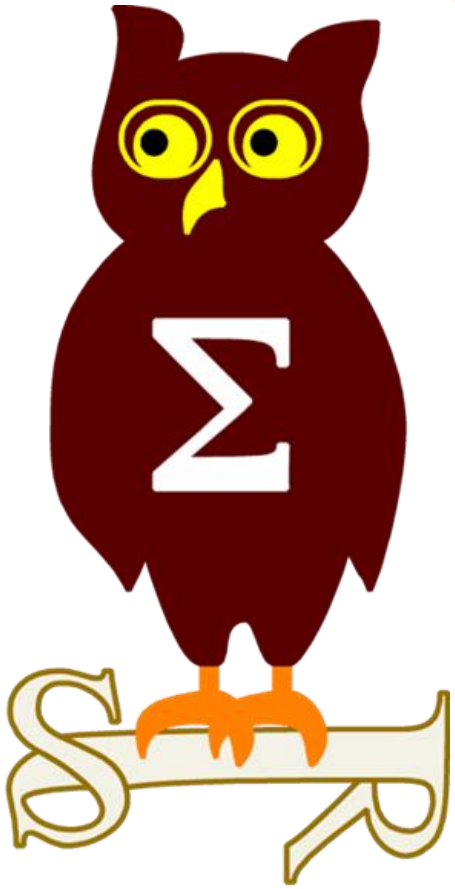
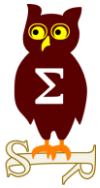


Revue d'actualité

12/12/2017

Préparée par

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



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS17-108 Vulnérabilités dans Internet Explorer (12 CVE)

- Exploit:
  - 9 x Remote Code Execution
  - 3 x Information Disclosure
- Publiés: CVE-2017-11848, CVE-2017-11827
- Credits:
  - Hui Gao de Palo Alto Networks (CVE-2017-11834, CVE-2017-11791)
  - Anonymous par Trend Micro's Zero Day Initiative (CVE-2017-11869)
  - Huang Anwen de ichunqiu Ker Team par Trend Micro's Zero Day Initiative (CVE-2017-11858)
  - Cybellum Technologies LTD (CVE-2017-11827)
  - Wei de Qihoo 360 Vulcan Team (CVE-2017-11843)
  - ? (CVE-2017-11848)
  - Ivan Fratric de Google Project Zero, Hui Gao de Palo Alto Networks and Heige (a.k.a. SuperHei) de Knownsec 404 Security Team (CVE-2017-11855)
  - The UK s National Cyber Security Centre (NCSC) (CVE-2017-11838)
  - Hui Gao and Zhanglin He de Palo Alto Networks, Anonymous par Trend Micro's Zero Day Initiative (CVE-2017-11856)
  - Qixun Zhao de Qihoo 360 Vulcan Team, Wei de Qihoo 360 Vulcan Team (CVE-2017-11837)
  - Yuki Chen de Qihoo 360 Vulcan team (CVE-2017-11846)

MS17-109 Vulnérabilités in Edge (24 CVE)

- Exploit:
  - 3 x Security Feature Bypass
  - 17 x Remote Code Execution
    - https://bugs.chromium.org/p/project-zero/issues/detail?id=1357
    - https://bugs.chromium.org/p/project-zero/issues/detail?id=1363
    - https://bugs.chromium.org/p/project-zero/issues/detail?id=1364
    - https://bugs.chromium.org/p/project-zero/issues/detail?id=1365
    - https://bugs.chromium.org/p/project-zero/issues/detail?id=1366
    - https://bugs.chromium.org/p/project-zero/issues/detail?id=1367
    - https://bugs.chromium.org/p/project-zero/issues/detail?id=1343
  - 4 x Information Disclosure
- Published: CVE-2017-11827
- Credits:
  - The UK s National Cyber Security Centre (NCSC) (CVE-2017-11838)
  - Hui Gao de Palo Alto Networks (CVE-2017-11791)
  - Qixun Zhao de Qihoo 360 Vulcan Team, Lokihardt de Google Project Zero (CVE-2017-11873)
  - Qixun Zhao de Qihoo 360 Vulcan Team, Wei de Qihoo 360 Vulcan Team (CVE-2017-11837)
  - Yuki Chen de Qihoo 360 Vulcan team (CVE-2017-11846)
  - Johnathan Norman Microsoft et Lokihardt de Google Project Zero (CVE-2017-11870)
  - Debasish Mandal (@debasishm89) de McAfee IPS Vulnerability Research, Omair (CVE-2017-11844)
  - Stefano Calzavara and Alvise Rabitti de Universit Ca'Foscari, Venezia (CVE-2017-11863)
  - Alexander Inf hr (@insertScript) de Cure53 (CVE-2017-11833)
  - Omair (CVE-2017-11845)
  - Liu Long de Qihoo 360Vulcan Team (CVE-2017-11803)Microsoft ChakraCore Team (CVE-2017-11836, CVE-2017-11862)
  - Ivan Fratric de Google Project Zero. (CVE-2017-11874)
  - Huang Anwen de ichunqiu Ker Team par Trend Micro's Zero Day Initiative (CVE-2017-11858)
  - Prakash Sharma (@1lastBr3ath) (CVE-2017-11872)
  - Cybellum Technologies LTD (CVE-2017-11827)
  - Wei de Qihoo 360 Vulcan Team (CVE-2017-11843)
  - ? (CVE-2017-11871, CVE-2017-11866)
  - Lokihardt de Google Project Zero (CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11861)

Dont 7 communes avec IE:

- CVE-2017-11791
- CVE-2017-11827
- CVE-2017-11837
- CVE-2017-11838
- CVE-2017-11843
- CVE-2017-11846
- CVE-2017-11858

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS17-150 Vulnerabilities dans Windows Kernel (5 CVE)

- Affected:
  - Windows toutes versions supportées
- Exploit:
  - 4 x Information Disclosure
    - https://bugs.chromium.org/p/project-zero/issues/detail?id=1362
  - 1 x Elevation of Privilege
- Credits:
  - Mateusz Jurczyk de Google Project Zero (CVE-2017-11853)
  - nyaacate de Viettel Cyber Security par Trend Micro's Zero Day Initiative (CVE-2017-11847)
  - Georgios Baltas de MSRC Vulnerabilities & Mitigations Team (CVE-2017-11842)
  - fanxiaocao and pjf de IceSword Lab, Qihoo 360 (CVE-2017-11849)
  - Marcin Wiazowski par Trend Micro's Zero Day Initiative (CVE-2017-11851)

MS17-151 Vulnerabilities dans Office (5 CVE)

- Affected:
  - Microsoft Office 2007, 2010, 2013, 2016
- Exploit:
  - 4 x Remote Code Execution
    - https://29wspy.ru/reversing/CVE-2017-11882.pdf
  - 1 x Security Feature Bypass
- Credits:
  - Wayne Low (@x9090) de Fortinet s FortiGuard Lab (CVE-2017-11854)
  - Jonathan Birch Microsoft Corporation (CVE-2017-11877)
  - Denis Selianin from Embedi (CVE-2017-11882)
  - Jaanus Kp Clarified Security par Trend Micro's Zero Day Initiative (CVE-2017-11878)
  - Dhanesh Kizhakkinan de FireEye Inc, Dmitri Kaslov par Trend Micro's Zero Day Initiative (CVE-2017-11884)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS17-152 Vulnerabilities dans Microsoft Graphics (GDI) (4 CVE)

- Affected:
  - Windows toutes versions supportées
- Exploit:
  - 4 x Information Disclosure
- Credits:
  - Wayne Low (@x9090) de Fortinet s FortiGuard Lab (CVE-2017-11832)
  - Hossein Lotfi, Secunia Research at Flexera Software, kdot par Trend Micro's Zero Day Initiative, Wayne Low (@x9090) de Fortinet s FortiGuard Lab (CVE-2017-11835)
  - Seonunghardt(@seonunghardt) and Team Pwn4Fun from Best de Best (BOB) (CVE-2017-11852)
  - fanxiaocao and pjf de IceSword Lab, Qihoo 360 (CVE-2017-11850)

MS17-153 Vulnerabilities dans ASP.NET (3 CVE)

- Affected:
  - ASP.NET Core 1.0, 1.1, 2.0
- Exploit:
  - 1 x Denial of Service
  - 1 x Information Disclosure
  - 1 x Elevation of Privilege
- Published: CVE-2017-8700, CVE-2017-11883
- Credits:
  - K vin Chalet (CVE-2017-11879)
  - ? (CVE-2017-8700, CVE-2017-11883)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS17-154 Vulnerabilities dans Windows (2 CVE)

- Affected:
  - Windows toutes versions supportées
- Exploit:
  - 2 x Information Disclosure
    - https://bugs.chromium.org/p/project-zero/issues/detail?id=1361
- Credits:
  - Mateusz Jurczyk de Google Project Zero (CVE-2017-11831, CVE-2017-11880)

MS17-155 Vulnerability dans Windows Media Player (1 CVE)

- Affected:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Information Disclosure
- Credits:
  - James Lee de Kryptos Logic (CVE-2017-11768)

MS17-156 Vulnerability dans .Net (1 CVE)

- Affected:
  - .NET Core 1.0, 1.1, 2.0
- Exploit:
  - 1 x Denial of Service
- Credits:
  - Bachraty Gergely (CVE-2017-11770)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS17-157 Vulnerability dans Device Guard (1 CVE)

- Affected:
  - Windows 10, Server 2016
- Exploit:
  - 1 x Security Feature Bypass
- Credits:
  - James Forshaw de Google Project Zero (CVE-2017-11830)

MS17-158 Vulnerability dans Windows Search (1 CVE)

- Affected:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Denial of Service
- Credits:
  - Lei Shi de Qihoo 360 Inc (CVE-2017-11788)

MS17-159 Vulnerability dans SharePoint (1 CVE)

- Affected:
  - Microsoft Project Server 2013, 2016
- Exploit:
  - 1 x Elevation of Privilege
- Credits:
  - ? (CVE-2017-11876)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

Publication hors bande

MS17-160 Vulnerabilities dans Defender (Malware Protection Engine) (2 CVE)

- Affected:
  - Microsoft Endpoint Protection, Forefront Endpoint Protection, Security Essentials
  - Microsoft Exchange Server 2013, 2016
  - Windows Defender on Windows
  - Windows Intune Endpoint Protection
- Exploit:
  - 2 x Remote Code Execution
    - https://www.cyberscoop.com/critical-vulnerability-hits-microsoft-malware-protection-engine/
- Credits:
  - The UK's National Cyber Security Centre (NCSC) (CVE-2017-11940, CVE-2017-11937)

Failles / Bulletins / Advisories

Microsoft - Autre

Vulnérabilité CVE-2017-11826 exploitée dans la nature par du phishing

- Corrigée dans le bulletin MS17-136 d'octobre 2017
- Possible utilisation par un service gouvernemental

https://blog.fortinet.com/2017/11/22/cve-2017-11826-exploited-in-the-wild-with-politically-themed-rtf-document

Contourner Windows Defender grâce au UNC

- Utiliser **\\localhost\c$** plutôt que **c:**

https://www.exploit-db.com/exploits/43229/

Microsoft rend accessible une clef privée signant *.sandbox.operations.dynamics.com

- Plateforme de dev permettant d'exécuter du code
- Chaque serveur dispose d'un certificat Wildcard et sa clef privée
- Pas d'information sur la prod

https://medium.com/matthias-gliwka/microsoft-leaks-tls-private-key-for-cloud-erp-product-10b56f7d648

Publications des slides de la conférence BlueHat

https://www.slideshare.net/MSbluehat/

Failles / Bulletins / Advisories

Système (principales failles)

Exim, exécution de code à distance (CVE-2017-16943)

- Longue attente côté client, envoie d'une taille de données (BDAT) puis du payload

  https://bugs.exim.org/show_bug.cgi?id=1052

- Debian (stable) n'est pas affecté

  https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=882648#16

WGET stack et heap overflow / CVE-2017-13089 et CVE-2017-13090

https://xorl.wordpress.com/2017/11/11/cve-2017-13090-wget-file-retrieval-integer-overflow/

OpenSSH, déni de service par sur-consommation du CPU / CVE-2016-6515

- En saisissant un mot de passe de plus de 1000 caractères
- Le correctif ne fait que limiter l'entrée à 1024 caractères

  https://xorl.wordpress.com/2017/11/10/cve-2016-6515-openssh-remote-dos/

OpenSSH, écriture arbitraire en SFTP

- Vérification des clefs READ, WRITE mais pas CREATE

  https://xorl.wordpress.com/2017/11/13/openssh-sftp-server-remote-security-vulnerability/

Failles / Bulletins / Advisories

Système (principales failles)

Dirty COW est de retour, la vache broot à nouveau / CVE-2017–1000405

- Même attaque sur les « huge pages »

  https://medium.com/bindecy/huge-dirty-cow-cve-2017-1000405-110eca132de0

Xen, évasion de la machine virtuelle

- Ainsi que déni de service et atteinte à la confidentialité des données

  http://xenbits.xen.org/xsa/advisory-246.html

  http://xenbits.xen.org/xsa/advisory-247.html

pfSense, exécution de code à distance

- Depuis le portail web d’administration

  http://0day.today/exploits/29078

Failles / Bulletins / Advisories

Système (principales failles)

Vulnérabilités dans WordPress “Formidable Forms”

- XSS réfléchie, XSS stockée, SQLi, exécution de code sans authentification

  https://klikki.fi/adv/formidable.html

TeamViewer, Injection de DLL

- En cas d’accès déjà autorisé

  https://thehackernews.com/2017/12/teamviewer-hacking-tool.html

  https://github.com/gellin/TeamViewer_Permissions_Hook_V1

Failles / Bulletins / Advisories

Système (principales failles)

macOS X, initialisation du compte root sans mot de passe / CVE-2017-13872

https://www.macrumors.com/2017/11/28/macos-high-sierra-bug-admin-access/

- Proposé comme une astuce sur le forum officiel d'aide d'Apple

  https://forums.developer.apple.com/thread/79235#277225

- Risque si un service réseau (ssh, vlc, ard) est activé (ce qui n'est pas le cas par défaut)

macOS X, exécution de code à l'insertion d'une clef USB

- Si celle-ci est formatée en FAT et un index des répertoires négatif
- Par un appel automatique à **fsck_msdos**

  http://blog.trendmicro.com/trendlabs-security-intelligence/october-macos-patch-fixes-fatusb-vulnerability/

macOS X, bulletin cumulatif des correctifs

- Désintalle le correctif de la vulnérabilité CVE-2017-13872

  https://support.apple.com/en-us/HT208315

macOS X, tâches planifiées accessibles à tous

https://m4.rkw.io/blog/macos-high-sierra-10131-insecure-cron-system.html

Failles / Bulletins / Advisories

Réseau (principales failles)

Vulnérabilité ridicule sur FortiWebManager 5.8.0 / CVE-2017-14189

- Le bulletin de Fortinet est clair : `<< FortiWebManager 5.8.0 fails to check the admin password, granting access regardless the provided string.>>`

  https://fortiguard.com/psirt/FG-IR-17-248

Les imprimantes HP vulnérables à l'exécution de code à distance

https://support.hp.com/nz-en/document/c05839270

https://www.theregister.co.uk/2017/11/21/patch_coming_for_hp_printer_vulnerabilities/

https://github.com/foxglovesec/HPwn

Failles / Bulletins / Advisories

Intel Management Engine

Encore des Vulnérabilités dans Intel Management Engine

- 8 vulnérabilités critiques, principalement des élévations locales de privilèges
  - Intel® Management Engine 11.x: CVE-2017-5705 , CVE-2017-5708, CVE-2017-5711, CVE-2017-5712
  - Intel® Server Platform Service 4.0.x.x : CVE-2017-5706 , CVE-2017-5709
  - Intel® Trusted Execution Engine 3.0 : CVE-2017-5707 , CVE-2017-5710

  https://security-center.intel.com/advisory.aspx?intelid=intel-sa-00086&languageid=en-fr
- Un outil pour tester si vous êtes vulnérable
  - Ne marche pas depuis une VM

  https://downloadcenter.intel.com/download/27150

L'auteur de Minix écrit une lettre ouverte à Intel

- Pas de critique violente, il note juste le manque de courtoisie d'Intel de ne pas l'avoir informé
- Du fait de Management Engine, Minix, serait l'un des OS les plus déployés au monde

  https://www.techpowerup.com/238677/minix-creator-andrew-tanenbaum-sends-open-letter-to-intel-over-minix-drama

Dell propose des ordinateurs portables avec Management Engine désactivé

- Par contre, cela coûterait entre $20 et $40

  https://hardware.slashdot.org/story/17/12/03/2113220/dell-begins-offering-laptops-with-intels-management-engine-disabled

A noter que le BIOS va disparaître, au profit d'UEFI

- C'est Intel qui le dit

  http://www.uefi.org/sites/default/files/resources/Brian_Richardson_Intel_Final.pdf

Failles / Bulletins / Advisories

Intel Management Engine

Bonus : Management Engine accessible depuis le WiFi

- Des cartes WiFi Intel vulnérables à KRACK ne sont plus supportées et n'auront pas de correctif
- Le Wake in Lan permet de démarrer le PC sur WiFi
- L'exploitation de KRACK permet d'injecter et d'exploiter les vulnérabilités ME

  https://security-center.intel.com/advisory.aspx?intelid=intel-sa-00101&languageid=en-fr

Failles / Bulletins / Advisories

Hardware / IoT

HP iLo4, également des vulnérabilités

- Exécutions de code à distance
- Présenté à Recon 2018 par Alexandre Gazet, Joffrey Czarny et Fabien Perigaud

  https://twitter.com/reconbrx/status/933081813064519680

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Les Buckets S3 ne sont pas sécurisés

- 100 Go de fichiers confidentiels défense du service US Army's Intelligence and Security Command

  https://www.upguard.com/breaches/cloud-leak-inscom

Vol de cryptotokens

- 30 millions de “tethers”

  https://nakedsecurity.sophos.com/2017/11/23/tether-hits-back-after-31m-cryptocurrency-hack/

  https://journalducoin.com/altcoins/tether-usdt-tourmente-scam-or-not/

Imgur: vol de données de 1.7 millions d’utilisateurs en 2014

https://techcrunch.com/2017/11/27/imgur-says-1-7m-emails-and-passwords-were-breached-in-2014-hack/

https://twitter.com/haveibeenpwned/status/934210666335891456

https://blog.imgur.com/2017/11/24/notice-of-data-breach/

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Amazon Key, déjà piraté

- Le livreur peut brouiller/déconnecter le WiFi de la webcam

https://www.wired.com/story/amazon-key-flaw-let-deliverymen-disable-your-camera/

TEMPEST de la NSA, à la maison

https://twitter.com/darksidelemm/status/934005125932204032/photo/1

Piratages, Malwares, spam, fraudes et DDoS
Espionnage

Les Chinois espionnent sur Linkedin, selon les renseignements Allemands

- Ils créent de faux profils pour espionner
- Mais Linkedin n'est-il pas LA source de renseignement des services américains ?

  http://www.bbc.com/news/world-europe-42304297

HP fournit un pilote de clavier avec capacité de "keylogger"

- Possibilité de l'activer avec une clef de registre

  https://zwclose.github.io/HP-keylogger/

Surveillance (tracking) des utilisateurs mobiles de…

- LeParisien, Linkedin, CandyCrush, Skype...

  http://www.lemonde.fr/pixels/article/2017/11/24/des-mouchards-caches-dans-vos-applications-pour-smartphones_5219892_4408996.html

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Uber, fuite massive de données dissimulée en 2016

- Données personnelles de 57 millions d'utilisateurs
- Récupération d'une clé SSH Amazon sur un dépot Github
- Fuite non révélée au public

  https://www.uber.com/newsroom/2016-data-incident/

  https://nakedsecurity.sophos.com/2017/11/22/uber-suffered-massive-data-breach-then-paid-hackers-to-keep-quiet/
- L'État de Washington poursuit Uber pour sa fuite de données

  https://www.nextinpact.com/brief/l-etat-de-washington-poursuit-uber-pour-sa-fuite-de-donnees-1542.htm
- Hervé en grande forme :

  http://www.solutions-numeriques.com/dirigeants/fuite-de-donnees-duber-revele-le-pire-de-ce-que-lon-peut-imaginer-selon-lexpert-en-cybersecurite-herve-schauer/
- Un ancien employé les accuse d'avoir une branche dédiée au vol de secrets

  https://www.nextinpact.com/brief/un-ex-employe-d-uber-accuse-la-societe-d-avoir-une-branche-dediee-au-vol-de-secrets-industriels-et-commerciaux-1552.htm

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Piratage du Cercle de l'Union interalliée

- Publication des noms, mails, identifiants et mots de passe
- Beaucoup de dirigeants de grandes entreprises y sont
- Cause : mauvaise manipulation d’un de leur intervenant informatique

Ashley Madison perd encode des données personnelles

- Partage bidirectionnel d’une clef d’accès aux photos en cas de partage unidirectionnel

https://amp.ibtimes.co.uk/ashley-madison-leaking-users-private-explicit-photos-yet-again-1650509

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Rançongiciel ciblant les NAS

- Chiffre les données et demande 0,4 et 2 Bitcoins

  http://securityaffairs.co/wordpress/66401/malware/storagecrypt-ransomware-sambacry.html

Arrêtez d'exposer du SMB publiquement sur Internet

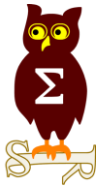
Piratages, Malwares, spam, fraudes et DDoS

IOT

Ouverture de coffrets pour armes à feu Bluetooth

- Le code d'appairage Bluetooth est le même que le code secret. On peut donc identifier le code secret par force brute sur l'appairage
- Envoi du code en clair contrairement à la mention sur le site "AES 256"
- Ouverture possible via une commande Bluetooth sans connaître le code PIN

https://www.twosixlabs.com/bluesteal-popping-gatt-safes/



Nouveautés, outils et techniques

Crypto et Divers

Spécial Autorités de Certificats

Détecter les ajouts de nouvelle AC sous Windows

https://isc.sans.edu/forums/diary/Keep+An+Eye+on+your+Root+Certificates/23030/

Nouvelle loi en Hollande concernant l'interception des communications

- Mozilla supprime l'AC néerlandaise "PKIOverheid / Logius"

  https://bugzilla.mozilla.org/show_bug.cgi?id=1408647

Une histoire de Bitcoin

- Quand la clé privée = SHA256(clé_publique)

  https://pastebin.com/jCDFcESz

  https://www.reddit.com/r/Bitcoin/comments/7gka3b/evidence_some_bitcoin_address_generation_code_is/

Crypto et Divers

Divers

Chrome 65, utilisation du champ SAN dans les certificats

- « Common Name » déprécié depuis plus de 2 ans
- Remplacé par le champ « Subject Alternative Name », mais tout le monde utilise les deux
- Suppression du support du CN à partir de Chrome 58 et définitivement dans Chrome 65

https://www.chromium.org/administrators/policy-list-3#EnableCommonNameFallbackForLocalAnchors

Chrome 65, fin du PunyCode si le TLD n'est pas en PunyCode

- **https://www.xn--80ak6aa92e.com** s'affichera tel quel et non **https://www.apple.com**

https://www.thesslstore.com/blog/security-changes-in-chrome-58/

Trouver des buckets S3 avec bucketstream

- Grâce à “certificate transparency”

  https://github.com/eth0izzle/bucket-stream

Les fichiers SCF de l’explorateur Windows

- « Windows Explorer **C**ommand **F**ile » (le S est pour « Scripting »)
- Personnalisation de l’icone d’un répertoire, pouvant se trouver sur Internet ou SMB

  https://www.information-security.fr/vol-didentifiants-windows-via-fichier-scf/

Récupérer certains clefs en mémoire d'un Linux

- Dans **certains** cas et pour **certains** outils, clefs de symétriques (AES) et asymétriques (RSA)

  https://github.com/cryptolok/CryKeX

Quelle architecture pour mon infrastructure de C2 ?

https://posts.specterops.io/designing-effective-covert-red-team-attack-infrastructure-767d4289af43

Pentest
Techniques & outils

Outil d’attaque radio

- Notamment pour les codes “rolling”

  https://github.com/cclabsInc/RFCrack

Guide de détection de comportements louches avec Sysmon

https://blogs.technet.microsoft.com/motiba/2017/12/07/sysinternals-sysmon-suspicious-activity-guide/

Détecter les keyloggers avec Sysmon

https://twitter.com/c_APT_ure/status/939066596894629888/photo/1

Récupération des événements Windows supprimés par Danderspritz

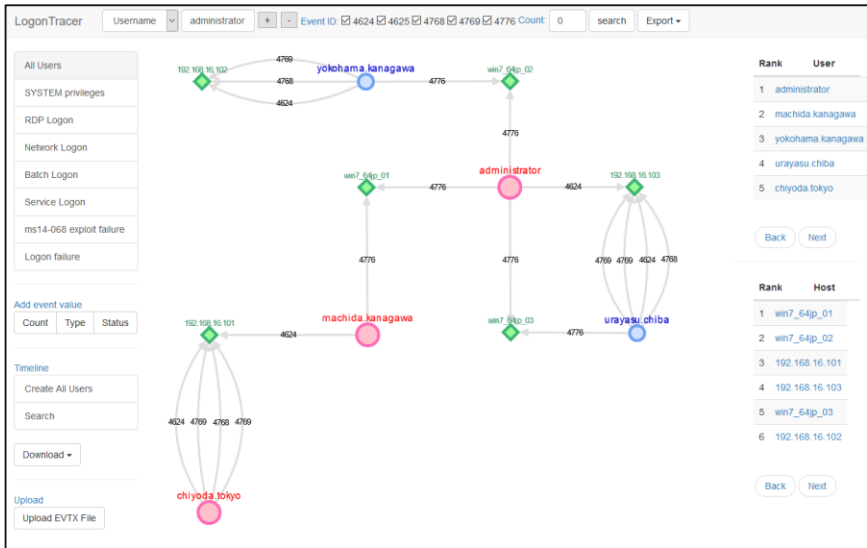
- Framework de post-exploitation de la NSA
- Permet d'effacer de manière sélective des événements Windows
- Le module ne fait que déréférencer l'événement, il ne l'efface pas

https://blog.fox-it.com/2017/12/08/detection-and-recovery-of-nsas-covered-up-tracks/

LogonTracer

- Visualisation des connexions AD à partir des logs

https://github.com/JPCERTCC/LogonTracer



Outils pour tester des IDS/IPS

- Flowsynth génère des captures réseau
- Dalton permet de jouer une capture sur un IDS

https://www.secureworks.com/blog/new-open-source-ids-tools

Business et Politique

Business

International

Les prix et marges du DarkNet

- Un malware bancaire vaut entre $3,000 et $5,000
- Swap de SIM entre $150 et $300
- ...

https://www.recordedfuture.com/cyber-operations-cost/

Droit / Politique

France

Jouets connectés I-QUE et My Friend Cayla

- Mise en demeure publique pour atteinte grave à la vie privée en raison d'un défaut de sécurité
  - Appairage sans code PIN
  - Ecoute à distance

https://twitter.com/CNIL/status/937626542859079680

Droit / Politique
International

Jugement de l'agent de la NSA qui avait sorti des outils, récupérés par Kaspersky

- Nghia Hoang Pho, 67 ans, développeur pour la TAO, plaide coupable
- Il a sorti des documents et outils de la NSA entre 2010 et 2015
- Il risque 10 ans de prison

https://thehackernews.com/2017/12/nghia-hoang-pho-nsa.html

Allemagne vs IoT

- Interdiction des montres connectées qui permettent aux parents d'espionner leurs enfants.

https://www.nextinpact.com/news/105651-le-regulateur-allemand-interdit-montres-connectees-pour-enfants-trop-intrusives.htm

Pays-bas vs IoT

- motion imposant des tests de piratage sur les IoT avant leur commercialisation dans le pays.

http://m.datanews.levif.be/ict/actualite/les-pays-bas-adoptent-une-motion-imposant-des-tests-de-piratage-aux-appareils-iot/article-normal-739361.html

L'aéroport d'Heathrow perd une clef USB

- Retrouvée par un passant, et lance une enquête

http://www.lemonde.fr/europe/article/2017/10/30/une-cle-usb-contenant-des-donnees-confidentielles-sur-l-aeroport-d-heathrow-retrouvee-dans-la-rue_5207636_3214.html

Droit / Politique
International

Hackeur Russe arrêté aux Maldives

- Roman Valerevich Seleznev
- Fils d'un membre du parlement, son arrestation est considérée comme un kidnapping
- 27+14 ans de prison et $51+$2 millions d'amende

https://thehackernews.com/2017/12/russian-hacker-prison.html

Un pirate canadien reconnaît avoir aidé le FSB

- Impliqué dans le piratage de Yahoo

http://www.lemonde.fr/pixels/article/2017/11/29/un-pirate-canadien-reconnait-avoir-aide-le-renseignement-russe_5222062_4408996.html

Trois chinois inculpés aux USA pour piratage et espionnage industriel

- Ils n'ont pas encore été arrêtés car habitant en Chine

http://www.lemonde.fr/pixels/article/2017/11/28/espionnage-industriel-trois-chinois-inculpes-aux-etats-unis-pour-des-piratages_5221530_4408996.html

Suite à tous ces procès, les agents de la TAO commencent à faire dans leur slip

- Ils risquent eux aussi d'être condamnés par les autres pays

https://twitter.com/h_miser/status/936144804353859584?refsrc=email&s=11

Conférences

Conférences

Passées

- Botconf - 6 au 8 décembre 2017 à Montpellier
  - Excellente édition !
- Hack.lu - 17-19 October 2017 à Luxembourg
- BlackHat Europe : 6-7 décembre 2017 à Londres

A venir

- 34C3 - 27-30 décembre à Leipzig

Divers / Trolls velus

Divers / Trolls velus

La commission européenne lance un Bug Bounty sur VLC

- Par la plateforme américaine HackerOne

  https://joinup.ec.europa.eu/news/hackerone-vlc

> **The European Commission has launched its first ever bug bounty. It will award between EUR 100 and EUR 3000 for bugs found in VLC media player. The programme will run until the first weeks of January or until the bounty budget is exhausted.**
>
> Which bugs will qualify for an award is at the discretion of the VLC team, according to the announcement by HackerOne, a commercial bug bounty platform. "Qualified security vulnerabilities will be rewarded based on severity and impact," HackerOne says.

Quad9 un résolveur DNS qui ne ment pas et protège l'internaute

- "Quoi de neuf"

  https://www.nextinpact.com/news/105638-quad9-resolveur-dns-ouvert-qui-veut-vous-proteger-en-respectant-votre-vie-privee.htm

Divers / Trolls velus

Mauvaise journée pour OVH

- Panne avec de lourdes conséquences d'indisponibilités

  http://www.zdnet.fr/actualites/mega-panne-ovh-3-millions-de-sites-potentiellement-touches-incident-en-cours-de-resolution-39859762.htm

- Le malheur des uns…

  https://twitter.com/online_fr/status/933795549639299080

Le blues du pentester

- Des vieilles vulnérabilités encore présentes partout (SQLi)
- Rapports non lus
- Failles non corrigées
- Pas de compétences sécurité chez les opérationnels ou les clients
  - Nous ne partageons pas de constats

  https://medium.com/@deusexmachina667/dealing-with-security-nihilists-b08e9f87052c

Divers / Trolls velus

iCon, le préservatif connecté arrive vraiment

- Sorte d'élastique à positionner à la base du pénis
- Mesure les performances : vitesse, durée, fréquence… !!?

http://geeko.lesoir.be/2017/11/29/le-premier-preservatif-connecte-arrive-sur-le-marche/

Le skimming fait par des enfants !!?

- Et surement avec une imprimante 3D

https://twitter.com/darksim905/status/939555682478682113/photo/1

Divers / Trolls velus

Les stages MinDef (Commision Armées-Jeunesse)

https://twitter.com/newsoft/status/934009406332825600/photo/1

- Programmation ACCESS, VBA et rédaction documents
  http://www.stages.defense.gouv.fr/index.php?page=StageVisualisationPage&stage=5457&parent=FrancePage&pc=2
- CONCEPTION D'UN SIMULATEUR PEDAGOGIQUE DE MODEM
  http://www.stages.defense.gouv.fr/index.php?page=StageVisualisationPage&stage=5552&$parent=FrancePage&pc=2
- MISE EN CONFORMITE DE LOGICIEL EN VB.NET
  http://www.stages.defense.gouv.fr/index.php?page=StageVisualisationPage&stage=5390&$parent=FrancePage&pc=2
- Intégrer un formulaire de recherche dans Drupal 8
  http://www.stages.defense.gouv.fr/index.php?page=StageVisualisationPage&stage=5564&$parent=FrancePage&pc=2
- Et au milieu de tout ça, on trouve : Deep learning et images sonar de synthèse
  http://www.stages.defense.gouv.fr/index.php?page=StageVisualisationPage&stage=5518&parent=FrancePage&pc=1

Prochains rendez-vous de l’OSSIR

Prochaine réunion

- Mardi 9 janvier 2018

After Work

- Toujours pas...

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous