Panos Kalorogiannis
System Security Engineer

Alexandros Malathounis
Network Security Engineer

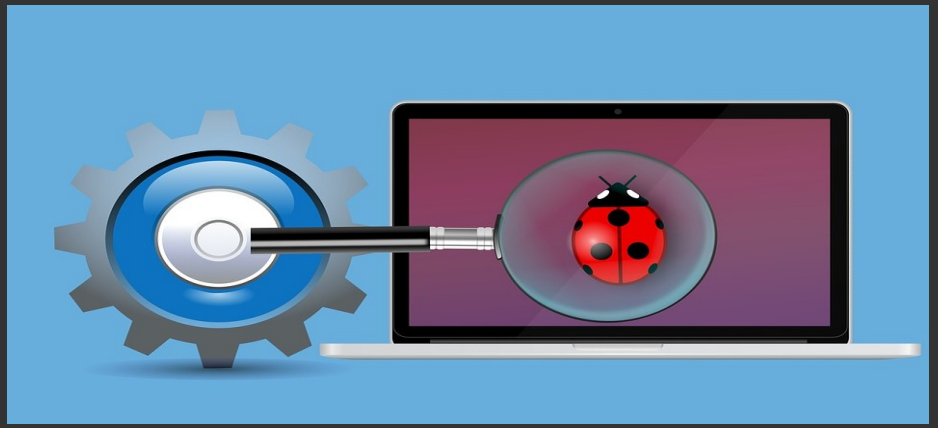
Konstantinos Lymperis
Penetration Tester

Μία Περίληψη των γενονότων του 2020..

Σημαντικές απειλές:

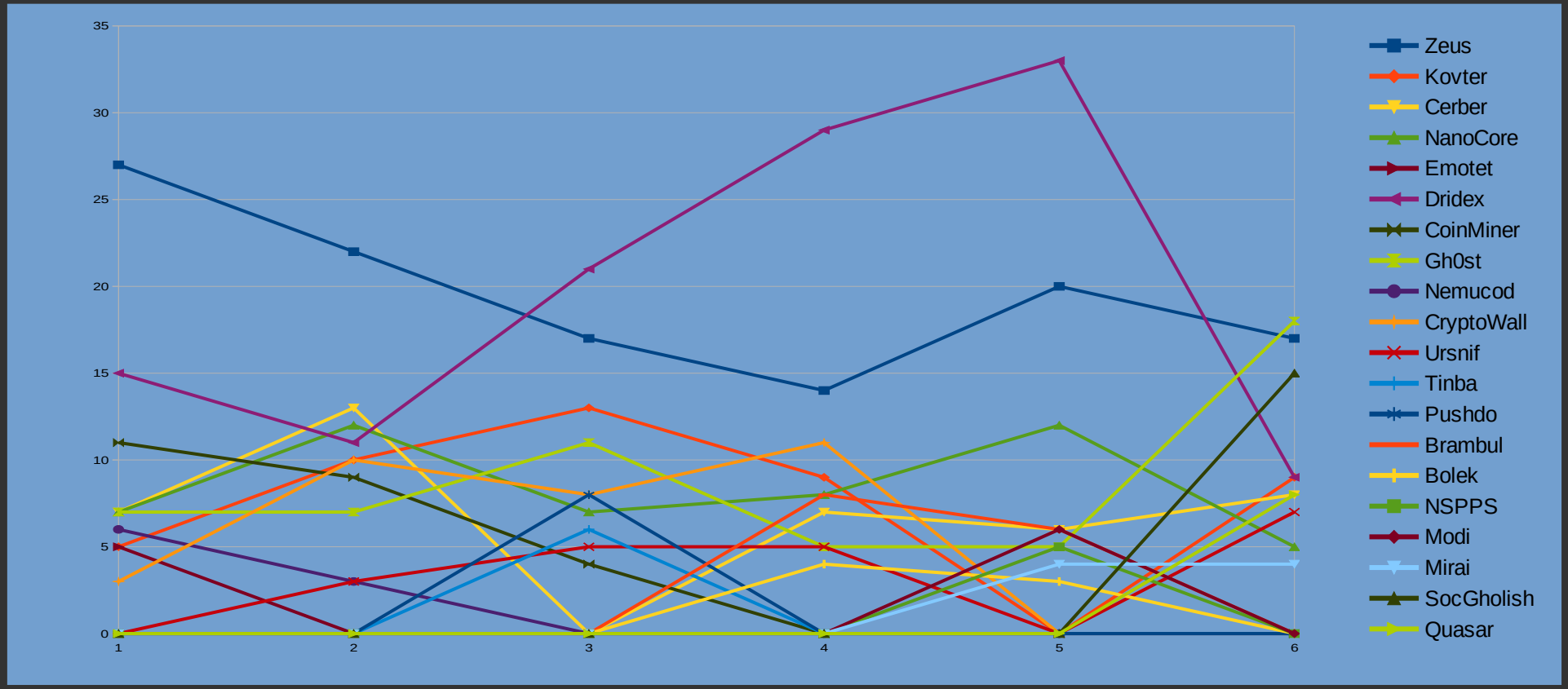
- Επιθέσεις με χρήση Trojan, RAT κακόβουλου λογισμικού
- Επιθέσεις με χρήση Ransomware
- Επιθέσεις Phishing & Social Engineering
- Διαρροή Δεδομένων (Data Breaches)

Επιθέσεις με Trojan, RAT κακόβουλο λογισμικό

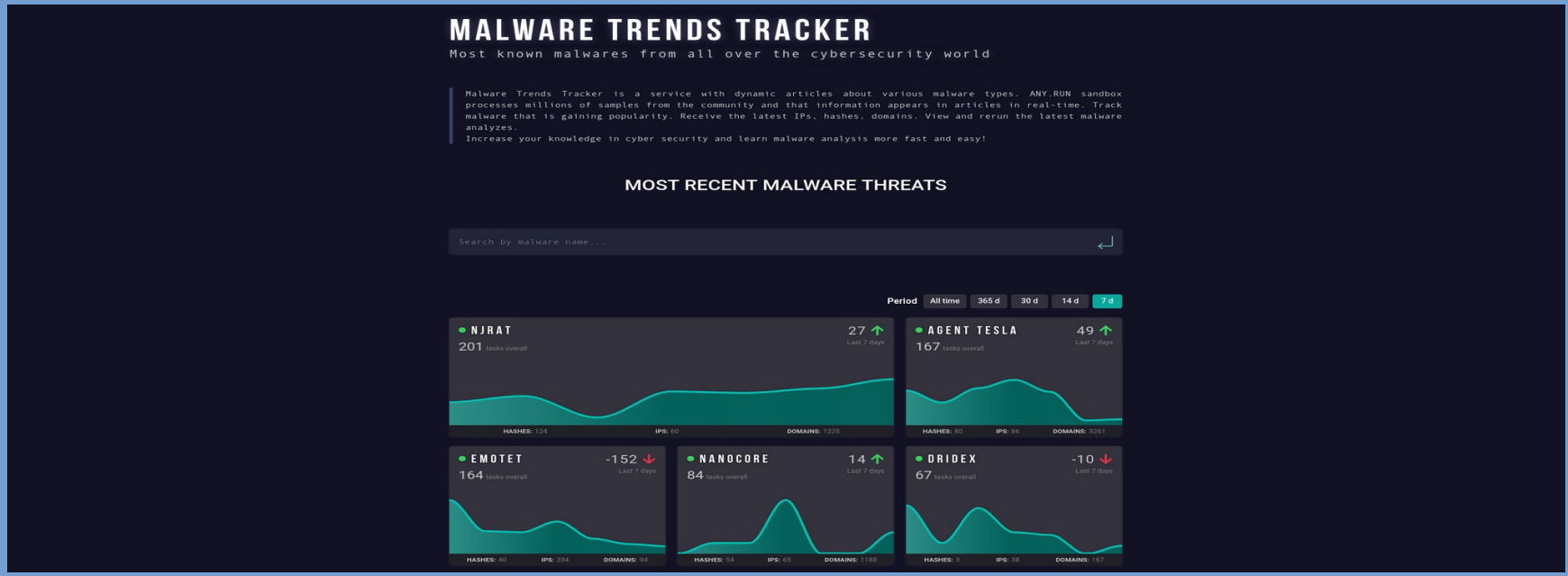


Επιθέσεις με Trojan, RAT κακόβουλο λογισμικό(2)

Επιθέσεις με Trojan, RAT κακόβουλο λογισμικό(3)



Παρατήρηση Trojan, RAT κακόβουλου λογισμικού(4)



Link: https://any.run/malware-trends/

Προστασία από Trojan, RAT κακόβουλο λογισμικό(5)

- Αναβάθμιση των αποθετηρίων και των πακέτων του Λειτουργικού Συστήματος.

  Σε Debian/Ubuntu: apt update && apt full-upgrade

  Σε Redhat/Centos: yum update ή dnf update
- Έλεγχος της ψηφιακής υπογραφής του αρχείου.

  Εργαλεία: sha1sum, sha512sum, md5sum
- Έλεγχο του αρχείου με κάποιο AV ή στο Virus Total. Link: https://www.virustotal.com/gui/

  Ανοιχτού κώδικα Anti-Virus: ClamAV
- Χρήση πληροφοριακών συστημάτων σε κρυπτογραφημένα δίκτυα.

Επιθέσεις με χρήση Ransomware

Maze Ransomware

RANSOM

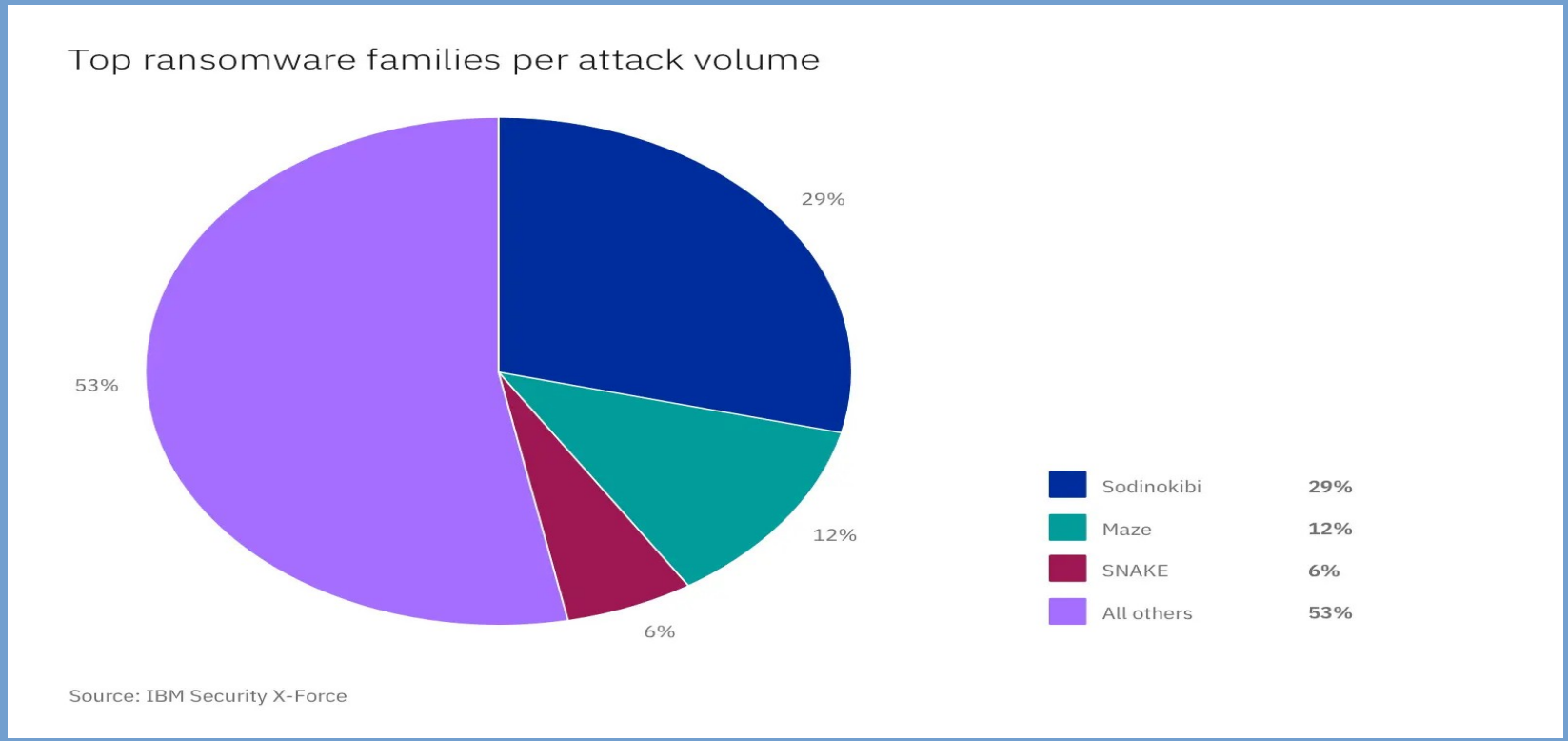
Επιθέσεις με χρήση Ransomware(2)

- 25% αύξηση των επιθέσεων με Ransomware το Q1 του 2020, από το Q4 του 2019
- Δημοφιλή Ransomware: Maze, Ryuk, Sodinokibi, DoppelPaymer
- Η ζημιά που έχει επιφέρει μέχρι στιγμής: $144 εκατ.

Σύμφωνα με το IBM Security X-Force:

- Το 41% των επιθέσεων, γίνεται σε εταιρίες παροχής υπηρεσιών.
- Οι επιτειθέμενοι στοχεύουν Πανεπιστήμια και σχολεία.

Επιθέσεις με χρήση Ransomware(3)



Επιθέσεις με χρήση Ransomware(4)

	Maze Ransomware	Ryuk Ransomware	Sodinokibi Ransomware	DoppelPaymer Ransomware
Exploited Vulnerability	CVE-2018-15982 CVE-2018-4878 CVE-2019-11510 CVE-2018-8174	CVE-2013-2618 CVE-2017-6884 CVE-2018-8389 CVE-2018-12808	CVE-2019-2725	CVE-2019-19781

Επιθέσεις με χρήση Ransomware(4)

Vulnerability Details : CVE-2018-4878

A use-after-free vulnerability was discovered in Adobe Flash Player before 28.0.0.161. This vulnerability occurs due to a dangling pointer in the Primetime SDK related to media player handling of listener objects. A successful attack can lead to arbitrary code execution. This was exploited in the wild in January and February 2018.

Publish Date : 2018-02-06 Last Update Date : 2018-05-03

Collapse All Expand All Select Select&Copy Scroll To Comments External Links

Search Twitter Search YouTube Search Google

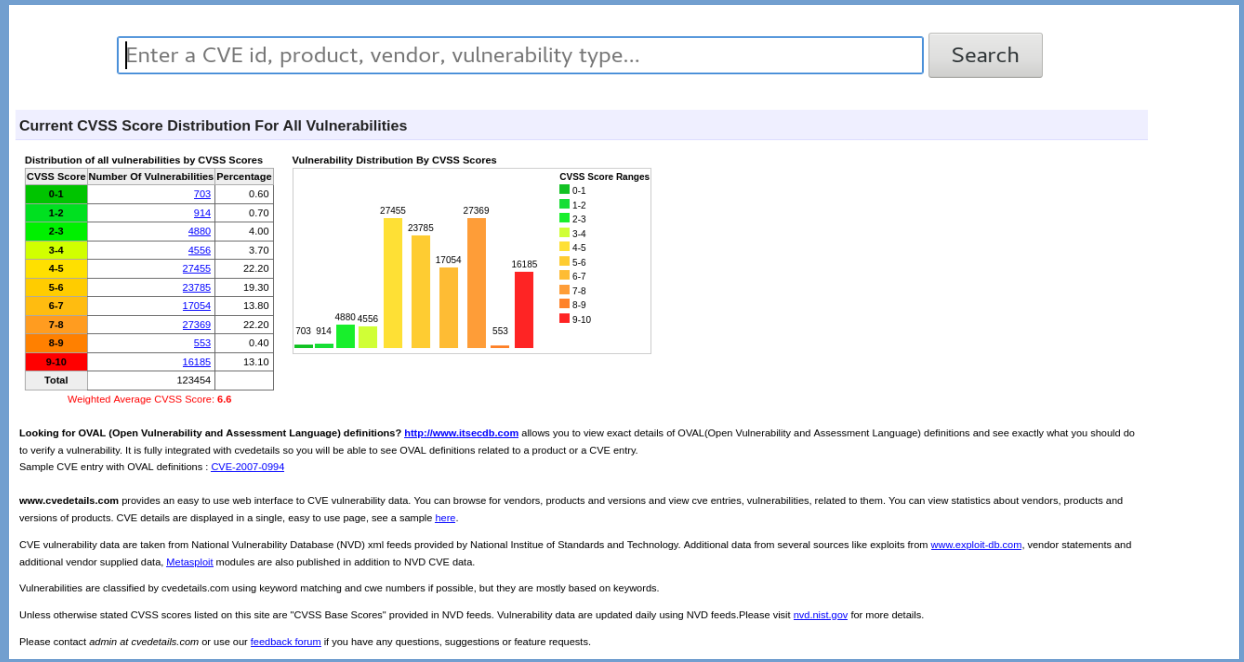
- CVSS Scores & Vulnerability Types

CVSS Score	7.5
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	416

- Products Affected By CVE-2018-4878

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	Application	Adobe	Flash Player	-				Version Details Vulnerabilities
2	Application	Adobe	Flash Player	2				Version Details Vulnerabilities
3	Application	Adobe	Flash Player	3				Version Details Vulnerabilities
4	Application	Adobe	Flash Player	4				Version Details Vulnerabilities
5	Application	Adobe	Flash Player	5				Version Details Vulnerabilities
6	Application	Adobe	Flash Player	6				Version Details Vulnerabilities
7	Application	Adobe	Flash Player	6.0.21.0				Version Details Vulnerabilities
8	Application	Adobe	Flash Player	6.0.79				Version Details Vulnerabilities
9	Application	Adobe	Flash Player	7				Version Details Vulnerabilities
10	Application	Adobe	Flash Player	7.0				Version Details Vulnerabilities

Επιθέσεις με χρήση Ransomware(4)



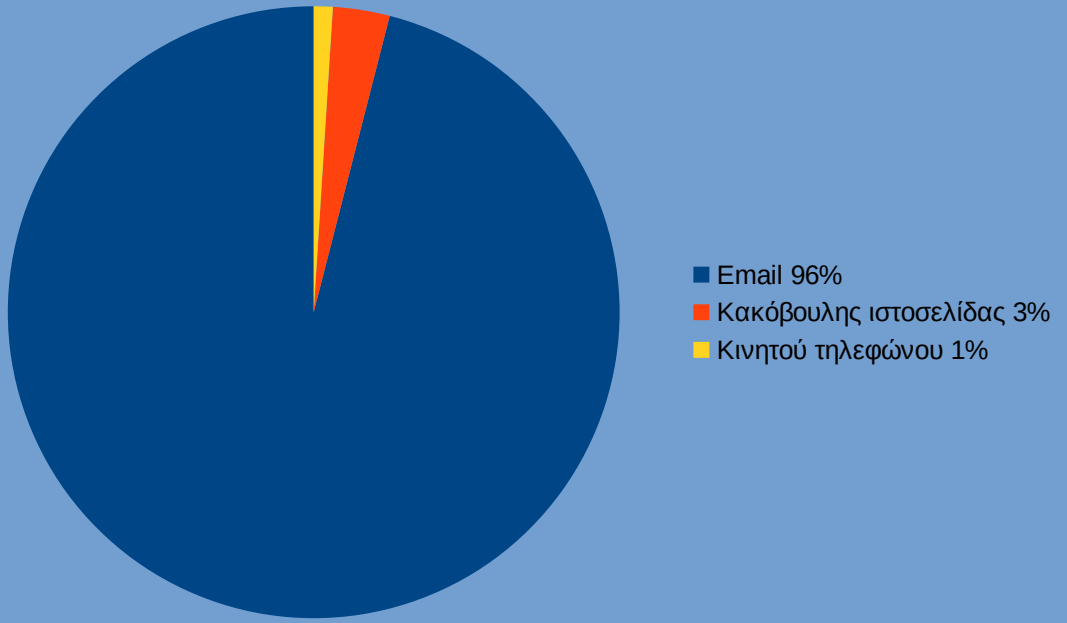
Link: https://www.cvedetails.com/

Phishing Επιθέσεις

Phishing Επιθέσεις - Στατιστικά

Παγκοσμίως:

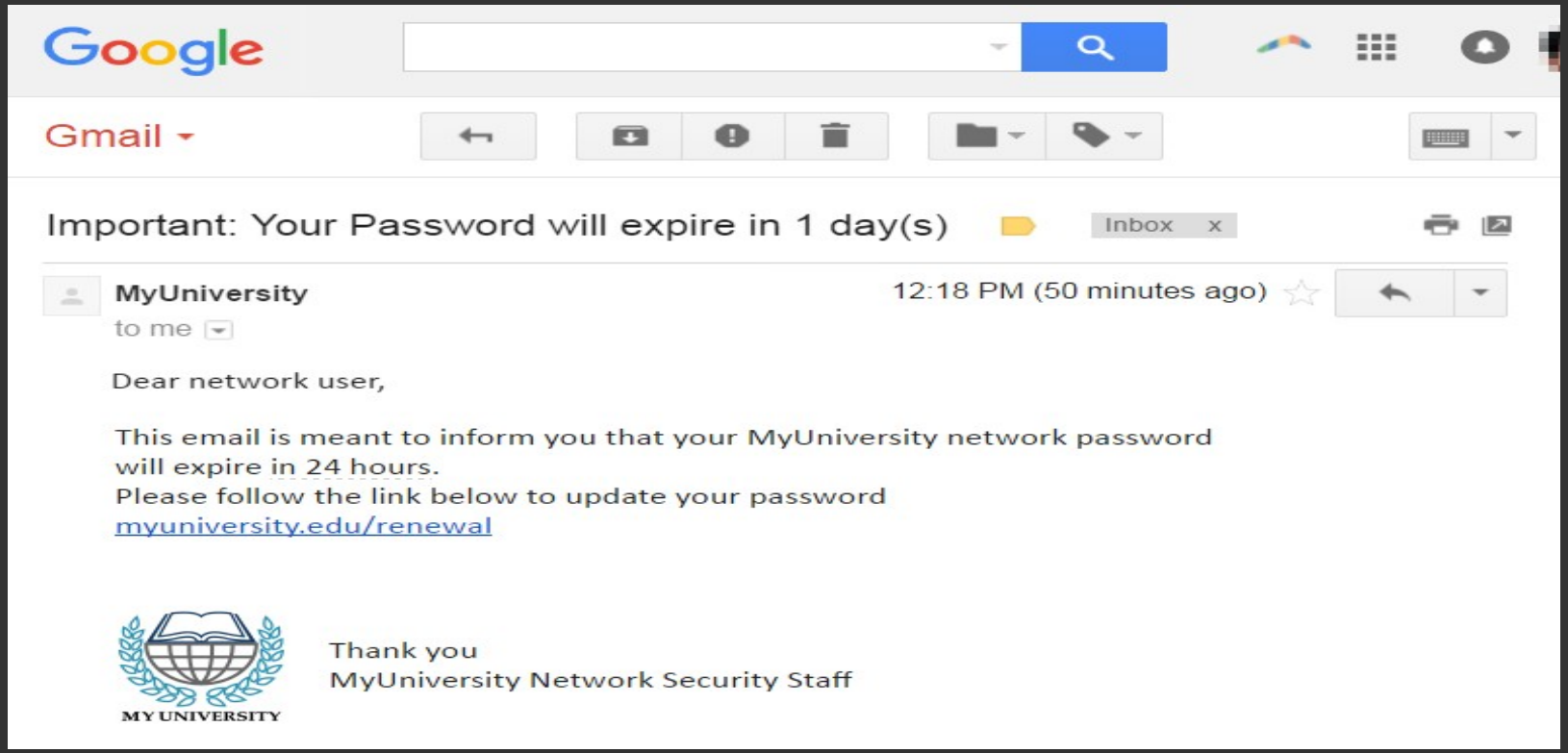
- Το 80% των κυβερνοεπιθέσεων
- 600% αύξηση(Covid-19)
- 65% των Οργανισμών/Επιχειρήσεων
- 1 Phishing / 39 sec
- 90% Data breach



Phishing Επιθέσεις - Κατηγορίες

- Email Phishing
- Spear Phishing
- Whaling
- Smishing
- Vishing
- Clone Phishing

Phishing Επιθέσεις – Email Phishing



Phishing Επιθέσεις – Spear Phishing and Whaling

Χαρακτηριστικά:

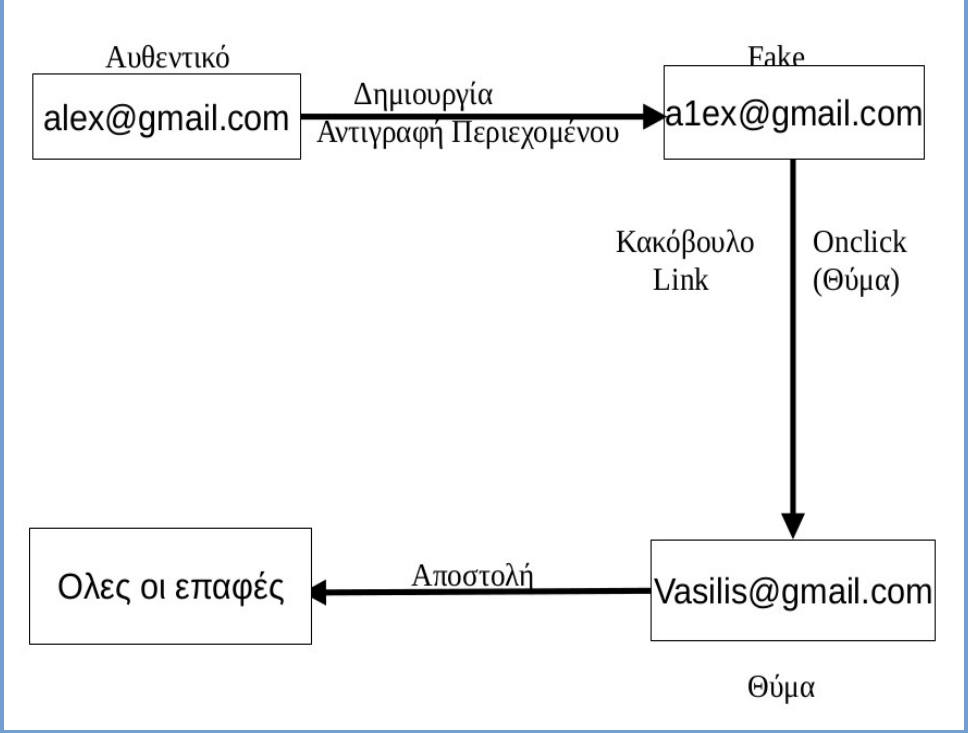
- Στοχευμένη επίθεση
- Ιδιαίτερο Υφος
- Συλλογή πληροφοριών
- Συγκεκριμένα κίνητρα

Phishing Επιθέσεις – Smishing and Vishing

Link: https://www.youtube.com/watch?v=fHhNWAKw0bY&t=184s

Phishing Επιθέσεις – Clone Phishing

- Πλαστογραφημένη διεύθυνση
- Αντικατάσταση αρχείου
- Επανάληψη μηνύματος



Impersonated Brands

Microsoft

YAHOO!

ebay

PayPal

NETFLIX

amazon

Phishing Επιθέσεις – Προστασία(1)

Προσοχή στην διεύθυνση email:

alexandros@fosscomm.com

al3xandros@fosscomm.com

alexandro$@fosscomm.com

alexandros@foscomm.com

alexandros@f0sscomm.com

alexandr0s@fosscomm.com

alexandros@fosscornm.com

Phishing Επιθέσεις – Προστασία(2)

Συντακτικά λάθη:

Google translate

Ύφος μηνύματος

Τακτικές αποπροσανατολισμού:

Φόβος

Άγχος

Ενθουσιασμός

Άμεση αποστολή δεδομένων:

Προσωπικά στοιχεία

Στοιχεία τρίτων

Οικονομικά δεδομένα

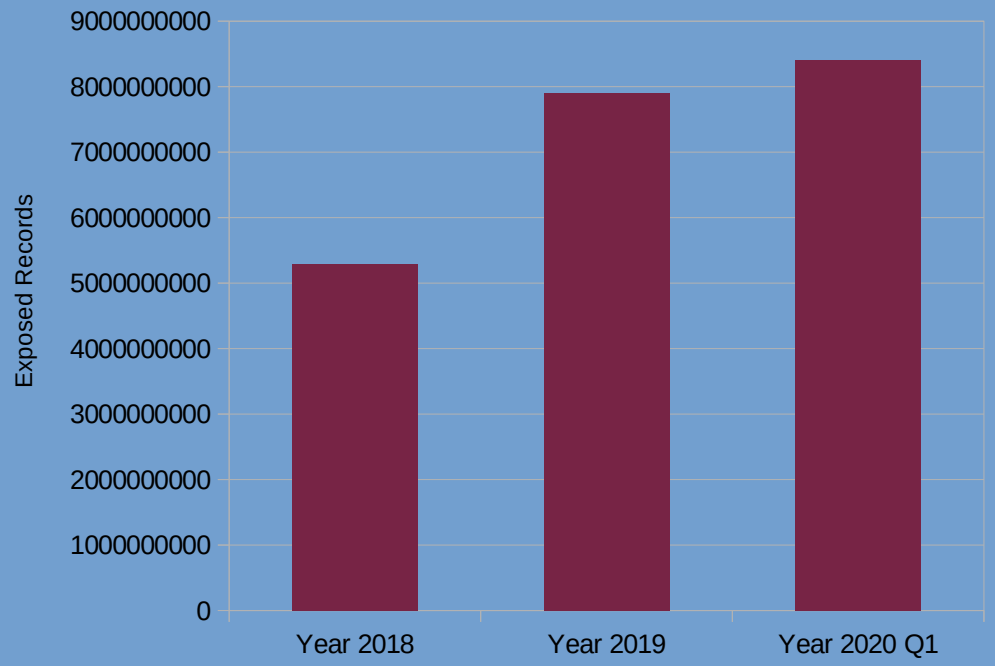
Πληροφορίες σχετικά με το περιβάλλον του χρήστη

Data Breaches

Data Breaches(2)

- Επίθεση στη Marriot International (03/2020) : 5.2 εκατ. guests
- Επίθεση στη Nintendo (04/2020) : 160 χιλ. accounts
- Επίθεση στη Magellan Health (04/2020) : 360 χιλ. patients
- Επίθεση στη Zoom Video Communications (04/2020) : 500 χιλ. accounts
- Επίθεση στη BJC Healthcare (05/2020) : 287,876 patients
- Επίθεση στο Twitter (07/2020) : 130 accounts

Data Breaches(3) – Στατιστικά Μοντέλα



Τέλος Παρουσίασης

Ευχαριστούμε για την προσοχή σας!

Email us:
panoskalorog@gmail.com
a.malathounis@gmail.com