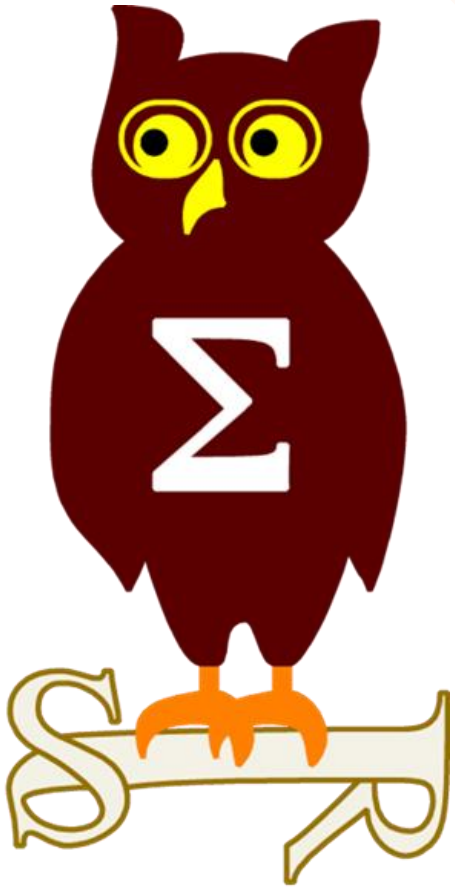
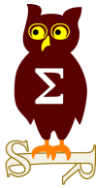


Revue d'actualité

13/06/2017

Préparée par

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



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories

Microsoft - Avis

Vulnérabilité dans Internet Explorer (5 CVE)

- Affecte:
  - Windows (toutes versions supportées)
- CVE:
  - CVE-2017-0064, CVE-2017-0222, CVE-2017-0226, CVE-2017-0228, CVE-2017-0231
- Exploit:
  - 2 x Corruptions de mémoire aboutissant à une exécution de code
    - CVE-2017-0222 exploitée dans la nature
  - 1 x Contournement des filtres SmartScreen
  - 1 x Exécution de code à partir de Javascript
  - 1 x Chargement de contenu HTTP depuis une page HTTPS

Vulnérabilité dans Edge (14 CVE)

- Affecte:
  - Windows 8.1, 10
- CVE:
  - CVE-2017-0221, CVE-2017-0224, CVE-2017-0227, CVE-2017-0229, CVE-2017-0230, CVE-2017-0231, CVE-2017-0233, CVE-2017-0234, CVE-2017-0235, CVE-2017-0236, CVE-2017-0238, CVE-2017-0240, CVE-2017-0241, CVE-2017-0266
- Exploit:
  - 8 x Corruptions de mémoire aboutissant à une exécution de code
  - 1 x Contournement des filtres SmartScreen
  - 4 x Exécution de code à partir de Javascript
  - 1 x Évasion de la sandbox
  - SHA-1 déprécié

Dont 1 commune avec IE:

- CVE-2017-0231

Failles / Bulletins / Advisories

Microsoft - Avis

Vulnérabilité dans Ms Defender “Malware Protection Engine” (1 CVE)

- Affecte:
  - Windows 7, 8.1, 10, 2012, 2016, Microsoft Security Essentials
- CVE:
  - CVE-2017-0290
- Exploit:
  - Exécution de code en tant que SYSTEM à la consultation d'un mail, site...

https://bugs.chromium.org/p/project-zero/issues/detail?id=1252&desc=5
https://0patch.blogspot.fr/2017/05/0patching-worst-windows-remote-code.html

Vulnérabilités dans Ms Defender “Malware Protection Engine” (4 CVE) *Corrigées silencieusement*

- Affecte:
  - Windows 8.1, 10, 2012, 2016, Microsoft Security Essentials
- CVE:
  - CVE-2017-8538, CVE-2017-8537, CVE-2017-8536, CVE-2017-8535
- Exploit:
  - Dénis de service. Exécution de code non confirmée.

https://bugs.chromium.org/p/project-zero/issues/detail?id=1261
https://threatpost.com/microsoft-quietly-patches-another-critical-malware-protection-engine-flaw/125951/

Failles / Bulletins / Advisories

Microsoft - Avis

Encore une Vulnérabilité dans Ms Defender “Malware Protection Engine” (1 CVE)

- Affecte:
  - Windows 8.1, 10, 2012, 2016, Microsoft Security Essentials
- CVE:
  - CVE-2017-8540
- Exploit:
  - Exécution de code en tant que SYSTEM

https://bugs.chromium.org/p/project-zero/issues/detail?id=1258

Vulnérabilité dans Hyper-V (1 CVE)

- Affecte:
  - Windows 10, 2016
- CVE:
  - CVE-2017-0212
- Exploit:
  - Elévation de privilèges à partir de vSMB

Failles / Bulletins / Advisories

Microsoft - Avis

Vulnérabilités noyau (5 CVE)

- Affecte:
  - Windows (toutes versions supportées)
- CVE:
  - CVE-2017-0175, CVE-2017-0220, CVE-2017-0244, CVE-2017-0258, CVE-2017-0259
- Exploit:
  - 4 x Fuites d'information
  - 1 x Elévation de privilèges

https://bugs.chromium.org/p/project-zero/issues/detail?id=1127
https://bugs.chromium.org/p/project-zero/issues/detail?id=1161

Vulnérabilités noyau Win32k (3 CVE)

- Affecte:
  - Windows (toutes versions supportées)
- CVE:
  - CVE-2017-0245, CVE-2017-0246, CVE-2017-0263
- Exploit:
  - 1 x Fuite d'information
  - 2 x Elévations de privilèges

https://bugs.chromium.org/p/project-zero/issues/detail?id=1182

Failles / Bulletins / Advisories

Microsoft - Avis

Vulnérabilités dans Microsoft SMBv1 (14 CVE)

- Affecte:
  - Windows (toutes versions supportées)
- CVE:
  - CVE-2017-0212
  - CVE-2017-0267, CVE-2017-0268, CVE-2017-0269, CVE-2017-0270, CVE-2017-0271, CVE-2017-0272, CVE-2017-0273, CVE-2017-0274, CVE-2017-0275, CVE-2017-0276, CVE-2017-0277, CVE-2017-0278, CVE-2017-0279, CVE-2017-0280
- Exploit:
  - 1 x Elévation de privilèges à partir de vSMB
  - 4 x Exécutions de code à distance en tant que SYSTEM
  - 7 x Contournements ASLR et/ou fuite d'information
  - 3 x Déni de service

Vulnérabilités dans Office (16 CVE)

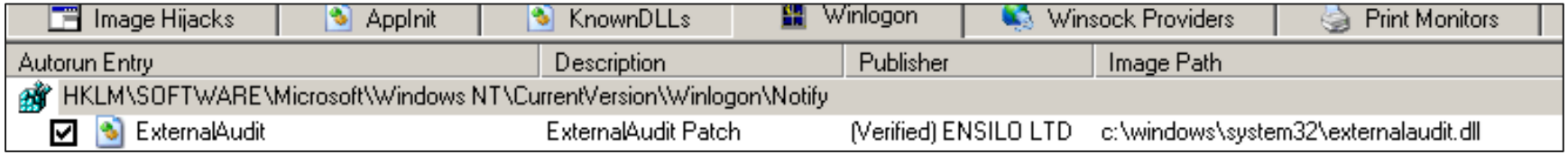
- Affecte:
  - Office 2007, 2010, 2013, 2013RT, 2016, Mac 2011 et 2016
  - Sharepoint 2010, 2013
- CVE:
  - CVE-2017-0254, CVE-2017-0261, CVE-2017-0262, CVE-2017-0264, CVE-2017-0265, CVE-2017-0281
- Exploit:
  - Corruptions de mémoire aboutissant à une exécution de code à l'ouverture d'un fichier Office
  - CVE-2017-0261 exploitée dans la nature

Failles / Bulletins / Advisories

Microsoft - Avis

Vulnérabilité EsteeMaudit (NSA), un correctif non officiel pour Windows XP et 2003

- EsteeMaudit = Exécution de code à distance sur RDP
- Le correctif fonctionne sur Windows XP SP3 32 et 64 bits ainsi que 2003 R2
- Ajouter une DLL au démarrage qui patch WinLogon en mémoire



http://pages.ensilo.com/download-the-patch-for-esteemaudit-exploit

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 - Autre

Microsoft Azure support OpenBSD 6.1

https://azure.microsoft.com/en-us/blog/running-openbsd-on-azure/

Windows 10 build 16215

- Activation de Arbitrary Code Guard et Code Integrity Guard pour svhost

https://twitter.com/epakskape/status/873042557705478145/photo/1

Déploiement par erreur d'une version instable de Windows 10

- Uniquement pour ceux ayant souscrit au programme "Windows Insider"

https://www.nextinpact.com/news/104441-insider-microsoft-a-deploye-par-erreur-preversion-instable-comment-sen-debarrasser.htm

Microsoft Malware Protection Engine, l'émulateur x86 de l'antivirus de Windows...

- Offre une API pour contrôler l'émulateur
  - Chargement de code, modification des paramètres d'exécution...

https://bugs.chromium.org/p/project-zero/issues/detail?id=1260

Première mise à jour ne fonctionnant plus sur les anciens CPU

- Pour les systèmes Windows 7 ou 8.1

https://www.nextinpact.com/news/104031-windows-78-1-microsoft-active-blocage-mises-a-jour-sur-pc-kaby-lake-et-ryzen.htm

Failles / Bulletins / Advisories

Système (principales failles)

Samba, exécution de code à distance nécessitant une authentification

- Depuis Samba 3.5 (2010)

  https://lists.samba.org/archive/samba-announce/2017/000406.html

  - Déjà intégré dans Metasploit
- Preuve de concept: https://github.com/omri9741/cve-2017-7494
- En PowerShell: `powershell -c [System.IO.File]::Exists('\??\UNC\{srv}\pipe\/mod.so')`

Sudo, c'est fait pour réaliser des actions en root CVE-2017-1367

- Elévation de privilèges depuis sudo

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

OpenVPN, le rapport d'audit payé par l'OSTIF suite à un vote en 2016

- Principalement des dénis de service

  https://blog.quarkslab.com/security-assessment-of-openvpn.html

VLC, exécution de code à partir des sous-titres

- Affecte aussi Kodi, PopcornTime et StremIO
- Pleins d'autres vulnérabilités dont des heap overflow
  - CVE-2017-8310, CVE-2017-8311, CVE-2017-8312, CVE-2017-8313…

  http://blog.checkpoint.com/2017/05/23/hacked-in-translation/
- Appel à l'aide de JB (créateur de VLC) lors d'une RUMP à SSTIC

Failles / Bulletins / Advisories

Système (principales failles)

TrendMicro ServerProtect

- CSRF, XSS, téléchargement de mises à jours en HTTP, aucune vérification de l'intégrité des mises à jour…

  http://seclists.org/fulldisclosure/2017/May/91

Intel Active Management Technology (AMT) / CVE-2017-5689

- Si vos constructeurs vous ont dit ne pas être vulnérables, pensez à revérifier
- Chez DELL, une nouvelle liste a été publiée

Irsii, déréférencement d'un pointeur Null (CVE-2017-5193)

- Déni de service, pas d'exécution de code

  https://irssi.org/2017/05/12/fuzzing-irssi/

Oracle, une "Blind" XXE aboutissant à une exécution de code

https://www.ambionics.io/blog/oracle-peoplesoft-xxe-to-rce

Failles / Bulletins / Advisories

Réseau (principales failles)

Symantec Messaging Gateway, injection de commande sur le portail d'administration

- Sur un chemin passé en paramètre
  https://pentest.blog/unexpected-journey-5-from-weak-password-to-rce-on-symantec-messaging-gateway/

Cisco, vulnérabilité publique non corrigées

- Exécutions de code à distance CVE-2017-3881 sur le protocole CMP
  https://www.sourceclear.com/blog/Un-patched-for-months-could-Cisco-0-day-lead-to-another-round-of-WannaCry---SourceClear/

Juniper JunOS

- Contournement du firewall (SRX), Déni de service, élévation de privilèges sur l'interface d'administration
  https://cve.circl.lu/link/refmap.confirm/https%253A%252F%252Fkb.juniper.net%252FJSA10770

Failles / Bulletins / Advisories

Divers

Nintendo 3DS/2DS/New3DS, vulnérabilité dans le parseur RSA

- Permet de charger une bootrom auto-signée

  http://www.sighax.com/

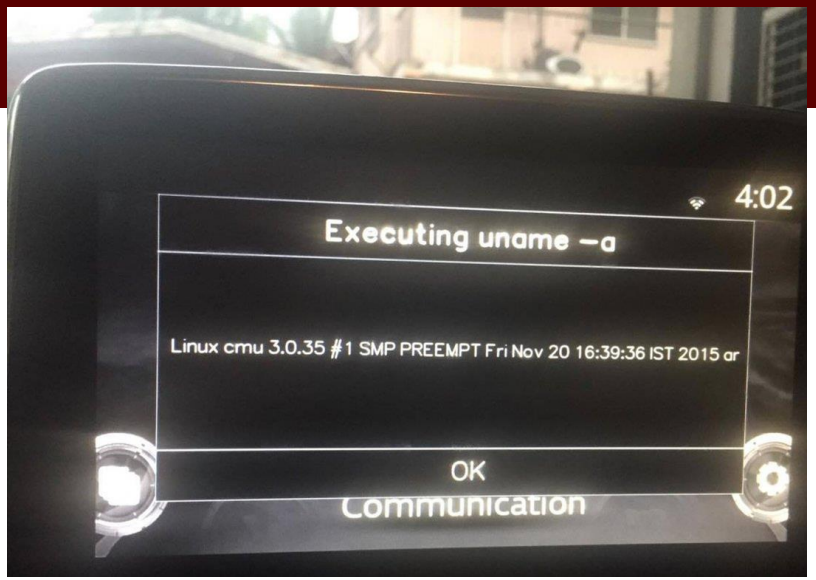
Sécurité des bases de données chiffrées

https://eprint.iacr.org/2017/468.pdf

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0



Voiture Mazda, injection de commande Linux

- A partir du port USB

  https://twitter.com/shipcod3/status/872003054995943424
  https://github.com/shipcod3/mazda_getInfo

CBM : Car Backdoor Maker

- Implant matériel à connecter à une voiture
- Permet d'envoyer des trames sur le bus CAN

  https://github.com/UnaPibaGeek/CBM

Une analyse technique des systèmes de triche pour les émission polluantes

https://www.ieee-security.org/TC/SP2017/papers/101.pdf

Rapport sur la vulnérabilité des sous-marins nucléaires Trident (UK)

- Peu d'informations précises

  https://media.scmagazine.com/documents/302/hacking_uk_trident_75338.pdf

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Persistance via Intel AMT pour les attaquants du groupe PLATINIUM

- Utilisation de la fonctionnalité SOL (Serial Over LAN) de la puce Intel ME pour contourner tous les mécanismes de sécurité de l'OS (firewall, ..)
- En gros, les PCs infectés communiquent entre eux sans passer par l'OS

  https://blogs.technet.microsoft.com/mmpc/2017/06/07/platinum-continues-to-evolve-find-ways-to-maintain-invisibility/?platform=hootsuite

Utilisation de réseaux neuronaux pour deviner des mots de passe

https://www.password-guessing.org/blog/post/cupslab-neural-network-cracking-manual/

Etude sur l'analyse de signaux chiffrés dans l'IoT

http://datworkshop.org/papers/dat16-final37.pdf

Vol de voiture Jeep en 2014

- Un gang de motards mexicains utilisait la base de données des clefs
- Pour les dupliquer

  https://www.documentcloud.org/documents/3760575-Jeep-Indictment.html

Piratages, Malwares, spam, fraudes et DDoS

DDoS

Cedexis, l'aiguilleur des CDN subit un DDoS

- Ébranlant ses infrastructures

  https://www.cedexis.com/blog/ddos-attack-details/

Piratages, Malwares, spam, fraudes et DDoS

Portes dérobées

Keylogger dans les ordinateurs HP

- Pilote enregistrant toutes les frappes claviers dans un fichier
- Fonctionnalité censée détecter les touches d'accès rapide (volume, mute...)

  http://www.zdnet.fr/actualites/faille-un-keylogger-decouvert-sur-certains-pc-hp-maj-39852364.htm
- Publication d'un correctif, désactivant la fonctionnalité, réactivable par la base de registre
  - SeeScanCode -> si mis à 1, alors la capture est activée
  - EnableLog -> si mis à 1, alors la capture est enregistrée dans un fichier.

  https://twitter.com/__ths__/status/863324677019770880/photo/1

Un RFID dans un CPU intel Core i9-7800X

https://www.heise.de/newsticker/meldung/RFID-Tag-im-Intel-Core-X-Prozessor-3730254.html

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

WannaCry, le vers exploitant les vulnérabilités de la NSA publiées en mars

- Exploitation de MS17-010 en réseau, pas de phishing
  - Peu de dégâts en France
  - Publication de correctifs pour XP et 2003
  - MalwareTech dépose le nom de domaine detectant les sandbox
    - Et arrête une partie des infections
- Divers PoC de MS17-010 ont été publiés
  - 64 bits pour Windows 8.1 et 2012 R2

  https://gist.github.com/worawit/074a27e90a3686506fc586249934a30e
- Un premier outil pour récupérer indirectement les clef : WannaKey

  https://github.com/aguinet/wannakey
- Version plus aboutie de Benjamin Delpy pour XP et 7 : WanaKiwi

  https://github.com/gentilkiwi/wanakiwi/releases
- Des sénateurs souhaitent que la NSA informe les autres agences de leurs vulnérabilités

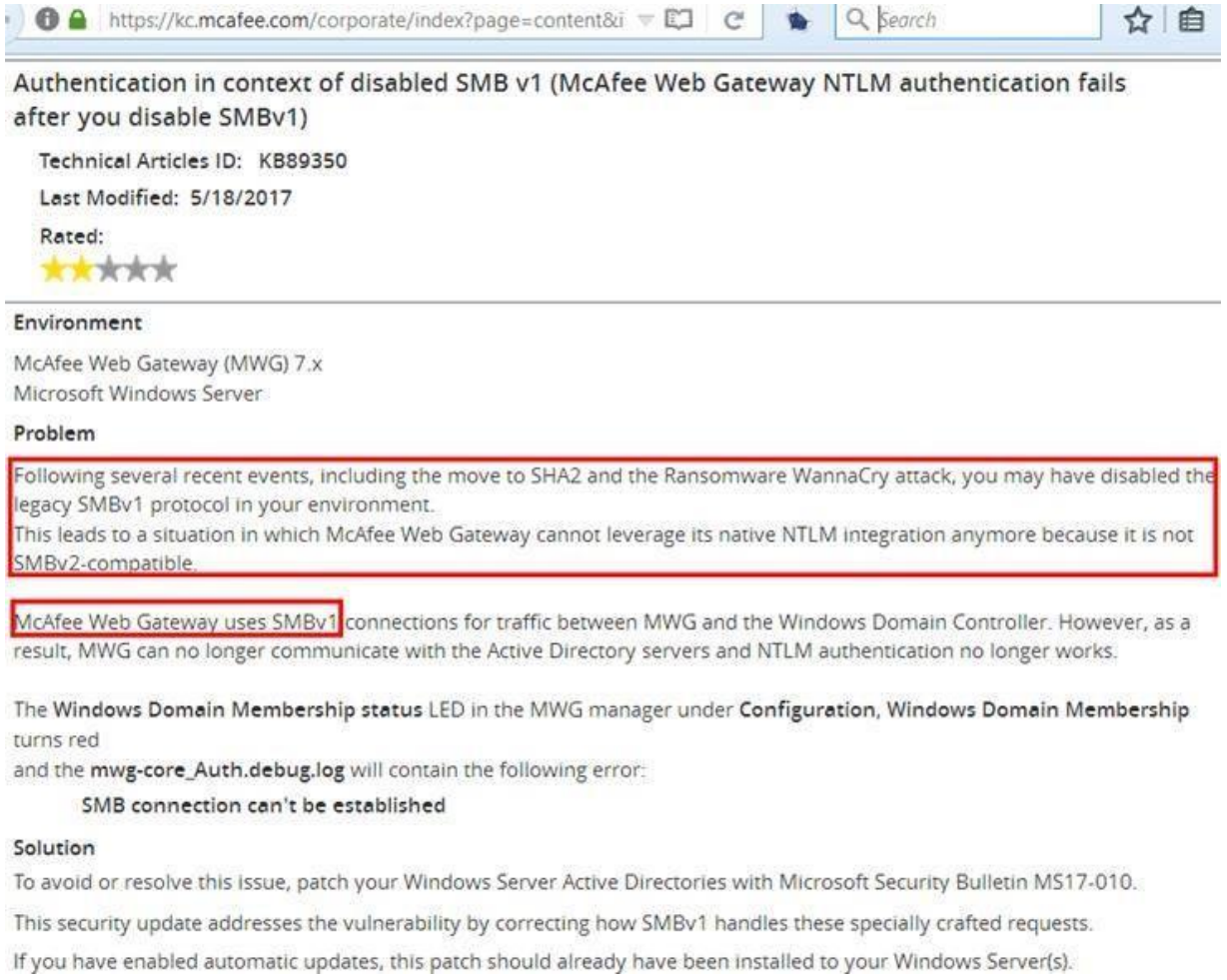
  http://www.reuters.com/article/us-cyber-attacks-nsa-legislation-idUSKCN18D2WK

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

WannaCry (suite)

- Désactiver SMB v1 chez McAfee? Difficile
  https://kc.mcafee.com/corporate/index?page=content&id=KB89350



https://kc.mcafee.com/corporate/index?page=content&i

Search

Authentication in context of disabled SMB v1 (McAfee Web Gateway NTLM authentication fails after you disable SMBv1)

Technical Articles ID: KB89350

Last Modified: 5/18/2017

Rated:

Environment

McAfee Web Gateway (MWG) 7.x
Microsoft Windows Server

Problem

Following several recent events, including the move to SHA2 and the Ransomware WannaCry attack, you may have disabled the legacy SMBv1 protocol in your environment.
This leads to a situation in which McAfee Web Gateway cannot leverage its native NTLM integration anymore because it is not SMBv2-compatible.

McAfee Web Gateway uses SMBv1 connections for traffic between MWG and the Windows Domain Controller. However, as a result, MWG can no longer communicate with the Active Directory servers and NTLM authentication no longer works.

The **Windows Domain Membership status** LED in the MWG manager under **Configuration**, **Windows Domain Membership** turns red
and the **mwg-core_Auth.debug.log** will contain the following error:

SMB connection can't be established

Solution

To avoid or resolve this issue, patch your Windows Server Active Directories with Microsoft Security Bulletin MS17-010.

This security update addresses the vulnerability by correcting how SMBv1 handles these specially crafted requests.

If you have enabled automatic updates, this patch should already have been installed to your Windows Server(s).

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

WannaCry (suite)

- Désactiver SMB v1 sur les imprimantes Konica ? Impossible.
  https://kc.mcafee.com/corporate/index?page=content&id=KB89350

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Booz Allen Hamilton stocke des données classifiées sur un bucket S3 public

- Données classifiées “top secret” accessibles publiquement sur Amazon S3
- Relatives aux drones et programmes satellites militaires

https://arstechnica.com/security/2017/05/defense-contractor-stored-intelligence-data-in-amazon-cloud-unprotected/

Piratages, Malwares, spam, fraudes et DDoS

Malwares

Les malwares utilisent de plus en plus des plate-formes collaboratives…

- Comme canal de contrôle-commande

  http://blog.trendmicro.com/trendlabs-security-intelligence/using-third-party-apis-cc-infrastructure/

Piratages, Malwares, spam, fraudes et DDoS
SCADA

Caméras Foscam

- Compte par défaut caché, comptes en dur, service telnet caché
- Injection de commande dont non authentifié, problèmes d'autorisations, mauvaises restrictions d'accès,

  http://images.news.f-secure.com/Web/FSecure/%7B43df9e0d-20a8-404a-86d0-70dcca00b6e5%7D_vulnerabilities-in-foscam-IP-cameras_report.pdf

SCADA et Cloud

- Une analyse de la sécurité des applications permettant de piloter son installation à distance

  https://www.slideshare.net/dark_k3y/s4xeurope-scada-mobile-in-the-iot-age

CrashOverride

- Framework de malware utilisé dans l'attaque de l'Ukraine en décembre 2016
- Spécifiquement créée pour les attaques sur les infrastructures électriques, via le protocole OPC et IEC 104
- Rapport très détaillé

  https://dragos.com/blog/crashoverride/CrashOverride-01.pdf

Piratages, Malwares, spam, fraudes et DDoS

Hardware / IoT

Sécurité des Pacemaker

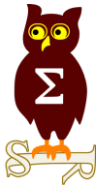
- Prptocole radio non sécurisé
- Rappelez vous, en 2013, Dick Cheney, vice président américain avait désactivé le sien

  http://blog.whitescope.io/2017/05/understanding-pacemaker-systems.html

9% des constructeurs d'appareils médicaux testent pas la sécurité des produits

- 17% font des efforts pour sécuriser leurs produits

  http://www.bbc.com/news/technology-40042584



Nouveautés, outils et techniques

Frida 10.0.12

- Avec le support des class dynamique sous Android

  https://www.frida.re/

Retrouver les mots de passe WiFi sous Windows 10

```
> netsh wlan show profiles
> netsh wlan show profile name=<profile> key=clear
```

https://twitter.com/x0rz/status/873559877217648640?s=09

Exécution de code R sur MS SQL Server 2016

https://pastebin.com/zBDnzELT

Mimikatz, changer son mot de passe sans respecter les politiques de complexité

- En collaboration avec Vincent Le Toux

  https://github.com/vletoux/NTLMInjector
  https://github.com/gentilkiwi/mimikatz/releases/tag/2.1.1-20170608

Pentest

Techniques & outils

MailSniper, pour identifier les BAL Exchange accessibles

https://www.blackhillsinfosec.com/?p=5871

Désactivation discrète de la journalisation d'événement Windows

https://github.com/hlldz/Invoke-Phant0m

PRET : Printer Exploitation Toolkit

https://github.com/RUB-NDS/PRET

Exécuter du PowerShell sans utiliser powershell.exe

- Permet à l'attaquant d'être plus discret
- Utilisation de MSBuild pour générer un fichier .cmd

  https://github.com/Mr-Un1k0d3r/PowerLessShell

Pentest

Techniques & outils

Outil de création de macro Office malveillantes

https://github.com/Shellntel/luckystrike

Ensemble de techniques pour l'évasion des environnements Citrix XenApp

https://www.pentestpartners.com/security-blog/breaking-out-of-citrix-and-other-restricted-desktop-environments/

Utiliser Slack comme canal de contrôle-commande

https://github.com/bkup/SlackShell

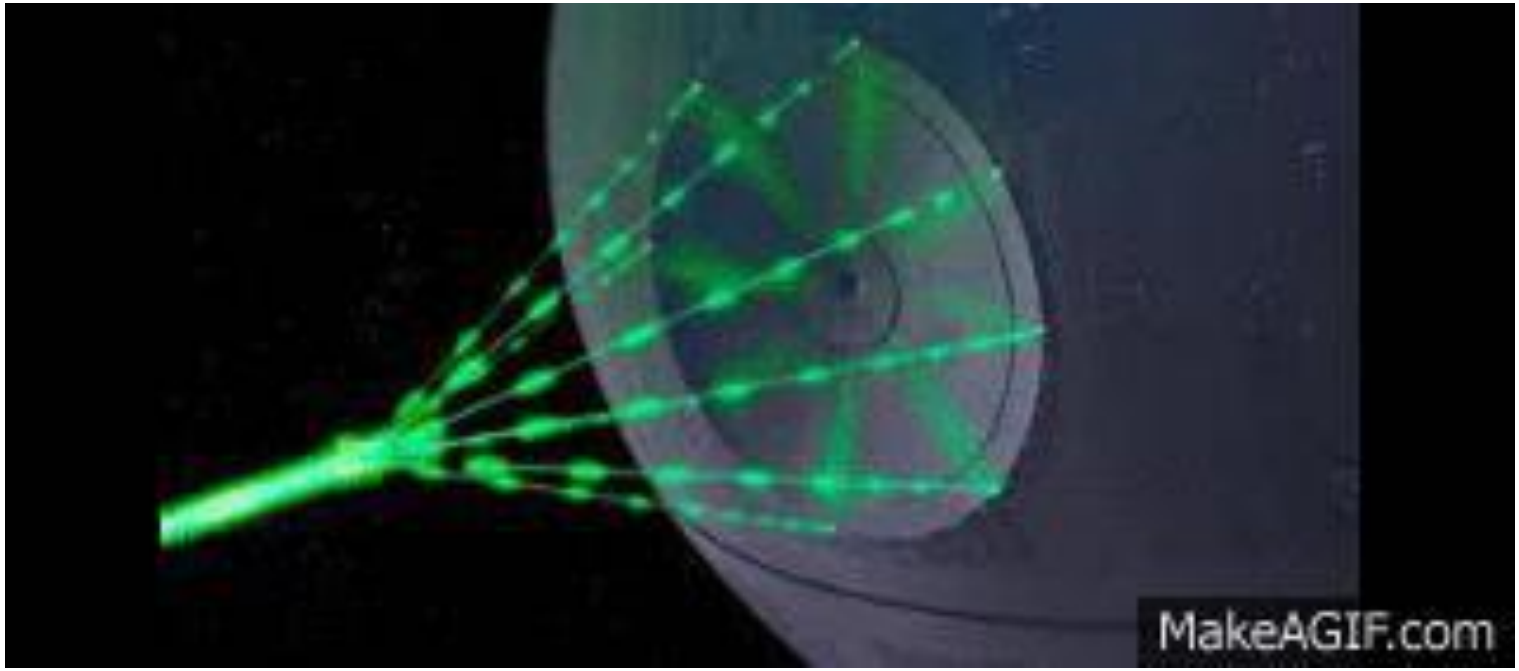
Kerberom pour le Kerberoasting

https://github.com/Synacktiv/kerberom

Death Star

- Outil permettant d'automatiser la compromission d'un domaine Active Directory
- Lance une analyse BloodHound
- Automatise les actions nécessaires à l'atteinte des privilèges "admin de domaine"

https://byt3bl33d3r.github.io/automating-the-empire-with-the-death-star-getting-domain-admin-with-a-push-of-a-button.html



Le NIST publie un guide sur le contrôle des applications par liste blanche

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf

Analyse de documents PowerPoint malveillants

- Avec des outils open-source
- Exemple sur les dernières campagnes abusant du “mouse over”

https://blog.nviso.be/2017/06/07/malicious-powerpoint-documents-abusing-mouse-over-actions/

Cartographie des IMSI catchers utilisés

- Travail universitaire basé sur un “war driving” mesurant :
  - la puissance, la fréquence et les propriétés des BTS

https://seaglass.cs.washington.edu/

Création d’un HoneyPot SMB

https://doublepulsar.com/eternalpot-lessons-from-building-a-global-nation-state-smb-exploit-honeypot-infrastructure-3f2a0b064ffe

Nouveautés (logiciel, langage, protocole...)

Open Source

Utiliser des applications sans OS sur Google Cloud

- Permet de n’inclure que les binaires nécessaires à l’application, pour réduire la surface d’attaque

  https://github.com/GoogleCloudPlatform/distroless

Business et Politique

Droit / Politique

France

Contrat Microsoft avec la Défense, une sénatrice y est opposée

- Et demande la suspension du contrat

  https://www.nextinpact.com/news/104363-contrat-open-bar-microsoft-la-defense-senatrice-reclame-suspension-negociations.htm

Mooc SecNumacadémie de l'ANSSI

- plus de 20 000 inscrits

  https://secnumacademie.gouv.fr/

Droit / Politique
International

[hors sujet, mais il faut bien rire en ces temps difficiles]

… ca ose tout, c'est même à ca qu'on les reconnait

http://www.news.com.au/world/europe/british-politician-wants-death-penalty-for-suicide-bombers/news-story/0eec0b726cef5848baca05ed1022d2ca

L'Angleterre souhaiterait mettre des portes dérobées dans la crypto

- Fuite de documents présentant le plan visant les opérateurs pour surveiller Internet

https://www.theregister.co.uk/2017/05/04/uk_bulk_surveillance_powers_draft/

Droit / Politique
International

Facebook

- Europe, amende de 110 millions d'euros suite au rachat de Whatsapp
  - Facebook disant ne pas pouvoir croiser les bases

  http://www.ouest-france.fr/high-tech/facebook/l-europe-inflige-une-amende-facebook-pour-le-rachat-de-whatsapp-5000249
- Idem en Italie, avec une amende de 3 millions d'euros

  http://www.lemonde.fr/pixels/article/2017/05/16/whatsapp-condamne-en-italie-pour-son-partage-de-donnees-avec-facebook_5128277_4408996.html

USA, les autorités peuvent demander vos comptes des réseaux sociaux

https://www.usatoday.com/story/tech/news/2017/06/01/us-now-can-ask-travelers-facebook-twitter-handles/102393236/

Contourner la censure en Russie ?

- Possible, Youporn a fourni des comptes gratuits aux autorités

  https://tjournal.ru/44867-rozigrish-premium-podpisok-na-pornhub-ot-roskomnadzora

Business

France

Ami RSSI, avec GDPR, ton salaire augmente !

- 6 à 10 ans d'expérience = 70 à 100K/an
- > 10 ans d'expérience = 150K/an avec 30 % de variable
- Dans certaines grandes entreprises, cela atteint le million

  http://www.silicon.fr/avant-le-gdpr-le-salaire-des-rssi-flambe-176133.html

Business
International

BugBounty Microsoft pour Hyper-V, jusqu'à $150,000

- Pour une évasion de machine virtuelle fonctionnelle, sinon c'est $100,000
  https://technet.microsoft.com/en-us/security/mt784431?f=255&MSPPError=-2147217396

Conférences

Conférences

Passées

- SSTIC - 7 au 9 juin 2017 à Rennes
  - Excellent CR : http://www.n0secure.org/2017/06/sstic-2017-j1.html

A venir

- Nuit du Hack - 24-25 juin 2017 à Paris (Eurodisney)
- BeeRump - 22 juin à Paris (Epita)

Divers / Trolls velus

Divers / Trolls velus

Un émulateur Android dans un navigateur

- Solution en mode SaaS, de l'AaaS ? Android as a Service

  https://aic-project.github.io/

ElcomSoft récupère les notes effacées dans iCloud

- Jusqu'à 30 jours après effacement

  https://blog.elcomsoft.com/2017/05/we-did-it-again-deleted-notes-extracted-from-icloud/

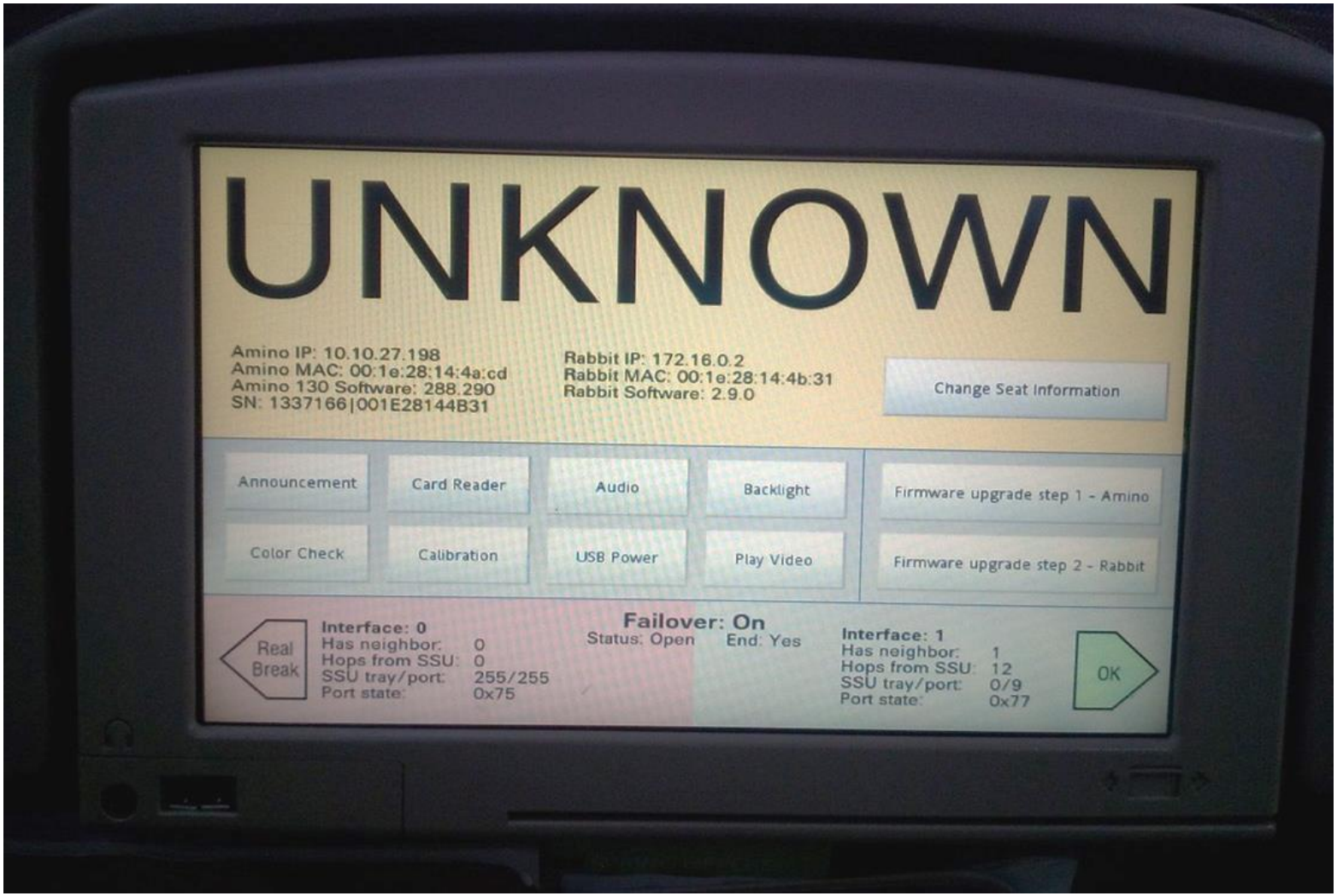
Vos bases de données sont sécurisées… pas les nôtres

https://twitter.com/x0rz/status/865515940183658497/photo/1

Divers / Trolls velus

Vous êtes dans un avion, quand soudain…

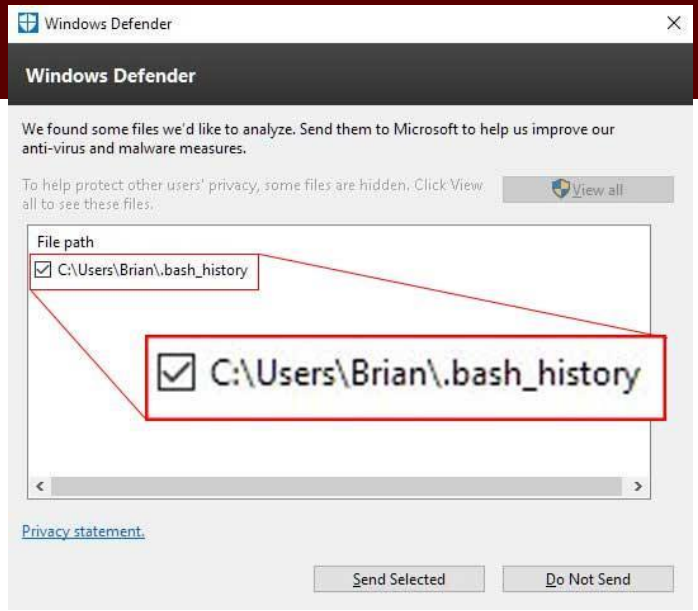
https://twitter.com/gwendallecoguic/status/867666189023162368?refsrc=email&s=11



Divers / Trolls velus

Windows Defender n’aime pas le monde Unix

https://twitter.com/bbaskin/status/870707089282183169/photo/1



Office 2016, cette tâche planifiée toutes les heures

- OfficeBackgroundTaskHandlerRegistration se lance toutes les heures et apparait un quart de seconde !!!

https://answers.microsoft.com/en-us/msoffice/forum/msoffice_officeinsider-mso_win10/officebackgroundtaskhandlerregistration-flashes-a/2600497e-78e4-41a1-9040-461cd2c3ea13

Panne de Windows 7 et 8.1 "à l'ancienne"

- Plantage du système en cas d’accès à `c:\$M F T\123`
- Similaire aux vieux c:\con\con , c:\nul\nul … de Windows 95

https://habrahabr.ru/company/aladdinrd/blog/329166/

Divers / Trolls velus

Pourquoi les hackeurs réussissent à pirater ?

- A cause de mises à jour manquant ou d'erreurs humaines

  https://www.undernews.fr/reseau-securite/intrusions-informatiques-f-secure-revele-les-deux-raisons-pour-lesquelles-les-pirates-parviennent-a-leur-fins.html

Crowdfunding pour l'achat des vulnérabilités de ShadowBroker

- Vulnérabilités vendues $24K
- Projet abandonné

  https://pastebin.com/raw/guccKU2F

  https://pastebin.com/raw/6VJ7XcM0
- Inspiré du crowdfunding par les attaquants de l'épisode NoLimitSécu d'avril 2017 ?

  https://www.nolimitsecu.fr/securite-predictive/

Divers / Trolls velus

Systemd, en cas d'impossibilité d'accès au DNS, "fallback" sur les DNS de Google

https://twitter.com/PowerDNS_Bert/status/873863741925978113

iOS, accès au NFC en dehors d'ApplePay

https://www.youtube.com/watch?v=fD7sBp2figc

Une comparaison des différents VPN

- En particulier, ceux qui acceptent Bitcoin et annoncent ne pas coopérer avec les autorités

https://thatoneprivacysite.net/vpn-comparison-chart/

Déverrouiller un Samsung Galaxy S8 avec une photo et une lentille

- Avec une simple photo prise en infra rouge (avec un banal appareil photo numérique) et une lentille de contact posée sur la photo

https://media.ccc.de/v/biometrie-s8-iris-en

SSTIC 2017, le compte-rendu de news0ft

- Made in news0ft

http://news0ft.blogspot.fr/2017/06/un-compte-rendu-alternatif-du-sstic-2017.html

Divers / Trolls velus

Selon l’avocat américain Jay Leiderman, Signal est compromis !!!

https://twitter.com/jayleidermanlaw/status/872849686914191363

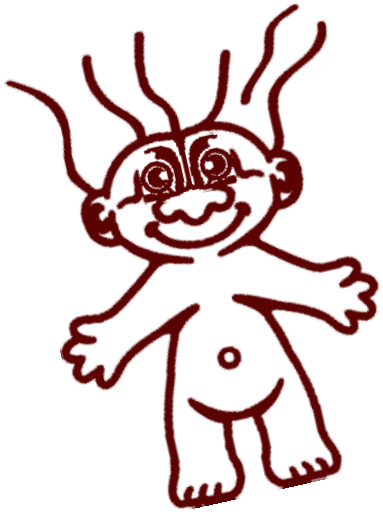
- N’est-ce pas plutôt l'intelligence qui est compromise ?
- Le protocole Signal a été vérifié formellement

  https://eprint.iacr.org/2016/1013.pdf

Wardriving avec un IMSI catcher

- Attention à la puissance du signal et la santé du conducteur

  https://seaglass.cs.washington.edu/



Le grand maître
archi-mage
du Troll
du chaos
...

Divers / Trolls velus

Quand Putin parle des hackeurs Russes

- La vidéo est du pur caviar

<<Les hackeurs sont des gens libres. Ils sont comme les artistes qui se lèvent le matin de bonne humeur et commencent à peindre.
Les Hackeurs sont pareil. Ils se lèvent le matin, ils lisent des avancées sur des affaires internationales et s'ils sont patriotes, alors ils essaient de contribuer d'une façon qu'ils considèrent juste contre ceux qui ont de mauvaises choses à dire sur la Russie>>
<< Les hackeurs ne peuvent pas influencer de façon importante des élections d'un autre pays>>

https://www.rferl.org/a/russia-putin-patriotic-hackers-target-critics-not-state/28522639.html

Prochains rendez-vous de l’OSSIR

Prochaine réunion

- Mardi 11 juillet 2017

After Work

- En septembre

Prochaines réunions

Afterwork de Mai -> Gros succès

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous