
OSSIR
Groupe Paris
Réunion du 14 octobre 2008



Revue des dernières vulnérabilités



EdelWeb

Olivier REVENU
olivier.revenu (à) edelweb.fr

Mickaël DEWAELE
mickael.dewaele (à) edelweb.fr

Jérémy LEBOURDAIS
jeremy.lebourdais (à) edelweb.fr



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

Avis Microsoft (1/7)

■ Correctifs de Septembre 2008

- **MS08-052 Failles dans GDI+ (x5)**

- **Affecte** : tout logiciel utilisant "gdiplus.dll" / "vgx.dll"

- La liste est longue ...

- **Exploit(s)** :

- Corruptions mémoire variées

- Formats concernés: VML, EMF, GIF, WMF, BMP

- **Crédit** :

- Greg MacManus / VeriSign iDefense Labs

- Bing Liu / FortiGuard Global Security Research Team

- Peter Winter-Smith / NGSSoftware & Ivan Fratric / ZDI

- Assurent Secure Technologies

- Anonymous / ZDI

- **Voir aussi** :

- <http://blogs.technet.com/swi/archive/2008/09/09/ms08-052-explaining-the-windows-side-by-side-cache.aspx>

Avis Microsoft (2/7)

- **MS08-053 Faille dans Windows Media Encoder 9**
 - Affecte : WMEX.DLL
 - Accessible à travers des ActiveX marqués "safe for scripting"
 - Exploit(s) : "buffer overflow"
 - Crédit :
 - Nguyen Minh Duc & Le Manh Tung / Bach Khoa Internetwork Security Center (BKIS) Hanoi University of Technology
- **MS08-054 Vulnérabilité dans Windows Media Player**
 - Affecte : Windows Media Player 11 (toutes versions supportées)
 - Exploit(s) :
 - Faille dans le support SSPL (Server Side PlayList) dans un flux RSTP
 - Crédit : n/d
- **MS08-055 Vulnérabilité dans Office**
 - Affecte : OneNote
 - Office XP SP3, Office 2003 SP2/SP3, Office 2007 SP0/SP1
 - Exploit(s) :
 - Lien "onenote://" malformé permettant l'exécution de commandes
 - "Buffer overflow" (non exploitable sans OneNote)
 - Crédit : Brett Moore / Insomnia Security
 - Voir aussi :
 - <http://blogs.technet.com/swi/archive/2008/09/09/ms08-055-microsoft-security-response-process-behind-the-scenes.aspx>

Avis Microsoft (3/7)

■ Voir également:

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

■ Prévisions pour Octobre 2008

- Bulletins critiques / exécution de code
 - Active Directory (Windows 2000 SP4)
 - IE (toutes versions supportées)
 - Host Integration Server (toutes versions supportées)
 - Excel (toutes versions supportées, y compris Mac et SharePoint)

Avis Microsoft (4/7)

- **Bulletins importants / élévation de privilèges**
 - Windows XP et 2003 (toutes versions supportées)
 - (2x) Windows (toutes versions supportées)
- **Bulletins importants / exécution de code**
 - (2x) Windows (toutes versions supportées)
 - Windows 2000 SP4
- **Bulletin modéré / exécution de code**
 - Office XP SP3

Avis Microsoft (5/7)

■ D'après le CERTA

- Correction d'une faille (non exploitable) sur OLE32.DLL datant de mars 2007
- Correction d'une faille (non exploitable) dans PowerPoint XP et 2003 datant d'octobre 2006
- Mise à jour sur la faille "null.htw" (Q328832)

■ Advisories

- Q951306
 - Publication d'un code d'exploitation pour le "Token Kidnapping"

Avis Microsoft (6/7)

■ Révisions

- **MS07-047**
 - Version 2.1 : WMP9 sur Windows XP SP3 n'est pas affecté
- **MS08-009**
 - Version 1.2 : précision sur le fait que des versions non vulnérables se voient proposer la mise à jour
- **MS08-012**
 - Version 1.2 : précision sur le fait que des versions non vulnérables se voient proposer la mise à jour
- **MS08-014**
 - Version 3.3 : mise à jour de la FAQ
- **MS08-018**
 - Version 1.3 : explication sur le classement "critique" pour Project 2000, et "important" pour les autres versions
- **MS08-043**
 - Version 1.3 : mise à jour de la FAQ
- **MS08-049**
 - Version 1.1 : correction d'une clé de BdR

Avis Microsoft (7/7)

- **MS08-051**
 - Version 2.1 : Live Meeting 2005 et 2007 ne sont pas affectés
- **MS08-052**
 - Version 2.0 : Office XP SP2, Office Viewer 2003 et Office Viewer 2007 sont affectés
 - Version 2.1 : Project XP SP2 -> Project XP SP1
- **MS08-053**
 - Version 1.1 : précision sur le déploiement Vista/2008
 - Version 2.0 : problème avec la version norvégienne de WME 9
- **MS08-054**
 - Version 1.1 : "mitigating factors" erronés
 - Version 2.0 : problème avec la version norvégienne de WMP11
- **MS08-055**
 - Version 1.1 : précisions sur OneNote 2007

Infos Microsoft (1/5)

■ Sorties logicielles

- **Un patch passé inaperçu**
 - <http://support.microsoft.com/kb/955417/fr>
 - <http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-389.pdf>
- **Hyper-V disponible gratuitement**
 - <http://www.microsoft.com/servers/hyper-v-server/default.mspx>
- **Microsoft Enterprise Search (Express) gratuit**
 - <http://www.microsoft.com/enterprisesearch/serverproducts/searchserverexpress/download.aspx>
- **Microsoft Security Assessment Tool (MSAT) 4.0**
- **Sysinternals Procmon 2**
- **Versions Alpha/Beta/RC ...**
 - Visual Studio 2010 / .NET Framework 4.0
 - SilverLight 2 RC0

Infos Microsoft (2/5)

- **Microsoft PhotoSynth désormais ouvert au public**
 - En mode Web
 - <http://photosynth.net/>
- **Quelques extras Windows Ultimate**
 - DreamScene Pack #4 et Microsoft Tinker
- **Roadmap Windows 7**
 - <http://www.microsoft.com/windows/letter.html>
- **"Windows Cloud" disponible d'ici 1 mois (???)**
 - Système d'exploitation basé sur .NET
 - Déploiement rapide d'applications Web
 - Sans doute un lien avec les projets "Singularity" / "Midori"
 - http://news.zdnet.com/2424-9595_22-239003.html
- **La base du futur Windows Strata ?**
 - <http://www.infos-du-net.com/actualite/14608-windows-strata-cloud.html>

Infos Microsoft (3/5)

■ Actualité

- **Le SDL vs. Les mécapoulets**
 - <http://msdn.microsoft.com/fr-fr/security/cc835583.aspx>
 - <http://www.mecapoulets-lefilm.fr/>
 - <http://www.youtube.com/watch?v=1ldIZ3lyKsc>
- **Encore une com' géniale**
 - **Search Engine Rap Battle**
 - <http://searchenginebattle.com/>
 - **I'm a PC**
 - <http://www.microsoft.com/presspass/windows/default.aspx>
- **Microsoft propage la bonne parole du SDL**
 - <http://msdn.microsoft.com/en-us/security/cc967276.aspx>

Infos Microsoft (4/5)

- **Fake fail**
 - <http://gizmodo.com/5048411/bsod-repeatedly-strikes-nine-inch-nails-concerts>
- **"Facebook est le nouvel Outlook"**
 - <http://www.techcrunch.com/2008/09/13/microsofts-real-problem-facebook-is-the-new-outlook-and-other-ways-that-remond-is-not-listening-to-generation-y/>
 - http://news.cnet.com/8301-13505_3-10041396-16.html
- **Microsoft investit \$1 milliard dans la R&D**
 - **Un centre de recherche à côté de son nouveau siège à Issy-Les-Moulineaux**
 - <http://www.20minutes.fr/article/258528/High-Tech-Microsoft-pourrait-investir-1-milliard-d-euros-pour-un-centre-de-recherche-en-France.php>
 - **Orienté moteurs de recherche**

Infos Microsoft (5/5)

■ **Les membres initiaux du "SDL Pro Network"**

- **Cigital Inc., Dulles, Va.**
- **IOActive Inc., Seattle**
- **iSEC Partners Inc., San Rafael, Calif.**
- **Leviathan Security Group Inc., Westminster, Colo.**
- **Next Generation Security Software Ltd. (NGS), Sutton, United Kingdom**
- **n.runs AG, Oberursel, Germany**
- **Security Innovation Inc., Wilmington, Mass.**
- **Security University Inc., Stamford, Conn.**
- **Verizon Business, Basking Ridge, N.J.**

Infos Réseau

- **12 failles critiques d'un coup chez Cisco**
 - **Rappel: Cisco publie désormais 2 fois par an**
 - <http://www.cisco.com/warp/public/707/cisco-sa-20080924-bundle.shtml>
 - <http://isc.sans.org/diary.html?storyid=5078>

- **Nokia se sépare de ses solutions de sécurité**
 - <http://www.neteco.com/165978-nokia-vente-solutions-securite-entreprises-demission-directeur-technique.html>

- **Une implémentation d'*opportunistic encryption*: Obfuscated TCP**
 - <http://code.google.com/p/obstcp/>

- **Stallman vs. Web 2.0**
- **Larry Ellison vs. Cloud Computing**
 - <http://www.pcpro.co.uk/news/227235/gnu-creator-lashes-out-at-web-services.html>

- **OVH suspend (temporairement) son offre de serveurs dédiés**
 - **Raisons principales: les impayés ... et les attaques internes**
 - <http://www.lesnouvelles.net/articles/attaques/ovh-abus-dedies>

Infos Unix

- **La NSA lance un toolkit pour écrire des applications Open Source "hautement sécurisées"**
 - Basé sur SPARK ADA ...
 - <http://www.adacore.com/home/gnatpro/tokeneer/>
- **Linux 2.6.27rc1 peut *détruire* les cartes réseau Intel e1000**
 - <http://www.heise-online.co.uk/news/Intel-e1000e-user-Don-t-install-the-new-SUSE-betas--/111583>
- **Emacs supporte OOXML (ISO 29500)**
 - <http://xmlguru.cz/2008/05/first-application-supporting-is-29500>
 - Rappel: c'est le format Microsoft ☺

Failles

■ Produits tiers vulnérables

- **QuickTime < 7.5.5**
 - <http://support.apple.com/kb/HT1222>
 - Très nombreux bogues corrigés (cf. ZDI / iDefense)
 - Note: QuickTime 8.0 est sorti
- **Bonjour < 1.0.5**
- **iPhone < 2.1**
 - <http://support.apple.com/kb/HT3129>
- **Mac OS X < 10.5.5**

- **Firefox < 3.0.2 et < 2.0.0.17 + ThunderBird < 2.0.0.17**
 - Firefox 3.0.3 ne semble pas corriger de problème de sécurité
- **Chrome < 0.2.149.27**
- **Opera < 9.60**

- **Wordpress < 2.6.2**
 - Il est possible de réinitialiser le mot de passe à une valeur aléatoire
 - Et l'aléa est prédictible ☺

Failles

- "0day" dans QuickTime
 - Affecte: 7.5.5 et 8.0
 - Exploit :
 - <http://www.milw0rm.com/exploits/6471>
 - "Off by one" + QuickTime compilé avec /GS = inexploitable !
 - <http://www.avertlabs.com/research/blog/index.php/2008/09/18/the-true-of-recent-0day-for-quicktime755itunes80/>

- N'oublions pas ...
 - WinZip < 11.2sr1 (GDI+)
 - MPlayer
 - RealWin 2.0 (un système SCADA)
 - <http://xforce.iss.net/xforce/xfdb/45465>
 - Pas de patch disponible
 - (Nombreuses failles dans) Java pour Mac OS X

 - VMWare Server/Workstation/Player (64 bits uniquement)
 - Elévation de privilèges *guest user* -> *guest kernel*
 - Plus quelques failles dans VMWare ESX 3.5 ...

Failles

- **Des failles dans la plupart des implémentations TCP/IP (?)**
 - **Présenté lors de la conférence T2**
 - <http://sec-t.org/2008/files/SEC-T2008.zip>
 - **Couverture médiatique**
 - http://www.darkreading.com/blog.asp?blog_sectionid=403&doc_id=164939&WT.svl=tease2_2
 - http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1332898,00.html
 - http://www.theregister.co.uk/2008/10/01/fundamental_net_vuln/
 - **Old news ?**
 - <http://shlang.com/netkill/>

Failles

- **Metasploit 3.2 sous licence BSD**

- <http://blog.metasploit.com/2008/10/metasploit-32-bsd-licensing.html>

- **Fabriquer un certificat EV-SSL**

- <http://www.keyon.ch/de/News/Faking%20Extended%20Validation%20SSL%20Certificates%20in%20Internet%20Explorer%207%20V1.1b.pdf>

- **"Click-jacking" de la webcam et du micro via Flash**

- **Workaround:**

- <http://www.adobe.com/support/security/advisories/apsa08-08.html>

- **Failles de sécurité: où est la limite ?**

- **Flash permet de manipuler le presse-papier**

- <http://www.securityfocus.com/bid/31117/discuss>

- **Ca sera corrigé dans Flash 10 ☺**

Malwares et spam (1/4)

- **Spam == Freedom of Speech ?**
 - http://voices.washingtonpost.com/securityfix/2008/09/virginia_anti-spam_law_overtur.html
- **Microsoft et l'état de Washington portent plainte contre des *scarewares***
 - <http://www.atg.wa.gov/pressrelease.aspx?id=21026>
 - http://voices.washingtonpost.com/securityfix/2008/09/microsoft_washington_state_tar.html
- **Gartner: les antivirus sont trop chers pour ce qu'ils sont**
 - <http://www.01net.com/editorial/391842/les-antivirus-sont-trop-chers-et-pas-assez-performants-selon-gartner/>

Malwares et spam (2/4)

■ L'Asus EEE Box infectée par un virus en usine

- <http://www.generation-nt.com/eeebox-virus-production-virus-infection-actualite-168221.html>

■ McAfee "Artemis" (Cloud Computing)

- Très "tendance"

- <http://www.lesnouvelles.net/articles/produits/artemis-service-in-the-cloud-de-mcafee>
- http://www.mcafee.com/us/enterprise/products/artemis_technology/index.html
- <http://www.avertlabs.com/research/blog/index.php/2008/10/01/artemis-backstage-1-malware-mapping/>

Malwares et spam (3/4)

■ YTFakeCreator

- Pour créer rapidement de "faux" sites YouTube ...
 - <http://www.zdnet.fr/actualites/informatique/0,39040745,39383264,00.htm>

■ La fin de NeoSploit ?

- http://www.rsa.com/blog/blog_entry.aspx?id=1314

■ Il semblerait que non ...

- <http://www.itrnews.com/articles/82417/neosploit-est-pas-mort.html?>
- http://www.vnunet.fr/news/cyber_attaque_une_certaine_de_milliers_de_sites_web_pris_d_assaut_-2028873

■ Mais ne serait-ce qu'une opération marketing d'Aladdin ... ?

- <http://www.lesnouvelles.net/articles/divers/aladdin-neosploit-secret>

Malwares et spam (4/4)

- **Le retour du virus macro**
 - <http://isc.sans.org/diary.html?storyid=5029>
- **Un virus techniquement original**
 - <http://www.f-secure.com/weblog/archives/00001507.html>
 - Elève ses privilèges via la faille GDI
 - Désactive les hooks noyau
- **Les botnets passent le 2.0**
 - <http://www.lesnouvelles.net/articles/virus/botnets-web-20>
- **Le spam aime les lettres A, M et S**
 - Jusqu'à 40% de spam en plus
 - <http://news.bbc.co.uk/2/hi/technology/7591370.stm>

Failles 2.0

■ Google Chrome

- **Déconseillé par les gouvernements allemands et hollandais**
 - <http://www.zdnet.fr/actualites/internet/0,39020774,39383091,00.htm?xtor=EPR-100>
 - <http://www.computerworld.co.ke/articles/2008/09/09/security-agencies-rally-against-google-chrome>

- **Quelques articles intéressants**
 - **Revue du code source**
 - Utilisation de la librairie Microsoft WTL
 - *Reverse-engineering* de `NtSetProcessInformation()` sous Windows XP pour supporter DEP
 - <http://www.hanselman.com/blog/TheWeeklySourceCode33MicrosoftOpenSourceInsideGoogleChrome.aspx>
 - **Revue de la licence**
 - <http://www.pcinpact.com/actu/news/45721-google-chrome-publicite-licence-EULA.htm>
 - **Les données collectées**
 - http://src.chromium.org/svn/trunk/src/chrome/browser/metrics_service.cc

- **La part de marché de Chrome passe de 1,5% à 1%**
 - http://www.vnunet.fr/news/google_chrome_seduit_moins_un_mois_plus_tard-2028929

Failles 2.0

■ Google (suite)

- Google fournit 85% des revenus de Mozilla
 - <http://www.generation-nt.com/mozilla-google-partenariat-recherche-firefox-actualite-144451.html>
- 45% des logiciels Google sont en Beta
 - <http://www.01net.com/editorial/391773/le-chiffre-du-jour-45-pour-cent-des-logiciels-de-google-sont-des-betas/>

■ Nouvelle attaque : le click-jacking

- Présentation OWASP annulée à la demande d'Adobe et Microsoft (IE)
- On comprend assez bien le principe
 - <http://securite.reseaux-telecoms.net/actualites/lire-le-clickjacking-revient-sur-le-devant-de-la-scene-au-grand-dam-d-adobe-18794.html>
 - <http://lists.whatwg.org/pipermail/whatwg-whatwg.org/2008-September/016284.html>
 - <http://blogs.zdnet.com/security/?p=1972>

Failles 2.0

■ La magie eBay opère toujours

- Une passerelle VPN entièrement configurée
 - <http://www.pcpro.co.uk/news/227190/council-sells-security-hole-on-ebay.html>
- Un appareil photo contenant des photos du MI6
 - <http://www.pcpro.co.uk/news/227376/mi6-photos-sold-on-ebay.html>

■ Le "vrai-faux" e-passeport est disponible

- <http://freeworld.thc.org/thc-epassport/>
- <http://securite.reseaux-telecoms.net/actualites/lire-elvis-presley-passe-la-douane-en-hollande-18889.html>

■ Le "skimming" ... par WiFi et SMS

- <http://fr.news.yahoo.com/zdnet/20081010/ttc-le-wi-fi-et-les-sms-au-service-des-p-79c9bc8.html>

■ Le chiffrement BlackBerry "cassé" pour le gouvernement indien ?

- N'affecte pas les transmissions de BB à BB
 - <http://blogs.zdnet.com/security/?p=1964>
- Dans l'ensemble pas très clair ...

Failles 2.0

- **Erreur de design dans le SSO Google Apps**
 - Basé sur SAML, mais "simplifié" par Google
 - <http://www.ai-lab.it/armando/pub/fmse9-armando.pdf>
 - <http://www.identityblog.com/?p=1011>

- **BusinessWeek.com piraté**
 - http://www.theregister.co.uk/2008/09/16/businessweek_hacked/

- **Le système de contrôle du LHC piraté**
 - <http://www.timesonline.co.uk/tol/news/uk/science/article4744329.ece>

- **Des pirates indiens connectés à la console d'un trader**
 - <http://www.lavienumerique.com/articles/81695/pirates-manipulent-cours-bourse.html>

Failles 2.0

- **"Skype espionne ses utilisateurs pour les autorités chinoises"**

- <http://www.01net.com/editorial/392057/skype-espionne-ses-utilisateurs-pour-les-autorites-chinoises>

- **Pages 47 et 73:**

- <http://2006.recon.cx/en/f/vskype-part2.pdf>

- **La cryptographie quantique ... crackée !**

- <http://technology.newscientist.com/article/dn14866-laser-cracks-unbreakable-quantum-communications.html>

- **Au moment où elle commençait à être utilisée ...**

- <http://news.bbc.co.uk/2/hi/science/nature/7661311.stm>

Failles 2.0

- **Un faux émetteur GPS ... capable de crasher un avion**
 - <http://www.msnbc.msn.com/id/26992456/>
- **Theo de Raadt vs. Sun Hardware**
 - <http://seclists.org/fulldisclosure/2008/Sep/0144.html>
- **Téléphoner ou pirater ?**
 - L'OpenMoko a l'air meilleur pour pirater que pour téléphoner ☺
 - <http://www.neopwn.com/>

Failles 2.0

■ Vol / pertes de données

- Les 17 millions de compte perdus par Deutsche Telekom refont surface
 - <http://www.pcworld.fr/actualite/17-millions-de-comptes-hackes-chez-deutsche-telekom/14221/>
- Le gouvernement anglais perd les données de 100,000 militaires et 600,000 candidats
 - http://tempsreel.nouvelobs.com/actualites/international/20081010.OBS5246/des_donnees_personnelles_sur_100.000_militaires_dispar_a.html
- Asus met son code source sur le CD de Recovery
 - <http://www.pcpro.co.uk/news/224892/asus-ships-software-cracker-on-recovery-dvd.html>

Failles 2.0

■ WiFi

- **Le propriétaire d'un AP WiFi "ouvert" arrêté en Inde après un attentat**
 - <http://www.rediff.com/news/2008/sep/14delblast4.htm>
- **Se connecter en WiFi dans les hôtels, une mauvaise idée ?**
 - <http://www.journaldunet.com/solutions/securite/actualite/connexion-internet-dans-un-hotel-prudence.shtml>
- **La mairie de Paris remet en service le WiFi dans les bibliothèques**
 - <http://www.zdnet.fr/actualites/telecoms/0,39040748,39384001,00.htm>
- **Mauvaise passe pour WPA-PSK**
 - ElcomSoft fait x100 sur la performance de cassage
 - <http://mobile.slashdot.org/mobile/08/10/12/1724230.shtml>
 - TKIP pourrait bientôt être cracké

Actualité (France)

■ La biométrie ne s'impose pas

- https://www.cdse.fr/fileadmin/Documents/Etudes/enquetebiometrie20_05.pdf
- Facteurs limitants
 - 1. problèmes juridiques
 - 2. obsolescence des systèmes
 - 3. manque de fiabilité
 - 4. coût d'installation
 - 5. problèmes éthiques
 - 6. réactions des employés

■ Le SGDN déconseille Opera Beta, Chrome Beta et IE 8 Beta

- <http://www.pcworld.fr/actualite/les-beta-d-ie-8-de-chrome-et-d-opera-ont-deconseillees-par-matignon/12411/>

■ Le Challenge T2 remporté par 2 français

- <http://www.t2.fi/2008/09/29/t2%C2%B408-challenge-winners/>

Actualité (France)

- **Les attaques par déni de service identifiées comme "critique" par la DCSSI**
 - "Et surtout, la France ne s'interdit plus, comme d'autres Etats, de se doter de capacités à lancer elle-même des attaques informatiques rapides et ciblées hors de ses frontières."
 - <http://securite.reseaux-telecoms.net/actualites/lire-les-attaques-massives-par-deni-de-service-2eme-menace-exterieure-contre-la-france-18833.html>

- **30% de "l'Internet français" reste vulnérable à la faille DNS**
 - <http://www.nbs-system.com/securite/dns.html>
 - Information à prendre avec des pincettes
 - Comment sont réalisés les tests ?

- **La "riposte graduée" mise à mal par l'Europe**
 - <http://fr.news.yahoo.com/pcinpact/20080924/ttc-l-europe-signe-l-arret-de-mort-de-la-c2f7783.html>
 - "(...) certains États membres malveillants, dont la France (...)"
 - <http://www.numerama.com/magazine/10783-President-de-l-UE-Sarkozy-exige-le-retrait-de-l-amendement-138.html>

Actualité (France)

■ La loi anti-phishing meure avec son auteur

- http://www.silicon.fr/fr/news/2008/10/06/france___mort_de_la_loi__anti_phishing__

■ Le Forum des Droits de l'Internet (FDI) vous demande votre avis

- <http://forums.foruminternet.org/forumdisplay.php?f=42>

Actualité (USA)

■ Les 10 ans de Google

- Une idée géniale : chercher dans l'Internet de 2001 !
 - <http://www.google.com/search2001.html>

■ Google va "anonymiser" les journaux au bout de 9 mois

- <http://www.lemondeinformatique.fr/actualites/lire-google-ramene-a-neuf-mois-la-duree-de-conservation-des-logs-26874.html>

■ Apple pose un brevet sur le "baladeur dans la chaussure"

- <http://www.webpronews.com/topnews/2008/09/14/apple-declares-war-on-sneaker-hackers>

■ Le ".gov" sous DNSSEC ?

- <http://snad.ncsl.nist.gov/dnssec/>

Actualité (USA)

- Sarah Palin utilise Yahoo! Mail pour éviter les obligations légales de transparence
 - Dans ces conditions, il vaut mieux éviter de perdre son mot de passe ...
 - <http://blogs.abcnews.com/politicalpunch/2008/09/how-transparent.html>
 - http://wikileaks.org/wiki/Sarah_Palin_Yahoo_inbox_2008
 - *"The hacker guessed that Alaska's governor had met her husband in high school, and knew Palin's date of birth and home Zip code. Using those details, the hacker tricked Yahoo Inc.'s service into assigning a new password (...)"*
- Les USA, plus grosse source d'attaques dans le monde
 - http://www.vnunet.fr/news/les_etats_unis_premiers_dans_le_domaine_des_attaques_informatiques-2028769
- Integrated Cyber Exercise 2
 - Fun ☺
 - <https://www.sans.org/ns2008/whitewolf.php>

Actualité (USA)

- **Scientifique American: "vie privée et technologie"**
 - <http://www.internetactu.net/2008/09/17/la-vie-privee-et-la-technologie/>

- **Détecter les "terroristes" par le stress**
 - http://www.usatoday.com/news/nation/2008-09-18-bioscanner_N.htm

- **Symantec achète MessageLabs pour \$695m**
 - Une société anglaise offrant des services de messagerie sécurisée
 - <http://www.lesnouvelles.net/articles/business/symantec-achete-messagelabs>

- **McAfee acquière Secure Computing**

- **Cisco acquière Jabber**
 - http://newsroom.cisco.com/dlls/2008/corp_091908.html

- **Le CFO de McAfee (ex-NAI) condamné**
 - 1 an de prison
 - \$200,000 d'amende
 - ... pour des faits remontant à 1998

Actualité

- **Uninformed, volume 10**
 - <http://uninformed.org/?v=10>

- **VMWare lance son propre système: VDC-OS**
 - <http://www.zdnet.fr/actualites/informatique/0,39040745,39383377,00.htm>

- **La norme ISO 27799:2008 est publiée**
 - Destinée aux professions de santé
 - http://www.iso.org/iso/fr/catalogue_detail?csnumber=41298

- **Une nouvelle certification proposée par l'ISC² pour les développeurs : le CSSLP**
 - <http://www.techworld.com/news/index.cfm?RSS&NewsID=104781>

- **Le consortium SafeCode produit un guide de développement sécurisé**
 - <http://www.safecode.org/>

Actualité

- **Citrix publie ses symboles de débogage**
 - <http://support.citrix.com/article/CTX118622>
- **Sortie du téléphone Google Android**
 - <http://gizmodo.com/5053734/how-many-google-phone-engineers-does-it-take-to-tell-the-time>
 - http://cache.gawker.com/assets/images/4/2008/09/Dilbert_Android_2.jpg
- **Mixi adopte OpenID ... et partage les données de profil**
 - http://www.readwriteweb.com/archives/mixi_brings_sophisticated_open.php
- **Un logiciel de tracking pour les portables volés ... en Open Source**
 - <http://adeona.cs.washington.edu/>
- **11 octobre: la journée contre la cybersurveillance**
 - <http://www.vorratsdatenspeicherung.de/content/view/242/144/>

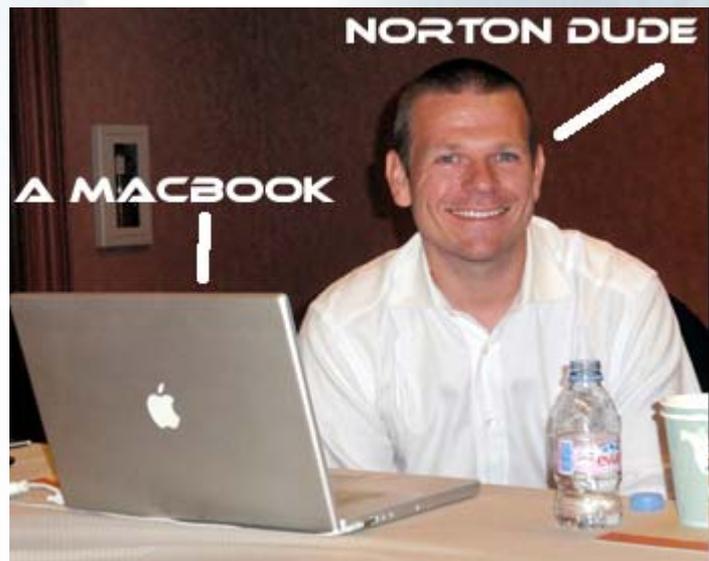
Fun

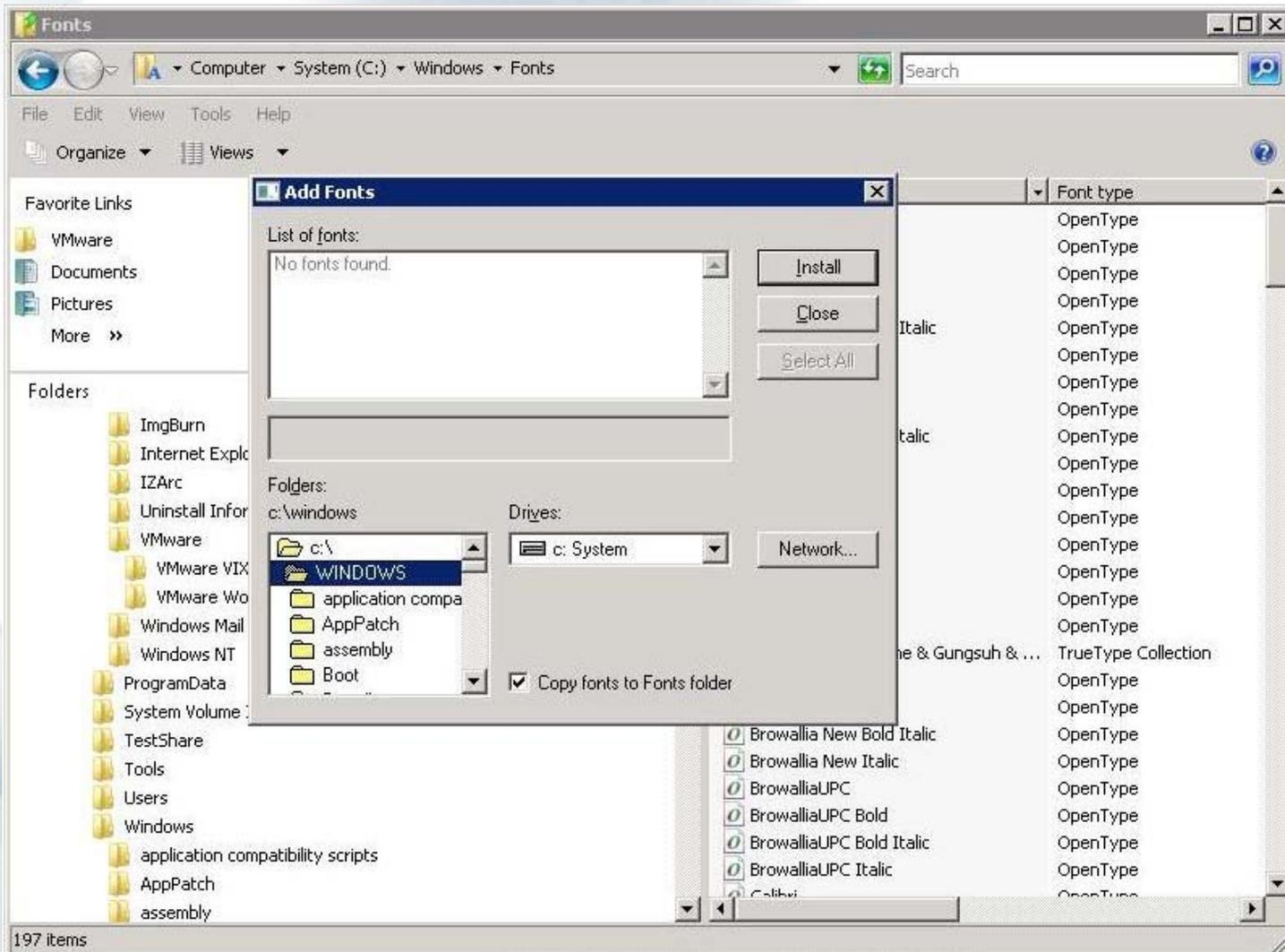
- **Apple ne serait pas l'inventeur de l'iPod**
 - <http://mp3.generationmp3.com/2008/09/08/apple-nest-pas-inventeur-de-ipod/>
- **Le MI6 recrute sur Facebook**
 - <http://www.pcpro.co.uk/news/227040/mi6-recruits-through-facebook.html>
- **2^{43,112,609}-1 est premier**
 - <http://mersenne.org/>
- **Bill Gates et les Easter Eggs (fascinant !)**
 - <http://www.pagetable.com/?p=43>
- **Un réseau sans-fil ... via l'éclairage ambiant**
 - <http://www.pcinpact.com/actu/news/46534-eclairage-LED-reseau-fil-entreprises.htm>
- **L'histoire de la police Comic Sans**
 - <http://www.connare.com/whycomic.htm>
 - <http://achewood.com/index.php?date=07052007>

Fun

- **BSoD happens**
 - <http://royal.pingdom.com/2008/10/09/blue-screen-of-death-in-unexpected-locations/>
- **Google renforce la sécurité de GMail ☺**
 - <http://gmailblog.blogspot.com/2008/10/new-in-labs-stop-sending-mail-you-later.html>
- **Cisco livre un CD ... de musique mexicaine**
 - <http://idle.slashdot.org/article.pl?sid=08/10/08/1418232>
- **L'abus de Mac est dangereux pour la santé**
 - <http://www.liberation.fr/terre/010133618-mac-pro-le-pepin-toxique-pour-apple>
- **La fin d'une époque ?**
 - <http://fravia.com/illness.htm>

Fun





Questions / réponses

- Questions / réponses
- Prochaine réunion le mardi 4 novembre 2008
- N'hésitez pas à proposer des sujets et des salles