OSSIR
Groupe Sécurité Windows

Réunion du 9 juin 2008

Revue des dernières vulnérabilités Microsoft

Cette veille est réalisée par les coanimateurs du groupe Windows

EdelWeb

Olivier REVENU
olivier.revenu (à) edelweb.fr

Mickaël DEWAELE
mickael.dewaele (à) edelweb.fr

Jérémy LEBOURDAIS
jeremy.lebourdais (à) edelweb.fr

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

Dernières vulnérabilités
Avis Microsoft

- **Correctifs de Avril 2008**

  - **MS08-018 Faille dans MS Project**
    - **Affecte : MS Project, toutes versions antérieures à 2003 SP3**
    - **Exploit : corruption mémoire à l'ouverture d'un fichier malformé**
    - **Crédit : National Cyber Security Center (Corée)**

  - **MS08-019 Failles dans MS Visio (x2)**
    - **Affecte : toutes versions supportées**
      - **sauf les Viewers**
    - **Exploit : corruption mémoire à l'ouverture d'un fichier malformé**
    - **Crédit : anonyme (x2)**

Dernières vulnérabilités
Avis Microsoft

- **MS08-020 Vulnérabilité du client DNS**
  - **Affecte : Windows toutes versions supportées**
    - **sauf Vista SP1 et 2008**
  - **Exploit : mauvaise génération d'aléa des requêtes, permettant d'envoyer des réponses spoofées**
  - **Crédits :**
    - **Amit Klein / Trusteer ; Alla Berzroutchko / Scanit ; Roy Arends / Nominet UK**
  - **Détails :**
    - **http://blogs.technet.com/swi/archive/2008/04/09/ms08-020-how-predictable-is-the-dns-transaction-id.aspx**

- **MS08-021 Failles dans les formats WMF / EMF (x2)**
  - **Affecte : Windows toutes versions supportées**
  - **Exploit :**
    - **heap overflow à la lecture d'un fichier WMF / EMF malformé**
    - **stack overflow à la lecture d'un fichier WMF / EMF malformé**
    - **code d'exploitation sur Milw0rm**
  - **Crédits :**
    - **Jun Mao / iDefense ; Sebastian Apelt /ZDI ; Thomas Garnier / SkyRecon ; Yamata Li / Palo Alto Networks**

Dernières vulnérabilités
Avis Microsoft

- MS08-022 Faille VBScript / JScript
  - Affecte : VBScript / JScript 5.6
    - Windows toutes versions supportées sauf Vista et 2008
  - Exploit : corruption mémoire via un script malformé
  - Crédit : Peter Ferrie / Symantec

- MS08-023 Failles ActiveX (x3)
  - Affecte :
    - Windows toutes versions supportées (composant hxvz.dll)
    - Yahoo! Music Jukebox (x2)
  - Exploit : corruption mémoire via une page Web malveillante
  - Crédits : anonymous / iDefense
  - Détails :
    - http://blogs.technet.com/swi/archive/2008/04/09/same-bug-four-different-security-bulletin-ratings.aspx

Dernières vulnérabilités
Avis Microsoft

- MS08-024 Patch cumulatif pour IE
  - Affecte : IE toutes versions supportées
  - Exploit : corruption mémoire via une page Web malveillante
  - Crédit : Carsten Eiram / Secunia
  - Mais surtout ... retour de l'activation automatique des ActiveX
    - http://blogs.msdn.com/ie/archive/2008/04/08/ie-automatic-component-activation-now-available.aspx
- MS08-025 Failles locales dans le moteur graphique (x3 ?)
  - Affecte : Windows toutes versions supportées
  - Exploit : élévation de privilèges locale
    - Code d'exploitation sur ReverseMode.com
  - Crédit : Thomas Garnier
  - Détails :
    - http://blogs.technet.com/swi/archive/2008/04/09/ms08-025-win32k-vulnerabilities.aspx

Dernières vulnérabilités
Avis Microsoft

- **Correctifs de Mai 2008**
  - **MS08-026 Vulnérabilités (x2) dans Word**
    - **Affecte : Word toutes versions supportées (y compris Mac et 2007 SP1)**
    - **Exploit :**
      - **Fichier ".rtf" malformé**
      - **"Cascading Style Sheet" malformée**
    - **Crédit :**
      - **wushi / team509 + ZDI**
      - **Jun Mao / iDefense**
    - **Détails : http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=700**
  - **MS08-027 Vulnérabilité dans Publisher**
    - **Affecte : Publisher toutes versions supportées (y compris 2007 SP1)**
    - **Exploit : exécution de code à l'ouverture d'un fichier ".pub" malformé**
    - **Crédit : Cocoruder / Fortinet**
    - **Détails :**

Dernières vulnérabilités
Avis Microsoft

- MS08-028 Vulnérabilité dans le moteur Jet
  - Affecte : msjet40.dll < 4.0.9505.0
    - Windows 2000 SP4
    - Windows XP SP2 (x86), Windows XP "Gold" (x64)
    - Windows 2003 SP1 (x86), Windows 2003 "Gold" (x64), Windows 2003 SP1 (IA64)
  - Exploit : exécution de code à l'ouverture d'un fichier ".MDB" malformé
  - Crédit :
    - CERT/CC
    - ISC/SANS
    - Aaron Portnoy / TippingPoint
  - Détails : exploité dans la nature ...

Dernières vulnérabilités
Avis Microsoft

- MS08-029 Vulnérabilités (x2) dans le moteur anti-malware
  - Affecte : OneCare, Antigen, Defender, ForeFront, Standalone System Sweeper
  - Exploit :
    - Déni de service
    - Consommation d'espace disque
  - Crédit : SoWhat / Nevis

Dernières vulnérabilités
Avis Microsoft

- Prévisions pour Juin 2008
  - Bulletins critiques : 3
    - BlueTooth, IE, DirectX (toutes versions supportées)
  - Bulletins importants : 3
    - WINS (élévation de privilèges)
    - Active Directory, PGM (déni de service)
  - Bulletin modéré : 1
    - Kill Bits variés

- Advisories
  - Q951306 : élévation de privilèges locale
    - http://www.argeniss.com/research/TokenKidnapping.pdf
  - Q932596 : PatchGuard v4
  - Q953818 : mauvaise interaction Safari + Windows
    - http://www.oreillynet.com/onlamp/blog/2008/05/safari_carpet_bomb.html

Dernières vulnérabilités
Avis Microsoft

- Révisions
  - MS06-069
    - Version 2.0 : XP SP3 est affecté (réinstallation d'une version de Flash vulnérable)
  - MS07-015
    - Version 1.2 : précision sur Visio (ne fait pas partie de la suite Office)
  - MS07-025
    - Version 2.1 : le pack de compatibilité Office 2007 SP1 n'est pas affecté
  - MS07-040
    - Version 3.0 : .NET 1.0, 1.1 et 2.0 / Windows XP SP3 affectés
    - Version 3.1 : correction sur Windows XP x64 SP3
    - Version 3.2 : pas de .NET 1.0 dans Windows 2008 x64
  - MS08-009
    - Version 1.1 : précision sur les défenses intégrées à Office 2003 SP2
  - MS08-010
    - Version 1.3 : correction sur la désinstallation
  - MS08-011
    - Version 1.1 : précision sur les défenses intégrées à Office 2003 SP2

Dernières vulnérabilités
Avis Microsoft

- MS08-013
  - Version 1.3 : précision sur les défenses intégrées à Office 2003 SP2
- MS08-014
  - Version 3.1 : précision sur les défenses intégrées à Office 2003 SP2
  - Version 3.2 : mise à jour de la FAQ
- MS08-015
  - Version 1.3 : problèmes connus
  - Version 1.4 : précision sur les défenses intégrées à Office 2003 SP2
  - Version 1.5 : mise à jour de la FAQ
- MS08-016
  - Version 2.0 (re-release) : Word Viewer 2003 est également affecté
  - Version 2.1 : précision sur les défenses intégrées à Office 2003 SP2
- MS08-017
  - Version 1.3 : problèmes connus (933103)
- MS08-018
  - Version 1.1 : Projet 2003 SP3 n'est pas affecté
  - Version 1.2 : précision sur les défenses intégrées à Office 2003 SP2

Dernières vulnérabilités
Avis Microsoft

- MS08-019
  - Version 1.1 : problèmes connus
  - Version 1.2 : problème de détection avec Visio 2007
  - Version 1.3 : précision sur les défenses intégrées à Office 2003 SP2
  - Version 1.4 : problème de détection avec Visio 2007
  - Version 1.5 : mise à jour de la FAQ
- MS08-020
  - Version 1.1 : Vista 64 bits est affecté
  - Version 1.2 : précision sur les risques, retrait d'une référence à une version non supportée
- MS08-021
  - Version 1.1 : problèmes connus
  - Version 1.2 : retrait d'une référence à une version non supportée
- MS08-022
  - Version 1.1 : fusion des risques JScript et VBScript
- MS08-023
  - Version 1.1 : correction sur la désinstallation
  - Version 1.2 : correction sur Windows 2003 x64

Dernières vulnérabilités
Avis Microsoft

- MS08-024
  - Version 1.1 : correction sur la désinstallation
  - Version 2.0 : IE7 / Windows XP SP3 est affecté
  - Version 2.1 : correction sur Windows XP x64 SP3
- MS08-025
  - Version 1.1 : problèmes connus
  - Version 1.2 : précision sur les risques, retrait d'une référence à une version non supportée
- MS08-026
  - Version 1.1 : précisions sur Outlook 2007, Office 2004 et Office 2008 pour Mac
- MS08-027
  - Version 1.1 : problèmes connus (951208)
- MS08-028
  - Version 1.1 : ce bulletin corrige également CVE-2005-0944
  - Version 1.2 : problèmes connus (950749)

Dernières vulnérabilités
Infos Microsoft - sorties

- **Sorties logicielles**
  - **Windows Vista SP1**
    - **sur WindowsUpdate**
  - **Windows XP SP3**
    - **sur WindowsUpdate**
    - **La première sortie a été immédiatement bloquée suite à un problème de compatibilité avec Microsoft Dynamics**
      - **http://securite.reseaux-telecoms.net/actualites/lire-dialectique-toc-18081.html**
    - **Bon à savoir :**
      - **IE 7 ne peut plus être désinstallé**
      - **Processeur AMD + intelppm.sys = BSoD**
        - **http://msinfluentials.com/blogs/jesper/archive/2008/05/08/does-your-amd-based-computer-boot-after-installing-xp-sp3.aspx**

Dernières vulnérabilités
Infos Microsoft - sorties

- Visual Studio 2008 "Feature Pack"
  - Quelques problèmes également ...
    - http://blogs.msdn.com/vcblog/archive/2008/04/12/visual-c-2008-feature-pack-setup-deployment-issues.aspx
- Microsoft Search 4.0
- Visual Studio 2008 SP1 Beta
- .NET 3.5 SP1 Beta
- Quelques bonus pour "Vista Edition Intégrale"
  - http://www.guwiv.com/portal/blogs/news/archive/2008/04/23/bonus-vista-int-233-grale-nouveaux-sons-et-retour-des-packs-linguistiques.aspx
- http://live.sysinternals.com/
  - Les outils SysInternals en "live"

Dernières vulnérabilités
Infos Microsoft

- Office Open XML normalisé ISO 29500
  - http://en.wikipedia.org/wiki/Office_Open_XML
  - http://www.openxmlpourtous.com/
- Microsoft "Albany"
  - Office + OneCare en location mensuelle
- L'analyse de MS08-020 par le SWI blog réfutée
  - http://www.securityfocus.com/archive/1/491392
  - Déjà le cas sur la faille MS08-001 ...
- EV SSL – une vaste blague ?
  - http://isc.sans.org/diary.html?storyid=4309
- SQLInjectionFinder.exe
  - Face à la masse des attaques en injection SQL, un outil pour vérifier ses logs IIS
    - http://www.codeplex.com/Release/ProjectReleases.aspx?ProjectName=WSUS&ReleaseId=13436

Dernières vulnérabilités
Infos Microsoft

- Gartner : Windows is 'collapsing'
  - http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9076698
- COFEE : Computer Online Forensic Evidence Extractor
  - Clé USB contenant tous les outils d'espionnage utiles
  - Conçue par Microsoft et livrée aux services de police (y compris étrangers)
    - http://www.portal.itproportal.com/articles/2008/04/30/microsofts-device-provides-backdoor-access-vista-and-others/
    - http://seattletimes.nwsource.com/html/microsoft/2004379751_msftlaw29.html
- IE 8 supporte l'installation d'ActiveX "par utilisateur"
  - Une fausse bonne idée ?
    - http://blogs.msdn.com/ie/archive/2008/05/07/ie8-security-part-ii-activex-improvements.aspx

Dernières vulnérabilités
Infos Microsoft

- SDL Guidance
  - http://www.microsoft.com/downloads/details.aspx?FamilyID=2412C443-27F6-4AAC-9883-F55BA5B01814
- IE 8 active DEP par défaut
  - http://blogs.msdn.com/ie/archive/2008/04/08/ie8-security-part-I_3A00_-dep-nx-memory-protection.aspx
  - Les plugins compilés avec ATL < 7.1 (Visual Studio 2003) ne seront pas compatibles
- Microsoft pour la dépérimétrisation
  - http://www.microsoft.com/mscorp/twc/endtoendtrust/default.mspx
- Un site de référence
  - http://support.microsoft.com/dllhelp/

Dernières vulnérabilités
Infos Microsoft

- Microsoft encourage la recherche de failles sur ses sites Web
  - http://www.theregister.co.uk/2008/04/21/microsoft_oks_online_flaw_finding/
  - Dans le cadre de la future norme ISO 29147 sur le "*Responsible Disclosure*" ?
    - http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45170
- Passé, présent et futur du SDL
  - http://blogs.msdn.com/sdl/archive/2008/04/24/sdl-threat-modeling-toorcon.aspx
- Un particulier remboursé de sa licence Windows XP préinstallée
  - http://news.slashdot.org/article.pl?sid=08/05/19/0154224

Dernières vulnérabilités
Infos Microsoft - Vista

- 90% des professionnels ne veulent pas de Vista
  - Raison principalement invoquée : l' (in)stabilité
  - http://it.slashdot.org/article.pl?sid=07/11/19/1341253
- Vista meilleur que XP SP2 face aux rootkits ?
  - http://www.pcinpact.com/actu/news/43817-windows-vista-rootkits-uac-antivirus.htm
- Plus de son dans Vista SP1
  - Problème avec le driver SigmaTel
    - http://www.crn.com/software/207500472
- Plus de périphériques USB non plus
  - http://www.theregister.co.uk/2008/04/16/vista_defender_sp1/
  - Cf. KB938371
- Windows "Seven" aura le même noyau que Vista
  - http://www.presence-pc.com/actualite/Windows-7-kernel-29551/
- Blague ou erreur de communication ?
  - http://www.techcrunch.com/2008/04/16/microsoft-does-some-amazing-things-this-isnt-one-of-them/

Dernières vulnérabilités
Autres avis – failles

- Produits tiers
  - 33 failles dans Lotus Notes (!)
  - 7 failles dans Flash < 9.0.124
    - http://www.adobe.com/support/security/bulletins/apsb08-11.html
    - Un code d'exploitation venu d'une autre planète ?
      - http://www.iss.net/threats/289.html
      - http://www.matasano.com/log/1032/this-new-vulnerability-dowds-inhuman-flash-exploit/
    - Largement exploité dans la nature
      - http://ddanchev.blogspot.com/2008/05/malware-attack-exploiting-flash-zero.html
  - FireFox 2.0.0.14
    - Corrige une faille de sécurité dans JavaScript
    - http://www.mozilla.org/security/announce/2008/mfsa2008-20.html

Dernières vulnérabilités
Autres avis – failles

- Safari 3.1.1
  - Corrige la faille exploitée à Pwn2Own 2008
- Acrobat Reader < 8.1.2 et 7.1.0
  - Une autre faille avait été corrigée silencieusement
  - http://www.adobe.com/support/security/bulletins/apsb08-13.html
- Java 6 Update 6
  - Pas de faille de sécurité documentée
- Mac OS X 10.5.3
  - http://support.apple.com/kb/HT1897

Dernières vulnérabilités
Autres avis – failles

- VMWare (versions variées)
  - Service "vmware-authd" (set-uid root sous Linux)
    - http://www.vmware.com/security/advisories/VMSA-2008-0009.html
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=713
  - Faille intra-guest dans le driver "hgfs.sys"
    - http://www.vmware.com/security/advisories/VMSA-2008-0009.html
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=712
  - Evasion de VM via VMCI (expérimental, non activé par défaut)
    - http://www.vmware.com/security/advisories/VMSA-2008-0008.html

Dernières vulnérabilités
Autres avis – failles

- Sans parler de ...
  - Oracle
    - Sortie du patch trimestriel
    - Mot de passe "en dur" pour le compte "OUTLN"
      - http://www.securityfocus.com/archive/1/490950
  - Cisco
    - Sortie du patch semestriel
      - Backdoor dans CiscoWorks IPM
        - http://www.heise-online.co.uk/security/Insecure-by-design-Cisco-product-shipped-with-backdoor--/news/110320
      - NAC : capture du secret serveur sur le réseau et dans les logs
        - http://www.securiteam.com/securitynews/5RP0J1PO0M.html
    - Plus quelques patches "hors bande"
      - DoS dans SSH, etc.

Dernières vulnérabilités
Autres avis – failles

- Une faille dans le contrôle ActiveX "Microsoft HeartbeatCtl" patchée silencieusement
  - Corrigée par MS07-069
  - CLSID: E5D419D6-A846-4514-9FAD-97E826C84822
  - Référence :
    - http://www.kb.cert.org/vuls/id/570089

- Une faille dans un contrôle ActiveX lié à Microsoft Works exploitée dans la nature
  - http://www.avertlabs.com/research/blog/index.php/2008/04/17/potential-microsoft-works-activex-0-day-surfaces/
  - CLSID: 00E1DB59-6EFD-4CE7-8C0A-2DA3BCAAD9C6

- Le code d'exploitation pour la faille Centrino de l'année dernière est disponible
  - http://milw0rm.com/exploits/5461

Dernières vulnérabilités
Autres avis – failles

- Ajout "presque" silencieux d'un certificat client dans FireFox
  - http://0x90.eu/ff_tls_poc.html
- Core Security cherche des failles "*high profile*"
  - Librairie CDF
    - Créée par la NASA pour l'échange de données satellitaires
    - http://blogs.zdnet.com/security/?p=1074
  - WonderWare SuiteLink
    - Librairie utilisée par 1/3 des systèmes SCADA
  - NASA BigView
- Du patch Microsoft à l'exploit en ... 3 minutes
  - Automatic Patch-Based Exploit Generation
    - http://www.cs.cmu.edu/~dbrumley/pubs/apeg.html
  - Attention
    - Ca ne marche pas dans tous les cas
    - Par "exploit" comprendre "déni de service"

Dernières vulnérabilités
Autres avis – malwares et spam

- Le bot "Kraken" fait parler de lui
  - http://www.darkreading.com/document.asp?doc_id=150292
  - Plus gros que Storm ?
- Le site de l'AMTSO est en ligne
  - Anti Malware Testing Standards Organization
  - http://www.amtso.org/
- Quels sont les points chauds sur Internet ?
  - La réponse sur le site "Malware Threat Center"
  - Données issue du Honeynet Cyber-TA
  - http://mtc.sri.com/
- La contre-attaque numérique encore évoquée lors de la conférence RSA 2008
  - Sujet aussi vieux que les honeypots ☺
  - http://www.informationweek.com/blog/main/archives/2008/04/is_it_time_for_1.html

Dernières vulnérabilités
Autres avis – malwares et spam

- Les tests comparatifs sur les logiciels antivirus bientôt interdits par les CLUF ?
  - http://www.01net.com/editorial/376029/les-tests-d-antivirus-de-plus-en-plus-remis-en-question/
- Le 3 mai 2008, le spam a 30 ans
  - http://www.avertlabs.com/research/blog/index.php/2008/05/05/30th-anniversary-of-spam/
- Un virus dans le pack de langue vietnamien pour Firefox
  - Le développeur était infecté par un virus scannant tous les ".html"
    - https://bugzilla.mozilla.org/show_bug.cgi?id=432406
    - http://blog.mozilla.com/security/2008/05/07/compromised-file-in-vietnamese-language-pack-for-firefox-2/

Dernières vulnérabilités
Autres avis – malwares et spam

- L'ICANN va prendre des mesures contre les *registrars* les plus complaisants
  - http://www.icann.org/announcements/announcement-23may08.htm
- 4300 relais de spam fermés en Chine
  - http://www.lesnouvelles.net/articles/justice/chine-ferme-relais-spam
- Spam sur MySpace : 230 millions de dollars d'amende
  - http://www.lefigaro.fr/international/2008/05/15/01003-20080515ARTFIG00409-amende-record-pour-un-delit-sur-internet.php
- Art et Malware
  - http://cert.lexsi.com/weblog/index.php/2008/04/19/230-ceci-n-est-pas-un-malware

Dernières vulnérabilités
Autres avis – attaques 2.0

- Le site Boursorama piraté
  - http://www.zataz.com/news/17012/Boursorama----0wn3d-by--owned-EmBrAtOuR.html
  - Heureusement un simple défacement ...
- Des cartes réseau re-flashables par le réseau ...
  - http://www.links.org/?p=330
- Arrestation conjointe d'un gang de *carding* : USA / Roumanie
  - http://newhaven.fbi.gov/dojpressrel/2008/nh051908.htm
- "*All your SmartCards are belong to us*"
  - http://blog.wired.com/27bstroke6/2008/05/hacker-at-cente.html
- Une vingtaine de "pirates" français arrêtés
  - Agés de 14 à 25 ans
  - http://security.forum-actif.net/index.htm

Dernières vulnérabilités
Autres avis – attaques 2.0

- Un WebBug pour Office 2007 : la gestion des CRLs
  - https://www.klink.name/security/aklink-sa-2008-004-office2007-signatures.txt
- Un virus sur une clé USB
  - http://isc.sans.org/diary.html?storyid=4247
  - Pas courant lorsqu'il s'agit d'une mise à jour pour HP ProLiant ou CheckPoint ...
- Un outil Chinois pour de l'injection SQL automatique
  - http://isc.sans.org/diary.html?storyid=4294
  - Largement utilisé dans la nature ...
    - http://securite.reseaux-telecoms.net/actualites/lire-dialectique-toc-18081.html
- Une base SQL dans les navigateurs
  - Prévu par la norme HTML 5
  - Implémenté dans WebKit
    - http://webkit.org/blog/126/webkit-does-html5-client-side-database-storage/
  - Pour un monde plus sûr ... ?

Dernières vulnérabilités
Autres avis – attaques 2.0

- Shopping 2.0 : le *tracking* par téléphone portable
  - http://technology.timesonline.co.uk/tol/news/tech_and_web/article3945496.ec
- Le site de Phoenix Mars Lander défacé
  - Encore un coup des Chinois ? ☺
    - http://news.cnet.com/8301-10784_3-9957275-7.html?tag=ne.fd.mnbc
- Le site de Metasploit défacé
  - Une attaque par ARP Poisoning sur le site d'hébergement !
    - http://cert.lexsi.com/weblog/index.php/2008/06/03/239-metasploited
- Le Montenegro "online"
  - L'extension ".me" va se vendre chère ("love.me", "call.me", ...)
    - http://cert.lexsi.com/weblog/index.php/2008/06/05/238-you-will-have-to-payme

Dernières vulnérabilités
Autres avis – attaques 2.0

- "Internet Crime Report", édition 2007
  - http://www.ic3.gov/media/annualreports.aspx

- Symantec "Global Internet Security Threat Report"
  - Volume 13
    - http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf
  - Des données intéressantes sur les prix
    - cf. slide suivant
  - Une analyse en français
    - http://lejournaldunjournaliste.blogspot.com/2008/04/cybercriminalit-le-rapport-de-symantec.html
  - Symantec détecte plus de 1 million de virus
    - http://news.bbc.co.uk/2/hi/technology/7340315.stm
    - La notion de "souche" a-t-elle encore un sens ?
  - Symantec financé par l'Europe (projet WOMBAT)
    - http://www.globalsecuritymag.fr/La-Commission-Europeenne-attribue,20080416,2694

Dernières vulnérabilités
Autres avis – attaques 2.0

Goods and services	Percentage	Range of prices
Bank accounts	22%	$10-$1000
Credit cards	13%	$0.40-$20
Full identities	9%	$1-$15
eBay accounts	7%	$1-$8
Scams	7%	$2.5/week - $50/week for hosting. $25 for design
Mailers	6%	$1-$10
Email addresses	5%	$0.83/MB-$10/MB
Email passwords	5%	$4-$30
Drop (request or offer)	5%	10%-50% of total drop amount
Proxies	5%	$1.50-$30

Dernières vulnérabilités
Autres avis – actualités

- Les services Allemands reconnaissent avoir envoyé des chevaux de Troie dans les ministères Afghans
  - http://www.spiegel.de/international/germany/0,1518,550212,00.html
  - Amusant quand on a lu :
    - http://www.timesonline.co.uk/tol/news/world/europe/article2332130.ece

- L'armée américaine a-t-elle besoin d'un botnet ?
  - http://www.securityfocus.com/brief/737

- Le retour des routeurs Cisco contrefaits ... et backdoorés
  - Un peu moins de FUD et un peu plus d'informations
  - http://www.abovetopsecret.com/forum/thread350381/pg1

- Utiliser les capacités offensives de la NSA pour améliorer la sécurité des systèmes américains ?
  - http://www.washingtonpost.com/wp-dyn/content/article/2008/05/02/AR2008050201646.html

Dernières vulnérabilités
Autres avis – actualités

- Phorm, ou comment se faire sniffer par son ISP
  - http://www.f-secure.com/weblog/archives/00001420.html
- Le nouveau code bancaire rendra-t-il responsable les utilisateurs des fraudes ?
  - http://www.theregister.co.uk/2008/04/04/banking_code_2008/
- L'USAF recrute pour la "Cyber Offense"
  - http://www.sourceboston.com/blog/?p=16
  - Ont-ils les moyens de recruter et conserver les meilleurs ?
  - Ils n'arrivent même pas à décider du site géographique ☺
- L'OTAN fait de même
  - http://www.zataz.com/news/17127/OTAN--armee--cyberguerriers--Centre-d-excellence-de-l-Otan-pour-la-defense-cybernetique.html
- 26 pays créent le groupe IMPACT contre le cyber-terrorisme
  - http://www.zdnet.fr/actualites/internet/0,39020774,39381239,00.htm

Dernières vulnérabilités
Autres avis – actualités

- L'administration électronique en marche
  - http://www.synergies-publiques.fr/article.php?id_article=935
- Le Guide Pratique des Communications Electroniques
  - http://www.industrie.gouv.fr/gpce/index.php
- Les douaniers américains ont bien le droit de fouiller les portables
  - http://www.reseaux-telecoms.net/actualites/lire-les-douaniers-americains-ont-bien-le-droit-de-copier-les-disques-durs-des-visiteurs-18062.html
- HoaxBuster, version anglaise
  - http://www.lookstoogoodtobetrue.com/
- Phrack 65 est sorti
- Aucun rapport avec Windows
  - Mais comment ne pas évoquer la faille Debian/OpenSSL ?

Dernières vulnérabilités
Autres avis – actualités

- Le concours "Race to Zero" (DefCon 16) fait déjà parler de lui
  - Le principe : rendre un virus indétectable
    - http://www.racetozero.net
  - Les commentaires pleuvent :
    - http://cert.lexsi.com/weblog/index.php/2008/04/30/234-race-to-zero-l-embarras-des-editeurs-anti-virus
    - http://expertmiami.blogspot.com/2008/04/les-av-cest-chier.html
    - http://www.vulnerabilite.com/race-to-zero-virus-vx-concours-antivirus-actualite-20080505235710.html

Dernières vulnérabilités
Autres avis – just for fun

- Ca progresse
  - Cette année, seulement 45% des femmes donnent leur mot de passe contre une barre de chocolat
    - http://www.infosec.co.uk/page.cfm/T=m/Action=Press/PressID=1071
    - Autour de 60% l'année dernière
    - Note: les hommes font 10% ☺
- S'attaquer au GSM n'est pas sans risque
  - http://blog.thc.org/index.php?/archives/1-GSM-Researcher-stopped-at-Heathrow-Airport-by-UK-government-officials.html
- Le crawler de Google remplit désormais les formulaires
  - Pas toujours une bonne idée ...
    - http://www.out-law.com/default.aspx?page=9052
- Des "AdWords" parfois curieux
  - http://royal.pingdom.com/?p=298

Dernières vulnérabilités
Autres avis – just for fun

- Ne pas partir jouer en salle de réunion avec la X-Box
  - http://windowsitpro.com/article/articleid/50428/the-website-is-down-because-someone-removed-the-x-box.html
- IE6, le pire navigateur de tous les temps ?
  - http://www.savethedevelopers.org/
- Un disque dur sécurisé
  - http://www.myglobull.fr/
- Google, toujours aussi "cool" ?
  - http://google.com/health/
- Ca existait déjà chez Microsoft ☺
  - http://www.healthvault.com/

Questions / réponses

- Questions / réponses
- Prochaine réunion le 7 juillet 2008
- N'hésitez pas à proposer des sujets et des salles