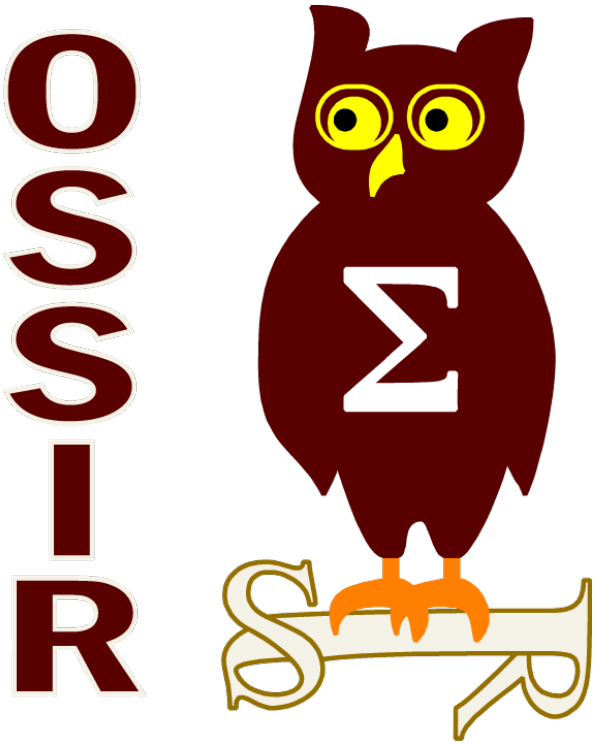


Groupe Paris

Réunion du 11/02/2014

Bulletins Microsoft

Janvier 2014

MS14-001 Failles Office [x3]

- Affecte: Word pour Office (toutes versions supportées) mais aussi Sharepoint 2010 / 2013
- Exploit: Exécution de code lors de l'ouverture d'un fichier Word malformé - CVE-2014-0258, CVE-2014-0259, CVE-2014-0260
- Crédits: Mateusz Jurczyk, Ivan Fratric et Ben Hawkes / Google

MS14-002 Faille noyau [x1]

- Affecte: Windows XP SP3 et Pro adm64 SP2, Windows 2003 SP2, amd64 SP2, Itanium SP2 (remplace MS10-099)
- Exploit:
    - Elévation de privilège locale grace à NDProxy.sys, gestionnaire de l'API de téléphonie Windows - CVE-2013-5065
    - Un workaround avait été proposé en décembre 2013 envoyant les appels à NDProxy vers Null.sys
- Crédits: FireEye

MS14-003 Faille noyau dans Win32k.sys pour les drivers

- Affecte: Windows 7 SP1, Windows 2008 R2 SP1 (“Core” compris)
- Exploit: Execution de code en tant que SYSTEM - CVE-2014-0262
- Crédits: Yujie Wen et Renguang Yuan / Qihoo (Société Chinoise de sécurité)

MS14-004 Faille Microsoft Dynamics AX (ERP de Microsoft)

- Affecte: Microsoft Dynamics AX 4.0 SP1, 2009 SP1, 2012 et 2012 R2
- Exploit: Deni de service distant
- Crédits: Andrey Maykov / FTO (Intégrateur Russe d’ERP)

Bulletins Microsoft

Advisories

2916652 Autorité de certification de l'ANSSI

- v2.1 : modification dans la logique de detection

2914486 Elévation de privilèges locale sur Windows

- v2.0 : mise à jour (du texte) de l'avis pour mieux correspondre au bulletin de sécurité

2755801

- v17.0 : nouvelle mise à jour de Flash Player

Infos Microsoft

Fin de support

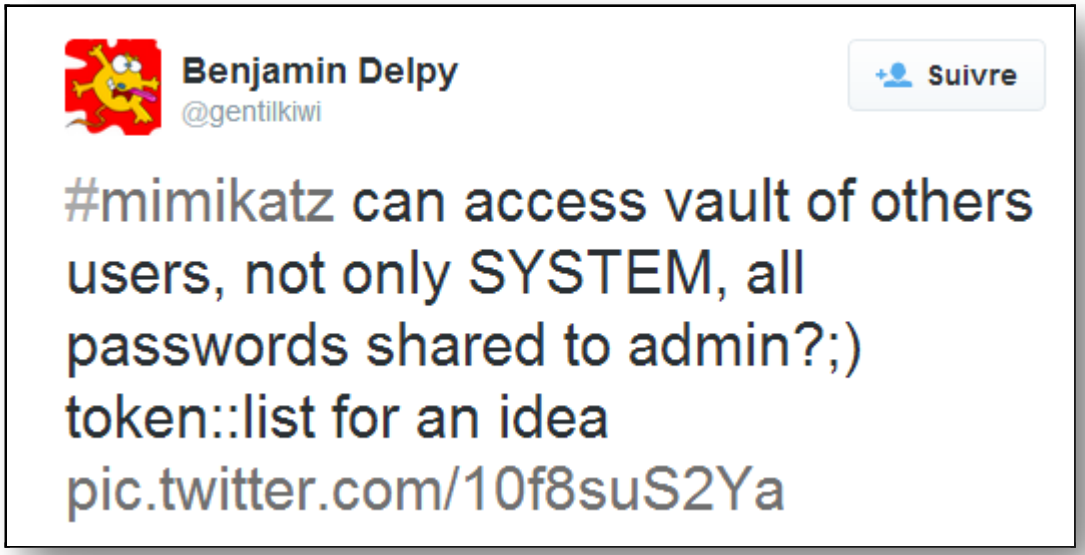
- Avril 2014 pour Windows XP
- Janvier 2015 (Mainstream) pour Windows 7

http://windows.microsoft.com/en-us/windows/lifecycle

Mimikatz permet de récupérer le contenu du “vault” de tous les utilisateurs

Le vault contient les mots de passe enregistrés (type partage réseau, sites web, etc..)

https://twitter.com/gentilkiwi/status/427189145111236608



Infos réseau

- Attaques DDoS par amplification NTP
  https://labs.ripe.net/Members/mirjam/ntp-reflections

- Metasploit publie plusieurs modules pour exploiter le protocole PJL des imprimantes
  https://community.rapid7.com/community/metasploit/blog/2014/01/23/weekly-metasploit-update
  https://community.rapid7.com/community/metasploit/blog/2014/01/23/hacking-printers-with-metasploit

- Après TrendNet, c'est au tour des webcam IP Foscam d'exposer leurs utilisateurs
  http://krebsonsecurity.com/2014/01/bug-exposes-ip-cameras-baby-monitors/

Failles

- DUAL EC DRBG, la preuve
  http://blog.0xbadc0de.be/archives/155
- Des vulnérabilités sur Google Chrome permettent d'espionner le micro des utilisateurs
  http://www.talater.com/chrome-is-listening/
- RCE sur Yahoo
  http://www.sec-down.com/wordpress/?p=87
- La sécurité de TOR remise en question à cause des noeuds de sortie
  http://www.cs.kau.se/philwint/spoiled_onions/
- Vulnérabilité critique sur Drupal 6
  https://drupal.org/SA-CORE-2014-001
- Vulnérabilité critique sur MediaWiki
  http://www.exploit-db.com/exploits/31329
- CVE 2014-0497 : Adobe publie en urgence une mise à jour pour Flash (exécution de code arbitraire)
  http://helpx.adobe.com/security/products/flash-player/apsb14-04.html

Hacks

- **Vol de données CB chez Target**
  - 40 millions de n° de CB
  - ~~70~~ 110 millions de données de clients (nom, prénom, adresses postales et mail).
  - Un trojan sur les caisses de paiement
    - Ecrit en VBScript.
    - Spécifique à l'attaque et non reconnu par l'antivirus installé (mais qui croit encore en l'utilité d'un AV)
    - Developpé et vendu par un jeune Russe de 17 ans
  - 11Go de données exfiltrées sur un serveur américain, puis de là vers un serveur russe
- http://www.lemondeinformatique.fr/actualites/lire-affaire-target-11-go-de-donnees-envoyees-vers-un-serveur-russe-56296.html
- http://www.undernews.fr/malwares-virus-antivirus/le-malware-blackpos-utilise-lors-du-piratage-de-target-developpe-par-pirate-russe-de-17-ans.html
- L'intrusion aurait eu lieu via le réseau HVAC (climatisation/chauffage) et les credentials d'un prestataire

- **Des extensions Chrome rachetées pour diffuser du malware**
  http://arstechnica.com/security/2014/01/malware-vendors-buy-chrome-extensions-to-send-adware-filled-updates/

- **Linkedin victime d'une visite massive de comptes par l'intermédiaire du cloud d'Amazon**
  http://arstechnica.com/security/2014/01/hackers-use-amazon-cloud-to-scrape-mass-number-of-linkedin-member-profiles/

- **Les voleurs utilisent les réseaux sociaux pour le repérage**
  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/

Hacks

- **Yahoo! Attaqué**
  « Yahoo! a annoncé, jeudi 30 janvier, avoir identifié « un effort coordonné pour accéder de manière non autorisée » à des comptes sur sa messagerie Yahoo Mail »
  http://arstechnica.com/security/2014/01/mass-hack-attack-on-yahoo-mail-accounts-prompts-password-reset/

- **Les radars fixes russes piratés**
  http://www.tomsguide.fr/actualite/windows-xp-radar-russe-virus,40146.html

- **16 millions de données personnelles dérobées par un botnet en Allemagne**
  http://www.thelocal.de/20140121/agency-warns-of-16-million-email-accounts-hacked-bsi-germany

- **Un consultant vole 20 millions de données bancaires en Corée du Sud**
  http://www.theregister.co.uk/2014/01/22/sk_data_breach_apology/
  http://www.bbc.co.uk/news/technology-25808189

- **Orange se fait dérober les coordonnées de 800 000 clients**
  http://www.lemonde.fr/technologies/article/2014/02/02/les-donnees-personnelles-de-800-000-clients-d-orange-derobees_4358636_651865.html
  http://www.orangeinfo.fr/263²31-orange-met-en-place-une-cellule-daccompagnement-pour-les-800-000-clients-pirates.html

Hacks

- Déni de service : l'armée syrienne électronique modifie les enregistrements DNS d'eBay et Paypal UK et entraine ainsi des indisponibilités temporaires de sites et messageries
  http://www.theregister.co.uk/2014/02/03/ebay_dns_hijack_sea/

- Malware bancaire : GameOver Zeus revient dans une version chiffrée (.enc) capable de contourner les composants de sécurité
  http://threatpost.com/gameover-zeus-now-using-encryption-to-bypass-detection/104019

- iOS7 : un bug permet de désactiver la fonctionnalité « find my iPhone » sans saisir le mot de passe utilisateur
  http://www.theinquirer.net/inquirer/news/2327573/ios-7-exploit-disables-find-my-iphone-without-a-password

- Propagation de malwares : des chercheurs ont montré comment injecter du code malveillant dans les métadonnées d'une image PNG
  http://blog.sucuri.net/2014/02/new-iframe-injections-leverage-png-image-metadata.html

Actualité francophone

- **Sogeti recrute l'ancien directeur technique de la DGSE**
  http://pro.01net.com/editorial/611908/sogeti-recrute-un-ex-directeur-de-la-dgse-comme-conseiller-en-cybersecurite/

- **Patrick Pailloux devient responsable de la NSA à la Francaise**
  http://www.lemonde.fr/technologies/article/2014/01/21/patrick-pailloux-prend-la-tete-de-la-direction-technique-de-la-dgse_4352081_651865.html

- **Rapport sur la fuite d'information dans les transports**
  - 14% des gens ont déjà capté des informations confidentielles ou ultra sensibles
  - 52% des gens n'hésiteraient pas à récupérer des informations sur la concurrence et à en faire part à leur entreprise
  - http://www.globalsecuritymag.fr/Quels-risques-pour-vos-donnees,20140114,42209.html

- **Le PDG de cloudwatt s'en va**
  http://philippe.scoffoni.net/75-millions-euros-argent-public-pdg-cloudwatt-sen-va/

- **Danone migre 25 000 boîtes dans le cloud d'IBM**
  http://pro.01net.com/editorial/612828/danone-migre-25-000-boites-email-dans-le-nuage-d-ibm/

Actualité francophone

- Google récolte une amende de 900 000€ par la CNIL espagnole
  http://www.zdnet.fr/actualites/vie-privee-google-condamne-en-espagne-39796504.htm

- 4 entreprises épinglées par la CNIL pour refus de collaboration
  http://pro.01net.com/editorial/611442/quatre-entreprises-epinglees-par-la-cnil-pour-refus-de-cooperer/

- Le sénat adopte la loi Amazon pour des livres plus chers
  http://www.numerama.com/magazine/28003-le-senat-adopte-la-loi-pour-des-livres-plus-chers-sur-internet.html

- On ne dit pas digital, bordel !
  http://www.academie-francaise.fr/digital

- La CNIL et l'opendata
  http://www.pcinpact.com/news/85263-open-data-cnil-lance-consultation-et-devoile-sa-feuille-route.htm

Actualité internationale

- **RSA Conférence boycottée suite aux révélations sur DUAL EC DRBG**
  OWASP https://twitter.com/EoinKeary/status/421300860044705792
  Mikko Hypponen http://www.f-secure.com/weblog/archives/00002651.html

- **Non, Ford ne revend pas vos données**
  Mais sait tout ce que vous faites en voiture…
  http://www.businessinsider.com/ford-exec-gps-2014-1#ixzz2q6TdQ9zf

- **La NSA a accès à des ordinateurs non-connectés**
  http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html

- **La NSA exploite Angry Birds et autres applications mobiles pour espionner**
  http://www.numerama.com/magazine/28188-la-nsa-exploite-angry-birds-et-autres-applications-mobiles-pour-espionner.html

Actualité internationale

- **Vie privée : sanction américaine suite à exposition de données médicales sur les moteurs de recherche**
  Les données, hébergées sur les serveurs de la société ne faisait pas l'objet d'un contrôle d'accès et ont été indexées par les moteurs de recherche.
  http://www.networkworld.com/news/2014/013114-ftc-medical-transcription-firm-allowed-278329.html

- **Le secrétaire du groupe de l'IETF en charge des standards de chiffrement est un employé de la NSA_**
  http://www.zdnet.fr/actualites/la-nsa-garde-les-standards-de-chiffrement-a-l-oeil-39796876.htm

- **Panne d'Internet pour 600 millions de Chinois : interception DNS?**
  http://www.theregister.co.uk/2014/01/21/china_dns_poisoning_attack/
  www.informationweek.com/security/security-monitoring/china-blames-massive-internet-blackout-on-hackers/d/d-id/1113551

- **Un site français recense les programmes de la NSA**
  http://www.zdnet.fr/actualites/nsa-observer-un-site-francais-recense-les-programmes-de-la-nsa-39797495.htm

Conférences

Conférences passées

FIC 2014

- 21-22 janvier

http://www.forum-fic.com/2014/fr/

- "*La sécurité est un échec mais l'échec est la mère de la réussite*"
- "*Tous les pires paranoiaques étaient bien naifs finalement quand on voit tout ce que fait la NSA*"
- Sondage "la sécurité est-elle un échec" permettant de voter indéfiniement ;-) (Augmenté seulement jusqu'à 72% de "oui la sécurité est un échèc", par manque de temps ^_^)
- Les stands des exposants "hackés" par Maxime Musqua pour Le Petit Journal ;-) http://www.canalplus.fr/c-divertissement/c-le-petit-journal/pid6383-le-defi-musqua.html?vid=1008946

Sorties logicielles

- **Shapeshifter : le polymorphisme pour protéger les serveurs Web**
  http://www.lemondeinformatique.fr/actualites/lire-shape-security-utilise-le-polymorphisme-en-temps-reel-pour-proteger-les-serveurs-web-56348.html

- **NameTag la fin de l'anonymat dans la rue (reconnaissance faciale)**
  http://www.clubic.com/application-mobile/actualite-611124-reconnaissance-faciale-nametag-depasse-limites-google.html
  http://nametag.ws/

- **WPUpdate : un script pour mettre à jour WordPress automatiquement**
  WordPress installe désormais automatiquement les mises à jour, mais nécessite des droits étendus. Trustsec propose un script pour se charger de cela :
  https://www.trustedsec.com/january-2014/introducing-wpupdate-automatic-updates-wordpress/

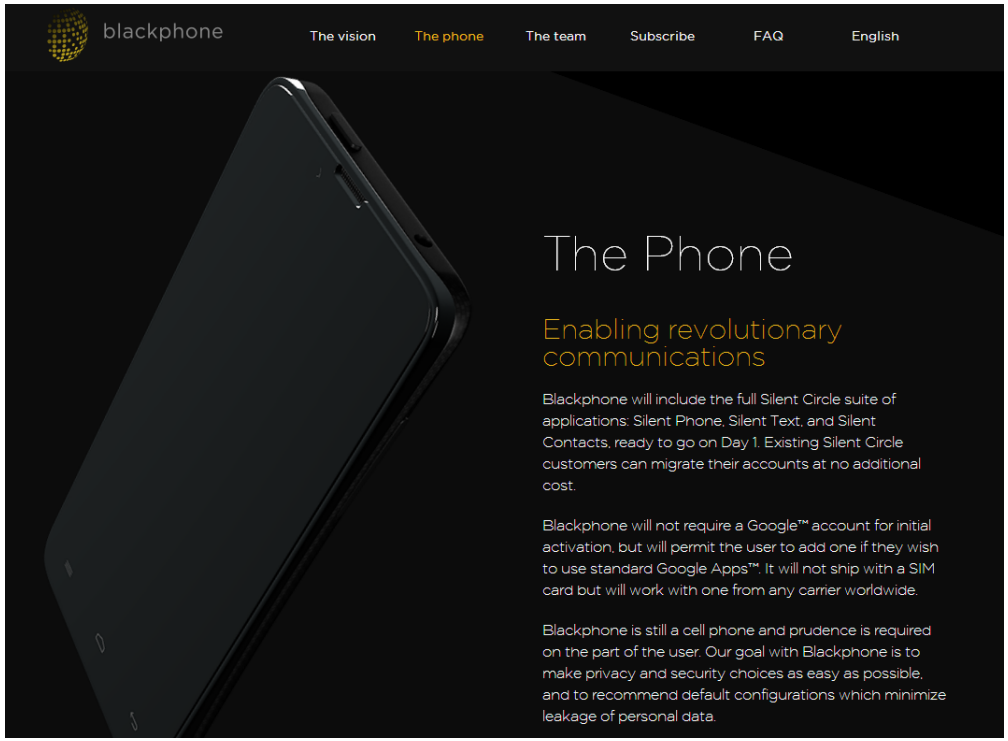
- **RedHat intègre CentOS**
  http://pro.01net.com/editorial/611474/linux-red-hat-integre-la-communaute-centos/

- **120 outils d'autopsie**
  http://forensiccontrol.com/resources/free-software/

Sorties matérielles

Blackphone

- Basé sur Android
- Avec Phil Zimmermann dans l'équipe de developpement
- http://www.presse-citron.net/blackphone-un-smartphone-ultra-securise-pour-dejouer-la-nsa



Blackphone.ch

Divers

- **NSA Cloud Backup**
  Souriez, vous êtes déjà abonnés ;-)
  https://www.youtube.com/watch?v=1tSTtmX3v3w

- **Nouvelle distribution Linux Free BSD 10.0**

  - Corrigé depuis…
    http://www.developpez.com/actu/66602/FreeBSD-10-0-abandonne-GCC-et-Bind-la-distribution-Linux-sort-avec-des-amelioration-de-son-temps-de-demarrage/
  - Mais toujours dans le cache Google ;-)
    http://webcache.googleusercontent.com/search?q=cache:AQcwYiv9TN0J:www.developpez.com/actu/66602/FreeBSD-10-0-abandonne-GCC-et-Bind-la-distribution-Linux-sort-avec-des-amelioration-de-son-temps-de-demarrage/+&cd=1&hl=fr&ct=clnk&gl=fr

- **Amazon autorise les app html5 sur son appstore**
  http://frenchweb.fr/amazon-autorise-la-vente-dapplications-web-html5-sur-son-appstore/139874

- **Petit quizz sur la DGSE**
  http://www.slate.fr/story/82001/quiz-dgse-marches-publics

Divers

- **Serveur HTTP en assembleur de moins de 4ko**
  http://canonical.org/~kragen/sw/dev3/server.s
- **Un palindrome amusant ;-)**
  - GSM SMS MSG
- **Don't feed the troll…**
  - Une critique par Bluetouff d'un article sur iTrust par le site Toulouse7.com
  - En réponse, iTrust fait un scan de vuln sauvage de BlueTouff
  - Effet Streisand garanti !
  - http://reflets.info/itrust-penteste-reflets-info-sans-notre-consentement-fic2014/
- **XBox Sign Out**
  https://www.youtube.com/watch?v=mWZLa4AnN5k#t=161
- **Pour faire plaisir à Nicolas**
  - Magic Quadrant Endpoint Protection 2014
    - "When 35% of reference customers for EPP (EndPoint Protection) solutions have been successfully compromised, it is clear that the industry is failing in its primary goal of keeping malicious code off PCs."
- **La plupart des distributeurs de billets sont sous Windows XP, que faire après l'arrêt du support**
  http://gizmodo.com/most-atms-are-still-running-windows-xp-which-is-about-1503367754
- **Un anti-virus empêche le paiement sur le web**
  http://www.le-paiement-sur-internet.fr/2014/01/avast-impacte-sur-le-3d-secure.html

Questions ?