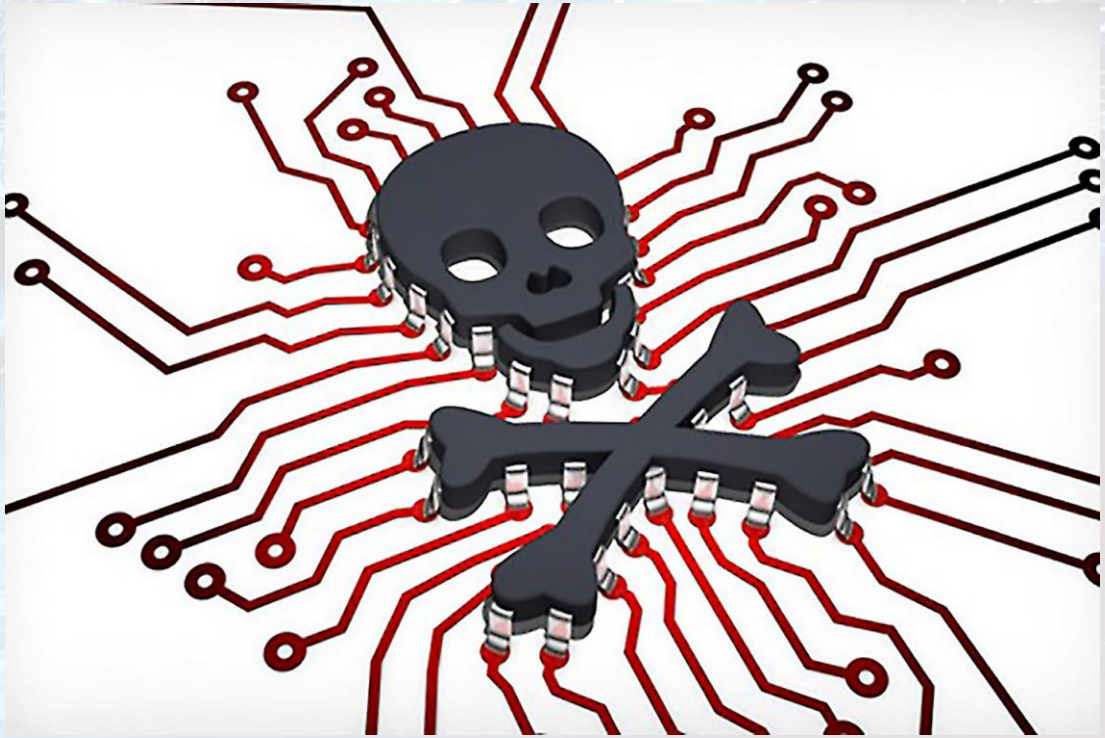
Petros Vassilikos
vassilikosp@gmail.com
pvasilikos@sch.gr

In this presentation

1. Cybersecurity – Smishing – Vishing – Phishing – Quishing
2. Security Awareness – tests – Εκπαιδευτικές Διαδικασίες
3. Σελίδες με live Επιθέσεις
4. SOC (**S**ecurity **O**perations **C**enter)
5. AI in SOC / Cybersecurity – IBM Watson
6. AI in Cybersecurity – Nvidia Morpheus
7. Βασικές υποδομές AI – DGX – HGX – GB200
8. Cryptography & Cybersecurity in Quantum Computer era

Cyber Threats

- Malware
- Phishing / Smishing / Vishing / Quishing
- Store (Harvest) Now, Decrypt Later
- Identity Theft
- Man-in-the-middle attack (MITM)
- Advance Persistence Threats
- Botnet – DDoS / Cryptojacking
- Data Manipulation / Destruction
- IoT-Based Attacks



Κύριοι άξονες ενεργειών για την προστασία έναντι των απειλών

NIST Cyber Security Framework - Domains

Identify	Protect	Detect	Respond	Recover
Αναγνώριση Ευπαθειών & κενών Ασφαλείας	Προστασία πόρων έναντι αναγνωρισμένων ευπαθειών	Έγκαιρη/Άμεση αναγνώριση επίθεσης	Δυνατότητα άμεσης αντίδραση σε επίθεση	Επανάκαμψη μετά από επίθεση

Threat Actor and Capabilities

Organized Criminals

Email account takeover

Phishing

Commodity Malware

Social Engineering

Credential Replay

'APT'-style Attacks

Hacktivists

Cyber Vandalism

DDoS

State-Sponsored

'APT'-style Attacks

Custom malware/exploits

Phishing

Insider

Unintentional (Error) or intentional Malicious)

Data Leakage

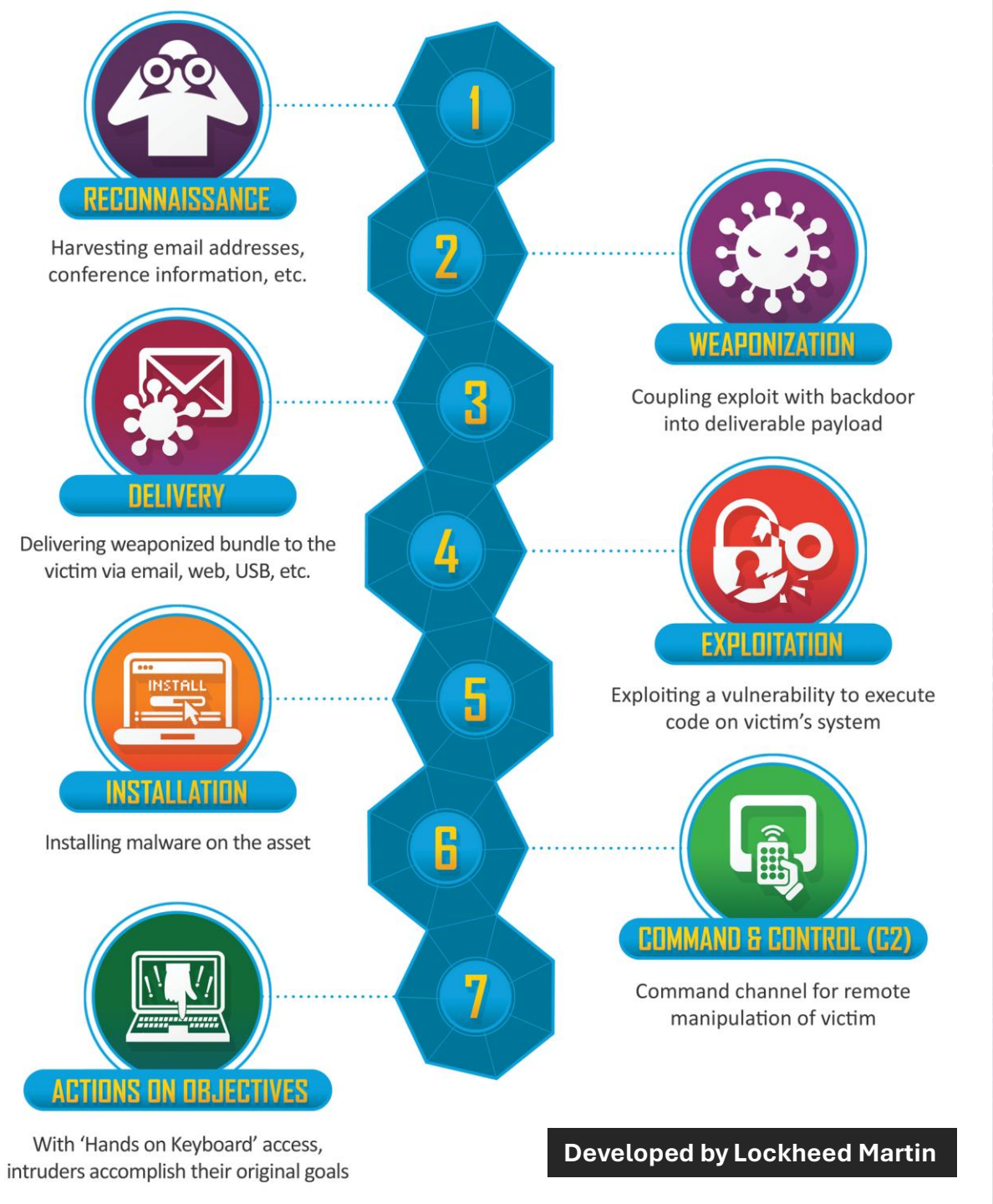
Credential Replay

Lost/Stolen IP

Μεθοδολογία επίθεσης (Kill Chain)

Developed by Lockheed Martin

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command and Control
7. Actions on Objectives



Social Engineering

Viber

WhatsApp

Telegram

Κοινωνική μηχανική (Social engineering) είναι η πράξη της προφορικής χειραγώγησης ατόμων με σκοπό την απόσπαση πληροφοριών. Αν και είναι παρόμοια με το τέχνασμα ή την απλή απάτη, ο όρος είναι κυρίως συνδεδεμένος με την εξαπάτηση ατόμων με σκοπό την απόσπαση εμπιστευτικών πληροφοριών που είναι απαραίτητες για την πρόσβαση σε κάποιο υπολογιστικό σύστημα

Bait Scenarios (δολώματα) . Προτροπή να καταβάσεις κάποιο καυτό βίντεο , συνήθως μέσα από τα Κοινωνικά Δίκτυα.

Θυμηθείτε:

- **Κινηθείτε αργά**. Οι scammers βασίζονται στο γεγονός ότι κάποιος πρώτα ενεργεί και μετα σκέφτεται
- **Μην ακολουθείτε** υπερσυνδεσμους
- **Η παραβίαση email είναι ανεξέλεγκτη**. Οι scammers παίρνουν τον έλεγχο και αποστέλλουν μέσα από “γνωστά” άτομα. Προσοχή στο περιεχόμενο
- Να είμαστε **καχύποπτοι** σε κάθε download

Phone Call:
This is John, the System Administrator. What is your password?

In Person:
What ethnicity are you? Your mother’s maiden name?

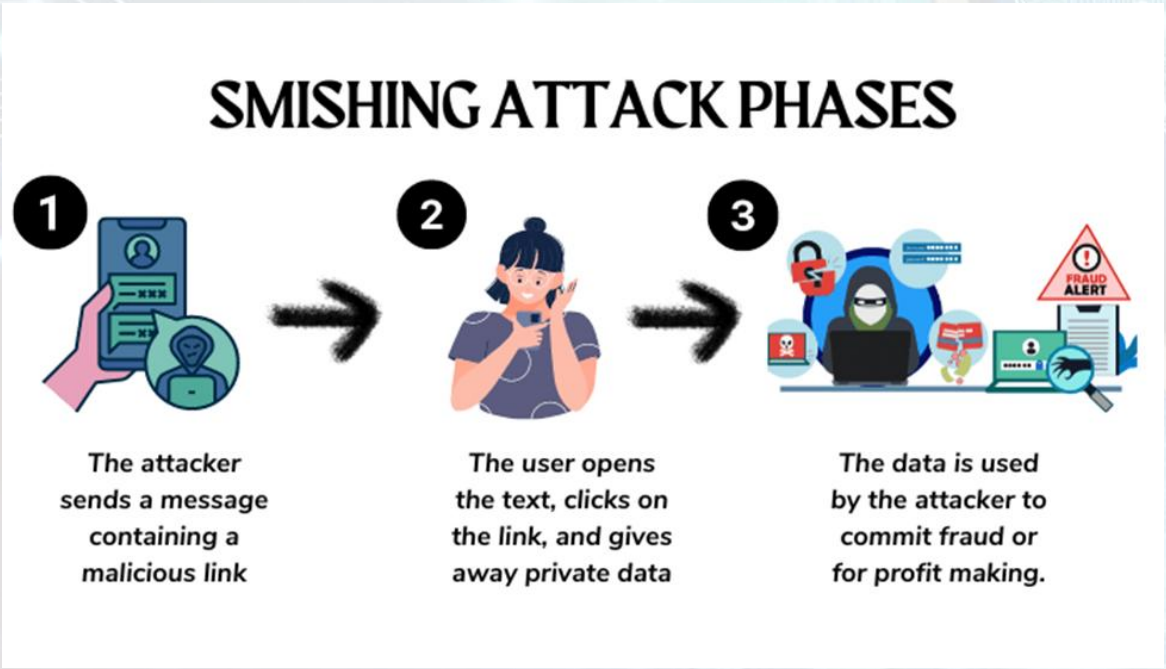
Email:
ABC Bank has noticed a problem with your account…

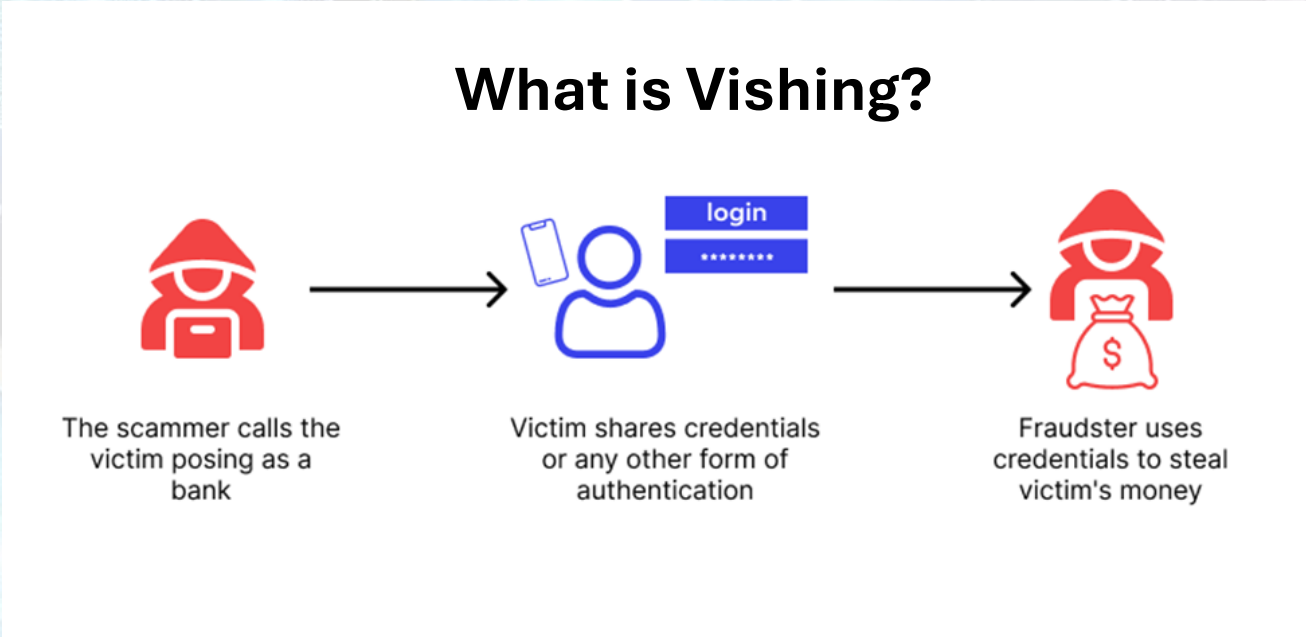
I have come to repair your machine…

and have some lovely software patches!

Phishing **vs** Smishing **vs** Vishing

Methods of Contact for Phishing, Smishing and Vishing	
Phishing	Email
Smishing	SMS/text message
Vishing	Phone, robocall, voicemail, voice over internet protocol (VoIP)





Phishing:

Scammers στέλνουν emails που μιμούνται αξιόπιστες πηγές, προκαλώντας άμεση δράση με επείγοντα μηνύματα. Τα θύματα οδηγούνται σε fake websites ή κατεβάζουν malicious attachments, κλέβοντας προσωπικά δεδομένα.

Tips:

- ✓ Ελέγξτε το sender’s email.
- ✓ Μην κλικάρετε απερίσκεπτα links ή attachments.
- ✓ Χρησιμοποιήστε anti-virus software.

Smishing:

Scammers στέλνουν SMS που υποδύονται τράπεζες ή υπηρεσίες, ζητώντας να κλικάρετε links ή να καλέσετε αριθμούς. Τα θύματα δίνουν προσωπικά δεδομένα ή κατεβάζουν malware.

Tips:

- ✓ Μην ανοίγετε links από άγνωστες πηγές.
- ✓ Επαληθεύστε τα αιτήματα μέσω επίσημων καναλιών.
- ✓ Χρησιμοποιήστε mobile security software.
- ✓ Αποκλεισμός 5-ψηφιων υψηλής χρέωσης

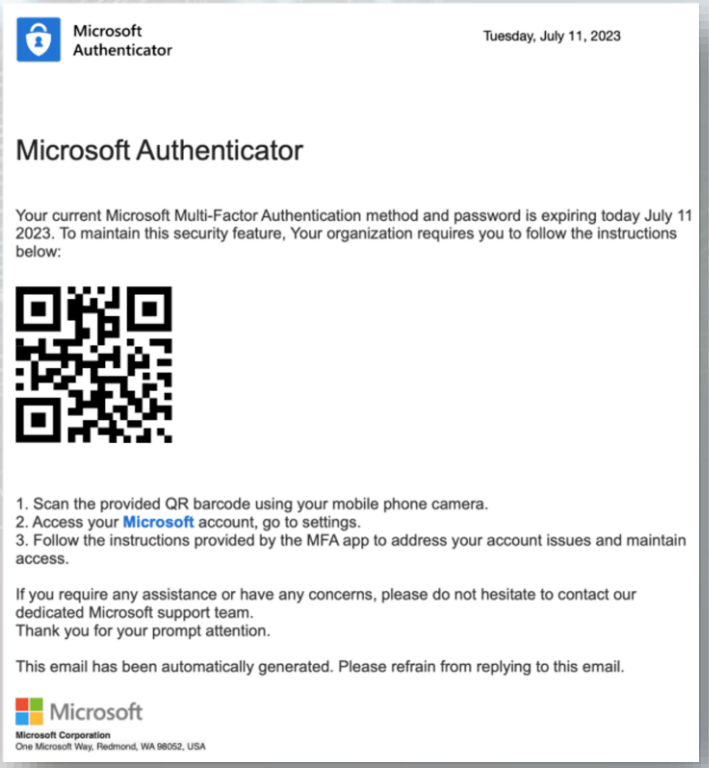
Vishing:

Scammers καλούν τηλεφωνικά, υποδυόμενοι αξιόπιστους οργανισμούς, και χρησιμοποιούν social engineering για να αποσπάσουν προσωπικά δεδομένα.

Tips:

- ✓ Μην δίνετε πληροφορίες σε μη αναζητημένες κλήσεις.
- ✓ Επαληθεύστε τον καλούντα μέσω επίσημων αριθμών.
- ✓ Χρησιμοποιήστε caller ID και call blocking.

Quishing (ή **QR phishing**) είναι μια κυβερνοαπειλή όπου οι επιτιθέμενοι χρησιμοποιούν **QR codes** για να ανακατευθύνουν θύματα σε κακόβουλες ιστοσελίδες ή να τους κάνουν να κατεβάσουν επιβλαβές περιεχόμενο. Στόχος είναι η κλοπή ευαίσθητων δεδομένων, όπως κωδικοί πρόσβασης, οικονομικές πληροφορίες ή **Personally Identifiable Information** , για πράξεις όπως κλοπή ταυτότητας, οικονομική απάτη ή **ransomware**.



Microsoft Authenticator

Tuesday, July 11, 2023

Microsoft Authenticator

Your current Microsoft Multi-Factor Authentication method and password is expiring today July 11 2023. To maintain this security feature, Your organization requires you to follow the instructions below:

1. Scan the provided QR barcode using your mobile phone camera.
2. Access your Microsoft account, go to settings.
3. Follow the instructions provided by the MFA app to address your account issues and maintain access.

If you require any assistance or have any concerns, please do not hesitate to contact our dedicated Microsoft support team.
Thank you for your prompt attention.

This email has been automatically generated. Please refrain from replying to this email.

Microsoft
Microsoft Corporation
One Microsoft Way, Redmond, WA 98052, USA

Πέρα από την αποστολή email ένας συνήθης τρόπος είναι ο επιτιθέμενος να εχει τυπώσει το QR code και το κολλάει πάνω από το legitim QR code.

Ελέγξτε το URL πριν το ανοίξετε. Αν μοιάζει με ένα URL που αναγνωρίζετε, βεβαιωθείτε ότι δεν είναι πλαστό — ψάξτε για ορθογραφικά λάθη ή γραμματική ασυνέχεια.
Μην σκανάρετε έναν κώδικα QR σε ένα email ή μήνυμα κειμένου που δεν περιμένατε — ειδικά αν σας προτρέπει να ενεργήσετε αμέσως.

Σε αυτήν την πραγματική επίθεση με **QR code**, το email φαίνεται αξιόπιστο – μια φιλική υπενθύμιση από τη Microsoft ότι ο κωδικός **MFA** σας λήγει και πρέπει να τον ενημερώσετε. Απλώς σκανάρετε το **QR code** με το τηλέφωνό σας και ανακατευθύνεστε σε μια σελίδα σύνδεσης της Microsoft για να εισάγετε τα διαπιστευτήριά σας.
Δυστυχώς, η σελίδα είναι κακόβουλη **spoof**, και τα διαπιστευτήριά σας καταλήγουν σε έναν επιτιθέμενο. Ο λογαριασμός σας έχει παραβιαστεί.

Πώς οι κυβερνοεγκληματίες εκμεταλλεύονται την Τεχνητή Νοημοσύνη

1. Σχήματα κοινωνικής μηχανικής (Social engineering schemes):
- Αυτοματοποιημένες επιθέσεις που βασίζονται σε ψυχολογική χειραγώγηση.
- Χρήση AI για τη δημιουργία πιο πειστικών, εξατομικευμένων μηνυμάτων
- Περιλαμβάνουν phishing, vishing και απάτες μέσω παραβίασης επαγγελματικής αλληλογραφίας – emails.
- Μεγαλύτερος όγκος επιθέσεων και αυξημένα ποσοστά επιτυχίας.

2. Παραβίαση κωδικών πρόσβασης (Password hacking):
- Χρήση AI για τη βελτίωση αλγορίθμων αποκρυπτογράφησης κωδικών.
- Ταχύτερη και ακριβέστερη πρόβλεψη κωδικών πρόσβασης.
- Αυξημένη αποτελεσματικότητα και κερδοφορία για τους χάκερς.
- Μεγαλύτερη εστίαση στην παραβίαση κωδικών πρόσβασης από πλευράς των κυβερνοεγκληματιών.

3. Deepfakes:
- Παραγωγή ψεύτικου ήχου/βίντεο με AI για προσποίηση ταυτότητας.
- Διασπορά σε κοινωνικά δίκτυα με σκοπό τη σύγχυση, τον φόβο ή τον εκβιασμό.
- Συνδυάζεται με κοινωνική μηχανική, εκβιασμούς και chatbots.

4. Δηλητηρίαση δεδομένων (Data poisoning):
- Αλλοίωση των δεδομένων εκπαίδευσης ενός AI μοντέλου.
- Παραποιημένα δεδομένα στην είσοδο οδηγούν σε λανθασμένα αποτελέσματα στην έξοδο (*garbage in, garbage out*).
- Δύσκολος και χρονοβόρος εντοπισμός, ώστε μέχρι να ανιχνευθεί η ζημιά μπορεί να είναι ήδη σοβαρή.

5. Παραβίαση CAPTCHA με χρήση ΤΝ (AI CAPTCHA Cracking):
- Η AI μαθαίνει να αναγνωρίζει πρότυπα ανθρώπινης συμπεριφοράς.
- Μπορεί να επιλύει CAPTCHA πιο αποδοτικά από τους ανθρώπους.
- Υπονομεύεται η αξιοπιστία των μηχανισμών επιβεβαίωσης ανθρώπινης οντότητας.

Στατιστικά για την ΤΝ στο Hacking και την Κυβερνοασφάλεια.

1. Μέχρι το 2026, έως και το 90% του online περιεχομένου ενδέχεται να είναι τεχνητό – δηλαδή να έχει παραχθεί από συστήματα τεχνητής νοημοσύνης ή άλλες μορφές συνθετικής τεχνολογίας (*open USD , Unreal Engine*...). (WeForum)
2. Οι επιχειρήσεις που πέφτουν θύματα απατών μέσω AI αντιμετωπίζουν όχι μόνο οικονομικές απώλειες, αλλά και απώλεια εμπιστοσύνης από τους πελάτες καθώς και πιθανές νομικές συνέπειες. (2024 Sophos Threat Report)
3. Το 75% των επαγγελματιών ασφάλειας παρατήρησαν αύξηση στις επιθέσεις τους τελευταίους 12 μήνες, ενώ το 85% αποδίδει την αύξηση στη χρήση generative AI από κακόβουλους φορείς. (SecurityMagazine)
4. Περίπου το 48% των υπευθύνων λήψης αποφάσεων στην IT δεν είναι σίγουροι ότι διαθέτουν την τεχνολογία για να αμυνθούν απέναντι σε επιθέσεις με χρήση AI. (Forbes)
5. Μόνο το 52% των IT decision-makers δηλώνουν ότι έχουν υψηλή εμπιστοσύνη στην ικανότητά τους να εντοπίσουν ένα deepfake του CEO τους. (Forbes)

SONICWALL

PRODUCTS SOLUTIONS PARTNERS SUPPORT

HOW IS YOUR PHISHING IQ?

Don't get phished! Get smart. Stay ahead of the hackers.

ΔΡΑΣΤΗΡΙΟΤΗΤΑ

https://www.sonicwall.com/phishing-iq-test/

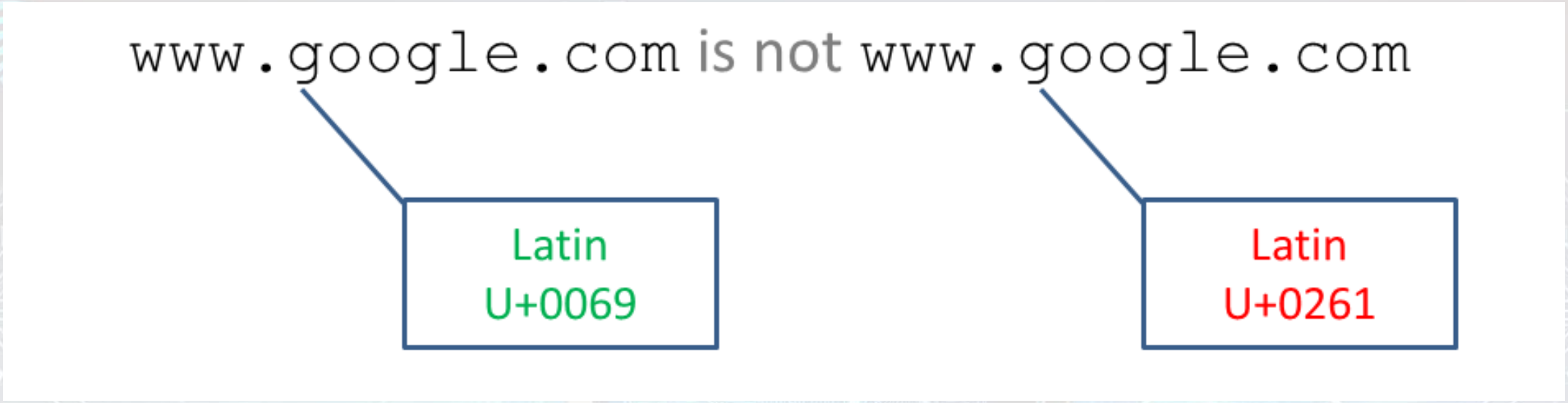
OpenDNS ENTERPRISE MSP & PARTNERS CONSUMER ABOUT US SUPPORT

PHISHING QUIZ

Think you can Outsmart Internet Scammers?

Ever wonder how good you are at telling the difference between a legitimate website and one that's a phishing attempt? Take this quiz to find out.

https://www.opendns.com/phishing-quiz/



Σημαντικό να καταλάβουν την διαφορά στον κώδικα ASCII

Link nr1 : www.souroti.gr

Link nr2 : www.souroti.gr

Βρείτε την διαφορά ...

Μια απλή διαδικασία για να διαπιστωθεί το ψεύτικο domain

https://www.car.gr/

```
C:\Users\vassi>ping www.car.gr

Pinging www.car.gr [104.21.72.178] with 32 bytes of data:
Reply from 104.21.72.178: bytes=32 time=368ms TTL=58
Reply from 104.21.72.178: bytes=32 time=29ms TTL=58
Reply from 104.21.72.178: bytes=32 time=28ms TTL=58
Reply from 104.21.72.178: bytes=32 time=28ms TTL=58

Ping statistics for 104.21.72.178:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 28ms, Maximum = 368ms, Average = 113ms
```

https://whois.domaintools.com/104.21.72.178

DOMAINTOOLS PROFILE CONNECT MONITOR SUPPORT

Home > Whois Lookup > 104.21.72.178

IP Information for 104.21.72.178

Quick Stats

IP Location	United States Of America San Francisco Cloudflare Inc.
ASN	AS13335 CLOUDFLARENET, US (registered Jul 14, 2010)
Whois Server	whois.arin.net
IP Address	104.21.72.178
Reverse IP	380 websites use this address.

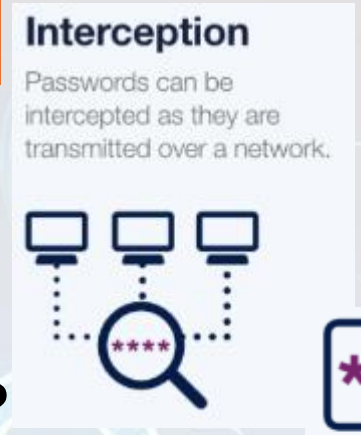
```
NetRange:       104.16.0.0 - 104.31.255.255
CIDR:           104.16.0.0/12
NetName:        CLOUDFLARENET
NetHandle:      NET-104-16-0-0-1
Parent:         NET104 (NET-104-0-0-0-0)
NetType:        Direct Assignment
OriginAS:       AS13335
Organization:   Cloudflare, Inc. (CLOUD14)
RegDate:        2014-03-28
Updated:        2017-02-17
Comment:        All Cloudflare abuse reporting can be done via
https://www.cloudflare.com/abuse
Ref:            https://rdap.arin.net/registry/ip/104.16.0.0

OrgName:        Cloudflare, Inc.
OrgId:          CLOUD14
Address:        101 Townsend Street
City:           San Francisco
StateProv:      CA
PostalCode:     94107
Country:        US
RegDate:        2010-07-09
Updated:        2021-01-11
Ref:            https://rdap.arin.net/registry/entity/CLOUD14

OrgTechHandle: ADMIN2521-ARIN
OrgTechName:   Admin
OrgTechPhone:  +1-650-319-8930
```

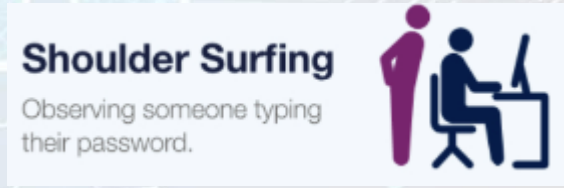
Create passwords

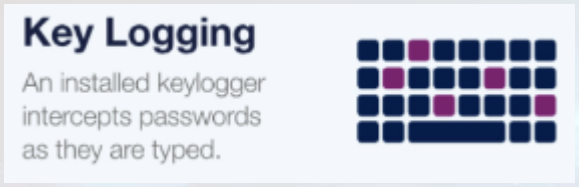
https://haveibeenpwned.com/

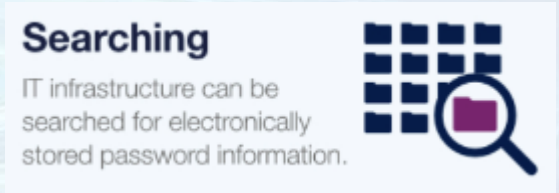
Προστασία Συσκευών – Δημιουργία passwords

- Ποιος ο λόγος να προστατέψουμε τις συσκευές μας ?
- Κινδυνεύουμε ?
- Αποτελούμε πιθανό στόχο ?
- Για ποιο λόγο θα μπορούσαμε να αποτελέσουμε στόχο ?









Άλλο ένα παράδειγμα «**My favourite team is PAOK**». Επιλέγω τα αρχικά κάπως έτσι: **MftiPAOK**, σε ένα συνδυασμό που να περιέχει και πεζούς άλλα και κεφαλαίους χαρακτήρες. Έπειτα προσθέτω έναν αριθμό. Στην προκειμένη ταιριάζει το **1926** καθώς είναι το έτος ίδρυσης της ομάδας. Έτσι προκύπτει το **MftiPAOK1926**

Από κάθε υπηρεσία επιλέγω τα αρχικά γράμματα (αν πρόκειται για σύνθετη λέξη, π.χ. F, B για το **F**ace**B**ook) ή το πρώτο γράμμα αν είναι μια λέξη (T για **T**witter) ή τα αρχικά αν είναι αρκτικόλεξο (π.χ. I, B, M αν είναι **IBM**) και τα συνδέω με το πρώτο κομμάτι κάνοντας χρήση 2 συμβόλων. Έτσι έχω τους εξής κωδικούς:

για το Facebook: MftiPAOK1926#FB#
Για το Twitter: MftiPAOK1926#T#
Για το Google: MftiPAOK1926#G#

Combination	Combinations per character	Example	Password Space
Lower case only	26	pass	456,976
Lower case only	26	password	208,827,064,576
Lower+upper case	52	Password	53,459,728,531,456
Lower+upper case + digits	62	Pa55w0rd	218,340,105,584,896
Lower+upper case + digits + symbols	92 (approx.)	Pa$$w0rd	5,132,188,731,375,616

Έλεγχος ισχυρού password εδώ :
https://www.security.org/how-secure-is-my-password/

1. 123456
2. 123456789
3. password
4. qwerty
5. 12345678
6. 12345
7. 123123
8. 111111
9. 1234
10. 1234567890
11. 1234567
12. abc123
13. 1q2w3e4r5t
14. q1w2e3r4t5y6
15. iloveyou
16. 123
17. 000000
18. 123321
19. 1q2w3e4r
20. qwertyuiop
21. 654321
22. qwerty123
23. 1qaz2wsx3edc
24. password1
25. 1qaz2wsx
26. 666666
27. dragon
28. ashley
29. princess
30. 987654321
31. 123qwe
32. 159753
33. monkey
34. q1w2e3r4
35. zxcvbnm
36. 123123123
37. asdfghjkl
38. pokemon
39. football
40. killer
41. 112233
42. michael
43. shadow
44. 121212
45. daniel
46. asdasd
47. qazwsx
48. 1234qwer
49. superman
50. 123456a
51. azerty
52. qwe123
53. master
54. 7777777
55. sunshine
56. N0=Acc3ss
57. 1q2w3e
58. abcd1234
59. 1234561
60. computer
61. f***you [censored
62. aaaaaa
63. 555555
64. asdfgh
65. asd123
66. baseball
67. 0123456789
68. charlie
69. 123654
70. qwer1234
71. naruto
72. a123456
73. jessica
74. soccer
75. jordan
76. liverpool
77. thomas
78. lol123
79. michelle
80. 123abc
81. nicole
82. 11111111
83. starwars
84. samsung
85. 1111
86. secret
87. joshua
88. 123456789a
89. andrew
90. 222222
91. q1w2e3r4t5
92. 147258369
93. hunter
94. Password
95. qazwsxedc
96. lovely
97. 999999
98. jennifer
99. letmein

Password Vaults - Password Management Tools

Τι είναι το θησαυροφυλάκιο κωδικών πρόσβασης;

- Οι διαχειριστές κωδικών πρόσβασης (Password Management Tools) αποθηκεύουν όλους τους κωδικούς πρόσβασης και άλλες βασικές πληροφορίες σε ένα θησαυροφυλάκιο κωδικών πρόσβασης.
- Σκεφτείτε το σαν ένα φυσικό χρηματοκιβώτιο αλλά για τα διαδικτυακά πολύτιμα είδη.
- Το θησαυροφυλάκιο είναι η βάση σας για όλα όσα έχετε αποθηκεύσει, συμπεριλαμβανομένων κωδικών πρόσβασης, ασφαλών σημειώσεων και στοιχείων πιστωτικής κάρτας.
- Σαν επέκταση του προγράμματος περιήγησης, θα καταγράφονται αυτόματα κωδικοί πρόσβασης καθώς τους εισάγετε σε κάθε ιστότοπο.

Ένα παράδειγμα ενός δωρεάν (*για κάποιες δυνατότητες*) Password Vault , από την AVIRA

Avira

https://www.avira.com/en/password-manager

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
2	0.086295	52.111.231.2	192.168.178.111	TLSv1.2	88	Application Data
3	0.086472	192.168.178.111	52.111.231.2	TCP	54	59489 → 443 [ACK] Seq=37 Ack=33 Win=1022 Len=0
4	0.334824	192.168.178.2	255.255.255.255	UDP	673	53596 → 29810 Len=631
5	2.477762	192.168.178.111	192.168.178.100	TCP	164	57340 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=510 Len=110 [TCP segment of a reassembled PDU
6	2.484676	192.168.178.100	192.168.178.111	TCP	164	8009 → 57340 [PSH, ACK] Seq=1 Ack=111 Win=1453 Len=110 [TCP segment of a reassembled
7	2.530815	192.168.178.111	192.168.178.100	TCP	54	57340 → 8009 [ACK] Seq=111 Ack=111 Win=509 Len=0
8	3.296573	192.168.178.111	151.101.2.110	TCP	55	61244 → 443 [ACK] Seq=1 Ack=1 Win=516 Len=1 [TCP segment of a reassembled PDU]
9	3.366026	192.168.178.111	151.101.2.133	TCP	55	61245 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
10	3.373034	151.101.2.110	192.168.178.111	TCP	68	443 → 61244 [ACK] Seq=1 Ack=2 Win=133 Len=0 SLE=1 SRE=2
11	3.440386	151.101.2.133	192.168.178.111	TCP	68	443 → 61245 [ACK] Seq=1 Ack=2 Win=133 Len=0 SLE=1 SRE=2
12	4.315151	192.168.178.111	151.101.1.253	TCP	55	60696 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
13	4.389136	151.101.1.253	192.168.178.111	TCP	68	443 → 60696 [ACK] Seq=1 Ack=2 Win=133 Len=0 SLE=1 SRE=2
14	5.352823	192.168.178.2	255.255.255.255	UDP	673	53596 → 29810 Len=631
15	5.370816	192.168.178.111	52.114.104.166	TCP	55	61353 → 443 [ACK] Seq=1 Ack=1 Win=515 Len=1 [TCP segment of a reassembled PDU]
16	5.456260	192.168.178.111	192.168.178.1	TCP	66	61379 → 8013 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
17	5.456553	52.114.104.166	192.168.178.111	TCP	68	443 → 61353 [ACK] Seq=1 Ack=2 Win=2049 Len=0 SLE=1 SRE=2
18	5.472532	192.168.178.1	192.168.178.111	TCP	60	8013 → 61379 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
19	5.988315	192.168.178.111	192.168.178.1	TCP	66	[TCP Retransmission] 61379 → 8013 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PE
20	6.004512	192.168.178.1	192.168.178.111	TCP	60	8013 → 61379 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
21	6.484352	192.168.178.111	192.168.178.1	TCP	66	61380 → 8013 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
22	6.500554	192.168.178.1	192.168.178.111	TCP	60	8013 → 61380 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	7.007221	192.168.178.111	192.168.178.1	TCP	66	[TCP Retransmission] 61380 → 8013 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PE
24	7.024609	192.168.178.1	192.168.178.111	TCP	60	8013 → 61380 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	7.486943	192.168.178.111	192.168.178.100	TCP	164	57340 → 8009 [PSH, ACK] Seq=111 Ack=111 Win=509 Len=110 [TCP segment of a reassembled

```
> Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{0DB1458C-A6A1-41D2-9BA7-6A33BDBCFD97}, id 0
> Ethernet II, Src: IntelCor_d4:8a:e6 (94:e6:f7:d4:8a:e6), Dst: zte_16:bd:b4 (d4:76:ea:16:bd:b4)
> Internet Protocol Version 4, Src: 192.168.178.111, Dst: 52.111.231.2
> Transmission Control Protocol, Src Port: 59489, Dst Port: 443, Seq: 1, Ack: 1, Len: 36
```

```
0000  d4 76 ea 16 bd b4 94 e6  f7 d4 8a e6 08 00 45 00   ·v·····  ·····E·
0010  00 4c 0e e2 40 00 80 06  5d 40 c0 a8 b2 6f 34 6f   ·L··@···  ]@···o4o
0020  e7 02 e8 61 01 bb 89 c0  44 3f ec 08 d5 52 50 18   ···a····  D?···RP·
0030  03 fe 4d 83 00 00 17 03  03 00 1f 00 00 00 00 00   ··M·····  ········
0040  00 00 82 2d 1e 2e 2c 28  59 97 5f 52 00 4b 85 a4   ···-.,(  Y·_R·K··
0050  a4 95 51 c3 d5 83 51 41  f4 a6                     ··Q···QA  ··
```

WIRESHARK

Network Protocol Analyzer

Capturing from Local Area Connection* 4

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Current filter: http

No.	Time	Source	Destination	Protocol	Length	Info
80	6.876483	192.168.137.55	84.205.2[redacted]	HTTP	870	GET /oam/server/osso_login?Site2pstoreToken=v3.0~B01F8
89	6.933032	84.205.2[redacted]	192.168.137.55	HTTP	838	HTTP/1.1 200 OK (text/html)
143	20.083511	192.168.137.55	84.205.2[redacted]	HTTP	149	POST /oam/server/auth_cred_submit HTTP/1.1 (applicati
154	20.145329	84.205.[redacted]	192.168.137.55	HTTP	997	HTTP/1.1 200 OK (text/html)

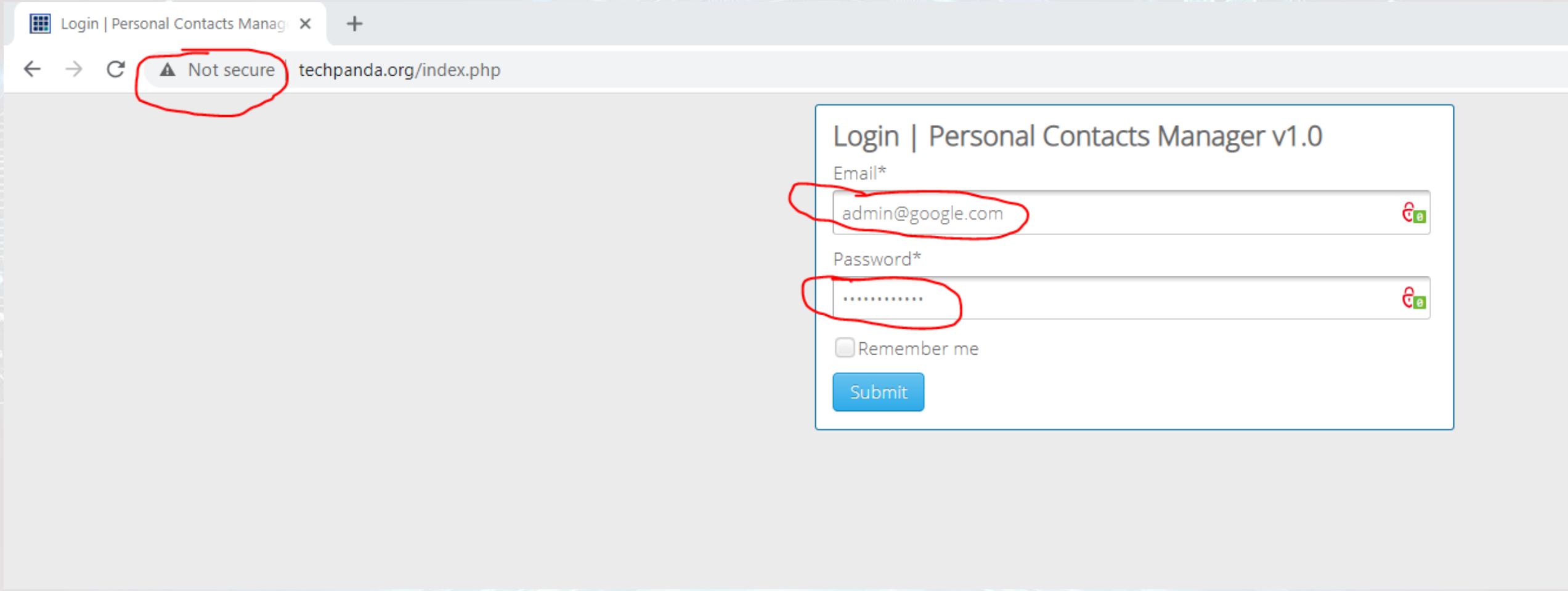
Wireshark · Packet 143 · Local Area Connection* 4

```
Origin: http://www.[redacted].gov.gr\r\n
User-Agent: Mozilla/5.0 (iPad; CPU OS 14_4 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Cr
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
 [truncated]Referer: http://www.[redacted].gov.gr/oam/server/osso_login?Site2pstoreToken=v3.0~B01F86650D28
> Content-Length: 83\r\n
> [truncated]Cookie: OAM_REQ_0=VERSION_4~%2ftaGV9RUUGbYkBRnTTcv0TH1i%2fHjQ%2bzFMpK%2blSLu3eiDcSQ9zMI1c
\r\n
[Full request URI: http://www.[redacted].gov.gr/oam/server/auth_cred_submit]
[HTTP request 1/1]
[Response in frame: 154]
File Data: 83 bytes
v HTML Form URL Encoded: application/x-www-form-urlencoded
> Form item: "username" = "vassilikosp@gmail.com"
> Form item: "password" = "SovaraTora"
> Form item: "request_id" = "4270846873496618080"
```

```
> Frame 143: 149 bytes on wire (1192 bits)
> Ethernet II, Src: 92:2f:b7:46:9e:ce (92:
> Internet Protocol Version 4, Src: 192.16
> Transmission Control Protocol, Src Port:
> [5 Reassembled TCP Segments (5168 bytes)
v Hypertext Transfer Protocol
  > POST /oam/server/auth_cred_submit HTT
    Host: www.[redacted].gov.gr\r\n
    Accept: text/html,application/xhtml+x
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-us\r\n
```

```
0000  96 e6 f7 d4 8a e6 92 2f  b7 46 9e ce 08 00 45 02   ·······/ ·F····E·
0010  00 87 00 00 40 00 40 06  9d 61 c0 a8 89 37 54 cd   ····@·@· ·a···7T·
0020  fe 60 cc af 00 50 2b 95  f2 56 25 b5 84 0d 80 18   ·`···P+· ·V%·····
0030  08 04 15 fb 00 00 01 01  08 0a 18 58 98 91 20 2d   ········ ···X·· -
0040  5f b9 75 73 65 72 6e 61  6d 65 3d 76 61 73 73 69   _·userna me=vassi
0050  6c 69 6b 6f 73 70 25 34  30 67 6d 61 69 6c 2e 63   likosp%4 0gmail.c
0060  6f 6d 26 70 61 73 73 77  6f 72 64 3d 53 6f 76 61   om&passw ord=Sova
0070  72 61 54 6f 72 61 26 72  65 71 75 65 73 74 5f 69   raTora&r equest_i
0080  64 3d 34 32 37 30 38 34  36 38 37 33 34 39 36 36   d=427084 68734966
0090  31 38 30 38 30                                     18080
```

```
0000  96 e6 f7 d4 8a e6 92 2f  b7 46 9e ce
```


Login | Personal Contacts Manag
Not secure
techpanda.org/index.php
Login | Personal Contacts Manager v1.0
Email*
admin@google.com
Password*
Remember me
Submit

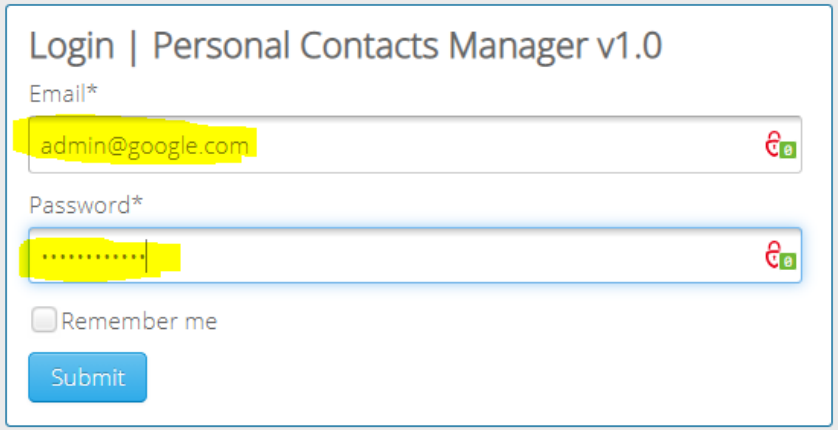
http

	Time	Source	Destination	Protocol	Length	Info
139	3.594802	192.168.178.111	64.91.242.213	HTTP	557	GET / HTTP/1.1
150	3.767703	64.91.242.213	192.168.178.111	HTTP	1182	HTTP/1.1 200 OK (text/ht
513	31.971646	192.168.178.111	64.91.242.213	HTTP	778	POST /index.php HTTP/1.1
553	32.146095	64.91.242.213	192.168.178.111	HTTP	1222	HTTP/1.1 302 Moved Tempor
555	32.149799	192.168.178.111				
588	32.319418	64.91.242.213				
591	32.322639	192.168.178.111				
683	32.488799	64.91.242.213				

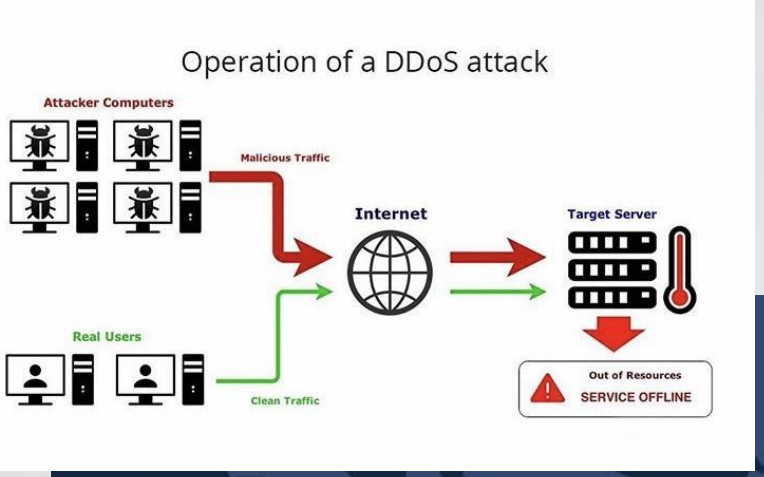
Wireshark · Packet 513 · Wi-Fi

```
> Frame 513: 778 bytes on wire (6224 bits), 778 bytes captured (6224 bits) on int
> Ethernet II, Src: IntelCor_d4:8a:e6 (94:e6:f7:d4:8a:e6), Dst: zte_16:bd:b4 (d4
> Internet Protocol Version 4, Src: 192.168.178.111, Dst: 64.91.242.213
> Transmission Control Protocol, Src Port: 58857, Dst Port: 80, Seq: 1, Ack: 1,
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  v Form item: "email" = "admin@google.com"
      Key: email
      Value: admin@google.com
  v Form item: "password" = "Password2010"
      Key: password
      Value: Password2010
```

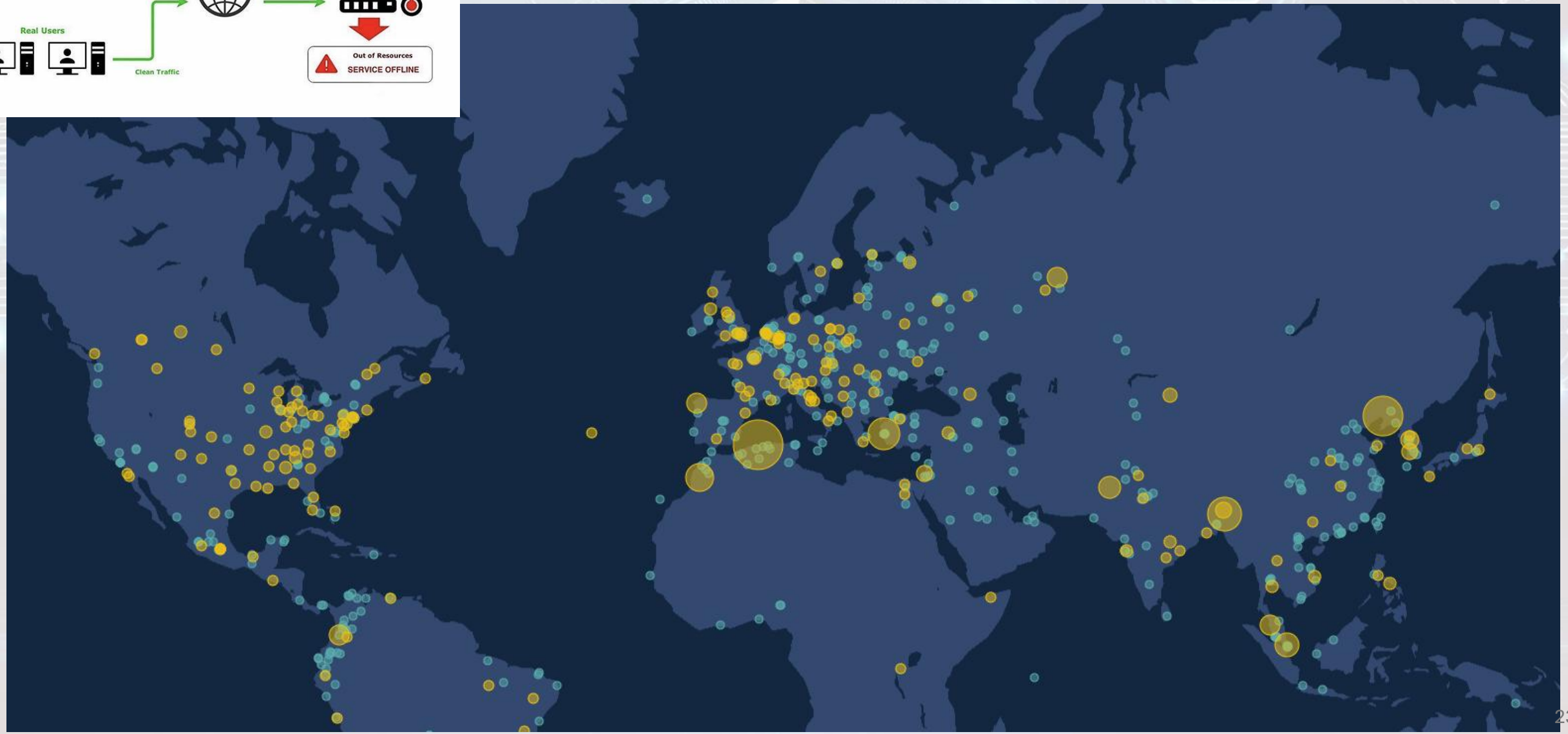
```
01c0  68 74 6d 6c 2b 78 6d 6c  2c 61 70 70 6c 69 63 61   html+xml ,applica
01d0  74 69 6f 6e 2f 78 6d 6c  3b 71 3d 30 2e 39 2c 69   tion/xml ;q=0.9,i
01e0  6d 61 67 65 2f 61 76 69  66 2c 69 6d 61 67 65 2f   mage/avi f,image/
01f0  77 65 62 70 2c 69 6d 61  67 65 2f 61 70 6e 67 2c   webp,ima ge/apng,
0200  2a 2f 2a 3b 71 3d 30 2e  38 2c 61 70 70 6c 69 63   */*;q=0. 8,applic
0210  61 74 69 6f 6e 2f 73 69  67 6e 65 64 2d 65 78 63   ation/si gned-exc
0220  68 61 6e 67 65 3b 76 3d  62 33 3b 71 3d 30 2e 39   hange;v= b3;q=0.9
0230  0d 0a 52 65 66 65 72 65  72 3a 20 68 74 74 70 3a   ··Refere r: http:
0240  2f 2f 77 77 77 2e 74 65  63 68 70 61 6e 64 61 2e   //www.te chpanda.
0250  6f 72 67 2f 0d 0a 41 63  63 65 70 74 2d 45 6e 63   org/··Ac cept-Enc
0260  6f 64 69 6e 67 3a 20 67  7a 69 70 2c 20 64 65 66   oding: g zip, def
0270  6c 61 74 65 0d 0a 41 63  63 65 70 74 2d 4c 61 6e   late··Ac cept-Lan
0280  67 75 61 67 65 3a 20 65  6e 2d 55 53 2c 65 6e 3b   guage: e n-US,en;
0290  71 3d 30 2e 39 2c 65 6c  2d 47 52 3b 71 3d 30 2e   q=0.9,el -GR;q=0.
02a0  38 2c 65 6c 3b 71 3d 30  2e 37 0d 0a 43 6f 6f 6b   8,el;q=0 .7··Cook
02b0  69 65 3a 20 50 48 50 53  45 53 53 49 44 3d 39 73   ie: PHPS ESSID=9s
02c0  72 71 35 62 65 38 64 37  31 6c 6b 6e 67 63 68 6c   rq5be8d7 1lkngchl
02d0  38 62 63 73 36 39 70 37  0d 0a 0d 0a 65 6d 61 69   8bcs69p7 ····emai
02e0  6c 3d 61 64 6d 69 6e 25  34 30 67 6f 6f 67 6c 65   l=admin% 40google
02f0  2e 63 6f 6d 26 70 61 73  73 77 6f 72 64 3d 50 61   .com&pas sword=Pa
0300  73 73 77 6f 72 64 32 30  31 30                    ssword20 10
```



DDOS botnet attack

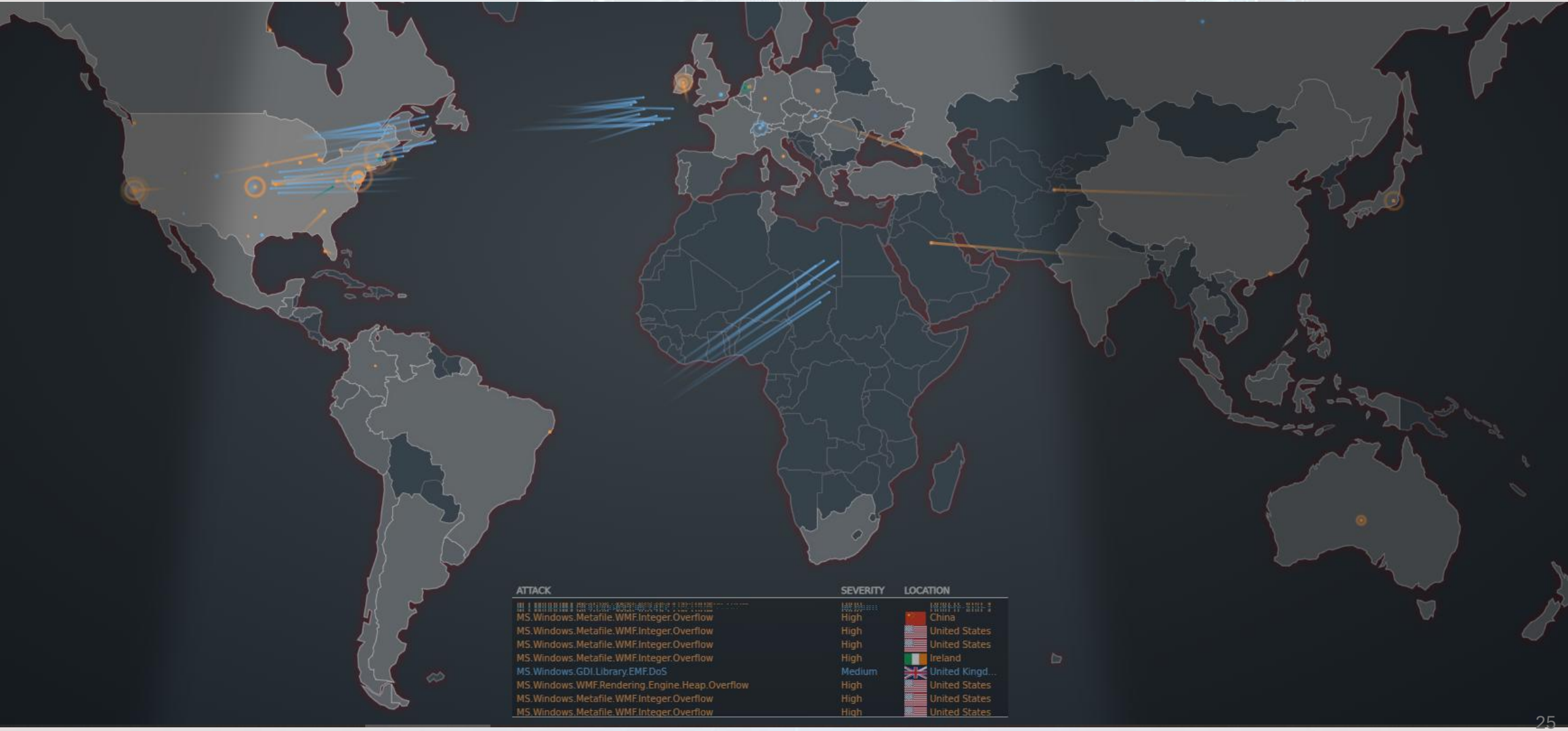


https://www.spamhaus.com/threat-map/



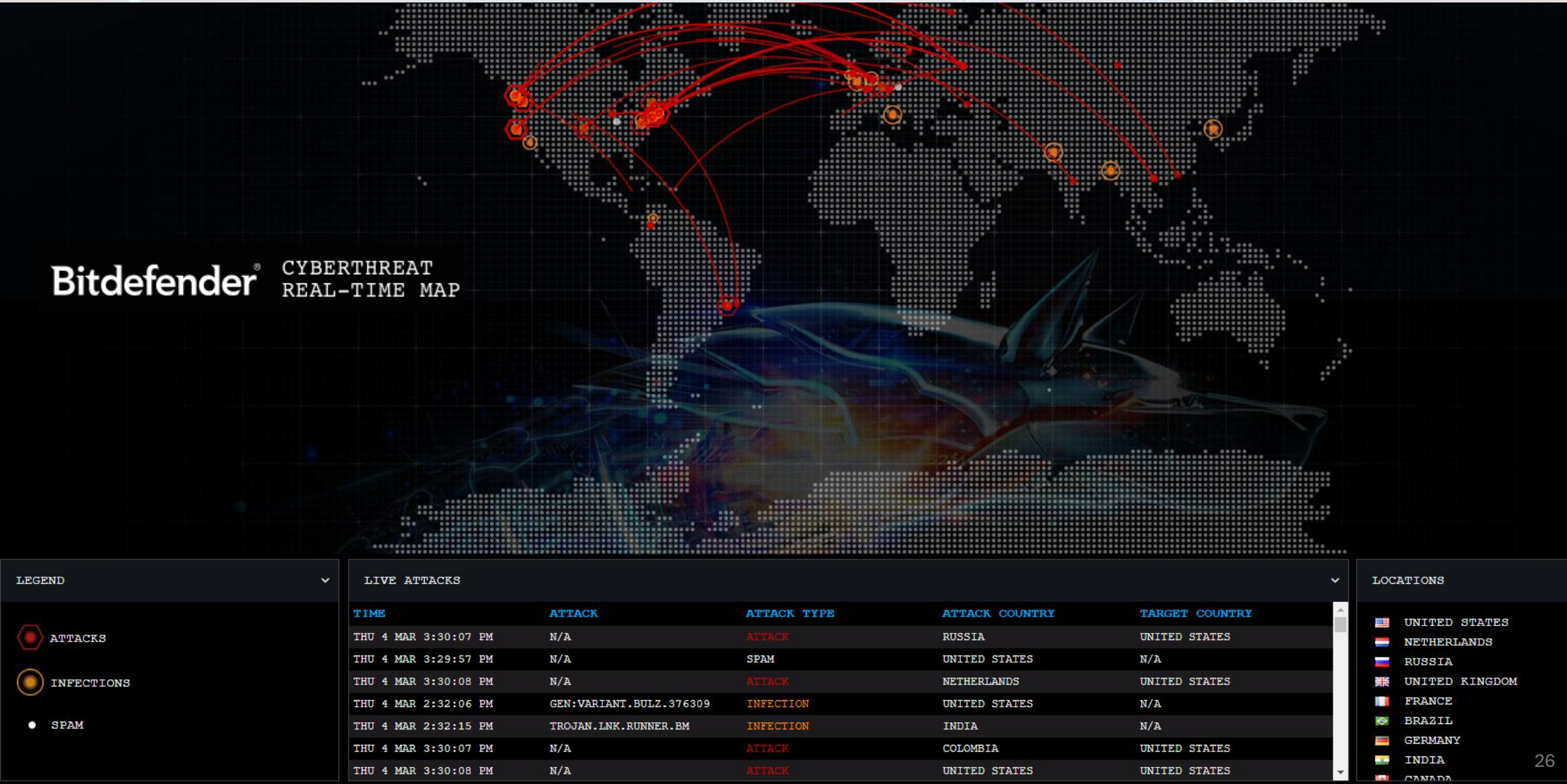
Χάρτης επιθέσεων της Fortinet

https://threatmap.fortiguard.com/

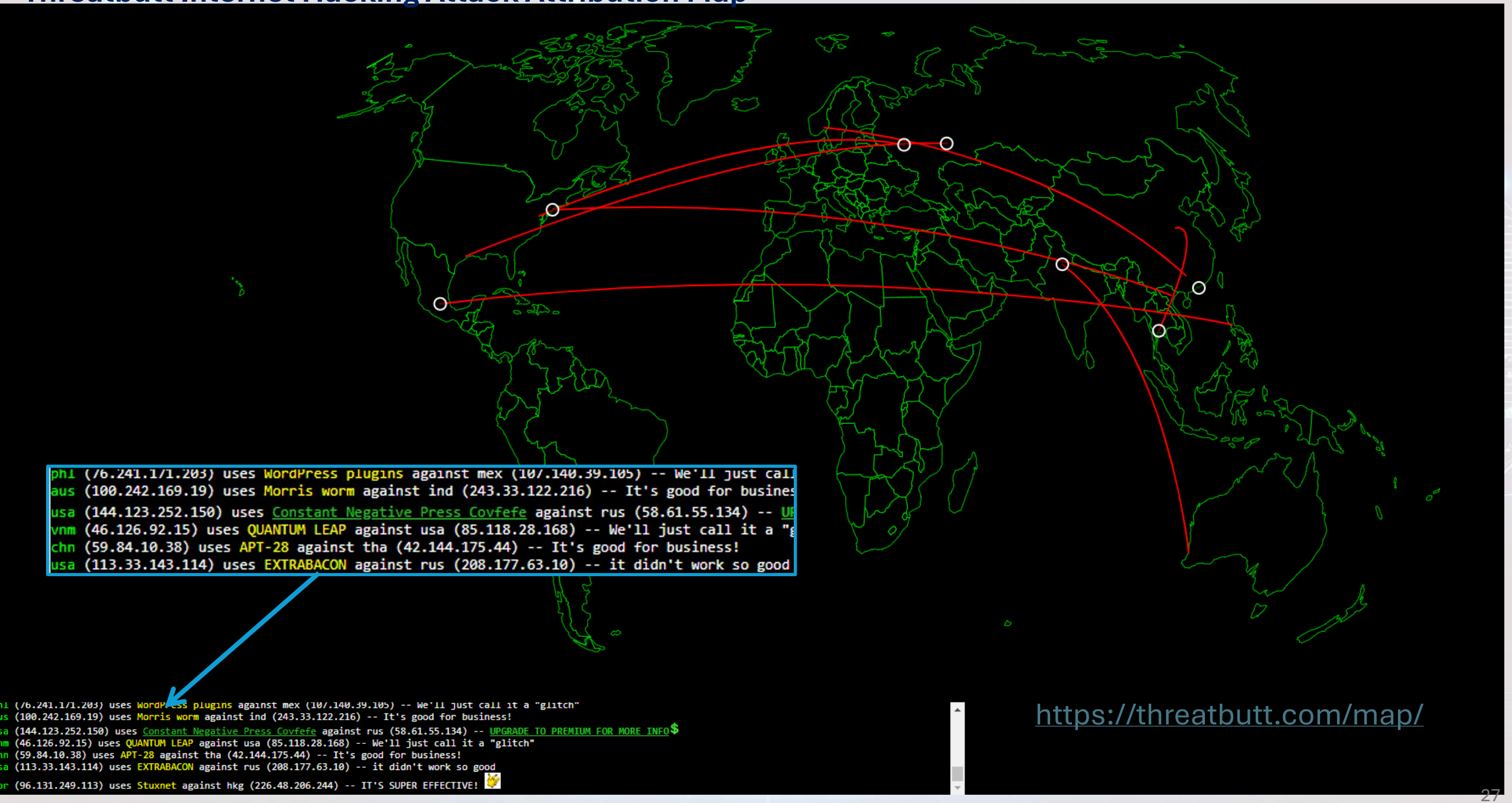


Bitdefender CYBERTHREAT Real-Time MAP

https://threatmap.bitdefender.com/

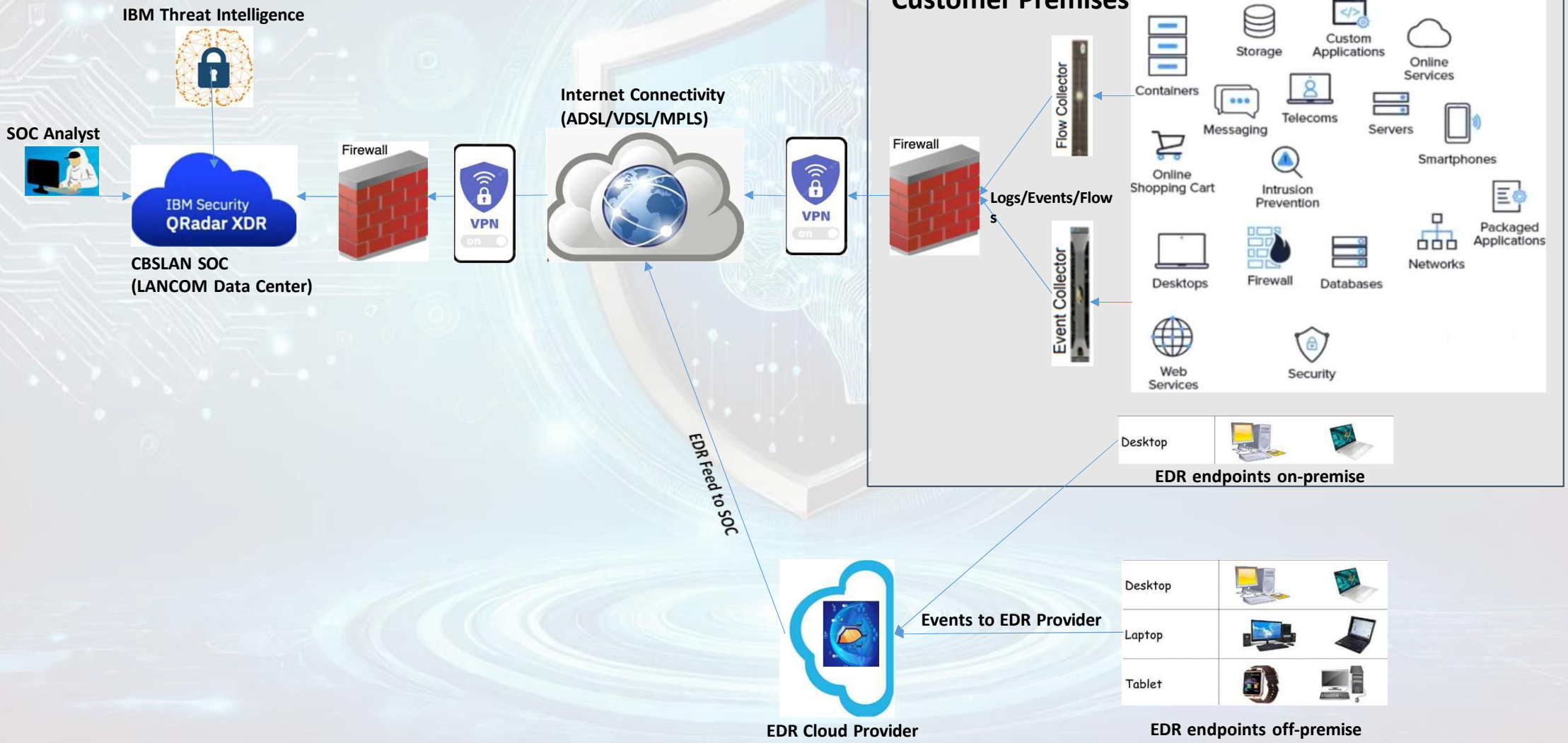


Threatbutt Internet Hacking Attack Attribution Map



https://threatbutt.com/map/

SOC Service


IBM Threat Intelligence
SOC Analyst
IBM Security
QRadar XDR
CBSLAN SOC
(LANCOM Data Center)
Firewall
VPN
Internet Connectivity
(ADSL/VDSL/MPLS)
VPN
Firewall
Customer Premises
Flow Collector
Event Collector
Logs/Events/Flows
Containers
Storage
Custom Applications
Online Services
Messaging
Telecoms
Servers
Smartphones
Online Shopping Cart
Intrusion Prevention
Packaged Applications
Networks
Desktops
Firewall
Databases
Web Services
Security
Desktop
EDR endpoints on-premise
EDR Feed to SOC
Events to EDR Provider
EDR Cloud Provider
Desktop
Laptop
Tablet
EDR endpoints off-premise

AI για την κυβερνοασφάλεια
IBM Watson

Η τεχνητή νοημοσύνη (AI) επιτρέπει την **γρήγορη ανάλυση μεγάλων όγκων δεδομένων**, βελτιώνοντας την ανίχνευση και πρόβλεψη απειλών σε πραγματικό χρόνο μέσω της **μοντελοποίησης απειλών** (threat modeling). Αυτή η διαδικασία αναγνωρίζει πιθανές απειλές, ποσοτικοποιεί τη σοβαρότητά τους και βοηθά στην προτεραιοποίηση των μέτρων αντιμετώπισης. Η AI μπορεί να εντοπίσει ύποπτες δραστηριότητες, όπως η δημιουργία πανομοιότυπων domains ή αναφορές σε συμβάντα ασφαλείας, πριν ξεκινήσει μια επίθεση.

Η **IBM Watson** στη **Κυβερνοασφάλεια** προσφέρει λύσεις όπως:

- **Αυτοματοποιημένη Ανάλυση Απειλών** (Automated Threat Analysis)
- **Εμπλουτισμός Δεδομένων** με Threat Intelligence (Threat Intelligence Enrichment)
- **Αυτόματος Εντοπισμός και Ειδοποιήσεις** (Automated Detection & Alerts)
- **Κυνήγι Απειλών** (Threat Hunting) με χρήση AI
- **Αυτοματοποίηση Αντιμετώπισης Περιστατικών** (Incident Response Automation)
- **Αξιοποίηση Συλλογικής Νοημοσύνης** (Collective Intelligence Insights)
- **Μείωση Χρόνου Ανταπόκρισης** σε απειλές (Reduced Response Time)

Ένα σημαντικό πρόβλημα στην ανίχνευση επιθέσεων είναι τα **false positives** (FP). Η AI βοηθά στη μείωσή τους, επιτρέποντας στους αναλυτές να επικεντρωθούν στις πραγματικές απειλές. Ωστόσο, η AI δεν εξαλείφει εντελώς τα FP και απαιτεί συνεχή βελτίωση των μοντέλων μηχανικής μάθησης.

IBM QRadar

Dashboard | Offenses | Log Activity | Network Activity | Assets | Reports | Risks | Vulnerabilities | Admin | Log Sources | Pulse | Use Case Manager | QDI | User Analytics | Watson | Reference Data Management | AQL Search Helper | Threat Intelligence | YARA & SIGMA Rule Manager | System Time: 1:38

Watson Investigations / ID: Offense 84562 / Relationship Graph

Relationships for
Source IP 192.168.1.8

CBS | Investigated

Evaluation

Watson determined this offense is a **high priority**. Do you agree?

Yes, I agree | No, I don't | I'm not sure

Adding your evaluation will not close the offense.

Relationships

- [x] Local - in offense (5)
- [x] Watson Enriched (53)
- [x] Local - outside offense (16)
- [ ] Local Blocked (0)
- [ ] Watson Enriched Blocked (0)

Scenarios

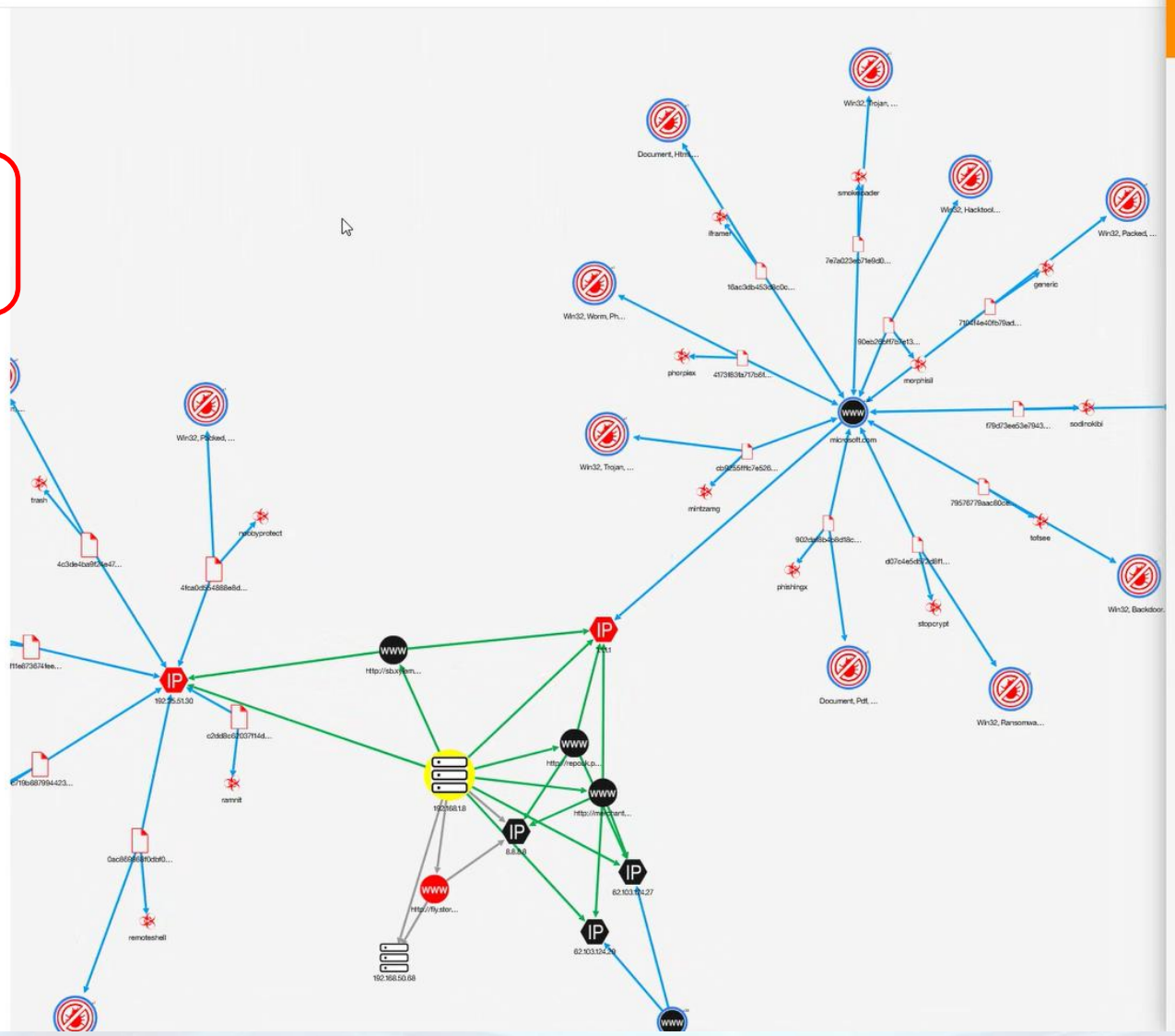
- [ ] Malware Executed (0)

Concern

- [ ] Critical (16)
- [ ] High (7)
- [ ] Medium (30)
- [ ] Low (10)

Observables

Important



Concern
Medium

IP Address
192.35.51.30

Insights

Relevance	5 of 10
Toxicity	1 of 10
Trend	↘

MITRE ATT&CK Tactics & Techniques

No data available

X-Force Exchange Report

Error encountered while attempting to contact X-Force Exchange, please contact an Administrator

WHOIS Record

Error encountered while attempting to contact X-Force Exchange, please contact an Administrator

Reputation

Malware - ReversingLabs detection ratio: - very low

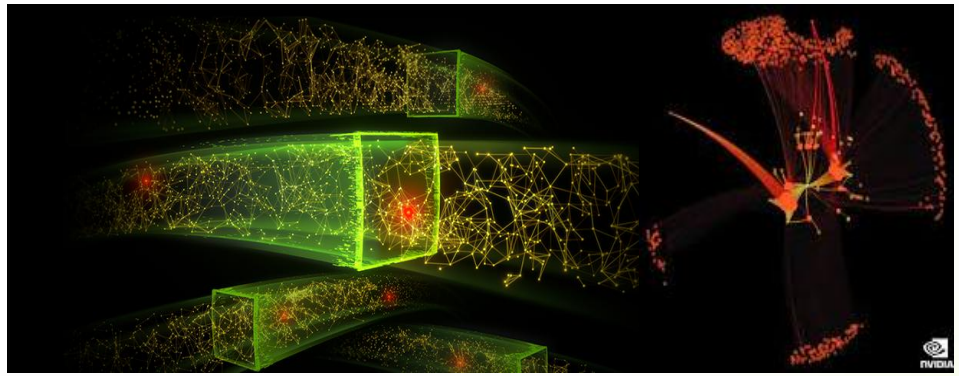
Threat Intelligence Sets Matched

No data available

References

> **Trusted business partner threat intelligence (7)**

AI για την κυβερνοασφάλεια
NVIDIA Morpheus



Το **NVIDIA Morpheus** είναι ένα ανοιχτό, **GPU-accelerated πλαίσιο τεχνητής νοημοσύνης (AI framework)** σχεδιασμένο για **cybersecurity**, επιτρέποντας **real-time analysis**, **threat detection** και **αυτοματοποιημένες αποκρίσεις** σε **data centers, cloud** και **edge environments**. Δίνει τη δυνατότητα να δημιουργηθούν **βελτιστοποιημένες ροές TN** για **filtering, processing** και **classifying** μεγάλων όγκων **streaming cybersecurity data**. Το **Morpheus** χρησιμοποιεί **τεχνητή νοημοσύνη** για να αναγνωρίζει και να προσαρμόζει **τα μέτρα ασφαλείας δυναμικά**, ενώ ταυτόχρονα παρέχει **συνεχή εποπτεία** των δικτύων μέσω τηλεμετρίας σε **πραγματικό χρόνο**. Αξιοποιώντας το **generative AI**, επεκτείνει τις δυνατότητες των αναλυτών μέσω **automation, synthetic data generation** και **προσομοιώσεων σεναρίων**, βελτιώνοντας συνολικά την ανίχνευση κινδύνων και την απόκριση.

1. Real-time Threat Detection and Response

- Χρησιμοποιεί **deep learning** για ανάλυση **network traffic** σε **real-time**, εντοπίζοντας **cyber threats** όπως **phishing** και **malware**.

2. Automated Security Operations

- Αυτοματοποιεί την ανίχνευση και ταξινόμηση απειλών, μειώνοντας την ανάγκη για χειροκίνητη παρέμβαση.

3. Generative AI for Cybersecurity

- Προσομοιώνει **cyberattacks**, δημιουργεί **synthetic data** και βελτιώνει την εκπαίδευση **security models**.

4. NLP for Threat Intelligence

- Αναλύει **security logs** και **alerts** με **NLP**, επιταχύνοντας την εξαγωγή πληροφοριών και τη λήψη αποφάσεων.

5. Adaptive Security Policies

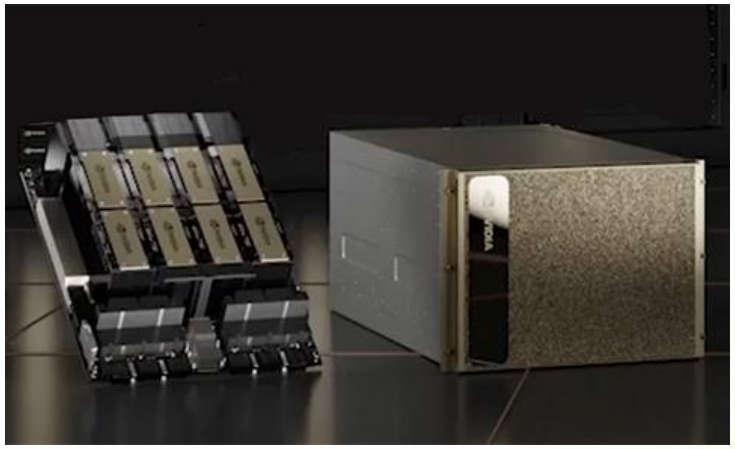
- Τα **AI models** μαθαίνουν από νέες απειλές και προσαρμόζουν δυναμικά τις **security policies**.

6. Reducing False Positives

- Βελτιώνει την ακρίβεια, μειώνοντας τα **false positives** και διευκολύνοντας τις **security teams**.

DGX H100

Hopper Architecture



Component	Description
GPU	For H100: 8 x NVIDIA H100 GPUs that provide 640 GB total GPU memory
CPU	2 x Intel Xeon 8480C PCIe Gen5 CPUs with 56 cores each 2.0/2.9/3.8 GHz (base/all core turbo/Max turbo)
NVSwitch	4 x 4th generation NVLinks that provide 900 GB/s GPU-to-GPU bandwidth
Power	10.2 kW max.
Performance	32 petaFLOPS FP8

FP8 = Floating Point 8-bits **AI training** and inference

DGX H200

Hopper Architecture

Component	Description
GPU	For H200: 8 x NVIDIA H200 GPUs that provide 1,128 GB total GPU memory
CPU	2 x Intel Xeon 8480C PCIe Gen5 CPUs with 56 cores each 2.0/2.9/3.8 GHz (base/all core turbo/Max turbo)
NVSwitch	4 x 4th generation NVLinks that provide 900 GB/s GPU-to-GPU bandwidth
Power	10.2 kW max.
Performance	32 petaFLOPS FP8

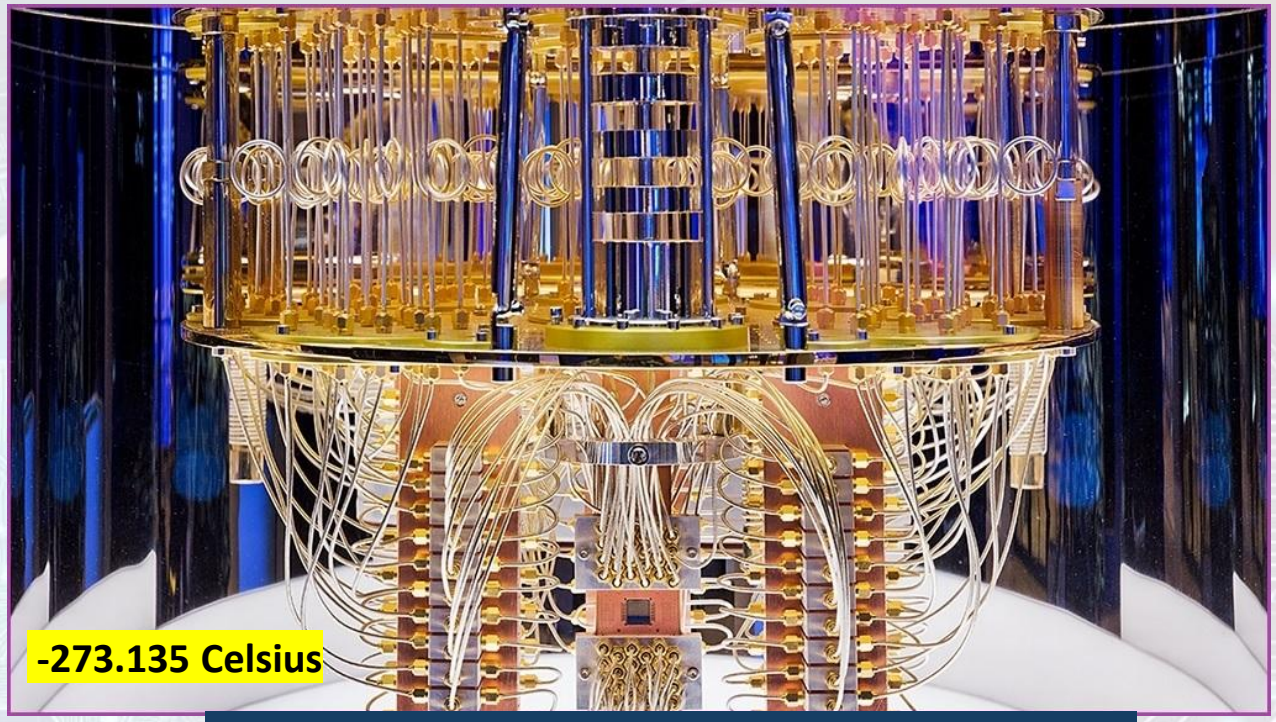
DGX B200

Blackwell GPU – Q2 2025

Component	Description
GPU	8x NVIDIA Blackwell GPUs that provide 1,440 GB total GPU memory
CPU	2 x Intel Xeon Platinum 8570 Processors 112 Cores total, 2.1 GHz (Base), 4 GHz (Max Boost)
NVSwitch	4 x 4th generation NVLinks that provide 900 GB/s GPU-to-GPU bandwidth
Power	~14.3 kW max.
Performance	72 petaFLOPS FP8

Τι είναι ένας κβαντικός υπολογιστής;

- **Κλασικοί υπολογιστές** χρησιμοποιούν bits που μπορούν να είναι είτε 0 είτε 1.
- **Κβαντικοί υπολογιστές** χρησιμοποιούν qubits, τα οποία μπορούν να είναι 0, 1, ή και τα δύο ταυτόχρονα (αυτό ονομάζεται "υπέρθεση"). Αυτή η ιδιότητα τους επιτρέπει να εκτελούν πολλούς υπολογισμούς παράλληλα.



IBM Condor – 1.121 qubits
By **2025**, **Kookaburra processor** with over **4.000 qubits**

Σε έναν κλασικό υπολογιστή, το πρόβλημα του πλανόδιου πωλητή (TSP) έχει πολυπλοκότητα O($n!$). Για 15 πόλεις (15!=1,3 τρισεκατομμύρια διαδρομές), η αναζήτηση θα πάρει περίπου 22 λεπτά ($\frac{1.307.674.368.000}{1.000.000.000} = 1.307\ \text{sec} \cong 22\ min$) , υποθέτοντας αξιολόγηση 10^9 διαδρομών/δευτερόλεπτο.
Οι κβαντικοί υπολογιστές, με αλγόριθμους όπως ο Grover ή ο Quantum Approximate Optimization Algorithm (QAOA) , μπορούν να επιταχύνουν δραματικά τη διαδικασία, μειώνοντας τον χρόνο σε περίπου 0,001 δευτερόλεπτο για 15 πόλεις ($\frac{1.143.000}{1.000.000.000} = 0{,}001\ \text{sec}$) .

Πώς επηρεάζει η κβαντική υπολογιστική την κρυπτογράφηση;

Πολλά συστήματα κρυπτογράφησης, όπως το RSA και το ECC (Elliptic Curve Cryptography), βασίζονται στην δυσκολία επίλυσης συγκεκριμένων μαθηματικών προβλημάτων.

Ο **αλγόριθμος του Shor**, που μπορεί να τρέξει σε κβαντικό υπολογιστή, μπορεί να λύσει αυτά τα προβλήματα πολύ γρήγορα, κάνοντας τους περισσότερους αλγορίθμους ασύμμετρης κρυπτογράφησης ευάλωτους.

Επιθέσεις Brute Force (Attacks)

- Σε έναν **κλασικό υπολογιστή**, μια επίθεση **Brute Force Attack** απαιτεί τη δοκιμή όλων των πιθανών συνδυασμών μέχρι να βρεθεί ο σωστός. Αυτό μπορεί να πάρει πολύ χρόνο, ειδικά αν ο κωδικός είναι αρκετά μεγάλος.
- Ο αλγόριθμος του Grover, όταν υλοποιείται σε κβαντικό υπολογιστή, επιταχύνει δραστικά την αναζήτηση σε μη ταξινομημένα δεδομένα, μειώνοντας τον απαιτούμενο χρόνο σε τάξη μεγέθους ίση με την τετραγωνική ρίζα του χρόνου που χρειάζεται ένας κλασικός υπολογιστής. Για παράδειγμα, αν ένας κλασικός υπολογιστής χρειάζεται 2^{128} δοκιμές για να σπάσει έναν κωδικό, ένας κβαντικός υπολογιστής θα χρειαστεί περίπου 2^{64} δοκιμές.
- **VPNs και Ασφαλείς Επικοινωνίες:**
  - Τα πρωτόκολλα ασφαλείας όπως το SSL/TLS και τα VPNs που βασίζονται σε ανταλλαγή κλειδιών Diffie-Hellman ή RSA θα μπορούσαν να σπάσουν από έναν ισχυρό κβαντικό υπολογιστή

Blockchain και Κρυπτονομίσματα:

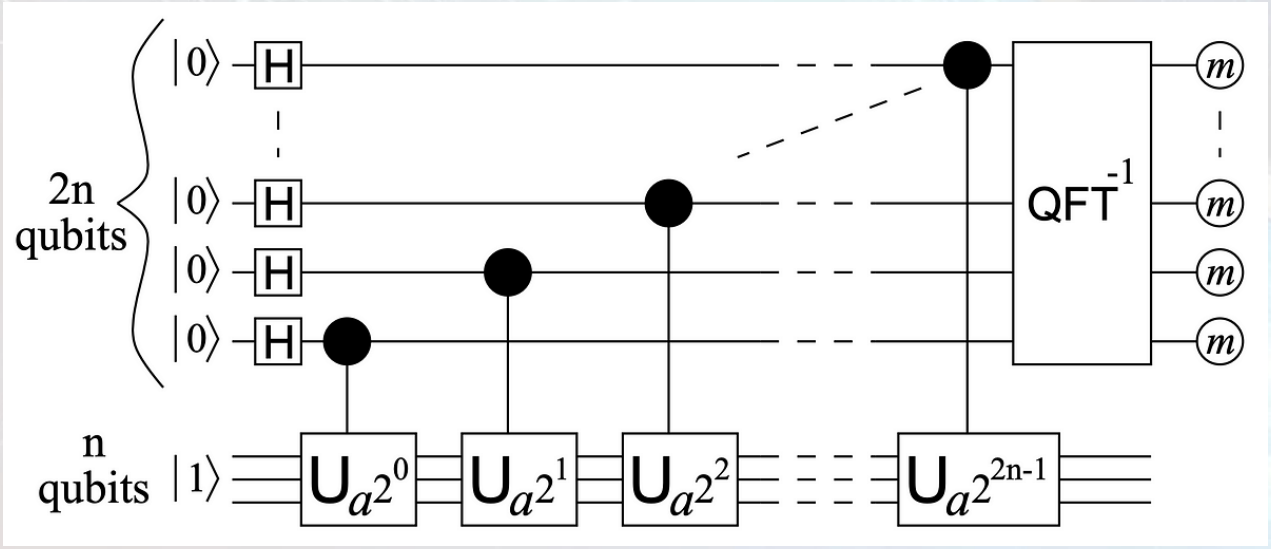
- Η ασφάλεια των κρυπτονομισμάτων όπως το Bitcoin, που βασίζεται σε κρυπτογραφία ECC, θα μπορούσε να απειληθεί, επιτρέποντας την παραβίαση ψηφιακών πορτοφολιών και συναλλαγών.

Παράδειγμα 1: Παραβίαση ενός VPN

Ένα VPN που χρησιμοποιεί RSA-2048 για την κρυπτογράφηση της ανταλλαγής κλειδιών:

Με κλασικό υπολογιστή:

- Με κλασικό υπολογιστή: Η ασφάλεια του RSA-2048 βασίζεται στο γεγονός ότι η παραγοντοποίηση ενός αριθμού 2048 bit (περίπου 617 ψηφία) είναι εξαιρετικά δύσκολη. Ακόμη και με υπερυπολογιστές, θα χρειάζονταν χιλιάδες χρόνια για να παραβιαστεί.



Με κβαντικό υπολογιστή (αλγόριθμος Shor):

- Με κβαντικό υπολογιστή (αλγόριθμος Shor): Ένας κβαντικός υπολογιστής με περίπου 4000 σταθερά qubits θα μπορούσε να σπάσει το RSA-2048 μέσα σε δευτερόλεπτα έως λεπτά. Ο αλγόριθμος Shor μειώνει τον χρόνο παραγοντοποίησης από εκθετικό σε πολυωνυμικό, καθιστώντας το σπάσιμο του RSA εξαιρετικά γρήγορο.

Παράδειγμα 2: Επίθεση σε Κωδικό Πρόσβασης μήκους 11 χαρακτήρων (*64 bit*) **vs** 21 χαρακτήρων (*128 bit*)

Παραδοχές και Δεδομένα:

- **Σύνολο χαρακτήρων:** 72 (Κεφαλαία, μικρά, αριθμοί, ειδικοί χαρακτήρες)
- **Ταχύτητα κλασικού υπολογιστή:** 10^{11} δοκιμές/δευτερόλεπτο (100 δισεκατομμύρια) (Nvidia DGX H200)
- **Ταχύτητα κβαντικού υπολογιστή:** 10^{6} δοκιμές/δευτερόλεπτο (1 εκατομμύριο "Grover iterations /sec")
- **Αλγόριθμος του Grover:** Μειώνει τις απαιτούμενες δοκιμές σε $\sqrt{N}$

1. Nvidia DGX H200 - **100 δισεκατομμύρια (10^{11}) password attempts per second**
2. IBM quantum computer **IBM Condor** με **1.121 qubits -** μπορεί να αναπαραστήσει **2^{1121}** καταστάσεις ταυτόχρονα, με μια συντηρητική προσέγγιση, μπορεί να εκτελεί το ελάχιστο 1 εκατομμύριο (10^{6}) κβαντικές πράξεις ανά sec.

A. Κωδικός με **64-bit** ασφάλεια (11 χαρακτήρες):

- **Συνολικοί συνδυασμοί:** 72^{11}=269.561.249.468.963.000.000 = (269×10^{18})

Απαιτούμενος Χρόνος ολοκλήρωση Brute force attack:

1. **Nvidia DGX H200 :** 85,5 χρόνια
2. **IBM quantum computer Condor :** 4,55 Ώρες

B. Κωδικός με **128-bit** ασφάλεια (21 χαρακτήρες):

- **Συνολικοί συνδυασμοί:** 72^{21}= 1.009.212.044.656.510.000.000.000.000.000.000.000.000 = ($1{,}010*10^{39}$)

Απαιτούμενος Χρόνος ολοκλήρωση Brute force attack:

1. **Nvidia DGX H200 :** 320.019.040.035.676.000.000 χρόνια ($3{,}2 *10^{20}$)
2. **IBM quantum computer Condor :** 1.007.360 χρόνια

Computer	Password Length	Time Required (in years)
Nvidia DGX H200	11	85,5 χρόνια
Nvidia DGX H200	21	320.019.040.035.676.000.000 χρόνια
IBM Quantum	11	4,55 Ωρες
IBM Quantum	21	1.007.360 χρόνια

Τι είναι η "Harvest Now, Decrypt Later" επίθεση ?

Η επίθεση βασίζεται στην ιδέα ότι τα δεδομένα που είναι ασφαλή σήμερα (λόγω ισχυρών αλγορίθμων κρυπτογράφησης όπως το RSA ή το ECC) μπορεί να γίνουν ευάλωτα στο μέλλον. Οι εισβολείς συλλέγουν κρυπτογραφημένα δεδομένα χωρίς να προσπαθήσουν να τα αποκρυπτογραφήσουν αμέσως, περιμένοντας την ανάπτυξη της τεχνολογίας (π.χ. κβαντικών υπολογιστών) που θα μπορέσει να σπάσει τους αλγόριθμους κρυπτογράφησης. Τα δεδομένα που κλέβονται σήμερα μπορεί να αποκρυπτογραφηθούν σε 5, 10 ή και 20 χρόνια, όταν η τεχνολογία θα το επιτρέψει

Οι εισβολείς στοχεύουν οποιαδήποτε κρυπτογραφημένα δεδομένα μπορεί να έχουν μελλοντική αξία. Αυτά μπορεί να περιλαμβάνουν:

1. **Ευαίσθητες επικοινωνίες**: Email, μηνύματα, τηλεφωνικές συνομιλίες.
2. **Οικονομικά δεδομένα**: Πληροφορίες πληρωμών, τραπεζικές συναλλαγές, πιστωτικές κάρτες.
3. **Προσωπικά δεδομένα**: Αριθμούς ταυτότητας, κωδικούς πρόσβασης, βιομετρικά δεδομένα.
4. **Επαγγελματικά μυστικά**: Διπλώματα ευρεσιτεχνίας, εμπορικά μυστικά, ερευνητικά δεδομένα.
5. **Στρατιωτικές ή κυβερνητικές πληροφορίες**: Ευαίσθητα δεδομένα που αφορούν την εθνική ασφάλεια.

Πώς μπορούμε να προστατευτούμε;

1. **Χρήση Post-Quantum Cryptography**: Η ανάπτυξη και υιοθέτηση κβαντο-ανθεκτικών αλγορίθμων κρυπτογράφησης που είναι ασφαλείς ακόμα και έναντι κβαντικών υπολογιστών.
2. **Ενημέρωση Συστημάτων**: Η τακτική ενημέρωση των κρυπτογραφικών πρωτοκόλλων και συστημάτων ασφαλείας.
3. **Πολιτικές Καταστροφής Δεδομένων**: Η διασφάλιση ότι τα δεδομένα που δεν χρειάζονται πλέον καταστρέφονται ασφαλώς.

Πότε Αναμένεται η Απειλή;

- **Βραχυπρόθεσμα (5-10 έτη)**: Δεν υπάρχουν ακόμη κβαντικοί υπολογιστές με αρκετά qubits και χαμηλό error rate για πρακτικές επιθέσεις.
- **Μεσοπρόθεσμα (10-20 έτη)**: Πιθανή ανάπτυξη **κβαντικών υπολογιστών ευρείας κλίμακας** (≥ 1 εκατομμύριο qubits με διόρθωση σφαλμάτων).
- **Μακροπρόθεσμα**: Η προετοιμασία πρέπει να ξεκινήσει **τώρα**, λόγω της μεγάλης διάρκειας ζωής πολλών κρυπτογραφικών συστημάτων (π.χ., TLS πιστοποιητικά με 20ετή ισχύ).

Συμπεράσματα

- Οι κβαντικοί υπολογιστές απειλούν την κυβερνοασφάλεια **επειδή** καταρρίπτουν τα μαθηματικά προβλήματα στα οποία βασίζεται η κλασική κρυπτογράφηση.
- Η μετάβαση σε **μετακβαντική κρυπτογράφηση** και η ενημέρωση υποδομών είναι **επείγουσα.**

Ευχαριστούμε για την προσοχή σας

Petros Vassilikos
pvasilikos@sch.gr
vassilikosp@gmail.com