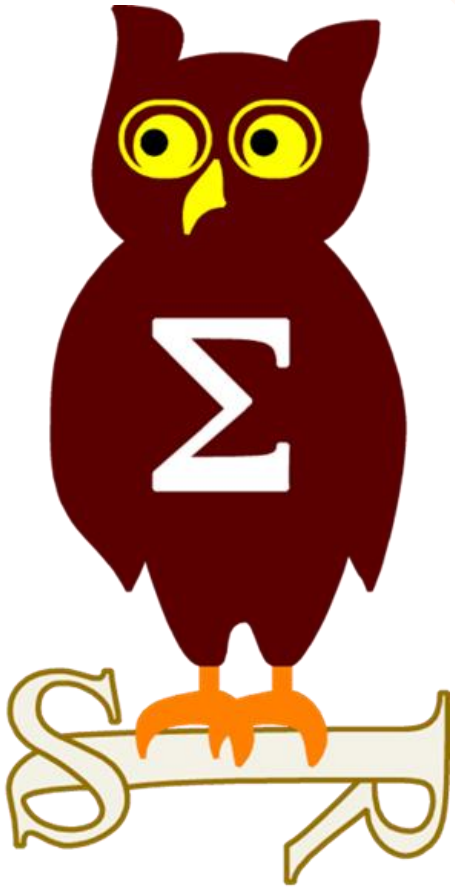
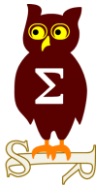


Revue d'actualité

09/01/2018

Préparée par

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



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS17-161 Vulnérabilités in Internet Explorer (13 CVE)

- Exploit:
  - 10 x Remote Code Execution
  - 3 x Information Disclosure
- Crédits:
  - Ivan Fratric de Google Project Zero (CVE-2017-11890, CVE-2017-11907, CVE-2017-11906, CVE-2017-11903)
  - Anonymous par Trend Micro's Zero Day Initiative (CVE-2017-11901)
  - Qixan Zhao de Qihoo 360 Vulcan Team (CVE-2017-11895)
  - Anonymous par Trend Micro's Zero Day Initiative, Yuki Chen de Qihoo 360 Vulcan Team (CVE-2017-11887)
  - Huang Anwen ichunqiu Ker Team (CVE-2017-11894, CVE-2017-11930)
  - Yuki Chen de Qihoo 360 Vulcan Team, Anonymous par Trend Micro's Zero Day Initiative (CVE-2017-11913)
  - Hui Gao de Palo Alto Networks (CVE-2017-11886)
  - Wei de Qihoo 360 Vulcan Team (CVE-2017-11919)
  - ? (CVE-2017-11912)

MS17-162 Vulnérabilités in Edge (14 CVE)

- Exploit:
  - 13 x Remote Code Execution
  - 1 x Information Disclosure
- Crédits:
  - Qixan Zhao de Qihoo 360 Vulcan Team (CVE-2017-11895)
  - Debasish Mandal (debasishm89) de McAfee (CVE-2017-11888)
  - Huang Anwen ichunqiu Ker Team (CVE-2017-11894)
  - Qixun Zhao de Qihoo 360 Vulcan Team Liu Long de Qihoo 360 Vulcan Team (CVE-2017-11889)
  - Wei de Qihoo 360 Vulcan Team (CVE-2017-11919)
  - ? (CVE-2017-11905, CVE-2017-11912, CVE-2017-11910, CVE-2017-11908)
  - Lokihardt de Google Project Zero (CVE-2017-11893, CVE-2017-11914, CVE-2017-11911, CVE-2017-11909, CVE-2017-11918)

Dont 4 communes avec IE:

- CVE-2017-11894
- CVE-2017-11895
- CVE-2017-11912
- CVE-2017-11919

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS17-163 Vulnerabilities in Office (3 CVE)

- Affected:
  - Microsoft Office 2013, 2016, 2016 for Mac
- Exploit:
  - 1 x Remote Code Execution
  - 2 x Information Disclosure
- Crédits:
  - Alex Harmon, Microsoft (CVE-2017-11939)
  - Dhanesh Kizhakkinan de FireEye Inc (CVE-2017-11934, CVE-2017-11935)

MS17-164 Vulnerabilities in Windows (2 CVE)

- Affected:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Security Feature Bypass
  - 1 x Information Disclosure
- Crédits:
  - ? (CVE-2017-11927)
  - James Forshaw de Google Project Zero (CVE-2017-11899)

MS17-165 Vulnerability in Scripting Engine (JScript and/or VBScript) (1 CVE)

- Affected:
  - ChakraCore
- Exploit:
  - 1 x Remote Code Execution
- Crédits:
  - Lokihardt de Google Project Zero (CVE-2017-11916)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS17-166 Vulnerability in Windows Routing and Remote Access (1 CVE)

- Affected:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Remote Code Execution
- Crédits:
  - V ctor Portal Gonz lez (CVE-2017-11885)

MS17-167 Vulnerability in SharePoint (1 CVE)

- Affected:
  - Microsoft SharePoint Enterprise Server 2016
- Exploit:
  - 1 x Elevation of Privilege
- Crédits:
  - Ashar Javed de Hyundai AutoEver Europe GmbH (CVE-2017-11936)

MS17-168 Vulnerability in Microsoft Exchange Server (1 CVE)

- Affected:
  - Microsoft Exchange Server 2016
- Exploit:
  - 1 x Spoofing
- Crédits:
  - ? (CVE-2017-11932)

Failles / Bulletins / Advisories

Microsoft - Avis

Mise à jour pour Windows XP Embedded POSReady

- Windows XP Embedded Service Pack 3 (SP3) fin de support en **janvier 2016**
- Windows Embedded POSReady 2009 fin de support en **avril 2019**

Failles / Bulletins / Advisories

Microsoft - Autre

Keeper Password Manager, vol des mots de passe depuis une page web

- Installé par défaut avec certaines dernières versions de Windows

  https://bugs.chromium.org/p/project-zero/issues/detail?id=1481&desc=3

Meltdown et Spectre, Microsoft suspend les correctifs de janvier

- Impossibilité de démarrer sur certains CPUs AMD
  - Semble lié à l'antivirus
- January 9, 2018 - KB4056895 (Monthly Rollup)

  https://support.microsoft.com/en-us/help/4073707/windows-operating-system-security-update-block-for-some-amd-based-devi

Failles / Bulletins / Advisories

Système (principales failles)

pfSense, encore une vulnérabilité

- Exécution de code non authentifiée en tant que root

  https://github.com/rapid7/metasploit-framework/pull/9362

aPAColypse, exécution de code grâce à WPAD

- Interception des requêtes WPAD
- Réponse d'un proxy.pac exploitant une vulnérabilité Javascript

  https://googleprojectzero.blogspot.fr/2017/12/apacolypse-now-exploiting-windows-10-in_18.html?m=1

Symantec Encryption Desktop Windows, élévation locale de privilèges

https://labs.nettitude.com/blog/symantec-encryption-desktop-local-privilege-escalation-exploiting-an-arbitrary-hard-disk-read-write-vulnerability-over-ntfs/

Failles / Bulletins / Advisories

Système (principales failles)

VMWare Workstation, élévation locale de privilèges

- Plugin pour MetaSploit

  https://github.com/rapid7/metasploit-framework/pull/8581#unofficialweeklywrapup

Vulnérabilité dans la bibliothèque pysaml2 (CVE-2017-1000433)

- Vérification du mot de passe par un “assert”
- Si Python est lancé en mode optimisé, les “assert” sont ignorés, on peut se logger avec n’importe quel mot de passe

  https://github.com/rohe/pysaml2/issues/451

Failles / Bulletins / Advisories

Réseau (principales failles)

NAS D-Link DNS-320 ShareCenter

- Porte dérobée, compte codé en dur : ydlinkBRionyg/abc12345cba

  https://www.exploit-db.com/exploits/43434/

Fortinet, client VPN, exécution de code en tant que SYSTEM

- A partir de la popup d'alerte
- Si la fonctionnalité "VPN before logon" est activée
- Sans authentification

  https://fortiguard.com/psirt/FG-IR-17-070

Juniper JunOS, 39 vulnérabilités

- Beaucoup de vulnérabilités XML (libxml2)
  - Avec beaucoup de précisions <<...allows attackers to have **unspecified** impact via format string specifiers in **unknown** vectors.>>
- Des exécutions de code, des dénis de service...

  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10770&cat=SIRT_1&actp=LIST

Failles / Bulletins / Advisories

Hardware / IoT

HP Color LaserJet, exécution de code à distance / CVE-2017-2750

- La majorité des imprimantes récentes sont vulnérables

  https://support.hp.com/nz-en/document/c05839270

- Code d'exploitation publié

  https://github.com/foxglovesec/HPwn

- HP, les <<produits les plus sécurisés>>
  - Style et acteur de Mr Robot
  - <<Voici une imprimante professionnelle HP , elle a des fonctionnalités incroyables comme la détection des intrusions à l'exécution qui la protègent en cherchant constamment les attaques de programmes malveillants ou tout autre acte douteux. Si elle détecte quelque chose qu'elle n'aime pas, clac, elle s'autorépare sans avoir à lever le petit doigt.>>

  http://www8.hp.com/fr/fr/solutions/business-solutions/printingsolutions/securityoverview.html

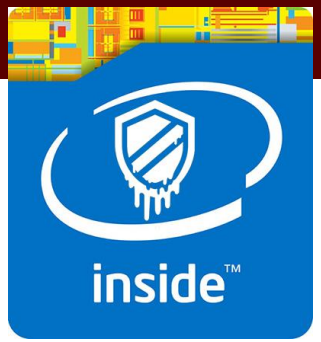
Vulnérabilité dans les services de localisation GPS

- Notamment utilisé pour des objets destinés aux enfants
- Authentifié uniquement par un numéro de série

https://0x0.li/trackmageddon/

Failles / Bulletins / Advisories

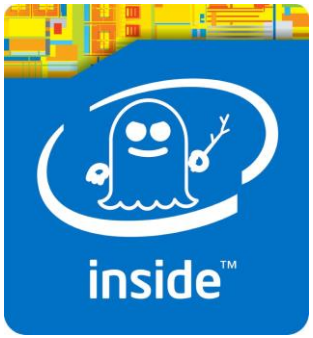
Hardware / IoT



Vulnérabilité Intel Meltdown (CVE-2017-5754)

- Accès à la mémoire kernel, depuis userland
- Utilisation de cache des prédictions de branchement

https://meltdownattack.com/meltdown.pdf



Vulnérabilités Intel/AMD/ARM Spectre (CVE-2017-5715, CVE-2017-5753)

- Accès à la mémoire des autres applications
- Utilisation de cache des prédictions de branchement

https://spectreattack.com/spectre.pdf

Pourquoi les raspberry Pi ne sont pas vulnérables ?

https://www.raspberrypi.org/blog/why-raspberry-pi-isnt-vulnerable-to-spectre-or-meltdown/

Firewall, routeurs, IoT, NAS, SAN… s'il y'a de l'Intel ou de l'ARM

- Mais cela reste une élévation de privilège **locale**
- Ou un accès à la mémoire des autres processus

Failles / Bulletins / Advisories

Hardware / IoT

Meltdown et Spectre

- Un PoC fonctionnel

  https://www.exploit-db.com/exploits/43427/

- Les actions en justice commencent à arriver

  https://www.theguardian.com/technology/2018/jan/05/intel-class-action-lawsuits-meltdown-spectre-bugs-computer

- Linus Torvald n'est pas content

  http://www.tomshardware.fr/articles/linus-torvalds-arm-x86,1-61456.html

- Le correctif = baisse de performance de 10% pour RedHat et 10-15% selon MongoDb

  https://access.redhat.com/articles/3307751

  - Déjà constaté en décembre 2017 ?

  https://forums.aws.amazon.com/thread.jspa?threadID=269858

- Quelques problèmes avec les antivirus

  https://docs.google.com/spreadsheets/d/184wcDt9I9TUNFFbsAVLpzAtckQxYiuirADzf3cL42FQ/htmlview?usp=sharing&sle=true

- Les navigateurs intègrent également des contre-mesures
  - Désactivation de SHaredArrayBuffer
  - Réduction de la précision du temps (!)
  - Consommation supplémentaire mémoire de 20%

  https://www.chromium.org/Home/chromium-security/ssca

  https://www.mozilla.org/en-US/security/advisories/mfsa2018-01/

Failles / Bulletins / Advisories

Hardware / IoT

Meltdown et Spectre, et pendant ce temps là, à Vera Cruz

- Selon Intel <<No. This is not a bug >>

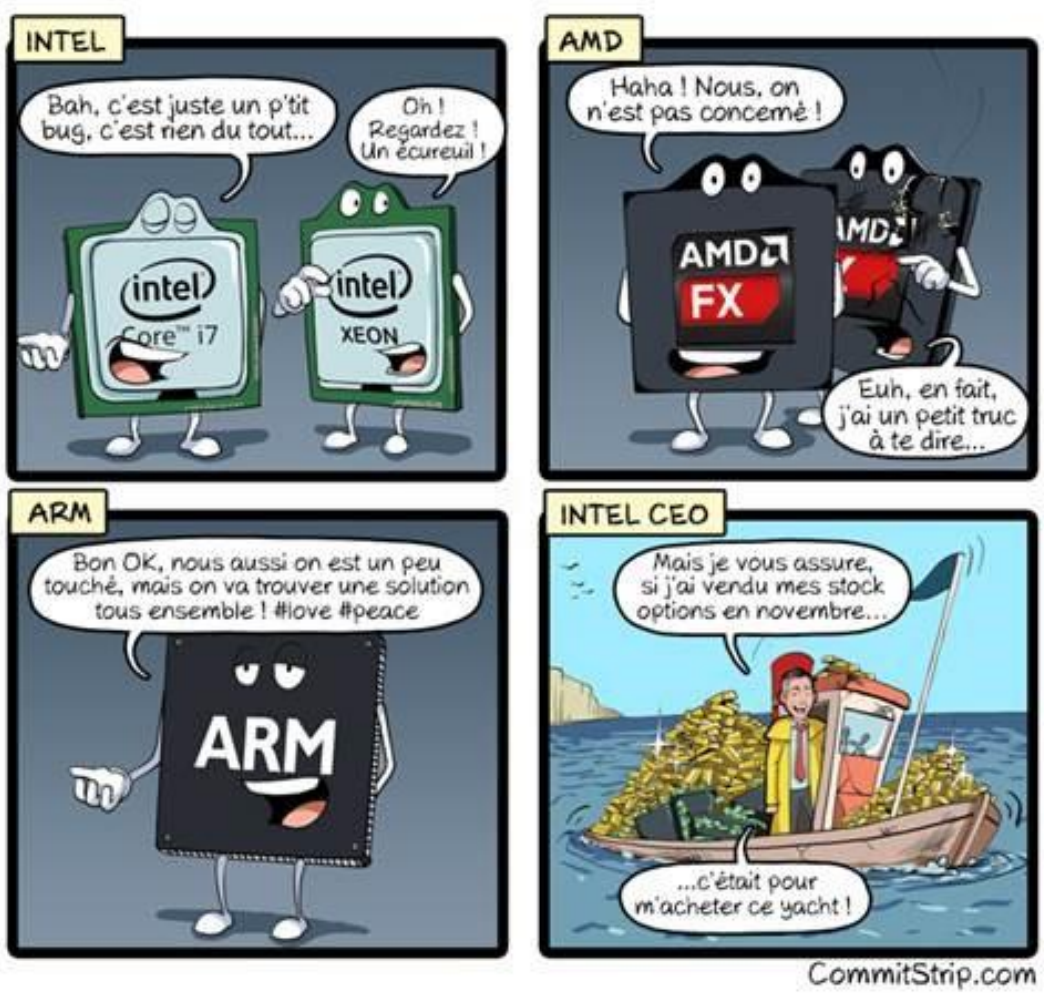
  https://www.intel.com/content/www/us/en/architecture-and-technology/facts-about-side-channel-analysis-and-intel-products.html

- Intel fait de la publicité sur sa sécurité matériel

Failles / Bulletins / Advisories

Hardware / IoT

Meltdown et Spectre : un résumé en images

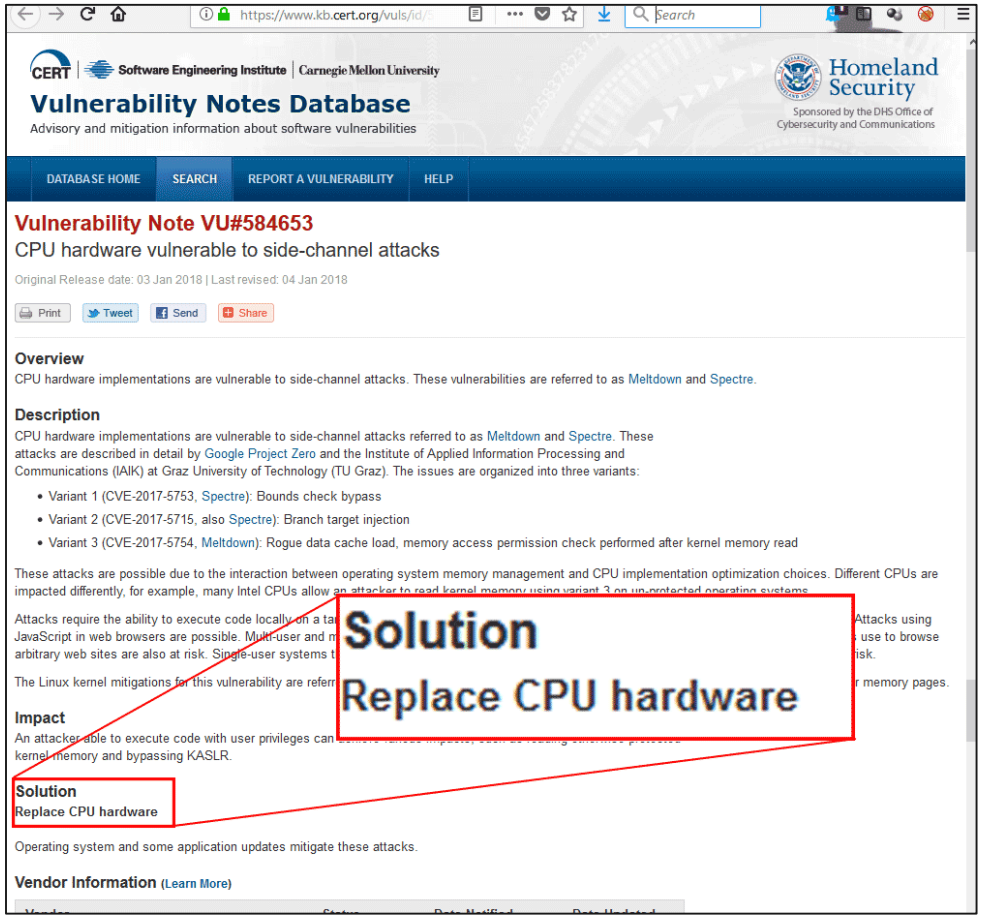


http://www.commitstrip.com/fr/2018/01/04/reactions-to-meltdown-and-spectre-exploits/

Failles / Bulletins / Advisories

Hardware / IoT

Meltdown et Spectre : la coupe du meilleur correctif



https://www.kb.cert.org/vuls/id/584653

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Attention à vos Interface d'administration SOAP Apache Axis

- Risque d'exécution de code

  https://s3cur3.it/blog/5

Comment je vole l'ensemble de votre vie depuis 2 ans

- Il développe un package Javascript basique mais contenant une porte dérobée
- Personne ne vérifie et l'installe même sur du bancaire…
- Vol des données

  https://hackernoon.com/im-harvesting-credit-card-numbers-and-passwords-from-your-site-here-s-how-9a8cb347c5b5

Coût de la crypto ?

- D'après CloudFlare, 1.8% du temps processeur

  https://blog.cloudflare.com/how-expensive-is-crypto-anyway/

Attaque sur les réseau neuronaux

- Création de lunettes qui perturbent la reconnaissance faciale

  https://arxiv.org/pdf/1801.00349.pdf

Fig. 4: An example of digital dodging. Left: An image of actor Owen Wilson, correctly classified by VGG143 with probability 1.00. Right: Dodging against VGG143 using AGN's output (probability assigned to the correct class: < 0.01).

Piratages, Malwares, spam, fraudes et DDoS
Malwares

WannaCry, la suite

- Les auteurs ont attendu le fork de Bitcoin pour toucher l'argent en août (~53 BTC)

  https://blockchain.info/address/115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn?filter=1

  https://blockchain.info/address/12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw?filter=1

  https://blockchain.info/address/13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94?filter=1

- Les USA accusent ouvertement la Corée du Nord

  https://www.nextinpact.com/news/105848-wannacry-etats-unis-accusent-coree-nord-et-appellent-au-rassemblement.htm

Conficker, encore des traces près de 10 ans après

- Rapport de Trend Micro
- Encore des infections dans la santé, l'industrie et les gouvernements

  https://www.darkreading.com/attacks-breaches/conficker-the-worm-that-wont-die/d/d-id/1330594

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Données de 18 millions d'électeurs californiens volés

- Sur une base MongoDB accessible à tous, sur Internet
  https://www.darkreading.com/attacks-breaches/19-m-california-voter-records-held-for-ransom-in-mongodb-attack/d/d-id/1330656

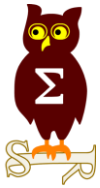
Piratages, Malwares, spam, fraudes et DDoS
SCADA

Triton, un malware ciblant l'industrie

- Cibles les SIS (*Systèmes Instrumentés de Sûreté*) Triconex
- Découvert dans la nature
- Développé en Python

https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

https://dragos.com/blog/trisis/TRISIS-01.pdf



Nouveautés, outils et techniques

Dupliquer une AC root pour signer son malware

https://posts.specterops.io/code-signing-certificate-cloning-attacks-and-defenses-6f98657fc6ec

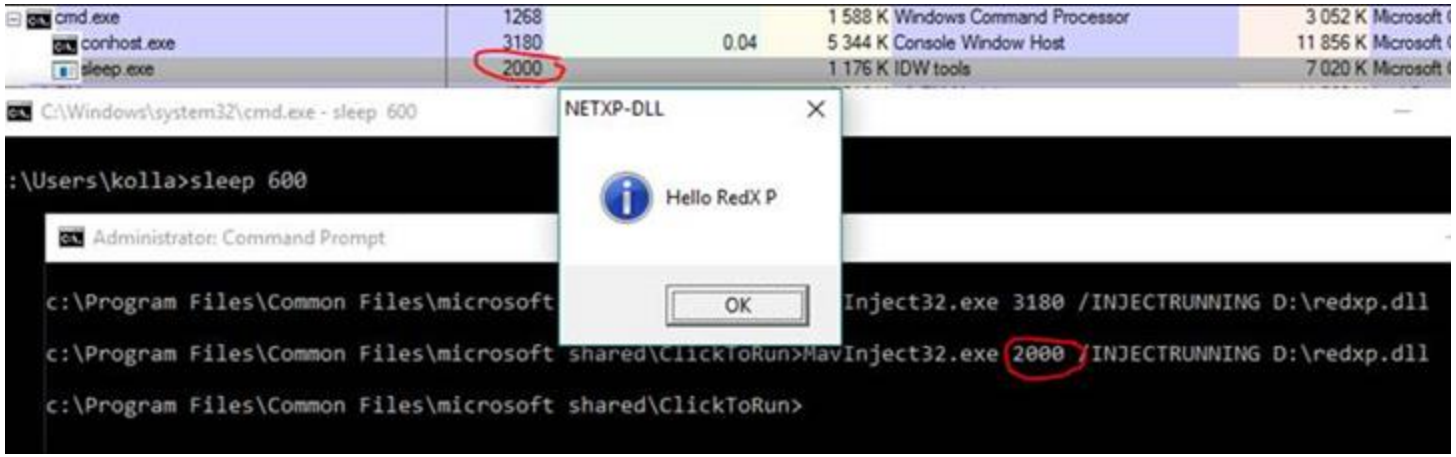
- Existant depuis longtemps, exemple publié 2016 :

  https://github.com/mynameisv/AcaGasbi

Injecter “légitimement” une DLL 32 bits dans un processus Windows grâce à Office

- Grâce à Office l’outil est « Microsoft Application Virtualization (App-V) »

```
# "C:\Program Files\Common Files\microsoft shared\ClickToRun\MavInject32.exe" <PID> /INJECTRUNNING <DLL>
```



Pentest

Techniques & outils

Contourner les outils Sysinternals

- Nommer son executable `%environment variable%.exe`
- Puis ajouter une clef de démarrage : `HKCU\...\Run:"foobar"="%USERNAME%"`

http://www.hexacorn.com/blog/2018/01/04/yet-another-way-to-hide-from-sysinternals-tools/

Meterpreter pour iOS

- Fonctionnel !

https://github.com/rapid7/metasploit-framework/pull/9296

Pirater les pirates

Exécution de code à distance dans Acunetix

https://github.com/dzonerzy/acunetix_0day/blob/master/acu0day.py

Tutoriel pour l'utilisation de Mutiny et Decept

- Outils publié par Talos pour le fuzzing de protocoles inconnus

  http://blog.talosintelligence.com/2018/01/tutorial-mutiny-fuzzing-framework-and.html?utm_source=dlvr.it&utm_medium=twitter&utm_campaign=Feed%3A+feedburner%2FTalos+%28Talos%E2%84%A2+Blog%29

FAT : Assistance à l'analyse de firmware

- Identification du firmware, de l'archi, emulation avec qemu

https://github.com/attify/firmware-analysis-toolkit

Analyse cryptographique différentielle

- Sur une télécommande de climatisation
- Pour comprendre le mode de calcul du checksum

  http://www.righto.com/2017/12/decoding-air-conditioner-controls.html

Business et Politique

Business

France

AWS ouvre son Datacenter en France

https://aws.amazon.com/fr/about-aws/global-infrastructure/

Droit / Politique

France

WhatsApp mis en demeure par la CNIL

- Suite de l'affaire des transmissions de données à Facebook

  https://www.nextinpact.com/news/105845-whatsapp-mis-en-demeure-par-cnil-pour-ses-transmissions-donnees-a-facebook.htm

Droit / Politique
International

WannaCry, les USA accusent publiquement la Corée du Nord

- Ceci aurait pu être mis dans “troll”

https://www.nextinpact.com/news/105848-wannacry-etats-unis-accusent-coree-nord-et-appellent-au-rassemblement.htm

Mirai, les accusés plaident coupable

- Paras Jha 22 ans (alias Anna Senpai), Josiah White 20 ans (alias Lightspeed) et Norman Dalton 21 ans (alias Drake)
- Coupable de la Création du ver, son exploitation l’avoir utilisé pour de la fraude au clic
- Ils encourent chacun une peine de prison de 5 ans et $250 000 d’amende.

https://www.justice.gov/opa/pr/justice-department-announces-charges-and-guilty-pleas-three-computer-crime-cases-involving

Droit / Politique
International

Fuite des cerveaux à la NSA

- 5,6% à 9% de départs ces dernières années
- **Snowden** : une trahison créant de la suspicion
- **GAFA** : salaires plus importants
- **Réorganisation interne** : promotions à l'ancienneté et non la compétence
- **ShadowBroker** (non cité dans l'article) : baisse du moral et suspicions

https://www.lesechos.fr/monde/etats-unis/0301098066952-renseignement-quand-les-cracks-de-la-nsa-filent-dans-la-silicon-valley-2142200.php

Conférences

Conférences

Passées

- Hack.lu - 17-19 October 2017 à Luxembourg
- BlackHat Europe : 6-7 décembre 2017 à Londres
- Botconf - 6 au 8 décembre 2017 à Montpellier
- 34C3 - 27-30 décembre 2017 à Leipzig

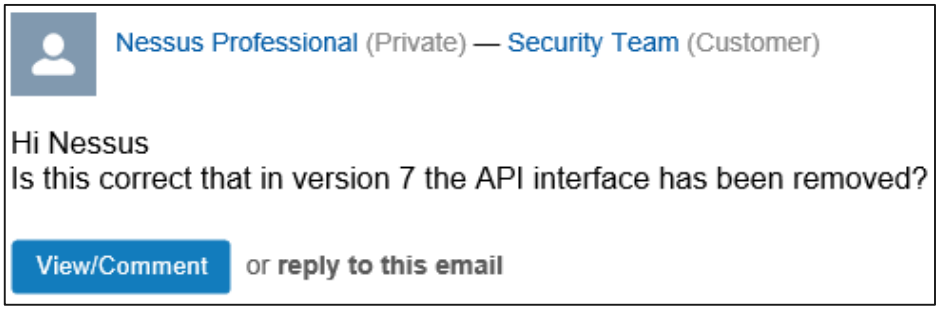
A venir

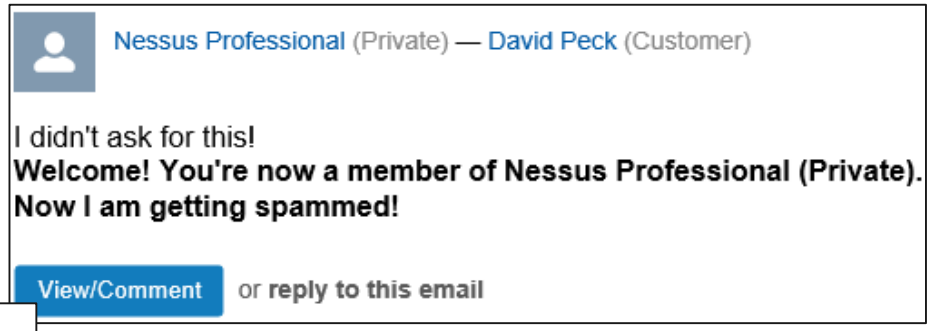
- CORI&IN - 23 janvier 2018 à Lille
- FIC - 23 et 24 janvier 2018 à Lille
- JSSI - mardi 13 mars 2018 à Paris

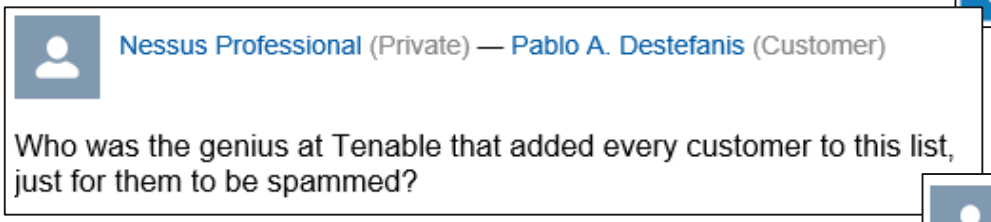
Divers / Trolls velus

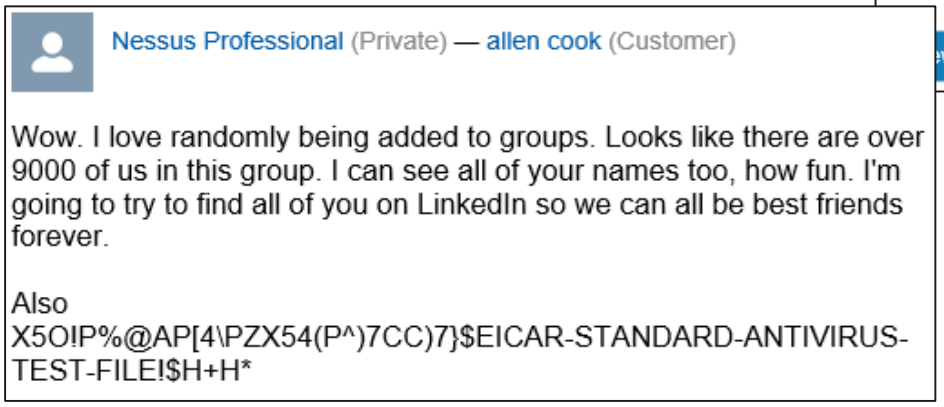
Divers / Trolls velus

Quelques petits problèmes avec Tenable Commmunity





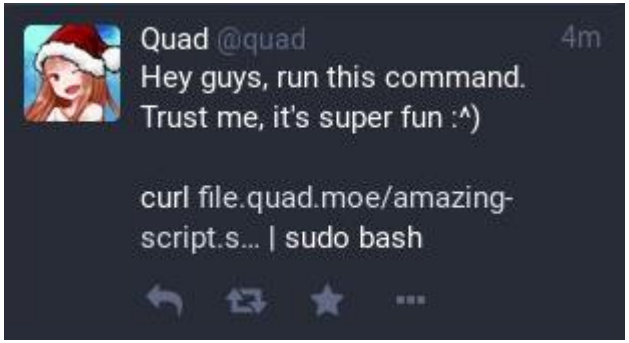


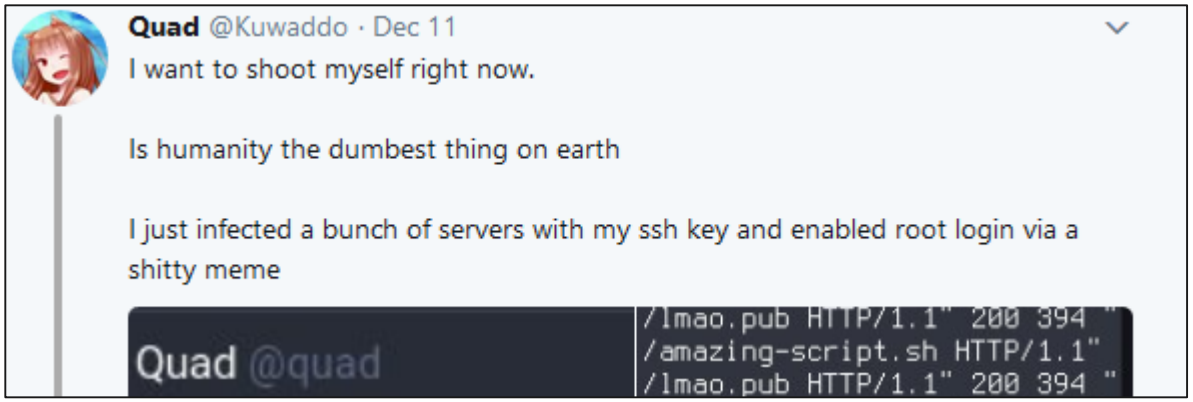


Divers / Trolls velus

Le tweet qui tue

https://twitter.com/Kuwaddo/status/940558616775491584





CISO (aux USA) un métier en pleine mutation chez les Fortune 500

- Durée moyenne en poste : 4,5 ans
- 45% de MBA

https://www.darkreading.com/careers-and-people/cisos-play-rising-role-in-business/d/d-id/1330708

Divers / Trolls velus

L’opérateur d’un botnet Mirai hébergeait le serveur de contrôle…

- Chez lui, à son domicile !!?

https://assets.documentcloud.org/documents/4327736/Paras-Jha-plea-agreement.pdf (page 7)

<<From August to September 2016, Jha set up and maintained technical infrastructure essential to the operation of Mirai. Jha ran Mirai on virtual machines running on his **own hardware,** which he **stored** and maintained **at his family residence.**>>

Bug bounty is a joke

- Arrêtez d'être nuls et de travailler comme des nuls ;)

https://medium.com/@phwd/bug-bounty-is-a-joke-91bc1875c890

Miner des bitcoins avec des pacemaker

- Il en faut 44,000 pendant 1 mois pour miner 1 bitcoin

https://motherboard.vice.com/en_us/article/vby7ny/bitcoin-body-heat-mining?utm_source=mbtwitter

Kidnapping et rançon d’un millions de dollars en bitcoins

https://www.zerohedge.com/news/2017-12-29/bitcoin-exchange-ceo-released-after-paying-1-million-ransom

Divers / Trolls velus

La meilleure protection contre les piratages a enfin été trouvée !!!

- Faire supprimer son mot de passe de toutes les dictionnaires des hackeurs

  https://github.com/danielmiessler/SecLists/pull/155

```
<<Remove my password from lists so hackers won't be able to hack
 me>>
```

Les Top arbitraires de l’année écoulée

Les Top arbitraires de l'année écoulée

2017, l'année des **mots de passe vides** ou **non vérifiés**

- Vulnérabilité critique sur **Oracle** Identity Manager / CVE-2017-10151
- **macOS**, contournement enfantin du mot de passe root / CVE-2017-13872
- Non vérification du mot de passe admin sur **FortiWebManager** 5.8.0 / CVE-2017-14189

2017, l'année des **vulnérabilités** touchant de très **larges périmètres**

- WPA2 est cassé / **KRACK** ou Key Reinstallation Attacks
- Puce **TPM Infineon** et leur entropie cassée
- Vulnérabilités dans **Intel Management Engine** et ses composants (AMT)
- Exécutions de code à distance dans Apache **Struts2** (permettant la compromission d'Equifax)

2017, l'année confirmant que même **l'antivirus** de **Microsoft** est **bourré** de **vulnérabilités** (>10)

- Tout comme les autres antivirus du marché

Les Top arbitraires de l'année écoulée

Bonne année 2018

2017, l'année des **fuites massives** de **données** dans la continuité de 2016

- Fuite de 900Go de données de **Cellebrite**
- **Booz Allen Hamilton** stocke des données classifiées sur un bucket S3 public (drones et programmes satellites militaires)
- **EquiFax**, fuite des données de 143 millions de personnes
- **Deloitte** victime d'une attaque sur sa messagerie Office 365
- **Vault7**, le piratage des hackeurs de la **CIA**
- **ShadowBrokers** publie à nouveau une partie de ce qui a été volé à la NSA / EquationGroup
- Fuite chez la **NSA** par un **sous traitant** (Nghia Hoang Pho) ayant ramené les outils chez lui

2017, l'année des **arrestations** fortement **visibles**

- Les pirates de **Yahoo** (2 hackeurs, mais les 2 membres du FSB identifiés n'ont pas été arrêtés)
- **MalwareTech** (Marcus Hutchins) au retour de la BlackHat
- **Mirai**, identification des auteurs par Brian Krebs (puis arrestation) : des américains de 20 ans

Les Top arbitraires de l'année écoulée

2017, l'année de la **fin** de **SHA-1**

- Collision SHA1 par des chercheurs de Google et "CWI Amsterdam"

2017, l'année des outils **d'audit Active Directory**

- BTA
- PingCastle
- ALSID

2017, l'année de la **fin** des **bulletins** Microsoft **MS**yy-xxx

- Mais aussi de leur retour avec MMSBGA

2017, aussi l'année du **pire article** sur la sécurité informatique

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

Les Top arbitraires de l'année écoulée

Mais surtout, **2017** aura été l'année des **rançongiciels** et **vers-rançongiciels**

- Des pirates bloquent des serrures d'un hôtel et demandent une rançon
- Chiffrement des bases MongoDB et ElasticSearch sur internet, puis demandent une rançon
- **WannaCry**, ver exploitant les vulnérabilités de la NSA et chiffrant les disques
- Faux-Rançongiciel **NotPetya**
- BadRabbit, ce lapin n'est pas gentil

Donc...

Les Top arbitraires de l'année écoulée

2017 peut être **conclue** par une phrase* qui, prononcée il y'a quelques années, aurait fait **perdre toute crédibilité** à son annonceur 😃 :

<< **Donald Trump**, président américain, accuse ouvertement la **Corée du Nord** d'être les auteurs d'un ver numérique prenant ses victimes en otages contre une rançon en **Bitcoins** et réutilisant des **armes numériques** volées à la **NSA** par des **Russes**.

Ces mêmes Russes, qui ont repris l'idée et les armes, en créant un ver faux-rançongiciel, afin de détruire les systèmes d'information d'entreprises Ukrainiennes, impactant gravement de nombreuses entreprises à l'international. >>

**Gain garanti à un loto/bingo des buzz-words* 😉

Prochains rendez-vous de l’OSSIR

Prochaine réunion

- Mardi 13 février 2018

After Work

- Fin Février 2018
- Près de gare de Lyon

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous