OSSIR
Groupe Paris

Réunion du 12 février 2013

Revue des dernières vulnérabilités

Nicolas RUFF
EADS-IW
nicolas.ruff (à) eads.net

Avis Microsoft

- **Janvier 2013**

  - **MS13-001 Faille dans le spooler d'impression (x1) [1]**
    - **Affecte: Windows 7 / 2008R2**
    - **Exploit: exécution de code à distance**
    - **Crédit: n/d**

  - **MS13-002 Failles MS-XML (x2) [1]**
    - **Affecte: MS-XML (toutes versions supportées)**
    - **Exploit: exécution de code lors du traitement d'un document XML**
      - **Corruption mémoire via "integer truncation"**
      - **Corruption mémoire via XSLT**
    - **Crédit: Nicolas Grégoire / Agarri**

Avis Microsoft

- **MS13-003 XSS dans SCOM (x2) [1]**
  - **Affecte: SCOM 2007**
  - **Exploit: XSS**
  - **Crédit: Andy Yang / BAE Systems Detica**

- **MS13-004 Failles dans .NET (x4) [1]**
  - **Affecte: .NET Framework (toutes versions supportées, sauf 3.5SP1)**
  - **Exploit: évasion de la sandbox**
    - **Lecture mémoire arbitraire avec System.Drawing**
    - **"Buffer overflow" dans WinForms**
    - **"Buffer overflow" dans System.DirectoryServices.Protocols**
    - **"Double construction" (?)**
  - **Crédit:**
    - **Jon Erickson / iSIGHT Partners**
    - **Vitaliy Toropov + ZDI (x2)**
    - **James Forshaw / Context IS**

Avis Microsoft

- **MS13-005 Faille dans WIN32K.SYS (x1) [1]**
  - **Affecte: Windows (toutes versions supportées, sauf XP et 2003)**
  - **Exploit: élévation de privilèges**
    - **Envoi de messages en broadcast à un processus de niveau d'intégrité plus élevé**
    - **http://blog.cmpxchg8b.com/2013/02/a-few-years-ago-while-working-on.html**
    - **https://github.com/0vercl0k/stuffz/blob/master/ms13-005-funz-poc.cpp**
  - **Crédit: n/d**

- **MS13-006 Faille SSL/TLS (x1) [1]**
  - **Affecte: Windows (toutes versions supportées, sauf XP et 2003)**
  - **Exploit: contournement de la sécurité par injection de trafic (?)**
  - **Crédit: Kenichiro Katayama**

Avis Microsoft

- **MS13-007 Faille dans le protocole "Open Data" (x1) [1]**
  - **Affecte: .NET Framework 3.5 et 4.0**
  - **Exploit: déni de service via la fonction Replace**
  - **Crédit: n/d**

■ Correctif "hors bande"

- **MS13-008 Faille dans IE (x1) [1]**
  - **Affecte: IE 6 / 7 / 8**
  - **Exploit: "use after free"**
  - **Crédit: Exodus Intelligence**

Avis Microsoft

- **Advisories**
  - **Q973811 "Extended Protection for Authentication"**
    - **V1.14: activation de NTLMv2 uniquement via un "fix it"**
  - **Q2755801 Faille Flash Player dans IE 10**
    - **V6.0: nouvelle faille**
    - **V7.0: nouvelle faille**
  - **Q2798897 Certificat frauduleux**
    - **V1.1: correction de la date de révocation**
  - **Q2794220 Faille IE exploitée dans la nature**
    - **V1.0: publication du bulletin**
    - **V2.0: sortie du correctif "hors bande" MS13-008**

Avis Microsoft

- **Prévisions pour Février 2013**
  - **11 bulletins, 57 failles**
  - **5 bulletins critiques**
  - **Windows, IE (x2), Exchange (x1), FAST Search Server (x1)**

- **Failles à venir**
  - **Un 0day Office en vente pour $5000**
    - **http://1337day.com/exploits/20229**

- **Retour sur des failles antérieures**
  - **MS12-081**
    - **http://www.ioactive.com/pdfs/Windows_Kernel_Library_Vulnerability.pdf**

Avis Microsoft

- **Révisions**
  - **MS13-002**
    - **V1.1: correction documentaire (liens de téléchargement)**
  - **MS12-004**
    - **V1.1: ajout d'un problème connu**
    - **V2.0: re-publication du correctif pour Windows 7 / 2008R2**
  - **MS13-005**
    - **V1.1: correction documentaire**

Infos Microsoft

- **Sorties logicielles**
  - **System Center 2012 SP1**
  - **Rappel: Microsoft TMG est "deprecated" depuis septembre 2012**

Infos Microsoft

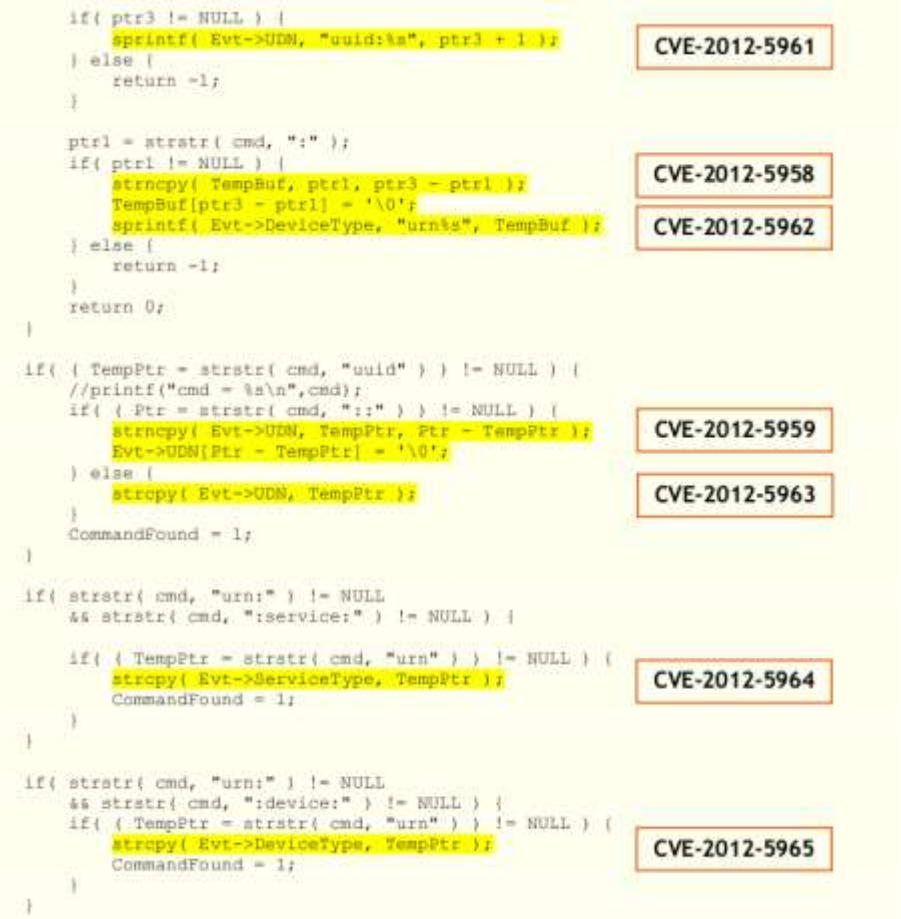
- **Autre**
  - **Jailbreak Windows RT**
    - **WinDbg + CSRSS**
      - **http://surfsec.wordpress.com/2013/01/06/circumventing-windows-rts-code-integrity-mechanism/**
  - **A méditer**
    - **http://www.businessinsider.com/steve-ballmers-nightmare-is-coming-true-2012-11**
  - **Cambriolage chez Microsoft**
    - **Seuls les iPads ont été volés**
      - **http://lebruitduweb.fr/bruits/insolite/des-ipad-voles-chez-microsoft-1346**

Infos Réseau

- **(Principales) faille(s)**
  - **Faille exploitable à distance dans libupnp**
    - **https://community.rapid7.com/docs/DOC-2150**
    - **http://www.kb.cert.org/vuls/id/922681**
  - **Affecte des millions d'équipements de vendeurs différents**
    - **http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130129-upnp**
  - **Voir aussi**
    - **http://www.defensecode.com/public/DefenseCode_Broadcom_Security_Advisory.pdf**
    - **http://www.defensecode.com/article/upcoming_cisco_linksys_remote_preauth_root_exploit-33**

Infos Réseau

- Source
  - https://twitter.com/meikk/status/296611946755653632/photo/1



Infos Réseau

- Faille(s) Ruby on Rails
  - Faille YAML
    - http://rubysource.com/anatomy-of-an-exploit-an-in-depth-look-at-the-rails-yaml-vulnerability/
    - https://community.rapid7.com/community/metasploit/blog/2013/01/09/serialization-mischief-in-ruby-land-cve-2013-0156
    - http://www.insinuator.net/2013/01/rails-yaml/
  - Affecte Mac OS X Server, entre autres
    - http://support.apple.com/kb/HT5644

- Cisco Prime LAN Management
  - "rsh root@" … sans mot de passe
    - https://community.rapid7.com/community/metasploit/blog/2013/01/16/hacking-like-its-1985-rooting-the-cisco-prime-lan-management-solution

- XXE dans F5
    - http://seclists.org/fulldisclosure/2013/Jan/192

- Backdoor(s) dans les produits Barracuda
    - http://archives.neohapsis.com/archives/fulldisclosure/2013-01/0221.html
  - Première publication: 2006 …
    - http://blog.nibblesec.org/2013/01/how-to-patch-your-barracuda-virtual.html

Infos Réseau

- Faille dans les caméras TrendNet
  - Pourtant connue depuis plus d'un an …
    - http://www.20minutes.fr/high-tech/1086597-images-centaines-cameras-privees-visibles-direct-net
- Faille(s) dans Apache CXF
  - Framework de Web Services
    - http://cxf.apache.org/cve-2012-5633.html
    - http://cxf.apache.org/cve-2013-0239.html
- Faille(s) dans Cisco WLC
  - wIPS, SIP, HTTP (exécution de code via l'entête "User-Agent"), backdoor SNMP
    - http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130123-wlc
- Base de données de failles
  - Classées par routeur
    - http://routerpwn.com/
- Le retour du "RA Flood"
  - Microsoft Surface est affectée
    - http://samsclass.info/ipv6/proj/RA_flood2.htm

Infos Réseau

- Autres infos

  - Retour du filtrage anti-pub chez Free
    - Désactivé par défaut
      - http://obsession.nouvelobs.com/les-forfaits-free-mobile/20130118.OBS5863/le-blocage-des-pubs-de-retour-chez-free.html
  - IPv6 ou "carrier grade NAT" ?
      - http://tech.slashdot.org/story/13/01/16/1417244/uk-isp-plusnet-testing-carrier-grade-nat-instead-of-ipv6
      - http://tech.slashdot.org/story/13/01/23/1537253/uk-isps-respond-to-the-dangers-of-using-carrier-grade-nat-instead-of-ipv6
  - Cisco revend Linksys à Belkin
    - http://www.zdnet.com/belkin-buying-ciscos-home-networking-business-linksys-7000010297/

Infos Unix

- **(Principales) faille(s)**
  - **Déni de service sur le serveur FTP de FreeBSD 9.1**
    - **STAT + globbing**
      - **http://cxsecurity.com/issue/WLB-2013020003**
  - **Faille côté client dans CURL**
    - **http://curl.haxx.se/docs/adv_20130206.html**

Infos Unix

- **Autres infos**

  - **GNU/Hurd va avoir le support USB, SATA et 64 bits**
    - **Bientôt ☺**
      - **http://www.phoronix.com/scan.php?page=news_item&px=MTI5ODM**

  - **Alan Cox "se recentre sur sa famille"**
      - **http://linux.slashdot.org/story/13/01/24/1334234/alan-cox-exits-intel-linux-development**

Failles

- **Principales applications**

  - **Chrome < 24**
  - **Firefox < 18.0.2**
    - **https://www.mozilla.org/en-US/firefox/18.0.2/releasenotes/**
  - **Thunderbird < 17.0.2**

  - **Flash**
    - **http://www.adobe.com/support/security/bulletins/apsb13-01.html**
    - **http://www.adobe.com/support/security/bulletins/apsb13-04.html**
    - **http://www.adobe.com/support/security/bulletins/apsb13-05.html**
    - **Utilisé dans des attaques ciblées**
      - **http://labs.alienvault.com/labs/index.php/2013/adobe-patches-two-vulnerabilities-being-exploited-in-the-wild/**
    - **Technique d'exploitation inconnue**
      - **https://sites.google.com/site/zerodayresearch/smashing_the_heap_with_vector_Li.pdf?attredirects=0**
  - **ShockWave**
    - **http://www.adobe.com/support/security/bulletins/apsb13-06.html**
  - **Adobe Reader < 10.1.5, 11.0.1**
    - **http://www.adobe.com/support/security/bulletins/apsb13-02.html**
  - **ColdFusion (contournement de l'authentification)**
    - **http://www.adobe.com/support/security/bulletins/apsb13-03.html**

Failles

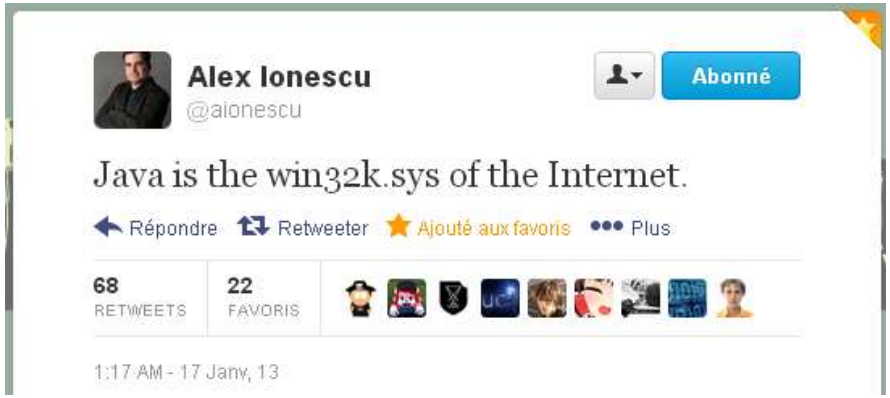
- Java < 1.6.38, < 1.7.11
  - Java 1.7 présente des failles supplémentaires
    - http://www.certa.ssi.gouv.fr/site/CERTA-2013-ALE-001/index.html
  - Faille largement exploitée dans la nature
    - https://partners.immunityinc.com/idocs/Java%20MBeanInstantiator.findClass%200day%20Analysis.pdf
  - Le plugin Java a rapidement été blacklisté par les principaux navigateurs
    - http://www.macbidouille.com/news/2013/01/31/apple-bloque-la-derniere-mise-a-jour-de-java
  - Corrigé en urgence … pas forcément de manière fiable
    - http://uk.reuters.com/article/2013/01/14/uk-java-oracle-security-idUKBRE90C0JA20130114
  - Note: un nouveau paramétrage de sécurité est disponible
    - http://blogs.computerworld.com/cybercrime-and-hacking/21664/understanding-new-security-java-7-update-11

- Java < 1.6.39, < 1.7.13
  - Cette fois c'est le bon ?
    - http://www.security-explorations.com/en/SE-2012-01-details.html
    - http://tyranidslair.blogspot.co.uk/2013/02/fun-with-java-serialization-and.html

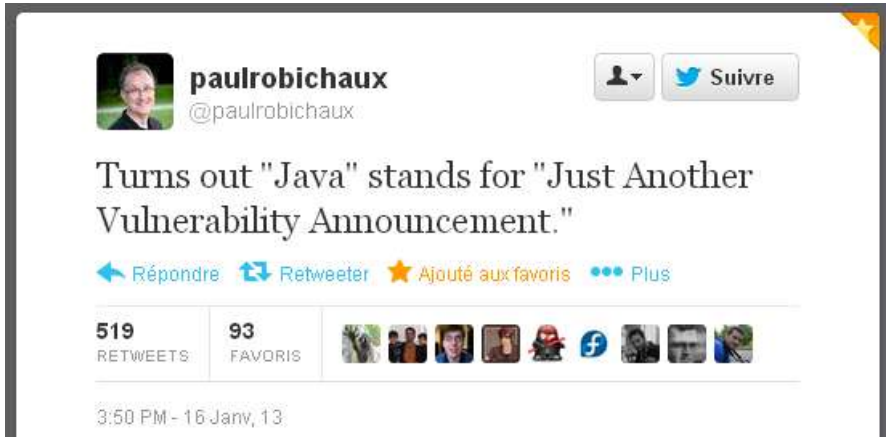
- Oracle Quaterly Patch, janvier 2013
  - 86 failles corrigées
    - http://www.oracle.com/technetwork/topics/security/cpujan2013-1515902.html

Failles

- Source
  - https://twitter.com/aionescu/status/291700845630877698

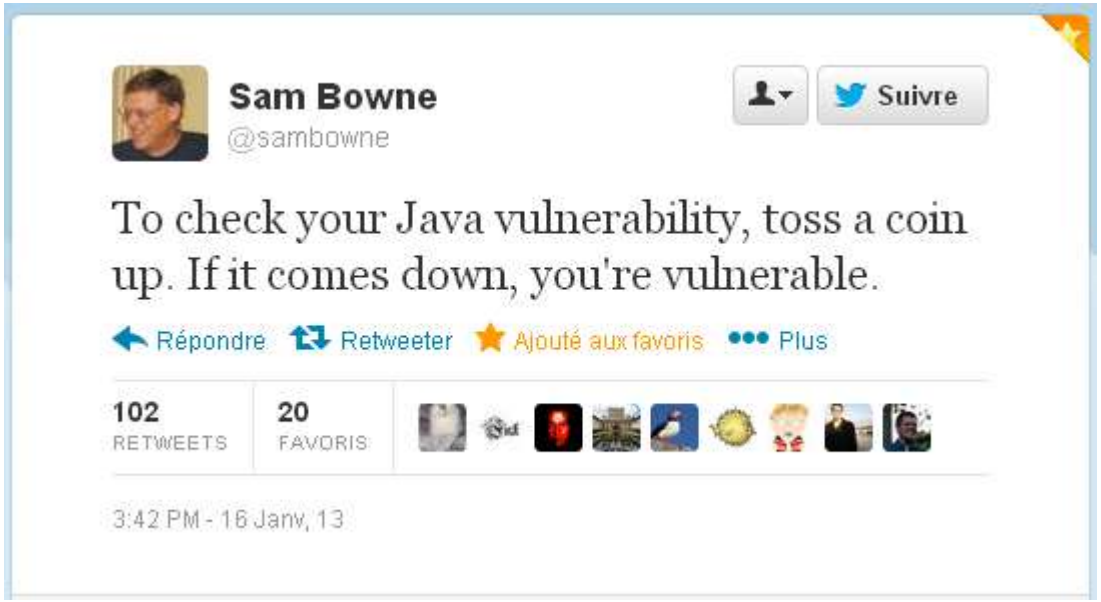


  - https://twitter.com/paulrobichaux/status/291558057174003713



Failles

- **Source**
  - **https://twitter.com/sambowne/status/291556097117011968**



Failles

- VMWare
  - Elévation de privilèges dans VMCI.SYS
    - http://www.vmware.com/security/advisories/VMSA-2013-0002.html
- Qemu
  - "Stack overflow" dans le driver e1000
    - CVE-2012-6075

Failles 2.0

- Nouvelles failles dans HP JetDirect
  - https://viaforensics.com/security/exploiting-printers-via-jetdirect-vulns.html
- Idem dans les imprimantes Brother
  - http://seclists.org/fulldisclosure/2013/Feb/40
- CVE-YYYY-NNNN ne suffit plus
  - Il y a plus de 9999 failles découvertes par an !
    - http://seclists.org/fulldisclosure/2013/Jan/217
- Faille UEFI dans les BIOS Samsung
  - … permettant à n'importe quel programme de "briquer" l'ordinateur
    - http://hardware.slashdot.org/story/13/02/09/2146207/samsung-laptop-bug-is-not-linux-specific
- Comment saisir un disque chiffrant ?
  - Il suffit de débrancher le câble de données sans débrancher l'alimentation
    - https://www1.cs.fau.de/sed
- Une nouvelle base de données de failles
  - https://db.risk.io/

Failles 2.0

- Des clés privées sur GitHub
  - http://nakedsecurity.sophos.com/2013/01/25/do-programmers-understand-private/
  - … mais pas seulement
    - Recherche Google: "github.com inurl:.bash_history"
    - Recherche GitHub: "path:.ssh/id_rsa"
- Facebook Graph Search
  - … fait peur
    - http://actualfacebookgraphsearches.tumblr.com/
- Le saviez-vous ?
  - http://x.co/ vole les authentifiants NTLM
    - https://thegentlemanhackersclub.com/godaddy-leaking-ntlm/
- Quand un paquet SIP fait planter le hardware d'une carte réseau …
  - http://blog.krisk.org/2013/02/packets-of-death.html

Sites piratés

- **Les sites piratés du mois (liste partielle)**
  - **"Wall Street Journal", "New York Times", etc. (depuis 4 mois)**
    - **"Over the course of three months, attackers installed 45 pieces of custom malware. The Times - which uses antivirus products made by Symantec - found only one instance in which Symantec identified an attacker's software as malicious and quarantined it, according to Mandiant. A Symantec spokesman said that, as a matter of policy, the company does not comment on its customers."**
      - **http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html**
      - **http://online.wsj.com/article/SB10001424127887323926104578276202952260718.html**
  - **4000 banquiers "doxés"**
    - **#OpLastResort**
      - **http://www.zdnet.com/anonymous-posts-over-4000-u-s-bank-executive-credentials-7000010740/**
  - **"Brazilian Cyber Army" vs. "gouv.fr"**
    - **http://pastebin.com/raw.php?i=PwWxJGaf**
    - **http://pastebin.com/raw.php?i=U4HLH7yk**
  - **Quelques écoles françaises**
    - **http://pastebin.com/w4m4L1Wu**

Sites piratés

- Le "Department of Energy"
  - http://nakedsecurity.sophos.com/2013/02/04/epartment-of-energy-hacked-employees-personal-information-stolen/
- "Directory Traversal" sur un site du DHS
  - http://nakedsecurity.sophos.com/2013/01/07/dhs-website-falls-victim-to-hacktivist-intrusion/
- Injection(s) SQL sur eBay
  - http://www.garage4hackers.com/blogs/78/sql-injection-vulnerability-ebay-677/
- XSS trivial sur Amazon
  - http://www.h-online.com/security/news/item/Critical-security-vulnerability-at-Amazon-fixed-1787328.html
- 250,000 comptes Twitter piratés
  - Par une méthode qui reste inconnue
    - http://blog.twitter.com/2013/02/keeping-our-users-secure.html
- Le PC de la famille Bush
  - http://www.theregister.co.uk/2013/02/08/bush_family_email_hack/

Sites piratés

- wiki.wireshark.org
  - http://www.wireshark.org/news/20130109.html
- La chambre de commerce allemande
  - http://www.cyberwarnews.info/2013/01/04/huge-leak-of-intel-from-german-chamber-of-commerce-ahk-de/
- L'éditeur d'antivirus Bit9
  - Certificat utilisé pour signe du malware (!)
    - http://it.slashdot.org/story/13/02/08/2237201/bit9-hacked-stolen-certs-used-to-sign-malware
- Drake International (recrutement)
  - Vol de données + extorsion
    - http://www.cabinetbrechard.com/une-societe-de-recrutement-victime-de-cyber-extorsion/
- La société Britam (mercenaires)
  - http://cryptome.org/2013/01/britam-backup.htm
  - http://www.cyberwarnews.info/reports/a-look-into-the-britam-defence-data-leak-files/?show=slide

Malwares, spam et fraudes

- "Red October": la preuve que les Russes sont plus forts que les Chinois ☺
  - Backdoor persistante dans Office/Adobe Reader depuis 5 ans
  - Même les documents ACID sont ciblés ☺
    - http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_Operation_Red_October_an_Advanced_Cyber_Espionage_Campaign_Targeting_Diplomatic_and_Government_Institutions_Worldwide
    - http://arstechnica.com/security/2013/01/red-october-computer-espionage-network-may-have-stolen-terabytes-of-data/
    - http://www.wired.com/threatlevel/2013/01/red-october-spy-campaign/
    - http://code.google.com/p/malware-lu/wiki/en_malware_redoctober

- Carte des pays victimes de cyber-espionnage
  - Source: Kaspersky
    - http://www.securelist.com/en/images/pictures/klblog/208194085.png

Malwares, spam et fraudes

- Symantec + Microsoft démantèlent le botnet Bamital
  - http://blogs.technet.com/b/microsoft_blog/archive/2013/02/06/microsoft-and-symantec-take-down-bamital-botnet-that-hijacks-online-searches.aspx
- Le botnet Virut démantelé
  - http://krebsonsecurity.com/2013/01/polish-takedown-targets-virut-botnet/
- Des criminels montent une société en bonne et due forme
  - … pour acheter des certificats frauduleux
    - http://www.h-online.com/security/news/item/Front-company-used-to-sign-malware-1799101.html
- Les pirates des bornes de commande Subway condamnés
  - 21 mois de prison
    - http://www.wired.com/threatlevel/2013/01/subway-hacking-scam/
- La version de WinRar diffuse par 01net/ZDNet/Clubic/…
  - … infectée par un virus
    - http://www.lesnumeriques.com/logiciel-bureautique/telecharger-depuis-01net-nuit-gravement-a-sante-pc-n26763.html

Malwares, spam et fraudes

- Piratage des plafonds de paiement
  - 11 M$ retirés en 1 week-end avec des cartes volées
    - http://krebsonsecurity.com/2013/02/crooks-net-millions-in-coordinated-atm-heists/
- Nouvelle monnaie virtuelle: Amazon Coins
    - http://phx.corporate-ir.net/phoenix.zhtml?c=97664&p=irol-newsArticle&ID=1781495&highlight=
- 1M de téléphones Android dans un botnet
  - En Chine
    - http://www.theregister.co.uk/2013/01/15/android_malware_botnet_china/
- Un générateur de malwares pour Android
    - http://www.ninjasecurity.org/2013/01/android-malware-engine_5987.html

Actualité (francophone)

- Publications de l'ANSSI
  - Guide d'hygiène informatique, version finale (1.1)
    - http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/l-anssi-publie-la-version-finalisee-du-guide-d-hygiene-informatique.html
  - Qu'est-ce qu'un expert en sécurité ?
    - http://www.ssi.gouv.fr/fr/anssi/publications/autres-publications-233/l-anssi-publie-un-referentiel-metier-de-l-architecte-referent-en-securite-des.html

- L'ANSSI recrute un reverser analyste en vulnérabilités et codes malveillants
    - http://www.ssi.gouv.fr/fr/anssi/emploi/cossi/division-techniques-operationnelles-210/bureau-failles-et-reponse-aux-incidents-214/ingenieur-analyste-en-vulnerabilites-et-codes-malveillants.html

- "Guide méthodologique: le format PDF"
    - http://www.tge-adonis.fr/sites/default/files/ressourcesdoc/guide_format_fichiers_pdf.pdf

- Rapport final sur la fiscalité du numérique
    - http://www.redressement-productif.gouv.fr/files/rapport-fiscalite-du-numerique_2013.pdf

Actualité (francophone)

- Publications de la CNIL
  - "Compteurs intelligents"
    - http://www.cnil.fr/nc/la-cnil/actualite/article/article/compteurs-communicants-premieres-recommandations-de-la-cnil/
  - Hervé Machi nommé directeur juridique
    - http://www.cnil.fr/la-cnil/actualite/article/article/herve-machi-est-nomme-directeur-des-affaires-juridiques-internationales-et-de-lexpertise/
- L'article 323-3 devient une QPC
    - http://www.courdecassation.fr/jurisprudence_2/questions_prioritaires_constitutionnalite_3396/constitutionnalite_soumises_3643/3_code_25157.html
- La carte d'identité électronique s'éloigne
    - http://www.pcinpact.com/news/76488-valls-lancement-carte-d-identite-electronique-nest-pas-souhaitable.htm
- ISO 27031 devient une norme AFNOR
    - http://www.afnor.org/profils/activite/tic/securite-informatique-mettez-en-place-un-plan-de-continuite-d-activite-de-vos-tic-avec-la-norme-nf-iso-cei-27031

Actualité (francophone)

- Conseil National du Numérique
  - Tariq Krim (Jolicloud), Tristan Nitot (Mozilla Europe), …
    - http://obsession.nouvelobs.com/high-tech/20130117.OBS5805/exclusif-le-nouveau-conseil-national-du-numerique-devoile.html
- Des ministres partout
  - Dans les centres de lutte contre la cybercriminalité
    - http://www.itespresso.fr/le-gouvernement-tour-brigades-anti-cybercriminalite-60755.html
- La France intègre le Centre d'Excellence en CyberDéfense de l'OTAN en 2013
    - http://www.defense.gouv.fr/actualites/articles/la-france-integrera-le-ccdcoe-en-2013
- Ouvrir la porte d'une banque avec un ordinateur ?
    - http://www.lepoint.fr/technologie/avec-mon-ordinateur-j-ai-ouvert-et-ferme-la-porte-d-une-banque-08-02-2013-1625195_58.php

Actualité (anglo-saxonne)

- **Aaron Swartz se suicide**
  - **... et provoque une onde de choc aux USA**
    - **http://tech.mit.edu/V132/N61/swartz.html**
- **Huawei et ZTE**
  - **Rapport final**
    - **http://www.scribd.com/doc/109385466/Huawei-ZTE-Investigative-Report-FINAL**
- **Une usine arrêté pendant 3 semaines**
  - **A cause d'une clé USB**
    - **http://in.reuters.com/article/2013/01/16/cyber-security-powerplants-virus-idINDEE90F0H720130116**
- **Un étudiant pirate son université**
  - **… et se fait virer**
    - **http://news.nationalpost.com/2013/01/20/youth-expelled-from-montreal-college-after-finding-sloppy-coding-that-compromised-security-of-250000-students-personal-data/**
- **Une pétition pour la légalisation du DDoS**
  - **Expirée sans succès**
    - **https://petitions.whitehouse.gov/petition/make-distributed-denial-service-ddos-legal-form-protesting/X3drjwZY**

Actualité (européenne)

- ENISA
  - Publication: "Consumerization Of IT" (COIT)
    - http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/COIT_Mitigation_Strategies_Final_Report
  - Publication: "Threat Landscape"
    - https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape
  - L'ENISA recrute
    - http://www.enisa.europa.eu/recruitment/vacancies/expert-in-network-and-information-security-3
  - L'ENISA pourra-t-elle espionner comme la NSA ?
    - http://www.dailymail.co.uk/news/article-2276282/EU-super-spies-right-snoop-emails-website-visits-medical-data-police-records.html
  - Rapport de l'exercice "Cyber Europe 2012"
    - http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/cyber-europe-2012/cyber-europe-2012-key-findings-report-1

Actualité (européenne)

- "Fighting Cyber Crime and protecting privacy in the Cloud"
  - http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050
- La déclaration des incidents de sécurité bientôt obligatoire ?
  - Pour le secteur de l'énergie, du transport, des banques, des hôpitaux, etc.
    - http://www.reuters.com/article/2013/02/06/us-eu-cybersecurity-idUSBRE91519020130206
- La neutralité du net menacée ?
  - https://www.laquadrature.net/fr/neutralite-du-net-neelie-kroes-cede-sous-la-pression-des-operateurs

Actualité (Google)

- Concours Pwnium III
  - Cible: Chrome OS
  - Total des prix: $3,14159 millions
    - http://blog.chromium.org/2013/01/show-off-your-security-skills-pwn2own.html
- Un bug de Google exploité pour du SEO
    - http://www.quora.com/Google-Search/What-does-4-1-4-mean-and-why-is-it-connected-to-porn
- Eric Schmidt en … Corée du Nord ?!
    - http://bigbrowser.blog.lemonde.fr/2013/01/21/perdre-le-nord-la-visite-tres-bizarre-de-la-fille-du-patron-de-google-en-coree-du-nord/
- Google vs. Microsoft
  - YouTube délibérément plus lent sur Windows Phone ?
    - https://blogs.technet.com/b/microsoft_on_the_issues/archive/2013/01/02/still-seeking-resolution-to-search-competition-issues.aspx
  - Plus de Google Maps sur Windows Phone
    - http://www.theverge.com/2013/1/5/3840620/google-bringing-maps-back-to-windows-phone

Actualité (Apple)

- **Sortie de iOS 6.1**
  - **Failles corrigées**
    - **"Authentication relying on certificate-based Apple ID authentication may be bypassed"**
    - **"A user-mode process may be able to access the first page of kernel memory"**
    - **"Multiple memory corruption issues existed in WebKit. These issues were addressed through improved memory handling"**
      - **Quelques dizaines …**
    - **"An out of bounds read issue exists in Broadcom's BCM4325 and BCM4329 firmware's handling of 802.11i information elements."**
    - **Révocation du certificat TURKTRUST**
    - **Etc.**
  - **Article de KB**
    - **http://support.apple.com/kb/HT5642**

Actualité (Apple)

- "The bug" dans Mac OS X
  - Taper "file:///" n'importe où fait crasher le système
  - Y compris le Crash Reporter ☺
    - https://news.ycombinator.com/item?id=5154648
    - http://nakedsecurity.sophos.com/2013/02/06/anatomy-of-a-bug-how-mac-os-x-chokes-if-you-type-file/

- Apple: la prison dorée
    - http://news.ycombinator.com/item?id=5064306

Actualité (crypto)

- Mega et la crypto
  - http://fail0verflow.com/blog/2013/megafail.html
- Un nouveau nombre de Mersenne découvert
  - http://science.slashdot.org/story/13/02/05/1439236/new-largest-known-prime-number-257885161-1
- Reconstruction d'une clé privée par SAT Solver
  - A partir quelques bits
    - http://eprint.iacr.org/2013/026
- Les clés USB "sécurisées"
  - … sont en fait vulnérables
    - http://www.darkreading.com/security/article/222200174/index.html

Actualité (crypto)

- Attaque "Lucky Thirteen" sur TLS-CBC
  - Il faut quand même avoir de la chance …
    - http://www.imperialviolet.org/2013/02/04/luckythirteen.html

- Résumé des attaques sur SSL/TLS
    - http://armoredbarista.blogspot.de/2013/01/a-brief-chronology-of-ssltls-attacks.html

- "How SSL works ?"
    - http://security.stackexchange.com/questions/20803/how-does-ssl-work

Actualité

- **Conférences passées**
  - **CES 2013**
    - **http://www.gizmodo.fr/tag/ces2013**
  - **FIC 2013**

Actualité

- Conférences à venir
  - OSSIR / JSSI 2013
    - http://www.ossir.org/
  - GS Days 2013
    - http://www.gsdays.fr/
  - SSTIC 2013
    - https://www.sstic.org/
  - NoSuchCon 2013 (CFP: 31/03)
    - http://www.nosuchcon.org
  - HES "canal historique"
    - http://2013.hackitoergosum.org
  - HIP 2013 (CFP: 22/02)
    - https://www.hackinparis.com/node/155
  - Nuit du Hack (CFP: 30/03)
    - http://www.nuitduhack.com/en/call-for-papers-nuit-du-hack
  - BotConf (CFP: 30/06)
    - https://www.botconf.eu/

Actualité

- **Sous-traitance non déclarée …**
  - Cette histoire est un "must read"
    - http://www.theregister.co.uk/2013/01/16/developer_oursources_job_china/
- **Sortie de BlackBerry 10**
  - Avec le terminal Z10
    - http://global.blackberry.com/blackberry-10.html
- **Packet Storm lance son Bug Bounty**
  - Avec publication sous 60 jours
    - http://packetstormsecurity.com/bugbounty/
- **Sony condamné à £250,000**
  - … suite à son attaque
    - http://www.indianexpress.com/news/Sony-fined-in-Britain-for-cyber-attack-data-breach/1064391/
- **La DARPA donne 3 M$ à Python**
    - http://developers.slashdot.org/story/13/02/06/0225259/python-gets-a-big-data-boost-from-darpa

Actualité

- **H.265 devient un standard**
  - **http://yro.slashdot.org/story/13/01/26/142257/itu-approves-h264-video-standard-successor-h265**
- **Michael Dell rachète Dell Inc.**
  - **http://www.citeworld.com/consumerization/21386/dell-goes-private-bought-michael-dell-and-silver-lake**
- **Seriez-vous prêts à payer $100 pour que Mark Zuckerberg lise votre email ?**
  - **http://www.forbes.com/sites/kashmirhill/2013/01/11/would-you-pay-100-to-send-mark-zuckerberg-a-facebook-message/**

Divers

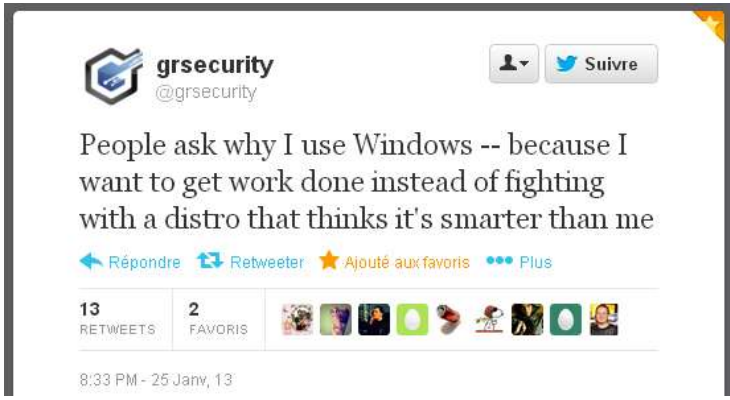
- Etes-vous dans la Liste ? ;)
  - http://resources.infosecinstitute.com/worlds-largest-public-hacker-database/
- L'OMC autorise Antigua & Barbuda à héberger des sites "pirates"
  - En représailles au blocage des casinos en ligne par les USA
    - http://www.linformaticien.com/actualites/id/27888/l-omc-autorise-le-piratage-d-etat.aspx
- Orange lance son "simulateur d'opérateur réseau" sur Facebook
  - http://www.pcinpact.com/news/77350-hellopolys-dorange-jeu-pour-creer-et-developper-son-reseau-telecom.htm
- Pour une fois, iOS Maps n'est pas en cause
  - http://spectrum.ieee.org/riskfactor/computing/it/it-hiccups-of-the-week-digital-navigation-error-leads-to-dismantling-of-us-navy-ship

Divers

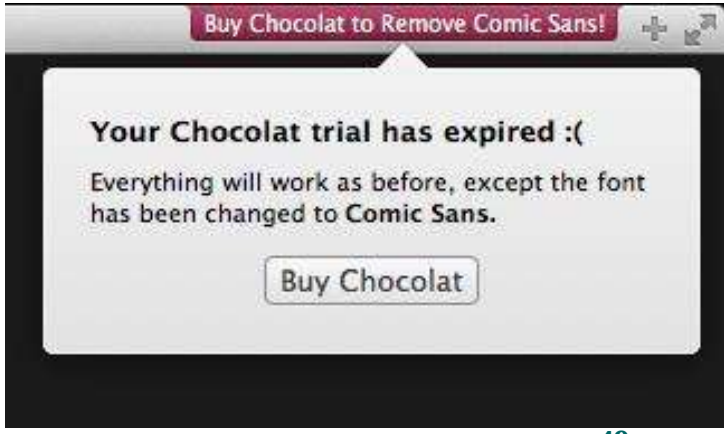
- Nokia réalise un MITM sur son navigateur Xpress pour les sessions HTTPS
  - http://gigaom.com/2013/01/10/nokia-yes-we-decrypt-your-https-data-but-dont-worry-about-it/
- Atari US se déclare en faillite
  - http://www.gamekult.com/actu/en-faillite-atari-us-veut-rompre-avec-la-structure-infogrames-A106953.html
- Un système de sécurité ?
  - http://qntm.org/suicide
- Le crash d'une comète dans le soleil pourrait détruire toute l'électronique sur Terre
  - C'est déjà arrivé en 775 et 1859
    - http://www.bulletins-electroniques.com/actualites/72045.htm

Divers

- Source
  - https://twitter.com/grsecurity/status/294890868110942210



  - https://twitter.com/Intrepidd/status/290513181019893762/photo/1



Questions / réponses

- Questions / réponses
- AfterWork de l'OSSIR
  - Mardi 26 février 2013
    - Sujet: Mimikatz
- Conférence JSSI de l'OSSIR
  - Mardi 19 mars 2013
    - http://www.ossir.org/jssi/
- Prochaine réunion
  - Mardi 9 avril 2013