OSSIR
Groupe Paris

Réunion du 7 juillet 2009

Revue des dernières vulnérabilités

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

Avis Microsoft (1/12)

- **Correctif de Juin 2009**
  - **Avec [*exploitability index*]**
  - **MS09-018 Faille(s) dans Active Directory [3*,3]**
    - **Affecte: Windows 2000, 2003 et ADAM**
    - **Exploit: "*double free*" & "*memory leak*"**
      - **Exécution de code sur Windows 2000**
      - **Déni de service sur les autres systèmes**
      - **http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=804**
    - **Crédit:**
      - **Joshua J. Drake / iDefense**
      - **Justin Wyatt / Beavertown School District**
    - **Notes:**
      - *** anciennement 1**
        - **http://expertmiami.blogspot.com/2009/06/exploitability-index-ou-comment-perdre.html**

Avis Microsoft (2/12)

- MS09-019 Patch cumulatif pour IE [3,3,3,1,3,2,2,3,3]
  - Affecte: IE (toutes versions supportées)
  - Exploit: multiples, allant jusqu'à l'exécution de code à la consultation d'une page Web malformée
    - Une faille serait connue depuis mai 2004
  - Crédit:
    - David Bloom / Google
    - Jorge Luis Alvarez Medina / Core
    - Haifei Li / Fortinet
    - TippingPoint / ZDI
      - Anonymous
      - Peter Vreugdenhil
      - Wushi (x2)
      - Nils

Avis Microsoft (3/12)

- Notes sur MS09-019
  - Faille #1 (exploitée lors de pwn2own)
    - http://blogs.technet.com/srd/archive/2009/06/09/cve-2009-1532-the-pwn2own-vulnerability.aspx
    - Origine du problème S_FALSE = 1 alors que FALSE = 0 ...
  - Faille #2
    - http://blogs.technet.com/srd/archive/2009/06/09/cve-2009-1140-benefits-of-ie-protected-mode-additional-network-protocol-lockdown-workaround.aspx
    - Exploit: \\127.0.0.1\c$\(...)\index.dat
  - Le point de vue de Michal Zalewski : "Been There, Done That" (x4)
    - http://archives.neohapsis.com/archives/fulldisclosure/2009-06/0094.html

Avis Microsoft (4/12)

- MS09-020 Faille(s) WebDAV dans IIS [3,1]
  - Affecte: IIS 5.0, 5.1 et 6.0
  - Exploit: activement exploité dans la nature
  - Crédit: Yamata Li / Palo Alto Networks

- MS09-021 Faille(s) dans Excel [2,1,2,1,3,1,1]
  - Affecte:
    - Excel (toutes versions supportées, dont Excel Viewer et Mac OS X)
    - SharePoint 2007 (toutes versions supportées)
  - Exploit: exécution de code à l'ouverture d'un fichier malformé
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=805
  - Crédit:
    - Bing Liu / Fortinet (x3)
    - Carsten H. Eiram / Secunia (x2)
    - TELUS Security Labs
    - Sean Larsson & Joshua Drake / iDefense
    - anonymous / ZDI

Avis Microsoft (5/12)

- MS09-022 Faille(s) dans le service *spooler* [1,3,1]
  - Affecte: Windows (toutes versions supportées)
  - Exploit:
    - Windows 2000: exécution de code à distance sur RPC anonyme
    - Windows autre: élévation de privilèges locale
    - Disponible dans le produit CANVAS
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=806
  - Crédit: Jun Mao / iDefense

- MS09-023 "Fuite d'information" dans Windows Search [3]
  - Affecte: Windows Search 4.0 sur Windows XP et 2003
  - Exploit: la fonction *preview* exécute les scripts
    - http://blogs.technet.com/srd/archive/2009/06/09/ms09-023-windows-search-and-mshtml-host-apps.aspx
  - Crédit: Yair Amit / IBM Rational Application Security

Avis Microsoft (6/12)

- MS09-024 Faille dans le convertisseur Works [1]
  - Affecte:
    - Office 2000 / XP / 2003 / 2007 (sauf Office 2007 SP2)
    - Works 8.5 et 9.0
  - Exploit: exécution de code à l'ouverture d'un fichier malformé
    - http://blogs.technet.com/srd/archive/2009/06/09/ms09-024.aspx
  - Crédit:
    - Shaun Colley / NGS Software
    - Yuji Ukai / Fourteenforty

- MS09-025 Faille(s) dans le noyau Windows [2,1,1,1]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: élévation de privilèges locale
    - Failles exploitées dans la nature d'après Microsoft
  - Crédit: Thomas Garnier (x2)

Avis Microsoft (7/12)

- **MS09-026 Faille dans le moteur RPC [2]**
  - **Affecte: Windows (toutes versions supportées)**
  - **Exploit: exécution de code à distance**
    - **Faille exploitée dans la nature d'après Microsoft**
    - **Mais affecte uniquement le type "*non-conformant varying array*"**
    - **http://blogs.technet.com/srd/archive/2009/06/09/ms09-026-how-a-developer-can-know-if-their-rpc-interface-is-affected.aspx**
  - **Crédit: n/d**

- **MS09-027 Faille(s) dans Word [2,1]**
  - **Affecte: Word (toutes versions supportées, dont Mac OS X et Viewers)**
  - **Exploit: exécution de code à l'ouverture d'un fichier malformé**
  - **Crédit:**
    - **Wushi / team509**
    - **Nicolas Joly / VUPEN**

Avis Microsoft (8/12)

- 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 (9/12)

- Advisories
  - Q971888: mise à jour de la logique du client DNS
    - http://www.microsoft.com/technet/security/advisory/971888.mspx
    - Voir aussi "UseDomainNameDevolution"
      - http://technet.microsoft.com/en-us/library/cc959477.aspx
      - http://support.microsoft.com/kb/957579
  - Q969898: mise à jour des "kill bits"
    - Microgaming
    - eBay Image Uploader
    - HP Virtual Room 7.0 (développé par RIM)
  - Q972890: faille "0day" dans Microsoft DirectShow
    - Composant affecté: msVidCtl
    - Code d'exploitation public
    - CVE-2008-0015
  - Note: faille différente de Q971778 (datant du 28 mai 2009)
    - http://dvlabs.tippingpoint.com/blog/2009/06/30/exploiting-ms-advisory-971778---quicktime-directshow-vulnerability

Avis Microsoft (10/12)

- Q971492 -> MS09-020
- Q945713 -> MS09-008

■ Prévisions pour Juillet 2009

- Pas encore disponible

Avis Microsoft (11/12)

- Révisions
  - MS99-031 (v3.0)
  - MS99-045 (v3.0)
  - MS00-011 (v3.0)
  - MS00-059 (v2.0)
  - MS00-075 (v2.0)
  - MS00-081 (v2.0)
  - MS02-013 (v3.0)
  - MS02-052 (v2.0)
  - MS02-069 (v2.0)
  - MS03-011 (v2.0)
    - Ces correctifs ne sont plus téléchargeables, car la JVM Microsoft n'est plus distribuée

Avis Microsoft (12/12)

- MS09-017
  - Version 2.0: intégration des correctifs Mac OS X et Works
- MS09-010
  - Version 1.3: précisions documentaires
- MS09-018
  - Version 1.1: précisions documentaires
- MS09-020
  - Version 1.1: précisions documentaires
- MS09-021
  - Version 1.1: ajout d'un problème connu (cf. Q969462)
- MS09-022
  - Version 1.1: nouveau *workaround* (désactiver le service Spooler)

Infos Microsoft

- Sorties logicielles

  - L'antivirus "Morro" en Beta
    - 75,000 exemplaires distribués en une journée
    - Fin de la Beta le jour même
    - Note: OneCare n'est plus supporté
      - http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9134254
  - SilverLight 3.0 disponible le 10 juillet 2009
    - http://www.seethelight.com/
  - IE8 disponible sur WSUS le 25 août 2009

Infos Microsoft

- **Autre**
  - **Microsoft met le paquet sur IE8**
    - **http://www.microsoft.com/windows/internet-explorer/get-the-facts/mythbusting.aspx**
  - **Fin de vente pour Microsoft Money**
    - **http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9134237**
  - **Fin du support Office 2000**
    - **Au 14 juillet 2009**
  - **L'édition Windows Seven "Familiale Premium" annoncée à 50 euros**
    - **http://guw7.com/blogs/actu/archive/2009/06/25/microsoft-windows-7-disponible-224-partir-de-50-euros.aspx**

Infos Microsoft

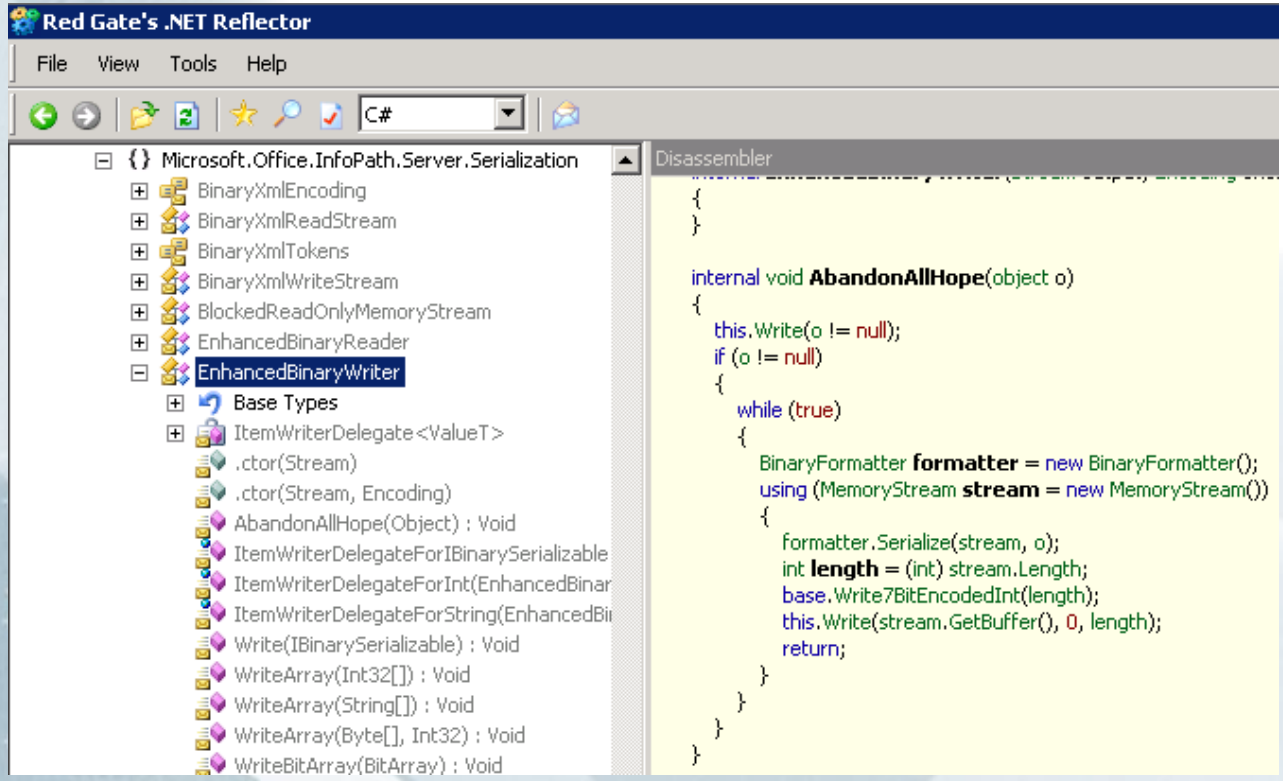
- Bing met le feu
  - http://isc.sans.org/diary.html?storyid=6721
- Les utilisateurs d'IE6 forcés d'utiliser Bing ?
  - http://thenextweb.com/2009/06/02/microsoft-forcing-bing-ie6-users/
- Des patches installés sans confirmation de l'utilisateur ?
  - http://windowssecrets.com/2009/06/25/01-Windows-may-install-updates-without-asking
- SharePoint 2007 SP2 provoque l'expiration du produit au bout de 180 jours
  - http://blogs.technet.com/office/archive/2009/05/26/probl-me-de-date-d-expiration-suite-l-application-du-sp2.aspx

Infos Microsoft

- Windows Seven
  - Autre contournement de l'UAC "simplifiée" dans Windows Seven
    - http://www.pretentiousname.com/misc/W7E_Source/win7_uac_poc_details.html
  - Windows Seven sera 40% à 100% plus cher en Europe qu'aux USA
    - Comme le reste des logiciels Microsoft
    - http://www.zdnet.fr/actualites/informatique/0,39040745,39700823,00.htm
- Microsoft France
  - Microsoft France lance "j'en ai rien à déployer"
    - http://technet.microsoft.com/fr-fr/dd902179.aspx
  - Microsoft France déménage à Issy-les-moulineaux
    - http://www.microsoft.com/france/core/my-campus-microsoft-france.aspx

Infos Microsoft

- La source du Mal ?
  - http://blogs.media-tips.com/bernard.opic/2007/10/16/microsoft-the-source-of-all-evil/
- Ou du désespoir ...



Infos Réseau

- **Déni de service contre Apache**
  - **Affecte: Apache (et ses dérivés), Squid, etc.**
    - **IIS n'est pas affecté**
  - **Exploit: connexions HTTP "lentes"**
    - **Outil "Slow Loris"**
    - **http://ha.ckers.org/slowloris/**
  - **Remarque:**
    - **Connu et documenté par Apache depuis longtemps ...**
    - **http://pub.mud.ro/~cia/computing/apache-httpd-denial-of-service-example.html**

Infos Réseau

- Failles dans Cisco ASA
  - Dont un *cross-site scripting* via l'encodage ROT-13 (!)
    - http://tools.cisco.com/security/center/viewAlert.x?alertId=18373
    - http://tools.cisco.com/security/center/viewAlert.x?alertId=18442
    - http://tools.cisco.com/security/center/viewAlert.x?alertId=18536
- ComCast passe l'IPv6
    - http://www.internetnews.com/infra/article.phpr/3825696/Comcast+Embraces+IPv6.htm
- L'AFNIC encourage le passage à DNSSEC
- Chris Hoff recruté chez Cisco
  - Animateur du *Rational Survivability blog*
  - Missions: virtualisation et cloud computing

Infos Unix

- (Principales) failles
  - Linux
    - eCryptFS stocke la *passphrase* en clair dans un fichier de log
      - Affecte: Ubuntu 9.04
      - http://lwn.net/Alerts/336770/
    - libpng < 1.2.37
      - http://downloads.sourceforge.net/libpng/libpng-1.2.34-ADVISORY.txt
      - http://www.libpng.org/pub/png/libpng.html
    - Pilote pour la carte Intel Pro 1000 < 7.5.5
      - http://www.intel.com/support/network/sb/CS-030543.htm

Infos Unix

- Samba <= 3.3.5
  - Contournement des contrôles d'accès si "dos filemode=yes"
  - http://www.samba.org/samba/security/CVE-2009-1888.html
- PHPMyAdmin #1
  - Affecte: < 2.11.9.5, < 3.1.3.1
  - http://www.phpmyadmin.net/home_page/security/PMASA-2009-3.php
- PHPMyAdmin #2
  - Affecte: < 3.1.3.2
  - http://www.phpmyadmin.net/home_page/security/PMASA-2009-4.php

Infos Unix

- Nagios < 3.1.1
  - Injection de commandes via le séparateur ';'
    - http://tracker.nagios.org/view.php?id=15
  - IMHO le problème vient de PEAR::Net::Ping
    - http://news0ft.blogspot.com/2008/12/ceci-nest-pas-du-sport.html
- OCS Inventory NG < 1.02.1
  - Injection SQL (+ injection de commandes ?)
    - http://www.ocsinventory-ng.org/index.php?mact=News,cntnt01,detail,0&cntnt01articleid=140&cntnt01returnid=111
- Mutt 1.5.19 (yeah)
  - Problème de validation dans une chaine de certificats
    - https://bugzilla.redhat.com/show_bug.cgi?id=504979

Infos Unix

- Solaris
  - Affecte: pile IP (Jumbo Frames + driver Cassini gigabit)
    - http://sunsolve.sun.com/search/document.do?assetkey=1-66-257008-1
  - Affecte: UDP
    - http://sunsolve.sun.com/search/document.do?assetkey=1-66-262048-1
  - Affecte: Kerberos
    - http://sunsolve.sun.com/search/document.do?assetkey=1-66-252787-1
  - Affecte: rpc.nisd
    - http://sunsolve.sun.com/search/document.do?assetkey=1-66-256748-1
- FreeBSD
  - Affecte: ntpd < 4.2.4p7
    - http://security.freebsd.org/advisories/FreeBSD-SA-09:09.pipe.asc
    - http://security.freebsd.org/advisories/FreeBSD-SA-09:10.ipv6.asc
- OS/400 (pas courant !)
  - Affecte: traitement XML en Java
    - http://www-01.ibm.com/support/docview.wss?uid=nas2741c96b7c573b81a862575cc003c726e
    - http://www-01.ibm.com/support/docview.wss?uid=nas2e858199605d67111862575cc003c7276

Infos Unix

- **Autre**
  - **OpenSSL offre désormais un support payant**
    - **http://permalink.gmane.org/gmane.comp.encryption.openssl.announce/65**

Failles

- Principales applications
  - 13 failles[*] dans Acrobat Reader ...
    - [*] au minimum, car Adobe a aussi corrigé des failles trouvées "en interne"
    - Affecte: Acrobat Reader < 9.1.2, 8.1.6, 7.1.3
    - Exploit:
      - http://www.adobe.com/support/security/bulletins/apsb09-07.html
      - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=807
    - Crédit:
      - anonymous / ZDI
      - Jun Mao & Ryan Smith / iDefense
      - Haifei Li / Fortinet
      - "Apple Product Security Team"
      - Matthew Watchinski / SourceFire
      - Alin Rad Pop / Secunia
      - Mark Dowd / IBM ISS
      - Will Dormann / CERT
      - Nicolas Joly / VUPEN
  - Adobe et Microsoft vont travailler ensemble sur la sécurité
    - http://blogs.msdn.com/sdl/archive/2009/06/17/microsoft-adobe-protecting-our-customers-together.aspx

Failles

- 50 failles corrigées dans Safari 4
  - Affecte: Safari < 4 (et Chrome < 2.0.172.31)
  - Exploit:
    - http://support.apple.com/kb/HT3613
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=803
  - Dont le vol de fichiers locaux par *XML External Entity* (XXE)
    - http://scarybeastsecurity.blogspot.com/2009/06/apples-safari-4-fixes-local-file-theft.html
  - Notez le nombre de failles remontées par Google
    - http://www.net-security.org/advisory.php?id=10247
- 46 failles corrigées dans le firmware 3.0 pour iPhone
  - Affecte: iPhone / iPod Touch < 3.0
  - Exploit: http://support.apple.com/kb/HT3639
- Compromission à distance de l'iPhone … par un SMS
    - http://tech.yahoo.com/news/pcworld/20090702/tc_pcworld/applepatchingseriousssmsvulnerabilityoniphone

Failles

- Autres applications
  - Firefox < 3.0.11 (failles multiples)
    - http://www.mozilla.org/security/known-vulnerabilities/firefox30.html#firefox3.0.11
  - Thunderbird < 2.0.22 (failles multiples)
    - http://www.mozilla.org/security/known-vulnerabilities/thunderbird20.html#thunderbird2.0.0.22
  - Google Chrome < 2.0.172.33
    - *Buffer overflow* dans le traitement des réponses HTTP
    - http://code.google.com/p/chromium/issues/detail?id=14508
  - Foxit Reader < 3.0.1817
    - Faille dans le décodeur JBIG2 ...
    - http://www.foxitsoftware.com/pdf/reader/security.htm#0602
  - ShockWave <= 11.5.0.596
    - http://www.adobe.com/support/security/bulletins/apsb09-08.html

Failles

- VMWare ESX 3.5 est affecté par la faille Kerberos 5
  - Note: Kerberos non activé par défaut
  - http://lists.vmware.com/pipermail/security-announce/2009/000059.html
- Tomcat < 5.5.27, < 4.1.39
  - http://marc.info/?l=tomcat-user&m=124404378413736&w=2
  - http://marc.info/?l=tomcat-user&m=124404378913734&w=2
  - http://marc.info/?l=tomcat-user&m=124412001618125&w=2
- IBM WebSphere 6 et 7
  - http://www-01.ibm.com/support/docview.wss?uid=swg21386826
  - http://www-01.ibm.com/support/docview.wss?uid=swg27006876#60235
  - http://www-01.ibm.com/support/docview.wss?uid=swg27007951

- Metasploit ajoute le support AIX sur PowerPC
  - http://www.risesecurity.org/entry/all-your-power-are-belong-to-us/

Malwares et spam

- La liste des mots clés les plus dangereux
  - http://newsroom.mcafee.com/article_display.cfm?article_id=3526

Category	Maximum Risk (Average)	Category Risk (Average)
Screensavers	59.1%	34.4%
Free Games	24.7%	6.8%
Work From Home	15.6%	3.1%
Rihanna	12.6%	2.4%
Webkinz	11.4%	1.9%
Powerball	9.3%	1.5%
iPhone	7.9%	1.2%
Jonas Brothers	7.9%	1.2%
Twilight	6.8%	0.9%
Barack Obama	6.2%	0.7%
Taxes	4.9%	0.4%
Viagra	1.6%	0.1%

Malwares et spam

- La Chine, nouveau paradis du spam
  - http://garwarner.blogspot.com/2009/06/spam-crisis-in-china.html
- La fin du service SORBS ?
  - http://www.us.sorbs.net/
- McAfee antivirus (epic) fail
  - http://www.eweek.com/c/a/Security/McAfee-Update-a-Headache-for-Enterprises-With-Old-Software-842314/

Failles 2.0

- Le service d'URLs raccourcies "cli.gs" piraté
  - 2,2 millions de pointeurs vers un site "hostile" ...
    - http://www.net-security.org/secworld.php?id=7633
- Month of Twitter Bugs
    - http://aviv.raffon.net/2009/06/15/MonthOfTwitterBugs.aspx
- Jolie faille dans TwitPic
  - La sécurité repose sur un code PIN à 4 chiffres ...
    - http://www.msuiche.net/2009/06/29/security-20-is-not-even-a-failure-it-is-a-nightmare/
- Faille dans l'éditeur FCKEditor
    - http://www.ocert.org/advisories/ocert-2009-007.html
  - Affecte les installations ColdFusion
    - http://www.codfusion.com/blog/post.cfm/cf8-and-fckeditor-security-threat

Failles 2.0

- **Blanchiment d'argent ...**
  - **... via la vente et l'achat de musiques sur iTunes**
    - **http://www.timesonline.co.uk/tol/news/uk/crime/article6471432.ece**
  - **Mais que fait HADOPI ? ☺**
- **Révolution 2.0**
    - **http://threatchaos.com/2009/06/hactivism-in-action-twitter-being-used-to-spread-ddos-instructions/**
- **Opera 10 ... fait aussi serveur Web**
    - **http://unite.opera.com/**

Failles 2.0

- Il est devenu pratiquement impossible de vendre un PC sur eBay
  - Beaucoup trop de fraude(s) !
    - http://www.schneier.com/blog/archives/2009/06/fraud_on_ebay.html
    - http://consumerist.com/5007790/its-now-completely-impossible-to-sell-a-laptop-on-ebay
- Le plugin "Acajoom" (pour Joomla) backdooré ... par son auteur ?
    - http://www.securityfocus.com/bid/35459
- L'OWASP publie "ASVS"
  - Application Security Verification Standards
    - http://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project
- L'initiative CSP (*Content Security Policy*) de Mozilla
  - Sécurité déclarative pour le Web
    - https://wiki.mozilla.org/Security/CSP/Spec

Actualité (France)

- La loi HADOPI retoquée par le Conseil Constitutionnel
  - http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/cc-2009580dc.pdf
- HADOPI n'est qu'un début
  - http://www.numerama.com/magazine/13159-Jean-Francois-Cope-l-Hadopi-n-est-que-le-point-de-depart.html
- Le RGI publié
  - http://www.references.modernisation.gouv.fr/rgi-interoperabilite
- Les Directives Nationales de Sécurité
  - Quel impact sur l'activité industrielle ?
    - http://www.globalsecuritymag.fr/Directives-Nationales-de-Securite,20090626,10640

Actualité (France)

- Un "livre blanc sur la cybersécurité" ?
  - Pas très "green" tous ces livres blancs ☺
    - http://www.lefigaro.fr/flash-actu/2009/06/17/01011-20090617FILWWW00569-un-livre-blanc-sur-la-cybersecurite.php
- L'ANSSI, c'est pour bientôt
    - http://www.lemagit.fr/article/securite-dcssi-cybercriminalite-cybersecurite-anssi/3734/1/l-agence-nationale-pour-securite-des-systemes-information-devrait-naitre-semaine-prochaine/
- Les projets du défi SEC&SI disponibles
    - http://adullact.net/forum/forum.php?forum_id=2412
- (Mais toujours pas ANSMO)
    - http://www.securite-informatique.gouv.fr/gp_article220.html

Actualité (France)

- Quels AS contrôlent les DNS français ?
  - http://www.links.org/?p=650

- L'ARCEP rend sa décision concernant le déploiement de la fibre optique
  - Communiqué de presse:
    - http://www.arcep.fr/fileadmin/reprise/dossiers/fibre/conf-220609/note-gnl-thtdebit-220609.pdf
  - Site officiel:
    - http://www.arcep.fr/index.php?id=8571&tx_gsactualite_pi1[uid]=1177&tx_gsactualite_pi1[annee]=&tx_gsactualite_pi1[theme]=&tx_gsactualite_pi1[motscle]=&tx_gsactualite_pi1[backID]=26&cHash=a72424f18f
  - Commentaires:
    - http://www.lesechos.fr/info/hightec/300357384-fibre-optique-l-interet-general-ce-n-est-pas-l-interet-d-un-seul-operateur-.htm
    - http://www.journaldunet.com/ebusiness/breve/40367/france-telecom-fait-du-chantage-a-la-fibre.shtml

Actualité (anglo-saxonne)

- Les rootkits "ring -3" annoncés à BlackHat
  - Mais où s'arrêteront-ils ?
    - http://blackhat.com/html/bh-usa-09/bh-usa-09-speakers.html#Tereshkin
- La présentation de Barnaby Jack annulée (à la demande de Juniper)
  - Sujet: vider un ATM à distance ...
    - http://risky.biz/news_and_opinion/patrick-gray/2009-06-30/juniper-networks-gags-atm-jackpot-researcher
- La femme du chef du MI6 sur Facebook
    - http://tempsreel.nouvelobs.com/actualites/international/europe/20090705.OBS3150/le_futur_chef_du_mi6_en_maillot_de_bain_sur_facebook.html
- Une liste de sites nucléaires américains publiée "par accident"
    - http://www.nytimes.com/2009/06/03/us/03nuke.html
- La NSA surveillerait tous les emails américains
  - Sans rire ?
    - http://www.nytimes.com/2009/06/17/us/17nsa.html?_r=2&hp=&pagewanted=all

Actualité (Google)

- Chrome vs. FFMpeg (LGPL)
  - http://yro.slashdot.org/story/09/06/07/2318210/Google-Chromes-Inclusion-of-FFMpeg-vs-the-LGPL
- Google s'inquiète de Bing
  - ... qui pourtant n'a hissé la part de marché que de 8% à 11%
    - http://www.nypost.com/seven/06142009/business/fear_grips_google_174235.htm
  - "Bing, c'est de la daube"
    - http://www.theregister.co.uk/2009/06/27/google_mocks_microsoft_online_infrastructure/
- Google défend sa sécurité
  - http://googleonlinesecurity.blogspot.com/2009/06/https-security-for-web-applications.html
  - En réponse à:
    - http://www.wired.com/images_blogs/threatlevel/2009/06/google-letter-final2.pdf

Actualité

- Collisions sur SHA-1 en 2^52
  - http://eprint.iacr.org/2009/259.pdf
- MD5 meurt un peu plus
  - http://www.win.tue.nl/hashclash/SingleBlock/
- Une attaque sur AES
  - http://www.cgisecurity.com/2009/07/new-attack-on-aes.html
- IBM annonce un système de chiffrement homomorphique
  - Seul(s) problème(s): c'est lent et moins sûr ...
    - http://science.slashdot.org/story/09/06/25/1736230/IBM-Claims-Breakthrough-In-Analysis-of-Encrypted-Data
- Des améliorations dans le domaine de la factorisation
  - Par des français
    - http://eprint.iacr.org/2009/318.pdf
- MD6 retiré du challenge NIST à la demande des auteurs

Actualité

- Phrack#66 est disponible
  - http://www.phrack.org/issues.html?issue=66
  - TCP est mort ?
    - Outil Nkiller2
    - http://www.phrack.org/issues.html?issue=66&id=9#article
- Firefox 3.5 est disponible
- Un outil d'analyse des sessions RDP
  - http://rautor.sourceforge.net/
- Kantara va-t-il réussir fédérer la gestion d'identités ?
  - http://kantarainitiative.org/

Actualité

- ThePirateBay racheté pour $7.8m
  - Par "Global Gaming Factory"
    - http://thepiratebay.org/blog/164
- Des outils d'écoute de claviers mis dans le domaine public
  - Projet Keykeriki
- Le *profiling* des échanges d'emails permet(trait) de détecter les faillites
  - Pas d'analyse du contenu
  - Cas d'école avec Enron
    - http://www.newscientist.com/article/mg20227135.900-email-patterns-can-predict-impending-doom.html

Actualité

- L'Allemagne prépare sa solution de filtrage d'Internet
  - Basée sur DNS
    - http://netzpolitik.org/2009/the-dawning-of-internet-censorship-in-germany/

Actualité

- La Chine impose l'installation d'un logiciel de filtrage du Web sur tout PC vendu en Chine ("Green Dam")
  - Officiellement un filtre contre la pornographie
    - http://online.wsj.com/article/SB124464392279802213.html
  - Quelques problèmes identifiés
    - Des failles exploitables à distance
      - http://www.cse.umich.edu/~jhalderm/pub/gd/
    - Le filtrage détecte Johnny Depp, Garfield et Paris Hilton comme des images pornographiques
      - http://www.reuters.com/article/technologyNews/idUSTRE55T26Y20090630
    - La société "Solid Oak Software" se plaint de vol de propriété intellectuelle
  - … et au final, tout le projet est annulé (!)
    - http://fr.news.yahoo.com/4/20090701/tsc-chine-internet-011ccfa.html

Fun

- Quand le *background checking* dérape
  - http://scitech.blogs.cnn.com/2009/06/19/want-a-job-hand-over-your-facebook-password/
- Un député du Parti Pirate au parlement européen
  - http://arstechnica.com/tech-policy/news/2009/06/swedish-pirate-party-headed-to-european-parliament.ars
- Paris Girl Geek Dinners
  - Est-ce que Teh-win y est ?
    - http://www.parisgirlgeekdinners.fr/

Fun

- Le site de Kevin Mitnick "défiguré"
- Teh-win, le retour ?
  - http://www.teh-win.fr/
- Apple devient raisonnable
  - http://www.journaldunet.com/ebusiness/breve/telecoms-fai/40234/l-iphone-s-ouvre-au-marche-du-charme.shtml
- La géolocalisation sur iPhone, ça marche ...
  - http://happywaffle.livejournal.com/5890.html
- Un américain propose les mots de passe de sa femme et de sa fille sur Full Disclosure
  - http://archives.neohapsis.com/archives/fulldisclosure/2009-06/0299.html

Fun


Reverso
TRADUCTION
Bienvenue sur le service gratuit de traduction
en ligne avec les logiciels de traduction Reverso
Traduction
Dictionnaire
Conjugaison
Plus...
Contact
Aide
Favoris
Recommander
Bienvenue sur Reverso.net, service gratuit de traduction en ligne en anglais, allemand, espagnol, italien, russe, chinois
1 Texte d'origine
geek
nerd
2 Traduction de Reverso en Français
Ballot de dégénéré

Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 8 septembre 2009
- N'hésitez pas à proposer des sujets et des salles
- ... et d'ici là ... bonnes vacances !