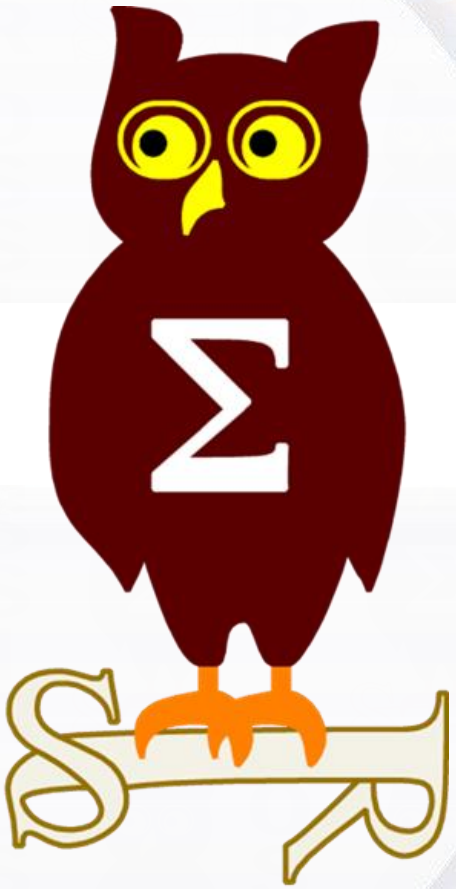


Revue d'actualité

07/07/2015

Préparée par

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

Failles / Bulletins / Advisories

Microsoft - Avis Juin 2015

MS15-056 Vulnérabilités dans Internet Explorer (24 CVE)  [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportées)
  - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
  - Remplace MS15-043
- Exploit:
  - 20 x Corruptions de mémoire aboutissant à une exécution de code
  - 1 x Accès à l'historique de navigation
  - 3 x Élévation de privilèges (exécution de code avec privilèges élevés)
- Crédits:
  - 0016EECD9D7159A949DAD3BC17E0A939 par ZDI(CVE-2015-1755)
  - Anonymous avec Beyond Security et Ashutosh Mehra par ZDI(Defense-in-depth)
  - Anonymous par ZDI(CVE-2015-1736)
  - Bo Qu de Palo Alto Networks (CVE-2015-1736, CVE-2015-1744, CVE-2015-1750)
  - Chen Zhang (demi6od) de NSFOCUS Security Team (CVE-2015-1740, CVE-2015-1741, CVE-2015-1742)
  - Dhanesh Kizhakkinan de FireEye, Inc. (CVE-2015-1737)
  - Exploitsky (CVE-2015-1752)
  - Haifei Li de McAfee Labs IPS Team (CVE-2015-1743)
  - Heige (a.k.a. SuperHei) de Knownsec 404 Security Team (CVE-2015-1740)
  - Jack Tang de Trend Micro (CVE-2015-1754)
  - Jason Kratzer working avec VeriSign iDefense Labs (CVE-2015-1751)
  - Jihui Lu de KeenTeam (@K33nTeam) (CVE-2015-1753)
  - Qihoo 360 et Vulcan 360 Team
    - Linan Hao (CVE-2015-1732)
    - Pengfei Guo (CVE-2015-1687)
    - Yuki Chen (CVE-2015-1745, CVE-2015-1743)
  - lokihardt@ASRT par ZDI (CVE-2015-1747, CVE-2015-1748)
  - National Engineering Laboratory for Mobile Internet System and Application Security, China (CVE-2015-1744)
  - SkyLined avec VeriSign iDefense Labs (CVE-2015-1730)
  - Thomas Vanhoutte par ZDI(CVE-2015-1739)
  - Zheng Huang de Baidu Scloud XTeam (CVE-2015-1731, CVE-2015-1735)

Failles / Bulletins / Advisories

Microsoft - Avis Juin 2015

MS15-057 Vulnérabilité dans Windows Media Player (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows Media Player 10, 11 et 12 (Windows 2003, 7, 8, 2008 et R2)
  - Remplace MS10-082
- Exploit:
  - Évasion de la sandbox IE et exécution de code à l'ouverture d'un fichier audio/vidéo spécialement formaté
    http://answers.microsoft.com/en-us/windows/forum/windows_7-performance/is-anything-wrong-with-this-process/c0645cc7-b6e0-45f4-a336-4e4cd117dbf5?auth=1
- Crédits:
  - bilou avec VeriSign iDefense Labs (CVE-2015-1728)

MS15-058 Vulnérabilité dans Office (3 CVE) [Exploitabilité 1]

- Affecte:
  - Correctif non publié !
- Exploit:
  - Exécution de code à l'ouverture d'un fichier Office spécialement formaté
- Crédits:
  - ?

Failles / Bulletins / Advisories

Microsoft - Avis Juin 2015

MS15-059 Vulnérabilité dans Office (3 CVE) [Exploitabilité 1]

- Affecte:
  - Microsoft Office 2007, 2010, 2013 et RT
  - Remplace MS13-091
- Exploit:
  - Exécution de code à l'ouverture d'un fichier WordPerfect (.doc) spécialement formaté
    https://code.google.com/p/google-security-research/issues/detail?id=317
    https://code.google.com/p/google-security-research/issues/detail?id=315
- Crédits:
  - Ben Hawkes de Google Project Zero (CVE-2015-1759, CVE-2015-1760)
  - Yong Chuan Koh (@yongchuank) MWR Labs (@mwrlabs) (CVE-2015-1770)

MS15-060 Vulnérabilité dans Microsoft Common Controls (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportées)
  - Remplace MS15-043
- Exploit:
  - Corruption de mémoire aboutissant à une exécution de code à l'accès à un Common Control non initialisé ou effacé
  - Contrôles utilisés par le menu de développeur d'IE et peut-être exploité par ce biais depuis une page web
- Crédits:
  - ?

Failles / Bulletins / Advisories

Microsoft - Avis Juin 2015

MS15-061 Vulnérabilité noyau Win32k.sys (5 CVE) [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportées)
  - Remplace MS15-023
- Exploit:
  - 10 x Élévations de privilèges
    - cf. "Espionnage" avec Duqu 2.0
  - 1 x fuite d'information du noyau permettant de lire n'importe quelle zone mémoire
- Crédits:
  - enSilo Research Team (CVE-2015-2360)
  - Guo Pengfei de Qihoo 360 (CVE-2015-1719)
  - Nils Sommer x 7 de Google Project Zero (CVE-2015-1721, CVE-2015-1722, CVE-2015-1723, CVE-2015-1724, CVE-2015-1725, CVE-2015-1726, CVE-2015-1727)
  - KK de Tencent's Xuanwu LAB (CVE-2015-1720)
  - Maxim Golovkin, Kaspersky Lab (CVE-2015-2360)

MS15-062 Vulnérabilité Active Directory (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows Server 2008, R2, 2012
- Exploit:
  - XSS avec ADFS

    /adfs/ls/?wa=wsignin1.0&wtrealm=https://victime.com/RefinishUserAdmin/&wctx=rm=0&id=passive&ru=%2fRefinishUserAdmin%2f%3fwhr%3dhttp%3a%2f%2fsso.victime.com%2fadfs%2fservices%2ftrust&wct=2015-06-30T11:30:12Z78b0f<script>alert(“ossir”)</script>b032e&whr=http://sso.victime.com/adfs/services/trust
- Crédits:
  - John Hollenberger et Tate Hansen de FishNet Security (CVE-2015-1757)

Failles / Bulletins / Advisories

Microsoft - Avis Juin 2015

MS15-063 Vulnérabilité noyau (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportées)
  - Remplace MS14-019
- Exploit:
  - Élévation de privilèges depuis LoadLibrary (~DLL preloading)
- Crédits:
  - Takashi Yoshikawa de Mitsui Bussan Secure Directions, Inc. (CVE-2015-1758)

MS15-064 Vulnérabilité dans Exchange Server (3 CVE) [Exploitabilité 2]

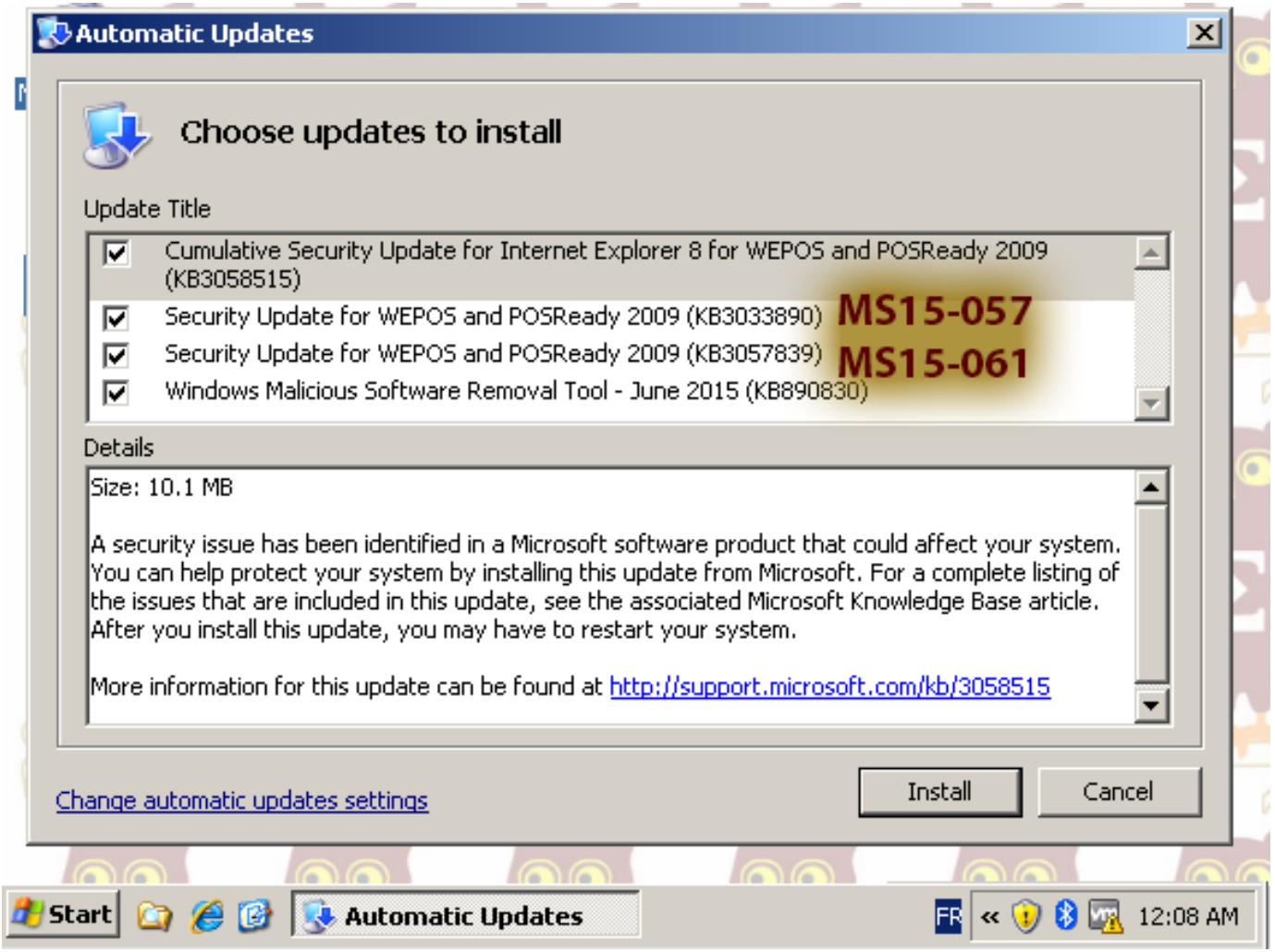
- Affecte:
  - Microsoft Exchange Server 2013 SP1 et Cumulative Update 8
- Exploit:
  - 2 x fuites d'information dans OWA et contournement du "Same Origin Policy" (Server-Side Request Forgery et CSRF)
  - 1 x élévation de privilèges dans OWA (injection d'une page HTML)
- Crédits:
  - ?

Failles / Bulletins / Advisories

Microsoft - Avis Juin 2015

Mise à jour pour Windows XP Embedded POSReady

- Encore et toujours sans documenter dans les bulletins…



Failles / Bulletins / Advisories

Microsoft - Advisories et Revisions Juin 2015

2962393 Mise à jour du client Juniper Pulse (VPN SSL)

- V2.0 Ajout d'un correctif Juniper (déni de service sur OpenSSL)

2755801 Mise à jour de Flash Player

- V41.0 Nouvelle mise à jour de Flash Player (Bulletin adobe APSB15-09)
- V42.0 Nouvelle mise à jour de Flash Player

Adobe Type Manager Font Driver (ATMFD.DLL), multiples vulnérabilité par j00ru

- Reverse de la DLL utilisé de Win NT 4 à Win 8
  - Le code est supposé très mauvais
  - Beaucoup d'options non document des formats PostScript

  http://j00ru.vexillium.org/?p=2520

Ajout de 17 CA root dans Windows

- Pas de bulletin, pas de KB, pas d'advisories

  http://hexatomium.github.io/2015/06/26/ms-very-quietly-adds-18-new-trusted-root-certs/

Failles / Bulletins / Advisories

Microsoft - Autre

Microsoft ouvre son code source... aux agences gouvernementales européennes

- Ouverture de son « Transparency Center » à Bruxelles
  https://blogs.microsoft.com/eupolicy/2015/06/03/microsoft-transparency-center-opens-in-brussels/

Windows 10 et la vie privée

- Collecte comme tout le monde, mais pris la main dans le sac
  - Synchro des données dans le Cloud Microsoft
    - Comme Firefox , Google Android, Apple iOS, Google Chrome...
  - Collecte des informations comme les BSSID
    - Comme Android et iOS
  - Identifiant publicitaire
    - Comme sur iOS
  - Chiffrement et sauvegarde de la clef dans le cloud
  - ...

  http://www.undernews.fr/libertes-neutralite/windows-10-vs-vie-privee-des-points-problematiques.html

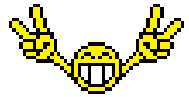
Windows 10 - Partage de clé Wifi avec les amis

- Fonctionnalité “Wi-Fi Sense” déjà présente sur les Windows phones
- Partage vos clés WiFi avec les contacts Outlook, Skype, Facebook (opt-in)
- Sensé ne donner accès qu’à Internet, pas au LAN
  http://www.windowsphone.com/en-us/how-to/wp8/connectivity/use-wi-fi-sense-to-get-connected

Failles / Bulletins / Advisories

Système (principales failles)

VMWare Workstation, Player, Horizon

- Évasion d'une machine virtuelle grâce au port COM1 (CVE-2015-2336)
- Par Kostya Kortchinsky 
  - Pas de site 
  - Pas de nom 
  - Pas de logo 
  - Un article + une vidéo de démonstration + un code d'exploitation => **La grande classe** 

  https://docs.google.com/document/d/1sIYgqrytPK-CFWfqDntraA_Fwi2Ov-YBgMtl5hdrYd4/edit?pli=1#heading=h.xj3viib4n5
- Pleins de vulnérabilités

  https://code.google.com/p/google-security-research/issues/list?can=1&q=vprintproxy

Adobe Flash Player

- Exécution de code (CVE-2015-3113)
- Exploité par les pirates chinois APT3 pour injecter le trojan ShotPut

  http://www.developpez.com/actu/86838/Adobe-publie-un-correctif-d-urgence-pour-une-faille-zero-day-dans-Flash-qui-serait-exploitee-par-des-pirates-chinois/
- 4 j. après la publication du correctif, inclusion de l'exploit dans des kits d'exploitation criminels

  http://malware.dontneedcoffee.com/2015/06/cve-2015-3113-flash-up-to-1800160-and.html

Failles / Bulletins / Advisories

Système (principales failles)

Antivirus ESET NOD32, Smart Security, Endpoint Security

- Par Tavis Ormandy
- Exécution de code à distance en tant que root/system depuis le filtre I/O
  - Exploitable depuis un navigateur, un mail...
  - Vulnérabilité donnée “de la main à la main”

  https://code.google.com/p/google-security-research/issues/detail?id=456&can=1&start=200
- Exécution de code

  https://code.google.com/p/google-security-research/issues/detail?id=466&can=1&start=200

Exécution de commande avec les utilisateurs unix standards

- Pas une vulnérabilité, mais néanmoins intéressant
- De nombreux utilitaires permettent d’exécuter du code : tar, tcpdump, zip, man
- Attention aux permissions !
  - `man -P /tmp/runme.sh man`
  - `tar c a.tar -I ./runme.sh a`

  http://0x90909090.blogspot.fr/2015/07/no-one-expect-command-execution.html

Sécurité des parseurs XSLT

- Comparaison des possibilités offerte par les parseurs les plus utilisés

  http://blog.csnc.ch/2015/06/xslt-security-and-server-side-request-forgery/

Failles / Bulletins / Advisories

Matériel

Piratage de la console Sony PS4

- Mis au point par des Russes ? Mais revendu au Brésil
- Consister à cloner une PS4 bourrer de jeux sur une seconde
  - Vendu 130 à 180 euros par des magasins brésiliens

    http://jogos.uol.com.br/ultimas-noticias/2015/05/12/por-precos-a-partir-de-r-300-pirataria-chega-ao-playstation-4-no-brasil.htm
- Sony a réagit avec des mises en demeure

  http://www.newsinside.org/playstation/sony-comeca-a-notificar-empresas-que-estao-vendendo-o-desbloqueio-do-playstation-4

L'USB3 interfère dans la bande des 2,4GHz

http://www.intel.com/content/www/us/en/io/universal-serial-bus/usb3-frequency-interference-paper.html

Attaque par canal cachée via SDR

http://www.wired.com/2015/06/radio-bug-can-steal-laptop-crypto-keys-fits-inside-pita

Failles / Bulletins / Advisories

Réseau (principales failles)

Routeur SOHO : TP-Link ADSL2+ et TD-W8950ND

- Changement des DNS à distance, sans authentification
  https://packetstormsecurity.com/files/132191/tplink-tdw8950nd.txt?utm_medium=twitter&utm_source=twitterfeed
- Exploit : http://IP-de-la-Cible/dnscfg.cgi?dnsPrimary=8.8.8.8&dnsDynamic=0&dnsRefresh=1

Switch Netgear ProSafe

- Portail web de management : Injections SQL, injections d'entêtes, XSS
  https://packetstormsecurity.com/files/132457/NETGEAR²-ProSafe-Cross-Site-Scripting-SQL-Injection-Header-Injection.html

Cisco WSAv, ESAv, SMAv ([Web | Email | Content] Security Virtual Appliance)

- Clefs SSH en dur sans ses appliances virtuelles

Failles / Bulletins / Advisories

Réseau (principales failles)

FireEye : Contournement avec une collision MD5

- Stockage des condensats / empreintes (hash) des fichiers et urls sains avec MD5
  - @JP, nous n'avons pas dit "sauvegarde en MD5"
- Il suffit s'envoyer un fichier sain, puis un code malveillant avec une collision MD5
  http://blog.silentsignal.eu/2015/06/10/poisonous-md5-wolves-among-the-sheep/

Sécurité des VPNs commerciaux (mode SaaS)

- Pas de sécurisation des flux IPv6, qui peuvent passer en dehors du tunnel
- Pas de sécurisation des requêtes DNS (modifiable par DHCP, injection de route)
  http://www.eecs.qmul.ac.uk/~hamed/papers/PETS2015VPN.pdf

SessionID faible sur l'interface web des switch Alcatel

- Sont vulnérables : OmniSwitch 6450,6250,6850E,9000E,6400,6855

  http://seclists.org/fulldisclosure/2015/Jun/22

Failles / Bulletins / Advisories

Apple

QuickTime

- Exécution de code à la lecture d'une vidéo .MOV
  http://blogs.cisco.com/security/talos/apple-stbl-atom

iPad : Contournement des restrictions logicielles

- Restrictions permettant notamment de désactiver Internet, etc
- Nécessite un code à 4 chiffres pour être déverrouillé
- La protection anti-bruteforce peut être contournée….
- ...En changeant l'heure :)
- Automatisable avec un RubberDucky et l'utilisation de fonctions d'accessibilité
  https://www.offensivebits.com/?p=33

Mac OS X

- Contournement des contrôles de l'Apple Store et envoie d'une application malveillante
- Récupération de données dont photos, contacts et trousseau de clefs
- Publication du fait de l'inaction d'Apple pendant 6 mois
  https://drive.google.com/file/d/0BxxXk1d3yyuZOFlsdkNMSGswSGs/view

Utilisation de librairies tierces dans iTunes et Quicktime pour Windows

- libcurl date d'il y a 9 ans

  http://seclists.org/fulldisclosure/2015/Jul/6

Failles / Bulletins / Advisories

Google

Spoofing de l'url d'un site

- Sans interaction de l'utilisateur
  - Et sans intérêt pour l'équipe des développeurs !!?

http://seclists.org/fulldisclosure/2015/Jun/108

Chrome Hotword : écoute vos conversations

- Installation silencieuse d'une extension de Chromium permettant l'interaction vocale (Ok Google)

http://thehackernews.com/2015/06/google-chrome-spying.html

Failles / Bulletins / Advisories

Crypto

OpenSSL

- Pas encore de détails, diffusion jeudi 9 juillet

  https://mta.openssl.org/pipermail/openssl-announce/2015-July/000037.html

Failles / Bulletins / Advisories

Divers

Vulnérabilité XXE dans SAP Netweaver Portal

http://erpscan.com/advisories/erpscan-15-004-sap-netweaver-portal-xmlvalidationcomponent-xxe/

LG va finalement corriger la vulnérabilité de non-vérification du certificat serveur

- Pas de vérification du certificat lors des mises à jour sur les modèles pré-Lollipop

  http://www.scmagazineuk.com/lg-pledges-to-fix-android-smart-phone-vulnerability/article/424375/

Vulnérabilité dans le clavier “Swiftkey” des ordiphones Samsung

- Mises à jour via HTTP
- Vérification d’une signature SHA-1 elle-même récupérée via HTTP

  https://nakedsecurity.sophos.com/2015/06/17/samsung-keyboard-app-could-let-a-crook-crack-your-phone/

Vulnérabilité dans le module OpenID de Drupal

- Versions 6 et 7 affectées
- Permet d’usurper l’identité d’administrateurs
- Limité à un attaquant disposant d’un compte OpenID Verisign, LiveJournal ou StackExchange, étrange

  https://www.drupal.org/SA-CORE-2015-002

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Java : Exécuter du code depuis les commentaires, c'est possible !!!

- Grâce à des caractères unicodes interprétés par le compilateur

  ```
  // \u000d System.out.println("Hello World!");
  ```

- Méfiez-vous des codes téléchargés et backdoorés en commentaire 

  http://stackoverflow.com/questions/30727515/why-is-executing-java-code-in-comments-with-certain-unicode-characters-allowed

Anti-cuckoo sandbox

- Détecter et plantage d'une VM Cuckoo Sandbox

  https://github.com/David-Reguera-Garcia-Dreg/anticuckoo

Application iOS malveillantes sur iPhone non-jailbreaké

- Création d'un compte Apple Developer Enterprise Program, à $299/ans
- Demandant pourtant des vérifications
- Demande de l'installation de l'application lors de navigation sur des sites pornos

  http://www.symantec.com/connect/blogs/japanese-one-click-fraudsters-target-ios-users-malicious-app-delivered-over-air

Les hackeurs gouvernementaux s'intéressent aux Antivirus

- Plus particulièrement à leurs failles

  https://firstlook.org/theintercept/2015/06/22/nsa-gchq-targeted-kaspersky/

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Faux portail Wifi captif usurpant Apple Pay

- Pour récupérer des n° de CB
- Attaque très basique affichant directement une page demandant les infos de CB

http://arstechnica.com/security/2015/06/evil-wifi-captive-portal-could-fool-users-into-giving-up-apple-pay-data/

87% des attaques contre la France viennent… de France

- D'une IP français mais l'attaquant ?

http://info.threatmetrix.com/rs/threatmetrix/images/TM_CyberCrimeReport_Q1_2015_May2015.pdf

Obfuscation d'url

IP en décimal : http://7763631671/obscure.htm
IP en octal : http://0316.0277.0236.067/obscure.htm
IP en hexa : http://0x9A3F0800CEBF9E37/obscure.htm
pleins de zéros : http://00000000316.000277.00000236.00000000067/obscure.htm
dotless : http://206.12557879/obscure.htm

http://www.pc-help.org/obscure.htm

Contourner NoScript pour $11

- En achetant un sous domaine d'un domaine de confiance

http://thehackerblog.com/the-noscript-misnomer-why-should-i-trust-vjs-zendcdn-net/

Piratages, Malwares, spam, fraudes et DDoS

Malware

Tentative d'exploitation de RawHammer

- Depuis un langage compilé dynamiquement (JIT / Just in time compilation)
- C’est un échec 

https://xuanwulab.github.io/2015/06/09/Research-report-on-using-JIT-to-trigger-RowHammer/

90% des lecteurs de CB vulnérables

- Car installés chez le commerçant avec le mot de passe usine (166816 et Z66816)

http://www.undernews.fr/banque-cartes-bancaires/un-code-unique-pour-pirater-90-des-lecteurs-de-cb.html

Piratages, Malwares, spam, fraudes et DDoS

DDoS

DDoS réflectif à base d'un vieux protocole de routage : RIPv1

- C'est dans les vieux pots…
- Surtout à partir de routeurs SOHO (encore…)

  http://www.infoworld.com/article/2942749/network-security/obsolete-internet-protocol-once-again-becomes-an-attack-vector.html

Des anonymes lancent une opération contre les banques #OpHitTheBanks

- Peu suivi

  https://www.facebook.com/anonymousforjustice/photos/a.273927042756537.1073741828.273925916089983/495492507266655/?type=1

Piratages, Malwares, spam, fraudes et DDoS
Espionnage

Dino, le cousin de Babar, Casper et Bunny

- Le gentil petit dinosaure végétalien 😜
- Le nouvel implant gouvernemental français 
- C'est la “ferme des animaux” mais :
  - Le nom "claque" moins que Stuxnet et Duqu
  - Les fonctionnalités sont bien loin de GrayFish et Duqu 2.0

  http://www.lemonde.fr/pixels/article/2015/06/30/dino-le-nouveau-programme-espion-developpe-par-des-francophones_4664675_4408996.html
- L'analyse d'ESET :

  http://www.welivesecurity.com/2015/06/30/dino-spying-malware-analyzed/

Duqu 2.0, le nouvel implant américano-israelien

- Intrusion chez Kaspersky et découverte “par hasard”
- Binaire signé avec un certificat volé à Foxconn
- Repose sur les fonctionnalités des domaines Microsoft AD pour sa résilience et infecte les DC
- S’injecte sur les postes de travail par exécution d’un MSI
  - Déchiffré à la volée avec un mot de passe passé en paramètre
  - Tourne uniquement en mémoire, pas de trace
  - Élévations de privilèges
    - Noyau windows CVE-2014-4148 et CVE-2015-2360
    - La fameuse vulnérabilité Kerberos CVE-2014-6324 / MS14-068
  - Hook et injection avec des instructions SSE2
- Utilisé pour espionner les négociation dites « P5+1 » sur le nucléaire iranien

  https://securelist.com/blog/research/70504/the-mystery-of-duqu-2-0-a-sophisticated-cyberespionage-actor-returns/

Piratages, Malwares, spam, fraudes et DDoS

Espionnage

La NSA c'est fait pour l'espionnage économique "bis" (cf. revue 2014-04-08)

- Publication de câbles diplomatiques par Wikileaks demandant d'espionner la France sur :
  - Les télécommunications
  - Les installations et entreprises du secteur énergétique (électricité, gaz, pétrole et nucléaires)
  - Les installations et entreprises du transport (aéroports et ferroviaires)
  - Les nouvelles technologiques comme la biotechnologie
  - Tous les contrats et en particulier ceux d'un montant dépassant 200 millions d'euros

https://wikileaks.org/nsa-france/spyorder/

La DGSE aussi collecte toutes les télécommunications

- A moindre échelle que la NSA mais sans doute les meilleurs (moins mauvais) d'Europe !

http://www.lemonde.fr/pixels/article/2015/07/01/comment-sarkozy-et-hollande-ont-autorise-une-vaste-surveillance-d-internet_4666310_4408996.html

http://www.01net.com/editorial/659369/supercalculateurs-et-fibres-optiques-comment-la-france-espionne-le-monde/

Skynet, le programme de la NSA pour localiser les terroristes

- A base de collecte de métadonnées
  - Et envoyer un drone bardé de missiles ?

www.developpez.com/actu/85171/La-NSA-a-developpe-un-programme-baptise-Skynet-pour-identifier-les-terroristes-en-se-basant-sur-la-localisation-et-les-metadonnees-des-communications/

Piratages, Malwares, spam, fraudes et DDoS
Espionnage

En 2011, l'Elysée découvrait un (des) implant américain

- Heureusement qu'Hollande n'a pas d'ordinateur ;-)
  http://www.lepoint.fr/politique/quand-les-americains-espionnaient-les-ordinateurs-de-l-elysee-24-06-2015-1939611_20.php

La NSA a espionné nos 3 derniers présidents

http://www.lemonde.fr/pixels/article/2015/06/23/revelation-apres-revelation-le-silence-de-la-france-face-a-l-espionnage-de-la-nsa_4660310_4408996.html

- Holland et Ayrault aussi auraient été écouté
  - Ils ont donc eu une valeur stratégique, l'honneur est sauf ! 
  http://electrospaces.blogspot.fr/2015/06/wikileaks-publishes-some-of-most-secret.html#methods
- Mais Obama assure que la NSA a arrêté 
  - N'aurions plus de valeur stratégique ?
  http://www.france24.com/fr/20150624-franceleaks-obama-hollande-nsa-wikileaks-ecoute-plus-etats-unis-france-presidents

Quelques détails sur XKeyScore

- Le moteur de recherche de la NSA
  http://www.01net.com/editorial/659392/comment-fonctionne-xkeyscore-le-google-de-la-nsa/
- Utilisé comme base pour intercepter des connections aux stores Google/Apple et injecter des malwares
  https://firstlook.org/theintercept/2015/05/21/nsa-five-eyes-google-samsung-app-stores-spyware/

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Piratage de 1337day.com (Suite de Milw0rm et Inj3ctor)

- Piratage ou domaine réquisitionné par la CIA ?
  https://www.facebook.com/inj3ct0rs/photos/a.188734184521282.47586.121674351227266/923154241079269/
  http://www.infosecfeeder.com/1337day-com-hacked-by-rab3oun-and-x-gun/

Piratage de sites e-commerce basés sur Magento

- Avec injection de code et enregistrement du contenu de tous les POST, chiffré avec RSA
  https://blog.sucuri.net/2015/06/magento-platform-targeted-by-credit-card-scrapers.html

LastPass

- Vol des mails, indices et hash des mots de passe maîtres
- Les contenus des coffres numériques n'auraient pas été touchés
- *Pour rappel : le nom d'utilisateur et le mot de passe maître sont tous les deux hashés sur l'ordinateur de l'utilisateur avec 5,000 itérations PBKDF2-SHA256, puis ajout d'un sel et 100 000 itérations de hashage côté serveur*
  https://blog.lastpass.com/2015/06/lastpass-security-notice.html/

Grosse campagne de phishing

- Exploitation des macro Office
- Téléchargement de trojan en VBS sur Pastebin ou de binaires sur d'autres sites
  - VBS obfusqué avec des StrReverse()

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Un serveur de la fondation Apache

- Transformé en serveur IRC
  https://blogs.apache.org/infra/entry/buildbot_master_currently_off_line

Un casino pour bitcoin perd $1M

Car les résultats du PRNG étaient prédictibles
https://medium.com/@Stunna/breaking-the-house-63f1021a3e6d

Les serveurs PLEX piratés

- Uniquement les forums et le blog, pas d'accès au code (à priori)
  http://www.theregister.co.uk/2015/07/02/plex_targeted_by_hackers/

L'université de Harvard piratée

- Vol des logins/mots de passe des étudiants et professeurs
  http://www.darkreading.com/cloud/harvard-suffers-data-breach-spanning-multiple-schools-administration-networks/d/d-id/1321184

Piratages, Malwares, spam, fraudes et DDoS

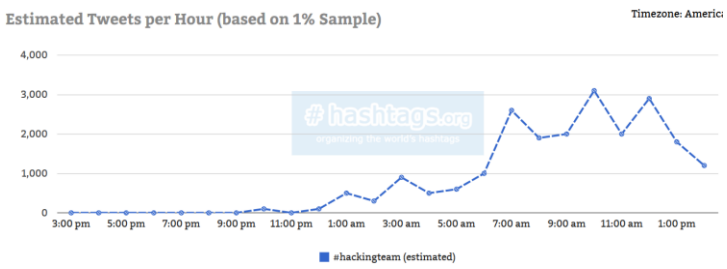
Sites Piratés

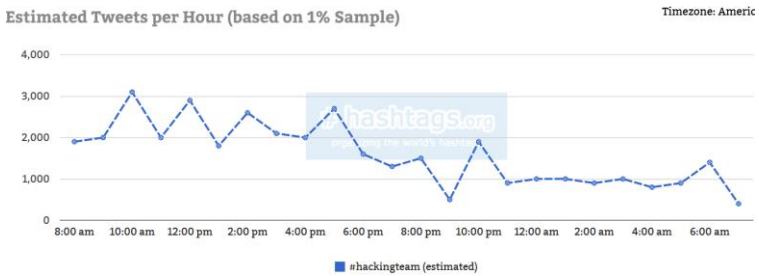
Hacking Team

- Société italienne offensive
- Piratage par le même hackeur de pour Gamma
  - Mais sans que tout soit chiffré
- Publication de **400 Go** de données
  - Emails (des gigas de PST)
  - Contrats avec la NSA, l'Egypte, le Soudan…
  - Codes source des trojans :
    - Windows 32 et 64 bits
    - iOS
    - Android
  - Des vulnérabilités provenant de chez VUPEN
  - Fichier Excel en clair avec tous les login/pass de leurs VPS
  - Mots de passe Firefox, youporn...
  - SQLi dans leur propre code (backdoor?)

http://www.csoonline.com/article/2943968/data-breach/hacking-team-hacked-attackers-claim-400gb-in-dumped-data.html
http://www.csoonline.com/article/2944333/data-breach/hacking-team-responds-to-data-breach-issues-public-threats-and-denials.html

- Mozilla ouvre un Bug Bounty pour toute vulnérabilité remonté grâce au leak





Sales Report

Hacking Team

FAE		**Report Type**	Customer meeting follow-up
Sales	Philippe Vinci	**Country**	France
Partner		**City**	Paris
Customer	Ministère de l'Intérieur (?)	**Date**	02/04/2015

Activities performed: Follow-up Meeting

3 participants on MOI side: Tancrede Lecluse (ex DGSI), Yvan X (?), Y (?)
2 participants on HT side: Emanuele Levi, Philippe Vinci

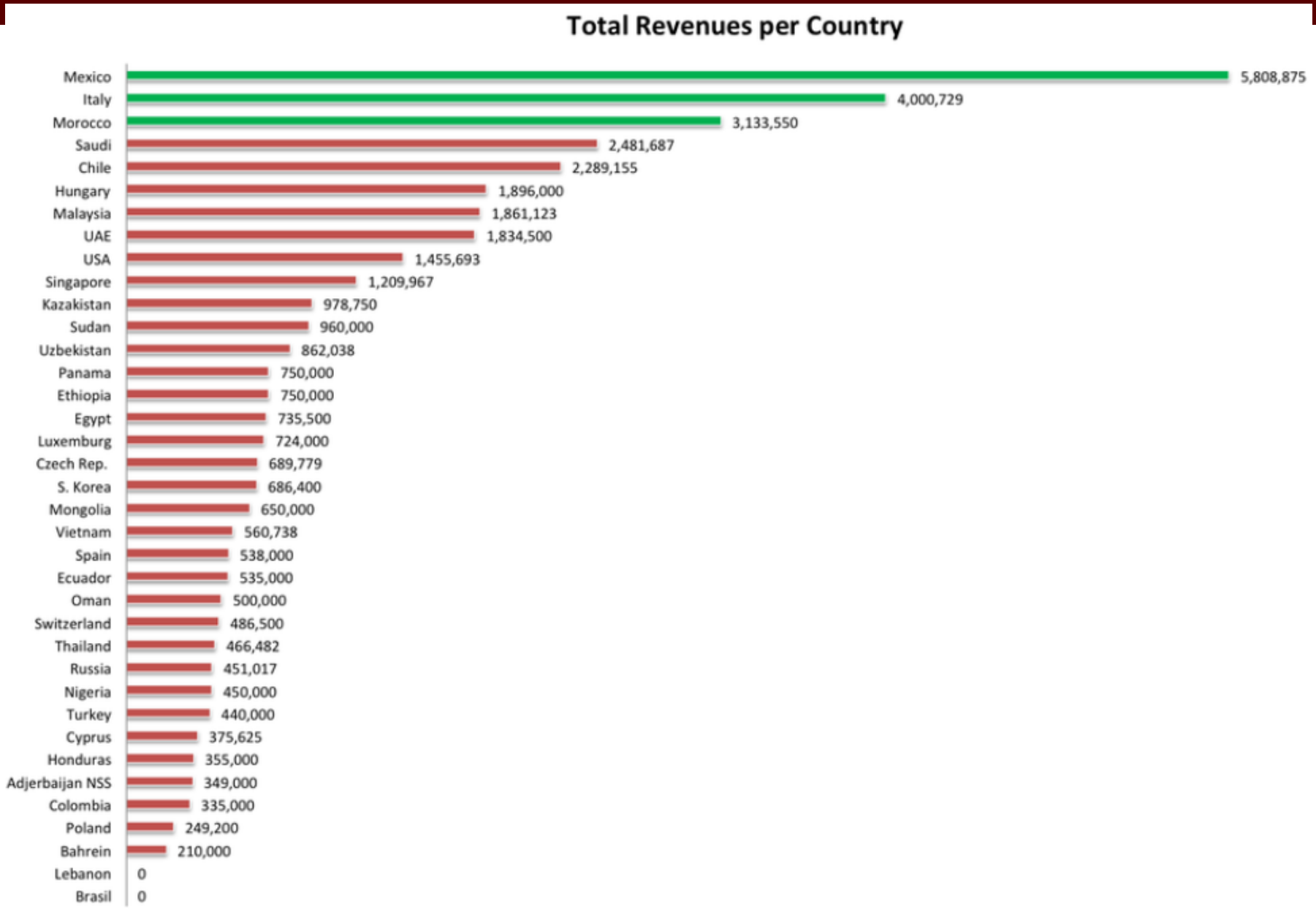
Objective of the meeting was to touch base again with French **Ministère de l'Intérieur**, update them on Hacking Team and above all qualify their "appetite" on solutions such as Galileo.

Internal objective was to get them interested sufficiently so that they request a complete product presentation and demo, a) in France, or b) in Milano. Our goal was to find the arguments to bring them to Milano.

3. **ISP Network Injection** solution (I think this one caused an excellent "body language" reaction)
4. The **Architecture** with separated components such as Master Node, Collectors, Anonymizers. All controlled by them
5. Target-Centric solution with a unified Graphical User Interface independent of Platform and independent on Infection methods.
6. **Multi-stage infection** our **Event / Action** easily configurable for each scenario.
7. **RITE** or our Testing-Ecosystem
8. A clear published Customer Policy
9. **Crisis Management Process** (although we were not able to describe the process in detail)
10. A pure Software License business model + including M&S with Upgrades + EDN Services

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés



Crypto
Divers

s2n d'Amazon

- Après GnuTLS, LibreSSL, TLS en OCaml (revue 2014-09-09), BoringSSL de Google (revue 2014-09-09)...
- Voici une nouvelle implémentation de TLS, cette fois-ci par Amazon
  - Seulement 6k lignes de code, ne supporte que fonctionnalités les plus communes
  - Basé sur la crypto d'OpenSSL (ou ses fork)

http://blogs.aws.amazon.com/security/post/TxCKZM94ST1S6Y/Introducing-s2n-a-New-Open-Source-TLS-Implementation
https://github.com/awslabs/s2n

Casser des mots de passe en Cloud

- Sagitta, vendeur d'appliance et possiblement de services SaaS
- En complément de la présentation du 14 avril 2015 Octopus Password Breaker
- WPA/WPA2 à 2 526,0 kH/s (~ 2 000 000 hash/s.)
- NTLM à 311,6 GH/s (~ 300 000 000 000 hash/s.)

https://gist.github.com/epixoip/63c2ad11baf7bbd57544

Comment créer une porte dérobée cryptographique

http://blog.cryptographyengineering.com/2015/04/how-do-we-build-encryption-backdors.html

Chiffrement homomorphique quantic !

http://eprint.iacr.org/2015/551

Pentest
Techniques & outils

IDA Pro full instruction reference plugin

- plugin https://github.com/nologic/idaref

Reverse Shell Cheat Sheet

- https://highon.coffee/blog/reverse-shell-cheat-sheet/

HTTP sur Sysinternals

- Après smb:\\live.sysinternals.com\tools
- Voici https://live.sysinternals.com/ et http://live.sysinternals.com

Pyxiewps pour casser du WPS (automatiquement)

http://n0where.net/wireless-attack-tool-pyxiewps/

Mimikatz

- Déchiffrement des clefs DPAPI
  https://twitter.com/gentilkiwi/status/609890409830064129/photo/1
- Création de tickets avec SID parents/externes dans la config par défaut
  https://twitter.com/gentilkiwi/status/615289503029305345

Un module Metasploit pour voler les mots de passe locaux stockés avec LAPS

http://www.rapid7.com/db/modules/post/windows/gather/credentials/enum_laps

Dumper les hash de domaine proprement avec un Meterpreter

- Utilisation des APIs Windows, plus besoin de copier ntds.dit
  https://community.rapid7.com/community/metasploit/blog/2015/07/01/safely-dumping-domain-hashes-with-meterpreter

Meterpreter en mode “parano”

- Combinaison de deux fonctions sur un Meterpreter reverse HTTPS
- Certificate Pinning : Assure que les victimes se connectent uniquement à votre serveur
- UUID payload filtering : seules les machines qui ont reçu votre payload sont acceptées
  https://github.com/rapid7/metasploit-framework/wiki/Meterpreter-Paranoid-Mode

WS-Attacker : framework d’exploitation de WebServices

https://github.com/RUB-NDS/WS-Attacker

M/o/vfuscator

- Outil d’ “obfuscation” de code qui compile un programme uniquement en instructions MOV
- Fonctionnel uniquement pour Brainfuck pour le moment
  https://github.com/xoreaxeaxeax/movfuscator

Pentest

Techniques & outils

Backdoorer un domaine AD en chainant les droits

https://www.exploit-db.com/papers/17167/

Meterpreter pour contourner le déchiffrement SSL

- En sur-chiffrant

  http://rwhitcroft.github.io/blog/2015/05/28/defeating-ssl-inspection-with-meterpreter/

Scada
Divers

Rapport du SANS sur le niveau de sécu des SI industriels

https://www.sans.org/reading-room/whitepapers/analyst/state-security-control-systems-today-36042

N-Tron’s 702-W Point d'accès Wifi

- Clefs SSH en dur
- Vulnérabilités SSL/TLS

http://www.isssource.com/n-tron-encryption-key-vulnerability/

Clés hardcodées dans les produits GarettCom Magnum

- CVSS 4.2 pour une clé SSH en dur, on n’a pas la même calculette …

https://ics-cert.us-cert.gov/advisories/ICSA-15-167-01

Exécution de code locale sur Schneider Wonderware

- Par le chargement d’une dll

https://ics-cert.us-cert.gov/advisories/ICSA-15-169-02

Séquence TCP prédictible sur VxWorks

- Notamment utilisé dans les automates Schneider

https://ics-cert.us-cert.gov/advisories/ICSA-15-169-01

Scada
Divers

Analyse du niveau de sécurité des applications SCADA pour mobile

- Oui, oui, ça existe
- Certaines docs montrent clairement un accès aux installations depuis l'externe
- Présenté à la BlackHat Mobile à Londres

  http://fr.slideshare.net/dark_k3y/scada-and-mobile-blackhat-london-mobile-security-summit-2015

Vulnerability/weakness	Control-room app	OPC-/MES- client	Remote SCADA client
M1: Weak server-side controls	0	1	0
M2: Insecure Data Storage	2	0	3
M3: Insufficient transport layer protection	0	3	6
M5: Poor authorization and authentication	*n/a*	3	4
M6: Broken crypto	0	2	7
M7: Client side injection	1	0	0
M8: Security decisions via untrusted inputs	*n/a*	0	1
No password protection	4	5	4
Denial of Service	1	0	3

Nouveautés (logiciel, langage, protocole...)

Open Source

Mozilla relance le multi process pour Firefox

- Pour faire tourner chaque onglet dans un processus différent
  http://www.computerworld.com/article/2936593/web-browsers/mozilla-restarts-work-on-multi-process-firefox.html

Kali 2.0

- Lien à venir

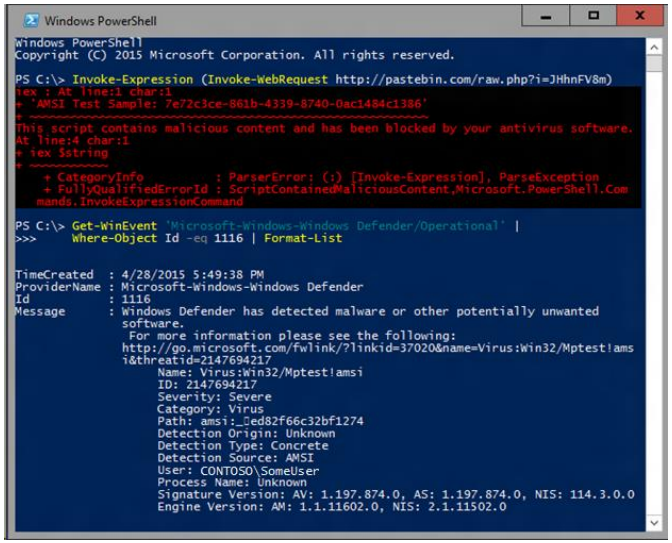
Nouveautés (logiciel, langage, protocole...)

Divers

Nouveautés sécurité dans Windows

- AMSI : *AntiMalware Scanning Interface* : permet à chaque application de demander un scan AV, dispo également en PowerShell

http://blogs.technet.com/b/mmpc/archive/2015/06/09/windows-10-to-offer-application-developers-new-malware-defenses.aspx



Nouveauté dans Mac OSX : *System Integrity Protection*

- Fonctionnelle de base à partir de OSX El Capitain
- Au programme
  - Protection en écriture des répertoires et fichiers système (/system, /bin, /usr, /sbin)
  - Nouveau flag pour les processus restreints
  - L'ensemble des extensions (kext) doivent être signées
  - Désactivable via un boot sur un CD de récupération
- ⇒ Fini le root, comme sur iOS, Android, etc..
  http://devstreaming.apple.com/videos/wwdc/2015/706nu20qkag/706/706_security_and_your_apps.pdf
  http://devstreaming.apple.com/videos/wwdc/2015/706nu20qkag/706/706_sd_security_and_your_apps.mp4?dl=1

Business

France

IBM + Sogeti = SOC de l'ANSSI.lu

http://www.lessentiel.lu/fr/economie/story/IBM-et-Sogeti-luttent-contre-les-cyberattaques-16264506

Rachat de Lexsi par…

- Une grosse entreprise américaine 😜

Business
International

Certifications

- DropBox certifié ISO 27001 et 27018 (mais n'existe pas encore)
  https://www.dropbox.com/static/business/resources/dropbox-certificate-iso-27001.pdf
  https://www.dropbox.com/static/business/resources/dropbox-certificate-iso-27018.pdf
- Oodrive certifié ISO 27001:2013
  https://cloud.google.com/files/ISO27001_Digital_V2.pdf
- Par Ernst and Young CertifyPoint, qui a déjà certifié :
  - Google Apps en 2012 https://cloud.google.com/files/ISO27001_Digital_V2.pdf
  - AWS en 2010 https://d0.awsstatic.com/certifications/iso_27001_global_certification.pdf

Microsoft revend une partie de Bing (Nokia Here) à Uber

- Mais pourra continuer à utiliser la base d'image
  http://www.clubic.com/moteur-de-recherche/bing/actualite-772092-microsoft-aol-uber.html

L'US Navy dépenserait $30 millions pour maintenir le support de Windows XP

- Pour ses 100 000 PC

  https://nakedsecurity.sophos.com/2015/06/24/us-navy-pays-millions-to-cling-to-windows-xp/

Business
International

Cisco pourrait racheter OpenDNS

- Pour $635 millions !!!

https://www.opendns.com/cisco-opendns/

DuckDuckGo : +600% depuis les révélations sur la NSA

https://duckduckgo.com/traffic.html

Gros écart d'investissement entre opérateurs européens et américains

- Entre 2006 et 2023 : US = +39 % , EU = +6%

http://www.lesechos.fr/tech-medias/hightech/021101728907-telecoms-lecart-sest-creuse-dans-les-investissements-entre-operateurs-europeens-et-americains-1123851.php

Droit / Politique

France

CIC : Application intrusive, tweet et clôture de compte

http://korben.info/cic-violence.html

Loi de renseignement adoptée par le Sénat

- Par des experts techniques :
  - <<Qui sait parmi nous ce qu'est un algorithme quand certains ici utilisent encore un téléphone d'un autre âge ?>>

http://rue89.nouvelobs.com/2015/06/09/senat-sait-parmi-quest-algorithme-259663

Droit / Politique
International

Microsoft ouvre son code source aux gouvernements

- Dans son centre à Bruxelles, annoncé début en 2014
- C'est l'ANSSI qui doit être contente
  - Préparez-vous à payer des tournées à vos copains de l'ANSSI pour des soirées alcool et anecdotes truculentes sur le code de Microsoft

https://blogs.microsoft.com/eupolicy/2015/06/03/microsoft-transparency-center-opens-in-brussels/

La Russie développera son propre OS mobile

- Basé sur SailFish, lui même basé sur MeeGo de Konia

https://translate.google.com/translate?sl=auto&tl=en&js=y&prev=_t&hl=en&ie=UTF-8&u=http%3A%2F%2Ftop.rbc.ru%2Ftechnology_and_media%2F17%2F05%2F2015%2F55585f5b9a79471191c70fb3&edit-text=&act=url

Silk Road : Les agents de la DEA corrompus ont plaidé coupable

https://nakedsecurity.sophos.com/2015/06/25/dea-agent-who-lined-his-pockets-with-silk-road-bitcoins-pleads-guilty/

Notepad++ quitte sourceforge

- Suite l'ajout de poubelleware par sourceforge dans plusieurs projets (Gimp, nmap, vlc...)

https://notepad-plus-plus.org/news/notepad-plus-plus-leaves-sf.html

Arrestation du gang « Zeus » par Europol

- Gang Ukrainien soupçonné de développer Zeus et SpyEye
- mais pas Evgeniy MIKHAILOVICH BOGACHEV, toujours recherché par le FBI (cf. revue 2015-04-14)

http://www.undernews.fr/malwares-virus-antivirus/europol-arrestation-du-gang-derriere-les-trojans-bancaires-zeus-et-spyeye.html

Droit / Politique
International

Procès Google vs Oracle

- violation du droit d'auteur par Google sur 37 API Java
- En première instance, Oracle avait obtenu gain de cause
- L'appel de Google vient d'être rejeté
  http://www.supremecourt.gov/orders/courtorders/062915zor_4g25.pdf

Justice et objets connectés

- Accusations de viol en Floride
- La supposée “victime” donnes ses authentifiant Fitbit aux policiers
- L’analyse de données ne corrobore pas sa version ⇒ elle est accusée de faux témoignage
  http://fusion.net/story/158292/fitbit-data-just-undermined-a-womans-rape-claim

Conférences

Texte en gris = déjà traité précédemment

Passées

- SSTIC 2015 - 3, 4 et 5 juin 2015 à Rennes
  - Compte rendu donné à l'afterwork de l'OSSIR
- Hack in the Box - 26 au 29 mai 2015 à Amsterdam
  http://conference.hitb.org/hitbsecconf2015ams/
- Hack in Paris - 15 au 19 juin 2015 + Nuit du Hack - 20 au 21 juin 2015 à l'Académie Fratellini
  - Compte rendu ce jour

A venir

- Black Hat USA 2015 - 1 au 6 aout 2015 à Las Vegas
- DefCon 23 - 6 au 9 aout 2015 à Las Vegas
- BruCon - 8 au 9 octobre 2015 à Gand, Belgique
- Botconf - 2 au 4 décembre 2015 à Paris

Divers / Trolls velus

Audit sauvage sur le SI d'un membre de l'association

- Par bspeek
- "Professionnels, retailers, fabriquants : et si vous disposiez d'une armée de plusieurs milliers de personnes pour collecter des données commerciales sur 100, 300 ou 3000 lieux en temps réel afin de développer votre business ?"

  http://blog.bpeek.com/project/campus-mission-connectee

Les développeurs web chez Pole Emploi

```
//alert("je désactive  la css structure");
…
//alert("ayé");
…
//alert("je réajoute la css structure");
…
});
//alert("ayé");
…
}
/* tester les templates, bof.....
*/
```

Divers / Trolls velus

La position de “singe intercepteur”... par l’ANSSI

http://www.cert.ssi.gouv.fr/site/CERTFR-2015-ACT-025/
http://ailleti-saycuriti.tumblr.com/

Selon le FBI : Chiffrer c’est aider les terroristes

- Toujours mieux que de tuer un enfant (cf. revue du 2014-12-09)
  http://www.zdnet.fr/actualites/pour-le-fbi-le-chiffrement-est-un-service-rendu-aux-terroristes-39820328.htm

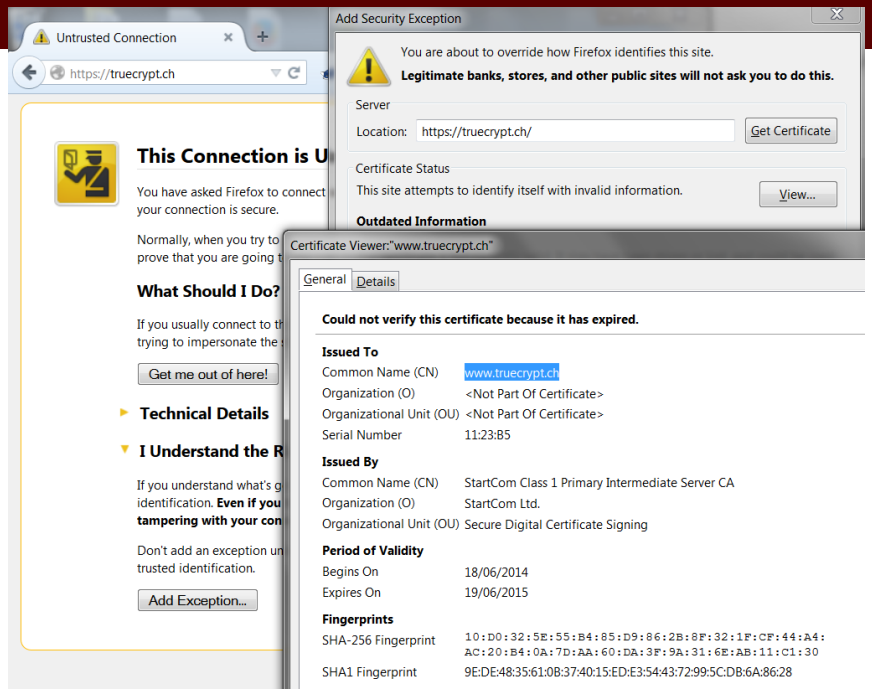
Un QG de l’État Islamique en Irak et Al-Sham » (ISIS) bombardé grâce à un Selfie

- Ou plutôt “localisé” grâce à un selfie
  https://www.schneier.com/blog/archives/2015/06/us_identifies_a.html

Divers / Trolls velus

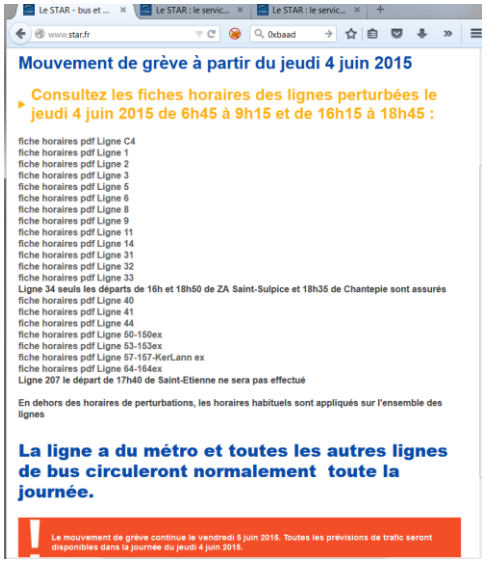
TrueCryptNext : Tous les certificats web ont périmés le 19/06

- ahhh… les bonnes pratiques et le renouvellement des certificats…
- <<La sécurité est un échec ©>>



Les conférences de sécurité *vs* les grèves

- SSTIC 2015 et la grève de la STAR
  http://www.20minutes.fr/rennes/1622003-20150602-rennes-preavis-greve-depose-jeudi-reseau-star
- JSSI 2015 et la grève de la grève SNCF
  http://www.tourmag.com/Greve-SNCF-tres-peu-de-perturbations-a-prevoir-mardi-10-mars-2015_a72672.html



Divers / Trolls velus

Frontières US bloquées.. à cause d'une panne Oracle

http://travel.state.gov/content/travel/english/news/technological-systems-issue.html

Samsung vs Windows Update

- La raison de la désactivation de Windows Update est plus que discutable…
  - Windows pouvait installer les mauvais pilotes

https://grahamcluley.com/2015/06/samsung-disabled-windows-update/

Project Vault, un ordinateur sur une carte MicroSD

- Une sorte de mini HSM par Google pour Smartphone
  - CPU ARM
  - NFC
  - 4GB de stockage
  - un OS temps réel

https://github.com/ProjectVault/orp

http://thehackernews.com/2015/05/google-vault-microsd.html

Les utilisateurs ont (enfin) moins confiance vis à vis des Antivirus

http://www.bromium.com/sites/default/files/bromium-report-endpoint-survey.pdf

- Alors ils rusent/bidouillent

http://www.cnet.com/how-to/i-dont-use-anti-virus-software-am-i-nuts/

Divers / Trolls velus

Un vandale sectionne des fibres en Californie

- Déjà 11 sabotages
  https://nakedsecurity.sophos.com/2015/07/02/mystery-vandals-are-cutting-fiber-optic-cables-in-california-how-worried-should-we-be/

iOS Jailbreak stories

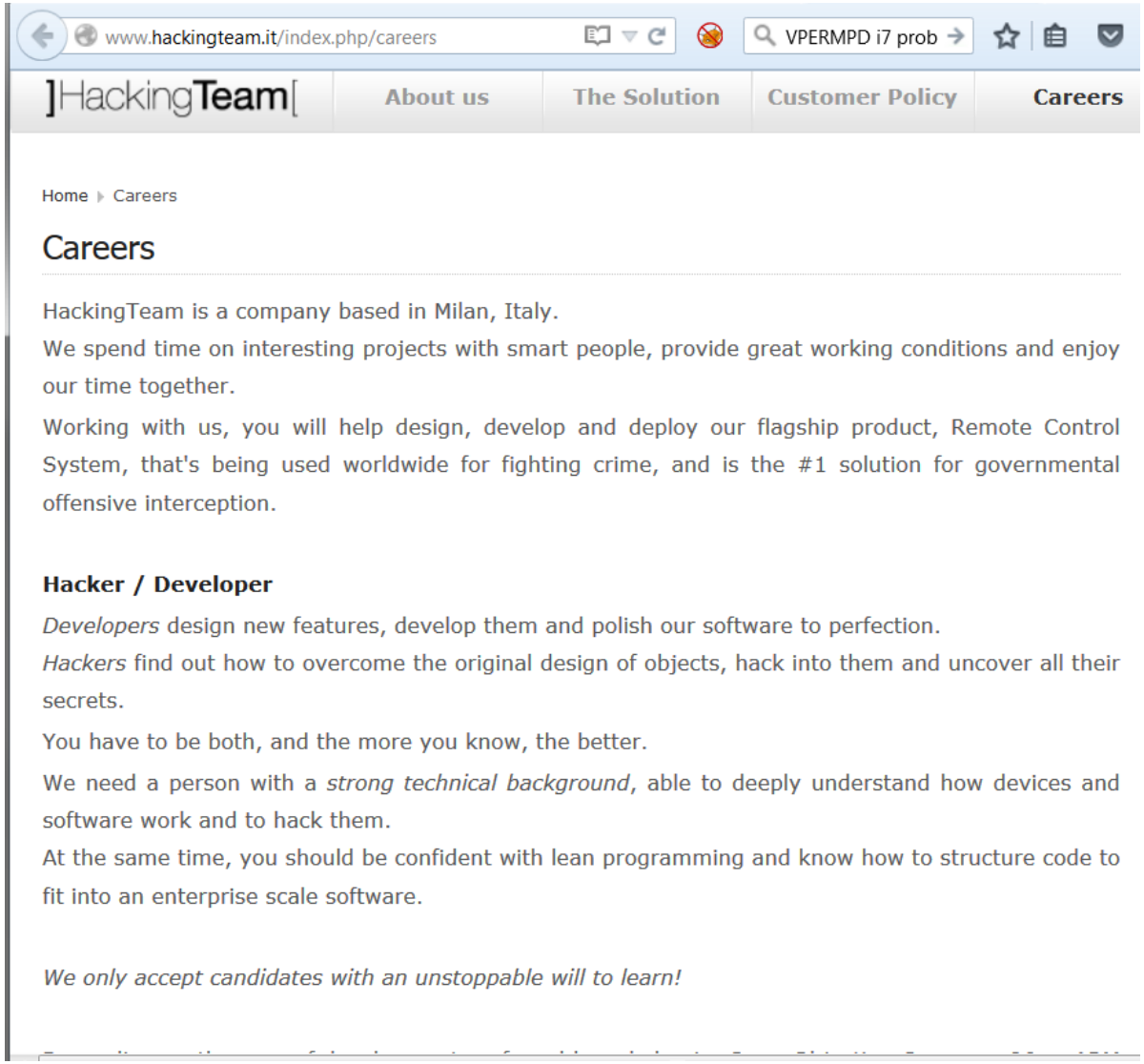
- Stefan Esser mécontent que Pangu présente à la BlackHat (cf. revue du 2014-11-18)
  https://twitter.com/i0n1c/status/615933676745031680
- 25ppcom aurait volé des éléments de Taig pour le jailbreak d'iOS 8.4
  https://twitter.com/cammywrites/status/615933579881807872
  https://twitter.com/taig_jailbreak/status/615939601463508993
- TaiG sort donc son JailbreakTool V2.2.0
  https://twitter.com/taig_jailbreak/status/615963170440478720

VNC Roulette

- Déjà coupé :-/
  http://www.reddit.com/r/sysadmin/comments/3bfeyt/vncroulette_crawls_shodanio_for_rfb_auth_disabled/

Divers / Trolls velus

Hacking Team recrute !



Prochaines réunions

- Mardi 8 septembre 2015

AfterWork

- Mardi 22 septembre 2015

  Bar "La Kolok"
  20 rue du croissant
  75002 Paris

Questions ?