OSSIR
Groupe Paris

Réunion du 14 février 2012

Revue des dernières vulnérabilités

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

Avis Microsoft

- **Janvier 2012**
  - **7 bulletins, ??? failles**
  - **MS12-001 Faille dans le noyau Windows [1]**
    - **Affecte: Windows (toutes versions supportées, sauf XP SP3)**
    - **Exploit: permet de contourner le SafeSEH**
      - **Seules les applications compilées avec Visual Studio 2003 sont vulnérables**
    - **Crédit: Joshua J. Drake / Accuvant LABS**

Avis Microsoft

- MS12-002 Faille dans Windows Object Packager [1]
  - Affecte: Windows XP et 2003 (toutes versions supportées)
  - Exploit: exécution de code
  - Crédit: Parvez Anwar / Secunia Research

- MS12-003 Faille dans CSRSS [3,1]
  - Affecte: Windows (toutes versions supportées sauf Seven et 2008R2)
    - Versions chinoises, japonaises et coréennes uniquement …
  - Exploit: élévation de privilèges
  - Crédit: Kang Wu / Shenzhen Jowto Research Dep

Avis Microsoft

- MS12-004 Failles dans Windows Media [1,1]
  - Affecte: Windows Media Library et DirectShow
    - Windows (toutes versions supportées sauf Seven SP1 et 2008R2 SP1)
  - Exploit:
    - Exécution de code à l'ouverture d'un fichier MIDI malformé
    - Exécution de code à l'ouverture d'un fichier multimédia malformé
    - https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/windows/browser/ms12_004_midi.rb
  - Crédit:
    - Shane Garrett / IBM X-Force
    - Neel Mehta / Google

- MS12-005 Faille dans Windows Packager [1,1]
  - Affecte: Windows (toutes versions supportées)
  - Exploit:
    - Exécution de code à l'ouverture d'un document Office contenant une application ClickOnce
      - http://www.cc.gatech.edu/~blee303/exploit/ms12-005/MS12-005.ppsx
      - http://packetstormsecurity.org/files/108683
  - Crédit:
    - Yorick Koster / Beyond Security's SecuriTeam Secure Disclosure Program

Avis Microsoft

- **MS12-006 Failles dans SSL/TLS [3,3]**
  - **Affecte: Windows (toutes versions supportées)**
  - **Exploit: attaque "BEAST"**
  - **Crédit: n/d**

- **MS12-007 Failles dans la librairie AntiXSS [3,3]**
  - **Affecte: AntiXSS 3.0 et 4.0**
  - **Exploit: contournement du filtre anti-XSS**
  - **Crédit:**
    - **Adi Cohen / IBM Rational Application Security**

Avis Microsoft

- Prévisions pour Février 2012

- Advisories
  - Q2588513 attaque sur SSL/TLS
    - V2.0: publication du bulletin

Avis Microsoft

- Retour sur des failles antérieures
  - MS11-014
    - http://newsoft-tech.blogspot.com/2012/01/ms11-014-this-is-not-bug-your-are.html
  - MS11-077
    - https://community.qualys.com/blogs/securitylabs/2011/12/02/ms11-077-from-patch-to-proof-of-concept
  - MS11-080
    - http://www.offensive-security.com/vulndev/ms11-080-voyage-into-ring-zero/
  - MS11-100
    - http://blogs.technet.com/b/srd/archive/2011/12/27/more-information-about-the-december-2011-asp-net-vulnerability.aspx
    - Code d'exploitation
      - https://github.com/HybrisDisaster/aspHashDoS
  - Un site d'intérêt
    - https://code.google.com/p/it-sec-catalog/wiki/Exploitation

Avis Microsoft

- **Révisions**
  - **MS11-025**
    - **V4.2: changement dans la logique de détection**
  - **MS11-049**
    - **V2.2: précision sur les produits affectés (y compris les version SQL "Express")**
    - **V2.3: changement dans la logique de détection**
  - **MS11-098**
    - **V1.1: ajout d'un problème connu**
  - **MS11-099**
    - **V1.2: offre une protection combinée avec MS12-006**
  - **MS11-100**
    - **V1.2: publication d'une mise à jour pour Windows 8**
    - **V1.3: correction des clés de BdR et des paramètres d'installation**
  - **MS12-004**
    - **V1.1: explication sur les vecteurs d'exploitation**
    - **V1.2: modification de la sévérité**
  - **MS12-006**
    - **V1.1: correction documentaire**
  - **MS12-007**
    - **V2.0: la librairie AntiXSS est passée en version 4.2.1**
    - **V2.1: ajout d'un problème connu**

Infos Microsoft

- **Sorties logicielles**
  - **Lancement mondial de SQL Server 2012**
    - **Le 7 mars 2012**
      - **http://www.sqlserverlaunch.com/**
  - **Microsoft Private Cloud RC**
    - **A travers System Center 2012 RC**
  - **Office 15 entre en beta privée**
      - **http://www.linformaticien.com/actualites/id/23378/office-15-demarrage-du-programme-d-evaluation.aspx**

Infos Microsoft

- Autre
  - Le directeur du développement Windows Phone part
    - … travailler sur le Kindle d'Amazon
      - http://www.linformaticien.com/actualites/id/23455/amazon-debauche-le-directeur-du-developpement-windows-phone.aspx
  - C++ AMP
    - Programmer les GPU avec Visual Studio 11
      - http://blogs.msdn.com/b/somasegar/archive/2012/02/03/c-amp-open-specification.aspx
  - Microsoft TechDays 2012
    - C'était du 7 au 9 février
      - http://www.microsoft.com/france/mstechdays/
  - Une faille dans WIN32K.SYS en ligne depuis 2 mois
    - Exploitable ?
      - https://twitter.com/#!/w3bd3vil/status/148454992989261824
  - Un "bug" dans .NET Framework x64
      - http://sourceforge.net/mailarchive/message.php?msg_id=28250469

Infos Microsoft

- Windows 8
  - Storage Spaces
    - http://blogs.msdn.com/b/b8/archive/2012/01/05/virtualizing-storage-for-scale-resiliency-and-efficiency.aspx
  - Système de fichiers ReFS (Windows Server uniquement)
    - http://blogs.msdn.com/b/b8/archive/2012/01/16/building-the-next-generation-file-system-for-windows-refs.aspx
  - Le système sera verrouillé par UEFI sur plateformes ARM …
    - http://www.softwarefreedom.org/blog/2012/jan/12/microsoft-confirms-UEFI-fears-locks-down-ARM/
  - Le WiFi sera plus rapide à démarrer
    - http://blogs.msdn.com/b/b8/archive/2012/01/20/engineering-windows-8-for-mobility.aspx
  - Aperçu du magasin embarqué
    - http://www.linformaticien.com/actualites/id/23246/microsoft-devoile-l-experience-sur-le-windows-store.aspx
  - Une beta publique pour la fin du mois

Infos Réseau

- (Principales) faille(s)
  - Support de l'IGMP dans Linux
    - Déni de service
      - http://seclists.org/fulldisclosure/2012/Jan/263

Infos Réseau

- Autres infos
  - Rappel salutaire
    - Si vous ne désactivez pas "SFR WiFi Public" sur votre box …
    - … tout le monde peut utiliser votre adresse IP
      - http://wireless-fr.org/spip.php?article209
  - OVH lance son CDN
    - http://www.ovh.com/fr/cdn/
  - Les IDN en ".fr" vont bientôt ouvrir
    - http://www.afnic.fr/fr/l-afnic-en-bref/actualites/actualites-operationnelles/5658/showOperational/idn-specifications-techniques.html
  - Internet passe à IPv6
    - C'est décidé pour le 6 juin 2012
      - http://www.lemondeinformatique.fr/actualites/lire-la-journee-ipv6-programmee-le-6-juin-2012-47509.html

Infos Unix

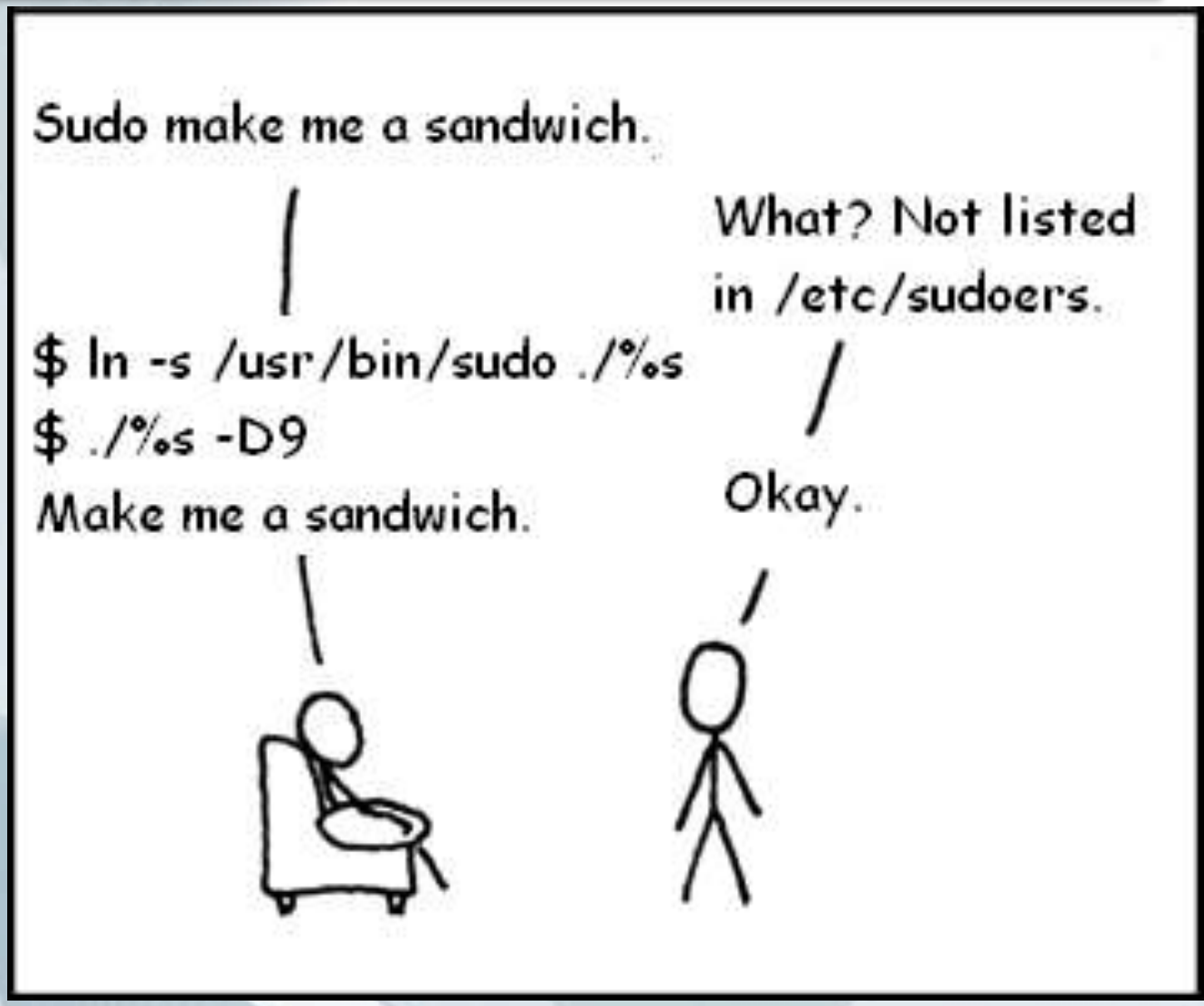
- (Principales) faille(s)
  - PHP < 5.3.9
    - Corrige la faille BEAST et plein d'autres
      - http://www.php.net/ChangeLog-5.php#5.3.9
    - Dont quelques perles
      - https://bugs.php.net/bug.php?id=55475
      - http://cxsecurity.com/research/103
    - Attention à "security.limit_extensions"
      - https://bugs.php.net/bug.php?id=60763
  - PHP < 5.3.10
    - Le correctif induisait une faille de sécurité …
      - http://www.php.net/archive/2012.php#id2012-02-02-1

Infos Unix

- La faille FreeBSD/Telnetd du mois dernier …
  - … est exploitable sur IronPort
    - http://www.flickr.com/photos/mcnail/6668077717/
- /proc/mem en écriture même dans les processus sudo
    - http://git.zx2c4.com/CVE-2012-0056/tree/mempodipper.c
- Ctrl+Alt+* tue tous les économiseurs d'écran X11
    - http://seclists.org/oss-sec/2012/q1/191
    - http://fedoraforum.org/forum/showthread.php?t=275367
- Faille locale dans sudo
  - "Format string" …
    - http://archives.neohapsis.com/archives/fulldisclosure/2012-01/att-0591/advisory_sudo.txt

Infos Unix

- Source: XKCD



Infos Unix

- **Exécution de *commandes* à distance dans gitorious**
  - **http://archives.neohapsis.com/archives/fulldisclosure/2012-01/att-0525/advisory_gitorious.txt**
- **OpenSSL < 0.9.8s, < 1.0.0f**
  - **Attaques variées**
    - **http://www.openssl.org/news/secadv_20120104.txt**
  - **Déni de service via DTLS**
    - **http://www.openssl.org/news/secadv_20120118.txt**
- **Les certificats OpenSSH "legacy" contiennent du "padding" indésirable**
  - **http://www.openssh.com/txt/legacy-cert.adv**

Infos Unix

- **Autre**
  - **Le support Debian 5 est terminé depuis le 6 février**
    - **http://www.debian.org/News/2012/20120209**
  - **Canonical ne supportera plus Kubuntu**
    - **https://lists.ubuntu.com/archives/kubuntu-devel/2012-February/005782.html**
  - **Mozilla aussi se met au "*product metrics*"**
    - **https://bugzilla.mozilla.org/show_bug.cgi?id=718066**

Failles

- **Principales applications**
  - **Adobe Reader < 9.5, < 10.1.2**
    - **6 failles corrigées**
      - **http://www.adobe.com/support/security/bulletins/apsb12-01.html**
    - **… dont la faille "U3D" activement exploitée dans la nature**
      - **http://www.adobe.com/support/security/advisories/apsa11-04.html**
  - **Oracle Quaterly Patch**
    - **78 correctifs**
      - **http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html**
  - **Correctif 2012-001 pour Mac OS X**
    - **1,3 Go de mises à jour pour 10.7.3 …**
      - **http://support.apple.com/kb/HT5130**
    - **Et une mise à jour qui bogue**
      - **Le correctif ImageIO a été supprimé dans la V1.1**
  - **Chrome < 16.0.912.75**
    - **http://googlechromereleases.blogspot.com/2012/01/stable-channel-update.html**

Failles

- ThunderBird < 3.1.11, < 10.0
- FireFox < 3.6.26, < 10.0
  - Des corrections de sécurité ?
    - https://www.mozilla.org/en-US/firefox/10.0/releasenotes/
  - Oui
    - http://www.mozilla.org/security/known-vulnerabilities/firefox36.html#firefox3.6.26
- FireFox < 10.0.1
    - https://www.mozilla.org/en-US/firefox/10.0.1/releasenotes/
- Putty < 0.62
  - Conserve le mot de passe en clair dans la mémoire pendant toute la durée de la session
    - http://lists.tartarus.org/pipermail/putty-announce/2011/000017.html

Failles

- Flash Player sandboxé
  - Disponible en beta pour le moment
  - Nécessite FireFox 4+ et Windows Vista+
    - http://blogs.adobe.com/asset/2012/02/flash-player-sandboxing-is-coming-to-firefox.html
- Adobe se plaint des pirates …
    - http://www.zdnet.com/blog/security/offensive-security-research-community-helping-bad-guys/10228

Failles

- Adobe …

https://twitter.com/#!/manzuik/status/166242945694044161/photo/1

Failles 2.0

- Les systèmes de visioconférence pas forcément bien protégés
  - … et souvent connectés à Internet
    - https://community.rapid7.com/community/solutions/metasploit/blog/2012/01/23/video-conferencing-and-self-selecting-targets
- Le gouvernement allemand distribue les bons points
  - Chrome, Adobe Reader X (vs. 9), Secunia PSI
    - http://www.computerworld.com/s/article/9223957/German_gov_t_endorses_Chrome_as_most_secure_browser
- Oracle DB vulnérable "par conception"
    - http://www.infoworld.com/d/security/fundamental-oracle-flaw-revealed-184163-0
- *Guess what*
  - 97% des pertes de données sont liées à des injections SQL
    - http://news.techworld.com/security/3331283/barclays-97-percent-of-data-breaches-still-due-sql-injection/

Failles 2.0

- Tir groupé sur les SCADA
  - http://threatpost.com/en_us/blogs/state-scada-security-laughable-researchers-say-020312
  - Ca n'est pas forcément faux, ex. Niagara
    - http://reflets.info/scada-lediteur-niagara-a-poil-sur-le-net/
- Ecouter les fréquences de la police
  - Il y a une appli pour ça !
    - https://threatpost.com/en_us/blogs/losing-cops-foot-chase-theres-app-010512
- Twitter
  - … reçoit $300m du prince saoudien Al-Walid Ben Talal
    - http://www.kingdom.com.sa/en/MC_PR_NewsDetails.asp?p=3&ID=904
  - … va se conformer plus strictement aux législations locales
    - http://blog.twitter.com/2012/01/tweets-still-must-flow.html

Sites piratés

- Les sites piratés du mois
  - DreamHost
    - http://blog.sucuri.net/2012/01/dreamhost-security-issue-prompts-ftp-password-resets.html
  - Zappos (racheté par Amazon)
    - 24M comptes piratés
      - http://www.v3.co.uk/v3-uk/news/2137729/amazon-owned-zappos-hit-huge-breach
  - Core Security
    - http://thehackernews.com/2012/01/third-security-breach-at-core-security.html
  - Microsoft Store (Inde)
    - http://www.linformaticien.com/actualites/id/23559/microsoft-store-inde-victime-d-une-cyberattaque.aspx

Sites piratés

- T-Mobile
  - Pas grand-chose
    - http://pastebin.com/HhaPZ1BE
- KPN
  - Ils n'ont pas réussi à mettre les attaquants dehors après une semaine d'efforts …
- usa.gov, cia.gov, …
  - Idem, juste humiliant
    - http://thehackernews.com/2012/02/ciagov-tango-down-fuckfbifriday-by.html
    - http://pastebin.com/1qpUgjKW

Sites piratés

- Foxconn
  - http://thepiratebay.se/torrent/7016541/Foxconn_Leaked___-_Swagg_Security_-
- VeriSign
  - … en 2010 (mais les techniciens avaient omis de prévenir la direction)
    - https://press.verisign.com/easyir/customrel.do?easyirid=AFC0FF0DB5C560D3&version=live&prid=847869&releasejsp=custom_97
  - Potentiellement impacté: DNS racines, interceptions CALEA …
- Une conf'call de 15 minutes entre le FBI et Scotland Yard piratée par Anonymous
  - Sujet: la lutte contre Anonymous …
    - http://thehackernews.com/2012/02/anonymous-hacks-fbi-and-records.html
- Des boites email de dirigeants Syriens (par Anonymous)
  - Mot de passe le plus courant: "12345"
    - http://pastebin.com/uaYDfCz0
    - http://bigbrowser.blog.lemonde.fr/2012/02/07/anonymous-ouvre-les-boites-mails-de-responsables-syriens/

Sites piratés

- Le site officiel de Justin Bieber
  - Note: contrairement aux mails syriens, les mots de passe sont stockés hashés …
    - http://pastebin.com/GpMB15Sy
- Plusieurs services d'infrastructure israéliens
  - Bourse, aéroport, banques, …
  - (Sites Web publics uniquement)
    - http://www.msnbc.msn.com/id/46012902/ns/technology_and_science-security/t/hackers-disrupt-israels-stock-exchange-airline-banks/
- Le cabinet Puckett & Faraj
  - En charge de la défense d'un Marine américain
  - 300 Go de données volées
- Les laboratoires médicaux à poil sur Internet
    - http://www.zataz.com/news/21861/fuite--donnees--patients--laboratoires--analyses--medicales.html

Sites piratés

- **MegaUpload fermé par la justice américaine**
  - **Un impact non négligeable sur le trafic mondial**
    - **http://ddos.arbornetworks.com/2012/01/the-megaupload-shutdown-effect-2/**
    - **http://reflets.info/megaupload-visualisons-la-baisse-de-la-facture-du-transit-des-fai/**
  - **Suites …**
    - **https://www.eff.org/deeplinks/2012/01/eff-requests-information-innocent-megaupload-users**
    - **http://www.maitre-eolas.fr/post/2012/01/23/Quelques-mots-sur-l-affaire-Megaupload**
    - **http://tempsreel.nouvelobs.com/la-fermeture-de-megaupload/20120123.OBS9577/les-concurrents-de-megaupload-paniquent.html**
    - **http://torrentfreak.com/megaupload-alternatives-see-surge-in-traffic-after-shutdown-120126/**
  - **Note: les conversations Skype ont été espionnées**
    - **Comment ?**
      - **http://www.stuff.co.nz/technology/6314435/Dotcom-associates-fears-revealed**

Sites piratés

- **MegaUpload fermé par la justice américaine (suite)**
  - **Et là … c'est la (cyber)guerre !**
    - **http://anonops.blogspot.com/2012/01/internet-strikes-back-opmegaupload.html**
  - **Parmi les victimes françaises:**
    - **Elysee.fr**
    - **Modernisation.gouv.fr**
    - **Rgpp.gouv.fr**
    - **Un syndicat de police**
    - **Hadopi**
    - **…**

Sites piratés

- MegaUpload fermé par la justice américaine (suite)

Sites piratés

- **Symantec #fail**
  - **Finalement Symantec a bien été piraté en 2006**
    - **https://www.computerworld.com/s/article/9223495/Symantec_backtracks_admits_own_network_hacked**
  - **Donc il faut absolument arrêter d'utiliser pcAnywhere**
    - **http://www.reuters.com/article/2012/01/25/us-symantec-hacking-idUSTRE80O1UY20120125**
  - **Parce que:**
    - **Un nom d'utilisateur > 0x108 caractères provoque un "buffer overflow" …**
      - **http://www.zerodayinitiative.com/advisories/ZDI-12-018/**
    - **Le protocole propriétaire utilisé n'est pas sûr**
      - **http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&suid=20120124_00**
    - **Le code source de pcAnywhere a finalement été publié sur Internet**
      - **http://legionnairesawaken.sexyi.am/LegionNET/2012/02/07/symantecs-pcanywhere-leaked-source-code-antisec-anonymous/**
    - **Symantec est prêt à payer $50,000 pour empêcher la diffusion du code source de son antivirus**
      - **http://pastebin.com/GJEKf1T9**

Sites piratés

- Note(s)

  - Toutes les analyses Stratfor sont temporairement gratuites
    - http://stratfor.com/hacking-news

  - L'intrusion chez RSA leur aura coûté $66 millions
    - http://articles.boston.com/2012-01-14/business/30624096_1_computer-security-security-breach-rsa-security

Malwares et spam

- Le pilotage des drones américains passe de Windows à Linux
  - Suite à des infections virales "embarrassantes" …
    - http://www.theregister.co.uk/2012/01/12/drone_consoles_linux_switch/
- Un nouveau cheval de Troie ciblé
  - … qui s'attaque aux dongles ActivIdentity
    - http://thehackernews.com/2012/01/chinese-hackers-deploy-sykipot-trojan.html
- Un policier allemand espionne sa fille avec le BundesTrojan
  - Les amis de sa fille prennent le contrôle du centre de commandement
    - http://www.spiegel.de/netzwelt/netzpolitik/0,1518,807820,00.html
- Il y a des plus en plus de virus sur Mac OS X
  - D'après F-Secure
    - http://www.f-secure.com/weblog/archives/00002300.html

Malwares et spam

- Des auteurs de malwares identifiés
  - Koobface
    - http://www.linformaticien.com/actualites/id/23157/le-groupe-de-pirates-derriere-koobface-identifie.aspx
  - Cutwail
    - https://krebsonsecurity.com/2012/01/pharma-wars-google-the-cutwail-botmaster/
  - Kelihos
    - Géré par un ancien de la société Agnitum
      - http://www.linformaticien.com/actualites/id/23290/un-editeur-d-antivirus-derriere-un-botnet.aspx
    - … ou pas
      - http://www.mag-securs.com/News/tabid/62/articleType/ArticleView/articleId/28891/L-employe-russe-dement-etre-derriere-le-botnet-Kelihos.aspx

Actualité (francophone)

- L'ANSSI a de l'ambition
  - https://twitter.com/#!/ncaproni/status/157415761571356674
  - https://twitter.com/#!/ncaproni/status/165830473057181696
- La loi sur les "outils intrusifs" va être mise à jour
  - Pour intégrer la cybersurveillance
    - http://www.pcinpact.com/news/68829-sgdn-autorisation-vie-privee-informatique.htm
- PIRANET 2012
  - http://www.ssi.gouv.fr/fr/anssi/publications/communiques-de-presse/cyber-attaques-l-exercice-piranet-2012-met-l-etat-a-l-epreuve-d-une-crise.html
- Orange CERT/CC
  - http://www.first.org/members/teams/orange-cert-cc

Actualité (francophone)

- Les risques de la carte bleue sans contact
  - Aucune confirmation en dessous de 20 euros
    - http://www.ladepeche.fr/article/2011/12/12/1237781-les-dangers-de-la-carte-bancaire-sans-contact.html
- Cloud français: l'état va trancher
    - http://www.google.com/hostednews/afp/article/ALeqM5ib4k87qHfHtHOMrvZu-7zzcNKsaQ
- NetAsq rachète EdenWall
    - http://www.securityvibes.fr/marche-business/netasq-rachete-edenwall/
- CS rachète Prélude-IDS
    - http://www.c-s.fr/CS-acquiert-la-solution-Prelude-IDS-dans-le-cadre-de-son-offre-de-cyber-securite_a444.html
- Dassault Systèmes rachète Netvibes

Actualité (francophone)

- **Pôle Emploi fait appel à Google pour géolocaliser les chômeurs**
  - **http://blog.lefigaro.fr/social/2012/02/google-futur-prestataire-de-po.html**
- **HADOPI vs. iPhone**
  - **Le deuxième fait plus que la première pour encourager le téléchargement légal de musique …**
    - **http://www.lemonde.fr/technologies/article/2012/01/24/hadopi-source-de-la-croissance-d-itunes_1633919_651865.html**
- **Le nouveau logo de l'ANSSI disponible en fond d'écran**
  - **Avec un *challenge inside***
    - **http://www.ssi.gouv.fr/fr/anssi/mediatheque/ecran.html**

Actualité (anglo-saxonne)

- L'Internet contre les lois SOPA / PIPA
  - http://sopastrike.com/
- La SEC va imposer la divulgation des intrusions
  - http://www.siliconvalley.com/news/ci_19820870
- Un train piraté
  - http://www.examiner.com/homeland-security-in-chicago/tsa-memo-reveals-railway-computer-hacked
- Il est impossible de défendre le Pentagone contre les cyberattaques
  - Le réseau est trop bordélique ☺
    - http://intelnews.org/2012/01/13/01-908/
- La liste des sites "surveillés"
  - http://cryptome.org/2012/01/0001.pdf

Actualité (européenne)

- Le traité ACTA a été signé

- Nouvelle directive pour la protection des données personnelles en préparation
  - http://www.lemondeinformatique.fr/actualites/lire-protection-des-donnees-l-ue-confirme-le-droit-a-l-oubli-et-les-amendes-47541.html

  - Perte de données: l'amende sera finalement de 2% du CA

  - Intègre le droit à l'oubli

  - La loi du pays de l'entreprise s'appliquerait
  - La CNIL n'est pas pour …
    - http://www.linformaticien.com/actualites/id/23322/bruxelles-dessine-la-nouvelle-protection-des-donnees-critiquee-par-la-cnil.aspx

Actualité (Google)

- Google change ses conditions générales d'utilisation
  - Au moins c'est clair
    - http://www.google.fr/intl/fr/policies/
    - http://www.framablog.org/index.php/post/2012/01/25/google-is-evil
  - Les CNIL européennes ont eu environ 48h pour réagir
    - http://www.zdnet.fr/actualites/confidentialite-google-a-impose-ses-nouvelles-regles-a-la-cnil-39768309.htm
  - Non, ça n'est pas *evil* (d'après Google)
    - http://googlepublicpolicy.blogspot.com/2012/02/busting-myths-about-our-approach-to.html
  - Et le pire … c'est que personne n'en veut
    - http://searchenginewatch.com/article/2145297/Google-Users-Dislike-Personalized-Search-Results-Survey

Actualité (Google)

- Google Bouncer
  - De nouvelles mesures d'analyse statique anti-malware sur Android Market
    - http://googlemobile.blogspot.com/2012/02/android-and-security.html
  - Déjà contournée par la preuve de concept "Rootsmart"
    - http://www.ubergizmo.com/2012/02/newly-discovered-android-malware-could-bypass-google-bouncer/
- Android/Counterclank
  - Un malware, ou une publicité trop agressive ?
    - http://www.symantec.com/security_response/writeup.jsp?docid=2012-012709-4046-99
  - Microsoft s'en donne à cœur joie
    - http://www.slashgear.com/microsoft-revisits-droidrage-bash-android-malware-incident-01211625/
- Google Chrome pour Android
  - 4.0 uniquement
    - https://market.android.com/details?id=com.android.chrome
- OCSP is dead, baby
    - http://www.imperialviolet.org/2012/02/05/crlsets.html

Actualité (Google)

- Google indexe Google+
  - Twitter râle … mais avait refusé d'être indexé
    - http://www.linformaticien.com/actualites/id/23040/google-dans-google-twitter-rale-mais-s-embrouille.aspx
- Google Screenwise
  - Vendre sa vie privée pour $25 ?
- Google Drive en préparation ?
  - Un concurrent direct de DropBox et iCloud
    - http://online.wsj.com/article_email/SB10001424052970204369404577211961645711988-lMyQjAxMTAyMDAwODEwNDgyWj.html
- Google Maps finalement condamné
  - Au bénéfice de Bottin Cartographes
    - http://pro.clubic.com/entreprises/google/actualite-473866-maps-google-condamne-france-abus-position-dominante.html
- Obama fait du Google Hangout
    - http://www.whitehouse.gov/photos-and-video/video/2012/01/30/president-obama-s-google-hangout

Actualité (Apple)

- FileVault 2 "cassé"
  - A travers un accès FireWire
    - http://news.techworld.com/security/3334788/apple-filevault-2-encryption-cracked-by-forensic-software/
- Jailbreak "untethered" pour iPad 2 et iPhone 4S (iOS 5)
    - http://www.linformaticien.com/actualites/id/23233/un-jailbreak-untethered-pour-l-iphone-4s-et-l-ipad-2.aspx
- Une application malveillante sur l'AppStore officiel
  - Aspire tout le carnet d'adresses à la première exécution
    - http://www.pcinpact.com/news/68846-path-application-ios-carnet-contacts.htm
  - Pas vu, pas pris ?

Actualité (Apple)

- Apple devient le 1er fabriquant d'ordiphones au monde
  - http://www.linformaticien.com/actualites/id/23292/apple-devient-le-premier-fabricant-de-smartphones-au-monde.aspx
- Faits
  - L'iPhone génère plus d'argent que le chiffre d'affaires de Microsoft
    - http://www.linformaticien.com/actualites/id/23465/incroyable-le-business-de-l-iphone-depasse-le-chiffre-d-affaires-de-microsoft.aspx
  - La capitalisation boursière d'Apple dépasse Microsoft + IBM réunis
    - http://www.latribune.fr/technos-medias/electronique/20120213trib000682858/l-action-apple-depasse-les-500-dollars.html
- Apple ne veut pas payer la taxe "copie privée"
  - http://www.lesechos.fr/entreprises-secteurs/tech-medias/actu/0201866598736-copie-privee-apple-refuse-de-payer-la-redevance-280589.php
  - En fait personne ne veut payer
    - http://www.linformaticien.com/actualites/id/23478/copie-privee-les-industriels-se-rebiffent.aspx

Actualité (crypto)

- Une collision MD5 sur un bloc
  - http://marc-stevens.nl/research/md5-1block-collision/
- Un injecteur de contenu dans un flux HDCP
  - Ce projet nécessite la clé maitre HDCP mais n'est pas soumis au DMCA
    - http://www.bunniestudios.com/blog/?p=2117
- Le chiffrement des téléphones satellites "cassé"
  - Algorithmes GMR-1 et GMR-2
    - http://gmr.crypto.rub.de/
    - http://cryptanalysis.eu/blog/2012/02/02/dont-trust-satellite-phones-the-gmr-1-and-gmr-2-ciphers-have-been-broken/

Actualité (crypto)

- "Surprise": TrustWave a délivré des certificats SSL d'interception
  - http://blog.spiderlabs.com/2012/02/clarifying-the-trustwave-ca-policy-update.html
  - Du coup Mozilla n'en veut plus
    - https://bugzilla.mozilla.org/show_bug.cgi?id=724929
- Résumé de l'année 2011
  - http://blog.cryptographyengineering.com/2011/12/2011-redux.html
- Cryptome relance la "backdoor du FBI"
  - C'est RSA qui est cassé !
    - http://cryptome.org/2012/01/0032.htm

Actualité

- Conférences passées
  - Microsoft TechDays 2012
- Conférences à venir (inscriptions ouvertes)
  - Insomni'hack 2012
    - 2 mars 2012
      - http://blog.scrt.ch/2012/01/20/insomnihack-2012-le-programme/
  - JSSI
    - 13 mars 2012
      - http://www.ossir.org/jssi/jssi2012/index.shtml
  - GS-Days
    - 3 avril 2012
  - Hackito Ergo Sum
    - 12-14 avril 2012
      - http://hackitoergosum.org/
- Sorties logicielles
  - Maltego 3.1
  - Hydra 7.2

Actualité

- Secunia lance son propre programme d'acquisition de failles
  - http://secunia.com/community/research/svcrp
- Crackmes.de de retour
  - http://crackmes.de/
- Intel rachète RealNetworks
  - http://www.linformaticien.com/actualites/id/23344/intel-rachete-les-technologies-de-realnetworks.aspx
- Facebook va entrer en bourse
  - Les chiffres sont désormais publiés
    - http://www.linformaticien.com/actualites/id/23416/facebook-en-bourse-c-est-parti.aspx
  - Et Mark Zuckerberg fait l'apologie des +hackers+ …
    - http://www.ladepeche.fr/article/2012/02/02/1275945-marc-zuckerberg-expose-sa-vision-d-un-monde-meilleur-quand-il-est-connecte.html

Actualité

- Un nouveau moteur de recherche
  - http://launch.volunia.com/
- Cyberguerre: qui est prêt ?
  - Les USA … mais aussi la France !
    - http://www.3dcommunication.fr/SMR/McAfee/Cyberdefense/Executive%20Summary%20France.pdf
- 1er février: journée mondiale du changement de mot de passe
  - http://pro.01net.com/editorial/554038/comment-choisir-un-mot-de-passe-difficile-a-deviner-mais-facile-a-retenir/
- 7 février: *Safer Internet Day*
  - http://www.internetsanscrainte.fr/le-projet/safer-internet-day-2012-presentation

Divers

- Victoire totale de l'Open Source
  - https://github.com/id-Software
- Parfois il vaut mieux ne pas publier son code source
  - https://github.com/twitter/time_constants/blob/master/lib/time_constants.rb
- Le Web a été inventé en France
  - http://davidgalbraith.org/uncategorized/the-exact-location-where-the-web-was-invented/2343/
- L'invention du mot de passe
  - http://www.wired.com/wiredenterprise/2012/01/computer-password/
- Le caractère Unicode indispensable
  - http://www.fileformat.info/info/unicode/char/1f4a9/index.htm
- Les codes 7xx pour HTTP
  - https://github.com/joho/7xx-rfc
- Un CLUF très clair
  - https://addons.mozilla.org/en-US/firefox/addon/screenshot-pimp-screengrab-scr/privacy/

Questions / réponses

- Questions / réponses
- Conférence JSSI le 13 mars 2012
  - Inscriptions ouvertes !
    - http://www.ossir.org/jssi/jssi2012/index.shtml
- Prochaine réunion
  - Mardi 10 avril 2012