Revue d'actualité de l'OSSIR

~~8 juin 2021~~

~~13 juillet 2021~~

~~aout 2021~~

14 septembre 2021

Aurélien Denis

*Vladimir Kolla @mynameisv_*

Nicolas Ruff @newsoft (le retour, he's back !)

Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

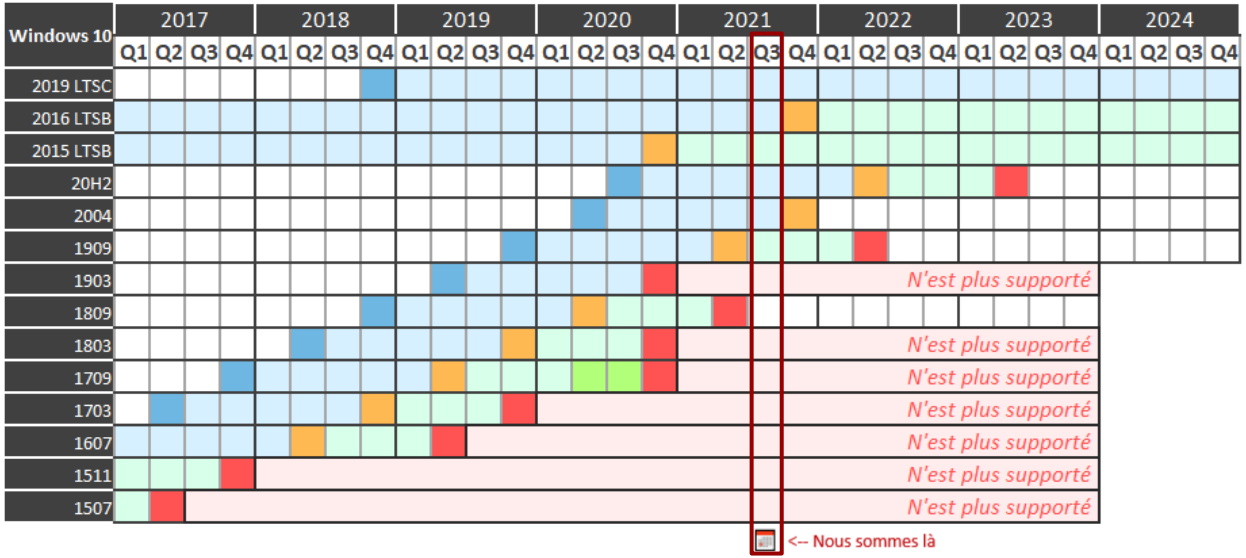
Report des fins de support de produits Microsoft suite au Covid-19

- 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

WIP

En juin :

- 50 vulnérabilités corrigées, dont 10 critiques

- A retenir :
  - CVE-2021-31955 : NTOSKRNL.EXE
    - Divulgation d'infos des adresses des structures EPROCESS
  - CVE-2021-31956 : Buffer overflow
    - Utilisées par le groupe d'attaquants PuzzleMaker
      https://www.kaspersky.fr/blog/chrome-windows-zero-day/17104/
  - PrintNightmare
    - Plus de détails juste après :)

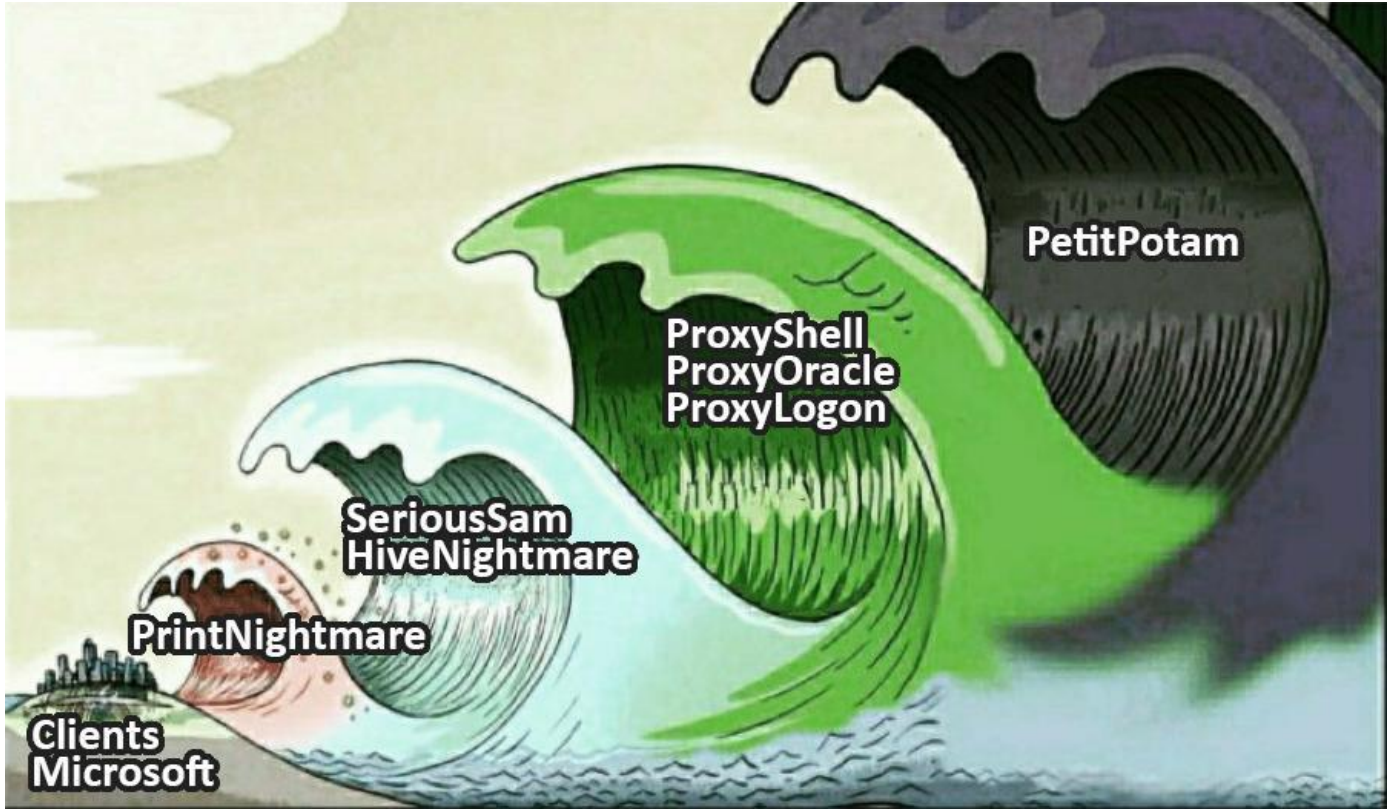
Composants impactés

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, PowerPoint, Outlook) ;
Microsoft Edge ;
Microsoft Internet Explorer ;
Visual Studio ;
Windows Admin Center ;
Microsoft Visio.

Failles / Bulletins / Advisories
Microsoft

WIP

Les clients de Microsoft….



Failles / Bulletins / Advisories
Microsoft - ProxyShell

WIP

Exchange en 2021

- ProxyLogon (CVE-2021-26855, CVE-2021-27065) par Orange Tsai
  - Obtenir un webshell depuis OWA, sans authentification, exploité par le groupe Hafnium

https://blog.orange.tw/2021/08/proxylogon-a-new-attack-surface-on-ms-exchange-part-1.html

- 4 RCE (CVE-2021-28480, CVE-2021-28481, CVE-2021-28482, CVE-2021-28483) par la NSA
- ProxyOracle (CVE-2021-31196, CVE-2021-31195) par Orange Tsai
  - Le bourrage “padding oracle” fonctionne toujours en 2021
  - Une XSS réfléchie pour voler le cookie du client

https://blog.orange.tw/2021/08/proxyoracle-a-new-attack-surface-on-ms-exchange-part-2.html

- ProxyShell présenté à Pwn2Own (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207) par Orange Tsai
  - Obtenir un shell depuis OWA, sans authentification
    - CVE-2021-34473 Contournement d’ACL du fait d’une confusion de chemin / path
    - CVE-2021-34523 Elévation de privilèges avec Exchange PowerShell Backend, car oui, Exchange exécute du PowerShell
    - CVE-2021-31207 Écriture arbitraire de fichier après authentification permettant d’aboutir à une exécution de code

https://blog.orange.tw/2021/08/proxyshell-a-new-attack-surface-on-ms-exchange-part-3.html

- Bonus (CVE-2021-33768)
- Un PoC parmis d’autres : https://github.com/dmaasland/proxyshell-poc/blob/main/proxyshell-enumerate.py

Failles / Bulletins / Advisories
Microsoft - PetitPotam

WIP

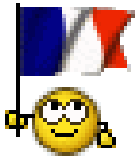
SeriousSAM ou **HiveNightmare (CVE-2021-36934)**

- Erreur d’attribution des droits à la base SAM
- La base SAM accessible en lecture sans privilèges
- Récupérable avec les Volume Shadow Copy
- Un correctif manuel:
  - `icacls $env:windir\system32\config\*.* /inheritance:e`
- Petit PoC : https://github.com/cube0x0/CVE-2021-36934

Failles / Bulletins / Advisories
Microsoft - PetitPotam

WIP

PetitPotam ou EfsPotato



- Obtenir un compte du domaine (son condensat)… sans authentification
  - Compte machine d'un contrôleur de domaine (NTLMv2 ou v1)

  https://github.com/topotam/PetitPotam
- C'est une fonctionnalité, donc pas de correctif prévu
- Un correctif non officiel chez 0patch

  https://blog.0patch.com/2021/08/free-micropatches-for-petitpotam.html
- La meilleure solution reste de filtrer les appels RPC depuis le firewall Windows:

  https://twitter.com/gentilkiwi/status/1421949715986403329
- Interview de **topotam** dans Hack'n Speak

  https://open.spotify.com/episode/45lYLpa935c7AI8DvzlBxw

Mise à jour :

- Considéré comme une vulnérabilité : CVE-2021-36942
- Un correctif "incomplet" en Aout : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36942

Failles / Bulletins / Advisories
Microsoft - PrintNightmare

WIP

***(exploit)* Prise de contrôle du système et élévation de privilèges via 2 vulnérabilités au sein des systèmes Windows**

- CVE-2021-1675 : LPE
- CVE-2021-34527 : RCE
- Exploit publics dispos
- Et module mimikatz 💣

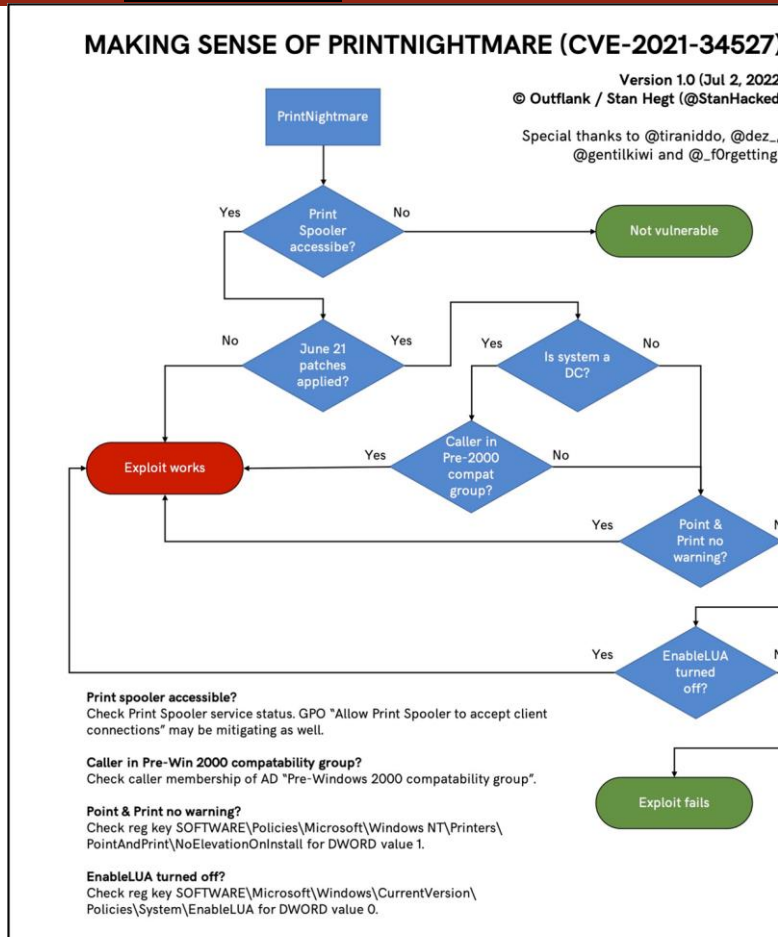
https://github.com/afwu/PrintNightmare

Failles / Bulletins / Advisories
Microsoft - PrintNightmare

WIP

Les réactions et recommandations

- Premières recos : Désactiver le spouleur d'impression
  - Compliqué à mettre en place
  - Le spouleur sert au DC à gérer les jobs d'impression
- Compliqué de savoir si on est vuln également
- Microsoft publie un **<u>patch hors cycle</u>**

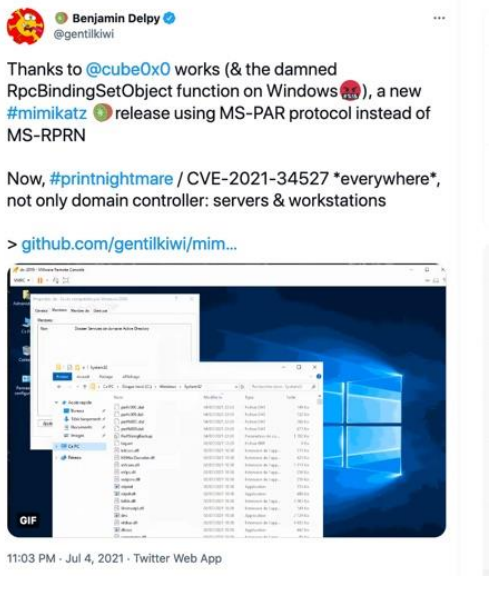


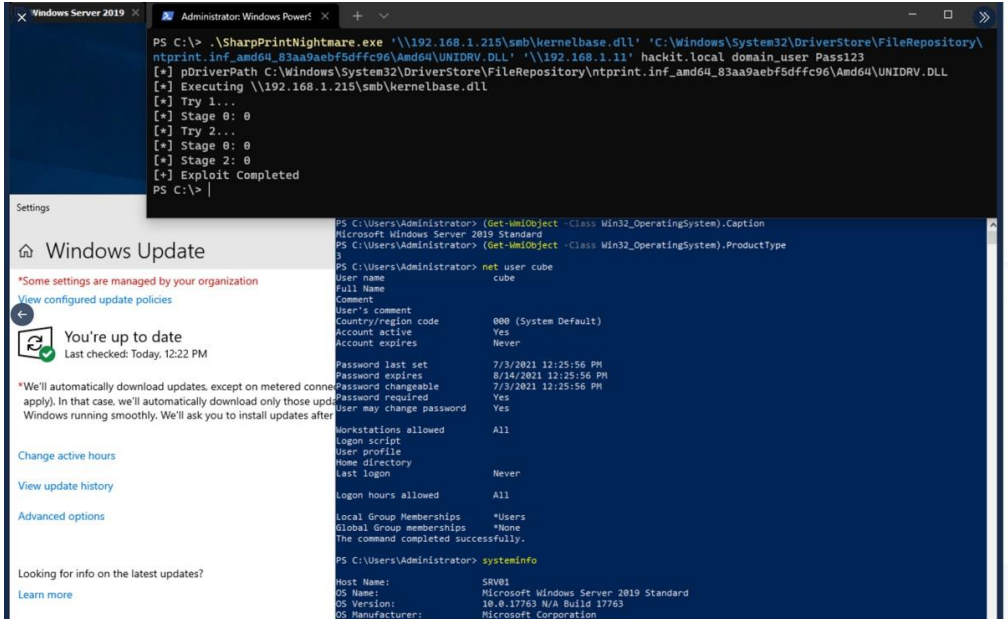
Failles / Bulletins / Advisories
Microsoft - PrintNightmare

WIP

(exploit) **Prise de contrôle du système et élévation de privilèges via 2 vulnérabilités au sein des systèmes Windows**

- Premières recos : Désactiver le spouleur d'impression
- Microsoft publie un patch hors cycle

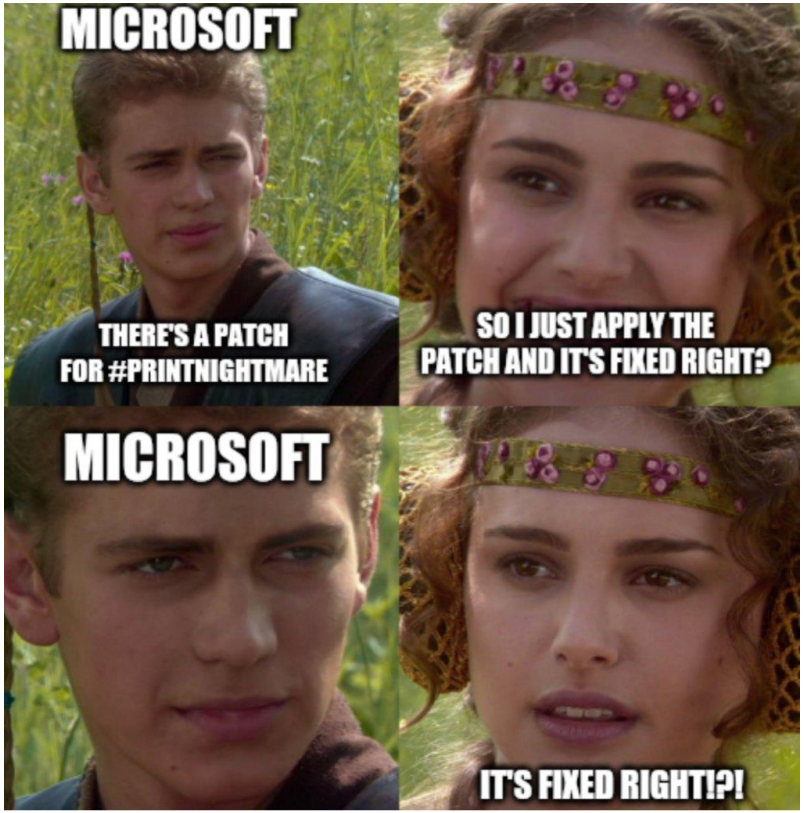




Failles / Bulletins / Advisories

Microsoft - PrintNightmare - Un fix ?

WIP



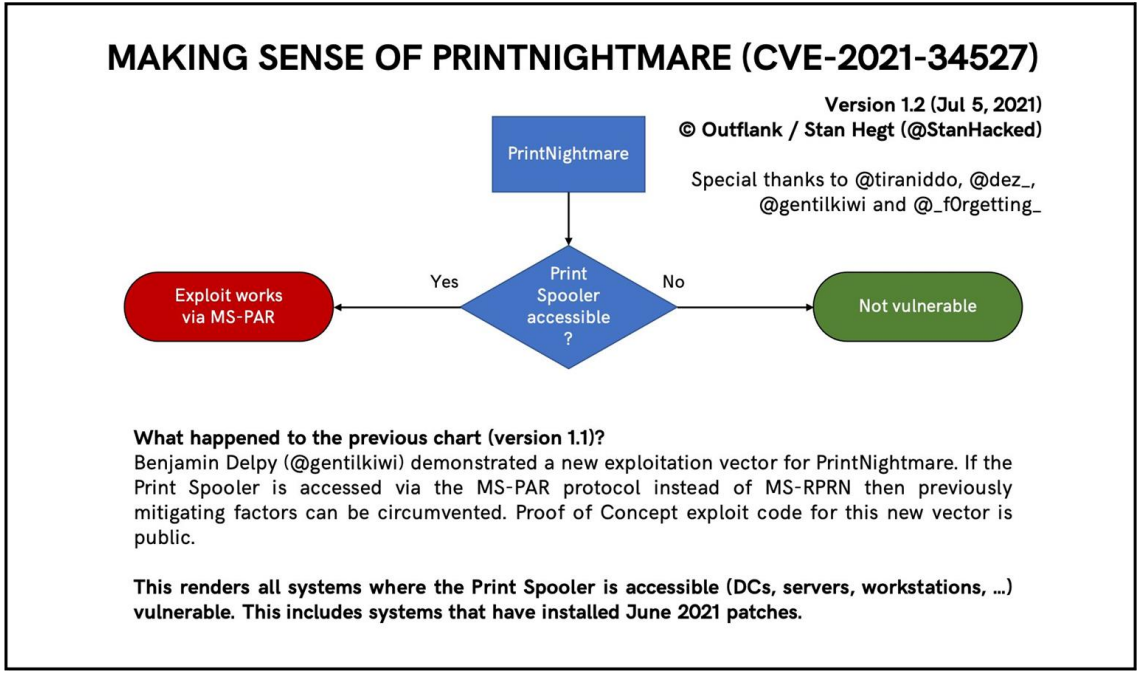
Failles / Bulletins / Advisories
Microsoft - PrintNightmare - L'état actuel ?

WIP

Résultat :

- Flou mais globalement pas bon
- On espère un fix ce soir ? 🤞🙏

  https://github.com/afwu/PrintNightmare



https://twitter.com/StanHacked/status/1412060814488608773/

Failles / Bulletins / Advisories
Microsoft - Exploit

WIP

(exploit) Prise de contrôle du système via une vulnérabilité Powershell (CVE-2021-26701)

- Erreur dans le framework .NET embarqué

  https://azure.microsoft.com/en-us/updates/update-powershell-versions-70-and-71-to-protect-against-a-vulnerability/

Faille dans Internet Explorer (MSHTML) CVE-2021-40444

- Exploité dans la nature
  - Doc, docx, rtf… envoyé par mail
  - Contient un object OLE pointant vers une URL
  - Word télécharge ce qu'il y'a derrière l'URL et parse le contenu avec MSHTML
  - L'HTML contient du Javascript interprété qui télécharge un CAB, le décompresse et appelle une DLL renommée avec une sorte de path traversal

https://www.trendmicro.com/en_us/research/21/i/remote-code-execution-zero-day--cve-2021-40444--hits-windows--tr.html

```
_0xfed1ef['Script']['location'] = '.cpl:123',
_0xfed1ef['Script']['location'] = '.cpl:../../../AppData/Local/Temp/Low/championship.inf',
_0x5f3191['Script']['location'] = '.cpl:../../../AppData/Local/Temp/championship.inf',
_0xafc795['Script']['location'] = '.cpl:../../../../AppData/Local/Temp/Low/championship.inf',
_0x5a6d4b['Script']['location'] = '.cpl:../../../../AppData/Local/Temp/championship.inf',
_0x258443['Script']['location'] = '.cpl:../../../../../Temp/Low/championship.inf',
_0x5a6d4b['Script']['location'] = '.cpl:../../../../../Temp/championship.inf',
_0x5a6d4b['Script']['location'] = '.cpl:../../Low/championship.inf',
_0x5a6d4b['Script']['location'] = '.cpl:../../championship.inf';
```

Failles / Bulletins / Advisories
Microsoft - Exploit

WIP

(exploit) RCE via une vulnérabilité au sein de Windows Defender

- BSoD via une requête par WinRM (user-after-free)
- On espère que y’aura pas de RCE

https://github.com/0vercl0k/CVE-2021-31166

Failles / Bulletins / Advisories
Navigateurs (principales failles)

Google Chrome, Prise de contrôle du système et manipulation de données via 18 vulnérabilités

- WebGL, WebAudio, etc.
- CVE-2021-30554 : Exploitée in the wild
- CVE-2021-30551 : Exploit disponible

https://chromereleases.googleblog.com/2021/06/stable-channel-update-for-desktop_17.html
https://securelist.com/puzzlemaker-chrome-zero-day-exploit-chain/102771

Microsoft Edge, Élévation de privilèges et manipulation de données via 3 vulnérabilités

- Exécution via le moteur de scripting

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26419

Mozilla Firefox, Divulgation d'informations via une vulnérabilité (mfsa 2021-27)

- OoB - Read

https://www.mozilla.org/en-US/security/advisories/mfsa2021-27/

Failles / Bulletins / Advisories
Systèmes

GitLab, Prise de contrôle du système et manipulation de données via 20 vulnérabilités

- CSRF sur l'API GraphQL

https://about.gitlab.com/releases/2021/06/01/security-release-gitlab-13-12-2-released/

SAP, Contournement de sécurité et manipulation de données via 37 vulnérabilités (2021-Jun)

- Commerce, NetWeaver, Business…
- Manque de vérifications et injection de code

https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=576094655

Confluence, exécution de code (CVE-2021-26084)

- Pour un utilisateur authentifié

https://confluence.atlassian.com/doc/confluence-security-advisory-2021-08-25-1077906215.html

Failles / Bulletins / Advisories
Systèmes

WIP

iOS 12, Prise de contrôle du système via 3 vulnérabilités (HT212548)

- Erreur de validation des certificats ASN.1 (CVE-2021-30737)
- RCE via pages web spécifiquement conçues sur WebKit
  - CVE-2021-30761 et CVE-2021-30762
  - Exploitées in the Wild !

    https://support.apple.com/en-us/HT212548

Ghostscript, exécution de code lors du traitement d'un .ps (CVE-2021-3781)

- Mauvaise validation du contenu après un %pipe%

  https://git.ghostscript.com/?p=ghostpdl.git;a=commitdiff;h=a9bd3dec9fde

  Exploit : `%!PS\r\n(%pipe%/tmp/ 2>/dev/null & id)`
- Surface importante car beaucoup d'outils utilisent Ghostscript comme "less"

  https://twitter.com/jensvoid/status/1435631308294795264?s=11

Failles / Bulletins / Advisories
Systèmes

WIP

Linux, élévation locale de privilèges non considéré comme sécurité

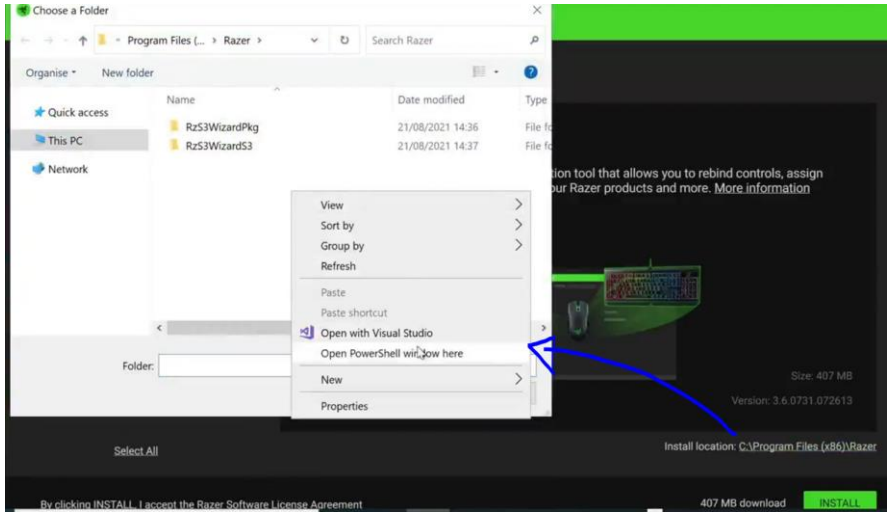
- Dépassement de tampon dans access_remote_vm()
- Encore une vulnérabilité sans CVE...

https://lore.kernel.org/lkml/20210726153850.880812722@linuxfoundation.org/

Windows, élévation locale de privilèges grâce aux souris Razer

- Installer une souris Razer, mettez à jours les pilotes et… ouvrez l'explorateur en SYSTEM
https://twitter.com/j0nh4t/status/1429049506021138437
- Tous les Vendor ID et Products ID pour Windows 10
  - Afin de les usurper et tester

https://pastebin.com/k2Hb0bPU



Failles / Bulletins / Advisories
Mobile

WIP

iOS 14.0, chaine d'exploits RCE+LPE

- Exploit privé mais qui ne le restera pas longtemps 😂
  https://twitter.com/pattern_F_/status/1432599008757760000

Ghostscript, exécution de code lors du traitement d'un .ps (CVE-2021-3781)

- Mauvaise validation du contenu après un %pipe%
  https://git.ghostscript.com/?p=ghostpdl.git;a=commitdiff;h=a9bd3dec9fde
  Exploit : `%!PS\r\n(%pipe%/tmp/ 2>/dev/null & id)`
- Surface importante car beaucoup d'outils utilisent Ghostscript comme "less"
  https://twitter.com/jensvoid/status/1435631308294795264?s=11

Failles / Bulletins / Advisories
Réseau (principales failles)

WIP

Cisco

16 bulletins, dont **aucun critique**

- Cisco WebEx
  - Corruption mémoire via la lecture de fichiers ARF ou WRF
  - CVE-2021-1502, CVE-2021-1503, CVE-2021-1526
- Cisco SD-WAN
  - PrivEsc via l'appel à un processus privilégié (CVE-2021-1528)

- Produits vulnérables
  - Cisco SD-WAN
  - Cisco WebEx
  - Cisco ThousandEyes Recorder
  - Cisco Video Surveillance 7000 Series IP
  - Cisco ASR 5000
  - Cisco Common Services Platform Collector
  - Cisco Small Business 100,300,500 Series Wireless Access Points
  - Cisco DNA Spaces Connector
  - Cisco Finesse
  - Cisco Modelling Labs
  - Cisco ADE OS

Failles / Bulletins / Advisories
Réseau (principales failles)

Stormshield Network Security, 3 Dénis de service (STORM-2021-033/STORM-2021-017/STORM-2021-009)

- Mise à jour de ClamAV et OpenSSL

  https://advisories.stormshield.eu/2021-009/

  https://advisories.stormshield.eu/2021-017/

  https://advisories.stormshield.eu/2021-033/

SolarWinds Network Performance Monitor, exécution de code à distance (CVE-2021–31474)

- Par une simple requête POST et du contenu XML

  https://gist.github.com/testanull/dcb536b409a28d74430a441d53b14456?fbclid=IwAR0aAnZndfZR2isO4I0UNt9FzMAIB7EJy7e4X7dtTdKouhnFu7qZ7NQ8W8M

Contournement de sécurité et déni de service via 2 vulnérabilités sur le client Windows F5

- Bump de lib

  https://support.f5.com/csp/article/K33101555

  https://support.f5.com/csp/article/K52494142

Failles / Bulletins / Advisories
Réseau (principales failles)

WIP

Fortinet

- Suppression arbitraire de fichier via une requête POST
- Permet le reset du mdp admin

https://www.fortiguard.com/psirt/FG-IR-21-048

Paloalto PanOS (firewall)

- Buffer overflow sur Telnet 😱 https://security.paloaltonetworks.com/CVE-2020-10188
- Injection de commande (CLI) depuis le portail web d'administration https://security.paloaltonetworks.com/CVE-2021-3050

Juniper JunOS, Manipulation de données et divulgation d'information (JSA11159)

- Erreurs CRLF

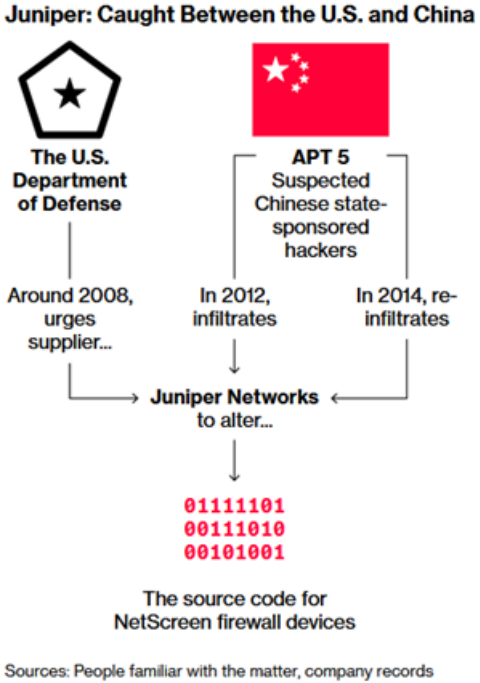
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11159&cat=SIRT_1&actp=LIST

Failles / Bulletins / Advisories
Réseau (principales failles)

WIP

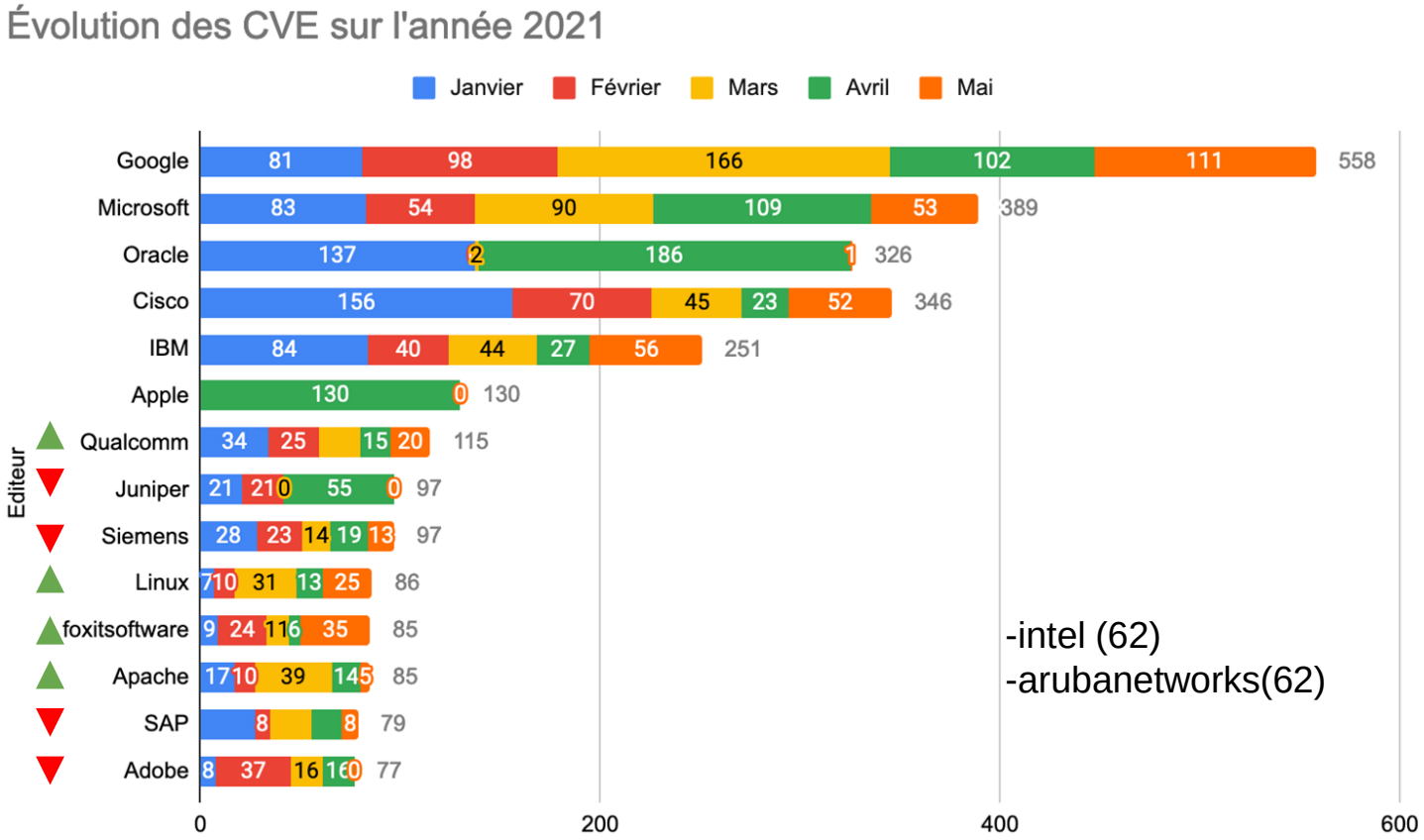
Firewalls Juniper, les origines des portes dérobées découvertes en 2015

- L'article de Bloomberg : https://www.bloomberg.com/news/features/2021-09-02/juniper-mystery-attacks-traced-to-pentagon-role-and-chinese-hackers
- Tout se résume à un seul petit graphique:



Stats du mois

WIP



-intel (62)
-arubanetworks(62)

Piratages, Malwares, spam, fraudes et DDoS

WIP

Pirater Azure CosmoDB avec Jupyter Notebook

- Microsoft fournit Jupyter Notebook pour visualiser ses données
- Activé par défaut en février 2021 pour tout utilisateur d'Azure CosmoDB
- Rebond d'un Notebook aux autres et fuite de la clef CosmoDB
  - La victime ne voit rien
  - Microsoft ne peut pas changer la clef des clients
  - Détails techniques non publiés à cet instant

https://www.wiz.io/blog/chaosdb-how-we-hacked-thousands-of-azure-customers-databases

Piratages, Malwares, spam, fraudes et DD
Piratages

WIP

NSO Group, encore et toujours...

- Aide au piratage d'activiste au sultanat du Bahrain

  https://thehackernews.com/2021/08/bahraini-activists-targeted-using-new.html
- Perd une liste de 50 000 "potentielles" cibles, fournies à des journalistes
  - Journalistes, politiques, avocats, Macron 🤔, des princes, chefs d'entreprises...

  https://www.lemonde.fr/projet-pegasus/article/2021/07/18/projet-pegasus-revelations-sur-un-systeme-mondial-d-espionnage-de-telephones_6088652_6088648.html
- Se fait couper ses infrastructures AWS, par AWS

  https://www.vice.com/en/article/xgx5bw/amazon-aws-shuts-down-nso-group-infrastructure
- Moody's baisse leur note (Performance décevantes, procès, baisse du nombre de clients...

  https://m.moodys.com/research/Moodys-downgrades-NSO-to-B3-with-negative-outlook--PR_446947
- Le malware pour android décompilé

  https://github.com/jonathandata1/pegasus_spyware
- Une partie de la chaîne zero-click identifiée, **mettez à jour**
  - Vulnérabilité sur le traitement d'un PDF contenant une image au format JBIG2
  - CVE-2021-30860 touchant dans Apple iMessage (iOS, macOS, watchOS)

  https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/

Piratages, Malwares, spam, fraudes et DD
Piratages

WIP

NSO Group, Scanner son mobile à la recherche de Pegasus

- Merci Amnesty International et CitizenLab
  - Mais… les IoC risquent d'être "burned" pour les prochaines version de Pegasus

https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

https://arkadiyt.com/2021/07/25/scanning-your-iphone-for-nso-group-pegasus-malware/

Piratages, Malwares, spam, fraudes et DD
Piratages

WIP

Le ministère de l'Intérieur belge compromis depuis 2019

- Par le groupe Hafnium (cf. ProxyLogon)
- Investigation en 2021 pour vérifier si la vuln avait été exploitée
  - Ont retrouvés une backdoor de 2019

https://therecord.media/belgium-government-discovers-old-2019-hack-during-hafnium-investigation/

https://www.zdnet.fr/actualites/le-ministere-de-l-interieur-belge-pirate-depuis-plus-de-deux-ans-39923497.htm

Plus d'informations sur le hack de Colonial Pipelines

- C'était une attaque avancée… 🤔
- Ah non : Accès initial via un VPN qui n'avait pas la MFA d'activé :(

https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password?sref=ylv224K8

Piratages, Malwares, spam, fraudes et DD
Fuite de données / Supply Chain

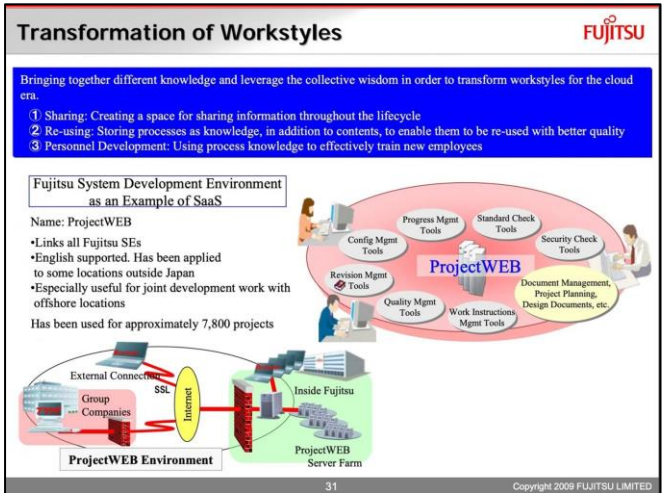
WIP

Fuite de code source de la société Rapid7 suite à l'incident Codecov

- Attaque de la chaîne d'approvisionnement
  https://www.rapid7.com/blog/post/2021/05/13/rapid7s-response-to-codecov-incident/

La compromission d'une plateforme de Fujitsu mène à la fuite d'informations d'agences gouvernementales

- L'application ProjectWEB
  https://www.teiss.co.uk/japanese-government-agencies-suffered-breaches-following-fujitsus-projectweb-hack/

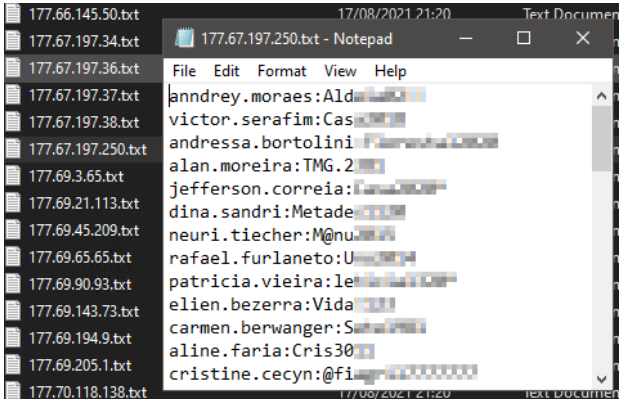


Piratages, Malwares, spam, fraudes et DD
Fuite de données / Supply Chain

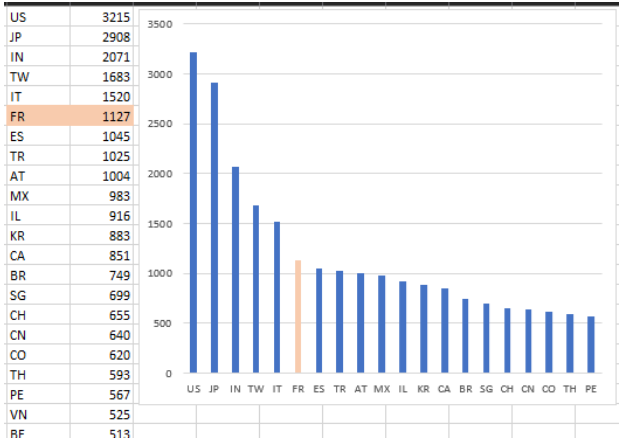
WIP

Fuite des identifiants+mot de passe de 86 939 VPN Fortinet

- Suite à une collecte automatisée exploitant la vulnérabilité CVE-2018-13379
- IP, pays, logins et mots de passe :



Top 20



- Pensez à vérifier à minima si vos IP y sont :

  http://flhnknbdg7yddsu3gj5lyn2wjkb3mmuoatmi5z5qe2oddiiyizlwyyad.onion/forti/

  https://ghostbin.com/paste/neBjh

- L'article Bleeping

  https://www.bleepingcomputer.com/news/security/hackers-leak-passwords-for-500-000-fortinet-vpn-accounts/

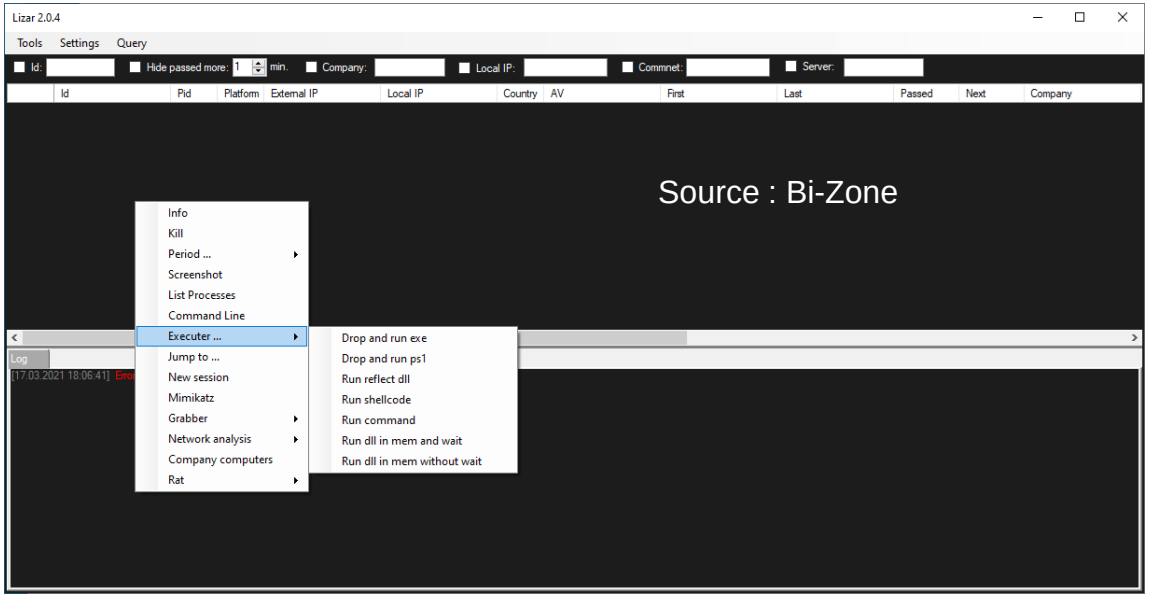
Piratages, Malwares, spam, fraudes et DD
Malware

WIP

Le groupe FIN7 est de retour avec un nouveau malware baptisé Lizar

- Basé sur Carbanak
- “Disguised as a legitimate cybersecurity company, the group distributes Lizar as a pentesting tool for Windows networks”

https://bi-zone.medium.com/from-pentest-to-apt-attack-cybercriminal-group-fin7-disguises-its-malware-as-an-ethical-hackers-c23c9a75e319



Piratages, Malwares, spam, fraudes et DD
Ransomwares - Pwn

WIP

L'entreprise CNA Financial paie une rançon de 40 millions de dollars

- Après une cyberattaque
- Selon l'entreprise, le paiement a suivi les législations en vigueur

https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack

Le ransomware du groupe Conti a attaqué 16 organisations américaines de soins de santé et de premiers secours.

- Conti semble être assez éclectique en ce moment

https://www.aha.org/system/files/media/file/2021/05/fbi-tlp-white-report-conti-ransomware-attacks-impact-healthcare-and-first-responder-networks-5-20-21.pdf

Piratages, Malwares, spam, fraudes et DD
Ransomwares - Pwn

WIP

Les services de santé irlandais attaqués par un ransomware

- Conti à l'origine
- La rançon ne sera pas payée

https://www.zdnet.fr/actualites/une-attaque-au-ransomware-bloque-les-services-de-sante-irlandais-39922713.htm

https://www.bleepingcomputer.com/news/security/irish-healthcare-shuts-down-it-systems-after-conti-ransomware-attack/#:~:text=Conti%20operates%20as%20a%20private,shares%20of%20

Piratages, Malwares, spam, fraudes et DD
Ransomwares - Clap de fin?

WIP

Des groupes d'attaquants décident de restreindre l'accès à leurs ransomwares

- Bannissement des pubs pour les ransomwares sur certaines plateformes de hack

  https://www.helpnetsecurity.com/2021/05/18/raas-gangs/

Après avoir extorqué près de 350 000$, le ransomware Qlocker a cessé d'accepter les paiements

- Après un mois d'activité

  https://www.tripwire.com/state-of-security/featured/qlocker-ransomware-gang-shuts-shop-extorting-qnap-nas-drives/

Vous vous souvenez de DarkSide ?

- Le hack de trop ?

  https://www.nytimes.com/2021/05/14/business/darkside-pipeline-hack.html

  https://www.usine-digitale.fr/article/le-fbi-recupere-une-partie-de-la-rancon-versee-par-pipeline-colonial-mais-refuse-de-dire-comment.N1100884

Piratages, Malwares, spam, fraudes et DD
Ransomwares - Clap de fin?

WIP

Inculpation d'un membre du groupe Trickbot

- Véritable organisation "professionnelle"
- Arrestation à Miami, en Létonie...
- Le document est très complet

https://www.helpnetsecurity.com/2021/05/18/raas-gangs/

57. Defendant ALLA WITTE, aka MAX, was a national of Russia. During the timeframe of this indictment, WITTE resided in Suriname. WITTE was a Malware Developer for the Trickbot Group, overseeing the creation of code related to the monitoring and tracking of authorized users of the Trickbot malware, the control and deployment of ransomware, obtaining payments from ransomware victims, and developing tools and protocols for the storage of credentials stolen and exfiltrated from victims infected by Trickbot.

59. Co-Conspirator 8 ("CC8") was a Malware Manager who outlined programming needs, managed finances and deployed Trickbot.

66. The objects of the conspiracy included for the Defendants to:

a. infect victims' computers with Trickbot malware designed to capture victims' online banking login credentials;

b. obtain and harvest other personal identification information, including credit cards, emails, passwords, dates of birth, social security numbers, and addresses;

c. infect other computers networked with the initial victim computer;

d. use the captured login credentials to fraudulently gain unauthorized access to victims' online bank accounts at financial institutions;

e. steal funds from victims' bank accounts and launder those funds using U.S. and foreign beneficiary bank accounts provided and controlled by conspirators; and

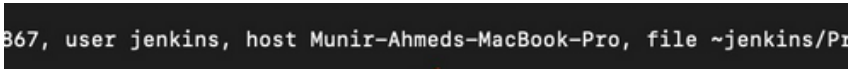
f. infect victims' computers with ransomware.

Piratages, Malwares, spam, fraudes et DD
Ransomwares - Clap de fin?

WIP

OpSec fail

- Un malware macOS qui contient un fichier .swp
- Qui lui-même contient le nom de l'ordinateur
  - Nommé avec le nom du l'auteur du malware



https://twitter.com/lordx64/status/1430623098718535681

Piratages, Malwares, spam, fraudes et DD
Ransomwares - Evolution

WIP

Évolution des ransomwares : Prometheus, Grief et Payload.bin

- Pwn d'un ministère mexicain
- Prometheus se présente comme une filiale de REvil
- Bientôt Sodinokibi Holding LLC ?

https://securityaffairs.co/wordpress/118446/cyber-crime/prometheus-grief-ransomware.html

Le FBI et l'ACSC publient des avertissements à propos d'une campagne d'attaques utilisant le ransomware Avaddon

- Partage de TTPs et IOCs

https://www.cyber.gov.au/sites/default/files/2021-05/2021-003%20Ongoing%20campaign%20using%20Avaddon%20Ransomware%20-%2020210508.pdf

https://blog.malwarebytes.com/ransomware/2021/05/avaddon-ransomware-campaign-prompts-warnings-from-fbi-acsc/

Piratages, Malwares, spam, fraudes et DD
Publication

WIP

La CNIL publie sa stratégie annuelle de contrôle pour l'année 2021

- L’accent est mis sur :
  - La cybersécurité des sites web
  - La sécurité des données de santé
  - Le contrôle du respect des règles applicables aux cookies et autres traceurs

https://www.avocats-mathias.com/actualites/strategie-controle-2021

https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article32

Recommandations aux opérateurs de solutions numériques

- Pour l’enseignement et la recherche
- Par SupDPO (DPO des établissements d'enseignement supérieur et de recherche)

https://reseau.supdpo.fr/wp-content/uploads/2021/05/SupDPO-Privacy-Shield-Reco-publiques-aux-operateurs-de-solutions-numeriques-US-V1.pdf

Piratages, Malwares, spam, fraudes et DD
Pirater les pirates

WIP

150 vulnérabilités trouvées dans une soixantaine de spyware Android

- Mais pas de CVE ;-)
- Met en avant que les applications “malveillantes” restent avant tout des applications avec les bugs associés

https://www.welivesecurity.com/2021/05/17/android-stalkerware-threatens-victims-further-exposes-snoopers-themselves/

https://www.welivesecurity.com/wp-content/uploads/2021/05/eset_android_stalkerware.pdf

L’une des applications de communication des criminels appartenait au FBI

- Takeover de la messagerie “Anom”
- Stockage des messages pendant leur transit

https://www.vice.com/en/article/akgkwj/operation-trojan-shield-anom-fbi-secret-phone-network

https://www.youtube.com/watch?v=e443mE8l-_0

Attaque
Techniques & outils

WIP

Cheatsheet pour ~~pirater~~ auditer les mobiles par RandoriSec

- 4 fiches assez complètes

  https://twitter.com/randorisec/status/1430545306735812608

Un proxy HTTPS en C# utilisable en tant qu'assembly

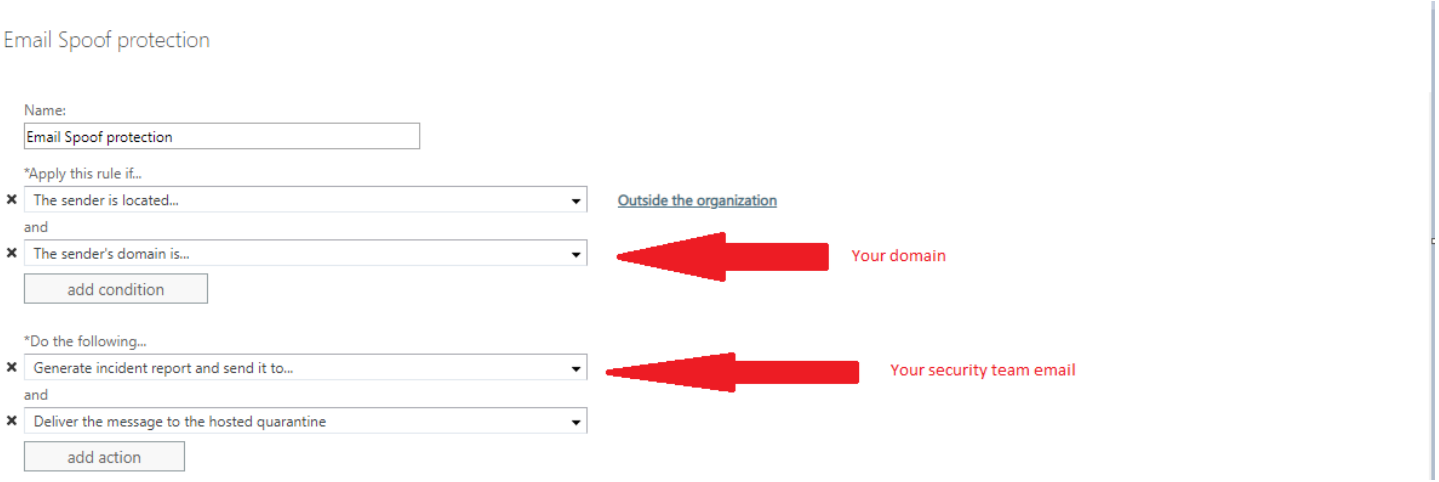
https://github.com/secdev-01/HTTPS_CSharp_Server

WIP

Empêcher les phishing depuis des blog storage Azure

- En 3 clics

  https://www.bleepingcomputer.com/news/security/office-365-custom-rules-to-block-azure-blob-storage-phishing-attacks/



DFIR / OSINT
Techniques & outils

WIP

Emulateur VBS

- Fait par le développeur d'oletools
- Permet de désobfusquer les macros
- La présentation est par ici ---> https://www.sstic.org/2021/presentation/oletools/

https://github.com/decalage2/ViperMonkey

Les outils de Thibault pour l'analyse de TinyNuke

- Analyse de la config, extraction de la DLL, script de désobfuscation...

https://github.com/Heat-Miser/tinynuke-toolset

Vie privée
Données & Cookies

WIP

Firefox active dorénavant par défaut la protection contre les cookies intersites en mode « navigation privée »

- Blocage des trackeurs, isolation des cookies par site etc.

  https://blog.mozilla.org/security/2021/06/01/total-cookie-protection-in-private-browsing/

Le respect des données des utilisateurs d'Apple en Chine pourrait être en danger

- Partenariat entre Apple et l'entreprise chinoise GCBD
- Hébergement des données sur des datacenters locaux pour iCloud

  https://thehackernews.com/2021/05/how-apple-gave-chinese-government.html

  https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html

Business et Politique

Business
Monde

WIP

FireEye est vendu pour 1,2 milliards de dollars

- Seulement la partie FireEye Products
- Vendu à Symphony Technology Group (RSA Security / McAfee Enterprise)
- Produit FireEye et Conseil Mandiant se bloquaient mutuellement (indépendance, tout ça…)

https://investors.fireeye.com/news-releases/news-release-details/fireeye-announces-sale-fireeye-products-business-symphony

Changement des conditions générales de TikTok

- Et collecte massive des données biométriques des américains
- Sera parfait croisé avec la fuite de données sur les 250 millions d'américains

https://techcrunch.com/2021/06/03/tiktok-just-gave-itself-permission-to-collect-biometric-data-on-u-s-users-including-faceprints-and-voiceprints/

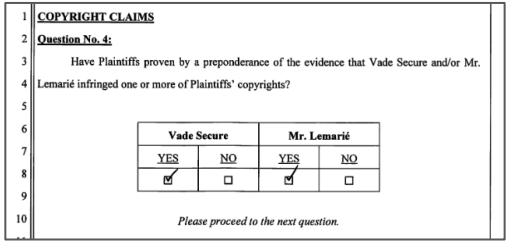
WIP

Vade Secure se fait “Alstomer” par les USA

- Le protectionnisme américain à encore frappé
- Cloudmark est une société de sécurité du mail dans le Cloud
  - 2010 à 2016, Olivier Lemarié y est VP
  - Nov. 2016, il quitte Cloudmark pour VadeSecure
  - 2017, ProofPoint rachète Cloudmark pour $110 millions
  - 2019, ProofPoint attaque VadeSecure en justice pour vol de secret (IP et bouts de code)
  - “Je ne sais pas quand”
    - Vade Secure attaque le marché américain
    - Lance une grosse levée de fonds auprès d’un fond américain… annulée
      https://business.lesechos.fr/amp/03/339403.php
  - Vade Secure perd avec une amende de $14 millions
    - Plus les frais de justice 😢

    https://regmedia.co.uk/2021/08/24/proofpoint_verdict.pdf

https://www.zdnet.com/article/proofpoint-awarded-13-5-million-in-ip-theft-lawsuit-against-vade-secure/



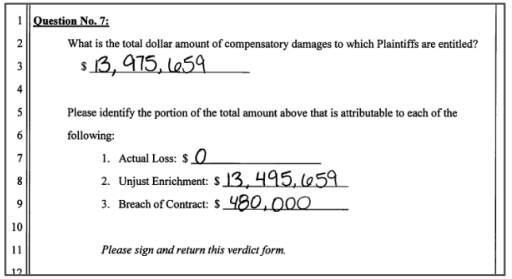
COPYRIGHT CLAIMS

Question No. 4:

Have Plaintiffs proven by a preponderance of the evidence that Vade Secure and/or Mr. Lemarié infringed one or more of Plaintiffs' copyrights?

Vade Secure		Mr. Lemarié	
YES	NO	YES	NO
☑	☐	☑	☐

Please proceed to the next question.



Question No. 7:

What is the total dollar amount of compensatory damages to which Plaintiffs are entitled?

$ 13,975,659

Please identify the portion of the total amount above that is attributable to each of the following:

1. Actual Loss: $ 0
2. Unjust Enrichment: $ 13,495,659
3. Breach of Contract: $ 480,000

Please sign and return this verdict form.

WIP

Nexa et Amesys mis en examen

- Par les juges d'instruction du pôle « crimes contre l'humanité » du tribunal judiciaire de Paris
- Les dirigeants d'Amesys dans le volet Lybien pour :
  - « complicité d'actes de **tortures** »
- Les dirigeants de Nexa dans le volet égyptien pour :
  - « complicité d'actes de **torture** et de **disparitions** forcées »
- Nexa = Intellexa
  - Fusion de Nexa et WiSpear (Israel) puis Senpai Technologies (Israel, anciens de l'Unité 8200)

https://triloguenews.com/mee-cybersurveillance-en-libye-et-en-egypte-quatre-dirigeants-dentreprises-francaises-mis-en-examen-par-eleonore-dermy

Droit / Politique
Monde

WIP

Le Conseil européen prolonge les sanctions émises contre les acteurs responsables de cyberattaques ciblant ses pays membres

- Gel des assets, persona non grata, etc.

  https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02019D0797-20201124&qid=1620137455138

  https://www.consilium.europa.eu/fr/press/press-releases/2021/05/17/cyber-attacks-council-prolongs-framework-for-sanctions-for-another-year/

  https://www.consilium.europa.eu/fr/press/press-releases/2020/10/22/malicious-cyber-attacks-eu-sanctions-two-individuals-and-one-body-over-2015-bundestag-hack/

  https://www.consilium.europa.eu/fr/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/

L'application WhatsApp a été interdite de récupérer les données personnelles des utilisateurs en Allemagne

- La HmbBfDI a tranché
- Facebook va faire appel

  https://thenextweb.com/news/german-regulator-bans-facebook-from-processing-whatsapp-user-data

Droit / Politique
Monde

WIP

Le doxxing, c’est à présent illégal

- Précédemment pas défini dans le code pénal et donc pas réprimé en tant que tel
- Le directeur de la publication peut voir sa responsabilité engagée
- Quid des infractions passées encore accessibles ?

https://www.legifrance.gouv.fr/jorf/jo/2021/08/25/0197

Conférences

Conférences

Passée

- Le Netmask et la Plume
- Barbhack le 28 aout 2021 à Toulon
- CORI&IN et FIC 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

A venir

- Le Hack?
- BotConf les 26-29 avril 2022

Divers / Trolls velus

Divers / Trolls velus

WIP

Taviso et les vulns Microsoft Defender

- Parsing des formats compressés et “packés” en mode Kernel… et simplifié face à ASProtect

  https://bugs.chromium.org/p/project-zero/issues/detail?id=2189

Améliorez vos tentatives de cassage de mot de passe

- Permet de générer des masques à partir d’une liste de mot de passe
- Permet de créer une variation d’un dictionnaire en incrémentant/décrémentant les entiers
- La présentation du tool se fait ici : https://static.sstic.org/rumps2021/SSTIC_2021-06-03_P11_RUMPS_03.mp4

  https://github.com/mynameisv/PROUT

La NSA a eu accès aux écoutes du Danemark

- En partenariat avec les services danois
- Et aurait ciblé, entre autre, des politiques allemand dont Angela MERKEL

  https://www.lemonde.fr/pixels/article/2021/05/30/comment-des-dirigeants-europeens-ont-ete-espionnes-par-la-nsa-depuis-le-danemark_6082102_4408996.html

Divers / Trolls velus

WIP

WANTED : Zerodium souhaite acquérir des 0-Day sur le logiciel Pidgin

- Plébiscité par les groupes d'attaquants

  https://therecord.media/zerodium-acquiring-zero-days-in-pidgin-an-im-client-popular-with-cybercriminals/

Découverte d'une campagne en cours du malware WastedLoader ciblant Internet Explorer

- C'est dans les vieux navigateurs qu'on sort les meilleurs pwn?

  https://labs.bitdefender.com/2021/05/new-wastedloader-campaign-delivered-through-rig-exploit-kit/

  https://www.bitdefender.com/files/News/CaseStudies/study/397/Bitdefender-PR-Whitepaper-RIG-creat5362-en-EN.pdf

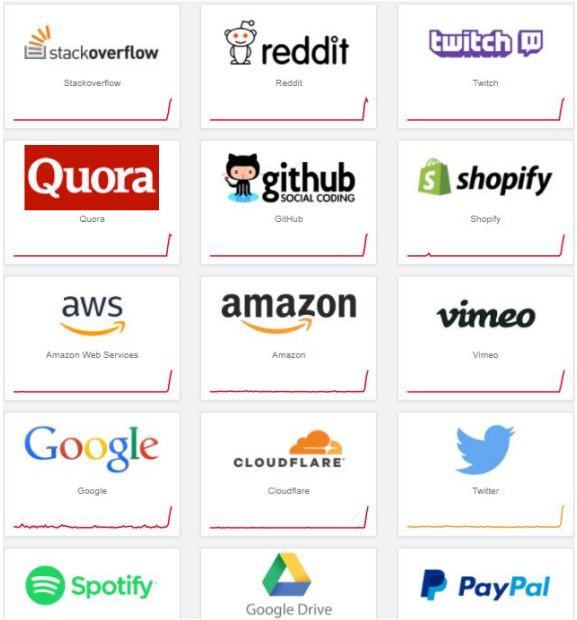
Breaking news ?

WIP

Le CDN Fastly a eu une “courte” panne

- Impacts en cascade
- Déjà de retour :)

https://apnews.com/article/ap-top-news-business-europe-technology-7c607c931faba19584975da74c8fa633



Divers / Trolls velus

WIP

Exagrid et Conti

- Avaient-ils leur solution de déployée ?

  https://twitter.com/hrbrmstr/status/1400386526614331393/photo/1

EXAGRID

ExaGrid Concludes 2020 with 7 Industry Award Wins and New Ransomware Recovery Solution

Exagrid pays $2.6m to Conti ransomware attackers

Backup appliance specialist hit by Conti ransomware in May with cyber criminals downloading employee and customer data, confidential contracts and source code

Divers / Trolls velus

WIP

Une belle démontration d'OSINT

- Lire tout le thread

  https://twitter.com/brechtcastel/status/1431612326759829513

Prochaines réunions

WIP

Prochaine réunion

- 12 octobre 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 ?