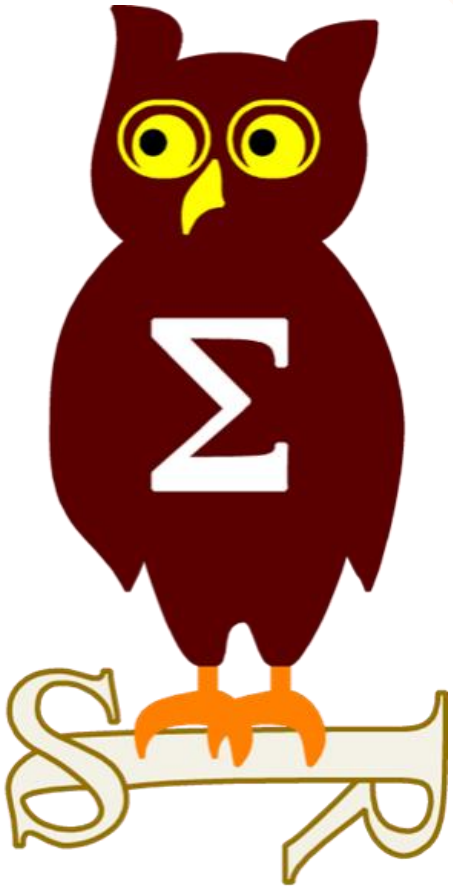
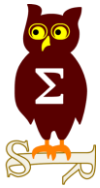


Revue d'actualité

08/01/2019

Préparée par

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



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-180 Vulnérabilités dans Internet Explorer (5 CVE)

- Exploit:
  - 5 x Remote Code Execution
    - Activement exploitée dans la nature : CVE-2018-8653

    https://www.computerworld.com/article/3329717/microsoft-windows/microsoft-delivers-emergency-patch-for-under-attack-ie.html
- Crédits:
  - Clement Lecigne de Google s Threat Analysis Group (CVE-2018-8653)
  - Yu Haiwan and Wu HongJun from Nanyang Technological University par Trend Micro's Zero Day Initiative (CVE-2018-8643)
  - Ivan Fratric de Google Project Zero (CVE-2018-8619, CVE-2018-8625, CVE-2018-8631)

MS18-181 Vulnérabilités dans Edge (5 CVE)

Dont 0 communes avec IE:

- Exploit:
  - 5 x Remote Code Execution

    CVE-2018-8629 : https://securityaffairs.co/wordpress/79264/hacking/microsoft-edge-poc-exploit.html
- Crédits:
  - Bruno Keith (CVE-2018-8629)
  - Anonymous par Trend Micro's Zero Day Initiative, Yuki Chen de Qihoo 360 Vulcan Team (CVE-2018-8618)
  - Qixun Zhao de Qihoo 360 Vulcan Team (CVE-2018-8583, CVE-2018-8624)
  - Lokihardt de Google Project Zero, MoonLiang de Tencent Security Xuanwu Lab, Zhenhuan Li(@zenhumany) de Tencent Zhanlu Lab, Qixun Zhao de Qihoo 360 Vulcan Team, Simon Zuckerbraun par Trend Micro's Zero Day Initiative, Simon Zuckerbraun par Trend Micro's Zero Day Initiative (CVE-2018-8617)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-182 Vulnérabilités dans .Net (2 CVE)

- Affected:
  - Microsoft .NET Framework 3.5, 3.5.1, 4.5.2, 4.6, 4.6.2/4.7/4.7.1/4.7.2
- Exploit:
  - 1 x Denial of Service
  - 1 x Remote Code Execution
    - Publiée publiquement: CVE-2018-8517
- Crédits:
  - Peter St ckli de Alphabot Security, Switzerland (CVE-2018-8540)
  - ? (CVE-2018-8517)

MS18-183 Vulnérabilité dans Windows DNS Server (1 CVE)

- Affected:
  - Windows 10, 2012 R2, 2016, 2019
- Exploit:
  - 1 x Remote Code Execution
- Crédits:
  - Mitch Adair, Microsoft Windows Enterprise Security Team (CVE-2018-8626)

MS18-184 Vulnérabilité dans Text-To-Speech (1 CVE)

- Affected:
  - Windows 10, 2012 R2, 2016, 2019
- Exploit:
  - 1 x Remote Code Execution
- Crédits:
  - Marcin Towalski (@mtowalski1) (CVE-2018-8634)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-185 Vulnérabilités dans Office (6 CVE)

- Affected:
  - Office
- Exploit:
  - 4 x Remote Code Execution
  - 2 x Information Disclosure
- Crédits:
  - Nathan Shomber de Microsoft (CVE-2018-8636)
  - Yangkang(@dnpushme) & Jinquan(@jq0904) de Qihoo360 CoreSecurity(@360CoreSec) (CVE-2018-8627)
  - Omair par Trend Micro's Zero Day Initiative (CVE-2018-8597, CVE-2018-8598)
  - Jaanus Kp Clarified Security par Trend Micro's Zero Day Initiative (CVE-2018-8628)
  - Yonghui Han de Fortinet s FortiGuard Labs (CVE-2018-8587)

MS18-186 Vulnérabilités dans le noyau Windows (4 CVE)

- Affected:
  - Windows toutes versions supportées
- Exploit:
  - 3 x Information Disclosure
  - 1 x Elevation of Privilege
  - Activement exploitée dans la nature : CVE-2018-8611
- Crédits:
  - JunGu and ZiMi de Alibaba Orion Security Lab. (CVE-2018-8621)
  - ZiMi and JunGu de Alibaba Orion Security Lab (CVE-2018-8477, CVE-2018-8622)
  - Igor Soumenkov de Kaspersky Lab Boris Larin de Kaspersky Lab (CVE-2018-8611)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-187 Vulnérabilités dans Microsoft Win32K and/or Graphics Component (3 CVE)

- Affected:
  - Windows toutes versions supportées
- Exploit:
  - 2 x Information Disclosure
  - 2 x Elevation of Privilege
- Crédits:
  - Alex Ionescu, CrowdStrike Inc. (CVE-2018-8637)
  - ? (CVE-2018-8641)
  - bear13oy de DBAPPSecurity Co., Ltd (CVE-2018-8639)

MS18-188 Vulnérabilités dans SharePoint (2 CVE)

- Affected:
  - SharePoint 2010, 2013, 2016
- Exploit:
  - 1 x Information Disclosure
  - 1 x Elevation of Privilege
- Crédits:
  - Nethanel Gelernter de Cyberpion (CVE-2018-8580)
  - Ivan Vagunin (CVE-2018-8635)

MS18-189 Vulnérabilités dans Microsoft Graphics (GDI) (2 CVE)

- Affected:
  - Windows toutes versions supportées
- Exploit:
  - 2 x Information Disclosure
- Crédits:
  - Kamlapati Choubey par Trend Micro's Zero Day Initiative, Behzad Najjarpour Jabbari, Secunia Research at Flexera, Fritz Sands de Trend Micro's Zero Day Initiative (CVE-2018-8595)
  - Fritz Sands de Trend Micro's Zero Day Initiative, Pengsu Cheng de Trend Micro Security Research (CVE-2018-8596)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-190 Vulnérabilité dans Microsoft Dynamics 365 (1 CVE)

- Affected:
  - Microsoft Dynamics NAV 2016, 2017
- Exploit:
  - 1 x Spoofing
- Crédits:
  - Mayank Kapoor de Lateral Security (CVE-2018-8651)

MS18-191 Vulnérabilité dans Telemetry (1 CVE)

- Affected:
  - Windows 10, 2012 R2, 2016, 2019
- Exploit:
  - 1 x Denial of Service
- Crédits:
  - Wayne Low de Fortinet s FortiGuard Labs (CVE-2018-8612)

MS18-192 Vulnérabilité dans Windows Diagnostics Hub (1 CVE)

- Affected:
  - Windows 10, 2012 R2, 2016, 2019
- Exploit:
  - 1 x Elevation of Privilege
- Crédits:
  - Bryan De Houwer de PwC Belgium Cyber&Privacy team (CVE-2018-8599)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-193 Vulnérabilité dans Windows (1 CVE)

- Affected:
  - Windows 10 Version 1809, 2019
- Exploit:
  - 1 x Denial of Service
- Crédits:
  - Krystian Bigaj (CVE-2018-8649)

MS18-194 Vulnérabilité dans RPC (1 CVE)

- Affected:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Information Disclosure
- Crédits:
  - Alex Ionescu, CrowdStrike Inc. (CVE-2018-8514)

MS18-195 Vulnérabilité dans Windows Azure Pack (1 CVE)

- Affected:
  - Windows Azure Pack Rollup 13.1
- Exploit:
  - 1 x Remote Code Execution
- Crédits:
  - Cedric Van Bockhaven on behalf de KPN (CVE-2018-8652)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-196 Vulnérabilité dans Microsoft Exchange Server (1 CVE)

- Affected:
  - Microsoft Exchange Server 2016
- Exploit:
  - 1 x Tampering
- Crédits:
  - Cameron Vincent (CVE-2018-8604)

MS18-197 Vulnérabilité dans DirectX (1 CVE)

- Affected:
  - Windows 10, 2019
- Exploit:
  - 1 x Information Disclosure
- Crédits:
  - Laith AL-Satari (CVE-2018-8638)

Failles / Bulletins / Advisories

Microsoft - Autre

Projet “Mu” : Microsoft ouvre (un peu) UEFI

https://www.nextinpact.com/news/107446-project-mu-microsoft-veut-aller-vers-uefi-plus-modulaires-et-plus-ouverts.htm

https://github.com/topics/projectmu

Avril 2019, fin de support de Windows Embedded POSReady 2009

- Votre fournisseur de distributeur de billet ou de caisse est-il prêt ?

Elévation de privilèges dans Exchange (corrigée en nov.) **/ CVE-2018-8581**

- Permet de lire la boite mail d’un autre utilisateur

https://github.com/WyAtu/CVE-2018-8581/

Failles / Bulletins / Advisories

Système (principales failles)

SQLite - “Magellan”

- Remote Code Execution concernant la “Web SQL API” (Fonction dépréciée depuis 2014)

  https://blade.tencent.com/magellan/index_en.html

  https://meterpreter.org/sqlite-remote-code-execution-vulnerability-alert/

  https://softwareengineering.stackexchange.com/questions/220254/why-is-web-sql-database-deprecated
- Concerne notamment les navigateurs basés sur Chromium
- POC pour Chrome 70 : https://worthdoingbadly.com/sqlitebug/

Jenkins - Un utilisateur anonyme peut devenir administrateur

- CVE-2018-1999001: requête d’authentification spécialement forgée déplace le fichier de configuration “config.xml” dans un autre répertoire. Au prochain redémarrage s’effectuera avec la configuration par défaut.
- CVE-2018-1999043: ajout d’utilisateur temporaire en mémoire
- Plus de 75000 serveurs Jenkins référencés par Shodan

  https://www.zdnet.com/article/thousands-of-jenkins-servers-will-let-anonymous-users-become-admins/

Wordpress 5.0.1 - Security Release

- Publiée 1 semaine après la version 5.0
- Corrige 7 problèmes de sécurité dont certains présents depuis wordpress 3.7

  https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/

Failles / Bulletins / Advisories

Système (principales failles)

Elasticsearch Kibana Console, une belle LFI / CVE-2018-17246

```
GET /api/console/api_server?sense_version=%40%40SENSE_VERSION&apis=../../../../../../../../../../../etc/passwd
```

Multiples vulnérabilités dans Go / CVE-2018-16873 CVE-2018-16874 CVE-2018-16875

- Exécution de code, directory traversal, déni de service
  - `go get -u` exécute du code, en cas d'import d'un package malveillant

https://github.com/golang/go/issues/29230

https://groups.google.com/forum/m/#!topic/golang-announce/Kw31K8G7Fi0

Failles / Bulletins / Advisories

Réseau (principales failles)

Cisco ASA, élévation de privilèges

- Requêtes avec l'utilisateur "notadmin" dans mot de passe
  - Téléchargement de la configuration
  - Ajout d'un utilisateur avec un simple POST

https://www.tenable.com/security/research/tra-2018-46

Les Livebox d'Orange Espagne exposent leurs identifiants WiFi

- 20 000 équipements impactés
- noms et mot de passe dévoilés via une requête GET
- => la plupart des identifiants compromis étaient les mots de passe par défaut, la sensibilisation des utilisateurs doit donc se poursuivre...

https://badpackets.net/over-19000-orange-livebox-adsl-modems-are-leaking-their-wifi-credentials/

Failles / Bulletins / Advisories

Hardware / IoT

Déverrouiller un Android ? Simple comme un appel Skype

- Décrocher à un appel donne accès aux photos, contacts, sms, navigateur...

  https://www.theregister.co.uk/2019/01/03/android_skype_app_unlock/

Déverrouiller un Android ? Simple comme une impression 3D d'un visage

- Fonctionne sur LG G7 Linq, Samsung S9 et Note 8, OnePlus 6

  https://www.tripwire.com/state-of-security/featured/unlocking-android-phones-with-a-3d-printed-head/

Failles / Bulletins / Advisories

SCADA

Vulnérabilité de type DoS sur les produits Yokogawa

- Vulnérabilité dans le driver VNET / OpenIP communication
- Permet de stopper les communications réseau
- Certains produits liés à la safety sont également impactés

https://web-material3.yokogawa.com/YSAR-18-0008-E.pdf

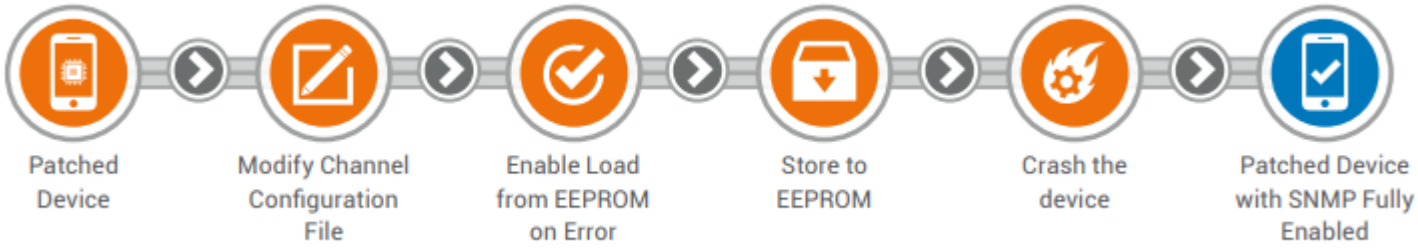
Vulnérabilités dans certains produits Moxa

Absence d'authentification sur des passerelles Ethernet pour les automates de surêté

https://ics-cert.us-cert.gov/advisories/ICSA-18-352-01

Vulnérabilité sur les automates Rockwell MicroLogix

- Chaînage de vulnérabilités intéressant



https://talos-intelligence-site.s3.amazonaws.com/production/document_files/files/000/047/124/original/Micrologix_WhitePaper_v6.pdf

Piratages, Malwares, spam, fraudes et DDoS

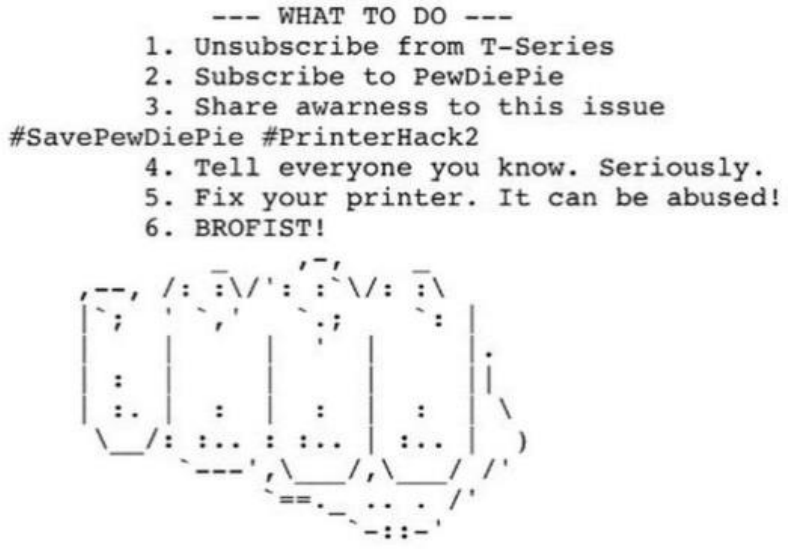
Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

PewDiePie: HackerGiraffe a encore frappé

- Cible: 100 000 imprimantes exposées sur internet (50 000 imprimantes lors du round 1)
- Technique: utilisation de PRET - Printer Exploitation Toolkit (GitHub)
- Objectif: promouvoir la chaine YouTube PewDiePie contre TSeries

  https://www.bbc.com/news/technology-46552339
- Idem sur les Chromecasts, Google Home et SmartTVs



PRETty outil pour automatiser les attaques sur les imprimantes

- PRinter Exploitation Toolkit

  https://github.com/BusesCanFly/PRETty

Collision MD5

- Collision préimage

  https://github.com/corkami/pocs/blob/master/collisions/README.md#gotta-collide-em-all

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Fraude publicitaire par des applications android

- Les clics provenant d'application iOS rapportent plus
- Le malware "Andr/Clickr-ad" se fait passer pour un iPhone
- Implémenté dans plus de 25 applications disponibles sur Google Play Store

https://www.theregister.co.uk/2018/12/10/android_ios_clickfraud/

https://nakedsecurity.sophos.com/2018/12/10/android-click-fraud-apps-mimic-apple-iphones-to-boost-revenue/

Un malware Android siphonne les comptes PayPal

- Trojan camouflé dans un outil d'optimisation de batterie sur des stores non officiel
- Utilise "Android Accessible Service"
- Après installation, transfert de 1000€ (la devise dépend de la configuration du téléphone)
- Contourne le 2FA mis en place par PayPal

https://www.welivesecurity.com/2018/12/11/android-trojan-steals-money-paypal-accounts-2fa/

Le DRM Google Widevine L3 notamment utilisé par Netflix et Spotify a été cassé

- L3 est moins sécurisé que L1 (qui nécessite du matériel spécifique)
- via un défaut de conception du à une implémentation hasardeuse
- attaque basé sur la comparaison du flux chiffré avec le flux déchiffré (DFA)
- le chercheur va poursuivre ses recherches sur L1 dans les semaines à venir

https://twitter.com/David3141593/status/1080606827384131590

Comment Linkedin espionne les extensions des navigateurs

- 2 méthodes : requêtes vers chrome-extension:// et vers les ressources des extensions

https://github.com/dandrews/nefarious-linkedin

Piratages, Malwares, spam, fraudes et DDoS

Fuites de données

Fuites de données sur Facebook et Twitter

- Une erreur au sein de Twitter permettait à certains services tiers d'accéder aux messages personnels
- Twitter touché également par une fuite d'informations via son API de support
- Facebook aurait permis à 150 sociétés d'accéder aux données personnelles des utilisateurs
- Facebook : un bug a exposé des photos non partagées de 6,8 millions d’utilisateurs

https://securityaffairs.co/wordpress/78933/social-networks/twitter-bug-dm-exposure.html

https://help.twitter.com/en/support-form

https://newsroom.fb.com/news/2018/12/facebooks-partners/

https://developers.facebook.com/blog/post/2018/12/14/notifying-our-developer-ecosystem-about-a-photo-api-bug/

Les données de 2,4 millions d'utilisateurs du gestionnaire de mot de passe Blur ont fuité

- emails, noms prénoms, indice pour certains mots de passe et le mots de passe chiffrés des utilisateurs
- un chercheur indépendant aurait découvert un serveur exposant un fichier contenant les informations

https://www.abine.com/blog/2018/blur-security-update/

Piratages, Malwares, spam, fraudes et DDoS

Fuites de données

La chaîne de café américaine Caribou annonce une fuite de données concernant les cartes bancaires de ses clients

- 239 sur 603 points de vente physique impactés
- noms, numéros de cartes, dates d'expiration et codes de sécurité compromis

https://www.zdnet.com/article/caribou-coffee-chain-announces-card-breach-impacting-239-stores/

Des documents confidentiels provenant d'Allemagne publiés sur Twitter

- principales formations politiques touchés excepté le parti d'extrême droite qui est de fait supposé à l'origine
- Des personnalités du monde des médias et de la culture touchés également
- les documents publiés entre le 1er et le 28 décembre sur Twitter

https://www.lemonde.fr/international/article/2019/01/05/vive-emotion-en-allemagne-apres-les-revelations-d-une-cyberattaque-massive_5405339_3210.html

Piratages, Malwares, spam, fraudes et DDoS

Espionnage

Le groupe The Dark Overlord publie des fichiers liés aux attentats du 11 septembre 2001

- publication de documents par paliers de bitcoin reçus
- 650 fichiers publiés dont certains présentés comme hautement confidentiels

https://steemit.com/@thedarkoverlord/

La République Tchèque déconseille l'utilisation de produits Huawei et ZTE

- L'arrestation du directeur financier de Huawei à Vancouver pour des transactions avec l'Iran prohibées par les États-Unis ne joue pas en faveur de l'équipementier.

https://www.voanews.com/a/czech-republic-warns-against-using-huawei-zte-products/4704151.html

https://isc.sans.edu/forums/diary/Arrest+of+Huawei+CFO+Inspires+Advance+Fee+Scam/24396/

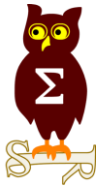
Les USA ont peur de Huawei

https://www.developpez.com/actu/239399/Voici-6-raisons-pour-lesquelles-Huawei-donne-aux-Etats-Unis-et-a-ses-allies-des-cauchemars-en-matiere-de-securite-informatique/

Les USA accusent les chinois du vol de données à la NASA, la Navy et l'industrie technologique

- deux chinois accusé d'être en lien avec APT10 et d'avoir dérobé des informations à plus de 45 entreprises ou organisations

https://www.cnet.com/news/us-charges-chinese-hackers-with-massive-theft-from-nasa-navy-and-tech-sector/



Nouveautés, outils et techniques

Crypto et Divers

Divers

Autorité de certification Symantec retirée de Firefox 64

- Initialement prévu dans la version 63 mais reporté car cette AC était encore trop utilisée

  https://blog.mozilla.org/security/2018/03/12/distrust-symantec-tls-certificates/

  https://blog.mozilla.org/security/2018/10/10/delaying-further-symantec-tls-certificate-distrust/

Utilisation de cartes à puces dans un domaine AD 2016

- Possibilité de faire expirer automatiquement le mot de passe

  https://medium.com/@rootsecdev/virtual-smart-cards-and-password-hashes-in-active-directory-2016-environments-dd0340a4126

Lancement d'un programme d'authentification entre produits USB Type-C

- Authentifier tout appareil se connectant au système hôte (chargeur, périphérique, câble)
- Authentification avant tout transfert de données ou **d'énergie**

  https://www.zdnet.com/article/usb-type-c-gets-authentication-to-protect-against-malicious-devices/

Pentest
Techniques & outils

Modlishka et phishing 2FA

- Fonctionnement de type reverse proxy
- Permet de réaliser des campagnes de phishing pour des sites qui requièrent un second facteur d'authentification

https://github.com/drk1wi/Modlishka

Restaurer un contrôleur de domaine à partir de NTDS.DITR et SYSVOL

https://github.com/MichaelGrafnetter/DSInternals

Identifier les faiblesses de configuration de SYSMON

https://github.com/mkorman90/sysmon-config-bypass-finder

ss7MaPer, un outil pour auditer SS7

https://www.developpez.com/actu/239399/Voici-6-raisons-pour-lesquelles-Huawei-donne-aux-Etats-Unis-et-a-ses-allies-des-cauchemars-en-matiere-de-securite-informatique/

https://github.com/ernw/ss7MAPer

uncaptcha2

- Permet de contourner le ReCaptcha Google avec 91% de réussite grâce… à Google Speech2Text API

  https://github.com/ecthros/uncaptcha2

Pentest

Pirater les pirates

Bleeping Computer propose plusieurs guides pour récupérer vos données chiffrées par un rançongiciel

- InsaneCrypt:

  https://www.bleepingcomputer.com/ransomware/decryptor/how-to-decrypt-the-insanecrypt-or-everbe-1-family-of-ransomware/

- HiddenTear (et ses déclinaisons)

  https://www.bleepingcomputer.com/ransomware/decryptor/how-to-decrypt-hiddentear-ransomware-variants/

  => Dans les 2 cas, cela nécessite de télécharger un exécutable (prudence)

Troller les bots en leur répondant un challenge crypto consommateur en ressources CPU

https://twitter.com/J0hnnyXm4s/status/1081227041255706626

Business et Politique

Business

France

Responsable du CERT BdF

- L’offre pour remplacer Saad est toujours en ligne…

  https://docs.google.com/presentation/d/1h27ga2aoT1cDkE1MV3YQ70nAsBO0VOBpdvJtUN-Ku0I/edit#slide=id.g365da3a17_2_20

Business

International

Interactions des applications Android avec Facebook

- 61% des applications testées envoient des informations à Facebook, que l'on soit connecté ou non, que l'on ai un compte ou non
- Certains informations très sensibles sont envoyées: recherche de vols d'avion par exemple
- Les informations sont envoyées avec l'identifiant unique Google (AAID)
- La politique de gestion des cookies sélectionnée pour Facebook ne semble pas influer sur les données envoyées

https://privacyinternational.org/campaigns/investigating-apps-interactions-facebook-android

Internet, nid de bots, tout est faux!

- Plus de la moitié du trafic serait lié à de l'arnaque à la publicité

http://nymag.com/intelligencer/2018/12/how-much-of-the-internet-is-fake.html

Droit / Politique

France

La CNIL condamne Bouygues Telecom pour manquement à la sécurité des données personnelles de ses clients

- Amende de 250 000 €
- CNIL informée en mars 2018 de l'existence d'une vulnérabilité conduisant à l'exposition de données personnelles de clients B&You
- La vulnérabilité permettait d'accéder à des contrats et des factures en modifiant un élément de l'URL sur le site Web de Bouygues Telecom.
- Présente depuis 2 ans, plus 2 millions de clients seraient concernés

https://www.cnil.fr/fr/bouygues-telecom-sanction-pecuniaire-pour-manquement-la-securite-des-donnees-clients

Décret sur les modalités de l'application de l'article 34 de la LPM

- Renforcement des missions de l'ANSSI
  - Détection d'attaques chez les opérateurs
  - Déploiements (temporaire) de sondes de l'ANSSI chez les opérateurs
  - Ces actions seront contrôlées par l'ARCEP

https://www.ssi.gouv.fr/actualite/lpm-2019-2025-la-publication-du-decret-dapplication-de-larticle-34-renforce-les-missions-de-lanssi/

Droit / Politique
International

L'EU lance un BugBounty sur plusieurs outils open source

- Dont FileZilla, notepad++, KeePass, 7zip, Drupal (!!?), tomcat, kafka, putty…
- 2 plateformes : HackerOne (US) et Intigriti/Deloitte (fat four)
- Total des primes par programme : entre 25k€ et 90k€
  - Comparaison avec Zerodium : RCE sur 7-Zip payée $80k

https://juliareda.eu/2018/12/eu-fossa-bug-bounties/

L'Australie veut écouter les communications chiffrées (excuse: le terrorisme)

- Projet de loi pour forcer les sociétés technologiques à collaborer avec le gouvernement Australien

  https://parlinfo.aph.gov.au/parlInfo/download/legislation/billsdgs/6370016/upload_binary/6370016.pdf
- Adoptée par le parlement australien le 7 décembre 2018

  https://www.wired.com/story/australia-encryption-law-global-impact/
- Réaction de Signal:
  - Secure by design : backdoor impossible
  - Bloquer l'accès aux utilisateurs situés en australie
  - Conséquence pour les personnes de passage (touristes, déplacement d'affaire, …)
  - Méthode peut efficace (VPN, Store Apple/Android alternatif)

  https://signal.org/blog/setback-in-the-outback/

Droit / Politique
International

Medical Informatics Engineering (MIE) poursuivi

- MIE est un prestataire d'hébergement de dossier de santé
- Fuite d'informations en 2015
  - 3,9 millions de personnes
  - Données: nom, adresse, numéro de sécurité social, résultat test médicaux, police d'assurance, …
- Poursuite par 12 états des USA pour violation du HIPAA

  https://www.hipaanswers.com/medical-informatics-engineering-faces-multi-state-lawsuit-over-3-9-million-record-breach
- Class Action en cours de création en vu d'obtenir un dédommagement

  http://www.journalgazette.net/news/local/20181204/local-med-data-firm-focus-of-breach-suit

Rhode Island poursuit Google suite aux fuites de données via Google+

- Fuite de données via Google+ connu en Mars 2018 mais Google a communiqué qu'en Novembre 2018 après avoir corrigé la faille
- Poursuites engagées par ERSRI (Employees Retirement System of Rhode Island), un fond de pension pour les employés municipaux.
- Motif des poursuites : "Google had an obligation to tell its users and investors that private information wasn't being protected"

  https://www.zdnet.com/article/rhode-island-sues-google-after-latest-google-api-leak/

Droit / Politique
International

P0rn et deep-fake

- Utilisation de machine learning pour créer de fausses vidéos
- Utilisé pour des campagnes d'intimidation

https://www.washingtonpost.com/technology/2018/12/30/fake-porn-videos-are-being-weaponized-harass-humiliate-women-everybody-is-potential-target/

Droit / Politique
International

Marriott rembourse les frais de renouvellement de passeport des victimes

- La victime doit néanmoins prouvé l'utilisation frauduleuse de son passeport

https://www.hotelmanagement.net/security/approximately-500-million-guests-impacted-marriott-data-breach

Department of Homeland Security (DHS) veut désanonymiser Zcash and Monero

- Il s'agit d'une "PRE-SOLICITATION" et non d'une "REQUEST FOR PROPOSALS"

https://www.fbo.gov/utils/view?id=f0e31ab37561cac3cc4a4ab88d9059b0

Border agents are copying travelers' data, leaving it on USB drives

- Si en passant les frontières américaines, vous avez été interrogé et que votre matériel informatique a été réquisitionné, il est fort probable que vos données trainent sur un disque dur USB au sein du US Customs and Border Protection.

https://nakedsecurity.sophos.com/2018/12/13/border-agents-are-copying-travelers-data-leaving-it-on-usb-drives/

Microsoft demande à ce que la reconnaissance facial soit légiférée

https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/

https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/

Conférences

Conférences

Passées

- CCC 35 - 27 au 30 décembre 2018 à Leipzig
  - 286 points d'accès WiFi
  - 10 821 utilisateurs sur le WiFi
  - 24 539 adresses Mac uniques
  - 558 points d'accès "Rogue"

A venir

- S4 (SI industriel) - 14 au 17 janvier à Miami
- CORI&IN - 22 janvier 2019 à Lille
- FIC - 22 au 23 janvier 2019 à Lille
- Troopers19 - 18 au 22 mars à Heidelberg (Allemagne)

Divers / Trolls velus

Divers / Trolls velus

Joyeux Noel, Zerodium augmente ses primes

- RCE Windows : $1 million
- RCE iOS : $2 millions
- RCE Apache ou IIS : $500k

https://zerodium.com/program.html

Support de PHP

- PHP 5.x n'est plus supporté
- PHP 7.0 n'est plus supporté
- PHP 7.1 l'est encore jusqu'à décembre 2019
- Plus de 70% des sites utilisent une version de PHP non supportée

https://w3techs.com/technologies/details/pl-php/all/all

Divers / Trolls velus

Pourquoi l'extension des fichiers temporaires de SQLite est sqlite_ ?

- A cause de McAfee

```
/*
** Temporary files are named starting with this prefix followed by 16 random
** alphanumeric characters, and no file extension. They are stored in the
** OS's standard temporary file directory, and are deleted prior to exit.
** If sqlite is being embedded in another program, you may wish to change the
** prefix to reflect your program's name, so that if your program exits
** prematurely, old temporary files can be easily identified. This can be done
** using -DSQLITE_TEMP_FILE_PREFIX=myprefix_ on the compiler command line.
**
** 2006-10-31:  The default prefix used to be "sqlite_".  But then
** Mcafee started using SQLite in their anti-virus product and it
** started putting files with the "sqlite" name in the c:/temp folder.
** This annoyed many windows users.  Those users would then do a
** Google search for "sqlite", find the telephone numbers of the
** developers and call to wake them up at night and complain.
** For this reason, the default name prefix is changed to be "sqlite"
** spelled backwards.  So the temp files are still identified, but
** anybody smart enough to figure out the code is also likely smart
** enough to know that calling the developer will not help get rid
** of the file.
*/
#ifndef SQLITE_TEMP_FILE_PREFIX
# define SQLITE_TEMP_FILE_PREFIX "etilqs_"
#endif
```

http://www.sqlite.org/cgi/src/raw/src/os.h?name=3e57a24e2794a94d3cf2342c6d9a884888cd96bf

Mitnick redécouvre le phishing pour contourner l'authentification à double facteur

- C'est dur de vieillir…

https://www.cnbc.com/amp/2019/01/04/how-secure-is-your-account-two-factor-authentication-may-be-hackable.html

Divers / Trolls velus

Baidu peut cloner une voix avec un enregistrement de moins de 4s

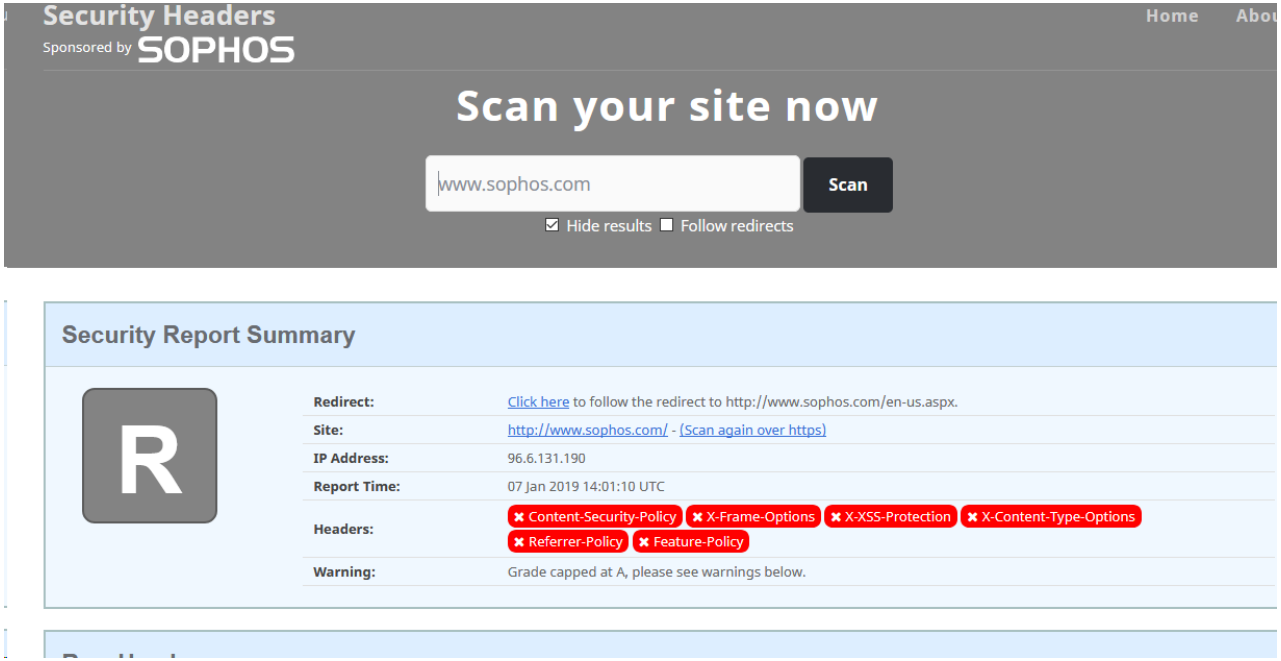
- Orange Labs le faisait déjà il y'a 8 ans : Orange Vallée -> Kagedo -> Voxygen
  - Mais avec un enregistrement des voix en studio
- Non la biométrie n'est pas une méthode d'authentification (cf. Philippe WOLF)

http://www.ehackingnews.com/2018/12/a-software-that-can-clone-anyones-voice.html

Analyse tes entêtes HTTP avec Sophos

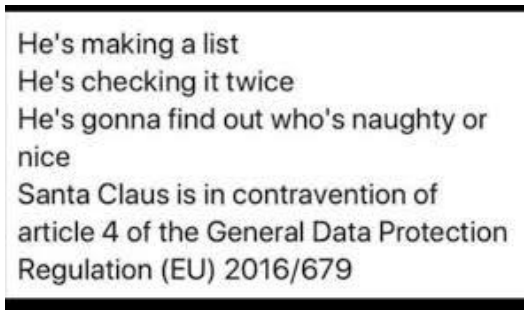
- … et surtout ne le configure pas comme Sophos 😂

https://securityheaders.com/



Divers / Trolls velus

Le Père Noël n'est pas conforme GDPR



Top 100 des plus mauvais mot de passe en 2018 (par SplashData)

- Nouveau dans le top 10 : 111111 (6ème) et sunshine (8ème)
- SplashData estime que 10% des personnes ont utilisé au moins une fois l'un des 25 des pires mots de passe

https://www.teamsid.com/100-worst-passwords/

https://www.teamsid.com/100-worst-passwords-top-50/

Audit du système de défense antimissile balistique américain

- Pas de chiffrement, authent faible, peu de supervision, de (très) vieilles vulns non corrigées

https://media.defense.gov/2018/Dec/14/2002072642/-1/-1/1/DODIG-2019-034.PDF

`<< The xxx CIO did not meet the program's expectations to manage risk when xxxx allowed critical and high vulnerabilities to remain unmitigated on their networks>>`

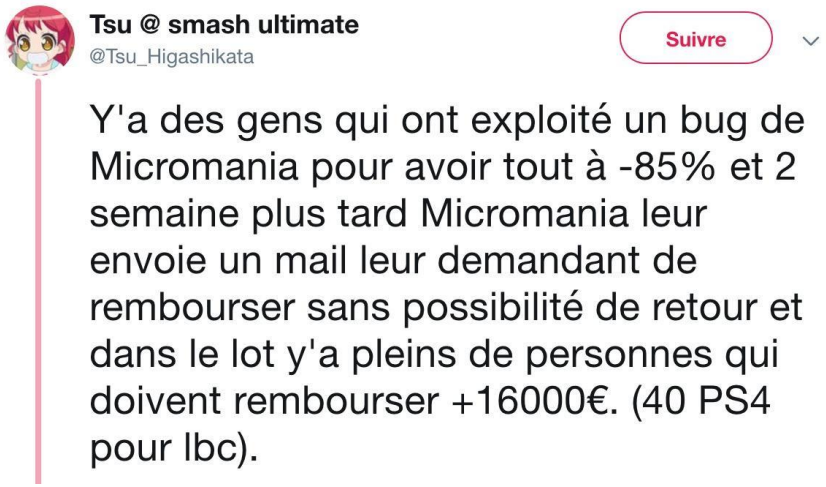
https://www.developpez.com/actu/238067/Le-systeme-de-defense-antimissile-balistique-US-echoue-lamentablement-a-un-audit-de-cybersecurite-des-manquements-graves-identifies-sur-des-sites/

Divers / Trolls velus

Une vulnérabilité exploitée pendant le Black Friday pour profiter de réductions chez Micromania

- Micromania a attendu la fin du délai de rétractation pour demander la différence

https://pastebin.com/5JSgdiX5



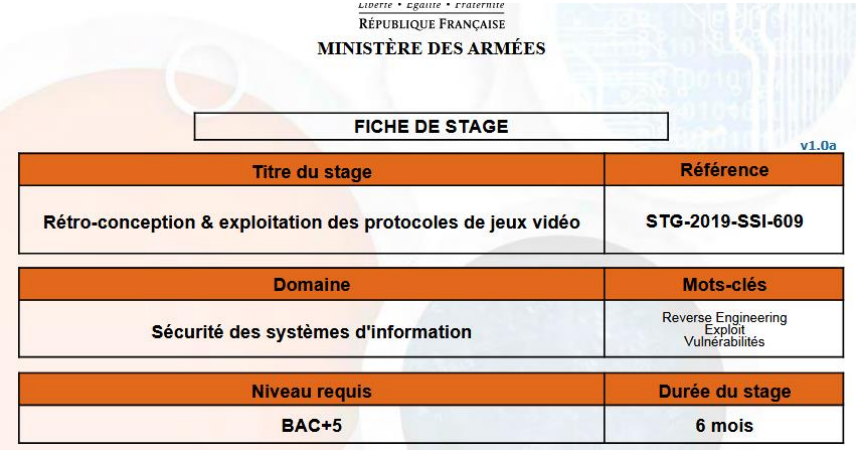

```
13. - J'ai arnaqué personne j'ai même pas pris de PS4 alors que j'aurais pu ! J'ai juste pris une switch, une Xbox, 300 euros de jeux, et des goodies. J'ai été super raisonnable, ils n'ont pas le droit de poursuivre les gens honnêtes et raisonnables !!
14.
```

Divers / Trolls velus

Tu cherches un stage sympa ?

- Viens donc jouer à Fortnite à la DGSE

  https://perso.univ-rennes1.fr/sylvain.duquesne/master/documents/stages_mindef.pdf



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DES ARMÉES

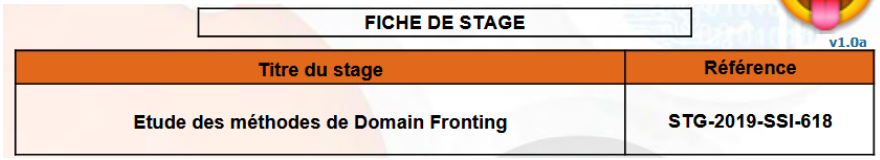
FICHE DE STAGE v1.0a

Titre du stage	Référence
Rétro-conception & exploitation des protocoles de jeux vidéo	STG-2019-SSI-609

Domaine	Mots-clés
Sécurité des systèmes d'information	Reverse Engineering Exploit Vulnérabilités

Niveau requis	Durée du stage
BAC+5	6 mois

- Certains stages sont tellement 2018….



FICHE DE STAGE v1.0a

Titre du stage	Référence
Etude des méthodes de Domain Fronting	STG-2019-SSI-618

- Ou comment passer la douane US

FICHE DE STAGE v1.0a

Titre du stage	Référence
Développement d'une solution simulant un smartphone éteint	STG-2019-SSI-624

Les Top arbitraires de l’année écoulée

Les Top arbitraires de l'année écoulée

2018, l'année de l'explosion du nombre de **vulnérabilités** sur les **CPU**

- BranchScope, Spectre Next Gen, MOV SS, POP SS et beaucoup de variantes

2018, l'année confirmant une nouvelle fois l'insécurité des solutions de sécurité

- Cisco **ASA**, exécution de code à distance sans authentification / CVE-2018-0101
- Cisco IOS, 2 exécutions de code à distance sans authentification + une backdoor
- Cisco **ASA**, déni de service / CVE-2018-15454
- **Prim'X Zed!**, création de fichier arbitraire
- **CyberArk Password Vault**, fuite mémoire sans authentification / CVE-2018-9842
- **IBM QRadar**, exécution de code à distance / CVE-2018-1418

2018, une mauvaise années (publiquement) pour les services Russes

- Les renseignements néerlandais (AIVD) ont compromis les Russes d'APT29 / Cozy Bear
- Rapport estonien sur les capacités offensives Russes
- Les services hollandais doxxent des agent du GRU

2018, l'année dans la continuité des précédentes sur les **fuites de données**

- Under Amour, MyHeritage, les informations personnelles de 200 millions de Japonais, Marriott, Quora...

Les Top arbitraires de l'année écoulée

2018, une nouvelle année de **vulnérabilités** touchant de très **larges périmètres**

- Les hyperviseurs (VMware, Virtualbox, Xen)
- Les consoles (Nintendo Switch, PS4)
- Ledger
- Les imprimantes
- *BSD (x.org)
- Les disques SSD auto-chiffrés
- Bluetooth
- Les pompes à essence (avec vol d'essence)
- RawHammer depuis le réseau avec un composant "Remote Direct Memory Access/RDMA"
- Les ports iLo des serveurs

2018, l'année des **problèmes** récurrents avec les mises à jour **Windows 10**

2018, une nouvelle année de la **concentration** des acteurs du **marché** français de la sécurité

- Fusion de NetXP et Provadys
- Rachat de SysDream par HubOne
- Rachat de NES par Serma
- Fusion de CDP, Avisa et Lexfo *(Cabinet Demeter Partners : défense de la réputation sur le Web)*

Les Top arbitraires de l'année écoulée

2018, l'année des **vulnérabilités** et **portées dérobées incompréhensibles**

- Deux vulnérabilités de jQuery File Upload avec vidéo sur Youtube depuis 2015
- Bibliothèques malveillantes PyPi
- Porte dérobée dans la librairie Python SSH-Decorator
- Porte dérobée dans la librairie NodeJS getcookies
- Porte dérobée dans la librairie NodeJS getcookies event-stream
- Malware pré-installés par défaut sur 141 équipements Android low cost
- Porte dérobée dans 17 images Docker sur Docker Hub

2018, l'année des vulnérabilités des **années 90**

- Contournement d'authentification sur libssh
- Nginx, avec ".." après un nom de répertoire
- Elévation de privilège locale sous linux depuis 8 ans (DisplayLink)

Les Top arbitraires de l'année écoulée

Mais il faut rester **positif** :

- GDPR / RGPD est là !
- TLS 1.3 est enfin sorti
- Le framework ATT&CK est sorti
- Windows 10 supporte les Yubikey
- Microsoft abandonne son moteur de navigation web pour Chromium
- Nos renseignements ont une alternative à Palantir (projet Artemis par CapGemini et Atos prévu pour 2019)
- Le prix journalier des experts de l'ANSSI passe à 1200€

Prochains rendez-vous de l’OSSIR

Prochaines réunions

Prochaine réunion

- Mardi 12 février 2019

After Work

- ?

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous

Dernière revue d’actu pour Vlad

Bonne année 2019 à tous

Bonne année 2019 à tous