

# Αναφορές Περιστατικών Ασφάλειας

Καθ. Χρ. Δουληγέρης

Z. Γαροφαλάκη, [z.garofalaki@unipi.gr](mailto:z.garofalaki@unipi.gr)

# Αναφορές Περιστατικών Ασφάλειας

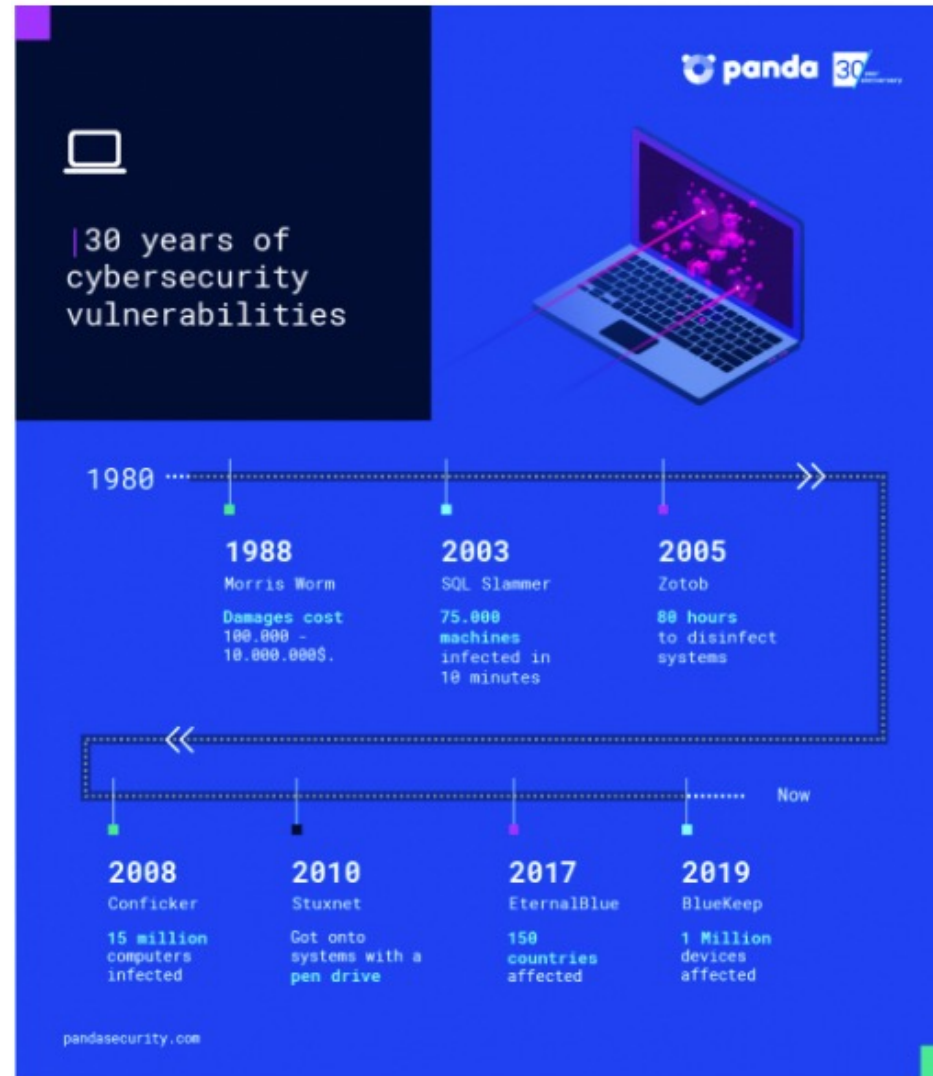
Ιστορικά στοιχεία, Κυβερνο-απειλές, Κατηγορίες επιτιθέμενων, Αλυσίδα καταστροφής, MITRE ATT&CK, Αναφορικά στοιχεία 2021, Χάρτες επιθέσεων σε πραγματικό χρόνο

# 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

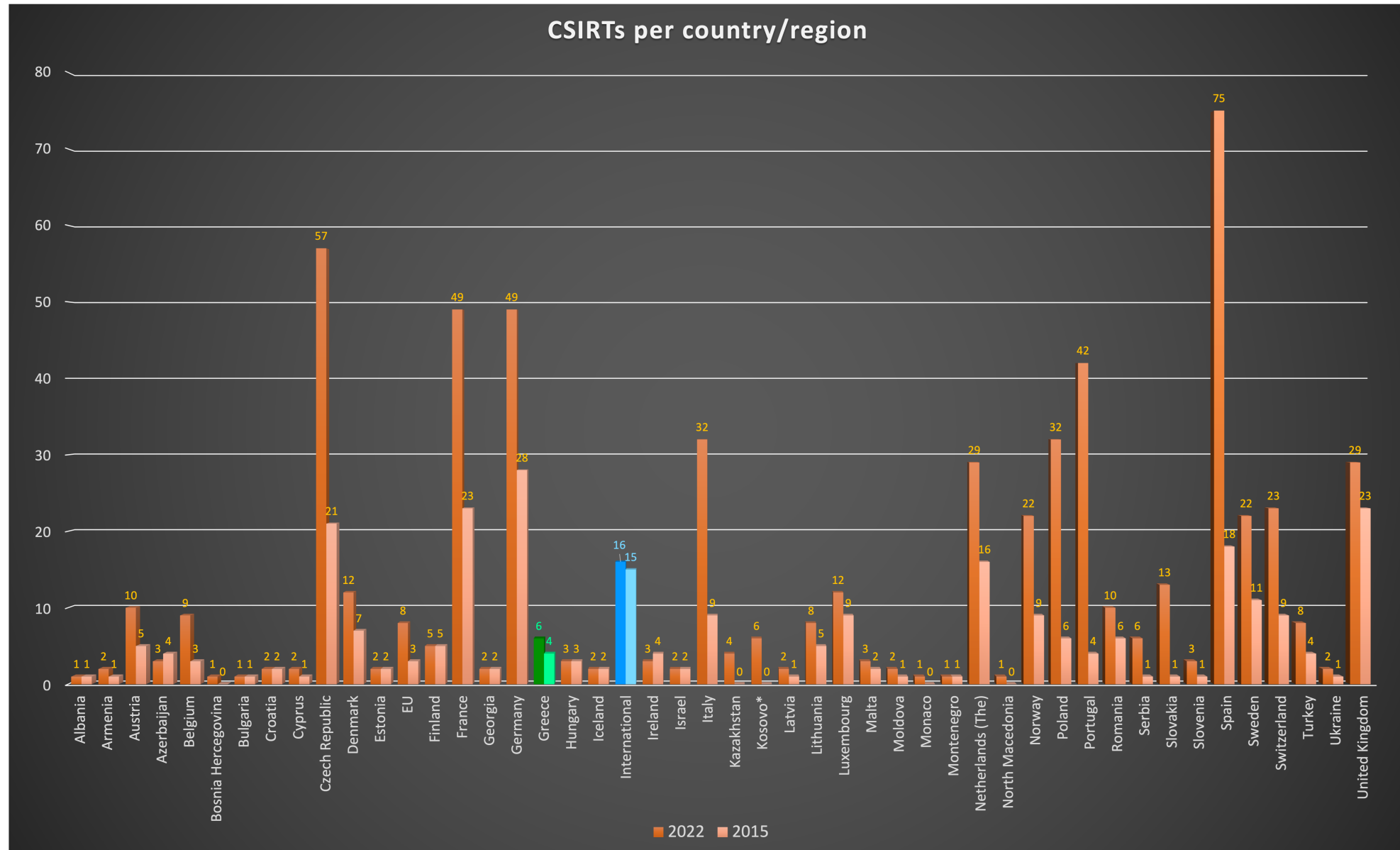
## **Σύσταση της πρώτης CSIRT μόλις λίγες μέρες μετά το Περιστατικό Morris**

- 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	<a href="http://auth.gr">auth.gr</a>
FORTHcert	FOUNDATION OF RESEARCH AND TECHNOLOGY CERT (formerly FORTH CERT)	Service Provider Customer Base	<a href="http://forth.gr/forthcert/">forth.gr/forthcert/</a>
GRNET-CERT	GRNET-CERT	NREN	<a href="http://cert.grnet.gr">cert.grnet.gr</a>
NCERT-GR	Greek National Authority Against Electronic Attacks	Government, National	<a href="http://cert.gov.gr">cert.gov.gr</a>
<b>AB-CSIRT</b>	<b>Alpha Bank Computer Security Incident Response Team</b>	<b>Financial</b>	<a href="http://alpha.gr">alpha.gr</a>
<b>GR-CSIRT</b>	<b>Hellenic Cyber Security Incident Response Team</b>	<b>Government</b>	<a href="http://csirt.cd.mil.gr/">csirt.cd.mil.gr/</a>



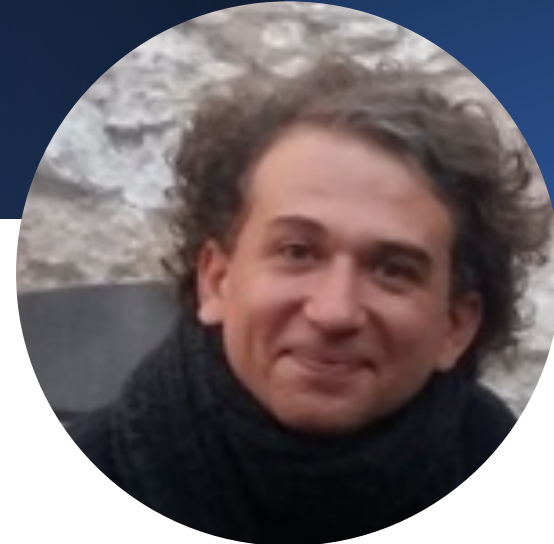
## UPRC team



**Χρ. Δουληγιέρης**  
Καθηγητής  
Πανεπιστήμιο Πειραιά  
cdoulig@unipi.gr



**Ζαχ. Γαροφαλάκη**  
Διδακτορική ερευνήτρια  
Πανεπιστήμιο Πειραιά  
z.garofalaki@uniwa.gr

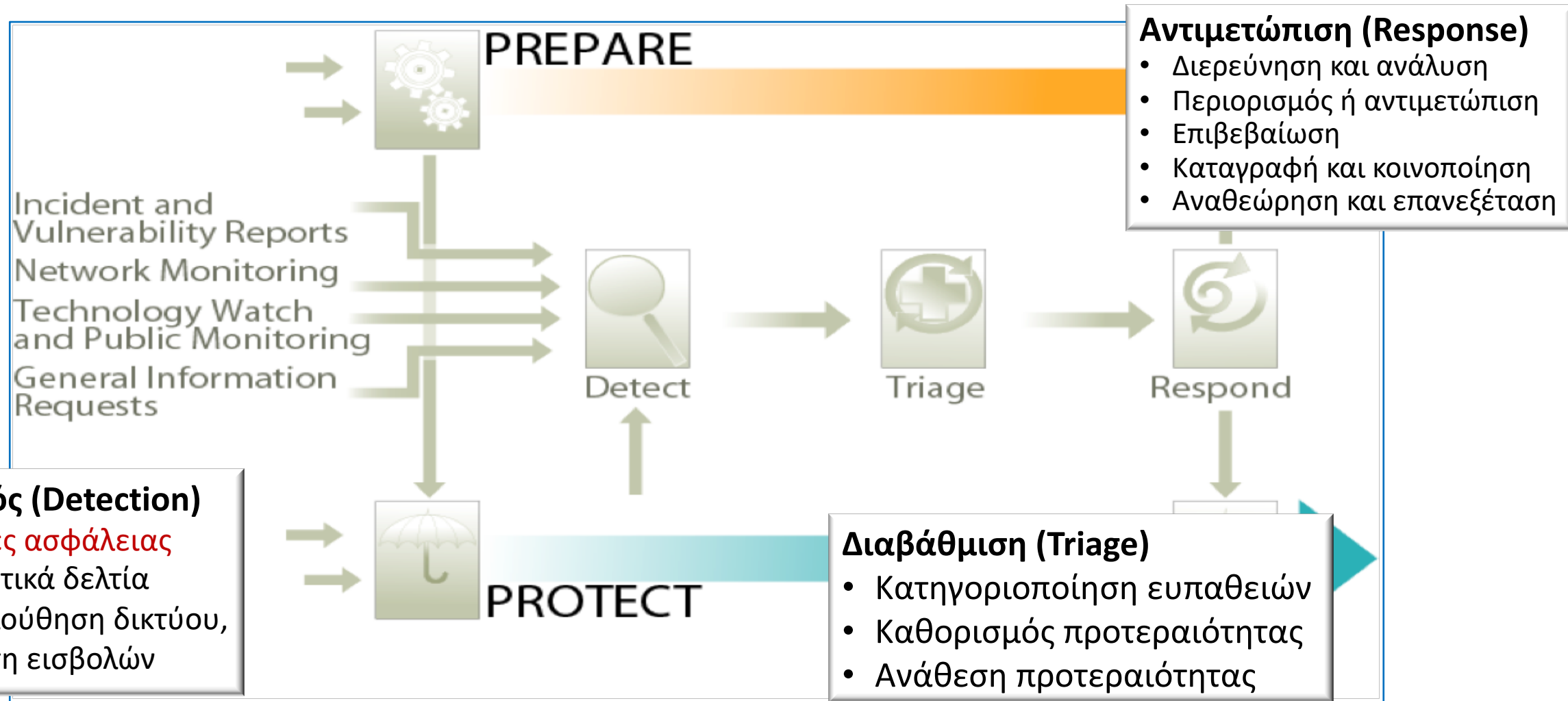


**Δημ. Καλλέργης**  
Λέκτορας  
Πανεπιστήμιο Δυτικής Αττικής  
d.kallergis@uniwa.gr

# Αναφορές Περιστατικών Ασφάλειας

Κυβερνο-απειλές

# Αναφορές και διαχείριση περιστατικών



## Μοντέλο βέλτιστης πρακτικής διαχείρισης περιστατικών

# 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	Drive-by Exploits	Web-based attacks <sup>[5]</sup>
Worms/Trojans	Malicious Code: Worms/Trojans	Malicious Code: Worms/Trojans
Code Injection Attacks	Code Injection Attacks	Code Injection Attacks/Injection attacks <sup>[6]</sup>
Exploit Kits	Exploit Kits	
Botnets		
Denial of service		

**Edward Snowden: the whistleblower behind the NSA surveillance revelations**

Until very recently, the source of the data sold by SSNDOB had remained hidden. It began to unravel in March 2013, when teenage hackers allegedly associated with the group UGNazi showed just how deeply the service's access went. The young hackers used 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.

- 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 Service (SSNDOB)  
 [4] Replaced 2012 Search Engine Poisoning

[9] The Snowden revelations in 2013-2014

# Ταξινόμηση ENISA 2014-2020

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

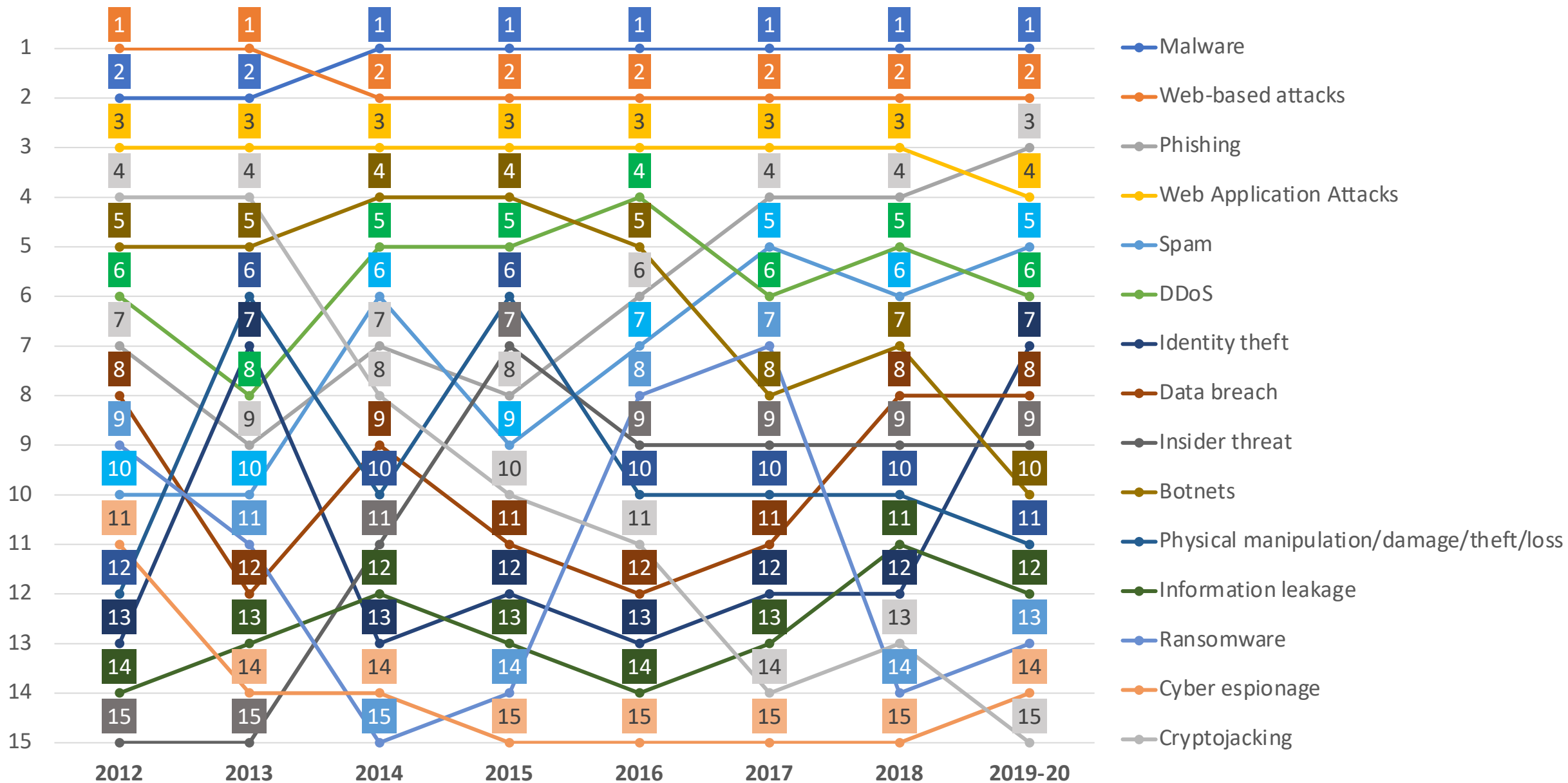
[12] 2016 ATM fraud

[13] 2018: Year of cryptojacking (600% more attacks than in 2017)

# Νέα ταξινόμηση 2021-...

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

# Κατάταξη απειλών 2014-2020



# Αναφορές Περιστατικών Ασφάλειας

Κατηγορίες επιτιθέμενων

# Κατηγορίες επιτιθέμενων

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



# Τάσεις επιτιθέμενων

	Cyber-criminals	Insiders	Nation states	Corporations	Hacktivists	Cyber-terrorists	Script kiddies
Malware	Dark	Light	Dark	Dark	Light	Light	Light
Web Based Attacks	Dark	White	Dark	Dark	Dark	Dark	Light
Web Application Attacks	Dark	White	Dark	Dark	Dark	Light	Light
Phishing	Dark	Dark	Dark	Dark	Dark	White	Light
Denial of Service	Dark	White	Light	Light	Dark	Light	Dark
Spam	Light	Dark	Light	Light	White	White	White
Botnets	Dark	White	Dark	Dark	Light	Dark	Light
Data Breaches	Dark	Dark	Dark	Dark	Dark	Dark	Light
Insider Threat	Dark	White	Light	Dark	White	Light	White
Physical manipulation/damage/theft	Dark	Dark	Dark	Dark	Light	Light	Light
Information Leakage	Dark	Light	Dark	Dark	Light	Light	Light
Identity Theft	Dark	Dark	Dark	Dark	Dark	Light	Light
Cryptojacking	Dark	Dark	Light	Light	White	White	Dark
Ransomware	Dark	Light	Dark	Dark	White	White	Light
Cyber Espionage	White	Light	Light	Light	White	White	White



# 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

	Reconnaissance	Weaponisation	Delivery	Exploitation	Installation	Command and Control	Actions on Targets
Malware							
Web Based Attacks							
Web Application Attacks							
Phishing							
Denial of Service							
Spam							
Botnets							
Data Breaches							
Insider Threat							
Physical manipulation/damage/theft							
Information Leakage							
Identity Theft							
Cryptojacking							
Ransomware							
Cyber Espionage							

# MITRE ATT&CK

## MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)

Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/4)	Exploitation of Remote Services	Archive Collected Data (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (0/12)	Boot or Logon Autostart Execution (0/12)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Clipboard Data	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Scheduled Task/Job (0/6)	Browser Extensions	Boot or Logon Initialization Scripts (0/5)	Direct Volume Access	Input Capture (0/4)	Cloud Service Dashboard	Remote Services (0/6)	Data from Cloud Storage Object	Data Obfuscation (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Create or Modify System Process (0/4)	Execution Guardrails (0/1)	Man-in-the-Middle (0/2)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (0/2)	Dynamic Resolution (0/3)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)		Supply Chain Compromise (0/3)	Software Deployment Tools	Event Triggered Execution (0/15)	Event Triggered Execution (0/15)	Exploitation for Defense Evasion	Modify Authentication Process (0/4)	Domain Trust Discovery	Software Deployment Tools	Data from Information Repositories (0/2)	Encrypted Channel (0/2)	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)		Trusted Relationship	System Services (0/2)	Create Account (0/3)	Create or Modify System Process (0/4)	File and Directory Permissions Modification (0/2)	Network Sniffing	File and Directory Discovery	Taint Shared Content	Data from Local System	Fallback Channels	Exfiltration Over Web Service (0/2)	Firmware Corruption
Search Open Websites/Domains (0/2)		Valid Accounts (0/4)	User Execution (0/2)	Create or Modify System Process (0/4)	Event Triggered Execution (0/15)	Group Policy Modification	OS Credential Dumping (0/8)	Network Service Scanning	Use Alternate Authentication Material (0/4)	Data from Network Shared Drive	Ingress Tool Transfer	Exfiltration Over Web Service (0/2)	Inhibit System Recovery
Search Victim-Owned Websites			Windows Management Instrumentation	Event Triggered Execution (0/15)	External Remote Services	Group Policy Modification	Steal Application Access Token	Network Share Discovery		Data from Removable Media	Multi-Stage Channels	Scheduled Transfer	Network Denial of Service (0/2)
				Hijack Execution Flow (0/11)	Hijack Execution Flow (0/11)	Hijack Execution Flow (0/11)	Steal or Forge Kerberos Tickets (0/4)	Network Sniffing		Data from Removable Media	Non-Application Layer Protocol	Transfer Data to Cloud Account	Resource Hijacking
				Hijack Execution Flow (0/11)	Process Injection (0/11)	Impair Defenses (0/7)	Steal Web Session Cookie	Password Policy Discovery		Data Staged (0/2)	Non-Standard Port		Service Stop
				Implant Container Image	Scheduled Task/Job (0/6)	Indicator Removal on Host (0/6)	Two-Factor Authentication Interception	Peripheral Device Discovery		Email Collection (0/3)	Protocol Tunneling		System Shutdown/Reboot
				Office Application Startup (0/6)	Valid Accounts (0/4)	Indirect Command Execution	Unsecured Credentials (0/6)	Permission Groups Discovery (0/3)		Input Capture (0/4)	Remote Access Software		
				Pre-OS Boot (0/5)		Masquerading (0/6)		Process Discovery		Man in the Browser	Traffic Signaling (0/1)		
				Scheduled Task/Job (0/6)		Modify Authentication Process (0/4)		Query Registry		Man-in-the-Middle (0/2)	Web Service (0/3)		
				Server Software Component (0/3)		Modify Cloud Compute Infrastructure (0/4)		Remote System Discovery		Screen Capture			
								Software Discovery (0/1)		Video Capture			

# Στοιχεία ΑΤΤ&Κ

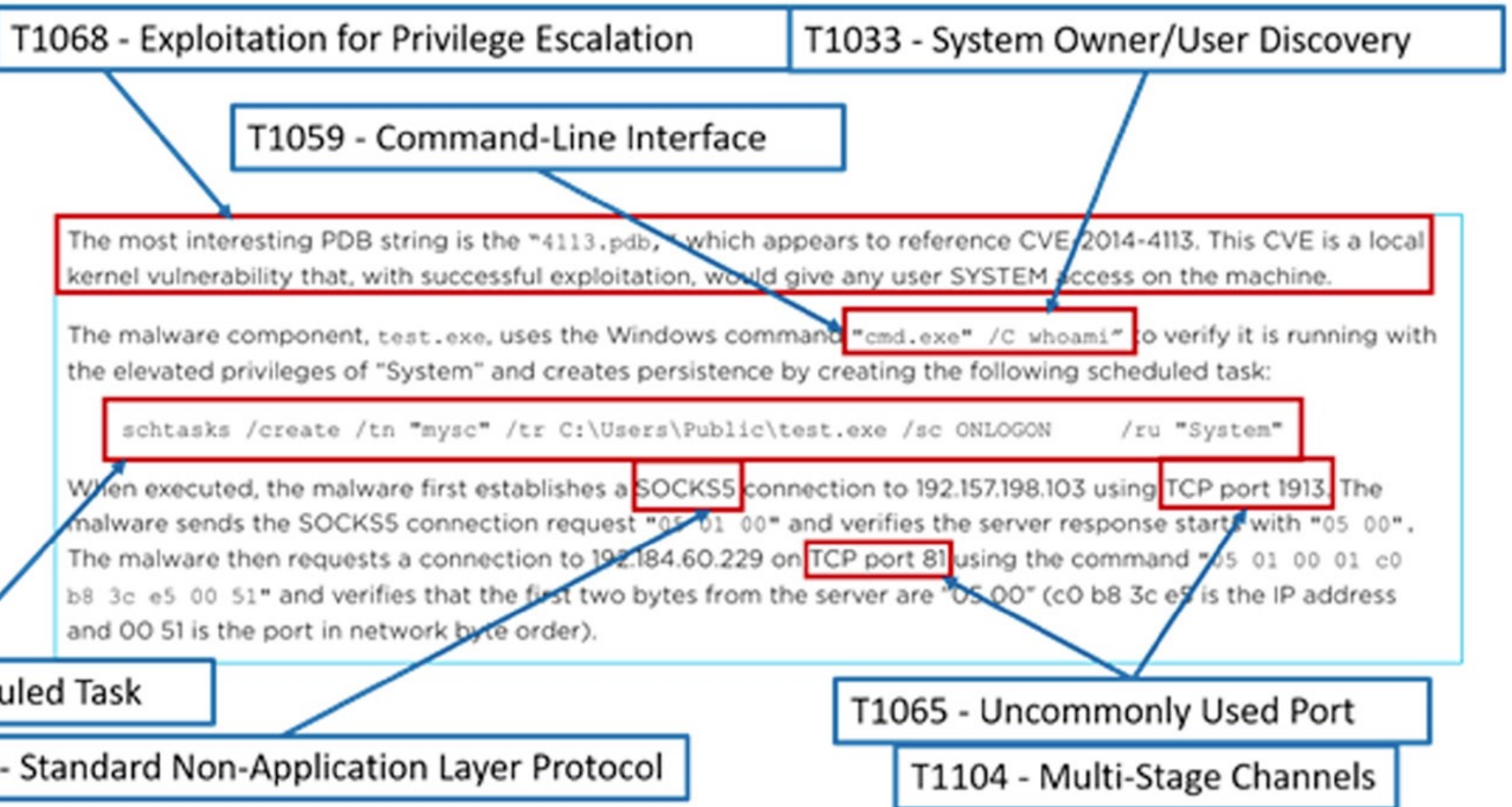
- Βάσεις/μήτρες [**matrices**]
  - Επιχειρησιακή [Enterprise]
    - Windows, macOS, Linux, PRE, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Network, Containers
  - Κινητών συσκευών [Mobile]
    - Android, iOS
  - Βιομηχανικών συστημάτων ελέγχου [Industrial Control Systems (ICS)]
    - SCADA,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

# Στοιχεία ΑΤΤ&ΣΚ

- Πηγές δεδομένων [[data sources](#)]
  - Κατηγορίες δεδομένων από αισθητήρες/καταγραφή
  - Πηγές δεδομένων που σχετίζονται με τον εντοπισμό μιας τεχνικής ΑΤΤ&ΣΚ
- 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

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
Active Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevated Privilege	Abuse Elevated Privilege
Host Information	Compromise Accounts	Exploit Public-Facing Application	Remote Administration Command	BITS Jobs	Access Token Manipulation	Access Token Manipulation
Gather Victim Identity Information	Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Log on Autostart Execution	Boot or Log on Autostart Execution	Boot or Log on Autostart Execution
Gather Victim Network Information	Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Boot or Log on Initialization Scripts	Boot or Log on Initialization Scripts	Boot or Log on Initialization Scripts
Gather Victim Information	Establish Accounts	Phishing	Internal Process Communication	Browser Extensions	Client Software Binary	Client Software Binary
Phishing for Information	Obtain Capabilities	Replication Through Remote Media	Native API	Compromise Policy Modification	Domain Policy Modification	Domain Policy Modification
Search Closed Sources	Stage Capabilities	Supply Chain Compromise	Schedule TaskJob	Create Account	Direct Volume Access	Direct Volume Access
Search Open Technical Databases		Trusted Relationship	Share Modules	Create or Modify System Process	Domain Policy Modification	Domain Policy Modification
Search Open Websites/Domains		Valid Accounts	Software Deployment Tools	Event Triggered Execution	Exploitation Guardrails	Exploitation Guardrails
Search Victim-Owned Websites			System Services	External Remote Services	Exploitation for Defense Evasion	Exploitation for Defense Evasion
			User Execution	Hijack Execution Flow	File and Directory Permissions Modification	File and Directory Permissions Modification
			Windows Management Instrumentation	Impair Integrity Image	Hide Artifacts	Hide Artifacts
				Modify Authentication Process	Hijack Execution Flow	Hijack Execution Flow
				Office Application Startup	Impair Defenses	Impair Defenses
				Pre-OSBoot	Indicator Removal on Host	Indicator Removal on Host
				Schedulable TaskJob	Indirect Command Execution	Indirect Command Execution
				Server Software Component	Malware	Malware
				Traffic Signaling	Modify Registry	Modify Registry
				Valid Accounts	Modify System Image	Modify System Image
					Network Boundary Bridging	Network Boundary Bridging
					Obfuscated Files or Information	Obfuscated Files or Information
					Pre-OSBoot	Pre-OSBoot
					Process Injection	Process Injection
					Reflective Code Loading	Reflective Code Loading
					Register Domain Controller	Register Domain Controller
					Rootkit	Rootkit
					Signed Binary Proxy Execution	Signed Binary Proxy Execution
					Signed Script Proxy Execution	Signed Script Proxy Execution
					Subvert Trust Controls	Subvert Trust Controls
					Template Injection	Template Injection
					Traffic Signaling	Traffic Signaling
					Trusted Developer Utilities Proxy Execution	Trusted Developer Utilities Proxy Execution
					Unusual Dispositioned Cloud Regions	Unusual Dispositioned Cloud Regions
					User Account Authentication Material	User Account Authentication Material
					Valid Accounts	Valid Accounts
					Virtualization Sandbox Evasion	Virtualization Sandbox Evasion
					Weaken Encryption	Weaken Encryption
					XSS Script Processing	XSS Script Processing

Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Remote Media	Data Transfer Size Limits	Data Destruction
Credentials from Password Stores	Browser Bookmarks Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation
Forged Authentication	Cloud Service Dashboard	Remote Services	Browser Session Hijacking	Dynamic Resolution	Exfiltration Over Network Medium	Defacement
Forge Web Credentials	Cloud Service Discovery	Replication Through Remote Media	Clipboard Data	Encrypt Channel	Exfiltration Over Physical Medium	Disk Wipe
Input Capture	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Failback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
Modify Authentication Process	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository	Ingress Tool Transfer	Exfiltration Over Web Service	Inhibit System Recovery
Network Sniffing	Domain Trust Discovery	User Account Authentication Material	Data from Information Repositories	Multi-Stage Channels	Schedule Transfer	Firmware Corruption
OS Credential Dumping	File and Directory Discovery		Data from Local System	Non-Application Layer Protocol	Transfer Data to Cloud Account	Network Denial of Service
Steal Application Access Token	Group Policy Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
Steal or Forge Kerberos Tickets	Network Service Scanning		Data from Removable Media	Protocol Tunneling		Service Stop
Steal Web Session Cookies	Network Share Discovery		Data Staged	Proxy		System Shutdown/Reboot
Two-Factor Authentication Interception	Network Sniffing		Email Collection	Remote Access Software		
Unsecured Credentials	Password Policy Discovery		Input Capture	Traffic Signaling		
	Perimeter Device Discovery		Screen Capture	Web Service		
	Process Discovery		Video Capture			
	Quey Registry					
	Remote System Discovery					
	Software Discovery					
	System Information Discovery					
	System Location Discovery					
	System Network Configuration Discovery					
	System Network Connections Discovery					
	System User Discovery					
	System Service Discovery					
	System Time Discovery					
	Virtualization Sandbox Evasion					

legend	
#e60d0d	BEC
#3182bd	Phishing, Spearphishing
#31a354	Phishing
#756bb1	Phishing, Spam, Spearphishing
#fce93b	BEC, Phishing, Spearphishing
#e6550d	Smishing

# E-mail related threats [2]

about  
E-mail

domain  
Mobile ATT&CK v10

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact	Network Effects	Remote Service Effects
<ul style="list-style-type: none"> <li>Deliver Malicious App via Authorized App Store</li> <li>Deliver Malicious App via Other Means</li> <li>Drive-by Compromise</li> <li>Exploit via Charging Station or PC</li> <li>Exploit via Radio Interfaces</li> <li>Install Insecure or Malicious Configuration</li> <li>Lockscreen Bypass</li> <li>Masquerade as Legitimate Application</li> <li>Supply Chain Compromise</li> </ul>	<ul style="list-style-type: none"> <li>Broadcast Receivers</li> <li>Command-Line Interface</li> <li>Native Code</li> <li>Scheduled Task/Job</li> </ul>	<ul style="list-style-type: none"> <li>Broadcast Receivers</li> <li>Code Injection</li> <li>Compromise Application Executable</li> <li>Foreground Persistence</li> <li>Modify Cached Executable Code</li> <li>Modify OS Kernel or Boot Partition</li> <li>Modify System Partition</li> <li>Modify Trusted Execution Environment</li> <li>Scheduled Task/Job</li> </ul>	<ul style="list-style-type: none"> <li>Code Injection</li> <li>Device Administrator Permissions</li> <li>Exploit OS Vulnerability</li> <li>Exploit TEE Vulnerability</li> </ul>	<ul style="list-style-type: none"> <li>Application Discovery</li> <li>Code Injection</li> <li>Delete Device Data</li> <li>Device Lockout</li> <li>Disguise Root/Jailbreak Indicators</li> <li>Download New Code at Runtime</li> <li>Evade Analysis Environment</li> <li>Geofencing</li> <li>Hooking</li> <li>Input Injection</li> <li>Install Insecure or Malicious Configuration</li> <li>Masquerade as Legitimate Application</li> <li>Modify OS Kernel or Boot Partition</li> <li>Modify System Partition</li> <li>Modify Trusted Execution Environment</li> <li>Native Code</li> <li>Obfuscated Files or Information</li> <li>Proxy Through Victim</li> <li>Suppress Application Icon</li> <li>Uninstall Malicious Application</li> <li>User Evasion</li> </ul>	<ul style="list-style-type: none"> <li>Access Notifications</li> <li>Access Sensitive Data in Device Logs</li> <li>Access Stored Application Data</li> <li>Capture Clipboard Data</li> <li>Capture SMS Messages</li> <li>Exploit TEE Vulnerability</li> <li>Input Capture</li> <li>Input Prompt</li> <li>Keychain</li> <li>Network Traffic Capture or Redirection</li> <li>URI Hijacking</li> </ul>	<ul style="list-style-type: none"> <li>Application Discovery</li> <li>Evade Analysis Environment</li> <li>File and Directory Discovery</li> <li>Location Tracking</li> <li>Network Service Scanning</li> <li>Process Discovery</li> <li>System Information Discovery</li> <li>System Network Configuration Discovery</li> <li>System Network Connections Discovery</li> </ul>	<ul style="list-style-type: none"> <li>Attack PC via USB Connection</li> <li>Exploit Enterprise Resources</li> </ul>	<ul style="list-style-type: none"> <li>Access Calendar Entries</li> <li>Access Call Log</li> <li>Access Contact List</li> <li>Access Notifications</li> <li>Access Sensitive Data in Device Logs</li> <li>Access Stored Application Data</li> <li>Call Control</li> <li>Capture Audio</li> <li>Capture Camera</li> <li>Capture Clipboard Data</li> <li>Capture SMS Messages</li> <li>Data from Local System</li> <li>Foreground Persistence</li> <li>Input Capture</li> <li>Location Tracking</li> <li>Network Information Discovery</li> <li>Network Traffic Capture or Redirection</li> <li>Screen Capture</li> </ul>	<ul style="list-style-type: none"> <li>Alternate Network Mediums</li> <li>Call Control</li> <li>Commonly Used Port</li> <li>Domain Generation Algorithms</li> <li>Remote File Copy</li> <li>Standard Application Layer Protocol</li> <li>Standard Cryptographic Protocol</li> <li>Uncommonly Used Port</li> <li>Web Service</li> </ul>	<ul style="list-style-type: none"> <li>Alternate Network Mediums</li> <li>Commonly Used Port</li> <li>Data Encrypted</li> <li>Standard Application Layer Protocol</li> </ul>	<ul style="list-style-type: none"> <li>Call Control</li> <li>Carrier Billing Fraud</li> <li>Clipboard</li> <li>Data Encrypted for Impact</li> <li>Delete Device Data</li> <li>Device Lockout</li> <li>Generate Fraudulent Advertising Revenue</li> <li>Input Injection</li> <li>Manipulate App Store Rankings or Ratings</li> <li>Modify System Partition</li> <li>SMS Control</li> </ul>	<ul style="list-style-type: none"> <li>Downgrade to Insecure Protocols</li> <li>Eavesdrop on Insecure Network Communication</li> <li>Exploit SS7 to Redirect Phone Calls/SMS</li> <li>Exploit SS7 to Track Device Location</li> <li>Jamming or Denial of Service</li> <li>Manipulate Device Communication</li> <li>Rogue Cellular Base Station</li> <li>Rogue Wi-Fi Access Points</li> <li>SIM Card Swap</li> </ul>	<ul style="list-style-type: none"> <li>Obtain Device</li> <li>Cloud Backups</li> <li>Remotely Track Device Without Authorization</li> <li>Remotely Wipe Data Without Authorization</li> </ul>

legend

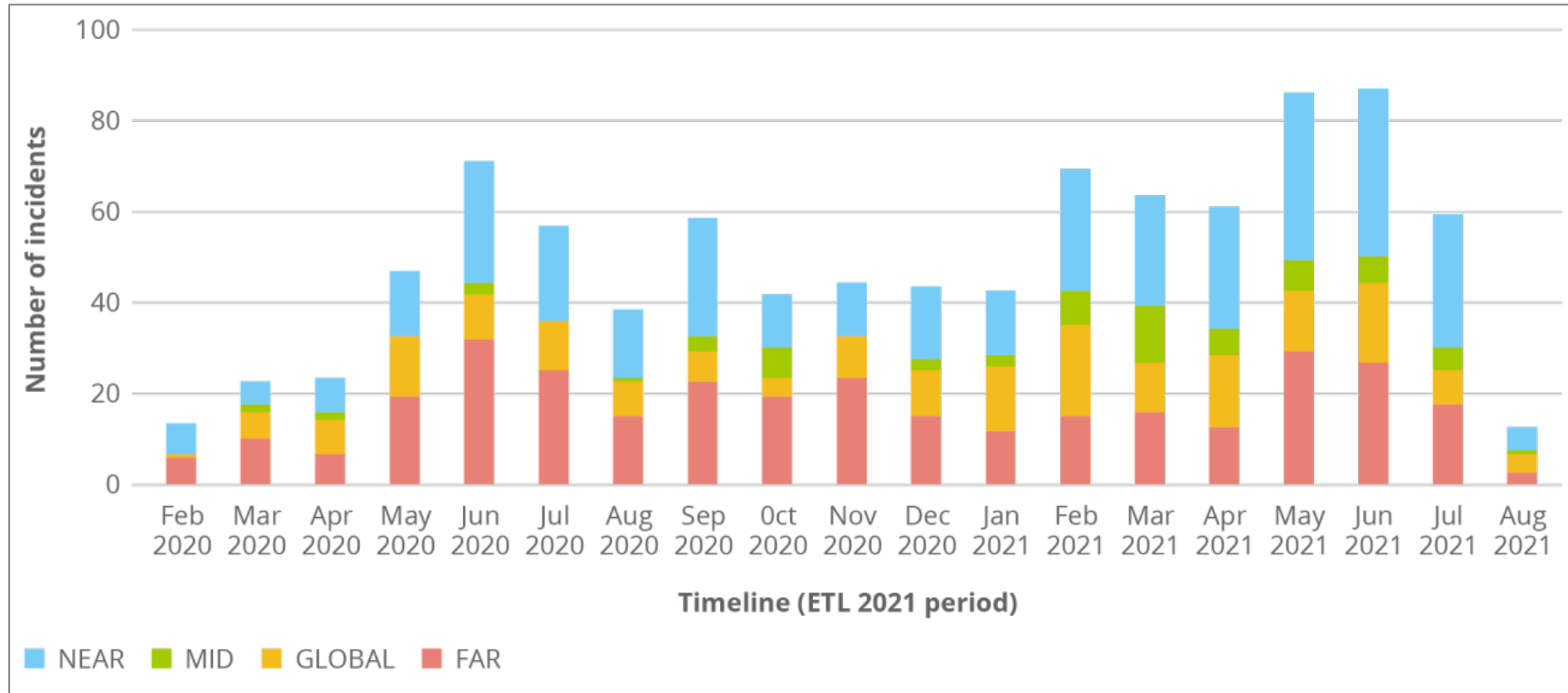
- #e60d0d BEC
- #3182bd Phishing, Spearphishing
- #31a354 Phishing
- #756bb1 Phishing, Spam, Spearphishing
- #fce93b BEC, Phishing, Spearphishing
- #e6550d Smishing

# Αναφορές Περιστατικών Ασφάλειας

Αναφορικά στοιχεία 2021

# ETL 2021

## Γεωπολιτικά στοιχεία περιστατικών ασφάλειας



Χρονοδιάγραμμα καταμερισμού περιστατικών

Near: Εντός ΕΕ

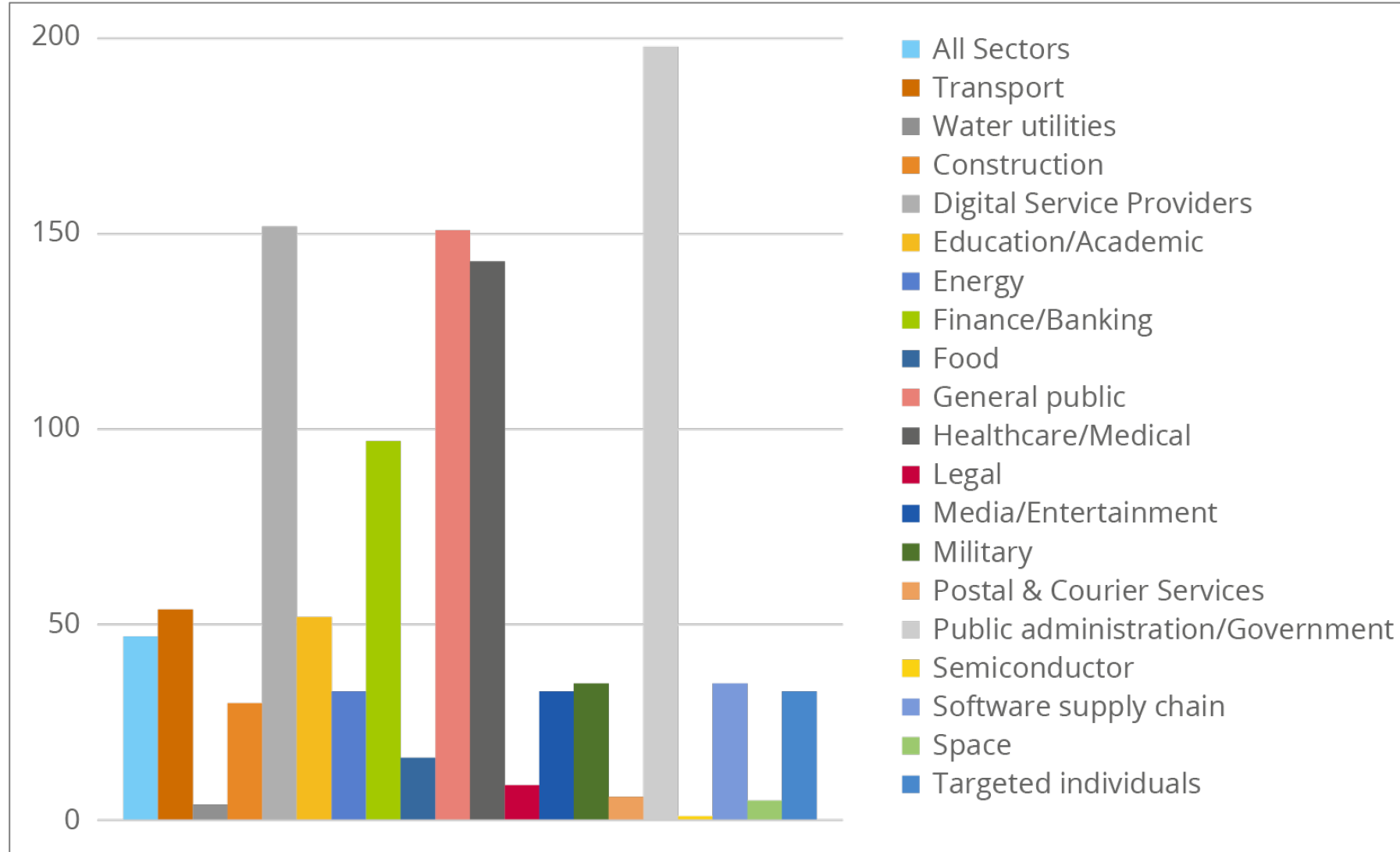
Mid: Εντός ΕΕ και συνοριακά (Ευρωπαϊκές χώρες εκτός ΕΕ, Ισραήλ, Τουρκία, κ.λπ.)

Global: Παγκόσμια

Far: Ασία, Βόρεια και Νότια Αμερική, Ωκεανία

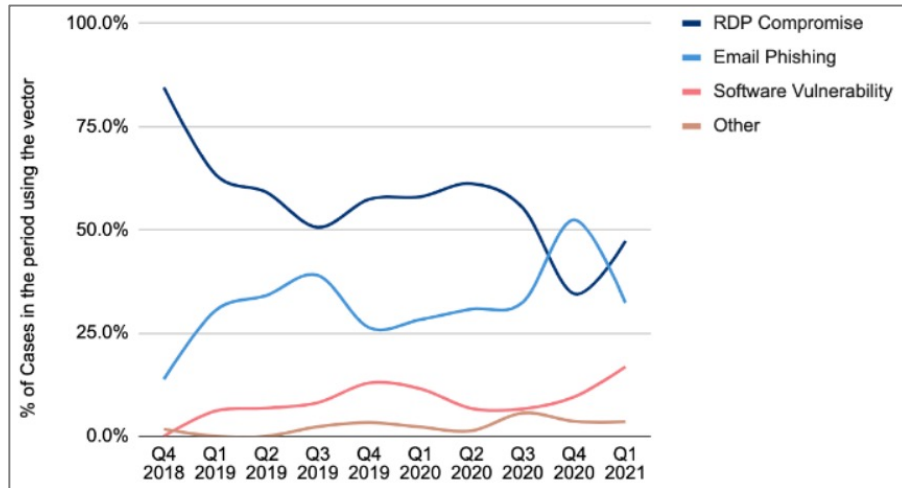
# ETL 2021

## Περιστατικά ασφάλειας ανά κλάδο



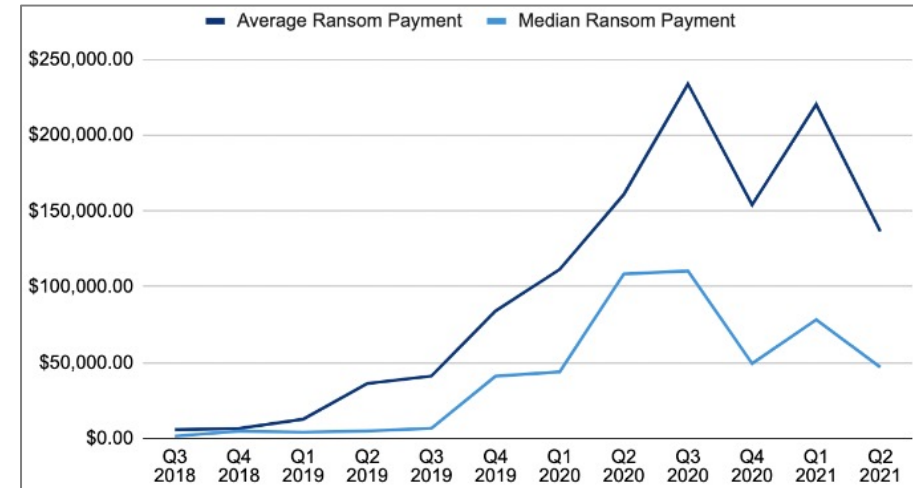
# Ransomware 2021

## Φορείς επιθέσεων



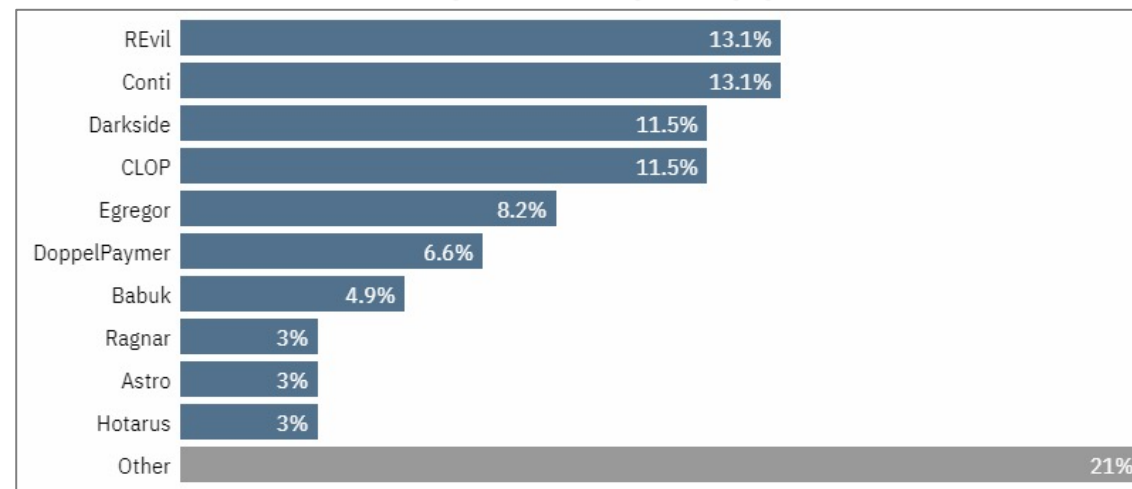
Ποσοστό περιστατικών ανά φορέα (vector)

## Κόστος επιθέσεων



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

## Αποτελεσματικότητα εργαλείων

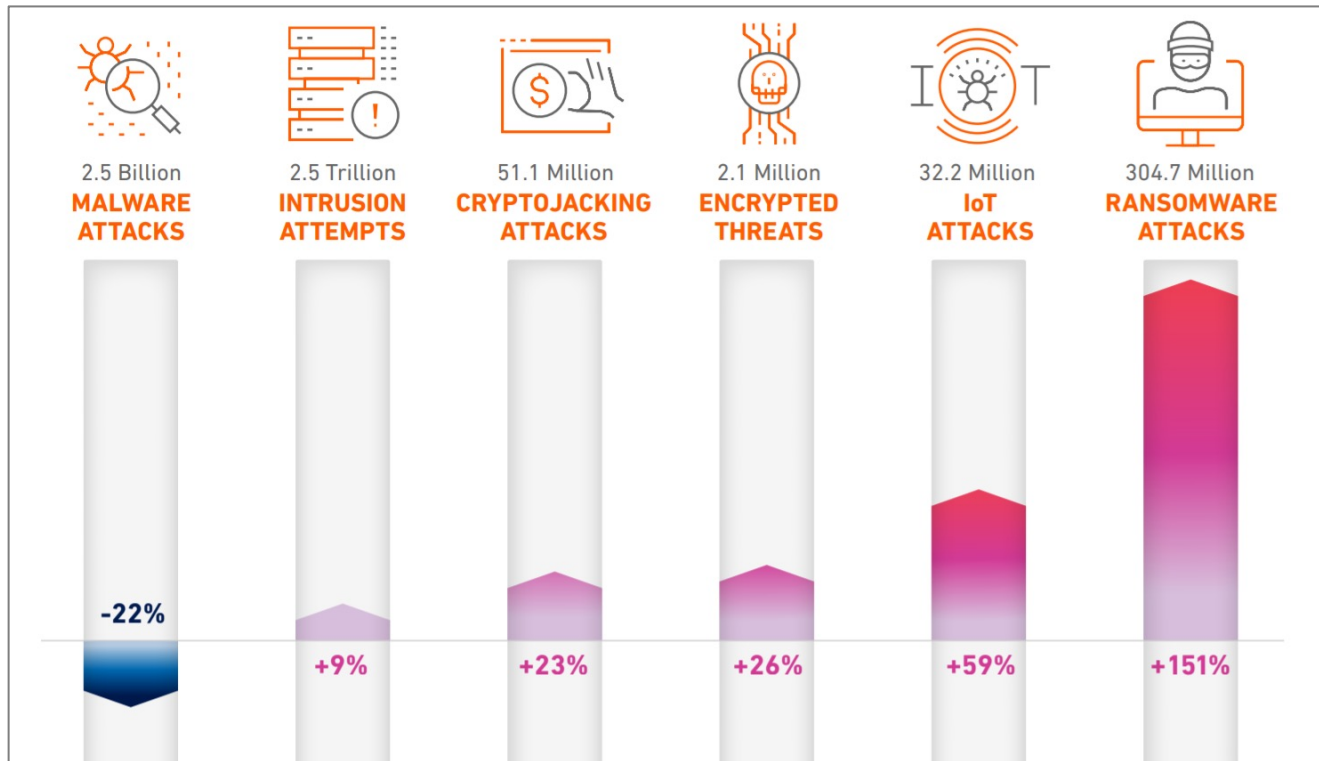


Ποσοστό απώλειας δεδομένων ανά εργαλείο



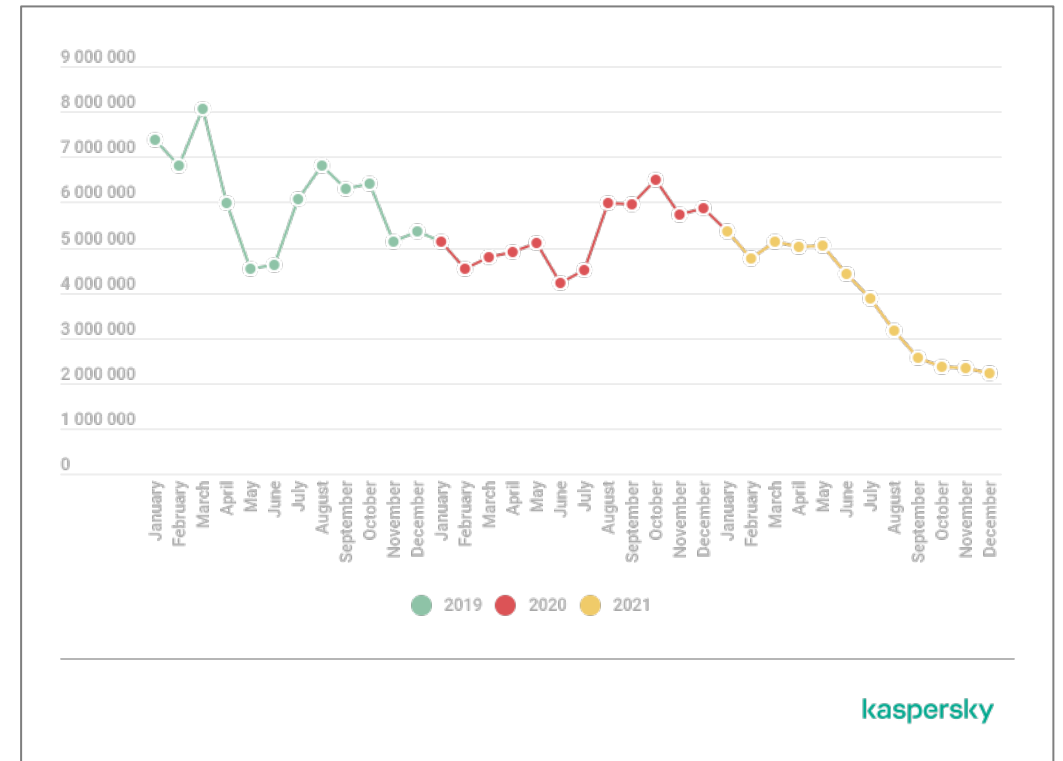
# Malware 2021

## Τάση επιθέσεων



Ποσοστό ανόδου/πτώσης επιθέσεων ανά κατηγορία

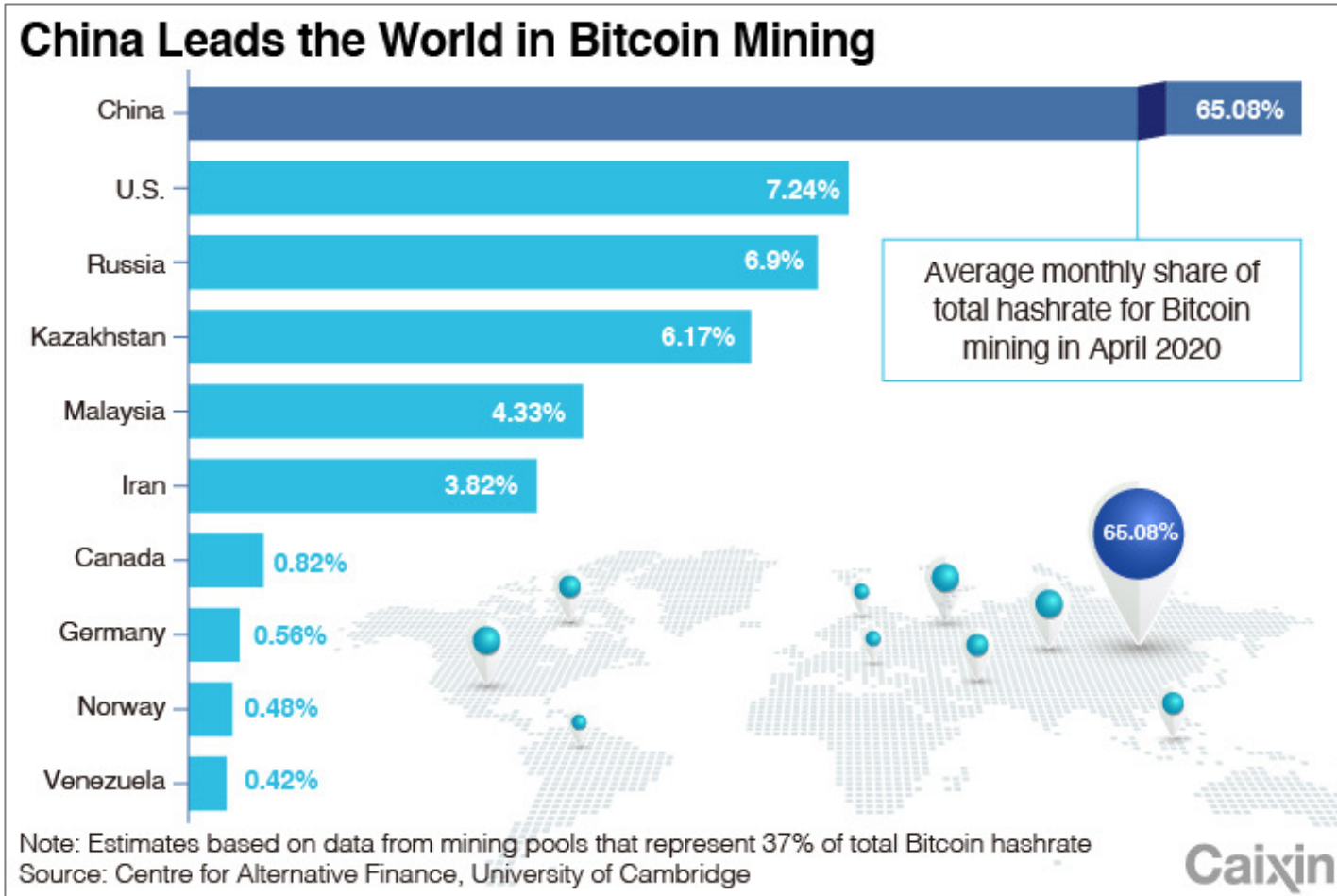
## Κακόβουλο λογισμικό κινητών



Πλήθος επιθέσεων ανά μήνα

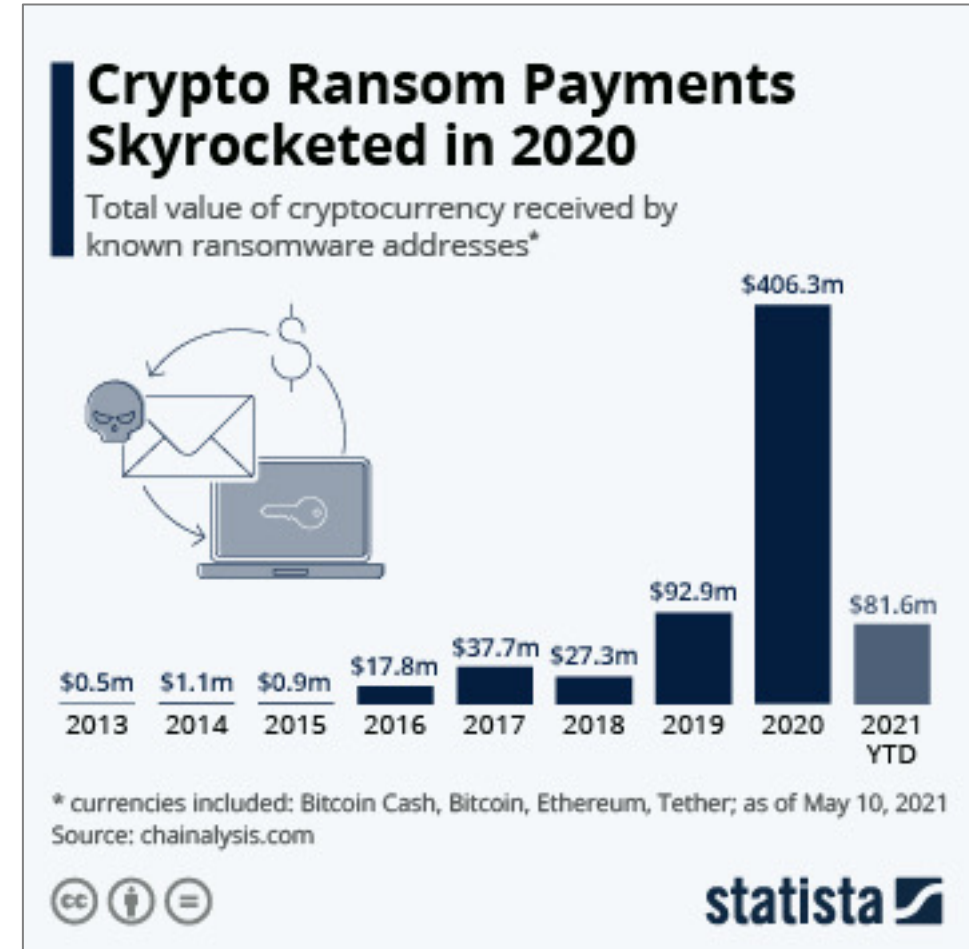
# Cryptojacking 2021

## Γεωπολιτικά χαρακτηριστικά



Μηνιαίο ποσοστό ανά χώρα

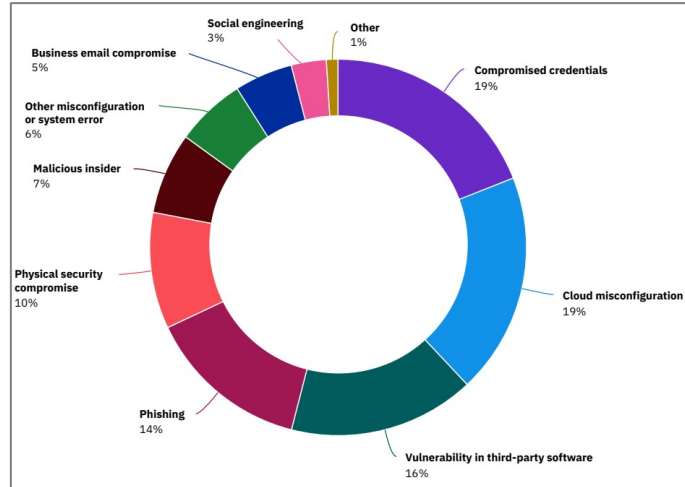
## Κόστος επιθέσεων



Ποσά καταβληθέντων λύτρων σε κρυπτονόμισμα

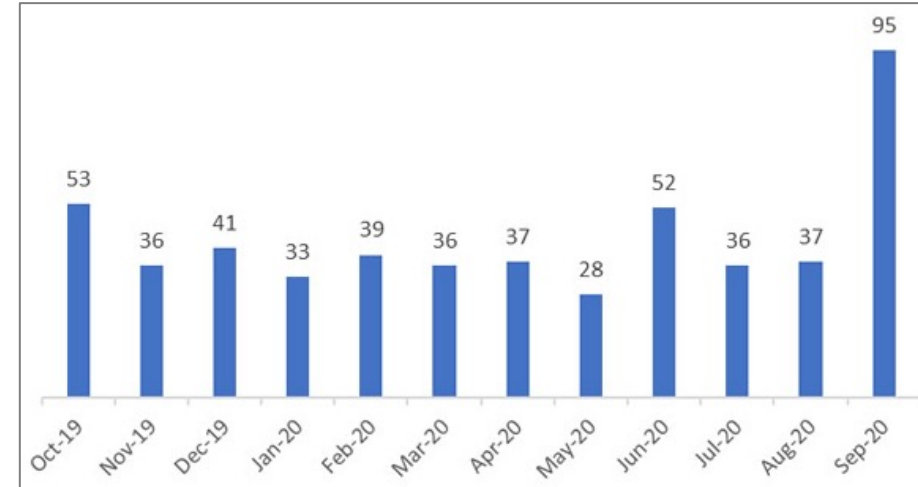
# E-mail related threats 2021

## Παραβίαση δεδομένων



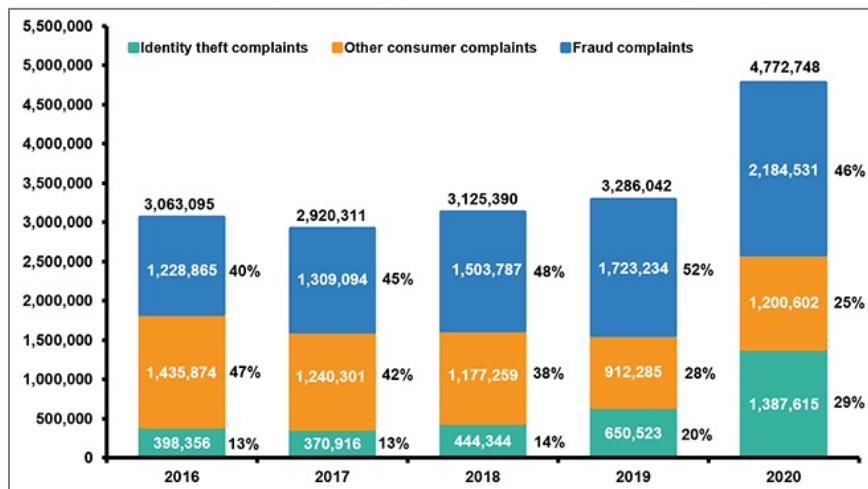
Ποσοστό απωλειών δεδομένων ανά φορέα (vector)

## Παραβίαση δεδομένων υγείας



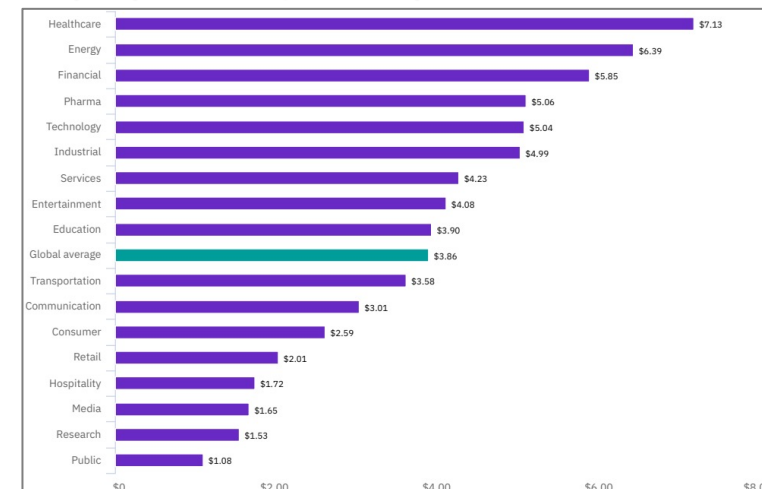
Όγκος απολεσθέντων δεδομένων ανά μήνα

## Κλοπές στοιχείων ταυτότητας



Κλοπές στοιχείων ταυτότητας και απάτες ανά έτος

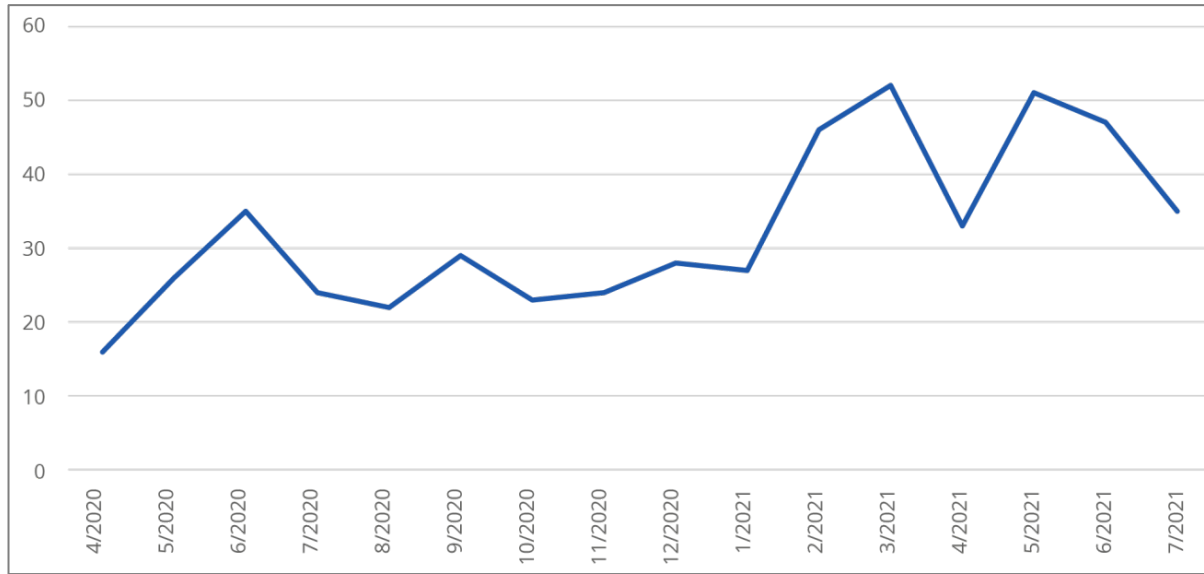
## Παραβιάσεις δεδομένων ανά κλάδο



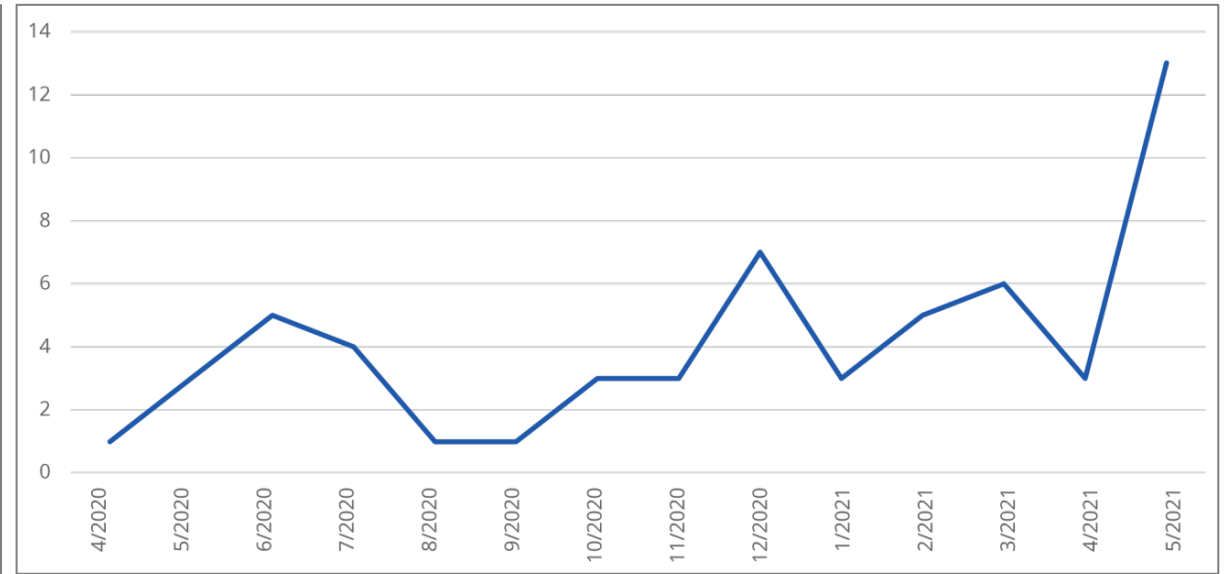
Μέσος όρος συνολικού κόστους λόγω παραβίασης δεδομένων

# 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](http://BankInfoSecurity.com)
- [ComputerWeekly.com](http://ComputerWeekly.com)
- [HelpNetSecurity.com](http://HelpNetSecurity.com)
- [NewsWeek.com](http://NewsWeek.com)
- [SecuringTomorrow.mcafee.com](http://SecuringTomorrow.mcafee.com)
- [SecurityWeek.com](http://SecurityWeek.com)
- CNN news
- CBN news
- BBC news Cyber-security
- CNET Security

## Darknet

- [DarkReading.com](http://DarkReading.com)
- Explore at your own risk



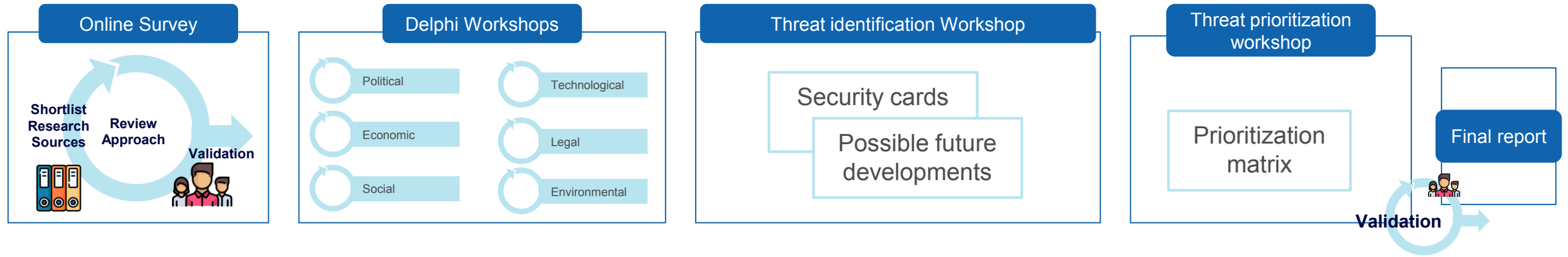
# Αναφορές Περιστατικών Ασφάλειας

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



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

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

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

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)

# References

1. Jögi, 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*<sup>®</sup>, <https://attack.mitre.org/>
4. ATT&CK<sup>®</sup> 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>