OSSIR
Groupe Paris

Réunion du 10 janvier 2012

Revue des dernières vulnérabilités

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

Avis Microsoft

- **Décembre 2011**
  - **14 bulletins, 20 failles**
  - **MS11-087 Faille dans le support des polices TTF [1]**
    - **Affecte: Windows (toutes versions)**
    - **Exploit: élévation de privilèges locale**
      - **Exploité par DuQu**
    - **Crédit:**
      - **Symantec**
      - **CrySys**

Avis Microsoft

- MS11-088 Faille dans Microsoft Office [1]
  - Affecte: Microsoft Office 2010 IME (version chinoise)
  - Exploit: élévation de privilèges
  - Crédit: Yang Yanbei

- MS11-089 Faille dans Microsoft Office [1]
  - Affecte:
    - Office 2007
    - Office 2010
    - Office 2011 (Mac)
  - Exploit: exécution de code à l'ouverture d'un fichier malformé
  - Crédit:
    - Nikita Tarakanov / CISS Research Team
    - Alexey Sintsov / Digital Security Research Group
    - + ZDI

Avis Microsoft

- MS11-090 Mise à jour des Kill Bits [1]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: exécution de code au travers des composants ActiveX suivants
    - Microsoft Time
    - Dell IT Assistant
    - HP Easy Printer Care
    - HP Photo Creative
    - Yahoo! CD Player
  - Crédit: anonymous + iDefense

- MS11-091 Failles dans Publisher (x4) [1,1,2]
  - Affecte: Office 2003, Office 2007
  - Exploit: exécution de code à l'ouverture d'un ".pub" malformé
  - Crédit: Will Dormann / CERT/CC (x3)

Avis Microsoft

- **MS11-092 Faille dans Windows Media [1]**
  - **Affecte: Windows XP / Vista / Seven**
  - **Exploit: exécution de code au travers d'un fichier ".dvr-ms" malformé**
  - **Crédit: anonymous + iDefense**

- **MS11-093 Faille dans OLE [1]**
  - **Affecte: Windows XP / 2003**
  - **Exploit: exécution de code à l'ouverture d'un objet OLE malformé**
  - **Crédit: anonymous + iDefense**

Avis Microsoft

- MS11-094 Faille dans PowerPoint [2]
  - Affecte: Office 2007, Office 2010, Office 2008 (Mac), Compatibility Pack 2007, PowerPoint Viewer 2007
  - Exploit:
    - "DLL Preloading"
    - Exécution de code à l'ouverture d'un fichier ".ppt" malformé
  - Crédit:
    - Greg MacManus / iSight Partners
    - Anonymous + ZDI

- MS11-095 Faille dans Active Directory [1]
  - Affecte: AD, ADAM, LDS
    - Windows (toutes versions supportées sauf Itanium)
  - Exploit: "buffer overflow" exploitable à distance après authentification (!)
  - Crédit: n/d

Avis Microsoft

- **MS11-096 Faille dans Excel [1]**
  - **Affecte: Office 2003, Office 2004 (Mac)**
  - **Exploit: exécution de code à l'ouverture d'un fichier ".xls" malformé**
  - **Crédit: anonymous + iDefense**

- **MS11-097 Faille dans CSRSS [1]**
  - **Affecte: Windows (toutes versions supportées)**
  - **Exploit: élévation de privilèges locale**
    - **http://www.archive.org/details/Shattering_the_Windows_Message_Passing_Architecture_and_Security_Model**
  - **Crédit: Alex Ionescu**

Avis Microsoft

- MS11-098 Faille noyau [1]
  - Affecte: Windows 32 bits (toutes versions supportées)
  - Exploit: élévation de privilèges locale
    - https://twitter.com/#!/daveaitel/status/147053799205388289
  - Crédit: Matthew Jurczyk + iDefense

- MS11-099 Correctif cumulatif pour IE (x3) [3,1]
  - Affecte: IE (toutes versions supportées)
  - Exploit:
    - Evasion du DOM à l'aide du filtre anti-XSS
    - "DLL Preloading"
    - Contournement du DOM lors d'un téléchargement
  - Crédit:
    - Thomas Stehle
    - Andy Cooper / Citrix Security Team
    - Robert Swiecki / Google Inc.
    - Yosuke Hasegawa
    - Jan Schejbal

Avis Microsoft

- Avis "hors bande"

  - MS11-100 Correctif cumulatif pour .NET
    - Affecte: .NET Framework (toutes versions supportées)
    - Exploit:
      - Déni de service via des collisions dans les tables de hachage
      - "Open Redirect" via les formulaires ASP.NET
      - Contournement de l'authentification par injection de %00
        - http://archives.neohapsis.com/archives/fulldisclosure/2011-12/0489.html
        - https://twitter.com/#!/peibolcode/status/154311904066666496
      - Vulnérabilité dans le cache d'authentification par formulaire ASP.NET
    - Crédit:
      - Irene Abezgauz / Seeker
      - Kestutis Gudinavicius / SEC Consult
      - Oliver Dewdney / LBi

Avis Microsoft

- **Prévisions pour Janvier 2012**
  - Critique (x1), importants (x6)
  - Windows (x6), outils de développement (x1)
  - Correction de la faille BEAST
- **Advisories**
  - Q2639658 Faille TTF (exploitée par DuQu)
    - V2.0: publication du bulletin
  - Q2269637 "DLL Preloading"
    - V13.0: ajout des bulletins MS11-094 et MS11-099
  - Q2659883 Déni de service distant sur ASP.NET
    - V1.0: publication suite à la conférence du CCC
    - V2.0: publication du bulletin MS11-100

Avis Microsoft

- Révisions
  - MS11-088
    - V1.1: ajout d'un problème connu
  - MS11-089
    - V1.1: correction documentaire
  - MS11-090
    - V1.1: correction documentaire
  - MS11-094
    - V1.1: mise à jour de la FAQ (PowerPoint 2010 SP1)
  - MS11-096
    - V1.1: le Pack de Compatibilité SP3 n'est pas vulnérable
  - MS11-099
    - V1.1: correction des "mitigating factors" et des "severity ratings"
  - MS11-100
    - V1.1: mise à jour de la FAQ

Infos Microsoft

- **Sorties logicielles**
  - **SQL Server 2012 RC0**
  - **Exchange 2010 SP2**
  - **SilverLight 5**
    - **Support 64 bits, accélération 3D, …**

Infos Microsoft

- **Autre**
  - La mise à jour automatique sans confirmation arrive pour Internet Explorer
    - Toutes les versions de Windows sont concernées
      - http://windowsteamblog.com/ie/b/ie/archive/2011/12/15/ie-to-start-automatic-upgrades-across-windows-xp-windows-vista-and-windows-7.aspx
  - Un SMS malveillant fait rebooter Windows Phone
    - http://www.winrumors.com/windows-phone-sms-attack-discovered-reboots-device-and-disables-messaging-hub/
  - Un nouveau patron pour Windows Phone
    - http://www.linformaticien.com/actualites/id/22667/microsoft-nomme-un-nouveau-responsable-pour-windows-phone.aspx

Infos Microsoft

- Windows Azure
  - Le SDK en Open Source sur GitHub
    - https://github.com/WindowsAzure
  - Support Java, Hadoop, MongoDB, et Apache Solr …
  - … et même Linux
    - http://www.linformaticien.com/actualites/id/22907/microsoft-bientot-des-vm-linux-sur-windows-azure.aspx
- Microsoft et HP partenaires sur le Cloud et Office 365
    - http://www.solutions-logiciels.com/actualites.php?actu=10810
- Windows 8
  - … aura un mode "factory reset"
    - http://www.linformaticien.com/actualites/id/22966/windows-8-remise-a-zero-et-restauration-des-pc.aspx

Infos Microsoft

- Live Messenger accessible en protocole XMPP
  - http://windowsteamblog.com/windows_live/b/windowslive/archive/2011/12/14/anyone-can-build-a-windows-live-messenger-client-with-open-standards-access-via-xmpp.aspx
- Windows 8
  - Ouvrir sa session avec une image ?
    - http://blogs.msdn.com/b/b8/archive/2011/12/16/signing-in-with-a-picture-password.aspx
- Démenti: Bill Gates ne reviendra pas chez Microsoft
  - http://www.smh.com.au/technology/technology-news/bill-gates-speaks-out-in-sydney--on-microsoft-steve-jobs-and-the-weather-20111215-1owak.html
- La rumeur du rachat de Nokia par Micrsoft relancée
  - http://www.linformaticien.com/actualites/id/22695/et-si-microsoft-rachetait-nokia.aspx

Infos Réseau

- (Principales) faille(s)
  - WiFi Protected Setup
    - … ou comment remplacer une clé 128 bits par un code PIN à 8 chiffres …
      - http://sid.rstack.org/blog/index.php/522-wps-talon-d-achille-du-wpa
  - Un bogue assez subtil découvert dans BIND
    - < 9.8.1-P1, < 9.7.4-P1, < 9.6-ESV-R5-P1, < 9.4-ESV-R5-P1
      - https://www.isc.org/software/bind/advisories/cve-2011-4313
  - SlowLoris + SockStress = SlowHTTPTest
      - https://community.qualys.com/blogs/securitylabs/2011/08/25/new-open-source-tool-for-slow-http-attack-vulnerabilities
  - Faille dans les produits WebSense
    - Injection de commandes (dans l'interface d'administration)
      - http://www.websense.com/support/article/kbarticle/v7-6-About-Hotfix-24-for-Websense-Web-Security-Websense-Web-Filter-and-Web-Security-Gateway

Infos Réseau

- **Autres infos**
  - **L'attaque HashDos affecte aussi:**
    - **PHP, Ruby, Apache/Tomcat, …**
    - **Des correctifs sont disponibles**

Infos Unix

- (Principales) faille(s)
  - Struts: OGNL a encore frappé
    - http://seclists.org/fulldisclosure/2012/Jan/41
  - Faille "include" dans TYPO3 < 4.5.9, < 4.6.2
    - http://typo3.org/teams/security/security-bulletins/typo3-core/typo3-core-sa-2011-004/?mid=5551891
  - Injection SQL dans Cacti < 0.8.7h
    - Paramètre "login_username"
      - http://www.cacti.net/release_notes_0_8_7h.php
  - Moodle
    - Cf. failles MSA-11-0042 à MSA-11-0054

Infos Unix

- XSS ...
  - PhpMyAdmin
    - http://www.phpmyadmin.net/home_page/security/PMASA-2011-20.php
    - http://www.phpmyadmin.net/home_page/security/PMASA-2011-19.php
  - TikiWiki
    - http://info.tiki.org/article183
  - Nagios XI
    - http://assets.nagios.com/downloads/nagiosxi/CHANGES-2011.TXT
  - Wordpress < 3.3.1
    - http://wordpress.org/news/2012/01/wordpress-3-3-1/
  - Jboss < 5.2.0
    - http://rhn.redhat.com/errata/RHSA-2011-1822.html

Infos Unix

- FreeBSD / telnetd
  - Buffer overflow "basique"
    - http://security.freebsd.org/advisories/FreeBSD-SA-11:08.telnetd.asc
- FreeBSD / pam_ssh
  - Il est possible de se connecter sous l'identité de n'importe quel utilisateur n'ayant pas de passphrase sur sa clé SSH
    - http://security.freebsd.org/advisories/FreeBSD-SA-11:09.pam_ssh.asc
- FreeBSD / chroot
  - Evasion de la chroot via ftpd
    - http://security.freebsd.org/advisories/FreeBSD-SA-11:07.chroot.asc
- FreeBSD + NetBSD
  - Elévation de privilèges locale via OpenPAM
    - http://security.freebsd.org/advisories/FreeBSD-SA-11:10.pam.asc
    - http://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2011-008.txt.asc
- Quand "init" efface "/" …
  - #fail
    - https://bugs.launchpad.net/ubuntu/+source/upstart/+bug/557177

Infos Unix

- **Autre**
  - **Suite aux problèmes de licence, Oracle Java va être supprimé de toutes les installations Ubuntu**
    - **Il faudra passer aux JVM alternatives comme OpenJDK**
      - **https://lists.ubuntu.com/archives/ubuntu-security-announce/2011-December/001528.html**

Failles

- Principales applications
  - Adobe Flash Player ≤ 11.1.102.55
    - Exploité dans la nature
    - Pas de correctif
      - http://secunia.com/advisories/47161
  - Adobe Reader < 9.4.7, ≤ 10.1.1
    - Faille "U3D" activement exploitée dans la nature
      - http://www.adobe.com/support/security/advisories/apsa11-04.html
    - Adobe Reader 9.4.7 publié en urgence
      - http://www.adobe.com/support/security/bulletins/apsb11-30.html
    - Adobe X sera corrigé le 10 janvier
  - Adobe (autres bulletins)
    - XSS dans Flex SDK
      - http://www.adobe.com/support/security/bulletins/apsb11-25.html
    - XSS dans ColdFusion
      - http://www.adobe.com/support/security/bulletins/apsb11-29.html

Failles

- FireFox < 3.6.25, < 9.0.1
  - http://www.mozilla.org/security/known-vulnerabilities/firefox36.html#firefox3.6.25
- Google Chrome < 16.0.912.63
- Opera < 11.60
- VLC < 1.1.13
  - http://www.videolan.org/security/sa1108.html
- RealPlayer
  - 19 failles …
    - http://service.real.com/realplayer/security/11182011_player/en/
- VMWare ESXi 5
  - http://www.vmware.com/security/advisories/VMSA-2011-0009.html
- Pilote NVidia Stereoscopic 3D
  - Elévation de privilèges locale (via un canal nommé mal protégé)
    - http://technet.microsoft.com/en-us/security/msvr/msvr11-016

Failles

- Intel/TXT
  - "Buffer overflow" dans SINIT "Authenticated Code Module"
    - http://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00030&languageid=en-fr

- SCADA
  - Siemens Simatic : le mot de passe par défaut est "100"
    - Et autres joyeusetés
      - http://xs-sniper.com/blog/2011/12/20/the-siemens-simatic-remote-authentication-bypass-that-doesnt-exist/

Failles 2.0

- Botnets russes vs. Twitter
  - Après les élections
    - http://www.bbc.co.uk/news/technology-16108876
- Facebook et Paypal se mettent d'accord
  - … pour pouvoir envoyer facilement de l'argent avec un compte Facebook
    - http://apps.facebook.com/paypal_sendmoney/

Sites piratés

- **Les sites piratés du mois**
  - **Stratfor**
    - **Un acteur majeur de la cybersécurité américaine**
      - **http://cryptome.org/0005/stratfor-hack.htm**
      - **http://www.theregister.co.uk/2012/01/03/stratfor_mega_hack/**
    - **Les numéros de CB volés ont été utilisés pour donner de l'argent à des œuvres de bienfaisance**
      - **http://thehackernews.com/2011/12/stratfor-hacked-by-anonymous-hackers.html**
  - **GlobalSign (autorité de certification)**
    - **Seul le Web public a été affecté**
      - **http://www.globalsign.co.uk/company/press/121411-security-incident-report.html**
  - **CSDN (Chinese Software Developer Network)**
    - **6 millions de comptes**
  - **Un site du Ministère de la Défense**
      - **http://www.zone-h.org/mirror/id/16259909**

Sites piratés

- Un processeur de paiements européen
  - "Non spécifié"
    - http://www.romania-insider.com/visa-says-european-card-processor-notified-about-database-security-breach/43598/#
  - A noter que de nombreuses CB françaises sont à vendre sur un site underground
    - https://cert.xmco.fr/blog/index.php?post/2011/12/19/50-000-cartes-bancaires-fran%C3%A7aises-pirat%C3%A9es-en-septembre
- *Plein* de gens
  - Google, Boeing, Arbor Networks, Yahoo!, Apple, Core Labs, Cisco, …
    - http://kizmiaz.dis.org/mm.txt
- *Plein* d'agences de notation
    - http://www.zataz.com/news/21851/agence-notation--piratage--anonymous--lulzsec.html
- Une unité de la défense indienne
  - Les outils de surveillance Apple
    - http://imgur.com/a/8XoGf#0
  - Les sources de Symantec Antivirus
    - http://inagist.com/briankrebs/154924810022043648/
  - … et probablement plein d'autres choses intéressantes

Sites piratés

- Les sources de Solaris 11
  - Ou du moins celles du noyau
- Square Enix
  - 800,000 comptes américains piratés
    - http://www.jeuxvideo.com/news/2011/00055343-les-serveurs-de-square-enix-pirates.htm
- Senat.fr
  - Après le vote de la loi sur le génocide arménien
    - http://www.linformaticien.com/actualites/id/22843/negation-du-genocide-armenien-senat-fr-pirate.aspx
- Amnesty International
  - "Exploit Pack" classique
    - https://krebsonsecurity.com/2011/12/amnesty-international-site-serving-java-exploit/

Sites piratés

- VirusTotal victime de DDoS
  - https://twitter.com/#!/cedricpernet/status/147257981086605312
- Pastebin victime de DDoS
- Un drone américain ultra-secret piraté
  - Avec un brouilleur GPS à $100 ?
    - http://www.theregister.co.uk/2011/12/15/us_spy_drone_gps_spoofing/
- OVH + ProFTPd vulnérable = FAIL
  - http://travaux.ovh.com/?do=details&id=6222

Sites pas encore piratés

- Arcelor-Mittal
  - http://www.linformaticien.com/actualites/id/22893/arcelor-mittal-prochaine-cible-des-anonymous.aspx

Malwares et spam

- "Lilupophilupop" s'injecte dans des millions de sites Web
  - http://thehackernews.com/2012/01/one-million-pages-infected-by.html
  - Grâce à une technique originale (en deux étapes)
    - http://tibosecurity.blogspot.com/2012/01/sql-attacks-are-quite-funny-too.html
- Le gouvernement japonais prépare des armes numériques
  - … pour détruire les botnets
    - http://www.v3.co.uk/v3-uk/news/2134982/japan-offensive-cyber-weapon-plans-leaked
- Un robot de spam qui utilise des URLs raccourcies
  - … fournies par McAfee
    - https://twitter.com/#!/jsokoly/status/155066992594927616/photo/1
- Analyse "boite noire" d'un canal caché sur Twitter
  - http://malwareandsecurity.blogspot.com/2011/11/anoncommunicate.html

Actualité (francophone)

- Le référentiel des exigences applicables aux prestataires d'audit
  - Version 1.0
    - http://www.ssi.gouv.fr/IMG/pdf/referentiel-exigences_labellisation_prestataires-audit-teleservices_v1-0.pdf
- Un appel d'offres pour assurer le support des logiciels libres
    - https://www.marches-publics.gouv.fr/index.php5?page=entreprise.EntrepriseDetailConsultation&refConsultation=8460&orgAcronyme=g6l
- On pourra bientôt ouvrir sa boite aux lettres en NFC
    - http://cups-corp.fr/2011/12/la-poste-technologie-nfc-boites-aux-lettres/
- CNIL vs. SmartPhones
  - Recommandation: "installez un antivirus quand cela est possible"
    - http://www.cnil.fr/la-cnil/actu-cnil/article/article/smartphone-et-vie-privee-un-ami-qui-vous-veut-du-bien/

Actualité (francophone)

- Appel à commentaires de l'AFNOR
  - … sur les coffres forts numériques
  - … jusqu'au 10/02/2012
    - http://www.enquetes-publiques.afnor.org/recherche/coffre-fort.html
- Le Cloud français prend l'eau
  - Dassault Systèmes quitte le projet Andromède
    - http://www.itespresso.fr/cloud-computing-dassault-systemes-quitte-le-projet-andromede-49729.html
  - Atos pour les remplacer ?
    - http://www.linformaticien.com/actualites/id/22968/atos-pour-remplacer-dassault-dans-le-projet-cloud-andromede.aspx
  - Le projet Nu@ge saura-t-il faire mieux ?
    - http://www.linformaticien.com/actualites/id/22866/cloud-porte-par-8-pme-le-projet-nu-ge-prend-son-envol.aspx
- Il y aura bien un fichier des gens honnêtes
    - http://www.lioneltardy.org/archive/2011/12/14/ppl-identite.html

Actualité (francophone)

- Lancement de Free Mobile
  - Un cas d'école de buzz online
    - http://live.free.fr/
    - http://www.mamie-du-cantal.com/
    - http://www.linformaticien.com/actualites/id/22967/mamie-du-cantal-un-depute-interpelle-le-pdg-de-france-telecom.aspx
- La pré-plainte en ligne se généralise
  - "Nous savons qui vous êtes" … ou pas
    - http://www.journaldugeek.com/2012/01/09/ippolice-fail/
- ARJEL: le blocage des sites de jeux illégaux est entré en vigueur par décret
  - Blocage par DNS …
    - http://www.pcinpact.com/news/67984-blocage-arjel-decret-indemnisation-cgiet.htm
    - http://www.linformaticien.com/actualites/id/22909/les-fai-vont-bloquer-les-sites-de-paris-illegaux.aspx

Actualité (francophone)

- Le référé contre les FAI repoussé en mars 2012
  - Objet: le blocage du site AlloStreaming
    - http://www.linformaticien.com/actualites/id/22709/le-possible-blocage-d-allostreaming-est-reporte-a-2012.aspx

- Etes-vous un pirate ?
    - http://www.youhavedownloaded.com/

  - Du téléchargement illégal à l'Elysée ?
  - Heureusement "l'adresse IP n'est pas une donnée fiable" …
    - http://www.numerama.com/magazine/20940-des-pirates-a-l-elysee.html

  - Du téléchargement illégal au ministère de la Culture ?
    - http://pastebin.com/RJy3FnpC
    - http://www.linformaticien.com/actualites/id/22860/le-ministere-de-la-culture-aurait-pirate-des-films-et-de-la-musique.aspx

  - … dommage que le site soit un "fake" ☹

Actualité (anglo-saxonne)

- La loi SOPA fait débat
  - En résumé:
    - L'hébergeur est responsable des contenus
    - Filtrage de l'Internet par DNS
  - Les acteurs majeurs de l'Internet sont contre
    - http://www.linformaticien.com/actualites/id/22673/wikipedia-veut-se-saborder-pour-lutter-contre-la-sopa.aspx
    - http://www.theinquirer.fr/2012/01/05/loi-sopa-facebook-twitter-et-google-menacent-de-fermer.html
  - Un plugin FireFox déjà disponible pour contourner le filtrage DNS
    - http://www.linformaticien.com/actualites/id/22831/firefox-un-plug-in-anti-sopa.aspx
  - GoDaddy est "pour"
    - Ils perdent 21,000 clients
      - http://thenextweb.com/insider/2011/12/24/go-daddy-lost-21054-domains-yesterday-in-wake-of-sopa-pr-disaster/
  - Sony est "pour"
    - Ils se font immédiatement pirater

Actualité (anglo-saxonne)

- Le plus important groupe de lobbyistes américains piraté par les chinois pendant 1 an
  - http://online.wsj.com/article/SB10001424052970204058404577110541568535300.html

- Le Pentagone officiellement autorisé à déclencher des "cyber guerres" en 2012
  - http://www.wired.com/threatlevel/2011/12/internet-war-2/

Actualité (européenne)

- **Une amende de 5% du CA en cas de perte de données ?**
  - **Projet de loi à venir**
    - **http://www.silicon.fr/leu-veut-sanctionner-lourdement-la-perte-de-donnees-67607.html**
- **Nouvel accord sur le partage des données de voyage**
  - **Les américains ont désormais accès à tout**
    - **https://www.eff.org/deeplinks/2011/12/new-agreement-between-united-states-and-europe-will-compromise-privacy-rights**

Actualité (Google)

- Android 4.0 implémente complètement l'ASLR
  - http://permalink.gmane.org/gmane.comp.handhelds.android.security.discuss/1865
- Google renouvelle son support financier à Mozilla
  - http://www.linformaticien.com/actualites/id/22788/google-prolonge-finalement-son-soutien-a-firefox.aspx
- Google pose un brevet sur la voiture sans pilote
  - Espérons qu'il n'y ait pas de bogue dans le code !
    - http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=8,078,349.PN.&OS=PN/8,078,349&RS=PN/8,078,349
- La guerre des brevets continue
  - Google attaqué par BT
    - http://www.linformaticien.com/actualites/id/22773/bt-poursuit-google-sur-des-brevets.aspx

Actualité (Google)

- Google AppEngine en version finale
  - http://www.solutions-logiciels.com/actualites.php?actu=10808
- Le rachat de Motorola Mobile par Google
  - … suspendu par la commission européenne
    - http://www.linformaticien.com/actualites/id/22703/l-union-europeenne-suspend-le-rachat-de-motorola-par-google.aspx
- Mieux que la correction des bogues
  - La prédiction !
    - http://google-engtools.blogspot.com/2011/12/bug-prediction-at-google.html
- La blague de Noël
  - http://www.google.fr/search?q=let+it+snow

Actualité (Apple)

- Untethered Jailbreak pour iOS 5.0.1
  - Sauf iPhone 4S et iPad 2
    - http://www.greenpois0n.us/
  - Détails techniques
    - "Format string" dans un fichier de configuration Racoon
    - "Kernel Heap Overflow" dans le support HFS
    - http://pod2g-ios.blogspot.com/2012/01/details-on-corona.html
- Le vice-président en charge de la sécurité contraint de démissionner
  - Après la "fuite" de l'iPhone 4S
  - … il s'était fait passer pour un policier afin de fouiller la maison du suspect
    - http://9to5mac.com/2011/11/03/exclusive-apple-vice-president-of-global-security-john-theriault-departs-company-following-lost-iphone-4s-investigation/
- L'acte de création de la société Apple vendu aux enchères
  - Parti à $1,6 million !
    - http://www.linformaticien.com/actualites/id/22701/l-acte-fondateur-d-apple-vendu-pour-1-6-million-de-dollars.aspx

Actualité (crypto)

- Pourquoi révoque-t-on un certificat ?
  - Une analyse des CRLs sur l'année 2011
    - http://www.foo.be/cgi-bin/wiki.pl/2011-12-17_Certificate_Revocation_Reasons_2011

Actualité

- Conférences
  - 28C3
    - Attaque "HashDos"
      - Cf. MS11-100
    - La sécurité des réseaux GSM par pays
      - http://gsmmap.org/
    - "Global Grid Hackerspace": un réseau de satellites pour les hackers
      - http://shackspace.de/wiki/doku.php?id=project:hgg
    - Des français comme speakers
      - http://events.ccc.de/congress/2011/Fahrplan/

Actualité

- Sorties logicielles

  - SEAndroid
    - http://selinuxproject.org/page/SEAndroid
  - Cain 4.9.43
    - Support SAP R/3
    - Support MSCACHEv2
  - BlackBerry Mobile Fusion
    - "Coming in 2012"
      - http://press.rim.com/release.jsp?id=5285
  - SWFScan
    - http://h30499.www3.hp.com/t5/Following-the-White-Rabbit-A/SWFScan-FREE-Flash-decompiler/ba-p/5440167
  - FreeDOS 1.1

Actualité

- Ca sent le roussi pour Flash
  - Arrêt du produit Flash Catalyst par Adobe
    - http://www.linformaticien.com/actualites/id/22793/adobe-une-revolution-est-a-venir.aspx
- Ca sent le roussi pour RIM
    - http://www.linformaticien.com/actualites/id/22774/blackberry-la-descente-aux-enfers-de-rim.aspx
- BlueCoat racheté par un fond d'investissement
    - http://www.itnews.com.au/News/282938,blue-coat-acquired-by-equity-firm-for-us13-billion.aspx
- Oberthur aussi
    - http://www.zdnet.fr/actualites/oberthur-sur-le-point-d-etre-cede-au-fonds-advent-pour-plus-d-1-milliard-d-euros-39762905.htm

Actualité

- Intel: CA en baisse de $1 milliard sur le dernier trimestre
  - En cause: les inondations en Thaïlance et la chute des ventes de PC …
    - http://www.linformaticien.com/actualites/id/22727/1-milliard-de-dollars-de-ventes-en-moins-que-prevu-pour-intel-au-4eme-trimestre.aspx
- Intel remplacé par Marvell (ARM) dans les Google TV
    - http://www.linformaticien.com/actualites/id/22962/google-tv-intel-remplace-par-marvell-arm.aspx
- Intel compte sur le SoC "Medfield" pour se lancer sur le marché des tablettes
    - http://www.linformaticien.com/actualites/id/22797/intel-presente-des-prototypes-de-tablettes-et-smartphones-intel-inside.aspx

Divers

- Déjà qu'il est difficile de recruter …
  - http://1.61803398874.com/
- Tout le monde est d'accord: c'est indispensable
  - http://www.flickr.com/photos/girliemac/sets/72157628409467125/
- L'église de Kopimism reconnue par la Suède
  - http://www.linformaticien.com/actualites/id/22964/en-suede-le-partage-de-fichiers-est-une-religion.aspx
- L'ordinateur à 19€ pour bientôt
  - http://www.linformaticien.com/actualites/id/22833/raspberry-pi-l-ordinateur-a-19-euros-arrive.aspx

Divers

- RFC 6474
  - On va pouvoir ajouter sa date de décès dans sa vCard
    - http://tools.ietf.org/html/rfc6474
- Santa Gets Hacked!
    - http://vimeo.com/33402842
- Transformer "Optimus Prime" (Hasbro)
  - … porte plainte contre …
- "Eee Pad Transformer Prime" (Asus)

Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 14 février 2012