

OSSIR
Groupe Paris
Réunion du 9 avril 2013



Revue des dernières vulnérabilités

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

Avis Microsoft

■ Février 2013

- **MS13-009 Correctif cumulatif pour IE (x13) [1]**
 - **Affecte: IE (toutes versions supportées)**
 - **Exploit:**
 - **Contournement de la SOP via Shift JIS**
 - **Exécution de code via "use after free" (x12)**
 - **Notes:**
 - **Disponible dans Metasploit**
 - **http://www.security-assessment.com/files/documents/advisory/ms13_009_ie_slayoutrun_uf.pdf**
 - **<http://www.exploit-db.com/exploits/24495/>**

Avis Microsoft

- **Crédits:**

- Masato Kinugawa
- Omair
- Omair + ZDI
- SkyLined + ZDI
- Arthur Gerkis + Exodus Intelligence
- Arthur Gerkis + ZDI
- Stephen Fewer / Harmony Security + ZDI (x2)
- Tencent PC Manager
- anonymous + ZDI
- Scott Bell / Security-Assessment.com (x2)
- Jose A Vazquez / Yenteasy Security Research + Exodus Intelligence
- Jose A Vazquez / Yenteasy Security Research + ZDI
- Mark Yason / IBM X-Force
- Aniway.Aniway@gmail.com + ZDI
- Ollie Whitehouse / NCC Group

Avis Microsoft

- **MS13-010 Faille dans VML (x1) [1]**
 - Affecte: IE (toutes versions supportées)
 - Exploit: exécution de code
 - Utilisé "dans la nature" par des attaques ciblées
 - Crédit: n/d

- **MS13-011 Faille dans DirectShow (quartz.dll) (x1) [1]**
 - Affecte: Windows XP / 2003 / Vista / 2008
 - Exploit: exécution de code à l'ouverture d'un flux malformé
 - Exploitable via MPG, PPT ...
 - Crédit: Tencent Security Team

- **MS13-012 Faille dans WebReady Document Viewing (x2) [2]**
 - Affecte: Exchange 2007 SP3, 2010 SP2
 - Exploit: failles dans les moteurs de rendu "Oracle Outside"
 - Exécution de code sous "LocalService" par un utilisateur OWA
 - Crédit: n/d

Avis Microsoft

- **MS13-013 Faille dans FAST Search Server (x2) [1]**
 - **Affecte:** FAST Search Server 2010 for SharePoint SP1 / Advanced Filter Pack
 - **Exploit:** exécution de code
 - Via l'indexation d'un document
 - **Crédit:** n/d

- **MS13-014 Faille dans NFS (x1) [3]**
 - **Affecte:** Windows 2008R2, 2012
 - **Exploit:** déni de service
 - Via un pointeur NULL
 - **Crédit:** n/d

Avis Microsoft

- **MS13-015 Faille dans .NET Framework (x1) [1]**
 - **Affecte: .NET Framework (toutes versions supportées, sauf ...)**
 - .NET 1.0 SP3
 - .NET 1.1 SP1
 - .NET 3.0 SP2
 - .NET 3.5 SP1
 - .NET 4.5 RT
 - **Exploit: évasion de la sandbox**
 - Via un callback dans WinForms
 - **Crédit: James Forshaw / Context Information Security**

- **MS13-016 Faille dans WIN32K.SYS (x30 !) [2]**
 - **Affecte: Windows (toutes versions supportées)**
 - **Exploit: élévation de privilège**
 - Via une "race condition"
 - **Crédit:**
 - Mateusz "j00ru" Jurczyk / Google (x27)
 - Gynvael Coldwind & Mateusz "j00ru" Jurczyk / Google (x3)

Avis Microsoft

- **MS13-017 Faille noyau (x3) [1]**
 - **Affecte: Windows (toutes versions supportées)**
 - **Exploit: élévation de privilèges**
 - Via "race condition" (x2)
 - Via un compteur de références (x1)
 - **Crédit: Mateusz "j00ru" Jurczyk / Google (x2)**

- **MS13-018 Faille TCP/IP (x1) [3]**
 - **Affecte: Windows (toutes versions supportées, sauf XP et 2003)**
 - **Exploit: déni de service**
 - Via des connexions en état "TCP FIN WAIT"
 - **Crédit: n/d**

Avis Microsoft

- **MS13-019 Faille dans CSRSS (x1) [2]**
 - Affecte: Windows 7, 2008R2
 - Exploit: élévation de privilèges
 - Via un compteur de références
 - Crédit: Max DeLiso

- **MS13-020 Faille dans OLE Automation (x1) [1]**
 - Affecte: Windows XP SP3
 - Exploit: exécution de code via un document OLE malformé
 - Exploitable via Office, Wordpad, ...
 - Crédit: anonymous + ZDI

Avis Microsoft

■ Mars 2013

- **MS13-021 Correctif cumulatif pour IE (x9) [1]**
 - Affecte: IE (toutes versions supportées)
 - ... sauf IE10 pour Windows 7 / 2008R2
 - Exploit: "use after free" (x9)
 - Crédit:
 - Arseniy Akuney / TELUS Security Labs
 - Anonymous + ZDI (x2)
 - Stephen Fewer / Harmony Security
 - SkyLined
 - Jose A. Vazquez / Yenteasy Security Research + Exodus
 - Aniway.Aniway@gmail.com + ZDI (x2)
 - Simon Zuckerbraun + ZDI
 - Gen Chen / Venustech ADLab
 - Qihoo 360 Security Center

- **MS13-022 Faille SilverLight (x1) [1]**
 - Affecte: SilverLight 5 (Windows et Mac)
 - Exploit: évacion de la *sandbox* via "double dereference"
 - Crédit: James Forshaw / Context Information Security

Avis Microsoft

- **MS13-023 Faille Visio Viewer (x1) [2]**
 - Affecte: Visio Viewer 2010 SP1
 - Exploit: exécution de code à l'ouverture d'un fichier .VSD malformé
 - Crédit: Aniway.Aniway@gmail.com + iDefense

- **MS13-024 Failles SharePoint (x4) [1]**
 - Affecte: SharePoint 2010 SP1
 - Exploit:
 - XSS
 - "Directory traversal"
 - "Buffer overflow"
 - "Problème avec les callbacks"
 - Crédit:
 - Emanuel Bronshtein / BugSec
 - Sunil Yadav / INR Labs (Network Intelligence India)
 - Moritz Jodeit / n.runs AG

Avis Microsoft

- **MS13-025 Faille OneNote (x1) [3]**
 - Affecte: OneNote 2010 SP1
 - Exploit: fuite d'information à l'ouverture d'un fichier ".ONE"
 - Crédit: Christopher Gabriel / Telos Corporation

- **MS13-026 Faille dans Outlook pour Mac (x1) [3]**
 - Affecte: Office 2008 et 2011
 - Exploit: chargement de contenu externe HTML5 sans confirmation à la prévisualisation d'un email
 - Crédit: Nick Semenkovich

- **MS13-027 Failles dans des pilotes USB (x3) [1]**
 - Affecte: Windows (toutes versions supportées sauf Windows RT)
 - Exploit: élévation de privilèges locale
 - Crédit: Andy Davis / NCC Group

Avis Microsoft

■ Advisories

- **Q2755801 Faille Flash dans IE10**
 - V8.0: nouveau correctif
 - V9.0: nouveau correctif

- **Q2819682 Faille dans une application du Store**
 - V1.0: faille dans Windows Modern Mail

Avis Microsoft

■ Prévisions pour Avril 2013

- 9 bulletins (2 critiques)

■ Failles à venir

- BSOD / processus immortel
 - <http://waleedassar.blogspot.com.es/2013/02/kernel-bug-1-processiopriority.html>
- Exécuter un programme non signé depuis un programme signé
 - <http://www.exploit-monday.com/2013/02/WindowsFileConfusion.html>
- "Download & execute" avec Office 2010
 - <http://www.exploit-db.com/exploits/24526/>
- Faille WIN32K.SYS
 - https://bugs.freedesktop.org/show_bug.cgi?id=62764

Avis Microsoft

■ Retour sur des failles antérieures

- **MS12-081**
 - <http://blog.ptsecurity.com/2013/02/surprise-for-network-resources-from.html>
- **MS13-009**
 - Disponible dans Metasploit
- **MS13-020**
 - <https://twitter.com/VUPEN/status/302115103334076416>
- **MS13-027**
 - <http://blog.ssfighter.com/2011/04/a-simple-analysis-about-rndis-driver/>
 - <https://twitter.com/ponez/status/318352766173077505/photo/1>

■ Révisions

- **MS12-034**
 - V1.6: correction des bulletins remplacés
- **MS12-043**
 - V4.1: mise à jour documentaire
- **MS12-057**
 - V2.1: mise à jour documentaire
- **MS12-060**
 - V2.1: mise à jour documentaire

Avis Microsoft

- **MS13-003**
 - V2.0: publication d'un correctif pour SCOM 2007 SP1
- **MS13-004**
 - V2.1: changement de la logique de détection pour .NET 1.1 SP1
- **MS13-005**
 - V1.2: ajout d'un problème connu
- **MS13-006**
 - V1.1: ajout d'un problème connu
- **MS13-007**
 - V1.1: ajout d'un contournement sur Windows 2012
- **MS13-009**
 - V1.1: ajout d'un problème connu
- **MS13-010**
 - V1.1: ajout d'un problème connu
- **MS13-012**
 - V1.1: Exchange 2010 SP3 n'est pas affecté

Avis Microsoft

- **MS13-016**
 - V1.1: ajout d'un problème connu
- **MS13-017**
 - V1.1: ajout d'un problème connu
- **MS13-018**
 - V1.1: ajout d'un problème connu
- **MS13-020**
 - V1.1: corrections documentaires dans la FAQ
- **MS13-022**
 - V1.2: ajout d'un problème connu
- **MS13-023**
 - V1.1: corrections documentaires dans la FAQ
- **MS13-026**
 - V1.1: corrections documentaires dans la FAQ

Infos Microsoft

■ Sorties logicielles

- IE 10 pour Windows 7

Infos Microsoft

■ Autre

- **Windows 7 SP0 n'est plus supporté**
 - Depuis le 9 avril 2013
 - <http://blogs.windows.com/windows/b/springboard/archive/2013/02/14/windows-7-rtm-end-of-support-is-right-around-the-corner.aspx>
- **Vrai ou faux antivirus ?**
 - (Le challenge est une application Facebook)
 - https://www.facebook.com/msftmmpc/app_236330836495399
- **Azure en panne le 22 février**
 - ... à cause d'un certificat expiré
 - <http://www.zdnet.fr/actualites/longue-panne-de-windows-azure-a-cause-d-un-certificat-ssl-expire-39787583.htm>
- **A quoi sert Azure ?**
 - C'est un "pierre, feuille, ciseau" géant !
 - <http://www.rockpaperazure.com/>

Infos Microsoft

- **Microsoft propose ses services aux ccTLD**
 - <http://technet.microsoft.com/en-us/security/jj992598>
- **Facebook rachète Atlas à Microsoft**
 - <http://www.theverge.com/2013/2/28/4041058/facebook-buys-microsoft-ad-platform-atlas>
- **Le SDL devient (ou va devenir) ISO 27034**
 - <http://www.iso27001security.com/html/27034.html>
- **Mise à jour du Jailbreak pour Windows RT**
 - <http://forum.xda-developers.com/showthread.php?t=2092158>
- **Un émulateur x86 sur Windows RT**
 - <http://forum.xda-developers.com/showthread.php?t=2095934>

Infos Microsoft

- **Surface peine à émerger**
 - <http://www.20minutes.fr/web/1119365-20130315-tablettes-surface-ventent-toujours>
- **Bill Gates: "la stratégie mobile de Microsoft n'est pas bonne"**
 - <http://venturebeat.com/2013/02/18/bill-gates-microsoft-mobile-strategy-mistake/>
- **... il est temps que ça change**
 - <http://readwrite.com/2013/04/08/microsofts-board-of-directors-time-for-a-change>

Infos Microsoft

- **L'état français réclame 52,5 M€ à Microsoft France**
 - http://www.lemonde.fr/technologies/article/2013/02/15/le-fisc-francais-reclamerait-52-5-millions-d-euros-a-microsoft_1833500_651865.html
- **L'Europe inflige une amende de 561 M€ à Microsoft**
 - <http://www.leparisien.fr/high-tech/microsoft-encore-lourdement-mis-a-l-amende-par-bruxelles-06-03-2013-2621115.php>
- **Microsoft attaqué par l'APRIL**
 - **Pour son contrat avec le MinDef**
 - <http://www.april.org/open-bar-microsoft-defense-pas-de-reponse-de-ladministration-lapril-saisit-la-cada>

Infos Microsoft

■ Skype

- **Quelle surprise ...**
 - <http://www.fhimt.com/2012/05/17/microsoft-a-installe-un-logiciel-espion-dans-skype/>
- **La carte des réquisitions légales**
 - <https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/>
- **Les russes écoutent Skype**
 - <http://www.lemagit.fr/technologie/reseaux-telecoms/toip-voip/2013/03/18/le-renseignement-russe-pourrait-intercepter-les-conversations-skype/>
- **Ainsi que les chinois (depuis plus longtemps)**
 - <http://www.businessweek.com/articles/2013-03-08/skypes-been-hijacked-in-china-and-microsoft-is-o-dot-k-dot-with-it>

Infos Réseau

■ (Principales) faille(s)

- **Les bulletins Cisco (mars 2013)**
 - http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html
- **L'entrée SNMP "UserInfoEntry" contient les mots de passe d'accès aux produits réseau HP**
 - ... ainsi que certains produits Huawei
 - <http://packetstormsecurity.com/files/cve/CVE-2012-3268>
- **Le registrar du Malawi (.mw) compromis**
 - <http://www.zone-h.com/archive/notifier=TiGER-M@TE>
 - <http://www.zone-h.com/archive/notifier=h311%20c0d3>
- **Les nouveaux mots de passe Cisco "type 4"**
 - ... sont beaucoup moins sécurisés !
 - <http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20130318-type4>

Infos Réseau

■ Autres infos

- **Internet a été scanné**
 - Compter 570 Go de données environ ☺
 - <http://internetcensus2012.bitbucket.org/paper.html>
- **DDoS contre SpamHaus**
 - 300Gb/s de trafic (via des DNS ouverts)
 - Internet victime collatérale ... ou pas
- **Un opérateur ajoute des publicités dans le trafic de ses clients**
 - <http://arstechnica.com/tech-policy/2013/04/how-a-banner-ad-for-hs-ok/>
- **Les "ennemis d'Internet" selon RSF**
 - Gamma, Trovicor, Hacking Team, Amesys et Blue Coat
 - <http://surveillance.rsf.org/>
- **Un IDS à l'échelle d'Internet**
 - Selon T-System
 - <http://www.sicherheitstacho.eu/>

■ (Principales) faille(s)

- **Élévation de privilèges dans le noyau Linux**
 - Race condition dans PTRACE_SETREGS
 - **Crédit: Google Security Team**
 - <http://seclists.org/oss-sec/2013/q1/326>
- **Élévation de privilèges dans le noyau Linux**
 - **Cause: sock_diag_handlers**
 - <http://www.exploit-db.com/exploits/24746/>
- **Faille dans le générateur d'aléa NetBSD < 6.1**
 - <http://www.h-online.com/security/news/item/Weak-keys-in-NetBSD-1829336.html>

Infos Unix

- **Faille dans Ruby On Rails**
 - **Désérialisation YAML**
 - http://threatpost.com/en_us/blogs/ruby-rails-patches-dos-remote-execution-flaws-021313
- **Faille (?) dans "sudo -k"**
 - **Si l'utilisateur contrôle l'horloge**
 - http://www.sudo.ws/sudo/alerts/epoch_ticket.html
- **Exécution de commandes via pam_fprintd ...**
 - ... en passant un doigt sur le lecteur d'empreintes
 - <http://stealth.openwall.net/xSports/darklena.c>

Infos Unix

■ Autres infos

- **Brad vs. Linux**
 - <http://lwn.net/Articles/538600/>
- **PAX supporte KERNEXEC et UDEREF sur ARM**
 - <http://forums.grsecurity.net/viewtopic.php?f=7&t=3292>
- **Red Hat doit-il faire signer son bootloader par Microsoft ?**
 - **Linus n'est pas d'accord ☺**
 - <http://www.muktware.com/5276/linus-torvalds-secure-boot-supporters-not-dick-sucking-contest>
- **GCC 4.8 est sorti**
 - <http://linuxfr.org/news/la-version-4-8-du-compileur-gcc-est-disponible>
- **OpenSSH 6.2 est sorti**
 - <http://www.openssh.com/txt/release-6.2>

- **Utiliser nginx à vos risques et périls**
 - ... sur Debian/Ubuntu
 - https://twitter.com/ns_m/status/320937463554113539
- **cPanel compromis**
 - <http://nakedsecurity.sophos.com/2013/03/01/cpanel-suffers-break-in-loses-root-passwords/>
- **Le rootkit "Linux.Sshdkit" déployé en masse**
 - Un rapport ?
 - <http://letsbytecode.com/security/dr-web-mass-hacking-linux-based-servers-by-linux-sshdkit/>
 - <https://isc.sans.edu/diary/SSHD+rootkit+in+the+wild/15229>
- **NetBSD va supporter le scripting LUA en kernelland**
 - <http://bsd.slashdot.org/story/13/02/16/2329259/netbsd-to-support-kernel-development-in-lua-scripting>

Failles

■ Principales applications

- **Adobe Reader**

- <http://blogs.adobe.com/psirt/2013/02/adobe-reader-and-acrobat-vulnerability-report.html>
- <https://www.adobe.com/support/security/bulletins/apsb13-07.html>

- **Faille exploitée "dans la nature"**

- **... Avec évvasion de sandbox**

- <http://blogs.mcafee.com/mcafee-labs/analyzing-the-first-rop-only-sandbox-escaping-pdf-exploit>

- **Note: "Protected Mode" est désactivé par défaut (!)**

- <http://www.darkreading.com/advanced-threats/167901091/security/attacks-breaches/240148632/new-sophisticated-zero-day-attacks-cheat-key-security-features-in-adobe-reader-acrobat.html>
- <http://eromang.zataz.com/2013/02/13/new-adobe-pdf-reader-0day-and-acrobat-found-exploited-in-the-wild/>

Failles

- **Java < 1.6.41, < 1.7.15**
 - **Faille exploitée pour compromettre Facebook, Apple et Microsoft**
 - <http://www.reuters.com/article/2013/02/19/us-apple-hackers-idUSBRE91I10920130219>
 - **... via Mac OS X ☺**
 - https://blogs.oracle.com/security/entry/updates_to_february_2013_critical
- **Java < 1.6.43, < 1.7.17**
 - <http://www.oracle.com/technetwork/topics/security/alert-cve-2013-1493-1915081.html>
- **La mise à jour Java est impossible depuis l'Iran**
 - **Oracle se conforme à la loi américaine**
 - <http://cryptome.org/2013/03/oracle-ir-block.htm>
- **Pour conclure:**
 - <http://istherejava0day.com/>
 - <http://java-0day.com/>

Failles

- **Flash**

- Depuis février 2013:

- <https://www.adobe.com/support/security/bulletins/apsb13-04.html>
 - <https://www.adobe.com/support/security/bulletins/apsb13-05.html>
 - <https://www.adobe.com/support/security/bulletins/apsb13-08.html>
 - <https://www.adobe.com/support/security/bulletins/apsb13-09.html>

- **ShockWave**

- <https://www.adobe.com/support/security/bulletins/apsb13-06.html>

- **Wireshark < 1.8.6**

- **Firefox < 20**

- <http://www.mozilla.org/security/known-vulnerabilities/firefox.html>

- **ThunderBird < 17.0.5**

- <http://www.mozilla.org/security/known-vulnerabilities/thunderbird.html>

Failles

- **Faille dans libtiff**
 - <https://bugzilla.redhat.com/attachment.cgi?id=616925>
 - **Affecte également BlackBerry MDS**
 - <http://btsc.webapps.blackberry.com/btsc/viewdocument.do?externalId=KB33425&sliceId=1&cmd=displayKC&docType=kc&noCount=true&ViewedDocsListHelper=com.kanisa.apps.common.BaseViewedDocsListHelperImpl>
- **Faille dans le serveur SSH de VxWorks**
 - **CVSS 10/10**
 - <https://cxsecurity.com/cveshow/CVE-2013-0714/>
- **VMWare**
 - **Depuis le début de l'année**
 - <http://www.vmware.com/security/advisories/VMSA-2013-0001.html>
 - <http://www.vmware.com/security/advisories/VMSA-2013-0002.html>
 - <http://www.vmware.com/security/advisories/VMSA-2013-0003.html>
 - <http://www.vmware.com/security/advisories/VMSA-2013-0004.html>
 - <http://www.vmware.com/security/advisories/VMSA-2013-0005.html>

Failles 2.0

■ OAuth encore cassé sur Facebook

- (Et d'autres)

- <http://www.nirgoldshlager.com/2013/02/how-i-hacked-facebook-oauth-to-get-full.html>
- <http://techcrunch.com/2013/04/03/goldschlager-saves-the-day/>

■ La clé d'API Twitter sur GitHub

- http://threatpost.com/en_us/blogs/twitter-oauth-api-keys-leaked-030713

■ On a pas fini de trouver des trucs rigolos sur GitHub

- <https://github.com/search?q=.netrc+password+login&ref=searchresults&type=Code>

■ Brouiller le GPS

- De moins en moins cher

- <http://arstechnica.com/security/2012/12/how-to-bring-down-mission-critical-gps-networks-with-2500/>

■ Identifier les motifs clavier dans les mots de passe

- <http://www.digininja.org/projects/passpat.php>

Failles 2.0

- **HTC condamné ... à distribuer des correctifs pour ses téléphones Android**
 - Par la FTC
 - <http://business.ftc.gov/blog/2013/02/device-squad-story-behind-ftcs-first-case-against-mobile-device-maker>

- **Motorola TrustZone vulnérable**
 - <http://blog.azimuthsecurity.com/2013/04/unlocking-motorola-bootloader.html>

- **Récupérer des données dans le "buckets" Amazon S3**
 - Aussi simple que de deviner l'URL
 - <https://community.rapid7.com/community/infosec/blog/2013/03/27/1951-open-s3-buckets>

- **Code source du BIOS AMI + clé de signature UEFI**
 - ... sur un FTP anonyme
 - http://www.reddit.com/r/netsec/comments/1bqe59/ami_uefi_key_leaked/
 - <http://it.slashdot.org/story/13/04/05/1731230/ami-firmware-source-code-private-key-leaked>

Sites piratés

■ Les sites piratés du mois (liste partielle)

- Facebook, Microsoft, Apple ...
 - Via un drive-by download de Java
 - <https://www.facebook.com/notes/facebook-security/protecting-people-on-facebook/10151249208250766>
 - <http://blogs.technet.com/b/msrc/archive/2013/02/22/recent-cyberattacks.aspx>
- Evernote
 - <http://www.h-online.com/security/news/item/Evernote-note-service-hacked-password-reset-mails-worry-users-1815485.html>
- Les radars automatiques
 - A Moscou ☹
 - http://www.theregister.co.uk/2013/02/28/malware_hobbles_moscow_speed_cams/
- Les zombies attaquent
 - ... ou pas
 - <http://nakedsecurity.sophos.com/2013/02/12/hackers-zombie/>

Sites piratés

- **Michelle Obama, Beyoncé, Hillary Clinton ...**
 - <http://exposed.su/>
- **Le "Defence Research and Development Organisation" (DRDO) indien**
 - Organise un challenge public de contre-attaque
 - ... et le challenge a été gagné (!)
- **La National Vulnerability Database (NVD) du NIST**
 - Sert du malware (!)
 - <http://paritynews.com/security/item/820-us-national-vulnerability-database-down-following-malware-infestation>
- **EADS (?)**
 - http://www.lemonde.fr/technologies/article/2013/02/24/eads-attaque-par-des-hackers-chinois_1837971_651865.html
- **La "fuite" de données s'élève à 1To/jour**
 - D'après Team Cymru
 - <http://www.theverge.com/2013/2/27/4035378/new-report-finds-hackers-stealing-terabyte-daily>

Sites piratés

- **Anonymous #OpIsrael**
 - <http://thehackernews.com/2013/04/opisrael-7-april-anonymous-calls-to.html>
- **InstaWallet**
 - <http://thehackernews.com/2013/04/bitcoins-wallet-service-instawallet.html>
- **Inj3ct0r / 1337day.com**
 - **Empoisonnement du DNS**
 - <http://news.thehackernews.com/exploit-database-website-inj3ct0r-defaced>
- **De nombreuses sociétés opérant à Dubai**
 - <http://gulfnews.com/news/gulf/uae/crime/gang-arrested-for-hacking-dubai-exchange-companies-accounts-1.1153543>
- **Le compte Twitter de BurgerKing**
 - https://twitter.com/unix_root/status/303559941594177536/photo/1
- **ZenDesk**
 - <https://twitter.com/TheHackersNews/status/305006265950683136/photo/1>

Sites piratés

- **Australian Broadcasting Corporation (ABC)**
 - 50,000 comptes
 - <http://www.esecurityplanet.com/hackers/australian-broadcasting-corporation-hacked.html>
- **Avast.de**
 - 20,000 comptes
 - <http://www.security-faqs.com/avast-de-hacked-and-defaced-20000-user-accounts-leaked.html>
- **NBC.com**
 - Malware déposé
 - <http://www.nbcnews.com/technology/technolog/nbc-com-hacked-say-security-researchers-1C8483074>
- **Bible.org**
 - Malware déposé
- **(Si vous en voulez d'autres)**
 - <https://twitter.com/dumpmon>

Malwares, spam et fraudes

- **Etude de cas: une unité de cyber-espionnage chinoise**
 - http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf
 - ... ajouter à cela
 - <http://www.f-secure.com/weblog/archives/00002221.html>
 - ... et ses suites
 - http://www.malware.lu/Pro/RAP002_APT1_Technical_backstage.1.0.pdf

- **"La Chine ne pratique pas la cyberattaque"**
 - http://www.china.org.cn/china/2013-02/28/content_28090377.htm

- **"La Chine est prête à coopérer avec les USA sur le sujet de la cybersécurité"**
 - <http://www.reuters.com/article/2013/03/12/us-usa-china-cybersecurity-idUSBRE92A0XO20130312>

- **"Sur Internet, tout le monde sait que vous êtes un chinois"**
 - "Tawnya Grilth" == "Zhang Changhe"
 - <http://www.businessweek.com/articles/2013-02-14/a-chinese-hackers-identity-unmasked>

Malwares, spam et fraudes

■ Source:

- <https://twitter.com/daveaitel/status/304988550783434752/photo/1>



Malwares, spam et fraudes

■ RSA Conference 2013

- Source:

- <https://twitter.com/y0m/status/304972967786467329/photo/1>

20' Stonesoft 20' 1953	20' Dell Quest Software 20' 2053	20' AirWatch 20' 2153	20' VMware 20' 2253	Key Source 2355	Mocana 2454	Behavioric 2455	Sourcefire 20'	Stouthbits Tech Inc 2555	HB Gary 30'	20' Huawei Tech Co., Ltd 30' 2651
20' Cyber-Ark Software 20' 1947	20' Norman ASA 20' 2047	20' VSS Monitoring 20' 2147	20' Rapid7 20' 2247	20' Solera Net 20' 2345	20' Core Security 20' 2445	20' Napatech 20'	Thycotic Software 20' 2644	20' Juniper Networks 20' 2645		
20' Oracle 20' 1941	20' SAIC 20' 2041	20' GFI Software 20' 2141	20' Fasoo.com 20' 2241	20' Netronome 20' 2339	20' Mandiant 20' 2439	20' Prolexic Technology 20' 2539	20' Manage Engne 2641	Verdasys 20'		
20' Dell SecureWorks 30' 1933	20' Beijing Zhongguancun Overseas Science Park Co.,Ltd 30' 2033	20' Beijing Zhongguancun Overseas Science Park Co.,Ltd 30' 2133	20' Damballa 30' 2233	20' Spyrus, Inc. 20' 2333	20' Cyberoam 20' 2433	20' CounterTack 20' 2533	Digital Defense 2637	Comodo 20'		
							CloudLock 2635	2734	CHERRY 2633	Klocwork 2732

Malwares, spam et fraudes

■ Des attaques avancées à n'en plus finir

- "MiniDuke"

- C&C sur Twitter
- Chiffrement du code par PC
- ... et plein d'autres astuces
- http://www.securelist.com/en/blog/208194129/The_MiniDuke_Mystery_PDF_0_da_y_Government_Spy_Assembler_0x29A_Micro_Backdoor

- "TeamSpy"

- Utilise TeamViewer comme backdoor
- <http://www.crysys.hu/teamspy/teamspy.pdf>

■ FinFisher dans le monde

- <https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/>

■ L'auteur du Phoenix Exploit Kit arrêté en Russie

- <http://krebsonsecurity.com/2013/04/phoenix-exploit-kit-author-arrested-in-russia/>

Malwares, spam et fraudes

- **Gapz: un bootkit très élaboré**
 - <http://www.welivesecurity.com/2013/04/08/is-gapz-the-most-complex-bootkit-yet/>

- **McAfee révoque "par accident" son certificat de signature Apple ...**
 - <http://arstechnica.com/security/2013/02/a-world-of-hurt-after-mcafee-mistakenly-revokes-key-for-signing-mac-apps/>

- **Un journaliste rançonné par un pirate chinois**
 - http://www.slate.com/articles/technology/future_tense/2013/02/new_york_times_security_breach_how_a_chinese_hacker_tried_to_blackmail_me.html

- **\$33m détournés dans un casino**
 - ... en piratant le système de vidéosurveillance
 - http://www.theregister.co.uk/2013/03/15/cctv_hack_casino_poker/

- **Il va être possible d'acheter via un hashtag Twitter**
 - <http://tech.slashdot.org/story/13/02/12/2031246/twitter-american-express-letting-people-purchase-goods-via-hashtag>

Actualité (francophone)

■ Publication de l'ANSSI

- Sécurité des dispositifs de vidéoprotection
 - Recommandation: changer les mots de passe par défaut ...
 - <http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-des-dispositifs-de-videoprotection/recommandations-de-securite-pour-la-mise-en-oeuvre-de-dispositifs-de.html>
- Configurer son pare-feu
 - http://www.ssi.gouv.fr/IMG/pdf/NP_Politique_pare_feu_NoteTech.pdf
- Configurer son WiFi
 - http://www.ssi.gouv.fr/IMG/pdf/NP_WIFI_NoteTech.pdf

■ Publication de la CNIL

- La vie privée en 2020
 - http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/DEIP/CNIL-CAHIERS_IPn1.pdf

■ Publication du CIGREF

- Cloud Computing et protection des données
 - <http://www.cigref.fr/publications-numeriques/Guide-cloud-computing-2013/files/assets/common/downloads/Guide-cloud-computing-2013.pdf>

Actualité (francophone)

■ Publications du gouvernement

- Numérique

- http://www.gouvernement.fr/sites/default/files/fichiers_joints/feuille_de_route_du_gouvernement_sur_le_numerique.pdf

- THD

- http://www.gouvernement.fr/sites/default/files/fichiers_joints/plan_tres_haut_debit.pdf

- Open Data

- http://www.gouvernement.fr/sites/default/files/fichiers_joints/donnees-publiques.pdf

■ "Cadre stratégique commun du SI de l'Etat"

- http://circulaire.legifrance.gouv.fr/pdf/2013/03/cir_36639.pdf

■ Les parlementaires français interdits de Twitter en séance ?

- <http://www.assemblee-nationale.fr/14/propositions/pion0709.asp>

■ Quelques néologismes ...

- http://www.education.gouv.fr/pid25535/bulletin_officiel.html?cid_bo=66811

■ 11,5 M€ pour le "Big Data"

- <http://proxy-pubminefi.diffusion.finances.gouv.fr/pub/document/18/14672.pdf>

Actualité (francophone)

■ Qui ne parle pas de cyber défense aujourd'hui ?

- "Le risque numérique: en prendre conscience pour mieux le maîtriser ?"
 - http://www.senat.fr/fileadmin/Fichiers/Images/opecst/programme_auditions_publicques/prog_risques_numeriques21fev2013.pdf
- "Office parlementaire d'évaluation des choix scientifiques et technologiques"
 - <http://www.assemblee-nationale.fr/14/cr-oecst/12-13/c1213020.asp>
 - <http://www.senat.fr/compte-rendu-commissions/20130218/opecst.html>
- Centre d'analyse stratégique: "cybersécurité, l'urgence d'agir"
 - <http://www.strategie.gouv.fr/content/cybersecurite-urgence-na324>
 - <http://www.strategie.gouv.fr/tv-cas/10?id=xybigq&nid=2613>
- Défense & Stratégie: "le cybertalk"
 - <https://allchemi.eu/course/view.php?id=89>

Actualité (francophone)

- **La "Réserve Citoyenne Cyberdéfense"**
 - <http://magazine.qualys.fr/cyber-pouvoirs/reserve-citoyenne-cyberdefense/>

- **CNNum**
 - "La neutralité du Net, une liberté fondamentale"
 - <http://www.cnnumerique.fr/neutralite/>

- **ANSSI vs. OpenVPN sur l'AppStore**
 - <https://forums.openvpn.net/topic11983.html>

- **France vs. Skype**
 - Skype est-il un opérateur télécom ?
 - <http://www.engadget.com/2013/03/12/france-investigates-skype-after-it-doesnt-register-as-telecom/>

- **Une clé USB personnelle qui a été branchée sur un ordinateur professionnel**
 - ... peut être inspectée par l'employeur hors de la présence du salarié
 - <http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000027073247&fastReqlid=2119388883&fastPos=1>

Actualité (francophone)

- **Xavier Niel + Nicolas Sadirac = une école de programmation gratuite**
 - **Projet "Born 2 Code"**
 - <http://www.42.fr/>
 - **Les 1000 premiers diplômés se voient déjà proposer un CDI (!)**
 - <http://recrutementweb.com/ametix-recrute-lensemble-des-1000-premiers-eleves-de-42-lecole-montee-par-xavier-niel/>

- **CerberHost Spring Challenge**
 - <http://www.nbs-system.com/blog/cerberhost-spring-challenge.html>

- **Bilan de <http://www.phishing-initiative.com/>**
 - **80,000 sites identifiés en 2 ans**
 - <http://www.leparisien.fr/flash-actualite-high-tech/hameconnage-sur-le-net-80-000-sites-signales-par-le-grand-public-en-france-21-03-2013-2659025.php>

- **Des terminaux de paiement piégés ... en France**
 - **Un relais Bluetooth inséré à l'insu du commerçant**
 - <http://www.leparisien.fr/faits-divers/l-ingenieur-systeme-des-escrocs-a-la-carte-bancaire-05-04-2013-2699609.php>

- **Arkoon lance "Open Community"**
 - <http://open.arkoon.net/>

Actualité (francophone)

■ La DCRI découvre Streisand

– https://meta.wikimedia.org/wiki/Legal_and_Community_Advocacy/Statement_on_France/fr

• Du boulot pour eux

– <http://www.pcinpact.com/news/78874-parfois-sur-bing-maps-il-suffit-zoomer-pour-voir-batiments-floutes.htm>

■ Critiquer le vote électronique, c'est mal

– <http://www.numerama.com/magazine/25271-numerama-doit-avoir-plus-de-mesure-dans-la-critique-du-vote-electronique.html>

■ Un dossier médical sur Internet

– <http://www.laprovence.com/article/actualites/2233348/marseille-une-mere-decouvre-son-dossier-medical-sur-internet.html>

Actualité (francophone)

■ EDF vs. GreenPeace

- EDF relaxé en appel
 - http://www.legalis.net/spip.php?page=breves-article&id_article=3679

■ HADOPI

- "Sony devrait autoriser la lecture des BluRays avec VLC"
 - http://www.lemonde.fr/technologies/article/2013/04/08/la-hadopi-rend-son-avis-sur-la-lecture-des-blu-ray-par-vlc_3156110_651865.html

■ Un radar automatique découpé à la disqueuse

- <http://blog.radars-auto.com/index.php?post/un-radar-decoupe-a-la-disqueuse-et-vole-838>

■ Fin du site Ghosts In The Stack

- <http://ghostsinthestack.org/>

Actualité (anglo-saxonne)

- **La NSA déclassifie les anciennes éditions de sa newsletter (Cryptolog)**
 - 157 Go de stockage ... en 1977
 - *"Quite apart from the fact that the subject matter as such is foreign to a woman's mentality, it must be added that it is extremely difficult for most women to engage in work about which no work must be spoken"*
 - http://www.schneier.com/blog/archives/2013/03/the_nsas_crypto.html

- **Nouvelle règle: la "cyber attaque préventive"**
 - <http://www.01net.com/editorial/585979/barack-obama-peut-de-lancer-des-cyber-attaques-preventives/>

- **Le "Cybersecurity Order" du président**
 - <http://www.defense.gov/news/newsarticle.aspx?id=119286>

- **Loi CISPA: le retour**
 - <https://www.eff.org/deeplinks/2013/02/cispa-privacy-invading-cybersecurity-spying-bill-back-congress>

Actualité (anglo-saxonne)

- **Note pour plus tard: éviter les blagues sexistes aux USA**
 - **Exemple 1**
 - <http://www.theverge.com/2013/3/21/4132752/thug-mentality-how-two-dick-jokes-exploded-into-ddos-and-death-threats>
 - **Exemple 2**
 - <http://adainitiative.org/2013/02/keeping-it-on-topic-the-problem-with-discussing-sex-at-technical-conferences/>

Actualité (européenne)

■ Publications de l'ENISA

- Cloud vs. SCADA

- <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/critical-cloud-computing>

- Les cyberattaques

- <http://www.enisa.europa.eu/media/press-releases/enisa-flash-note-cyber-attacks>

■ Un nouveau projet de directive sur la sécurité informatique

- <http://www.donneespersonnelles.fr/un-nouveau-projet-de-directive-dangereux-sur-la-securite-informatique>

Actualité (européenne)

- **Les CNIL européennes vont se fâcher contre Google**
 - ... mais elles n'ont pas de pouvoir répressif
 - <http://www.lefigaro.fr/hightech/2013/02/18/01007-20130218ARTFIG00653-les-cnil-europeennes-vont-sevir-contre-google.php>

- **Google menacé de procès antitrust en Europe**
 - A cause des applications préinstallées avec Android
 - <http://www.engadget.com/2013/04/08/eu-antitrust-complaint-google-android/>

- **"Information Security Solutions Europe Conference" (ISSE)**
 - Organisée par l'ENISA
 - CFP: 30 avril
 - <http://www.enisa.europa.eu/media/news-items/isse-2013-call-for-contributions>

Actualité (européenne)

■ Les allemands accusent la Chine de pirater

- ...et ouvrent un département "anti piratage"
 - http://french.ruvr.ru/2013_03_24/Le-service-de-renseignement-allemand-ouvre-le-departement-danti-piratage/
- Réponse de la Chine: "l'occident justifie la mise en place de cyber-arsenaux"
 - <http://www.globaltimes.cn/content/764116.shtml>

■ ~~L'Islande~~ L'Europe veut bannir l'accès à la pornographie en ligne

- <http://www.dailymail.co.uk/news/article-2277769/Iceland-bid-ban-web-porn.html>
- <http://www.linformaticien.com/actualites/id/28337/internet-et-porno-la-censure-fait-rage.aspx>

■ La marque "Python" menacée en Europe

- Par une société UK
 - <http://pyfound.blogspot.fr/2013/02/python-trademark-at-risk-in-europe-we.html>

Actualité (Google)

■ Qui peut faire peur à Google ?

- Samsung !

- <http://arstechnica.com/gadgets/2013/02/report-google-thinks-it-created-a-monster-in-samsung/>

■ Samsung KNOX

- SELinux pour Android

- <http://www.samsung.com/uk/news/presskit/samsung-unveils-samsung-knox-for-secure-byod>

■ Google "forke" WebKit

- Et crée Blink

- <http://blog.chromium.org/2013/04/blink-rendering-engine-for-chromium.html>
- <https://plus.google.com/u/0/116560594978217291380/posts/AeCnq76cAXb>

■ Google va éteindre Google News

- Conséquence: de nombreux utilisateurs commencent à se méfier des services en ligne ...

Actualité (Google)

- **Des outils pour les webmasters piratés**
 - <http://www.google.com/webmasters/hacked/>

- **L'authentification à 2 facteurs contournée**
 - **Via l'API Android**
 - <http://www.h-online.com/security/news/item/Google-s-two-factor-authentication-bypassed-1811825.html>

- **"Cold Boot Attack" vs. Android**
 - **Nécessite que le bootloader ait été préalablement débloqué**
 - <https://www1.informatik.uni-erlangen.de/frost>

- **Google Play transmet les coordonnées complètes des clients aux développeurs d'applications**
 - <http://mashable.com/2013/02/13/google-play-app-developers-personal-information/>

Actualité (Apple)

■ iOS 6.1

- Corrige quelques failles ...
 - <http://support.apple.com/kb/HT5642>
- Retour du contournement de l'écran de verrouillage ...
 - <http://www.zdnet.com/apple-confirms-ios-6-1-lock-screen-flaw-promises-fix-7000011363/>
 - <http://nakedsecurity.sophos.com/2013/02/27/second-iphone-passcode-hack-vulnerability-discovered/>

■ Jailbreak "evasi0n"

- Une œuvre d'art
 - <http://evasi0n.com/>

■ iOS 6.1.3

- Corrige le jailbreak "evasi0n"

■ Mac OS 10.8.3

- Corrige quelques failles
 - <http://support.apple.com/kb/HT5612>

Actualité (Apple)

■ Mac OS X

- Les versions vulnérables de Flash Player bloquées
 - <https://isc.sans.edu/diary/Apple+Blocks+Older+Insecure+Versions+of+Flash+Player/15316>

■ Réinitialiser un mot de passe iCloud

- ... en connaissant uniquement la date de naissance
 - <http://arstechnica.com/security/2013/03/apple-suspends-password-resets-after-critical-account-hijack-bug-is-found/>

■ Pas de SSL sur l'AppStore avant Janvier 2013 (?!)

- <http://www.01net.com/editorial/588641/l-app-store-est-reste-vulnerable-pendant-des-mois-voire-des-annees/>

■ Apple va un peu trop loin dans le filtrage ...

- <http://www.cultofmac.com/217557/apples-deleting-icloud-emails-that-contain-the-phrase-barely-legal-teens/>

Actualité (crypto)

■ RC4 est cassé

- Attaque en 2^{24}
 - <http://blog.cryptographyengineering.com/2013/03/attack-of-week-rc4-is-kind-of-broken-in.html>
 - <http://eprint.iacr.org/2013/178>

■ MD5 est cassé (déjà connu)

- Attaque en 2^{47}
 - <http://eprint.iacr.org/2013/170.pdf>

■ SHA1 est cassé

- Attaque en $2^{57,5}$
 - <http://marc-stevens.nl/research/papers/EC13-S.pdf>
 - <https://lock.cmpxchg8b.com/shatter/visualize.html?stevens=1>

■ Extraction triviale de la clé HDCP

- <http://adamsblog.aperturelabs.com/2013/02/hdcp-is-dead-long-live-hdcp-peek-into.html>

■ Récupération des clés depuis le "secure chip" AT91SAM7XC

- La commande ERASE n'efface pas la RAM
 - <http://adamsblog.aperturelabs.com/2013/02/atmel-sam7xc-crypto-co-processor-key.html>

Actualité (crypto)

- **L'application Silent Text (de la société Silent Circle)**
 - Nouvelle création de Phil Zimmermann
 - <http://www.france24.com/fr/20130308-silent-text-application-amie-dissidents-criminels-silent-circle-cryptographie-censure-smartphone-ios-internet>

- **Thawte Crypto Challenge**
 - <https://www.cryptochallenge.com/>

- **Les produits ZoneCentral inscrits au catalogue de l'OTAN**
 - <http://www.ssi.gouv.fr/fr/menu/actualites/687.html>

- **Attaque crypto contre le plugin Bakery pour Drupal**
 - <http://heine.familiedeelstra.com/bakery-sso-from-bug-to-exploit>

■ Conférences passées

- RSA

- Adi Shamir

- "L'intérêt de la crypto diminue ... si les endpoints sont piratés"
 - "La meilleure solution pour éviter la fuite de données ... c'est d'avoir des fichiers énormes"
 - <http://magazine.qualys.fr/produits-technologies/cryptographie-shamir-obesite/>

- Où investir en sécurité informatique ?

- <http://www.mag-secur.com/News/tabid/62/articleType/ArticleView/articleId/29689/Le-futur-de-la-securite-informatique-vu-par-un-investisseur-en-capital-risque.aspx>

- CrowdStrike éteint un botnet sur scène

- <http://www.mag-secur.com/News/tabid/62/articleType/ArticleView/articleId/29688/Crowdstrike-fait-tomber-un-botnet-en-live.aspx>

Actualité

- **Black Hat EU 2013**
- **OSSIR / JSSI 2013**
- **GS Days 2013**
- **Insomnihack**
 - <http://www.insomnihack.ch/>
- **Résultat du concours de reverse**
 - (ouvert uniquement aux femmes)
 - <http://addxorrol.blogspot.fr/2013/03/congratulations-marion.html>

Actualité

- **CanSecWest 2013**
- **... et son ineffable "pwn2own"**
 - **Victimes: Chrome, IE, Firefox, Java, Flash**
 - <https://hg.mozilla.org/mozilla-central/rev/cddf5f75843f>
 - http://googlechromereleases.blogspot.ca/2013/03/stable-channel-update_7.html
 - **VUPEN star du concours**
 - **Personne ne s'attaque à Safari**

 - **Récap**
 - <http://h30499.www3.hp.com/t5/HP-Security-Research-Blog/Pwn2Own-2013/ba-p/5981157>
 - <http://h30499.www3.hp.com/t5/HP-Security-Research-Blog/Pwn2Own-2013-Recap/ba-p/5996085>

 - <http://www.esecurityplanet.com/browser-security/chrome-firefox-and-ie-fall-at-pwn2own-2013.html>
 - <http://labs.mwrinfosecurity.com/blog/2013/03/06/pwn2own-at-cansecwest-2013/>

Actualité

■ Conférences à venir

- **Etranger**

- **Recent Advances in Reverse Engineering**

- <http://rareconference.org/>

- **RAID 2013**

- **À Ste Lucie ☺**

- **Recon**

- <http://recon.cx/2013/index.html>

Actualité

- **France**
 - **SSTIC 2013**
 - <https://www.sstic.org/>
 - **Le challenge SSTIC ... trop facile cette année !**
 - <http://communaute.sstic.org/ChallengeSSTIC2013>
 - **NoSuchCon 2013**
 - <http://www.nosuchcon.org>
 - **HES "canal historique"**
 - <http://2013.hackitoergosum.org>
 - **HIP 2013**
 - <https://www.hackinparis.com/node/155>
 - **Nuit du Hack**
 - <http://www.nuitduhack.com/en/call-for-papers-nuit-du-hack>
 - **BotConf (CFP: 30/06)**
 - <https://www.botconf.eu/>

Actualité

■ Sorties logicielles

- **Kali (la suite de BackTrack)**
 - <http://www.kali.org/>
- **Nessus 5.0.3**
- **Digital Forensics Framework 1.3**
 - <http://www.digital-forensic.org/media/downloads/RELEASENOTES-1.3.txt>
- **Cyber Security Evaluation Tool (CSET)**
 - <http://ics-cert.us-cert.gov/satool.html>
- **Le code source de Photoshop 1.0 offert à un musée de l'informatique**
 - <http://www.computerhistory.org/adobe-ps-source/>

Actualité

■ Le manuel de la cyberguerre par l'OTAN

- "Il est légitime de tuer des hackers"
 - <http://www.theverge.com/2013/3/21/4130740/tallin-manual-on-the-international-law-applicable-to-cyber-warfare>

■ Etat de cyber-guerre en Corée du Sud

- Des chaînes de télé et des banques perturbées par un malware destructeur
 - <http://french.yonhapnews.co.kr/national/2013/03/20/0300000000AFR20130320003500884.HTM>

■ Le fournisseur de Cloud "2e2" fait faillite

- Les clients ont dû payer très cher pour récupérer leurs données ...
 - <http://www.droit-technologie.org/actuality-1577/cloud-la-perde-totale-des-donnees-est-possible-la-preuve-par-2e2-et.html>

■ Code.org

- Pour apprendre le code à l'école
- Soutenu par Bill Gates, Mark Zuckerberg, ...
 - <http://www.code.org/>

■ Opera abandonne Presto pour WebKit ?

- <http://my.opera.com/haavard/blog/2013/02/13/webkit>

Actualité

■ ZeroBay

- Une nouvelle plateforme de trading pour exploits
 - <http://zerobay.co.uk/>

■ BugCrowd

- "Crowdsourcer" ses "audits" de produits
 - <http://bugcrowd.com/faq/>

■ IBM X-Force Trend & Risk Report 2012

- <http://blogs.iss.net/archive/2012-XFTR-EOY.html>

■ Un système de lutte contre les cyberattaques en Russie

- http://french.ruvr.ru/2013_02_14/Creer-un-systeme-uni-pour-lutter-contre-les-cyberattaques-Poutine/

Actualité

- **La gestion des DRM en ligne, ça ne fonctionne toujours pas**
 - Exemple avec SimCity
 - <http://www.20minutes.fr/high-tech/1114973-20130308-simcity-nouveau-fiasco-drm>

- **Journée de la libération des documents**
 - 27 mars 2013
 - <http://www.april.org/journee-de-liberation-des-documents-le-27-mars-2013>

- **Toute résistance est futile**
 - Préparez vous à l'assimilation
 - http://www.huffingtonpost.com/2013/03/06/facebook-privacy-study-carnegie-mellon-university_n_2823535.html

- **Nokia Bug Bounty**
 - <http://www.nokia.com/global/security/security/>

- **Le gouvernement japonais organise son premier concours de "hacking"**
 - <http://www.bulletins-electroniques.com/actualites/72176.htm>

Actualité

■ HP Moonshot

- Le "Raspberry Pi" du datacenter
 - <http://cloudcomputing.sys-con.com/node/2608549>

■ Yahoo! envisage de racheter DailyMotion

- <http://www.20minutes.fr/economie/1121877-20130320-yahoo-pourrait-racheter-75-dailymotion>

■ Yahoo! a déjà racheté une application Android à un étudiant

- ... plusieurs millions !
 - <http://www.bbc.co.uk/news/technology-21924243>

■ Le 1^{er} avril cette année

- **Google arrête YouTube**
 - http://news.cnet.com/8301-1023_3-57577172-93/google-declares-end-of-youtube-in-april-fools-prank/
- **Google Nose**
- **Google Treasure Map**
 - <https://maps.google.com/treasure>
- **La mamie du Cantal va recevoir son courrier par drone**
 - <http://www.laposte.fr/legroupe/Actualites/Le-groupe-La-Poste-va-tester-avec-Parrot-la-livraison-de-la-presse-quotidienne-par-Drone>
- **Programme de rêve pour NoSuchCon**
 - <http://sid.rstack.org/blog/images/billets/585/nsc-aprilfool2013.jpg>
- **Les blagues Carambar vont disparaître**
- ...
 - <http://money.cnn.com/2013/04/01/news/april-fools/index.html>

Divers

- **"echo.c" dans toutes les versions d'Unix**
 - <https://gist.github.com/dchest/1091803>
- **Un Bomberman multi joueurs qui accepte 1000 participants**
 - <http://bombermine.com/>
- **Worms en HTML5**
 - <http://ciaranmccann.me/wormsjs/>
- **Créer un comic XKCD-like depuis une interface HTML5**
 - <http://cmx.io/>
- **La MMU d'Intel est Turing-complete**
 - <https://github.com/jbangert/trapcc>
- **Belle démo(s) HTML5/JS**
 - <http://codepen.io/stuffit/pen/KrAwX>
 - <http://www.extremetech.com/gaming/151900-unreal-engine-3-ported-to-javascript-and-webgl-works-in-any-modern-browser>

Divers

- **Le code source du premier compilateur C sur PDP-11**
 - Retrouvé sur une bande de sauvegarde !
 - <http://cm.bell-labs.com/cm/cs/who/dmr/primevalC.html>

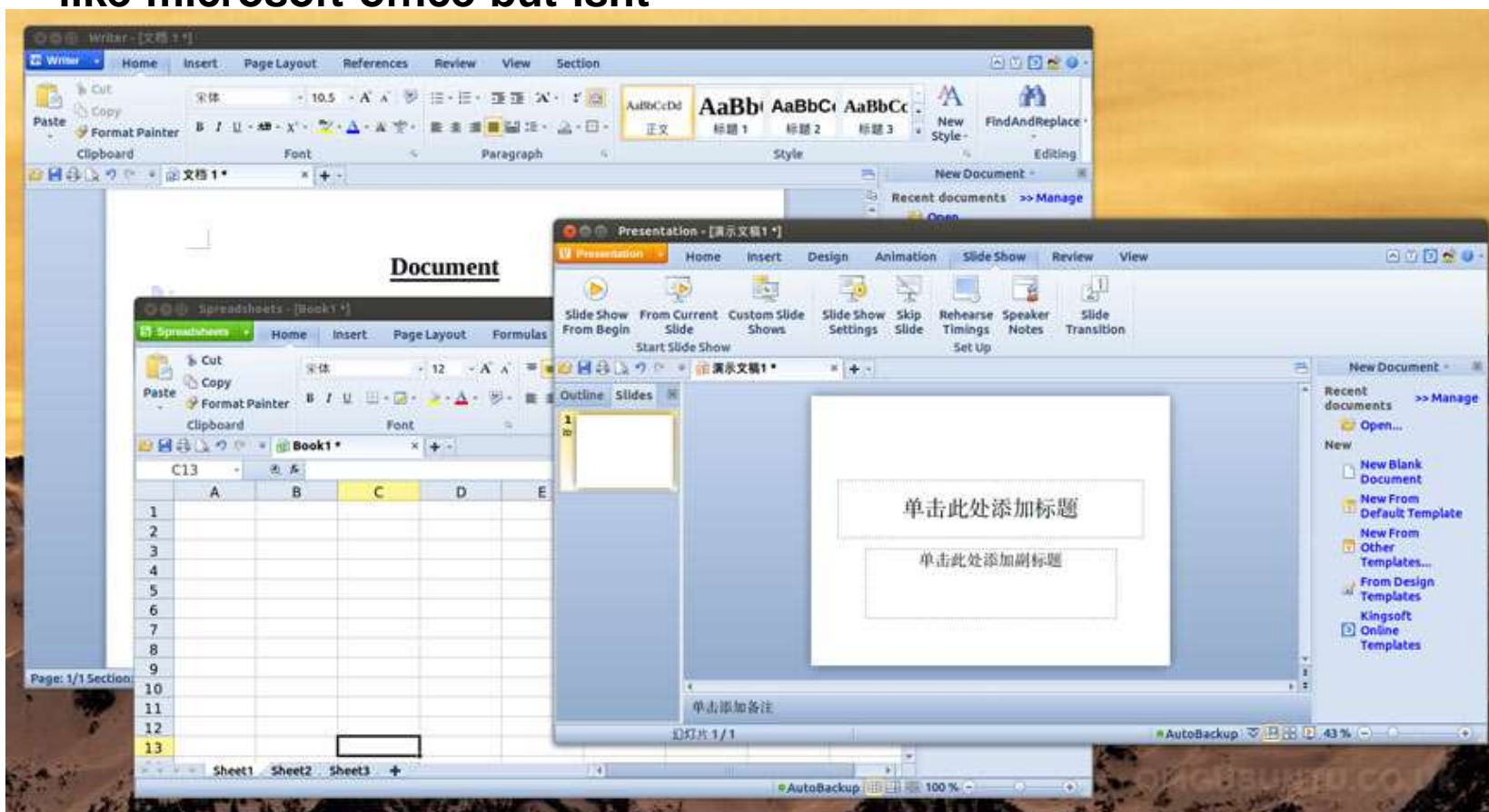
- **Un prison piratée de l'intérieur**
 - Le prof d'informatique ... était détenu pour hacking
 - <http://www.gizmodo.fr/2013/03/05/prison-hacker-informatique.html>

- **L'ADE 651**
 - Un détecteur de balles de golf
 - http://www.lepoint.fr/insolite/angleterre-cet-escroc-la-c-est-de-la-balle-08-03-2013-1637757_48.php

Divers

■ Office sur Ubuntu

- <http://www.omgubuntu.co.uk/2013/03/wps-office-for-linux-looks-like-microsoft-office-but-isnt>



Divers

■ Source

– <https://products.butterflylabs.com/>

The Bitforce line of ASIC Super Computer (SC) bitcoin miners are next generation bitcoin mining hardware available in 4 different configurations.

5 GH/S BITCOIN MINER



\$274.00

Order Now

25 GH/S BITCOIN MINER



\$1,249.00

Order Now

50 GH/S BITCOIN MINER



\$2,499.00

Order Now

1,500 GH/S BITCOIN MINER



Out of stock

Divers

■ Source

- <https://twitter.com/jonoberheide/status/302238650454900736/photo/1>



Divers

■ Source

- <http://acidcow.com/pics/44293-external-battery-from-china-5-pics.html>



Divers

■ Source

- <http://acidcow.com/pics/42981-chinese-walnuts-5-pics.html>



■ Source

- http://www.pvv.org/~oma/DeepC_Scandev_Mar2013.pdf

Exercise

What do you think this code snippet might print if you compile, link and run it in your development environment?

foo.c

```
#include <stdio.h>

int main(void)
{
    int v[] = {0,2,4,6,8};
    int i = 1;
    int n = i + v[++i] + v[++i];
    printf("%d\n", n);
}
```

Questions / réponses

- Questions / réponses
- Prochaine réunion
 - Mardi 14 mai 2013