46 PM	Application exten...	603 KB
	module.1640.207bda0.7c9c0000.dll	9/8/2019 2:46 PM	Application exten...	8,263 KB
	module.1640.207bda0.7c420000.dll	9/8/2019 2:46 PM	Application exten...	536 KB
	module.1640.207bda0.7c800000.dll	9/8/2019 2:46 PM	Application exten...	967 KB
	module.1640.207bda0.7c900000.dll	9/8/2019 2:46 PM	Application exten...	690 KB
	module.1640.207bda0.7e410000.dll	9/8/2019 2:46 PM	Application exten...	565 KB

8.9. Ανάλυση μνήμης με το εργαλείο Strings

Στις προηγούμενες ενότητες, τα εργαλεία Redline και Volatility επικεντρώνονταν σε εκείνα τα τμήματα της εικόνας μνήμης που είναι χαρτογραφημένα. Σε περίπτωση που κάποια δεδομένα δεν είναι σωστά χαρτογραφημένα, αυτά τα εργαλεία δεν θα μπορούν να τα εξαγάγουν και να τα παρουσιάσουν σωστά. Αυτό είναι ένα από τα μειονεκτήματα αυτών των εργαλείων για ανάλυση μνήμης. Υπάρχει σημαντική ποσότητα δεδομένων που μπορεί να γίνει μη δομημένη και αόρατη σε αυτά τα εργαλεία. Αυτό μπορεί να συμβεί όταν οι δικτυακές συνδέσεις τερματίζονται ή οι διεργασίες ολοκληρώνονται. Ακόμη και αν δεν εμφανίζονται κατά την εξέταση της RAM μέσω Redline ή Volatility, συχνά παραμένουν ίχνη στοιχείων (trace evidence).

Ένα εργαλείο που είναι χρήσιμο για την εξαγωγή αυτών των ιχνών είναι η εντολή **strings**, η οποία υπάρχει σε πολλές εκδόσεις Linux και Windows. Το Strings επιτρέπει σε έναν αναλυτή να αναζητήσει αναγνώσιμους χαρακτήρες (human-readable strings). Με δεδομένο ένα σύνολο λέξεων-κλειδιών ή εντολών **GREP** (Global Regular Expression Print), ο αναλυτής μπορεί να εξαγάγει επιπλέον σχετικά δεδομένα, ακόμη και από captures μνήμης που μπορεί να έχουν υποστεί αλλοίωση από κακόβουλο λογισμικό ή εσφαλμένη εξαγωγή.

Εγκατάσταση του Strings

Το Strings συνήθως περιλαμβάνεται προεγκατεστημένο σε πολλές διανομές Linux. Στα Windows υπάρχει ένα αυτόνομο εκτελέσιμο για αναζήτηση strings διαθέσιμο στη διεύθυνση: <https://docs.microsoft.com/en-us/sysinternals/downloads/strings>

Αν το Strings δεν είναι εγκατεστημένο στη Linux πλατφόρμα που χρησιμοποιεί ο αναλυτής, η εγκατάσταση γίνεται με την εντολή:

```
dfir@Desktop-SFARF6G~$ sudo apt install binutils
```

Παρόλο που πρόκειται για ένα σχετικά απλό εργαλείο, το Strings είναι πολύ ισχυρό για αναζήτηση συγκεκριμένων λέξεων-κλειδιών μέσα σε μεγάλα σύνολα δεδομένων. Σκοπός εδώ είναι η εξαγωγή συγκεκριμένων σημείων δεδομένων με την εξής σύνταξη:

```
dfir@Desktop-SFARF6G~$ strings cridex_laptop.mem | grep <Regular Expression>
```

Στην παραπάνω εντολή, το Strings αναζητά στην εικόνα μνήμης cridex_laptop.mem την κανονική έκφραση (regular expression) που ακολουθεί την εντολή grep. Η κανονική έκφραση μπορεί να περιλαμβάνει IP διευθύνσεις, URLs, εντολές ή πιθανώς scripts που έχουν εκτελεστεί στο σύστημα.

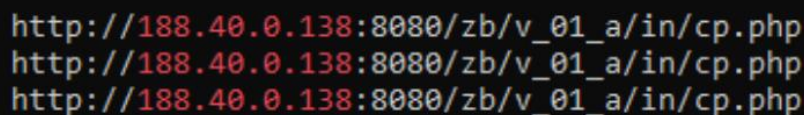
Αναζήτηση IP διευθύνσεων

Στην προηγούμενη ενότητα σχετικά με το Volatility, η IP διεύθυνση 41.168.5.140 εντοπίστηκε με τη χρήση του plugin connscan. Το μειονέκτημα αυτής της μεθόδου είναι ότι αν η σύνδεση έχει κλείσει και δεν υπάρχει δραστηριότητα, δεν μπορεί να φανεί με το Volatility. Σε αυτή την περίπτωση, για να επεκταθεί η αναζήτηση των IP διευθύνσεων που βρίσκονται στη μνήμη, χρησιμοποιείται η εντολή:

```
strings cridex_laptop.mem | grep -oE "\b([0-9]{1,3}\.){3}[0-9]{1,3}\b"
```

Αυτή η εντολή αναζητά οποιοδήποτε μοτίβο που αντιστοιχεί σε IP διευθύνσεις. Στην ανάλυση της μνήμης του Cridex, εμφανίζονται αρκετές IP διευθύνσεις, συμπεριλαμβανομένων εσωτερικών IP και broadcast διευθύνσεων. Η ανάλυση έδειξε ότι η IP 188.40.0.138 βρέθηκε κάποια στιγμή στη μνήμη. Για να γίνει δεύτερη αναζήτηση συγκεκριμένα για αυτή την IP, χρησιμοποιείται η εντολή:

```
strings cridex_laptop.mem | grep 188.40.0.138
```

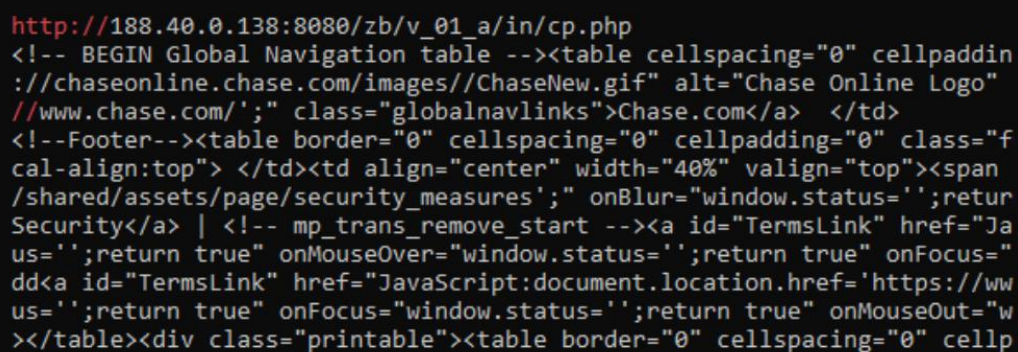


```
http://188.40.0.138:8080/zb/v_01_a/in/cp.php
http://188.40.0.138:8080/zb/v_01_a/in/cp.php
http://188.40.0.138:8080/zb/v_01_a/in/cp.php
```

Αναζήτηση HTTP

Συχνά, οι επιτιθέμενοι χρησιμοποιούν μια IP διεύθυνση ως μέρος ενός URL που χρησιμοποιείται ως μηχανισμός παράδοσης κακόβουλου λογισμικού. Για να αναζητηθούν καταχωρήσεις HTTP στη μνήμη, χρησιμοποιείται η εντολή:

```
strings cridex_laptop.mem | grep "http://"
```



```
http://188.40.0.138:8080/zb/v_01_a/in/cp.php
<!-- BEGIN Global Navigation table --><table cellpadding="0" cellspacing="0" border="0">
|  |
| --- |
|  |


<!-- Footer --><table border="0" cellpadding="0" cellspacing="0" class="f
cal-align:top"> </td><td align="center" width="40%" valign="top"><span
/shared/assets/page/security_measures';" onBlur="window.status='';retur
Security</a> | <!-- mp_trans_remove_start --><a id="TermsLink" href="Ja
us='';return true" onMouseOver="window.status='';return true" onFocus="
dd<a id="TermsLink" href="JavaScript:document.location.href='https://ww
us='';return true" onFocus="window.status='';return true" onMouseOut="w
></table><div class="printable"><table border="0" cellpadding="0" cellspacing="0">
```

Από την ανάλυση του αποτελέσματος, εμφανίζονται ενδιαφέροντα δεδομένα, όπως η URL <http://chaseonline.com/> και σχετικός κώδικας ιστοσελίδας. Έρευνα για το Cridex δείχνει ότι χρησιμοποιείται για κλοπή τραπεζικών στοιχείων μέσω hooking διαφόρων APIs στον web browser και ανακατεύθυνση της κυκλοφορίας, μεταξύ άλλων και για το Chase Bank.

Αυτό το παράδειγμα δείχνει πώς το Strings μπορεί να χρησιμοποιηθεί για τη συλλογή επιπλέον αποδεικτικών στοιχείων και για την παροχή πρόσθετου πλαισίου σε μια διερεύνηση περιστατικού. Το Strings περιορίζεται μόνο από τις λέξεις-κλειδιά που μπορεί να χρησιμοποιήσει ο αναλυτής.

Το κεφάλαιο αυτό ανέλυσε δύο κύριους τομείς της ανάλυσης μνήμης. Πρώτον, τα διαθέσιμα δεδομένα και η μεθοδολογία που μπορεί να ακολουθηθεί. Επιπλέον, εξετάστηκαν διάφορα εργαλεία, όπως τα Redline, Volatility και Strings. Εκτός από μια επισκόπηση αυτών των εργαλείων, αναλύθηκαν και αρκετές από τις δυνατότητές τους. Αυτό αποτελεί μόνο μια επιφανειακή παρουσίαση του πλήθους

των χαρακτηριστικών που προσφέρει το κάθε εργαλείο στον αναλυτή απάντησης σε περιστατικά. Συνδυασμένα με μια μεθοδολογία ανάλυσης της μνήμης RAM του συστήματος, αυτά τα εργαλεία μπορούν να προσφέρουν στον αναλυτή ένα ισχυρό μέσο για τον εντοπισμό αν ένα σύστημα έχει παραβιαστεί. Καθώς το κακόβουλο λογισμικό γίνεται ολοένα πιο προηγμένο, συμπεριλαμβανομένου λογισμικού που εκτελείται εξ ολοκλήρου στη μνήμη RAM, είναι κρίσιμο οι αναλυτές να ενσωματώσουν την ανάλυση μνήμης στις δυνατότητές τους. Ο συνδυασμός αυτών των τεχνικών με τη συλλογή δικτυακών αποδεικτικών στοιχείων μπορεί να παρέχει στους αναλυτές και στους οργανισμούς τους ένα ισχυρό εργαλείο για τον εντοπισμό και την αντιμετώπιση ενός περιστατικού.

9

Ανάλυση Αποθηκευτικού Χώρου Συστήματος

Μέχρι στιγμής, τα στοιχεία που έχουν αναλυθεί επικεντρώνονται σε εκείνα που προέρχονται από το δίκτυο ή τη μνήμη του συστήματος. Αν και η βασική αιτία ενός περιστατικού μπορεί να εξαχθεί από αυτές τις πηγές αποδεικτικών στοιχείων, είναι σημαντικό να κατανοήσουμε πώς να αποκτούμε στοιχεία από τον αποθηκευτικό χώρο ενός συστήματος, είτε πρόκειται για αφαιρούμενα μέσα όπως USB, είτε για μεγαλύτερους συνδεδεμένους δίσκους. Σε αυτά τα μέσα υπάρχει τεράστιος όγκος δεδομένων που μπορούν να αξιοποιηθούν από τους αναλυτές ανταπόκρισης σε περιστατικά για τον προσδιορισμό της βασικής αιτίας. Σημειώνεται ότι αυτό το κεφάλαιο θα αγγίξει μόνο την επιφάνεια του θέματος, καθώς υπάρχουν ολόκληροι τόμοι αφιερωμένοι στο βάθος των διαθέσιμων εγκληματολογικών στοιχείων. Για να δοθεί καλύτερη κατανόηση της ανάλυσης αποθηκευτικού χώρου συστήματος, αυτό το κεφάλαιο θα επικεντρωθεί στα εξής θέματα.

Πλατφόρμες εγκληματολογίας: Υπάρχει μια ποικιλία εμπορικών και ανοικτού κώδικα πλατφορμών που μπορούν να χρησιμοποιηθούν για την ανάλυση αποθηκευτικού χώρου συστήματος. Αυτή η ενότητα θα αναδείξει τα βασικά χαρακτηριστικά και τις πιθανές επιλογές που έχουμε.

Autopsy: Για να παρουσιαστεί μια πλατφόρμα ανοικτού κώδικα που μπορεί να χρησιμοποιηθεί στην ανάλυση αποθηκευτικού χώρου, το μεγαλύτερο μέρος του κεφαλαίου θα χρησιμοποιήσει το εργαλείο Autopsy. Ορισμένα από τα χαρακτηριστικά του θα αναδειχθούν μέσω της χρήσης μιας δοκιμαστικής εικόνας.

Ανάλυση Master File Table (MFT): Η MFT περιέχει μια πλήρη λίστα όλων των αρχείων στο σύστημα και αποτελεί βασική πηγή δεδομένων για τους αναλυτές. Αυτή η ενότητα αναφέρεται στην εξαγωγή και ανάλυση της MFT.

Ανάλυση Registry: Αγαπημένος στόχος των δημιουργών malware και άλλων εκμεταλλεύσεων, οι αναλυτές θα πρέπει να εξοικειωθούν με την ανάλυση του registry. Αυτή η ενότητα παρέχει επισκόπηση της εξαγωγής και ανάλυσης του registry.

Η ανάλυση του αποθηκευτικού χώρου συστήματος είναι μια σύνθετη διαδικασία. Το βάθος και η έκτασή της δεν μπορούν να καλυφθούν σε ένα μόνο κεφάλαιο. Ωστόσο, το κεφάλαιο αυτό προσφέρει συγκεκριμένους τομείς εστίασης, δίνοντας στους αναλυτές καλύτερη κατανόηση των εργαλείων που μπορούν να χρησιμοποιηθούν, καθώς και των κρίσιμων δεδομένων που μπορούν να αξιοποιηθούν.

Πλατφόρμες εγκληματολογίας: Τα τελευταία 15 χρόνια, έχει αυξηθεί η ισχύς των πλατφορμών δισκοεγκληματολογίας. Για τον αναλυτή ανταπόκρισης σε περιστατικά, υπάρχουν επιλογές ως προς τον τύπο πλατφόρμας που μπορεί να χρησιμοποιηθεί για εξέταση δίσκων. Συχνά, ο περιοριστικός παράγοντας είναι το κόστος πιο προηγμένων συστημάτων, ενώ μια χαμηλότερου κόστους εναλλακτική μπορεί να είναι εξίσου αποτελεσματική για μια ομάδα ανταπόκρισης σε περιστατικά.

Υπάρχουν αρκετοί παράγοντες που πρέπει να ληφθούν υπόψη κατά την εξέταση λογισμικού για ανάλυση δίσκων. Πρώτον, έχει δοκιμαστεί η πλατφόρμα; Υπάρχουν οργανισμοί που ελέγχουν την αποτελεσματικότητα των πλατφορμών, όπως το **National Institute of Standards and Technology Computer Forensic Tools Testing Program** (<https://www.cfft.nist.gov/>). Δεύτερον, εξετάζεται η χρήση του εργαλείου σε ποινικές και αστικές διαδικασίες. Δεν υπάρχει ένα καθολικά αποδεκτό πρότυπο δικαστηρίου, αλλά τα εργαλεία πρέπει να συμμορφώνονται με τους κανόνες αποδεικτικών στοιχείων. Η χρήση μιας μη δοκιμασμένης ή μη σύμφωνης πλατφόρμας μπορεί να οδηγήσει σε αποκλεισμό των στοιχείων από νομικές διαδικασίες ή, σε χειρότερη περίπτωση, σε λανθασμένα συμπεράσματα από τον αναλυτή.

Ένα παράδειγμα μη δοκιμασμένης και εγκληματολογικά ακατάλληλης εργαλειοθήκης ήταν η υπόθεση **State of Connecticut vs. Amero**, όπου οι αρχές χρησιμοποίησαν ακατάλληλες μεθόδους και εργαλεία για να καταδικάσουν μια γυναίκα για την υποτιθέμενη έκθεση παιδιών σε πορνογραφικές διαφημίσεις. Η ανασκόπηση αποκάλυψε σημαντικές ελλείψεις στην εγκληματολογική εξέταση.

Ένας τελευταίος παράγοντας είναι πώς το εργαλείο εντάσσεται στο συνολικό σχέδιο ανταπόκρισης σε περιστατικά. Για παράδειγμα, τα εμπορικά εργαλεία δισκοεγκληματολογίας είναι εξαιρετικά στην εντοπισμό εικόνων και web artifacts, καθώς και στην εξαγωγή δεδομένων από τον ύποπτο δίσκο. Αυτό συχνά οφείλεται στη χρήση αυτών των εργαλείων από τις αρχές για διερεύνηση εγκλημάτων σεξουαλικής εκμετάλλευσης παιδιών. Αν και είναι χρήσιμες δυνατότητες, οι αναλυτές περιστατικών μπορεί να ενδιαφέρονται περισσότερο για εργαλεία που επιτρέπουν αναζητήσεις λέξεων-κλειδιών και ανάλυση χρονικών γραμμών για ανακατασκευή των γεγονότων πριν, κατά τη διάρκεια και μετά από ένα περιστατικό.

Συχνά χρησιμοποιούμενα χαρακτηριστικά σε πλατφόρμες εγκληματολογίας:

- **Προβολή δομής αρχείων:** Σημαντικό για γρήγορη ανασκόπηση γνωστών αρχείων.
- **Hex viewer:** Δίνει λεπτομερή εικόνα των αρχείων, χρήσιμη σε περιπτώσεις malware ή custom exploits.
- **Web artifacts:** Επιτρέπει ανάλυση δεδομένων που συνδέονται με αναζητήσεις και κοινωνική μηχανική.
- **Email carving:** Βοηθά στην ανάκτηση email για υποθέσεις παραβίασης πολιτικής ή παράνομης δραστηριότητας.
- **Image viewer:** Επιτρέπει προβολή εικόνων που μπορεί να σχετίζονται με πολιτικές ή εγκληματικές παραβάσεις.

- **Metadata:** Πληροφορίες όπως ημερομηνία/ώρα δημιουργίας, hashes αρχείων, και θέση αρχείου στο δίσκο.

Εμπορικές πλατφόρμες:

- **OpenText EnCase:** Πλήρης πλατφόρμα δισκοεγκληματολογίας με δυνατότητες για κινητές συσκευές.
- **AccessData Forensic Toolkit (FTK):** Συνοδεύεται από FTK Imager για απόκτηση δίσκων και μνήμης, χρησιμοποιείται από FBI και άλλες υπηρεσίες.
- **X-Ways Forensics:** Πιο οικονομική, λιγότερο απαιτητική σε πόρους, μπορεί να τρέξει από USB, κατάλληλη για μικρότερες ομάδες ή οργανισμούς.

Κάθε πλατφόρμα προσφέρει ένα πλήρες σύνολο χαρακτηριστικών για ευρύ φάσμα εγκληματολογικών εργασιών. Η εκπαίδευση των αναλυτών στη χρήση αυτών των πλατφορμών είναι απαραίτητη για την πλήρη αξιοποίηση των δυνατοτήτων τους.

9.1. Autopsy

Μία εναλλακτική λύση στα εμπορικά προγράμματα ψηφιακής εγκληματολογίας είναι το Autopsy. Το Autopsy είναι μια πλατφόρμα ψηφιακής εγκληματολογίας με γραφικό περιβάλλον (GUI), βασισμένη στο ανοικτού κώδικα εργαλείο The Sleuth Kit. Αυτή η πλατφόρμα ανοικτού κώδικα διαθέτει λειτουργίες που συνήθως βρίσκονται και σε εμπορικές πλατφόρμες, όπως ανάλυση χρονολογικών γεγονότων (timeline analysis), αναζήτηση με λέξεις-κλειδιά, ανάλυση ιστοσελίδων και email, καθώς και δυνατότητα φιλτραρίσματος αποτελεσμάτων βάσει γνωστών κακόβουλων hashes αρχείων. Ένα από τα βασικά της χαρακτηριστικά είναι η ευκολία χρήσης, που επιτρέπει στους αναλυτές περιστατικών να έχουν μια ελαφριά πλατφόρμα εστιασμένη σε κρίσιμες εργασίες και να αποκτούν τα απαραίτητα κρίσιμα αποδεικτικά στοιχεία.

Εγκατάσταση Autopsy

Πολλές από τις διανομές Linux που αναφέρθηκαν προηγουμένως έχουν ήδη εγκατεστημένο το Autopsy. Είναι καλή πρακτική για τους αναλυτές να διασφαλίζουν ότι η πλατφόρμα που χρησιμοποιούν είναι ενημερωμένη.

Για το λειτουργικό σύστημα Windows, κατεβάστε το Microsoft self-installer αρχείο από το: <https://www.sleuthkit.org/autopsy/download.php>

Μόλις κατέβει, εκτελέστε το αρχείο MSI και επιλέξτε τη θέση εγκατάστασης. Μετά την ολοκλήρωση, η εφαρμογή θα είναι έτοιμη προς χρήση.

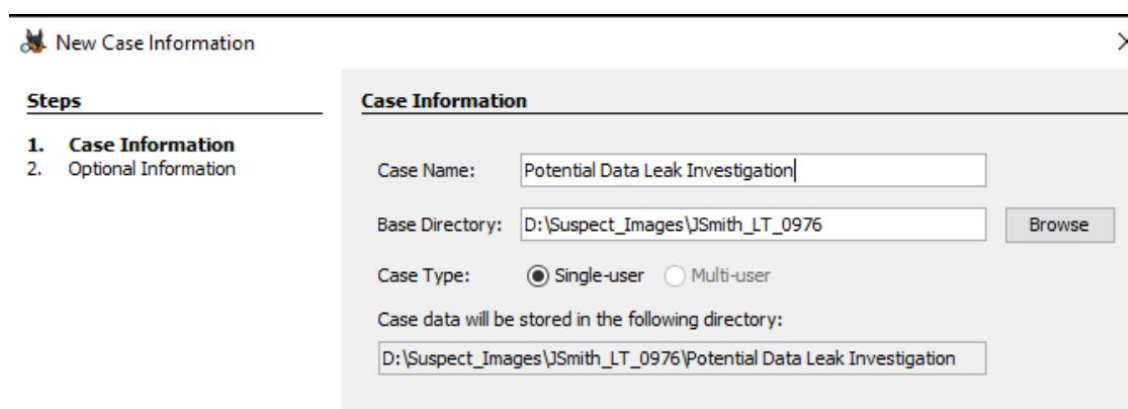
Ανοιγμα υπόθεσης

Αφού εγκατασταθεί το Autopsy, ο αναλυτής μπορεί να ανοίξει μια υπόθεση με ελάχιστη προδιαμόρφωση. Τα βασικά βήματα είναι τα εξής:

1. Για να ξεκινήσει η ανάλυση, βεβαιωθείτε ότι η πλήρης εικόνα του δίσκου βρίσκεται σε έναν μόνο κατάλογο. Αυτό επιτρέπει τη χρήση ολόκληρης της εικόνας κατά την ανάλυση. Στο παράδειγμα, μια εικόνα αρχείου έχει ληφθεί από το σύστημα ενός υπόπτου και χωριστεί σε τέσσερα αρχεία των 2 GB. Το Autopsy μπορεί να τα ανασυνθέσει σε όγκο εικόνας.

Name	Date modified	Type	Size
 JSmith_LT_0976.e04	9/9/2019 3:26 PM	E04 File	1,350,414 KB
 JSmith_LT_0976.e03	9/9/2019 3:11 PM	E03 File	2,097,138 KB
 JSmith_LT_0976.e02	9/9/2019 2:35 PM	E02 File	2,097,123 KB
 JSmith_LT_0976.e01	9/9/2019 2:10 PM	E01 File	2,097,133 KB

2. Ανοίξτε το Autopsy και επιλέξτε **New Case**. Εισάγετε τον τίτλο της υπόθεσης και τη διαδρομή όπου θα αποθηκευτούν τα αρχεία της υπόθεσης. Αυτό είναι χρήσιμο αν χρειάζεται να αποθηκευτούν σε ασφαλές περιβάλλον. Πατήστε **Next**.



New Case Information

Steps

1. **Case Information**
2. Optional Information

Case Information

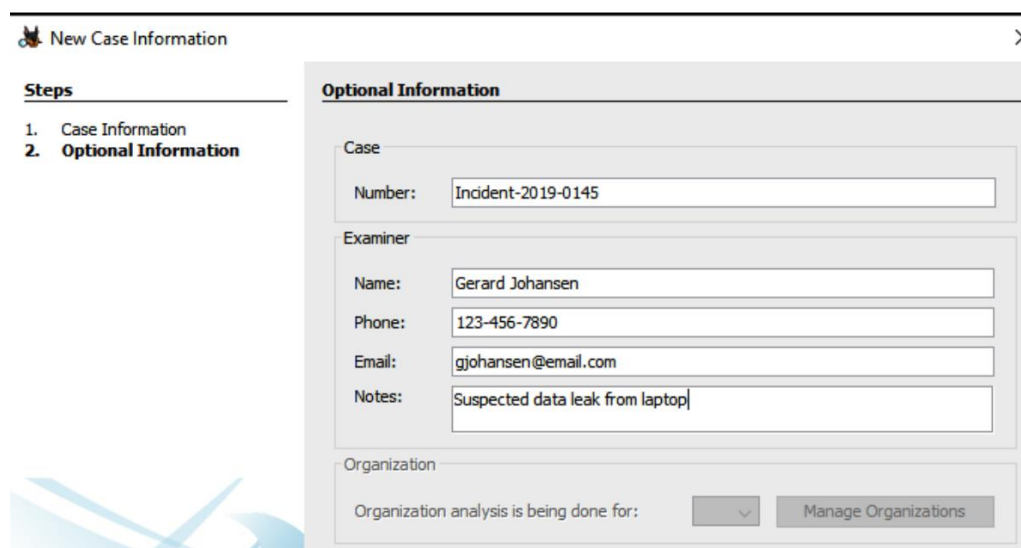
Case Name:

Base Directory:

Case Type: ☒ Single-user ☐ Multi-user

Case data will be stored in the following directory:

3. Στην επόμενη οθόνη, εισάγετε τον αριθμό υπόθεσης, το όνομά σας, τα στοιχεία επικοινωνίας και μια σύντομη περιγραφή στα **Notes**. Πατήστε **Finish**.



New Case Information

Steps

1. Case Information
2. **Optional Information**

Optional Information

Case

Number:

Examiner

Name:

Phone:

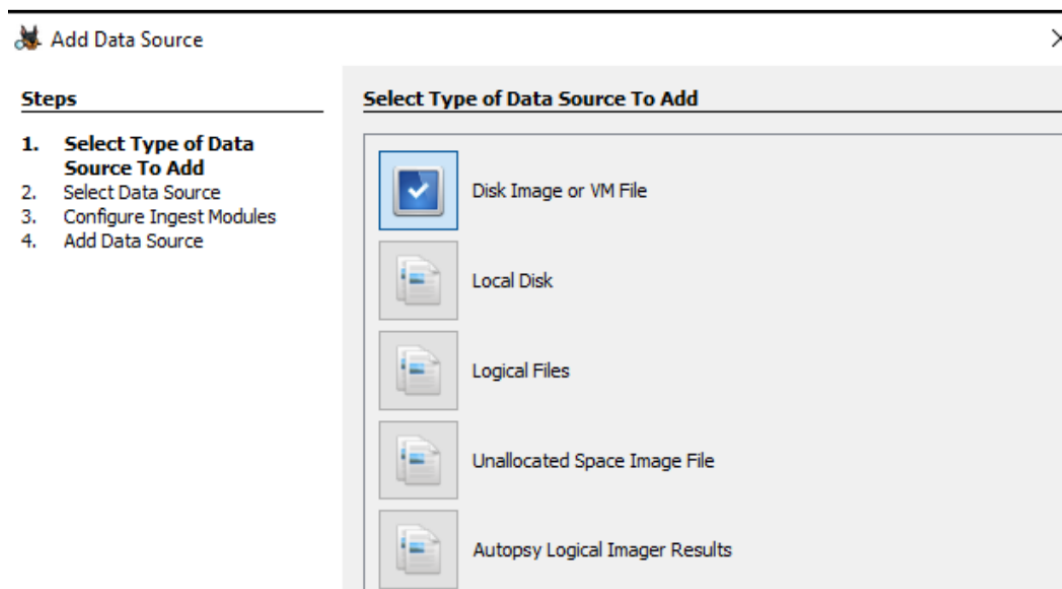
Email:

Notes:

Organization

Organization analysis is being done for:

- Μετά την εισαγωγή των στοιχείων υπόθεσης, φορτώστε το αρχείο εικόνας που δημιουργήθηκε προηγουμένως. Επιλέξτε τον τύπο δεδομένων. Το Autopsy μπορεί να αναλύσει αρχεία εικόνας ή αρχεία .vmdk από εικονικές μηχανές.



- Επιλέξτε τη θέση του αρχείου .E01. Αυτό θα περιλάβει όλα τα υπολοιπόμενα αρχεία εικόνας στον φάκελο. Επιλέξτε τη σωστή ζώνη ώρας και πατήστε **Next**.
- Στην επόμενη οθόνη, επιλέξτε τα modules που θα χρησιμοποιηθούν. Στην αρχή, επιλέξτε όλα για πλήρη ανάλυση. Μην ξεχάσετε να ενεργοποιήσετε και την **ανάλυση μη εκχωρημένου χώρου (unallocated space)**, καθώς εκεί μπορεί να κρύβεται σημαντική πληροφορία. Πατήστε **Next**.
- Ελέγξτε ότι η πηγή δεδομένων έχει φορτωθεί και πατήστε **Finish**.
- Το Autopsy θα ξεκινήσει την ανάλυση των αρχείων εικόνας. Ο χρόνος ανάλυσης εξαρτάται από το μέγεθος της εικόνας και την ταχύτητα επεξεργασίας του υπολογιστή.

Πλοήγηση στο Autopsy

Το GUI του Autopsy χωρίζεται σε τρία κύρια τμήματα:

- Αριστερό πλαίσιο:** περιέχει πηγές δεδομένων, δομή φακέλων και αποτελέσματα αναζητήσεων. Το σύμβολο + επεκτείνει τα αποτελέσματα, ενώ το – τα συμπύσσει.
- Κεντρικό πλαίσιο:** εμφανίζει καταλόγους ή αποτελέσματα αναζητήσεων, π.χ. cookies του συστήματος.
- Κάτω πλαίσιο:** εμφανίζει μεταδεδομένα και πληροφορίες για τα αρχεία, όπως timestamps και MD5 hash. Μπορεί επίσης να εμφανιστεί το περιεχόμενο σε δεκαεξαδική μορφή (**Hex tab**) για ανάλυση πιθανών κακόβουλων αρχείων.

Potential Data Leak Investigation - Autopsy 4.12.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Timeline Close Case Generate Report

Keyword Lists Keyword Search

Listing Recent Documents 24 Results

Table Thumbnail Save Table as CSV

Source File	S	C	Path	Date/Time	Data Source
inf.lnk			C:\Windows\inf	2015-03-22 15:57:31 UTC	JSmith_LT_0976.e01
setupapi.dev.lnk			C:\Windows\inf\setupapi.dev.log	2015-03-22 15:57:30 UTC	JSmith_LT_0976.e01
(secret_project)_pricing_decision.xlsx.LNK			\\10.11.11.128\SECURED_DRIVE\Secret Project Data\pric...	2015-03-23 20:26:53 UTC	JSmith_LT_0976.e01
Desktop.LNK			C:\Users\informant\Desktop	2015-03-24 18:48:40 UTC	JSmith_LT_0976.e01

Hex Text Application Message File Metadata Results Annotations Other Occurrences

Page: 1 of 1 Page Go to Page: Jump to Offset 0 Launch in HxD

```

0x00000000: 4C 00 00 00 01 14 02 00 00 00 00 00 C0 00 00 00 L.....
0x00000010: 00 00 00 46 93 00 20 00 20 00 00 00 6E 29 02 13 ..F.....n)..
0x00000020: 75 66 D0 01 CC 0B 1B 14 75 66 D0 01 B9 AE EA 7B uf.....uf...{
0x00000030: 44 04 CA 01 6B DE 0B 00 00 00 00 01 00 00 00 D...k.....
0x00000040: 00 00 00 00 00 00 00 00 00 00 00 00 A1 00 14 00 .....
0x00000050: 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 .P.O...i.....+0
0x00000060: 30 5D 28 00 2F 44 3A 5C 00 00 00 00 00 00 00 00 0.)/D:\.....
0x00000070: 00 00 00 00 00 00 00 00 00 01 01 05 8A EB FE EE .....
0x00000080: BE 42 44 80 4E 40 9D 6C 45 15 F9 62 00 32 00 6B .BD.Ng.iE...b.2.k
0x00000090: DE 0B 00 EE 3A 10 2C 20 00 50 65 6E 67 75 69 6E .....Penguin
0x000000A0: 73 2E 6A 70 67 00 00 46 00 08 00 04 00 EF BE 78 s.jpg...F.....x
0x000000B0: 46 21 A7 78 46 22 A7 2A 00 00 00 19 00 00 00 01 Fl.xp...F.....
0x000000C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x000000D0: 00 00 00 65 00 00 00 67 00 75 00 69 00 6E 00 73 .P.e.n.g.u.i.n.s
0x000000E0: 00 2E 00 6A 00 70 00 67 00 00 00 1C 00 00 00 46 ...j.p.g.....F
0x000000F0: 00 00 00 1C 00 00 00 01 00 00 00 1C 00 00 00 35 .....5
0x00000100: 00 00 00 00 00 00 00 45 00 00 00 19 00 00 00 05 .....E.....
0x00000110: 00 00 00 76 F1 88 AE 10 00 00 00 49 41 4D 41 4E ...v.....TAMAN
0x00000120: 20 43 44 00 44 3A 5C 50 65 6E 67 75 69 6E 73 2E CD.D:\Penguins.
0x00000130: 6A 70 67 00 00 03 00 44 00 3A 00 5C 00 28 00 00 jpg....D...:\(..
0x00000140: 00 09 00 00 A0 1C 00 00 00 31 53 50 53 E2 8A 58 .....ISPS..X
0x00000150: 46 BC 4C 38 43 BB FC 13 93 26 98 6D CE 00 00 00 F.L8C....&.m....
0x00000160: 00 00 00 00 00 00 00 00 00

```

Στο κύριο τμήμα της οθόνης, φαίνονται διάφορα αρχεία και δεδομένα, όπως συνδέσμους (links) από το "C:\Windows\inf" και το "C:\Users\Informant\Desktop", καθώς και ένα αρχείο σχετικό με ένα "Secret Project" σε έναν ασφαλισμένο δίσκο (SECURED_DRIVE). Οι ημερομηνίες κυμαίνονται από τον Μάρτιο του 2015, υποδεικνύοντας ότι η ανάλυση βασίζεται σε δεδομένα από εκείνη την περίοδο. Η λίστα περιλαμβάνει επίσης hex κείμενο και μεταδεδομένα, που βοηθούν στην ερμηνεία του περιεχομένου. Η διεπαφή προσφέρει εργαλεία όπως η δυνατότητα προσθήκης πηγών δεδομένων, η δημιουργία αναφορών και η αναζήτηση με λέξεις-κλειδιά. Στο αριστερό μέρος, υπάρχουν κατηγορίες όπως "File System", "Recent Documents", "Web History" και "E-Mail Messages", που δείχνουν ότι το λογισμικό καλύπτει ένα ευρύ φάσμα δεδομένων για λεπτομερή έρευνα. Αυτό το εργαλείο είναι ιδανικό για ερευνητές που χρειάζονται να εντοπίσουν ύποπτη δραστηριότητα ή να ανακτήσουν πληροφορίες από ένα σύστημα.

Από την εικόνα του Autopsy, κάτι ενδιαφέρον που ξεχωρίζει είναι η παρουσία ενός αρχείου με τίτλο "(Secret Project) pricing_decision.xlsx" σε έναν ασφαλισμένο δίσκο (SECURED_DRIVE), με ημερομηνία 2015-03-23. Αυτό υποδηλώνει ότι μπορεί να πρόκειται για ευαίσθητα δεδομένα, όπως οικονομικές πληροφορίες ή αποφάσεις τιμολόγησης, που ενδέχεται να αποτελούν αντικείμενο έρευνας για διαρροή δεδομένων.

Το Autopsy προσφέρει δυνατότητες που συναντώνται και σε εμπορικές πλατφόρμες, αλλά για πιο σύνθετες υποθέσεις ίσως απαιτηθούν πιο εξειδικευμένα εργαλεία. Παρέχει όμως μια φιλική πλατφόρμα για νέους αναλυτές.

Εξέταση υπόθεσης

Μετά την επεξεργασία της υπόθεσης, το αριστερό πλαίσιο θα εμφανίζει τα artifacts του συστήματος. Στο **Extracted Content** μπορεί κανείς να δει εγκατεστημένα προγράμματα, πληροφορίες λειτουργικού και πρόσφατα έγγραφα. Η πλήρης δομή φακέλων της εικόνας μπορεί να εξεταστεί για τον εντοπισμό ύποπτων αρχείων.

Listing									
Web Cookies									
Table Thumbnail									
Source File	S	C	URL	Date/Time	Name	Value	Program Name	Domain	Data Source
Cookies			.youtube.com	2015-03-22 15:55:30 UTC	VISITOR_INFO1_LIVE		Chrome	youtube.com	JSmith_LT_0976.e01
Cookies			.google.com	2015-03-22 15:55:30 UTC	__utmt		Chrome	google.com	JSmith_LT_0976.e01
Cookies			.google.com	2015-03-22 15:55:30 UTC	__utma		Chrome	google.com	JSmith_LT_0976.e01
Cookies			.google.com	2015-03-22 15:55:30 UTC	__utmb		Chrome	google.com	JSmith_LT_0976.e01
Cookies			.google.com	2015-03-22 15:55:30 UTC	__utmz		Chrome	google.com	JSmith_LT_0976.e01
Cookies			.google.com	2015-03-22 15:55:40 UTC	PREF		Chrome	google.com	JSmith_LT_0976.e01
Cookies			.google.com	2015-03-22 15:55:40 UTC	NID		Chrome	google.com	JSmith_LT_0976.e01
Cookies			.youtube.com	2015-03-24 19:00:58 UTC	VISITOR_INFO1_LIVE		Chrome	youtube.com	JSmith_LT_0976.e01
Cookies			.youtube.com	2015-03-24 19:00:58 UTC	YSC		Chrome	youtube.com	JSmith_LT_0976.e01
Cookies			.google.com	2015-03-22 15:12:06 UTC	__utma		Chrome	google.com	JSmith_LT_0976.e01

Η έρευνα εξαρτάται από τον τύπο περιστατικού:

- Για malware από κακόβουλη ιστοσελίδα, μπορεί να εξεταστούν URLs και πρόσφατες διαδικτυακές δραστηριότητες.
- Αν έχει εντοπιστεί ύποπτη διεργασία μέσω Volatility ή Redline, το Autopsy μπορεί να δείξει πότε εκτελέστηκε για τελευταία φορά το αντίστοιχο εκτελέσιμο αρχείο.
- Σε περιπτώσεις διαρροής εμπιστευτικών αρχείων, μπορεί να εξεταστούν χρόνοι πρόσβασης, email, cloud storage ή USB συνδέσεις.

Type	Value
URL	.youtube.com
Date/Time	2015-03-24 19:00:58
Name	YSC
Value	
Program Name	Chrome
Domain	youtube.com
Source File Path	/img_JSmith_LT_0976.e01/vol_vol3/Users/informant/AppData/Local/Google/Chrome/User Data/Default/Cookies
Artifact ID	-9223372036854775654

Από τα δεδομένα που παρέχονται, φαίνεται ότι πρόκειται για πληροφορίες cookie από το πρόγραμμα περιήγησης Google Chrome, που σχετίζονται με την επίσκεψη στον ιστότοπο youtube.com στις 24 Μαρτίου 2015, στις 19:00:58. Το όνομα του cookie είναι "YSC" και η τιμή του είναι "Chrome", ενώ η διαδρομή του αρχείου αποθηκεύεται στον τοπικό φάκελο του χρήστη "informant" στο σύστημα

(img_JSmith_LT_0976.e01). Αυτό υποδηλώνει ότι η πληροφορία συλλέχθηκε πιθανότατα ως μέρος μιας δικανικής έρευνας, με το Artifact ID (-9223372036854775654) να χρησιμοποιείται για την ταυτοποίηση του συγκεκριμένου αντικειμένου.

Κάνοντας κλικ στην καρτέλα **File Metadata** εμφανίζονται πληροφορίες που αφορούν συγκεκριμένα το αρχείο. Αυτές περιλαμβάνουν τους χρονοσφραγίδες (timestamps) του αρχείου, καθώς και το MD5 hash του.

Name	/img_JSmith_LT_0976.e01/vol_vol3/Users/informant/AppData/Local/Google/Chrome/User Data/Default/Cookies
Type	File System
MIME Type	application/x-sqlite3
Size	137216
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	2015-03-24 21:07:21 UTC
Accessed	2015-03-22 15:11:57 UTC
Created	2015-03-22 15:11:57 UTC
Changed	2015-03-24 21:07:21 UTC
MD5	7a247be5ff943b90262c755dfdefeca7
Hash Lookup Results	UNKNOWN
Internal ID	9952

Τέλος, το δεκαεξαδικό περιεχόμενο του αρχείου μπορεί να προβληθεί κάνοντας κλικ στην καρτέλα **Hex**. Αυτή η προβολή είναι ιδανική όταν ένας αναλυτής θέλει να ελέγξει μια εφαρμογή ή άλλο αρχείο που υποψιάζεται ότι μπορεί να είναι κακόβουλο λογισμικό (malware).

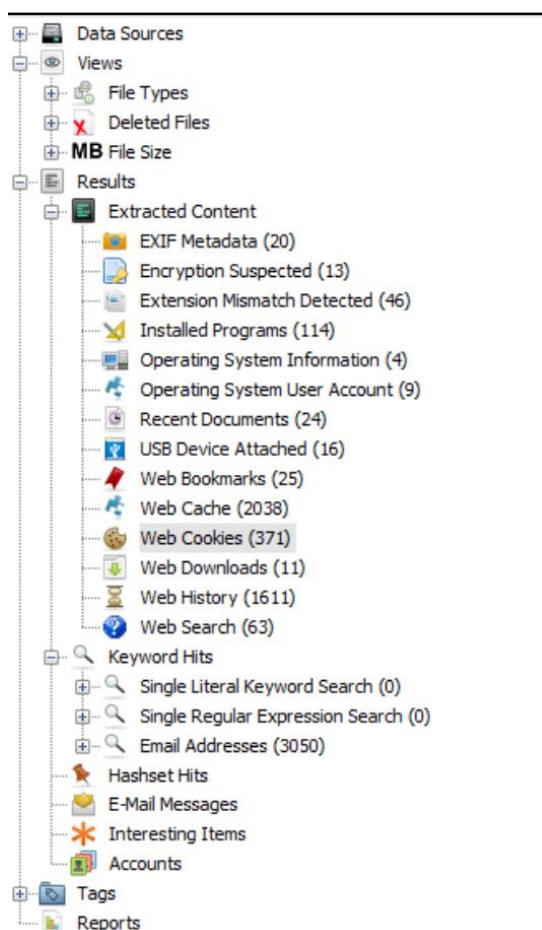
Hex	Text	Application	Message	File Metadata	Results	Annotations	Other Occurrences
Page: 1 of 9	Page	←	→	Go to Page:		Jump to Offset	0
0x00000000:	53 51 4C 69 74 65 20 66	6F 72 6D 61 74 20 33 00	SQLite format 3.				
0x00000010:	04 00 01 01 00 40 20 20	00 00 00 40 00 00 00 86	@ ...@....				
0x00000020:	00 00 00 4E 00 00 00 01	00 00 00 03 00 00 00 01	...N.....				
0x00000030:	00 00 00 00 00 00 00 00	00 00 00 01 00 00 00 00					
0x00000040:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00					
0x00000050:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 40	@				
0x00000060:	00 2D E2 1E 0D 03 FC 00	05 01 40 00 03 6B 03 D3	...-.....@..k..				
0x00000070:	01 83 03 3C 01 40 00 00	00 00 00 00 00 00 00 00	...<.@.....				
0x00000080:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00					
0x00000090:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00					
0x000000a0:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00					
0x000000b0:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00					
0x000000c0:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00					
0x000000d0:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00					
0x000000e0:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00					
0x000000f0:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00					
0x00000100:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00					
0x00000110:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00					
0x00000120:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00					
0x00000130:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00					
0x00000140:	41 05 06 17 19 1B 01 5D	69 6E 64 65 78 64 6F 6D	A.....]indexdom				
0x00000150:	61 69 6E 63 6F 6F 6B 69	65 73 06 43 52 45 41 54	aincookies.CREAT				
0x00000160:	45 20 49 4E 44 45 58 20	64 6F 6D 61 69 6E 20 4F	E INDEX domain O				

Το Autopsy προσφέρει τη δυνατότητα εκτέλεσης ορισμένων ενεργειών και αναλύσεων που βρίσκονται και σε άλλες εμπορικές πλατφόρμες. Ωστόσο, πρέπει να σημειωθεί ότι σε πιο σύνθετες έρευνες μπορεί

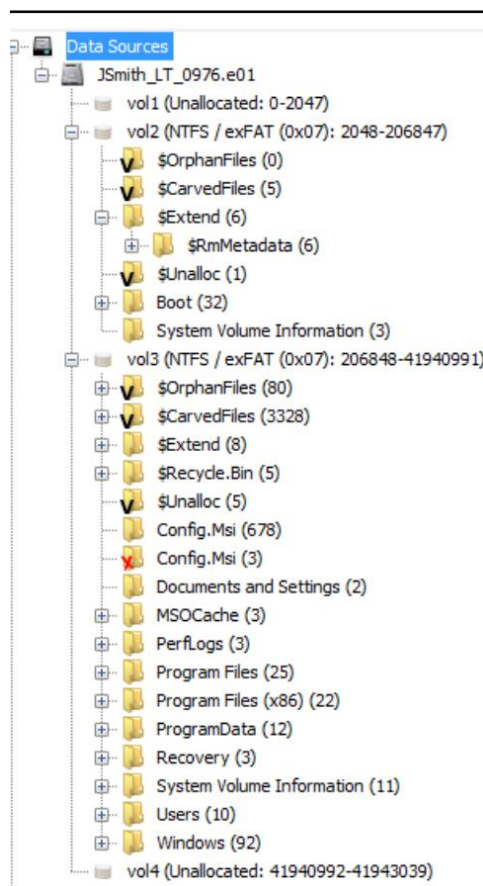
να γίνει απαραίτητη η χρήση πιο προηγμένων πλατφορμών. Το Autopsy παρέχει επίσης σε νέους αναλυτές στον τομέα της δισκο-εγκληματολογίας (disk forensics) μια πιο φιλική προς τον χρήστη πλατφόρμα, ώστε να αποκτήσουν εμπειρία πριν προχωρήσουν σε πιο σύνθετες εμπορικές λύσεις.

9.2. Εξέταση μιας υπόθεσης

Μόλις η υπόθεση επεξεργαστεί, το αριστερό παράθυρο θα γεμίσει με τον αριθμό των αντικειμένων (artifacts) που εντοπίστηκαν στο σύστημα:



Στο προηγούμενο στιγμιότυπο, υπάρχουν αρκετά αντικείμενα καταγεγραμμένα στην ενότητα *Extracted Content*. Αυτά περιλαμβάνουν πληροφορίες σχετικά με τα προγράμματα που έχουν εγκατασταθεί, τα στοιχεία του λειτουργικού συστήματος και τα πρόσφατα έγγραφα. Μια ακόμη σημαντική λειτουργία του Autopsy είναι η δυνατότητα εξέτασης ολόκληρης της δομής φακέλων του αρχείου εικόνας. Κάνοντας κλικ στο σύμβολο συν (+) δίπλα στα *Data Sources*, επεκτείνεται ολόκληρη η δομή φακέλων. Αυτό είναι χρήσιμο αν, μέσω άλλων πηγών, ένας αναλυτής μπορέσει να εντοπίσει τη θέση ενός ύποπτου αρχείου.



Υπάρχουν διαφορετικά σημεία δεδομένων που μπορούν να εξεταστούν χρησιμοποιώντας το Autopsy. Τι θα αναζητηθεί και πώς θα αναζητηθεί εξαρτάται συχνά από τον τύπο του συμβάντος ή της διερεύνησης. Για παράδειγμα, μια μόλυνση από κακόβουλο λογισμικό που προέρχεται από έναν παραβιασμένο ιστότοπο μπορεί να απαιτεί έλεγχο του συστήματος για URLs που ο χρήστης ενδέχεται να έχει πληκτρολογήσει ή επισκεφθεί μέσω του προγράμματος περιήγησης. Επιπλέον, το ίδιο το αρχείο μπορεί να εντοπιστεί χρησιμοποιώντας πληροφορίες που έχουν ληφθεί από την ανάλυση της μνήμης του συστήματος, όπως καλύφθηκε στο προηγούμενο κεφάλαιο. Για παράδειγμα, αν ένας αναλυτής μπορέσει να εντοπίσει μια ύποπτη διαδικασία μέσω Volatility ή Redline και στη συνέχεια βρει το εκτελέσιμο αρχείο, μπορεί να χρησιμοποιήσει το Autopsy για να βρει την τελευταία φορά που εκτελέστηκε το αρχείο. Αυτό παρέχει στους υπεύθυνους στοιχεία για τον χρόνο, ώστε να μπορούν να εξετάσουν άλλα συστήματα για αποδεικτικά στοιχεία παραβίασης.

Σε ένα άλλο σενάριο, οι υπεύθυνοι ενδέχεται να κληθούν να προσδιορίσουν αν ένας υπάλληλος είχε πρόσβαση σε εμπιστευτικά αρχεία για να τα μεταφέρει σε ανταγωνιστή. Αυτό μπορεί να περιλαμβάνει έλεγχο του συστήματος για τους χρόνους και τις ημερομηνίες πρόσβασης στα αρχεία, τις χρησιμοποιούμενες διευθύνσεις email, τους εξωτερικούς χώρους αποθήκευσης cloud που επισκέφτηκαν ή τις συνδεδεμένες συσκευές USB. Τέλος, μια πλήρης λίστα αυτών των αρχείων μπορεί να παρέχει εικόνα για τα εμπιστευτικά έγγραφα που μετακινήθηκαν.

Αρχεία web (Web artifacts): Υπάρχουν αρκετοί τύποι συμβάντων όπου μπορεί να χρειαστεί η εξέταση ενός συστήματος για αποδεικτικά στοιχεία κακόβουλης δραστηριότητας που έχει πραγματοποιηθεί από έναν χρήστη. Προηγουμένως αναφέρθηκε η πρόσβαση σε αποθηκευτικούς χώρους cloud όπου ένας κακόβουλος υπάλληλος έχει ανεβάσει εμπιστευτικά έγγραφα. Σε άλλες περιπτώσεις, επιθέσεις κοινωνικής μηχανικής μπορεί να οδηγήσουν έναν ανυποψίαστο υπάλληλο σε έναν παραβιασμένο ιστότοπο, ο οποίος στη συνέχεια κατεβάζει κακόβουλο λογισμικό. Σε κάθε περίπτωση, το Autopsy μας δίνει τη δυνατότητα να εξετάσουμε διάφορους τομείς των web artifacts.

Ο πρώτος από αυτούς είναι το ιστορικό περιήγησης (web history). Σε περίπτωση επίθεσης κοινωνικής μηχανικής, όπου ο χρήστης πλοηγείται σε ιστότοπο διανομής κακόβουλου λογισμικού, αυτά τα δεδομένα μπορεί να παρέχουν πληροφορίες για το συγκεκριμένο URL που επισκέφθηκε. Το URL αυτό μπορεί στη συνέχεια να εξαχθεί και να συγκριθεί με γνωστές λίστες κακόβουλων ιστοτόπων από εσωτερικές ή εξωτερικές πηγές. Σε άλλες περιπτώσεις, όπου ένας υπάλληλος έχει επισκεφθεί εξωτερικό χώρο αποθήκευσης cloud, το ιστορικό περιήγησης μπορεί να παρέχει αποδεικτικά στοιχεία αυτής της δραστηριότητας.

Λεπτομερής εξέταση:

1. Κάνοντας κλικ στην ενότητα *Web History* στο αριστερό παράθυρο ανοίγει το κεντρικό παράθυρο και εμφανίζονται λεπτομέρειες για ένα URL που επισκέφτηκε το σύστημα.

Listing					
Web History					
Table Thumbnail					
Source File	S	C	URL	Date Accessed	Referrer URL
History			https://www.google.com/webhp?hl=en#q=leaking+confid...	2015-03-23 18:03:31 UTC	https://www.google.com/webhp?hl=en#q=leaking+confid...
History			https://www.google.com/webhp?sourceid=chrome-instant...	2015-03-22 15:55:40 UTC	https://www.google.com/webhp?sourceid=chrome-instant...
History			https://www.google.com/webhp?sourceid=chrome-instant...	2015-03-22 15:55:44 UTC	https://www.google.com/webhp?sourceid=chrome-instant...
index.dat			https://www.google.com/xjs/_js/k=xjs.hp.en_US.votPZM...	2015-03-22 22:10:52 UTC	
index.dat			https://www.gstatic.com/external_hosted/modernizr/mode...	2015-03-22 22:11:13 UTC	
index.dat			https://www.gstatic.com/external_hosted/threejs-r49/Thr...	2015-03-22 22:10:54 UTC	
History			https://www.icloud.com/icloudcontrolpanel	2015-03-23 19:55:34 UTC	https://www.icloud.com/icloudcontrolpanel
History			https://www.icloud.com/icloudcontrolpanel/	2015-03-23 19:55:34 UTC	https://www.icloud.com/icloudcontrolpanel/
WebCacheV01.da			https://www.youtube.com/embed/EWRk51oB-1Y	2015-03-24 03:56:29 UTC	

2. Στο προηγούμενο στιγμιότυπο, το Autopsy δείχνει ότι το σύστημα προσέβαλε την υπηρεσία iCloud. Επιπλέον, παρέχονται πληροφορίες που επιτρέπουν στον αναλυτή να αξιολογήσει στοιχεία όπως η θέση του artifact και ο τύπος προγράμματος περιήγησης που χρησιμοποιήθηκε. Αυτές οι πληροφορίες είναι προσβάσιμες μέσω της καρτέλας *Results* στο κάτω παράθυρο.

Result: 97 of 169 Result  

Web History

Type	Value
URL	https://www.icloud.com/icloudcontrolpanel
Date Accessed	2015-03-23 19:55:34
Referrer URL	https://www.icloud.com/icloudcontrolpanel
Title	iCloud
Program Name	Chrome
Domain	www.icloud.com
Source File Path	/img_JSmith_LT_0976.e01/vol_vol3/Users/informant/AppData/Local/Google/Chrome/User Data/Default/History
Artifact ID	-9223372036854775707

3. Επιπλέον, το Autopsy παρέχει τα μεταδεδομένα του συγκεκριμένου αρχείου που εξετάζεται. Κάνοντας κλικ στην καρτέλα *File Metadata* εμφανίζονται τα σχετικά δεδομένα.

Hex	Text	Application	Message	File Metadata	Results	Annotations	Other Occurrences
Name	/img_JSmith_LT_0976.e01/vol_vol3/Users/informant/AppData/Local/Google/Chrome/User Data/Default/History						
Type	File System						
MIME Type	application/x-sqlite3						
Size	135168						
File Name Allocation	Allocated						
Metadata Allocation	Allocated						
Modified	2015-03-24 21:07:21 UTC						
Accessed	2015-03-22 15:11:53 UTC						
Created	2015-03-22 15:11:53 UTC						
Changed	2015-03-24 21:07:21 UTC						
MD5	db1f9e1a7fb6b9252d903dfafe25f2da						
Hash Lookup Results	UNKNOWN						
Internal ID	11578						

4. Όπως φαίνεται στο στιγμιότυπο, υπάρχουν περισσότερες λεπτομέρειες για το αρχείο. Για παράδειγμα, ο αναλυτής μπορεί να συλλέξει πληροφορίες χρόνου, θέση αρχείου και MD5 hash, τα οποία μπορούν να χρησιμοποιηθούν για τη σύγκριση με άλλα αρχεία που εξετάζονται περαιτέρω. Σε ορισμένες περιπτώσεις, ένας ύποπτος μπορεί να διαγράψει το ιστορικό περιήγησης για να καλύψει κακόβουλη δραστηριότητα.

Μια άλλη τοποθεσία που μπορεί να παρέχει στοιχεία για τους ιστότοπους που επισκέφθηκε ένας κακόβουλος υπάλληλος είναι τα web cookies. Αυτά μπορούν να εντοπιστούν στο αριστερό παράθυρο υπό *Web Cookies*. Κάνοντας κλικ εμφανίζεται η λίστα των cookies που παραμένουν στο σύστημα.

Ανάλογα με τον τύπο του συμβάντος, τα web artifacts μπορεί να παίξουν σημαντικό ρόλο. Το Autopsy παρέχει κάποια λειτουργικότητα γι' αυτό, αλλά οι υπεύθυνοι ενδέχεται να διαπιστώσουν ότι άλλες εμπορικές λύσεις προσφέρουν πιο ολοκληρωμένη πλατφόρμα. Για παράδειγμα, το *Evidence Finder* της Magnet Forensics σαρώνει ολόκληρο το σύστημα για στοιχεία διαδικτύου και τα παρουσιάζει με τρόπο εύκολο για τον αναλυτή.

Web Cookies										371 Results
Table Thumbnail										Save Table as CSV
Source File	S	C	URL	Date/Time	Name	Value	Program Name	Domain	Data Source	
Cookies			.youtube.com	2015-03-22 15:55:30 UTC	VISITOR_INFO1_LIVE		Chrome	youtube.com	J5mith_LT_0976.e01	
Cookies			.google.com	2015-03-22 15:55:30 UTC	__utmt		Chrome	google.com	J5mith_LT_0976.e01	
Cookies			.google.com	2015-03-22 15:55:30 UTC	__utma		Chrome	google.com	J5mith_LT_0976.e01	
Cookies			.google.com	2015-03-22 15:55:30 UTC	__utmb		Chrome	google.com	J5mith_LT_0976.e01	
Cookies			.google.com	2015-03-22 15:55:30 UTC	__utmz		Chrome	google.com	J5mith_LT_0976.e01	
Cookies			.google.com	2015-03-22 15:55:40 UTC	PREF		Chrome	google.com	J5mith_LT_0976.e01	
Cookies			.google.com	2015-03-22 15:55:40 UTC	NID		Chrome	google.com	J5mith_LT_0976.e01	
Cookies			.youtube.com	2015-03-24 19:00:58 UTC	VISITOR_INFO1_LIVE		Chrome	youtube.com	J5mith_LT_0976.e01	
Cookies			.youtube.com	2015-03-24 19:00:58 UTC	YSC		Chrome	youtube.com	J5mith_LT_0976.e01	
Cookies			.google.com	2015-03-22 15:12:06 UTC	__utma		Chrome	google.com	J5mith_LT_0976.e01	
Cookies			.google.com	2015-03-22 15:12:06 UTC	__utmc		Chrome	google.com	J5mith_LT_0976.e01	
Cookies			.google.com	2015-03-22 15:12:06 UTC	__utmz		Chrome	google.com	J5mith_LT_0976.e01	
Cookies			.google.com	2015-03-24 21:06:40 UTC	PREF		Chrome	google.com	J5mith_LT_0976.e01	
Cookies			.bing.com	2015-03-24 21:07:20 UTC	_FS		Chrome	bing.com	J5mith_LT_0976.e01	

Ένα ακόμη πλεονέκτημα αυτών των εμπορικών λύσεων είναι ότι η λειτουργικότητά τους ενημερώνεται συνεχώς. Ανάλογα με τη συχνότητα αναζήτησης διαδικτυακών στοιχείων, η χρήση τέτοιων εργαλείων μπορεί να είναι επωφελής.

Email: Ο εντοπισμός ύποπτων email είναι μια συχνή εργασία για τους υπεύθυνους αντιμετώπισης συμβάντων.

Αυτό μπορεί να περιλαμβάνει περιστατικά όπως επιθέσεις κοινωνικής μηχανικής, όπου οι υπεύθυνοι εντοπίζουν ύποπτα email που περιέχουν κακόβουλο λογισμικό. Σε άλλες περιπτώσεις, κακόβουλοι υπάλληλοι μπορεί να έχουν στείλει ή λάβει μηνύματα που παραβιάζουν την πολιτική της εταιρείας. Σε αυτές τις περιπτώσεις, οι υπεύθυνοι ανακτούν τα email για να συμπεριληφθούν σε διαδικασίες απόλυσης ή νομικής ενέργειας.

Listing	
(\{?[a-zA-Z0-9%+_-]+\}+)(\.[a-zA-Z0-9%+_-]+\}+)*(\{?[a-zA-Z0-9%+_-]+\}+)(\.[a-zA-Z0-9%+_-]+\}+)*[a-zA-Z]{2,4}	
Table Thumbnail	
List Name	Files with Hits
cfoster@nist.gov (1)	1
cglein@microsoft.com (1)	1
chambersignroot@chambersign.org (8)	8
chambersroot@chambersign.org (8)	8
charles.camp@nist.gov (1)	1
chihan@microsoft.com (1)	1
chipc@microsoft.com (1)	1
chirag.parikh@nist.gov (1)	1
chrichristian.enloe@nist.gov (1)	1
chris.glein@gmail.com (1)	1
christian.enloe@nist.gov (1)	1
christopher.bertrand@nist.gov (1)	1
christopher.mckinney@nist.gov (1)	1
christopher.soles@nist.gov (1)	1
chrome@example.com (2)	2

Το Autopsy μπορεί να εντοπίσει email που περιέχονται στο σύστημα. Από αυτά, μπορεί να αναγνωριστούν ύποπτα email και domains για περαιτέρω έρευνα σχετικά με πιθανή κοινωνική μηχανική ή άλλη κακόβουλη δραστηριότητα. Αρκεί να γίνει κλικ στην καρτέλα *Email Addresses* στο αριστερό παράθυρο, όπου εμφανίζονται οι διευθύνσεις email που εντοπίζονται στο σύστημα.

9.3. Συσκευές που έχουν συνδεθεί

Ένα ακόμη σημαντικό στοιχείο που μπορεί να είναι χρήσιμο για έναν αναλυτή είναι τα δεδομένα σχετικά με το πότε συγκεκριμένες συσκευές συνδέθηκαν στο σύστημα. Στο σενάριο ενός κακόβουλου εσωτερικού χρήστη που προσπαθεί να κλέψει εμπιστευτικά έγγραφα, η γνώση για το αν χρησιμοποίησε μια συσκευή USB μπορεί να είναι χρήσιμη. Το Autopsy χρησιμοποιεί τις ρυθμίσεις του μητρώου που βρίσκονται στο σύστημα για να εντοπίσει τους τύπους των συνδεδεμένων συσκευών και την τελευταία φορά που χρησιμοποιήθηκαν. Σε αυτή την περίπτωση, το αποτέλεσμα του κλικ στο **Devices Attached** (Συσκευές που έχουν συνδεθεί) στο αριστερό πάνελ παράγει τα ακόλουθα αποτελέσματα:

USB Device Attached							
Table		Thumbnail					
Source File	S	C	Date/Time	Device Make	Device Model	Device ID	Data Source
SYSTEM			2015-03-25 13:05:35 UTC		ROOT_HUB	58:3bb57b8&0	J5mith_LT_0976.e01
SYSTEM			2015-03-25 13:05:35 UTC		ROOT_HUB20	58:299e1c9f8&0	J5mith_LT_0976.e01
SYSTEM			2015-03-24 13:38:00 UTC	SanDisk Corp.	Cruzer Fit	4C530012450531101593	J5mith_LT_0976.e01
SYSTEM			2015-03-24 19:38:09 UTC	SanDisk Corp.	Cruzer Fit	4C530012550531106501	J5mith_LT_0976.e01
SYSTEM			2015-03-25 13:05:36 UTC	VMware, Inc.	Virtual USB Hub	68b77da92808&2	J5mith_LT_0976.e01
SYSTEM			2015-03-25 13:05:36 UTC	VMware, Inc.	Virtual Mouse	68b77da92808&1	J5mith_LT_0976.e01
SYSTEM			2015-03-25 13:05:36 UTC	VMware, Inc.	Virtual Mouse	782a7d3009808&0000	J5mith_LT_0976.e01
SYSTEM			2015-03-25 13:05:36 UTC	VMware, Inc.	Virtual Mouse	782a7d3009808&0001	J5mith_LT_0976.e01
SYSTEM			2015-03-25 13:05:35 UTC		ROOT_HUB	58:3bb57b8&0	J5mith_LT_0976.e01
SYSTEM			2015-03-25 13:05:35 UTC		ROOT_HUB20	58:299e1c9f8&0	J5mith_LT_0976.e01
SYSTEM			2015-03-24 13:38:00 UTC	SanDisk Corp.	Cruzer Fit	4C530012450531101593	J5mith_LT_0976.e01
SYSTEM			2015-03-24 19:38:09 UTC	SanDisk Corp.	Cruzer Fit	4C530012550531106501	J5mith_LT_0976.e01
SYSTEM			2015-03-25 13:05:36 UTC	VMware, Inc.	Virtual USB Hub	68b77da92808&2	J5mith_LT_0976.e01
SYSTEM			2015-03-25 13:05:36 UTC	VMware, Inc.	Virtual Mouse	68b77da92808&1	J5mith_LT_0976.e01
SYSTEM			2015-03-25 13:05:36 UTC	VMware, Inc.	Virtual Mouse	782a7d3009808&0000	J5mith_LT_0976.e01
SYSTEM			2015-03-25 13:05:36 UTC	VMware, Inc.	Virtual Mouse	782a7d3009808&0001	J5mith_LT_0976.e01

Εξετάζοντας την καρτέλα **Results**, ο αναλυτής θα μπορεί να προσδιορίσει τον τύπο της συσκευής και την ημερομηνία και ώρα που συνδέθηκε η συσκευή USB.

Result: 3 of 9		Result	←	→
Type	Value			
Date/Time	2015-03-24 13:38:00			
Device Make	SanDisk Corp.			
Device Model	Cruzer Fit			
Device ID	4C530012450531101593			
Source File Path	/img_J5mith_LT_0976.e01/vol_vol3/Windows/System32/config/RegBack/SYSTEM			
Artifact ID	-9223372036854769619			

Μια πιο λεπτομερής εξέταση των **File Metadata** (Μεταδεδομένα Αρχείων) θα δείξει επιπλέον δεδομένα που μπορούν να χρησιμοποιηθούν για την ανακατασκευή της χρονικής στιγμής που προσπελάστηκε η συσκευή USB στο σύστημα.

Hex	Text	Application	Message	File Metadata	Results	Annotations	Other Occurrences
Name	/img_JSmith_LT_0976.e01/vol_vol3/Windows/System32/config/RegBack/SYSTEM						
Type	File System						
MIME Type	application/x.windows-registry						
Size	12419072						
File Name Allocation	Allocated						
Metadata Allocation	Allocated						
Modified	2015-03-25 13:24:16 UTC						
Accessed	2015-03-25 13:24:10 UTC						
Created	2015-03-25 10:15:18 UTC						
Changed	2015-03-25 13:24:16 UTC						
MD5	a26cbec95c053ca113b9bef2fd4878						
Hash Lookup Results	UNKNOWN						
Internal ID	76202						

Διαγραμμένα αρχεία: Αρχεία που έχουν διαγραφεί μπορούν επίσης να ανακατασκευαστούν, είτε μερικώς είτε πλήρως. Το λειτουργικό σύστημα Windows δεν διαγράφει τα αρχεία όταν ο χρήστης επιλέγει διαγραφή. Το λειτουργικό σύστημα σημειώνει τον χώρο που καταλαμβάνει ένα διαγραμμένο αρχείο στον **Master File Table (MFT)** ως διαθέσιμο για εγγραφή νέων αρχείων. Ως αποτέλεσμα, οι αναλυτές ενδέχεται να μπορούν να δουν διαγραμμένα αρχεία που δεν έχουν αντικατασταθεί.

Ένα πρόβλημα που αντιμετωπίζουν οι δικαστικοί αναλυτές είναι η χρήση **σκληρών δίσκων SSD** σε tablet και υπολογιστές. Διαγραμμένα αρχεία μπορούν συχνά να ανακτηθούν από παραδοσιακούς σκληρούς δίσκους, ακόμη και μετά την απενεργοποίηση του συστήματος. Με τα SSD, το λειτουργικό σύστημα συχνά αφαιρεί τα διαγραμμένα αρχεία για να βελτιώσει την αποθήκευση. Περισσότερες πληροφορίες μπορεί να βρει κανείς στον ακόλουθο ιστότοπο: <https://www.datanarro.com/the-impact-of-ssds-on-digitalforensics/>

Για να δείτε τα διαγραμμένα αρχεία σε ένα σύστημα, κάντε κλικ στην καρτέλα **Deleted Files** στο αριστερό πάνελ. Από εκεί, ο αναλυτής μπορεί να δει όλα τα αρχεία που έχουν σημειωθεί για διαγραφή.

Στη συνέχεια, ο αναλυτής μπορεί να αναζητήσει μέσα στα διαγραμμένα αρχεία. Αυτά τα αρχεία μπορεί να έχουν αξία ως αποδεικτικά στοιχεία. Για παράδειγμα, σε περίπτωση κακόβουλης δραστηριότητας εσωτερικού χρήστη, αν πολλά ευαίσθητα αρχεία βρεθούν στα διαγραμμένα, όλα διαγραμμένα μέσα στην ίδια χρονική περίοδο, αυτό μπορεί να υποδηλώνει προσπάθεια του χρήστη να καλύψει τα ίχνη του.

Name	S	C	Location	Modified Time	Change Time	Access Time
System.Data.Entity.dll			/img_J5mith_LT_0976.e01/vol_vol3/Program Files (x86)/Re...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
nb.lproj			/img_J5mith_LT_0976.e01/vol_vol3/Program Files (x86)/Ap...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
ko.lproj			/img_J5mith_LT_0976.e01/vol_vol3/Program Files (x86)/Bo...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
it.lproj			/img_J5mith_LT_0976.e01/vol_vol3/Program Files (x86)/Co...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
es.lproj			/img_J5mith_LT_0976.e01/vol_vol3/Program Files (x86)/Co...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
ru.lproj			/img_J5mith_LT_0976.e01/vol_vol3/Program Files (x86)/Co...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
ColorSync.resources			/img_J5mith_LT_0976.e01/vol_vol3/Program Files (x86)/Co...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
libdispatch.dll			/img_J5mith_LT_0976.e01/vol_vol3/Program Files (x86)/Co...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
es.lproj			/img_J5mith_LT_0976.e01/vol_vol3/Program Files (x86)/Co...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
pthreadVC2.dll			/img_J5mith_LT_0976.e01/vol_vol3/Program Files (x86)/Co...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
fi.lproj			/img_J5mith_LT_0976.e01/vol_vol3/Program Files (x86)/Co...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
AuditResultView.js			/img_J5mith_LT_0976.e01/vol_vol3/Program Files (x86)/Co...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
buildSystemOnly.js			/img_J5mith_LT_0976.e01/vol_vol3/Program Files (x86)/Co...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
ConsoleView.js			/img_J5mith_LT_0976.e01/vol_vol3/Program Files (x86)/Co...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
DOMAgent.js			/img_J5mith_LT_0976.e01/vol_vol3/Program Files (x86)/Co...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
ElementsPanelDescriptor.js			/img_J5mith_LT_0976.e01/vol_vol3/Program Files (x86)/Co...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00

Αναζητήσεις με λέξεις-κλειδιά: Ένα βασικό πλεονέκτημα των εφαρμογών ψηφιακής εγκληματολογίας είναι η δυνατότητα εκτέλεσης αναζητήσεων με λέξεις-κλειδιά. Αυτό είναι ιδιαίτερα χρήσιμο καθώς οι δίσκοι έχουν γίνει μεγαλύτεροι και οι αναλυτές θα έπρεπε να επεξεργάζονται τεράστιες ποσότητες δεδομένων. Οι λέξεις-κλειδιά προέρχονται συχνά από άλλα στοιχεία της έρευνας ή από εξωτερικές πηγές. Για παράδειγμα, αν ένας αναλυτής διερευνά ένα περιστατικό κακόβουλου λογισμικού, μπορεί να χρησιμοποιήσει ένα ύποπτο DLL ή εκτελέσιμο από την ανάλυση της μνήμης. Σε άλλες περιπτώσεις, όπως η υπόνοια ότι ένας κακόβουλος εσωτερικός χρήστης προσέβαλε εμπιστευτικά αρχεία, οι λέξεις-κλειδιά μέσα σε αυτά τα έγγραφα μπορούν να χρησιμοποιηθούν για να διαπιστωθεί αν ο ύποπτος χρησιμοποίησε το σύστημα για πρόσβαση.

Το Autopsy έχει τη δυνατότητα εκτέλεσης αναζητήσεων λέξεων-κλειδιών με ακριβή ή μερική αντιστοίχιση. Για παράδειγμα, αν ένας αναλυτής πρέπει να διαπιστώσει αν ένα σύστημα χρησιμοποιήθηκε για πρόσβαση σε ένα αρχείο με τίτλο **pricing decision**, θα ψάξει για οποιαδήποτε ένδειξη ότι το σύστημα το προσέβαλε και ποιος χρήστης το έκανε.

Ο αναλυτής θα μεταβεί στην πάνω δεξιά γωνία και θα εισάγει το κείμενο **pricing decision** στο πεδίο αναζήτησης. Θα επιλεγεί η ακριβής αντιστοίχιση και στη συνέχεια θα πατήσει **Search**. Το αριστερό πάνελ θα δείξει αν υπήρχαν αποτελέσματα για το κείμενο. Στο κεντρικό πάνελ θα εμφανιστεί μια λίστα με τα αρχεία που περιείχαν τις αντιστοιχίες.

{9b365807-d2ef-11e4-b734-000c29ff2429}{3808876b-c176-4e48}	/img_J5mith_LT_0976.e01/vol_vol3/System Volume Inform...	dvisory.zip(H «pricing decision«PRICIN~1FILE0 RCDR(
\$MFT	/img_J5mith_LT_0976.e01/vol_vol3/\$MFT	desktop.ini\$I30«pricing decision«PRICIN~1progress
pricing decision.lnk	/img_J5mith_LT_0976.e01/vol_vol3/Users/informant/AppD...	ret Project Data\«pricing decision«1SP5010.11.11.128

Περαιτέρω εξέταση δείχνει ότι υπάρχουν δύο αρχεία συντόμευσης (**link files**) που σχετίζονται με το spreadsheet **pricing decision**. Ένα αρχείο συντόμευσης δημιουργείται όταν ανοίγεται ένα έγγραφο, και το Windows OS δημιουργεί ένα αρχείο .LNK μέσα στο MFT. Η νέα καταχώρηση τοποθετείται επίσης

στο φάκελο **Recents**, επιτρέποντας πρόσβαση σε πρόσφατα έγγραφα. Σε αυτή την περίπτωση, το link file δείχνει ότι το spreadsheet **pricing decision** ανοίχθηκε.

 (secret_project)_pricing_decision.xlsx.lnk	/img_JSmith_LT_0976.e01/vol_vol3/Users/informant/AppD...
 \$UsnJrnl:\$J	/img_JSmith_LT_0976.e01/vol_vol3/\$Extend/\$UsnJrnl:\$J
 (secret_project)_pricing_decision.xlsx.LNK	/img_JSmith_LT_0976.e01/vol_vol3/Users/informant/AppD...

Επιλέγοντας το πρώτο link file στο πάνω πάνελ, μπορούν να αποκαλυφθούν επιπλέον λεπτομέρειες στο κάτω πάνελ, όπως πότε το αρχείο προσπελάστηκε. Από την ανάλυση αυτών των δεδομένων, ο αναλυτής μπορεί να συμπεράνει ότι το σύστημα όντως προσέβαλε έναν κοινόχρηστο υπολογιστή στη διεύθυνση 10.11.11.128 και άνοιξε το spreadsheet **pricing decision**.

```
(secret_project)_pricing_decision.xlsx.lnk \\10.11.11.128\SECURED_DRIVE\Secret Project Data\pricing decision\
pricing decision
1SPS0
10.11.11.128
1SPS:
1SPS=C
\\10.11.11.128\secured_drive\Microsoft Network\Company's Secured Network Drive
SECRET~1
Secret Project Data
PRICIN~1
pricing decision
(S2BBE~1.XLS
(secret_project)_pricing_decision.xlsx
\\10.11.11.128\secured_drive\Secret Project Data\pricing decision (secret_project)_pricing_decision.xlsx
\\10.11.11.128\secured_drive\Secret Project Data\pricing decision (secret_project)_pricing_decision.xlsx
1SPS
```

Τα μεταδεδομένα δείχνουν όχι μόνο την ώρα πρόσβασης αλλά και ποιος λογαριασμός χρησιμοποίησε το αρχείο. Αυτό γίνεται εμφανές από τα δεδομένα του MFT και των link files.

Name	/img_JSmith_LT_0976.e01/vol_vol3/Users/informant/AppData/Roaming/Microsoft/Windows/Recent/(secret_project)_pricing_decision.xlsx.lnk
Type	File System
MIME Type	application/octet-stream
Size	1952
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	2015-03-23 20:26:53 UTC
Accessed	2015-03-23 20:26:53 UTC
Created	2015-03-23 20:26:53 UTC
Changed	2015-03-23 20:26:53 UTC
MD5	a9a4d030a0e6124ef8610617ee9125fc

Κάνοντας κλικ στο **Operating System User Account** στο αριστερό πάνελ, ο αναλυτής θα βρει πληροφορίες για τον ύποπτο λογαριασμό χρήστη.

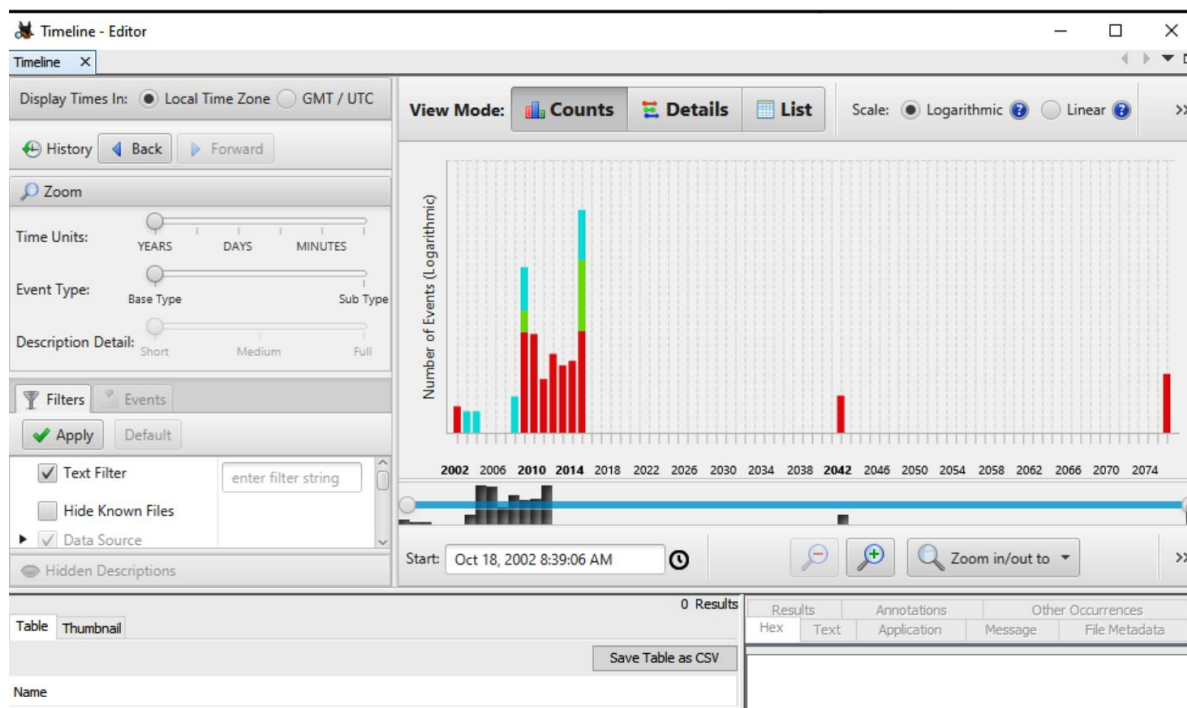
Type	Value
Username	informant
User ID	S-1-5-21-2425377081-3129163575-2985601102-1000

Η δυνατότητα αναζήτησης με λέξεις-κλειδιά είναι μία πτυχή των πλατφορμών ψηφιακής εγκληματολογίας που τις καθιστά πραγματικά χρήσιμες. Δίνει τη δυνατότητα στους αναλυτές να επικεντρωθούν σε κρίσιμα στοιχεία και να επανασυναρμολογήσουν την αλληλουχία των γεγονότων γρήγορα, παρά τις μεγάλες ποσότητες δεδομένων.

9.3. Ανάλυση Χρονολογίου (Timeline analysis)

Όταν διερευνάται ένα περιστατικό, είναι κρίσιμο να υπάρχει σαφής εικόνα για το πότε εκτελέστηκαν εφαρμογές ή αρχεία. Τα χρονικά σήματα (timestamps) μπορούν μερικές φορές να βρεθούν και σε άλλα στοιχεία της έρευνας, όπως κατά την εξέταση εικόνων μνήμης. Επιπλέον, η αναγνώριση συγκεκριμένων DLL αρχείων ή εκτελέσιμων αρχείων στην εικόνα μνήμης μπορεί να συγκριθεί με την ημερομηνία και ώρα που είχαν προσπελαστεί, ώστε να συσχετιστούν άλλες δραστηριότητες που έχουν παρατηρηθεί στο σύστημα.

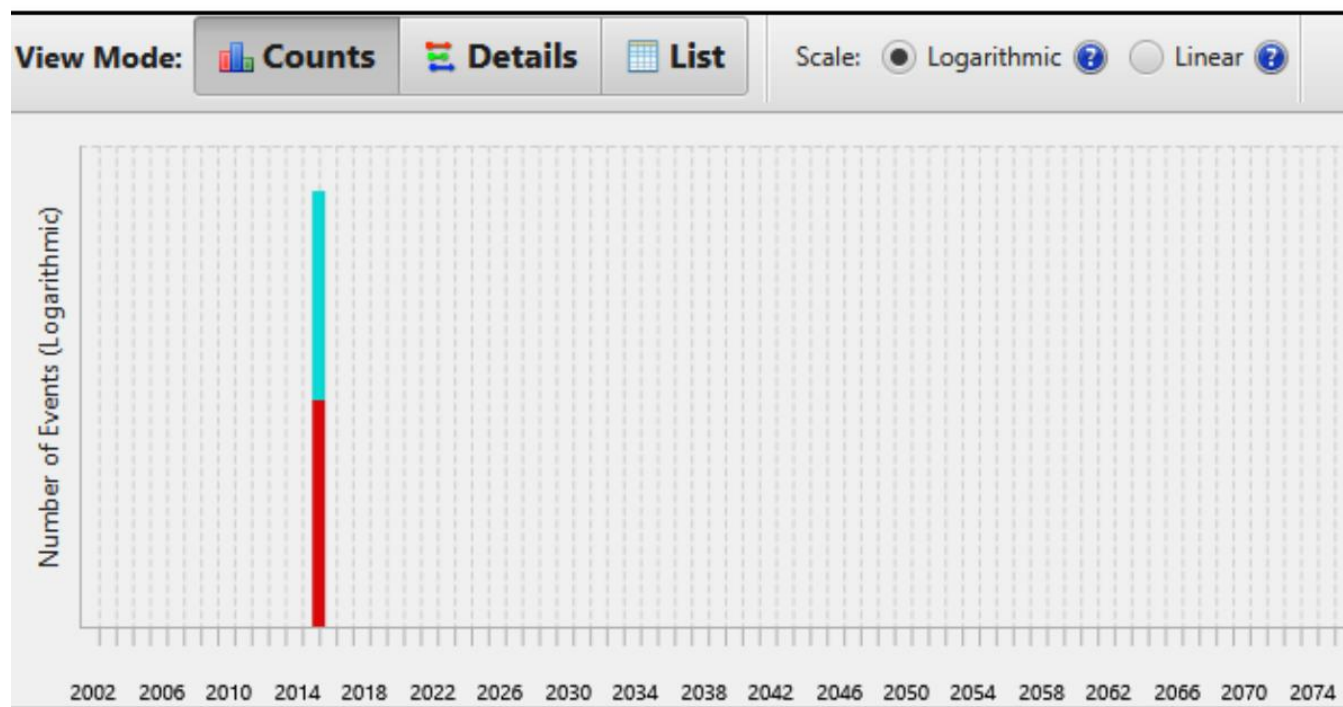
Ένα σημαντικό στοιχείο της ψηφιακής εγκληματολογίας που αξίζει να τονιστεί είναι η διασφάλιση ότι όλα τα συστήματα χρησιμοποιούν την ίδια ζώνη ώρας. Σε δικτυακά συστήματα, αυτό συνήθως επιτυγχάνεται μέσω του Network Time Protocol (NTP). Υπάρχουν περιπτώσεις όπου τα συστήματα δεν έχουν κανονικοποιημένη ώρα μέσω NTP. Οι αναλυτές θα πρέπει να δώσουν ιδιαίτερη προσοχή στο ποια ζώνη ώρας και συγχρονισμό πρέπει να χρησιμοποιηθεί. Η καλύτερη πρακτική είναι να ρυθμίζονται όλα τα συστήματα σε UTC, ειδικά αν η οργάνωση είναι γεωγραφικά διασκορπισμένη.



Το **Autopsy** διαθέτει λειτουργικότητα ειδικά για ανάλυση χρονολογίου. Απλά πατώντας το κουμπί **Timeline** στην κορυφή του παραθύρου, το Autopsy ξεκινά την επεξεργασία των δεδομένων

χρονολογίου. Ανάλογα με το μέγεθος της εικόνας που αναλύεται, η διαδικασία μπορεί να διαρκέσει λίγα λεπτά. Μόλις ολοκληρωθεί, θα ανοίξει το αντίστοιχο παράθυρο.

Από εδώ, ο αναλυτής μπορεί να χρησιμοποιήσει διάφορες δυνατότητες. Πρώτη είναι η **αναζήτηση κειμένου** στην αριστερή πλευρά της οθόνης. Για παράδειγμα, ο αναλυτής μπορεί ήδη να έχει εντοπίσει ότι ένα υπολογιστικό φύλλο με όνομα *pricing decision* είχε προσπελαστεί από το σύστημα υπό διερεύνηση. Αν θέλει να δει αν το αρχείο αυτό προσπελάστηκε και άλλες φορές, μπορεί να πληκτρολογήσει *pricing* στο πεδίο **Text Filter** και να πατήσει **Apply**, παράγοντας τα αντίστοιχα αποτελέσματα.



Από το γράφημα που εμφανίζεται, ο αναλυτής μπορεί να εξετάσει πιο λεπτομερώς τις συγκεκριμένες ώρες που το αρχείο προσπελάστηκε, κάνοντας κλικ στις χρωματιστές μπάρες. Οι αναλυτές μπορούν τώρα να δουν ότι το αρχείο προσπελάστηκε μόνο σε μία συγκεκριμένη ημερομηνία και ώρα από αυτό το σύστημα.

9.4. Ανάλυση MFT

Μία άλλη τεχνική για ανάλυση χρονολογίου είναι η χρήση εξωτερικών εργαλείων για την ανάλυση του **MFT (Master File Table)**. Το Autopsy επιτρέπει στον αναλυτή να εξάγει το MFT για ανάλυση με εργαλεία τρίτων. Σε αυτήν την περίπτωση, ο αναλυτής μπορεί να χρησιμοποιήσει ένα Python script που ονομάζεται **analyzeMFT**, διαθέσιμο στο GitHub. Το script δημιουργεί ένα αρχείο Excel με πληροφορίες ημερομηνίας και ώρας. Μπορεί επίσης να συνδυαστεί με άλλα scripts, όπως το **Log2Timeline**, για τη δημιουργία αρχείων που θα επιτρέπουν την ανασκόπηση των timestamps.

Βήματα για τη δημιουργία του αρχείου Excel με το **analyzeMFT**:

1. Κατέβασε και εγκατέστησε το **analyzeMFT** από το GitHub.
2. Εξήγαγε το MFT από το σύστημα που έχει παραβιαστεί. Στο Autopsy, βρες το αρχείο **\$MFT** στη δομή αρχείων του Volume 3, κάνε δεξί κλικ και επέλεξε **Extract File(s)**. Αποθήκευσε το αρχείο σε έναν φάκελο αποθήκευσης. Είναι καλό να αλλάξεις το όνομα του αρχείου, π.χ., σε *JSmith_LT_0976*.
3. Στον φάκελο με το εξαγόμενο αρχείο, τρέξε την εντολή:
4. `python analyzeMFT.py -f JSmith_LT_0976_$MFT -c JSMith_LT_0976_Timeline`

Η εντολή αυτή λέει στο **analyzeMFT** να επεξεργαστεί το MFT και να εξάγει τα αποτελέσματα σε αρχείο CSV, που μπορεί να ανοίξει με Microsoft Excel.

2010-11-21 07:06:15.881506 TZ ...B FILE NTFS	\$MFT SFN	[...B] time user host /Windows/winsxs/amd64_microsoft-windows-alg.resources_31bf3856ad364e35_6.1.
2009-07-14 03:20:30.316587 TZ ...B FILE NTFS	\$MFT SFN	[...B] time user host /Windows/winsxs/amd64_microsoft-windows-alg_31bf3856ad364e35_6.1.7600.1638
2010-11-21 07:06:26.337038 TZ ...B FILE NTFS	\$MFT SFN	[...B] time user host /Windows/winsxs/amd64_microsoft-windows-alttab.resources_31bf3856ad364e35_
2009-07-14 05:30:18.216305 TZ ...B FILE NTFS	\$MFT SFN	[...B] time user host /Windows/winsxs/amd64_microsoft-windows-alttab_31bf3856ad364e35_6.1.7600.16
2015-03-23 20:26:53.986593 TZ ...B FILE NTFS	\$MFT SFN	[...B] time user host /Users/informant/AppData/Roaming/Microsoft/Windows/Recent/(secret_project)_
2015-03-23 20:26:54.002193 TZ ...B FILE NTFS	\$MFT SFN	[...B] time user host /Users/informant/AppData/Roaming/Microsoft/Windows/Recent/pricing decision.In
2009-07-14 05:30:10.993492 TZ ...B FILE NTFS	\$MFT SFN	[...B] time user host /Windows/winsxs/amd64_microsoft-windows-appcompat-adm_31bf3856ad364e35_
2010-11-21 07:06:19.819912 TZ ...B FILE NTFS	\$MFT SFN	[...B] time user host /Windows/winsxs/amd64_microsoft-windows-appid.resources_31bf3856ad364e35_
2010-11-21 03:17:30.539425 TZ ...B FILE NTFS	\$MFT SFN	[...B] time user host /Windows/winsxs/amd64_microsoft-windows-appid_31bf3856ad364e35_6.1.7601.17
2010-11-21 07:06:15.881506 TZ ...B FILE NTFS	\$MFT SFN	[...B] time user host /Windows/winsxs/amd64_microsoft-windows-appwiz.resources_31bf3856ad364e35_

5. Βρες το CSV αρχείο στο φάκελο και, αν χρειαστεί, πρόσθεσε την κατάληξη `.csv` για να ανοίξει σωστά. Από εκεί, μπορείς να εξετάσεις ολόκληρο το χρονολόγιο και να χρησιμοποιήσεις εργαλεία αναζήτησης του Excel.

Άλλα scripts και εργαλεία, όπως το **Log2Timeline**, μπορούν να βοηθήσουν περαιτέρω στην επεξεργασία αυτών των δεδομένων.

9.5. Ανάλυση Μητρώου (Registry analysis)

Στο λειτουργικό σύστημα Windows, υπάρχει σημαντική δραστηριότητα που καταγράφεται στο **Windows Registry**. Το Registry είναι μια βάση δεδομένων που αποθηκεύει ρυθμίσεις χαμηλού επιπέδου για το λειτουργικό σύστημα, όπως ρυθμίσεις συσκευών, ασφάλειας, υπηρεσιών και των λογαριασμών χρηστών στο **Security Accounts Manager (SAM)**.

Το Registry αποτελείται από δύο στοιχεία:

- **Keys** (κλειδιά): δοχεία που περιέχουν τις τιμές.
- **Values** (τιμές): αποθηκεύουν συγκεκριμένες πληροφορίες ρυθμίσεων.

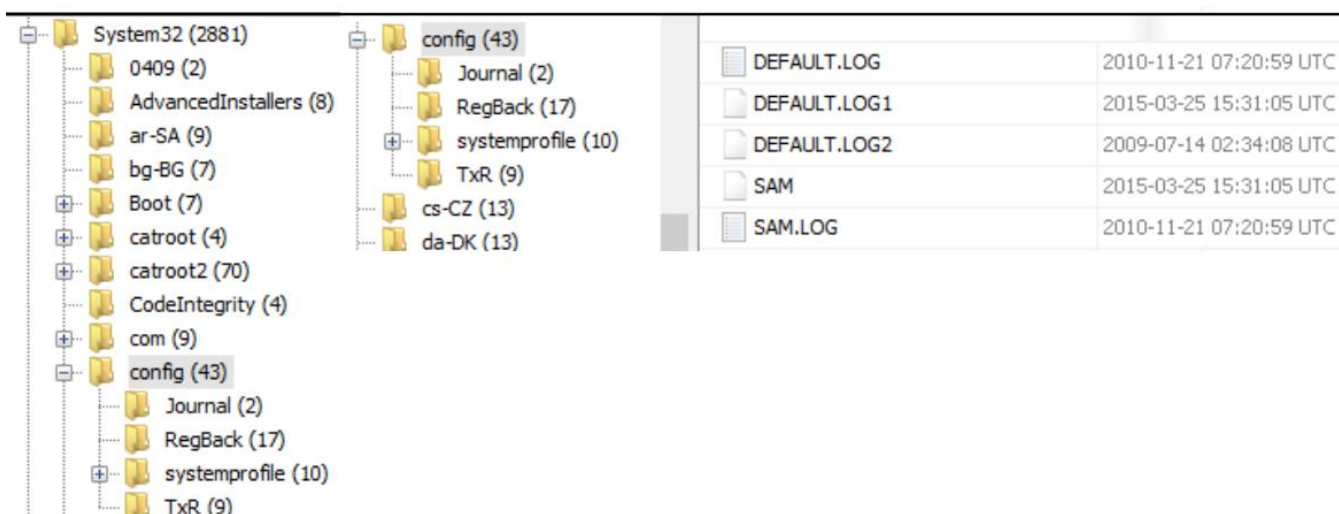
Τα κύρια κλειδιά (root keys) στο Windows OS είναι πέντε και βρίσκονται στους registry hives στο φάκελο `%SystemRoot%\system32\config`:

- HKEY_CURRENT_USER
- HKEY_USERS
- HKEY_CLASSES_ROOT
- HKEY_LOCAL_MACHINE
- HKEY_CURRENT_CONFIG

Κατά τη διερεύνηση περιστατικών, το πιο σημαντικό είναι το **HKEY_LOCAL_MACHINE (HKLM)**, το οποίο περιέχει υποκλειδιά όπως:

- **SAM**: αποθηκεύει κωδικούς χρηστών σε μορφή LM ή NTLM hash.
- **Security**: πληροφορίες ασφάλειας του domain που είναι συνδεδεμένο το σύστημα.
- **Software**: αποθηκεύει ρυθμίσεις λογισμικού και Windows, χρήσιμο για εντοπισμό αλλαγών από malware.
- **System**: περιέχει ρυθμίσεις συστήματος και πληροφορίες για τις τρέχουσες συνδεδεμένες συσκευές.

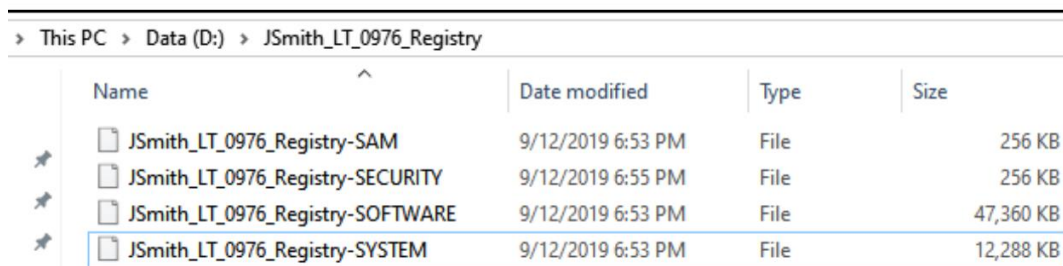
Άλλη σημαντική πηγή πληροφοριών είναι το **HKEY_CURRENT_USER**, όπου οι αλλαγές σε λογαριασμούς χρηστών καταγράφονται στο αρχείο **NTUSER.dat**, το οποίο βρίσκεται σε **C:\Users*UserName***. Το αρχείο περιέχει τις ρυθμίσεις του προφίλ χρήστη και μπορεί να δώσει στοιχεία για συνδεδεμένα συστήματα, δικτυακές συνδέσεις ή άλλες ρυθμίσεις. Οι αναλυτές μπορούν να έχουν πρόσβαση στα registry hives μέσω του Autopsy, πηγαίνοντας στο φάκελο **vol3/Windows/System32/config**. Το αρχείο **SAM** βρίσκεται στο κεντρικό παράθυρο.



Η εξέταση των ρυθμίσεων των κλειδιών του Registry είναι λεπτομερής. Αν και δεν μπορεί να καλυφθεί πλήρως σε αυτό το κεφάλαιο, είναι σημαντικό οι αναλυτές να μπορούν να αποκτήσουν τα κλειδιά για αξιολόγηση και να γνωρίζουν εργαλεία τρίτων για πρακτική εξέταση.

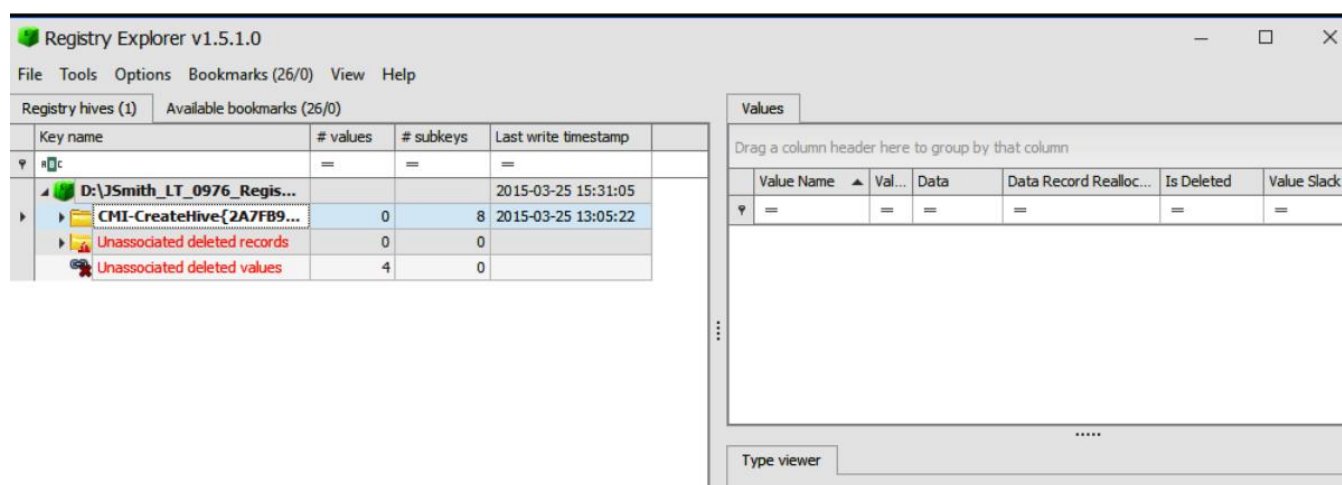
Για παράδειγμα, για την ανάλυση:

1. Πήγαινε στο φάκελο /System32/config στο τρίτο volume της εικόνας συστήματος.
2. Επιλέξτε τα τέσσερα κλειδιά (System, SAM, Security, Software) με Ctrl + δεξί κλικ και επίλεξε **Export File(s)**.
3. Επιλέξτε φάκελο για την αποθήκευση.
4. Επιβεβαιώσε ότι τα αρχεία έχουν αποθηκευτεί σωστά.



Name	Date modified	Type	Size
JSmith_LT_0976_Registry-SAM	9/12/2019 6:53 PM	File	256 KB
JSmith_LT_0976_Registry-SECURITY	9/12/2019 6:55 PM	File	256 KB
JSmith_LT_0976_Registry-SOFTWARE	9/12/2019 6:53 PM	File	47,360 KB
JSmith_LT_0976_Registry-SYSTEM	9/12/2019 6:53 PM	File	12,288 KB

Μετά, ο αναλυτής μπορεί να χρησιμοποιήσει εργαλεία τρίτων για την εξέταση των registry files. Το προηγούμενο στιγμιότυπο εμφανίζει τα τέσσερα αρχεία μητρώου (registry) που έχουν αποκτηθεί. Αφού τα αρχεία μητρώου της ύποπτης εικόνας αποθηκευτούν, ο αναλυτής μπορεί να χρησιμοποιήσει ένα εργαλείο τρίτου κατασκευαστή για να εξετάσει το μητρώο. Σε αυτή την περίπτωση, θα χρησιμοποιηθεί το εργαλείο **Registry Explorer/RECmd Έκδοση 1.5.1.0**, το οποίο αναπτύχθηκε από τον **Eric Zimmerman**, για την ανάλυση των κλειδιών του μητρώου. Αυτή η δωρεάν εφαρμογή μπορεί να ληφθεί από το: <https://ericzimmerman.github.io/#!index.md>. Αποσυμπίεστε το αρχείο σε μια ασφαλή τοποθεσία και εκτελέστε την εφαρμογή.



Καθώς η ανάλυση της εικόνας προχωρά, ο αναλυτής έχει εντοπίσει ότι πιθανώς έχει συμβεί **απώλεια δεδομένων μέσω συσκευής USB** που είχε συνδεθεί κάποια στιγμή στο σύστημα. Παρόλο που το **Autopsy** μας παρείχε κάποιες σχετικές πληροφορίες, ίσως είναι απαραίτητο να διαπιστωθεί ποια

κλειδιά του μητρώου έχουν τροποποιηθεί ως αποτέλεσμα της σύνδεσης αυτής της USB συσκευής. Το καλύτερο σημείο για πρόσθετες πληροφορίες βρίσκεται στο **system registry hive**.

USBSTOR	0
Disk&Ven_SanDisk&Prod_Cruzer_Fit&Re...	0
4C530012450531101593&0	12
4C530012550531106501&0	12

Το λειτουργικό σύστημα **Windows** καταγράφει και διατηρεί τεκμήρια για το πότε USB συσκευές, όπως mass storage, iOS συσκευές, ψηφιακές κάμερες και άλλες, συνδέθηκαν. Αυτό οφείλεται στον **Plug and Play manager (PnP)**, που αποτελεί μέρος του λειτουργικού. Ο PnP λαμβάνει ειδοποίηση ότι μια USB συσκευή έχει συνδεθεί και την αναζητά για πληροφορίες, ώστε να φορτώσει τον κατάλληλο driver. Μετά την ολοκλήρωση, το λειτουργικό καταχωρεί την συσκευή μέσα στις ρυθμίσεις του μητρώου.

Για να προσδιοριστεί ποιες USB συσκευές είχαν συνδεθεί, ακολουθήστε τα παρακάτω βήματα:

1. Ανοίξτε το **Registry Explorer**.
2. Επιλέξτε **File** και έπειτα **Load Hive**.
3. Πλοηγηθείτε στο **system registry hive**.
4. Μόλις φορτωθεί, θα εμφανιστεί το ακόλουθο παράθυρο:
Από εδώ, μεταβείτε στην κατάλληλη θέση του μητρώου USB στη διαδρομή:
ControlSet001\Enum\USBSTOR
5. Κάντε κλικ στην πρώτη τιμή μητρώου, **4C530012450531101593&0**. Θα εμφανιστούν οι εξής πληροφορίες στο επάνω δεξί τμήμα:

Value Name ▲	Value Type	Data	Data Record Reall...	Is Deleted	Value Slack
Capabilities	RegDword	16	☐	☐	
Class	RegSz	DiskDrive	☐	☐	
ClassGUID	RegSz	{4d36e967-e325-...	☐	☐	00-00-00-00-00-00
CompatibleIDs	RegMultiSz	USBSTOR\Disk US...	☐	☐	
ConfigFlags	RegDword	0	☐	☐	
ContainerID	RegSz	{4933888a-6002-...	☐	☐	00-00-00-00-00-00
DeviceDesc	RegSz	@disk.inf,%disk_...	☐	☐	22-00-00-00
Driver	RegSz	{4d36e967-e325-...	☐	☐	00-00-00-00
FriendlyName	RegSz	SanDisk Cruzer Fit...	☐	☐	
HardwareID	RegMultiSz	USBSTOR\DiskSan...	☐	☐	00-00-00-00
Mfg	RegSz	@disk.inf,%genm...	☐	☐	B7-DA-00-00-00-00
Service	RegSz	disk	☐	☐	50-00

Από αυτό το σημείο, ο αναλυτής έχει στη διάθεσή του πολλές πληροφορίες προς εξέταση. Ιδιαίτερης σημασίας είναι το **HardwareID**. Κάνοντας κλικ σε αυτό το τμήμα του αποτελέσματος, εμφανίζονται πρόσθετες λεπτομέρειες στο κάτω δεξί παράθυρο.

Type viewer	Slack viewer	Binary viewer
Value name	HardwareID	
Value type	RegMultiSz	
Value	USBSTOR\DiskSanDisk_Cruzer_Fit_____2.01 USBSTOR\DiskSanDisk_Cruzer_Fit_____ USBSTOR\DiskSanDisk_ USBSTOR\SanDisk_Cruzer_Fit_____2 SanDisk_Cruzer_Fit_____2 USBSTOR\GenDisk GenDisk	
Raw value	55-00-53-00-42-00-53-00-54-00-4F-00-52-00-5C-00-44-00-69-00-73-00-6B-00-53-00-61-00-6E-00-44-00-69-00-73-00-6B-00-5F-00-43-00-72-00-75-00-7A-00-65-00-72-00-5F-00-46-00-69-00-74-00-5F-00-5F-00-5F-00-5F-00-5F-00-32-00-2E-00-30-00-31-00-00-00-55-00-53-00-42-00-53-00-54-00-4F-00-52-00-	
Slack	00-00-00-00	

Αυτό που κατάφερε να αποκαλύψει ο αναλυτής, αξιολογώντας την ημερομηνία και την ώρα, είναι ότι ένα **SanDisk Cruzer Fit** είχε συνδεθεί στο σύστημα. Διαπιστώθηκε ότι συνδέθηκε στις **13:38:00 της 24/03/2015**. Η πληροφορία αυτή είναι κρίσιμη, καθώς συγκρίνεται με την ημερομηνία και ώρα που είχαν προσπελαστεί τα εμπιστευτικά αρχεία.

Όπως αναφέραμε προηγουμένως, η ανάλυση του μητρώου αποτελεί από μόνη της **βαθύ υποσύνολο της ψηφιακής εγκληματολογίας**. Έχουν γραφτεί ολόκληροι τόμοι σχετικά με την αποδεικτική αξία που εμπεριέχεται στις ρυθμίσεις και τις εγγραφές των hives του μητρώου. Το ελάχιστο που πρέπει να κάνουν οι responders είναι να προετοιμάζονται για την απόκτηση αυτών των τεκμηρίων, ώστε να εξεταστούν περαιτέρω από ειδικούς. Παρόλα αυτά, καθώς οι αναλυτές αποκτούν περισσότερη εμπειρία και δεξιότητες, το μητρώο θα πρέπει να αποτελεί περιοχή που μπορεί να αξιοποιηθεί για εξαγωγή αποδεικτικών στοιχείων κατά την ανάλυση μιας εικόνας δίσκου.

Σε πολλές περιπτώσεις, το παρόν κεφάλαιο απλώς αγγίζει την επιφάνεια των πληροφοριών που μπορούν να εντοπιστούν με την αξιοποίηση εργαλείων ψηφιακής ανάλυσης δίσκου. Η διερεύνηση μιας εικόνας δίσκου με το **Autopsy** ανέδειξε ορισμένες από τις δυνατότητες που είναι διαθέσιμες στους αναλυτές. Από εκεί και πέρα, εξετάστηκαν άλλες πηγές δεδομένων, όπως το **Windows Registry** και ο **MFT (Master File Table)**, ώστε να δοθεί στους αναλυτές μια ιδέα για το ποια δεδομένα μπορούν να αξιοποιηθούν κατά την ανάλυση ενός περιστατικού.

Τα συγκεκριμένα εργαλεία και τεχνικές εξαρτώνται σε μεγάλο βαθμό από το εργαλείο που χρησιμοποιείται. Το σημαντικό είναι να γίνει κατανοητό ότι τα σύγχρονα λειτουργικά συστήματα αφήνουν ίχνη της δραστηριότητάς τους σε ολόκληρο τον δίσκο, από τα στοιχεία αλλαγής αρχείων στον MFT έως τις ρυθμίσεις των κλειδιών μητρώου κατά την προσθήκη νέων λογαριασμών χρηστών.

Οι αναλυτές περιστατικών θα πρέπει να διαθέτουν την απαραίτητη τεχνογνωσία για το πώς τα σύγχρονα λειτουργικά συστήματα αποθηκεύουν δεδομένα και πώς μπορούν να αξιοποιήσουν εμπορικά ή ελεύθερα εργαλεία λογισμικού για τον εντοπισμό αυτών των δεδομένων.

Σε συνδυασμό με άλλα αποδεικτικά στοιχεία που συλλέγονται από **δικτυακές πηγές** και από τη **μνήμη (RAM)**, τα δεδομένα από τον δίσκο μπορούν να προσφέρουν μεγαλύτερη σαφήνεια σε σχέση με ένα περιστατικό και να συμβάλουν στον εντοπισμό της ρίζας του προβλήματος. Ένα από τα βασικά σημεία εστίασης στην ανάλυση της αποθήκευσης συστήματος είναι η **εξαγωγή και εξέταση των αρχείων καταγραφής (log files)**, τα οποία αποτελούν κρίσιμο σημείο δεδομένων που παρέχει στους αναλυτές σημαντικό όγκο πληροφοριών.

10

Ανάλυση Αρχείων Καταγραφής (Log Files)

Ο Σέρλοκ Χολμς της Γαλλίας, ο Δρ. Edmond Locard, υπήρξε πρωτοπόρος στον τομέα της εγκληματολογικής επιστήμης. Ως εγκληματολόγος και δάσκαλος, ο Locard ανέπτυξε τεχνικές και μεθοδολογίες που εξακολουθούν να επηρεάζουν την εγκληματολογική επιστήμη σήμερα. Μία από τις αρχές για τις οποίες είναι γνωστός είναι η **Αρχή της Ανταλλαγής του Locard**. Η αρχή αυτή δηλώνει ότι όταν ένας ύποπτος αλληλεπιδρά με μια σκηνή εγκλήματος, αφήνει πίσω του ίχνη. Στον φυσικό κόσμο, αυτό μπορεί να περιλαμβάνει τρίχες, ίνες από ρούχα, αίμα ή δέρμα, τα οποία μένουν σε επιφάνειες και αντικείμενα της σκηνής εγκλήματος. Αντίστοιχα, η σκηνή εγκλήματος αφήνει ίχνη πάνω στον ύποπτο. Ίνες από το χαλί, σκόνη, μεταλλικά θραύσματα ή γυαλί από σπασμένο παράθυρο μπορεί να βρεθούν στον ύποπτο. Η εγκληματολογική επιστήμη έχει αναπτύξει ολοένα και πιο προηγμένες πρακτικές και τεχνολογίες για την ανίχνευση ακόμη και των πιο μικροσκοπικών ιχνών.

Το έργο του Locard επικεντρώθηκε στον φυσικό κόσμο, πολύ πριν την εμφάνιση των υπολογιστών. Ωστόσο, η αρχή ότι κάθε ενέργεια ενός δράστη σε μια σκηνή εγκλήματος αφήνει ίχνη, ισχύει εξίσου και στην **ψηφιακή εγκληματολογία**. Για παράδειγμα, όταν ένας επιτιθέμενος παραβιάζει ένα σύστημα και εγκαθιστά υποδομή command-and-control σε έναν web server, αφήνει ίχνη με τη μορφή καταγραφών στο firewall. Η εκτέλεση κακόβουλου λογισμικού στον server μπορεί να αφήσει ίχνη στη μνήμη, στα αρχεία καταγραφής συμβάντων, καθώς και κακόβουλο κώδικα στη μονάδα αποθήκευσης. Σε όλη την αλυσίδα των γεγονότων, ο επιτιθέμενος θα αφήσει ίχνη της παρουσίας του στις διάφορες συσκευές με τις οποίες ήρθε σε επαφή.

Στα προηγούμενα κεφάλαια συζητήθηκαν οι διάφορες τοποθεσίες και τεχνικές που μπορούν να αξιοποιήσουν οι αναλυτές για την αποκάλυψη αυτών των ιχνών από τη μνήμη, τους σκληρούς δίσκους και την κυκλοφορία του δικτύου. Μία πηγή πλούσια σε δεδομένα που μπορεί να αξιοποιηθεί είναι τα **αρχεία καταγραφής (log files)**. Οι ενέργειες καταγράφονται σε πλήθος υλικού και λογισμικού. Αυτό που απαιτείται από τους αναλυτές είναι να κατανοήσουν πώς να αποκτήσουν πρόσβαση σε αυτά τα logs, πώς να τα εξετάσουν και τι πληροφορίες περιέχουν. Έτσι μπορούν να εντοπίσουν σημαντικές ενδείξεις σχετικά με τη ρίζα ενός περιστατικού.

Σε αυτό το κεφάλαιο η συζήτηση θα εστιάσει:

- στα αρχεία καταγραφής και στη διαχείρισή τους,

- στη χρήση εργαλείων συγκέντρωσης καταγραφών, όπως τα συστήματα **SIEM (Security Information and Event Management)**,
- στα αρχεία καταγραφής συμβάντων των **Windows**,
- και στην ανάλυση αρχείων καταγραφής συμβάντων **Windows**.

Στόχος είναι, μέσα από τη συζήτηση αυτών των τεχνικών, οι αναλυτές να κατανοήσουν πώς τα logs είναι κρίσιμα σε μια έρευνα περιστατικών ασφαλείας και πώς εντάσσονται σε μια συνολικότερη διερεύνηση.

10.1. Καταγραφή και Διαχείριση Καταγραφών

Η «ζωογόνο δύναμη» μιας σωστής έρευνας περιστατικών είναι τα αποδεικτικά στοιχεία από ένα ευρύ φάσμα πηγών. Ακόμη και μια μόλυνση με κακόβουλο λογισμικό σε έναν host χρειάζεται επιβεβαίωση από πολλαπλές πηγές. Ένα κοινό πρόβλημα στην απόκριση περιστατικών, ειδικά σε μικρότερα δίκτυα, είναι ο τρόπος με τον οποίο ο οργανισμός διαχειρίζεται τα logs. Για μια ολοκληρωμένη έρευνα, οι αναλυτές πρέπει να έχουν πρόσβαση σε όσο το δυνατόν περισσότερα δεδομένα δικτύου. Πολύ συχνά, όμως, οι οργανισμοί δεν διαθέτουν τους κατάλληλους πόρους για τη συλλογή πλήρων αρχείων καταγραφής από τις συσκευές του δικτύου και άλλα συστήματα.

Πριν από οποιοδήποτε περιστατικό, είναι κρίσιμο να καθοριστεί σαφώς τι και πώς θα καταγράφει ένας οργανισμός, καθώς και πώς θα διατηρεί αυτά τα logs. Αυτό πρέπει να αποτυπώνεται σε **πολιτική διαχείρισης καταγραφών** και στις αντίστοιχες διαδικασίες. Η **Ομάδα Απόκρισης Περιστατικών Ασφάλειας Υπολογιστών (CSIRT)** πρέπει να συμμετέχει σε κάθε συζήτηση σχετικά με το ποια logs είναι απαραίτητα, καθώς διαθέτει γνώση για την αξία των διαφορετικών πηγών καταγραφής.

Το **NIST** έχει δημοσιεύσει έναν σύντομο οδηγό για τη διαχείριση καταγραφών, διαθέσιμο στη διεύθυνση:

<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf>

10.2. Νομικά Ζητήματα Σχετικά με τα Logs

Εκτός από τα τεχνικά ζητήματα, υπάρχουν και νομικά θέματα που πρέπει να διευθετηθούν. Μερικά από αυτά είναι:

- **Καθιέρωση της καταγραφής ως κανονική επιχειρηματική πρακτική:** Ανάλογα με το είδος της επιχείρησης και τη δικαιοδοσία, οι χρήστες μπορεί να έχουν εύλογη προσδοκία ιδιωτικότητας, εάν δεν υπάρχει σαφής πολιτική παρακολούθησης. Αν τα logs ενεργοποιηθούν αποκλειστικά για την ανίχνευση κακόβουλων ενεργειών, μπορεί να προκύψουν νομικά ζητήματα. Συνεπώς, η πολιτική πρέπει να δηλώνει ότι η καταγραφή της δραστηριότητας αποτελεί μέρος της κανονικής επιχειρηματικής λειτουργίας.

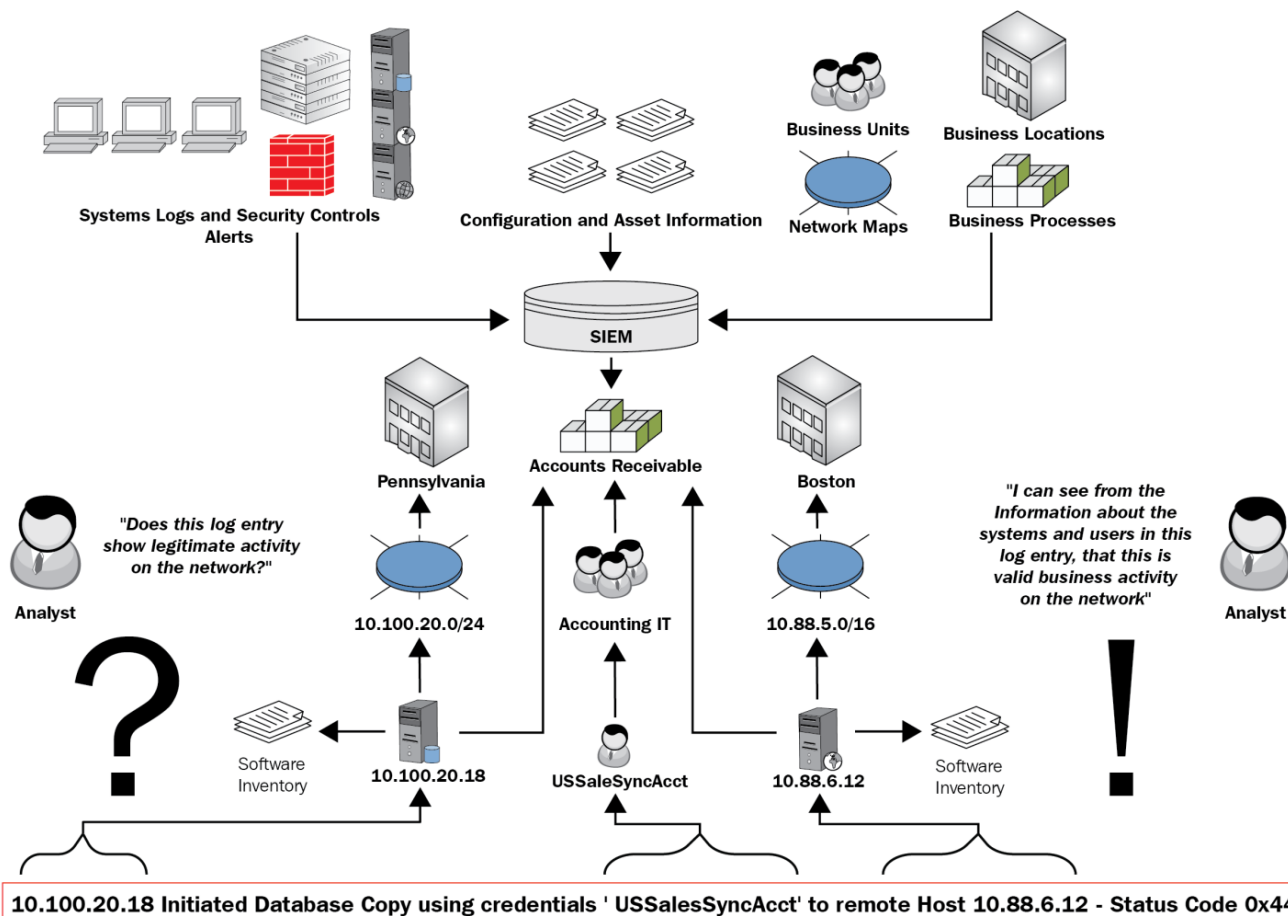
- **Καταγραφή κοντά στο συμβάν:** Αν και η αυτόματη καταγραφή γίνεται συνήθως τη στιγμή του συμβάντος, από πλευράς αποδεικτικής αξίας, όσο πιο μακριά χρονικά δημιουργούνται τα logs από το συμβάν, τόσο μειώνεται η αξία τους σε δικαστήριο.
- **Εξειδικευμένο προσωπικό:** Η αξιοπιστία των logs εξαρτάται συχνά από το ποιος τα δημιούργησε και αν ήταν γνώστης του συμβάντος. Στα logs από συσκευές δικτύου, το λογισμικό καταγραφής καλύπτει αυτό το ζήτημα, εφόσον μπορεί να αποδειχθεί ότι λειτουργούσε σωστά.
- **Ολοκληρωμένη καταγραφή:** Η καταγραφή σε επίπεδο επιχείρησης πρέπει να καλύπτει όσο το δυνατόν περισσότερα συστήματα και να είναι συνεπής. Τυχαία ή αποσπασματική καταγραφή έχει μικρότερη αξία σε δικαστήριο από μια συνεπή πολιτική.
- **Ορισμός υπεύθυνου φύλακα δεδομένων:** Η πολιτική πρέπει να ορίζει ένα άτομο ως custodian, το οποίο θα εκπροσωπεί τη διαδικασία καταγραφής, τα εργαλεία που χρησιμοποιούνται και θα μπορεί να καταθέσει για την ακρίβεια των logs.
- **Τεκμηρίωση αποτυχιών:** Τυχόν αποτυχίες ή παρατεταμένες ελλείψεις στην καταγραφή συμβάντων πρέπει να καταγράφονται με σαφή αιτιολόγηση, αλλιώς μειώνεται η αποδεικτική τους αξία.
- **Ανακάλυψη αρχείων καταγραφής:** Οι οργανισμοί πρέπει να γνωρίζουν ότι τα logs που χρησιμοποιούνται σε δικαστικές διαδικασίες θα είναι διαθέσιμα και στο αντίδικο.
- **Logs από παραβιασμένα συστήματα:** Θεωρούνται ύποπτα και απαιτούν ειδική μαρτυρία για την αξιοπιστία τους.
- **Πρωτότυπα αντίγραφα:** Τα logs πρέπει να διατηρούνται σε πρωτότυπη μορφή, με σωστή αλυσίδα φύλαξης (chain of custody) μέχρι την επίσημη καταστροφή τους με δικαστική εντολή.

Η διαδικασία **log management** θέτει τα θεμέλια για τον εντοπισμό των γεγονότων που θεωρούνται απαραίτητα από τον οργανισμό. Το επόμενο βασικό στοιχείο είναι η τεχνολογία που χρησιμοποιείται για τη συγκέντρωση και ανασκόπηση των logs. Αυτό περιλαμβάνει την ενσωμάτωση ενός **συστήματος SIEM** ως μέρος της συνολικής στρατηγικής διαχείρισης καταγραφών.

10.3. Εργασία με Συστήματα Διαχείρισης Συμβάντων

Μία σημαντική πρόκληση που αντιμετωπίζουν πολλοί οργανισμοί είναι η φύση της καταγραφής στα δικτυακά τους συστήματα. Λόγω περιορισμένου χώρου, τα αρχεία καταγραφής (logs) συχνά **επανεγγράφονται** (rolled over), με αποτέλεσμα τα νέα logs να αντικαθιστούν τα παλαιότερα. Αυτό έχει ως συνέπεια, σε ορισμένες περιπτώσεις, ένας οργανισμός να διαθέτει μόνο λίγες ημέρες ή ακόμα και λίγες ώρες κρίσιμων καταγραφών. Εάν ένα πιθανό περιστατικό συνέβη αρκετές εβδομάδες πριν, το προσωπικό απόκρισης περιστατικών θα στερηθεί σημαντικά αποδεικτικά στοιχεία.

Ένα εργαλείο που έχει υιοθετηθεί από πολλές επιχειρήσεις είναι τα **συστήματα SIEM (Security Information and Event Management)**. Οι πλατφόρμες αυτές έχουν τη δυνατότητα να συγκεντρώνουν δεδομένα καταγραφών και συμβάντων από πολλαπλές πηγές δικτύου και να τα συνδυάζουν σε μια κεντρική τοποθεσία. Αυτό επιτρέπει στην ομάδα **CSIRT** και στο προσωπικό ασφαλείας να παρακολουθούν δραστηριότητα σε ολόκληρο το δίκτυο, χωρίς να χρειάζεται να εξετάσουν ξεχωριστά κάθε σύστημα.



Διάφορες πηγές, από μηχανισμούς ασφαλείας μέχρι βάσεις δεδομένων SQL, μπορούν να ρυθμιστούν ώστε να στέλνουν καταγραφές στο SIEM. Για παράδειγμα, μια βάση δεδομένων SQL στη διεύθυνση **10.100.20.18** μπορεί να δείξει ότι ο λογαριασμός **USSalesSyncAcct** χρησιμοποιήθηκε για την αντιγραφή μιας βάσης δεδομένων σε έναν απομακρυσμένο host με διεύθυνση **10.88.6.12**. Το SIEM επιτρέπει τον άμεσο έλεγχο τέτοιων ενεργειών. Εάν διαπιστωθεί ότι ο λογαριασμός **USSalesSyncAcct** έχει παραβιαστεί, οι αναλυτές CSIRT μπορούν γρήγορα να ελέγξουν τη χρήση του μέσα από το SIEM, εντοπίζοντας σχετικές καταγραφές. Χωρίς το SIEM, οι αναλυτές θα έπρεπε να ελέγξουν χειροκίνητα κάθε σύστημα στο οποίο πιθανώς έγινε χρήση, διαδικασία ιδιαίτερα χρονοβόρα.

10.4. Δυνατότητες που παρέχει ένα SIEM

Από την πλατφόρμα SIEM, οι αναλυτές ασφαλείας και δικτύου μπορούν να εκτελούν διάφορες λειτουργίες που σχετίζονται με την απόκριση περιστατικών, όπως:

- **Συγκέντρωση καταγραφών (Log aggregation):** Οι περισσότερες επιχειρήσεις διαθέτουν χιλιάδες συσκευές στο εσωτερικό τους δίκτυο, καθεμία με δικά της logs. Το SIEM μπορεί να συγκεντρώσει όλα αυτά τα δεδομένα σε μία κεντρική τοποθεσία.
- **Διατήρηση καταγραφών (Log retention):** Μια σημαντική λειτουργία των SIEM είναι η δυνατότητα διατήρησης των logs. Πλαίσια κανονιστικής συμμόρφωσης, όπως το **PCI-DSS**, ορίζουν ότι τα logs πρέπει να διατηρούνται για διάστημα 1 έτους, με τουλάχιστον 90 ημέρες διαθέσιμες άμεσα. Τα SIEM διευκολύνουν τη διαχείριση, αρχειοθετώντας τα logs με οργανωμένο τρόπο και επιτρέποντας την άμεση ανάκτησή τους.
- **Περιοδική ανάλυση (Routine analysis):** Είναι καλή πρακτική η τακτική ανασκόπηση των δεδομένων μέσω της πλατφόρμας SIEM. Συνήθως προσφέρεται πίνακας ελέγχου (dashboard) που παρουσιάζει βασικά στοιχεία, όπως αριθμό συνδέσεων, ροή δεδομένων και κρίσιμες ειδοποιήσεις. Παράλληλα, παρέχεται δυνατότητα δημιουργίας αναφορών ώστε οι υπεύθυνοι να ενημερώνονται για τη δραστηριότητα.
- **Ειδοποιήσεις (Alerting):** Οι πλατφόρμες SIEM μπορούν να ενεργοποιούν ειδοποιήσεις για συγκεκριμένες συνθήκες που υποδηλώνουν κακόβουλη δραστηριότητα. Αυτό περιλαμβάνει ειδοποιήσεις από antivirus, IPS/IDS και άλλα συστήματα. Επιπλέον, διαθέτουν τη δυνατότητα **συσχέτισης συμβάντων (event correlation)**, δηλαδή τον εντοπισμό συσχετίσεων ανάμεσα σε διαφορετικά γεγονότα. Για παράδειγμα, εάν ένας λογαριασμός χρήστη προσπαθήσει να συνδεθεί επανειλημμένα σε πολλαπλά συστήματα, το SIEM μπορεί να αναγνωρίσει αυτήν τη δραστηριότητα και να ειδοποιήσει τους αρμόδιους.
- **Αντιμετώπιση περιστατικών (Incident response):** Επειδή το SIEM συγκεντρώνει και αναλύει κεντρικά τα logs, οι αναλυτές CSIRT το χρησιμοποιούν συχνά κατά τη διάρκεια ενός περιστατικού. Μπορούν να εκτελούν ερωτήματα ή να κατεβάζουν logs για offline ανάλυση. Η κεντροποίηση μειώνει σημαντικά τον χρόνο που απαιτείται για αναζήτηση και συλλογή συμβάντων. Για παράδειγμα, αν εντοπιστεί παραβίαση λογαριασμού, χωρίς SIEM ο αναλυτής θα έπρεπε να ελέγξει πολλά συστήματα. Με το SIEM, αρκεί μία αναζήτηση στον συγκεντρωτικό πίνακα, αποκτώντας άμεσα πλήρη εικόνα της δραστηριότητας του λογαριασμού.

10.5. Κόστος και Επιλογές

Οι πλατφόρμες SIEM απαιτούν σημαντικό χρόνο και κόστος για την προμήθεια και υλοποίησή τους. Προστίθενται, επίσης, οι ανάγκες συνεχούς συντήρησης, ενημέρωσης και προσαρμογής κανόνων. Ωστόσο, από την πλευρά της απόκρισης περιστατικών, ένα σωστά ρυθμισμένο και συντηρημένο SIEM είναι ζωτικής σημασίας για τη γρήγορη συλλογή αποδεικτικών στοιχείων σε επίπεδο δικτύου.

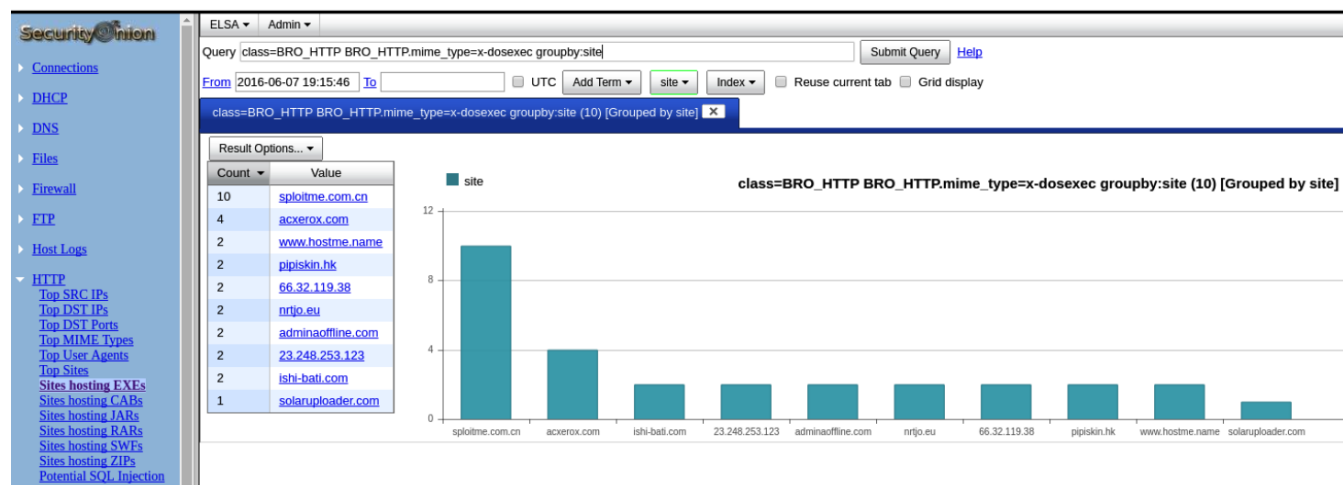
Επιπλέον, οι δυνατότητές του μπορούν να μειώσουν σημαντικά τον χρόνο που απαιτείται για τον εντοπισμό της ρίζας ενός περιστατικού. Ένα άρθρο με αναλυτική παρουσίαση των περιπτώσεων χρήσης SIEM σε εταιρικά περιβάλλοντα βρίσκεται στη διεύθυνση: <https://gbhackers.com/security-information-and-eventmanagement-siem-a-detailed-explanation>

Υπάρχουν πολλές εμπορικές αλλά και ανοικτού κώδικα επιλογές για SIEM. Δύο δημοφιλείς λύσεις ανοικτού κώδικα είναι το **Security Onion** και το **Elastic Stack**, που προσφέρουν πλήρεις δυνατότητες και μπορούν να υποστηρίξουν τους αναλυτές στην εξέταση αρχείων καταγραφής.

10.6. Security Onion

Οι πλήρως εξοπλισμένες πλατφόρμες SIEM μπορεί να είναι απαγορευτικά δαπανηρές για ορισμένους οργανισμούς. Μία διαθέσιμη επιλογή είναι η ανοικτού κώδικα πλατφόρμα **Security Onion**. Το Security Onion συνδέει ένα ευρύ φάσμα εργαλείων ασφαλείας —όπως τα **OSSEC**, **Suricata** και **Snort**— σε μία ενιαία πλατφόρμα.

Το Security Onion περιλαμβάνει επίσης λειτουργίες όπως **πίνακες ελέγχου (dashboards)** και εργαλεία για εις βάθος ανάλυση αρχείων καταγραφής (log files). Για παράδειγμα, το παρακάτω στιγμιότυπο δείχνει το επίπεδο λεπτομέρειας που είναι διαθέσιμο:



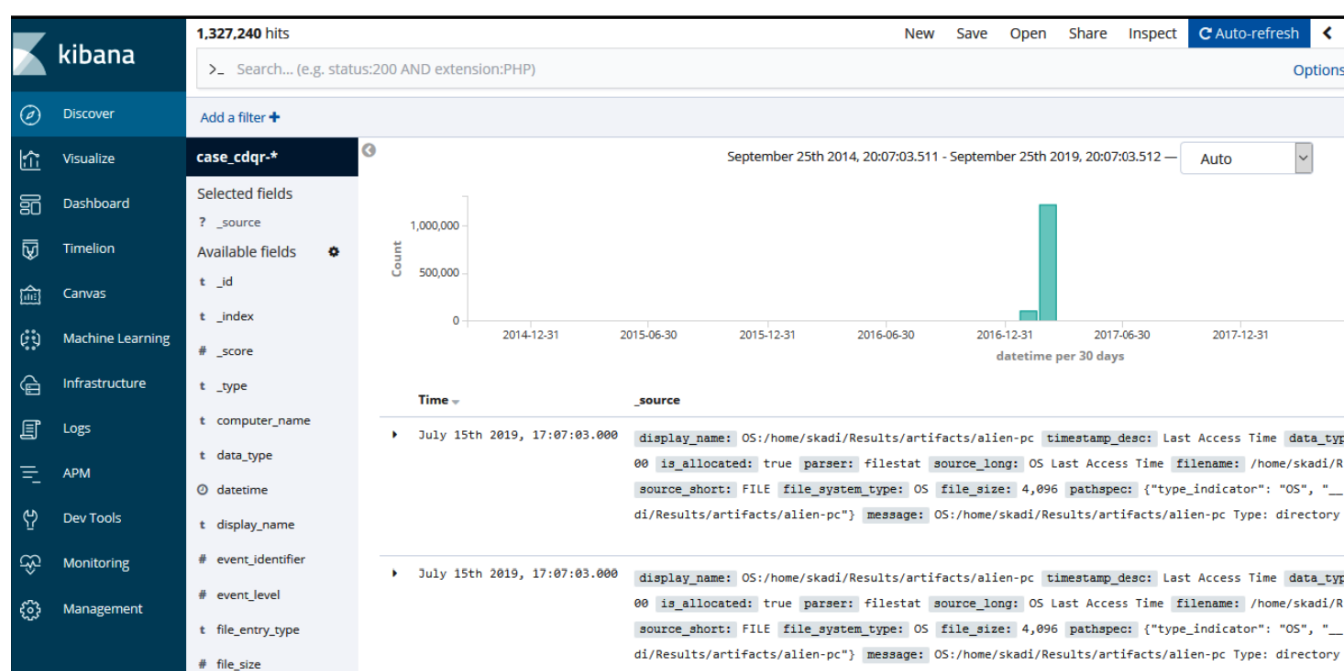
Αν και η εγκατάσταση και ανάπτυξη της πλατφόρμας Security Onion μπορεί να απαιτεί ορισμένους πόρους σε ό,τι αφορά τον χρόνο, αποτελεί μια ισχυρή και χαμηλού κόστους εναλλακτική λύση, προσφέροντας μια επιλογή σε οργανισμούς που δεν μπορούν να αναπτύξουν μια πλήρως εξοπλισμένη λύση SIEM. (Η πλατφόρμα Security Onion και η σχετική τεκμηρίωση είναι διαθέσιμες στη διεύθυνση: <https://securityonion.net>)

10.7. Το Elastic Stack

Μια ακόμη επιλογή ανοιχτού κώδικα για SIEM είναι το **Elastic Stack** (ή αλλιώς **ELK Stack**, όπως είναι ευρέως γνωστό). Το Elastic Stack αποτελεί συνδυασμό τριών εργαλείων σε ένα: τα ανοιχτού κώδικα εργαλεία **Elasticsearch**, **Logstash** και **Kibana** ενοποιούνται για να προσφέρουν στους κυνηγούς απειλών (threat hunters) μια πλατφόρμα ανοιχτού κώδικα που συλλέγει δεδομένα και τα μετατρέπει σε μορφή κατάλληλη για προβολή και ανάλυση μέσω του γραφικού περιβάλλοντος **Kibana**. Αυτό δίνει τη δυνατότητα στους κυνηγούς απειλών να οπτικοποιούν δεδομένα καταγραφών (log data) από πολλαπλά συστήματα ταυτόχρονα.

Το Elastic Stack έχει ενσωματωθεί σε διάφορα εργαλεία ασφάλειας ανοιχτού κώδικα, όπως το προαναφερθέν **Security Onion**. Επίσης, μπορεί να διαμορφωθεί ως αυτόνομη λύση SIEM, με τη χρήση εργαλείων όπως το **Winlogbeat**, το οποίο προωθεί τα Windows event logs στο Elastic Stack.

Το πιο ορατό τμήμα του Elastic Stack είναι η διεπαφή **Kibana**. Η διεπαφή αυτή επιτρέπει την οπτικοποίηση και αναζήτηση δεδομένων, όπως φαίνεται εδώ:

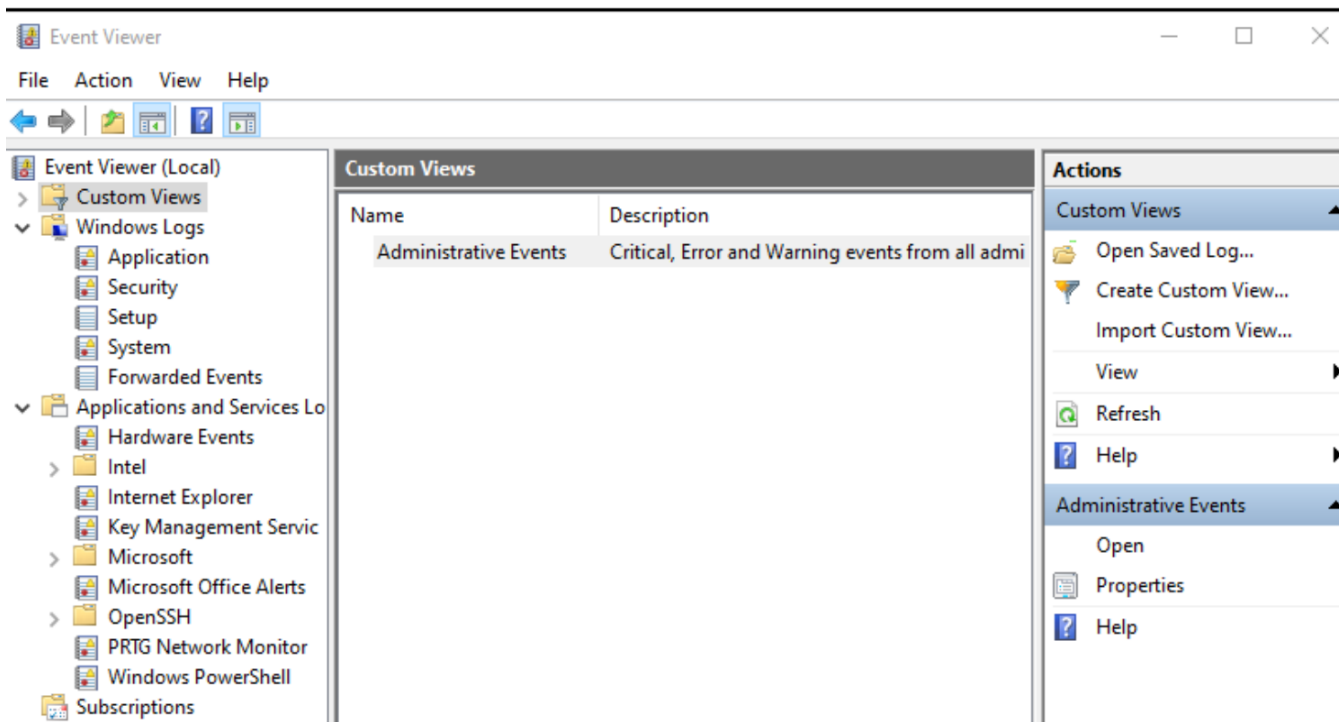


Οι πλατφόρμες SIEM αποτελούν εξαιρετικό μέσο για τους αναλυτές απόκρισης περιστατικών (responders) ώστε να εξετάζουν ένα ευρύ φάσμα αρχείων καταγραφής από μεγάλο αριθμό συστημάτων. Ένα σημείο στο οποίο αυτό γίνεται κρίσιμο είναι η εξέταση των **Windows event logs**. Η επόμενη ενότητα θα εξετάσει τα διάφορα είδη Windows event logs και τις πληροφορίες που μπορούν να παρέχουν στους αναλυτές σχετικά με τη χρήση λογαριασμών και εφαρμογών.

10.8. Κατανόηση των Windows Logs

Το πιο διαδεδομένο λειτουργικό σύστημα τερματικών σημείων (endpoints) που θα χρειαστεί να εξετάσουν οι αναλυτές κατά τη διάρκεια ενός περιστατικού είναι, χωρίς αμφιβολία, το **Windows OS**.

Λόγω του τεράστιου μεριδίου αγοράς που κατέχει η Microsoft, η συντριπτική πλειονότητα των εταιρικών τερματικών συστημάτων είναι **επιτραπέζιοι/φορητοί υπολογιστές, servers ή εικονικά συστήματα Windows**. Ως αποτέλεσμα, είναι κρίσιμο οι αναλυτές να έχουν μια σταθερή κατανόηση του τρόπου αξιοποίησης των **Windows event logs** για ανάλυση περιστατικών.



Τα Windows event logs παρέχουν εκτενή δεδομένα σχετικά με τις ενέργειες του λειτουργικού συστήματος, τις συνδέσεις από άλλα συστήματα και τη χρήση διαπιστευτηρίων, καθώς και τη χρήση του **PowerShell**. Τακτικές αντιπάλων —από την αρχική παραβίαση μέσω κακόβουλου λογισμικού ή άλλων exploits, την πρόσβαση σε διαπιστευτήρια και την κλιμάκωση/πλάγια κίνηση (lateral movement) με χρήση εσωτερικών εργαλείων του Windows OS— καταγράφονται συχνά στα Windows event logs.

Τα συγκεκριμένα logs που καταγράφονται κατά τις δραστηριότητες του λειτουργικού συστήματος εξαρτώνται σε μεγάλο βαθμό από το πώς τα έχει ρυθμίσει ο εκάστοτε οργανισμός. Οι περισσότερες επιχειρήσεις αξιοποιούν τις **ρυθμίσεις Group Policy** για να καθορίσουν ποιες ενέργειες θα καταγράφει το σύστημα, καθώς και τον χώρο αποθήκευσης που θα διατίθεται για τα αρχεία logs. Ανάλογα με τις πρακτικές διαχείρισης των logs, το Windows OS μπορεί να ρυθμιστεί ώστε να καταγράφει:

- τη χρήση PowerShell,
- τη χρήση του **Server Message Block (SMB)**,
- δραστηριότητα εφαρμογών,
- διαχείριση DHCP client,

- συντήρηση του Task Scheduler.

Τις περισσότερες φορές, οι διαμορφώσεις καταγραφής logs γίνονται μέσω του **Windows Group Policy**, το οποίο επιτρέπει στους διαχειριστές να ελέγχουν μια ευρεία γκάμα συστημάτων μέσα από μία πολιτική.

Προβολή διαθέσιμων logs σε τοπικό σύστημα

Για να εντοπίσετε ποια logs είναι διαθέσιμα σε ένα τοπικό σύστημα:

1. Αναζητήστε **Event Viewer** στο πεδίο Αναζήτησης της γραμμής εργασιών των Windows. Κάντε κλικ στο **Event Viewer** και θα ανοίξει το αντίστοιχο παράθυρο.
2. Μέσα από το Event Viewer, ο αναλυτής μπορεί να δει τι καταγράφεται, να αναζητήσει συγκεκριμένες εγγραφές, ή να αποκτήσει άμεση πρόσβαση στα αρχεία για offline ανάλυση στον προεπιλεγμένο φάκελο αποθήκευσης:
C:\Windows\System32\winevt\logs

PC > OS (C:) > Windows > System32 > winevt > Logs			
Name	Date modified	Type	Size
 Security	9/25/2019 3:48 PM	Event Log	20,484 KB
 Microsoft-Windows-Store%4Operational	9/25/2019 3:33 PM	Event Log	19,588 KB
 Microsoft-Windows-Storage-ClassPnP%4Operational	9/23/2019 5:59 PM	Event Log	6,148 KB
 Microsoft-Windows-AppXDeploymentServer%4Operational	9/25/2019 3:14 PM	Event Log	5,124 KB
 System	9/25/2019 3:14 PM	Event Log	4,164 KB
 Microsoft-Windows-SmbClient%4Connectivity	9/25/2019 1:44 PM	Event Log	3,140 KB
 Application	9/25/2019 3:14 PM	Event Log	2,116 KB
 Microsoft-Windows-GroupPolicy%4Operational	9/25/2019 2:47 PM	Event Log	2,116 KB
 Microsoft-Windows-Ntfs%4Operational	9/25/2019 3:43 PM	Event Log	2,116 KB

Αυτό εμφανίζει την ποικιλία των γεγονότων (events) που μπορεί να καταγραφούν.

Κύριες κατηγορίες Windows event logs

Για τους σκοπούς αυτής της ενότητας, η έμφαση δίνεται σε τρεις βασικούς τύπους Windows event logs:

- **Security logs:** Περιλαμβάνουν δεδομένα που σχετίζονται με την ασφάλεια του συστήματος, όπως logons, logoffs, συμμετοχές σε security groups και εκτελέσεις προγραμμάτων.
- **Application logs:** Δημιουργούνται από εφαρμογές, ανάλογα με το ποιες ενέργειες επιλέγουν οι προγραμματιστές να καταγράφονται.

- **System logs:** Συχνά χρησιμοποιούνται για την αντιμετώπιση μη κακόβουλων προβλημάτων. Περιέχουν δεδομένα που δημιουργεί το ίδιο το Windows OS.

Σημαντικά event IDs για τους αναλυτές

Υπάρχουν αρκετές εκατοντάδες τύποι event logs στα Windows. Μερικά εμφανίζονται σπάνια, ενώ άλλα είναι πολύ συχνά. Από τα πιο χρήσιμα για τους αναλυτές είναι:

- **4624 και 4634 — logon και logoff:** Καταγράφουν τη χρήση διαπιστευτηρίων. Το 4624 δείχνει αν το logon έγινε τοπικά ή απομακρυσμένα (χρήσιμο για εντοπισμό lateral movement μέσω SMB).
- **4625 — αποτυχημένο logon:** Λίγες εμφανίσεις μπορεί να είναι τυχαίες, αλλά υπερβολικός αριθμός δηλώνει πιθανή brute-force επίθεση.
- **4672 — ειδικά προνόμια σε νέο logon:** Δείχνει προσπάθεια ανύψωσης δικαιωμάτων σε administrator/root επίπεδο. Χρήσιμο για εντοπισμό privilege escalation.
- **4688 — δημιουργία νέας διεργασίας:** Καταγράφει κάθε φορά που τρέχει ένα πρόγραμμα. Οι αναλυτές μπορούν να εστιάσουν σε ύποπτες διεργασίες όπως PsExec, CMD.EXE, Whami.exe.
- **4768–4773 — Kerberos service:** Συνδέεται με το Kerberoasting attack, που εκμεταλλεύεται τα Kerberos TGTs για κλιμάκωση προνομίων.
- **5140 — πρόσβαση σε network share object:** Δείχνει logon σε δικτυακό κοινόχρηστο πόρο. Ασυνηθιστη δραστηριότητα μπορεί να υποδηλώνει εξαγωγή δεδομένων ή ransomware.
- **7045 — εγκατάσταση νέας υπηρεσίας:** Εμφανίζεται όταν εγκαθίσταται νέα υπηρεσία. Ορισμένα malware τοποθετούν τον εαυτό τους ως υπηρεσία.

Διαχείριση και χρήσιμες πηγές

Παρότι υπάρχουν πάνω από εκατό τύποι event logs, ο οργανισμός πρέπει να αποφασίζει ποιοι θα αξιοποιούνται, σταθμίζοντας το κόστος αποθήκευσης έναντι της χρησιμότητάς τους για την έρευνα.

Χρήσιμοι πόροι:

- **ultimatewindowssecurity.com:** παρέχει βάση δεδομένων με αναζήτηση ανά event ID. Πολύτιμο όταν εμφανίζονται άγνωστα event IDs.
- **MITRE ATT&CK knowledge base:** μπορεί να αναζητηθεί για Windows event log IDs που σχετίζονται με συγκεκριμένες τακτικές/τεχνικές.

Παράδειγμα: Αναλυτής που εξετάζει πιθανή μόλυνση από το **Carbanak malware** μπορεί να δει ότι το Carbanak δημιουργεί λογαριασμό, με event ID **4720**. Ο αναλυτής μπορεί να αναζητήσει το συγκεκριμένο ID και να διαπιστώσει αν έχουν δημιουργηθεί ύποπτοι λογαριασμοί.

Όπως φαίνεται, το **Windows OS** διαθέτει έναν τεράστιο αριθμό event types και IDs. Η επόμενη ενότητα θα παρουσιάσει μεθόδους συλλογής και ανάλυσης αυτών των log files.

Ανάλυση αρχείων καταγραφής των Windows

Η ανάλυση των αρχείων καταγραφής των Windows είναι μια λεπτομερής διαδικασία. Μια πρόκληση που συχνά αντιμετωπίζουν οι αναλυτές είναι ο τεράστιος αριθμός καταγραφών που μπορεί να χρειαστεί να εξετάσουν κατά τη διάρκεια ενός περιστατικού. Στην περίπτωση πολλών συστημάτων, ο αναλυτής μπορεί να βρεθεί αντιμέτωπος με εκατομμύρια ξεχωριστές εγγραφές καταγραφής. Η μείωση αυτών απαιτεί τη χρήση εξειδικευμένων εργαλείων και διαδικασιών, ξεκινώντας με την απόκτηση (acquisition), περνώντας στη διαλογή (triage) και, τελικά, επικεντρώνοντας την ανάλυση στα βασικά αρχεία καταγραφής που σχετίζονται με την έρευνα του περιστατικού.

Απόκτηση (Acquisition)

Υπάρχουν διάφορες μέθοδοι που μπορεί να χρησιμοποιήσει ένας αναλυτής για την απόκτηση των αρχείων καταγραφής των Windows. Ιδανικά, τα αρχεία καταγραφής θα πρέπει να αποστέλλονται σε ένα SIEM, ώστε οι αναλυτές να μπορούν να αναζητούν εγγραφές καταγραφής σε όλο το εταιρικό περιβάλλον. Δυστυχώς, πολλές οργανώσεις αντιμετωπίζουν σημαντικό πρόβλημα με το κόστος αποθήκευσης σε εμπορικές ή ακόμη και ανοιχτού κώδικα πλατφόρμες. Το αποτέλεσμα είναι ότι συχνά πρέπει να κάνουν συμβιβασμό, αφήνοντας τα τοπικά συστήματα να χειρίζονται την αποθήκευση.

Δεδομένου ότι τα περισσότερα από αυτά τα αρχεία βρίσκονται στο τοπικό σύστημα, οι αναλυτές θα χρειαστεί να χρησιμοποιήσουν τεχνικές για τη συλλογή τους. Η πρώτη από αυτές τις τεχνικές είναι απλώς η αντιγραφή των αρχείων καταγραφής από το τοπικό σύστημα σε κάποιο αφαιρούμενο μέσο. Αρκεί να πλοηγηθείτε στον προεπιλεγμένο φάκελο: C:\Windows\System32\winevt\Logs και να αντιγράψετε τα σχετικά αρχεία καταγραφής.

```
echo Log Files
wevtutil epl Setup > \\%COMPUTERNAME%\Logs\%COMPUTERNAME%_Setup.evtx
wevtutil epl System > \\%COMPUTERNAME%\Logs\%COMPUTERNAME%_System.evtx
wevtutil epl Security > \\%COMPUTERNAME%\Logs\%COMPUTERNAME%_Security.evtx
wevtutil epl Application > \\%COMPUTERNAME%\Logs\%COMPUTERNAME%_Application.evtx
```

Αυτή η μέθοδος απαιτεί τοπική πρόσβαση και αρκετή αλληλεπίδραση με το σύστημα. Είναι υποχρέωση του αναλυτή να καταγράψει κάθε ενέργεια που εκτέλεσε στο σύστημα για σωστή αναφορά.

Οι αναλυτές έχουν επίσης την επιλογή να αυτοματοποιήσουν την απόκτηση αρχείων καταγραφής μέσω απλών batch scripts. Η απόκτηση μπορεί να γίνει ταυτόχρονα με άλλες ενέργειες συλλογής αποδεικτικών στοιχείων από ένα τοπικό σύστημα. Για παράδειγμα, μπορεί να εκτελεστεί ένα script

που θα συλλέγει τέσσερις τύπους αρχείων καταγραφής των Windows από ένα τοπικό σύστημα. Τέτοια scripts μπορούν να τρέχουν από συσκευή USB ή μέσω απομακρυσμένων συνεδριών, μειώνοντας έτσι την αλληλεπίδραση με το σύστημα.

Το Κεφάλαιο 5, "Acquiring Host-Based Evidence", εισήγαγε το εργαλείο **CyLR.exe** για την τοπική συλλογή αποδεικτικών στοιχείων. Ένα από τα βασικά σύνολα αποδεικτικών στοιχείων που συλλέγει το CyLR.exe είναι τα αρχεία καταγραφής των Windows. Όπως αναφέρθηκε προηγουμένως, αυτά τα αρχεία μπορούν να αποκτηθούν από το τοπικό σύστημα και να εξαχθούν σε USB. Μια άλλη επιλογή που θα εξεταστεί σε αυτήν την ενότητα είναι η χρήση του CyLR.exe για τη συλλογή αρχείων καταγραφής των Windows και την προώθησή τους στην πλατφόρμα **Skadi** για ανασκόπηση καταγραφών. Η πλατφόρμα Skadi θα εξεταστεί αργότερα, αλλά πρώτα θα εκτελεστεί το CyLR.exe σε ένα σύστημα και η έξοδος θα αποσταλεί στον διακομιστή Skadi.

Βήματα για την απόκτηση αρχείων καταγραφής και αποστολή τους σε Skadi:

1. Ανοίξτε το **Command Prompt των Windows** ως διαχειριστής.
2. Πλοηγηθείτε στον φάκελο όπου βρίσκεται το αρχείο **CyLR.exe**.
3. Εισάγετε την ακόλουθη εντολή στο Command Prompt:

```
C:\Users\JSmith\Desktop>CyLR.exe -s 192.168.207.130:22 -u admin -p password
```

- Το -s είναι η διεύθυνση IP ή το domain name του απομακρυσμένου συστήματος όπου θα σταλεί η έξοδος του CyLR.exe. Σε αυτή την περίπτωση, το συμπιεσμένο αρχείο αποδεικτικών στοιχείων θα σταλεί στο σύστημα 192.168.207.130 μέσω **SFTP**.
 - Το -u είναι το όνομα χρήστη για την πρόσβαση στο απομακρυσμένο σύστημα.
 - Το -p είναι ο κωδικός πρόσβασης για τον λογαριασμό στο απομακρυσμένο σύστημα.
4. Όπως και με την τοπική απόκτηση, το **CyLR.exe** θα εκτελεστεί και η διαδικασία θα εμφανιστεί στο Command Prompt.

```
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-Security-Adminless%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-Security-Audit-Configuration-Client%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-Security-EnterpriseData-FileRevocationManager%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-Security-LessPrivilegedAppContainer%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-Security-Mitigations%4KernelMode.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-Security-Mitigations%4UserMode.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-Security-Netlogon%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-Security-SPP-UX-GenuineCenter-Logging%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-Security-SPP-UX-Notifications%4ActionCenter.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-Security-UserConsentVerifier%4Audit.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-SecurityMitigationsBroker%4Operational.evtx
```

Αυτή η τεχνική απομακρυσμένης συλλογής μπορεί να πραγματοποιηθεί με οποιοδήποτε διαθέσιμο εργαλείο απομακρυσμένης πρόσβασης. Το κύριο πλεονέκτημα αυτής της μεθόδου είναι η δυνατότητα συλλογής δεδομένων καταγραφής μαζί με άλλα αποδεικτικά στοιχεία που συλλέγει το CyLR.exe και η αυτόματη προώθησή τους σε ένα κεντρικό αποθετήριο. Αυτό το κεντρικό αποθετήριο μπορεί να

είναι η πλατφόρμα Skadi ή απλώς ένας διακομιστής SFTP που έχει ρυθμιστεί να δέχεται αυτά τα δεδομένα.

Ανάλογα με το περιστατικό, μπορεί να υπάρχει σημαντικός όγκος δεδομένων. Μάλιστα, μπορεί να είναι υπερβολικός για να εξεταστεί χειροκίνητα από τον αναλυτή. Σε αυτές τις περιπτώσεις, είναι απαραίτητο να γίνει **διαλογή (triage)** των δεδομένων για να προσδιοριστεί ποιες εγγραφές καταγραφής είναι πιο σημαντικές.

10.9. Διαλογή (Triage)

Όπως συζητήθηκε προηγουμένως, ανάλογα με το περιστατικό, οι ανταποκριτές μπορεί να εξετάζουν πολλαπλά συστήματα Windows. Κάθε ένα από αυτά τα συστήματα μπορεί να περιέχει αρκετές χιλιάδες ή ακόμη και εκατό χιλιάδες εγγραφές στα αρχεία καταγραφής συμβάντων (event logs). Δεν υπάρχει δυνατότητα για έναν ανταποκριτή ή μια ομάδα ανταποκριτών να εξετάσει τόσες πολλές μεμονωμένες εγγραφές. Αυτό αντιστοιχεί στη γνωστή φράση «είναι σαν να ψάχνεις βελόνα σε άχυρα».

Για να αντιμετωπιστούν τα μεγάλα σύνολα δεδομένων που συχνά συναντώνται στην ανάλυση των Windows event logs, οι ανταποκριτές μπορούν να χρησιμοποιήσουν το εργαλείο **DeepBlueCLI**. Αυτό το PowerShell script, που αναπτύχθηκε από τον Eric Conrad, ανιχνεύει ύποπτες εγγραφές στα Windows event logs, όπως η δημιουργία υπηρεσιών, η δημιουργία λογαριασμών, ο μεγάλος αριθμός αποτυχημένων συνδέσεων και η κακόβουλη χρήση PowerShell. Εστιάζοντας σε αυτούς τους πιο κρίσιμους τύπους συμβάντων, οι ανταποκριτές θα μπορούν να αναλύσουν περισσότερα αρχεία καταγραφής και ενδεχομένως να εντοπίσουν ύποπτη δραστηριότητα.

Για να τρέξετε το DeepBlueCLI, ακολουθήστε τα εξής βήματα:

1. Κατεβάστε το PowerShell script από το GitHub: <https://github.com/sans-blue-team/DeepBlueCLI>
2. Ανοίξτε το PowerShell και μεταβείτε στον φάκελο που περιέχει το αρχείο **DeepBlue.ps1**.
3. Εκτελέστε το PowerShell script **DeepBlue.ps1** δείχνοντάς του ένα συγκεκριμένο αρχείο καταγραφής Windows – στην περίπτωση αυτή, το αρχείο καταγραφής ασφαλείας των Windows, όπως φαίνεται παρακάτω.
4. Ενεργοποιήστε το script, αν χρειάζεται, πληκτρολογώντας **R**, όπως φαίνεται.

```
PS C:\Users\IRProactive-WKST\Desktop\DeepBlueCLI-master> .\DeepBlue.ps1 C:\Users\IRProactive-WKST\Desktop\evtx\Security.evtx

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your
computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning
message. Do you want to run C:\Users\IRProactive-WKST\Desktop\DeepBlueCLI-master\DeepBlue.ps1?
[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"): R
```

Αφού εκτελεστεί το script, θα παραχθεί ένα κείμενο εξόδου στο παράθυρο του PowerShell. Σε αυτή την περίπτωση, το DeepBlueCLI εκτελέστηκε σε Windows security event logs από ένα ενδεχομένως παραβιασμένο σύστημα. Η ανασκόπηση της εξόδου υποδεικνύει πιθανά σημάδια ότι το σύστημα έχει δεχθεί επίθεση από έναν επιτιθέμενο, όπως φαίνεται στο παρακάτω στιγμιότυπο οθόνης.

```
Date : 2/15/2017 11:05:20 PM
Log : Security
EventID : 4625
Message : High number of logon failures for one account
Results : Username: War_Machine
          Total logon failures: 2287
Command :
Decoded :

Date : 2/15/2017 11:05:20 PM
Log : Security
EventID : 4625
Message : High number of logon failures for one account
Results : Username: IIS_WPG
          Total logon failures: 2290
Command :
Decoded :

Date : 2/15/2017 11:05:20 PM
Log : Security
EventID : 4625
Message : High number of total logon failures for multiple accounts
Results : Total accounts: 7
          Total logon failures: 10006
```

Από το προηγούμενο στιγμιότυπο οθόνης, υπάρχουν τρεις ενδείξεις πιθανής προσπάθειας brute-force διαπιστευτηρίων:

- Ο χρήστης **War_Machine** είχε συνολικά 2287 αποτυχημένες προσπάθειες σύνδεσης.
- Ο χρήστης **IIS_WPG** είχε συνολικά 2290 αποτυχημένες προσπάθειες σύνδεσης.
- Τέλος, η έξοδος υποδεικνύει ότι συνολικά επτά λογαριασμοί είχαν υψηλό αριθμό αποτυχημένων συνδέσεων.

Αυτά τα δεδομένα επιτρέπουν στους ανταποκριτές να επικεντρωθούν στο **event ID 4625** και στους αντίστοιχους λογαριασμούς, αναζητώντας πιθανά στοιχεία παραβίασης.

Το DeepBlueCLI παρέχει επίσης δεδομένα σχετικά με τη δημιουργία λογαριασμών. Όπως έχει συζητηθεί, το **event ID 4720** υποδεικνύει ότι έχει δημιουργηθεί ένας νέος λογαριασμός στο σύστημα. Για παράδειγμα, αν ο ανταποκριτής έχει ενδείξεις ότι το σύστημα που εξετάζεται έχει μολυνθεί με το Carbanak, μπορεί να δει αν έχουν δημιουργηθεί νέοι λογαριασμοί στο σύστημα.

Από την έξοδο, φαίνονται τρεις νέοι λογαριασμοί που έχουν δημιουργηθεί. Κάθε ένας ακολουθεί πολύ παρόμοια σύμβολα ονοματολογίας. Από εδώ, ο ανταποκριτής μπορεί να ελέγξει με την ομάδα διαχείρισης πρόσβασης ή τον διαχειριστή συστήματος αν αυτά τα ονόματα είναι νόμιμα. Σε περίπτωση που υπάρχει ένδειξη ότι ένα ή περισσότερα από αυτά τα ονόματα δεν είναι νόμιμα, ο

ανταποκριτής διαθέτει πλέον ένα σημείο δεδομένων από το οποίο μπορεί να προχωρήσει σε περαιτέρω αναζητήσεις.

```
Date : 2/22/2017 6:35:08 PM
Log : Security
EventID : 4720
Message : New User Created
Results : Username: MBadegain
          User SID: S-1-5-21-2865824651-146060924-1132756725-1019

Command :
Decoded :

Date : 2/22/2017 6:34:55 PM
Log : Security
EventID : 4720
Message : New User Created
Results : Username: BFernandez
          User SID: S-1-5-21-2865824651-146060924-1132756725-1018

Command :
Decoded :

Date : 2/22/2017 6:34:27 PM
Log : Security
EventID : 4720
Message : New User Created
Results : Username: MMartin
          User SID: S-1-5-21-2865824651-146060924-1132756725-1017
```

Το βασικό μειονέκτημα των εργαλείων Windows event log triage όπως το DeepBlueCLI είναι ότι συχνά επικεντρώνονται στην εύρεση των πιο εμφανών στοιχείων, ή εκείνων των logs που συνήθως υποδεικνύουν κατάχρηση. Κάνουν ευκολότερη την ταξινόμηση ενός μεγαλύτερου συνόλου δεδομένων, αλλά οι ανταποκριτές πρέπει να γνωρίζουν ότι δεν είναι αλάνθαστα και υπάρχει πιθανότητα να παραλειφθεί κάποια εγγραφή ή εγγραφές στο event log. Μόλις ένας ανταποκριτής περιορίσει τις σημαντικές εγγραφές, υπάρχουν αρκετά εργαλεία και τεχνικές που μπορούν να χρησιμοποιηθούν για την περαιτέρω ανάλυση των σημαντικών αρχείων καταγραφής.

10.10. Event Log Explorer

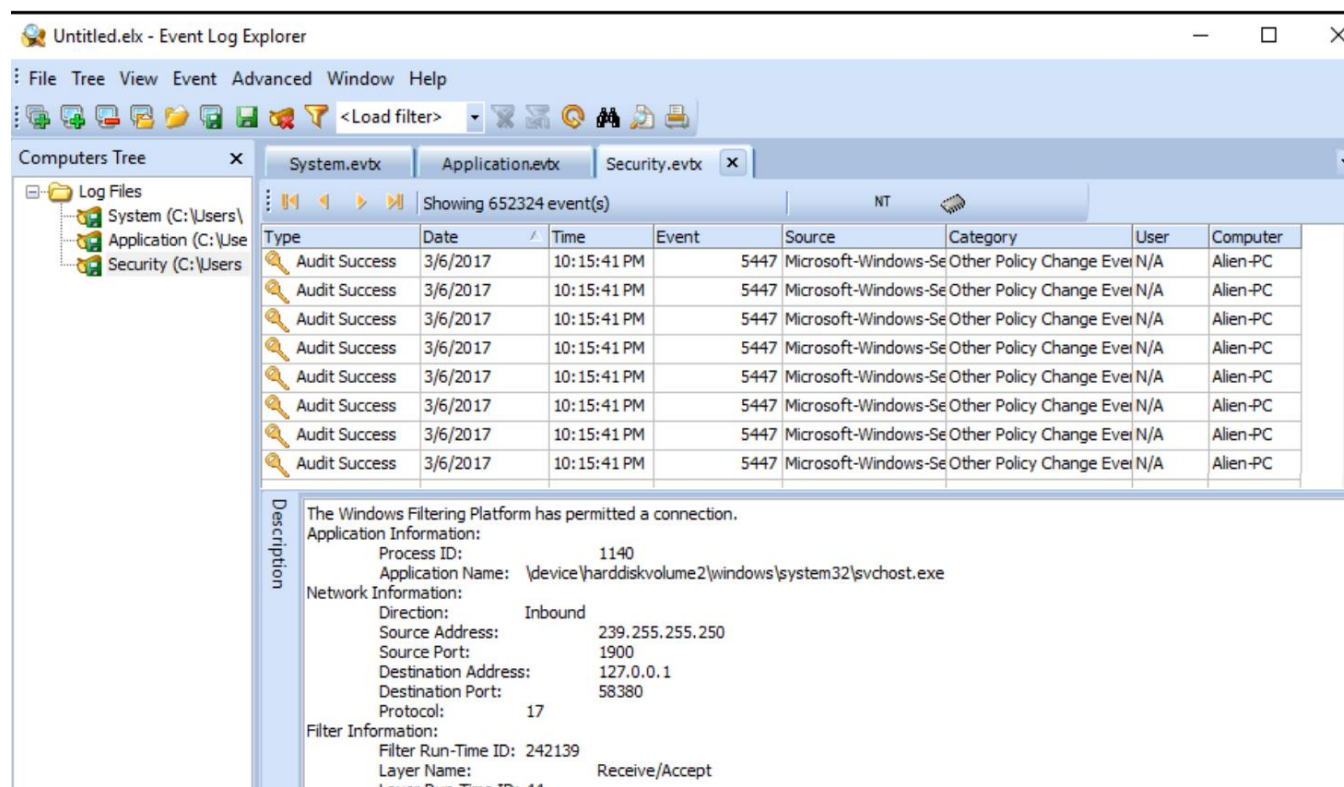
Όπως αναφέρθηκε, η χρήση εργαλείων τριάζ (triage) αποτελεί ένα χρήσιμο πρώτο βήμα, αλλά οποιαδήποτε διερεύνηση περιστατικού όπου υπάρχουν διαθέσιμα αρχεία καταγραφής συμβάντων (event logs) θα απαιτήσει τη χρήση εξειδικευμένων εργαλείων για πιο εις βάθος ανάλυση των δεδομένων που αυτά παρέχουν. Το λειτουργικό σύστημα Windows διαθέτει έναν εγγενή προβολέα αρχείων καταγραφής συμβάντων (Event Log Viewer). Σύμφωνα με την εμπειρία πολλών ερευνητών, ο προβολέας αυτός είναι περισσότερο κατάλληλος για περιορισμένη αντιμετώπιση προβλημάτων παρά για εκτεταμένη ανάλυση των αρχείων καταγραφής.

Υπάρχουν διάφορα εργαλεία, είτε ανοικτού κώδικα είτε εμπορικά, που μπορούν να χρησιμοποιηθούν για την ανάλυση των αρχείων καταγραφής συμβάντων. Τα εργαλεία SIEM παρέχουν ένα από τα καλύτερα είδη εργαλείων, ιδιαίτερα αν έχουν τη δυνατότητα ανάλυσης εκτός σύνδεσης (offline) των αρχείων ή αυτών που έχουν αποκτηθεί μέσω scripts ή άλλων εργαλείων.

Σε αυτό το κεφάλαιο θα συζητηθούν δύο εργαλεία: **Event Log Explorer** και **Skadi**. Το καθένα από αυτά είναι χρήσιμο για ανάλυση αρχείων καταγραφής, αλλά διαθέτει μοναδικά χαρακτηριστικά που το καθιστούν κατάλληλο για διαφορετικές πτυχές της ανάλυσης. Για παράδειγμα, το **Event Log Explorer** επιτρέπει καλύτερο φιλτράρισμα αποτελεσμάτων, μαζί με δυνατότητα αναζήτησης με συμβολοσειρές (string searching). Επίσης, παρέχει τη δυνατότητα συνδυασμού πολλαπλών πηγών δεδομένων. Άλλα εργαλεία, όπως το **Skadi**, επιτρέπουν την απομακρυσμένη απόκτηση αρχείων καταγραφής και συνδυάζουν τις καταχωρήσεις με άλλα δεδομένα, όπως τα στοιχεία του master file table και τις ρυθμίσεις κλειδιών μητρώου (registry keys). Μειονέκτημα του Skadi είναι ο χρόνος που απαιτείται για την εισαγωγή (ingest) και επεξεργασία των δεδομένων για ανασκόπηση. Συνεπώς, η επιλογή του κατάλληλου εργαλείου εξαρτάται από τον ερευνητή και το είδος του περιστατικού που διερευνάται.

Το **Event Log Explorer** είναι ένα εργαλείο ανάλυσης αρχείων καταγραφής συμβάντων (event logs) που διαθέτει περισσότερες δυνατότητες και εύχρηστο περιβάλλον εργασίας (GUI). Διατίθεται ως εμπορικό εργαλείο, και οι δημιουργοί του, **FSPRO Labs**, παρέχουν μια δοκιμαστική περίοδο 30 ημερών για να αξιολογηθεί το εργαλείο. Το εργαλείο μπορεί να κατεβεί από την ιστοσελίδα <https://eventlogxp.com/> και να εγκατασταθεί σε λειτουργικό σύστημα Windows. Για να ξεκινήσετε την ανάλυση εκτός σύνδεσης (offline) των αρχείων καταγραφής συμβάντων, ακολουθήστε τα εξής βήματα:

1. Ανοίξτε το **Event Log Explorer**. Θα εμφανιστεί το παρακάτω παράθυρο:



Το GUI έχει τρεις βασικές περιοχές.

- Το κεντρικό παράθυρο περιέχει τις μεμονωμένες καταχωρήσεις (log entries) που περιλαμβάνονται στο τύπο αρχείου καταγραφής των Windows. Το κάτω παράθυρο περιέχει τις λεπτομέρειες κάθε καταχώρησης. Το αριστερό παράθυρο περιλαμβάνει τους τύπους αρχείων καταγραφής Windows που υπόκεινται σε ανάλυση.
2. Το Event Log Explorer θα εισάγει αυτόματα τα αρχεία καταγραφής του localhost. Για να αφαιρέσετε αυτά τα αρχεία, κάντε δεξί κλικ στο όνομα του υπολογιστή και επιλέξτε **Remove Computer**. Κάντε κλικ στο **YES**. Αυτό θα αφαιρέσει τα υπάρχοντα αρχεία καταγραφής των Windows.
 3. Για να εισάγετε ένα ή περισσότερα αρχεία καταγραφής, κάντε κλικ στο **File | Open Log File | Standard**. Στη συνέχεια, φορτώστε το αρχείο από έναν κατάλογο και κάντε κλικ στο **Open**.
 4. Μόλις φορτωθεί το αρχείο ή τα αρχεία, ο αναλυτής μπορεί να χρησιμοποιήσει το φίλτρο για να επικεντρωθεί σε συγκεκριμένα δεδομένα που περιέχονται στα αρχεία καταγραφής. Για να ανοίξετε το φίλτρο, αναζητήστε το εικονίδιο φίλτρου στη γραμμή εργαλείων.
 5. Θα ανοίξει η οθόνη φίλτρου. Από εδώ, ο αναλυτής μπορεί να φιλτράρει τα αρχεία καταγραφής βάσει διαφόρων χαρακτηριστικών.

Filter

Apply filter to:

☒ Active event log view (File: C:\Users\IRProactive-WKST\Desktop\alien-pc\Security.evbx)

☐ Event log view(s) on your choice

Event types

☒ Information

☒ Warning

☒ Error

☒ Critical

☒ Audit Success

☒ Audit Failure

Source: ☐ Exclude

Category: ☐ Exclude

User: ☐ Exclude

Computer: ☐ Exclude

Event ID(s):

4625 ☐ Exclude

Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19, 100, 250-450! 10, 255)

Text in description:

IIS_WPG ☐ RegExp ☐ Exclude

Filter by description params (for security event logs, e.g. Object\Object Name contains elcx.exe)

New condition Delete condition Clear list

Name	Operator	Value

☐ Date ☐ Time ☐ Separately

From: 7/15/2019 12:00:00 AM To: 7/15/2019 12:00:00 AM ☐ Exclude

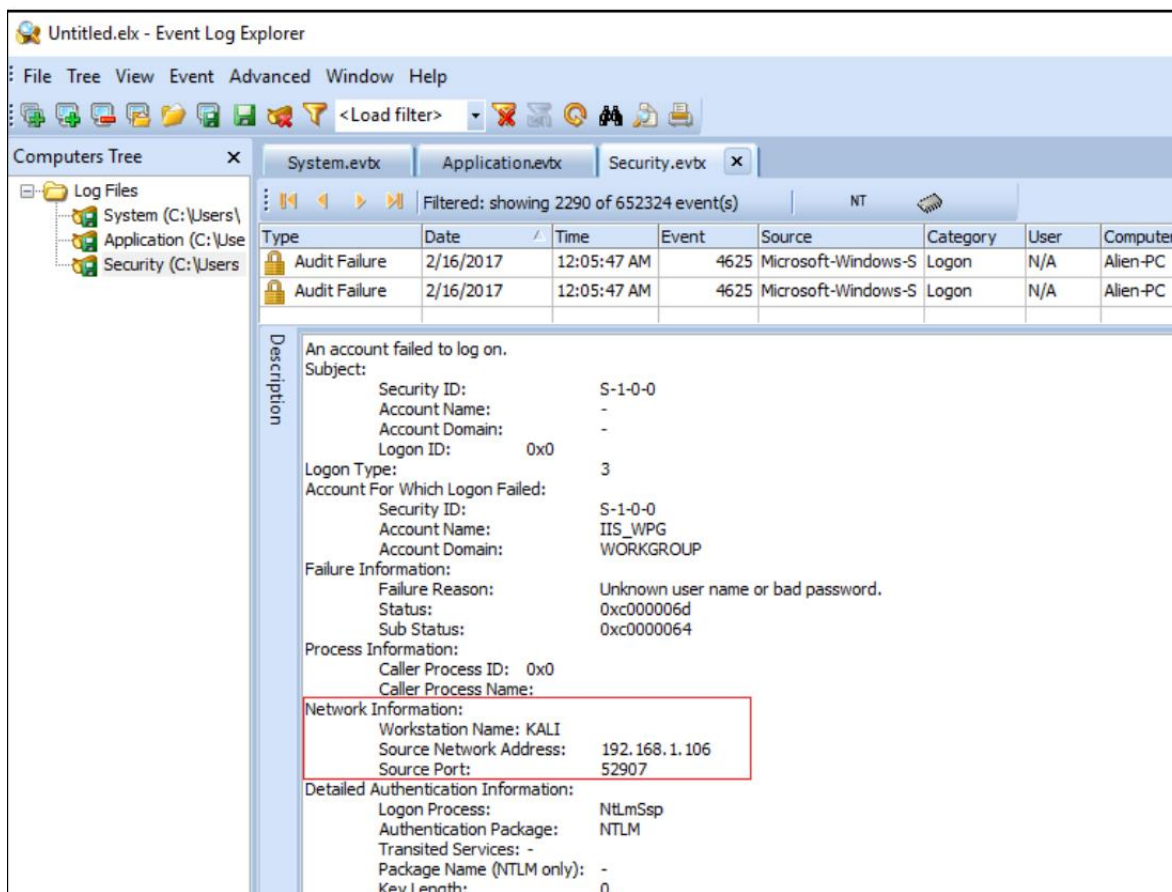
Display event for the last 0 days 0 hours ☐ Exclude

Clear Load... Save... OK Cancel

όπως: τύποι συμβάντων, **event ID**, και αναζήτηση λέξεων-κλειδιών στο κείμενο της καταχώρησης. Στο συγκεκριμένο παράδειγμα, ο αναλυτής εξετάζει τις καταχωρήσεις αποτυχημένων συνδέσεων (failed logins) με **event ID 4625**, που περιλαμβάνουν το όνομα χρήστη **IIS_WPG**, όπως είχε εντοπιστεί

με το script τριάζ **DeepBlueCLI**. Ο αναλυτής εισάγει το event ID ως 4625 και στο πεδίο **Text in description** το όνομα λογαριασμού σε απλό κείμενο, **IIS_WPG**.

6. Το αποτέλεσμα, μετά το πάτημα του **OK**, εμφανίζει τις καταχωρήσεις που ταιριάζουν με τα φίλτρα που εισήχθησαν. Η εξέταση των λεπτομερειών των καταχωρήσεων δείχνει ότι ο υπολογιστής που επιχειρούσε τη χρήση των διαπιστευτηρίων ονομαζόταν **Kali**, με διεύθυνση IP **192.168.1.106**.



Σε αυτό το σύντομο σενάριο, ο αναλυτής μπόρεσε να εξαγάγει δύο πολύ σημαντικά δεδομένα από τα Windows security logs: το hostname (**Kali**, μια γνωστή πλατφόρμα penetration testing) και τη διεύθυνση IP του συστήματος που εκτελούσε την επίθεση. Με αυτές τις πληροφορίες, μπορεί τώρα να εξετάσει άλλες πηγές αρχείων καταγραφής για την ίδια IP και hostname, προκειμένου να εντοπίσει πρόσθετες πληροφορίες σχετικά με τη δραστηριότητα του συστήματος.

Το Event Log Explorer διαθέτει πολλές λειτουργίες που δεν μπορούν να καλυφθούν πλήρως σε αυτόν τον τόμο. Μερικά από τα υπόλοιπα χαρακτηριστικά περιλαμβάνουν:

- Δημιουργία προσαρμοσμένων προβολών (custom views).
- Φιλτράρισμα σε συγκεκριμένα σημεία δεδομένων (data points).
- Αναζήτηση κειμένου μέσα σε καταχωρήσεις σε πολλαπλά αρχεία καταγραφής.

Παρά αυτές τις δυνατότητες, υπάρχουν κάποιες μικρές περιορισμοί. Πρώτον, οι αναλυτές πρέπει να συγκεντρώσουν τα αρχεία καταγραφής στο σύστημα για ανάλυση και να τα φορτώσουν χειροκίνητα. Δεύτερον, ανάλογα με το μέγεθος των αρχείων, μπορεί να εμφανιστούν προβλήματα απόδοσης, όπως «πάγωμα» της εφαρμογής. Οι αναλυτές πρέπει να βεβαιωθούν ότι δεν υπερφορτώνουν το εργαλείο.

10.11. Ανάλυση καταγραφών με το Skadi

Τα περιστατικά συχνά αφορούν πολλαπλά συστήματα μέσα σε ένα εταιρικό δίκτυο. Η συσχέτιση αυτής της δραστηριότητας είναι συχνά πολύ δύσκολη χωρίς ανάλυση των καταγραφών συμβάντων από πολλαπλά συστήματα. Εδώ είναι που οι προαναφερθέντες μηχανισμοί SIEM είναι ιδιαίτερα χρήσιμοι. Μια άλλη επιλογή, εάν το SIEM δεν έχει προρυθμιστεί για τη συλλογή και ανάλυση καταγραφών συμβάντων, είναι η πλατφόρμα Skadi. Αυτή η πλατφόρμα ανοιχτού κώδικα, διαθέσιμη στο GitHub στη διεύθυνση <https://github.com/orlikoski/Skadi>, αποτελείται από μια ομάδα εφαρμογών και εργαλεία ψηφιακής εγκληματολογίας που εγκαθίστανται σε έναν διακομιστή με βάση το Ubuntu 16.04 LTS.

Το κύριο εργαλείο στο οποίο επικεντρώνεται αυτό το κεφάλαιο είναι το **Elastic Stack**, το οποίο περιλαμβάνεται ως μέρος της πλατφόρμας Skadi. Ένα άλλο σημαντικό χαρακτηριστικό που προσφέρει το Skadi είναι η δυνατότητα εισαγωγής καταγραφών και άλλων εγκληματολογικών δεδομένων που αποκτώνται μέσω του **CyLR.exe**. Όπως συζητήθηκε προηγουμένως, το CyLR.exe μπορεί να ρυθμιστεί ώστε να στέλνει την έξοδό του μέσω **SFTP** σε έναν απομακρυσμένο διακομιστή. Το Skadi συνδυάζει ένα επιπλέον εργαλείο με το CyLR.exe για να δημιουργήσει ένα σύνολο δεδομένων που μπορεί να εισαχθεί από το Elastic Stack στο Skadi. Αυτή η δυνατότητα επιτρέπει στους αναλυτές να εκτελέσουν το CyLR.exe σε πολλά διαφορετικά συστήματα και να στείλουν απευθείας τα δεδομένα στο Skadi, όπου μπορούν να επεξεργαστούν, να ευρετηριαστούν, να αναζητηθούν και να συσχετιστούν.

Για παράδειγμα, μια αρχική έρευνα ενός περιστατικού έχει εντοπίσει ένα σύστημα με το όνομα **alien-pc** που φαίνεται να έχει παραβιαστεί. Οι αναλυτές αναπτύσσουν το CyLR.exe στο σύστημα και εκτελούν την ακόλουθη εντολή:

```
C:\Users\alien-pc\Desktop>CyLR.exe -s 192.168.49.132:22 -u skadi -p skadi
```

Στην παραπάνω εντολή, το **-s** είναι η διεύθυνση IP του διακομιστή Skadi. Το προεπιλεγμένο όνομα χρήστη και ο κωδικός για τον διακομιστή Skadi είναι **skadi**. Αφού ολοκληρωθεί το CyLR.exe, ο αναλυτής συνδέεται στην κονσόλα του Skadi. Από εκεί, εκτελείται το εργαλείο **CDQR** (συντομογραφία του Cold Disk Quick Response), για να μετατρέψει τα αποκτηθέντα δεδομένα σε μορφή που μπορεί να εισαχθεί από το Elasticsearch. Η ακόλουθη εντολή ξεκινά την επεξεργασία με το CDQR:

```
skadi@skadi:~$cdqr in:alien-pc.zip out:Results -z -max_cpu
```

```
skadi@skadi:~$ cdqr in:alien-pc.zip out:Results -z --max_cpu
docker run -v /etc/hosts:/etc/hosts:ro --network host -v /home/skadi/alien-pc.zip:/home/skadi/alien-pc.zip -v /home/skadi/Results:/home/skadi/Results aorlikoski/cdqr:4.4.0 -y /home/skadi/alien-pc.zip /home/skadi/Results -z --max_cpu
```

Το CDQR δημιουργεί ένα αρχείο με όνομα alien-pc.plaso στον φάκελο Results. Τα αποτελέσματα του CyLR.exe δεν έχουν ακόμη μετατραπεί σε μορφή για εισαγωγή στο Elasticsearch. Το CDQR χρησιμοποιείται ξανά στο επόμενο βήμα με την εντολή:

```
skadi@skadi:~$ cdqr in:Results/alien-pc.plaso -plaso_db -es_kb winevt
```

```
skadi@skadi:~$ cdqr in:Results/alien-pc.plaso --plaso_db --es_kb winevt
docker run -v /etc/hosts:/etc/hosts:ro --network host -v /home/skadi/Results/alien-pc.plaso:/home/skadi/Results/alien-pc.plaso aorlikoski/cdqr:4.4.0 -y /home/skadi/Results/alien-pc.plaso --plaso_db --es_kb winevt
CDQR Version: 4.4
Plaso Version: 20190131
WARNING!! Known compatible version of Plaso NOT detected. Attempting to use default parser list. Try using the --no_dependencies_check if Plaso dependancies are the issue.
Using parser: win
Number of cpu cores to use: 1
Destination Folder: Results
Source data: /home/skadi/Results/alien-pc.plaso
Log File: Results/alien-pc.plaso.log
Database File: Results//home/skadi/Results/alien-pc.plaso

Total start time was: 2019-07-16 01:51:32.335461
WARNING: File must be plaso database file otherwise it will not work. Example: artifact.plaso (from CDQR)

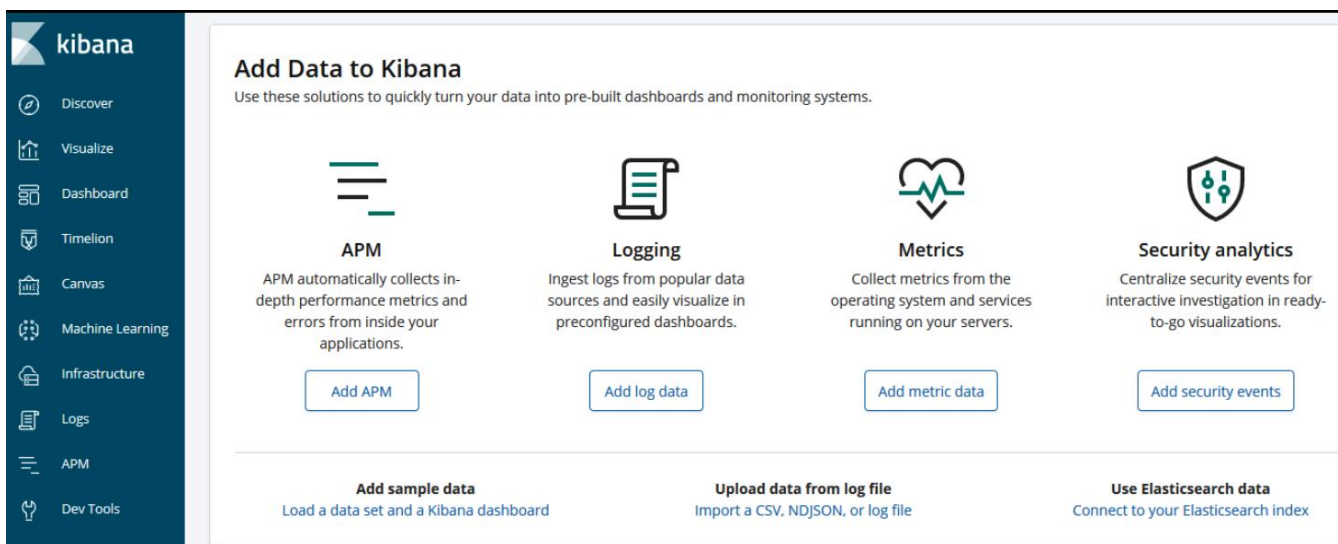
Process to export to ElasticSearch started
Exporting results in Kibana format to the ElasticSearch server
"psort.py" "-o" "elastic" "--status_view" "linear" "--index_name" "case_cdqr-winevt" "--server" "127.0.0.1" "--port" "9200" "/home/skadi/Results/alien-pc.plaso"
All entries have been inserted into database with case: case_cdqr-winevt

Process to export to ElasticSearch completed
ElasticSearch export process duration was: 0:13:03.303455
```

Με την ολοκλήρωση αυτής της διαδικασίας, το αρχείο CyLR.exe, που είχε μετατραπεί σε .plaso, έχει επεξεργαστεί και μεταφερθεί στο Elasticsearch μέρος του Elastic Stack.

Αφού ολοκληρωθεί η διαδικασία, τα αποτελέσματα μπορούν να προβληθούν στο GUI του **Kibana** ως εξής:

1. Μεταβείτε στη διεύθυνση IP του διακομιστή Skadi. Θα εμφανιστεί το παρακάτω portal.
2. Κάντε κλικ στο **Kibana**, και εμφανίζεται η αντίστοιχη οθόνη.
3. Από εδώ, κάντε κλικ στο **Discover**.



Add Data to Kibana
Use these solutions to quickly turn your data into pre-built dashboards and monitoring systems.

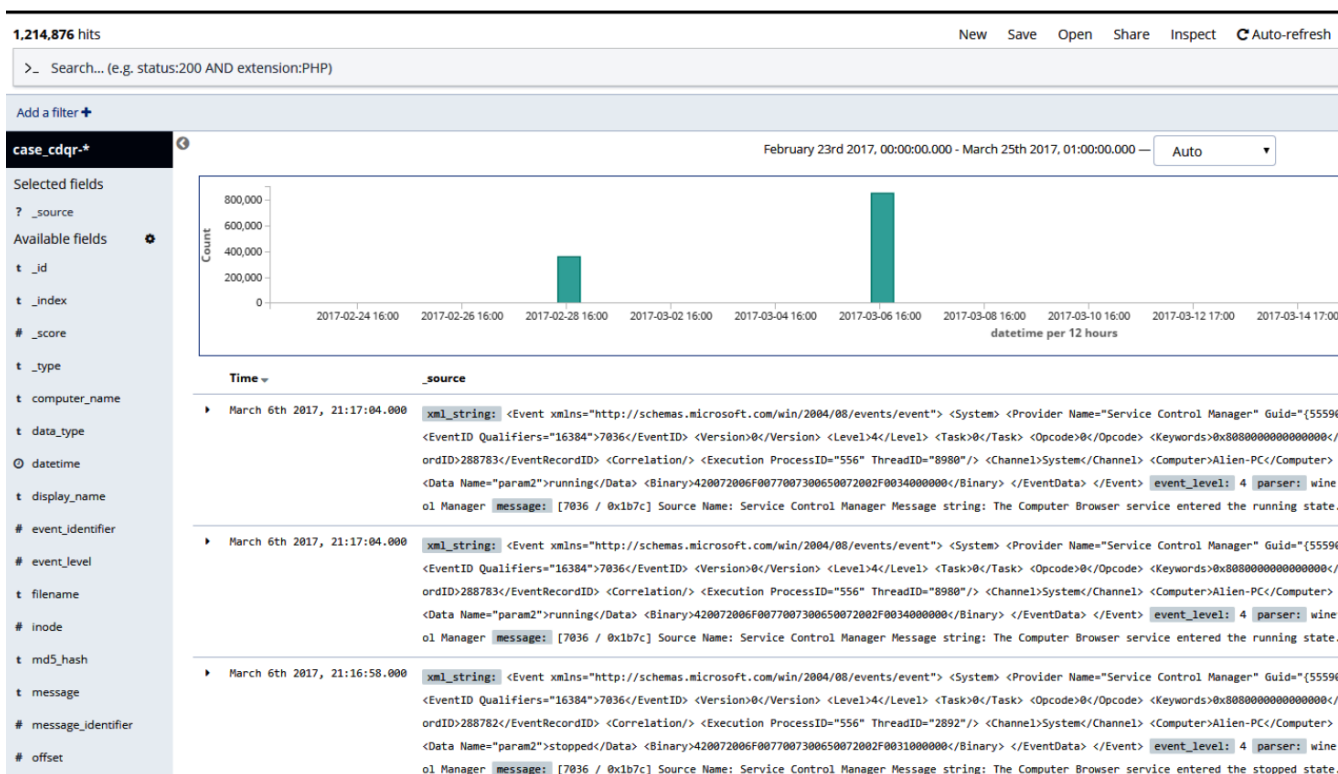
- APM**: APM automatically collects in-depth performance metrics and errors from inside your applications. [Add APM](#)
- Logging**: Ingest logs from popular data sources and easily visualize in preconfigured dashboards. [Add log data](#)
- Metrics**: Collect metrics from the operating system and services running on your servers. [Add metric data](#)
- Security analytics**: Centralize security events for interactive investigation in ready-to-go visualizations. [Add security events](#)

Add sample data: Load a data set and a Kibana dashboard

Upload data from log file: Import a CSV, NDJSON, or log file

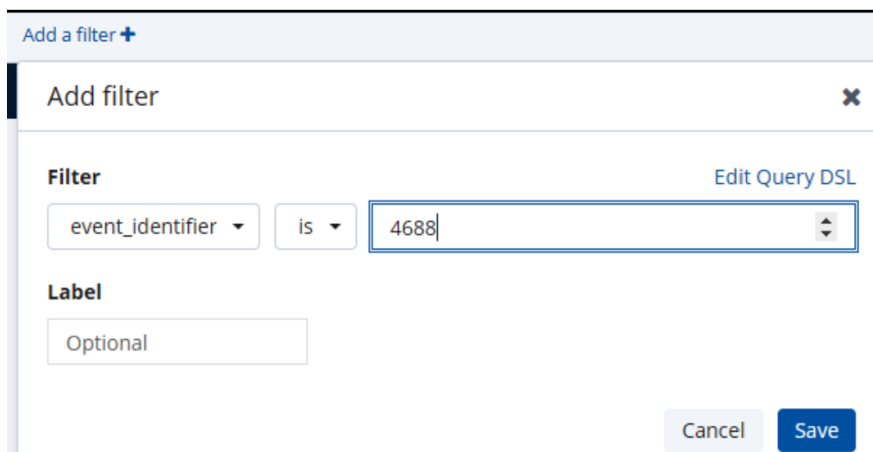
Use Elasticsearch data: Connect to your Elasticsearch index

4. Στο επάνω δεξί μέρος, ορίστε το χρονικό διάστημα που σας ενδιαφέρει. Το Kibana από προεπιλογή δείχνει τα τελευταία 15 λεπτά. Για εκτός σύνδεσης δεδομένα, ορίστε το κατάλληλο χρονικό διάστημα ή επιλέξτε 5 χρόνια.

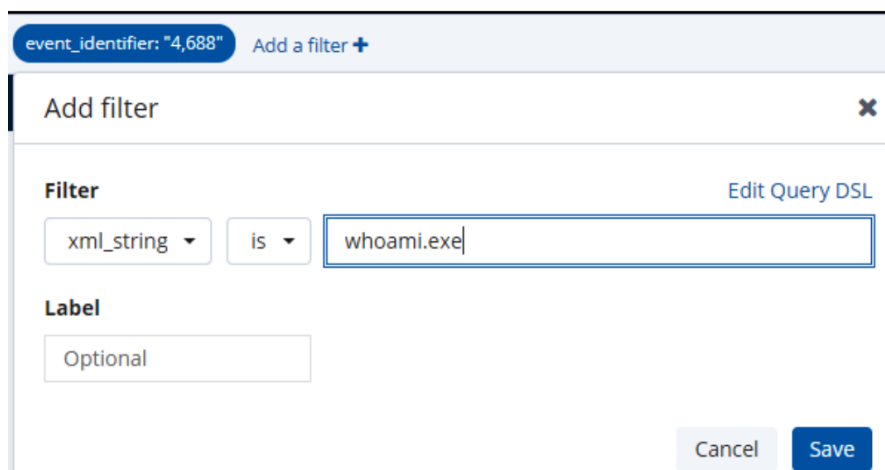


5. Το Kibana είναι πλούσιο σε λειτουργίες και παρέχει πολλές επιλογές για την ανάλυση δεδομένων, όπως προσαρμοσμένα ερωτήματα, αναζήτηση με Event IDs, λέξεις-κλειδιά και XML strings. Σε αυτό το παράδειγμα, ο αναλυτής επικεντρώνεται στο **Event ID 4688**, που υποδεικνύει την εκτέλεση νέας διαδικασίας για τον εντοπισμό πιθανώς κακόβουλου κώδικα ή

άλλης συμπεριφοράς. Η δυνατότητα **Add a filter** στο αριστερό πλαίσιο επιτρέπει στους αναλυτές να φιλτράρουν συγκεκριμένα δεδομένα.



6. Μόλις οριστεί το φίλτρο στο Event ID 4688, ο αναλυτής κάνει κλικ στο **Save** και στη συνέχεια ανανεώνει το Kibana με το κουμπί **Refresh** στην επάνω δεξιά γωνία. Το φίλτρο περιορίζει τα αποτελέσματα από περίπου 1,3 εκατομμύρια σε 784.
7. Στη συνέχεια, ο αναλυτής πραγματοποιεί μια προκαταρκτική αναζήτηση και εντοπίζει το εκτελέσιμο **whoami.exe**. Δεν πρόκειται για κακόβουλο αρχείο, αλλά είναι ύποπτο, καθώς μπορεί να υποδεικνύει ότι ένας αντίπαλος έχει παραβιάσει το σύστημα και προσπάθησε να διαπιστώσει το όνομα του συστήματος χρησιμοποιώντας το Windows **whoami.exe**. Το φίλτρο μπορεί να ενισχυθεί περαιτέρω προσθέτοντας αυτή τη λέξη-κλειδί.



8. Το επιπλέον φίλτρο παράγει μια καταγραφή που μπορεί να αναλυθεί από τον αναλυτή.
9. Από εδώ, ο αναλυτής μπορεί να προσδιορίσει την ημερομηνία, την ώρα και τον λογαριασμό που εκτέλεσε την εντολή. Υπάρχει πιθανώς νόμιμος λόγος για έναν διαχειριστή να εκτελέσει την εντολή στις καθημερινές του δραστηριότητες, αλλά είναι πιθανό να αποτελεί μέρος ευρύτερης παραβίασης και ο αναλυτής πρέπει να επαληθεύσει τη χρήση αυτού του εργαλείου.

```

xml_string  🔍 📄 * <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  <System>
    <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" />
    <EventID>4688</EventID>
    <Version>1</Version>
    <Level>0</Level>
    <Task>13312</Task>
    <Opcode>0</Opcode>
    <Keywords>0x8020000000000000</Keywords>
    <TimeCreated SystemTime="2017-03-07T05:11:01.568600000Z" />
    <EventRecordID>9505938</EventRecordID>
    <Correlation/>
    <Execution ProcessID="4" ThreadID="68" />
    <Channel>Security</Channel>
    <Computer>Alien-PC</Computer>
    <Security/>
  </System>
  <EventData>
    <Data Name="SubjectUserSid">S-1-5-21-2865824651-146060924-1132756725-500</Data>
    <Data Name="SubjectUserName">Administrator</Data>
    <Data Name="SubjectDomainName">Alien-PC</Data>
    <Data Name="SubjectLogonId">0x00000000162e98c</Data>
    <Data Name="NewProcessId">0x000000000001a68</Data>
    <Data Name="NewProcessName">C:\Windows\System32\whoami.exe</Data>
    <Data Name="TokenElevationType">%1936</Data>
    <Data Name="ProcessId">0x000000000001a0c</Data>
    <Data Name="CommandLine" />
  </EventData>
</Event>

```

10. Ο συνδυασμός **CyLR.exe** και **Skadi** δίνει στους αναλυτές τη δυνατότητα απομακρυσμένης πρόσβασης σε αρχεία καταγραφών και αυτοματοποιημένης εισαγωγής τους σε μια πλατφόρμα που επιτρέπει πιο λεπτομερή ανάλυση. Το Skadi μπορεί να εγκατασταθεί εύκολα, ακόμη και ως εικονική μηχανή. Οι αναλυτές μπορούν να προωθήσουν όλα τα απαραίτητα αρχεία καταγραφής και να συσχετίσουν δραστηριότητα σε πολλαπλά συστήματα σε σύντομο χρόνο. Ο συνδυασμός αυτός είναι ισχυρός και χαμηλού κόστους.

Ο συνδυασμός **Skadi** και **CyLR.exe** παρέχει τη δυνατότητα απόκτησης και ανάλυσης αρχείων καταγραφών από πολλά συστήματα που εμπλέκονται στο περιστατικό. Η δυνατότητα εστίασης σε συγκεκριμένα Event IDs ή λέξεις-κλειδιά καθιστά το Skadi ένα ισχυρό εργαλείο για την ανίχνευση πρόσθετων αποδεικτικών στοιχείων σε μια διερεύνηση περιστατικού.

Στην ουσία της ανάλυσης αρχείων καταγραφής (logs) βρίσκεται η υπόθεση ότι οι ενέργειες ενός επιτιθέμενου αφήνουν πίσω τους ίχνη. Όπως και στον φυσικό κόσμο, η ικανότητα των αναλυτών να εντοπίζουν αυτά τα ίχνη εξαρτάται από τα εργαλεία και τις τεχνικές που χρησιμοποιούν. Το κεφάλαιο αυτό ανέλυσε τα βασικά στοιχεία των αρχείων καταγραφής και της διαχείρισής τους, παρουσίασε εργαλεία όπως τα SIEM για τη συγκέντρωση και εξέταση των logs, και τέλος, εστίασε στα εργαλεία και τις τεχνικές για την ανάλυση των πιο διαδεδομένων logs που προέρχονται από το λειτουργικό σύστημα Windows. Το κεφάλαιο αυτό μόλις αγγίζει την επιφάνεια της σημασίας που έχουν τα αρχεία καταγραφής σε μια έρευνα περιστατικού.

11

Σύνταξη της Έκθεσης Περιστατικού

Μια ομάδα αντίδρασης σε περιστατικά λειτουργεί με πολύ παρόμοιο τρόπο με έναν πυροσβεστικό σταθμό. Και οι δύο ομάδες αφιερώνουν χρόνο στην προετοιμασία τους μέσω εκπαίδευσης στις αντίστοιχες τεχνικές, εργαλεία και πρακτικές τους, και μπορούν να ανταποκριθούν σε ένα περιστατικό ή πυρκαγιά άμεσα. Κατά την ανταπόκρισή τους σε μια πυρκαγιά, οι πυροσβέστες κρατούν σημειώσεις και καταγράφουν τις ενέργειές τους, εξασφαλίζοντας ότι οι κρίσιμες αποφάσεις τεκμηριώνονται και οι ατομικές συνεισφορές σημειώνονται. Μόλις η πυρκαγιά τεθεί υπό έλεγχο, εξετάζουν τα συντρίμια για να καθορίσουν τα αίτια και την προέλευση της πυρκαγιάς. Αφού προετοιμαστεί η κατάλληλη τεκμηρίωση, ο πυροσβεστικός σταθμός διεξάγει μια ανασκόπηση μετά την ενέργεια (after-action review) προκειμένου να αξιολογήσει την απόδοσή του και να βρει τρόπους βελτίωσης. Άλλες αναφορές επιτρέπουν στους πυροσβέστες και στους ειδικούς ασφαλείας να ενημερώνουν τους κανονισμούς κατασκευής και να βελτιώνουν την ανθεκτικότητα των κτιρίων σε περίπτωση πυρκαγιάς.

Οι ομάδες αντίδρασης σε περιστατικά χρησιμοποιούν παρόμοια ροή εργασίας. Κατά τη διάρκεια ενός περιστατικού, κρατούνται σημειώσεις και καταγράφονται οι ενέργειες. Τα στοιχεία αποδεικτικά στοιχεία συλλέγονται από τα συστήματα και διατηρούνται με τρόπο που σέβεται τις διαδικασίες εγκληματολογίας. Διενεργείται ανάλυση της ρίζας του προβλήματος (root cause analysis) χρησιμοποιώντας τις σημειώσεις, τις παρατηρήσεις και τα στοιχεία που συλλέχθηκαν κατά το περιστατικό. Αυτή η ανάλυση χρησιμοποιείται από το προσωπικό πληροφορικής για να κλείσει τυχόν ευπάθειες και να ενισχύσει περαιτέρω τα συστήματα. Τέλος, η ομάδα διεξάγει τη δική της ανασκόπηση μετά την ενέργεια, όπου περιγράφεται και αξιολογείται η σειρά των γεγονότων ώστε να βελτιωθούν οι διαδικασίες, τα εργαλεία και οι τεχνικές της ομάδας, καθώς και να γίνουν τυχόν διορθώσεις στο σχέδιο αντίδρασης περιστατικού.

Για να μεγιστοποιηθούν τα οφέλη της ανάλυσης της ρίζας του προβλήματος και της ανασκόπησης μετά την ενέργεια, οι απαντητές σε περιστατικά πρέπει να διασφαλίσουν ότι όλες οι ενέργειές τους καταγράφονται με τον σωστό τρόπο. Επιπλέον, απαιτείται να προετοιμάσουν αρκετά έγγραφα τα οποία οι ανώτεροι υπεύθυνοι και οι λήπτες αποφάσεων θα χρησιμοποιήσουν όταν εξετάζουν την μελλοντική κατάσταση της υποδομής IT. Για να προετοιμαστούν καλύτερα οι απαντητές στη σύνταξη της απαραίτητης τεκμηρίωσης, θα καλυφθούν τα εξής θέματα:

- **Επισκόπηση τεκμηρίωσης:** Αυτή η επισκόπηση καλύπτει τα διάφορα στοιχεία προετοιμασίας αναφορών, συμπεριλαμβανομένων των δεδομένων που πρέπει να καταγραφούν, του κοινού

που θα εξετάσει τις αναφορές και των πηγών από τις οποίες μπορούν να αντλήσουν πληροφορίες οι απαντητές.

- **Παρακολούθηση περιστατικών:** Για οργανισμούς που πραγματοποιούν τακτική ανταπόκριση σε περιστατικά, το λογισμικό παρακολούθησης είναι χρήσιμο για την καταγραφή ενεργειών και σχετικών δεδομένων. Στην περίπτωση αυτή, θα εξεταστεί το σύστημα παρακολούθησης Fast Incident Response (FIR).
- **Γραπτές αναφορές:** Ανάλογα με τη σοβαρότητα ή την πολυπλοκότητα ενός περιστατικού, θα συντάσσεται γραπτή αναφορά. Με τη δημιουργία μιας καλά γραμμένης και προσεκτικής αναφοράς προς τους ανώτερους διευθυντές και εξωτερικούς ενδιαφερόμενους, οι απαντητές σε περιστατικά παρέχουν στους κύριους λήπτες αποφάσεων μια ακριβή εικόνα των γεγονότων και των μέτρων πρόληψης στο μέλλον.

11.1. Επισκόπηση τεκμηρίωσης

Η τεκμηρίωση που σχετίζεται με ένα περιστατικό μπορεί να έχει πολλές μορφές. Το μέγεθος οποιασδήποτε τεκμηρίωσης συχνά καθορίζεται από τον τύπο του περιστατικού. Απλά περιστατικά, που απαιτούν πολύ λίγο χρόνο για διερεύνηση και έχουν περιορισμένο αντίκτυπο, μπορεί να τεκμηριώνονται ανεπίσημα σε ένα υπάρχον σύστημα ticketing. Ωστόσο, σε πιο σύνθετες έρευνες περιστατικών, όπως μια παραβίαση δεδομένων που οδήγησε στη διαρροή εμπιστευτικών πληροφοριών (π.χ. ιατρικά αρχεία ή πληροφορίες πιστωτικών καρτών), ενδέχεται να απαιτούνται εκτενείς γραπτές αναφορές και υποστηρικτικά στοιχεία.

Τι πρέπει να τεκμηριώνεται

Κατά την τεκμηρίωση ενός περιστατικού, δεν είναι πολύ δύσκολο να προσδιοριστεί τι πρέπει να καταγραφεί. Η χρήση των πέντε W (Who, What, Where, When, Why – Ποιος, Τι, Πού, Πότε, Γιατί) και μερικές φορές του H (How – Πώς) αποτελεί εξαιρετική βάση για τον προσδιορισμό των στοιχείων που πρέπει να τεκμηριωθούν. Ένα ακόμα σημαντικό ρητό όταν συζητάμε την τεκμηρίωση, ιδιαίτερα σε νομικά πλαίσια ασφάλειας, είναι: *"Αν δεν το έγραψες, δεν συνέβη"* (If you didn't write it down, it didn't happen). Αυτή η αρχή τονίζει ότι η σωστή τεκμηρίωση πρέπει να περιλαμβάνει όσο το δυνατόν περισσότερες λεπτομέρειες. Οι αναλυτές μπορεί να εμπλακούν σε περιστατικά που καταλήγουν σε αστικές διαδικασίες, και καθώς η δικαιοσύνη προχωρά αργά, ένας αναλυτής μπορεί να κληθεί ως μάρτυρας ακόμη και 18 μήνες μετά, κατά τους οποίους μπορεί να έχουν συμβεί άλλα 10 περιστατικά. Η διαθέσιμη λεπτομερής τεκμηρίωση επιτρέπει στους αναλυτές να ανακατασκευάσουν σωστά τα γεγονότα.

Ένα παράδειγμα εφαρμογής των πέντε W και του H είναι η εργασία ψηφιακής εγκληματολογίας, όπως η απόκτηση εικόνας ενός σκληρού δίσκου. Στο Κεφάλαιο 6, **Forensic Imaging**, η σωστή τεκμηρίωση αναφέρθηκε εν μέρει με τη διαδικασία φωτογράφισης του ύποπτου δίσκου. Ακολουθεί ένα πιο λεπτομερές παράδειγμα:

- **Who (Ποιος):** Το πιο εύκολο στοιχείο για καταγραφή. Ποιος συμμετείχε στη διαδικασία; π.χ., ο αναλυτής Jane Smith.
- **When (Πότε):** Καταγραφή ημερομηνίας και ώρας έναρξης και λήξης της διαδικασίας imaging. π.χ., η διαδικασία ξεκίνησε 16 Αυγούστου 2019 στις 21:08 UTC και ολοκληρώθηκε στις 22:15 UTC. Είναι κρίσιμο να χρησιμοποιείται και να αναφέρεται ζώνη ώρας.
- **Where (Πού):** Αναλυτική τοποθεσία, π.χ., γραφείο.
- **What (Τι):** Η ενέργεια που εκτελέστηκε, π.χ., απόκτηση logs μνήμης ή firewall, ή imaging δίσκου.
- **Why (Γιατί):** Η αιτιολόγηση της ενέργειας βοηθά στην κατανόηση του λόγου εκτέλεσής της.
- **How (Πώς):** Περιγραφή του τρόπου εκτέλεσης της ενέργειας. Αν η ομάδα χρησιμοποιεί playbooks ή standard operating procedures, αυτό πρέπει να περιλαμβάνεται, και οποιαδήποτε απόκλιση από τις διαδικασίες πρέπει επίσης να καταγράφεται.

Συνδυάζοντας όλες αυτές τις πληροφορίες, η ακόλουθη υπόδειξη γλώσσας μπορεί να εισαχθεί στην αναφορά:

Στις 16 Αυγούστου 2019, η αναλύτρια Jane Smith έφτασε στο γραφείο 217 του Corporate Office Park που βρίσκεται στην οδό 123 Maple St., Anytown, Η.Π.Α., στο πλαίσιο της διερεύνησης. Κατά την άφιξή της, η Smith ανέλαβε τον έλεγχο του φορητού υπολογιστή Dell, με αριθμό περιουσιακού στοιχείου #AccLT009 και σειριακό αριθμό #7895693-862. Ένα σήμα από το firewall IDS/IPS υποδείκνυε ότι ο φορητός υπολογιστής είχε επικοινωνήσει με γνωστό διακομιστή Command and Control. Ο φορητός υπολογιστής θα αποτυπωνόταν (imaged) σε μια προσπάθεια να διαπιστωθεί αν είχε μολυνθεί από κακόβουλο λογισμικό. Στις 21:08 UTC, η Smith αποτύπωσε τον δίσκο χρησιμοποιώντας την τεχνική ζωντανής αποτύπωσης (live imaging) σύμφωνα με τη Διαδικασία Λειτουργίας IR-002. Η διαδικασία ολοκληρώθηκε στις 22:15 UTC της 16ης Αυγούστου 2019.

Η καταχώρηση αυτή παρέχει επαρκείς λεπτομέρειες για την ανακατασκευή των γεγονότων που συνέβησαν. Σε συνδυασμό με άλλα έγγραφα, όπως φωτογραφίες και την αλυσίδα φύλαξης (chain of custody), η αναλύτρια έχει σαφή εικόνα της διαδικασίας και του αποτελέσματος.

11.2. Τύποι τεκμηρίωσης

Δεν υπάρχει ένα ενιαίο πρότυπο που να καθορίζει τον τρόπο καταγραφής ενός περιστατικού, αλλά υπάρχουν μερικές ξεκάθαρες κατηγορίες. Όπως αναφέρθηκε προηγουμένως, το βάθος της τεκμηρίωσης εξαρτάται συχνά από τον τύπο, την κλίμακα και το εύρος ενός περιστατικού· ωστόσο, γενικά εφαρμόζονται οι ακόλουθες κατηγορίες:

Σύστημα καταγραφής προβλημάτων (trouble ticketing system): Οι περισσότερες επιχειρήσεις διαθέτουν ένα υπάρχον σύστημα καταγραφής εισητηρίων (ticketing system) για την παρακολούθηση

διακοπών συστήματος και άλλων προβλημάτων που εμφανίζονται συνήθως στις σημερινές δικτυακές υποδομές. Αυτά τα συστήματα καταγράφουν μεγάλο όγκο δεδομένων που σχετίζονται με ένα περιστατικό. Μια καταχώρηση συνήθως περιλαμβάνει την ημερομηνία και ώρα έναρξης και λήξης, το αρχικό πρόσωπο που ανέφερε το περιστατικό και τις ενέργειες που πραγματοποιήθηκαν, ενώ παρέχεται και χώρος για σημειώσεις. Το κύριο μειονέκτημα των συστημάτων αυτών είναι ότι αρχικά σχεδιάστηκαν για την υποστήριξη των γενικών λειτουργιών των επιχειρησιακών υποδομών. Ως εκ τούτου, πιο σύνθετα περιστατικά απαιτούν πολύ περισσότερη τεκμηρίωση από ό,τι είναι δυνατόν σε αυτά τα συστήματα. Για το λόγο αυτό, συχνά χρησιμοποιούνται για μικρά περιστατικά, όπως μεμονωμένες μολύνσεις από κακόβουλο λογισμικό ή άλλα μικρά περιστατικά που επιλύονται γρήγορα.

Ορχήστρωση ανταπόκρισης σε περιστατικά (Incident response orchestration): Ορισμένες οργανώσεις έχουν αναγνωρίσει την ανάγκη για μια αφιερωμένη πλατφόρμα ανταπόκρισης σε περιστατικά και έχουν δημιουργήσει εφαρμογές ή άλλου τύπου υποδομές που υποστηρίζουν τις ομάδες ανταπόκρισης. Αυτές οι πλατφόρμες επιτρέπουν στους αναλυτές να εισάγουν δεδομένα, να επισυνάπτουν αρχεία αποδεικτικών στοιχείων, να συνεργάζονται με άλλα μέλη της ομάδας και να αντλούν εξωτερικούς πόρους, όπως ανάλυση κακόβουλου λογισμικού και feeds πληροφοριών απειλών.

Υπάρχουν πολλές από αυτές τις πλατφόρμες διαθέσιμες τόσο εμπορικά όσο και δωρεάν. Το κύριο πλεονέκτημά τους είναι ότι αυτοματοποιούν την καταγραφή πληροφοριών, όπως ημερομηνία, ώρα και ενέργειες του αναλυτή. Ένα ακόμη πλεονέκτημα είναι η δυνατότητα περιορισμού της πρόσβασης σε συγκεκριμένα άτομα. Σε συστήματα εισητηρίων υπάρχει πιθανότητα κάποιο μη εξουσιοδοτημένο άτομο να παρατηρήσει λεπτομέρειες που ο οργανισμός θέλει να κρατήσει εμπιστευτικές. Η ύπαρξη ενός συστήματος ορχήστρωσης παρέχει ένα επίπεδο εμπιστευτικότητας. Ένα άλλο βασικό πλεονέκτημα είναι η δυνατότητα των μελών της ομάδας να βλέπουν ποιες ενέργειες έγιναν και ποιες πληροφορίες αποκτήθηκαν, μειώνοντας τον αριθμό κλήσεων και τις πιθανότητες παρεξηγήσεων.

Γραπτές αναφορές: Ακόμα και με τη χρήση αυτοματοποιημένων πλατφορμών, ορισμένα περιστατικά απαιτούν εκτεταμένη γραπτή αναφορά. Γενικά, αυτές οι αναφορές μπορούν να χωριστούν σε τρεις βασικούς τύπους, οι οποίοι θα επεκταθούν αργότερα σε αυτό το κεφάλαιο:

- **Σύνοψη για τη διοίκηση (Executive summary):** Πρόκειται για μια αναφορά 1–2 σελίδων που αποσκοπεί να περιγράψει τα βασικά σημεία του περιστατικού για τη διοίκηση. Μια σύντομη περίληψη των γεγονότων, η κύρια αιτία, αν μπορεί να προσδιοριστεί, και προτάσεις για αποκατάσταση συχνά αρκούν.
- **Αναφορά περιστατικού (Incident report):** Αναλυτική αναφορά που προορίζεται για διάφορα άτομα μέσα στον οργανισμό. Περιλαμβάνει λεπτομέρειες της έρευνας, ανάλυση της κύριας αιτίας και προτάσεις για την αποτροπή επανάληψης του περιστατικού.
- **Δικαστική αναφορά (Forensic report):** Η πιο λεπτομερής αναφορά, που δημιουργείται όταν διεξάγεται δικαστική εξέταση αρχείων καταγραφής, μνήμης ή εικόνων δίσκων. Αυτές οι

αναφορές μπορεί να είναι πολύ τεχνικές και συχνά περιλαμβάνουν εξόδους εργαλείων και αποσπάσματα στοιχείων, όπως αρχεία καταγραφής.

Η κατανόηση των διαφορετικών κατηγοριών που απαρτίζουν μια αναφορά περιστατικού επιτρέπει στους ανακριτές να οργανώνουν σωστά το υλικό τους. Ακόμα και μικρά περιστατικά δημιουργούν τεκμηρίωση, που μπορεί να γίνει υπερβολική. Σε συνδυασμό με τον μεγάλο αριθμό πηγών δεδομένων, η διαδικασία αναφοράς μπορεί να γίνει χρονοβόρα. Για καλύτερη ροή, οι ανακριτές πρέπει να είναι προετοιμασμένοι να αντιμετωπίσουν τις διάφορες κατηγορίες από την αρχή ενός περιστατικού και να οργανώσουν την τεκμηρίωση αναλόγως.

11.3. Πηγές

Κατά την προετοιμασία αναφορών, υπάρχουν διάφορες πηγές δεδομένων που περιλαμβάνονται στην τεκμηρίωση, είτε το περιστατικό είναι μικρό, απαιτώντας μόνο μια καταχώρηση σε σύστημα εισηγηρίων, είτε πολύπλοκο, όπως παραβίαση δεδομένων που απαιτεί εκτεταμένη αναφορά περιστατικών και δικαστική αναφορά. Κάποιες πηγές περιλαμβάνουν:

- **Προσωπικές παρατηρήσεις:** Οι χρήστες μπορεί να διαθέτουν πληροφορίες που σχετίζονται με την υπόθεση, π.χ., άνοιγμα ενός αρχείου σε email που φαινόταν νόμιμο. Οι αναλυτές μπορεί να παρατηρήσουν συμπεριφορά στο σύστημα και να την καταγράψουν.
- **Εφαρμογές:** Ορισμένες εφαρμογές παράγουν αρχεία καταγραφής ή άλλα δεδομένα που χρειάζεται να συμπεριληφθούν στην αναφορά.
- **Δικτυακές/υπολογιστικές συσκευές:** Πολλά συστήματα σε περιβάλλοντα επιχειρήσεων παρέχουν δυνατότητες εξαγωγής αναφορών που μπορούν να ενσωματωθούν στην αναφορά περιστατικού ή δικαστική αναφορά.
- **Δικαστικά εργαλεία:** Αυτά συχνά διαθέτουν αυτοματοποιημένες λειτουργίες αναφοράς, από απλή περίληψη ενεργειών έως πραγματικές εξόδους, όπως hash αρχείων, που περιλαμβάνονται στη δικαστική αναφορά.

Όποια και αν είναι η πηγή, ένας κανόνας που πρέπει να ακολουθείται είναι να καταγράφεται και να περιλαμβάνεται όσο το δυνατόν περισσότερη πληροφορία στην αναφορά. Είναι προτιμότερο να υπάρχει υπερβολική πληροφορία παρά έλλειψη.

11.4. Κοινό

Ένας τελευταίος παράγοντας που πρέπει να έχετε υπόψη κατά την προετοιμασία της τεκμηρίωσης είναι ποιος θα διαβάσει μια αναφορά περιστατικού σε σχέση με μια λεπτομερή εγκληματολογική (forensic) αναφορά. Γενικά, τα ακόλουθα είναι μερικά από τα άτομα, τόσο εσωτερικά όσο και εξωτερικά στον οργανισμό, που ενδέχεται να διαβάσουν τις αναφορές σχετικές με ένα περιστατικό:

Στελέχη: Σε περιπτώσεις υψηλού προφίλ, το περιστατικό μπορεί να φτάσει στην προσοχή του CEO ή του CFO, ειδικά αν εμπλέκονται τα μέσα ενημέρωσης. Μια εκτελεστική περίληψη μπορεί να είναι αρκετή, αλλά μην εκπλαγείτε αν η ανώτερη ηγεσία απαιτήσει μια πιο λεπτομερή αναφορά και ενημέρωση κατά τη διάρκεια και στο τέλος του περιστατικού.

Προσωπικό πληροφορικής (IT): Αυτά τα άτομα πιθανότατα θα ενδιαφέρονται περισσότερο για τα ευρήματα των αναλυτών αντίδρασης σε περιστατικά. Συνήθως, θα εξετάσουν πολύ σοβαρά την ανάλυση της ρίζας του προβλήματος και τις προτάσεις αποκατάστασης.

Νομικό τμήμα: Σε περίπτωση που αναμένεται αγωγή ή άλλη νομική ενέργεια, το νομικό τμήμα θα εξετάσει την αναφορά περιστατικού για να εντοπίσει τυχόν κενά στην ασφάλεια ή τις σχετικές διαδικασίες που χρειάζονται διευκρίνιση. Μην εκπλαγείτε αν χρειαστούν τροποποιήσεις.

Τμήμα μάρκετινγκ: Το μάρκετινγκ ενδέχεται να χρειαστεί να εξετάσει είτε την εκτελεστική περίληψη είτε την αναφορά περιστατικού για να δημιουργήσει μήνυμα προς τους πελάτες σε περίπτωση εξωτερικής παραβίασης δεδομένων.

Ρυθμιστικές αρχές: Σε ρυθμιζόμενους κλάδους, όπως η υγειονομική περίθαλψη και οι χρηματοπιστωτικοί οργανισμοί, οι ρυθμιστικές αρχές συχνά εξετάζουν τις αναφορές περιστατικών για να καθορίσουν αν υπάρχει πιθανή ευθύνη εκ μέρους του οργανισμού. Πρόστιμα μπορεί να επιβληθούν βάσει του αριθμού των εμπιστευτικών αρχείων που παραβιάστηκαν ή αν φαίνεται ότι ο οργανισμός επέδειξε αμέλεια.

Αρχές επιβολής του νόμου: Ορισμένα περιστατικά απαιτούν εμπλοκή της αστυνομίας ή άλλων αρχών επιβολής του νόμου. Σε αυτές τις περιπτώσεις, οι αρχές ενδέχεται να ζητήσουν αντίγραφα των αναφορών περιστατικών και εγκληματολογικών αναφορών για εξέταση.

Εξωτερική υποστήριξη: Υπάρχουν περιπτώσεις όπου είναι απαραίτητο να εμπλακούν εξωτερικοί ειδικοί σε εγκληματολογική ανάλυση ή αντίδραση σε περιστατικά. Σε αυτές τις περιπτώσεις, οι υπάρχουσες αναφορές διευκολύνουν την ενημέρωσή τους.

Κατανόηση του κοινού δίνει στους αναλυτές αντίδρασης σε περιστατικά μια εικόνα για το ποιος θα διαβάσει τις αναφορές τους. Η αναφορά πρέπει να είναι σαφής και συνοπτική, ενώ οι τεχνικές λεπτομέρειες μπορεί να χρειάζονται επεξήγηση για όσους δεν έχουν την απαιτούμενη γνώση ή εμπειρία.

11.5. Παρακολούθηση περιστατικών

Πολλοί οργανισμοί χρησιμοποιούν συστήματα παρακολούθησης αιτημάτων πληροφορικής (IT trouble ticket) για περιστατικά, όπως τα ServiceNow και Jira. Αυτή η μέθοδος λειτουργεί καλά όταν υπάρχουν λίγα περιστατικά και δεν απαιτείται αυτοματοποίηση των διαδικασιών αντίδρασης. Οι οργανισμοί με πιο ανεπτυγμένη ικανότητα αντίδρασης σε περιστατικά μπορεί να χρειαστεί να

χρησιμοποιήσουν μια πλατφόρμα αντίδρασης σε περιστατικά για την παρακολούθηση και σωστή εκτέλεση της διαδικασίας και της τεκμηρίωσης.

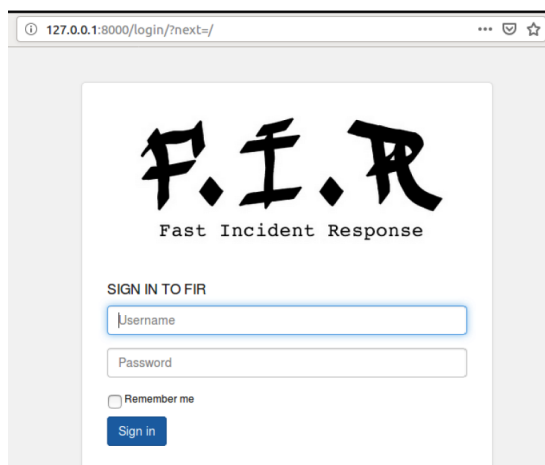
Οι εμπορικές λύσεις για παρακολούθηση περιστατικών κυβερνοασφάλειας ανήκουν συνήθως στην κατηγορία **Security Orchestration Automation Response (SOAR)**. Ορισμένες από αυτές μπορούν να ενσωματωθούν με άλλα εργαλεία για αυτοματοποίηση σημαντικού μέρους της διαδικασίας. Επίσης, μπορεί να περιλαμβάνουν **playbooks** ώστε οι ομάδες αντίδρασης να έχουν άμεση πρόσβαση και να ακολουθούν τη διαδικασία ενώ καταγράφουν τις ενέργειες στην ίδια την πλατφόρμα. Ένα από τα μεγαλύτερα πλεονεκτήματα μιας αφιερωμένης πλατφόρμας είναι η δυνατότητα παρακολούθησης περιστατικών με την πάροδο του χρόνου και η κατανόηση των τύπων επιθέσεων που αντιμετωπίζει ο οργανισμός.

11.6. Γρήγορη αντίδραση σε περιστατικά

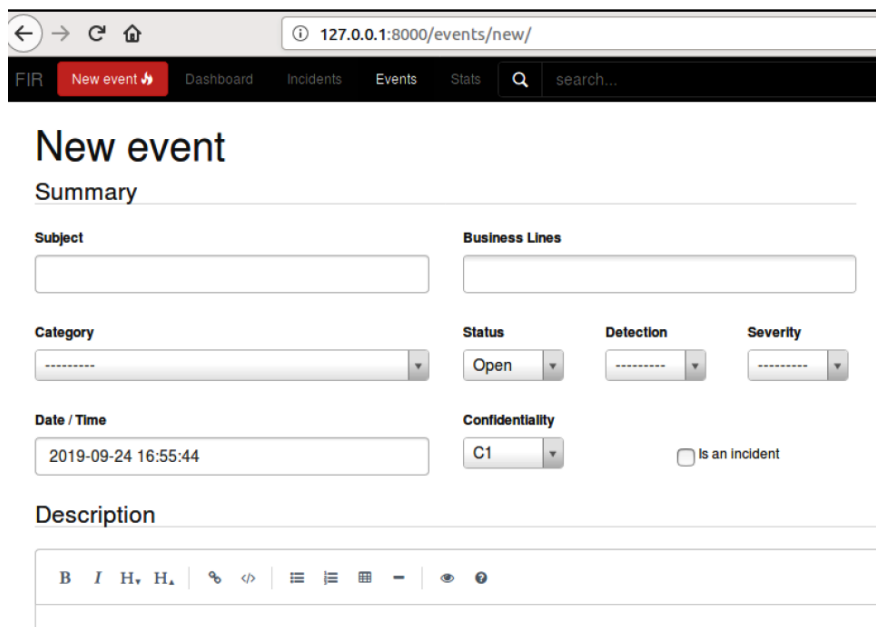
Η **Société Générale CERT** δημιούργησε την πλατφόρμα **FIR** ως freeware εργαλείο για τη βοήθεια των ομάδων αντίδρασης στην δημιουργία, παρακολούθηση και αναφορά περιστατικών. Αυτή η διαδικτυακή εφαρμογή επιτρέπει σε οποιονδήποτε εντός του οργανισμού να δημιουργεί περιστατικά, να κρατά σημειώσεις και να παρακολουθεί την ολοκλήρωση των περιστατικών. Το εργαλείο διαθέτει πολλές δυνατότητες χρήσιμες για ομάδες με περιορισμένο προϋπολογισμό. Χρησιμοποιεί **MySQL** για τη βάση δεδομένων και συνδυασμό **Python, Django και Bootstrap** για τη δημιουργία του περιβάλλοντος web εφαρμογής, επιτρέποντας στους αναλυτές να εισάγουν δεδομένα και να εκτελούν ερωτήματα. Μια σημαντική δυνατότητα του FIR είναι η προσαρμογή πεδίων ώστε να ταιριάζουν στον οργανισμό. Μπορεί να εγκατασταθεί σε **Docker** ή σε Linux σύστημα, όπως το Ubuntu.

Το FIR είναι διαθέσιμο για **αναπτυξιακό και παραγωγικό περιβάλλον**, ανάλογα με το μέγεθος του οργανισμού και τη συχνότητα εισαγωγής δεδομένων. Ο πλήρης οδηγός εγκατάστασης είναι διαθέσιμος [εδώ](#). Για τη χρήση του FIR:

1. Μετά την εγκατάσταση, ανοίξτε τον browser και εισάγετε `http://localhost:8000` για να εμφανιστεί η οθόνη σύνδεσης. Για το αναπτυξιακό περιβάλλον, χρησιμοποιήστε `admin/admin`.

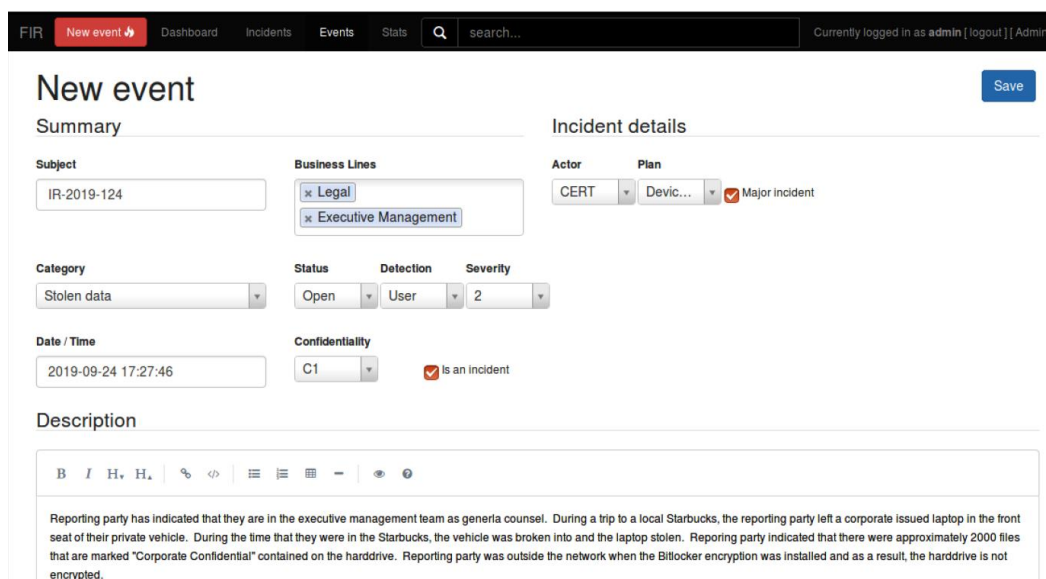


2. Μετά τη σύνδεση, το dashboard θα είναι άδειο. Κάντε κλικ στο **New Event** στην πάνω αριστερή γωνία.



The screenshot shows the 'New event' form in the FIR system. The form is titled 'New event' and has a 'Summary' section. It includes fields for 'Subject', 'Business Lines', 'Category', 'Status' (set to 'Open'), 'Detection', 'Severity', 'Date / Time' (2019-09-24 16:55:44), 'Confidentiality' (C1), and a checkbox 'Is an incident'. There is also a 'Description' section with a rich text editor.

3. Στη φόρμα υπάρχουν πεδία για την καταγραφή περιστατικού. **Subject:** Πεδίο ελεύθερου κειμένου, π.χ. αριθμός περιστατικού. **Business Lines:** Προκαθορισμένο πεδίο, μπορεί να τροποποιηθεί. **Category:** Προκαθορισμένες κατηγορίες περιστατικών, δυνατότητα προσθήκης νέων. **Status:** Κατάσταση περιστατικού (ανοιχτό/κλειστό). **Detection:** Ποιος ή τι ανίχνευσε πρώτος το περιστατικό. **Severity:** Προκαθορισμένα επίπεδα σοβαρότητας (1-4). **Date/Time:** Αυτόματο timestamp, με δυνατότητα αλλαγής ζώνης ώρας. **Confidentiality:** Κλίμακα εμπιστευτικότητας.
4. Καταχωρήστε τα δεδομένα. Παράδειγμα: κλεμμένος φορητός υπολογιστής με 2.000 μη κρυπτογραφημένα αρχεία.



The screenshot shows the 'New event' form in the FIR system, with the 'Incident details' section expanded. The form is titled 'New event' and has a 'Summary' section. It includes fields for 'Subject' (IR-2019-124), 'Business Lines' (Legal, Executive Management), 'Category' (Stolen data), 'Status' (Open), 'Detection' (User), 'Severity' (2), 'Date / Time' (2019-09-24 17:27:46), 'Confidentiality' (C1), and a checkbox 'Is an incident'. There is also a 'Description' section with a rich text editor.

Reporting party has indicated that they are in the executive management team as general counsel. During a trip to a local Starbucks, the reporting party left a corporate issued laptop in the front seat of their private vehicle. During the time that they were in the Starbucks, the vehicle was broken into and the laptop stolen. Reporting party indicated that there were approximately 2000 files that are marked "Corporate Confidential" contained on the harddrive. Reporting party was outside the network when the Bitlocker encryption was installed and as a result, the harddrive is not encrypted.

5. Με την επιλογή του περιστατικού, εμφανίζονται δύο επιπλέον πεδία: **Actor** και **Plan**.
6. Αφού συμπληρωθούν, κάντε κλικ στο **Save**.

Incident / Stolen data / IR-2019-124

Opened on Sept. 24, 2019, 5:27 p.m. by admin

DESCRIPTION

Reporting party has indicated that they are in the executive management team as general counsel. During a trip to a local Starbucks, the reporting party left a corporate issued laptop in the front seat of their private vehicle. During the time that they were in the Starbucks, the vehicle was broken into and the laptop stolen. Reporting party indicated that there were approximately 2000 files that are marked "Corporate Confidential" contained on the harddrive. Reporting party was outside the network when the Bitlocker encryption was installed and as a result, the harddrive is not encrypted.

TO-DO LIST

Action

Accountable

+ Add To-Do Item

Comments (1)

		Comment	Action
2019-09-24 17:27	admin	Incident opened	Opened  

+ Add  Comment  Edit  Block  Close  Incident followup  Alert  Takedown

7. Στο παράθυρο του περιστατικού, κάντε κλικ στο **Add and To-Do**, εισάγετε το task και τον υπεύθυνο.

STARRED INCIDENTS

No incidents to show.

Open

Blocked

Old

Tasks

Date ▼	Category	Subject	Business Lines	Severity	Status	Detection	Leader	Last Action	Plan	Lvl	IH	Edit
2019-09-24 ★	Stolen data	IR-2019-124	Legal, Executive Management	2	Open	User	CERT	Opened in 9 hours	Device Loss	C1	admin	

(page 1 of 1)

8. Το task εμφανίζεται στο dashboard, επιτρέποντας την ανάθεση εργασιών σε άτομα.

STARRED INCIDENTS

No incidents to show.

Open

Blocked

Old

Tasks

Task	Incident	Category	Business line	Delete
☐ Execute Device Loss Playbook	IR-2019-124	Stolen data	CERT	

(page 1 of 1)

Ο διαχειριστής μπορεί να τροποποιήσει πεδία όπως μονάδες επιχειρήσεων ή ενέργειες μέσω του εικονιδίου **Admin** στην πάνω δεξιά γωνία. Μπορούν να προστεθούν playbooks, όπως για malware, ώστε να ειδοποιούνται τα μέλη της CSIRT για την εκτέλεση συγκεκριμένων διαδικασιών.

Με τη χρήση της πλατφόρμας **FIR**, μια ομάδα αντιμετώπισης περιστατικών μπορεί να διαθέτει ένα ενιαίο αποθετήριο για τα δεδομένα του περιστατικού, καθώς και τη δυνατότητα ανάθεσης συγκεκριμένων εργασιών σε άτομα. Για να ενισχυθεί περαιτέρω αυτή η δυνατότητα, το **FIR** επιτρέπει στον διαχειριστή του συστήματος να πραγματοποιεί τροποποιήσεις σε πεδία, όπως οι επιχειρηματικές μονάδες ή οι ενέργειες. Για να αποκτήσετε πρόσβαση σε αυτά, κάντε κλικ στο εικονίδιο **Admin** στην επάνω δεξιά γωνία του παραθύρου.

Πολλά από αυτά τα πεδία δεν έχουν ακόμη διαμορφωθεί, επιτρέποντας στον διαχειριστή να ορίσει συγκεκριμένους τύπους ειδοποιήσεων και τεκμηρίων (artifacts). Μία περιοχή που ο διαχειριστής μπορεί να θελήσει να ρυθμίσει πριν από τη χρήση είναι οι πληροφορίες του περιστατικού. Κάνοντας κύλιση προς τα κάτω, εμφανίζονται τα ακόλουθα πεδία περιστατικών που μπορούν να τροποποιηθούν από τον διαχειριστή.

Για παράδειγμα, ας υποθέσουμε ότι ο διαχειριστής θέλει να προσθέσει το **malware playbook** στο αναπτυσσόμενο μενού *Plan*. Αυτή η προσθήκη θα ειδοποιήσει άμεσα τα υπόλοιπα μέλη της CSIRT ότι πρέπει να εκτελεστεί το συγκεκριμένο playbook:

Django administration

Site administration

AUTH TOKEN

Tokens

+ Add

Change

AUTHENTICATION AND AUTHORIZATION

Groups

+ Add

Change

Users

+ Add

Change

FIR_ALERTING

Category templates

+ Add

Change

Recipient templates

+ Add

Change

FIR_ARTIFACTS

Artifact blacklist items

+ Add

Change

Artifacts

+ Add

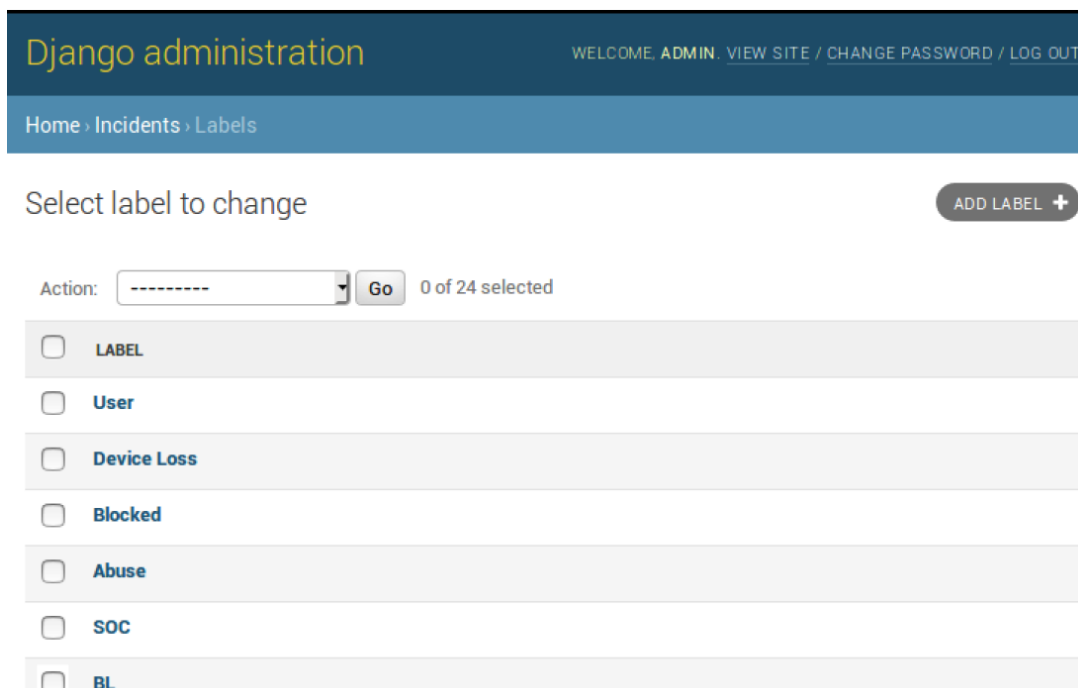
Change

Files

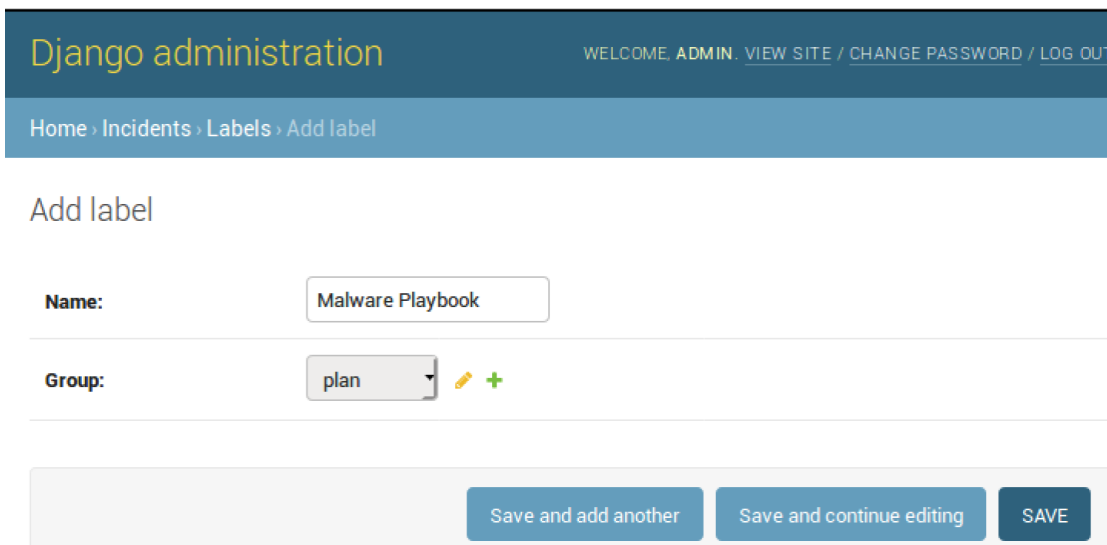
+ Add

Change

1. Κάντε κλικ στο **Labels** και θα εμφανιστεί το ακόλουθο παράθυρο:



2. Κάντε κλικ στο **ADD LABEL**. Στο πεδίο κειμένου, εισάγετε **Malware Playbook**. Στο αναπτυσσόμενο μενού, επιλέξτε *plan*. Τέλος, κάντε κλικ στο **SAVE**.



3. Επιστρέψτε στην αρχική οθόνη και κάντε κλικ στο **New Event**. Επιλέξτε το κουτάκι **Major Incident**. Στο πεδίο *Plan* θα πρέπει πλέον να εμφανίζεται η επιλογή **Malware Playbook**.

Αυτό αποτελεί παράδειγμα των πολλών επιλογών που είναι διαθέσιμες για τροποποίηση, ώστε οι αναλυτές αντιμετώπισης περιστατικών και τα μέλη της ομάδας να μπορούν να προσαρμόζουν το FIR στις λειτουργικές τους ανάγκες.

Incident details

Actor	Plan	
CERT	-----	☐ Major incident
	2	
	5	
	6	
	Device	
	Loss	
	Playbook	
	Malware	
	Playbook	

Η εφαρμογή FIR, καθώς και άλλες παρόμοιες εφαρμογές, δίνουν στις ομάδες αντίδρασης σε περιστατικά τη δυνατότητα να παρακολουθούν περιστατικά από την ανίχνευση έως την ολοκλήρωση, παρέχοντας παράλληλα έναν κεντρικό χώρο αποθήκευσης για τις πληροφορίες της υπόθεσης. Αυτό είναι κρίσιμης σημασίας κατά το κλείσιμο της έρευνας και την προετοιμασία της απαραίτητης τεκμηρίωσης για τα ενδιαφερόμενα μέρη και τους υπεύθυνους λήψης αποφάσεων.

11.7. Γραπτές αναφορές

Ο τρόπος με τον οποίο δομείται μια γραπτή αναφορά καθορίζεται συχνά από διάφορους παράγοντες. Υπάρχουν πολλά στοιχεία που συνθέτουν μια διαδικασία απόκρισης σε περιστατικό, όπως:

- το προσωπικό που συμμετείχε,
- ο τύπος και το βάθος της διεξαχθείσας έρευνας,
- ο αριθμός των πόρων που χρησιμοποιήθηκαν,
- καθώς και πόσα άτομα από τον οργανισμό συμμετείχαν όχι μόνο στην έρευνα του περιστατικού, αλλά και ως ενδιαφερόμενοι για την έκβασή του.

Ως αποτέλεσμα, ορισμένοι οργανισμοί μπορεί να επιλέξουν να συνδυάσουν τα βασικά στοιχεία της **αναφοράς περιστατικού**, της **εκτελεστικής περίληψης** και της **εγκληματολογικής αναφοράς** σε ένα ενιαίο έγγραφο. Άλλοι οργανισμοί ενδέχεται να θεωρήσουν ότι ο διαχωρισμός της τεκμηρίωσης σε ξεχωριστά μέρη εξυπηρετεί καλύτερα τα διαφορετικά επίπεδα εμπλοκής και ενδιαφέροντος των ατόμων που συμμετείχαν ή επηρεάζονται από την έρευνα.

Η αναφορά περιστατικού έχει πιθανότατα το ευρύτερο κοινό, τόσο εντός όσο και εκτός του οργανισμού. Ακόμα κι αν υπάρχουν άτομα με περιορισμένες τεχνικές δεξιότητες που θα εξετάσουν την αναφορά αυτή, είναι σημαντικό να χρησιμοποιείται η κατάλληλη ορολογία και τα αντίστοιχα δεδομένα. Θα υπάρχει πάντοτε χρόνος για την επεξήγηση τεχνικών λεπτομερειών σε όσους ενδέχεται να μην τις κατανοούν πλήρως.

Τα παρακάτω είναι μερικά από τα βασικά δεδομένα που πρέπει να καταγράφονται και να ενσωματώνονται στην αναφορά:

- **Υπόβαθρο (Background):** Το υπόβαθρο αποτελεί τη γενική επισκόπηση του περιστατικού από την ανίχνευση έως την τελική διευθέτηση. Πρέπει να περιλαμβάνει πώς η ομάδα CSIRT ενημερώθηκε αρχικά για το περιστατικό και ποιες πληροφορίες ήταν διαθέσιμες στην αρχή. Στη συνέχεια, θα πρέπει να εξάγονται συμπεράσματα σχετικά με τον τύπο και την έκταση του περιστατικού. Η αναφορά οφείλει επίσης να περιλαμβάνει τον αντίκτυπο στα συστήματα και ποια εμπιστευτικά δεδομένα ενδέχεται να έχουν παραβιαστεί. Τέλος, πρέπει να παρέχει μια επισκόπηση της στρατηγικής περιορισμού που χρησιμοποιήθηκε και πώς τα συστήματα επανήλθαν σε κανονική λειτουργία.
- **Χρονολόγιο γεγονότων (Events timeline):** Καθώς η αναφορά μεταβαίνει από το υπόβαθρο στο χρονολόγιο των γεγονότων, δίνεται αυξημένη έμφαση στη λεπτομέρεια. Το χρονολόγιο γεγονότων είναι καλύτερο να διαμορφώνεται σε μορφή πίνακα. Για κάθε ενέργεια που πραγματοποιήθηκε, θα πρέπει να υπάρχει αντίστοιχη καταγραφή στο χρονολόγιο. Ο παρακάτω πίνακας δείχνει το επίπεδο λεπτομέρειας που πρέπει να περιλαμβάνεται:

Date	Time	Description	Performed by
6/17/19	19:08	SOC alerted CSIRT on-call about attempted C2 traffic from an internal host.	John Q. Examiner
6/17/19	19:10	Examined firewall log and determined that host 10.25.4.5 had connected to a known malware C2 server.	John Q. Examiner
6/17/19	19:14	Contacted the network security CSIRT member to administratively down the port connecting host 10.25.4.5 on switch 009.	John Q. Examiner
6/17/19	19:25	Removed connectivity to the internal network from host 10.25.4.5 from the network switch 009.	Dale Mitchell

Το καταγεγραμμένο χρονολόγιο μπορεί να περιλαμβάνει πολλές σελίδες καταχωρήσεων, ωστόσο είναι κρίσιμο να γίνει κατανοητή η ακολουθία των γεγονότων και ο χρόνος που απαιτήθηκε για την εκτέλεση συγκεκριμένων ενεργειών. Οι πληροφορίες αυτές μπορούν να αξιοποιηθούν τόσο για την αναπαράσταση της ακολουθίας των γεγονότων, όσο και για τη βελτίωση της διαδικασίας απόκρισης σε περιστατικά, μέσω της εξέτασης του χρόνου απόκρισης και των διαδικαστικών καθυστερήσεων.

- **Επισκόπηση υποδομής δικτύου (Network infrastructure overview):** Στην περίπτωση που το περιστατικό αφορά πολλαπλά συστήματα εντός του δικτύου, αποτελεί καλή πρακτική η

συμπερίληψη διαγράμματος του δικτύου με τα επηρεαζόμενα συστήματα, καθώς και μιας επισκόπησης του τρόπου σύνδεσης και επικοινωνίας μεταξύ τους. Άλλες πληροφορίες, όπως οι κανόνες firewall που σχετίζονται άμεσα με το περιστατικό, θα πρέπει επίσης να συμπεριληφθούν.

- **Επισκόπηση ψηφιακής ανάλυσης (Forensic analysis overview):** Στα περιστατικά που απαιτούν ψηφιακή ανάλυση αρχείων καταγραφής, μνήμης ή δίσκων, θα πρέπει να περιλαμβάνεται μια επισκόπηση της διαδικασίας και των αποτελεσμάτων. Με αυτόν τον τρόπο, οι ενδιαφερόμενοι μπορούν να κατανοήσουν τι είδους αναλύσεις πραγματοποιήθηκαν και ποια ήταν τα αποτελέσματα, χωρίς να χρειάζεται να εισέλθουν σε υπερβολικά τεχνικές λεπτομέρειες. Οι αναλυτές πρέπει να διασφαλίζουν ότι τα συμπεράσματα που εξάγονται μέσω της ψηφιακής ανάλυσης καταγράφονται σε αυτή την ενότητα. Σε περιπτώσεις εκτεταμένης χρήσης τεχνικών ψηφιακής ανάλυσης, αυτές μπορεί να καταγραφούν σε ξεχωριστή αναφορά.
- **Ενέργειες περιορισμού (Containment actions):** Μία από τις βασικές αρμοδιότητες της ομάδας απόκρισης περιστατικών είναι να περιορίσει το εύρος της ζημίας σε άλλα συστήματα μετά την ανίχνευση του περιστατικού. Το τμήμα αυτό της αναφοράς πρέπει να περιγράφει τις ενέργειες περιορισμού που εφαρμόστηκαν, όπως η απενεργοποίηση ενός συστήματος, η αποσύνδεσή του από το δίκτυο ή ο περιορισμός της πρόσβασής του στο διαδίκτυο. Οι αναλυτές πρέπει επίσης να καταγράψουν την αποτελεσματικότητα των μέτρων αυτών. Για παράδειγμα, αν η απομάκρυνση της πρόσβασης στο δίκτυο ήταν δύσκολο να γίνει διοικητικά μέσω του switch και έπρεπε να εφαρμοστεί χειροκίνητη διαδικασία, η γνώση αυτού του γεγονότος θα βοηθήσει το CSIRT να δημιουργήσει νέες διαδικασίες που θα απλοποιήσουν την ενέργεια και θα περιορίσουν τη δυνατότητα ενός συμβιβασμένου συστήματος να επηρεάσει άλλα τμήματα του δικτύου.
- **Ευρήματα / Ανάλυση ρίζας αιτίας (Findings / Root cause analysis):** Το πιο ουσιαστικό τμήμα της αναφοράς, το οποίο είναι ιδιαίτερα χρήσιμο για την ανώτερη διοίκηση και το προσωπικό πληροφορικής, αφορά τα ευρήματα και, εφόσον έχει ανακαλυφθεί, τη ρίζα του προβλήματος. Η ενότητα αυτή πρέπει να είναι ολοκληρωμένη και να ενσωματώνει στοιχεία από το χρονολόγιο γεγονότων. Ειδικοί παράγοντες σε επίπεδο συστημάτων, λογισμικού, υλικού και χρηστών, που συνέβαλαν θετικά ή αρνητικά στην εξέλιξη του περιστατικού, πρέπει να αναδεικνύονται. Αν έχει προσδιοριστεί το συγκεκριμένο exploit ή η ευπάθεια που αξιοποιήθηκε από τον επιτιθέμενο, θα πρέπει να καταγραφεί. Στόχος είναι να εξηγηθεί πώς η απειλή κατόρθωσε να συμβιβάσει την υποδομή, ώστε να τεκμηριωθούν οι δράσεις αποκατάστασης και οι συστάσεις που ακολουθούν.
- **Αποκατάσταση (Remediation):** Εάν ελήφθησαν μέτρα αποκατάστασης κατά τη διάρκεια του περιστατικού για την αντιμετώπιση ευπαθειών ή άλλων ελλείψεων, αυτά πρέπει να καταγραφούν. Με αυτόν τον τρόπο, το CSIRT μπορεί να ενημερώσει πλήρως το προσωπικό IT για τις αλλαγές που εφαρμόστηκαν, ώστε να ενσωματωθούν στις κανονικές διαδικασίες διαχείρισης αλλαγών και να αξιολογηθούν. Αυτό εξασφαλίζει ότι οι αλλαγές δεν θα έχουν αρνητικές συνέπειες σε άλλα συστήματα μελλοντικά.
- **Τελικές συστάσεις (Final recommendations):** Οποιαδήποτε σύσταση για βελτίωση της υποδομής, επιδιόρθωση ευπαθειών ή προσθήκη επιπλέον ελέγχων πρέπει να καταγράφεται. Ωστόσο, οι

συστάσεις πρέπει να βασίζονται σε παρατηρήσεις και ενδελεχή ανάλυση της ρίζας του προβλήματος.

- **Ορισμοί (Definitions):** Οποιοιδήποτε ειδικοί ορισμοί που μπορούν να βοηθήσουν το τεχνικό προσωπικό να κατανοήσει το περιστατικό πρέπει να συμπεριλαμβάνονται στην αναφορά. Για παράδειγμα, τεχνικοί όροι όπως το *Server Message Block (SMB)* πρέπει να οριστούν, ειδικά εάν η επίθεση εκμεταλλεύτηκε ευπάθειες στο πρωτόκολλο SMB σε κάποιο συγκεκριμένο σύστημα.

Είναι κρίσιμο να γίνει κατανοητό ότι η αναφορά αυτή είναι η πιο πιθανή να διαμοιραστεί σε διάφορες οντότητες, εντός και εκτός του οργανισμού. Η αναφορά πρέπει επίσης να περνάει από τουλάχιστον έναν ποιοτικό έλεγχο, ώστε να διασφαλιστεί ότι είναι απαλλαγμένη από λάθη ή παραλείψεις και ότι μπορεί να διαβαστεί αποτελεσματικά από το στοχευόμενο κοινό.

11.8 Αναφορά Ψηφιακής Εγκληματολογίας (Forensic Report)

Οι αναφορές ψηφιακής εγκληματολογίας είναι οι πιο τεχνικά σύνθετες από τους τρεις βασικούς τύπους αναφορών. Οι αναλυτές πρέπει να είναι ελεύθεροι να είναι όσο το δυνατόν πιο τεχνικά ακριβείς και να μην απλοποιούν την αναφορά για μη τεχνικά άτομα. Οι αναλυτές θα πρέπει επίσης να γνωρίζουν ότι η εγκληματολογική αναφορά θα είναι κρίσιμη για τη συνολική αναφορά περιστατικού, εάν καταφέρει να προσδιορίσει συγκεκριμένο άτομο, όπως για παράδειγμα έναν κακόβουλο εσωτερικό χρήστη.

Σε περιπτώσεις όπου έχει ταυτοποιηθεί ο δράστης ή όπου το περιστατικό ενδέχεται να έχει νομικές συνέπειες, η εγκληματολογική αναφορά θα υποβληθεί σε ενδελεχή έλεγχο. Συνεπώς, ο αναλυτής πρέπει να καταβάλει μεγάλη προσπάθεια ώστε να την ολοκληρώσει με ακρίβεια και πληρότητα:

Στοιχεία/Ιστορικό εξεταστή: Για το κοινό που περιλαμβάνει νομικούς ή εξωτερικούς ελεγκτές, είναι κρίσιμο να υπάρχει σαφής εικόνα του υπόβαθρου και των προσόντων των εγκληματολογικών αναλυτών. Αυτό πρέπει να περιλαμβάνει τυπική εκπαίδευση, κατάρτιση, εμπειρία, καθώς και μια επισκόπηση της εμπειρίας τους σε δικαστική αίθουσα, όπως το αν έχουν αναγνωριστεί ως πραγματογνώμονες μάρτυρες. Ένα πλήρες βιογραφικό σημείωμα μπορεί να επισυναφθεί στην αναφορά, ιδιαίτερα εάν προβλέπεται ότι η αναφορά θα χρησιμοποιηθεί σε δικαστική υπόθεση.

Εργαλεία που χρησιμοποιήθηκαν: Η αναφορά πρέπει να περιλαμβάνει πλήρη λίστα του υλικού (hardware) και του λογισμικού (software) που χρησιμοποιήθηκε για την ανάλυση των αποδεικτικών στοιχείων. Αυτό περιλαμβάνει μάρκα, μοντέλο και σειριακό αριθμό εξοπλισμού (π.χ. write blocker), καθώς και το όνομα και την έκδοση κάθε λογισμικού. Μπορεί να προστεθεί επίσης ότι όλα τα εργαλεία ήταν ενημερωμένα πριν από τη χρήση τους.

Αποδεικτικά στοιχεία: Μια πλήρης λίστα αποδεικτικών στοιχείων πρέπει να περιλαμβάνει εικόνες δίσκων (disk images), καταγραφές μνήμης (memory captures) ή αρχεία καταγραφής (log files) που αποκτήθηκαν κατά τη διάρκεια του περιστατικού. Θα πρέπει να αναφέρονται η ημερομηνία, η ώρα, η τοποθεσία και ο αναλυτής που απέκτησε το εκάστοτε στοιχείο. Ενδέχεται να απαιτείται η

επισύναψη εντύπων αλυσίδας φύλαξης (chain of custody) για φυσικά αποδεικτικά στοιχεία. Αν τα τεκμήρια είναι πολλά, η ενότητα αυτή μπορεί να προστεθεί ως παράρτημα ώστε η ανάγνωση να παραμένει ομαλή.

Εγκληματολογική ανάλυση: Εδώ οι αναλυτές πρέπει να είναι πολύ συγκεκριμένοι σχετικά με τις ενέργειες που έγιναν κατά τη διερεύνηση. Οι λεπτομέρειες ημερομηνιών και χρόνων είναι κρίσιμες, όπως και οι αναλυτικές περιγραφές των ενεργειών που εκτελέστηκαν.

Έξοδος εργαλείων: Πολλά εργαλεία που χρησιμοποιούνται στις έρευνες περιστατικών, όπως τα **Volatility** ή **Rekall**, δεν έχουν δυνατότητα δημιουργίας αναφοράς. Ο αναλυτής είναι υπεύθυνος να καταγράψει την έξοδο αυτών των εργαλείων. Μπορούν να συμπεριληφθούν στιγμιότυπα οθόνης ή κείμενα εξόδου από γραμμή εντολών και να ενσωματωθούν στην αναφορά. Αυτό είναι κρίσιμο όταν η έξοδος σχετίζεται άμεσα με το περιστατικό.

Άλλα εργαλεία, όπως το **Autopsy**, διαθέτουν δυνατότητα εξαγωγής αναφορών που μπορούν να συμπεριληφθούν απευθείας. Για παράδειγμα:

1. Άνοιγμα της υπόθεσης στο Autopsy.
2. Μετάβαση στο **Tools** → **Generate Report**.
3. Επιλογή **Results – HTML**, έπειτα **Next** και **All Results**.
4. Δημιουργείται αναφορά HTML που ανοίγει στον προεπιλεγμένο φυλλομετρητή.

The screenshot displays the 'Autopsy Forensic Report' interface. On the left is a 'Report Navigation' sidebar with a list of report sections, each with an icon and a count in parentheses. The main panel on the right is titled 'Autopsy Forensic Report' and includes a timestamp 'HTML Report Generated on 2019/09/23 17:51:51'. Below the title, case details are listed: Case (Potential Data Leak Investigation), Case Number (Incident-2019-0145), Number of Images (1), Notes (Suspected data leak from laptop), and Examiner (Gerard Johansen). A section titled 'Image Information:' follows, showing a table with one entry: 'JSmith_LT_0976.e01'. Below this, a list of paths is shown for each image file, all located in 'D:\Suspect_Images\JSmith_LT_0976\'. The paths are: JSmith_LT_0976.e01, JSmith_LT_0976.e02, JSmith_LT_0976.e03, and JSmith_LT_0976.e04.

Path:
D:\Suspect_Images\JSmith_LT_0976\JSmith_LT_0976.e01
D:\Suspect_Images\JSmith_LT_0976\JSmith_LT_0976.e02
D:\Suspect_Images\JSmith_LT_0976\JSmith_LT_0976.e03
D:\Suspect_Images\JSmith_LT_0976\JSmith_LT_0976.e04

Ο αναλυτής μπορεί να ελέγξει τις πληροφορίες εκεί. Επιπλέον τεχνικές, όπως η εκτύπωση σε PDF, επιτρέπουν την απευθείας επισύναψη της εξόδου στην αναφορά. Η εξοικείωση με τα εργαλεία μειώνει τα σφάλματα και αυξάνει την εγκυρότητα της αναφοράς.

Συμπεράσματα: Τα συμπεράσματα που προκύπτουν από τα αποδεικτικά στοιχεία μπορούν να συμπεριληφθούν. Για παράδειγμα, αν ένας αναλυτής εντοπίσει ότι ένα εκτελέσιμο αρχείο είναι κακόβουλο λογισμικό συγκρίνοντας το hash με γνωστό δείγμα, και διαπιστώσει ότι αυτό υποκλέπτει διαπιστευτήρια, τότε είναι απολύτως βάσιμο να συμπεριληφθεί αυτό το συμπέρασμα. Ωστόσο, οι αναλυτές πρέπει να αποφεύγουν υποθέσεις ή συμπεράσματα χωρίς τα κατάλληλα στοιχεία. Δεν επιτρέπεται η διατύπωση απόψεων ή εικασιών.

Ορισμοί: Επειδή η εγκληματολογική αναφορά είναι ιδιαίτερα τεχνική, είναι σημαντικό να περιλαμβάνονται οι απαραίτητοι ορισμοί. Εσωτερικοί ενδιαφερόμενοι, όπως νομικοί εκπρόσωποι, συχνά θα χρειαστούν διευκρινίσεις για τεχνικές λεπτομέρειες, ιδιαίτερα σε περίπτωση νομικής δράσης.

Παραρτήματα: Έξοδοι εργαλείων που είναι πολύ μεγάλες για το κυρίως σώμα της αναφοράς μπορούν να μπουν ως παράρτημα. Για παράδειγμα, αν η έξοδος μιας εντολής του Volatility εκτείνεται σε αρκετές σελίδες, αλλά το ουσιαστικό σημείο είναι μία γραμμή, τότε ο αναλυτής μπορεί να ενσωματώσει μόνο αυτή τη γραμμή στην κύρια ενότητα και να παραθέσει την πλήρη έξοδο στο παράρτημα. Η πλήρης καταγραφή είναι σημαντική ώστε να αντέξει σε εξονυχιστικό έλεγχο.

Ένας από τους βασικούς παράγοντες για την εγκληματολογική αναφορά είναι η διαδικασία εσωτερικής αξιολόγησης (peer review) πριν από την έκδοσή της. Αυτό διασφαλίζει ότι οι ενέργειες, η ανάλυση και τα συμπεράσματα ευθυγραμμίζονται με τα στοιχεία. Για αυτόν τον λόγο, οι αναλυτές πρέπει να περιλαμβάνουν όσο το δυνατόν περισσότερα δεδομένα από τα εργαλεία.

Αν η αναφορά οδηγηθεί σε δικαστήριο, πρέπει να αναμένεται ότι θα εξεταστεί από ισάξιους ή και ανώτερους ειδικούς, οι οποίοι θα κρίνουν την εργασία. Ένας άλλος αναλυτής πρέπει να μπορεί να διαβάσει την αναφορά, να κατανοήσει τις περιγραφές και να καταλήξει στα ίδια συμπεράσματα. Αυτή η γνώση ωθεί τους αναλυτές να συντάσσουν πιο προσεγμένες αναφορές.

Είτε ένας οργανισμός επιλέξει να διαχωρίσει την τεκμηρίωση είτε να ετοιμάσει μια ενιαία αναφορά, υπάρχουν συγκεκριμένα δεδομένα που πρέπει να καταγράφονται. Η σαφής εικόνα για αυτά τα δεδομένα βοηθά τους υπεύθυνους αντιμετώπισης περιστατικών να κρατούν σωστές σημειώσεις και να καταγράφουν παρατηρήσεις κατά τη διάρκεια της διερεύνησης. Η αποτυχία να καταγραφούν μπορεί να σημαίνει ότι ενέργειες ή παρατηρήσεις δεν θα συμπεριληφθούν στην αναφορά. Επιπλέον, σε περίπτωση δικαστικής διαδικασίας, στοιχεία μπορεί να αποκλειστούν. Είναι προτιμότερο να τεκμηριώνεται υπερβολικά παρά ανεπαρκώς.

Οι ομάδες αντιμετώπισης περιστατικών καταβάλλουν μεγάλη προσπάθεια για να προετοιμαστούν και να εκτελέσουν τα απαραίτητα καθήκοντα ώστε να χειριστούν σωστά ένα περιστατικό. Εξίσου

σημαντική είναι η ορθή τεκμηρίωση του περιστατικού, ώστε οι υπεύθυνοι λήψης αποφάσεων, αλλά και η ίδια η ομάδα αντιμετώπισης, να έχουν σαφή εικόνα των ενεργειών που πραγματοποιήθηκαν και του τρόπου με τον οποίο συνέβη το περιστατικό. Μέσα από τη χρήση αυτής της τεκμηρίωσης και την ανάλυση της ριζικής αιτίας, οι οργανισμοί μπορούν να βελτιώσουν την ασφάλειά τους και να μειώσουν τον κίνδυνο εμφάνισης παρόμοιων περιστατικών στο μέλλον. Ένας τομέας μείζονος ανησυχίας για τους ανταποκριτές περιστατικών και τους αναλυτές ψηφιακής εγκληματολογίας είναι ο ρόλος που διαδραματίζει το κακόβουλο λογισμικό (malware) στα περιστατικά.

12

Ανάλυση Κακόβουλου Λογισμικού

Το κακόβουλο λογισμικό συνεχίζει να αποτελεί μια συνεχώς εξελισσόμενη απειλή για τα συστήματα επιχειρήσεων και καταναλωτών. Μόλις δημιουργηθούν μέτρα άμυνας, οι προγραμματιστές κακόβουλου λογισμικού δημιουργούν μια νέα παραλλαγή με τη δύναμη να καταστρέψει ή να βλάψει ένα σύστημα. Το κακόβουλο λογισμικό χρησιμοποιείται ακόμη και ως όπλο κατά κρατών και διεθνών οργανισμών. Πολλές από τις παραβιάσεις δεδομένων που έχουν γίνει γνωστές στα μέσα ενημέρωσης περιλαμβάνουν, εν μέρει ή πλήρως, τη χρήση κακόβουλου λογισμικού για την επίτευξη κάποιου στόχου. Οργανισμοί σε κάθε τομέα της οικονομίας έχουν αντιμετωπίσει την απειλή του κακόβουλου λογισμικού. Με την προσθήκη επιθέσεων ransomware όπως τα WannaCry και Petya, οι οργανισμοί χρειάστηκε να ενεργήσουν άμεσα για την αντιμετώπισή τους.

Δεδομένου ότι το κακόβουλο λογισμικό αποτελεί μόνιμη απειλή, είναι κρίσιμο οι αναλυτές αντιμετώπισης περιστατικών να έχουν γνώση των μεθόδων και των εργαλείων που χρησιμοποιούνται στην ανάλυση κακόβουλου κώδικα. Είναι αδύνατο να καλυφθούν όλες οι λεπτομέρειες της ανάλυσης κακόβουλου λογισμικού σε ένα κεφάλαιο. Επομένως, το κεφάλαιο αυτό θα επικεντρωθεί στα θεμελιώδη στοιχεία της ανάλυσης κακόβουλου λογισμικού, εξετάζοντας παράλληλα μερικά από τα εργαλεία που χρησιμοποιούνται. Αυτό θα δώσει στον αναλυτή μια σταθερή κατανόηση αυτών των μεθόδων, ώστε στη συνέχεια να μπορεί να αξιολογήσει τα αποτελέσματα μιας τέτοιας ανάλυσης στο πλαίσιο ενός περιστατικού.

Σε αυτή τη συζήτηση για την ανάλυση κακόβουλου λογισμικού, θα εξεταστούν τα εξής θέματα:

- Κατηγοριοποίηση κακόβουλου λογισμικού
- Επισκόπηση της ανάλυσης κακόβουλου λογισμικού
- Ανάλυση κακόβουλου λογισμικού
- Εργαλεία ανάλυσης
- Εργαλεία και τεχνικές sandbox

12.1. Κατηγοριοποίηση κακόβουλου λογισμικού

Το κακόβουλο λογισμικό, ή malware, είναι ένας γενικός όρος για οποιοδήποτε λογισμικό δημιουργείται για να βλάψει, να απενεργοποιήσει ή να προκαλέσει ανεπιθύμητες καταστάσεις σε ένα υπολογιστικό σύστημα. Αυτή η οριστική, αν και λειτουργική, περιγραφή είναι επίσης πολύ ευρεία στην κατηγοριοποίηση του malware. Υπάρχει malware που έχει κωδικοποιηθεί ειδικά για να κλέβει αριθμούς πιστωτικών καρτών από συστήματα πληρωμών, ενώ άλλο malware χρησιμοποιείται για να αποκτήσει τον έλεγχο ενός συστήματος, επιτρέποντας σε έναν επιτιθέμενο να το χειρίζεται εξ αποστάσεως. Οι αναλυτές που παρατηρούν αυτές τις συγκεκριμένες συμπεριφορές — όπως π.χ. πώς ένα μολυσμένο σύστημα στέλνει επικοινωνίες στο Διαδίκτυο μετά τη μόλυνση ή ποιες ενέργειες λαμβάνονται σε ένα μολυσμένο σύστημα — μπορούν να προσδιορίσουν τον τύπο του κακόβουλου λογισμικού και τον τελικό στόχο του επιτιθέμενου.

Συνοπτικά, όταν μιλάμε για malware, μερικές από τις πιο συγκεκριμένες κατηγορίες είναι οι εξής:

- **Ιός (Virus):** Ο όρος χρησιμοποιούνταν αρχικά για οποιοδήποτε κακόβουλο κώδικα με επιβλαβείς συνέπειες σε ένα σύστημα. Καθώς αυξήθηκαν οι τύποι malware, ο όρος περιορίστηκε για να σημαίνει οποιονδήποτε κώδικα με σκόπιμα κακόβουλη επίδραση.
- **Σκουλήκι (Worm):** Συχνά μέρος ενός ιού, ένα worm μπορεί όχι μόνο να επηρεάσει ένα σύστημα αλλά και να αναπαράγεται αυτόνομα, επηρεάζοντας άλλα συστήματα συνδεδεμένα σε αυτό. Ένα από τα πιο γνωστά worms ήταν το Morris worm το 1988, που προκάλεσε επιθέσεις άρνησης υπηρεσίας (DoS) σε όλο το Διαδίκτυο.
- **Δούρειος ίππος (Trojan):** Εμπνευσμένος από τον μύθο του Δούρειου Ίππου, το Trojan malware συχνά κρύβεται μέσα σε ένα νόμιμο αρχείο ή εφαρμογή. Όταν ο ανυποψίαστος χρήστης ανοίξει το αρχείο, το malware μολύνει το σύστημα. Συνήθως χρησιμοποιεί τεχνικές κοινωνικής μηχανικής.
- **Keylogger:** Αυτό το malware κρύβεται στο παρασκήνιο και καταγράφει τα πλήκτρα που πατά ο χρήστης, στέλνοντας τις πληροφορίες στον επιτηρητή του. Συχνά χρησιμοποιείται για την απόκτηση credentials.
- **Rootkit:** Χρησιμοποιείται για να κρύψει άλλο κακόβουλο λογισμικό, όπως το Remote Access Trojan (RAT), που επιτρέπει στον επιτιθέμενο να ελέγχει εξ αποστάσεως ένα σύστημα.
- **Κακόβουλο λογισμικό για κλοπή πληροφοριών:** Συνήθως προγραμματισμένο για συγκεκριμένο σκοπό, χρησιμοποιείται για την απόκτηση πληροφοριών, όπως αριθμοί πιστωτικών καρτών ή τραπεζικοί κωδικοί (π.χ. το Shylock malware για τραπεζικά logins).
- **Backdoor:** Μια παραλλαγή απομακρυσμένης πρόσβασης που μολύνει ένα σύστημα και επιτρέπει στον επιτιθέμενο να αποκτήσει τον έλεγχο.
- **Downloader:** Τμήμα ενός πολυβάθμιου προγράμματος malware. Ο downloader μολύνει το σύστημα και στη συνέχεια συνδέεται με απομακρυσμένο server για να κατεβάσει τον υπόλοιπο κώδικα, παρακάμπτοντας μέτρα ασφαλείας.

- **Botnet:** Σειρά υπολογιστών που ελέγχονται μέσω ενός κεντρικού συστήματος στο Διαδίκτυο. Οι μολυσμένοι υπολογιστές μπορούν να χρησιμοποιηθούν για επιθέσεις DDoS.
- **Ransomware:** Νέα μορφή malware που κρυπτογραφεί αρχεία του θύματος και ζητά λύτρα (συνήθως σε κρυπτονόμισμα) για το κλειδί αποκρυπτογράφησης.
- **File wipers:** Καταστρέφουν αρχεία ή μολύνουν το Master Boot Record (MBR), καθιστώντας τα αρχεία μη προσβάσιμα.

Πολλές παραλλαγές χρησιμοποιούνται μαζί, δημιουργώντας αλυσίδες επιθέσεων. Για παράδειγμα, ένα RAT μπορεί να μολύνει αρχικά ένα σύστημα, να κατεβάσει δεύτερο payload, να αποκτήσει απομακρυσμένη πρόσβαση και τελικά να στοχεύσει σε συστήματα πληρωμών για κλοπή αριθμών πιστωτικών καρτών.

Ένα άλλο βασικό χαρακτηριστικό του malware είναι η συνεχής εξέλιξή του. Υπάρχει τεράστια ποικιλία παραλλαγών και η ποσότητα κακόβουλου κώδικα αυξάνεται καθημερινά. Οι τεχνικές κωδικοποίησης, παράδοσης και εκτέλεσης αλλάζουν ταχύτατα, και οι αναλυτές πρέπει να παρακολουθούν αυτές τις αλλαγές ώστε να είναι προετοιμασμένοι για τον πιο πρόσφατο και επικίνδυνο κώδικα.

Επισκόπηση Ανάλυσης Κακόβουλου Λογισμικού: Η ανάλυση κακόβουλου λογισμικού είναι η διαδικασία μελέτης του κακόβουλου κώδικα για να κατανοηθεί η λειτουργία, ο στόχος, και η επίδρασή του σε ένα σύστημα. Στόχος της ανάλυσης είναι:

- **Κατανόηση της λειτουργίας του malware:** πώς εισέρχεται, εξαπλώνεται, και ποιες ενέργειες εκτελεί.
- **Ανίχνευση συμπεριφοράς:** προσδιορισμός αλλαγών στο σύστημα, όπως δημιουργία αρχείων, τροποποίηση μητρώου, ή επικοινωνία με servers.
- **Ανάπτυξη εργαλείων ανίχνευσης και αντιμετώπισης:** δημιουργία signatures για antivirus ή IDS, καθώς και στρατηγικές απομόνωσης και καθαρισμού.

Η ανάλυση κακόβουλου λογισμικού μπορεί να πραγματοποιηθεί με δύο βασικούς τρόπους:

1. Στατική ανάλυση (Static Analysis)

- Γίνεται χωρίς να εκτελείται ο κώδικας.
- Εξετάζονται οι δομές αρχείων, οι επικεφαλίδες, οι αλυσίδες λειτουργιών, και οι συμβολικές βιβλιοθήκες.
- Χρησιμοποιούνται εργαλεία όπως disassemblers και decompilers.
- Παρέχει εικόνα για την προέλευση του malware, τις εξαρτήσεις του και πιθανές ευπάθειες που εκμεταλλεύεται.

2. Δυναμική ανάλυση (Dynamic Analysis)

- Γίνεται με την εκτέλεση του κακόβουλου λογισμικού σε ασφαλές περιβάλλον (sandbox ή virtual machine).
- Παρακολουθείται η συμπεριφορά του συστήματος, η δημιουργία αρχείων, οι επικοινωνίες δικτύου, και οι αλλαγές στο μητρώο ή στο αρχείο συστήματος.
- Επιτρέπει την κατανόηση του τρόπου με τον οποίο το malware αλληλεπιδρά με το λειτουργικό σύστημα και το δίκτυο σε πραγματικό χρόνο.

Συνήθως, η ανάλυση κακόβουλου λογισμικού συνδυάζει και τις δύο προσεγγίσεις για πλήρη κατανόηση. Η στατική ανάλυση μπορεί να αποκαλύψει τις δυνατότητες του malware χωρίς κίνδυνο εκτέλεσης, ενώ η δυναμική ανάλυση αποκαλύπτει την πραγματική συμπεριφορά του κατά την εκτέλεση.

12.2. Στατική Ανάλυση (Static Analysis)

Η στατική ανάλυση είναι η εξέταση του πραγματικού κώδικα κακόβουλου λογισμικού χωρίς να εκτελείται σε κάποιο σύστημα. Για τους ερευνητές κακόβουλου λογισμικού, ο κώδικας μπορεί να αποκτηθεί από συστήματα που έχουν αφεθεί σκόπιμα να μολυνθούν ή από παραγωγικά συστήματα που έχουν επηρεαστεί από το malware.

Σε αυτή την περίπτωση, οι αναλυτές απόκρισης σε περιστατικά μπορούν να αποκτήσουν τον πραγματικό πηγαίο κώδικα ή το εκτελέσιμο αρχείο μέσω συνδυασμού ανάλυσης μνήμης και απόκτησης του εκτελέσιμου κατά την ανάλυση του σκληρού δίσκου. Η στατική ανάλυση συχνά περιλαμβάνει διάφορες τεχνικές, όπως οι εξής:

1. **Fingerprinting** (Αποτύπωση Ψηφιακού Δακτυλικού Αποτυπώματος): Μία από τις πιο βασικές τεχνικές είναι η απόκτηση ενός κρυπτογραφικού hash του κώδικα. Αυτά τα hashes μπορούν να συγκριθούν με άλλα γνωστά hashes, για να προσδιοριστεί αν ο κώδικας έχει εμφανιστεί ξανά.
2. **Σάρωση με Αντιβιοτικό Λογισμικό (Anti-virus scanning)**: Οι προμηθευτές antivirus συχνά δεν ανιχνεύουν κάθε ιό. Για παράδειγμα, κάποιοι προμηθευτές μπορεί να έχουν αναλύσει τον κώδικα και να έχουν αναπτύξει ένα signature για το δικό τους προϊόν, ενώ άλλοι ίσως δεν είχαν πρόσβαση στον κώδικα ή δεν ανέπτυξαν δικό τους signature. Μία καλή πρακτική είναι να χρησιμοποιούνται πολλοί διαφορετικοί προμηθευτές antivirus για σάρωση ενός αρχείου.
3. **Εξαγωγή Συμβολοσειρών (String extraction)**: Οι δημιουργοί malware συχνά ενσωματώνουν διευθύνσεις IP, μηνύματα σφάλματος ή άλλα δεδομένα μέσα στο κακόβουλο λογισμικό σε απλό κείμενο. Η εύρεση αυτών των συμβολοσειρών μπορεί να επιτρέψει στους αναλυτές να εντοπίσουν έναν διακομιστή Command and Control (C2) ή άλλα δεδομένα που μπορεί να υποδεικνύουν τον σκοπό του malware.

4. **Μορφή Αρχείου (File format):**
Κάθε εκτελέσιμο αρχείο, είτε νόμιμο είτε όχι, έχει συσχετιζόμενα μεταδεδομένα. Οι αναλυτές malware μπορούν να εξετάσουν τον χρόνο μεταγλώττισης, τις συναρτήσεις, τις συμβολοσειρές, τα μενού και τα εικονίδια των εφαρμογών σε μορφή portable executable.
5. **Ανάλυση Packer (Packer analysis):**
Για να παρακάμψουν τα antivirus, οι δημιουργοί malware χρησιμοποιούν packers. Αυτά τα packers χρησιμοποιούν συμπίεση ή κρυπτογράφηση ώστε να μην αφήνουν ανιχνεύσιμο hash αρχείου. Υπάρχουν διαθέσιμα κάποια εργαλεία, αλλά συχνά η στατική ανάλυση σε packed malware είναι δύσκολη.
6. **Αποσυναρμολόγηση (Disassembly):**
Η αντιστροφή του κώδικα μέσω εξειδικευμένου λογισμικού επιτρέπει στους αναλυτές να δουν τον assembly κώδικα. Από εκεί, ο αναλυτής μπορεί να καθορίσει ποιες ενέργειες επιχειρεί να εκτελέσει το malware.

Σε σύγκριση με τη δυναμική ανάλυση, η στατική ανάλυση μπορεί να φαίνεται πιο χρονοβόρα. Παρόλο που γίνεται πολλή αναζήτηση και ανάλυση με το χέρι, υπάρχουν κάποια πλεονεκτήματα. Πρώτον, είναι ασφαλέστερο να εξετάζει κανείς τον κώδικα χωρίς να τον εκτελεί. Αυτό ισχύει ιδιαίτερα σε οργανισμούς όπου δεν υπάρχει πλήρης λύση sandbox. Επίσης, παρέχει πιο ολοκληρωμένη ανάλυση και καλύτερη κατανόηση των προθέσεων του δημιουργού του malware.

Υπάρχουν επίσης αρκετά μειονεκτήματα στη στατική ανάλυση. Αυτή η τεχνική απαιτεί τον πλήρη κώδικα του κακόβουλου λογισμικού για τα καλύτερα αποτελέσματα. Ένα ακόμα σημαντικό μειονέκτημα είναι ο χρόνος που απαιτείται για τη διεξαγωγή της ανάλυσης. Καθώς το malware γίνεται ολοένα και πιο σύνθετο, ο χρόνος που χρειάζεται για μια στατική ανάλυση μπορεί να είναι μεγαλύτερος από ό,τι μπορεί να αντέξει ένας οργανισμός. Αυτό αποτελεί ακόμη μεγαλύτερο πρόβλημα κατά τη διάρκεια ενός περιστατικού, όπου η ομάδα απόκρισης ενδέχεται να είναι καλύτερα εξοπλισμένη με μια ανάλυση που καλύπτει τα περισσότερα ζητήματα άμεσα, αντί να περιμένει για την πιο ολοκληρωμένη ανάλυση.

12.3. Δυναμική Ανάλυση

Στη στατική ανάλυση, η έμφαση δίνεται στην εξέταση του πιθανώς κακόβουλου λογισμικού σε ένα ελεγχόμενο περιβάλλον. Επικεντρώνεται στην ανάλυση του πραγματικού κώδικα ή στην αναζήτηση συγκεκριμένων χαρακτηριστικών αρχείων που μπορούν να συγκριθούν με άλλες πηγές. Στη δυναμική ανάλυση, η έμφαση δίνεται στην εκτέλεση του πιθανώς κακόβουλου λογισμικού μέσα σε ένα ελεγχόμενο περιβάλλον και στην παρατήρηση των συμπεριφορών που εμφανίζει το πρόγραμμα.

Υπάρχουν αρκετά πλεονεκτήματα που προσφέρει η δυναμική ανάλυση στους ερευνητές κακόβουλου λογισμικού και στις ομάδες απόκρισης περιστατικών. Καταρχάς, η πλήρης εκτέλεση του κώδικα αφαιρεί εμπόδια όπως η κρυπτογράφηση ή άλλες τεχνικές συγκαλύψεων που χρησιμοποιούνται από

τους δημιουργούς malware. Δεύτερον, υπάρχουν αρκετά αυτοματοποιημένα εργαλεία που μπορούν να αξιοποιηθούν για δυναμική ανάλυση. Αυτό μειώνει τη χειροκίνητη διαδικασία, η οποία μπορεί να είναι πολύ χρονοβόρα καθώς το malware γίνεται ολοένα και πιο περίπλοκο. Τέλος, η δυναμική ανάλυση είναι συχνά πολύ ταχύτερη, καθώς ο ερευνητής μπορεί να παρακολουθήσει σε πραγματικό χρόνο πώς λειτουργεί ένα πιθανό κακόβουλο λογισμικό σε ένα σύστημα.

Υπάρχουν δύο ευρείες κατηγορίες δυναμικής ανάλυσης malware που μπορούν να χρησιμοποιηθούν:

1. **Ανάλυση σε καθορισμένα σημεία:** Σε αυτή τη μέθοδο, ένα λειτουργικό σύστημα δοκιμής, όπως τα Windows 7, διαμορφώνεται σε ζωντανή κατάσταση παραγωγής. Οι αναλυτές καταγράφουν διάφορες ρυθμίσεις του μητρώου, διεργασίες και συνδέσεις δικτύου. Αφού ολοκληρωθεί η καταγραφή, το ύποπτο malware εκτελείται στο σύστημα. Όταν οι αναλυτές διαπιστώσουν ότι η εκτέλεση του malware ολοκληρώθηκε πλήρως, συγκρίνουν δύο σημεία του συστήματος, όπως τις τρέχουσες διεργασίες ή εντοπίζουν αλλαγές. Αυτός ο τύπος ανάλυσης μπορεί να αξιοποιήσει ορισμένες από τις δικανικές τεχνικές που αναφέρθηκαν σε προηγούμενα κεφάλαια. Για παράδειγμα, οι αναλυτές μπορούν να πάρουν ένα φρεσκοεγκατεστημένο λειτουργικό σύστημα και να πραγματοποιήσουν λήψη της μνήμης (memory capture). Η λήψη αυτή, μαζί με μια επόμενη λήψη από το μολυσμένο μηχάνημα, παρέχει στους αναλυτές σημεία σύγκρισης για τον εντοπισμό συγκεκριμένων συμπεριφορών του malware.
2. **Ανάλυση συμπεριφοράς κατά την εκτέλεση (runtime behavior analysis):** Σε αυτή τη μέθοδο, οι αναλυτές χρησιμοποιούν εργαλεία όπως το Process Explorer και άλλες βοηθητικές εφαρμογές για να παρατηρήσουν τη συμπεριφορά του ύποπτου malware κατά την εκτέλεσή του. Υπάρχουν επίσης εργαλεία που αυτοματοποιούν μεγάλο μέρος αυτής της διαδικασίας, παρέχοντας στους αναλυτές πλήρη κατανόηση του τρόπου εκτέλεσης του malware.

Παρά τα σαφή πλεονεκτήματα της δυναμικής ανάλυσης, οι ομάδες απόκρισης περιστατικών πρέπει να κατανοούν ορισμένες ανησυχίες που πρέπει να αντιμετωπιστούν πριν από την εκτέλεση ύποπτου malware σε ένα σύστημα. Καταρχάς, πρέπει να διαμορφωθεί ένα ελεγχόμενο περιβάλλον. Το ύποπτο malware δεν πρέπει ποτέ να εκτελείται σε περιβάλλον παραγωγής. Οι ερευνητές και οι ομάδες απόκρισης πρέπει να εξασφαλίζουν ότι οποιοδήποτε δοκιμαστικό ή αναλυτικό περιβάλλον είναι πλήρως απομονωμένο από το περιβάλλον παραγωγής.

Μια ακόμα ανησυχία αφορά τον αριθμό των πόρων που απαιτούνται για τη δημιουργία κατάλληλου περιβάλλοντος για δυναμική ανάλυση. Οι ερευνητές malware και οι ομάδες απόκρισης χρησιμοποιούν ένα sandbox περιβάλλον για την ανάλυση του malware. Ένα sandbox είναι απλώς ένα ελεγχόμενο περιβάλλον όπου εκτελείται το ύποπτο malware και πραγματοποιείται η αντίστοιχη ανάλυση. Για οργανισμούς που ερευνούν malware, αυτό το sandbox μπορεί να γίνει αρκετά μεγάλο, καθώς πρέπει να διατηρούνται αντίγραφα διαφόρων λειτουργικών συστημάτων και των επιπέδων ενημερώσεων (patch levels). Για παράδειγμα, για να ελέγξει ένας οργανισμός ένα δείγμα malware που επηρεάζει το Windows OS, θα πρέπει συχνά να διαθέτει περιπτώσεις Windows XP, Windows 7, Windows 8 και Windows 10 με τα αντίστοιχα patch levels. Αυτό επιτρέπει την εστίαση στα συγκεκριμένα λειτουργικά

συστήματα που επηρεάζονται από το malware. Εκτός από τα λειτουργικά συστήματα, οι αναλυτές θα χρειαστούν επίσης εικόνες της μνήμης.

12.4. Ανάλυση κακόβουλου λογισμικού

Τα εργαλεία για την ανάλυση κακόβουλου λογισμικού ποικίλλουν, από απλούς hex editors και διαδραστικούς αποσυμπίεστες (interactive disassemblers) μέχρι εργαλεία με γραφικό περιβάλλον (GUI) που ενσωματώνουν αναζητήσεις και ανάλυση στο διαδίκτυο. Κάθε περιστατικό συχνά καθορίζει τα συγκεκριμένα εργαλεία ή τεχνικές που θα χρησιμοποιηθούν. Για παράδειγμα, μια πιθανή μόλυνση μέσω email κοινωνικής μηχανικής (social engineering) που βρίσκεται στη διαδικασία μόλυνσης συστημάτων δικτύου μπορεί να απαιτεί από τους αναλυτές να δράσουν γρήγορα για να εντοπίσουν τη συμπεριφορά του κακόβουλου λογισμικού και να δημιουργήσουν μια λύση για την αφαίρεσή του. Σε άλλες περιπτώσεις, ένας μηχανισμός ασφαλείας μπορεί να έχει εντοπίσει ένα αρχείο που θεωρεί ύποπτο. Χωρίς ενεργό περιστατικό, οι αναλυτές ανταπόκρισης μπορεί να θέλουν να διασπάσουν πλήρως τον κώδικα, για να προσδιορίσουν αν είχε κάποιο συγκεκριμένο σκοπό. Σε κάθε περίπτωση, τα εργαλεία που περιγράφονται στην επόμενη ενότητα είναι χρήσιμα για την υποβοήθηση της διαδικασίας, αλλά η λίστα τους δεν είναι καθολική.

Υπάρχουν αρκετοί ιστότοποι που παρέχουν δείγματα κακόβουλου λογισμικού για εκπαίδευση και έρευνα. Για παράδειγμα, σε αυτό το κεφάλαιο, δύο δείγματα ελήφθησαν από τον ιστότοπο <http://malware-traffic-analysis.net/>. Αυτά τα αρχεία μπορούν να ληφθούν σε μορφή ZIP. Ως γενικός κανόνας, κάθε δείγμα κακόβουλου λογισμικού θα προστατεύεται με κωδικό πρόσβασης που είναι η λέξη **infected**.

Πριν αναλάβετε την ανάλυση, βεβαιωθείτε ότι το σύστημα που θα χρησιμοποιηθεί είναι σωστά απομονωμένο από το δίκτυο και ότι το anti-virus είναι απενεργοποιημένο. Μια τεχνική είναι να χρησιμοποιηθεί μια εικονική μηχανή (virtual machine) που μπορεί να δημιουργηθεί snapshot πριν από τη χρήση και να επανέλθει σε αυτή την κατάσταση μετά την ανάλυση.

12.5. ClamAV

Ένα πρώτο βήμα στην **στατική ανάλυση** είναι να προσδιοριστεί αν το πιθανό κακόβουλο λογισμικό που αναλύεται έχει ήδη εντοπιστεί στο παρελθόν. Ένα μοναδικό δείγμα μπορεί να συγκριθεί με βάση το **hash** του σε ιστότοπους όπως το VirusTotal. Ωστόσο, αν ένας αναλυτής έχει συγκεντρώσει πολλά αρχεία κατά την ανάλυση, χρειάζεται τρόπος να προσδιορίσει ποια από αυτά αξίζει να εξεταστούν περαιτέρω.

Μια τεχνική είναι η χρήση ενός εμπορικού antivirus για σάρωση του φακέλου με τα αρχεία. Στην περίπτωση αυτή, ένα **δωρεάν, ανοιχτού κώδικα εργαλείο** που μπορεί να χρησιμοποιηθεί είναι το **ClamAV**.

Το **ClamAV** είναι ένα εργαλείο γραμμής εντολών (command-line utility) που επιτρέπει στους αναλυτές να σαρώσουν φακέλους με διάφορους τύπους ύποπτων αρχείων. Τα αρχεία που εντοπίζονται ως ύποπτα μπορούν στη συνέχεια να αναλυθούν περαιτέρω.

Οδηγίες χρήσης ClamAV:

1. Μεταβείτε στη σελίδα λήψης του ClamAV: <https://www.clamav.net/downloads>
2. Κατεβάστε την έκδοση που αντιστοιχεί στο λειτουργικό σας σύστημα. Για Windows, η έκδοση που θα χρησιμοποιηθεί είναι: ClamAV-0.102.1.exe
3. Ακολουθήστε τις οδηγίες για τη **διαμόρφωση και ενημέρωση του signature αρχείου**: Installing ClamAV on Windows
4. Ανοίξτε ένα **Command Prompt** ή **Windows PowerShell**
5. Για παράδειγμα, αρχεία από τον ιστότοπο Malware Traffic Analysis μπορούν να εξεταστούν. Τα αρχεία βρίσκονται εδώ: Malware Traffic Analysis – 2019/09/04. Στο τερματικό, πληκτρολογήστε:

```
PS C:\Program Files\ClamAV> .\clamav.exe -m D:\MalwareSamples\2019-09-04-malware-from-Ursnif-and-Trickbot-infection
```

6. Η εντολή αυτή εκτελεί τον scanner ClamAV σε όλα τα αρχεία του φακέλου 2019-09-04-malware-from-Ursnif-and-Trickbot-infection. Πατήστε **Enter** για να δείτε τα αποτελέσματα.

```
2019-09-04-Windows-registry-updates-caused-by-Ursnif.txt: OK
2019-09-04-Word-doc-from-password-protected-zip-archive.doc: Doc.Malware.Sagent-7159046-0 FOUND
```

7. Το ClamAV εντοπίζει, για παράδειγμα, ότι ένα αρχείο .doc αντιστοιχεί στη **malware signature** Doc.Malware.Sagent-7159046.

Η αποτελεσματικότητα του ClamAV εξαρτάται σε μεγάλο βαθμό από τα **signature** που περιλαμβάνονται στο πακέτο σάρωσης. Ορισμένα malware μπορεί να μην έχουν αντίστοιχη signature και, επομένως, να μην εντοπιστούν. Παρόλα αυτά, το ClamAV παραμένει χρήσιμο εργαλείο για τη **σαρώση μεγάλου όγκου πιθανών malware αρχείων** και την **αναγνώριση αυτών που είναι ήδη γνωστά**.

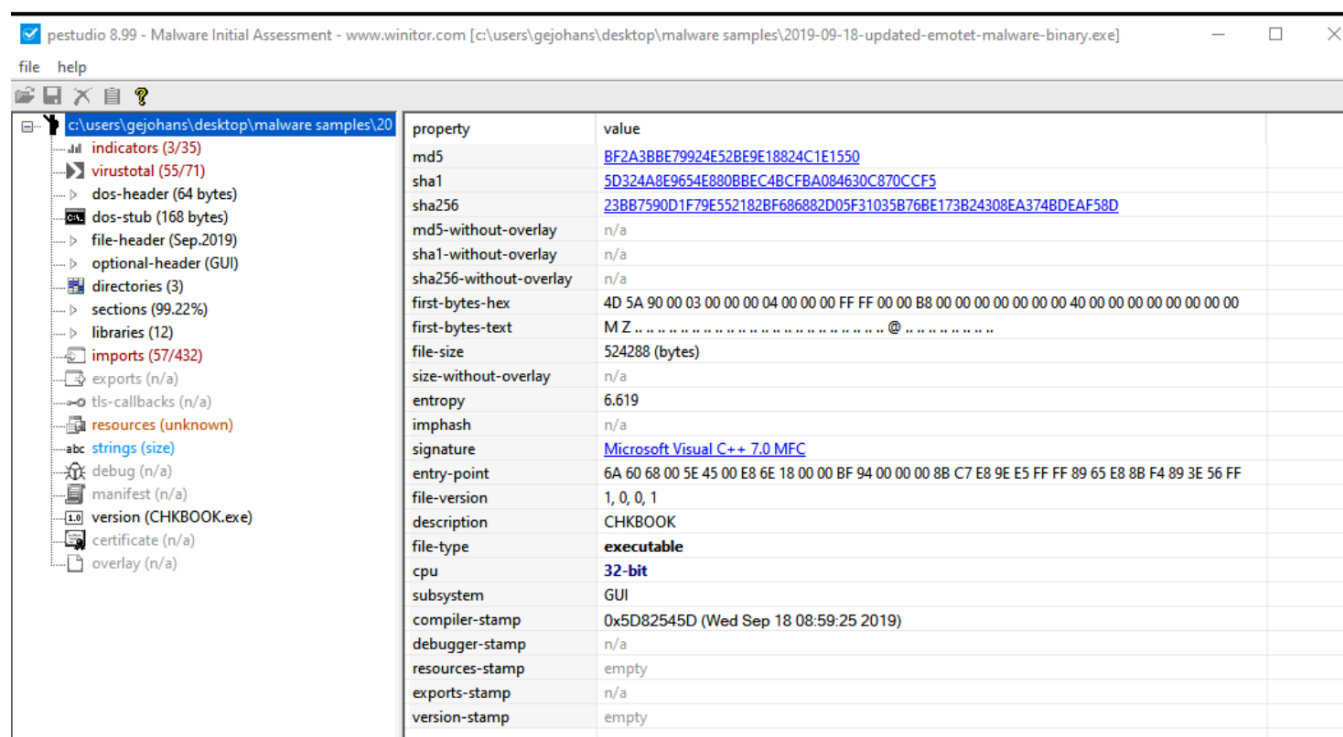
12.6. PeStudio

Ένα καλό σημείο για να ξεκινήσει κανείς την στατική ανάλυση ενός μεμονωμένου αρχείου είναι με το **PeStudio**. Στο Κεφάλαιο 8, «Ανάλυση Μνήμης Συστήματος», παρουσιάστηκε αυτή η εφαρμογή κατά την εξέταση ύποπτου κακόβουλου λογισμικού που αποκτήθηκε μέσω της ανάλυσης μιας εικόνας μνήμης. Σε αυτή την περίπτωση, θα αναλυθεί ένα πραγματικό δείγμα κακόβουλου λογισμικού χρησιμοποιώντας το PeStudio. Το εργαλείο αυτό επιτρέπει στους αναλυτές να επικεντρωθούν σε συγκεκριμένα χαρακτηριστικά του malware για περαιτέρω ανάλυση.

Σε αυτό το σενάριο, θα εξεταστεί ένα ζωντανό δείγμα κακόβουλου λογισμικού. Το δείγμα malware είναι μια μόλυνση **Emotet** σε συνδυασμό με **TrickBot**. Το δείγμα αυτό ελήφθη από τη διεύθυνση: <https://www.malware-traffic-analysis.net/2019/09/18/index.html>.

Βεβαιωθείτε ότι έχει γίνει η σωστή προκαθορισμένη ρύθμιση πριν από τη λήψη οποιουδήποτε malware, καθώς οποιοδήποτε πρόγραμμα antivirus θα θέσει το malware σε καραντίνα, καθιστώντας οποιαδήποτε ανάλυση αδύνατη. Μόλις το αρχείο ληφθεί σε έναν φάκελο, είναι έτοιμο για ανάλυση. Ακολουθήστε τα παρακάτω βήματα:

1. Ανοίξτε το **PeStudio**. Κάντε κλικ στο εικονίδιο φακέλου στην επάνω αριστερή γωνία και πλοηγηθείτε στο δείγμα malware με το όνομα αρχείου: 2019-09-18-updated-Emotet-malware-binary.exe.
2. Αφού φορτωθεί, θα εμφανιστεί το ακόλουθο παράθυρο. Στο αριστερό τμήμα υπάρχουν αρκετά στοιχεία που το PeStudio εξετάζει σε σχέση με το malware. Ορισμένα από αυτά τα στοιχεία (σε κόκκινο) υποδηλώνουν ότι ο κώδικας θεωρείται ύποπτος για περιέχον malware, όπως φαίνεται εδώ:



3. Κάντε πρώτα κλικ στα **indicators (δείκτες)** για να αποκτήσετε μια επισκόπηση των συγκεκριμένων στοιχείων του malware που έχουν αναγνωριστεί ως κακόβουλα. Το PeStudio έχει εντοπίσει τρεις συγκεκριμένους δείκτες:
 - ο Το αρχείο έχει 55/71 ανιχνεύσεις στο VirusTotal,
 - ο Υπάρχουν αρκετά strings που βρίσκονται σε blacklist, και

- ο Τέλος, το αρχείο εισάγει σύμβολα που βρίσκονται σε blacklist, όπως φαίνεται στο σχετικό στιγμιότυπο οθόνης.

1430	The file references string(s) tagged as blacklist	count: 85	1
1120	The file is scored by virustotal	score: 55/71	1
1266	The file imports symbol(s) tagged as blacklist	count: 57	1

4. Κάντε κλικ στα **imports (εισαγωγές)**. Από εδώ, ο αναλυτής μπορεί να δει τα βιβλιοθήκες (library files) που εισάγονται και βρίσκονται σε blacklist, όπως φαίνεται στο στιγμιότυπο οθόνης.

name (432)	group (14)	MITRE-Technique (5)	type (1)	anonymous (6)	blacklist (57)
GetCapture	windowing	-	implicit	-	x
GetClassLongA	windowing	-	implicit	-	x
GetForegroundWindow	windowing	-	implicit	-	x
SetForegroundWindow	windowing	-	implicit	-	x
SetWindowLongA	windowing	-	implicit	-	x
GetDesktopWindow	windowing	-	implicit	-	x
GetTimeZoneInformation	system-information	-	implicit	-	x
GetVolumeInformationA	storage	-	implicit	-	x
WinHelpA	shell	-	implicit	-	x
EnumResourceLanguagesA	resource	-	implicit	-	x
LockResource	resource	-	implicit	-	x
WritePrivateProfileStringA	registry	-	implicit	-	x
RegDeleteValueA	registry	T1112	implicit	-	x
RegSetValueA	registry	T1112	implicit	-	x
RegDeleteKeyA	registry	T1112	implicit	-	x
RegEnumKeyA	registry	T1012	implicit	-	x
RegCreateKeyA	registry	-	implicit	-	x
RegSetValueExA	registry	T1112	implicit	-	x
VirtualProtect	memory	-	implicit	-	x
GetKeyState	keyboard-and-mouse	-	implicit	-	x
SetWindowsHookExA	hooking	T1179	implicit	-	x
CallNextHookEx	hooking	T1179	implicit	-	x
UnhookWindowsHookEx	hooking	T1179	implicit	-	x
GetShortPathNameA	file	-	implicit	-	x
FindFirstFileA	file	-	implicit	-	x
FindClose	file	-	implicit	-	x

5. Κάντε κλικ στα **strings**. Αυτό δίνει στους αναλυτές μια σαφή εικόνα των διαφόρων συμβολοσειρών (strings) εντός του malware που είναι ύποπτες. Από εδώ, ο αναλυτής μπορεί να επικεντρωθεί σε αυτές τις strings κατά την διεξαγωγή βαθύτερης ανάλυσης, όπως φαίνεται στο στιγμιότυπο οθόνης.

unicode	6	0x000694A5	x	x	Port :
unicode	64	0x0006BE13	x	x	No error occurred.-An unknown error occurred while accessing %1.
ascii	13	0x0005F6AD	x	-	SetWindowLong
ascii	19	0x0005F7E8	x	-	SetForegroundWindow
ascii	19	0x0005F96C	x	-	GetForegroundWindow
ascii	12	0x0005FA11	x	-	GetClassLong
ascii	10	0x0005FA58	x	-	GetCapture
ascii	16	0x0005FC84	x	-	GetDesktopWindow
ascii	18	0x0005138D	x	-	EnumDisplayDevices
ascii	19	0x000513B0	x	-	EnumDisplayMonitors
ascii	22	0x0005F22C	x	-	GetTimeZoneInformation
ascii	20	0x0005EE8D	x	-	GetVolumeInformation
ascii	7	0x0005FA67	x	-	WinHelp
ascii	12	0x0005041C	x	-	LockResource
ascii	12	0x0005EB4A	x	-	LockResource
ascii	21	0x0005ED65	x	-	EnumResourceLanguages
ascii	25	0x0005EF43	x	-	WritePrivateProfileString
ascii	11	0x00060495	x	-	RegSetValue
ascii	12	0x000604FF	x	-	RegDeleteKey
ascii	10	0x0006050F	x	-	RegEnumKey
ascii	13	0x00060541	x	-	RegSetValueEx

Το PeStudio επιτρέπει στους αναλυτές περιστατικών (incident responders) να αποκτήσουν μια επισκόπηση σε **υψηλό επίπεδο** (10.000 πόδια) πάνω στο ύποπτο malware. Συχνά, αυτό μπορεί να είναι αρκετό για να δουλέψουν οι αναλυτές, όσον αφορά την ταυτοποίηση άλλων μολύνσεων. Σε άλλα περιστατικά, μπορεί να είναι απαραίτητο να πραγματοποιηθεί βαθύτερη ανάλυση, όπου εμπλέκονται και άλλα εργαλεία.

12.7. REMnux

Το REMnux είναι ένα δωρεάν εργαλείο βασισμένο σε γραμμή εντολών για την ανάλυση κακόβουλου λογισμικού. Αναπτύχθηκε και συντηρείται από τον Lenny Zeltser και διαθέτει διάφορα εργαλεία που επιτρέπουν στους αναλυτές να εξετάζουν ύποπτα έγγραφα, JavaScript και άλλα αντικείμενα που σχετίζονται με κακόβουλο λογισμικό. Επιπλέον, υπάρχουν εργαλεία όπως το Wireshark που μπορούν να χρησιμοποιηθούν όχι μόνο για την ανάλυση του κακόβουλου λογισμικού αλλά και για την αναγνώριση συνδέσεων ή κυκλοφορίας δικτύου.

Πληροφορίες για το REMnux βρίσκονται στην ιστοσελίδα <https://remnux.org/> και μπορεί να κατεβεί σε μορφή αρχείου OVA από εδώ.

Μόλις κατέβει, το αρχείο μπορεί να μετατραπεί από το λογισμικό εικονικοποίησης που έχει επιλέξει ο αναλυτής. Στην επιφάνεια εργασίας υπάρχουν δύο συνδέσεις σε αρχεία .html και ένα έγγραφο PDF που περιέχει όλες τις απαραίτητες πληροφορίες για να πραγματοποιηθεί η ανάλυση. Για να ξεκινήσει η ανάλυση, κάντε κλικ στο εικονίδιο του Terminal, και θα εμφανιστεί ένα παράθυρο εικονιδίων. Για τις περισσότερες εντολές, η συνήθης μορφή είναι η εξής:

```
remnux@remnux:~$ <Εντολή><Αρχείο Κακόβουλου Λογισμικού>
```


Στο παρακάτω παράδειγμα, θα αναλυθεί ένα εκτελέσιμο αρχείο κακόβουλο λογισμικού. Σε αυτήν την περίπτωση, το αρχείο θα είναι ένα δυαδικό αρχείο που σχετίζεται με το Ursnif doc. Το αρχείο μπορεί να βρεθεί στη διεύθυνση <https://www.malwaretraffic-analysis.net/2019/09/04/index.html>. Και πάλι, βεβαιωθείτε ότι λαμβάνονται τα κατάλληλα μέτρα ασφαλείας όταν εργάζεστε με κακόβουλο λογισμικό. Ένα πλεονέκτημα του REMnux ως πλατφόρμα Linux είναι ότι υπάρχει μικρός κίνδυνος να κατέβει απευθείας ένα Windows-based malware δείγμα στο σύστημα.

Μόλις το αρχείο τοποθετηθεί σωστά, μπορεί να εκτελεστεί η εντολή pescanner πάνω στο αρχείο. Το pescanner είναι ένα εργαλείο που εξετάζει στατικά ένα αρχείο μορφής PE. Για να εκτελεστεί το εργαλείο, χρησιμοποιείται η εξής εντολή:

```
remnux@remnux:~$ pescanner 2019-09-04-initial-Ursnif-binary.exe
```

Η εντολή παρέχει πολλές πληροφορίες. Αρχικά εμφανίζει τα μεταδεδομένα, όπως το hash του αρχείου, το μέγεθος του δυαδικού αρχείου και την αρχιτεκτονική για την οποία έχει προγραμματιστεί, όπως φαίνεται στο αντίστοιχο στιγμιότυπο οθόνης.

```
remnux@remnux:~/MalwareSamples$ pescanner 2019-09-04-initial-Ursnif-binary.exe
#####
[0] File: 2019-09-04-initial-Ursnif-binary.exe
#####

Meta-data
=====
Size           : 300032 bytes
Type           : PE32 executable (GUI) Intel 80386, for MS Windows
Architecture   : 32 Bits binary
MD5            : b2490c2f4f8d22ddb34b4cbeed3c69b3
SHA1           : 59154cb6a203e00fbe0431281b2bb33e1b00061a
ssdeep        : 6144:TJ8mth3sLtIAqj3FVzpe5ZFzbLXLe86HGrHnQ2Jx:uWJsIY5ZFzPy86H0HH
imphash        : 0e1c43d49561655b09b5f1bc6792fa38
Date           : 0x4AA0FBD5 [Fri Sep  4 11:36:53 2009 UTC]
Language       : ENGLISH
CRC: (Claimed) : 0x0, (Actual): 0x54247 [SUSPICIOUS]
Entry Point    : 0x4207ae .text 0/5
```

Ένα ακόμα σημαντικό σημείο είναι ότι το REMnux εντόπισε ότι το CRC (Cyclic Redundancy Check) δεν ταιριάζει, γεγονός που υποδεικνύει ύποπτη συμπεριφορά. Έλεγχοι CRC χρησιμοποιούνται συνήθως για την ανίχνευση σφαλμάτων ή αλλαγών στα δεδομένα μέσα στον κώδικα λογισμικού, χρησιμοποιώντας μια συνάρτηση κατακερματισμού (hashing function). Σε αυτήν την περίπτωση, τα μεταδεδομένα του εκτελέσιμου δείχνουν ότι το CRC είναι 0x0, ενώ στην πραγματικότητα είναι 0x54247. Αυτή η ανωμαλία είναι ακόμα ένας δείκτης που μπορεί να υποδηλώνει ότι το αρχείο είναι κακόβουλο.

Άλλες πληροφορίες περιλαμβάνουν τις οδηγίες που έχει προγραμματιστεί να εκτελεί το κακόβουλο λογισμικό.

Offset	Instructions
0	call 0x423e7c
5	jmp 0x420631
10	push byte 0xc
12	push dword 0x43b3e0
17	call 0x4210f0
22	and dword [ebp-0x1c], 0x0
26	mov esi, [ebp+0x8]
29	cmp esi, [0x44e2d0]
35	ja 0x4207f5
37	push byte 0x4
39	call 0x42408e
44	pop ecx
45	and dword [ebp-0x4], 0x0
49	push esi
50	call 0x4248a0
55	pop ecx
56	mov [ebp-0x1c], eax
59	mov dword [ebp-0x4], 0xffffffff
66	call 0x4207fe
71	mov eax, [ebp-0x1c]
74	call 0x421135
79	ret
80	push byte 0x4
82	call 0x423fb4
87	pop ecx
88	ret
89	mov edi, edi
91	push ebp
92	mov ebp, esp
94	push esi
95	mov esi, [ebp+0x8]
98	cmp esi, 0x0

Στη συνέχεια, το rescanner εντόπισε τις περιοχές μνήμης που χρησιμοποιούνται από το κακόβουλο λογισμικό. Υπάρχει επίσης μια ενότητα που δείχνει την εντροπία συγκεκριμένων περιοχών. Υψηλή εντροπία υποδηλώνει ότι ένα αρχείο είναι συμπιεσμένο ή κρυπτογραφημένο. Σε αυτή την περίπτωση, το rescanner δείχνει ότι δεν υπάρχει κάποια συγκεκριμένη περιοχή μνήμης που θεωρείται ύποπτη, καθώς βρίσκεται εντός των φυσιολογικών ορίων εντροπίας.

Sections

Name	VirtAddr	VirtSize	RawSize	MD5	Entropy
.text	0x1000	0x2e9c7	0x2ea00	ea80d5c83da498d1b76c537bdfc80370	6.717635
.rdata	0x30000	0xdc66	0xde00	0f5ff6da63a54786b653ce46fe4c1830	5.805477
.data	0x3e000	0x1041c	0x4c00	a5297d66be916d217b1f5f18812916a5	5.463237
.rsrc	0x4f000	0x530	0x600	15f94e54fda75a4b78243579f4c48870	3.658907
.reloc	0x50000	0x742a	0x7600	8e489f790699d5a7eda31642e180e611	2.852141

Κατεβαίνοντας στα αποτελέσματα, το rescanner δείχνει ποια αρχεία δυναμικών βιβλιοθηκών (DLL) εισάγονται από το κακόβουλο λογισμικό. Από αυτά, ο αναλυτής μπορεί να προσδιορίσει περισσότερα για τη συμπεριφορά του κακόβουλου αρχείου, εξετάζοντας τα συγκεκριμένα αρχεία.

Imports

```
=====
[1] KERNEL32.dll
[2] USER32.dll
[3] WINSPOOL.DRV
[4] COMCTL32.dll
[5] ole32.dll
[6] OLEAUT32.dll
[7] SHLWAPI.dll
[8] ADVAPI32.dll
[9] CLUSAPI.dll
[10] OLEACC.dll
[11] GDI32.dll
```

Τέλος, το rescanner θα υποδείξει ποιες ύποπτες εγγραφές του Import Address Table (IAT) καλούνται από το κακόβουλο λογισμικό. Αυτό επιτρέπει στους αναλυτές να προσδιορίσουν τη συμπεριφορά του κακόβουλου κώδικα και πιθανώς ποιες ενέργειες εκτελεί στο μολυσμένο σύστημα, εξετάζοντας αυτές τις εγγραφές.

Suspicious IAT alerts

```
=====
[1] CreateDirectoryW
[2] CreateFileA
[3] CreateFileW
[4] FindResourceW
[5] GetCommandLineW
[6] GetModuleFileNameA
[7] GetModuleFileNameW
[8] GetModuleHandleA
[9] GetModuleHandleW
[10] GetProcAddress
[11] GetStartupInfoA
[12] GetStartupInfoW
[13] GetTickCount
```

Με τον μεγάλο αριθμό εργαλείων που διαθέτει, το REMnux αποτελεί εξαιρετική πηγή για την εκτέλεση διαφόρων εργασιών σχετικών με την εξέταση αρχείων. Επιπλέον, το REMnux περιλαμβάνει εργαλεία όπως τα Rekall και Volatility, ώστε οι αναλυτές να μπορούν να εκτελούν ένα πλήθος εργασιών από την ανάλυση εικόνας μνήμης σε συνδυασμό με την ανάλυση κακόβουλου λογισμικού.

12.8. YARA Rules

Ένα ακόμη εργαλείο με το οποίο οι ανταποκριτές θα πρέπει να είναι εξοικειωμένοι όσον αφορά την ανάλυση κακόβουλου λογισμικού είναι το εργαλείο αντιστοίχισης προτύπων YARA. Το YARA (συντομογραφία του Yet Another Ridiculous Acronym) είναι ένα σχήμα για την αναγνώριση και ταξινόμηση κακόβουλου λογισμικού, μέσω της δημιουργίας κανόνων βασισμένων σε κείμενο. Οι κανόνες YARA είναι ένας συνδυασμός συμβολοσειρών και λογικών εκφράσεων που συνδέονται με μια συνθήκη, για να προσδιοριστεί αν ένα συγκεκριμένο αρχείο περιέχει οποιοδήποτε από τα χαρακτηριστικά που περιλαμβάνονται στον κανόνα YARA.

Για παράδειγμα, ο ακόλουθος κανόνας YARA δημιουργήθηκε από τον Florian Roth για το κακόβουλο λογισμικό Stuxnet και είναι διαθέσιμος στο https://github.com/Yara-Rules/rules/blob/master/malware/APT_Stuxnet.yar. Ο κανόνας αυτός έχει γραφτεί για να εξετάσει ένα ύποπτο αρχείο για πλήρεις λέξεις που σχετίζονται με το Stuxnet, και ο κώδικας φαίνεται εδώ:

```
rule Stuxnet_Malware_3
{
  meta:
    description = "Stuxnet Sample - file ~WTR4141.tmp"
    author = "Florian Roth"
    reference = "Internal Research"
    date = "2016-07-09"
    hash1 = "6bcf88251c876ef00b2f32cf97456a3e306c2a263d487b0a50216c6e3cc07c6a"
    hash2 = "70f8789b03e38d07584f57581363afa848dd5c3a197f2483c6dfa4f3e7f78b9b"
    strings:
      $x1 = "SHELL32.DLL.ASLR." fullword wide
      $s1 = "~WTR4141.tmp" fullword wide
      $s2 = "~WTR4132.tmp" fullword wide
      $s3 = "totalcmd.exe" fullword wide
      $s4 = "wincmd.exe" fullword wide
      $s5 = "http://www.realtek.com0" fullword ascii
      $s6 = "{%08x-%08x-%08x-%08x}" fullword wide
    condition:
      ( uint16(0) == 0x5a4d and filesize < 150KB and ( $x1 or 3 of ($s*) ) )
      or ( 5 of them )
}
```

Ο παραπάνω κανόνας έχει γραφτεί ώστε να ενεργοποιείται αν το μέγεθος του αρχείου είναι μικρότερο από 150 KB, και αν είτε η πλήρης συμβολοσειρά SHELL32.DLL.ASLR είτε τρεις από τις συμβολοσειρές \$s* εντοπιστούν στο αρχείο. Οι κανόνες YARA μπορούν να γραφτούν σε έναν απλό επεξεργαστή κειμένου ως μεμονωμένος κανόνας ή πολλαπλοί κανόνες μέσα στο ίδιο αρχείο YARA.

Οι κανόνες YARA μπορούν να χρησιμοποιηθούν με διάφορους τρόπους. Πρώτον, μπορούν να δημιουργηθούν βασισμένοι στην στατική ανάλυση κακόβουλου λογισμικού ή εκμεταλλεύσεων και να χρησιμοποιηθούν για την ανίχνευση εικόνων μνήμης μέσω του plugin yarascan του Volatility. Αυτό επιτρέπει στους ανταποκριτές να προσδιορίζουν αν υπάρχουν ίχνη ενός συγκεκριμένου κακόβουλου λογισμικού σε μια εικόνα μνήμης. Δεύτερον, πολλαπλοί κανόνες μπορούν να εκτελεστούν σε αρχεία και εικόνες δίσκου για να ανιχνευθεί η παρουσία κακόβουλου λογισμικού ή εκμεταλλεύσεων. Υπάρχουν επίσης σαρωτές όπως το Loki, διαθέσιμο στο <https://github.com/Neo23x0/Loki>, που χρησιμοποιούν πολλούς κανόνες YARA για να σαρώσουν ζωντανούς δίσκους για δείκτες παραβίασης (IoCs).

Η συγγραφή κανόνων YARA μπορεί μερικές φορές να δημιουργήσει πρόβλημα κατά τη διάρκεια ενός περιστατικού. Αυτό οφείλεται στο γεγονός ότι απαιτούνται και άλλες τεχνικές ανάλυσης κακόβουλου λογισμικού, όπως το PeStudio ή το rescanner, για την εξαγωγή συμβολοσειρών και άλλων δεικτών. Μια άλλη επιλογή σχετικά με τους κανόνες YARA είναι το εργαλείο yarGen του Florian Roth. Αυτό το

script σε Python, διαθέσιμο στο <https://github.com/Neo23x0/yarGen>, επιτρέπει στους ανταποκριτές να δημιουργούν κανόνες YARA για συγκεκριμένα αρχεία που έχουν εντοπιστεί κατά τη διάρκεια ενός περιστατικού.

Για το παράδειγμα αυτό, ένα αρχείο που σχετίζεται με το σετ αρχείων malware της 2019-09-04 από Ursnif και Trickbot περιείχε ένα έγγραφο Microsoft Word. Οι δείκτες που εξήχθησαν από αυτό το αρχείο μπορεί να είναι χρήσιμοι για την ανάλυση άλλων συστημάτων. Το yarGen μπορεί να χρησιμοποιηθεί για να δημιουργηθεί ένας κανόνας από αυτό το αρχείο. Η διαδικασία είναι η εξής:

1. Κατεβάστε το yarGen από το GitHub: <https://github.com/Neo23x0/yarGen>.
2. Αποσυμπιέστε το αρχείο ZIP.
3. Μεταβείτε στον κατάλογο που περιέχει το script yarGen.py. Είναι καλή πρακτική να τοποθετούνται τα δείγματα σε έναν μόνο κατάλογο, καθώς το yarGen λειτουργεί με τα αρχεία που βρίσκονται μέσα σε έναν κατάλογο.
4. Χρησιμοποιήστε την ακόλουθη σύνταξη εντολής για να δημιουργήσετε τον κανόνα YARA. Σε αυτή την περίπτωση, το -m υποδεικνύει στο yarGen να σαρώσει τον κατάλογο Malware για τα αρχεία για τα οποία θα δημιουργηθεί ο κανόνας. Το -o είναι το αρχείο εξόδου, συνήθως ένα αρχείο κειμένου με την επέκταση .yar:

```
remnux@remnux:~/Desktop/yarGen-master$ python yarGen.py -m Malware -o sample.yar
```

[illegible]

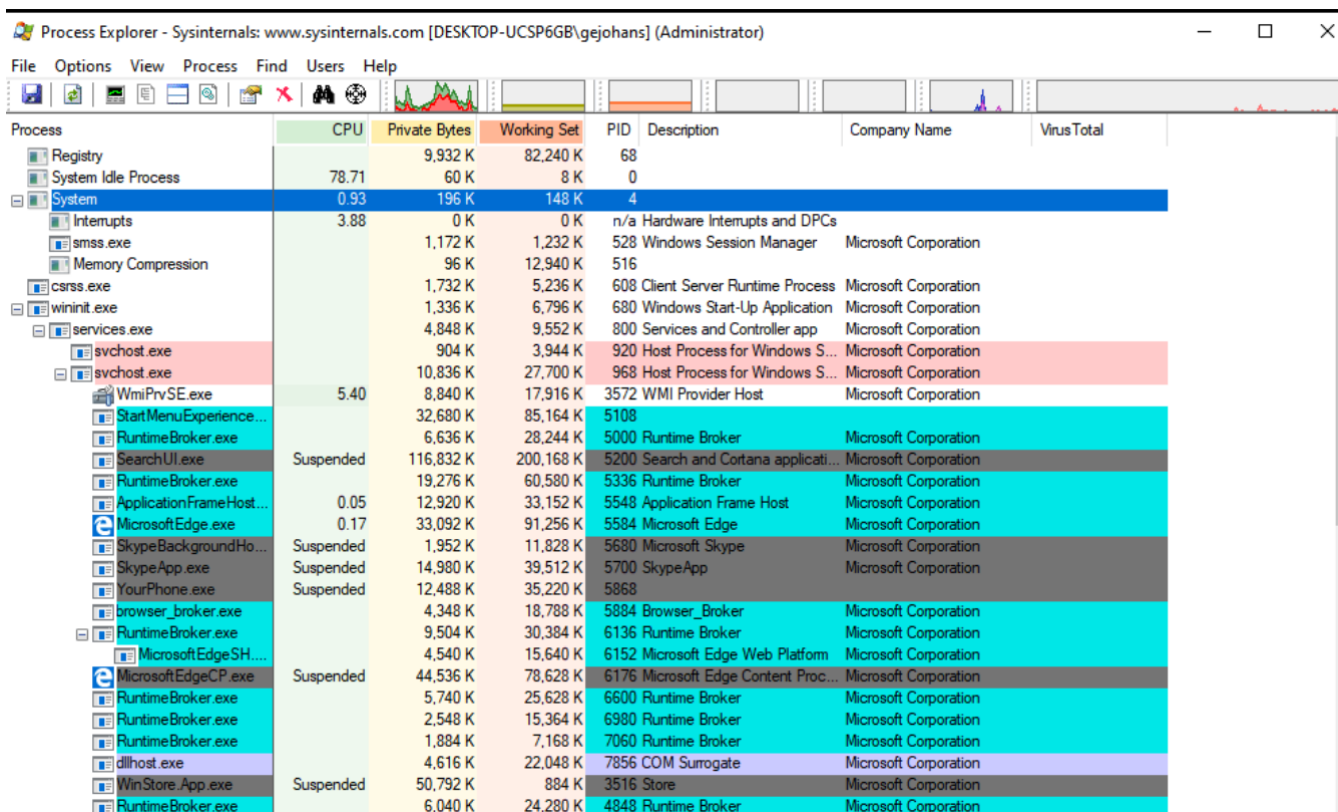
Το script θα εκτελεστεί και στη συνέχεια θα δημιουργήσει έναν κανόνα YARA όπως ο παραπάνω. Το yarGen έχει πάρει τις διάφορες συμβολοσειρές που σχετίζονται με το συγκεκριμένο αρχείο και έχει δημιουργήσει τον κανόνα. Το yarGen αποτελεί μια καλή επιλογή για τους ανταποκριτές σε περίπτωση που ασχολούνται με πολλά συστήματα ή αρχεία και δεν διαθέτουν τον απαραίτητο χρόνο για πλήρη στατική ανάλυση για την εξαγωγή συμβολοσειρών.

Αυτή ήταν μια πολύ περιορισμένη διερεύνηση του YARA και των δυνατοτήτων του. Οι κανόνες YARA αποτελούν ένα ισχυρό εργαλείο που μπορεί να αξιοποιηθεί κατά τη διάρκεια ενός περιστατικού. Καθώς οι κανόνες μπορούν να δημιουργηθούν όχι μόνο για κακόβουλο λογισμικό αλλά για οποιοδήποτε αρχείο, οι ανταποκριτές έχουν τη δυνατότητα να σαρώσουν άλλα συστήματα για IoCs που σχετίζονται με εκμεταλλεύσεις ή scripts που έχει χρησιμοποιήσει ένας αντίπαλος ως μέρος της επίθεσής του, τα οποία μπορεί να έχουν παρακάμψει antivirus ή άλλα ελεγκτικά μέτρα.

12.9. Process Explorer

Ένα από τα βασικά εργαλεία που επιτρέπει λεπτομερή ανάλυση κακόβουλου λογισμικού κατά την εκτέλεσή του είναι το **Process Explorer**. Αυτό το εργαλείο αποτελεί μέρος της σουίτας εργαλείων **Windows Sysinternals** και παρέχει μια δωρεάν πλατφόρμα στους αναλυτές για να αποκτήσουν μια εικόνα για το τι εκτελεί κάθε διαδικασία και ποια είναι η γονική της διαδικασία, καθώς και για την παρακολούθηση της χρήσης της CPU. Απλώς κατεβάστε την εφαρμογή από τον ακόλουθο ιστότοπο: <https://technet.microsoft.com/en-us/sysinternals/procexpexplorer.aspx>.

Αποσυμπίστε τα περιεχόμενα και στη συνέχεια κάντε διπλό κλικ στην έκδοση του **Process Explorer** (32-bit ή 64-bit) που αντιστοιχεί στο σύστημά σας. Θα εμφανιστεί το παρακάτω παράθυρο:



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal
Registry		9,932 K	82,240 K	68			
System Idle Process	78.71	60 K	8 K	0			
System	0.93	196 K	148 K	4			
Interrupts	3.88	0 K	0 K	n/a	Hardware Interrupts and DPCs		
smss.exe		1,172 K	1,232 K	528	Windows Session Manager	Microsoft Corporation	
Memory Compression		96 K	12,940 K	516			
csrss.exe		1,732 K	5,236 K	608	Client Server Runtime Process	Microsoft Corporation	
wininit.exe		1,336 K	6,796 K	680	Windows Start-Up Application	Microsoft Corporation	
services.exe		4,848 K	9,552 K	800	Services and Controller app	Microsoft Corporation	
svchost.exe		904 K	3,944 K	920	Host Process for Windows S...	Microsoft Corporation	
svchost.exe		10,836 K	27,700 K	968	Host Process for Windows S...	Microsoft Corporation	
WmiPrvSE.exe	5.40	8,840 K	17,916 K	3572	WMI Provider Host	Microsoft Corporation	
StartMenuExperience...		32,680 K	85,164 K	5108			
RuntimeBroker.exe		6,636 K	28,244 K	5000	Runtime Broker	Microsoft Corporation	
SearchUI.exe	Suspended	116,832 K	200,168 K	5200	Search and Cortana applicati...	Microsoft Corporation	
RuntimeBroker.exe		19,276 K	60,580 K	5336	Runtime Broker	Microsoft Corporation	
ApplicationFrameHost...	0.05	12,920 K	33,152 K	5548	Application Frame Host	Microsoft Corporation	
MicrosoftEdge.exe	0.17	33,092 K	91,256 K	5584	Microsoft Edge	Microsoft Corporation	
SkypeBackgroundHo...	Suspended	1,952 K	11,828 K	5680	Microsoft Skype	Microsoft Corporation	
SkypeApp.exe	Suspended	14,980 K	39,512 K	5700	SkypeApp	Microsoft Corporation	
YourPhone.exe	Suspended	12,488 K	35,220 K	5868			
browser_broker.exe		4,348 K	18,788 K	5884	Browser_Broker	Microsoft Corporation	
RuntimeBroker.exe		9,504 K	30,384 K	6136	Runtime Broker	Microsoft Corporation	
MicrosoftEdgeSH...		4,540 K	15,640 K	6152	Microsoft Edge Web Platform	Microsoft Corporation	
MicrosoftEdgeCP.exe	Suspended	44,536 K	78,628 K	6176	Microsoft Edge Content Proc...	Microsoft Corporation	
RuntimeBroker.exe		5,740 K	25,628 K	6600	Runtime Broker	Microsoft Corporation	
RuntimeBroker.exe		2,548 K	15,364 K	6980	Runtime Broker	Microsoft Corporation	
RuntimeBroker.exe		1,884 K	7,168 K	7060	Runtime Broker	Microsoft Corporation	
dllhost.exe		4,616 K	22,048 K	7856	COM Surrogate	Microsoft Corporation	
WinStore.App.exe	Suspended	50,792 K	884 K	3516	Store	Microsoft Corporation	
RuntimeBroker.exe		6,040 K	24,280 K	4848	Runtime Broker	Microsoft Corporation	

Όπως φαίνεται, υπάρχουν αρκετά βασικά στοιχεία διαθέσιμα για τον αναλυτή. Το κύριο πλεονέκτημα αυτού του εργαλείου είναι η **οπτική αναπαράσταση**. Αντί να προσπαθεί ο αναλυτής να

χρησιμοποιήσει εγγενή εργαλεία των Windows ή άλλα εργαλεία ανάλυσης μνήμης μετά τη λήψη, μπορεί να δει γρήγορα αν κάποια διαδικασία φαίνεται ύποπτη.

Οι αναλυτές έχουν τη δυνατότητα να στείλουν μια διαδικασία και τα συνοδευτικά δεδομένα της στο VirusTotal. Αν εντοπιστεί κάποια ύποπτη διαδικασία, το Process Explorer θα στείλει τις πληροφορίες στον ιστότοπο για ανάλυση και σύγκριση. Αν εντοπιστεί μια διαδικασία, κάντε κλικ πάνω της στο παράθυρο, πλοηγηθείτε στο **Process** και επιλέξτε **Check VirusTotal**. Τα αποτελέσματα θα εμφανιστούν ως αριθμός από 70, όπως φαίνεται στο σχετικό στιγμιότυπο οθόνης.

Ένα ακόμη σημαντικό χαρακτηριστικό του Process Explorer είναι η δυνατότητα **αποθήκευσης (dump) του περιεχομένου μιας διαδικασίας**, με τρόπο παρόμοιο με το Volatility. Η κύρια διαφορά είναι ότι ο αναλυτής μπορεί να εκτελέσει το dump χωρίς να χρειάζεται να αποκτήσει μια εικόνα μνήμης. Για να αποθηκεύσετε τη μνήμη, κάντε κλικ στη διαδικασία, πλοηγηθείτε στο **Process** και μετά στο **Create Dump**. Ο αναλυτής μπορεί να επιλέξει μεταξύ **mini-dump** ή **full dump**. Ως βέλτιστη πρακτική, συνιστάται η λήψη πλήρους dump. Το dump μπορεί στη συνέχεια να αποθηκευτεί σε έναν φάκελο της επιλογής σας.

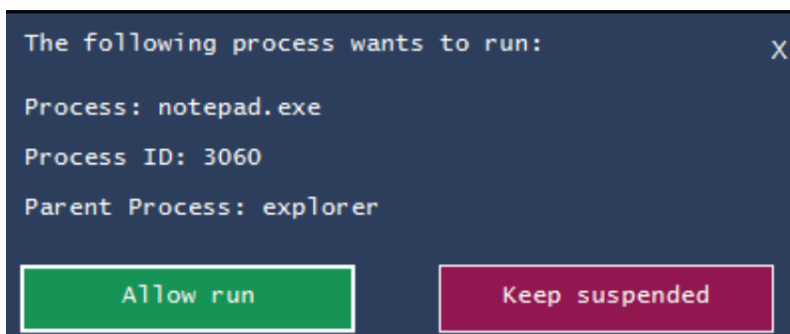
Process Spawn Control

Μια τεχνική που μπορεί να χρησιμοποιηθεί για την ανάλυση κακόβουλου λογισμικού είναι η δημιουργία μιας **εικονικής μηχανής** με το κατάλληλο λειτουργικό σύστημα Windows. Είναι προτιμότερο να ξεκινήσετε με ένα βασικό λειτουργικό σύστημα, με εγκατεστημένη τη σουίτα **Microsoft Office**. Άλλα προγράμματα τρίτων μπορούν να εγκατασταθούν αργότερα, αν διαπιστωθεί ότι ο κακόβουλος κώδικας εκμεταλλεύεται ευπάθεια σε αυτά τα προγράμματα.

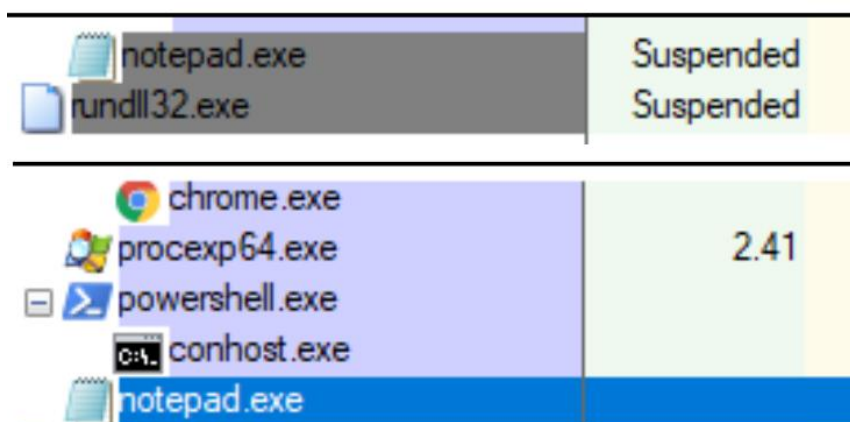
Ένα χρήσιμο εργαλείο για αυτόν τον τύπο ανάλυσης είναι το **Process Spawn Control**. Αυτό το script για **PowerShell**, διαθέσιμο στο [GitHub](#), επιτρέπει στους αναλυτές να ελέγχουν την εκτέλεση κακόβουλου λογισμικού και να παρατηρούν τις ενέργειες μέσω του Process Explorer.

Για να εκτελέσετε αυτή την ανάλυση, ακολουθήστε τα εξής βήματα:

1. Εκκινήστε το **Process Explorer** και αφήστε το να τρέξει για λίγα δευτερόλεπτα.
2. Στο τερματικό PowerShell, εκτελέστε το script **ProcessSpawnControl.ps1**. Επιλέξτε **Run Once**, αν σας ζητηθεί.
3. Το Process Spawn Control θα σταματήσει όλες τις εκτελέσιμες διαδικασίες, όχι μόνο το πιθανό κακόβουλο λογισμικό. Μόλις τρέξει, ανοίξτε το εκτελέσιμο των Windows, **notepad.exe**. Θα εμφανιστεί το παρακάτω παράθυρο:



4. Στο παράθυρο του Process Explorer, η διαδικασία **notepad.exe** θα εμφανίζεται ως **suspended** (ανασταλμένη), όπως φαίνεται στο σχετικό στιγμιότυπο. Κάντε κλικ στο **Allow run** στο παράθυρο του PowerShell και η διαδικασία **notepad.exe** θα εκτελεστεί κανονικά.



Η χρήση αυτών των εργαλείων σε συνδυασμό επιτρέπει στον αναλυτή να κατανοήσει **πώς λειτουργεί ένα πιθανό εκτελέσιμο κακόβουλο λογισμικό** και ποια διαδρομή εκτέλεσης μπορεί να ακολουθήσει. Αυτά τα δεδομένα, σε συνδυασμό με άλλα στοιχεία που αποκτώνται μέσω ανάλυσης μνήμης ή αρχείων καταγραφής, παρέχουν πρόσθετο πλαίσιο για το **πώς το κακόβουλο λογισμικό έχει υπονομεύσει ένα σύστημα**.

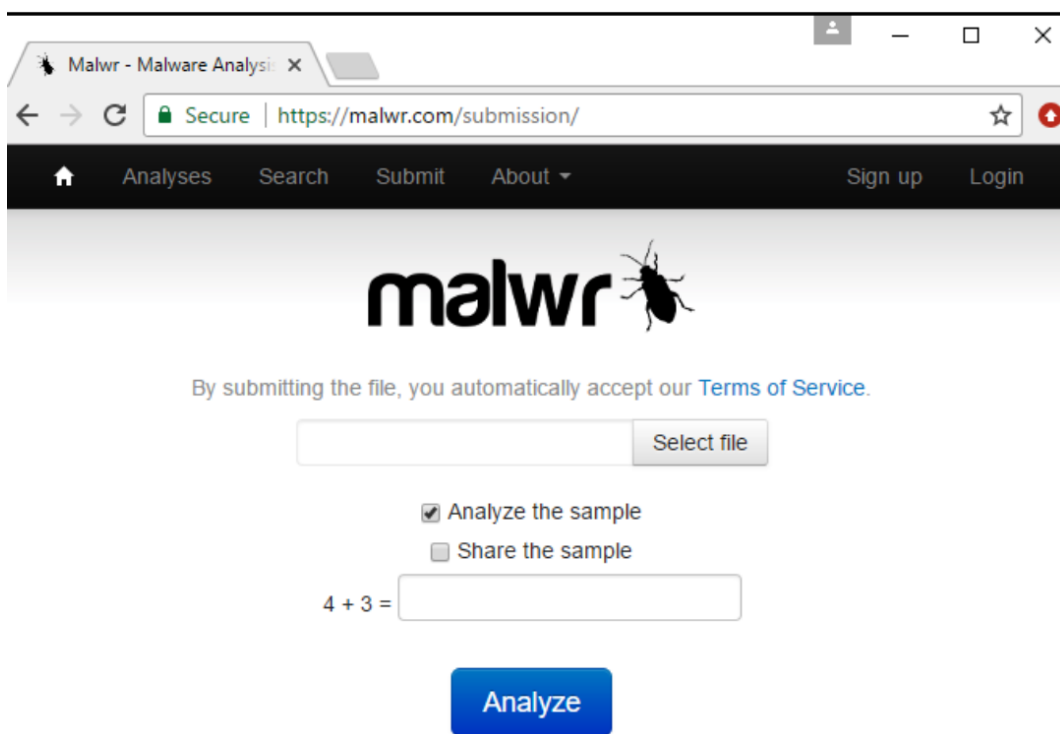
12.10. Cuckoo Sandbox

Το Cuckoo Sandbox είναι ένα σύστημα ανάλυσης κακόβουλου λογισμικού που αυτοματοποιεί πολλές από τις εργασίες που σχετίζονται με την ανάλυση malware. Αυτή η εφαρμογή ανοικτού κώδικα έχει τη δυνατότητα να αναλύει διάφορα ύποπτα αρχεία, όπως εκτελέσιμα αρχεία των Windows, έγγραφα και Java applets, όλα μέσα σε ένα εικονικοποιημένο περιβάλλον. Αυτή η ανάλυση περιλαμβάνει την εξέταση της δικτυακής κίνησης και της μνήμης, αξιοποιώντας το Volatility.

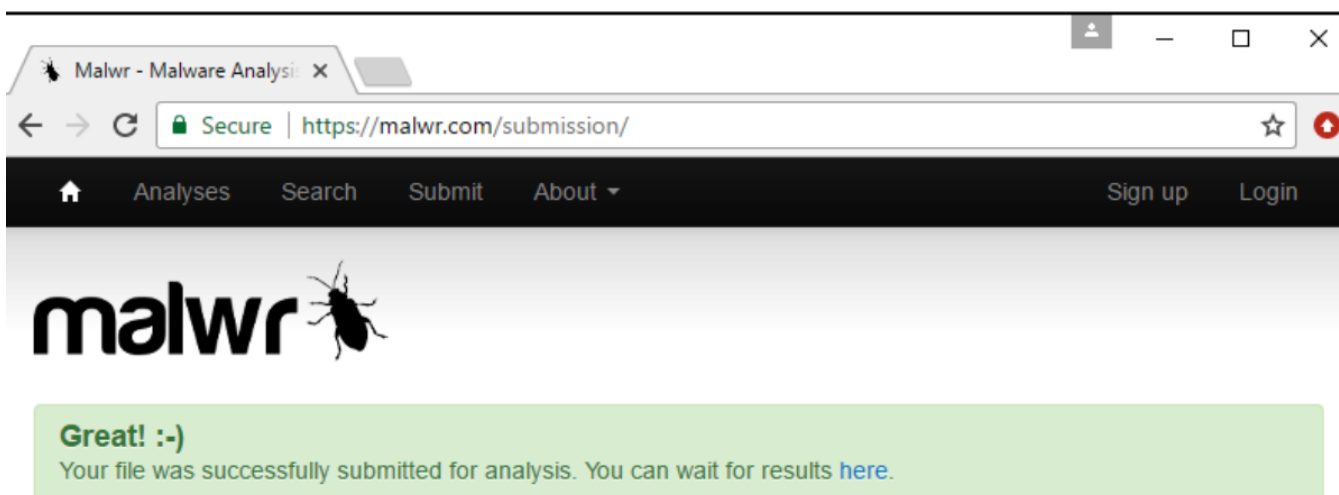
Η εγκατάσταση του Cuckoo Sandbox μπορεί να απαιτήσει κάποιο χρόνο και προσπάθεια. Ένας εξαιρετικός πόρος για την εγκατάσταση του τοπικού sandbox μπορεί να βρεθεί εδώ: <https://bdaviscybersecurity.blogspot.com/2016/11/cuckoo-sandbox-installationpart-1.html>

Εκτός από την τοπική έκδοση του Cuckoo Sandbox, οι αναλυτές μπορούν να χρησιμοποιήσουν και μια διαδικτυακή έκδοση. Η ιστοσελίδα <https://malwr.com/> παρέχει μια δωρεάν υπηρεσία που επιτρέπει στους αναλυτές να ανεβάσουν ένα αντίγραφο του κακόβουλου λογισμικού και να πραγματοποιηθεί δυναμική ανάλυση από τον ιστότοπο. Στη συνέχεια, η ιστοσελίδα παράγει μια αναφορά που μπορεί να εξεταστεί. Στο ακόλουθο παράδειγμα, θα χρησιμοποιηθεί το <http://malwr.com/> για την ανασκόπηση του LokiBot malspam, το οποίο μπορεί να ληφθεί από: <http://www.malware-traffic-analysis.net/2017/06/12/index.html>

1. Πλοηγηθείτε στον ιστότοπο <http://malwr.com> και κάντε κλικ στο **Submit** στην επάνω αριστερή γωνία. Αυτό θα ανοίξει το ακόλουθο παράθυρο.

The image shows a web browser window with the address bar displaying 'https://malwr.com/submission/'. The page has a dark navigation bar with links for 'Analyses', 'Search', 'Submit', and 'About', along with 'Sign up' and 'Login' buttons. The main content area features the 'malwr' logo with a beetle icon. Below the logo, a message states: 'By submitting the file, you automatically accept our Terms of Service.' There is a file upload section with a text input field and a 'Select file' button. Below this, there are two checkboxes: 'Analyze the sample' (checked) and 'Share the sample' (unchecked). A CAPTCHA question '4 + 3 =' is followed by an input field. At the bottom, there is a large blue 'Analyze' button.

2. Κάντε κλικ στο **Select file** και πλοηγηθείτε στο αρχείο malware που θέλετε να αναλύσετε. Το Malwr επιτρέπει στον αναλυτή να μοιραστεί το δείγμα malware με την κοινότητα ή όχι. Σε αυτή την περίπτωση, καθώς το malware που δοκιμάζεται είναι γνωστό, δεν επιλέγεται η κοινή χρήση. Τέλος, ολοκληρώστε την εξίσωση και κάντε κλικ στο **Analyze**. Θα εμφανιστεί το ακόλουθο παράθυρο:



3. Ανάλογα με τον τύπο και το μέγεθος του malware, η ανάλυση μπορεί να διαρκέσει μερικά λεπτά. Κατά τη διάρκεια αυτού του χρόνου, θα εμφανιστεί το ακόλουθο παράθυρο.
4. Μόλις ολοκληρωθεί η ανάλυση, θα ανοίξει ένα παράθυρο με τα αποτελέσματα. Τα αποτελέσματα ανάλυσης περιλαμβάνουν στοιχεία στατικής και δυναμικής ανάλυσης, όπως συμπεριφορικά και δικτυακά στοιχεία για εξέταση, όπως φαίνεται στο ακόλουθο στιγμιότυπο:

CATEGORY	STARTED	COMPLETED	DURATION
FILE	2017-07-05 17:35:43	2017-07-05 17:38:04	141 seconds

FILE NAME	PO12062017.exe
FILE SIZE	327680 bytes
FILE TYPE	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	aab1bb5073188ffdae1af3cb038c0b7
SHA1	ba40300913aaa8c0745da6502ab4fa547304cd81
SHA256	7e9c05cff0e0ac10640100c801c3f56470fb6166bbf4e67fa28c63af683458e4
SHA512	9cf107260177fcc2d27685e863409d9558929164143019af465136572317a09fbfc88ce5ebf525316a131e64d154e0f587eced1ba1a40caa0d
CRC32	A074F9AF
SSDEEP	6144:4WR7thWyL1fHz+m4h5dXP6RR7kjgMTIPf:4WR7thDEHhyXctln

Η εικόνα που προέρχεται από την πλατφόρμα Malware Traffic Analysis (malwr.com) και δείχνει μια ανάλυση ενός ύποπτου αρχείου με το όνομα "PO12062017.exe". Αυτή η ανάλυση πραγματοποιήθηκε στις 7 Ιουλίου 2017 και ολοκληρώθηκε σε 141 δευτερόλεπτα, υποδεικνύοντας ότι πρόκειται για στατική ανάλυση ενός πιθανού κακόβουλου λογισμικού.

Τύπος Αρχείου: Το αρχείο είναι ένα εκτελέσιμο PE32 (Portable Executable) για GUI, συμβατό με επεξεργαστές Intel 80386 για Windows. Αυτό είναι τυπικό για κακόβουλα προγράμματα που μολύνουν συστήματα Windows.

Μέγεθος: Με 327680 bytes (περίπου 320 KB), το μέγεθος είναι λογικό για ένα εκτελέσιμο αρχείο, αλλά δεν αποκαλύπτει από μόνο του τη φύση του.

Hash Values: Οι τιμές MD5, SHA1, SHA256 και SHA512 είναι μοναδικά αποτυπώματα του αρχείου, τα οποία μπορούν να χρησιμοποιηθούν για την αναγνώριση και τον εντοπισμό του σε βάσεις δεδομένων κακόβουλου λογισμικού. Η παρουσία αυτών των hashes υποδηλώνει ότι το αρχείο έχει υποβληθεί σε ανάλυση για να ελεγχθεί αν ταιριάζει με γνωστές απειλές.

CRC32 και \$SDEEP: Η τιμή CRC32 (A074F9AF) και η αλυσίδα \$SDEEP (6144:4WR7thWY11fHz+m4h5dX>P6RR7kgMTIPf:4WR7thDEHyXctIn) είναι επιπλέον δείκτες ακεραιότητας και ομοιότητας με άλλα δείγματα, που χρησιμοποιούνται για τη σύγκριση με γνωστά κακόβουλα προγράμματα.

5. Κάντε κλικ στην **Static Analysis** (Στατική Ανάλυση). Από εδώ, ο αναλυτής μπορεί να δει συγκεκριμένα στοιχεία, όπως οι συμβολοσειρές (strings) και ποια στοιχεία εισάγονται ως μέρος του αρχείου DLL, το οποίο στην περίπτωση αυτή είναι το **MSVBVM60.dll**, όπως φαίνεται στο ακόλουθο στιγμιότυπο:

Χειρισμός Συμβολοσειρών: Συναρτήσεις όπως vbaStrl2, lCicos, vbaStrCat, και vbaLenBstrB υποδεικνύουν ότι το πρόγραμμα χειρίζεται συμβολοσειρές, πιθανώς για επεξεργασία δεδομένων ή δημιουργία μηνυμάτων.

Διαχείριση Μνήμης: Οι συναρτήσεις vbaVarMove, vbaFreeVar, vbaFreeVarList, και vbaEnd δείχνουν τη διαχείριση μεταβλητών και την απελευθέρωση μνήμης, κάτι που είναι κρίσιμο για την αποφυγή διαρροών μνήμης.

Αριθμητικές Πράξεις: Οι συναρτήσεις adj_fdiv_m64 και adj_fprem1 αναφέρονται σε αριθμητικές πράξεις με κινητή υποδιαστολή (floating-point), ενώ adj_fdiv_m32 υποδηλώνει παρόμοιες λειτουργίες για 32-bit αριθμούς.

Διαχείριση Σφαλμάτων: Οι vbaSetSystemError και vbaHresultCheckObj υποδηλώνουν μηχανισμούς χειρισμού

Imports

Library MSVBVM60.DLL:

- 0x401000 __vbaStrl2
- 0x401004 _lCicos
- 0x401008 _adj_fptan
- 0x40100c __vbaVarMove
- 0x401010 __vbaFreeVar
- 0x401014 None
- 0x401018 __vbaFreeVarList
- 0x40101c None
- 0x401020 __vbaEnd
- 0x401024 _adj_fdiv_m64
- 0x401028 _adj_fprem1
- 0x40102c __vbaStrCat
- 0x401030 __vbaSetSystemError
- 0x401034 __vbaHresultCheckObj
- 0x401038 __vbaLenBstrB
- 0x40103c _adj_fdiv_m32
- 0x401040 __vbaExitProc
- 0x401044 None

σφαλμάτων, πιθανώς για την αναφορά προβλημάτων κατά την εκτέλεση.

Τερματισμός: Η vbaExitProc υποδηλώνει μια συνάρτηση που καλείται κατά την έξοδο της διαδικασίας, δείχνοντας τη διαχείριση του κύκλου ζωής του προγράμματος.

Η παρουσία αυτών των συναρτήσεων από τη MSVBVM60.DLL υποδηλώνει ότι το αρχείο είναι πιθανότατα μια εφαρμογή Visual Basic 6.0. Αυτό από μόνο του δεν αποδεικνύει ότι είναι κακόβουλο, καθώς πολλές νόμιμες εφαρμογές χρησιμοποιούν αυτή τη βιβλιοθήκη. Ωστόσο, σε συνδυασμό με άλλα στοιχεία (π.χ. από την προηγούμενη ανάλυση του "PO12062017.exe"), μπορεί να υποδηλώνει ένα κακόβουλο πρόγραμμα που έχει γραφτεί σε Visual Basic, το οποίο είναι συνηθισμένο για trojans ή άλλα malware που στοχεύουν παλαιότερα Windows συστήματα. Για ακριβέστερο συμπέρασμα, απαιτείται περαιτέρω ανάλυση της συμπεριφοράς και του κώδικα.

- Ενώ βρίσκεστε στην ενότητα Static Analysis, κάντε κλικ στο **Antivirus**. Αυτό παρέχει στους αναλυτές μια ανάλυση των αποτελεσμάτων του VirusTotal για το δείγμα που ανεβάστηκε, όπως φαίνεται στο ακόλουθο στιγμιότυπο:

Quick Overview

Static Analysis

Behavioral Analysis

Network Analysis

Dropped Files

Comment Board (0)

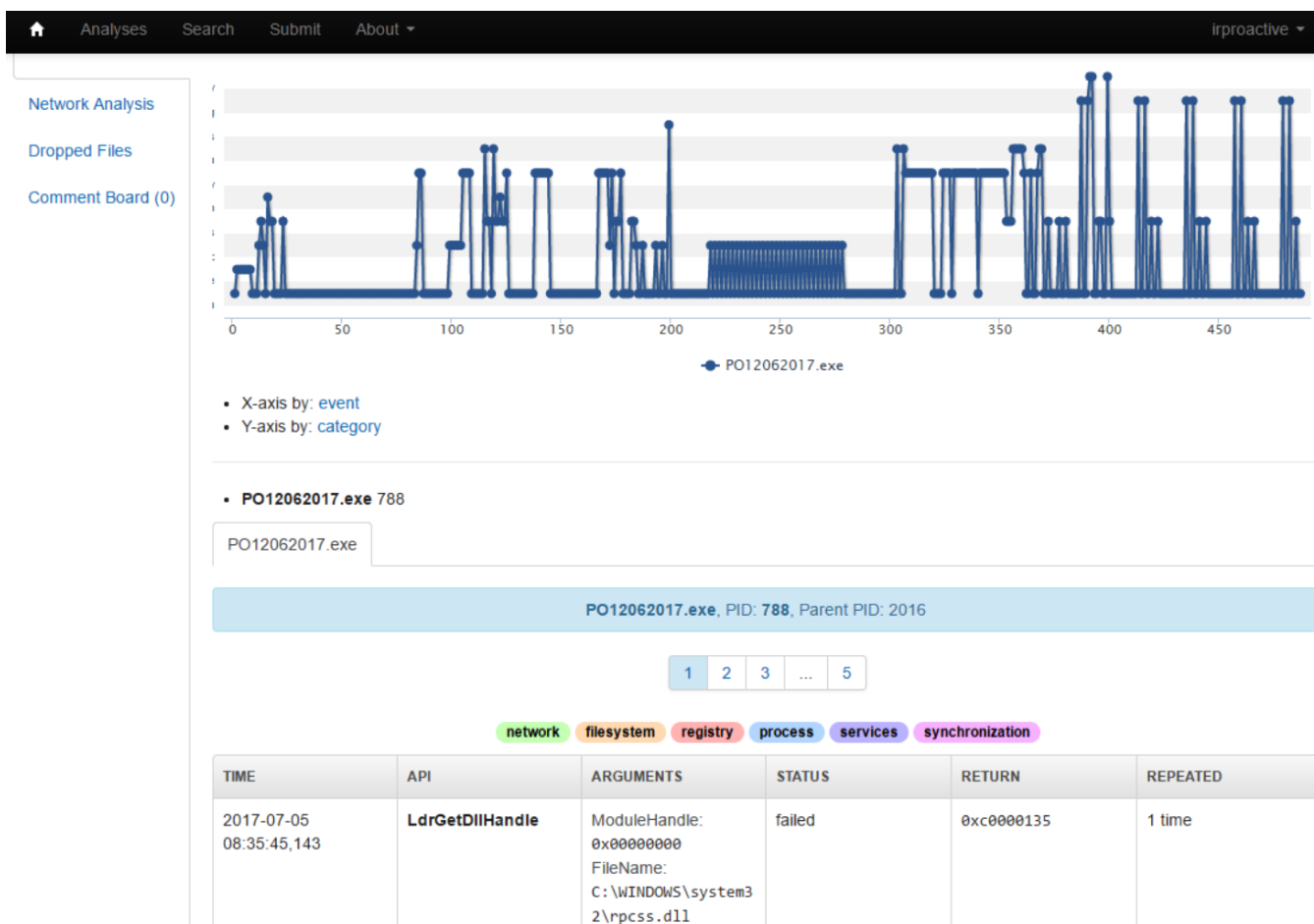
Static Analysis

Strings

Antivirus

ANTIVIRUS	SIGNATURE
Bkav	Clean
MicroWorld-eScan	Gen:Variant.Graftor.380641
nProtect	Clean
CMC	Clean
CAT-QuickHeal	Trojan.Dynamer
McAfee	Fareit-FILIAAB1BB507318
Malwarebytes	Clean
VIPRE	Trojan.Win32.Generic!BT
SUPERAntiSpyware	Clean
Tencent	Win32.Trojan.Generic.Lpkz
TheHacker	Clean
K7GW	Trojan (0050fca31)

- Στη συνέχεια, κάντε κλικ στο **Behavioral Analysis** (Συμπεριφορική Ανάλυση). Από εδώ, παρουσιάζονται οι συγκεκριμένες συμπεριφορές του αρχείου. Υπάρχουν γραφήματα που αναλύουν τη σειρά των γεγονότων που συνέβησαν μετά την εκτέλεση του malware. Αυτό επιτρέπει στους αναλυτές να δουν τα συγκεκριμένα στοιχεία με μεγαλύτερη λεπτομέρεια, όπως φαίνεται στο ακόλουθο στιγμιότυπο:



Η εικόνα προέρχεται από την πλατφόρμα Hybrid Analysis και παρουσιάζει την ανάλυση της συμπεριφοράς του αρχείου "PO12062017.exe", το οποίο έχει υποβληθεί σε έλεγχο για πιθανή κακόβουλη δραστηριότητα. Το διάγραμμα στην κορυφή δείχνει τη χρονική κατανομή των γεγονότων (events) που σχετίζονται με το αρχείο, με τον άξονα X να αντιπροσωπεύει τη χρονική ακολουθία και τον άξονα Y τις κατηγορίες δραστηριότητας (network, filesystem, registry, process, services, synchronization). Οι κορυφές στο διάγραμμα υποδεικνύουν σημεία αυξημένης δραστηριότητας, με μια έντονη περίοδο γύρω από το 250, που μπορεί να υποδηλώνει προσπάθεια φόρτωσης ή εκτέλεσης.

Το αρχείο "PO12062017.exe" εκτελέστηκε με PID 788 και έχει γονικό PID 2016, όπως φαίνεται στη λεζάντα. Η ανάλυση δείχνει μια αποτυχημένη κλήση API, συγκεκριμένα την LdrGetDllHandle, η οποία πραγματοποιήθηκε στις 08:35:45.143 στις 5 Ιουλίου 2017. Αυτή η συνάρτηση χρησιμοποιείται συνήθως για τη φόρτωση μιας δυναμικής βιβλιοθήκης σύνδεσης (DLL) στο μνήμη, και εδώ φαίνεται να αποτυγχάνει με όρισμα το "ModuleHandle: 0xe0000000" και όνομα αρχείου "FileName: C:\WINDOWS\system32\2\rpcss.dll". Η αποτυχία αυτή επιστρέφει την τιμή "0xc0000135", η οποία υποδηλώνει ότι η DLL δεν βρέθηκε ή δεν μπόρεσε να φορτωθεί.

Η αποτυχία φόρτωσης της "2\rpcss.dll" μπορεί να υποδηλώνει ότι το αρχείο "PO12062017.exe" προσπάθησε να εκτελέσει μια κακόβουλη ενέργεια, όπως η έγχυση κώδικα ή η πρόσβαση σε μια κακόβουλη βιβλιοθήκη. Ωστόσο, το γεγονός ότι η κλήση απέτυχε (status: failed) και επαναλήφθηκε

μόνο μία φορά, υποδηλώνει ότι η δραστηριότητα μπορεί να μην ολοκληρώθηκε επιτυχώς. Αυτό θα μπορούσε να οφείλεται σε προστασία του συστήματος, απουσία της DLL, ή σε ελλιπή ρύθμιση του περιβάλλοντος ανάλυσης. Συνολικά, η συμπεριφορά αυτή ενισχύει την υποψία ότι το "PO12062017.exe" είναι κακόβουλο λογισμικό, πιθανώς ένα trojan ή dropper, που προσπάθησε να φορτώσει επιπλέον συστατικά για τη λειτουργία του.

8. Συχνά, το malware δημιουργεί και άλλα αρχεία ως μέρος της μόλυνσης. Το Malwr επιτρέπει επίσης στον αναλυτή να δει αυτά τα αρχεία. Κάντε κλικ στο **Dropped Files**. Το Malwr υποδεικνύει ότι δύο αρχεία δημιουργήθηκαν μέσω αυτού του malware, όπως φαίνεται στο ακόλουθο στιγμιότυπο:

FILE NAME	filename.vbs
FILE SIZE	384 bytes
FILE TYPE	ASCII text, with CRLF line terminators
MD5	899dbb13af252b6cd89a6de23048cf8c
SHA1	857745ec21332c7e3a2f6f44af1113ecd9ec3f6a
SHA256	bf01560f94fd75d02a21b8cd133cab3d6e181f7eb4d41b6d415b65fe63665e96
CRC32	DA5FB4F1
SSDEEP	3:j+qAHmFE86oQ/FERMQsNC2xA+KdIH1MARm5IRMQbm34MkWJJFhRLl:j+q9Nht6G9KdEARm5Mm34M9
YARA	embedded_win_api - A non-Windows executable contains win32 API functions names

FILE NAME	filename.exe
FILE SIZE	327680 bytes
FILE TYPE	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	1f54f93c28df730aa1c13d0090c7eeb5
SHA1	c152e04d928a5397943d9285af8373813affed25
SHA256	75d49db3c12349a5be3da567ed9ca169e05d0ced8e6a15846bf9b884ed954f0c
CRC32	9E4A0D9D
SSDEEP	6144:9WR7thWyL1fHz+m4h5dXP6RR7kjmTIPv:9WR7thDEHhyXctIX
YARA	None matched

Περισσότερες πληροφορίες μπορούν να ληφθούν μέσω του Malwr, συμπεριλαμβανομένης της εξέτασης της δικτυακής δραστηριότητας και των σχολίων που παρέχει η κοινότητα του Malwr. Μια σημαντική σημείωση που πρέπει να γίνει κατά την εξέταση αυτής της πλατφόρμας σε σύγκριση με μια τοπική λύση είναι η εξής: οι δημιουργοί malware παρακολουθούν τα forums της κοινότητας και το VirusTotal για να δουν αν ένα hash—ή το ίδιο το αρχείο—έχει ανεβεί. Εάν το malware είναι συγκεκριμένο για έναν οργανισμό, όπως μια κυβερνητική υπηρεσία ή έναν μεγάλο λιανοπωλητή, θα γνωρίζουν ότι οι αναλυτές incident response έχουν εντοπίσει τη δημιουργία τους. Οι ομάδες incident

response πρέπει να ισορροπήσουν την ταχύτητα και την ευκολία αυτής της τεχνικής με την πιθανότητα ότι οι προσπάθειές τους μπορεί να γίνουν αντιληπτές.

Αυτό το κεφάλαιο ασχολήθηκε με τα διάφορα στοιχεία της ανάλυσης κακόβουλου λογισμικού για τον αναλυτή αντιμετώπισης περιστατικών. Αρχικά, είναι απαραίτητο να υπάρχει κατανόηση του κακόβουλου λογισμικού γενικά, καθώς αποτελεί μακράν την πιο συχνή απειλή που μπορούν να αξιοποιήσουν οι αντίπαλοι. Δεύτερον, οι τεχνικές ανάλυσης κακόβουλου λογισμικού—στατική και δυναμική—παρέχουν στους αναλυτές εργαλεία και μεθόδους για την εξαγωγή κρίσιμων δεδομένων. Τέλος, η χρήση συστημάτων sandboxing επιτρέπει στους αναλυτές να αποκτούν γρήγορα και με ελεγχόμενο τρόπο πληροφορίες σχετικά με τη συμπεριφορά και τα χαρακτηριστικά του κακόβουλου λογισμικού.

Με πολλούς τρόπους, αυτό το κεφάλαιο απλώς έθιξε την επιφάνεια όσον αφορά την ανάλυση κακόβουλου λογισμικού. Πρέπει να γίνει σαφές ότι, ακόμη και με εργαλεία για στατική και δυναμική ανάλυση, οι αναλυτές αντιμετώπισης περιστατικών έχουν ακόμη μεγάλη ανάγκη από εξάσκηση και ανάπτυξη δεξιοτήτων αν θέλουν να κυριαρχήσουν σε αυτό το ιδιαίτερα εξειδικευμένο υποσύνολο της ψηφιακής εγκληματολογίας. Αν και μπορεί να είναι δύσκολο, είναι σημαντικό να υπάρχει τουλάχιστον λειτουργική γνώση αυτού του τύπου ανάλυσης, καθώς οι κυβερνοεγκληματίες και τα κράτη συνεχίζουν να χρησιμοποιούν όλο και πιο εξελιγμένο κακόβουλο λογισμικό.

Το κεφάλαιο αυτό εμβάθυνε στην ανάλυση κακόβουλου λογισμικού, εξετάζοντας τους τύπους κακόβουλου λογισμικού που παρατηρούνται σήμερα. Η επισκόπηση των δύο κύριων μεθόδων ανάλυσης—στατική και δυναμική—παρείχε κάποιο πλαίσιο σχετικά με τα διαθέσιμα εργαλεία. Τα εργαλεία που συζητήθηκαν επιτρέπουν σε έναν αναλυτή να εντοπίζει συμπεριφορές στο κακόβουλο λογισμικό που μπορούν να χρησιμοποιηθούν για την ταυτοποίησή του. Τέλος, η εκτέλεση κακόβουλου λογισμικού μπορεί να παρέχει περαιτέρω λεπτομέρειες. Το επόμενο κεφάλαιο θα συνδέσει τη χρήση της πληροφοριογνωσίας απειλών (threat intelligence) με την ανάλυση κακόβουλου λογισμικού, δίνοντας στους αναλυτές τη δυνατότητα να συσχετίσουν τις παρατηρήσεις τους με όσα συμβαίνουν σε άλλους οργανισμούς.

13

Αξιοποίηση της Πληροφορίας Απειλών (Threat Intelligence)

Ένας τομέας της ανταπόκρισης σε περιστατικά που έχει σημαντικό αντίκτυπο στην ικανότητα ενός οργανισμού να ανταποκριθεί σε κυβερνοεπιθέσεις είναι η χρήση της πληροφορίας κυβερνοαπειλών ή, απλώς, πληροφοριών απειλών. Ο όρος «πληροφορία κυβερνοαπειλών» καλύπτει ένα ευρύ φάσμα πληροφοριών, δεδομένων και τεχνικών που επιτρέπουν στους αναλυτές να εντοπίζουν τύπους επιθέσεων στο δίκτυό τους, να ανταποκρίνονται κατάλληλα και να προετοιμάζονται για μελλοντικές επιθέσεις. Για να μπορέσουν οι αναλυτές ασφάλειας πληροφοριών να αξιοποιήσουν σωστά αυτή τη δυνατότητα, θα πρέπει να έχουν μια σταθερή βάση στις διάφορες ορολογίες, μεθοδολογίες και εργαλεία που μπορούν να χρησιμοποιηθούν σε συνδυασμό με τις πληροφορίες απειλών. Εάν οι αναλυτές μπορούν να χρησιμοποιήσουν αυτά τα δεδομένα, θα βρίσκονται σε καλύτερη θέση για να λάβουν προληπτικά μέτρα ασφαλείας και, σε περίπτωση περιστατικού ασφαλείας, να ανταποκριθούν πιο αποτελεσματικά.

Στη συζήτηση αυτού του κεφαλαίου σχετικά με την πληροφορία κυβερνοαπειλών θα καλυφθούν τα εξής βασικά θέματα:

- **Κατανόηση της πληροφορίας απειλών:** Η πληροφορία κυβερνοαπειλών είναι ένα μείγμα υπαρχουσών και αναδυόμενων πειθαρχιών στην κατασκοπεία. Η επισκόπηση παρέχει μια συνολική εικόνα των διαφόρων θεμάτων που αποτελούν μέρος της πληροφορίας κυβερνοαπειλών.
- **Μεθοδολογία πληροφορίας απειλών:** Η παραγωγή και η ενσωμάτωση πληροφοριών κυβερνοαπειλών είναι μια διαδικασία που καθοδηγείται από συγκεκριμένα βήματα. Αυτή η ενότητα παρέχει μια επισκόπηση της μεθοδολογίας της πληροφορίας κυβερνοαπειλών.
- **Πηγές πληροφοριών απειλών:** Υπάρχουν αρκετές πηγές από τις οποίες οι υπεύθυνοι ανταπόκρισης μπορούν να αποκτήσουν πληροφορίες κυβερνοαπειλών. Αυτό το τμήμα εξετάζει ορισμένες από τις βασικές διαθέσιμες πηγές.
- **Πλατφόρμες πληροφοριών απειλών:** Η πληροφορία απειλών παρέχει μεγάλο όγκο δεδομένων στους υπεύθυνους. Η εξέταση μιας πλατφόρμας πληροφοριών απειλών θα παρέχει στους υπεύθυνους μια επιλογή για να αντιμετωπίσουν πιθανή υπερφόρτωση δεδομένων.

- **Χρήση πληροφοριών απειλών:** Η πληροφορία κυβερνοαπειλών προορίζεται να χρησιμοποιηθεί είτε προληπτικά είτε αντιδραστικά. Αυτή η ενότητα παρέχει ορισμένα βασικά εργαλεία και τεχνικές για την εφαρμογή της.

Με πολλούς τρόπους, αυτό το κεφάλαιο απλώς αγγίζει την επιφάνεια των εργαλείων, τεχνικών και μεθοδολογιών της πληροφορίας κυβερνοαπειλών. Ελπίζεται ότι αυτή η επισκόπηση παρέχει ένα σημείο εκκίνησης για τους υπεύθυνους ώστε να ενσωματώσουν την πληροφορία απειλών στις λειτουργίες τους.

13.1. Κατανόηση της Πληροφορίας Απειλών

Όπως με ορισμένους όρους στην ασφάλεια πληροφοριών και την ανταπόκριση σε περιστατικά, η πληροφορία απειλών είναι κάπως ασαφής. Διάφοροι οργανισμοί, όπως κυβερνητικοί φορείς και ακαδημαϊκοί, παράγουν πληροφορίες και δεδομένα που συχνά προβάλλονται ως πληροφορία απειλών. Διάφοροι εμπορικοί πάροχοι διαθέτουν επίσης πληροφορίες, είτε δωρεάν είτε μέσω συνδρομών, που προβάλλονται ως πληροφορία απειλών. Αυτό συχνά δημιουργεί δυσκολία στον προσδιορισμό του τι αποτελεί πραγματικά πληροφορία απειλών και τι απλώς δεδομένα ή πληροφορίες.

Ένα καλό σημείο εκκίνησης για τον καθορισμό του τι αποτελεί πληροφορία απειλών είναι η χρήση ενός ορισμού. Ο ορισμός της εταιρείας Gartner είναι ο εξής:

"Πληροφορία απειλών είναι η γνώση που βασίζεται σε αποδείξεις, περιλαμβάνοντας το πλαίσιο, τους μηχανισμούς, τους δείκτες, τις επιπτώσεις και τις πρακτικές συμβουλές, σχετικά με μια υπάρχουσα ή αναδυόμενη απειλή ή κίνδυνο για περιουσιακά στοιχεία, που μπορεί να χρησιμοποιηθεί για την ενημέρωση αποφάσεων σχετικά με την ανταπόκριση σε αυτή την απειλή ή κίνδυνο."

Όταν εξετάζεται αυτός ο ορισμός, υπάρχουν αρκετά βασικά στοιχεία που πρέπει να είναι παρόντα για να θεωρηθούν τα δεδομένα ή οι πληροφορίες ως πληροφορία απειλών:

- **Βασισμένη σε αποδείξεις (Evidence-based):** Το κεφάλαιο αυτό θα εξετάσει πώς τα στοιχεία που λαμβάνονται μέσω άλλων διαδικασιών, όπως η ανάλυση κακόβουλου λογισμικού, παράγουν πληροφορία απειλών. Για να είναι ένα προϊόν πληροφοριών χρήσιμο, πρέπει πρώτα να αποκτηθεί μέσω σωστών μεθόδων συλλογής αποδεικτικών στοιχείων, ώστε οι αναλυτές να μπορούν να διασφαλίσουν την εγκυρότητά του.
- **Χρησιμότητα (Utility):** Για να έχει η πληροφορία απειλών θετικό αντίκτυπο στο αποτέλεσμα ενός περιστατικού ασφάλειας ή στη στάση ασφάλειας ενός οργανισμού, πρέπει να έχει κάποια χρησιμότητα. Η πληροφορία πρέπει να παρέχει σαφήνεια, όσον αφορά το πλαίσιο και τα δεδομένα, σχετικά με συγκεκριμένες συμπεριφορές ή μεθόδους, ώστε να καθοριστεί εάν ένας αναλυτής αξιολογεί ένα περιστατικό σε σύγκριση με άλλα παρόμοια περιστατικά.

- **Εφαρμοσιμότητα (Actionable):** Το βασικό στοιχείο που διαχωρίζει τα δεδομένα ή τις πληροφορίες από την πληροφορία απειλών είναι η δράση. Η πληροφορία πρέπει να οδηγεί σε δράση, είτε πρόκειται για μια συγκεκριμένη ακολουθία ενεργειών είτε για ένα συγκεκριμένο σημείο εστίασης ενός περιστατικού, ή για την εφαρμογή ενός συγκεκριμένου ελέγχου ασφαλείας με βάση πληροφορίες σχετικά με τις πιο πιθανές κυβερνοαπειλές που αντιμετωπίζει ο οργανισμός.

Για να γίνει πιο σαφές, ας φανταστούμε ένα σενάριο όπου μια ομάδα ανταπόκρισης περιστατικών σε έναν οργανισμό υγειονομικής περίθαλψης προσπαθεί να καθορίσει ποιοι τύποι επιθέσεων είναι πιο πιθανό να συμβούν στο δίκτυό τους. Ασαφή δεδομένα σχετικά με κυβερνοεγκληματίες που θέλουν να κλέψουν δεδομένα δεν είναι χρήσιμα. Δεν υπάρχει συγκεκριμένο πλαίσιο ή πληροφορία στο σύνολο αυτό των δεδομένων και το τελικό αποτέλεσμα είναι ότι ο οργανισμός δεν μπορεί να τα αξιοποιήσει.

Αντίθετα, αν η ομάδα ανταπόκρισης χρησιμοποιήσει έναν τρίτο πάροχο πληροφοριών απειλών, ο πάροχος αυτός μπορεί να προσδιορίσει μια συγκεκριμένη εγκληματική ομάδα με όνομα, να υποδείξει ότι χρησιμοποιούν PDF αρχεία που στέλνονται μέσω email σε υπαλλήλους του νοσοκομείου, τα οποία περιέχουν Trojan για απομακρυσμένη πρόσβαση (C2) με servers στην Ευρώπη, και να παρέχει MD5 hashes αρχείων κακόβουλου λογισμικού, IP και domain των servers και ονόματα αρχείων των PDF.

Με αυτές τις πληροφορίες, η ομάδα μπορεί να ευθυγραμμίσει τα μέτρα ασφαλείας για να αποτρέψει το άνοιγμα PDF συνημμένων, να ελέγξει το δίκτυό τους για πιθανή μόλυνση και να ρυθμίσει λύσεις διαχείρισης συμβάντων για ειδοποίηση αν κάποιος host επικοινωνήσει με τους C2 servers.

Η κύρια διαφορά μεταξύ των δύο σεναρίων είναι ότι το δεύτερο οδηγεί σε δράσεις μέσα στον οργανισμό, ενώ το πρώτο ήταν τόσο ασαφές και άχρηστο που ο οργανισμός δεν κέρδισε τίποτα.

13.2. Απειλές και ομάδες απειλών

Η πληροφορία απειλών αποτελεί απάντηση στην αυξημένη πολυπλοκότητα και τεχνική δεξιότητα των δραστών κυβερνοαπειλών. Ο στόχος της πληροφορίας απειλών επικεντρώνεται στις εξής ομάδες:

- **Κυβερνοεγκληματίες:** Οργανωμένοι και τεχνικά ικανοί, υπεύθυνοι για διάφορα οικονομικά εγκλήματα κατά τραπεζών, λιανεμπορίου και άλλων οργανισμών. Ο στόχος τους είναι η απόκτηση δεδομένων που μπορούν να εκμεταλλευτούν οικονομικά, όπως η κλοπή δεδομένων πιστωτικών καρτών από Target ή Home Depot.
- **Hacktivism (Χακερικές πολιτικές ενέργειες):** Ομάδες όπως οι Anonymous ή η Idlib Martyrs' Brigade στοχεύουν μεγάλες επιχειρήσεις, κυβερνήσεις ή θρησκευτικούς οργανισμούς για πολιτικούς σκοπούς.
- **Κυβερνοκατασκοπεία:** Κράτη όπως οι Ηνωμένες Πολιτείες, η Ρωσία, η Κίνα, το Ιράν και η Βόρεια Κορέα συμμετέχουν συνεχώς σε δραστηριότητες κατασκοπείας που περιλαμβάνουν τη διείσδυση σε δίκτυα και την απόκτηση πληροφοριών. Μία από τις πιο γνωστές

κυβερνοεπιθέσεις, ο ιός **Stuxnet**, φέρεται να πραγματοποιήθηκε από τις Ηνωμένες Πολιτείες και το Ισραήλ.

Ένα ακόμα βασικό στοιχείο για την κατανόηση της **απειλητικής πληροφοριολογίας** (threat intelligence) είναι η έννοια της **Προηγμένης Επίμονης Απειλής** (Advanced Persistent Threat – APT). Ο όρος **APT** υπάρχει περίπου εδώ και μια δεκαετία και χρησιμοποιείται για να περιγράψει έναν **δράστη κυβερνοαπειλής** του οποίου η ικανότητα και τα κίνητρα υπερβαίνουν κατά πολύ αυτά ενός κοινού κυβερνοεγκληματία ή «ψηφιακού βανδάλου».

Οι **ομάδες APT** συχνά στοχεύουν οργανισμούς για έναν **σκοπό με σαφή στόχο** και για **μεγάλο χρονικό διάστημα**. Όπως περιγράφει ο όρος APT, αυτές οι ομάδες έχουν τα ακόλουθα χαρακτηριστικά:

Προηγμένες ομάδες APT (Advanced): Οι δράστες APT διαθέτουν **προηγμένες δεξιότητες**. Αυτές οι δεξιότητες περιλαμβάνουν συχνά **τεχνικές συλλογής πληροφοριών** που υπερβαίνουν αυτά που μπορούν να αποκτηθούν μέσω ανοικτών πηγών. Τέτοιες πηγές περιλαμβάνουν:

- **Imagery Intelligence (IMINT):** Πληροφορίες που προέρχονται από εικόνες, όπως αυτές που είναι διαθέσιμες σε ιστοτόπους όπως το Google Earth.
- **Signals Intelligence (SIGINT):** Πληροφορίες που συλλέγονται μέσω της παραβίασης φωνητικών και δεδομένων επικοινωνιών, που χρησιμοποιούν τηλεφωνικές υποδομές, κινητά δεδομένα ή ραδιοσήματα.
- **Human Intelligence (HUMINT):** Συλλογή πληροφοριών από αλληλεπίδραση με ανθρώπινες πηγές.

Επιπλέον, οι ομάδες APT μπορούν όχι μόνο να χρησιμοποιούν **προηγμένα εργαλεία διείσδυσης σε δίκτυα**, αλλά είναι επίσης ικανές στο **εντοπισμό ευπαθειών μηδενικής ημέρας** και στη δημιουργία **προσαρμοσμένου κακόβουλου λογισμικού** και exploits που στοχεύουν ειδικά αυτές τις ευπάθειες.

Επίμονη (Persistent): Οι δράστες APT επικεντρώνονται σε έναν **σαφώς καθορισμένο στόχο** και συχνά παραμελούν άλλες ευκαιρίες προκειμένου να προχωρήσουν προς την επίτευξη του αντικειμενικού τους σκοπού. Συχνά, χρειάζονται **μήνες ή ακόμα και χρόνια** για να επιτύχουν τον στόχο τους, αξιοποιώντας έξυπνα τις ευπάθειες και διατηρώντας έναν ρυθμό που τους επιτρέπει να παρακάμπτουν τα συστήματα ανίχνευσης. Ένα από τα βασικά χαρακτηριστικά που διαχωρίζουν τους δράστες APT από άλλους είναι η **πρόθεση να παραμείνουν στο δίκτυο-στόχο για μεγάλο χρονικό διάστημα**. Ενώ μια ομάδα κυβερνοεγκληματιών θα μείνει αρκετά ώστε να κατεβάσει μια βάση δεδομένων με αριθμούς πιστωτικών καρτών, μια ομάδα APT θα **διατηρήσει την πρόσβαση στο δίκτυο όσο το δυνατόν περισσότερο**.

Απειλή (Threat): Για τους οργανισμούς που αντιμετωπίζουν ομάδες APT, αυτές αποτελούν **σαφή και σοβαρή απειλή**. Οι δράστες APT εκτελούν τις επιθέσεις τους με **συγκεκριμένο στόχο** και διαθέτουν την **αναγκαία υποδομή και δεξιότητες** για να επιτεθούν σε στόχους όπως **μεγάλες εταιρείες, τον στρατό και κυβερνητικούς οργανισμούς**.

Απειλητική Πληροφοριολογία (Threat Intelligence): Η απειλητική πληροφοριολογία είναι ένας ευρύς τομέας μελέτης που περιλαμβάνει πολλά στοιχεία τα οποία συνδέονται μεταξύ τους. Στο τέλος, η πληροφοριολογία απειλών πρέπει να οδηγεί σε δράση μέσα σε έναν οργανισμό. Η φύση αυτής της δράσης καθορίζεται συχνά μετά από προσεκτική αξιολόγηση των πληροφοριών. Αυτό περιλαμβάνει την κατανόηση του τύπου της πληροφοριολογίας που εξετάζεται και το πλεονέκτημα που παρέχει κάθε τύπος στον οργανισμό.

13.3. Τύποι πληροφοριών απειλών (Threat Intelligence Types)

Όταν συζητάμε για την ευρεία ποικιλία τύπων πληροφοριών και συνόλων δεδομένων που αποτελούν την πληροφορία απειλών, συχνά κατατάσσονται σε μία από τις τρεις κύριες κατηγορίες:

Τακτική πληροφορία απειλών (Tactical threat intelligence): Αυτή είναι η πιο λεπτομερής από τις τρεις κατηγορίες πληροφοριών απειλών. Οι πληροφορίες σε αυτήν την κατηγορία περιλαμβάνουν είτε **Δείκτες Συμβιβασμού (Indicators of Compromise – IOCs)**, είτε **Δείκτες Επίθεσης (Indicators of Attack – IOAs)**, είτε **Τακτικές, Τεχνικές και Διαδικασίες (Tactics, Techniques, and Procedures – TTPs)**:

- **IOCs (Indicators of Compromise):** Ένας IOC είναι ένα στοιχείο που παρατηρείται σε ένα σύστημα και υποδεικνύει κάποιο είδος συμβιβασμού. Για παράδειγμα, μια διεύθυνση IP C2 ή ένα MD5 hash ενός κακόβουλου αρχείου αποτελούν IOCs.
- **IOAs (Indicators of Attack):** Ένας IOA είναι ένα στοιχείο που παρατηρείται σε ένα σύστημα και υποδεικνύει επίθεση ή προσπάθεια επίθεσης. Διαφέρει από τον IOC, καθώς ο IOA δεν δείχνει ότι ένα σύστημα έχει συμβιβαστεί, αλλά ότι δέχτηκε επίθεση, μέσω ενδείξεων που άφησε ο επιτιθέμενος. Ένα παράδειγμα μπορεί να είναι προσπάθειες σύνδεσης που καταγράφονται σε ένα firewall log και υποδεικνύουν μια αυτοματοποιημένη σάρωση θυρών (port scan) με χρήση εργαλείων όπως το Nmap ή άλλο εργαλείο δικτυακής σάρωσης.
- **TTPs (Tactics, Techniques, and Procedures):** Οι άνθρωποι έχουν συνήθειες και, ως αποτέλεσμα, οι επιτιθέμενοι στον κυβερνοχώρο συχνά αναπτύσσουν μοναδικές μεθοδολογίες για την επίθεση σε ένα δίκτυο. Για παράδειγμα, μια ομάδα κυβερνοεγκληματιών μπορεί να προτιμά ένα phishing email με ένα Excel αρχείο που εκτελεί Trojan απομακρυσμένης πρόσβασης. Στη συνέχεια, μπορεί να επιχειρήσουν να αποκτήσουν πρόσβαση σε συσκευή πληρωμών με πιστωτική κάρτα (POS) και να τη μολύνουν με άλλο κακόβουλο λογισμικό. Ο τρόπος με τον οποίο αυτή η ομάδα εκτελεί μια επίθεση θεωρείται η TTP της ομάδας.

Λειτουργική πληροφορία απειλών (Operational threat intelligence): Την τελευταία δεκαετία παρατηρούνται όλο και πιο συντονισμένες επιθέσεις που δεν στοχεύουν μόνο σε έναν οργανισμό, αλλά μπορεί να επηρεάσουν ολόκληρο κλάδο, περιοχή ή χώρα. Η λειτουργική πληροφορία απειλών είναι δεδομένα και πληροφορίες σχετικά με τους ευρύτερους στόχους των κυβερνοεπιθέσεων και των δραστών απειλών. Αυτό συχνά περιλαμβάνει όχι μόνο την ανάλυση της ίδιας της οργάνωσης από την ομάδα αντιμετώπισης περιστατικών (incident response team), αλλά και τον τρόπο με τον οποίο οι

επιτιθέμενοι στοχεύουν τον ευρύτερο κλάδο. Για παράδειγμα, επιστρέφοντας σε προηγούμενο παράδειγμα όπου η ομάδα αντιμετώπισης περιστατικών σε μια υγειονομική δομή προετοιμαζόταν για επίθεση, η γνώση για το ποιες επιθέσεις συμβαίνουν σε άλλες υγειονομικές δομές παρόμοιου μεγέθους και προσωπικού θα ήταν χρήσιμη για την ευθυγράμμιση των δικών τους μέτρων ασφάλειας με τις κυρίαρχες απειλές.

Στρατηγική πληροφορία απειλών (Strategic threat intelligence): Τα ανώτερα στελέχη, όπως ο CIO ή ο CISO, πρέπει συχνά να ασχολούνται με τους στρατηγικούς στόχους της οργάνωσης παράλληλα με τα απαραίτητα μέτρα για να διασφαλίσουν ότι η οργάνωση αντιμετωπίζει το τοπίο των κυβερνοαπειλών. Η στρατηγική πληροφορία απειλών εξετάζει τις τάσεις στις κυβερνοεπιθέσεις, ποιοι επιτιθέμενοι είναι κυρίαρχοι και ποιοι κλάδοι αποτελούν κύριους στόχους. Άλλα σημαντικά δεδομένα είναι οι τεχνολογικές αλλαγές που μπορεί να αξιοποιήσει ένας επιτιθέμενος ή ομάδα σε μια επίθεση.

Βέλτιστη χρήση των πληροφοριών απειλών: Η καλύτερη χρήση των πληροφοριών απειλών είναι να κατανοήσουμε ότι κάθε τύπος μπορεί να ενσωματωθεί σε μια συνολική στρατηγική. Η αξιοποίηση εσωτερικών και εξωτερικών πληροφοριών απειλών και των τριών τύπων παρέχει:

- Στους αποφασιστές (key decision makers) κατανόηση του τοπίου απειλών.
- Στους διαχειριστές (managers) τη δυνατότητα να εφαρμόσουν κατάλληλους ελέγχους και διαδικασίες ασφάλειας.
- Στους αναλυτές (analysts) τη δυνατότητα να αναζητήσουν συνεχιζόμενα ζητήματα ασφάλειας ή να προετοιμάσουν τη δική τους ανταπόκριση σε μια κυβερνοεπίθεση.

13.4. Πυραμίδα του πόνου (Pyramid of Pain)

Ένα χρήσιμο εργαλείο για την περιγραφή των διαφόρων τύπων IOCs και IOAs που μπορεί να αξιοποιήσει ένας αντίπαλος, καθώς και της ικανότητάς του να τα τροποποιεί κατά τη διάρκεια μιας επίθεσης, είναι η **πυραμίδα του πόνου**.

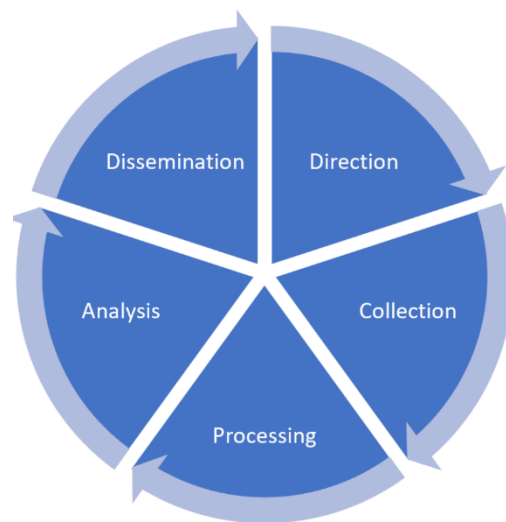
Η κατασκευή αυτή, που αναπτύχθηκε από τον **David Bianco**, περιγράφει τη σχέση μεταξύ των IOCs, IOAs και TTPs που καθίστανται διαθέσιμα από τον επιτιθέμενο μέσω παρατηρήσεων του αμυνόμενου, και την ικανότητα του επιτιθέμενου να αλλάζει αυτούς τους δείκτες. Το ακόλουθο διάγραμμα παρουσιάζει τη σχέση με τους διάφορους δείκτες και την απαιτούμενη προσπάθεια για την τροποποίησή τους ώστε να παρακαμφθούν οι μηχανισμοί ασφαλείας:

Για παράδειγμα, ένας επιτιθέμενος μπορεί να έχει δημιουργήσει ένα κακόβουλο λογισμικό που εξαπλώνεται μέσω πλευρικής κίνησης (lateral movement) με το πρωτόκολλο **Windows SMB**. Για να παρακάμψει τα παραδοσιακά εργαλεία πρόληψης κακόβουλου λογισμικού που βασίζονται σε υπογραφές, ο επιτιθέμενος χρησιμοποιεί έναν **πολυμορφικό ιό** που αλλάζει το hash του κάθε φορά που εγκαθίσταται. Αυτή η αλλαγή επιτρέπει στο κακόβουλο λογισμικό να παρακάμψει αυτόν τον έλεγχο.

Άλλοι δείκτες, όπως τα δικτυακά ή τα αρχεία καταγραφής (host artifacts), είναι πολύ πιο δύσκολο να τροποποιηθούν από τον επιτιθέμενο και, ως αποτέλεσμα, οι αναλυτές ανταπόκρισης έχουν μεγαλύτερη πιθανότητα να σταματήσουν με επιτυχία μια επίθεση ευθυγραμμίζοντας τους ελέγχους ασφαλείας με τα **ανώτερα επίπεδα της πυραμίδας**.

Από την οπτική της **πληροφορίας απειλών**, η πυραμίδα του πόνου επιτρέπει στους αναλυτές να ευθυγραμμίζουν τις απαιτήσεις τους με ό,τι είναι πιο χρήσιμο σε μια **μακροπρόθεσμη στρατηγική**. Η ύπαρξη λεπτομερών πληροφοριών για τα **TTPs** που χρησιμοποιούν οι δράστες παρέχει περισσότερη διορατικότητα στον τρόπο λειτουργίας τους. Αντίθετα, οι δείκτες χαμηλότερου επιπέδου, όπως οι **IP διευθύνσεις C2 servers**, είναι μεν χρήσιμοι, αλλά οι αναλυτές πρέπει να κατανοήσουν ότι μπορούν εύκολα να αλλαχθούν από τον αντίπαλο.

Μεθοδολογία Πληροφορίας Απειλών (Threat Intelligence Methodology): Η πληροφορία απειλών ακολουθεί έναν **κύκλο ανατροφοδότησης** προκειμένου να συμβαδίζει με το συνεχώς μεταβαλλόμενο περιβάλλον. Παρόλο που υπάρχουν πολλές μεθοδολογίες που μπορούν να δώσουν πλαίσιο σε αυτήν την πρόκληση, μία που χρησιμοποιείται συχνά είναι ο **κύκλος πληροφοριών (intelligence cycle)**, ο οποίος υιοθετείται από το **Υπουργείο Άμυνας των Η.Π.Α.** Αυτός ο κύκλος παρέχει το πλαίσιο και το σημείο εκκίνησης για τους οργανισμούς ώστε να ενσωματώσουν την πληροφορία απειλών στις λειτουργίες τους.



Φάσεις του κύκλου πληροφοριών:

- Κατεύθυνση (Direction):** Οι υπεύθυνοι λήψης αποφάσεων, όπως ο CISO, το προσωπικό ασφάλειας πληροφοριών ή οι αναλυτές αντιμετώπισης περιστατικών, καθορίζουν ποιες πληροφορίες απειλών είναι απαραίτητες.
 - Π.χ. ένας **CISO** μπορεί να θέλει πληροφορίες για τις τάσεις στις κυβερνοεπιθέσεις που αναμένονται εναντίον νοσοκομείων το επόμενο έτος.
 - Ένας **αναλυτής αντιμετώπισης περιστατικών** μπορεί να χρειάζεται πληροφορίες για τα **IOCs** που παρατηρούνται σε άλλες υγειονομικές δομές.
 - Ένα καλό σημείο εκκίνησης είναι η αποτίμηση κρίσιμων συστημάτων, εφαρμογών και δεδομένων που πρέπει να προστατευτούν, καθώς και ήδη διαθέσιμων πληροφοριών για πιθανές απειλές.
- Συλλογή (Collection):** Στο στάδιο της συλλογής, ο οργανισμός αποκτά δεδομένα και πληροφορίες από τις πηγές του.

- ο Αυτές μπορεί να προέρχονται από κυβερνητικούς φορείς, όπως τα εθνικά **CERTs**,
 - ο από τρίτους οργανισμούς που πωλούν πληροφορίες απειλών,
 - ο ή από πολλές πηγές **Ανοιχτής Πληροφορίας (OSINT feeds)**.
3. **Επεξεργασία (Processing)**: Ο όγκος των δεδομένων μπορεί να είναι τεράστιος. Σε αυτό το στάδιο, ο οργανισμός παίρνει τα ακατέργαστα δεδομένα, αξιολογεί τη συνάφεια και την αξιοπιστία τους και τα οργανώνει για το επόμενο βήμα.
 4. **Ανάλυση (Analysis)**: Τα δεδομένα που έχουν υποστεί επεξεργασία συνδυάζονται με άλλα από διαφορετικές πηγές. Από εδώ ερμηνεύονται και παράγεται το «τελικό προϊόν»: πληροφορία απειλών κατάλληλα επιμελημένη και αξιολογημένη.
 5. **Διάχυση (Dissemination)**: Η νέα, επιμελημένη πληροφορία απειλών διανέμεται στους διάφορους χρήστες εντός του οργανισμού για αξιοποίηση.

Η **κυκλική φύση** αυτής της μεθοδολογίας διασφαλίζει ότι η **ανατροφοδότηση** αποτελεί μέρος της διαδικασίας. Οι αναλυτές που συμμετέχουν στη συλλογή και επεξεργασία πρέπει να βεβαιώνονται ότι λαμβάνουν σχόλια σχετικά με τη συνάφεια και την ακρίβεια της πληροφορίας που διανέμεται. Έτσι, μπορούν να προσαρμόσουν το προϊόν πληροφοριών με την πάροδο του χρόνου. Αυτό εξασφαλίζει το υψηλότερο επίπεδο συνάφειας και αξιοπιστίας για τους τελικούς χρήστες.

13.5. Κατεύθυνση Πληροφοριών Απειλής (Threat Intelligence Direction)

Υπάρχει μεγάλος όγκος πληροφοριών και δεδομένων διαθέσιμων σε έναν οργανισμό όσον αφορά τις πληροφορίες απειλής. Ένα από τα κύρια εμπόδια που θα πρέπει να υπερβούν οι οργανισμοί είναι η προσδιορισμός των απαιτήσεων τους για πληροφορίες απειλής. Με το βάθος των διαθέσιμων πληροφοριών απειλής, είναι απαραίτητο να φιλτραριστεί ο θόρυβος και να επικεντρωθούν μόνο στις πληροφορίες απειλής που οδηγούν σε δράση εντός του οργανισμού.

Για να προσδιορίσει ένας οργανισμός τις απαιτήσεις του σε πληροφορίες απειλής, συνιστάται να εξεταστεί ποιοι παράγοντες (actors) αποτελούν απειλή για τον οργανισμό και πώς αυτοί οι παράγοντες θα μπορούσαν να πραγματοποιήσουν μια επίθεση στο δίκτυο του οργανισμού. Για τον προσδιορισμό αυτό, υπάρχουν διαθέσιμα εργαλεία όπως η μεθοδολογία **MITRE ATT&CK**, η **Cyber Kill Chain**, και το **Diamond Model**, που μπορούν να βοηθήσουν έναν οργανισμό να κατανοήσει το τοπίο απειλών του και να ευθυγραμμίσει καλύτερα τη χρήση των πληροφοριών απειλής για την αντιμετώπιση αυτών των απειλών.

Cyber Kill Chain: Η **Cyber Kill Chain** είναι μια έννοια που αρχικά αναπτύχθηκε από τρεις ερευνητές της **Lockheed Martin** (πρώτο άρθρο). Η **Cyber Kill Chain** περιγράφει τα στάδια μιας διείσδυσης σε δίκτυο που ένας επιτιθέμενος πρέπει να περάσει για να φτάσει στον τελικό στόχο του. Από εδώ, οι οργανισμοί μπορούν να εξάγουν τις διάφορες μεθόδους και τα **IOCs** (Indicators of Compromise) που

μπορεί να παρατηρήσουν χρησιμοποιώντας δυνατότητες ανίχνευσης ενισχυμένες με πληροφορίες απειλής. Η Cyber Kill Chain χωρίζει μια επίθεση σε δίκτυο σε επτά βήματα:

1. **Αναγνώριση (Reconnaissance):** Οι επιτιθέμενοι συχνά αφιερώνουν σημαντικό χρόνο στην ανασκόπηση πληροφοριών ανοιχτής πηγής, όπως μέσα κοινωνικής δικτύωσης, εταιρικές ιστοσελίδες και εγγραφές domain, για να χαρτογραφήσουν το εξωτερικά προσβάσιμο δίκτυο ενός οργανισμού-στόχου. Άλλες μέθοδοι αναγνώρισης περιλαμβάνουν τη χρήση εργαλείων χαρτογράφησης και σάρωσης δικτύου όπως τα **Nmap** και **Netcat** για τον προσδιορισμό ανοιχτών θυρών ή ενεργών υπηρεσιών. Οι δραστηριότητες αναγνώρισης είναι συχνά δύσκολο να εντοπιστούν, καθώς οι παράγοντες απειλής μπορούν να τις διεξάγουν χωρίς άμεση ενέργεια ή να προσαρμόζουν τις σαρώσεις ώστε να κρύβονται πίσω από την κανονική κίνηση του δικτύου.
2. **Οπλοποίηση (Weaponization):** Μετά την αναγνώριση, οι παράγοντες απειλής κατασκευάζουν τα εργαλεία τους για την πραγματική διείσδυση. Αυτό μπορεί να είναι ένα πολυβάθμιο κακόβουλο λογισμικό (malware) που διακυβεύει ένα σύστημα. Η εξέταση των εργαλείων που χρησιμοποιούνται σε μια επίθεση παρέχει συγκεκριμένα δεδομένα, όπως πώς το malware είναι συσκευασμένο ή ποια exploits χρησιμοποιούνται, τα οποία συνδυάζονται για να δημιουργήσουν ένα «μοτίβο» μοναδικό για τον επιτιθέμενο, σχεδόν σαν ένα γενετικό προφίλ (DNA profile) για σύγκριση.
3. **Παράδοση (Delivery):** Οι παράγοντες απειλής χρειάζονται ένα μέσο για να παραδώσουν το malware ή το exploit τους. Μπορεί να χρησιμοποιήσουν **VPN** ή να στείλουν malware συνδεδεμένο σε έγγραφο Word μέσω email σε υπάλληλο του οργανισμού-στόχου.
4. **Εκμετάλλευση (Exploitation):** Σε αυτό το στάδιο, ο παράγοντας απειλής εκμεταλλεύεται μια ευπάθεια στο δίκτυο του στόχου ή τη λειτουργικότητα εργαλείων όπως το **PowerShell**.
5. **Εγκατάσταση (Installation):**
Για να αποκτήσει περισσότερη από προσωρινή πρόσβαση, ο παράγοντας απειλής εγκαθιστά το exploit ή το malware του. Αυτό μπορεί να περιλαμβάνει ακόμη και την τροποποίηση ρυθμίσεων ή άλλων λειτουργιών στο συμβιβασμένο σύστημα.
6. **Διαχείριση (C2 – Command & Control):** Για να ελέγξει το σύστημα μετά την επιτυχή εγκατάσταση, ο παράγοντας απειλής διαμορφώνει ένα απομακρυσμένο κανάλι C2 προς έναν κεντρικό server. Από εδώ, μπορεί να διατηρεί τον έλεγχο, να φορτώνει πρόσθετα exploits ή malware και να παρατηρεί τις ενέργειες του οργανισμού-στόχου.
7. **Ενέργειες στον στόχο (Actions on the Objective):** Αφού ολοκληρωθούν τα προηγούμενα έξι βήματα, ο παράγοντας απειλής προχωρά στην επίτευξη του στόχου της διείσδυσης. Για λιανικές επιχειρήσεις, αυτό μπορεί να σημαίνει μόλυνση POS συσκευών με malware και απόκτηση αριθμών πιστωτικών καρτών. Σε κυβερνητικούς οργανισμούς, μπορεί να σημαίνει απόκτηση βάσεων δεδομένων εμπιστευτικών πληροφοριών για πώληση.

Χρήση IOCs και TTPs: Δουλεύοντας μέσα από αυτά τα βήματα, ένας οργανισμός μπορεί να εντοπίσει πού μπορούν να ληφθούν μεμονωμένα **IOCs** και πιο γενικές **TTPs** (Tactics, Techniques, and Procedures) σχετικά με τους παράγοντες απειλής. Μια συχνά χρησιμοποιούμενη τεχνική είναι να προσδιοριστεί ποιες απειλές είναι εφαρμόσιμες σε έναν οργανισμό και στη συνέχεια να αντιστοιχιστούν σε κάθε στάδιο στα μεμονωμένα IOCs για τα οποία απαιτούνται συγκεκριμένες πληροφορίες απειλής.

Παράδειγμα: Ο οργανισμός μπορεί να έχει αναφορά για μια ομάδα κυβερνοεγκληματιών που στοχεύει POS συσκευές. Στη συνέχεια, κατανοεί ότι πρέπει να γνωρίζει ποια είναι τα IOCs για τα αρχικά εργαλεία που χρησιμοποιούνται στο στάδιο της οπλοποίησης. Ακολουθεί η ανάλυση των TTPs σχετικά με το πώς ο παράγοντας απειλής παραδίδει το exploit ή το malware. Ο οργανισμός χρειάζεται επίσης να κατανοήσει πώς ο επιτιθέμενος εκμεταλλεύεται το δίκτυο μέσω ευπαθειών ή χρησιμοποιώντας εγγενή εργαλεία. Η εγκατάσταση του exploit ή malware παράγει IOCs στη μνήμη σε λειτουργία και στις ρυθμίσεις μητρώου (registry) του συμβιβασμένου συστήματος. Η πρόσβαση σε αυτά τα συγκεκριμένα IOCs βοηθά τον οργανισμό να αναπτύξει επιπλέον δυνατότητες ανίχνευσης ή να τα εντοπίσει κατά τη διάρκεια διερεύνησης περιστατικών.

13.6. Μοντέλο Diamond (Diamond Model)

Το **Diamond Model** της ανάλυσης εισβολών είναι μια μεθοδολογία που χρησιμοποιείται για να περιγράψει τη διαδικασία διαφοροποίησης των απειλών APT (Advanced Persistent Threats) από τα συγκεκριμένα χαρακτηριστικά τους. Το διαμάντι αποτελείται από τέσσερα στοιχεία: **Αντίπαλος (Adversary)**, **Υποδομή (Infrastructure)**, **Ικανότητα (Capability)**, και **Θύμα (Victim)**.

Το μοντέλο προσπαθεί να προσδιορίσει την αλληλεπίδραση μεταξύ αυτών των τεσσάρων ομάδων.

Παράδειγμα:

Σε μια απλή επίθεση με κακόβουλο λογισμικό, ο **Αντίπαλος** χρησιμοποιεί ένα προσαρμοσμένο κακόβουλο πρόγραμμα. Η δυνατότητα ανάπτυξης προσαρμοσμένου λογισμικού υποδηλώνει την **Ικανότητά του (Capability)**. Ο Αντίπαλος στη συνέχεια αξιοποιεί αυτήν την ικανότητα για να αναπτύξει το κακόβουλο πρόγραμμα μέσω ενός παραβιασμένου web server ή άλλης υποδομής. Αυτό συνδέεται με το **Θύμα**, όπου η ικανότητα εκμεταλλεύεται μια ευπάθεια μέσω κοινωνικής μηχανικής (social engineering).

Αυτό το απλό παράδειγμα αναδεικνύει μόνο ένα μικρό τμήμα του τρόπου με τον οποίο το Diamond Model μπορεί να χρησιμοποιηθεί για την κατηγοριοποίηση των επιθέσεων. Για βαθύτερη κατανόηση, συνιστάται η μελέτη της αρχικής εργασίας για το Diamond Model, η οποία μπορεί να ληφθεί από: <http://www.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf>

Με την ενσωμάτωση αυτού του μοντέλου, ένας οργανισμός μπορεί να κατανοήσει καλύτερα τις απειλές που αντιμετωπίζει και πώς αυτές οι απειλές αλληλεπιδρούν κατά τη διάρκεια μιας επίθεσης

στην υποδομή του. Από εκεί, θα είναι σε θέση να προσαρμόσει τις απαιτήσεις πληροφοριών απειλών ώστε να ανταποκρίνονται καλύτερα στις μοναδικές του προκλήσεις.

Αναφορά για Απαιτήσεις Πληροφοριών Απειλών

Μία βασική αναφορά για τον προσδιορισμό των απαιτήσεων πληροφοριών απειλών είναι το **MITRE ATT&CK** **wiki**:

https://attack.mitre.org/wiki/Main_Page

Το ATT&CK (Adversarial Tactics, Techniques, & Common Knowledge) είναι μια εκτενής συλλογή τακτικών και τεχνικών που χρησιμοποιούνται από αντιπάλους. Οι τακτικές καλύπτουν κάθε στάδιο της αλυσίδας επίθεσης (kill chain) και περιλαμβάνουν ανάλυση κάθε τεχνικής σε βάθος.

Επιπλέον, το ATT&CK παρέχει λεπτομερείς πληροφορίες για διάφορες ομάδες APT που έχουν αναγνωριστεί από οργανισμούς ασφάλειας πληροφοριών και έρευνας περιστατικών. Οι καταχωρήσεις στο ATT&CK είναι καλά τεκμηριωμένες και με σημειώσεις, ώστε οι αναλυτές να μπορούν να δουν τόσο συνοπτική όσο και πλήρη αναφορά.

Η αξία του ATT&CK είναι ότι παρέχει στους αναλυτές λεπτομερείς πληροφορίες για τις ομάδες απειλών, τις τεχνικές και τις τακτικές τους. Αυτό μπορεί να ενημερώσει άλλα μοντέλα, όπως το Cyber Kill Chain και το Diamond Model, επιτρέποντας στους οργανισμούς να κατανοούν πλήρως τις απειλές και να ευθυγραμμίζουν τις απαιτήσεις πληροφοριών απειλών με τις ανάγκες τους.

Πηγές Πληροφοριών Απειλών

Υπάρχουν τρεις βασικές πηγές πληροφοριών απειλών που ένας οργανισμός μπορεί να αξιοποιήσει:

1. **Εσωτερικά ανεπτυγμένες πηγές:** Οι πιο σύνθετες πηγές απειλών είναι αυτές που αναπτύσσονται εσωτερικά από έναν οργανισμό, λόγω της υποδομής που απαιτείται για την απόκτηση **IOC** (Indicators of Compromise) από καμπάνιες malware και TTPs (Tactics, Techniques, and Procedures) από τους αντιπάλους. Για να αποκτηθούν IOC, ένας οργανισμός μπορεί να χρησιμοποιήσει **honeypots** ή άλλους σκόπιμα ευάλωτους συστήματα, να συλλέξει δείγματα malware και να πραγματοποιήσει **αντίστροφη μηχανική** (reverse engineering). Επιπλέον, πλατφόρμες όπως **SIEM** μπορούν να χρησιμοποιηθούν για την παρακολούθηση των TTPs των επιτιθέμενων. Οι αναλυτές SOC μπορούν να καταγράψουν τη συμπεριφορά διαφορετικών επιτιθέμενων, δημιουργώντας προφίλ συγκεκριμένων ομάδων και βοηθώντας στην ευθυγράμμιση των μέτρων ασφάλειας.
2. **Εμπορικές πηγές:** Εναλλακτικά, ένας οργανισμός μπορεί να χρησιμοποιήσει υπηρεσίες τρίτων, δηλαδή **προμηθευτές εμπορικών πληροφοριών απειλών**, οι οποίοι συλλέγουν, αναλύουν και ερευνούν malware και επιθέσεις. Οι προμηθευτές αυτοί μπορούν να προσαρμόσουν τις

πληροφορίες στον πελάτη και να προσφέρουν **SIEM** και υπηρεσίες **SOC**, αξιοποιώντας δεδομένα από πελάτες σε όλο τον κόσμο, προσφέροντας ένα ολοκληρωμένο προϊόν.

3. **Ανοιχτές πηγές (OSINT):** Οι πηγές **OSINT** (Open Source Intelligence) γίνονται ολοένα και πιο δημοφιλείς. Κοινότητες και εμπορικοί φορείς παρέχουν δωρεάν πληροφορίες για απειλές και ευπάθειες. Παραδείγματα περιλαμβάνουν SANS, US-CERT, και AlienVault Open Threat Exchange (OTX), όπου η κοινότητα μοιράζεται IOC και TTPs. Άλλοι οργανισμοί παρέχουν αναφορές για ομάδες APT και στρατηγικές απειλών.

Διαφορετικά πρότυπα για OSINT περιλαμβάνουν:

- **OpenIOC:** XML σχήμα για περιγραφή τεχνικών IOC.
- **STIX:** Machine-readable μορφή για ανταλλαγή πληροφοριών απειλών.
- **TAXII:** Πρωτόκολλο εφαρμογών για διαμοιρασμό πληροφοριών μέσω HTTPS.
- **VERIS:** Σχήμα για τυποποίηση καταγραφής περιστατικών κυβερνοασφάλειας και συλλογή δεδομένων.

Με τις διαθέσιμες πηγές, μία πρόκληση είναι η δυνατότητα συγκέντρωσης, οργάνωσης και αξιοποίησης των πληροφοριών απειλών. Η επόμενη ενότητα του κεφαλαίου εστιάζει στις **πλατφόρμες πληροφοριών απειλών (Threat Intelligence Platforms)** για την αντιμετώπιση αυτού του ζητήματος.

Μία από τις περιοχές πληροφόρησης που έχει γίνει ιδιαίτερα δημοφιλής σε οργανισμούς κάθε μεγέθους είναι οι πάροχοι OSINT. Κοινοτικές ομάδες και ακόμη και εμπορικές επιχειρήσεις κάνουν διαθέσιμη την πληροφορία απειλών (threat intelligence) στο ευρύ κοινό δωρεάν. Ομάδες όπως οι SANS και US-CERT παρέχουν συγκεκριμένες πληροφορίες σχετικά με απειλές και ευπάθειες. Εμπορικοί πάροχοι, όπως η AlienVault, προσφέρουν το Open Threat Exchange (OTX), που επιτρέπει στην κοινότητα χρηστών να μοιράζεται πληροφορίες απειλών όπως Indicators of Compromise (IOCs) και Tactics, Techniques, and Procedures (TTPs). Άλλες εμπορικές οργανώσεις παρέχουν whitepapers και αναφορές σχετικά με ομάδες APT ή στρατηγική πληροφορία για απειλές σχετικά με αναδυόμενες τάσεις στον κλάδο της ασφάλειας πληροφοριών. Ανάλογα με τον οργανισμό, το OSINT είναι συχνά πολύ χρήσιμο και παρέχει μια χαμηλού κόστους εναλλακτική λύση σε σχέση με εμπορικές υπηρεσίες.

Η ευρεία χρήση του OSINT οδήγησε διάφορους οργανισμούς στη δημιουργία μεθόδων για την ανταλλαγή πληροφοριών απειλών μεταξύ οργανισμών. Ανάλογα με την πηγή, ο τρόπος με τον οποίο ένας οργανισμός μπορεί να αποκτήσει πληροφορίες απειλών εξαρτάται από τον τρόπο που έχει διαμορφωθεί.

Αν και δεν είναι πλήρης κατάλογος, τα παρακάτω είναι ορισμένα από τα διαθέσιμα format OSINT για κυβερνοαπειλές:

- **OpenIOC:** Το OpenIOC αναπτύχθηκε αρχικά ώστε τα προϊόντα της Mandiant, όπως η εφαρμογή Redline που χρησιμοποιείται στο Κεφάλαιο 6, «Forensic Imaging», να μπορούν να εισάγουν πληροφορίες απειλών και να τις χρησιμοποιούν για την αναζήτηση στοιχείων

παραβίασης στα αναλυόμενα συστήματα. Έχει εξελιχθεί σε ένα XML σχήμα που περιγράφει τα τεχνικά IOCs που μπορεί να χρησιμοποιήσει ένας υπεύθυνος αντιμετώπισης περιστατικών για να προσδιορίσει αν ένα σύστημα έχει παραβιαστεί.

- **STIX:** Το Structured Threat Information Exchange (STIX) είναι προϊόν του OASIS consortium. Αυτό το μηχανικά αναγνώσιμο format επιτρέπει στους οργανισμούς να μοιράζονται πληροφορίες απειλών μέσω διάφορων εμπορικών και δωρεάν πλατφορμών συγκέντρωσης πληροφοριών απειλών.
- **TAXII:** Το Trusted Automated Exchange of Intelligence Information (TAXII) είναι ένα πρωτόκολλο επιπέδου εφαρμογής που μοιράζεται πληροφορίες απειλών μέσω HTTPS. Το TAXII ορίζει ένα API που μπορεί να χρησιμοποιηθεί για την ανταλλαγή πληροφοριών απειλών σε μορφή STIX.
- **VERIS:** Το Vocabulary for Event Recording and Incident Sharing (VERIS) είναι ένα ολοκληρωμένο σχήμα για την τυποποίηση της γλώσσας που χρησιμοποιείται σε περιστατικά κυβερνοασφάλειας. Το κύριο πρόβλημα που προσπαθεί να επιλύσει το σχήμα VERIS είναι η έλλειψη ενός τυποποιημένου τρόπου για την τεκμηρίωση των περιστατικών ασφάλειας. Το VERIS παρέχει μια δομή στην οποία οι οργανισμοί έχουν έναν καθορισμένο τρόπο να κατηγοριοποιούν την ποικιλία επιθέσεων που μπορεί να συμβούν. Το σχήμα VERIS χρησιμεύει επίσης ως σημείο συλλογής δεδομένων που παρέχονται από οργανισμούς και ενσωματώνονται στη Μελέτη Δεδομένων Παραβίασης της Verizon (Verizon Data Breach Study).

Με τη διαθεσιμότητα μιας ποικιλίας πηγών πληροφοριών, μία από τις προκλήσεις που προκύπτει είναι η ικανότητα των οργανισμών να συγκεντρώνουν, οργανώνουν και αξιοποιούν τις πληροφορίες απειλών. Στην επόμενη ενότητα, η συζήτηση γύρω από τις πλατφόρμες πληροφοριών απειλών θα προσφέρει μια εικόνα για την επίλυση αυτών των ζητημάτων.

13.7. Πλατφόρμες Threat Intelligence

Καθώς οι οργανισμοί αρχίζουν να συγκεντρώνουν πληροφορίες απειλών, είτε δημιουργούνται εσωτερικά είτε προέρχονται από εξωτερικές πηγές, θα χρειαστούν μια πλατφόρμα για να τις συγκεντρώνουν. Κάθε πλατφόρμα θα πρέπει να μπορεί να αποθηκεύει δείκτες απειλών (Indicators of Compromise – IOCs), καθώς και να παρέχει στους αναλυτές μια εύκολα αναζητήσιμη βάση δεδομένων που να τους επιτρέπει να συνδέουν IOCs από ένα περιστατικό με τις διαθέσιμες πληροφορίες. Υπάρχουν αρκετές εμπορικές πλατφόρμες, καθώς και εκδόσεις freeware, που παρέχουν στους αναλυτές αυτή τη δυνατότητα. Η επιλογή της κατάλληλης πλατφόρμας εξαρτάται από τις ανάγκες του κάθε οργανισμού.

Κοινοποίηση απειλών με το MISP: Μια δωρεάν πλατφόρμα που είναι διαθέσιμη είναι η **Malware Information Sharing Platform (MISP)**. Αυτό το κοινοτικό έργο έχει δημιουργήσει μια πλατφόρμα

λογισμικού που μπορούν να χρησιμοποιούν οι αναλυτές για να αποθηκεύουν δεδομένα σχετικά με κακόβουλο λογισμικό και άλλες εκμεταλλεύσεις (exploits). Από εκεί, μπορούν να μοιράζονται αυτές τις πληροφορίες εντός της ομάδας τους ή με άλλο προσωπικό. Το MISP είναι μια εφαρμογή πλούσια σε λειτουργίες, όπως αναζήτηση, μηχανή συσχέτισης, δυνατότητα εισαγωγής και εξαγωγής IOCs, και υποστήριξη από την κοινότητα, όπου οι χρήστες μπορούν να μοιράζονται δεδομένα.

Η εγκατάσταση του MISP εξαρτάται από τον τύπο του λειτουργικού συστήματος που χρησιμοποιείται. Οδηγίες εγκατάστασης υπάρχουν διαθέσιμες στο: <https://github.com/MISP/MISP/tree/2.4/INSTALL>. Οι δημιουργοί του MISP έχουν επίσης προσφέρει μια πλήρη εγκατάσταση σε μορφή **Open Virtualization Format (OVA) virtual machine**, η οποία μπορεί να κατεβεί για δοκιμές. Το αρχείο OVA είναι διαθέσιμο στο: https://www.circl.lu/assets/files/misp-training/MISP_v2.4.77.ova. Αυτή είναι μια καλή επιλογή καθώς επιτρέπει στους αναλυτές να δοκιμάσουν τη λειτουργικότητα της εφαρμογής χωρίς να χρειάζεται να γεμίσουν τη βάση δεδομένων.

Χρήση της πλατφόρμας MISP (παράδειγμα εκπαίδευσης): Για την παρακάτω επίδειξη θα χρησιμοποιηθεί η έκδοση εκπαίδευσης του MISP. Αφού συνδεθεί ο χρήστης, εμφανίζεται το ακόλουθο παράθυρο: Το παράθυρο περιέχει όλα τα **γεγονότα (events)** που έχει καταχωρημένα η βάση δεδομένων του MISP. Περιλαμβάνει πολλά δεδομένα, όπως ετικέτες που προσδιορίζουν την κατηγοριοποίηση των γεγονότων, την ημερομηνία προσθήκης τους και βασικές πληροφορίες που επιτρέπουν στους αναλυτές να ταξινομήσουν γρήγορα τις καταχωρήσεις.

Published	Org	Owner Org	Id	Clusters	Tags	#Attr	#Corr	Email	Date	Threat Level
☒	MISP	MISP	717		misp-galaxy:rat="Adwind RAT" tlp:white osint:source-type="blog-post"	24		admin@misp.training	2017-07-12	Low
☒	MISP	MISP	725		tlp:white osint:source-type="blog-post" enisa:nefarious-activity-abuse="mobile-malware"	146		admin@misp.training	2017-07-10	Low
☒	MISP	MISP	722		tlp:white certsi:critical-sector="energy" osint:source-type="blog-post"	22		admin@misp.training	2017-07-07	Low
☒	MISP	MISP	730		tlp:white	17		admin@misp.training	2017-07-06	Low

Κάνοντας κλικ σε ένα **Event ID** ή στο εικονίδιο **View** στα δεξιά ενός γεγονότος, ανοίγει ένα νέο παράθυρο:

Home

Event Actions

Galaxies

Input Filters

Global Actions

Sync Actions

Administration

Audit

MISP

Admin

Log out

View Event

View Correlation Graph

View Event History

Edit Event

Delete Event

Add Attribute

Add Attachment

Populate from...

Merge attributes from...

Propose Attribute

Propose Attachment

Publish event to ZMQ

Contact Reporter

Download as...

List Events

Add Event

OSINT - Spam Campaign Delivers Cross-platform Remote Ac...

Event ID717

Uuid59663a31-f174-44a6-adb7-4339950d210f

OrgCIRCL

Owner orgMISP

Contributors

Emailadmin@misp.training

Tagsmisp-galaxy:rat="Adwind RAT" x tlp:white x osint:source-type="blog-post" x +

Date2017-07-12

Threat LevelLow

AnalysisCompleted

DistributionAll communities

InfoOSINT - Spam Campaign Delivers Cross-platform Remote Access Trojan Adwind

PublishedYes

#Attributes24

Sightings0 (0) - restricted to own organisation only.

Activity

Pivots

Galaxy

Attributes

Discussion

717: OSINT ...

Galaxies

Add new cluster

previous

next

view all

Σε αυτό το παράθυρο, οι αναλυτές βλέπουν πολλές πληροφορίες για το συγκεκριμένο γεγονός. Πρώτα εμφανίζονται τα δεδομένα του γεγονότος, που είναι μια επισκόπηση των χαρακτηριστικών των IOCs που περιλαμβάνονται σε αυτό:

OSINT - Spam Campaign Delivers Cross-platform Remote Ac...

Event ID	717
Uuid	59663a31-f174-44a6-adb7-4339950d210f
Org	CIRCL
Owner org	MISP
Contributors	
Email	admin@misp.training
Tags	misp-galaxy:rat="Adwind RAT" x tlp:white x osint:source-type="blog-post" x +
Date	2017-07-12
Threat Level	Low
Analysis	Completed
Distribution	All communities
Info	OSINT - Spam Campaign Delivers Cross-platform Remote Access Trojan Adwind
Published	Yes
#Attributes	24
Sightings	0 (0) - restricted to own organisation only.
Activity	

Αυτά τα δεδομένα παρέχουν στους αναλυτές μια γενική εικόνα των πληροφοριών του γεγονότος που ήταν διαθέσιμες στην αρχική οθόνη. Πιο κάτω, το παράθυρο εμφανίζει τα συγκεκριμένα στοιχεία του γεγονότος:

2017-07-12	External analysis	link	https://www.virustotal.com/file/705325922c56c632ddb/analysis/1499247775/	+	BKDR64_AGENT.TYUCT - Xchecked via VT: 705325922c56c632ddb/analysis/1499247775/
2017-07-12	External analysis	link	https://www.virustotal.com/file/97d585b6aff62fb4e43e7e6a5f816dcd7a14be11a88b109a9ba9e8cd4c456eb9/analysis/1499851519/	+	JAVA_ADWIND.AUJC - Xchecked via VT: 97d585b6aff62fb4e43e7e6a5f816dcd7a14be11a88b109a9ba9e8cd4c456eb9

Σε αυτό το σημείο, ο συγκεκριμένος Trojan που αναφέρεται στις πληροφορίες έχει αξιολογηθεί από το VirusTotal και, ακολουθώντας τον σύνδεσμο, φαίνεται ότι 46 από 61 παρόχους antivirus έχουν εντοπίσει ότι το γεγονός σχετίζεται με Trojan:

46 / 61

Community Score

46 engines detected this file

705325922c56c632ddb
server.jar

jar

213.71 KB
Size

2019-02-26 10:41:49 UTC
7 months ago

DETECTION	DETAILS	RELATIONS	COMMUNITY 2
Ad-Aware	Trojan.GenericKD.3449865	AegisLab	Trojan.Win64.Agent.41c
AhnLab-V3	JAVA/Agent	ALYac	Trojan.Java.Adwind
Antiy-AVL	Trojan[Backdoor]/Win64.Agent	Arcabit	Trojan.Generic.D34A409
Avast	Win64:Malware-gen	AVG	Win64:Malware-gen
Avira (no cloud)	BDS/Agent.FL	BitDefender	Trojan.Generic.19649538
CAT-QuickHeal	Backdoor.Agent	ClamAV	Win.Trojan.Agent-1821671

Η πραγματική αξία της πλατφόρμας MISP είναι οι IOCs που συνδέονται με το γεγονός. Κατεβαίνοντας στο παράθυρο, ο αναλυτής μπορεί να δει τους μεμονωμένους δείκτες που σχετίζονται με το κακόβουλο λογισμικό αυτού του γεγονότος:

2017-07-12	Network activity	url	https://nup.pw/Qcaq5e.jar	+	Files and URLs related to Adwind/jRAT
2017-07-12	Network activity	url	http://vacanzaimmobiliare.it/testla/WebPanel/post.php	+	Related C&C servers:
2017-07-12	Network activity	url	http://ccb-ba.adv.br/wp-admin/network/ok/index.php	+	Files and URLs related to Adwind/jRAT
2017-07-12	Network activity	url	https://nup.pw/e2BXtK.exe	+	Files and URLs related to Adwind/jRAT

Από εδώ, ο αναλυτής μπορεί να εντοπίσει συγκεκριμένα URLs που συνδέονται είτε με επικοινωνίες C2 είτε αν το malware είναι μέρος μιας πολυφασικής επίθεσης. Στη συνέχεια, μπορεί να συσχετίσει αυτά τα URLs με logs του firewall ή να τα μπλοκάρει μέσω web proxy για να περιορίσει μια πιθανή εξάπλωση malware.

Πιο κάτω, υπάρχουν πιο συγκεκριμένες πληροφορίες δικτύου:

☐	2017-07-12	Payload delivery	ip-dst port	174.127.99.234:1033	+	Related C&C servers - Port 1033	☒
--------------------------	------------	------------------	-------------	---------------------	---	---------------------------------	-------------------------------------

Αυτές οι πληροφορίες επιτρέπουν στους αναλυτές να εστιάσουν σε συγκεκριμένη IP διεύθυνση και είτε να την μπλοκάρουν είτε να δημιουργήσουν ειδοποίηση στο σημείο εξόδου του δικτύου, ώστε να διαπιστώσουν αν υπάρχουν άλλα συστήματα που έχουν παραβιαστεί.

Το MISP επιτρέπει επίσης στους αναλυτές να δουν συγκεκριμένα αρχεία που σχετίζονται με το γεγονός:

☐	2017-07-12	Payload delivery	sha1	9ce4518ebcb5be6d1f0b5477fa00c26860fe9a68	+	JAVA_ADWIND.AUJC - Xchecked via VT: 97d585b6aff62fb4e43e7e6a5f816dcd7a14be11a88b109a9ba9e8cd4c456eb9	☒
☐	2017-07-12	Payload delivery	md5	781fb531354d6f291f1ccab48da6d39f	+	JAVA_ADWIND.AUJC - Xchecked via VT: 97d585b6aff62fb4e43e7e6a5f816dcd7a14be11a88b109a9ba9e8cd4c456eb9	☒
☐	2017-07-12	Payload delivery	sha256	705325922cfffac1bca8b1854913176f8b2df83a70e0df0c8d683ec56c6632ddb	+	BKDR64_AGENT.TYUCT	☒

Από εκεί, οι αναλυτές μπορούν να χρησιμοποιήσουν **images μνήμης ή δίσκου** και να αναζητήσουν αντίστοιχα hashes. Αυτό επιτρέπει στους αναλυτές αντίδρασης να εστιάσουν στα συγκεκριμένα αρχεία που χρειάζονται ανάλυση και δραστηριότητες αποκατάστασης.

Ενημέρωση και εμπλουτισμός δεδομένων απειλών

Οι πληροφορίες απειλών πρέπει να είναι **έγκαιρες** για να είναι αποτελεσματικές. Στον χώρο των κυβερνοεπιθέσεων, οι πληροφορίες γίνονται γρήγορα παρωχημένες. Κάθε πλατφόρμα που συγκεντρώνει πληροφορίες απειλών θα πρέπει να μπορεί να ενημερώνεται. Το MISP έχει τη δυνατότητα να ενσωματώνει διάφορες **πηγές πληροφοριών απειλών (threat intelligence feeds)** και να προσθέτει αυτά τα δεδομένα στην προβολή γεγονότων:

1. Για να γίνει επίδειξη, μεταβείτε στην καρτέλα **Sync Actions** και κάντε κλικ στο **List Feeds**.
2. Στη συνέχεια, μεταβείτε στην κάτω δεξιά γωνία και στο βέλος μέσα σε κύκλο. Αυτό θα φέρει όλα τα γεγονότα από την πηγή. Για παράδειγμα, πατήστε το κουμπί για την πηγή αριθμός πέντε. Μετά το συγχρονισμό, μια επιπλέον καταχώρηση εμφανίζεται στο παράθυρο των γεγονότων.

Ανάλογα με τον τύπο της πηγής πληροφοριών που χρησιμοποιεί ο οργανισμός, το MISP μπορεί να **εμπλουτίσει το dataset** του αξιοποιώντας σύνδεση με αυτές τις πηγές. Αυτό επιτρέπει στους αναλυτές να διατηρούν τα δικά τους δεδομένα από διάφορους παρόχους σε ένα ενιαίο, αναζητήσιμο μέρος. Στη

συνέχεια, μπορούν να χρησιμοποιήσουν αυτά τα δεδομένα είτε για προληπτική ανίχνευση είτε για υποστήριξη κατά τη διάρκεια διερεύνησης περιστατικών.

Feeds

Generate feed lookup caches

All Freetext/CSV MISP

« previous next »

Default feeds Custom Feeds All Feeds Enabled Feeds												
Id	Name	Feed Format	Provider	Input	Url	Target	Publish	Delta Merge	Override IDS	Distribution	Tag	Enabled
1	CIRCL OSINT Feed MISP	MISP Feed	CIRCL	network	https://www.circl.lu/doc/misp/feed-osint					All communities		✓
2	The Botvrij.eu Data MISP	MISP Feed	Botvrij.eu	network	http://www.botvrij.eu/data/feed-osint					All communities		✓
3	inThreat OSINT Feed MISP	MISP Feed	inThreat	network	https://feeds.inthreat.com/osint/misp/					Your organisation only	osint:source-type="block-or-filter-list"	✗
4	ZeuS IP blocklist (Standard) MISP	Simple CSV Parsed Feed	zeustracker.abuse.ch	network	https://zeustracker.abuse.ch/blocklist.php?download=ipblocklist	New fixed event	✗	✓	✓	Your organisation only	osint:source-type="block-or-filter-list"	✗
5	ZeuS compromised URL blocklist MISP	Simple CSV Parsed Feed	zeustracker.abuse.ch	network	https://zeustracker.abuse.ch/blocklist.php?download=compromised	Fixed event 733	✗	✓	✓	Your organisation only	osint:source-type="block-or-filter-list"	✓
6	blockrules of rules.emergingthreats.net MISP	Simple CSV Parsed Feed	rules.emergingthreats.net	network	http://rules.emergingthreats.net/blockrules/compromised-ips.txt	New fixed event	✗	✓	✓	Your organisation only	osint:source-type="block-or-filter-list"	✗

Η παρακάτω καταχώρηση αναφέρεται σε ένα γεγονός (event) που σχετίζεται με το ransomware Locky, το οποίο καταγράφηκε στις 26 Ιουνίου 2017. Ο μοναδικός αναγνωριστικός κωδικός του γεγονότος (Event ID) είναι 711, με UUID "550fd5be-4d9-92d9-4ba8950d10f" και ανήκει στον οργανισμό CIRCL (Computer Incident Response Center Luxembourg).

View Event
View Correlation Graph
View Event History
Edit Event
Delete Event
Add Attribute
Add Attachment
Populate from...
Merge attributes from...
Propose Attribute
Propose Attachment
Publish event to ZMQ
Contact Reporter
Download as...
List Events
Add Event

M2M - Locky 2017-06-26 : Affid=3 : "12_Invoice_3456" -...

Event ID	711
Uuid	5950fd85-deb8-4a7d-92c9-4ba8950d210f
Org	CIRCL
Owner org	MISP
Contributors	
Email	admin@misp.training
Tags	tlp:white x ecsirt:malicious-code="ransomware" x misp-galaxy:ransomware="Locky" x +
Date	2017-06-26
Threat Level	Low
Analysis	Ongoing
Distribution	All communities
Info	M2M - Locky 2017-06-26 : Affid=3 : "12_Invoice_3456" - "001_4321.zip"
Published	Yes
#Attributes	164
Sightings	0 (0) - restricted to own organisation only
Activity	

Pivots Galaxy Attributes Discussion

✗ 711: M2M - ...

Οι συνεισφέροντες περιλαμβάνουν τον "admin@misp.training", και οι ετικέτες (tags) περιγράφουν το γεγονός ως ransomware Locky, με επιπλέον αναφορές σε κακόβουλο κώδικα και γαλαξία MISP για ransomware.

Η ανάλυση του γεγονότος χαρακτηρίζεται ως "Ongoing" (σε εξέλιξη), με επίπεδο απειλής χαμηλό και διανομή σε όλες τις κοινότητες. Το γεγονός δημοσιεύτηκε στις 26 Ιουνίου 2017 και περιλαμβάνει 164 χαρακτηριστικά (#Attributes), με την πρόσβαση να είναι περιορισμένη στον ιδιοκτήτη οργανισμό (sightings: 0, restricted to own org only). Η πληροφορία υποδηλώνει ότι το Locky διανεμήθηκε μέσω ενός συμπίεσμένου αρχείου ("001_4321.zip"), το οποίο πιθανότατα περιείχε ένα παραπλανητικό τιμολόγιο ("12_Invoice_3456") ως δόλωμα για να εξαπατήσει τους χρήστες.

Η καταχώρηση περιλαμβάνει επιλογές για διαχείριση, όπως προβολή του γραφήματος συσχέτισης, ιστορικού γεγονότων, επεξεργασία, διαγραφή, προσθήκη χαρακτηριστικών ή συνημμένων, και σύνδεση με το σύστημα διαχείρισης μηνυμάτων ZMQ. Η παρουσία του Locky, ενός γνωστού ransomware που κρυπτογραφεί αρχεία και απαιτεί λύτρα, υπογραμμίζει τη σοβαρότητα του γεγονότος, ενώ η ημερομηνία και οι λεπτομέρειες δείχνουν μια συγκεκριμένη καμπάνια που εντοπίστηκε και καταγράφηκε από την CIRCL για περαιτέρω έρευνα και κοινή χρήση πληροφοριών.

13.8. Χρήση πληροφοριών απειλών (Threat Intelligence)

Υπάρχουν δύο σαφή πλεονεκτήματα στην ενσωμάτωση πληροφοριών απειλών στη μεθοδολογία ασφάλειας και στην ικανότητα αντίδρασης ενός οργανισμού. Από την **προληπτική προσέγγιση**, οι οργανισμοί μπορούν να χρησιμοποιούν αυτά τα δεδομένα για να αυξήσουν την αποτελεσματικότητα των ελεγκτικών και προληπτικών μηχανισμών τους. Αυτό επιτρέπει στους οργανισμούς να ενισχύσουν την ικανότητά τους είτε να **αποκλείουν επιθέσεις** μέσω μηχανισμών όπως η μαύρη λίστα γνωστών κακόβουλων ιστοτόπων, είτε μέσω της ικανότητας ανίχνευσης, ειδοποιώντας για συγκεκριμένη συμπεριφορά κεντρικών συστημάτων που υποδηλώνει πιθανή παραβίαση.

Από μια **αντιδραστική προσέγγιση**, οι οργανισμοί μπορούν να ενσωματώσουν τις πληροφορίες απειλών στο υπάρχον σύνολο εργαλείων τους και να τις χρησιμοποιήσουν σε μια διερεύνηση. Αυτό τους επιτρέπει να εντοπίσουν στοιχεία που μπορεί να είχαν παραμείνει αδιόρατα με παραδοσιακές μεθόδους πληροφορίας.

Προληπτική πληροφορία απειλών

Οι πάροχοι πληροφοριών απειλών συχνά παρέχουν στις ομάδες CSIRT και SOC δεδομένα που μπορούν εύκολα να ενσωματωθούν στο SIEM της επιλογής τους. Αυτό επιτρέπει σε αυτές τις ομάδες να ενισχύσουν την ικανότητά τους ανίχνευσης με **έγκαιρη πληροφόρηση**, ενδεχομένως επιτρέποντάς τους να παρακολουθούν τις τρέχουσες απειλές και να αυξάνουν την πιθανότητα να ανιχνεύσουν μία ή περισσότερες από αυτές πριν προκληθεί ζημιά.

Στην πλατφόρμα **MISP**, τα γεγονότα με συγκεκριμένα **IOC** μπορούν να μετατραπούν σε διάφορους τύπους κανόνων ανίχνευσης. Για παράδειγμα, ένας οργανισμός ανησυχεί για **ransomware** που μπορεί να επηρεάσει τον οργανισμό και θέλει να ενισχύσει την ικανότητά του στην ανίχνευση. Το γεγονός αριθμός 225 στην πλατφόρμα MISP σχετίζεται με την καμπάνια ransomware **Locky**. Κάνοντας κλικ στον αριθμό του γεγονότος εμφανίζεται η ακόλουθη οθόνη:



Μεταβείτε στην αριστερή στήλη και κάντε κλικ στο **Download as....** Αυτό εμφανίζει το ακόλουθο παράθυρο:

Choose the format that you wish to export the event in

MISP XML (metadata + all attributes)	Encode Attachments ☒
MISP JSON (metadata + all attributes)	Encode Attachments ☒
OpenIOC (all indicators marked to IDS)	
CSV	Include non-IDS marked attributes ☐
STIX XML (metadata + all attributes)	Encode Attachments ☐
STIX JSON (metadata + all attributes)	Encode Attachments ☐
RPZ Zone file	
Download Suricata rules	
Download Snort rules	
Download Bro rules	
Export all attribute values as a text file	Include non-IDS marked attributes ☐
Cef Export	

Cancel

Από προληπτική/ανιχνευτική σκοπιά, οι αναλυτές μπορούν να εξάγουν τα **IOC** ως κανόνα για τρία ανοιχτού κώδικα συστήματα ανίχνευσης εισβολών δικτύου. Σε αυτήν την περίπτωση, οι κανόνες μπορούν να εξαχθούν για **Suricata**, **Snort** ή **Bro**. Κάθε ένα από αυτά είναι ένα σύστημα ανίχνευσης εισβολών δικτύου ανοιχτού κώδικα που εξετάζει την κυκλοφορία δικτύου και τη συγκρίνει με ένα καθορισμένο σύνολο κανόνων.


```
1 #This part might still contain bugs, use and your own risk and report any issues.
2 #
3 # MISP export of IDS rules - optimized for snort
4 #
5 # These NIDS rules contain some variables that need to exist in your configuration.
6 # Make sure you have set:
7 #
8 # $HOME_NET - Your internal network range
9 # $EXTERNAL_NET - The network considered as outside
10 # $SMTP_SERVERS - All your internal SMTP servers
11 # $HTTP_PORTS - The ports used to contain HTTP traffic (not required with suricata export)
12 #
13 alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg: "MISP e711 [] Outgoing HTTP URL:
14 alert udp any any -> any 53 (msg: "MISP e711 [] Hostname: 1010technologies.com"; content:"|
15 alert tcp any any -> any 53 (msg: "MISP e711 [] Hostname: 1010technologies.com"; content:"|
```

Κάθε εργαλείο έχει συγκεκριμένη **σύνταξη για τους κανόνες ανίχνευσης**. Για παράδειγμα, θα εξεταστεί ο κανόνας Snort. Κατεβάστε τον κανόνα Snort που σχετίζεται με αυτό το γεγονός κάνοντας κλικ στο **Download Snort rules**. Το αρχείο θα κατέβει. Αφού ολοκληρωθεί, ανοίξτε το αρχείο με έναν επεξεργαστή κειμένου και θα φανούν οι διάφοροι κανόνες που συνδέονται με το γεγονός:

Υπάρχουν πολλοί κανόνες που μπορούν να οριστούν με αυτή τη λήψη. Εξετάζοντας τη γραμμή 14, για παράδειγμα, φαίνεται ότι ο συγκεκριμένος κανόνας καθορίζει το Snort να σας ειδοποιεί εάν υπάρχει οποιαδήποτε προσπάθεια σύνδεσης μέσω **UDP port 53** προς τον host **1010technologies.com**. Αυτός ο host σχετίζεται με την καμπάνια ransomware με κάποιο τρόπο. Εάν ενσωματωθεί αυτός ο κανόνας, ο οργανισμός θα ειδοποιείται για αυτόν τον τύπο σύνδεσης και θα μπορεί να αντιδράσει πολύ πιο γρήγορα, σε αντίθεση με το να ανακαλύψει τη δραστηριότητα ransomware όταν ένας χρήστης επικοινωνεί με το helpdesk δηλώνοντας ότι τα αρχεία του έχουν κρυπτογραφηθεί.

Το πλεονέκτημα των κανόνων Snort είναι ότι πολλοί **εμπορικοί πάροχοι IDS/IPS** έχουν τη δυνατότητα να ενσωματώνουν κανόνες Snort στην ιδιόκτητη πλατφόρμα τους. Αυτό επιτρέπει στο προσωπικό SOC και CSIRT να φορτώνει αυτούς τους κανόνες από διάφορες πηγές, ενισχύοντας τις δυνατότητές τους χωρίς να χρειάζεται να διατηρούν πολλές διαφορετικές πλατφόρμες.

Αντιδραστική πληροφορία απειλών

Κατά τη διάρκεια μιας διερεύνησης, το CSIRT ή οι αναλυτές μπορεί να βρεθούν σε κατάσταση όπου μια **έρευνα περιστατικού φαίνεται να έχει σταματήσει**. Αυτό μπορεί να συμβαίνει επειδή οι αναλυτές γνωρίζουν ότι κάτι δεν πάει καλά ή έχουν δείκτες παραβίασης, αλλά δεν διαθέτουν **συγκεκριμένα αποδεικτικά στοιχεία** για να κατευθύνουν την έρευνα. Οι πληροφορίες απειλών μπορούν να αξιοποιηθούν από τους αναλυτές για να ενισχύσουν την ικανότητά τους να ανακαλύπτουν στοιχεία που προηγουμένως δεν είχαν εντοπιστεί.

13.8. Autopsy

Υπάρχουν πολλοί διαθέσιμοι εργαλεία που μπορούν να επεξεργαστούν threat intelligence και να χρησιμοποιηθούν από αναλυτές incident response. Για παράδειγμα, οι πλατφόρμες forensics δίσκων που αναφέρθηκαν στο Κεφάλαιο 8, *Analyzing System Memory*, έχουν τη δυνατότητα να εισάγουν hashes από feeds threat intelligence για την αναζήτηση IOCs.

uuid	event_id	category	type	value	comment	to_ids	date
5950fd86-	711	Artifacts dropped	md5	8cd9f803947baddbafac584edfdeebb		1	20170627
5950fd87-	711	Artifacts dropped	md5	a0d81f0bffb0e20a34191385031cf17a		1	20170627
59520c6b-	711	Artifacts dropped	sha1	f5fce485a72ab82a5e5b48b98befd5e0568a83e1	#NAME?	1	20170627
59520c6b-	711	Artifacts dropped	sha256	83b366204ef60cca5468c2db1baadeb7590f97493c451fa005f9b583ce691133	- Xchecked	1	20170627
59520c6b-	711	Artifacts dropped	sha1	3e19f754ea0fef9e62d91dfd4f22e6c73240bcbc	- Xchecked	1	20170627
59520c6b-	711	Artifacts dropped	sha256	8015133c16d41fdfeb5f86f5d82ffb124a131ed012375d3cf70babe2f440ac8	#NAME?	1	20170627

Εκτός από τα εμπορικά εργαλεία forensics δίσκων, η πλατφόρμα Autopsy μπορεί να εκτελεί αναζητήσεις βάσει ενός hash set. Επιστρέφοντας στη μορφή εξαγωγής στο MISP, υπάρχει η δυνατότητα λήψης ενός αρχείου .csv με τους δείκτες του event. Για το event 711, κατεβάστε το αρχείο CSV. Στη συνέχεια, φιλτράρετε τα δεδομένα και επιλέξτε τις τιμές hash από τη στήλη τύπου. Αυτό παράγει την ακόλουθη λίστα:

Από εδώ, οι τιμές hash μπορούν να φορτωθούν στο Autopsy:

1. Στο Autopsy, κάντε κλικ στο *Tools* και έπειτα στο *Options*. Μετά, κάντε κλικ στο *Hash Sets* και στη συνέχεια στο *New Hash Set*. Θα εμφανιστεί το ακόλουθο παράθυρο:

2. Εισάγετε ένα όνομα για το hash set. Προτείνεται να χρησιμοποιηθεί ένας τίτλος μαζί με τον αριθμό του MISP event, π.χ., 711. Κάντε κλικ στο *Save As...* και επιλέξτε πού θα αποθηκευτεί η βάση δεδομένων. Αφήστε τις προεπιλεγμένες ρυθμίσεις. Αυτό θα σημαίνει ότι θα υπάρχει ταίριασμα με οποιοδήποτε από τα αρχεία hash που βρίσκονται εκεί. Κάντε κλικ στο *OK*.
3. Στο επόμενο παράθυρο, κάντε κλικ στο *Add Hashes to Database*. Αντιγράψτε τα hashes από το αρχείο CSV και κάντε δεξί κλικ στον κενό χώρο, επιλέγοντας *Paste*.

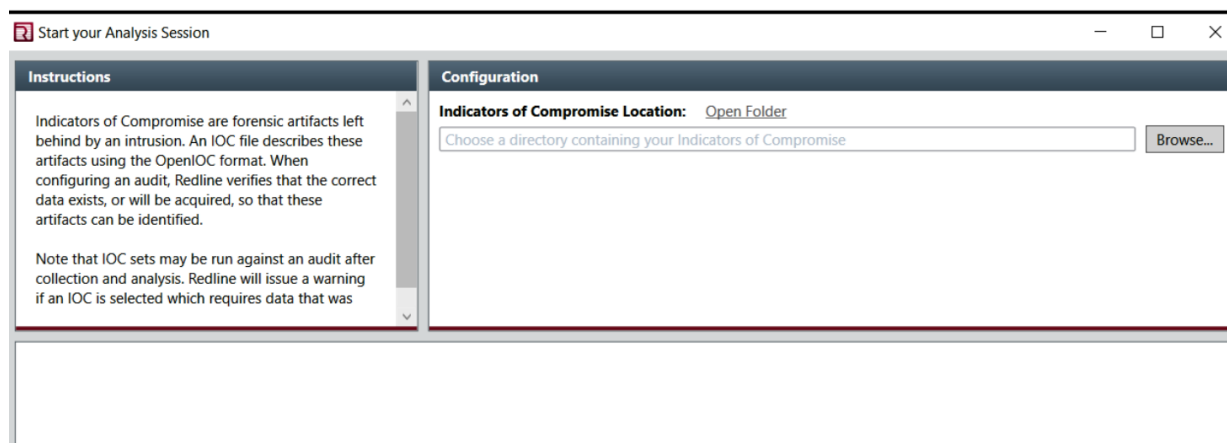
4. Τα hashes έχουν πλέον φορτωθεί. Κάντε κλικ στο *Add Hashes to Database*.

Αυτή η δυνατότητα επιτρέπει στους αναλυτές να αναζητούν μέσα σε εικόνες δίσκων για ταιριασμένα hashes. Είναι πολύ πιο αποτελεσματικός τρόπος αναζήτησης αποδεικτικών στοιχείων από την προσπάθεια εύρεσης των αρχείων με άλλες μεθόδους. Το Autopsy επιτρέπει επίσης διαφορετικές βάσεις δεδομένων ανάλογα με το περιστατικό. Η δυνατότητα συνεχούς τροφοδότησης ενημερωμένων πληροφοριών επιτρέπει στους αναλυτές να εντοπίζουν αποδείξεις ενός νέου τύπου συμβιβασμού από ένα γεγονός πριν από μία ή δύο εβδομάδες, το οποίο θα είχε παραμείνει ανεκτό αν χρησιμοποιούσαν παραδοσιακές μεθόδους αναζήτησης.

Προσθήκη IOC's στο Redline

Η threat intelligence μπορεί επίσης να χρησιμοποιηθεί με το Redline. Το Redline επιτρέπει αναζήτηση IOC's μέσω ενός collector, ή τα IOC's μπορούν να φορτωθούν και να αναζητηθούν σε μια υπάρχουσα καταγραφή μνήμης. Για παράδειγμα, αν οι αναλυτές θέλουν να αναζητήσουν ταιριασμένα IOC's σε μια εικόνα μνήμης:

1. Στην κάτω-αριστερή γωνία, κάντε κλικ στην καρτέλα *IOC Reports*. Αυτό θα δημιουργήσει ένα νέο κουμπί με τίτλο *Create a New IOC Report*.

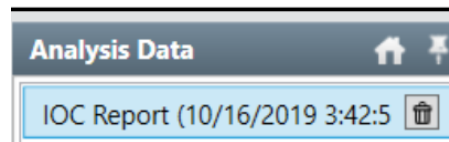


2. Το Redline έχει τη δυνατότητα να εισάγει IOC's σε μορφή OpenIOC. Οι αναλυτές θα πρέπει να δημιουργήσουν έναν φάκελο στο σύστημά τους όπου θα τοποθετηθούν τα αρχεία IOC, καθώς το Redline δεν θα διαβάσει ένα μόνο αρχείο αλλά όλα τα αρχεία IOC μέσα στον φάκελο.

Indicator Information

Name: APT30 (REPORT)
Author: FireEye **Created:** 4/10/2015 2:51:19 PM
Path: D:\IOCs\APT30\eeffc8e8-caee-4fe1-8ace-7a994b5d893f.ioc
Description: This IOC contains indicators detailed in the "APT30 and the Mechanics of a Long-Running Cyber Espionage Operation" report that can be read here: https://www.fireeye.com/blog/threat-research/2015/04/apt_30_and_the_mecha.html This IOC contains indicators for the BACKSPACE, NETEAGLE, SHIPSHAPE, SPACESHIP, and FLASHFLOOD malware families that are attributed to APT30.

3. Κάντε κλικ στο *Browse* και επιλέξτε το φάκελο με τα IOC. Τα IOCs φορτώνονται και οι σχετικές πληροφορίες εμφανίζονται στην πλατφόρμα Redline.



4. Κάνοντας κλικ στο *OK*, τα IOCs εκτελούνται πάνω στην καταγραφή μνήμης. Ανάλογα με τον αριθμό των αρχείων IOC και την εικόνα μνήμης, η διαδικασία μπορεί να διαρκέσει μερικά λεπτά. Μόλις ολοκληρωθεί, η αναφορά IOC θα εμφανιστεί στην ενότητα *Analysis Data*. Οποιοδήποτε ταίριασμα με IOCs θα εμφανιστεί εκεί.

13.9. Yara και Loki

Δύο ενσωματωμένα εργαλεία που επιτρέπουν τη χρήση threat intelligence κατά τη διάρκεια ενός περιστατικού είναι τα **Yara** και **Loki**.

Branch: master rules / malware / APT_Cobalt.yar Find file Copy path

jholgui Updated and renamed name file APT_FIN7 76d87e8 on Sep 11

1 contributor

25 lines (18 sloc) 705 Bytes Raw Blame History

```
1  /*
2      This Yara ruleset is under the GNU-GPLv2 license (http://www.gnu.org/licenses/gpl-2.0.html) and open to any user or organization, as
3
4  */
5  rule Cobalt_functions
6  {
7
8      meta:
9
10         author="@j0sm1"
11         url="https://www.securityartwork.es/2017/06/16/analisis-del-powershell-usado-fin7/"
12         description="Detect functions coded with ROR edi,D; Detect CobaltStrike used by differents groups APT"
13
14     strings:
15
16         $h1={58 A4 53 E5} // VirtualAllocEx
17         $h2={4C 77 26 07} // LoadLibraryEx
18         $h3={6A C9 9C C9} // DNSQuery_UTF8
19         $h4={44 F0 35 E0} // Sleep
20         $h5={F4 00 8E CC} // strlen
21
22     condition:
23         2 of ( $h* )
24 }
```

- Το **Yara** συχνά αναφέρεται ως "Swiss Army Knife" της ανίχνευσης προτύπων. Δημιουργήθηκε για να βοηθά τους ερευνητές malware στην ταξινόμηση κακόβουλου λογισμικού. Μέσω boolean εκφράσεων και strings, ένα δείγμα malware μπορεί να ταξινομηθεί.
- Ένα παράδειγμα κανόνα Yara για παραλλαγή του Cobalt Strike δείχνει πώς το Yara μπορεί να ειδοποιεί για οποιοδήποτε string αναγνωρίζεται ως Cobalt_functions.

Το Yara είναι διαθέσιμο ως εργαλείο για χρήση στην έρευνα malware, αλλά ένα από τα χρήσιμα χαρακτηριστικά είναι η δυνατότητα ενσωμάτωσής του σε άλλα εργαλεία. Ένα τέτοιο εργαλείο είναι το **Loki**—ένας απλός IOC scanner. Αυτή η ελαφριά πλατφόρμα επιτρέπει στους αναλυτές incident response να σαρώσουν φακέλους, αρχεία ή ακόμα και ολόκληρους δίσκους για IOCs, όπως κανόνες Yara, γνωστά κακόβουλα hashes, filename IOCs και γνωστούς C2 servers. Το Loki περιλαμβάνει μια εκτενή βιβλιοθήκη IOCs που ενημερώνεται τακτικά.

Για τη χρήση του Loki:

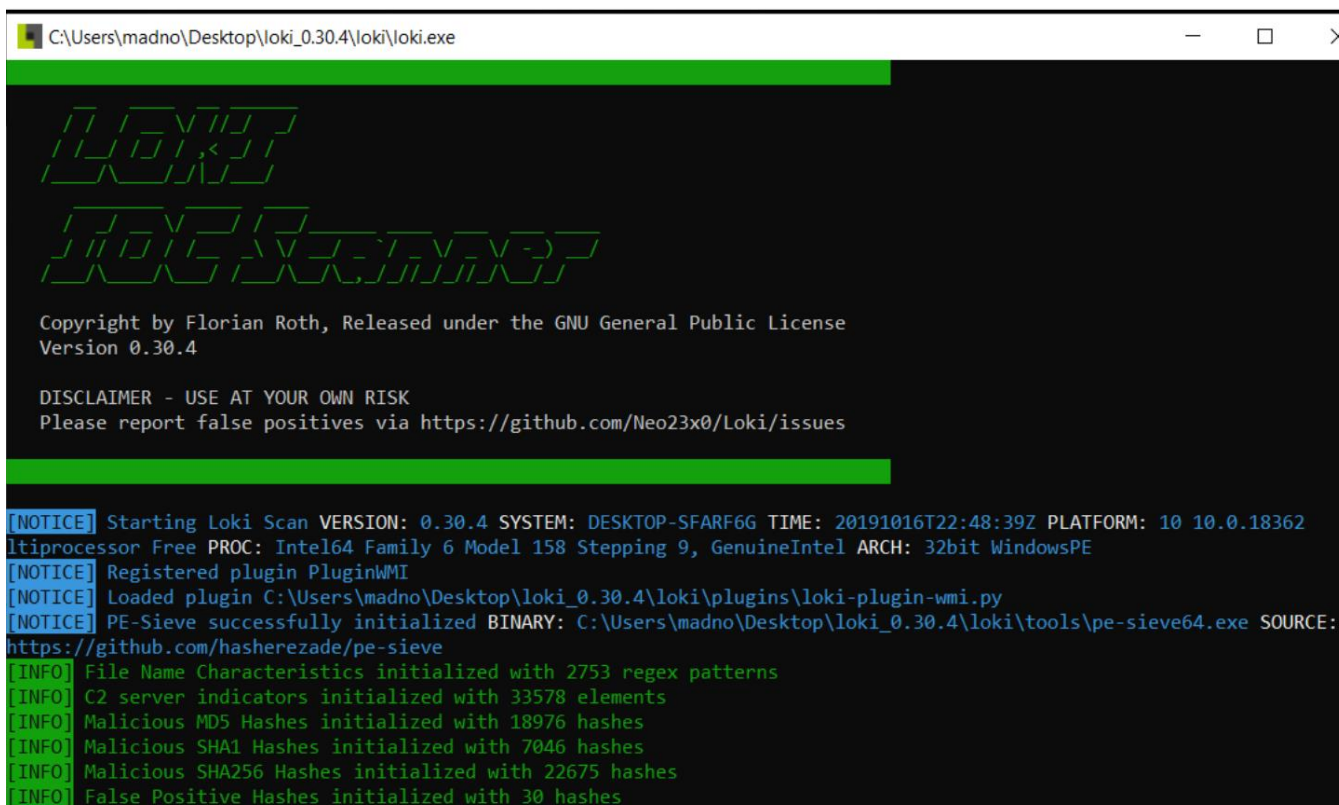
1. Κατεβάστε και αποσυμπιέστε το Loki σε μια συσκευή USB.

	config	10/16/2019 3:44 PM	File folder	
	docs	10/16/2019 3:44 PM	File folder	
	plugins	10/16/2019 3:44 PM	File folder	
	tools	10/16/2019 3:44 PM	File folder	
	LICENSE	10/16/2019 3:44 PM	File	35 KB
	loki	10/16/2019 3:44 PM	Application	9,174 KB
	loki-upgrader	10/16/2019 3:44 PM	Application	8,419 KB
	README.md	10/16/2019 3:44 PM	MD File	14 KB
	requirements	10/16/2019 3:44 PM	Text Document	1 KB

2. Εκτελέστε τον lokiupgrader ως διαχειριστής για να ενημερωθούν τα εκτελέσιμα και τα αρχεία signatures.
3. Επιστρέψτε στο φάκελο Loki και θα δείτε ένα νέο αρχείο signature-base που περιέχει όλα τα IOCs που μπορεί να σαρώσει η πλατφόρμα. Οι αναλυτές μπορούν επίσης να φορτώσουν δικούς τους κανόνες Yara εδώ.

	config	10/16/2019 3:44 PM	File folder	
	docs	10/16/2019 3:44 PM	File folder	
	plugins	10/16/2019 3:44 PM	File folder	
	signature-base	10/16/2019 3:46 PM	File folder	
	tools	10/16/2019 3:44 PM	File folder	
	LICENSE	10/16/2019 3:46 PM	File	35 KB
	loki	10/16/2019 3:46 PM	Application	9,174 KB
	loki-upgrade	10/16/2019 3:46 PM	Text Document	53 KB
	loki-upgrader	10/16/2019 3:44 PM	Application	8,419 KB
	README.md	10/16/2019 3:46 PM	MD File	14 KB
	requirements	10/16/2019 3:46 PM	Text Document	1 KB

4. Για να σαρώσετε ένα σύστημα, εκτελέστε την εφαρμογή Loki ως διαχειριστής. Μετά την ενημέρωση των κανόνων, το Loki θα ξεκινήσει την αναζήτηση στον δίσκο για ταιριαστά μοτίβα ή IOCs.



Η εικόνα δείχνει την έξοδο της εκτέλεσης του εργαλείου Loki, μιας open-source λύσης ανίχνευσης κακόβουλου λογισμικού, η οποία αναπτύχθηκε από τον Florian Roth και κυκλοφορεί υπό την GNU General Public License, έκδοση 0.30.4. Το εργαλείο ξεκινά μια σάρωση (scan) στο σύστημα DESKTOP-SFARF6G στις 10 Ιουνίου 2019 στις 16:22:48, σε μια πλατφόρμα Windows 10 (έκδοση 10.0.18362) με επεξεργαστή Intel Core Family 6, Model 158, Stepping 9. Η σάρωση χρησιμοποιεί το πρόσθετο (plugin) "loki-plugin-wmi.py" και το δυαδικό αρχείο "pe-sieve64.exe" από το GitHub αποθετήριο "hasherazade/pe-sieve", το οποίο υποστηρίζει την ανάλυση εκτελέσιμων αρχείων PE.

Η εκκίνηση της σάρωσης περιλαμβάνει την αρχικοποίηση διάφορων βάσεων δεδομένων και δεικτών για την ανίχνευση απειλών. Συγκεκριμένα, αρχικοποιούνται 2753 regex μοτίβα για την ανάλυση χαρακτηριστικών ονομάτων αρχείων, 3358 στοιχεία για ενδείξεις διακομιστή C2 (command-and-control), και εκτεταμένες λίστες κατακερματισμών (hashes) για κακόβουλα δεδομένα: 18976 MD5 hashes, 7046 SHA1 hashes, 22675 SHA256 hashes, και 730 false positive hashes. Αυτές οι βάσεις δεδομένων επιτρέπουν στο Loki να συγκρίνει τα σαρωθέντα αρχεία με γνωστές υπογραφές κακόβουλου λογισμικού, βοηθώντας στην ταυτοποίηση πιθανών απειλών.

Το εργαλείο συνοδεύεται από μια προειδοποίηση (DISCLAIMER) που τονίζει ότι η χρήση γίνεται με δική σας ευθύνη, και ενθαρρύνει την αναφορά ψευδών θετικών (false positives) μέσω του GitHub του έργου. Αυτή η προσέγγιση αντικατοπτρίζει την ανοιχτή φύση του εργαλείου και την εξάρτησή του από την κοινότητα για τη βελτίωση της ακρίβειας. Συνολικά, η έκδοση υποδεικνύει ότι το Loki είναι έτοιμο να σαρώσει το σύστημα για κακόβουλο λογισμικό, αξιοποιώντας μια ισχυρή βάση δεδομένων και προσαρμόσιμα πρόσθετα για την ανίχνευση πιθανών απειλών σε πραγματικό χρόνο.

Το Loki μπορεί να αναπτυχθεί σε πολλαπλά συστήματα για triage ύποπτων συστημάτων. Για παράδειγμα, ένας αναλυτής incident response μπορεί να αναζητήσει IOC του ransomware Petya χρησιμοποιώντας κανόνες Yara από έναν πάροχο threat intelligence, όπως το Kaspersky Securelist.



```
C:\Users\madno\Desktop\loki_0.30.4\loki\loki.exe
[INFO] Scanning Process PID: 6732 NAME: svchost.exe OWNER: SYSTEM CMD: C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s NgcSvc PATH: C:\Windows\system32\svchost.exe
[INFO] PE-Sieve reported no anomalies PID: 6732 NAME: svchost.exe OWNER: SYSTEM CMD: C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s NgcSvc PATH: C:\Windows\system32\svchost.exe
[INFO] Scanning Process PID: 6780 NAME: svchost.exe OWNER: LOCAL SERVICE CMD: C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s NgcCntrSvc PATH: C:\Windows\system32\svchost.exe
[INFO] PE-Sieve reported no anomalies PID: 6780 NAME: svchost.exe OWNER: LOCAL SERVICE CMD: C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s NgcCntrSvc PATH: C:\Windows\system32\svchost.exe
[INFO] Scanning Process PID: 6848 NAME: svchost.exe OWNER: madno CMD: C:\Windows\system32\svchost.exe -k ClipboardSvcGroup -p -s cbdhsvc PATH: C:\Windows\system32\svchost.exe
[INFO] PE-Sieve reported no anomalies PID: 6848 NAME: svchost.exe OWNER: madno CMD: C:\Windows\system32\svchost.exe -k ClipboardSvcGroup -p -s cbdhsvc PATH: C:\Windows\system32\svchost.exe
[WARNING] svchost.exe process owner is suspicious PID: 6848 NAME: svchost.exe OWNER: madno CMD: C:\Windows\system32\svchost.exe -k ClipboardSvcGroup -p -s cbdhsvc PATH: C:\Windows\system32\svchost.exe
[INFO] Scanning Process PID: 764 NAME: StartMenuExperienceHost.exe OWNER: madno CMD: "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe" -ServerName:App.AppXywbbrabmsek0gm3tkwpr5kwzbs55tkqay.mca PATH: C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe
[INFO] PE-Sieve reported no anomalies PID: 764 NAME: StartMenuExperienceHost.exe OWNER: madno CMD: "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe" -ServerName:App.AppXywbbrabmsek0gm3tkwpr5kwzbs55tkqay.mca PATH: C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe
[INFO] Scanning Process PID: 940 NAME: RuntimeBroker.exe OWNER: madno CMD: C:\Windows\System32\RuntimeBroker.exe -Embedding PATH: C:\Windows\System32\RuntimeBroker.exe
[INFO] PE-Sieve reported no anomalies PID: 940 NAME: RuntimeBroker.exe OWNER: madno CMD: C:\Windows\System32\RuntimeBroker.exe -Embedding PATH: C:\Windows\System32\RuntimeBroker.exe
[INFO] Scanning Process PID: 7256 NAME: SearchUI.exe OWNER: madno CMD: "C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe" -ServerName:CortanaUI.AppXa50dqq5gqv4a428c9y1jjw7m3btvepj.mca PATH: C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe
```

Η εικόνα παρουσιάζει την έξοδο του εργαλείου Loki (έκδοση 0.30.4), το οποίο εκτελείται από τον χρήστη "madno" σε έναν υπολογιστή με Windows, με σκοπό την ανίχνευση κακόβουλου λογισμικού. Η σάρωση ξεκινά με την ανάλυση διαφόρων διεργασιών (processes) που τρέχουν στο σύστημα, όπως το "svchost.exe", το "StartMenuExperienceHost.exe", το "RuntimeBroker.exe", και το "SearchUI.exe". Κάθε διεργασία παρακολουθείται με βάση το PID (Process ID), το όνομα, τον κάτοχο (OWNER), την εντολή εκκίνησης (CMD), και τη διαδρομή (PATH), ενώ το εργαλείο PE-Sieve χρησιμοποιείται για την ανίχνευση ανωμαλιών, χωρίς να εντοπίζονται προβλήματα σε αυτή την έξοδο.

Οι διεργασίες "svchost.exe" εμφανίζονται πολλαπλές φορές με διαφορετικά PIDs (6732, 6780, 6848) και κατόχους (SYSTEM, LOCAL SERVICE, madno), υποδεικνύοντας ότι πρόκειται για τη γνωστή υπηρεσία φιλοξενίας (Service Host) του Windows, η οποία φιλοξενεί διάφορες υπηρεσίες συστήματος. Οι παραλλαγές περιλαμβάνουν διαφορετικές ομάδες (groups) όπως "NgCsvc" και

"ClipboardSvcGroup", με τις περισσότερες να τρέχουν από τη διαδρομή "C:\Windows\system32\svchost.exe". Η απουσία ανωμαλιών από το PE-Sieve υποδηλώνει ότι αυτές οι διεργασίες φαίνονται νόμιμες μέχρι στιγμής.

Άλλες διεργασίες, όπως το "StartMenuExperienceHost.exe" (PID: 764), το "RuntimeBroker.exe" (PID: 940), και το "SearchUI.exe" (PID: 7256), είναι μέρη της σύγχρονης διεπαφής χρήστη του Windows 10, που τρέχουν από διαδρομές όπως "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_" και "C:\Windows\SystemApps\Microsoft.Windows.Cortana_". Αυτές οι διεργασίες συνδέονται με το μενού Έναρξης, τη διαχείριση δικαιωμάτων, και την αναζήτηση Cortana αντίστοιχα, και επίσης δεν παρουσιάζουν ανωμαλίες σύμφωνα με το PE-Sieve. Η έξοδος αυτή υποδηλώνει ότι η σάρωση του Loki δεν εντόπισε κακόβουλη δραστηριότητα σε αυτές τις διεργασίες, αν και η πλήρης ανάλυση μπορεί να απαιτεί περισσότερο χρόνο ή επιπλέον δεδομένα.

Οι κανόνες Yara μπορούν στη συνέχεια να τροφοδοτηθούν στο Loki ή σε άλλη πλατφόρμα για triage ύποπτων συστημάτων.

Από εδώ, ο αναλυτής μπορεί να καταγράψει τυχόν εντοπισμένα αποτελέσματα και να πραγματοποιήσει περαιτέρω ανάλυση αργότερα. Ένα ακόμα σημαντικό χαρακτηριστικό είναι ότι το Loki μπορεί να αναπτυχθεί σε πολλαπλά συστήματα ως μέρος της αξιολόγησης (triage) συστημάτων που ενδέχεται να έχουν μολυνθεί από μια νέα παραλλαγή κακόβουλου λογισμικού. Για παράδειγμα, ένας αναλυτής απόκρισης περιστατικών μπορεί να αναζητήσει τα IOC του ransomware Petya χρησιμοποιώντας κανόνες Yara που παρέχονται από έναν πάροχο πληροφοριών απειλών, όπως η Securelist της Kaspersky, η οποία περιλαμβάνει δυνατότητα λήψης των κανόνων Yara.

Από εκεί, οι κανόνες Yara μπορούν στη συνέχεια να φορτωθούν στο Loki ή σε κάποια άλλη πλατφόρμα και να χρησιμοποιηθούν για την αξιολόγηση των ύποπτων συστημάτων.

Ο αριθμός των εργαλείων που μπορεί να χρησιμοποιήσει ένας αναλυτής incident response αυξάνεται καθημερινά. Περιλαμβάνουν εμπορικά εργαλεία και δωρεάν εργαλεία που ενσωματώνουν διάφορα feeds threat intelligence και λειτουργίες. Αυτά τα εργαλεία μπορούν να χρησιμοποιηθούν προληπτικά για ανίχνευση και ειδοποίηση, αλλά και για διερεύνηση ενός περιστατικού σε εξέλιξη. Οι ομάδες CSIRT θα πρέπει να εξετάζουν αυτά τα εργαλεία και να τα ενσωματώνουν στις διαδικασίες τους για πιο αποτελεσματική ανίχνευση και διερεύνηση περιστατικών.

13.10 Περίληψη

Η «Τέχνη του Πολέμου» του Sun Tzu περιλαμβάνει την στρατηγική έννοια της γνώσης του αντιπάλου και της αυτογνωσίας. Μέσω αυτής, μπορεί κανείς να έχει εμπιστοσύνη στην ικανότητά του να επικρατήσει στον αγώνα. Οι πληροφορίες απειλών (threat intelligence) έχουν γρήγορα καταστεί κρίσιμο στοιχείο των προληπτικών μέτρων ασφαλείας ενός οργανισμού, καθώς και σημαντικός παράγοντας στην ικανότητά του να ανταποκριθεί σε ένα περιστατικό. Αυτό το κεφάλαιο εξέτασε τις

αναδυόμενες τεχνικές και μεθοδολογίες της κυβερνο-πληροφορίας απειλών, καθώς και τις πηγές, την τεχνολογία και τις μεθόδους αξιοποίησης αυτών των δεδομένων.

Για να προχωρήσουν, οι οργανισμοί που θέλουν να αξιοποιήσουν τα πλεονεκτήματα που παρέχουν οι πληροφορίες απειλών πρέπει πρώτα να κατανοήσουν την απειλή. Από εκεί, μπορούν να ορίσουν τις απαιτήσεις τους και να ξεκινήσουν τη διαδικασία συλλογής πληροφοριών. Τέλος, ενσωματώνοντας τα εργαλεία τους για την αξιοποίηση των πληροφοριών απειλών, μπορούν να τοποθετηθούν έτσι ώστε να διαθέτουν πιο αποτελεσματικά προληπτικά μέτρα και ικανότητα να ανταποκριθούν αποτελεσματικά. Αν και οι πληροφορίες απειλών μπορεί να μην εξαλείψουν πλήρως τον φόβο απέναντι σε έναν αντίπαλο, παρέχουν στους οργανισμούς πολύ περισσότερα «όπλα» για την αντιμετώπιση των σημερινών απειλών. Επιπλέον, οι πληροφορίες απειλών εξυπηρετούν σημαντική λειτουργία κατά την προληπτική πρακτική εντοπισμού απειλών σε ένα περιβάλλον μέσω του threat hunting, που αποτελεί το αντικείμενο του επόμενου κεφαλαίου.

14

Ανίχνευση Απειλών (Threat Hunting)

Ο σκοπός του **threat hunting** (ανίχνευσης απειλών) είναι να μειωθεί ο χρόνος μεταξύ μιας παραβίασης και της ανακάλυψής της. Η συντόμευση αυτού του χρόνου μπορεί να κάνει τη διαφορά μεταξύ της δαπάνης μερικών χιλιάδων δολαρίων για αποκατάσταση και εκατομμυρίων για την αντιμετώπιση μιας πλήρους παραβίασης.

Η δημοσίευση της έκθεσης **APT1 της Mandiant** παρείχε στους επαγγελματίες της ασφάλειας πληροφοριών μια βαθιά εικόνα για μια από τις πιο έμπειρες και παραγωγικές ομάδες απειλών που δραστηριοποιούνται. Η γνώση για την **Μονάδα 61398 του PLA της Κίνας** παρείχε επίσης το πλαίσιο γύρω από αυτούς τους προηγμένους επιτιθέμενους. Ο όρος **Advanced Persistent Threat (APT)** έγινε πλέον μέρος του λεξιλογίου της ασφάλειας πληροφοριών. Οι επαγγελματίες ασφάλειας και οι υπεύθυνοι αντιμετώπισης περιστατικών είχαν πλέον εικόνα για απειλές που διεξήγαγαν τις δραστηριότητές τους χωρίς να εντοπίζονται και για σημαντικό χρονικό διάστημα.

Συνεχιζόμενη έρευνα έχει επίσης δείξει ότι οι οργανισμοί εξακολουθούν να υστερούν σημαντικά στην ικανότητά τους να ανιχνεύσουν μια παραβίαση που έχει ήδη συμβεί ή που βρίσκεται σε εξέλιξη. Η μελέτη **2018 Cost of a Data Breach Study: Global Overview**, που εκπονήθηκε από την IBM και το Ponemon Institute, κατέληξε στο συμπέρασμα ότι από τις 477 οργανώσεις που συμμετείχαν στην έρευνα, πέρασαν κατά μέσο όρο **197 ημέρες** πριν ανιχνευθεί η παραβίαση. Αυτός ο μέσος όρος δείχνει ότι οι επιτιθέμενοι είχαν πάνω από μισό χρόνο για να διεξάγουν τις δραστηριότητές τους χωρίς την παρέμβαση των αμυντικών.

Ωστόσο, πολλές οργανώσεις δεν έχουν ακόμη δημιουργήσει ομάδες ανίχνευσης. Αυτό γίνεται εμφανές αν σκεφτούμε ότι πάνω από το 20% των αναφερόμενων παραβιάσεων εντοπίζονται από τρίτους ή εξωτερικούς φορείς αντί από τον ίδιο τον οργανισμό-θύμα. Για να μειωθεί αυτός ο αριθμός και να μειωθεί το συνολικό κόστος της ασφάλειας, πρέπει να υποθέτουμε ότι έχουν συμβεί παραβιάσεις και να αναζητούμε τα στοιχεία τους **πριν προκληθεί ζημιά**.

Με την απειλή που παρουσιάζουν οι APT, σε συνδυασμό με τον χρόνο που μπορούν να παραμείνουν στο δίκτυο οι έστω και μετρίως προηγμένες ομάδες, οι οργανισμοί άρχισαν να μετακινούνται από την παθητική ανίχνευση και απόκριση σε μια πιο **ενεργητική προσέγγιση**, για να εντοπίζουν πιθανές απειλές στο δίκτυο. Αυτή η πρακτική, που ονομάζεται **threat hunting** (ανίχνευση απειλών), είναι μια **προληπτική διαδικασία**, κατά την οποία τεχνικές **ψηφιακής εγκληματολογίας (digital forensics)** χρησιμοποιούνται για την ανάλυση συστημάτων και δικτυακών στοιχείων, ώστε να εντοπιστούν και

να απομονωθούν απειλές που προηγουμένως δεν είχαν εντοπιστεί. Όπως και στην **αντιμετώπιση περιστατικών (incident response)**, η ανίχνευση απειλών είναι ένας συνδυασμός **διαδικασιών, τεχνολογίας και ανθρώπινου παράγοντα**, που δεν βασίζεται σε προρυθμισμένες ειδοποιήσεις ή αυτοματοποιημένα εργαλεία, αλλά ενσωματώνει διάφορα στοιχεία από την αντιμετώπιση περιστατικών, τις πληροφορίες απειλών και την ψηφιακή εγκληματολογία.

Η ανίχνευση απειλών περιλαμβάνει τη διατύπωση υποθέσεων σχετικά με τη συμπεριφορά των επιτιθέμενων και την επαλήθευση αυτών των υποθέσεων στο περιβάλλον σας. Για παράδειγμα, μπορεί να διατυπώσετε την υπόθεση ότι ένας επιτιθέμενος έχει εγκαταστήσει μηχανισμούς επιμονής (**persistence**) σε έναν ή περισσότερους τερματικούς σταθμούς στο περιβάλλον σας, ώστε να επιβιώσει από επανεκκινήσεις συστήματος. Η συλλογή και ανάλυση δεδομένων για πιθανούς χώρους επιμονής σε τερματικούς σταθμούς σε ολόκληρη την επιχείρηση και η διερεύνηση ανωμαλιών αποτελεί **threat hunting**. Η χρήση μόνο των IoCs για την αναζήτηση της επιμονής ενός επιτιθέμενου δεν αποτελεί ανίχνευση απειλών.

Πρώτον, είναι απαραίτητη η κατανόηση του **μοντέλου ωριμότητας της ανίχνευσης απειλών (threat hunting maturity model)**, το οποίο παρέχει ένα πλαίσιο για τις διάφορες πτυχές της ανίχνευσης απειλών. Δεύτερον, ο **κύκλος ανίχνευσης απειλών (threat hunt cycle)** εξετάζει τη διαδικασία που περιλαμβάνει την ανίχνευση απειλών, από την αρχή έως το τέλος. Τρίτον, καθώς η ανίχνευση απειλών είναι μια **προληπτική διαδικασία**, για να διασφαλιστεί ότι εκτελείται σωστά, είναι απαραίτητος ο **αποτελεσματικός σχεδιασμός**. Αυτό το κεφάλαιο θα παρέχει μια επισκόπηση του τρόπου σχεδιασμού μιας ανίχνευσης απειλών. Η κατανόηση αυτών των θεμάτων θα σας προσφέρει τα θεμέλια για να ενσωματώσετε την ανίχνευση απειλών στις δικές σας επιχειρησιακές διαδικασίες και θα σας επιτρέψει να είστε καλύτερα προετοιμασμένοι για τον εντοπισμό απειλών που προηγουμένως δεν είχαν αναγνωριστεί.

Σε αυτό το κεφάλαιο θα καλύψουμε τα ακόλουθα θέματα:

- Το μοντέλο ωριμότητας της ανίχνευσης απειλών (threat hunting maturity model)
- Ο κύκλος ανίχνευσης απειλών (threat hunt cycle)
- MITRE ATT&CK
- Σχεδιασμός ανίχνευσης απειλών (threat hunt planning)
- Αναφορά ανίχνευσης απειλών (threat hunt reporting)

14.1. Τι είναι το Threat Hunting

Η **Παρακολούθηση Ασφαλείας (Security Monitoring)** αφορά τη συνεχή παρακολούθηση συστημάτων, εφαρμογών και δικτύων με στόχο την ανίχνευση ύποπτων ή κακόβουλων δραστηριοτήτων. Μέσα όπως τα SIEM, IDS/IPS και EDR συλλέγουν και αναλύουν δεδομένα σε πραγματικό χρόνο και δημιουργούν ειδοποιήσεις (alerts) όταν εντοπιστεί κάτι ανωμαλικό. Ο ρόλος της παρακολούθησης

είναι κυρίως αντιδραστικός, καθώς βασίζεται στην αυτόματη ανίχνευση γεγονότων που ταιριάζουν με γνωστά μοτίβα κακόβουλης συμπεριφοράς.

Το **Κυνήγι Απειλών (Threat Hunting)**, σε αντίθεση με την παρακολούθηση, είναι μια ενεργητική και προληπτική διαδικασία. Οι αναλυτές δεν περιμένουν τα συστήματα να τους δώσουν ειδοποιήσεις· αντίθετα, ερευνούν μεθοδικά τα δεδομένα για να ανακαλύψουν ενδείξεις κρυφών ή εξελιγμένων επιθέσεων που μπορεί να ξεφύγουν από τα αυτοματοποιημένα εργαλεία. Χρησιμοποιούνται συχνά custom queries, συσχετίσεις και υποθέσεις βασισμένες σε intelligence. Ο σκοπός είναι να αποκαλυφθούν "σιωπηλές" επιθέσεις, όπως Advanced Persistent Threats (APTs), πριν αυτές εξελιχθούν σε μεγάλης κλίμακας περιστατικά.



Η Ψηφιακή Εγκληματολογία και Απόκριση σε Περιστατικά (Digital Forensics & Incident Response – DFIR) έρχεται συνήθως μετά την ανίχνευση ή αποκάλυψη ενός περιστατικού. Στο σκέλος της εγκληματολογίας (forensics), οι ειδικοί αναλύουν δεδομένα συστημάτων, δίσκους και μνήμες για να κατανοήσουν πώς έγινε η επίθεση, ποια ήταν τα ίχνη του επιτιθέμενου και ποια δεδομένα επηρεάστηκαν. Στο σκέλος της απόκρισης (incident response), η ομάδα επικεντρώνεται στον περιορισμό της απειλής, στην αποκατάσταση της λειτουργίας και στην πρόληψη επανάληψης. Ο στόχος είναι τόσο η τεχνική όσο και η στρατηγική αντιμετώπιση των επιθέσεων. Συνοπτικά, οι διαφορές είναι ξεκάθαρες:

- Η Παρακολούθηση Ασφαλείας μοιάζει με έναν συναγερμό που χτυπά όταν συμβεί κάτι γνωστό.
- Το Κυνήγι Απειλών είναι σαν ένας ερευνητής που ψάχνει ενεργητικά για ύποπτα ίχνη πριν υπάρξει συναγερμός.
- Η DFIR είναι η ομάδα διάσωσης και ερευνητών που επεμβαίνει αφού έχει εκδηλωθεί η επίθεση, με στόχο την ανάλυση, την αποκατάσταση και την αποτροπή επανάληψης.

Σενάριο: Στοχοποίηση οργανισμού με Ransomware μέσω Phishing Email

Ένας υπάλληλος δέχεται ένα φαινομενικά νόμιμο email με συνημμένο αρχείο Word που περιέχει κακόβουλο macro. Με το άνοιγμα του αρχείου, εγκαθίσταται ένα **remote access trojan (RAT)** που επιτρέπει στον επιτιθέμενο να κινείται πλευρικά στο δίκτυο.

1. Security Monitoring (Παρακολούθηση Ασφαλείας). Το SIEM ανιχνεύει:

- Επαναλαμβανόμενες αποτυχημένες προσπάθειες login σε έναν server.
- Μια ασυνήθιστη outbound σύνδεση προς IP σε χώρα υψηλού ρίσκου.
- Αύξηση στον όγκο δεδομένων που μεταφέρονται εκτός δικτύου.

Το Security Monitoring παράγει alerts, τα οποία ειδοποιούν την ομάδα SOC. Σε αυτό το στάδιο, τα συστήματα “σήμαναν συναγερμό” αλλά δεν έχουν ακόμη πλήρη εικόνα.

2. Threat Hunting (Κυνήγι Απειλών): Ένας αναλυτής αναλαμβάνει να διερευνήσει πέρα από τα alerts. Εξετάζει τα logs και εντοπίζει ότι το κακόβουλο PowerShell script εκτελείται σε διάφορους σταθμούς εργασίας τις βραδινές ώρες. Ανακαλύπτει επίσης ότι το RAT χρησιμοποιεί “living off the land” τεχνικές, δηλαδή νόμιμα εργαλεία των Windows (π.χ. wmic, rundll32) για να αποφύγει την ανίχνευση.

Το Threat Hunting καταφέρνει να εντοπίσει το **μοτίβο πλευρικής κίνησης** και αναδεικνύει ότι πρόκειται για προετοιμασία ransomware. Αυτή η φάση είναι κρίσιμη, διότι η επίθεση βρίσκεται ακόμη σε **πρώιμο στάδιο**.

3. DFIR (Digital Forensics & Incident Response): Η επίθεση τελικά εκδηλώνεται: το ransomware ενεργοποιείται και αρχίζει να κρυπτογραφεί αρχεία σε αρκετούς servers. Η DFIR ομάδα επεμβαίνει άμεσα:

- **Incident Response:** Απομονώνει τους μολυσμένους servers από το δίκτυο, κλείνει τις ύποπτες συνδέσεις και ενεργοποιεί διαδικασίες αποκατάστασης μέσω ασφαλών backups.
- **Digital Forensics:** Συλλέγει memory dumps, αναλύει τα logs και τα artifacts από τους δίσκους για να χαρτογραφήσει την πλήρη αλυσίδα επίθεσης: από το phishing email, στο RAT, στις κινήσεις πλευρικής διείσδυσης και τελικά στο ransomware. Αυτή η ανάλυση οδηγεί στην εφαρμογή security patches και στην αναβάθμιση πολιτικών ασφαλείας ώστε να αποτραπεί παρόμοια επίθεση στο μέλλον.

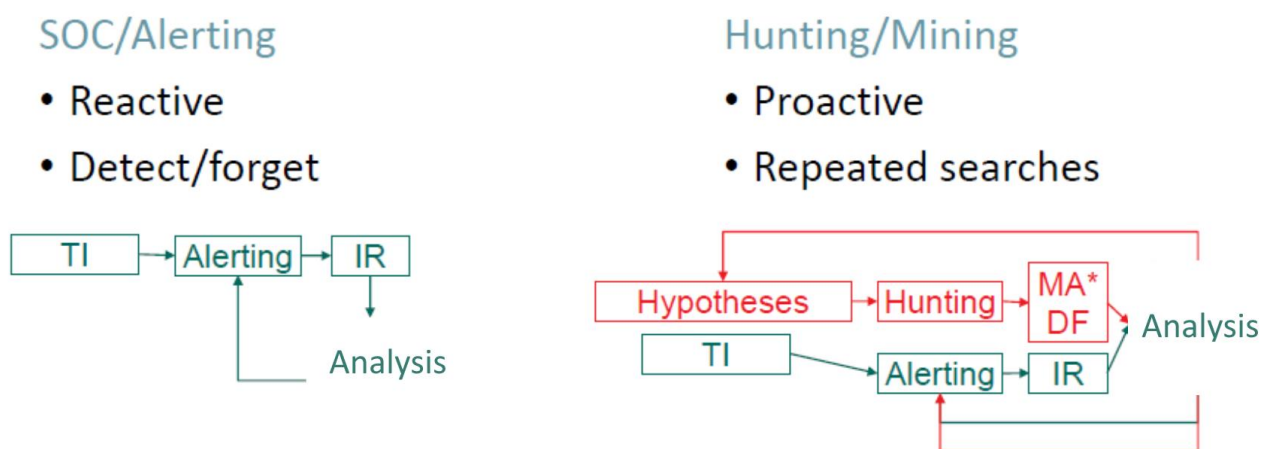
Σε αυτό το σενάριο βλέπουμε ότι:

- Το **Security Monitoring** σήμανε πρώτο τον συναγερμό με τα αρχικά alerts.
- Το **Threat Hunting** ερευνήσε πιο βαθιά και αποκάλυψε τη μεθοδολογία του επιτιθέμενου πριν εκδηλωθεί η επίθεση.
- Το **DFIR** επενέβη μετά την ενεργοποίηση του ransomware για να περιορίσει τις ζημιές, να αποκαταστήσει τα συστήματα και να εξάγει πολύτιμα συμπεράσματα για μελλοντική άμυνα.

Έτσι, τα τρία αυτά πεδία δεν είναι ανταγωνιστικά αλλά **συμπληρωματικά**, σχηματίζοντας μια συνεκτική αλυσίδα άμυνας: ανίχνευση → διερεύνηση → αντιμετώπιση και μάθηση.

14.2. Το μοντέλο ωριμότητας της ανίχνευσης απειλών

Ο ειδικός στην κυβερνοασφάλεια David Bianco, ο δημιουργός της «Πυραμίδας του Πόνου» που καλύφθηκε στο προηγούμενο κεφάλαιο, ανέπτυξε το **μοντέλο ωριμότητας της ανίχνευσης απειλών (threat hunting maturity model)** ενώ εργαζόταν στην εταιρεία κυβερνοασφάλειας Sqrrl. Είναι σημαντικό να κατανοηθεί αυτό το μοντέλο ωριμότητας σε σχέση με την ανίχνευση απειλών, καθώς παρέχει στους κυνηγούς απειλών και στον οργανισμό τους ένα πλαίσιο για τον καθορισμό του χάρτη πορείας (roadmap) για την ωρίμανση της διαδικασίας ανίχνευσης απειλών στον οργανισμό τους.



* MA – malware analysis, DF – digital forensics, IR – incident response

Το μοντέλο ωριμότητας αποτελείται από **πέντε επίπεδα**, ξεκινώντας από το **Hunt Maturity 0 (HM0)** έως το **HM4**. Ακολουθεί μια επισκόπηση των πέντε επιπέδων του μοντέλου:

HM0—Αρχικό (Initial): Κατά το αρχικό στάδιο, οι οργανισμοί βασίζονται αποκλειστικά σε αυτοματοποιημένα εργαλεία, όπως συστήματα πρόληψης/ανίχνευσης εισβολών (network- ή host-based), antivirus ή συστήματα διαχείρισης ασφάλειας και συμβάντων (SIEM), για να παρέχουν ειδοποιήσεις στην ομάδα ανίχνευσης απειλών. Αυτές οι ειδοποιήσεις στη συνέχεια διερευνώνται και αντιμετωπίζονται χειροκίνητα. Μαζί με την έντονη εξάρτηση από τις ειδοποιήσεις, δεν χρησιμοποιούνται δείκτες απειλών (threat intelligence indicators) σε αυτό το στάδιο ωριμότητας. Τέλος, αυτό το επίπεδο χαρακτηρίζεται από περιορισμένη ικανότητα συλλογής τηλεμετρικών δεδομένων από τα συστήματα. Οι οργανισμοί σε αυτό το στάδιο **δεν είναι ικανοί να εκτελέσουν ανίχνευση απειλών**.

HM1—Ελάχιστο (Minimal): Στο ελάχιστο στάδιο, οι οργανισμοί συλλέγουν περισσότερα δεδομένα και, στην πραγματικότητα, μπορεί να έχουν πρόσβαση σε μεγάλο όγκο τηλεμετρικών δεδομένων

συστημάτων. Επιπλέον, αυτοί οι οργανισμοί δείχνουν πρόθεση να ενσωματώσουν την πληροφορία απειλών στις διαδικασίες τους, αλλά βρίσκονται πίσω όσον αφορά τα τελευταία δεδομένα και πληροφορίες για τους δράστες απειλών. Αν και αυτή η ομάδα εξακολουθεί συχνά να βασίζεται σε αυτοματοποιημένες ειδοποιήσεις, η αυξημένη διαθεσιμότητα τηλεμετρικών δεδομένων της δίνει τη δυνατότητα να εξάγει δείκτες απειλών από αναφορές και να αναζητά αντίστοιχους δείκτες στα διαθέσιμα δεδομένα. **Αυτό είναι το πρώτο επίπεδο στο οποίο μπορεί να ξεκινήσει η ανίχνευση απειλών.**

HM2—Διαδικαστικό (Procedural): Σε αυτό το στάδιο, ο οργανισμός χρησιμοποιεί διαδικασίες ανίχνευσης απειλών που έχουν αναπτυχθεί από άλλους οργανισμούς, τις οποίες εφαρμόζει σε συγκεκριμένες περιπτώσεις χρήσης. Για παράδειγμα, ένας οργανισμός μπορεί να βρει μια παρουσίαση ή μια περιγραφή περίπτωσης χρήσης που αφορά **πλευρική κίνηση (lateral movement)** μέσω εργαλείων ενός συστήματος Windows. Από εκεί, θα εξάγει τα σχετικά χαρακτηριστικά της διαδικασίας και θα τα εφαρμόσει στα δικά του δεδομένα. Σε αυτό το στάδιο, ο οργανισμός **δεν είναι σε θέση να δημιουργήσει δική του διαδικασία ανίχνευσης απειλών**. Το στάδιο HM2 αντιπροσωπεύει επίσης το πιο κοινό επίπεδο ωριμότητας για οργανισμούς που διαθέτουν προγράμματα ανίχνευσης απειλών.

HM3—Καινοτόμο (Innovative): Σε αυτό το επίπεδο ωριμότητας, οι κυνηγοί απειλών αναπτύσσουν τις δικές τους διαδικασίες. Υπάρχει επίσης αυξημένη χρήση διαφόρων μεθόδων πέρα από τις χειροκίνητες διαδικασίες, όπως **μηχανική μάθηση, στατιστική ανάλυση και ανάλυση συνδέσεων (link analysis)**. Επίσης, υπάρχει διαθέσιμος μεγάλος όγκος δεδομένων σε αυτό το επίπεδο.

HM4—Προηγμένο (Leading): Αντιπροσωπεύοντας το **κορυφαίο επίπεδο της ανίχνευσης απειλών**, το Leading επίπεδο ενσωματώνει πολλά χαρακτηριστικά του HM3 με μία σημαντική διαφορά: τη **χρήση αυτοματοποίησης**. Διαδικασίες που έχουν αποδώσει αποτελέσματα στο παρελθόν αυτοματοποιούνται, παρέχοντας στους κυνηγούς απειλών την ευκαιρία να δημιουργήσουν νέες διαδικασίες ανίχνευσης απειλών, πιο ικανές να συμβαδίζουν με τις αναδυόμενες απειλές.

Το **μοντέλο ωριμότητας της ανίχνευσης απειλών** αποτελεί ένα χρήσιμο εργαλείο για τους οργανισμούς, ώστε να **εντοπίζουν το τρέχον επίπεδο ωριμότητάς τους** και να **σχεδιάζουν την ενσωμάτωση μελλοντικών τεχνολογιών και διαδικασιών**, για να παραμένουν σε ρυθμό με το συνεχώς εξελισσόμενο τοπίο απειλών.

14.3. Σχεδιασμός Ανίχνευσης Απειλών

Ο **Threat Hunter** χρειάζεται πάνω απ' όλα **αναλυτική σκέψη**. Αυτό σημαίνει περιέργεια, ικανότητα δημιουργίας και διερεύνησης υποθέσεων, καθώς και την ικανότητα να θέτει συγκεκριμένα ερωτήματα προς απάντηση. Για παράδειγμα, ένας αναλυτής μπορεί να αναρωτηθεί εάν εκτελούνται ασυνήθιστες PowerShell εντολές εκτός ωραρίου και να εξετάσει τα σχετικά logs.

Δεξιότητα	Περιγραφή	Παράδειγμα
Αναλυτική Σκέψη (Analytical Mindset)	Περιέργεια, δημιουργία και διερεύνηση υποθέσεων, στοχευμένες ερωτήσεις.	Έλεγχος αν υπάρχουν PowerShell εντολές εκτός ωραρίου.
Γνώση Λειτουργικών Συστημάτων (OS Knowledge)	Κατανόηση εσωτερικών μηχανισμών, μηχανισμών ασφαλείας και τυπικών ευπαθειών.	Registry στα Windows, SELinux σε Linux.
Δικτυακή Αρχιτεκτονική (Network Architecture)	Γνώση OSI, TCP/IP, βασικών πρωτοκόλλων (DNS, DHCP, HTTP, SMTP, FTP, SMB).	Εντοπισμός κακόβουλης DNS επικοινωνίας.
Μέθοδοι Επίθεσης (Attack Methods / TTPs / Lifecycle)	Κατανόηση σταδίων επίθεσης, εργαλείων και τεχνικών που χρησιμοποιούν οι εισβολείς.	Χρήση phishing για αρχική πρόσβαση.
Ανάλυση Καταγραφών (Log Analysis)	Γνώση πηγών logs, ανίχνευση ανωμαλιών, pivot μεταξύ δεδομένων.	Συσχέτιση firewall logs με Windows event logs.
Ανάλυση Δικτύου (Network Analysis)	Ανάγνωση και κατανόηση packet captures (PCAP), αναγνώριση κακόβουλης κίνησης.	Εντοπισμός C2 επικοινωνίας σε PCAP.
Πληροφορία Απειλών (Threat Intelligence)	Αξιοποίηση αναφορών CTI για εμπλουτισμό έρευνας και αναζήτηση νέων δεικτών.	Ενσωμάτωση IoCs από αναφορά APT.
Ανάλυση Κακόβουλου Λογισμικού (Malware Analysis)	Προσδιορισμός προέλευσης, λειτουργίας και σκοπού malware.	Ανάλυση ransomware δείγματος σε sandbox.
Εργαλεία Threat Hunting	Χρήση SIEM, ELK, packet sniffers, PCAP viewers, συλλογή & εξαγωγή logs.	Ανάλυση logs στο ELK stack, χρήση Wireshark.

Η βαθιά γνώση λειτουργικών συστημάτων είναι απαραίτητη. Ο hunter πρέπει να κατανοεί τους εσωτερικούς μηχανισμούς (internals), τα χαρακτηριστικά ασφαλείας τους και τα συνηθισμένα κενά που παρουσιάζουν διαφορετικές πλατφόρμες (Windows, Linux, macOS). Επιπλέον, χρειάζεται κατανόηση της δικτυακής αρχιτεκτονικής. Αυτό περιλαμβάνει την καλή γνώση του OSI μοντέλου, του TCP/IP, αλλά και βασικών πρωτοκόλλων, όπως DNS, DHCP, HTTP, SMTP, FTP και SMB.

Η γνώση των μεθόδων επίθεσης και του κύκλου ζωής μιας επίθεσης (TTPs/Attack Life Cycle) είναι κρίσιμη. Ο Threat Hunter πρέπει να κατανοεί πώς ένας εισβολέας επιχειρεί να διεισδύσει στο δίκτυο, ποια εργαλεία και τεχνικές μπορεί να χρησιμοποιήσει σε κάθε στάδιο, και ποια σημάδια αφήνει πίσω του. Για να εκτελέσει αποτελεσματικά την έρευνά του, ο Threat Hunter χρειάζεται δεξιότητες στην **ανάλυση καταγραφών (log analysis)**. Αυτό σημαίνει ικανότητα αναγνώρισης ανωμαλιών μέσα σε logs, αλλά και ικανότητα να “στρέφεται” (pivot) από μια πηγή δεδομένων σε άλλη για να σχηματίσει συνολική εικόνα. Η **ανάλυση δικτύου (network analysis)** είναι επίσης απαραίτητη, καθώς ο hunter πρέπει να μπορεί να διαβάζει και να ερμηνεύει δεδομένα από packet captures (π.χ. PCAPs) και να αναγνωρίζει κακόβουλη δραστηριότητα μέσα στην κυκλοφορία του δικτύου.

Η αξιοποίηση της **πληροφορίας απειλών (cyber threat intelligence)** ενισχύει σημαντικά τη διαδικασία. Ο Threat Hunter πρέπει να ενημερώνεται συνεχώς από αναφορές και πηγές threat intelligence, ώστε να εμπλουτίζει την έρευνά του με νέες τεχνικές και δείκτες κακόβουλης δραστηριότητας.

Μια ακόμα εξειδικευμένη δεξιότητα είναι η **ανάλυση κακόβουλου λογισμικού (malware analysis)**, η οποία στοχεύει στον εντοπισμό της προέλευσης και του σκοπού ενός δείγματος malware. Αν και είναι απαιτητικό πεδίο, προσφέρει κρίσιμη πληροφόρηση σε περιβάλλον threat hunting.

Τέλος, σημαντική είναι η γνώση και χρήση των **εργαλείων threat hunting**. Αυτό περιλαμβάνει:

- Πλατφόρμες ανάλυσης ασφαλείας, όπως ELK και SIEM.
- Χρήση packet sniffers και ανάλυσης PCAP.
- Διαχείριση και εξαγωγή logs από λειτουργικά συστήματα.
- Συλλογή logs από πολλαπλές πηγές για κεντρική ανάλυση.

Η έναρξη μιας ανίχνευσης απειλών δεν απαιτεί εκτενή σχεδιασμό, αλλά πρέπει να υπάρχει κάποια δομή σχετικά με τον τρόπο που θα διεξαχθεί η ανίχνευση, τις πηγές δεδομένων και την χρονική περίοδο στην οποία θα επικεντρωθεί η ανίχνευση. Ένα σύντομο γραπτό σχέδιο θα καλύψει όλα τα βασικά σημεία που είναι απαραίτητα και θα θέσει όλη την ομάδα ανίχνευσης σε κοινό πλαίσιο, ώστε να μειωθούν τα περιττά δεδομένα που δεν σχετίζονται με την ανίχνευση. Τα ακόλουθα είναι επτά βασικά στοιχεία που πρέπει να καλύπτονται σε κάθε σχέδιο:

Υπόθεση (Hypothesis): Μία ή δύο προτάσεις υπόθεσης όπως συζητήθηκε νωρίτερα. Η υπόθεση αυτή πρέπει να είναι σαφώς κατανοητή από όλα τα μέλη της ομάδας ανίχνευσης.

Τακτική(ές) MITRE ATT&CK: Στο προηγούμενο κεφάλαιο συζητήθηκε το πλαίσιο MITRE ATT&CK και η εφαρμογή του στην πληροφορία απειλών και την αντιμετώπιση περιστατικών. Στην περίπτωση της ανίχνευσης απειλών, θα πρέπει να συμπεριληφθούν συγκεκριμένες τακτικές που χρησιμοποιούνται από κακόβουλους παράγοντες. Επιλέξτε τις τακτικές που είναι πιο σχετικές με την υπόθεση.

Πληροφορίες Απειλών (Threat Intelligence): Η ομάδα ανίχνευσης θα πρέπει να αξιοποιήσει όσο το δυνατόν περισσότερες εσωτερικά αναπτυγμένες και εξωτερικά προερχόμενες πληροφορίες απειλών. Οι εξωτερικές πηγές μπορούν να είναι είτε εμπορικοί πάροχοι είτε OSINT. Οι πληροφορίες απειλών πρέπει να περιλαμβάνουν **IoCs** (Δείκτες Συμβάντων), **IoAs** (Δείκτες Επίθεσης) και **TTPs** που σχετίζονται άμεσα με την υπόθεση και τις τακτικές MITRE ATT&CK που είχαν προηγουμένως εντοπιστεί. Αυτά είναι τα δεδομένα που η ομάδα θα χρησιμοποιήσει κατά την ανίχνευση.

Πηγές αποδεικτικών στοιχείων (Evidence Sources): Αυτή θα πρέπει να είναι μια λίστα με τις διάφορες πηγές αποδεικτικών στοιχείων που θα χρησιμοποιηθούν κατά την ανίχνευση απειλών. Για παράδειγμα, αν η ομάδα αναζητά δείκτες πλευρικής κίνησης μέσω SMB, μπορεί να αξιοποιήσει **NetFlow** ή επιλεγμένες καταγραφές πακέτων. Άλλοι δείκτες πλευρικής κίνησης μέσω **Remote Desktop** μπορούν να βρεθούν στα **Windows event logs**.

Εργαλεία (Tools): Αυτή η ενότητα του σχεδίου περιγράφει τα συγκεκριμένα εργαλεία που απαιτούνται για την ανασκόπηση των αποδεικτικών στοιχείων. Για παράδειγμα, στο Κεφάλαιο 10, **Analyzing Log Files**, εξετάστηκε η ανάλυση αρχείων καταγραφής με το εργαλείο ανοικτού κώδικα **Skadi**. Αν η ανίχνευση θα χρησιμοποιήσει αυτό το εργαλείο, πρέπει να συμπεριληφθεί στο σχέδιο.

Μία ομάδα εργαλείων που βοηθά σημαντικά στην ανίχνευση απειλών είναι τα **Endpoint Detection and Response (EDR)**. Αυτά τα εργαλεία βασίζονται στη μεθοδολογία των πλατφορμών antivirus και πολλές από αυτές τις πλατφόρμες έχουν τη δυνατότητα να αναζητούν σε ολόκληρη την επιχείρηση συγκεκριμένα IoCs και άλλα δεδομένα, επιτρέποντας στις ομάδες ανίχνευσης να εξετάσουν έναν μεγάλο αριθμό συστημάτων για τυχόν αντιστοιχίες με IoCs. Αυτά τα εργαλεία πρέπει να αξιοποιούνται εκτενώς κατά την ανίχνευση.

Πεδίο εφαρμογής (Scope): Αναφέρεται στα συστήματα που θα περιλαμβάνονται στην ανίχνευση απειλών. Το σχέδιο πρέπει να υποδεικνύει είτε ένα μεμονωμένο σύστημα ή συστήματα, υποδίκτυο ή τμήμα δικτύου στο οποίο θα επικεντρωθεί η ανίχνευση. Στην αρχή, οι κυνηγοί απειλών πρέπει να επικεντρώνονται σε περιορισμένο αριθμό συστημάτων και να προσθέτουν περισσότερα καθώς εξοικειώνονται με τα εργαλεία και με το πόσα αποδεικτικά στοιχεία μπορούν να εξετάσουν στο δεδομένο χρονικό διάστημα.

Χρονικό πλαίσιο (Timeframe): Καθώς η ανίχνευση απειλών συχνά περιλαμβάνει αναδρομική εξέταση στοιχείων, είναι απαραίτητο να οριστεί ένα χρονικό διάστημα στο οποίο θα επικεντρωθεί η ομάδα. Για παράδειγμα, αν ένα αρχικό συμβάν είναι σχετικά πρόσφατο (π.χ., 48 ώρες), το χρονικό πλαίσιο που θα υποδεικνύεται στο σχέδιο μπορεί να περιορίζεται στις τελευταίες 72 ώρες, ώστε να αντιμετωπιστούν τυχόν προηγούμενες ανιχνευμένες ενέργειες του αντιπάλου. Άλλα χρονικά πλαίσια μπορούν να διευρύνουν την ανίχνευση σε 14 ή ακόμη και 30 ημέρες, ανάλογα με την υπόθεση και τις διαθέσιμες πληροφορίες απειλών.

Ακολουθεί ένα παράδειγμα σχεδίου ανίχνευσης απειλών που ενσωματώνει αυτά τα στοιχεία σε ένα εύκολο στην προβολή πλαίσιο.

Hypothesis	An adversary has compromised a webserver in the DMZ and has gained access to the system and configured a remote access tool.
MITRE ATT&CK Tactics	- T1190 Exploit Public-Facing Application - T1219 Remote Access Tools - T1071 Standard Application Layer Protocol
Threat Intelligence	- VirusTotal - Alien Vault OTX - US-CERT
Sources	- Windows Event Logs, Packet Capture - IIS Logs, Web logs - Web application firewall logs
Tools	- Event log review tool - Wireshark or Moloch - File Search tools
Scope	All Webservers in the DMZ
Timeframe	Last 90 Days for Log Reviews

Στο παράδειγμα αυτού του σχεδίου, η υπόθεση είναι ότι ένας αντίπαλος έχει αποκτήσει έλεγχο σε έναν ή περισσότερους web servers της DMZ. Οι σχετικοί τακτικοί στόχοι του MITRE ATT&CK περιλαμβάνουν είτε την εκμετάλλευση της web εφαρμογής είτε την εγκαθίδρυση καναλιού Command and Control. Σε αυτό το σχέδιο, η ομάδα αναζήτησης απειλών θα αξιοποιήσει πληροφορίες από OSINT. Οι πηγές δεδομένων και τα εργαλεία περιλαμβάνουν αρχεία καταγραφής και πακέτα δεδομένων (packet captures), τα οποία θα εξεταστούν για τις τελευταίες 90 ημέρες. Πρόκειται για ένα απλό σχέδιο, αλλά παρέχει σε κάθε μέλος της ομάδας αναζήτησης απειλών όλες τις οδηγίες που είναι απαραίτητες για τη διεξαγωγή της αναζήτησης.

14.4. Αναφορά Ανίχνευσης Απειλών (Threat Hunt Reporting)

Το Κεφάλαιο 11, «Σύνταξη Αναφοράς Περιστατικού», περιέχει τις λεπτομέρειες που χρειάζονται οι υπεύθυνοι αντιμετώπισης περιστατικών για να αναφέρουν σωστά τις ενέργειες και τα ευρήματά τους. Η αναφορά μιας αναζήτησης απειλών είναι εξίσου κρίσιμη, καθώς παρέχει στους διευθυντές και στους υπεύθυνους χάραξης πολιτικής γνώση σχετικά με τα εργαλεία, τις τεχνικές και τις διαδικασίες που χρησιμοποίησε η ομάδα αναζήτησης, καθώς και πιθανή δικαιολόγηση για πρόσθετα εργαλεία ή τροποποίηση των υπαρχουσών διαδικασιών. Τα βασικά στοιχεία μιας αναφοράς αναζήτησης απειλών περιλαμβάνουν:

Εκτελεστική περίληψη: Αυτή η συνοπτική επισκόπηση των ενεργειών που πραγματοποιήθηκαν, των δεικτών που εντοπίστηκαν και αν η αναζήτηση απέδειξε ή αναιρεί την υπόθεση, παρέχει στους λήπτες αποφάσεων μια σύντομη αφήγηση που μπορεί να χρησιμοποιηθεί για άμεση δράση.

Σχέδιο αναζήτησης απειλών: Το σχέδιο, συμπεριλαμβανομένης της υπόθεσης της αναζήτησης, θα πρέπει να περιλαμβάνεται στην αναφορά. Αυτό παρέχει στον αναγνώστη όλες τις λεπτομέρειες που χρησιμοποίησε η ομάδα κατά την εκτέλεση της αναζήτησης.

Διεξοδική αναφορά ανάλυσης (Forensic report): Όπως εξετάστηκε στο Κεφάλαιο 11, τα εργαλεία ανάλυσης παρέχουν μεγάλο όγκο δεδομένων, όπως και οι ίδιοι οι υπεύθυνοι αντιμετώπισης περιστατικών. Το τμήμα αυτό της αναφοράς είναι το πιο εκτενές, καθώς θα πρέπει να τεκμηριώνεται η λεπτομερής εξέταση κάθε συστήματος ή πηγής στοιχείων. Επιπλέον, πρέπει να υπάρχει μια πλήρης λίστα όλων των στοιχείων που εξετάστηκαν κατά τη διάρκεια της αναζήτησης.

Ευρήματα (Findings): Αυτό το τμήμα θα αναφέρει αν η ομάδα αναζήτησης μπόρεσε να αποδείξει ή να αναιρέσει την υπόθεση που είχε τεθεί στην αρχή της αναζήτησης. Σε περίπτωση που η υπόθεση αποδειχθεί, θα πρέπει να τεκμηριώνονται οι επόμενες ενέργειες, όπως τροποποίηση της υπόθεσης, διατύπωση νέας υπόθεσης ή ενεργοποίηση της ικανότητας αντιμετώπισης περιστατικών. Τέλος, οποιοδήποτε δείκτης IoC, IoA ή TTP που βρέθηκε κατά τη διάρκεια της αναζήτησης πρέπει επίσης να τεκμηριώνεται.

Ένα ακόμη σημαντικό στοιχείο της ενότητας των Ευρημάτων είναι η αξιολόγηση του κατά πόσο οι υπάρχουσες διαδικασίες και τεχνολογίες διευκόλυναν μια λεπτομερή αναζήτηση. Για παράδειγμα, αν

η αναζήτηση έδειξε ότι τα Windows event logs δεν ήταν επαρκή σε χρόνο ή ποσότητα, αυτό πρέπει να αναφέρεται στην αναφορά. Τέτοιου είδους πληροφορίες επιτρέπουν τη δικαιολόγηση πρόσθετου χρόνου και πόρων για τη δημιουργία ενός περιβάλλοντος όπου η ορατότητα στο δίκτυο και τα συστήματα είναι επαρκής για μια λεπτομερή αναζήτηση.

Μη σχετιζόμενα ευρήματα (Non-security/incident-related findings): Μερικές φορές οι αναζητήσεις απειλών εντοπίζουν ευάλωτα συστήματα, υπάρχοντα σφάλματα διαμόρφωσης ή άλλα δεδομένα μη σχετιζόμενα με περιστατικά. Αυτά πρέπει να αναφέρονται ώστε να μπορούν να διορθωθούν.

Συστάσεις (Recommendations): Ακόμα και σε αναζητήσεις που αναιρούν την υπόθεση ή δεν περιλαμβάνουν ευρήματα ασφαλείας, οι συστάσεις για τη βελτίωση μελλοντικών αναζητήσεων, της ασφάλειας του οργανισμού ή των ρυθμίσεων των συστημάτων πρέπει να περιλαμβάνονται. Οι συστάσεις μπορούν να ομαδοποιηθούν, π.χ.:

- **Στρατηγικές συστάσεις:** μακροπρόθεσμες βελτιώσεις διαμόρφωσης ή ασφάλειας που απαιτούν αυξημένους πόρους και χρόνο.
- **Τακτικές συστάσεις:** βραχυπρόθεσμες ή απλές βελτιώσεις στη διαδικασία αναζήτησης ή στις ρυθμίσεις συστημάτων, για μεγαλύτερη ακρίβεια ειδοποιήσεων. Μπορεί επίσης να καθοριστεί η **κριτική σημασία** των συστάσεων, δίνοντας προτεραιότητα σε αυτές που βελτιώνουν την ασφάλεια ή αποτρέπουν υψηλού κινδύνου επιθέσεις έναντι εκείνων που απλώς βελτιώνουν διαδικασίες ή ρυθμίσεις.

Η αναφορά αναζήτησης απειλών περιέχει σημαντικά δεδομένα που μπορούν να χρησιμοποιηθούν για συνεχή βελτίωση της διαδικασίας. Ένα άλλο στοιχείο είναι η αναφορά μετρικών στους ανώτερους διαχειριστές, όπως: ώρες που δαπανήθηκαν, εντοπισμένοι προηγούμενως άγνωστοι δείκτες, μολυσμένα συστήματα, εντοπισμένες απειλές και αριθμός περιορισμένων συστημάτων. Τέτοια δεδομένα αποδεικνύουν την ικανότητα της αναζήτησης να εντοπίζει νέες απειλές και ενισχύουν την ενσωμάτωσή της στις καθημερινές διαδικασίες ασφάλειας ενός οργανισμού.

Παρόλο που στις περισσότερες δραστηριότητες ανίχνευσης απειλών μπορείτε να ακολουθήσετε μια μη δομημένη προσέγγιση, εδώ **θα πρέπει να καθορίσετε κάποια δομή**. Ο ορισμός μιας διαδικασίας για κάθε κυνηγητό βοηθά στο να γίνουν τα βήματα επαναλαμβανόμενα. Αυτό καθιστά πιο εύκολη τη μέτρηση των αποτελεσμάτων και την αξιολόγηση της απόδοσης των εργαλείων σας και των μεθόδων της ομάδας σας. Επιπλέον, σας επιτρέπει να παρουσιάζετε τα ευρήματα στη διοίκηση με συνεπή τρόπο μεταξύ των διαφόρων κυνηγητών.

Αν μόλις ξεκινάτε αυτή τη διαδικασία, η **επιστημονική μέθοδος** παρέχει κάποιες χρήσιμες διαδικαστικές οδηγίες:

- Καθορίστε το πρόβλημα που πρέπει να λυθεί και μια υπόθεση για την επίλυσή του
- Προτείνετε μια διαδικασία για τη συλλογή και ανάλυση των στοιχείων
- Ορίστε μετρικές για την αξιολόγηση της επιτυχίας της προσπάθειας

- Εκτελέστε τη διαδικασία και μετρήστε το/τα αποτέλεσμα/τα

Μην πέφτετε στην παγίδα να ψάχνετε μόνο για απειλές που σχετίζονται με τον κλάδο σας. Δεν ξέρετε τι δεν ξέρετε, και οι ομάδες απειλών μπορούν να αλλάξουν δυναμικά τους στόχους τους για λόγους που οι αμυντικοί δεν μπορούν πάντα να προβλέψουν. Τεχνικές που αναπτύχθηκαν για ένα συγκεκριμένο είδος θύματος μπορούν να εμπνεύσουν απειλές που στοχεύουν ευρύ κοινό. Πλαίσια όπως το MITRE ATT&CK μπορούν να σας βοηθήσουν να εφαρμόσετε μια προσέγγιση ανεξάρτητη από την απειλή.

14.5. Δομή της Διαδικασίας Κυνηγιού (Hunt Process)

Κάθε «κυνήγι» είναι διαφορετικό, αλλά όπως αναφέραμε νωρίτερα, η δομή του βασισμένη στη **επιστημονική μέθοδο** βοηθά να γίνουν τα βήματα επαναλήψιμα και τα αποτελέσματα μετρήσιμα. Αυτή η ενότητα εστιάζει στην εφαρμογή της επιστημονικής μεθόδου στην ανάπτυξη μεθοδολογίας κυνηγιού.



Στο Διαδίκτυο: Ο Robert M. Lee και ο David Bianco έχουν γράψει μια εξαιρετική λευκή βίβλο για το «κυνηγητό απειλών» με βάση υποθέσεις: *Generating Hypotheses for Successful Threat Hunting* ([link](#)).

Βήμα 1: Διατύπωση υποθέσεων: Διατυπώστε μια λογική υπόθεση σχετικά με έναν ή περισσότερους αντιπάλους και τις τεχνικές που μπορεί να χρησιμοποιήσουν για να εισέλθουν ή να παραμείνουν στο περιβάλλον σας.

Παράδειγμα: «Κακόβουλοι χρήστες χρησιμοποιούν το εγγενές εργαλείο `msfcompr.exe` για να τροποποιήσουν κακόβουλα τη βάση δεδομένων WMI CIMv2.»

Για να αποφύγετε την εκτροπή του εύρους (*scope creep*), περιορίστε τον αριθμό των ωρών που θα αφιερώσετε στο κυνήγι για να αποδείξετε ή να απορρίψετε την υπόθεση και προσδιορίστε τα

συστήματα που βρίσκονται εκτός του εύρους. Αυτές οι αποφάσεις θα βοηθήσουν να περιοριστεί η εστίαση του κυνηγιού.

Βήμα 2: Προσδιορισμός στοιχείων για την απόδειξη της υπόθεσης: Προσδιορίστε τα είδη στοιχείων που μπορούν να αποδείξουν ή να απορρίψουν την υπόθεση και καθορίστε πώς μπορούν να συλλεχθούν.

Στο παράδειγμα παραπάνω, μπορείτε να ενεργοποιήσετε **audit εκτέλεσης διαδικασιών** (Windows EID 4688 ή Sysmon EID 1) και να ξεκινήσετε τη συλλογή:

- Ονόματα διαδικασιών, διαδρομές και hashes
- Παραμέτρους γραμμής εντολών
- Αρχεία και άλλα τεκμήρια
- Οποιοδήποτε προορισμοί δικτύου ή ονόματα domain που έχουν καταγραφεί

Το Sysmon παρέχει τις ίδιες πληροφορίες όπως η λεπτομερής παρακολούθηση διαδικασιών των Windows και περισσότερες. Προσφέρει πληροφορίες για τις γονικές διαδικασίες, πολλούς τύπους hash αρχείων και περιγραφές των συνδέσεων δικτύου.

Συμβουλή: Συνήθως χρειάζονται δύο ή περισσότερα είδη στοιχείων για να αποδειχθεί μια υπόθεση με υψηλό βαθμό εμπιστοσύνης. Μια μόνο πηγή μπορεί να αποδειχθεί παραπλανητική ή ανεπαρκής, συνήθως την πιο ακατάλληλη στιγμή.

Μην ξεχνάτε: Είναι σημαντικό να καταγράφετε τις πηγές στοιχείων που έχετε επιλέξει και να διασφαλίζετε ότι τα δεδομένα που συλλέγονται από κάθε πηγή είναι συνεπή. Διαφορετικά, μπορεί να έχετε κομμάτια δεδομένων που δεν μπορούν να συγκριθούν ή να συνδυαστούν. Για παράδειγμα, αν σκοπεύετε να ταιριάξετε κωδικοποιημένα δεδομένα με λέξεις-κλειδιά, βεβαιωθείτε ότι πραγματοποιείται πρώτα η αποκωδικοποίηση.

Βήμα 3: Ανάπτυξη αναλύσεων: Περιγράψτε πώς τα στοιχεία μπορούν να μειωθούν, να ομαδοποιηθούν και να αναλυθούν για να εξαχθεί ένα συμπέρασμα. Συνήθως, αυτό περιλαμβάνει τον εντοπισμό ανωμαλιών ή ακολουθιών γεγονότων που σχετίζονται με επιθέσεις. Η εφαρμογή ανθρώπινης εμπειρογνωμοσύνης και γνώσης είναι σημαντική σε αυτό το στάδιο. Η κατανόηση των τεχνικών των αντιπάλων και του τι είναι «φυσιολογικό» στο περιβάλλον σας είναι κρίσιμη για να διαχωρίσετε ύποπτες από φυσιολογικές συμπεριφορές.

Τεχνικές όπως η **συχνότητα εμφάνισης** και η **εμπλουτισμένη πληροφορία** (π.χ., εξωτερικά metadata για να καθορίσετε αν ένα αντικείμενο είναι κακόβουλο ή όχι) μπορούν να μειώσουν σημαντικά την ανθρώπινη προσπάθεια στην ανάλυση. Κατά την ανάπτυξη αναλύσεων, σκεφτείτε τα τακτικά και στρατηγικά πλεονεκτήματα αυτών των τεχνικών στην αποφυγή ψευδών θετικών και στη μείωση του όγκου των δεδομένων προς ανάλυση.

Βήμα 4: Αυτοματοποίηση: Συνήθως μπορείτε να αυτοματοποιήσετε και να προγραμματίσετε τις διαδικασίες συλλογής γεγονότων, μείωσης δεδομένων και αντιστοίχισης λέξεων-κλειδιών. Η αυτοματοποίηση αντικαθιστά χειροκίνητες διαδικασίες και απελευθερώνει τους αναλυτές για να εφαρμόσουν τη κρίση τους στα αποτελέσματα. Ιδανικά, οι εργασίες που δεν απαιτούν γνώση ανατίθενται σε μηχανές, ενώ εκείνες που απαιτούν κρίση παραμένουν στους ανθρώπινους αναλυτές.

Βήμα 5: Τεκμηρίωση: Κατά τη διάρκεια ενός κυνηγιού, είναι πολύ δελεαστικό να συνεχίζετε την ανάλυση δεδομένων και να αναβάλετε την τεκμηρίωση, ή ακόμα να την παραλείπετε. Ωστόσο, αυτό είναι τακτικά λάθος. Συνήθως είναι αδύνατο να θυμηθεί κανείς λεπτομέρειες του κυνηγιού εκ των υστέρων: τα στοιχεία που συλλέχθηκαν, οι τύποι ανάλυσης που πραγματοποιήθηκαν, η λογική για την αποφυγή ψευδών θετικών και η αιτιολόγηση των συμπερασμάτων. Αυτές οι πληροφορίες χάνονται αν δεν καταγραφούν κατά τη διάρκεια του κυνηγιού.

Συμβουλή: Οι έμπειροι αναλυτές πρέπει να καταγράφουν τις μεθόδους τους για τον εντοπισμό ύποπτων γεγονότων. Οι οδηγίες αυτές είναι πολύτιμες για λιγότερο έμπειρα μέλη της ομάδας. Σκεφτείτε να δημιουργήσετε ένα «training dataset» βασισμένο σε κοινά κυνηγιά που πραγματοποιήθηκαν, για εκπαίδευση νέων αναλυτών.

Συμβουλή: Κατά την τεκμηρίωση, εντοπίστε ευκαιρίες για μείωση του όγκου δεδομένων που συλλέγονται, π.χ. φιλτράροντας γνωστά ή αξιόπιστα γεγονότα. Αυτό βελτιώνει την ικανότητα γρήγορης απάντησης σε ερωτήματα.

Βήμα 6: Επικοινωνία και Αναφορά: Αποφασίστε από την αρχή τι θα επικοινωνείται στη διοίκηση και πότε. Αυτό περιλαμβάνει πότε θα ανακοινωθεί ότι εντοπίστηκε περιστατικό και πόσο συχνά θα παρέχονται ενημερώσεις για την πρόοδο.

Στο τέλος του κυνηγιού, δημιουργήστε ένα αρχείο που περιλαμβάνει:

- Μετρήσεις του κυνηγιού
- Αιτία τυχόν παραβίασης
- Εύρος επηρεαζόμενων μηχανών, λογαριασμών και εφαρμογών
- Περιγραφή των ανιχνευμένων τεχνικών
- IOCs για τον εντοπισμό παρόμοιων επιθέσεων
- Μαθήματα και περιοχές για αύξηση ορατότητας και βελτίωση μελλοντικών κυνηγιών
- Προτάσεις για αλλαγές στους μηχανισμούς ασφαλείας
- Περιγραφή νέων αναλύσεων για ανίχνευση και ειδοποίηση

Συμβουλή: Καθώς η ομάδα ωριμάζει, παρακολουθήστε πότε γίνονται οι προτάσεις και πόσο χρόνο χρειάζεται για να υλοποιηθούν. Αυτό δίνει σημαντικές ενδείξεις για την επιρροή της ομάδας.

Μην ξεχνάτε: Η οργάνωση πρέπει να έχει επίσημη διαδικασία για κοινοποίηση των αποτελεσμάτων στο διοικητικό επίπεδο. Είναι κρίσιμο να υπάρχει **εκτελεστικός χορηγός** με επαρκή αρμοδιότητα για την προώθηση των στόχων της ομάδας. Γενικά, όσο μεγαλύτερη η υποστήριξη από τη διοίκηση, τόσο μεγαλύτερη επιρροή θα έχει η ομάδα.

Παράδειγμα

Threat Actor: Μια πρόσφατη οργανωσιακή εκτίμηση απειλών κατέληξε στο συμπέρασμα ότι η Ομάδα *Lazarus* συνιστά απειλή υψηλής προτεραιότητας για τον υπό εξέταση οργανισμό. Η συγκεκριμένη ομάδα έχει αποδοθεί με πολυάριθμες κακόβουλες εκστρατείες, οι οποίες έχουν καταγραφεί και ταξινομηθεί στο πλαίσιο γνώσης *MITRE ATT&CK Navigator*. Οι τεχνικές που χρησιμοποιούνται από την Ομάδα *Lazarus* περιλαμβάνουν ένα ευρύ φάσμα τακτικών, από την αρχική πρόσβαση μέχρι την εξαγωγή δεδομένων.

Υπόθεση: Εάν ο εν λόγω απειλητικός πράκτορας δραστηριοποιηθεί εντός του δικτύου μας, αναμένεται να παρατηρηθούν ενδείξεις εφαρμογής πολλαπλών τεχνικών, σε αλληλουχία και συνδυασμό που συνάδει με τα ήδη καταγεγραμμένα μονοπάτια επίθεσης, όπως αυτά περιγράφονται στο MITRE ATT&CK. Ως εκ τούτου, η ανίχνευση τέτοιων μοτίβων θα μπορούσε να αποτελέσει ένδειξη παρουσίας της ομάδας.

Εργαλείο: Η ανάλυση πληροφοριών κυβερνοαπειλών (Cyber Threat Intelligence - CTI), σε συνδυασμό με την τρέχουσα αξιολόγηση της ασφάλειας των συστημάτων μας, υποδεικνύει ότι ο οργανισμός μας παραμένει εκτεθειμένος σε επιθέσεις που αξιοποιούν παραλλαγές του *WannaCry ransomware*. Η ευαλωτότητα αυτή προκύπτει από τη συνεχιζόμενη χρήση του πρωτοκόλλου *SMBv1*, το οποίο είναι γνωστό ότι έχει καταστεί παρωχημένο και επιρρεπές σε εκμετάλλευση.

Υπόθεση: Σε περίπτωση μόλυνσης του δικτύου από το *WannaCry*, είναι αναμενόμενο να καταγραφούν ενδείξεις αυξημένης δραστηριότητας που σχετίζεται με την επεξεργασία και τη μετονομασία αρχείων. Συνεπώς, η παρατήρηση ασυνήθιστων ρυθμών μετονομασίας θα μπορούσε να λειτουργήσει ως αξιόπιστος δείκτης επίθεσης (Indicator of Attack – IoA).

Τεχνική: Η τεχνική πλευρικής κίνησης (*lateral movement*) μέσω *Exploitation of Remote Services* δύναται να πραγματοποιηθεί αξιοποιώντας την ευαλωτότητα *MS17-010*. Συγκεκριμένα, η εκμετάλλευση αυτή είναι εφικτή μέσω του πλαισίου *Metasploit*, με χρήση ειδικής μονάδας που αποστέλλει τροποποιημένο αίτημα *Server Message Block (SMB)* συγκεκριμένου μεγέθους, με στόχο την υπονόμηση του απομακρυσμένου συστήματος.

Υπόθεση: Εάν εφαρμοστεί η εν λόγω τεχνική σε δίκτυο του οργανισμού μας, αναμένεται ότι θα καταγραφούν ανωμαλίες στα αρχεία καταγραφής, οι οποίες θα συνδέονται με την αποστολή και επεξεργασία τέτοιων τροποποιημένων SMB αιτημάτων. Η απομόνωση και ανάλυση των αιτημάτων αυτών μπορεί να λειτουργήσει ως μέσο εντοπισμού της συγκεκριμένης τεχνικής.

Διαβάστε Περισσότερα:

<https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Detecting-the-Unknown-A-Guide-to-Threat-Hunting-v2.0.pdf>

Παραδοσιακός Ορισμός Απειλής

- **Απειλή = Ικανότητα + Πρόθεση:** Στο παραδοσιακό μοντέλο, μια απειλή αξιολογείται με βάση δύο βασικά στοιχεία:
 1. **Ικανότητα (Capability):** Τι μπορεί να κάνει ο επιτιθέμενος – δηλαδή, τα εργαλεία και οι δεξιότητες που διαθέτει για να εκτελέσει μια επίθεση.
 2. **Πρόθεση (Intent):** Η κίνηση ή η πρόθεση πίσω από την επίθεση – ποιο είναι το κίνητρο για την εκτέλεση της επίθεσης, π.χ., οικονομικό όφελος, πολιτική ατζέντα ή σαμποτάζ.

Νέος Ορισμός Απειλής

- **Απειλή = Ικανότητα + Πρόθεση + Γνώση:** Το νέο μοντέλο προσθέτει έναν τρίτο, κρίσιμο παράγοντα: τη γνώση.
 1. **Ικανότητα (Capability):** Περιλαμβάνει όχι μόνο τα εργαλεία αλλά και την πρόσβαση σε συστήματα, όπως π.χ. εργαλεία εκμετάλλευσης ευπαθειών (exploits), botnets ή πρόσβαση σε VPN.
 2. **Πρόθεση (Intent):** Η κίνηση πίσω από την επίθεση – για παράδειγμα, η υποκλοπή δεδομένων, η διακοπή υπηρεσιών ή η καταστροφή κρίσιμων υποδομών.
 3. **Γνώση (Knowledge):** Η εξειδικευμένη και σύνθετη ικανότητα να λειτουργήσει μέσα σε ένα σύστημα ή δίκτυο αφού αποκτηθεί πρόσβαση. Αυτό περιλαμβάνει την κατανόηση της αρχιτεκτονικής του συστήματος, των πολιτικών ασφάλειας, των διαδικασιών παρακολούθησης και των κενών ασφαλείας.

Παράδειγμα: Ένας επιτιθέμενος μπορεί να έχει εργαλεία phishing (ικανότητα) και να θέλει να κλέψει οικονομικά δεδομένα (πρόθεση). Ωστόσο, αν διαθέτει γνώση σχετικά με το πώς λειτουργούν τα εσωτερικά δίκτυα μιας τράπεζας και πώς να παρακάμψει τα IDS/IPS, η απειλή γίνεται πολύ πιο σοβαρή. Το νέο παράδειγμα απειλής είναι ιδιαίτερα εφαρμόσιμο σε **υψηλού επιπέδου απειλές**, όπως:

- Στοχευμένες επιθέσεις APT (Advanced Persistent Threats)
- Επιθέσεις κρατών ή μεγάλων οργανωμένων ομάδων
- Πολύπλοκο malware που προσαρμόζεται στις συνθήκες του στόχου

Το Πλεονέκτημα του Επιτιθέμενου

- Ο επιτιθέμενος χρειάζεται να είναι **επιτυχής μόνο μία φορά**, ενώ ο αμυνόμενος πρέπει να προστατεύει συνεχώς ολόκληρο το σύστημα.
- Οι επιτιθέμενοι είναι συχνά **αποφασισμένοι, έμπειροι και χρηματοδοτούμενοι**, γεγονός που τους δίνει πλεονέκτημα σε μακροχρόνιες επιθέσεις.

- Χρησιμοποιούν **εξατομικευμένο malware, 0-day ευπάθειες, πολλαπλά μονοπάτια επίθεσης (attack vectors) και social engineering.**
- Η επίθεση μπορεί να είναι **επίμονη (Persistent)**, με πολλαπλές προσπάθειες εισβολής και παραμονής μέσα στο σύστημα για εκτεταμένη χρονική διάρκεια.

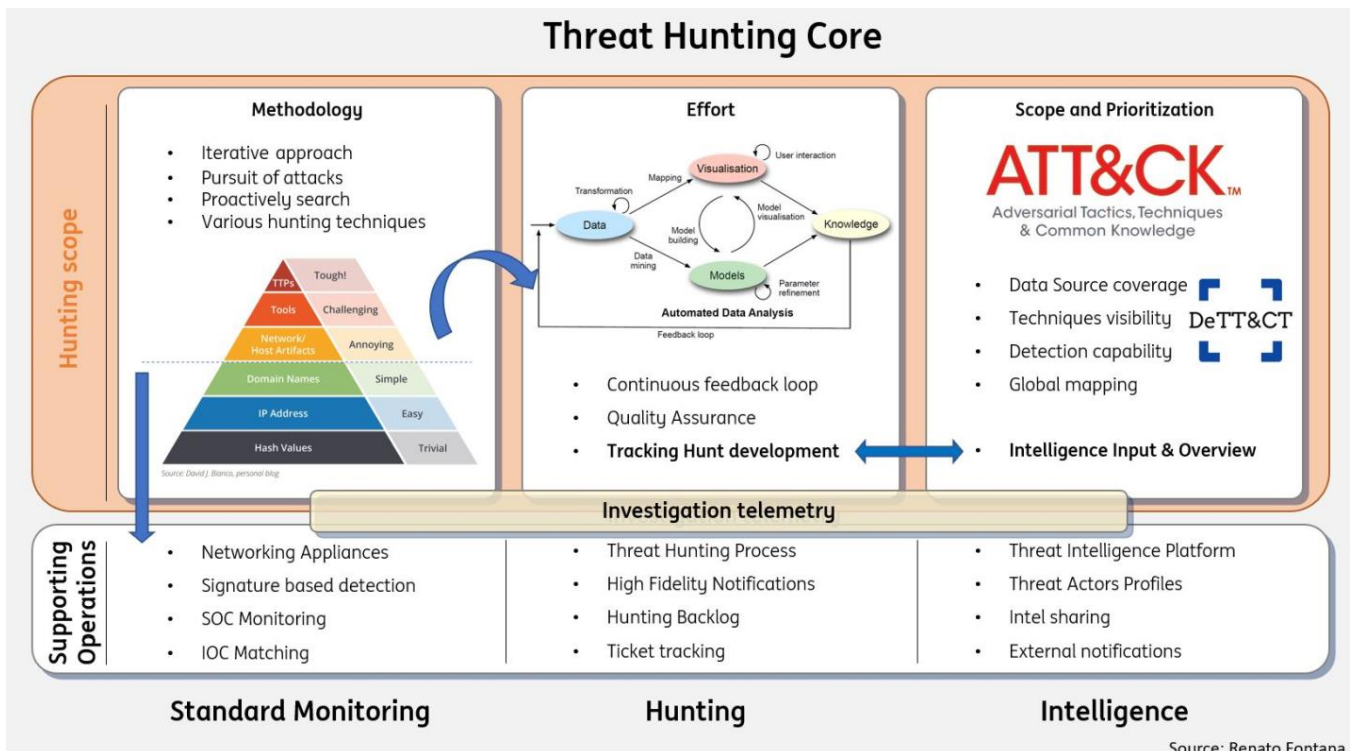
Παράδειγμα: Μια ομάδα APT μπορεί να χρησιμοποιήσει αρχικά spear-phishing για να αποκτήσει πρόσβαση σε έναν χρήστη, να χρησιμοποιήσει έναν 0-day exploit για να περάσει στο δίκτυο, και στη συνέχεια να κινηθεί lateral μέσω των εσωτερικών συστημάτων, συλλέγοντας ευαίσθητα δεδομένα για μήνες χωρίς να ανιχνευθεί.

Το Μειονέκτημα του Αμυνόμενου: Οι αμυνόμενοι συχνά θεωρούνται “**Unsung Heroes**”, καθώς αντιμετωπίζουν καθημερινά τεράστιες προκλήσεις με περιορισμένους πόρους.

- Είναι **υποστελεχωμένοι, πολυλειτουργικοί και υποχρηματοδοτούμενοι.**
- Η **αυξανόμενη πολυπλοκότητα των IT υποδομών** δυσχεραίνει την άμυνα:
 - Μεταφορά δεδομένων στο cloud
 - Εικονικοποίηση servers και εφαρμογών
 - Bring Your Own Device (BYOD) πολιτικές
- Οι **προληπτικοί έλεγχοι (prevention controls)** δεν μπορούν να μπλοκάρουν όλες τις επιθέσεις.
- Υπάρχουν **εκατοντάδες συστήματα και ευπάθειες** που πρέπει να ενημερώνονται και να επιδιορθώνονται, γεγονός που δημιουργεί μια “επιφάνεια επίθεσης” δύσκολα διαχειρίσιμη.

Παράδειγμα: Σε μια μεγάλη επιχείρηση με εκατοντάδες servers, εκατοντάδες εφαρμογές και πολλούς χρήστες, η ενημέρωση όλων των συστημάτων εγκαίρως είναι σχεδόν αδύνατη. Ένας επιτιθέμενος μπορεί να εκμεταλλευτεί ένα παλιό server ή έναν μη ενημερωμένο endpoint για να εισέλθει στο δίκτυο.

Το **Threat Hunting** αποτελεί μια **προληπτική προσέγγιση στην κυβερνοάμυνα**. Σε αντίθεση με τις παραδοσιακές μεθόδους ασφάλειας, οι οποίες περιμένουν να ενεργοποιηθούν οι ειδοποιήσεις (alerts) από συστήματα όπως IDS, IPS ή antivirus, το threat hunting **εντοπίζει απειλές πριν προκαλέσουν ζημιά.**



Τι κάνει το Threat Hunting:

- Προληπτική και επαναληπτική ανακάλυψη (Proactive & Iterative Discovery): Οι threat hunters εξετάζουν συνεχώς τα δίκτυα, τα endpoints (υπολογιστές, servers, κινητές συσκευές) και άλλες υποδομές για να ανιχνεύσουν ύποπτες δραστηριότητες. Αυτή η διαδικασία δεν είναι τυχαία· βασίζεται σε υποθέσεις και προηγούμενα μοτίβα επιθέσεων.
- Ανίχνευση απειλών που παρακάμπτουν τα υπάρχοντα μέτρα ασφαλείας: Ορισμένες απειλές, όπως εξελιγμένο malware ή stealthy APTs, μπορούν να αποφύγουν τα παραδοσιακά εργαλεία ασφαλείας. Το threat hunting εντοπίζει αυτές τις απειλές με ενεργητική ανάλυση και μηχανισμούς συλλογής πληροφοριών.

Τεχνικές Διαδικασίες:

1. Συλλογή δεδομένων (Data Collection):

- Καταγραφή logs από endpoints, firewalls, IDS/IPS, συσκευές cloud.
- Χρήση EDR (Endpoint Detection & Response) και SIEM (Security Information and Event Management) για συγκεντρωτική ανάλυση.

2. Ανάλυση και Υποθέσεις (Hypothesis-driven Analysis):

- Οι hunters δημιουργούν υποθέσεις για πιθανές επιθέσεις, π.χ. «Ένας χρήστης επιχειρεί πρόσβαση σε κρίσιμα δεδομένα εκτός ωραρίου εργασίας».
- Εφαρμόζουν queries και scripts για την επιβεβαίωση ή διάψευση της υπόθεσης.

3. Ανίχνευση και Απόκριση (Detection & Response):

- ο Εντοπισμός ανωμαλιών, όπως περίεργες συνδέσεις σε εξωτερικά IP, μη εξουσιοδοτημένη εκτέλεση διαδικασιών ή κρυφή κίνηση δεδομένων.
- ο Ανάλυση δράσης: απομόνωση endpoint, blocking IP, ειδοποίηση SOC (Security Operations Center).

Παραδείγματα: Εντοπισμός **lateral movement** μέσα στο δίκτυο που δεν ανιχνεύθηκε από firewall ή IDS. Αναγνώριση **stealthy malware** που κρύβεται σε processes υψηλής προτεραιότητας. ροληπτική αποτροπή επίθεσης μέσω **phishing email campaigns**, παρατηρώντας patterns στις email headers και attachments.

14.6. Πώς να κάνετε Threat Hunting (Κυνηγητό Απειλών)

Το **threat hunting** βασίζεται στη **επιστημονική μέθοδο**. Για να πραγματοποιήσει κάποιος ένα threat hunt, το μόνο που χρειάζεται είναι να αξιολογήσει και να δοκιμάσει μια υπόθεση. Η κύρια πρόκληση στο threat hunting είναι η ανάπτυξη υποθέσεων που να είναι εύκολα ελέγξιμες και που, όταν ελεγχθούν, να παρέχουν χρήσιμες πληροφορίες.

Διάγραμμα threat hunting δικτύου (clearnetwork threat hunting diagram)

Όπως φαίνεται στην παραπάνω εικόνα, το threat hunting μπορεί να χωριστεί σε πέντε κύρια στάδια:

1. Επιλογή στόχου: Αυτό το στάδιο της διαδικασίας threat hunting αποσκοπεί στο να καθοριστεί η **ερώτηση** που το threat hunt έχει σχεδιαστεί να απαντήσει. Ένας καλός πόρος για αυτήν την απόφαση είναι το **MITRE ATT&CK framework**, το οποίο περιγράφει τις φάσεις μιας κυβερνοεπίθεσης και διάφορες μεθόδους που μπορεί να χρησιμοποιήσει ένας επιτιθέμενος για να ολοκληρώσει κάθε φάση. Η επιλογή μιας από αυτές τις τακτικές και η προσπάθεια ανίχνευσής της στο δίκτυο αποτελεί ένα καλό σημείο εκκίνησης για ένα threat hunt.

2. Δημιουργία υπόθεσης: Σε αυτό το στάδιο, ο threat hunter δημιουργεί μια **ελέγξιμη υπόθεση** που θα βοηθήσει να προσδιοριστεί αν η επιλεγμένη τακτική χρησιμοποιείται στο δίκτυο. Οι υποθέσεις αυτές θα μπορούσαν να έχουν τη μορφή: *"Αν συμβαίνει X στο δίκτυο, τότε σημαίνει ότι συμβαίνει <επιλεγμένη τεχνική>."* Το **MITRE ATT&CK** είναι επίσης χρήσιμη εδώ, καθώς περιγράφει μια ποικιλία μηχανισμών ανίχνευσης για κάθε τεχνική.

3. Συλλογή δεδομένων: Σε αυτό το σημείο, ο threat hunter συλλέγει δεδομένα σχεδιασμένα να καθορίσουν την εγκυρότητα της υπόθεσης. Τα δεδομένα που συλλέγονται πρέπει να μπορούν να δείξουν εάν το X συμβαίνει ή όχι στο δίκτυο.

4. Ανάλυση δεδομένων: Τα περισσότερα δεδομένα που συλλέγονται κατά τη διάρκεια ενός threat hunt πιθανότατα θα είναι μεγάλα σε όγκο και με πολύ θόρυβο. Σε αυτό το στάδιο, ο threat hunter φιλτράρει και συγκεντρώνει τα δεδομένα για να βρει απάντηση στο αν το X συμβαίνει ή όχι στο δίκτυο.

5. Συμπεράσματα: Με βάση τα δεδομένα που συλλέχθηκαν, θα πρέπει να είναι δυνατό να **αποδειχθεί ή να διαψευσθεί η υπόθεση** και να ληφθούν διορθωτικά μέτρα αν η υπόθεση υποστηρίζεται. Αν τα συλλεχθέντα δεδομένα δεν απαντούν στην ερώτηση, η υπόθεση μπορεί να **βελτιωθεί** με βάση τα αποτελέσματα, ώστε να παρέχει μια πιο χρήσιμη απάντηση.

Επιπτώσεις του Threat Hunting: Ένας threat hunter **δοκιμάζει μια σειρά υποθέσεων** με την ελπίδα να ανιχνεύσει μια άγνωστη απειλή στο δίκτυο ή να αποδείξει ότι μια δεδομένη απειλή δεν υπάρχει. Ως αποτέλεσμα, το threat hunting μπορεί να είναι πολύτιμο για έναν οργανισμό, καθώς βοηθά στην **ανίχνευση τρεχουσών απειλών** στα συστήματά του και παρέχει μια **ακριβή εκτίμηση του τρέχοντος επιπέδου κυβερνοκινδύνου**. Ωστόσο, τα οφέλη του threat hunting δεν σταματούν εδώ. Κατά τη διάρκεια του threat hunt, ο hunter **ορίζει και βελτιώνει μια μέθοδο ανίχνευσης** μιας συγκεκριμένης απειλής στο δίκτυο. Στο τέλος, ακόμα και αν το αποτέλεσμα ήταν η διάψευση της υπόθεσης, αυτός ο μηχανισμός ανίχνευσης μπορεί να προστεθεί στο **εργαλειοθήκη κυβερνοασφάλειας** του οργανισμού. Με την αυτοματοποίηση των ελέγχων και της ανάλυσης, ο οργανισμός μπορεί να **εντοπίζει ταχύτερα μελλοντικές απειλές** ή ακόμη και να **ανιχνεύει και να αποκλείει επιθέσεις εν εξελίξει**. Το threat hunting επίσης **βελτιώνει τις γνώσεις του threat hunter** για την υποδομή του δικτύου και τις πιθανές απειλές που μπορεί να αντιμετωπίσει ο οργανισμός. Αυτή η γνώση μπορεί να είναι ανεκτίμητη για την ασφάλεια του οργανισμού, γι' αυτό μια ομάδα ασφαλείας με δυνατότητες threat hunting μπορεί να είναι ανεκτίμητη για οργανισμούς που προσπαθούν να διαχειριστούν το **κυβερνοασφαλές τους προφίλ κινδύνου**.

>> **Εργαστήριο:** Ένα από τα στοιχεία που μπορούν να συμβάλουν στη βελτίωση της αποδοτικότητας στη διαδικασία του *threat hunting* είναι το **Threat Hunting Playbook**. Το *playbook* αυτό περιλαμβάνει όλες τις υποθέσεις και τα βήματα της διαδικασίας εντοπισμού απειλών, τα οποία έχουν καταρτιστεί από τους *threat hunters*, αποτρέποντας έτσι την επαναλαμβανόμενη εκτέλεση των ίδιων διαδικασιών. Επιπλέον, το *playbook* μπορεί να ενσωματώνει ενδεικτικά σύνολα δεδομένων από προηγούμενες δραστηριότητες εντοπισμού απειλών, με στόχο να διευκολυνθούν νέοι *threat hunters* στην κατανόηση του περιεχομένου και της χρησιμότητάς του.

Παράδειγμα Ανοικτού Κώδικα Threat Hunting Playbook: *Jupyter Notebook* και *Mordor Datasets*
(από τον Roberto Rodriguez). [Σύνδεσμος](#)

<https://threathunterplaybook.com/hunts/windows/intro.html>

[https://github.com/OTRF/ThreatHunter-
Playbook/tree/f2961da43cca20e3ce0694afa048f144708cff98/docs/hunts/windows](https://github.com/OTRF/ThreatHunter-Playbook/tree/f2961da43cca20e3ce0694afa048f144708cff98/docs/hunts/windows)

Use Case 1: Εκκίνηση της διαδικασίας cmd.exe

Αναφορά MITRE: CAR-2013-02-003 [Σύνδεσμος](#)

Διαδικασία: Δημιουργία/εκκίνηση της διαδικασίας cmd.exe

Υπόθεση (Hypothesis): Το cmd.exe είναι το εργαλείο της Γραμμής Εντολών των Windows που παρέχει περιβάλλον εντολών (command line interface) στο λειτουργικό σύστημα. Μέσω αυτού μπορούν να εκτελεστούν επιπλέον προγράμματα και διαθέτει αρκετές ενσωματωμένες εντολές, όπως:

- dir (λίστα αρχείων και φακέλων)
- copy (αντιγραφή αρχείων)
- mkdir (δημιουργία φακέλου)
- type (προβολή περιεχομένου αρχείων)

Επίσης, μπορεί να εκτελεί batch scripts (.bat).

Συμπεριφορά χρήστη και προγράμματα: Συνήθως, όταν ένας χρήστης ανοίγει τη Γραμμή Εντολών, ο γονικός (parent) process είναι το explorer.exe ή άλλη instance του command prompt. Μπορεί να υπάρχουν αυτοματοποιημένα προγράμματα, scripts σύνδεσης (logon scripts) ή εργαλεία διαχείρισης που εκκινούν instances του cmd.exe για την εκτέλεση scripts ή ενσωματωμένων εντολών. Ωστόσο, η εκκίνηση της διαδικασίας cmd.exe από συγκεκριμένους γονικούς processes μπορεί να αποτελεί ένδειξη κακόβουλης δραστηριότητας.

Παράδειγμα Use Case Hunting (ανίχνευσης): Αν το Adobe Reader ή το Outlook εκκινήσει ένα command shell, αυτό μπορεί να υποδηλώνει ότι έχει φορτωθεί κάποιο κακόβουλο έγγραφο και χρειάζεται περαιτέρω έρευνα. Επομένως, παρακολουθώντας ασυνήθιστους γονικούς processes του cmd.exe, είναι δυνατό να εντοπιστούν ενέργειες επιτιθέμενων (adversaries).

Συνοπτική επεξήγηση: Αυτό το use case αφορά τον εντοπισμό πιθανών κακόβουλων ενεργειών μέσω της παρακολούθησης της δημιουργίας της διαδικασίας cmd.exe. Η εκτέλεση της Γραμμής Εντολών από μη συνηθισμένες εφαρμογές ή γονικές διεργασίες αποτελεί ύποπτο σημάδι και μπορεί να βοηθήσει στην έγκαιρη ανίχνευση επιθέσεων ή κακόβουλου λογισμικού.

Use Case 2: Δραστηριότητες RDP

Αναφορά MITRE: CAR-2016-04-005 [Σύνδεσμος](#)

Υπόθεση (Hypothesis): Η σύνδεση μέσω Remote Desktop (RDP) μπορεί να είναι φυσιολογική για έναν διαχειριστή συστήματος ή για το IT support, αλλά μόνο από συγκεκριμένους, εγκεκριμένους υπολογιστές εργασίας.

Σκοπός Παρακολούθησης: Η παρακολούθηση των συνδέσεων RDP και η σύγκριση με γνωστά/εγκεκριμένα συστήματα προέλευσης μπορεί να εντοπίσει **πλευρικές κινήσεις (lateral movement)** ενός επιτιθέμενου μέσα στο δίκτυο.

Παράδειγμα Use Case Hunting (ανίχνευσης): Αναζήτηση **επιτυχημένων συνδέσεων RDP** που (i) δεν προέρχονται από τη χώρα σας (χρήση GeoIP για εντοπισμό), (ii) γίνονται **μετά τις ώρες εργασίας**

Συνοπτική επεξήγηση: Αυτό το use case αφορά τον εντοπισμό ύποπτων προσπαθειών απομακρυσμένης σύνδεσης μέσω RDP. Αν μια επιτυχής σύνδεση προέρχεται από ασυνήθιστη τοποθεσία ή ώρα, μπορεί να αποτελεί ένδειξη ότι κάποιος επιτιθέμενος επιχειρεί να μετακινηθεί μέσα στο δίκτυο ή να αποκτήσει μη εξουσιοδοτημένη πρόσβαση.

Use Case 3: Διακοπή των Υπηρεσιών Άμυνας των Windows

Αναφορά MITRE: CAR-2016-04-003 [Σύνδεσμος](#)

Διαδικασία: Απενεργοποίηση ή διακοπή του Windows Defender ή του Windows Firewall

Υπόθεση (Hypothesis): Το spyware και το malware παραμένουν σοβαρό πρόβλημα, και η Microsoft ανέπτυξε υπηρεσίες ασφαλείας όπως το **Windows Defender** και το **Windows Firewall** για την προστασία των συστημάτων. Σε περίπτωση που αυτές οι υπηρεσίες απενεργοποιηθούν:

- Οι διαχειριστές πρέπει να επαναφέρουν άμεσα τη λειτουργία τους για να αποφευχθεί πιθανή μόλυνση ή περαιτέρω εξάπλωση κακόβουλου λογισμικού.
- Πρέπει να διερευνηθεί αν η απενεργοποίηση οφείλεται σε δυσλειτουργία (crash) ή σε χειρισμό από χρήστη ή κακόβουλο λογισμικό.

Συμπεριφορά χρήστη και προγράμματα: Συνήθως, οι υπηρεσίες ασφαλείας των Windows εκκινούν αυτόματα κατά την εκκίνηση του λειτουργικού. Αν διακοπούν απρόσμενα λίγο μετά από σύνδεση (logon) ενός χρήστη στο εσωτερικό δίκτυο ή μέσω δικτυακών υπηρεσιών, αυτό μπορεί να υποδηλώνει:

- Κακόβουλη ενέργεια (malware, spyware, ransomware) που προσπαθεί να παρακάμψει τα μέτρα ασφαλείας.
- Απρόβλεπτο σφάλμα ή crash της υπηρεσίας.

Παράδειγμα Use Case Hunting (ανίχνευσης):

- Οι υπηρεσίες antivirus (Windows Defender, Windows Firewall) σταματούν λίγο μετά από επιτυχημένη σύνδεση από χρήστη στο εσωτερικό δίκτυο μέσω δικτυακών υπηρεσιών.
- Παρακολούθηση ασυνήθιστων σταματημάτων υπηρεσιών μπορεί να αποκαλύψει κακόβουλες ενέργειες ή προσπάθειες παράκαμψης ασφαλείας.

Συνοπτική επεξήγηση: Αυτό το use case επικεντρώνεται στον εντοπισμό πιθανών επιθέσεων μέσω της παρακολούθησης της λειτουργίας των βασικών υπηρεσιών ασφαλείας των Windows. Η απενεργοποίηση του Windows Defender ή του Firewall από μη αναμενόμενες αιτίες αποτελεί ύποπτο σημάδι και μπορεί να χρησιμοποιηθεί για έγκαιρη ανίχνευση κακόβουλων ενεργειών ή συμβάντων ασφάλειας.

Use Case 4: Χρήση του Task Scheduler των Windows

Αναφορά MITRE: CAR-2020-09-001 [Σύνδεσμος](#)

Διαδικασία: Δημιουργία ή εκτέλεση προγραμματισμένων εργασιών μέσω του Windows Task Scheduler

Υπόθεση (Hypothesis): Για να αποκτήσει **επιμονή (persistence)**, **ανύψωση δικαιωμάτων (privilege escalation)** ή **απομακρυσμένη εκτέλεση (remote execution)**, ένας επιτιθέμενος μπορεί να χρησιμοποιήσει τον **Windows Task Scheduler** για να προγραμματίσει την εκτέλεση μιας εντολής σε συγκεκριμένη ώρα, ημερομηνία ή ακόμα και σε συγκεκριμένο υπολογιστή.

Ο Task Scheduler αποθηκεύει τις εργασίες ως αρχεία σε δύο κύριες τοποθεσίες:

- C:\Windows\Tasks (παλαιότερη μέθοδος)
- C:\Windows\System32\Tasks

Αυτό το use case επικεντρώνεται στην **ανίχνευση δημιουργίας αρχείων εργασιών** σε αυτές τις τοποθεσίες ως ένδειξη πιθανής κακόβουλης δραστηριότητας.

Συμπεριφορά χρήστη και προγράμματα: Ο Task Scheduler συνήθως χρησιμοποιείται για νόμιμες εργασίες συντήρησης, ενημερώσεις ή αυτοματισμούς. Ωστόσο, αν:

- Οι εργασίες εκτελούνται από **ύποπτους φακέλους** (π.χ. C:\Users\.. ή C:\Windows\temp\)
- Χρησιμοποιούνται **ύποπτα εργαλεία scripting** (LOLBAS) όπως: cscript.exe, rundll32.exe, mshta.exe, powershell.exe, regsvr32.exe

τότε αυτό αποτελεί ένδειξη πιθανής κακόβουλης δραστηριότητας.

Παράδειγμα Use Case Hunting (ανίχνευσης):

- Προγραμματισμένη εργασία που δημιουργείται ή εκτελείται από μη τυπική τοποθεσία φακέλου.
- Προγραμματισμένη εργασία που εκκινείται μέσω εργαλείων scripting ή εκτελέσιμων συνήθως χρησιμοποιούμενων για κακόβουλες ενέργειες (LOLBAS).

Συνοπτική επεξήγηση: Αυτό το use case στοχεύει στον εντοπισμό πιθανών επιθέσεων ή κακόβουλων ενεργειών μέσω της χρήσης του Task Scheduler. Η παρακολούθηση της δημιουργίας και εκτέλεσης προγραμματισμένων εργασιών σε μη τυπικές τοποθεσίες ή με ύποπτα εργαλεία βοηθά στην έγκαιρη ανίχνευση επιθέσεων και τη διαχείριση συμβάντων ασφάλειας.

Use Case 5: Credential Dumping μέσω του Windows Task Manager

Αναφορά MITRE: CAR-2020-09-001 [Σύνδεσμος](#)

Διαδικασία: Δημιουργία dump αρχείου της διαδικασίας lsass.exe μέσω του Windows Task Manager

Υπόθεση (Hypothesis): Ο **Windows Task Manager** μπορεί να χρησιμοποιηθεί για να δημιουργηθεί **αντίγραφο μνήμης (memory dump)** της διαδικασίας lsass.exe στο δίσκο, ώστε να επεξεργαστεί με εργαλεία **credential access** όπως το Mimikatz. Η διαδικασία περιλαμβάνει:

1. Εκκίνηση του Task Manager ως χρήστης με δικαιώματα διαχειριστή (privileged user).
2. Επιλογή της διαδικασίας lsass.exe.
3. Κλικ στο “Create dump file”.

Αυτό αποθηκεύει ένα dump αρχείο στο δίσκο με **ονομασία που περιλαμβάνει το όνομα της διαδικασίας** (lsass.exe), γεγονός που καθιστά τον εντοπισμό του πιο εύκολο.

Συμπεριφορά χρήστη και προγράμματα: Η νόμιμη χρήση του Task Manager δεν περιλαμβάνει συνήθως τη δημιουργία dump αρχείων του lsass.exe. Επομένως, η δημιουργία dump αρχείων από τον Task Manager αποτελεί ύποπτη δραστηριότητα που μπορεί να υποδηλώνει προσπάθεια **κλοπής διαπιστευτηρίων**.

Παράδειγμα Use Case Hunting (ανίχνευσης):

- Παρακολούθηση δημιουργίας αρχείων (File Creation) από το Sysmon Event ID 11.
- Ο γονικός ή εκτελούμενος process είναι taskmgr.exe.
- Αναζήτηση dump αρχείων που περιλαμβάνουν το όνομα lsass.exe.

Συνοπτική επεξήγηση: Αυτό το use case στοχεύει στον εντοπισμό πιθανών **κλοπών διαπιστευτηρίων (credential dumping)** μέσω της χρήσης του Task Manager. Η ανίχνευση δημιουργίας dump αρχείων του lsass.exe από μη συνηθισμένες διεργασίες αποτελεί ένδειξη κακόβουλης δραστηριότητας και μπορεί να επιτρέψει την έγκαιρη αντίδραση σε επίθεση.

Hypothesis 1: Ο χρήστης επισκέπτεται κακόβουλο ιστότοπο μέσω Phishing Email: Ένας χρήστης μπορεί να πέσει θύμα phishing και να ανοίξει έναν κακόβουλο σύνδεσμο από email, ο οποίος τον οδηγεί σε ιστοσελίδα που περιέχει κακόβουλο λογισμικό ή συλλέγει διαπιστευτήρια. Η δραστηριότητα αυτή αποτελεί **σημαντικό κίνδυνο ασφάλειας**, καθώς μπορεί να οδηγήσει σε υποκλοπή credentials, εγκατάσταση malware ή πρόσβαση σε εταιρικούς πόρους.

Πηγές Δεδομένων για Hunting (Data Sources): **Passive DNS Log / DNS Server Log:** Καταγραφή όλων των DNS queries. Χρησιμοποιείται για να εντοπιστούν αιτήματα προς γνωστά phishing domains ή domains που μοιάζουν με εταιρικά. **Proxy Log / NGFW Log (Next-Generation Firewall):** Καταγραφή των HTTP/HTTPS αιτήσεων των χρηστών. Επιτρέπει τον εντοπισμό επισκέψεων σε κακόβουλους ή ύποπτους ιστότοπους. **Sysmon Log:** Καταγράφει διεργασίες, δικτυακές συνδέσεις και file creations, χρήσιμο για να συσχετιστούν ενέργειες malware με την επίσκεψη σε phishing site. **Email Log / Mail Security Gateway Log:** Εντοπίζει emails που περιέχουν ύποπτους συνδέσμους ή attachments, συσχετίζοντας πιθανές επιθέσεις phishing με συγκεκριμένους χρήστες.

Πλατφόρμα για Hunting (Platform for Hunting): SIEM (Security Information and Event Management): Συλλέγει και συσχετίζει logs από όλα τα παραπάνω συστήματα. Παρέχει ειδοποιήσεις όταν ανιχνεύεται suspicious behavior. **Security Analytics Platform:** Αναλύει patterns, anomalies και trends, βοηθώντας στον εντοπισμό phishing campaigns που στοχεύουν πολλούς χρήστες.

Δεδομένα για Ανάλυση και Εμπλουτισμό (Analysis & Enrichment Data):

- **DNSTwist:** Ελέγχει για typosquatting domains που μοιάζουν με το εταιρικό domain.
- **Phishing Domain List / Threat Intelligence Feeds:** Παρέχουν λίστες γνωστών phishing domains και υποδομών επίθεσης.
- **VirusTotal / HybridAnalysis:** Αναλύουν URLs ή attachments για malware, phishing ή suspicious behavior.
- **URL / Domain Sandbox Analysis:** Εκτελεί το URL σε ασφαλές περιβάλλον και παρακολουθεί τη συμπεριφορά του (downloads, redirections, exploits).

Πώς αξιοποιούνται τα εργαλεία και οι διαδικασίες (Τεχνική Ανάλυση):

1. **Ανίχνευση μέσω DNS & Proxy Logs:** Συσχετισμός DNS queries με γνωστά phishing domains. Παράδειγμα: Έλεγχος αν ο χρήστης επισκέφτηκε το paypal.com αντί για το paypal.com (typosquatting).
2. **Ανάλυση Email & Mail Security Gateway Logs:** Αναγνώριση suspicious emails με links ή attachments. Παράδειγμα: Email από εξωτερικό sender με domain που μιμείται το corporate domain και URL προς malicious site.
3. **Enrichment με Threat Intelligence Feeds:** Συγκρίνεται το URL ή domain με λίστες phishing. Παράδειγμα: Αν το example-login.com είναι σε threat feed, trigger alert.
4. **Sandbox Testing:** Αυτόνομη εκτέλεση του URL ή attachment σε sandbox για ανάλυση συμπεριφοράς. Παράδειγμα: Εντοπισμός ότι το URL κάνει drive-by download malware ή keylogger.
5. **Sysmon / SIEM Correlation:** Συσχετισμός download αρχείων ή suspicious process creation με προηγούμενη επίσκεψη σε phishing site. Παράδειγμα: Μετά την επίσκεψη του site, δημιουργείται διεργασία powershell.exe που κατεβάζει exe από C2 server → πιθανή επίθεση.

Συνοπτικά: Ο συνδυασμός logging, threat intelligence, sandbox analysis και SIEM correlation επιτρέπει Έγκαιρη ανίχνευση phishing attacks. Αποτροπή πρόσβασης σε κακόβουλους ιστότοπους. Εντοπισμό πιθανών επιθέσεων malware / credential theft μετά την επίσκεψη σε phishing site.

Hypothesis 2: Ο χρήστης κατεβάζει κακόβουλο αρχείο μετά την επίσκεψη σε κακόβουλο ιστότοπο (πιθανό Drive-by Download): Μετά την επίσκεψη σε έναν κακόβουλο ιστότοπο, ένας χρήστης μπορεί να κατεβάσει ακούσια κακόβουλο αρχείο (drive-by download), το οποίο μπορεί να εγκαταστήσει malware, ransomware, keylogger ή να προσπαθήσει να αποκτήσει credentials. Η επίθεση μπορεί να είναι αόρατη, χωρίς να απαιτείται ενεργή συμμετοχή του χρήστη πέρα από την επίσκεψη στον ιστότοπο.

Πηγές Δεδομένων για Hunting (Data Sources): **Passive DNS / DNS Server Log:** Ανίχνευση requests προς γνωστά ή ύποπτα domains που συνδέονται με drive-by downloads. **Proxy Log / NGFW Log:** Καταγραφή downloads ή access requests προς κακόβουλα URLs. **Sysmon Log:** Καταγραφή δημιουργίας αρχείων, διεργασιών και network connections που σχετίζονται με το κακόβουλο αρχείο.

Πλατφόρμα για Hunting (Platform for Hunting): **SIEM:** Συλλογή, correlation και alerting σε ύποπτες ενέργειες κατεβάσματος αρχείων. **Security Analytics Platform:** Εντοπισμός patterns drive-by downloads, αναγνώριση επαναλαμβανόμενων κινδύνων και συσχετισμός με προηγούμενα phishing incidents.

Δεδομένα για Ανάλυση και Εμπλουτισμό (Analysis & Enrichment Data): **Threat Intelligence Feeds:** Αναγνωρίζουν κακόβουλα domains και IPs. **Alexa Top 1M Domains:** Επιτρέπει σύγκριση με γνωστά δημοφιλή sites για να εντοπιστούν typosquatting domains ή newly registered domains. **VirusTotal / HybridAnalysis:** Σάρωση και ανάλυση των αρχείων για malware. **URL / Domain Sandbox Analysis:** Εκτέλεση URL σε ασφαλές περιβάλλον για να παρατηρηθεί behavior (downloads, payloads, connections). **Blacklisted Domain Checker:** Ελέγχει αν το domain είναι γνωστό κακόβουλο.

Πώς αξιοποιούνται τα εργαλεία και οι διαδικασίες (Τεχνική Ανάλυση):

- **DNS & Proxy Analysis:** Εντοπισμός αιτημάτων σε domains με drive-by downloads. Παράδειγμα: Ο χρήστης επισκέπτεται malicious-downloads.com και κατεβάζεται αυτόματα .exe αρχείο.
- **Sysmon Monitoring:** Ανίχνευση δημιουργίας αρχείων σε temp directories ή χρήστη (C:\Users\<User>\AppData\Local\Temp) μετά από επίσκεψη site. Παράδειγμα: Δημιουργία αρχείου random.exe και εκκίνηση powershell.exe για εκτέλεση.
- **Sandbox / VirusTotal / HybridAnalysis:** Ανάλυση του αρχείου για κακόβουλη συμπεριφορά (dropping payloads, C2 connections).
- **Threat Intelligence & Domain Checks:** Συγκρίνεται το domain με blacklists ή newly registered suspicious domains. Παράδειγμα: Domain βρίσκεται σε blacklist → SIEM trigger alert.
- **SIEM Correlation:** Συσχέτιση DNS/Proxy logs με sysmon events για να επιβεβαιωθεί ότι το download συνδέεται με συγκεκριμένη επίσκεψη. Παράδειγμα: Αντιστοιχία μεταξύ request προς malicious-downloads.com και τοπικού αρχείου random.exe → δημιουργία alert.

Συνοπτικά: Η διαδικασία αυτή επιτρέπει: Έγκαιρη ανίχνευση drive-by downloads. Σύλληψη και απομόνωση κακόβουλων αρχείων πριν εκτελεστούν. Προστασία των χρηστών από malware και credential theft.

Hypothesis 3: Εκτέλεση Malware στο σύστημα του χρήστη μετά το κατέβασμα: Μετά από την επιτυχή λήψη κακόβουλου αρχείου (π.χ. μέσω phishing ή drive-by download), το malware μπορεί να εκτελεστεί στο σύστημα του χρήστη. Η εκτέλεση μπορεί να προκαλέσει παραβιάσεις όπως κλοπή credentials, ransomware attacks, persistence, lateral movement ή άλλα κακόβουλα activities.

Πηγές Δεδομένων για Hunting (Data Sources): Prefetch / Shimcache / Amcache: Καταγράφουν πρόσφατα εκτελεσμένα προγράμματα και αρχεία, βοηθώντας στον εντοπισμό malware που τρέχει ή έχει τρέξει. **Process Running / Volatile Data (Memory):** Παρακολούθηση ενεργών διεργασιών και δεδομένων μνήμης για ύποπτη συμπεριφορά. **Sysmon:** Καταγραφή δημιουργίας διεργασιών, parent-child relationships, network connections. **Auditd (Linux):** Ανίχνευση εκτέλεσης νέων processes και πρόσβασης σε κρίσιμα αρχεία.

Πλατφόρμα για Hunting (Platform for Hunting): SIEM / Security Analytics Platform: Ανάλυση logs και correlation events για εντοπισμό malware execution patterns. **EDR (Endpoint Detection & Response):** Πραγματικός χρόνος monitoring και alerting για εκτελούμενα κακόβουλα binaries.

Δεδομένα για Ανάλυση και Εμπλουτισμό (Analysis & Enrichment Data): File Hash of Executed Process: Ανάλυση για γνωστό malware (hash lookup σε VirusTotal, internal database). **Parent-Child Process Analysis:** Αναγνώριση suspicious process trees, π.χ. ένα web browser που εκτελεί cmd.exe ή powershell.exe. **Folder Location of Executables:** Κακόβουλα αρχεία συχνά τρέχουν από temp directories ή χρήστη. **Signed Binary Check:** Ελέγχει αν το εκτελέσιμο έχει έγκυρη ψηφιακή υπογραφή. **VirusTotal / HybridAnalysis:** Αναλύουν το binary για malicious behavior ή malware indicators.

Πώς αξιοποιούνται τα εργαλεία και οι διαδικασίες (Τεχνική Ανάλυση):

1. **Prefetch / Shimcache / Amcache Analysis:** Εντοπισμός πρόσφατα εκτελεσμένων αρχείων σε μη συνηθισμένα paths (C:\Users\<User>\AppData\Local\Temp, C:\Windows\Temp). Παράδειγμα: random.exe εκτελέστηκε χωρίς user initiation → πιθανό malware.
2. **Process & Memory Monitoring:** Συσχέτιση διεργασιών με parent-child relationships. Παράδειγμα: explorer.exe → powershell.exe → malicious.exe.
3. **EDR / SIEM Alerts:** Trigger alerts για νέα ή suspicious binaries που τρέχουν. Παράδειγμα: Ένα εκτελέσιμο χωρίς ψηφιακή υπογραφή που τρέχει από temp folder → alert.
4. **Hash & Threat Intelligence Check:** Ανίχνευση αν το εκτελέσιμο είναι γνωστό malware μέσω VirusTotal ή HybridAnalysis.
5. **Behavioral Analysis:** Ανάλυση σε sandbox ή live monitoring για suspicious network connections, registry modifications ή persistence mechanisms.

Συνοπτικά: Η διαδικασία αυτή επιτρέπει: Έγκαιρη ανίχνευση malware execution. Ανάλυση διεργασιών και parent-child trees για ανίχνευση lateral movement ή persistence. Εμπλουτισμένη ανάλυση με threat intelligence και hash lookup για γρήγορη απόκριση και αποτροπή περαιτέρω ζημιάς.

Hypothesis 4: Malware εκτελεί persistence mechanism στο μολυσμένο ή εκμεταλλευμένο σύστημα: Μετά την εκτέλεση στο σύστημα του χρήστη, το malware συχνά προσπαθεί να εγκατασταθεί μόνιμα (persistence) ώστε να συνεχίσει τη λειτουργία του ακόμα και μετά από επανεκκίνηση ή αποσύνδεση του χρήστη. Αυτό μπορεί να γίνει μέσω: Registry modifications, Startup services / folders, Scheduled tasks (Windows Task Scheduler), Cron jobs (σε Linux), ASEP (Auto Start Extensibility Points)

Πηγές Δεδομένων για Hunting (Data Sources): ASEP (Auto Start Extensibility Points): Σημεία αυτόματης εκκίνησης εφαρμογών στο σύστημα. **Registry:** Ειδικά κλειδιά όπως HKCU\Software\Microsoft\Windows\CurrentVersion\Run ή HKLM\Software\Microsoft\Windows\CurrentVersion\Run. **Startup Services & Folders:** Έλεγχος εκτελέσιμων αρχείων που τρέχουν κατά την εκκίνηση του συστήματος. **Task Scheduler / Cron Jobs:** Έλεγχος προγραμματισμένων εργασιών που μπορεί να εκτελούν malware.

Πλατφόρμα για Hunting (Platform for Hunting): SIEM / Security Analytics Platform: Ανάλυση και correlation logs για δημιουργία alerts σε suspicious persistence mechanisms. **EDR:** Παρακολούθηση real-time αλλαγών στο σύστημα και ανίχνευση persistence artifacts.

Δεδομένα για Ανάλυση και Εμπλουτισμό (Analysis & Enrichment Data): Signature Check / File Hash Check: Επαλήθευση εκτελέσιμων αρχείων για known malware. **Autoruns Sysinternals:** Αναλυτική επισκόπηση όλων των σημείων αυτόματης εκκίνησης. **Date of Creation:** Συγκριτική ανάλυση ημερομηνίας δημιουργίας αρχείων για ανίχνευση ύποπτων πρόσφατων αλλαγών.

Πώς αξιοποιούνται τα εργαλεία και οι διαδικασίες (Τεχνική Ανάλυση):

1. **Registry & ASEP Analysis:** Ανίχνευση νέων ή τροποποιημένων keys που δείχνουν malware persistence. Παράδειγμα: Ένα εκτελέσιμο στο HKCU\Software\Microsoft\Windows\CurrentVersion\Run που δεν ανήκει σε νόμιμο software.
2. **Startup Folder & Services:** Εντοπισμός executables σε non-standard locations που τρέχουν κατά την εκκίνηση. Παράδειγμα: C:\Users\<User>\AppData\Roaming\malicious.exe εκτελείται κατά boot.
3. **Task Scheduler / Cron Jobs:** Έλεγχος για scheduled tasks που εκτελούν αρχεία με ύποπτα ονόματα ή από temp directories. Παράδειγμα: Task που τρέχει powershell.exe -exec bypass -file C:\Temp\malware.ps1.
4. **File Hash & Signature Check:** Επαλήθευση αν το εκτελέσιμο είναι γνωστό malware ή unsigned binary. VirusTotal ή internal threat feeds για εμπλουτισμένη ανάλυση.
5. **SIEM Correlation:** Συνδυασμός δεδομένων από Registry, Task Scheduler, Prefetch, Sysmon για πλήρη εικόνα persistence. Παράδειγμα alert: "New autorun executable detected from non-standard path + unsigned binary + suspicious hash".

Συνοπτικά: Η διαδικασία αυτή επιτρέπει να: Εντοπίζουμε malware persistence mechanisms. Αποτρέπουμε μακροχρόνια παραμονή malware στο σύστημα. Συνδέουμε τεχνικά δεδομένα (hashes, autoruns, scheduled tasks) με threat intelligence για γρήγορη αντίδραση.

Υπόθεση (Hypothesis 5): Μετά την εκτέλεση και εγκατάσταση, το malware συχνά προσπαθεί να **επικοινωνήσει με τον Command and Control (C2) server** του επιτιθέμενου. Αυτή η επικοινωνία μπορεί να χρησιμοποιηθεί για: Απόσπαση ευαίσθητων δεδομένων, Λήψη νέων εντολών ή malware modules, Διατήρηση persistence και έλεγχο του συστήματος. Ο στόχος του hunting είναι να **εντοπίσουμε ασυνήθιστη δικτυακή δραστηριότητα που υποδεικνύει επικοινωνία με C2 servers**.

Πηγές Δεδομένων (Data Sources): **Netflow / Firewall Log / NGFW Log:** Ανάλυση ροών δικτύου και κανόνων firewall για επικοινωνία με ύποπτες IPs ή ports. **IDS / IPS Logs:** Ανίχνευση signatures γνωστών C2 patterns. **Proxy Logs:** Καταγραφή HTTP/HTTPS requests προς εξωτερικούς servers. **Full Packet Capture:** Βαθύτερη ανάλυση επικοινωνίας, payload inspection. **DNS Logs:** Έλεγχος για ύποπτα domain lookups ή DGA (Domain Generation Algorithm) domains.

Πλατφόρμα για Hunting (Platform for Hunting): **SIEM / Security Analytics Platform:** Συλλογή, correlation και alerting για ύποπτη επικοινωνία. **NDR (Network Detection & Response) / XDR:** Παρακολούθηση δικτύου σε πραγματικό χρόνο και ανίχνευση επιθέσεων.

Δεδομένα για Ανάλυση και Εμπλουτισμό (Analysis & Enrichment Data): **Date of Creation Domain:** Εντοπισμός νεοσύστατων domains που μπορεί να χρησιμοποιούνται για C2. **SSL Certificate Attribute Checks:** Έλεγχος μη έγκυρων ή self-signed πιστοποιητικών. **JA3 SSL Fingerprint:** Ταυτοποίηση ύποπτων SSL/TLS fingerprints για known malware. **GeolP Location Data:** Εντοπισμός επικοινωνιών με ασυνήθιστες ή υψηλού κινδύνου γεωγραφικές περιοχές. **Threat Intelligence Feeds:** Συγκρίσεις με blacklists IPs/domains που σχετίζονται με malware C2 servers.

Πως αξιοποιούνται τα εργαλεία και οι διαδικασίες (Τεχνική Ανάλυση)

1. **DNS & Network Analysis:** Αναγνώριση domains με ύποπτα μοτίβα ή DGA. Παράδειγμα: DNS queries για domain τύπου xj9q3kz.com από μη-γνωστό user process.
2. **Netflow / Firewall / Proxy Correlation:** Έλεγχος για connections προς non-standard ports ή ασυνήθιστες εξωτερικές IPs. Παράδειγμα: Outbound TCP traffic σε Port 443 αλλά με self-signed SSL certificate.
3. **JA3 SSL Fingerprinting:** Ταυτοποίηση γνωστών malware SSL fingerprints σε TLS connections. Παράδειγμα: Connection με JA3 hash που έχει συνδεθεί στο παρελθόν με malware families.
4. **Threat Intelligence Enrichment:** Cross-reference IPs/domains με TI feeds για άμεση αναγνώριση C2 servers. Παράδειγμα: Block ή alert για επικοινωνία με IP που βρίσκεται σε malware blacklist.
5. **Full Packet Capture / Deep Inspection:** Ανάλυση περιεχομένου επικοινωνίας για ανίχνευση commands ή data exfiltration.

Συνοπτικά: Η ανάλυση της δικτυακής επικοινωνίας επιτρέπει: Γρήγορο εντοπισμό malware C2 communication. Πρόληψη exfiltration ή further compromise. Σύνδεση δικτυακών ενδείξεων με threat intelligence για επαλήθευση και mitigation.

Υπόθεση (Hypothesis 6): Μετά την επιτυχή εκτέλεση του malware ή της κακόβουλης ενέργειας, ο **επιτιθέμενος προσπαθεί να εξάγει ευαίσθητα δεδομένα ή έγγραφα** από το θύμα προς τον **Command and Control (C2) server** του. Τύποι δεδομένων: έγγραφα Word/Excel/PDF, βάσεις δεδομένων, credentials, ή άλλα εμπιστευτικά αρχεία. Στόχος του hunting: **εντοπισμός ασυνήθιστης ή μη εξουσιοδοτημένης μεταφοράς δεδομένων σε εξωτερικούς servers.**

Πηγές Δεδομένων (Data Sources): Netflow / Firewall / NGFW Logs: Ανάλυση ροών για μεγάλα outbound data transfers ή connections σε ύποπτους hosts. **IDS / Proxy Logs:** Ανίχνευση ανωμαλιών σε HTTP/HTTPS/SFTP/FTP επικοινωνίες. **Full Packet Capture:** Εξαγωγή λεπτομερών στοιχείων μεταφερόμενων αρχείων. **DNS Logs:** Έλεγχος για domains που χρησιμοποιούνται αποκλειστικά για εξαγωγή δεδομένων ή DGA domains.

Πλατφόρμα για Hunting (Platform for Hunting): SIEM / Security Analytics Platform: Correlation μεταξύ δικτυακής ροής, DNS queries, και ανωμαλιών στο traffic. **NDR / XDR:** Παρακολούθηση δικτύου και endpoints για εκπομπή δεδομένων σε C2.

Δεδομένα για Ανάλυση και Εμπλουτισμό (Analysis & Enrichment Data): **Date of Creation Domain:** Ανάλυση νεοσύστατων domains που μπορεί να χρησιμοποιούνται για exfiltration. **SSL Certificate Attribute Checks:** Έλεγχος για self-signed ή ύποπτα SSL certs. **JA3 SSL Fingerprint:** Ταυτοποίηση γνωστών fingerprints που χρησιμοποιούνται από malware για C2/exfiltration. **GeolP Location Data:** Ανίχνευση μεταφοράς δεδομένων σε ασυνήθιστες ή υψηλού κινδύνου γεωγραφικές περιοχές. **Threat Intelligence Feeds:** Cross-check με blacklists IPs/domains γνωστών C2/exfil servers.

Τεχνική Αξιοποίηση & Παραδείγματα

1. **Network Traffic Analysis:** Εντοπισμός μεγάλων outbound flows προς άγνωστους ή ύποπτους hosts. Παράδειγμα: 500 MB TCP traffic σε νεοσύστατο domain abcd1234.info από μη-εξουσιοδοτημένο user process.
2. **Proxy / IDS Correlation:** Ανίχνευση ασυνήθιστων μεταφορών αρχείων μέσω HTTP/HTTPS/SFTP. Παράδειγμα: POST request με περιεχόμενο PDF προς domain που δεν ανήκει σε εταιρικό whitelist.
3. **JA3 SSL Fingerprinting & Cert Analysis:** Ταυτοποίηση SSL/TLS fingerprints που χρησιμοποιούνται από γνωστά malware families για C2/exfiltration. Παράδειγμα: Connection σε port 443 με self-signed certificate και JA3 hash συνδεδεμένο με malware C2.
4. **GeolP & Threat Intel Enrichment:** Ανάδειξη ασυνήθιστων destination locations και cross-check με threat intelligence feeds για known exfil servers.
5. **Full Packet Capture / Deep Inspection:** Ανάλυση περιεχομένου μεταφερόμενων αρχείων, π.χ., ανίχνευση ευαίσθητων documents (Word, PDF, Excel) που στέλνονται εκτός εταιρικού δικτύου.

Συνοπτικά: Με το Hypothesis 6, στόχος είναι να: Ανιχνεύσουμε **εξαγωγή ευαίσθητων δεδομένων** σε C2. Προλάβουμε **data exfiltration ή leak**. Συνδέσουμε δικτυακές ενδείξεις με threat intelligence για **άμεσο mitigation**.

Υπόθεση (Hypothesis 7): Μετά την επιτυχή εξαγωγή ευαίσθητων δεδομένων (Hypothesis 6), υπάρχει πιθανότητα τα δεδομένα να διαρρεύσουν ή να δημοσιευθούν στο **Internet**, σε **Dark Web forums**, **paste sites** ή **code repositories**. Στόχος του hunting: **εντοπισμός ευαίσθητων δεδομένων που έχουν ήδη διαρρεύσει**, ώστε να προληφθεί περαιτέρω διάδοση ή κακόβουλη χρήση.

Πηγές Δεδομένων (Data Sources): OSINT: Αναζήτηση σε δημόσιες πηγές για διαρρεύσαντα credentials, αρχεία ή πληροφορίες. **Dark Web / Underground Forums:** Παρακολούθηση forums όπου οι επιτιθέμενοι μοιράζονται ή πωλούν stolen data. **Threat Intelligence Feeds:** Alerts για leaked data, compromised accounts ή exposed sensitive files.

Πλατφόρμα για Hunting (Platform for Hunting): Threat Intelligence Platform: Συλλογή, ανάλυση και correlation πληροφοριών από OSINT, Dark Web, forums, και feeds.

Δεδομένα για Ανάλυση και Εμπλουτισμό (Analysis & Enrichment Data): Pastebin / GitHub: Έλεγχος για ανεπιθύμητη δημοσίευση credentials ή ευαίσθητων αρχείων. **Honeypot:** Ανάλυση πιθανών leaks ή malware samples που εμφανίζονται σε controlled fake assets.

Τεχνική Αξιοποίηση & Παραδείγματα

1. **OSINT & Dark Web Search:** Παρακολούθηση αναφορών για leaked data. Παράδειγμα: Αναφορά σε forum για διαρροή εταιρικών passwords με συγκεκριμένο domain name.
2. **Monitoring Paste Sites & Code Repositories:** Ανίχνευση credentials ή sensitive information σε Pastebin, GitHub, GitLab. Παράδειγμα: Public gist σε GitHub που περιέχει API keys ή internal database connection strings.
3. **Threat Intelligence Correlation:** Εμπλουτισμός με feeds που αναφέρουν compromised accounts ή breached data sets. Παράδειγμα: Feed ενημερώνει για leaked customer records που αντιστοιχούν σε internal database hashes.
4. **Honeypot Detection:** Δημιουργία ελεγχόμενων φακέλων ή accounts με fake sensitive data. Παρατήρηση αν τα honeypot στοιχεία εμφανιστούν σε forums ή paste sites, δείχνοντας πιθανή εξαγωγή.

Συνοπτικά: Με το Hypothesis 7, στόχος είναι: **Να ανιχνεύσουμε αν τα ευαίσθητα δεδομένα έχουν διαρρεύσει** στο Internet ή στο Dark Web. **Να ενεργοποιήσουμε incident response** για mitigation, password resets, ή ειδοποίηση stakeholders. Συνδυάζεται με προηγούμενα Hypotheses (1–6) για πλήρη **αλυσίδα επίθεσης από phishing μέχρι data leak**.
