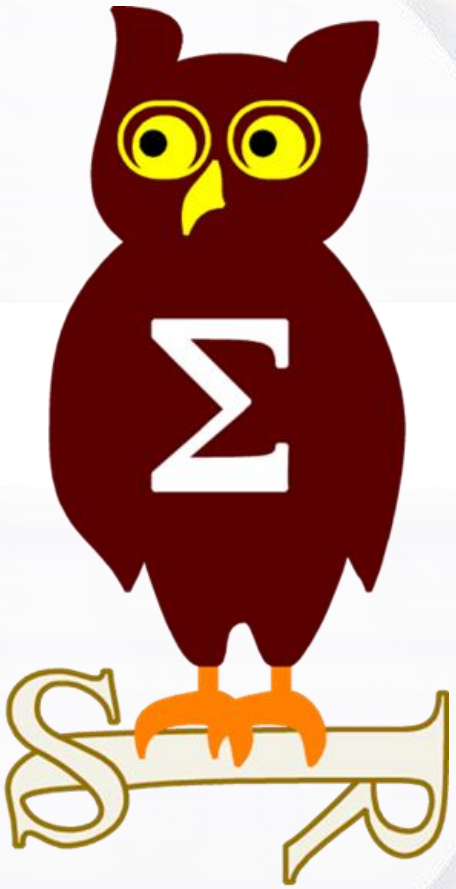


Revue d'actualité

13/01/2015

Préparée par

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

Failles / Bulletins / Advisories

Microsoft - Avis Décembre 2014

MS14-075 Élévation de privilèges dans Exchange (4 CVE) [Exploitabilité 2]

- Affecte:
  - Microsoft Exchange Server 2007 SP3, 2010 SP3, 2013 SP1
  - Annoncé en novembre, publié en décembre
  - Replaces MS13-105
- Exploit:
  - 2 x XSS (CVE-2014-6325 et CVE-2014-6326)
  - Spoofing d'un token d'authentification danw Outlook Web Access, permettant d'usurper l'identité d'un expéditeur (CVE-2014-6319)
  - redirection d'URL (CVE-2014-6336)
- Crédits:
  - Nikolay Anisenya (CVE-2014-6319)
  - John Koerner (CVE-2014-6325)
  - Adi Ivascu (CVE-2014-6326)
  - Jason Tsang Mui Chung (CVE-2014-6336)

Failles / Bulletins / Advisories

Microsoft - Avis Décembre 2014

MS14-080 Vulnérabilités dans Internet Explorer (14 CVE)  [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportées)
  - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
- Exploit:
  - 10 x Corruptions de mémoire (use after free et buffer overflows) aboutissant à une exécution de code
  - 2 x contournement du filtrage anti XSS
  - 1 x contournement ASLR
  - 1 x vulnérabilité VBScript
- Crédits:
  - A Qihoo researcher (CVE-2014-6330)
  - Dieyu: right-write-Correct wrong-run-hitting-NotCorrect (CVE-2014-6365)
  - Donghai Zhu (CVE-2014-6373)
  - Garage4Hackers par ZDI (CVE-2014-6327, CVE-2014-6329, CVE-2014-6376)
  - Jack Tang de Trend Micro (CVE-2014-6368)
  - Jihui Lu de KeenTeam (@K33nTeam) (CVE-2014-6375)
  - Liu Long de Qihoo 360 (CVE-2014-6366)
  - Sky par ZDI (CVE-2014-6375, CVE-2014-8966)
  - SkyLined par ZDI (CVE-2014-6374)
  - SkyLined parVeriSign iDefense Labs (CVE-2014-6363)
  - Takeshi Terada (CVE-2014-6328)
  - Yuki Chen of Qihoo 360 (CVE-2014-6369)

- En 2014, il y’aura eu **243** CVE sur Internet Explorer 

Failles / Bulletins / Advisories

Microsoft - Avis Décembre 2014

MS14-081 Vulnérabilité dans Word (2 CVE) [Exploitabilité 2]

- Affecte:
  - Microsoft Office 2007 SP3, 2010 SP2, Word 2010 SP2, Office 2013 et 2013 RT
  - Microsoft Office pour Mac et le pack de compatibilité Office
  - Microsoft SharePoint Server 2010, 2013
  - Microsoft Office Web Apps 2010 et 2013
- Exploit:
  - Exécutions de code à l'ouverture d'un fichier Word (doc et docx) spécialement formaté
- Crédits:
  - Ben Hawkes de Google Project Zero (CVE-2014-6356 et CVE-2014-6357)

MS14-082 Vulnérabilité dans Office (1 CVE) [Exploitabilité 2]

- Affecte:
  - Microsoft Office 2007, 2010, 2013 et 2013 RT
- Exploit:
  - Exécution de code à l'ouverture d'un fichier Office spécialement formaté
- Crédits:
  - Ben Hawkes de Google Project Zero (CVE-2014-6364)

Failles / Bulletins / Advisories

Microsoft - Avis Décembre 2014

MS14-083 Vulnérabilité dans Excel (2 CVE) [Exploitabilité 2]

- Affecte:
  - Excel 2007, 2010, 2013, 2013 RT et le pack de compatibilité Office
- Exploit:
  - Exécutions de code à l'ouverture d'un fichier Excel spécialement formaté
- Crédits:
  - Ben Hawkes de Google Project Zero (CVE-2014-6361 et CVE-2014-6360)

MS14-084 Vulnérabilité dans le moteur VBScript (1 CVE) [Exploitabilité 1]

- Affecte:
  - VBScript 5.6, 5,7 et 5.8
  - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
- Exploit:
  - Exécutions de code lors de l'éxécution d'un script VB (use after free)
  - Vulnérabilité commune avec MS14-080
- Crédits:
  - SkyLined par VeriSign iDefense Labs (CVE-2014-6363)

Failles / Bulletins / Advisories

Microsoft - Avis Décembre 2014

MS14-085 Vulnérabilité dans le moteur graphique Windows (1 CVE) [Exploitabilité 2]

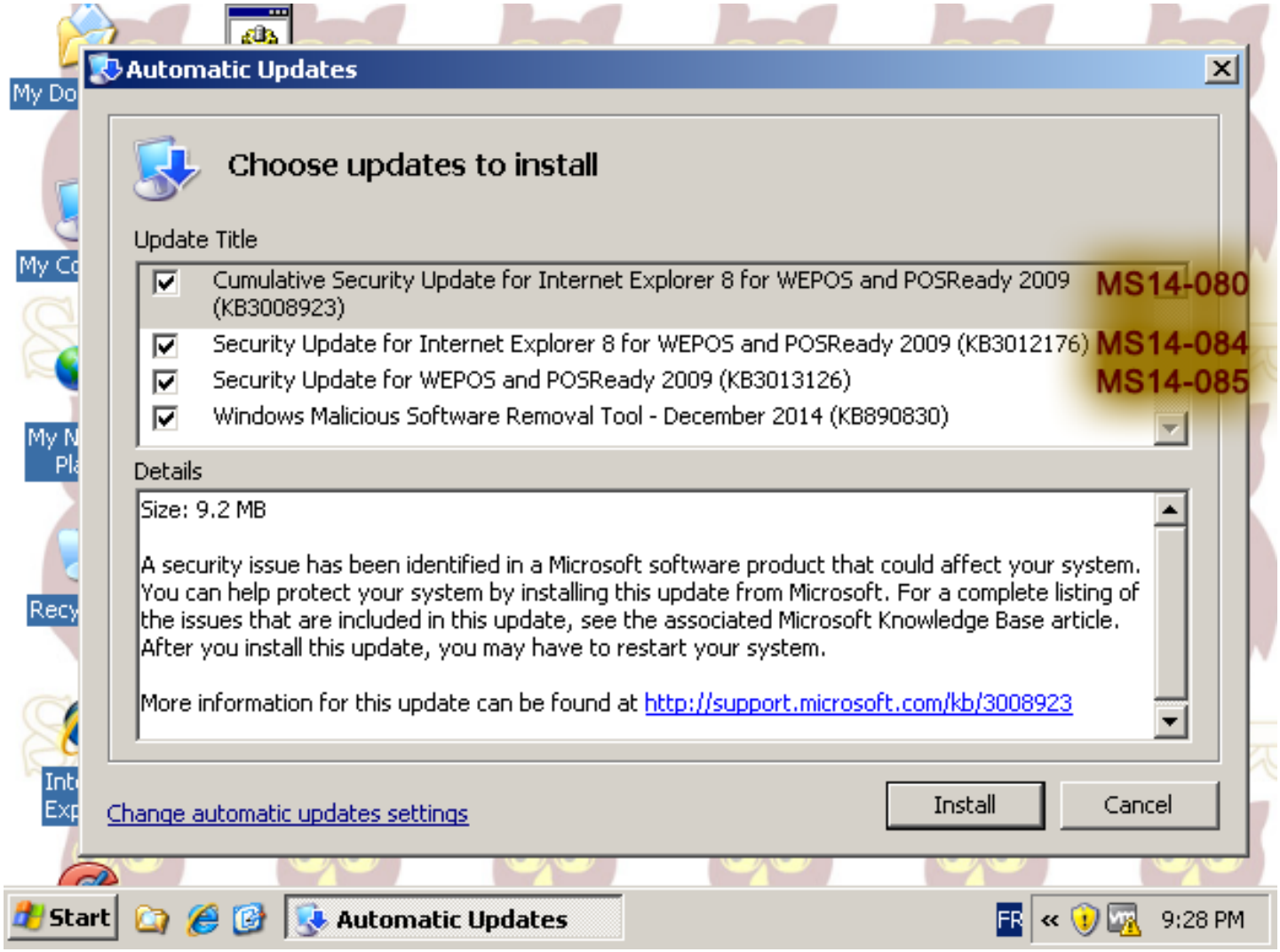
- Affecte:
  - Windows (toutes versions supportées)
  - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
- Exploit:
  - Divulgation d'informations sur la pile et contournement potentiel d'ASLR lors du traitement d'une image JPEG
- Crédits:
  - Michal Zalewski de Google (CVE-2014-6355)

Failles / Bulletins / Advisories

Microsoft - Avis Décembre 2014

Mise à jour pour Windows XP Embedded POSReady

- Encore et toujours sans documenter dans les bulletins…



Failles / Bulletins / Advisories

Microsoft - Autre

Encore une republication de patch

- http://www.clubic.com/windows-os/windows-7/actualite-744873-patch-tuesday-microsoft-supprime-dangereuse-windows-7.html

Microsoft revoit sa politique de notification avancée de vulnérabilités

- L'information ne sera disponible que pour les clients Premium
  http://grahamcluley.com/2015/01/microsoft-security-patches/

Publication d'une vulnérabilité Windows 8.1

- Élévation de privilèges locale
- Publiée par Project Zero initiative, après le délais de 90 jours
  https://code.google.com/p/google-security-research/issues/detail?id=118
  http://www.securityweek.com/google-discloses-unpatched-windows-81-vulnerability

Failles / Bulletins / Advisories

Système (principales failles)

NTPd

- Stack Overflow aboutissant à une exécution de code à distance (CVE-2014-9295)
- Clef de chiffrement par défaut faible (CVE-2014-9293)
- ...
  http://www.kb.cert.org/vuls/id/852879
- La liste des systèmes vulnérables est très longue :
  - Routeurs Soho : Belkin, D-Link
  - Firewalls : Checkpoint, Juniper, Palo Alto Networks, Fortinet
  - Fun : Open et Net BSD, CA Technologies, Cray Inc, Extreme Networks, Google
    http://www.kb.cert.org/vuls/byvendor?searchview&Query=FIELD+Reference=852879&SearchOrder=4

K7 *(Durcisseur de noyau Windows)*

- Déni de service local lors du nommage d'un fichier avec la chaîne "crashme$$"
  https://www.portcullis-security.com/security-research-and-downloads/security-advisories/cve-2014-8608/

Attaques sur OpenID

- 11 frameworks vulnérables sur 16 testés
  http://arxiv.org/pdf/1412.1623v1.pdf

Failles / Bulletins / Advisories

Système (principales failles)

L’attaque DNS de délégation infinie

- Vulnérabilité découverte par Florian Maury / ANSSI (cf. Revue du 2014-12-09) 
- La publication :
  http://www.ssi.gouv.fr/en/the-anssi/events/vulnerabilty-disclosure-the-infinitely-delegating-name-servers-idns-attack.html

Vulnérabilité dans bsd-mailx

- Fonctionnalité non documentée traite les adresses emails comme des commandes shell ...
  http://packetstormsecurity.com/files/129593/dsa-3104-1.txt

PHP

- User after free dans la fonction unserialize() CVE-2014-8142
  https://bugzilla.redhat.com/show_bug.cgi?id=1175718

Failles / Bulletins / Advisories

Réseau (principales failles)

XSS persistante dans le module ASM de F5 Big-IP

- Élévation de privilège
- Il faut déjà un compte sur l'interface d'administration

http://seclists.org/fulldisclosure/2015/Jan/40

Failles / Bulletins / Advisories

Apple

Apple Mac OS X

- Injection de firmware malveillant (bootkit) grâce au port Thunderbolt
- Vulnérabilité identifiée il y a 2 ans
  https://trmm.net/EFI

Apple Mac OS X et NTPd

- Exploitation de la faille NTPd sur OSx par un manque de filtrage de l'ip ::1
  http://googleprojectzero.blogspot.ch/2015/01/finding-and-exploiting-ntpd.html

Blocage du Brute force iCloud

www.cso.com.au/article/563508/apple-blocks-tool-brute-forces-icloud-passwords/

- Solution qui semble contournable...

Failles / Bulletins / Advisories

Crypto

OpenSSL

- Dénis de service par un message DTLS (CVE-2014-3571, CVE-2015-0206)
- Authentification par certificat client sans la clef privée, lors de la négociation Diffie-Helman (CVE-2015-0205)
  - Vulnérabilité découverte par Karthikeyan Bhargavan de l'INRIA 
- Erreur aléatoire lors d'un carré de grand nombre, mais semble peu exploitable (CVE-2014-3570)
- Dégradation de la sécurité lors de l'usage d'une clef RSA (CVE-2015-0204)
  - Vulnérabilité découverte par Karthikeyan Bhargavan de l'INRIA 
- Désactivation du Forward Secrecy avec ECDH + ECDSA (CVE-2014-3572)
  - Vulnérabilité découverte par Karthikeyan Bhargavan de l'INRIA 
- Contournement des vérifications uniquement des empreintes des certificats (blacklist) (CVE-2014-8275)

Failles / Bulletins / Advisories

Crypto

Multiples failles dans le protocole de signalisation SS7 (GSM)

- Écoute et déchiffrement, simplement en demandant la clef !
  - Présenté au 31C3
  - Mais ou sont les CVE ? ;-)

http://www.01net.com/editorial/638199/des-failles-dans-les-reseaux-3g-permettent-d-ecouter-tous-les-appels/

POODLE revisité sur TLS

- 10% des sites web les plus populaires sont vulnérables

http://www.developpez.com/actu/78917/Une-nouvelle-version-de-la-faille-POODLE-affecte-cette-fois-le-protocole-TLS-10-pourcent-des-sites-web-les-plus-populaires-sont-vulnerables/

Failles / Bulletins / Advisories

Divers

XSS chez AliExpress, d'Alibaba

- Découvert par AppSec Labs
  http://thehackernews.com/2014/12/alibaba-aliexpress-vulnerability.html

Cafetière Keurig 2.0

- Spoof des dosettes de café
  - En récupérant l'opercule d'une dosette officielle

  http://seclists.org/fulldisclosure/2014/Dec/37

Redirection arbitraire dans Good for entreprise (MDM / Mobile Device Management)

- Redirection automatique vers un site web lors de la lecture d'un email avec Good sur Android
- WONTFIX
  https://labs.integrity.pt/articles/good-for-enterprise-android-html-injection-cve-2014-4925/

Super cookies HSTS

- Utilisation de cette fonctionnalité pour tracker des utilisateurs
  http://www.radicalresearch.co.uk/lab/hstssupercookies/

Failles / Bulletins / Advisories

Divers

Management Engine : l'autre système et ses composants

- Antivol, accès au réseau sans besoin du BIOS, activable à distance dans besoin du CPU...
- Mémoire non accessible par le CPU
- et... Exécution de code Java uploadé
  http://recon.cx/2014/slides/Recon%202014%20Skochinsky.pdf

Faille critique UEFI

- Script de boot positionné dans une zone mémoire non protégée (demande un accès physique pour exploiter)
  http://www.silicon.fr/le-firmware-de-demarrage-pc-uefi-victime-dune-faille-critique-105103.html

Usurpation d'identité sur GitHub

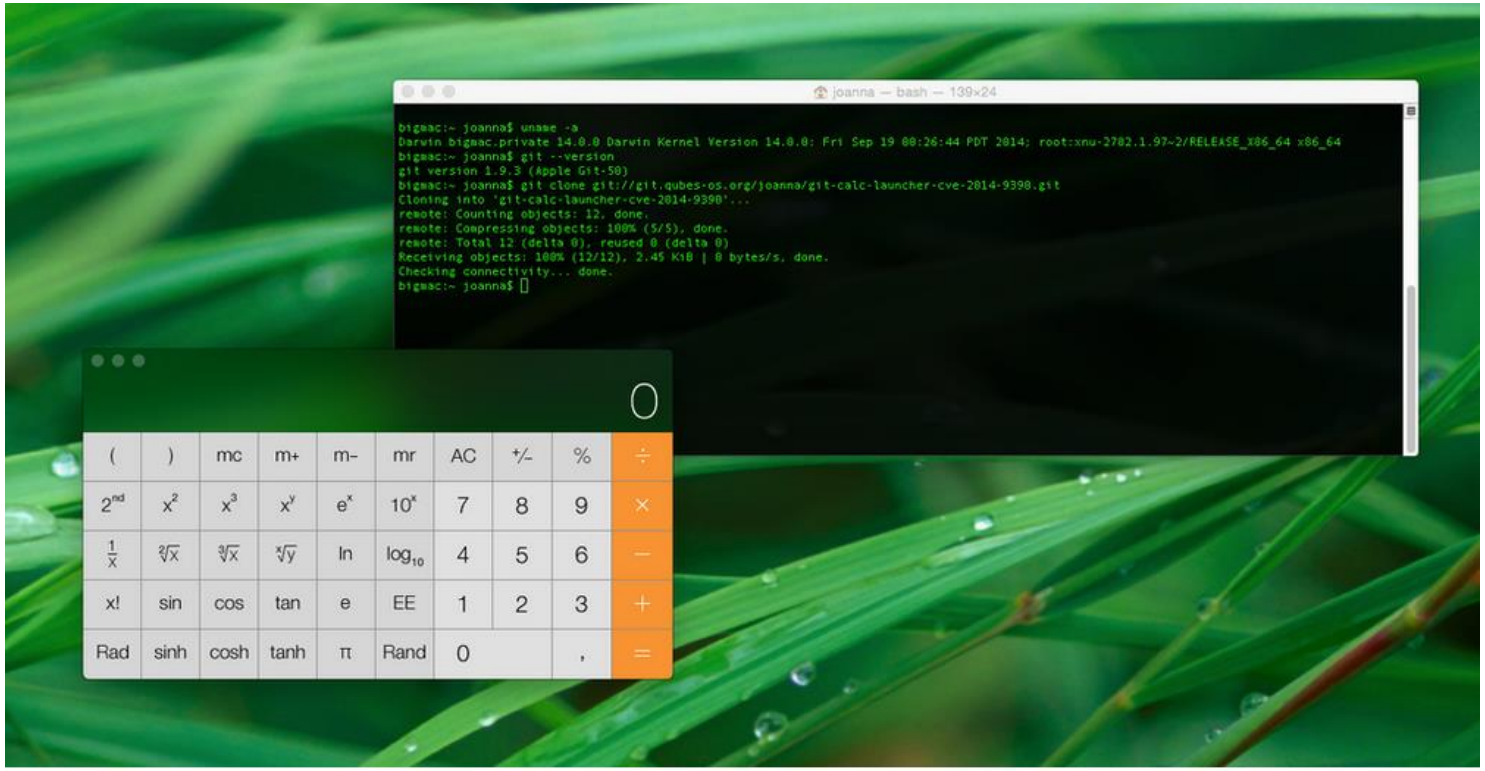
- Le nom d'utilisateur dans un commit est contrôlé localement
- Problématique pour les grands projets open-source
  http://carnal0wnage.attackresearch.com/2015/01/devooops-spoofing-github-users.html

Failles / Bulletins / Advisories

Divers

Vulnérabilités dans les clients GIT

- Permet l'exécution de code lors du "clone" d'un projet par exemple
  https://github.com/blog/1938-vulnerability-announced-update-your-git-clients



Joanna Rutkowska @rootkovska · Dec 19
I'm at the heights of my OSX commandline kungfu now: pic.twitter.com/FExEGz9B9H

24 26

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Désanonymisation de TOR par le FBI

- Grace à Metasploit et au plugin Decloaking Engine, utilisant Flash

  http://www.lemonde.fr/pixels/article/2014/12/11/ce-que-revelent-les-milliers-de-documents-confidentiels-voles-a-sony-pictures_4537271_4408996.html

  http://www.techworm.net/2014/12/fbi-used-metasploit-for-illegal-warrantless-snooping-on-tor-users.html

  http://securityaffairs.co/wordpress/31174/cyber-crime/operation-tornado-fbi-against-tor.html

Misfortune Cookie sur des routeurs SOHO

- Prise de contrôle à distance de routeurs D-Link, Edimax, Huawei, TP-Link, ZTE, et ZyXEL (CVE-2014-9222)

  http://www.undernews.fr/reseau-securite/misfortune-cookie-12-millions-de-routeurs-vulnerables.html

Piratages, Malwares, spam, fraudes et DDoS
Espionnage

Le guide de la CIA pour infiltrer et espionner

- En particulier l'espace Schengen et l'UE
- Surtout des bonnes pratiques pour éviter de passer pour un immigré clandestin ou un trafiquant
  https://wikileaks.org/cia-travel/press-release.html

Des antennes de téléphonie frauduleuses découvertes à Oslo

- Leur mission : intercepter les communications téléphoniques des parlementaires norvégiens
  http://rt.com/news/214327-snooping-mobile-towers-norway/
  https://www.schneier.com/blog/archives/2014/12/fake_cell_tower.html
  http://www.aftenposten.no/nyheter/iriks/Secret-surveillance-of-Norways-leaders-detected-7825278.html
  http://securityaffairs.co/wordpress/31109/intelligence/stingray-used-spy-norway-politicians.html

Les collaborateurs d'Angela Merkel ciblé par Regin

- Virus étatique dont nous vous parlions en novembre, cf. Veille du 2014-12-09
  http://news.softpedia.com/news/Angela-Merkel-s-Staff-Member-Targeted-with-Regin-Advanced-Persistent-Threat-468553.shtml

NSA vs Crypto

- De nouveau documents présentent les systèmes résistants à la NSA
- En 2012, la NSA :
  - Surveillait plus de 20 000 VPN par heure
  - Déchiffrait plus de 10 millions de connexions HTTPS pour y trouver des identifiants
  - Etait également capable de déchiffrer certaines sessions SSH
- PGP, Tor+VoIP ZRTP, TrueCrypt… « semblent » poser des problèmes à la NSA
  http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html

Piratages, Malwares, spam, fraudes et DDoS

DDoS

Le réseau Internet Nord-Coréen ébranlé par des attaques DDoS

http://www.scmagazineuk.com/north-koreas-internet-downed-by-suspected-ddos-attacks/article/389888/

http://www.extremetech.com/extreme/196375-north-korea-kicked-off-the-internet-by-giant-ddos-was-it-the-usa-or-someone-else

http://blog.erratasec.com/2015/01/anybody-can-take-north-korea-offline.html#.VKajcSuG_ng

DDoS sur le site du ministère de la Défense

http://www.linformaticien.com/actualites/id/35322/anonymous-frappe-de-nouveau-le-site-du-ministere-de-la-defense.aspx

DDoS sur une banque scandinave “Finnish bank OP Pohjola Group”

http://www.net-security.org/secworld.php?id=17785

Piratages, Malwares, spam, fraudes et DDoS

DDoS

Déni de service sur le Playstation Network et le XBox Live

- par Lizard Squad
  http://www.franceinfo.fr/vie-quotidienne/high-tech/article/les-reseaux-de-playstation-et-x-box-live-pirates-623613
- Kim dot com s'en mêle et offre des comptes Mega en échange d'un arrêt du DDoS
  - Car il ne pouvait plus jouer à ses jeux préférés

  http://krebsonsecurity.com/2014/12/whos-in-the-lizard-squad/

Lizard Squad crée un service de DDoS à la demande (parmi tant d'autres)

- Plusieurs offres :
  - 100 Secondes pour $5.99/mois
  - 3 minutes pour $8.99/mois
  - ...
  - 2 heures pour $44,99/mois
  - 3 heures pour $89.99/mois
- Slogan vendeur : Our current power stands at 100-125Gbps average with a total network of 600Gbps!
  https://lizardstresser.su/

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Sony (suite)

- Le RSSI (Phil Reitinger) a quitté son poste le 5 septembre 2014
  http://cryptome.org/2014/12/sony-ciso.htm
- La scène du film polémique montrant la mort de Kim Jong-un
  http://www.theverge.com/2014/12/16/7400963/sony-hack-leaked-clip-the-interview-kim-jong-un-death-scene
- Selon le FBI, les hackeurs sont Nord-Coréens
  http://krebsonsecurity.com/2014/12/fbi-north-korea-to-blame-for-sony-hack/
- Selon d'autres ce n'est pas la Corée du Nord
  http://marcrogers.org/2014/12/18/why-the-sony-hack-is-unlikely-to-be-the-work-of-north-korea/
- Les mails de l'avocat de Sony exposés
  http://gizmodo.com/sony-pictures-top-lawyer-s-emails-exposed-in-latest-lea-1669594084

Après Sony, des casinos de Las Vegas sont touchés par un logiciel malveillant destructeur

http://arstechnica.com/security/2014/12/iranian-hackers-used-visual-basic-malware-to-wipe-vegas-casinos-network/

http://www.reuters.com/article/2014/12/12/us-lasvegassands-cybersecurity-idUSKBN0JQ04520141212

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Un oléoduc en Turquie a explosé en 2012

- Le coupable « serait » une arme numérique (Un cousin de Stuxnet)
  http://www.bloomberg.com/news/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.html

Piratage d'un opérateur nucléaire en Corée du Sud

- Attaque sur le système d'information de gestion (pas SCADA)
- Vol de blueprints de certains éléments de centrales (non sensibles)
- Fuite et publication des plans des bâtiments
  http://www.techweekeurope.co.uk/security/korean-nuclear-hack-158045

Piratage d'un opérateur électrique en Corée du Sud

- Malware effaçant le MBR / Master Boot Record
  http://blog.trendmicro.com/trendlabs-security-intelligence/mbr-wiper-attacks-strike-korean-power-plant/

NAS QNAP

- Piratage automatisé grâce à l'utilisation de la faille ShellShock
- La page d'authentification au portail d'un QNAP est codée en GCI : /cgi-bin/authLogin.cgi
- Principalement pour faire de la fraude au clic
  http://thehackernews.com/2014/12/malware-shellshock-hack.html

Intrusion chez NVidia

http://hackread.com/nvidia-network-breach-500-staff-affected/

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Ars Technica piraté

- Base de données de ses utilisateurs a été volée, depuis un backup
  http://arstechnica.com/staff/2014/12/ars-was-briefly-hacked-yesterday-heres-what-we-know/
  https://twitter.com/stevekovach/status/544587122964172801

L'ICANN piraté

- par du classique SpreaFishing
  http://gizmodo.com/icann-has-been-hacked-1672648059

Madonna s'est fait voler son futur album

- Diffusé publiquement sur internet
  http://www.clubic.com/mag/trendy/actualite-745675-madonna-victime-piratage-futur-nouvel-album-internet.html

11 000 sites WordPress piratés

- Par le vers SoakSoak
- Bloqués par Google
  http://www.nextinpact.com/news/91439-plus-11-000-sites-wordpress-bloques-par-google-a-cause-dun-malware.htm

hijack de 1481 prefixes BGP par un opérateur Syrien

- Pendant quelques minutes
  http://www.bgpmon.net/bgp-hijack-incident-by-syrian-telecommunications-establishment/

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Vol et publication du SDK de la XBox One

https://nakedsecurity.sophos.com/2015/01/06/hacking-group-publishes-xbox-one-sdk-threatens-to-leak-unreleased-game-builds/

Des anonymous ont piratés des serveurs du gouvernement suédois

- En représailles à la fermeture de ThePirateBay
  http://techcrunch.com/2014/12/16/anonymous-allegedly-attacking-swedish-servers-for-pirate-bay-shutdown/

TorrentLocker (~cryptolocker)

- Infection de plus de 9 000 PC en Australie (39 000 dans le monde)
- Rançon unitaire de $1 500 en Bitcoins bien sûr !
- Aurait rapporté près de $600 000 aux pirates
  http://www.cso.com.au/article/562658/over-9-000-pcs-australia-infected-by-torrentlocker-ransomware/

Vol de la base de données des citoyens Serbes (tous?)

- Par le piratage du backbone du système de gestion des identités du pays
  http://securityaffairs.co/wordpress/31068/cyber-crime/serbia-hackers-stolen-national-database.html

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Vol de 4 à 5 millions d'euros chez Bitstamp

- Places de marché de Bitcoins
  http://www.01net.com/editorial/639470/le-site-d-echange-bitstamp-s-est-fait-voler-plus-de-4-millions-d-euros-en-bitcoin/

Vol de 1.9 million de données chez TF1.fr

- Plus précisément, chez la boutique en ligne, externalisée
  http://www.zataz.com/des-pirates-passent-par-le-site-de-tf1-et-annoncent-le-piratage-de-pres-de-2-millions-dinternautes/#axzz3NgKy98l8

Vol de 1,1 million de numéros de CB chez Staples

- Avec cryptogramme
  http://news.softpedia.com/news/Over-1-1-Million-Cards-Exposed-in-Staples-Data-Breach-468037.shtml

Publication de données volées à 13 entreprises

- Dont Domino's Pizza et Numéricable
  http://www.lesoir.be/747105/article/economie/2015-01-02/13-entreprises-refusent-ceder-au-chantage-d-un-hacker

Vol de $25 millions dans des banques Russes et Ukrainiennes

- 42 jours pour compromettre une cible
- Toutes les attaques semblent démarrer par du spearfishing et du drive-by downloads
- Rapport sur les attaques :
  http://www.group-ib.com/files/Anunak_APT_against_financial_institutions.pdf

Piratages, Malwares, spam, fraudes et DDoS

Internet des Objets

Hipsters beware ! Piratage de skateboards

- Skatebaoard motorisés contrôlés via Bluetooth

  http://www.theregister.co.uk/2014/12/19/hack_hijacks_boosted_skateboards_kills_hipsters

Internet of Toilets

- Conférence au 31C3

  http://media.ccc.de/browse/congress/2014/31c3_-_6370_-_en_-_saal_g_-_201412281900_-_internet_of_toilets_-_tbsprs.html#video

Pentest

Techniques & outils

Un script PowerShell pour créer des documents Office malveillants

https://github.com/enigma0x3/Generate-Macro/blob/master/Generate-Macro.ps1

Contourner les mécanismes de certificate-pinning sur iOS

http://chargen.matasano.com/chargen/2015/1/6/bypassing-openssl-certificate-pinning-in-ios-apps.html

Framework de tests d'intrusion réseau : SPARTA

- Permet l'automatisation de certaines tâches

http://n0where.net/sparta-network-infrastructure-penetration-testing-tool/

Utiliser WMIC pour passer un Golden Ticket Kerberos

http://blog.cobaltstrike.com/2015/01/07/pass-the-golden-ticket-with-wmic/

Outils d'attaque pour Oracle : ODAT

https://github.com/quentinhardy/odat

Un nouvel outil de brute-force : Crowbar

http://hack-tools.blackploit.com/2015/01/crowbar-brute-forcing-tool-for-pentests.html?utm_source=dlvr.it&utm_medium=twitter

Pentest

Techniques & outils

Inverser les mots de passe CISCO ACS

http://www.synacktiv.com/ressources/cisco_acs_repo_decrypt.py

Générateur de mots de passe

- Basé sur la combinaison de mots

http://reusablesec.blogspot.fr/2014/12/tool-deep-dive-prince.html

Phishing automatisé sur Hotspot malveillant : Wifiphisher

https://github.com/sophron/wifiphisher

Un module MS14-068 pour Metasploit !

- Une version de Mimikatz non publique inclue également l'exploit

https://community.rapid7.com/community/metasploit/blog/2014/12/25/12-days-of-haxmas-ms14-068-now-in-metasploit

PuttyRider

- Permet à un attaquant de s"insérer dans les sessions Putty si le poste est compromis

https://github.com/seastorm/PuttyRider

Scada
Divers

3 interventions intéressantes lors du 31C3

- *Switches get stitches* : déni de service sur des switchs industriels
  http://fr.slideshare.net/44Con/switches-getstitches
  https://www.youtube.com/watch?v=CWZjQ4BTD0k
- *Damn Vulnerable Chemical Process* : Il ne suffit pas d'avoir accès aux automates
  https://www.youtube.com/watch?v=TPUzNMcFb4A
- *Too smartgrid in da cloud* : Sécurité des énergies renouvelables pour particuliers
  https://www.youtube.com/watch?v=iuMd11kDUz8
  http://scadastrangelove.blogspot.de/2014/12/sos-secure-open-smartgrids.html

Vulnérabilité dans le composant DTM utilisé par Emerson

- Comme démontré à la BlackHat Europe par Alexander Bolshev
  https://ics-cert.us-cert.gov/advisories/ICSA-15-008-01A

Les SI industriels ciblés par les malwares classiques

- Chevaux de troie bancaires
- se faisant passer pour des logiciels SCADA
- 32 variantes identifiées par un chercheur de TrendMicro
  http://www.darkreading.com/attacks-breaches/banking-trojans-disguised-as-ics-scada-software-infecting-plants/d/d-id/1318542?_mc=sm_dr_editor_kellyjacksonhiggins

Scada
Divers

Incident dans une aciérie allemande

- Seulement le 2ème cas d'une attaque sur un SI industriel qui cause des dommages physiques
- Présent dans le rapport annuel du BSI (équivalent allemand de l'ANSSI)
- Infection via spear-phishing, puis rebond du SI de gestion vers le SI industriel
- L'attaque a mis un haut fourneau dans un état instable, et a engendré des dommages importants sur l'ensemble de l'usine
- Les attaquants disposaient d'un niveau de connaissance avancé du procédé industriel

http://www.wired.com/2015/01/german-steel-mill-hack-destruction/
http://dragossecurity.com/blog/

Vulnérabilité des routeurs RuggedCom

- Contournement de l'authentification en 2012
- Routeurs compromis détectables sur Shodan

http://defensive-targeteering.net/pwned-up-industrial-routers/

Vulnérabilité des systèmes ProClima de Schneider

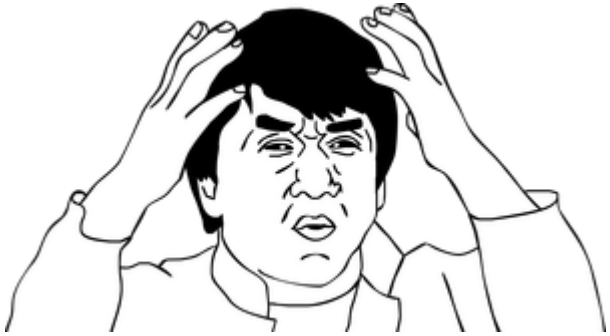
- Exécution de code à distance
  https://ics-cert.us-cert.gov/advisories/ICSA-14-350-01

Vulnérabilitié dans HoneyWell Experion PKS

https://www.honeywellprocess.com/library/support/Public/Documents/ExperionPKS.R311.Server.Patch282.PAR1-2VNCSKZ_SCN.pdf

Vulnérabilités dans les RTU Emerson

- Vulnérabilités classiques : mots de passe hardcodés, contournement d'authentification
  https://ics-cert.us-cert.gov/advisories/ICSA-13-259-01B



--------- Begin Update B Part 1 of 2 --------

Emerson Process Management has produced a patch that mitigates all but the authentication bypass vulnerability. The researchers who identified these vulnerabilities have tested the patch to validate that it mitigates all other vulnerabilities. As a mitigation for the authentication bypass vulnerability, Emerson Process Management recommends installing a third-party device in front of the ROC800.

--------- End Update B Part 1 of 2 ----------

Nouveautés (logiciel, langage, protocole...)

Open Source

Scapy 2.3 !!!

- Toujours aussi bien documenté ;-)
  http://www.secdev.org/projects/scapy/files/

Nouvelle version de Dependency Check

- Projet OWASP pour identifier les bibliothèques vulnérables dans un projet
  https://www.owasp.org/index.php/OWASP_Dependency_Check

Générateur de configuration SSL par Mozilla

https://mozilla.github.io/server-side-tls/ssl-config-generator/

Un gem Ruby pour se connecter aux bases de données Oracle

http://blog.spiderlabs.com/2014/12/announcing-nettns-for-ruby-a-gem-for-connecting-to-oracle-databases.html

RFC 7435: Opportunistic Security: Some Protection Most of the Time

- Solution de sécurité trop complexe = peu ou pas déployé
  http://www.bortzmeyer.org/7435.html

Nouveautés (logiciel, langage, protocole...)

Open Source

Mimikatz

- Nouvelle fonctionnalité... affichant la grille du démineur ;)
  https://twitter.com/gentilkiwi/status/536666232192507906

SSH Brute-Forcer monitoring tool

https://github.com/pronto/SSH-Ranking

tcpdump : filtres avancés

http://www.wains.be/pub/networking/tcpdump_advanced_filters.txt

Bind

- Nouvelle clef de signature du code
  - La précédente expirant au 31 janvier 2015

https://www.isc.org/blogs/new-code-signing-key-for-2015-2017/

Nouveautés (logiciel, langage, protocole...)

Divers

End-to-End : une extension open-source de Google pour chiffrer les mails de bout en bout.

http://www.undernews.fr/reseau-securite/end-to-end-une-extension-google-chrome-pour-chiffrer-les-mails-de-bout-en-bout.html
http://www.lemondeinformatique.fr/actualites/lire-google-met-sur-github-son-projet-de-chiffrement-end-to-end-59650.html

IDA 6.7

- Meilleurs support ARM, Dalvik et Android
  https://www.hex-rays.com/products/ida/6.7/index.shtml

Nouvelle version des notations CVSS

- CVE-2014-0001
- CVE-2014-10000
- CVE-2014-100000
- CVE-2014-1000000
  https://cve.mitre.org/cve/identifiers/syntaxchange.html

Business
France

Premier incident de paiement pour une plateforme de crowdfunding Française

- A cause de la mise en redressement judiciaire de Smok-it
  http://votreargent.lexpress.fr/placements/premier-incident-de-paiement-chez-unilend-un-acteur-francais-du-crowdfunding_1633589.html

L'ANSSI recrute

- un responsable d'opérations de cyberdéfense
  http://rpdefense.over-blog.com/2014/12/l-anssi-recrute-un-responsable-d-operations-de-cyberdefense.html

Les patrons de la sécurité informatique demandent le soutien des DSI

http://business.lesechos.fr/directions-numeriques/0203961630361-les-patrons-de-la-securite-informatique-demandent-le-soutien-des-dsi-105792.php

Business
France

Il fallait au moins un slide entier juste pour cette nouvelle

Deloitte et HSC se “rapprochent”

http://www2.deloitte.com/fr/fr/pages/presse/2014/Deloitte-renforce-ses-expertises-de-conseil-et-d-audit-en-securite-des-systemes-d-information.html

Business

France

IPv6 chez Orange en 2015

https://twitter.com/Orange_conseil/status/547019794038652928

3DSecure : Pannes à répétition avant Noël !

http://www.wizishop.com/blog/news-ecommerce/3dsecure-panne-a-repetition-avant-noel.html

Cointreau abandonne IBM lotus notes pour Microsoft Office 365

http://pro.01net.com/editorial/638004/remy-cointreau-abandonne-lotus-notes-pour-office-365/

Business
International

Google, Microsoft et Adobe se retirent de Russie
http://pro.clubic.com/technologie-et-politique/actualite-744913-google-microsoft-adobe-retirent-russie.html

Google agrandit ses bureaux en Suisse
- Opération séduction !
  http://mobile2.24heures.ch/articles/24883334

Kostya quitte Microsoft
https://twitter.com/crypt0ad/status/550445073901441024

Servers by Huawei chez Qwant
- No backdoor
  http://blog.qwant.com/servers-by-huawei/

Licenciement chez Morgan Stanley
- De l'employé ayant publié des données clientes sur Pastebin
  http://www.net-security.org/secworld.php?id=17792

Comment les USA veulent imposer le Cloud sans frontières pour tous
http://www.numerama.com/magazine/31639-comment-les-usa-veulent-imposer-le-cloud-sans-frontieres-pour-tous.html

Droit / Politique

France

Le volet numérique du projet de loi Macron

http://www.nextinpact.com/news/91420-le-volet-numerique-projet-loi-macron.htm

Dailymotion condamné en appel pour contrefaçon et concurrence déloyale

http://www.lemonde.fr/culture/article/2014/12/02/dailymotion-condamne-en-appel-pour-contrefacon-et-concurrence-deloyale_4533098_3246.html

Suspension de permis pour 15 internautes ayant signalé des radars sur Facebook

http://www.nextinpact.com/news/91227-suspension-permis-pour-15-internautes-ayant-signale-radars-sur-facebook.htm

Condamnation pour usurpation d'identité et exploitation d'une faille XSS

- Exploitation d'un XSS sur le site de Rachida Dati => introduction frauduleuse de données dans un STAD
- Humour potache => Atteinte à l'honneur de Rachida Dati en particulier, des femmes, en général

http://www.nextinpact.com/news/91561-condamnation-pour-usurpation-d-identite-et-exploitation-d-une-faille-xss.htm

La Cnil épingle les Wi-Fi ouverts en accès libre

- Conservation des données personnelles trop longues

http://www.01net.com/editorial/638443/la-cnil-epingle-les-bornes-wifi-en-libre-acces/

Quadrature du Net est sauvée

http://www.zdnet.fr/actualites/quadrature-du-net-mission-sauvetage-reussie-39811887.htm

Droit / Politique

France

Les PASSI sont publiés sur le site de l'ANSSI

Attaque massive de hackeurs prévue le 15 janvier

- Visant les institutions et sociétés françaises
- Pour répondre aux attaques de sites supposés islamistes, par des Anonymous
  - Faisant suite aux attentats à Paris

http://www.lemondeinformatique.fr/actualites/lire-charlie-hebdo-des-cyberpirates-musulmans-repondent-aux-anonymous-59874.html

Droit / Politique
International

Sony

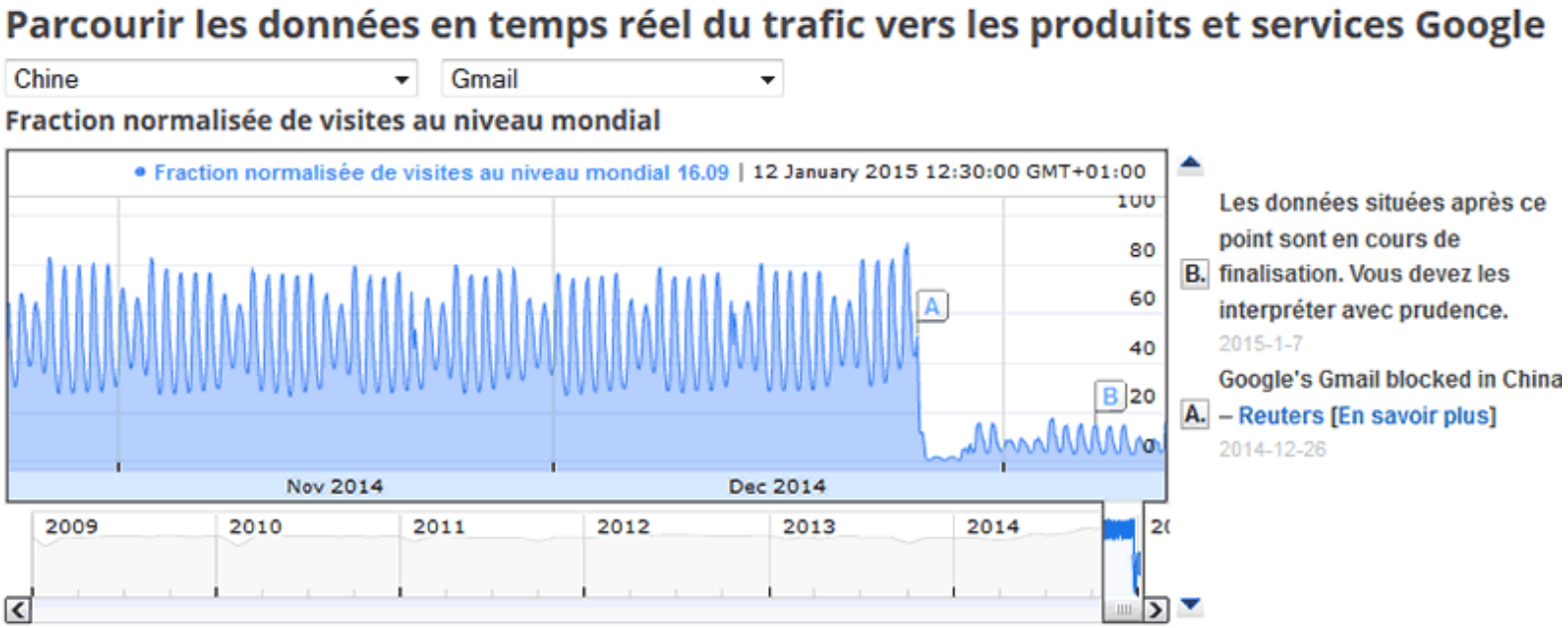
- D'anciens salariés portent plainte pour défaut de sécurité
  http://www.01net.com/editorial/637591/hack-de-sony-pictures-danciens-salaries-portent-plainte-pour-defaut-de-securite/

Un sénateur américain veut interdire les backdoors

http://www.nextinpact.com/news/91255-un-senateur-americain-veut-interdire-backdoors.htm

Blocage de GMail en Chine

- Le blocage n'est pas total mais s'apparente à des "perturbations"
  http://bigbrowser.blog.lemonde.fr/2014/12/29/gmail-bloque-en-chine/
  http://www.google.com/transparencyreport/traffic/explorer/?r=CN&l=GMAIL&csd=1414139400000&ced=1421031854482



Conférences

Texte en gris	=	déjà traité précédemment

Passées

- Bot Conf - 3 au 5 Décembre 2014 à Nancy
  https://www.botconf.eu/botconf-2014/documents-and-videos/
- 31C3
  https://www.youtube.com/user/mediacccde/videos
  http://media.ccc.de/

A venir

- FIC 2015 - 20 et 21 janvier 2015 à Lille
  - Avec du Bruce Schneier dedans !
- JSSI 2015 - 10 mars 2015 à Paris
  - Soumission encore ouverte
  - Venez nombreux !
- GS Days - 24 mars 2015 à Paris
- SSTIC 2015 - 3, 4 et 5 juin 2015 à Rennes
- Peut-être pas de NoSuchCon en 2015

Divers / Trolls velus

Obama fait du code

http://techcrunch.com/2014/12/08/barack-obama-becomes-the-first-president-to-write-code/

Nettoyage des bots chez Intragram

- Perte de millions de followers (56% pour Akon, 14% pour Justin Bieber)
  http://64px.com/instagram/

Pantalon jean “cage de faraday” par Norton

http://www.betabrand.com/think-tank/crowdfunding/mens-rfid-blocking-pocket-norton-denim-jeans.html

Le coût du S d’https

- Charge CPU supplémentaire côté serveur/infra
- Temps de chargement
- Overhead / Latence
- Vie des batteries

  http://www.cs.cmu.edu/~dnaylor/CostOfTheS.pdf

Divers / Trolls velus

Un blog intéressant pour les “old school”

- Assembleur, SSE…
  http://blogs.msdn.com/b/oldnewthing

Attention à la seconde intercalaire le 30 juin prochain

- Votre système d’information est-il prêt pour gérer l’heure 23:59:60 ?
  http://www.atlantico.fr/decryptage/annee-plus-longue-2015-durera-seconde-plus-et-internet-va-sentir-passer-1944758.html

Ingénierie inverse de la PS1

- Explication didactique de 11 minutes
  https://www.youtube.com/watch?v=MPXpH2hxuNc

Divers / Trolls velus

Kerckhoffs et OATH ont trop bu ?

- Carte bancaire avec cryptogramme en mode OTP
- Mais le seed serait le PAN
  - <<le diversificateur correspondant au numéro de carte PAN >>

http://www.google.com/patents/EP1978479A1?cl=fr

La mauvaise idée du mois

https://twitter.com/HouseMonitor

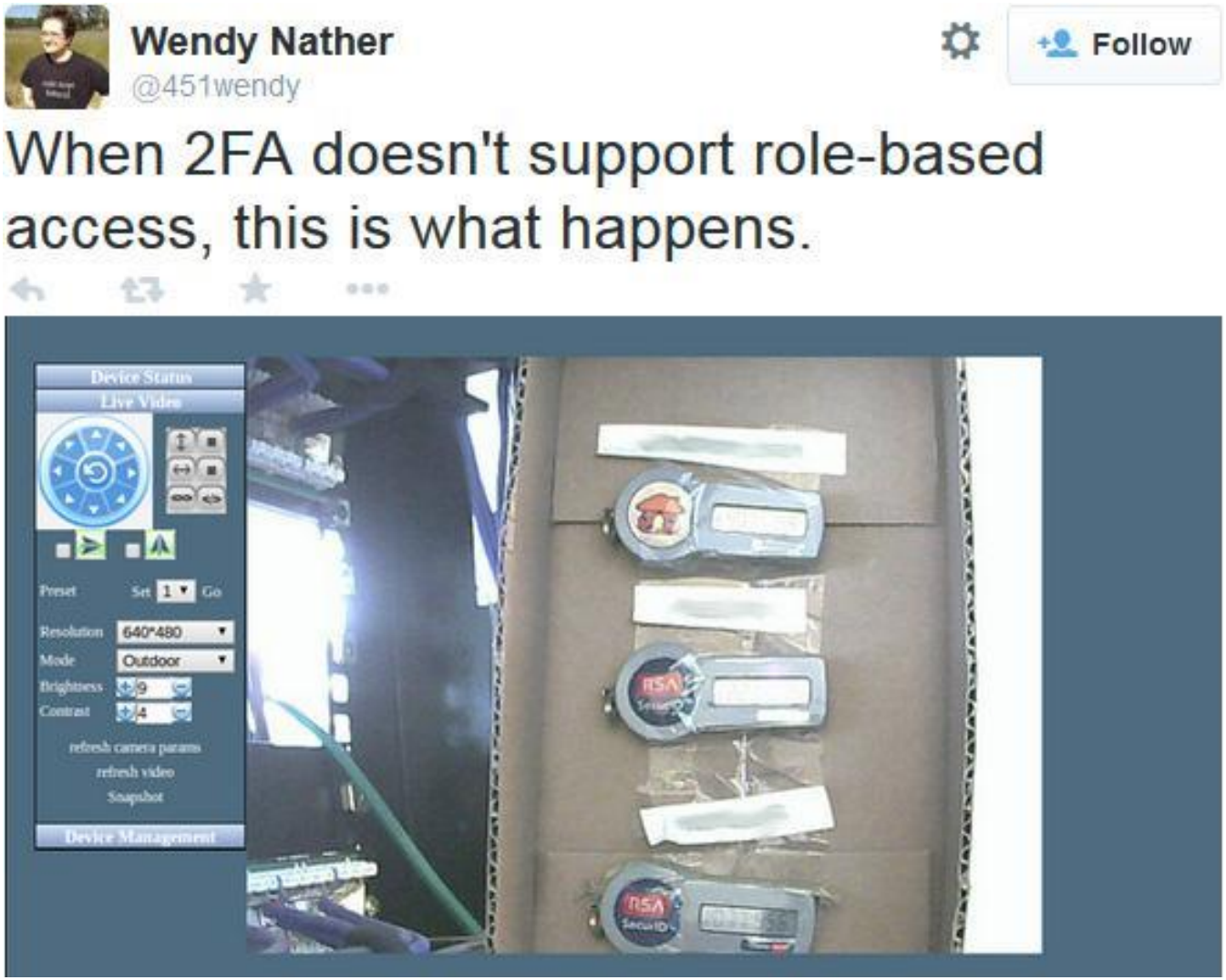
Égayez vos présentations avec “Qui attaque Qui”

http://krebsonsecurity.com/2015/01/whos-attacking-whom-realtime-attack-trackers/

- Attention, la version de Mandiant est bruyante http://dds.ec/pewpew/index.html

Divers / Trolls velus

L'authentification à Double facteur et la gestion des rôles
https://twitter.com/451wendy/status/544497374388039680



Divers / Trolls velus

C’est la nouvelle année, alors voici notre TOP 20 des évènements de sécurité 2014

- Vulnérabilités
  - La faille **Microsoft** CVE-2014-6324 sur **Kerberos**
  - Les **backdoors** dans **iOS** (ou plutôt les fonctionnalités de « debug »)
  - La découverte que les **objets connectés** sont totalement **insécurisés**
  - **Heartbleed** et **POODLE**
  - **Shellshock**
  - Les « **goto fail** » d’Apple et GnuTLS
- Piratages
  - Le Fapening ou **CelebGate**
  - Utilisation**s** dans la vraie vie **d’OpenBTS** et **Osmocom**
  - **Sony**
  - **Home Depot** (56 millions de numéro de CB)
  - **Target** (110 millions de données bancaire)
  - **Gamma** Group, éditeur du trojan FinFisher et la diffusion de noms de clients, prix...
  - La découverte que la NSA récolte, avant tout, des données de vie privée des gens ordinaires
- Fin de
  - Windows **XP**
  - **TrueCrypt**
  - **Bull** (racheté par Atos)
  - **Full Disclosure…** et sa renaissance
- Autre
  - **RGS** 2.0
  - **VUPEN** quitte la France
  - Rapprochement de **Deloitte** et **HSC**

Prochaines réunions

Prochaines réunions

- Mardi 10 Février 2015

Afterwork

- Mardi 27 janvier 2015, à partir de 19h

  Bar "La Kolok"
  20 rue du croissant
  75002 Paris

Questions ?