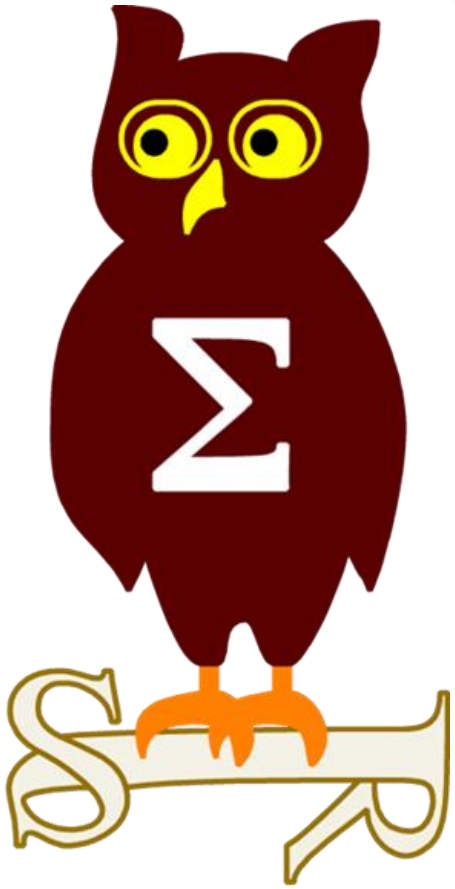
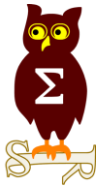


Revue d'actualité

13/02/2018

Préparée par

*Vladimir **K**OLLA @mynameisv_*
*David **P**ELTIER*
*Arnaud **S**OULLIE @arnaudsoullie*



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-001 Vulnérabilités dans Internet Explorer (2 CVE)

- Exploit:
  - 2 x Remote Code Execution
- Crédits:
  - Tao Yan (@Ga1ois) de Palo Alto Networks (CVE-2018-0762)
  - Anonymous par Trend Micro's Zero Day Initiative (CVE-2018-0772)

MS18-002 Vulnérabilités dans Edge (18 CVE)

Dont 2 communes avec IE:
- CVE-2018-0762
- CVE-2018-0772

- Exploit:
  - 13 x Remote Code Execution
  - 4 x Information Disclosure
    - Lecture arbitraire de mémoire depuis Javascript https://bugs.chromium.org/p/project-zero/issues/detail?id=1420
    - Ecriture arbitraire en mémoire depuis Javascript https://bugs.chromium.org/p/project-zero/issues/detail?id=1429
    - https://bugs.chromium.org/p/project-zero/issues/detail?id=1411
  - 1 x Elevation of Privilege
    - https://bugs.chromium.org/p/project-zero/issues/detail?id=1433
- Crédits:
  - Joshua Graham with TSS (CVE-2018-0803)
  - Wei de Qihoo 360 Vulcan Team, Lokihardt de Google Project Zero, 010 par Trend Micro's Zero Day Initiative (CVE-2018-0758)
  - Wei de Qihoo 360 Vulcan Team (CVE-2018-0768, CVE-2018-0773)
  - Anonymous par Trend Micro's Zero Day Initiative (CVE-2018-0772)
  - Tao Yan (@Ga1ois) de Palo Alto Networks (CVE-2018-0762)
  - Johnathan Norman de Windows Devices Group Operating System Security Team (CVE-2018-0800)
  - ? (CVE-2018-0778, CVE-2018-0781, CVE-2018-0766)
  - Lokihardt de Google Project Zero (CVE-2018-0775, CVE-2018-0780, CVE-2018-0777, CVE-2018-0769, CVE-2018-0767, CVE-2018-0776, CVE-2018-0770, CVE-2018-0774)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-003 Vulnérabilités dans Office (21 CVE)

- Affecté:
  - Microsoft Office 2007, 2010, Web Apps 2010, 2013, Web Apps 2013, 2016, 2016 for Mac
  - Microsoft SharePoint 2010, 2013, 2016
- Exploit:
  - 1 x Tampering
  - 1 x Spoofing
  - 19 x Remote Code Execution
    - CVE-2018-0819, code d'exploitation public
    - CVE-2018-0802, éditeur d'équations, exploité dans la nature https://twitter.com/ITh4cker/status/956055429829812225
      - Exemple de code d''exploitation https://github.com/rxwx/CVE-2018-0802
- Crédits:
  - Yuki Chen de Qihoo 360 Vulcan Team, Gal De Leon de Palo Alto Networks, bee13oy de Qihoo 360 Vulcan Team (CVE-2018-0807)
  - Steven Hunter de MSRC Vulnerabilities & Mitigations, Yuki Chen de Qihoo 360 Vulcan Team (CVE-2018-0801)
  - Wayne Low de Fortinet s FortiGuard Lab (CVE-2018-0797)
  - Ben Faull de Microsoft Office Security (CVE-2018-0795)
  - Debasish Mandal de McAfee (CVE-2018-0792)
  - Sabri Haddouche (@pwnsdx) de Wire Swiss GmbH (CVE-2018-0819)
  - Adrian Ivascu (CVE-2018-0799)
  - Yuki Chen de Qihoo 360 Vulcan Team (CVE-2018-0848, CVE-2018-0849, CVE-2018-0862, CVE-2018-0845, CVE-2018-0804, CVE-2018-0806, CVE-2018-0812)
  - Nicolas Joly de Microsoft Corporation (CVE-2018-0794, CVE-2018-0793, CVE-2018-0791)
  - bee13oy de Qihoo 360 Vulcan Team, Yuki Chen de Qihoo 360 Vulcan Team, Nicolas Joly de Microsoft Corporation, Gal De Leon de Palo Alto Networks, Huang Yi de Qihoo 360 Core Security (CVE-2018-0798)
  - Yuki Chen de Qihoo 360 Vulcan Team, Wenxuan Zheng de Tencent PC Manager, bee13oy de Qihoo 360 Vulcan Team (CVE-2018-0805)
  - zhouat de Qihoo 360 Vulcan Team, Zhiyuan Zheng, bee13oy de Qihoo 360 Vulcan Team, Luka Treiber de 0patch Team - ACROS Security, Yang Kang, Ding Maoyin and Song Shenlei, and Jinquan de Qihoo 360 Core Security (@360CoreSec), Liang Yin de Tencent PC Manager, Yuki Chen de Qihoo 360 Vulcan Team, Netanel Ben Simon and Omer Gull de Check Point Software Technologies (CVE-2018-0802)
  - Omair par Trend Micro's Zero Day Initiative (CVE-2018-0796)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-004 Vulnérabilités dans Windows (7 CVE)

- Affectés:
  - Windows toutes versions supportées
- Exploit:
  - 3 x Information Disclosure
  - 4 x Elevation of Privilege
    - Impersonnification de jeton de privilèges https://bugs.chromium.org/p/project-zero/issues/detail?id=1415 et https://bugs.chromium.org/p/project-zero/issues/detail?id=1414
    - Contournement des vérifications de sécurité à la création d'un fichier NTFS https://bugs.chromium.org/p/project-zero/issues/detail?id=1407
- Crédits:
  - Mateusz Jurczyk de Google Project Zero (CVE-2018-0745, CVE-2018-0747, CVE-2018-0746)
  - Tavis Ormandy de Google Project Zero (CVE-2018-0744)
  - James Forshaw de Google Project Zero (CVE-2018-0751, CVE-2018-0752, CVE-2018-0748)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-005 Vulnérabilités dans Microsoft Graphics (GDI) (4 CVE)

- Affectés:
  - Windows toutes versions supportées
- Exploit:
  - 4 x Information Disclosure
    - https://bugs.chromium.org/p/project-zero/issues/detail?id=1399
    - https://bugs.chromium.org/p/project-zero/issues/detail?id=1401
    - https://bugs.chromium.org/p/project-zero/issues/detail?id=1402
- Crédits:
  - Mateusz Jurczyk de Google Project Zero (CVE-2018-0788, CVE-2018-0754)
  - Lucas Leong (@_wmliang_) de Trend Micro (CVE-2018-0741)
  - Seonung Jang(@seonunghardt) (CVE-2018-0750)

MS18-006 Vulnérabilités dans .Net (2 CVE)

- Affectés:
  - .NET toutes versions supportées (Core 1.0, 1.1, 2.0, Framework 2.0, 3.5.*, 4.5.2, 4.6.*, 4.7.*)
  - PowerShell Core 6.0.0
- Exploit:
  - 1 x Denial of Service
  - 1 x Security Feature Bypass
- Crédits:
  - ? (CVE-2018-0786, CVE-2018-0764)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-007 Vulnérabilités dans SharePoint (2 CVE)

- Affectés:
  - Microsoft SharePoint Enterprise Server 2010, 2013, 2016
- Exploit:
  - 1 x Spoofing
  - 1 x Information Disclosure
- Crédits:
  - Ashar Javed de Hyundai AutoEver Europe GmbH (CVE-2018-0789)
  - ? (CVE-2018-0790)

MS18-008 Vulnérabilités dans ASP.NET (2 CVE)

- Affectés:
  - ASP.NET Core 2.0
- Exploit:
  - 1 x Tampering
    - 1 x Elevation of Privilege
- Crédits:
  - K vin Chalet (CVE-2018-0785, CVE-2018-0784)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-009 Vulnérabilité dans Scripting Engine (JScript and/or VBScript) (1 CVE)

- Affectés:
  - ChakraCore
- Exploit:
  - 1 x Security Feature Bypass
- Crédits:
  - Ivan Fratric de Google Project Zero (CVE-2018-0818)

MS18-010 Vulnérabilité dans Windows Subsystem for Linux (1 CVE)

- Affectés:
  - Windows 10
- Exploit:
  - 1 x Elevation of Privilege, à partir de la fonction execve()

    https://github.com/saaramar/execve_exploit
- Crédits:
  - Saar Amar (CVE-2018-0743)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-011 Vulnérabilité dans Windows IPSec (1 CVE)

- Affectés:
  - Windows 8.1, 10, Server 2012, 2012 R2, 2016
- Exploit:
  - 1 x Denial of Service
- Crédits:
  - ? (CVE-2018-0753)

MS18-012 Vulnérabilité dans Windows SMB (1 CVE)

- Affectés:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Elevation of Privilege, redirection locale d'un accès SMB vers n'importe quel "device", comme un pipe nommé
    - https://bugs.chromium.org/p/project-zero/issues/detail?id=1416
- Crédits:
  - James Forshaw de Google Project Zero (CVE-2018-0749)

Failles / Bulletins / Advisories

Microsoft - Advisories

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**

ADV180002, correctif pour Spectre et Meltdown

- CVE-2017-5753 - Bounds check bypass
- CVE-2017-5715 - Branch target injection
- CVE-2017-5754 - Rogue data cache load

Failles / Bulletins / Advisories

Microsoft - Autre

Nouveau correctif pour Spectre

- Supprimant le code créant des problèmes d'instabilité, le temps d'avoir un correctif stable

  http://www.catalog.update.microsoft.com/Search.aspx?q=KB4078130

Microsoft souhaite apporter plus de transparence sur sa télémétrie

https://www.nextinpact.com/news/105396-microsoft-veut-aller-plus-loin-sur-vie-privee-notamment-avec-explorateur-telemetrie.htm

Failles / Bulletins / Advisories

Système (principales failles)

MySQL 5.6.39 et 5.7.21, déni de service sur l'authentification (CVE-2018-2696 et CVE-2018-270)

- Déni de service en cas de mot de passe trop long et utilisation de SHA256
  - Similaire à OpenSSH du mois dernier

http://seclists.org/oss-sec/2018/q1/59

Elévation de privilèges pour le sous-système Linux de Windows

- Vulnérabilité sur execve()

https://github.com/saaramar/execve_exploit

Vulnérabilité dans KDE (Plasma Desktop)

- Insérer une clé USB nommée `` or $() déclenche l'exécution de code

https://www.kde.org/info/security/advisory-20180208-2.txt

Les jeux Blizzard, encore un serveur web local

- Écoutant sur le port 1120 des données en Json
  - Altération du cache DNS local
  - Modification du répertoire du jeu

https://bugs.chromium.org/p/project-zero/issues/detail?id=1471

Failles / Bulletins / Advisories

Système (principales failles)

MacOS, contournement de l'authentification des préférences de l'app Store

- Risque limité car nécessite déjà d'avoir un accès admin

  http://securityaffairs.co/wordpress/67649/hacking/macos-high-sierra-flaw.html

Exécution de code distant sur Google Chrome Android (CVE-2017-5116 et CVE-2017-14904)

- Présenté durant le PwnFest2016, cet enchaînement d'exploit permet d'injecter du code via une URL malicieuse dans Chrome sur Android.
- Récompense de $105,000 par Google

  https://android-developers.googleblog.com/2018/01/android-security-ecosystem-investments.html

iOS, déni de service à la réception d'un message

- Préchargement et prévisualisation des contenus (url, carte de visite…)

  https://vincedes3.com/crash-message-app-iphone/ (attention, lien avec beaucoup de publicités)

Lenovo, porte dérobée sur lecteur d'empreintes

- Possible de récupérer les informations stockées…
- ...Mais aussi de s'authentifier avec un mot de passe codé en dur

  https://www.bleepingcomputer.com/news/security/lenovos-fingerprint-scanner-can-be-bypassed-via-a-hardcoded-password/

  https://support.lenovo.com/fr/fr/product_security/len-15999

  https://wccftech.com/lenovo-fingerprint-scanner-hardcoded-password/

Failles / Bulletins / Advisories

Système (principales failles)

VirtualBox, évasion de la machine virtuelle / CVE-2018-2698

- Lecture/Ecriture arbitraire par le composant graphique
- Tous les détails avec un exploit : https://blogs.securiteam.com/index.php/archives/3649

  https://twitter.com/_niklasb/status/953604276726718465/photo/1

Failles / Bulletins / Advisories

Réseau (principales failles)

AsusWRT, contournement d'authentification et exécution de code (CVE-2018-5999 et CVE-2018-6000)

- Routeur principalement utilisé par les particuliers

https://www.exploit-db.com/exploits/43881/

Lenovo découvre une porte dérobée dans un de ses produits

- Et décide de la supprimer
- Porte dérobée dans le microcode des commutateurs RackSwitch et BladeCenter depuis 2004
  - Entreprises rachetés par Lenovo en 2014

https://www.bleepingcomputer.com/news/security/lenovo-discovers-and-removes-backdoor-in-networking-switches/

VPN Pulse, exécution de code

- Buffer overflow sur le serveur VPN

http://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA43604/

Failles / Bulletins / Advisories

Réseau (principales failles)

Cisco ASA, exécution de code à distance sans authentification / CVE-2018-0101

- “Double Free” lors de l’initialisation de connexions VPN SSL
- Cisco met 80 jours à publier un correctif
- Le premier correctif était incomplet et un second a été publié le 05/02/2018

  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1

- Les slides expliquant la vulnérabilité, présentés à la conférence Recon Bruxelles

  https://www.nccgroup.trust/globalassets/newsroom/uk/events/2018/02/reconbrx2018-robin-hood-vs-cisco-asa.pdf

- Code d’exploitation en 3 lignes d’XML :

```
<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="a" type="a" aggregate-auth-version="a">
    <host-scan-reply>A</host-scan-reply>
</config-auth>
```

- Près de 140 000 firewall Cisco ASA avec VPN sur Internet
  - Bientôt un WannaCry-ASA ?

Failles / Bulletins / Advisories

Hardware / IoT

Exécution de code sur une pompe médical de perfusion

- Particularité: le README Github explique de fond en comble comment le chercheur a procédé. Un must-read!

https://github.com/sgayou/medfusion-4000-research/blob/master/doc/README.md

HP iLo, exécution de code “triviale” à distance

- Publication des slides et des codes d’exploitation
- Ajouter un entête HTTP “Connection:” et vous êtes admin !!!

https://github.com/airbus-seclab/ilo4_toolbox

Autosploit, attaques à grande échelle

- Outil qui combine Shodan et Metasploit pour compromettre un maximum de cibles
- Relance le débat des outils d’attaque…

https://twitter.com/Real__Vector/status/958412549044801536

https://motherboard.vice.com/en_us/article/xw4emj/autosploit-automated-hacking-tool

https://github.com/NullArray/AutoSploit

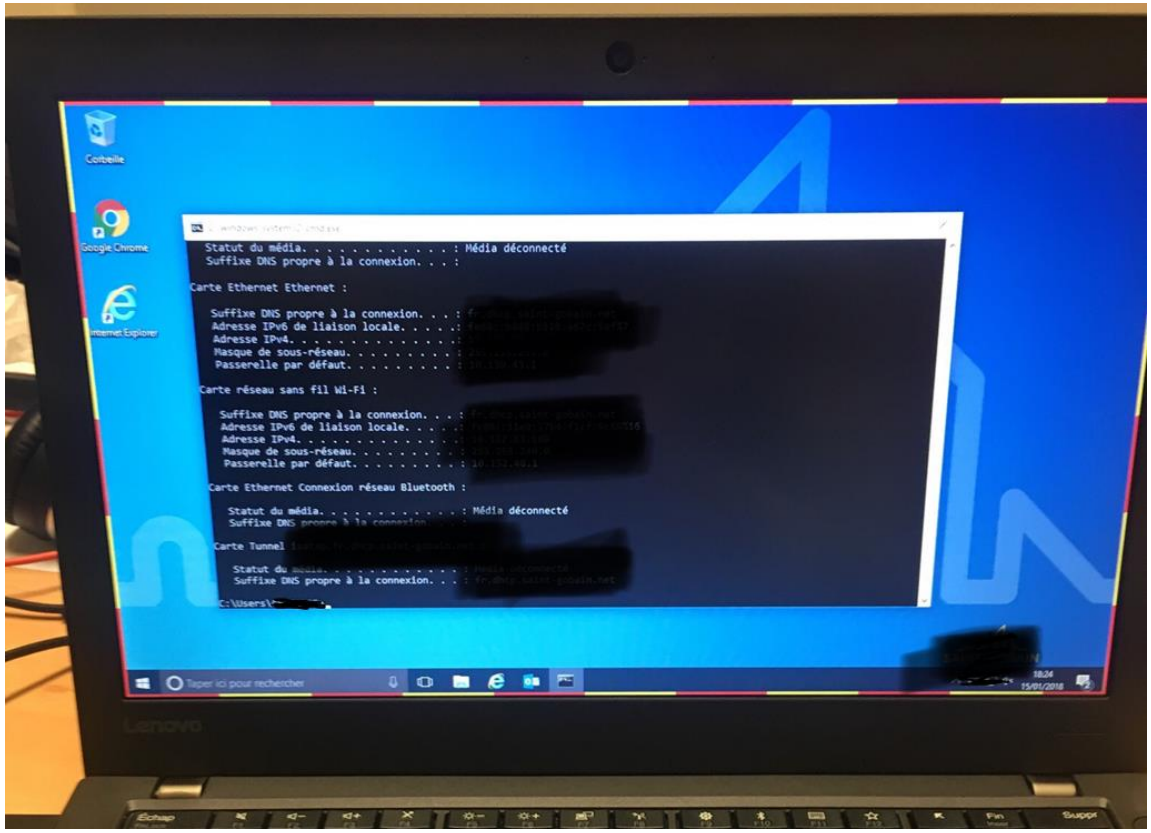
Failles / Bulletins / Advisories

Hardware / IoT

Intel AMT / Management Engine

- Ctrl+P au démarrage (si activé) et accès à Intel Management Engine BIOS Extension
- Mot de passe par défaut “admin”
- Permet de configurer un accès distant fenêtré (kvm) sans validation par l’utilisateur
- Contourne l’accès protégé au Bios par un mot de passe

https://business.f-secure.com/intel-amt-security-issue

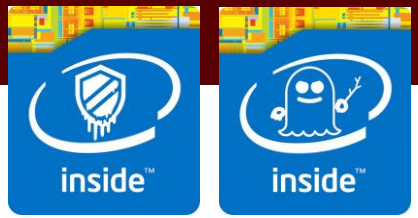


Intel AMT / Management Engine, et pendant ce temps là, à Vera Cruz

- Intel fait de la publicité sur AMT

Failles / Bulletins / Advisories

Hardware / IoT



Spectre/Meldown - la suite

- Problèmes d'instabilité avec les correctifs d'**Intel**
  - Impacts sur la performance et redémarrages aléatoires
- Retrait des correctifs chez:
  - Intel

    http://securityaffairs.co/wordpress/67905/breaking-news/meltdown-and-spectre-patches.html
  - RedHat

    https://access.redhat.com/solutions/3315431
  - VMWare

    https://www.vmware.com/us/security/advisories/VMSA-2018-0002.html
  - Dell

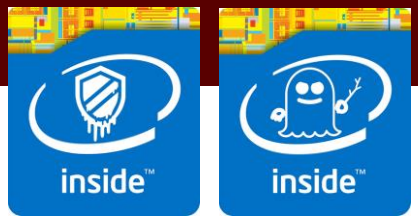
    http://www.dell.com/support/article/fr/fr/frbsdt1/sln308588/microprocessor-side-channel-vulnerabilities-cve-2017-5715-cve-2017-5753-cve-2017-5754-impact-on-dell-emc-products-dell-enterprise-servers-storage-and-networking-?lang=en
- Comment visualiser ces impacts sur les performances avec VMware

  https://blogs.vmware.com/management/2018/01/assess-performance-impact-spectre-meltdown-patches-using-vrealize-operations-manager.html
- Démonstration des pertes de performances

  https://www.virtualizationhowto.com/2018/01/vmware-performance-impact-of-meltdown-and-spectre-patches/

Failles / Bulletins / Advisories

Hardware / IoT



Spectre/Meldown - la suite

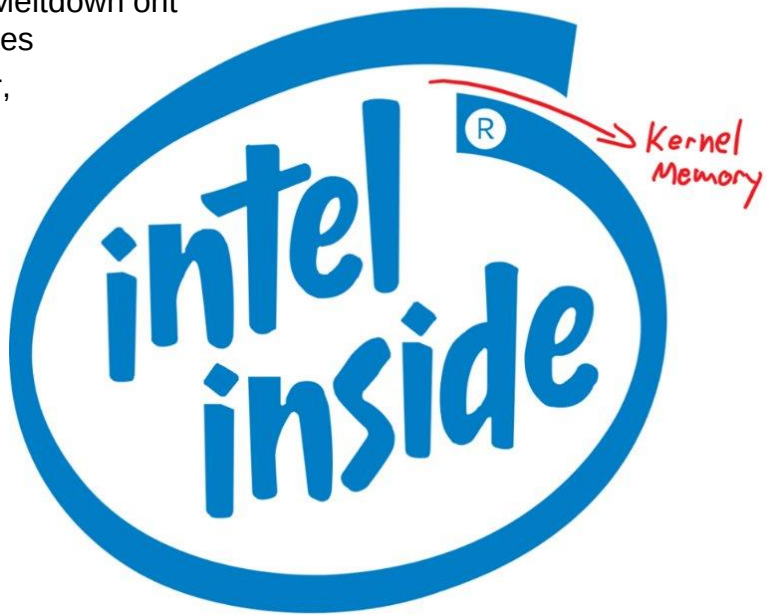
- Impossible d'exploiter en PHP, le langage est trop lent 

  https://secure.phabricator.com/T13038
- Les fabricants chinois auraient été avertis avant le gouvernement US

  https://www.wsj.com/articles/intel-warned-chinese-companies-of-chip-flaws-before-u-s-government-1517157430
- Nouveau logo d'intel ?

  https://twitter.com/helios748/status/957898779826335744

- Les vulnérabilités commencent à être exploitées
  - Plus de 130 codes malveillants exploitant les failles Spectre et Meltdown ont été repérés par les chercheurs d'AV-TEST, de différentes sources
  - En grande partie basés sur le PoC Javascript sorti début janvier,
  .



Failles / Bulletins / Advisories

Android / iOS

Telegram, directory traversal

- En cas d'envoie d'un fichier, contrôle du nom et du chemin, permettant une écriture arbitraire
  https://bugs.chromium.org/p/project-zero/issues/detail?id=1470

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Fuites de données avec Chrome

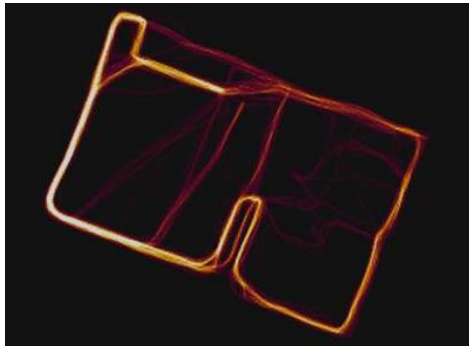
- Recherche d'un seul mot = sous windows, requêtes Netbios

```
  707 40.141683  172.20.[redacted]172.20.0.255 NBNS       92 Name query NB MCI<00>
  722 40.892010  172.20.[redacted] 172.20.0.255 NBNS       92 Name query NB MCI<00>
  727 41.642772  172.20.[redacted]172.20.0.255 NBNS       92 Name query NB MCI<00>

20233 462.518746 172.20.[redacted]172.20.0.255 NBNS       92 Name query NB DELPIERRE<00>
20242 463.263928 172.20.[redacted]172.20.0.255 NBNS       92 Name query NB DELPIERRE<00>
20244 463.676651 172.20.[redacted]172.20.0.255 NBNS       92 Name query NB SS4.TISCALI.COM<00>
20247 464.016081 172.20.[redacted]172.20.0.255 NBNS       92 Name query NB DELPIERRE<00>
20252 464.422864 172.20.[redacted]172.20.0.255 NBNS       92 Name query NB SS4.TISCALI.COM<00>
20277 465.172879 172.20.[redacted]172.20.0.255 NBNS       92 Name query NB SS4.TISCALI.COM<00>
20872 492.662671 172.20.[redacted]172.20.0.255 NBNS       92 Name query NB BITLY<00>

  21817 545.766785 172.20.[redacted]172.20.0.255 NBNS       92 Name query NB DSIA<00>
  21992 555.211843 172.20.[redacted] 172.20.0.255 NBNS       92 Name query NB SFUSER<00>

18113 221.060177 172.20.[redacted] 172.20.0.255 NBNS       92 Name query NB CTFTIME<00>
19931 295.018187 172.20.[redacted]172.20.0.255 NBNS       92 Name query NB EUROVIA<00>

67987 1226.795…  172.20.[redacted]172.20.0.255 NBNS       92 Name query NB INTERNE<00>
68167 1227.545…  172.20.[redacted]172.20.0.255 NBNS       92 Name query NB INTERNE<00>

72067 1360.591…  172.20.[redacted]172.20.0.255 NBNS       92 Name query NB AV.NETXP.FR<00>
72074 1361.341…  172.20.[redacted]172.20.0.255 NBNS       92 Name query NB AV.NETXP.FR<00>
```

Contours de bases militaires grâce à une application de running

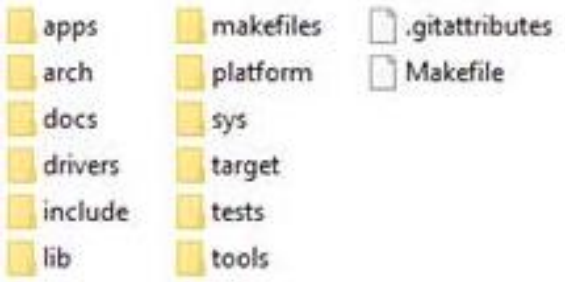
- Visualisation grâce aux cartes (heatmap) publiques des courses

  https://labs.strava.com/heatmap/#16.69/38.92967/36.25852/hot/all



Fuite du code source d'Apple iBoot pour iOS 9.3

- Publication partielle du code source
  - Au début limité à 5 amis intéressés par le jailbreak
  - Perte du contrôle de la diffusion...
- Quelques découvertes intéressantes :
  - Apple fait du fuzzing des ses interfaces




```
Introduction
============

A number of iBoot modules have fuzzing interfaces. This document describes
how to fuzz those modules, and how to set up a new module for fuzzing.

There are a number of open and closed-source fuzzers available, but by far
the best is AFL (american fuzzy lop): <http://lcamtuf.coredump.cx/afl/>.
The rest of this document is geared towards fuzzing with AFL, but the
interface is fairly generic.

Getting AFL
===========
AFL is available in source format at http://lcamtuf.coredump.cx/afl/.
Building should just be a matter of typing "make".

The source includes a good README. The following AFL docs are also
useful (in the AFL source):
- docs/technical_details.txt
- docs/status_screen.txt
- docs/notes_for_asan.txt

Instrumenting Test Binaries
===========================
```

https://motherboard.vice.com/en_us/article/xw5yd7/how-iphone-iboot-source-code-leaked-on-github

Piratages, Malwares, spam, fraudes et DDoS
Espionnage

Dark Caracal, opération visant des dizaines de pays

- Fausses applications mobiles (whatsapp, signal) contenant une porte dérobée
  - Infection par harponnage / spear phishing
  - Uniquement Android
- En fonction depuis 2012
- EFF and Lookout attribuant l'attaque aux services libanais

https://www.eff.org/press/releases/eff-and-lookout-uncover-new-malware-espionage-campaign-infecting-thousands-around

Piratages, Malwares, spam, fraudes et DDoS
Espionnage

Les renseignements néerlandais (AIVD) ont compromis les Russes d'APT29 / Cozy Bear

- Depuis 2014, avec prise de contrôle des caméras de surveillance
  - Le site serait dans une université près du Kremlin
- Ils ont assistés aux attaques visant la maison blanche en 2014 et le DNC en 2016
  - Pas d'information sur Shadow Broker
- L'AIVD a averti les USA
- Mécontentement des néerlandais suite à la publication

  https://www.washingtonpost.com/world/national-security/new-details-emerge-about-2014-russian-hack-of-the-state-department-it-was-hand-to-hand-combat/2017/04/03/d89168e0-124c-11e7-833c-503e1f6394c9_story.html

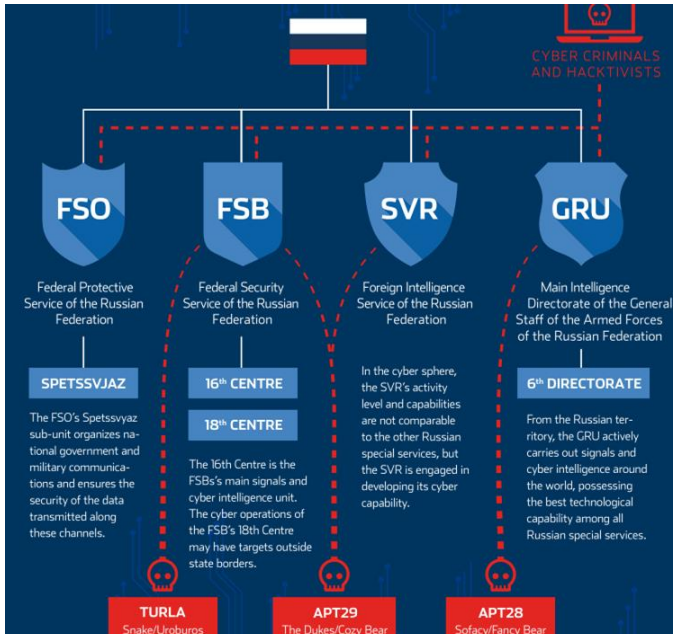
- En décembre, un hackeur Russe emprisonné accusait déjà Poutine et le FSB

  https://www.nextinpact.com/news/105816-emails-dhillary-clinton-pirate-russe-emprisonne-accuse-poutine-et-fsb.htm

Rapport estonien sur les capacités offensives Russes

- APT29 serait lié au FSB

  https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf



Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Boutique OnePlus piraté?

- Les cartes bancaire des clients utilisées frauduleusement après achat sur la boutique.

  https://www.nextinpact.com/brief/oneplus-enquete-sur-des-transactions-frauduleuses--le-paiement-par-cb-desactive-2158.htm

Site de la région Ile de France, fuite de documents personnels

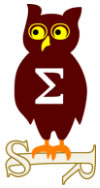
- CV, RIB, copie de passeports et de cartes d'identité

  https://www.nextinpact.com/news/105784-quand-site-region-ile-de-francelaissait-fuiter-cv-passeports-rib-bilans-medicaux.htm

Un hôpital paie une rançon de $55,000 d'un rançongiciel...

- Alors qu'ils avaient des sauvegardes

  https://www.bleepingcomputer.com/news/security/hospital-pays-55k-ransomware-demand-despite-having-backups/



Nouveautés, outils et techniques

Crypto et Divers
Divers

Skype adopte le chiffrement de bout en bout avec le protocole OpenWhisper (Signal)

- Réservé pour le moment aux testeurs
- Pas de date de déploiement prévue

http://www.zdnet.fr/actualites/skype-microsoft-teste-le-chiffrement-de-bout-en-bout-des-conversations-39862620.htm

Google vs Symantec, suite et fin ?

- Chrome 66 (17 avril 2018) ne reconnaîtra plus les autorités de certification de de Symantec
  - Datant d'avant 2016

https://security.googleblog.com/2017/09/chromes-plan-to-distrust-symantec.html

Proposition de sécurisation de l'UEFI par HP

- Le SMM permet de modifier le firmware durant le runtime
- Surveillance du processeur par Control-Flow Integrity via un co-processeur

https://ronny.chevalier.io/files/coprocessor-based-behavior-monitoring-acsac-chevalier-2017.pdf

Quiet, TCP/UDP over sound

- Un peu comme un modem
- Permet d'échanger de l'info entre deux périphériques via le son

https://github.com/quiet/org.quietmodem.Quiet

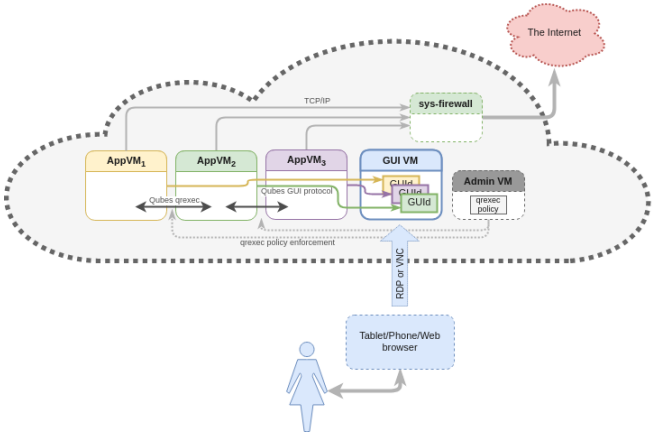
Crypto et Divers

Divers

Qubes AIR !

- Concept d'utilisation de Qubes en mode Cloud ou hybride
- Permettrait de simplifier l'installation et l'usage au quotidien

https://www.qubes-os.org/news/2018/01/22/qubes-air/



Attaques sur la reconnaissance vocale

- Insertion inaudible de commandes Google, Alexa…

https://nicholas.carlini.com/code/audio_adversarial_examples/

Pentest
Techniques & outils

Contournement Windows Defender avec OLE/COM

- Exploit Guard: Controlled folder access
  - Nouvelle fonctionnalité limitant les privilèges des logiciels, contre les rançongiciels
- Contournement en utilisant les objets COM d'Office pour réaliser des actions
  - Comme chiffrer des documents
- Dans la liste blanche par défaut

http://www.securitybydefault.com/2018/01/microsoft-anti-ransomware-bypass-not.html?m=1

DCShadow, nouvelle technique de persistance en environnement Active Directory

- En post-exploitation et après avoir obtenu les privilèges d'administration du domaine
  - Promotion d'un poste de travail comme Contrôleur de Domaine
  - Modification d'objets AD et synchronisations avec les autres contrôleurs de domaines et
- Non détecté par les SOC s'ils ne font que collecter des logs
- Détecté par Microsoft Advanced Threat Analytics (ATA)

https://www.dcshadow.com/

https://www.nolimitsecu.fr/dcshadow/

Installation d'un certificat Root sans validation utilisateur

- En envoyant la valeur d'un clic sur "oui" à la fenêtre

https://twitter.com/subtee/status/955986568170188800

Pentest
Techniques & outils

Reelphish

- Outil de phishing pour les authentifications à deux facteurs

  https://github.com/fireeye/ReelPhish

Utilisation des Shadow copy pour l'exécution de code et la persistance

https://bohops.com/2018/02/10/vshadow-abusing-the-volume-shadow-service-for-evasion-persistence-and-active-directory-database-extraction/

Grouper, reconnaissance Active Directory

- Permet d'analyser les GPOs et d'identifier les réglages exploitables

  https://github.com/l0ss/Grouper/blob/master/README.md

Phantom evasion

- Génère des payloads non détectées par les AV

  https://github.com/oddcod3/Phantom-Evasion

APTSimulator, comme son nom l’indique

- Permet de tester ses outils de détection

  https://github.com/NextronSystems/APTSimulator

Malware DarkComet, exécution de code sur le serveur

- Téléchargement arbitraire de fichiers sur le serveur (mais il faut deviner le chemin)
- Téléversement arbitraire de fichiers sur le serveur (sans savoir où)
  - Fuite du nom d'utilisateur exécutant le serveur (téléchargement vers un UNC)
  - Exécution de code en téléversant upnp.exe dans %tmp%

https://pseudolaboratories.github.io/DarkComet-upload-vulnerability/

Business et Politique

Business

France

BugBounty : Imposer une déclaration à l'ANSSI pour les chercheurs français

- Qui chercheraient sur des OIV

  https://www.nextinpact.com/news/105975-les-deputes-fi-plaident-pour-statut-chasseur-faille-et-dubug-bounty.htm

Business

International

Google créé sa société de cyber-securité: Chronicle

- Objectif: analyser et détecter les attaques menées contre les entreprises par du machine learning
- VirusTotal en fait partie
- A sa tête: Stephen Gillett, ancien dirigeant chez Symantec

https://www.numerama.com/business/324290-avec-chronicle-la-maison-mere-de-google-se-lance-dans-la-cybersecurite.html

NotPetya, Maersk a réinstallé “45 000 PC, 4000 serveurs et 2500 applications en 10 jours”

- Attaqué en août 2017
- Perte de 200$ à 300$ millions en raison des interruptions de services
- Réinstallation pratiquement d’une infrastructure complète
- Très bonne communication!

http://securityaffairs.co/wordpress/68227/security/maersk-notpetya-attack.html

Le 1er robot licencié !

- Moins productif que les humains

https://www.sciencesetavenir.fr/high-tech/pepper-robot-conseiller-licencie-pour-inefficacite_120428

Business

International

AWS achète Sqrrl, société spécialisée dans la Threat Detection

- Pour une somme avoisinant les $40 millions
- Société proche de la NSA

http://www.zdnet.com/article/aws-acquires-threat-detection-firm-sqrrl/

Droit / Politique

France

Darty épinglé par la CNIL et condamnation à une amende de 100 000€

- <<négligence dans le suivi des actions de son sous-traitant>>
  - Abordé à l'OSSIR le jour des faits 😉

https://www.silicon.fr/donnees-clients-darty-cnil-195907.html

Droit / Politique
International

Peur d'une plainte = consentement dans une chaîne de blocs

- Une application entérine un consentement sexuel dans une chaîne de blocs

  https://gizmodo.com/men-try-to-redefine-sexual-consent-with-blockchain-1821964907

Contre les hackeurs, une seule vraie solution : la bombe atomique !

- Idée marquée du logo "Trump Inside"

  https://www.nytimes.com/2018/01/16/us/politics/pentagon-nuclear-review-cyberattack-trump.html

La dystopie, c'est aujourd'hui

- La vie des Ouighurs en Chine (Xinjang)
- Identité gravée sous forme d'un QR code lors de l'achat d'un couteau
- Tracker GPS dans tous les véhicules
- Collecte de l'ADN lors de contrôles médicaux obligatoires
- Tracking video des déplacements des personnes

  https://www.nytimes.com/2018/02/03/opinion/sunday/china-surveillance-state-uighurs.html

Extension des pouvoirs de la NSA

- L'espionnage massif de la planète va pouvoir reprendre

  https://extranewsfeed.com/we-need-just-41-senators-to-stop-congress-from-reauthorizing-and-expanding-unconstitutional-nsa-1154e3371d27

Conférences

Conférences

Passées

- CORI&IN - 23 janvier 2018 à Lille
- FIC - 23 et 24 janvier 2018 à Lille

A venir

- JSSI - mardi 13 mars 2018 à Paris
- Defcon China - Mai 2018 !!!!

  https://www.defcon.org/html/defcon-china/dc-cn-cfp-form.html

Divers / Trolls velus

Divers / Trolls velus

Scandaleux : Akaoma dépose à l'INPI les termes usuels de la sécurité

- Sécurité périmétrique https://bases-marques.inpi.fr/Typo3_INPI_Marques/marques_fiche_resultats.html?index=1&refId=3947213_201734_fmark

  <<nous scannons, analysons le Web afin de collecter toutes les informations associées à votre client, présentes sur l'internet de manière visible ou non. Nous définissons le niveau d'exposition aux risques, et assurons la veille en intelligence sur tous les éléments néfates à l'exposition sur le Web>>

- Sécurité offensive https://bases-marques.inpi.fr/Typo3_INPI_Marques/marques_fiche_resultats.html?index=1&refId=3930533_201734_fmark
- Sécurité défensive https://bases-marques.inpi.fr/Typo3_INPI_Marques/marques_fiche_resultats.html?index=1&refId=3946877_201734_fmark&y=0
- <<nous menons un audit de vulnérabilité du site internet, marchand ou non. Nous détectons les failles, batissons un rapport et nous vous permettons d'accroître la sécurité des sites dont vous avez la responsabilité.>>

Divers / Trolls velus

Vous avez demandé du troll ?

- <<Bitcoin's fluctuations are too much for even ransomware cybercriminals>>
- Source: Proofpoint, car en décembre, un malware aurait demandé une rançon en dollars

  https://www.theguardian.com/technology/2018/jan/18/bitcoin-fluctuations-ransomware-cybercrminals-malware-developers

Chouchous, Beignets... Budgets cybersécurité, qui veut des budgets ?

- Baromètre des risques 2018 d'Allianz, la Cybersécurité prend la deuxième place

  https://www.latribune.fr/entreprises-finance/banques-finance/assurance/le-risque-cyber-le-2eme-le-plus-redoute-par-les-entreprises-764826.html

Hacking Team, ils sont toujours là !

- 2015, pertes de $1 million
- 2016, profits de $600,000
- L'entreprise saoudienne Tablem Limited prend 20% des parts (immatriculée à Chypre)

  https://motherboard.vice.com/en_us/article/8xvzyp/hacking-team-investor-saudi-arabia

Divers / Trolls velus

<<Nous avons affaire à la crème de la crème de la #cyberattaque. C'est du jamais vu.>>

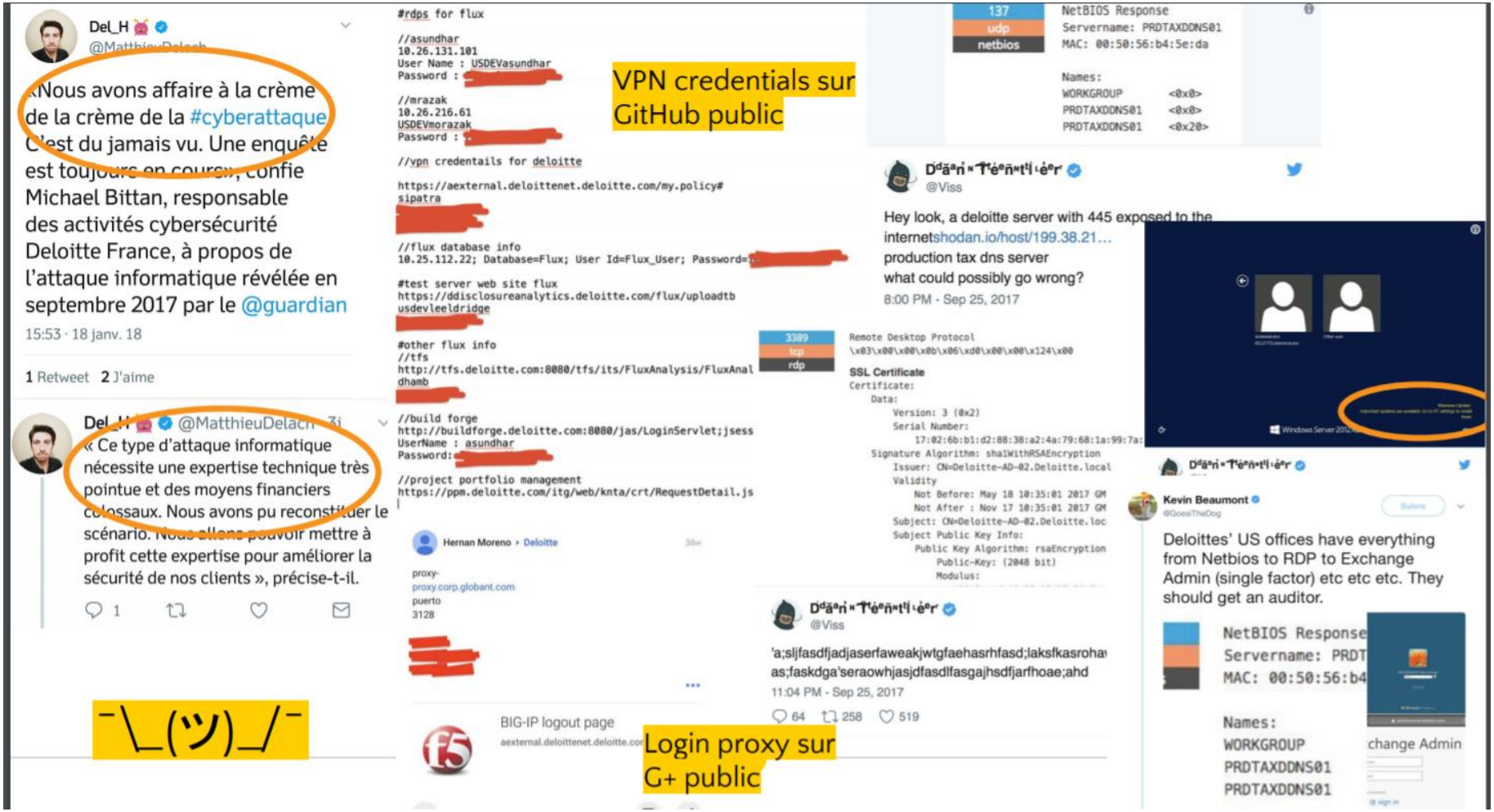
- Quand Deloitte essai de faire passer une attaque **triviale** pour pointue
- Rappels :
  - RDP sur Internet avec administrateurs authentifiés
  - SMB sur Internet
  - Portail d'admin exchange sur internet en simple authentification
  - Comptes et mots de passe VPN sur GitHub

https://twitter.com/MatthieuDelach/status/954003900243247104

Divers / Trolls velus

<<Nous avons affaire à la crème de la crème de la #cyberattaque. C'est du jamais vu.>>

- Présentation à la conférence CORI&IN



Divers / Trolls velus

Serait-ce un aveux ?

https://twitter.com/deloittefrance/status/956452902876393472

Deloitte France
@DeloitteFrance

Follow

#Cybersécurité 63% des incidents de sécurité dont les #entreprises sont victimes proviennent d'un employé bit.ly/2DmFmGN

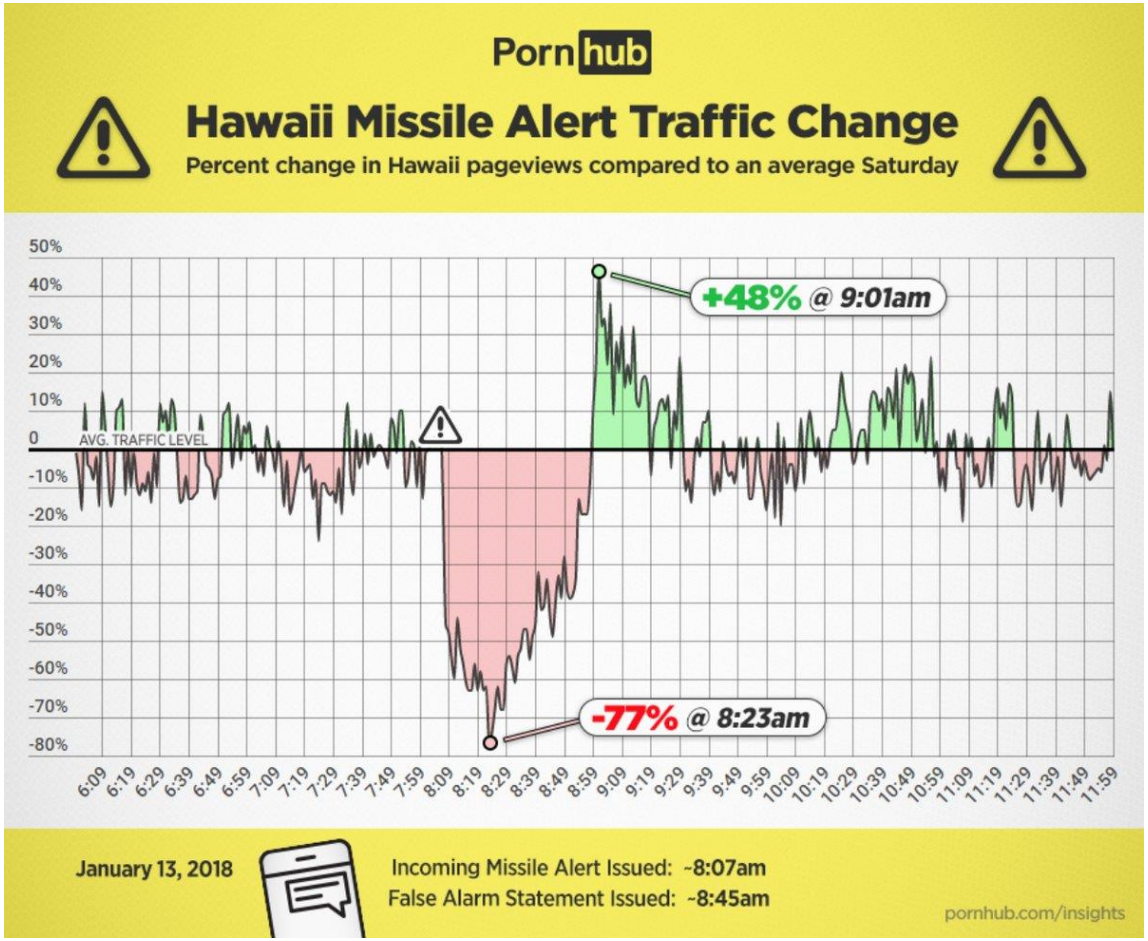
1:05 AM - 25 Jan 2018

Divers / Trolls velus

Une fausse alerte au missile crée la panique à Hawaï

- Du fait de la panique, chute du trafic chez PornHub
- Une fois l'erreur annoncée, énorme remontée du trafic

https://twitter.com/broderick/status/953932791250673664



Divers / Trolls velus

La bonne blague TCP/UDP

Kirk Bater
@KirkBater

Suivre

This image is a TCP/IP Joke. This tweet is a UDP joke. I don't care if you get it.

À l'origine en anglais

Thread
iamkirkbater and jkjustjoshing

iamkirkbater Aug 23rd, 2017 at 9:37 AM
in #www

Do you want to hear a joke about TCP/IP?

7

7 replies

jkjustjoshing 5 months ago
Yes, I'd like to hear a joke about TCP/IP

iamkirkbater 5 months ago
Are you ready to hear the joke about TCP/IP?

jkjustjoshing 5 months ago
I am ready to hear the joke about TCP/IP

iamkirkbater 5 months ago
Here is a joke about TCP/IP.

iamkirkbater 5 months ago
Did you receive the joke about TCP/IP?

jkjustjoshing 5 months ago
I have received the joke about TCP/IP.

iamkirkbater 5 months ago
Excellent. You have received the joke about TCP/IP. Goodbye.

Divers / Trolls velus

C3 Luxembourg…

- oooooooooohhhhhhhhhhhh

  https://twitter.com/Latliq/status/955486549533188096

Prochains rendez-vous de l’OSSIR

Prochaine réunion

- Mardi 10 Avril 2018 [ISEP / Issy les Moulineaux]
  - BTG, outil de qualification d'observables et Machoke, outil de classification de malware (Conix)
  - Introduction à Ethereum, l'ordinateur en blockchain (Jérôme de Tychey)
  - Revue d'actualité (Arnaud Soullié, Vladimir Kolla)

After Work

- Fin février ?

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous