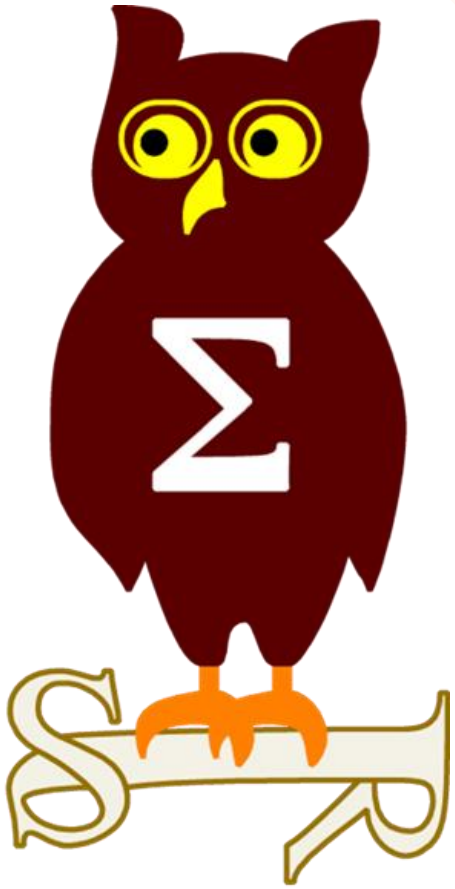
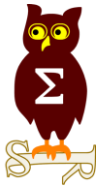


Revue d'actualité

09/04/2019

Préparée par

*Arnaud **S**OULLIE @arnaudsoullie*
*Étienne **B**audin @etiennebaudin*



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (NMMSBGA)

Microsoft - Avis

MS19-018 Vulnérabilités dans Internet Explorer (15 CVE)

- Exploit:
  - 3 x Security Feature Bypass
  - 9 x Remote Code Execution
  - 2 x Information Disclosure
  - 1 x Spoofing
- Crédits:
  - ? (CVE-2019-0761, CVE-2019-0780)
  - Nafiez (CVE-2019-0763)
  - James Forshaw of Google Project Zero (CVE-2019-0768)
  - Soyeon Park and Wen Xu from SSLab at Georgia Tech (CVE-2019-0609)
  - bo13oy of Qihoo 360 Vulcan Team (CVE-2019-0746)
  - Prakash of Threat Nix (CVE-2019-0762)
  - Steven Hunter of MSRC Vulnerabilities & Mitigations (CVE-2019-0783)
  - Yuki Chen of Qihoo 360 Vulcan Team (CVE-2019-0665, CVE-2019-0666, CVE-2019-0680, CVE-2019-0606)
  - Ivan Fratric of Google Project Zero (CVE-2019-0667)
  - Clement Lecigne of Google's Threat Analysis Group (CVE-2019-0676)
  - Jonathan Birch of Microsoft Corporation (CVE-2019-0654)

MS19-019 Vulnérabilités dans Edge (35 CVE)

- Exploit:
  - 3 x Security Feature Bypass
  - 23 x Remote Code Execution
  - 6 x Information Disclosure
  - 2 x Elevation of Privilege
- Crédits:
  - ? (CVE-2019-0780, CVE-2019-0634, CVE-2019-0644)
  - bo13oy of Qihoo 360 Vulcan Team (CVE-2019-0746)
  - Bruno Keith (@bkth_) working Trend Micro's Zero Day Initiative (CVE-2019-0593)
  - dannywei of Tencent Security Xuanwu Lab (CVE-2019-0643)
  - dwfault of ADLab of Venustech (CVE-2019-0607)
  - Hearmen of Tencent Security Xuanwu Lab (CVE-2019-0642)
  - Ivan Fratric of Google Project Zero (CVE-2019-0612, CVE-2019-0641)
  - Jihui Lu of Tencent KeenLab (CVE-2019-0645)
  - Jonathan Birch of Microsoft Corporation (CVE-2019-0654)
  - MoonLiang of Tencent Security Xuanwu Lab (CVE-2019-0640, CVE-2019-0590, CVE-2019-0591)
  - Nikhil Mittal of Payatu Labs (CVE-2019-0678)
  - Prakash of Threat Nix (CVE-2019-0762)
  - Qixun Zhao of Qihoo 360 Vulcan Team (CVE-2019-0651, CVE-2019-0605, CVE-2019-0769, CVE-2019-0770, CVE-2019-0771)
  - Soyeon Park and Wen Xu from SSLab at Georgia Tech (CVE-2019-0609)
  - Yuki Chen of Qihoo 360 Vulcan Team (CVE-2019-0610, CVE-2019-0649, CVE-2019-0652, CVE-2019-0655, CVE-2019-0658, CVE-2019-0611, CVE-2019-0639, CVE-2019-0773, CVE-2019-0592)

Dont 5 communes avec IE:

- CVE-2019-0609
- CVE-2019-0654
- CVE-2019-0746
- CVE-2019-0762
- CVE-2019-0780

Failles / Bulletins / Advisories (NMMSBGA)

Microsoft - Avis

MS19-020 Vulnérabilités dans .NET Framework (2 CVE)

- Exploit:
  - 1 x Spoofing
  - 1 x Remote Code Execution
- Crédits:
  - Jonathan Birch of Microsoft Corporation (CVE-2019-0657)
  - Soroush Dalili of NCC Group (CVE-2019-0613)

MS19-021 Vulnérabilités dans Microsoft Office (8 CVE)

- Exploit:
  - 2 x Security Feature Bypass
  - 6 x Remote Code Execution
- Crédits:
  - Bar Lahav and Gal De Leon of Palo Alto Networks (CVE-2019-0748)
  - Pieter Ceelen & Stan Hegt of Outflank (CVE-2019-0540)
  - rgod of 9sg Security Team - rgod@9sgsec.com working Trend Micro's Zero Day Initiative (CVE-2019-0671, CVE-2019-0672, CVE-2019-0673, CVE-2019-0674)
  - Gal De Leon and Bar Lahav of Palo Alto Networks (CVE-2019-0675)
  - Jinquan of 360CoreSec (CVE-2019-0669)

Failles / Bulletins / Advisories (NMMSBGA)

Microsoft - Avis

MS19-022 Vulnérabilités dans Microsoft Windows (14 CVE)

- Affectés : Toutes versions
- Exploit:
  - 1 x Denial of Service
  - 4 x Remote Code Execution
  - 2 x Elevation of Privilege
  - 3 x Information Disclosure
  - 4 x Security Feature Bypass
- Crédits:
  - ? (CVE-2019-0754, CVE-2019-0636, CVE-2019-0637)
  - @j00sean based on the previous work of @magicmac2000 (CVE-2019-0765)
  - Wayne Low of Fortinet's FortiGuard Labs (CVE-2019-0766)
  - Yuki Chen of Qihoo 360 Vulcan Team (CVE-2019-0772)
  - Anonymous working Trend Micro's Zero Day Initiative (CVE-2019-0784)
  - John Simpson working Trend Micro's Zero Day Initiative (CVE-2019-0603)
  - Wayne Low of Fortinet's FortiGuard Labs (CVE-2019-0659)
  - Lucas Leong (@_wmliang_) working Trend Micro's Zero Day Initiative (CVE-2019-0600, CVE-2019-0601)
  - Matt Graeber of SpecterOps (CVE-2019-0627, CVE-2019-0631, CVE-2019-0632)
  - Jihui Lu of Tencent KeenLab (CVE-2019-0565)

MS19-023 Vulnérabilités dans Windows Kernel-Mode Drivers (1 CVE)

- Affectés : Toutes versions
- Exploit:
  - 1 x Information Disclosure
- Crédits:
  - JunGu and ZiMi of Alibaba Orion Security Lab (CVE-2019-0776)

Failles / Bulletins / Advisories (NMMSBGA)

Microsoft - Avis

MS19-024 Vulnérabilités dans Windows Kernel (12 CVE)

- Affectés : Toutes versions
- Exploit:
  - 9 x Information Disclosure
  - 3 x Elevation of Privilege
- Crédits:
  - Piotr Krysiuk of Symantec (CVE-2019-0755)
  - ZiMi and JunGu of Alibaba Orion Security Lab (CVE-2019-0767, CVE-2019-0775, CVE-2019-0782, CVE-2019-0702)
  - Axel Souchet (@0vercl0k) of MSRC Vulnerabilities and Mitigations Team (CVE-2019-0696)
  - guangmingliu of Tencent ZhanluLab (CVE-2019-0623)
  - JunGu and ZiMi of Alibaba Orion Security Lab (CVE-2019-0628)
  - bee13oy of Qihoo 360 Vulcan Team (CVE-2019-0656)
  - ZiMi and JunGu of Alibaba Orion Security Lab (CVE-2019-0661, CVE-2019-0621, CVE-2019-0663)

MS19-025 Vulnérabilités dans Microsoft XML (1 CVE)

- Affectés : Toutes versions
- Exploit:
  - 1 x Remote Code Execution
- Crédits:
  - Yuki Chen of Qihoo 360 Vulcan Team (CVE-2019-0756)

Failles / Bulletins / Advisories (NMMSBGA)

Microsoft - Avis

MS19-026 Vulnérabilités dans Windows Print Spooler Components (1 CVE)

- Affectés : Toutes versions
- Exploit:
  - 1 x Information Disclosure
- Crédits:
  - Ke Liu of Tencent Security Xuanwu Lab (CVE-2019-0759)

MS19-027 Vulnérabilités dans Microsoft Graphics Component (12 CVE)

- Affectés : Toutes versions
- Exploit:
  - 8 x Information Disclosure
  - 4 x Elevation of Privilege
- Crédits:
  - riusksk of VulWar Corp working Trend Micro's Zero Day Initiative (CVE-2019-0774, CVE-2019-0614, CVE-2019-0660)
  - (Vasily Berdnikov) of Kaspersky Lab / (Boris Larin) of Kaspersky Lab (CVE-2019-0797)
  - Clément Lecigne of Google's Threat Analysis Group (CVE-2019-0808)
  - Fei Shu at Network Security Laboratory of State Grid Xinjiang Electric Power Research Institute (CVE-2019-0662)
  - Behzad Najjarpour Jabbari, Secunia Research at Flexera (CVE-2019-0664, CVE-2019-0618)
  - riusksk of VulWar Corp working Trend Micro's Zero Day Initiative (CVE-2019-0602, CVE-2019-0616, CVE-2019-0619)
  - Lin Wang of Beihang University working Trend Micro's Zero Day Initiative (CVE-2019-0615)

MS19-028 Vulnérabilités dans Skype for Business (1 CVE)

- Exploit:
  - 1 x Spoofing
- Crédits:
  - Malte Batram (CVE-2019-0798)

Failles / Bulletins / Advisories (NMMSBGA)

Microsoft - Avis

MS19-029 Vulnérabilités dans Office SharePoint (5 CVE)

- Affectés : Toutes versions
- Exploit:
  - 1 x Tampering
  - 1 x Elevation of Privilege
  - 1 x Spoofing
  - 2 x Remote Code Execution
- Crédits:
  - ? (CVE-2019-0778, CVE-2019-0670)
  - Ashar Javed of Hyundai AutoEver Europe GmbH (CVE-2019-0668)
  - Markus Wulftange working Trend Micro's Zero Day Initiative (CVE-2019-0594, CVE-2019-0604)

MS19-030 Vulnérabilités dans Microsoft JET Database Engine (7 CVE)

- Affectés : Toutes versions
- Exploit:
  - 7 x Remote Code Execution
- Crédits:
  - rgod of 9sg Security Team - rgod@9sgsec.com working Trend Micro's Zero Day Initiative (CVE-2019-0617, CVE-2019-0625, CVE-2019-0595, CVE-2019-0596, CVE-2019-0597, CVE-2019-0598, CVE-2019-0599)

MS19-031 Vulnérabilités dans Active Directory (1 CVE)

- Affecte : Windows 7 et Server 2008
- Exploit:
  - 1 x Elevation of Privilege
- Crédits:
  - Will Schroeder (@harmi0y) of SpecterOps (CVE-2019-0683)

Failles / Bulletins / Advisories (NMMSBGA)

Microsoft - Avis

MS19-032 Vulnérabilités dans Windows Subsystem for Linux (5 CVE)

- Affectés : Windows 10 et Server 2019 / 1709 / 1803
- Exploit:
  - 5 x Elevation of Privilege
- Crédits:
  - Anthony LAOU HINE TSUEI (CVE-2019-0682, CVE-2019-0689, CVE-2019-0692, CVE-2019-0693, CVE-2019-0694)

MS19-033 Vulnérabilités dans Windows Hyper-V (4 CVE)

- Affectés : Toutes versions
- Exploit:
  - 3 x Denial of Service
  - 1 x Information Disclosure
- Crédits:
  - Marcel de Wijs (CVE-2019-0690)
  - Shawn Denbow of Windows Security Team (CVE-2019-0695)
  - ? (CVE-2019-0701)
  - Peter Hlavaty (@zer0mem), KeenLab at Tencent (CVE-2019-0635)

MS19-034 Vulnérabilités dans Microsoft Exchange Server (2 CVE)

- Exploit:
  - 2 x Elevation of Privilege
- Crédits:
  - n1nty and pr0mise @ 360 A-TEAM (CVE-2019-0686, CVE-2019-0724)

Failles / Bulletins / Advisories (NMMSBGA)

Microsoft - Avis

MS19-032 Vulnérabilités dans Windows Subsystem for Linux (5 CVE)

- Affectés : Windows 10 et Server 2019 / 1709 / 1803
- E
- C

-0694)

MS1

- A
- E
- C

MS1

- E
- Credits:
  - n1nty and pr0mise @ 360 A-TEAM (CVE-2019-0686, CVE-2019-0724)

OSSIR - 2019-02-12

Un chercheur publie une série de comportements par défaut permettant de devenir administrateur de domaine à partir d'une boite mail compromise

- Abus de la fonctionnalité Exchange Web Services (EWS) pour s'authentifier sur un serveur de l'attaquant avec le compte du serveur Exchange
- Authentification réalisée via NTLM envoyés par HTTP (vol du hash NTLM et possibilité d'attaques par relai)
- Les serveurs Exchange sont installés avec des privilèges trop élevés

https://www.zdnet.com/article/microsoft-exchange-vulnerable-to-privexchange-zero-day/

Failles / Bulletins / Advisories (NMMSBGA)

Microsoft - Avis

MS19-035 Vulnérabilités dans Windows DHCP (4 CVE)

- Affectés : Toutes versions
- Exploit:
  - 4 x Remote Code Execution
- Crédits:
  - Mikhail Tsvetkov of Positive Technologies (CVE-2019-0697)
  - Mitch Adair, Microsoft Windows Enterprise Security Team (CVE-2019-0698)
  - Mark Barnes (@incanus) of MWR Labs (CVE-2019-0726)
  - Brandon Falk (@gamozolabs) of the Enterprise Team (CVE-2019-0626)

MS19-036 Vulnérabilités dans Windows SMB Server (5 CVE)

- Affectés : Toutes versions
- Exploit:
  - 3 x Information Disclosure
  - 2 x Remote Code Execution
- Crédits:
  - Andrew Burkhardt of MSRC Vulnerabilities & Mitigations Team (CVE-2019-0703, CVE-2019-0704)
  - ? (CVE-2019-0821)
  - ASD (CVE-2019-0630)
  - Peter Hlavaty (@zer0mem), KeenLab at Tencent (CVE-2019-0633)

Failles / Bulletins / Advisories (NMMSBGA)

Microsoft - Avis

MS19-037 Vulnérabilités dans Visual Studio (2 CVE)

- Affectés : Toutes versions
- Exploit:
  - 2 x Remote Code Execution
- Crédits:
  - ? (CVE-2019-0809)
  - Sven Nobis of ERNW GmbH (CVE-2019-0728)

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**

Support de SHA-2 requis pour la signature des mises à jour

- updates dédiées à installer **d’ici juillet**

Failles / Bulletins / Advisories

Microsoft - Autre

Déni de service sur IIS Server

- erreur dans la gestion des requêtes HTTP/2

  https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV190005

Double 0-day sur IE, Edge

- permet de contourner le mécanisme de Same Origin Policy
- POC disponible

  https://securityaffairs.co/wordpress/83080/hacking/microsoft-browser-zero-day.html

Un code d'exploitation publié pour Internet Explorer

- vulnérabilité corrigée en janvier
- RCE

  https://cxsecurity.com/issue/WLB-2019030135

Un code d'exploitation publié pour Windows 10, Server 1709, 1803, 2019

- vulnérabilité corrigée en mars
- DOS via DHCP

  https://labs.mwrinfosecurity.com/advisories/windows-dhcp-client/

Failles / Bulletins / Advisories

Microsoft - Autre

Des attaques massives sur le protocole IMAP ont permis de contourner l'authentification à facteurs multiples sur des comptes Office 365 et G Suite

- MFA peut être contourné avec IMAP sous certaines conditions
- 100 000 connexions non autorisées sur des millions de compte

https://www.proofpoint.com/us/threat-insight/post/threat-actors-leverage-credential-dumps-phishing-and-legacy-email-protocols

Failles / Bulletins / Advisories

Système (principales failles)

72 vulnérabilités corrigées sur Adobe Acrobat

- RCE, EOP, Vol d'informations

  https://helpx.adobe.com/security/products/acrobat/apsb19-07.html

  https://helpx.adobe.com/security/products/acrobat/apsb19-13.html

RCE sur Jenkins Declarative, Groovy et Script Security

- deux vulnérabilités affectant la mauvaise gestion de l'annotation @Grab
- code d'exploitation disponible

  https://www.exploit-db.com/exploits/46453

Vol de secret sur Spring

- défaut de contrôle au sein du paramètre "redirect_uri" utilisé lors de l'authentification.
- un attaquant pouvait rediriger sa victime vers un site dont il a le contrôle afin de récupérer son code d'autorisation.

  https://pivotal.io/security/cve-2019-3778

Vol d'informations sur OpenSSL

- oubli de mise à jour du contexte au sein des fonctions ssl3_send_alert, ssl3_read_bytes et dtls1_read_bytes lors d'une suppression de session liée au traitement d'une erreur fatale.

  https://www.openssl.org/news/secadv/20190226.txt

Failles / Bulletins / Advisories

Système (principales failles)

snapD - Dirty Socks

- erreur de traitement et manque de validation de l'adresse du socket distant lors de l'exécution des contrôles d'accès sur le socket UNIX. Code d’exploitation disponible
- Un attaquant local peut obtenir un accès privilégié à l'API snapd puis obtenir un accès administrateur à la machine.

https://usn.ubuntu.com/3887-1/

Google Chrome

- Use-after-free permettant une prise de contrôle du système
- exploitation observées sur Internet

https://chromereleases.googleblog.com/2019/03/stable-channel-update-for-desktop.html

Adobe Coldfusion

- erreur non spécifiée lors de l’upload de fichiers permettant une prise de contrôle du système
- campagnes d’attaques observées

https://helpx.adobe.com/security/products/coldfusion/apsb19-14.html

Apache HTTPd

- 6 vulnérabilités corrigées (exéc de code, contournement de sécurité, etc.),
- code d’exploitation prochainement publié

https://httpd.apache.org/security/vulnerabilities_24.html

Failles / Bulletins / Advisories

Système (principales failles)

RCE via une vulnérabilité au sein de WinRAR

- absence de traitement du dossier de destination par une bibliothèque obsolète, utilisée par WinRAR
- à l'aide d'une archive .RAR malveillante au format ACE, il était possible d’écrire des fichiers à des emplacements arbitraires sur le système de la victime
- Attaques massives observées

https://research.checkpoint.com/extracting-code-execution-from-winrar/

RCE sur Drupal

- catégorisé “Highly Critical”
- manque de validation des données sur certains types de champs non spécifiés
- installation des versions 8.6.10 ou 8.5.11 recommandée, pas d’update nécessaire pour la version 7 mais un update de plugins recommandée
- Exploit disponible, attaques massives...

https://www.drupal.org/sa-core-2019-003

To immediately mitigate the vulnerability, you can disable all web services modules, or configure your web server(s) to not allow **GET**/PUT/PATCH/POST requests to web services resources. Note

Failles / Bulletins / Advisories

Système (principales failles)

2 vulnérabilités au sein de Wordpress

- Prise de contrôle d'un système via une erreur de vérification des permissions des images JPG et d'assainissements des fichiers image contenant deux extensions
- code d'exploitation disponible

https://wordpress.org/news/2019/02/betty/

1 nouvelle vulnérabilité sur les processeurs Intel

- Appelée Spoiler, tous les Intel Core touchés
- liée à l'exécution spéculative

https://arxiv.org/pdf/1903.00446.pdf

Les dix image docker les plus utilisées contiennent au moins 30 vulnérabilités chacune

- Node.js contient à lui seul 580 vulnérabilités
- suivi par postgres à 89 vulnérabilités puis nginx à 85
- le reste autour de 50 vulnérabilité excepté ubuntu à 30

https://snyk.io/blog/top-ten-most-popular-docker-images-each-contain-at-least-30-vulnerabilities/

Failles / Bulletins / Advisories

Système (principales failles)

6 vulnérabilités au sein de produits VMware (Workstation, ESXi, Fusion)

- élévation de privilèges sur la machine hôte via des erreurs de gestion des classes COM et des chemins réseau par le processus VMX, rce via une API sans auth sur Fusion

https://www.vmware.com/security/advisories/VMSA-2019-0002.html

https://www.vmware.com/security/advisories/VMSA-2019-0005.html

3 vulnérabilités au sein de Zimbra

- désérialisation et configuration incorrecte de parsers XML (XXE)
- => exécution de code arbitraire, lecture et manipulation de données

https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories

23 vulnérabilités au sein de Firefox

- provenant de diverses erreurs au sein de plusieurs composants et paramètres du navigateur Firefox (use-after-free, corruption de la mémoire, manque de validation, ...)

https://www.mozilla.org/en-US/security/advisories/mfsa2019-07/

https://www.mozilla.org/en-US/security/advisories/mfsa2019-10/

https://www.mozilla.org/en-US/security/advisories/mfsa2019-09/

37 vulnérabilités au sein de Magento

- menant à divers dommages allant d'une vol d'informations à une RCE
- exploit publié par Ambionics (Lexfo) pour une SQLi

https://magento.com/security/patches/magento-2.3.1-2.2.8-and-2.1.17-security-update

Failles / Bulletins / Advisories

Réseau (principales failles)

RCE sur VPN Cisco

- lié au traitement des entrées sur l'interface
- pas d'authentification nécessaire, permet d'obtenir des privilèges élevés

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190227-rmi-cmd-ex

RCE sur Cisco WebEx

- lié au mécanisme de mise à jour
- nécessite d'être authentifié et d'être en local
- code d'exploitation disponible

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190227-wmda-cmdinj

21 vulnérabilités sur Cisco NX-OS

- menant à de l'exécution de code locale pour certaines

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-sig-verif
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-privesca
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-privesc
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-pe
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-npv-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-netstack
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-file-access
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-fabric-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-escalation
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-cmdinj-1613
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-cmdinj-1612
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-cmdinj-1611
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-cmdinj-1610
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-cmdinj-1609
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-cmdinj-1608
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-cmdinj-1607
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-cmdinj-1606
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-NXAPI-cmdinj
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nx-os-lan-auth
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nx-os-bash-escal

Failles / Bulletins / Advisories

Hardware / IoT

36 vulnérabilités découvertes dans le protocole LTE

- vie LTEFuzz développé par l'Institut supérieur coréen des sciences et technologies
- dues au non chiffrement des communications du protocole RRC et à l'absence de contrôle d'intégrite sur celui-ci
- => possible de déconnecter un utilisateur du réseau LTE, de se faire passer pour un autre utilisateur, de forcer l'utilisateur à se connecter à un réseau LTE malveillant et d'intercepter les SMS d'une cible

https://syssec.kaist.ac.kr/pub/2019/kim_sp_2019.pdf

20 % des systèmes industriels seraient impactés par des vulnérabilités jugées critiques

- d'après Karspesky Lab ICS
- +50% des 415 vulnérabilités détectés disposaient d'un score CVSS > 7
- secteur de l'énergie, l'approvisionnement en eau, des chaînes de nourriture, agriculture
- 342 vulnérabilités seraient exploitables à distance sans authentification

https://www.bleepingcomputer.com/news/security/20-percent-of-industrial-control-systems-affected-by-critical-vulnerabilities/

Failles / Bulletins / Advisories

Android / iOS

128 vulnérabilités sur Android

- RCE, EOP, ID, …
- dont exécution de code via un fichier malveillant

https://source.android.com/security/bulletin/2019-03-01

https://source.android.com/security/bulletin/2019-04-01

51 vulnérabilités sur iOS

- RCE, EOP, ID, …
- dont exécution de code via un SMS

https://support.apple.com/en-us/HT209599

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Des enregistrements d'appels téléphoniques à un service de santé suédois ont été exposés durant 6 ans

- données en libre accès depuis 2013 sur un serveur hébergé par un sous-traitant
- 2,7 millions d'appels, pour un total de 170 000 heures de conversation
- le serveur est desormais indisponible

https://www.bleepingcomputer.com/news/security/27-million-health-related-calls-sensitive-info-exposed-for-six-years/

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Le fournisseur de messagerie VFEmail victime d'une attaque destructrice

- incident remonté par Twitter le 11 février
- les serveurs basés sur différents OS avec credentials différents dans plusieurs datacenter hors service
- Toutes les données perdues à l'exception d'un serveur aux Pays-Bas

https://krebsonsecurity.com/2019/02/email-provider-vfemail-suffers-catastrophic-hack

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Vol de 13 millions d'euros suite à une cyber attaque à l'encontre de la banque maltaise Valletta (BOV)

- fermeture de la banque pendant 1 journée
- Nouvelle fermeture

https://www.timesofmalta.com/articles/view/20190213/local/bank-of-valletta-goes-dark-after-detecting-cyber-attack.701896

Des informations supplémentaires sont disponibles sur la fuite de données de Mariott

- 383 millions de données clientes ;
- 18,5 millions de numéros de passeports chiffrés;
- 5,25 millions de numéros de passeport en clair;
- 9,1 millions de données bancaires chiffrées;
- Des milliers de données bancaires non chiffrées

https://www.helpnetsecurity.com/2019/03/12/marriott-data-breach-details/

Une base de données divulguée sur Internet liste les femmes chinoises disposées à procréer

- informations personnelles de 2 millions de femmes, de 15 à 95 ans, célibataires, divorcées ou veuves, majoritairement à Pekin
- application de rencontre ou registre gouvernematal supposé à l'origine de la fuite
- une fuite similaire en inde => https://securitydiscovery.com/large-privacy-breach-in-india/

https://twitter.com/0xDUDE/status/1104528181846032385/

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Fuite d'informations sur la plateforme Box.com

- Plusieurs TB sur plusieurs sous domaines (https://companyname.account.box.com) identifiés avec :
  - Des centaines de photos de passeport
  - Des numéros de sécurité sociale et des numéros de compte bancaire
  - Des prototypes de haute technologie et des fichiers de conception
  - Des listes d'employés
  - Des données financières, factures, suivi de problèmes internes
  - Des liste de clients et archives des années de réunions internes
  - Des données informatiques, configurations VPN, schémas de réseau

https://twitter.com/0xDUDE/status/1104528181846032385/

Facebook stockait le mode passe de centaines de millions d'utilisateurs en clair

- découvert lors d'audit interne en janvier
- des mots de passe en clair accessible à environ 20 000 employés
- 2 000 ingénieurs ont effectivement accédé aux données
- données disponible depuis 2012

https://newsroom.fb.com/news/2019/03/keeping-passwords-secure/

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

540 millions d'identifiants Facebook rendus publics sur des serveurs Amazon

- identifié par la société UpGuard
- Bucket S3 accessible sans authentification
- 146 Go : identifiants, réactions, commentaires, etc.
- 22 000 mots de passe en clair issues d'une application Tierce nommé "At the Pool"

https://www.upguard.com/breaches/facebook-user-data-leak

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Un Lituanien escroque Facebook et Google en leur faisant payer 172 millions de dollars de fausses factures

- via des mails de phishing conçus pour ressembler à des factures d'une société de matériel informatique
- il risque jusqu'à 30 ans de prison. Facebook et Google ont pu récupérer l'argent dérobé.

https://www.news.com.au/finance/business/technology/lithuanian-man-tricks-facebook-and-google-into-paying-172-million-worth-of-fake-invoices/news-story/e96e3d30652e27d9ff03a6085715ba7b

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Norsk Hydro, victime du ransomware LockerGoga

- attaque le 18 mars
- conférence le 19 mars pour déclarer l'incident
- production ralentie, certains site revenus à des processus manuels
- conférence le 26 mars pour annoncer la fin de l'incident, reprise complète de la production en cours et pertes d'environ 40 millions de dollars
- applaudie par la communauté pour sa transparence
  - site web temporaire
  - communication à la presse
  - communication interne
  - webcast journalier avec des responsables de la société et prise de questions des spectateurs
  - vidéo publiée pour communiquer autour de l'évènement
  - etc.

https://www.reuters.com/article/us-norsk-hydro-cyber/aluminum-producer-hydro-hit-by-cyber-attack-shuts-some-plants-idUSKCN1R00NJ

https://www.zdnet.com/article/norsk-hydro-ransomware-incident-losses-reach-40-million-after-one-week/

https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880

Piratages, Malwares, spam, fraudes et DDoS

Espionnage

DNSPIONAGE

- Attaques *depuis plusieurs mois* sur l'infrastructure DNS dans divers pays
- début en février 2017
- l'attaquant cherche à rediriger le trafic destiné à certains sites vers ses propres systèmes
- Les sociétés et les entités gouvernementales de pays du Moyen-Orient ciblés dans une attaque récente
- L'ICANN appelle au déploiement massif de DNSSEC
- Info relayée massivement en France

https://www.icann.org/news/announcement-2019-02-15-en

https://www.icann.org/news/announcement-2019-02-22-en

Citrix victime d'une intrusion par un groupe iranien

- 6 TB dérobé
- Citrix prévenu par le FBI du vol de donnée
- pas de rupture de service ou de produit affecté

https://www.bleepingcomputer.com/news/security/citrix-learns-about-internal-network-security-breach-from-fbi/

Piratages, Malwares, spam, fraudes et DDoS
Espionnage

Campagne d'attaques orchestrée par le groupe APT10 (associé au gouvernement chinois)

- découvert par Insikt Group et Rapid7
- effective entre nov 2017 et sept 2018.
- 3 sociétés européénne ciblés : une société d'hébergement, un fabricant de vêtement et un cabinet d'avocat dont les clients sont dans des secteurs stratégique (pharmaceutique, électronique, automobile et biomédical)
- Données sensibles exfiltrées

https://www.recordedfuture.com/apt10-cyberespionage-campaign/

Campagne d'attaques orchestrée par le groupe APT28 (associé au gouvernement russe)

- découvert par Microsoft
- effective entre oct 2018 et dec 2018 dans 12 pays
- spearphishing utilisé sur des organisations politiques européenne
- impact non indiqué

https://www.zdnet.com/article/microsoft-reveals-new-apt28-cyber-attacks-against-european-political-entities/

Mozilla envisage de ne plus considérer les certificats émis par DarkMatter comme dignes de confiance

- Suite à l'implication de DarkMatter dans une opération offensive par les Emirats arabes unis

https://mobile.reuters.com/article/amp/idUSKCN1QL28T

Piratages, Malwares, spam, fraudes et DDoS

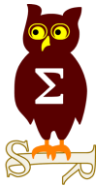
Espionnage

Asus annonce la compromission de son utilitaire de mise à jour par un groupe APT

- mécanisme de mise à jour pour “notebooks” compromis
- découvert par Kaspersky qui dit avoir vu près de +1M machines compromises
- Asus de son côté indique qu’une poignée d’utilisateur étaient ciblés

https://www.bleepingcomputer.com/news/security/asus-admits-its-live-update-utility-was-backdoored-by-apt-group/

https://www.asus.com/News/hqfgVUyZ6uyAyJe1



Nouveautés, outils et techniques

Crypto et Divers

Divers

Le W3C adopte officiellement le standard WebAuthn pour remplacer les mots de passe

- But : remplacer le traditionnel mot de passe par une authentification biométrique, un appareil mobile ou une clé USB sécurisée.
- Sa prise en charge était déjà effective pour la plupart des navigateurs, son déploiement devrait désormais s'accélérer pour les sites web.

https://www.w3.org/2019/03/pressrelease-webauthn-rec.html

Heartbleed fête ses 5 ans

- Référencée CVE-2014-0160, elle a marqué les esprits avec un vol d'informations critiques sur un composant logiciel utilisé par tout le monde
- Un employé d'AWS a partagé un thread sur twitter détaillant leur mode de réaction : lancement du déploiement du hotfix en 1h, opération terminée en quelques heures. Pas d'impact clients.

Crypto et Divers

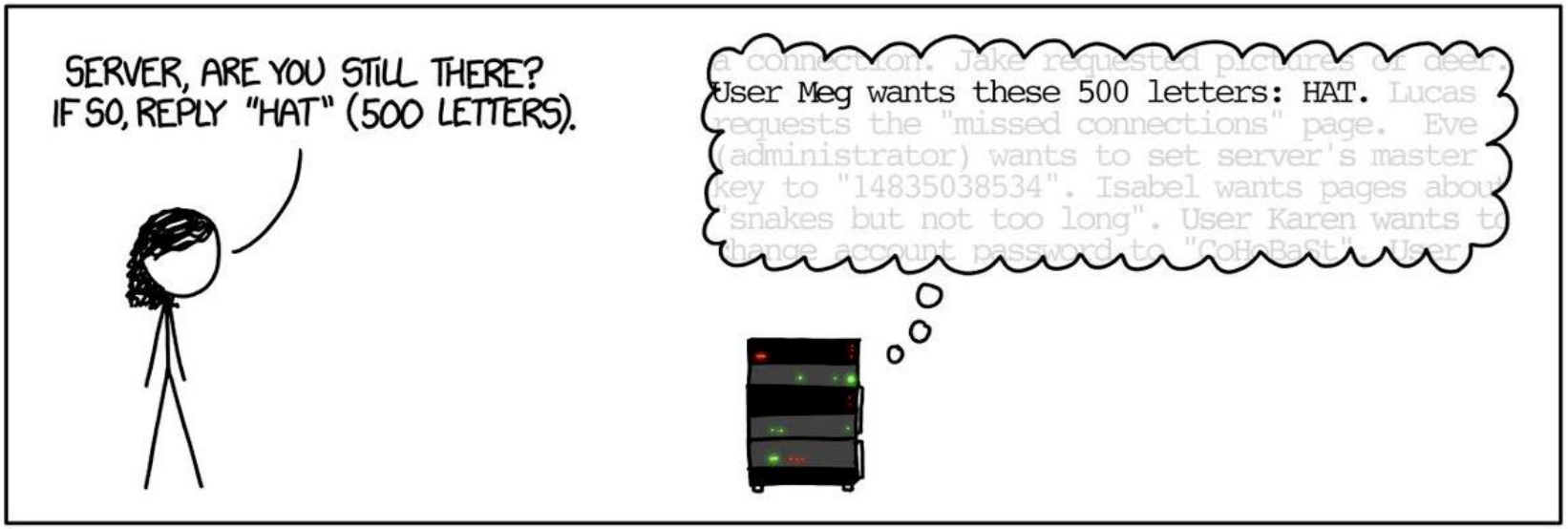
Divers

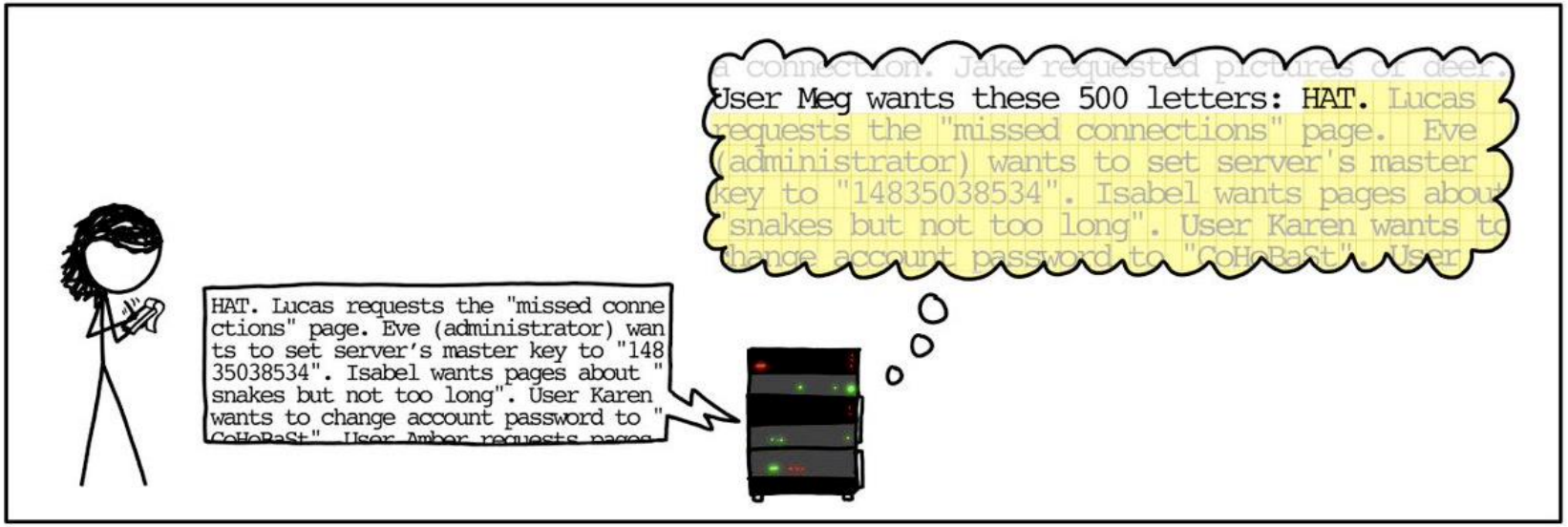
Le

- E
- S

Hea

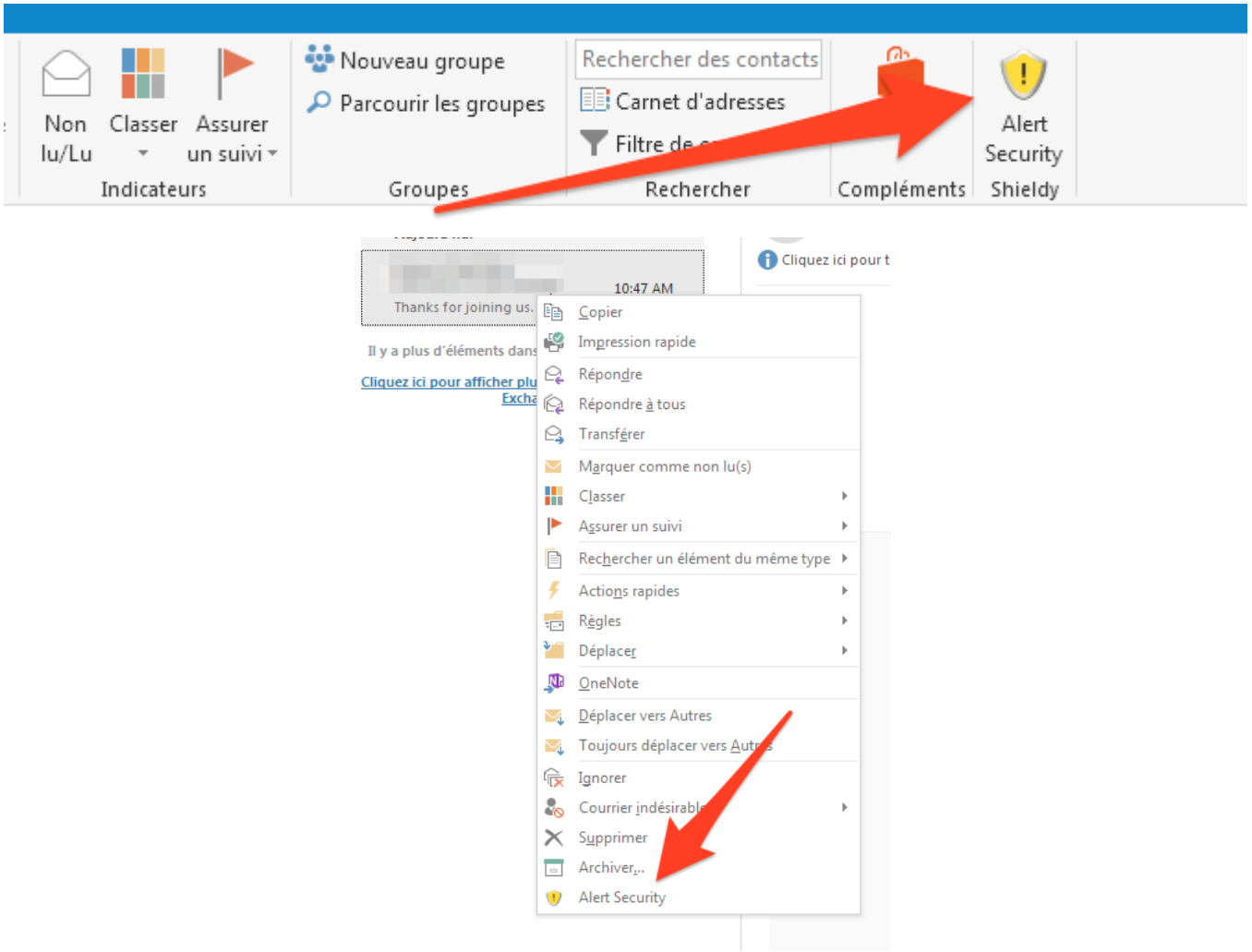
- F
- L





Le CERT-SG partage son add-in Outlook pour remonter les mails suspicieux

https://github.com/certsocietegenerale/NotifySecurity



La NSA partage son framework de RE Ghidra sur Github

https://github.com/NationalSecurityAgency/ghidra

FireEye partage sa VM windows pour du Pentest / Red Team

- nommée Commando VM

  https://github.com/fireeye/commando-vm

Pentest

Pirater les pirates

Business et Politique

Business

France

Business

International

NGINX racheté par F5

- pour 670 millions de dollars

  https://www.nginx.com/blog/nginx-joins-f5/

Droit / Politique

France

« Atelier RGPD » : La CNIL met en ligne sa formation d'initiation au règlement européen

- MOOC gratuit adressée principalement aux DPO
- 4 modules de 5h chacun
  - « Le RGPD et ses notions clés », abordant la définition de ce qu'est un traitement de données à caractère personnel ;
  - « Les principes de la protection des données », précisant notamment les 8 règles d'or à respecter ;
  - « Les responsabilités des acteurs, » et le partage de celles-ci avec les sous-traitants ;
  - « Le DPO et les outils de la conformité », précisant le rôle du délégué à la protection des données et notamment l'analyse d'impact sur la vie privée (Privacy Impact Assessment - PIA).

https://atelier-rgpd.cnil.fr/

Droit / Politique
International

Un rapport propose la mise en place d'un GDPR américain

- supporté par beaucoup de monde dont Apple

  https://www.zdnet.com/google-amp/article/gao-gives-congress-go-ahead-for-a-gdpr-like-privacy-legislation/

Adoption du règlement sur la cybersécurité par le parlement européen

- crée le premier dispositif de certification en matière de sécurité informatique à l'échelle européenne
- renforce le pouvoir de l'Agence européenne pour la sécurité des réseaux et de l'information (ENISA) qui dispose dorénavant d'un mandat permanent
  - nouveau rôle à l'agence, centré sur l'intensification de la coopération en matière de cybersécurité entre les pays de l'UE et donc davantage de ressources humaines et financières
- informer les utilisateurs européens sur l'importance et sur les manières de protéger leurs données

  http://www.europarl.europa.eu/doceo/document/A-8-2018-0264_FR.pdf

Conférences

Conférences

Passées

- Insomni’hack - 21 et 22 mars
- JSSI - 19 mars 2019
- GSDAYS - 2 avril 2019

A venir

- SSTIC - 13 au 15 juin 2018
- Pass the Salt - 2 au 4 juillet 2018

Divers / Trolls velus

Divers / Trolls velus

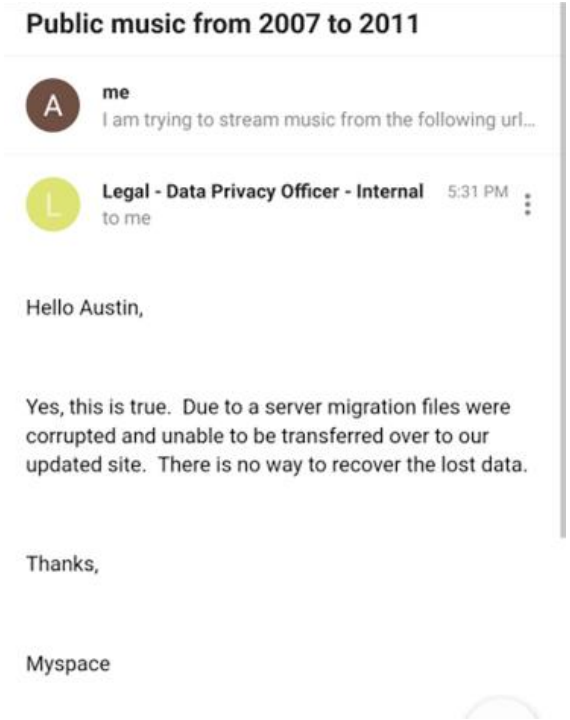
Les fonctions d'administration des trottinettes Xiaomi accessibles à distance sans authentification

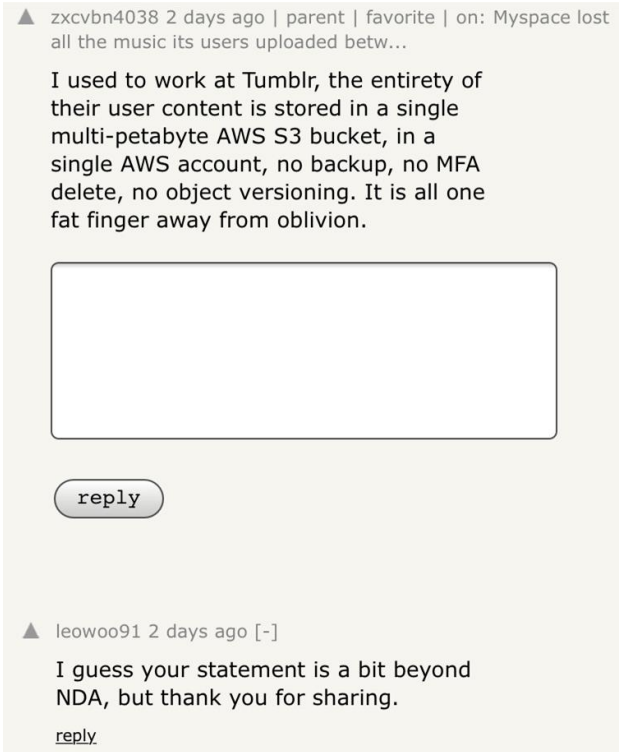
https://www.zdnet.com/article/xiaomi-electric-scooters-vulnerable-to-remote-hijacking/

MySpace perds 13 ans de données utilisateur lors d'une migration

- photos, chansons et vidéos uploadés entre 2003 et 2015 perdues
- Est-ce vraiment une mauvaise nouvelle ?

https://www.zdnet.fr/actualites/myspace-trebuche-sur-un-serveur-et-perd-13-ans-de-donnees-utilisateur-39882197.htm





Divers / Trolls velus

Veronique Loquet
@vloquet

Follow

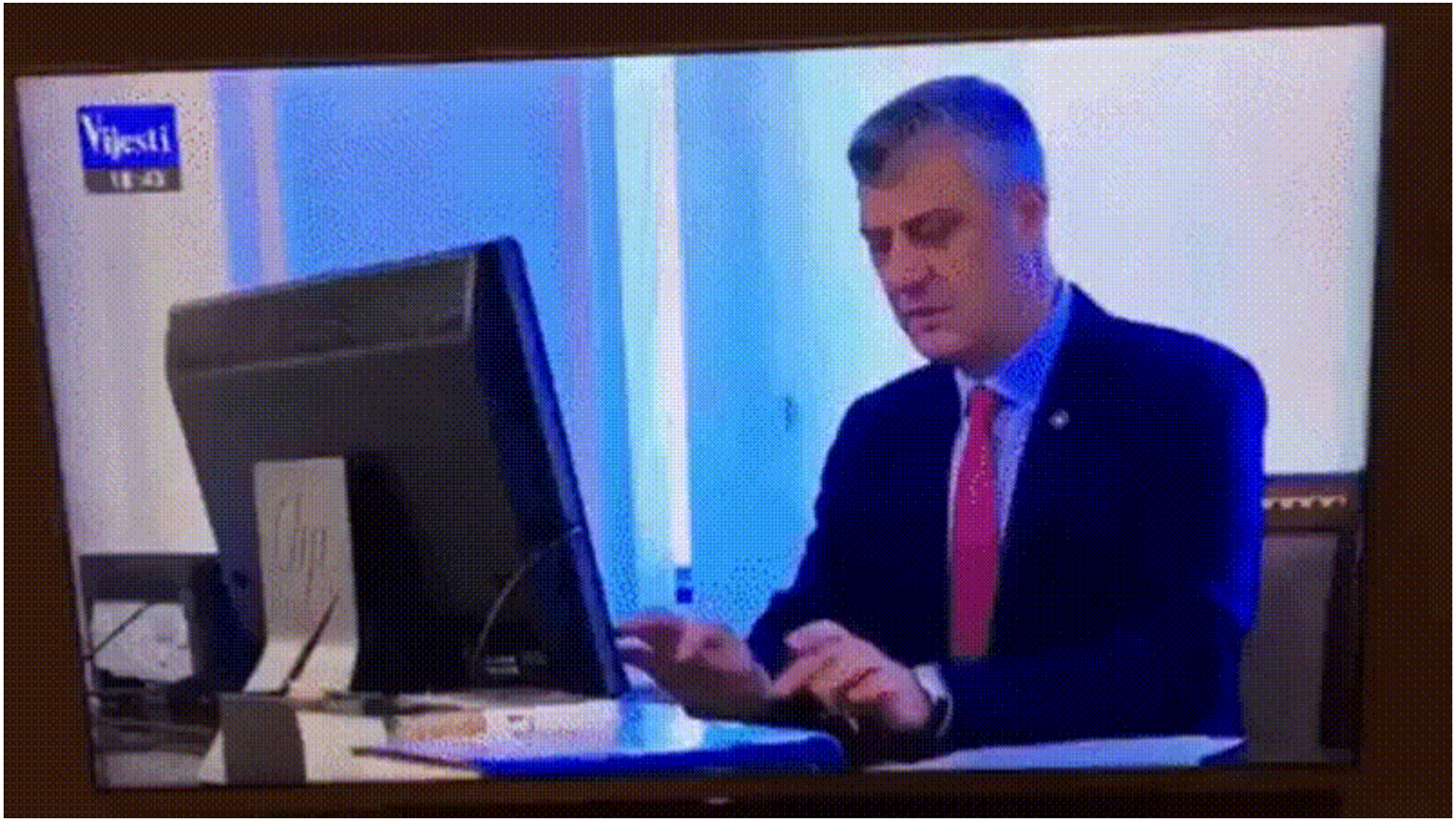
Quand @RTLFrance nous parle de backdoor, c'est de l'or ! #cybersecurite

"Quand on fait des tests, on voit bien qu'il y a des choses particulières dans le réseau des Chinois, comme les bagues d'or qui permettent de prendre et de regarder des choses sur un réseau à distance.

10:58 AM - 14 Mar 2019

228 Retweets **423** Likes

Divers / Trolls velus



https://external-preview.redd.it/GrXHiyTWjLozmWZFMubLPthk4ctFxEV7t2ATD3V2t6c.gif?format=mp4&s=01fef2439bd38055fdb643e60cedc155154af6e3

Divers / Trolls velus

Plus de 120 000 litres d’essences dérobés à cause d’un code de sécurité par défaut

- 5 hommes français arrêté pour avoir dérobé 120 000 litres (environ 150k€) dans des stations Total
- un mode opératoire :
  - une voiture passe et déverrouille la pompe avec le code 0000 #supersecure
  - une camionnette contenant une cuve dérobe le carburant

http://www.leparisien.fr/faits-divers/coup-de-frein-au-pillage-de-carburant-26-03-2019-8040411.php

Divers / Trolls velus

http://www.youtube.com/watch?v=XKr3Vb9ABHs

Prochains rendez-vous de l’OSSIR

Prochaines réunions

Prochaine réunion

- Mardi 14 mai 2019

After Work

- ?

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous