OSSIR
Groupe Paris

Réunion du 12 octobre 2010

Revue des dernières vulnérabilités

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

Avis Microsoft

- **Septembre 2010**
  - **Références**
    - **http://blogs.technet.com/b/msrc/archive/2010/09/13/september-2010-security-bulletin-release.aspx**
    - **http://blogs.technet.com/b/msrc/archive/2010/09/17/september-2010-security-release-bulletin-webcast-q-amp-a.aspx**
  - **MS10-061 Faille dans le service Spooler [1]**
    - **Affecte: Windows (toutes versions supportées)**
    - **Exploit: *upload* de fichiers arbitraires si au moins une imprimante est partagée**
    - **Crédit:**
      - **Sergey Golovanov, Alexander Gostev, Maxim Golovkin, Alexey Monastyrsky / Kaspersky Lab**
      - **Vitaly Kiktenko, Alexander Saprykin / Design and Test Lab**
      - **Liam O Morchu / Symantec**
    - **Notes:**
      - **Exploité en "0day" par le ver StuxNet**
      - **http://blogs.technet.com/b/srd/archive/2010/09/14/ms10-061-printer-spooler-vulnerability.aspx**

Avis Microsoft

- MS10-062 Faille dans le codec MPEG-4 [1]
  - Affecte: Windows (toutes versions supportées sauf 7 / 2008R2)
  - Exploit: exécution de code à l'ouverture d'un fichier MPEG-4 malformé
  - Crédit: Matthew Watchinski / Sourcefire VRT

- MS10-063 Faille dans le rendu du texte Unicode [2]
  - Affecte:
    - Windows (toutes versions supportées sauf 7 / 2008R2)
    - Office XP / 2003 / 2007
  - Exploit: exécution de code à l'ouverture d'un texte Unicode malformé
    - Composant affecté: "usp10.dll" (Unicode Script Processor)
  - Crédit:
    - Carsten Book / Mozilla
    - Marc Schoenefeld / Red Hat
  - Notes:
    - "Exploitability Index" ultérieurement ramené à "1"
      - http://secunia.com/blog/137/

Avis Microsoft

- **MS10-064 Faille Outlook [2]**
  - **Affecte: Office XP / 2003 / 2007**
  - **Exploit: exécution de code à la lecture d'un email**
    - **Une simple prévisualisation suffit (pas de confirmation)**
    - **Affecte uniquement le mode "Exchange Online"**
      - **Tous les autres modes ("Exchange Cached", IMAP et POP) ne permettent pas de déclencher la vulnérabilité**
    - **La lecture des emails en "*plain text*" est un *workaround* efficace**
  - **Crédit: Dyon Balding / Secunia**

Avis Microsoft

- **MS10-065 Failles IIS [1,1,3]**
  - **Affecte:**
    - **IIS + ASP (toutes versions supportées)**
    - **IIS + FastCGI (disponible uniquement avec IIS 7.5)**
    - **IIS Authentication (disponible uniquement avec IIS 5.1)**
  - **Exploit:**
    - **Déni de service**
    - ***Buffer overflow* (FastCGI uniquement)**
    - **Contournement de l'authentification (IIS 5.1 uniquement)**
  - **Crédit:**
    - **Jinsik Shim**
    - **Travis Raybold / Rubicon West**
  - **Notes:**
    - **Faille(s) divulguée(s) dans la nature avant le correctif**
    - **http://blogs.technet.com/b/srd/archive/2010/09/14/ms10-065-vulnerability-in-iis-s-fastcgi-handler.aspx**

Avis Microsoft

- **MS10-066 Faille dans le moteur RPC *côté client* [1]**
  - **Affecte: Windows XP / 2003**
  - **Exploit: exécution de code anonyme à distance**
    - **Le client doit se connecter à un serveur RPC malveillant**
    - **L'exécution de code s'effectue dans le contexte du client**
  - **Crédit: Yamata Li / Palo Alto Networks**

- **MS10-067 Faille dans un convertisseur WordPad [1]**
  - **Affecte: Windows XP / 2003**
  - **Exploit: exécution de code à l'ouverture d'un fichier Word97 malformé dans WordPad**
  - **Crédit: S0lute / iDefense Labs**

Avis Microsoft

- MS10-068 Faille dans LSASS [1]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: exploitable via une requête LDAP malformée vers Active Directory ou ADAM
    - Nécessite une authentification préalable
    - Heap overflow complexe à exploiter
  - Crédit: n/d
  - Références:
    - http://expertmiami.blogspot.com/2010/09/ms10-068-indice-1-mais-pas-vraiment.html
- MS10-069 Faille dans CSRSS [1]
  - Affecte: Windows XP/2003
    - Versions japonaise, coréenne et chinoise uniquement
  - Exploit: élévation de privilèges locale
  - Crédit: IBM Japan

Avis Microsoft

- Correctif "hors cycle"
  - MS10-070 Faille(s) dans ASP.NET
    - Affecte: .NET (toutes versions supportées, sauf .NET 1.0 SP3)
    - Exploit:
      - Implémentation cryptographique défaillante
      - Lecture de fichiers arbitraires (.NET 3.5 SP1 et ultérieur)
    - Crédit: n/d
    - Notes:
      - http://blogs.technet.com/b/msrc/p/september-2010-oob-security-bulletin-q-a.aspx
      - Voir plus loin pour les détails
- Prévisions Microsoft pour ce soir
  - 16 bulletins
  - 49 failles
- Note: prévoir 81 failles chez Oracle également ce mois-ci

Avis Microsoft

- **Advisories**
  - **Q973811 "*Extended Protection for Authentication*"**
    - **V1.6: désormais supporté par Outlook Express et Windows Mail**
      - **Sous réserve de télécharger un correctif optionnel**
  - **Q2401593 Vol de session OWA**
    - **Affecte: Exchange 2003 (toutes versions) et 2007 (< SP3)**
    - **V1.0: publication de l'avis**

Avis Microsoft

- **Q2416728 Faille ASP.NET**
  - **Affecte: ASP.NET (toutes versions supportées)**
  - **V1.0: publication de l'avis**
  - **V1.1: exploitation en cours sur Internet ; disponibilité d'un *workaround***
  - **V1.2: mise à jour du *workaround***
    - **http://blogs.technet.com/b/msrc/archive/2010/09/24/security-advisory-2416728-workaround-update.aspx**
  - **V2.0: publication du correctif MS10-070**

  - **Explications**
    - **Le serveur peut être utilisé comme oracle (message d'erreur spécifique en cas de *padding* incorrect)**
    - **Il alors est possible d'implémenter une attaque sur DES-CBC**

  - **Impact**
    - **Faille cryptographique extrêmement critique (du jamais vu depuis "Code Red")**
    - **Altération de toute donnée chiffrée/scellée par le serveur (ex. ViewState)**
    - **Accès à des fichiers arbitraires de l'application (avec .NET 3.5 SP1 et plus récent)**
    - **SharePoint est impacté**
      - **http://blogs.msdn.com/b/sharepoint/archive/2010/09/21/security-advisory-2416728-vulnerability-in-asp-net-and-sharepoint.aspx**

Avis Microsoft

- Références
  - http://blogs.technet.com/b/srd/archive/2010/09/17/understanding-the-asp-net-vulnerability.aspx
  - http://blogs.technet.com/b/srd/archive/2010/09/20/additional-information-about-the-asp-net-vulnerability.aspx
  - http://weblogs.asp.net/scottgu/archive/2010/09/18/important-asp-net-security-vulnerability.aspx
  - http://weblogs.asp.net/scottgu/archive/2010/09/24/update-on-asp-net-vulnerability.aspx

  - http://netifera.com/research/
  - http://twitter.com/julianor
  - http://ekoparty.org/juliano-rizzo-2010.php

Avis Microsoft

- **Révisions**
  - **MS10-050**
    - **V1.2: disponibilité d'un "Fix It"**
  - **MS10-060**
    - **V1.2: modification du *workaround***
  - **MS10-061**
    - **V1.1: ajout d'un problème connu**
  - **MS10-064**
    - **V1.1: suppression des références à Outlook Express 6**

Infos Microsoft

- **Sorties logicielles**
  - **SQL Server 2008 R2**
    - **Sortie du SP2 et du FP2**
  - **UPHClean 1.6g**
    - **Corrige une vulnérabilité à la faille "*DLL Preloading*"**
      - **http://blogs.technet.com/b/uphclean/archive/2010/09/13/uphclean-v1-6-security-vulnerability-fix.aspx**
  - **Internet Explorer 9 (Beta 1)**
      - **http://www.beautyoftheweb.com/**
  - **Microsoft Security Essentials en version PME (10 postes)**
      - **http://blogs.msdn.com/b/mssmallbiz/archive/2010/09/22/announcing-microsoft-security-essentials-available-free-to-small-businesses-in-october.aspx**
  - **Microsoft Lync Server 2010 (en version RC)**
    - **Alias "Microsoft Communications Server 14"**

Infos Microsoft

- **Autre**
  - **Octobre 2010: lancement de Windows Phone 7**
    - **1 milliard de budget "communication" (minimum)**
      - **http://www.zdnet.com/blog/microsoft/a-billion-to-launch-windows-phone-7-i-bet-microsoft-is-paying-a-lot-more/7238**

Infos Réseau

- **(Principales) faille(s)**
  - **Les failles Cisco IOS**
    - **H.323**
      - **http://www.cisco.com/warp/public/707/cisco-sa-20100922-h323.shtml**
    - **IGMP**
      - **http://www.cisco.com/warp/public/707/cisco-sa-20100922-igmp.shtml**
    - **NAT**
      - **http://www.cisco.com/warp/public/707/cisco-sa-20100922-nat.shtml**
    - **SIP**
      - **http://www.cisco.com/warp/public/707/cisco-sa-20100922-sip.shtml**
    - **SIP (sur CUCM)**
      - **http://www.cisco.com/warp/public/707/cisco-sa-20100922-cucmsip.shtml**
    - **VPN-SSL**
      - **http://www.cisco.com/warp/public/707/cisco-sa-20100922-sslvpn.shtml**
  - ***Backdoor* dans les *switches* Accton**
    - **http://www.attackvector.org/vendor-response-to-backdoor-in-accton-switches-post/**
  - **Faille dans les produits 3Com H3C**
    - **Un paquet DHCP malformé provoque un "déni de service"**
      - **http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-464/CERTA-2010-AVI-464.html**

Infos Réseau

- **Autres infos**

  - **Sortie de SNORT 2.9.0**
    - **http://www.snort.org/snort-downloads**
  - **Le serveur racine "H" a été coupé du monde pendant 18h**
    - **Et personne ne s'en est rendu compte**
      - **http://isc.sans.edu/diary.html?storyid=9655**
  - **Le domaine ".ly" (Lybie) applique désormais la charia**
    - **Dommage pour les raccourcisseurs d'URLs …**
      - **http://benmetcalfe.com/blog/2010/10/the-ly-domain-space-to-be-considered-unsafe/**

Infos Unix

- (Principales) faille(s)
  - Noyau Linux
    - *Integer overflow* dans la gestion des périphériques audio
      - http://git.kernel.org/?p=linux/kernel/git/tiwai/sound-2.6.git;a=commitdiff;h=5591bf07225523600450edd9e6ad258bb877b779
  - Régression sur une faille datant de 2007
    - Réintroduite en avril 2008
    - N'affecte que les noyaux 64 bits
      - http://xorl.wordpress.com/2009/08/07/cve-2007-4573-linux-kernel-ia32-system-call-emulation-vulnerability/
    - Exploitée dans la nature avant publication
      - http://archives.neohapsis.com/archives/fulldisclosure/2010-09/0273.html

Infos Unix

- **Samba < 3.5.5**
  - ***Buffer overflow* exploitable (?) à distance**
    - **http://us1.samba.org/samba/history/samba-3.5.5.html**
- **BZip2 < 1.0.6**
  - ***Integer overflow***
    - **http://www.bzip.org/index.html**
- **Epiphany sous Debian**
  - **Ne vérifie aucun certificat SSL/TLS**
    - **http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=564690**
- **BIND < 9.7.2-P2**
  - **Encore des failles liées au support DNSSEC …**
    - **https://lists.isc.org/pipermail/bind-announce/2010-September/000655.html**
- **PostgreSQL**
  - **Elévation de privilèges (via PERL ou TCL)**
    - **http://www.postgresql.org/about/news.1244**

Infos Unix

- **MIT Kerberos 5**
  - **Déni de service distant (pointeur NULL)**
    - **http://web.mit.edu/kerberos/advisories/MITKRB5-SA-2010-006.txt**
- **RSA Authentication Agent 7.0**
  - ***Directory traversal***
    - **http://archives.neohapsis.com/archives/bugtraq/2010-09/att-0181/rsa2.txt.asc**
- **RSA Authentication Client**
  - **Extraction de la clé privée du token SecurID 800 (!)**
    - **http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-478/CERTA-2010-AVI-478.html**

Infos Unix

- Typo3
  - Correction de failles critiques, dont la lecture de fichiers arbitraires
    - http://typo3.org/teams/security/security-bulletins/typo3-sa-2010-020/
  - Note sur le correctif:
    - if ($juHash == $calcJuHash) {
    - Devient
    - if ($juHash === $calcJuHash) {

- Plesk SiteBuilder 4.5.8
  - Aucune information n'est communiquée par l'éditeur (!)
    - http://autoinstall.plesk.com/SiteBuilder/SiteBuilder_4.5.0/autoupdate/patches/sitebuilder-4.5.8_build2010090700_linux.html

Infos Unix

- **Failles dans "Alcatel-Lucent OmniTouch Contact Center Standard Edition"**
  - **Accès non authentifié à la console d'administration**
    - **(Si le protocole de communication propriétaire est connu)**
  - **Vérification de l'authentification côté client**
  - **(Bienvenue en 2010 !)**
    - **http://www.alcatel-lucent.com/wps/DocumentStreamerServlet?LMSG_CABINET=Corporate&LMSG_CONTENT_FILE=Support/Security/2010001.pdf**

Infos Unix

- Autre
  - Ubuntu 10.10 disponible
    - http://www.ubuntu.com/
  - Noyau Linux
    - commit 1ee89bd0/70789d70
      - "netfilter/ipv6 : discard overlapping IPv6 fragments (per RFC 5722)"
    - CONFIG_NETFILTER_XT_MATCH_CPU

Failles

- **Principales applications**
  - **Mac OS X**
    - **Accès à un partage AFP sans mot de passe**
      - **Il suffit de connaitre un nom d'utilisateur valide (!)**
      - **http://support.apple.com/kb/HT4361**
  - **QuickTime < 7.6.8**
    - **Corrige les failles "_Marshaled_pUnk" et "*DLL preloading*"**
      - **http://support.apple.com/kb/HT4339**

Failles

- Adobe Flash Player < 10.1.85.3
  - Corrige une faille exploitée en "0day" dans la nature
    - http://www.adobe.com/support/security/bulletins/apsb10-22.html
- Adobe Reader < 8.2.5, < 9.4.0
  - Corrige 23 failles, dont une déjà largement exploitée dans la nature
    - http://www.adobe.com/support/security/bulletins/apsb10-21.html
    - Adobe a du avancer son correctif d'une semaine
  - Note: il est possible de protéger Adobe Reader avec l'outil EMET
    - http://blogs.technet.com/b/srd/archive/2010/09/10/use-emet-2-0-to-block-the-adobe-0-day-exploit.aspx
- Foxit Reader < 4.2
  - Signature PDF mal (ou non) vérifiée
    - http://www.foxitsoftware.com/pdf/reader/security_bulletins.php#identity

Failles

- Crédits:
  - Red Hat Security Response Team
  - Tavis Ormandy / Google (x7)
  - James Quirk / Los Alamos
  - Felipe Andres Manzano /iSIGHT Partners Global Vulnerability Partnership
  - Billy Rios / Google
  - Ricardo Narvaja / Core Security Technologies
    - http://www.coresecurity.com/content/adobe-acrobat-acrord23-reader-use-after-free
  - Bing Liu / FortiGuard Labs
  - Will Dormann / CERT
  - Brett Gervasoni / Sense of Security
  - Knud Erik Højgaard / nSense Vulnerability Research Team
  - Sebastian Apelt / ZDI (x2)
  - Anonymous / ZDI
    - http://www.zerodayinitiative.com/advisories/ZDI-10-191/
    - http://www.zerodayinitiative.com/advisories/ZDI-10-192/
    - http://www.zerodayinitiative.com/advisories/ZDI-10-193/

Failles

- FireFox < 3.6.10
  - Corrige simplement un problème de stabilité dans la 3.6.9
- ThunderBird < 3.1.4
  - Pas de corrections de sécurité
- Chrome < 6.0.472.63
  - 6.0.472.59
    - http://googlechromereleases.blogspot.com/2010/09/stable-beta-channel-updates_14.html
  - 6.0.472.62
    - http://googlechromereleases.blogspot.com/2010/09/stable-beta-channel-updates_17.html
- VMWare Workstation < 7.1.1 (ainsi que Player et ACE)
  - Correction des failles libPNG et "*DLL Preloading*"
    - http://www.vmware.com/security/advisories/VMSA-2010-0014.html

Failles

- Un nouvel outil offensif sur le marché
  - INSECT
    - http://www.faltaenvido.org/
- Une nouvelle place de marché pour les *0day*
  - Avec publication forcée au bout de 180 jours
    - https://upsploit.com/

Failles 2.0

- Deux terminaux de paiements Ingenico révoqués par Visa
  - Certification PCI/DSS retirée aux modèles i3070MP01 et i3070EP01
  - Il est trop facile de les remplacer par des clones "backdoorés"
    - http://www.storefrontbacktalk.com/securityfraud/visa-revokes-pci-approval-from-ingenico-pin-pads-following-breach/
- Un ver XSS sur Twitter
  - Suite à une régression du code
    - http://blog.twitter.com/2010/09/all-about-onmouseover-incident.html
- EverCookie
  - Pour pister les utilisateurs du Web quoiqu'il arrive
    - http://samy.pl/evercookie/
- Tous les sites de Malaysie blacklistés
  - Suite à la compromission du seul hébergeur publicitaire local
    - http://www.innity.com/announcement/
  - Au travers d'une faille découverte en "0day" dans le serveur publicitaire OpenX
    - http://blog.sucuri.net/2010/09/openx-users-time-to-upgrade.html

Malwares et spam

- Le ver "Here You Have"
  - Est écrit en Visual Basic
  - Arrive sous forme d'un ".SCR"
  - Se propage à tout le carnet d'adresses
  - Et infecte néanmoins des sociétés comme Comcast, Disney, Procter & Gamble …
  - (… bienvenue en 2010 !)
- Stuxnet Aftermath
  - http://www.pcworld.com/businesscenter/article/205465/microsoft_reveals_stuxnet_worm_exploits_multiple_zero_days.html
  - http://www.digitalbond.com/index.php/2010/09/16/stuxnet-target-theory/
  - http://www.securelist.com/en/blog/2291/Myrtus_and_Guava_Episode_MS10_061
  - http://www.langner.com/en/index.htm
  - (…)

Malwares et spam

- IMDDOS: un service de DDoS "commercial"
  - Basé en Chine
    - http://www.lemondeinformatique.fr/actualites/lire-un-service-chinois-d-attaques-ddos-a-la-demande-31649.html
- Un shellcode pour Windows Mobile 6.5
  - Qui passe des appels téléphoniques ☺
    - http://www.exploit-db.com/exploits/15136/
- Zeus arrive sur Symbian et BlackBerry
  - Permet de récupérer le SMS de confirmation envoyé par la banque
    - http://securityblog.s21sec.com/2010/09/zeus-mitmo-man-in-mobile-i.html
- Une faille exploitée par les "gentils" dans le serveur de contrôle Zeus
    - http://xs-sniper.com/blog/2010/09/27/turning-the-tables/
  - Heureusement (?) le support est réactif
    - http://twitter.com/botnetbiz
- Nombreuses arrestations autour de Zeus
    - http://www.avertlabs.com/research/blog/index.php/2010/09/30/arrest-coming-to-the-us-for-zeus-touting-cybercriminals/

Actualité (francophone)

- La France participe à Cyber Storm III
  - http://www.ssi.gouv.fr/site_article261.html
- Le compte Twitter des Affaires Etrangères piraté
  - Un message en lien avec l'actualité a été posté
    - http://pro.clubic.com/blog-forum-reseaux-sociaux/twitter/actualite-365912-compte-twitter-affaires-etrangeres-pirate.html
- references.modernisation.gouv.fr FAIL
  - http://safebrowsing.clients.google.com/safebrowsing/diagnostic?client=Firefox&hl=fr&site=http://www.references.modernisation.gouv.fr/
- Des failles sur le site de la CNIL
  - http://www.cnil.fr/la-cnil/actu-cnil/article/article/non-le-site-de-la-cnil-nest-pas-grand-ouvert/

Actualité (francophone)

- **Lancement en fanfare du site HADOPI.FR**
  - **http://bluetouff.com/2010/09/23/hadopi-ddos-annonce-hadopi-fr/**
- **Free vs. HADOPI**
  - **http://www.journaldugeek.com/2010/09/22/quand-free-joue-avec-lhadopi/**
  - **http://www.numerama.com/magazine/17008-hadopi-free-sera-rembourse-65-centimes-par-ip-identifiee.html**
- **Un site qui *buzze***
  - **http://surveillermonsalarie.com/**
- **Prim'X annonce la certification EAL3+ de son logiciel "Zed!"**

Actualité (anglo-saxonne)

- Tous les fournisseurs de services de communications devront fournir un point d'entrée aux autorités américaines
  - Inclus Facebook, Skype, BlackBerry, …
    - http://www.nytimes.com/2010/09/27/us/27wiretap.html
- Le "pre-crime" devient réalité
    - http://www.schneier.com/blog/archives/2010/10/monitoring_empl.html
- La nouvelle campagne du DHS pour sensibiliser à la sécurité informatique
  - "Stop. Think. Connect."
    - http://www.dhs.gov/ynews/releases/pr_1286211160622.shtm
  - Note: octobre est le mois de la "Cyber Awareness"
- La stratégie de Cyber Sécurité du Canada
    - http://www.securitepublique.gc.ca/prg/em/cbr/ccss-scc-fra.aspx
- Radware bientôt racheté ?
  - Par HP ou IBM ?
    - http://www.bloomberg.com/news/2010-09-15/radware-represents-best-valuation-for-hp-or-ibm-kreizman-says.html

Actualité (européenne)

- L'Europe va renforcer ses moyens de défense contre les "cyberattaques"
  - http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1239&format=HTML&aged=0&language=FR&guiLanguage=en

Actualité (Google)

- Google ajoute l'authentification "2 facteurs" sur Google Apps
  - Mot de passe + token généré par une application tierce
    - http://googleonlinesecurity.blogspot.com/2010/09/moving-security-beyond-passwords.html
    - http://googleenterprise.blogspot.com/2010/09/more-secure-cloud-for-millions-of.html
    - http://code.google.com/p/google-authenticator/
- Google Chrome Frame en version finale
    - http://www.google.com/chromeframe
- "Google Wave" devient "Wave in the Box"
    - http://googlewavedev.blogspot.com/2010/09/wave-open-source-next-steps-wave-in-box.html
- "Google New"
  - Pour suivre toute l'actualité Google !
    - http://www.google.com/newproducts/

Actualité (crypto)

- **Armadillo FAIL**
  - **http://baboon.rce.free.fr/index.php?post/2010/09/04/Armadillo-mange-des-ours-en-slips**
- **Elcomsoft vs. chiffrement des sauvegardes BlackBerry**
  - **http://www.elcomsoft.com/news/418.html**

Actualité

- OpenOffice n'existe plus
  - Alors, Oracle Cloud Office ou LibreOffice ?
- Oracle pourrait racheter un fabriquant de puces
  - AMD ou nVidia ?
- La virtualisation à venir dans les processeurs ARM
  - http://www.infoworld.com/d/hardware/arms-next-chip-design-will-support-virtualization-software-101

Actualité

- Cryptome.org piraté
  - Les sources ont-elles été compromises ?
    - http://www.wired.com/threatlevel/2010/10/cryptome-hacked/
- La société ACS:Law sévèrement piratée
  - Mais personne ne va les regretter …
    - http://fr.readwriteweb.com/2010/09/26/divers/touch-coul-4chan-vise-acslaw/
- Encore un système de vote électronique piraté
  - Heureusement en phase d'évaluation
    - http://www.wired.com/threatlevel/2010/10/dc-voting-system-hacked/
    - http://voices.washingtonpost.com/debonis/2010/10/hacker_infiltration_ends_dc_on.html

Actualité

- "Low Orbit Ion Cannon"
  - Un outil de DDoS collaboratif
  - Utilisé avec succès contre la RIAA
    - http://techcrunch.com/2010/09/19/riaa-attack/
  - … en représailles aux déclaration de la société Aiplex Software
    - http://www.smh.com.au/technology/technology-news/film-industry-hires-cyber-hitmen-to-take-down-internet-pirates-20100907-14ypv.html
- Opération de police contre ThePirateBay
    - http://bluetouff.com/2010/09/08/the-pirate-bay-les-polices-de-14-pays-unies-pour-un-raid-contre-le-tracker-torrent/
  - Notons que WikiLeaks, THC, … sont actuellement injoignables
- Outils
  - THC-Hydra 5.8
    - http://freeworld.thc.org/thc-hydra/
  - Hex-Rays / IDA Pro 6
    - Entièrement réécrit en QT
    - Interface graphique native Linux

Fun

- Mark Zuckerberg (Facebook) est devenu plus riche que Steve Jobs (Apple)
- Un client BitTorrent pour iPhone
  - Les téléchargements arrivent directement sur ImageShack
    - http://www.intomobile.com/2010/10/04/bittorrent-iphone-appstore/
- NAT et IPv6
    - http://www.xtranormal.com/watch/7011357/
- Plus rapide que l'ADSL
  - Le pigeon !
    - http://www.cnis-mag.com/adsl-pigeons-et-comparaisons-absurdes.html
- Informatique et poésie
    - http://research.google.com/archive/papers/review_in_verse.html

Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 9 novembre 2010
- N'hésitez pas à proposer des sujets et des salles