Corfu

Ψηφιακή Εγκληματολογία και Αναγνώριση Απειλών: Ανάλυση Δικτυακών Αποδεικτικών Στοιχείων

Dr. Stylianos Karagiannis (PhD)
Ionian University, Corfu, Greece

NMS.LAB

IONIAN UNIVERSITY

DEPARTMENT OF INFORMATICS
IONIAN UNIVERSITY

</> Stylianos Karagiannis

Corfu, Kozani, Greece Lisbon, Portugal

PhD in Cybersecurity - Post Doc @ Ionian University Department of Informatics, Corfu, Greece
Senior Researcher @ PDMFC, Lisbon, Portugal

Research Interests: Cybersecurity, Privacy, Capture The Flag (CTF) Challenges, Cyber Ranges
Gamification, Incident Handling, Virtual Labs, Game-Based Learning
Social Constructivism, Learning Theories

Email: skaragiannis@ionio.gr, LinkedIn, NMSLab

Συλλογή Δικτυακών Αποδεικτικών Στοιχείων

Η δικτυακή δραστηριότητα αφήνει ίχνη στα πρωτόκολλα και στις συνδέσεις. Η ανάλυσή τους επιτρέπει την αναγνώριση ύποπτων ενεργειών και τον εντοπισμό επιτιθέμενων.

- **Firewall & Proxy Logs:** Τα αρχεία καταγραφής από firewalls και proxies δείχνουν προσπάθειες σύνδεσης και ύποπτη κίνηση. Παρέχουν στοιχεία για αρχική και συνεχή επικοινωνία των αντιπάλων.
- **NetFlow:** Το NetFlow καταγράφει μεταδεδομένα επικοινωνιών (IP, θύρες, διάρκεια). Χρησιμοποιείται για παρακολούθηση ροών δεδομένων και εντοπισμό ύποπτης δραστηριότητας σε περιστατικά.
- **Packet Captures:** Οι καταγραφές πακέτων είναι από τις πιο ακριβείς πηγές στοιχείων. Αποκαλύπτουν exploits, command & control ή εξαγωγή δεδομένων, προσφέροντας σαφή εικόνα της επίθεσης.
- **Αναγνώριση & Σάρωση:** Οι επιτιθέμενοι χρησιμοποιούν αυτοματοποιημένα εργαλεία σάρωσης σε firewalls και routers. Οι απόπειρες αφήνουν ίχνη στα logs, αποκαλύπτοντας την εξωτερική υποδομή τους.
- **Αρχική Μόλυνση:** Η εισβολή ξεκινά με πολυσταδιακές εκμεταλλεύσεις και malware. Το πρώτο στάδιο επικοινωνεί με εξωτερικά URLs· στοιχεία εντοπίζονται σε firewall/proxy logs.
- **Πλευρική Κίνηση & C2:** Αφού διεισδύσουν, κινούνται πλευρικά με reconnaissance και εκμετάλλευση. Χρησιμοποιούν command & control, που ανιχνεύεται μέσω logs, packet captures και NetFlow.
- **Εξαγωγή Δεδομένων:** Συχνός στόχος είναι η μεταφορά δεδομένων εκτός δικτύου. Τα proxies δείχνουν προορισμούς, το NetFlow τις ροές, ενώ τα packet captures αποκαλύπτουν αρχεία και περιεχόμενο.

Firewall & Proxy Logs

 # Firewall (syslog)

```
Oct 12 08:14:22 fw1 kernel: DENY IN=eth0 OUT= MAC=00:0c:29:aa:bb:cc SRC=198.51.100.45 DST=10.8.5.23 LEN=60 TOS=0x00 PREC=0x00 TTL=50 ID=54321 DF PROTO=TCP SPT=34567 DPT=22 WINDOW=29200 RES=0x00 SYN URGP=0
```

- **Περιγραφή:** Το firewall εντόπισε εισερχόμενη σύνδεση από εξωτερική IP (198.51.100.45) προς εσωτερικό σύστημα (10.8.5.23) στη θύρα 22 (SSH). Το πακέτο είχε TCP σημαία SYN, δείχνοντας προσπάθεια έναρξης σύνδεσης. Η πολιτική ασφαλείας απέρριψε την προσπάθεια (DENY). Πρόκειται πιθανότατα για απόπειρα σάρωσης θυρών (port scan) ή brute-force SSH. Εάν παρατηρηθεί επαναλαμβανόμενα ή από πολλές IP, υποδεικνύει αυτοματοποιημένο εργαλείο αναγνώρισης (scanner). Ενέργεια: Προσθήκη IP σε blacklist.Ενεργοποίηση IDS/IPS κανόνων για Nmap ή masscan signatures.Έλεγχος για άλλες απόπειρες προς ευαίσθητες θύρες (RDP, SMB, 3389, 445).

 # Firewall (stateful allow)

```
2025-10-12T08:14:22Z fw1 policy=allow src=203.0.113.45:443 dst=10.8.5.23:49212 proto=TCP session_id=0x7fa2 action=accept bytes=15324 duration=00:01:02
```

- **Περιγραφή:** Εξερχόμενη TCP σύνδεση από εσωτερικό host (10.8.5.23) σε εξωτερικό server (203.0.113.45) στη θύρα 443 (HTTPS).Η πολιτική του firewall επέτρεψε τη σύνδεση και κατέγραψε διάρκεια και όγκο δεδομένων. Συνήθως πρόκειται για κανονική web επικοινωνία χρήστη ή εφαρμογής. Ωστόσο, αν η IP ή το domain δεν είναι γνωστό, μπορεί να υποδεικνύει command & control (C2) σύνδεση μετά από μόλυνση. **Ενέργεια:** Έλεγχος IP/domain σε threat intelligence feeds.Ανάλυση συμπεριφοράς ροής (π.χ. επαναλαμβανόμενες μικρές ροές ανά 60 sec → beaconing).Επιβεβαίωση με proxy ή endpoint logs.

Firewall & Proxy Logs

 # Proxy (Squid combined)
2025-10-12T08:14:24.123 proxy1 TCP_MISS/200 153240 GET http://malicious.example/payload.exe - HIER_DIRECT/198.51.100.77 application/octet-stream 0 0.453 "curl/7.68.0“

- **Περιγραφή:** Το proxy καταγράφει αίτημα GET για λήψη αρχείου .exe από domain malicious.example.Ο client χρησιμοποιεί εργαλείο γραμμής εντολών (curl), όχι browser.Ο server απάντησε με HTTP 200 και τύπο αρχείου application/octet-stream.Ερμηνεία:Πρόκειται για ύποπτη λήψη εκτελέσιμου αρχείου, πιθανό malware payload.Συνήθως αποτελεί πρώτο στάδιο μόλυνσης (initial compromise).Η χρήση curl ή wget συχνά υποδηλώνει αυτοματοποιημένο script.Ενέργεια:Εξαγωγή URL και hash αρχείου για sandboxing/ανάλυση.Εντοπισμός endpoint που εκτέλεσε το αίτημα.Έλεγχος εάν ακολούθησαν επικοινωνίες HTTPS ή DNS με τον ίδιο domain.

 # Proxy (HTTP auth + cache hit)
2025-10-12T09:02:11 proxy1 TCP_HIT/304 512 GET http://updates.corp/internal/patch.zip user1 HIER_DIRECT/10.0.0.5 - 0 0.031 "Mozilla/5.0«

- **Περιγραφή:** Ο proxy δείχνει αίτημα από τον χρήστη user1 προς εσωτερικό web server (updates.corp).Η απάντηση ήταν 304 Not Modified, που σημαίνει ότι το αντικείμενο υπήρχε ήδη στην cache (TCP_HIT). Πρόκειται για συνηθισμένο αίτημα ενημέρωσης (patch). Κανονική, εσωτερική δραστηριότητα στο εταιρικό δίκτυο. Δεν δείχνει κακόβουλη συμπεριφορά· μπορεί να χρησιμοποιηθεί ως baseline για κανονική κυκλοφορία. **Ενέργεια:** Καμία ενέργεια απαιτείται.Χρήσιμο για μοντέλα ανωμαλιών (anomaly detection) – βοηθά να ξεχωρίζουν νόμιμες από ύποπτες ροές.

NetFlow / IPFIX


```
# NetFlow line (CSV-like)
2025-10-12T08:10:00,10.8.5.23,198.51.100.7,49212,443,6,125434,134,300
# meaning: time,src,dst,sport,dport,proto,bytes,pkts,duration(sec)

2025-10-12T22:13:05,10.8.5.45,203.0.113.77,44444,8080,6,1048576,10240,2700

2025-10-12T07:55:12,192.168.1.100,198.51.100.9,39012,53,17,512,4,1
# (many small UDP DNS queries – possible exfil or high-frequency beacons)

2025-10-13T02:05:00,10.8.5.23,198.51.100.7,49230,443,6,98304,210,600
```

- Το **10.8.5.23 → 198.51.100.7 (TCP/443)** διατηρεί επαναλαμβανόμενες HTTPS συνδέσεις.
- Το **10.8.5.45 → 203.0.113.77 (TCP/8080)** μεταφέρει μεγάλο όγκο δεδομένων σε μία μακρά συνεδρία.
- Το **192.168.1.100 → 198.51.100.9 (UDP/53)** στέλνει συνεχή DNS αιτήματα.

Packet Captures / tcpdump


```
# tcpdump -nn -ttt summary
08:14:24.123456 IP 10.8.5.23.49212 > 198.51.100.77.443: Flags [P.], seq 1:512 ack 1, win 64240, length 511
<contains TLS ClientHello SNI: "malicious.example">

09:12:01.123789 IP 10.8.5.23.49212 > 198.51.100.7.443: Flags [P.], seq 1:1024 ack 1, length 1023
<HTTP over TLS: POST /api/v1/upload Content-Length: 204800>

07:55:13.456012 IP 45.77.23.9.31337 > 192.168.1.10.22: Flags [S], seq 0, win 64240, length 0
07:55:13.456078 IP 45.77.23.9.31338 > 192.168.1.10.23: Flags [S], seq 0, win 64240, length 0
# (series of SYNs to sequential ports — scanning)

22:05:40.987654 IP 10.8.5.23.54321 > 198.51.100.7.53: 12345+ A? exfil.example. (64)
# (large DNS query with long payload-like name)
```

Ο εσωτερικός υπολογιστής **10.8.5.23** φαίνεται να έχει ενεργή και ύποπτη επικοινωνία με τον εξωτερικό **198.51.100.7** μέσω **TLS (TCP/443)**. Το πρώτο πακέτο δείχνει **ClientHello** προς το domain **malicious.example**, δηλαδή ξεκάθαρη απόπειρα σύνδεσης σε κακόβουλο HTTPS server. Αργότερα, από τον ίδιο host και την ίδια σύνδεση, φαίνεται **HTTP POST αίτημα μέσα στο TLS** προς `/api/v1/upload` με μεγάλο `Content-Length (≈200 KB)`, που σημαίνει **ανέβασμα δεδομένων** προς τον εξωτερικό server — πρακτικά **εξαγωγή αρχείων ή πληροφοριών**.

Παράλληλα, ο εξωτερικός host **45.77.23.9** στέλνει **σειρά SYN πακέτων** προς **192.168.1.10** στις **θύρες 22 και 23** (SSH και Telnet), κάτι που αποτελεί **σάρωση θυρών** (port scan) για εύρεση ανοιχτών υπηρεσιών.

Τέλος, ο **10.8.5.23** στέλνει **DNS ερώτημα (UDP/53)** προς **198.51.100.7** με όνομα `exfil.example.` που έχει **μεγάλο και ασυνήθιστο payload**, δείχνοντας πιθανή **εξαγωγή δεδομένων μέσω DNS (DNS exfiltration)**.

Αναγνώριση & Σάρωση (recon / IDS)


```
# IDS / Suricata alert (eve.json style)
{"timestamp":"2025-10-
12T07:55:13.456","event_type":"alert","src_ip":"45.77.23.9","src_port":31337,"dest_ip":"192.168.1.10","dest_port":22,"alert":{"signatu
re_id":2000001,"signature":"ET SCAN Nmap Scripting Engine User-Agent","severity":2}}

# Firewall log marking port-scan
2025-10-12 07:55:12 fw1: port-scan detected src=45.77.23.9 dst=192.168.1.0/24 count=120 threshold=100 action=drop

# Zeek/conn.log style
<2025-10-12T07:55:12.456> 45.77.23.9 192.168.1.10 31337 22 tcp 120 0 0 S 0.001 0.000 - - - - - - - -

# Webserver access logs showing mass probing
2025-10-12T10:20:01 GET /wp-login.php 200 512 "-" "Mozilla/5.0 (compatible; mass-scanner/1.0)" src=203.0.113.88
```

- Ο εξωτερικός υπολογιστής **45.77.23.9** εκτελεί **σάρωση θυρών (port scan)** στο εσωτερικό δίκτυο **192.168.1.0/24**, προσπαθώντας να συνδεθεί κυρίως στη **θύρα 22 (SSH)**. Το Suricata IDS το αναγνωρίζει ως **“ET SCAN Nmap Scripting Engine”**, επιβεβαιώνοντας ότι πρόκειται για αυτοματοποιημένο εργαλείο αναγνώρισης. Το firewall επίσης καταγράφει πάνω από **120 προσπάθειες σύνδεσης**, τις οποίες **μπλόκαρε**.
- Το Zeek log δείχνει τις ίδιες προσπάθειες (SYN πακέτα χωρίς απάντηση), που σημαίνει ότι η σάρωση εντοπίστηκε αλλά **δεν υπήρξε επιτυχής πρόσβαση**.
- Παράλληλα, άλλος εξωτερικός host **203.0.113.88** πραγματοποιεί **μαζικές HTTP αιτήσεις** προς τη σελίδα **/wp-login.php** με user-agent mass-scanner/1.0, κάτι που αποτελεί **προσπάθεια εύρεσης ή δοκιμής ευπάθειας σε WordPress**.

Αρχική Μόλυνση (initial compromise)


```
# Email gateway (smtp proxy)
2025-10-12T06:48:22 mailgw msg_id=abc123 from=badguy@external.example to=victim@corp.com subject="Invoice"
attachment="Invoice_2025.zip" verdict=allowed reason=signature-miss

# Endpoint AV
2025-10-12T07:05:11 endpoint1 AV: Trojan:Win32/Generic detected file="C:\Users\victim\Downloads\Stage1.exe" sha256=abcd...
action=quarantine

# Proxy (download event)
2025-10-12T07:04:59 proxy1 TCP_MISS/200 41234 GET http://dropbox.malicious/Stage1.exe - HIER_DIRECT/198.51.100.77 - 0 0.389
"Mozilla/5.0"

# Sysmon (process create) on endpoint
2025-10-12T07:05:12 Sysmon EventID=1 Image="C:\Users\victim\Downloads\Stage1.exe" CommandLine="C:\Users\victim\Downloads\Stage1.exe -
install" ParentImage="C:\Windows\explorer.exe" User="CORP\victim"
```

- Τι έγινε: ο χρήστης **victim@corp.com** έλαβε μήνυμα (msg_id=**abc123**) και κατέβασε/έτρεξε το **Stage1.exe** από dropbox.malicious (**198.51.100.77**). Το AV το εντόπισε και το καραντίναρε.
- IOCs: badguy@external.example, msg_id=abc123, Stage1.exe (sha256=abcd...), 198.51.100.77, domain dropbox.malicious.
- Άμεσα βήματα (το πολύ 3): 1) **Απομόνωσε** αμέσως το endpoint (endpoint1). 2) **Σώσε logs & PCAPs** (mailgw, proxy, Sysmon, AV). 3) **Μπλόκαρε** IP/domain στο firewall/proxy και άλλαξε credentials του χρήστη.

Πλευρική Κίνηση & Command & Control (lateral movement & C2)


```
# Email gateway (smtp proxy)
2025-10-12T06:48:22 mailgw msg_id=abc123 from=badguy@external.example to=victim@corp.com subject="Invoice"
attachment="Invoice_2025.zip" verdict=allowed reason=signature-miss

# Endpoint AV
2025-10-12T07:05:11 endpoint1 AV: Trojan:Win32/Generic detected file="C:\Users\victim\Downloads\Stage1.exe" sha256=abcd...
action=quarantine

# Proxy (download event)
2025-10-12T07:04:59 proxy1 TCP_MISS/200 41234 GET http://dropbox.malicious/Stage1.exe - HIER_DIRECT/198.51.100.77 - 0 0.389
"Mozilla/5.0"

# Sysmon (process create) on endpoint
2025-10-12T07:05:12 Sysmon EventID=1 Image="C:\Users\victim\Downloads\Stage1.exe" CommandLine="C:\Users\victim\Downloads\Stage1.exe -
install" ParentImage="C:\Windows\explorer.exe" User="CORP\victim"
```

Ο χρήστης **victim@corp.com** έλαβε e-mail (msg_id=`abc123`) με συνημμένο `Invoice_2025.zip` από `badguy@external.example`. Το μήνυμα πέρασε από το gateway (verdict=allowed) επειδή οι υπογραφές δεν το εντόπισαν. Ο χρήστης κατέβασε το `Stage1.exe` από `http://dropbox.malicious/Stage1.exe` (IP **198.51.100.77**) μέσω του proxy, και στη συνέχεια το εκτέλεσε (Sysmon process create — `Stage1.exe -install`, εκτελέστηκε από `explorer.exe` με χρήστη `CORP\victim`). Το endpoint AV εντόπισε το αρχείο ως **Trojan:Win32/Generic** (sha256=`abcd...`) και το έβαλε σε καραντίνα λίγα δευτερόλεπτα/λεπτά μετά — αυτό σημαίνει ότι υπήρξε εκτέλεση του κακόβουλου προγράμματος αλλά ο AV φάνηκε να περιορίζει ή να αποκόπτει το συγκεκριμένο αρχείο.

Πλευρική Κίνηση & Command & Control (lateral movement & C2)

Τι σημαίνει σε επίπεδο κινδύνου

Υπήρξε επιτυχημένη παράδοση και εκτέλεση αρχείου — άρα υπάρχει ρεαλιστικός κίνδυνος ότι το malware πρόλαβε να κάνει ενέργειες (π.χ. φόρτωση δεύτερου σταδίου, δημιουργία persistence, κλήσεις σε C2, εξαγωγή στοιχείων).
Το γεγονός ότι το AV έκανε quarantine μειώνει τον κίνδυνο αλλά **δεν εξαφανίζει** την πιθανότητα ότι εντολές/αρχεία δημιουργήθηκαν ή ότι credentials υπερπροβλήθηκαν.

Η αλυσίδα δείχνει phishing → download → execution → ανίχνευση, επομένως απαιτείται forensics και containment.

Συγκεκριμένα IOCs (για γρήγορο blocking/αναζήτηση)
`badguy@external.example`, `msg_id=abc123`, `Stage1.exe` (sha256=abcd...), `dropbox.malicious`, `198.51.100.77`, `C:\Users\victim\Downloads\Stage1.exe`.

Πλευρική Κίνηση & Command & Control (lateral movement & C2)

Σύντομα, προτεραιοποιημένα βήματα (εφαρμόστε τώρα)

- **Απομόνωση endpoint1**: αποσυνδέστε/απομονώστε δικτυακά το μηχάνημα.
- **Συλλογή αποδεικτικών**: εξάγετε και ασφαλίστε Sysmon events, AV quarantine file, πλήρες proxy entry (headers, referrer), mailgw full message (με headers & attachment), και τυχόν διαθέσιμα PCAPs για τη συνεδρία προς 198.51.100.77. Κάντε image μνήμης & δίσκου αν έχετε δυνατότητα.
- **Ταχεία αναζήτηση εξόδου C2**: ελέγξτε SIEM/NetFlow/IDS για εξερχόμενες συνδέσεις από το endpoint προς 198.51.100.77 ή άλλες άγνωστες IPs στο ίδιο διάστημα.
- **Μπλοκάρισμα & containment**: μπλοκάρετε IP `198.51.100.77` και domain `dropbox.malicious`, και μαρκάρετε/μπλοκάρετε αποστολέα `badguy@external.example` στο gateway.
- **Έλεγχος persistence & artifacts**: ψάξτε για scheduled tasks, νέα services, autorun registry keys, αρχεία σε %APPDATA%/Temp, και καταχωρήσεις στο startup.
- **Αλλαγή credentials & εποπτεία**: αναγκαστικό reset password για το χρήστη `victim`, έλεγχος πρόσβασης σε ευαίσθητα συστήματα και προσωρινή αυστηρή παρακολούθηση (MFA enforcement όπου είναι εφικτό).

Εξαγωγή Δεδομένων (data exfiltration)


```
# Proxy POST large upload
2025-10-12T22:13:05 proxy1 TCP_MISS/200 1048576 POST https://cloud-storage.example/upload user=victim bytes=1048576 time=5.231
"curl/7.68.0"

# NetFlow large outbound transfer
2025-10-12T22:13:05,10.8.5.23,203.0.113.77,49212,8443,6,2048000,4096,2700

# DNS tunnel fragments (DNS query log)
2025-10-12T21:58:03 dns1 QUERY src=10.8.5.23 qname="Y29udGVudF8xNjAwX2RhdGE=.exfil.example" type=TXT size=512
2025-10-12T21:58:04 dns1 QUERY src=10.8.5.23 qname="Y29udGVudF8xNjAxX2RhdGE=.exfil.example" type=TXT size=512

# PCAP summary showing HTTP upload with multipart
22:13:06.123456 IP 10.8.5.23.49212 > 198.51.100.77.8443: Flags [P.], seq 1:4097 ack 1, length 4096
<HTTPs (POST /upload) Content-Type: multipart/form-data; boundary=----WebKit... Content-Length: 2048000>
```

Τι βλέπουμε : Ο host **10.8.5.23** φορτώνει *μεγάλα* δεδομένα προς εξωτερικό cloud: proxy δείχνει `POST https://cloud-storage.example/upload` από χρήστη `victim` (bytes=1 048 576, `curl/7.68.0`). Το PCAP επιβεβαιώνει HTTPS POST `multipart/form-data` με `Content-Length: 2 048 000`. Το NetFlow την ίδια ώρα δείχνει μεγάλη εξερχόμενη ροή: **10.8.5.23 → 203.0.113.77, TCP/8443, bytes=2 048 000, pkts=4096, duration=2700s** — δηλαδή ολοκληρωμένη/μεγάλης κλίμακας εξαγωγή δεδομένων.

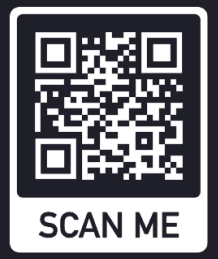
- Ταυτόχρονα, το DNS log δείχνει **σπασμένα/κατακερματισμένα TXT queries** από **10.8.5.23** προς `exfil.example` με ονόματα που μοιάζουν με base64 κομμάτια (`Y29udGVudF8x...`) — τυπικό pattern DNS tunneling / exfiltration μέσω TXT records.

Συμπέρασμα: Ο **10.8.5.23** πραγματοποιεί *συνδυασμένη* εξαγωγή δεδομένων — μεγάλος HTTPS upload σε `cloud-storage.example` (203.0.113.77:8443) **και** ταυτόχρονη εξαγωγή δεδομένων μέσω DNS TXT fragments προς `exfil.example` — δηλωμένη, ενεργή data-exfiltration.

NMSLab

Ευχαριστώ για την Προσοχή σας!

Dr. Stylianos Karagiannis, PhD



https://nmslab.di.ionio.gr