



GDPR: ΣΥΝΤΟΜΟΣ ΟΔΗΓΟΣ ΕΠΙΒΙΩΣΗΣ

ΒΑΣΙΛΕΙΟΣ ΒΛΑΧΟΣ

ΕΠΙΚΟΥΡΟΣ ΚΑΘΗΓΗΤΗΣ Τ.Ε.Ι. ΘΕΣΣΑΛΙΑΣ

ΜΕΛΟΣ Δ.Σ. ΕΜηΠΕΕ

ΗΛΕΚΤΡΟΝΙΚΟΣ ΜΗΧΑΝΙΚΟΣ ΚΑΙ ΜΗΧΑΝΙΚΟΣ ΥΠΟΛΟΓΙΣΤΩΝ

Τι θα συμβεί στις 25 Μαΐου;



Τι είναι ο GDPR / ΓΚΠΔ;



PrivacyFlag AddOn User

Third party tracker or advertising company



Cookies,

Fingerprinting

Traffic analysis



Γιατί είναι σημαντικός ο GDPR / ΓΚΠΔ;

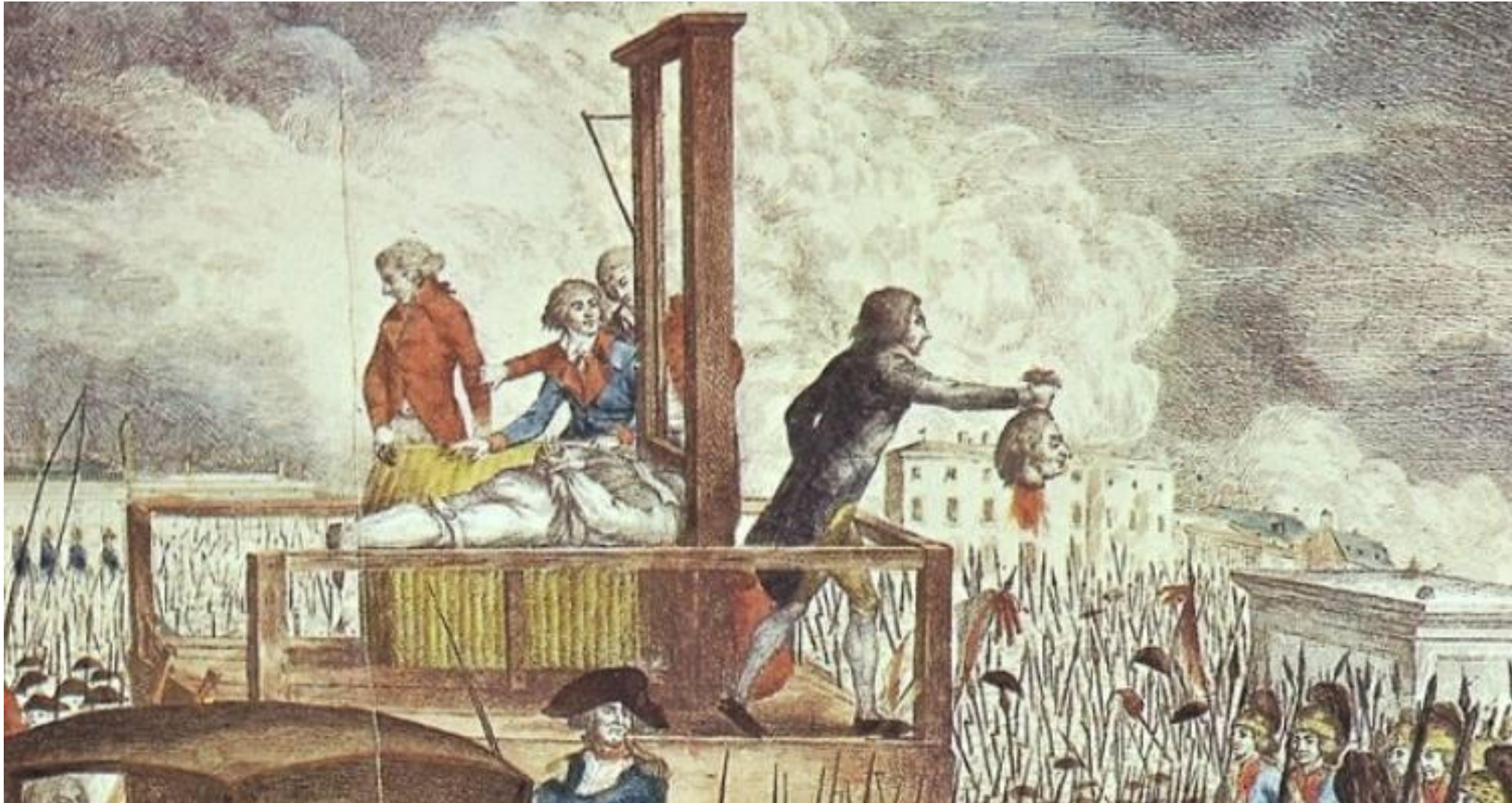


“DATA IS THE NEW GOLD”



Neelie Kroes
Αντιπρόεδρος της Ευρωπαϊκής Ένωσης
υπεύθυνη για την Ψηφιακή Ατζέντα

Γιατί είναι σημαντικός ο GDPR / ΓΚΠΔ;



Αποφύγετε τους Αλεξιπτωτιστές

Για την επιλογή συνεργατών για το GDPR πληροφορηθείτε:

- Πόσα χρόνια εμπειρία έχουν στο χώρο της Ασφάλειας ΠΣ;
- Ποια έργα έχουν υλοποιήσει;
- Με ποιες εταιρίες / φορείς έχουν συνεργαστεί;
- Σε τι εξειδικεύονται;



Μην Ελπίζετε σε Θαύματα

- Ο ΓΚΠΔ είναι διαδικασία, δεν είναι προϊόν
- Ή συμμόρφωση είναι σταδιακή, όχι απότομη
- Δεν αγοράζεται αλλά υλοποιείται
- Δεν είναι εναντίον αλλά υπέρ της επιχείρησης



Λογισμικό Προστασίας Διαρροής Δεδομένων



opendlp

Data Loss Prevention

- Σύνολο εργαλείων και διαδικασιών για τη διασφάλιση των ευαίσθητων δεδομένων από διαρροή, τροποποίηση και πρόσβαση από μη εξουσιοδοτημένους χρήστες

Open DLP

- Ανοικτό λογισμικό
- Παρακολουθεί τα ευαίσθητα αποθηκευμένα δεδομένα σε ολόκληρο το δίκτυο
- Αποτροπή από τυχαία διαρροή πληροφοριών εκτός δικτύου ή σκόπιμη κλοπή αυτών μέσω email, διαδικτύου, εξωτερικών συσκευών αποθήκευσης, εκτυπωτών κ.α.

Source: <https://www.darknet.org.uk/2010/05/opendlp-free-open-source-data-loss-prevention-dlp-tool/>

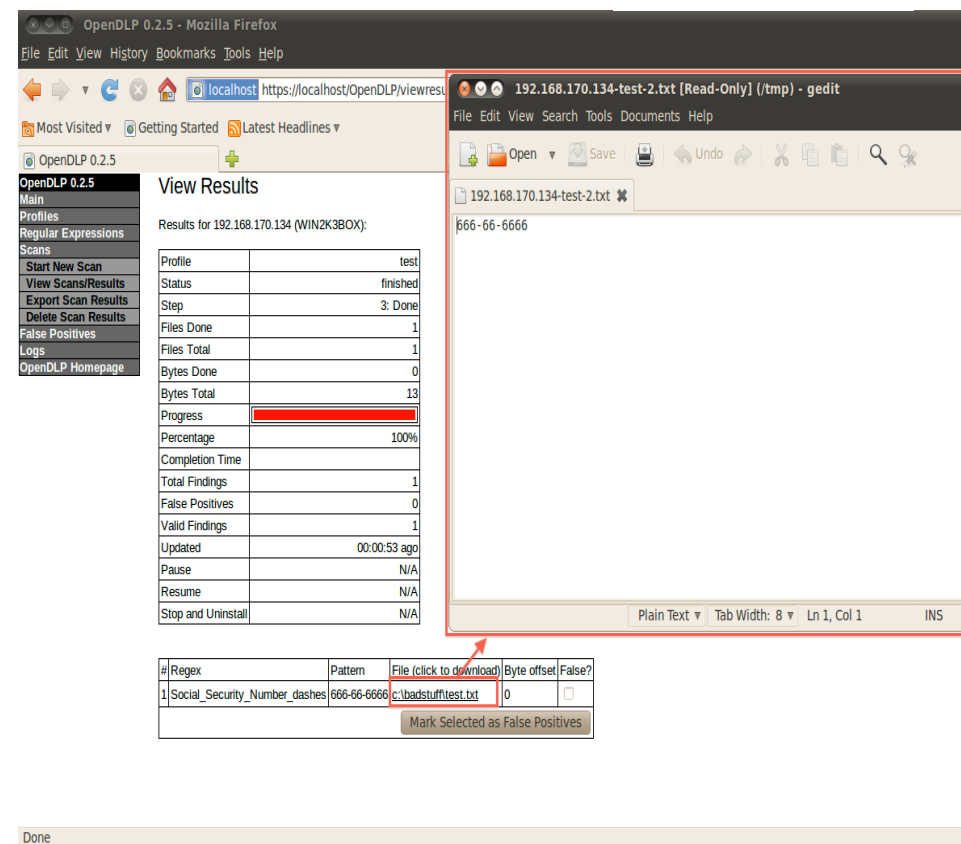
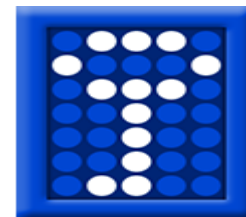


Image Source: <http://console-cowboys.blogspot.gr/2011/02/opendlp-pass-hash.html>

Λογισμικό Κρυπτογράφησης Δεδομένων

- Κρυπτογράφηση των δεδομένων σε μια άλλη μορφή ή κώδικα ώστε να είναι προσβάσιμα μόνο από εξουσιοδοτημένα άτομα που έχουν στην κατοχή τους ένα μυστικό κλειδί ή κωδικό πρόσβασης



TrueCrypt

- Χρησιμοποιείται για συνεχή κρυπτογράφηση (on-the-fly). Μπορεί να δημιουργήσει έναν εικονικό κρυπτογραφημένο δίσκο μέσα σε ένα αρχείο ή να κρυπτογραφήσει ένα διαμέρισμα ή ολόκληρη τη συσκευή αποθήκευσης

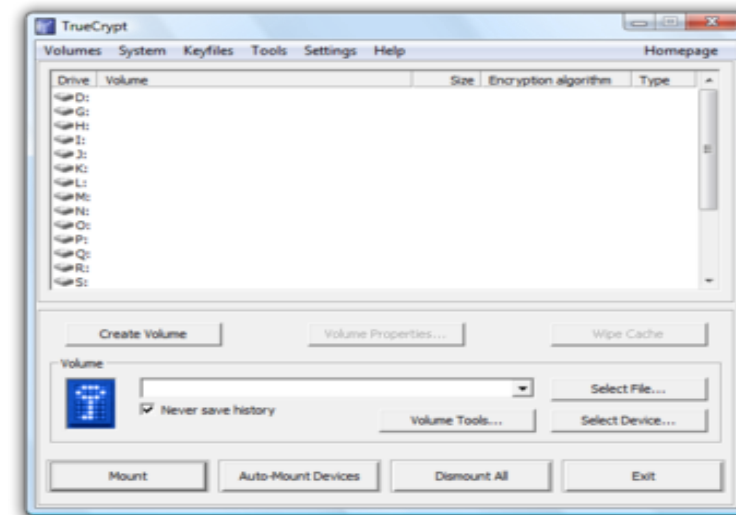
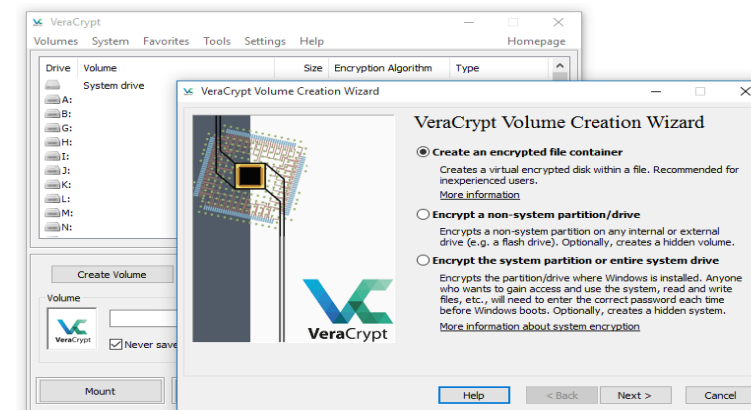


Image Source: https://en.wikipedia.org/wiki/TrueCrypt#/media/File:TrueCrypt_on_windows_vista.png

VeraCrypt

- Αποτελεί σύγχρονη έκδοση του TrueCrypt και διαθέτει βελτιστοποιημένες εφαρμογές κρυπτογραφικών λειτουργιών κατακερματισμού και κρυπτογράφησης, οι οποίες ενισχύουν την απόδοση στις σύγχρονες CPU



Source: <https://sourceforge.net/projects/veracrypt/>

Image Source: https://en.wikipedia.org/wiki/TrueCrypt#/media/File:TrueCrypt_on_windows_vista.png

Κρυπτογράφηση Μηνυμάτων Ηλεκτρονικού Ταχυδρομείου

- Κρυπτογράφηση των μηνυμάτων email για προστασία από μη εξουσιοδοτημένη χρήση

GnuPG

- Επιτρέπει την κρυπτογράφηση και υπογραφή των δεδομένων και των επικοινωνιών
- Διαθέτει ένα ευέλικτο σύστημα διαχείρισης κλειδιών και υποστήριξη για S / MIME και Secure Shell (ssh)

Source: <https://www.gnupg.org/>

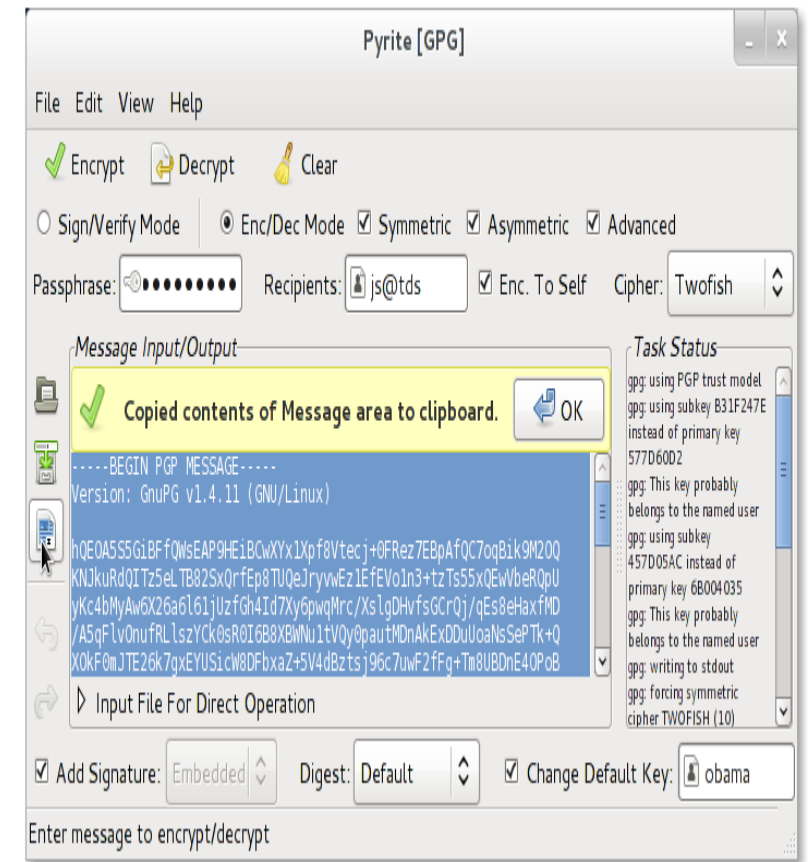


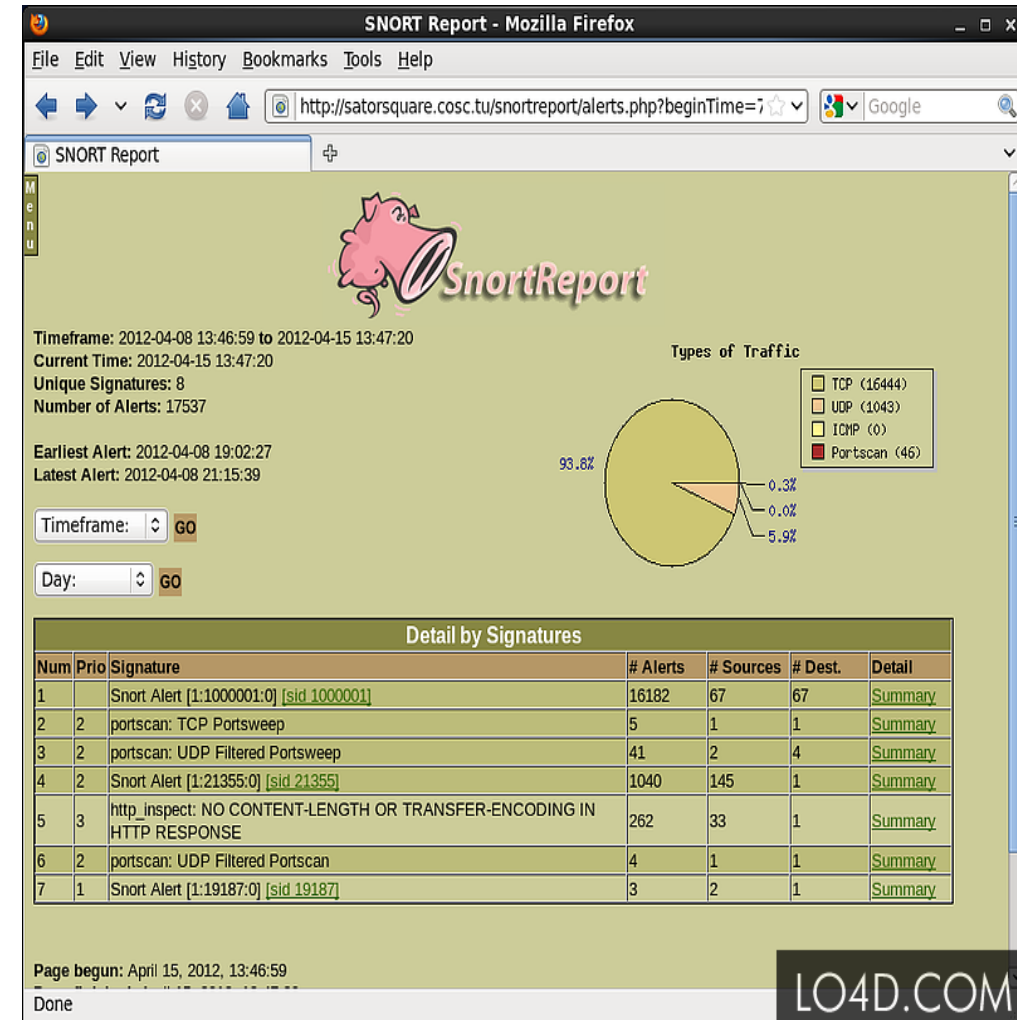
Image Source: <https://github.com/ryran/pyrite>

Αναγνώριση Παραβιάσεων Δεδομένων

- Αναγνώριση περιστατικών παραβίασης ευαίσθητων και εμπιστευτικών δεδομένων

Snort

- Λογισμικό ανίχνευσης εισβολών (Intrusion Detection System - IDS) ανοικτού κώδικα
- Δυνατότητα ανάλυσης κυκλοφορίας σε πραγματικό χρόνο
- Καταγραφή πακέτων σε δίκτυα Internet Protocol (IP)
- Ανάλυση πρωτοκόλλου, αναζήτηση περιεχομένου και αντιστοίχιση
- Ανίχνευση επιθέσεων, προσπαθειών αποτύπωσης λειτουργικού συστήματος, σημασιολογικών επιθέσεων URL, υπερχείλισης buffer, κ.α.



Προστασία από Ιούς

- Πρόγραμμα υπολογιστή που χρησιμοποιείται για την πρόληψη, ανίχνευση και κατάργηση κακόβουλου λογισμικού

ClamAV

- Δωρεάν εργαλείο λογισμικού προστασίας από ιούς, ανοικτού κώδικα, που επιτρέπει την ανίχνευση πολλών τύπων κακόβουλου λογισμικού. Μία από τις κύριες χρήσεις του είναι στους διακομιστές αλληλογραφίας ως σαρωτής ιού ηλεκτρονικού ταχυδρομείου διακομιστή

Source: <https://www.clamav.net/>



```
clamscan
File Edit View Scrollback Bookmarks Settings Help
-desktop:~$ sudo freshclam
ClamAV update process started at Sun May 16 13:38:10 2010
main.cvd is up to date (version: 52, sigs: 704727, f-level: 44, builder: sven)
daily.cld is up to date (version: 11020, sigs: 70708, f-level: 51, builder: guit
ar)
bytecode.cld is up to date (version: 20, sigs: 3, f-level: 51, builder: nervous)
-desktop:~$ clamscan ~/Downloads/setup.exe
/home/~/Downloads/setup.exe: Trojan.FakeAV-136 FOUND

----- SCAN SUMMARY -----
Known viruses: 774736
Engine version: 0.96
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 7.00 MB
Data read: 6.77 MB (ratio 1.03:1)
Time: 4.332 sec (0 m 4 s)
-desktop:~$
```

Image Source:

https://en.wikipedia.org/wiki/Clam_AntiVirus#/media/File:Clamav096.png

Άλλες Σημαντικές Απαιτήσεις

- **Ψευδωνυμοποίηση (Pseudonymization):** Αντικαθιστά την ταυτότητα του υποκειμένου των δεδομένων με τέτοιο τρόπο ώστε να απαιτούνται πρόσθετες πληροφορίες για την εκ νέου αναγνώριση του. Ο νέος κανονισμός απαιτεί τα αποθηκευμένα δεδομένα για τους ανθρώπους εντός της ΕΕ να υποβάλλονται είτε σε ψευδωνυμοποίηση είτε σε πλήρη ανώνυμοποίηση (Anonymization)
Source: <https://www.protegrity.com/pseudonymization-vs-anonymization-help-gdpr/>
- **Μεταφερισιμότητα των Δεδομένων:** Η ικανότητα τα υποκείμενα των δεδομένων να έχουν μεγαλύτερο έλεγχο στα προσωπικά τους δεδομένα, ιδίως για την επαναχρησιμοποίησή τους και τη διαχείριση τους ή για την εναλλαγή μεταξύ παρόχων υπηρεσιών
Source: <https://www.itgovernance.eu/blog/en/the-gdpr-understanding-the-right-to-data-portability>
- **Ασφάλεια Περιμέτρου:** το εμπλουτισμένο όριο του δικτύου που μπορεί να περιλαμβάνει τις ακόλουθες πτυχές: border routers, firewalls, IDS, IPSs, συσκευές VPN, αρχιτεκτονική λογισμικού, DMZ και τα υποδίκτυα που έχουν υποβληθεί σε έλεγχο
Source: <http://www.informit.com/articles/article.aspx?p=376256>

Άλλες Σημαντικές Απαιτήσεις

- Υπηρεσίες Αποθήκευσης και Κοινής Χρήσης του cloud: Υπηρεσίες όπως το Dropbox, Box, Microsoft OneDrive and Google Drive χρησιμοποιούνται εκτεταμένα από πολλούς εργαζόμενους ανά τον κόσμο. Ο νέος κανονισμός απαιτεί οι επιχειρήσεις να γνωρίζουν τις εφαρμογές αποθήκευσης και χρήσης του cloud που χρησιμοποιούνται από τους υπαλλήλους τους και να διασφαλίζουν ότι οι υπηρεσίες cloud που χρησιμοποιούνται είναι συμβατές και ενσωματωμένες στις διαδικασίες GDPR

Source: <https://www.clearswift.com/blog/2016/12/15/cloud-storage-file-sharing-apps-and-gdpr-could-get-ugly-fast>

- Ασφάλεια Εφαρμογών: Περιλαμβάνει μέτρα που λαμβάνονται για τη βελτίωση της ασφάλειας μιας εφαρμογής συχνά με την εύρεση, τον καθορισμό και την αποτροπή των τρωτών σημείων ασφαλείας

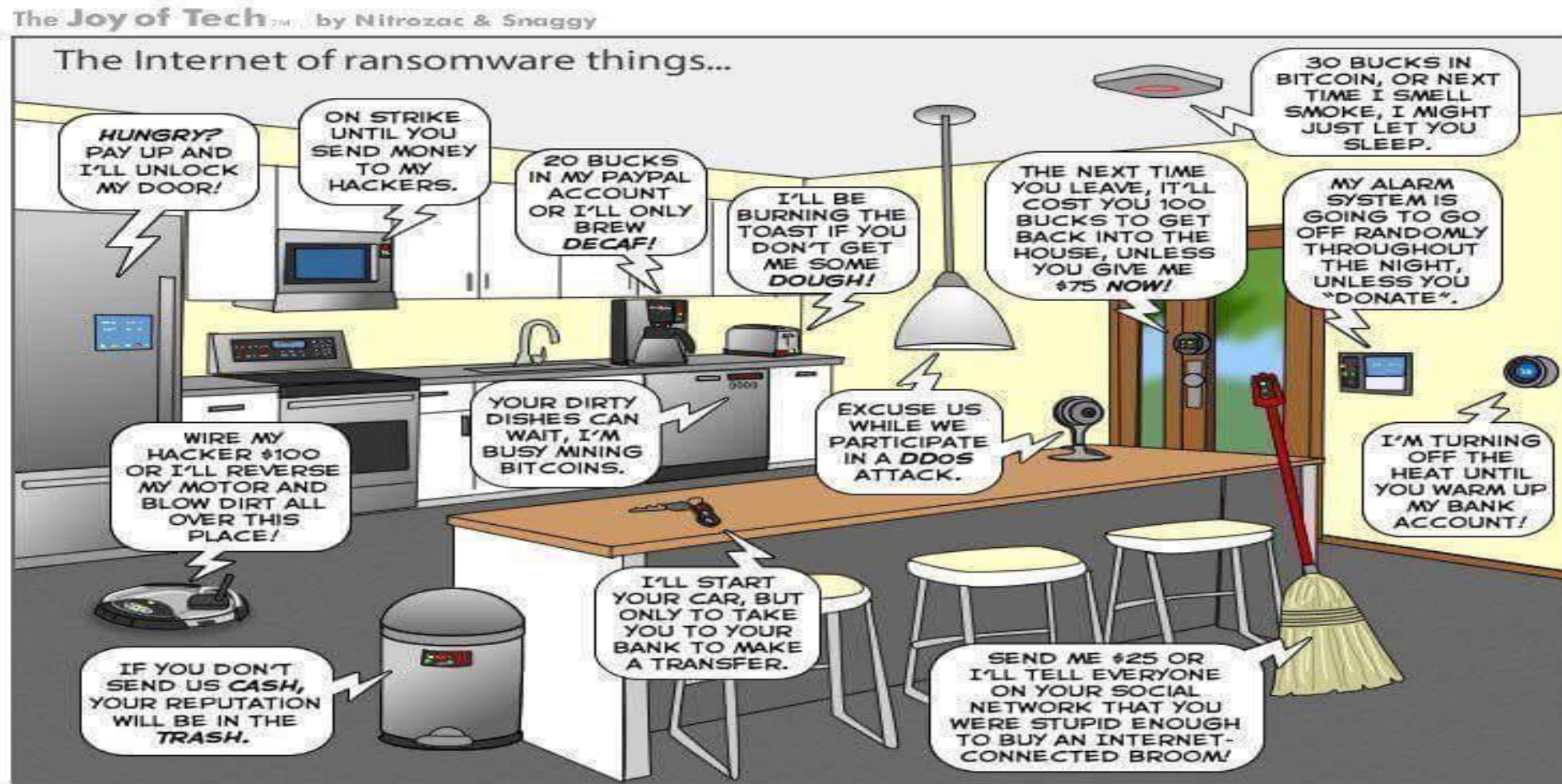
Source: <https://www.checkmarx.com/technology/application-security-testing/>

- Ασφάλεια και Διαχείριση Κινητών Συσκευών

Πέρα από το GDPR / ΓΚΠΔ: Το OWASP Top 10

Top 10 2013	Top 10 2017
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting
A4 – Insecure Direct Object References	A4 – Broken Access Control
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control	A7 – Insufficient Attack Protection
A8 – Cross-site Request Forgery (CSRF)	A8 – Cross-site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	A10 – Unprotected APIs

Μετεξεταστέοι: IoT (in)security

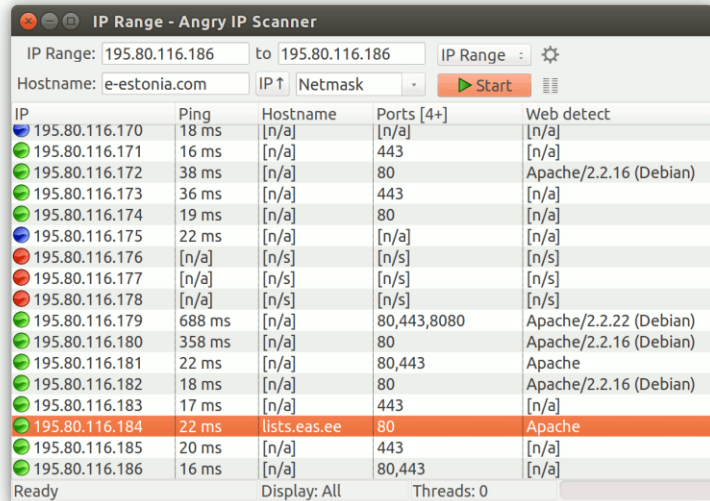


You can help us keep the comics coming by becoming a patron!
www.patreon/joyoftech

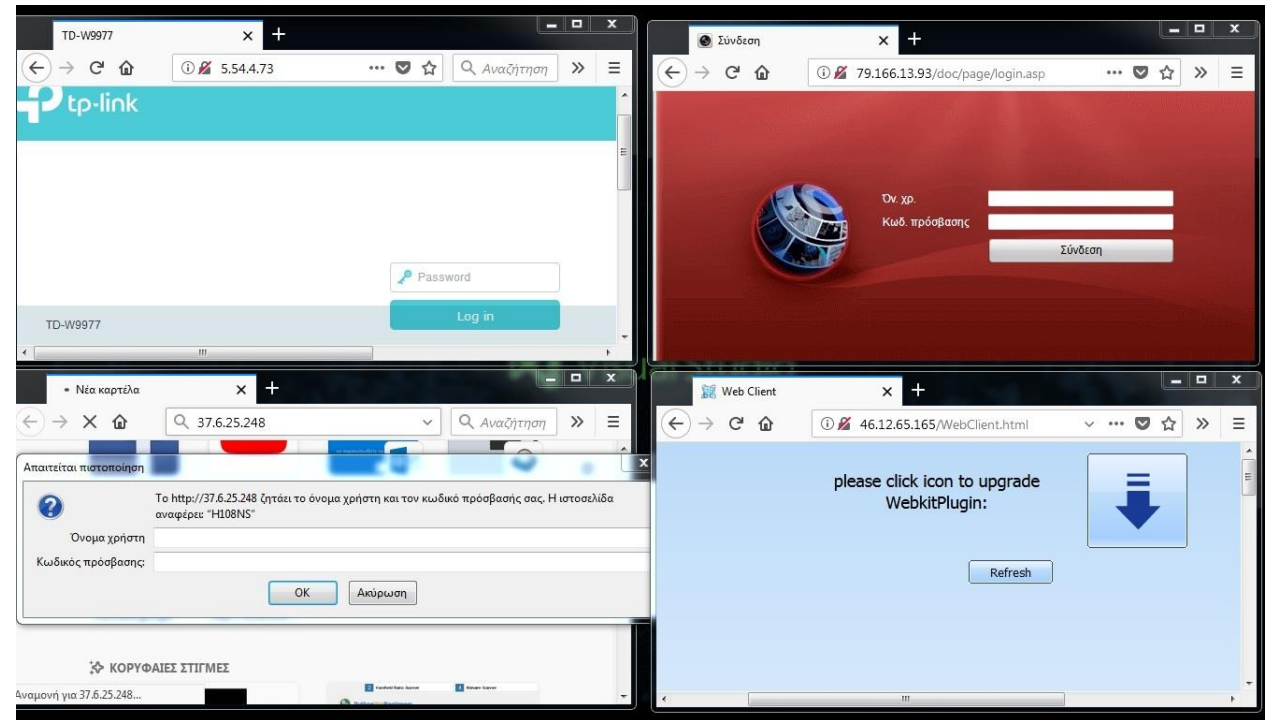
joyoftech.com

Ένα μικρό πείραμα

Μετά από λίγο: Απομακρυσμένης πρόσβασης δρομολογητές για περαιτέρω αξιολόγηση με έναν σαρωτή θυρών (port scanner)



IP	Ping	Hostname	Ports [4+]	Web detect
195.80.116.170	18 ms	[n/a]	[n/a]	[n/a]
195.80.116.171	16 ms	[n/a]	443	[n/a]
195.80.116.172	38 ms	[n/a]	80	Apache/2.2.16 (Debian)
195.80.116.173	36 ms	[n/a]	443	[n/a]
195.80.116.174	19 ms	[n/a]	80	[n/a]
195.80.116.175	22 ms	[n/a]	[n/a]	[n/a]
195.80.116.176	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.177	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.178	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.179	688 ms	[n/a]	80,443,8080	Apache/2.2.22 (Debian)
195.80.116.180	358 ms	[n/a]	80	Apache/2.2.16 (Debian)
195.80.116.181	22 ms	[n/a]	80,443	Apache
195.80.116.182	18 ms	[n/a]	80	Apache/2.2.16 (Debian)
195.80.116.183	17 ms	[n/a]	443	[n/a]
195.80.116.184	22 ms	lists.eas.ee	80	Apache
195.80.116.185	20 ms	[n/a]	443	[n/a]
195.80.116.186	16 ms	[n/a]	80,443	[n/a]



Από τον φοιτητή του ΤΕΙ Θεσσαλίας: Χρήστος Ζέρβας

SAINT Ο Χάρτης του Κυβερνοεγκλήματος

Deep Web Probes

Online:

- Markets
- Forums
- Vendor Shops

Offline:

- Cybercrime Statistical Data
- Archived of Black Markets

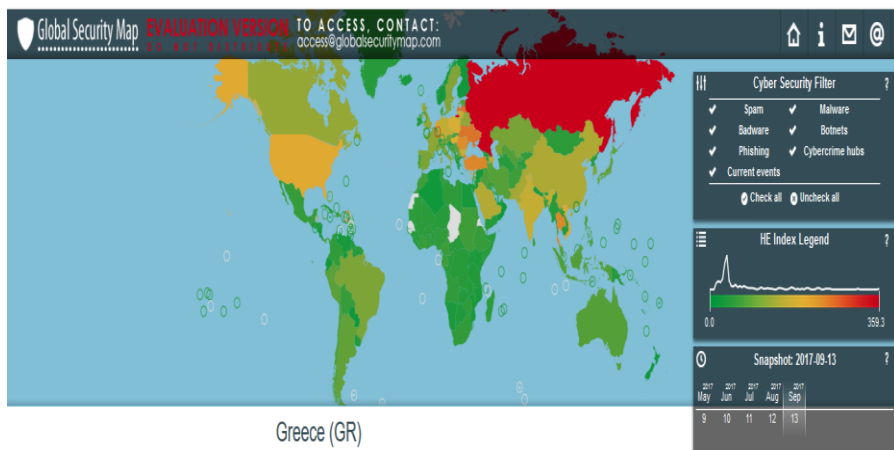
Dark Market Analysis

- Stolen Data:
 - Hacked Accounts
 - Credit Cards
- CaaS: Crime as a Service:
 - Botnets
 - Spam
 - Hackers for hire
 - Malware
 - Bulletproof providers
 - Pharma programs
- General Black Market Activity:
 - Posts
 - Members



SAINT: Ο Χάρτης του Κυβερνοεγκλήματος

SAINT: Ο Χάρτης του Κυβερνοεγκλήματος



Greece (GR)

Cyber security summary

Greece is ranked #911 out of 224 countries on the Host Exploit index for cyber security (HE-index) at 2017-09-13 (a higher rank equals worse security). The lowest ranking of Greece was 53 on 2014-09-06. The country's highest ranking was observed on 2011-12-24, where the country ranked 216.

There are a total of 145 ASs (Autonomous Systems) linked to this country. 133 (91.7%) are registered to this country and, of these, 13 (9.0%) are routed from another country. Of the ASs belonging to Greece, 12 (8.3%) ASs are routed abroad of the country.

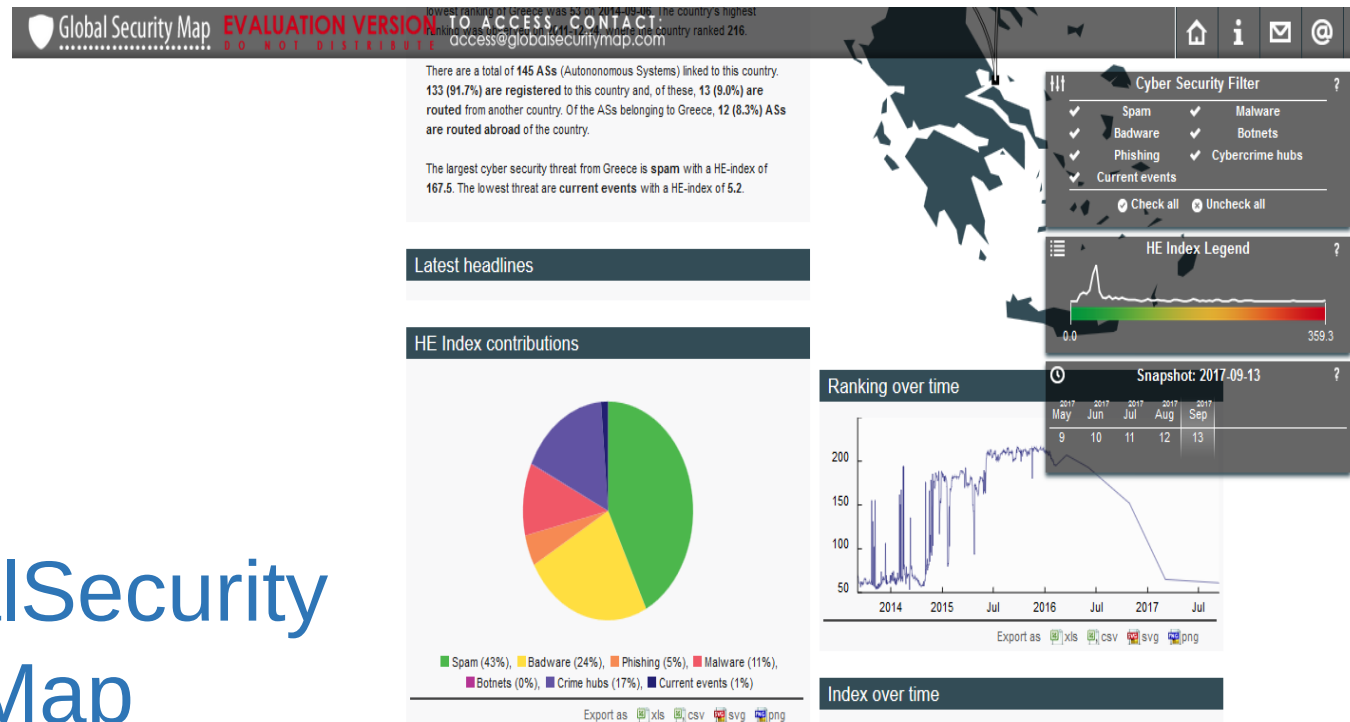
The largest cyber security threat from Greece is spam with a HE-index of 167.5. The lowest threat are current events with a HE-index of 5.2.

Latest headlines



GlobalSecurity Map

<http://globalsecuritymap.com/#>



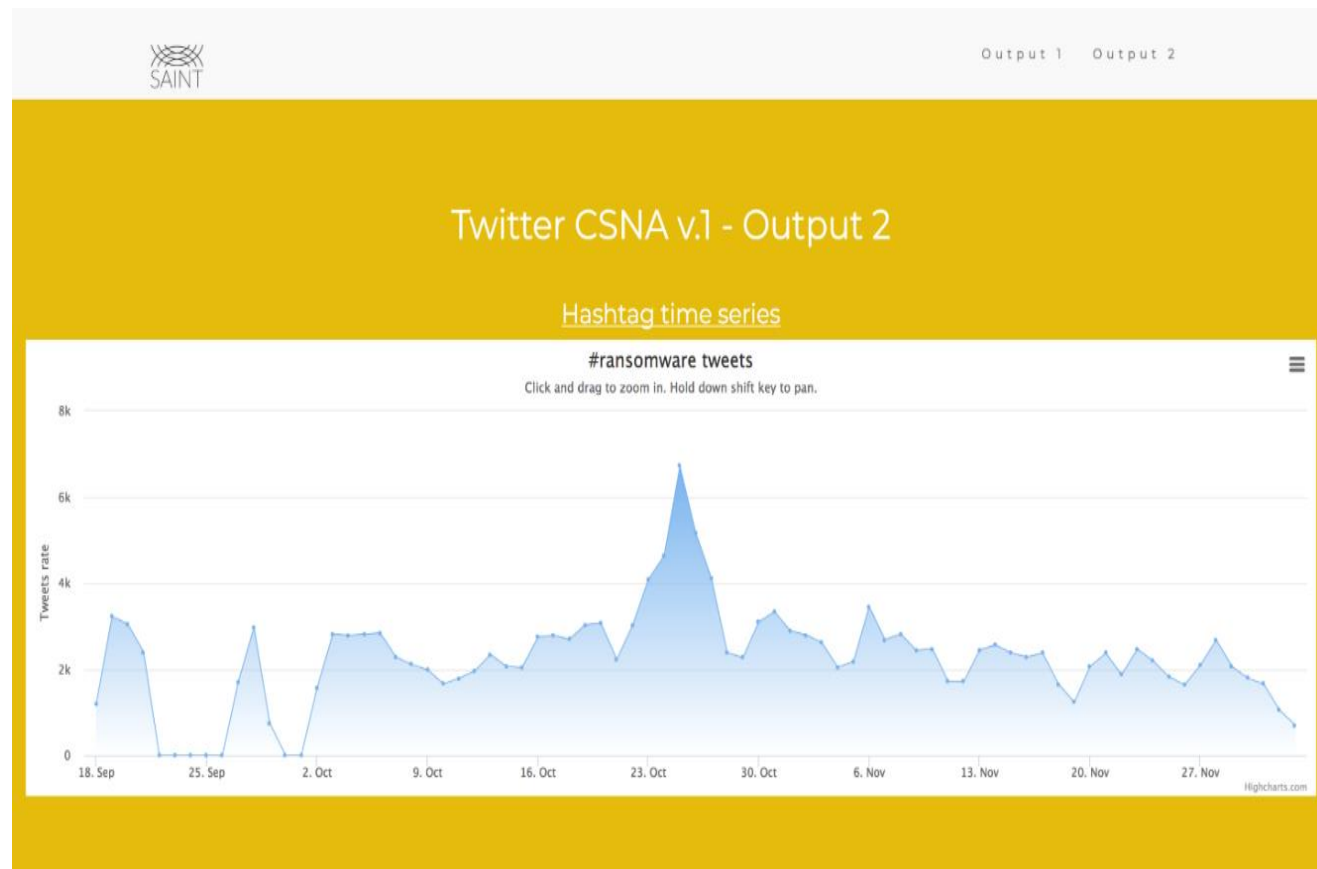
The Project is funded by the European Union

SAINT: Ο Χάρτης του Κυβερνοεγκλήματος

<http://150.140.193.154:2080/saint/>

Ανάλυση κοινωνικών δικτύων - Social Network Analysis (SNA):

Twitter hastags frequency monitoring:
 #bugs #bounties #malware #hacking #spam
 #osint #deepweb #darkmarket
 #vulnerability #0day #apt #rat #bot #c&c
 #zombiepc #exploit #carders #phising #ddos
 #stressers #backdoor #logicbomb #dox
 #shell #blackhat #spoof #socialengineer
 #trojan #ransomware #crimeware #resolver
 #scriptkiddie #root #rootkit #deface #XSS
 #SQLinjection #bufferoverflow #hactivism



GDPR is coming... Are we ready?

10-Day Privacy Flag Challenge

10 days, 10 sites, 10 friends

1. Download the Add-On via Chrome web store and/or the App via Google Play
2. Evaluate at least one website/App each day
3. Get a friend to join the challenge!



**PRIVACY
FLAG**



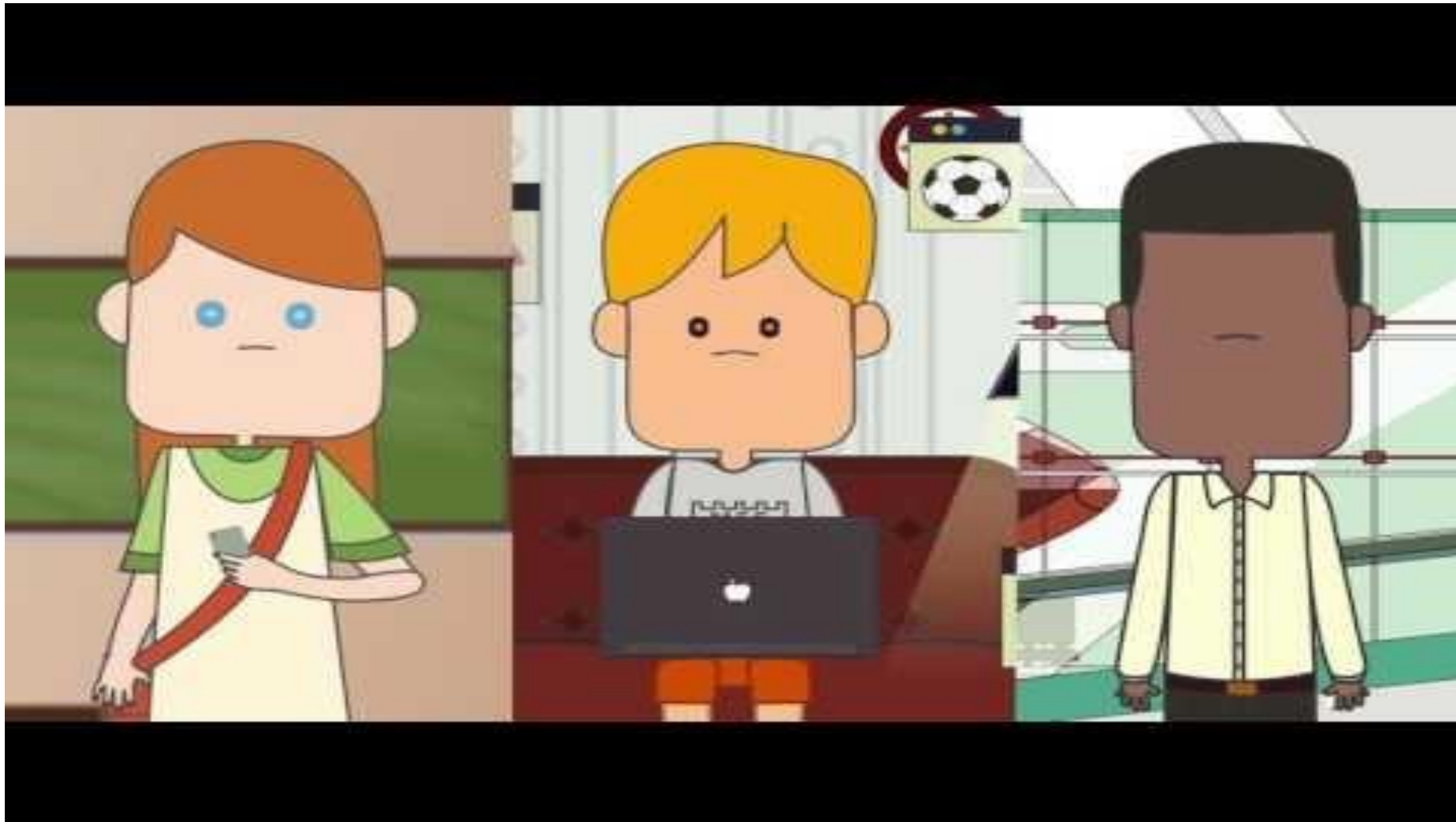
Co-funded by the
European Union



Co-funded by the
Swiss Confederation

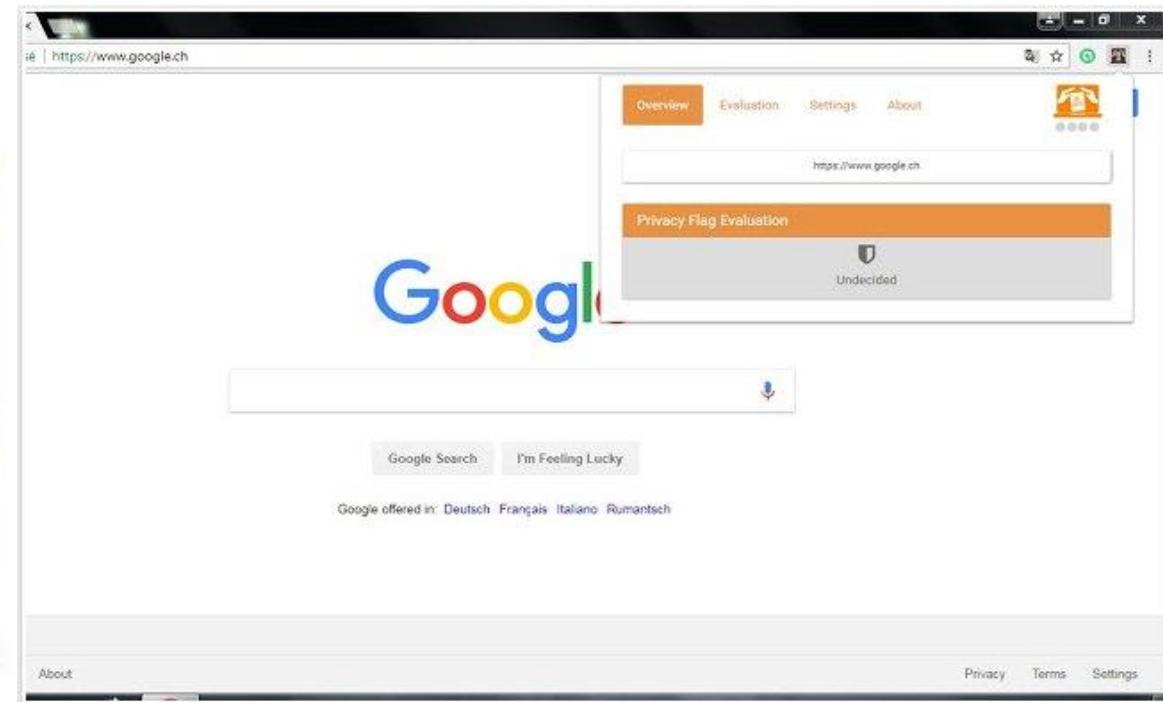
Help us make the Internet safer

Σύντομα κοντά σας: PrivacyFlag

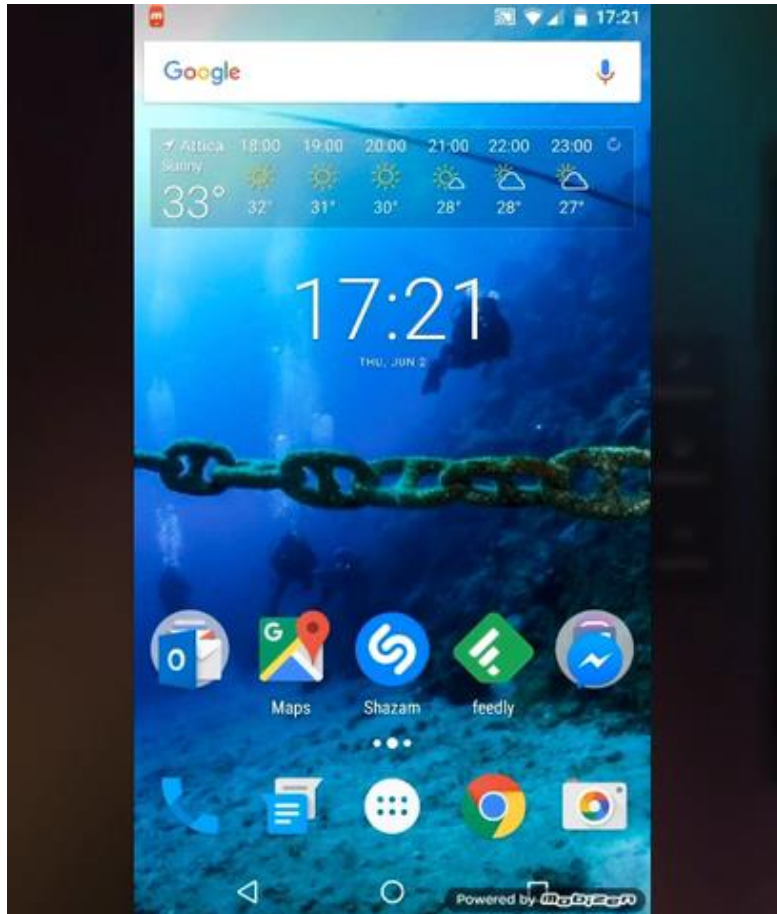


Ανάλυση Κινδύνων για την Ιδιωτικότητα μέσω Πληθοπορισμού

Το Top25 Threat Matrix αναλύεται αυτόματα ή και χειροκίνητα



Ανάλυση Κινδύνων για την Ιδιωτικότητα μέσω Πληθοπορισμού



Ανάλυση Κινδύνων για την Ιδιωτικότητα μέσω Πληθοπορισμού

The Top25 Web Privacy Threat Matrix

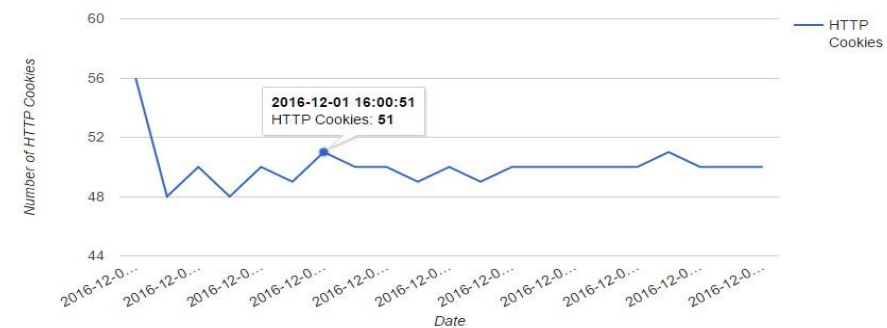
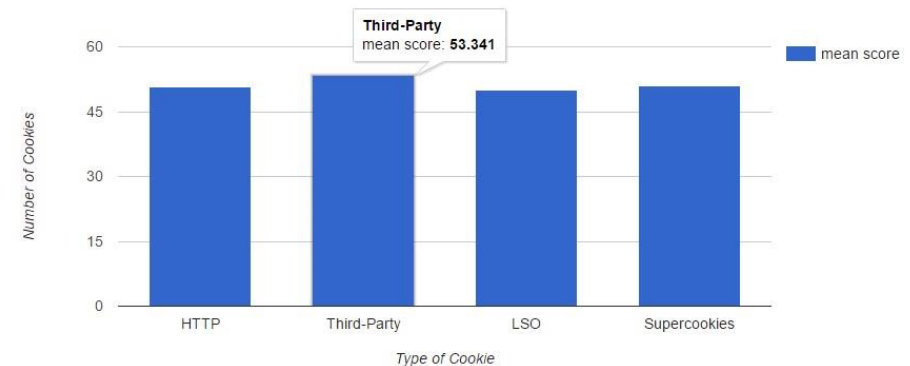
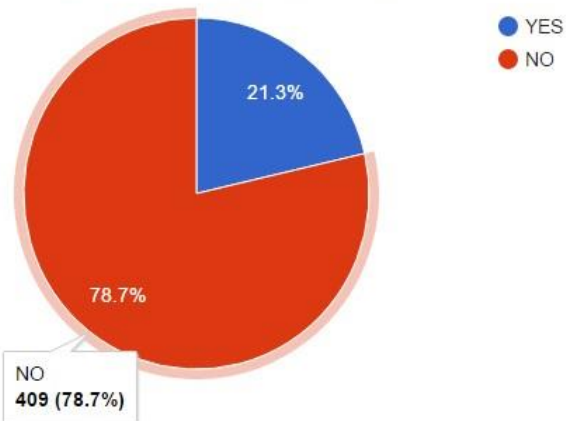
	The problem to address	Output
1	Does the website provide data encryption (SSL/TLS)?	True / False
2	Does the website provide HSTS?	True / False
3	Is the encryption method (cipher suite) negotiated between client and server considered as secure?	True / False
4	What information does the website/server directly learn about a user (using forms)?	submitted information
5	Does the website use a trustworthy certification chain?	True / False
6	Does the website use Certificate pinning?	True / False
7	Which communication parties is data transferred to?	list of parties
8	Does the website use HTTP cookies?	[0...n]
9	Does the website use Third party cookies?	[0...n]
10	Does the site exploits users Web history?	True / False
11	Does the website use HTML5 Web SQL database	True / False
12	Does the website use LSOs?	[0...n]
13	Does the website use Supercookies?	[0...n]

	The problem to address	Output
14	Does the website use technologies with known security issues - PDF?	True / False
15	Does the website use known fingerprinting techniques?	[0...n]
16	Does the website use technologies with known security issues - Flash?	True / False
17	Does the website contain links to malicious sites (Google's Safe browsing API)?	[0...n]
18	Does the website use potentially dangerous advanced HTML5 APIs: Web Audio API?	True / False
19	Does the website use potentially dangerous advanced HTML5 APIs: WebRTC?	True / False
20	Does the website use potentially dangerous advanced HTML5 APIs: Geolocation (GPS)?	True / False
21	Does the website use technologies with known security issues - ActiveX?	True / False
22	Does the website use technologies with known security issues - Java?	True / False
23	Does the website use technologies with known security issues - Silverlight?	True / False
24	Does the website use HTML5 Local Storage?	True / False
25	Does the website comply with any known privacy policy eTrust, P3P, published privacy policy?	True / False

Παρατηρητήριο για την Ασφάλεια και Ιδιωτικότητα στο Διαδίκτυο

- <http://app.privacyflag.eu:2080/privacy/addon/observatory.php>
- Τεχνολογίες ιδιωτικότητας με μια ματιά

Websites that provide data encryption (SSL/TLS)



Συμπεράσματα

- Τα δεδομένα σας ενδέχεται να είναι προϊόν, αλλά η ασφάλεια και η προστασία προσωπικών δεδομένων είναι μια διαδικασία που δεν αποτελεί προϊόν
- Το GDPR δεν είναι το τέλος του κόσμου
- Εμπιστοσύνη σε επαγγελματίες - Αποφύγετε τους ερασιτέχνες
- "Доверяй, но проверяй" {Dovergai, no proveryai} (εμπιστέψου, αλλά επιβεβαίωσε)



Ευχαριστώ για την προσοχή σας!

E&A

ΒΑΣΙΛΕΙΟΣ ΒΛΑΧΟΣ

ΕΠΙΚΟΥΡΟΣ ΚΑΘΗΓΗΤΗΣ Τ.Ε.Ι. ΘΕΣΣΑΛΙΑΣ

ΜΕΛΟΣ Δ.Σ. ΕΜηΠΕΕ

ΗΛΕΚΤΡΟΝΙΚΟΣ ΜΗΧΑΝΙΚΟΣ ΚΑΙ ΜΗΧΑΝΙΚΟΣ ΥΠΟΛΟΓΙΣΤΩΝ