OSSIR
Groupe Paris

Réunion du 12 novembre 2013

Revue des dernières vulnérabilités

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

Avis Microsoft

- **Octobre 2013**

  - **MS13-080 Correctif cumulatif pour IE (x10) [1]**
    - **Affecte: IE 6 – IE 11**
      - **Sauf le *backport* de IE 11 pour Windows 7 / 2008 R2**
    - **Exploit: corruption mémoire conduisant à l'exécution de code arbitraire**
    - **Crédits:**
      - **Aniway.Anyway@gmail.com + ZDI**
      - **Jose A. Vazquez / Yenteasy - Security Research (x2)**
      - **Jose A. Vazquez / Yenteasy - Security Research + ZDI**
      - **Jose A. Vazquez / Yenteasy - Security Research + VeriSign (x2)**
      - **Amol Naik + ZDI**
      - **Ivan Fratric / Google Security Team**
      - **Yoshihiro Ishikawa / LAC Co.**
      - **Hoodie22 + National Cyber Security Centre of the Netherlands**
      - **Daniel Chechik / Trustwave SpiderLabs Team**
      - **Renato Ettisberger / IOprotect GmbH**

Avis Microsoft

- MS13-081 Failles noyau (x7) [1,2]
  - Affecte: Windows (toutes versions supportées)
    - Sauf Windows 8.1 et 2012 R2
  - Exploit:
    - "OpenType Font Parsing Vulnerability" - CVE-2013-3128
    - "Windows USB Descriptor Vulnerability" - CVE-2013-3200
    - "Win32k Use After Free Vulnerability" - CVE-2013-3879
    - "App Container Elevation of Privilege Vulnerability" - CVE-2013-3880
    - "Win32k NULL Page Vulnerability" - CVE-2013-3881
    - "DirectX Graphics Kernel Subsystem Double Fetch Vulnerability" - CVE-2013-3888
    - "TrueType Font CMAP Table Vulnerability" - CVE-2013-3894
  - Crédits:
    - Anonymous + ZDI
    - Andy Davis / NCC Group
    - Lucas Bouillot / ANSSI
    - Seth Gibson & Dan Zentner / Endgame
    - ZombiE + ZDI

Avis Microsoft

- MS13-082 Failles .NET (x3) [1,2,3]
  - Affecte: .NET Framework (toutes versions supportées)
    - Sauf .NET 1.0, .NET 1.1, Windows 8.1 et Windows 2012 R2
  - Exploit:
    - Exécution de code noyau au travers d'une police OTF malformée (depuis une application XBAP)
    - DoS dans "Entity Expansion"
    - DoS dans "JSON Parsing"
  - Crédits:
    - Anonymous + ZDI
    - James Forshaw + Context IS

- MS13-083 Faille dans "Windows Common Controls" (x1) [1]
  - Affecte: Windows (toutes versions supportées)
    - Exploitable sur les versions 64 bits uniquement
    - Sauf: Windows XP SP3, Windows 8.1 et Windows 2012 R2
  - Exploit: exécution de code lors de l'envoi d'une requête malformée vers une application ASP.NET
    - Fonction DSA_InsertItem()
  - Crédits:
    - 孙晓山

Avis Microsoft

- **MS13-084 Failles SharePoint (x2) [3,2]**
  - **Affecte: SharePoint 2007 / 2010 / 2013 et Office Web Apps 2010**
  - **Exploit:**
    - **Exécution de code lors de l'ouverture d'un fichier Excel malformé**
    - **XSS**
  - **Crédits:**
    - **Mateusz Jurczyk, Ivan Fratric & Ben Hawkes / Google Security Team**
    - **Nutan kumar panda**

- **MS13-085 Failles Excel (x2) [1,2,3]**
  - **Affecte: Office (toutes versions supportées sauf 2003)**
  - **Exploit:**
    - **Exécution de code lors de l'ouverture d'un fichier Excel malformé (x2)**
  - **Crédits:**
    - **Mateusz Jurczyk, Ivan Fratric & Ben Hawkes / Google Security Team (x2)**

Avis Microsoft

- MS13-086 Failles Word (x2) [1,3]
  - Affecte: Office 2003 / 2007 et Compatibility Pack
  - Exploit:
    - Exécution de code lors de l'ouverture d'un fichier Word malformé (x2)
  - Crédits:
    - Yuhong Bao
    - Mateusz Jurczyk, Ivan Fratric & Ben Hawkes / Google Security Team

- MS13-087 Faille SilverLight (x1) [3]
  - Affecte: SilverLight 5
  - Exploit: fuite d'information sur la mémoire
    - http://packetstormsecurity.com/files/123731/
  - Crédits:
    - Vitaliy Toropov

Avis Microsoft

- Advisories
  - Q2862973 Les autorités de certification ne doivent plus utiliser MD5
    - V1.2: pas de mise à jour pour Windows 8.1 et Windows 2012 R2 avant février 2014
  - Q2887505 Faille IE (disponible dans Metasploit)
    - V2.0: publication du correctif
  - Q2896666 Faille "0day" en cours d'exploitation "dans la nature"
    - V1.0: publication du correctif
      - http://blogs.technet.com/b/srd/archive/2013/11/05/cve-2013-3906-a-graphics-vulnerability-exploited-through-word-documents.aspx

Avis Microsoft

- **Prévisions pour Novembre 2013**
  - **8 failles (3 critiques, 5 importants)**
- **Failles à venir**
- **Retour sur des failles antérieures**
  - **MS13-022**
    - **Faille dans SilverLight**
      - **http://packetstormsecurity.com/files/123731/**
  - **MS13-052**
    - **Faille dans .NET Framework**
      - **http://weblog.ikvm.net/PermaLink.aspx?guid=50d94ff6-f418-42b4-8cc5-33996d0c7cf3**

Avis Microsoft

- **Révisions**
  - **MS13-034**
    - **V1.2: changement dans la logique de détection**
  - **MS13-080**
    - **V1.2: disponibilité de la mise à jour via Windows Update**
    - **V1.3: correction documentaire (CVE erroné)**
  - **MS13-081**
    - **V1.1: changement dans la logique de détection**
    - **V1.2: correction documentaire (bulletins remplacés)**
  - **MS13-082**
    - **V1.1: Windows 2012 "Core" est aussi vulnérable**

Infos Microsoft

- **Sorties logicielles**
  - **Surface (Pro) 2**
  - **Windows 8.1 en mise à jour automatique**
    - **Seul problème: certaines Surface RT ont été "brickées" (0,1% environ)**
      - **http://www.ubergizmo.com/2013/10/microsoft-pulls-windows-8-1-rt-update-after-bricking-surface-rt-tablets/**
      - **http://www.theverge.com/2013/10/21/4861538/surface-rt-recovery-image-windows-rt-8-1-update-issues**
  - **Sysinternals SigCheck intègre VirusTotal**
    - **https://twitter.com/markrussinovich/status/390635117997072384**
  - **Nouveautés MSDN**
    - **Windows Server 2012 R2**
    - **System Center 2012 R2**
    - **System Center 2012 R2 Configuration Manager**
    - **Hyper-V Server 2012 R2**
    - **SQL Server 2014 CTP2**
    - **SQL Server 2014 Express CTP2**
    - **Windows Server 2012 R2 Essentials**
    - **Windows Azure Pack**

Infos Microsoft

- **Autre**
  - **$100,000 pour un contournement des protections IE11**
    - **Payés à James Forshaw**
      - **http://blogs.technet.com/b/bluehat/archive/2013/10/08/congratulations-to-james-forshaw-recipient-of-our-first-100-000-bounty-for-new-mitigation-bypass-techniques.aspx**
  - **Améliorations de sécurité dans Windows 8.1**
    - **http://blogs.technet.com/b/srd/archive/2013/11/06/software-defense-safe-unlinking-and-reference-count-hardening.aspx**
  - **Microsoft vs. Vest Corporation**
    - **0 - 1**
      - **http://basse-normandie.france3.fr/2013/10/22/la-start-caennaise-gagne-son-proces-contre-microsoft-skype-343693.html**
  - **Bill Gates: "Internet ne sauvera pas le monde"**
    - **http://www.ft.com/intl/cms/s/2/dacd1f84-41bf-11e3-b064-00144feabdc0.html**

Infos Réseau

- **(Principales) faille(s)**

  - **Cisco ASA**
    - **cisco-sa-20131009-asa**
      - **IPsec VPN Crafted ICMP Packet Denial of Service Vulnerability**
      - **SQL*Net Inspection Engine Denial of Service Vulnerability**
      - **Digital Certificate Authentication Bypass Vulnerability**
      - **Remote Access VPN Authentication Bypass Vulnerability**
      - **Digital Certificate HTTP Authentication Bypass Vulnerability**
      - **HTTP Deep Packet Inspection Denial of Service Vulnerability**
      - **DNS Inspection Denial of Service Vulnerability**
      - **AnyConnect SSL VPN Memory Exhaustion Denial of Service Vulnerability**
      - **Clientless SSL VPN Denial of Service Vulnerability**

  - **Cisco Firewall Service Module**
    - **cisco-sa-20131009-fwsm**
      - **Cisco FWSM Command Authorization Vulnerability**
      - **SQL*Net Inspection Engine Denial of Service Vulnerability**

Infos Réseau

- Cisco ISE
  - cisco-sa-20131023-ise
    - Exécution de commandes avant authentification …
- Cisco * (inclus CUPS, ISE, MXE, …)
  - cisco-sa-20131023-struts2
    - Exécution de commandes à distance via les failles Struts 2
- Cisco IOS XR
  - cisco-sa-20131023-iosxr
    - DoS fragmentation TCP
- Cisco IOS XE
  - cisco-sa-20131030-asr1000
    - DoS ICMP
    - DoS PPTP
    - DoS fragmentation TCP
    - DoS EoGRE

Infos Réseau

- **Faut-il avoir confiance dans son routeur SoHo ?**
  - **D-Link**
    - **http://www.devttys0.com/2013/10/reverse-engineering-a-d-link-backdoor/**
  - **Tenda**
    - **http://www.devttys0.com/2013/10/from-china-with-love/**
  - **NetGear WNDR3700v4 et WNDR4700**
    - **http://seclists.org/fulldisclosure/2013/Oct/182**
    - **http://seclists.org/fulldisclosure/2013/Oct/234**
  - **DD-WRT v24-SP2**
    - **http://seclists.org/fulldisclosure/2013/Oct/241**
  - **ASUS RT-N13U**
    - **http://seclists.org/fulldisclosure/2013/Oct/271**

Infos Réseau

- **Faille dans WatchGuard**
  - **"Stack overflow" sur un cookie de session trop long …**
    - **http://funoverip.net/2013/10/watchguard-cve-2013-6021-stack-based-buffer-overflow-exploit/**
- **Faille dans StrongSwan**
  - **Falsification d'identité**
    - **CVE-2013-6075**
- **Attaque pratique contre PHP / mt_rand**
    - **http://www.openwall.com/lists/announce/2013/11/04/1**

Infos Réseau

- **Autres infos**
  - **ICANN et IANA veulent se libérer du joug américain**
    - **http://www.icann.org/fr/news/press/releases/release-07oct13-fr**
  - **La carte des DDoS en temps réel**
    - **Joli … mais probablement pas scientifique**
      - **http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&time=16011&view=map**

Infos Unix

- (Principales) faille(s)
  - "Remote root" dans OpenSSH 6.2 et 6.3
    - Peut-être exploitable ☺
      - http://www.openssh.com/txt/gcmrekey.adv
  - Exploit publié pour CVE-2012-1823
    - Apache + PHP-CGI sur Debian et Ubuntu
      - http://www.exploit-db.com/exploits/29290/
  - Faille exploitable dans Aircrack-NG ☺
      - https://pyrit.wordpress.com/2010/03/28/remote-exploit-against-aircrack-ng/

Infos Unix

- **Autres infos**
  - **nf_tables passe dans le "trunk"**
    - **http://marc.info/?l=netfilter-devel&m=138176887917614&w=2**
  - **OpenBSD 5.4**
    - **http://undeadly.org/cgi?action=article&sid=20131101142807&mode=expanded&count=0**
  - **Debian 8.0 (Jessie) passe en "frozen"**
    - **http://lists.debian.org/debian-devel-announce/2013/10/msg00004.html**
  - **Ubuntu 13.10 (Saucy Salamander)**
    - **N'intègre pas Mir (le remplaçant de X11 à la sauce Ubuntu)**
      - **http://www.zdnet.com/ubuntu-13-10-saucy-salamander-review-smart-scopes-in-mir-out-7000022022/**
  - **Wordpress 3.7 apporte la mise à jour automatique**

Failles

- **Principales applications**
  - **Oracle Quaterly Patch**
    - **127 failles (dont 51 pour Java < 1.7.0_45) …**
      - **http://www.oracle.com/technetwork/topics/security/cpuoct2013-1899837.html**
  - **Adobe Reader < 11.0.05 (Windows)**
    - **Régression dans la configuration JavaScript**
      - **http://www.adobe.com/support/security/bulletins/apsb13-25.html**
    - **Crédit: Mario Heiderich**
  - **Flash Player 11.9 / AIR 3.9 … ne semblent pas être une mise à jour de sécurité**
  - **Firefox < 25**
    - **http://www.mozilla.org/security/known-vulnerabilities/firefox.html**
  - **Thunderbird < 24.1**
    - **http://www.mozilla.org/security/known-vulnerabilities/thunderbird.html**

Failles

- VMWare ESX
  - VMSA-2013-0012
    - http://www.vmware.com/security/advisories/
- Java …
    - http://seclists.org/fulldisclosure/2013/Oct/116
- Quelques techniques pour exploiter des failles malgré ASLR
    - http://www.fireeye.com/blog/technical/cyber-exploits/2013/10/aslr-bypass-apocalypse-in-lately-zero-day-exploits.html
- Contournement de toutes les options EMET grâce à une faille ShockWave
    - https://www.exodusintel.com/files/Aaron_Portnoy-Bypassing_All_Of_The_Things.pdf

Failles 2.0

- Toyota condamné pour la piètre qualité logicielle de son code embarqué
  - … ayant conduit à un accident mortel
    - http://www.edn.com/design/automotive/4423428/Toyota-s-killer-firmware--Bad-design-and-its-consequences
- HackerOne: un Bug Bounty pour les failles conceptuelles
  - Sponsorisé par Facebook et Microsoft
    - https://hackerone.com/
  - $2,500 pour une faille OpenSSL ☺
- Un bug logiciel fait perdre $172,222 par seconde
    - http://pythonsweetness.tumblr.com/post/64740079543/how-to-lose-172-222-a-second-for-45-minutes
- Le système de tracking des bateaux en mer
    - http://blog.trendmicro.com/trendlabs-security-intelligence/captain-where-is-your-ship-compromising-vessel-tracking-systems/
- Le système de *tracking* GPS des tigres du Bengale
  - Piraté par des braconniers
    - http://news.nationalgeographic.com/news/2013/10/131010-poaching-technology-tigers-endangered-animals-science/

Failles 2.0

- CIA: "la démarche de chaque personne peut être identifiée de manière unique grâce à l'accéléromètre de son téléphone portable"
  - http://www.businessinsider.com/cia-presentation-on-big-data-2013-3
- "Emergency Alerting System" … toujours vulnérable
  - http://blog.ioactive.com/2013/10/strike-two-for-emergency-alerting.html
- Yahoo! lance son Bug Bounty
  - http://yahoodevelopers.tumblr.com/post/65622522325/the-bug-bounty-program-is-now-live
- LinkedIn vous propose de faire "proxy IMAP" sur votre iPhone
  - http://pro.clubic.com/blog-forum-reseaux-sociaux/linkedin/actualite-595114-linkedin-enrichit-client-mail-ios-technologie-rapportive.html
- Votre site Web est-il "secure" ?
    - http://blog.whitehatsec.com/wp-content/uploads/Hackability-Index-090413_v2.jpeg

Sites piratés

- **Les sites piratés du mois (liste partielle)**
  - **LeaseWeb**
    - **Pour défigurer AVG, Avira et WhatsApp**
      - **http://news.softpedia.com/news/Avira-Confirms-Network-Solutions-Has-Been-Hacked-389422.shtml**
  - **Register.com**
    - **Pour défigurer ESET, BitDefender, et Rapid7 / Metasploit**
  - **… le tout par la même équipe (pro-palestinienne)**
  - **Adobe**
    - **Code source de tous les produits**
    - **130M comptes (mot de passe chiffré en 3DES-ECB)**
      - **http://www.hydraze.org/2013/10/some-information-on-adobe-135m-users-leak/**
      - **http://arstechnica.com/security/2013/11/how-an-epic-blunder-by-adobe-could-strengthen-hand-of-password-crackers/**
  - **International SOS**
    - **De nombreuses sociétés françaises sont clientes pour la gestion de leurs expatriés**
      - **http://www.businesstravelnews.com/Worldwide-Travel/Travel-Security-Firm-International-SOS-Victimized-By-Cyber-Attack/**

Sites piratés

- PHP.NET
- Les feux rouges à Haifa (Israël)
  - http://thehackernews.com/2013/10/israeli-road-control-system-hacked.html
- Buffer
  - http://thenextweb.com/socialmedia/2013/10/26/social-sharing-service-buffer-hacked-pauses-shares-temporarily/
- MongoHQ
  - http://security.mongohq.com/notice

Sites piratés

- vmbuild.apache.org
  - http://en.wooyun.org/bugs/wooyun-2013-06
- Generation-nt.com
  - Infecté par DarkLeech
- Healthcare.gov
  - http://money.cnn.com/2013/10/29/technology/obamacare-security/index.html
- AIEA
  - http://lexpansion.lexpress.fr/economie/l-aiea-fait-etat-d-une-nouvelle-attaque-informatique_408730.html

Malwares, spam et fraudes

- "BadBIOS"
  - FUD … ou technologie extraterrestre ?
    - Infection persistante du BIOS
    - Modification de la configuration du système d'exploitation (Windows, Linux, …)
    - C&C sur IPv6
    - Communication P2P via une implémentation *Software Defined Radio* (SDR) dans la carte son
    - …
      - https://plus.google.com/app/basic/stream/z13tzhpzvpqyuzv1n23cz52wykrrvjjce

- "Ploutus"
  - Le malware qui vide les distributeurs de billets …
    - http://www.symantec.com/connect/blogs/criminals-hit-atm-jackpot
    - http://blog.spiderlabs.com/2013/10/having-a-fiesta-with-ploutus.html

- Une puce malveillante … dans un fer à repasser ?
    - http://www.bbc.co.uk/news/blogs-news-from-elsewhere-24707337

Malwares, spam et fraudes

- **La station spatiale internationale infectée**
  - **Par une clé USB apportée par un russe ☺**
    - **http://www.ibtimes.co.uk/articles/521246/20131111/international-space-station-infected-malware-russian-astronaut.htm**
- **Les participants au G20 infectés par les russes**
  - **Au travers de clés USB et de chargeurs malveillants …**
    - **http://www.telegraph.co.uk/news/worldnews/europe/russia/10411473/Russia-spied-on-G20-leaders-with-USB-sticks.html**
    - **http://www.latimes.com/world/worldnow/la-fg-wn-russia-g20-summit-gifts-spy-devices-20131029,0,1499023.story**
- **Eric Filiol démissionne de EICAR**
    - **http://magazine.qualys.fr/marche-business/eric-filiol-demission-eicar/**

Malwares, spam et fraudes

- "CryptoLocker"
  - Cette fois-ci c'est $300 pour récupérer vos fichiers
    - http://nakedsecurity.sophos.com/2013/10/12/destructive-malware-cryptolocker-on-the-loose/
- "Blackhole" disparait progressivement d'Internet
  - … suite à l'arrestation de son auteur
    - http://www.f-secure.com/weblog/archives/00002622.html
- Mieux que "Zeus" ? "PowerZeus" ☺
    - http://www.cert.pl/news/7649/langswitch_lang/en
- Les banques anglaises vont réaliser un cyberexercice
  - "Waking Shark 2"
    - http://www.telegraph.co.uk/finance/newsbysector/banksandfinance/10359520/Banks-put-to-the-test-over-cyber-security.html

Actualité (francophone)

- Publications ANSSI
  - "Abusing anti-DDoS mechanisms to perform DNS cache poisoning"
    - 100Mb/s pendant 8h = 50% de chances de succès
      - http://www.ssi.gouv.fr/en/the-anssi/publications-109/scientific-publications/conference/abusing-anti-ddos-mechanisms-to-perform-dns-cache-poisoning.html
  - "0-Day: prévention et bonnes pratiques"
      - http://www.ssi.gouv.fr/IMG/pdf/guide_vulnerabilites_0day.pdf
  - "27 attaques majeures contre des entreprises françaises l'année dernière"
      - http://www.opex360.com/2013/10/29/lan-passe-27-cyberattaques-majeures-ont-ete-traitees-en-france/

- Loi de Programmation Militaire
  - L'ANSSI adoubée, contre-attaque, détention d'outils, reverse engineering, …
    - http://www.sgdsn.gouv.fr/site_article132.html
  - La police aura accès aux données de connexion en temps réel chez les opérateur
    - http://www.pcinpact.com/news/84026-cyberdefense-terrorisme-nouveaux-super-pouvoirs-pour-etat.htm

Actualité (francophone)

- **Le ministère de l'intérieur très satisfait de sa migration Outlook vers Thunderbird**
  - **http://www.pcinpact.com/news/83970-linterieur-vante-economies-dues-au-passage-d-outlook-a-thunderbird.htm**
- **Inauguration du CoFIS**
  - **Comité de la Filière Industrielle de Sécurité**
    - **http://www.gouvernement.fr/presse/installation-par-le-premier-ministre-du-comite-de-la-filiere-industrielle-de-securite**
- **APRIL vs. MinDef et Microsoft, suite**
  - **http://www.april.org/en/open-bar-contract-between-microsoft-and-french-ministry-defence-new-documents-support-political-game**
- **Orange obligé de démonter ses équipements Huawei**
  - **http://www.bfmtv.com/economie/gouvernement-part-chasse-contre-equipementiers-chinois-628920.html**

Actualité (francophone)

- DAVFI … c'est pour le 15 novembre
  - http://alx-communication.over-blog.com/article-le-consortium-davfi-annonce-en-avant-premiere-le-demonstrateur-de-la-solution-de-securite-davfi-andr-120642017.html
- CLUSIF vs. PCI-DSS
  - http://clusif.fr/fr/production/ouvrages/pdf/CLUSIF-2013-PCIDSS-Demarche-projet.pdf
- RENATER choisit CloudWatt
  - http://www.renater.fr/renater-choisit-cloudwatt-pour-la-mise-en-oeuvre
- Atos et OVH à la manœuvre dans le Cloud "souverain"
  - Cette fois-ci tout le monde est là
    - http://pro.clubic.com/it-business/cloud-computing/actualite-587810-atos-ovh-cloud-francais.html

Actualité (francophone)

- HADOPI n'a toujours pas indemnisé les FAI …
  - http://www.pcinpact.com/news/83907-hadopi-et-indemnisation-fai-lionel-tardy-entre-dans-boucle.htm
- Le site du zéro ferme
  - http://fr.openclassrooms.com/forum/sujet/demission-partielle-du-staff
- Vous voulez recruter des "hackers" ?
  - Hmm …
    - https://yeswehack.com/
- Un spot de sensibilisation pour le mois de la cybersécurité
  - Lancé par l'ISSA … et financé de manière collaborative
    - http://www.dailymotion.com/video/x15zh2u_spot-citizensec-cybersecmonth_tech

Actualité (francophone)

- Source
  - https://twitter.com/microsoftfrance/status/392603920989560832

Actualité (francophone)

- Source
  - https://twitter.com/bortzmeyer/statuses/394774162008707072

Actualité (anglo-saxonne)

- **PRISM: une actualité sans fin … (1/3)**
  - **De bonnes synthèses**
    - **http://www.tedgioia.com/nsa_facts.html**
    - **http://libwalk.so/liste-des-programmes-outils-nsa/**
  - **Les slides officiels**
    - **http://cryptome.org/2013/10/nsa-prism-13-1021.pdf**
  - **La France espionnée**
    - **Communications téléphoniques, Wanadoo, Alcatel-Lucent, …**
      - **http://www.lemonde.fr/technologies/article/2013/10/21/comment-la-nsa-espionne-la-france_3499758_651865.html**
    - **… et d'autres aussi**
      - **http://www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies**
  - **Les dirigeants européens espionnés**
    - **… mais les ministres français refusent d'utiliser leur téléphone chiffré ☺**
      - **http://www.seenthis.net/messages/190322**
      - **http://lecanardenchaine.fr/wp-content/uploads/2013/10/une_canard_30102013-S.png**
  - **.. mais la DGSE coopère étroitement avec la NSA depuis 2011**

Actualité (anglo-saxonne)

- **PRISM: une actualité sans fin … (2/3)**
  - **Google et Yahoo! cambriolés par la NSA**
    - **… pour poser des sondes sur les fibres du réseau interne**
      - **http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html**
  - **La NSA pirate aussi les chinois**
    - **http://www.theregister.co.uk/2013/10/18/snowden_china_spy_documents/**
  - **Le DataCenter de la NSA part en fumée**
    - **$2 milliards partis en fumée …**
      - **http://www.thefiscaltimes.com/Articles/2013/10/08/2-Billion-NSA-Spy-Center-Going-Flames**
  - **LavaBit est-il honnête ?**
    - **http://www.thoughtcrime.org/blog/lavabit-critique/**

Actualité (anglo-saxonne)

- **PRISM: une actualité sans fin … (3/3)**
  - **Le Luxembourg enquête sur Skype**
    - **… et la fuite de données vers la NSA**
      - **http://www.wort.lu/en/view/luxembourg-data-protection-commissioner-confirms-skype-probe-52582881e4b0127de7dda1b3**
  - **Les acteurs majeurs de l'Internet ne pourront rien révéler sur les interceptions légales**
    - **http://www.zdnet.fr/actualites/prism-il-n-y-aura-pas-plus-de-transparence-pour-les-geants-du-web-39794528.htm**
  - **Deutsche Telekom propose un réseau "PRISM-free"**
    - **http://www.thelocal.de/sci-tech/20131014-52385.html**
  - **La présentation de @tomchop à l'ISSA sur le sujet**
    - **http://tomchop.me/slideware/PRISM/**

Actualité (anglo-saxonne)

- **Source**
  - **https://twitter.com/ioerror/status/398059565947699200**

Actualité (anglo-saxonne)

- La DARPA vous donne $2m
  - Si vous pouvez corriger automatiquement les failles de sécurité dans les logiciels
    - http://www.theregister.co.uk/2013/10/22/darpa_sets_2_million_cash_prize_for_the_ultimate_vulnerability_scanner/

- La Grande-Bretagne va recruter des hackers
  - … même condamnés
    - http://www.telegraph.co.uk/technology/internet-security/10395348/Convicted-hackers-could-help-fight-cyber-crime-in-the-UK.html

Actualité (européenne)

- L'OTAN dispose d'un CIRC
  - … depuis octobre 2013
    - http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5324
- ENISA
  - Recommandations cryptographiques
    - https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report/at_download/fullReport
  - Documents de support pour les CERT
    - https://www.enisa.europa.eu/activities/cert/support/exercise
- Les hébergeurs ne sont pas que des tuyaux
    - http://libertescheries.blogspot.fr/2013/10/la-cour-europeenne-et-la-responsabilite.html?spref=tw

Actualité (Google)

- Un nouveau "Bug Bounty"
  - Améliorez la qualité du code Open Source
  - … et vous pourrez gagnez entre $500 et $3,133.7
    - http://googleonlinesecurity.blogspot.fr/2013/10/going-beyond-vulnerability-rewards.html
- Google Chrome sera supporté sur Windows XP jusqu'en 2015
  - http://googleenterprise.blogspot.fr/2013/10/extending-chrome-support-for-xp-users.html
- Google uProxy
  - Un proxy en P2P pour contourner la censure
    - http://mashable.com/2013/10/21/google-uproxy-internet-freedom/
- Project Shield
  - Pour héberger les sites susceptibles d'être DDoSés
    - http://mashable.com/2013/10/21/google-project-shield/
- Travailler chez Google ?
    - http://www.quora.com/Working-at-Google-1/Whats-the-worst-part-about-working-at-Google

Actualité (Google)

- Plus d'AdSense pour Numerama
  - Pour cause de seins nus
    - http://bigbrowser.blog.lemonde.fr/2013/10/22/censure-google-coupe-les-vivres-de-numerama-pour-une-photo-devoilant-des-seins-nus/

- "Android est plus sécurisé que l'iPhone"
  - Source: Eric Schmidt
    - http://www.pcinpact.com/news/82795-eric-schmidt-android-est-plus-securise-que-l-iphone.htm

- On peut trouver des données confidentielles dans le cache de Chrome
    - http://lastwatchdog.com/google-defends-chrome-browsers-security-settings/

Actualité (Apple)

- **iOS 7.0.3 (déjà)**
  - Pas de bulletin de sécurité
  - Changelog:
    - "Ajout du trousseau iCloud pour que vos noms de compte, mots de passe et numéros de carte bancaire soient mémorisés sur tous les appareils que vous avez autorisés"
    - "Ajout d'un générateur de mots de passe permettant à Safari de suggérer des combinaisons uniques et complexes pour vos comptes en ligne"
    - "Correction d'un problème permettant le contournement du code de l'écran de verrouillage"
    - "Résolution d'un problème pouvant faire que les appareils supervisés cessent de l'être lors d'une mise à jour de logiciel"
    - …

- **Mac OS X 10.9 (mise à jour gratuite)**
  - Inclus Safari 7.0
  - Quelques dizaines de failles corrigées
    - http://support.apple.com/kb/HT6011
    - "*If the kernel random number generator was not accessible to srandomdev(), the function fell back to an alternative method which had been removed by optimization, leading to a lack of randomness. This issue was addressed by modifying the code to be correct under optimization.*"
    - "*A format string vulnerability existed in Screen Sharing Server's handling of the VNC username.*"

Actualité (Apple)

- **Mise à jour Java**
  - http://support.apple.com/kb/HT5982
- **Le MITM est possible contre iMessage**
  - http://blog.quarkslab.com/imessage-privacy.html
  - https://github.com/quarkslab/iMITMProtect
  - https://www.youtube.com/watch?v=EbqZnTKDVU0
  - Rassurez-vous, Apple ne le fait pas ☺
    - http://www.imore.com/apple-says-theoretical-exploits-be-damned-they-cant-read-your-imessages
- **La maison de Steve Jobs classée monument historique**
  - http://www.lemonde.fr/economie/article/2013/10/30/la-maison-d-enfance-de-steve-jobs-classee-monument-historique_3505283_3234.html
- **iCloud**
  - Les sauvegardes sont en clair
  - … et ne peuvent pas être protégées par une authentification forte
    - http://www.zdnet.com/apples-icloud-cracked-lack-of-two-factor-authentication-allows-remote-download-7000022196/

Actualité (crypto)

- ~ 150 clés factorisées
  - … sur les 2,2m de cartes d'identité électronique taïwanaises
  - Signe d'un problème dans le générateur d'aléa
    - http://arstechnica.com/security/2013/09/fatal-crypto-flaw-in-some-government-certified-smartcards-makes-forgery-a-snap/
- Auditer TrueCrypt ?
  - Pourtant l'ANSSI lui a donné le CSPN ☺
    - http://blog.cryptographyengineering.com/2013/10/lets-audit-truecrypt.html
- Des courbes elliptiques "sûres"
    - http://safecurves.cr.yp.to/
- Nouvelles suites cryptographiques dans TLS
  - ChaCha20 et Poly1305
    - https://tools.ietf.org/html/draft-agl-tls-chacha20poly1305-01

Actualité

- Conférences passées
  - ASFWS 2013
    - http://fr.slideshare.net/ASF-WS/
  - Hack.Lu 2013
    - http://2013.hack.lu/archive/2013/
  - Congrès du CESIN
    - http://inscriptions.cesin.fr/
  - ZeroNights 2013
    - http://2013.zeronights.org/
  - Power of Community 2013
    - http://www.powerofcommunity.net/

Actualité

- Conférences à venir
  - GreHack 2013
    - 15 novembre
      - http://grehack.org/
  - C&ESAR 2013
    - 19-21 novembre
      - http://www.cesar-conference.org/?page_id=6&lang=fr
  - BotConf 2013
    - 5-6 décembre
      - https://www.botconf.eu/
  - AFCDP
    - 27 janvier 2014
      - http://www.globalsecuritymag.fr/Universite-AFCDP-des-CIL-du-27,20131020,40452.html
  - SSTIC 2014
    - Soumissions libres !
      - https://www.sstic.org/2014/news/CFP_SSTIC_2014/

Actualité

- **Sorties logicielles**
  - **Volatility 2.3**
    - **Support Mac OS X et Android**
      - **http://volatility-labs.blogspot.fr/2013/10/volatility-23-released-official-mac-os.html**
  - **MoonSols 2.0**
    - **http://www.moonsols.com/**
  - **LightBeam**
    - **Un add-on FireFox pour découvrir qui vous tracke sur Internet**
      - **https://addons.mozilla.org/en-US/firefox/addon/lightbeam/**

Actualité

- **Décès de Cédric "Sid" Blancher**
  - **Lors d'un saut en parachute**

Actualité

- Problèmes de recrutement ?
  - Ca n'est pas fini …
    - http://www.developpez.com/actu/63104/Les-jeunes-se-desinteressent-de-l-industrie-de-la-cybersecurite-un-secteur-ou-bien-souvent-l-offre-est-superieure-a-la-demande/
- Très bonne réflexion sur les conférences de sécurité …
  - http://thinkst.com/stuff/44Con_2013/talk_about_talks.pdf
- Gartner: "BlackBerry est mort"
  - http://www.computerworld.com/s/article/9242767/Update_Gartner_tells_IT_shops_that_it_s_game_over_for_BlackBerry
- Le premier ATM … qui délivre des bitcoins
  - http://blog.malwarebytes.org/cyber-crime/2013/10/worlds-first-bitcoin-atm-comes-to-canada/
- Archive.org a brûlé
  - Heureusement il existe des backups
    - https://blog.archive.org/2013/11/06/scanning-center-fire-please-help-rebuild/

Divers

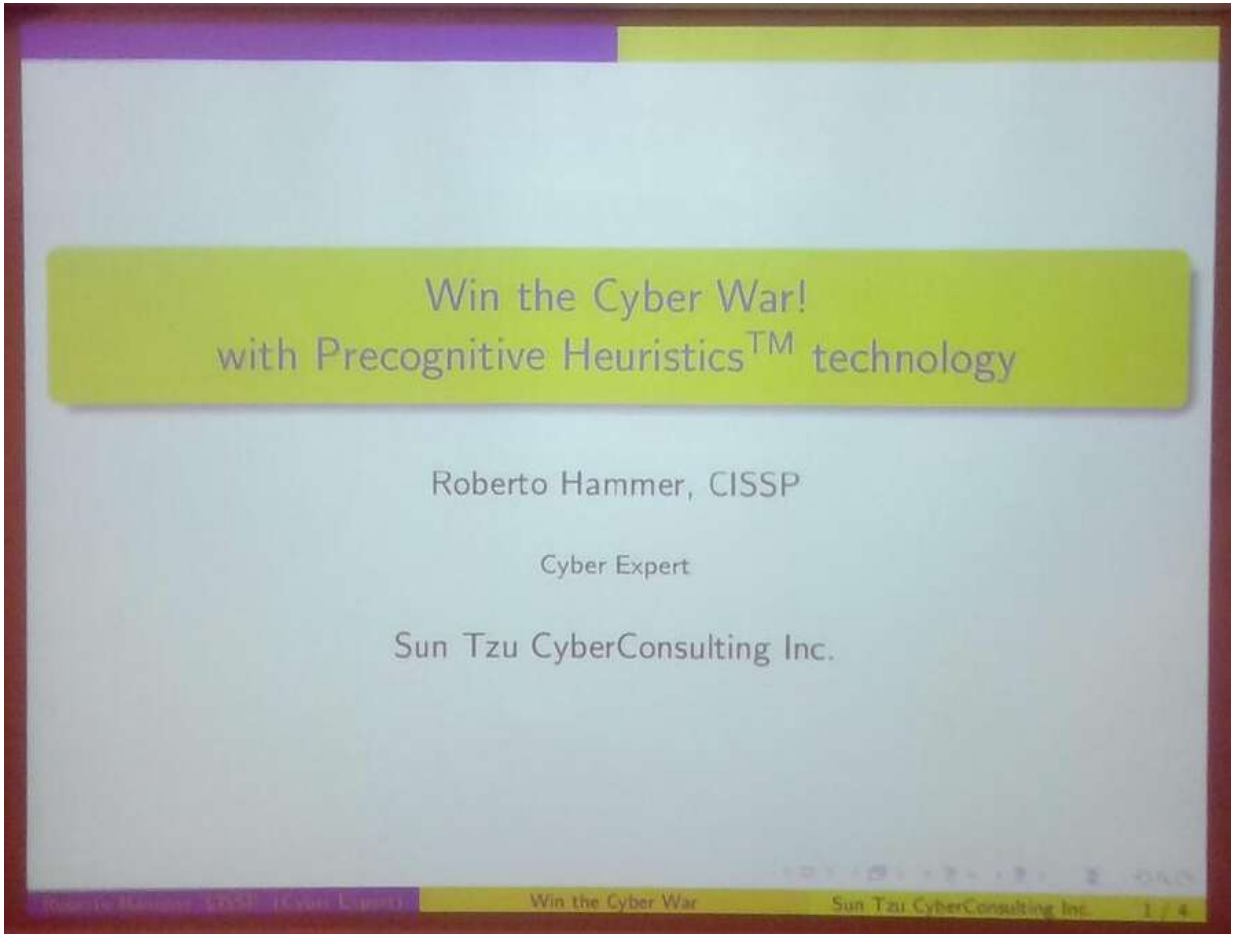
- Le créateur de l'ISO 27000 trolle ISO 27000
  - "*compliance is killing security innovation*"
    - http://www.tripwire.com/state-of-security/regulatory-compliance/david-lacey-whats-wrong-todays-iso27k-standards/
- Une application pour soigner l'acné ?
  - … ou pas
    - http://www.nbcnews.com/id/44440180/ns/business-consumer_news/t/ftc-treating-acne-no-there-no-app/
- Une JVM en node.js
    - https://github.com/YaroslavGaponov/node-jvm
- Mario en HTML5
  - (Déjà victime de DMCA)
    - http://www.fullscreenmario.com/

Divers

- **Bienvenue au DAAS**
  - **http://devnull-as-a-service.com/**
- **La barbe est à la mode de Paris**
  - **http://www.lefigaro.fr/sortir-paris/2013/10/08/30004-20131008ARTFIG00450-les-barbus-de-paris.php**
- **Binary under pressure**
  - **http://toys.usvsth3m.com/binary/**
- **…**
  - **http://superuser.com/questions/231273/what-are-the-windows-a-and-b-drives-used-for/231278**
- **Le saviez-vous ?**
  - **http://stackoverflow.com/questions/19210935/why-does-the-c-preprocessor-interpret-the-word-linux-as-the-constant-1**

Divers

- **Source:**
  - **https://twitter.com/joernchen/status/393700097722437632/photo/1**



Divers

- **Unicode U+1F595**

Browser Test Page
Outline (as SVG file)
Fonts that support U+1F595

Encodings	
HTML Entity (decimal)	🖕
HTML Entity (hex)	🖕
How to type in Microsoft Windows	Alt +1F595
UTF-8 (hex)	0xF0 0x9F 0x96 0x95 (f09f9695)
UTF-8 (binary)	11110000:10011111:10010110:10010101
UTF-16 (hex)	0xD83D 0xDD95 (d83ddd95)
UTF-16 (decimal)	55 357 56 725
UTF-32 (hex)	0x0001F595 (1f595)
UTF-32 (decimal)	128 405
C/C++/Java source code	"\uD83D\uDD95"
Python source code	u"\U0001F595"
More...	

Divers

- telnet://107.21.219.86

Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 10 décembre 2013
- Prochaine JSSI
  - Lundi 17 mars 2014
  - Profitez du combiné avec les GS-Days le mardi 18 mars
- N'hésitez pas à proposer des sujets et/ou des salles