OSSIR
Groupe Paris

Réunion du 15 mai 2012

Revue des dernières vulnérabilités

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

Avis Microsoft

- **Avril 2012**

  - **MS12-023 Correctif cumulatif pour IE (x5) [1]**
    - **Affecte: IE (toutes versions supportées)**
    - **Exploit:**
      - **Faille à l'impression d'une page malformée**
      - **Faille dans le moteur JScript9**
      - **Faille dans OnReadyStateChange()**
      - **Faille dans SelectAll()**
      - **Faille dans les styles VML**
    - **Crédit:**
      - **linx2008 / aisec.cn**
      - **Roel Spilker / TOPdesk**
      - **Jose Antonio Vazquez Gonzalez + iDefense**
      - **Anonymous + ZDI (x2)**
      - **Masato Kinugawa**

Avis Microsoft

- MS12-024 Faille dans Authenticode [1]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: modification d'un exécutable sans invalidation de la signature
    - https://blog.avast.com/2012/04/12/beware-of-a-new-windows-security-vulnerability-ms12-024
    - http://badishi.com/ms12-024-cve-2012-0151-some-exploitation-details/
  - Crédit: Robert Zacek & Igor Glucksmann / Avast

- MS12-025 Faille dans .NET Framework [1]
  - Affecte: .NET Framework
    - Toutes versions supportées sauf 3.0SP2 et 3.5SP1
  - Exploit: évasion de la sandbox
    - http://archives.neohapsis.com/archives/fulldisclosure/2012-04/0264.html
    - "(…) fixes approximately a zillion vulnerabilities in System.Drawing.dll"
      - http://weblog.ikvm.net/PermaLink.aspx?guid=b3525cd1-8788-4d6d-b299-4722ddebad94
    - Note: le XBAP ne s'exécute plus sans confirmation dans IE
      - http://blogs.technet.com/b/srd/archive/2012/04/10/ms12-025-and-xbap-no-longer-a-driveby-threat.aspx
  - Crédit: Vitaliy Toropov + iDefense

Avis Microsoft

- **MS12-026 Failles dans ForeFront UAG (x2) [3]**
  - **Affecte: ForeFront UAG 2010 SP1 / SP1 Update 1**
  - **Exploit:**
    - **Accès au site par défaut sans authentification depuis l'extérieur**
    - **Redirection arbitraire**
  - **Crédit: n/d**

- **MS12-027 Faille dans l'ActiveX "Windows Common Controls" [1]**
  - **Affecte MSCOMCTL.OCX livré avec certaines versions de:**
    - **Office**
    - **SQL Server**
    - **BizTalk Server**
    - **Commerce Server**
    - **Visual FoxPro 8 et 9**
    - **VB6 Runtime**
  - **Exploit: exécution de code**
    - **Exploité "in the wild"**
  - **Crédit: n/d**

Avis Microsoft

- **MS12-028 Faille dans le convertisseur WPS [1]**
  - **Affecte: Office 2007 SP2, Works 9, convertisseur Works 6 à 9**
  - **Exploit: "heap overflow"**
  - **Crédit: Shaun Colley / IOActive**

Mai 2012

- **MS12-029 Faille dans le convertisseur RTF de Word [1]**
  - **Affecte: Word (toutes versions supportées, sauf 2010 et Viewer)**
  - **Exploit: exécution de code à l'ouverture d'un fichier RTF malformé**
  - **Crédit: anonymous + ZDI**

Avis Microsoft

- MS12-030 Failles Excel (x6) [3,3,1,1,2,1]
  - Affecte: Office (toutes versions supportées, y compris Mac et Viewer)
  - Exploit: exécution de code à l'ouverture d'un fichier Excel malformé
  - Crédit:
    - Omair (x3)
      - http://krash.in/
    - Sean Larsson & Jun Mao + iDefense (x2)
    - anonymous + ZDI

- MS12-031 Faille Visio Viewer [1]
  - Affecte: Visio Viewer 2010
  - Exploit: exécution de code à l'ouverture d'un fichier Visio malformé
  - Crédit: Luigi Auriemma + iDefense

Avis Microsoft

- MS12-032 Failles dans TCP/IP [1]
  - Affecte: Windows Vista / 2008 / Seven / 2008R2
  - Exploit:
    - Elévation locale de privilèges
      - Via une erreur d'implémentation IPv6 (*double free*)
      - http://stackoverflow.com/questions/9472603/calling-socket-bind-results-in-windows-bluescreen
      - http://www.helpppers.com/questions/view/9472603
    - Contournement du pare-feu
      - L'émission de requêtes en broadcast est possible
  - Crédit:
    - Anatoliy Glagolev / Genesys Telecommunications
    - Bojan Zdrnja / INFIGO IS

- MS12-033 Faille dans le gestionnaire de partitions (?) [1]
  - Affecte: Windows Vista / 2008 / Seven / 2008R2
  - Exploit: élévation de privilèges via le "PnP Configuration Manager"
  - Crédit: n/d

Avis Microsoft

- MS12-034 Correctif total pour Office / Windows / .NET / SilverLight (x10) [1,1,1,1,2,1,1,1,1,1]
  - Affecte: …
    - Sauf .NET 2.0 SP2, .NET 3.5 SP1, Office 2008 & 2011 (Mac), Office Compatibility Pack, Works 9
  - Exploit:
    - Exécution de code en mode noyau à l'ouverture de polices TrueType (x2)
    - Evasion de sandbox .NET + DoS via WPF
    - Exécution de code à l'ouverture d'un fichier EMF malformé dans GDI+ (x2)
    - "Double Free" dans SilverLight
    - Faille noyau dans la gestion des messages
    - Faille noyau dans le support des fichiers de *layout* clavier
      - http://www.coresecurity.com/content/windows-kernel-readlayoutfile
      - https://twitter.com/#!/kernelpool/status/200044518853189633
      - Note: les fichiers de *layout* ne sont plus chargés depuis un emplacement autre que %windir%\system32
      - Patch insuffisant ?
      - http://dl.dropbox.com/u/22903093/MS12-034_fail.png
    - Faille noyau dans le calcul des *scrollbars*

Avis Microsoft

- Explication:
  - http://blogs.technet.com/b/srd/archive/2012/05/08/ms12-034-duqu-ten-cve-s-and-removing-keyboard-layout-file-attack-surface.aspx
- Crédit:
  - Alin Rad Pop + ZDI
  - Vitaliy Toropov + ZDI
  - Omair
  - anonymous + iDefense (x2)
  - Alex Plaskett / MWR InfoSecurity
  - Tarjei Mandt / Azimuth Security
  - Nicolas Economou / Core Security Technologies
  - Geoff McDonald / Symantec
  - h4ckmp

Avis Microsoft

- **MS12-035 Failles dans .NET Framework (x2) [1]**
  - **Affecte: .NET Framework (toutes versions supportées)**
  - **Exploit: contournement de la sandbox (x2)**
  - **Crédit: James Forshaw / Context Information Security (x2)**

Avis Microsoft

- Prévisions pour Juin 2012
- Advisories
- Retour sur des failles antérieures
  - Injection SQL dans la commande RESTORE DATABASE
    - Affecte SQL Server (toutes versions)
    - Pas de correctif Microsoft prévu
      - https://www.teamshatter.com/?p=3373
  - Faille RDP: la source de la fuite identifiée
    - Un "partenaire" chinois
      - http://blogs.technet.com/b/msrc/archive/2012/05/03/mapp-update-taking-action-to-decrease-risk-of-information-disclosure.aspx

Avis Microsoft

- **Révisions**
  - **MS11-025**
    - **V4.3: changement dans la logique de détection**
  - **MS11-030**
    - **V1.1: ajout d'un problème connu**
  - **MS11-067**
    - **V1.1: changement dans la logique de détection**
  - **MS11-100**
    - **V1.4: ce bulletin corrigeait également CVE-2012-0160 et CVE-2012-0161**
  - **MS12-017**
    - **V1.1: ajout d'un problème connu**
  - **MS12-026**
    - **V1.1: correction documentaire**
  - **MS12-027**
    - **V2.0: SQL 2008 R2 SP1 est aussi affecté**
  - **MS12-028**
    - **V1.1: explication sur la fourniture du correctif aux utilisateurs d'Office 2007 SP3**
  - **MS12-029**
    - **V1.1: correction documentaire**
  - **MS12-030**
    - **V1.1: correction documentaire**
  - **MS12-032**
    - **V1.1: correction documentaire (*mitigating factors*)**
  - **MS12-035**
    - **V2.0: correction documentaire sur le couple { .NET 1.1 SP1 ; Windows 2003 SP2 }**

Infos Microsoft

- **Sorties logicielles**
  - **SQL Server 2012**
  - **System Center 2012**

Infos Microsoft

- **Autre**
  - **Enorme #fail pour Hotmail.com**
    - **Réinitialisation triviale de n'importe quel mot de passe**
      - **http://www.whitec0de.com/new-hotmail-exploit-can-get-any-hotmail-email-account-hacked-for-just-20/**
    - **Mauvaise gestion de la communication**
      - **https://twitter.com/#!/msftsecresponse/status/195568235654021121**
    - **Et mauvais correctif**
      - **http://thehackernews.com/2012/04/yet-another-hotmail-aol-and-yahoo.html**
  - **Microsoft Security Intelligence Report (SIR) volume 12**
    - **Conficker n'est pas mort …**
      - **http://www.microsoft.com/security/sir/default.aspx**
  - **IE sera-t-il le seul navigateur du prochain Windows 8 / ARM ?**
      - **http://blog.mozilla.org/blog/2012/05/09/windows-on-arm-users-need-browser-choice-too/**
  - **Windows 7 et Xbox 360 interdits en Allemagne**
    - **Pour cause de violation d'un brevet Motorola**

Infos Réseau

- (Principales) faille(s)
  - "Remote root preauth" dans F5 FirePass VPN SSL
    - Injection SQL …
      - https://www.sec-consult.com/files/20120328-0_F5_FirePass_SSL_VPN_unauthenticated_remote_root_v1.0.txt

Infos Réseau

- **Autres infos**
  - **Les WebSockets HTML5 ne passent pas par Tor**
    - **https://blog.torproject.org/blog/firefox-security-bug-proxy-bypass-current-tbbs**
  - **Tous les supernodes de Skype sont désormais hébergés chez Microsoft**
    - **http://expertmiami.blogspot.fr/2012/05/skype-does-away-with-random-supernodes.html**

Infos Unix

- **(Principales) faille(s)**
  - **OpenSSL < 0.9.8v, < 1.0.0i, < 1.0.1a**
    - **Faille dans asn1_d2i_read_bio() qui affecte de nombreux logiciels par effet de bord**
      - **http://www.openssl.org/news/secadv_20120419.txt**
    - **… sauf OpenSSH qui a réimplémenté cette partie du code**
    - **Crédit: Tavis Ormandy (Google)**
      - **http://lists.grok.org.uk/pipermail/full-disclosure/2012-April/086585.html**
    - **… mais la publication originale date de 2006 !**
      - **https://twitter.com/#!/mdowd/status/192986878138523648**

Infos Unix

- Enorme #fail de PHP (en mode CGI)
  - http://ompldr.org/vZGxxaQ
  - "?-s" permet de voir le source
  - "?-d" permet d'exécuter du code
    - http://blog.spiderlabs.com/2012/05/php-cgi-exploitation-by-example.html
  - Le correctif était aussi bogué
  - Note: "facebook.com/?-s" était un challenge de recrutement ☺
- Par ailleurs: PHP + contrôle d'accès par ".htaccess" = FAIL
  - http://eguaj.tumblr.com/post/2361187940/re-hackers-bypass-htaccess-security-by-using-gets
  - http://armoredcode.com/blog/bypassing-basic-authentication-in-php-applications/

Infos Unix

- "Remote root preauth" dans Samba < 3.6.4
  - https://www.samba.org/samba/security/CVE-2012-1182
  - Exploitation possible
    - http://jmprsp.blogspot.de/2012/04/zuverlassige-exploitation-von-zdi-can.html
    - http://partners.immunityinc.com/movies/CANVAS-SambaNDR.mov

Infos Unix

- **Injection de code PHP dans WooThemes pour WordPress**
  - **https://gist.github.com/2523147**
- **Gajim**
  - **Exécution de commandes *shell* à travers un lien dans un chat**
    - **https://lwn.net/Alerts/492647/**
- **PolarSSL**
  - **http://polarssl.org/trac/changeset?old_path=%2Ftrunk&old=1220&new_path=%2Ftrunk&new=1221**

Infos Unix

- **Autre**
  - **Ubuntu 12.04 LTS est sorti**

Failles

- **Principales applications**
  - **FireFox < 12.0**
    - **https://www.mozilla.org/security/known-vulnerabilities/firefox.html**
  - **ThunderBird < 12.0.1**
    - **https://www.mozilla.org/security/known-vulnerabilities/thunderbird.html**
  - **Opera < 11.64**
    - **Exécution de code via une URL malformée**
      - **http://www.opera.com/support/kb/view/1016/**
  - **VMWare (WorkStation et ESX)**
    - **Evasion invité vers hôte à travers les VMTools**
      - **http://www.vmware.com/security/advisories/VMSA-2012-0009.html**
      - **http://seclists.org/bugtraq/2012/May/22**

Failles

- iOS < 5.1.1
  - http://support.apple.com/kb/HT5278
- Mac OS X < 10.7.4
  - http://support.apple.com/kb/HT5167
  - http://support.apple.com/kb/HT5281
  - FileVault enregistrait le mot de passe de l'utilisateur en clair …
    - http://seclists.org/fulldisclosure/2012/May/44
- Safari < 5.1.7
  - Note: Flash est désormais désactivé dans Safari s'il n'est pas à jour
    - http://support.apple.com/kb/HT5282

Failles

- ShockWave Player < 11.6.5.635
  - http://www.adobe.com/support/security/bulletins/apsb12-13.html
  - Exploits
    - http://seclists.org/fulldisclosure/2012/May/71
    - http://seclists.org/fulldisclosure/2012/May/72
    - http://seclists.org/fulldisclosure/2012/May/73
- Flash Player corrigé en urgence
  - http://www.adobe.com/support/security/bulletins/apsb12-09.html
  - Suite à des attaques ciblées
    - https://twitter.com/#!/diocyde/status/199621955916267520
- Adobe va faire payer les correctifs de sécurité
  - http://www.zdnet.com.au/adobe-users-required-to-pay-for-security-339337601.htm
  - Ou pas
    - http://www.computerworld.com/s/article/9227119/Adobe_backpedals_will_now_patch_software_for_free

Failles

- Oracle Quaterly Patch
  - 88 correctifs (hors Java)
    - http://www.oracle.com/technetwork/topics/security/cpuapr2012-366314.html
  - Exploits
    - https://www.teamshatter.com/topics/general/team-shatter-exclusive/advisory-failed-authentication-using-ocipassword-not-recorded/
    - https://www.teamshatter.com/topics/general/team-shatter-exclusive/advisory-sql-injection-in-oracle-enterprise-manager-searchpage-web-page-2/
    - https://www.teamshatter.com/topics/general/team-shatter-exclusive/advisory-http-response-splitting-in-oem-prevpage/
    - https://www.teamshatter.com/topics/general/team-shatter-exclusive/advisory-incomplete-protection-of-oracle-database-locked-accounts/
    - https://www.teamshatter.com/topics/general/team-shatter-exclusive/advisory-ocipasswordchange-leaks-information-pwdhash/
    - https://www.teamshatter.com/topics/general/team-shatter-exclusive/advisory-oem-vulnerable-to-session-fixation/
    - https://www.teamshatter.com/topics/general/team-shatter-exclusive/advisory-sqli-oem-comparewizfirstconfig/
    - https://www.teamshatter.com/topics/general/team-shatter-exclusive/advisory-sql-injection-in-oracle-enterprise-manager-searchpage-web-page/
    - http://www.security-explorations.com/en/SE-2012-01-status.html
    - http://www.vulnerability-lab.com/get_content.php?id=478

Failles

- Oracle
  - "By design", il est possible d'ajouter une instance de réplication et de récupérer tout le trafic destiné à la base de données
    - http://seclists.org/fulldisclosure/2012/Apr/204
  - Remarque: aucun correctif n'est disponible …
    - http://archives.neohapsis.com/archives/fulldisclosure/2012-04/0342.html
- Rappel: Java 1.6 est EOL en novembre 2012
    - https://blogs.oracle.com/henrik/entry/updated_java_6_eol_date

Failles

- SumatraPDF < 2.1.1
- PCAnywhere
  - Détails du "remote root preauth" découvert par NGS
    - http://www.securityfocus.com/archive/1/522534
- "HP Secure Web Server"
  - … alias PHP pour OpenVMS …
    - http://www.securityfocus.com/archive/1/522375
- ZTE: simple, efficace
  - /system/bin/sync_agent ztex1609523

Failles 2.0

- Une attaque contre les sites pétroliens iraniens
  - Le "virus" attaquerait les BIOS des PC ciblés pour les rendre inopérants
    - http://english.sina.com/world/2012/0423/460971.html
    - http://french.ruvr.ru/2012_04_23/Iran-hackers-cyberattaques/
- Tentatives d'intrusion répétées dans des systèmes de contrôle de gazoducs
    - www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Apr2012.pdf
- Des mises à jour malveillantes distribuées dans des réseaux d'hôtels
    - http://www.ic3.gov/media/2012/120508.aspx
- La réallocation d'espace disque dans le Cloud
  - … ne se fait pas toujours avec effacement
    - http://www.contextis.co.uk/research/blog/dirtydisks/
- Un keylogger pour Android
  - Basé sur le capteur de mouvements
    - http://www.cse.psu.edu/~szhu/papers/taplogger.pdf

Sites piratés

- Les sites piratés du mois
  - ESA, NASA, USAF, Renault, www.servicehistorique.sga.defense.gouv.fr, …
    - http://thehackernews.com/2012/05/hacker-claims-to-hack-european-space.html
    - http://www.zdnet.com/blog/security/nasa-esa-confirm-hacks-the-unknowns-says-systems-patched/11902
    - Victimes du groupe "The Unknowns"
      - https://twitter.com/1_The_Unknown_1
  - www.performance-publique.budget.gouv.fr
    - http://research.zscaler.com/2012/04/french-budget-minister-website-hijacked.html
  - Le MoD
    - http://www.guardian.co.uk/technology/2012/may/03/hackers-breached-secret-mod-systems

Sites piratés

- Cryptic Studios
  - http://venturebeat.com/2012/04/25/cryptic-hacked/
- Dexia racketée
  - http://www.undernews.fr/banque-cartes-bancaires/la-banque-dexia-piratee-puis-menacee-par-des-cybercriminels.html
  - http://pastebin.com/E8ADVeHG
- Nissan victime d'APT
  - http://www.darkreading.com/database-security/167901020/security/news/232900999/nissan-hack-a-harsh-reminder-about-protecting-data-stores-from-spies.html
- Le code source de VMWare ESX avait été volé en 2003
  - http://blogs.vmware.com/security/2012/04/vmware-security-note.html
  - … chez les chinois du CEIEC
    - http://pastebin.com/JGxdK6vw

Malwares, spam et fraudes

- Un opérateur de botnet parle
  - http://www.reddit.com/r/IAmA/comments/sq7cy/iama_a_malware_coder_and_botnet_operator_ama/
- Une base de virus
  - http://www.malware.lu/
- DFBootKit
  - Un "bootkit" pour Android
    - http://research.nq.com/?p=391
- John McAfee arrêté au Bélize
  - http://edition.channel5belize.com/archives/69892

Actualité (francophone)

- Le RGS v2 arrive
  - http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/evolution-du-referentiel-general-de-securite.html
- L'envoi de données professionnelles sur une adresse email "perso" sanctionné
  - Dans un cas quand même assez malveillant
    - http://www.zataz.com/news/22137/entreprise--salarie--denigrement--courriel--transfert.html
- Les actes d'huissier peuvent être numériques
  - http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025524395&dateTexte=categorieLien=id
- Cassidian crée une filiale dédiée à la "Cyber Sécurité"
  - http://www.cassidian.com/en_US/web/guest/EADS%20CASSIDIAN%20announce%20the%20creation%20of%20Cassidian%20CyberSecurity
- L'AFNOR crée un groupe de travail sur les fuites de données
  - http://www.lemondeinformatique.fr/actualites/lire-l-afnor-cree-un-groupe-de-travail-pour-prevenir-les-fuites-de-donnees-sensibles-48640.html

Actualité (francophone)

- La CNIL enquête sur les cartes de paiement NFC
  - http://www.cnil.fr/nc/la-cnil/actualite/article/article/securite-des-cartes-bancaires-sans-contact-expertise-en-cours/
- Il y aura un antivirus français
  - https://twitter.com/#!/timstrazz/status/199410969233993729
  - Et Iranien aussi
    - http://news.techworld.com/security/3355680/paranoia-drives-iran-develop-homegrown-antvirus-program/
- Les assises de l'insécurité …
  - http://www.google.fr/search?q=site%3Ales-assises-de-la-securite.com

Actualité (anglo-saxonne)

- Toutes les entreprises américaines ont été piratées par les Chinois
  - http://news.slashdot.org/story/12/03/27/1757248/richard-clarke-all-major-us-firms-hacked-by-china
- "*We need wiretap-ready Web sites now*" (FBI)
  - http://news.cnet.com/8301-1009_3-57428067-83/fbi-we-need-wiretap-ready-web-sites-now/
- La NSA archiverait toutes les correspondances électroniques
  - http://www.democracynow.org/2012/4/20/whistleblower_the_nsa_is_lying_us

Actualité (européenne)

- **Appel à candidatures pour l'ENISA**
  - **http://www.enisa.europa.eu/media/press-releases/appel-a-candidature-pour-le-PSG**
- **On ne peut pas breveter un langage de programmation en Europe**
  - **http://www.groklaw.net/article.php?story=20120502083035371**

Actualité (Google)

- (pwn2own) Chrome 17.0.963.78 corrige une faille à $60,000
  - http://googlechromereleases.blogspot.fr/2012/03/chrome-stable-channel-update.html
- Google augmente les récompenses pour son "Bug Bounty"
  - http://googleonlinesecurity.blogspot.fr/2012/04/spurring-more-vulnerability-research.html
- Google *savait* que le contenu du WiFi était enregistré par les Google Cars
  - http://www.theregister.co.uk/2012/04/30/google_slurp_ok/

Actualité (Apple)

- Kaspersky: "Apple a 10 ans de retard sur Microsoft"
  - http://malware.cbronline.com/news/apple-10-years-behind-microsoft-on-security-kaspersky-250412

Actualité (crypto)

- Ivan Golubev's Password Recovery Suite
  - http://www.golubev.com/igprs/

Actualité

- Conférences passées
  - EICAR
- Conférences à venir
  - Recon (Juin 2012)
    - http://recon.cx/
  - Hack.lu (Octobre 2012)
    - http://2012.hack.lu/hacklu2012-cfp.txt
- Sorties logicielles
  - OphCrack 3.4.0

Actualité

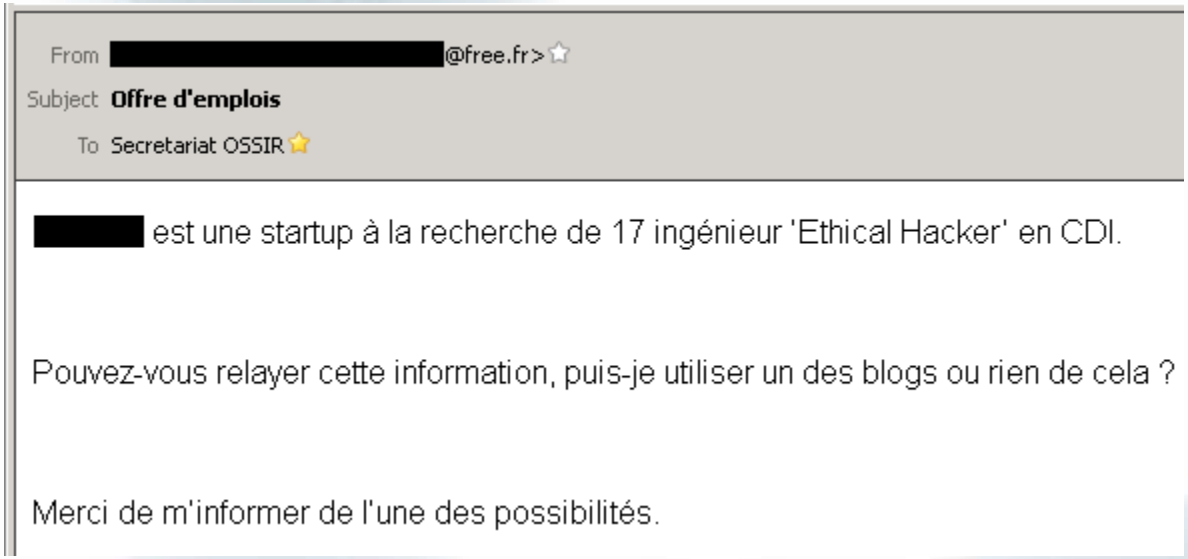
- **Phrack #68**
  - http://www.phrack.com/
- **Ce site ne fonctionne plus**
  - Mais il marchait très bien avant
    - http://skype-ip-finder.tk
- **L'Argentine sous écoutes illégales ?**
  - La société chinoise CEIEC aurait vendu $900,000 de matériel au gouvernement argentin
    - http://cryptome.org/2012/05/argentine-warrantless-wiretap.7z
- **Un moteur de recherche qui ne référence pas les 1m de sites les plus populaires**
  - http://millionshort.com/
- **Journée mondiale contre les DRM**
  - C'était le 4 mai
- **LinkedIn rachète SlideShare**
  - $119 millions
    - http://www.lesechos.fr/entreprises-secteurs/tech-medias/actu/0202046145971-linkedin-s-offre-slideshare-pour-119-millions-de-dollars-319700.php

Divers

- Décès de Roland Moreno
  - http://www.leparisien.fr/high-tech/deces-de-roland-moreno-l-inventeur-de-la-carte-a-puce-29-04-2012-1977091.php
- Le code source de Prince of Persia publié sur GitHub
  - http://jordanmechner.com/blog/2012/03/prince-of-persia-source-code-found/
- L'origine du <blink>
  - http://www.montulli.org/theoriginofthe%3Cblink%3Etag
- Un XSS dans PhpMyBible
  - http://archives.neohapsis.com/archives/fulldisclosure/2012-04/0243.html
- Oh, drama
  - http://eddy.bordi.fr/jordi-chancel

Divers

- Hmmm …



From [redacted]@free.fr>

Subject **Offre d'emplois**

To Secretariat OSSIR

[redacted] est une startup à la recherche de 17 ingénieur 'Ethical Hacker' en CDI.

Pouvez-vous relayer cette information, puis-je utiliser un des blogs ou rien de cela ?

Merci de m'informer de l'une des possibilités.

Divers

- Re-hmmm …

Catégorie : Forum de discussion — Choisir une catégorie

[redacted] recrute des pentesters

101 Lectures | 1 Commentaire

1 Message

Anne-sophie Laurent
Chargée de gestion de ressources humaines, [redacted] REGIONS
Albigny sur Saône, France

mardi 24 avril 2012

Présentation de la société :
Le Groupe [redacted] (150 personnes) est un cabinet de conseil indépendant spécialisé en sécurité informatique. Tester les systèmes de nos clients, auditer leurs procédures et proposer des solutions pragmatiques est le quotidien de nos équipes.

Journée type d'un pentester [redacted] :
• 10mn d'injection SQL pour récupérer les hash et les cracker grâce aux outils [redacted]
• Une matinée pour exploiter la 0-day trouvée la veille : l'AD est sous contrôle, le reste ne saurait tarder.
• Prendre 2 tasses de café, échanger avec les collègues sur le forum interne avant de tester des SCADA dans le labo.
• Finaliser la publication sur la 0-day trouvée au cours du pentest et présentation des résultats des tests en vidéoconférence : un client satisfait.
• Préparer une RUMP pour le SSTIC avec les collègues de [redacted] Montréal et Singapour.
• Rooter un ipad et un iphone pour un client grand compte.
• Reprendre un peu de café …

Vous souhaitez faire de cette journée votre quotidien ? Rejoignez-nous.

Votre parcours :
Diplômé BAC+5 ou équivalent, passionné par les problématiques de sécurité des systèmes, vous souhaitez approfondir vos connaissances en pentest, reverse, forensic.
Vous êtes rigoureux et développez un excellent relationnel client.

6

Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 12 juin 2012