Revue d'actualité de l'OSSIR

9 mars 2021

Aurélien Denis
*Vladimir Kolla @mynameisv_*
Étienne Baudin @etiennebaudin

Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

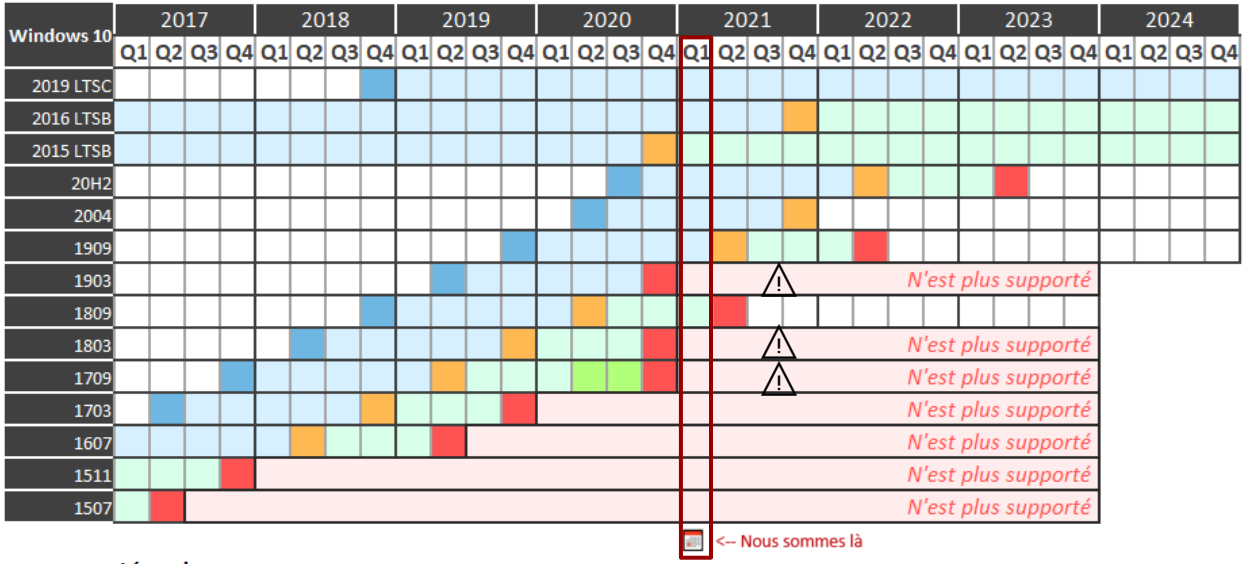
Report des fins de support de produits Microsoft suite au Covid-19

- Report de 6 mois
  - Windows 10, version 1709
  - Windows 10, version 1809
  - Windows Server, version 1809
  - Configuration Manager 1810
  - SharePoint Server 2010, SharePoint Foundation 2010, and Project Server 2010
  - Dynamics 365 cloud services
  - Basic Authentication in Exchange Online

https://www.bleepingcomputer.com/news/microsoft/microsoft-delays-end-of-support-for-older-windows-software-versions/

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Rappel du support Windows 10 en couleurs



mardi 13 novembre 2018	mardi 9 janvier 2024	mardi 9 janvier 2029
mardi 2 août 2016	mardi 12 octobre 2021	mardi 13 octobre 2026
mercredi 29 juillet 2015	mardi 13 octobre 2020	mardi 14 octobre 2025
mardi 20 octobre 2020	mardi 10 mai 2022	mardi 9 mai 2023
mercredi 27 mai 2020	mardi 14 décembre 2021	mardi 14 décembre 2021
mardi 12 novembre 2019	mardi 11 mai 2021	10 mai 2022**
mardi 21 mai 2019	mardi 8 décembre 2020	mardi 8 décembre 2020
mardi 13 novembre 2018	mardi 10 novembre 2020	11 mai 2021**
lundi 30 avril 2018	mardi 12 novembre 2019	mardi 10 novembre 2020
mardi 17 octobre 2017	~~9 avril~~ 4 sept. 2019	~~14 avril~~ 13 oct. 2020
5 avril 2017*	mardi 9 octobre 2018	mardi 8 octobre 2019
mardi 2 août 2016	mardi 10 avril 2018	mardi 9 avril 2019
mardi 10 novembre 2015	mardi 10 octobre 2017	mardi 10 octobre 2017
mercredi 29 juillet 2015	9 mai 2017	mardi 9 mai 2017

Légende :

- Date de mise à disposition pour le public et les entreprises
- Support
- Fin de support pour les versions Home, Pro, Pro Education et Pro for Workstations / fin de support standard pour LTSB/LTSC
- Support uniquement pour les versions Enterprise et Education
- Prolongation exceptionnelle suite au Coronavirus
- Fin de support pour toutes les versions / fin de support étendu pour LTSB/LTSC

Failles / Bulletins / Advisories
Microsoft - Avis

En février :

- 56 vulnérabilités corrigées, dont 9 critiques

- A retenir :
  - CVE-2021-1732 : **En cours d'exploitation**
    - Elévation de privilèges via Win32K
  - CVE-2021-21148 : **En cours d'exploitation**
    - RCE dans Edge
  - CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 et CVE-2021-27065 : **En cours d'exploitation** (Exchange)

Composants impactés

Windows 10
Windows 7
Windows RT 8.1
Windows Server (1903)
Windows Server (1909)
Windows Server (2004)
Windows Server (20H2)
Windows Server 2008 R2
Windows Server 2012 R2
Windows Server 2016
Windows Server 2019
Framework .NET
Microsoft 365 Apps
Microsoft Azure
Microsoft Dynamics 365
Microsoft Dynamics
Microsoft Edge
Microsoft Exchange
Microsoft Lync Server
Microsoft Office (Word, Excel, PowerP
Microsoft Security Essentials
Microsoft System Center Endpoint Pro
Microsoft Teams
Microsoft Windows Defender
Sharepoint
Skype
Visual Studio

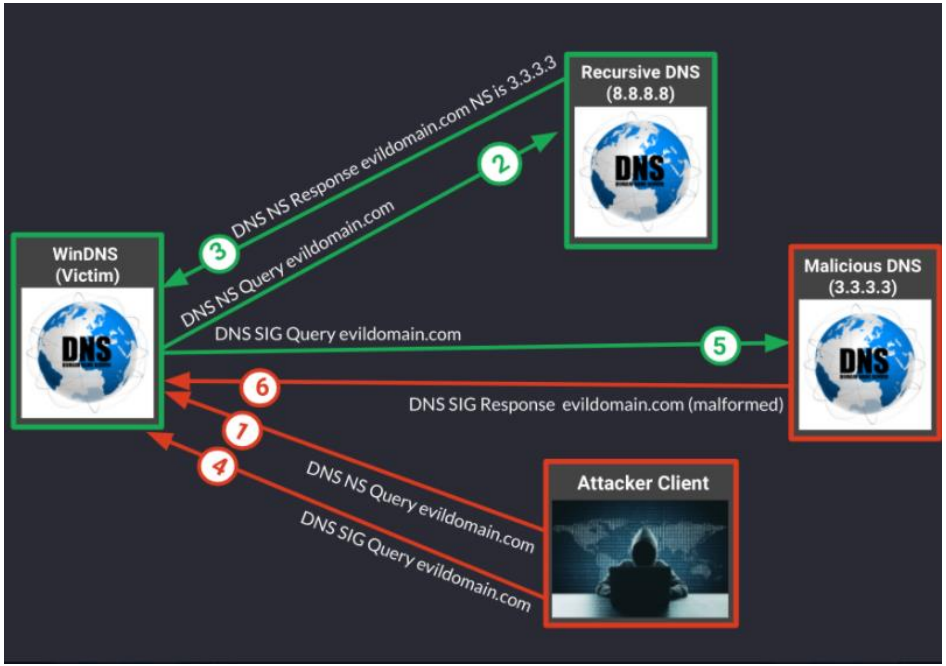
Failles / Bulletins / Advisories
Microsoft - Avis

*(exploit)*Prise de contrôle du système via une vulnérabilité au sein du serveur DNS Windows (SIGRED)

- RCE via le champ SIG
- Corrigé en Octobre 2020
- Code d'exploitation public

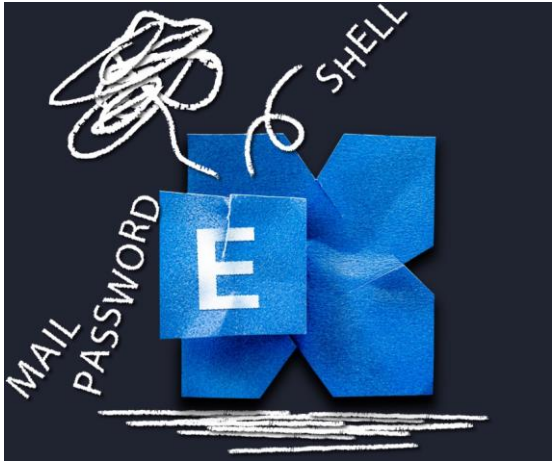
  https://github.com/chompie1337/SIGRed_RCE_PoC
- Toutes les explications ici :

  https://www.graplsecurity.com/post/anatomy-of-an-exploit-rce-with-cve-2020-1350-sigred



Failles / Bulletins / Advisories
Microsoft - Avis

Spoiler pour le Patch Tuesday de Mars 2021 : ProxyLogon !



- 4 CVE
  - CVE-2021-26855
  - CVE-2021-26857
  - CVE-2021-26858
  - CVE-2021-27065
- SSRF/PrivEsc/arbitrary file upload
- Utilisé massivement par le groupe *HAFNIUM*
  - (lié à ChinaChopper?)
- L'article de base :
  https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
- Les contournements si la mise à jour n'est pas possible
  - Pensez à tester à nouveau la présence des vulnérabilités après-coup

https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2(
https://github.com/microsoft/CSS-Exchange/tree/main/Security

Failles / Bulletins / Advisories
Microsoft - Avis

Spoiler pour le Patch Tuesday de Mars 2021 : ProxyLogon !

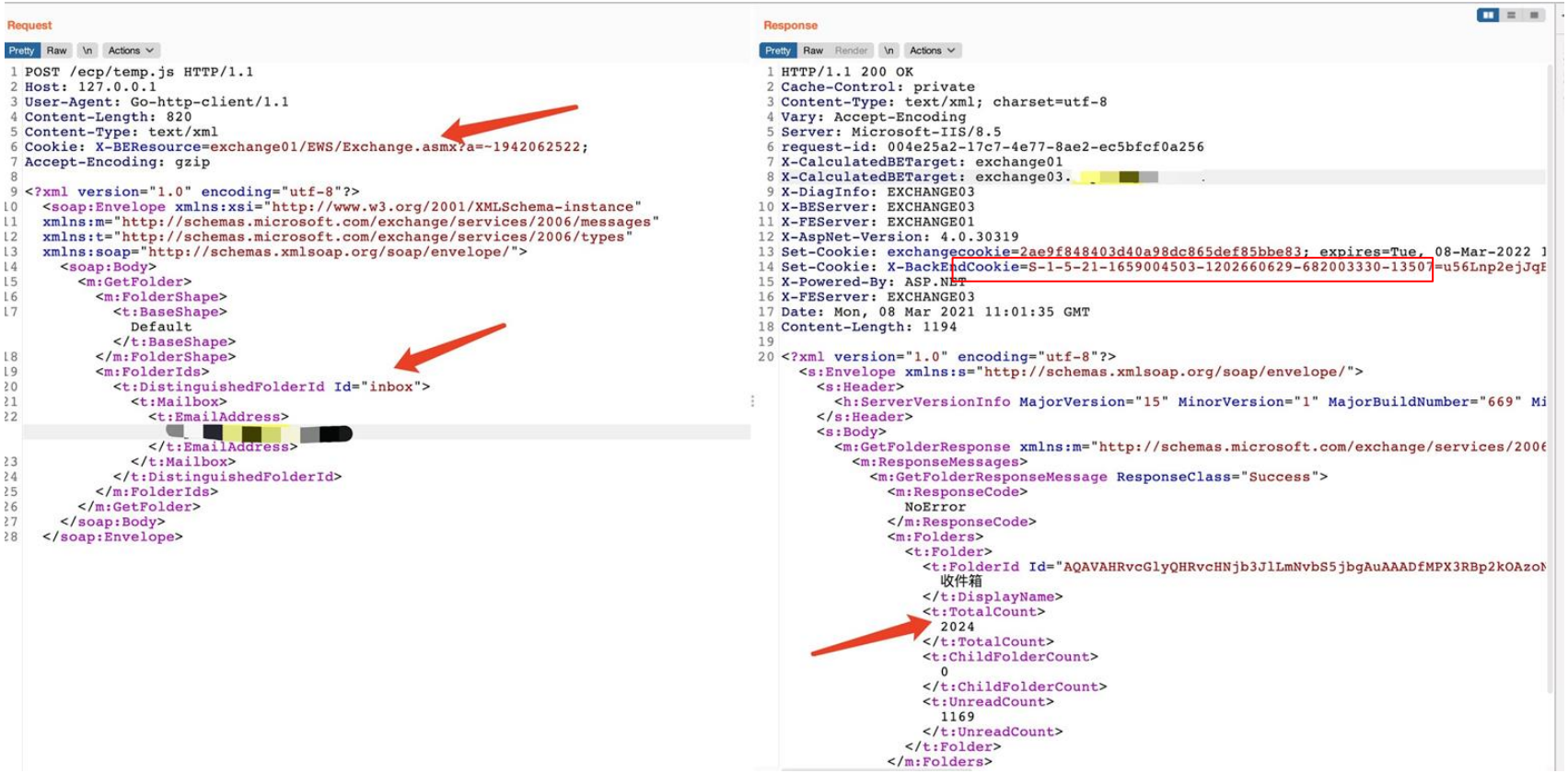
- Internet est massivement scanné puis exploité par d'autres groupes/individus
- Piratage de :
  - Plus de 30,000 administrations américaines (agences, gouvernementales, villes … mais aussi des entreprises)
  - L'Autorité Bancaire Européenne

  https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/
- Le bulletin CERT-FR est régulièrement mis à jour

  https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-004/
- Microsoft a publié des scripts pour aider à la détection

  https://github.com/microsoft/CSS-Exchange/

Failles / Bulletins / Advisories
Systèmes de sécurité



source: https://twitter.com/jas502n/status/1368882907893223425

Failles / Bulletins / Advisories
Navigateurs (principales failles)

Prise de contrôle du système et manipulation de données via 47 vulnérabilités au sein de Google Chrome

- Dont 3 dépassements de mémoire tampon sur le tas

https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html

Prise de contrôle du système et contournement de sécurité via 12 vulnérabilités au sein de Firefox et Firefox ESR (mfsa2021-07/mfsa2021-08)

- "Content Security Policy violation report could have contained the destination of a redirect"

https://www.mozilla.org/en-US/security/advisories/mfsa2021-07/

https://www.mozilla.org/en-US/security/advisories/mfsa2021-08/

Manipulation de données et déni de service via 9 vulnérabilités au sein de Microsoft Edge

- Proviennent du moteur Chromium

Failles / Bulletins / Advisories
Systèmes

Déni de service OpenSSL

https://www.openssl.org/news/vulnerabilities.html#CVE-2021-2384

VMWare vSphere / CVE-2021- 21972 et CVE-2021-21973

- Touche 6.5, 6.7, 7.0 et Cloud Foundation 3.x et 4.x.
- Publication du “write-up” concernant ces vulnérabilités :
  - Contournement de l’authentification
  - Dépôt d’un JSP en archive ZIP spécialement construit
    - Dans un répertoire accessible sans authentification
    - Mauvaise vérification du contenu de l’archive (path traversal)
  - Consultation du JSP et exécution de code

https://swarm.ptsecurity.com/unauth-rce-vmware/

- Exploitation dans la nature...

Failles / Bulletins / Advisories
Réseau (principales failles)

Cisco

3 vulnérabilités critiques :

- Upload arbitraire dans Cisco NX-OS
- Contournement de la mire d'authentification dans Cisco ACI Multi Site Orchestrator
- Accès arbitraire dans le moteur Cisco Application Services

- Produits vulnérables
  - Cisco Aci multi-site orchestrator
  - Cisco Anyconnect secure mobility client
  - Cisco Application services engine
  - Cisco Identity services engine
  - Cisco IOS XR
  - Cisco Managed services accelerator
  - Cisco NX-OS
  - Cisco rv016 multi-wan vpn router firmware
  - Cisco rv160w wireless-ac vpn router firmware
  - Cisco Staros
  - Cisco Unified Computing System Central Software
  - Cisco Webex Meetings

Failles / Bulletins / Advisories
Réseau (principales failles)

Routeurs SOHO, une sécurité toujours catastrophique

- Beaucoup de CVE critiques
- Peu de durcissement à la compilation (NX, stack canaries...)
- Des identifiants de mots de passe codés en dur

https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HomeRouter/HomeRouterSecurity_2020_Bericht.pdf

Windows, 3 vulnérabilités sur la pile TCP/IP

- Encore sur de la fragmentation IP :
  - CVE-2021-24074, exécution de code à distance dans le traitement des paquets fragmentés en IPv4 (réseau local)
  - CVE-2021-24094, déni de service limité au réseau local et potentiellement une exécution de code (non confirmée pour l'instant)
  - CVE-2021-24086 **déni** de **service** encore et toujours avec des paquets fragmentés en IPv6 mais **routable**
- Correctifs dans le bulletin de février 2021

Failles / Bulletins / Advisories
Autre (principales failles)

***(exploit)* Manipulation de données via une vulnérabilité au sein de VMWare vCenter (CVE-2021-21972)**

- Téléversement de fichiers via l'endpoint /ui/vropspluginui/rest/services/uploadova

https://github.com/horizon3ai/CVE-2021-21972

***(exploit)* Élévation de privilèges et contournement de sécurité via une vulnérabilité au sein de Dell OpenManage Server Administrator**

- curl -ki -d 'manuallogin=true&targetmachine=**localhost**&user=AAAA&password=BBBB&application=omsa&ignorecertificate=1' 'https://<omsa_webserver>:1311/LoginServlet?flag=true&managedws=false'

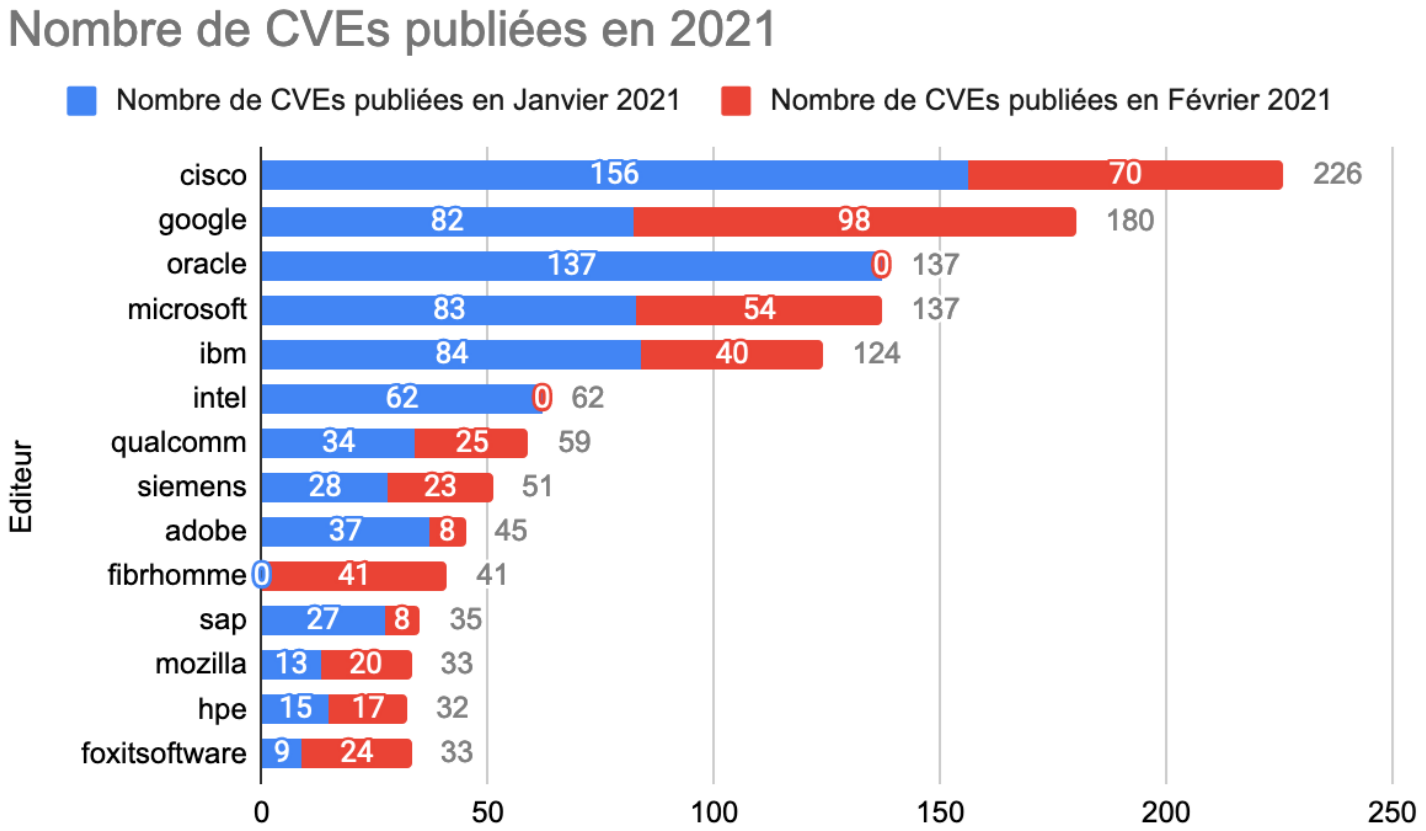
  https://fr.tenable.com/security/research/tra-2021-07

Prise de contrôle du système via une vulnérabilité au sein de SAP Solution Manager (CVE-2020-6207)

- Compromission des agents via l'envoi de fichiers XML spécifiquement conçus
- Possibilité d'exécuter du code, de récupérer des informations, voire d'ouvrir un invite distant

https://github.com/chipik/SAP_EEM_CVE-2020-6207

Stats du mois de février !



Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Vols de données médicales de 491 840 français dont 300 000 bretons

- Piratage “probable” de Dedalus aboutissant à une fuite folle :
  - Nom, conjoint, adresse, téléphone, date de naissance, pathologies, nom du médecin, groupe sanguin…
  - Dont les données de gens habilités

https://www.ouest-france.fr/bretagne/rennes-35000/piratage-informatique-les-donnees-medicales-de-300-000-bretons-en-pature-sur-le-dark-web-7166088

- Un salarié lanceur d’alerte avait tenté de signaler et faire corriger les très nombreuses problématiques de sécurité
  - Il a été “remercié” par un licenciement pour faute grave en 2020

https://www.nextinpact.com/article/43405/un-leader-europeen-donnees-sante-licencie-lanceur-dalerte-pour-faute-grave

- Communiqué de presse de Dedalus:

Dedalus
HEALTHCARE SYSTEMS GROUP

Communiqué de presse

Dedalus France a été mentionné dans des articles de presse relatant des fuites de données

Le Plessis Robinson, 24 février 2021- Dedalus France a été mentionné dans des articles de presse relatant des fuites de données.

Dedalus rappelle que la sécurité et la protection des données sont sa priorité.

Face à la gravité des sujets évoqués, Dedalus France est pleinement mobilisé et une enquête approfondie est en cours avec le support d’une équipe d’experts indépendants.

Les équipes de Dedalus sont aux côtés des laboratoires et de leurs patients dont les informations ont été divulguées.

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Hack de forums de Hackeurs

- Piratage et publication des informations des utilisateurs du forum Mazafaka
  - Mail, IP, ICQ…
- Plusieurs autres forums piratés : Verified, Crdclub
- Les administrateurs du site ont même publié leur plan d'action suite à la compromission

https://krebsonsecurity.com/2021/03/three-top-russian-cybercrime-forums-hacked/

https://www.shadowbanker.io/2021/03/hydra-admins-doxed-maybe-spotlighting-billions-minted-from-bath-salts-trade/

Le RIPE NCC victime de credential stuffing

- Visait son SSO
- L'attaque a été stoppée (ouf!)

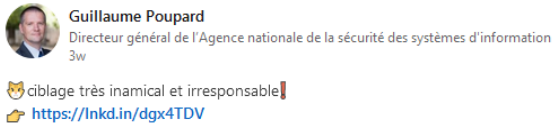
https://www.ripe.net/publications/news/announcements/attack-on-ripe-ncc-access

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Piratage d'entreprises en utilisant Centreon

- Solution de supervision comme Solarwinds Orion
- Compromission de:
  - Versions non à jour de Centreon
  - Exposées à internet
  - Ajout du webshell PHP : P.A.S.
- Analyse de l'ANSSI avec IOC et Yara

  https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-004/
- Guillaume Poupard a réagit:



- Finissons sur une touche d'humour :

  `<< En juillet 2007, le logiciel Oreon change de nom pour devenir Centreon en raison d'un conflit de nom avec Orion (logiciel de supervision édité par SolarWinds).>>`

  https://fr.wikipedia.org/wiki/Centreon la boucle est bouclée 😎

Piratages, Malwares, spam, fraudes et DDoS
Ransomwares

Qualys compromis par Cl0p

- Compromission réalisée via l'exploitation du logiciel FTA Accellion
- Logiciel...en fin de support dû aux problèmes de sécurité avérés
- La fuite a été retirée du site, Qualys a payé ?

https://www.lemagit.fr/actualites/252497205/Avec-Qualys-les-operateurs-de-Cl0p-continuent-daligner-les-victimes

https://www.accellion.com/sites/default/files/resources/fta-eol.pdf

L'Afnor subit une attaque du ransomware Ryuk

- Réponse avec philosophie

https://www.lemagit.fr/actualites/252496619/Cyberattaque-lAfnor-reconnait-etre-confrontee-au-ransomware-Ryuk

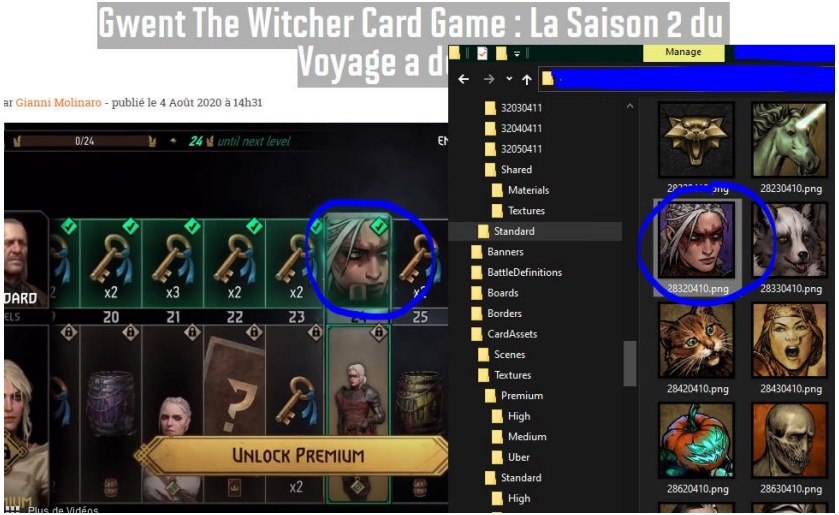
Mise à dispose d'un déchiffreur pour les victimes du ransomware Avaddon

- Publication de l'outil le 8 février
- Ransomware mis à jour le 12 😢

Piratages, Malwares, spam, fraudes et DDoS
Ransomwares

CD Projekt piraté

- Vol des codes sources de Cyberpunk 2077, The Witcher 3, Gwent…
- Chiffrement des données des serveurs compromis
  - Heureusement, ils avaient des sauvegardes
- https://twitter.com/xssfox/status/1359072804973334532/photo/1
- Publication du code source du jeu de carte Gwent

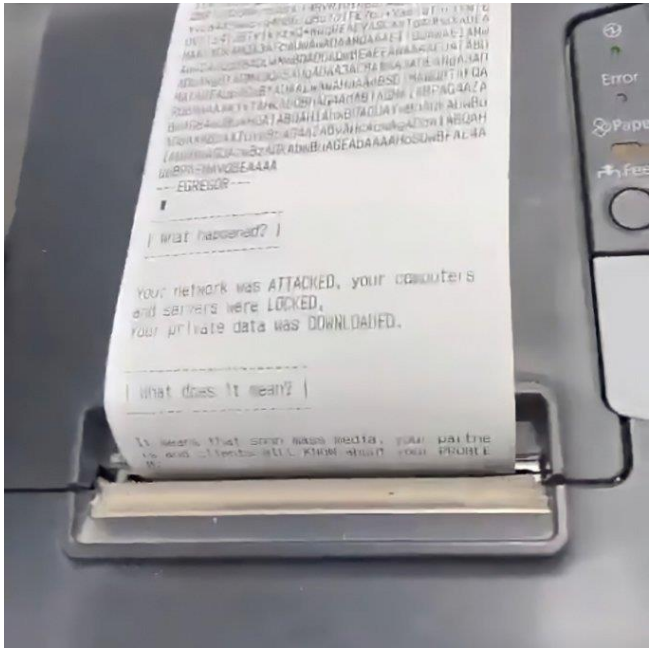


Piratages, Malwares, spam, fraudes et DDoS
Ransomwares

Interpellation d'opérateurs d'Egregor

- Opérateurs derrière le hack de Gefco/Ouest France/Ubisoft
- Site d' extortion DOWN
- Infrastructure C2 DOWN :)

https://www.franceinter.fr/justice/cybersecurite-des-pirates-egregor-a-l-origine-de-l-attaque-contre-ouest-france-interpelles-en-ukraine



Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

npm run for your lives

- Publication sur des dépôts publics des paquets portant le nom de paquets utilisés en interne
  - En particulier NodeJS
- Mauvaise gestion des dépendances allant chercher sur les dépôts publics
- Liste non exhaustive des entreprises vulnérables : Apple, Amazon, Yelp, Microsoft, Slack

  https://portswigger.net/daily-swig/researcher-hacks-apple-microsoft-and-other-major-tech-companies-in-novel-supply-chain-attack
  https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610
  https://dev.to/sumstrm/control-your-npm-packages-avoid-dependency-confusion-1cjh

Une entreprise russe rémunère les développeurs d'extensions de navigateur afin qu'ils installent des portes dérobées

- L'entreprise Infatica
- Le code injecté permet de transformer le navigateur en une sorte de proxy pour les clients de l'entreprise

  https://krebsonsecurity.com/2021/03/is-your-browser-extension-a-botnet-backdoor/

Piratages, Malwares, spam, fraudes et DDoS
Publications de l'ANSSI

L'ANSSI publie un référentiel pour les vérifications d'identité à distance

- Après PASSI, PDIS, PRIS, PACS voici venir PVID :)
- Ouverture prévue à partir de début avril
  https://www.ssi.gouv.fr/actualite/publication-du-referentiel-dexigences-applicables-aux-prestataires-de-verification-didentite-a-distance-pvid/

L'ANSSI publie "la cybersécurité pour les TPE / PME en 12 questions"

- Bon complément au "Guide relatif à la maturité SSI"
- Avant le guide d'hygiène essayez déjà d'être conforme à celui-là 😜
  https://www.ssi.gouv.fr/guide/la-cybersecurite-pour-les-tpepme-en-douze-questions/

L'ANSSI publie "son" Top 10 des vulnérabilités marquants de 2020

- Pulse, Citrix, Fortinet *(Lecture de n'importe quel fichier sans authentification)*, Microsoft DNS, ZeroLogon...
  https://www.cert.ssi.gouv.fr/actualite/CERTFR-2021-ACT-008/

- Forcément inspiré du "Top arbitraire de l'année écoulée 2020" de l'OSSIR ->

Piratages, Malwares, spam, fraudes et DDoS
Publication

Le CESIN publie son 6eme baromètre de la cybersécurité chez les grandes entreprises FR

- Enquête menée avec OpinionWay
- Constats pessimistes pour le moment

https://www.cesin.fr/document/view/4e0928de075538c593fbdabb0c5ef2c3

Vous aussi, mettez vous au Zero Trust avec la NSA

- Présentation du modèle
- Plutôt porté sur les concepts que l'implémentation technique

https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

Le Norwegian Intelligence Service publie son rapport des risques et met un accent sur les risques cyber

- Fake News
- Elections
- Vol de P.I.
- Attaques sur les infrastructures

https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus/rapporter/Focus2021-english.pdf/_/attachment/inline/450b1ed0-1983-4e6b-bc65-4aa7631aa36f:21c5241a06c489fa1608472c3c8ab855c0ac3511/Focus2021-english.pdf

Piratages, Malwares, spam, fraudes et DDoS
Crypto

L'authentification forte obligatoire pour les banques, c'est le 15 mai

- Pour les transactions en ligne de plus de 30 euros

https://www.banque-france.fr/sites/default/files/media/2021/02/19/210218_osmp-trajectoire-soft-decline.pdf

Besoin d'un code PIN pour payer ? Pour le reste il y a Mastercard

- Utilisation d'un faux AID
- Authentification faite via Google/Apple Pay

https://emvrace.github.io/

Immunity voit son cadriciel Canvas fuiter et divulgue… un exploit fonctionnel pour Spectre !

- Cadriciel retrouvé sur VirusTotal
- Permet de récupérer les hashs NT/LM sur Windows et le contenu de /etc/shadow sur Linux

https://www.bleepingcomputer.com/news/security/working-windows-and-linux-spectre-exploits-found-on-virustotal/

Publication du code d'exploitation de CVE-2020-1350

- Touchant Microsoft DNS
  https://github.com/chompie1337/SIGRed_RCE_PoC
- Toutes les explications ici :
  https://www.graplsecurity.com/post/anatomy-of-an-exploit-rce-with-cve-2020-1350-sigred

Business et Politique

Business
Monde

Okta rachète Auth0

- En espérant que la fusion se passe correctement

https://www.usine-digitale.fr/article/okta-s-empare-de-la-plateforme-d-authentification-auth0-pour-6-5-milliards-de-dollars.N1068134

Tenable rachète Alsid pour $98m

- Tenable, entreprise américaine fondée par un français

https://www.lesechos.fr/tech-medias/hightech/cybersecurite-le-rachat-dalsid-par-tenable-sous-loeil-de-bercy-1291452

Datadog rachète Sqreen pour un montant non communiqué

- Datadog, entreprise américaine fondée par un français

Droit / Politique
RGPD

La CNIL met en garde : L'utilisation de reconnaissance faciale pour détecter ceux qui ont une interdiction commerciale de stade

- Repose sur un traitement de données biométriques
- Interdit par le RGPD + la loi I&L

https://www.cnil.fr/fr/reconnaissance-faciale-et-interdiction-commerciale-de-stade-la-cnil-adresse-un-avertissement-un-club

Conférences

Conférences

Passée

- Pas grand chose...

A venir

- Le Hack
- SSTIC 2021 - en distanciel, du 2 au 4 juin 2021
- FIC 2021 - en distanciel ou présenciel, du 8 ou 10 juin 2021

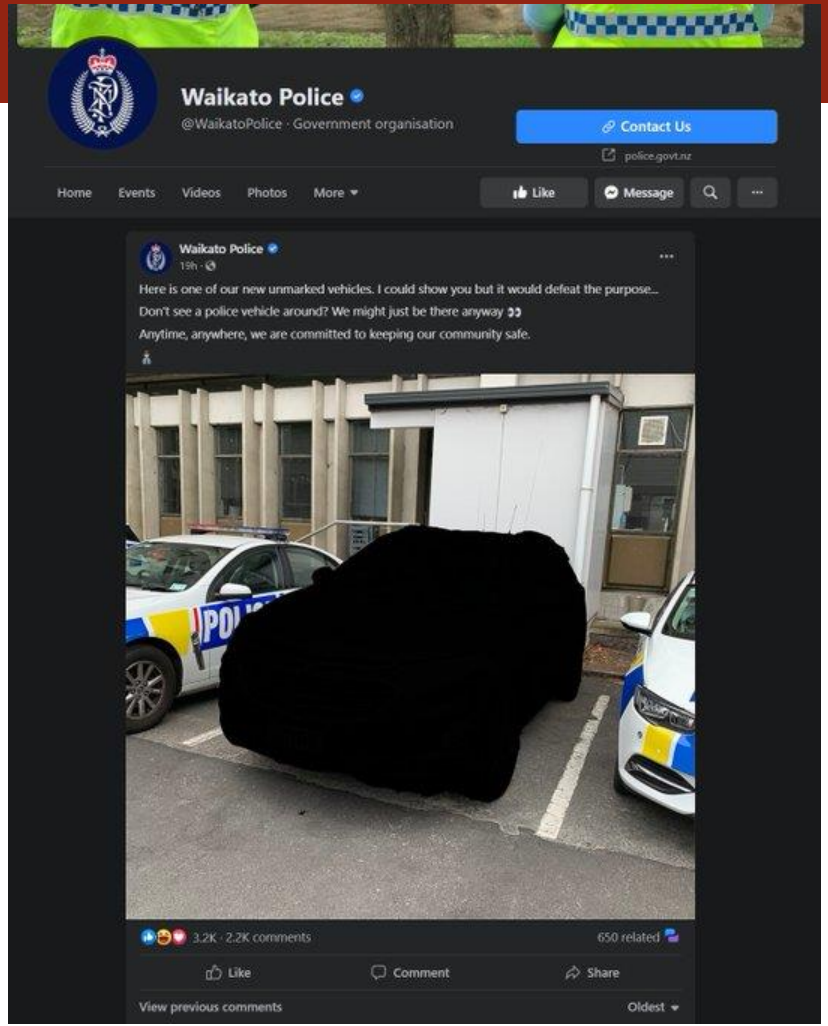
Divers / Trolls velus

Divers / Trolls velus

Quand tu veux montrer tes muscles

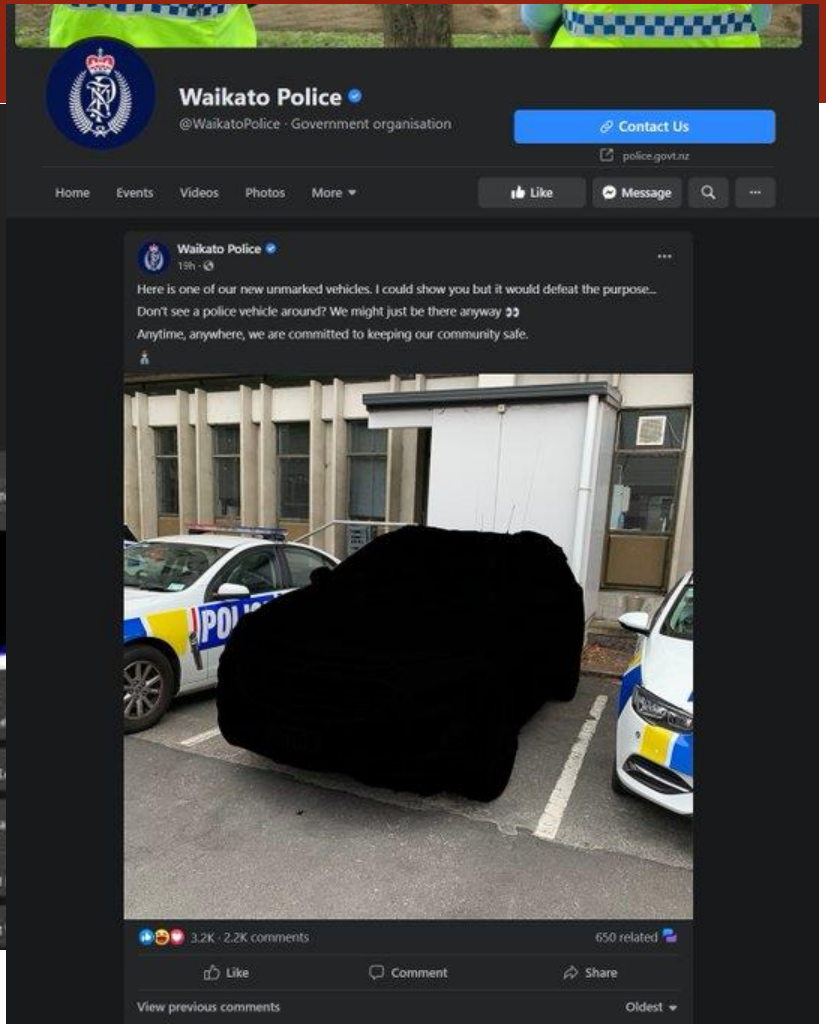
- Mais que tu ne sais pas utiliser Photoshop

https://twitter.com/alexbloor/status/1359515437093031936?s=09

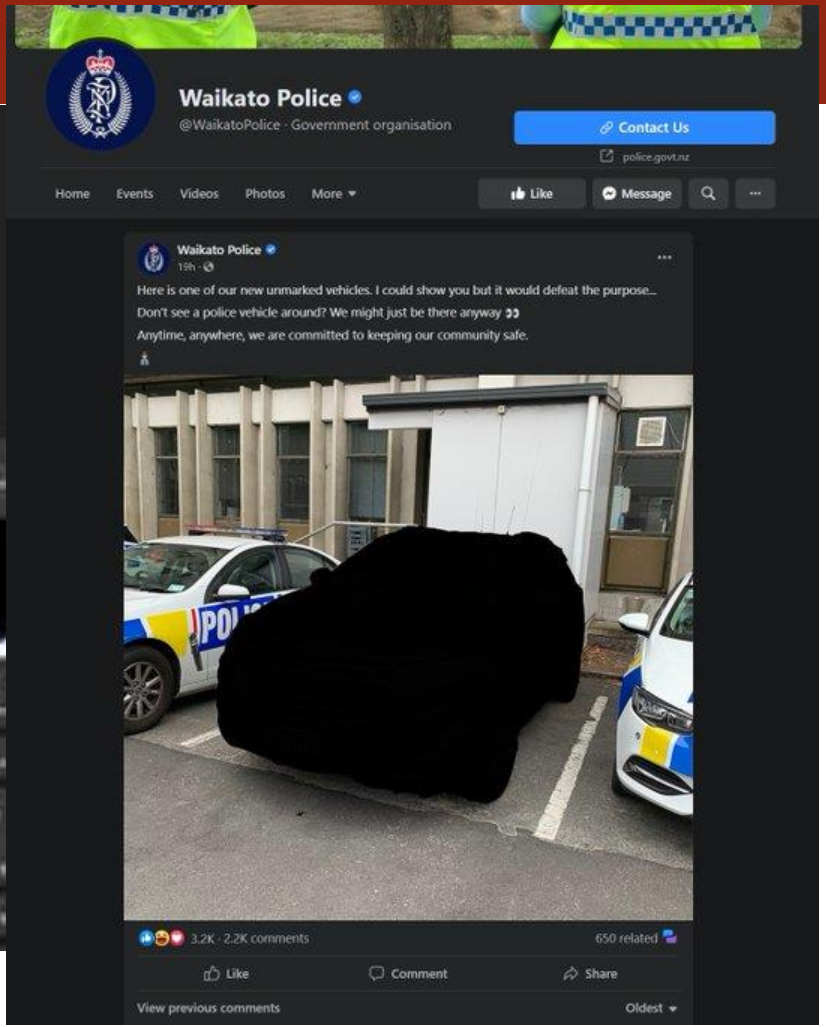


La suite au slide suivant...

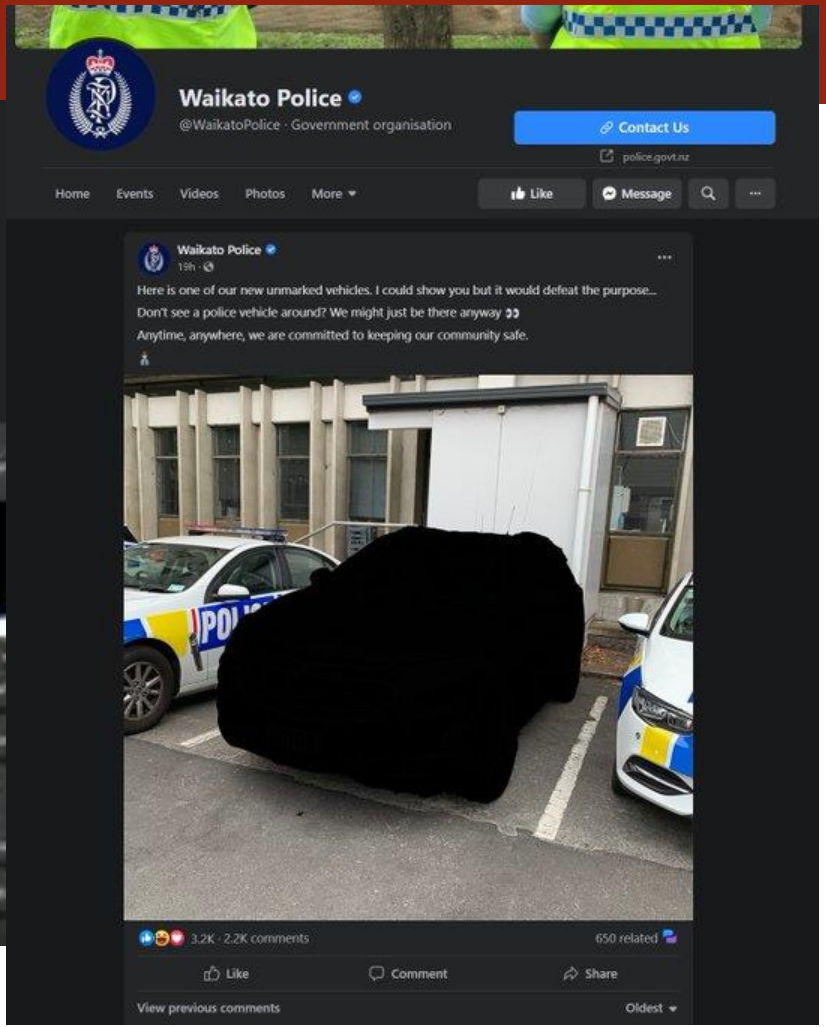
Divers / Trolls velus



Divers / Trolls velus



Divers / Trolls velus

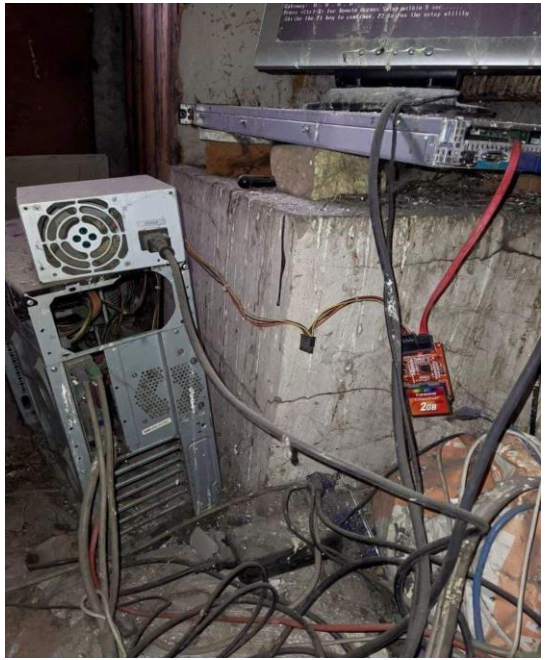


Divers / Trolls velus

Quand on critique ton local technique ou ta salle d’hébergement

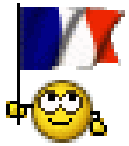
- Il y’a pire ailleurs, bien pire

  https://twitter.com/Sun_Ultra10/status/1365219185140391937



Divers / Trolls velus

L’ANSSI cité dans Wired



- Au sujet de l’attaque sur Centreon

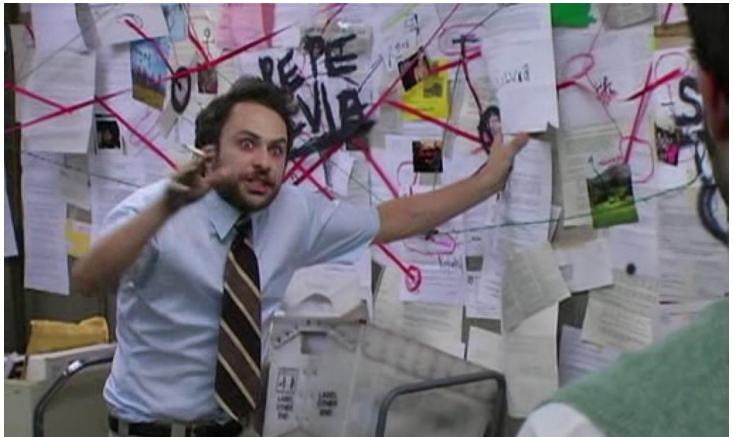
  https://www.wired.com/story/sandworm-centreon-russia-hack/

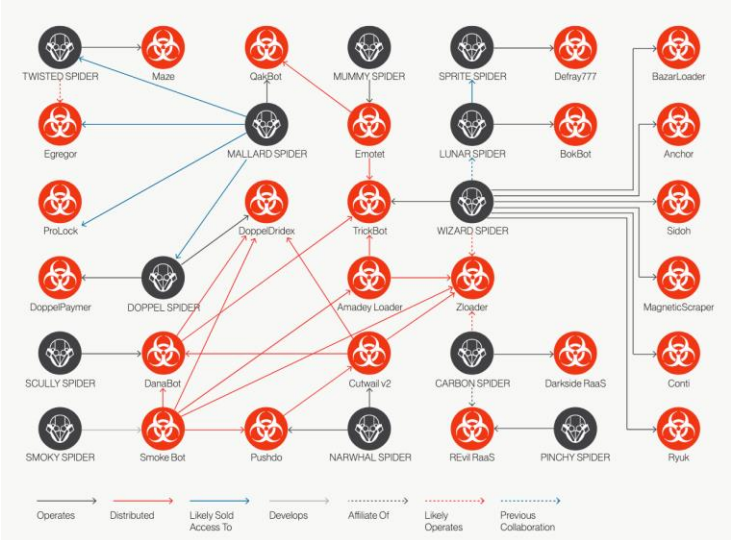
Crowdstrike introduit son nouvel eCrime Index

- Ainsi qu'une cartographie des liens entre attaquants et malwares

  https://adversary.crowdstrike.com/

  https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf





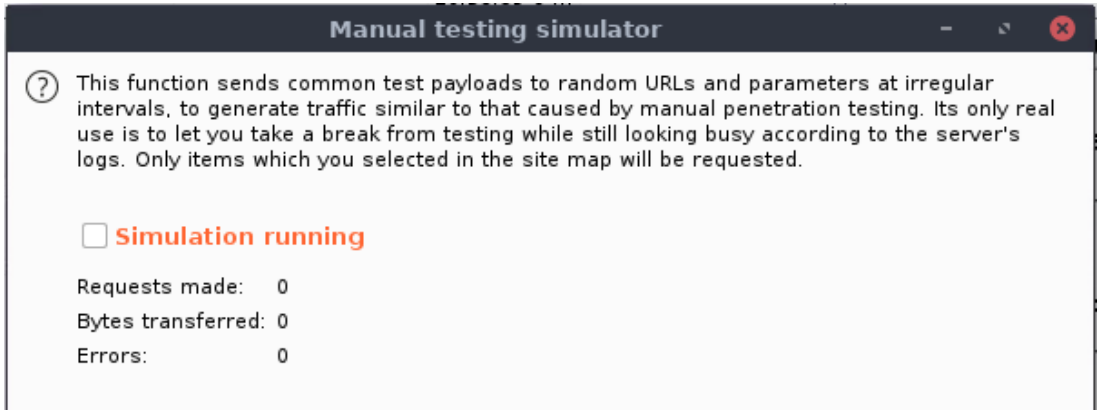
Divers / Trolls velus
Solarwinds

Microsoft - "Combien faut-il d'ingénieurs pour réaliser une attaque sur la supply Chain ?"

https://www.infosecurity-magazine.com/news/microsoft-1000-hackers-worked/

“LA” fonctionnalité qu’il manquait à Burp Suite

https://twitter.com/Daviey/status/1368164355611693056/photo/1



Divers / Trolls velus

Fail : NoLimitSécu publie l'épisode du 1er avril… le 1er mars

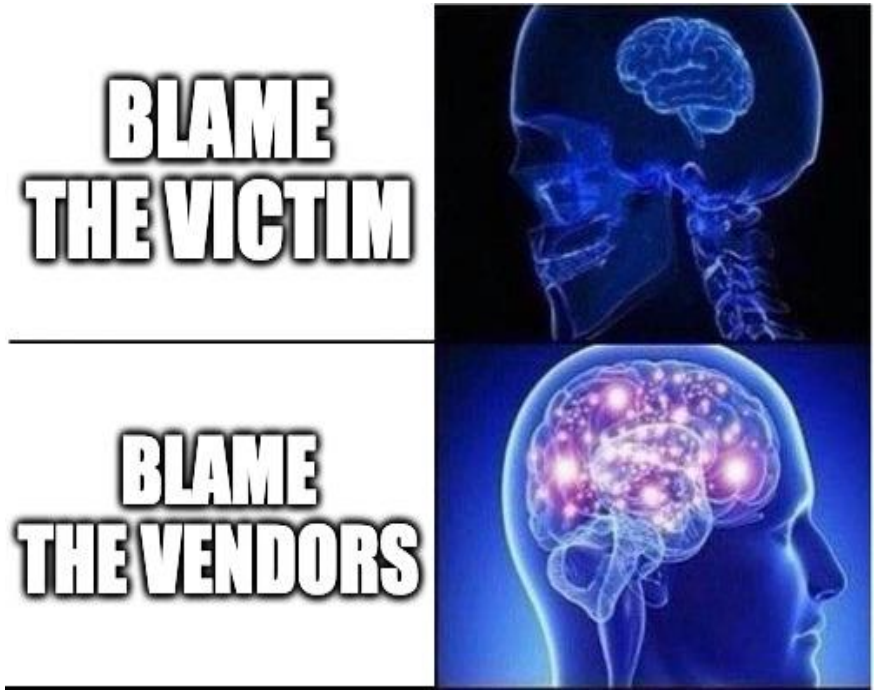
- Serait-ce un coup du stagiaire ?
  https://twitter.com/nolimitsecu/status/1366403415576875013

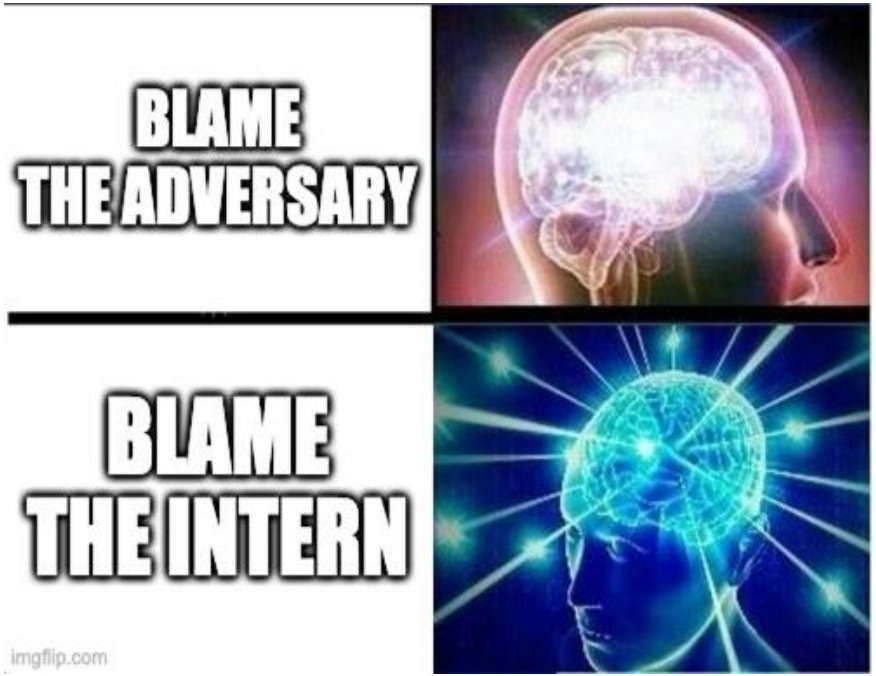
En mode "Tracking Protection: Strict", Firefox remplace les trackers…

- Par un Javascript qui redéfinie les principales fonctions à vide
- Google Analytics, Facebook SDK, Live, Eluminate...
  https://bugzilla.mozilla.org/show_bug.cgi?id=1493602
  https://github.com/mozilla/gecko-dev/tree/master/browser/extensions/webcompat/shims

Divers / Trolls velus
Solarwinds

SolarWinds - "C'est pas notre faute, c'est le stagiaire !"





Divers / Trolls velus
Solarwinds

SolarWinds - "C'est pas notre faute, c'est le stagiaire !"

- Comment ne **pas** communiquer
- Et si c'est vraiment le stagiaire qui a mis un mot de passe faible …
  - Pourquoi le stagiaire peut créer un serveur sans supervision ?
  - Pourquoi les managers n'ont-ils pas vérifiés le travail effectué ?
  - Pourquoi n'y-a-t-il pas de politique de mot de passe fort sur ce serveur sensible ?

- Katie Porter `<<I've got a stronger password than 'solarwinds123' to stop my kids from watching too much YouTube on their iPad>>`
  https://edition.cnn.com/2021/02/26/politics/solarwinds123-password-intern/index.html

- Nouvelles cibles identifiées
  - La NASA et la FAA

https://www.wired.com/story/solarwinds-nasa-faa-robot-dog-fight-security-news/

Prochains rendez-vous de l’OSSIR

Prochaines réunions

Prochaine réunion

- 13 Avril 2021… toujours en visio

After Work

- Pas avant Q3 2021 ?

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?