
OSSIR
Groupe Paris
Réunion du 14 janvier 2014



Revue des dernières vulnérabilités

Nicolas RUFF
nicolas.ruff (à) gmail.com

■ Décembre 2013

- **MS13-096 Faille dans le support TIFF par GDI+ (x1) [1]**
 - **Affecte:**
 - Windows Vista / 2008
 - Office (toutes versions supportées sauf 2013)
 - Lync 2010 / 2013
 - **Exploit: exécution de code arbitraire à l'ouverture d'un fichier TIFF malformé**
 - Exploité dans la nature en "0day"
 - <http://www.crowdstrike.com/blog/analysis-cve-2013-3906-exploit/index.html>
 - **Crédits: Haifei Li / McAfee Labs IPS Team**

Avis Microsoft

- **MS13-097 Correctif cumulatif pour IE (x7) [1,1,1,1,1,2,1]**
 - **Affecte: IE (toutes versions supportées)**
 - **Exploit:**
 - **Élévation de privilèges**
 - **Corruptions mémoire conduisant à l'exécution de code arbitraire**
 - **Crédits:**
 - **James Forshaw / Context Information Security (x2)**
 - **Abdul-Aziz Hariri / ZDI**
 - **Anonymous + ZDI**
 - **Jose Antonio Vazquez Gonzalez + ZDI**
 - **Atte Kettunen / OUSPG**
 - **Bo Qu / Palo Alto Networks**
 - **Alex Inführ**

- **MS13-098 Contournement de la signature Authenticode (x1) [1]**
 - Affecte: Windows (toutes versions supportées)
 - Exploit: modification d'un exécutable sans invalider sans signature
 - Exploité dans la nature en "0day"
 - <http://blogs.technet.com/b/srd/archive/2013/12/10/ms13-098-update-to-enhance-the-security-of-authenticode.aspx>
 - Crédits: Kingsoft Internet Security Center

- **MS13-099 Faille dans Windows Script (x1) [1]**
 - Affecte: Windows Script 5.6, 5.7 et 5.8 (Windows toutes versions supportées)
 - Exploit: "use after free" conduisant à l'exécution de code arbitraire
 - Crédits: n/d

Avis Microsoft

- **MS13-100 Faille SharePoint (x1) [1]**
 - **Affecte:**
 - SharePoint Server 2010 SP1 / 2010 SP2 / 2013
 - Office Web Apps 2013
 - **Exploit: exécution de code sous l'identité W3WP**
 - Authentification requise
 - **Crédits: n/d**

- **MS13-101 Failles noyau (x5) [2,1,3,2,3]**
 - **Affecte: Windows (toutes versions supportées)**
 - **Exploit: élévation de privilèges locale**
 - Corruptions mémoire dans WIN32K.SYS
 - "Use after free" dans WIN32K.SYS
 - Faille dans le support TrueType
 - "Double fetch" dans PORTCLS.SYS
 - "Integer overflow" dans WIN32K.SYS
 - **Crédits:**
 - Renguang Yuan / Qihoo
 - Ling Chuan Lee / F13 Laboratory
 - Nicolas Economou / Core Security Technologies

Avis Microsoft

- **MS13-102** **Élévation de privilèges via LPC (x1) [1]**
 - **Affecte:** Windows XP / 2003
 - **Exploit:** "buffer overflow" conduisant à une élévation de privilèges locale
 - <http://seclists.org/fulldisclosure/2013/Dec/175>
 - **Crédits:** Renguang Yuan / Qihoo

- **MS13-103** **Élévation de privilèges via ASP.NET (x1) [1]**
 - **Affecte:**
 - ASP.NET SignalR 1.1.x / 2.0.x
 - <http://www.asp.net/signalr>
 - Visual Studio Team Foundation Server 2013
 - **Exploit:** XSS
 - **Crédits:** n/d

- **MS13-104 Fuite d'information via Office (x1) [3]**
 - Affecte: Office 2013
 - Exploit: fuite du token d'authentification utilisé lors de l'accès à des fichiers en ligne (e.g. Office 365)
 - <http://www.adallom.com/blog/severe-office-365-token-disclosure-vulnerability-research-and-analysis/>
 - Crédits: Noam Liran / Adallom

- **MS13-105 Failles Exchange (x4) [3]**
 - Affecte: Exchange 2007 / 2010 / 2013
 - Exploit:
 - Failles dans la librairie "Oracle Outside" exploitables depuis OWA
 - Absence de MAC conduisant à l'exécution de code dans le contexte du service OWA
 - XSS dans OWA
 - Crédits: Minded Security (audit pour Criteo)

Avis Microsoft

- **MS13-106 Contournement de l'ASLR (x1) [-]**
 - **Affecte: Office 2007 / 2010**
 - **Exploit: le composant HXDS.DLL était compilé sans ASLR**
 - **Utilisé dans des attaques ciblées**
 - **<http://blogs.technet.com/b/srd/archive/2013/12/09/ms13-106-another-aslr-bypass-is-gone.aspx>**
 - **Crédits: n/d**

■ Advisories

- **Q2755801 Faille(s) Flash**
 - V17.0: publication d'une mise à jour
- **Q2871690 Révocation de modules UEFI**
 - V1.0: publication du bulletin
- **Q2896666 Faille "0day" dans un composant graphique**
 - V2.0: publication d'un correctif
- **Q2905247 Elévation de privilèges dans ASP.NET en cas de mauvaise configuration**
 - V1.0: publication du bulletin
- **Q2915720 Faille Authenticode**
 - V1.0: publication du bulletin
 - V1.1: mise à jour des clés de base de registre
- **Q2916652 Certificat IGC/A frauduleux**
 - V2.0: sortie du correctif Q2917500

Avis Microsoft

■ Prévisions pour Janvier 2014

- 4 bulletins (seulement)

■ Failles à venir

- Faille IE11 (sans Flash)
 - <https://twitter.com/ca0nguyen/status/422884667344166912/photo/1>

■ Retour sur des failles antérieures

- MS13-052 (élévation de privilèges .NET)
 - http://www.contextis.com/research/blog/Expressing_Yourself_Analysis_Dot_Net_Elevation_Pri/
- Exemple d'utilisation d'un "0day" Microsoft "dans la nature"
 - <http://blog.trendmicro.com/trendlabs-security-intelligence/recent-windows-zero-day-targeted-embassies-used-syria-related-email/>

Avis Microsoft

■ Révisions

- **MS13-002**
 - V1.2: changement dans la logique de détection sur Windows RT
- **MS13-004**
 - V2.2: changement dans la logique de détection sur Windows RT
- **MS13-006**
 - V1.3: changement dans la logique de détection sur Windows RT
- **MS13-039**
 - V1.1: changement dans la logique de détection sur Windows RT
- **MS13-046**
 - V1.1: changement dans la logique de détection sur Windows RT
- **MS13-050**
 - V1.1: changement dans la logique de détection sur Windows RT
- **MS13-054**
 - V1.3: changement dans la logique de détection sur Windows RT
- **MS13-062**
 - V1.1: changement dans la logique de détection sur Windows RT

Avis Microsoft

- **MS13-075**
 - V1.1: précision documentaire
- **MS13-081**
 - V1.3: changement dans la logique de détection sur Windows RT
- **MS13-096**
 - V1.1: mise à jour documentaire concernant la suppression du *workaround*
 - V1.2: précision documentaire
- **MS13-098**
 - V1.1: ajout d'un problème connu
 - V1.2: aucun problème connu
- **MS13-105**
 - V1.1: ajout d'un problème connu

Infos Microsoft

- Sorties logicielles

Infos Microsoft

■ Autre

- Microsoft s'associe à OVH pour son offre Cloud
- Le menu "Démarrer" reviendra
 - <http://www.theverge.com/2013/12/9/5192742/windows-threshold-start-menu-rumor>
- Le Twitter et le blog de Microsoft piratés par SEA
 - http://www.theregister.co.uk/2014/01/13/microsoft_twitter_blog_sea_compromised/
- Des recommandations "crypto" pragmatiques ☺
 - <https://research.microsoft.com/en-us/people/mickens/thisworldofours.pdf>

Infos Réseau

■ (Principales) faille(s)

- La farandole des backdoors sur les routeurs "grand public"
 - <https://github.com/elvanderb/TCP-32764>

Infos Réseau

■ Autres infos

- Juniper ne fonctionne plus après le 31 décembre 2013 ☺
 - <http://kb.juniper.net/InfoCenter/index?page=content&id=TSB16290&actp=SUBSCRIPTION>
- 802.11ac ratifié

■ (Principales) faille(s)

- **"Local root" dans X11**
 - Un stack overflow présent ... depuis 23 ans
 - <http://lists.x.org/archives/xorg-announce/2014-January/002389.html>
- **"Use after free" dans UDP sous Linux**
 - <http://www.spinics.net/lists/netdev/msg260799.html>
- **Faille dans le support des certificats par PHP**
 - https://www.sektioneins.de/advisories/advisory-012013-php-openssl_x509_parse-memory-corruption-vulnerability.html
- **Memcached**
 - La deuxième tentative d'authentification réussit toujours ...
 - <https://code.google.com/p/memcached/issues/detail?id=316>
 - <https://github.com/memcached/memcached/commit/87c1cf0f20be20608d3becf854e9cf0910f4ad32>

Infos Unix

- **"Remote root" sur ProFTPd**
 - En vente pour \$11,000
 - <http://niebezpiecznik.pl/post/0day-na-proftpd-1-3-3g/>
- **Ca n'est pas la fin des bugs ptrace()**
 - <http://kernel.opensuse.org/cgit/kernel/commit/?id=d049f74f2dbe71354d43d393ac3a188947811348>

■ Autres infos

- **CentOS retourne chez Red Hat**
 - <http://www.redhat.com/about/news/press-archive/2014/1/red-hat-and-centos-join-forces>
- **Afficher une version de noyau aléatoire ?**
 - <https://lkml.org/lkml/2013/12/13/195>
- **Alerter les sysadmins sur les tentatives d'exploitation noyau ?**
 - <https://lkml.org/lkml/2013/12/12/358>
 - <https://lkml.org/lkml/2013/12/12/658>
- **Une fausse bonne idée ?**
 - <https://twitter.com/grsecurity/status/411530714304106496>

Infos Unix

- **OpenBSD signe ses packages**
 - <https://twitter.com/jedisct1/status/418005093666275328>
- **SteamOS (basé sur Debian, en beta)**
 - <http://linux.slashdot.org/story/13/12/14/0045211/valve-releases-debian-based-steamos-beta>
- **FireFox MarketPlace**
 - <https://marketplace.firefox.com/>

Failles

■ Principales applications

- **Oracle Quaterly Patch**
 - 144 failles (dont Java)
 - <http://www.oracle.com/technetwork/topics/security/alerts-086861.html>
- **Adobe Flash Player (+ Adobe AIR)**
 - APSB13-28
 - <http://helpx.adobe.com/security/products/flash-player/apsb13-28.html>
- **Adobe ShockWave Player**
 - APSB13-29
 - <http://helpx.adobe.com/security/products/flash-player/apsb13-29.html>
- **Un symbole "osTestBackdoorATI" dans le pilotes ATI ...**
 - <http://pastebin.com/b4x1pTWG>

Failles 2.0

- **Panne du réseau de paiement CB en Belgique**
 - L'apocalypse 2.0 grandeur nature
 - Opéré par Atos Worldline
 - <http://www.lefigaro.fr/flash-eco/2013/12/23/97002-20131223FILWWW00616-belgique-les-paiement-electroniques-en-panne.php>

- **Des distributeurs de billets piratés ... avec une clé USB**
 - <http://www.numerama.com/magazine/27925-des-distributeurs-de-billets-pilles-avec-une-cle-usb.html>

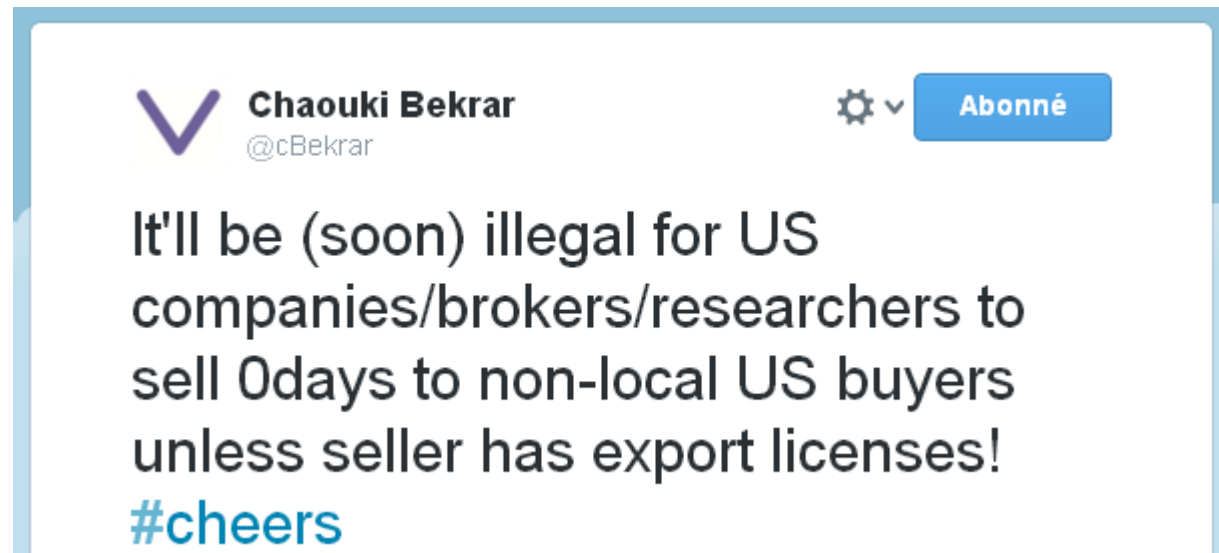
- **Extraire la photo de quelqu'un depuis une rétine**
 - <http://www.plosone.org/article/info%3Adoi%2F10.1371%2Fjournal.pone.0083325>
 - Ou un code PIN
 - <http://delivery.acm.org/10.1145/2520000/2516709/p1063-xu.pdf>

- **Pirater un contrôleur de carte microSD**
 - <http://www.bunniestudios.com/blog/?p=3554>

Failles 2.0

■ Les accords de Wassenaar en action

– <https://twitter.com/cBekrar/status/420659038222041088>



Sites piratés

■ Les sites piratés du mois (liste partielle)

- **Plusieurs banques israéliennes (3.7M clients)**
 - Le pirate demande une rançon en bitcoins
 - <http://thehackernews.com/2013/12/hacker-Israeli-Bank-botnet-malware-extortion-bitcoin.html#>
- **Target (100M CC ?)**
 - <http://www.reuters.com/article/2013/12/19/us-target-breach-idUSBRE9BH1GX20131219>
 - **Neiman Marcus**
 - <http://nakedsecurity.sophos.com/2014/01/13/payment-data-hacked-at-us-luxury-retailer-neiman-marcus/>
 - <http://krebsonsecurity.com/2014/01/hackers-steal-card-data-from-neiman-marcus/>
 - ... et d'autres
- **Le plus gros site de poker en bitcoins (42,000 utilisateurs)**
 - http://thehackernews.com/2013/12/SealsWithClubs-bitcoin-poker-hacked-password-dump_20.html

Sites piratés

- **SnapChat**

- ... utilise une clé de chiffrement "en dur"
- ... se fait voler 4.6M de comptes
 - <http://venturebeat.com/2013/12/31/snapchat-cracked-4-6-million-username-and-phone-numbers-published/>
- ... ne supprime pas réellement vos photos
 - <http://www.decipherforensics.com/index.php/blog-landing-page-2/56-snapchat>
- ... a eu la bonne réaction (ou pas)
 - <http://www.engadget.com/2014/01/07/snapchat-hires-lobbyist-podesta/>

Sites piratés

- **Washington Post**
 - 3 fois en 3 ans ...
 - http://www.washingtonpost.com/business/technology/hackers-break-into-washington-post-servers/2013/12/18/dff8c362-682c-11e3-8b5b-a77187b716a3_story.html
- **OpenSuse forums (80,000 utilisateurs)**
 - Via une faille vBulletin
- **OpenSSL**
 - Site Web mutualisé
 - https://www.openssl.org/news/secadv_hack.txt

Malwares, spam et fraudes

■ Les radars de vitesse russes en panne

- A cause d'un malware Windows XP

- http://translate.google.com/translate?langpair=ru|en&u=http%3A%2F%2Fwww.gazeta.ru%2Fauto%2F2014%2F01%2F13_a_5845877.shtml

■ Des publicités malveillantes diffusées via la régie Yahoo!

- <http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/06/everything-you-need-to-know-about-yahoos-security-breach/>

Malwares, spam et fraudes


- "McAfee Antivirus" devient "Intel Antivirus"
 - <https://twitter.com/mikko/status/420480939785867266>

www.bbc.co.uk/news/technology-25631183

The controversial founder of the security business, John McAfee, told the BBC he was overjoyed by the news.

"I am now everlastingly grateful to Intel for freeing me from this terrible association with the worst software on the planet. These are not my words, but the words of millions of irate users.

"My elation at Intel's decision is beyond words."

A photograph of John McAfee, a man with a dark beard and mustache, wearing a dark suit jacket over a light-colored shirt. He is speaking and looking slightly to the right. The background shows an outdoor event with palm trees, a building with blue accents, and other people. A "GETTY IMAGES" watermark is visible in the bottom right corner of the photo.

John McAfee says he is elated by Intel's decision to drop his name from their software

Actualité (francophone)

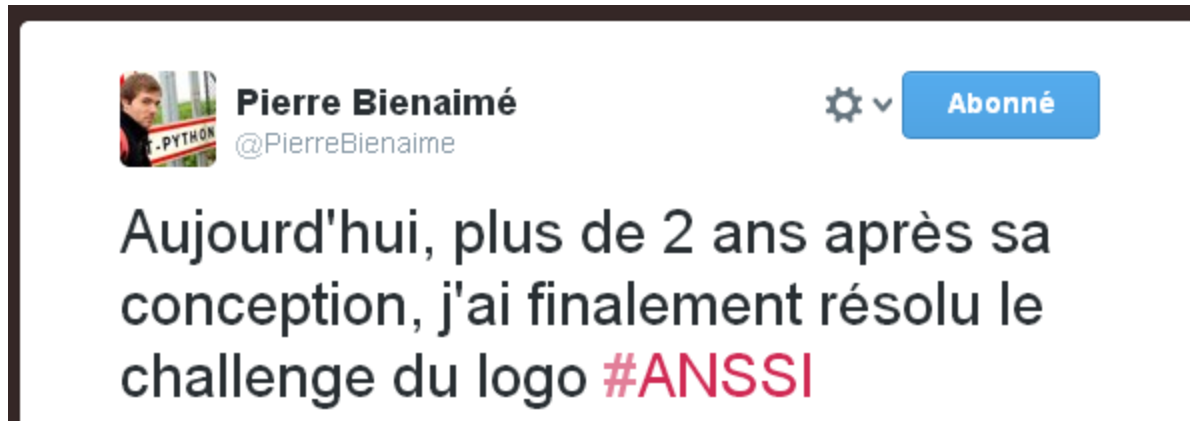
■ ANSSI

- "Aucune grande entreprise française n'a été épargnée par les hackers"
 - <http://pro.01net.com/editorial/611076/aucune-grande-entreprise-francaise-n-a-ete-epargnee-par-les-hackers/>
- Un CDI de la fonction publique pour mettre en place des procédures à l'ANSSI 😊
 - <http://emploi.silicon.fr/216978/auditeur-senior-organisation-et-fonctionnement-de-la-cybersecurite-hf/>
- Liste des formations en "cybersécurité"
 - <http://www.ssi.gouv.fr/fr/anssi/formations/les-formations-de-specialistes-en-cybersecurite-en-france.html>
- Document de sensibilisation pour les collectivités locales
 - http://www.ssi.gouv.fr/IMG/pdf/sensibilisation_collectivites_locales-ANSSI.pdf
- Note technique sur AppLocker
 - http://www.ssi.gouv.fr/IMG/pdf/NP_Applocker_NoteTech-v1.pdf

Actualité (francophone)

■ "Ca, c'est fait"

– <https://twitter.com/PierreBienaime/status/422799888640790528>



Actualité (francophone)

■ No comment

- <https://twitter.com/lauMarot/status/422397063230283776/photo/1>



The screenshot shows a web browser window with the address bar containing <https://www.defense.gouv.fr>. The page displays the RSA SecurID logo at the top. Below the logo, there is a section titled "Connexion" (Connection) with the instruction "Veuillez saisir votre identifiant." (Please enter your identifier.). A text input field is labeled "Identifiant :" and is currently empty. Below the input field, there is a button labeled "Etape suivante" (Next step).

Actualité (francophone)

■ CNIL

- Amende de 150,000€ contre Google
 - <http://www.cnil.fr/linstitution/actualite/article/article/la-formation-restreinte-de-la-cnil-prononce-une-sanction-pecuniaire-de-150000-EUR-a-lencontre/>

■ Législation

- La LPM rend-t-elle possible la publication de failles ?
 - <http://pro.clubic.com/it-business/securite-et-donnees/actualite-608568-recherche-securite-informatique-publication-vulnerabilites-legale.html>
- La LPM est-elle constitutionnelle ?
 - <http://www.donneespersonnelles.fr/qui-va-faire-sauter-la-lpm-ou-le-jeu-de-la-course-a-la-qpc>
- Le code source des logiciels de compatibilité devra être fourni à l'administration fiscale
 - <http://travauxpublics.wordpress.com/2013/12/17/lutte-contre-la-fraude-fiscale-quand-le-legislateur-sinteresse-au-code-des-logiciels-de-comptabilite/>

Actualité (francophone)

■ Les premiers certifiés PASSI par LSTI

- Sogeti, AMOSSYS

- http://www.lsti-certification.fr/images/liste_entreprise/PASSI.pdf

■ OBS rachète Atheos

- <http://www.orange.com/fr/presse/communiques/communiques-2014/Orange-Business-Services-acquiert-la-societe-Atheos-et-consolide-son-positionnement-d-acteur-majeur-de-la-cyberdefense>

■ Bernard Barbier (directeur technique de la DGSE) va chez Sogeti

- <http://www.intelligenceonline.fr/intelligence-economique/2013/12/04/dgse-bernard-barbier-passe-chez-sogeti,107997758-ART>

Actualité (francophone)

- **Les sites Web des Agences Régionales de Santé victimes d'injection SQL**
 - <http://www.zataz.com/news/23219/ars--paps--hack.html>
- **Vol d'ordinateurs chez Siemens**
 - <http://www.leparisien.fr/hauts-de-seine-92/chatillon-vol-d-ordinateurs-contenant-des-donnees-sensibles-chez-siemens-10-01-2014-3480581.php>
- **GDF-Suez vs. SAP**
 - <http://www.larevuedudigital.com/2013/12/alaune/la-dsi-de-gdf-suez-en-a-assez-des-grands-editeurs-qui-veulent-faire-cracher-la-bete/>
- **Xavier Niel balance fort**
 - <http://www.lejdd.fr/Economie/Xavier-Niel-J-ai-beaucoup-de-peine-pour-mes-concurrents-644110>

Actualité (anglo-saxonne)

■ PRISM: une actualité sans fin ...

- **Le catalogue des outils d'intrusion utilisés par la NSA ... en 2008**
 - Backdoors logicielles persistantes pour Juniper, Cisco, Huawei ...
 - BIOS malveillants
 - Backdoors matérielles
 - Cartes JTAG, I2C, ...
 - Faux ports USB
 - Faux ports Ethernet
 - Accès distant complet aux iPhones
 - Drones de collecte WiFi
 - ...
- **La NSA intercepte le matériel informatique avant sa livraison pour le modifier**

Actualité (anglo-saxonne)

■ PRISM: une actualité sans fin ...

- Quelques cibles piratées par ces techniques
 - Le gouvernement mexicain
 - RIM (BlackBerry)
 - Câble sous-marin SMW-4 (partant de Marseille et co-opéré par Orange)
 - <http://www.mediapart.fr/journal/international/291213/la-nsa-americaine-pirate-orange>
 - Total, Thales, Unicef, Médecins du Monde, Skype, ...
- La NSA finance le développement d'un ordinateur quantique
 - Quel est l'état d'avancement ?
- La NSA ré-utilise ...
 - ... les crashes Windows (watson.microsoft.com)
 - ... le tracking des annonceurs
 - <http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking/>

Actualité (anglo-saxonne)

■ PRISM: une actualité sans fin ...

- **RSA s'est vendu \$10m à la NSA**
 - <http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220>
 - ... et le paie cher aujourd'hui
 - <http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/07/at-least-six-security-experts-boycott-prominent-security-conference-over-nsa-ties/>
- **Tout cela est-il bien constitutionnel ?**
 - <http://www.nytimes.com/2013/12/17/opinion/a-powerful-rebuke-of-mass-surveillance.html>
- **"Clean Pipe": le réseau "NSA free" de Deutsche Telekom (2016)**
 - <http://www.silicon.fr/clean-pipe-bouclier-numerique-deutsche-telekom-finalise-2016-91976.html>
- **Idem pour la Suisse (2020)**
 - <http://www.rts.ch/info/suisse/5522540-la-suisse-planche-sur-un-reseau-securise-de-communications-pour-2020.html>

Actualité (anglo-saxonne)

■ PRISM: une actualité sans fin ...

- **Le groupe de travail "crypto" à l'IETF est dirigé par un employé de la NSA**
 - <http://www.zdnet.fr/actualites/la-nsa-garde-les-standards-de-chiffrement-a-l-oeil-39796876.htm>
- **Idem pour le TCG (groupe de travail sur les TPM)**
 - <http://pro.01net.com/editorial/611204/trusted-platform-module-pour-le-meilleur-ou-pour-le-pire/>
- **La NSA avait prévu le scénario "Snowden" en ... 1991**
 - <http://www.latribune.fr/technos-medias/internet/20140108trib000808439/snowden-la-nsa-prevoyait-une-telle-affaire-il-y-a-23-ans.html>
- **Snowden viendra témoigner devant le parlement européen**
 - <http://www.euronews.com/2014/01/09/snowden-to-testify-to-european-parliament-s-civil-liberties-committee/>

Actualité (anglo-saxonne)

■ PRISM: une actualité sans fin ...

- La NSA partage tout avec Israël

- <http://i-hls.com/2013/12/israel-had-access-to-raw-nsa-data/>

- LOL

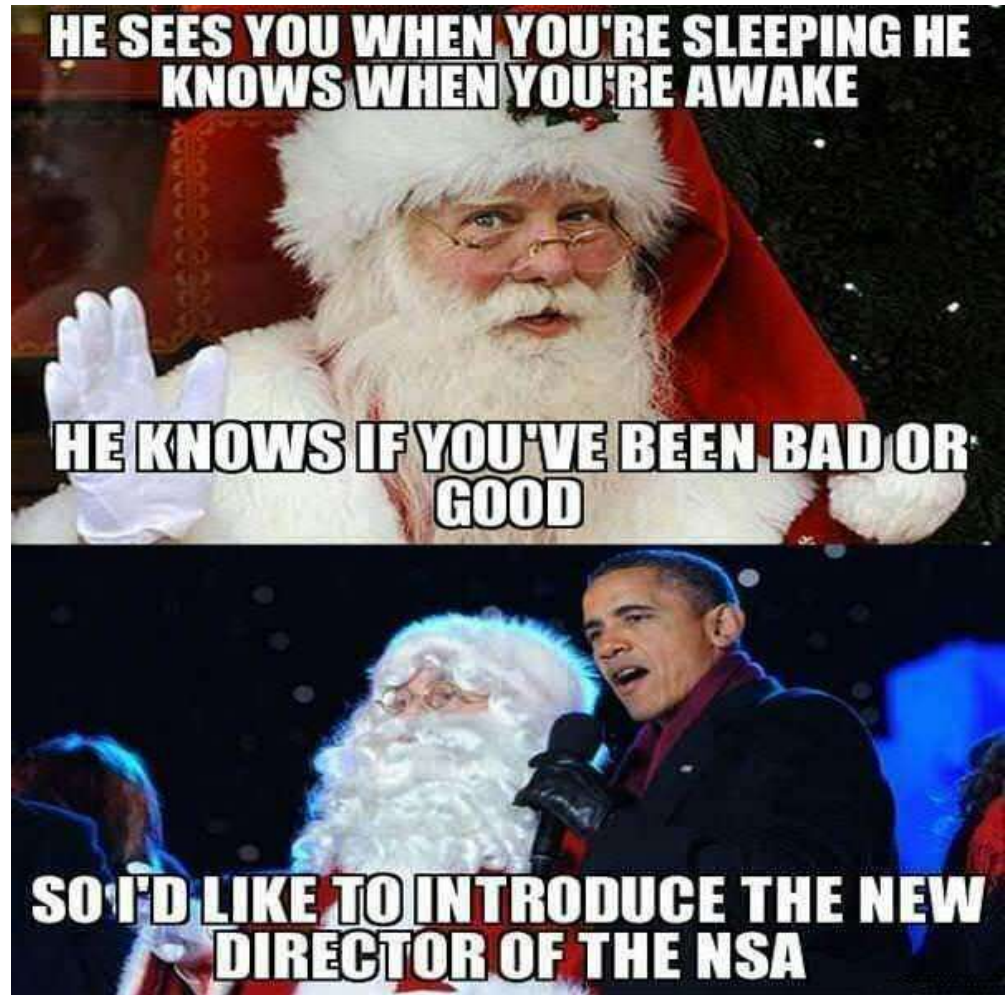
- <http://ternus.github.io/nsaproductgenerator/>

- Références

- <http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html>
- <http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969-3.html>
- <http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20131229-der-spiegel>
- <http://leaksource.wordpress.com/2013/12/30/nsas-ant-division-catalog-of-exploits-for-nearly-every-major-software-hardware-firmware/>
- http://www.lemonde.fr/technologies/article/2013/12/20/medecins-du-monde-total-unicef-la-surveillance-tous-azimuts-de-la-nsa_4338321_651865.html

Actualité (anglo-saxonne)

- PRISM: une actualité sans fin ...



Actualité (anglo-saxonne)

■ FireEye rachète Mandiant

- http://lexpansion.lexpress.fr/high-tech/fireeye-acquiert-mandiant-pour-environ-1-milliard-de-dollars_422423.html

■ 20 ans de prison pour une tentative de hacking ?

- <http://thehackernews.com/2014/01/hacker-Personal-Data-Privacy-Security-Act.html>

■ Alan Turing réhabilité par la reine d'Angleterre

- http://www.lemonde.fr/europe/article/2013/12/24/royaume-uni-grace-posthume-pour-alan-turing-condamne-pour-homosexualite_4339295_3214.html

Actualité (européenne)

■ ENISA

- Rapport sur les menaces
 - http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats/at_download/fullReport

■ Parlement européen

- Rapport sur PRISM
- La DCRI et la DGSE ont décliné l'invitation 😊
 - <http://statewatch.org/news/2014/jan/ep-draft-nsa-surveillance-report.pdf>

Actualité (Google)

- **Apple + Microsoft + ... + brevets Nortel = Rockstar**
 - Un consortium dédié au "patent troll"
 - ... qui s'en prend à Google
 - <http://www.linformaticien.com/actualites/id/31510/google-passe-a-l-offensive-pour-defendre-android-face-a-rockstar.aspx>
- **La gestion des permissions par application supprimée dans Android 4.4**
 - C'était un "glitch" de développement ☺
 - <https://www.eff.org/deeplinks/2013/12/google-removes-vital-privacy-features-android-shortly-after-adding-them>
- **L'IGC/A ne pourra plus signer que du ".fr" (et DOM-TOM)**
 - Dans Chrome
- **Le stockage des cookies désormais chiffré dans Chrome**
 - <https://codereview.chromium.org/24734007>
- **Google attire les stars ☺**
 - <http://www.begeek.fr/un-developpeur-star-de-microsoft-part-chez-google-113982>

Actualité (Apple)

- Jailbreak "evasi0n" pour iOS 7
 - ... et installation d'un Market chinois: "Taig"
 - <http://evasi0n.com/l.html>

Actualité (crypto)

- **FreeBSD ne fait plus confiance aux générateurs d'aléa matériels**
 - Trop faciles à backdoorer
 - <http://arstechnica.com/security/2013/12/we-cannot-trust-intel-and-vias-chip-based-crypto-freebsd-developers-say/>
 - Pourtant RDRAND est parfois utilisé comme seule source d'entropie par OpenSSL 1.0
 - <http://seclists.org/fulldisclosure/2013/Dec/99>
- **Récupérer une clé RSA-4096 ... en écoutant le micro**
 - Adi Shamir et al.
 - <http://www.tau.ac.il/~tromer/papers/acoustic-20131218.pdf>
- **Tester votre client SSL**
 - <https://www.howssmyssl.com/>
- **Difficile de concevoir une application "sécurisée" ...**
 - <http://telegram.org/>
 - <http://translate.google.com/translate?hl=en&sl=ru&u=http://habrahabr.ru/post/206900/>

Actualité

■ Conférences passées

- **CCC**

- <https://events.ccc.de/congress/2013/Fahrplan/>
- https://www.youtube.com/playlist?list=PLOcrXzpA0W82rsJJKrmeBIY3_MS0uQv3h

- **PRISM**

- <http://youbroketheinternet.org/>

- **CHIASMUS**

- <http://janschejbal.wordpress.com/2013/09/11/advisory-unsichere-verschluesselung-bei-gstool/>

- **SCADA StrangeLove**

- <http://scadastrangelove.blogspot.co.at/2014/01/30c3-releases-all-in-one.html#more>

- ...

- **CES**

- **Un PC ... de la taille d'une carte SD**

- http://www.theregister.co.uk/2014/01/07/intel_demos_pconsd_tiny_computer_for_internet_of_things_and_wearables/

Actualité

■ CCC

- <https://twitter.com/juliocesarfort/status/417245924986195969/photo/1>



Actualité

■ Conférences à venir

- **CLUSIF / Panorama de la cybercriminalité**
 - 16 janvier
- **FIC**
 - 21-22 janvier
- **AFCDP**
 - 27 janvier
 - <http://www.globalsecuritymag.fr/Universite-AFCDP-des-CIL-du-27,20131020,40452.html>
- **Microsoft TechDays**
 - 11-13 février
 - <http://www.microsoft.com/france/mstechdays/>
- **Insomnihack**
 - 21 mars
- **SSTIC**
 - **Soumissions libres !**
 - https://www.sstic.org/2014/news/CFP_SSTIC_2014/
- **PSES**
 - 26 au 29 juin
- **NoSuchCon**
 - Novembre

Actualité

■ Sorties logicielles

- IDA 6.5
- Mimikatz implémente l'attaque "Golden Ticket"
 - <https://twitter.com/gentilkiwi/status/415147415474167808>
- Cuckoo Sandbox 1.0
 - <http://www.cuckoosandbox.org/2014-01-09-cuckoo-sandbox-10.html>
- Qubes R2 Beta3
 - <http://theinvisiblethings.blogspot.fr/2013/12/qubes-r2-beta-3-has-been-released.html>
- OpenSSL 1.0.0 L

Actualité

■ IOCCC 2013

- Un émulateur PC XT en 4 Ko !?
 - <http://ioccc.org/2013/whowon.html>

■ 11 février, c'est le Safer Internet Day

- <http://www.saferinternet.org/safer-internet-day>

■ Intel va commercialiser des smartphones "dual boot"

- WinDroid: Android + Windows
 - <http://venturebeat.com/2014/01/06/windroid-confirmed-intel-ceo-offers-dual-android-windows-systems/>

■ Marissa Meyer s'excuse pour un gros bug de Yahoo! Mail

- <http://yahoo.tumblr.com/post/69929616860/an-update-on-yahoo-mail>

■ VMS n'est plus supporté par cPython

- <http://hg.python.org/cpython/rev/568391b3eda9>

Divers

■ Faille Jira

- Une typo dans "Lorem Ipsum"
 - <https://jira.atlassian.com/browse/CONF-32190>

Divers

■ CAPTCHA #win

- <http://i.imgur.com/DpKTbXw.png>

Security challenge

Enter the following:

domestic
spying

Your Answer

SOLVE media

Questions / réponses

- **Questions / réponses**

- **Prochaine réunion**
 - **Mardi 11 février 2014**

- **Prochain AfterWork**
 - **Mardi 28 février 2014**

- **Prochaine JSSI**
 - **Lundi 17 mars 2014**
 - **Profitez du combiné avec les GS-Days le mardi 18 mars**

- **N'hésitez pas à proposer des sujets et/ou des salles**