Αναφορές Περιστατικών Ασφάλειας

Καθ. Χρ. Δουληγέρης

Ζ. Γαροφαλάκη, z.garofalaki@unipi.gr

Αναφορές Περιστατικών Ασφάλειας

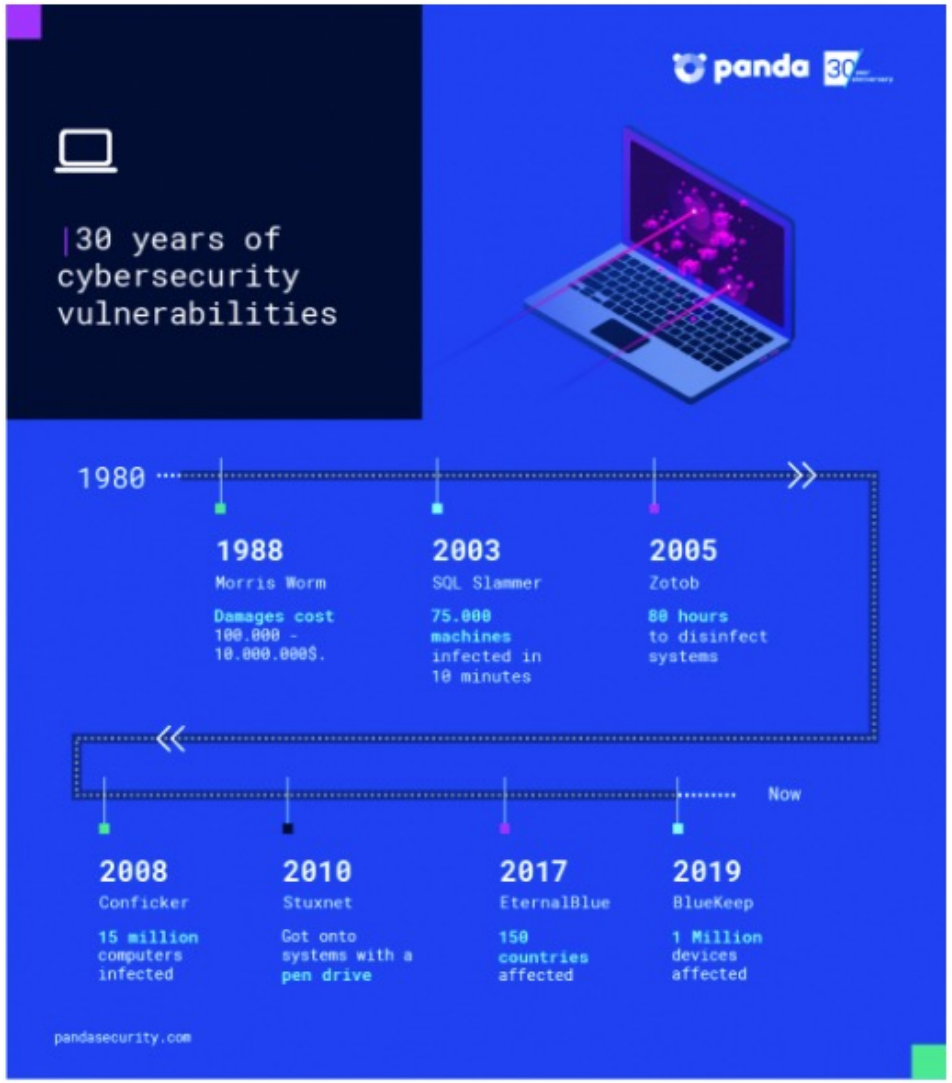
Ιστορικά στοιχεία, Κυβερνο-απειλές, Κατηγορίες επιτιθέμενων, Αλυσίδα καταστροφής, MITRE ATT&CK, Αναφορικά στοιχεία 2021, Χάρτες επιθέσεων σε πραγματικό χρόνο

ENISA

- **Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών**
  - European Network and Information Security Agency (ENISA) [2004-2019]
  - EU Agency for Cybersecurity [2019-…]
- Ιδρύθηκε στις 10 Μαρτίου 2004
- Εδρεύει στην Αθήνα και στο Ηράκλειο Κρήτης
- Στόχοι
  - Διασφάλιση δικτύων και πληροφοριών εντός της ΕΕ
  - Ενημέρωση πολιτών, καταναλωτών, εταιρειών και δημόσιων/κρατικών οργανισμών
  - Συγκρότηση Ομάδας Αντιμετώπισης Περιστατικών Ασφαλείας σε Υπολογιστές
    - Computer Security Incident Response Team (CSIRT)
    - Ευρωπαϊκό ανάλογο του κατοχυρωμένου όρου Computer Emergency Response Team Coordination Centre (CERT, CERT/CC, Η.Π.Α.)

Περιστατικό Morris

Δύο χρόνια πριν την αποκάλυψη του WWW



- **Morris Worm (1988).** To see one of the first examples of a computer virus that exploited known vulnerabilities, we have to go back to 1988, two years before the World Wide Web was invented. Morris Worm was one of the first computer worms to spread via the Internet. It exploited known vulnerabilities in Unix Sendmail, rsh/rexec, as well as weak passwords. While the creator's intention wasn't to cause any damage, rather to highlight security weaknesses, it caused between $100,000 and $10,000,000 in damages.

https://www.pandasecurity.com/en/mediacenter/panda-security/three-decades-vulnerabilities/

Ιστορικά στοιχεία CSIRT

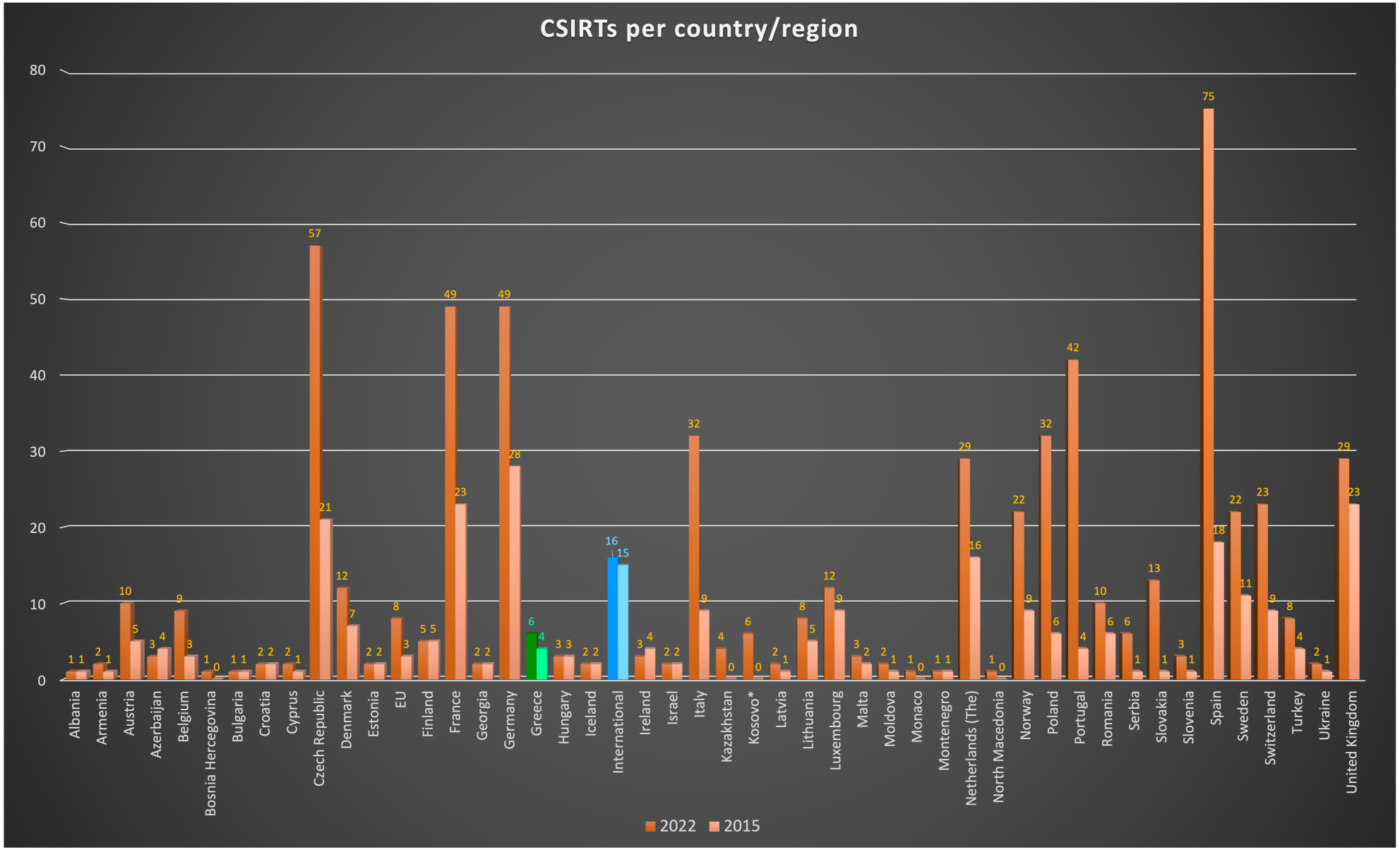
Σύσταση της πρώτης CSIRT μόλις λίγες μέρες μετά το Περιστατικό Morris

- Κέντρο Συντονισμού CERT (CERT/CC3) στο Πανεπιστήμιο Carnegie Mellon University του Pittsburgh (Pennsylvania)
  - Δημιουργήθηκε από την Υπηρεσία Έρευνας Προηγμένων Αμυντικών Προγραμμάτων (DARPA)

Ευρωπαϊκή εφαρμογή CSIRT

- SURFnet-CERT
  - Δημιουργήθηκε από τον ολλανδικό ακαδημαϊκό πάροχο υπηρεσιών SURFnet
- 260 καταγεγραμμένες CSIRT σε 42 Ευρωπαϊκές χώρες (Νοέμ. 2015)

Καταγεγραμμένες CSIRT 2022



Ελληνικές CSIRT 2022

Team name	Full name	Constituency	Contact
AUTH-CERT	Aristotle University of Thessaloniki CERT	NREN	auth.gr
FORTHcert	FOUNDATION OF RESEARCH AND TECHNOLOGY CERT (formerly FORTH CERT)	Service Provider Customer Base	forth.gr/forthcert/
GRNET-CERT	GRNET-CERT	NREN	cert.grnet.gr
NCERT-GR	Greek National Authority Against Electronic Attacks	Government, National	cert.gov.gr
AB-CSIRT	Alpha Bank Computer Security Incident Response Team	Financial	alpha.gr
GR-CSIRT	Hellenic Cyber Security Incident Response Team	Government	csirt.cd.mil.gr/

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

UNIVERSITY OF PIRAEUS

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

UPRC team

Χρ. Δουληγέρης

Καθηγητής

Πανεπιστήμιο Πειραιά

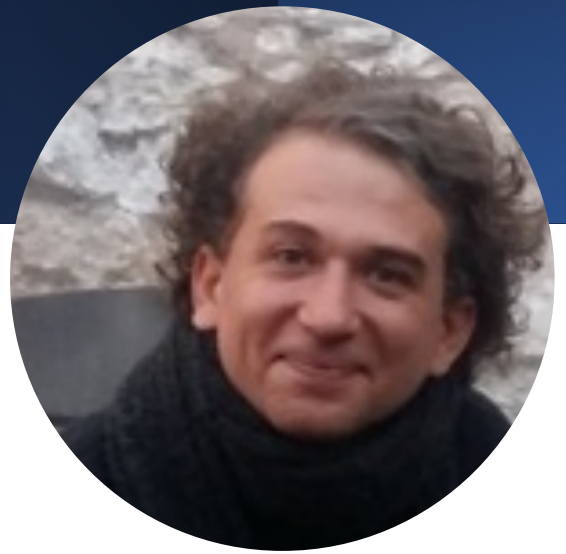
cdoulig@unipi.gr

Ζαχ. Γαροφαλάκη

Διδακτορική ερευνήτρια

Πανεπιστήμιο Πειραιά

z.garofalaki@uniwa.gr



Δημ. Καλλέργης

Λέκτορας

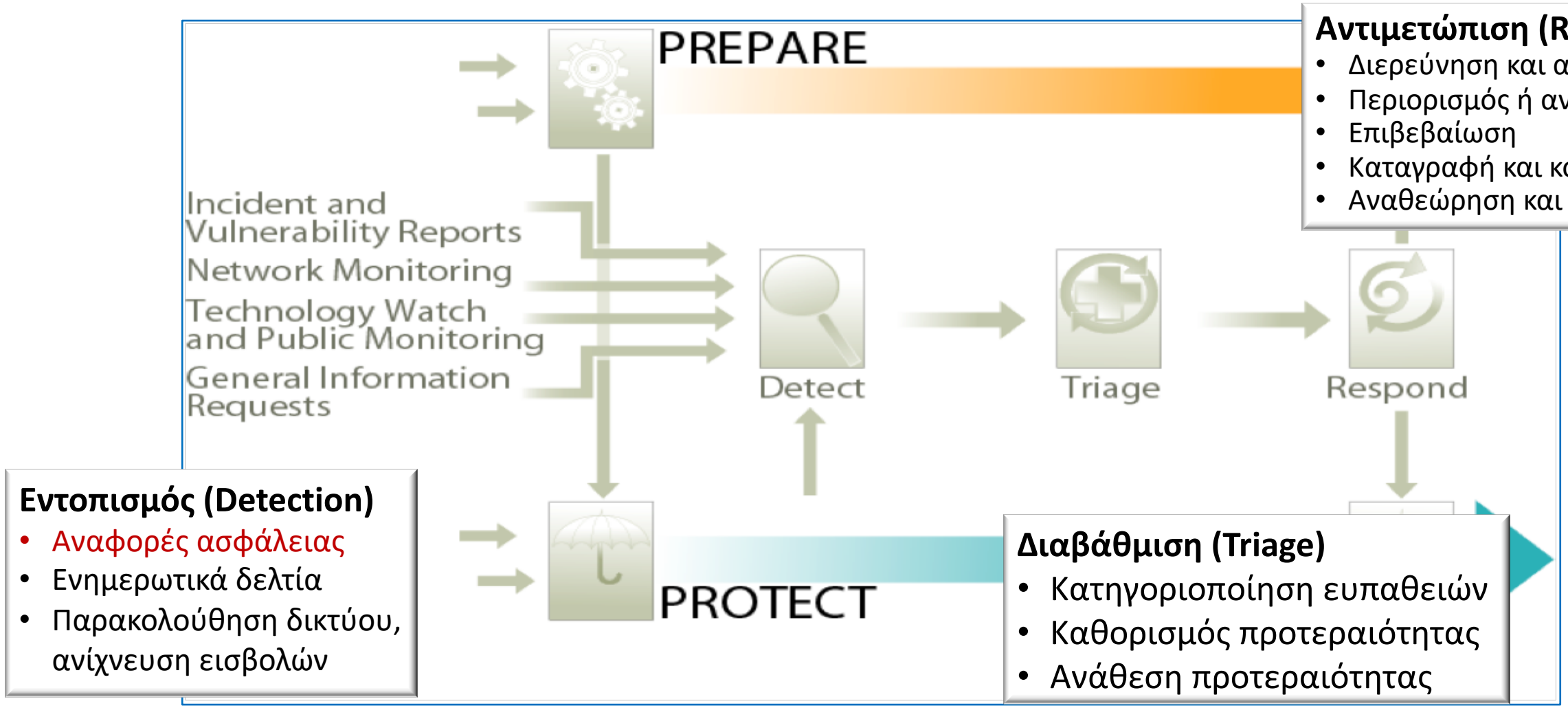
Πανεπιστήμιο Δυτικής Αττικής

d.kallergis@uniwa.gr

Αναφορές Περιστατικών Ασφάλειας

Κυβερνο-απειλές

Αναφορές και διαχείριση περιστατικών



Αντιμετώπιση (Response)
- Διερεύνηση και ανάλυση
- Περιορισμός ή αντιμετώπιση
- Επιβεβαίωση
- Καταγραφή και κοινοποίηση
- Αναθεώρηση και επανεξέταση

Εντοπισμός (Detection)
- Αναφορές ασφάλειας
- Ενημερωτικά δελτία
- Παρακολούθηση δικτύου, ανίχνευση εισβολών

Διαβάθμιση (Triage)
- Κατηγοριοποίηση ευπαθειών
- Καθορισμός προτεραιότητας
- Ανάθεση προτεραιότητας

Μοντέλο βέλτιστης πρακτικής διαχείρισης περιστατικών

Killcrece, G. (2012). *Incident Management*. [online] Cybersecurity and Infrastructure Security Agency (CISA). Available at: https://www.us-cert.gov/bsi/articles/best-practices/incident-management/incident-management

Στοιχεία αναφοράς κυβερνο-απειλής

- Σύντομη περιγραφή κυβερνο-απειλής στην περίοδο αναφοράς
- Ενδιαφέροντα στοιχεία και παρατηρήσεις
- Τάσεις και στατιστικά στοιχεία με τοπολογικές αναφορές
- Σημαντικότερα περιστατικά
- Συγκεκριμένοι φορείς επίθεσης (attack vectors)
- Μέτρα πρόληψης, περιορισμού ή αντιμετώπισης
- Αλυσίδα καταστροφής της κυβερνο-απειλής
- Αξιοσημείωτες πηγές

Προέχει η ταξινόμηση των κυβερνο-απειλών

Ταξινόμηση ENISA 2012-2014

Threat Landscape		
2012	2013	2014
Drive-by Exploits	Dri	Web-based attacks[5]
Worms/Trojans	M	licious Code: Worms/Trojans
Code Injection Attacks	C	ttacks/Injection attacks[6]
Exploit Kits	F	
Botnets		
Denial of servi		
		Ransomwa
		Spam
Abuse of Information Leakage		
Search Engine Poisoning		
Rogue certificates		

[1] Includes 2012 Rogue certificates
[2] CryptoLocker Ransomware Infections
[3] Data Broker Giants Hacked by ID Theft Ser
(SSNDOB)
[4] Replaced 2012 Search Engine Poisoning

and 2013 Watering hole attacks
[9] The Snowden revelations in 2013-2014
, and CryptoWall)

Edward Snowden: the whistleblower behind the NSA surveillance revelations

Until very recently, the source of the data sold by SSNDOB ha
began to unravel in March 2013, when teenage hackers allegedly asse
group UGNazi showed just how deeply the service's access went. The young ha
SSNDOB to collect data for exposed.su, a Web site that listed the SSNs, birthdays, phone
numbers, current and previous addresses for dozens of top celebrities — such as performers
Beyonce, Kanye West and Jay Z — as well as prominent public figures, including First Lady
Michelle Obama, CIA Director John Brennan, and then-FBI Director Robert Mueller.

Scandal starts

5 June 2013: Guardian journalist Glenn Greenwald reports the US National
Security Agency (NSA) is **collecting the telephone records** of millions of
Verizon customers under a top secret court order granting the government
unlimited authority to obtain communications data for a three-month period.

Ταξινόμηση ENISA 2014-2020

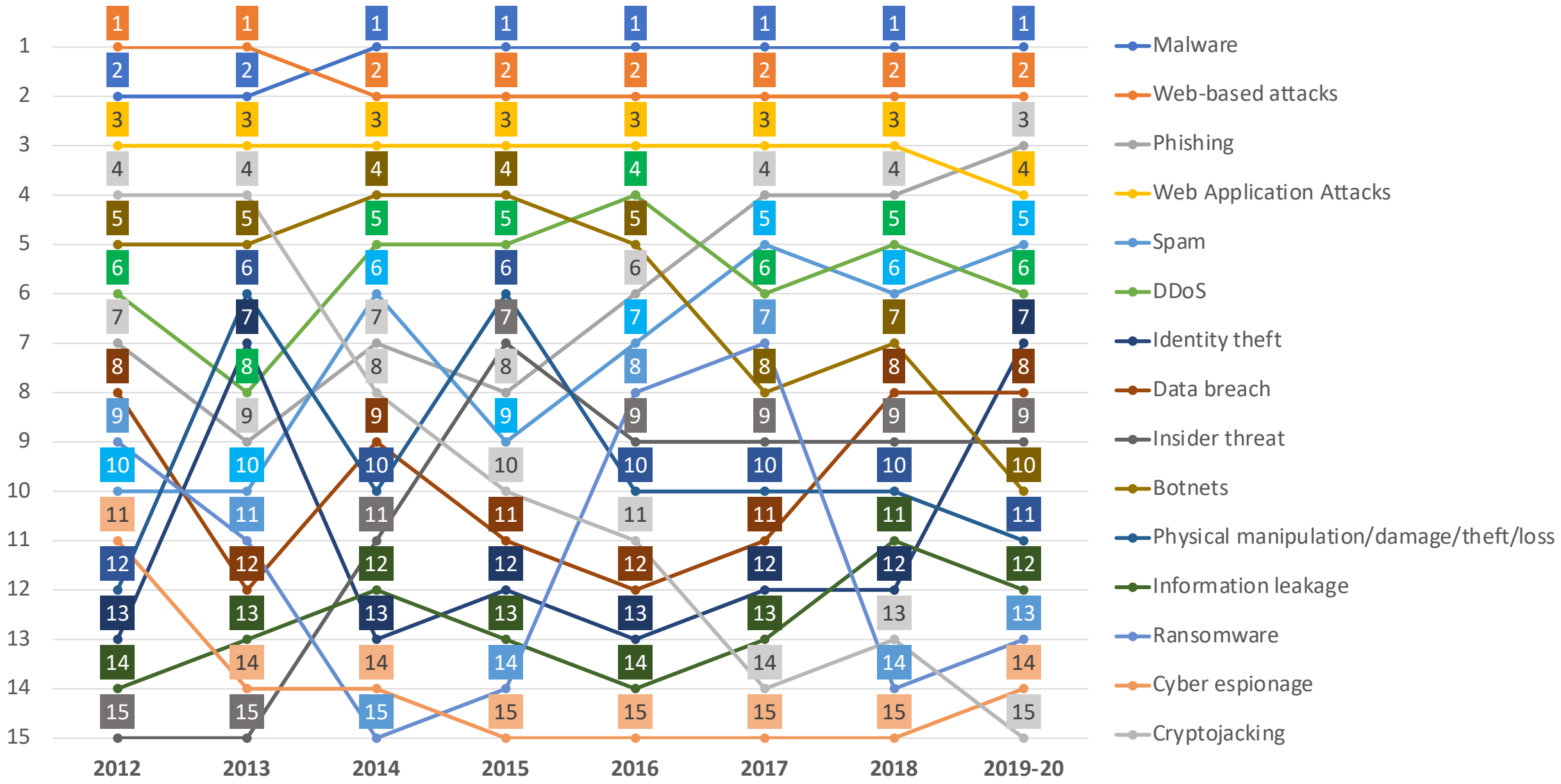
Threat Landscape		
2015	2016, 2017	2018-2020
Web based attacks	Web-based attacks	Web-based attacks
Malware[10]	Malware	Malware
Web application attacks	Web application attacks	Web application attacks
Exploit kits	Exploit kits	Cryptojacking[13]
Botnets	Botnets	Botnets
Denial of service	Denial of Service	Denial of Service
Phishing	Phishing	Phishing
Data Breaches	Data breaches	Data breaches
Ransomware[11]	Ransomware	Ransomware
Spam	Spam	Spam
Cyber Espionage	Cyber espionage	Cyber espionage
Physical damage/theft/loss	Physical manipulation/damage/theft/loss[12]	Physical manipulation/damage/theft/loss
Identity theft	Identity theft	Identity theft
Information leakage	Information leakage	Information leakage
Insider threat	Insider threat	Insider threat

[10] Renamed 2014 Malicious Code: Worms/Trojans
[11] 2015: Year of ransomware (100% more attacks than in 2014)
[12] 2016 ATM fraud
[13] 2018: Year of cryptojacking (600% more attacks than in 2017)

Νέα ταξινόμηση 2021-…

Threat Landscape	
2018-2020	2021-…
Ransomware	**Ransomware**
Malware	**Malware**
Botnets	RAT, Skimmers, Botnets
Cryptojacking	**Cryptojacking**
Spam	**E-mail related threats**
Phishing	Spam, Phishing, Spear phishing, BEC, Smishing
Data breaches	**Threats against data**
Information leakage	
Identity theft	
Cyber espionage	
Physical manipulation/damage/theft/loss	
Insider threat	
Web-based attacks	**Threats against availability and integrity**
Denial of Service	DoS / DDoS / Ransom Denial of Service (RDoS)
Web application attacks	
Cyber espionage	
	Disinformation-misinformation
Physical manipulation/damage/theft/loss	**Non-malicious threats**
	Upgrades, Vulnerabilities, Zero day, CVEs, Libraries/software bugs

Κατάταξη απειλών 2014-2020



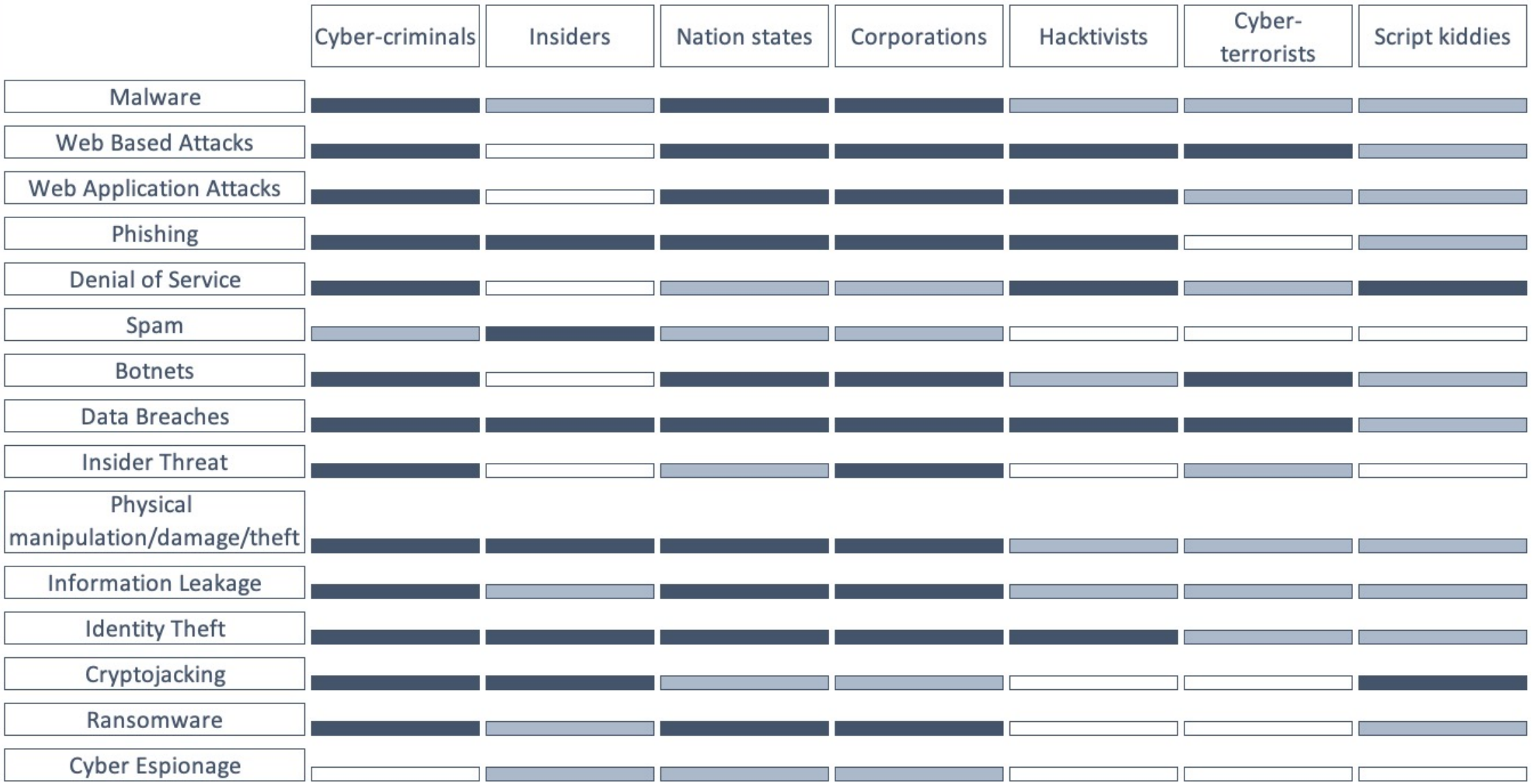
Αναφορές Περιστατικών Ασφάλειας

Κατηγορίες επιτιθέμενων

Κατηγορίες επιτιθέμενων

	Κίνητρα/αίτια	Εκλογίκευση	Επιτήδευση
CYBER CRIMINALS	Οικονομικά οφέλη, έξαψη	Χαμηλή	Υψηλή
INSIDERS	Προσωπικό όφελος, ακούσια	Υψηλή	Υψηλή
NATION STATES	Άμυνα	Υψηλή	Υψηλή
CORPORATIONS	Εταιρική (αντί)κατασκοπία	Υψηλή	Κυμαίνεται
HACKTIVISTS	Πολιτικά, κοινωνικά, ιδεολογικά	Μέτρια	Μέτρια
CYBER TERRORISTS	Καταστροφή	Μέτρια	Μέτρια
SCRIPT KIDDIES	Έξαψη	Πολύ χαμηλή	Χαμηλή

Τάσεις επιτιθέμενων



Ενδιαφέροντα στοιχεία και παρατηρήσεις

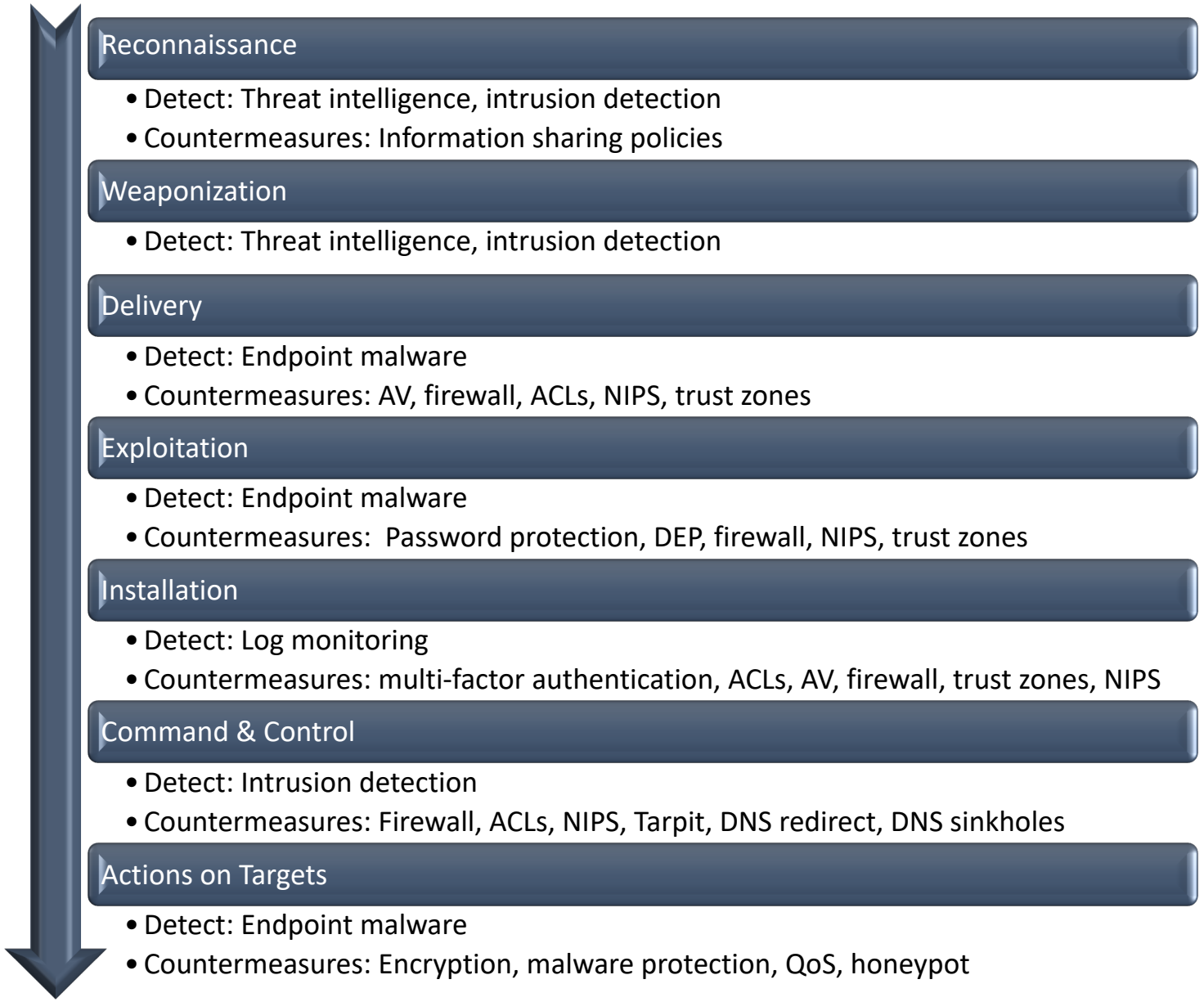
Κριτήρια επιλογής

- Νέος τρόπος εκδήλωσης της απειλής
  The first malware targeting safety systems of critical infrastructure
- Πλήθος επιθέσεων ευρείας κλίμακας
  Necurs is the top spamming botnet
- Στόχευση συγκεκριμένου οικονομικού ή κοινωνικού κλάδου
  Fewer vulnerabilities observed for Finance, Retail and Healthcare
- Στόχευση με γεωγραφικά κριτήρια
  DDoS and geo-politics landscape
- Επιθέσεις που επιτάσσουν ή επηρεάζονται από τεχνικές, τακτικές ή νομικές αλλαγές
  Insider threat perception changed with GDPR

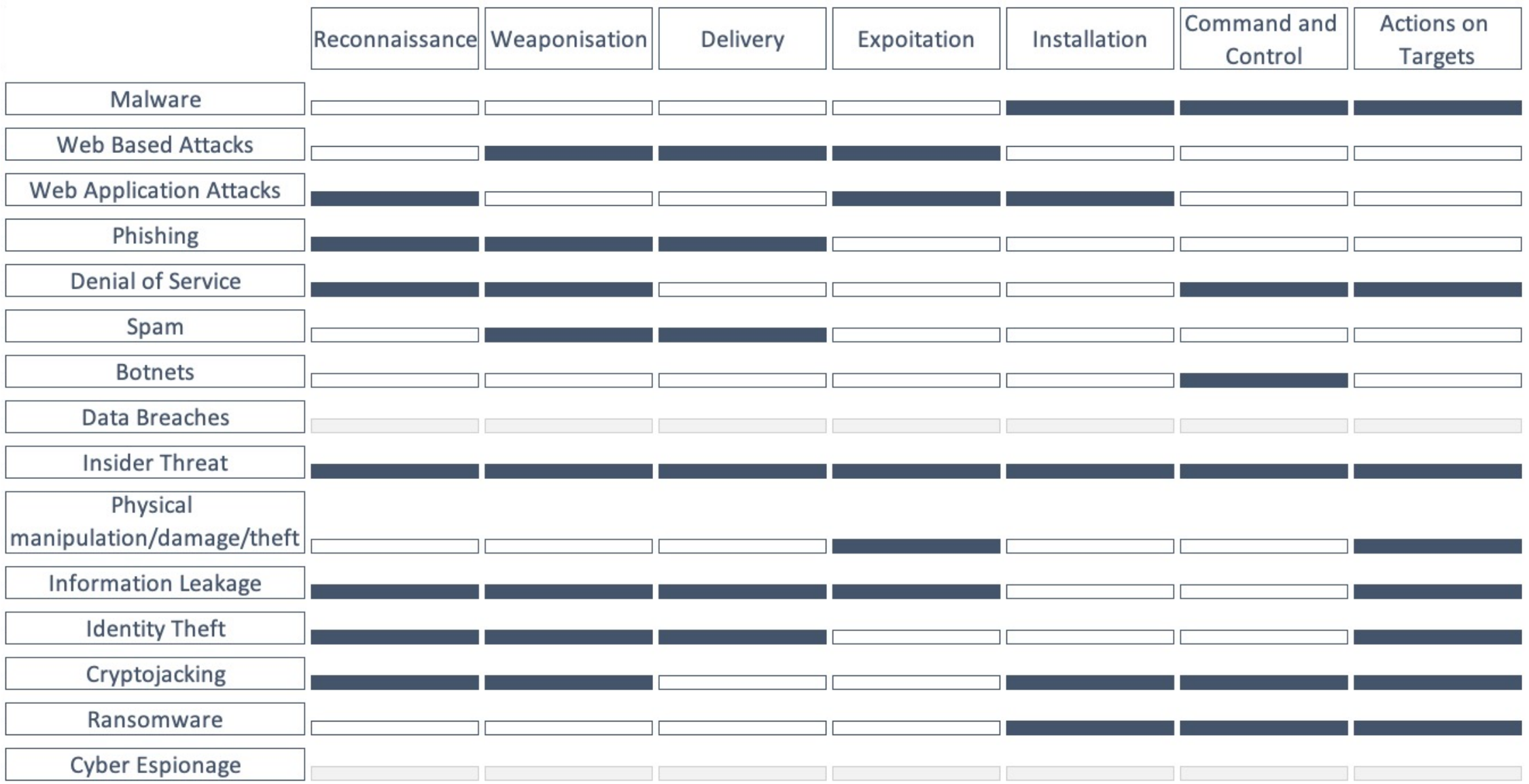
Αναφορές Περιστατικών Ασφάλειας

Αλυσίδα καταστροφής, MITRE ATT&CK

Αλυσίδα καταστροφής

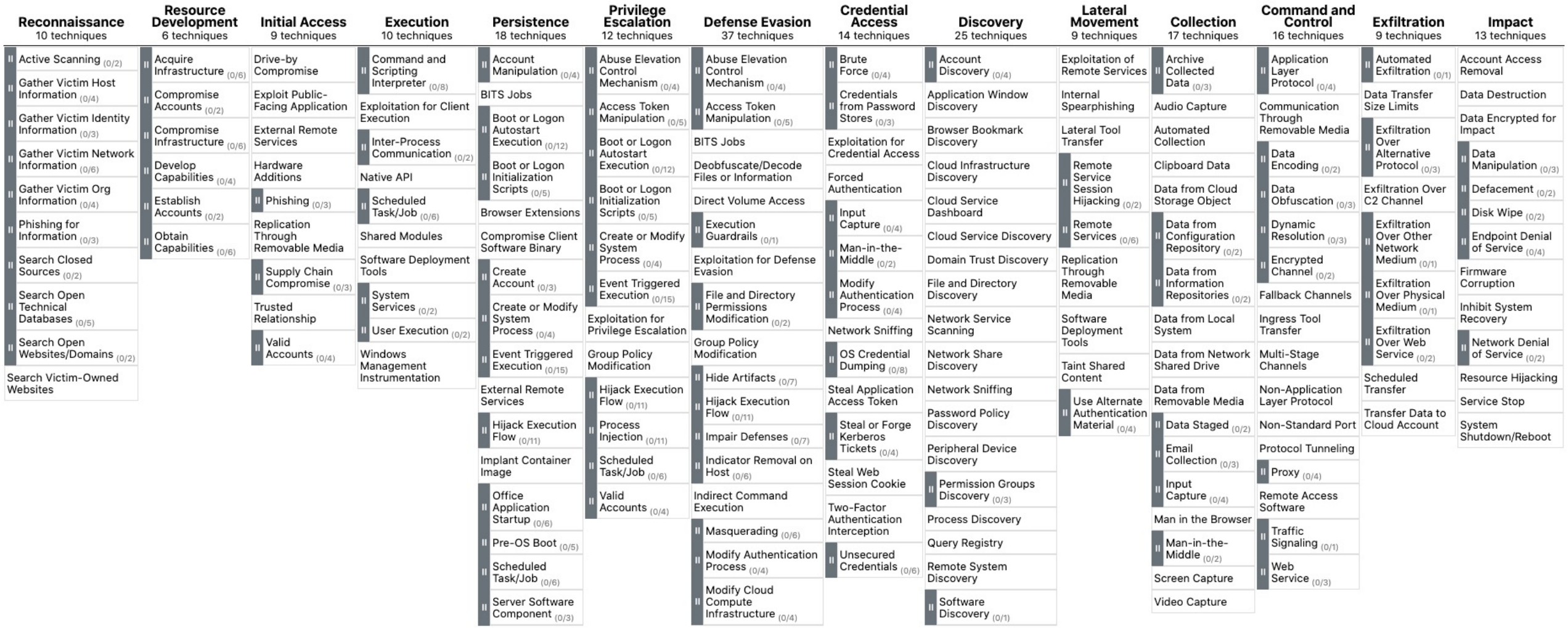


Αλυσίδα καταστροφής απειλών



MITRE ATT&CK

MITRE **A**dversarial **T**actics, **T**echniques, and **C**ommon **K**nowledge (ATT&CK)



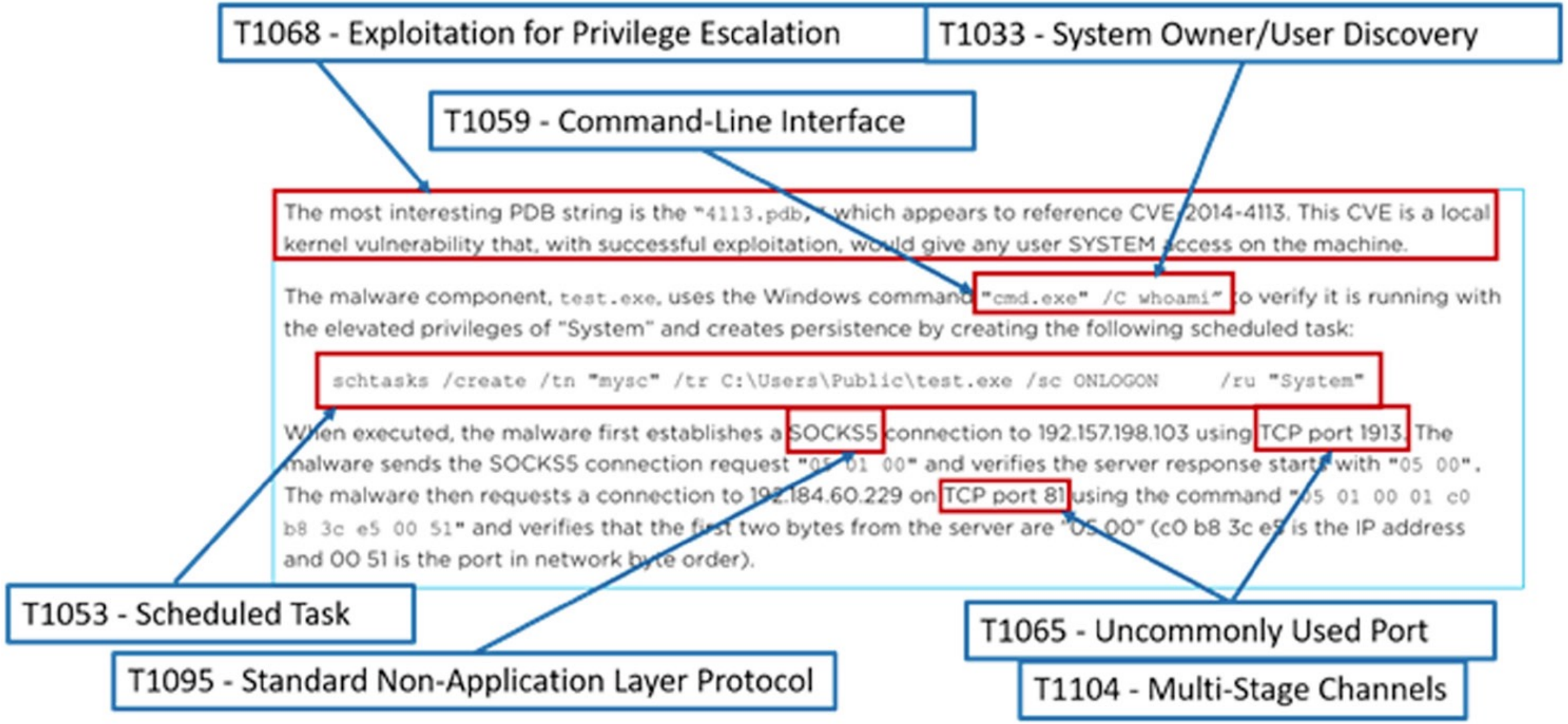
Στοιχεία ATT&CK

- Βάσεις/μήτρες [matrices]
  - Επιχειρησιακή [Enterprise]
    - Windows, macOS, Linux, PRE, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Network, Containers
  - Κινητών συσκευών [Mobile]
    - Android, iOS
  - Βιομηχανικών συστημάτων ελέγχου [Industrial Control Systems (ICS)]
    - SCADA, Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), etc.
- Τακτικές [tactics]
  - Λόγος/σκοπός επίθεσης
- Τεχνικές [techniques]
  - Τρόπος εκδήλωσης επίθεσης

Στοιχεία ATT&CK

- Πηγές δεδομένων [data sources]
  - Κατηγορίες δεδομένων από αισθητήρες/καταγραφή
  - Πηγές δεδομένων που σχετίζονται με τον εντοπισμό μιας τεχνικής ATT&CK
- Μετριάσεις [mitigations]
  - Μέτρα αποφυγής ή περιορισμού μίας τεχνικής
  - Επιχειρησιακές [Enterprise]
  - Κινητών συσκευών [Mobile]
- Ομάδες [groups]
- Λογισμικό [software]

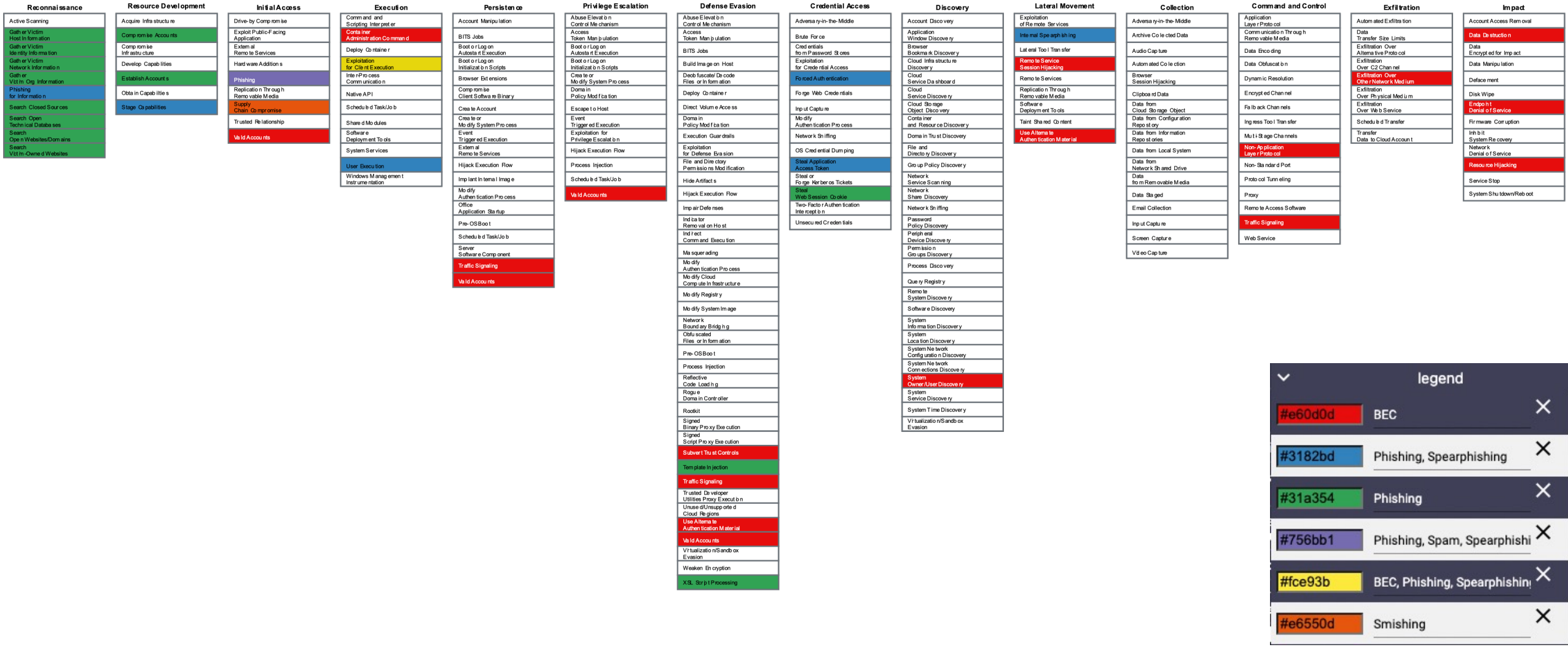
ATT&CK από αναφορά



E-mail related threats [1]

about
E-mail

domain
Enterprise ATT&CK v10



E-mail related threats [2]

about
E-mail

domain
Mobile ATT&CK v10

Initial Access
- Deliver Malicious App via Authorized App Store
- Deliver Malicious App via Other Means
- Drive-by Compromise
- Exploit via Charging Station or PC
- Exploit via Radio Interfaces
- Install Insecure or Malicious Configuration
- Lockscreen Bypass
- Masquerade as Legitimate Application
- Supply Chain Compromise

Execution
- Broadcast Receivers
- Command-Line Interface
- Native Code
- Scheduled Task/Job

Persistence
- Broadcast Receivers
- Code Injection
- Compromise Application Executable
- Foreground Persistence
- Modify Cached Executable Code
- Modify OS Kernel or Boot Partition
- Modify System Partition
- Modify Trusted Execution Environment
- Scheduled Task/Job

Privilege Escalation
- Code Injection
- Device Administrator Permissions
- Exploit OS Vulnerability
- Exploit TEE Vulnerability

Defense Evasion
- Application Discovery
- Code Injection
- Delete Device Data
- Device Lockout
- Disguise Root/Jailbreak Indicators
- Download New Code at Runtime
- Evade Analysis Environment
- Geofencing
- Hooking
- Input Injection
- Install Insecure or Malicious Configuration
- Masquerade as Legitimate Application
- Modify OS Kernel or Boot Partition
- Modify System Partition
- Modify Trusted Execution Environment
- Native Code
- Obfuscated Files or Information
- Proxy Through Victim
- Suppress Application Icon
- Uninstall Malicious Application
- User Evasion

Credential Access
- Access Notifications
- Access Sensitive Data in Device Logs
- Access Stored Application Data
- Capture Clipboard Data
- Capture SMS Messages
- Exploit TEE Vulnerability
- Input Capture
- Input Prompt
- Keychain
- Network Traffic Capture or Redirection
- URI Hijacking

Discovery
- Application Discovery
- Evade Analysis Environment
- File and Directory Discovery
- Location Tracking
- Network Service Scanning
- Process Discovery
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery

Lateral Movement
- Attack PC via USB Connection
- Exploit Enterprise Resources

Collection
- Access Calendar Entries
- Access Call Log
- Access Contact List
- Access Notifications
- Access Sensitive Data in Device Logs
- Access Stored Application Data
- Call Control
- Capture Audio
- Capture Camera
- Capture Clipboard Data
- Capture SMS Messages
- Data from Local System
- Foreground Persistence
- Input Capture
- Location Tracking
- Network Information Discovery
- Network Traffic Capture or Redirection
- Screen Capture

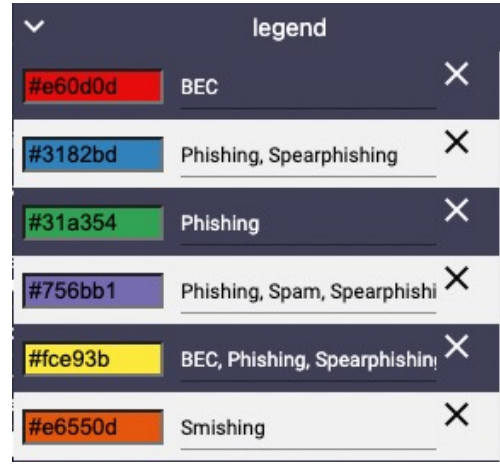
Command and Control
- Alternate Network Mediums
- Call Control
- Commonly Used Port
- Domain Generation Algorithms
- Remote File Copy
- Standard Application Layer Protocol
- Standard Cryptographic Protocol
- Uncommonly Used Port
- Web Service

Exfiltration
- Alternate Network Mediums
- Commonly Used Port
- Data Encrypted
- Standard Application Layer Protocol

Impact
- Call Control
- Carrier Billing Fraud
- Clipboard Modification
- Data Encrypted for Impact
- Delete Device Data
- Device Lockout
- Generate Fraudulent Advertising Revenue
- Input Injection
- Manipulate App Store Rankings or Ratings
- Modify System Partition
- SMS Control

Network Effects
- Downgrade to Insecure Protocols
- Eavesdrop on Insecure Network Communication
- Exploit SS7 to Redirect Phone Calls/SMS
- Exploit SS7 to Track Device Location
- Jamming or Denial of Service
- Manipulate Device Communication
- Rogue Cellular Base Station
- Rogue Wi-Fi Access Points
- SIM Card Swap

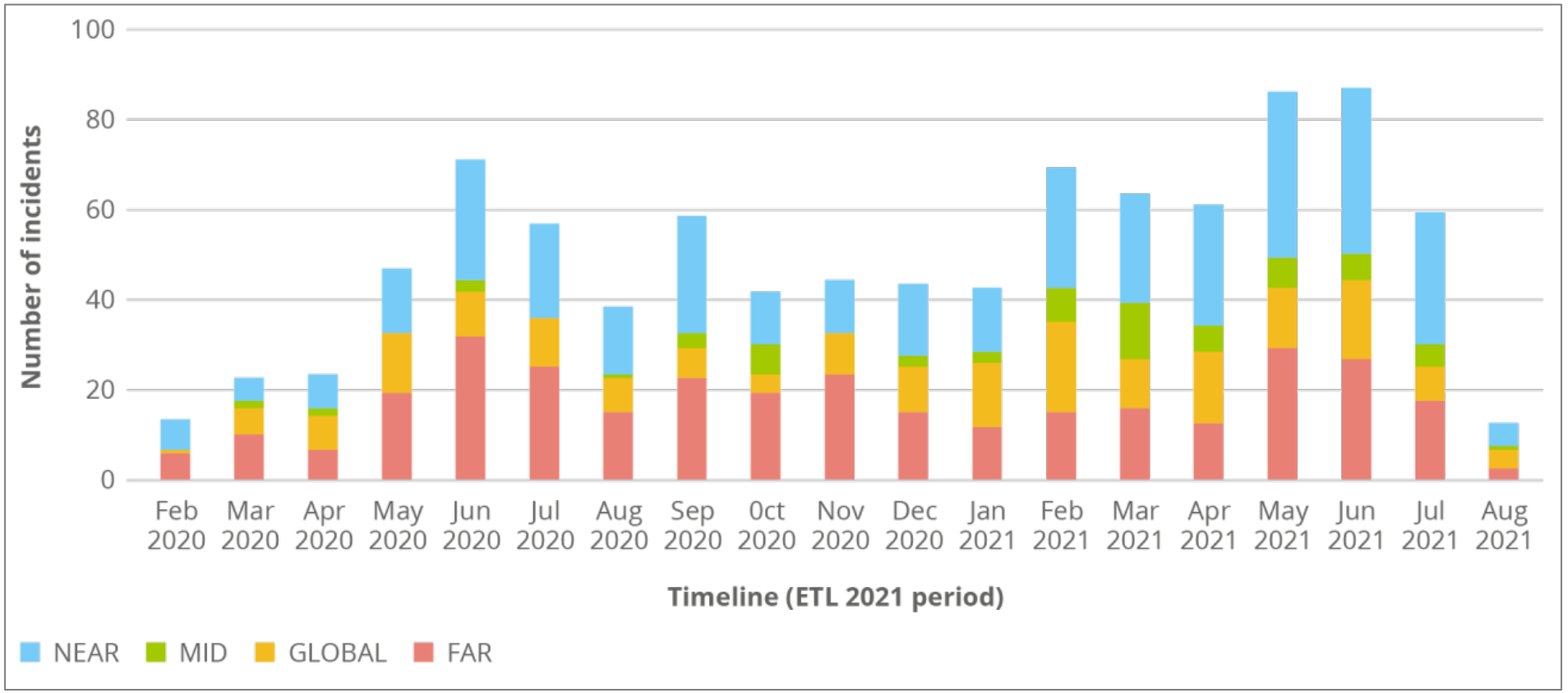
Remote Service Effects
- Obtain Device Cloud Backups
- Remotely Track Device Without Authorization
- Remotely Wipe Data Without Authorization



Αναφορές Περιστατικών Ασφάλειας

Αναφορικά στοιχεία 2021

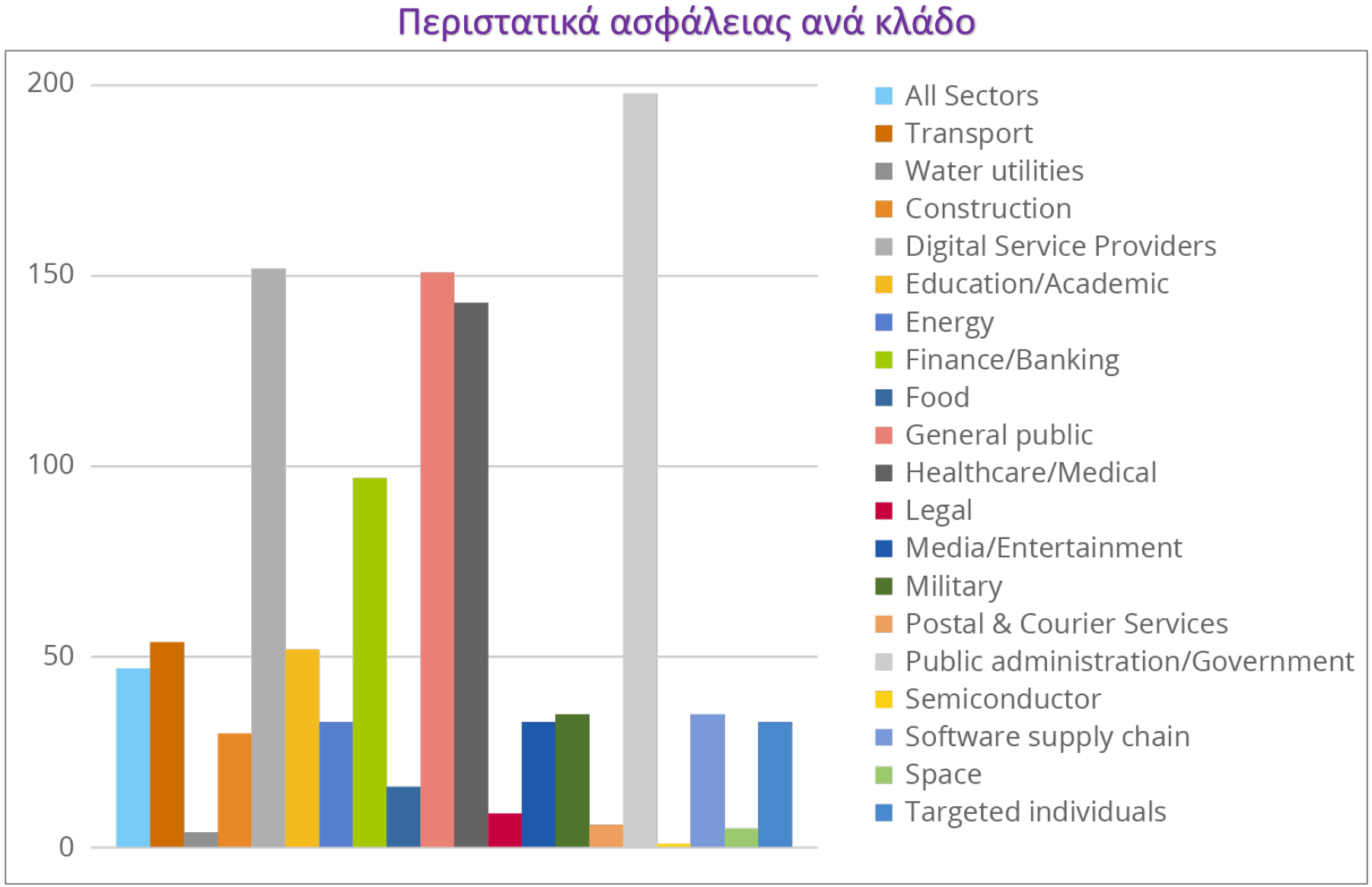
ETL 2021



Χρονοδιάγραμμα καταμερισμού περιστατικών

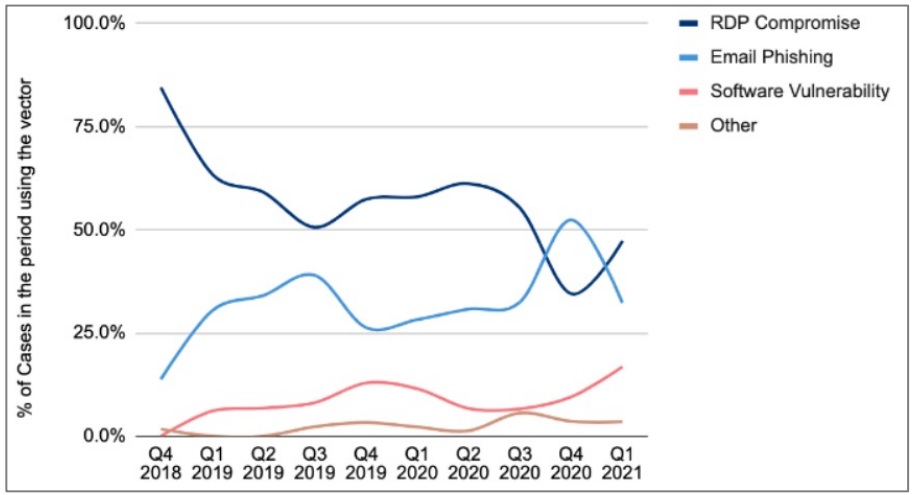
Near: Εντός ΕΕ
Mid: Εντός ΕΕ και συνοριακά (Ευρωπαϊκές χώρες εκτός ΕΕ, Ισραήλ, Τουρκία, κ.λπ.)
Global: Παγκόσμια
Far: Ασία, Βόρεια και Νότια Αμερική, Ωκεανία

ETL 2021


Περιστατικά ασφάλειας ανά κλάδο
200
150
100
50
0
All Sectors
Transport
Water utilities
Construction
Digital Service Providers
Education/Academic
Energy
Finance/Banking
Food
General public
Healthcare/Medical
Legal
Media/Entertainment
Military
Postal & Courier Services
Public administration/Government
Semiconductor
Software supply chain
Space
Targeted individuals

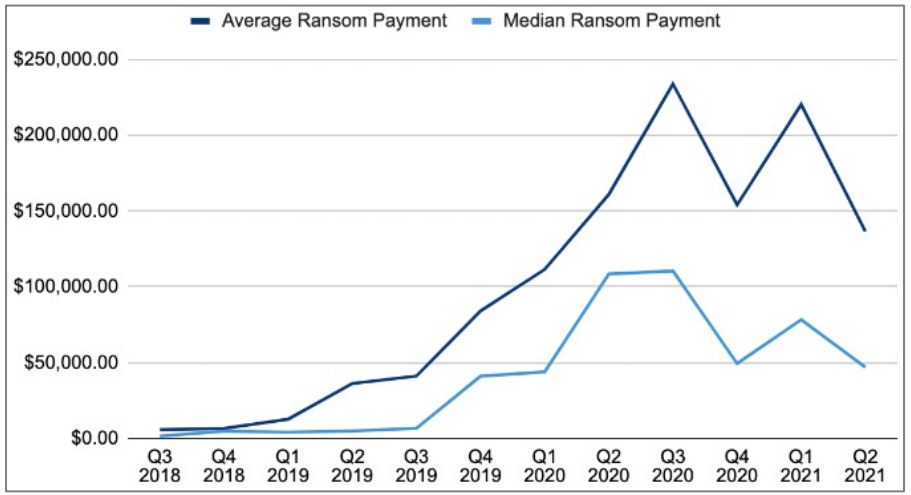
Ransomware 2021

Φορείς επιθέσεων



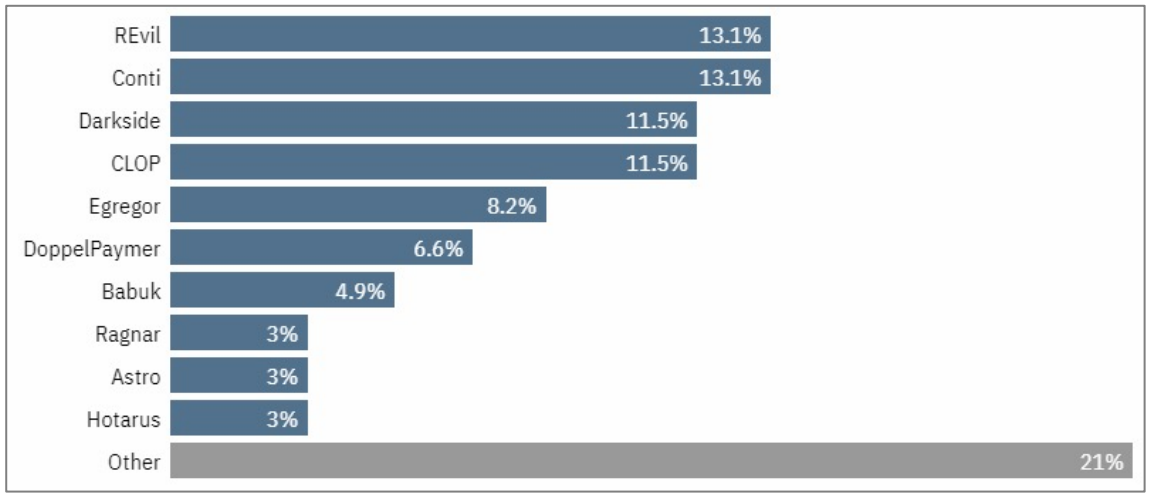
Πoσoστό περιστατικών ανά φορέα (vector)

Κόστος επιθέσεων



Μέσος όρος καταβληθέντων ποσών (average) και μέσο ποσό καταβολής λύτρων (median)

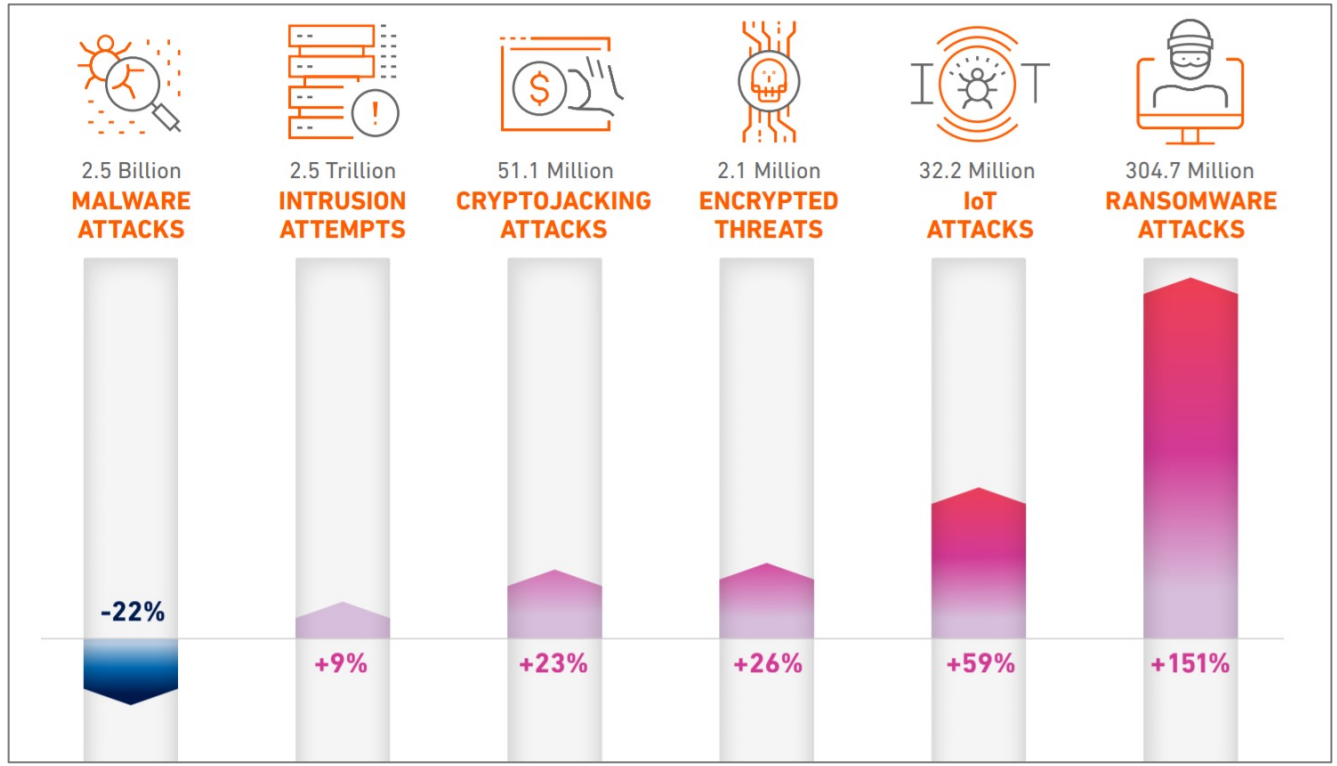
Αποτελεσματικότητα εργαλείων



Ποσοστό απώλειας δεδομένων ανά εργαλείο

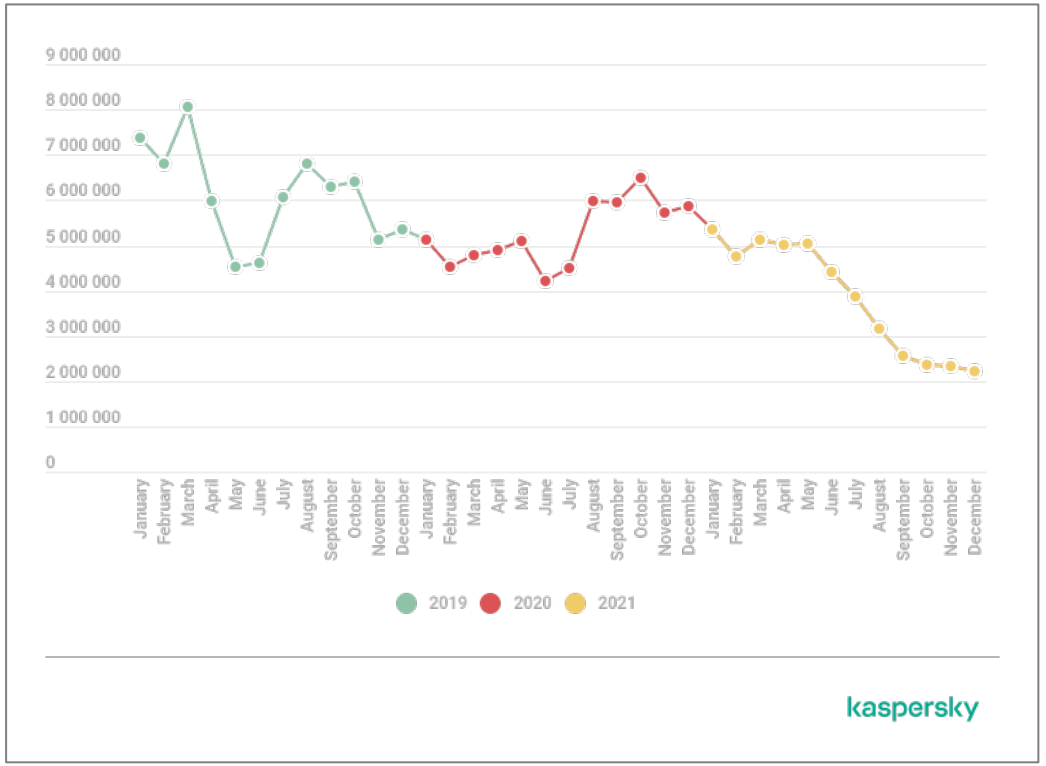
Malware 2021

Τάση επιθέσεων



Ποσοστό ανόδου/πτώσης επιθέσεων ανά κατηγορία

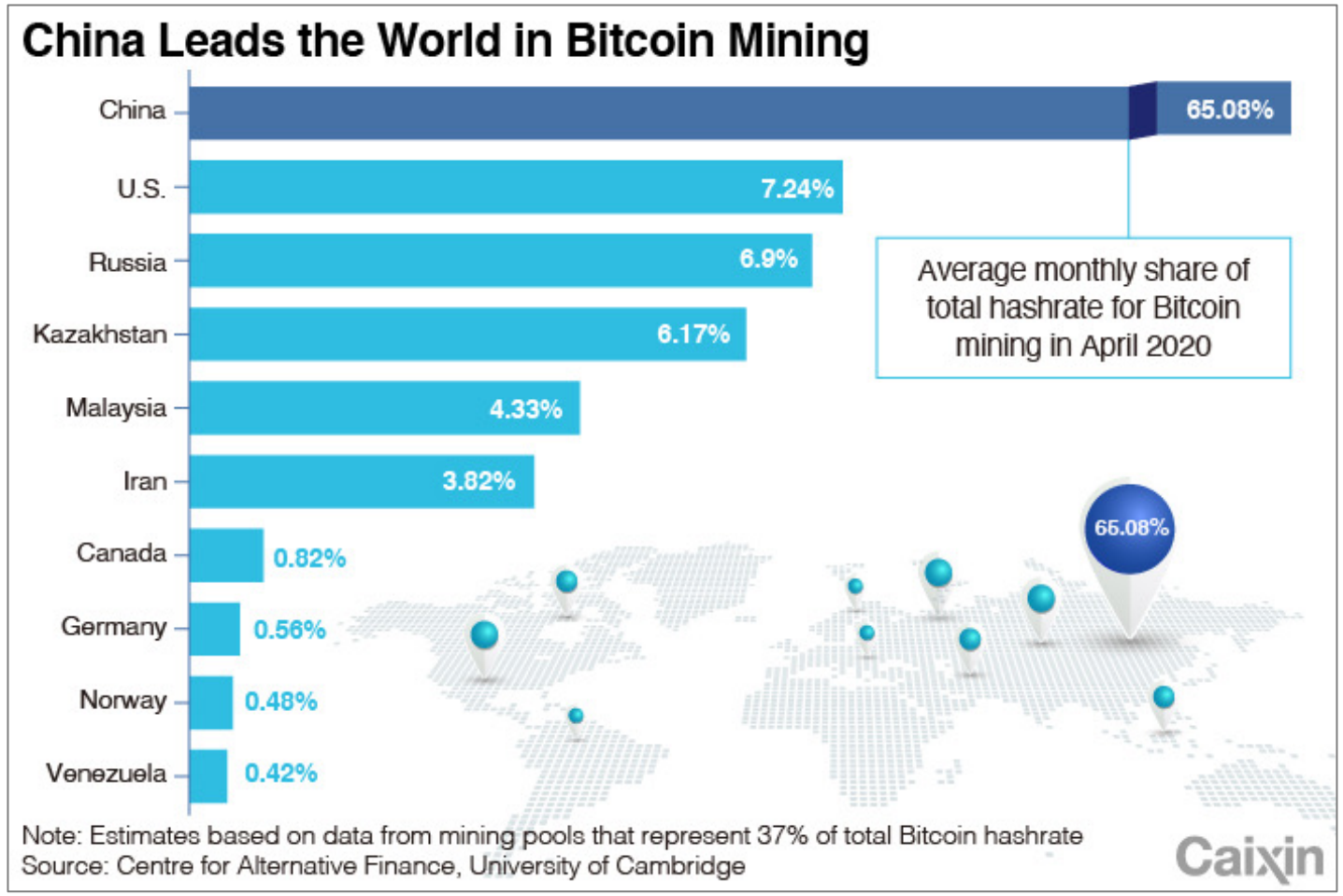
Κακόβουλο λογισμικό κινητών



Πλήθος επιθέσεων ανά μήνα

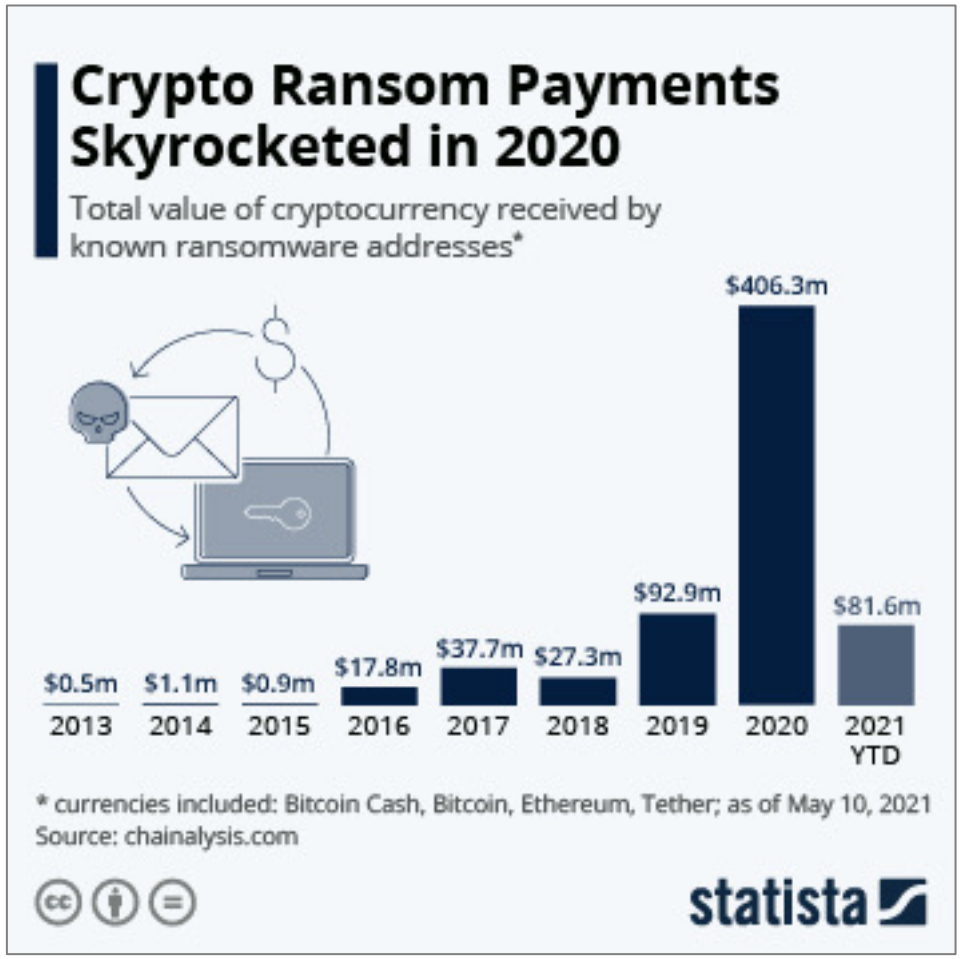
Cryptojacking 2021

Γεωπολιτικά χαρακτηριστικά



Μηνιαίο ποσοστό ανά χώρα

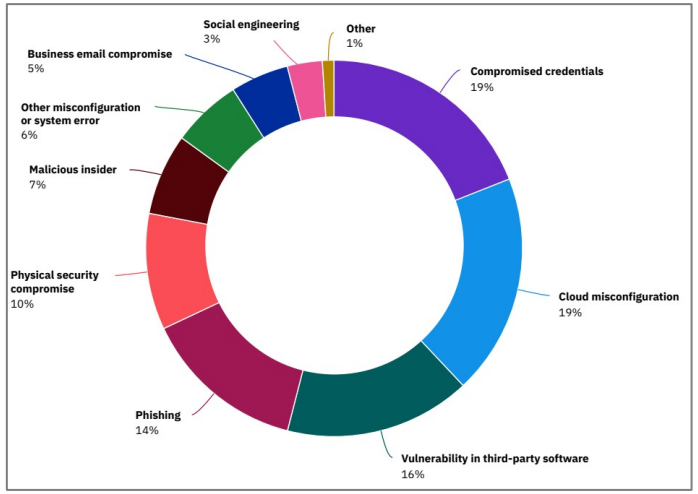
Κόστος επιθέσεων



Ποσά καταβληθέντων λύτρων σε κρυπτονόμισμα

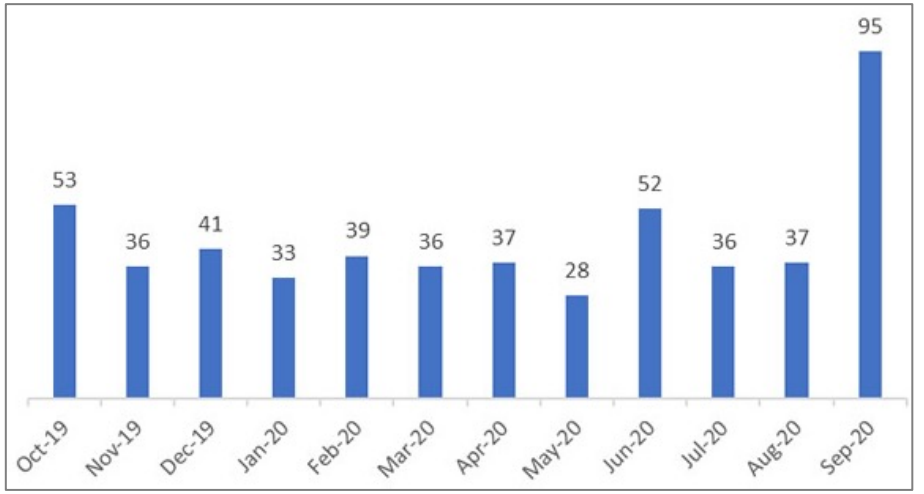
E-mail related threats 2021

Παραβίαση δεδομένων



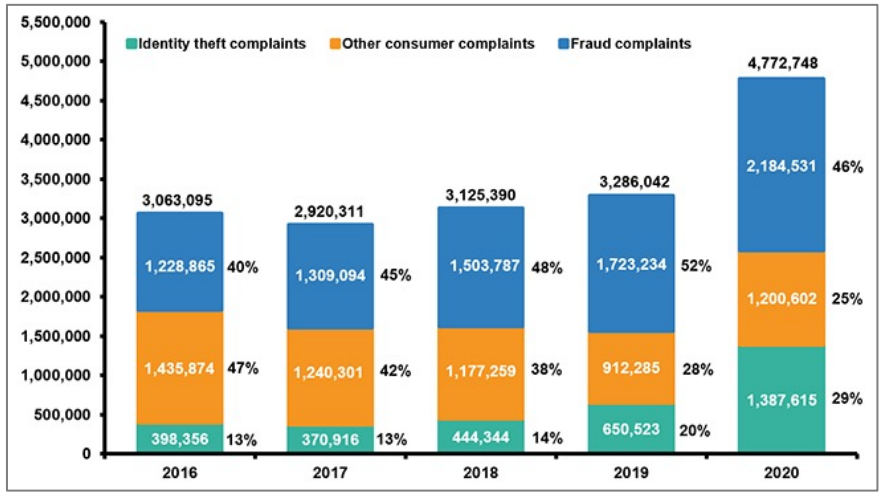
Ποσοστό απωλειών δεδομένων ανά φορέα (vector)

Παραβίαση δεδομένων υγείας



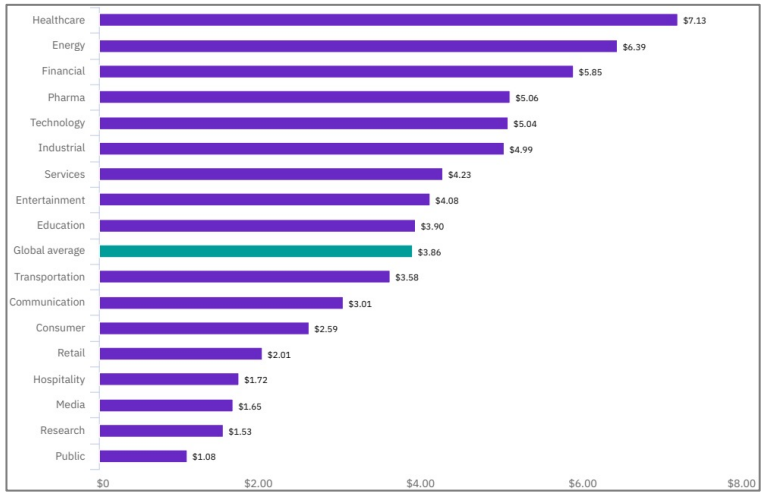
Όγκος απολεσθέντων δεδομένων ανά μήνα

Κλοπές στοιχείων ταυτότητας



Κλοπές στοιχείων ταυτότητας και απάτες ανά έτος

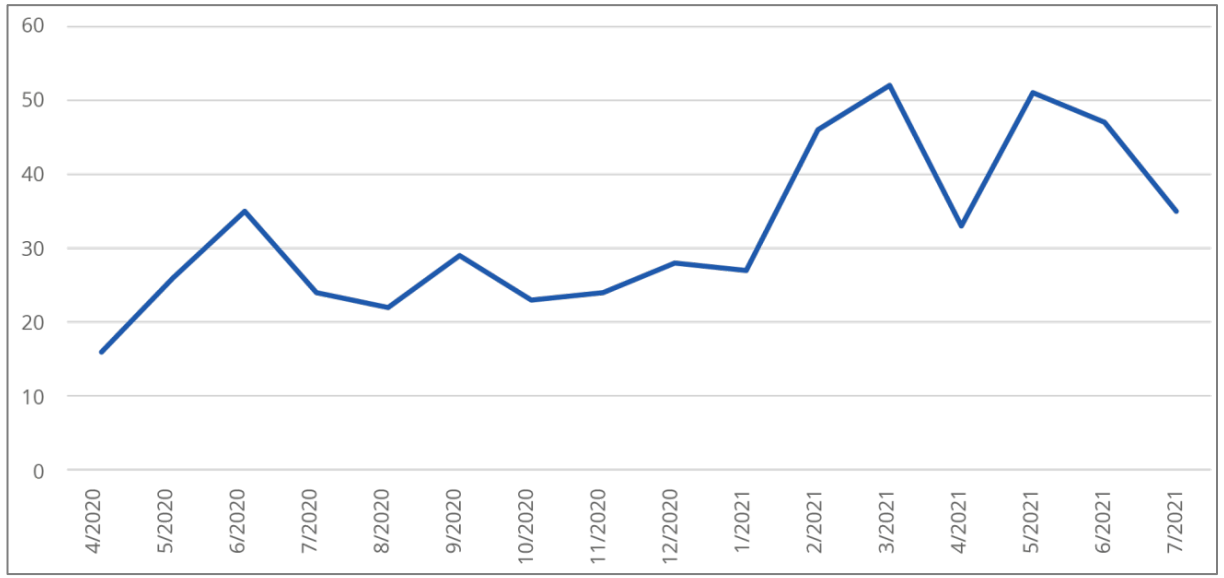
Παραβιάσεις δεδομένων ανά κλάδο



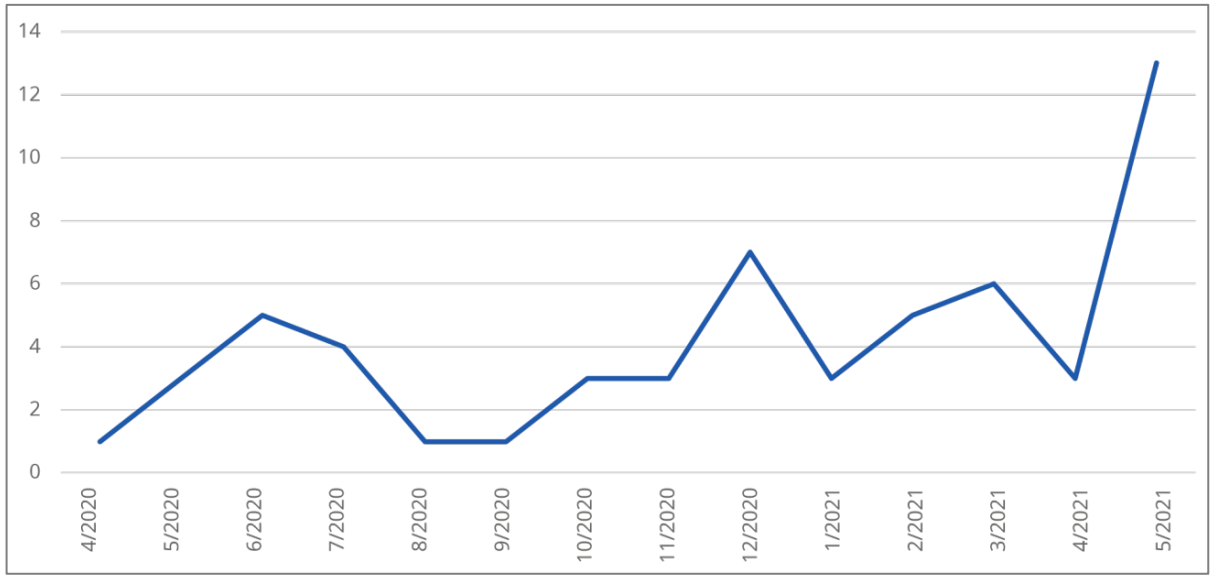
Μέσος όρος συνολικού κόστους λόγω παραβίασης δεδομένων

Threats against data 2021

Περιστατικά απειλών δεδομένων



Περιστατικά απειλών δεδομένων υγείας



Περιστατικά ανά μήνα Απρ. 2020 – Ιουλ. 2021

Αξιοσημείωτες πηγές

Εταιρίες του κλάδου κυβερνο-ασφάλειας

- Fortinet
- Kaspersky Lab
- McAfee, Inc.
- NortonLifeLock Inc. - Symantec
- Proofpoint, Inc.
- Sophos Group Plc

Κατασκευάστριες υλικού ή λογισμικού

- Carbon Black, Inc.
- Cisco Systems, Inc.
- Computer Associates International, Inc. - CA
- IBM Security Systems
- Splunk, Inc.

Αξιοσημείωτες πηγές

Εταιρίες του κλάδου τηλεπικοινωνιών

- AT&T Inc.
- Cellco Partnership, Inc. - Verizon Wireless
- Deutsche Telekom AG
- Verizon Communications Inc.
- Vodafone Group Plc

Διεθνείς ή κρατικοί οργανισμοί

- ENISA, EU
- Europol’s European Cybercrime Center (EC3)
- European Defence Agency, EU
- National Cyber Security Centre, UK
- National Security Agency, USA
- NATO Communications and Information Agency
- United States Department of Homeland Security, USA

Αξιοσημείωτες πηγές

Ηλεκτρονικός τύπος

- BankInfoSecurity.com
- ComputerWeekly.com
- HelpNetSecurity.com
- NewsWeek.com
- SecuringTomorrow.mcafee.com
- SecurityWeek.com
- CNN news
- CBN news
- BBC news Cyber-security
- CNET Security

Darknet

- DarkReading.com
- Explore at your own risk

Αναφορές Περιστατικών Ασφάλειας

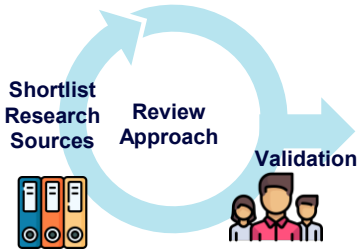
Χάρτες επιθέσεων σε πραγματικό χρόνο

Χάρτες επιθέσεων σε πραγματικό χρόνο

- *Kaspersky Lab cyber attack map:* https://cybermap.kaspersky.com/
- *Deteque botnet threat map:* https://www.deteque.com/live-threat-map/
- *Fortinet live cyber attack map:* https://threatmap.fortiguard.com/
- *FireEye real-time cyber attack map:* https://www.fireeye.com/cyber-map/threat-map.html
- *Bitdefender live cyber threat map:* https://threatmap.bitdefender.com/
- SonicWall live cyber attacks map: https://securitycenter.sonicwall.com/m/page/worldwide-attacks

Project Methodology

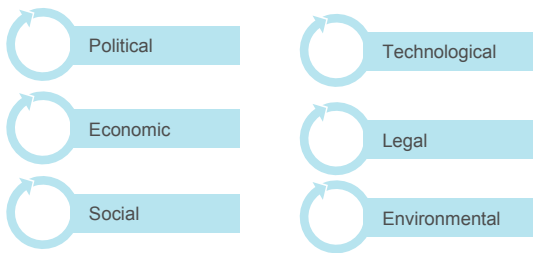
Online Survey



For each PESTLE dimension, the *Foresight working group* will:

- Review the material on trends
- Will provide feedback on the relevance of each trend and propose any changes needed to the compilation of trend candidates

Delphi Workshops

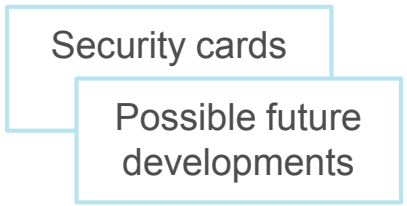


For each workshop 3-8 participants of the *PESTLE working group*: highly diverse, multidisciplinary backgrounds.

Tasks in the workshop:

- Review the gathered information and feedback
- Discuss, explore and reevaluate the assessments for each trend

Threat identification Workshop

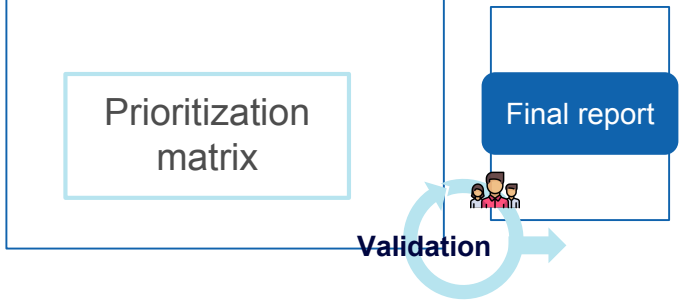


Participants: 8 stakeholders of the *security/ ENISA strategist working group:* expertise in cybersecurity, business, technology, psychology/sociology, etc.

Tasks of the workshop:

1. Focus on the main character of the SFP
2. Shift to the perspective of an adversary;
3. The team will try to identify what systems need to be in place to successfully launch an attack
4. What vulnerabilities there may be to facilitate such an attack

Threat prioritization workshop



Participants: stakeholders of the *security/ ENISA strategist working group:*

Tasks of the workshop:

- Prioritization on a matrix: likelihood of occurrence, novelty of that threat, the severity of the consequences (impact)

ENISA working groups

References

1. Jõgi, K. (2015). Inventory of CERT teams and activities in Europe. [online] European Union Agency For Network And Information Security (ENISA). Available at: https://www.enisa.europa.eu/publications/inventory-of-cert-activities-in-europe
2. European Union Agency for Cybersecurity (ENISA), (2022), CSIRTs by Country - Interactive Map, https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#country=
3. MITRE ATT&CK knowledge base *MITRE ATT&CK®*, https://attack.mitre.org/
4. ATT&CK® Navigator https://mitre-attack.github.io/attack-navigator/
5. Using ATT&CK for Cyber Threat Intelligence Training, https://attack.mitre.org/resources/training/cti/
6. Pennington, A., Applebaum, A., Nickels, K., Schulz, T., Strom, B. and Wunder, J., (2019), Getting Started with ATT&CK, https://www.mitre.org/sites/default/files/publications/mitre-getting-started-with-attack-october-2019.pdf