OSSIR
Groupe Paris

Réunion du 12 mai 2009

Revue des dernières vulnérabilités

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

Avis Microsoft (1/14)

- **Correctifs d'Avril 2009**
  - **Avec [*exploitability index*]**
    - **http://blogs.technet.com/srd/archive/2009/04/14/prioritizing-the-deployment-of-the-april-security-bulletins.aspx**
    - **http://blogs.technet.com/msrc/archive/2009/04/14/april-2009-monthly-bulletin-release.aspx**
  - **MS09-009 Failles Excel (x2) [2,1]**
    - **Affecte: Excel (toutes versions supportées)**
    - **Exploit:**
      - **L'une des deux failles est exploitée dans la nature en "0day"**
    - **Crédit: Haifei Li / Fortinet**

Avis Microsoft (2/14)

- MS09-010 Failles dans les convertisseurs de documents (x4) [1,2,1,1]
  - Affecte:
    - Wordpad sur Windows 2000 / XP / 2003
    - Office 2000 / XP
  - Exploit:
    - Convertisseurs Word 6, Word 97 et WordPerfect 6
    - L'une des failles est exploitée dans la nature en "0day"
    - http://blogs.technet.com/srd/archive/2009/04/14/ms09-010-reducing-the-text-converter-attack-surface.aspx
  - Crédit:
    - Sean Larsson & Jun Mao / iDefense Labs
    - Fortinet
    - iDefense
      - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=782
      - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=783
      - 06/28/2006 - Initial Contact
      - (...)
      - 04/14/2009 - Coordinated Public Disclosure

Avis Microsoft (3/14)

- MS09-011 Faille dans le support MJPEG [2]
  - Affecte: DirectX 8.1 – 9.0c
  - Exploit: exécution de code via un fichier MJPEG malformé
    - http://www.piotrbania.com/all/adv/ms-directx-mjpeg-adv.txt
  - Crédit: Piotr Bania / Kryptos Logic

Avis Microsoft (4/14)

- MS09-012 Protections contre le *Token Kidnapping* (x4) [1,1,1,1]
  - Affecte: Windows (toutes versions supportées)
    - Composants: MSDTC / WMI providers / RPCSS / Thread Pools
    - Exploitable via IIS ou SQL Server par exemple (toutes versions)
  - Exploit: élévation de privilèges
    - Utilisateur standard vers LocalService / NetworkService
    - LocalService / NetworkService vers SYSTEM
    - "Addressing this issue required one of the most epic engineering efforts (...)"
      - http://blogs.technet.com/srd/archive/2009/04/14/ms09-012-fixing-token-kidnapping.aspx
      - http://blogs.technet.com/msrc/archive/2009/04/14/token-kidnapping.aspx
    - Attention ! Toutes les protections ne sont pas actives par défaut !
    - Lire attentivement:
      - http://support.microsoft.com/kb/956572
  - Crédit: Cesar Cerrudo / Argeniss
    - Code d'exploitation publié il y a 2 ans

Avis Microsoft (5/14)

- **MS09-013 Failles multiples dans le client WinHTTP (x3) [1,1,1]**
  - **Affecte: Windows (toutes versions supportées)**
  - **Exploit:**
    - **Exécution de code via une faille d'implémentation (*integer underflow*)**
    - **Validation incorrecte de certificats**
    - ***Credential Reflection* via l'authentification HTTP NTLM**
    - **http://blogs.technet.com/srd/archive/2009/04/14/ntlm-credential-reflection-updates-for-http-clients.aspx**
  - **Crédit:**
    - **Greg MacManus / iSight**
    - **Wan-Teh Chang & Cem Paya / Google**

Avis Microsoft (6/14)

- **MS09-014 Correctif cumulatif pour IE (x6) [3,1,2,3,3,1]**
  - **Affecte: IE (toutes versions supportées sauf IE 8)**
  - **Exploit:**
    - ***Carpet Bombing***
    - ***Credential Reflection***
    - **Corruption mémoire sur une transition de page**
    - ***Use-after-free* (x3)**
    - **http://blogs.technet.com/srd/archive/2009/04/14/ntlm-credential-reflection-updates-for-http-clients.aspx**
  - **Crédit:**
    - **Aviv Raff**
    - **Michal Zalewski / Google**
    - **Ivan Fratric / iSight**
    - **Skylined / Google**
    - **ADLab / VenusTech**

Avis Microsoft (7/14)

- **MS09-015 Correction de l'ordre de recherche des DLL [2]**
  - **Affecte: Windows (toutes versions supportées)**
  - **Exploit: *Carpet Bombing* (ex. Safari)**
  - **Crédit: Aviv Raff**

- ***Carpet Bombing* ?**

  - **Utilisation des APIs SetDllDirectory() et SetSearchPathMode() par IE**
    - **http://msdn.microsoft.com/en-us/library/ms686203(VS.85).aspx**
    - **http://msdn.microsoft.com/en-us/library/dd266735(VS.85).aspx**
  - **Conséquence: le répertoire système est toujours en premier dans la recherche des DLL (pour IE uniquement)**

  - **Attention: la protection n'est pas active par défaut (!)**
    - **Il faut activer la *feature* FEATURE_ENABLESEARCHPATH_KB963027**

  - **Voir:**
    - **FAQ du correctif MS09-014**
    - **http://blogs.technet.com/srd/archive/2009/04/14/ms09-014-addressing-the-safari-carpet-bomb-vulnerability.aspx**

Avis Microsoft (8/14)

- MS09-016 Failles ISA Server / ForeFront TMG (x2) [3,3]
  - Affecte: toutes versions supportées (sauf ISA 2000 SP2)
  - Exploit:
    - Déni de service sur le proxy Web
      - Nécessite au moins un site publié
      - ISA en mode pare-feu uniquement n'est pas vulnérable
    - XSS via cookieauth.dll
  - Crédit: New York State Chief Information Officer

Avis Microsoft (9/14)

- 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
  - Autres mises à jour notables sur Windows Update
    - Internet Explorer 8
    - Office 2007 SP2
    - Windows Live Messenger (mise à jour non sécurité)
      - http://support.microsoft.com/kb/961503

Avis Microsoft (10/14)

- Modification du fonctionnement AutoPlay/AutoRun sur les périphériques amovibles
  - Affecte Windows Seven RC
  - Et bientôt Windows XP et Vista
    - http://blogs.technet.com/srd/archive/2009/04/28/autorun-changes-in-windows-7.aspx

Avis Microsoft (11/14)

- **Autres failles**
  - **Republication du DoS dans Media Player**
    - **http://blogs.technet.com/srd/archive/2009/04/14/prioritizing-the-deployment-of-the-april-security-bulletins.aspx**
  - **Faille dans le contrôle ActiveX "WhlMgr.dll"**
    - **http://osvdb.org/show/osvdb/53933**
  - **Faille dans Windows Live Messenger**
    - **Affecte: WLM 2009**
    - **Exploit: déni de service via un jeu de caractères malformé**
      - **http://xforce.iss.net/xforce/xfdb/48810**
  - **Faille dans le support GZIP**
    - **Affecte: Services for Unix (inclus dans Windows 2008)**
    - **Exploit: http://secunia.com/advisories/34428/**
  - **Faille "noyau" exploitée dans la nature (x2)**
    - **http://www.avertlabs.com/research/blog/index.php/2009/04/09/windows-kernel-again-found-vulnerable/**
    - **Affecte: win32k.sys et atapi.sys**

Avis Microsoft (12/14)

- Advisories
  - 968272
    - Version 3.0: publication de MS09-009
  - 960715
    - Version 1.1: Windows 2008 Core n'est pas affecté
  - 960906
    - Version 2.0: publication de MS09-010
  - 953818
    - Version 2.0: publication de MS09-014 & MS09-015
  - 951306
    - Version 3.0: publication de MS09-012

Avis Microsoft (13/14)

- **Prévisions pour Mai 2009**
  - **1 bulletin critique affectant toutes les versions de PowerPoint**
- **Révisions**
  - **MS08-076**
    - **Version 4.0: Windows Media Services sur Windows 2008 SP2 est affecté**
  - **MS08-069**
    - **Version 2.0: XML Core Services 4.0 sur Windows Vista SP2 / 2008 SP2 sont affectés**
  - **MS09-009**
    - **Version 1.1: correction du tableau MBSA / SMS**
  - **MS09-010**
    - **Version 1.1: le *workaround* doit être désactivé avant l'installation du correctif**
  - **MS09-011**
    - **Version 1.1: DirectX 7 n'est pas affecté**

Avis Microsoft (14/14)

- MS09-012
  - Version 1.1: correction de la FAQ
  - Version 1.2: documentation de problèmes connus
  - Version 2.0: problème avec Windows 2000 SP4 Norvégien
- MS09-013
  - Version 1.1: documentation de problèmes connus
- MS09-014
  - Version 1.1: mise à jour de la FAQ
  - Version 1.2: mise à jour de la FAQ sur Windows 2000
- MS09-015
  - Version 1.1: mise à jour de la FAQ
- MS09-016
  - Version 1.1: erreur dans la clé de base de registre

Infos Microsoft (1/4)

- **Sorties logicielles**

  - **Windows Seven RC1**
    - **Version active jusqu'en mars 2010**
      - **Entre mars 2010 et juin 2010 le système s'éteindra toutes les 2h ☺**
    - **Une version finale dès le 23 octobre ?**
    - **Attention aux versions disponibles sur BitTorrent !**
      - **http://www.slashgear.com/leaked-windows-7-rc-torrents-infected-with-trojan-2842048/**
    - **Fail, already ?**
      - **Masquage des doubles extensions:**
        - **http://www.f-secure.com/weblog/archives/00001675.html**
      - **Bogue sur les droits:**
        - **http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9132738**

Infos Microsoft (2/4)

- Et aussi ...
  - Windows 2008 R2 RC1
  - Windows Vista & 2008 SP2 (final)
  - Exchange 2010 Beta
  - SQL Server 2008 SP1 CTP
  - SharePoint Designer 2007 devient gratuit
  - WSUS 2.0 SP1 en fin de support
- Windows Server 2008 "Foundation"
  - Un nouveau venu pour les PME < 15 personnes ...
    - http://www.microsoft.com/windowsserver2008/en/us/foundation.aspx
- Watcher: un plugin Fiddler pour automatiser la recherche de failles Web
  - http://websecuritytool.codeplex.com/

Infos Microsoft (3/4)

- **Autre**
  - **Microsoft Security Intelligence Report, volume 6**
    - **http://www.microsoft.com/sir**
    - **http://www.microsoft.com/downloads/details.aspx?FamilyID=aa6e0660-dc24-4930-affd-e33572ccb91f**
  - **ISA Server 2006 obtient la certification EAL4+**
    - **http://blogs.technet.com/stanislas/archive/2009/03/09/isa-server-2006-standard-et-entreprise-obtiennent-la-certification-cc-eal4.aspx**
  - **"Project Quant": une métrique pour la gestion des patches**
    - **http://blogs.zdnet.com/security/?p=3151**
    - **http://securosis.com/projectquant**

Infos Microsoft (4/4)

- MSDN Code Search
  - http://msdn.krugle.com/
- "Vista SP2 est le système le plus sûr et le plus stable de tous les OS actuels"
  - Source: Microsoft
  - http://www.microsoft.com/presspass/exec/turner/2009/04-06MMCIOSummit.mspx
- Communication Microsoft, *again*
  - http://technet.microsoft.com/fr-fr/sqlserver/dd787700.aspx
- Le bar du campus Microsoft ferme avant d'avoir ouvert
  - http://slashdot.org/article.pl?sid=09/04/11/224237

Infos Réseau

- **BIND 10 en chantier**
  - **https://www.isc.org/bind10**
- **L'ARIN met la pression pour le passage à IPv6**
  - **http://isc.sans.org/diary.html?storyid=6301**
- **5 failles dans le pare-feu Cisco PIX/ASA**
  - **http://www.cisco.com/en/US/products/products_security_advisory0918 6a0080a994f6.shtml**
    - ***VPN Authentication Bypass when Account Override Feature is Used vulnerability***
    - ***Crafted HTTP packet denial of service (DoS) vulnerability***
    - ***Crafted TCP Packet DoS vulnerability***
    - ***Crafted H.323 packet DoS vulnerability***
    - ***SQL*Net packet DoS vulnerability***
    - ***Access control list (ACL) bypass vulnerability***

Infos Unix

- Actualité
  - OpenBSD 4.5
    - http://www.openbsd.org/45.html
  - Snort 2.8.4 est sorti
    - Une sortie notable car le format des signatures change
      - Pour le protocole DCE/RPC
    - Et les anciennes signatures ne sont plus supportées
      - http://isc.sans.org/diary.html?storyid=6151
  - Debian ajoute le noyau FreeBSD dans les architectures supportées
    - http://lists.debian.org/debian-devel-announce/2009/04/msg00001.html

Infos Unix

- apt-p2p pour passer à Ubuntu 9.04
  - http://blog.chenhow.net/os/linux/ubuntu/using-apt-p2p-for-faster-upgrades-from-intrepid-to-jaunty/
- Une pub pour Linux
  - http://video.linuxfoundation.org/video/1106
- Gnome Shell
  - http://live.gnome.org/GnomeShell
  - "GNOME Shell will use the OpenGL-based Clutter for rendering, and is written primarily in Javascript."

Infos Unix

- **Failles**
  - **Avis de gros temps pour Linux**
    - **Faille #1: exit_notify() corrigé presque silencieusement**
      - **Affecte: Linux < 2.6.29**
      - **Exploit:**
        - **http://xorl.wordpress.com/2009/04/08/linux-kernel-exit_notify-invalid-capability-check/**
        - **http://www.milw0rm.com/exploits/8369**
    - **Faille #2: support CIFS corrigé presque silencieusement**
      - **Affecte: Linux < 2.6.29.1**
      - **Exploit:**
        - **http://blog.fefe.de/?ts=b72905a8**
      - **Remarque: le correctif est-il correct ?**
        - **http://lists.samba.org/archive/linux-cifs-client/2009-April/004322.html**

Infos Unix

- Faille #3: faille critique dans UDEV
  - Affecte: udev < 1.4.1
  - Exploit:
    - http://blog.cr0.org/2009/04/interesting-vulnerability-in-udevd.html
- Et de nombreux lecteurs PDF affectés par des failles "JBIG2" ...
  - Xpdf
  - CUPS pdftops
- Faille dans APT
  - Pas de vérification de la révocation sur les clés OpenPGP
- Faille dans CUPS
  - Affecte: CUPS < 1.3.10
  - Exploit: PNG ou TIFF malformé
    - http://cups.org/articles.php?L582

Infos Unix

- **Fuite d'informations sur /etc/passwd dans FreeBSD**
  - **Affecte: FreeBSD 6 et 7 (toutes versions supportées)**
  - **Exploit: fuite d'information dans Berkeley DB**
    - **http://security.freebsd.org/advisories/FreeBSD-SA-09:07.libc.asc**

- **Déni de service dans le pare-feu OpenBSD**
  - **Affecte: OpenBSD 4.3, 4.4 et 4.5**
  - **Exploit: déni de service lors de la NAT d'un paquet ICMPv6**
    - **Pointeur NULL => *kernel panic***

Infos Unix

- **Faille locale dans HP/UX**
  - **Affecte: HP/UX 11.***
  - **Exploit: faille dans la commande *useradd***
    - **http://itrc.hp.com/service/cki/docDisplay.do?docId=c01539431**

- **Elévation de privilèges locale dans AIX**
  - **Affecte: AIX 5.2, 5.3 et 6.1**
  - **Exploit: *buffer overflow* dans la commande *muxatmd***
    - **http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=784**

Failles

- **Principales applications**
  - **Adobe Acrobat**
    - **De nouvelles failles non corrigées, détectées dans la nature**
    - **Fonctions JavaScript getAnnots() & spell.customDictionaryOpen()**
      - **http://blogs.adobe.com/psirt/2009/04/update_on_adobe_reader_issue.html**
      - **http://www.adobe.com/support/security/advisories/apsa09-02.html**
  - **Adobe Flash Media Server**
    - **Prise de contrôle à distance du serveur**
      - **http://www.adobe.com/support/security/bulletins/apsb09-05.html**
  - **VMWare**
    - **Attention à bien appliquer tous les patches !**
      - **http://lists.vmware.com/pipermail/security-announce/2009/000055.html**
    - **Une tentative de correction de bogue critique en silence ?**

Failles

- FireFox < 3.0.10
  - La version 3.0.9 avait également corrigé l'accès aux LSO (Flash) et le filtre des caractères IDN
- Chrome < 1.0.154.65
  - XSS et exécution de commandes (triviale) via chromehtml://
  - D'autres problèmes commencent à apparaitre ...
    - *Integer Overflow*
    - http://code.google.com/p/chromium/issues/detail?id=10736
    - *Heap Overflow*
    - http://code.google.com/p/chromium/issues/detail?id=10869
- WireShark < 1.0.7
- Winamp < 5.552

Failles

- Failles multiples dans les produits Symantec
  - SYM09-006
    - http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=2009&suid=20090428_01
  - SYM09-007
    - http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=2009&suid=20090428_02
  - L'une d'entre elles est particulièrement fatale
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=786
- Oracle Quaterly Patch
  - 43 failles corrigées
    - http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html
- *Pass-the-hash* avec Oracle
  - Pas une "faille" à proprement parler ...
    - http://www.dsecrg.com/pages/pub/show.php?id=17

Malwares et spam

- W32/Winemmem
  - Un infecteur de fichier d'installation
    - ... qui passe les signatures et les contrôles d'intégrité embarqués
  - Pour cela, il réécrit le point d'entrée de l'exécutable dès qu'il s'est exécuté
    - http://www.avertlabs.com/research/blog/index.php/2009/04/09/w32winemmem-know-your-enemy/
- Une analyse du botnet Torpig
  - Menée de l'intérieur
    - http://isc.sans.org/diary.html?storyid=6358
- Mebroot passe la seconde
    - http://www.avertlabs.com/research/blog/index.php/2009/04/19/stealthmbr-gets-a-makeover/
- FUD ou réalité ?
  - Un vieux téléphone Nokia permettrait d'intercepter des SMS (!?)
    - http://www.pcworld.com/businesscenter/article/163409/criminals_pay_top_money_for_hackable_nokia_phone.html

Malwares et spam

- Conficker
  - L'implémentation MD6 dans Conficker a été corrigée
    - http://blog.fortify.com/blog/fortify/2009/03/21/Look-Whos-Reading
  - Les DNS malmenés: un effet de bord de Conficker ?
    - http://isc.sans.org/diary.html?storyid=6121
  - Une mise à jour pour Conficker
    - Distribuée par le réseau P2P
- 1 spam == 0,3g de CO^2
    - http://img.en25.com/Web/McAfee/CarbonFootprint_12pg_web_REV_NA.pdf
- Trend Micro rachète Third Brigade
  - Donc OSSEC
    - http://www.ossec.net/
- BitDefender communique "à la Symantec"
    - http://www.malwarecity.fr/

Failles 2.0

- Un ver sur Twitter (et même plusieurs)
  - Lancé par la concurrence (!)
    - http://www.f-secure.com/weblog/archives/00001653.html
  - Son auteur a immédiatement reçu des propositions d'embauche (!!)
    - http://abcnews.go.com/Technology/Story?id=7356353&page=1
  - Et il a écrit un deuxième ver dans la foulée (!!!)
    - http://news.cnet.com/8301-1009_3-10222373-83.html?part=rss&subj=news&tag=2547-1_3-0-5
  - Mais il a aussi été entièrement piraté ☺
    - http://seclists.org/fulldisclosure/2009/Apr/0168.html
- Twitter à nouveau piraté
  - Via un compte Yahoo!
  - Mais par un français cette fois-ci ☺
    - http://www.zataz.com/forum/index.php?showtopic=10005

Failles 2.0

- **Faille conceptuelle (*session fixation attack*) dans OAuth**
  - **Twitter, Yahoo et d'autres coupent le service en urgence**
  - **Tentative pour garder la faille secrète**
    - **http://news.cnet.com/8301-13577_3-10225103-36.html**
    - **http://groups.google.com/group/oauth/browse_thread/thread/20e12ace524dba3?pli=1**
  - **Ce qui est impossible, bien sûr ...**
    - **http://oauth.net/advisories/2009-1**
    - **http://www.hueniverse.com/hueniverse/2009/04/explaining-the-oauth-session-fixation-attack.html#more**

Failles 2.0

- **Verizon Data Breach Report 2009**
  - **Quelques chiffres:**
    - **285 millions d'enregistrements volés dans 90 incidents**
    - **93% des incidents dans le domaine de la finance**
    - **90% sont liés à des groupes organisés**
    - **74% des incidents proviennent d'attaquants externes**
      - **Contre 20% interne**
    - **69% des incidents sont détectés par des tierces parties**
    - **(...)**
  - **http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf**

Actualité (France)

- La loi HADOPI rejetée (en première lecture)
  - http://www.numerama.com/magazine/12594-URGENT-le-Parlement-rejette-la-loi-Creation-et-Internet.html
- Initiation à l'intelligence économique
  - http://www.ielovepme.com/images/logo_ielovepme/guide_des_bonnes_pratiques_en_matiere_d_ie.pdf
- L'affaire "EDF vs. GreenPeace" rebondit
  - Le cabinet Kargus aurait également travaillé pour Vivendi et Floyd Landis
    - http://www.mediapart.fr/journal/france/170409/espionnage-apres-edf-des-affaires-vivendi-et-landis
- Big Brother Awards 2009
  - http://bigbrotherawards.eu.org/-Communiques-.html

Actualité (France)

- Le site de l'INPI devient gratuit
  - http://www.inpi.fr/
- LogLogic rachète ExaProtect
  - http://www.loglogic.com/news/news-releases/2009/04/loglogic-signs-agreement-to-acquire-exaprotect/
- La DCSSI, client du produit SCA Fortify
  - http://www.itrmanager.com/articles/89639/dcssi-audite-applications-sca-fortify.html
- Lancement du programme "écoles numériques interactives"

Actualité (anglo-saxonne)

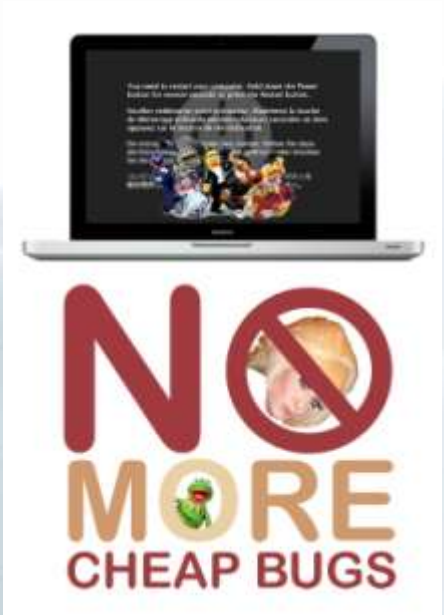
- Le président américain aura-t-il un bouton rouge pour couper Internet ?
  - http://www.lemonde.fr/technologies/article/2009/04/07/un-projet-de-loi-autoriserait-obama-a-couper-des-pans-entiers-d-internet_1177880_651865.html
- La FAA piratée à plusieurs reprises
  - Impacte également le contrôle aérien
    - http://it.slashdot.org/article.pl?sid=09/05/08/192227
- Le réseau électrique américain piraté (?)
  - Il aurait été piraté par les Chinois *et* les Russes ...
    - http://www.reuters.com/article/topNews/idUSTRE53729120090408
    - http://online.wsj.com/article/SB123914805204099085.html
- Les données du projet Joint Strike Fighter piratées (?)
  - http://online.wsj.com/article/SB124027491029837401.html

Actualité (anglo-saxonne)

- L'affaire du "Federal Trojan" CIPAV prend de l'ampleur
  - http://blog.wired.com/27bstroke6/2009/04/fbi-spyware-pro.html
- Le gouvernement américain recrute 200 "cyber-experts"
  - http://www.silicon.fr/fr/news/2009/04/20/des_hackers_a_la_maison_blanche
- Les machines à voter victimes de "dérive de calibration"
  - http://www.salina.com/news/story/vote-machine-4-9-2009
- Sun finalement racheté par Oracle !
  - http://www.itrmanager.com/articles/90154/oracle-rachete-sun.html
- Le *registrar* Néo-Zélandais DOMAINZ.NET piraté
  - Tous ses clients ont été victimes de redirection
    - http://www.zone-h.org/news/id/4708

Actualité (anglo-saxonne)

- La base de données OpenSecrets devient publique
  - http://www.opensecrets.org/news/2009/04/opensecretsorg-goes-opendata.html
- Campagne "No More Free Bugs"
  - http://blog.trailofbits.com/2009/03/22/no-more-free-bugs/
  - http://nomorefreebugs.org/



Actualité (Google)

- Partage de connaissances avec Google
  - http://knol.google.com/k?hl=fr
- Google People Search
  - http://googlesystem.blogspot.com/2009/04/google-people-search.html
- Recherche par couleur dominante dans Google Image
  - http://actu.abondance.com/2009/04/la-recherche-dimages-par-couleurs.html
- Google vs. journaux en ligne
  - En cause: l'indexation des contenus payants
    - http://news.slashdot.org/article.pl?sid=09/04/08/121210

Actualité (Google)

- **Skytone: un Netbook sous Android**
  - **http://www.itrmanager.com/articles/90423/premier-netbook-systeme-exploitation-android.html**
- **Le casse-tête Google Docs**
  - **Comment protéger des données partagées ?**
    - **http://peekay.org/2009/03/26/security-issues-with-google-docs/**
    - **http://googledocs.blogspot.com/2009/03/just-to-clarify.html**

Actualité

- Black Hat Europe 2009
  - http://www.blackhat.com/html/bh-europe-09/bh-eu-09-schedule.html
  - http://www.securityvibes.com/blackhat-amsterdam-2009-jsaiz-news-3003078.html
  - Attaque sur MPLS
    - http://www.darkreading.com/securityservices/services/data/showArticle.jhtml?articleID=216403220
    - Nécessite d'être un opérateur télécom (!)
    - Déjà vu, déjà fait ... en 2002 (?)
      - http://www.securite.org/presentations/secip/BHUS-IPBackboneSecurity.pdf
  - Démonstration Maltego
    - Sur des données issues d'un proxy d'entreprise ...
  - Outil VAASeline contre VNC

Actualité

- Framework d'injection de code via /dev/mem
- Reconfiguration à distance d'un téléphone par SMS
  - Auteurs: Roberto Gassira, Roberto Piccirillo
- "Développer des logiciels sécurisés n’est pas une décision business raisonnable"
  - Auteurs: Jon Miller, Neel Mehta, Alex Wheeler, David Bonvillian

EuroCrypt 2009

- Amélioration des attaques sur SHA-1
- Collisions en 2^52
  - http://eurocrypt2009rump.cr.yp.to/837a0a8086fa6ca714249409ddfae43d.pdf

Actualité

- VMWare vSphere
  - Un système ... de Cloud Computing
    - http://www.vmware.com/vSphere
- Nessus 4 disponible
    - http://www.nessus.org/download/
- Un disque SSD avec du chiffrement hardware
  - Disque Samsung et portable Dell
    - http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9131684
- Le projet DeDECT progresse
  - Un plugin Kismet pour décoder le DECT !
    - https://dedected.org/

Actualité

- La Corée du Sud demande un numéro de carte d'identité pour poster des commentaires sur YouTube
  - http://www.appscout.com/2009/04/comments_and_uploads_disappear.php
- HP propose l'outil gratuit SWFScan
  - Pour chercher des failles dans les applications Flash "*closed source*"
- L'auteur de la faille TCP "ultime" retrouvé mort dans un incendie
  - http://www.infoworld.com/d/security-central/researchers-death-casts-pall-over-major-tcp-fix-794
  - http://blog.robertlee.name/2009/03/jack-c-louis-loss-of-dear-friend.html
  - A voir aussi (prévu pour juin 2009):
    - http://sockstress.com/
- +fravia devient ✝fravia
  - http://en.wikipedia.org/wiki/Fravia

Actualité

- Firefox déclaré "browser le moins sûr" par Secunia
  - De beaux trolls en perspective
    - http://secunia.com/gfx/Secunia2008Report.pdf
    - http://www.neowin.net/news/main/09/04/15/firefox-rated-most-vulnerable-web-browser
- Les auteurs de Skype vont-ils le racheter à eBay ?
  - En tout cas Skype est redevenu une société indépendante
    - http://www.techchuck.com/2009/04/10/cross-your-fingers-zennstrom-and-friis-might-buy-back-skype-from-ebay/
- Challenge DFRWS 2009
  - Cibles: PS3 et PSP
    - http://www.dfrws.org/2009/challenge/
- Challenge SSTIC 2009
    - http://communaute.sstic.org/ChallengeSSTIC2009

Fun

- Répartition des systèmes d'exploitation
  - Windows 88%, Linux 1%, iPhone 0,5% (!)
    - http://marketshare.hitslink.com/operating-system-market-share.aspx?qprid=8&sample=35
- Se faire *hacker* son ADN ?
    - http://www.newscientist.com/article/mg20127013.800-special-investigation-how-my-genome-was-hacked.html?full=true
- L'informatique, ça n'est pas (toujours) de tout repos
    - http://www.infoworld.com/d/adventures-in-it/even-dirtier-it-jobs-muck-stops-here-002
- Ubunchu!
  - Le manga Ubuntu, disponible en anglais et en français
    - http://doctormo.wordpress.com/2009/04/02/ubunchu-the-ubuntu-manga-is-now-in-english/
- Un travail de rêve ?
    - http://jobs.perl.org/job/10462

Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 9 juin 2009
- N'hésitez pas à proposer des sujets et des salles