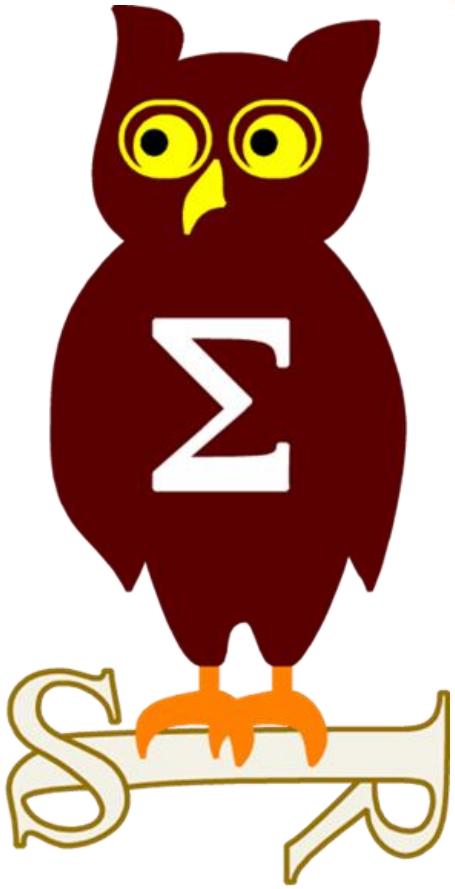
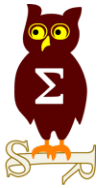


Revue d'actualité

14/04/2017

Préparée par

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



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories

Microsoft - Avis

MS17-006 Vulnérabilités dans Internet Explorer (12 CVE) [Exploitabilité 2,1,3,1,1,1,1,2,2,1,0,1]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - 6 x Corruptions de mémoire aboutissant à une exécution de code
    https://bugs.chromium.org/p/project-zero/issues/detail?id=1076
  - 4 x Contournements ASLR (fuite d'information)
  - 1 x Contournement du Same Origin Policy
  - 1 x Usurpation du contenu d'une page
    https://www.cracking.com.ar/demos/edgesmartscreen/patch-bypass-1.html
- Crédits:
  - Ivan Fratric de Google Project Zero (CVE-2017-0059, CVE-2017-0037)
  - Kai Song exp-sky de Tencent's Xuanwu Lab par Trend Micro's Zero Day Initiative (ZDI) (CVE-2017-0018)
  - Scott Bell de Security-Assessment.com (CVE-2017-0009, CVE-2017-0040, CVE-2017-0049, CVE-2017-0130)

MS17-007 Vulnérabilités dans Edge (32 CVE)  [Exploitabilité 1,1,2,3,1,2,1,1,1,1,1,2,2,1,2,2,1,1,1,2,1,1,1,3,1,1,2,2,1,1,1]

- Affecte:
  - Windows 10
- Exploit:
  - 20 x Corruptions de mémoire aboutissant à une exécution de code
  - 1 x Corruption de mémoire du lecteur PDF aboutissant à une exécution de code
  - 5 x Contournements ASLR (fuite d'information)
  - 3 x Usurpation du contenu d'une page
  - 3 x Contournement du Same Origin Policy
    https://www.securify.nl/advisory/SFY20170101/microsoft_edge_fetch_api_allows_setting_of_arbitrary_request_headers.html
- Crédits:
  - Anonymous par Trend Micro's Zero Day Initiative (ZDI) (CVE-2017-0032)
  - Dhanesh Kizhakkinan de FireEye Inc (CVE-2017-0010, CVE-2017-0035, CVE-2017-0067, CVE-2017-0131, CVE-2017-0133)
  - Gary Kwong (CVE-2017-0067)
  - Hao Linan de Qihoo 360 Vulcan Team (CVE-2017-0032)
  - Henri Aho - https://www.linkedin.com/in/henri-aho-497abab6/ (CVE-2017-0065)
  - Henry Li (zenhumany) de Trend Micro (CVE-2017-0067)
  - Ivan Fratric par Google Project Zero (CVE-2017-0037)
  - Jordan Rabet, Microsoft Offensive Security Research Team (CVE-2017-0134)
  - Jun Kokatsu (@shhnjk) (CVE-2017-0066, CVE-2017-0068, CVE-2017-0069)
  - Lokihart de Google Project Zero (CVE-2017-0070, CVE-2017-0071)
  - Lokihart par ROC/PwnFest (CVE-2017-0015)

Dont 5 communes avec IE:

- CVE-2017-0009
- CVE-2017-0012
- CVE-2017-0015
- CVE-2017-0033
- CVE-2017-0037

Failles / Bulletins / Advisories

Microsoft - Avis

MS17-008 Vulnérabilités dans Hyper-V (11 CVE) [Exploitabilité 2,3,3,2,3,2,3,3,3,3]

- Affecte:
  - Windows Hyper-V
- Exploit:
  - 4 x Exécutions de code à partir (dont avec vSMB) -> évasion de machine virtuelle
  - 6 x Dénis de service
  - 1 x Contournement ASLR (fuite d'information)
- Crédits:
  - Alexander Malysh, Microsoft Network Virtualization Team (CVE-2017-0074)
  - Joe Bialek, MSRC Vulnerabilities et Mitigations Team (CVE-2017-0076)
  - Jonathan Bar Or, Windows Defender ATP Research Team (CVE-2017-0095)
  - Jordan Rabet, Microsoft Offensive Security Research Team (CVE-2017-0021, CVE-2017-0075, CVE-2017-0096, CVE-2017-0099)
  - Lakewood Communications (CVE-2017-0097)
  - MSRC Vulnerabilities et Mitigations Team (CVE-2017-0097, CVE-2017-0109)
  - Peter Hlavaty (@zer0mem), KeenLab, Tencent (CVE-2017-0051)
  - Saruhan Karademir (CVE-2017-0021)
  - Sumit Dhoble, Microsoft Network Virtualization Team (CVE-2017-0074)
  - Yanhui Zhao, Ke Sun de Intel SeCoE Ya Ou, Xiaomin Song, Xiaoning Li de Intel Labs (----------)

MS17-009 Vulnérabilité dans la librairie PDF (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows 8.1, 10, 2012, 2016
- Exploit:
  - Corruption de mémoire aboutissant à une exécution de code
- Crédits:
  - Henry Li (zenhumany) de Trend Micro (CVE-2017-0023)

Failles / Bulletins / Advisories

Microsoft - Avis

MS17-010 Samba (6 CVE) [Exploitabilité 1,1,1,1,1,1]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - 5 x Corruptions de mémoire aboutissant à une exécution de code
  - 1 x Contournement ASLR (fuite d'information)
- Crédits:
  - ?

MS17-011 Vulnérabilités dans Uniscribe / Typographie (29 CVE) [Exploitabilité 2,3,3,3,2,2,2,2,2,3,3,3,3,3,3,3,3,3,3,3,3,2,3,3,3,3,3,3,3]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - 8 x Corruptions de mémoire aboutissant à une exécution de code

    https://www.exploit-db.com/exploits/41647/

    https://bugs.chromium.org/p/project-zero/issues/detail?id=1019 et 1022, 1023, 1025, 1026, 1027, 1028, 1029, 1030, 1031
  - 21 x Contournements ASLR (fuite d'information)
- Crédits:
  - Mateusz Jurczyk de Google Project Zero (CVE-2017-0072, CVE-2017-0083, CVE-2017-0084, CVE-2017-0085, CVE-2017-0086, CVE-2017-0087, CVE-2017-0088, CVE-2017-0089, CVE-2017-0090, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, CVE-2017-0128)

Failles / Bulletins / Advisories

Microsoft - Avis

MS17-012 Vulnérabilités dans Windows (6 CVE) [Exploitabilité 2,1,2,3,3,2,3]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - 1 x Élévation de privilège locale https://github.com/Cn33liz/MS17-012
  - 1 x Contournement de Device Guard (copier/coller une signature authenticode sur un autre script fonctionne)
  - 1 x Déni de service
  - 2 x Corruptions de mémoire aboutissant à une exécution de code
  - 1 x Élévation de privilège locale avec MSBuild.exe https://github.com/Cn33liz/MS17-012
  - 1 x Contournement ASLR (fuite d'information)
- Crédits:
  - Fortinet's FortiGuard Labs (CVE-2017-0104)
  - James Forshaw de Google Project Zero (CVE-2017-0100)
  - Martin Knafve - http://martinknafve.com/ (CVE-2017-0057)
  - Matt Nelson (@enigma0x3) (CVE-2017-0007) **--> cf. slide suivant**
  - lywang de Tencent's Xuanwu LAB (CVE-2017-0039)

MS17-013 Vulnérabilité GDI (12 CVE) [Exploitabilité 2,0,1,1,2,1,2,3,2,3,2,2]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - 6 x Élévations de privilège locale
    http://blogs.flexerasoftware.com/secunia-research/2016/12/microsoft_windows_loaduvstable_heap_based_buffer_overflow_vulnerability.html
    http://0day.today/exploits/27362
  - 6 x Contournements ASLR (fuite d'information)
- Crédits:
  - Hossein Lotfi, Secunia Research at Flexera Software (CVE-2017-0014)
  - Lockheed Martin Computer Incident Response Team (CVE-2017-0005)
  - Lokihart par POC/PwnFest (CVE-2017-0025)
  - Mateusz Jurczyk de Google Project Zero (CVE-2017-0038, CVE-2017-0060, CVE-2017-0061, CVE-2017-0062, CVE-2017-0063, CVE-2017-0108)
  - Peter Hlavaty (@zer0mem), KeenLab, Tencent (CVE-2017-0001)
  - Symeon Paraschoudis de SensePost (CVE-2017-0073)

Failles / Bulletins / Advisories

Microsoft - Avis

CVE-2017-0007

```
c:\windows\system32\windowspowershell\v1.0\examples\profile.ps1:
        Verified:       Signed
        Signing date:   06:51 28/02/2008
        Publisher:      Microsoft Corporation
        Company:        n/a
        Description:    n/a
        Product:        n/a
        Prod version:   n/a
        File version:   n/a
        MachineType:    n/a

C:\Users\[redacted]>sigcheck c:\Users\[redacted]\Desktop\a.ps1

Sigcheck v2.53 - File version and signature viewer
Copyright (C) 2004-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

c:\users\[redacted]\desktop\a.ps1:
        Verified:       The digital signature of the object did not verify.
        File date:      14:11 10/04/2017
        Publisher:      n/a
        Company:        n/a
        Description:    n/a
        Product:        n/a
        Prod version:   n/a
        File version:   n/a
        MachineType:    n/a
```

```
call    SoftpubAuthenticode
mov     rax, [r12]
lea     rcx, [rbp+4Fh+Dst] ; this
mov     rdx, r15           ; struct _CRYPT_PROVIDER_DATA *
mov     r8b, [rax+688h]
and     r8b, 1             ; unsigned __int8
call    ?ConvertFromProvData@SiChainInfo@@QEAAJPEBU_CRYP
```

Failles / Bulletins / Advisories

Microsoft - Avis

MS17-014 Vulnérabilités dans Office (12 CVE) [Exploitabilité 1,1,1,2,3,2,1,1,1,2,2,3]

- Affecte:
  - Office 2007, 2010, 2013, 2013RT, 2016, Mac 2011 et 2016
  - Sharepoint 2010, 2013
- Exploit:
  - 7 x Corruptions de mémoire aboutissant à une exécution de code à l'ouverture d'un fichier Office
  - 2 x Contournements ASLR (fuite d'information)
  - 1 x Déni de service
  - 1 x XSS dans Sharepoint
  - 1 x Contournement de la vérification de certificats de Lync
- Crédits:
  - @j00sean (CVE-2017-0030, CVE-2017-0031)
  - Cheah Khai Ee, (@MercurialSec) (CVE-2017-0107)
  - David Wind de XSEC infosec GmbH (CVE-2017-0029)
  - Fortinet's FortiGuard Labs (CVE-2017-0105)
  - Haifei Li de Intel Security (CVE-2017-0053)
  - Jaanus Kääp de Clarified Security (CVE-2017-0027)
  - Jerry Decime, Hewlett Packard Enterprise (CVE-2017-0129)
  - Qiang Liu, McAfee (CVE-2017-0020)
  - Steven Vittitoe de Google Project Zero (CVE-2017-0019)
  - Tony Loi de Fortinet's FortiGuard Labs (CVE-2017-0019)
  - Yangkang & Liyadong & Wanglu de Qihoo 360 Qex Team (CVE-2017-0006, CVE-2017-0052)

MS17-015 Security Update for Microsoft Exchange Server (1 CVE) [Exploitabilité 3]

- Affecte:
  - Exchange 2013, 2016
- Exploit:
  - 1 x Élévation de privilège locale / injection de script
- Crédits:
  - Gabruel Lima (@gabrielpato) (CVE-2017-0110)

Failles / Bulletins / Advisories

Microsoft - Avis

MS17-016 Microsoft IIS (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - Injection de Javascript / XSS
- Crédits:
  - David Fernandez de Sidertia Solutions (CVE-2017-0055)

MS17-017 Vulnérabilités Noyau win32k (4 CVE) [Exploitabilité 1,2,2,2]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - 4 x Élévations de privilège locale

    https://bugs.chromium.org/p/project-zero/issues/detail?id=993
- Crédits:
  - James Forshaw de Google Project Zero (CVE-2017-0103)
  - Mateusz Jurczyk de Google Project Zero (CVE-2017-0103)
  - Peter Hlavaty (@zer0mem), KeenLab, Tencent (CVE-2017-0101)

Failles / Bulletins / Advisories

Microsoft - Avis

MS17-018 Vulnérabilités Noyau win32k (7 CVE) [Exploitabilité 1,1,2,1,2,2,2]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - 7 x Élévations de privilège locale
- Crédits:
  - Hao Linan de Qihoo 360 Vulcan Team par POC/PwnFest (CVE-2017-0024, CVE-2017-0026)
  - Peter Hlavaty (@zer0mem), KeenLab, Tencent (CVE-2017-0056, CVE-2017-0056, CVE-2017-0078, CVE-2017-0079, CVE-2017-0080, CVE-2017-0081 ,CVE-2017-0082)
  - pgboy de Qihoo 360 Vulcan Team par POC/PwnFest (CVE-2017-0024, CVE-2017-0026)
  - zhong_sf de Qihoo 360 Vulcan Team par POC/PwnFest (CVE-2017-0024, CVE-2017-0026)

MS17-019 Vulnérabilité ADFS (1 CVE) [Exploitabilité 3]

- Affecte:
  - Windows 2008, 2008R2, 2012, 2016
- Exploit:
  - Fuite d'information sensible, à la suite d'une requête XML authentifiée

MS17-020 Vulnérabilité Windows DVD Maker (1 CVE) [Exploitabilité 3]

- Affecte:
  - Windows 7 et Vista
- Exploit:
  - Fuite d'information sensibles par une XSRF dans les fichiers .msdvd
    https://cxsecurity.com/issue/WLB-2017030149
- Crédits:
  - John Page (hyp3rlinx), ApparitionSec (CVE-2017-0045)

Failles / Bulletins / Advisories

Microsoft - Avis

MS17-021 Vulnérabilité dans DirectShow (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - Fuite d'information
- Crédits:
  - Abdulrahman Alqabandi (@qab) (CVE-2017-0042)

MS17-022 Vulnérabilité dans le parseur XML (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - Fuite d'information sensible dans le parseur XML : MSXML
- Crédits:
  - Brooks Li et Joseph C Chen, Trend Micro (CVE-2017-0022)
  - Will Metcalf et Kafeine de Proofpoint (CVE-2017-0022)

Failles / Bulletins / Advisories

Microsoft - Avis

MS17-023 Vulnérabilité dans Adobe Flash Player (7 CVE) [Exploitabilité]

- Affecte:
  - Windows 8.1, 10, 2012, 2016
- Exploit:
  - Exécutions de code à l'ouverture d'une page web contenant un Flash
- Crédits:
  - ?

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 - Advisories et Revisions

Aucune publication ce mois-ci

- Vx.x

Failles / Bulletins / Advisories

Microsoft - Autre

Délégation contrainte Kerberos, quoi de neuf ?

- Permet de limiter l'utilisation de l'identité d'un utilisateur à un ensemble de SPN
- Le secret utilisé pour le chiffrement du TGS étant le condensat du mot de passe
  - Possible de s'authentifier sur tous les services exécutés par le même utilisateur
- Publication d'un outil PowerShell pour faciliter les attaques sur la délégation :

  https://github.com/machosec/Mystique

  https://www.blackhat.com/docs/asia-17/materials/asia-17-Hart-Delegate-To-The-Top-Abusing-Kerberos-For-Arbitrary-Impersonations-And-RCE.pdf

  https://www.coresecurity.com/blog/kerberos-delegation-spns-and-more

Exploitation dans la nature d'une 0day Office

- L'exploit télécharge un .HTA pour contourner les solutions de sécurité

  https://securingtomorrow.mcafee.com/mcafee-labs/critical-office-zero-day-attacks-detected-wild/

  https://www.fireeye.com/blog/threat-research/2017/04/acknowledgement_ofa.html

Failles / Bulletins / Advisories

Microsoft - Autre

Windows Vista, fin de support aujourd'hui

- Mardi 11 avril 2017

  https://support.microsoft.com/fr-fr/help/13853/windows-lifecycle-fact-sheet

Les mises à jour Windows 7-8.1 et les nouveaux CPU

- Fin du support des CPU récents dans les mises à jour, à partir de juillet 2017
- Il faudra faire évoluer votre master vers Windows 10 (ou Linux) 😓

  https://www.nextinpact.com/news/103715-kaby-lake-et-ryzen-mises-a-jour-windows-7-et-8-1-pourraient-echouer.htm

Failles / Bulletins / Advisories

Système (principales failles)

VMware Workstation (CVE-2017-4898)

- Levier pour exécuter du code non signée dans le noyau de Windows 10

  https://github.com/ivildeed/vmw_vmx_overloader

VMware ESXi, Fusion, Workstation, évasion de la machine virtuelle

- Exploit utilisé lors de la compétition Pwn2Own 2017 (CVE-2017-4903 et CVE-2017-4902)

  http://www.vmware.com/security/advisories/VMSA-2017-0006.html

Hyper-V, évasion de la machine virtuelle

- cf. bulletins MS17-008

Xen, évasion de la machine virtuelle

- A cause de la fonction access_ok()

  https://googleprojectzero.blogspot.fr/2017/04/pandavirtualization-exploiting-xen.html

TcpDump, 42 CVE !!!

https://www.debian.org/security/2017/dsa-3775

Failles / Bulletins / Advisories

Système (principales failles)

Apache Struts, Exécution de code à distance

- Vulnérabilité dans le composant « Jakarta Multipart » qui traite le type des contenus envoyés
- Vulnérabilité “wormable”

http://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html

Typo3, injection sql

- Contournement des filtres en mettant un paramètre en minuscule 
- Injection dans “Order By”

```
uid*(case(ord(substring((select(password)from(be_users)where(uid=1))from(2)for(1))))when(48)then(1)else(-1)end)
```

https://www.ambionics.io/blog/typo3-news-module-sqli

Failles / Bulletins / Advisories

Système (principales failles)

LastPass, exécution de code (encore)

- Et encore trouvé par Tavis

  https://twitter.com/taviso/status/845717082717114368/photo/1

Les vulnérabilités des gestionnaires de mot de passe

https://team-sik.org/trent_portfolio/password-manager-apps/

OpenElec, exécution de code en cas de MitM

- Récupération des mises à jour en HTTP et sans vérification de signature
- Désactivé par défaut

  http://seclists.org/fulldisclosure/2017/Mar/11

Elévation de privilèges Linux CVE-2017-2636

- Daterait de 2009
- Exploit avec contournement de SMEP !

  https://a13xp0p0v.github.io/2017/03/24/CVE-2017-2636.html

Failles / Bulletins / Advisories

Réseau (principales failles)

NAS WesternDigital MyCloud, exécution de code

- Exécution de code à distance sans authentification “à l’ancienne”

```
http://$IP/web/addons/jqueryFileTree.php?host=x&pwd=x&user=x&dir=x&l
  ang=x\"\;<os-command-here>\; echo \"x
```

http://seclists.org/fulldisclosure/2017/Mar/19

NAS Synology, vulnérabilités dans Photo

- Contournement de l’authentification, de l’exécution de code et de l’élévation de privilèges

http://kb.hitcon.org/post/158891385842/synology-bug-bounty-report#Vul-03-Read-Write-Arbitrary-Files

Exécution de code dans les firmware WiFi Broadcom

https://googleprojectzero.blogspot.fr/2017/04/over-air-exploiting-broadcoms-wi-fi_4.html

Cisco Catalyst, exécution de code à distance avant authentification

- Sur le service Telnet
- Provient de la fuite des outils de la CIA “Vault7”
- Réécriture de l’exploit

https://artkond.com/2017/04/10/cisco-catalyst-remote-code-execution/

Failles / Bulletins / Advisories

Réseau (principales failles)

Vulnérabilité sur le baseband Huawei

- Smartphones, carte WWAN des portables et IoT sont impactés
- Des dizaines de millions d'équipements failles en cours d'utilisation
- Coeur sous VxWorks avec interpréteur de commande CSH

https://threatpost.com/baseband-zero-day-exposes-millions-of-mobile-phones-to-attack/124833

Failles / Bulletins / Advisories

Les Antivirus

F-Secure, exécution de code en cas de MitM

- Mises à jour en tant que SYSTEM et en HTTP
- Fix: `<<the vendor does not see this as a security problem>>`

  http://seclists.org/fulldisclosure/2017/Mar/28

ESET Endpoint Antivirus 6 pour macOS, exécution de code en cas de MitM

- Parseur POCO XML, basé sur Expat, vulnérable à l'exécution de code CVE-2016-0718
- Exploitable à l'activation en ligne de la licence car le certificat du site n'est pas vérifié

  http://seclists.org/fulldisclosure/2017/Feb/68

Contournements de Comodo, Avira…

- cf. Vault7

Failles / Bulletins / Advisories

Apple, Google, Facebook...

XSS sur Google Maps

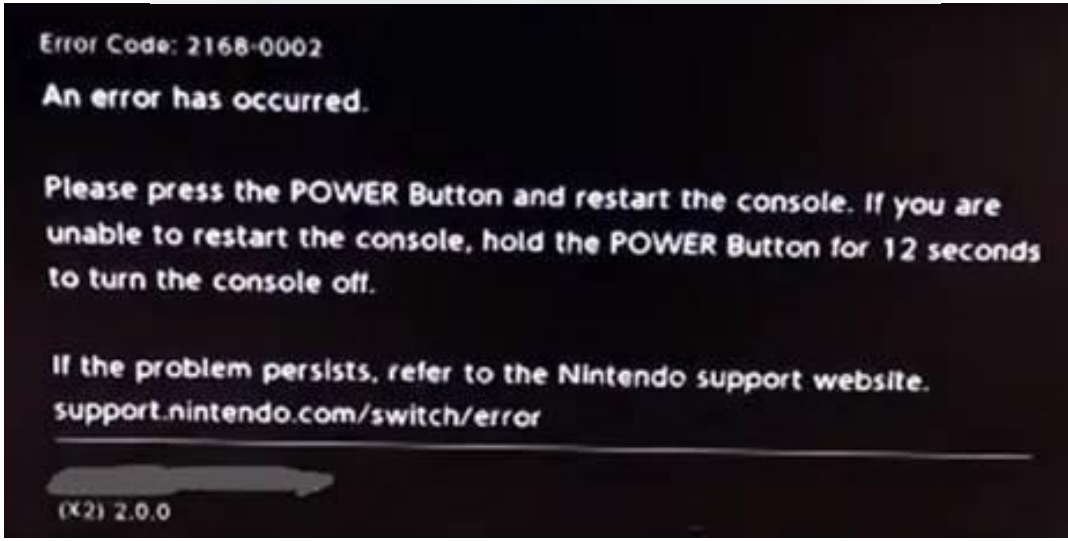
- Rétro-conception complète du processus de sérialisation de Google, non documenté : Protobuf

https://medium.com/@marin_m/how-i-found-a-5-000-google-maps-xss-by-fiddling-with-protobuf-963ee0d9caff#.euyvwhem7

Nintendo Switch, exécution de code

- Navigateur WebKit caché et non à jour
  - Sert à détecter les portails captifs
- Exécution de code CVE-2016-4657
  - Commune avec iOS 9.3 (NSO Group)

https://www.youtube.com/watch?v=xkdPjbaLngE



Failles / Bulletins / Advisories

Apple, Google, Facebook...

CloudBleed, le bug de fuite de mémoire chez ClouFlare

- Découvert (encore) par Tavis Ormandy
- Dépassement de tampon dans l'analyseur syntaxique Ragel depuis le 22 septembre 2016
  - De gros sites impactés : Uber, 1Password, Fitbit, OkCupid …
  - Récupération des cookies, password, login, adresse IP …
- Réaction très rapide de CloudFlare (47 minutes)

https://blog.cloudflare.com/incident-report-on-memory-leak-caused-by-cloudflare-parser-bug/

https://bugs.chromium.org/p/project-zero/issues/detail?id=1139

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

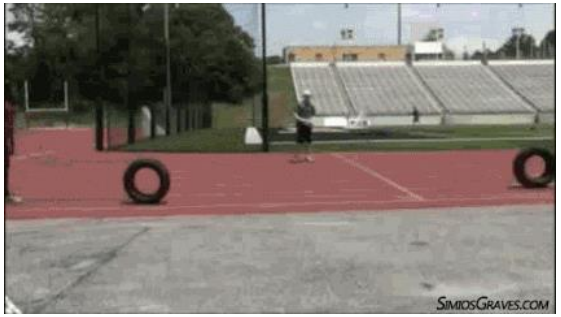
Hack 2.0

Communications entres VMs sur le même Hyperviseur à partir d'un Canal caché

- Basé sur le cache CPU
- Applicable à Amazon EC2

https://github.com/IAIK/CJAG

https://cmaurice.fr/pdf/ndss17_maurice.pdf



Contourner EMET 5.52

- Désactivation de la protection anti-ROP

https://blog.ropchain.com/2017/04/03/disarming-emet-5-52/

- Sinon, il y'a aussi des cours à la BlackHat pour le contourner

https://www.blackhat.com/us-17/training/advanced-security-for-hackers-and-developers.html

Attaquer un smartphone à partir des écouteurs (CVE-2017-0510)

https://alephsecurity.com/2017/03/08/nexus9-fiq-debugger/

Windows 10, exécuter du code noyau

- En débuggant à partir du port série

https://tyranidslair.blogspot.fr/2017/03/getting-code-execution-on-windows-by.html

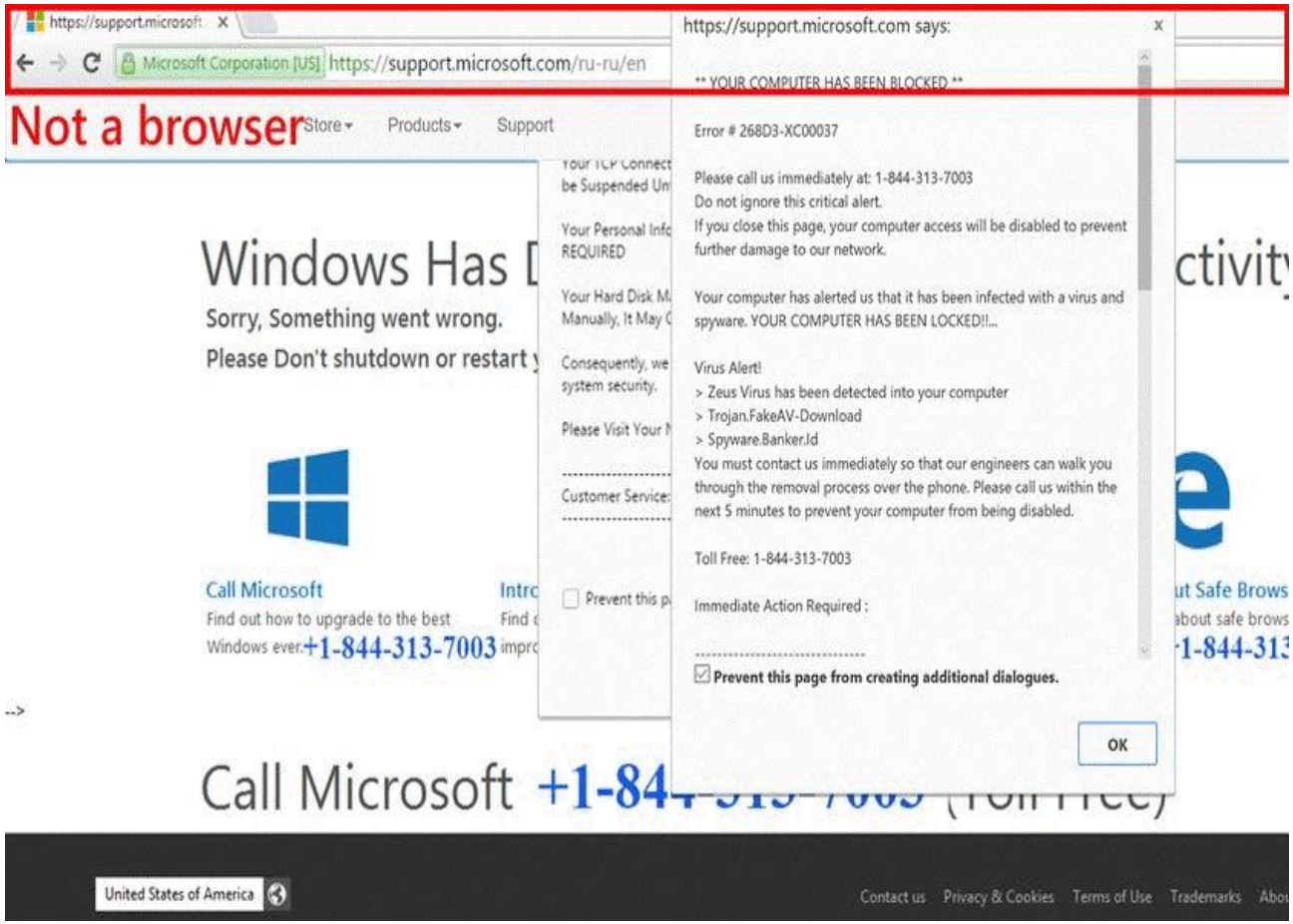
Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Abus du mode plein écran

- Fausse barre d'adresse Microsoft
- Alerte avec pour objectif de faire installer un faux antivirus

https://twitter.com/martijn_grooten/status/838523521416323072/photo/1



Le Domain Fronting, utilisé par APT29 (cf. revue de février)

- A partir d'un plugin pour Tor faisant croire à des accès aux services de Google

  https://www.fireeye.com/blog/threat-research/2017/03/apt29_domain_frontin.html

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Sans maitrise, ~~la puissance~~ l'externalisation dans le Cloud n'est bien

- Piratage d'hébergeurs de Cloud afin de viser les clients
- Campagne en cours de 2014

  http://www.silicon.fr/pirates-chinois-attaquent-entreprises-services-cloud-171551.html

OVH, nouvelle intrusion par un serveur compromis et oublié

- Premier piratage datant de 2015

  http://travaux.ovh.net/?do=details&id=23300

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Piratage raté ciblant Darty

- Par sécurité, ils font une campagne de communication

https://www.nextinpact.com/news/103884-victime-dune-attaque-ratee-darty-va-rappeler-a-ses-clients-regles-elementaires-securite.htm

Objet : Renouvellement de votre mot de passe Darty.com
Envoyé : 11 avr. 2017 10:46 AM
De : Darty <darty@courriel2.gocad.info>
À [redacted]

Information concernant votre compte Darty.com

DARTY

Cher(e) Client(e),

Soucieux d'assurer la sécurité des données de ses clients, Darty lance une campagne de renforcement des mots de passe client créés antérieurement à 2016.

C'est dans le cadre de cette opération de prévention que nous vous sollicitons afin de vous demander de procéder au renouvellement de votre mot de passe sur Darty.com.

Vous trouverez toutes les instructions nécessaires pour réaliser facilement cette opération, ainsi que des conseils pour créer un mot de passe sécurisé, sur le site Darty.com en cliquant sur le lien ci-dessous :
http://www.darty.com/achat/securite/mot-de-passe/index.html

Dans le cas où vous ne seriez pas en mesure de procéder à cette modification dans un délai de 10 jours, nous procéderions à une réinitialisation de votre mot de passe pour vous.
Pas d'inquiétude, vous pourrez alors demander la création d'un nouveau mot de passe sur Darty.com en cliquant sur le lien "se connecter", puis sur "mot de passe oublié".
En cas de question, vous pouvez nous contacter via notre formulaire dédié en cliquant sur le lien ci-joint : http://www.darty.com/achat/contacts/index.html

Merci de votre compréhension.

Cordialement,
Votre Service Client Darty

CLICK

Piratages, Malwares, spam, fraudes et DDoS

Malwares

Rançongiciel qui demande de jouer au jeu Touhou Seirensen ~ Undefined Fantastic Object

- Et d'atteindre un haut score

  https://twitter.com/malwrhunterteam/status/850031671244193792

Verizon pré-installe un outil de collecte sur les smartphones de ses clients

- Réponse de Verizon : il faut valider l'utilisation de l'app et seuls les LG K20 V sont concernés

  https://www.eff.org/deeplinks/2017/03/first-horseman-privacy-apocalypse-has-already-arrived-verizon-announces-plans

Démonstration d'un rançongiciel UEFI

- Débutant par un document Word et une Macro

  https://github.com/REhints/Publications/blob/master/Conferences/BHASIA%202017/BHASIA_2017_final.pdf

Piratages, Malwares, spam, fraudes et DDoS
SCADA

Utiliser la clim' comme canal auxiliaire

https://arxiv.org/ftp/arxiv/papers/1703/1703.10454.pdf

Piratage des alarmes alertant de sinistres (tornades) à Dallas

- Le système est actuellement déconnecté
- Une intrusion physique aurait été nécessaire

  https://www.washingtonpost.com/news/the-intersect/wp/2017/04/09/someone-hacked-every-tornado-siren-in-dallas-it-was-loud/
- Et pendant ce temps-là, à Veracruz... ou plutôt à Boulogne, les alarmes ont également sonné
  - Du fait d'un dysfonctionnement

  https://www.google.fr/amp/m.leparisien.fr/amp/boulogne-billancourt-92100/une-alarme-assourdissante-perturbe-boulogne-billancourt-08-04-2017-6836055.php

Schneider

- Encore des mots de passe en dur dans les firmwares
- Clef de chiffrement en dur impossible à changer "SoMachineBasicSoMachineBasicSoMa"

  https://nakedsecurity.sophos.com/2017/04/10/hard-coded-passwords-put-industrial-systems-at-risk/

Piratages, Malwares, spam, fraudes et DDoS
Hardware / IoT

Piratage de TV par ondes hertziennes

- 90% des téléviseurs vendus seraient vulnérables
- Le standard hbbTV peut demander aux téléviseurs de charger une URL
  - Les téléviseurs se connectent à la source la plus puissante
  - URL vers un site malveillant exploitant une vulnérabilité dans le navigateur (Flash, Javascript)

https://www.bleepingcomputer.com/news/security/about-90-percent-of-smart-tvs-vulnerable-to-remote-hacking-via-rogue-tv-signals/

https://www.youtube.com/watch?v=bOJ_8QHX6OA

Piratage de TV par… le clavier visuel

- En changeant le nom de la télé, précédé d'une apostrophe

```
`cat /etc/passwd && sleep 2`
```

https://www.netsparker.com/blog/web-security/hacking-smart-tv-command-injection/

Rétro-ingénierie d'une alarme connectée

http://blog.seekintoo.com/diy-smart-home-security-meh.html

Compromettre une tablette Nexus 9 par les écouteurs

- Accès à l'UART depuis le câble Jack

https://alephsecurity.com/2017/03/08/nexus9-fiq-debugger/

Piratages, Malwares, spam, fraudes et DDoS

Hardware / IoT

Peluche Spiral Toys, victime d'un piratage... ou victime de l'incompétence du fabriquant ?

- Enregistrement des conversations et messages personnalisés dans une BDD sur Internet
- Base de données librement accessible...

https://www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages/

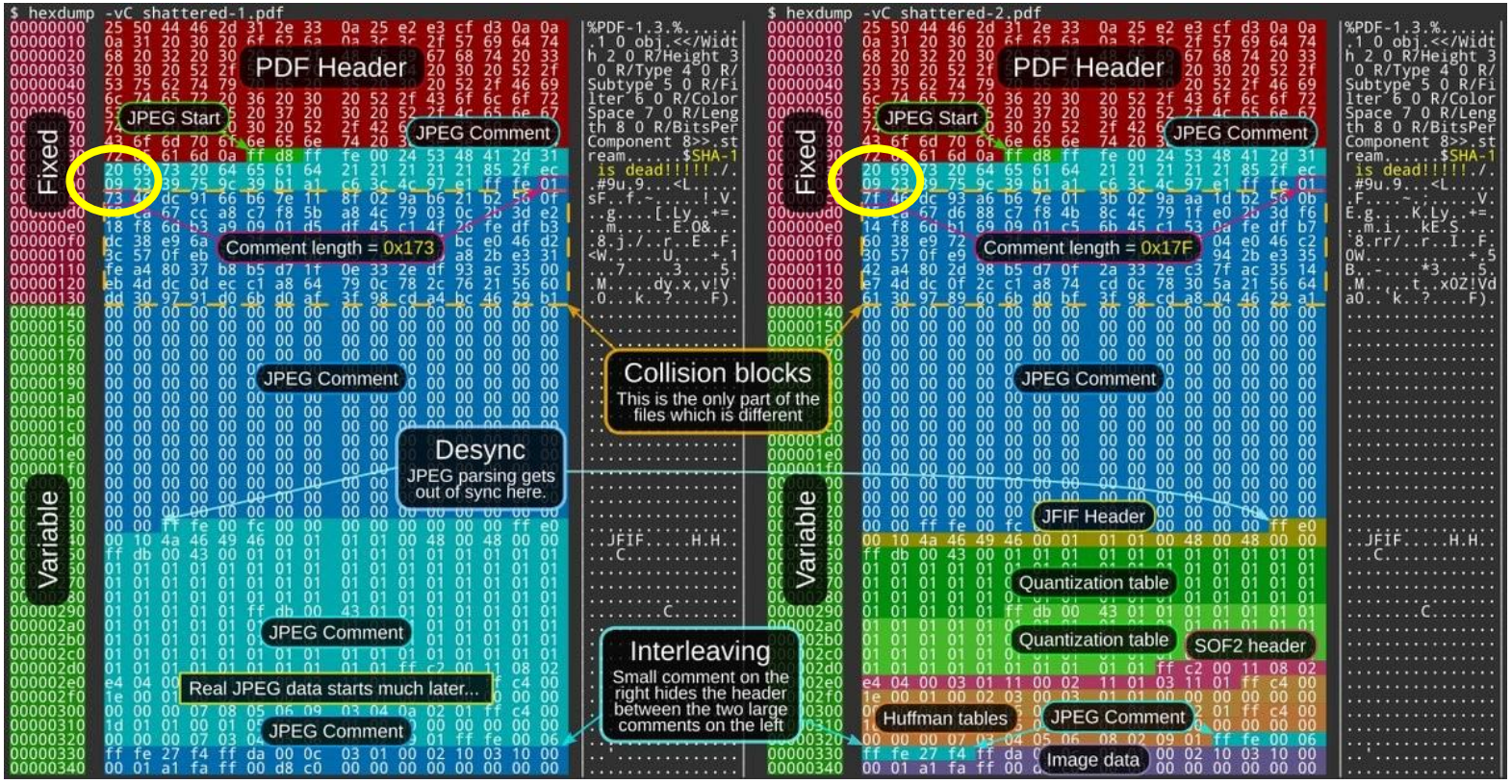
Piratages, Malwares, spam, fraudes et DDoS

Crypto

Collision SHA1

- Collision, mais pas “préimage”
- Réalisé par Google et CWI Amsterdam
- Sur un fichier créé par Ange Albertini
  - Non réutilisable pour un exécutable
  - Et contenant un IoC « SHA-1 is dead !!!!! »

https://shattered.io/



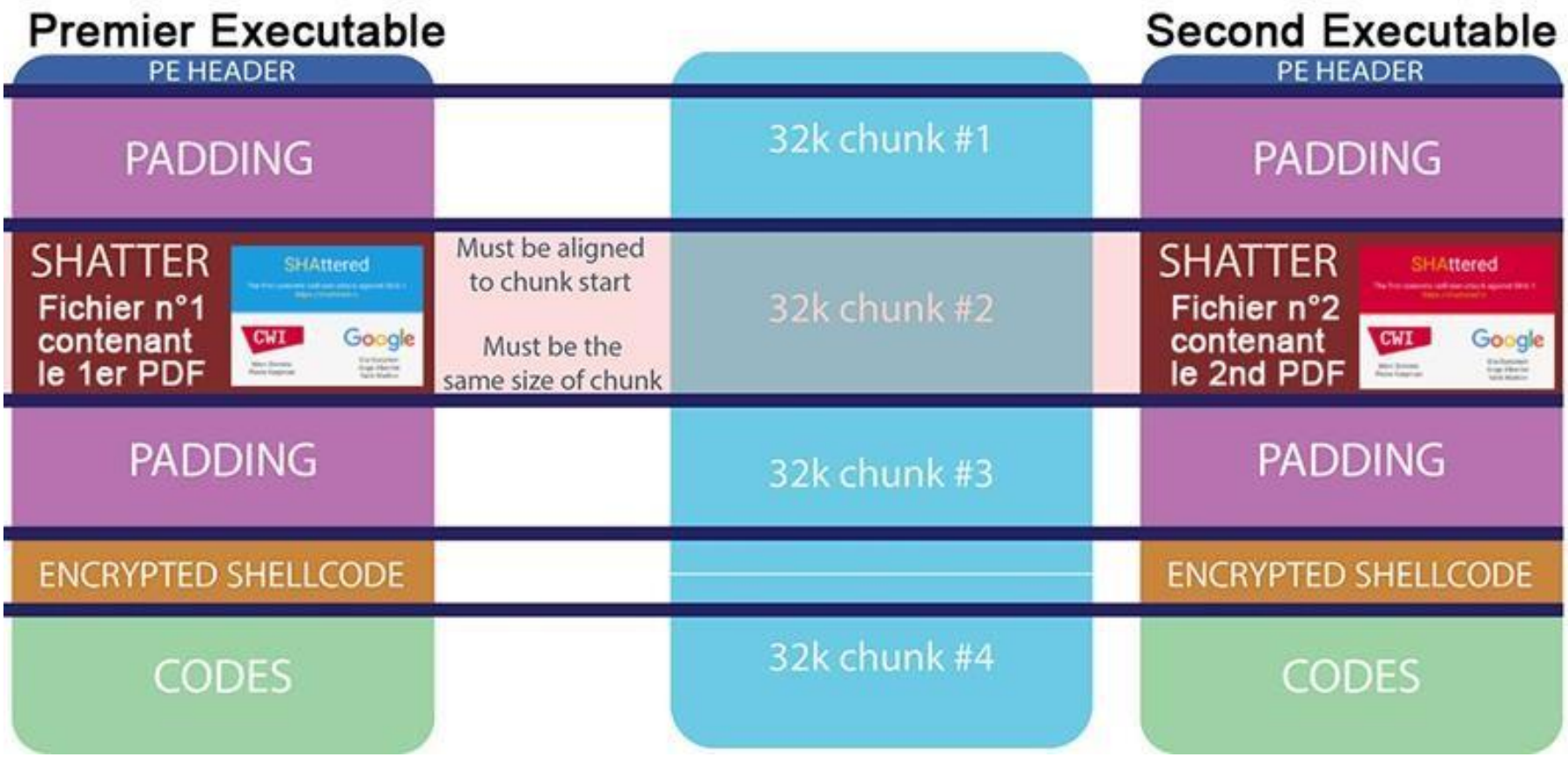
Piratages, Malwares, spam, fraudes et DDoS

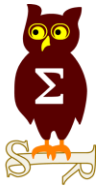
Crypto

Collision SHA1 sur BitTorent

- “Non réutilisable pour un exécutable”
- Mais… réutilisé pour backdooré un exécutable sur BitTorent

  https://biterrant.io/





Nouveautés, outils et techniques

10 ans de Tor

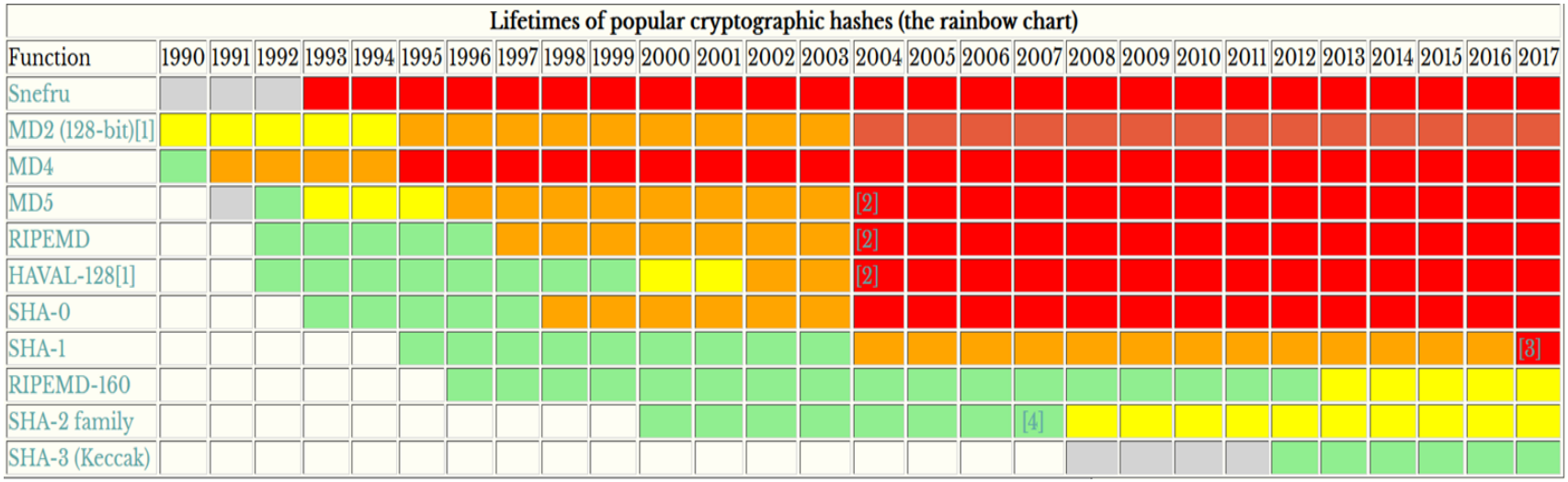
- Pour réaliser une attaque de désanonymisation des gens ont monté des relais :
  - Avec les mêmes bi-clefs
  - En changeant l'exposant RSA

https://nymity.ch/anomalous-tor-keys/

La durée de vie des algorithmes de condensat (hash)

- En moyenne, elle oscille entre 5 et 10 ans

http://valerieaurora.org/hash.html



Pentest
Techniques & outils

WMInplant, post-exploitation en Powershell

- Basé WMI pour lancer des commandes, stocker des données et le contrôle-commande
- Fonctionne avec Device Guard

https://www.slideshare.net/CTruncer/windows-10-endpoint-security-improvements-and-the-implant-since-windows-2000

https://github.com/ChrisTruncer/WMImplant

Utiliser DropBox comme Contrôle-Commande

https://truneski.github.io/blog/2017/03/03/dropbox-command-and-control-over-powershell-with-invoke-dbc2/

Usurper une session RDP

- Avec “tscon.exe” en tant que SYSTEM
- Mais c’est une “fonctionnalité”

https://medium.com/@networksecurity/rdp-hijacking-how-to-hijack-rds-and-remoteapp-sessions-transparently-to-move-through-an-da2a1e73a5f6

Attaques sur RDP

- **P**roof **o**f **C**oncept pour de l’interception réseau

https://www.exploit-db.com/docs/41621.pdf

Invoke-the-Hash

- CrackMapExec en Powershell
- Exécution de commandes via SMB et/ou WMI en fournissant un hash NTLM

https://github.com/Kevin-Robertson/Invoke-TheHash

Identifier les machines Unix intéressantes dans un domaine Windows

- Par du principe que même si les machines sont hors-domaine, elles sont souvent accédés/administrés depuis un poste de travail Windows qui l'est.
- Création de SessionGopher, un outil qui permet de chercher dans la base de registre de postes de travail des traces d'outils comme WinSCP, Putty, etc...

https://www.fireeye.com/blog/threat-research/2017/03/using_the_registryt.html

https://github.com/fireeye/SessionGopher

Mimipenguin, la version Linux de Mimikatz

- Entièrement en Bash

https://github.com/huntergregal/mimipenguin

Pentest
Techniques & outils

AllTheThings

- Un seul script pour tester 5 techniques d'évasion de restriction applicatives (AppLocker)

  https://github.com/subTee/AllTheThings

Exfiltration de données via RCE basée sur le temps

https://securitycafe.ro/2017/02/28/time-based-data-exfiltration/

KeeThief, pour voler le contenu d'un KeePass

- En PowerShell et ne nécessite pas d'être administrateur

  https://raw.githubusercontent.com/HarmJ0y/KeeThief/master/PowerShell/KeeThief.ps1

Dislocker v0.7.1

- Supporté sur macOS

  http://www.hsc.fr/ressources/outils/dislocker/

Se protéger des attaques par downgrade PowerShell

- Powershell v5 inclut de nombreuses fonctionnalités de sécurité : meilleure journalisation, interface avec l'antivirus (AMSI), sécurisation des entrées utilisateurs, etc….
- Mais un attaquant peut forcer l'utilisation de PowerShell v2 : `PowerShell –Version 2 XXXX`
- Il est possible de détecter l'utilisation de PowerShell v2 dans les journaux d'événement, ou de le bloquer via AppLocker

http://www.leeholmes.com/blog/2017/03/17/detecting-and-preventing-powershell-downgrade-attacks/

Détection d'injection inter-processus avec Windows Defender ATP

https://blogs.technet.microsoft.com/mmpc/2017/03/08/uncovering-cross-process-injection-with-windows-defender-atp/

ReverseMap, pour rechercher des tentatives de SQLi dans ses logs

- Uniquement les logs apache

https://github.com/z00nx/reversemap

Nouveautés (logiciel, langage, protocole...)
Open Source

FireEye met à disposition monitor.app

- “procmon-like” pour MacOS
- Code source fermé

https://www.fireeye.com/services/freeware/monitor.html

Générateur de trafic open source

- “reverse Wireshark”

http://ostinato.org/

Business et Politique

Droit / Politique

France

Prison avec sursis pour les lanceurs d'alerte de LuxLeak

http://www.arretsurimages.net/breves/2017-03-15/Luxleaks-peines-allegees-ou-scandaleuses-id20505

Pour échapper aux poursuites judiciaires et blocages, T411 change encore de domaine

- Et passe de https://www.t411.li à https://www.t411.ai

Macron vs la cryptographie

- <<communiquer leurs clés de chiffrement ou de donner accès au contenu>>
- Impossible technique, donc ca sent la backdoor

http://www.liberation.fr/elections-presidentielle-legislatives-2017/2017/04/10/terrorisme-macron-en-marche-contre-la-cryptographie_1561864

Droit / Politique
International

Les pirates de Yahoo, un des criminels arrêté

- 2 hackeurs et 2 membres du FSB
- Harponnage (SpearPhishing) et persistance pendant 2 ans
- But: accéder aux boîtes mails de journalistes Russes, d'employés du gouvernement américain et d'employés d'entreprises Russe de CyberSécurité

https://www.justice.gov/opa/press-release/file/948201/download

La Chine développerait du cyber-offensives contre les infrastructures militaires US

- Tout comme les américains contre le reste du monde…

https://www.thecipherbrief.com/article/asia/china-developing-cyber-capabilities-disrupt-us-military-operations-1092

L'Allemagne va monter une cyber-armée de 13'500 combattants

- D'ici l'été 2017 !!!
- Pour 260 personnes actuellement
- Contre 3 200 en France, prévu en 2018

http://www.lci.fr/international/cyberguerre-l-allemagne-se-dote-d-une-cyber-armee-de-hackers-d-elite-une-premiere-dans-l-otan-2044433.html

https://www.infosecurity-magazine.com/news/germany-considers-firststrike/

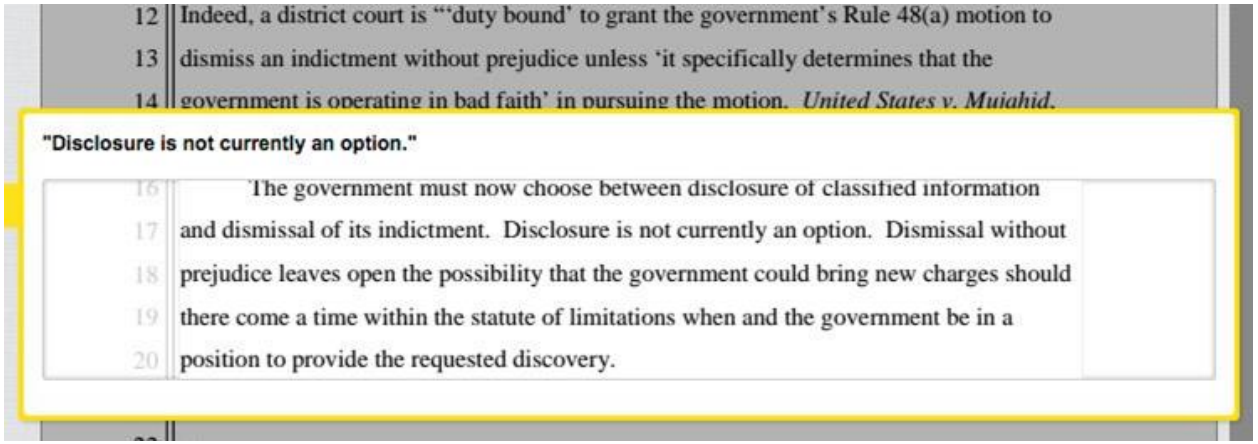
https://www.lesechos.fr/monde/europe/0211960690781-lallemagne-investit-lourdement-dans-la-cyberdefense-2078959.php

Droit / Politique
International

Arrêter des Pédophiles vs Conserver une faille, le FBI a choisi

- Le FBI préfère abandonner des poursuites contre un pédophile
- Plutôt que de révéler une faille dans TOR

https://arstechnica.com/tech-policy/2017/03/doj-drops-case-against-child-porn-suspect-rather-than-disclose-fbi-hack/



L'Europe veut que sa police accès aux données chiffrées

- Ca sent la backdoor...

http://www.euractiv.com/section/data-protection/news/eu-to-propose-new-rules-on-police-access-to-encrypted-data-in-june/

Droit / Politique
International

Procès contre des Vibromasseurs connectés

- Gagné par les plaignantes
- Suite à une présentation à la Defcon

http://www.numerama.com/politique/240568-objets-connectes-les-victimes-dun-vibromasseur-espion-remportent-leur-proces.html

Aux USA, les opérateurs peuvent vendre l'historique de navigation pour de la publicité

- Vote du Sénat à 50 contre 48

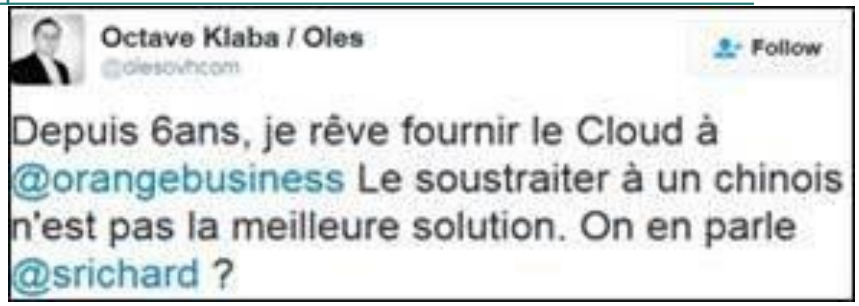
https://arstechnica.com/tech-policy/2017/03/senate-votes-to-let-isps-sell-your-web-browsing-history-to-advertisers/

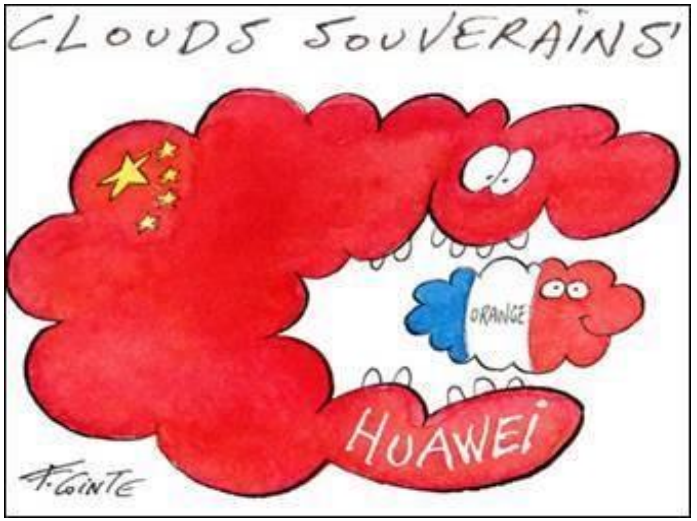
Business
France

Orange s'associe à Huawei pour monter son Cloud mondial de 2020

- Orange n'apporte que les datacenters et le réseau
- Huawei fournira l'infrastructure et OpenStack
- C'est sur qu'il n'y avait personne d'autre…

https://twitter.com/olesovhcom/status/819073311212797953





- Et cela ne plaît pas à nos espions

Les "chinoiseries" d'Orange affolent nos espions

L'opérateur fait-il entrer le loup dans la bergerie ?

La réunion ultra-secrète s'est tenue à l'Elysée quelques jours avant Noël. Autour de la table, rien que du beau monde, *habilité « secret-défense »* : une dizaine de hauts fonctionnaires représentant la DGSE, la DGSI, le coordinateur national du Renseignement, le secrétariat général de la Défense, mais aussi Bercy. Au menu ? Le fort intérêt que les Chinois portent à Orange.

Depuis plusieurs mois, la DGSE soupçonne les espions de l'empire du Milieu d'avoir mis en fiches l'équipe dirigeante d'Orange, à commencer par son pédégé, Stéphane Richard. Un travail à l'ancienne, digne du KGB d'antan, avec recherche des points de vulnérabilité et collecte d'infos sur les secrétaires et les chauffeurs… Pourquoi se gêner ?

nées sensibles donne des sueurs froides aux services. D'où la réunion du 21 décembre, officiellement consacrée au cloud « souverain ». Le Château rêve d'imposer un nuage bleu-blanc-rouge, avec des *data centers* implantés sur le sol national. Cocorico !

La main sur le cœur, Huawei jure ne rien avoir à faire avec les espions chinois. Sauf que personne n'y croit. Sans doute parce que l'entreprise a été créée par un ex-colonel de l'armée chinoise. Abreuvée de contrats militaires par Pékin, elle est devenue une multinationale high-tech, employant 170 000 salariés pour un chiffre d'affaires annuel de 72 milliards d'euros. Jean-Louis Borloo, qui vient d'entrer au conseil d'administration de la firme chinoise, a sans doute son avis sur la question.

My Chinois is clean

Chez Orange, on ne voit pas où est le problème, et on promet que l'alliance avec Huawei ne concernera que les *« services de cloud public »*, et pas les données sensibles. Tout en prévenant, sous le couvert de l'anonymat : *« En autorisant Free comme quatrième opérateur, l'Etat a déclenché une guerre des prix. Si on veut rester compétitifs sans avoir à licencier, il faut bien qu'on noue des alliances avec les acteurs les moins chers du marché, comme Huawei. »* Oh ! le joli chantage à l'emploi… Nos espions, eux, considèrent que Hollande est trop mou du genou. Et citent l'exemple de leurs collègues d'outre-Manche.

Pour avoir le droit de travailler sur le sol anglais, Huawei a dû accepter que ses produits soient passés au peigne fin par une quarantaine de techniciens détachés du GCHQ – les grandes oreilles britanniques. *« Ils vérifient notamment qu'il n'y a pas de porte dérobée installée en douce par laquelle pourraient s'échapper des infos sensibles, tout en récupérant au passage des renseignements sur la technologie chinoise »*, s'émerveille une barbouze. Sans compter que ces opérations de contrôle sont facturées… à Huawei.

La perfide Albion a résolu le casse-tête chinois.

C. L. et D. H.

Business
International

Augmentation des BugBounty de Microsoft et Google

- Chez Google, la plus grosse prime passe de $20,000 à $31,337

  https://www.google.com/about/appsecurity/reward-program/

- Chez Microsoft, la plus grosse prime passe de $20,000 à $30,000

  https://technet.microsoft.com/en-us/dn800983.aspx

Conférences

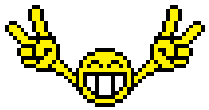
Conférences

Passées

- CORI&IN - 23 janvier 2017 à Lille
- FIC - 24-25 janvier 2017 à Lille
- JSSI - 14 mars 2017 à Paris
- Troopers - 12-14 mars 2017 à Heidelberg
- BlackHat Asia - 28-29 mars 2017 à Singapour

A venir

- Meetup Univershell - 26 avril 2017 à Paris *(chez Vente Privée)*
  https://www.eventbrite.fr/e/billets-meet-up-securite-univershell-sthack-33561859425
- Nuit du Hack - 24-25 juin 2017 à Paris *(à Eurodisney)*
- SSTIC - 7 au 9 juin 2017 à Rennes
  - Avec une nouvelle salle de 600 places



Divers / Trolls velus

Divers / Trolls velus

La cybersécurité Française

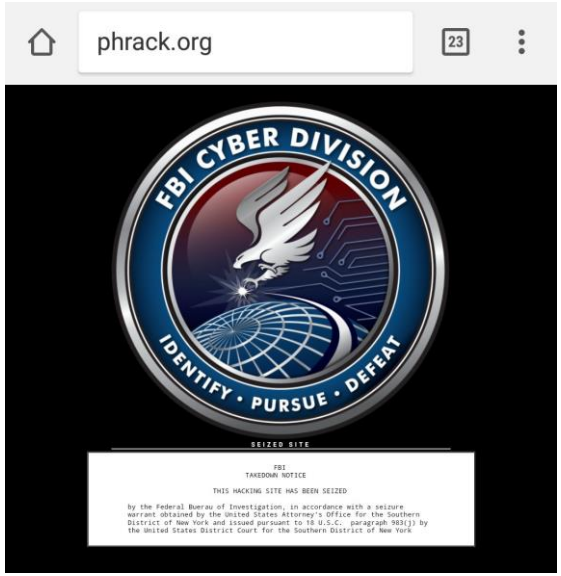
- Mais qui sont ces gens ? Les représentants de la cybersécurité Française !!?
  http://izibook.eyrolles.com/produit/4661/9782212158625/Lessentiel%20de%20la%20securite%20numerique%20pour%20les%20dirigeants?search_text=s%C3%A9curit%C3%A9

Divers / Trolls velus

Le site de l'ezine Phrack bloqué par le FBI

- Joyeux 1er avril

  http://phrack.org/



Quand tu fais un poisson d'avril…

- et que c'est repris (et cru?) dans des veilles, dont celle de l'ARCSI

  https://cybercriminalite.wordpress.com/2017/04/05/securite-predictive/

Une blockchain formellement vérifiable implémentée en OCaml

- On dirait un titre de poisson d'avril

  https://tezos.com/index.html

Divers / Trolls velus

Pwn2Own

- 51 bugs et $833,000 distribués
- Chaînage de vulnérabilités épique par Qihoo 360 Security :
  1. Exploit Javascript EDGE et sortie de la SandBox
  2. Exploit Kernel Windows 10
  3. Exploitation d'une vulnérabilité VMWare permettant une évasion de la VM et une exécution de code sur l'hyperviseur
- La vulnérabilité VMware touche tous les produits
  - Voici une aide pour choisir ses correctifs : https://esxi-patches.v-front.de/vm-Help.html

http://blog.trendmicro.com/results-pwn2own-2017-day-one/

http://blog.trendmicro.com/pwn2own-2017-day-two-schedule-results/

http://blog.trendmicro.com/pwn2own-2017-day-three-schedule-results/

Divers / Trolls velus

S’échapper d’une discussion en faisant sonner son téléphone

- Via le click sur un bouton du navigateur

  http://nopebutton.com/?ref=producthunt

Nintendo DSi

- Le vecteur d’initialisation de l’AES est “**Nintendo Co., Ltd.**” en japonais : **任天堂株式会社**

  https://twitter.com/marcan42/status/847849898879762432?refsrc=email&s=11

Les agriculteurs américain hackent leur tracteur avec des firmwares Ukrainiens

- Le constructeur (John Deere) interdit les réparations “non autorisées”
- Seuls les réparateurs agréés peuvent les réparer, à des prix prohibitifs

  https://motherboard.vice.com/en_us/article/why-american-farmers-are-hacking-their-tractors-with-ukrainian-firmware

Des préservatifs connectés

- Pour mesurer ses performances !!?

  https://www.cnet.com/news/icon-smart-condom-ring/?ftag=COS-05-10aaa0b&linkId=35064659

Prochains rendez-vous de l’OSSIR

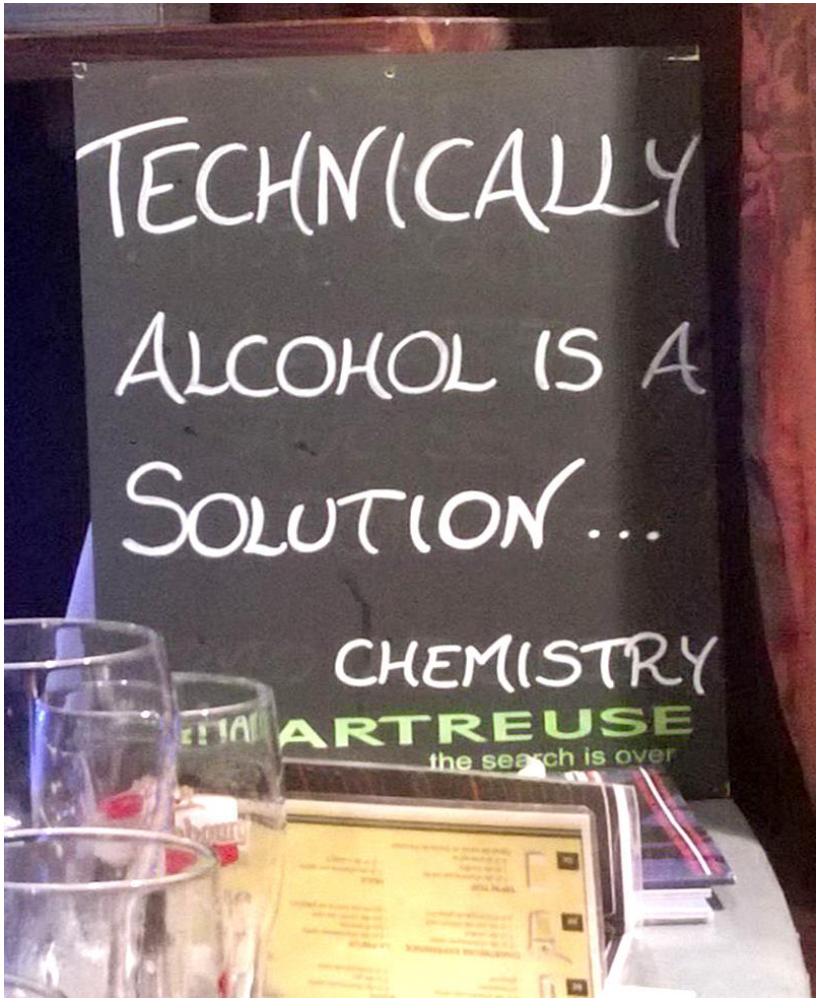
Prochaines réunions

Prochaine réunion

- Mardi 9 mai 2017

After Work

- Mardi 25 mars 2017



Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous