Revue d'actualité de l'OSSIR

9 février 2021

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

OSSIR

Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

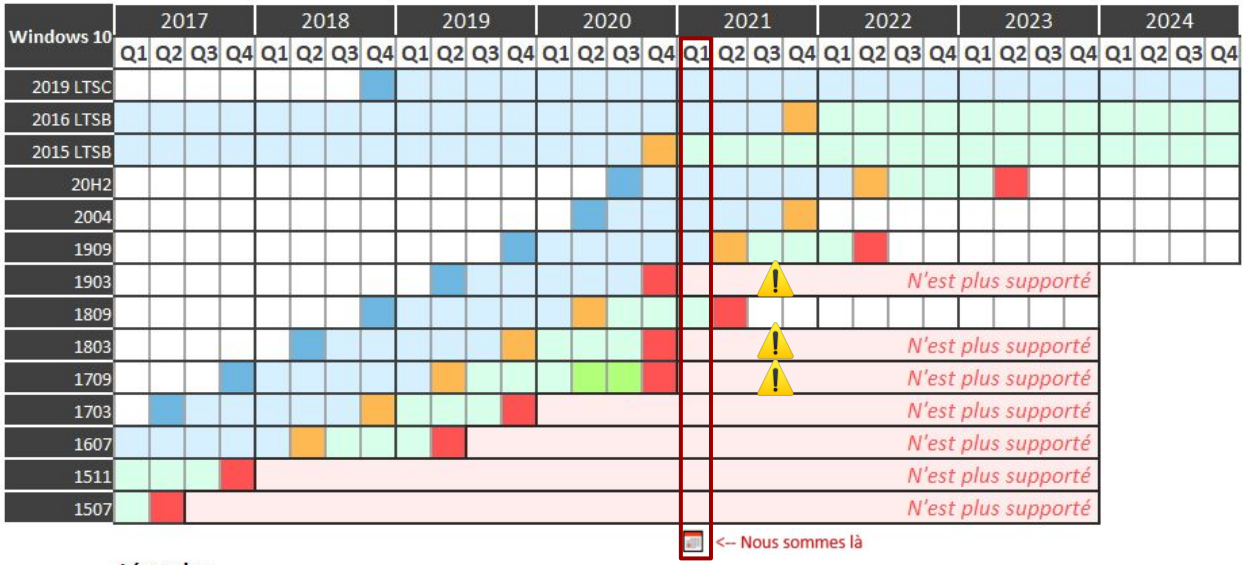
Report des fins de support de produits Microsoft suite au Covid-19

- 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 janvier :

- 83 vulnérabilités corrigées, dont 10 critiques

- A retenir :
  - CVE-2021-1647 : **<u>En cours d'exploitation</u>**

Composants impactés
Azure Functions
Microsoft .NET Framework
Microsoft Dynamics
Microsoft Exchange Server
Microsoft JET Database Engine
Microsoft Office
Microsoft Windows
Microsoft Windows Codecs Library
PowerShellGet
Visual Studio
Windows 10
Windows 10 (1607)
Windows 10 (1709)
Windows 10 (1803)
Windows 10 (1809)
Windows 10 (1903)
Windows 10 (1909)
Windows 10 (2004)
Windows 7
Windows 8.1
Windows Server 2008 R2
Windows Server 2008 SP2
Windows Server 2012

Failles / Bulletins / Advisories
Microsoft - Avis

Contrôle surprise : Avez-vous bien mis à jour vos systèmes contre ZeroLogon ? (CVE-2020-1472)

- Rappel : Correctif en 2 temps
- Août 2020 : Correctif en mode "passant"
- Février 2021: Correctif final en mode "bloquant"
- Vérifiez vos events IDs 5829 !

Failles / Bulletins / Advisories
CPU - Janvier 2021

Oracle

- 329 correctifs de sécurité ont été publiés pour 23 produits.
- 47 vulnérabilités sont jugées critiques (score CVSS supérieur ou égal à 9.8).
- Correctifs à installer en priorité (RCE à distance sans authentification) :
  - Oracle Fusion Middleware et ses dérivés
  - CVE-2021-1994
  - CVE-2021-2047
  - CVE-2021-2064
  - CVE-2021-2108
  - CVE-2021-2075
  - + patchs pour CVE-2020-14750 (bypass de la CVE-2020-14882)
- Détails techniques sur la CVE-2020-2109 (https://mp.weixin.qq.com/s/wX9TMXI1KVWwB_k6EZOklw)

https://www.oracle.com/security-alerts/cpujan2021.html

Produits impactés :

Oracle Communications Applications
Oracle Communications
Oracle Construction and Engineering
Oracle Database Server
Oracle E-Business Suite
Oracle Enterprise Manager
Oracle Financial Services Applications
Oracle Food and Beverage Applications
Oracle Fusion Middleware
Oracle GraalVM
Oracle Health Sciences Applications
Oracle Hyperion
Oracle Insurance Applications
Oracle Java SE 8
Oracle JD Edwards
Oracle MySQL
Oracle PeopleSoft
Oracle Retail Applications
Oracle Siebel CRM
Oracle Supply Chain
Oracle Systems
Oracle Utilities Applications
Oracle Virtualization

Failles / Bulletins / Advisories
Navigateurs (principales failles)

Prise de contrôle du système et manipulation de données via 6 vulnérabilités au sein de Google Chrome

- UaF dans le composant Payments
- V8

https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop.html

Prise de contrôle du système et contournement de sécurité via une vulnérabilité au sein de Microsoft Edge (2020-Jan)

- Corruption mémoire
- Exploitable via une page HTML

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV200002

Prise de contrôle du système et contournement de sécurité via 13 vulnérabilités au sein de Firefox

- Possibilité de faire du clickjacking

https://www.mozilla.org/en-US/security/advisories/mfsa2021-03/

https://www.mozilla.org/en-US/security/advisories/mfsa2021-04/

Failles / Bulletins / Advisories
Systèmes

(exploit) Élévation de privilèges via une vulnérabilité au sein de sudo (BaronSamedit)

- Mauvaise interprétation des flags par l'utilitaire sudoedit
  - Permet d'obtenir un shell root

https://www.exploit-db.com/exploits/49263

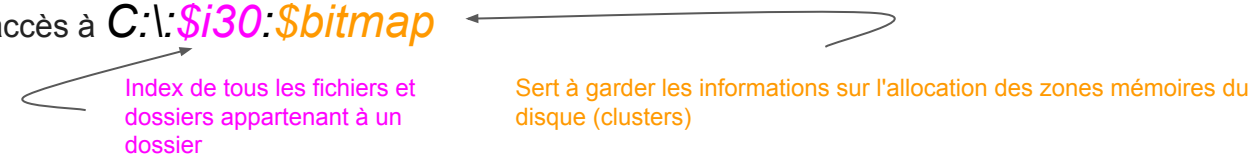
DNSpooq : Le retour de l'empoisonnement DNS

- Possibilité d'ajouter une entrée arbitraire au cache DNS

https://www.jsof-tech.com/disclosures/dnspooq/

Corrompre son disque NTFS (voire sa MFT) en une commande

- Erreur lors de l'accès à *C:\:$i30:$bitmap*



- Déclenchable via une page HTML ou un fichier spécifiquement conçu
- Le disque peut être sauvé via CHKDSK

Failles / Bulletins / Advisories
Systèmes de sécurité

Divulgation d'informations via une vulnérabilité au sein de libgcrypt

- Découvert par Tavis Ormandy de Google Project Zero
- Heap overflow lors du déchiffrement de données

https://lists.gnupg.org/pipermail/gnupg-announce/2021q1/000456.html

Fortinet FortiWeb, des vulnérabilités sans authentification… en 2021

- Une belle collection de failles “**sans authentification**” sur un équipement de sécurité
  - SQL Injection (CVE-2020-29015)
  - Buffer Overflow (CVE-2020-29016)
  - Buffer Overflow (CVE-2020-29019)
  - Format String (CVE-2020-29018)
  - XSS (CVE-2021-22122)

https://www.fortiguard.com/psirt?date=01-2021

https://www.fortiguard.com/psirt/FG-IR-20-122

Failles / Bulletins / Advisories
Réseau (principales failles)

Cisco

- RCE dans les interfaces web VPN Small Business
- Injection de commandes et BoF dans SD-WAN
- API DNA Center vulnérable à une injection de code

https://tools.cisco.com/security/center/Search.x?publicationTypeIDs=1&securityImpactRatings=critical&firstPublishedStartDate=2020%2F11%2F11&firstPublishedEndDate=2020%2F12%2F07&limit=100

- Produits vulnérables
  - Cisco Advanced malware protection
  - Cisco Advanced malware protection for endpoints
  - Cisco Anyconnect secure mobility client
  - Cisco Connected mobile experiences
  - Cisco Content security management appliance
  - Cisco Data center network manager
  - Cisco DNA center
  - Cisco Elastic services controller
  - Cisco Emergency responder
  - Cisco Enterprise NFV infrastructure software
  - Cisco Firepower management center
  - Cisco IOS XE
  - Cisco IOS XE SD-WAN
  - Cisco Jabber
  - Cisco RV016 multi-wan vpn router firmware
  - Cisco RV110w firmware
  - Cisco RV110w wireless-n vpn firewall firmware
  - Cisco SD-WAN firmware
  - Cisco SD-WAN vmanage
  - Cisco Smart Software manager on-prem
  - Cisco Smart Software manager satellite
  - Cisco Unified Communications Manager
  - Cisco Video Surveillance 8000p ip camera firmware
  - Cisco Web Security virtual appliance
  - Cisco Webex Meetings
  - Cisco Webex Teams

Failles / Bulletins / Advisories
Autre (principales failles)

Liferay 7.x, exécution de commande par désérialisation / CVE-2020-7961

- Problème de désérialisation

  https://www.synacktiv.com/publications/how-to-exploit-liferay-cve-2020-7961-quick-journey-to-poc.html

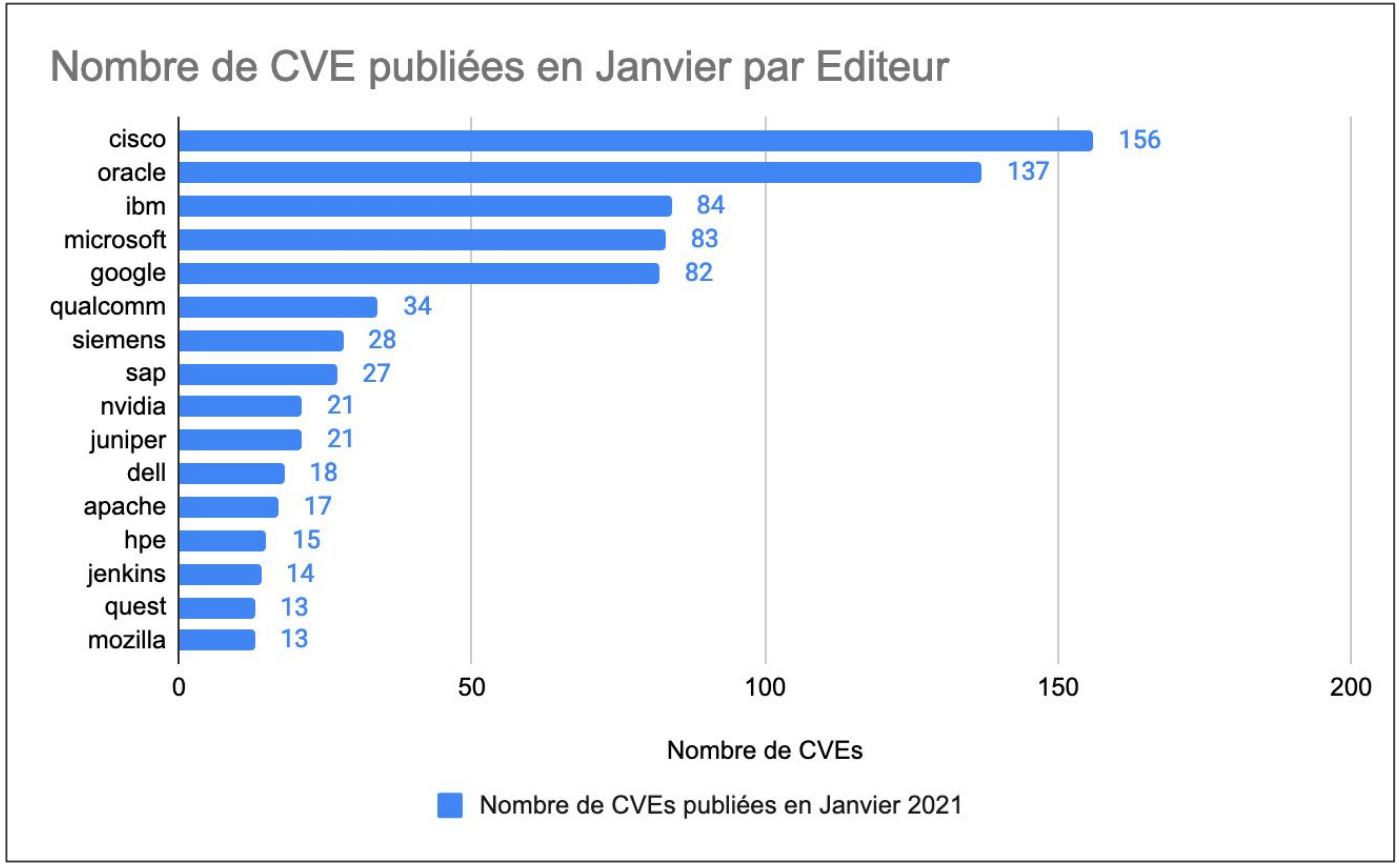
- Un autre PoC

  https://gist.github.com/pikpikcu/0b1cd516088f10577ec5973e595a377f

IBM Qradar, exécution de code par désérialisation / CVE-2020-4888

https://gist.github.com/testanull/e9ba06d0c0c403402f6941fe2dbb868a

Stats du mois de janvier !



Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Takedowns

Emotet

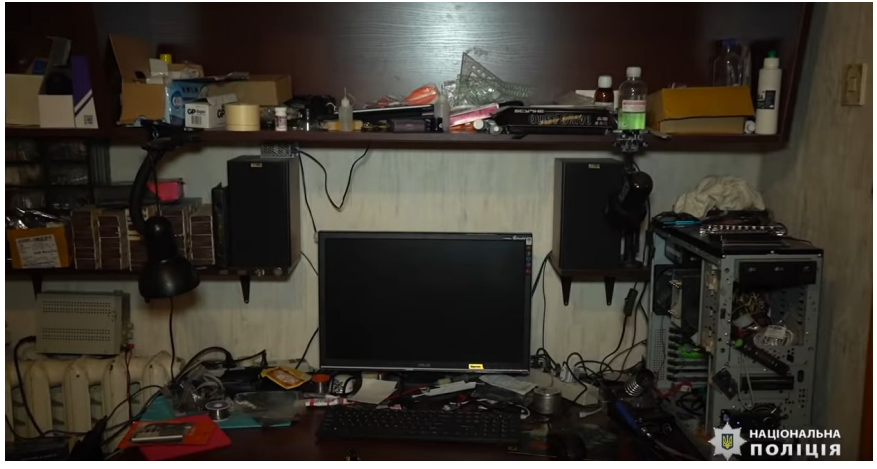
- Enquête de près de 2 ans par Europol et Eurojust
- Surtout un intermédiaire
- Ça ne signifie pas la fin définitive

  https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

  https://www.politie.nl/themas/controleer-of-mijn-inloggegevens-zijn-gestolen.html

- Vidéo de la perquisition… on dirait une parodie

  https://www.youtube.com/watch?v=_BLOmClsSpc



Piratages, Malwares, spam, fraudes et DDoS
Takedowns

Netwalker sous pression

- Takedown des sites de rançon
- Autorités bulgare et américaines

https://www.zdnet.com/article/us-and-bulgarian-authorities-dirsupt-netwalker-ransomware-operation/

Piratages, Malwares, spam, fraudes et DDoS
Ransomwares

Fonix arrête le rançonnage et fourni un outil pour déchiffrer

- Véritable arrêt ? Suite à Emotet ? Ou changement de nom ?

  https://twitter.com/fnx67482837

Ziggy aussi

- Base SQL avec les 922 clés de déchiffrement
- Décrypteur publié également

  https://www.bleepingcomputer.com/news/security/ziggy-ransomware-shuts-down-and-releases-victims-decryption-keys/

Ouest France se livre sur un ancien incident

- Heureusement des sauvegardes étaient disponibles

  https://www.ouest-france.fr/societe/cyberattaque/dans-les-coulisses-de-la-cyberattaque-vecue-a-ouest-france-7139874

Piratages, Malwares, spam, fraudes et DDoS
Malwares

Focus sur un malware en AppleScript

- Reverse engineering du code binaire AppleScript
- Utilisation du binaire Caffeinate
- Publication d'un outil pour décompiler ces codes

https://labs.sentinelone.com/fade-dead-adventures-in-reversing-malicious-run-only-applescripts/

STEELCORGI, un binaire tout-en-un tuxien

- bleach, suppression de logs ciblés
- SSHock, outil de bruteforce SSH
- Backfire, pour ouvrir des reverse shells
- Ricochet, sorte de scapy intégré

https://yoroi.company/research/opening-steelcorgi-a-sophisticated-apt-swiss-army-knife/

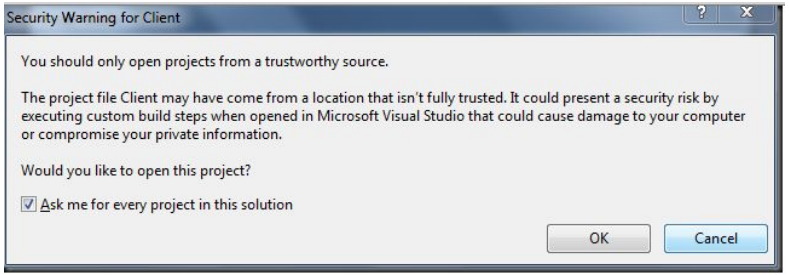
Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Une campagne d'espionnage ciblait des chercheurs en sécurité

- Analysé par le Google Threat Analysis Group (TAG)

  https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/

- Campagne complexe :
  - Créations de faux profils de chercheurs
  - Publication d'articles volés ou faux de 0days
  - Prise de contact avec des chercheurs et nombreux échanges
  - Envoi de projets Visual Studio piégés
  - Envoie d'URL de site pour du WaterHoling
    - Avec un 0-day Chrome ?
    - Et ce n'est pas la CVE-2021-21148 : https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_4.html



Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Une update sur SolarWinds

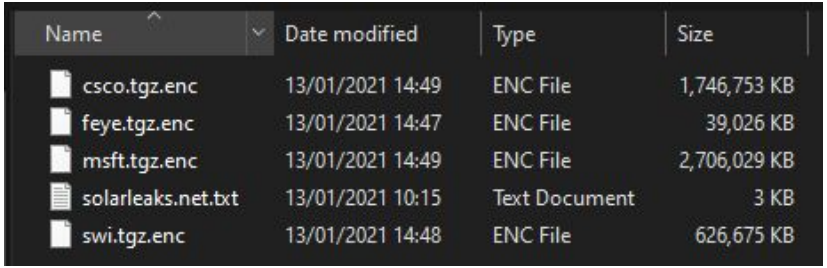
- Compromission de Qualys, MalwareBytes, Mime et Palo Alto

  https://www.sonicwall.com/support/product-notification/urgent-patch-available-for-sma-100-series-10-x-firmware-zero-day-vulnerability-updated-feb-3-2-p-m-cst/210122173415410/

- Publication “potentielle” d’une partie des données volées “à la ShadowBrokers”

  https://solarleaks.net

```
[...]
[Microsoft Windows (partial) source code and various Microsoft repositories]
price: 600,000 USD
data: msft.tgz.enc (2.6G)
link: https://mega.nz/file/1ehgSSpD#nrtzQwh-qyCaUHBXo2qQ1dNbWiyVHCvg8J0As8VjrX0

[Cisco multiple products source code + internal bugtracker dump]
price: 500,000 USD
data: csco.tgz.enc (1.7G)
link: https://mega.nz/file/sSgQmJLT#NqaaYXsFkASwAc51lcjBnWjP4zrbqiN-XQ7GVZGbL_o

[SolarWinds products source code (all including Orion) + customer portal dump]
price: 250,000 USD
data: swi.tgz.enc (612M)
link: https://mega.nz/file/xawhBQgJ#f3X6lPORF16wh-O9GiNVMVDZ6rxRKX64_XVR5y9KpFM

[FireEye private redteam tools, source code, binaries and documentation]
price: 50,000 USD
data: feye.tgz.enc (39M)
link: https://mega.nz/file/hOBnVYjL#l3qojAvaFWtYtcB3vX4ZABG3tBLGyhJarBBbYaHnM-0

[More to come in the next weeks]

ALL LEAKED DATA FOR 1,000,000 USD (+ bonus)
[...]
```



Name	Date modified	Type	Size
csco.tgz.enc	13/01/2021 14:49	ENC File	1,746,753 KB
feye.tgz.enc	13/01/2021 14:47	ENC File	39,026 KB
msft.tgz.enc	13/01/2021 14:49	ENC File	2,706,029 KB
solarleaks.net.txt	13/01/2021 10:15	Text Document	3 KB
swi.tgz.enc	13/01/2021 14:48	ENC File	626,675 KB

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Une update sur SolarWinds - suite

- Publication … sur un site non durci et avec mod-status actif 🤦 🤦 🤦

Apache Server Status for 5bpasg2kotxllmzsv6swwydbojnfuvfb7d6363pwe5wrzhjyn2ptvdqd.onion (via 127.0.0.1)

Server Version: Apache/2.4.38 (Debian)
Server MPM: event
Server Built: 2020-08-25T20:08:29

Current Time: Tuesday, 12-Jan-2021 17:07:41 UTC
Restart Time: Tuesday, 12-Jan-2021 13:00:45 UTC
Parent Server Config. Generation: 1
Parent Server MPM Generation: 0
Server uptime: 4 hours 6 minutes 55 seconds
Server load: 0.06 0.07 0.07
Total accesses: 44 - Total Traffic: 51 kB - Total Duration: 8981
CPU Usage: u.45 s.92 cu0 cs0 - .00925% CPU load
.00297 requests/sec - 3 B/second - 1186 B/request - 204.114 ms/request
1 requests currently being processed, 49 idle workers

Slot	PID	Stopping	Connections		Threads		Async connections		
			total	accepting	busy	idle	writing	keep-alive	closing
0	3358	no	0	yes	1	24	0	0	0
1	3359	no	0	yes	0	25	0	0	0
Sum	2	0	0		1	49	0	0	0

_____W_____.....
.....
.....

Scoreboard Key:
"_" Waiting for Connection, "S" Starting up, "R" Reading Request,
"W" Sending Reply, "K" Keepalive (read), "D" DNS Lookup,
"C" Closing connection, "L" Logging, "G" Gracefully finishing,
"I" Idle cleanup of worker, "." Open slot with no current process

Srv	PID	Acc	M	CPU	SS	Req	Dur	Conn	Child	Slot	Client	Protocol	VHost	Request
0-0	3358	0/1/1	_	0.00	14812	0	0	0.0	0.00	0.00		http/1.1	127.0.1.1:80	GET / HTTP/1.1
0-0	3358	0/1/1	_	0.00	14439	0	0	0.0	0.00	0.00		http/1.1	127.0.1.1:80	GET / HTTP/1.1
0-0	3358	0/1/1	_	0.00	14438	0	0	0.0	0.00	0.00		http/1.1	127.0.1.1:80	GET /favicon.ico HTTP/1.1

0-0	3358	0/1/1	_	0.00	6018	0	0	0.0	0.00	0.00		http/1.1	127.0.1.1:80	GET /wp-login.php HTTP/1.1
0-0	3358	0/1/1	_	0.00	6018	0	0	0.0	0.00	0.00		http/1.1	127.0.1.1:80	GET /phpmyadmin/index.php HTTP/1.1
0-0	3358	0/1/1	_	0.01	4940	2	2	0.0	0.00	0.00		http/1.1	127.0.1.1:80	GET / HTTP/1.1
0-0	3358	0/1/1	_	0.01	4939	0	0	0.0	0.00	0.00		http/1.1	127.0.1.1:80	GET /favicon.ico HTTP/1.1
0-0	3358	0/0/0	W	0.00	0	0	0	0.0	0.00	0.00		http/1.1	127.0.1.1:80	GET /server-status HTTP/1.1
1-0	3359	0/4/4	_	0.34	799	0	3	0.0	0.00	0.00		http/1.1	127.0.1.1:80	GET / HTTP/1.1
1-0	3359	0/1/1	_	0.30	797	0	0	0.0	0.00	0.00		http/1.1		
1-0	3359	0/2/2	_	0.34	771	0	111	0.0	0.00	0.00		http/1.1	127.0.1.1:80	GET / HTTP/1.1
1-0	3359	0/2/2	_	0.34	771	0	1	0.0	0.00	0.00		http/1.1	127.0.1.1:80	GET /favicon.ico HTTP/1.1
1-0	3359	0/1/1	_	0.33	765	1	8832	0.0	0.00	0.00		http/1.1	127.0.1.1:80	GET / HTTP/1.1
1-0	3359	0/2/2	_	0.33	2395	0	0	0.0	0.00	0.00		http/1.1	127.0.1.1:80	GET /favicon.ico HTTP/1.1
1-0	3359	0/1/1	_	0.29	2394	0	0	0.0	0.00	0.00		http/1.1		
1-0	3359	0/3/3	_	0.34	1869	0	1	0.0	0.00	0.00		http/1.1	127.0.1.1:80	GET / HTTP/1.1
1-0	3359	0/1/1	_	0.33	2360	0	0	0.0	0.00	0.00		http/1.1	127.0.1.1:80	GET / HTTP/1.1
1-0	3359	0/1/1	_	0.29	2376	0	0	0.0	0.00	0.00		http/1.1		
1-0	3359	0/1/1	_	0.31	2355	0	0	0.0	0.00	0.00		http/1.1	127.0.1.1:80	GET / HTTP/1.1
1-0	3359	0/1/1	_	0.32	1872	1	1	0.0	0.00	0.00		http/1.1	127.0.1.1:80	GET / HTTP/1.1
1-0	3359	0/2/2	_	0.33	2378	0	1	0.0	0.00	0.00		http/1.1	127.0.1.1:80	GET / HTTP/1.1
1-0	3359	0/2/2	_	0.34	964	1	1	0.0	0.00	0.00		http/1.1	127.0.1.1:80	GET / HTTP/1.1
1-0	3359	0/2/2	_	0.31	2355	0	0	0.0	0.00	0.00		http/1.1	127.0.1.1:80	GET /favicon.ico HTTP/1.1
1-0	3359	0/1/1	_	0.30	766	0	0	0.0	0.00	0.00		http/1.1		
1-0	3359	0/2/2	_	0.34	963	0	3	0.0	0.00	0.00		http/1.1	127.0.1.1:80	GET /favicon.ico HTTP/1.1
1-0	3359	0/2/2	_	0.30	2397	1	9	0.0	0.00	0.00		http/1.1		
1-0	3359	0/1/1	_	0.30	2377	1	1	0.0	0.00	0.00		http/1.1		
1-0	3359	0/2/2	_	0.33	2376	0	0	0.0	0.00	0.00		http/1.1	127.0.1.1:80	GET /favicon.ico HTTP/1.1
1-0	3359	0/1/1	_	0.33	1877	1	1	0.0	0.00	0.00		http/1.1	127.0.1.1:80	GET / HTTP/1.1
1-0	3359	0/1/1	_	0.29	958	0	0	0.0	0.00	0.00		http/1.1	127.0.1.1:80	GET /pma/index.php HTTP/1.1
1-0	3359	0/1/1	_	0.29	1872	0	0	0.0	0.00	0.00		http/1.1	127.0.1.1:80	GET /config/getuser?index=0 HTTP/1.1

Srv Child Server number - generation
PID OS process ID
Acc Number of accesses this connection / this child / this slot
M Mode of operation
CPU CPU usage, number of seconds
SS Seconds since beginning of most recent request

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Sonicwall

- Découverte d'une attaque le 22/01/2021 via l'exploitation d'une 0-Day sur leurs appliances VPN SMA-100
- Patch sorti le 3/02/2021
- Le processus de communication était propre 👏

https://www.sonicwall.com/support/product-notification/urgent-patch-available-for-sma-100-series-10-x-firmware-zero-day-vulnerability-updated-feb-3-2-p-m-cst/210122173415410/

Stormshield : Double peine

- Accès illégitime à des informations stockés dans un portail de support technique
- Vol du code source des produits SNS et SNI
    - Résultat : L'ANSSI met sous observation les qualifications et agréments des dits produits

https://www.stormshield.com/fr/incident-de-securite-stormshield/

https://www.ssi.gouv.fr/actualite/incident-de-securite-chez-stormshield/

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Une station d'épuration de Floride a été compromise

- L'attaquant a essayé de changer le taux d'hydroxyde de sodium dans l'eau
- Heureusement, un opérateur a réussi à reprendre la main
- La différence entre la sécurité et la sûreté

https://www.reuters.com/article/us-usa-cyber-florida/hackers-broke-into-florida-towns-water-treatment-plant-attempted-to-poison-supply-sheriff-says-idUSKBN2A82FV

Piratages, Malwares, spam, fraudes et DDoS
Publication

PatrowlHears

- Plateforme de consolidation d'informations sur les vulnérabilités

  https://makyotox.medium.com/patrowlhears-open-source-vulnerability-intelligence-center-a8577c462257

  https://github.com/Patrowl/PatrowlHears

ANSSI et le GIP ACYMA publient une liste de recommandations concernant la sécurisation du télétravail

- Systématiser l'utilisation de VPN
- Superviser et journaliser l'activité sur le S.I.
- Mettre en place des sauvegardes et les tester
- Restreindre les accès externes
- Sensibiliser les collaborateurs

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/securisation-du-teletravail.

Le code source du moteur ESE est publié en open source

- Sous licence MIT !
- Format utilisé pour stocker les DB Exchange notamment

https://github.com/microsoft/Extensible-Storage-Engine

Cobalt a encore de beaux jours devant lui : Un générateur de shellcode Cobalt

- Possibilité de le chiffrer (via AES)
- Possibilité d'adapter la sortie

https://www.kitploit.com/2021/01/cssg-cobalt-strike-shellcode-generator.html

Vous aussi vous voulez décompiler du malware AppleScript ?

https://github.com/SentineLabs/aevt_decompile

Business et Politique

Business
Monde

Rapid7 rachète la start-up Alcide pour sécuriser les environnements Kubernetes

- 50M$

https://www.lemondeinformatique.fr/actualites/lire-rapid7-rachete-la-start-up-alcide-pour-securiser-les-environnements-kubernetes-81831.html

Droit / Politique
RGPD

171 M€ d'amendes en Europe sur le RGPD

https://finbold.com/gdpr-fines-2020/

EU countries ranked by total GDPR fine amount in 2020:

Rank	Country	Total fine per country in EUR	Number of fines
1	Italy	€58,161,601	34
2	United Kingdom	€43,901,000	3
3	Germany	€37,398,708	3
4	Sweden	€14,278,800	15
5	Spain	€8,021,210	128
6	France	€3,309,000	5
7	Netherlands	€2,080,000	3
8	Norway	€1,050,800	11
9	Belgium	€793,000	13
10	Ireland	€630,000	4

https://www.enforcementtracker.com/

Droit / Politique
RGPD

Big Brüder ist beobachten dich

- Surveillance vidéo non-stop sans fondement juridique
- 10 millions d'amende
  https://www.zdnet.com/article/gdpr-german-laptop-retailer-fined-eur10-4m-for-video-monitoring-employees/

Compromis par credential stuffing la CNIL sanctionne !

- 150 k€ pour le site d'e-commerce et 75k pour son sous-traitant
- Pas de mesure pour se protéger contre les attaques par bruteforce
- Le manque d'action est surtout condamné
- (Certains veulent les noms 👀)
  https://www.cnil.fr/fr/credential-stuffing-la-cnil-sanctionne-un-responsable-de-traitement-et-son-sous-traitant

Droit / Politique
France

Vendre sur le “darknet” les données auxquelles on a accès, c’est mal

- Un haut responsable de CDiscount à tenté de vendre 33m de données

  https://www.rtl.fr/actu/justice-faits-divers/cdiscount-un-cadre-du-site-mis-en-examen-pour-vol-de-donnees-7900000429

- Un brigadier “anti-terro” vend des données venant des interceptions légales

  https://www.lavoixdunord.fr/898936/article/2020-11-26/haurus-l-ex-agent-de-la-dgsi-soupconne-d-avoir-vendu-des-infos-sur-le-darknet

  https://www.nextinpact.com/article/45487/haurus-nous-repond-alors-je-dis-aux-avocats-osez-analyser-donnees

Droit / Politique
France

Fichiers de renseignements élargis : le Gouvernement obtient l'aval du Conseil d'Etat

- « opinions politiques »
- « convictions philosophiques et religieuses »
- « appartenance syndicale »
- Avis de la CNIL uniquement consultatif

https://www.lemondeinformatique.fr/actualites/lire-fichiers-de-renseignements-elargis-le-gouvernement-obtient-l-aval-du-conseil-d-etat-81537.html

https://www.nextinpact.com/article/45210/fichiers-policiers-cnil-en-porte-a-faux

Conférences

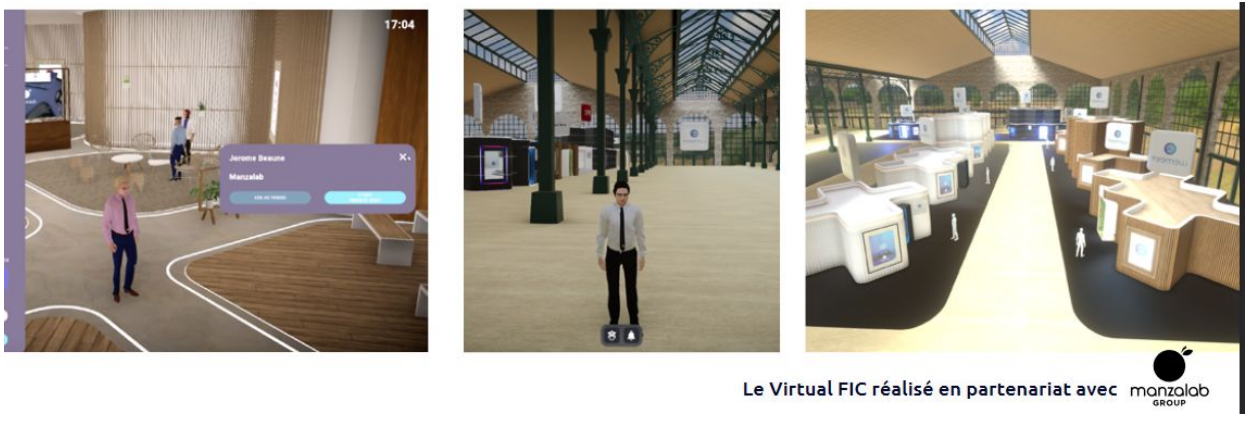
Conférences

Passée

- GreHack - en ligne, en novembre 2020 https://www.youtube.com/channel/UCXpdxLSDlJmgphPCRK9kR_Q
- Botconf - en ligne, en décembre 2020 https://www.botconf.eu/botconf-2020/schedule/

A venir

- FIC - Reporté en avril 2021 - présentiel et en virtuel, version “Second Life”

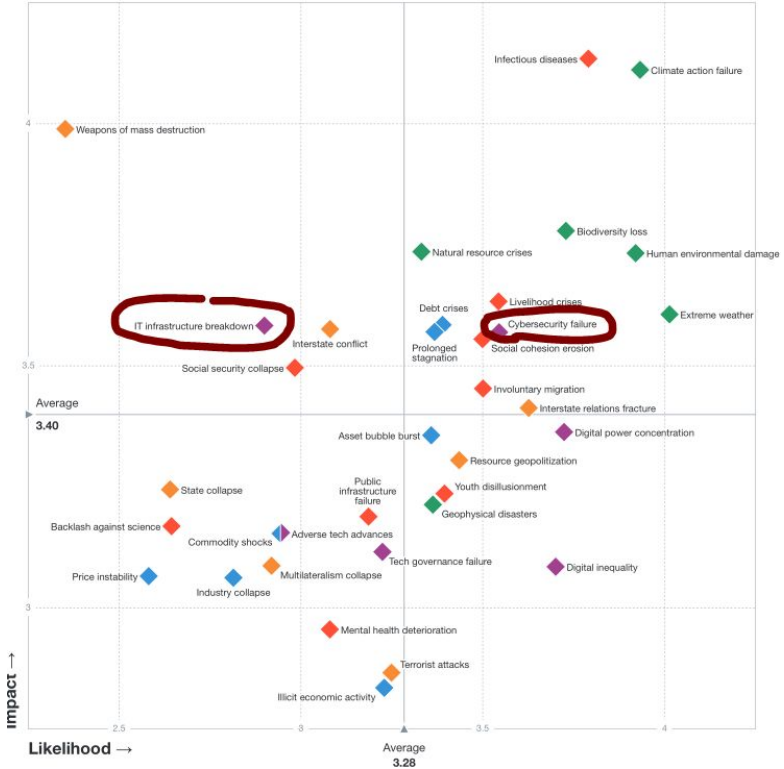


Divers / Trolls velus

Divers / Trolls velus

Le risque cyber selon le "forum de Davos"

- En plus du forum, la fondation publie son rapport annuel des risques
  http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf



Divers / Trolls velus

Le CERT de Corée du Nord sur Twitter !!?

- Très vraisemblablement un fake

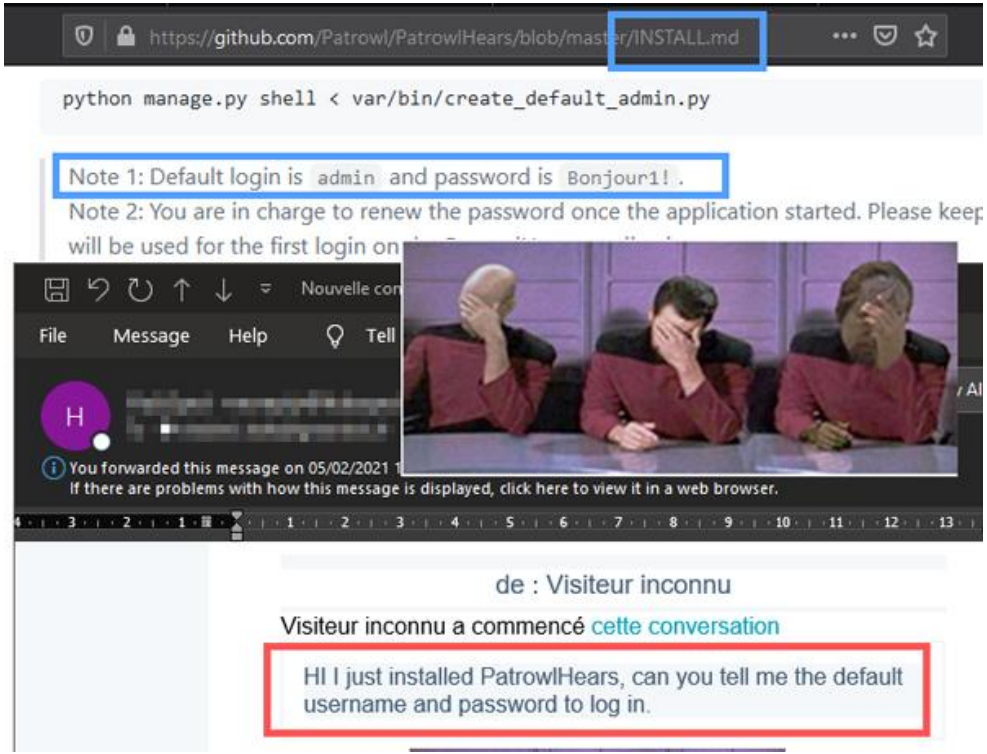
  https://twitter.com/dprkcert

Whatsapp change ses conditions d'utilisation

- cf. revue de janvier 2021
- Passage massif à Signal
- En quelques jours, l'action de Signal passe de $4 à plus de $41
- Signal Advance, Inc. (SIGL), aucun rapport avec l'application Signal

Divers / Trolls velus

Quand tu publies de l'Open Source...



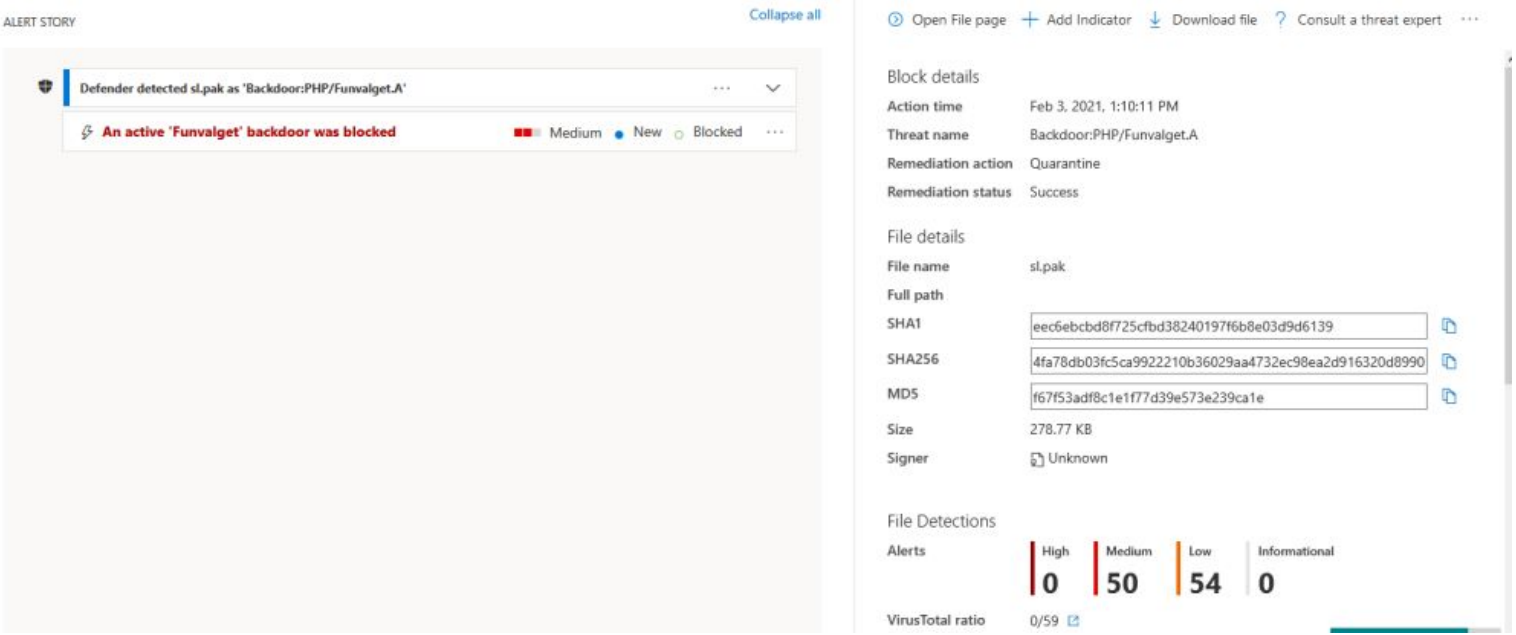
Divers / Trolls velus
Les perles de la presse

Iran's centrifuges. That attack, known as Stuxnet, spread using seven holes, known as "zero days," in Microsoft and Siemens industrial software. (Only one had been previously disclosed, but

In modern warfare, "active defense" amounts to hacking enemy networks. It's mutually assured destruction for the digital age: V

Divers / Trolls velus

Un antivirus pas nickel Chrome



https://www.zdnet.com/article/microsoft-defender-atp-is-detecting-yesterdays-chrome-update-as-a-backdoor/

Divers / Trolls velus

2 enfants parviennent à contourner le screensaver Linux MINT

- Ouvrir le clavier virtuel Cinnamon
- Appuyer sur la touche "ē"
- Le verrouilleur d'écran plante et donne accès à la session

https://blog.koddos.net/vulnerability-in-linux-mint-screensaver-lock-discovered-by-two-kids/

Prochains rendez-vous de l’OSSIR

Prochaines réunions

Prochaine réunion

- 9 Mars 2021… toujours en visio

After Work

- Pas avant Q2 2021 ?

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?