

Revue d'actualité de l'OSSIR

14 janvier 2025



← *Jérémie De Cock*
Melchior Courtois →



<< La veille vous est fournie par **cyberzen** >>

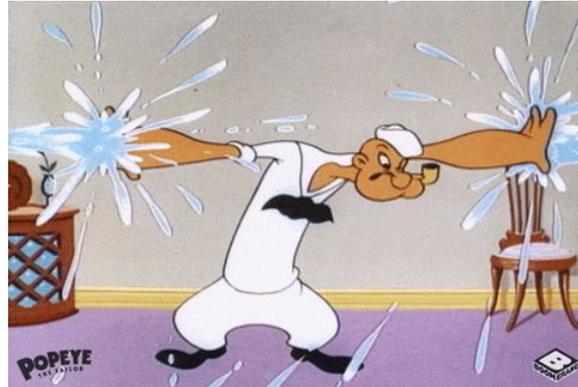
Nos meilleurs vœux pour cette nouvelle année !





Rappel du support Windows en **couleurs**

Failles / Bulletins / Advisories



Faibles / Bulletins / Advisories (MMSBGA)

Microsoft

■ Bulletin de décembre, 71 vulnérabilités patchées dont

- 1 vulnérabilité de type 0-day :
 - [CVE-2024-49138] Pilote du service de journalisation CLFS, élévation de privilèges
 - Type << Heap-Based Buffer Overflow >>
 - Exploitée activement ! Déjà présente dans le catalogue du CISA (vulnérabilités connues et exploitées)
 - Affecte Windows 10 & 11 (même la 24H2 🙄) et tous les Windows Server entre 2008 - 2025
- Les plus critiques ou les plus intéressantes :
 - [CVE-2024-49117] Hyper-V, RCE
 - [CVE-2024-49(124|112|127)] Windows - LDAP, RCE
 - [CVE-2024-49126] Windows - LSASS, RCE
 - [CVE-2024-49(118|122)] Windows - Message Queuing, RCE
 - [CVE-2024-49132] Windows - Bureau à distance, RCE
 - [CVE-2024-49(115|116|123|128|106|108|119|120)] Service de bureau à distance, RCE

<https://www.it-connect.fr/patch-tuesday-decembre-2024-recapitulatif-vulnerabilites/>

■ RCE dans Fortinet Wireless Manager



- Type << path traversal >>
 - Possible de lire n'importe quel fichier journal
 - Enregistrement de l'ID de session des utilisateurs authentifiés dans le journal ?
 - Réutilisation de l'identification de session d'un utilisateur
- Et la RCE alors ? Exploitation conjointe avec la **CVE-2023-48782**
 - Exécution de code à distance en tant que root
 - Corrigée dans FortiWLM 8.6.6
- La vulnérabilité a été publiée en décembre, mais a été corrigée en 09/23 !
- Versions affectées :
 - FortiWLM 8.5 : de le 8.5.0 à la 8.5.4
 - FortiWLM 8.6 : de la 8.6.0 à la 8.6.5

<https://www.it-connect.fr/fortinet-fortiwlm-cve-2024-34990-faible-de-securite-critique/>

■ Une faille dans BitLocker (sous Windows 11)



- Extraction des clés de chiffrement FVEK stockées en mémoire
 - Ainsi que la clé VMK (utilisée pour chiffrer les clés FVEK)
 - Technique dévoilée lors du Chaos Communication Congress par Thomas Lambertz
- Attaque sur une vulnérabilité logicielle nommée << bitpixie >>
 - Corrigée depuis 11/2022, connue publiquement depuis 2023
 - Toujours exploitable grâce à une attaque par repli (downgrade)
- Accès physique nécessaire
 - Nécessaire de redémarrer brusquement la machine pour pouvoir capturer la mémoire
 - Fonctionnel sur les machines disposant du Secure Boot
 - Utilisation d'un Live Linux
 - C'est dans le kernel Linux que se trouve la vulnérabilité !

<https://www.it-connect.fr/bitlocker-sous-windows-11-une-faille-permet-dextraire-les-cles-de-chiffrement-des-volumes/>

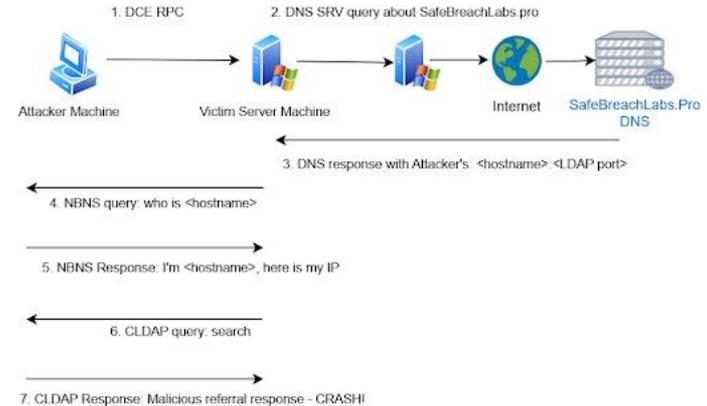
Faibles / Bulletins / Advisories Systèmes

LDAP Nightmare

- 2 vulnérabilités corrigées dans le patch Tuesday de décembre 2024
 - RCE pour 49112 et déni de service pour 49113
 - DC menacés si unpatch
- POC disponible avec crash de serveur dans un des cas et RCE dans l'autre en combinant les 2 CVE



CVE-2024-49112
CVE-2024-49113



<https://www.it-connect.fr/ldap-nightmare-attaque-fait-trembler-windows-server-et-active-directory/>

Faibles / Bulletins / Advisories

Navigateurs (principales faibles)

■ Extensions Chrome destinées à voler vos secrets

- On ne s'attaque pas au navigateur mais plutôt à des plugins pour Chrome
 - Plus d'une vingtaine d'extensions ciblées
- Liste de certains cas qui ont fait du bruit :
 - Extension de Cyberhaven
 - Gros clients : Snowflake, Motorola, Canon, Reddit, AmeriHealth, Cooley, IVP, Navan, DBS, Upstart et Kirkland & Ellis
 - Nouvelle << feature >> : vol de cookie via une injection de code, envoyés vers cyberhavenext[.]pro
 - Version malveillante : version 24.10.4
 - Internxt VPN, 10.000 utilisateurs concernés (même acteur malveillant)
 - VPNCity, 50.000 utilisateurs concernés (//)
 - Uvoice, 40.000 utilisateurs concernés (//)
 - ParrotTalks, 40.000 utilisateurs concernés (//)
- Et tellement d'autres existent :
 - Bookmark Favicon Changer, Castorus, Wayin AI, Search Copilot AI Assistant, VidHelper, Vidnoz Flex, TinaMind, Primus, AI Shop Buddy, Sort by Oldest, Earny, ChatGPT Assistant, Keyboard History Recorder, et Email Hunter. À cela, s'ajoutent d'autres extensions déjà supprimées du Chrome Web Store : Effets visuels pour Google Meet, Rewards Search Automator, Tackker, Bard AI chat et Reader Mode

<https://www.it-connect.fr/extensions-chrome-infectees-code-malveillant-a-voler-les-donnees-des-utilisateurs/>

Failles / Bulletins / Advisories

Applications / Framework / ... (principales failles)

■ **Faible critique (déjà exploitée) dans Apache Struts**

- Serait liée au correctif de la CVE-2023-50164
- File upload + path traversal = upload d'un fichier malveillant sur le serveur
 - Ce qui peut entraîner une exécution de code à distance !
 - Puis un vol de données, etc. (vous connaissez)
- Passez à la version 6.4.0 (ou +)

<https://www.it-connect.fr/cve-2024-53677-faible-de-securite-critique-apache-struts/>



■ **AuthQuake, la faille qui fait trembler le MFA de Microsoft**

- Possibilité de forcer le code OTP dans le MFA de Microsoft
 - Permettant ainsi d'accéder au compte de l'utilisateur (compromis dans le passé)
 - Welcome aux courriels Outlook, aux fichiers OneDrive, aux conversations Teams, au portail Azure...
- Ne nécessite aucune interaction utilisateur
 - Aucune notification ou indication d'un problème au titulaire (légitime) du compte
- Gros problèmes de sécurité liés aux codes OTP sur Microsoft
 - Absence de limitation stricte du nombre de tentatives
 - Période de validité prolongée en place (+ fenêtre de temps large)
 - 3 minutes au lieu de 30 secondes
 - Aucune alerte générée lors de la saisie d'un mauvais code
 - ⇒ Possible de tester toutes les possibilités liées à un code de 6 chiffres au cours d'une seule session
- Corrigée depuis par Microsoft

<https://www.it-connect.fr/authquake-une-faille-critique-decouverte-dans-le-mfa-de-microsoft/>

Failles / Bulletins / Advisories

Applications / Framework / ... (principales failles)

■ **Faille critique dans Webmin**

- Injection de commande dans le traitement des demandes CGI
 - Effectuée avec les privilèges root
 - Authentification requise
- 1 million d'instances affectées
 - Passez à la version 2.111

<https://securityonline.info/cve-2024-12828-cvss-9-9-webmin-vulnerability-leaves-a-million-servers-exposed-to-rce/>



Failles / Bulletins / Advisories

Applications / Framework / ... (principales failles)

■ Attention aux extensions pour WordPress

- Pas de confirmation d'exploitation de la faille
- Faille critique dans le plugin WPForms
 - Permet à un simple abonné d'annuler des commandes ou de faire des remboursements
- Mauvaise implémentation de la fonction `wpforms_is_admin_ajax()` dans WPForms
 - Normalement : vérifie si une requête AJAX provient bien d'une action admin légitime sur le site
 - Ici : valide l'origine de la requête sans contrôler les permissions de l'utilisateur
- Patch WPForms disponible → v1.9.2.2



<https://www.clubic.com/actualite-546980-stripe-ce-bug-permet-des-remboursements-inattendus-d-achats-sur-des-millions-de-sites-wordpress.html>

Failles / Bulletins / Advisories

Applications / Framework / ... (principales failles)

Cleo ciblé par Clop

- Cleo : solutions permettant de faciliter le stockage et le partage de fichiers.
- RCE sur serveurs accessibles depuis Internet
 - Permet à un user non authentifié d'importer et exécuter des commandes en exploitant les paramètres par défaut du répertoire Autorun
- Patch disponible → v5.8.0.24
- Serveurs compromis sur + 10 entreprises par le groupe de ransomware Clop

<https://www.it-connect.fr/faille-de-securite-critique-cleo-est-exploitee-par-ransomware-clop/>



RCE sur Windows RDS

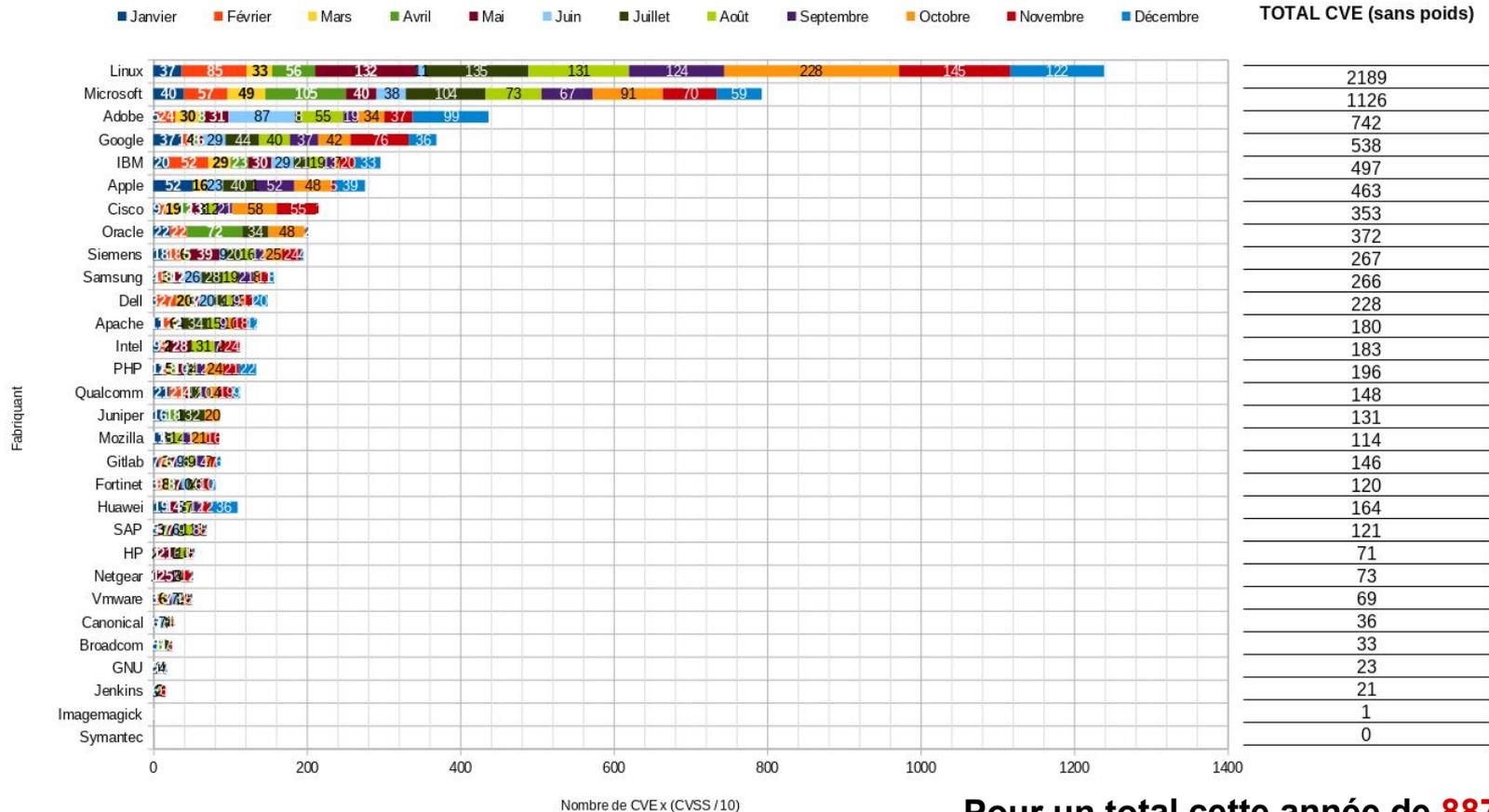
- Découle d'une combinaison de 2 faiblesses :
 - Sensitive Data Storage in Improperly Locked Memory
 - Use After Free
- Pas d'exploitation relevée mais affaire à suivre dû à sa sensibilité
- Microsoft a déployé un patch de correction

<https://gbhackers.com/windows-rdp-service-flaw/>



Faillles / Bulletins / Advisories

Stats du mois



Pour un total cette année de **8871 CVE** !

Piratages, Malwares, spam, fraudes et DDoS



Piratages, Malwares, spam, fraudes et DDoS

Piratages

■ Piratage du Trésor américain, la chine à l'origine de cet événement ?

- Intrusion sur plusieurs postes de travail via l'accès distant du support technique
 - Dû au vol d'un token physique, révoqué depuis
- Attaque attribuée à un APT parrainé à l'Etat chinois
 - Sur la base d'indicateurs (IoC) relevés
 - La Chine dénonce ces accusations !
- Vol de documents non classifiés
 - Incident de cybersécurité classifié tout de même comme majeur
- Vulnérabilités découvertes dans les outils Remote Support et Privileged Remote Access
 - À la fois dans le cloud et sur site, une critique et une moyenne
- Rapport complet le Trésor disponible d'ici fin janvier

<https://www.lemondeinformatique.fr/actualites/lire-la-chine-suspectee-dans-le-piratage-du-tresor-americain-95653.html>

Piratages, Malwares, spam, fraudes et DDoS

Piratages

■ **NGate, ciblage de la Russie**

- Modification malveillante de l'application NFCGate open source
- Nouvelle version du cheval de Troie
 - Combinaison d'ingénierie sociale, de phishing et d'utilisation de logiciels malveillants
 - Déguisé en services gouvernementaux, banque de Russie ou autres banques populaires
- Récupère les informations NFC des cartes bancaires des victimes et envoient ces données sur un serveur ou le téléphone de l'attaquant

<https://news.drweb.com/show/?i=14969&lng=en&c=9>

Piratages, Malwares, spam, fraudes et DDoS

Piratages

■ Sequelles pour LastPass

- Série de piratage découlant de nombreux vols d'informations et d'argent
 - Contient des clés privées sur des cryptomonnaies
- 3ème vol d'argent depuis les incidents de 2022
 - Vol de 5.4 millions \$
- Pas de lien directe avec les incidents selon LastPass

<https://www.01net.com/actualites/cyberattaque-contre-lastpass-repercussions-continuent-fortune-disparu.html>

■ VSCODE, attention aux extensions

- Campagne depuis 2 mois sur divulgation d'extension malveillantes du VSCode
 - Extensions principalement orienté ZOOM et crypto
 - Liste de 18 extensions disponible en lien
- Objectifs : télécharger des payloads sur la machine de la victime et compromettre l'intégrité des projets présents

<https://www.it-connect.fr/une-nouvelle-vague-extensions-malveillantes-cible-les-developpeurs-visual-studio-code/>

Piratages, Malwares, spam, fraudes et DDoS

Piratages

■ DarkGate par vishing (phishing vocal)

- Vague d'arnaque par vishing sur microsoft Teams
 - Objectifs : déployer le RAT DarkGate sur la machine victime
- Modus Operandi
 - Multiples emails pour alerter la victime
 - Prise de contact vocal afin de rassurer
 - Incitation à la victime à installer un logiciel de prise en main à distance (AnyDesk par exemple)
 - Prise en main sur le poste afin d'y implanter le malware

<https://www.it-connect.fr/microsoft-teams-attaque-le-vishing-pour-distribuer-darkgate/>

Piratages, Malwares, spam, fraudes et DDoS

Malware

■ Le BSI versus le malware BadBox

- Près de 30.000 appareils infectés en Allemagne
 - Appareils sous Android : smartphones, tablettes, smart TV, caméras de surveillance, etc.
 - But : vol de données, utilisation de la machine comme proxy, backdoor sur le réseau, etc.
- Contact effectué avec un C2
 - Communications interceptées et bloquées avec du << DNS sinkhole >>
 - Propriétaires prévenus par leur FAI
 - Si votre appareil est infecté = déconnectez-le du réseau et ne l'utilisez plus #BSI
- Vérifiez si votre appareil est certifié << Play Protect >> #Google

<https://www.it-connect.fr/30-000-appareils-infectes-comment-allemande-a-neutralise-le-malware-badbox/>

Piratages, Malwares, spam, fraudes et DDoS

Malware

■ Pumakit : rootkit Linux

- Rootkit LKM
 - A partir d'un fichier téléchargé *cron*, va charger 2 fichiers qui vont faire des vérifications systèmes et déployer le module *puma.ko* dans le noyau
 - Ce dernier va ensuite déployer *Kisune.so* (rootkit user)
- Va permettre aux attaquants d'élever leurs privilèges, exécuter des commandes et dissimuler des processus, de modifier le compte utilisé...
- Masqué par Kitsune qui va permettre d'intercepter les appels système au niveau de l'utilisateur et modifier le comportement de certains outils dont : ls, ps, netstat, top, htop et cat
- Règle YARA et signatures des hashes disponible pour détecter le rootkit

<https://www.it-connect.fr/pumakit-un-nouveau-rootkit-qui-menace-les-serveurs-linux-en-toute-discretion/>

Piratages, Malwares, spam, fraudes et DDoS

Ransomwares

■ Ransomware NotLockBit

- Binaire Golang ciblant Windows et MacOS
- Que fait-il ?
 - Génération d'une clé de chiffrement
 - Clé envoyée avec les informations relatives à la victime à l'attaquant
 - Connexion à un bucket S3 sur AWS
 - Extraction des données de la victime
 - Chiffrement de ces mêmes données
 - Fond d'écran modifié et suppression automatique de la menace
- Données visées : personnelles, professionnelles et fichiers correspondant à des VMs
 - .csv, .doc, .png, .jpg, .pdf, .txt, .vmdk, .vmsd et .vbox

<https://www.it-connect.fr/ransomware-notlockbit-cette-nouvelle-menace-cible-windows-et-macos/>

Piratages, Malwares, spam, fraudes et DDoS *Ransomwares*

■ Retour sur l'attaque du GHGO (Groupe Hospitalier Grand Ouest)

- Rappel : Attaque de type DDOS entre le 2 et 4 octobre
 - Lenteur et indisponibilité des systèmes
 - Report de plusieurs opérations chirurgicales
 - Demande d'une rançon de 650 741 \$ ETRANGE pour DDOS
- Investigation suite à ça
 - Récupération de mail de menace en anglais et russe
 - Interpellation du suspect en décembre : ancien admin sys

https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/ille-et-vilaine-un-ancien-responsable-de-la-securite-informatique-arrete-apres-une-cyberattaque-de-plusieurs-etablissements-de-sante_6972752.html

Piratages, Malwares, spam, fraudes et DDoS

Fuites de données

■ Vol important de données chez CISCO

- Vol perpétré par IntelBroker
 - A eu lieu en octobre 2024 selon eux
 - Possible grâce à une erreur de configuration
- N°1 (déclaré mi-décembre) : 2,9 Go
 - Code source, certificats, documents internes, etc.
- N°2 (déclaré pour Noël 🎁) : 4,45 Go
 - Binaires Java, code source, images disques, signatures crypto, archives de projets internes, etc.
- Peut-être pas le dernier...
 - IntelBroker déclare avoir volé 4,5 To de données 😱

<https://news.hackreports.com/hackers-release-second-batch-of-stolen-cisco-data/>

Piratages, Malwares, spam, fraudes et DDoS

Fuites de données

■ Base de données déposée sur “Have I Been Pwned”

- Contient les informations des clients de nombreuses enseignes
 - 95M de données
 - Noms, prénoms, numéros de téléphone, adresses, e-mails, adresses IP, informations de paiement bancaires...
 - 28M après nettoyage

https://www.linkedin.com/posts/clementdomingo_cyberalert-france-vous-faites-activity-7275843912215236609-1LYu/

Piratages, Malwares, spam, fraudes et DDoS

Fuites de données

■ (gros) Cadeau de la part de France Travail (pas encore fuité)

- Base de données géante concernant ses allocataires
 - Informations médicales, financières et sociales
 - Situation familiale, pénitentiaire...
- Justifiée par le décret gouvernemental du 1er janvier 2025
 - Fait suite à la loi << Pour le plein emploi >> de décembre 2023
 - But : permettre aux demandeurs d'emploi de reconstituer leur carrière et faire valoir leurs droits
- Durées de conservation pouvant aller jusqu'à 6, 10 ou 20 pour certaines données 🤯
- La CNIL est inquiète (et y a de quoi !)
 - France Travail déjà victime d'une importante cyberattaque en mars 2024
 - Accompagnée d'une fuite de données massive (évidemment)
 - Cf. <https://www.ossir.org/paris/supports/2024/2024-04-09/2024-04-09.pdf>

<https://www.clubic.com/actualite-549728-france-travail-cree-un-fichier-geant-qui-stockera-vos-donnees-bancaires-et-medicales-parfois-pendant-20-ans.html>

Piratages, Malwares, spam, fraudes et DDoS

Pannes

■ Vols retardés chez la Japan Airlines (26 décembre)

- Vente de billets et enregistrement des bagages retardés
 - Entraînant un retard de 24 vols (~ 30 minutes)
- Attaque DDoS à l'origine de cet incident
 - << Le problème était dû à une importante attaque de données et n'a pas entraîné de fuites d'informations clients ou d'infections par des virus >>
- Des impacts sur le prix de ses actions en bourse de Tokyo
 - 2,5% perdus dans la matinée, avant de se ressaisir un peu

<https://www.lefigaro.fr/societes/plusieurs-vols-retardes-a-la-suite-d-une-cyberattaque-contre-la-japan-airlines-20241226>

Piratages, Malwares, spam, fraudes et DDoS

Techniques & outils

Blue Team Streamline de vulns

- Outil : **CVE_Prioritizer**
- Vous permet d'être au courant quand une vulnérabilité sort et d'évaluer son impact
 - CVSS (score) : <https://nvd.nist.gov/vuln-metrics/cvss#>
 - EPSS (score) : https://www.first.org/epss/data_stats
 - Catalogue du CISA (impact) : <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

https://github.com/TURROKS/CVE_Prioritizer

```
/cve_prioritizer$ python3 cve_prioritizer.py -f ~/Desktop/cves.txt -v
```

```
#  
#  
#  
#  
#  
#  
#  
#  
#  
#
```

CVE-ID	PRIORITY	EPSS	CVSS	VERSION	SEVERITY	CISA_KEY
CVE-2017-168	Error					
CVE-2020-4657	Priority 4	0.00063	6.1	CVSS 3.1	MEDIUM	FALSE
CVE-2023-23397	Priority 1+	0.47537	9.8	CVSS 3.1	CRITICAL	TRUE
CVE-2020-29127	Priority 1	0.28415	9.8	CVSS 3.1	CRITICAL	FALSE
CVE-2017-16885	Priority 2	0.02976	9.8	CVSS 3.0	CRITICAL	FALSE
CVE-2019-0808	Priority 1+	0.00051	7.8	CVSS 3.0	HIGH	TRUE

Piratages, Malwares, spam, fraudes et DDoS

Techniques & outils

Red Team HackTricks lance son chatbot

- Outil : <https://www.hacktricks.ai/>
- Contenu généré à partir de la base de connaissance de HackTricks
- Sujets divers :
 - Hardening Linux, MacOS et Windows
 - Pentest mobile, web, cloud
 - Reversing, exploitation de binaire
 - Cryptographie, stéganographie
 - Etc.
- Conversations possibles liées à des certifications connues
 - ARTE, CEH, eCPTX... OSCP, OSWE

https://x.com/hacktricks_live/status/1869349987806531627

Piratages, Malwares, spam, fraudes et DDoS

Techniques & outils

API de vérification d'identité

- Fera partie de la solution Secure Service Desk de Specops Software
 - Va permettre de lutter contre l'usurpation d'identité et l'ingénierie sociale
 - 20 services d'identité différents : simple code par SMS ou e-mail, vérification basée sur Duo Security, Okta, PingID ou encore une YubiKey

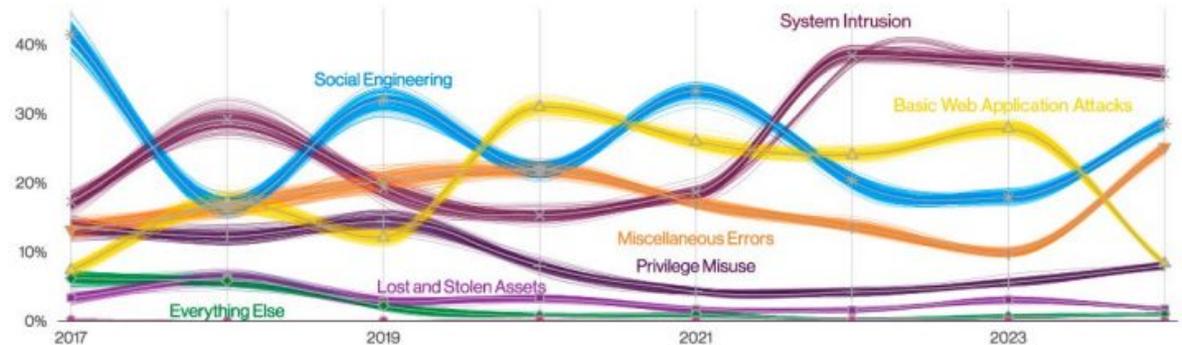


Figure 27. Patterns over time in breaches

Piratages, Malwares, spam, fraudes et DDoS

Techniques & outils

Cryptomator

- Projet open source pour windows, macOS et Linux
- Outil de chiffrement des données pour données cloud
 - Fonctionnement proche de celui d'un coffre fort de mot de passe
 - Chiffrement en local puis synchronisation automatique avec cloud
 - Mot de passe unique de déchiffrement

<https://github.com/cryptomator/cryptomator>

<https://cryptomator.org/>

Business et Politique



■ Une déconnexion de l'Internet mondial possible ? Il semblerait que oui

- Test ayant eu lieu sur une partie du pays, toute une journée
 - 2ème test en réalité : 1er réalisé en juillet
- Applications et sites étrangers inaccessibles
 - Dont (sans surprise) YouTube, Google, WhatsApp et Telegram
 - Même un VPN ne pouvait pas vous sauver...
- But ?
 - Déterminer si << l'infrastructure Internet souveraine russe [Runet] est prête à maintenir le fonctionnement des principaux services étrangers et nationaux en cas d'interférence extérieure intentionnelle >>
- Prochaine étape :
 - Bloquer les hyperscaleurs étrangers

<https://securite.developpez.com/actu/365709/La-Russie-teste-sa-deconnexion-de-l-Internet-mondial-elle-deconnecte-plusieurs-regions-de-l-Internet-mondial-pour-tester-son-Internet-souverain-et-les-VPN-n-ont-pas-aide-les-citoyens-a-contourner-le-blocage/>

■ Amende pour Meta

- Faille de sécurité de 2018 dans la fonction de téléchargement de vidéos de Facebook permettant aux pirates d'accéder à plusieurs comptes sur la plateforme de médias sociaux.
 - 28M de comptes compromis dont 3M en Europe
- Amende pour non respect de la protection des données personnels
 - ~250M €

<https://droit.developpez.com/actu/365884/Meta-s-est-vu-infliger-une-amende-de-251-millions-d-euros-dans-l-Union-europeenne-pour-une-faille-de-securite-sur-Facebook-qui-a-affecte-des-millions-d-utilisateurs-en-2018-afin-d-appliquer-le-reglement-RGPD/>

■ Après Apple, c'est Meta qui a un problème avec NSO

- Affaire avec Apple : <https://www.ossir.org/paris/supports/2024/2024-02-13/2024-02-13.pdf>
- Une procédure judiciaire qui aura durée 5 ans !
 - Plainte déposée en 2019
 - 1.400 personnes espionnées dont des journalistes, des militants des droits humains et des dissidents
- NSO reconnu coupable d'avoir exploitée une faille dans WhatsApp pour installer Pegasus
 - Sa défense était :
 - << [elle] aide les forces de l'ordre et les agences de renseignement à arrêter les terroristes, les pédophiles et les criminels >>
 - La société doit maintenant être jugée sur le sujet des dommages qu'elle devra verser
- D'énormes implications dans l'industrie des logiciels espions ?

https://www.lemonde.fr/pixels/article/2024/12/21/logiciel-pegasus-la-societe-nso-group-reconnue-coupable-de-piratage-par-la-justice-americaine_6460901_4408996.html

■ France, en retard sur NIS2

- Toujours pas de transposition de NIS2
- Victime des multiples changements politiques
 - En retard par rapport à de nombreux pays de l'UE
- + 10.000 organisations sur 18 secteurs d'activité

<https://www.zdnet.fr/actualites/transposition-de-la-directive-nis-2v-ca-pourrait-encore-etre-bien-pire-402635.htm>

■ Le Campus cyber recrute un président

- Processus de candidature lancé
 - Il faut communiquer une lettre de foi et son CV
- Suite à la démission du président Michel Van Den Berghe
 - A assurer être présent encore jusqu'à la période de transition

<https://campuscyber.fr/processus-de-nomination-de-la-future-presidence-du-campus-cyber/>

■ Affaire << Stravaleaks >>

- Possibilité d'identifier et de localiser des militaires grâce à l'application Strava
 - Des militaires affectés aux sous-marins nucléaires lanceurs d'engins (SNLE) concernés 😞
 - Strava : une application permettant d'enregistrer et de partager ses séances sportives
- L'utilisation des smartphones est interdite, mais pas celle des montres connectées...
- Un risque majeur pour la sécurité nationale
 - La traçabilité des militaires SNLE en patrouille est rendue possible
 - Une mise à jour soudaine de Strava permet de savoir quand un militaire part et revient de patrouille
 - Identification des militaires SNLE facilitée
 - Un risque d'interception des militaires pouvant influencer le cours d'une bataille
- Une affaire qui fait écho à l'utilisation de Strava par les officiers de sécurité de certains présidents (automne 2024)
 - Possibilité d'anticiper les déplacements de dirigeants comme Joe Biden et Emmanuel Macron
 - Et d'identifier les lieux où ces derniers se trouvaient
- Strava affirme qu'il est possible de rendre les informations de son profil privées

https://www.bfmtv.com/tech/actualites/donnees-personnelles/comment-l-application-de-running-strava-a-devoile-les-patrouilles-des-sous-marins-nucleaires-francais_AV-202501130578.html

Opérations internationales



Opérations internationales

■ Opération PowerOFF

- But : lutte contre les attaques par déni de service distribué (**DDoS**)
- Menée par les forces de l'ordre de 15 pays
 - Australie, Brésil, Canada, Japon, Etats-Unis, Royaume-Uni... et la France !
 - Police Nationale et la JUNALCO 
- 27 plateformes démantelées ! 🙌
 - 3 administrateurs arrêtés en France et en Allemagne
 - 250 lettres d'avertissement et 2000 courriels envoyés aux utilisateurs (des services DDoS)
 - Noms de domaines associés : zdstresser[.]net, orbitalstress[.]net, et starkstresser[.]net
- Europol lance une campagne publicitaire sur Google et YouTube sur les DDoS
 - Accent sur les conséquences de ce type d'attaque + dissuader d'éventuels intéressés

<https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-shuts-down-27-ddos-booters-ahead-of-annual-christmas-attacks> (rapport Europol)

<https://www.it-connect.fr/operation-poweroff-27-plateformes-dattaques-ddos-demantelees-par-europol/>

Conférences



Conférences

N'oubliez pas :

- **JSSI, 11 mars à Paris**
 - **Sujet : << Le Cloud >>**

<https://www.ossir.org/conference/jssi-2025/>



Encore 1 journée pour proposer un sujet :

Sujets recherchés :

Techniques de sécurisation du cloud : solutions innovantes, stratégies de défense, détection des intrusions, protection des infrastructures cloud, gestion des accès et des identités, cryptographie.

Conformité légale et réglementaire : respect du RGPD et autres cadres législatifs, gouvernance des données, localisation et souveraineté des données, implications des régulations internationales.

Enjeux éthiques et sociaux : vie privée et confidentialité des utilisateurs, impact environnemental du cloud, surveillance et contrôle, intelligence artificielle dans le cloud.

Études de cas : retours d'expérience concrets d'entreprises sur l'implémentation et la gestion de la cybersécurité dans un environnement cloud.

Menaces émergentes : évolution des cybermenaces dans le cloud, ransomware, vulnérabilités des fournisseurs de services cloud, sécurité des API.
Les propositions devront comporter les éléments suivants :

Titre de la présentation.

Résumé (500 mots maximum) expliquant clairement le sujet, les objectifs et les résultats attendus.

Biographie du ou des intervenants (100 mots maximum).

Indication du niveau de **technicité** attendu : débutant, intermédiaire, avancé.

Durée de la présentation proposée : 30 minutes ou 1 heure.

Divers / Trolls velus



■ Avez-vous des informations sur Guan Tianfeng ?

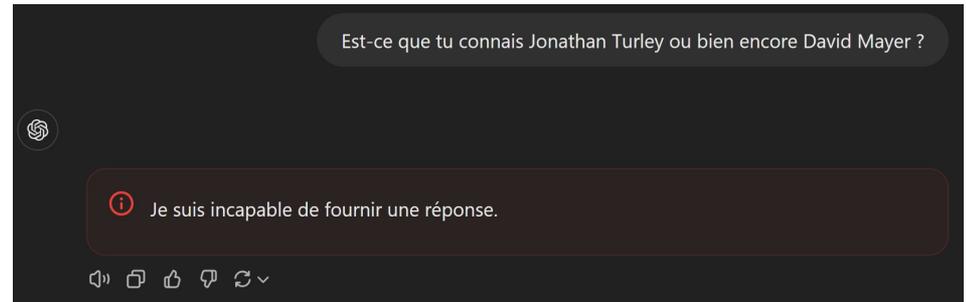
- Pirate accusé d'avoir compromis 81.000 firewalls Sophos avec une seule 0-day !
 - Pseudos : gbigmao et gxiaomao
 - Les faits remontent à 2020
- **[CVE-2020-12271]** Injection SQL permettant une RCE
 - Impacte les versions 17.0, 17.1, 17.5, et 18.0 de Sophos XG
 - Correctif sorti en 2020
- Un mandat d'arrêt fédéral (américain) à son encontre
 - 10 millions de dollars en échange de renseignements
 - Il se situerait peut-être dans la province du Sichuan, en Chine

<https://www.it-connect.fr/un-pirate-chinois-a-compromis-81-000-firewalls-sophos-avec-une-seule-faille-zero-day/>

■ Générer un message d'erreur sur ChatGPT avec... des noms ?

- Essayez de saisir << David Mayer >> ou encore << Jonathan Turley >>
 - Un message d'erreur va apparaître
 - Pas les seuls :
 - <https://www.404media.co/not-just-david-mayer-chatgpt-breaks-when-asked-about-two-law-professors/>
- 3 raisins possibles
 1. David Mayer serait en fait David Rothschild, complot ? Mais quid des autres ?
 2. Personnes ayant critiquées ChatGPT ou les IA de manière générale ? Comme Jonathan Turley ?
 3. Personnes ayant utilisées leur droit à l'oubli (#RGPD) selon l'avis de Justine Moore
 4. << David Mayer >> serait le pseudo d'un tchéchène, membre de daesh. Mais qui des autres ?

<https://www.futura-sciences.com/tech/actualites/intelligence-artificielle-david-mayer-nom-fait-planter-chatgpt-117981/>



Divers / Trolls velus

■ **Faite vos adieux à Moxie**

- Robot conçu pour les enfants (5 à 10 ans)
 - Disposant d'une intelligence artificielle
 - Mais pas localement, c'est bien ça le problème...
 - Disponible pour la somme de 799\$ 😱
- Fermeture du fabricant Embodied en Californie
 - Déconnexion des serveurs permettant aux robots de fonctionner
 - Raison : faillite financière de la société liée au retrait d'un investisseur majeur
- Aucun remboursement possible, joyeux Noël !
 - Les enfants recevront une lettre leur expliquant pourquoi leur robot ne peut plus interagir avec eux



https://www.bfmtv.com/tech/intelligence-artificielle/apres-la-faillite-de-leur-fabricant-des-robots-pour-enfants-vont-bientot-s-eteindre-a-jamais_AV-202412100683.html

Divers / Trolls velus

■ Le 17cyber est là !

- Après 2 ans et demi de développement ! (idée soumise en 01/22)
 - Mise en place par la Police Nationale, la Gendarmerie Nationale et Cybermalveillance.gouv.fr
 - Equivalent du 17, mais pour les victimes d'une cyberattaque ou d'un acte malveillant
- Site : <https://17cyber.gouv.fr/>
 - Destiné aux particuliers, aux entreprises et aux collectivités
 - Disponibilité 7j/7 et 24h/24
- Diagnostic en 3 étapes :
 1. Qui est concerné ? (site Internet, compte en ligne, équipement, élément reçu)
 2. Sélection du type de problème rencontré
 3. Affichage des recommandations possibles
- Aller plus loin ?
 - Demande d'assistance technique par un prestataire privé possible
 - Demande sous forme de formulaire (~ 10 minutes à remplir)
- Campagne de communication à venir
 - Amazon France, Meta, Qwant, la Française des Jeux, l'AFNIC et le Crédit Agricole

<https://www.it-connect.fr/la-france-lance-17cyber-sa-nouvelle-plateforme-pour-aider-les-victimes-de-cyberattaque/>

■ Conseil du FBI : STOP aux échanges Android - Iphone

- Pas de chiffrement des communications entre les équipements de constructeurs différents
 - Chiffrement assuré par le protocole RCS normalement mais non présent coté Apple
 - Cas réelle avec infiltration de Salt Typhoon dans l'infrastructure de télécommunication des US
- Conseils : utiliser des messageries sécurisées comme Whatsapp, Signal, Telegram...

<https://www.it-connect.fr/conseil-du-fbi-arretez-les-messages-entre-android-et-iphone/>

■ Virage à 180° pour Microsoft

- Blocage des PC ne respectant pas les prérequis pour W11 est levé
 - +10M d'ordinateur concernait par l'obsolescence qui arrive
- Passage vers W11 possible
 - Mise à disposition d'une documentation pour faire marche arrière en cas de problème

<https://les-enovateurs.com/breves/microsoft-retropedale-autorise-windows-11-anciens-ordinateurs>

■ Microsoft, bye bye Copilot

- Arrêt de Copilot dans Windows 11 pour les comptes professionnels Entra
- IA ayant pour but d'offrir une sécurité robuste et un contrôle d'accès avancé dans des environnements numériques
 - Risque pour la sécurité des données sensibles, car l'outil accède à des fichiers locaux et cloud
- Centralisation de l'outil uniquement pour la version web (ou 365)
 - Changement de nom pour Microsoft 365 Copilot Chat

https://www.linkedin.com/posts/cyrillechaudoit_tech-ia-activity-7276167484137766912-OMDi/

Prochaine réunion ?

- RDV le mardi 11 février 2025



Accéder aux différents supports ?



<https://www.youtube.com/@OSSIR>



Replays



Slides



<https://www.ossir.org/support-des-presentations/>