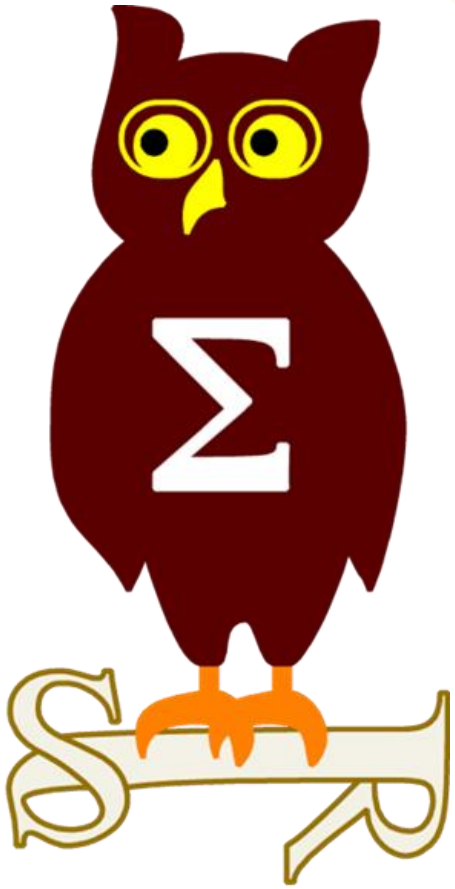
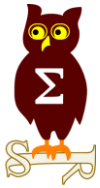


Revue d'actualité

12/02/2019

Préparée par

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



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS19-001 Vulnérabilités dans Internet Explorer (1 CVE)

- Exploit:
  - 1 x Exécution de code à distance

Dont 0 communes avec IE:

MS19-002 Vulnérabilités dans Edge (5 CVE)

- Exploit:
  - 4 x Exécution de code à distance
  - 1 x Élévation de privilèges
- Crédits:
  - Jihui Lu of Tencent KeenLab (CVE-2019-0565)
  - James Forshaw of Google Project Zero (CVE-2019-0566)
  - MoonLiang of Tencent Security Xuanwu Lab (CVE-2019-0567)
  - Zhenhuan Li(@zenhumany) of Tencent Zhanlu Lab (CVE-2019-0567)
  - Yuki Chen of Qihoo 360 Vulcan Team (CVE-2019-0567)
  - Qixun Zhao of Qihoo 360 Vulcan Team (CVE-2019-0567)
  - Lokihardt of Google Project Zero (CVE-2019-0567, CVE-2019-0568)
  - Qixun Zhao of Qihoo 360 Vulcan Team (CVE-2019-0567)
  - Hearmen of Tencent Security Xuanwu Lab (CVE-2019-0567)
  - Guangzhou University (CVE-2019-0539)
  - Lokihardt of Google Project Zero (CVE-2019-0539)
  - MoonLiang of Tencent Security Xuanwu Lab (CVE-2019-0539)
  - Tencent Warriors (CVE-2019-0539)
  - Zhenhuan Li(@zenhumany) of Tencent Zhanlu Lab (CVE-2019-0539)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS19-003 Vulnérabilités dans Windows Kernel (4 CVE)

- Affectés
  - Windows 7, 8.1, 10, Server 2008, 2012, 2016, 2019
- Exploit:
  - 4 x Fuite d'informations
- Crédits:
  - Ruibo Liu of Baidu XLab Tianya Team (CVE-2019-0536, CVE-2019-0554)
  - ZiMiand JunGuof Alibaba Orion Security Lab (CVE-2019-0569)

MS19-004 Vulnérabilités dans Windows Jet Database Engine (11 CVE)

- Affectés
  - Windows 7, 8.1, 10, Server 2008, 2012, 2016, 2019
- Exploit:
  - 11 x Exécution de code arbitraire
- Crédits:
  - rgod of 9sg Security Team - rgod@9sgsec.com working with Trend Micro's Zero Day Initiative (CVE-2019-0582, CVE-2019-0583, CVE-2019-0581, CVE-2019-0584, CVE-2019-0580)
  - Bar Lahav and Gal De Leon of Palo Alto Networks (CVE-2019-0583, CVE-2019-0538, CVE-2019-0584, CVE-2019-0580, CVE-2019-0577, CVE-2019-0576, CVE-2019-0575)
  - Honggang Ren of Fortinet's FortiGuard Labs (CVE-2019-0538)
  - Mitja Kolsek of 0patch Team - ACROS Security (CVE-2019-0579)
  - Gal De Leon and Bar Lahav of Palo Alto Networks (CVE-2019-0579)
  - Behzad Najjarpour Jabbari, Secunia Research at Flexera (CVE-2019-0579)
  - Steven Seeley (mr_me) of Source Incite (CVE-2019-0578, CVE-2019-0577, CVE-2019-0576, CVE-2019-0575)
  - Anonymous working with Trend Micro's Zero Day Initiative (CVE-2019-0577)
  - Hardik Shahof McAfee (CVE-2019-0576)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS19-005 Vulnérabilités dans Windows Hyper-V (2 CVE)

- Affectés
  - Windows 10, Server 2016, 2019
- Exploit:
  - 2 x Exécution de code arbitraire

MS19-006 Vulnérabilités dans Windows Data Sharing Service (4 CVE)

- Affectés
  - Windows 10, Server 2016, 2019
- Exploit:
  - 4 x Élévaiton de privilèges
- Crédits:
  - James Forshaw of Google Project Zero (CVE-2019-0572, CVE-2019-0573, CVE-2019-0574, CVE-2019-0571)

MS19-007 Vulnérabilités dans .NET Framework (1 CVE)

- Affectés
  - .NET
- Exploit:
  - 1 x Fuite d'informations

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS19-008 Vulnérabilités dans ASP.NET (2 CVE)

- Affectés
  - ASP.NET, PowerShell Core
- Exploit:
  - 2 x Denial of service
- Crédits:
  - James Forshaw of Google Project Zero (CVE-2019-0572, CVE-2019-0573, CVE-2019-0574, CVE-2019-0571)

MS19-009 Vulnérabilités dans SharePoint (4 CVE)

- Affectés
  - SharePoint
- Exploit:
  - 1 x Elévation de privilèges
  - 3 x Fuites d'informations
- Crédits:
  - Ashar Javedof Hyundai AutoEver Europe GmbH (CVE-2019-0562, CVE-2019-0558, CVE-2019-0557, CVE-2019-0556)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS19-010 Vulnérabilités dans Exchange (2 CVE)

- Affectés
  - SharePoint
- Exploit:
  - 1 x Fuites d'informations
  - 1 x Exécution de code arbitraire
- Crédits:
  - Cameron Vincent (CVE-2019-0588)
  - Nicolas Jolyof Microsoft Corporation (CVE-2019-0586)

MS19-011 Vulnérabilités dans Office (4 CVE)

- Affectés
  - Office 2010, 2013, 2019, 365 ProPlus
- Exploit:
  - 1 x Fuites d'informations
  - 1 x Exécution de code arbitraire
- Crédits:
  - Jaanus Kp, Clarified Security working with Trend Micro's Zero Day Initiative (CVE-2019-0585)
  - Pieter Ceelen& Stan Hegt, Outflank (CVE-2019-0561)
  - Tal Dery and Menahem Breuer of Mimecast Research Labs (CVE-2019-0560)
  - Rick Roane (CVE-2019-0559)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS19-012 Vulnérabilités dans Windows Runtime (1 CVE)

- Affectés
  - Windows 8.1, 10, Server 2012, 2016, 2019
- Exploit:
  - 1 x Elévation de privilèges
- Crédits:
  - James Forshaw of Google Project Zero (CVE-2019-0570)

MS19-013 Vulnérabilités dans XMLDocument (1 CVE)

- Affectés
  - Windows 8.1, 10, Server 2012, 2016, 2019
- Exploit:
  - 1 x Elévation de privilèges
- Crédits:
  - James Forshaw of Google Project Zero (CVE-2019-0555)

MS19-014 Vulnérabilités dans Windows (1 CVE)

- Affectés
  - Windows 7, 8.1, 10, Server 2008, 2012, 2016, 2019
- Exploit:
  - 1 x Elévation de privilèges
- Crédits:
  - James Forshaw of Google Project Zero (CVE-2019-0543)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS19-015 Vulnérabilités dans Windows DHCP (1 CVE)

- Affectés
  - Windows 10, Server 1803
- Exploit:
  - 1 x Exécution de code arbitraire
- Crédits:
  - Mitch Adair, Microsoft Windows Enterprise Security Team (CVE-2019-0547)

MS19-016 Vulnérabilités dans Windows Subsystem for Linux (1 CVE)

- Affectés
  - Windows 10, Server 2019
- Exploit:
  - 1 x Fuite d'informations
- Crédits:
  - Anthony LAOU HINE TSUEI (CVE-2019-0553)

MS19-017 Vulnérabilités dans Windows COM Desktop Broker (1 CVE)

- Affectés
  - Windows 8.1, 10, Server 2012, 2016, 2019
- Exploit:
  - 1 x Élévation de privilèges
- Crédits:
  - James Forshaw of Google Project Zero (CVE-2019-0552)

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**

Microsoft recommande de ne plus utiliser IE

- Au profit d'Edge et bientôt de son remplaçant basé sur Chromium

  https://www.numerama.com/tech/462999-microsoft-vous-en-supplie-arretez-dutiliser-internet-explorer.html

Failles / Bulletins / Advisories

Microsoft - Autre

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/

Un chercheur publie une série de méthodes permettant d'accéder au système et pouvant mener à la compromission de l'AD

- le premier scénario permet d'élever ses privilèges
- le second permet d'exécuter du code arbitraire sur le système
- les scénarios exploitent le mécanisme de délégation Kerberos

https://shenaniganslabs.io/2019/01/28/Wagging-the-Dog.html

Prise du contrôle d'un système via une vulnérabilité au sein d'Outlook

- via une erreur dans la gestion des liens hypertextes au sein des VCards

https://www.exploit-db.com/exploits/46167

Failles / Bulletins / Advisories

Microsoft - Autre

25 vulnérabilités dans les clients RDP

- Recherche menée par CheckPoint
- RCE dans freerdp, rdesktop, et path traversal dans le client officiel (mstsc.exe)

https://research.checkpoint.com/reverse-rdp-attack-code-execution-on-rdp-clients/

Désactiver la PPL (protection légère de processus (?)) sur Windows 10

- Outil nommé Windows D
- A priori via le chargement d'un pilote noyau
- Peut être utile pour désactiver un antivirus , EDR, dumper lsass…

https://github.com/katlogic/WindowsD

Failles / Bulletins / Advisories

Système (principales failles)

Patch trimestriel Oracle

- 5 vulnérabilités dans Java SE
- 29 vulnérabilités dans Oracle MySQL
- 3 vulnérabilités dans Oracle Database Server
- 50 vulnérabilités dans Oracle Fusion Middleware
- 50 vulnérabilités au sein d'Oracle VM Virtualbox et Secure Global Desktop

https://www.oracle.com/technetwork/security-advisory/cpujan2019-5072801.html

2 vulnérabilités au sein de PhpMyAdmin

- Lecture de fichiers arbitraires
- Injection SQL

https://www.phpmyadmin.net/security/PMASA-2019-1/
https://www.phpmyadmin.net/security/PMASA-2019-2/

1 vulnérabilité au sein de runC

- impacte les conteneurs Docker, Kubernetes ou encore Rancher
- élévation de privilèges sur le système hôte, code d'exploitation disponible
- vulnérabilité similaire pour LXC

https://seclists.org/oss-sec/2019/q1/119

Failles / Bulletins / Advisories

Système (principales failles)

4 vulnérabilités au sein de clients SCP découvertes

- OpenSSH, WinSCP et PuTTY touchés
- vieilles de 36 ans
- Manipulation des réponses du serveurs et compromission des postes des victimes

https://sintonen.fi/advisories/scp-client-multiple-vulnerabilities.txt

1 vulnérabilité au sein de Ghostscript découverte puis patchée

- exécution de code arbitraire, by Tavis Ormandy

https://www.bleepingcomputer.com/news/security/no-patch-available-yet-for-new-major-vulnerability-in-ghostscript-interpreter/

2 vulnérabilités critique au sein de Gitlab

- Lecture des titres des issues et des merges requests d'autres projets et XSS persistante

https://about.gitlab.com/2019/02/05/critical-security-release-gitlab-11-dot-7-dot-4-released/

Selon la société Sonatype, de nombreuses entreprises du Fortune 100 seraient toujours vulnérable à la faille ayant impacté Equifax

- 2 ans après sa publication

http://fortune.com/2018/05/07/security-equifax-vulnerability-download/

Failles / Bulletins / Advisories

Système (principales failles)

Le dépôt d'extension et d'applications PHP PEAR compromis depuis 6 mois

- code malveillant introduit dans le fichier d'installation
- => le nombre de serveurs touchés est potentiellement très élevé étant donné la popularité du projet et son inclusion au sein de l'installation de PHP
- Site officiel offline depuis la publication de la vulnérabilité

https://www.cert.be/fr/le-gestionnaire-de-packets-de-php-pear-remplace-par-une-version-compromise

Exécution de code au sein du gestionnaire de paquet APT

- mises à jour récupérées en HTTP

https://www.cert.ssi.gouv.fr/alerte/CERTFR-2019-ALE-001/

Exécution de code arbitraire au sein de Horde IMP

- sans authentification, exploit disponible

https://www.exploit-db.com/exploits/46136

1 vulnérabilité permet le vol des données du Keychain de macOS

- Le chercheur a uniquement partagé une vidéo démontrant la vulnérabilité
- Il ne partagera pas d'informations complémentaire tant qu'Apple ne proposera pas de Bug Bounty pour macOS

https://www.bleepingcomputer.com/news/security/researcher-declines-to-share-zero-day-macos-keychain-exploit-with-apple/

Failles / Bulletins / Advisories

Système (principales failles)

3 vulnérabilités identifiées au sein de systemd par la société Qualys

- toutes les distributions basés sur systemd impacté sauf (car utilisant l'option -fstack-clash-protection de gcc):
  - USE Linux Enterprise 15
  - OpenSUSE Leap 15.0
  - Fedora 28
  - Fedora 29
- permettent d'obtenir un terminal avec les droits administrateur sur la machine

https://www.qualys.com/2019/01/09/system-down/system-down.txt

Failles / Bulletins / Advisories

Hardware / IoT

Compromission d’objets connectés via le chipset WiFi (Marvell Avastar)

https://embedi.org/blog/remotely-compromise-devices-by-using-bugs-in-marvell-avastar-wi-fi-from-zero-knowledge-to-zero-click-rce/

Failles / Bulletins / Advisories

Hardware / IoT

Failles / Bulletins / Advisories

Android / iOS

Un adolescent a découvert une vulnérabilité au sein de l'application de VoIP Facetime

- permet à un attaquant d'entendre les sons captés par l'iPhone avant que le destinataire ne décroche
- Corrigé dans iOS 12.1.4

https://www.igen.fr/ios/2019/02/ios-1214-corrige-la-grosse-faille-de-securite-de-facetime-106678

2 vulnérabilités permettant un jailbreak à distance sous iOS 12 découvertes

- exécution de code arbitraire depuis une page web + élévation de privilèges et installation d'une application malveillante

https://www.infosecurity-magazine.com/news/hacker-demos-jailbreak-of-ios-on/

Parmi les vulnérabilités corrigées au sein d'Android en février, deux d'entres sont particulièrement critiques

- Exécution de code arbitraire à l'aide d'une image PNG
- Exécution de code arbitraire à l'aide d'une connexion Bluetooth

https://source.android.com/security/bulletin/2019-02-01

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Campagne de rançongiciel

- la France ciblé par Shade et Anatova
- développement du Ransomware as a Service

https://www.cert.ssi.gouv.fr/alerte/CERTFR-2019-ALE-003/

Dailymotion victime d'une attaque de type "credential stuffing"

- (compromission de compte via réutilisation de mots de passe compromis)

https://threatpost.com/dailymotion-credential-stuffing/141223/

Altran touché par une cyberattaque

- aucun vol de données, pas de propagation chez les clients

https://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/altran-reconnait-avoir-ete-victime-d-une-cyberattaque-805334.html

Airbus Commercial Aircraft victime d'une fuite de données

- données à caractères personnelles dérobées

https://www.theregister.co.uk/2019/01/31/airbus_hacked_eurofighter_link/

4 000 domaines usurpés pour du scam / phishing via GoDaddy.com

- il était possible de revendiquer un nom de domaine sans payer (paiement requis après 30

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Attaque dite des 51% touchant la cryptomonnaie “Ethereum Classic”

- Attaquant dispose de 51% de la puissance de calcul disponible sur le réseau
- 1 million d’euros dérobés via l’imposition au système d’une blockchain alternative autorisant des opérations non référencées

https://www.thestreet.com/investing/bitcoin/attack-against-ethereum-classic-14832327

La NASA touchée par une fuite de données

- données confidentielles sur ses employés et projets internes exposés pendant 3 semaines via un défaut de configuration sur une application Jira

https://medium.com/@logicbomb_1/bugbounty-nasa-internal-user-and-project-details-are-out-2f2e3580421b

La société Roxane Nord (eaux minérales) touchée par une arnaque au président

- via une société partenaire compromise

http://lavdn.lavoixdunord.fr/530700/article/2019-01-31/la-societe-roxane-nord-victime-d-une-escroquerie-trois-millions-d-euros

La banque indienne SBI aurait laissé un serveur contenant plusieurs millions de données clientes pendant une durée indéterminée

https://www.businesstoday.in/technology/sbi-data-leak-what-happened-sbi-data-breach-financial-data/story/316071.html

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Une base MongoDB non protégée de 854 Go contenant 200 millions de CV de chinois identifiée

https://thenextweb.com/security/2019/01/11/200-million-chinese-resumes-leak-in-huge-database-breach/

5 bases nommées Collection #1 à #5 vendues sur le Dark Web

- regroupe des bases déjà compromises et partagées en plus de nouvelles
- Près de 3.5 milliards d'identifiants et mots de passe partagées

https://www.lemondeinformatique.fr/actualites/lire-collection-2-5-fuite-record-avec-845-go-de-donnees-personnelles-volees-74195.html

https://www.cnetfrance.fr/news/collection-1-l-une-des-plus-importantes-fuites-de-donnees-a-ce-jour-39879449.htm

Un serveur en Oklahoma exposait 3 To de données

- documents d'enquêtes du FBI et données personnelles exposées via un rsync non sécurisé

https://www.forbes.com/sites/thomasbrewster/2019/01/16/massive-oklahoma-government-data-leak-exposes-7-years-of-fbi-investigations/

1 base de données Elastic Search exposait 108 millions d'informations de sites de casinos

- données personnelles

https://www.forbes.com/sites/thomasbrewster/2019/01/16/massive-oklahoma-government-data-leak-exposes-7-years-of-fbi-investigations/

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Piratages, Malwares, spam, fraudes et DDoS

Espionnage

Les États-Unis énoncent 13 chefs d'accusation contre Huawei

- Action d'association de malfaiteurs en vue de voler des secrets industriels (T-Mobile)
- Arrestation de Mme Meng, fille du fondateur, déjà à l'origine de vives tensions

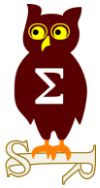
https://www.challenges.fr/high-tech/usa-huawei-inculpe-pour-vol-de-technologies_639408

Facebook a donné 17 euros par mois des ados en échange de leur vie privée

- … sous forme de carte cadeaux pour les 13 à 35 ans
- quasi intégralité des données contenues dans le smartphone demandée, voir même des screenshots d'historique d'achat Amazon
- => Apple a bloqué l'ensemble des applications internes Facebook pour iOS via la révocation d'un certificat
- => Apple a fait de même avec Google sur une plus courte durée pour l'application Screenwise Meter

https://www.numerama.com/tech/459207-facebook-a-donne-17-euros-par-mois-a-des-ados-en-lechange-de-leur-vie-privee.html

https://www.theverge.com/2019/1/30/18203551/apple-facebook-blocked-internal-ios-apps



Nouveautés, outils et techniques

Crypto et Divers

Divers

Google rend open-source ClusterFuzz

Outil de fuzzing à grande échelle (utilisé par Google sur 25 000 coeurs)

https://opensource.googleblog.com/2019/02/open-sourcing-clusterfuzz.html

Comprendre les permissions des services Windows

https://decoder.cloud/2019/02/07/demystifying-windows-service-permissions-configuration/

Firefox bloquera bientôt le cryptojacking et le pistage des utilisateurs

https://www.bleepingcomputer.com/news/security/mozilla-adding-cryptomining-and-fingerprint-blocking-to-firefox/

Persistence sur MacOS via les extensions Chrome

- Peuvent s'installer via des profils de configurations (par un mail de phishing par exemple)

  https://posts.specterops.io/no-place-like-chrome-122e500e421f

Metasploit 5.0

- Première version majeure depuis 2011
- exposition de la base de données et de fonctionnalités d'automatisation de Metasploit via APIs
- ajout de mécanismes visant à éviter la détection des programmes malveillants par les antivirus
- utilisation de modules d'exploitation sur plusieurs cibles en même temps ;
- amélioration des performances du framework ;
- support des langages Go et Python (en plus de Ruby) pour le développement de modules
  https://blog.rapid7.com/2019/01/10/metasploit-framework-5-0-released/

Faire croire que son Meterpreter est signé

- En exploitant le format MSI, on l'ajoute à un binaire signé (ex: Google Chrome)
  https://medium.com/forensicitguy/making-meterpreter-look-google-signed-using-msi-jar-files-c0a7970ff8b7

Pentest

Techniques & outils

Empêcher le cassage de mots de passe avec John the Ripper

- Grâce à une archive PKZIP un peu mal formée

  https://www.openwall.com/lists/john-users/2013/12/23/1

Business et Politique

Business

France

Vente-Privée devient VeePee

- Reprise du nom de l'opérateur/hébergeur racheté par SPIE en 2010

  https://www.veepee.com/fr-fr/about.html

Business

International

Failles critiques sur les CPU = Record de ventes !!?

- **2018** = **2017** + **13%**
- +10% sur la division PC (bureautique et jeu)
- +24% sur la division Cloud
- +25% sur la division mémoire

https://www.techpowerup.com/251832/intel-reports-fourth-quarter-and-full-year-2018-financial-results

Google propose un service équivalent à Have I Been Pwned au travers d'une extension pour savoir si ses mots de passe sont compromis

https://thenextweb.com/apps/2019/02/06/googles-new-extension-tells-you-if-your-passwords-have-been-compromised/

Droit / Politique

France

Plus de 1 200 notifications de la CNIL reçues depuis l'entrée en vigueur du RGPD

https://www.lesechos.fr/tech-medias/hightech/0600534426461-rgpd-la-cnil-a-enregistre-1200-signalements-en-huit-mois-2237105.php

Plus de 59 000 fuites de données ont été déclarées depuis la mise en place du RGPD

https://www.bleepingcomputer.com/news/security/59k-data-breaches-reported-91-fines-imposed-since-gdpr-enactment/

La CNIL inflige une amende de 50 millions d'euros à Google

https://www.usine-digitale.fr/article/la-cnil-impose-une-amende-de-50-millions-d-euros-a-google-pour-non-respect-du-rgpd.N796300

La France se dote d'une doctrine pour la lutte informatique offensive

- 1,6 milliards d'euros consacrés à la lutte dans l'espace numérique, +1 500 postes à pourvoir

https://www.challenges.fr/top-news/la-france-se-dote-d-une-doctrine-offensive-pour-la-cyber-guerre_637269

L'ANSSI redoute un "cyber Pearl Harbor"

https://www.latribune.fr/technos-medias/telecoms/le-gendarme-de-la-securite-informatique-redoute-un-cyber-pearl-harbor-805282.html

Droit / Politique
International

Le Zimbabwe coupe Internet pour masquer la violence commise par l'armée lors de la répression de manifestations

https://www.apnews.com/7cf7713da14c46909800f74fd8f08cb2

xDedic, site marchands d'accès à des machines compromises fermé par les forces de polices internationales

https://www.europol.europa.eu/newsroom/news/xdedic-marketplace-shut-down-in-international-operation

L'Allemagne met un frein à la collecte de données par Facebook

- violation des règles européennes en matière de protection de données
- « une case à cocher » ne constitue pas une base suffisante pour permettre un « traitement de données aussi intensif »

https://newsroom.fb.com/news/2019/02/bundeskartellamt-order/

https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook_FAQs.pdf?__blob=publicationFile&v=5

Les données ADN partagées avec le FBI

- Service d'analyse ADN (*FamilyTreeDNA*) pour retrouver ses origines, donne accès à la base de données au FBI

https://nakedsecurity.sophos.com/2019/02/05/home-dna-kit-company-says-its-working-with-the-fbi/

Droit / Politique
International

QuadrigaCX (bourse de crypto-monnaie) annonce faire faillite suite au décès de son fondateur et par conséquent la perte de l'accès aux fonds

Histoire louche, doute sur le fait que la société dispose de "cold wallet" et n'ai jamais disposé des fonds en question

https://www.ccn.com/wheres-the-missing-150-million-crypto-exchange-quadrigacxs-fiasco-gets-weirder-with-new-research

Le gouvernement japonais va "pirater" les objets connectés

Pour prévenir les citoyens qui disposent d'équipements sans mot de passe ou avec des mots de passe par défaut

https://www3.nhk.or.jp/nhkworld/en/news/20190125_44/

Conférences

Conférences

Passées

- BOTCONF
- FIC

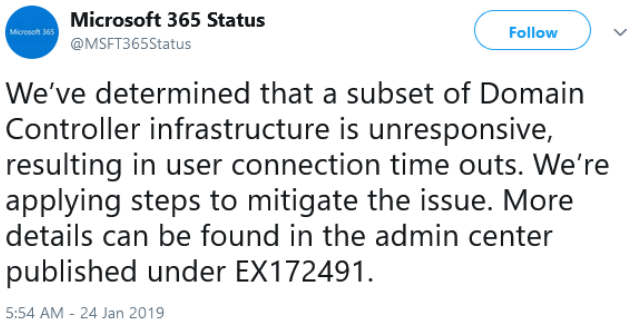
A venir

- Troopers
- Hack in Paris
- SSTIC

Divers / Trolls velus

Divers / Trolls velus

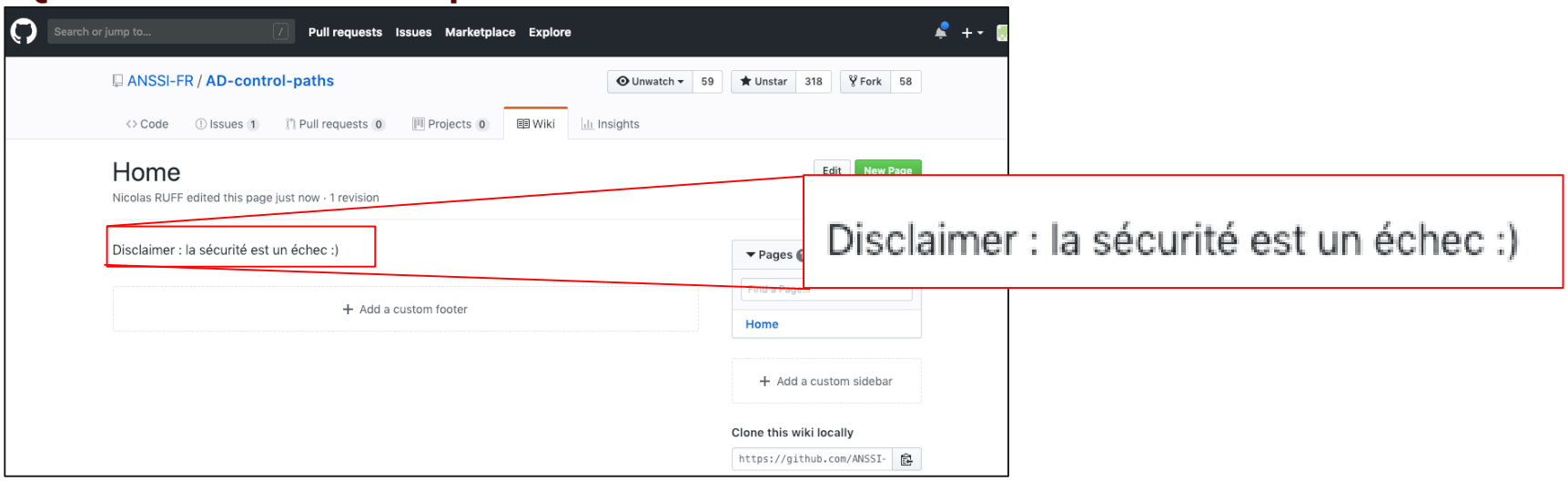
Le Cloud c'est bien… quand ça marche



https://twitter.com/MSFT365Status/status/1088434889014370304

Divers / Trolls velus

Quand tu ne sécurises pas bien le Wiki de ton Github



Shit Storm is coming…

<<Dès le début, je leur expliquais tout le mal que je pensais de ces pseudo-experts de la sécurité dont la mission première était de faire peur à leurs clients en leur montrant par des tests d'intrusion – ou penetration tests – à quel point leur système d'information était faillible. La plupart de ces gugusses, pour parvenir à leur fin, utilisent des outils dont ils ne comprennent pas grand chose au fonctionnement, mettant parfois en danger les réseaux des entreprises où ils appliquent des tutos venus des forums de l'Internet>>

<<Dans ce moment singulier où nous voyons fleurir toutes ces entreprises de Pentest, il est bon de rappeler qu'elles sont le plus souvent peuplées d'incompétents notoires ayant recours à des procédés illégaux et susceptibles de perturber très lourdement le fonctionnement de votre système d'information et de votre réseau..>>

https://twitter.com/bloginfo/status/1093163784213065734

https://www.dsfc.net/infrastructure/securite/pentest-et-pentesteur/

Divers / Trolls velus

Divers / Trolls velus

Divers / Trolls velus

Prochains rendez-vous de l’OSSIR

Prochaine réunion

- JSSI le 19 mars : les inscriptions sont ouvertes!

After Work

- A planifier

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous