# OSSIR
# Groupe Paris

## Réunion du 13 janvier 2009

# 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 (1/12)

- **Correctifs de Décembre 2008**
  - **Avec [*exploitability index*]**
  - **MS08-070 Failles dans les contrôles livrés avec Visual Basic 6 (CVEx6) [1/1/1/2/2/2]**
    - **Affecte:**
      - **FrontPage 2002 SP3 (versions asiatiques)**
      - **Project 2003 SP3 / 2007 / 2007 SP1**
      - **VB6, Visual Studio 2002 SP1 / 2003 SP1**
      - **FoxPro 8 SP1 / 9 SP1 / 9 SP2**
    - **Exploit:**
      - **Plusieurs contrôles standard sont vulnérables: DataGrid, FlexGrid, Hierarchical FlexGrid, Charts, Masked Edit, *parser* AVI**
      - **Au moins une faille était connue en août 2008**
    - **Crédit:**
      - **AdLab / VenusTech (x3), Jason Medeiros / Affiliated Computer Services, Carsten Eiram / Secunia, Mark Dowd / McAfee, Brett Moore / Insomnia Security, CHkr_D591 / ZDI, Michal Bucko / CERT, Security Intelligence Analysis Team / Symantec**

# Avis Microsoft (2/12)

- MS08-071 Failles GDI (CVEx2) [2/3]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: fichier WMF malformé
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=762
  - Crédit: Jun Mao / iDefense, Juan Caballero / BitBlaze Group
    - http://bitblaze.cs.berkeley.edu/

- MS08-072 Failles multiples dans Word (CVEx8) [2/2/2/2/2/2/2/3]
  - Affecte:
    - Word 2000 SP3 / 2002 SP3 / 2003 SP3 / 2007 / 2007 SP1
    - Outlook 2007 / 2007 SP1
    - Office 2004 / 2008 pour Mac
    - Convertisseur OpenXML pour Mac
    - Pack de compatibilité OpenXML pour Office 2003
    - Works 8
    - Viewers Word 2003 / 2007
  - Exploit: fichier Word malformé (fichier RTF x5)
    - http://seclists.org/fulldisclosure/2008/Dec/0313.html
  - Crédit: Ricardo Narvaja / Core Security, Dyon Balding / Secunia, Yamata Li / Palo Alto Networks, Wushi / ZDI (x3), Aaron Portnoy / TippingPoint (x2)
  - Note: seul Works 8.5 est supporté par ce correctif

# Avis Microsoft (3/12)

- MS08-073 Patch cumulatif pour IE (CVEx4) [1/1/1/2]
  - Affecte: Internet Explorer (toutes versions supportées)
  - Exploit: corruptions mémoire diverses, conduisant à l'exécution de code
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=761
  - Crédit: Carlo Di Dato, Brett Moore / ZDI, Chris Weber / Casaba Security, Jun Mao / iDefense

- MS08-074 Failles multiples dans Excel (CVEx3) [1/1/2]
  - Affecte:
    - Excel 2000 SP3 / 2002 SP3 / 2003 SP3 / 2007 / 2007 SP1
    - Office 2004 / 2008 pour Mac
    - Convertisseur OpenXML pour Mac
    - Pack de compatibilité OpenXML pour Office 2003
    - Viewers Excel 2003 / 2007
  - Exploit: fichier Excel malformé
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=763
  - Crédit: Joshua J. Drake / iDefense, Claes M Nyberg / Signedness.org, Dyon Balding / Secunia

# Avis Microsoft (4/12)

- MS08-075 Failles multiples dans Windows Search (CVEx2) [1/2]
  - Affecte: Windows Vista SP0&SP1, Windows 2008
  - Exploit:
    - Recherche sauvegardée
    - Lien search-ms://
  - Crédit: Andre Protas / eEye, Nate McFeters
  - SWI Blog:
    - http://blogs.technet.com/swi/archive/2008/12/09/ms08-075-reducing-attack-surface-by-turning-off-protocol-handlers.aspx

# Avis Microsoft (5/12)

- **MS08-076 Failles multiples dans Windows Media (CVEx2) [1/1]**
  - **Affecte: Windows Media Runtime (toutes versions supportées, y compris Windows 2008 Core)**
  - **Exploit:**
    - **"Credential Reflection" due à une mauvaise gestion du Service Principal Name (SPN)**
    - **Fuite des *credentials* NTLM si le protocole ISATAP est utilisé**
  - **Crédit: n/d**
  - **SWI Blog:**
    - **http://blogs.technet.com/swi/archive/2008/12/09/windows-media-components-part-1-of-2.aspx**
    - **http://blogs.technet.com/swi/archive/2008/12/09/ms08-076-windows-media-components-part-2-of-2.aspx**

# Avis Microsoft (6/12)

- MS08-077 Contournement de l'authentification dans SharePoint 2007 [1]
  - Affecte:
    - SharePoint 2007 SP0 / 2007 SP1 (32 et 64 bits)
    - Search Server 2008 (32 et 64 bits) (versions complète et express)
  - Exploit: possibilité d'effectuer des actions administratives sans authentification
    - Ajouter l'option "mode=ssp" dans les requêtes
  - Crédit: anonymous

- 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

# Avis Microsoft (7/12)

- Advisories
  - 2+1 failles dans la nature le lendemain du Patch Tuesday
    - http://www.breakingpointsystems.com/community/blog/patch-tuesdays-and-drive-by-sundays
  - Q960906 : convertisseur Word 97 -> Wordpad
    - Affecte : Windows (toutes versions antérieures à XP SP3 et Vista)
    - Exploit : via un fichier ".wri"
    - http://www.microsoft.com/technet/security/advisory/960906.mspx

# Avis Microsoft (8/12)

- Q961051 : *parser* XML dans IE
  - Affecte : toutes les versions d'IE (y compris IE8 Beta2)
  - Exploit : détails publics ... et disponibles dans Metasploit
    - http://blog.zoller.lu/2008/12/in-wild-ie7-0day-update.html
    - http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20081211
  - Workarounds :
    - http://www.microsoft.com/technet/security/advisory/961051.mspx
    - http://blogs.technet.com/swi/archive/2008/12/12/Clarification-on-the-various-workarounds-from-the-recent-IE-advisory.aspx
    - http://www.eweek.com/c/a/Security/Microsoft-Gets-More-Detailed-About-IE-Vulnerability-and-Workarounds/
- Corrigé par MS08-078 le 17 décembre

# Avis Microsoft (9/12)

- **Q961040 : *buffer overflow* dans SQL Server**
  - **Affecte : SQL Server 2000 et 2005**
  - **Exploit : sp_replwritetovarbin()**
    - **http://www.certa.ssi.gouv.fr/site/CERTA-2008-ALE-017/CERTA-2008-ALE-017.html**
    - **http://www.sec-consult.com/files/20081209_mssql-sp_replwritetovarbin_memwrite.txt**
    - **http://www.milw0rm.com/exploits/7501**
    - **http://blogs.technet.com/swi/archive/2008/12/22/more-information-about-the-sql-stored-procedure-vulnerability.aspx**
- **Q961509 : exploitation de collisions MD5 dans une PKI**
  - **Voir plus loin ...**
- **Attention à la surmédiatisation des failles ...**
  - **Windows Media Player / quartz.dll**
    - **http://isc.sans.org/diary.html?storyid=5563**
    - **http://blogs.technet.com/swi/archive/2008/12/29/windows-media-player-crash-not-exploitable-for-code-execution.aspx**

# Avis Microsoft (10/12)

- **Prévisions pour Janvier 2009**
  - **1 bulletin "critique" affectant toutes les versions de Windows**

# Avis Microsoft (11/12)

- Révisions
  - MS04-032
    - Version 1.1 : mise à jour de la FAQ
  - MS05-002
    - Version 2.1 : mise à jour de la FAQ
  - MS05-018
    - Version 1.1 : mise à jour de la FAQ
  - MS05-053
    - Version 1.2 : mise à jour de la FAQ
  - MS07-017
    - Version 1.1 : mise à jour de la FAQ
  - MS08-052
    - Version 3.0 : les packs de compatibilité Office 2007 SP0 / SP1 + Groove 2007 + Expression Web 1 et 2 sont vulnérables

# Avis Microsoft (12/12)

- MS08-068
  - Version 1.2 : ajout d'un problème connu
- MS08-069
  - Version 1.1 :
    - retrait du "kill bit" comme *workaround*
    - /overwriteoem ne marche pas
  - Version 1.2 : précision sur le fichier journal d'installation
- MS08-070
  - Version 1.1 : mise à jour du patch pour VB6 SP6
- MS08-071
  - Version 1.1 : mise à jour de la criticité pour la faille CVE-2008-3465
- MS08-072
  - Version 1.1 :
    - MBSA ne marche pas avec Word 2000 SP3
    - Ce patch remplace les précédents pour Outlook 2007 et 2007 SP1
  - Version 1.2 :
    - Word Viewer 2003 n'est pas vulnérable
- MS08-075
  - Version 1.1 : corrections des clés de base de registre dans le *workaround*
- MS08-078
  - Version 1.1 : Server Core n'est pas affecté

# Infos Microsoft (1/4)

- Sorties logicielles
  - Windows Seven Beta1 (publique)
  - SQL Server 2005 SP3
  - "Writing Secure Code for Windows Vista"
    - En téléchargement gratuit
      - http://csna01.libredigital.com/?urrs4gt63d
  - Microsoft propose une application pour iPhone
    - http://www.silicon.fr/fr/news/2008/12/15/microsoft_propose_une_application_pour_l_iphone
  - Y aura-t-il un ZunePhone ?
    - http://blog.wired.com/gadgets/2008/12/rumor-zune-phon.html

# Infos Microsoft (2/4)

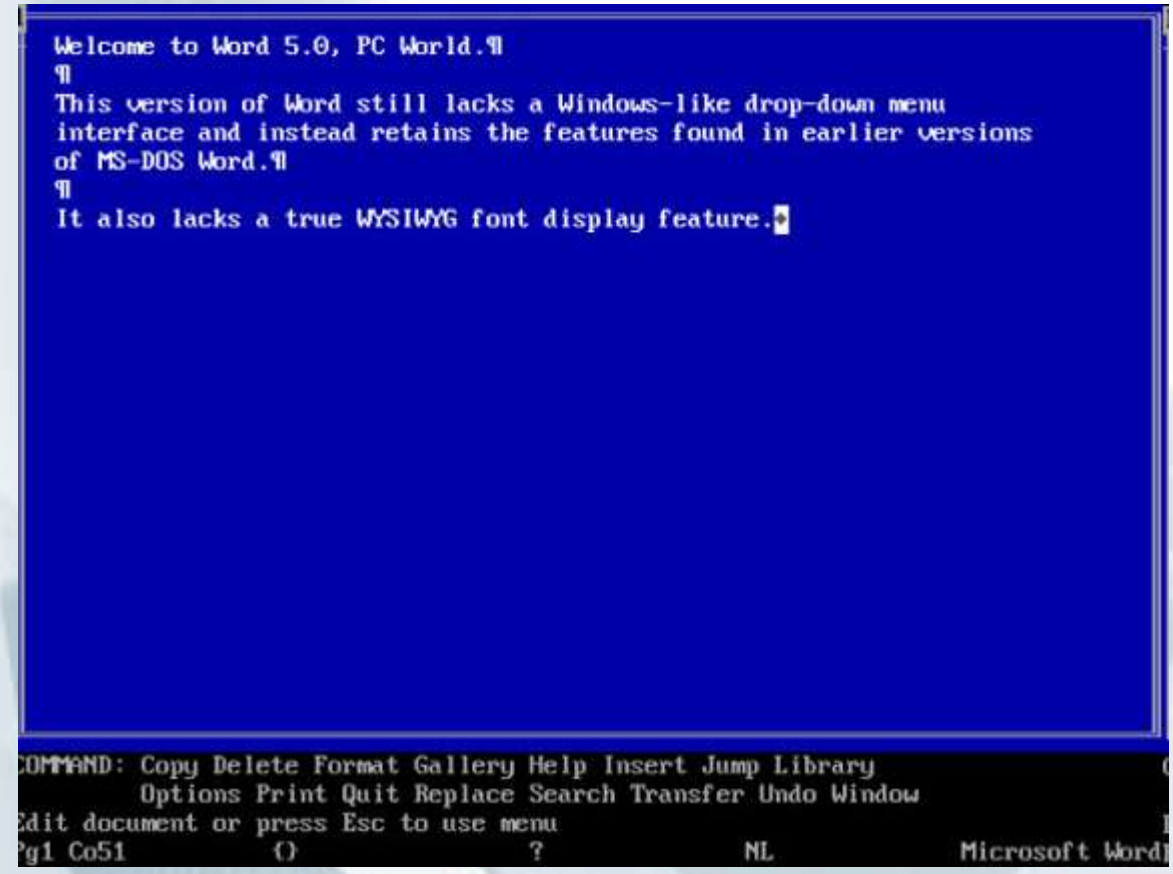
- Le saviez-vous ?
  - Le créateur de Latex travaille chez Microsoft
    - http://fr.wikipedia.org/wiki/Leslie_Lamport
  - Michael Youn a été commercial chez Microsoft
    - http://www.commeaucinema.com/personne=michael-youn,23210.html
- Actualité
  - Le bug du Zune 30
    - http://www.aeroxp.org/2009/01/lesson-on-infinite-loops/
  - 15,000 licenciements à venir chez Microsoft ?
    - http://www.itrmanager.com/articles/85838/microsoft-appreterait-reductions-postes-importantes.html

# Infos Microsoft (3/4)

- **Actualité (suite)**
  - **Le format ODF (OpenOffice) sera supporté dans Office 2007 SP2**
    - **C'est vieux, mais le SP2 approche ☺**
    - **http://www.lemondeinformatique.fr/actualites/lire-microsoft-va-supporter-odf-dans-office-et-participer-a-son-evolution-26130.html**
  - **La communication Microsoft ...**
    - **http://www.acdcrocks.com/excel/**

# Infos Microsoft (4/4)

- Word a 25 ans
  - http://blogs.msdn.com/frogzfr/archive/2008/11/18/word-a-25-ans.aspx



# Infos Réseau

- ATT et Level3 plantés
  - Cause : un accident de train a coupé un câble
  - Affecte : CNN, OWASP, ...
    - http://isc.sans.org/diary.html?storyid=5572
    - http://isc.sans.org/diary.html?storyid=5569
- D.J.Bernstein vs. DNSSEC
    - http://dnscurve.org/
- Une implémentation pour la surconsommation de ressources TCP (?)
    - http://freshmeat.net/projects/complemento/

# Infos Unix

- Actualité
  - SlackWare 12.2 ne supporte plus le noyau 2.4
  - Linux embarqué dans une patate ?
    - http://www.bbspot.com/News/2008/12/linux-on-a-potato.html
  - Alan Cox quitte Red Hat pour Intel
    - http://ostatic.com/blog/alan-cox-bids-farewell-to-red-hat-moves-to-intel
  - OpenSolaris présintallé sur des portables Toshiba
    - http://ostatic.com/blog/opensolaris-coming-to-toshiba-laptops-continuing-a-trend
  - La différence entre "correction" et "faille de sécurité" ...
    - http://esec.fr.sogeti.com/blog/index.php?2009/01/08/48-correction-silencieuse-d-une-vulnerabilite-dans-le-noyau-linux

# Infos Unix

- **Failles**
  - **OpenSSL < 0.9.8j**
    - **Le code de retour de EVP_VerifyFinal() n'est pas toujours correctement vérifié**
    - **Affecte les signatures DSA et ECDSA (peu utilisée en pratique)**
      - **http://www.openssl.org/news/secadv_20090107.txt**
    - **Conduit à un empoisonnement possible dans BIND si DNSSEC est activé**
      - **http://isc.sans.org/diary.html?storyid=5641**
    - **Affecte NTP également**
  - **Une régression dans GnuTLS**
    - **4 patches successifs pour corriger une faille !**
      - **http://lists.gnu.org/archive/html/gnutls-devel/2008-12/msg00008.html**
  - **Faille(s) dans SPIP < 2.0.2**
    - **CVE-2008-5812, CVE-2008-5813 (injection SQL dans le champ "id")**
      - **http://zine.spip.org/spip.php?article65**
  - **Faille dans Samba < 3.2.7**
    - **Accès à '/' si "registry shares = yes" (ce n'est *pas* la config par défaut)**
      - **http://us1.samba.org/samba/security/CVE-2009-0022.html**

# Infos Unix

- Failles (suite)
  - Faille dans XTerm
    - La lecture d'un fichier peut provoquer l'exécution de commandes
      - http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=510030
      - allowWindowOps et allowFontOps ne sont pas à "false" sous Debian/Ubuntu
  - La mise à jour vers PHP 5.2.7 désactive l'option "magic_quotes"
    - http://www.suspekt.org/2008/12/07/php-527-beware-magic_quotes_gpc-broken/
  - Elévation de privilèges locale dans toutes les versions de FreeBSD
    - http://security.freebsd.org/advisories/FreeBSD-SA-08:13.protosw.asc
  - Archive::Tar n'enlève pas les ".."
  - Elévation de privilèges locale dans Solaris 10 via *nscd*
    - http://sunsolve.sun.com/search/document.do?assetkey=1-66-242006-1

# Failles

- Principales applications
  - Firefox < 3.0.5, < 2.0.0.20
  - Thunderbird < 2.0.0.19
  - Opera < 9.63
  - Mac OS X < 10.5.6, < 10.4.11
    - Plus de 20 correctifs, dont Flash Player
  - Flash Player Linux < 10.0.15.3, < 9.0.152.0
    - Analyse de la faille : une injection ";" dans system() ...
      - http://basonbugs.blogspot.com/2008/12/you-can-only-sit-down-if-you-are-human.html

- Patch Oracle trimestriel
  - 41 failles dont plusieurs exploitables à distance sans authentification (dont WebLogic)
    - http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2009.html

# Failles

- Le fuzzer Flash du pauvre
  - http://blog.metasploit.com/2009/01/fuzzing-flash-for-fun-asnative.html
- Les applications tierces, sources de failles
  - (Attention, lien commercial)
    - http://www.bit9.com/files/Vulnerable_Apps_DEC_08.pdf

# Malwares et spam

- Un nouveau ver se propage sur MS08-067
  - W32.Downadup
    - http://isc.sans.org/diary.html?storyid=5596
- Un malware bloque l'accès à des sites de téléchargement illégal
    - http://www.clubic.com/actualite-249200-malware-bloque-acces-pirate-bay-mininova.html
- CastleCops ferme
    - http://www.castlecops.com/

# Malwares et spam

- Malware Hash Registry
  - http://www.team-cymru.org/Services/MHR/
- La page éducative de l'Anti-Phishing Working Group
  - http://education.apwg.org/r/how_to.html
- Le *social engineering* arrive en français
  - $6 la traduction en ligne !
    - http://ddanchev.blogspot.com/2008/12/localized-social-engineering-on-demand.html
- 60% des guichets de transfert d'argent infectés par des *keyloggers*
  - Sur un échantillon de 300 (Los Angeles + Las Vegas)
    - http://www.enterprise-security-today.com/story.xhtml?story_id=63524&page=1

# Failles 2.0

- Des comptes Twitter piratés
  - Dont Barack Obama et Britney Spears
    - http://blog.twitter.com/2009/01/monday-morning-madness.html
    - http://www.networkworld.com/news/2009/010609-3-ways-a-twitter-hack.html
  - Via l'accès à un compte de support Twitter
    - Mot de passe: "happiness"

- XSS (x4) sur Facebook
    - http://www.xssed.com/news/80/New_highly_critical_Facebook_XSS_vulnerabilities_pose_serious_privacy_risks/

- Un XSS sur le site d'American Express
  - Pourtant fondateur de la norme PCI/DSS
    - http://www.theregister.co.uk/2008/12/16/american_express_website_bug/

- Google Chrome et Safari ont les pires gestionnaires de mots de passe
    - http://www.info-svc.com/news/2008/12-12/

# Failles 2.0

- Metasploit Decloak v2
  - http://blog.metasploit.com/2008/12/metasploit-decloak-v2-unanonymizer.html
- Les sources de CheckPoint FW-1 volées ?
  - + 1 faille distante trouvée ?
    - http://seclists.org/fulldisclosure/2008/Dec/0344.html
- Les applications d'espionnage arrivent sur iPhone
  - http://flexispy.com/spyphone-flexispy-apple-iphone.htm
  - http://mobile-spy.com/iphone.html
- eCL0WN
  - Pour copier son passeport dans un téléphone (!)
    - http://www.dexlab.nl/

# Actualité (France)

- La fibre chez les particuliers, pas pour tout de suite
  - http://www.zdnet.fr/actualites/telecoms/0,39040748,39385523,00.htm
- Un DoS sur la Livebox
  - Exploit : GET /-
    - http://www.securityfocus.com/archive/1/499010
- Un faux correctif Microsoft à destination des francophones
  - http://securitylabs.websense.com/content/Alerts/3252.aspx
- Des sociétés françaises victimes de *carding*
  - 750,000 euros d'achats frauduleux sur un seul site
    - http://www.01net.com/editorial/398904/pixmania-victime-d-une-fraude-aux-numeros-de-cartes-bancaires-voles/
- Internet-Signalement(.gouv.fr) est ouvert

# Actualité (France)

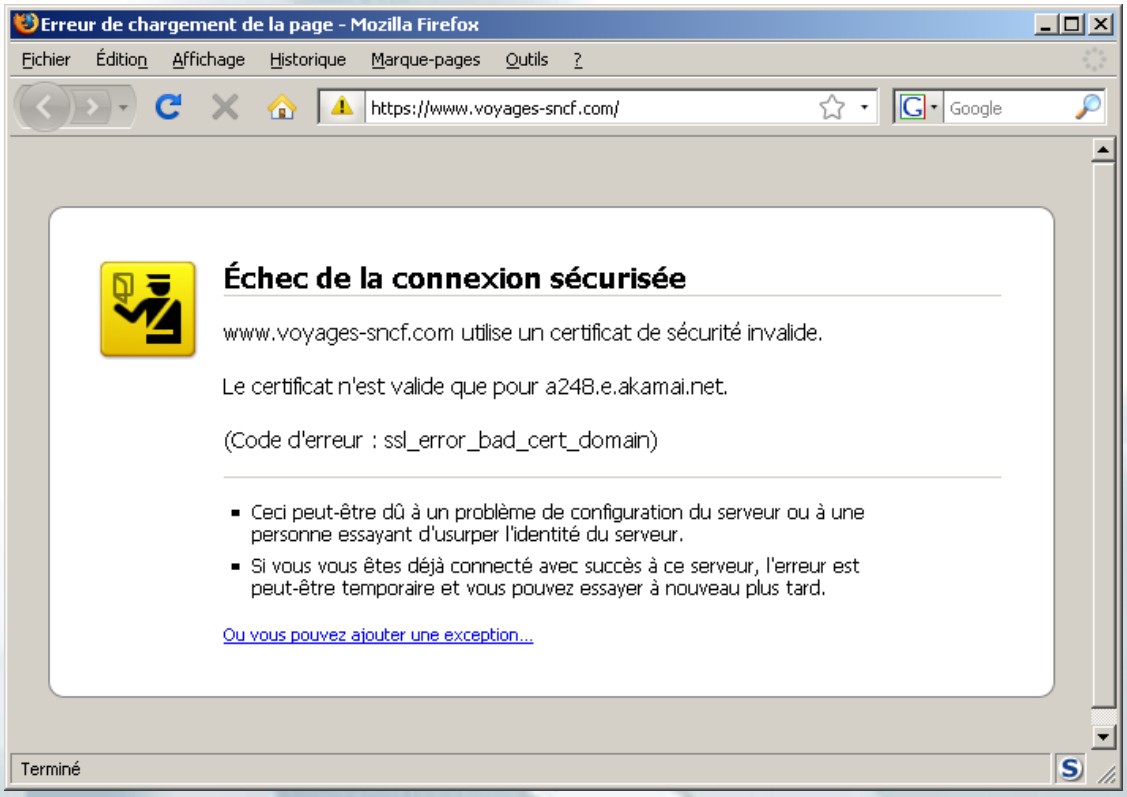
- La bataille pour la "riposte graduée" continue
  - http://www.zdnet.fr/actualites/internet/0,39020774,39385147,00.htm
- Le rapport HADOPI
  - http://www.guim.fr/blog/files/Equancy-Tera-Rapport_Hadopi.pdf
- Pour résumer ...
  - Internet, un nid à « psychopathes, violeurs, racistes et voleurs »
    - http://www.pcinpact.com/actu/news/47913-frederic-lefebvre-internet-mafia-drogue.htm
- Les "assises du piratage"
  - http://www.ecrans.fr/Des-Assises-du-piratage-a-sens,5997.html

# Actualité (France)

- "L'affaire" du TGI de Bonneville
  - http://www.clubic.com/actualite-249154-warez-telechargement-site-tribunal.html
  - La vérité (?)
    - http://scteam.canalblog.com/archives/2009/01/07/12004462.html
  - La "victime" collatérale s'appelle Florian Lefebvre ☺
    - http://www.linuxfr.org/~efyx/27714.html
    - http://forum.ubuntu-fr.org/viewtopic.php?id=283553&p=1
- Un petit malin fait croire au retrait de la candidature de Grenoble pour les JO 2018
  - http://securite.reseaux-telecoms.net/actualites/lire-un-hacker-fait-croire-au-retrait-de-la-candidature-de-grenoble-aux-jeux-olympiques-de-2018-19268.html
- Il ne faut pas fâcher les Chinois
  - http://www.thedarkvisitor.com/2008/12/chinese-hackers-targeting-french-embassy-websites-around-the-world/
- Equiper la France d'en bas avec Windows 98 ?
  - http://www.ordi2-0.fr/

# Actualité (France)

- Quelques problèmes chez Voyages-Sncf.com ...
  - http://www.pcinpact.com/actu/news/47981-maj-voyages-sncf-vilaine-anomalie.htm
  - http://linuxfr.org/~Dinofly/27645.html



# Actualité (USA)

- Annonces MacWorld Expo
  - La fin des DRM sur iTunes
    - http://www.rtlinfo.be/rtl/news/article/208709/itunes-se-d-barrasse-des-dispositifs-anticopie/
  - Sinon pas d'annonce notable ...
    - http://www.nowhereelse.fr/resume-apple-keynote-macworld-2009-14701/
- La RIAA cesse de faire appel à MediaSentry
  - http://www.theinquirer.net/inquirer/news/232/1050232/riaa-dumps-dodgy-detectives
- Un exemple de dossier passager
  - Même l'adresse IP utilisée pour commander les billets est notée
    - http://current.newsweek.com/budgettravel/2008/12/whats_in_your_government_trave.html
- Le bundle qui tue : Nessus + CANVAS + D2
  - http://blog.tenablesecurity.com/2009/01/nessus-professionalfeed-canvas-and-dsquare-bundled-penetration-testing-and-compliance-suite.html

# Actualité (USA)

- L'administration Obama va-t-elle passer la seconde en matière de sécurité ?
  - http://www.lepoint.fr/actualites-technologie-internet/usa-des-experts-veulent-fortifier-les-reseaux-sensibles/1387/0/298355
- CheckPoint rachète les *appliances* Nokia
  - http://www.checkpoint.com/press/2008/checkpoint_to_acquire_nokia_sab_221208.html
- Window Snyder quitte Mozilla
  - http://blog.mozilla.com/security/2008/12/10/leaving-mozilla/
  - http://blogs.zdnet.com/security/?p=2294
- JournalSpace est mort
  - http://journalspace.com/this_is_the_way_the_world_ends/not_with_a_bang_but_a_whimper.html
- Les machines à voter, une source de divertissement infinie
  - 197 bulletins "disparaissent" purement et simplement
    - http://blog.wired.com/27bstroke6/2008/12/unique-election.html

# Actualité

- Compte-rendu de la conférence 25C3
  - Du 27 au 30 décembre à Berlin
    - http://events.ccc.de/congress/2008/wiki/Streaming
  - Une fausse CA basée sur les collisions de MD5
    - Références
      - http://www.win.tue.nl/hashclash/rogue-ca/
      - http://www.phreedom.org/research/rogue-ca/
      - http://broadcast.oreilly.com/2008/12/the-sky-is-not-falling-on-toda.html
    - 14% du Web affecté ?
      - http://news.netcraft.com/archives/2009/01/01/14_of_ssl_certificates_signed_using_vulnerable_md5_algorithm.html
    - Un bon plugin FireFox
      - http://www.codefromthe70s.org/sslblacklist.aspx
    - Pourtant ça n'est pas très compliqué d'obtenir un faux certificat ...
      - https://blog.startcom.org/?p=145

# Actualité

- DECT cassé
  - http://dedected.org/
- Des détails sur la "faille TCP"
  - http://events.ccc.de/congress/2008/Fahrplan/events/2909.en.html
- Sécurité des terminaux de paiement par carte
  - http://events.ccc.de/congress/2008/Fahrplan/events/2953.en.html
- Système KeeLoq (pour les portes de parking)
  - http://events.ccc.de/congress/2008/Fahrplan/events/3030.en.html
- Exploitation IOS fiable (sur modèles 1700 et 2600 / PPC)
  - http://events.ccc.de/congress/2008/Fahrplan/events/2816.en.html
- Un réseau GSM parallèle disponible pendant la conférence
  - http://bs11-abis.gnumonks.org/trac/
- Localisation de téléphones via SS7
  - http://events.ccc.de/congress/2008/Fahrplan/events/2997.en.html
- Le "SMS of Death" pour Nokia S60
- (...)

- Quelques commentaires
  - http://www.avertlabs.com/research/blog/index.php/2008/12/30/25c3-nothing-to-hide/
- Et les dommages collatéraux
  - http://events.ccc.de/congress/2008/wiki/Hacked

# Actualité

- Une attaque contre la technologie Intel/TXT
  - http://theinvisiblethings.blogspot.com/2009/01/attacking-intel-trusted-execution.html
- 21 millions de comptes bancaires volés en Allemagne
  - A vendre, mise à prix : 12 millions d'euros
    - http://www.theregister.co.uk/2008/12/09/stolen_german_bank_accounts_for_sale/
- La Grande-Bretagne inaugure la perquisition électronique
  - http://www.timesonline.co.uk/tol/news/politics/article5439604.ece
- OllyDbg 2 en version beta
  - http://www.ollydbg.de/version2.html

# Actualité

- Un OS secret testé chez Google ?
  - Des *headers* HTTP jamais vu ailleurs
    - http://www.internetnews.com/dev-news/print.php/3788821
    - http://www.forbes.com/2008/12/05/google-operating-system-tech-enter-cx_ew_1205google.html
- Google Chrome
  - Disponible en version 1.0
    - http://www.informationweek.com/news/internet/browsers/showArticle.jhtml?articleID=212400455
  - Un scanner de ports utilisant le mode FTP PASV
    - http://seclists.org/bugtraq/2009/Jan/0010.html
- Le *Browser Security Handbook* ... par Google
  - 60 pages
    - http://code.google.com/p/browsersec/wiki/Main
- Un téléphone au lieu de la prime annuelle chez Google
    - http://tech.slashdot.org/article.pl?sid=08/12/22/2232242
    - http://technology.timesonline.co.uk/tol/news/tech_and_web/article5391660.ece

# Actualité

- AT&T vs. Google
  - "Google devrait payer 10% du coût d'Internet"
    - http://tech.slashdot.org/article.pl?sid=08/12/07/1610222
- L'Egypte obtient la désactivation de la fonction GPS dans les iPhones
  - Probablement une arme de destruction massive ...
    - http://tech.slashdot.org/tech/08/12/09/1413243.shtml
- La Chine impose l'utilisation de son propre système d'exploitation dans tous les cybercafés
  - China's Red Flag Linux operating system
    - http://www.toolinux.com/toolinux_information/revue_de_presse/linux_un_arme_de_surveillance_en_chine_ar11553.html
  - Tous les utilisateurs sont également filmés
- Un administrateur IT (et espion israélien) exécuté en Iran
    - http://www.timesonline.co.uk/tol/news/world/middle_east/article5258057.ece

# Actualité

- La faillite de l'indien Satyam pourrait affecter de nombreuses entreprises qui ont externalisé leur informatique

- Après Free, au tour de Cisco/Linksys d'être poursuivi pour violation de GPL
  - http://www.linuxdevices.com/news/NS6803262843.html

- Cisco publie son analyse de l'année 2008
  - http://cisco.com/en/US/prod/vpndevc/annual_security_report.html
    - 90% de spam dans les emails (200 milliards / jour)
    - +11% de failles par rapport à 2007
    - +300% de failles dans les solutions de virtualisation
    - +90% pour les attaques proviennent de domaines "légitimes"

- N'oubliez pas que 2008 a eu 1 seconde de plus ☺

# Fun

- Le Web'08 tourne à la rixe
  - http://www.lexpansion.com/economie/actualite-high-tech/leweb-08-degenere-en-affrontement-entre-l-europe-et-les-etats-unis_170110.html
- Le logiciel indispensable sur les forums
  - http://stupidfilter.org/
- Le BioHacking devient tendance
  - http://news.yahoo.com/s/ap/do_it_yourself_dna

# Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 10 février 2008
- N'hésitez pas à proposer des sujets et des salles