OSSIR
Groupe Paris

Réunion du 8 janvier 2013

Revue des dernières vulnérabilités

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

Avis Microsoft

Décembre 2012

- MS12-077 Correctif cumulatif pour IE (x3) [1]
  - Affecte: IE 9 / 10
  - Exploit: "use after free"
  - Crédit:
    - Rosario Valotta (x2)
      - https://sites.google.com/site/tentacoloviola/
    - Fermin J. Serna / Google (x1)

- MS12-078 Failles dans le noyau Windows (x2) [1]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: élévation de privilèges à l'ouverture d'un fichier OTF ou TTF malformé
  - Crédit:
    - Eetu Luodemaa & Joni Vähämäki / Documill + Chromium Security Rewards Program

Avis Microsoft

- MS12-079 Faille dans le support RTF (x1) [1]
  - Affecte: Office, SharePoint, Web Apps (sauf 2013 et Mac)
  - Exploit: exécution de code à l'ouverture d'un fichier RTF malformé
  - Crédit: anonymous + SecuriTeam

- MS12-080 Failles dans Exchange (x3) [1]
  - Affecte: Exchange 2007 / 2010
  - Exploit:
    - Exécution de code dans le composant Oracle Outside (x2)
    - DoS via un flux RSS
  - Crédit: n/d

Avis Microsoft

- **MS12-081 Faille dans le traitement des noms de fichier (x1) [1]**
  - **Affecte: Windows (toutes versions supportées, sauf 8 / 2012 / RT)**
  - **Exploit: exécution de code au travers d'un nom de fichier malformé**
  - **Crédit: Lucas Apa / IOActive**

- **MS12-082 Faille dans DirectPlay (x1) [1]**
  - **Affecte: Windows (toutes versions supportées, sauf 2008 / 2008R2 / 2012 / RT)**
  - **Exploit: "heap overflow"**
  - **Crédit: Aniway + iDefense**

Avis Microsoft

- **MS12-083 Contournement IP-HTTPS (x1) [1]**
  - **Affecte: Windows 2008 / 2008R2 / 2012**
  - **Exploit:**
    - **Absence de vérification de révocation sur les certificats IP-HTTPS**
    - **Note: IP-HTTPS est utilisé par DirectAccess**
  - **Crédit: n/d**

Avis Microsoft

- Advisories

  - Q2749655 Signature incorrecte
    - V2.0: republication de MS12-043, MS12-057,MS12-059, MS12-060
  - Q2755801 Faille Flash Player dans IE 10
    - V5.0: nouvelle faille
  - Q2794220 Faille IE exploitée dans la nature
    - V1.0: publication du bulletin
    - V1.1: publication d'un workaround

  - Q2798897 Certificat(s) frauduleux émis par TURKTRUST
    - V1.0: publication du bulletin
    - Notes:
      - Mozilla et Google réagissent également
        - http://googleonlinesecurity.blogspot.fr/2013/01/enhancing-digital-certificate-security.html
      - Il est possible de supprimer toutes les CA préinstallées …
        - http://netsekure.org/2010/05/results-after-30-days-of-almost-no-trusted-cas/

Avis Microsoft

- **Prévisions pour Janvier 2013**
  - **2 critiques**
    - **Affecte: Windows 7/2008R2 et ***
  - **5 importants**
    - **Affecte: SCOM 2007, Windows (x4)**

- **Failles à venir**

  - **Contournement UIPI**
    - **… par HWND_BROADCAST**
      - **https://twitter.com/taviso/status/279328380254576642**

  - **Hotmail et Outlook.com**
    - **Fermer la session n'invalide pas le cookie**

  - **Tracking de la souris par IE**
      - **http://iedataleak.spider.io/demo**
      - **http://www.zdnet.fr/actualites/une-faille-dans-internet-explorer-permet-de-suivre-les-mouvements-de-la-souris-39785384.htm**

Avis Microsoft

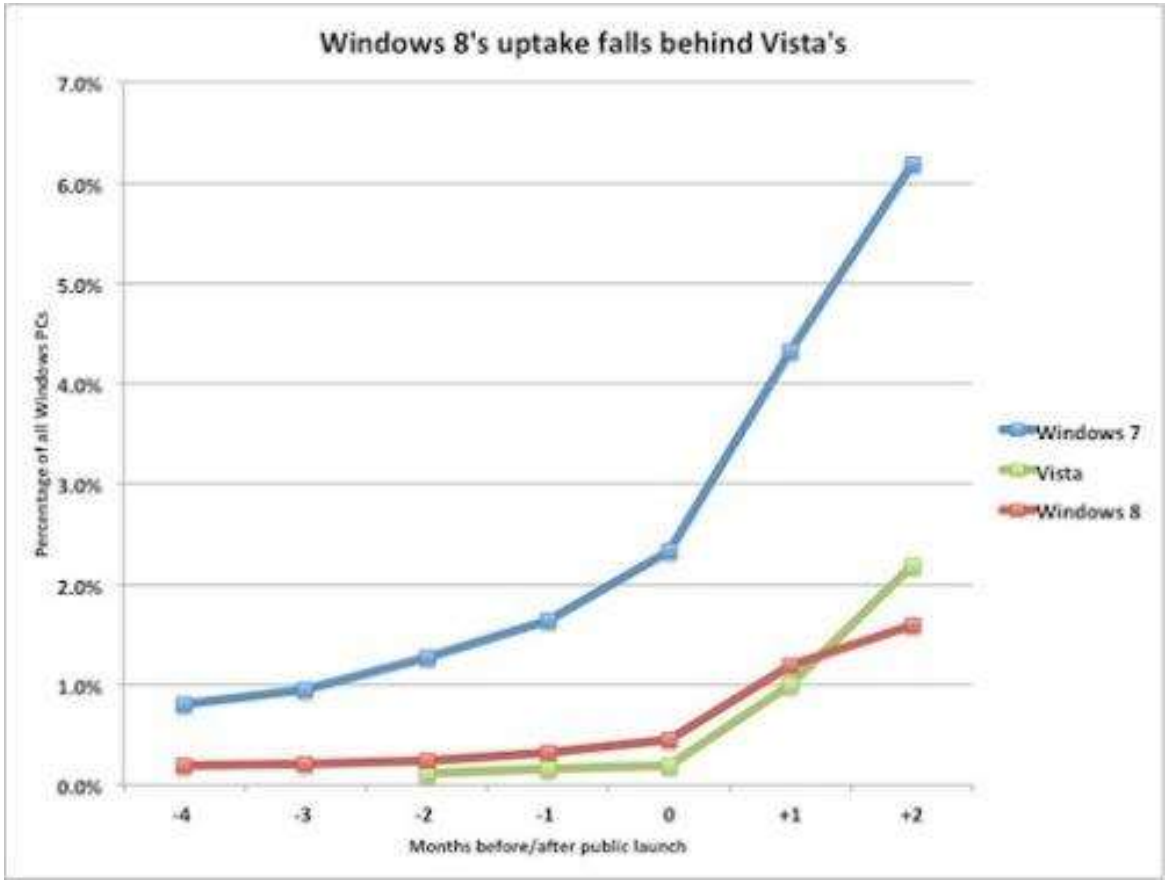
- Révisions
  - MS12-043
    - V4.0: republication du correctif, avec des versions corrigées de MSXML 5.0
  - MS12-050
    - V2.0: publication d'un correctif pour SharePoint Services 2.0
    - V2.1: la mise à jour pour SharePoint Services 2.0 n'est disponible que depuis le Download Center
  - MS12-057
    - V2.0: republication du correctif avec une nouvelle signature
  - MS12-059
    - V2.0: republication du correctif avec une nouvelle signature
  - MS12-060
    - V2.0: republication du correctif avec une nouvelle signature
  - MS12-078
    - V1.1: ajout d'un problème connu
      - http://www.infoworld.com/t/microsoft-windows/buggy-microsoft-patch-causing-fonts-disappear-209207
    - V2.0: republication du correctif
  - MS12-082
    - V1.1: correction documentaire

Infos Microsoft

- **Autre**
  - **Comment obtenir une clé Windows 8 valide gratuitement et légalement ?**
    - **Hack valable jusqu'au 31/01/2013**
      - **http://www.extremetech.com/computing/141052-microsoft-accidentally-gifts-pirates-with-a-free-windows-8-pro-license-key**
  - **Security Essentials ne passe pas AV-Test**
    - **http://www.av-test.org/en/tests/home-user/windows-7/sepoct-2012/**
  - **Microsoft baisse le prix du stockage Azure**
    - **http://blogs.msdn.com/b/windowsazure/archive/2012/12/05/announcing-reduced-pricing-for-windows-azure-storage.aspx**
  - **Lutter contre le "pass the hash"**
    - **C'est pas gagné …**
      - **http://blogs.technet.com/b/security/archive/2012/12/11/new-guidance-to-mitigate-determined-adversaries-favorite-attack-pass-the-hash.aspx**
      - **http://blogs.technet.com/b/trustworthycomputing/archive/2012/12/11/mitigating-targeted-attacks-on-your-organization.aspx**
  - **Publicité en ligne**
    - **Microsoft pourrait revendre Atlas à Facebook**
      - **http://www.linformaticien.com/actualites/id/27335/facebook-et-microsoft-en-negociations-sur-la-pub.aspx**

Infos Microsoft

- **Les ventes de Windows 8**
  - **Source: Net Application**



Infos Réseau

- **(Principales) faille(s)**
  - **WordPress "W3 Total Cache" (plugin) < 0.9.2.5**
    - **http://git.zx2c4.com/w3-total-fail/tree/w3-total-fail.sh**
  - **TWiki < 5.1.3**
    - **Exécution de commandes**
    - **… due à Locale::Maketext**
      - **http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2012-6329**
  - **MyBB < 1.6.9**
    - **Injection SQL**
      - **http://blog.mybb.com/2012/12/14/mybb-1-6-9-security-release/**

Infos Réseau

- **Autres infos**
  - **TCP/IP a 30 ans**
    - **http://www.bortzmeyer.org/tcpip-transition.html**
  - **Debian publie le rapport d'intrusion du 25/07/2012**
    - **"They appeared particularly interested in the password hashes of users from Debian, Intel, Dell, Google, Microsoft, GNU, any .gov and any .edu"**
      - **http://wiki.debian.org/DebianWiki/SecurityIncident2012**
  - **La France ne signe pas le Règlement des Télécommunications Internationales**
    - **Débattu lors de la conférence de l'ITU à Dubaï**
      - **http://www.itespresso.fr/fleur-pellerin-nouveau-traite-telecoms-remet-cause-principes-59982.htmlz**
  - **Sur l'Internet chinois, on saura que vous êtes un chien**
    - **http://www.zdnet.fr/actualites/la-chine-decide-la-fin-de-l-anonymat-sur-internet-39785755.htm**
  - **Free rétablit la neutralité du net …**
    - **… en bloquant les publicités Google ☺**
      - **http://www.pcinpact.com/news/76470-la-freebox-server-se-met-a-jour-1-1-9-arrivee-dun-bloqueur-publicites.htm**

Infos Unix

- **(Principales) faille(s)**
  - **Faille dans grep …**
    - **http://www.openwall.com/lists/oss-security/2012/12/22/1**
  - **RPM < 4.10.2**
    - **Vérification incorrecte des signatures**
      - **http://rpm.org/wiki/Releases/4.10.2**

Infos Unix

- **Autres infos**
  - **GnuTLS pourrait … ne plus être GNU**
    - **http://lists.gnu.org/archive/html/gnutls-devel/2012-12/msg00002.html**
    - **http://lists.gnu.org/archive/html/gnutls-devel/2012-12/msg00003.html**
  - **Paolo Bonzini (mainteneur de sed et grep) quitte le projet GNU**
    - **http://lwn.net/Articles/530460/**
  - **Le 80386 n'est plus supporté par Linux**
    - **http://git.kernel.org/?p=linux/kernel/git/torvalds/linux.git;a=commit;h=743aa456c1834f76982af44e8b71d1a0b2a82e21**
  - **"Stack overflow" dans le support SCSI**
    - **https://patchwork.kernel.org/patch/1751861/**
  - **Linux Kernel 3.7**
    - **… introduit le parsing ASN1 en espace noyau ☺**
      - **http://linuxfr.org/news/sortie-du-noyau-linux-3-7**

Infos Unix

- Samba 4.0 remplace entièrement Active Directory
  - https://www.samba.org/samba/news/releases/4.0.0.html
- E17 est sorti
  - http://www.enlightenment.org/p.php?p=news/show&l=en&news_id=77
- 90% des problèmes de latence sur Android
  - … introduit par /dev/(u)random ?
    - http://www.reddit.com/r/Android/comments/15w1qi/fix_90_of_lags_in_android_needs_root/
- L'esseimage de l'Open Source
  - http://www.forbes.com/sites/anthonykosner/2013/01/01/how-open-source-software-blooms-gource-version-control-visualizations-from-google/
- Ubuntu pour mobiles
  - Présenté le 2 janvier … pour une disponibilité en 2014
    - http://www.lemonde.fr/technologies/article/2013/01/03/ubuntu-se-devoile-sur-les-terminaux-mobiles_1812514_651865.html

Failles

- **Principales applications**
  - **Flash Player …**
    - **3 failles avec CVSS == 10.0**
      - **http://www.adobe.com/support/security/bulletins/apsb12-27.html**
  - **ShockWave installe les "extras" signés par Adobe sans confirmation**
    - **Notification: 27 octobre 2010**
    - **Publication: 17 décembre 2012**
    - **Correctif: aucun**
      - **http://www.kb.cert.org/vuls/id/519137**
  - **Java < 1.7.10**
    - **Aucun bulletin de sécurité initialement disponible …**
  - **VMWare View**
    - **"Directory Traversal"**
      - **https://www.vmware.com/security/advisories/VMSA-2012-0017.html**

Failles

- Elévation de privilèges via le service Nvidia
  - Faille publiée pour Noël
    - http://hardware.slashdot.org/story/13/01/06/0318242/nvidia-releases-fix-for-dangerous-display-driver-exploit
- SandboxIE
    - http://www.kernelmode.info/forum/viewtopic.php?f=13&t=2244
- Symantec PGP Desktop
  - Elévation de privilèges locale
    - http://pastebin.com/pEBSjsmC

Failles 2.0

- Backdoor dans le SCADA "Niagara AX Framework"
  - Exploitée dans la nature
    - http://arstechnica.com/security/2012/12/intruders-hack-industrial-control-system-using-backdoor-exploit/
- "Path Traversal" dans SFR MediaCenter 10.4.27.0
    - http://espacee.blogspot.fr/2012/12/sfr-mediacenter-path-traversal.html
- Clone de "/dev/mem" en lecture/écriture pour le monde
  - Affecte: de nombreux téléphones Samsung sous Android
    - http://forum.xda-developers.com/showthread.php?t=2050297
- La Samsung Smart TV piratée à distance
  - Source: Luigi Auriemma (ReVuln)
    - http://vimeo.com/55174958

Failles 2.0

- La magie des "bug bounties"
  - $5000 pour une exécution de commandes à distance sur les systèmes de Paypal
    - http://www.rafayhackingarticles.net/2012/12/wow-paypal-sends-me-5000-for-command.html
- "Sécurité du paiement en ligne en Chine"
  - "6.8% users find out the criminals themselves and recover the loss" (?!)
    - http://www1.cnnic.cn/AU/MediaC/rdxw/2012nrd/201211/t20121128_37296.htm
- Les chinois attaquent aussi les russes
    - http://krebsonsecurity.com/2012/12/chinese-espionage-attacks-against-ruskies/

Sites piratés

- **Les sites piratés du mois (liste non exhaustive)**
  - **ExploitHub**
    - **Via le répertoire /install/ de Magento …**
      - **http://priv8.1337day.com/exploitHUB.txt**
  - **#ProjectWhiteFox**
    - **ESA, NASA, …**
      - **http://pastebin.com/agUFkEEa**
  - **"Bharat Sanchar Nigam Limited" (FAI indien)**
    - **De nombreuses bases de données détruites**
    - **Mot de passe: "Password123"**
  - **"Fort Monmouth" (36,000 utilisateurs)**
      - **http://www.ehackingnews.com/2012/12/hackers-steal-personal-data-of-36k.html**
  - **"Australian Defence Force Academy"**
      - **http://thehackernews.com/2012/12/hacker-ruined-australian-military.html**

Sites piratés

- Une clinique Australienne rançonnée
  - http://au.news.yahoo.com/technology/news/article/-/15594002/hackers-target-gold-coast-medical-centre/
- Verizon (3m utilisateurs)
  - http://www.androidcentral.com/verizon-customer-database-hacked-300000-entries-leaked-online
  - http://www.zdnet.com/hacker-verizon-duel-over-customer-record-claims-7000009151/
  - 300,000 publiés
    - http://pastebin.com/Nf9ThT03
- La société des chemins de fer Belge (SNCB)
  - 1,5m de données clients … en accès libre sur leur site
    - http://www.01net.com/editorial/583059/la-sncb-belge-divulgue-les-donnees-de-ses-clients-sur-le-net/
    - http://storify.com/xdamman/sncbgate-nmbsgate

Sites piratés

- Un entreprise d'électricité "verte" victime de DDoS
  - http://www.euractiv.com/fr/energie/le-reseau-energie-renouvelable-t-news-516550
  - http://www.smartplanet.fr/smart-technology/en-allemagne-une-cyberattaque-a-vise-un-reseau-denergie-renouvelable-19963/
- Les banques américaines à nouveau menacées par les "Izz ad-Din al-Qassam Cyber Fighters"
  - http://pastebin.com/E4f7fmB5
  - http://www.infoworld.com/t/hacking/hacker-group-makes-good-promise-attack-major-banks-209085
  - … sans parler du projet "Blitzkrieg" du pirate "vorVzakone"
    - http://blogs.mcafee.com/mcafee-labs/new-labs-report-analyzing-project-blitzkrieg
- Yahoo! Mail ?
  - http://www.reddit.com/r/netsec/comments/163uph/a_bunch_of_people_i_know_with_yahoo_email/
  - Lié à ?
    - http://www.ehackingnews.com/2012/12/yahoo-hacked-virus-hima.html

Malwares, spam et fraudes

- UK: Orange, T-Mobile et EE livrent des téléphones Android avec l'antivirus Lookout préinstallé
  - http://www.zdnet.com/uk/orange-preloads-lookout-android-security-suite-after-funding-boost-7000008262/
- WinNT/Exforel.A s'injecte au niveau NDIS
  - https://blogs.technet.com/b/mmpc/archive/2012/12/09/the-quot-hidden-quot-backdoor-virtool-winnt-exforel-a.aspx
- Nouvelle attaque ciblée contre Mac OS X: OSX/Dockster.A
  - Exploite une faille Java connue
    - http://www.intego.com/mac-security-blog/new-mac-spyware-discovered-osxdockster-a/
- La saga John McAfee continue !
  - http://arstechnica.com/tech-policy/2013/01/the-bizarre-tale-of-john-mcafee-spymaster/
- Encore une fraude simple chez Amazon
  - http://www.htmlist.com/rants/two-for-one-amazon-coms-socially-engineered-replacement-order-scam/

Malwares, spam et fraudes

- La valeur d'un mot de passe (non bancaire)
  - http://krebsonsecurity.com/2012/12/exploring-the-market-for-stolen-passwords/
- La police japonaise offre $36,000 pour l'arrestation d'un pirate
  - http://thehackernews.com/2012/12/36000-usd-reward-for-wanted-hacker.html
- Des QR codes malveillants collés sur des affiches
  - http://www.theregister.co.uk/2012/12/10/qr_code_sticker_scam/
- Démantèlement du botnet Mariposa/Butterfly
  - … grâce à Facebook
  - Dégâts estimés par le FBI: $850m (?!)
    - http://www.fbi.gov/news/pressrel/press-releases/fbi-international-law-enforcement-disrupt-international-organized-cyber-crime-ring-related-to-butterfly-botnet

Actualité (francophone)

- Fichier STIC #fail
  - http://www.pcinpact.com/news/76436-le-viol-vocal-ou-comment-pirater-fichier-stic-par-simple-coup-fi.htm
- On peut porter plainte …
  - … depuis une page Facebook
    - http://www.numerama.com/magazine/24529-porter-plainte-aupres-de-la-police-sur-facebook-c-est-possible.html
- Publication de la PGSSI-S (Santé)
  - http://esante.gouv.fr/services/politique-generale-de-securite-des-systemes-d-information-de-sante-pgssi-s/en-savoir-plus-0
- Le permis de conduire électronique arrive
  - … mais pas la carte d'identité électronique
    - http://www.bfmtv.com/high-tech/carte-didentite-electronique-eportee-sine-die-401872.html
- CNIL
  - Guide pour la publication de photos sur Internet
    - http://www.cnil.fr/la-cnil/actualite/article/article/publication-des-photos-sur-internet-comment-partager-sans-se-sur-exposer/
    - http://www.quizphotocnil.fr/

Actualité (francophone)

- Lutte contre les "rançongiciels"
  - http://stopransomware.fr/
- Nouvelle idée: une taxe sur la collecte de données personnelles
  - http://www.zdnet.fr/actualites/collecte-de-donnees-personnelles-vers-une-nouvelle-taxe-39785734.htm
- Questionnaire sur l'expatriation
  - L'informatique ne fait pas partie des secteurs d'activité proposés ☺
    - http://questionnaires.ministere-affaires-etrangeres.com/index.php?sid=81234&newtest=Y&lang=fr
- Les français sont nuls en sécurité informatique :/
  - http://www.01net.com/editorial/582411/etude-les-francais-sont-assez-ignorants-en-securite-informatique/

Actualité (anglo-saxonne)

- UK: il faut cyber-attaquer avant d'être attaqué
  - http://www.telegraph.co.uk/news/uknews/law-and-order/9750614/Attack-cyber-enemies-before-they-attack-us-says-public.html
- Le programme "Perfect Citizen" de la NSA fait jaser
  - http://news.cnet.com/8301-1023_3-57560644-93/revealed-nsa-targeting-domestic-computer-systems-in-secret-test/
- USA: les sous-traitants de la défense devront notifier en cas d'intrusion
  - http://www.govtrack.us/congress/bills/112/hr4310/text
- L'USAF dépense $1 Md pour un logiciel (Oracle)
  - … qui ne marche pas
    - http://www.opex360.com/2012/12/17/lus-air-force-a-depense-un-milliard-de-dollars-pour-un-logiciel-inutilisable/

Actualité (européenne)

- **Europol**
  - **Ouverture de l'European CyberCrime Center (EC3)**
    - **https://www.europol.europa.eu/content/news/ec3-opening-european-cybercrime-centre-1933**

- **ENISA**
  - **Etude sur le ROI en sécurité (ROSI)**
    - **http://www.enisa.europa.eu/activities/cert/other-work/introduction-to-return-on-security-investment/at_download/fullReport**

Actualité (Google)

- Android 4.2 intègre un service de "Cloud Reputation"
  - Efficacité: 15% …
    - http://www.h-online.com/security/news/item/Only-15-of-known-malware-caught-by-Android-4-2-s-verifier-1765724.html
- Google va arrêter de supporter la synchro Exchange
    - http://www.pcinpact.com/news/76118-google-supprime-connectivite-exchange-activesync-gmai.htm
- La fin du monde a bien eu lieu
  - Gmail indisponible pendant 18 minutes …
  - … y compris Chrome via Sync
    - http://www.google.com/appsstatus#hl=en&v=issue&ts=1355288399000&iid=4abb2f6c40f6bd39677195b9a60ad77d
    - http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en/us/appsstatus/ir/plibxfjh8whr44h.pdf
    - http://www.wired.com/wiredenterprise/2012/12/google-bug/

Actualité (Apple)

- Google Maps revient sur iPhone ☺
- Hackulo.us ferme
  - … mais la relève s'organise: Vshare, Zeusmos, Kuaiyong …
    - http://www.linternaute.com/hightech/mobile/jailbreak-ces-applications-a-l-assaut-de-l-iphone-0113.shtml
- Apple recrute Kristin (ex-Chris) Paget
    - http://www.01net.com/editorial/582157/apple-embauche-une-hacker-qui-avait-cause-le-retard-de-windows-vista/

Actualité (crypto)

- "One Year of SSL Internet Measurement"
  - Par l'ANSSI ☺
    - http://www.acsac.org/2012/openconf/modules/request.php?module=oc_proceedings&action=summary.php&a=Accept&id=163&OPENCONF=20be685e9344f50b40a32f9fb48befde
- Les chaines de confiance SSL
    - http://notary.icsi.berkeley.edu/trust-tree/

Actualité

- Conférences passées

  - Microsoft BlueHat 2012
  - Black Hat Abu Dhabi 2012
    - Backdoor pour Microsoft Dynamics Great Plains
      - http://www.securestate.com/Downloads/Exploits/project_mayhem_v1.0.zip
      - http://www.securestate.com/Insights/Documents/WhitePapers/Project-Mayhem-Whitepaper.pdf
  - 29C3
    - Cf. présentation ce jour

Actualité

Conférences à venir

- OSSIR / JSSI 2013 (CFP: 06/01)
  - http://www.ossir.org/jssi/index/jssi-2013-appel-a-communications.shtml
- GS Days 2013 (CFP: 15/01)
  - http://www.gsdays.fr/373/actualites/appel-a-communication-2013/
- SSTIC 2013 (CFP: 21/01)
  - https://www.sstic.org/2013/cfp/
- HIP 2013 (CFP: 22/02)
  - https://www.hackinparis.com/node/155
- Nuit du Hack (CFP: 30/03)
  - http://www.nuitduhack.com/en/call-for-papers-nuit-du-hack

Actualité

- **Sorties logicielles**
  - **Shodan ajoute POP(S) et IMAP(S)**
  - **Hopper (pour Windows et Linux)**
    - **http://www.hopperapp.com/**
  - **Hydra 7.4**
  - **Suricata 1.4**
  - **IDA 6.4 (beta)**
    - **Ajout le support de PIN pour le tracing**
  - **BB10 (beta)**
    - **Intègre une liste noire de mots de passe "faibles"**
      - **http://rapidberry.net/106-passwords-that-blackberry-10-wont-let-you-use/**
  - **Aperçu de Firefox OS**
    - **https://hacks.mozilla.org/2012/12/firefox-os-simulator-1-0-is-here/**

Actualité

- **Amazon Web Services: un maquis juridique**
  - **http://pro.01net.com/editorial/582019/les-contrats-de-services-cloud-sont-un-veritable-maquis-juridique/**
- **MANDIANT s'installe à Dublin**
  - **… et crée 100 emplois**
    - **http://www.idaireland.com/news-media/press-releases/minister-bruton-announces-1/index.xml**
- **L'Inde va créer son propre OS**
  - **D'ici 3 ans**
    - **http://www.ehackingnews.com/2012/12/india-developing-own-secure-os-to.html**
- **La sécurité chez Twitter**
  - **http://www.infosecisland.com/blogview/22812-Heres-How-The-Amazing-Twitter-Infosec-Team-Helps-DevOps.html**

Actualité

- Le nouveau CLUF d'Instagram fait le buzz (négatif)
  - http://www.pcinpact.com/news/76281-conditions-dutilisation-instagram-fait-marche-arriere.htm
- Le compte @YourAnonNews suspendu (temporairement)
  - Pour non respect des conditions d'utilisation
    - http://www.pcinpact.com/news/76241-anonymous-compte-twitter-youranonnews-momentanement-suspendu.htm
- Le procès MegaUpload va dévoiler des informations sur Echelon
  - http://reason.com/blog/2012/12/10/echelon-spy-network-secrets-to-be-reveal
- Facebook vend l'accès à votre boite email
  - https://www.eff.org/deeplinks/2012/12/experimenting-privacy-facebook-sells-access-your-inbox
- Des écrans impossibles à prendre en photo
  - http://blog.persistent.info/2012/12/screenshot-proof-images-via-temporal.html

Divers

- Smartphone Pentest Framework …
  - … est lui-même vulnérable
    - http://seclists.org/bugtraq/2012/Dec/74
- De l'information à l'état pur
  - … ou pas
    - http://www.universfreebox.com/article19094.html
- L'apnée de l'email
  - … un risque sérieux
    - http://www.businessinsider.com/email-apnea-how-email-change-breathing-2012-12
- Le PDG de PornHub et YouPorn arrêté pour fraude fiscale en Allemagne
    - http://www.huffingtonpost.com/2012/12/11/fabian-thylman-arrested-pornhub-youporn-taxes_n_2276381.html

Divers

- Yeah, right
  - http://linuxfr.org/news/how-to-inviter-richard-stallman-a-une-conference
- La Wii U est crackée
  - http://hackmii.com/2012/12/hbc-release-for-a-new-wii-u/
  - Ainsi que la 3DS
    - http://www.esecurityplanet.com/hackers/nintendo-3ds-hacked.html
- Android
  - Un émulateur d'applications Windows 95 pour Android
    - http://www.winulator.com/
  - Un Android dans une coque de Minitel
    - http://www.youtube.com/watch?v=OzrYish2XbQ

Divers

- **Une Hacking School recherche … des candidatEs**
  - **https://www.hackerschool.com/**
- **Google sur carte perforée**
  - **http://www.masswerk.at/google60/**
- **Le fil électrique étirable**
  - **http://www.gizmodo.fr/2012/12/26/fils-electriques-etirables.html**

Divers

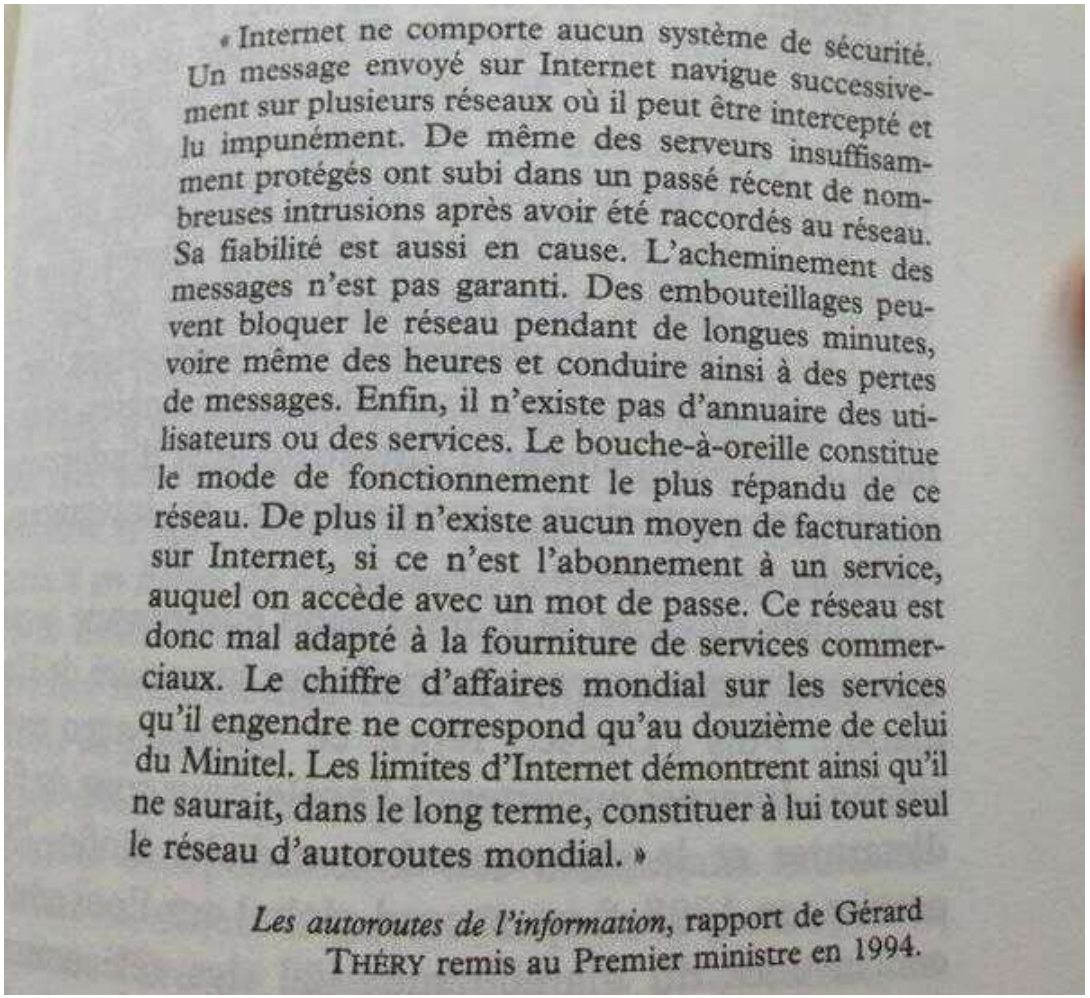
- **Trop de pression chez Apple !**
  - **Source: https://twitter.com/dchest/status/288047420229681152/photo/1**

```
/*
 * This will derive a 128 bit (16 byte) key from a set of answers to questions in a CFArray of CFStrings.
 * it normalizes each answer and concats them into a collector buffer.  The resulting string is run through
 * PBKDF2-HMAC-SHA256 to form a key.
 *
 * Todo: For version 2 it would be better to randomly generate the salt and make the iteration count flexible.
 * This would require a different return value because that information would need to be returned up the stack
 * to the callers.  Given the time left in this release (Lion) we're going with set values for this.
 */

#define RETURN_KEY_SIZE 16
#define MAXANSWERBUFF 4096
#define PBKDF_ROUNDS 100000
static uint8_t salt[16] = { 0x0A, 0x1F, 0x0A, 0x1F, 0x0A, 0x1F, 0x0A, 0x1F, 0x0A, 0x1F, 0x0A, 0x1F, 0x0A, 0x1F, 0x0A, 0x1F };
static int saltLen = sizeof(salt);
```

Divers

- **Source: http://barrabe.tumblr.com/post/38636687151/ce-ramassis-de-conn-s-nous-a-ete-pondu-par-gerard**



« Internet ne comporte aucun système de sécurité. Un message envoyé sur Internet navigue successivement sur plusieurs réseaux où il peut être intercepté et lu impunément. De même des serveurs insuffisamment protégés ont subi dans un passé récent de nombreuses intrusions après avoir été raccordés au réseau. Sa fiabilité est aussi en cause. L'acheminement des messages n'est pas garanti. Des embouteillages peuvent bloquer le réseau pendant de longues minutes, voire même des heures et conduire ainsi à des pertes de messages. Enfin, il n'existe pas d'annuaire des utilisateurs ou des services. Le bouche-à-oreille constitue le mode de fonctionnement le plus répandu de ce réseau. De plus il n'existe aucun moyen de facturation sur Internet, si ce n'est l'abonnement à un service, auquel on accède avec un mot de passe. Ce réseau est donc mal adapté à la fourniture de services commerciaux. Le chiffre d'affaires mondial sur les services qu'il engendre ne correspond qu'au douzième de celui du Minitel. Les limites d'Internet démontrent ainsi qu'il ne saurait, dans le long terme, constituer à lui tout seul le réseau d'autoroutes mondial. »

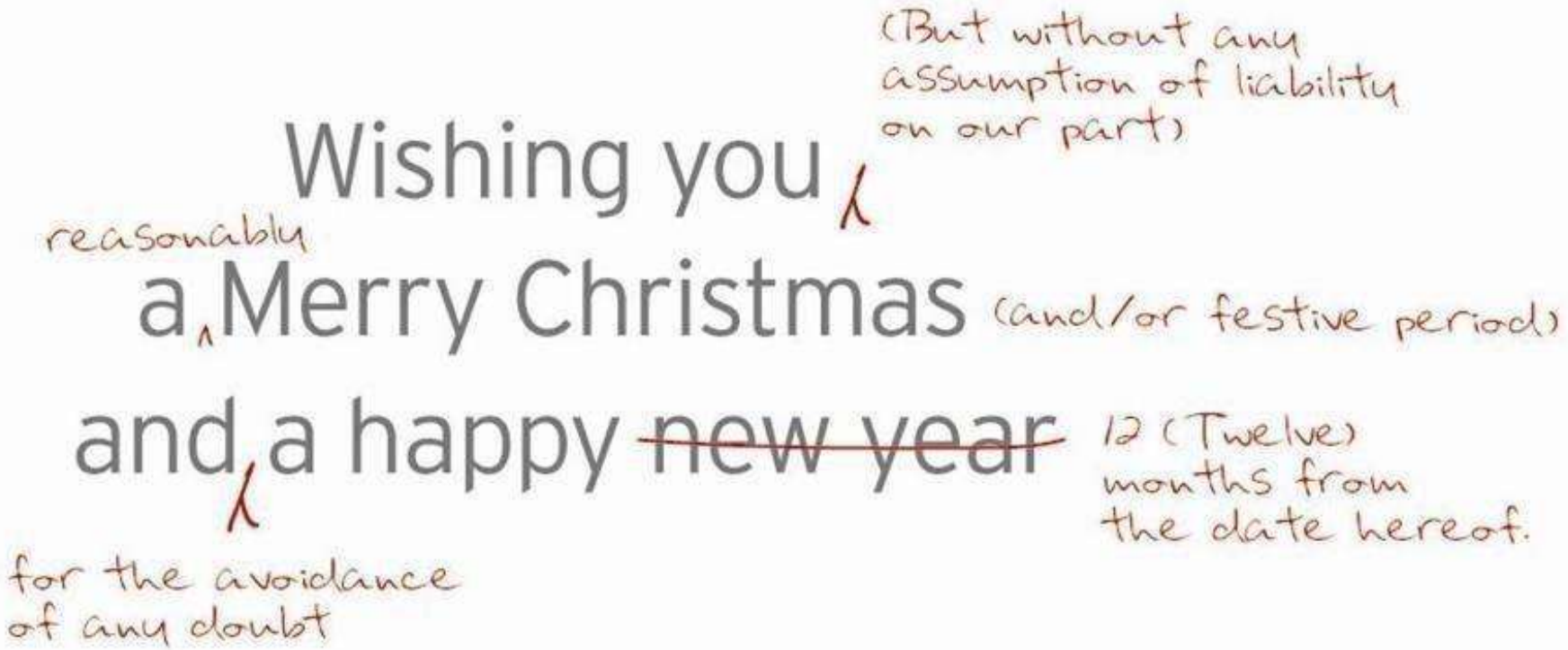
Les autoroutes de l'information, rapport de Gérard THÉRY remis au Premier ministre en 1994.

Divers

- Source: https://twitter.com/squallidon/status/282573851462889472/photo/1

Divers

- Source: https://twitter.com/CedricManara/status/282827939089895425/photo/1



Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 12 février 2013
- Conférence JSSI de l'OSSIR
  - Mardi 19 mars 2013
    - http://www.ossir.org/jssi/