OSSIR
Groupe Paris

Réunion du 17 mai 2011

Revue des dernières vulnérabilités

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

Avis Microsoft

- **Avril 2011**
  - **17 bulletins (9 critiques), 64 failles**
    - **http://blogs.technet.com/b/srd/archive/2011/04/12/assessing-the-risk-of-the-april-security-updates.aspx**
    - **http://blogs.technet.com/b/msrc/archive/2011/04/12/april-2011-security-bulletin-release.aspx**
    - **http://blogs.technet.com/b/msrc/archive/2011/04/14/q-amp-a-from-april-2011-security-bulletin-webcast.aspx**
  - **MS11-018 Correctif cumulatif pour Internet Explorer [1,1,?,3,1]**
    - **Affecte: IE (toutes versions supportées, sauf IE9)**
    - **Exploit:**
      - **Fuite d'information sur la mémoire**
      - **Exécution de code**
    - **Crédit:**
      - **Anonymous / iDefense**
      - **MITRE**
      - **Michal Zalewski / Google**
      - **David Bloom / Google (x2)**
      - **Stephen Fewer / Harmony / ZDI-11-119 / pwn2own**
        - **http://blogs.technet.com/b/srd/archive/2011/04/12/ms11-018-addresses-the-ie8-pwn2own-vulnerability.aspx**

Avis Microsoft

- **MS11-019 Failles dans le client SMB [2,1]**
  - **Affecte: Windows (toutes versions supportées)**
  - **Exploit: exécution de code en mode noyau sur une réponse SMB malformée**
    - **http://blogs.technet.com/b/srd/archive/2011/04/12/ms11-019-and-ms11-020-april-smb-updates.aspx**
  - **Crédit: n/d**

- **MS11-020 Failles dans le serveur SMB [1]**
  - **Affecte: Windows (toutes versions supportées)**
  - **Exploit: exécution de code en mode noyau sur une requête SMB malformée**
    - **http://blogs.technet.com/b/srd/archive/2011/04/12/ms11-019-and-ms11-020-april-smb-updates.aspx**
  - **Crédit: n/d**

Avis Microsoft

- MS11-021 Failles dans Excel [1,1,1,2,2,2,1,1,1]
  - Affecte: Office (toutes versions supportées sauf Works 9)
  - Exploit: exécution de code à l'ouverture d'un document malformé
    - ZDI-11-120, ZDI-11-121
  - Crédit:
    - Alin Rad Pop / Secunia Research (x2)
    - Muhammad Junaid Bohio / Telus Security Labs
    - Rodrigo Rubira Branco / Check Point Vulnerability Discovery Team (VDT)
    - Aniway / ZDI (x3)
    - Anonymous / ZDI (x2)
    - Anonymous / iDefense

- MS11-022 Failles dans PowerPoint [2,2,1]
  - Affecte: Office (toutes versions supportées)
    - Y compris Office Web Apps
    - Sauf Works 9
  - Exploit: exécution de code à l'ouverture d'un document malformé
  - Crédit: Anonymous / ZDI-11-123, ZDI-11-124, ZDI-11-125

Avis Microsoft

- MS11-023 Failles dans Office [1,2]
  - Affecte: Office XP / 2003 / 2007, Office 2004 / 2008 pour Mac, convertisseur pour Mac
  - Exploit:
    - "DLL Preloading"
    - Exécution de code à l'ouverture d'un document malformé
  - Crédit: Haifei Li / Fortinet

- MS11-024 Faille dans Windows Fax Cover Page Editor [3]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: exécution de code à l'ouverture d'un fichier ".cov" malformé
  - Crédit: Carsten Eiram / Secunia
    - http://secunia.com/blog/216/

Avis Microsoft

- **MS11-025 Faille MFC [1]**
  - **Affecte: Visual Studio (toutes versions supportées)**
  - **Exploit: "DLL Preloading" dans toutes les applications compilées**
  - **Crédit: n/d**

- **MS11-026 Faille dans le support du protocole mhtml:// [3]**
  - **Affecte: Windows (toutes versions supportées)**
  - **Exploit: *cross-site scripting* universel**
    - **Exploité dans la nature avant la disponibilité du correctif**
  - **Crédit: Google Security Team**

Avis Microsoft

- MS11-027 Mise à jour des "kill bits" [?,?,?]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: exécution de code au travers de composants ActiveX vulnérables
    - IE8 Developer Tools
    - WMITools
    - Windows Messenger
    - (Oracle) Java Deployment Toolkit
    - (CA) WebScan
    - (IBM) Rational Suite License
  - Crédit:
    - Chris Ries / Carnegie Mellon University Information Security Office
    - RadLSneak / iSIGHT Partners Global Vulnerability Partnership

- MS11-028 Faille dans .NET [1]
  - Affecte: .NET Framework (toutes versions supportées)
    - Sauf 1.1 SP1, 2.0 SP1, 3.0, 3.0 SP1, 3.5 … et SilverLight
  - Exploit: évasion de la sandbox
    - http://weblog.ikvm.net/PermaLink.aspx?guid=19f8fefc-d782-48ef-8c6c-f4a2aef471e4
  - Août 2010 …
    - https://connect.microsoft.com/VisualStudio/feedback/details/583519/generic-list-of-value-types-with-sequential-layout-and-pack-size-x86-jit-engine-bug
  - Crédit: n/d

Avis Microsoft

- **MS11-029 Faille dans GDI+ [1]**
  - **Affecte:**
    - **Windows (toutes versions supportées, sauf Seven et 2008R2)**
    - **Office XP SP3**
  - **Exploit: exécution de code à l'ouverture d'un fichier ".emf" malformé**
  - **Crédit: Nicolas Joly & Chaouki Bekrar / VUPEN**

- **MS11-030 Faille dans la résolution DNS [2]**
  - **Affecte: Windows (toutes versions supportées)**
  - **Exploit: exécution de code lors d'une réponse LLMNR malformée**
  - **Crédit: Neel Mehta / Google**

Avis Microsoft

- MS11-031 Faille dans JScript/VBScript [2]
  - Affecte: JScript/VBScript <= 5.8 (si IE9 n'est pas installé)
  - Exploit: exécution de code natif depuis un script (par corruption mémoire)
  - Crédit: Jesse Ruderman / Mozilla

- MS11-032 Faille dans le support des polices OpenType CFF [3]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: exécution de code en mode noyau
    - Exploitable via une page Web sur Windows Vista/2008/Seven/2008R2
  - Crédit: Adam Twardoch / Fontlab

Avis Microsoft

- **MS11-033 Faille dans Wordpad [1]**
  - **Affecte: Windows XP & 2003**
  - **Exploit: exécution de code à l'ouverture d'un fichier Word malformé**
  - **Crédit: Carsten Eiram / Secunia**

- **MS11-034 Failles dans Win32k.sys [1, 1, 1, 1, 1, 1, 1, 1, 1, 1 ,1 ,1 ,1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 2, 1, 1, 1, 3, 1, 1, 1, 1]**
  - **Affecte: Windows (toutes versions supportées)**
  - **Exploit: élévation de privilèges locale**
    - **http://blogs.technet.com/b/srd/archive/2011/04/12/ms11-034-addressing-vulnerabilities-in-the-win32k-subsystem.aspx**
  - **Crédit: Tarjei Mandt / Norman (x30) (!)**

Avis Microsoft

- **Mai 2011**
  - **2 bulletins (1 critique), 3 failles**
    - **http://blogs.technet.com/b/msrc/archive/2011/05/10/may-2011-security-bulletin-release.aspx**
    - **http://blogs.technet.com/b/msrc/archive/2011/05/12/q-amp-a-from-may-2011-security-bulletin-webcast.aspx**
  - **La méthode de calcul de "l'exploitability index" change**
    - **http://blogs.technet.com/b/msrc/archive/2011/05/05/exploitability-index-improvements-amp-advance-notification-service-for-may-2011-bulletin-release.aspx**
    - **http://blogs.technet.com/b/msrc/archive/2011/05/05/exploitability-index-improvements-amp-advance-notification-service-for-may-2011-bulletin-release-2.aspx**
  - **MS11-035 Faille dans le serveur WINS [2]**
    - **Affecte: Windows 2003 / 2008 / 2008R2**
    - **Exploit: exécution de code lors d'une requête malformée**
    - **Crédit: Luigi Auriemma / ZDI-11-167**
  - **MS11-036 Failles dans PowerPoint [1,3]**
    - **Affecte: Office (toutes versions supportées)**
      - **Sauf 2010, 2011 (Mac), Viewer, Works 9**
      - **Le correctif pour la version Mac (2004 & 2008) sera disponible plus tard**
    - **Exploit: exécution de code à l'ouverture d'un fichier malformé**
    - **Crédit: Will Dormann / CERT-CC**

Avis Microsoft

- Advisories
  - KB973811 "Extended Protection for Authentication"
    - V1.12: *opt-in* pour Microsoft Outlook
  - KB2269637 "DLL Preloading"
    - V7.0: publication de MS11-023 et MS11-025
  - KB2501584
    - V1.0: disponibilité de l'outil "Office File Validation"
  - KB2501696 Faille mhtml://
    - V2.0: correctif publié (MS11-026)
  - KB2506014
    - V1.0: mise à jour du *loader* Windows (winload.exe)
      - Il est possible de charger des drivers non signés
      - Technique utilisée par le rootkit Alureon/TDL4

Avis Microsoft

- KB2524375
  - V2.0: les plateformes suivantes sont affectées: WM6, WP7, Kin et Zune
  - V3.0: mise à jour disponible pour WP7
  - V4.0: mise à jour disponible pour WM6

- KB2526954
  - Mise à jour pour SilverLight (6 failles corrigées)

Avis Microsoft

- Révisions (mois antérieurs)
  - MS10-070
    - V4.1: correction de la clé de base de registre (.NET 3.5 SP1 / XP, 2003)
  - MS10-087
    - V2.1: la mise à jour pour Office 2004 Mac est disponible (MS11-021, MS11-022 et MS11-023)
  - MS10-088
    - V1.3: la mise à jour pour Office 2004 Mac est disponible (MS11-021, MS11-022 et MS11-023)
  - MS11-014
    - V1.1: documentation d'un problème connu
  - MS11-017
    - V1.3: mise à jour documentaire
    - V1.4: mise à jour documentaire
    - V1.5: mise à jour documentaire

Avis Microsoft

- Révisions (mois en cours)
  - MS11-018
    - V2.0: IE7 / Windows XP et 2003 n'était pas géré correctement
      - http://blogs.technet.com/b/msrc/archive/2011/05/16/ms11-018-re-released-for-ie7-on-windows-xp-and-server-2003.aspx
  - MS11-019
    - V1.1: mise à jour documentaire (description de la vulnérabilité)
  - MS11-020
    - V1.1: mise à jour documentaire
  - MS11-022
    - V1.1: mise à jour documentaire
  - MS11-024
    - V1.1: documentation d'un problème connu
    - V1.2: ajout du CVE-2010-4701

Avis Microsoft

- MS11-025
  - V1.1: ajout d'une section destinée aux développeurs
  - V2.0: problème de détection avec le correctif d'origine
  - V2.1: mise à jour documentaire
- MS11-028
  - V2.0: la présence de KB979744 entrainait un problème connu
- MS11-031
  - V1.1: cette mise à jour remplace MS09-045
- MS11-036
  - V1.1: mise à jour documentaire

Infos Microsoft

- **Sorties logicielles**
  - **Internet Explorer 10 (Platform Preview)**
  - **Microsoft Security Update Guide, 2ème édition**
    - **http://blogs.technet.com/b/msrc/archive/2011/04/04/announcing-the-microsoft-security-update-guide-second-edition.aspx**
  - **La politique de publication de failles chez Microsoft**
    - **"Coordinated Vulnerability Disclosure"**
      - **http://blogs.technet.com/b/msrc/archive/2011/04/19/coordinated-vulnerability-disclosure-from-philosophy-to-practice.aspx**
  - **Un outil de conversion**
    - **Application iPhone -> Application WP7 (!)**
      - **http://windowsteamblog.com/windows_phone/b/wpdev/archive/2011/04/29/leveraging-your-iphone-development-expertise-to-build-windows-phone-7-applications.aspx**

Infos Microsoft

- **Autre**
  - **Windows 7 certifié EAL4+**
    - **http://windowsteamblog.com/windows/b/windowssecurity/archive/2011/04/27/windows-7-is-now-common-criteria-certified.aspx**
  - **Microsoft rachète Skype**
    - **$8,5 milliards … en cash**
  - **Fuites (multiples) de Windows 8**
    - **Exemples:**
      - **http://pastebin.com/9Y9rJ8V6**
      - **http://www.windows8italia.com/**
    - **Et ça ne sont pas des fuites organisées !**
      - **http://www.presence-pc.com/actualite/Windows-licenciement-43630/**
  - **Windows 8 aura (peut-être)**
    - **Un écran d'accueil "à la Android"**
    - **Un "App Store"**

Infos Microsoft

- Secunia rejoint la "System Center Alliance"
  - http://secunia.com/blog/196/
- Sécurité de l'implémentation Office vs. Sécurité OpenOffice
  - Spoiler: Office gagne largement ☺
    - http://www.cert.org/blogs/certcc/2011/04/office_shootout_microsoft_offi.html
- Partenariat Microsoft / BlackBerry
  - Bing et Bing Maps par défaut dans Blackberry OS 7
- Les utilisateurs de Windows Phone 7 priés de ne pas installer de mises à jour "sauvages"
  - http://windowsteamblog.com/windows_phone/b/windowsphone/archive/2011/04/06/weekly-update-status.aspx
- La Cour Suprême va trancher dans l'affaire du "brevet Word"
  - http://www.linformaticien.com/actualites/id/20403/la-cour-supreme-americaine-examine-l-affaire-word.aspx
- Le patron de Microsoft Lybie emprisonné
  - http://www.linformaticien.com/actualites/id/20300/le-patron-de-microsoft-libye-emprisonne.aspx

Infos Microsoft

- Pourquoi récupérer un hash … quand on peut récupérer un mot de passe ?
  - http://blog.gentilkiwi.com/securite/pass-the-pass
- Le "binary planting" affecte aussi Internet Explorer 9
  - http://blog.acrossecurity.com/2011/05/silently-pwning-protected-mode-ie9-and.html

Infos Réseau

- **(Principales) faille(s)**
  - **Exécution de commandes dans le client ISC DHCP**
    - **Injection de commandes dans le hostname …**
      - **https://bugzilla.redhat.com/show_bug.cgi?id=689832**
      - **https://www.isc.org/software/dhcp/advisories/cve-2011-0997**
  - **Faille dans l'implémentation IPCOMP**
    - **Toutes les branches de code *BSD et dérivées**
      - **http://seclists.org/fulldisclosure/2011/Apr/0**
  - **Cisco UCM**
    - **DoS (x3), injection SQL (x2), directory traversal …**
      - **http://www.cisco.com/warp/public/707/cisco-sa-20110427-cucm.shtml**
      - **ZDI-11-143**
  - **Cisco WLC**
    - **DoS ICMP**
      - **http://www.cisco.com/warp/public/707/cisco-sa-20110427-wlc.shtml**

Infos Réseau

- Cisco IOS 15.1(1)S release notes
  - http://www.cisco.com/en/US/docs/ios/15_1s/release/notes/15_1s_caveats_15_1_1s.html
  - http://www.doecirc.energy.gov/bulletins/t-611.shtml
- Cisco Secure Desktop
  - ZDI-11-091, ZDI-11-092 (publié en "0day" suite à l'expiration du délai)
- BIND < 9.8.0-p1
  - DoS (si la fonction RPZ est utilisée - donc DNSSEC)
    - https://www.isc.org/CVE-2011-1907

Infos Réseau

- **Autres infos**
  - **IOS Software Checker**
    - **Pour s'y retrouver dans la jungle des patches …**
      - **http://tools.cisco.com/security/center/selectIOSVersion.x**
      - **http://blogs.cisco.com/security/introducing-the-cisco-ios-software-checker/**
  - **L'attaque "Split Handshake" sur TCP**
    - **"On" a redécouvert que le 3-way handshake pouvait être un 4-way handshake**
      - **http://watchguardsecuritycenter.com/2011/04/15/what-is-the-tcp-split-handshake-attack-and-does-it-affect-me/**
  - **L'attaque "SLAAC"**
    - **Interception de trafic avec le mécanisme NAT-PT pour IPv6**
      - **http://resources.infosecinstitute.com/slaac-attack/**
  - **Verisign passe à DNSSEC**
      - **https://press.verisign.com/easyir/customrel.do?easyirid=AFC0FF0DB5C560D3&version=live&prid=739224&releasejsp=custom_97**

Infos Réseau

- Coupure de fibre pendant les travaux du tramway à Vélizy
  - defense.gouv.fr (et d'autres) indisponibles pendant 16h
    - http://www.linformaticien.com/actualites/id/20645/coupure-de-fibre-optique-dans-les-yvelines.aspx
- Un vol de de câbles coupe l'Arménie d'Internet
    - http://www.20minutes.fr/article/702851/high-tech-l-internet-toute-armenie-coupe-hackeuse-75-ans
- USA vs. Chine
  - Autour du site "change.org"
    - http://www.dailytech.com/China+Tries+to+Silence+American+Advocacy+Site+With+Attacks+FBI+Fires+Back/article21561.htm
- L'American Bankers Association propose de créer (et de gérer) le ".bank"
    - http://www.bankinfosecurity.com/articles.php?art_id=3625&rf=2011-05-11-eb
- "Level 3" rachète "Global Crossing"
    - http://www.linformaticien.com/actualites/id/20330/concentration-dans-les-backbones-level-3-s-offre-global-crossing-pour-3-milliards.aspx

Infos Unix

- (Principales) faille(s)
  - Evasion de KVM
    - http://git.kernel.org/?p=virt/kvm/qemu-kvm.git;a=commit;h=52c050236eaa4f0b5e1d160cd66dc18106445c4d
  - Déni de service sur Xen 5
    - http://support.citrix.com/article/CTX129208
    - http://support.citrix.com/article/CTX129228
  - Déni de service (et plus) sur Xen < 5
    - http://lists.xensource.com/archives/html/xen-devel/2011-05/msg00483.html
  - OpenSSH < 5.8p2
    - Accès à la clé privée (si ssh-rand-helper est utilisé)
      - http://www.openssh.com/txt/portable-keysign-rand-helper.adv

Infos Unix

- Exim
  - Un '%' dans une signature DKIM provoque le crash de l'application
    - http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=624670
- Postfix + SASL
    - http://www.postfix.org/CVE-2011-1720.html
- Python + Urllib
  - Urllib accepte les redirections (HTTP/302) vers "file://"
    - http://bugs.python.org/issue11662
- Wordpress < 3.1.2
    - http://codex.wordpress.org/Version_3.1.2
- MIT Kerberos
  - Execution de code (?) lors d'un changement de mot de passe
    - http://web.mit.edu/kerberos/advisories/MITKRB5-SA-2011-004.txt
- FreeBSD
  - Accès à un montage NFS si le masque de sous-réseau n'est pas multiple de 8
    - http://security.freebsd.org/advisories/FreeBSD-SA-11:01.mountd.asc

Infos Unix

- **Autre**
  - **Sorties logicielles**
    - **OpenBSD 4.9**
      - **http://www.openbsd.org/49.html**
    - **Ubuntu 11.04**
    - **Gnome 3**
      - **http://gnome3.org/**
  - **OpenOffice redevient libre et gratuit**
    - **http://www.linformaticien.com/actualites/id/20394/oracle-cede-le-controle-d-openoffice-a-la-communaute-open-source.aspx**
  - **Brad Spender n'est pas content ☺**
    - **http://forums.grsecurity.net/viewtopic.php?f=7&t=2596**
  - **Ubuntu vise 200 millions d'utilisateurs en 2015**
    - **http://www.linformaticien.com/actualites/id/20619/ubuntu-veut-200-millions-d-utilisateurs-en-2015.aspx**

Failles

- **Principales applications**
  - **Flash Player <= 10.2.153.1, < 10.2.159.1**
    - **Exploitée en "0day"**
      - **http://www.adobe.com/support/security/advisories/apsa11-02.html**
      - **http://www.adobe.com/support/security/bulletins/apsb11-07.html**
  - **Adobe Reader <9.4.4, < 10.0.3**
    - **Via la faille "Flash" précédente**
      - **http://www.adobe.com/support/security/bulletins/apsb11-08.html**
  - **Flash Player < 10.3.181.14**
    - **Cette version permet aussi de nettoyer proprement les "super cookies"**
      - **http://www.adobe.com/support/security/bulletins/apsb11-12.html**

Failles

- FireFox < 3.6.17, < 4.0.1
  - http://www.mozilla.org/security/known-vulnerabilities/firefox36.html#firefox3.6.17
  - ZDI-11-157, ZDI-11-158, ZDI-11-159
  - FireFox 3.6.14 corrigeait: ZDI-11-103
- ThunderBird < 3.1.10
  - http://www.mozilla.org/security/known-vulnerabilities/thunderbird31.html#thunderbird3.1.10
- Chrome
  - http://www.microsoft.com/technet/security/advisory/msvr11-001.mspx
- Chrome & Opera
  - http://www.microsoft.com/technet/security/advisory/msvr11-002.mspx
- WebKit
  - Donc Chrome, Safari, Android, iPhone, et plein d'autres …
    - ZDI-11-104 (pwn2own), ZDI-11-135 (pwn2own)
    - ZDI-11-138, ZDI-11-139, ZDI-11-140

Failles

- Oracle Quaterly Patch
  - 73 failles corrigées
    - http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html
    - ZDI-11-137
- Java < 1.6.0_26
  - A priori pas de correctifs de sécurité (?)

Failles

- Apple iTunes < 10.2.2
  - http://support.apple.com/kb/DL1103
  - http://support.apple.com/kb/HT4609
  - iTunes 10.2 corrigeait:
    - ZDI-11-095 … 101
- Apple iOS < 4.3.2
  - Révoque aussi les certificats Comodo "frauduleux"
    - http://support.apple.com/kb/HT4606
- Safari < 5.0.5
  - http://support.apple.com/kb/HT4596
- Mac OS X "Snow Leopard"
  - Note: patch 2011-001 corrigeait ZDI-11-108, ZDI-11-109 (pwn2own)
  - Patch 2011-002
    - http://support.apple.com/kb/DL1376

Failles

- BES
  - http://www.blackberry.com/btsc/search.do?cmd=displayKC&docType=kc&externalId=KB26296
  - Apache/Tomcat
    - http://www.blackberry.com/btsc/search.do?cmd=displayKC&docType=kc&externalId=KB25966
- SAP NetWeaver
  - https://service.sap.com/sap/support/notes/1512134
  - https://service.sap.com/sap/support/notes/1513182
- VMWare ESXi 4.1
  - http://kb.vmware.com/kb/1035108
- VMWare vCenter 2.5, 4.0 et 4.1
  - Directory traversal …
    - http://www.securityfocus.com/bid/47735
- RealPlayer
  - http://service.real.com/realplayer/security/04122011_player/en/

Failles

- Skype (version Mac OS)
  - http://blogs.skype.com/security/2011/05/security_vulnerability_in_mac.html
- VLC < 1.1.9
  - http://www.videolan.org/security/sa1103.html
- WireShark < 1.2.16, < 1.4.5
- Produits HP …
  - ZDI-11-054 … 057 (février 2011)
  - ZDI-11-094 publié sans correctif (délai expiré)
  - ZDI-11-144 … 152
  - ZDI-11-160 … 165 et ZDI-11-167
  - Rappel: ZDI appartient à HP ☺

Failles 2.0

- Les pratiques des applications mobiles inquiètent les autorités américaines
  - http://www.lemonde.fr/technologies/article/2011/04/05/des-applications-sur-smartphones-scrutees-par-les-autorites-americaines_1503130_651865.html
- L'iPhone est-il un mouchard ?
  - L'affaire du fichier "consolidated.db" remonte très haut
    - http://petewarden.github.com/iPhoneTracker/
  - iOS 4.3.3 corrige le problème
    - … même si ça n'en est pas un d'après Steve Jobs
  - La géolocalisation dans Windows Phone 7
    - http://news.cnet.com/8301-31921_3-20057329-281.html
  - D'autres affaires ressortent
    - http://www.engadget.com/2011/04/27/tomtom-user-data-sold-to-danish-police-used-to-determine-ideal/
- DropBox
  - Une solution non sûre … par conception
    - http://dereknewton.com/2011/04/dropbox-authentication-static-host-ids/

Failles 2.0

- La fuite d'un "token" d'authentification dans une IFRAME
  - … aurait pu permettre à des développeurs Facebook d'accéder à toutes les données
    - http://www.symantec.com/connect/blogs/facebook-applications-accidentally-leaking-access-third-parties
- Facebook vs. Google
  - Encore un épisode peu glorieux …
    - http://www.thedailybeast.com/blogs-and-stories/2011-05-12/facebook-busted-in-clumsy-smear-attempt-on-google/
- Les API d'accélération graphique ne sont pas "Web safe"
  - Il vaut mieux désactiver WebGL pour le moment …
    - http://www.linformaticien.com/actualites/id/20631/il-faut-desactiver-webgl-dans-chrome-et-firefox.aspx
- Le filtrage du Web: un business juteux
    - http://www.internetactu.net/2011/04/11/le-marche-florissant-de-la-censure/
- Une espionne qui opère … sur Twitter
    - http://www.wired.com/dangerroom/2011/04/unfollowed-how-a-possible-social-network-spy-came-undone/

Sites piratés

- Les sites piratés du mois
  - Sony PlayStation Network (77 millions de comptes)
    - http://blog.us.playstation.com/2011/04/26/update-on-playstation-network-and-qriocity/
  - Sony Online Entertainment
    - https://www.soe.com/securityupdate/index_fr.vm
    - Anonymous nie être impliqué ☺
    - Sur la brèche:
      - FBI, Data Forte, Guidance Software, Robert Half International, …
    - Les bonnes pratiques "de base" n'étaient pas respectées par Sony
      - http://www.eweek.com/c/a/Security/Sony-Networks-Lacked-Firewall-Ran-Obsolete-Software-Testimony-103450/
    - Le "chat" des pirates ?
      - http://pastebin.com/m0ZxsjAb
    - Le "Cloud" est-il à blâmer ?
      - http://www.theregister.co.uk/2011/05/14/playstation_network_attack_from_amazon/

Sites piratés

- Square Enix
  - Editeur de Final Fantasy et Tomb Raider, entre autres
    - http://www.linformaticien.com/actualites/id/20665/apres-sony-c-est-square-enix-qui-est-pirate.aspx
- Wordpress.com
    - http://en.blog.wordpress.com/2011/04/13/security/
- CCAvenue.com
  - Piraté
    - http://seclists.org/fulldisclosure/2011/May/127
  - … ou pas ?
    - http://packetstormsecurity.org/news/view/19110/CCAvenue-Denies-Hacking-Attack.html
- Fox
    - http://pastebin.com/zDMHmmAr
  - Ainsi que l'émission X-Factor
    - http://thepiratebay.org/torrent/6372763/X_Factor_Leaked_Contestants_Database

Sites piratés

- Barracuda Networks
  - Injection SQL … pendant une "opération de maintenance"
    - http://hmsec.tumblr.com/
- L'agence spatiale européenne (ESA)
    - http://tinkode27.baywords.com/european-space-agency-esa-int-hacked-full-disclosure/
- Lastpass.com
  - Le problème avec les gestionnaires de mots de passe … c'est quand ils sont piratés (!)
    - http://blog.lastpass.com/2011/05/lastpass-security-notification.html
  - Surtout quand la contre-mesure détruit tous les mots de passe (!!)
    - http://forums.lastpass.com/viewtopic.php?f=12&t=24329&start=50
- TMG
  - Le prestataire HADOPI
    - http://reflets.info/le-honeypot-de-tmg/
  - Un contrôle CNIL est en cours
    - http://twitter.com/#!/CNIL/status/70430432503676928

Sites piratés

- DSLReports.com
  - http://www.dslreports.com/forum/r25793356-site-user-password-intrusion-info
- Age.fr
  - http://reflets.info/age-fr-pirate-les-donnees-personnelles-des-clients-dans-la-nature-depuis-1-an/
- Une banque coréenne rendue complètement inopérante
  - ... À cause d'un laptop infecté !
    - http://spectrum.ieee.org/riskfactor/computing/it/south-korean-banks-weeklong-system-failure-affecting-30-million-an-inside-job
- L'état du Texas
  - Un fichier rendu accessible "par erreur" depuis Internet
    - http://nakedsecurity.sophos.com/2011/04/12/state-of-texas-leaks-data-on-3-5-million-people/
- Kennebec Savings Bank
  - http://www.kjonline.com/news/hackers-breach-banks-online-system_2011-03-30.html

Sites piratés

- **Pas vraiment du piratage, mais …**
  - **La NASA mal protégée**
    - **D'après un audit gouvernemental**
      - **http://science.slashdot.org/story/11/03/29/1952244/NASA-Vulnerable-To-Crippling-Cyber-Attacks**
  - **Après son piratage, le NASDAQ fait appel à la NSA**
    - **http://news.cnet.com/8301-1009_3-20048996-83.html**
  - **Amazon EC2 en panne**
    - **21h de *downtime* et des données perdues**
    - **Suite à une erreur humaine …**
      - **http://aws.amazon.com/message/65648/**
    - **Comment se préparer à une panne ☺**
      - **http://www.codinghorror.com/blog/2011/04/working-with-the-chaos-monkey.html**
  - **… mais aussi …**
    - **Des images préinstallées … et compromises**
      - **http://dvlabs.tippingpoint.com/blog/2011/04/11/cloud-security-amazons-ec2-serves-up-certified-pre-owned-server-images**

Sites piratés

- Retour sur l'affaire RSA
  - RSA n'était pas la seule cible lors de cette vague d'attaques
    - http://www.darkreading.com/blog/229402216/a-not-so-targeted-targeted-attack.html
- Guerre civile chez Anonymous
  - Le canal IRC a été auto-piraté
    - http://www.thinq.co.uk/2011/5/9/anonymous-civil-war-anonops-sites-are-hacked/
- Jailbreak de l'iPad 2: la motivation augmente
    - http://www.lemondeinformatique.fr/actualites/lire-le-defi-de-deux-hackers-pour-jailbreaker-l-ipad-2-33624.html
- Le site Web de McAfee truffé de failles ?
  - Pas très bon quand on vend le logo "Hacker Safe"
    - http://it.slashdot.org/story/11/03/28/209230/McAfees-Website-Full-of-Security-Holes
- Débits injustifiés chez CommBank
  - Suite à une "opération de maintenance"
    - http://www.smh.com.au/technology/technology-news/backlash-over-commbanks-iron-fist-on-atm-glitch-20110415-1dhcb.html

Sites piratés

- **Verizon Data Breach Report 2011**
  - **http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf**

- **Symantec: rapport sur les menaces 2010**
  - **Les smartphones et les réseaux sociaux sont les nouvelles cibles**
    - **http://www.lemondeinformatique.fr/actualites/lire-symantec-pointe-les-smartphones-et-les-reseaux-sociaux-comme-prochaines-victimes-d-attaques-33352.html**

Malwares et spam

- Mac OS X largement victime de MACDefender
  - Un "Rogue AV"
    - http://www.macrumors.com/2011/05/02/new-macdefender-malware-threat-for-mac-os-x/
- Le code source de Zeus en téléchargement sur Internet
    - http://www.csis.dk/en/csis/blog/3229/
- Un kit "clés en main" pour la création de malwares Mac OS X
    - http://www.csis.dk/en/csis/blog/3195/
- Le botnet "Coreflood" démantelé
  - Et les serveurs de contrôle remplacés par des serveurs de désinfection !
    - http://www.securityvibes.fr/cyber-pouvoirs/botnet-coreflood-takedow/

Malwares et spam

- McAfee détecte SAP comme un virus
  - DAT 6329
    - https://kc.mcafee.com/corporate/index?page=content&id=KB71739
- L'Iran ciblé également par le ver "Stars" ?
    - http://www.linformaticien.com/actualites/id/20488/l-iran-aurait-ete-vise-par-un-second-ver-stars.aspx
- Le fils d'Eugène Kaspersky enlevé
  - … et libéré contre rançon
    - http://www.computerworld.com/s/article/9216034/Security_firm_founder_Kaspersky_s_son_reportedly_kidnapped_in_Russia

Actualité (francophone)

- Un référentiel applicable aux prestataires d'audit sécurité
  - http://www.ssi.gouv.fr/site_article328.html
- Le CERT-SG publie ses bonnes pratiques
  - http://cert.societegenerale.com/en/publications.html
- Un pirate se vante à la télé du piratage de THALES
  - http://www.lemonde.fr/technologies/article/2011/04/11/un-pirate-presume-mis-en-examen-apres-une-emission-de-complement-d-enquete_1506095_651865.html
- Espionnage industriel chez SAFRAN
  - http://www.lemonde.fr/economie/article/2011/04/13/soupcons-d-espionnage-chez-safran-sans-vol-de-donnees-a-caractere-industriel_1506757_3234.html

Actualité (francophone)

- MyID.is et La Poste lancent "Identic"
  - https://identic.laposte.fr/
- Les entreprises françaises très exposées au piratage informatique
  - D'après McAfee ..
    - http://www.lefigaro.fr/actualite-france/2011/04/10/01016-20110410ARTFIG00210-les-firmes-francaises-tres-vulnerables.php
- Une proposition de loi pour réprimer plus durement les délits informatiques
  - Est-ce vraiment utile/efficace ?
    - http://sid.rstack.org/blog/index.php/477-de-l-optimalite-de-la-legislation
- Un coffre-fort électronique pour les PME
  - Et plein d'autres mesures législatives à venir …
    - http://www.linformaticien.com/actualites/id/20531/un-coffre-fort-numerique-pour-simplifier-la-vie-des-pme.aspx
- Une initiative de la CCI Provence-Alpes-Côte d'Azur
  - http://www.lenumeriquepourmonentreprise.com/

Actualité (francophone)

- Les cibles de la CNIL en 2011
  - Vidéoprotection et données de santé
    - http://www.cnil.fr/la-cnil/actu-cnil/article/article/programme-des-controles-2011-une-ambition-reaffirmee-des-competences-elargies/?tx_ttnews[backPid]=2&cHash=91ae300acd
- TIC: forces et faiblesses de la France
    - http://www.industrie.gouv.fr/tc2015/
- La "fracture numérique" revient
    - http://www.strategie.gouv.fr/IMG/pdf/CAS_Fosse_numerique_18avril2011.pdf
- Création du "Conseil National du Numérique"
    - http://www.gouvernement.fr/gouvernement/creation-du-conseil-national-du-numerique

Actualité (anglo-saxonne)

- Le FBI "saisit" plusieurs sites de poker en ligne
  - Full Tilt Poker, Absolute Poker, Poker Stars
    - http://www.20minutes.fr/article/710849/poker-le-black-friday-poker
- Encore une erreur de masquage dans un fichier PDF
  - Et non des moindres
    - http://cryptome.org/0003/mod-nuke-leak.htm
- Les américains poussent toujours aussi fort pour une identification en ligne
    - http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf
  - … mais est-ce vraiment utile ?
    - http://theinvisiblethings.blogspot.com/2011/04/why-us-password-revolution-wont-work.html

Actualité (européenne)

- Rapport de l'exercice "Cyber Europe 2010"
  - http://www.enisa.europa.eu/act/res/cyber-europe-2010/cyber-europe-2010-report/
- Rapport d'évaluation concernant la directive sur la conservation des données
  - http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_fr.pdf
- Un "firewall" européen (?)
  - Pour filtrer les sites illégaux, pas pour nous protéger des agressions extérieures
  - Sous la pression du groupe Law Enforcement Working Party
    - http://www.linformaticien.com/actualites/id/20643/un-firewall-europeen-est-en-projet.aspx

Actualité (Google)

- Chrome 11 est sorti
  - Commande vocale, accélération 3D, nouveau logo …
- VUPEN vs. Chrome
  - Evasion de la sandbox
    - http://www.vupen.com/demos/VUPEN_Pwning_Chrome.php
- SafeBrowsing inclut désormais les téléchargements
    - http://blog.chromium.org/2011/04/protecting-users-from-malicious.html
- Google: le seul endroit où ingénieur >> manager
    - http://digitaldaily.allthingsd.com/20110405/exlusive-larry-page-mulls-google-reorg/
- Procès Google vs. Bedrock
  - L'utilisation de Linux n'est pas libre …
    - http://www.linformaticien.com/actualites/id/20470/google-ne-peut-pas-utiliser-linux-librement.aspx
- Google aurait accepté de faire de la publicité illégale
  - Pour des pharmacies en ligne
    - http://www.linformaticien.com/actualites/id/20654/google-sous-le-coup-d-une-investigation-criminelle.aspx

Actualité (Google)

- Les nouveautés annoncées lors de Google I/O
  - Google Music
  - SmartBooks sous Chrome OS
    - C'est pour le 15 juin a priori
    - SFR aura l'exclusivité en France
    - Des offres à $20/mois pour les étudiants américains

- Autres nouveautés
  - Google change son moteur d'indexation
    - Nom de code: Google Panda
  - Une nouvelle version de YouTube
    - En prévision de GoogleTV ?
  - Google Docs en application native sous Android
  - #EPIC
    - http://chrome.angrybirds.com/

Actualité (mobile)

- Android pour équiper le *smartphone* des fantassins américains
  - http://www.securityvibes.fr/cyber-pouvoirs/armee-americaine-android/
- Les E.A.U. finissent par interdire complètement le BlackBerry
  - http://www.securityvibes.fr/cyber-pouvoirs/blackberry-inde-emirats/
- Nokia supprime 4,000 emplois et transfère Symbian à Accenture

Actualité (crypto)

- L'algorithme NTRU approuvé comme standard X9.98
  - http://pr-usa.net/index.php?option=com_content&task=view&id=688677&Itemid=32
- Toshiba: un disque dur chiffré capable de s'autoprotéger
  - http://www.linformaticien.com/actualites/id/20356/toshiba-un-disque-dur-capable-de-s-auto-effacer.aspx

Actualité

- **Sorties logicielles**
  - **BackTrack 5**
    - **Dont une version ARM**
      - **http://www.backtrack-linux.org/bt/roadmap/**
  - **Metasploit 3.7**
    - **http://blog.metasploit.com/2011/05/metasploit-framework-370-released.html**
  - **Nessus 4.4.1**
  - **Version "communautaire" du scanner Retina**
    - **http://www.eeye.com/products/retina/community**
  - **Qubes Beta1**
    - **http://theinvisiblethings.blogspot.com/2011/04/qubes-beta-1-has-been-released.html**
    - **Et une première faille détectée …**
      - **https://groups.google.com/group/qubes-devel/browse_thread/thread/911412422adc60a9#**

Actualité

- **Sorties logicielles (suite)**
  - **Secunia Vulnerability Intelligence Manager 3.1**
    - **http://secunia.com/blog/206/**
  - **Mono pour Android**
    - **Note: les développeurs du projet Mono ne sont plus "stratégiques" depuis le rachat de Novell par Attachmate**
      - **http://mono-android.net/**
  - **Pentest Magazine**
    - **Par la maison d'édition de Hakin9**
      - **http://pentestmag.com/**

Actualité

- MafiaaFire … légal ou pas ?
  - Oui d'après Mozilla
    - https://addons.mozilla.org/en-US/firefox/addon/mafiaafire-redirector/
    - http://news.cnet.com/8301-31921_3-20060636-281.html
- La première version du système d'exploitation national russe sera disponible fin 2011
  - Massivement basé sur Linux
    - http://www.developpez.com/actu/30759/Le-gouvernement-russe-developpe-son-propre-systeme-d-exploitation-la-premiere-version-de-l-OS-sera-disponible-d-ici-fin-2011/
- Comment faire du mail de manière anonyme
  - En utilisant des porteurs de clés USB
    - http://www.linformaticien.com/actualites/id/20652/les-communications-mail-de-ben-laden.aspx
    - http://www.lemonde.fr/technologies/article/2011/05/13/l-astuce-de-ben-laden-pour-envoyer-ses-e-mails-discretement_1521338_651865.html
- Le facteur humain
    - http://www.securingthehuman.org/

Actualité

- Sophos rachète Astaro
  - http://blogs.csoonline.com/1498/sophos_acquires_astaro
- Un SCADA hacké … et publié sur Full Disclosure
  - http://archives.neohapsis.com/archives/fulldisclosure/2011-04/0254.html
- Une pénurie d'ordinateurs portables à venir
  - A partir de septembre
  - A cause de l'arrêt de la production au Japon
    - http://www.linformaticien.com/actualites/id/20405/plus-d-ordinateurs-portables-a-partir-de-septembre.aspx
- Le réseau social chinois "RenRen" valorisé $743 million lors de son entrée en bourse
  - Pas grand'chose comparé aux $100 milliards de Facebook ☺

Fun

- Les hackers sont les messagers de Dieu
  - D'après le Vatican
    - http://www.msnbc.msn.com/id/42459193/ns/technology_and_science-security
- Comme dans les films
    - http://hackertyper.net/
- Un émulateur PC … en JavaScript
    - http://bellard.org/jslinux/
- Raspberry Pi
  - L'ordinateur à 15€ (basé sur processeur ARM)
    - http://www.linformaticien.com/actualites/id/20582/un-ordinateur-a-15-euros-de-la-taille-d-une-cle-usb.aspx
- Computer Associates ne perd pas le nord
    - http://www.ca.com/fr/news/Press-Releases/emea/2011/CA-Technologies-propose-aux-utilisateurs-de-tokens-RSA-fr-fr.aspx

Fun

- Un keylogger hardware … et wifi
  - http://www.keydemon.com/hardware_keylogger_wifi/
- Les autorités de certification
  - Mieux vaut en rire qu'en pleurer
    - https://bugzilla.mozilla.org/show_bug.cgi?id=647959
- La série TV "Breaking In" est finalement annulée
  - http://content.usatoday.com/communities/entertainment/post/2011/05/fox-cancels-five-series-/1
- Recrutement agressif
  - http://www.recruit.co.nz/node/4262

Fun

- La contrefaçon va très loin
  - http://www.blogeee.net/2011/04/des-contrefacteurs-inventent-le-stockage-usb-illimite/

Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 14 juin 2011
- N'hésitez pas à proposer des sujets et des salles