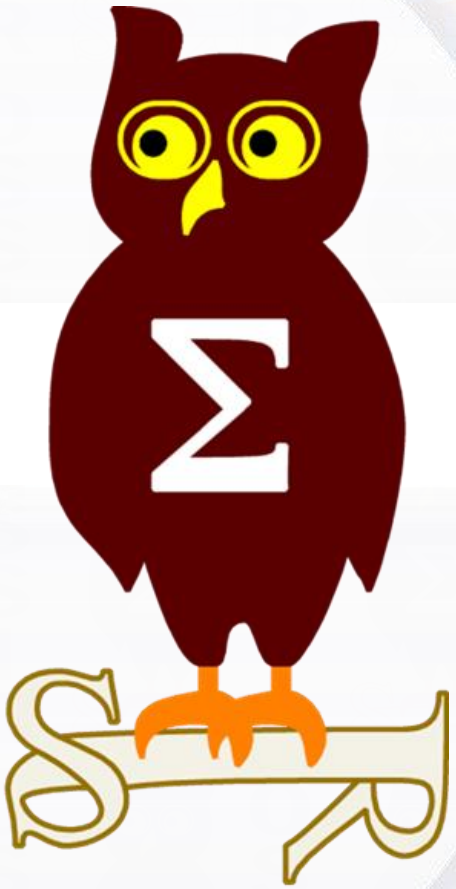


Revue d'actualité

09/09/2014

Préparée par

Jean-Philippe GAULIER
Ary KOKOS
Vladimir KOLLA
Arnaud SOULLIE

Failles / Bulletins / Advisories

Microsoft - Retour sur Juin 2014

MS14-35 (cf. Revue Juillet 2014)

- CVE-2014-2777 Contournement de la sandbox d'IE 8 à 11, pour écrire en local
- Que s'est il passé entre la découverte en 2011 et la diffusion en 2014 ?
  - 2011-02-12 - Vulnerability Discovered by VUPEN Security
  - 2014-03-14 - Vulnerability Reported to ZDI and Microsoft During Pwn2Own 2014
  - 2014-06-10 - Vulnerability Fixed by Microsoft
  - 2014-07-16 - Public disclosure

    http://packetstormsecurity.com/files/127495

Failles / Bulletins / Advisories

Microsoft - Avis Juillet 2014

MS14-037 Vulnérabilités dans Internet Explorer (24 CVE)  [Exploitabilité 1]

- Affecte:
  - Internet Explorer (toutes versions supportées)
  - Correctif également pour Windows XP Embedded POSReady, kb2962872 (cf. screenshot après)
- Exploit:
  - Exécution**s** de code à l'ouverture d'une page Web spécialement formatée
  - CVE-2014-2783 publiée publiquement et permettant de faire passer un certificat Wildward (*) pour un certificat Extended Validation (EV)
  - ...
- Crédits : *liste encore trop longue, donc voici un extrait 100% subjectif*
  - VUPEN par ZDI (CVE-2014-1763) 
  - Bo Qu de Palo Alto Networks **x 8** (CVE-2014-2785, CVE-2014-2786, CVE-2014-2787, CVE-2014-2788, CVE-2014-2789, CVE-2014-2798, CVE-2014-2800, CVE-2014-2801)
  - Eric Lawrence (CVE-2014-2783)

Failles / Bulletins / Advisories

Microsoft - Avis Juillet 2014

MS14-038 Vulnérabilité dans le Journal Windows (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportées)
  - Sauf Windows 2003 et 2008 Core
  - Correctif également pour Windows XP Embedded POSReady, kb2962872 (cf. screenshot après)
- Exploit:
  - Exécutions de code à l'ouverture d'un fichier .JNT spécialement formaté
  - Le Journal est peu utilisé mais présent par défaut
    - Permet de sortir des classiques doc/xls/pdf
- Crédits:
  - Hamburgers.maccoy@gmail.com (CVE-2014-1824)

MS14-039 Vulnérabilité dans le Clavier Visuel (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportées)
  - Sauf Windows 2003 et 2008 Core
- Exploit:
  - Élévation de privilèges. Combiné à une faille IE, permettrait une évasion de la sandbox
- Crédits:
  - lokihardt@asrt par ZDI (CVE-2014-2781)

Failles / Bulletins / Advisories

Microsoft - Avis Juillet 2014

MS14-040 Vulnérabilité dans AFD.sys (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportées)
  - Correctif également pour Windows XP Embedded POSReady, kb2962872 (cf. screenshot après)
- Exploit:
  - Ancillary Function Driver = support des sockets BSD et Raw Sockets
  - Élévation de privilèges
- Crédits:
  - Sebastian Apelt par ZDI (CVE-2014-1767)

MS14-041 Élévation de privilèges par DirectShow (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows Vista, 7, 8.x (Hors RT) 2008 (Hors Core et Itanium) et 2012
- Exploit:
  - Élévation de privilèges en utilisant DirectShow lors du traitement et la désérialisation d'objet "Stretch"
  - Contournement de Enhanced Protected Mode (EPM) en 32bits
  - Utilisé par VUPEN à Pwn2Own 2014
    http://www.zerodayinitiative.com/advisories/ZDI-14-221/
- Crédits:
  - VUPEN par ZDI (CVE-2014-2780)

http://packetstormsecurity.com/files/127500/Microsoft-Windows-DirectShow-Privilege-Escalation.html

Failles / Bulletins / Advisories

Microsoft - Avis Juillet 2014

MS14-042 Déni de service sur Microsoft Service Bus (1 CVE) [Exploitabilité 1]

- Affecte:
  - 2008 R2 64bits, 2012 et 2012 R2
- Exploit:
  - Déni de service distant, par l'envoie, par un utilisateur authentifié, d'un message Advanced Message Queuing Protocol (AMQP) Crédits:
- Crédits:
  - ?

MS14-043 Use After Free dans Windows Media Center (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows 7 (sauf Starter et Home Basic), Windows 8.x Pro
  - Add-on gratuit depuis Vista et payant sur Windows 8
- Exploit:
  - Exécution de code à l'ouverture d'un fichier office appelant le composant CSyncBasePlayer de Media Center (MCPlayer.dll)
- Crédits:
  - Alisa Esage (@alisaesage) / ZDI (CVE-2014-4060)

Failles / Bulletins / Advisories

Microsoft - Avis Aout 2014

MS14-044 Élévation de privilèges dans SQL Serveur (2 CVE) [Exploitabilité 1]

- Affecte:
  - SQL Server 2008 et 2008 R2, SQL Server 2012 SP1
  - 1er patch pour SQL Server 2014 (64bits seulement)
- Exploit:
  - XSS sur le composant SQL Master Data Services (MDS)
  - Déni de service lors du traitement de requêtes Transact-SQL spécialement formaté
- Crédits:
  - ?

Failles / Bulletins / Advisories

Microsoft - Avis Aout 2014

MS14-045 Failles Noyau dans win32k.sys (3 CVE) [Exploitabilité 1]

- Affecte:
  - Windows, toutes versions supportées
- Exploit:
  - Divulgation d'information (adresses mémoires) lors de l'allocation de pool (CVE-2014-4064)
  - Elévation de privilèges (noyau) due à la gestion de la mémoire des objets d'un thread de fenêtre (CVE-2014-0318)
  - Elévation de privilèges lors du traitement d'un fichier de police de caractères spécialement formaté (Font Double Fetch) (CVE-2014-1819)
    - BSOD au reboot si :
      - Polices de caractères OpenType Font (OTF) dans un répertoire non standard
      - Chemin complet dans la base de registre

      http://nakedsecurity.sophos.com/2014/08/18/microsoft-pulls-patch-tuesday-kernel-update-ms14-045-can-cause-blue-screen-of-death
- Crédits:
  - Wang Yu de Qihoo 360 (CVE-2014-1819)
  - Ilja Van Sprundel (CVE-2014-4064)

Failles / Bulletins / Advisories

Microsoft - Avis Aout 2014

MS14-046 Contournement d'ASLR depuis .Net (1 CVE) [Exploitabilité 1]

- Affecte:
  - .Net 2, 3, 3.5 sauf SP1, 3.5.1
  - Donc Windows Vista à 8 (sauf RT), 2008, 2008 R2 et Core, 2012, 2012 R2 et Core
- Exploit:
  - Contournement d'ASLR à la visite d'une page Web spécialement formatée
  - Nécessite une autre vulnérabilité pour une exécution de code
- Crédits:
  - ?

MS14-047 Contournement d'ASLR depuis LRPC (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows 7, 8.x et RT, 2008 R2 SP1, 2012, 2012 Core et R2
- Exploit:
  - Contournement d'ASLR lors du traitement d'un message RPC malformé. Les données associées au message ne sont pas libérées en mémoire
  - Nécessite une autre vulnérabilité pour une exécution de code
- Crédits:
  - ?

Failles / Bulletins / Advisories

Microsoft - Avis Aout 2014

MS14-048 Exécution de code dans OneNote (1 CVE) [Exploitabilité 1]

- Affecte:
  - Microsoft OneNote 2007 SP3
- Exploit:
  - Exécutions de code à l'ouverture d'un fichier OneNote spécialement formaté
- Crédits:
  - Eduardo Prado par Beyond Security (CVE-2014-2815)

MS14-049 Élévation de privilèges dans Windows Installer (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows toutes versions supportées
- Exploit:
  - Élévation de privilèges à l'exécution d'un programme tentant de réparer une installation existante
- Crédits:
  - Denis Gundarev de Entisys (CVE-2012-4784)
  - Stepfan Kanthak pour l'aide apportée

MS14-050 Élévation de privilèges dans Sharepoint Serveur (1 CVE) [Exploitabilité 1]

- Affecte:
  - Sharepoint 2013, 2013 SP1
- Exploit:
  - Contournement des permissions des applications Sharepoint permettant d'exécuter un script sur le serveur
- Crédits:
  - ?

Failles / Bulletins / Advisories

Microsoft - Avis Aout 2014

MS14-051 Multiples vulnérabilités dans Internet Explorer (26 CVE) [Exploitabilité 1]

- Affecte:
  - Toutes versions supportées sauf Core
  - Correctif également pour Windows XP Embedded POSReady, kb2962872 (cf. screenshot après)
- Exploit:
  - Exécutions de code et élévations de privilèges
  - Blocage (Ou alerte) concernant les ActiveX obsolètes
    - **Repoussé** du 12 août au 9 septembre suite à des retours d'utilisateurs sur le délai trop court pour s'adapter

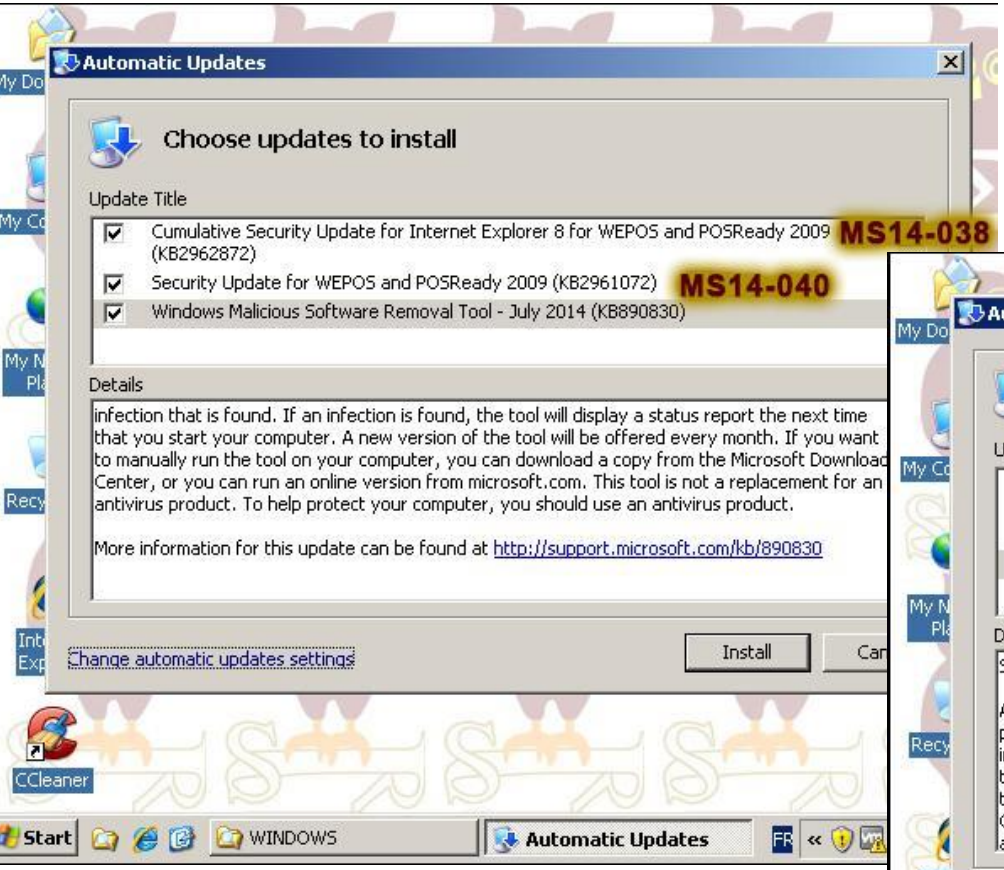
    http://blogs.msdn.com/b/ie/archive/2014/08/06/internet-explorer-begins-blocking-out-of-date-activex-controls.aspx
    http://blogs.technet.com/b/security/archive/2014/08/13/ie-increases-protections-implements-out-of-date-activex-control-blocking.aspx
- Crédits: *liste très, extrait 100% subjectif avec de plus en plus d'asiatiques*
  - Bo Qu de Palo Alto Networks **x 3** (CVE-2014-2796, CVE-2014-2821, CVE-2014-2822)
  - Chen Zhang (demi6od) de NSFOCUS Security Team **x 5** (CVE-2014-2808, CVE-2014-2810, CVE-2014-2823, CVE-2014-2825, CVE-2014-2826)
  - Yujie Wen de Qihoo 360 **x 2** (CVE-2014-2784, CVE-2014-2824)
  - Zeguang Zhao de Team509 et Liang Chen de KeenTeam (@K33nTeam) par ZDI (CVE-2014-2819)

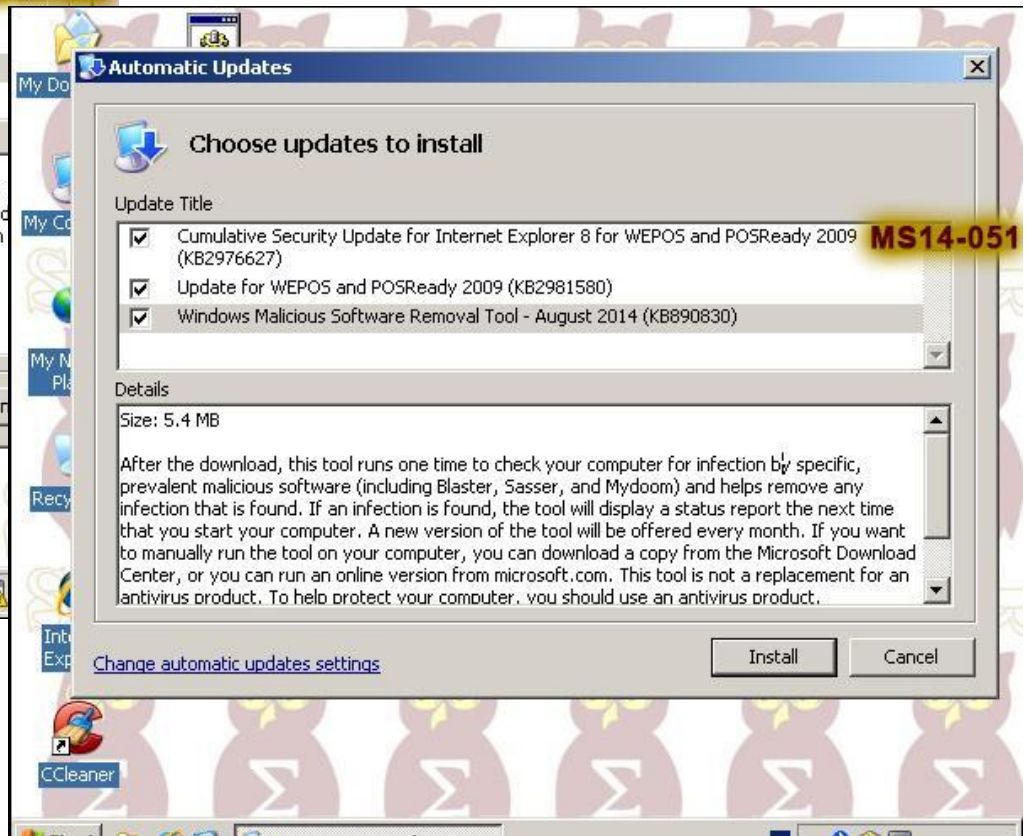
Failles / Bulletins / Advisories

Microsoft - Avis Juillet/Aout 2014

Mise à jour pour Windows XP Embedded POSReady

- Encore et toujours sans documenter dans les bulletins…





Failles / Bulletins / Advisories

Microsoft - Advisories et Revisions Juillet/Aout 2014

2982792 Révocation de certificats SSL

- v1.0 Révocation des AC du “National Informatics Centre” Indien (cf. Divers / Trolls velus)
  - NIC Certifying Authority
  - NIC CA 2011
  - NIC CA 2014
- v2.0 Ajout du support de Windows Server 2003

2915720 Vérification des signatures Authenticode des binaires

- v1.4 Devient optionnel du fait de l’activation du correctif MS13-098 au 12 août 2014
  - MS13-098 : modification d'un exécutable sans invalider sans signature

2755801 Mise à jour de Flash Player

- v27.0 Nouvelle mise à jour de Flash Player

2981580 Modification cumulatives des fuseaux horaires

- Toutes version supportée dont "Windows XP Embedded" (Windows XP Embedded POSReady)
- Modification cumulatives pour Jordanie, Fiji, Paraguay, Turquie, Egypte...
  - Heure d'été
  - Nouveaux lieu de fuseaux horaires

Failles / Bulletins / Advisories

Microsoft - Autre

Fin de support standard de Windows 7 SP1 au 31 janvier 2015

- Fin des mises à jour de sécurité prévue pour janvier 2020
  http://support.microsoft.com/gp/support-reaching-end-2nd

Fin du support de Java 7 sur Windows XP

http://java.com/en/download/help/sysreq.xml

Windows XP Unofficial SP4

- Affecte:
  - Windows XP, MCE et Tablet PC.
  - Microsoft .NET Frameworks 4.0, 3.5, 1.1 et 1.0
  - Inclusion de l'astuce faisant passer son XP pour "Windows XP Embedded POSReady"

http://www.ryanvm.net/forum/viewtopic.php?t=10321&postdays=0&postorder=asc&start=0

Failles / Bulletins / Advisories

Microsoft - Avis publics

MQAC.sys et BthPan.sys (CVE-2014-4971)

- Affecte:
  - Windows XP SP3
- Exploit **MQAC.sys** (Microsoft MQ Access Control) :
  - Injection de code en mémoire et exécution de code par l'écrasement de HalDispatchTable+0x4 puis l'appel à NtQueryIntervalProfile
    - 2014.04.28 - Initial contact; sent Microsoft report and PoC.
    - 2014.04.28 - Microsoft acknowledges [...] XP is no longer supported [...]
    - ...
    - 2014.07.18 - Public disclosure

http://packetstormsecurity.com/files/127536/Microsoft-XP-SP3-MQAC.sys-Arbitrary-Write-Privilege-Escalation.html

- Exploit **BthPan.sys** (Microsoft Bluetooth Personal Area Networking) :
  - Injection de code en mémoire et exécution de code par l'écrasement de HalDispatchTable+0x4 puis l'appel à NtQueryIntervalProfile
    - 2014.04.28 - Initial contact; sent Microsoft report and PoC.
    - 2014.04.28 - Microsoft acknowledges [...] XP is no longer supported [...]
    - ...
    - 2014.07.18 - Public disclosure.

http://packetstormsecurity.com/files/127535/Microsoft-XP-SP3-BthPan.sys-Arbitrary-Write-Privilege-Escalation.html

- Crédit: VUPEN

Failles / Bulletins / Advisories

Microsoft - Divers

Insecure Temporary File Dropping + Vidéo

- Fichiers RTF “Drop File” (ActiveX "Package") + Dll-Preloading d’une autre appli faillible
  http://blogs.mcafee.com/mcafee-labs/dropping-files-temp-folder-raises-security-concerns
  http://justhaifei1.blogspot.fr/2014/08/demonstration-of-windowsoffice-insecure.html

Exécution de Javascript depuis RunDLL32

- Utilisé dans la nature par le malware Win32/PowerLiks.A
  http://www.kernelmode.info/forum/viewtopic.php?f=16&t=3[illegible]7

```
C:\>rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";document.write("\74script
  language=javascript>"+(new%20ActiveXObject("WScript.Shell")).Run("calc.exe")+"\74/scrip
  t>")
```

Azure en panne (Cloud de Microsoft)

- Plusieurs pannes entre le 15 et le 19 aout
  http://azure.microsoft.com/en-us/status/#history

Failles / Bulletins / Advisories

Système (principales failles)

Linux LibXML2

- Déni de service par consommation excessive de la mémoire
  - parser.c:xmlParserHandlePEReference() (CVE-2014-0191)
  - Sur du prolog ;-)

  http://www.debian.org/security/dsa-2978
- Sortie du correctif Debian 2 mois après RedHat !!?

  https://access.redhat.com/security/cve/CVE-2014-0191

Apache 2.4.x

- mod_status (activé par défaut)
- Exécution de code à distance par un heap overflow (CVE-2014-0226)

  http://mail-archives.apache.org/mod_mbox/httpd-cvs/201407.mbox/%3C20140714195504.EF60D23889E2@eris.apache.org%3E

Failles / Bulletins / Advisories

Système (principales failles)

Librairie LZO (Surface d'attaque gigantesque, mais exploitation complexe)

- Affecte:
  - Le noyau Linux
  - Android
  - FreeBSD
  - Les systèmes de fichier ZFS (de SUN pour Solaris et Sparc, mais également FreeBSD, FreeNAS, FreeBSD…) et ButterFS (BRFS, encore en développement et censé remplacer Ext4)
  - OpenVPN
  - MPlayer2 et FFmpeg
  - LibAV
  - MySQL
  - Hadoop
  - On trouve même une librairie faillible sur la planète Mars, dans le robot « Mars Curiosity » !
- Exploit:
  - Dépassement d'entier

  http://www.theregister.co.uk/2014/07/11/firefox_lzo_rce/
- Crédits:
  - Ludwig Strigeus

Failles / Bulletins / Advisories

Réseau (principales failles)

Cisco

- Firewall ASA 55xx
  - Déni de service dû à l'inspecteur de protocole “inspect” (CVE-2013-5567)
- Cisco Unified Communications Domain Manager
  - Clef SSH commune sur tous équipements

http://www.securityweek.com/default-ssh-private-key-exposes-ciscos-voip-manager-remote-attack

Juniper

- JunOS
  - Déni de service sur des flux SIP (CVE-2014-3815)
  - Élévation de privilèges et exécution de commandes en root pour un utilisateur non-authentifié (CVE-2014-3816)
  - Dénis de service en cas de translation IPv4 vers IPv6 (CVE-2014-3817, CVE-2014-3822)
  - Déni de service lors du traitement de paquets PIM (Multicast) (CVE-2014-3819)
  - XSS (CVE-2014-3821)

http://kb.juniper.net/JSA10633 , http://kb.juniper.net/JSA10634 , http://kb.juniper.net/JSA10635 , http://kb.juniper.net/JSA10637 , http://kb.juniper.net/JSA10640 , http://kb.juniper.net/JSA10641

Citrix

- NetScaler Gateway (Souvent exposé en frontal d'internet)
  - XSS réfléchit (CVE-2014-4346)
  - Fuite de cookie (CVE-2014-4347)

http://support.citrix.com/article/CTX140863

Failles / Bulletins / Advisories

Réseau (principales failles)

Une backdoor dans les routeurs Netis/Netcore

- Un mot de passe codé en dur permet de se connecter à distance
- 2 millions de routeurs accessibles sur Internet, principalement en Chine
- La recommandation : remplacer le matériel :)

  http://www.theregister.co.uk/2014/08/27/netis_routers_have_a_backdoor_say_reserachers/?mt=1409159264121

  http://blog.trendmicro.com/trendlabs-security-intelligence/netis-routers-leave-wide-open-backdoor/

Failles / Bulletins / Advisories

Virtualisation

QEmu 0.1.x / OpenStack 3.0 et 4.0

- Évasion de la machine virtuelle
  - Exécutions de code dans l'hôte (hyperviseur) en exploitant plusieurs failles dans les pilotes VirtIO (net, scsi et usb)
    - CVE-2013-4148, CVE-2013-4151, CVE-2013-4535, CVE-2013-4536, CVE-2013-4541, CVE-2013-4542, CVE-2013-6399, CVE-2014-0182, CVE-2014-3461

https://rhn.redhat.com/errata/RHSA-2014-0888.html

VirtualBox

- Évasion de la machine virtuelle
  - Exécution de code dans l'hôte (hyperviseur) en exploitant une faille de l'accélération 3D de VirtualBox 3D pour OpenGL
  - Exploitation stable sous Windows 64 bits
    - CVE-2014-0983

http://www.vupen.com/blog/20140725.Advanced_Exploitation_VirtualBox_VM_Escape.php

Xen Desktop (En plein essor du VDI)

- Accès non autorisé d'un utilisateur au poste virtuel d'un autre
  - Si ShutdownDesktopsAfterUse désactivé et fonctionnement par polling
    - CVE-2014-4700

http://support.citrix.com/article/CTX139591

Failles / Bulletins / Advisories

Virtualisation

FireEye

- Rooter une appliance AX 5400
  http://blog.silentsignal.eu/2014/07/28/how-to-got-root-access-on-fireeye-os/

- Malware Analysis System (MAS) 6.4.1
  - XSS, CSRFet SQLi
  - Cf. “Divers / Troll”

  http://pastebin.com/PWvU62tG

Failles / Bulletins / Advisories

Apple

iOS et ses Backdoors

« Great security of iOS has been compromised… by Apple… by design »

- Récupération de (quasiment) tout
  - Capture de Paquets : libpcap par défaut sur les iOS
    - Il est légitime de demander l'intérêt de cette capacité sur des smartphones et tablettes personnels
  - Contournement du chiffrement des sauvegardes
  - Contournement du code pin ou l'empreinte digitale
  - Récupération de données (photo, contacts, logs gps, clavier…) même effacées (Liste complète au slide 23).

  http://www.zdziarski.com/blog/?p=3441

  https://pentest.com/ios_backdoors_attack_points_surveillance_mechanisms.pdf
- Réponse d'Apple
  - Pas de Backdoor, juste du "troubleshooting "

  http://www.zdziarski.com/blog/?p=3447

Pendant ce temps, en Chine…

- Selon F-Secure, le chinois **Xiaomi** collecterait les données des utilisateurs de façon systématique avec son nouveau modèle RedMi 1S (envoi à un serveur à Pékin numéro IMEI, numéro IMSI, le détail de tous les contacts et les messages textes)

  http://securityaffairs.co/wordpress/27486/security/xiaomi-handset-usersdata.html

  http://www.f-secure.com/weblog/archives/00002731.html

Failles / Bulletins / Advisories

Apple

Brute force iCloud

- Possibilité de réaliser une attaque par brute force
  - Grâce à l'API "Find My iPhone"
  - Sans seuil limite

  https://github.com/hackappcom/ibrute/
- Intéressant, combiné à "Elcomsoft Phone Password Breaker 3.01"
  - ou tout autre outil du même acabit

Failles / Bulletins / Advisories

Google

Rapports d'erreur de Chrome avec l'extension GPG

- <<How safe are private keys in memory?
  Please note that enabling Chrome's "Automatically send usage statistics and crash reports to Google" means that, in the event of a crash, parts of memory containing private key material might be sent to Google.>>
  https://code.google.com/p/end-to-end/
- Au fait, avez vous activé la synchronisation des favoris ?
  http://www.numerama.com/magazine/30290-comment-chrome-envoie-tous-vos-mots-de-passe-a-google.html

Chrome

- Correction de 50 vulnérabilités
- Support du 64bits sous Windows

Failles / Bulletins / Advisories

Facebook

Désanonymisation d'un visiteur de votre site grâce à Facebook

- CSP / Content-Security-Policy + www.facebook.com/me
- Le visiteur doit être authentifié sur Facebook et utiliser Chrome
- Fonctionnel sur une petite population, irréaliste à grande échelle
  http://www.myseosolution.de/deanonymizing-facebook-users-by-csp-bruteforcing/

Failles / Bulletins / Advisories

Crypto

LibreSSL + Linux = Problème de PRNG

- Risque de générer des PRN identiques après plusieurs fork
  - Car le PID d'un processus fils, peut être le même que celui du grand-père

  https://www.agwa.name/blog/post/libressls_prng_is_unsafe_on_linux
- Exemple fonctionnel

  https://gist.github.com/AGWA/eb84e55ca25a7da1deb0
- Corrigé depuis

  http://opensslrampage.org/post/91910269738/fix-for-the-libressl-prng-issue-under-linux
- Conclusion
  - Même avec les meilleures intentions, forker OpenSSL n'est pas si simple et présente des risques

Attaques offline sur WPS

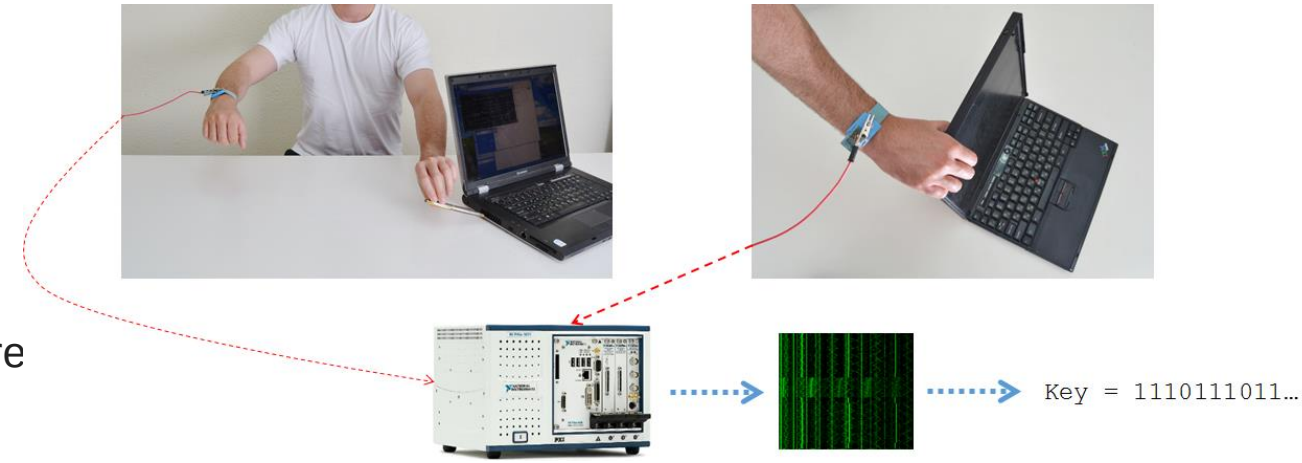
- Début de négociation WPS puis cassage hors-ligne
- Des implémentassions sont vulnérables
  - PRNG faible
  - Seed toujours à NULL
- Conclusion (Excessive?) : Disable WPS Now !

  http://fr.slideshare.net/0xcite/offline-bruteforce-attack-on-wifi-protected-setup

Toucher un ordinateur pour voler ses clefs

- Un nouveau canal auxiliaire démontré par 3 universitaires de Tel-Aviv
  - Mesure du signal électrique en touchant le métal du châssis, un port ethernet, vga, USB…
  - Extraction avec succès de clefs RSA 4096bits et ElGamal 3072 bit

  http://www.cs.tau.ac.il/~tromer/handsoff/



- La contre

Failles / Bulletins / Advisories

Divers

Les coffres forts d'hôtel ne sont pas sécurisés

- En lisant la doc :
  - Master key rarement changée
  - Procédure de réinitialisation
- Certains coffres forts doivent être activés par une carte bancaire
  - Possible de les reprogrammer pour voler le contenu de la piste magnétique des cartes utilisées.

http://www.net-security.org/secworld.php?id=17137

Prise de contrôle de 2 milliards de smartphones

- Protocole OMA

http://www.wired.com/2014/07/hackers-can-control-your-phone-using-a-tool-thats-already-built-into-it/

Android Fake ID

- Usurpation de l'identité d'une autre application car... l'installer ne vérifie pas la chaîne de certification

http://bluebox.com/blog/technical/android-fake-id-vulnerability/

Injection de Malware par LATEX

- A base de \write

http://cseweb.ucsd.edu/~hovav/dist/tex-login.pdf

Failles / Bulletins / Advisories

Divers

Exploiter les fonctions “Export CSV/Excel/OpenOffice” des sites web

- Les consultants de Context propose un nouveau vecteur d’attaque basé sur l’injection de macro dans des fichiers de tableur, en insérant le signe “=” dans les valeurs de certains champs
- Une fois le fichier exporté vers Excel, la macro va s’exécuter
- Utilisation du protocole DDE (*Dynamic Data Exchange*) pour lancer un exécutable depuis Excel
- Sur Open/Libre Office, certaines macros pouvaient s’exécuter avant un message d’information, mais la vulnérabilité a été corrigée depuis
  http://contextis.com/blog/comma-separated-vulnerabilities/

Failles / Bulletins / Advisories

Divers

Piratage et désactivation de certains systèmes d'alarme

- Classique : Mot de passe en dur, fréquences radio facilement accessibles et déchiffrabl

  http://www.wired.com/2014/07/hacking-home-alarms/

Modification des firmwares USB : BadBios

https://srlabs.de/blog/wp-content/uploads/2014/07/SRLabs-BadUSB-BlackHat-v1.pdf

Empreinte unique d'un navigateur / tracking

- Après :
  - Les flash cookies
  - Le stockage de données en HTML 5 (LocalStorage)
  - L'image unique générée par visiteur
  - L'empreinte unique des capteurs de mouvement des Smarphones (Gyroscope, boussole...)
  - L'empreinte unique du micro
- Voici l'empreinte unique, basée sur les différences de calculs des canvas

  http://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block

  https://securehomes.esat.kuleuven.be/~gacar/persistent/the_web_never_forgets.pdf
- Utilisé par AddThis
  - Suite à cette révélation, YouPorn a désactivé la fonctionnalité
- Liste des sites utilisant cette méthode

  https://securehomes.esat.kuleuven.be/~gacar/sticky/index.html

Failles / Bulletins / Advisories

Divers

Le Blackphone rooté en 5 minutes.

- Par des failles Android
  http://www.ubergizmo.com/2014/08/blackphone-rooted-in-five-minutes-at-blackhat-conference/

Leak de Hex-Rays IDA Pro 6.5 + ARM.Decompiler.v1.7.0

- Non, nous ne fournirons pas de lien :-)

Leak de licences Hex-Rays IDA Pro 5.x à 6.4

- Dont celles de Microsoft, Symantec...

Failles / Bulletins / Advisories

Internet of (insecure) things

Les firmwares des objets connectés sont vraiment troués

- Étude de chercheur d'Eurocom sur 26 275 firmwares
  - Routeurs, imprimantes, voip, caméras…
- Avant de passer à la sécurité, ils ont constaté que :
  - 86% des firmwares sont basés sur Linux, ce qui n'est pas une mauvaise chose
    - Le reste étant basé sur Vx-Works, Nucleus RTOS et Windows CE
  - 63% des firmwares tournent sur des CPU ARM
    - Le reste sur du MIPS ou d'autres choses plus exotiques
- Vulnérabilités classiques :
  - Mots de passe en dur
  - Clefs SSH en dur également
  - Mots de passe triviaux
  - Portes dérobées
  - Applications ou services intégrés mais très anciens, donc vulnérables
  - Exécution de tous les processus en root
  - Serveur web mal configurés ou faillibles
  - …

http://www.eurecom.fr/fr/publication/4323/download/rs-publi-4323.pdf

Failles / Bulletins / Advisories

Internet of (insecure) things

Dyson 360 Eye

- Un robot aspirateur mobile
  - + une caméra à 360°
  - + une connexion à internet
- What could possibly go wrong ?

  http://www.clubic.com/video/ifa-2014/video-ifa-2014-360-eye-l-aspirateur-intelligent-selon-dyson-454401.html

Piratages, Malwares, spam, fraudes et DDoS

Malwares

Pitty Tigger

- Forensique d’un cyber espionnage par Cassidian
- En activité depuis 2010 mais découvert en 2014
- Infections par Spear phishing, parfois signés avec de vraies clefs, volées grâce à HeartBleed
- Attaque peut-être d'origine Chinoise

http://blog.cassidiancybersecurity.com/post/2014/07/The-Eye-of-the-Tiger2
http://bitbucket.cassidiancybersecurity.com/whitepapers/downloads/Pitty%20Tiger%20Final%20Report.pdf

Piratages, Malwares, spam, fraudes et DDoS

Malwares

Energetic Bear - Crouching Yeti

- Cyber espionnage d'entreprises, principalement des secteurs industriel et énergétique
- En activité depuis 2010
- Infections par :
  - Spear phishing avec une faille Flash dans un PDF (CVE-2011-0611)
  - Waterholing avec des failles java et internet explorer
  - Installeur légitimes "repackagés"
- "Command and Control" sur des sites légitimes piratés
- Recherche de SCADA sur le réseau
- Quelques perles :
  - The OPC module strings include typos and bad grammar. Some are so bad they are almost silly [...]
  - There are also three interesting strings inside the Karagany backdoor: identifiant (which is French for identifier), fichier (French for file) and liteliteliteskot (lite scotis Swedish for little sheet)
  - There is nothing especially sophisticated in the exploits used

http://securelist.com/files/2014/07/EB-YetiJuly2014-Public.pdf

Piratages, Malwares, spam, fraudes et DDoS

Malwares

Decrypt Cryptolocker

- Fox-it et FireEye récupèrent des clefs privées sur des serveurs saisis
  - et montent un portail permettant déchiffrer ses fichiers

https://www.decryptcryptolocker.com

Le malware “Backoff” visant les POS a été “sinkholé”

- Une centaine de clients infectés, mais ne représentent que 5% du total

https://securelist.com/blog/research/66305/sinkholing-the-backoff-pos-trojan/

Kaspersky met à jour une campagne de spear-phishing nommée « Machete »

- Plus de 770 victimes en 4 ans principalement en Amérique latine

http://www.scmagazineuk.com/targeted-spear-phishing-campaign-targets-governments-law-enforcement/article/367133/
https://securelist.com/blog/research/66108/el-machete/

Icoscript

- Malware communiquant grâce aux webmails publiques

https://www.virusbtn.com/pdf/magazine/2014/vb201408-IcoScript.pdf

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Piratage de LiveBox Orange

- Modification des DNS de certains modèles de LiveBox avec les identifiants par défaut
- Man-in-the-Middle
- Corrigé depuis (DNS non modifiable)

http://www.01net.com/editorial/624138/des-milliers-de-livebox-orange-piratees-par-un-detournement-de-dns/

Vol d'identifiants de banque suisse suivant plusieurs vecteurs

- Installation du Malware Retefe par Spear Phishing
  - Modifiant les DNS
  - Ajoutant une nouvelle AC
- Proposition d'installation d'une App Android pour sécuriser son compte bancaire ;)
  - Interception des SMS contenant un code d'authentification pour la banque

http://www.theregister.co.uk/2014/07/23/ruskie_vxers_change_dns_nuke_malware_in_swiss_bank_raids/

Entre 1,2 et 4,5 milliards de comptes volés par des Russes

- par le piratage de 420 000 sites (SQLi)
- Propose d'envoyer son mot de passe pour savoir s'il fait partie des comptes volés….

http://www.holdsecurity.com/news/cybervor-breach/

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

UPS a détecté un malware sur ses terminaux de paiement dans 51 boutiques aux US

- Près de 100 millions de transactions ont pu être interceptées
- Le malware a été détecté lors d'un audit commandité par UPS suite à un bulletin de l'US-CERT métant en garde contre les malwares sur les POS

http://www.theregister.co.uk/2014/08/20/ups_raises_hands_owns_up_to_hack/?mt=1408606018691

http://www.ups.com/pressroom/us/press_releases/press_release/Press+Releases/Current+Press+Releases/ci.The+UPS+Store%2C+Inc.+Notifies+Customers+Of+Potential+Data+Compromise+and+Incident+Resolution.syndication

Le régulateur du nucléaire américain (NRC) piraté 3 fois en 3 ans

- Du phishing, du phishing et encore du phishing

http://www.networkworld.com/article/2466707/microsoft-subnet/nuclear-regulatory-commission-hacked-3-times-in-3-years.html

SynoLocker

- Attaque automatisée chiffrant les fichiers du NAS et demandant une rançon de 0,6 bitcoins
- Exploitation en juillet 2014 d'une faille corrigée en décembre 2013

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Gamma International Ltd, piratée

- Entreprise germano-anglaise développant FinFisher (trojan) pour les agences gouvernementales
- 40 GB de données internes liées à leurs solutions de surveillance ont été volées, ainsi qu'une partie de la liste des clients
- La majorité des fichiers intéressants sont chiffrés, dont du code source (GPG)
  - Restent les présentations commerciales, les tarifs… (cf. Slide suivant)

http://www.zdnet.com/top-govt-spyware-company-hacked-gammas-finfisher-leaked-7000032399/

http://www.scmagazineuk.com/government-spyware-exposed-after-massive-data-breach/article/365047/

http://www.reddit.com/r/Anarchism/comments/2cjlop/gamma_international_leaked/

http://pastebin.com/kZQ5J0js

http://pastebin.com/raw.php?i=cRYvK4jb

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Gamma International Ltd, piratée (suite)

				Costs		End-user Price		Elaman Price		Agent & Reseller Price		ırk-up from FinFisher Market Pr		ırk-up from Agent & Resell	
						Discount SW & Support		25,00% scount SW & Support		20,00%				Discount SW & Support	2
						Discount HW & Training		15,00% scount HW & Training		10,00%				Discount HW & Training	1
ITEM	DESCRIPTION	MODEL	QTY	UNIT PRICE EURO	LINE TOTAL EURO	UNIT PRICE EURO	LINE TOTAL EURO	UNIT PRICE EURO	LINE TOTAL EURO	UNIT PRICE EURO	LINE TOTAL EURO	UNIT PRICE EURO	LINE TOTAL EURO	UNIT PRICE EURO	LINE TOT EURO
PRICE OVERVIEW															
A	**Tactical Intrusion Solutions**														
1	FinIntrusion Kit		1				30 600,00		23 250,00		24 780,00		32 211,00		26 0
2	FinUSB Suite		1				13 080,00		10 110,00		10 764,00		13 769,00		11 3
3	FinFireWire		1				13 080,00		10 110,00		10 764,00		13 769,00		11 3
B	**Remote Intrusion Solutions**														
1	FinSpy		1				1 445 940,00		1 093 172,00		1 165 356,00		1 522 176,00		1 226 7
2	FinSpy Test system		1				60 000,00		45 000,00		48 000,00		63 158,00		50 5
3	Extension: FinSpy Data Submission (LEMF Integration)		1				91 128,00		68 346,00		72 903,00		95 925,00		76 1
C	**Remote Deployment Tools**														
1	FinFly USB		1				4 620,00		3 519,00		3 750,00		4 864,00		3 9
2	FinFly LAN		1				50 637,60		39 349,00		41 881,00		53 304,00		44 0
3	FinFly Web		1				55 581,60		42 997,00		45 776,00		58 510,00		48 1
4	FinFly Net		1				205 523,00		162 335,00		172 610,00		216 342,00		181 6
5	FinFly Exploit		1				698 134,00		580 800,00		577 000,00		734 881,00		587 9
D	**IT Intrusion Training Program**														
1	Basic IT Intrusion		1				21 000,00		17 850,00		18 900,00		22 106,00		19 89
2	Advanced IT Intrusion		1				21 000,00		17 850,00		18 900,00		22 106,00		19 89
3	Wireless IT Intrusion		1				25 560,00		21 726,00		23 004,00		26 906,00		24 2
4	Practical Software Exploitation		1				27 000,00		22 950,00		24 300,00		28 422,00		25 57
5	Practical Software Exploitation (Extended)		1				27 000,00		22 950,00		24 300,00		28 422,00		25 57
6	Practical Web Application Exploitation		1				27 000,00		22 950,00		24 300,00		28 422,00		25 57
7	Practical Web Application Exploitation (Extended)		1				27 000,00		22 950,00		24 300,00		28 422,00		25 57
8	Practical Penetration Testing		1				27 000,00		22 950,00		24 300,00		28 422,00		25 57
9	Practical Penetration Testing (Extended)		1				27 000,00		22 950,00		24 300,00		28 422,00		25 57
10	Training in FinFisher Facilities		1				29 575,26		29 575,26		29 575,26		29 575,26		29 57
11	Custom IT Intrusion Training Courses & Consulting on Request						On Request		On Request		On Request		On Request		On Re
						SUBTOTAL I	2 927 459,46	SUBTOTAL I	2 303 689,26	SUBTOTAL I	2 409 763,26	SUBTOTAL I	3 080 134,26	SUBTOTAL I	2 515 633
						DISCOUNT		DISCOUNT		DISCOUNT		DISCOUNT		DISCOUNT	
						SUBTOTAL II		SUBTOTAL II		SUBTOTAL II		SUBTOTAL II		SUBTOTAL II	
						FREIGHT	3 500,00	FREIGHT	3 500,00	FREIGHT	3 500,00	FREIGHT	3 500,00	FREIGHT	3 50
						TOTAL PRICE	2 930 959,46	TOTAL PRICE	2 307 189,26	TOTAL PRICE	2 413 263,26	TOTAL PRICE	3 083 634,26	TOTAL PRICE	2 519 133

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Vol (?) de 4,5 millions de données personnelles aux USA

- Par l'intermédiaire de la société de service qui gère l'IT des hôpitaux américains : Community Health Systems
  - Nom, prénom, n° sécurité sociale, adresse, n° de téléphone…
- Exploitation de HeartBleed sur les VPN SSL Juniper (Secure Access ou Media Access Gateway)
  - Pour voler et usurpé l'identité des collaborateurs

    https://www.trustedsec.com/august-2014/chs-hacked-heartbleed-exclusive-trustedsec/
  - Alors que cette solution permet l'authentification par certificat ou OTP pour les VPN
- Selon FireEye/Mandiant, ce seraient les chinois

  Pour aider l'industrie pharmaceutique chinoise à soigner le cancer

  http://www.fireeye.com/blog/technical/2014/08/searching-for-the-cure-targeted-threat-actors-pursuing-the-pharmaceutical-industry.html
- D'après Mandiant, les attaquants Chinois cherchaient à voler des informations sur les équipements médicaux mais le système de défense les en a empêchés. Les autorités confirment pour le moment qu'aucun dossier médical n'aurait été volé

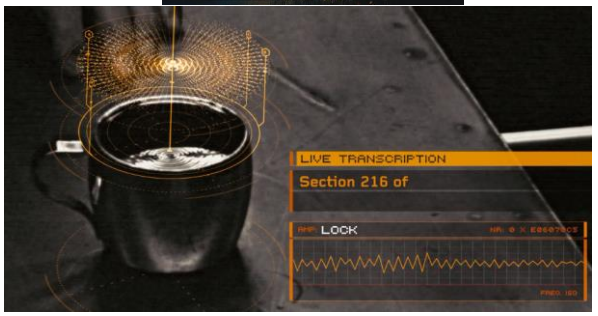
  http://www.theregister.co.uk/2014/08/18/hospital_chain_claims_chinese_hackers_stole_45_million_user_details/
  http://www.theregister.co.uk/2014/08/20/heartbleed_chs_hospital_mega_breach_link/
  https://www.trustedsec.com/august-2014/chs-hacked-heartbleed-exclusive-trustedsec/
  http://www.sec.gov/Archives/edgar/data/1108109/000119312514312504/d776541d8k.htm

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Enregistrement des sons grâces aux vibrations des objets

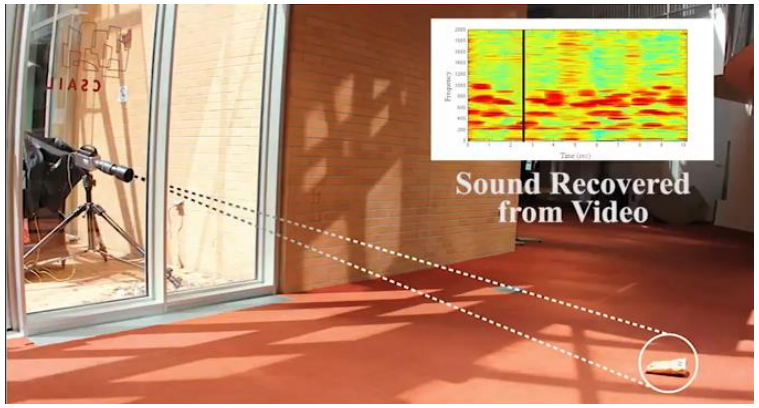
- 2008 Spielberg produit un (mauvais) film : Eagle Eye
  - Une IA de la défense US décide de tout contrôler
  - Scène irréaliste : écoute d'une conversation par les vibrations d'une tasse à café (01:23:00)



- 2014 le MIT réalise l'écoute sur les feuilles d'une plante !
  - Fonctionnel avec une simple caméra 60i/s
    - Et Shannon-Nyquist !!?

    http://www.telegraph.co.uk/science/science-news/11016706/How-pot-plants-and-crisp-packets-could-be-spying-on-you.html
  - Les plus paranoïaques pensent que l'usage est d'écouter à partir des satellites

    https://www.youtube.com/watch?v=_tQEtmCjfhk



Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Le scam Nigérian toujours efficace

- Vol de plus de 2 millions d'euros sur 3 ans (2011->2014)
- En passant des commandes en ligne au nom d'une société bretonne
  http://www.01net.com/editorial/625308/deux-ivoiriens-arretes-apres-avoir-vole-2-4-millions-deuros-a-une-entreprise-francaise/

Piratages, Malwares, spam, fraudes et DDoS

DDoS

Sites de vente de “Stress Test”

Ticket & Live Support!

Great User Experience

24/7 Live Support

- En moyenne, 10min de DDoS = $5
- Possibilité de retrouver l’adresse réelle d’un serveur derrière CDN
  http://www.undernews.fr/hacking-hacktivisme/quand-des-services-ddos-se-camouflent-en-stress-test-en-ligne-legitimes.html
- Toujours accessible :
  http://ragebooter.net/

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

PayPal

- Possibilité de changer le montant facturé, après validation par l'acheteur
  - Ce n'est pas un bug, c'est une fonctionnalité
  - <<this is 'intended behaviour' due to small changes in shipping costs and such.>>

http://seclists.org/bugtraq/2014/Jul/85

XSS chez La Poste

http://www.zataz.com/la-poste-corrige-plusieurs-failles-serieuses/

Supervalu

- Comme pour Target : Point-of-Sale (PoS) ciblés par un malware de type “Ram Scraper”

http://nakedsecurity.sophos.com/2014/08/19/supervalu-says-it-was-breached-is-it-the-next-target/

Java.com (et autres) diffuse des malware via leurs régies publicitaires

- Distribution d’un exploit kit via une des régies publicitaires
- On se connecte sur Java.com pour mettre à jour Java et on reçoit un exploit kit :)

http://blog.fox-it.com/2014/08/27/malvertising-not-all-java-from-java-com-is-legitimate/

Piratages, Malwares, spam, fraudes et DDoS

Phishing

www.voyages-tgvs.com

- Réduction de 50% sur le tarif de la carte pour appâter le chaland
  http://www.zataz.com/piege-efficace-aux-couleurs-de-la-sncf/

Crypto
TrueCrypt-like

TrueCryptNext change de nom

- Et devient CipherShed
- Relève sérieuse mais reste le problème de licence TrueCrypt

  https://twitter.com/TrueCryptNext
- Dernière minute :
  - <<CipherShed has complied with the original TrueCrypt license. Now completing security review for alpha release to ensure safety of your data>>
    https://twitter.com/TrueCryptNext/status/508963734136836096

Crypto
TrueCrypt-like

TOR allié et ennemie de la NSA et du GCHQ

- Ces agences utilisent TOR, ils doivent veiller à ce qu'il reste solide
- Les "méchants" utilisent TOR, ces agences doivent donc casser TOR
  - Cruelle dilemme

http://www.bbc.com/news/technology-28886465

- Inutile de casser TOR pour briser l'anonymat
  - Tracker communs (Google et autre)
  - Tracker publicitaire de la NSA
  - Injection de backdoor par l'exploitation de faille de navigateur en « faussant » le site web visité (par le biais de leurs programmes QUANTUM et FOXACID)
  - Injection de javascript / iframe et exploitation de faille du navigateur Firefox fourni avec Tor Bundle
  - Attaques classiques sur les nœuds de sortie (sslstrip, vrais faux certificats…)
  - Faille qui devait être présentée à la BlackHat USA 2014
    - Faille corrigée suite à l'ajout de 116 noeuds malveillants ?

https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack

  - Forcer l'utilisateur à passer par un noeud contrôlé par l'attaquant

http://www.nrl.navy.mil/itd/chacs/sites/edit-www.nrl.navy.mil.itd.chacs/files/pdfs/13-1231-3743.pdf

- Bill Blunden, chercheur indépendant en sécurité et participant à Cryptome

A la question : Doit-on faire confiance à Tor ?
Il répond : Pas si votre vie est en jeu
http://cryptome.org/2014/07/trusting-tor-not.pdf

Crypto
Divers

Corrections de bug de BoringSSL commence à apparaître dans LibReSSL

http://freshbsd.org/search?project=openbsd&q=BoringSSL
https://boringssl.googlesource.com/boringssl/

TLS "fonctionnel" en OCaml !!?

http://openmirage.org/blog/introducing-ocaml-tls

- Site de démo avec possibilité de visualiser, en détails, chaque étape de la négociation

  https://tls.openmirage.org

- Qualys SSL Server Test : note entre A- et B
  - Tout à fait respectable pour une réécriture complète et une démo

  https://www.ssllabs.com/ssltest/analyze.html?d=tls.openmirage.org&hideResults=on
  https://www.ssllabs.com/ssltest/analyze.html?d=tls.openmirage.org&s=23.253.164.126&hideResults=on

Crypto JS fail ?

- Pas totalement :
  - à condition de respecter les bonnes pratiques
  - et si l'attaquant n'est pas trop fort

http://blog.kotowicz.net/2014/07/js-crypto-goto-fail.html

Snowden a-t-il aidé des terroristes par ses révélations ?

- Non 
- Mais ceux-ci ont développé de nouveaux outils
  - Basé sur les algorithmes de chiffrement standards (Se réinventer en crypto = échec)
  - Avec des implémentations maison ?

https://www.recordedfuture.com/al-qaeda-encryption-technology-part-1/
https://www.recordedfuture.com/al-qaeda-encryption-technology-part-2/

- L'utilisation de ces outils fait de vous une cible
  - Bruce Schneier : <<There's nothing that screams "hack me" more than using specially designed al Qaeda encryption software. There's probably a QUANTUMINSERT attack and FOXACID exploit already set on automatic fire.>>

https://www.schneier.com/blog/archives/2014/08/the_security_of_9.html

Scada
Divers

Attaque massive dans les secteurs du pétrole et de l'énergie en Norvège

- Près de 50 sociétés liées à ce domaine piratées, dont Statoil, la plus grande compagnie pétrolière du pays.
- Encore une fois, une pièce-jointe malveillante serait à l'origine de ces attaques

http://nakedsecurity.sophos.com/2014/08/28/massive-cyber-attack-on-oil-and-energy-industry-in-norway/?utm_content=buffer9ac15&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

Vulnérabilités dans le produit CG automation ePAQ-9410 Substation Gateway

- Problème de validation des données via le protocole DNP3
- Encore une fois, une pièce-jointe malveillante serait à l'origine de ces attaques

https://ics-cert.us-cert.gov/advisories/ICSA-14-238-01

Mise à jour des outils de reconnaissance de DigitalBond

- Script Nmap permettant de détecter certains périphériques SCADA

https://github.com/digitalbond/Redpoint

Un projet Kickstarter pour une plate-forme de démonstration Scada

https://www.kickstarter.com/projects/85810353/cybatiworks-ics-scada-iot-cybersecurity-education

Scada
Divers

Déni de service pour les Siemens S7-1500

- Découvert par l'ANSSI 
  https://ics-cert.us-cert.gov/advisories/ICSA-14-226-01

Le NIST, l'institut américain en charge des normes et de la technologie, souhaite construire un banc d'essai pour auditer les systèmes industriels SCADA

- Objectif d'évaluer les performances des ICS équipés de protection pour la cybersécurité
  http://www.theregister.co.uk/2014/08/12/nist_wants_better_scada_security/
  https://www.fbo.gov/index?s=opportunity&mode=form&id=34058f1c96ba5cab935633acc50011c9&tab=core&_cview=0

Nouveautés (logiciel, langage, protocole...)
Open Source

Kali Lunix 1.0.8

- Prise en charge du boot UEFI
- Boot sur partition Live USB chiffrée

http://www.kali.org/news/kali-1-0-8-released-uefi-boot-support/

x64_dbg 2.0 alpha

- Debugger Open Source pour Windows 32bits et 64bits

http://x64dbg.com/

OpenWrt BarrierBreaker 14.07-rc2

https://openwrt.org/

L'ANSSI publie son outil d'analyse Active Directory

- Qui a testé ??

https://github.com/ANSSI-FR/AD-control-paths

L'ANSSI publie un guide de sécurisaton Active Directory

- Sa lecture est vivement conseillée

http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/recommandations-de-securite-relatives-a-active-directory.html

Nouveautés (logiciel, langage, protocole...)

Open Source

NetFlix publie ses outils d'e-Réputation contre le DDoS

- **Scumblr**, scan des forums et réseaux sociaux pour trouver des sujets en rapport avec le DDoS
  https://github.com/netflix/scumblr
- **Workflowable**, générateur de workflow associés aux résultats des recherches de Scumblr
  https://github.com/netflix/workflowable
- **Sketchy**, capture de texte ou d'écran des résultats de Scumblr
  https://github.com/netflix/sketchy

http://techblog.netflix.com/2014/08/announcing-scumblr-and-sketchy-search.html

Nouveautés (logiciel, langage, protocole...)

Divers

IDAPython 1.7.0

- Support d'IDA Pro 6.6
  https://code.google.com/p/idapython/

IDA : Module pour CPU Qualcomm Hexagon (QDSP6)

- Utilisé dans les baseband iPhone, Samsung...
  https://github.com/gsmk/hexagon
- La chasse aux backdoors est ouverte !

Hopper 3.3.8

- Désassembleur, décompileur et debuggeur
  http://www.hopperapp.com/

BinWalk 2.0

- Analyse et ingénierie inverse de firmware
  http://www.devttys0.com/2014/07/binwalk-v2-0-released/

Nouveautés (logiciel, langage, protocole...)

Divers

LiveDump.exe

- Dump de la mémoire physique, sans privilège spécifique, avec Windows 8 (NtSystemDebugControl)
  http://crashdmp.wordpress.com/2014/08/01/introducing-livedump-exe/
  http://crashdmp.wordpress.com/2014/08/01/windows-8-1-update-live-dump-capability/

Contourner l'analyse dynamique des antivirus

- L'accent est mis sur le contournement des sandboxes et autres systèmes d'émulation proposés par les antivirus
  http://packetstorm.foofus.com/papers/virus/BypassAVDynamics.pdf

Exfiltration de données via canal sonore

- Via ultrasons ou vibration du smartphone
- Le code est disponible!
  https://bitbucket.org/ladeshot/ultrasonicfsk.git
  https://www.usenix.org/system/files/conference/woot14/woot14-deshotels.pdf

Nouveautés (logiciel, langage, protocole...)

Divers

EMET 5.0

http://blogs.technet.com/b/srd/archive/2014/07/31/announcing-emet-v5.aspx

- Permet la désactivation de certains plugins dans Internet Explorer
- A voir si Bromium Labs réussira à outre passer cette nouvelle version
  http://bromiumlabs.files.wordpress.com/2014/02/bypassing-emet-4-1.pdf

The Car hacker's handbook

- En vente sur Amazon, mais disponible gratuitement en ligne
  http://opengarages.org/handbook/

Nouveautés (logiciel, langage, protocole...)
Divers

Scanner d'aéroport ou lieux publique Qylatron de Qylur Security Systems

- Testé avec succès lors de la coupe du monde de foot au Brésil
  http://www.latribune.fr/technos-medias/innovation-et-start-up/20140716trib000840225/l-invention-qui-va-revolutionner-les-controles-a-l-aeroport.html
- Ne se repose plus sur la vision des agents mais sur une base de données d'objets interdits
  - Gain de temps
  - Évite des fouilles corporelles, sauf en cas de détection
  - *(Chomage?)*

  http://www.qylur.com/public/products

- Design des années 80 ? *(Série V)*

Business

France

NFC, le stock d'étuis anti-NFC des banques / Plan anti-crise NFC

- Stock d'étui "cage de faraday" en cas de panique
- Beaucoup de bruit pour pas grand chose, soyons tolérants

http://www.01net.com/editorial/621956/piratage-des-cartes-nfc-le-plan-de-crise-secret-des-banques-francaises/

Panne SFR, l'ANSSI ouvre une enquête

http://www.linformaticien.com/actualites/id/33727/panne-sfr-l-anssi-ouvre-une-enquete.aspx

Business
International

Juniper vend sa filiale Junos Pulse

- Au fond Siris Capital
- http://siriscapital.com/pressreleases/Siris_Pulse_acquisition_July_2014.pdf
- Raison invoquée par le CEO de Juniper :
  - "pulse is a good asset. The issue is that it's not in line with our strategy which is very much focused on cloud and high IQ networks and how those markets are shaping"
- Transfert d'une partie du personnel Juniper chez Siris (avant vente, support et dev).
- "Des engagements existent pour que Siris continue le développement et le support du VPN SSL sur le long terme"

IBM acquière Lighthouse Security Group

- Spécialiste du SSO dans le cloud
  http://www-935.ibm.com/services/us/en/it-services/security-services/cloud-identity-service/announcement/

La NSA, la DEA, la CIA... dans le Cloud

- Les 17 agences du renseignement américain (CIA, NSA, DEA…) sur le Cloud Amazon (AWS)
  - Région (regroupement de datacenters) dédiée aux organisations gouvernementales US
  - Le CISO d'AWS est un ancien de la NSA.

  http://www.01net.com/editorial/624090/amazon-au-service-de-la-cia-et-de-la-nsa/

Business
International

8,5% des comptes twitter sont des bots

- Ou plutôt, sont des utilisateurs passant par des applications tierces
  - et ne visualisant donc pas les pub

http://www.01net.com/editorial/625022/23-millions-de-twittos-actifs-sont-des-robots/

Microsoft et Google sont du même avis : le Cloud améliore la sécurité

- Microsoft : surtout face à la contrefaçon
  http://www.lepoint.fr/chroniqueurs-du-point/guerric-poncet/microsoft-le-piratage-a-considerablement-baisse-21-08-2014-1855431_506.php
- Google : surtout face à l'intrusion
  http://www.businessinsider.com/google-explains-the-cloud-in-three-words-2014-8

TwitPic fermera le 25 sept. 2014

- Après le pattent troll, voici le trademark troll
  http://blog.twitpic.com/2014/09/twitpic-is-shutting-down/

Droit / Politique

France

Quand l'administratif à la française transpose la directive européenne AIFM (Alternative Investment Fund Managers)

- Et impose des mesures excessives
  - certification AMF des gérants sinon 3 ans de prison et 375Ke d'amende,
  - 125Ke placés en prudentiel
  - ...

http://acteursdeleconomie.latribune.fr/debats/opinion/2014-07-09/la-french-tech-mise-en-danger-par-une-directive-europeenne.html

Droit / Politique
International

1er rapport officiel sur les activités de la NSA

- Quelques chiffres, principalement sur les demandes FISA
  http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2013

Un juge Brésilien demande la suppression d'une application à distance

- Sur smartphone iOS, Android et Windows Phone
  http://9to5mac.com/2014/08/19/brazillian-judge-orders-apple-to-remove-secret-from-the-app-store-remotely-delete-from-users-phones/

Le piratage citoyen en Inde

- L'inde "recruterait" des jeunes
  - Suite à l'explosion d'un pipeline de gaz du fait d'un vers et de tentatives de sabotage de centrales électriques

  http://www.openthemagazine.com/article/nation/the-nation-wants-the-smart-hacker

Conférences

Passées

- BlackHat du 2 au 7 août 2014
- DefCON du 7 au 10 août 2014

A venir

- BlackHat Europe - 16/17 octobre 2014
- HACK.LU - 21 au 24 octobre 2014
- ASFWS - 4 au 6 novembre 2014 en Suissecf. revue d'actualité de juillet 2014
- No Such Con - 19 au 21 novembre 2014 à Paris
- Bot Conf - 3 au 5 Décembre 2014 à Nancy
- JSSI 2015 - 10 mars 2015 à Paris
  - Organisée par l'OSSIR
- GS Days - 24 mars 2015 à Paris

Divers / Trolls velus

Le "Projet Zero" de Google

- Une équipe de pentesteurs d'élite pour auditer toutes les applications du monde
  - Car la sécurité des utilisateurs des services Google ne dépend pas uniquement de Google
  - Avec :
    - Tavis Ormandy, Ben Hawkes, George Hotz, Chris Evans...

  http://www.wired.com/2014/07/google-project-zero/
- Force est de constater que ça ne chôme pas chez Google !

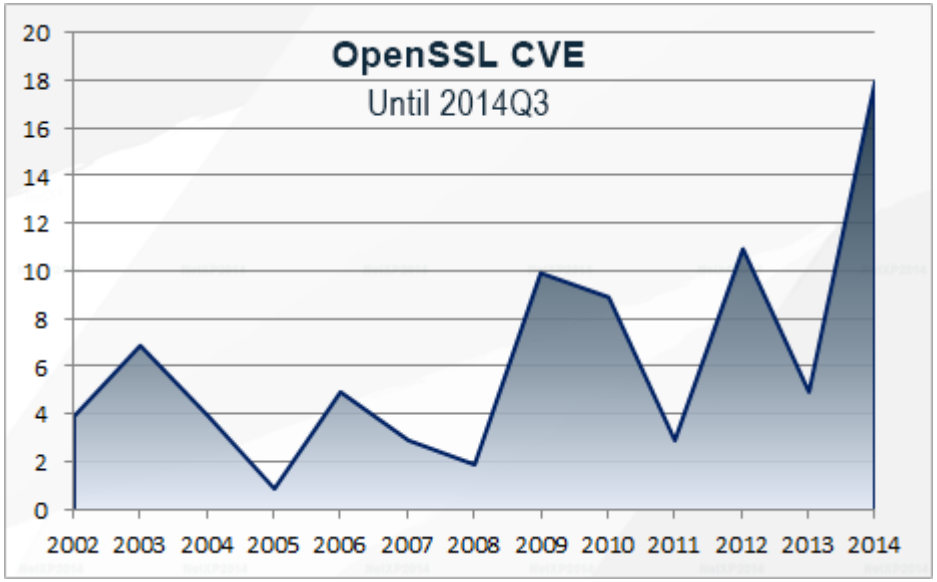
  https://www.google.com/about/appsecurity/research/
- Quelques failles expliquées
  - Dont certaines trouvées par audit du code

  http://googleprojectzero.blogspot.ca/2014/07/mac-os-x-and-iphone-sandbox-escapes.html

Divers / Trolls velus

HeartBleed a eu du bon !

- Failles OpenSSL depuis 2002 jusqu'à août 2014
  https://www.openssl.org/news/secadv_20140806.txt



Divers / Trolls velus

Quand LeBonCoin invente le recel à flux tendu

http://www.numerama.com/magazine/30087-quand-leboncoin-permet-aux-voleurs-de-faire-du-flux-tendu.html

Certificats Google et Microsoft signés par une AC publique indienne

- Usage des certificats générés non déterminé pour l'instant
  - Mais les AC ont déjà été révoquées
  - Tout comme pour l'ANSSI (cf. Revue Décembre 2013),

http://timesofindia.indiatimes.com/tech/tech-news/Government-probing-unauthorised-digital-certificates-issue/articleshow/38372978.cms

Divers / Trolls velus

BlackBerry troll l'insécurité d'Android

- Peut-être faudrait-il leur rappeler la parabole biblique de la paille et de la poutre...
  http://www.lemondeinformatique.fr/actualites/lire-blackberry-s-acharne-sur-les-lacunes-de-securite-d-android-58023.html

BlackBerry troll également BlackPhone

http://pro.clubic.com/entreprises/rim/actualite-715341-blackberry-blackphone-place-entreprise.html

- Blackphone répond
  https://medium.com/@Blackphone/blackphone-privacy-people-want-to-buy-308c9694d910

Les utilisateurs Pro veulent le retour de BlackBerry

http://www.lemondeinformatique.fr/actualites/lire-des-utilisateurs-pro-reclament-le-retour-des-blackberry-58139.html

Divers / Trolls velus

OpenOffice n’imprime pas le Mardi (date de 2009)

- Tue = magics bytes d’un fichier “Erlang JAM”
  https://bugs.launchpad.net/ubuntu/+source/cupsys/+bug/255161/comments/28

Pokémon ou BigData ?

https://docs.google.com/forms/d/1kckcq_uv8dk9-W5rIdtqRwCHN4Uh209ELPUjTEZJDxc/viewform

Le Faraday Café à Vancouver

- Dans une cage de Faraday
  http://www.wired.co.uk/news/archive/2014-07/15/faraday

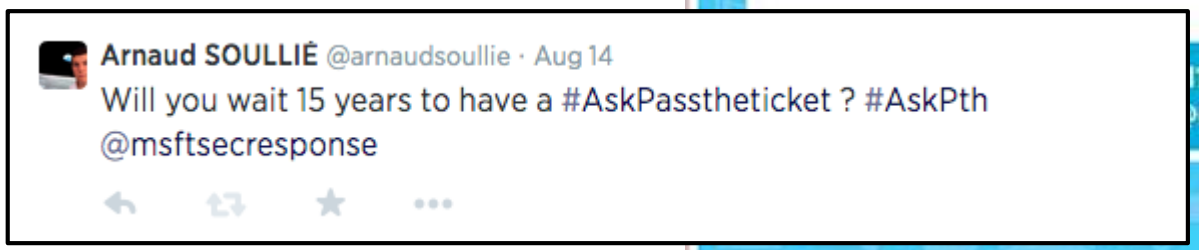
Retrouver la nationalité d'une personne écrivant en anglais

http://www.csail.mit.edu/node/2283

Divers / Trolls velus

Gagnez une XBox One avec Pass-The-Hash !!?

https://twitter.com/msftsecurity/status/500772994953003009



Divers / Trolls velus

NSA et Cie

Le FBI a peur des voitures autonomes

- Risques d'attentats, de criminels tirant sur la police sans conduire...

  http://www.theguardian.com/technology/2014/jul/16/google-fbi-driverless-cars-leathal-weapons-autonomous

La CIA a peur des objets connectés / Internet of Things (IoT)

- Table ronde avec Dawn Meyerriecks, directeur adjoint Acquisition et Technologie de la CIA
  - La faible sécurité des IoT implique des risques de SPAM, DDoS
  - 7'10 : <<from system engineering complexities perspective, we are the best in the world>> ;-)

  https://www.youtube.com/watch?v=3e-pMgmb4wk

Divers / Trolls velus

NSA et Cie

La NSA et le GCHQ sont des pirates

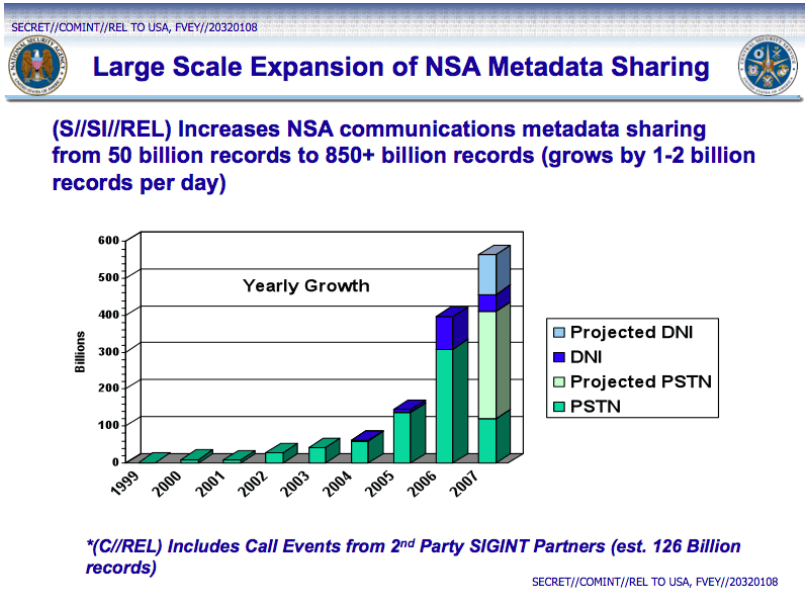
- Ils font du scan de ports !!!
  http://www.heise.de/ct/artikel/NSA-GCHQ-The-HACIENDA-Program-for-Internet-Colonization-2292681.html

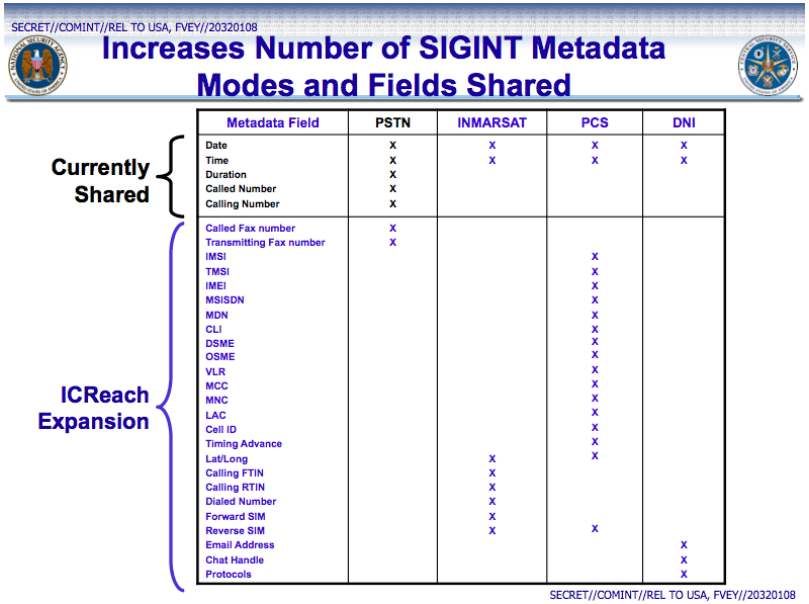
ICReach de la NSA, le moteur d'indexation des communications

- Indexe 850 milliards de données *(entre 30 et 50 trillions de pages pour Google)*
  - Dont 2 à 5 milliards nouvelles données chaque jour

https://firstlook.org/theintercept/article/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/

- Les Slides:
  https://www.eff.org/files/2014/08/25/sharing-communications-metadata-across-the-u-s.pdf

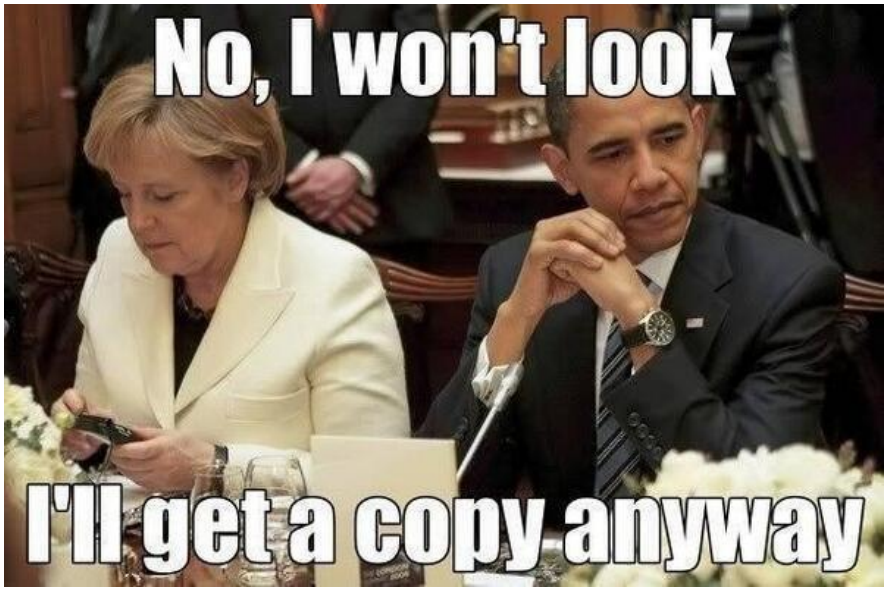




Divers / Trolls velus

Mieux vaut en rire…

https://twitter.com/noruweijin/status/487790977994985473/photo/1



Obama est un individu comme les autres

- Qui fait fuiter son numéro de carte bancaire

https://twitter.com/ihackedwhat/status/488847983882948609

Divers / Trolls velus

La NSA récolte, avant tout, des données de vie privée des gens ordinaires

- Snowden a fourni un échantillon des données collectées par la NSA
  - Grande majorité : Données normales échangées entre utilisateurs normaux
  - Echanges d'amour, banals, de tous les jours… photos d'enfant, de famille, de fesses…

  http://www.01net.com/editorial/623332/la-nsa-recolte-avant-tout-des-donnees-de-vie-privee-de-gens-ordinaires/
- La NSA a embauché beaucoup des jeunes hommes de 18 à 22 ans
  - Avec un haut niveau de confidentialité / confiance
  - Des accès à toutes les données collectées par la NSA et leurs outils
- Naturellement, ils sont tombés « par hasard » sur des photos de jeunes filles dénudées
  - Ont approfondit les dossiers
  - Puis ont échangé entre eux les photos / noms / données personnelles…

  http://www.theguardian.com/world/video/2014/jul/17/edward-snowden-video-interview

Divers / Trolls velus

FireEye, Sogeti et Full Disclosure “sauvage” sont dans un bateau...

- Un auditeur d’ESEC Sogeti (sous NDA tacite par contrat) audite des appliances FireEye en boite noire, sur du temps personnel
  - 7 juillet, publication des failles trouvées sur Exploit DB (XSS, CSRF, SQLi)
    - Sans avertir Sogeti
    - Sans avertir FireEye
  - Quelques heures après, retrait de la page, suite à une demande de FireEye
    https://twitter.com/kmkz_security/status/486509374165508096
  - « mirroring » sur PasteBin par un anonyme http://pastebin.com/PWvU62tG
  - 8 juillet, mise à pied de l’auditeur pour ne pas avoir respecter le processus de divulgation des failles
- Pendant ce temps-là, FireEye lançait un challenge public de sécurité

  http://www.fireeye.com/blog/technical/malware-research/2014/07/announcing-the-flare-team-and-the-flare-on-challenge.html

Divers / Trolls velus

Cloud : on vous avait prévenu...

- Vol de centaines de photos de célébrités hollywoodiennes
  - A partir d'iCloud et Dropbox
  - Phishing + Ingénierie sociale sur plusieurs mois, voire années
    - La collection de photos privées de stars existe depuis les débuts du cinéma (Volées par des assistants, gardes du corps…)

http://www.latimes.com/local/lanow/la-me-ln-celebrity-nude-photos-accessed-by-phishing-source-says-20140902-story.html

- Un gros malin aurait acheté des photos et tenté de les revendre
  - Mais il publie une capture d'écran avec son voisinage réseau !!?
  - Et est identifié en quelques heures

http://tempsreel.nouvelobs.com/vu-sur-le-web/20140903.OBS8016/photos-de-stars-nues-comment-la-traque-s-organise-au-fin-fond-du-web.html

- Des théories sur la diffusion

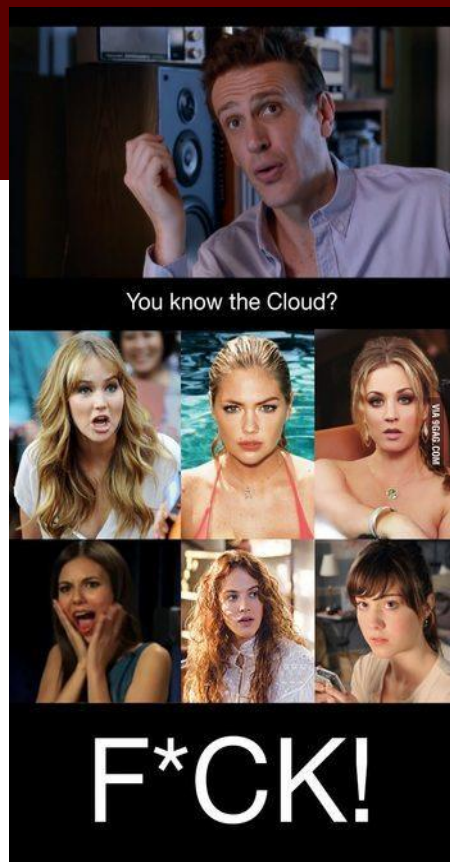
https://twitter.com/jerometomasini/timelines/506785550825975808

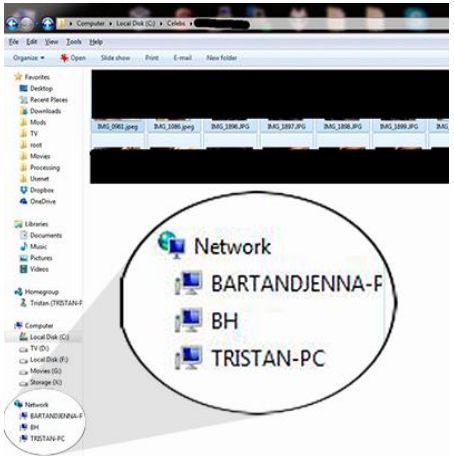
- Même une journaliste arrive à "pirater" iCloud

http://mashable.com/2014/09/04/i-hacked-my-own-icloud-account/

- Prises de conscience générale
  - des risques du Cloud ?
  - de l'existence d'internautes malveillants ?

"Always free, fast and discreet. Will make it alot easier if you have the password," writes one hacker with the email address eppbripper@hush.ai. "Willing to rip anything iclouds – gf/bf/mom/sister/classmate/etc!! Pics, texts, notes etc!"
http://www.wired.com/2014/09/eppb-icloud





Divers / Trolls velus

Pour le vivre chaque mois avec cette revue 
https://twitter.com/veorq/status/489496314917687296

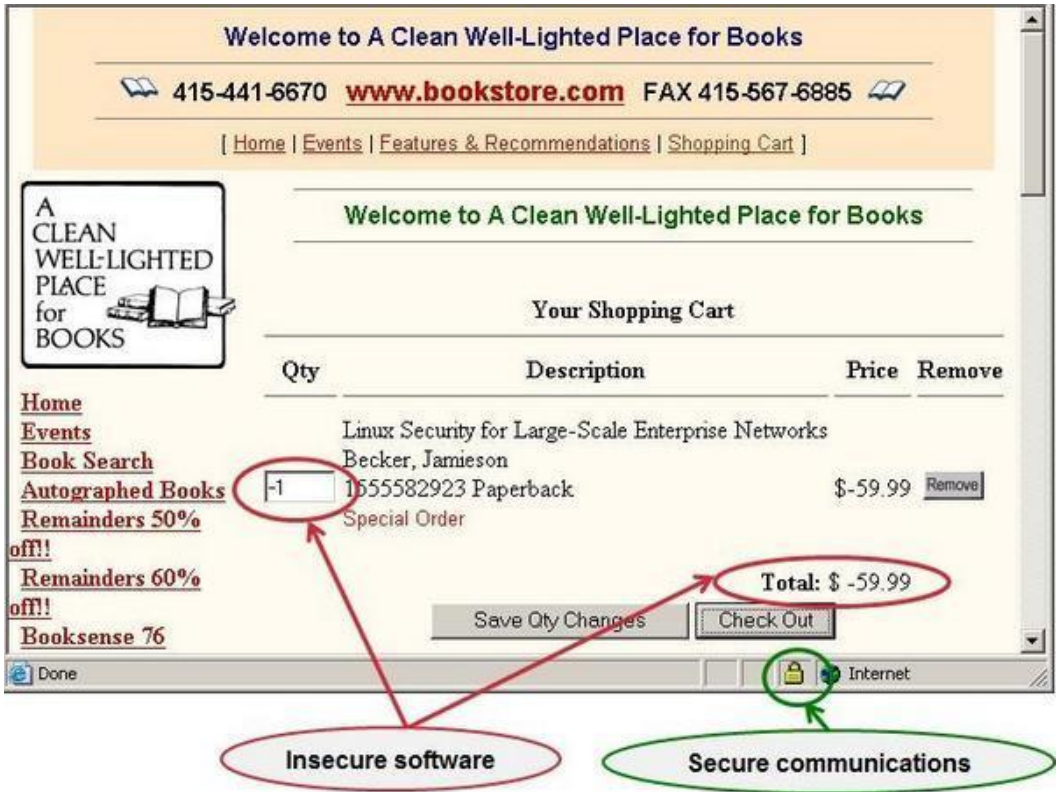
JP Aumasson @veorq · 17h

Google is doing driving cars and project zero and amazing things, but can't properly convert Google Slides to PPTX

2 2

La sécurité des applications web

- En une seule image
  https://twitter.com/binitamshah/status/493703072728621056



Divers / Trolls velus

Les AWACS de la France passent sous Windows 7

http://www.4erevolution.com/awacs-windows/

SIRROCO est encore sous Windows XP

- Tout du moins pour l'affichage
  http://microfail.blogspot.fr/2014/09/air-france-fail.html

Prochaines réunions

Prochaines réunions

- Mardi 14 octobre 2014

Afterwork

- Mardi 23 septembre
  - Réservé aux membres, ayant le droit d’inviter un non-membre

Questions ?