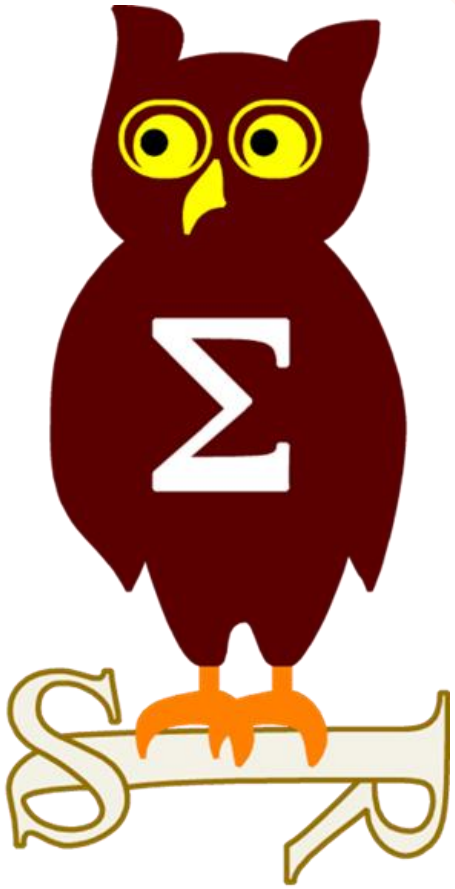
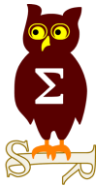


Revue d'actualité

14/11/2017

Préparée par

*Arnaud **S**OULLIE @arnaudsoullie*
*Vladimir **K**OLLA @mynameisv_*



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS17-129 Vulnérabilités dans Internet Explorer (5 CVE)

- Affectés:
  - Internet Explorer 9, 10, 11
- Exploit:
  - 4 x Exécution de code
  - 1 x Fuite d'information / contournement d'ASLR
- Crédits:
  - Hui Gao de Palo Alto Networks and Heige (a.k.a. SuperHei) de Knownsec 404 Security Team (CVE-2017-11822)
  - Dmitri Kaslov, Telspace Systems, Jaanus Kp Clarified Security par Trend Micro's Zero Day Initiative (CVE-2017-11790)
  - Hui Gao de Palo Alto Networks and Yixiang Zhu de National Engineering Lab for Mobile Internet System and Application Security, China (CVE-2017-11793)
  - Ivan Fratric de Google Project Zero (CVE-2017-11810)
  - Atte Kettunen de F-Secure (CVE-2017-11813)

MS17-130 Vulnérabilités dans Edge (17 CVE)

- Affectés:
  - ChakraCore
  - Microsoft Edge
- Exploit:
  - 15 x Exécution de code
    https://bugs.chromium.org/p/project-zero/issues/detail?id=1333
    https://bugs.chromium.org/p/project-zero/issues/detail?id=1334
    https://bugs.chromium.org/p/project-zero/issues/detail?id=1338
  - 2 x Fuite d'information / contournement d'ASLR
- Crédits:
  - Abdulrahman Alqabandi (@qab) (CVE-2017-8726)
  - Hao Linan de Qihoo 360 Vulcan Team, Lokihardt de Google Project Zero (CVE-2017-11802)
  - Anonymous par Trend Micro's Zero Day Initiative (CVE-2017-11794, CVE-2017-11800)
  - Huang Anwen ichunqiu Ker Team (CVE-2017-11798)
  - Microsoft ChakraCore Team (CVE-2017-11796, CVE-2017-11792, CVE-2017-11808, CVE-2017-11804, CVE-2017-11805, CVE-2017-11807, CVE-2017-11806)
  - Microsoft ChakraCore Team, Simon Zuckerbraun par Trend Micro's Zero Day Initiative (CVE-2017-11812)
  - ? (CVE-2017-11821)
  - Lokihardt de Google Project Zero (CVE-2017-11811, CVE-2017-11799, CVE-2017-11809)

Dont 0 commune avec IE

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS17-131 Vulnérabilités dans Microsoft Graphics (GDI) (5 CVE)

- Affectés:
  - Windows toutes versions supportées
- Exploit:
  - 2 x Exécutions de code, lors du traitement de polices de caractères (CVE-2017-11762 et CVE-2017-11763)
  - 2 x Fuite d'information / contournement d'ASLR
  - 1 x Élévation de privilèges
- Crédits:
  - Wayne Low (@x9090) de Fortinet s FortiGuard Lab (CVE-2017-11763)
  - Symeon Paraschoudis de SensePost (CVE-2017-11816)
  - Enrique Nissim de IOActive (CVE-2017-8693)
  - ? (CVE-2017-11824)
  - Jaanus Kp de Clarified Security par Trend Micro's Zero Day Initiative (CVE-2017-11762)

MS17-132 Vulnérabilités dans Windows Shell (2 CVE)

- Affectés:
  - Windows toutes versions supportées
- Exploit:
  - 2 x Exécutions de code
- Crédits:
  - Zhong Zhaochen (@asnine) de Neusoft (CVE-2017-11819)
  - Zhang Yunhai de NSFOCUS (CVE-2017-8727)

C’est une faute d’orth ?

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS17-133 Vulnérabilités dans Scripting Engine (JScript and/or VBScript) (2 CVE)

- Affectés:
  - ChakraCore
- Exploit:
  - 2 x Exécutions de code
- Crédits:
  - Microsoft ChakraCore Team (CVE-2017-11797, CVE-2017-11801)

MS17-134 Vulnérabilités dans Windows Search (2 CVE)

- Affectés:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Exécution de code, exploitation depuis SMB et utilisé par la NSA
  - 1 x Fuite d'information / contournement d'ASLR
- Crédits:
  - Swamy Shivaganga Nagaraju de MSRC Vulnérabilités & Mitigations (CVE-2017-11772, CVE-2017-11771)

MS17-135 Vulnérabilité dans Windows DNS Client (1 CVE)

- Affectés:
  - Windows toutes versions supportées, sauf Windows 7
- Exploit:
  - 1 x Exécution de code, lors du traitement de la réponse à une requête DNS
    https://www.bishopfox.com/blog/2017/10/a-bug-has-no-name-multiple-heap-buffer-overflows-in-the-windows-dns-client/
- Crédits:
  - Nick Freeman de Bishop Fox, Nelson William Gamazo Sanchez - Trend Micro par Trend Micro's Zero Day Initiative (CVE-2017-11779)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS17-136 Vulnérabilités dans Office (7 CVE)

- Affectés:
  - Microsoft Office 2010, 2013, 2016, 2016 for Mac
  - Microsoft Office Web Apps Server 2010, 2013 Service Pack 1
  - Microsoft SharePoint Enterprise Server 2013 Service Pack 1, 2016
- Exploit:
  - 1 x Contournement d'une mesure de sécurité
  - 2 x Exécution de code
    - CVE-2017-11826 exploitée dans la nature

      https://0patch.blogspot.fr/2017/11/0patching-pretty-nasty-microsoft-word.html
  - 1 x Fuite d'information, mails non chiffrés avec SMIME (CVE-2017-11776)
  - 3 x Élévations de privilèges
- Crédits:
  - Simon Hofer and Stefan Viehb ckSEC Consult Vulnérabilités Lab, Florian Gattermeier and Heinrich WiederkehrERNW GmbH (CVE-2017-11776)
  - Marco Pizer and Sven EngelSTIHL (CVE-2017-11777)
  - Etienne Stalmans de SensePost (CVE-2017-11774)
  - Andrew Watts & Adam Awan, eShare LtdCompany (CVE-2017-11820)
  - Yang Kang, Ding Maoyin and Song Shenlei de Qihoo 360 Core Security (@360CoreSec) (CVE-2017-11826)
  - Cybellum Technologies LTD (CVE-2017-11825)
  - ? (CVE-2017-11775)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS17-137 Vulnérabilités dans Windows (5 CVE)

- Affectés:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Exécution de code
  - 2 x Contournements d'une mesure de sécurité
  - 1 x Fuite d'information / contournement d'ASLR
  - 1 x Élévation de privilèges
- Crédits:
  - Matt Nelson (@enigma0x3) de SpecterOps (CVE-2017-8715)
  - Clement Rouault (@hakril) and Thomas Imbert (@masthoon) from Sogeti ESEC R&D (CVE-2017-11783)
  - Richard ShupakIndividual (CVE-2017-11769)
  - Mateusz Jurczyk de Google Project zero (CVE-2017-11817)
  - James Forshaw de Google Project Zero (CVE-2017-11823)

MS17-138 Vulnérabilités dans Windows Kernel (4 CVE)

- Affectés:
  - Windows toutes versions supportées
- Exploit:
  - 4 x Fuites d'information / contournement d'ASLR
- Crédits:
  - Mateusz Jurczyk de Google Project Zero (CVE-2017-11785, CVE-2017-11784)
  - WenQunWang de Tencent's Xuanwu LAB (CVE-2017-11765, CVE-2017-11814)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS17-139 Vulnérabilités dans Windows SMB (4 CVE)

- Affectés:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Denial of Service
  - 1 x Exécution de code
  - 1 x Fuite d'information / contournement d'ASLR
  - 1 x Élévation de privilèges
- Crédits:
  - Nicolas Joly de MSRC Vulnérabilités & Mitigations (CVE-2017-11780)
  - pesante par Trend Micro's Zero Day Initiative (CVE-2017-11781)
  - ? (CVE-2017-11782, CVE-2017-11815)

MS17-140 Vulnérabilités dans JET Database Engine (2 CVE)

- Affectés:
  - Windows toutes versions supportées
- Exploit:
  - 2 x Exécutions de code
- Crédits:
  - Zhou Yu par Trend Micro's Zero Day Initiative (CVE-2017-8717, CVE-2017-8718)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS17-141 Vulnérabilités dans Microsoft Win32K and/or Graphics Component (2 CVE)

- Affectés:
  - Windows toutes versions supportées
- Exploit:
  - 2 x Élévations de privilèges
- Crédits:
  - hungtt28 & nyancat par Trend Micro's Zero Day Initiative, pgboy and zhong_sf de Qihoo 360 Vulcan Team (CVE-2017-8689)
  - bear13oy de DBAPP Security (CVE-2017-8694)

MS17-142 Vulnérabilité dans Windows Subsystem for Linux (1 CVE)

- Affectés:
  - Windows 10 Version 1703 for x64-based Systems
- Exploit:
  - 1 x Denial of Service
- Crédits:
  - Noam Kushinsky, Tianyang Yang (CVE-2017-8703)

MS17-143 Vulnérabilité dans Windows Storage (1 CVE)

- Affectés:
  - Windows toutes versions supportées, sauf Windows 7
- Exploit:
  - 1 x Contournement d’une mesure de sécurité
- Crédits:
  - ? (CVE-2017-11818)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS17-144 Vulnérabilité in WPA/WPA2 (1 CVE)

- Affectés:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Spoofing
- Crédits:
  - Mathy Vanhoef (@vanhoefm) de imec-DistriNet, KU Leuven (CVE-2017-13080)

Microsoft et l'information...

- Publié dans le bulletin d'octobre (10/10/2017) **sans** information sur la CVE, ni n° de CVE
  - Noté uniquement **ADV170016**
  - Pas la moindre indication que cela concernait le WiFi
- Mise à jour du site de Microsoft le 16/10, mais toujours rien sur l'API MSRC
- Mise à jour MSRC courant octobre

  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-13080

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS17-145 Vulnérabilité dans Skype (1 CVE)

- Affectés:
  - Microsoft Lync 2013, Skype for Business 2016
- Exploit:
  - 1 x Élévation de privilèges
- Crédits:
  - Jerry Decime, Hewlett Packard Enterprise (CVE-2017-11786)

MS17-146 Vulnérabilité dans Windows Update (1 CVE)

- Affectés:
  - Windows 10 et Server 2016
- Exploit:
  - 1 x Élévation de privilèges
- Crédits:
  - ? (CVE-2017-11829)

MS17-147 Vulnérabilité in Adobe Flash (1 CVE)

- Affectés:
  - Adobe Flash Player pour Windows 8.1 et 10, Server 2012, Server 2012 R2, Server 2016
- Exploit:
  - 1 x Exécution de code, exploité dans la nature
- Crédits:
  - ? (CVE-2017-11292.)

Failles / Bulletins / Advisories

Microsoft - Autre

Windows 10, Passage de Windows 10 pro à Entreprise simplement

- A la première connexion de l'utilisateur
- Simplifie l'installation des "master" d'entreprise
- Nécessite Azure AD

https://www.computerworld.com/article/3235244/microsoft-windows/windows-10-now-does-hands-free-no-reboot-upgrades.html

Microsoft, la croissance tirée par le Cloud

- Office 365 : 28 millions de particuliers et 120 millions de pro

https://www.nextinpact.com/news/105508-microsoft-azure-et-office-365-continuent-tirer-croissance.htm

Failles / Bulletins / Advisories

Système (principales failles)

macOS, contournement du chiffrement de disque APFS (CVE-2017-13786)

- Tout équipement Thunderbolt accède buffer du contrôleur de disque
  - Noté comme découvert par un anonyme selon Apple

https://support.apple.com/en-us/HT208221

  - Alors que Dmytro Oleksiuk l'avait annoncé sur Twitter en juillet

https://twitter.com/d_olex/status/886320724641628160

macOS, récupération du mot de passe en cas de chiffrement de disque APFS

- Possibilité de laisser un indice pour se remémorer le mot de passe du chiffrement
- Quand l'indice est demandé, c'est le mot de passe qui est donné

https://www.youtube.com/watch?time_continue=47&v=by_nIjcHmEo

Vous avez utilisé SMIME avec Outlook ? (CVE-2017-11776)

- Il y'a de fortes chances que vos mails n'aient pas été chiffrés
- Envoie des mails avec le contenu chiffré et… en clair
  - Entre mai et octobre 2017

https://www.sec-consult.com/en/blog/2017/10/fake-crypto-microsoft-outlook-smime-cleartext-disclosure-cve-2017-11776/index.html

http://www.securityinsider-wavestone.com/2017/10/cve-2017-11776-outlook-vs-smime.html

Failles / Bulletins / Advisories

Système (principales failles)

OpenSSL, possibilité de déchiffrer et de modifier le contenu

- Mais très difficilement exploitable

  https://www.openssl.org/news/secadv/20171102.txt

Yet another Linux privesc

- Vulnérabilité noyau Linux en version 4.14.0-rc4
- Utilisation d'un pointeur vers la mémoire noyau avec l'appel à waitid()

  https://www.exploit-db.com/exploits/43029/

  http://seclists.org/oss-sec/2017/q4/78

Adobe ColdFusion, exécution de code par désérialisation (CVE-2017-11283, CVE-2017-11238)

- A cause de Java RMI (Remote Method Invocation)

  https://nickbloor.co.uk/2017/10/13/adobe-coldfusion-deserialization-rce-cve-2017-11283-cve-2017-11238/

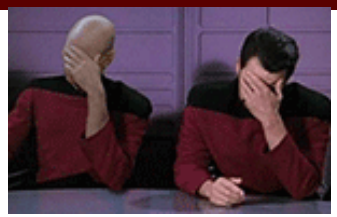
Libcurl, dépassement de tampon de la heap (CVE-2017-1000101 and CVE-2017-7407)

- Lors de l'utilisation du protocole IMAP

  http://www.geeknik.net/7k9et2d9e

Failles / Bulletins / Advisories

Réseau (principales failles)



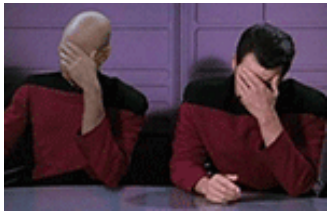
Cisco UCS (CVE-2017-12243)

- Exécution de code sans authentification en… ajoutant “**;**” à une IP

`http://1.2.3.4/settings/ping?ping_num=1&ping_ip_addr=5.6.7.8%3bcat+/etc/passwd%3b#`

https://blogs.securiteam.com/index.php/archives/3362

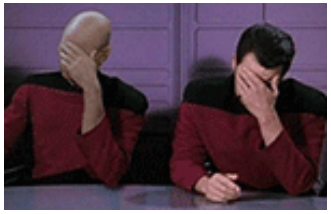
« Circle with Disney », la honte a un nom



- 22 vulnérabilités, dont :
  - Exécution de code en mettant “`;commande`” a la fin du nom d’un SSID
  - Récupération de jeton valide en envoyer une requête spécialement formatée
  - Des tas d'exécutions de code à distance

http://blog.talosintelligence.com/2017/10/Vulnérabilités-spotlight-circle.html

Oracle Identity Manager, prise de contrôle à distance (CVE-2017-10151)



- Compte OIMINTERNAL“oublié”
- Prise de contrôle de la solution

https://thehackernews.com/2017/10/oracle-identity-manager.html

Failles / Bulletins / Advisories

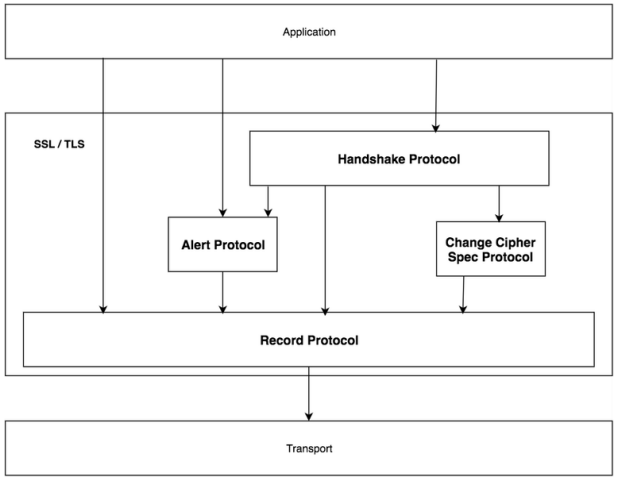
Réseau (principales failles)

DUHK : un couac chez Fortinet / CVE-2016-8492

- Générateur de nombres pseudos aléatoire ANSI X9.3 avec diversificateur fixe
- Clefs VPN et HTTPS prédictibles

https://duhkattack.com

Juniper ScreenOS, déni de service sur SSL/TLS



- En cas de réception d'un message **Alert** durant la négociation

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10808

Juniper SRX300, faiblesse cryptographique des TPM / CVE-2017-10606

- Aucune allusion à infineon dans le bulletin
  - Basé sur les TPM1.2 d'Infineon

https://kb.juniper.net/InfoCenter/index?page=content&id=KB32288&pmv=print&actp=RSS&searchid=&type=currentpaging

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10809&actp=METADATA

Failles / Bulletins / Advisories

Divers

Google Buganizer

- Création de compte valide, notification de bugs sans en avoir les droits et accéder aux bugs depuis l'API
- Vulnérabilités non exploitées selon Google
  - Ce qui rappelle la compromission de Bugzilla en 2015 avec la fuite d'informations sur 53 vulns
- Gain pour le chercheur: $15k… alors qu'il avait accès à des dizaines de vulnérabilités

https://threatpost.com/flaw-in-google-bug-tracker-exposed-reports-about-unpatched-Vulnérabilités/128687/

PUT your JSP

- Une vulnérabilité présente sur les branches 7, 8 et 9 des serveurs Tomcat ayant activé la méthode PUT permet à un attaque de déposer et d'exécuter des fichiers JSP arbitraires sur le serveur. Un plugin Metasploit a déjà été développé pour exploiter cette vulnérabilité.
- Sources complémentaires :

https://www.exploit-db.com/exploits/43008/

https://www.alphabot.com/security/blog/2017/java/Apache-Tomcat-RCE-CVE-2017-12617.html

SFR

- Accès aux portails d'administration des autres box, depuis sa propre box
- Accès aux serveurs de mise à jour (effet NotPetya)

http://www.lepoint.fr/high-tech-internet/sfr-la-faille-a-un-million-de-box-02-11-2017-2169217_47.php

Failles / Bulletins / Advisories

Divers

WPA2 est cassé / KRACK ou Key Reinstallation Attacks

- Rejeu d'une trame de l'authentification "4-way handshake"
- Réinitialisation du vecteur d'initialisation (nonce) et donc attaque en « clair connu »
  - Plusieurs vulnérabilités : CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13082, CVE-2017 -13084, CVE-2017-13086, CVE-2017-13087 et CVE-2017-13088.
- Déchiffrement des flux, injection…

  https://github.com/vanhoefm/krackattacks
- Démonstration : https://www.youtube.com/watch?v=Oh4WURZoR98

Adieu, un premier exploit noyau pour PS4

- Récupération du kernel par une attaque de MitM sur PCIe
- Noyau FreeBSD

  https://fail0verflow.com/blog/2017/ps4-namedobj-exploit/

Failles / Bulletins / Advisories

Hardware / IoT

IoTroop / Reaper

- Près d'un an après Mirai, un nouveau botnet d'objets connectés prend vie.
- Des millions d'équipements utilisables (caméras de sécurité IP exposées sur Internet…)

https://threatpost.com/iotroop-botnet-could-dwarf-mirai-in-size-and-devastation-says-researcher/128560/

https://research.checkpoint.com/new-iot-botnet-storm-coming/

https://www.exploitthis.com/2017/10/27/fear-the-reaper-or-reaper-madness/

Fobrob

- Cible les véhicules connectés de la marque Subaru
- Permettre à un attaquant d'accéder de manière illégitime au véhicule
- Vulnérabilité au sein de la fonction de génération de codes aléatoires, les rendant partiellement prédictibles et rejouables par l'attaquant, clonant alors de manière efficace la clé de voiture

https://www.trendmicro.com/vinfo/us/security/news/Vulnérabilités-and-exploits/Vulnérabilités-in-key-fob-can-let-hackers-open-subaru-cars

https://www.bleepingcomputer.com/news/security/unpatched-exploit-lets-you-clone-key-fobs-and-open-subaru-cars/

Failles / Bulletins / Advisories

Hardware / IoT

Google Home Mini

- Il enregistrait l'intégralité des conversations des utilisateurs
- Un bouton défectueux selon Google
  - Ne semble pas toucher la version grand public

http://www.journaldugeek.com/2017/10/11/google-a-patche-en-urgence-certains-google-home-mini-qui-enregistraient-lintegralite-des-conversations-des-utilisateurs/

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

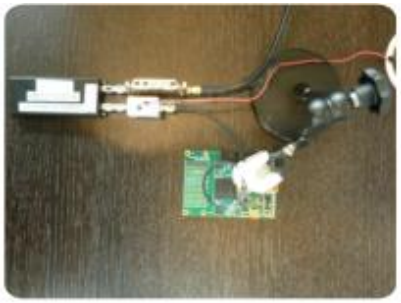
Récupération de clefs AES par une attaque de type TEMPEST

- Écoute de la consommation électrique
- Fonctionne à une distance d'un mètre

https://www.fox-it.com/nl/insights/blogs/blog/tempest-attacks-against-aes/

Loop antenna

External amplifier and bandpass filters



Example attack setup

SR-7100 Data Recorder

High-end
€200k
500 MHz (max BW)
1.3 GB/s (max data rate)

USRP B200

Low-end
€755
56 MHz
184 MB/s

RTLSDR

Budget
€20
2.4 MHz
5.2 MB/s

Désanonymisation de TOR avec Tormoil

- Bug de Firefox devenant une faille de sécurité dans TorBrowser
- Contournement du proxy avec un lien file://

https://blog.torproject.org/tor-browser-75a7-released

https://blog.torproject.org/tor-browser-709-released

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Bitcoin mine

- Hausse du prix du Bitcoin(~$6000)
- Création de la bibliothèque JavaScript “CoinHive” pour prêter son CPU et miner du Monero.
- Injection de la bibliothèque sur des sites piratés

  http://www.bbc.com/news/technology-41693556

BadRabbit, Ce lapin n'est pas gentil

- Clone du ransomware/wiper NotPetya
- Utilisation des ETERNALBLUE et ETERNALROMANCE
- Récupération des mots de passe en mémoire
- Chiffrement des fichiers de l'utilisateurs et destruction de la MFT
- Possibilité de récupérer des données avec les Shadow Copies
  - Si pas supprimés…
- Recommandations en cas d’infection :
  - Faire une capture de la mémoire vive
  - Faire un backup du disque (partiellement) chiffré au cas où les clefs seraient publiées

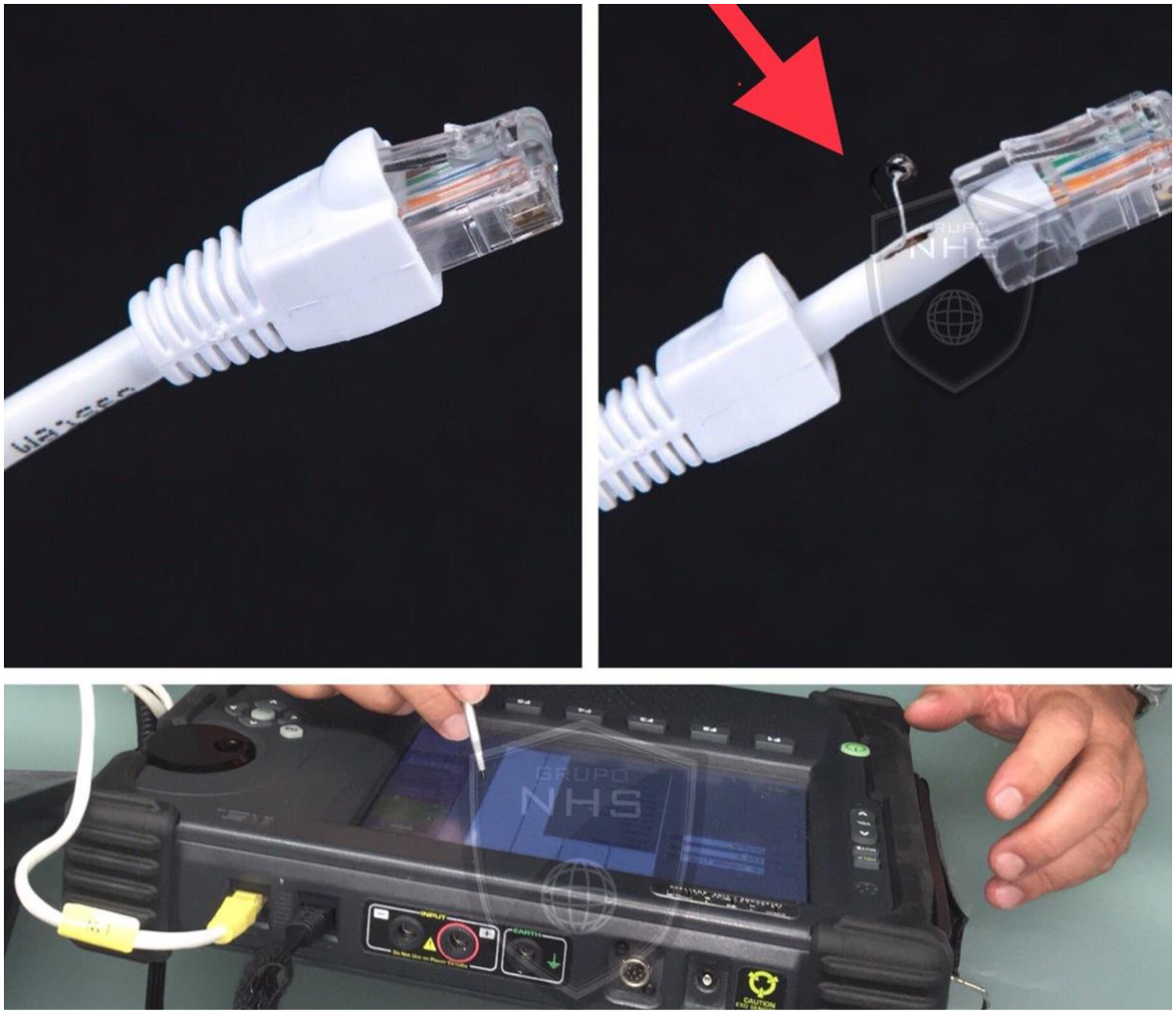
https://arstechnica.com/information-technology/2017/10/bad-rabbit-used-nsa-eternalromance-exploit-to-spread-researchers-say/
https://www.cybereason.com/blog/cybereason-researcher-discovers-vaccine-for-badrabbit-ransomware
https://www.developpez.com/actu/169438/Certaines-victimes-du-ransomware-Bad-Rabbit-pourraient-parvenir-a-recuperer-leurs-fichiers-en-profitant-de-deux-erreurs-operationnelles/

Piratages, Malwares, spam, fraudes et DDoS

Espionnage

Un micro dans un câble USB !!?

https://twitter.com/Grupo_Nhs/status/928248047586480131/photo/1

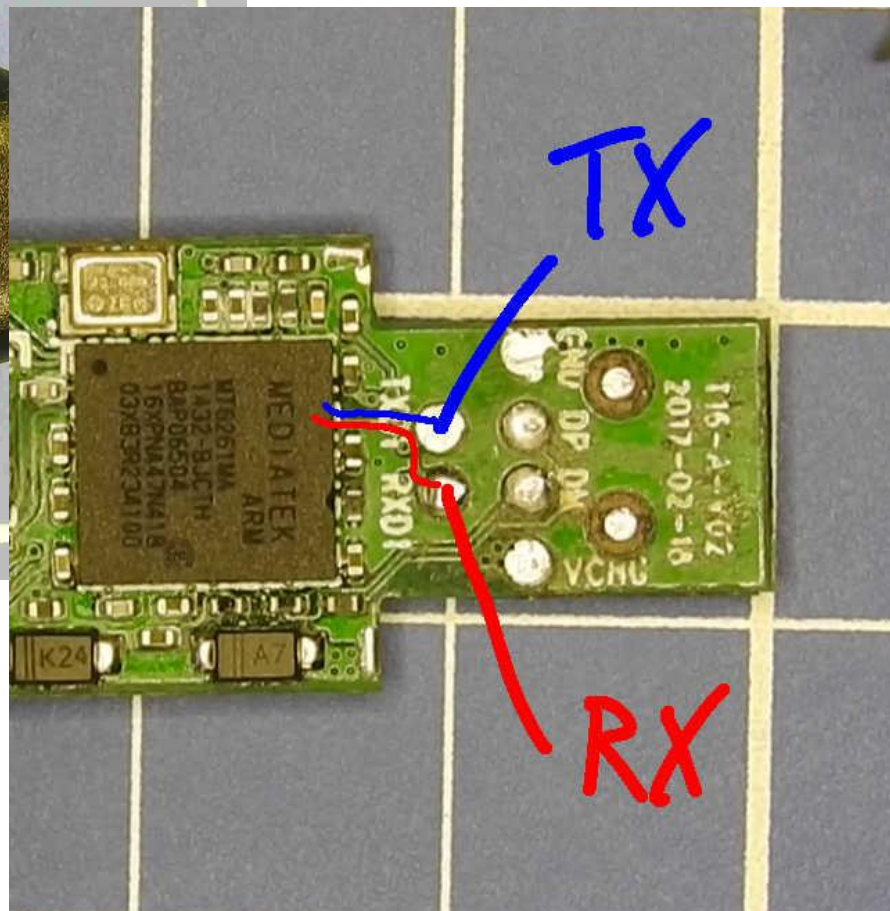


Piratages, Malwares, spam, fraudes et DDoS

Espionnage

Rétro-ingénierie d'un câble USB avec micro

https://ha.cking.ch/s8_data_line_locator/



Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Equifax

- Finalement, au lieu des 400 000 annoncés, c'est 15 millions d'anglais qui sont impactés

  https://www.grahamcluley.com/equifax-data-breach-uk/
- Ils encourageaient les gens à espionner/dénoncer leurs voisins
- Ils auraient été piratés 2 fois

  https://boingboing.net/2017/09/19/dirtier-than-imagined.html
- A priori les directeurs ayant vendu leurs actions n'étaient pas au courant du piratage

  https://gizmodo.com/equifax-investigation-clears-execs-who-dumped-stock-bef-1820127634

Piratage de Disqus, 15 millions de comptes dans la nature

https://blog.disqus.com/security-alert-user-info-breach

Le leak de la semaine en Afrique du Sud

- Des hackeurs récupèrent une sauvegarde de base de données de l'entreprise Jigsaw Holdings
- Noms, numéros de carte d'identité, adresses, salaires… de 75 millions d'habitants
- Base intégrée sans haveibeenpwned.com.

https://mybroadband.co.za/news/security/233853-massive-south-african-database-leak-just-got-bigger-60-million-records-online.html

https://mybroadband.co.za/news/security/234790-massive-south-african-data-leak-now-over-75-million-records-at-risk.html

Piratages, Malwares, spam, fraudes et DDoS

SCADA

Contourner un airgap sur des automates Siemens

- Un automate compromis peut émettre des ondes RF au niveau AM
- Les signaux peuvent être récupérés via un dongle SDR sur le PC de l'attaquant

https://www.darkreading.com/threat-intelligence/stealthy-new-plc-hack-jumps-the-air-gap-/d/d-id/1330381?_mc=sm_dr&hootPostID=d791564b3e4740d1d22d47749248be48

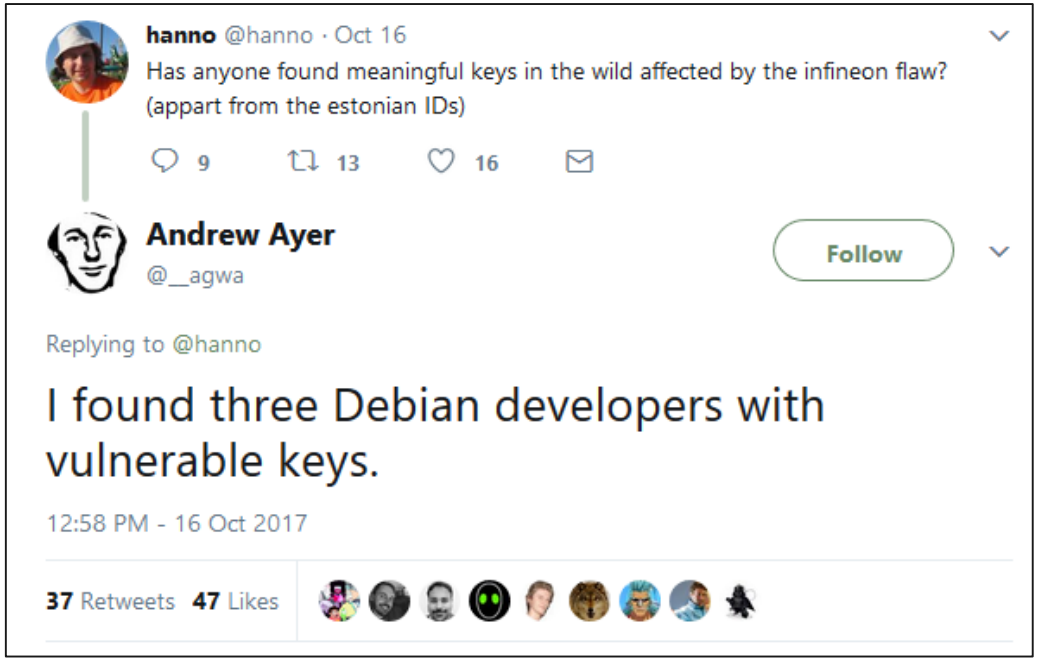
Piratages, Malwares, spam, fraudes et DDoS

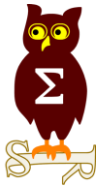
Crypto

Puce TPM Infineon, des effets largement sous-estimés

- Des clefs de développeurs vulnérables

  https://twitter.com/__agwa/status/920016011138494466





Nouveautés, outils et techniques

Comparaison VM / Conteneur

- Utilisation d'unikernels et pré-chargement des VMs
- Consommation en ressources et performances similaires à des conteneurs

  https://dl.acm.org/citation.cfm?id=3132763

DDE, la fonctionnalité idéale pour le phishing ?

- **DDE** = **D**ynamic **D**ata **E**xchange. Fonctionnalité permettant d'intégrer des données provenant d'une autre application
- Affiche un message d'erreur laconique sur la mise à jour de données, pas de warning sécurité, pas nécessaire d'activer les macros
- Permet l'exécution de code
- Exploitable depuis Excel, Word, mais également directement depuis un mail Outlook !

https://www.cybereason.com/blog/leveraging-excel-dde-for-lateral-movement-via-dcom

https://nakedsecurity.sophos.com/2017/10/22/office-dde-attack-works-in-outlook-too-heres-what-to-do/?platform=hootsuite

https://technet.microsoft.com/en-us/library/security/4053440.aspx

Pentest
Techniques & outils

Mettre une porte dérobée dans iMessage

- Exécution de scripts AppleScript au démarrage

  https://github.com/checkyfuntime/iMessagesBackdoor

Attaque sur les relations d'approbations Active Directory

- Mise à jour du guide SpecterOps

  https://posts.specterops.io/a-guide-to-attacking-domain-trusts-971e52cb2944

Un malware dans le sous-système Linux pour Windows

- Inception… Un malware Windows qui tourne dans Wine dans le WSL dans Windows (!)
- Pour échapper aux mécanismes de détection

  https://ibreak.software/2017/10/executing-windows-malware-in-windows-subsystem-for-linux-bashware/

CertStream, automatiser la récupération des certificats “Certificate Transparancy”

- Peut-être utile pour anticiper des phishings

https://certstream.calidog.io/

Autopsy 4.5.0

https://github.com/sleuthkit/autopsy/releases

Sleuth Kit 4.5.0

- Support des partitions HFS compressées

https://github.com/sleuthkit/sleuthkit/releases

Atomic RedTeam testing

- Initiative visant à tester de manière automatisé les actions référencées par le MITRE ATT&CK Framework

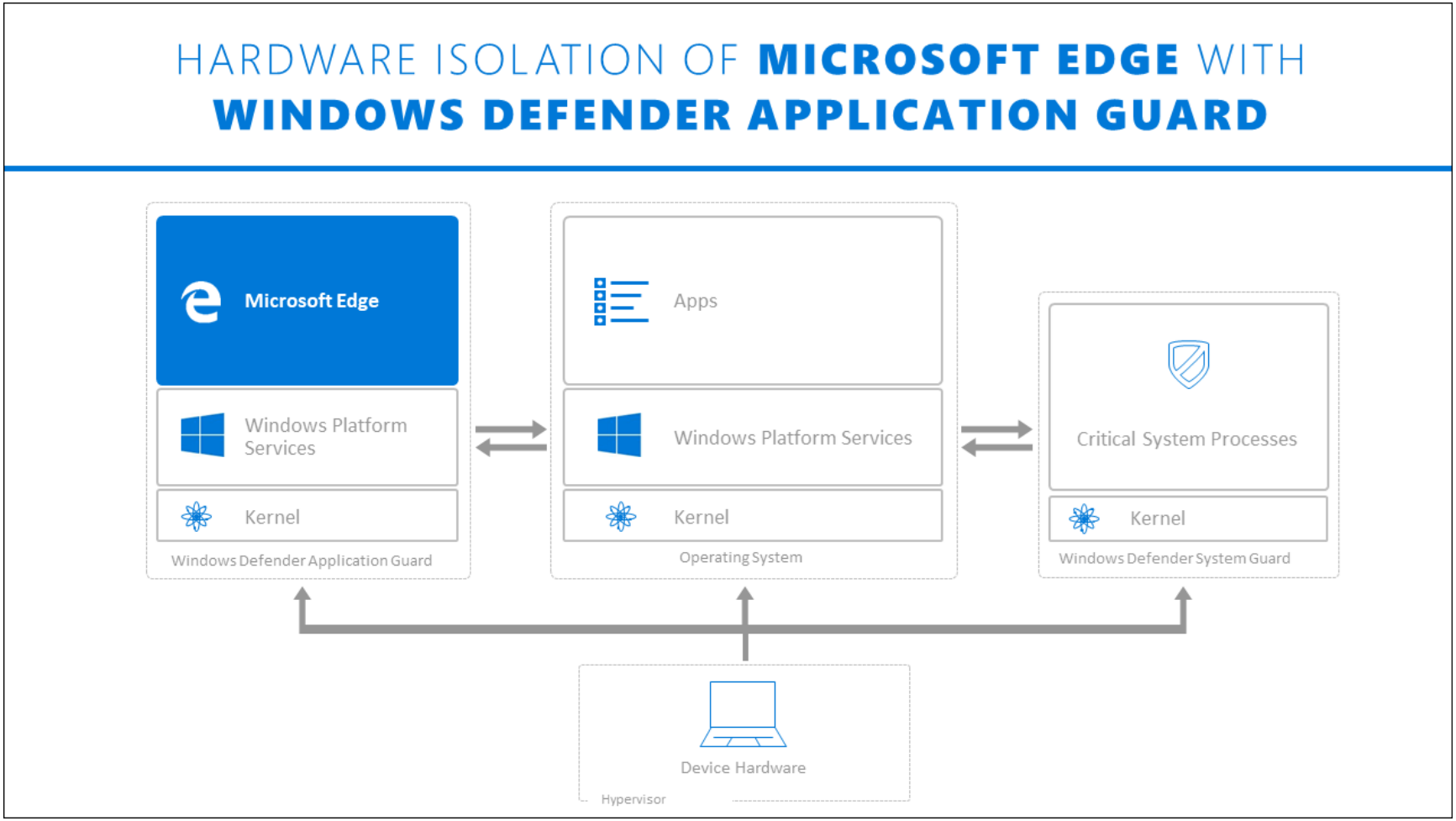
https://www.redcanary.com/blog/atomic-red-team-testing/

https://github.com/redcanaryco/atomic-red-team

Windows Defender Application Guard

- Faire tourner le navigateur Edge dans une VM

  https://docs.microsoft.com/en-us/windows/threat-protection/windows-defender-application-guard/install-wd-app-guard



Business et Politique

Droit / Politique
International

Télévision Vizio

- Mode "surveillance" activé par défaut pendant 2 ans
- Amende de $2,2 millions
- Mais les autres télévisions modernes font la même chose...

https://www.theverge.com/2017/2/7/14527360/vizio-smart-tv-tracking-settlement-disable-settings

Conférences

Conférences

Passées

- Hack.lu - 17-19 Octobre 2017 à Luxembourg

A venir

- BlackHat Europe : 6-7 décembre 2017 à Londres
- Botconf - 6 au 8 décembre 2017 à Montpellier
- 34C3 - 27-30 décembre à Leipzig

Divers / Trolls velus

Divers / Trolls velus

Coupure sauvage des serveurs HSC par Deloitte

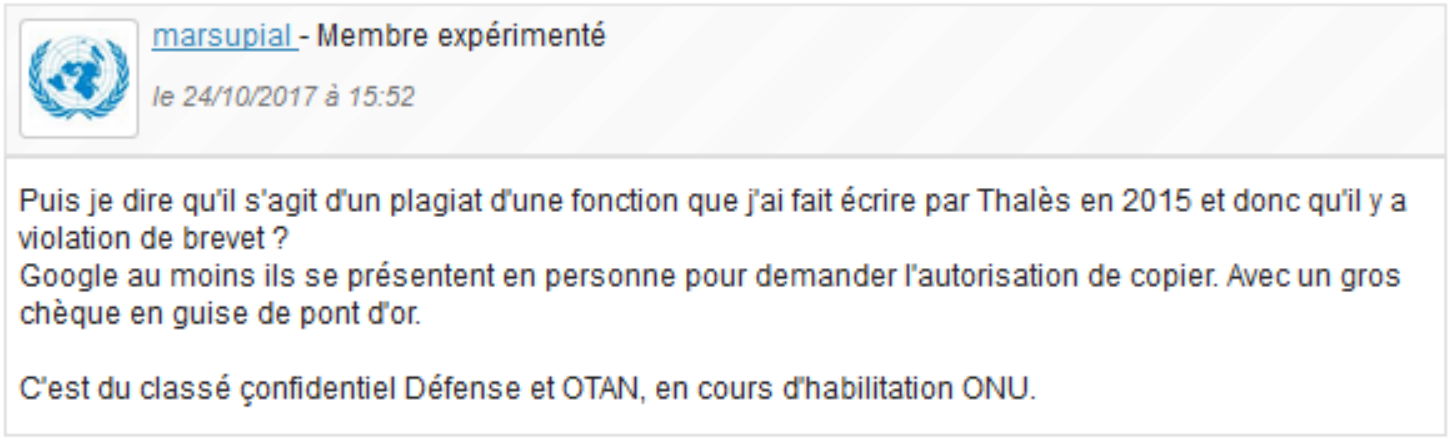
- Plus d’accès au Club ISO27001
- Plus d’accès aux formations sécurité HSC/Deloitte
- C’est la fin d’une époque 😭

Divers / Trolls velus

100% pur troll !

- Windows 10 « Controlled Folder Access »
- Un membre du forum publie un commentaire… particulier

https://www.developpez.com/actu/168383/Windows-10-avec-sa-fonctionnalite-Controlled-Folder-Access-Microsoft-espere-mieux-vous-proteger-des-ransomwares-grace-a-Windows-Defender/



marsupial - Membre expérimenté

le 24/10/2017 à 15:52

Puis je dire qu'il s'agit d'un plagiat d'une fonction que j'ai fait écrire par Thalès en 2015 et donc qu'il y a violation de brevet ?
Google au moins ils se présentent en personne pour demander l'autorisation de copier. Avec un gros chèque en guise de pont d'or.

C'est du classé çonfidentiel Défense et OTAN, en cours d'habilitation ONU.

Les .IO c'est rigolo (et à la mode) mais…

- L'infrastructure en charge de l'infra associée ne tient pas le coup

https://getstream.io/blog/stop-using-io-domain-names-for-production-traffic/

Ethereum, une erreur humaine bloque $260 millions d'ether

- Un développeur révoque une clef utilisée pour les transactions de dizaines de comptes

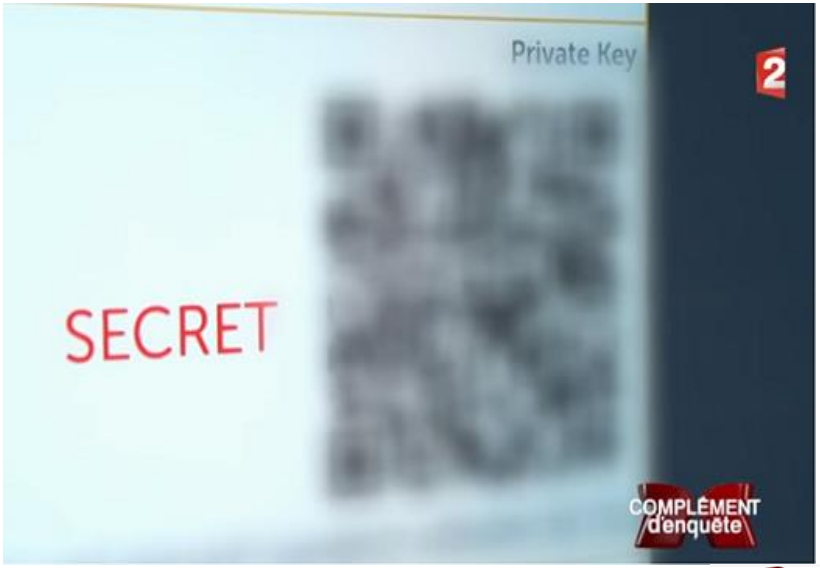
https://www.coindesk.com/ethereum-client-bug-freezes-user-funds-fallout-remains-uncertain/

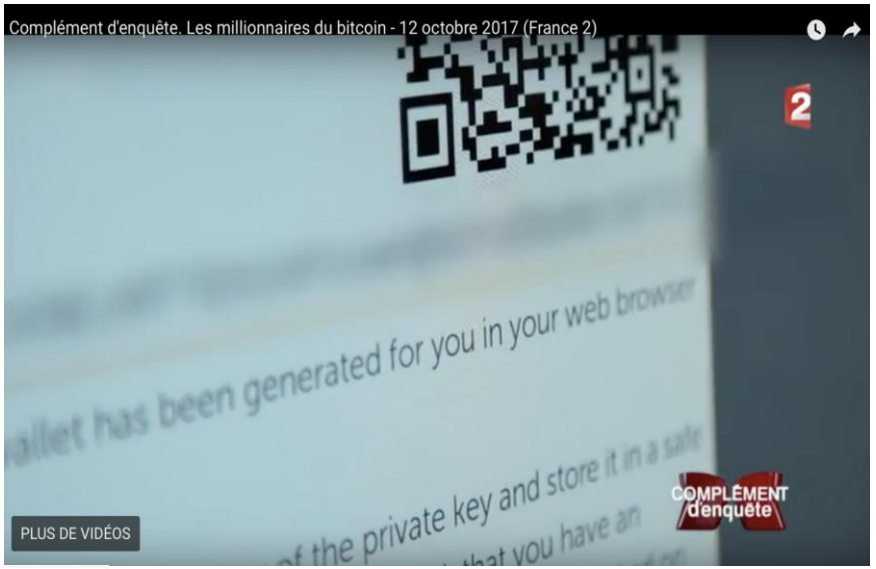
Divers / Trolls velus

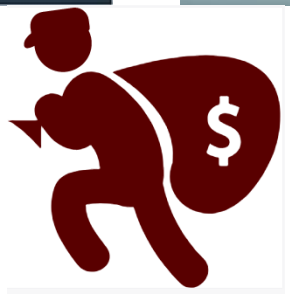
Vidéo de complément d'enquête sur les millionnaires du Bitcoin

- Un interviewé présente Bitcoin et son wallet
- Le QRCode du secret est mal flouté et présenté en gros plan à 17min. 40s.
- Une partie du QRCode visible à 17min. 51s.
- Bilan : vol de $1000 en bitcoins

https://medium.freecodecamp.org/lets-enhance-how-we-found-rogerkver-s-1000-wallet-obfuscated-private-key-8514e74a5433







$1,000

Divers / Trolls velus

Kasperky a bien récupéré du code source de le NSA

- L'affaire date de 2014
- L'antivirus a détecté des objets malveillants dans une archive
  - et a tout envoyé sur les serveurs de Kaspersky pour analyse
- Fun fact : l'utilisateur avait son pc infecté par un malware, venant d'un crack Office

https://theintercept.com/document/2017/10/24/kaspersky-lab-preliminary-results-of-the-internal-investigation-into-alleged-incident-reported-by-u-s-media/

Le MOOC "SecNumAcadémie de l'ANSSI

- Est critiquable...

https://news0ft.blogspot.fr/2017/10/ma-contribution-au-mois-de-la.html

OWASP 2017 RC2

+ XXE, désérialisations, log insuffisantes

- Insufficient Attack Protection

- Disparition des RASP

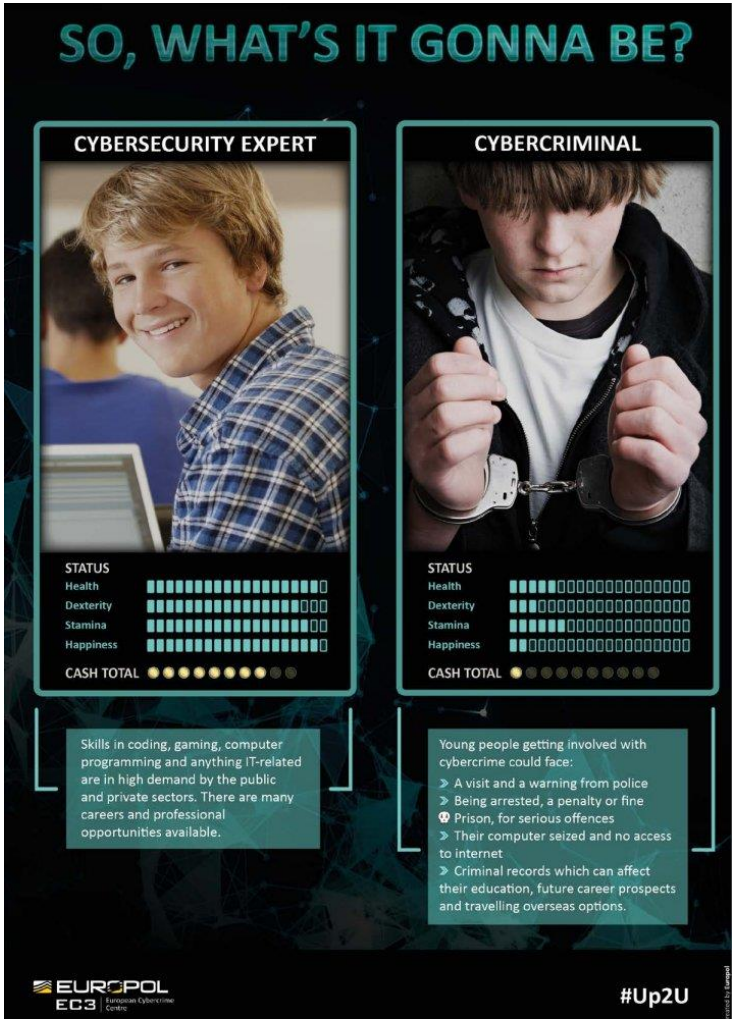
https://t.co/UmKcTYaufK

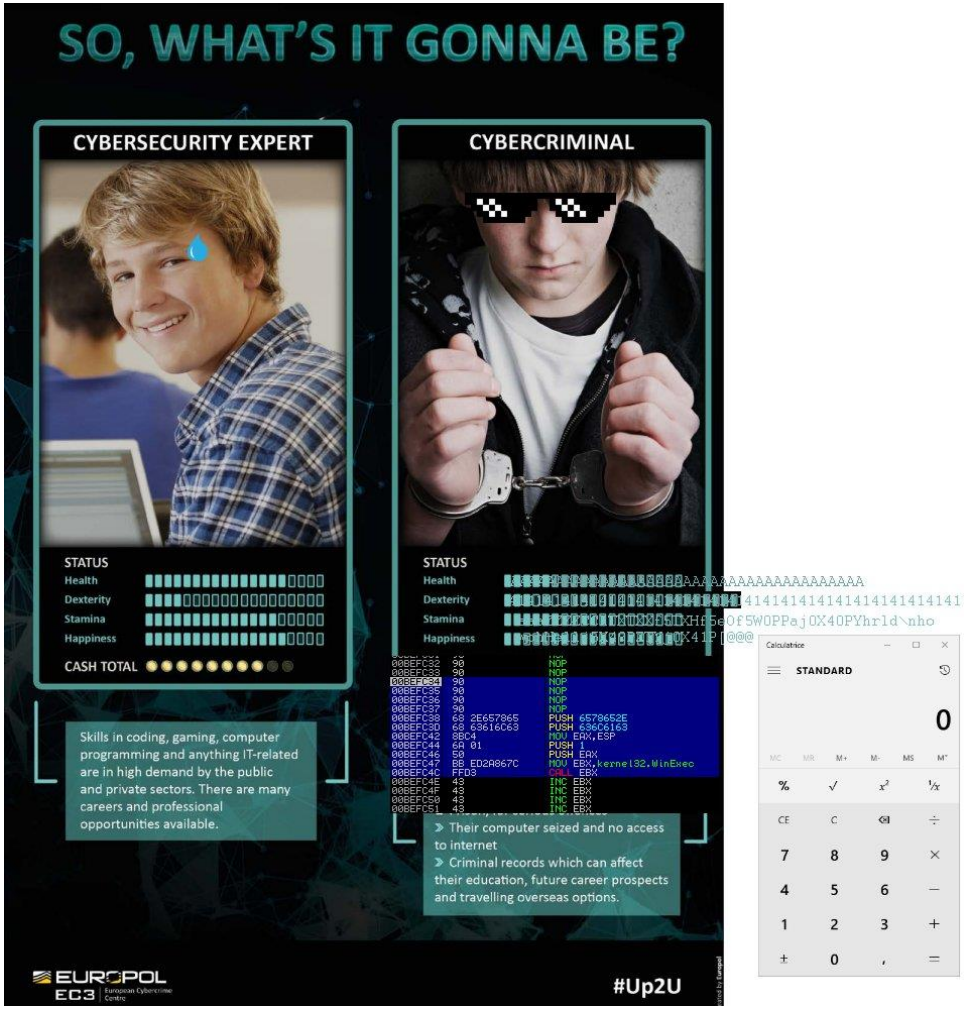
OWASP Top 10 2013	±	OWASP Top 10 2017
A1 – Injection	→	A1:2017 – Injection
A2 – Broken Authentication and Session Management	→	A2:2017 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	↘	A3:2013 – Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017 – XML External Entity (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017 – Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017 – Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017 – Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017 – Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017 – Insufficient Logging & Monitoring [NEW, Comm.]

Divers / Trolls velus

La nouvelle campagne de communication de l'EC3

- Déjà détournée
  https://twitter.com/x0rz/status/920229650684633088





Divers / Trolls velus

Le **pire** article de l'année sur la sécurité informatique

<<Pour déjouer les mécanismes de détection des antivirus et des pare-feu ("firewall"), ils opèrent désormais "sans fichier">>

<<au lieu d'utiliser un fichier "malin" (un "malware" en anglais) >>

<< En informatique, il suffit aujourd'hui d'incorporer une ligne de code au sein d'une image.>>

<<"Un pixel suffit", explique Patrice Puichaud, directeur des ventes en Europe et en Afrique du groupe de cybersécurité Sentinel One>>

<<Cette technique, connue des services secrets depuis l'Antiquité>>

...

http://www.lepoint.fr/high-tech-internet/cyberattaques-plus-besoin-de-virus-pour-pirater-un-ordinateur-27-10-2017-2167874_47.php

Prochains rendez-vous de l’OSSIR

Prochaine réunion

- Mardi 12 décembre 2017
  BNPP CIB
  Salles 0B 165
  140-142 Boulevard Macdonald - 75019 PARIS

After Work

- Plus de lieu / bar 

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous