OSSIR
Groupe Paris

Réunion du 10 avril 2012

Revue des dernières vulnérabilités

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

Avis Microsoft

- **Février 2012**
  - **??? bulletins, ??? failles**
  - **MS12-008 Failles noyau [1,2]**
    - **Affecte: Windows (toutes versions supportées)**
    - **Exploit: élévation de privilèges locale**
      - **Faille dans le support des layouts clavier**
      - **Faille dans GDI**
    - **Crédit: Tarjei Mandt / Azimuth Security**

Avis Microsoft

- **MS12-009 Faille noyau dans AFD.SYS [1,1]**
  - **Affecte: Windows (toutes versions supportées)**
    - **Sauf XP SP3 / Vista SP2 / 2008 SP2 (x86) / Seven SP0 & SP1 (x86)**
  - **Exploit: élévation de privilèges locale**
  - **Crédit: Tarjei Mandt / Azimuth Security (x2)**

- **MS12-010 Correctif cumulatif pour IE [1,3,-,-]**
  - **Affecte: IE 6 – 9 (toutes versions supportées)**
  - **Exploit:**
    - **Exécution de code à travers une page HTML malformée (ZDI-12-035)**
    - **Exécution de code à travers un fichier VML malformé (ZDI-12-036)**
    - **Fuite d'information via le presse-papiers**
    - **Fuite d'information sur la mémoire du processus**
  - **Crédit:**
    - **Jan Schejbal**
    - **Stephen Fewer / Harmony Security + ZDI (x2)**
    - **Jason Hullinger / HP Cloud Services**

Avis Microsoft

- MS12-011 XSS dans SharePoint [1,1,1]
  - Affecte: SharePoint 2010 SP0 & SP1 (versions Server et Foundation)
  - Exploit: XSS dans les pages suivantes
    - inplview.aspx
    - themeweb.aspx
    - wizardlist.aspx
  - Crédit:
    - John Hollenberger
    - Rocco Calvi / stratsec
    - Giorgio Fedon / Minded Security

- MS12-012 "DLL Preloading" dans le panneau de configuration [1]
  - Affecte: Windows 2008 et 2008R2
  - Exploit: "DLL Preloading" dans le panneau "Couleurs"
  - Crédit: n/d

Avis Microsoft

- MS12-013 "Buffer overflow" dans MSVCRT.DLL [1]
  - Affecte: Windows Vista / 2008 / Seven / 2008R2
  - Exploit: "heap overflow" dans printf("%f")
  - Crédit: Alexander Gavrun + ZDI-12-034

- MS12-014 "DLL Preloading" dans le codec Indeo [1]
  - Affecte: Windows XP SP3
  - Exploit: "DLL Preloading"
  - Crédit: n/d

Avis Microsoft

- MS12-015 Failles dans Visio Viewer [1,1,3,3,3]
  - Affecte: Visio Viewer 2010 SP0 & SP1
  - Exploit: exécution de code à l'ouverture d'un fichier ".VSD" malformé
  - Crédit: Xin Ouyang / Palo Alto Networks (x5)

- MS12-016 Failles dans .NET Framework [1,1]
  - Affecte: .NET Framework et SilverLight (toutes versions supportées)
    - Sauf .NET 1.1 SP1, .NET 3.5 SP1 et SilverLight 5
  - Exploit:
    - Faille .NET
    - "Heap overflow"
  - Crédit: Jeroen Frijters / Sumatra

Avis Microsoft

- **Mars 2012**
  - **??? bulletins, ??? failles**
  - **MS12-017 Faille dans le serveur DNS [3]**
    - **Affecte: Windows 2003, 2008 et 2008R2**
      - **Versions x86 et x64**
    - **Exploit: déni de service distant**
    - **Crédit: n/d**

Avis Microsoft

- MS12-018 Elévation de privilèges locale [2]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: faille dans l'API PostMessage()
  - Crédit: Nikolaos Bougalis

- MS12-019 Faille dans DirectWrite [?]
  - Affecte: Windows Vista / 2008 / Seven / 2008R2
  - Exploit: déni de service au travers d'une séquence Unicode malformée
  - Crédit: Khaled M. Salameh

Avis Microsoft

- MS12-020 Faille RDP / Terminal Server [1,3]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: déni de service distant avant authentification
    - Une faille qui a suscité beaucoup d'activité
    - … mais a priori non exploitable (hors DoS)
      - http://istherdpexploitoutyet.com/
      - http://expertmiami.blogspot.fr/2012/03/ms12-020-round-up.html
    - Le PoC fourni par Microsoft dans le cadre du programme MAPP s'est retrouvé sur un forum chinois …
      - http://aluigi.org/adv/ms12-020_leak.txt
  - Crédit: Luigi Auriemma + ZDI-12-044

Avis Microsoft

- MS12-021 Faille dans les plugins Visual Studio [1]
  - Affecte: Visual Studio 2008 et 2010
  - Exploit: sorte de "DLL Preloading" d'un plugin
    - http://www.laplinker.com/2012/03/msrc-patch-tuesday-march-2012.html
  - Crédit: Laplinker

- MS12-022 "DLL Preloading" dans Expression Design [1]
  - Affecte: Expression Design (toutes versions supportées)
  - Exploit: "DLL Preloading"
    - http://www.laplinker.com/2012/03/msrc-patch-tuesday-march-2012.html
  - Crédit: Laplinker

Avis Microsoft

- Prévisions pour Avril 2012

- Advisories
  - Q2269637 "DLL Preloading"
    - V14.0: publication des correctifs MS12-012 et MS12-014
    - V15.0: publication du correctif MS12-022

- Retour sur des failles antérieures
  - MS11-093
    - http://aluigi.org/adv/ole32_1-adv.txt

Avis Microsoft

- **Révisions**
  - **MS10-058**
    - **V2.0: changement dans la logique de détection (devient indépendant de MS10-029)**
  - **MS11-025**
    - **V4.3: changement dans la logique de détection**
  - **MS11-030**
    - **V1.1: ajout d'un problème connu**
  - **MS11-049**
    - **V2.4: correction des numéros de version SQL Server**
  - **MS11-067**
    - **V1.1: changement dans la logique de détection**
  - **MS11-088**
    - **V1.2: Office Pinyin SimpleFast * 2010 ne sont plus supportés**
  - **MS11-089**
    - **V1.2: ajout de numéros de KB**
  - **MS12-001**
    - **V1.1: ajout d'un problème connu**
  - **MS12-014**
    - **V1.1: ajout d'un problème connu**
  - **MS12-016**
    - **V1.1: changement dans la logique de détection**
    - **V1.2: suppression des problèmes connus**
  - **MS12-022**
    - **V1.1: retrait d'un paramètre de ligne de commande invalide**

Infos Microsoft

- **Sorties logicielles**
  - **Windows Phone 7.5.1 "Tango"**
  - **Windows 8 est prévu pour octobre**
    - **Selon les plans actuels**
  - **ForceASLR**
    - **Pour Windows 7 et 2008R2**
      - **http://support.microsoft.com/kb/2639308/en-us**

Infos Microsoft

- Autre
  - "Microsoft c'est mieux que Google"
    - http://www.whymicrosoft.com/en-us/pages/google-apps.aspx
    - http://www.youtube.com/watch?v=k4EbCkotKPU
  - 29 février: le bug de Windows Azure
    - http://www.generation-nt.com/cloud-windows-azure-annee-bissextile-actualite-1550161.html
    - http://www.zdnet.fr/blogs/infra-net/retour-sur-l-incroyable-panne-d-azure-le-cloud-de-microsoft-vers-de-lourdes-consequences-39769234.htm
    - http://www.cedexis.com/fr/blog/outage-of-windows-azure-cloud-why-you-need-a-multi-cloud-strategy-now/
  - Microsoft dément un Office pour iPad
    - http://www.linformaticien.com/actualites/id/23708/office-sur-ipad-microsoft-dement.aspx
  - ASP.NET devient Open Source
    - http://weblogs.asp.net/scottgu/archive/2012/03/27/asp-net-mvc-web-api-razor-and-open-source.aspx
  - Microsoft partage ses données sur les infections
    - Note: l'infrastructure est construite sur Java + Hadoop ☺
      - http://www.clubic.com/antivirus-securite-informatique/actualite-469526-securite-microsoft-planche-flux-information-global.html

Infos Réseau

- (Principales) faille(s)
  - Bulletins Cisco IOS
    - RSVP
      - http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-rsvp
    - Smart Install
      - http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-smartinstall
    - SSH
      - http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ssh
    - Zone-based firewall
      - http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfw
    - IKE
      - http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ike
    - Traffic Optimization
      - http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-mace
    - SIP+NAT
      - http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-nat
    - Multicast Source Discovery Protocol
      - http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp
    - Contournement du niveau d'accès par AAA
      - http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

Infos Réseau

- Autres infos
  - Nouvelle règle: tous les ".com" appartiennent au gouvernement américain
    - http://blog2.easydns.org/2012/02/29/verisign-seizes-com-domain-registered-via-foreign-registrar-on-behalf-of-us-authorities/
    - http://www.zdnet.fr/actualites/le-gouvernement-us-s-affranchit-des-frontieres-pour-saisir-les-noms-de-domaines-en-com-39769367.htm
  - BIND 10 final
    - https://lists.isc.org/pipermail/bind10-announce/2012-March/000018.html
  - Anonymous: opération "Global BlackOut" le 31 mars 2012
    - … ou pas
  - Grosse panne d'Internet en Afrique
    - Suite à plusieurs incidents simultanés
      - http://www.linformaticien.com/actualites/id/23794/panne-d-internet-en-afrique.aspx

Infos Réseau

- **Huawei banni du cœur de réseau Australien**
  - **En cause: le risque de "backdoor"**
    - **http://www.google.com/hostednews/afp/article/ALeqM5gYMRz3tSa-yO2knsnRKebfatDfaQ?docId=CNG.af406032f7b2ea5c88b6f7c165f6cad0.2a1**

- **Les certificats NetASQ expirent le 12 mai 2012**
    - **http://blog.actn.fr/?p=172**

Infos Unix

- (Principales) faille(s)
  - Injection de commandes depuis l'écran de login
    - Avec LDM, c'est possible
      - http://www.ubuntu.com/usn/usn-1398-1/
  - Horde < 3.3.13 et Groupware < 1.2.11 backdoorés
    - Depuis novembre 2011 …
      - http://dev.horde.org/h/jonah/stories/view.php?channel_id=1&id=155
  - CVE-2011-4182
    - Toute commande shell présente dans un SSID
    - … est exécutée par ifup-services

Infos Unix

- **Autre**
  - **Linux 3.3 est sorti**
    - **Intègre du code Android**
      - **http://linuxfr.org/news/sortie-du-noyau-linux-3-3**
  - **Ubuntu pour Android**
    - **http://www.ubuntu.com/devices/android**
  - **Plus de Flash sous Linux (hors Chrome)**
    - **http://www.ubuntuvibes.com/2012/03/adobe-releases-last-linux-version-of.html**
  - **FreeBSD 9 intègre Capsicum**
    - **Une sandbox applicative**
      - **http://www.freebsdfoundation.org/press/FreeBSD%209.0%20Announcement.shtml**
  - **Le coût de développement de Debian**
    - **Estimé à $19 milliards …**
      - **http://blog.james.rcpt.to/2012/02/13/debian-wheezy-us19-billion-your-price-free/**

Failles

- Principales applications
  - ThunderBird < 3.1.20
    - http://www.mozilla.org/security/known-vulnerabilities/thunderbird31.html
  - FireFox < 3.6.28
    - http://www.mozilla.org/security/known-vulnerabilities/firefox36.html
  - FireFox < 9.0
    - ZDI-12-056
  - FireFox < 10.0
    - ZDI-12-059
  - FireFox, ThunderBird < 10.0.2
    - "Integer Overflow" dans LibPNG
      - http://www.h-online.com/open/news/item/Vulnerability-in-libpng-prompts-Firefox-and-Thunderbird-updates-1436810.html
    - Corrigé également dans Chrome
    - … et affecte de nombreux autres logiciels
  - FireFox, ThunderBird < 11.0

Failles

- Flash Player < 10.3.183.18, < 11.2.202.228
  - Pour commencer …
    - http://www.adobe.com/support/security/bulletins/apsb12-03.html
    - http://www.adobe.com/support/security/bulletins/apsb12-05.html
  - Puis … ZDI-12-057 / pwn2own
    - http://www.adobe.com/support/security/bulletins/apsb12-07.html
  - Flash Player dispose désormais d'une fonction de mise à jour automatique
  - Certaines failles ont été découvertes "dans la nature" …
    - http://www.darkreading.com/advanced-threats/167901091/security/attacks-breaches/232601036/flash-zero-day-used-in-targeted-email-attacks.html
  - Voir aussi
    - http://zhodiac.hispahack.com/my-stuff/security/Flash_ASLR_bypass.pdf

Failles

- Adobe Reader < 9.5.1, < 10.1.3
  - http://www.adobe.com/support/security/bulletins/apsb12-08.html
- ColdFusion 8 et 9
  - "Fameux" déni de service par collision de hash
    - http://www.adobe.com/support/security/bulletins/apsb12-06.html
- Safari < 5.1.4
  - ZDI-12-055
- QuickTime
  - ZDI-12-058

Failles

- Java < 1.6.31
  - http://www.oracle.com/technetwork/topics/security/javacpufeb2012-366318.html
  - ZDI-12-032, ZDI-12-037, ZDI-12-038, ZDI-12-039, ZDI-12-060
- Les failles n'ont pas tardé à être exploitées …
  - http://blogs.technet.com/b/mmpc/archive/2012/03/20/an-interesting-case-of-jre-sandbox-breach-cve-2012-0507.aspx
- … résultat: plus de 500,000 Mac infectés
  - http://krebsonsecurity.com/2012/04/urgent-fix-for-zero-day-mac-java-flaw/
  - Apple ne joue pas Fair Play sur ce coup
    - http://www.forbes.com/sites/andygreenberg/2012/04/09/apple-snubs-firm-who-discovered-mac-botnet-tries-to-cut-off-its-server-monitoring-infections/
- … et des virus techniquement innovants
  - http://www.kaspersky.com/about/news/virus/2012/Unique_fileless_bot_attacks_visitors_to_news_sites

Failles

- **Polycom HDX 8000: injection de commandes**
  - **http://blog.tempest.com.br/joao-paulo-campello/polycom-web-management-interface-os-command-injection.html**
- **Elévation de privilèges dans toute machine virtuelle VMWare**
  - **Niveau #epic**
    - **http://www.securityfocus.com/archive/1/522141**

Failles 2.0

- Injection de commandes dans un système de vote électronique
  - https://jhalderm.com/pub/papers/dcvoting-fc12.pdf
- Twitter passe en HTTPS par défaut !
  - http://blog.twitter.com/2012/02/securing-your-twitter-experience-with.html
  - Et pour être en HTTPS partout
    - https://www.eff.org/https-everywhere
- Il va être possible de chercher au-delà des 30 derniers jours …
  - … en payant
    - http://www.linformaticien.com/actualites/id/23795/twitter-ouvre-ses-archives-aux-entreprises.aspx

Failles 2.0

- Saturation du standard téléphonique depuis des téléphones portables
  - Simple mais efficace
    - http://datasecuritybreach.fr/actu/ddos-par-telephone-portable-pour-une-pme-francaise/

Sites piratés

- **Les sites piratés du mois**
  - **Un étudiant anglais condamné pour le piratage de Facebook**
    - **http://www.bbc.co.uk/news/uk-england-york-north-yorkshire-17079853**
  - **RockYou condamné à une amende de $250,000**
    - **http://www.scmagazine.com/rockyou-to-pay-ftc-250k-after-breach-of-32m-passwords/article/233992/**
  - **Les emails de Stratfor publiés sur WikiLeaks**
    - **http://wikileaks.org/the-gifiles.html**
  - **Un disque dur de 1 To volé chez Nexter**
    - **L'armoire de sécurité était restée ouverte pendant 3 jours suite à des travaux …**
      - **http://www.leparisien.fr/versailles-78000/des-donnees-militaires-sensibles-volees-chez-nexter-a-versailles-01-03-2012-1884953.php**

Sites piratés

- Un important processeur de paiements (Global Payments)
  - Plus de 10 millions de cartes compromises
    - http://krebsonsecurity.com/2012/03/mastercard-visa-warn-of-processor-breach/
- Kevin Mitnick (encore …)
    - https://twitter.com/#!/kevinrnitnick/status/184850883996164097
- Des Mac compromis par des attaques ciblées
    - http://arstechnica.com/apple/news/2012/03/james-bond-style-malware-attacks-come-to-the-mac.ars
- La NASA
  - Piratée 13 fois l'année dernière
    - http://www.reuters.com/article/2012/03/02/us-nasa-cyberattack-idUSTRE8211G320120302
  - Dont au moins une fois par les Chinois
    - http://www.linformaticien.com/actualites/id/23874/des-hackers-chinois-derriere-le-hack-de-la-nasa.aspx
  - Se fait voler un PC contenant les codes de la station internationales
    - http://www.zdnet.fr/actualites/nasa-vol-d-un-pc-avec-les-codes-de-la-station-spatiale-internationale-39769154.htm

Sites piratés

- DDoS Anonymous sur le site du Home Office (UK)
  - Attaque prévue tous les samedis désormais
    - http://www.bbc.co.uk/news/uk-17648852
- Les emails du président syrien étaient lus
  - … bien avant les Anonymous
    - http://www.lemonde.fr/technologies/article/2012/03/15/les-codes-du-compte-email-d-assad-sur-un-simple-bout-de-papier_1669394_651865.html
- Le Sénat
  - (Enfin non, mais c'est pas loin)
    - http://reflets.info/opendata-sur-lextranet-ump-du-senat/
- Idem pour prevention-delinquance.interieur.gouv.fr
    - https://twitter.com/#!/bluetouff/status/172344005311475712
- YouPorn (Chat)
    - http://pastebin.com/ieC6eTB7

Sites piratés

- GitHub
  - http://www.zdnet.fr/blogs/developpeur-zone/github-hacke-l-industrie-du-logiciel-menacee-39769326.htm
  - https://gist.github.com/1978249
- Linode
  - Le propriétaire s'est fait voler ses bitcoins …
    - http://bitcoinmedia.com/compromised-linode-coins-stolen-from-slush-faucet-and-others/
- Des employés indélicats dans un Call Center indien
  - http://nakedsecurity.sophos.com/2012/03/22/corrupt-call-center-workers-selling-your-private-information-for-pennies/

Malwares, spam et fraudes

- DNSChanger
  - Etes-vous infecté ?
    - http://dns-ok.fr/
  - Les "faux" DNS devait être éteints le 8 mars par le FBI
    - http://securityaffairs.co/wordpress/2682/malware/dnschanger-and-legal-consequences-of-operation-ghost-click.html
  - … sous la pression populaire, ça serait finalement le 9 juillet
    - http://securityaffairs.co/wordpress/3116/malware/dnschanger-fbis-internet-blackout-postponed-from-8-march-to-9-july.html
- Le code source de Symantec Antivirus est public
    - https://thepiratebay.se/torrent/7087027/
- Pour toute solution technique …
  - … il existe une meilleure attaque technique
    - http://www.lemondeinformatique.fr/actualites/lire-des-cartes-sim-frauduleuses-a-l-assaut-des-banques-en-ligne-48164.html

Malwares, spam et fraudes

- Que se passe-t-il quand on perd son téléphone ?
  - Symantec a testé pour vous
    - 50% des smartphones sont restitués
    - 96% sont fouillés
      - http://www.symantec.com/connect/blogs/introducing-symantec-smartphone-honey-stick-project
- Embargo sur les antivirus à destination de l'Iran
  - http://securityaffairs.co/wordpress/2725/malware/stopped-antivirus-for-iran-controversial-penalty.html
- DarkComet utilisé par le gouvernement syrien
  - http://www.gmanetwork.com/news/story/249307/scitech/technology/skype-malware-used-in-syrian-confilct
  - http://resources.infosecinstitute.com/darkcomet-analysis-syria/
  - Et c'est un outil français !
    - http://www.darkcomet-rat.com/
- Social Engineering #win
  - http://www.swtor.com/community/showthread.php?t=329727

Malwares, spam et fraudes

- DFBootKit
  - Un "bootkit" pour Android
    - http://research.nq.com/?p=391

Actualité (francophone)

- Une nouvelle organisation pour l'ANSSI
  - http://www.ssi.gouv.fr/fr/anssi/organisation/
- La FPTI renait
  - http://www.fpti.pro/
- Décès de Pascal Lointier
  - Lazaro Pejsachowicz est élu président du CLUSIF
    - http://www.clusif.fr/
- Une pétition face à l'explosion des "fichiers"
  - http://www.uspsy.fr/Petition-En-2012-sauvons-la-vie.html
- Notification des pertes de données: on y vient
  - Cf. autre présentation du jour

Actualité (francophone)

- Le "livre noir et blanc du logiciel"
  - Conclusion: les éditeurs français sont trop petits
    - http://www.syntec-numerique.fr/Actualites/Syntec-Numerique-publie-le-Livre-Noir-et-Blanc-du-Logiciel
- La taxe sur l'expatriation ("Exit Tax") empêche OVH de se développer au Canada
    - http://www.ovh.com/fr/a696.lettre_ouverte_sarkozy_exit_tax_canada
- La vente forcée de logiciels déclarée illégale
    - http://www.cuifavocats.com/Double-condamnation-de-SAMSUNG-la
- DMP: seulement 100,000 dossiers créés
  - Contre 500,000 attendus
    - http://www.itespresso.fr/e-sante-le-dmp-ne-passe-pas-la-barre-des-100000-inscriptions-51795.html

Actualité (francophone)

- Canopy: un troisième projet de Cloud
  - Mais celui-ci n'est pas "français": Atos + VMWare + EMC
- Une loi pour imposer 8 Mb/s de débit avant 2015
  - Applicable ?
    - http://www.pcinpact.com/news/69004-france-senat-8mbps-debit-minimum.htm
- Une loi pour imposer le "haut débit pour tous"
    - http://www.hautdebitpourtous.telecom.gouv.fr/cahier_des_charges.php
- Nouvelle idée: taxer les FAI pour renflouer la presse écrite
    - http://www.lesechos.fr/entreprises-secteurs/tech-medias/actu/0201909239787-les-quotidiens-proposent-de-taxer-les-acteurs-du-numerique-292071.php
- Surcouf en redressement judiciaire
    - http://www.linformaticien.com/actualites/id/23840/surcouf-en-redressement-judiciaire-six-mois-pour-rebondir.aspx

Actualité (anglo-saxonne)

- La NSA achève de construire le plus gros datacenter du monde
  - … avec un objectif de stockage et de déchiffrement
    - http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1

- FBI: "les hackers sont les plus forts"
  - "… il faut donc être plus offensifs" (!?!)
    - http://thehackernews.com/2012/03/fbi-cyber-chief-says-us-losing-war.html

Actualité (européenne)

- **ACTA: la cour de justice européenne saisie**
  - **Par la commission européenne**
    - **http://www.linformaticien.com/actualites/id/23681/acta-la-cour-de-justice-de-l-ue-va-etre-saisie.aspx**

- **Criminaliser les outils logiciels ?**
  - **http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/884/884601/884601en.pdf**
  - **http://www.infosecisland.com/blogview/20901-EU-Possession-of-Hacking-Tools-to-Become-a-Criminal-Offense.html**

- **Le filtrage des réseaux sociaux interdit par la cour de justice européenne**
  - **http://www.linformaticien.com/actualites/id/23603/la-justice-europeenne-interdit-le-filtrage-sur-un-reseau-social.aspx**

Actualité (européenne)

- **Cisco lutte contre le rachat de Skype par Microsoft**
  - **Demande une interopérabilité avec Skype**
    - **http://www.linformaticien.com/actualites/id/23604/microsoft-skype-cisco-remet-en-cause-l-accord-de-l-ue.aspx**

- **Le Conseil de l'Europe se positionne sur la gouvernance de l'Internet**
    - **http://cidris-news.blogspot.fr/2012/03/strategie-pour-la-gouvernance-de.html**

Actualité (Google)

- Google exploite les failles de Safari pour traquer les internautes
  - "This is a bug, not a feature"
    - http://www.h-online.com/security/news/item/Google-found-evading-Safari-s-privacy-controls-1436587.html
- Google implémente le "Do Not Track" dans Chrome
  - … d'ici la fin de l'année
  - … déjà disponible sous forme d'add-on
    - https://chrome.google.com/webstore/detail/hhnjdplhmcnkiecampfdgfjilccfpfoe/details
- Faille (non publiée) dans Google Wallet
    - http://www.lemondeinformatique.fr/actualites/lire-le-systeme-de-paiement-sans-contact-google-wallet-vulnerable-47758.html

Actualité (Google)

- Nouveautés de Google Docs
  - … dont le support Android
    - http://www.linformaticien.com/actualites/id/23695/nouvelles-fonctions-pour-google-docs.aspx
- Google Assistant pour lutter contre Siri
  - … d'ici la fin de l'année
    - http://techcrunch.com/2012/03/02/2011-was-the-year-of-social-for-google-2012-is-the-year-of-assistant/
- Contrôle fiscal pour Google France
  - Probable redressement de €100 millions
    - http://www.linformaticien.com/actualites/id/24097/google-france-dans-l-il-du-fisc.aspx
- Comment protéger ses data centers ?
  - En éteignant la lumière
    - http://www.wired.com/wiredenterprise/2012/03/google-miner-helmet/

Actualité (Apple)

- Surprise: il n'y a pas que l'application Path qui vole tous vos contacts iPhone
  - Viber, Twitter …
    - http://www.latimes.com/business/technology/la-fi-tn-twitter-contacts-20120214,0,5579919.story
- Le "new iPad" jailbreaké dès sa sortie
    - http://www.zdnet.com/blog/security/new-ipad-jailbroken-on-day-one/10902
- iPhone + Paypal + hardware audio = solution de paiement mobile
  - 2,7% de commission quand même …
    - http://www.linformaticien.com/actualites/id/24072/avec-paypal-here-l-iphone-devient-un-terminal-de-paiement.aspx
- Guide de sécurisation iOS 5
    - http://dsd.gov.au/publications/iOS5_Hardening_Guide.pdf
- Première beta de Mac OS 10.8 "Mountain Lion"
  - La convergence avec iOS est flagrante
    - Signature de code obligatoire, sandboxing, …

Actualité (crypto)

- Pour faire de bonnes clés RSA
  - Il faut un bon générateur d'aléa
  - Ca n'est pas le cas pour 0,4% des clés utilisées sur Internet
    - http://eprint.iacr.org/2012/064.pdf
    - https://freedom-to-tinker.com/blog/nadiah/new-research-theres-no-need-panic-over-factorable-keys-just-mind-your-ps-and-qs
- La NSA sait casser AES
  - (Ou pas)
    - http://www.schneier.com/blog/archives/2012/03/can_the_nsa_bre.html#c726943
- Mozilla rappelle à l'ordre les autorités de certification
  - Et particulièrement celles qui délivrent des certificats d'interception
    - http://blog.mozilla.com/security/2012/02/17/message-to-certificate-authorities-about-subordinate-cas/
- Attaque sur HMAC
    - http://eprint.iacr.org/2012/074
- La crypto quantique progresse
    - http://www.linformaticien.com/actualites/id/23769/ibm-des-progres-de-geant-dans-l-informatique-quantique.aspx

Actualité

- Conférences passées
  - JSSI de l'OSSIR
  - GSDays
  - CanSecWest
  - Concours "pwn2own"
    - La guerre est déclarée entre VUPEN et Google
      - https://twitter.com/#!/cBekrar/status/183184507912994817
      - http://scarybeastsecurity.blogspot.fr/2012/03/on-failings-of-pwn2own-2012.html
    - L'escarmouche s'étend au marché du "0day" dans son ensemble
      - http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/
      - https://www.eff.org/deeplinks/2012/03/zero-day-exploit-sales-should-be-key-point-cybersecurity-debate
- Conférences à venir
  - HES 2012 (à partir de jeudi prochain)

Actualité

- **Source**
  - **http://blogs-images.forbes.com/andygreenberg/files/2012/03/exploitpricechart.jpg**

ADOBE READER	$5,000–$30,000
MAC OSX	$20,000–$50,000
ANDROID	$30,000–$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000–$100,000
MICROSOFT WORD	$50,000–$100,000
WINDOWS	$60,000–$120,000
FIREFOX OR SAFARI	$60,000–$150,000
CHROME OR INTERNET EXPLORER	$80,000–$200,000
IOS	$100,000–$250,000

Actualité

- Sorties logicielles
  - Nessus 5
    - http://www.tenable.com/products/nessus

Actualité

- Microsoft + Google + Netflix = DRM dans HTML5
  - http://dvcs.w3.org/hg/html-media/raw-file/tip/encrypted-media/encrypted-media.html
- Paypal bloque l'argent de RapidGator
  - http://www.linformaticien.com/actualites/id/23798/apres-megaupload-rapidgator.aspx
- The Pirate Bay hébergé dans un réseau de drones volants ?
  - https://thepiratebay.se/blog/210
- Une erreur de procédure contre Kim Dotcom
  - … devrait lui permettre de récupérer ses biens
    - http://www.journaldugeek.com/2012/03/19/affaire-megaupload-une-erreur-de-procedure/
- Le créateur de Ruby récompensé par la FSF
  - https://www.fsf.org/news/2011-free-software-awards-announced

Actualité

- Oracle vs. PCI(/DSS)
  - En cause: Oracle ne veut pas communiquer sur ses failles
    - https://blogs.oracle.com/maryanndavidson/entry/pain_comes_instantly1
- Ca va mal pour Yahoo!
  - Licencie
  - Menace d'une guerre des brevets
- Filtrage actif de Tor par la Chine
  - En scannant les nœuds actifs
    - http://arxiv.org/pdf/1204.0447v1.pdf
    - http://www.technologyreview.com/blog/arxiv/27697/
- Le Tadjikistan bloque Facebook
    - http://www.lemonde.fr/technologies/article/2012/03/03/le-tadjikistan-bloque-facebook-et-des-sites-independants_1651575_651865.html

Divers

- Nouveaux challenges
  - http://pastebin.com/QMjRKcgy
  - http://communaute.sstic.org/ChallengeSSTIC2012
  - http://2012.hackitoergosum.org/blog/crypto-challenge
  - http://anssi.santo.fr/
- Le jeu Syndicate embarque une petite annonce de recrutement
  - … destinée aux pirates
    - http://arstechnica.com/gaming/news/2012/02/syndicate-game-files-hide-recruitment-message-aimed-at-pirates.ars
- Google GAG
  - http://code.google.com/p/gag/
- Parmi les meilleurs poissons d'avril …
  - Google Maps 8 bits
    - http://maps.google.com/?t=8&utm_campaign=8bit&utm_source=yt
  - Le projet "E3"
    - http://www.securityvibes.fr/menaces-alertes/wikileaks-e3-google-facebook-publicite/

Divers

- **Stockage dans le Cloud … infini ?**
  - **http://www.bitcasa.com/**
- **Des confettis fabriqués avec des documents confidentiels …**
  - **http://newyork.cbslocal.com/2012/02/08/report-confetti-dropped-during-giants-parade-contained-confidential-information/**
- **YouPorn passe à 100% sur Redis**
  - **https://groups.google.com/group/redis-db/browse_thread/thread/77841c595d29f983?pli=1**
- **PHP …**
  - **http://www.reddit.com/r/lolphp/comments/ps6x5/0x0_wat/**

Divers

- Enorme succès pour le Rasperry Pi
  - http://www.raspberrypi.org/
- Tetris en 140 octets de JavaScript
  - https://gist.github.com/1672254
- La "Transparency Grenade"
  - Précision: c'est une œuvre d'art
    - http://www.wired.com/underwire/2012/02/transparency-grenade/
- "NOUVEL ALGORITHME D'ENCRYPTION-DÉSENCRYPTION DYNAMIQUE (INFAILLIBLE)"
  - http://www.cppfrance.com/codes/NOUVEL-ALGORITHME-ENCRYPTION-DESENCRYPTION-DYNAMIQUE-INFAILLIBLE_52476.aspx

Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 15 mai 2012