OSSIR
Groupe Paris

Réunion du 9 octobre 2012

Revue des dernières vulnérabilités

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

Avis Microsoft

- **Septembre 2012**
  - **MS12-061 XSS dans Visual Studio 2010 "Team Foundation Server"**
    - **Affecte: Visual Studio 2010 TFS SP1**
    - **Exploit: XSS**
    - **Crédit: Sunil Yadav / INR Labs**
  - **MS12-062 XSS dans SMS et SCCM**
    - **Affecte: SMS 2003 SP3, SCCM 2007**
    - **Exploit: XSS**
    - **Crédit: Andy Yang / Stratsec**

Avis Microsoft

- **Hors bande**
  - **MS12-063 Failles dans IE (x5)**
    - **Affecte: IE (toutes versions sauf IE 10)**
    - **Exploit: "*use after free*" dans**
      - **OnMove()**
      - **Event Listener**
      - **Layout**
      - **cloneNode()**
      - **execCommand() ← la faille publique**
    - **Crédit:**
      - **Anonymous + iDefense**
      - **Rosario Valotta (https://sites.google.com/site/tentacoloviola/)**
      - **Stephen Fewer / Harmony Security**
      - **Anonymous + ZDI (x2)**
      - **MITRE**

Avis Microsoft

- Notes:
  - Le BSI préconise d'utiliser un autre navigateur
  - Le CERTFR préconise le workaround Microsoft (EMET)
    - http://www.lemagit.fr/article/securite-ie-faille-certa/11838/1/faille-allemagne-deconseille-usage-france-suit-les-recommandations-microsoft/
  - La faille a-t-elle fuitée chez ZDI ?
    - http://eromang.zataz.com/2012/09/21/microsoft-internet-explorer-0day-reported-by-zdi-to-microsoft/
  - Le "fix it" ne corrige pas la faille
    - http://imageshack.us/a/img163/2069/screenshot20120919at715.png

Avis Microsoft

- Advisories
  - Q2661254 Retrait des certificats < 1024 bits
    - V1.2: toutes les applications faisant appel à CertGetCertificateChain() sont impactées
  - Q2728973
    - V1.2: correction documentaire (CN du certificat révoqué)
  - Q2757760 Faille IE, exploitée dans la nature
    - V1.0: publication du bulletin
    - V1.1: publication d'un workaround avec EMET
    - V1.2: publication d'un "fix it"
    - V2.0: publication du correctif
  - Q2755801 IE 10 est livré avec une version vulnérable de Flash
    - V1.0: publication du bulletin
    - Probablement corrigé avant la sortie "officielle"
      - http://www.mag-securs.com/News/tabid/62/articleType/ArticleView/articleId/29251/Vulnerabilite-dans-Internet-Explorer-10-sur-Windows-8.aspx

Avis Microsoft

- **Prévisions pour Octobre 2012**
  - **1 bulletin "critique", 6 "importants"**
  - **20 vulnérabilités**
  - **Q2737111 (FAST Search Server) sera corrigé**
  - **Q2661254 (plus de clés RSA < 1024 bits) sera diffusé**
- **Failles antérieures**
- **Failles à venir**

Avis Microsoft

- Révisions
  - MS12-035
    - V2.3: corrections documentaires (nom des clés de base de registre)
  - MS12-045
    - V1.3: ajout d'un problème connu
  - MS12-061 Faille dans Visual Studio TFS
    - V1.1: ajout d'un problème connu, la mise à jour n'est plus automatique
  - MS12-062
    - V1.1: corrections documentaires

Infos Microsoft

- **Sorties logicielles**
  - **Dynamics GP 2013**
  - **Message Analyzer (Beta)**
    - **La suite de Network Monitor**
  - **SysInternals PsPing**
    - **http://technet.microsoft.com/en-us/sysinternals/jj729731**
  - **TypeScript**
    - **Un concurrent de Google Dart**
      - **http://www.typescriptlang.org/**

Infos Microsoft

- **Autre**
  - **Tous les employés Microsoft recevront une tablette Surface, un Windows Phone et un PC Windows 8**
    - **http://www.linformaticien.com/actualites/id/26279/les-microsoftees-rhabilles-de-pied-en-cape.aspx**
  - **Windows 8: 26 octobre**
  - **Windows Phone 8: 29 octobre**
  - **Développer pour Windows 8**
    - **http://www.microsoft.com/france/msdn/generation-app/**
  - **"Windows 8" n'est pas fini**
    - **Source: Intel, meeting interne**
      - **http://www.bloomberg.com/news/2012-09-25/windows-8-bugs-plaguing-microsoft-intel-ceo-said-to-tell-staff.html**
  - **… et ça pourrait être vrai**
    - **http://www.computerworld.com/s/article/9231900/Poor_pre_launch_showing_plagues_Windows_8**

Infos Microsoft

- Tarification Office 2013
  - 9 euros/mois pour 5 PC et/ou Mac
- Alain Crozier remplace Eric Boustouller en tant que président de Microsoft France
- Google vaut désormais plus cher que Microsoft
  - http://www.linformaticien.com/actualites/id/26512/valorisation-boursiere-google-depasse-microsoft.aspx
- Microsoft rachète PhoneFactor
  - Authentification "forte"
- 97% des licences Windows sont piratées chez China National Petroleum
  - http://www.linformaticien.com/actualites/id/26383/piratage-de-logiciels-microsoft-se-fache-contre-la-chine.aspx

Infos Réseau

- (Principales) faille(s)
  - FreeRADIUS 2.1.10 - 2.1.12
    - "*Remote pre-auth stack overflow*"
      - http://seclists.org/fulldisclosure/2012/Sep/83

Infos Réseau

- **Autres infos**
  - **Plus d'adresses IPv4 en Europe**
    - **http://www.ripe.net/internet-coordination/news/ripe-ncc-has-approximately-four-million-ipv4-addresses-before-reaching-last-8**
    - **Le business des netblocks a commencé**
      - **http://arstechnica.com/tech-policy/2012/09/ipv4-address-transfer-markets-are-forming-where-we-least-expected/**
  - **IPv6 aux USA**
    - **Finalement, ça ne va pas le faire …**
      - **http://www.zdnet.fr/actualites/ipv6-la-transition-prend-l-eau-aux-etats-unis-39783075.htm**
  - **L'Iran prépare son propre Internet**
    - **http://www.washingtonpost.com/world/national-security/iran-preparing-internal-version-of-internet/2012/09/19/79458194-01c3-11e2-b260-32f4a8db9b7e_story.html**
  - **Proposition de loi (française) sur la neutralité du net**
    - **http://www.linformaticien.com/actualites/id/26280/proposition-de-loi-sur-la-neutralite-du-net-en-france.aspx**

Infos Réseau

- Orange gagne face à Cogent
  - Sur l'asymétrie du peering
    - http://www.linformaticien.com/actualites/id/26375/peering-orange-gagne-face-a-cogent.aspx
- HTTP/2.0 sur les rails
    - http://lists.w3.org/Archives/Public/ietf-http-wg/2012OctDec/0004.html
- Surveiller les surveillants grâce à Shodan
    - http://infosecisland.com/blogview/22437-Network-Surveillance-Devices-Discovered-via-Shodan.html
  - … ainsi que les chantiers
    - https://twitter.com/shawnmer/status/250654051149176832

Infos Unix

- (Principales) faille(s)
  - Tavis Ormandy vs. Gnome Shell Extensions
    - http://seclists.org/oss-sec/2012/q3/415
  - La meilleure backdoor WordPress ?
    - Celle qu'on pousse soi-même ☺
      - http://news.ycombinator.com/item?id=4464044
  - Un exploit pour Samba 3.6.3
    - A priori une faille d'avril 2012
      - http://pastebin.com/AwpsBWVQ

Infos Unix

- Autre
  - Sortie de Linux 3.6
    - http://www.h-online.com/open/features/What-s-new-in-Linux-3-6-1714690.html
  - Bientôt des voitures sous Linux ?
    - http://automotive.linuxfoundation.org/

Failles

- Publications ZDI (sans date)

Failles

- **Principales applications**
  - **Adam Gowdiak a encore des failles en stock dans la JVM**
    - **Mais peut-il y avoir une fin ?**
  - **Il manquait des failles dans le dernier Flash Player ☺**
    - **https://twitter.com/Jindroush/status/249071669669404672**
    - **http://www.adobe.com/support/security/bulletins/apsb12-19.html**
  - **Re-failles au mois d'octobre**
    - **http://www.adobe.com/support/security/bulletins/apsb12-22.html**
  - **Exécution de *commandes* dans le gestionnaire de licences CA**
    - **Installé avec tous les produits de la marque**
    - **Reporté par l'ANSSI**
    - **2 ans pour corriger … ne vaut-il mieux pas faire appel à ZDI ? ☺**
      - **http://seclists.org/fulldisclosure/2012/Oct/3**
  - **UXSS dans Opera**
    - **http://blog.volema.com/opera-svg-xml-shortcut-uxss.html**

Failles 2.0

- **Brésil: la faille était dans le modem ADSL**
  - **http://arstechnica.com/security/2012/10/dsl-modem-hack-infects-millions-with-malware/**
- **PlaceRaider**
  - **Explorer l'environnement physique depuis un smartphone piraté**
    - **http://arxiv.org/pdf/1209.5982v1.pdf**
- **Trop de sécurité tue la sécurité**
  - **Le lecteur d'empreinte AuthenTec UPEK stocke les mots de passe en clair**
    - **http://www.h-online.com/security/news/item/Fingerprint-reader-reveals-passwords-1704058.html**
- **La location de PC**
  - **… *with a twist***
    - **http://www.forbes.com/sites/adriankingsleyhughes/2012/09/28/spy-software-on-rental-pcs-captured-webcam-pictures-of-children-partially-undressed-individuals-and-intimate-activities-at-home/**

Failles 2.0

- Très bonne arnaque sur eBay
  - http://unjourvous.tumblr.com/post/31589561555/un-jour-vous-serez-arnaques-sur-ebay
- Bientôt une version de PHP pour mobiles
  - http://venturebeat.com/2012/10/02/php-andi-gutmans-future-mobile/
- Le gouvernement canadien fait de la pub sur TPB
  - Par erreur ☺
    - http://thenextweb.com/ca/2012/09/29/canadian-government-accidentally-sponsors-the-pirate-bay-blames-yahoo-mistake/

Sites piratés

- Les sites piratés du mois
  - Adobe #epic #fail (again?)
    - Des "pirates" ont eu accès au HSM de signature depuis le 10 juillet dernier
      - http://www.adobe.com/support/security/advisories/apsa12-01.html
      - http://blogs.adobe.com/asset/2012/09/inappropriate-use-of-adobe-code-signing-certificate.html
    - Plus de 5000 malwares (dont PWDUMP 7.1) ont été signé depuis
      - http://thenextweb.com/apps/2012/09/27/adobe-finds-hacked-build-server-used-code-signing-plans-revoke-certificate-october-4/
  - 100,000 mots de passe en clair un FTP de l'IEEE
    - "It's not a hack, it's a feature"
      - http://www.scmagazine.com/passwords-of-100k-ieee-members-lie-bare-on-ftp-server/article/260721/
    - … et en plus, les mots de passe sont mauvais

Sites piratés

- APT "Mirage" contre le secteur de l'énergie
  - Telvent (filiale américaine de Schneider Electric)
    - http://www.computerworld.com/s/article/9231748/Energy_giant_confirms_breach_of_customer_project_files
  - … et d'autres victimes
    - http://www.computerweekly.com/news/2240163620/Dell-SecureWorks-uncovers-cyber-espionage-targeting-energy-firms
    - http://www.secureworks.com/research/threats/the-mirage-campaign/
- Opération "West Wind" / "Ghost Shell"
  - De nombreuses universités piratées, dont l'ENS
    - http://www.zataz.com/news/22443/Project-West-Wind_-ProjectWestWind_-TeamGhostShell_-Team-Ghost-Shell.html

Sites piratés

- Orange
  - http://www.cyberwarnews.info/2012/10/07/telecom-giant-orange-hacked-data-leaked-by-nullcrew/
  - La faille était dans le PHPMyAdmin …
    - http://nsa30.casimages.com/img/2012/10/02/121002031647878642.png
- Un serveur vocal de la Banque de France
  - Mot de passe: "123456"
    - http://www.20minutes.fr/societe/1007331-relaxe-apres-avoir-pirate-systeme-informatique-banque-France
- Unesco
  - http://pastebin.com/HJ6UUQQX
- Le Midi Libre
  - http://www.montpellier-journal.fr/2012/09/le-site-de-midi-libre-pirate-les-informations-clients-diffusees.html
- Domino's pizza
  - http://www.computerworld.com/s/article/9231198/Domino_s_Pizza_says_website_hacked

Sites piratés

- GoDaddy
  - Piraté par Anonymous ou pas ?
- Virgin Mobile USA
  - 6 millions de comptes protégés par … un code à 6 chiffres
- Les bornes de commande Subway
  - Un Windows connecté à Internet avec RDP ouvert
    - http://www.networkworld.com/news/2012/092112-what-to-learn-from-the-262659.html
  - Résultat: $10m de fraude à la CB par 2 roumains
- UGC (www.ugcac.in)
    - http://pastebin.com/DHTiPDAd
- DDoS contre différentes banques américaines
- "Spear Phishing" contre la maison blanche
    - http://news.cnet.com/8301-1009_3-57523621-83/white-house-confirms-spearphishing-intrusion/

Malwares, spam et fraudes

- "Nitol"
  - Un botnet qui infecte les ordinateurs en usine (!)
    - http://blogs.technet.com/b/microsoft_blog/archive/2012/09/13/microsoft-disrupts-the-emerging-nitol-botnet-being-spread-through-an-unsecure-supply-chain.aspx
- Sophos *peut* s'auto-terminer
    - http://www.sophos.com/fr-fr/support/knowledgebase/118311.aspx
- D'où vient StuxNet ?
  - Le rôle de la CIA
    - https://secure.cryptome.us/2012/10/corrupt-ir-us-12-1001.htm
- "Zeus in the Mobile" (Android & BlackBerry)
  - Selon Kaspersky
    - http://www.securelist.com/en/blog/208193760/New_ZitMo_for_Android_and_Blackberry
- BlackHole Exploiter Kit 2.0
  - Faille(s) Java, URL à usage unique, sélection du navigateur, filtrage des clients Tor …
    - http://datasecuritybreach.fr/actu/blackhole-exploiter-kit-2-0-est-sorti/
- Les malwares protégés par le DMCA ?
    - http://contagiodump.blogspot.fr/2012/09/contagio-file-downloads-are-not.html
  - … ou juste une victime de la société LeakID ?
    - http://korben.info/leakid-la-solution-anti-direct-download.html

Actualité (francophone)

- **Patrick Pailloux aux Assises de la Sécurité: "oser dire non"**
  - **… au BYOD**
    - **http://www.numerama.com/magazine/23920-cybersecurite-l-anssi-estime-que-les-societes-n-ont-plus-d-excuses.html**
    - **http://www.lesechos.fr/entreprises-secteurs/tech-medias/actu/0202307729069-la-mobilite-lance-un-nouveau-defi-a-la-securite-informatique-369383.php**
  - **L'ANSSI publie un guide d'hygiène informatique**
    - **http://www.pcinpact.com/news/74291-l-anssi-publie-son-precis-d-hygiene-informatique.htm**
  - **Le sénateur Bockel se défausse sur l'ANSSI**
    - **http://www.linformaticien.com/actualites/id/26573/routeurs-chinois-jean-marie-bockel-se-defausse-sur-l-anssi.aspx**
    - **http://www.lesechos.fr/entreprises-secteurs/tech-medias/actu/0202307148775-le-cyberespionnage-n-est-pas-de-la-science-fiction-369434.php**
  - **TL;DR**
    - **https://twitter.com/pentesteur/status/253473044721459202**
  - **RGS 2.0**
    - **http://www.pcinpact.com/news/73697-de-nouvelles-regles-dhygiene-informatique-pour-administrations.htm**
  - **En 2013, l'ANSSI devra recruter dans les autres ministères**
    - **http://www.economie.gouv.fr/files/projet-loi-finances-2013-plf-missions.pdf**

Actualité (francophone)

- Fabrice Bellard …
  - Implémentation 4G 100% logicielle
    - http://bellard.org/lte/
- Acquisitions tous azimuts chez Cassidian
  - NetAsq
    - http://www.eads.com/eads/int/en/news/press.20121002_cassidian_netasq.html
  - Carl Zeiss Optronics
  - Partenariat avec AXA MATRIX Risk Consultants
    - http://www.eads.com/eads/int/en/news/press.20121004_cassidian_axa_matrix.html
- Bull lance le "sphone"
    - http://www.businessmobile.fr/actualites/bull-presente-un-telephone-mobile-ultra-securise-39783194.htm
- CNIL vs. Facebook
  - C'était bien un bug
    - http://www.cnil.fr/nc/la-cnil/actualite/article/article/les-conclusions-de-la-cnil-sur-le-bug-facebook/

Actualité (francophone)

- La DGA/MI recrute 200 personnes
  - http://www.defense.gouv.fr/dga/recrutement2/dga-fiches-de-postes
- Des réservistes pour la "cyber défense"
  - http://www.defense.gouv.fr/actualites/articles/des-reservistes-specialises-en-cyberdefense
- Circulaire pour l'usage du logiciel libre dans l'administration
  - http://circulaire.legifrance.gouv.fr/pdf/2012/09/cir_35837.pdf
- Transmission des résultats électoraux par Internet ?
  - http://www.pcinpact.com/breve/74117-un-depute-propose-remonter-resultats-electoraux-par-internet.htm
- Une taxe sur les opérateurs … pour financer l'élagage des arbres
  - http://www.senat.fr/questions/base/2012/qSEQ121002173.html
- L'enseignement de l'informatique revient au Lycée
  - http://www.rue89.com/2012/09/04/linformatique-revient-au-lycee-trois-raisons-denseigner-le-code-lecole-235059
  - Le programme informatique au Bac
    - http://www.education.gouv.fr/pid25535/bulletin_officiel.html?cid_bo=57572

Actualité (francophone)

- Les propositions de l'association "France Digitale"
  - http://www.francedigitale.org/wp-content/uploads/2012/09/NoteFD-LoideFinances2013.pdf
- Encore un nouveau Cloud français
  - Microsoft + Bouygues
    - http://www.linformaticien.com/actualites/id/26323/cloud-microsoft-s-allie-a-bouygues-pour-une-offre-pme-iaas.aspx
- Première condamnation pour HADOPI
  - 150 euros d'amende …
    - http://www.pcinpact.com/news/73806-300-euros-requis-contre-premier-abonne-denonce-par-hadopi.htm
- 10 millions de français victimes de la cybercriminalité
  - D'après Symantec
    - http://www.linformaticien.com/actualites/id/26194/10-millions-de-francais-victimes-de-la-cybercriminalite-en-2011.aspx

Actualité (francophone)

- **Libération en panne … informatique**
  - **http://www.liberation.fr/medias/2012/09/02/liberation-est-de-retour_843429**
- **CharlieHebdo.fr … toujours pas *scalable***
  - **https://twitter.com/nbs_system/status/248375376127078401**
- **Seesmic réussit à se faire racheter par HootSuite**
  - **http://www.linformaticien.com/actualites/id/26191/hootsuite-s-offre-le-francais-seesmic.aspx**

Actualité (anglo-saxonne)

- Cyberattaques de l'Iran contre les USA
  - FUD ?
    - http://gulfnews.com/business/economy/iran-seen-launching-cyber-attacks-against-us-companies-1.1079807
  - L'inverse est probablement vrai …
    - http://securityaffairs.co/wordpress/9173/intelligence/new-cyber-attacks-have-caused-serious-damage-to-internet-connection-in-iran.html
- Le DHS recrute 600 "cyber ninjas"
  - http://www.federalnewsradio.com/241/3066466/DHS-urged-to-hire-600-cyber-ninjas
- La NSA passe au BYOD
  - http://www.schneier.com/blog/archives/2012/09/the_nsa_and_the.html

Actualité (anglo-saxonne)

- La DARPA va financer des "Hacker Spaces"
  - http://www.nytimes.com/2012/10/06/us/worries-over-defense-dept-money-for-hackerspaces.html
- Le patron de la sécurité du réseau électrique anglais se fait voler son laptop dans un hôtel
  - Mais il était chiffré !
    - http://www.independent.co.uk/news/uk/crime/national-grid-security-boss-warren-bamfords-laptop-is-stolen-8190641.html
- FinQloud: le NASDAQ sur Amazon Web Services
  - http://www.ictjournal.ch/fr-CH/News/2012/09/25/Amazon-et-le-NASDAQ-developpent-un-cloud-pour-les-services-financiers.aspx

Actualité (européenne)

- **Création du CERT-UE**
  - **http://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html**
- **Un exercice de cyber-défense européen**
  - **Incluant banques & opérateurs telecom**
    - **http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/1062&format=HTML&aged=0&language=FR&guiLanguage=en**

Actualité (Google)

- GMail vs. "state sponsored attacks"
  - http://support.google.com/mail/bin/answer.py?hl=fr&ctx=mail&answer=2591015
- OAuth 2.0 pour IMAP et XMPP
  - Dommage qu'aucun client ne le supporte …
    - http://googledevelopers.blogspot.fr/2012/09/adding-oauth-20-support-for-imapsmtp.html
- Le patron de Google Brésil arrêté
  - Pour avoir tardé à retirer une vidéo de YouTube
    - http://www.linformaticien.com/actualites/id/26459/le-president-de-google-bresil-arrete.aspx
- De matériel Google dans la nature ?
  - http://www.wired.com/wiredenterprise/2012/09/pluto-switch/all/

Actualité (Google)

- webOS 1.0 porté sur Google Nexus
  - http://blog.openwebosproject.org/post/32477144913/news-flash
- Mode "moniteur" sur Android
  - Supporte BCM4329 (ex. Nexus One, EVO 4G)
    - http://bcmon.blogspot.fr/
  - … et iPhone !
    - https://github.com/tuter/monmob
- Google TV est arrivé en France le 24 septembre (via Sony)
- Google rachète Snapseed

Actualité (Apple)

- **Mac OS 10.7.5**
  - Introduit la fonction "GateKeeper", présenté comme anti-malware ☺
    - http://support.apple.com/kb/HT5313?viewlocale=fr_FR&amp%3blocale=fr_FR&locale=fr_FR
- **iTunes 10.7**
  - Corrige 163 failles dans WebKit …
    - http://support.apple.com/kb/HT5485
- **iOS 6**
  - Corrige quelques dizaines de failles (dont "Passcode Lock") …
  - Et quelques centaines dans WebKit …
    - http://support.apple.com/kb/HT5503
- **Exécution de code sur Mac OS 10.7**
  - A l'insertion d'une clé USB
    - http://www.securityfocus.com/archive/1/524248
- **Un rootkit fiable sur OS X**
    - http://www.nullsecurity.net/tools/backdoor/rubilyn-0.0.1.tar.gz

Actualité (Apple)

- Le meilleur antivirus sur Mac ? XCode !
  - http://waxy.org/2012/04/flashback_trojan_creators_scared_of_xcode_users_but_not_norton_antivir/
- Les futurs MacBook sous ARM ?
  - http://www.businessweek.com/articles/2012-10-03/mapping-a-path-out-of-steve-jobs-shadow#p3
- Alcatel-Lucent vs. Apple
  - Sur un brevet de compression
    - http://www.linformaticien.com/actualites/id/26152/alcatel-lucent-attaque-apple-pour-violation-de-brevets.aspx
- HTC vs. Apple
  - Sur un brevet 4G/LTE
    - http://www.linformaticien.com/actualites/id/26244/iphone-5-htc-defend-ses-brevets-sur-la-4g.aspx
- Note: Apple et Google ont dépensé plus d'argent en procès qu'en R&D en 2011
  - http://www.nytimes.com/2012/10/08/technology/patent-wars-among-tech-giants-can-stifle-competition.html

Actualité (Apple)

- "Ping" ferme le 30 septembre
- iOS 6
  - "PassBook" centralise billets de concert, cartes d'embarquement …
  - "Maps" ne fait pas l'unanimité
    - http://theamazingios6maps.tumblr.com/
    - http://www.apple.com/letter-from-tim-cook-on-maps/
    - http://www.linformaticien.com/actualites/id/26396/apple-debauche-des-employes-de-google-maps.aspx
  - Déjà jailbreaké
    - https://twitter.com/chpwn/status/249304699738664961/photo/1
- L'échec de Retina
  - L'écran souffre de "pixel burn"
    - http://blog.rinik.net/so-long-retina
- L'iPhone 4S et l'iPhone 5 sont compatibles GLONASS
  - Une obligation pour vendre en Russie
- Note: camper devant l'AppStore *est* une stratégie marketing
    - http://www.linformaticien.com/actualites/id/26304/camper-devant-l-apple-store-comme-strategie-marketing.aspx

Actualité (crypto)

- "CRIME": SSL encore "cassé"
  - Cette fois-ci c'est la compression
    - http://security.stackexchange.com/questions/19911/crime-how-to-beat-the-beast-successor/19914#19914
  - Immédiatement désactivé dans Chrome
    - http://www.reddit.com/r/netsec/comments/zrss0/google_disables_openssl_compression_in_chrome/
- Le paiement mobile "cassé"
  - Système Audio-jack Magnetic Stripe Reader (AMSR)
    - https://www.usenix.org/conference/woot12/security-analysis-smartphone-point-sale-systems
- Keccak devient SHA-3
    - http://www.nist.gov/itl/csd/sha-100212.cfm
- Usage des extensions SSL/TLS à l'échelle d'Internet
    - https://journal.paul.querna.org/articles/2012/09/07/adoption-of-tls-extensions/
- Les discussions du CA/Browser Forum désormais publiques
    - https://www.cabforum.org/
- Un challenge du "Art of Computer Programming" résolu
    - http://www.mersenneforum.org/showpost.php?p=311753&postcount=61
  - Les nombres premiers étaient ln(Φ) et ln(π) …
    - http://www.mersenneforum.org/showpost.php?p=311759&postcount=65

Actualité

- **Conférences passées**
  - **Assises de la Sécurité 2012**
  - **ekoParty**
    - **http://www.ekoparty.org/**
    - **Attaque "CRIME" contre SSL/TLS**
    - **Attaque contre les mots de passe Oracle 10 et 11**
      - **http://www.teamshatter.com/topics/general/team-shatter-exclusive/advisory-ocipasswordchange-leaks-information-pwdhash/**
    - **Attaque contre les téléphones InmarSat GMR-2**
    - **Faille USSD permettant de réinitialiser tous les Samsung Galaxy depuis une page Web**
      - **<frame src="tel:*2767*3855%23" />**
    - **"VGA Rootkit"**
  - **Mobile pwn2own @ EuSecWest**
    - **Intègre NFC, SMS, baseband …**
    - **… et sponsorisé par RIM ☺**
      - **http://dvlabs.tippingpoint.com/blog/2012/07/20/mobile-pwn2own-2012**
    - **iPhone 4S pwn via WebKit**
    - **Galaxy SIII pwn via NFC**
      - **http://www.infosecurity-magazine.com/view/28367/iphone-and-android-both-hacked-at-eusecwest/**

Actualité

- Conférences à venir
  - 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/
  - SSTIC 2013
    - CFP
      - https://www.sstic.org/2013/cfp/

Actualité

- Sorties logicielles
  - OllyDbg 2.01g
  - Burp 1.5-rc2
  - SleuthKit 4.0.0
    - Désormais disponible sous Windows
  - (…)

Actualité

- La Chine va renforcer sa coopération internationale en matière de cybersécurité
  - http://china.org.cn/china/2012-10/05/content_26706352.htm
- Apple et Google négocient sur les brevets
  - http://www.linformaticien.com/actualites/id/26120/brevets-google-et-apple-negocient-en-coulisses.aspx
- Le système BlackBerry 10 dévoilé
  - http://www.linformaticien.com/actualites/id/26431/rim-devoile-enfin-l-os-de-sa-renaissance-bb10.aspx
- Lenovo
  - Rachète Stoneware (pour se lancer dans le Cloud ?)
  - Pourrait racheter RIM (!)
    - http://www.linformaticien.com/actualites/id/26160/lenovo-part-a-la-peche.aspx
- Intel pourrait abandonner les processeurs OMAP
  - Qu'on trouve dans le Kindle Fire ou le Samsung Galaxy
    - http://www.linformaticien.com/actualites/id/26481/texas-instruments-pourrait-abandonner-les-processeurs-mobiles.aspx

Actualité

- Qualys (QLYS) entre au Nasdaq
  - http://pro.clubic.com/it-business/securite-et-donnees/actualite-513629-qualys-bourse.html
- Facebook revendique 1 milliard d'utilisateurs actifs
  - … et va permettre la promotion de posts pour $7
    - http://newsroom.fb.com/News/Testing-Promoted-Posts-for-People-in-the-U-S-1c6.aspx
- Comment Kim a-t-il su qu'il était surveillé ?
  - Son PING sur Xbox Live a considérablement augmenté
    - http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10838484

Actualité

- Encore une preuve que les politiques de sécurité ne fonctionnent pas
  - http://www.mag-securs.com/News/tabid/62/articleType/ArticleView/articleId/29289/Les-fonctionnaires-taiwanais-pieges-par-un-pourriel-sulfureux.aspx
- Résultats du concours IOCCC 21
  - http://www.ioccc.org/2012/whowon.html
- The Pirate Bay conserve les adresses IP
  - 48h ? Ou plus ?
    - http://torrentfreak.com/yes-the-pirate-bay-stores-ip-addresses-121005/
- Les informaticiens du Tokyo Stock Exchange pénalisés de 30% sur leur salaire
  - Suite aux pannes à répétition
    - http://www.linformaticien.com/actualites/id/26138/pannes-informatiques-le-tokyo-stock-exchange-met-a-l-amende-ses-cadres.aspx
- Charlie Miller recruté chez Twitter
  - http://www.zdnet.fr/actualites/twitter-recrute-l-expert-en-securite-charlie-miller-39782557.htm
- Anonymous recrute !
  - http://anonpr.net/join-anonymous/

Divers

- Slashdot et SourceForge ont été rachetés
  - http://finance.yahoo.com/news/dice-holdings-buys-geeknet-websites-125531940.html
- Python pour les enfants
  - https://code.google.com/p/swfk/
- Le "cat face detector"
  - http://harthur.github.com/kittydar/
- DICKS
  - Probablement le meilleur troll de la saison d'automne
    - http://www.theregister.co.uk/2012/10/05/hakin9_silliness/
    - http://hakin9.org/statement/
    - http://www.reddit.com/r/netsec/comments/10xvgt/hakin9_spam_kings_please_stop_supporting_these/

Divers

- Productivité--;
  - http://xkcd.com/1110/
  - La solution
    - http://www.mrphlip.com/xkcd1110/
    - http://azttm.wordpress.com/2012/09/19/map-of-xkcds-click-and-drag/
- L'actu qui tue
  - http://www.charentelibre.fr/2012/10/02/pleuville-il-menace-son-voisin-avec-un-fusil-car-il-lui-reproche-de-tuer-ses-vaches-grace-a-un-logiciel-informatique,1116993.php
- Comment une grand-mère a été retrouvée en train de creuser dans un dépôt d'Uranium militaire
  - http://thebulletin.org/web-edition/columnists/fissile-materials-working-group/security-y-12-nun-too-good
- Autres liens (non classés)
  - http://www.pointerpointer.com/
  - https://github.com/humans.txt

Divers

- La cyber-guerre, c'est moche
  - Des cités entières ravagées
    - http://wow.joystiq.com/2012/10/07/reports-entire-cities-dead-on-certain-realms

Divers

- On a retrouvé le Père Noël
  - https://twitter.com/codelancer/status/254180046590320640/photo/1

Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 13 novembre 2012
- Prochain Afterwork
  - Mardi 23 octobre 2012
- JSSI
  - Mardi 19 mars 2013
    - À la Maison des Associations