Εθνική Υπηρεσία Πληροφοριών
Διεύθυνση Κυβερνοχώρου
Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT

Περιστατικά Κυβερνοασφάλειας

Ημερίδα Κυβερνοασφάλειας: «Διαχείριση κινδύνου κυβερνοαπειλών: Ανίχνευση, ανάσχεση και κοινοποίηση συμβάντων ασφαλείας»

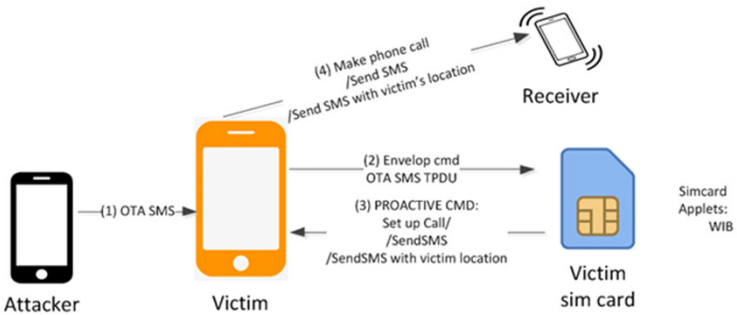
Εθνική Σχολή Δημόσιας Διοίκησης και Αυτοδιοίκησης

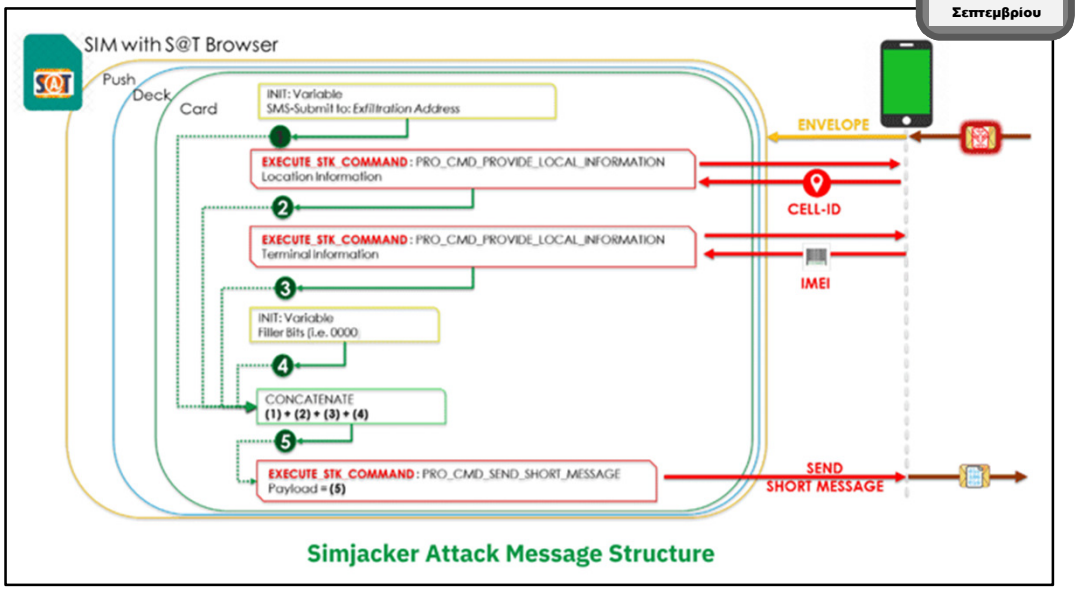
4 Νοεμβρίου 2019


CONNECTION
ELECTRONIC
CYBER ATTACK
ΤΡΕΧΟΥΣΑ
ΕΠΙΚΑΙΡΟΤΗΤΑ


New kinds of cyber attacks

Simjacker Attack

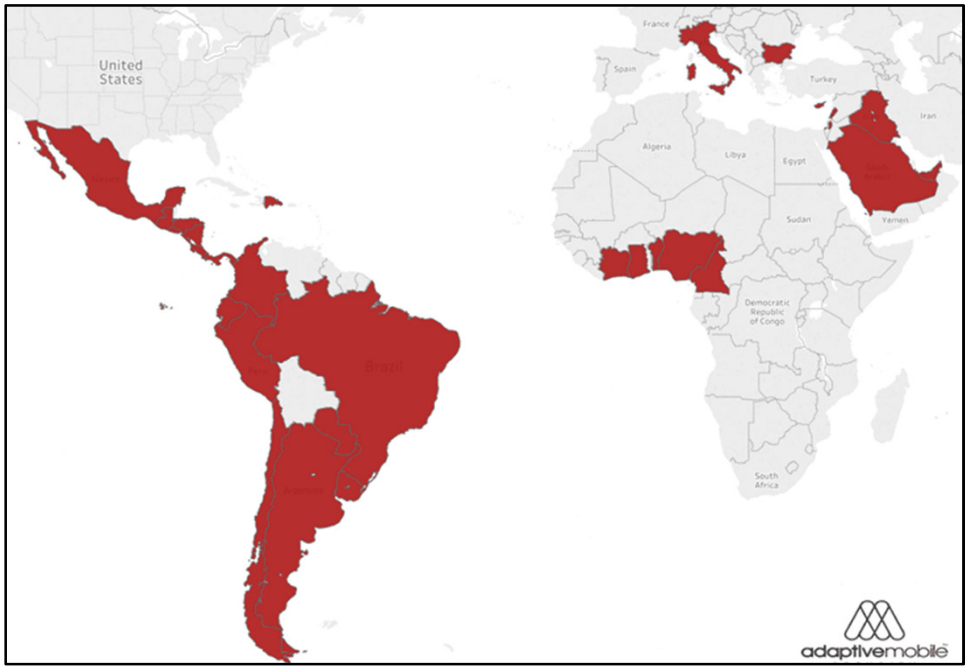




Simcard Applets: WIB

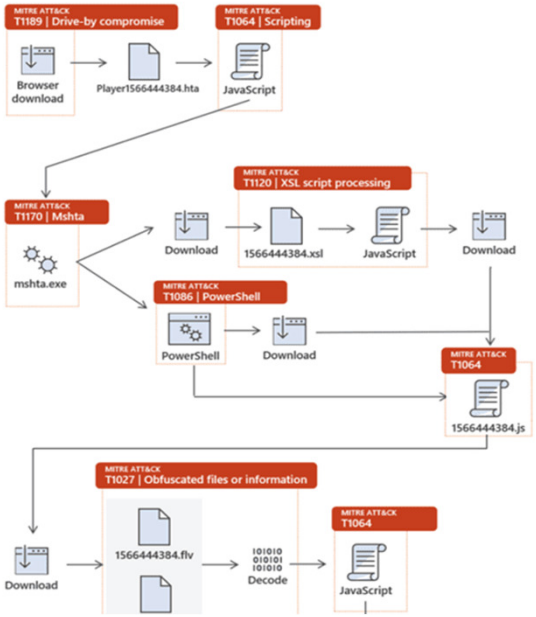
Simjacker Attack

North America: Mexico, Guatemala, Honduras, Costa Rica, Nicaragua, Belize, El Salvador, Dominican Republic, and Panama.
South America: Peru, Colombia, Brazil, Ecuador, Chile, Argentina, Uruguay, and Paraguay.
Africa: Nigeria, Ghana, Benin, Ivory Coast, and Cameroon.
Europe: Italy, Bulgaria, and Cyprus.
Asia: Saudi Arabia, Iraq, Palestine and Lebanon.

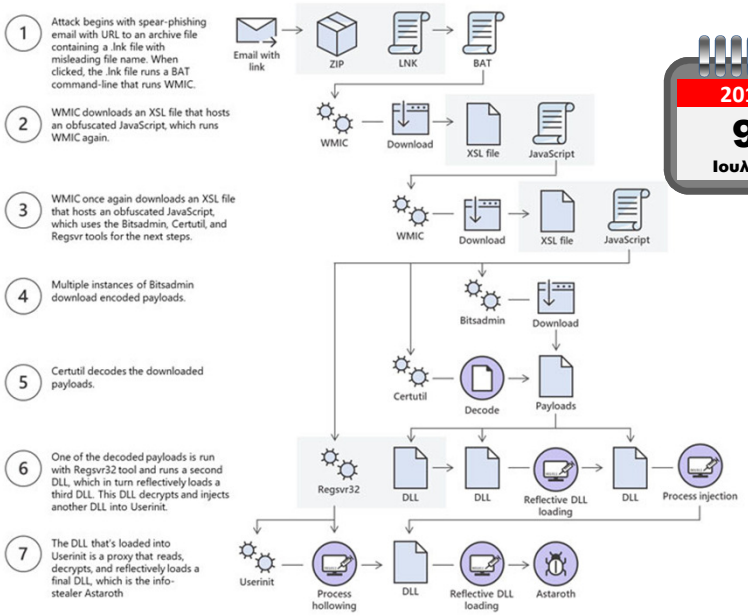


Fileless Malware

Microsoft Warns of a New Rare Fileless Malware Hijacking Windows Computers



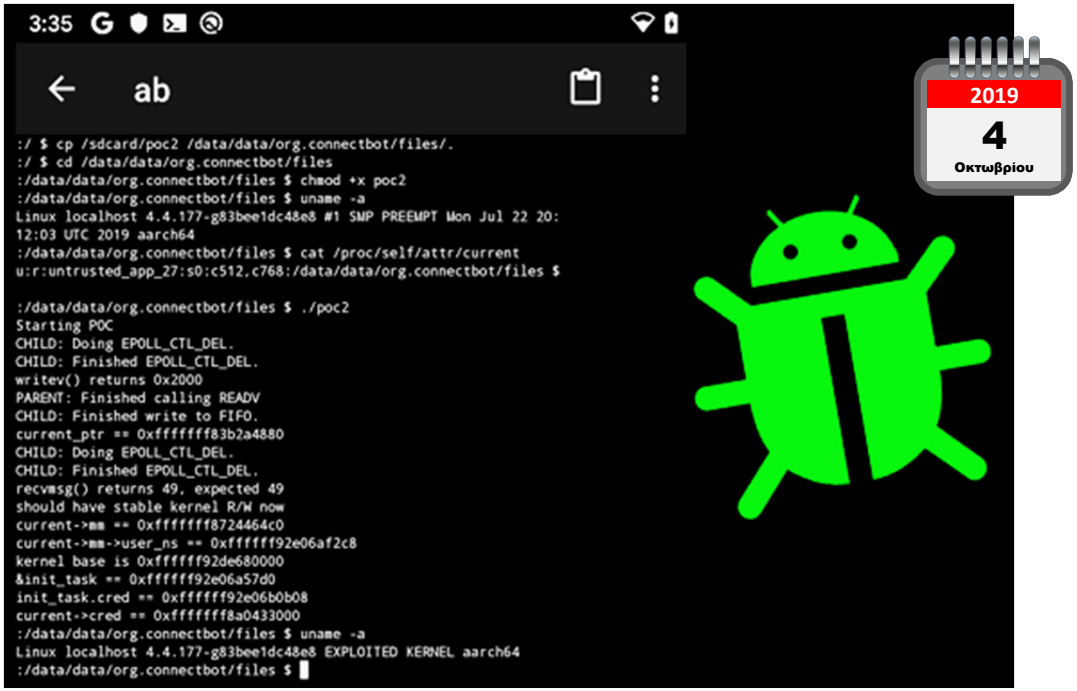
Microsoft Spotted Spike in Astaroth Fileless Malware Attacks




» SECURITY «
DAY
0
#0DAY

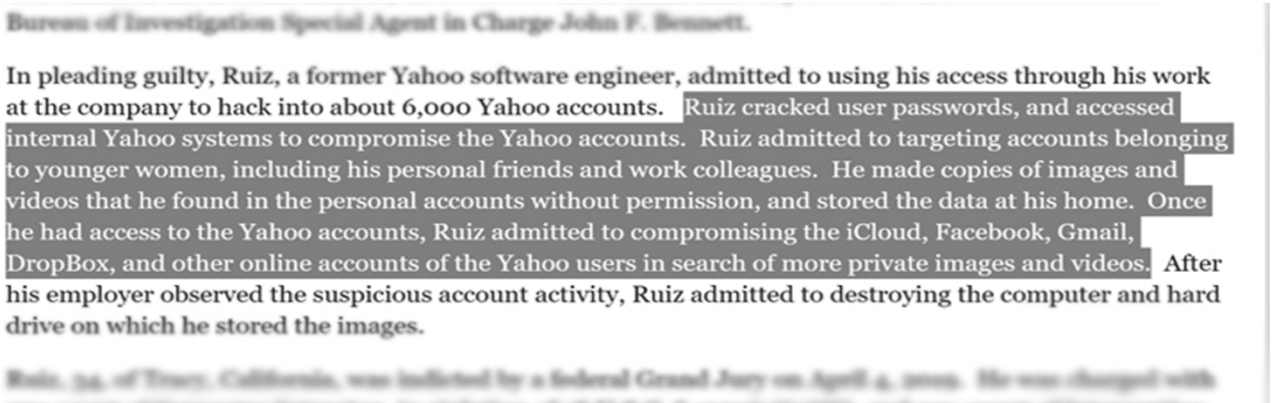
New 0-Day Flaw Affecting Most Android Phones Being Exploited in the Wild

- **Vulnerable Android Devices**
  - Huawei P20
  - Xiaomi Redmi 5A
  - Xiaomi Redmi Note 5
  - Xiaomi A1
  - Samsung S7
  - Samsung S8
  - Samsung S9
  - Pixel 1
  - Pixel 2
- **Android Flaw Can Be Exploited Remotely**
- **Google will release a patch for this vulnerability**




BEWARE INSIDER
THREATS!
20%
15%
35%
50%

Former Yahoo Employee Admits Hacking into 6000 Accounts for Sexual Content



Bureau of Investigation Special Agent in Charge John F. Bennett.

In pleading guilty, Ruiz, a former Yahoo software engineer, admitted to using his access through his work at the company to hack into about 6,000 Yahoo accounts. Ruiz cracked user passwords, and accessed internal Yahoo systems to compromise the Yahoo accounts. Ruiz admitted to targeting accounts belonging to younger women, including his personal friends and work colleagues. He made copies of images and videos that he found in the personal accounts without permission, and stored the data at his home. Once he had access to the Yahoo accounts, Ruiz admitted to compromising the iCloud, Facebook, Gmail, DropBox, and other online accounts of the Yahoo users in search of more private images and videos. After his employer observed the suspicious account activity, Ruiz admitted to destroying the computer and hard drive on which he stored the images.

Ruiz, 34, of Tracy, California, was indicted by a federal Grand Jury on April 4, 2019. He was charged with

Ο Reyes Daniel Ruiz, 34ετών, κάτοικος Καλιφόρνιας και πρώην μηχανικός λογισμικού της Yahoo, παραδέχτηκε ότι έχοντας την πρόσβαση στα εσωτερικά συστήματα της Yahoo, απέκτησε παράνομη πρόσβαση σε λογαριασμούς που ανήκαν σε νέες γυναίκες, συμπεριλαμβανομένων προσωπικών του φίλων και συναδέλφων.
Ο Ruiz δήλωσε ένοχος σε παράνομη πρόσβαση σε υπολογιστές, για την οποία θα μπορούσε να αντιμετωπίσει μέχρι πέντε χρόνια φυλάκισης και ένα πρόστιμο ύψους 250.000 δολαρίων ως αποζημίωση για τα θύματά του. Ο Ruiz βρίσκεται επί του παρόντος ελεύθερος με εγγύηση 200.000 δολαρίων, καθώς περιμένει την απόφαση της ποινής στις 3 Φεβρουαρίου 2020.

Insider Threat

- **Easier to bribe telco staff than build backdoors**

Απαιτείται τόσο μεγάλη προσπάθεια για τη δημιουργία backdoors σε δικτυακές υποδομές που διασυνδέονται σε διαφορετικά παγκόσμια επικοινωνιακά δίκτυα και έχουν τόσο διαφορετικές ρυθμίσεις, που φαίνεται ευκολότερο και αποτελεσματικότερο να δωροδοκήσει κανείς το κατάλληλο στέλεχος τηλεπικοινωνιών,
ισχυρίζεται ο Chief Cybersecurity Officer της Huawei.

John Suffolk
Huawei Global Cyber Security Officer


TODAY'S NEWS
FAKE
NEWS

Fake News

Hackers issued false news about the deployment of nuclear weapons

Hackers διασκόρπησαν είδηση για αίτημα του Προέδρου της Λιθουανίας προς τις ΗΠΑ για δημιουργία στρατιωτικής βάσης στη Λιθουανία και μεταφορά πυρηνικών όπλων εκεί από την Τουρκίας. Η πληροφορία αυτή στάλθηκε από το email **media@urm.lt** που ανήκει στο Department of Communication and Cultural Diplomacy του ΥΠ.ΕΞ της Λιθουανίας. Το Λιθουανικό ΥΠ.ΕΞ αρνήθηκε την πληροφορία και αναφέρθηκε σε κυβερνοεπίθεση.

Cyber Espionage

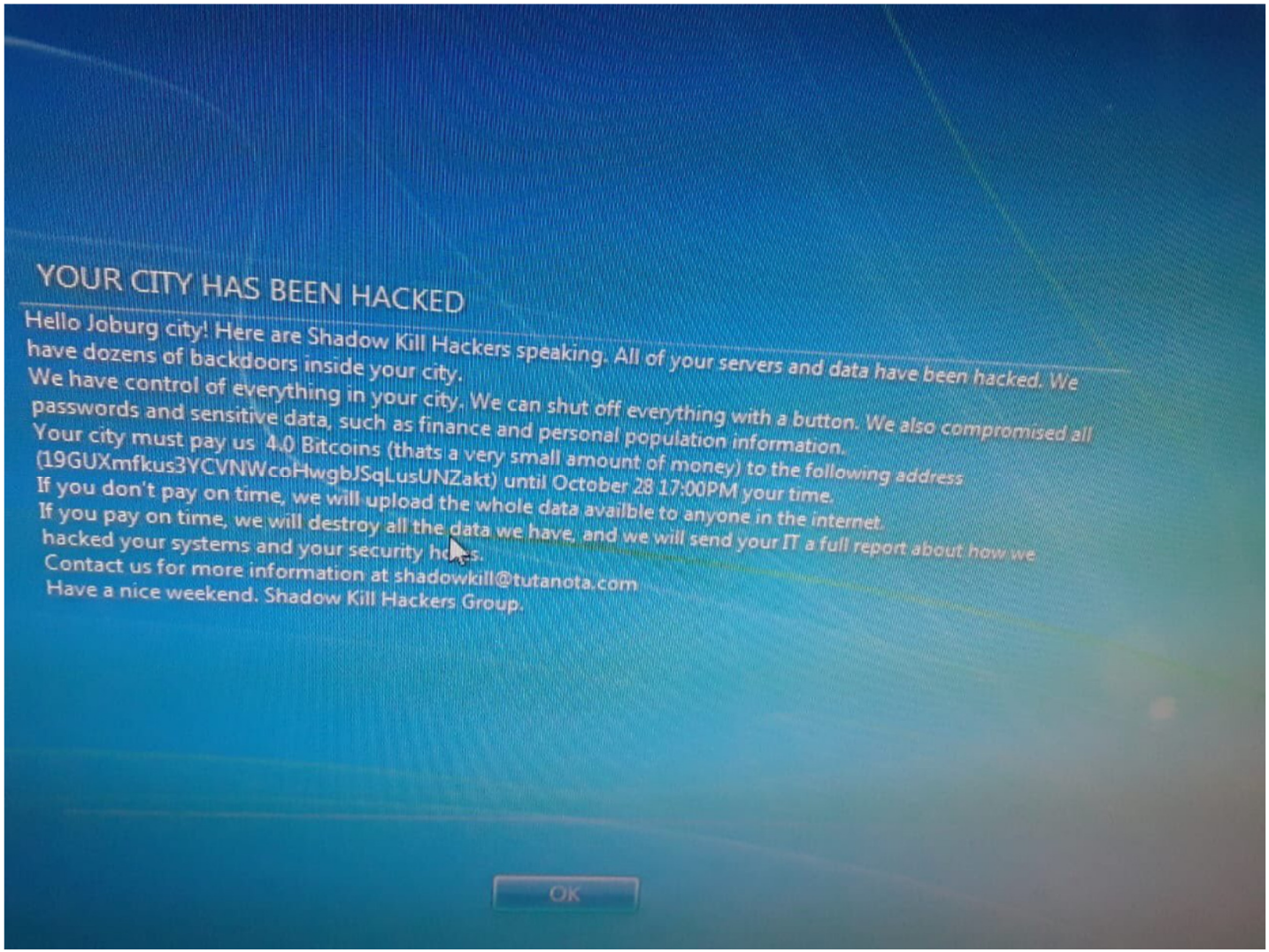
The Russian Embassy in Prague denied the statement of a Russian spy network in the Czech Republic

- Στις 21 Οκτωβρίου η Τσέχικη Υπηρεσία Πληροφοριών (BIS) ανέφερε την εξάρθρωση σε συνεργασία με την Τσέχικη Αστυνομία ρώσικου δικτύου κατασκοπείας.
- Είπε ότι το δίκτυο αυτό λειτουργούσε διαμέσου της Ρωσικής πρεσβείας στην Πράγα "was created by people associated with the Russian intelligence services, and funded from Russia and the Russian Embassy.“.
- Η Ρωσική Πρεσβεία στην Πράγα το διέψευσε.


RANSOMWARE

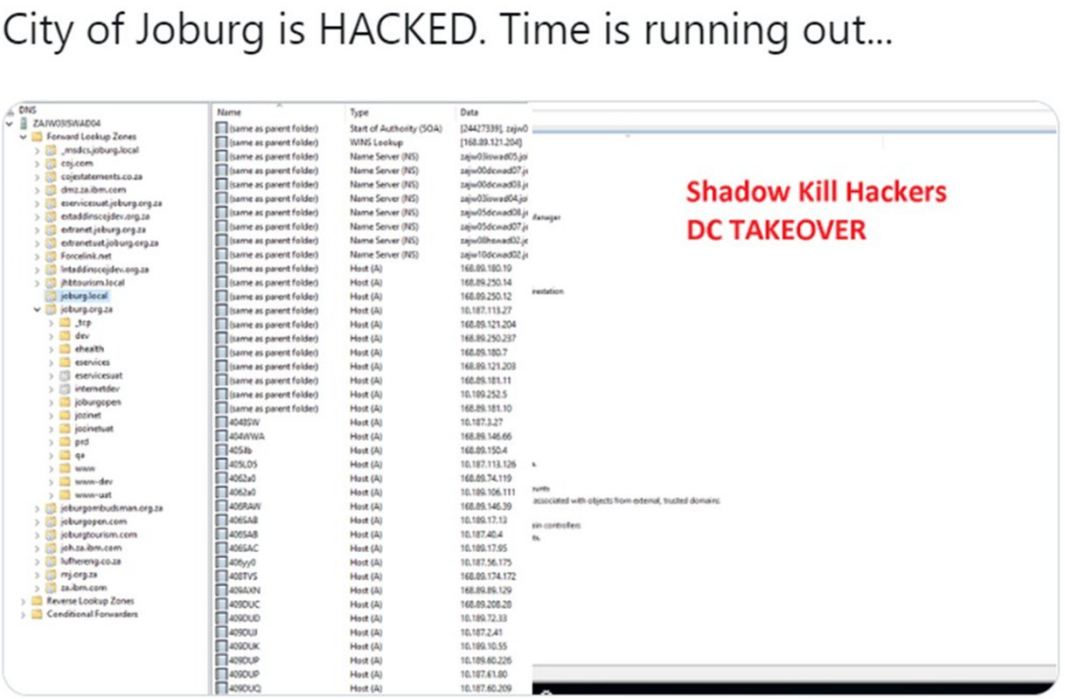
City of Johannesburg hit by Ransomware

- Η μεγαλύτερη πόλη της Νοτίου Αφρικής δέχεται επιτυχημένη επίθεση ransomware για δεύτερη φορά σε τέσσερις μήνες
- Το hacker group **Shadow Kill Hackers** μόλυνε το εσωτερικό δίκτυο της πόλης με ransomware και εκβιάζει τη μεγαλύτερη πόλη της Ν. Αφρικής
- Οι hackers ζητούσαν **4 bitcoins έως τη Δευτέρα 28 Οκτωβρίου** , στις 17:00. Αλλιώς εκβιάζουν ότι θα δημοσιεύσουν τα δεδομένα της πόλης στο Internet.
- **"Your servers and data have been hacked, We have dozens of back doors inside your city. We have control of everything in your city. We also compromised all passwords and sensitive data such as finance and personal population information"** the note said.


YOUR CITY HAS BEEN HACKED
Hello Joburg city! Here are Shadow Kill Hackers speaking. All of your servers and data have been hacked. We have dozens of backdoors inside your city.
We have control of everything in your city. We can shut off everything with a button. We also compromised all passwords and sensitive data, such as finance and personal population information.
Your city must pay us 4.0 Bitcoins (thats a very small amount of money) to the following address (19GUXmfkus3YCVNWcoHwgbJSqLusUNZakt) until October 28 17:00PM your time.
If you don't pay on time, we will upload the whole data availble to anyone in the internet.
If you pay on time, we will destroy all the data we have, and we will send your IT a full report about how we hacked your systems and your security holes.
Contact us for more information at shadowkill@tutanota.com
Have a nice weekend. Shadow Kill Hackers Group.
OK

City of Johannesburg hit by Ransomware

- Οι τεχνικοί κατόρθωσαν να επαναφέρουν σε σημαντικό βαθμό τα συστήματα μετά από την επίθεση.
- Η Δημοτική Σύμβουλος Funzela Ngobeni δήλωσε ότι αν συνεχίσουν με τον ίδιο ρυθμό, τότε το 80% των συστημάτων θα έχουν αποκατασταθεί σε 4 ημέρες.
- Η προθεσμία των Hacker πέρασε:
- Η πόλη του Johannesburg δηλώνει ότι δεν πληρώνει!



City of Johannesburg hit by Ransomware

- Αναστάλθηκε η λειτουργία του λογαριασμού Twitter των «Shadow Kill Hackers».
- Δεν πληρώθηκαν λύτρα.


EXPLORING
VULNERABILITIES IN
NETWORK SECURITY

Στο στόχαστρο των Hackers vulnerabilities σε προϊόντα της Fortinet και της Pulse Secure

Fortinet

Κυκλοφόρησε patches τον Απρίλιο και το Μάιο 2019 για άμεση εγκατάσταση.

Pulse

Κυκλοφόρησε ένα patch fix στις 24 Απριλίου 2019 για άμεση εγκατάσταση στο Pulse Connect Secure (VPN).

Στη Black Hat 2019 στο Las Vegas 3 έως 8 Αυγούστου 2019, ερευνητές ασφάλειας παρουσιάζουν πως μπορεί να γίνει εκμετάλλευση των παραπάνω security vulnerabilities.

Οι συγκεκριμένες ευπάθειες επηρεάζουν τα enterprise virtual private network (VPN) προϊόντα της Fortinet και της Pulse Secure.

Πρόκειται για κενά ασφαλείας στο FortiOS SSL VPN web portal της Fortinet και στο Pulse Connect Secure.

Microsoft Releases
October 2019 Patch Tuesday Updates

- Στις 8 Οκτωβρίου 2019 η Microsoft ανακοίνωσε και κυκλοφόρησε τις October 2019 Security Updates.
- Με αυτό θωρακίζει 59 vulnerabilities στα Windows, 9 κρίσιμες, 49 σημαντικές και 1 μέτριας σπουδαιότητας.

Κυβερνοαπειλές

ΣΥΝΟΨΗ

Κυβερνοαπειλές

Συνήθεις απειλές

- Μη ενημερωμένο
  - Λογισμικό
  - Υλικό
- Αδυναμίες 0-Day
- Ransomware
- Insiders
- Fake news

Επερχόμενες απειλές

- Νέα είδη απειλών
- Quantum computing

Νέες Τεχνολογίες → Νέες Κυβερνοαπειλές

Υφιστάμενες τεχνολογίες

- Internet
- Cloud
- Blockchain

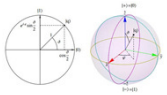
Νεότερες τεχνολογίες

- Internet of things (IoT)
- 5G
- Smart cities

Νέες Κυβερνοαπειλές

Επερχόμενες τεχνολογίες

Artificial Intelligence (AI)



Quantum computing

Απαραίτητα Μέτρα Ασφαλείας

1. Ενημερώσεις (Updates/Upgrades)

- **ΛΟΓΙΣΜΙΚΟ**
  - Λειτουργικά συστήματα
  - Εφαρμογές office
  - Εφαρμογές email
  - Άλλα προγράμματα
  - Οδηγοί (drivers)
  - Αντιιικά
  - Firewalls
- **ΥΛΙΚΟ**
  - Bios/Firmware
  - Network devices
  - Εκτυπωτές
  - Κάμερες
  - IoT devices

- Υπεύθυνος για ενημερώσεις
- Διαδικασία ενημέρωσης
  - Αυτοματοποιημένη
  - On demand
  - Online
  - Offline

2. Απεγκατάσταση μη χρησιμοποιούμενων εφαρμογών

3. Απενεργοποίηση μη χρησιμοποιούμενων λογαριασμών

4. Χρήση πολυπλοκότητας κωδικών

5. Dual factor authentication

6. …..

Κυβερνοασφάλεια
Αναφορά Περιστατικού

Δημόσιος Τομέας
Διαδικασία Αναφοράς

Ποια περιστατικά πρέπει να αναφέρονται στο Εθνικό CERT;

- Όλες τις επιτυχημένες επιθέσεις hacking
- Διαρροή δεδομένων
- Παρακολούθηση
- Μολύνσεις από ιούς
- Επίθεση Denial of Service (DOS)
- Σημαντικές ανεπιτυχείς προσπάθειες επίθεσης
- Phishing emails
- Κακόβουλα προγράμματα που ανιχνεύτηκαν από αντιιικά με heuristic scanning, μετά από ύποπτη συμπεριφορά
- Network probes and scans
- Ύποπτη συμπεριφορά σε hardware ή software

Ενέργειες αντιμετώπισης περιστατικού από το Εθνικό CERT

- Ενημέρωση από/προς τον φορέα
- Συλλογή στοιχείων
- Άμεσες ενέργειες – μέτρα αποκατάστασης
- Ανάλυση – Επεξεργασία στοιχείων
- Αξιοποίηση πληροφορίας από Ηλεκτρονική Επίθεση
- Έλεγχος ασφαλείας (Penetration Test)
- Γνωστοποίηση πορίσματος & προτεινόμενων μέτρων ασφαλείας στον φορέα

Προτεινόμενη διαδικασία αναφοράς περιστατικού ηλεκτρονικής επίθεσης (1/2)

- Διαπίστωση περιστατικού – Αξιολόγηση
- Εσωτερική ενημέρωση
  - Δνση Πληροφορικής
  - Δνση Ασφάλειας
  - Διοίκηση οργανισμού

- Ενημέρωση αρμόδιων αρχών
  - Υπουργείο Ψηφιακής Πολιτικής/Δνση Κυβερνοασφάλειας **ncsa@gsdp.gr**
  - Εθνικό CERT **cert@nis.gr**
  - Δίωξη Ηλεκτρονικού Εγκλήματος (τηλ. **11188**) **ccu@cybercrimeunit.gov.gr**
  - Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα **databreach@dpa.gr**

Προτεινόμενη διαδικασία αναφοράς περιστατικού ηλεκτρονικής επίθεσης (2/2)

Αναφορά προς Εθνικό CERT (email: cert@nis.gr, τηλέφωνο: 2106973121)

- Ονοματεπώνυμο
- Οργανισμός
- Στοιχεία επικοινωνίας (email, τηλέφωνο)

- Περιγραφή περιστατικού
- Ενέργειες που έχουν γίνει
- Επιπτώσεις περιστατικού

- Για ενημέρωση ή αίτημα συνδρομής

Κυβερνοασφάλεια
Αναφορά Περιστατικού

Δημόσιος Τομέας
Πολιτική Ασφάλειας & Μέτρα

Πολιτική Ασφάλειας & Μέτρα

- Αναλυτική καταγραφή πληροφοριακών συστημάτων
  - Αναλυτική καταγραφή hardware
  - Αναλυτική καταγραφή software
  - **Διαγράμματα Δικτύου**
  - **IP διευθυνσιοδότηση**
  - Καταγραφή Χρηστών (πχ Domain admin, Local admin, Users)
- Διαδικασίες **Backup**
- Διαδικασίες Ανάκτησης – Επαναφοράς
- Πρόβλεψη διατήρησης αρχείων καταγραφής (**log files**)
- Διαδικασία εφαρμογής ενημερώσεων (**updates**)
- Χρήση προγραμμάτων ασφαλείας (πχ. **antivirus, firewalls**)
- Καταγραφή διαδικασιών λειτουργίας και ελέγχου του πληροφοριακού συστήματος
- Καταγραφή ρόλων προσώπων
- Καταγραφή ειδικών μέτρων ασφάλειας

Άμεσα Επόμενα Βήματα
Δημόσιος Τομέας

- Δημιουργία δομών κυβερνοασφάλειας σε κάθε οργανισμό
  - (πχ. Τμήμα Κυβερνοασφάλειας σε κάθε οργανισμό, εκμετάλλευση υπαρχουσών δομών πχ. φυσικής ασφάλειας, προστασίας προσωπικών δεδομένων)
- Δημιουργία πολιτικών ασφάλειας – κυβερνοασφάλειας
- Καθορισμός μέτρων κυβερνοασφάλειας
  - (καθορισμός ειδικών μέτρων ασφαλείας για κάθε πληροφοριακό σύστημα)
- Ορισμός υπεύθυνου κυβερνοασφάλειας ανά πληροφοριακό σύστημα
  - (γνωρίζει πλήρως το πληροφοριακό σύστημα και τις προβλεπόμενες διαδικασίες αντιμετώπισης περιστατικών)
- Ορισμός σημείων επαφής (24/7) για κυβερνοπεριστατικά
  - (τουλάχιστον ένα POC ανά οργανισμό)
- Δημιουργία λίστας POC για κάθε πληροφοριακό σύστημα
  - (διαθέσιμη στις αρμόδιες αρχές)
- Καθορισμός επίσημης διαδικασίας αναφοράς περιστατικών
  - (σε Αρχή Κυβερνοασφάλειας - CERT – Αστυνομία)

Σας ευχαριστώ για την προσοχή σας.

Ερωτήσεις?

ΕΘΝΙΚΗ ΥΠΗΡΕΣΙΑ ΠΛΗΡΟΦΟΡΙΩΝ
ΔΙΕΥΘΥΝΣΗ ΚΥΒΕΡΝΟΧΩΡΟΥ
ΕΘΝΙΚΗ ΑΡΧΗ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΠΙΘΕΣΕΩΝ – ΕΘΝΙΚΟ CERT
Ταχ. Δ/νση: Π. Κανελλοπούλου 4, Αθήνα 10177
www.cert.gov.gr