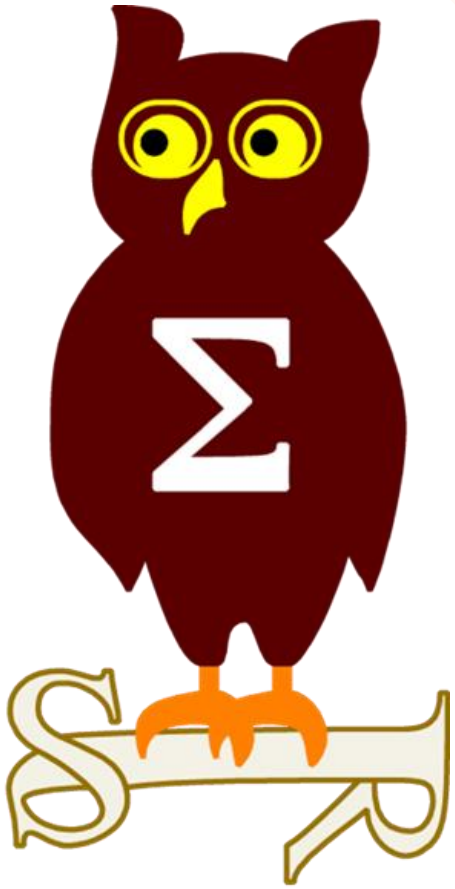


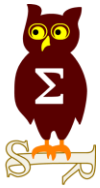
Revue d'actualité

13/09/2016

Préparée par

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


Actualité trèèèèès chargées
70 slides



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-084 Vulnérabilités dans Internet Explorer (15 CVE) [Exploitabilité 1,1,1,1,1,3,1,1,1,2,3,2,2,1]

- Affecte:
  - Windows (toutes versions supportées), remplace MS16-063, KB3160005, KB3163017, KB3163018
- Exploit:
  - 9 x Corruptions de mémoire aboutissant à une exécution de code
  - 1 x Contournement du filtrage anti XSS
  - 3 x Contournement ASLR (fuite d'information)
  - 2 x Usurpation de site web
- Crédits:
  - 62600BCA031B9EB5CB4A74ADDDD6771E par ZDI de Trend Micro (CVE-2016-3241, CVE-2016-3242)
  - Henry Li (zenhumany) de Trend Micro (CVE-2016-3277)
  - Hui Gao de Palo Alto Networks (CVE-2016-3240)
  - Jaehun Jeong (nesk), Individual (CVE-2016-3259)
  - Jordan Rabet de Microsoft Offensive Security Research Team (CVE-2016-3260)
  - Li Kemeng, Baidu Security Lab (CVE-2016-3261)
  - Masato Kinugawa de Cure53 (CVE-2016-3245, CVE-2016-3273)
  - Tao Yan (@Ga1ois) de Palo Alto Networks (CVE-2016-3275)
  - Zheng Huang de Baidu Security Lab (CVE-2016-3243)
  - exp-sky de Tencent's Xuanwu LAB par ZDI (CVE-2016-3264)

MS16-068 Vulnérabilités dans Edge (13 CVE) [Exploitabilité 2,1,2,1,1,1,1,1,2,3,2,2,1]

- Affecte:
  - Windows 10
- Exploit:
  - 9 x Corruptions de mémoire aboutissant à une exécution de code
  - 1 x Contournement du filtrage anti XSS
  - 1 x Contournement ASLR (fuite d'information)
  - 2 x Usurpation de site web
- Crédits:
  - Ferenc Lutischán de Magyar Telekom Nyrt (CVE-2016-3274)
  - Henry Li (zenhumany) de Trend Micro (CVE-2016-3244, CVE-2016-3277)
  - Jaehun Jeong (nesk), Individual (CVE-2016-3259)
  - Jordan Rabet, Microsoft Offensive Security Research Team (CVE-2016-3265, CVE-2016-3269)
  - Kai Song (exp-sky) de Tencent's Xuanwu LAB (CVE-2016-3244)
  - Masato Kinugawa de Cure53 (CVE-2016-3273)
  - Microsoft ChakraCore Team (CVE-2016-3248)
  - WanderingGlitch par ZDI de Trend Micro (CVE-2016-3271)
  - Wenxiang Qian de Tencent QQBrowser http://browser.qq.com (CVE-2016-3276)
  - Zheng Huang de Baidu Security Lab (CVE-2016-3244)
  - cc par ZDI de Trend Micro (CVE-2016-3246)
  - exp-sky de Tencent's Xuanwu LAB par ZDI de Trend Micro (CVE-2016-3264)

Dont 8 communes avec IE:

- CVE-2016-3248
- CVE-2016-3259
- CVE-2016-3260
- CVE-2016-3264
- CVE-2016-3273
- CVE-2016-3274
- CVE-2016-3276
- CVE-2016-3277

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-086 Vulnérabilités dans JScript et VBScript (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportées)
  - Remplace MS16-069, KB3158363, KB3158364
- Exploit:
  - Corruptions de mémoire dans un script VBScript aboutissant à une exécution de code
- Crédits:
  - ?

MS16-087 Vulnérabilités dans le Spouleur d'Impression (2 CVE) [Exploitabilité 2,2]

- Affecte:
  - Windows (toutes versions supportées)
  - Remplace MS12-054, MS13-050, KB2712808, KB2839894, KB3163017, KB3163018
- Exploit:
  - Exécution de code et contournement de l'UAC depuis le Spouleur d'Impression (Fonction PSetupDownloadAndInstallLegacyDriver de ntprint.dll)
    http://blog.vectranetworks.com/blog/microsoft-windows-printer-wateringhole-attack
- Crédits:
  - Nicolas Beauchesne de Vectra Networks (CVE-2016-3238)
  - Shanti Lindström, Individual (CVE-2016-3239)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-088 Vulnérabilités dans Office (7 CVE) [Exploitabilité 3,2,2,1,2,1,2]

- 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
  - Contournement du mode protégé désactivant les macro, avec les fichiers XLA
    https://blogs.mcafee.com/mcafee-labs/patch-now-simple-office-protected-view-bypass-could-have-big-impact/
- Crédits:
  - Alexey Belyakov, Individual (CVE-2016-3284)
  - Haifei Li, Individual (CVE-2016-3279)
  - Jaanus Kääp de Clarified Security (CVE-2016-3281, CVE-2016-3282, CVE-2016-3283)
  - Lucas Leong de Trend Micro (CVE-2016-3280)
  - Xiaoning Li de Intel Labs (CVE-2016-3278)

MS16-089 Vulnérabilités noyau Win32k (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows 10
  - Remplace KB3163017, KB3163018
- Exploit:
  - Contournement ASLR (fuite d'information)
- Crédits:
  - ?

MS16-090 Vulnérabilités pilotes noyau (6 CVE) [Exploitabilité 1,3,2,1,1,1]

- Affecte:
  - Windows (toutes versions supportées)
  - Remplace MS16-073, KB3156387, KB3156421, KB3161664
- Exploit:
  - 5 x Élévations de privilège locale
  - 1 x Contournement KASLR (fuite d'information)
- Crédits:
  - bee13oy de CloverSec Labs (CVE-2016-3249)
  - fanxiaocao (@TinySec), et pjf de IceSword Lab, Qihoo 360 (CVE-2016-3252)
  - zhong_sf et pgboy de Qihoo 360 Vulcan Team (CVE-2016-3250, CVE-2016-3251, CVE-2016-3254, CVE-2016-3286)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-091 Vulnérabilités dans .NET (1 CVE) [Exploitabilité 2]

- Affecte:
  - .Net 2.0, 3.5.1, 4.5.2, 4.6, 4.6.1
- Exploit:
  - Fuite d'information lors du traitement de XML uploadés (XXE)
- Crédits:
  - Michael Weber, Henrique ArcoverdeNCC Group (CVE-2016-3255)

MS16-092 Vulnérabilités noyau Win32k (2 CVE) [Exploitabilité 2,2]

- Affecte:
  - Windows 8.1, 8.1RT, 10, 2012, 2012 R2
  - Remplace MS16-060, KB3153171, KB3163017, KB3163018
- Exploit:
  - Acces à des fichiers sensibles depuis un processus en "intégrité basse" (Low Integrity)
  - Fuite d'information
- Crédits:
  - Herbert Bos de Vrije Universiteit Amsterdam (CVE-2016-3272)
  - James Forshaw de Google Project Zero (CVE-2016-3258)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-093 Vulnérabilité dans Adobe Flash Payer (24 CVE) [Exploitabilité 1]

- Affecte:
  - Windows 8.1, 10, 2012, 2012R2
- Exploit:
  - Exécutions de code
- Crédits:
  - ?

MS16-094 Contournement de Secure Boot (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows 8.1, 10, 2012, 2012R2
  - Remplace KB3163017, KB3163018
- Exploit:
  - Contournement de Secure Boot
    - Politique UEFI "supplemental" permettant de contourner les signatures (debug) non liée à un équipement spécifique
    - Permet de "Jailbreaker" les terminaux bloqués

    https://rol.im/securegoldenkeyboot/
  - Le correctif inclue une liste noire de condensat SHA256 de politiques vulnérables
    - Mais la vérification se fait "après" le chargement des politiques
  - Secure Boot cassé ?
- Crédits:
  - Les vrais auteurs ne sont pas crédités !!! 😱

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-095 Vulnérabilités dans Internet Explorer (9 CVE) [Exploitabilité 1,1,1,1,1,1,2,2,3]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - 5 x Corruptions de mémoire aboutissant à une exécution de code
  - 4 x Contournement ASLR (fuite d'information)
- Crédits:
  - Ivan Fratric et Martin Barbella par Google Project Zero (CVE-2016-3288)
  - Kai Song (exp-sky) de Tencent's Xuanwu LAB (CVE-2016-3293)
  - Liu Long de Qihoo 360 (CVE-2016-3290)
  - Simon Zuckerbraun par ZDI de Trend Micro (CVE-2016-3326)
  - Soroush Dalili de NCC Group (CVE-2016-3327)
  - Yorick Koster de Securify B.V. (CVE-2016-3321)
  - Zheng Huang de Baidu Security Lab par ZDI de Trend Micro (CVE-2016-3289, CVE-2016-3322)

MS16-096 Vulnérabilités dans Edge (8 CVE) [Exploitabilité 1,1,1,2,1,2,2,3]

- Affecte:
  - Windows 10, remplace KB3163017, KB3163018
- Exploit:
  - 4 x Corruptions de mémoire aboutissant à une exécution de code
  - 3 x Contournement ASLR (fuite d'information)
  - 1 x Corruptions de mémoire du lecteur PDF aboutissant à une exécution de code
- Crédits:
  - Aleksandar Nikolic de Cisco Talos (CVE-2016-3319)
  - Kai Song (exp-sky) de Tencent's Xuanwu LAB (CVE-2016-3293)
  - Microsoft ChakraCore Team (CVE-2016-3296)
  - Simon Zuckerbraun par ZDI de Trend Micro (CVE-2016-3326)
  - Soroush Dalili de NCC Group (CVE-2016-3327)
  - Zheng Huang de Baidu Security Lab par ZDI de Trend Micro (CVE-2016-3289, CVE-2016-3322)

Dont 6 communes avec IE:

- CVE-2016-3289
- CVE-2016-3293
- CVE-2016-3322
- CVE-2016-3326
- CVE-2016-3327
- CVE-2016-3329

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-097 Vulnérabilités dans GDI (3 CVE) [Exploitabilité 1,1,1]

- Affecte:
  - Windows (toutes versions supportées), Office 2007, 2010, Skype 2016, Lync 2010, 2013
  - Remplace MS14-036, MS15-097, KB316912, KB2957503, KB3087135, KB3172985
- Exploit:
  - 3 x exécutions de code dans Office, Lync et Skype lors du traitement de polices de caractères
- Crédits:
  - Mateusz Jurczyk de Google Project Zero (CVE-2016-3301, CVE-2016-3303, CVE-2016-3304)

MS16-098 Vulnérabilités noyau Win32k (4 CVE) [Exploitabilité 1,1,1,1]

- Affecte:
  - Windows (toutes versions supportées)
  - Remplace MS16-090, KB3163912, KB3168965, KB3172985
- Exploit:
  - Elévations de privilèges (Win32k!bEndDocInternal, GreValidateVisRgn…)
    https://blog.fortinet.com/2016/08/17/root-cause-analysis-of-windows-kernel-uaf-vulnerability-lead-to-cve-2016-3310
- Crédits:
  - Martin Lenord (----------)
  - Peter (Keen) et ZeguangZhao (team509) par ZDI de Trend Micro (CVE-2016-3308)
  - Wayne Low de Fortinet’s Fortiguard Labs (CVE-2016-3310)
  - bee13oy de CloverSec Labs par ZDI de Trend Micro (CVE-2016-3309)
  - pgboy, zhong_sf de Qihoo 360 Vulcan Team (CVE-2016-3311)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-099 Vulnérabilités dans Office (5 CVE) [Exploitabilité 2,3,1,1,1]

- 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
    - Preuve de concept : https://smsecurity.net/microsoft-office-word-out-of-bounds-read-remote-code-execution-cve-2016-3313/
- Crédits:
  - Arun Kumar Sharma par ZDI de Trend Micro (CVE-2016-3318)
  - Dhanesh Kizhakkinan de FireEye Inc (CVE-2016-3317)
  - Francis Provencher de COSIG (CVE-2016-3316)
  - Jaanus Kaap (CVE-2016-3313)
  - Jerry Decime de Hewlett Packard Enterprise (----------)
  - Sébastien Morin de COSIG (CVE-2016-3313)
  - Udi Yavo de enSilo Inc (CVE-2016-0137)
  - dannywei de Tencent's Xuanwu Lab (CVE-2016-3315)

MS16-100 Contournement de Secure Boot (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows 8.1, 8.1RT, 10, 2012, 2012 R2
- Exploit:
  - Cf. MS16-094
    https://rol.im/securegoldenkeyboot/
- Crédits:
  - Les vrais auteurs ne sont toujours pas crédités !!?

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-101 Vulnérabilité Kerberos (2 CVE) [Exploitabilité 2,2]

- Affecte:
  - Windows (toutes versions supportées)
  - La suite de MS15-071, MS15-122 et MS16-014
- Exploit:
  - Contournement de l'authentification en bloquant les flux Kerberos ;-)
    - Après 6 minutes Windows passe alors en NTLM
    - MS15-122 et MS16-014 corrigé pour Kerberos mais pas NTLM

    https://blog.ahmednabeel.com/abusing-kerberos-to-ntlm-fallback-to-defeat-windows-authentication/
    - Ajout de nouvelles API : KerbILogonUserEx2 et KerbFreeSecpkgPrimaryCredentials
  - Elévation de privilège depuis NetLogon
- Crédits:
  - Nabeel Ahmed de Dimension Data (CVE-2016-3237)

MS16-102 Vulnérabilités dans la librairie PDF (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows 8.1, 10, 2012, 2012R2
  - Remplace KB3163912, KB3172985
- Exploit:
  - Exécutions de code lors du traitement d'un fichier PDF spécialement formatée
- Crédits:
  - Aleksandar Nikolic de Cisco Talos (CVE-2016-3319)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-103 Vulnérabilité dans ActiveSyncProvider (1 CVE) [Exploitabilité 3]

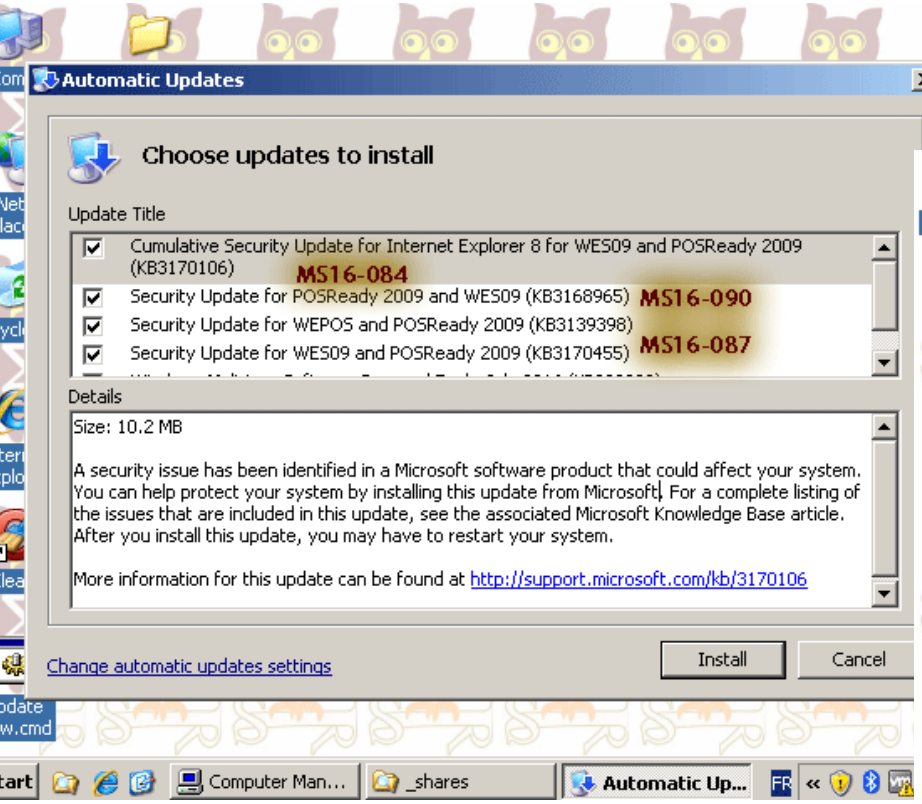
- Affecte:
  - Windows 10 (Universal Outlook)
  - Remplace KB3163912, KB3172985
- Exploit:
  - Récupération de l'identifiant et du mot de passe si SSL/TLS échoue
- Crédits:
  - ?

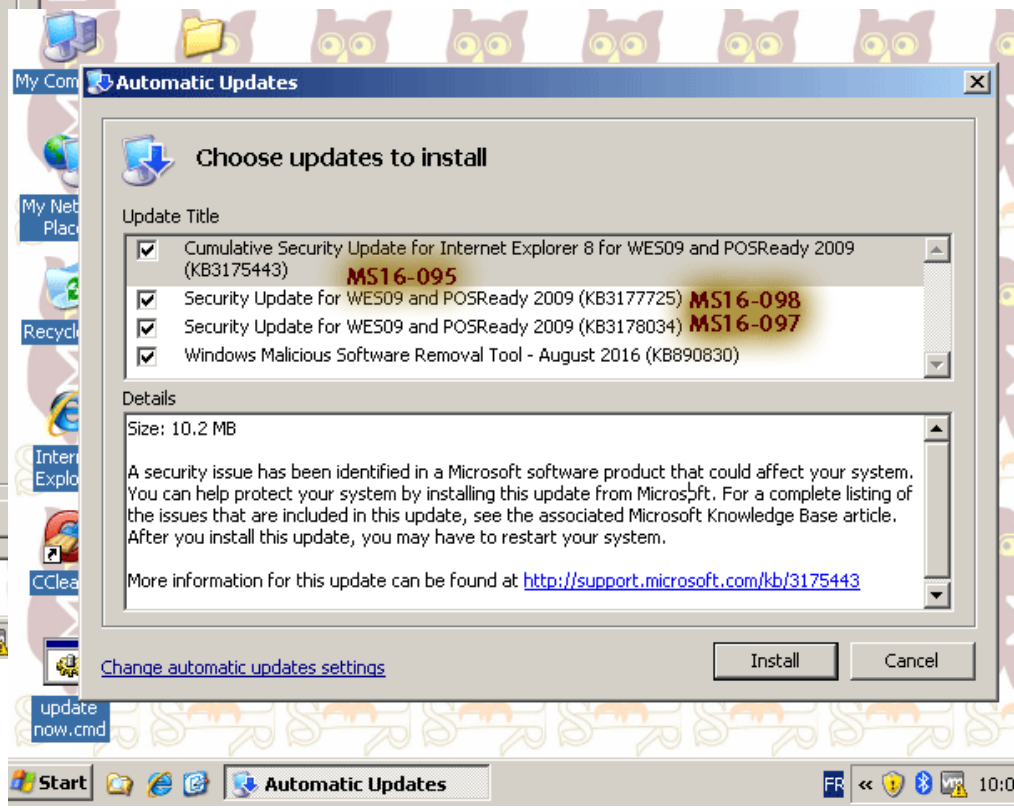
Failles / Bulletins / Advisories

Microsoft - Avis

Mise à jour pour Windows XP Embedded POSReady

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





Failles / Bulletins / Advisories

Microsoft - Advisories et Revisions

3179528 Mise à jour de la liste noire de secure kernel

- V1.0 création et premiers condensats (hash) des securekernel.exe vulnérables (MS16-089)

Failles / Bulletins / Advisories

Microsoft - Autre

Windows 7, 8 et 10, nouveaux contournements de l'UAC

- Avec :
  - TpmInit

    https://github.com/Cn33liz/TpmInitUACBypass
  - La tâche planifiée Disk Cleanup

    https://enigma0x3.net/2016/07/22/bypassing-uac-on-windows-10-using-disk-cleanup/
  - CompMgmtLauncher.exe

    https://github.com/mrfuzzy8/Scripts/blob/master/Invoke-CompMgmtLauncherBypass.ps1
  - Get Windows 10 / GWX 😱

    https://twitter.com/mynameisv_/status/765925639782338560
  - Eventvwr.exe et **sans fichier** 😍

    https://enigma0x3.net/2016/08/15/fileless-uac-bypass-using-eventvwr-exe-and-registry-hijacking/
  - En abusant de l'environnement d'un processus fils 😂

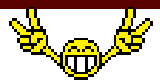
    http://breakingmalware.com/vulnerabilities/elastic-boundaries-elevating-privileges-by-environment-variables-expansion/
- Parmi les réglages de l'UAC, seul "Always Notify" est efficace

  https://blogs.msdn.microsoft.com/oldnewthing/20160816-00/?p=94105
- Mais UAC n'est pas une fonctionnalité de sécurité

Failles / Bulletins / Advisories

Microsoft - Autre

Windows 10 : la CNIL met en demeure Microsoft



- 3 mois pour se conformer à la loi Informatique et Libertés
- Principaux problèmes:
  - Données collectées non pertinentes ou excessives
  - Pas de consentement de l'utilisateur face à l'identifiant publicitaire
  - Code pin de 4 chiffres considéré comme un défaut de sécurité
  - Transfert des données personnelles aux USA sur la base du Safe Harbor

https://www.cnil.fr/fr/windows-10-la-cnil-met-publiquement-en-demeure-microsoft-corporation-de-se-conformer-dans-un-delai

On ne choisit plus ses patchs !

- Les patchs seront cumulatifs : impossible d'installer le patch n si vous n'avez pas le n-1
- Dès le mois prochain

https://blogs.technet.microsoft.com/windowsitpro/2016/08/15/further-simplifying-servicing-model-for-windows-7-and-windows-8-1/

Attaques RMS

- Possibilité de supprimer la protection d'un document
- Modification d'un document en lecture seule

https://github.com/RUB-NDS/MS-RMS-Attacks

Windows 10 : plus de VLAN ni de teaming

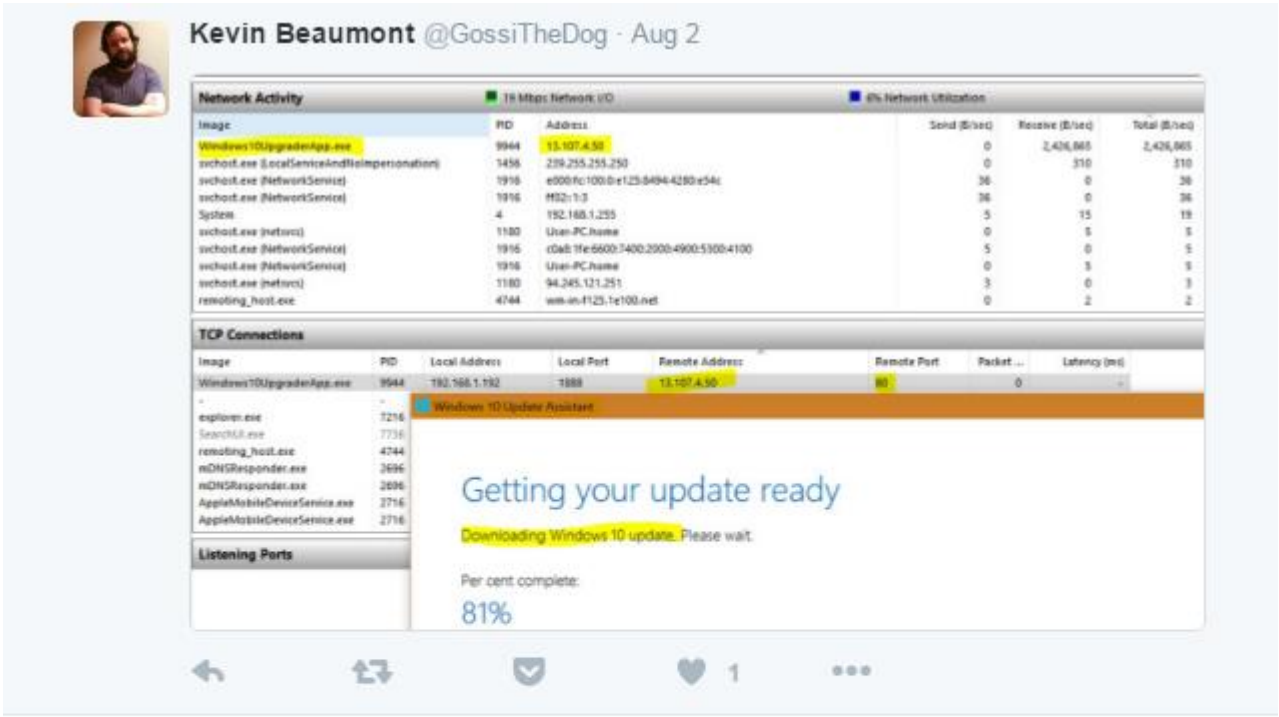
http://www.cpchardware.com/vlan-teaming-et-lavenir-de-windows/

Failles / Bulletins / Advisories

Microsoft - Autre

Le processus de migration Windows 10 discutable

- Info non vérifiée



Failles / Bulletins / Advisories

Antivirus

McAfee, Contourner les listes blanches et Application Control

- Du grand classique : PowerShell, Macro, Java...
  http://www.sicherheitsforschung-magdeburg.de/uploads/journal/MJS_046_Freingruber_McAfee.pdf

Failles / Bulletins / Advisories

Système (principales failles)

Enumération des comptes SSH (par brute force)

- Si un utilisateur existe, un condensat (hash) SHA2-256 (ou SHA2-512) est réalisé
- S'il n'existe pas, c'est BlowFish qui est utilisé
- Les deux ne sont pas en temps constant

http://seclists.org/fulldisclosure/2016/Jul/51

Drupal, exécution de code non-authentifié

- Sur le module API REST (RESTful Web Services)
- Sur le module Coders, qui vérifie la conformité du code Drupal
- Sur le module Webform Multiple File Upload
  - Encode de la désérialisation et appel à __wakeup() ou autre méthode personnalisée

https://www.drupal.org/psa-2016-001

Lib UPnP, lecture et écriture arbitraire à distance

- Une simple requête HTTP POST ou GET permet d'écrire et de lire sur le disque

https://github.com/mjg59/pupnp-code/commit/be0a01bdb83395d9f3a5ea09c1308a4f1a972cbd

- Plus de 8 mois pour corriger

https://twitter.com/mjg59/status/755062278513319936

Failles / Bulletins / Advisories

Système (principales failles)

TrueCrypt, cassage du "plausible deniability"

- Possibilité de détecter la présence d'un container caché
- Corrigé dans VeraCrypt 1.18

  https://sourceforge.net/p/veracrypt/discussion/technical/thread/b0fb9daa/?limit=25&page=2#364a
- Fortes présomption d'interceptions de mails

https://ostif.org/ostif-quarklab-and-veracrypt-e-mails-are-being-intercepted/

Httpoxy, écrasement de la variable HTTP_PROXY

- Un nom
- Un logo vectoriel en SVG 
- Un site web https://httpoxy.org/

Host of Troubles

- Empoisonnement du cache HTTP et contournement des politiques de sécurité
  - Apache, Nginx, CDN, Squid, Firewall next-gen, WAF...

  https://hostoftroubles.com/

  http://www.icir.org/vern/papers/host-of-troubles.ccs16.pdf

Failles / Bulletins / Advisories

Système (principales failles)

Microsoft Hyper-V, évasion d'une machine virtuelle

- A partir du protocole propriétaire de Microsoft RNDIS, virtualisant de l'Ethernet

  https://bugs.chromium.org/p/project-zero/issues/detail?id=688

Microsoft Live (signout.live.com), exécution de code

- Contournement de la liste noire filtrant les accès avec un "?"
  - A cause de l'utilisation du CMS : Adobe Experience Manager / AEM (CVE-2016-0957)
  - live.com utilise donc un CMS Adobe et du Java !!!
- Compte par défaut **admin / admin**
  - Accès à la console JMX d'Adobe CQ
  - Upload d'un objet Java (OSGi)
  - Exécution de code !

http://www.kernelpicnic.net/2016/07/24/Microsoft-signout.live.com-Remote-Code-Execution-Write-Up.html

Microsoft Azure, évasion de la sandbox

https://pen-testing.sans.org/blog/2016/08/19/azure-0day-cross-site-scripting-with-sandbox-escape

Failles / Bulletins / Advisories

Système (principales failles)

MySQL, écriture sur le disque et exécution de code à distance

- Ecriture à partir des fonctions de log

  http://legalhackers.com/advisories/MySQL-Exploit-Remote-Root-Code-Execution-Privesc-CVE-2016-6662.html

Evasion de VM dans XEN

- Démonstration avec QubesOS

  http://blog.quarkslab.com/xen-exploitation-part-3-xsa-182-qubes-escape.html

- Il y'a vraiment régulièrement des vulnérabilités critiques

  http://xenbits.xen.org/xsa/

Advisories, publicly released or pre-released

All times are in UTC. For general information about Xen and security see the Xen Project website and security policy.

Advisory	Public release	Updated	Version	CVE(s)	Title
XSA-188	2016-09-08 12:00	2016-09-08 12:00	3	CVE-2016-7154	use after free in FIFO event channel code
XSA-187	2016-09-08 12:00	2016-09-08 12:04	3	CVE-2016-7094	x86 HVM: Overflow of sh_ctxt->seg_reg[]
XSA-186	2016-09-08 12:00	2016-09-08 12:00	4	CVE-2016-7093	x86: Mishandling of instruction pointer truncation during emulation
XSA-185	2016-09-08 12:00	2016-09-08 12:00	3	CVE-2016-7092	x86: Disallow L3 recursive pagetable for 32-bit PV guests
XSA-184	2016-07-27 15:00	2016-07-27 16:06	2	CVE-2016-5403	virtio: unbounded memory allocation issue
XSA-183	2016-07-26 11:32	2016-07-26 11:32	5	CVE-2016-6259	x86: Missing SMAP whitelisting in 32-bit exception / event delivery
XSA-182	2016-07-26 11:32	2016-07-26 11:32	3	CVE-2016-6258	x86: Privilege escalation in PV guests
XSA-181	2016-06-03 09:47	2016-06-03 13:55	2	CVE-2016-5242	arm: Host crash caused by VMID exhaustion
XSA-180	2016-05-23 17:09	2016-05-23 17:09	1	CVE-2014-3672	Unrestricted qemu logging
XSA-179	2016-05-09 11:48	2016-05-10 11:23	5	CVE-2016-3710 CVE-2016-3712	QEMU: Banked access to VGA memory (VBE) uses inconsistent bounds checks
XSA-178	2016-06-02 12:00	2016-06-06 16:55	4	CVE-2016-4963	Unsanitised driver domain input in libxl device handling
XSA-177	2016-05-24 12:21		-	-	Unused Xen Security Advisory number
XSA-176	2016-05-17 10:54	2016-05-17 10:54	3	CVE-2016-4480	x86 software guest page walk PS bit handling flaw

RawHammer, ce n'est pas fini

- Inversion de bit en cas de déduplication de la mémoire

  https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_razavi.pdf

Failles / Bulletins / Advisories

Réseau (principales failles)

Linux, injection de trafic dans un session TCP

- Implémentation de RFC 5961, censée durcir TCP

  http://arstechnica.com/security/2016/08/linux-bug-leaves-usa-today-other-top-sites-vulnerable-to-serious-hijacking-attacks/

Cisco

- Exécution de code dans le lecteur WebEx

  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-meetings-player

- Exécution de code à distance sur les firewalls PIX/ASA (cf. “site piratés: Equation Group”)

  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-snmp

  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-cli

- Elévation de privilège grâce à RawHammer sur les switchs/routeurs Nexus 😱

  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150309-rowhammer

Fortinet FortiOS (Firewalls FortiGate et FortiSwitch)

- Exécution de code à distance à partir d’une simple requête web (cf. “site piratés: Equation Group”)

  http://fortiguard.com/advisory/FG-IR-16-023

Failles / Bulletins / Advisories

Apple, Google, Facebook...

Apple iOS FalseCONNECT, Singe intercepteur sur HTTP CONNECT

- Interception d'une réponse d'authent. non chiffrée du proxy "407 Proxy Authentication Required"

  http://falseconnect.com/

Apple iOS et Mac OS X, exécution de code à distance par la librairie ImageIO

- Librairie équivalente à Stagefright
- Exécution de code lors du traitement d'une image TIFF
  - Mac OS X <= 10.11.6 et iOS <= 9.3.3

http://www.talosintelligence.com/reports/TALOS-2016-0171/

Apple iOS 3 vulnérabilités exploitées par NSO, cf. "sites piratés"

Android Quadrooter

- 4 failles sur les pilotes des smartphones à base de composants Qualcomm
  - Présenté à la Defcon24 (2016)

    https://www.defcon.org/html/defcon-24/dc-24-speakers.html#Donenfeld
- Savoir si son smartphone est vulnérable (méfiance tout de même)

    https://play.google.com/store/apps/details?id=com.checkpoint.quadrooter

https://nakedsecurity.sophos.com/2016/08/09/900-million-androids-vulnerable-to-quadrooter-bugs-what-you-need-to-know/amp/

Failles / Bulletins / Advisories

Divers

Jailbreak pour tous les Kindle d'Amazon

http://hackaday.com/2016/07/09/a-jailbreak-for-every-kindle/

SEED32

- Exploitation du théorème des anniversaires sur CBC avec blocs de 64bits
- Fonctionnel sur OpenVPN + Blowfish-CBC

https://blog.cryptographyengineering.com/2016/08/24/attack-of-week-64-bit-ciphers-in-tls/

Clef privée d'une AC inclue dans des équipements Aruba Networks/Alcatel-Lucent

- AC signée par GeoTrust : securelogin.arubanetworks.com

http://seclists.org/fulldisclosure/2016/Sep/3

Rowhammer FFS

- Compromission des autres VMs d'un même hôte physique
- Modification de clé SSH

http://news.softpedia.com/news/new-ffs-rowhammer-attack-targets-linux-vm-setups-507290.shtml

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Attaques sur HTTP 2.0

- Les mêmes familles d'attaques que sur HTTP 1.x
- DoS :
  - Par saturation des ressources en jouant sur les fenêtres de débit (INITIAL_WINDOW_SIZE)
  - Par saturation de la mémoire avec la compression des entêtes (HPACK Bomb)
  - En générant un comportement inattendu grâce au multiplexage en utilisant un flux (stream) passé

http://www.imperva.com/docs/Imperva_HII_HTTP2.pdf

Pangu sur iOS 9, tous les détails

- Vulnérabilité Path Traversal
- Vulnérabilité noyau CVE-2016-4654

https://www.blackhat.com/docs/us-16/materials/us-16-Wang-Pangu-9-Internals.pdf

Injection de code dans une appli NodeJS sur Paypal

http://artsploit.blogspot.fr/2016/08/pprce2.html?m=1

ThinkPwn, exécution de code UEFI, cf. revue du 2015-07-12

- Évolutions et mises à jour

https://github.com/Cr4sh/ThinkPwn/commit/d496e7d9a4bbb1e2903a94802760d52c1e46c037

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Exfiltration de données par les émissions électromagnétiques de l'USB / air gap

- Exploité par le malware USBee

  http://arstechnica.com/security/2016/08/meet-usbee-the-malware-that-uses-usb-drives-to-covertly-jump-airgaps/

Exfiltration de données grâce aux disques à plateaux / air gap

- Par des chercheurs de l'université Cornell, à Ithaca
  - Déjà à l'origine d'exfiltration par les ventilateurs

    https://arxiv.org/abs/1606.05915

  http://arstechnica.com/security/2016/08/new-air-gap-jumper-covertly-transmits-data-in-hard-drive-sounds/

Exfiltration des frappes clavier à partir des variations sur le signal WiFi

https://www.sigmobile.org/mobicom/2015/papers/p90-aliA.pdf

Méfiez-vous des .pac avec PacDoor

- Portée dérobée “limitée” dans un fichier Proxy Auto-Configuration (PAC)

  https://www.blackhat.com/docs/us-16/materials/us-16-Kotler-Crippling-HTTPS-With-Unholy-PAC.pdf

Cacher des données dans une DLL signée, sans changer la signature

- Dans la structure de la signature
- Mais le condensat est modifié 😜

  https://www.blackhat.com/docs/us-16/materials/us-16-Nipravsky-Certificate-Bypass-Hiding-And-Executing-Malware-From-A-Digitally-Signed-Executable-wp.pdf

Piratages, Malwares, spam, fraudes et DDoS

Malware

Beaucoup les techniques de détection d'AV/Sandbox dans un seul virus

- Ciblant les ordinateurs de contrôle d'accès avec les logiciels de ZKTeco
- Mais peu de technique anti-debug

https://sentinelone.com/blogs/sfg-furtims-parent/

Bart Ransomware, publication d'un outil pour déchiffrer

- Exe précompilé… ou est le source !!?

http://www.bleepingcomputer.com/news/security/avg-releases-decryptor-for-bart-ransomware/

Sauron / Remsec / Strider, le nouveau virus étatique

- En activité depuis au moins 5 ans
- Utilisation de :
  - 0days
  - Serveurs intermédiaire pour l'exfiltration des données
  - Script LUA
  - Plugins reçus et exécutés directement en mémoire
- Stockage des fichiers à exfiltrer en attente de la connexion d'une clef USB spécifique
- ...

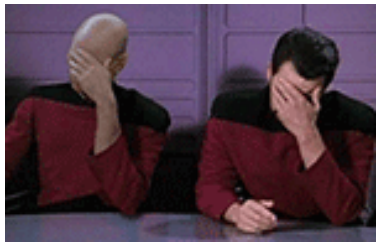
https://securelist.com/analysis/publications/75533/faq-the-projectsauron-apt/

Piratages, Malwares, spam, fraudes et DDoS

Malware

NSO Group, pris la main dans la culotte

- Société israélienne éditrice du malware/trojan Pegasus
  - Mandaté par les Émirats arabes unis pour espionner Ahmed Mansoor
  - Envoie d'un SMS avec un lien menant vers une chaine de **3** 0days iPhone (RCE, leak, EoL)
  - SMS transféré à "Citizen Lab Researchers"



- Tous les détails de l'histoire

  https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/
- Les 3 vulnérabilités sont corrigées avec iOS 9.3.5
- NSO, moqué par Zerodium

```
<<Looks like NSO's iOS Safari exploit crashes/closes the browser after
 exploitation, no process continuation / reparation? seriously?>>
```

  https://twitter.com/cbekrar/status/769163068999815168

- Les détails techniques de la vulnérabilité Kernel, par Stefan ESSER
  - Avec le PoC et des critiques "à la ESSER" 😆

  http://sektioneins.de/en/blog/16-09-02-pegasus-ios-kernel-vulnerability-explained.html

  http://sektioneins.de/en/blog/16-09-05-pegasus-ios-kernel-vulnerability-explained-part-2.html

Piratages, Malwares, spam, fraudes et DDoS

Malware

NSO, pris la main dans la culotte (suite)

- Hacking Team n'aimait pas trop NSO 😂

  https://wikileaks.org/hackingteam/emails/emailid/6204

- Pegasus vs RCS de Hacking Team →
- L'analyse complète de Pegasus

  https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis.pdf

NSO Pegasus	Remote Control System
Only supports Android, iOS, BlackBerry and Symbian.	Supports Android, iOS, BlackBerry, Symbian and also **Windows Phone**.
No support for desktop platforms.	Supports Windows, OS X and Linux.
Obsolete versions supported: • Android 4.2 (less than 60% of devices) • iOS 6.1.4 (less than 5% of devices)	Latest versions supported: • Android 5.0 Lollipop • iOS 8.1
Agent runs at low level, hence support for devices is limited and **risk of making the phone unusable** is high.	Agent runs at higher level, hence comprehensive support is possible. There is no risk of making the phone unusable.
Works on limited set of device models: • Samsung Galaxy • Sony Xperia • Apple iPhone 4/4S/5	Works on all devices models, including the latest LG official Google phones, and Apple iPhone 6.
Cannot collect encrypted calls on Android.	Captures Viber and Skype encrypted calls.
Captures chat from: • WhatsApp • Viber • Skype • BBM	Captures chat from: • WhatsApp • Viber • Skype • BBM And also: • Line • WeChat • Telegram We support applications on request.
Location identification is limited to GPS (does not work in buildings) and Cell-ID (inaccurate).	Location identification is comprehensive and done via: • GPS • Cell-ID • Wi-Fi Wi-Fi is usually very accurate in cities and buildings.
Collects historical data about the target.	Collects historical data about the target, including chats from Skype, Facebook and other social applications.

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

NSA / Equation, Group, Publication de 300Mo d'outils datant de 2013

- Par un/des hackeurs se nommant ShadowBrokers, surement anglophone

  http://www.theregister.co.uk/2016/08/23/nsa_hack_auction_looks_written_by_an_english_speaker_linguist/

  - Mais les américains attribuent l'attaque aux Russes
- Plus sérieusement, les piratages entre agences arrivent, mais pas les publications
  - Contenu : Shellcode et 0days (RCE, EoP) pour firewalls Fortinet, Cisco PIX/ASA et TopSec (Chinois)
- Les exploits sont en ligne:

  https://www.exploit-db.com/author/?a=8712

  - Fonctionnel sur ASA 9.2(4)

    https://twitter.com/SilentSignalHU/status/768095445444861952/photo/1

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

NSA / Equation, Group, Publication de 300Mo d'outils datant de 2013 (suite)

- Enchère délirante de **$568 Million** pour publier le reste

  https://blockchain.info/address/19BY2XCgbDe6WtTVbTyzM9eR3LYr6VitWK

  - Les adresses Bitcoins pour la rançon "never gonna give you up"

    https://blockchain.info/address/19BY2XCgbDe6WtTVbTyzM9eR3LYr6VitWK

- Réponse de Cisco

  http://blogs.cisco.com/security/shadow-brokers

- Le FBI aurait payé avec les bitcoins de SilkRoad ?

  https://krypt3ia.wordpress.com/2016/08/19/shadowbrokers-bitcoin-transactions-now-theres-some-taint-for-you/

  - Non, juste un troll

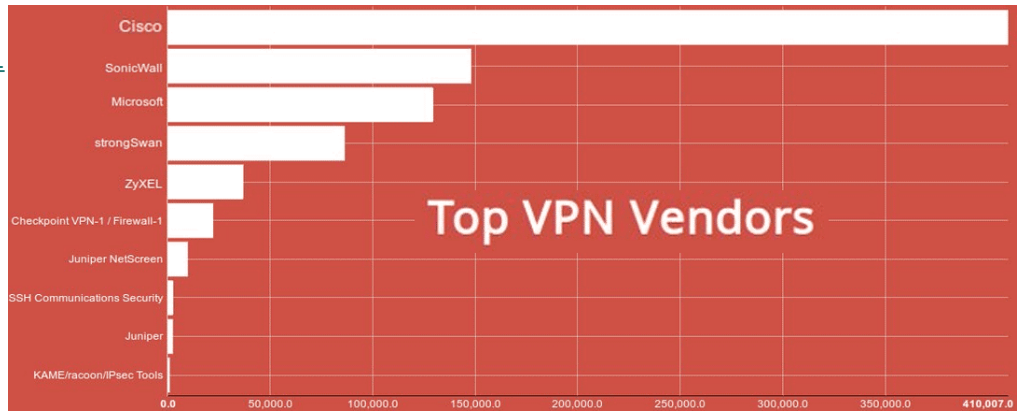
    https://www.malwaretech.com/2016/08/no-the-fbi-are-not-sending-bitcoins-to-the-shadowbrokers.html

- Au même moment, Fort Meade fait le coup de la panne

  http://www.zdnet.com/article/heres-what-brought-the-nsas-website-down-for-two-days/

- Cisco, numéro 1 des VPN

  https://twitter.com/achillean/status/769273046595149824/photo/1



Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Piratage de membres du parti démocrate américain / DNC

- Des milliers de mails et documents ont été publiés sur le site Wikileaks
  - Dont certains modifiés
- CrowdStrike enquête et pointe du doigt la Russie
- Même Snowden s'en mêle:

<< If Russia hacked the #DNC, they should be condemned for it. But during the #Sony hack, the FBI presented evidence.>>

https://twitter.com/Snowden/status/757573436059287552

http://www.slate.com/articles/news_and_politics/politics/2016/07/the_dnc_hack_is_watergate_but_worse.html

Piratage de scrutins locaux américains (Illinois et Arizona)

- Vol de login, mot de passe et résultats, pas de modification des votes en ligne
- "Selon le FBI", les Russes seraient les attaquants

https://www.washingtonpost.com/world/national-security/fbi-is-investigating-foreign-hacks-of-state-election-systems/2016/08/29/6e758ff4-6e00-11e6-8365-b19e428a975e_story.html

- Le FBI alerte sur les risques d'autres piratages

http://arstechnica.com/security/2016/08/after-illinois-hack-fbi-warns-of-more-attacks-on-state-election-board-systems/

Des hackeurs démontrent comment pirater des machines à voter

http://www.cbsnews.com/news/rigged-presidential-elections-hackers-demonstrate-voting-threat-old-machines/

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Transmission pour Mac OS X (client BitTorrent)

- Compromission des serveurs et dépôt d'un client (version 2.92) contenant un malware
  - Ce n'est pas la première fois...

https://transmissionbt.com/keydnap_qa/

Piratage de l'application Telegram (chat chiffré) **en Iran**

- En interceptant les codes PIN envoyés par SMS

https://www.wired.com/2016/08/hack-brief-hackers-breach-ultra-secure-messaging-app-telegram-iran/

  - Alors que le NIST recommande un autre second facteur d'authentification

https://threatpost.com/nist-recommends-sms-two-factor-authentication-deprecation/119507/

  - Et que la faiblesse du SMS est connue

http://www.forbes.com/forbes/welcome/?toURL=http://www.forbes.com/sites/thomasbrewster/2016/06/15/hackers-steal-facebook-account-ss7/

- La police fédérale allemande fait pareil 

http://genius.it/motherboard.vice.com/de/read/exklusiv-wie-das-bka-telegram-accounts-von-terrorverdaechtigen-knackt#annotations:10291650

- L'application est pourtant très appréciée de nos politiques

http://www.lefigaro.fr/secteur/high-tech/2016/07/21/32001-20160721ARTFIG00216-telegram-une-application-sulfureuse-appreciee-des-politiques-francais.php

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Piratage de Dropbox en 2012

- Fuite de 68 millions de comptes

  https://www.troyhunt.com/the-dropbox-hack-is-real/

  https://techcrunch.com/2016/08/30/dropbox-employees-password-reuse-led-to-theft-of-60m-user-credentials/

Voler de l'argent en indiquant un numéro surtaxé pour le 2FA

https://www.arneswinnen.net/2016/07/how-i-could-steal-money-from-instagram-google-and-microsoft

Sage UK

- Exfiltration des données personnelles de 157 000 clients
- Arrestation d'employés à l'origine de l'attaque

  http://www.telegraph.co.uk/business/2016/08/17/sage-group-employee-arrested-on-fraud-charge/

Piratage de DCNS ou plutôt « arnaque à l'appel d'offre »

- Annonce (par la concurrence) d'une compromission et remise en doute de la confiance envers DCNS
  - En plein appel d'offre par l'Australie pour des sous-marins

  http://www.lemonde.fr/international/article/2016/08/24/enquete-francaise-apres-une-fuite-massive-de-donnees-de-la-dcns-sur-le-sous-marin-scorpene_4987019_3210.html
- Les documents sortis ne sont que des documentations techniques non critiques
- DCNS remporte quand même l'appel d'offre 

  http://www.lesechos.fr/industrie-services/air-defense/021877913925-sous-marins-la-france-remporte-en-australie-le-contrat-du-siecle-1217447.php

Piratages, Malwares, spam, fraudes et DDoS

Internet des Objets

Muddy Water et le “profit disclosure”

1. Vente à découvert d’action St. Jude Medical
2. Publication d’un rapport sur des vulnérabilités de leurs équipements cardiaques

   http://d.muddywatersresearch.com/tos/?redirect=/wp-content/uploads/2016/08/MW_STJ_08252016_2.pdf
3. Baisse du cours en bourse et Profits !

   http://arstechnica.com/security/2016/08/trading-in-stock-of-medical-device-paused-after-hackers-team-with-short-seller/

   http://blog.erratasec.com/2016/08/notes-on-that-stjudemuddywattersmedsec.html

Vulnérabilités dans les ampoules OSRAM

https://community.rapid7.com/community/infosec/blog/2016/07/26/r7-2016-10-multiple-osram-sylvania-osram-lightify-vulnerabilities-cve-2016-5051-through-5059

Piratages, Malwares, spam, fraudes et DDoS

SCADA

Vulnérabilités dans VXWorks

http://blog.exodusintel.com/2016/08/09/vxworks-execute-my-packets/

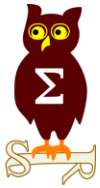
Honeypot SI industriels

- Simule plusieurs protocoles industriels

https://github.com/mushorg/conpot

OSISoft publie des outils d'audit de PI

https://pisquare.osisoft.com/groups/security/blog/2016/07/26/check-out-the-pi-security-audit-tools-on-github



Nouveautés, outils et techniques

Crypto
Divers

Utilisation de certificats HTTPS dont la clé privée est déjà connue

- Etude menée en 2015 par Sec-Consult et le CERT-CC 
- En 2016 : 40% pire (4,5 millions de services identifiés)

http://blog.sec-consult.com/2016/09/house-of-keys-9-months-later-40-worse.html?spref=tw

Module DES KPA pour hashcat

- Possibilité de cracker un hash netNTLMv1 pour en déduire le hash NT
- Fonctionne aussi pour MSCHAP-v2 et plus globalement WPA-2 entreprise
- Réussite assurée en 80h sur du matériel à 5k (à base de GTX 1080 😁)

https://hashcat.net/forum/thread-5832.html

Oversec

- Sur-chiffrez vos messages

http://www.oversec.io/

VeraCrypt 1.18

- Support de UEFI
- Inclusion de Camellia (Japonais), Streebog (Russe) et Magma (Russe, GOST)

https://veracrypt.codeplex.com/

Crypto
Divers

La clef maître DNSSEC va changer

http://www.techworld.com/security/dnssec-master-key-securing-dns-is-about-change-should-we-be-worried-3645538/

AMD va chiffrer la mémoire RAM

http://events.linuxfoundation.org/sites/events/files/slides/AMD%20x86%20Memory%20Encryption%20Technology%20LSS%20Slides.pdf

Pentest
Techniques & outils

Kali Linux 2016.2

https://www.kali.org/news/kali-linux-20162-release/

Bloodhound

- Identifier visuellement les voies d'élévations de privilèges dans Active Directory
  - Mais encore beaucoup de bugs en cours de correction
- Similaire à AD-Control-Paths présenté par l'ANSSI en 2014

https://github.com/adaptivethreat/Bloodhound

RaiseChild en Python et PowerShell

- Passer d'administrateur du domaine à administrateur de forêt : SID history + Golden Ticket

https://github.com/CoreSecurity/impacket/blob/master/examples/raiseChild.py

https://github.com/HarmJ0y/Misc-PowerShell

Détecter LAPS / Local Administrator Password Solution

```
powershell -ex bypass -nop -c  Get-ChildItem "c:\program files\LAPS\CSE\Admpwd.dll"
```

Détecter ImageTragick avec Burps

https://blog.silentsignal.eu/2016/05/13/detecting-imagetragick-with-burp-suite-pro/

Pentest
Techniques & outils

PCI-Leech, interaction DMA via port PCI

- Récupération de la mémoire, obtention d'un shell, récupération de fichiers, ...

https://github.com/ufrisk/pcileech

Base local de mots de passe par défaut

https://github.com/michenriksen/searchpass

Récupérer le hash/mot de passe d'un utilisateur sur PC verrouillé

- Utilisation d'un adaptateur USB-Ethernet + Responder.py
- Retour d'expérience : tous les PCs n'ont pas le bon driver 😓

https://room362.com/post/2016/snagging-creds-from-locked-machines/

Utiliser Google Docs comme Contrôle-Commande

http://www.blackhillsinfosec.com/?p=5230

Projet de Backdoor UEFI

http://seclist.us/pei-stage-backdoor-for-uefi-compatible-firmware.html

Pentest
Techniques & outils

Réimplémentation partielle de PowerView en Python

- Toutes les fonctions ne sont pas encore disponibles

https://github.com/the-useless-one/pywerview

Liste de rapports de tests d'intrusion publics

https://github.com/juliocesarfort/public-pentesting-reports

Récupérer des infos sur le déploiement de LAPS

https://adsecurity.org/?p=3164

Framework de pentest iOS : Needle

https://github.com/mwrlabs/needle

Contrôle-Commande via les propriétés des objets AD

https://gist.github.com/HarmJ0y/a219057e9d2faedf69d32e04c0f1874f

Nouvelle version de Responder.py

https://github.com/lgandx/Responder

L0phtCrack 7, la légende est de retour !

- Multi-CPU, GPU, support de plugins...

  http://www.l0phtcrack.com/2016/08/646/

Un générateur de ShellCode pour ARM

https://github.com/alexpark07/ARMSCGen

Un générateur de ShellCode générique

https://github.com/ixty/xarch_shellcode

Obtenir un shell linux sur un Cisco Catalyst

```
Switch# request system shell
[...]
`/bin/sh`
sh-3.2#
```

```
Switch# request system shell
[...]
`bash 1>&2`
bash-3.2#
```

```
Switch# request system shell
[...]
`sh 1>&2`
sh-3.2#
```

AIL, framework d'analyse de données non-structurées

https://github.com/CIRCL/AIL-framework

McAfee Stinger 12.1.0.2101

- Suppression de 6 000 virus communs en version portable

http://portableapps.com/news/2016-08-30--mcafee-stinger-portable-12.1.0.2101-released

MS16-099 : Microsoft porte sur Office 2013 la GPO de désactivation des Macro

- Macro pour des documents provenant d'internet
- A mettre en place rapidement !

https://support.microsoft.com/en-us/kb/3177451

KasperskyOS, pour les systèmes industriels

- Le système d'exploitation sécurisé selon Kaspersky
  - Réécriture complète
  - **Pas de vulnérabilité**

www.securelist.com/en/analysis/204792248/Securing_Critical_Information_Infrastructure_Trusted_Computing_Base

Nouveautés (logiciel, langage, protocole...)

Open Source

HatDBG, un debugger en PowerShell

https://n0where.net/minimal-powershell-win32-debugger-hatdbg/

OWASP Juice Shop

- Application intentionnellement vulnérable (à la webgoat)
- Technos plus modernes (Node, etc..)

https://www.owasp.org/index.php/OWASP_Juice_Shop_Project

Nouveautés (logiciel, langage, protocole...)

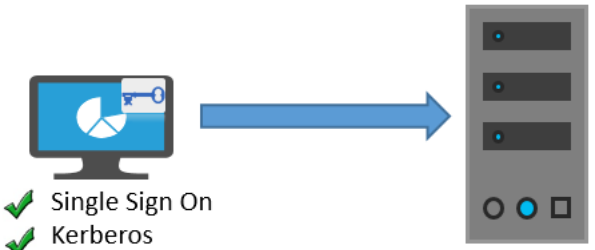
Microsoft

Remote Credential Guard

- Les tickets Kerberos ne sont plus envoyés sur la cible de connexion
- Uniquement pour Windows 10 et Windows Server 2016

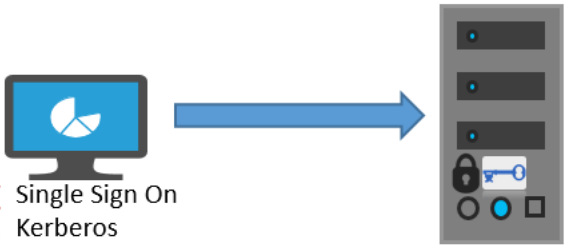
https://technet.microsoft.com/en-us/itpro/windows/keep-secure/remote-credential-guard

Remote Credential Guard



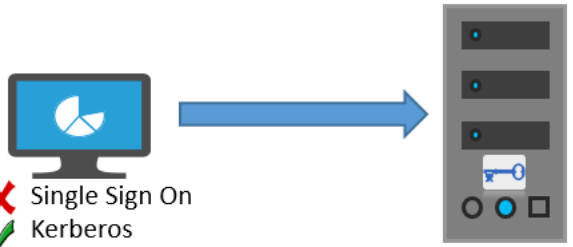
- ✓ Single Sign On
- ✓ Kerberos
- ✗ NTLM
- ✓ Access to services from Server
- ✓ Prevent Pass The Hash
- ✓ Prevent usage of credential after disconnection

Remote Desktop Connection and a server protected with Credential Guard



- ✗ Single Sign On
- ✓ Kerberos
- ✓ NTLM
- ✓ Access to services from server
- ✓ Prevent Pass The Hash
- ✗ Prevent usage of credential after disconnection

Remote Desktop Connection



- ✗ Single Sign On
- ✓ Kerberos
- ✓ NTLM
- ✓ Access to services from server
- ✗ Prevent Pass The Hash
- ✗ Prevent usage of credential after disconnection

ATA / Advanced Threat Analytics en version 1.7

- Devrait détecter les phases de reconnaissances type PowerView 😭

https://blogs.technet.microsoft.com/enterprisemobility/2016/08/31/introducing-advanced-threat-analytics-v1-7/

Business et Politique

Droit / Politique

France

Les boîtes noires ne sont pas encore prêtes

- Et les réseau sociaux ne jouent pas le jeu

  http://www.nextinpact.com/news/100809-renseignement-boites-noires-sont-toujours-en-cours-d-elaboration.htm

ANSSI, publication des Prestataires de Réponse à Incident de Sécurité

- En cours de qualification
- 1 petit, 2 moyens, 1 gros

  http://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-reponse-aux-incidents-de-securite-pris/

Droit / Politique

France

LPM, les arrêtés sectoriels

- Transports terrestres

  https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=B996AA0E9BECE2CC05829C575FBBEE0A.tpdila15v_3?cidTexte=JORFTEXT000033063035&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000033063030

- Transports maritime et fluvial

  https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=B996AA0E9BECE2CC05829C575FBBEE0A.tpdila15v_3?cidTexte=JORFTEXT000033063081&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000033063030

- Transports aériens

  https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=B996AA0E9BECE2CC05829C575FBBEE0A.tpdila15v_3?cidTexte=JORFTEXT000033063127&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000033063030

- Approvisionnement en énergie électrique

  https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=B996AA0E9BECE2CC05829C575FBBEE0A.tpdila15v_3?cidTexte=JORFTEXT000033063173&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000033063030

- Approvisionnement en gaz naturel

  https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=B996AA0E9BECE2CC05829C575FBBEE0A.tpdila15v_3?cidTexte=JORFTEXT000033063219&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000033063030

- Approvisionnement en hydrocarbures pétroliers

  https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=B996AA0E9BECE2CC05829C575FBBEE0A.tpdila15v_3?cidTexte=JORFTEXT000033063265&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000033063030

- Alimentation

  http://www.mag-securs.com/Portals/0/news/2016/06_juin/joe_20160623_0145_0005.pdf

- Produits de santé

  http://www.mag-securs.com/Portals/0/news/2016/06_juin/joe_20160623_0145_0003.pdf

- Gestion de l'eau

  http://www.mag-securs.com/Portals/0/news/2016/06_juin/joe_20160623_0145_0004.pdf

Droit / Politique
International

Pour entrer sur le territoire américain, il faudra donner son profil facebook 

http://arstechnica.com/tech-policy/2016/06/attention-us-bound-tourists-social-media-accounts-subject-to-inspection/

Il efface les configurations des principaux routeurs de Citibank

- Sorti d'un entretien d'évaluation, il efface les config des 10 principaux routeurs de coeur
  - Et justifie son geste par SMS à un collègue
- Prison et une amende de $77,200

http://www.tripwire.com/state-of-security/featured/citibank-it-guy-deliberately-wiped-routers-shut-down-90-of-firms-networks-across-america/

Singapour va couper ses services publics d'Internet par mesure de sécurité

http://www.usine-digitale.fr/article/singapour-va-couper-ses-services-publics-d-internet-par-mesure-de-securite.N428952

WhatsApp partagera vos données avec Facebook

http://www.phonandroid.com/vie-privee-whatsapp-partagera-donnees-facebook-ouille.html

Google est candidat pour le Privacy Shield

http://www.nextinpact.com/news/101157-donnees-personnelles-google-est-candidat-pour-privacy-shield.htm

Business
International

Bruce Schneier rejoint le projet TOR

http://www.theinquirer.net/inquirer/news/2465042/security-wizard-bruce-schneier-joins-the-tor-project

Intel revend McAfee pour $4,2 milliards

- Alors que l'achat avait coûté $7,86 milliards
- Mais garde 49% des parts

  http://www.zdnet.fr/actualites/securite-intel-se-debarrasse-de-mcafee-39841636.htm
- Et… John McAfee attaque Intel afin de récupérer son nom !

  http://www.infosecurity-magazine.com/news/mcafee-sues-intel-for-the-right-to/

Le Cloud AWS, c'est du bonheur pour la CIA

- Pour leur propre usage bien sûr 😊

  http://www.nextgov.com/cloud-computing/2016/08/cia-official-cloud-has-been-godsend/130716/

Conférences

Conférences

Passées

- BlackHat - 30 juillet au 4 aout 2016 à Las Vegas
  - Compte-rendu ce jour
- BSides Las Vegas : 2 & 3 août à Las Vegas
- Defcon - 4 au 7 aout à Las Vegas

A venir

- HackLU – 18 au 20 octobre 2016 au Luxembourg
- BruCON – 27 au 28 octobre 2016 à Gent
- Cyber Security Alliance - 1 au 3 novembre 2016 à Yverdon-les-Bains
- BlackHat Europe – 1 au 4 novembre 2016 à Londre
- Botconf - 30 novembre au 2 décembre 2016 à Lyon

Divers / Trolls velus

Divers / Trolls velus

Marché gris des vulnérabilités : prix chez Exodus

- 0days et n-days

  https://rsp.exodusintel.com/#zero

Current Hitlist

TARGET	MAXIMUM
iOS 9.3+	$500000
Google Chrome	$150000
Microsoft EDGE	$125000
Firefox	$80000
Windows 10 LPE	$75000
Adobe Reader	$60000
Adobe Flash	$60000

More items are available. Please login to see the complete list.

Current Hitlist

TARGET	DESCRIPTION
CVE-2016-2211	RCE in Symantec ATP
CVE-2016-1019	RCE in Flash
CVE-2016-1960	Firefox UAF
CVE-2016-1961	Firefox UAF
CVE-2016-0200	IE UAF

More items are available. Please login to see the complete list.

Divers / Trolls velus

Pokemon Go

- DDoS

  https://t.co/spfrElVfCs

- Rétro-ingénierie de l'application Android

  https://applidium.com/en/news/unbundling_pokemon_go/

  https://github.com/applidium/PokemonGo_Android_RE

- NecroBot, un bot en C# pour automatiser la recherche des pokémons

  https://github.com/NecronomiconCoding/NecroBot

Mais qui a assassiné ~~Hervé Schauer~~ Hector Douché !!? 

- Roman prenant place aux assises, écrit par un breton anonyme

  https://www.amazon.fr/Reich-num%C3%A9rique-Alain-Henri-ebook/dp/B01EFSNQJ4

Divers / Trolls velus

L'interview du hackeur de Hacking Team

- Et la mort de la crédibilité

  https://motherboard.vice.com/read/hacker-phineas-fisher-hacking-team-

RSSI, un des 5 métier permettant de gagner 100K€/an en France

http://bfmbusiness.bfmtv.com/emploi/5-jobs-meconnus-qui-permettent-de-gagner-100-000-euros-par-an-1031905.html

Les pentests ne servent à rien

- Il ne montre que les limites des auditeurs
  - Ils n'ont pas réussi à trouver de faille != pas de faille

- Plus sérieusement : c'est utile, à condition d'avoir une vraie démarche sécurité et d'être capable de mettre en place le plan d'action induit

http://www.ranum.com/security/computer_security/editorials/point-counterpoint/pentesting.html

Divers / Trolls velus

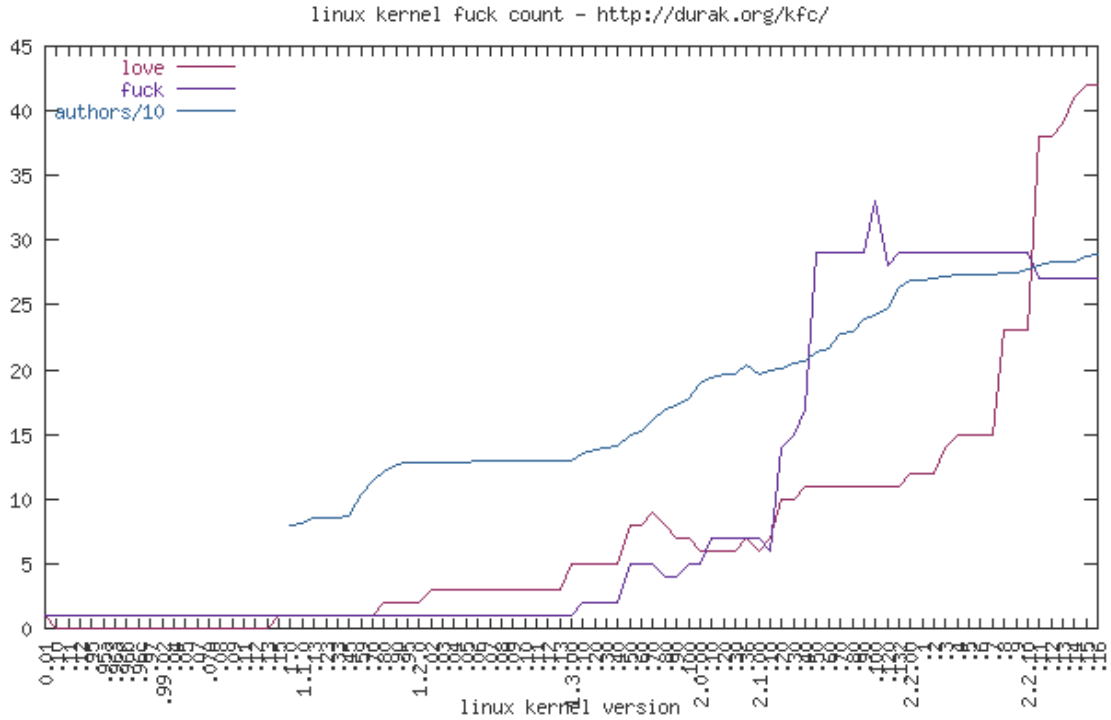
Les développeurs Whatsapp n'aiment pas trop Apple

https://www.reddit.com/r/technology/comments/51ncdt/fuck_apple_in_whatsapp_code_wtf/?st=isvjzrwm&sh=70af48d1

```
Log.d("FUCK APPLE return link:", MyActivity
Log.d("FUCK APPLE equaled in save:", MyAct
Log.d("FUCK APPLE equaled in unsave:", MyA
```

- Mais le noyau Linux n'est pas en reste

  http://durak.org/sean/pubs/kfc/

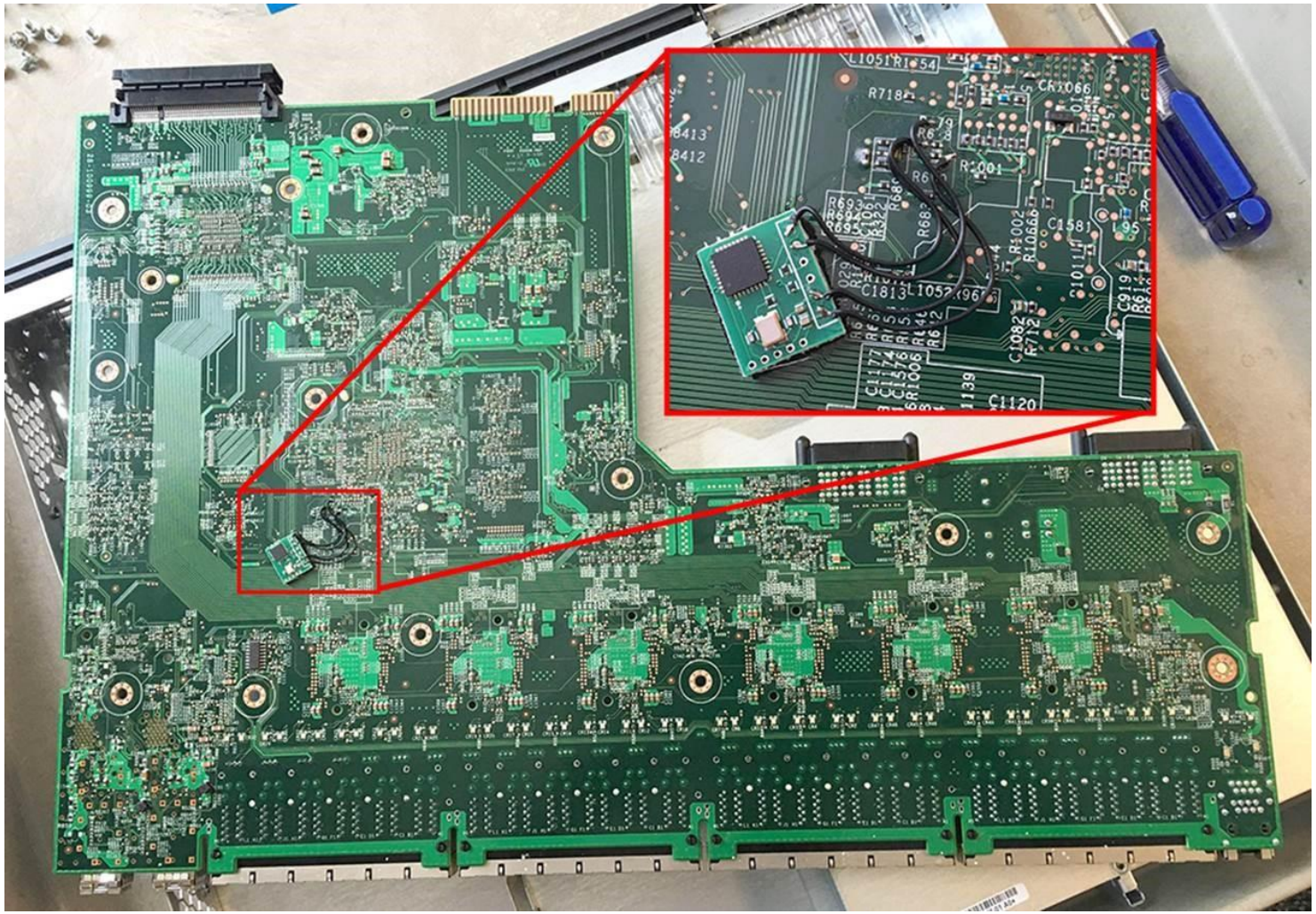


Divers / Trolls velus

Il achète un switch Cisco sur eBay, adjoint d'un "cadeau Bonux"

- Petite carte fille soudée à l'arrière de la carte mère

https://www.reddit.com/r/networking/comments/4iwa5f/possible_counterfeit_cisco_equipment_wphotos/

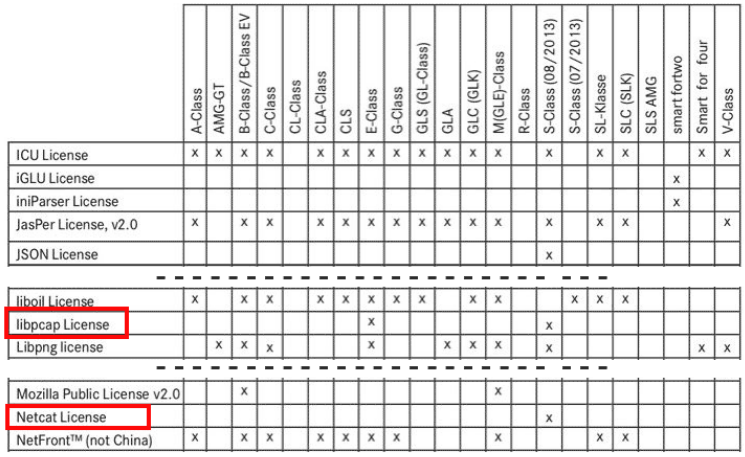


Divers / Trolls velus

La Mercedes Classe S avec des outils pour l'intrusion

- netcat et libpcap préinstallé
- Pour gagner du temps après vos RCE 😊

  https://twitter.com/dotMudge/status/769588040884817920/photo/1



	A-Class	AMG-GT	B-Class/B-Class EV	C-Class	CL-Class	CLA-Class	CLS	E-Class	G-Class	GLS (GL-Class)	GLA	GLC (GLK)	M(GLE)-Class	R-Class	S-Class (08/2013)	S-Class (07/2013)	SL-Klasse	SLC (SLK)	SLS AMG	smart fortwo	Smart for four	V-Class
ICU License	x	x	x	x		x	x	x	x	x	x	x	x		x		x	x		x	x	x
iGLU License																				x		
iniParser License																				x		
JasPer License, v2.0	x		x	x		x	x	x	x	x	x	x	x		x		x	x				x
JSON License															x							
liboil License	x		x	x		x	x	x	x	x		x	x			x	x	x				
libpcap License								x							x							
Libpng license		x	x	x				x			x	x	x		x						x	x
Mozilla Public License v2.0			x										x									
Netcat License															x							
NetFront™ (not China)	x		x	x		x	x	x	x				x				x	x				

Pirater Street Fighter 2, CPS2 avec Radar2

- Présentation en vidéo de 30 minutes

  https://www.youtube.com/watch?v=MnA11govEcI

Killer USB, une copie chinoise est en vente

- cf. Revue du 2015-11-10
- Permet de griller un ordinateur en se chargeant à partir de l'alimentation USB

  https://www.usbkill.com/

Divers / Trolls velus

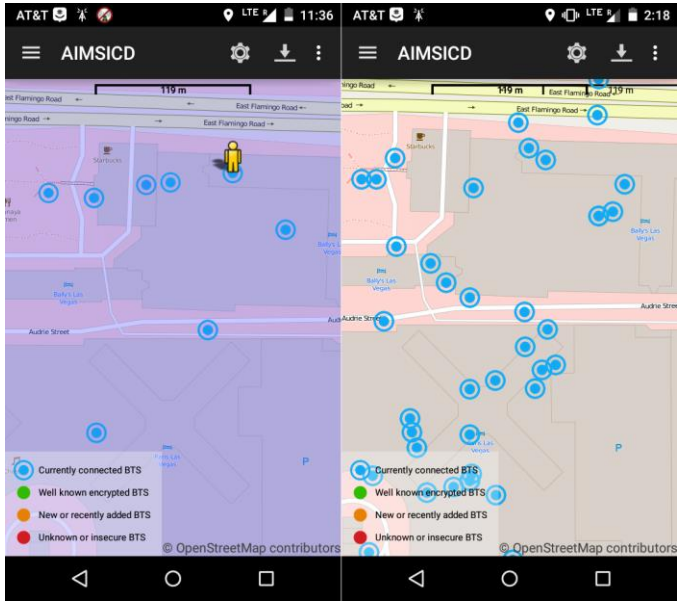
WMI sur Linux… avec Omi

https://github.com/Microsoft/omi

Defcon, des IMSI catcher en vue

- Des hackeurs font une carte des antennes GSM
- Dont beaucoup très douteuses

http://motherboard.vice.com/read/surprise-scans-suggest-hackers-put-imsi-catchers-all-over-defcon



L’ordinateur est complètement con

- Mais on ne lui demande pas d’être intelligent 😉
- A lire “comment est-il encore possible qu’il y ait des bugs ?“

http://rue89.nouvelobs.com/2016/08/26/gerard-berry-lordinateur-est-completement-con-257428

Prochains rendez-vous de l’OSSIR

Prochaine réunion

- Mardi 11 octobre 2016

After Work

- Fin octobre

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous