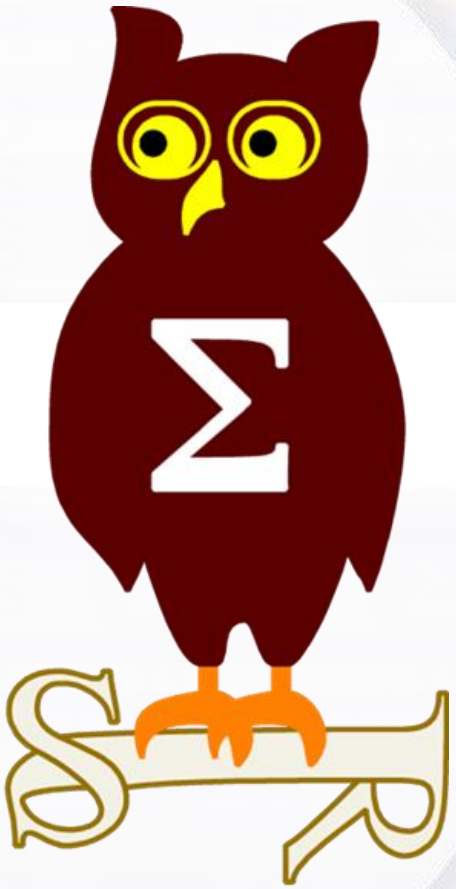


Revue d'actualité

09/12/2014

Préparée par

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

Failles / Bulletins / Advisories

Microsoft - Retour sur des vulnérabilités passées

MS14-038 Vulnérabilité dans le Journal Windows (Cf. Revue 2014-09-09)

- Nouvelle surface d'attaques : les fichiers du Journal Windows
  - Existe depuis premières tablettes sous Windows XP
- Publication de fichier contenant des 0-days
  http://pastebin.com/8Q9kkcwc
  https://mega.co.nz/#!nUUS3DhK!cQuL3x1Z-MmxOUsUwfDlVjfiJDyjlkhAacynW4FnAKc
- Détails
  http://blog.beyondtrust.com/cve-2014-1824-searching-for-windows-attack-surface

MS14-060 Vulnérabilité dans le composant OLE (Cf. Revue 2014-11-18)

- Exploité dans la nature par le malware Sandworm
  http://blogs.mcafee.com/mcafee-labs/new-exploit-sandworm-zero-day-bypass-official-patch

MS14-063 Vulnérabilité dans le pilote FAT32 (Cf. Revue 2014-11-18)

- Démonstration de l'exploitation de la vulnérabilité dans la fonctionnalité FASTFAT
  http://blogs.cisco.com/security/talos/ms14-063-a-potential-xp-exploit

Failles / Bulletins / Advisories

Microsoft - Avis Novembre 2014

MS14-064 Vulnérabilité dans le composant OLE (2 CVE) [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportées)
  - Correctif également pour Windows XP Embedded POSReady, kb2962872 (cf. screenshot après)
- Exploit:
  - Annoncé en Octobre : Cf. MS14-060 cf. Revue 2014-11-18
  - Exécution de code à l'ouverture d'un fichier contenant un appel OLE (Object Linking and Embedding)
  - Microsoft fournir une configuration EMET pour mitiger le risque
  - Exploité dans la nature dans des fichiers Office
    http://blogs.technet.com/b/srd/archive/2014/11/11/assessing-risk-for-the-november-2014-security-updates.aspx
  - Par les Chinois
  - http://www.securityweek.com/apt3-group-using-windows-ole-vulnerability-fireeye
  - Détails sur la CVE-2014-6332
    http://securityintelligence.com/ibm-x-force-researcher-finds-significant-vulnerability-in-microsoft-windows/#.VGLHinGUdfc
- Crédits:
  - Robert Freeman de IBM X-Force (CVE-2014-6332)
  - Drew Hintz, Shane Huntley et Matty Pellegrino de Google Security Team (CVE-2014-6352)
  - Haifei Li et Bing Sun de McAfee Security Team (CVE-2014-6352)
  - Yu Wang, Bin Wang et Donghui Zhang de Baidu Security Team / X-Team (CVE-2014-6352)

Failles / Bulletins / Advisories

Microsoft - Avis Novembre 2014

MS14-065 Vulnérabilités dans Internet Explorer (17 CVE)  [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportées)
  - Correctif également pour Windows XP Embedded POSReady, kb2962872 (cf. screenshot après)
- Exploit:
  - Contournement d'ASLR
  - 2 x Élévations de privilèges
  - Récupération du contenu du Clipboard
  - 3 x Divulgations d'informations
  - 10 x Corruptions de mémoire aboutissant à une exécution de code
- Crédits:
  - 0016EECD9D7159A949DAD3BC17E0A939 par ZDI (CVE-2014-6343)
  - A3F2160DCA1BDE70DA1D99ED267D5DC1EC336192 par ZDI (CVE-2014-6348)
  - Bo Qu de Palo Alto Networks (CVE-2014-6337, CVE-2014-6339,CVE-2014-6351)
  - Cloudfuzzer par ZDI (CVE-2014-6347)
  - Daniel Trebbien (CVE-2014-6323)
  - James Forshaw de Context Information Security (CVE-2014-6340)
    - Lecture d'un fichier local : http://tyranidslair.blogspot.co.uk/2014/11/whens-documenturl-not-documenturl-cve.html
  - James Forshaw par Google Project Zero (CVE-2014-6349, CVE-2014-6350)
    - Détails : http://googleprojectzero.blogspot.fr/2014/12/internet-explorer-epm-sandbox-escape.html
  - Jason Kratzer par ZDI (CVE-2014-6344)
  - Pengfei Guo de Qihoo 360 (CVE-2014-6353)
  - s3tm3m par ZDI (CVE-2014-4143, CVE-2014-6341)
  - SkyLined par ZDI (CVE-2014-6342, CVE-2014-6351)
  - Takeshi Terada (CVE-2014-6345, CVE-2014-6346)

- Sans compter décembre : **229 CVE** Internet Explorer sur 2014 (137 CVE en 2013)

Failles / Bulletins / Advisories

Microsoft - Avis Novembre 2014

MS14-066 Vulnérabilité dans le composant SChannel (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportées) et remplace MS10-085 et MS12-049
  - Correctif pour Windows XP Embedded POSReady, kb2939576 (cf. screenshot après)
- Exploit:
  - Exécution de code lors du traitement d'une négociation TLS/SSL contenant une signature par courbe eliptique, spécialement formatée
  - Détails : http://blog.beyondtrust.com/triggering-ms14-066
  - Combo à la Canvas : "LSASS eip control via ms14-066 + preauth RDP"

    https://twitter.com/daveaitel/status/533064909387747328
- Crédits:
  - Trouvé en interne lors d'un audit
- Bonus Microsoft
  - Ajout de 4 suites de chiffrement contenant le mode Galois/Counter Mode (GCM)

MS14-067 Vulnérabilité dans Microsoft XML Core Services (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportées)
  - Correctif pour Windows XP Embedded POSReady, kb2939576 (cf. screenshot après)
- Exploit:
  - Exécution de code à la visite d'un site hébergeant un XML "malfaisant"
- Crédits:
  - Alisa Esage Shevchenko de Esage Lab (CVE-2014-4118)

Failles / Bulletins / Advisories

Microsoft - Avis Novembre 2014

Publication Hors Bande le 18 Novembre 2014

MS14-068 Vulnérabilité dans Kerberos (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportées) remplace MS11-013 et MS10-014
  - Correctif pour Windows XP Embedded POSReady, kb2939576 (cf. screenshot après)
- Exploit:
  - Élévation de privilèges lors de la demande d'un ticket Kerberos (TGS / Ticket-Granting Service) à un KDC
    - Usurpation de quel utilisateur/groupe dont les admins de domaine
  - La requête (PAC / Pre-Authentication Datas) peut-être "signée" dans un algorithme de condensat type MD5, donc sans clef
  - Exploité dans la nature

    http://blogs.technet.com/b/srd/archive/2014/11/18/additional-information-about-cve-2014-6324.aspx
  - PyKEK (Python Kerberos Exploitation Kit) par Sylvain Monné et Benjamin Delpy
    - Pour manipuler les données Kerberos 5 + POC d'exploitation de MS14-068 https://github.com/bidord/pykek
  - Quelques détails supplémentaires http://blog.beyondtrust.com/a-quick-look-at-ms14-068
- Crédits:
  - Qualcomm Information Security & Risk Management team, avec l'aide de Tom Maddock (CVE-2014-6324)

Failles / Bulletins / Advisories

Microsoft

MS14-068 corrigée dans MIT Kerberos depuis 2010…

http://web.mit.edu/kerberos/advisories/MITKRB5-SA-2010-007.txt

```
MITKRB5-SA-2010-007

MIT krb5 Security Advisory 2010-007
Original release: 2010-11-30
Last update: 2010-11-30

Topic: Multiple checksum handling vulnerabilities

CVE-2010-1324
* krb5 GSS-API applications may accept unkeyed checksums
* krb5 application services may accept unkeyed PAC checksums
* krb5 KDC may accept low-entropy KrbFastArmoredReq checksums
```

Failles / Bulletins / Advisories

Microsoft - Avis Novembre 2014

MS14-069 Vulnérabilité Word 2007 (3 CVE) [Exploitabilité 1]

- Affecte:
  - Microsoft Office 2007 Service Pack 3 (Word)
  - Visionneuse Microsoft Word
- Exploit:
  - Exécution de code à l'ouverture d'un fichier Office spécialement formaté
- Crédits:
  - Ben Hawkes de Google Project Zero (CVE-2014-6333, CVE-2014-6334, CVE-2014-6335)

MS14-070 Vulnérabilité dans la pile TCP/IP (tcpip.sys) (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows 2003
  - Correctif pour Windows XP Embedded POSReady, kb2939576 (cf. screenshot après)
- Exploit:
  - Élévation de privilèges locale lors d'appels aux contrôles de la pile TCP/IP (Déréférencement de pointeur NULL dans tcpip.sys)
- Crédits:
  - Matt Bergin de KoreLogic Security (CVE-2014-4076)

Failles / Bulletins / Advisories

Microsoft - Avis Novembre 2014

MS14-071 Vulnérabilité du Service Audio de Windows (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - Élévation de privilèges locale par la lecture de lien symbolique dans le registre et évasion de la sandbox (d'IE par exemple)
  - Intéressant combiné une vulnérabilité d'exécution de code dans IE
- Crédits:
  - James Forshaw de Google Project Zero (CVE-2014-6322)

MS14-072 Élévation de privilèges dans .NET (1 CVE) [Exploitabilité 2]

- Affecte:
  - .NET Framework (toutes versions supportées)
- Exploit:
  - Élévation de privilèges à distance si l'application utilise .NET Remoting (Appel à des objets distants)
  - Détails : http://tyranidslair.blogspot.co.uk/2014/11/stupid-is-as-stupid-does-when-it-comes.html
  - Code d'exploitation : https://github.com/tyranid/ExploitRemotingService
- Crédits:
  - James Forshaw de Context Information Security (CVE-2014-4149)

Failles / Bulletins / Advisories

Microsoft - Avis Novembre 2014

MS14-073 Élévation de privilèges dans Sharepoint Serveur (1 CVE) [Exploitabilité 2]

- Affecte:
  - Microsoft SharePoint Server 2010 Service Pack 2
- Exploit:
  - XSS par un utilisateur authentifié
- Crédits:
  - Drew Calcott de EY (CVE-2014-4116)

MS14-074 Vulnérabilité dans RDP (1 CVE) [Exploitabilité 3]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - Contournement de l'enregistrement des traces de sécurité (audit logging events), permettant par exemple de brute-forcer un mot de passe sans trace.
- Crédits:
  - ?

MS14-075 (? CVE) [Exploitabilité ?]

"Release date to be determined."

Failles / Bulletins / Advisories

Microsoft - Avis Novembre 2014

MS14-076 Contournement de sécurité dans Microsoft IIS (1 CVE) [Exploitabilité 3]

- Affecte:
  - Windows 8, 8.1 (IIS 8.0 et 8.5)
  - Windows Server 2012 et R2 (IIS 8.0 et 8.5)
- Exploit:
  - Contournement de la fonctionnalité de restriction (filtrage) par IP et domaine de IIS
- Crédits:
  - ?

MS14-077 Vulnérabilité dans ADFS (1 CVE) [Exploitabilité 3]

- Affecte:
  - Windows 8 (ADFS 2.0)
  - Windows 2012 (ADFS 21 et 3.0)
- Exploit:
  - ADFS = SSO de Microsoft, transformation de jetons SAML en Kerberos...
  - Réutilisation d'un jeton dans le cas d'un utilisateur ne s’étant pas explicitement déconnecté
- Crédits:
  - ?

Failles / Bulletins / Advisories

Microsoft - Avis Novembre 2014

MS14-078 Vulnérabilité dans le clavier visuel (IME) (1 CVE) [Exploitabilité 0]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - Élévation de privilèges / évasion de la sandbox dans le cas de l'utilisation d'un clavier Japonais spécialement formaté (Input Method Editor / IME)
- Crédits:
  - Vitaly Kamluk et Costin Raiu de Kaspersky Lab (CVE-2014-4077)

MS14-079 Failles Noyau dans win32k.sys (1 CVE) [Exploitabilité 3]

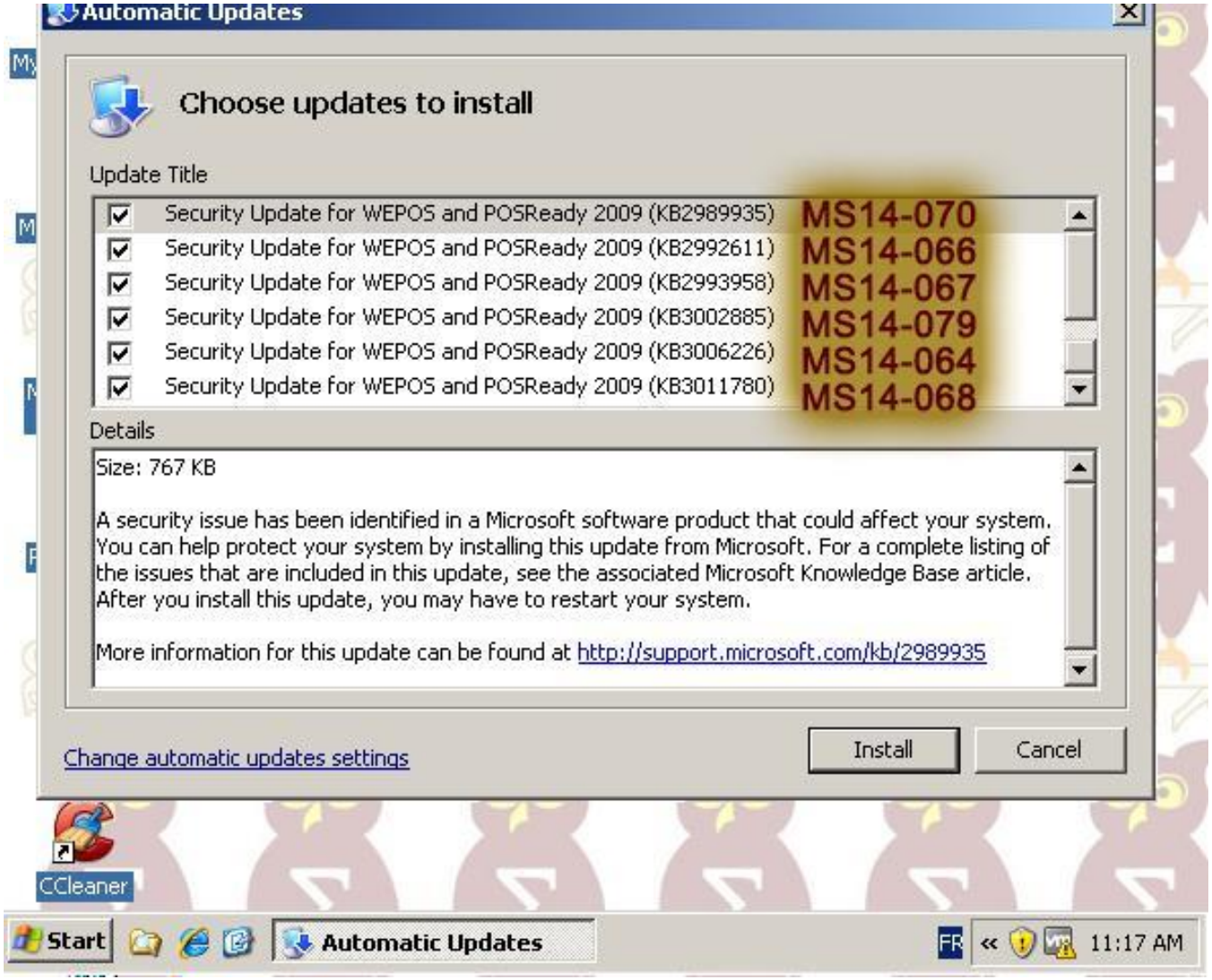
- Affecte:
  - Windows, toutes versions supportées
  - Correctif pour Windows XP Embedded POSReady, kb2939576 (cf. screenshot après)
- Exploit:
  - Déni de service lors du traitement d'un fichier de police de caractères spécialement formaté
- Crédits:
  - Secunia Research (CVE-2014-6317)

Failles / Bulletins / Advisories

Microsoft - Avis Novembre 2014

Mise à jour pour Windows XP Embedded POSReady

- Encore et toujours sans documenter dans les bulletins…



Failles / Bulletins / Advisories

Microsoft - Advisories et Revisions Novembre 2014

3010060 Vulnérabilité dans le composant OLE

- V2.0 Mise à jour liée à la publication du bulletin MS14-064

2755801 Mise à jour de Flash Player

- V32.0 Nouvelle mise à jour de Flash Player

Failles / Bulletins / Advisories

Microsoft - Autre

Windows 10

- Supportera HTTP/2
  http://www.zdnet.fr/actualites/http-2-microsoft-s-y-met-aussi-39807713.htm
- Passera du noyau 6 au 10
  http://arstechnica.com/information-technology/2014/11/why-windows-10-isnt-version-6-any-more-and-why-it-will-probably-work/

Azure

- Panne suite à une mise à jour pour optimisation
  http://www.lemondeinformatique.fr/actualites/lire-la-panne-d-azure-provoquee-par-une-mise-a-jour-de-performance-59336.html

Failles / Bulletins / Advisories

Système (principales failles)

OpenVPN

- Déni de service (CVE-2014-8104)
  http://www.net-security.org/secworld.php?id=17708

Puppet Enterprise

- Exécution de code (CVE-2014-3248) et divulgation d'information (CVE-2014-3249)
  http://puppetlabs.com/security/cve/cve-2014-3248
  http://puppetlabs.com/security/cve/cve-2014-3249

phpMyAdmin 4.0|1|2.x

- XSS, inclusion de fichier local...
  http://www.phpmyadmin.net/home_page/security/PMASA-2014-13.php
  http://www.phpmyadmin.net/home_page/security/PMASA-2014-14.php
  http://www.phpmyadmin.net/home_page/security/PMASA-2014-15.php
  http://www.phpmyadmin.net/home_page/security/PMASA-2014-16.php

Bind, Unbound et PowerDNS

- Dénis de service CVE-2014-8500, CVE-2014-8601 et CVE-2014-8602
  http://seenthis.net/messages/320210

Failles / Bulletins / Advisories

Apple

iOS et ses Backdoors, La suite (cf. Revue 2014-09-09)

- com.apple.mobile.file_relay désactivé mais réactivable (par MDM)
- Reste possible d'accéder à la sandbox des applications depuis une connexion physique
  http://www.zdziarski.com/blog/?p=3820
- Apple dispose toujours de la capacité de tout récupérer sans le consentement de l'utilisateur
  https://www.apple.com/legal/more-resources/law-enforcement/

Yosemite 10.10

- Enregistrement de l'activité utilisateur dans /tmp/CGLog_* par le service CoreGraphics
  http://blog.marcfredericgomez.com/mozilla-foundation-security-advisory-2014-90/
- Déjà corrigé par Mozilla
  https://www.mozilla.org/en-US/security/advisories/mfsa2014-90/

Failles / Bulletins / Advisories

Crypto

Nouvelle technique de désanonymisation de TOR / onion

- A base de NetFlow
  https://mice.cs.columbia.edu/getTechreport.php?techreportID=1545&format=pdf&
- Efficient sur un petit réseau mais trop de faux positifs dans la vie réelle
  https://blog.torproject.org/blog/traffic-correlation-using-netflows

Failles / Bulletins / Advisories

Divers

XSS permanent dans le CMS “LifeRay”

- Permet à un utilisateur authentifié d’injecter du code lors du téléversement d’un fichier

http://seclists.org/fulldisclosure/2014/Nov/61

Centreon, exécution de code à distance (remote) sans authentification (pre-auth)

- Lors de l'enregistrement des traces de l’authentification d’un utilisateur
  - exec("echo \"".$string."\" >> ".$this->errorType[$id]);
  - Au lieu d’un simple file_put_contents(fichier, données, FILE_APPEND) ou fopen/write/close

http://www.openwall.com/lists/oss-security/2014/11/28/2

Faille de sécurité dans un produit de la CNIL

http://seclists.org/fulldisclosure/2014/Nov/3

Piratages, Malwares, spam, fraudes et DDoS
Espionnage

Regin, le malware du GCHQ ou de la NSA

- Information publiée par Symantec le 23/11/2014 et Kaspersky

  http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/regin-analysis.pdf

  http://securelist.com/blog/research/67741/regin-nation-state-ownage-of-gsm-networks/
- Cible : Russie, l'Arabie Saoudite, Belgacom...
- Actif depuis au moins 2008
- Complexe et modulaire, difficile à analyser

  https://t.co/KGpFRD3Yc4
- C&C reposant sur l'échange de données avec d'autres pairs infectés, ainsi que des serveurs centraux, selon plusieurs protocoles (ICMP, HTTP, protocoles propriétaires)
- Le malware a notamment été détecté sur des équipements d'infrastructure réseau mobiles (BSC, *Base Station Controller*), et aurait ainsi pu permettre d'accéder aux données échangées

  https://firstlook.org/theintercept/2014/11/24/secret-regin-malware-belgacom-nsa-gchq/

  http://www.symantec.com/connect/blogs/regin-top-tier-espionage-tool-enables-stealthy-surveillance

  http://www.theregister.co.uk/2014/11/26/symantec_explains_why_regin_fingering_took_so_long_and_who_its_coming_for_next/

  https://firstlook.org/theintercept/2014/11/24/secret-regin-malware-belgacom-nsa-gchq/

Piratages, Malwares, spam, fraudes et DDoS

Espionnage

Stuxnet, le patient zéro ?

- Découvert par Kaspersky
- Déposé par un autre virus (Duqu?)
- Chez des fournisseurs de la centrale nucléaire iranienne de Natanz (Behpajooh et Kala)
- Propagation entre Behpajooh et Mobarakeh Steel Company, puis mondiale du fait de ses contacts commerciaux à l'international
  http://securelist.com/analysis/publications/67483/stuxnet-zero-victims/

US Marshals : programme d'écoute des communications

- Grâce à des avions simulant des antennes GSM
  http://online.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533

Les Chinois préfèrent installer des antennes

- Sur leurs ambassades, en proche banlieue Parisienne (Chevilly-Larue (Val-de-Marne)
  www.leparisien.fr/international/un-centre-d-ecoute-secret-chinois-decouvert-dans-le-val-de-marne-03-12-2014-4344093.php

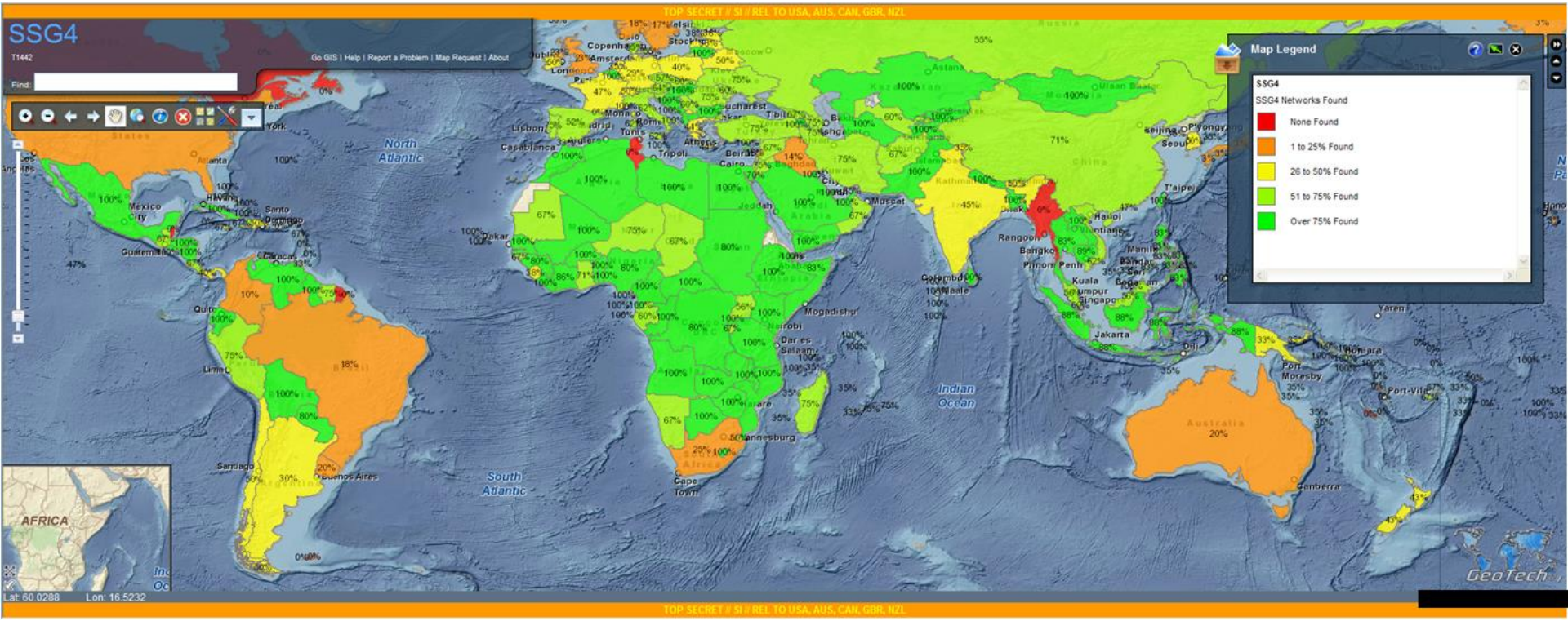
Piratages, Malwares, spam, fraudes et DDoS

Espionnage

Aurora Gold

- Espionnage des conversations GSM de la planète
- Participation aux groupes de travail des standards (GSMA)
  - Pour affaiblir la sécurité des standards

http://investmentwatchblog.com/new-snowden-docs-reveal-nsa-spy-tactic-a-new-report-by-the-intercept-exposes-a-massive-program-called-operation-aurora-gold/



Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Sony Pictures piraté

- Les employés se rendant au bureau le 24/11 ont découvert ce nouveau fond d'écran
- Vol de **11To** voir **100To** :
  - Films exclusifs (Annie, Mr. Turner, et Still Alice, To Write Love)
  - Numéros de CB
  - Numéros de sécurité sociale (dont Rambo)
  - Contrat de nudité de Sharon Stone ;-)
  - Données RH, primes...
- Menaces sur des employés et leur famille
  - S'ils ne coopèrent pas
- Les cafés du studio n'acceptent plus que le cash, au cas où les POS seraient affectés…

http://fusion.net/story/31116/inside-sony-pictures-employees-are-panicking-about-their-hacked-personal-data
http://threatpost.com/sony-pictures-dealing-with-apparent-network-compromise/109625
http://www.01net.com/editorial/633693/un-groupe-de-pirates-s-attaque-a-sony-pictures/
http://www.scmagazineuk.com/hackers-blackmail-sony-film-company/article/385140/

- L'intrusion aurait débuté par l'aide d'internes

http://www.silicon.fr/securite-fireeye-absorbe-mandiant-lutter-apt-91822.html

- Mandiant est sur le coup !

- C'est au tour du PlayStation Network

http://www.01net.com/editorial/635855/apres-sony-pictures-ce-serait-au-tour-du-playstation-network-d-etre-attaque/

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Des smartphones android pré-trojané avant l'achat

http://www.net-security.org/malware_news.php?id=2917

Mobile Pwn2Own Tokyo 2014

- Apple Phone 5S -> pwnd
- Android (Samsung Galaxy S5), mobile OS -> pwnd
- Android (Samsung Galaxy S5), Wi-Fi -> pwnd
- Android (LG Nexus 5), NFC -> pwnd
- Amazon Fire Phone, mobile OS -> pwnd
- Windows Phone (Nokia Lumia 1520?), navigateur -> partiel
- Android, Wi-Fi -> partiel
- BlackBerry Z30 -> ?

  http://h30499.www3.hp.com/t5/HP-Security-Research-Blog/Mobile-Pwn2Own-begins-Competitors-and-targets/ba-p/6669308#.VHxa9MkUpT0

Les Macro Word malveillantes fonctionnent toujours

- Sur les VIP 

  http://www.01net.com/editorial/635109/des-pdg-et-des-directeurs-financiers-pieges-avec-des-macros-word/

Piratages, Malwares, spam, fraudes et DDoS

Malware

Citadel

- La nouvelle version vise les gestionnaires de mots de passe sécurisés
  http://www.undernews.fr/malwares-virus-antivirus/la-nouvelle-version-du-trojan-citadel-sen-prend-aux-gestionnaires-de-mots-de-passe-securises.html

CryptoPhp

- Plus de 23 000 serveurs infectés
- Utilisé principalement pour d'améliorer le score de sites malveillants dans les moteurs de recherche (BHSEO / Black hat search engine optimisation)
  https://foxitsecurity.files.wordpress.com/2014/11/cryptophp-whitepaper-foxsrt-v4.pdf

Vietnam, Inde et Indonésie, nouvelles sources de botnet

- Principalement pour faire du DDoS
- Heureusement, leurs infrastructures ne suivent pas et ont une faible bande passante
  http://blog.blacklotus.net/2014/11/black-lotus-threat-report-reveals.html

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Piratage du site BrowserStack par l'exploitation de ShellShock

- Récupération de la clef secrète AWS (BrowserStack hébergé chez Amazon)
- Création d'un compte, pilotage de l'infrastructure et exfiltration de données
  http://www.browserstack.com/attack-and-downtime-on-9-November

Home Depot (Cf. Revue 2014-10-14 et 2014-11-18)

- $43 millions pour gérer l'intrusion
- Dont $15 millions de remboursés par les assurances ("it believes are reimbursable")
  http://www.sec.gov/Archives/edgar/data/354950/000035495014000047/hd_10qx11022014.htm#s32A1FFEE973AED8DE2D022502670CD7E

Piratage de Domino's Pizza

- Chantage sans succès
- Donc publication de la base sur internet
  - http://www.lemonde.fr/pixels/article/2014/11/21/apres-son-piratage-la-base-de-donnee-de-domino-s-pizza-publiee-sur-internet_4525393_4408996.html

Michelin, arnaque au président pour 1,6 million d'euros

http://www.francetvinfo.fr/faits-divers/michelin-victime-d-une-escroquerie-d-un-montant-de-1-6-million-d-euros_735729.html

Piratages, Malwares, spam, fraudes et DDoS
Internet des Objets

Une variante de Bashlite exploite la vulnérabilité Shellshock pour infecter tous les appareils utilisant le logiciel BusyBox

- La préclassiquesence de BusyBox dans l'embarqué complique considérablement la recommandation de mise à jour.

  http://securityaffairs.co/wordpress/30225/cyber-crime/bashlite-exploits-shellshock.html

  http://blog.trendmicro.com/trendlabs-security-intelligence/bashlite-affects-devices-running-on-busybox/

Des malwares USB dans les cigarettes électroniques chinoises ?

- Probablement un fake, bien que le scénario soit possible

  http://www.generation-nt.com/cigarette-electronique-malware-e-cigarette-usb-actualite-1909034.html

  http://www.undernews.fr/malwares-virus-antivirus/des-malwares-usb-dans-les-cigarettes-electroniques-chinoises.html

Ingénierie à reculons d'une alarme domestique sans fil

- Intéressant pour la méthodologie
- Pour une fois, ce n'est pas si catastrophique :)

  http://funoverip.net/2014/11/reverse-engineer-a-verisure-wireless-alarm-part-1-radio-communications/

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

Pentest

Techniques & outils

DevOOps ….

- Présentation de Carnal0wnage et Ken Johnson
- Aborde les vulnérabilités courantes des outils utilisés par le courant DevOps : git, chef, puppet, jenkins, …
  http://fr.slideshare.net/chrisgates/lascon-2014-devooops

Une interface REST en Python pour Nessus 6

https://github.com/tenable/nessrest

Utilisation de Shodan en ligne de commande

http://shodanio.wordpress.com/2014/12/01/using-shodan-from-the-command-line/

Scada
Divers

ICS Whitelist, une base de données de fichiers sains

- Plus de 350 000 fichiers existants
- Permet d'uploader un fichier et de le comparer à celui existant dans la base
- Les logiciels de plusieurs constructeurs sont présents : ABB, Rockwell, Siemens, GE, Matrikon, Schneider,...

http://icswhitelist.com/

Encore des vulnérabilités dans les logiciels Siemens (WinCC, TIA Portal, PCS7)

- Exécution de code arbitraire à distance

https://ics-cert.us-cert.gov/advisories/ICSA-14-329-02A

Déni de service sur le serveur OPC de Matrikon

- Via la pile DNP3

https://ics-cert.us-cert.gov/advisories/ICSA-14-329-01

Nouveautés (logiciel, langage, protocole...)

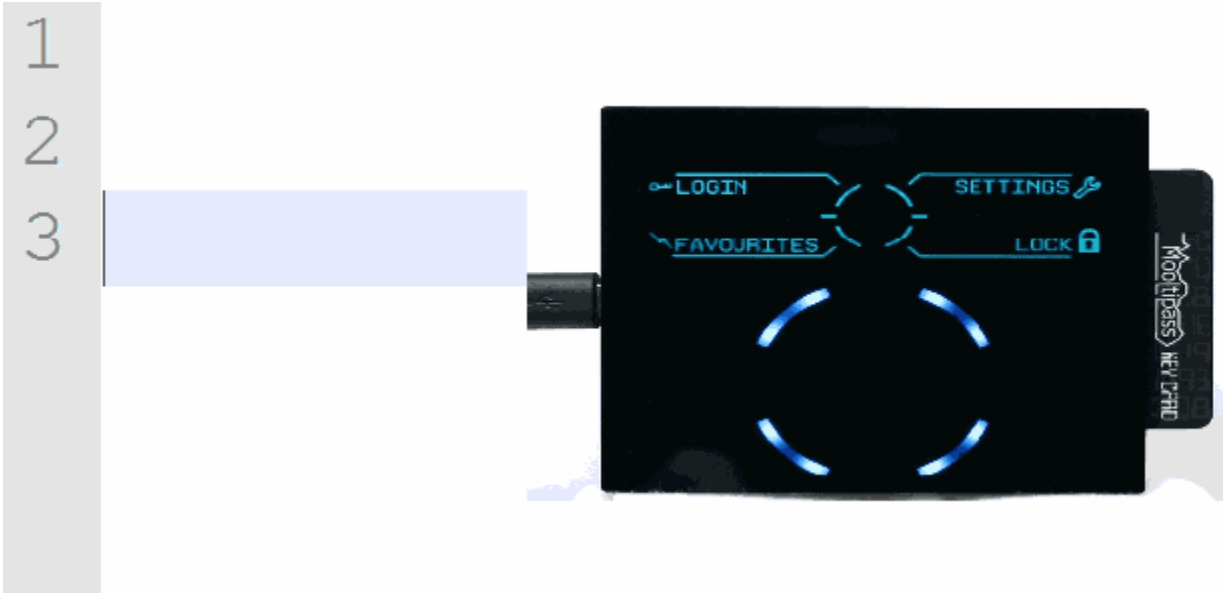
Open Source

Toolkit de test de couverture des scanners de vulnérabilités web

- Publié par Google
- Mais sans le nouveau scanneur de vulnérabilité web
  http://googleonlinesecurity.blogspot.fr/2014/11/ready-aim-fire-open-source-tool-to-test.html

Password manager offline open-source

- Actuellement sur Indiegogo (plateforme de financement collaboratif)
  http://blog.atmel.com/2014/12/02/mooltipass-is-an-open-source-offline-password-keeper/
  https://github.com/limpkin/mooltipass
  https://www.indiegogo.com/projects/mooltipass-open-source-offline-password-keeper



Nouveautés (logiciel, langage, protocole...)

Open Source

Guide de sécurisation des SCADA

- Par la Sécurité Civile Suédoise
  https://www.msb.se/RibData/Filer/pdf/26118.pdf
- Pour compléter ceux de l'ANSSI et du NIST
  http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf
  http://www.ssi.gouv.fr/fr/menu/actualites/l-anssi-publie-des-mesures-visant-a-renforcer-la-cybersecurite-des-systemes.html

Noping, le ping amélioré

http://noping.cc/

Git pour les nuls

http://articles.nissone.com/2014/11/gitpourlanulle/

Lock picking pour les nuls ?

http://sploid.gizmodo.com/this-cutaway-video-shows-how-to-pick-a-lock-perfectly-1655216796

Clé usb entièrement opensource avec crypto

http://inversepath.com/usbarmory

Nouveautés (logiciel, langage, protocole...)

Open Source

NetFlix, les ingénieurs du Chaos et l'armée des singes

- Des ingénieurs du chaos pour générer des pannes
  http://techblog.netflix.com/2014/09/introducing-chaos-engineering.html
- Des outils de génération de panne « Simian Army »
  http://techblog.netflix.com/2011/07/netflix-simian-army.html
- En bonus, leur outil de supervision « Hystrix »
  http://github.com/Netflix/Hystrix

Nouveautés (logiciel, langage, protocole...)

Divers

Let’s Encrypt, nouvelle autorité de certification pour favoriser l’adoption du HTTPS

- Créé gratuitement par L'EFF, Cisco, Mozilla et leurs partenaires
  - En concurrence de StartSSL
- Pour améliorer la sécurité globale d’Internet
- Disponible à l’été 2015

http://www.scmagazineuk.com/lets-encrypt-aims-to-drive-adoption-of-https/article/384136/
https://www.schneier.com/blog/archives/2014/11/a_new_free_ca.html
https://letsencrypt.org/2014/11/18/announcing-lets-encrypt.html

Le shodan des systèmes industriels accessibles sur Internet

https://icsmap.shodan.io/

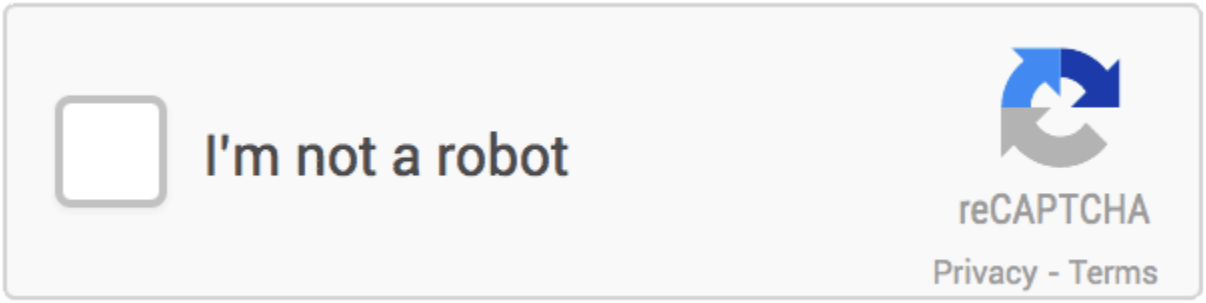
Nouveautés (logiciel, langage, protocole...)

Divers

No Captcha reCAPTCHA

- Nouvelle version des captchas Google
- Plus besoin d'entrer de texte, il suffit de cocher une case !
- Pas trop de détails techniques, mais il semblerait que le fonctionnement soit lié à la présence de cookies, indiquant la résolution passée de captchas

http://googleonlinesecurity.blogspot.fr/2014/12/are-you-robot-introducing-no-captcha.html



- Mais cette nouvelle version serait vulnérable au clickjacking, qui permettrait de "crowdsourcer" la résolution de captcha à l'insu des utilisateurs
  http://homakov.blogspot.fr/2014/12/the-no-captcha-problem.html

Business
France

Les sociétés d'écoutes téléphoniques se rebellent

- Suite à l'arrivée de la nouvelle plateforme d'interceptions judiciaires
  http://www.lefigaro.fr/flash-eco/2014/11/14/97002-20141114FILWWW00019-france-les-ecoutes-telephoniques-menacees.php

VUPEN quitte la France

- Pour le Maryland, le Luxembourg et Singapour
  http://lexpansion.lexpress.fr/high-tech/les-mercenaires-de-la-cyberguerre_1623549.html

Altice termine son rachat de SFR

http://pro.01net.com/editorial/634257/le-rachat-de-sfr-par-altice-et-numericable-est-boucle/

- Et continue sa boulimie avec Portugal Telecom pour plus de 7 milliards d'euros
  http://pro.clubic.com/actualite-e-business/investissement/actualite-742237-sfr-virgin-mobile-altice-offre-portugal-telecom.html

Bridage de Free sur ses lignes portées par Orange ?

- Le doute subsiste...
  http://www.zdnet.fr/actualites/free-mobile-enquete-sur-le-bridage-des-debits-en-itinerance-39805877.htm

Business

International

Officiel : Amazon possède désormais « .book »

http://rue89.nouvelobs.com/2014/11/13/officiel-amazon-possede-desormais-mot-book-256029

Facebook prépare une nouvelle version pour professionnels

http://techno.lapresse.ca/nouvelles/internet/201411/16/01-4819537-facebook-prepare-une-nouvelle-version-pour-professionnels.php

Droit / Politique

France

Détecteurs de fumée à chambre d'ionisation vs optique

- Obligatoire dès le 8 mars prochain chez les particuliers
- Détecteurs ioniques interdits depuis 2011 avec une limite au 31 déc. 2017
  http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=98797EDD5FD94A05AC97808311F403F8.tpdjo16v_2?cidTexte=JORFTEXT000024908599&dateTexte=&oldAction=rechJO&categorieLien=id

Lorsqu'on oublie les mentions légales

- Cela coûte 5000 euros
  http://www.donneespersonnelles.fr/mentions-legales-absentes-5000-euros-la-ligne

Fleur Pellerin décore la présidente de la Hadopi

http://www.nextinpact.com/news/90987-fleur-pellerin-decore-mireille-imbert-quaretta-hadopi.htm

L'administration demande beaucoup de réquisitions judiciaires aux réseaux sociaux

http://www.numerama.com/magazine/31185-l-inquietante-faible-qualite-des-demandes-de-la-france-a-facebook.html

Drones de loisir

- Officiellement autorisés en France début 2015
  http://drones.blog.lemonde.fr/2014/11/04/les-drones-de-loisirs-bientot-officiellement-autorises/

Droit / Politique

France

Un juge demande les empreintes d'un accusé pour déverrouiller son Smartphone
http://www.journaldugeek.com/2014/11/05/un-juge-demande-les-empreintes-dun-accuse-pour-deverrouiller-son-smartphone/

Copie privée

- Se faire rembourser en toute discrétion (pour les professionnels)
  http://www.nextinpact.com/news/90976-professionnels-voila-discrete-page-pour-se-faire-rembourser-copie-privee.htm

Traiter son patron de « boulet » et de « guignol » sur Facebook peut être une faute grave
http://www.nextinpact.com/news/90698-traiter-son-patron-boulet-et-guignol-sur-facebook-peut-etre-faute-grave.htm

Licencié pour téléchargement illégal, un salarié obtient gain de cause devant la justice
http://www.nextinpact.com/news/90813-licencie-pour-telechargement-illegal-salarie-obtient-gain-cause-devant-justice.htm

Droit / Politique
International

L'ICANN pourrait d'émanciper des USA

- Une nouvelle proposition de loi « pourrait » être votée l'année prochaine
  http://www.linformaticien.com/actualites/id/34488/gouvernance-d-internet-l-icann-s-emancipera-du-controle-americain-avant-2016.aspx

Amende aux USA suite au stockage de données en clair

- $10 millions pour YourTel America et TerraCom n'ayant pas respecté les lois de protection des données personnelles
  http://www.fcc.gov/document/fcc-plans-10m-fine-carriers-breached-consumer-privacy

Facebook et le tracking par Atlas

- Vision 306° (Smartphone, PC, tablette)
  http://pro.clubic.com/blog-forum-reseaux-sociaux/facebook/actualite-741209-atlas.html

Quand le Parlement Européen essaie de démanteler Google

http://www.01net.com/editorial/633579/l-ombre-du-groupe-axel-springer-plane-derriere-le-demantelement-de-google/

- Et quand l'UE veut passer les GAFA sous le contrôle des agences nationales de sécurité
  http://www.lesechos.fr/tech-medias/hightech/0203969133313-cybersecurite-frictions-entre-letat-et-le-monde-numerique-1068536.php
  http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/trans/145966.pdf

Droit / Politique

International

Pour Obama, Internet devrait être classé service d'utilité publique

http://www.nextinpact.com/news/90863-pour-obama-internet-devrait-etre-classe-service-dutilite-publique.htm

Compétences : France vs USA

- <<Aux US, un juge a appris Java pour mieux juger une affaire. En France, la justice se flatte de ne rien comprendre au fond technologique.>>
  https://twitter.com/pbeyssac/status/535080198593851392

Le gouvernement Allemand subit 3,000 attaques par jour

http://news.yahoo.com/top-german-spy-says-berlin-under-cyber-attack-185257560.html

L'Internet Achitecture Board (IAB) demande de tout chiffrer

http://www.numerama.com/magazine/31295-l-internet-achitecture-board-iab-demande-a-tout-chiffrer-par-defaut.html

Google refuse de blacklister des sites pirates

- Malgré les demandes de la MPAA
- Demandes de trop larges : Les listes contenaient les racines et non les pages précises
  http://www.01net.com/editorial/633593/google-refuse-la-demande-de-la-mpaa-de-blacklister-des-sites-pirates/

Droit / Politique
International

Twitter va récupérer la liste de vos applications

- « Cette mise à jour comprend des améliorations **mineures** »
- Pour faire de l'analyse comportementale et du profilage
  https://support.twitter.com/articles/20172069-what-is-app-graph-on-twitter

Wifi dans les avions Air France

http://www.nextinpact.com/news/91126-air-france-relance-wi-fi-via-satellite-dans-ses-avions-avec-orange.htm

La Russie bannira iPhone et iPad dès janvier 2015

- A cause d'iCloud
  http://www.ubergizmo.com/2014/11/russia-to-ban-the-iphone-and-ipad-on-january-1st-2015/
- Déjà initié en début d'année, Cf. Revue 2014-05-13
  - Avec en cible RomOS <<Российская мобильная операционная система>>

L'Allemagne pourrait forcer les sociétés américaines à dévoiler leurs codes-source

http://www.nextinpact.com/news/90772-l-allemagne-pourrait-forcer-societes-americaines-a-devoiler-leurs-codes-source.htm

Conférences

Texte en gris = déjà traité précédemment

Passées

- No Such Con - 19 au 21 novembre 2014 à Paris
  - Slides : http://www.nosuchcon.org/talks/2014/
- Bot Conf - 3 au 5 Décembre 2014 à Nancy
  - Slides et vidéos : https://www.botconf.eu/botconf-2014/documents-and-videos/

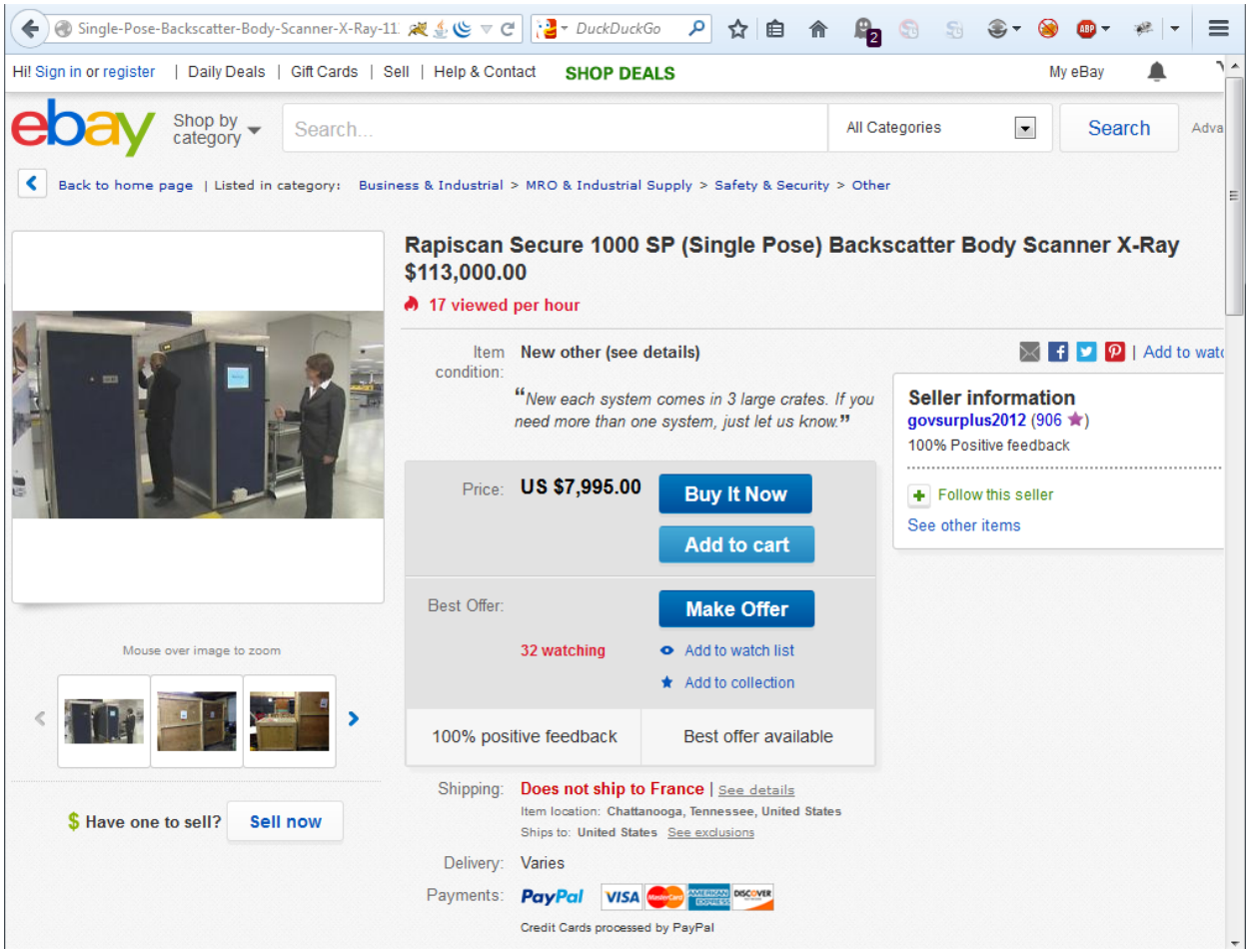
A venir

- FIC 2015 - 20 et 21 janvier 2015 à Lille
  - Avec du Bruce Schneier dedans !
- JSSI 2015 - 10 mars 2015 à Paris
- GS Days - 24 mars 2015 à Paris

Divers / Trolls velus

eBay...

- Rapiscan Secure 1000 SP (Single Pose) Backscatter Body Scanner X-Ray
  http://www.ebay.com/itm/Rapiscan-Secure-1000-SP-Single-Pose-Backscatter-Body-Scanner-X-Ray-113-000-00-/111519265986?pt=LH_DefaultDomain_0&hash=item19f710f4c2



Divers / Trolls velus

Surface vs MacBook

- Bien qu'autorisée, la publicité comparative se fait rare...
  https://www.youtube.com/watch?v=l_svTil_EFM

Huawei vs Windows Phone

- <<We didn’t make any money in Windows Phone. Nobody made any money in Windows Phone>>
  http://seattletimes.com/html/businesstechnology/2025131855_chinahuaweixml.html

Publicitaires francais vs Eyeo (éditeur d'AdBlock)

http://www.lesechos.fr/tech-medias/medias/0203983694287-les-editeurs-francais-prets-a-poursuivre-en-justice-les-bloqueurs-de-publicite-1070602.php

CNIL vs Quadrature du Net

- Droit à l'oubli vs liberté d'expression et accès à l'information
  https://www.laquadrature.net/fr/droit-a-loubli-la-cnil-sadoube-censeur-du-net

Créateur présumé du Bitcoin vs Newsweek

- Il nie, poursuit Newsweek en justice et … demande des dons en Bitcoins
  http://techcrunch.com/2014/10/13/dorian-nakamoto-is-suing-newsweek/

Divers / Trolls velus

Chiffrer sur Smartphone, c'est tuer un enfant !

- Heureusement qu'il reste les "fonctionnalités" de debug
  http://www.phonandroid.com/le-chiffrement-des-smartphones-va-mener-la-mort-denfants-selon-la-justice-americaine.html

<< They're not hackers - they're "undocumented admins">>

https://twitter.com/agentdarkapple/status/536927589253009409

Divers / Trolls velus

Comment j'ai “rétro ingénieré“ Google Docs

http://features.jsomers.net/how-i-reverse-engineered-google-docs/

Google Glass : les magasins physiques de Google vont fermer !

https://www.aruco.com/2014/11/google-glass-fermeture/

Après Google (cf. Revue 2014-10-14), c'est au tour de Facebook d'augmenter son Bug bounty

- Pour sa régie publicitaire

https://www.facebook.com/notes/protect-the-graph/doubling-up-on-ads-code-bounties/1519314984975314

Sortie de l'ombre Project Zero communique

- Avec des PoC de différentes vulnérabilités
  - MS, Adobe, Mac

http://googleprojectzero.blogspot.fr/2014/11/project-zero-patch-tuesday-roundup.html

Divers / Trolls velus

NSA Playset

- Michael Ossmann reconstruit certains outils d'écoute de la NSA à moins de $100
- Au programme :
  - De l'écoute et de l'injection Wifi (classique)
  - De l'écoute et de la triangulation GSM
  - Implant PCI, Ethernet, Routeur, câble VGA, Firewall (Cisco PIX, Huawei, Juniper), Bios, Firmware du disque dur, Master Boot Record…
- Le blog
  http://ossmann.blogspot.fr/2014/07/the-nsa-playset.html
- Les outils
  http://www.nsaplayset.org/

Divers / Trolls velus

Élection UMP

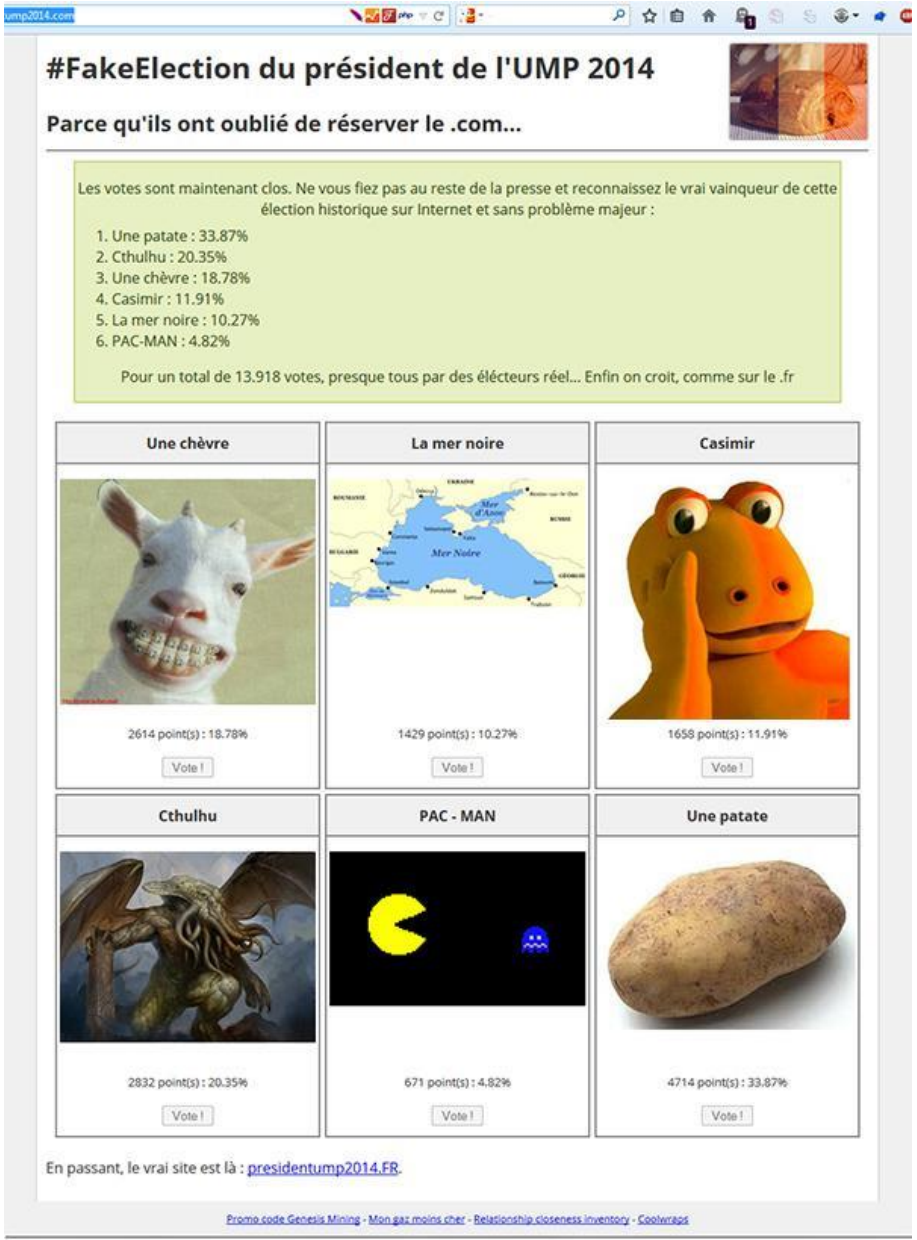
- DDoS, tentatives d'intrusion... tellement prévisible
- Infrastructure de vote gérée par un spécialiste... du vote de syndic d'immeuble
  http://reflets.info/elections-ump-et-le-gagnant-est-bozo-le-clown/
- "C'était des attaques très organisées, des attaques massives, de haut niveau."
  - Un botnet à 5$/h pour DDoSer, est-il une attaque de haut niveau ? ;-)

- 26 requêtes/s ou 26 000 requêtes/s ?
  http://www.01net.com/editorial/634550/vote-a-lump-une-attaque-par-deni-de-service-est-tres-simple-a-mettre-en-place/
- Autre liens
  http://www.bfmtv.com/politique/l-ump-porte-plainte-apres-des-cyber-attaques-contre-son-site-849527.html
  http://www.nextinpact.com/news/91153-vote-electronique-victime-cyber-attaques-l-ump-porte-plainte.htm?skipua=1

Divers / Trolls velus

Election UMP (suite)

- La version .com déposée par un plaisantin
  http://presidentump2014.com/



Prochaines réunions

Prochaines réunions

- Mardi 13 Janvier 2015

Afterwork

- Date à déterminer

En attendant…

Et d’ici la prochaine réunion...

Questions ?