
OSSIR
Groupe Paris
Réunion du 10 février 2009



Revue des dernières vulnérabilités



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

Avis Microsoft (1/3)

■ Correctifs de Janvier 2009

- Avec [*exploitability index*]
- MS09-001 failles SMB (x3) [3/3/3]
 - Affecte: Windows (toutes versions supportées)
 - Exploit: déni de service
 - Un code est disponible sur milw0rm
 - Exécution de code à distance possible, mais très difficile
 - Crédit: anonyme / ZDI
 - <http://blogs.technet.com/swi/archive/2009/01/09/ms09-001-prioritizing-the-deployment-of-the-smb-bulletin.aspx>
 - Note : le redémarrage n'est pas nécessaire sous Vista/2008

Avis Microsoft (2/3)

■ A noter également

- Mises à jour WSUS
 - <http://support.microsoft.com/kb/894199>
- Mises à jour "non sécurité"
 - <http://technet.microsoft.com/en-us/wsus/bb466214.aspx>

■ Advisories

■ Prévisions pour Mars 2009

- 4 patches
 - Internet Explorer 7, critique
 - Exchange (toutes versions), critique
 - SQL (toutes versions, y compris MSDE, sauf 2008), important
 - Visio (toutes versions), important

Avis Microsoft (3/3)

■ Révisions

- **MS05-022**
 - Version 2.0 : il n'est plus possible de télécharger une version de MSN 6.2 boguée
- **MS08-037**
 - Version 2.3 : mise à jour de la FAQ
- **MS08-040**
 - Version 1.7 : MSDE 2000 SP3a n'est pas affecté
- **MS08-066**
 - Version 1.1 : mise à jour de la FAQ
- **MS08-072**
 - Version 2.0 : Word Viewer est affecté
- **MS08-076**
 - Version 3.0 : remplacement du patch pour la version 9.5 / Windows XP

Infos Microsoft (1/6)

■ Sorties logicielles

- **Vista SP2 repoussé à mai 2009, au mieux**
 - <http://www.techarp.com/showarticle.aspx?artno=604&pgno=0>
- **Sur Microsoft Update ...**
 - SQL Server 2005 SP3
 - .NET Framework 3.5 SP1
- **En téléchargement ...**
 - IE 8 RC1
 - IEAK 8 Beta
 - OCS 2007 R2

Infos Microsoft (2/6)

- **Office Live**
 - Travailler à plusieurs *simultanément* sur un document Office !
 - <http://workspace.officelive.com/>
- **Prévu pour fusionner avec Windows Live**
 - Projet "Kumo"
 - <http://www.guwiv.com/portal/blogs/news/archive/2009/01/27/officiel-microsoft-va-fusionner-office-live-et-windows-live.aspx>
- **La bataille navale en réseau sous Excel**
 - <http://blogs.microsoft.fr/franckha/archive/2008/12/02/65249.aspx>

Infos Microsoft (3/6)

■ Autre

- **Le laboratoire commun Microsoft / INRIA présente ses premiers résultats**
 - <http://www.reseaux-telecoms.net/actualites/lire-le-laboratoire-microsoft-inria-devoile-sept-projets-orientes-informatique-scientifique-et-securite-19439.html>
- **Fin de support pour Windows 2003 SP1**
 - Avril 2009
- **Du POP3 sur Hotmail**
- **Nouvelle version des documents de spécifications, incluant Windows Seven**
 - [http://msdn.microsoft.com/en-us/library/cc216517\(PROT.10\).aspx](http://msdn.microsoft.com/en-us/library/cc216517(PROT.10).aspx)
- **Plus de 1600 bogues dans la documentation Microsoft**
 - Et ça augmente !
 - http://www.infoworld.com/article/09/01/22/Bugs_in_Microsoft_tech_documentation_continue_to_rise_1.html

Infos Microsoft (4/6)

- **Matt Pietrek passe dans l'équipe Hyper-V**
 - http://blogs.msdn.com/matt_pietrek/archive/2009/01/09/fast-forward-catching-up-on-what-i-m-up-to.aspx
- **Mike Reavey devient patron du MSRC**
 - http://www.cio.com/article/477472/Microsoft_Security_Response_Center_Gets_New_Boss

Infos Microsoft (5/6)

■ Windows Seven

- **Il y aura 5 versions: Starter, Home Premium, Pro, Enterprise, Ultimate**
 - Plus la version Home Basic pour les pays "émergents"
 - Version Starter : pas plus de 3 applications simultanées
 - <http://tech.slashdot.org/article.pl?sid=09/02/09/1348255>
 - Version Ultimate : plus "d'extras"
 - <http://arstechnica.com/microsoft/news/2009/02/microsoft-no-ultimate-extras-for-windows-7.ars>
- **Plus d'Outlook Express ni de Windows Mail dans Windows Seven**
 - Au temps pour CoStartOutlookExpress
 - <http://blogs.msdn.com/cjacks/archive/2009/01/20/deprecation-of-windows-mail-on-windows-7-and-the-mystery-of-costartoutlookexpress.aspx>

Infos Microsoft (6/6)

- **Changements apportés à UAC dans Windows Seven**
 - <http://www.istartedsomething.com/20090130/uac-security-flaw-windows-7-beta-proof/>
 - <http://www.istartedsomething.com/20090131/microsoft-dismisses-windows-7-uac-security-flaw-insists-by-design/>
- **De Windows 1.0 à Windows Seven en images**
 - <http://www.zdnet.fr/galerie-image/0,50018840,39385546,00.htm>
 - <http://vidberg.blog.lemonde.fr/2009/01/24/quel-ordinateur-acheter-en-2009/>

Infos Réseau

■ Cisco

- Une belle faille dans Cisco Security Manager
 - Arrêt 'root' sur un port TCP non fermé après la déconnexion d'un client
 - <http://www.cisco.com/warp/public/707/cisco-sa-20090121-csm.shtml>
- Faille(s) dans IronPort
- "Déni de service" via un paquet VTP maformé
- "Déni de service" sur Cisco ONS (commutateur optique)
- "Déni de service" sur Cisco Unified Communications Manager
 - <http://www.cisco.com/warp/public/707/cisco-sa-20090121-cucmcapf.shtml>
- Failles dans WiSM, WLC, ...
 - <http://www.cisco.com/warp/public/707/cisco-sa-20090204-wlc.shtml>
- (...)

■ Cisco sur le marché des serveurs ?

- http://blogs.cisco.com/news/comments/introducing_unified_computing_to_the_data_center/

■ Rapport de l'ICANN sur le *fast-flux*

- <http://gns0.icann.org/issues/fast-flux-hosting/fast-flux-initial-report-26jan09.pdf>

■ Actualité

- Qt passe en LGPL
 - <http://rcecafe.net/?p=45>
- "As far as I'm concerned, digital cameras have been more useful than kernel dumps to kernel debugging" – Linus Torvalds
 - <http://lwn.net/Articles/314769/>
- Debian 5 pour la St Valentin ☺
 - http://www.silicon.fr/fr/news/2009/02/03/linux___la_prochaine_debian_sera_lancee_pour_la_saint_valentin

■ Failles

- Les syscalls n'ont pas les mêmes numéros dans Linux x86 et Linux x86_64
 - Mais il est possible de faire un syscall32 depuis une application 64 bits et réciproquement
 - Permet de contourner les filtrages par syscalls
 - <http://scary.beasts.org/security/CESA-2009-001.html>
- Failles multiples dans Typo3
 - <http://typo3.org/teams/security/security-bulletins/typo3-sa-2009-001/>
 - Attention, le correctif initial introduit des régressions !
- Des plugins SquirrelMail backdoorés
 - <http://www.squirrelmail.org/>

Infos Unix

- **Faille Solaris #1**
 - Affecte: Solaris 8, 9,10
 - Exploit:
 - Elévation de privilèges locale via "AutoFS"
 - <http://sunsolve.sun.com/search/document.do?assetkey=1-66-249966-1>
- **Faille Solaris #2**
 - Affecte: Solaris 9, 10
 - Exploit:
 - Déni de service à distance dans le démon IKE
 - <http://sunsolve.sun.com/search/document.do?assetkey=1-66-247406-1>
- **Faille HP/UX**
 - Affecte : HP/UX 11
 - Exploit : déni de service via IPv6
 - <http://itrc.hp.com/service/cki/docDisplay.do?docId=c01662367>
- **Faille AIX**
 - Affecte: AIX 5 et 6
 - Exploit: élévation de privilèges via les commandes rmssock/rmssock64

Failles

■ Principales applications

- Failles dans:
 - Firefox < 3.0.6
 - QuickTime 7.6.x (7 failles)
 - <http://support.apple.com/kb/HT3403>
 - <http://support.apple.com/kb/HT3404>
- Faille dans VNC Viewer <= 4.1.2
 - <http://www.realvnc.com/pipermail/vnc-list/2008-November/059432.html>
- "Directory Traversal" dans le support Bluetooth/ObexFTP
 - Affecte : Windows Mobile 5 et 6
 - <http://www.securityfocus.com/bid/33359/info>

Failles

- **Lecture de fichiers arbitraires avec Safari**
 - <http://brian.mastenbrook.net/display/27>
- **Faille dans FFmpeg**
 - **Affecte : tous les logiciels basés sur libffmpeg (plusieurs dizaines)**
 - <http://ffmpeg.mplayerhq.hu/projects.html>
 - **Exploit : fichier ".4xm" malformé**
- **Failles multiples dans le système "e-terrahabitat" d'AREVA**
 - **Un système SCADA**
 - <http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-052/CERTA-2009-AVI-052.html>
 - http://www.theregister.co.uk/2009/02/05/areva_scada_security_bugs/

Failles

- **Oracle + PHP = le meilleur de 2 mondes ...**
 - **Bienvenue dans les années 90 !**
 - <http://labs.odefense.com/intelligence/vulnerabilities/display.php?id=768>
 - <http://labs.odefense.com/intelligence/vulnerabilities/display.php?id=769>
 - <http://www.zerodayinitiative.com/advisories/ZDI-09-003/>
 - (...)

- **Visiblement quelqu'un a découvert qu'il y avait des *parsers* dans un BES ...**
 - <http://labs.odefense.com/intelligence/vulnerabilities/display.php?id=764>
 - <http://labs.odefense.com/intelligence/vulnerabilities/display.php?id=765>
 - <http://labs.odefense.com/intelligence/vulnerabilities/display.php?id=766>
 - (...)

- **OpenOffice 3 installe une ancienne version de Java**
 - http://voices.washingtonpost.com/securityfix/2009/02/openoffice_installs_insecure_j.html?wprss=securityfix

- **Le TOP 25 du MITRE**
 - <http://cwe.mitre.org/top25/>

Malwares et spam

■ Ver Conficker/Downadup

- Plusieurs millions de machines sous contrôle
 - (Estimation basée sur la prise de contrôle d'un nom de domaine)
 - <http://www.f-secure.com/weblog/archives/00001579.html>

■ AUTORUN.INF n'est pas forcément un fichier texte

- <http://www.f-secure.com/weblog/archives/00001575.html>

■ Un patch à appliquer ...

- <http://support.microsoft.com/kb/953252>

Malwares et spam

- **Un nouveau site dédié à l'anti-malware**
 - <http://www.attackresearch.com/>
- **Entrevue avec un auteur d'Adware**
 - **Programmé en ... Scheme ...**
 - <http://philosecurity.org/2009/01/12/interview-with-an-adware-author>
- **Des félicitations pour Microsoft Windows Defender !**
 - <http://mad.internetpol.fr/archives/8-Zlob-Best-Wishes-With-A-Hidden-Message.html>
- **Kaspersky USA victime d'une injection SQL**
 - <http://hackersblog.org/2009/02/07/usakasperskycom-hacked-full-database-acces-sql-injection/>

Malwares et spam

- **Le mal est partout ...**
 - **Infecté via un prospectus publicitaire !**
 - <http://isc.sans.org/diary.html?storyid=5797>

- **Un outil de création de malware: BitTera.C**
 - **Gratuit !**
 - http://www.secuobs.com/news/09022009-bittera_creation_automatique_virus.shtml

- **McAfee: "le vol de données coûte 1000 milliards de dollars"**
 - http://www.silicon.fr/fr/news/2009/01/29/mcafee___le_vol_de_donnees_cout_eraut_1_trillion_de_dollars

- **Les logiciels anti malware font-ils plus de mal que de bien ?**
 - **+2369% de délai sur les performances disque ...**
 - <http://www.codinghorror.com/blog/archives/000803.html>

Malwares et spam

- **L'élection américaine déchaîne le malware**
 - Google Bombing
 - my.barackobama.com utilisé pour héberger du malware
 - ...

- **Les prévisions de McAfee pour 2009**
 - Abus du Cloud Computing
 - Attaques traduites en plusieurs langues
 - Infection par des cartes mémoire
 - Malvertising
 - Coopération internationale accrue
 - http://www.mcafee.com/us/local_content/reports/2009_threat_predictions_report.pdf

- **Un cheval de Troie dans des versions piratées d'iWork09 (Mac OS X)**
 - Techniquement avancé (P2P, chiffrement réseau ...)
 - http://vil.mcafeesecurity.com/vil/content/v_153893.htm
 - <http://isc.sans.org/diary.html?storyid=5743>

- **Peut-on être consultant en sécurité et gérer un botnet de 250k machines ?**
 - http://www.theregister.co.uk/2009/01/23/botmaster_sentencing_kerfuffle/

Failles 2.0

- **DDoS basé sur DNS**
 - Cibles: NetworkSolutions, ...
 - Globalement peu efficace (faible amplification)
 - <http://isc.sans.org/diary.html?storyid=5713>
 - <http://isc.sans.org/diary.html?storyid=5740>

- **Un campagne de DDoS triviale, basée sur GET /**
 - Sites visés: Milw0rm, PacketStorm, Metasploit, Immunity, ...

- **Se protéger contre les "cold boot" attacks**
 - En stockant la clé dans un cache du processeur
 - http://www.intelligence-economique.gouv.fr/article.php3?id_article=374

- **phpbb.com piraté**
 - Ils avaient oublié d'appliquer un patch pour l'addon PHPList ...
 - <http://hackedphpbb.blogspot.com/>
 - Une analyse statistique des mots de passe
 - http://www.darkreading.com/blog/archives/2009/02/phpbb_password.html

Failles 2.0

■ "In-session phishing"

- Principe (simplifié) : faire apparaître une pop-up d'authentification au moment où l'utilisateur se connecte à un site "intéressant"
 - <http://www.trusteer.com/files/In-session-phishing-advisory-2.pdf>

■ "Mem-Jacking"

- Pour résumer : memdump / strings (*sic*)
 - <http://packetstormsecurity.org/papers/attack/mem-jacking.pdf>

■ La fuite des données ultime

- Quand le cœur du système de paiement lui-même est compromis ...
 - http://voices.washingtonpost.com/securityfix/2009/01/payment_processor_breach_may_b.html

■ 9 millions de dollars détournés dans 49 villes américaines

- Via de "fausses cartes" issues du *hack* précédent
 - <http://www.foxnews.com/story/0,2933,487184,00.html>

Actualité (France)

■ Amen passe à l'IPv6

- <http://www.itrmanager.com/articles/86046/amen-passe-ipv6.html>

■ Free vs . Phishing

- Mais comment font-ils ?

- <http://www.freenews.fr/nat/6432-societe-phishing-quand-free-replique.html>

■ Nerim compromis

- Exemple de sites défacés

- <http://lolassoc.nerim.net/> <http://gbbeaucourt.nerim.net/>
<http://www.insidix.com/> ...

■ Zataz condamné pour divulgation de faille

- Un fichier sensible indexé dans Google (!)

- <http://www.zataz.com/news/18456/jugement--zataz.html>

Actualité (France)

- **Plusieurs réseaux militaires victimes d'un ver informatique**
 - **Conficker ?**
 - http://www.ouest-france.fr/ofdernmin_-La-Marine-nationale-victime-d-une-intrusion-informatique_-803619--BKN_actu.Htm
 - <http://fr.news.yahoo.com/12/20090206/ttc-les-reseaux-informatiques-de-l-armee-549fc7d.html>

- **Un internaute profilé au hasard ...**
 - <http://www.le-tigre.net/Marc-L.html>

- **La loi "Création et Internet" votée en mars ?**
 - **"Je n'ai pas été élu pour laisser voler au supermarché"**
 - <http://www.itrmanager.com/articles/86944/loi-antipiratage-internet-sera-adoptee-ici-fin-mars.html>
 - **La défense de Christine Albanel**
 - http://www.degrouppnews.com/actualite/n2963-christine_albanel-riposte_graduee-hadopi-senat-telechargement.html

Actualité (France)

■ Un phishing en français sur Facebook

- <http://pandalabs.pandasecurity.com/archive/Facebook-Phishing-Site-Targets-French-Users.aspx>

■ L'interview vérité

- "Tout le monde a intérêt à transformer Internet en Minitel"
 - <http://www.ecrans.fr/Tout-le-monde-a-interet-a,5762.html>

■ Quand les ministres donnent l'exemple

- <http://fr.news.yahoo.com/63/20090203/tod-la-ministre-du-numrique-ne-peut-pas-366b5ef.html>

Actualité (anglo-saxonne)

- **Barack Obama**
 - "Jamais sans mon BlackBerry"

- **Steve Jobs n'est pas mort**
 - <http://blog.wired.com/business/2009/01/wiredcom-imagev.html>

- **Le FBI craint le "Cyber Armageddon"**
 - http://www.silicon.fr/fr/news/2009/01/07/le_fbi_previent_de_la_venue_prochaine_du__cyber_armageddon_

- **£10,000 pour retrouver l'auteur d'un DDoS**
 - <http://news.zdnet.co.uk/security/0,1000000189,39599492,00.htm>

- **Brevets logiciels : ça ne s'arrange pas**
 - <http://www.cato-at-liberty.org/2009/01/17/patent-trolls-are-a-symptom-of-deeper-problems/>
 - **Ex. IBM brevète la fonction strip()**
 - <http://techdirt.com/articles/20090108/0230453331.shtml>

Actualité (anglo-saxonne)

■ Apple

- Plus de DRM sur iTunes - mais l'adresse email reste dans le fichier téléchargé
 - <http://crave.cnet.co.uk/digitalmusic/0,39029432,49300555,00.htm>

■ Intel, Microsoft, Google ... licencient

- Tous les services Google non rentables sont fermés
- Seul Apple s'en sort bien
 - <http://www.itrmanager.com/articles/86598/resultats-2008-intel-microsoft-google-br-licenciements-arret-projets.html>

■ 25 M\$ pour un centre d'entrainement en cyber-sécurité

- Financement DARPA
 - http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/DARPA010909.xml

■ Le MI5 veut écouter la VoIP

- <http://www.vnunet.com/computing/news/2233556/mi5-chief-concerned-web-phone>

Actualité (anglo-saxonne)

■ Une bombe logique chez Fanny Mae

- Prévue pour se déclencher le 31 janvier 2009
- Détectée par accident ...
 - http://www.informationweek.com/news/security/management/showArticle.jhtml?articleID=212903521&cid=nl_IWK_daily_H

■ Le "War Passport Cloning"

- http://www.theregister.co.uk/2009/02/02/low_cost_rfid_cloner/

Actualité (anglo-saxonne)

- **Le DoJ réalise un test de phishing "grandeur nature"**
 - <http://www.01net.com/editorial/402178/le-ministere-de-la-justice-americain-coupable-de-phishing/>

- **Une fuite de données pas banale**
 - Lecteur MP3 volé => eBay => Nouvelle-Zélande => fichier militaire
 - <http://isc.sans.org/diary.html?storyid=5761>
 - <http://tvnz.co.nz/view/page/413551/2453415>

- **Le guide du NIST pour la protection des données personnelles**
 - <http://csrc.nist.gov/publications/drafts/800-122/Draft-SP800-122.pdf>

Actualité (Google)

- **Chrome 2.0 en "pre-Beta"**
 - <http://googlesystem.blogspot.com/2009/01/google-chrome-20-pre-beta.html>

- **Le "bug"**
 - Quelques dizaines de minutes, mais des millions de commentaires ...
 - <http://googleblog.blogspot.com/2009/01/this-site-may-harm-your-computer-on.html>

- **Des responsables de Google Europe en prison**
 - Arrêtés en Italie pour violation de vie privée
 - https://www.privacyassociation.org/index.php?option=com_content&task=view&id=1745&Itemid=228

- **Google Latitude**
 - Pour localiser "vos amis"
 - <http://www.google.com/latitude/>

Actualité (Google)

■ Le plan pour éliminer Google

- La conjuration Microsoft et AT&T
- A lire au second degré
 - http://www.wired.com/techbiz/it/magazine/17-02/ff_killgoogle

■ Google doit faire des économies

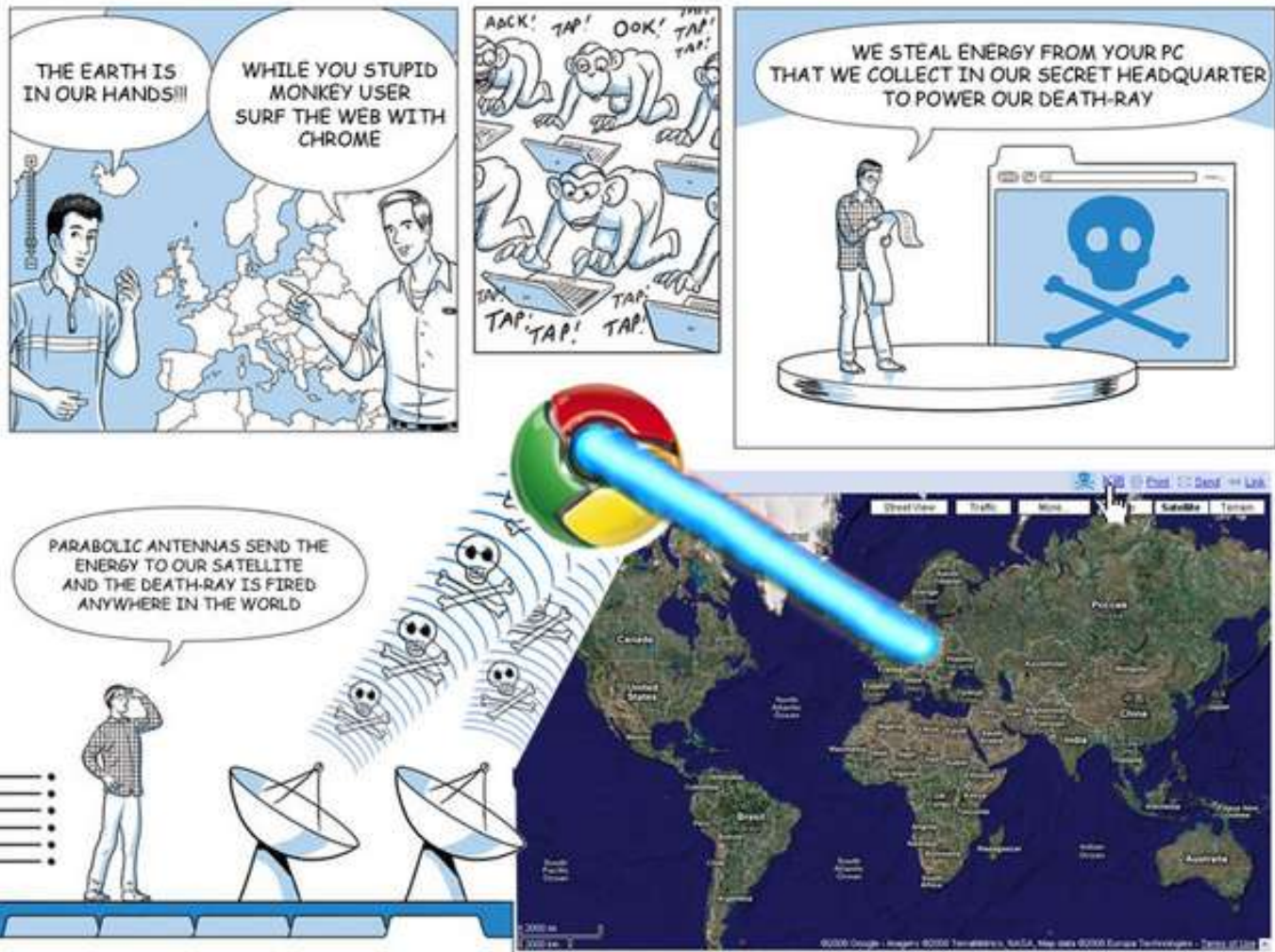
- http://money.cnn.com/galleries/2009/fortune/0901/gallery.google_perks.fortune/index.html

■ L'empreinte écologique de Google fait débat

- <http://www.fluctuat.net/blog/15563-Empreinte-ecologique-de-Google-bis-bouilloires-electriques-vs-machines-a-laver>

Actualité (Google)

■ Pour résumer ...



Actualité

- **Le problème avec les DRM ...**
 - **C'est quand l'éditeur de la solution ferme !**
 - <http://www.actualitte.com/actualite/7209-ebooks-DRM-fichiers-illisibles-remplacement.htm>
 - **Ou quand le certificat expire !**
 - cf. jeu "Gears of War" sur PC ...

- **La base de données Monster.com part dans la nature**
 - **... une deuxième fois**
 - http://www.readwriteweb.com/archives/monstercom_loses_user_data_aga.php

- **Piratage de la banque Sumitomo**
 - **Un keylogger physique réussit (presque) à détourner 240 millions d'euros**
 - <http://www.zataz.com/news/18437/Sumitomo-Mitsui-bank--spy--keylogger.html>
 - http://www.pcworld.com/businesscenter/article/158285/how_the_sumitomo_bank_hackers_failed.html

Actualité

■ "Open WiFi is for terrorists"

- Résultat : les policiers indiens patrouillent les rues avec Kismet !

– <http://blog.wired.com/defense/2009/01/open-wi-fi-is-f.html>

■ L'armée allemande monte une armée de hackers

– <http://tech.slashdot.org/article.pl?sid=09/02/08/2246251>

Actualité

■ Le TCG normalise le chiffrement des disques durs

- Nom de code "Opal"

- http://www.vnunet.fr/news/une_norme_unique_de_chiffrement_pour_les_disques_durs_va_voir_le_jour-2030017

■ La biométrie par les veines du doigt

- http://www.silicon.fr/fr/news/2009/02/02/biometrie_sony_devoile_sa_technologie_basee_sur_les_veines_du_doigt

■ Qui est l'ennemi ?

- "L'employé dangereux est paresseux, fainéant, angoissé, créateur de rumeurs et il est terriblement ambitieux"

- <http://www.zataz.com/news/18461/profil--pirate--entreprise.html>

- Une étude Clavister

■ 1 recherche sur Google

- = 2 à 10g de CO₂ = 1 tasse de thé
 - <http://www.fluctuat.net/blog/15388-Empreinte-ecologique-2-recherches-Google-1-tasse-de-the-bien-chaud->
- 0,2g d'après Google
 - <http://googleblog.blogspot.com/2009/01/powering-google-search.html>

■ Google Maps tue un faon

- http://www.lepost.fr/article/2009/01/29/1405318_internet-google-map-a-tue-une-biche.html

- **Bill Gates lâche une horde de moustiques dans une conférence**
 - Pour sensibiliser au problème du paludisme ...
 - <http://science.slashdot.org/article.pl?sid=09/02/05/1320208&from=rss>

- **Linus Torvalds fan de ... Microsoft SongSmith**
 - <http://www.pcinpact.com/actu/news/48857-microsoft-songmith-fan-linus-trovalds.htm>

- **L'entropie de la désintégration particulaire affectée par la distance terre-soleil**
 - Rien n'est parfaitement aléatoire en ce bas monde ...
 - <http://superconductor.voltage.com/2009/02/hardware-randomnumber-is-harder-that-you-might-think.html>

Fun

- **Le danger des mises à jour automatiques par Internet**
 - 2 lecteurs de DVD de salon "briqués" !
 - http://www.cerias.purdue.edu/site/blog/post/customer_disservice/

- **Les zombies attaquent**
 - <http://io9.com/5142117/hackers-warn-texas-of-coming-zombie-war>

- **Les *codebreakers* de demain**
 - <http://www.nsa.gov/kids/>

Questions / réponses

- Questions / réponses
- Prochaine réunion
 - Mardi 10 mars 2009
- JSSI 2009 le 17 mars 2009
 - <http://www.ossir.org/jssi/>
- N'hésitez pas à proposer des sujets et des salles