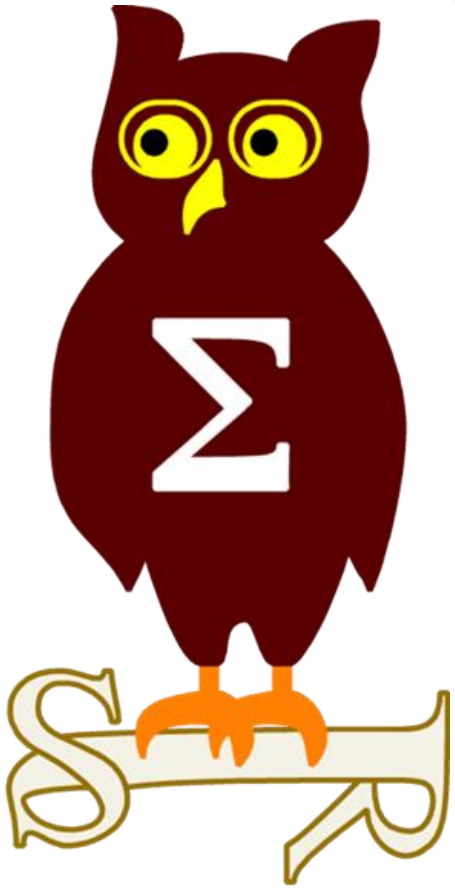
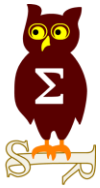


Revue d'actualité

14/06/2016

Préparée par

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



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-051 Vulnérabilités dans Internet Explorer (5 CVE) [Exploitabilité 1,3,1,2,2]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace KB3147458, KB3155413
- Exploit:
  - 1 x Corruptions de mémoire aboutissant à une exécution de code
  - 2 x Corruptions de mémoire dans un script VBScript aboutissant à une exécution de code
  - 1 x Contournement du filtrage anti XSS
  - 1 x Contournement ASLR (fuite d'information)
- Crédits:
  - Kai Kang (CVE-2016-0187)
  - Thomas Vanhoutte par ZDI de Trend Micro (CVE-2016-0194)
  - Zhang Yunhai de NSFOCUS (----------)
  - Zheng Huang de Baidu Security Lab par ZDI de Trend Micro (CVE-2016-0192)

MS16-052 Vulnérabilités dans Edge (4 CVE) [Exploitabilité 1,1,1,1]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace KB3147458, KB3147461
- Exploit:
  - 3 x Corruptions de mémoire dans un script VBScript aboutissant à une exécution de code
  - 1 x Corruptions de mémoire aboutissant à une exécution de code
- Crédits:
  - Bing Sun Intel Security Group (----------)
  - Brian Pak (cai) de Theori par Trend Micro's Zero Day Initiative (CVE-2016-0186)
  - Lokihart par ZDI de Trend Micro (CVE-2016-0191)
  - Simon Zuckerbraun par ZDI de Trend Micro (CVE-2016-0186)
  - Tencent Security Team Sniper par ZDI de Trend Micro (CVE-2016-0193)
  - Zheng Huang de Baidu Security Lab par ZDI de Trend Micro (CVE-2016-0192)

Dont 1 commune avec IE:

- CVE-2016-0192

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-053 Vulnérabilités dans JScript et VBScript (2 CVE) [Exploitabilité 1,0]

- Affecte:
  - VBScript 5.7 et 5.8 (Windows Vista, 2008)
  - Remplace KB3124625
- Exploit:
  - 2 x Corruptions de mémoire dans un script VBScript aboutissant à une exécution de code
    - Code d'exploitation public
- Crédits:
  - Kai Kang (CVE-2016-0187)

MS16-054 Vulnérabilités dans Microsoft Office (4 CVE) [Exploitabilité 2,1,2,1]

- Affecte:
  - Office 2007, 2010, 2013, 2013 RT, 2016, Mac 2011, Mac 2016
  - Remplace KB2760585, KB2760591, ...
- Exploit:
  - 4 x Corruptions de mémoire aboutissant à une exécution de code à l'ouverture d'un fichier Office
- Crédits:
  - An anonymous researcher par Beyond Security SecuriTeam (CVE-2016-0126)
  - Hao Linan de Qihoo 360Vulcan Team (CVE-2016-0126)
  - Lucas Leong de Trend Micro (CVE-2016-0183)
  - Steven Seeley de Source Incite par VeriSign iDefense Labs (CVE-2016-0140)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-055 Vulnérabilités dans GDI (5 CVE) [Exploitabilité 2,1,2,1,2]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace KB3035132, KB3124001, KB3147458, KB3147461
- Exploit:
  - 3 x Exécutions de code
  - 2 x Contournement ASLR (fuite d'information)

    https://bugs.chromium.org/p/project-zero/issues/detail?id=722

    https://bugs.chromium.org/p/project-zero/issues/detail?id=729

    https://bugs.chromium.org/p/project-zero/issues/detail?id=731
- Crédits:
  - Henry Li(zenhumany) de Trend Micro (CVE-2016-0184)
  - Mateusz Jurczyk de Google Project Zero (CVE-2016-0168, CVE-2016-0169, CVE-2016-0170)

MS16-056 Vulnérabilités dans le Journal Windows (1 CVE) [Exploitabilité 3]

- Affecte:
  - Windows (toutes versions supportes hors serveur)
  - Remplace KB3147458, KB3147461
- Exploit:
  - Exécutions de code à l'ouverture d'un fichier .JNT spécialement formaté
- Crédits:
  - Bingchang Liu de VARAS@IIE (CVE-2016-0182)
  - Jason Kratzer par VeriSign iDefense Labs (CVE-2016-0182)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-057 Vulnérabilités dans Windows Shell (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportes hors serveur)
  - Remplace KB3147458, KB3147461
- Exploit:
  - Exécutions de code à l'ouverture d'une page web
- Crédits:
  - Shi Ji (@Puzzor) de VARAS@IIE (CVE-2016-0179)

MS16-058 Vulnérabilité dans IIS (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows Vista, 2008
- Exploit:
  - Exécutions de code locale dans IIS (injection de DLL)

MS16-059 Vulnérabilités dans Media Player (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows Vista, 7, 8.1
  - Remplace KB3108669
- Exploit:
  - Exécutions de code à l'ouverture d'un fichier .MCL
    https://www.exploit-db.com/exploits/39805/
    `<application run="file:///\\127.0.0.1\c$\programdata\cpl.lnk"/>`
- Crédits:
  - Eduardo Braun Prado par ZDI de Trend Micro (CVE-2016-0185)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-060 Vulnérabilité noyau (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace KB3121212, KB3121212, KB3140410, KB3140410, KB3147458
- Exploit:
  - Elevation de privilège locale à partir des liens symboliques
- Crédits:
  - Loren Robinson et Alex Ionescu de CrowdStrike, Inc. (CVE-2016-0180)

MS16-061 Vulnérabilité dans les RPC (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace KB2978668, KB3140410, KB3147458, KB3147461
- Exploit:
  - Execution de code non authentifié sur les RPC
- Crédits:
  - Evgeny Kotkov et Ivan Zhakov de VisualSVN (CVE-2016-0178)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-062 Vulnérabilité noyau (7 CVE) [Exploitabilité 1,1,1,2,1,1,3]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace KB2976897, KB3139852, KB3145739, KB3147458, KB3147461, KB3147461
- Exploit:
  - 6 x Elevatione de privilège locale
  - 1 x Contournement ASLR
- Crédits:
  - Dhanesh Kizhakkinan de FireEye, Inc. (CVE-2016-0196)
  - Fermin J. Serna (----------)
  - Nils Sommer de bytegeist par Google Project Zero (CVE-2016-0171, CVE-2016-0173)
  - Qihoo 360Vulcan Team par ZDI de Trend Micro (CVE-2016-0173, CVE-2016-0196)
  - Tencent KeenLab par ZDI de Trend Micro (CVE-2016-0175, CVE-2016-0176)
  - Tencent Security Team Sniper par ZDI de Trend Micro (CVE-2016-0174)

MS16-064 Vulnérabilité dans Adobe Flash Payer (25 CVE) [Exploitabilité]

- Affecte:
  - Windows 8.1, 8.1RT, 10, 2012, 2012R2
  - Remplace KB3154132
- Exploit:
  - Exécutions de code
- Crédits:
  - ?

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-065 Déchiffrement TLS/SSL dans .Net (1 CVE) [Exploitabilité 3]

- Affecte:
  - Windows (toutes versions supportes) ,Remplace KB2972107, KB2978041, KB2978042, KB3140768
- Exploit:
  - Fuite d'information SSL/TLS par l'envoie de données non chiffrées, permettant le déchiffrement

MS16-066 Contournement HCVI (Implements Hypervisor Code Integrity) (1 CVE) [Exploitabilité 3]

- Affecte:
  - Windows 10 , Remplace KB3147458, KB3147461
- Exploit:
  - Contournement de HCVI localement
- Crédits:
  - Rafal Wojtczuk de Bromium (CVE-2016-0181)

MS16-067 Vulnérabilité RDP / RemoteFX (1 CVE) [Exploitabilité 3]

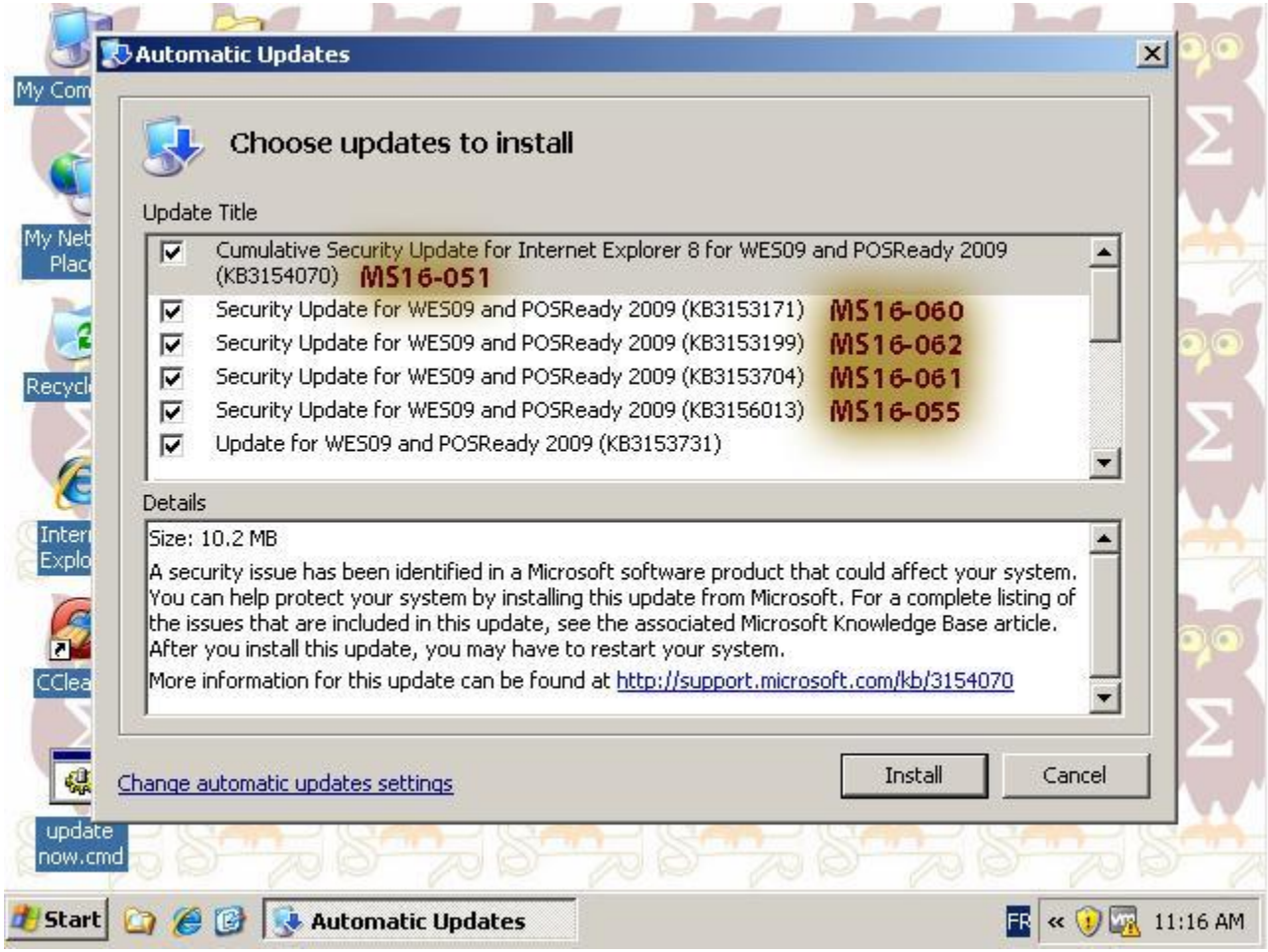
- Affecte:
  - Windows (touts versions supportes)
- Exploit:
  - Accès d'un autre utilisateur à une clef USB montée par en RDP en RemoteFX
- Crédits:
  - Sandeep Kumar, Citrix Systems Inc. (CVE-2016-0190)

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

2880823 Déprécation de l'algorithme SHA-1 pour les "Root CA"

- V2.0 ajout d'un lien vers la polituque de Microsoft concernant SHA1 : http://aka.ms/sha1

3155527 Mise à jour des suites cryptographiques supportant FalseStart

- V1.0 publication initiale

Failles / Bulletins / Advisories

Microsoft - Autre

0-day en vente $90,000 sur le marché noir

- Élévation de privilège locale

  https://www.helpnetsecurity.com/2016/06/01/windows-zero-day-exploit/

0-day : contournement du filtre XSS d'Internet Explorer

http://0day.today/exploit/25477

```
http://challenge.hackvertor.co.uk/xss.php?x=%3Cmeta%20charset=cp1025%3E%27%20L%C9%86%D9%81%D4%85%40%C9%84~[%40%D6%95%D4%96%E4%A2%85%D6%A5%C5%99~m~%60JZ^NNm^mm~mNm^mmmm~mmNmm^mmmmmm~mmmmNmm^[JMOO}}N}}]JmZNMOO}}N}}]JmmZNMOO}}N}}]JmmmmZNMO}}N}}]JmZNM[N}}]JmmmmmmZZMm]n
```

Microsoft Azure AD interdit les mots de passe ayant déjà fuité

- A noter que Microsoft voit passer 10 millions d'attaques par jour sur les comptes Azure

  https://blogs.technet.microsoft.com/ad/2016/05/24/another-117m-leaked-usernames-and-passwords-new-best-practices-azuread-and-msa-can-help/

Failles / Bulletins / Advisories

Microsoft - Windows 10 is coming

Windows 10 is coming !!!

Failles / Bulletins / Advisories

Antivirus

ClamAV 0-day

- Envoi de commandes CLAMAV, **sans authentification**, à distance sur le port 3310 
- Commandes possibles : SCAN, SHUTDOWN, VERSION
  - Plus de 5600 systèmes accessibles directement depuis Internet

https://twitter.com/nitr0usmx/status/740673507684679680

https://twitter.com/ErrataRob/status/742211624250003456

Sophos Safe Guard Enterprise Disk Encryption

- Bootloader OpenBSD de 2006 avec des exploits publics
- Chiffrement de ce bootloader avec une clef symétrique commune à tous (0x82564557)
- Existence d'une clef maître, codée en dur dans le bootloader
- Clef de déchiffrement du disque dérivée de cette clef et d'une information du disque

https://www.logicista.com/2016/sophosboot

Failles / Bulletins / Advisories

Système (principales failles)

VMware NSX

- Fuite d'information sensibles

  https://www.vmware.com/security/advisories/VMSA-2016-0007.html

VMWare vCenter

- Execution de code par désérialisation Java sur le service RMI d'Oracle JRE JMX

  https://www.vmware.com/security/advisories/VMSA-2016-0005.html

VLC <= 2.2.3

- Execution de code à la lecture d'une vidéo QuickTime

  http://www.videolan.org/security/sa1601.html

Failles / Bulletins / Advisories

Système (principales failles)

Boufficiel (bloatware) ASUS LiveUpdate

- Mise à jour du firmware en HTTP, injection dans un XML et exécution de code

  http://teletext.zaibatsutel.net/post/145370716258/deadupdate-or-how-i-learned-to-stop-worrying-and

Lenovo Solution Center (LSC)

- Elevation de privilèges locale + CSRF depuis le service backend, installé par défaut sur les PC Lenovo

  https://support.lenovo.com/fr/en/product_security/len_4326

Lenovo, Dell, HP, Acer : problèmes de mise à jour des Boufficiel

http://www.theregister.co.uk/2016/05/31/laptop_security_weak_crypto/

OEM vendor and software version	Manifest Transmitted Over TLS	Signed Manifest	Updates Transmitted Over TLS	Authenticode Validation
Acer	✗	✗	✗	✗
Asus	✗	✗	✗	✗
Dell DFS 2.1.3.1	✓	✗	✓	✗
Dell DFS 2.4.3.0	✓	✗	✓	✓
Dell Update 1.8.114.0	✓	✗	✓	✓
Hewlett-Packard HPSF 8	✗	✗	✓	✓
Lenovo UpdateAgent 1.0.0.4	✗	✗	✗	✗
Lenovo Solution Center 3.1.001	✓	✓	✓	✓

Failles / Bulletins / Advisories

Système (principales failles)

Keepass, mise à jour en HTTP

- Redirection vers une fausse passe de mise à jour et execution de code

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

Mise à jour en HTTP : un outil pour les exploiter tous

https://github.com/infobyte/evilgrade

- Un outil pour désinstaller les boufficiels

  http://www.decrap.org/

ASUS, accès R/W à toute la mémoire par un utilisateur sans privilèges

- Plus d'un an pour… ne pas corriger le problème !!!

  https://codeinsecurity.wordpress.com/2016/06/12/asus-uefi-update-driver-physical-memory-readwrite/

SAP

- Vulnérabilité d'exécution de code Java à distance, vieille de plus de 6 ans

  http://linkis.com/theregister.co.uk/Et7BE

Failles / Bulletins / Advisories

Réseau (principales failles)

Juniper Junos Space (Outil de gestion du réseau)

- Exécution de code à distance (désérialisation Java)
- Contournement de la politique de sécurité
- Utilisation de RC4
- Et pleins d’autres

http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10727&cat=SIRT_1&actp=LIST

Citrix NetScaler

- Vol des identifiants d'un autre utilisateur, simplement en modifiant son propre cookie

http://support.citrix.com/article/CTX213313

Firewall Cisco ASA

- Exécution de code non authentifé, si IPSec est activé (lors de la négociation)

http://linkis.com/com/vTavq

Failles / Bulletins / Advisories

Apple, Google, Facebook...

Quicktime, vulnérable à des exécutions de code à distance

- Abandonné sous Windows, donc vulnérable à jamais

  http://www.silicon.fr/quicktime-pour-windows-verole-apple-le-laisse-tomber-145004.html

- La défense américaine recommande de le désinstaller

  https://www.us-cert.gov/ncas/alerts/TA16-105A

Failles / Bulletins / Advisories

Divers

Vulnérabilité dans Nagios

- Exécution de commande via injection SQL non-authentifiée

  http://fr.0day.today/exploit/25398

Typosquatting sur les gestionnaires de paquet

- Étude académique et tests à large échelle de distribution de paquets malveillant, permettant l'exécution de code à distance, avec des noms proches et/ou similaires à des paquets reconnus

  http://incolumitas.com/2016/06/08/typosquatting-package-managers/

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Voitures

Pirater une Mistibushi Outlander hybride

- La voiture dispose d'un SSID WiFi, avec une clé codée en dur, cassée en 4 jours
- Possible de désactiver l'alarme de la voiture depuis le WiFi

https://www.pentestpartners.com/blog/hacking-the-mitsubishi-outlander-phev-hybrid-suv/

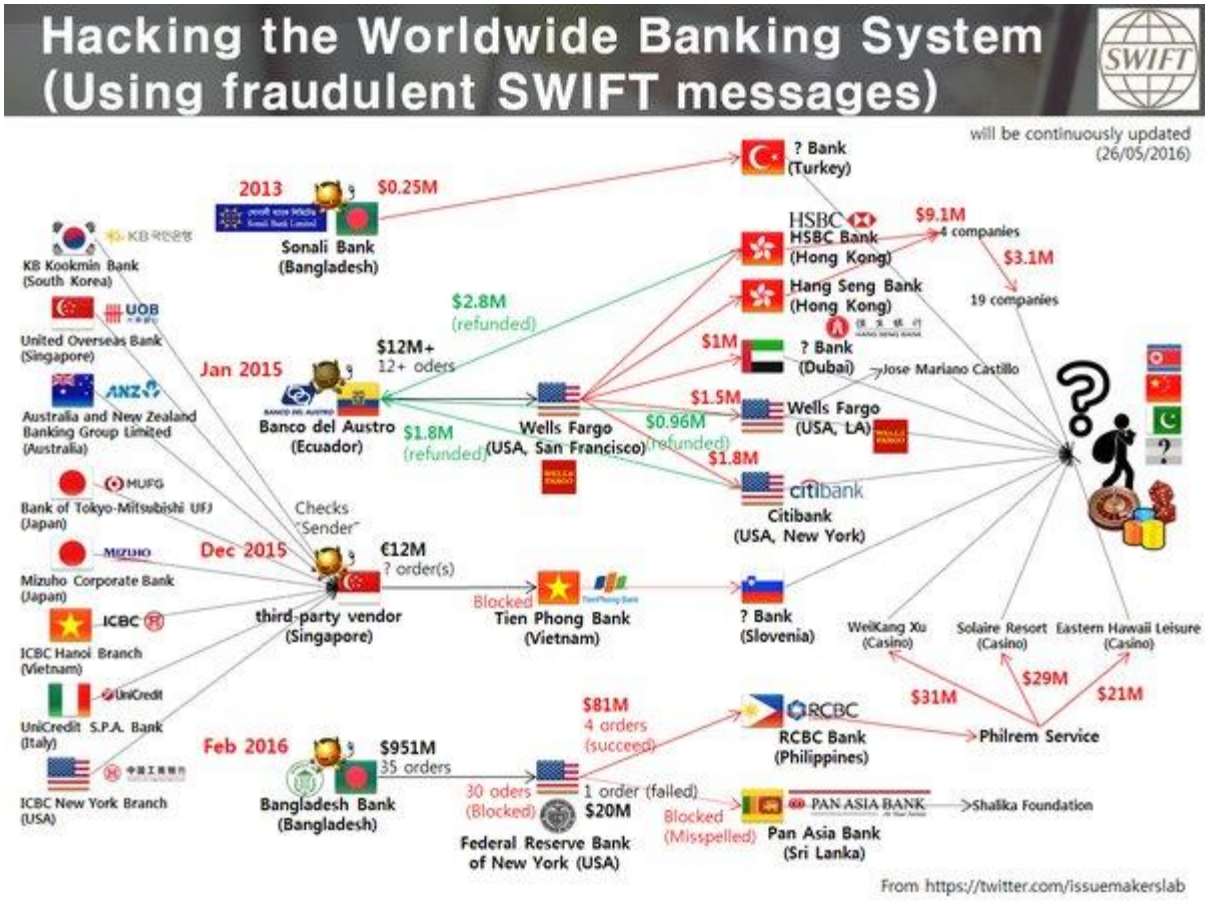
Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Piratage de Swift

- Détournement de $80 millions de la banque du Bangladesh vers des casinos Philippins
  - $951 millions tenté mais manqué du fait d'une faute d'orthorgraphe dans le nom du destinataire (Shalika Fandation au lieu de Shalika Foundation)

http://baesystemsai.blogspot.fr/2016/04/two-bytes-to-951m.html
https://twitter.com/issuemakerslab/status/735689375397208068/photo/1



Vulnérabilités dans Facebook Messenger

- Altération de l'historique des messages

  http://blog.checkpoint.com/2016/06/07/facebook-maliciouschat/

Les suggestions de Castorama sont… originales

http://www.huffingtonpost.fr/2016/06/08/suggestions-recherche-castorama-twitter-buzz_n_10356236.html

- Les meilleures sont sur castoche

  http://castoche.fr/

Récupération des clefs RSA par écoute du buit

- Après la récupération par imposition des mains (cf. revue du 2014-09-09)

  http://securityaffairs.co/wordpress/48025/hacking/encryption-keys-exfiltration.html

Piratages, Malwares, spam, fraudes et DDoS

Malware

Crypto-fail dans un rançongiciel

http://esec-pentest.sogeti.com/posts/2016/06/07/the-story-of-yet-another-ransomfailware.html

TeslaCrypt, publication de la clef maitre

- Un chercheur d'ESET a simplement contacté le SAV des criminels pour demander la clef

http://www.bleepingcomputer.com/news/security/teslacrypt-shuts-down-and-releases-master-decryption-key/

/http://www.welivesecurity.com/2016/05/18/eset-releases-decryptor-recent-variants-teslacrypt-ransomware/

33% des sociétés anglaises achètent des bitcoins en prévision de malwares

http://www.financemagnates.com/cryptocurrency/news/33-of-uk-firms-are-buying-bitcoin-in-anticipation-for-cyber-attacks/

Une porte dérobée matérielle analogique dans les processeurs

http://ieee-security.org/TC/SP2016/papers/0824a018.pdf

Piratages, Malwares, spam, fraudes et DDoS

Scada

IRONGATE, un nouveau malware ciblant les SI industriels découvert par FireEye

- Cible les systèmes Siemens
  - Les simulateurs Siemens, pas les équipements réèls
- Remplace une dll pour intercepter les échanges entre les automates et le poste de supervision
- Enregistre 5 secondes de trafic “normal” et le rejoue à l’opérateur, tout en envoyant des données différentres aux automates
- Détecte les sandboxes

https://www.fireeye.com/blog/threat-research/2016/06/irongate_ics_malware.html

Piratages, Malwares, spam, fraudes et DDoS

Internet des Objets

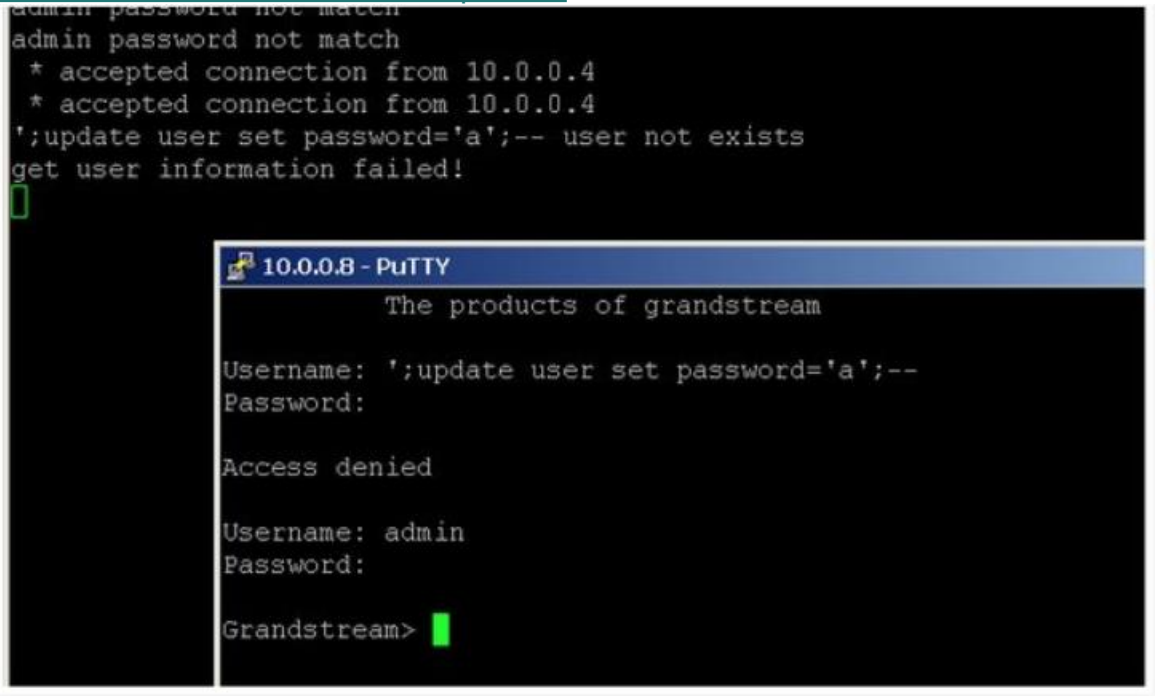
Rétro-inégnierie d'une caméra IP

http://www.contextis.com/resources/blog/push-hack-reverse-engineering-ip-camera/

Injection SQL dans une Webcam au login

- pour changer le mot de passe administrateur

https://twitter.com/Viss/status/738102212660846592/photo/1



It executed the statement below:
select * from users where name = ''; update user set password='a';--';

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Piratage ~~probable~~ confirmé de TeamViewer

- Infrastructure coupée (DDoS?) et serveur DNS pointant vers la Chine
- Teamviewer nie, mais de nombreux utilisateurs témoignent d'une compromission

  http://www.theregister.co.uk/2016/06/01/teamviewer_mass_breach_report/
- Teamviewer reconnaît la compromission
  - Qui serait liée aux fuites Linkedin, MySpace...

  http://arstechnica.com/security/2016/06/teamviewer-says-theres-no-evidence-of-2fa-bypass-in-mass-account-hack/

Pornhub, compromission et vente d'accès aux serveurs à $1,000

www.csoonline.com/article/3070420/security/pornhub-said-to-be-compromised-shell-access-available-for-1-000.html

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Lets Encrypt, fuite de 7618 mails

- Venant de la mailling list

  http://www.developpez.com/actu/99833/L-autorite-de-certification-Let-s-Encrypt-expose-par-inadvertance-7618-adresses-mail-de-ses-utilisateurs-suite-a-un-bogue-dans-un-de-ses-systemes/

Linkedin, vol de 167 millions de comptes

- En vente ~~5~~ 2 bitcoins (~$1,300), sur le forum « The Real Deal »

  http://motherboard.vice.com/read/another-day-another-hack-117-million-linkedin-emails-and-password

Twitter, vol de 32 millions de comptes

- En vente 0,5 bitcoins (~$300), sur le forum « The Real Deal »

  http://www.journaldugeek.com/2016/06/10/millions-donnees-twitter-piratage/

Tumblr, vol de 65 millions de comptes (datant de 2013 ?)

- Mots de passe sous forme de condensat (hash) avec diversificateur (salt)
- En vente 0,15 bitcoins (~$100), sur le forum « The Real Deal »

  http://www.nextinpact.com/news/100067-tumblr-fuite-plus-65-millions-didentifiants.htm

MySpace, vol de 500 millions de comptes

- Dont 360 000 000 uniques

  https://nakedsecurity.sophos.com/2016/05/31/myspace-breach-could-be-the-biggest-ever-half-a-billion-passwords/

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Russie : Mail.ru, Yahoo!, Google, Microsoft -> vol de 270 millions d'adresses mails

http://gizmodo.com/russian-hackers-have-270-million-email-logins-includin-1774848936

Russi: VK.com, vol de 100 millions de comptes

- En vente 1 bitcoin (~$700), sur le forum « The Real Deal »

https://www.hackread.com/russian-vk-com-accounts-on-dark-web/

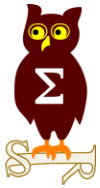
Le compte Twitter de Katy Perry piraté

http://www.bbc.co.uk/newsbeat/article/36416411/katy-perrys-twitter-account-was-hacked-she-didnt-tweet-taylor-swift

Comptes Linkedin, Twitter et Pinterest de Marc Zuckerberg piratés

- Mot de passe : "Dadada"

http://venturebeat.com/2016/06/05/mark-zuckerbergs-twitter-and-pinterests-accounts-hacked-linkedin-password-dump-likely-to-blame/



Nouveautés, outils et techniques

Apple embauche Jon Callas

- Légende de la cryptographie et cofondateur de PGP Corporation

  http://www.reuters.com/article/us-apple-encryption-callas-idUSKCN0YF2J1

Copier des fichiers via PowerShell remoting

http://powershell.com/cs/blogs/tips/archive/2016/05/24/copy-over-powershell-remoting-sessions.aspx

Spoofing de temps NTP

https://conference.hitb.org/hitbsecconf2016ams/materials/D2T1%20-%20Yuwei%20Zheng%20and%20Haoqi%20Shan%20-%20Forging%20a%20Wireless%20Time%20Signal%20to%20Attack%20NTP%20Servers.pdf

Outil d'attaque Wildcard linux

http://www.darknet.org.uk/2016/05/wildpwn-unix-wildcard-attack-tool/

Analyse sécurité de Microsoft Direct-Access

https://www.ernw.de/download/newsletter/ERNW_Newsletter_53_MS_DA_Security_Assessment_Signed.pdf

Contourner la protection antimalware de Microsoft

- Via le chargement de dll dans le dossier courant

http://cn33liz.blogspot.fr/2016/05/bypassing-amsi-using-powershell-5-dll.html

Backdoorer une dll

http://www.gironsec.com/blog/2016/06/backdooring-a-dll/

Pentest

Techniques & outils

15 méthodes pour contourner la politique d'exécution de PowerShell

https://blog.netspi.com/15-ways-to-bypass-the-powershell-execution-policy/

Injection de credential en mémoire avec Powershell

- Pour rester discret lors de la réutilisation de mots de passe volés

https://clymb3r.wordpress.com/2013/11/17/injecting-logon-credentials-with-powershell/

Récupérer les mots de passe en mémoire, comme Mimikatz, mais en Powershell

- Si UseLogonCredential est à 1

https://github.com/giMini/PowerMemory/tree/master/RWMC

Transférer un binaire sous Windows en ASCII

- Et le décoder avec “debug”

https://github.com/g0tmi1k/exe2hex

Pentest
Techniques & outils

Drakvuf

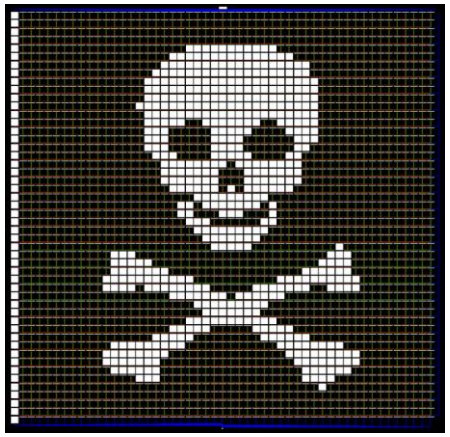
- Outil d'analyse de malware assez discret

  http://drakvuf.com/

Le retour du L33T Master Guru de l'obfuscation (cf. Revue du 2015-10-13)

- Publication de son outil de génération de graph à partir de dessins

  https://github.com/xoreaxeaxeax/REpsych



Comment tester des applications avec authentification Kerberos ?

https://www.insinuator.net/2016/02/how-to-test-kerberos-authenticated-web-applications/

Backdoor Factory 3.3.1

- Injection de shellcode automatisée en situation de Singe Intercepteur (MitM)

  http://www.darknet.org.uk/2016/05/backdoor-factory-bdf-patch-binaries-shellcode/

ADACLScan

- Outil de scan de permissions sur Active Directory en PowerShell

  https://adaclscan.codeplex.com/

File Server Resource Manager (FSRM)

- Rien de nouveau, mais pensez-y pour déclencher des actions en cas de rançongiciel

  http://www.it-connect.fr/fsrm-proteger-son-serveur-de-fichiers-des-ransomwares/

  https://blogs.technet.microsoft.com/heyscriptingguy/2012/07/20/use-powershell-to-create-a-permanent-wmi-event-to-launch-a-vbscript/

Désactiver Intel Management Engine ?

- C’est compliqué

  https://github.com/ptresearch/me-disablement

  https://github.com/ptresearch/me-disablement/raw/master/How%20to%20become%20the%20sole%20owner%20of%20your%20PC.pdf

Nouveautés (logiciel, langage, protocole...)

Open Source

CapTipper, rejouer du traffic

- Une alternative à xplico

  http://www.brunovalentin.com/securite-info/captipper-explorateur-trafic-http-malveillant/

Android Internals

https://github.com/keesj/gomo/wiki

PoshLZW

- Code de décompression en 688 octets pour Powershell 2.0

  https://github.com/mynameisv/PoshLZW

Nouveautés (logiciel, langage, protocole...)

Divers

Intel annonce le support matériel du Control Flow Integrity

- CET = Control-flow Enforcement Technology
- grsecurity propose des mesures similaires via le “module” RAP

http://blogs.intel.com/blog/intel-innovating-stop-cyber-attacks/

https://forums.grsecurity.net/viewtopic.php?f=7&t=4490

Scada

Divers

Vulnérabilités dans les routeurs BACNet de KMC Controls

https://ics-cert.us-cert.gov/advisories/ICSA-16-126-01

Modification du firmware sur les MOXA UC-7408-LX-Plus

- Poste de travail embarqué
- Possibilité de “briquer” définitivement l’équipement”

https://ics-cert.us-cert.gov/advisories/ICSA-16-152-01

Business et Politique

Business
International

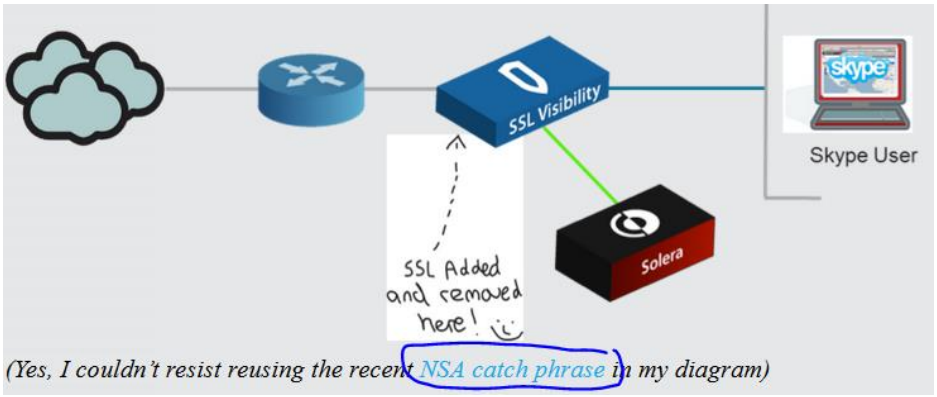
Symantec achète Bluecoat pour $4,6 milliards

- Et récupère donc Elastica, leader du CASB (Cloud Access Security Broker).

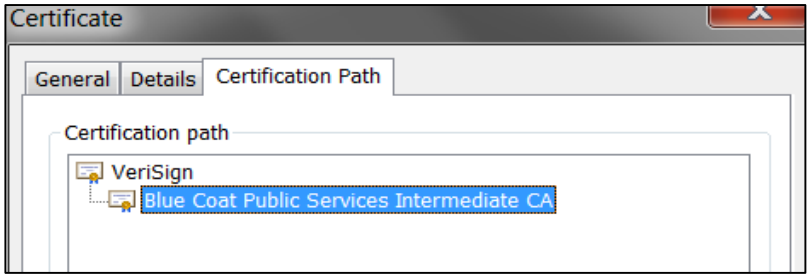
  http://www.zdnet.fr/actualites/symantec-s-offre-blue-coat-pour-46-milliards-de-dollars-39838220.htm

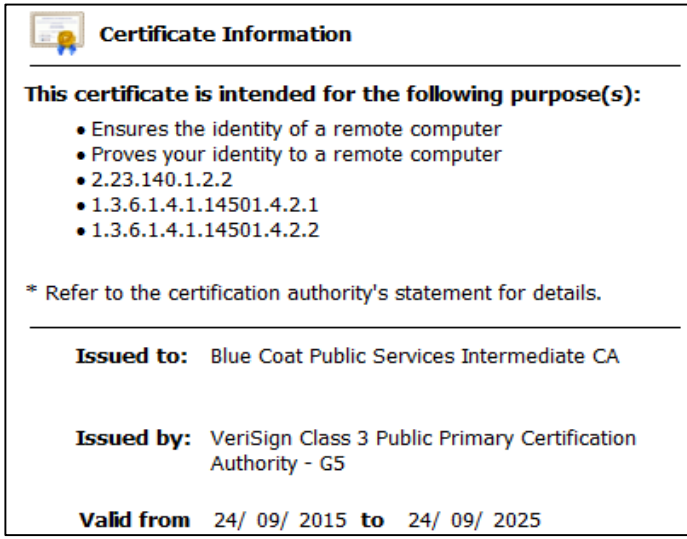
- Bluecoat utilise la NSA dans son marketing

  https://www.bluecoat.com/security-blog/2014-01-02/exploring-encrypted-skype-conversations-clear-text



- Symantec/Verisign délivre une AC intermédiaire à Bluecoat
  - Délivrée 3 semaines avant l'annonce du rachat





Business
International

Trend Micro a racheté ZDI

- En octobre 2015 ;-)

  http://newsroom.trendmicro.com/press-release/company-milestones/trend-micro-acquires-hp-tippingpoint

Twitter a payé $322,420 en BugBounty depuis 2014

https://www.helpnetsecurity.com/2016/05/31/twitter-bug-bounty/

John McAfee prend la tête d'un fond d'investissement pour défendre vos données

- Avant: “jeu de casino, paris en ligne, médical, protection de la propriété intellectuelles”
- A présent: “protection des données personnelles et la défense contre l’espionnage étatique des citoyens”

http://247wallst.com/technology-3/2016/05/10/john-mcafee-returns-to-cybersecurity-as-ceo-of-john-mcafee-global-technologies/

Droit / Politique

France

La CNIL sanctionne Ricard

- Du fait d'un accès non protégé aux données personnelles des clients
- Sanction après plusieurs contrôles et demandes de correction
- Seul Ricard est mis en cause, pas le sous-traitant

http://www.lemondeinformatique.fr/actualites/lire-la-cnil-inflige-une-sanction-a-ricard-pour-defaut-de-securite-64937.html

La CNIL publie 5 fiches sur les obligations des professionnels

1. Définir les objectifs du fichier
2. Vérifier la pertinence des données
3. Limiter la conservation des données
4. Respecter les droits des personnes
5. Sécuriser les données

https://www.cnil.fr/fr/comprendre-vos-obligations/les-principes-cles

ANSSI : Label sur les formations supérieures en sécurité du numérique

http://www.ssi.gouv.fr/administration/actualite/secnumedu-le-nouveau-label-des-formations-superieures-en-securite-du-numerique/

ANSSI : Surfez zen en une seule infographie

http://www.ssi.gouv.fr/actualite/surfez-zen-les-recommandations-de-lanssi-en-image/

Droit / Politique
International

Selon Europol, il ne faut pas affaiblir les systèmes

- Donc pas de backdoor

https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-investigation-that-respects-21st-century-data-protection

La fondation Mozilla paiera les audits d'applications Open Source

https://blog.mozilla.org/blog/2016/06/09/help-make-open-source-secure/

Conférences

Conférences

Texte en gris = déjà traité précédemment

Passées

- SSTIC - 1 au 3 juin 2016 à Rennes
  - Compte rendu lors du prochain mardi de l'OSSIR de Juillet

A venir

- Hack in Paris - 27 juin au 1er juillet 2016 à la Maison de la Chimie
- BeeRumP, des rumps et la bière - 16 juin 2016 à EPITA
  http://www.rump.beer/
- Nuit du Hack - 2 juillet 2016 chez Mickey
- Botconf - 30 novembre au 2 décembre 2016 à Lyon

Divers / Trolls velus

Divers / Trolls velus

Apple vs FBI le retour de la vengeance

- La NSA n'a pas la capacité de hacker un iPhone 5C iOS 9
- Ou alors, ils préfèrent ne pas le dire 😜

http://motherboard.vice.com/read/iphone-san-bernardino-nsa-hack

KickStarter : DataGateKeeper

- Solution de stockage Cloud sécurisée

https://www.kickstarter.com/projects/datagatekeeper/datagatekeeper-the-first-impenetrable-anti-hacking/description

Des objets connectés qui détectent la triche

- Qui pourraient être utilisés par les assureurs
- Mais le niveau de sécurité de ces IoT empechera-t-il vraiment de tricher ?

http://www.numerama.com/business/138437-les-assureurs-sauront-si-vous-trichez-avec-vos-objets-connectes.html

Craig Wright continue de se proclamer inventeur de Bitcoins

http://www.bbc.co.uk/news/technology-36168863

- Malgré les critiques

http://motherboard.vice.com/read/satoshis-pgp-keys-are-probably-backdated-and-point-to-a-hoax

Divers / Trolls velus

Le nouveau centre Russe de développement de leur OS mobile sécurisé

- C’est mieux que la tour-Maubourg 😜

  https://twitter.com/nnikiforov/status/728264659996950528

Un mot de passe qui résiste aux tortures ?

- Des systèmes de vrais-faux comptes existent déjà

  https://www.technologyreview.com/s/601445/how-to-make-passwords-that-cannot-be-compromised-by-torture-or-coercion/

Le code source de l’antivirus souverain est sur Github (ex-uhuru / davfi)

- RCE, contournement, élévation(s) de privilège locale…

  https://github.com/armadito/armadito-av

Les Pwnie Awards 2016 sont ouverts aux soumissions

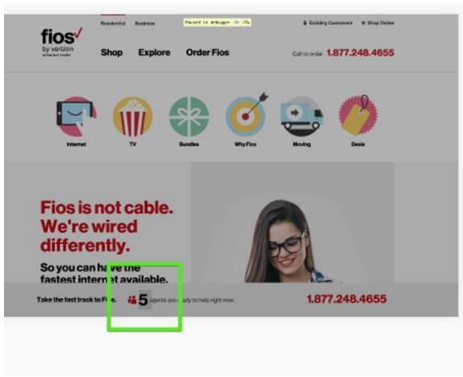
- Avec des nouvelles catégories dont “Best Backdoor”

  https://t.co/s9GMCBP5e5

Divers / Trolls velus

Fios by Verizon, le nombre d'agents joignables était tiré au hasard

https://twitter.com/mixonic/status/736575632226852865




```
$(document).on("ready", function() {
    function e() {
        var e = (new Date).getTime()
          , i = "/agent_queue.php?t=" + e;
        $.getJSON(i, function(e) {
            e && +e.available > 0 && (o.hide(),
            n.show(),
            t(e && +e.available > 14 ? 15 : e && +e.available >
        }).fail(function(e) {
            window.console && console.log("ERROR!", e)
        })
    }
    function t(e) {
        var n = e > 1 ? "agents are " : "agent is ";
        i.text(e),
        s.length > 0 && s.text(n),
        time_change = 1e3 * Math.floor(3 * Math.random() + 4),
        e > 11 ? agent_change = Math.floor(4 * Math.random() +
        setTimeout(function() {
            t(agent_change)
        }, time_change)
    }
    var i = $(".agents-available-wrapper .counter, .js-queue-st
      , s = $(".js-queue-stats-counter-label")
      , n = $(".js-is-banner-agents")
      , o = $(".js-is-banner-offer");
    e()
});
```

Le questionnaire de l'examen CEH a été publié

- Le niveau de difficulté semble réèl

https://www.synthsec.com/wp-content/uploads/2016/05/synthsec_certification_exam.pdf

Martine censure les documents confidentiels avec la NSA

https://ia800208.us.archive.org/9/items/CIABriefingRegardingMoneyLaunderingInMenaArkansasInTheLate1980sWithNSA/CIA%20Briefing%20Regarding%20Money%20Laundering%20in%20Mena,%20Arkansas%20in%20the%20Late%201980s%20with%20NSA_text.pdf

Q: Is the CIA or NSA aware of any attempts by federal or state officials to interfere with or terminate any investigation [by] the IRS, Justice Department, Arkansas State Police or any other law-enforcement authorities into Mena-related criminal conduct?

A: CIA, no. NSA, [redacted]

Divers / Trolls velus

Développer en C en 2016 ?

- Plusieurs bonnes pratiques modernes
  - <<The first rule of C is don't write C if you can avoid it>>

https://matt.sh/howto-c

Pentest d'une centrale electrique

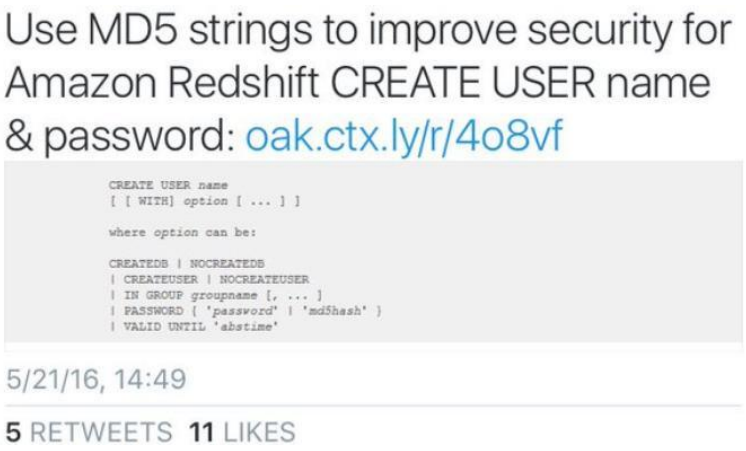
- En mode Red Team

https://www.youtube.com/watch?time_continue=31&v=pL9q2lOZ1Fw

En 2016, Amazon AWS recommande MD5

- Oups… le tweet a été effacé

https://twitter.com/aloria/status/734128454652854272/photo/1



Divers / Trolls velus

Go to the ATM and see this, what do you do?

https://twitter.com/hmier/status/740900636263211008

Divers / Trolls velus

Recherche Google sur Hacking Team

- Un nouveau logo ?

Divers / Trolls velus

Membre d’une RedTeam ?

- Faites peur à votre BlueTeam en prenant une MAC de la NSA
  - 00:20:91:xx:xx:xxx

http://www.coffer.com/mac_find/?string=00%3A20%3A91

John McAfee a réussit à casser le protocole Signal

- Et à lire des messages échangés entre 2 clients WhatsApp
- Ah non, il a juste infecté les 2 Android avec un malware ;-)

https://twitter.com/matthew_d_green/status/731930354060275713/photo/1

Divers / Trolls velus

Section “On va tous mourir”

Des missiles nucléaires gérés par une disquette 8 pouces

- Et sur des systèmes des années 70 sans support depuis plusieurs décennies

<< Coordinates the operational functions of the United States’ nuclear forces, such as intercontinental ballistic missiles, nuclear bombers, and tanker support aircrafts. This system runs on an IBM Series/1 Computer—a 1970s computing system—and uses 8-inch floppy disks>>

<< In addition, some legacy systems may use parts that are obsolete and more difficult to find. For instance, Defense is still using 8-inch floppy disks in a legacy system that coordinates the operational functions of the United States’ nuclear forces. 21 (See figure 4.)>>

http://www.gao.gov/assets/680/677454.pdf

http://www.techinsider.io/americas-nukes-floppy-disks-2016-5

Prochains rendez-vous de l’OSSIR

Prochaine réunion

- Mardi 12 juillet 2016

After Work

- à planifier à la rentrée

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous