Revue d'actualité de l'OSSIR

12 décembre 2023

Jérémy De Cock
Christophe Chasseboeuf
Vladimir Kolla

OSSIR

Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Bulletin de novembre, 58 vulnérabilités patchées dont

- **5** 0-day :
  - [**CVE-2023-36036**] Elévation de privilèges - Pilote “Cloud Files Mini Filter”
    - Affecte toutes les versions de Windows et Windows Server
  - [**CVE-2023-36033**] Elévation de privilèges - Librairie “DWM Core”
    - Affecte toutes les versions de Windows et Windows Server
  - [**CVE-2023-36025**] Bypass de SmartScreen
    - Possible à distance via un shortcut Internet malveillant
    - PoC : https://github.com/ka7ana/CVE-2023-36025
  - [**CVE-2023-36413**] Bypass du “Mode Protégé” afin d’ouvrir directement le document en mode édition
    - Affecte Office 2016, Office 2019, Office 2021 ainsi que les versions Microsoft 365 Apps
  - [**CVE-2023-36038**] DoS - ASP.NET Core
    - Affecte .NET 8.0, ASP.NET Core 8.0, ainsi que Visual Studio 2022
- Et d’autres **critiques** :
  - [**CVE-2023-36052**] RCE - Journaux d’activités d’Entra ID
  - [**CVE-2023-36400**] RCE - Méthode de dérivation de clés HMAC d’Hyper-V
  - [**CVE-2023-36397**] RCE - Pragmatic General Multicast (PGM)

https://www.it-connect.fr/patch-tuesday-novembre-2023-58-failles-de-securite-et-5-zero-day-corrigees/

Failles / Bulletins / Advisories
Microsoft - Divers

Bug sous Windows : HP Smart

- 3 actions liées à ce bug :
  - L'application HP Smart s'installe toute seule
  - Toutes les imprimantes sont renommées en "HP LaserJet M101-M106"
  - "Aucune tâche n'est disponible pour cette page" apparaît quand on double-clic sur l'imprimante
- Affecte uniquement les machines ayant accès au Store de Microsoft
- Impression toujours fonctionnelle
- Investigation en cours par Microsoft
- Affecte les machines :
  - Windows 10 >= 1809
  - Windows 11 >= 21H2
  - Windows Server >= 2012

https://answers.microsoft.com/en-us/windows/forum/all/why-all-my-printer-model-converted-to-hp-laserjet/1b39d3c1-199e-4a5f-987f-729401d7e8f5 (discussion sur le sujet)

Failles / Bulletins / Advisories
Microsoft - Divers

Contournement du lecteur d'empreinte (#WindowsHello)

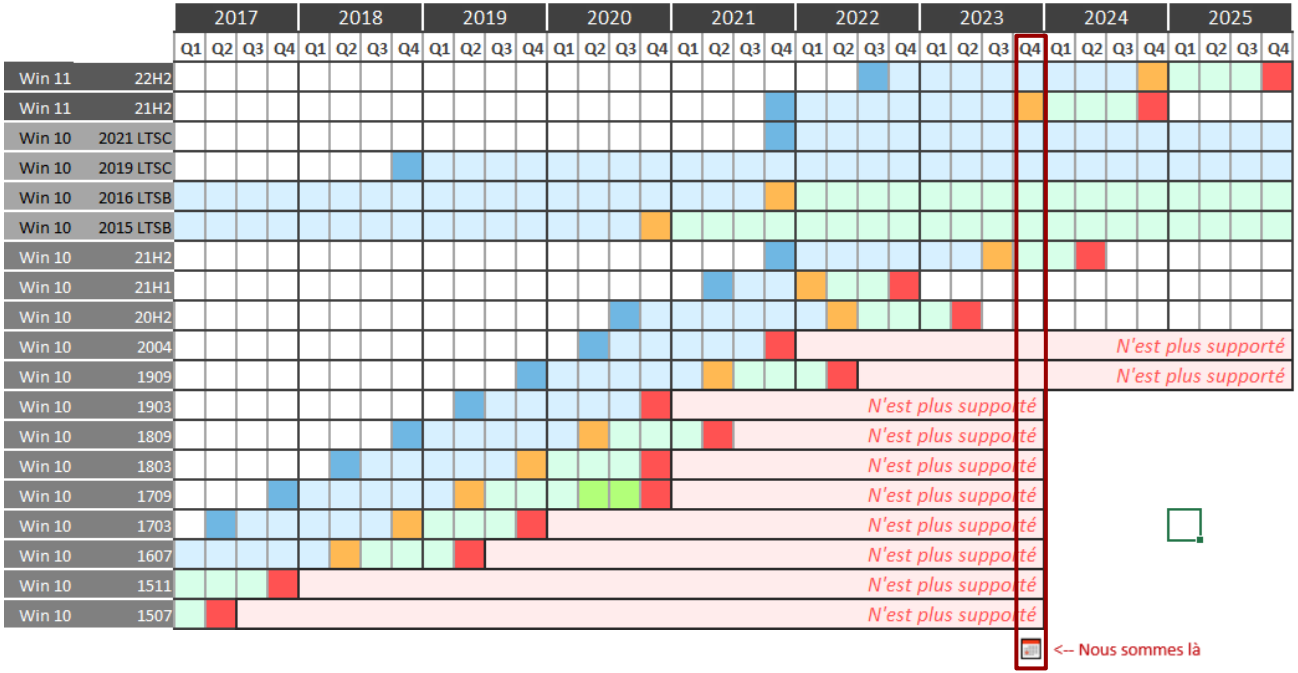
- Capteur de type "Match-on-Chip" impacté
  - Dispose de son propre microprocesseur et de sa propre mémoire
  - Modèles disposant de ce capteur :
    - Dell Inspiron 15 - lecteur d'empreinte de chez **ELAN**
    - Lenovo ThinkPad T14 - lecteur d'empreinte de chez **Synaptics**
    - Microsoft Surface Pro X - lecteur d'empreinte de chez **Goodix**
- Elan n'implémente pas le protocole SDCP (#Microsoft) = identifiants transmis en clair
- Synaptics l'implémente mais le désactive par défaut = stack TLS vulnérable utilisée
- Goodix est ok via SDCP mais …
  - Possible d'envoyer un paquet non authentifié au capteur pour lui définir une autre BDD à utiliser

https://www.it-connect.fr/lauthentification-windows-hello-contournee-sur-des-ordinateurs-dell-lenovo-et-microsoft/

https://github.com/microsoft/SecureDeviceConnectionProtocol (protocole SDCP)

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Rappel du support Windows 10 en couleurs



Sortie	Home, Pro	Entreprise
mardi 20 septembre 2022	mardi 8 octobre 2024	mardi 14 octobre 2025
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

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
Google

Bulletin de décembre, 85 vulnérabilités patchées dont

- 1 **très critique** :
  - [**CVE-2023-40088**] 0-click permettant une **RCE unauthenticated**
    - Provoqué par un use after free dans *com_android_bluetooth_AdapterServer.cpp*
    - Affecte Android 11, 12, 12L, 13 et 14
- 4 **critiques** :
  - [**CVE-2023-40077**] **Elévation de privilèges** provoquée via une Race Condition dans *MetaDataBase.cpp*
  - [**CVE-2023-40076**] **Leak d'informations** provoqué par un manque de contrôle dans *CredentialManagerUI.java*
  - [**CVE-2023-45866**] **Contournement de l'authentification Bluetooth** via des requêtes spécialement forgées
  - [**CVE-2022-40507**] **XEE** dans le composant Qualcomm

https://www.malwarebytes.com/blog/news/2023/12/android-phones-can-be-taken-over-remotely-update-when-you-can

Failles / Bulletins / Advisories
Apple

Bulletin de décembre, 2 vulnérabilités 0-day patchées

- Présentent dans le moteur de rendu de pages Web “WebKit”
- [**CVE-2023-42916**] Out-of-bounds permettant un leak d’informations
- [**CVE-2023-42917**] Corruption de la mémoire permettant une RCE
- Affectent IPhone, IPad & macOS alors → UPDATEZ
  - iOS 17.1.2
  - iPadOS 17.1.2
  - macOS Sonoma 14.1.2
  - Safari 17.1.2

https://www.bleepingcomputer.com/news/apple/apple-fixes-two-new-ios-zero-days-in-emergency-updates/

Failles / Bulletins / Advisories
Systèmes

LogoFAIL

- Présentée par Binarly lors de la BlackHat Europe 2023
- Affecte l'UEFI de toutes les puces x86 et ARM
  - Windows, Linux, tout le monde y passe
  - Bypass Intel Boot Guard
- Permet le déploiement d'un bootkit via la bibliothèque d'images du firmware
  - Cette dernière permet d'afficher les logs lors du processus de démarrage
  - Accès complet au disque et à la mémoire

https://arstechnica.com/security/2023/12/just-about-every-windows-and-linux-device-vulnerable-to-new-logofail-firmware-attack/

RCE sur FortSIEM (CVE-2023-36553)

- Mauvaise gestion des données envoyées en entrée à l'API
  - Improper neutralization
- RCE unauthenticated
- Toutes les versions comprises entre 4.7 et 5.4 sont vulnérables

https://www.bleepingcomputer.com/news/security/fortinet-warns-of-critical-command-injection-bug-in-fortisiem/

Failles / Bulletins / Advisories
Navigateurs (principales failles)

0-day sur Chrome

- CVE-2023-6345 exploitée dans la nature
- Integer overflow se trouvant dans Skia (bibliothèque d'images vectorielles en 2D)
  - Skia est également utilisée sur Mozilla Firefox
  - Permet d'avoir une RCE
- Mettez à jour Chrome :
  - Windows : 119.0.6045.199/.200
  - macOS & Linux : 119.0.6045.199

https://www.bleepingcomputer.com/news/security/google-chrome-emergency-update-fixes-6th-zero-day-exploited-in-2023/

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

Authentification forcée via Access

- Utilisation d'un fichier Microsoft Access (mécanisme OLE)
- Relayer l'authentification NTLM vers un serveur externe
  - Sur n'importe quel port ! 🐷
  - But ? Récupérer le hash NTLM et le casser en local
- Fonctionne sur toutes les versions d'Office
  - Patch disponible : version **2306**, build **16529.20182**

https://www.it-connect.fr/authentification-windows-cette-technique-basee-sur-microsoft-access-permet-de-voler-les-tokens-ntlm/

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

Multiples vulnérabilités critiques sur ownCloud

- + de 200 000 installations dans le monde
- [**CVE-2023-49103**] Leak les fichiers de configuration du serveur - Bibliothèque “graphapi”
  - Allant jusqu’au leak du mot de passe administrateur…
  - Recommandé de supprimer le fichier *owncloud/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php*
- [**CVE-2023-49103**] LFI unauthenticated sur les versions entre 10.6.0 et 10.13.0
  - Nécessite le nom d’un utilisateur existant
    - N’ayant pas configuré de clé de signature (cas par défaut)
- [**CVE-2023-49103**] Détournement de Oauth2 pour rediriger la cible

https://www.it-connect.fr/faille-securite-critique-owncloud-expose-mot-de-passe-admin/

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

Multiples vulnérabilités critiques sur OpenVPN

- [**CVE-2023-46849**] DoS causé par une “divide by zero”
  - Lié au paramètre de configuration “--fragment”
- [**CVE-2023-46850**] RCE causée par un “use after free”
  - Impacte toutes les installations où TLS est utilisé
- Les versions suivantes sont vulnérables :
  - 2.11.0 ≤ ≥ 2.11.3
  - 2.12.0 ≤ ≥ 2.12.1

https://www.it-connect.fr/multiple-vulnerabilites-dans-openvpn-deni-de-service-et-execution-de-code-a-distance-au-programme/

Failles / Bulletins / Advisories
Réseau (principales failles)

Attaques via le Bluetooth

- BLUFFS : **Blu**etooth **F**orward and **F**uture **S**ecrecy Attacks and Defenses
  - 6 attaques pouvant casser la sécurité des sessions Bluetooth
  - CVE-2023-24023
  - Affecte toutes les versions du Bluetooth de la 4.2 à la 5.4
- Modifications proposées par Eurecom pour atténuer ces attaques
  - Améliorer la fonction de dérivation des clés de sessions
  - Rejeter les connexions dont la force de la clé < 7 octets
  - Utiliser un chiffrement plus robuste

https://francozappa.github.io/post/2023/bluffs-ccs23/ (papier + slides + toolkit)

Failles / Bulletins / Advisories
Smartphones (principales failles)

Bypass de l'écran de verrouillage d'Android ?

- Oui mais c'est pas ce que vous pensez
  - À partir d'un lien Google Maps, vous pouvez leak des infos
- En n'ayant **pas** le mode conducteur **activé**
  - Accès aux emplacements récents et favoris et aux contacts
  - Possibilité de partager l'emplacement en temps réel avec les contacts ou avec un mail
- En ayant le mode conducteur **activé**
  - Comme avant ! Plus …
  - Accès aux photos de l'appareil (possibilité de les publier)
  - Accès au compte Google
- Affecte Android 13 et 14

https://securityaffairs.com/155588/hacking/android-14-13-lock-screen-bypass.html

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Malware

Nouvelle feature du côté de Lumma

- Info-stealer russe (MaaS) en service depuis août 2022
- Nouvelle feature disponible : restaurer les cookies Google expirés
  - `<< en utilisant une clé à partir des fichiers de restauration >>`
  - Ne s'applique qu'aux cookies Google, sans plus de détails
  - Cookie restauré = compromission du compte Google
- Fonctionnalité également présent chez "Rhadamanthys" (copie)
- Aucun moyen de s'en protéger…

https://www.it-connect.fr/compromission-de-comptes-google-le-malware-lumma-serait-capable-de-restaurer-les-cookies-expires/

https://malpedia.caad.fkie.fraunhofer.de/details/win.lumma (infos sur le malware)

Piratages, Malwares, spam, fraudes et DDoS
Malware

Malware Atomic Stealer sur macOS

- Info-stealer (MaaS) en service depuis avril 2023
- Déploiement via une fausse chaîne de mise à jour de Safari (#ClearFake)
  - ClearFake s'appuie sur des sites WP compromis
  - Fournie un DMG malveillant
- Siphone les données dans les navigateurs, dans les wallets, etc.

https://thehackernews.com/2023/11/clearfake-campaign-expands-to-deliver.html

https://malpedia.caad.fkie.fraunhofer.de/details/osx.amos (infos sur le malware)

Piratages, Malwares, spam, fraudes et DDoS
Ransomwares

Après Nevada en mars, Qilin

- Cible les serveurs VMware ESXI
  - Chiffre les machines virtuelles et détruit les snapshots
- Ransomware modulable
  - Mode débogage
  - Mode “simulation” pour tester le chiffrement sans altérer les fichiers
  - Extension définissable, etc.
- S’adapte à l’environnement détecté

```
for I in $(esxcli storage filesystem list |grep 'VMFS-5' |awk '{print $1}'); do vmkfstools -c
10M -d eagerzeroedthick $I/eztDisk > /dev/null; vmkfstools -U $I/eztDisk > /dev/null; done
for I in $(esxcli storage filesystem list |grep 'VMFS-5' |awk '{print $1}'); do vmkfstools -c
10M -d eagerzeroedthick $I/eztDisk; vmkfstools -U $I/eztDisk; done
for I in $(esxcli storage filesystem list |grep 'VMFS-6' |awk '{print $1}'); do vmkfstools -c
10M -d eagerzeroedthick $I/eztDisk > /dev/null; vmkfstools -U $I/eztDisk > /dev/null; done
for I in $(esxcli storage filesystem list |grep 'VMFS-6' |awk '{print $1}'); do vmkfstools -c
10M -d eagerzeroedthick $I/eztDisk; vmkfstools -U $I/eztDisk; done
esxcfg-advcfg -s 32768 /BufferCache/MaxCapacity
esxcfg-advcfg -s 20000 /BufferCache/FlushInterval
```

https://www.it-connect.fr/sophistique-et-personnalisable-le-ransomware-qilin-est-pret-a-chiffrer-les-vm-des-serveurs-vmware-esxi/

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

Piratage chez OKTA (suite)

- Piratage ayant eu lieu entre Septembre et Octobre
  - Vol de fichiers contenant des cookies et des jetons de session
  - 134 clients impactés dont 1Password, Cloudflare et BeyondTrust
- Fuite de données personnelles de tous les utilisateurs du système d'assistance d'OKTA
  - Nom, prénom, identifiant, adresse mail, adresse, n° de téléphone, dernière connexion, date de création du compte, date du dernier changement de mot de passe et le SAML Feferation ID

https://www.bleepingcomputer.com/news/security/okta-october-data-breach-affects-all-customer-support-system-users/

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

Leak chez WeMystic

- 34 GB de données utilisateurs
  - 13 millions d'enregistrements : nom, mail, date de naissance, @ IP, genre, etc.
- Base MongoDB ouverte + sans mot de passe 🎉
  - Données accessibles pendant 5 jours

https://cybernews.com/security/wemystic-data-leak/

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

Red Team CroxyProxy : Proxy Web

- Fonctionne sur n'importe quel navigateur / OS
- Prend en charge le streaming vidéo et l'audio

https://www.croxyproxy.com/ (site)

https://chromewebstore.google.com/detail/croxyproxy-free-web-proxy/lmmpgfjnchldhcieiiegcpdmaidkaanb (extension)

Red Team Guide ultime de l'OSINT

- Toutes sortes de ressources :
  - News, blogs, tools, podcasts, flux RSS, challenges, groupes Discord, etc.

https://start.me/p/DPYPMz/the-ultimate-osint-collection

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

Red Team Dot : outil de Deepfake

- Développé par Sensity
  - Travaille dans la détection de deepfake utilisé dans les médias
- Ne requiert pas d'entraînement additionnel
- Utile dans le cadre de tests sur les capteurs biométriques
- Windows, Linux, macOS, docker…

https://github.com/sensity-ai/dot

Red Team Visualiser sa Session Hijacking !

- Outil récent (< 1 semaine) & développé en Python
- Proxifie toutes les requêtes d'un attaquant et les joue à l'intérieur du navigateur de la victime
  - En utilisant XMLHttpRequest (XHR)
  - Fonctionne également avec les cookies ayant "httponly"

https://github.com/MatthisC/Session-Hijacking-Visual-Exploitation-Python-Version

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

Blue Team Mes secrets ont-il leak sur GitHub ?

- Nommé “Has My Secret Leaked” & fondée par GitGuardian 🇫🇷
- Base de 20 millions d’enregistrements de secrets
  - Mots de passe, clés d’accès, clés d’API, clés privées, etc.
  - Compilation de l’analyse de milliards de fichiers de code, de commits et de gists GitHub
    - Depuis 2017
- Aucun besoin de renseigner ses secrets sur le site
  - Lui fournir un hash de votre secret

https://www.gitguardian.com/hasmysecretleaked

Business et Politique

Droit / Juridique / Politique
National

Retour sur le 1er procès de piratage en cryptomonnaies

- Suite du vol de 9.5 millions $ à la plateforme Platypus
  - Via le système de prêts éclairs (retrait d'urgence)
- Auteur relaxé des chefs d'escroquerie et blanchiment
  - Parce qu'il avait << utilisé de mauvaise foi la possibilité d'avoir ce retrait >>
- Problème de jurisprudence…

https://www.sudouest.fr/justice/justice-relaxe-du-pirate-ethique-au-premier-proces-en-france-de-piratage-en-cryptomonnaies-17671303.php

Conférences

Conférences

Passée(s)

- Cloud & Cyber Security Expo, 15 et 16 novembre – Paris
- ECW, du 21-23 novembre 2023 sur Rennes (8ème éditions)
    - C&ESAR Conferences
- Trustech, 28 au 30 novembre – Paris

À venir

- JSSI, 12 mars 2024 à Paris « Intelligence artificielle et [in]sécurité »

Divers / Trolls velus

Divers / Trolls velus

Le BSOD arrive sur Linux ☠️

- Arrive avec systemd version 255
  - Gestionnaire de service présent sur la plupart des distributions Linux
  - Disponible au cours du 1er semestre 2024
- Affiche un message d'erreur explicite concernant la raison du plantage de la machine
  - Fourni également une version QR code

https://github.com/systemd/systemd/commit/fc7eb1325bd297634568528fb934698a68855121 (systemd-bsod)

ESU payant pour Windows 10 ?

- Fin de support pour Windows 10 → 14 octobre 2025
  - Ensuite ? Support étendu (ESU) payant ! 💰
- Windows 11 nécessite une puce TPM 2.0 (entre autre)

https://www.jeuxvideo.com/news/1830374/c-est-officiel-l-abonnement-payant-pour-mettre-a-jour-windows-arrive-il-faudra-payer-pour-chaque-pc-mais-uniquement-pour-ceux-qui-sont-toujours-sous-windows-10-et-qui-souhaitent-beneficier-des-mises-a-jour.htm

Divers / Trolls velus

Nouveau programme de Bug Bounty sur FranceConnect

- Sur FranceConnect & AgentConnect
  - Cible : le SSO fournie via OpenID Connect
- Jusqu'à 20k €
  - Encore faut-il trouver une faille permettant de se connecter avec une fausse identité
- Hébergé sur le site YesWeHack

https://yeswehack.com/programs/franceconnect-agentconnect-public

SCOPE	TYPE	ASSET VALUE	LOW	MEDIUM	HIGH	CRITICAL
Specific scenarios (see program description)	other	Critical	€100	€800	€3,000	€20,000
AgentConnect (see program description for github link)	web-application	Medium	€100	€500	€1,500	€5,000
FranceConnect+ (see program description for github link)	web-application	High	€100	€800	€3,000	€10,000
FranceConnect (see program description for github link)	web-application	High	€100	€800	€3,000	€10,000
eIDAS Bridge (see program description for github link)	web-application	High	€100	€800	€3,000	€10,000
User Dashboard (see program description for github link)	web-application	Medium	€100	€500	€1,500	€5,000

Divers / Trolls velus

L’ordinateur le plus infecté du monde

- Situé au sein du G(oogle)SEC à Malaga
- Petit-jouet de VirusTotal (rachetée en 2012)
- Relié à un HDD contenant 6 millions de virus
  - Du plus ancien virus (Ambulance - 1990)
  - Au vers le plus ravageur (Happy New Year - 1999)
- But : analyser les virus en temps réel

https://www.bfmtv.com/tech/google/six-millions-de-virus-voici-l-ordinateur-le-plus-infecte-du-monde-de-google_AV-202311300030.html

Prochaines réunions

Prochaine réunion ?

RDV le mardi **9 janvier**

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous