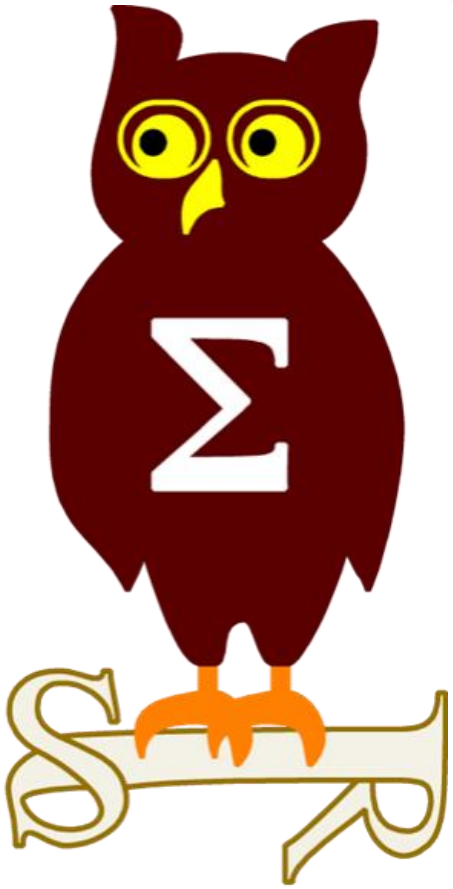
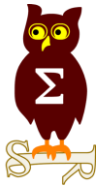


Revue d'actualité

11/12/2018

Préparée par

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



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-051 Vulnérabilités dans Internet Explorer (4 CVE)

- Exploit:
  - 2 x Remote Code Execution
- Crédits:
  - @j00sean par iDefense Labs (CVE-2018-8570)
  - Ivan Fratric de Google Project Zero (CVE-2018-8552)

MS18-052 Vulnérabilités dans Edge (8 CVE)

- Exploit:
  - 1 x Spoofing
  - 8 x Remote Code Execution
  - 1 x Information Disclosure
  - 1 x Elevation of Privilege
- Crédits:
  - dannywei de Tencent Security Xuanwu Lab (CVE-2018-8567)
  - Anonymous par iDefense Labs, Qixun Zhao de Qihoo 360 Vulcan Team, Jonathan Jacobi (@j0nathanj) de MSRC-IL (CVE-2018-8555)
  - Qixun Zhao de Qihoo 360 Vulcan Team, Anonymous par Trend Micro's Zero Day Initiative, Jonathan Jacobi (@j0nathanj) de MSRC-IL (CVE-2018-8588)
  - Jun Kokatsu, Windows & Devices Group - Operating System Security Team (CVE-2018-8564)
  - James Lee @Windowsrcer de Kryptos Logic (CVE-2018-8545)
  - Microsoft Chakra Core Team (CVE-2018-8551)
  - Qixun Zhao de Qihoo 360 Vulcan Team (CVE-2018-8556, CVE-2018-8542, CVE-2018-8557)
  - ? (CVE-2018-8541, CVE-2018-8543)

Dont 0 communes avec IE:

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-157 Vulnérabilités dans Microsoft Dynamics 365 (5 CVE)

- Affecté:
  - Microsoft Dynamics 365 (on-premises) version 8
- Exploit:
  - 4 x Spoofing
  - 1 x Remote Code Execution
- Crédits
  - Tim Kent de TSS Cyber, Marios Gyftos (CVE-2018-8607)
  - Manuel Sanchez Hernanz de CBRE Real Estate, Tim Kent de TSS Cyber (CVE-2018-8605)
  - ? (CVE-2018-8608, CVE-2018-8609, CVE-2018-8606)

MS18-158 Vulnérabilités dans Scripting Engine (JScript and/or VBScript) (2 CVE)

- Affecté:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Remote Code Execution
  - 1 x Security Feature Bypass
- Crédits
  - Anonymous par Trend Micro's Zero Day Initiative, Yuki Chen de Qihoo 360 Vulcan Team, Ivan Fratric de Google Project Zero (CVE-2018-8544)
  - Philip Tsukerman de Cybereason (CVE-2018-8417)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-159 Vulnérabilité dans TFTP service (1 CVE)

- Affecté:
  - Windows Server 2008, 2008 R2, 2016, 2019
- Exploit:
  - 1 x Remote Code Execution
- Crédits
  - Omer Gull de Checkpoint Software Technologies (CVE-2018-8476)

MS18-160 Vulnérabilité dans Microsoft Graphics (GDI) (1 CVE)

- Affecté:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Remote Code Execution
- Crédits
  - Lin Wang de Beihang University par Trend Micro's Zero Day Initiative (CVE-2018-8553)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-161 Vulnérabilités dans Office (10 CVE)

- Affecté:
  - Office toutes versions supportées
- Exploit:
  - 8 x Remote Code Execution
  - 2 x Information Disclosure
- Crédits
  - Jaanus Kp, Clarified Security par Trend Micro's Zero Day Initiative (CVE-2018-8573)
  - Nicolas Joly de Microsoft Corporation (CVE-2018-8574)
  - Yonghui Han de Fortinet s FortiGuard Labs (CVE-2018-8582, CVE-2018-8524, CVE-2018-8522, CVE-2018-8576)
  - ? (CVE-2018-8558, CVE-2018-8577, CVE-2018-8579)
  - Yangkang de 360CoreSec, Jinquan de 360CoreSec (CVE-2018-8539)

MS18-162 Vulnérabilités dans Windows (5 CVE)

- Affecté:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Tampering
  - 1 x Remote Code Execution, dans PowerShell
  - 1 x Security Feature Bypass
  - 2 x Elevation of Privilege
- Crédits
  - Snyk Security Research Team (CVE-2018-8256)
  - Amirreza Niakanlahiji (@DissectMalware) de University de North Carolina at Charlotte (CVE-2018-8415)
  - Igor Glucksmann de Avast Software (CVE-2018-8549)
  - ? (CVE-2018-8592)
  - James Forshaw de Google Project Zero (CVE-2018-8550)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-163 Vulnérabilités dans DirectX (4 CVE)

- Affecté:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Information Disclosure
  - 3 x Elevation of Privilege
- Crédits
  - Communications Security Establishment (CVE-2018-8485, CVE-2018-8561)
  - Alex Ionescu, CrowdStrike Inc., Thomas Imbert (@masthoon) de MSRC Vulnérabilités and Mitigations Team (CVE-2018-8554)
  - Scott Bell de Pulse Security (CVE-2018-8563)

MS18-164 Vulnérabilités dans SharePoint (3 CVE)

- Affecté:
  - Microsoft SharePoint Enterprise 2013, 2016, 2019
- Exploit:
  - 1 x Information Disclosure
  - 2 x Elevation of Privilege
- Crédits
  - Ashar Javed de Hyundai AutoEver Europe GmbH (CVE-2018-8568, CVE-2018-8572)
  - ? (CVE-2018-8578)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-165 Vulnérabilités dans Microsoft Win32K and/or Graphics Component (3 CVE)

- Affecté:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Information Disclosure
  - 2 x Elevation of Privilege, exploité dans la nature

    https://www.kaspersky.fr/blog/cve-2018-8589-vulnerability-detected/11177/
- Crédits
  - Igor Soumenkov (2igosha) de Kaspersky Lab, Boris Larin (Oct0xor) de Kaspersky Lab (CVE-2018-8589)
  - Long Li de Baidu XLab Tianya Team (CVE-2018-8565)
  - Laith AL-Satari (CVE-2018-8562)

MS18-166 Vulnerability dans Windows Search (1 CVE)

- Affecté:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Remote Code Execution
- Crédits
  - ? (CVE-2018-8450)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-167 Vulnerability dans Azure App Service (1 CVE)

- Affecté:
  - Azure App Service on Azure Stack
- Exploit:
  - 1 x Spoofing
- Crédits
  - Jayson Grace de Sandia National Labs (CVE-2018-8600)

MS18-168 Vulnerability dans Windows RCP (1 CVE)

- Affecté:
  - Windows 10, 2016, 2019
- Exploit:
  - 1 x Elevation of Privilege, publiée publiquement
- Crédits
  - ? (CVE-2018-8584)

MS18-169 Vulnerability dans Team Foundation Server (1 CVE)

- Affecté:
  - Team Foundation Server 2017, 2018
- Exploit:
  - 1 x Spoofing
- Crédits
  - ? (CVE-2018-8602)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-170 Vulnérabilité dans RPC (1 CVE)

- Affecté:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Information Disclosure
- Crédits
  - Ruibo Liu de Baidu XLab Tianya Team (CVE-2018-8407)

MS18-171 Vulnérabilité dans Windows Kernel (1 CVE)

- Affecté:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Information Disclosure
- Crédits
  - ZiMi and JunGu from Alibaba Orion Security Lab (CVE-2018-8408)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-172 Vulnerability dans Microsoft Exchange Server (1 CVE)

- Affecté:
  - Microsoft Exchange Server 2010, 2013, 2016, 2019
- Exploit:
  - 1 x Elevation of Privilege
- Crédits
  - Anonymous par Trend Micro's Zero Day Initiative (CVE-2018-8581)

MS18-173 Vulnerability dans Active Directory (1 CVE)

- Affecté:
  - Windows 8.1, 10, 2012 R2, 2016, 2019
- Exploit:
  - 1 x Spoofing
- Crédits
  - ? (CVE-2018-8547)

MS18-174 Vulnerability dans Windows RDP (1 CVE)

- Affecté:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Elevation of Privilege, avec Microsoft RemoteFX avec le GPU virtuel (2011, cf. MS16-067)
- Crédits
  - RanchoIce de Tencent ZhanluLab Chen Nan de Tencent ZhanluLab (CVE-2018-8471)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-175 Vulnérabilité dans BitLocker (1 CVE)

- Affecté:
  - Windows 10, 2016, 2016
- Exploit:
  - 1 x Security Feature Bypass, publié publiquement

MS18-176 Vulnérabilité dans Microsoft Project (1 CVE)

- Affecté:
  - Microsoft Project 2010, 2013, 2016
  - Office 365 ProPlus
- Exploit:
  - 1 x Remote Code Execution

MS18-177 Vulnérabilité dans Windows Audio Service (1 CVE)

- Affecté:
  - Windows 10, 2019
- Exploit:
  - 1 x Information Disclosure avec WNF, faille “A” à $5,000

    https://github.com/ionescu007/wnfun
- Crédits
  - Alex Ionescu, CrowdStrike Inc. (CVE-2018-8454)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-178 Vulnérabilité dans .Net (1 CVE)

- Affecté:
  - .NET Core 2.1
- Exploit:
  - 1 x Tampering
- Crédits
  - Danny Grander de Snyk (CVE-2018-8416)

MS18-179 Vulnérabilité dans Skype (1 CVE)

- Affecté:
  - Microsoft Lync 2013, Skype for Business 2016
- Exploit:
  - 1 x Denial of Service
- Crédits
  - Sabine Degen de SEC Consult Vulnerability Lab (CVE-2018-8546)

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

Le prochain navigateur Edge de Microsoft se basera sur Chromium

- Abandon du moteur EdgeHTML, c’est un immense aveux d'échec !

  https://www.nextinpact.com/brief/edge-embrasse-officiellement-chromium-6952.htm

BitLocker expose les clefs en mémoire

- La clef peut être interceptée au boot avec de l’USB type C

  https://support.microsoft.com/en-us/help/2516445/blocking-the-sbp-2-driver-and-thunderbolt-controllers-to-reduce-1394-d

Failles / Bulletins / Advisories

Système (principales failles)

Adobe Flash Player mis à jour

- 2 Vulnérabilités corrigées dont une exploitée a priori par la Russie depuis fin novembre
- Exploit public

https://helpx.adobe.com/security/products/flash-player/apsb18-42.html

Sennheiser HeadSetup pour casque audio (CVE-2018-17612)

- certificat racine avec clef privée commune à tous les ordinateurs
- Similaire a superfish de lenovo (2014)

https://www.nextinpact.com/brief/sennheiser---importante-faille-dans-le-logiciel-headsetup--pro---avec-un-arriere-gout-de-superfish-6777.htm

Failles / Bulletins / Advisories

Système (principales failles)

Élévation de privilèges au sein de Kubernetes (CVE-2018-1002105)

- CVSS 9,8
- Au travers du serveur d'API
- Poc disponible

https://github.com/kubernetes/kubernetes/issues/71411

4 Vulnérabilités au sein de Jenkins

- dont un défaut au sein du framework "Stapler" permettant l'exécution de code arbitraire via une requête HTTP spécifiquement conçue

https://github.com/kubernetes/kubernetes/issues/71411

Prise de contrôle d'un système via une Vulnérabilité au sein d'Hadoop

- CVE-2018-8009, défaut de contrôle au sein de la classe "org.apache.hadoop.fs.FileUtil"
- => upload d'un fichier arbitraire

https://bugzilla.redhat.com/show_bug.cgi?id=1593018

Failles / Bulletins / Advisories

Hardware / IoT

7 nouvelles attaques basés sur les principes de Spectre et Meltdown

- AMR, ARM et Intel touchés
- 2 variantes de Meltdown, 5 variantes de Spectre

  https://arxiv.org/pdf/1811.05441.pdf

Failles / Bulletins / Advisories

Hardware / IoT

Publication de TrendMicro sur la sécurité des protocoles IoT de remontée d'information

- Les brokers MQTT restent exposés sur internes et souvent mal sécurisés
- Le protocole COAP se développe et n'est pas suffisamment sécurisé

https://documents.trendmicro.com/assets/white_papers/wp-the-fragility-of-industrial-IoTs-data-backbone.pdf?v1

Recherche de Vulnérabilités sur les automates Schneider

- Par des gens qui n'y connaissent pas grand chose aux automates
- Mais qui trouvent tout de même quelques Vulnérabilités

https://medium.com/tenable-techblog/plc-bug-hunt-fa3a0aeae9ab

Attaques sur les distributeurs de billets

- 58% vulnérables à une attaque réseau sur les services exposés
- 27% vulnérable à l'impersonification du "processing center"
- 76% vulnérables à la sortie du mode kiosque

https://www.ptsecurity.com/upload/corporate/ww-en/analytics/ATM-Vulnerabilities-2018-eng.pdf

Failles / Bulletins / Advisories

Android / iOS

20 Vulnérabilités corrigées au sein d'iOS

https://support.apple.com/en-us/HT209340

Niveau de sécurité des applications de trading

- 34 applis mobiles, 30 sites web, 16 applis de bureau
- Résultats beaucoup moins bons que pour les applications bancaires traditionnelles

https://ioactive.com/wp-content/uploads/2018/08/Are-You-Trading-Stocks-Securely-Exposing-Security-Flaws-in-Trading-Technologies.pdf

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

50 000 imprimantes détournées pour promouvoir une chaine Youtube

- Via Shodan pour promouvoir PewDiePie (jeux vidéos)

  https://amp.thehackernews.com/thn/2018/11/pewdiepie-printer-hack.html

Détournement d'Apple Touch ID

- Application de suivi d'activité physique demande l'empreinte afin de proposer des recommandations
- En réalité, il s'agit d'achats en lignes

  https://www.clubic.com/application-mobile/actualite-848353-ios-touch-id-insu-utilisateurs-achats-malveillants.html

Des mots de passe de comptes Instagram rendus publics par la mauvaise configuration d'un outil interne

- due à l'utilisation de la fonctionnalité "Download Your Data" en vue d'une conformité GDPR
- Mot de passe en clair visible dans l'URL (censé être hashé pourtant ?!)

  https://securityaffairs.co/wordpress/78173/data-breach/instagram-glitch-exposed-passwords.html

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Une campagne d'exploitation de routeurs pour viser les machines vulnérables à EternalBlue

- Une nouvelle campagne d'exploitation de la fonctionnalité "Universal Plug and Play" (UPnP) permet aux attaquants d'exposer les ports 139 et 445 des machines du réseau interne
- Sans doute pour exploiter la Vulnérabilité EternalBlue

https://arstechnica.com/information-technology/2018/11/mass-router-hack-exposes-millions-of-devices-to-potent-nsa-exploit/

Rowhammer sur les mémoire ECC

- Concerne uniquement certains contrôleur mémoire (maintenant intégré dans les CPU) :
  - AMD Opteron 6376 Bulldozer
  - Intel Xeon E3-1270 v3 Haswell
  - Intel Xeon E5-2650 v1 Sandy Bridge
  - Intel Xeon E5-2620 v1 Sandy Bridge

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Exposition de 57 millions de données de citoyens américains et de 25 millions d'entreprises

- répertoriée sur Shodan
- Une instance Elasticsearch expose des données personnelles

https://blog.hackenproof.com/industry-news/new-data-breach-exposes-57-million-records

Possible fuite d'informations suite à un piratage sur le site Dell.com

- noms, adresses mail et mots de passe hashés

https://www.dell.com/learn/us/en/uscorp1/press-releases/2018-11-28-customer-update

La moitié des sites de phishing disposerait aujourd'hui d'un "cadenas" (SSL)

- Le premier moyen cité par le grand public pour éviter les fraudes sur Internet est aujourd'hui, plus que jamais, devenu inefficace.

https://it.slashdot.org/story/18/11/27/1521240/half-of-all-phishing-sites-now-have-the-padlock

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

La chaîne d'hôtels Marriott victime d'une fuite de données massive

- Starwood Guest Reservation, racheté en 2016
- 500 millions de clients touchés (noms, email, numéro de passeport, date de naissance)
- Données dérobées entre 2014 et 2018
- clés de déchiffrement également dérobées

https://answers.kroll.com/

Quora, 100 millions de comptes compromis

- Application tierce autorisée à accéder à des données sensibles par erreur
- nom, adresse mail, mots de passe chiffrés, etc.

https://blog.quora.com/Quora-Security-Update

Atrium Health: les données personnelles de 2,65 millions de patients potentiellement exposées

- Réseau hospitalier américain
- accès non autorisé à la base de données entre le 22 et 29 novembre

https://www.healthcareitnews.com/news/atrium-health-breach-data-265m-patients-potentially-exposed

Piratages, Malwares, spam, fraudes et DDoS

Malware

Un botnet de plus de 20 000 sites Wordpress cible d'autres sites Wordpress

- Via du bruteforce de mot de passe

https://www.zdnet.com/article/a-botnet-of-over-20000-wordpress-sites-is-attacking-other-wordpress-sites/

Un nouveau ransomware se déploie rapidement en Chine

- déployé via le logiciel de développement "EasyLanguage"
- Payment via WeChat
- dispose d'une signature légitime appartenant à Tencent Games
- vol également des identifiants pour des sites populaires
- clé de chiffrement stockée local (XOR)
- 1 suspect identifié

https://thehackernews.com/2018/12/china-ransomware-wechat.html

https://www.huorong.cn/info/1543934825174.html

Une backdoor a été découverte au sein d'une bibliothèque NodeJS téléchargée près de 2 millions de fois par semaine

- nommée "event-stream"
- utilisée dans des applications critique comme Copay (wallet Bitcoin)

https://www.theregister.co.uk/2016/03/23/npm_left_pad_chaos/

Piratages, Malwares, spam, fraudes et DDoS

Espionnage

Implant hardware sur les cartes SuperMicro via Bloomberg

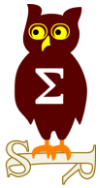
- Après un démenti en novembre de SuperMicro appuyés par des agences fédérales, Bloomberg maintient ses allégations, toujours sans preuve
- Le titre boursier de SuperMicro remonte peu à peu (à 75% de sa valeur originelle)
- Chacun reste sur ses positions

https://www.washingtonpost.com/blogs/erik-wemple/wp/2018/11/27/bloomberg-is-still-reporting-on-challenged-story-regarding-china-hardware-hack/

Plus de 6500 sites du dark web supprimés dans le piratage de l'hébergeur Daniel's Hosting

- via une faille PHP exploitée (CVE-2018-19518)

https://danwin1210.me/



Nouveautés, outils et techniques

Google Chrome révoque la anciennes AC Symantec

- Erreur NET: : ERR_CERT_SYMANTEC_LEGACY

  https://www.lemondeinformatique.fr/actualites/lireamp-chrome-rejette-desormais-des-certificats-pki-de-symantec-73536.html

Demiguise: outil de chiffrement de charge HTA

- La clé de déchiffrement est chargée dynamiquement
- Évite de se faire détecter

https://github.com/nccgroup/demiguise

Toyota créé un environnement open-source pour la car hacking

- Appelé PASTA
- “Bientôt” sur Github: https://github.com/pasta-auto

https://www.darkreading.com/vulnerabilities---threats/toyota-builds-open-source-car-hacking-tool/d/d-id/1333415

Linikatz

- Exploiter les faiblesses AD depuis des machines UNIX jointes au domaine

https://github.com/portcullislabs/linikatz

Pentest
Techniques & outils

Utiliser Google Traduction comme réseau de contrôle-commande

- Google Traduction permet la traduction de pages web, si on maîtrise une page on peut donc utiliser Google traduction pour aller chercher le contenu sans qu'aucune connexion vers le serveur de l'attaquant ne soit visible

  https://github.com/mthbernardes/GTRS

Identification de SPN dangereux et Kerberoasting

https://github.com/cyberark/RiskySPN

Smart Greybox fuzzing

- Pas tout compris, basé sur AFL
- Identification de 42 0-days grâce à ce nouvel outil

  https://arxiv.org/abs/1811.09447

  https://github.com/aflsmart/aflsmart (code pas encore disponible)

Nouveautés
Défense

Déployer facilement un environnement AD sur AWS

https://medium.com/palantir/active-directory-as-code-e9666a2e548d

Sécurisation d'un environnement Azure par Microsoft

https://azure.microsoft.com/en-us/resources/security-best-practices-for-azure-solutions/

Une sandbox Windows basée sur Hyper-V par Ionescu

https://github.com/ionescu007/Simpleator

Détecter "Evil Maid" par Ivan

- En compte les cycles de démarrage du disque dur
- En attendant que VeraCrypt stable inclut SecureBoot
- Ne résiste pas aux attaques de compromission du firmware du disque

https://github.com/JusticeRage/freedomfighting/blob/master/boot_check.py

Pentest

Pirater les pirates

Le FBI crée un faux site FedEx pour arrêter des cybercriminels

- suite à un vol de 82 000 dollars auprès de la société Gorbel
- le site de phishing a été envoyé aux attaquants dans le but de récupérer leurs IP
- Sans succès, le FBI leur a envoyé un document Word contenant une image hébergé au FBI
- Pas d'informations sur le succès de la mission mais un porte-parole du FBI a indiqué que ces techniques étaient efficace.

https://motherboard.vice.com/en_us/article/d3b3xk/the-fbi-created-a-fake-fedex-website-to-unmask-a-cybercriminal

Business et Politique

Business

France

NetXP et Provadys se rapprochent pour fusionner

- Et devenir un leader indépendant de la cybersécurité

https://www.netxp.fr/actualites/provadys-netxp-majj-se-rapprochent-leader-francais-independant-cybersecurite-cloud-infrastructure

Business

International

Facebook a bien donné accès aux données personnelles

- A des sociétés dites “amies” comme Netflix et AirBnb

  https://mashable.com/article/facebook-considered-selling-data-pdf-fail/?europe=true

- La liste de sociétés publiée en juillet peut-être complétée 😋

  https://www.zdnet.fr/blogs/marketing-reseaux-sociaux/ces-societes-a-qui-facebook-livrait-vos-donnees-utilisateur-39870520.htm

AWS rajoute une nouvelle option afin de désactiver définitivement la possibilité de rendre public tout bucket S3

https://aws.amazon.com/fr/blogs/aws/amazon-s3-block-public-access-another-layer-of-protection-for-your-accounts-and-buckets/

Google+, enfin la fin

- Nouvelle faille exposant 50 millions de données
- Fin prévu pour avril 2019

https://www.blog.google/technology/safety-security/expediting-changes-google-plus/?mod=article_inline

Droit / Politique

France

Premier bilan depuis la mise en vigueur du RGPD par la CNIL

- 1 000 notification de violations de données reçus (7 par jour)
- 15 000 DPO nommés
- 6 000 plaintes reçues (+34% que 2017)

https://www.cnil.fr/fr/rgpd-quel-bilan-6-mois-apres-son-entree-en-application

Un appel mondial pour la confiance et la sécurité dans le cyberespace lancé par Emmanuel Macron

- appel signé par 370 Etats, organisation de la société civile et entreprises
- aux absents : Russie, Chine, USA

https://www.latribune.fr/technos-medias/face-aux-pathologies-du-net-macron-lance-un-appel-mondial-pour-la-cybersecurite-797186.html

Droit / Politique

International

Première sanction GDPR en Allemagne, une amende de 20 000 euros pour une plate-forme de chat

- réseau social nommé Knuddels.de
- fait suite à un piratage d'environ 808 000 mails et 1,8 millions d’user/mdp en clair

https://www.bleepingcomputer.com/news/security/first-gdpr-sanction-in-germany-fines-flirty-chat-platform-eur-20-000/

L'OTAN se prépare aux cybermenaces à proximité de la Russie

- 700 responsables de 28 pays membres réunis à Tartu en Estonie pour un entraînement

https://www.nato.int/cps/ic/natohq/news_160898.htm

Conférences

Conférences

Passées

- Black Hat Europe - 3 au 6 décembre 2018 à Londres
- Botconf - 6 au 7 décembre à Toulouse

A venir

- CCC / 35C3 - 27 au 30 décembre 2018 à Leipzig

Divers / Trolls velus

Divers / Trolls velus

Linux remplace les occurrences du f-word par “hugs” dans les commentaires du Kernel

https://www.zdnet.com/article/linux-patch-replaces-f-words-with-hugs-in-kernel-comments-but-some-cry-censorship/

Ericsson désactive le réseau 4G O2 en UK à cause d’un certificat expiré

https://www.forbes.com/sites/daveywinder/2018/12/07/here-is-the-ridiculous-reason-32-million-telefonica-o2-users-waved-goodbye-to-4g-data-yesterday/#70a8598347de

PHP 7.0 c’est bientôt la fin…

- 7.0.* maintenue jusqu’au 3 décembre 2018
- 5.6.* maintenue jusqu’au 31 décembre 2018
- Mais…
  - Drupal a présent requiert une version supérieur à la 7.1 https://groups.drupal.org/node/518200
  - Joomla support PHP dès la version 5.3 https://docs.joomla.org/Technical_requirements
  - WordPress support PHP dès la version 5.2 https://wordpress.org/about/requirements/

Divers / Trolls velus

Le GCHQ soutient le chiffrement

- Mais propose de masquer certaines notifications sur le terminal de la cible
- Le processus de publication des vulnérabilités 0-day sera publié prochainement

https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate

Le WiFi de Starbuck filtre à présent le porno

- Trop de plaintes d'associations

https://www.nextinpact.com/brief/le-wi-fi-public-de-starbucks-dit-adieu-au-porno-6828.htm

ATT&CK pour tester les EDR

- Le MITRE a évalué les principaux éditeurs

https://attackevals.mitre.org/evaluations.html

- Le NSS Lab est contre, souhaitant tester les produits selon leurs propres règles

Divers / Trolls velus

OpenSSL il y'a du changement sur les numéros de version

- Le numéro du correctif de sécurité est intégré plus simplement MAJOR.MINOR.PATCH
- 1.2.3.**a** => 1.2.**a**

https://www.openssl.org/blog/blog/2018/11/28/version/

ProtonMail est-il sécurisé ?

- Réponse rapide : bof, tout du moins il n'y a pas de preuve
- Si un serveur est compromis, alors je Javascript qu'il envoi aussi
- Quelle confiance vis à vis des développeurs ?

https://www.01net.com/actualites/protonmail-service-de-courriels-chiffres-est-il-aussi-sur-qu-il-le-pretend-1571322.html

Chez Telegram aussi il y'a des problèmes

SHA1, Mac-Then-Encrypt, Cypher obscure (Infinite Garble Extension), pas d'authentification des clefs publiques

http://www.cryptofails.com/post/70546720222/telegrams-cryptanalysis-contest

Pannes à répétition sur l'authentification forte de Microsoft

- Modification du code avec effets de bord (latence + race condition)
- Manque de supervision

https://www.computerworld.com/article/3323382/office-software/microsofts-multi-factor-authentication-service-flakes-out-again.html

Divers / Trolls velus

Pas de détection de l'exfiltration des données chez Equifax à cause d'un certificat SSL/TLS

Attackers sent 9,000 queries on these 48 databases, successfully locating unencrypted personally identifiable information (PII) data 265 times. The attackers transferred this data out of the Equifax environment, unbeknownst to Equifax. Equifax did not see the data exfiltration because the device used to monitor ACIS network traffic had been inactive for 19 months due to an expired security certificate. On July 29, 2017, Equifax updated the expired certificate and immediately noticed suspicious web traffic.

After updating the security certificate, Equifax employees identified suspicious traffic from an IP address originating in China. The suspicious traffic exiting the ACIS application potentially contained image files related to consumer credit investigations. Equifax discovered it was under active attack and immediately launched an incident response effort.

https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf

Prochains rendez-vous de l’OSSIR

Prochaine réunion

- Assemblée générale : mardi 8 janvier 2019
  - *Dernière revue de Vlad*

After Work

- ?

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous

Joyeuses fêtes de fin d’année