OSSIR
Groupe Paris

Réunion du 11 septembre 2012

Revue des dernières vulnérabilités

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

Avis Microsoft

- **Juillet 2012**
  - **MS12-043 Correctif pour MS-XML [1]**
    - **Affecte: Windows (toutes versions supportées sauf Core)**
      - **MS-XML 3.0 / 4.0 / 6.0 sont mis à jour**
      - **Correctif pour MS-XML 5.0 publié ultérieurement**
        - **(livré avec Office 2003 et 2007, entre autres)**
    - **Exploit: exploité dans la nature dans le cadre d'attaques ciblées**
    - **Crédit:**
      - **Google Security Team**
      - **Qihoo 360 Security Center**
  - **MS12-044 Correctif cumulatif pour IE (x2) [1]**
    - **Affecte: IE 9**
    - **Exploit: corruption mémoire conduisant à l'exécution de code**
      - **http://krash.in/ie9-attr.html**
    - **Crédit:**
      - **Jose A. Vazquez / spa-s3c.blogspot.com + iDefense**
      - **Omair + iDefense**

Avis Microsoft

- MS12-045 Correctif pour MDAC [1]
  - Affecte: Windows (toutes versions supportées sauf Core)
    - MDAC 2.6 et 6.0
  - Exploit: corruption mémoire conduisant à l'exécution de code
  - Crédit: anonymous / ZDI-12-158

- MS12-046 "DLL Preloading" avec VBA [1]
  - Affecte: Office (toutes versions supportées sauf Mac et Viewer)
  - Exploit: exploité dans la nature dans le cadre d'attaques ciblées
    - http://www.symantec.com/connect/blogs/targeted-attacks-exploit-vba-vulnerability-july-ms-tuesday
  - Crédit: Bai Haowen / Huawei Security Labs

Avis Microsoft

- MS12-047 Failles noyau (x2) [1]
  - Affecte: Windows (toutes versions supportées)
  - Exploit:
    - Exécution de code par un layout clavier malformé
    - http://www.exploit-db.com/exploits/18894/
    - Faille Win32k.sys lors de la création d'un hook
  - Crédit:
    - Nicolas Economou / Core ST
    - Qihoo 360 Security Center
    - Lufeng Li / Neusoft Corporation

- MS12-048 Faille dans la gestion des noms de répertoires malformés [1]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: exécution de *commandes* via un fichier ou répertoire contenant des caractères invalides
    - http://blog.watchfire.com/wfblog/2012/07/microsoft-windows-shell-command-injection-1.html
  - Crédit: Adi Cohen / IBM Security Systems

Avis Microsoft

- MS12-049 Attaque "BEAST" sur SChannel et Crypto-NG [3]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: déchiffrement du trafic réseau si le mode CBC est utilisé
  - Crédit: n/d

- MS12-050 Failles SharePoint (x6) [1]
  - Affecte: SharePoint, InfoPath, Groove Server, Office Web Apps …
  - Exploit:
    - Faille dans le filtre HTML
    - XSS dans scriptresx.ashx
    - Fuite d'information dans les "Search Scopes"
    - Redirection arbitraire
    - XSS (x2)
  - Crédit:
    - Adi Cohen / IBM Security Systems
    - Yang Yang / Salesforce.com Product Security Team

Avis Microsoft

- **MS12-051 Faille dans Office 2011 pour Mac [1]**
  - **Affecte: Office 2011 (Mac)**
  - **Exploit: permission de répertoire incorrecte permettant à un autre utilisateur d'injecter un exécutable**
  - **Crédit: n/d**

Août 2012

- **MS12-052 Correctif cumulatif pour IE (x4) [1]**
  - **Affecte: IE (toutes versions supportées)**
  - **Exploit: corruption mémoire pouvant conduire à l'exécution de code**
  - **Crédit:**
    - **GWSlabs + iDefense**
    - **Derek Soeder + Beyond Security**
      - **http://seclists.org/bugtraq/2012/Aug/113**
    - **Sung-Ting Tsai & Ming-Chieh Pan / Trend Micro**
    - **Cris Neckar / Google**

Avis Microsoft

- MS12-053 Faille dans RDP [2]
  - Affecte: Windows XP SP3
  - Exploit: exécution de code à distance avant authentification
  - Crédit: Edward Torkington / NCC Group

- MS12-054 Faille dans des composants réseau (x4) [1]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: failles d'implémentation dans Remote Administration Protocol (RAP) pouvant conduire à l'exécution de code
    - http://blogs.technet.com/b/srd/archive/2012/08/14/ms12-054-not-all-remote-pre-auth-vulnerabilities-are-equally-appetizing-for-worms.aspx
    - DoS, stack overflow, heap overflow, format string (!)
      - http://msdn.microsoft.com/en-us/library/cc240190(v=prot.13).aspx
      - ftp://ftp.microsoft.com/developr/drg/CIFS/cifsrap2.txt
  - Crédit: Yamata Li / Palo Alto Networks (x4)

Avis Microsoft

- **MS12-055 Faille dans WIN32K.SYS [1]**
  - **Affecte: Windows (toutes versions supportées)**
  - **Exploit: élévation de privilèges locale**
  - **Crédit: Matthew Jurczyk / Google**

- **MS12-056 Faille JScript/VBScript [2]**
  - **Affecte: JScript/VBScript 5.8 sur toutes les versions 64 bits de Windows**
  - **Exploit: "integer overflow" pouvant conduire à l'exécution de code**
  - **Crédit: Cris Neckar / Google**

Avis Microsoft

- MS12-057 Faille Office [3]
  - Affecte: Office 2007 / 2010
  - Exploit: exécution de code à l'ouverture d'un fichier CGM malformé
  - Crédit: Andrei Costin
    - http://andreicostin.com/index.php/brain/2012/08/15/acsa_2012_16_microsoft_office_cgm_images

- MS12-058 Failles dans Exchange Server WebReady Document Viewing (x3) [1]
  - Affecte: Exchange 2007 / 2010
    - En fait 13 failles affectant Oracle Outside In
    - http://www.oracle.com/fr/technologies/embedded/025613.htm
  - Exploit: exécution de code sur le serveur lors du transcodage d'une pièce jointe depuis OWA
  - Crédit: Will Dorman / CERT-CC

Avis Microsoft

- **MS12-059 Faille Visio [1]**
  - **Affecte: Visio 2010, Visio Viewer 2010**
  - **Exploit: exécution de code à l'ouverture d'un fichier DXF malformé**
  - **Crédit: Alexander Gavrun + ZDI-12-143**

- **MS12-060 Faille dans MSCOMCTL.OCX [1]**
  - **Affecte: Office, SQL Server, Commerce Server, Host Integration Server, Visual FoxPro, VB6 Runtime …**
  - **Exploit: exécution de code au travers du contrôle ActiveX**
    - **http://bbs.pediy.com/showthread.php?t=154830**
    - **http://blogs.technet.com/b/srd/archive/2012/08/14/ms12-060-addressing-a-vulnerability-in-mscomctl-ocx-s-tabstrip-control.aspx**
  - **Crédit: n/d**

Avis Microsoft

- **Advisories**
  - **Q2661254 Taille de clé minimale pour les certificats: 1024 bits**
    - V1.0: publication de l'avis
    - V1.1: correction documentaire
  - **Q2269637: "DLL Preloading"**
    - V17.0: publication d'un nouveau bulletin
  - **Q2719615 Faille MS-XML**
    - V2.0: publication du bulletin
  - **Q2719662 Faille dans la gestion des Gadgets de bureau**
    - V1.0: publication (en prévision de la conférence BHUS: "We Have You By The Gadgets")
  - **Q2728973 Mise en liste noire de certificats potentiellement trop faibles**
    - V1.0: publication de l'avis
    - V1.1: correction de la date d'application
  - **Q2737111 Faille dans Exchange et FAST Search Server 2010**
    - V1.0: publication de l'avis (lié à un composant Oracle)
    - V1.1: correction documentaire dans le workaround
    - V2.0: publication du bulletin pour Exchange
  - **Q2743314 Faille de conception dans le protocole MS-CHAPv2**
    - V1.0: publication de l'avis

Avis Microsoft

- **Prévisions pour Septembre 2012**
  - **2 bulletins "importants"**
    - **Elévation de privilèges dans Visual Studio 2010 TFS**
    - **Elévation de privilèges dans SMS 2003 et SCCM 2007**

- **Failles antérieures**
  - **Metasploit: code d'exploitation pour MS10-104**
    - **Faille SharePoint 2007**
      - **http://packetstormsecurity.org/files/115099**
  - **MS11-050 (faille IE)**
    - **http://0c0c0c0c.com/?p=146**
  - **MS12-016 (faille .NET)**
    - **http://weblog.ikvm.net/PermaLink.aspx?guid=413fa3f3-bb9f-463b-a06c-6b37ac76cf3f**
  - **MS12-024 (WinVerifyTrust)**
    - **http://0c0c0c0c.com/?p=162**
  - **MS12-025 (faille .NET)**
    - **http://weblog.ikvm.net/PermaLink.aspx?guid=b3525cd1-8788-4d6d-b299-4722ddebad94**
  - **MS12-030 = ZDI-12-157**
  - **MS12-034 = ZDI-12-131**
  - **MS12-038 (faille .NET) = ZDI-12-141**
    - **http://weblog.ikvm.net/PermaLink.aspx?guid=10e37c9a-593f-4ff1-bb2c-6f8a152cd8ac**
  - **MS12-039 = ZDI-12-129**
  - **MS12-042 (SYSRET)**
    - **http://repret.wordpress.com/2012/08/25/windows-kernel-intel-x64-sysret-vulnerability-code-signing-bypass-bonus/**
  - **ASP.NET Partial Trust**
    - **http://weblog.ikvm.net/PermaLink.aspx?guid=509710e7-e9ce-4cf4-b7ed-130409a63161**

Avis Microsoft

- **Révisions**
  - **MS11-009**
    - **V2.1: mise à jour documentaire (IE9 n'est pas affecté)**
  - **MS11-044 Faille .NET**
    - **V1.3: changement dans la logique de détection**
  - **MS11-078 Faille .NET**
    - **V1.3: changement dans la logique de détection**
  - **MS11-092**
    - **V1.1: changement dans la logique de détection**
  - **MS11-100 Faille .NET**
    - **V1.6: changement dans la logique de détection**
  - **MS12-004**
    - **V1.3: changement dans la logique de détection**
  - **MS12-013**
    - **V1.1: changement dans la logique de détection**
  - **MS12-016 Faille .NET**
    - **V1.3: changement dans la logique de détection**
  - **MS12-020**
    - **V2.1: changement dans la logique de détection**
  - **MS12-024**
    - **V1.1: changement dans la logique de détection**
  - **MS12-034**
    - **V1.4: changement dans la logique de détection**
  - **MS12-035 Faille .NET**
    - **V2.2: changement dans la logique de détection**

Avis Microsoft

- MS12-036
  - V1.2: ce bulletin ne remplace pas MS11-065
- MS12-043
  - V1.1: changement dans la logique de détection
  - V2.0: publication des correctifs pour XML Core Services 5.0
  - V2.1: mise à jour documentaire (liens de téléchargement)
- MS12-045
  - V1.1: changement dans la logique de détection
  - V1.2: mise à jour documentaire (applicabilité à Windows 7 & 2008R2)
- MS12-050
  - V1.1: diminution du risque associé à la fuite d'information
- MS12-052
  - V1.1: mise à jour documentaire (Windows 8 RC n'est pas affecté)
- MS12-054
  - V1.1: mise à jour documentaire (Server Core)
- MS12-060
  - V1.1: ajout d'un problème connu
  - V1.2: mise à jour documentaire (liste des correctifs remplacés)

Infos Microsoft

- Sorties logicielles
  - .NET 4.5 est Open Source
    - http://blogs.msdn.com/b/dotnet/archive/2012/08/15/announcing-the-release-of-net-framework-4-5-rtm-product-and-source-code.aspx
    - http://referencesource.microsoft.com/netframework.aspx
  - mod_security pour IIS
    - En Open Source sur SourceForge
      - http://blogs.technet.com/b/srd/archive/2012/07/26/announcing-the-availability-of-modsecurity-extension-for-iis.aspx
  - Apercu de la nouvelle version d'Office
    - Windows 8, tactile, Cloud, social, intégration de Skype …
    - Consumer Preview:
      - http://www.microsoft.com/france/office/preview/
      - http://skydrive.live.com/?officebeta=1

Infos Microsoft

- Windows 8 et Windows 2012 "RTM"
  - Sortie le 26 octobre
    - … mais déjà disponibles pour tous en version d'évaluation "90 jours"
  - La migration depuis Windows 7 coûtera €15
    - https://windowsupgradeoffer.com/fr-FR
  - L'interface "Metro" s'appelle désormais "Modern UI"
    - http://www.linformaticien.com/actualites/id/25900/microsoft-abandonnerait-le-nom-metro-pour-sa-nouvelle-interface.aspx
  - Notes: Windows 8 …
    - … intègre nativement Skype (?)
    - … doit être activé immédiatement
    - … prévient Microsoft de toute installation logicielle
    - http://log.nadim.cc/?p=78

Infos Microsoft

- "Azure Web Site"
  - Un concurrent de Google Site ?
    - https://www.windowsazure.com/en-us/pricing/details/#web-sites%20
- "Windows Azure Active Directory" (Developer Preview)
    - http://blogs.msdn.com/b/windowsazure/archive/2012/07/12/announcing-the-developer-preview-of-windows-azure-active-directory.aspx
- Microsoft change de logo (après 25 ans !)

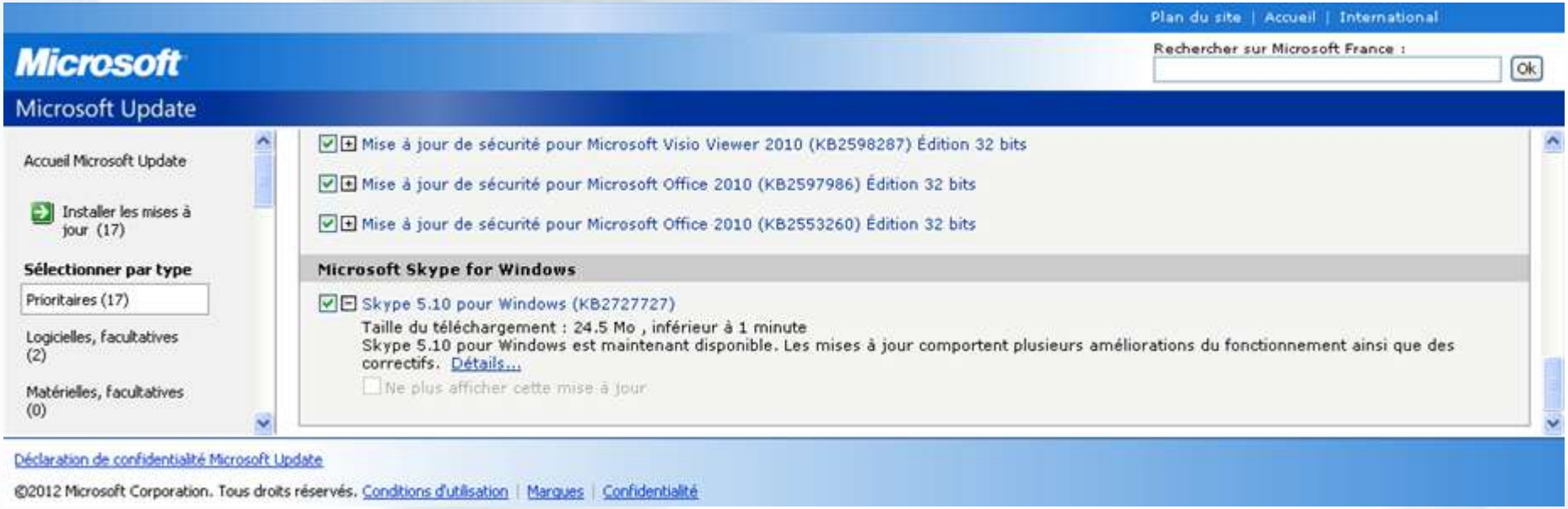
Infos Microsoft

- Autre
  - #define HV_LINUX_GUEST_ID_HI 0xB16B00B5
    - http://korben.info/barbus-et-poilues-ensemble-contre-microsoft.html
  - Microsoft enregistre sa première perte trimestrielle depuis 26 ans
    - … suite à la dépréciation d'une régie publicitaire
  - 14,187 sociétés disposent d'un certificat de signature
    - https://sysdev.microsoft.com/en-us/Hardware/signup/
  - Valve: "Windows 8 sera une catastrophe"
    - Les jeux Valve récents portés sous Linux
      - http://www.geek.com/articles/games/gabe-newell-steam-on-linux-a-response-to-the-coming-windows-8-catastrophe-20120725/
    - … ce qui n'est pas un mauvais choix
      - http://www.pcinpact.com/news/72861-selon-valve-left-4-dead-2-serait-16-rapide-sous-linux-que-sous-windows.htm
  - PC vs. Mac
    - Qui va gagner à moyen terme ?
      - http://www.asymco.com/2012/07/04/the-building-and-dismantling-of-the-windows-advantage/

Infos Microsoft

- Hotmail.com devient Outlook.com
  - http://www.lefigaro.fr/hightech/2012/08/01/01007-20120801ARTFIG00386-pour-rattraper-son-retard-hotmail-devient-outlook.php
  - 6 millions d'inscrits en 1 heure
    - http://www.linformaticien.com/actualites/id/25897/outlook-com-1-million-d-inscrits-en-6-heures.aspx
  - Et le phishing s'organise déjà
    - https://twitter.com/mikko/status/231028464080269313
- Changements dans Windows Live
  - Les mots de passe doivent être complexes …
  - … mais pas plus de 16 caractères (!)
    - http://www.linformaticien.com/actualites/id/25794/microsoft-la-securite-de-windows-live-renforcee.aspx

Infos Microsoft



Infos Réseau

- (Principales) faille(s)
  - N/A

Infos Réseau

- **Autres infos**
  - **"Les Chinois espionnent 80% du trafic mondial au travers de backdoors dans le matériel Huawei et ZTE"**
    - **http://threatpost.com/en_us/blogs/former-pentagon-analyst-warns-china-has-back-doors-global-telcos-071312**
  - **L'Internet ne passera pas sous contrôle de l'ONU**
    - **http://www.linformaticien.com/actualites/id/25904/les-etats-unis-ne-veulent-pas-d-un-internet-controle-par-l-onu.aspx**
  - **Broadcom impose son propre standard WiFi**
    - **… concurrent de l'IEEE pour la 5G WiFi**
      - **http://www.linformaticien.com/actualites/id/25855/broadcom-veut-imposer-le-prochain-standard-du-wifi.aspx**
  - **ZTE aurait violé l'embargo sur l'Iran**
    - **En revendant du matériel américain via une société écran**
      - **http://www.linformaticien.com/actualites/id/25668/zte-dans-le-collimateur-du-fbi.aspx**
  - **Nouvelle panne chez Orange**
    - **"Seulement" 800,000 clients touchés**
  - **Panne du réseau mobile O2 en Angleterre**
    - **Les bracelets électroniques ne fonctionnaient plus …**
      - **http://www.telegraph.co.uk/news/uknews/law-and-order/9396912/O2-network-outage-stopped-G4S-monitoring-criminals-tags.html**

Infos Unix

- (Principales) faille(s)
  - Faille dans Plesk
    - Exploitée en "0day"
      - http://labs.sucuri.net/?note=2012-07-09
  - Faille dans Magento
    - Lecture de fichiers arbitraires via XXE
      - http://seclists.org/fulldisclosure/2012/Jul/154
  - Faille(s) dans Django
      - https://www.djangoproject.com/weblog/2012/jul/30/security-releases-issued/
  - Injection SQL dans le module com_package pour Joomla
      - http://www.vulnerability-lab.com/get_content.php?id=652
  - Plusieurs failles à venir dans la GLIBC
      - http://permalink.gmane.org/gmane.comp.security.oss.general/8159
  - PHP …
      - http://lab.onsec.ru/2012/08/php-multiple-headers-bypass-available.html
      - http://blog.ptsecurity.com/2012/08/not-so-random-numbers-take-two.html
  - ISC-DHCP
    - Les patches ont été "oubliés" …
      - http://lists.debian.org/debian-security-announce/2012/msg00161.html

Infos Unix

- Autre
  - Debian 7 installe Xfce par défaut
    - Au lieu de GNOME
      - http://linux.slashdot.org/story/12/08/08/1455243/debian-changes-default-desktop-from-gnome-to-xfce
  - Décès accidentel de Eugeni Dodonov
    - Développeur de drivers Intel pour Linux
      - http://www.phoronix.com/scan.php?page=news_item&px=MTEzNTk

Failles

- **Publications ZDI (sans date)**
  - **Apple QuickTime**
    - **ZDI-12-125, 130, 135, 136, 153**
  - **Apple Mac OS X**
    - **ZDI-12-137**
  - **Produits SAP**
    - **ZDI-12-138 (Business Objects)**
    - **ZDI-12-139 (Crystal Reports)**
  - **McAfee SmartFilter Administration Server**
    - **ZDI-12-140 (exécution de code via Jboss/RMI)**
  - **EMC AutoStart ftAgent**
    - **ZDI-12-116, 117, 118, 119, 120, 121, 122, 123, 124, 144, 159, 160, 161**
  - **Lotus**
    - **ZDI-12-132, 134, 154**
  - **WebKit**
    - **ZDI-12-147**
  - **Symantec Endpoint Protection (SemSvc.exe)**
    - **ZDI-12-145**
    - **Directory traversal, exécution de commandes, à distance, sans authentification**
  - **Cisco AnyConnect VPN Client**
    - **ZDI-12-156: exécution de programmes arbitraires lors de la mise à jour automatique**
    - **ZDI-12-149: *downgrade* possible vers une version vulnérable**
  - **Failles dans des produits HP publiées en "0day"**
    - **Note: ZDI appartient à HP …**
    - **ZDI-12-126, 127, 162, 163, 164, 165, 166, 170, 171, 172, 173, 174, 175, 176, 177, 178**

Failles

- **Principales applications**
  - **Oracle Quaterly Patch**
    - **88 failles corrigées**
      - **http://www.oracle.com/technetwork/topics/security/cpujul2012-392727.html**
      - **ZDI-12-142 (exécution de commandes via Java Web Start)**
    - **Retour sur février 2012:**
      - **http://weblog.ikvm.net/PermaLink.aspx?guid=cd48169a-9405-4f63-9087-798c4a1866d3**
    - **Retour sur avril 2012:**
      - **ZDI-12-150, 151, 152**
  - **Faille(s) critique(s), non patchée(s), exploitée(s) dans la nature**
    - **Exploitable facilement sous Java < 1.7.7**
      - **http://pastie.org/4594319**
      - **http://contagiodump.blogspot.fr/2012/08/deepend-research-java-7-0-day.html**
      - **https://community.rapid7.com/community/metasploit/blog/2012/08/27/lets-start-the-week-with-a-new-java-0day**
      - **http://scrammed.blogspot.ch/2012/08/analysing-cve-2012-xxxx-latest-java-0day.html**
    - **Faille remontée depuis des mois par Adam Gowdiak**
      - **http://www.pcworld.com/businesscenter/article/261612/oracle_knew_about_currently_exploited_java_vulnerabilities_for_months_researcher_says.html**
      - **http://www.security-explorations.com/en/SE-2012-01-poc.html**
    - **Corrigée rapidement par Oracle**
      - **http://www.oracle.com/technetwork/topics/security/alert-cve-2012-4681-1835715.html**
    - **… et les autres ?**

Failles

- Adobe Flash Player
  - http://www.adobe.com/support/security/bulletins/apsb12-14.html
  - http://www.adobe.com/support/security/bulletins/apsb12-18.html
  - http://www.adobe.com/support/security/bulletins/apsb12-19.html
- Adobe Reader < 10.1.4
  - http://www.adobe.com/support/security/bulletins/apsb12-16.html
  - Voir aussi:
    - http://j00ru.vexillium.org/?p=1175
- Adobe ShockWave
  - http://www.adobe.com/support/security/bulletins/apsb12-17.html

- FireFox & ThunderBird < 15.0.1
  - Corrigent plusieurs failles
    - http://www.mozilla.org/security/known-vulnerabilities/firefox.html
    - Dont ZDI-12-128 (FF < 14.0.1)
  - Note: ThunderBird passe dans la "communauté"
    - https://blog.lizardwrangler.com/2012/07/06/thunderbird-stability-and-community-innovation/

- Exécution de code en JavaScript via un bogue des processeurs Core 2 Duo
  - (Je n'ai pas testé)
    - http://1337day.com/exploits/18984

Failles 2.0

- Les américains diffusent "Thunderstruck" (AC/DC) dans les centrales nucléaires iraniennes
  - Fake ?!?
    - http://www.f-secure.com/weblog/archives/00002403.html
- Exécution arbitraire de *commandes* au travers d'une page Web
  - Via un plugin installé par tous les jeux Ubisoft
    - http://news.ycombinator.com/item?id=4311264
    - http://www.ibtimes.co.uk/articles/368343/20120730/ubisoft-uplay-fix-patch-rootkit.htm
- InstaGram
  - Il est possible de voir toutes les photos d'un utilisateur (s'il en a publié au moins une)
    - http://sourceforge.net/projects/instagramdownlo/
- Kindle Touch < 5.1.1
  - Exécution de commandes sous le compte "root" via une page Web
    - http://www.h-online.com/security/news/item/Security-hole-in-Amazon-s-Kindle-Touch-1642718.html
    - http://www.mobileread.com/forums/showthread.php?t=175368
- RIM ne fabrique pas en Chine à cause des risques de backdoor
    - http://www.washingtontimes.com/news/2012/jul/12/blackberry-eschews-china-security-reasons/

Failles 2.0

- C'est la guerre du HTML5
  - Scission entre le WHATWG et le W3C
- Le patron de OAuth 2.0 jette l'éponge
  - "Ce standard est mauvais"
    - http://news.cnet.com/8301-1023_3-57481166-93/oauth-2.0-leader-resigns-says-standard-is-bad/
- Twitter en panne pendant 2 heures (le 26 juillet)
  - … après Google Talk
- Yahoo! Mail 1.4.4 pour Android n'utilise pas HTTPS
    - http://securitywatch.pcmag.com/none/300005-android-botnet-no-a-much-simpler-flaw-in-yahoo-mail-s-app
- A part ça …
  - Zynga s'effondre en bourse
    - http://www.linformaticien.com/actualites/id/25813/bourse-zynga-s-ecroule.aspx
  - Digg revendu $500,000
    - … alors qu'il avait refusé une offre de Google à $200 millions en 2008

Failles 2.0

- Facebook …
  - … ne vérifie pas les applications soumises par les développeurs
    - Y compris les applications "vérifiées" (!)
    - http://www.guardian.co.uk/technology/2012/aug/13/facebook-developers
  - … vous demande de dénoncer vos amis
    - http://www.nikopik.com/2012/07/facebook-vous-demande-de-denoncer-vos-amis-a-pseudonyme.html
  - … lit vos discussions en ligne
    - http://mashable.com/2012/07/12/facebook-scanning-chats/
  - … contient 8,7% de "faux" profils
    - http://www.bbc.com/news/technology-19093078
  - … perd de l'argent
    - Et divise sa capitalisation boursière par 2

Failles 2.0

- La Power Pwn, une prise pas comme les autres …
  - http://pwnieexpress.com/products/power-pwn
- Un journaliste complètement piraté "dans le Cloud"
  - http://www.emptyage.com/post/28679875595/yes-i-was-hacked-hard
  - http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/
  - Amazon corrige la faille
    - http://www.wired.com/gadgetlab/2012/08/amazon-changes-policy-wont-add-new-credit-cards-to-accounts-over-the-phone/
  - … et Apple aussi
    - http://www.wired.com/gadgetlab/2012/08/apple-icloud-password-freeze/

Sites piratés

- **Les sites piratés du mois**
  - **FormSpring - 28 millions de mots de passe**
    - **Salt + SHA-256**
      - **http://blog.formspring.me/2012/07/urgent-change-your-formspring-password/**
  - **Gamigo - 8 millions**
    - **http://pwnedlist.com/**
  - **Phandroid (forum) - 1 million**
  - **meetOne - 900,000**
    - **http://www.h-online.com/security/news/item/Password-leak-at-meetOne-1652783.html**
  - **Pearl.fr - 730,000**
    - **http://zataz.com/news/22310/piratage--clients--boutique-en-ligne.html**
  - **Yahoo Voices - 450,000**
    - **https://d33ds.co/archive/yahoo-disclosure.txt**
  - **Billabong - 35,000**
    - **http://arstechnica.com/security/2012/07/user-passwords-dumped-in-alleged-billabong-com-hack/**

Sites piratés

- Nvidia (forum)
  - http://www.nvidia.com/content/devzone/index.html
  - http://pastebin.com/G21ytATD
- AMD (forum)
  - http://www.zataz.com/news/22344/amd--hack--bdd-leak.html
- Reuters (blogs, x3)
  - En lien avec la guerre en Syrie ?
    - http://www.scmagazineuk.com/reuters-hacked-for-the-third-time-this-month/article/254846/
- Plein de sites israéliens
  - http://rememberemad.com/list.htm

Sites piratés

- Le réseau interne de l'Elysée
  - … par des "alliés" …
  - … d'un très bon niveau technique
    - http://www.letelegramme.com/ig/generales/france-monde/france/cyber-attaques-l-elysee-pirate-a-deux-reprises-avant-l-intronisation-de-hollande-11-07-2012-1769862.php
- Saudi Aramco (réseau interne)
  - Attaque "idéologique" ayant causé de gros dommages (plus de 30,000 systèmes "effacés")
    - http://zataz.com/news/22343/attack--petrole---hack--Saudi-Arabian-Oil-Co--Saudi-Aramco.html
- 12 million de comptes Apple (incluant UDID)
  - Piratés sur le PC d'un agent du FBI ?
    - http://pastebin.com/nfVT7b0Z
    - http://yro.slashdot.org/story/12/09/04/1241258/anonymous-leaks-1m-apple-device-udids
- fbiacademy.edu
    - http://zataz.com/news/22393/fbiacademy.edu--hacked--piratage--nullcrew.html
- BitFloor
  - $250,000 volés
    - http://bitcoinmagazine.net/bitfloor-hacked-250000-missing/

Sites piratés

- data.gov.uk
  - http://zataz.com/news/22367/Null-crew--anonymoous--hack--data--data.gov.uk.html
- Injection SQL sur "bull.fr"
  - http://www.zataz.com/news/22347/fawzi--hacker--audit--alegrien.html
- "Une société de crédit française" rançonnée
  - http://www.zataz.com/news/22348/rancon--maitre-chanteur--piratage--pirate.html
- Le Figaro stocke les mots de passe dans l'URL des commentaires
  - "A cause de Drupal"
    - http://plus.lefigaro.fr/note/faille-de-securite-mon-figaro-les-explications-techniques-20120711-1036803

Sites piratés

- Un APT observé à la loupe
  - http://www.bloomberg.com/news/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor.html
  - Avec une belle infographie
    - http://go.bloomberg.com/multimedia/china-hackers-activity-logged-reveals-multiple-victims-worldwide/
- Les pirates de l'opérateur coréens "KT" arrêtés
  - http://www.linformaticien.com/actualites/id/25850/deux-hackers-s-emparent-de-8-7-millions-de-donnees-de-l-operateur-coreen-kt.aspx
- Anonymous
  - … vs. Somalie
    - http://slashdot.org/submission/2166657/anonymousiwot-somaleaks-
  - … vs. AAPT (fournisseur australien)
    - http://cyberwarzone.com/cyberwarfare/breaking-news-anonymous-opaustralia-releases-aapt-leaked-files-internet
- De nombreux (nombreux, nombreux) autres sites
  - http://pastebin.com/BuabHTvr

- En résumé …
  - https://s3.amazonaws.com/infographics/Worst-IT-Security-Breaches-800.png
  - http://neirajones.blogspot.fr/2012/08/infographic-social-media-side-of.html?spref=tw

Malwares, spam et fraudes

- De nombreuses attaques au Moyen Orient
  - "Gauss"
    - http://www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_and_ITU_Discover_Gauss_A_New_Complex_Cyber_Threat_Designed_to_Monitor_Online_Banking_Accounts
  - "Crisis"
    - Supporte Windows, Mac OS X et Windows Mobile
    - S'injecte dans les machines virtuelles
      - http://www.symantec.com/connect/blogs/crisis-windows-sneaks-virtual-machines
  - "Shamoon"
    - http://www.securelist.com/en/blog/208193786/Shamoon_the_Wiper_Copycats_at_Work
    - http://www.infosecurity-magazine.com/view/27756/shamoon-too-buggy-to-be-statesponsored/
  - "Mahdi"
    - https://www.securelist.com/en/blog/208193677/The_Madi_Campaign_Part_I
    - Outils utilisé: PowerPoint + backdoor en Delphi + UPX
    - Même l'Iran indique pouvoir faire mieux …

Malwares, spam et fraudes

- Analyse d'un cheval de Troie vendu par FinFisher au Bahrain
  - https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/
- Attaque "High Roller" contre les clients fortunés
  - L'ENISA indique que les banques ne protègent pas assez leurs clients
    - http://www.enisa.europa.eu/media/press-releases/eu-cyber-security-agency-enisa-201chigh-roller201d-online-bank-robberies-reveal-security-gaps
- ESET vs. DAVFI
  - "n'oublions pas qu'un code ouvert permet à toute personne, éventuellement malveillante, d'identifier et exploiter des failles potentielles"
    - http://www.generation-nt.com/davfi-antivirus-open-source-reaction-eset-actualite-1600911.html
- Le français à l'origine de DarkComet dans Wired
  - http://www.wired.com/wiredenterprise/2012/07/dark-comet-syrian-spy-tool/
- Google rachète VirusTotal
  - http://blog.virustotal.com/2012/09/an-update-from-virustotal.html

Actualité (francophone)

- **Rapport Bockel sur la CyberDéfense**
  - http://www.senat.fr/notice-rapport/2011/r11-681-notice.html
  - **Le point de vue des chinois**
    - http://www.lepoint.fr/chroniqueurs-du-point/guerric-poncet/cyberdefense-les-geants-chinois-repliquent-au-rapport-bockel-30-07-2012-1491061_506.php

- **Publication(s) ANSSI**
  - **Sécurité de la virtualisation**
    - http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail/problematiques-de-securite-associees-a-la-virtualisation-des-systemes-d.html
  - **Sécurité GNU/Linux**
    - http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/recommandations-de-securite-relatives-a-un-systeme-gnu-linux.html

- **Activité de la CNIL**
  - **Record de plaintes à la CNIL en 2011 (5,738 plaintes déposées)**
    - http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/RA2011_CNIL_FR.pdf
  - **La CNIL condamne un employeur qui refusait l'accès d'un salarié à ses données**
    - http://www.netpme.fr/nouvelles-technologies/2287-cnil-condamne-employeur-qui-refusait-acces-salarie-ses-donnees.html
  - **CNIL vs. FNAC (qui conserve le numéro de CB en clair …)**
    - http://www.linformaticien.com/actualites/id/25869/conservation-des-donnees-la-fnac-avertie-par-la-cnil.aspx
  - **La CNIL s'intéresse à Google Street View**
    - http://www.cnil.fr/nc/la-cnil/actualite/article/article/street-view-la-cnil-demande-a-examiner-les-donnees-conservees-par-google/

Actualité (francophone)

- Les plans du palais de l'Elysée volés
  - Stockés sur une clé USB non chiffrée …
  - … par le prestataire qui installe la vidéosurveillance
    - http://bigbrowser.blog.lemonde.fr/2012/08/21/oups-on-a-vole-les-plans-du-palais-de-lelysee/
- Les outils de "captation" soumis à autorisation du SGDN
    - http://www.pcinpact.com/news/68829-sgdn-autorisation-vie-privee-informatique.htm
- Plusieurs sites gouvernementaux sous Drupal ont pour mot de passe "password"
  - Depuis 2 ans …
    - http://pro.01net.com/editorial/572055/la-securite-des-sites-internet-du-gouvernement-est-a-revoir/
- Grandes manœuvres dans le Cloud français
  - Gandi vs. Andromède
    - http://www.silicon.fr/stefan-ramoin-gandi-entretien-76494.html
  - SFR + Bull + CdC = Numergy
    - http://www.numergy.com/
  - Orange + Thalès + CdC = CloudWatt
    - http://cloudwatt.fr/

Actualité (francophone)

- CNIL vs. Open Data vs. Safe Harbor vs. …
  - Affaire "notrefamille.com"
    - http://www.rfgenealogie.com/s-informer/infos/archives/appel-gagnant-pour-les-archives-du-cantal
- HADOPI: toujours pas de budget pour 2013
    - http://www.linformaticien.com/actualites/id/25568/hadopi-pas-de-budget-2013-pour-le-moment.aspx
- Nouvelle version de risques.gouv.fr
- La vente liée est finalement légale
    - http://www.zdnet.fr/actualites/vente-liee-la-vente-de-windows-avec-un-pc-n-est-pas-deloyale-39774129.htm

Actualité (anglo-saxonne)

- Un texte controversé sur le contrôle des moyens de communication en cas d'urgence
  - http://www.theverge.com/2012/7/10/3149831/obama-national-security-emergency-preparedness-internet-order
- Apple, Microsoft, Google, Cisco … stockent $1,000 milliards dans des paradis fiscaux
  - … dont $891 milliards pour Apple
    - http://www.infodsi.com/articles/134552/pactole-geants-high-tech.html
- HP vs. Oracle
  - Oracle condamné à assurer le support de ses produits sur plateforme Itanium

Actualité (européenne)

- **Microsoft à nouveau attaqué par la commission européenne**
  - **Les utilisateurs de Windows 7 SP1 n'ont pas eu droit au "Ballot Screen"**
    - **http://www.microsoft.com/en-us/news/press/2012/Jul12/07-17statement.aspx**
- **La commission européenne lance une consultation sur la cyber-sécurité**
    - **http://www.clubic.com/antivirus-securite-informatique/cyberpolice/actualite-503076-cyberdefense-europe.html**
- **Homogénéiser les licences musicales en Europe ?**
    - **http://www.linformaticien.com/actualites/id/25658/l-ue-veut-encourager-les-plateformes-musicales-paneuropeennes.aspx**
- **Les administrations allemandes autorisées à vendre leurs données aux entreprises privées ?**
    - **http://www.bulletins-electroniques.com/actualites/70608.htm**
- **Le nouveau *board* de l'ENISA**
    - **http://www.enisa.europa.eu/media/press-releases/30-nouveaux-specialistes-de-la-cyber-securite-nommes-pour-le-groupe-dexperts-permanent-de-lagence-europeenne-enisa**
    - **https://www.enisa.europa.eu/about-enisa/structure-organization/psg/members**

Actualité (Google)

- **Android 4.1**
  - Publié en Open Source
  - Nouveautés:
    - PIE
    - RELRO
    - dmesg_restrict
    - kptr_restrict
    - http://source.android.com/tech/security/index.html
- **Flash n'est plus disponible sur Android**
  - Depuis le 15 août
- **Mise à jour du moteur d'indexation Google**
  - Incluant "Knowledge Graph"
- **Google+ for Enterprise**
  - En test chez les utilisateurs Google Apps jusqu'à fin 2013
- **"Pwnium 2"**
  - $2 million à distribuer lors de HITB 2012
    - http://blog.chromium.org/2012/08/announcing-pwnium-2.html

Actualité (Google)

- Google Chrome Linux
  - L'utilisateur des désormais notifié de l'installation de nouveaux plugins
    - https://chromiumcodereview.appspot.com/10821042/
- Google Chrome 21
    - http://threatpost.com/en_us/blogs/google-chrome-21-fixes-six-high-risk-vulnerabilities-073112
  - … sandboxe Flash sur toutes les versions de Windows
  - … permet de contrôler la caméra, le micro et le gamepad
- Google utilise Ubuntu en interne
    - http://www.zdnet.com/the-truth-about-goobuntu-googles-in-house-desktop-ubuntu-linux-7000003462/

Actualité (Google)

- L'algorithme CityHash64 complètement cassé
  - https://twitter.com/taviso/statuses/229899266116694016
- Marissa Mayer passe de Google à Yahoo
  - Elle était numéro 3 chez Google
  - Première mesure: la cantine gratuite ☺
    - http://www.linformaticien.com/actualites/id/25859/marissa-mayer-googlifie-yahoo.aspx
- Google rachète Sparrow
  - Une start-up française ☺
- YouTube permet désormais de "flouter" les visages
- Google demande $4 millions de dédommagement à Oracle
  - http://www.wired.com/wiredenterprise/wp-content/uploads//2012/07/Google-Expenses-Motion.pdf
- Google condamné à $22 million d'amende par la FTC
  - … pour avoir exploité Safari
    - http://tech.slashdot.org/story/12/07/11/141201/ftc-reportedly-fining-google-225-million-over-safari-privacy-abuse

Actualité (Apple)

- Sortie de Mac OS X "Mountain Lion" (10.8)
  - Et quelques critiques sur la vie privée …
    - http://nakedsecurity.sophos.com/2012/07/30/apple-to-mountain-lion-users-tell-us-who-your-friends-are-if-you-want-to-talk-to-us/
- iPhone: le PIN est stocké dans un keychain
    - http://www.h-onlineg.com/security/news/item/Researchers-criticise-the-iPhone-s-PIN-storing-practice-1644874.html
- Un malware sur l'AppStore
  - "Find & Call"
    - http://www.lemonde.fr/technologies/article/2012/07/06/un-premier-cas-de-virus-informatique-sur-l-app-store-d-apple_1730134_651865.html
- La sécurité de l'AppStore se contourne par un *man-in-the-middle* SSL
    - http://thehackernews.com/2012/07/app-store-bypassed-by-russian-hacker.html
- XSS dans iOS
  - Via l'entête Content-Disposition
    - http://www.laplinker.com/2012/07/xss-in-iphone-ios.html

Actualité (Apple)

- Apple, plus grosse capitalisation boursière de tous les temps ?
  - Pas tout à fait à $ constant
- Apple gagne en première instance contre Samsung
  - > $1 milliard de dommages et intérêts …
- Apple rachète AuthenTec
  - Spécialiste de l'authentification biométrique
    - http://www.linformaticien.com/actualites/id/25833/apple-achete-authentec-pour-356-millions-de.aspx
- Sortie de l'iPhone 5 / iOS 6 prévue le 12 septembre

Actualité (crypto)

- Amélioration des attaques sur les certificats utilisant le même P (ou le même Q)
  - https://factorable.net/weakkeys12.conference.pdf
  - https://factorable.net/keycheck.html
- Une puce quantique sur silicium
  - http://www.lemondeinformatique.fr/actualites/lire-une-puce-quantique-sur-silicium-devient-realite-50269.html
- TLS-SRP dans Apache
  - https://issues.apache.org/bugzilla/show_bug.cgi?id=51075
- Les disques chiffrés Seagate FDE.2 n'oublient pas la clé après un redémarrage à chaud
  - https://twitter.com/hdmoore/status/224569475557638144

Actualité

- **Black Hat US + Defcon 2012 (1/4)**
  - https://www.blackhat.com/html/bh-us-12/bh-us-12-archives.html

  - Conférences
    - Explication de la faille SYSRET
      - https://media.blackhat.com/bh-us-12/Briefings/Wojtczuk/BH_US_12_Wojtczuk_A_Stitch_In_Time_Slides.pdf
    - MS-CHAPv2 est mort
      - https://www.cloudcracker.com/blog/2012/07/29/cracking-ms-chap-v2/
    - …mais on le savait depuis l'année dernière
      - http://esec-pentest.sogeti.com/challenge-vpn-network/decipher-mppe-breaking-ms-chap-v2
    - Sécurité Windows 8: encore des failles …
      - http://www.scribd.com/doc/101419359/Blackhat-USA-2012-The-Line-8-Subway-Exploitation-of-Windows-8-Metro-Style-App-Slides
    - … mais ça s'améliore
      - https://media.blackhat.com/bh-us-12/Briefings/M_Miller/BH_US_12_Miller_Exploit_Mitigation_Slides.pdf
    - SAP, encore attaqué …
      - https://media.blackhat.com/bh-us-12/Briefings/Polyakov/BH_US_12_Polyakov_SSRF_Business_Slides.pdf

      - DilbertMSG FTW!

Actualité

- **Black Hat US + Defcon 2012 (2/4)**
  - **Conférences (suite)**
    - **Rootkit EFI pour Mac**
      - **http://www.h-online.com/security/news/item/EFI-rootkit-for-Macs-demonstrated-1655108.html**
    - **Cartes d'hôtel "Onity" vs. Arduino**
      - **http://demoseen.com/bhpaper.html**
    - **Android ne vérifie pas les certificats Exchange**
      - **http://arstechnica.com/security/2012/07/spoofing-microsoft-exchange-server-how-to/**
    - **Les terminaux de paiement Verifone vulnérables**
      - **Buffer overflow exploitables depuis un carte de paiement …**
      - **http://arstechnica.com/security/2012/07/german-security-experts-find-major-flaw-in-credit-card-terminals/**
    - **Les protocoles aéronautiques anti-collisions vulnérables**
      - **http://venturebeat.com/2012/07/28/plane-hack/**
    - **Cesar Cerrudo vs. Windows Kernel**
      - **https://media.blackhat.com/bh-us-12/Briefings/Cerrudo/BH_US_12_Cerrudo_Windows_Kernal_Slides.pdf**
    - **Charlie Miller vs. NFC**
      - **http://money.cnn.com/2012/07/26/technology/nfc-hack/index.htm**
    - **Les gadgets de bureau Windows sont dangereux**
      - **https://media.blackhat.com/bh-us-12/Briefings/Shkatov/BH_US_12_Shkatov_Kohlenberg_Blackhat_Have_You_By_The_Gadgets_Slides.pdf**

Actualité

- **Black Hat US + Defcon 2012 (3/4)**
  - **Conférences (suite)**
    - **SCADA #fail (ou SHODAN #win)**
      - **http://ia600505.us.archive.org/30/items/Defcon20Slides/DEFCON-20-Viss-SHODAN.pdf**
    - **Sécurité des téléphones (il y a 20 ans)**
      - **http://ia600505.us.archive.org/30/items/Defcon20Slides/DEFCON-20-Brashars-Exploit-Archaeology.pdf**
    - **Ne lire que le *disclaimer***
      - **https://media.blackhat.com/bh-us-12/Briefings/Jericho/BH_US_12_Jericho_Errata_Slides.pdf**
  - **Outils publiés**
    - **https://github.com/silviocesare/PackageCloneDetection**
    - **https://github.com/iSECPartners/ios-ssl-kill-switch**
    - **https://github.com/ironbee/waf-research**
    - **http://www.pentestit.com/smartphone-pentest-framework/ (financé par la DARPA)**
    - **http://evader.stonesoft.com/**

Actualité

- **Black Hat US + Defcon 2012 (4/4)**
  - **Mais aussi …**
    - **Une fille dans les conférences de sécurité**
      - **http://news.techeye.net/security/sexism-makes-hacker-conferences-a-nightmare**
    - **Une conférence sur la sécurité des centrales nucléaires annulée à la dernière minute**
      - **http://www.darkreading.com/advanced-threats/167901091/security/vulnerabilities/240004520/power-plant-hack-talk-free-tools-pulled-from-def-con-lineup.html**
    - **L'équipe sécurité Apple pas vraiment dans l'esprit**
      - **http://www.crn.com/news/security/240004608/analysis-apple-security-teams-oh-so-brief-black-hat-appearance.htm**
    - **Devinez quoi: la NSA recrute ☺**
      - **http://news.cnet.com/8301-1009_3-57481689-83/nsa-director-finally-greets-defcon-hackers/**
      - **http://www.nsa.gov/careers/dc20/**
    - **Microsoft Blue Hat Prizes**
      - **… et publication de EMET 3.5**
      - **http://www.microsoft.com/security/bluehatprize/**
    - **Pwnie Awards**
      - **http://pwnies.com/winners/**
    - **Crack Me If You Can**
      - **https://contest-2012.korelogic.com/**
    - **Attaque ciblée contre les participants à Black Hat**
      - **http://pastebin.com/BYUbgDAh**

Actualité

- **Defcon**
  - **https://twitter.com/smittyhalibut/status/229331792040194048/photo/1**

Actualité

- Conférences à venir
  - ekoParty
    - Attaque "CRIME" contre SSL/TLS
    - "VGA Rootkit"
      - http://www.ekoparty.org/
  - GreHack 2012
    - http://ensiwiki.ensimag.fr/index.php/GreHack-2012-english
  - Hack.lu
    - http://2012.hack.lu/index.php/Main_Page
  - ASFWS 2012
    - http://2012.appsec-forum.ch/conferences/
  - GS-Days 2013
    - http://www.gsdays.fr/
  - Mobile pwn2own
    - Intègre NFC, SMS, baseband …
    - … et sponsorisé par RIM ☺
      - http://dvlabs.tippingpoint.com/blog/2012/07/20/mobile-pwn2own-2012

Actualité

- Sorties logicielles
  - Metasploit 4.4
  - VMWare WorkStation 9.0
    - Ainsi que VMWare WSX
  - OllyDbg 2.01 (beta 2)
  - Qubes 1.0 final

  - "Facebook Open Source Library"
    - https://github.com/facebook/folly

Actualité

- NIST CMSS (Common Misuse Scoring System)
  - http://csrc.nist.gov/publications/nistir/ir7864/nistir-7864.pdf
- Le patron de Symantec débarqué
  - http://www.linformaticien.com/actualites/id/25810/le-patron-de-symantec-debarque.aspx
- Le logo Anonymous … déposé à l'INPI
  - http://bases-marques.inpi.fr/Typo3_INPI_Marques/getPdf?idObjet=3897981_FMARK-1%2CFMARK-2
- Amazon "Glacier" pour archiver ses données
  - http://www.lemagit.fr/article/archivage-amazon-glacier/11648/1/amazon-glacier-service-archivage-economique-condition-pas-sortir/

Actualité

- Le coût des bugs de sécurité … sujet de thèse
  - http://dl.acm.org/citation.cfm?id=2023459
- Reverse-engineering … d'iris
  - http://www.wired.com/threatlevel/2012/07/reverse-engineering-iris-scans/all/
- Les conditions d'utilisation du Web 2.0 pour les nuls
  - http://tos-dr.info/
- BlackBerry OS 10 repoussé en 2013
  - Il y aura un assistant "à la SIRI"

Divers

- Minecraft poursuivi en justice pour violation de brevet
  - http://notch.net/wp-content/uploads/2012/07/mojang.pdf
- Les bornes d'arcade Atari en HTML5
  - Démo pour IE 10
    - http://atari.com/arcade#!/arcade/atari-promo
- Traitements UTF-8 en SSE4
  - De l'art brut ☺
    - http://woboq.com/blog/utf-8-processing-using-simd.html
- Bill Gates a-t-il volé CP/M ?
  - http://spectrum.ieee.org/computing/software/did-bill-gates-steal-the-heart-of-dos/0

Divers

- La ROM de l'Apple][contient un *easter egg*
  - http://www.nycresistor.com/2012/08/21/ghosts-in-the-rom/
- Une console de jeu Open Source
  - http://www.kickstarter.com/projects/ouya/ouya-a-new-kind-of-video-game-console
- Le Cloud ? Un problème de météo …
  - http://www.citrix.com/English/NE/news/news.asp?newsID=2328309
- What else?
  - http://kim.com/
- Excellent ☺
  - http://securityreactions.tumblr.com/

Divers

- La première photo publiée sur Internet
  - http://gizmodo.com/5924748/heres-the-first-picture-ever-posted-on-the-internet

Divers

- Un aperçu de l'iPhone 5

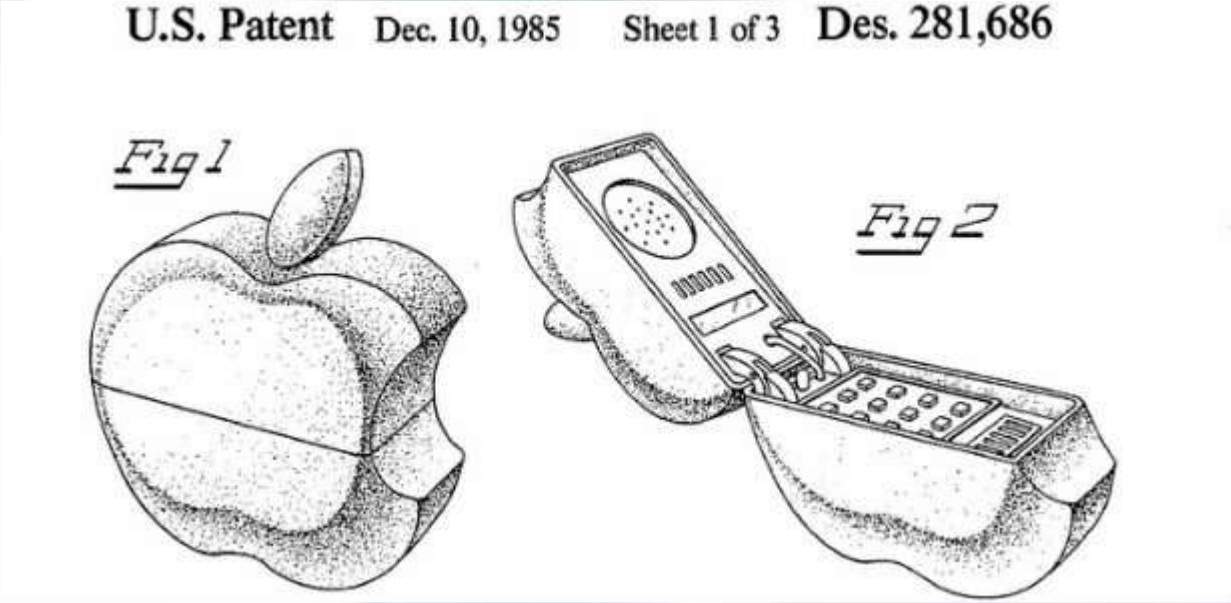

U.S. Patent Dec. 10, 1985 Sheet 1 of 3 Des. 281,686

Fig 1

Fig 2

Divers

- **Surcouf craque**
  - **http://media.surcouf.com/img/crea4.jpg**

Questions / réponses

- Questions / réponses
- Prochain AfterWork
  - Mardi 25 septembre 2012
- Prochaine réunion
  - Mardi 9 octobre 2012
- JSSI
  - Mardi 19 mars 2012