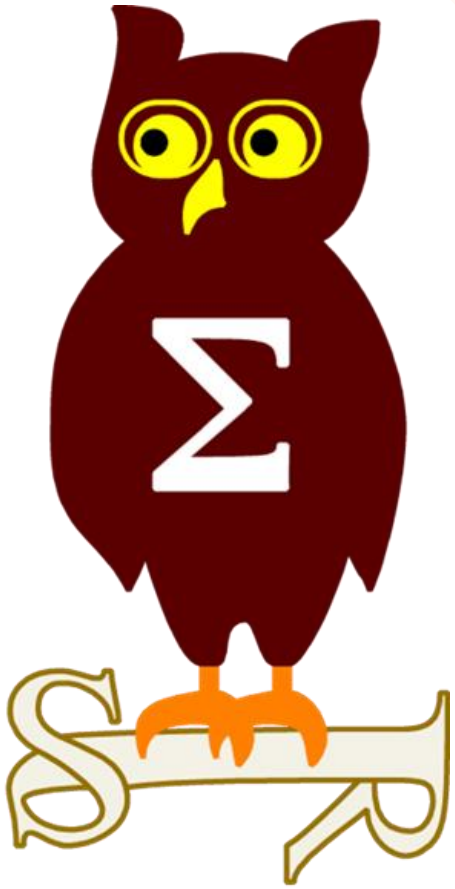
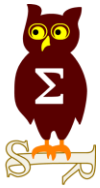


Revue d'actualité

21/02/2017

Préparée par

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



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories

Microsoft - Avis

MS17-001 Vulnérabilité dans Edge (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows 10
- Exploit:
  - Contournement du "Cross Domain Policy", à partir de about:blank
    - Exploité dans la nature
- Crédits:
  - ?

MS17-002 Vulnérabilité dans Office (1 CVE) [Exploitabilité 1]

- Affecte:
  - Office 2007, 2010, 2013, 2013RT, 2016, Mac 2011 et 2016
  - Sharepoint 2010, 2013
- Exploit:
  - Corruptions de mémoire aboutissant à une exécution de code
- Crédits:
  - Tony Loi de Fortinet’s FortiGuard Labs (CVE-2017-0003)

Failles / Bulletins / Advisories

Microsoft - Avis

MS17-003 Vulnérabilités dans Adobe Flash Player (13 CVE) [Exploitabilité 2,2,2,2,2,2,2,2,2,2,2,2,2]

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

MS17-004 Security Update for Local Security Authority Subsystem Service (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportées)
  - Remplace MS16-149, KB3204808
- Exploit:
  - Déni de service dans LSASS lors de l'authentification
- Crédits:
  - Laurent Gaffie (CVE-2017-0004)
  - Nicolás Economou de Core Security (CVE-2017-0004)

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**

Pas de correctif pour janvier 2017

- Ou arrêt du fonctionnement des mises à jours 😊

Failles / Bulletins / Advisories

Microsoft - Advisories et Revisions

4010983

- V1.0 Recommandations pour les développeurs pour corriger leurs applications concernant une vulnérabilité de déni de service d'ASP.NET Core

3214296

- V1.0 Recommandations pour les développeurs face à une vulnérabilité .Net d'élévation de privilèges en cas d'utilisation d'un token signé avec une clef symétrique avec Microsoft.IdentityModel.Tokens

Failles / Bulletins / Advisories

Microsoft - Autre

"Security Bulletin" deviendra "Security Updates Guide"

- Moteur de recherche par CVE, par produit…
- Accès par l'API RESTful

https://blogs.technet.microsoft.com/msrc/2016/11/08/furthering-our-commitment-to-security-updates/

Bulletin de février décalé

- Risque de panne non résolu dans les temps

https://blogs.technet.microsoft.com/msrc/2017/02/14/february-2017-security-update-release/

Windows 10 pour CPU ARM et donc smartphone

- Cela repose la question de l'avenir du poste de travail

http://www.theverge.com/2016/12/8/13881930/microsoft-turn-a-phone-into-a-pc-arm-continuum

Failles / Bulletins / Advisories

Microsoft - Autre

Le Javascript Zombie pour Internet Explorer 11

- Grâce à la création d'un objet ActiveX

  https://www.brokenbrowser.com/zombie-alert/

Code d'exploitation pour la vulnérabilité SMB "Tree Connect Response"

- Déni de service uniquement (pour l'instant)
- Pour retrouver nos années 2000, il ne reste qu'à coder un vers l'exploitant 😂

  https://github.com/lgandx/PoC/tree/master/SMBv3%20Tree%20Connect

Déni de service fonctionnaant de NT 3.51 à Windows 10

- A partir des API NtCreateProfile and NtCreateProfileEx ✌🏻

  http://www.geoffchappell.com/studies/windows/km/ntoskrnl/api/ex/profile/bugdemo.htm

Failles / Bulletins / Advisories

Système (principales failles)

Elévation de privilège locale dans OpenSSH

- Problème de gestion des privilèges lors de la création d'un tunnel SSH (option « -L »)

  https://www.exploit-db.com/exploits/40962/

Bash, exécution de code à l'auto-complétion (CVE-2017-5932)

- Si un fichier spécialement nommé existe dans le répertoire courant

  https://github.com/jheyens/bash_completion_vuln

Oracle, un énorme bulletin corrigeant 270 failles

- 5 pour Oracle Database
- 17 pour Java
- 18 pour Oracle Fusion
- 27 pour Oracle MySQL
- 32 pour Oracle E-Business Suite
- 37 pour Oracle FLEXCUBE

  https://www.nextinpact.com/news/102974-oracle-enorme-bulletin-securite-trimestriel-270-failles.htm

VirtualBox, élévation de privilèges

- Lors du téléchargement d'Extention Pack, sous forme d'archive TAR préservant les permissions

  https://tech.feedyourhead.at/content/privilege-escalation-in-virtualbox-cve-2017-3316

Failles / Bulletins / Advisories

Réseau (principales failles)

Déni de service sur Bind

https://kb.isc.org/article/AA-01453

TicketBleed, récupération de portion de RAM sur F5 BIG-IP

- Fuite de 31 octets par requête
- Exploit : https://www.exploit-db.com/exploits/41298/

  https://filippo.io/Ticketbleed/

Cisco FirePower, ajout d'un utilisateur (FirePower=firewall Next Generation de Cisco)

- Ajout après authentification

  https://www.exploit-db.com/exploits/41041/

Extension de navigateur Cisco WebEx, exécution de code

- Utilisation de l'API nativeMessaging et de sa méthode GpcInitCall
  - Exécution de code à la visite d'une page web

  https://bugs.chromium.org/p/project-zero/issues/detail?id=1096
- "Correction" par l'ajout d'une liste blanche de site
  - Contournable si l'on a une XSS sur webex.com, ce qui est le cas

  https://bugs.chromium.org/p/project-zero/issues/detail?id=1100

Failles / Bulletins / Advisories

Réseau (principales failles)

Porte dérobée dans les équipements réseau Meraki

- Encore un compte caché
- Exécution de commande sur le portail web d'administration

```
http://IP-BOITIER/run_shell.cgi
mf_test:$1$$ZbKKXKQQpKjTbTPeMZwk.. -> correspondant au mot de passe mf_test
adminn$$G7.z4WDwEF7FvCK4H6cah/

meraki:MvCWFGH8/CrXM:0:0:meraki:/tmp:/usr/bin/logincheck
mf:$1$$CgXoxAaejQmJWRkDiclb6/:0:0:meraki:/tmp:/usr/bin/mf_logincheck
```

https://research.trust.salesforce.com/Meraki-RCE-When-Red-Team-and-Vulnerability-Research-fell-in-love.-Part-1/
https://research.trust.salesforce.com/Meraki-RCE-When-Red-Team-and-Vulnerability-Research-fell-in-love.-Part-2/

Qnap, des tas de vulnérabilités

http://seclists.org/fulldisclosure/2017/Feb/2
http://0day.today/exploit/27040

Routeur D-Link, encore des tas de vulnérabilités

- Portes dérobées, PIN WPS codé en dur ou faible, injection de commande…

http://seclists.org/fulldisclosure/2017/Feb/8

Routeurs Juniper SRX, shell root

- A partir de 2 petites commandes
  - request system software et partition

http://securityaffairs.co/wordpress/55252/hacking/juniper-srx.html

Failles / Bulletins / Advisories

Antivirus

Trend Micro - Control Manager 6.0, contournement de l'authentification

https://remoteawesomethoughts.blogspot.fr/2017/01/trend-micro-control-manager-60.html

- Ce n'est rien à côté des 194 vulnérabilités exploitable à distance

  http://www.forbes.com/sites/thomasbrewster/2017/01/25/trend-micro-security-exposed-200-flaws-hacked/#2c58072455d6

C'est le tour de TrendMicro!

- Appliance virtuelle InterScan web
- Possibilité de rooter l'appliance via une requête web d'un utilisateur authentifié
- Absence de contrôle d'accès permettant à tout utiliser de changer le mot de passe de l'utilisateur "root"

  http://seclists.org/fulldisclosure/2017/Feb/30

  http://seclists.org/fulldisclosure/2017/Feb/31

  http://seclists.org/fulldisclosure/2017/Feb/32

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Compromission de macOS à partir de Macro Office

- Automatisation de la création de macro avec Empire, Empyre et Metasploit
- Technique d'Empire trouvée dans la nature

https://objective-see.com/blog/blog_0x17.html

Des hackeurs Russes font la rétro conception de l'algorithme de machines à sous

- Ils filmaient des essaies au bandit manchot, qu'ils envoyaient à Saint Petersbourg
  - Une douzaine de combinaisons suffisaient pour prédire la suivante
- En retour, le smartphone vibrait au moment exact où appuyer pour gagner
- Le groupe semble écumer les casinos depuis 2014

http://www.01net.com/actualites/ce-gang-de-hackers-siphonne-des-machines-a-sous-avec-de-simples-smartphones-1098976.html

Rétro-ingénierie et exploitation d'un HSM

https://fotisl.com/reverse/utimaco/recon2017/#/

Attaquer les drones avec du bruit

- Perturbation du gyroscope

https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/son

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

La sécurité des imprimantes, encore mise à mal

- Publication d'outils allant de l'exécution de code à la destruction

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

- Et du Wiki associé

  http://hacking-printers.net/wiki/index.php/Main_Page

Un hackeur pirate 150 000 imprimantes

- Avec un script automatisé

  https://www.bleepingcomputer.com/news/security/a-hacker-just-pwned-over-150-000-printers-left-exposed-online/

Les nouveaux CPU d'Intel incorporent un debugger accessible en USB 3.0

- Équivalent à un JTAG mais en USB 3.0
- Heureusement désactivé chez la plupart des constructeurs

  http://blog.ptsecurity.com/2017/01/intel-debugger-interface-open-to.html

Piratages, Malwares, spam, fraudes et DDoS

DDoS

La vérité sur le vers Mirai

- Enquête de Brian KREBS (victime en 2016)
- Le vers a été créé par des gamins américains voulant faire de l'argent avec l'écosystème du jeu vidéo Minecraft et à l'ego surdimensionnés !

  https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/
- Une version dédiée Windows fait son apparition

  https://www.bleepingcomputer.com/news/security/mirai-gets-a-windows-version-to-boost-distribution-efforts/

Détecter les dénis de services dans le code d'application

- Par analyse de code statique avec des expressions régulières

  https://arxiv.org/pdf/1701.04045v1.pdf

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Piratage des enregistreurs des caméras de Washington

- Demande de rançon
- Pas de paiement et réinstallation des systèmes, mais perte de 48h de vidéo
  - Dont l'investiture de Trump

https://www.washingtonpost.com/local/public-safety/hackers-hit-dc-police-closed-circuit-camera-network-city-officials-disclose/2017/01/27/d285a4a4-e4f5-11e6-ba11-63c4b4fb5a63_story.html

Fuite de 900Go de données de Cellebrite

- Provenant de serveurs web de Cellebrite.
- Les outils ont été déchiffrés et désobfusqués, on y retrouve (entre autre):
  - Limera1n de jailbreak d'iOS développé par Geohot (Georges Hotz)
  - L'outil QuickPwn

https://motherboard.vice.com/en_us/article/hacker-steals-900-gb-of-cellebrite-data

Hitachi Payment Service en Inde, vol de 3,2 millions de numéros de CB

- Intrusion vers 2016Q2-Q3, peut-être à partir d'un simple ATM

http://www.gadgetsnow.com/tech-news/3-2-million-debit-cards-hacking-in-india-hitachi-owns-up-to-security-flaw/articleshow/57060029.cms

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Giulio et Francesca Maria OCCHIONERO ont piraté plusieurs politiciens Italiens

- Dont Mario DRAGHI (BCE), Matteo RENZI (ex-1er ministre),Gianfranco RAVASI (Cardinal), Mario MONTI (ex- ministre de l'économie)...
- Malware « Evil Pyramid » écrit par Giulio
- Compromission par harponnage / spear phishing

http://www.nextquotidiano.it/giulio-francesca-occhionero-cyberspionaggio/

https://securelist.com/blog/incidents/77098/the-eyepyramid-attacks/

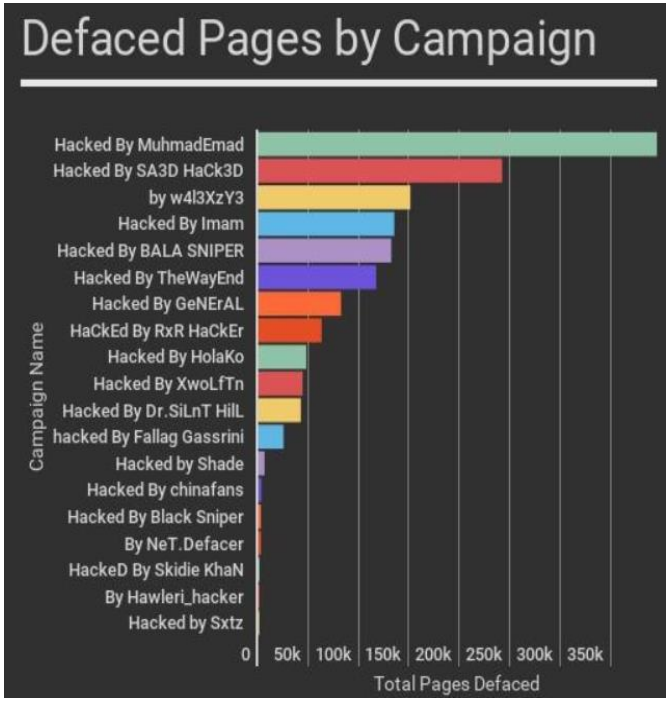
http://www.pandasecurity.com/mediacenter/news/eye-pyramid-cyber-espionage-italy/

Injection de contenu dans Wordpress

- Elévation de privilège via l'API REST
- Corrigé dans la version 4.7.2
  - Près de 1,5 millions de sites piratés

https://threatpost.com/1-5m-unpatched-wordpress-sites-hacked-following-vulnerability-disclosure/123691/

https://blog.sucuri.net/2017/02/content-injection-vulnerability-wordpress-rest-api.html



Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Shadow Broker, vend les outils de la NSA à la découpe

- Rappel : outils datant de 2013 “au mieux”
- Outils et 0-days ciblant principalement Windows
- Prix entre 10 et 650 bitcoins

http://www.01net.com/actualites/les-outils-de-piratage-windows-de-la-nsa-en-vente-sur-internet-1080103.html

Des pirates bloquent des serrures d’un hotel et demandent une rançon

- Hotel de luxe autrichien : Romantik Seehotel Jaegerwirt
- Ils ont payé la rançon de 1 500 euros

http://www.numerama.com/tech/228189-ransomware-des-pirates-bloquent-les-serrures-electroniques-dun-hotel-de-luxe.html

Après MongoDB, c’est au tour des bases ElasticSearch d’être rançonnées

- Plus de 600 instances piratée, pour des rançons de 0,2 bitcoins

http://blog.ptsecurity.com/2017/01/intel-debugger-interface-open-to.html

Piratages, Malwares, spam, fraudes et DDoS

Malwares

Un document Office avec une Macro signée

- La Macro est sur Pastebin

  http://pastebin.com/ck9y4Fsr

  https://twitter.com/JohnLaTwC/status/827319604674334720/photo/1

Dridex est de retour

- Avec une contournement de l'UAC basé sur recdisc.exe

  https://www.flashpoint-intel.com/blog-dridex-banking-trojan-returns/

Piratages, Malwares, spam, fraudes et DDoS
SCADA

Un administrateur IT condamné pour piratage du SI industriel de son ancien employeur

- Intrusions répétées via le VPN
- Dégâts estimés à 1 million de dollars

https://www.justice.gov/usao-mdla/pr/former-systems-administrator-sentenced-prison-hacking-industrial-facility-computer

L'ENISA publie un guide de sécurisation des communications pour les SI industriels

https://www.enisa.europa.eu/publications/ics-scada-dependencies

Firewall mGuard de Phoenix Contact

- Mot de passe admin redevient celui d'usine après une mise à jour

Contournement d'authentification sur Siemens SIMATIC Logon

- Authentification via nom d'utilisateur seulement…
- CVSS 9.0

https://ics-cert.us-cert.gov/advisories/ICSA-17-045-03

Vulnérabilités dans les switch Hirschmann GECKO

- Lors d'une mise à jour, la configuration actuelle, incluant les hash des mots de passe, est sauvegardée dans un répertoire accessible sans authentification

https://ics-cert.us-cert.gov/advisories/ICSA-17-026-02

Piratages, Malwares, spam, fraudes et DDoS

Hardware / IoT

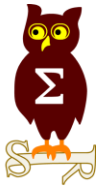
L’ENISA publie un panorama des menaces sur les attaques matérielles

https://www.enisa.europa.eu/publications/hardware-threat-landscape

Analyse du protocole Z-Wave et des possibilités de rejeu

- L’auteur n’a pas réussi, et ne sait pas pourquoi
- Cependant bonne intro à Z-Wave et au SDR en général

https://www.sans.org/reading-room/whitepapers/internet/security-assessment-z-wave-devices-replay-attack-vulnerability-37242



Nouveautés, outils et techniques

Crypto
Divers

Google devient sa propre autorité de certification

- Précédemment signés par GeoTrust Global CA
- Les sites et applications Google seront signés par Google Trust Services et Google Services

https://security.googleblog.com/2017/01/the-foundation-of-more-secure-web.html

Prim'X, enfin le succès !

- Editeur de ZoneCentral et Cryhod

http://www.lepoint.fr/high-tech-internet/cryptologie-la-start-up-francaise-que-tout-le-monde-s-arrache-24-01-2017-2099588_47.php

SHA1-160 bits, c'est bientôt fini dans Chrome

https://www.chromium.org/Home/chromium-security/education/tls/sha-1

Pentest
Techniques & outils

Exécution de commandes sur MSSQL sans xp_cmdshell

- Via la définition d'une procédure stockée en utilisant CLR (Custom Language Runtime)

  http://sekirkity.com/command-execution-in-sql-server-via-fileless-clr-based-custom-stored-procedure

Outil d'audit et de pentest MongoDB

- #ProTip : Ne pas exposer une base de données sur Internet sans authentification

  https://github.com/stampery/mongoaudit

Universal Radio Hacker

- Logiciel pour la rétro-ingénierie de protocoles sans fil

  https://github.com/jopohl/urh

Chassez l'admin du domaine

- Avec PowerView 2.0

  http://www.harmj0y.net/blog/penetesting/i-hunt-sysadmins/

Sitch, un RAT en python pour Windows, Linux et macOS

https://github.com/nathanlopez/Stitch

Pentest
Techniques & outils

Création de package Debian malveillants

https://github.com/ChaitanyaHaritash/kimi

Bella, outil de post-exploitation (RAT) pour macOS

https://github.com/manwhoami/Bella

RootHelper, aide à l'élévation de privilège sur Linux

- Rassemble plusieurs outils dont Linux_Exploit_Suggester

https://n0where.net/linux-privilege-escalation-roothelper/

Dernière présentation de @gentilkiwi à BlueHat Israël

- On parle de pkinit mustiness
- et beaucoup de kékéo, de kerberos et de PKI

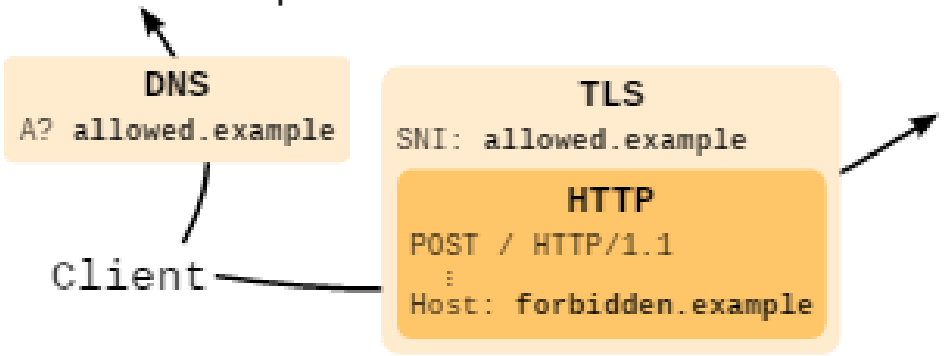
https://onedrive.live.com/view.aspx?resid=A352EBC5934F0254!3316&ithint=file%2cpptx&app=PowerPoint

Mouvement latéral avec DCOM, partie 2

https://enigma0x3.net/2017/01/23/lateral-movement-via-dcom-round-2/

“Domain Fronting”

- Technique consistant à faire croire à un proxy que l’on s’adresse à un domaine de confiance (ex: google.com) alors que l’on s’adresse à un autre domaine, mais via les mêmes serveurs frontaux (ex: xxxx.appspot.com).
- Requête à google.com avec dans le champ “Host” de la requête HTTPS la valeur xxx.appspot.com”
- Complique la vie des équipes de défense



https://www.bamsoftware.com/papers/fronting/

https://www.xorrior.com/Empire-Domain-Fronting/

https://www.securityartwork.es/2017/01/31/simple-domain-fronting-poc-with-gae-c2-server/

Module Burp pour les Javascript Web Service Proxies

- JWSP est une alternative au WSDL

https://blog.netspi.com/attacking-javascript-web-service-proxies-burp/

Kraken, un outil d’identification d’interfaces web

https://github.com/Sw4mpf0x/Kraken

Pentest
Défense

Utiliser ses logs DNS pour de la réponse à incident

https://blogs.technet.microsoft.com/teamdhcp/2015/11/23/network-forensics-with-windows-dns-analytical-logging/

Utiliser ses logs Azure dans Splunk, ELK, ArcSight ou encore QRadar

- L'agent du SIEM doit être installé sur un serveur intermédiaire, l'Azlog Integrator

https://docs.microsoft.com/en-us/azure/security/security-azure-log-integration-get-started

Comment Windows 10 se protège des vulnérabilités noyau 0-day

https://blogs.technet.microsoft.com/mmpc/2017/01/13/hardening-windows-10-with-zero-day-exploit-mitigations/

Présentation de M. Russinovich à RSA sur Sysmon

https://onedrive.live.com/view.aspx?resid=D026B4699190F1E6!2843&ithint=file%2cpptx&app=PowerPoint&authkey=!AMvCRTKB_V1J5ow

Des configurations Sysmon à la pelle

https://github.com/SwiftOnSecurity/sysmon-config/blob/master/sysmonconfig-export.xml

- Workstation : https://gist.github.com/Neo23x0/f56bea38d95040b70cf5
- Serveur : https://gist.github.com/Neo23x0/a4b4af9481e01e749409

ACL Active Directory à surveiller

- Peut permettre de détecter un attaquant voulant persister dans les systèmes

  https://blogs.technet.microsoft.com/pfesweplat/2017/01/28/forensics-active-directory-acl-investigation/

Détecter Mimikatz en mémoire

- Grâce aux librairies utilisées, formant une sorte de signature
- Gare aux faux positifs !

  https://securityriskadvisors.com/blog/post/detecting-in-memory-mimikatz/

ANSSI, publication d'un outil pour analyser le secteur de boot d'un disque

- Ne marche que sur une copie de disque

  https://github.com/ANSSI-FR/bootcode_parser

Business et Politique

Droit / Politique

France

Benoit Loutrel, directeur de l'Arcep part chez Google

- Qui a dit conflit d'intérêts ?
  - Le changement a été validé par la commission de déontologie

https://www.nextinpact.com/news/102929-remous-autour-depart-directeur-general-l-arcep-chez-google.htm

La loi (ou presque) vous impose un mot de passe de 12 caractères !

<<Cas n° 1. - Mot de passe seul

Si l'authentification repose uniquement sur un identifiant et un mot de passe, la commission considère que :
- la **taille** du mot de passe doit être **au minimum de 12 caractères** ; et
- le mot de passe doit comprendre des majuscules, des minuscules, des chiffres et des caractères spéciaux.>>

https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033928007

Fichier TES, compte rendu de l'audit de l'ANSSI

- Résultats assez flous : "plusieurs faiblesses"
- Recommandation de plus de traçabilité et d'authentification forte

http://videos.assemblee-nationale.fr/video.4585100_587f31f0a00c8

Droit / Politique
International

Après vos réseaux sociaux, les douanes américains regardent dans vos smartphones

- Demander de déverrouiller le smartphone pour regarder les photos, sms et mails

  http://www.capital.fr/art-de-vivre/high-tech/les-douaniers-americains-fouillent-maintenant-votre-smartphone-1207365

Abolition du "Privacy Act" pour les non-citoyens US (ou non-résidents permanents)

<<Sec. 14. Privacy Act. Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information.>>

https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united

La Russie, les Hackeurs et Trump

- Le mémo annonçant que Trump est piloté par Poutine, à cause d'une "sex tape"

  https://www.nytimes.com/2017/01/11/us/politics/donald-trump-russia-intelligence.html

- Témoignage de l'agent à l'origine du mémo sur Trump et la Russie

  http://www.motherjones.com/politics/2017/01/spy-who-wrote-trump-russia-memos-it-was-hair-raising-stuff

Preuve du piratage du DNC par les Russes

- Métadonnées louches, à l'origine des accusations de CrowdStrike
  - A notre petit niveau, nous utilisons un OS et Office anglais et nettoyons nos docs, alors un service gouvernemental...

https://medium.com/@thegrugq/the-russian-way-of-cyberwar-edb9d52b4876#.97zxg7ptl

Droit / Politique
International

Alexa témoin d'un meurtre, mais Amazon refuse de livrer les données

http://tempsreel.nouvelobs.com/rue89/rue89-tech/20170109.RUE6123/quand-une-machine-est-temoin-d-un-meurtre-c-est-complique.html

Trump nomme un ennemi de la neutralité du Net à la tête de la FCC

https://www.nextinpact.com/news/102994-donald-trump-nomme-opposant-a-neutralite-net-a-tete-regulateur.htm

RackSpace poursuivi pour "non application d'un correctif"

- Un hébergeur a perdu 2 clients à cause de pannes à répétitions
- A cause d'une mauvaise migration de WAF, aboutissant à des pannes

http://www.thewhir.com/web-hosting-news/rackspace-customer-sues-over-alleged-security-issues

Après USA vs Microsoft, voici USA vs Google

- Demande de fourniture de mails stockés à l'étranger

http://www.latribune.fr/technos-medias/internet/google-doit-remettre-a-la-justice-americaine-des-courriels-stockes-a-l-etranger-636162.html

Conférences

Conférences

Passées

- CORI&IN - 23 janvier 2017 à Lille
- FIC - 24-25 janvier 2017 à Lille

A venir

- JSSI - 14 mars 2017 à Paris
- Troopers - 20 au 24 mars 2017 à Heidelberg
- GS Days - 28 mars 2017 à Paris

Divers / Trolls velus

Divers / Trolls velus

Une porte dérobée dans la crypto de Whatsapp ?

- Non, un choix de design !
- Changement de la clef privée
  - Signal avertit et empêche les communications tant que l'utilisateur n'a pas accepté

https://www.theguardian.com/technology/2017/jan/13/whatsapp-backdoor-allows-snooping-on-encrypted-messages

Il faut désinstaller les antivirus, sauf celui de Microsoft

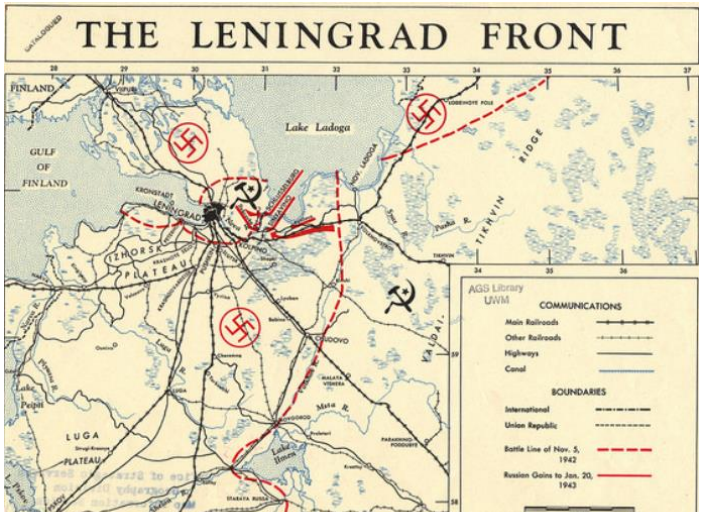
- L'antivirus ne sert à rien et augmente les risques / la surface d'attaque
- Il ralentit l'ordinateur

http://robert.ocallahan.org/2017/01/disable-your-antivirus-software-except.html

Historique de cartes géographiques de la CIA

- De 1940 à 2010

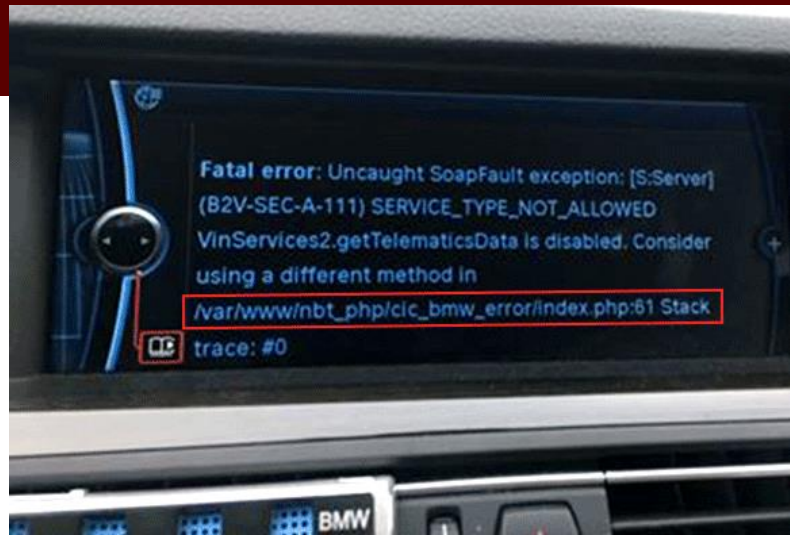
https://www.flickr.com/photos/ciagov/collections/72157674854602812/



Divers / Trolls velus

Du PHP dans une BWM !!?

https://twitter.com/antonioperic/status/824629419419561985/photo/1



<<Votre empreinte, votre nouveau mot de passe>>

- Ou quand Deloitte confond Authentification et Identification

  https://twitter.com/deloittefrance/status/826779987998969856

Pokémon Go interdit en Chine par mesure de sécurité

http://www.journaldugeek.com/2017/01/11/pokemon-go-interdit-chine-securite/

FBI vs Apple, document publie, mais censuré

- Une société a été sélectionnée parmi trois pour siphonner l'iPhone
  - Cellebrite ?

https://www.nextinpact.com/news/102840-iphone-deverrouille-fbi-revele-sa-methode-en-masquant-details.htm

Divers / Trolls velus

GitLab, un administrateur supprime 300Go de données par erreur

- Cela touche 5000 projets
- La restauration des sauvegardes ne fonctionne pas

https://www.nextinpact.com/news/103135-gitlab-erreur-humaine-et-sauvegardes-defaillantes-entrainent-perte-300-go-donnees.htm

https://about.gitlab.com/2017/02/10/postmortem-of-database-outage-of-january-31/

Mystère mystérieux, il change de CB et Amazon le sait déjà

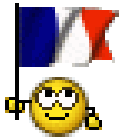
- Si l'histoire est vraie, il n'y a pas d'explication pour le moment

https://www.theguardian.com/money/2017/jan/12/how-amazon-know-new-visa-card-information-before-me-natwest

Un parc d'attraction espagnol impose de laisser ses empreintes digitales

https://twitter.com/CPCHardware/status/823495833576411136

Unicorn.js, émuler des CPU en Javascript



- ARM, ARM64, M68K, MIPS, SPARC et x86

https://alexaltea.github.io/unicorn.js/index.html

- Pour du RISC-V 64bits, allez voir chez notre Fabrice BELLARD national

http://bellard.org/riscvemu/js/

Divers / Trolls velus

Martine fait de l'inforensique pour Envoyé Spécial

- Ne font pas appel à des experts mais à un “hackeur de confiance”
- Accès directement depuis le PC portable HP à analyser

https://twitter.com/EnvoyeSpecial/status/824739119582547968

Google arriverait à zoomer comme dans Blade Runner !!!

http://phandroid.com/2017/02/07/google-zoom-and-enhance-ai/

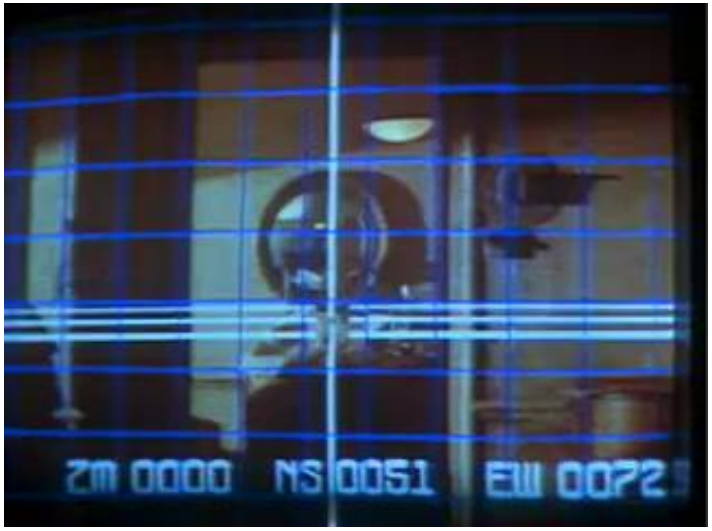
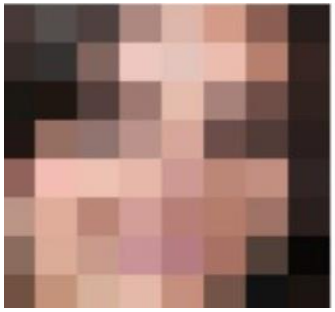


image à traiter



traitement par Google

image originale

Divers / Trolls velus

NextCloud (ex-owncloud) scan les sites utilisant leur application

- Et passe par l'ANSSI pour avertir les sites web vulnérables

Expéditeur: <incident@cert.ssi.gouv.fr>
Date: 15 février 2017 à [redacted] UTC+1
Destinataire: [redacted]
Objet: [ANSSI - CERT-FR] Liste d'un ou plusieurs instances ownClouse/NextCloud vulnérables - Du 13/02/2017

Bonjour,

Le CERT-FR, centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques, a été informé par le CERT-Bund qu'une ou plusieurs machines appartenant à votre réseau disposent d'instances ownCloud / Nextcloud accessibles sur Internet. Ces instances utiliseraient des versions non mises à jour et vulnérables.

Les vulnérablilités identifiées peuvent être exploitées pour obtenir un accès non autorisé aux données stockées dans le nuage. Par ailleurs des attaquants pourraient potentiellement accéder à des informations sensibles. D'autres vulnérabilités peuvent être exploitées pour exécuter du code arbitraire sur le ou les serveurs vulnérables et Un compromettre votre système d'information.

Vous trouverez ci-dessous la liste des instances identifiées sur votre réseau, ainsi que l'horodatage (fuseau horaire UTC) qui fait référence à la date de détection de l'instance vulnérable :

Format: ASN,Horodatage,IP,Port(TCP),Hostname,Severite,UUID
15830,2017-02-13 01:08:03,[redacted]

Chaque enregistrement comprend un niveau de risque et un ID individuel (UUID).

Des informations détaillées sur les vulnérabilités identifiés sont accessibles à l'adresse:
https://scan.nextcloud.com/results/[UUID]

Le paramètre [UUID] doit être remplacé par l'UUID fourni pour l'instance identifiée.
Exemple: https://scan.nextcloud.com/results/12345678-1234-1234-1234-12345678

Ce signalement vous est adressé à toutes fins utiles, nous vous remercions d'en informer le(s) propriétaire(s) / attributaire(s).
Des mises à jour logicielles, pour corriger les vulnérabilités identifiées sont disponibles pour tous les problèmes signalés.
En cas de questions sur les scans effectués par Nextcloud GmbH, nous vous invitons à contacter <cloud-security-scan@nextcloud.com> en nous mettant en copie de votre courriel.

Le CERT-FR se tient à votre disposition pour toute information ou conseil complémentaires.

Cordialement,
--
Bureau Réponse aux Incidents
Agence nationale de la sécurité des systèmes d'information
Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques
51, boulevard de La Tour-Maubourg - 75700 PARIS 07 SP
Tel : +33 (0)1 71 75 84 50 - Fax : +33 (0)1 71 75 84 70
Mel : incident@cert.ssi.gouv.fr - Web : www.cert.ssi.gouv.fr

Divers / Trolls velus

Une infographie qui vous expliquer les alertes des navigateurs

https://casecurity.org/browser-ui-security-indicators/

Quand CrowdStrike n’est pas content des résultats du NSS Labs, ils attaquent !

- CrowdStrike décrit la démarche du NSS Labs comme non éthique, illicite et subversive

  http://www.zdnet.com/article/crowdstrike-denied-bid-to-block-security-report-in-legal-challenge-against-subversive-nss-labs/

Divers / Trolls velus

Si vous vendez votre BlackPhone sur eBay, Silent Circle le bloque

- Le constructeur casse le marché de l'occasion

  https://arstechnica.com/information-technology/2017/01/silent-circle-bricks-grey-market-blackphones-with-os-update/

Nos espions doivent porter des slips en plomb

- Les puissances des gros IMSI catchers impose aux agents de prendre des précautions

  https://news.sfr.fr/actualites/societe/nos-espions-de-la-dgsi-obliges-de-porter-des-slips-anti-ondes-de-telephone.html

Les barbouzes sont cuites

DERNIERS joujoux à la mode au sein des services de renseignement, les Imsi-catchers donnent des sueurs froides aux espions et autres contre-espions. Ces engins, qui permettent d'identifier et d'écouter en temps réel les téléphones portables utilisés dans un périmètre donné, voire d'en pomper les données, émettent des ondes si puissantes qu'ils menacent la santé de leurs utilisateurs.

A tel point que les agents craignent de voir – dans certains cas extrêmes – leurs neurones et leurs gamètes caramélisés par le rayonnement. « *Pour les appareils les plus gros, cela équivaut à vivre scotché à une antenne-relais : il ne faut pas rester longtemps à côté* », explique un expert proche de la Direction générale de la sécurité intérieure. Soucieux d'éviter des désagréments fâcheux, les fonctionnaires ont dû mettre en place un lourd protocole. « *Il faut préparer la voiture,* ajoute la même source, *la transformer en cage de Faraday, installer une plaque de métal entre le local où se trouve l'Imsi et les sièges des passagers. Et, surtout, ne pas quitter sa place tant que l'engin fonctionne…* » Pour protéger les personnels utilisant des valises-espions portées près du corps et dotées d'Imsi-catchers miniaturisés, il a fallu trouver une autre astuce. Les manipulateurs sont désormais tenus de porter des sous-vêtements spéciaux qui préservent leur fertilité en formant une autre cage de Faraday à l'endroit approprié. Du genre slip en cotte de mailles ou ceinture de chasteté en acier trempé ? **J. C.**

Les vété

LA bagarre est silencieus

Prochains rendez-vous de l’OSSIR

Prochaines réunions

JSSI

- Mardi 14 mars 2017
  FIAP, 30 Rue Cabanis, 75014 Paris

Prochaine réunion

- Mardi 11 avril 2017

After Work

- Mardi 28 février 2017

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous