OSSIR
Groupe Paris

Réunion du 8 février 2011

Revue des dernières vulnérabilités

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

Avis Microsoft

- **Janvier 2010**
  - **2 bulletins, 3 failles**
  - **Références**
    - **http://blogs.technet.com/b/msrc/archive/2011/01/10/january-2011-security-bulletins.aspx**
    - **http://blogs.technet.com/b/msrc/p/january-2011-security-bulletin-q-a.aspx**
  - **MS11-001 Faille dans Windows Backup Manager [1]**
    - **Affecte: Windows Vista**
    - **Exploit: "*DLL Preloading*" à l'ouverture d'un fichier ".wbcat"**
    - **Crédit: n/d**

Avis Microsoft

- **MS11-002 Failles dans MDAC [1,1]**
  - **Affecte: MDAC 2.8 SP1, 2.8 SP2, 6.0**
    - **Donc toutes les versions de Windows supportées**
  - **Exploit:**
    - ***Buffer overflow* sur un DSN trop long**
    - ***Buffer overflow* dans la gestion des enregistrements ADO**
  - **Crédit:**
    - **AbdulAziz Hariri / ZDI-11-001**
    - **Peter Vreugdenhil / ZDI-11-002 (challenge pwn2own)**

Avis Microsoft

- **Prévisions Microsoft pour février**
  - 12 bulletins, dont 3 critiques
  - 22 failles
  - Windows, Internet Explorer, Office, Visual Studio, IIS (FTP sur 7.0 et 7.5)
  - Q2490606 (support des miniatures) et Q2488013 (IE)

- **Advisories**
  - Q973811 "Extended Protection for Authentication"
    - V1.10: ajout de Microsoft Office Live Meeting Service Portal
    - V1.11: correction d'un lien
  - Q2269637 "DLL Preloading"
    - V4.0: ajout de la référence à MS11-001
  - Q2488013 Faille dans les feuilles de style sous IE
    - V1.2: disponibilité d'un workaround logiciel
      - http://blogs.technet.com/b/srd/archive/2011/01/11/new-workaround-included-in-security-advisory-2488013.aspx
    - V1.3: impact du workaround = 150 ms

Avis Microsoft

- **Q2490606 Faille dans le support des miniatures**
  - **V1.1: disponibilité d'un "fix-it"**
  - **V1.2: le *workaround* ne fonctionne que sur Windows XP et 2003, nouveau *workaround***

- **Q2501696 XSS générique au travers du protocole mhtml://**

  - **Un problème ancien ?**
    - **Cf. Adobe Flash Player il y a quelques semaines**
    - **Cf. http://openmya.hacker.jp/hasegawa/security/ms07-034.txt**

  - **… mais qui refait surface grâce à Google**
    - **http://blogs.technet.com/b/srd/archive/2011/01/28/more-information-about-the-mhtml-script-injection-vulnerability.aspx**
    - **http://blogs.technet.com/b/msrc/archive/2011/01/28/microsoft-releases-security-advisory-2501696.aspx**

Avis Microsoft

- **Révisions**
  - **MS10-001**
    - **V1.1: ajout d'un problème connu**
  - **MS10-102**
    - **V1.1: le patch ne s'installe que sur les systèmes affectés**
      - **Avec le rôle Hyper-V**

Infos Microsoft

- **Sorties logicielles**
  - **System Center Service Manager 2010 SP1**
  - **SQL Server 2005 SP4 RTM**
  - **Windows 7 / 2008R2 SP1 RTM**
  - **El Jefe (Immunity)**
    - **Un outil Open Source et pragmatique pour détecter les comportements anormaux**
      - **http://www.immunityinc.com/products-eljefe.shtml**

Infos Microsoft

- Autre
  - Microsoft France organise la première "Fail Conference"
    - https://msevents.microsoft.com/CUI/EventDetail.aspx?EventID=103247 5040&Culture=fr-FR
  - Entropie du /GS en mode noyau: échec
    - http://j00ru.vexillium.org/?p=690
  - Secunia va couvrir le *patch Tuesday*
    - http://secunia.com/blog/172/
  - Bug FTP sur IIS 7.5
    - Inexploitable ?
      - http://illmatics.com/FTPOwned.PNG

Infos Microsoft

- **Du recrutement agressif**
  - **http://www.reddit.com/r/ReverseEngineering/comments/fg1d3/identity_of_sourceforge_and_unrealircd_backdoor/**
- **Hotmail offre des adresses jetables**
  - **http://windowsteamblog.com/windows_live/b/windowslive/archive/2011/02/03/hotmail-delivers-aliases-to-help-you-manage-and-secure-your-email-account.aspx**

Infos Réseau

- (Principales) faille(s)
  - Cisco Quaterly Patch
    - Cisco ASA: failles multiples
      - SIP, ACLs, Mobile User Security, multicast, LAN-to-LAN IPSEC, ASDM, IPv6 ND, EIGRP, Telnet, IPSEC, emWEB, "device startup" (!), OCSP, CIFS, SMTP, LDAP
        - http://www.cisco.com/en/US/docs/security/asa/asa82/release/notes/asarn82.pdf
        - http://www.cisco.com/en/US/docs/security/asa/asa83/release/notes/asarn83.pdf
    - Cisco IOS 15: failles multiples
      - IRC, H323, CallManager Express, SIP, TFTP, certificats, SCCP Telephony Control Application, IPv6 ND
        - http://www.cisco.com/en/US/docs/ios/15_0/15_0x/15_01_XA/rn800xa.pdf
    - Cisco Content Security Gateway
        - http://www.cisco.com/warp/public/707/cisco-sa-20110126-csg2.shtml

Infos Réseau

- Cisco CUCM
  - Evasion du *shell* restreint
    - http://vimeo.com/17757820
- Cisco Tandberg C Series, E/EX Personal Video
  - Login: root
  - Password: *aucun*
    - http://www.cisco.com/warp/public/707/cisco-sa-20110202-tandberg.shtml
- Cisco WebEx Player
  - Failles multiples dans le contrôle ActiveX
    - http://www.cisco.com/warp/public/707/cisco-sa-20110201-webex.shtml
- Cisco/Linksys WRT54GC
  - *Buffer overflow* dans le traitement d'une requête POST
    - http://tools.cisco.com/security/center/viewAlert.x?alertId=22228

Infos Réseau

- **BlueCoat**
  - **Version OpenSSL vulnérable à un *downgrade***
    - **https://kb.bluecoat.com/index?page=content&id=SA53**
- **ISC DHCPd**
  - **Crash sur une réponse DHCPv6 malformée**
    - **https://lists.isc.org/pipermail/isc-os-security/2011-January/000000.html**
- **Asterisk**
  - ***Stack overflow* dans la pile SIP**
    - **http://downloads.asterisk.org/pub/security/AST-2011-001.html**
- **Huawei FAIL**
    - **http://www.websec.ca/blog/view/mac2wepkey_huawei**

Infos Réseau

- Autres infos
  - La Tunisie intercepte le trafic SSL
    - Injection de JavaScript malveillant à la volée
    - Blocage du HTTPS
      - http://www.fastcompany.com/1715575/tunisian-government-hacking-facebook-gmail-anonymous
  - L'Egypte se coupe d'Internet
    - Grâce à BGP
      - http://extraexploit.blogspot.com/2011/01/egypt-telecom-as-isolation-bgplay-show.html
    - Les effets de bord sont intéressants
  - La possible création d'un ".music" attire les foudres de la RIAA
      - http://www.techdirt.com/articles/20110119/02303312714/riaa-threatening-icann-about-music-claiming-it-will-be-used-to-infringe.shtml

Infos Réseau

- "IPv6 Day"
  - Le 8 juin 2011
    - http://www.zdnet.fr/blogs/infra-net/ipv6-day-l-isoc-a-planifie-avec-des-acteurs-de-l-internet-un-grand-test-d-ipv6-le-8-juin-2011-39757439.htm
    - http://isoc.org/wp/worldipv6day/how-to-join/

- D'ailleurs, IPv4 … c'est fini !
    - http://www.ipv4depletion.com/?page_id=326

Infos Unix

- (Principales) faille(s)
  - OpenSSH 5.6 et 5.7
    - Fuite d'informations sur la pile si un certificat "legacy" est présenté
      - http://www.openssh.com/txt/legacy-cert.adv
  - sudo < 1.7.4p5
    - Pas de mot de passe demandé pour changer de groupe
      - http://www.sudo.ws/sudo/alerts/runas_group_pw.html
      - http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=609641
  - Bug "strtod()" sur PHP
    - Affecte aussi Java
    - Car le problème vient de GCC !
      - http://blog.mageekbox.net/?post/2011/02/01/%C3%80-propos-du-bug-53632-de-PHP

Infos Unix

- Majordomo EPIC FAIL
  - http://www.exploit-db.com/exploits/16103/
- LibPNG
  - Faille dans png_set_rgb_to_gray()
    - http://sourceforge.net/mailarchive/message.php?msg_id=26866318
- RedHat OpenJDK IcedTea6
  - Exécution de code grâce au ClassLoader
    - ZDI-11-014
- Exim4
  - Ecrasement de fichiers arbitraires
    - http://www.debian.org/security/2011/dsa-2154

Infos Unix

- SPIP < 2.1.8
  - http://core.spip.org/projects/spip/repository/revisions/16966
  - http://www.spip-contrib.net/SPIP-2-1-8-corrige-une-importante-faille-de-securite
- Struts <= 2.1.8.1
  - Exécution de code Java à distance (!)
  - Pourtant déjà patchée (!!)
    - http://struts.apache.org/2.2.1/docs/s2-005.html
  - Correctif: Struts 2.2.1
- Subversion < 1.6.15
  - http://svn.apache.org/repos/asf/subversion/tags/1.6.15/CHANGES
- Bugzilla
  - http://www.bugzilla.org/security/3.2.9/
- Prewikka
  - Le mot de passe de la base SQL est en lecture pour "world"
    - http://www.gentoo.org/security/en/glsa/glsa-201101-07.xml

Infos Unix

- Sybase EAServer
  - Installation d'applications à distance
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=888
  - *Directory traversal*
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=889

- IBM WebSphere MQ < 7.0.1.4
  - *Buffer overflow* exploitable à distance
    - http://xforce.iss.net/xforce/xfdb/64628

- IBM Tivoli Access Manager
  - *Directory traversal*
    - http://xforce.iss.net/xforce/xfdb/64737

Infos Unix

- EMC Networker
  - Il est possible de contourner les restrictions d'accès en envoyant un paquet UDP avec la source spoofée '127.0.0.1'
    - http://archives.neohapsis.com/archives/bugtraq/2011-01/att-0162/ESA-2011-003.txt

- HP/UX
  - Faille dans l'implémentation Kerberos
    - http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02657328

Infos Unix

- Autre
  - Debian 6 est sorti
    - http://news.debian.net/2011/02/06/debian-6-0-0-codename-squeeze-is-out/
  - Fedora compromis
    - Par des n00bs ☺
      - http://lists.fedoraproject.org/pipermail/devel-announce/2011-January/000746.html
      - https://threatpost.com/en_us/blogs/fedora-system-compromised-012511
  - Des news de l'équipe sécurité Debian
    - http://lists.debian.org/debian-devel-announce/2011/01/msg00006.html
  - Sécurité Ubuntu
    - Des choses intéressantes
      - https://wiki.ubuntu.com/Security/Features#ptrace

Failles

- **Principales applications**
  - **Oracle Quaterly Patch**
    - **66 failles corrigées**
      - **http://www.oracle.com/technetwork/topics/security/cpujan2011-194091.html**
      - **ZDI-11-016 … ZDI-11-020**
    - **Quelques trucs "rigolos"**
      - **Exécution anonymes de *commandes* sur Oracle Audit Vault**
        - **http://www.teamshatter.com/topics/security-advisory/advisory-oracleremexecservice-command-excution-via-named-pipe-vulnerability-windows-only/**
        - **http://www.teamshatter.com/topics/security-advisory/advisory-oracle-database-vault-administrator-web-console-session-id-disclosure/**
        - **http://www.teamshatter.com/topics/security-advisory/advisory-oracle-database-vault-administrator-web-console-vulnerable-to-cross-site-request-forgery/**
      - **Faille exploitable à distance dans Solaris CDE Calendar Manager**
      - **Faille dans le *parser* PowerPoint pour OpenOffice**

Failles

- Adobe Reader (ce soir)
  - http://www.adobe.com/support/security/bulletins/apsb11-03.html
- FireFox < 3.6.14 (bientôt)
  - https://wiki.mozilla.org/Releases
- Opera < 11.01
  - http://www.opera.com/docs/changelogs/windows/1101/
  - https://www.alternativ-testing.fr/blog/index.php?post/2011/[CVE-XXXX-XXXX]-Opera-11-Integer-Truncation-Vulnerability
- QuickTime < 7.6.9 (iTunes < 10.1.2 ?)
  - ZDI-11-038
- VLC < 1.1.7
  - http://www.videolan.org/security/sa1102.html

Failles

- Google Chrome < 8.0.552.237
  - La prime de $3,133.7 a été payée pour la première fois
    - http://googlechromereleases.blogspot.com/2011/01/chrome-stable-release.html
- Google Chrome < 9.0.597.84
    - http://googlechromereleases.blogspot.com/2011/02/stable-channel-update.html
- Android FAIL
    - http://blog.metasploit.com/2011/01/mobile-device-security-and-android-file.html

Failles

- WireShark < 1.2.14, < 1.4.3
  - http://www.wireshark.org/security/wnpa-sec-2011-01.html
  - http://www.wireshark.org/security/wnpa-sec-2011-02.html
- OpenOffice < 3.3.0
  - Cf. Oracle Quaterly Patch
    - http://www.openoffice.org/security/bulletin.html
    - http://development.openoffice.org/releases/3.3.0.html
- IBM DB2 9.x
  - Failles multiples (ZDI-11-035, ZDI-11-036, …)
    - https://www-304.ibm.com/support/docview.wss?uid=swg21426108
- RealPlayer
  - ZDI-11-033
- Citrix Provisioning Services < 5.6 SP1
  - ZDI-11-023
    - http://support.citrix.com/article/CTX127149

Failles

- Symantec Web Gateway
  - Injection SQL
    - http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=2011&suid=20110112_00
    - ZDI-11-013
- Symantec Alert Management Service
  - … dont des exécutions de *commandes*
    - ZDI-11-028 ... ZDI-11-032
    - http://telussecuritylabs.com/threats/show/FSC20100727-01
    - http://telussecuritylabs.com/threats/show/FSC20101213-06
- Symantec IM Manager Administrative Interface
    - ZDI-11-037

Failles

- BlackBerry PDF Distiller
  - (Encore) des failles découvertes
    - http://www.blackberry.com/btsc/search.do?cmd=displayKC&docType=kc&externalId=KB25382

- "Déni de service" sur le navigateur BlackBerry
  - Embarqué dans les téléphones
    - http://www.blackberry.com/btsc/search.do?cmd=displayKC&docType=kc&externalId=KB24841
    - http://blog.tehtri-security.com/2011/01/blackhat-dc-2011-inglourious-hackerds.html

Failles

- HP OpenView
  - Encore un certain nombre de failles …
    - ZDI-11-003 ... ZDI-11-012
    - … dont une injection de commandes (!)
  - … et une *backdoor* (!!)
    - ZDI-11-034
- HP LoadRunner 9.52
  - Exécution de code sans authentification sur les ports TCP/5001, TCP/5002, TCP/5003, TCP/50500, TCP/54345
    - ZDI-11-015
  - Correctif: fermer les ports ☺
    - http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02680678
- HP Data Protector
  - ZDI-11-024

Failles 2.0

- **Facebook: les applications auront accès à l'adresse postale et au numéro de portable**
  - **http://developers.facebook.com/blog/post/446**
- **Facebook passe sur HTTPS**
  - **http://blog.facebook.com/blog.php?post=486790652130**
- **Quelques comptes Facebook piratés**
  - **Nicolas Sarkozy**
  - **Mark Zuckerberg**

Failles 2.0

- Les sites piratés du mois
  - NASDAQ
    - http://online.wsj.com/article/SB10001424052748704709304576124502351634690.html
  - Zynga
    - £7.4m volés en jetons virtuels
    - http://www.thinq.co.uk/2011/2/3/brit-hacks-zynga-plunders-12m-poker-chips/
  - PlentyOfFish
    - Communication ratée
    - https://plentyoffish.wordpress.com/2011/01/31/plentyoffish-hacked/
  - Gregory Evans / Ligatt Security

Failles 2.0

- HBGary / Rootkit.com
  - http://xorl.wordpress.com/2011/02/07/news-recent-hacks/
- La bourse européenne du CO2
  - Un simple phishing, 28 M€ de pertes
  - http://www.nytimes.com/2011/01/21/business/global/21carbon.html
- L'intégralité des citoyens brésiliens
  - D'après Kaspersky
  - http://www.securelist.com/en/blog/11125/Your_personal_data_in_the_wrong_hands
- Le code source de Kaspersky
  - C'est confirmé
  - L'auteur de la fuite est un employé

Failles 2.0

- Qui veut un *shell* sur SourceForge ou army.mil ?
  - http://www.srblche.com/index.html
  - Et ça a l'air de fonctionner
    - http://extraexploit.blogspot.com/2011/01/sourceforge-entry-point-seems-still.html
  - SourceForge confirme avoir été compromis
    - http://sourceforge.net/apps/wordpress/sourceforge/2011/01/27/sourceforge-net-attack-update/
    - http://sourceforge.net/blog/sourceforge-attack-full-report/
- EFF vs. Sécurité des mobiles
  - https://www.eff.org/deeplinks/2011/01/dont-sacrifice-security-mobile-devices
- Avoir du WiFi partout avec son Android
  - … même illégalement
    - http://underdev.org/penetrate/

Failles 2.0

- Gawker passe sur OAuth
  - Suite à la compromission récente de sa base de données ?
    - http://www.securityvibes.com/community/en/blog/2011/01/12/end-in-sight-for-gawker-password-problems
- Sur quels sites êtes-vous logués ?
    - https://grepular.com/Abusing_HTTP_Status_Codes_to_Expose_Private_Information
- MySpace licencie 600 personnes
  - Soit la moitié de ses effectifs
    - http://networkeffect.allthingsd.com/20110110/myspace-plans-to-lay-off-550-to-600-employees-tomorrow/

Malwares et spam

- Dancho Danchev a disparu
  - http://www.zdnet.com/blog/security/we-need-help-with-the-strange-disappearance-of-dancho-danchev/7897
  - Interné dans un hôpital psychiatrique en Bulgarie (!?)
    - http://news.ycombinator.com/item?id=2112135
  - Mais tout est bien qui finit bien pour lui
- Un ver Twitter
  - … pour installer du *Rogue Antivirus*
    - http://isc.sans.edu/diary.html?storyid=10297
- Panda vs. cybercriminalité
  - http://press.pandasecurity.com/news/pandalabs-uncovers-alarming-statistics-on-cyber-crime-black-market/

Malwares et spam

- Le gouvernement anglais victime de Zeus
  - http://www.zdnet.co.uk/news/security-threats/2011/02/04/hague-uk-government-fell-victim-to-zeus-attack-40091685/
- Waledac a volé 500,000 comptes POP et 125,000 comptes FTP
  - https://threatpost.com/en_us/blogs/research-reveals-huge-cache-ftp-email-credentials-stolen-wal
- StuxNet *reversé* en C++
  - http://amrthabet.blogspot.com/2011/01/reversing-stuxnets-rootkit-mrxnet-into.html

Actualité (francophone)

- Un SSLL obtient l'annulation d'un marché public citant nommément des produits logiciels
  - A savoir Oracle et Business Objects
    - http://www.nexedi.com/fr/news-annulation.marche.public.hostile.au.libre
- Appel à projets "Cloud Computing"
    - http://www.telecom.gouv.fr/rubriques-menu/soutiens-financements/programmes-nationaux/investissements-avenir-developpement-economie-numerique/cloud-computing/lancement-appel-cloud-computing-2511.html
- Bientôt du télétravail dans la fonction publique ?
    - http://www.greenit.fr/article/bonnes-pratiques/le-teletravail-va-se-developper-dans-la-fonction-publique-3414
- Une interview de Michel Benedittini (ANSSI)
    - http://www.itespresso.fr/michel-benedittini-anssi-notre-mission-preparer-la-societe-francaise-a-resister-a-des-attaques-informatiques-40117.html
- Le CERT-LEXSI lance un site pour lutter contre le phishing
  - En partenariat avec Microsoft et Paypal
    - http://www.phishing-initiative.com/

Actualité (francophone)

- Un loi pour gérer le ".fr"
  - L'ancienne avait été annulée par le Conseil Constitutionnel
    - http://www.itespresso.fr/deputes-adoptent-nouvelle-loi-noms-domaine-40389.html
- Un loi pour "l'opt-in"
    - http://www.senat.fr/leg/ppl10-205.html
- Faille triviale sur le site du Ministère de la Culture
    - http://www.ecrans.fr/Un-bug-du-Ministere-de-la-Culture,11897.html
- La protection des portables au CNRS
    - http://www.univ-paris-diderot.fr/2011/01-CNRS-portables.pdf
- Quelques publications de la Haute Autorité de Santé
    - http://www.has-sante.fr/portail/jcms/c_1021245/systemes-informatiques-d-aide-a-la-decision-medicale
    - http://www.has-sante.fr/portail/jcms/c_1016364/referentiel-de-certification-par-essai-de-type-des-logiciels-hospitaliers-daide-a-la-prescription
- Buyster: le paiement par téléphone portable arrive
    - http://www.orange.com/fr_FR/presse/communiques/cp110203fr.jsp

Actualité (francophone)

- *Nearshore* … FAIL
  - http://www.itespresso.fr/tunisie-france-telecom-orange-a-enclenche-un-dispositif-d-urgence-40419.html
- La sécurité de l'Elysée entre de bonnes mains ?
  - http://causerie.blog.tdg.ch/archive/2011/01/20/la-securite-informatique-de-la-france-entre-les-mains-d-un-p.html
- HADOPI passe la seconde ?
  - Les premiers recommandés sont partis
    - http://lci.tf1.fr/high-tech/2011-01/hadopi-passe-la-deuxieme-et-promet-d-accelerer-6220598.html
- MegaUpload recommande de quitter Orange
  - http://www.pcinpact.com/actu/news/61346-megaupload-conseille-quitter-orange-sfr-free.htm

Actualité (anglo-saxonne)

- Il y a une application pour tout
  - … y compris pour se faire recruter par la NSA
    - http://www.nsa.gov/public_info/press_room/2011/new_recruit_tools.shtml
- CyberSecurity Challenge UK
    - https://cybersecuritychallenge.org.uk/
- USA: enregistrer tout le trafic Internet ?
    - http://news.cnet.com/8301-31921_3-20029393-281.html
- Les bibliothèques de Portsmouth fermées pendant 2 semaines (au moins)
  - Pour cause de virus
    - http://www.portsmouth.co.uk/newshome/Virus-shuts-down-computer-network.6691374.jp

Actualité (européenne)

- **Implications de la directive "Data Breach Notification"**
  - **http://www.enisa.europa.eu/act/it/library/deliverables/dbn/at_download/fullReport**
- **Un workshop sur les botnets**
  - **9 et 10 mars 2011 à Cologne**
    - **http://www.enisa.europa.eu/media/news-items/call-for-participation-workshop-on-botnets**
- **La Suisse se met à la CyberGuerre**
  - **http://www.swissinfo.ch/fre/sciences_technologies/La_Suisse_s_arme_pour_la_cyberguerre_de_demain.html?cid=29192718**

Actualité (Google)

- Bing utilise-t-il les résultats de Google ?
  - http://googleblog.blogspot.com/2011/02/microsofts-bing-uses-google-search.html
- Google vs. Egypte
  - http://www.google.com/crisisresponse/egypt.html
  - A noter aussi
    - http://twitter.com/#!/speak2tweet
- Google Cloud Print
  - http://googlemobile.blogspot.com/2011/01/cloud-printing-on-go.html
- Google filtre les recherches de Torrent
  - Particulièrement RapidShare et MegaUpload
    - http://torrentfreak.com/google-starts-censoring-bittorrent-rapidshare-and-more-110126/
- Android vs. Java: ça se précise
  - http://www.engadget.com/2011/01/21/android-source-code-java-and-copyright-infringement-whats-go/
- Eric Schmidt remplacé par Larry Page au poste de DG

Actualité (crypto)

- Le même *bullshit* qui revient sans cesse
  - Amazon Web Services utilisé pour casser du WPA
    - http://www.readwriteweb.com/cloud/2011/01/researcher-developbrute-force.php
  - … jusqu'à 6 caractères
- Les auteurs du "hack PS3" poursuivis par Sony
  - La factorisation est-elle légale ?
    - http://www.scribd.com/doc/46739945/Motion-for-TRO

Actualité

- **Sorties logicielles**
  - **Hydra 6.0 puis 6.1**
    - **http://freeworld.thc.org/thc-hydra/**
  - **OpenSSH 5.7 puis 5.8**
    - **Support des courbes elliptiques**
  - **Nmap 5.50**
    - **Support du protocole gopher://**
  - **Une place de marché pour les "exploits"**
    - **http://www.exploithub.com/**

Actualité

- **Conférence Black Hat Federal 2010**
  - **http://www.blackhat.com/html/bh-dc-11/bh-dc-11-briefings.html**

  - **Quelques conférences notables**
    - **Exploitation Android**
    - **Apple XNU Sandbox**
    - ***Kernel Pool Exploitation* sur Windows Seven**
    - **Attaque du *baseband***
    - ***…***

  - **Quelques annonces intéressantes de Microsoft**
    - **http://blogs.msdn.com/b/sdl/archive/2011/01/17/other-interesting-news-from-blackhat-dc.aspx**

    - **"Attack Surface Analyzer"**
      - **Un outil pour délimiter le périmètre d'une application … sur Windows 7 x64**
    - **"Threat Modeling Tool" 3.1.6**
    - **BinScope 1.2**
    - ***Consulting* autour du SDL (par Microsoft Services)**

Actualité

- Une étude internationale de l'ISACA
  - 40% des entreprises ne vont pas aller sur des solutions "Cloud"
    - La sécurité est un frein dans 50% de cas
  - 93% cherchent à externaliser leur informatique
    - http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/ITGI-Global-Survey-Results.aspx
- CLUSIF: panorama de la cybercriminalité 2010
    - http://www.clusif.asso.fr/fr/production/ouvrages/type.asp?id=CYBER-CRIMINALITE
- Cisco Annual Security Report
    - http://www.cisco.com/en/US/prod/vpndevc/annual_security_report.html
- Une étude de TrustWave sur les pertes de données
  - Note: enregistrement requis
    - https://www.trustwave.com/GSR

Actualité

- Faut-il riposter aux "cyber-attaques" ?
  - http://www.networkworld.com/news/2011/012011-retaliation-answer-cyber-attacks.html?hpg1=bn
- L'OCDE relativise la "cyber-guerre"
  - http://www.oecd.org/dataoecd/3/36/46895979.pdf
- Le "bouton rouge" refait surface
  - http://www.wired.com/threatlevel/2011/02/hoover/
- Du Cloud qui rapporte gros
  - 1 M$ distribué aux participants par tirage au sort
    - http://www.charity-engine.org/
    - http://www.crunchbase.com/company/the-charity-engine

Actualité

- OpenLeaks
  - http://openleaks.org/
- Apple nomme un nouveau "Director of Global Security"
  - David Rice
    - http://www.h-online.com/security/news/item/Apple-appoints-new-director-of-global-security-1175372.html
- Un site communautaire lancé par HP
  - http://cloud-experience.fr/
- Un moteur de recherche décentralisé
  - http://yacy.de/
- Dell rachète SecureWorks
  - http://content.dell.com/us/en/corp/d/secure/2011-01-04-ir-shld-release.aspx

Fun

- *Backdoor* OpenBSD == StuxNet
  - Attention, troll ☺
    - http://extendedsubset.com/?p=43
- Le *pentest* … sous forme de série TV !
    - http://www.youtube.com/watch?v=z0JelXjf_Lk
- Zero Day: le livre
  - Par Mark Russinovitch
    - http://blogs.technet.com/b/sysinternals/archive/2011/01/18/announcing-zero-day-a-novel-by-mark-russinovich.aspx
- Fun avec les IDN
    - http://twitter.com/postmodern_mod3/status/24986898254532608
- Fake or Fail ?
    - http://w0ofer.net/distortbox-examinez-votre-environnement/

Fun

- 32% des américains utilisent le WiFi de leur voisin
  - Lorsque celui-ci n'a pas de protection
    - http://www.usatoday.com/tech/news/2011-02-04-wifimoochers04_ST_N.htm
- Wikipedia par DNS
  - nslookup -q=txt *geek*.wp.dg.cx
- Le virus "Brain" a 25 ans
    - http://www.f-secure.com/weblog/archives/00002087.html
- Un bug pour l'histoire
  - Windows 95 vs. 80386
    - https://blogs.msdn.com/b/oldnewthing/archive/2011/01/12/10114521.aspx
- La PirateBox
    - http://www.korben.info/tuto-piratebox.html

Fun

- 30 millions de dollars pour les LolCats
  - http://www.lepost.fr/article/2011/01/20/2377707_les-lolcats-attirent-des-millions-comment-devenir-riches-avec-des-chats-mignons.html
- Le Pape contre les réseaux sociaux
  - http://www.smh.com.au/technology/technology-news/pope-warns-of-alienation-risk-in-social-networks-20110125-1a390.html

Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 5 avril 2011
  - Conférence JSSI le 22 mars 2011 - venez nombreux !
- N'hésitez pas à proposer des sujets et des salles