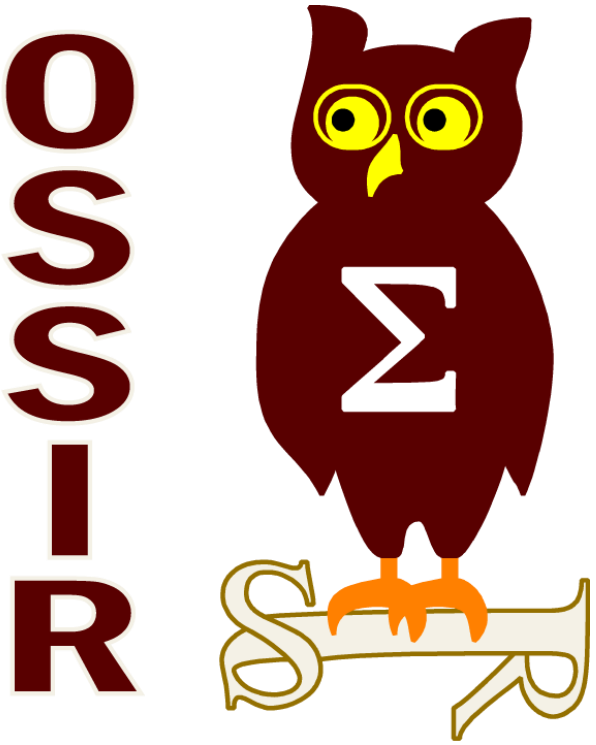


Groupe Paris

Revue d'actualité du 08/04/2014

Jean-Philippe GAULIER
Ary KOKOS
Vladimir KOLLA
Arnaud SOULLIE

Bulletins Microsoft

Février 2014

MS14-005 Faille dans Microsoft XML Core Services (1 CVE) [1]

- Affecte: Windows (toutes versions supportées)
- Exploit: Lecture de fichiers locaux chez la cible navigant sur un site exploitant la vulnérabilité (CVE-2014-0266)
- Crédits: FireEye, Inc.

MS14-006 Déni de service sur IPv6 (1 CVE) [1]

- Affecte: Windows 8 / 2012 / RT / Core
- Exploit: Similaire au vieux WinNuke par l'envoi massif de Router Advertisement" en IPv6 aboutissant à un BSOD (CVE-2014-0266)
- Crédits: Révélé publiquement fin 2012 http://samsclass.info/ipv6/proj/projL9-flood-router.htm

MS14-007 Faille dans Direct2D (1 CVE) [Exploitabilité 1]

- Affecte: Windows 7 / 8.x / 2012 / RT
- Exploit: Exécution de code à l'ouverture d'une page Web malformée appellant Direct2D (drive-by)
- Crédits: Omair / ZDI

Bulletins Microsoft

MS14-008 Faille dans Forefront pour Exchange (1 CVE) [Exploitabilité 2]

- Affecte: Microsoft Forefront Protection 2010
- Exploit: Exécution de code lors du traitement par Forefront avec les droits Forefront
- Crédits: Détectée en interne durant une analyse de code mais sans réussir à développer un exploit
  http://blogs.technet.com/b/srd/archive/2014/02/11/assessing-risk-for-the-february-2014-security-updates.aspx

MS14-009 Failles dans .Net (3 CVE) [Exploitabilité 1,1,1]

- Affecte: .NET Framework (Quasiment toutes versions supportées)
- Exploit:
  - Déni de service avec une attaque du type SlowPost (CVE-2014-0253)
  - Type Traversal (CVE-2014-0257)
  - bypass ASLR en appelant la librairie VsaVb7rt.dl (CVE-2014-0295)
    http://www.greyhathacker.net/?p=585
- Crédits: James Forshaw / Contextis (CVE-2014-0257)

Bulletins Microsoft

MS14-010 Correctif cumulatif pour IE (24 CVE) [Exploitabilité 1]

- Affecte: IE 6 à 11 (Toutes versions supportées)
- Exploit:
  - 22 exécutions de code à l'ouverture d'une page Web malformée (dont une relevée publiquement)
  - Une élévation de privilèges locale (CVE-2014-0268)
  - Corruption de mémoire VBScript (CVE-2014-0271)
  - Fuite d'information cross-domain ou cross-zone (CVE-2014-0293)
- Crédits:
  - 5 x Bo Qu of Palo Alto Networks
  - 4 x Simon Zuckerbraun / ZDI
  - 4 x Scott Bell / Security-Assessment.com
  - 2 x Arthur Gerkis / ZDI
  - 2 x lokihardt@ASRT / ZDI
  - 2 x Sachin Shinde
  - Code Audit Labs of VulnHunt
  - cons0ul and suto / ZDI
  - Dieyu dieu deus deva divine dio theos dievas dewa ilu Diyin Ayóo Át'éii atua tianzhu Yahweh Zeus Odin El
  - James Forshaw / Contextis
  - Jose A. Vazquez of Yenteasy / ZDI
  - Liang Chen of KeenTeam (@K33nTeam)
  - Peter 'corelanc0d3r' Van Eeckhoutte / Corelan
  - Yuki Chen / Trend Micro
  - Zhibin Hu / Qihoo

Bulletins Microsoft

MS14-011 Faille dans VBScript (1 CVE) [Exploitabilité 1]

- Affecte: VBScript 5.6 à 5.8 (Toutes versions supportées) donc tous OS Microsoft avec ces versions
- Exploit: Exécution de code à l'ouverture d'une page Web malformée appellant VBScript
- Crédits: n/a

Bulletins Microsoft

Mars 2014

MS14-012 Correctif cumulatif pour IE (18 CVE) [Exploitabilité 1]

- Affecte: IE 6 à 11 (Toutes versions supportées)
- Exploit: Exécutions de code à l'ouverture d'une page Web malformée dont 2 utilisées dans des attaques ciblées (une pour IE8 et une pour IE10)
- Crédits:
  - 4 x Bo Qu / Palo Alto Networks
  - 3 x lokihardt@ASRT / ZDI
  - 2 x Amol Naik / VeriSign iDefense Labs
  - 2 x Jason Kratzer / ZDI
  - 2 x Yujie Wen / Qihoo
  - Anil Aphale
  - FireEye, Inc.
  - Hui Gao / Palo Alto Networks
  - Jose A. Vazquez / Yenteasy (par ZDI)
  - Omair / ZDI
  - Scott Bell / Security-Assessment.com
  - Simon Zuckerbraun / ZDI
  - Tianfang Guo / Palo Alto Networks
  - Zhibin Hu / Qihoo

Bulletins Microsoft

MS14-013 Faille dans le support JPEG par DirectShow qedit.dll (24 CVE) [Exploitabilité 3]

- Affecte: Windows toutes version sauf Itanium, RT (Arm) et Server Core
- Exploit: Corruption mémoire conduisant à l'exécution de code à la visualisation d'une image JPEG malformée, rendue par DirectShow (qedit.dll)
  https://blogs.technet.com/b/srd/archive/2014/03/11/assessing-risk-for-the-march-2014-security-updates.aspx
- Crédits: anonymous / VeriSign iDefense Labs

MS14-014 Faille dans Silverlight (1 CVE) [Exploitabilité 1]

- Affecte: Silverlight 5 pour Windows et Max OS X ;-)
- Exploit: Contournement des sécurités DEP et ASLR en cas de combinaison avec une faille d'execution de code
- Crédits: NSFOCUS Information Technology (CVE-2014-0319)

MS14-015 Faille WIN32K.SYS (2 CVE) [Exploitabilité 1]

- Affecte: Windows (toutes versions supportées) même RT
- Exploit: Deux élévations de privilèges dont une revélée publiquement
- Crédits: Alexander Chizhov (CVE-2014-0323)

MS14-016 Faille Security Account Manager Remote (SAMR) (1 CVE) [Exploitabilité 1]

- Affecte: Windows toutes version sauf Itanium, 7, 8 et RT
- Exploit:
  - Contournement de la sécurité permettant de tenter un brute force sur un password sans déclencher les règles/politiques de vérouillage
  - Uniquement si déjà authentifié
- Crédits: Andrew Bartlett / Samba Team (CVE-2014-0317)

Bulletins Microsoft

Révisions

- MS14-005
  - V1.1: Changement du mode de detection dans Windows 8.1 et 2012 R2
- MS14-008
  - V1.1: Révision du niveau d'exploitabilité pour la CVE-2014-0294
- MS14-011
  - V1.2: Révision du niveau d'exploitabilité pour la CVE-2014-0271

Infos Microsoft

- Windows 8.x un OS sûr ;-)
  - DEP + ASLR + HEASLR + Null page allocating = OS plutôt robuste
    http://www.welivesecurity.com/2014/02/11/windows-exploitation-in-2013/

- Satya Nadella devient CEO de Microsoft
  http://www.microsoft.com/en-us/news/ceo/index.html

- Quand Microsoft demande d'acheter une nouvelle licence si vous changez la carte mère de votre ordinateur !
    http://www.courrier-picard.fr/accueil/le-geant-microsoft-contre-un-petit-vendeur-informatique-ia0b0n309007
  - ... et le délibéré
    http://rue89.nouvelobs.com/2014/03/13/microsoft-perd-proces-contre-petite-societe-picarde-250639

- Chemins de lecture de MS Word 13
  - Un atout pour le Forensique ;-)
    http://dfstream.blogspot.fr/2014/01/ms-word-2013-reading-locations.html

Infos Microsoft

- Le sénat examine l'accord openbar de Microsoft et de l'armée
  http://www.pcinpact.com/news/86200-le-contrat-open-bar-entre-microsoft-et-defense-sous-prisme-senat.htm

- Le Computer History Museum expose le code source historique de Microsoft MS-DOS et Word
  http://www.computerhistory.org/press/ms-source-code.html

- La SEA diffuse des factures de Microsoft à destination du FBI
  http://www.undernews.fr/libertes-neutralite/espionnage-la-sea-diffuse-des-factures-de-microsoft-a-destination-du-fbi.html

Infos Microsoft

Fin du support de Windows XP (aujourd'hui !!)

- Pose un réel problème aux banques et leur DAB / GAB / ATM

- Entre 2 et 3 millions de distributeurs de billets à travers le monde, dont 95% seraient sous Windows XP
  - Certains pensent même passer sous Linux
    http://www.linformaticien.com/actualites/id/32507/avec-la-fin-de-windows-xp-les-dab-bientot-sous-linux.aspx

- La migration ou la prolongation du support pourrait couter entre 50 et 60 millions de livres à chaque banque anglaise
  http://microsoft-news.com/banks-paying-microsoft-millions-in-support-costs-for-refusing-to-upgrade-atms-running-windows-xp/

- Quelques cas :
  - Bank of America, **18 000** DAB, négocie avec Microsoft pour prolonger le support
  - Barclays, **4 300** DAB, négocie avec Microsoft pour prolonger le support
  - BNP, **6 000** DAB en France, migre sous Windows 7 (fin de support en 2020, pas si loin que ca ^_^)
  - Citigroup, **12 000** DAB, migre sans donner plus de détails
  - HSBC, **3 200** DAB, migre sous Windows 7 mais prolonge le support le temps de la migration (surement comme beaucoup d'autres)
  - JPMorgan, **19 200** DAB, migre sous Windows 7
  - Lloyds Bank, **7 000** ATM, prolonge le support jusqu'en 2016
  - Royal Bank of Scotland, **9 000** DAB, migre sous Windows 7 mais prolonge le support
  - Société Générale, **5 000** DAB, migre sous Windows 7 mais prolonge le support

Infos réseau

(Principales) Faille(s)

- Execution de commande pour un utilisateur authentifié sur Cisco Prime
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140226-pi
- Accès root pour un utilisateur non-authentifié sur les AP Wifi
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140110-sbd
- Faille lors de la translation de paquets IP
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140326-nat
- Et pas mal d'autres…
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140326-RSP72010GE
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140326-ipv6
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140326-ios-sslvpn
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140326-sip

Infos réseau

Autres infos

- McAfee rachète StoneSoft
  http://www.mcafee.com/us/about/mcafee-stonesoft.aspx

- TeleHouse
  - Panne des climatiseurs sur le Datacenter TeleHouse 2 (75011), le 9 mars au soir

- Cisco
  - Rappel de matériel vendus entre 2005 et 2010 (stocks vendus jusqu'en 2012)
  - Mémoire défaillante se traduisant par une corruption durant une mise à jour ou un reboot
  - Remplacement des produits hors garantie estimé à $655 millions
    http://www.cisco.com/web/about/doing_business/memory.html#~overview
    http://www.cisco.com/web/about/doing_business/memory.html#~field

Rapports Annuels

C’est la saison des Panoramas ou Rapports annuels sur 2013

- La Cyber Criminalité par le Clusif https://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-2014-Panorama-cybercriminalite-annee-2013-Synthese.pdf

- The State of the Internet 2013Q3 , “selon” Akamai
  - Les pays à l’origine du plus gros trafic malveillant sont, dans l’ordre : la Chine, l’Indonésie puis les USA
  - Les ports les plus attaqués sont : TCP 445 (SMB), TCP 80 (HTTP), TCP 443 (HTTPS) puis TCP 1433 (MS SQL)
  - IPv6 est toujours loin d’être généralisé
  - La Corée du Sud dispose toujours du débit moyen le plus important (22,1Mbps) http://www.akamai.com/dl/akamai/akamai-soti-q313.pdf

- Rapport Kaspersky sur les malwares en 2013 https://www.securelist.com/en/analysis/204792318/Kaspersky_Security_Bulletin_2013_Overall_statistics_for_2013

- Rapport du RAND sur la CyberCriminalité http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf

Rapports Annuels

- Le cout de la CyberCriminalité en 2013 dans le monde
  - 110 Milliards d'euros en 2013 dans le monde
    http://www.lemondeinformatique.fr/actualites/lire-la-cyber-criminalite-a-coute-110-mdeteuro-en-2013-56489.html
  - Dell annonce qu'en moyenne, la CyberCriminalité couterait $1 million à chaque entreprise
    http://www.developpez.com/actu/67893/La-cyber-criminalite-coute-pres-d-un-million-de-dollars-par-an-aux-entreprises-d-apres-un-rapport-publie-par-Dell/

- Rapport annuel Arbor 2013 sur le DDoS
  http://www.arbornetworks.com/resources/infrastructure-security-report

- Tendances sur le phishing pour Q3 2013
  http://www.antiphishing.org/resources/apwg-reports/

Infos Unix

(Principales) Faille(s)

- Faille depuis 23 ans dans X11
  - Stack overflow et élévation de privilège locale
  - sscanf encore responsable
    http://lists.x.org/archives/xorg-announce/2014-January/002389.html

- Vulnérabilités dans les drivers 3D d'Oracle VirtualBox
  - Possibilité de prendre le contrôle de la machine hôte
    http://seclists.org/fulldisclosure/2014/Mar/95

- Vulnérabilités & backdoor dans les appliances Dell KACE K1000
  http://console-cowboys.blogspot.fr/2014/03/the-curious-case-of-ninjamonkeypiratela.html

- Faille Linux / KVM et exécution du code sur l'hyperviseur depuis la VM
  http://seclists.org/oss-sec/2014/q1/468

Infos Unix

Autres infos

- CentOS rejoint RedHat pour « développer et adopter les technologies open source next-generation » !
  http://pro.01net.com/editorial/611474/linux-red-hat-integre-la-communaute-centos/

Failles

- Exploitation de failles USB à distance grâce à RDP et RemoteFX
  https://www.nccgroup.com/media/481258/usb_physical_access_andy_davis_ncc_group_slides.pdf

- VMWare VMSA-2014-0002
  - “MON_GETLIST” activé par défaut sur le service NTP (CVE-2013-5211)
  - Mise à jour Oracle JRE 1.7 Update 45
  - Integer overflow dans libc (CVE-2013-4332)
    https://www.vmware.com/security/advisories/VMSA-2014-0002.html

Failles

- Multiples failles chez Barracuda (XSS, crash...)
  http://packetstormsecurity.com/files/125440/Barracuda-Networks-Backup-Appliance-Cross-Site-Scripting.html
  http://packetstormsecurity.com/files/125426/Barracuda-Web-Firewall-6.1.0.016-Cross-Site-Scripting.html
  http://packetstormsecurity.com/files/125395/Barracuda-Networks-Firewall-Filter-Bypass.html
  http://packetstormsecurity.com/files/125346/Barracuda-Firewall-Exception-Handling-Cross-Site-Scripting.html
  http://packetstormsecurity.com/files/125328/Barracuda-Networks-Web-Firewall-X300-Cross-Site-Scripting.html
  http://packetstormsecurity.com/files/125310/Barracuda-Message-Archiver-650-Cross-Site-Scripting.html

- Barracuda ouvre sa base de sites considérés comme malveillants ou compromis
  - Avec du .gouv.fr dedans http://www.threatglass.com/tiles?query=gouv.fr

- Pour rappel, en 2013, Barracuda laissait un compte SSH activé et caché sur ses appliances
  http://feedproxy.google.com/~r/KorbensBlog-UpgradeYourMind/~3/dIn7aL2fxHw/une-backdoor-dans-le-materiel-reseau-barracuda.html

Failles

- GotoFail : Apple Mac OS X et iOS (<6.1.6 et <7.0.6)
  - Une ligne de code doublée (« goto fail; »)
  - Présent depuis septembre 2012 dans l'implémentation SSL d'Apple : SecureTransport.
  - SecureTransport est Open Source, échec de l'auditabilité ?
  - Résultat : usurpation d'identité sur ssl et MitM possible
    http://www.zdnet.fr/actualites/goto-fail-la-vulnerabilite-tres-etonnante-d-apple-39798118.htm
  - Pour tester : https://gotofail.com/
  - Failles 2.0

- GotoFail : GnuTLS
  - Présent depuis 2005
  - Résultat : usurpation d'identité sur ssl et MitM possible
    http://arstechnica.com/security/2014/03/critical-crypto-bug-leaves-linux-hundreds-of-apps-open-to-eavesdropping/

- Backdoor Fail : La backdoor de la NSA dans OpenSSL n'a jamais marché
  - Pour être FIPS 140-2, il faut implémenter Dual EC DRBG
  - Implémentation d'OpenSSL était bugée et n'a jamais marché :-)
  - Pas de correctif prévu ;-)
    http://marc.info/?l=openssl-announce&m=138747119822324&w=2

Failles 2.0

- Oracle
  - Détails techniques sur les vulnérabilités Oracle VirtualBox de janvier http://seclists.org/fulldisclosure/2014/Feb/48
- Vulnérabilité XSS sur Office365
  - Permet à tout utilisateur de devenir Administrateur du compte Office365 de son groupe
  - Vidéo impressionnante, beau travail d'exploitation et de post-exploitation http://threatpost.com/details-on-patched-microsoft-office-365-xss-vulnerability-disclosed/103714
- D'un XSS à un shell sur le Cloud : Write-Up de vulnérabilités sur OwnCloud http://blog.noobroot.com/2014/02/owncloud-600a-when-xss-vulnerability.html
- Exécution de code à distance sur le manager SEP (Symantec Endpoint Protection) http://www.exploit-db.com/exploits/31853/
- Désactivation de Find My iPhone sans avoir le mot de passe iCloud http://www.theinquirer.net/inquirer/news/2327573/ios-7-exploit-disables-find-my-iphone-without-a-password
- 78% des cambrioleurs repèrent avec FaceBook, Twitter et Foursquare http://blog.hiscoxpro.fr/risques-de-cambriolage-pendant-les-fetes-78-des-voleurs-utilisent-facebook-twitter-et-foursquare-pour-faire-du-reperage-avant-un-vol/

Failles 2.0

- iOS : FireEye a découvert une faille permettant d'enregistrer toutes les actions d'un utilisateur
  http://www.fireeye.com/blog/technical/2014/02/background-monitoring-on-non-jailbroken-ios-7-devices-and-a-mitigation.html

- iOS : PRNG avec seulement 2^19 possibilités (524 288)
  http://blog.azimuthsecurity.com/2014/03/attacking-ios-7-earlyrandom-prng.html

- L'OS caché de nos smartphones avec backdoor baseband chez Samsung
  - La puce baseband des Smartphones Samsung permet de communiquer avec l'OS (Android) et de le contrôler
    https://www.fsf.org/blogs/community/replicant-developers-find-and-close-samsung-galaxy-backdoor

- Faille majeure chez Android
  - Pour l'exploiter, fournissez une vieille application ;-)
    http://www.silicon.fr/un-milliard-de-terminaux-android-touches-par-une-faille-de-securite-sans-precedent-93389.html?ModPagespeed=noscript

- Bell Canada victime d'une sqli
  http://www.databreaches.net/nullcrew-attack-on-bell-canada-was-sql-injection-and-bell-knew-weeks-ago-nullcrew/

Failles 2.0

- Base de 360 millions de comptes à vendre
  http://www.cnet.com/news/black-market-lights-up-with-360m-stolen-credentials-report/
  - Il y'aurait même une base à vendre contenant 1 milliard d'adresses mail !
- Les vulnérabilités du web les plus connues et la réponse via node.js
  https://speakerdeck.com/ckarande/top-overlooked-security-threats-to-node-dot-js-web-applications
- 300 000 routeurs exploités par des pirates
  http://www.datasecuritybreach.fr/300-000-routeurs-exploites-par-des-pirates/
- Twitter corrige un problème sur les comptes protégés
  http://www.pcinpact.com/news/86395-twitter-colmate-faille-touchant-93-788-comptes-proteges.htm
- APT, le nouveau standard
  http://nakedsecurity.sophos.com/advanced-persistent-threats-the-new-normal/
- Use after free chez Google Chrome
  http://www.securityfocus.com/bid/66243
- Hack d'Oracle, Prezi, Yahoo dans le cloud par Nicolas Grégoire
  http://www.agarri.fr/docs/Easy_hacks_for_complex_apps-INS14.pdf

Failles 2.0

- Vol de 20 et 100 millions de numéros de CB en Corée du Sud chez Korea Credit Bureau
  - Un consultant indélicat a récupéré sur une clef USB et sur 6 mois, les noms, numéros de sécurité sociale et numéros de CB de 20 millions de clients. http://www.theregister.co.uk/2014/01/22/sk_data_breach_apology/
  - Interdiction d'émettre des CB pendant 3 mois http://www.moneticien.com/veille-monetique/coreedusud-104-millions-de-cartes-volees-trois-banques-sanctionnees/
  - Mais de belles excuses. Notez le degré d'inclinaison :

Failles 2.0

- Exploitation de failles des routeurs Soho (cf. Actu de novembre 2013)
  - Le CERT Polonais a détecté des attaques massives sur ces routeurs https://www.networkworld.com/news/2014/020714-cybercriminals-compromise-home-routers-to-278566.html
- Spearfishing (avec succès) contre l'Administration Civile de la défense Israélienne http://www.linformaticien.com/actualites/id/31827/piratage-d-ordinateurs-de-la-defense-israelienne.aspx
- Ecouter les conversations grâce à Chrome
  - Toujours pas de correctif au moment où j'écris ces lignes http://www.01net.com/editorial/612618/la-reconnaissance-vocale-de-google-chrome-peut-espionner-vos-conversations/
- Des serveurs PHP vulnérables à une faille vieille de 2 ans
  - 16% des 244 millions de serveurs PHP, seraient vulnérables à la faille PHP CGI de 2012 http://www.scmagazine.com/unpatched-servers-still-enabling-exploitation-of-two-year-old-php-vulnerability/article/338973/

Failles 2.0

- Comment Facebook détecte si vous êtes célibataire ou en couple
  http://www.theatlantic.com/technology/archive/2014/02/when-you-fall-in-love-this-is-what-facebook-sees/283865/
- Créer un DDoS via Google Docs
  http://korben.info/google-ddos.html
- Backdoor PHP astucieuse et discrète
  @extract ($_REQUEST);
  @die ($ctime($atime));
  http://blog.sucuri.net/2014/02/php-backdoors-hidden-with-clever-use-of-extract-function.html
- Encore une belle preuve d'implémentation cryptographique maison chez Linksys
  http://www.devttys0.com/2014/02/cracking-linksys-crypto/

Failles 2.0

Dernière minute : vulnérabilité HeartBleed dans OpenSSL

Exploite une vulnérabilité dans l'implémentation du heart-beat TLS dans openSSL
L'exploitation permet de récupérer, par blocs de 64k, des données en mémoire sur le serveur

- Jetons de sessions
- Configuration
- Clé privée associée au certificat x.509

http://heartbleed.com/

Sites piratés

- Les militaires américains ciblés par une attaque “Watering Hole”
  - Avec utilisation d’un 0-day pour Internet Explorer 10
    http://www.securityweek.com/new-ie-10-zero-day-used-watering-hole-attack-targeting-us-military
  - Les industriels de l’aéronautique français également ciblés via le site du Gifas (Groupement des Industries Françaises Aéronautiques et Spatiales)
    http://www.developpez.com/actu/67655/Une-faille-zero-day-dans-IE-9-et-10-exploitee-pour-cibler-les-sites-de-la-defense-americaine-et-de-l-aeronautique-francaise/

- Kickstarter piraté
  - Mot de passe stocké en SHA-1 avec sel pour les plus anciens, bcrypt pour les plus récents
    http://blogs.csoonline.com/malwarecybercrime/2994/kickstarter-hacked
    https://www.kickstarter.com/blog/important-kickstarter-security-notice

- Le W3C piraté
  http://www.w3.org/blog/2014/03/w3c-password/

- Remonter les alertes c'est bien, les regarder c'est mieux !
  - Une intrusion chez Neiman Marcus pendant 8 mois
  - Vol d’un peu plus d’un million de données personnelles
  - Plus de 60 000 alertes mais pas de réaction
    http://www.businessweek.com/articles/2014-02-21/neiman-marcus-hackers-set-off-60-000-alerts-while-bagging-credit-card-data

Sites piratés

- L'espace éducation de FranceTv piraté
  http://www.zataz.com/news/23268/france-tv--faille--xss.html
- UK National Health Service Hacked, Site Set Up to Serve Malware (Updated)
  http://news.softpedia.com/news/UK-National-Health-Service-Hacked-Site-Set-Up-to-Serve-Malware-423282.shtml
- Le DNS 8.8.8.8 de google a été hijacké via BGP pendant 22 minutes
  http://thehackernews.com/2014/03/google-public-dns-server-traffic.html

Malwares, spam, fraudes et DDoS

- Mask / Careto , non détecté pendant 7 ans
  www.securelist.com/en/downloads/vlpdfs/unveilingthemask_v1.0.pdf
  - Utilisé pour réaliser de l'espionnage contre près de 31 pays
  - Disponible pour Windows 32bits, Windows 64bits, Mac OSX, Linux, Android et iOS
  - Signé par un certificat sans doute volé
  - Infectant un utilisateur grâce à des failles dans à peu près tous les domaines (Java, Flash, Chrome, Firefox…)
  - La faille utilisée pour Chrome est la CVE-2012-0773, utilisée par VUPEN pour gagner Pwn2Own 2012. Non vendue à Google pour $100k
    http://news.softpedia.com/news/Vupen-Sells-Exploits-to-Spy-Agencies-They-Pay-Much-More-than-Google-260058.shtml

- Skimming en bluetooth dans le distributeur
  - Boitier directement dans le système de lecteur de CB, communiquant en Bluetooth avec l'escroc
  - Trouvé aux Etats-Unis, dans des pompes à essence
    http://www.gizmodo.fr/2014/01/28/piratage-cb-appareil-bluetooth-dans-machine.html
  - Plus difficile à faire dans nos distributeurs emmurés

- Trouver des malware en fouillant la mémoire par une autopsie
  http://blog.eforensicsmag.com/finding-malware-using-memory-forensics

Malwares, spam, fraudes et DDoS

- Un vers se propage sur les routeurs Linksys
  https://isc.sans.edu/forums/diary/Linksys+Worm+TheMoon+Captured/17630
  http://www.reddit.com/r/netsec/comments/1xy9k6/that_new_linksys_worm/

- Prix des services du marché noir
  - $300 pour des comptes avec, au total, entre $70 000 et $150 000 d'avoir
  - Entre $2 et $5 de l'heure pour un DDoS
  - $100 à $300 pour hacker un site web... quand on voit le prix d'un audit
    http://robertsiciliano.com/blog/2014/01/27/stolen-identities-are-cheap-on-the-darknet/

- Linux aussi fait de bons botnets
  - 25 000 serveurs Linux infectés
    http://www.welivesecurity.com/2014/03/18/operation-windigo-the-vivisection-of-a-large-linux-server-side-credential-stealing-malware-campaign/
    http://www.zdnet.com/botnet-of-thousands-of-linux-servers-pumps-windows-desktop-malware-onto-web-7000027472/

- Selon Mandiant, SI compromis = seulement 54% de machines infectées
  http://magazine.qualys.fr/menaces-alertes/malwares-detection-mandiant/

Malwares, spam, fraudes et DDoS

- La Corée du Sud se met au malwares (virus) comme Stuxnet
  http://nakedsecurity.sophos.com/2014/02/24/south-korea-concocting-stuxnet-like-virus-to-infect-enemies/

- Uroburos (Ouroboros) un malware du gouvernement Russe actif depuis 2008
  - Mais pas le premier, contrairement à ce qui est dit dans l'article
    https://blog.gdatasoftware.com/blog/article/uroburos-highly-complex-espionage-software-with-russian-roots.html
    http://www.itespresso.fr/uruburos-g-data-rootkit-russe-espionnant-entreprises-73321.html

- Le DDoS utilisé pour masquer une intrusion
  http://www.globalsecuritymag.fr/Les-attaques-DDoS-tactique-de,20140326,43910.html

- Premier virus TOR pour Android
  http://www.securelist.com/en/blog/8184/The_first_Tor_Trojan_for_Android

- Un premier bootkit Android
  - Détecté par l'éditeur russe d'antivirus Doctor Web
  - A infecté près de 350 000 Smartphones !
    http://thenextweb.com/insider/2014/01/27/first-android-bootkit-malware-spotted-reportedly-found-350000-mobile-devices-china/

Malwares, spam, fraudes et DDoS

- Les cybercriminels prêts à tout pour des Bitcoins
  http://www.undernews.fr/malwares-virus-antivirus/les-cybercriminels-prets-a-tout-pour-des-bitcoins.html

- Des distributeurs automatiques de billets pillés avec de simples SMS ?
  http://www.undernews.fr/hacking-hacktivisme/des-distributeurs-automatiques-de-billets-pilles-avec-de-simples-sms.html

- #hackfail, des hackers effacent le site d'une banque qui s'avèrent être un site de phishing. Le groupe de hackers AnonGhost, « spécialisé » dans l'effacement de site web a récemment fait parler de lui en attaquant le site http://ybs-bank.com/ appartenant d'après eux à la banque « Yorkshire Bank ». Il s'avère cependant que ce site, détenu par un malaisien, était utilisé pour des attaques de type phishing puisque le vrai site s'avère être http://www.ybonline.co.uk/.

Hack

- L’OWASP créé une base de données des incidents web
  https://www.owasp.org/index.php/OWASP_WASC_Web_Hacking_Incidents_Database_Project

Hacking tools

- Une liste d'outils d'OSINT (recherche d'informations publiques)
  http://www.subliminalhacking.net/2012/12/27/osint-tools-recommendations-list/
- Une technique de poisoning ARP peu connue
  http://blog.zorinaq.com/?e=6
- Un nouvel outil pour injecter du code HTML sur un réseau Wifi
  https://github.com/DanMcInerney/LANs.py
- Florilège de techniques pour récupérer les mots de passes en environnement Windows
  https://www.securusglobal.com/community/2013/12/20/dumping-windows-credentials/
- Injection de code HQL (Hibernate)
  http://blog.h3xstream.com/2014/02/hql-for-pentesters.html
- Une collection de clé privées trouvées dans des appliances, utile en pentest
  https://code.google.com/p/littleblackbox/
- Extraire facilement les mots de passe AD avec une commande Windows
  http://blog.cyberis.co.uk/2014/02/obtaining-ntdsdit-using-in-built.html

Metasploit : Nouveautés

- Exploit pour Android (<4.2), 70% des mobiles vulnérables
- Fonctionnalité de surveillance de presse-papier dans meterpreter
  https://community.rapid7.com/community/metasploit/blog/2014/02/13/weekly-metasploit-update
- Module d'ingénierie sociale pour Safari
  https://community.rapid7.com/community/metasploit/blog/2014/03/13/metasploit-weekly-update

DFIR

- Un script Python pour scanner des éléments par plusieurs AV
  https://github.com/joxeankoret/multiav

- Le cryptolocker “BitCrypt” combattu par les équipes d’Airbus Defence & Space
  - Une mauvaise implémentation du chiffrement permet de récupérer les fichiers chiffrés
    http://blog.cassidiancybersecurity.com/post/2014/02/Bitcrypt-broken

Actualité francophone

- Eric Filiol renonce à son talk au CanSecWest
  http://www.lemagit.fr/actualites/2240215853/CanSecWest-Eric-Filiol-renonce-a-son-intervention
  - Annulé car classé confidentiel (!!?) selon Dragos RUIU (Organisateur)
    https://plus.google.com/103470457057356043365/posts/AscNwWvmXyA
  - Ces méthodes ou failles pourraient inspirer des terroristes, d'où l'annulation
    http://blogs.csoonline.com/security-industry/3050/cansecwest-talk-infrastructure-attacks-canceled-after-being-classified

- VUPEN au top à Pwn2Own
  - Firefox, IE, Safari, Chrome -> tous été piratés
  - $850 000 dollars de récompense

  http://threatpost.com/vupen-cashes-in-four-times-at-pwn2own/104754

Actualité francophone

- Steria rachète Beamap, un spécialiste du cloud
  http://www.channelnews.fr/actu-societes/ssii/18945-steria-rachete-un-specialiste-du-cloud.html
- SFR et Numéricable seraient en discussion
  http://www.pcinpact.com/news/86131-rapprochement-entre-numericable-et-sfr-vivendi-confirme-discussions.htm
- Vente de SFR : 5 questions pour tout comprendre
  http://www.01net.com/editorial/615502/vente-de-sfr-5-questions-pour-tout-comprendre/
- Les offres de rachat de SFR par Bouygues et Numéricable
  http://www.01net.com/editorial/615436/rachat-de-sfr-les-deux-offres-face-a-face/
- Télécoms : la guerre sans merci de Bouygues, Niel et Richard http://www.lemonde.fr/a-la-une/article/2014/02/26/la-guerre-sans-merci-de-bouygues-niel-et-richard_4373392_3208.html
- Loi sur la géolocalisation : députés et sénateurs se mettent d'accord en CMP
  http://www.pcinpact.com/news/86028-loi-sur-geolocalisation-deputes-et-senateurs-se-mettent-d-accord-en-cmp.htm
- Les sénateurs PS veulent restreindre l'usage de la biométrie en France
  http://www.pcinpact.com/news/86050-les-senateurs-ps-veulent-restreindre-usage-biometrie-en-france.htm

Actualité francophone

- Danone externalise 25 000 boîtes mails dans le cloud IBM SmartCloud
  - La NSA doit jubiler :-/

http://pro.01net.com/editorial/612828/danone-migre-25-000-boites-email-dans-le-nuage-d-ibm/

- Les retards de cloudwatt

http://www.lesechos.fr/entreprises-secteurs/tech-medias/actu/0203357157522-demarrage-poussif-de-cloudwatt-le-cloud-d-orange-655211.php

- Comment le cloud public peut-il être si peu cher ?

https://owncloud.com/blog/just-cheap-can-public-cloud-computing-get

Actualité francophone

- Récupérer un disque dur à Paris
  http://www.01net.com/editorial/615678/comment-sauver-un-disque-dur-endommage-video/

- Affaire bluetouff : coupable du manque de compétence informatique des magistrats
  - maintien frauduleux dans un STAD
    http://obsession.nouvelobs.com/hacker-ouvert/20140206.OBS5374/condamne-pour-une-recherche-google-le-blogueur-consterne.html
    http://www.pcinpact.com/news/85823-retour-sur-condamnation-bluetouff-par-cour-dappel-paris.htm

- Pourquoi les FAI vont devoir travailler à l'oeil pour l'État
  http://www.pcinpact.com/news/86016-pourquoi-fai-vont-devoir-travailler-a-oeil-pour-etat.htm

- Nouveau câble transatlantique entre le Brésil et l'Europe
  http://www.pcinpact.com/news/86149-un-nouveau-cable-reliera-bresil-et-europe-pour-contourner-nsa.htm

- Skype dans l'oeil de la justice
  http://lexpansion.lexpress.fr/high-tech/skype-dans-l-oeil-de-la-justice_1499029.html

Actualité francophone

- Orange discute avec Microsoft autour de Dailymotion
  http://www.linformaticien.com/actualites/id/32217/dailymotion-orange-discute-avec-microsoft-mais-veut-garder-le-controle.aspx

- Stéphane Richard confirme l'arrivée de Netflix en France
  http://www.journaldugeek.com/2014/03/10/orange-confirme-netflix-france/
  - Mais ils iraient plutot au Luxembourg
    http://m.lesechos.fr/tech-medias/netflix-se-lancera-en-france-en-passant-par-le-luxembourg-0203414658644.htm#Xtor=AD-6001

- Abandon de poursuites dû à un manque de coopération de Facebook
  http://www.pcinpact.com/news/86106-aucune-poursuite-engagee-contre-page-facebook-adopteungitan-com.htm

- Une étude pour mesurer l'efficacité de la vidéo protection
  http://www.pcinpact.com/news/85962-l-etat-commande-etude-pour-mesurer-l-efficacite-videosurveillance.htm

Actualité francophone

- Le challenge ANSSI qui avait été lancé en février 2012 a “enfin” été résolu
  http://www.ssi.gouv.fr/fr/menu/actualites/le-challenge-anssi-qui-avait-ete-lance-en-fevrier-2012-a-ete-resolu.html

- Les nouveaux locaux de l' ANSSI
  - Pas de photo révélant de grand secret, juste quelques écrans, avec des filles devant ;-)
    http://pro.01net.com/editorial/614570/decouvrez-les-nouveaux-locaux-parisiens-de-lanssi/

- Le nouveau directeur de l’ANSSI, Guillaume Poupard, vient de la DGA
    http://www.itespresso.fr/guillaume-poupard-nouveau-directeur-anssi-vient-dga-74070.html

- Budget 2014 pour la DGSE
  - Les détails du pacte de CyberDéfense et ses 1 milliard d’euros
    http://www.lepoint.fr/fil-info-reuters/la-france-tente-de-rattraper-son-retard-en-cyberdefense-07-02-2014-1789136_240.php

- La DGSE et Orange, main dans la main
  http://www.lemonde.fr/international/article/2014/03/20/dgse-orange-des-liaisons-incestueuses_4386264_3210.html
  http://www.lemonde.fr/international/article/2014/03/20/les-x-telecoms-maitres-d-uvre-du-renseignement_4386654_3210.html

Actualité francophone

- Recommandations 2014 de la CNIL concernant les paiements par CB
  http://www.cnil.fr/les-themes/argent/article/article/utilisation-des-cartes-bancaires-pour-le-paiement-a-distance-nouvelle-recommandation/
- La CNIL, e.leclerc et la biométrie
  http://pro.01net.com/editorial/613770/la-cnil-met-en-demeure-un-centre-e-leclerc-pour-son-acces-biometrique/
- Note de l'ENISA sur les systèmes ou logiciels non supportés
  https://www.enisa.europa.eu/publications/flash-notes/flash-note-risks-of-using-discontinued-software/at_download/fullReport
- Du matériel de formation mis à disposition par l'ENISA
  http://www.enisa.europa.eu/activities/cert/support/exercise
- Orange : à chaque attaque nous progressons
  http://www.lepoint.fr/chroniqueurs-du-point/guerric-poncet/exclusif-orange-stephane-richard-a-chaque-attaque-nous-progressons-07-02-2014-1789392_506.php

Actualité Européenne

- Règlementation Européenne sur la protection des données
  - Amende en cas de non-respect des règles, jusqu'à 5% du CA de l'entreprise
  - Pour sortir des données personnelles d'européen, il faudra en demander l'autorisation
    http://www.lemondeinformatique.fr/actualites/lire-cybersecurite-en-europe-les-geants-de-l-internet-dispenses-de-declarer-les-incidents-56868.html

- Pourquoi les employés peuvent souffrir dans une société sans hiérarchie comme GitHub
  http://www.wired.com/wiredenterprise/2014/03/tyranny-flatness/

- Google réinvente la facturation du cloud computing
  http://www.wired.com/wiredenterprise/2014/03/google-cloud-prices/

Actualité Européenne

- Il faudra montrer patte blanche à l'entrée de l'union européenne
  http://politiquedunetz.sploing.be/2014/04/controle-biometrique-aux-frontieres-et-base-de-donnee-europeenne-des-migrants/

- La gendarmerie ferme un site de téléchargement gratuit de mp3
  http://www.zataz.com/news/23310/Delamusique--sacem--gendarmerie--mp3.html

- Le parlement européen valide l'adoption d'un chargeur universel pour les appareils radioélectriques, Apple devra se conformer à la règle
  http://www.developpez.com/actu/68875/Le-parlement-europeen-valide-l-adoption-d-un-chargeur-universel-pour-les-appareils-radioelectriques-Apple-devra-se-conformer-a-la-regle/

- Le racket du téléchargement en Allemagne
  http://www.pcinpact.com/news/86298-108-975-pirates-allemands-sommes-payer-pour-eviter-poursuites.htm

Actualité Internationale

- Le rachat de Whatsapp par facebook menacé par les données personnelles
  http://www.01net.com/editorial/615506/donnees-personnelles-recours-depose-contre-le-rachat-de-whatsapp-par-facebook/

- Le DOJ ne peut pas détenir les metadata de manière indéfinie
  http://www.techdirt.com/articles/20140307/16401426487/fisa-court-shuts-down-dojs-attempt-to-hold-onto-section-215-metadata-indefinitely.shtml

- Paypal rentre dans les applications mobiles
  http://pro.01net.com/editorial/614826/paypal-s-embarque-dans-n-importe-quelle-application-mobile/

Actualité Internationale

- Les agences de renseignements US vont “scanner” en continu le comportement de leurs employés disposant de hautes habilitations
  http://gcn.com/articles/2014/03/11/cleared-worker-monitoring.aspx

- Fermeture de Full Disclosure à cause de Nicholas Lemonias :'(
  http://seclists.org/fulldisclosure/2014/Mar/332
  - Mais renaissance grace à Fyodor :-D
    http://insecure.org/news/fulldisclosure/

- Loi au Brésil pour stocker les données dans le pays
  http://www.itworld.com/internet/410669/brazil-drop-requirement-internet-firms-store-data-locally

- Quand la Turquie espionne les Turcs
  - Les attaques actuelles sont dues à un scandale de corruption du gouvernement
    http://mobile2.lematin.ch/articles/22025962

- Les Etats-Unis acceptent de ne plus gérer seuls les noms de domaine
  - Mais les conditions sont difficiles à mettre en œuvre
    http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions

Actualité Internationale

NSA / Prisme, toujours une actualité sans fin

- La liste des programmes d'espionnage
  https://nsa-observer.laquadrature.net/

- La NSA avait prévu le scénario Snowden... il y'a 23 ans ;-)
  http://www.latribune.fr/technos-medias/internet/20140108trib000808439/snowden-la-nsa-prevoyait-une-telle-affaire-il-y-a-23-ans.html

- La NSA fait bien de l'espionnage industriel (ou de l'intelligence économique si vous préférez)
  http://www.ndr.de/ratgeber/netzwelt/snowden277_page-1.html

- Attaque ciblée de la NSA sur un cryptographe Belge
  http://thehackernews.com/2014/02/nsa-allegedly-hacked-belgian.html

- MYSTIC de la NSA : enregistrement des conversations téléphoniques
  - Démarré en 2009 mais fonctionnel à partir de 2011
    http://nakedsecurity.sophos.com/2014/03/19/nsa-can-record-100-of-another-countrys-telephone-calls/

Actualité Internationale

- How the NSA Plans to Infect ‘Millions’ of Computers with Malware
  https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/
- La NSA aurait infiltré les serveurs du géant chinois Huawei
  http://www.lemonde.fr/technologies/article/2014/03/23/la-nsa-aurait-infiltre-les-serveurs-du-geant-chinois-huawei_4387917_651865.html
- La NSA et le GCHQ, « ennemis d'internet », Selon le rapport de Reporters Sans Frontières
  http://www.developpez.com/actu/69005/La-NSA-et-le-GCHQ-ennemis-d-internet-selon-le-rapport-de-Reporters-Sans-Frontieres/
- Les députés européens veulent geler les accords swift et safe arbor
  http://www.numerama.com/magazine/28730-nsa-le-parlement-europeen-veut-suspendre-certains-accords-avec-les-usa.html
- L’après Snowden : la confidentialité, c’est pas simple comme l’installation d’Ubuntu
  http://reflets.info/lapres-snowden-la-confidentialite-cest-pas-simple-comme-linstallation-dubuntu/
- Des images de millions de webcams collectées par les espions britanniques
  http://www.lemonde.fr/technologies/article/2014/02/27/les-images-de-webcams-de-millions-d-innocents-collectees-par-les-espions-britanniques_4375033_651865.html

Actualité Internationale

- Une chercheuse s'est-elle fait intercepter sa commande Amazon par la NSA ?
  http://www.infowars.com/tor-developer-suspects-nsa-interception-of-amazon-purchase/
  - Sur son suivi Amazon, on peut voir plusieurs relais étrange, proche de centre de renseignement du gouvernement américain
    https://twitter.com/puellavulnerata/status/426597381727989760/photo/1

- Turbine + Quantum + Chase the Admin = Own the Internet
  - Diffusion à grande échelle des trojans en reprenant les méthodes classiques des criminels
    - Water holing, infection d'un site légitime et utilisation d'une faille du navigateur pour injecter le trojan chez l'utilisateur
    - Spear Fishing, envoie de mails avec exploitation d'une faille ou pièce jointe vérolée
    - Spoofing, en se faisant passer pour un site légitime et utilisation d'une faille du navigateur pour injecter le trojan chez l'utilisateur
  - Les Administrateurs réseaux sont de très bonnes cibles et un simple email suffit
    https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/
    https://www.techdirt.com/articles/20140312/07334826545/nsa-aiming-to-infect-millions-computers-worldwide-with-its-malware-targets-telcoisp-systems-administrators.shtml
    http://www.itespresso.fr/turbine-machine-malware-nsa-espionner-monde-73660.html

Actualité Internationale

- Changement à la direction de la NSA
  - Le général Keith B. Alexander est remplacé par le Vice Amirale de la Navy Michael S. Rogers.
  - Sa spécialité me demanderez-vous ? La cryptologie ;-)
    http://www.computerworld.com/s/article/9245925/Obama_selects_Navy_cryptologist_to_head_NSA
  - Ce n'est donc finalement pas lui

Actualité Internationale

- La NSA, c'est fait pour espionner ;-)
  - C’est ce qu’écrivait le président américain Harry Truman, dans son mémo du 24 octobre 1952, annonçant la création de la NSA le 24 octobre 1952 :-)
  - Seconde phrase : <<They must be so organized and managed as to exploit to the maximum the available resources in all participating departments end agencies 2nd to satisfy the legitimate intelligence requirements of all such depztments and agencies>> http://www.nsa.gov/public_info/_files/truman/truman_memo.pdf

Actualité Google

- Google cherche (cherchait?) un expert l'Ingénierie Inverse sur Android et ARM
  - "The security of hundreds of millions of users will depend on your analysis results." https://www.google.com/about/careers/search/?#!t=jo&jid=14775001
- Google force ses services en SSL/TLS
  http://threatpost.com/google-encrypts-all-gmail-connections
- Google prend 6% du capital de Lenovo
  http://www.journaldugeek.com/2014/02/10/google-croque-dans-6-de-lenovo
- Google supprime le soulignage des liens
  http://www.theverge.com/2014/3/13/5503894/google-removes-underlined-links-site-redesign
- Google lance Chromecast en Europe et au Canada
  http://gigaom.com/2014/03/18/chromecast-international-launch-canada-uk-germany-france-europe/
- Android Wear : Google se lance à l'assaut du marché des montres connectées, Une preview du SDK est déjà disponible
  http://www.developpez.com/actu/68997/Android-Wear-Google-se-lance-a-l-assaut-du-marche-des-montres-connectees-une-preview-du-SDK-est-deja-disponible/

Actualité Google

- Google critiqué pour avoir scanné les mails de millions d'étudiants
  http://www.lemonde.fr/technologies/article/2014/03/19/google-critique-pour-avoir-scanne-les-mails-de-millions-d-etudiants_4385358_651865.html
- Google rachète SlickLogin pour authentifier par le son
  http://www.journaldugeek.com/2014/02/17/google-rachete-slicklogin-authentification-son/
- Avancée scientifique pour rendre les logiciels inviolables
  http://www.linformaticien.com/actualites/id/31945/cryptographie-avancee-scientifique-pour-rendre-les-logiciels-inviolables.aspx
- Retrouver l'algorithme de hashage d'un condensat
  https://github.com/psypanda/hashID
- Authentification sur tablette via biométrie par Morpho
  http://pro.01net.com/editorial/614922/morpho-lance-une-tablette-biometrique-pour-le-controle-d-identite/

Actualité Apple

- Apple souhaites $40 par Smartphone Samsung
  - Samsung aurait enfreint 5 principaux brevets
    http://pro.clubic.com/entreprises/apple/actualite-688958-brevets-apple-voudrait-payer-samsung-40-dollars-terminal-vendu-redevance.html

- Apple cible privilégiée du patent troll en 2013
  - 92 poursuites en 3 ans
    http://arstechnica.com/tech-policy/2014/02/apple-top-target-of-patent-trolls-faced-92-lawsuits-in-three-years/

- Plus de support pour Mac OS X Snow Leopard 10.6
  - Alors que le parc est estimé à 20% des Mac
    http://www.computerworld.com/s/article/9246609/Apple_retires_Snow_Leopard_from_support_leaves_1_in_5_Macs_vulnerable_to_attacks
  - Etrangement, à ce jour (mars 2014) l'OS est toujours vendu sur le site d'Apple !!?
    http://store.apple.com/us/product/MC573Z/A/mac-os-x-106-snow-leopard

Actualité Crypto

- Black Hat 2013, attaque fonctionnelle « side channel » permettant de retrouver des clefs probables depuis une trace électrique
  https://media.blackhat.com/us-13/US-13-OFlynn-Power-Analysis-Attacks-for-Cheapskates-Slides.pdf
  - Déjà démontré en France, en 2006, par une thèse réalisée avec la DCSSI
    http://www.ssi.gouv.fr/archive/fr/sciences/fichiers/lti/these-germain.pdf

- TOR faillible aux nœuds malveillants (Dump réseau, SSLStrip, MitM SSL, MitM SSH, Usurpation DNS dans certains cas)
  - Mais on le savait déjà… il faut “au moins” utiliser SSL/TLS
    http://www.cs.kau.se/philwint/spoiled_onions/

- Rapport d’audit sur CryptoCat
  http://isecpartners.github.io/publications/iSEC_Cryptocat_iOS.pdf

Conférences

Conférences passées

- JSSSI 2014
  - Une réussite ! Mais qui en doutait ;-)
  - L'ensemble des slides sont en ligne : http://www.ossir.org/jssi/index/jssi-2014.shtml

- INSOMNI'HACK14
  - "Deploying cyberdefense measures and Policies in a Critical Infrastructure " par S. Bombal
  - Lurking in clouds: easy hacks for complex apps , Nicolas Gregoire
  - When you can't afford 0days.Client-side exploitation for the masses Michele Orru, Krzysztof Kotowicz

Conférences

Conférences à venir

- Hack in Paris - 23 au 27 juin 2014 chez Mickey
- Hackito Ergo Sum - 24 au 26 avril 2014 à Paris
- SSTIC - 4 au 6 juin 2014 à Rennes
- No Such Con - 19 au 21 novembre 2014 à Paris
- Bot Conf - 3 au 5 Décembre 2014 à Nantes

Sorties Logicielles

- JSUnpack : Unpacker Javascript assez efficace
  http://jsunpack.jeek.org/?report=86cee6d09c27547d03c9a163b850264fa2171d39
- Pac4Mac 0.3 : Framework Forensique pour Mac OS X
  http://sud0man.blogspot.fr/2014/02/new-version-of-mac-os-x-forensics.html
- GoAccess : Visualisation en temps réel des logs Apache
  http://goaccess.prosoftcorp.com/
- Désassembler un binaire en ligne
  http://onlinedisassembler.com/odaweb/
- CapStone un désassembleur léger et standalone en C avec des bindings en Python
  https://github.com/aquynh/capstone
- Systernals
  - Process Explorer intègre VirusTotal
    http://technet.microsoft.com/en-us/sysinternals/bb896653
  - PSExec chiffre désormais les flux réseau

Sorties Logicielles

- Outil de pentest de spip
  https://github.com/PaulSec/SPIPScan
- Nouveau format de compression pour JPG
  https://blog.mozilla.org/research/2014/03/05/introducing-the-mozjpeg-project/
- Stack TCP/IP en gawk
  https://www.gnu.org/software/gawk/manual/gawkinet/gawkinet.html
- Valve sort un convertisseur directX vers OpenGL
  http://www.macg.co/logiciels/2014/03/valve-sort-un-outil-pour-porter-des-jeux-windows-sur-mac-et-linux-80613
- Un serveur web en un printf
  http://tinyhack.com/2014/03/12/implementing-a-web-server-in-a-single-printf-call/
- Sentinel , un concurrent d' EMET par CoreLab
  http://corelabs.coresecurity.com/index.php?module=Wiki&action=view&type=tool&name=sentinel

Sorties Logicielles

- Sortie de Libre Office 4.2
  http://linuxfr.org/news/libreoffice-4-2-0-est-disponible
- Mylar et le chiffrement côté navigateur
  http://www.01net.com/editorial/616856/le-mit-invente-un-web-anti-nsa/
- Lecture rapide avec Spritz
  http://www.spritzinc.com/
  - Gritz, la version OpenSource : https://github.com/xypiie/gritz
- HTTPie : CLI, cURL-like pour les humains
  https://github.com/jkbr/httpie

Sorties matérielles

- Le blackphone est disponible à la vente
  https://store.blackphone.ch/

Divers

- $8 / mois pour un accès à vos données Facebook, Twitter...
  https://datacoup.com/

- Auditez le code source de Firefox
  https://brendaneich.com/2014/01/trust-but-verify/

- Des éléments du F-35 Joint Strike Fighter Américain sur le J-20 Chinois
  - En 2000, attaque Chinois visant les américains et vole des plans
  - En 2012, le J-31 Chinois ressemblait au F-35. Pur hasard ? ;-)
    http://french.ruvr.ru/2012_11_08/93961238/
  - En 2014, le J-20 ressemble au F-35
    http://thediplomat.com/2014/03/f-35-secrets-in-chinas-j-20/

- Un cadre passe en moyenne 16 ans en réunion
  http://www.lefigaro.fr/vie-bureau/2014/02/17/09008-20140217ARTFIG00123-un-cadre-passe-en-moyenne-seize-ans-en-reunion.php

- Un stagiaire gagne plus qu'un ingénieur
  - Chez VMWare ou Google ou encore Palantir, ils gagnent plus que nous O_o
    http://www.lefigaro.fr/secteur/high-tech/2014/03/03/01007-20140303ARTFIG00256-un-stagiaire-chez-google-gagne-plus-de-5000-dollars-par-mois.php

Divers

- Apple, Google, Microsoft et Yahoo se réserve le droit de lire vos mails
  http://www.theguardian.com/technology/2014/mar/21/yahoo-google-and-apple-claim-right-to-read-user-emails

- PoC||GTFO 0x03 + mirroir
  http://jarmoc.com/pocorgtfo/pocorgtfo03.pdf
  http://jarmoc.com/pocorgtfo/

- Compter sérieusement le nombre d'attaques informatiques ?
  http://www.bortzmeyer.org/compter-attaques.html

- Premier distributeur de bitcoin dans un bar anglais
  http://www.coindesk.com/londons-first-bitcoin-atm-launches-cafe-whisky-bar/

- Trustwave poursuivi par les banques dans le cas de l'attaque Target
  http://www.chicagobusiness.com/article/20140325/BLOGS11/140329865

Divers

- Newsweek aurait trouvé le créateur du bitcoin
  http://mag.newsweek.com/2014/03/14/bitcoin-satoshi-nakamoto.html
- Carte du monde par connexion Internet
  http://rue89.nouvelobs.com/2014/02/23/surprises-carte-monde-selon-les-connections-a-internet-250180
- Carte de la Cyber Guerre en temps réèl, par Kaspersky
  http://cyberwar.kaspersky.com/

Divers

- Quel est l'avenir du poste de travail ?
  - Une piste
    http://pro.clubic.com/it-business/actualite-615878-dell-wyse-cloud-connect-client-leger-cle-hdmi.html

- Le DaaS (Desktop as a Service) arrive avec Nvidia Grid et VMWare Horizon (ex-VMWare View)
  http://blogs.vmware.com/smb/2013/08/vmware-view-virtual-desktops-with-3d-graphics-made-simple.html
  http://www.clubic.com/carte-graphique/carte-graphique-nvidia/gpu-tech/actu-gtc_nvidia_s_ouvre_a_la_virtualisation_gpu_avec_vmware-692238.html

Divers

- Et si Bitcoin était un botnet cryptographique créé par la NSA ?
  http://bitcoinisablackop.wordpress.com
  - Repris sur 01Net :-)
    http://www.01net.com/editorial/613590/et-si-bitcoin-etait-un-botnet-cryptographique-cree-par-la-nsa/

- La stratégie secrète de Google (IA , ADN , Robotique)
  - Avec une belle conclusion : « Quand "BigDog" aura un fusil d'assaut M16 dans les mains, il vaudra mieux ne pas se promener en forêt! »
    http://www.lejdd.fr/Economie/Entreprises/Laurent-Alexandre-La-strategie-secrete-de-Google-apparait-652106

- Envahir la Suisse en HNO
  http://www.bloomberg.com/news/2014-02-17/invading-switzerland-try-before-8-or-after-5.html

- 2048
  http://gabrielecirulli.github.io/2048/

- 2048 , TF1 vs StackOverflow
  - Qui est le plus fort à 2048, TF1 ou StackOverflow ?

  http://videos.tf1.fr/infos/2014/jeu-en-ligne-2048-on-a-teste-la-technique-du-coin-8386389.html
  https://stackoverflow.com/questions/22342854/what-is-the-optimal-algorithm-for-the-game-2048

Divers

- Video de promo Sogeti USA
  https://www.youtube.com/watch?v=BxaSJpsTPsM
- Merci à l'Académie Française
  http://www.academie-francaise.fr/digital
- Lorsque le public est questionné sur les termes informatiques
  http://korben.info/le-html-maladie-sexuellement-transmissible.html
- Transformer l'eau en vin
  http://themiraclemachine.net/
- Grâce au Digital Comic Museum, téléchargez plus de 15000 comics gratuitement
  http://www.journaldugeek.com/2014/03/10/grace-au-digital-comic-museum-telechargez-plus-de-15000-comics-gratuitement/

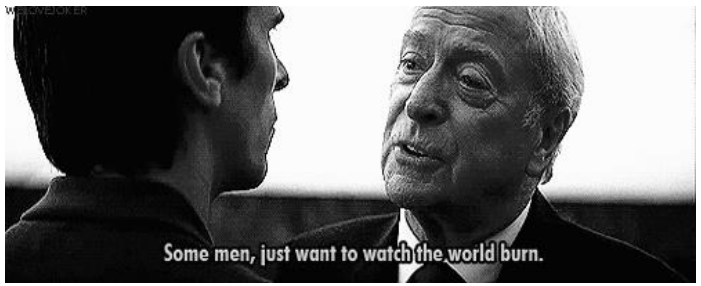
Divers

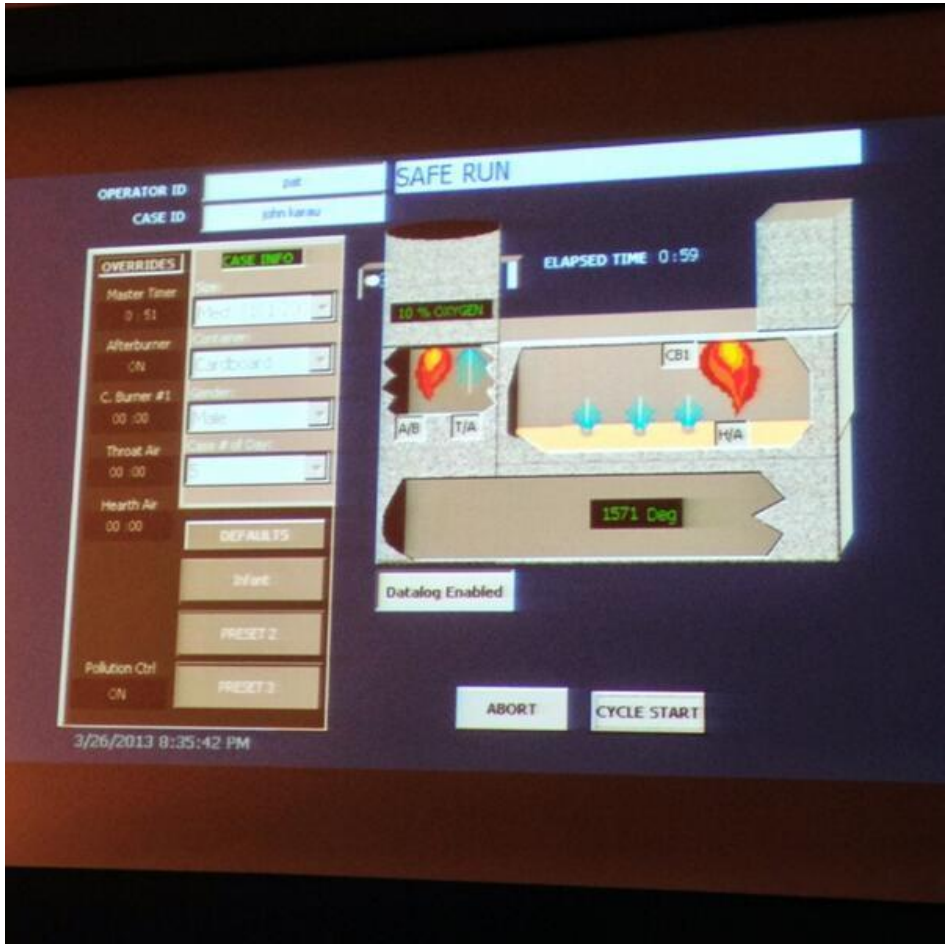
- Facebook publie en Open Source sa librairie de crypto pour Android : Conceal
  http://threatpost.com/facebook-releases-to-open-source-its-conceal-android-crypto-library/104040
- Japon, 12,8 millards d'attaques informatiques en 2013
  http://www.zdnet.com/japan-sees-record-12-8b-cyberattacks-7000026229/
- Quel gamer es-tu ?
  http://www.journaldugamer.com/2014/02/10/infographie-gamer
- Auto-destruction de composants electroniques
  http://thehackernews.com/2014/02/ibm-developing-self-destructing.html

Divers

- Un fichier qui est à la fois pdf, zip, jpg, afsk et png
  https://twitter.com/corkami/status/443121777913262080/photo/1

Le coin Scada





SCADA

- Librairie open-source pour dialoguer avec les automates Siemens PL7
  http://snap7.sourceforge.net

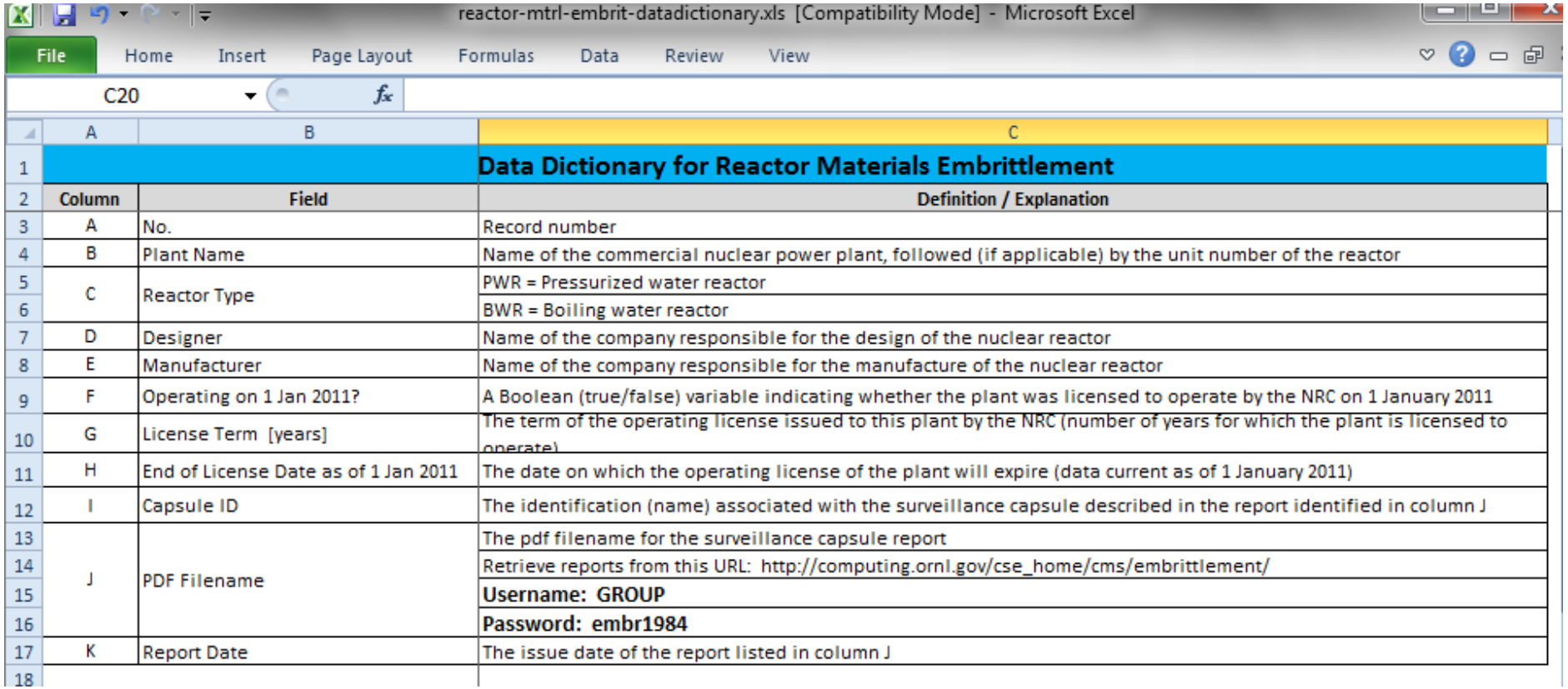
- Et si Stuxnet avait été introduit directement via le fournisseur d'automatisme ?
  http://www.csmonitor.com/World/Security-Watch/2014/0225/Exclusive-New-thesis-on-how-Stuxnet-infiltrated-Iran-nuclear-facility?cmpid=addthis_twitter#.Uw65Hcljhvw.twitter

- Vulnérabilités sur les systèmes Yokogawa
  https://community.rapid7.com/community/metasploit/blog/2014/03/10/yokogawa-centum-cs3000-vulnerabilities
  http://ics-cert.us-cert.gov/advisories/ICSA-14-070-01/

- Vulnérabilités sur Siemens S7-1500 (et S7-1200)
  http://ics-cert.us-cert.gov/advisories/ICSA-14-073-01/

SCADA

- C’est fou ce que l’on peut trouver sur Google : “ext:xls password inurl:http://nrc.gov”


reactor-mtrl-embrit-datadictionary.xls [Compatibility Mode] - Microsoft Excel

File Home Insert Page Layout Formulas Data Review View

C20

	A	B	C
1			**Data Dictionary for Reactor Materials Embrittlement**
2	**Column**	**Field**	**Definition / Explanation**
3	A	No.	Record number
4	B	Plant Name	Name of the commercial nuclear power plant, followed (if applicable) by the unit number of the reactor
5	C	Reactor Type	PWR = Pressurized water reactor
6			BWR = Boiling water reactor
7	D	Designer	Name of the company responsible for the design of the nuclear reactor
8	E	Manufacturer	Name of the company responsible for the manufacture of the nuclear reactor
9	F	Operating on 1 Jan 2011?	A Boolean (true/false) variable indicating whether the plant was licensed to operate by the NRC on 1 January 2011
10	G	License Term [years]	The term of the operating license issued to this plant by the NRC (number of years for which the plant is licensed to operate)
11	H	End of License Date as of 1 Jan 2011	The date on which the operating license of the plant will expire (data current as of 1 January 2011)
12	I	Capsule ID	The identification (name) associated with the surveillance capsule described in the report identified in column J
13	J	PDF Filename	The pdf filename for the surveillance capsule report
14			Retrieve reports from this URL: http://computing.ornl.gov/cse_home/cms/embrittlement/
15			**Username: GROUP**
16			**Password: embr1984**
17	K	Report Date	The issue date of the report listed in column J
18			

Questions ?

- Questions / réponses
- Prochaine réunion
  - Mardi 13 mai 2014
- Prochain AfterWork
  - Mardi 20 mai 2014
  - "Retour d’expérience CryptoLocker" (Patrick Asty)
- N'hésitez pas à proposer des sujets et/ou des salles