Revue d'actualité de l'OSSIR

13 avril 2021

Aurélien Denis
*Vladimir Kolla @mynameisv_*

Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

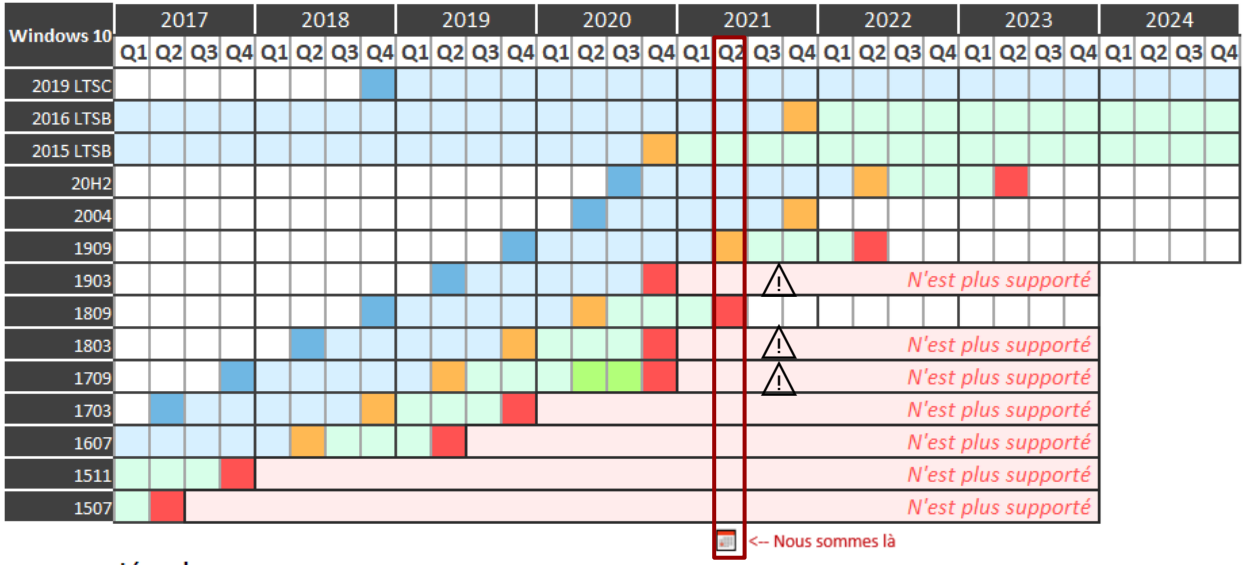
Report des fins de support de produits Microsoft suite au Covid-19

- 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 mars :

- 89 vulnérabilités corrigées, dont 10 critiques

- A retenir :
  - CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 et CVE-2021-27065 : **En cours d'exploitation** (Exchange)

Composants impactés

Windows Server (2004) ;
Windows Server (1909) ;
Windows Server (20H2) ;
Windows Server 2008 ;
Windows Server 2012 ;
Windows Server 2016 ;
Windows Server 2019 ;
Windows 10 ;
Windows 7 ;
Windows 8.1 ;
Sharepoint ;
Microsoft 365 Apps ;
Microsoft Azure ;
Microsoft Office (Word, Excel, PowerP
Microsoft Edge ;
Microsoft Internet Explorer ;
Visual Studio ;
Windows Admin Center ;
Microsoft Visio.

Failles / Bulletins / Advisories
Microsoft - ProxyLogon (update)

Manipulation de données via une vulnérabilité au sein d'Exchange

- Drop de fichier arbitraire

  https://f5.pm/go-62102.html

(exploit) Divulgation d'informations via une vulnérabilité au sein d'Exchange (CVE-2021-26855)

- Récupération d'une boîte mail

  https://gitlab.com/gvillegas/ohwaa/

Certains PoCs publiés sur GitHub mais takedown aussitôt

- Responsible disclosure ?
- L'effet Streisand

  https://www.vice.com/en/article/n7vpaz/researcher-publishes-code-to-exploit-microsoft-exchange-vulnerabilities-on-github

Pwn2Own : Nouveau variant de ProxyLogon ?

- Pas encore de leak public

  https://twitter.com/orange_8361/status/1379479323908792342

Failles / Bulletins / Advisories
Microsoft - Avis

(exploit) Déni de service IPv6 **routable** sur Windows (CVE-2021-24806)

- Déréférencement de pointeur NULL via la couche IPv6 (*tcpip.sys*)

  https://github.com/0vercl0k/CVE-2021-24086

(exploit) Élévation de privilèges via une vulnérabilité au sein de Windows (CVE-2021-1732)

- win32k

  https://github.com/rapid7/metasploit-framework/commit/2c1869f9df4e7bd0f4efbaab76a4471d0ae23f62

Failles / Bulletins / Advisories
Navigateurs (principales failles)

Google Chrome, 8 vulnérabilités au sein de UaF dans screen capture

- Prises de contrôle du système
- Divulgation d'informations

https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop_30.html

Microsoft Edge, 33 vulnérabilités

- Prises de contrôle du système
  - Venant du moteur Chromium

https://github.com/chompie1337/SIGRed_RCE_PoC

Firefox et Firefox ESR, 8 vulnérabilités (mfsa2021-10/mfsa2021-11)

- Prise sde contrôle du système
- Contournement de sécurité
- Lecture hors-champs dans WebGL

https://www.mozilla.org/en-US/security/advisories/mfsa2021-10/

https://www.mozilla.org/en-US/security/advisories/mfsa2021-11/

Failles / Bulletins / Advisories
Navigateurs (principales failles)

(exploit) Google Chrome, Implémentation de Spectre en Javascript

- Permettant une fuite d’information

  https://security.googleblog.com/2021/03/a-spectre-proof-of-concept-for-spectre.html

  https://leaky.page/

(exploit) Google Chrome, Divulgation d'informations

- ~~0~~ 1-Day
- Heureusement la sandbox protège.

  https://github.com/r4j0x00/exploits/tree/master/chrome-0day

Failles / Bulletins / Advisories
Systèmes

(exploit) **Exploit VMWare vSphere dans Metasploit** (CVE-2021-21972, cf. revue de mars 2021)

- Execution de commande à distance, sans authentification
- Envoie un .tar et le décompresse sur le serveur

https://github.com/rapid7/metasploit-framework/commit/2562a261e29e9981404f4ca9e604b99a86675291

Failles / Bulletins / Advisories
Systèmes

*(expl*oit) BleedingTooth, Prise de contrôle à distance sans authentification sur Linux

- Chaîne de 3 vulnérabilités
- BadVibes (CVE-2020-24490), DoS par dépassement de mémoire dans le tas (heap)
  https://github.com/google/security-research/security/advisories/GHSA-ccx2-w2r4-x649
- BadChoice (CVE-2020-12352), contourner de KASLR par une fuite de mémoire
  https://github.com/google/security-research/security/advisories/GHSA-7mh3-gq28-gfrq
- BadKarma (CVE-2020-12351), confusion de type permettant d'exécuter du code
  ttps://github.com/google/security-research/security/advisories/GHSA-h637-c88j-47wq
- Tous les détails :
  https://github.com/google/security-research/blob/master/pocs/linux/bleedingtooth/writeup.md
- Exploit :
  https://www.exploit-db.com/exploits/49754

Failles / Bulletins / Advisories
Réseau (principales failles)

Cisco

85 bulletins, dont **6 critiques**

- RCE dans Cisco SD-Wan
- Contournement de la mire d'authentification dans Cisco ACI Multi Site Orchestrator
- RCE sur Jabber via XMPP

- Produits vulnérables
  - Cisco Access Point Software
  - Cisco Advanced Malware Protection for Endpoints Windows Connector, ClamAV for Windows, and Immunet
  - Cisco Aironet Access Points
  - Cisco IOS and IOS XE Software
  - Cisco IOS XE ROM Monitor Software for Cisco Industrial Switches OS
  - Cisco IOS XE SD-WAN Software
  - Cisco IOS XE SD-WAN Software vDaemon
  - Cisco IOS XE Software
  - Cisco IOS XE Wireless Controller Software for the Catalyst 9000 Family CAPWAP
  - Cisco IOS XR Software
  - Cisco IOx Application Environment Path Traversal Vulnerability
  - Cisco IOx Application Framework
  - Cisco IOx for IOS XE Software
  - Cisco Jabber Desktop and Mobile Client
  - Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers
  - Cisco SD-WAN vManage
  - Cisco Small Business RV Series Routers
  - Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers Management Interface
  - Cisco Small Business RV132W and RV134W Routers Management Interface
  - Cisco Umbrella Link
  - Cisco Unified Communications Manager

Failles / Bulletins / Advisories
Réseau (principales failles)

Prise de contrôle du système et manipulation de données via 21 vulnérabilités au sein de F5

- 4 critiques
  - 2x injections de commande à distance sans authentification CVE-2021-22986 et CVE-2021-22987
    - Exploits :

      https://twitter.com/1ZRR4H/status/1373206181955653632

      https://twitter.com/dcuthbert/status/1374066969289297923
  - Exécution de code à distance par buffer overflow sur une URI CVE-2021-22991
  - Exécution de code à distance par buffer overflow dans ASM sur une réponse HTTP CVE-2021-22992

https://support.f5.com/csp/article/K02566623

Divulgation d'informations via 2 vulnérabilités au sein de Fortinet (FG-IR-19-244 / FG-IR-20-076)

- Le mot de passe était stocké en clair dans les logs. (FortiADC)
- Mot de passe stocké en clair dans l'applicatif de scan (FortiWeb)

Failles / Bulletins / Advisories
Autre (principales failles)

Prise de contrôle du système et élévation de privilèges via 17 vulnérabilités au sein de multiples produits SAP (2021-Mar)

- Injection de code, contournement d'authentification, ...

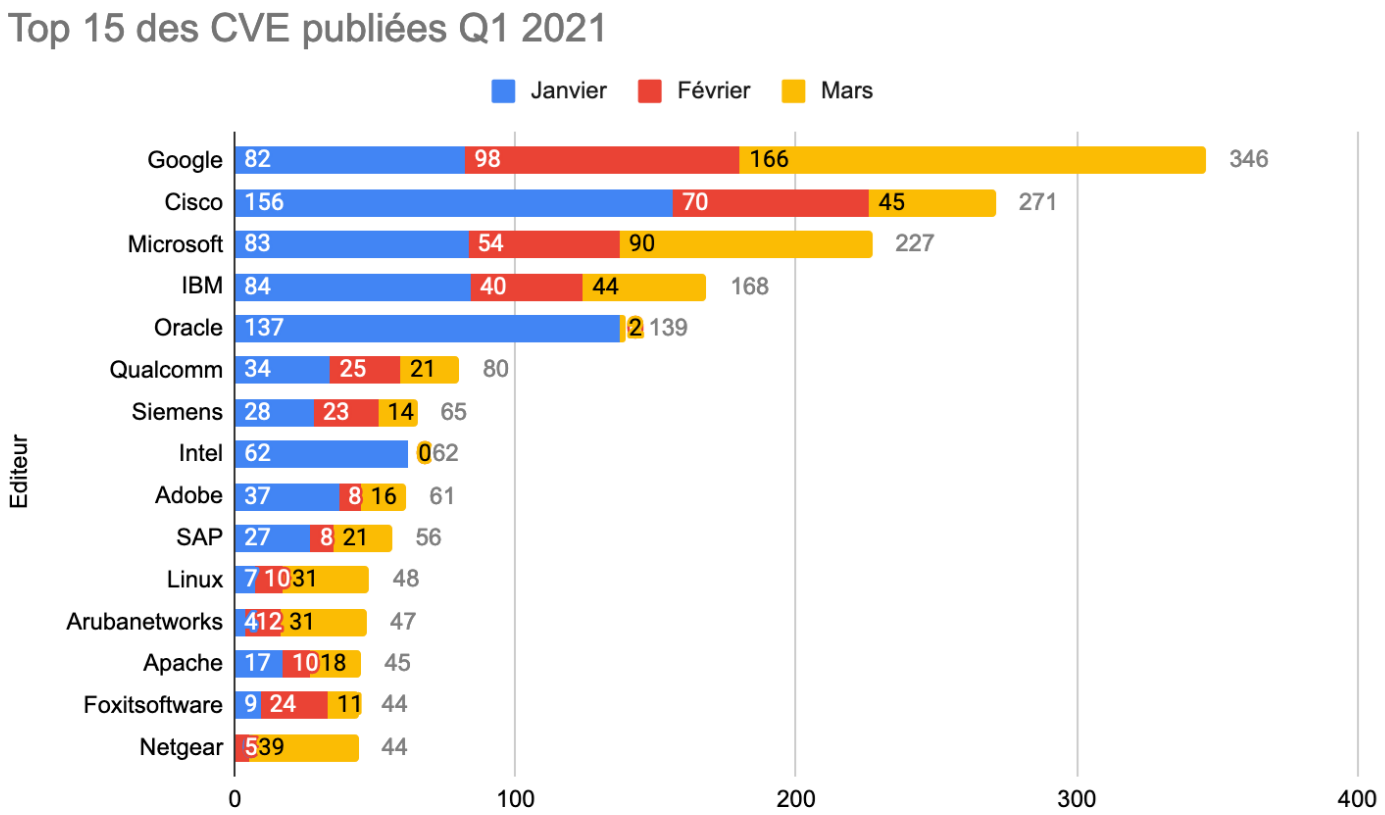
  https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=571343107

Divulgation d'informations via une vulnérabilité au sein d'OpenManage Server Administrator (DSA-2020-172)

- Requêtes vers les endpoints LoginServlet et DownloadServlet

  https://www.exploit-db.com/exploits/49750

Stats du mois



Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Facebook, publication de 533 millions de comptes

- Nom, prénom, FB_ID, tel, mail (parfois)...
- Scrapping comme pour Whatsapp
- Réponse de Facebook :

> <<Facebook says it did not notify users about the 2019 contact importer exploitation precisely because there are so many troves of semipublic user data—taken from Facebook itself and other companies—out in the world.>>

https://www.wired.com/story/facebook-data-leak-500-million-users-phone-numbers/

  - Revient à dire : Mais nous partageons tellement vos données et des fuites ça arrive tellement souvent vous savez...

```
[redacted]acebook 533m [2019]/france$ grep -nia 'nicolas.*sarkozy.*1955' francia.csv
11982983:3367[redacted]38,100003032333114,,Nicolas,Sarkozy,male,2011-10-12,01/28/1955,,,,,,1,0,2016-05-13,2018-07-23 07
[redacted]Facebook 533m [2019]/france$ grep -nia 'nicolas.*ruff.*google' francia.csv
262283:3360[redacted]25,545464602,,Nicolas,Ruff,male,2010-09-27,,,,,,Google,1,1,2008-11-28,2018-07-19 17:59:19
```

```
[redacted]acebook 533m [2019]/france$ grep -i 'hervé.*schauer' francia.csv
362[redacted]5,1053624551,,Hervé,Schauer,male,2010-09-11,[redacted]196[redacted],"b'Neuilly-sur-Seine, France'",[redacted],[redacted],HS2,1,1
3[redacted]4,68[redacted]08,,Q[redacted],male,2010-09-17,,"b'Paris, France'",b'[redacted]',,,Hervé Schauer Consultants - HSC (www.
```

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Linkedin, publication de 1 Milliards de comptes

- Cumul de plusieurs fuites de dizaines et centaines de millions de comptes
  https://raidforums.com/Thread-SELLING-LinkedIn-1Billion-1000Million-Record

LinkedIn	File folder	
1(167 340 940).sql--ID+Email.txt	Text Document	11,056,343 KB
1.sql.xlsx	Microsoft Excel W...	7 KB
1.xlsx	Microsoft Excel W...	7 KB
2.5M US B2B Linkedin.zip	WinRAR ZIP archive	668,138 KB
25M-Linkedin.zip	WinRAR ZIP archive	4,283,641 KB
35M LINKEDIN CONTACT (WITH COMPA...	WinRAR ZIP archive	14,573,915 KB
Australia Linkedin 194K.zip	WinRAR ZIP archive	14,999 KB
Linkedin - 250 758 057.txt	Text Document	11,091,160 KB
Linkedin - 250 758 057.zip	WinRAR ZIP archive	5,657,484 KB
Linkedin 34 Million Linkedin Emails.zip	WinRAR ZIP archive	63,690 KB
linkedin 37 million db-16M.zip	WinRAR ZIP archive	3,139,894 KB
Linkedin 45k With Full Details.zip	WinRAR ZIP archive	13,340 KB
linkedin db 35M.zip	WinRAR ZIP archive	6,927,944 KB
Linkedin DB with Profile URLS 21M.zip	WinRAR ZIP archive	6,708,053 KB
Linkedin Dehased 1GB.zip	WinRAR ZIP archive	1,051,722 KB
Linkedin Pakistan.zip	WinRAR ZIP archive	1,493 KB
Linkedin sorted by Titles.zip	WinRAR ZIP archive	67,602 KB
LinkedIn.rar	WinRAR archive	7,327,315 KB
Linkedin2.zip	WinRAR ZIP archive	404,272 KB
Linkedin-Company-Education_FR.zip	WinRAR ZIP archive	2,338 KB
LinkedInMain 16M.zip	WinRAR ZIP archive	2,367,669 KB

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Ubiquiti

- "We became aware of unauthorized access to certain of our information technology systems hosted by a third party cloud provider"
- Backdoor trouvée + leak du code source (+ demande de rançon et deuxième backdoor)

https://krebsonsecurity.com/2021/03/whistleblower-ubiquiti-breach-catastrophic/

Pwn de PHP

- Compromission de git.php.net
  → Migration vers GitHub

https://therecord.media/hackers-backdoor-php-source-code-after-internal-repo-hack/

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Campagnes d'attaques sur les applicatifs Fortinet et SAP

- CVE-2018-13379, CVE-2020-12812, CVE-2019-5591 (Fortinet)
- SAP - Temps entre patch et exploit : 72h

https://www.ic3.gov/Media/News/2021/210402.pdf

https://us-cert.cisa.gov/ncas/current-activity/2021/04/06/malicious-cyber-activity-targeting-critical-sap-applications

https://onapsis.com/active-cyberattacks-mission-critical-sap-applications#threat-report

Description du groupe SilverFish

- Groupe APT lié à la campagne contre SolarWinds et le groupe EvilCorp (aka TA505)
- Durcissement du C2 / Domain Fronting / Cobalt *(sic)*

https://www.prodaft.com/m/uploads/SilverFish_TLPWHITE.pdf

Comment faire en sorte qu'un utilisateur installe un malware ? Le guider via téléphone.

- BazarLoader + CallCenters = BazarCall

https://therecord.media/malware-uses-underground-call-centers-to-trick-users-into-infecting-themselves/

Piratages, Malwares, spam, fraudes et DDoS
Ransomwares

Acer pwn par REvil

- 50M$

  https://therecord.media/ransomware-gang-demands-50-million-from-computer-maker-acer/

Interview de REvil : "On s'en prend aux assurances pour trouver de nouvelles cibles"

- Objectif : L'argent, l'argent, l'argent

  https://therecord.media/i-scrounged-through-the-trash-heaps-now-im-a-millionaire-an-interview-with-revils-unknown/

Compromission de l'assurance CNA

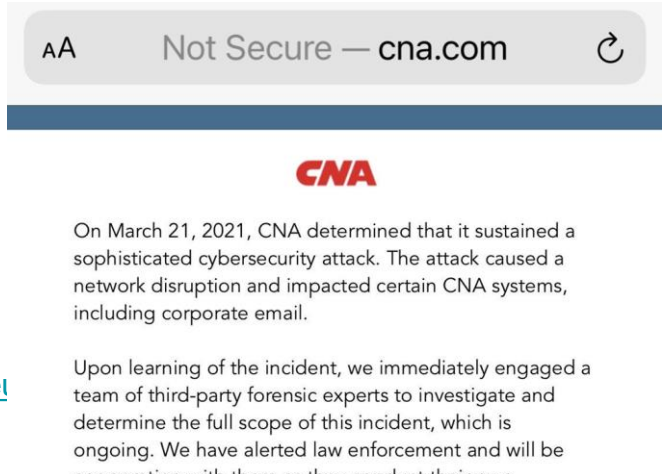
- ...Par REvil 'v'

  https://twitter.com/ryanaraine/status/1374842477169975301

Pierre Fabre compromis

- ...Par REvil aussi.

  https://www.lemondeinformatique.fr/actualites/lire-pierre-fabre-revil-a-la-manoeu



Piratages, Malwares, spam, fraudes et DDoS
Ransomwares

Attaque sur la ville de Douai

- Rançongiciel ayant des impacts sur plusieurs services
- Témoignage du Maire sur Youtube

  https://www.youtube.com/watch?v=F-9En2KSKAg

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Utiliser l'infra de GitHub pour miner des cryptomonnaies

- Abus des "*GitHub Actions*"
- Possibilité d'exécuter du code sur l'infra de GitHub via une PR

https://therecord.media/github-investigating-crypto-mining-campaign-abusing-its-server-infrastructure/

Leak info sur MacOSX via...l'éditeur de texte :O

- Erreur dans textedit qui peut lire un fichier TXT comme un fichier RTF-HTML
- Possibilité de forcer le mac à faire une requête via

```
<html><head></head><body><style>@import{ "file:///net/MYSERVER.COM/a.css"} </style>
```

https://www.paulosyibelo.com/2021/04/this-man-thought-opening-txt-file-is.html

Ukcybersecurity.org.uk : Réserver le ndd avant de le communiquer

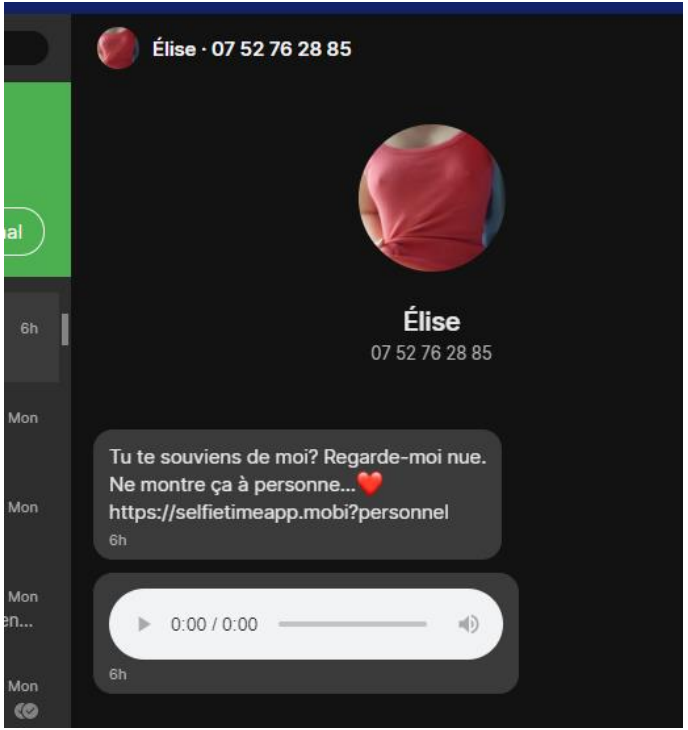
- Communiqué de presse réalisé légèrement trop vite..

https://www.revk.uk/2021/04/uk-cyber-security-council.html

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Chloé, Elise, Nathalie… Brigitte

- Messages indésirables sur Signal
  - Depuis des numéros Lyca Mobile
- Le but est de récupérer votre mail
- Objectif : sexting, camgirls et porno
  https://cyberguerre.numerama.com/11720-tu-te-souviens-de-moi-ce-spam-porno-sur-signal-dirige-vers-un-site-de-sexting-onereux.html

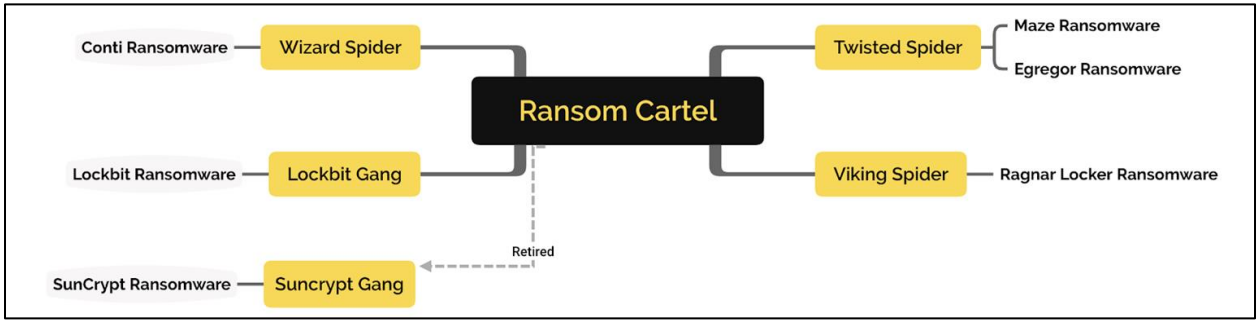


Piratages, Malwares, spam, fraudes et DDoS
Publication

Découpage du "Cartel MAZE"

- Pas vraiment un cartel...
- ...mais un certain partage de connaissances entre les acteurs

https://analyst1.com/blog/ransom-mafia-analysis-of-the-worlds-first-ransomware-cartel



3 agences de sécurité / 75 leak des infos en oubliant de retirer des informations des PDFs

- 3 fichiers sur 4 contiennent des informations sur le créateur du document
- L'ANSSI fait partie des bons élèves 💯

https://therecord.media/security-agencies-leak-sensitive-data-by-failing-to-sanitize-pdf-files

DFIR/OSINT
Techniques & outils

Gérez vos règles Yara en CLI

- Pip install yaramanager

https://github.com/3c7/yaramanager

Surveillez en continu des flux OSINT avec mihari

- Possibilité d'alerting sur plusieurs canaux
- Une interface web

https://github.com/ninoseki/mihari

Simulateur de ransomware pour tester vos EDR

- Possibilité d'émuler des TTPs liés aux ransomware (persistence, évasion, impact..)

https://blog.fraktal.fi/emulating-ransomware-behavior-in-purple-teaming-a3d48095d036?gi=ff36e4d95422

Simulateur d'attaque Microsoft (I.A.)

- Concept d'environnement vulnérable représenté sous la forme de graphe

https://github.com/microsoft/CyberBattleSim

Disponibilité

Incendie chez OVH

- Datacenter SBG2 à Strasbourg en feu à cause d'un onduleur

  https://twitter.com/olesovhcom/status/1369478732247932929?s=19

- Beaucoup de clients "IaaS" se plaignent de ne pas avoir de backup inclus par OVH…
  - sur du IaaS… 🤦‍♂️
  - Et comparent à du SaaS AWS 🤦‍♂️🤦‍♂️🤦‍♂️
  - Revient à dire ----------> <<Quoi!!? Il faut le permis pour conduire une voiture !!? Pourtant je prends Uber tous les jours et je n'ai jamais eu besoin de permis>>

Business et Politique

Business
Monde

ThreatQuotient lève $22 millions

- Pour continuer après leurs bonnes performances de 2020

https://www.helpnetsecurity.com/2021/04/07/threatquotient-funding/

Glimps lève 6 millions €

- Présentation à l'ossir en sept. 2020

https://www.linkedin.com/posts/acemanagement_glimps-activity-6787600387173052416-jh6e/

Bercy valide le rachat de Sqreen par Datadog

https://www.linkedin.com/posts/activity-6787637088683638784-8gpx

Droit / Politique
France / Europe

GAIA-X le Cloud Européen

- 100% Européen de souveraineté souveraine :
  - Palantir
  - Huawei
  - Alicloud
  - Palo alto networks
  - Salesforce
  - Snowflake
  - AWS
  - Emergency Reporting
  - Google
  - Haier COSMO
  - Intel
  - Oracle

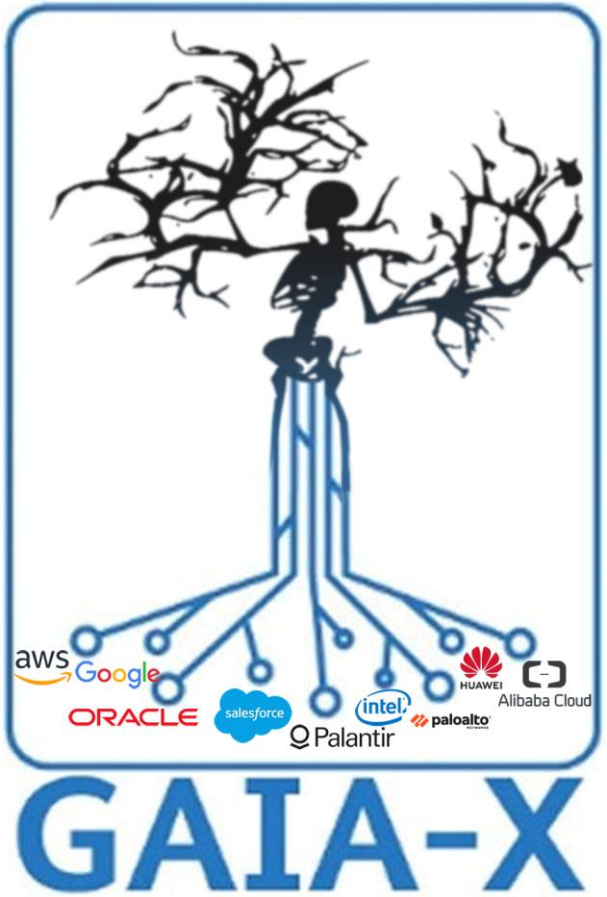
https://twitter.com/MaliciaRogue/status/1377653464570941441

Droit / Politique
France / Europe

GAIA-X le Cloud Européen

- 100% Européen de souveraineté souveraine :
  - Palantir
  - Huawei
  - Alicloud
  - Palo alto networks
  - Salesforce
  - Snowflake
  - AWS
  - Emergency Reporting
  - Google
  - Haier COSMO
  - Intel
  - Oracle

https://twitter.com/MaliciaRogue/status/1377653464570941441



Droit / Politique
France / Europe

Webedia fait payer la désactivation des cookies de tracking

- Acceptez les cookies ou payez 2€ ! (c'est un peu flou juridiquement…)

  https://www.numerama.com/tech/701279-payer-pour-eviter-les-cookies-publicitaires-est-ce-legal.html

Un jeu sur le refus des cookies :)

- Arriverez-vous à n'accepter que les cookies nécessaires ?

  https://cookieconsentspeed.run/

Droit / Politique
Monde

Google vs Microsoft

- `<<lobbying for regulations that benefit their own interests.>>`
  - venant de la part de Google cela en est presque risible
- `<< break the way the open web works in an effort to undercut a rival>>` 🤣
  - Ce n'est pas comme si Google fait tout pour imposer ses propres standards...

https://blog.google/products/news/google-commitment-supporting-journalism/amp/

La personne qui a tenté de faire introduire un malware chez Tesla a été jugé

- Cf. revue d'actualité de Septembre 2020 :)

https://www.justice.gov/opa/pr/russian-national-pleads-guilty-conspiracy-introduce-malware-us-company-s-computer-network

Conférences

Conférences

Passée

- FIC virtuel “béta” – 7 avril 2021

A venir

- Le Hack – annulé
- SSTIC 2021 “en distanciel” - du 2 au 4 juin 2021
- SSTIC 2022 au Château de Versailles (😷😉) ----------> Reverse Shell
  https://www.sstic.org/2021/news/sstic_2021_2022/

- FIC Virtuel – du 1er au 4 juin 2021
- FIC “présenciel” 2021… c’est compliqué :
  - ~~Du 19 au 21 janvier 2021~~
  - ~~Décalé, du 6 au 8 avril 2021~~
  - ~~Décalé, du 8 au 10 juin 2021~~
  - Décalé, du 7 au 9 septembre 2021

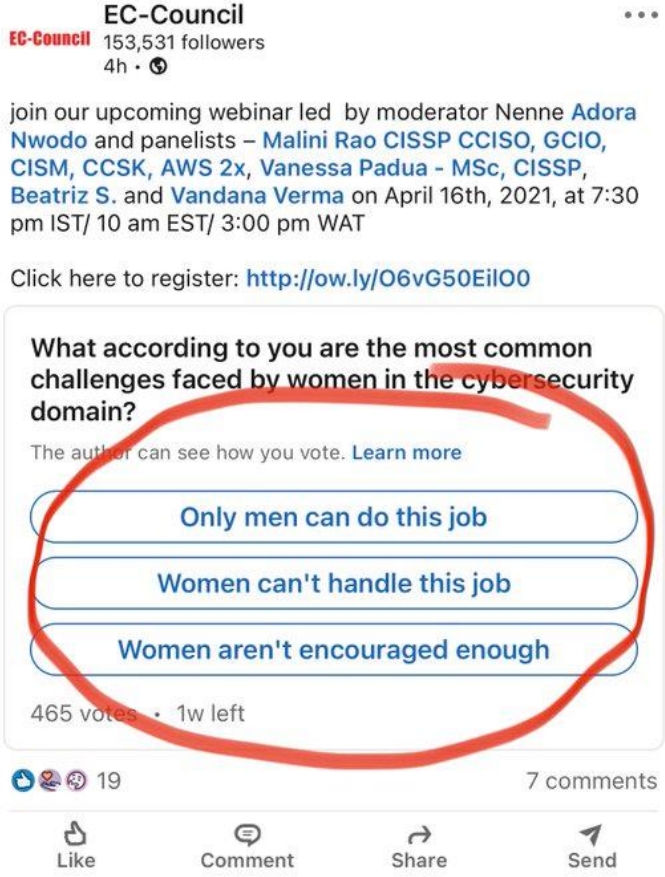
Divers / Trolls velus

Divers / Trolls velus

Le sexisme dans la Cybersécurité avec EC-Council

- EC-Council = Organisme américain de certification
- Sondage critiqué sur Twitter
  - Les critiques ont été bloqués par le CM d'EC-Council
  - Mauvaise publicité, nécessitant une réponse du CEO

https://www.linkedin.com/posts/jaybavisi_i-woke-up-this-morning-to-a-major-shock-activity-6786493451048488960-3KAb



Divers / Trolls velus

Les 0-days ces "Failles non corrigées"

- Traduction du légifrance:

  https://www.legifrance.gouv.fr/download/pdf?id=x5Au6KIZ7dCbg-_TGrJN

B. – Termes français

TERME FRANÇAIS (1)	DOMAINE/SOUS-DOMAINE	ÉQUIVALENT ÉTRANGER (2)
vulnérabilité non corrigée, faille non corrigée.	INFORMATIQUE.	zero-day, zero-day flaw, zero-day vulnerability.

(1) Les termes en caractères gras sont définis dans la partie I (*Termes et définitions*).
(2) Il s'agit d'équivalents anglais, sauf mention contraire.

- La définition détaillée est plus juste :

faille non corrigée
Domaine : INFORMATIQUE.
Synonyme : vulnérabilité non corrigée.
Définition : Faille identifiée par des utilisateurs d'un système informatique, à laquelle il n'existe pas encore de parade.
Note : Une faille non corrigée peut être exploitée à des fins malveillantes.
Voir aussi : prime à la faille détectée.
Équivalent étranger : zero-day, zero-day flaw, zero-day vulnerability.

Les VPN des entreprises qui collecter et de revendre vos données

- <<notre idée est de **remplacer** les **VPN**, ces outils utilisés pour sécuriser et anonymiser les connexions des **entreprises**, qui présentent le défaut de **collecter** et de **revendre** vos **données**.>> *Éric Léandri*

  https://www.francetvinfo.fr/replay-radio/nouveau-monde/nouveau-monde-lancien-patron-de-qwant-lance-une-solution-de-cybersecurite-respectueuse-des-donnees-personnelles_4321709.html

- Les RSSI et DPO vont être content d'apprendre qu'ils "collectent et vendent" les données des salariés

Divers / Trolls velus

Les 7 ans de Guillaume Poupard

https://www.linkedin.com/posts/guillaume-poupard-3604531b5_activity-6782172568922165248-SxDm

- Avec un QRCode

  https://eqrcode.co/a/TqKogD

  Merci aux agents de l'ANSSI, exceptionnels de compétence et de dévouement au service de la Nation. Merci aux partenaires du « C4 » et à ACYMA. Merci à notre belle « équipe de France » qui va se matérialiser encore un peu plus au sein du Campus Cyber. Et même si certains n'ont encore rien compris, **s'ingénient à nous ralenti**r, voir même **trahissent**, même si notre sécurité et notre souveraineté numériques sont plus que jamais menacées, cet engagement collectif est formidable et permet de continuer à y croire ! C'est cool :-)

Divers / Trolls velus

“Petit” problème de certificat expiré chez Pulse

- Touchant la version web du VPN
- Expiration du certificat signant l’exécutable
- Bug vérifiant la date d’expiration du certificat, plutot que la date de signature

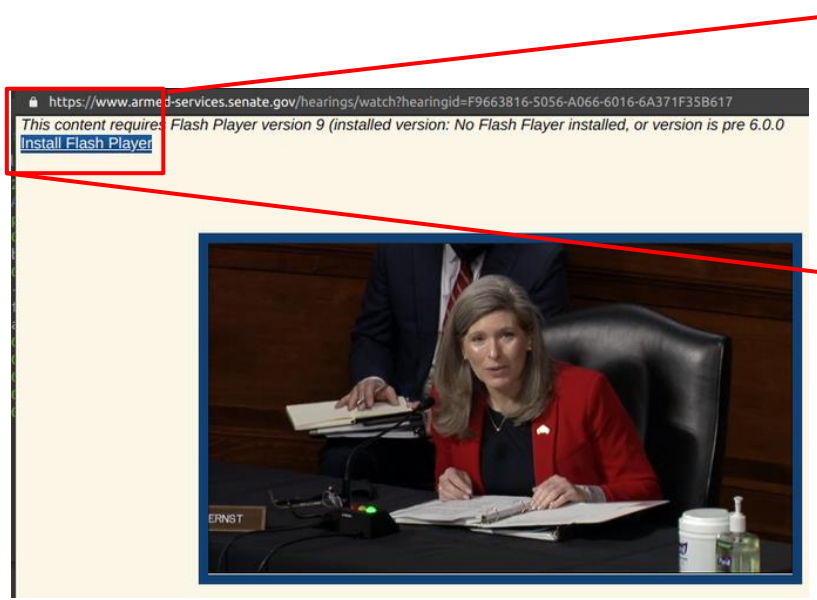
https://www.bleepingcomputer.com/news/security/pulse-secure-vpn-users-cant-login-due-to-expired-certificate/

Divers / Trolls velus

Staying alive, staying alive

- Plus supporté mais… :(

https://twitter.com/silascutler/status/1375097425262612485



Divers / Trolls velus

La “World War 3” pour bientôt ?

https://www.bloombergquint.com/opinion/one-wrong-hack-could-start-a-world-conflict-like-none-ever-seen-before

A Hack Like This Could Start the Next World War

BloombergOpinion

Tim Culpan

Bookmark

Published on March 08 2021, 6:54 AM
Last Updated on March 09 2021, 3:37 AM

(Bloomberg Opinion) -- It may be years before we get the Franz Ferdinand hack, but one cyber attack has the potential to set off a global war the likes of which we've never seen. Think beyond power and internet outages to banking failures, food shortages and poisoned water.

In the latest offensive, Chinese-backed operatives exploited vulnerabilities in Microsoft Corp.'s Exchange Server with vibrations felt around the world, mostly among small and medium-sized enterprises. Two months ago, the U.S. administration pointed the finger at Russia for a major attack on software provider SolarWinds Inc. which appeared to target government customers.

There's no end in sight. ✅

Divers / Trolls velus

Echelle de la cyber douille

Cyber Justin Bieber est nommé Cyber Czar

Cyber apocalypse (et ses quatre cyber-cavaliers)

VOUS ÊTES ICI

Cyber guerre mondiale

Cyber tchernobyl

Cyber pearl harbor

Cyber supply-chain attack
« The Big Hack »

Cyber attaque

Divers / Trolls velus

2020 vs 2021

- Fin 2020, Top arbitraires de l’année écoulée avec cette illustration


2020
Solarwinds
Curveball (CVE-2020-0601)
RCE Apple Mail (CVE-2020-9818)
SMBleed (CVE-2020-1206)
ZeroLogon (CVE-2020-1459)
BadNeighbour, local IPv6 DoS on Windows (CVE-2020-1459)
01/01/2021 : << Hold my beer >>

2020

Solarwinds
Curveball *(CVE-2020-0601)*
RCE Apple Mail *(CVE-2020-9818)*
SMBleed *(CVE-2020-1206)*
ZeroLogon *(CVE-2020-1459)*
BadNeighbour, local IPv6 DoS on Windows *(CVE-2020-1459)*

01/01/2021 : << Hold my beer >>

2021 Q1

Immunity Canvas leak -> Spectre exploit *(CVE-2017-5753, CVE-2017-5715)*
ProxyLogon, Exchange OWA pre-auth RCE *(CVE-2021-26855,..)*
pwn2own, 3 x Exchange OWA pre-auth RCE
Routable IPv6 DoS on Windows *(CVE-2021-24086)*
VMWare vSphere Client pre-auth RCE *(CVE-2021-21972)*
Fortinet, pre-auth RCE *(CVE-2020-29016, CVE-2020-29019..)*
F5 pre-auth Remote Command Injection *(CVE-2021-22986)*
Cisco small business, pre-auth RCE *(CVE-2021-1459)*
BleedingTooth, pre-auth RCE on Bluetooth *(CVE-2020-12352, CVE-2020-12351)*
Dedalus data leak of 500 000 french
Facebook data leak of 533 millions users
Linkedin data leak of 1 billion users

Prochaines réunions

Prochaine réunion

- 11 mai 2021… toujours en visio

After Work

- Pas avant ~~Q3~~ Q4 2021 ?

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?