OSSIR
Groupe Paris

Réunion du 11 janvier 2011

Revue des dernières vulnérabilités

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

Avis Microsoft

- **Décembre 2010**
  - **17 bulletins, 40 failles**
  - **Références**
    - **http://blogs.technet.com/b/msrc/archive/2010/12/14/december-2010-security-bulletin-release.aspx**
    - **http://blogs.technet.com/b/srd/archive/2010/12/14/assessing-the-risk-of-the-december-security-updates.aspx**
    - **http://blogs.technet.com/b/msrc/p/december-2010-security-bulletin-q-a.aspx**
  - **MS10-090 Correctif cumulatif pour Internet Explorer [1,?,1,1,1,?,1]**
    - **Affecte: Internet Explorer (toutes versions supportées)**
    - **Exploit:**
      - **Exécution de code à l'ouverture d'une page Web**
      - **Violation de la SOP**
      - **http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=885**
      - **http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=886**

Avis Microsoft

- **Crédits:**
  - **Aniway / iDefense Labs**
  - **Nicolas Joly / VUPEN**
  - **Stephen Fewer / ZDI**
  - **Peter Vreugdenhil / ZDI**
  - **Yosuke Hasegawa**
  - **Jose Antonio Vazquez Gonzalez / iDefense Labs**
- **Remarques**
  - **Plusieurs failles avaient été exploitées avant la disponibilité du correctif**
  - **D'autres ont été reportées en mars 2010 ...**

Avis Microsoft

- MS10-091 Faille dans le support des polices OTF [1,1,2]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: exécution de code en mode noyau
    - Exploitable depuis un partage réseau (prévisualisation)
      - Sauf sur Windows XP et 2003
  - Crédits:
    - Marc Schoenefeld / Red Hat (x2)
    - Paul-Kenji Cahier Furuya

- MS10-092 Faille dans le Task Scheduler [1]
  - Affecte: Windows Vista / 2008 / Seven / 2008 R2
  - Exploit: élévation de privilèges locale
    - Exploitée par StuxNet
  - Crédits:
    - Sergey Golovanov, Alexander Gostev, Maxim Golovkin, Alexey Monastyrsky / Kaspersky
    - Vitaly Kiktenko, Alexander Saprykin / Design and Test Lab
    - Liam O Murchu / Symantec
    - Alexandr Matrosov, Eugene Rodionov, Juraj Malcho, David Harley / ESET

Avis Microsoft

- MS10-093 "DLL Preloading" dans Windows Movie Maker [1]
  - Affecte: Windows Vista / Movie Maker 2.6
  - Exploit: cf. "DLL Preloading"
  - Crédits: n/d
- MS10-094 "DLL Preloading" dans Windows Media Encoder [1]
  - Affecte: Windows Media Encoder 9
  - Exploit: cf. "DLL Preloading"
  - Crédits: n/d

Avis Microsoft

- MS10-095 "DLL Preloading" dans Windows [1]
  - Affecte: Windows Seven / 2008 R2
  - Exploit: "DLL preloading" lié à l'utilisation de la fonction BranchCache
    - .eml
    - .rss (Windows Live Mail)
    - .wpost (Microsoft Live Writer)
  - Crédits: Haifei Li / Fortinet

- MS10-096 "DLL Preloading" dans Windows Address Book [1]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: "DLL preloading" à l'ouverture d'un fichier ".wab"
  - Crédits:
    - Simon Raner / ACROS Security
    - HD Moore / Rapid7
    - Muhaimin Dzulfakar / NGS Software

Avis Microsoft

- MS10-097 "DLL Preloading" dans "Internet Connection Sign up Wizard" [1]
  - Affecte: Windows XP / 2003
  - Exploit: cf. "DLL Preloading"
  - Crédits: Muhaimin Dzulfakar / NGS Software

- MS10-098 Failles dans win32k.sys [1,1,2,2,1,1]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: élévation de privilèges
  - Crédits:
    - Tarjei Mandt / Norman (x4)
    - Stéfan Le Berre / Sysdream

Avis Microsoft

- MS10-099 Faille dans RRAS [1]
  - Affecte: Windows XP / 2003
    - Composant noyau NDProxy
    - http://msdn.microsoft.com/en-us/library/ff568322(VS.85).aspx
  - Exploit: élévation de privilèges
  - Crédits: Honggang Ren / Fortinet

- MS10-100 Faille dans UAC [1]
  - Affecte: Windows Vista / 2008 / Seven / 2008 R2
  - Exploit: élévation de privilèges
    - Le processus CONSENT.EXE accède de manière non sûre à des clés de base de registre
    - L'attaquant doit disposer du droit SeImpersonatePrivilege
  - Crédits: Cesar Cerrudo / Argeniss

Avis Microsoft

- MS10-101 Faille dans NetLogon [3]
  - Affecte: Windows 2003 / 2008 / 2008 R2
  - Exploit: déréférencement de pointeur NULL
    - Faille exploitable à travers le service RPC de NetLogon
  - Crédits: Matthias Dieter Wallnöfer, Andrew Bartlett / Samba

- MS10-102 Faille dans Hyper-V [2]
  - Affecte: Windows 2008 / 2008 R2
  - Exploit: déni de service de l'hôte depuis un invité
    - Au travers du VMBus
  - Crédits: HP, techit.de

Avis Microsoft

- MS10-103 Faille dans Publisher [1,1,2,2,3]
  - Affecte: Publisher (toutes versions supportées)
  - Exploit: exécution de code à l'ouverture d'un fichier ".pub"
  - Crédits: Chaouki Bekrar / VUPEN (x5)

- MS10-104 Faille dans SharePoint [1]
  - Affecte: SharePoint 2007 SP2
  - Exploit:
    - "Remote code execution in the security context of a guest user if an attacker sent a specially crafted SOAP request to the Document Conversions Launcher Service in a SharePoint server environment that is using the Document Conversions Load Balancer Service."
    - Nécessite l'accès au port TCP/8082 et/ou TCP/8093
    - Ne fonctionne que sur les installations stand-alone
    - http://blogs.technet.com/b/srd/archive/2010/12/14/ms10-104-sharepoint-2007-vulnerability.aspx
  - Crédits: Oleksandr Mirosh / ZDI

Avis Microsoft

- MS10-105 Faille dans Office Graphics Filters [1,2,2,2,2,2,2]
  - Affecte: Office (toutes versions supportées)
    - Y compris Works 9
    - Mais pas les versions Mac ni le pack de compatibilité
  - Exploit: exécution de code à l'ouverture d'un fichier malformé
    - Images de type .cgm, .pict, .tiff, FlashPix
      - http://blogs.technet.com/b/srd/archive/2010/12/14/ms10-105-image-filters-update.aspx
      - http://secunia.com/secunia_research/2009-30/
      - http://secunia.com/secunia_research/2009-31/
      - http://secunia.com/secunia_research/2009-32/
      - http://secunia.com/secunia_research/2009-33/
      - http://secunia.com/secunia_research/2009-34/
      - http://secunia.com/secunia_research/2009-39/
  - Crédits:
    - Yamata Li / Palo Alto Networks (x2)
    - Alin Rad Pop / Secunia Research
    - Carsten Eiram / Secunia Research (x3)
    - Dyon Balding / Secunia Research (x2)
  - Note:
    - Le correctif permet à Office d'utiliser le moteur GDI+ par défaut
    - Le correctif permet de blacklister des formats d'images peu utilisés
      - http://support.microsoft.com/kb/2479871

Avis Microsoft

- MS10-106 Faille dans Exchange [3]
  - Affecte: Exchange 2007 SP2 (uniquement)
  - Exploit: déni de service (boucle infinie)
    - Exploitable au travers d'une connexion RPC authentifiée
  - Crédits: Oleksandr Mirosh / ZDI

Avis Microsoft

- Prévisions Microsoft pour janvier
  - 2 failles affectant Windows (1 importante, 1 critique)

- Advisories
  - Q973811 "Extended Protection for Authentication"
    - V1.8: ajout de Microsoft Outlook
    - V1.9: finalement … non !
      - Des problèmes d'incompatibilité détectés
      - http://blogs.msdn.com/b/outlook/archive/2010/12/17/issues-with-the-recent-update-for-outlook-2007.aspx
  - Q2269637 "DLL Preloading"
    - V3.0: ajout des bulletins du mois
  - Q2458511 "0day" dans Internet Explorer
    - V2.0: adressé par MS10-090

Avis Microsoft

- Les failles en cours
  - http://blogs.technet.com/b/srd/archive/2011/01/07/assessing-the-risk-of-public-issues-currently-being-tracked-by-the-msrc.aspx
- Deux "0day" dans Internet Explorer
  - Source: WooYun.org
    - "*Plateforme de reporting vulnérabilité de la liberté et l'égalité*"
    - D'après la traduction automatique Google ☺
- Q2488013 Problème dans le support des feuilles de style
  - Conduisant à l'exécution de code arbitraire
  - Références:
    - Metasploit
    - http://www.wooyun.org/bugs/wooyun-2010-0885
    - http://blogs.technet.com/b/srd/archive/2010/12/22/new-internet-explorer-vulnerability-affecting-all-versions-of-ie.aspx
  - V1.0: publication
  - V1.1: exploitation "dans la nature"
- Q??? Contrôle ActiveX "WMI Administrative Tools"
  - http://www.exploit-db.com/exploits/15809/

Avis Microsoft

- **Q2490606 Exécution de code à l'ouverture d'une miniature malformée**
  - **Affecte: Windows (toutes versions supportées sauf Windows 7 / 2008 R2)**
  - **Exploit:**
    - ***Stack overflow* dans "shimgvw.dll"**
    - **Disponible dans Metasploit**
  - **Crédit:**
    - **Moti & Xu Hao / http://www.powerofcommunity.net/schedule.html**

- **Q??? Exécution de code à l'ouverture d'un fichier ".cov"**
  - **http://retrogod.altervista.org/9sg_cov_bof.html**

- **Q??? Déni de service sur FTP (IIS 7.5)**
  - **Très similaire à la récente faille ProFTPd …**
    - **http://blogs.technet.com/b/srd/archive/2010/12/22/assessing-an-iis-ftp-7-5-unauthenticated-denial-of-service-vulnerability.aspx**
    - **http://www.exploit-db.com/exploits/15803/**

Avis Microsoft

- **Révisions**
  - **MS10-070**
    - **V3.0: republication de la mise à jour pour .NET 4.0**
  - **MS10-077**
    - **V2.0: republication de la mise à jour pour .NET 4.0**
  - **MS10-083**
    - **V2.0: mauvaise interaction entre Windows Search 4.0 et Windows Vista / 2008**
  - **MS10-087**
    - **V2.0: les mises à jour pour Mac ont été publiées**
  - **MS10-090**
    - **V1.1: changement dans la logique de détection**
  - **MS10-105**
    - **V1.1: ce correctif n'est pas cumulatif avec MS10-087 (il faut installer les deux)**

Infos Microsoft

- **Sorties logicielles**
  - **La fonction Office 2010 "File Validation" sera backportée dans Office 2003 et 2007**
    - **Intègrera à terme des "signatures" de fichiers malveillants**
      - **http://blogs.technet.com/b/msrc/archive/2010/12/14/benefits-of-office-2010-file-validation-being-made-available-for-office-2003-and-2007.aspx**
      - **http://blogs.technet.com/b/msrc/archive/2010/12/14/more-about-the-office-file-validation-backport-plan.aspx**

Infos Microsoft

- **Autre**
  - **Microsoft PinPoint**
    - **Une place de marché Microsoft**
      - **http://pinpoint.microsoft.com/fr-FR/default.aspx**
  - **Microsoft Platform Ready**
    - **Idem … pour le Cloud**
      - **http://www.microsoftplatformready.com/fr/home.aspx**
  - **Hotmail et Windows Live peuvent être configurés en 100% SSL**
      - **https://account.live.com/ManageSSL**
  - **Une tablette Microsoft sous Windows 8 ?**
      - **http://bits.blogs.nytimes.com/2010/12/13/microsoft-to-announce-new-slates-targeting-ipad/**
  - **Windows 8 disponible pour processeurs ARM ?**
      - **http://www.bgr.com/2010/12/22/microsoft-to-announce-arm-compatible-windows-at-ces/**

Infos Réseau

- (Principales) faille(s)
  - ISC DHCPd < 4.2.0-P2
    - Déni de service
      - https://www.isc.org/software/dhcp/advisories/cve-2010-3616
  - OpenSSL < 0.9.8q, < 1.0.0c
    - *Downgrade* de chiffrement
    - Problème avec le protocole J-PAKE
      - http://www.openssl.org/news/secadv_20101202.txt
  - NoMachine NX utilise des clés SSH "en dur"
    - Ancien, mais toujours intéressant
      - http://www.nomachine.com/ar/view.php?ar_id=AR01C00126

Infos Réseau

- **Autres infos**
  - **L'ONU doit-il être chargé de maintenir l'ordre sur Internet ?**
    - **http://www.developpez.com/actu/25882/Des-pays-proposent-que-l-ONU-soit-charge-de-maintenir-l-ordre-sur-Internet-dont-la-Chine-l-Inde-et-l-Arabie-Saoudite/**

Infos Unix

- (Principales) faille(s)
  - Redmine < 1.0.5
    - Plusieurs failles, dont une exécution de commandes
      - http://www.redmine.org/news/49
  - libc/regcomp
    - Affecte ProFTPd, par exemple
      - http://securityreason.com/achievement_securityalert/93
  - PHP < 5.3.5, < 5.2.17
    - Plusieurs failles de sécurité critiques corrigées
      - Ex. erreur dans le support des flottants
      - http://www.php.net/ChangeLog-5.php
    - Note: mbfl_strcut() permet de lire toute la mémoire
      - http://www.doecirc.energy.gov/bulletins/t-493.shtml
  - OpenSC
    - Buffer overflow si le numéro de série de la carte à puce insérée est trop long (!)

Infos Unix

- TYPO3
  - Plusieurs failles de sécurité corrigées
    - http://typo3.org/teams/security/security-bulletins/typo3-sa-2010-022/
- Django
  - Idem
    - http://www.djangoproject.com/weblog/2010/dec/22/security/
- SPIP < 2.1.5
- MediaWiki < 1.16.1
- J!People pour Joomla
  - Injection SQL
    - http://blog.zerial.org/seguridad/0-day-sql-injection-en-sitio-web-de-joomla/
- MantisBT < 1.2.4
  - Faille "include" (et quelques XSS)
    - http://www.mantisbt.org/bugs/changelog_page.php?project=mantisbt&version=1.2.4
- WordPress < 3.0.4
  - Problèmes identifiés dans le filtre anti-XSS générique
    - http://wordpress.org/news/2010/12/3-0-4-update/

Infos Unix

- Apache Subversion < 1.6.15
  - Déni de service distant
    - http://svn.haxx.se/dev/archive-2010-11/0475.shtml
- phpMyFaq backdooré
    - http://www.phpmyfaq.de/advisory_2010-12-15.php
- mod_mono pour Apache
  - Le code source des pages ASP.NET peut fuiter sous certaines conditions
    - http://www.mono-project.com/Vulnerabilities#XSP.2Fmod_mono_source_code_disclosure
- Evince
  - Exécution de code à l'ouverture d'un fichier DVI
    - http://git.gnome.org/browse/evince/commit/?id=d4139205b010ed06310d14284e63114e88ec6de2

Infos Unix

- Noyau Linux
  - Elévation de privilèges locale (entre 2.6.33 et 2.6.36.1) via debugfs et ACPI
    - https://bugzilla.redhat.com/show_bug.cgi?id=66345
  - Contournement de *mmap_min_addr* par *install_special_mapping*
    - http://xorl.wordpress.com/2010/12/09/tavisos-install_special_mapping-bypass-for-mmap_min_addr/

Infos Unix

- Autre

  - Une backdoor implantée dans la pile IPSEC d'OpenBSD
    - … par le FBI il y a 10 ans ?
    - Le troll fait rage ☺
      - http://marc.info/?l=openbsd-tech&m=129236621626462&w=2
      - http://blogs.csoonline.com/1296/an_fbi_backdoor_in_openbsd
    - Pas de conclusion évidente
      - http://marc.info/?l=openbsd-tech&m=129296046123471&w=2
      - …
      - (g) I believe that NETSEC was probably contracted to write backdoors as alleged.
      - (h) If those were written, I don't believe they made it into our tree. They might have been deployed as their own product.
      - …

Infos Unix

- Un mainteneur du paquet Ruby dans Debian jette l'éponge
  - Et balance sur Ruby au passage
    - http://www.lucas-nussbaum.net/blog/?p=617
- Trolls en cours
  - *False Boundaries and Arbitrary Code Execution*
    - http://forums.grsecurity.net/viewtopic.php?f=7&t=2522
  - *Assorted Notes on Defense and Exploitation*
    - http://forums.grsecurity.net/viewtopic.php?f=7&t=2521
- Autre lecture d'intérêt
    - http://justanothergeek.chdir.org/2010/12/la-securite-sous-linux-un-plus-tard.html

Failles

- **Principales applications**
  - **Lecture de n'importe quel fichier local avec Flash**
    - **http://xs-sniper.com/blog/2011/01/04/bypassing-flash%E2%80%99s-local-with-filesystem-sandbox/**
  - **Chrome < 8.0.552.224**
    - **http://googlechromereleases.blogspot.com/2010/12/stable-beta-channel-updates_13.html**
  - **Opera < 11**
    - **Failles multiples, non documentées sauf:**
      - **http://www.opera.com/support/kb/view/977/**
      - **http://www.opera.com/support/kb/view/979/**

Failles

- Mac OS X < 10.6.6
  - http://support.apple.com/kb/HT4498
- Apple Time Capsule < 7.5.2, Airport Extreme < 7.5.2
  - 5 failles corrigées, dont une faille vieille de 2 ans …
    - http://lists.apple.com/archives/security-announce/2010/Dec/msg00001.html
    - http://support.apple.com/kb/HT4298
- VLC < 1.1.6
  - http://www.videolan.org/security/sa1007.html
- VMWare
  - Faille dans l'authentification SFCB
    - http://www.vmware.com/security/advisories/VMSA-2010-0020.html
    - http://www.vmware.com/security/advisories/VMSA-2011-0001.html

Failles

- Injection de commandes dans Citrix Access Gateway
  - http://support.citrix.com/article/CTX127613
  - http://seclists.org/fulldisclosure/2010/Dec/540
- Traitement des fichiers PDF sur BlackBerry Attachment Server
  - http://www.blackberry.com/btsc/search.do?cmd=displayKC&docType=kc&externalId=KB24761
- Sophos SafeGuard (ex. Utimaco)
  - Utilisation de secrets "périmés"
    - http://www.sophos.com/support/knowledgebase/article/112655.html
- Symantec Endpoint Protection version 11
  - Faille dans l'application PHP exploitable par un client géré
    - http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=2010&suid=20101215_00
    - http://www.zerodayinitiative.com/advisories/ZDI-10-291/

Failles 2.0

- Cross_fuzz, un nouveau *fuzzer* dévastateur pour les navigateurs
  - Pourquoi le diffuser maintenant ? Parce que les chinois ont déjà les failles …
    - http://lcamtuf.blogspot.com/2011/01/announcing-crossfuzz-potential-0-day-in.html
- Facebook encourage la recherche "responsable" de failles dans ses services
    - http://www.scmagazineus.com/facebook-updates-bug-disclosure-policy/article/193090/
- FireFox 4 n'implémentera pas les WebSockets
  - Fonction jugée trop dangereuse en l'état
    - http://www.0xdeadbeef.com/weblog/2010/12/disabling-websockets-for-firefox-4/
- Indisponibilité massive du site Twitter
    - http://status.twitter.com/
- Indisponibilité massive du réseau Skype
  - Suite à une mise à jour boguée
    - http://blogs.skype.com/en/2010/12/skype_downtime_today.html
- Indisponibilité de Bank of America
  - Suite de l'affaire WikiLeaks

Failles 2.0

- **Sites compromis**
  - **Les mots de passe Gawker ne sont pas meilleurs que les autres …**
    - **#1 "123456"**
    - **#2 "password"**
    - **#3 "12345678"**
      - **http://blogs.wsj.com/digits/2010/12/13/the-top-50-gawker-media-passwords/**
  - **Addons.mozilla.org**
    - **40,000 comptes dans un fichier accessible à tous**
      - **http://blog.mozilla.com/security/2010/12/27/addons-mozilla-org-disclosure/**
  - **McDonald's**
    - **Accès à une base de données clients**
      - **http://www.linformaticien.com/Actualit%C3%A9s/tabid/58/newsid496/9782/vol-de-donnees-clients-chez-mcdonald-s/Default.aspx**
  - **CitySight NY**
    - **Accès à toutes les CB/CVV des clients par une injection SQL**
      - **http://doj.nh.gov/consumer/pdf/twin_america.pdf**
  - ***IBM Developer Works***
      - **http://zone-h.org/mirror/id/12878142**

Failles 2.0

- Base de données des clients Vodafone (y compris les n°CB)
  - Pas d'intrusion, juste un sous-traitant indélicat
    - http://slashdot.org/story/11/01/09/1325239/Vodafone-Customer-Database-Breached
- "0wned & Exposed n°2"
  - Carders.cc
  - inj3ct0r
  - SourceForge
  - Exploit-DB
  - BackTrack
  - Free-Hack
    - http://www.exploit-db.com/papers/15823/
- Mais aussi …
  - Scrollwars.com
  - HellRising.com

Malwares et spam

- Un BotNet sur Android: Geinimi
  - Source: un jeu infecté (pas de capacité de propagation)
    - http://blog.mylookout.com/2010/12/geinimi_trojan/
- Un virus se propage sur Facebook
    - http://www.theregister.co.uk/2011/01/10/facebook_worm_photo_chat_scam/
- Les produits F-Secure vulnérables au "DLL Preloading"
    - http://www.f-secure.com/en_EMEA/support/security-advisory/fsc-2010-4.html
- StuxNet n'est pas que virtuel
    - http://www.debka.com/article/20406/

Malwares et spam

- 4 chinois arrêté pour avoir envoyé 10 millions de spams "sans autorisation"
  - http://french.china.org.cn/china/txt/2011-01/05/content_21679880.htm
- Un ancien spammeur reconverti dans les poursuites judiciaires contre les spammeurs
  - http://danhatesspam.com
- La saison des prédictions pour 2011
  - http://www.sans.edu/resources/securitylab/security_predict2011.php
  - http://community.websense.com/blogs/securitylabs/archive/2010/12/17/five-security-predictions-for-2011.aspx
  - Etc.
- Ainsi que des rétrospectives
  - http://blog.trendmicro.com/2010s-most-dangerous-list/
  - http://press.pandasecurity.com/wp-content/uploads/2010/05/PandaLabs-Annual-Report-2010.pdf

Actualité (francophone)

- Revente du fichier de cartes grises
  - La polémique enfle
    - http://www.cnil.fr/la-cnil/actu-cnil/article/article/fichier-des-cartes-grises-les-automobilistes-ont-le-droit-de-sopposer-a-la-revente-de-leurs-d/
- La politique publique d'intelligence économique
    - http://www.economie.gouv.fr/actus/10/101208conseil-ministres-intelligence-economique.html
- La France championne du monde de l'espionnage industriel
    - http://www.lemonde.fr/documents-wikileaks/article/2011/01/04/wikileaks-l-espionnage-economique-de-paris-derange-ses-allies-europeens_1460661_1446239.html#ens_id=1460691
- 4chan déclare la guerre à la France
    - http://www.lepost.fr/article/2011/01/04/2359263_4chan-declare-la-guerre-a-la-france-pourrissons-leurs-sites.html
- *Shit happens*
    - http://www.ladepeche.fr/article/2010/12/15/970868-Les-Chinois-victimes-d-espions-francais.html

Actualité (francophone)

- Nicolas Sarkozy souhaite une loi "HADOPI 3"
  - http://twitter.com/Maitre_Eolas/status/15396074558595072
  - http://twitter.com/pressecitron/status/15401160915554304

- La nouvelle LOPPSI votée
  - Filtrage discrétionnaire et secret des sites "pédopornographiques"
    - Pour …
      - http://blog.crimenumerique.fr/2010/02/07/blocage-des-sites-pedopornographiques-suite/
    - Et contre …
      - http://www.pcinpact.com/actu/news/60884-hadopi-loppsi-blocage-site-ciotti.htm
      - http://www.laquadrature.net/fr/loppsi-censure-administrative-du-net-adoptee-les-pedophiles-sont-tranquilles
  - Création d'un délit d'usurpation d'identité
    - http://www.linformaticien.com/Actualit%C3%A9s/tabid/58/newsid496/9811/loppsi-2-le-delit-d-usurpation-d-identite-sur-le-web-est-cree/Default.aspx
  - Etc.

- Le décret sur les "moyens de sécurisation HADOPI" voté
  - http://www.pcinpact.com/actu/news/61037-verrou-labellise-label-moyens-securisation.htm

Actualité (francophone)

- "Protocole de coopération pour la protection des données personnelles des consommateurs sur internet"
  - Entre la CNIL et DGCCRF
    - http://www.economie.gouv.fr/presse/dossiers_de_presse/110106protocole_dataperso_web.pdf

- Une loi pour donner un sens au "confidentiel entreprise"
    - http://www.lefigaro.fr/actualite-france/2010/12/20/01016-20101220ARTFIG00590-une-loi-pour-proteger-le-secret-des-affaires.php

- La CNIL convoque Google
    - http://www.numerama.com/magazine/17774-la-cnil-auditionne-google-dans-le-cadre-d-une-enquete-sur-street-view.html

Actualité (anglo-saxonne)

- National Strategy for Trusted Identities in Cyberspace
  - http://www.whitehouse.gov/blog/2011/01/07/national-program-office-enhancing-online-trust-and-privacy
- LiPoSe (Lightweight Portable Security)
  - La distribution sécurisée de l'armée américaine
    - http://spi.dod.mil/lipose.htm
- Un sheriff du Colorado "égare" la base de données des 200,000 informateurs de la police
  - http://www.npr.org/templates/story/story.php?storyId=131970302
- Tous les militaires américains auront un iPhone/iPod de fonction
  - Avec les applications "qui vont bien", comme "Bullet Flight" ☺
    - http://www.bestofmicro.com/actualite/28657-iPhone-iPod-Armee.html

Actualité (européenne)

- ***Good Practice Guide for Incident Management***
  - **http://www.enisa.europa.eu/act/cert/support/incident-management/files/good-practice-guide-for-incident-management/at_download/fullReport**

- ***Commission's Communication on Interoperability***
  - **http://ec.europa.eu/isa/strategy/doc/110113__iop_communication_annex_eif.pdf**

Actualité (Google)

- Le réseau social Google Me repoussé
  - http://www.developpez.com/actu/24512/Google-Me-ne-sortira-pas-en-2010-mais-en-2011-le-projet-est-retarde-suite-a-des-desaccords-concernant-son-design/
- Un site Google vraiment utile ☺
  - http://www.teachparentstech.org/
- Un autre site Google vraiment distrayant
  - http://ngrams.googlelabs.com/
- Google Body
  - Requière WebGL
    - http://bodybrowser.googlelabs.com/

Actualité (Google)

- Chrome OS approche
  - http://www.google.com/chromeos/demolab/
- Google Wave devient Apache Wave
  - http://googlewavedev.blogspot.com/2010/12/introducing-apache-wave.html
- La saga du "Spy-Fi" continue
  - http://www.politico.com/news/stories/1210/46641.html

Actualité (crypto)

- Extraction de clés privées depuis un token CryptoFlex
  - http://www.spms.ntu.edu.sg/Asiacrypt2010/Rump%20Session-%207%20Dec%202010/AC2010_rump_IL.pdf
- Les processeurs Intel de la gamme "Sandy Bridge" intègrent une carte vidéo et des clés de chiffrement
  - Technologie "Insider"
  - Objectif annoncé: protéger du contenu multimédia de bout en bout
    - http://www.zdnet.fr/actualites/processeurs-intel-sandy-bridge-protection-materielle-integree-contre-le-piratage-39757191.htm
- Un consortium bancaire demande le retrait de la thèse "*Chip & PIN is broken*"
  - http://www.lightbluetouchpaper.org/2010/12/25/a-merry-christmas-to-all-bankers/
- EPIC FAIL de la PlayStation 3
  - La mise en œuvre de ECDSA permet de récupérer la clé privée
  - Présenté lors de la conférence 27c3
  - Voir aussi:
    - http://geohot.com/

Actualité

- Sorties logicielles
  - Metasploit 3.5.1
    - Nouvelles attaques Cisco & IPv6
    - Contournement de DEP/ASLR sur Internet Explorer grâce à .NET Framework 2.0
      - http://blog.metasploit.com/2010/12/metasploit-framework-351-released.html
  - INSECT 1.0
    - Une plateforme d'attaque … assez minimaliste
      - http://www.insecurityresearch.com/
  - OSSTMM 3.0
      - http://www.isecom.org/osstmm/
  - Secunia PSI 2.0
  - MySQL 5.5
  - Little Black Box
    - Une base de données des clés SSL "en dur"
      - http://code.google.com/p/littleblackbox/

Actualité

- **Conférence 27c3 à Berlin**
  - **Ma sélection personnelle**
    - **https://events.ccc.de/congress/2010/Fahrplan/**
  - **Jour 1**
    - **Désobfuscation**
      - **https://events.ccc.de/congress/2010/Fahrplan/events/4096.en.html**
    - ***JTAG/Serial/FLASH/PCB Embedded Reverse Engineering***
      - **https://events.ccc.de/congress/2010/Fahrplan/events/4011.en.html**
    - **USB**
      - **https://events.ccc.de/congress/2010/Fahrplan/events/4234.en.html**
    - **Smart Phones**
      - **https://events.ccc.de/congress/2010/Fahrplan/events/4265.en.html**
    - **IPv6**
      - **https://events.ccc.de/congress/2010/Fahrplan/events/3957.en.html**
    - **StuxNet**
      - **https://events.ccc.de/congress/2010/Fahrplan/events/4245.en.html**
    - **SAP**
      - **https://events.ccc.de/congress/2010/Fahrplan/events/4082.en.html**

Actualité

- Jour 2
  - Building Custom Disassemblers
    - https://events.ccc.de/congress/2010/Fahrplan/events/4061.en.html
  - Backdooring Embedded Controllers
    - https://events.ccc.de/congress/2010/Fahrplan/events/4174.en.html
- Jour 3
  - *Source routing* vs. SIP
    - https://events.ccc.de/congress/2010/Fahrplan/events/4181.en.html
  - PlayStation 3
    - https://events.ccc.de/congress/2010/Fahrplan/events/4087.en.html
  - RFID EasyCard
    - https://events.ccc.de/congress/2010/Fahrplan/events/4036.en.html
- Jour 4
  - PDF obfuscation
    - https://events.ccc.de/congress/2010/Fahrplan/events/4221.en.html
  - *Internet sees you*
    - https://events.ccc.de/congress/2010/Fahrplan/events/4301.en.html
  - Amélioration de l'attaque sur WEP
    - https://events.ccc.de/congress/2010/Fahrplan/events/4261.en.html
  - RTP
    - https://events.ccc.de/congress/2010/Fahrplan/events/4193.en.html

Actualité

- *Lightning Talks*
  - http://events.ccc.de/congress/2010/wiki/Lightning_Talks
  - "SAP vs. Sanity"
  - "Domain Cached Credentials"
  - "A GPU Exploit"
  - "Problems of the Criminalisation of Aviation Accidents"
  - "Console Hacking 2010: PS3 Demo"
  - http://incubator.apache.org/alois/
- Et à part ça … aucun système sous Mac OS X / Apple iOS ne pouvait se connecter au réseau
  - http://events.ccc.de/congress/2010/wiki/0day_Mystery_Challenge

Actualité

- Mac App Store piraté
  - http://www.20minutes.fr/article/649228/high-tech-le-mac-app-store-perd-verrous
- SourceFire rachète Immunet
  - http://blog.immunet.com/blog/2011/1/5/immunet-acquired-by-sourcefire.html
- L'avenir de Java incertain
  - Apache quitte le Java Community Process
    - http://www.jimjag.com/imo/index.php?/archives/242-The-JCP-Is-Dead.html
- La Russie abandonne Windows pour Mandriva
  - http://www.infoguerre.fr/edito/russie-s%E2%80%99associe-entreprise-francaise-dans-bataille-contre-microsoft-mandriva/
- Un consortium Microsoft - Oracle - Apple - EMC rachète les brevets détenus par Novell
  - http://www.bundeskartellamt.de/wDeutsch/zusammenschluesse/zusammenschluesse.php

Actualité

- Les processeurs Intel vendus en 2011 auront un "kill switch"
  - Activable à distance à travers la 3G machine éteinte
    - http://isc.sans.edu/diary.html?storyid=10111
- Skype bientôt interdit en Chine ?
    - http://www.reuters.com/article/idUSTOE6BU02120101231
- La Chine lance le développement d'un système d'exploitation "compatible Windows"
    - http://french.people.com.cn/Sci-Edu/7234633.html
- La Chine arrête 460 "hackers"
    - http://www.lemagit.fr/article/securite-piratage-chine-wikileaks/7607/1/la-chine-affirme-avoir-arrete-460-hackers-entre-janvier-novembre/

Fun

- $ whois afnic.fr | head

```
%%                                          *    .        *     *
%% This is the AFNIC Whois server.  *           .   .  /.\       .
%%                                                .        /.^'\  *
%% complete date format : DD/MM/YYYY    *         *    /'.'\
%% short date format    : DD/MM       .        *      /.^'.'\     .
%% version              : FRNIC-2.5              .   .  /'.^'.\   .
%%                                          *          ^^|_|^^     *
```

- Cryptique ☺

```
tee >(sed -e s/c/d/ -e s/Vy/dy/ | base64 -d | md5sum 1>&2)
<<<DjBlYVWap4fQC8b3C73+NATPA2WecE+FNMAP+2WcTIdAzJQv6y2hFaP0FVy7hgdJc4ZlbX0fNKQg
WdePWo3R7w== | base64 -d | md5sum
```

Fun

- Stocker des données … dans l'ADN des bactéries
  - http://bruneitimes.com.bn/features/2011/01/10/hong-kong-researchers-store-data-bacteria
- Un procès pas comme les autres
  - http://www.tgdaily.com/security-features/51920-worlds-hottest-female-hacker-appears-in-nyc-court
- Le BlueScreen réinventé
  - http://www.pauldestieu.com/landscape.php
- LoseThos
  - Un système d'exploitation 64 bits complet
  - Une seule personne … pendant 7 ans
    - http://www.losethos.com/

Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 8 février 2011
- N'hésitez pas à proposer des sujets et des salles