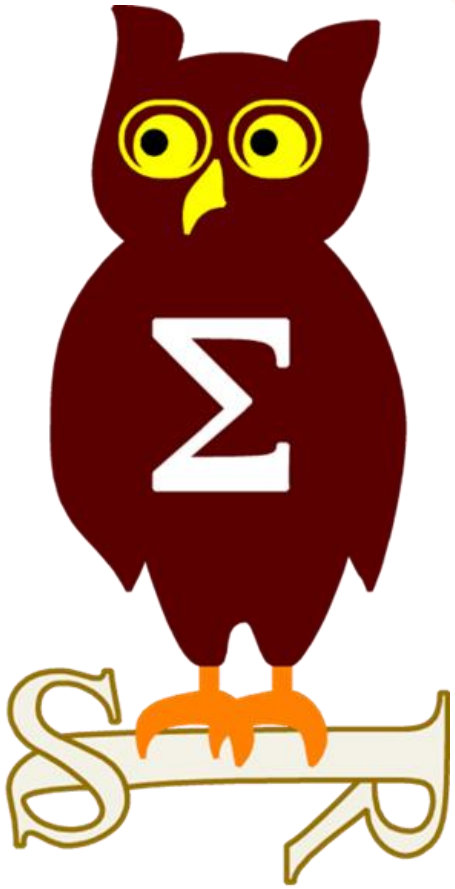
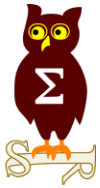


Revue d'actualité

11/10/2016

Préparée par

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



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-104 Vulnérabilités dans Internet Explorer (10 CVE) [Exploitabilité 3,3,1,1,1,1,1,1,1,1]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - 5 x Corruptions de mémoire aboutissant à une exécution de code
    - Code d'exploitation public disponible https://www.exploit-db.com/exploits/40374/
  - 3 x Contournements ASLR (fuite d'information)
  - Contournement du filtre anti-XSS
  - Elévation de privilèges
- Crédits:
  - Eduardo Braun Prado par Trend Micro's Zero Day Initiative (ZDI) (CVE-2016-3353)
  - Garage4Hackers par Trend Micro's Zero Day Initiative (ZDI) (CVE-2016-3295)
  - Jun Kokatsu (----------)
  - Kafeine, Brooks Li de Trend Micro (CVE-2016-3351)
  - Liu Long de Qihoo 360 (CVE-2016-3297)
  - Nathaniel Theis (XMPPwocky) (CVE-2016-3291)
  - SkyLined (CVE-2016-3324, CVE-2016-3325)
  - SkyLined par Trend Micro's Zero Day Initiative (ZDI) (CVE-2016-3247)
  - Thomas Vanhoutte par Trend Micro's Zero Day Initiative (ZDI) (CVE-2016-3292)
  - Yuki Chen de Qihoo 360 Vulcan Team (CVE-2016-3375)

MS16-105 Vulnérabilités dans Edge (12 CVE) [Exploitabilité 3,3,2,2,1,1,1,1,0,2,2,1]

- Affecte:
  - Windows 10
- Exploit:
  - 7 x Corruptions de mémoire aboutissant à une exécution de code
    - Code d'exploitation public disponible
  - 3 x Contournement ASLR (fuite d'information)
  - 2 x Evation du lecteur de PDF intégré
- Crédits:
  - F4B3CD de STARLAB (CVE-2016-3330)
  - Garage4Hackers par Trend Micro's Zero Day Initiative (ZDI) (CVE-2016-3295)
  - Henry Li (zenhumany) de Trend Micro (----------)
  - Jun Kokatsu (----------)
  - Kafeine, Brooks Li de Trend Micro (CVE-2016-3351)
  - Liu Long de Qihoo 360 (CVE-2016-3297)
  - Microsoft ChakraCore Team (CVE-2016-3350)
  - Nathaniel Theis (XMPPwocky) (CVE-2016-3291)
  - Richard Zhu (fluorescence) par Trend Micro's Zero Day Initiative (ZDI) (CVE-2016-3377)
  - Shi Ji (@Puzzor) de VARAS@IIE par Trend Micro's Zero Day Initiative (ZDI) (CVE-2016-3294)
  - SkyLined (CVE-2016-3325)
  - SkyLined par Trend Micro's Zero Day Initiative (ZDI) (CVE-2016-3247)

Dont 6 communes avec IE:

- CVE-2016-3247
- CVE-2016-3291
- CVE-2016-3295
- CVE-2016-3297
- CVE-2016-3325
- CVE-2016-3351

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-106 Vulnérabilités dans GDI (5 CVE) [Exploitabilité 1,1,2,2,2]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - 2 x élévation de privilèges noyau (Win32k)
  - Corruption de mémoire dans GDI aboutissant à une exécution de code
  - Contournement ASLR (fuite d'information) dans GDI
  - Elévation de privilèges
- Crédits:
  - Jun Mao de Tencent PC Manager via GeekPwn (CVE-2016-3355)
  - RanchoIce de Baidu Security Lab (CVE-2016-3348)
  - WanderingGlitch de Trend Micro's Zero Day Initiative (ZDI) (CVE-2016-3354)

MS16-107 Vulnérabilités dans Office (13 CVE) [Exploitabilité 1,2,2,2,2,2,2,2,2,2,2,3,2]

- 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
    - Détails et code d'exploitation pour Excel: https://medium.com/@steventseeley/ms16-107-microsoft-office-excel-eof-record-type-confusion-remote-code-execution-vulnerability-1105d52764ff
- Crédits:
  - A researcher par iDefense (CVE-2016-3358)
  - Eduardo Braun Prado (CVE-2016-3364)
  - Incident Response Team de Certego (CVE-2016-3366)
  - Steven Seeley de Source Incite (CVE-2016-3359, CVE-2016-3361, CVE-2016-3362, CVE-2016-3363)
  - Steven Seeley de Source Incite par Trend Micro's Zero Day Initiative (ZDI) (CVE-2016-3365)
  - Steven Vittitoe de Google Project Zero (CVE-2016-3357)
  - Udi Yavo de enSilo (CVE-2016-0137)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-108 Vulnérabilités dans Exchange (3 CVE) [Exploitabilité 2,2,2]

- Affecte:
  - Exchange Serveur 2007, 2010, 2013, 2016
  - Remplace KB3150501, KB3151086, KB3151097
- Exploit:
  - Détournement de la fonctionnalité "send as" permettant de récupérer des informations
  - Exécution de code dans une librairie Oracle inclue dans Exchange lors du traitement d'une pièce jointe à un mail
- Crédits:
  - Adrian Ivascu (CVE-2016-3379)
  - Bassel Rachid de DH CorporationLucie Brochu de (CVE-2016-0138)
  - John Page de ApparitionSec (CVE-2016-3378)

MS16-109 Vulnérabilité dans Silverlight (1 CVE) [Exploitabilité 3]

- Affecte:
  - Windows (toutes versions supportées)
  - Remplace MS16-006
- Exploit:
  - Corruption de mémoire aboutissant à une exécution de code à l'ouverture d'une page Web
- Crédits:
  - ?

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-110 Vulnérabilités diverses (4 CVE) [Exploitabilité 2,2,2,2]

- Affecte:
  - Windows (toutes versions supportées)
  - Remplace MS13-032, MS16-081, MS16-101
- Exploit:
  - Elévation de privilèges du fait de NTLM sur un partage SMB
  - Déni de service
  - Exécution de code en environnement Active Directory
- Crédits:
  - Jonathan Brown de VMware, Inc (CVE-2016-3368)

MS16-111 Vulnérabilités noyau Win32k (5 CVE) [Exploitabilité 2,2,2,2,2]

- Affecte:
  - Windows (toutes versions supportées)
  - Remplace KB2644615, KB3153171, KB3167679, KB3170377, KB3176492, KB3176493, KB3176495
- Exploit:
  - Diverses élévations de privilèges
  - Elévations de privilège lors du chargement et attachement de clefs de base de registre
    https://bugs.chromium.org/p/project-zero/issues/detail?id=870
    https://bugs.chromium.org/p/project-zero/issues/detail?id=865
- Crédits:
  - James Forshaw de Google Project Zero (CVE-2016-3371, CVE-2016-3373)
  - Marcin Wiazowski, individual (CVE-2016-3372)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-112 Security Update for Windows Lock Screen (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows 8.1, 10, 2012 R2
  - Remplace KB3176492, KB3176493, KB3176495
- Exploit:
  - Vol de l'identifiant et du mot de passe d'un utilisateur si sa session est verrouillée
    - Cumul d'outils et techniques connues avec Lan Turtle / Raspberry Pi / USB Armory

    http://elevatedprompt.com/2016/09/snagging-credentials-from-locked-machines-with-raspberry-pi-zero/
    https://room362.com/post/2016/snagging-creds-from-locked-machines/
- Crédits:
  - Auri A. Rahimzadeh de Auri's Ideas (CVE-2016-3302)

MS16-113 Vulnérabilités noyau Win32k (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportées)
  - Remplace KB3176492, KB3176493
- Exploit:
  - Contournements ASLR (fuite d'information)
- Crédits:
  - ?

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-114 Vulnérabilité dans SMB v1 (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportées)
  - Remplace KB3073921, KB3176492, KB3176493, KB3176495
- Exploit:
  - Exécutions de code à la réception de trames SMBv1 authentifiées et spécialement formatées
- Crédits:
  - ?

MS16-115 Vulnérabilité dans le lecteur de PDF (2 CVE) [Exploitabilité 2,2]

- Affecte:
  - Windows 8.1, 10, 2012 RT
  - Remplace KB3175887, KB3176492, KB3176493, KB3176495
- Exploit:
  - Contournements ASLR (fuite d'information) dans le lecteur de PDF
- Crédits:
  - Ke Liu de Tencent's Xuanwu Lab (CVE-2016-3370)
  - Roberto Suggi Liverani (@malerisch) de malerisch.net et Steven Seeley de Source Incite (CVE-2016-3374)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-116 Vulnérabilité dans VBScript (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportées)
  - Remplace KB3006226, KB3176492, KB3176493, KB3176495
- Exploit:
  - Corruption de mémoire aboutissant à une exécution de code à l'ouverture d'une page Web contenant un script VB spécialement formatée
    - Vulnérabilité différentes mais le principe est le même
      https://www.cgsec.co.uk/powershell-empire-cve-2016-0189-profit/
- Crédits:
  - An anonymous researcher par Trend Micro’s Zero Day Initiative (ZDI) (CVE-2016-3375)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-117 Security Update for Adobe Flash Player (**78** CVE) [Exploitabilité 2,2,2,...]

- Affecte:
  - Windows (toutes versions supportées)
  - Remplace KB3174060
- Exploit:
  - Plusieurs exploits publiquement accessibles

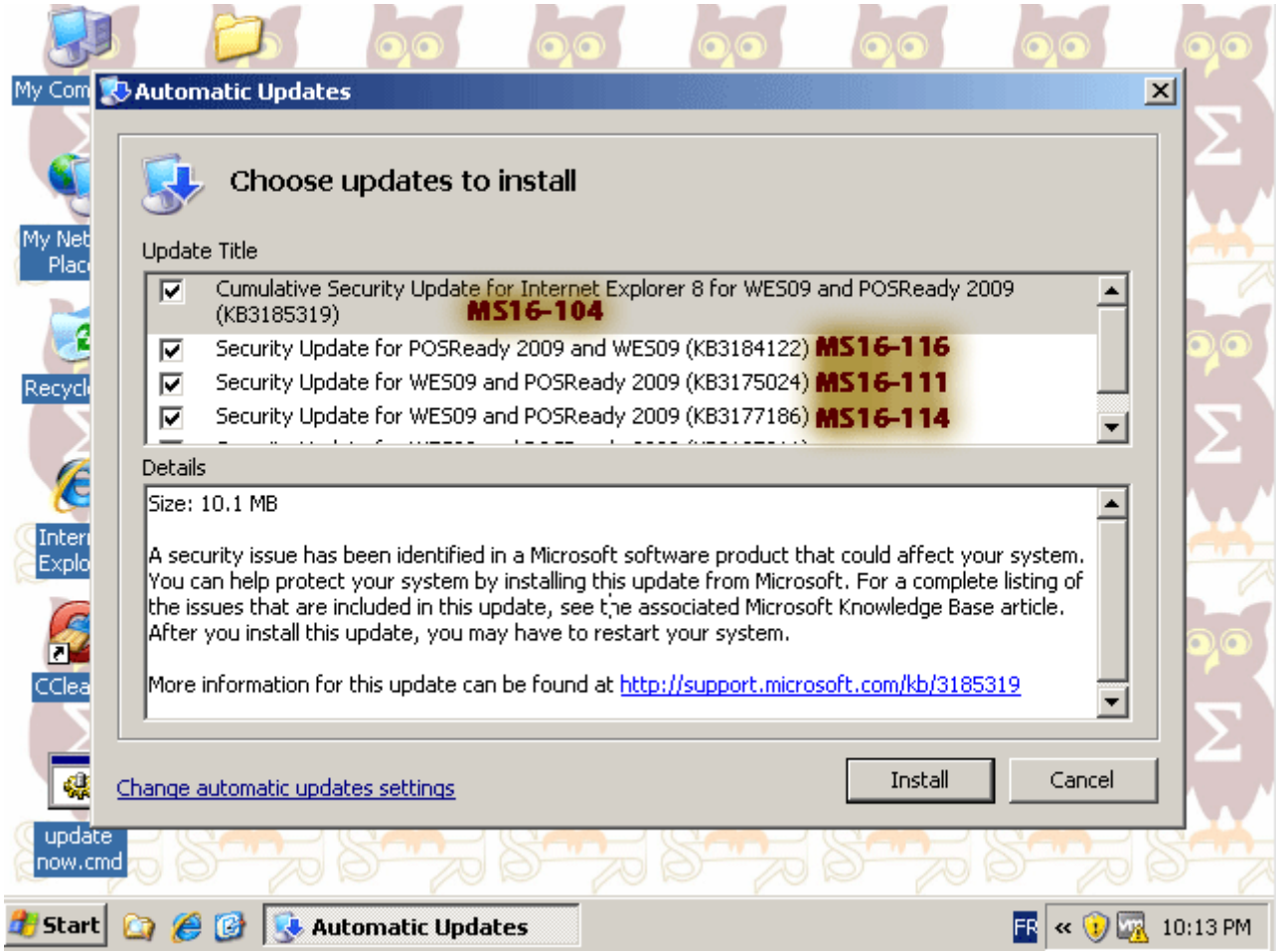
    https://github.com/offensive-security/exploit-database-bin-sploits/raw/master/sploits/40420.zip
    https://github.com/offensive-security/exploit-database-bin-sploits/raw/master/sploits/40421.zip
- Crédits:
  - ?

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

3181759 Elévation de privilège dans .Net

- V1.0 Première publication

3174644 Support de Diffie-Hellman

- V1.0 Support de DH 2048 bits, 3072 bits et 4096 bits. Par défaut 2048 sur Windows 10 et 1024 ailleurs

Failles / Bulletins / Advisories

Microsoft - Autre

Windows 2016 c’est pour octobre 2016

- Windows Containers, PowerShell 5.0, Credential Guard et Device Guard

http://www.nextinpact.com/news/101533-windows-server-2016-sera-disponible-en-version-finale-en-octobre.htm

Windows NT 4, publication du code source

https://t.co/gVSrpM0Nlb

Mise à jour de la politique des mises à jour et du support

- Support des produits sans fin
- Mais préavis de 12 mois minimum avant la fin du support

http://www.silicon.fr/microsoft-veut-mettre-fin-a-ses-produits-quand-il-le-souhaite-159631.html

Failles / Bulletins / Advisories

Microsoft - Autre

Springfield, le fuzzer en ligne de Microsoft

https://www.microsoft.com/en-us/springfield/

Microsoft recommande de supprimer le Journal

- Ceci fait suite aux différentes vulnérabilités d'exécution de code
- Est-ce un aveux d’échec ?

http://securityaffairs.co/wordpress/51678/hacking/windows-journal-removal.html

Usurpation de la base d’adresse de Microsoft Edge

- En cas de départ d’une page web malveillante

http://www.cracking.com.ar/demos/edgespoof/

Failles / Bulletins / Advisories

Antivirus

Désactiver l'antivirus Bit9 32bits (WoW64)

- En créant une clef de registre debug "parity.exe" pointant vers un malware

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image
  File Execution Options\parity.exe:debugger=malware.exe
```

https://twitter.com/waleedassar/status/780400925588455426/photo/1

Symantec, exécution de code lors du traitement de fichiers RAR

https://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20160919_00

Failles / Bulletins / Advisories

Système (principales failles)

OpenSSL

- Déni de service
  https://mta.openssl.org/pipermail/openssl-announce/2016-September/000080.html
- Puis quelques jours après, exécution de code (premier correctif erroné)
  https://mta.openssl.org/pipermail/openssl-announce/2016-September/000083.html

SSH

- Déni de service
  https://marc.info/?l=openssh-commits&m=147441986212897&w=2

Wordpress, exécution de code à distance

- Grâce aux fichiers de langage et l'entête "Plural-Forms:"
  https://gist.github.com/anonymous/908a087b95035d9fc9ca46cef4984e97

MySQL, suite des 0days de l'été

http://seclists.org/fulldisclosure/2016/Sep/59

Le pilote Capcom.sys

- Désactivation de SMEP, exécution de code user-land, réactivation de SMEP
  https://www.unknowncheats.me/forum/general-programming-and-reversing/189625-capcom-sys-usage-example.html

Irssi 0.8.20

- Déni de service à distance mais l'exécution de code semble complexe
  https://irssi.org/2016/09/21/irssi-0.8.20-released/

Failles / Bulletins / Advisories

Réseau (principales failles)

Routeurs SOHO le retour : Dlink 932B LTE et DWR-932B

- Portes dérobées, compte dissimulé, exécution de code à distance…
- Code PIN WPS par défaut fonctionnel, injection de firmware à distance, pas de sécurité UPnP

  http://www.securityfocus.com/archive/1/539502

  http://seclists.org/fulldisclosure/2016/Sep/70

F5 BigIP

- Extraction et modification de la configuration à partir de Nat64

  http://www.security-database.com/detail.php?alert=CVE-2016-5745

- Exécution de code, déni de service, contournement des politiques de sécurité

  http://www.cert.ssi.gouv.fr/site/CERTFR-2016-AVI-280/CERTFR-2016-AVI-280.html

Cisco nouvelle vulnérabilité corrigée

- Découverte lors des travaux sur vulnérabilités de la NSA / Equation Group

  http://www.nextinpact.com/news/101528-cisco-corrige-faille-dans-ses-produits-ios-liee-aux-outils-nsa.htm

Proxy Bluecoat, exécution de code à distance

- Vulnérabilités liée à OpenSSL : récupération des clefs, exécution de code...

  http://cert.ssi.gouv.fr/site/CERTFR-2016-AVI-333/index.html

Failles / Bulletins / Advisories

Apple, Google, Facebook...

Apple iOS 10, le chiffrement des sauvegarde est plus faible

- Ajout d'une méthode de vérification alternative
  - Précédemment AES256 CBC+IV à nul
  - Brute force à 6 millions de password/sec. contre 2 400 précédemment

http://blog.elcomsoft.com/2016/09/ios-10-security-weakness-discovered-backup-passwords-much-easier-to-break/

Apple Mac OS X, élévation de privilèges locale

- Adaptation des vulnérabilités utilisées par Pegasus

https://jaq.alibaba.com/community/art/show?articleid=532

Apple iOS 9, nouvelle explication des vulnérabilités utilisées par Pegasus

- Excellente explication (et PoC).

http://jndok.github.io/2016/10/04/pegasus-writeup/

Contourner Samsung Knox

https://media.wix.com/ugd/4e84e6_668d564cc447434a9a8fda3c13a63f6a.pdf

Failles / Bulletins / Advisories

Divers

Audit des HSM Nitrokey

- Extraction des clefs privées

  https://raymii.org/s/articles/Decrypt_NitroKey_HSM_or_SmartCard-HSM_private_keys.html

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

ThinkPwn, ce n’est pas fini…

https://github.com/Cr4sh/ThinkPwn

Lire des livres à distance

- Grâce à des ondes en terahertz

https://www.engadget.com/2016/09/12/mit-reads-closed-books-with-radiation/

Reconnaissance faciale 2.0, même pixélisé

https://www.wired.com/2016/09/machine-learning-can-identify-pixelated-faces-researchers-show/

Ajouter une porte dérobée aux nombres premiers

http://caramba.inria.fr/hsnfs1024.html

Fraude au paiement NFC, ca commence !

- Rapport d’Europol

http://www.bbc.com/news/technology-37495102?linkId=29351585

Les Macro Office sont majoritairement exécutées sous leur forme P-Code

- Stockées sous 3 formes:
  - Source Code
  - Pseudo Code (précompilé)
  - Execode, plus rapide à exécuter
- Modifier le source code d'une macro malveillante pour contourner les solutions de sécurité

  https://github.com/bontchev/pcodedmp

Objects connectés (IoT), après Sigfox, c'est au tour LoRaWan

- Problème de chiffrement avec l'utilisation d'une variante de CTR faible

  http://www.01net.com/actualites/objets-connectes-les-reseaux-lorawan-vulnerables-aux-attaques-de-hackers-1042538.html
- Une réponse et les commentaires de Renaud

  https://docs.google.com/document/d/1bXYguvRaH-5VqOgD490boLvI-G7_GP92n3V3Dl0ctfg/edit

Piratages, Malwares, spam, fraudes et DDoS

Malware

Rançongiciel Wildfire, un outil pour déchiffrer les fichiers

http://www.zdnet.com/article/wildfire-ransomware-code-cracked-victims-can-now-unlock-encrypted-files-for-free/

Rétro-ingénierie du Rançongiciel mamba

https://blog.fortinet.com/2016/09/27/dissecting-mamba-the-disk-encrypting-ransomware

StrongPity, nouveau groupe d'espionnage

- Mêlant 0days et Water Holing
- Usurpant TrueCrypt et WinRar

https://threatpost.com/strongpity-apt-covets-secrets-of-crypto-users/121185/

Piratages, Malwares, spam, fraudes et DDoS
DDoS

Le retour des gros DDoS / botnet Mirai

- DDoS (665Gbps) sur le site de Brian Krebs suite à un article sur le sujet

  http://krebsonsecurity.com/2016/09/ddos-mitigation-firm-has-history-of-hijacks/

  http://krebsonsecurity.com/2016/09/ddos-mitigation-firm-has-history-of-hijacks/

- DDoS (1Tbps) sur OVH avec le même botnet composé d'IoT (caméras, NAS, routeurs SOHO)

  https://twitter.com/olesovhcom/status/779297257199964160

  https://www.ovh.com/fr/news/articles/a2367.goutte-ddos-n-a-pas-fait-deborder-le-vac

- L'attaquant arrête et publie son code

  https://github.com/jgamblin/Mirai-Source-Code/blob/master/ForumPost.txt

  https://github.com/jgamblin/Mirai-Source-Code/

  - Attention aux portes dérobées
    https://twitter.com/_odisseus/status/782329521680842756/photo/1
  - Revue du code source
    https://medium.com/@cjbarker/mirai-ddos-source-code-review-57269c4a68f#.9lvfg2ety
  - Le code se connecte sur un jeu vidéo textuel et multi-joueur !!?
    https://twitter.com/mikko/status/782840133536063488

L'avis de Schneier

- Les IoT… pas assez cher mon fils, pour être sécurisé

  https://www.schneier.com/blog/archives/2016/10/security_econom_1.html

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Boris* Gropaquet:
<< Vous suspendez nos athlètes? Nous piratons l'agence mondiale antidopage. Des questions ? >>
**Cousin de Gilles*

L'agence mondiale antidopage

- Attribution : Les Russes Fancy Bear ou APT28
  - Par les américains de CrowdStrike
- Publication d'éléments accusant les sportifs américains de dopage

https://www.wired.com/2016/09/anti-doping-agency-attack-shows-russian-hackers-getting-bolder/

Piratage du DNC, la suite

- Le gouvernement américain accuse ouvertement la Russie

https://www.washingtonpost.com/world/national-security/us-government-officially-accuses-russia-of-hacking-campaign-to-influence-elections/2016/10/07/4e0b9654-8cbf-11e6-875e-2c1bfe943b66_story.html

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Fin d'année difficile pour Yahoo : compromission et espionnage

- Vol de 500 millions de données datant de 2014

  http://www.lefigaro.fr/flash-eco/2016/09/22/97002-20160922FILWWW00342-yahoo-confirme-le-piratage-de-500-millions-de-comptes.php

- Espionnage des mails des utilisateurs
  - Logiciel de la NSA, ajouté à l'anti-spam/malware sous forme de boîte noire
  - Objectif : détecter des terroristes islamo-nazi-pédophile-sauriens 😜 à partir de mots clefs
  - Détecté par la sécurité Yahoo et supposé être un RootKit de hackeurs
- Finalement, Verizon et Yahoo font la paire ✌🏻
  - Un technicien accusé de vendre les données personnelles des clients depuis des années (localisation et données d'appel)

  https://www.engadget.com/2016/09/28/verizon-technician-stole-customer-call-location-data/

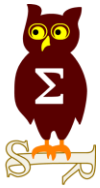
Un banque taïwanaise bloque ses ATM/DAB/GAB suite à un vol grâce à un malware

http://www.reuters.com/article/us-taiwan-banks-theft-idUSKCN0ZS19E

McDonnell Douglas F-15 Eagle, fuite de 42 000 documents

- Hautement plus critique que les 3 docs techniques de DCNS 😝

  http://www.reuters.com/article/us-northkorea-southkorea-cyber-idUSKCN0YZ0BE



Nouveautés, outils et techniques

ANSSI, mise à jour des recommandations TLS

- TLS 1.3 est le nouveau standard

  http://www.ssi.gouv.fr/uploads/2016/09/guide_tls_v1.1.pdf

shellsploit-library, une librairie pour développer ses propres exploits

https://github.com/b3mb4m/shellsploit-library

Mimikatz “Tiramisu Nutella+Speculoos”

- Permet de récupérer le code PIN des cartes à puce

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

Fluxion, attaquez du WPA/WPA2 sans brute force

- Crée un faux point d’accès
- Dé-authentifie les utilisateurs et capture la nouvelle authentification

http://www.kitploit.com/2016/10/fluxion-wpawpa2-security-hacked-without.html

Pentest

Techniques & outils

Invoke-Obfuscation, obfuscation de code PowerShell

https://github.com/danielbohannon/Invoke-Obfuscation

Contourner les listes blanches d'application (AppLocker) avec MSBuild

https://github.com/xorrior/RandomPS-Scripts/blob/master/Invoke-ExecuteMSBuild.ps1

Contourner les listes blanches d'application (AppLocker) avec C#

- Et le véritable outil encodé en base 64

http://subt0x10.blogspot.fr/2016/09/application-whitelisting-bypass-csiexe.html

Contourner les signatures d'un antivirus pour un PDF contenant un exploit

https://blog.digitalsecurity.fr/blog/Contourner-la-detection-AV-sur-un-exploit-PDF/

Cheat Sheet sur les désérialisations Java

- Sur les attaques par désérialisations 😊

https://github.com/GrrrDog/Java-Deserialization-Cheat-Sheet

VSAudit, pour auditer de la VOIP

https://github.com/sanvil/vsaudit

Pentest
Techniques & outils

Persistance Windows avec les “Failure Command” des services

1. Choisir un service inutile
2. Supprimer ses DLL
3. Configurer lui un script malveillant en cas de défaillance 😈

https://twitter.com/newsoft/status/775952760273383424

https://technet.microsoft.com/en-us/library/cc742019(v=ws.11).aspx#BKMK_remarks

Persistance, élévation de privilèges, pivot grâce à Microsoft SQL et PowerShell

- Présentation à la conférence DerbyCon 2016

http://www.slideshare.net/nullbind/derbycon2016-hacking-sql-server-on-scale-with-powershell

RC Exploiter, scan et brute force sur les protocoles classiques

- Proche de l’Hydra et Patator et Ncrack, avec l’exploitation en plus

https://sourceforge.net/p/rcexploiter/wiki/RC-EXPLOITER%20WIKI/

(re)-découvrez PowerShell

https://github.com/janikvonrotz/awesome-powershell

Détecter les “Failure Command” de Windows

- En 143 caractères 😎

```
gsv|foreach($_){if((gi($p="HKLM:\SYSTEM\CurrentControlSet\services\$($n=
$_.name)")).property-like($f="FailureCommand")){"$n $((gp $p $f).$f)"}}
```

Swift propose un reporting quotidien pour ~~empêcher~~ détecter les fraudes

- A partir de Décembre 2016, Swift enverra un rapport quotidien des transactions

  http://www.lemondeinformatique.fr/actualites/lire-swift-mise-sur-le-reporting-quotidien-pour-endiguer-les-fraudes-65992.html

Les Macro Office sont majoritairement exécutées sous leur forme P-Code

- Elles sont stockées sous 3 formes : Source Code, Pseudo Code et Execode
- Les outils et équipements de sécurité se focalisent sur le Source Code
- pcodedmp.py permet d’extraire les P-Codes

  https://github.com/bontchev/pcodedmp

Pentest
Défense

Installer et configurer Microsoft LAPS / Local Administrator Password Solution

- Scripts PowerShell inclus 😎

https://learn-powershell.net/2016/10/08/setting-up-local-administrator-password-solution-laps/

LittleFlocker, pour protéger votre Mac des malwares

https://www.littleflocker.com/

Voir le trafic SSL/TLS de son Android

- Nécessite de patcher
- Frida serait-il plus simple ?

https://blog.securityevaluators.com/how-to-view-tls-traffic-in-androids-logs-6a42ca7a6e55#.xi5wr3lxc

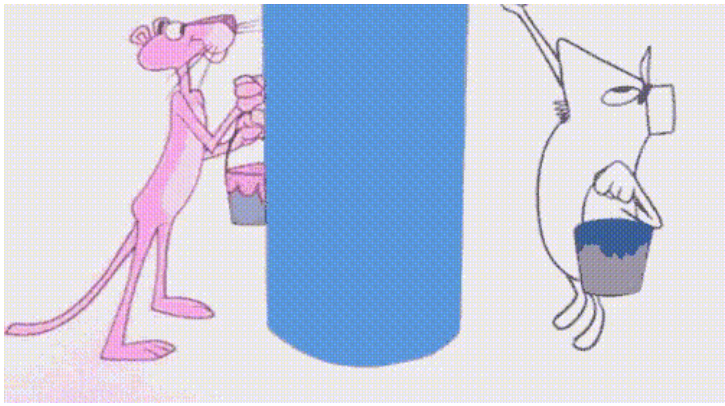
VolatilityBot, automatiser l'analyse de la mémoire

https://github.com/mkorman90/VolatilityBot

AIMSICD, détecter les IMSI catcher avec un Android

https://n0where.net/imsi-catcher-aimsicd/

PowerShell Empire <1.6



- Écraser n'importe quel fichier sur le serveur de contrôle
  - Si l'attaquant télécharge quelque chose

https://github.com/adaptivethreat/Empire/commit/f030cf6

Cobalt Strike

- Directory traversal et exécutions de code à distance

http://blog.cobaltstrike.com/2016/10/03/cobalt-strike-3-5-1-important-security-update/

http://blog.cobaltstrike.com/2016/09/28/cobalt-strike-rce-active-exploitation-reported/

Metasploit

- Exécution de code avant authentification
- Il y'a même un module Metasploit pour exploiter Metasploit

https://github.com/justinsteven/advisories/blob/master/2016_metasploit_rce_static_key_deserialization.md

Nouveautés (logiciel, langage, protocole...)

Open Source

Cappsule, la virtualisation par Quarkslab

- Fork du système démarré avec snapshot de la mémoire

http://blog.quarkslab.com/on-the-fly-virtualization-with-cappsule.html

OsQuery pour Windows

Instrumentalisation du système

https://blog.trailofbits.com/2016/09/27/windows-network-security-now-easier-with-osquery/

Frida 8.0.3

- 65% plus rapide

http://www.frida.re/news/2016/10/04/frida-8-0-released/

UEFITool, pour voir et éditer son firmware UEFI

https://n0where.net/uefi-firmware-image-viewer-uefitool/

Analyser un firmware avec Binwalk

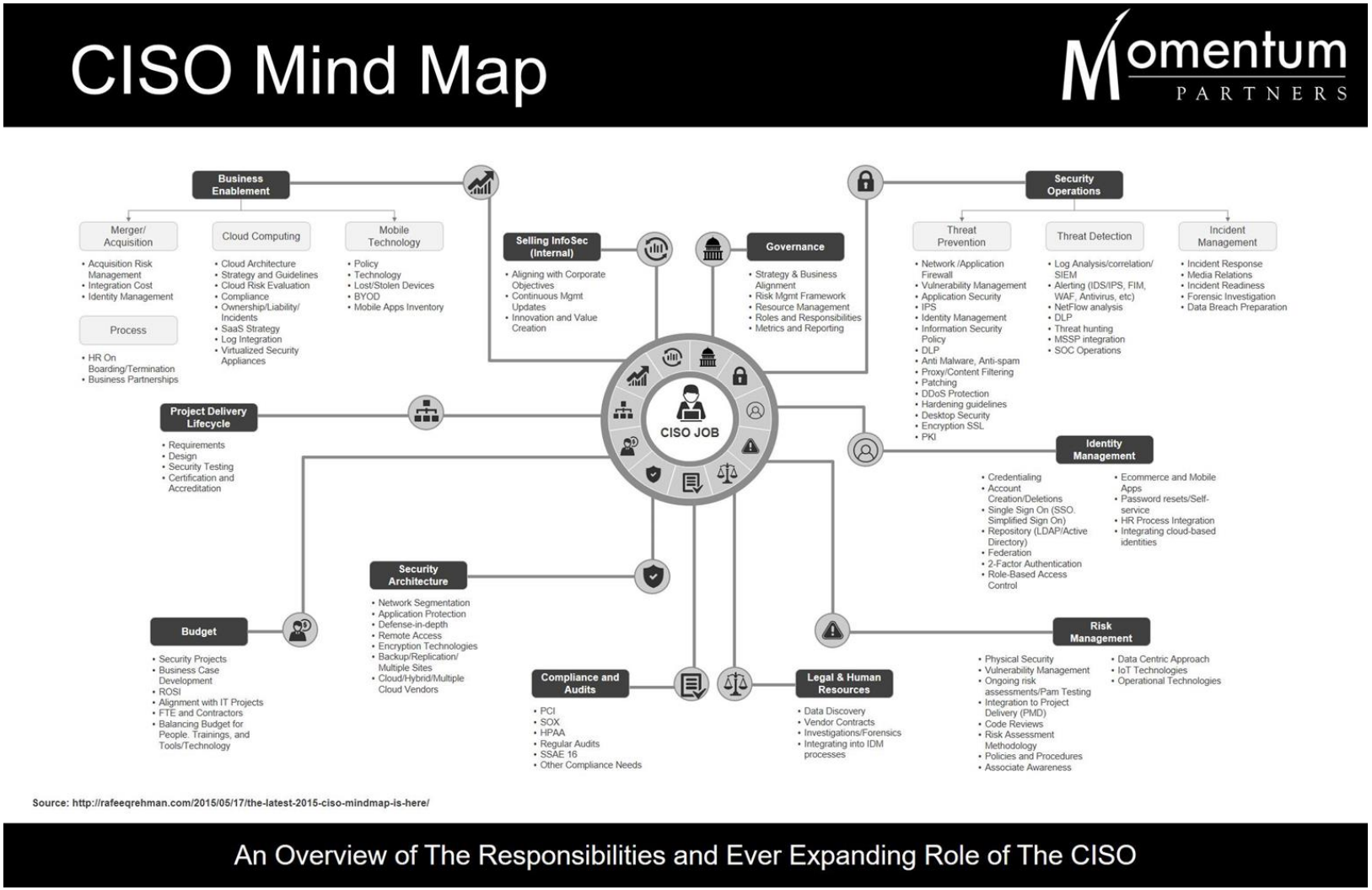
https://n0where.net/firmware-analysis-tool/

Nouveautés (logiciel, langage, protocole...)

Open Source

Un mind-map pour nos RSSI préférés

https://www.aurorait.com/wp-content/uploads/2016/06/CisoMindMap.jpg



Business et Politique

Droit / Politique

France

La France et le Japon unissent leur savoir-faire

- 7 groupes de travail : Méthodes formelles, Cryptographie, Analyse des malwares, Systèmes embarqués et IoT, Privacy, Réseau et un dernier non définit

  http://www.globalsecuritymag.fr/Cybersecurite-la-France-et-le,20160927,65637.html

ANSSI, les recommandations de base contre les rançongiciels

https://www.ssi.gouv.fr/actualite/ne-soyez-plus-otage-des-rancongiciels/

Droit / Politique
International

Il ne fait pas bon être “White Hat” en Chine

- Arrestation de plusieurs membres de Wooyun, communauté White

  http://www.ibtimes.co.uk/china-arrests-ethical-hacker-organisation-wooyuns-founder-1573538

Concours de recherche de vulnérabilité Android par Google Project Zero

- Premier prix à $200,000

  https://googleprojectzero.blogspot.fr/2016/09/announcing-project-zero-prize.html

Google Allo, enregistre à vie tous les messages

- Pour les rendre disponibles aux forces de l’ordre

  http://www.theverge.com/2016/9/21/12994362/allo-privacy-message-logs-google

iPhone de la tuerie de San Bernardino, le FBI attaqué

- Transparence sur l’utilisation des fonds publics = communiquer le prix et les détail de la vulnérabilité

  http://www.nextinpact.com/news/101421-iphone-verrouille-fbi-attaque-pour-utilisation-dune-faille-secrete.htm

Droit / Politique
International

Un autre Whistleblower venant de Booz Allen Hamilton (sous traitant de la NSA)

https://www.schneier.com/blog/archives/2016/10/nsa_contractor_.html

Equation Group

- Pleins de détails des codes d'exploitation

  https://www.ixiacom.com/company/blog/equation-groups-firewall-exploit-chain

- Les outils auraient été laissé sur un serveur par négligence

  http://www.reuters.com/article/us-cyber-nsa-tools-idUSKCN11S2MF

L'Allemagne refuse que Whatsapp partage le numéro de téléphone avec Facebook

- Tout du moins, la BFDI (CNIL allemande) est contre

  http://www.nextinpact.com/news/101550-lallemagne-refuse-que-whatsapp-partage-ses-donnees-avec-facebook.htm

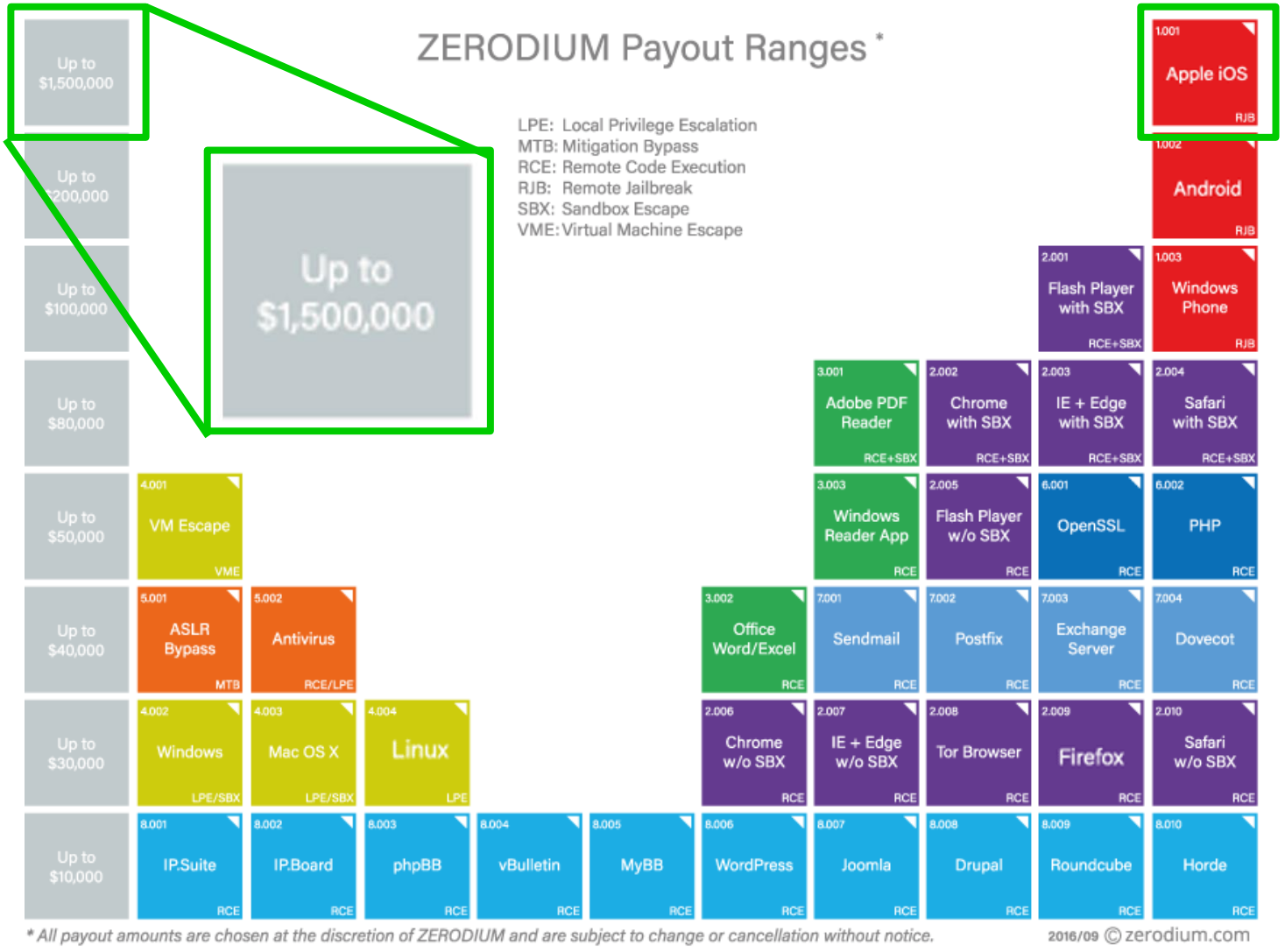
Epuisement des IPv4, le RIPE alerte

http://www.zdnet.fr/actualites/ipv6-avertissement-solennel-du-ripe-39837614.htm

Business
International

Zerodium, le jailbreak iOS passe à $1,500,000

https://www.zerodium.com/program.html



Conférences

Conférences

Passées

- Rien depuis le dernier mardi

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

Le clavier parfait ?

- Oscilloscope HP "1660CS-Series Logic Analyzer"

  https://twitter.com/bentsukun/status/775753995327565826

Faire du café en ligne de commande

- Après avoir fait de la rétro-ingénierie sur la cafetière

  https://www.evilsocket.net/2016/10/09/IoCOFFEE-Reversing-the-Smarter-Coffee-IoT-machine-protocol-to-make-coffee-using-terminal/

Lire un document Word docx pour les paranoïaques

```
#unzip -p ./file.docx|sed -e 's/<[^>]\{1,\}>//g; s/[^[:print:]]\{1,\}//g'
```

Divers / Trolls velus

Pirater les cerveaux

- En implantant de faux souvenirs

  http://motherboard.vice.com/read/memory-hacker-implant-false-memories-in-peoples-minds-julia-shaw-memory-illusion

- Une explication en français, sur une super chaîne Youtube

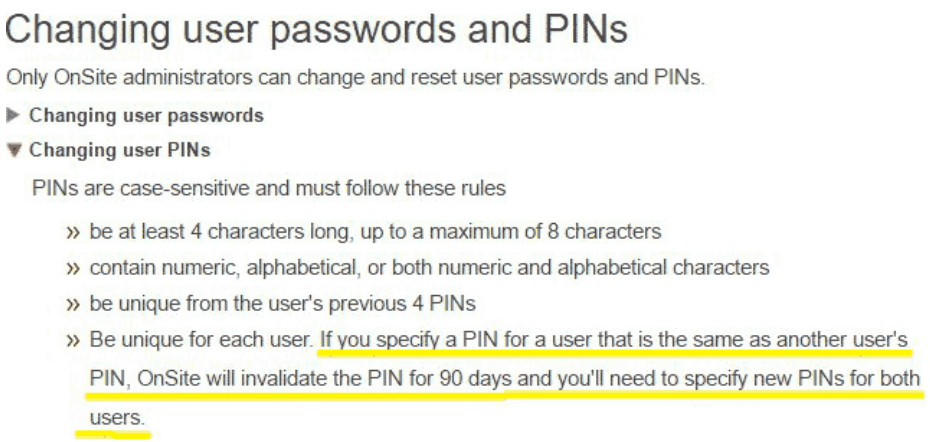
  https://www.youtube.com/watch?v=6G5SiVJnJM4

<<most powerful POS and eCommerce software>>

- Mais pas les plus puissants PIN

  https://twitter.com/PWTooStrong/status/778359986170826753

  https://www.lightspeedhq.com/



Changing user passwords and PINs

Only OnSite administrators can change and reset user passwords and PINs.

▶ **Changing user passwords**

▼ **Changing user PINs**

PINs are case-sensitive and must follow these rules

- » be at least 4 characters long, up to a maximum of 8 characters
- » contain numeric, alphabetical, or both numeric and alphabetical characters
- » be unique from the user's previous 4 PINs
- » Be unique for each user. If you specify a PIN for a user that is the same as another user's PIN, OnSite will invalidate the PIN for 90 days and you'll need to specify new PINs for both users.

Caramail est de retour, grâce à GMX

- Avec l'intégration d'OpenPGP

  http://www.itespresso.fr/gmx-caramail-chiffrement-139833.html

Divers / Trolls velus

L’antivirus Armadito cherche un community manager

http://www.teclib-edition.com/en/training-positions/#1454927583486-51a8b310-b5bb1c01-90a4

Pour contourner un antivirus fonctionnant par signature, il faut 1 à 2 minutes

- Pas pour écrire le malware, mais pour l'obfusquer

http://securityaffairs.co/wordpress/51714/malware/evading-antimalware.html

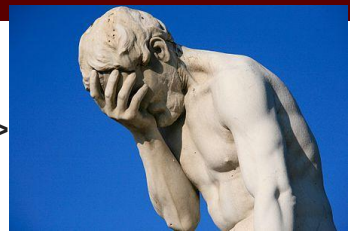
100% des entreprises ont des failles

- Tout comme 100% des pentests sont des réussites
- Et 100% des entreprises ont des utilisateurs qui cliquent 

http://korben.info/omg-100-grandes-entreprises-francaises-ont-failles-de-securite.html

Divers / Trolls velus

Quand la presse généraliste ne comprend rien aux Chaînes de Blocs



- <<Après un «cyber-casse», la technologie blockchain se cherche un avenir>>
- <<Les hackeurs n'ont pas vraiment triché>>

http://www.lemonde.fr/economie/article/2016/09/26/apres-un-cyber-casse-la-technologie-blockchain-se-cherche-un-avenir_5003434_3234.html

L'indentation à base d'espace ou tabulation, c'est surfait

- Passez aux points-virgules 

https://twitter.com/pelotom/status/779134762283732992/photo/1

```
/* "the pile o' semicolons" */
int main (int argc, char* arg[]) {
;;;;int i = 0
;;;;while (i < 10) {
;;;;;;;;printf("%d\n", i)
;;;;;;;;i ++
;;;;}
;;;;return 0
;}
```

Divers / Trolls velus

Être piraté coûte moins cher que de se sécuriser

- A vos marques, prêt, trolleeeezzzzz
  - Gros débat sur la liste SUR

http://www.theregister.co.uk/2016/09/23/if_your_company_has_terrible_it_security_that_could_be_a_rational_business_decision/

Publication du Top Level Domain de Corée du Nord

- Seulement 28 domaines !

https://github.com/mandatoryprogrammer/NorthKoreaDNSLeak#north-korea-kp-tld-zone-data

Brevet Google : manipuler le système nerveux à partir du champ magnétique d'un écran

- Avec des ondes de 2,4 Hz

https://www.google.com/patents/US6506148

Voir le frigidaire connecté… sous Windows 10

http://fr.ubergizmo.com/2016/09/05/ifa-2016-lg-frigo-xxl-windows-10.html

Prochains rendez-vous de l’OSSIR

Prochaine réunion

- Mardi 8 novembre 2016

After Work

- Mardi 25 octobre 2016

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous