



Revue d'actualité de l'OSSIR

14 novembre 2023

Jérémy De Cock

Christophe Chasseboeuf

Vladimir Kolla



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)

Microsoft

■ Bulletin de septembre, 104 vulnérabilités patchées dont

- 3 zero-day :
 - [CVE-2023-41763] Skype for Business (Server) : élévation de privilèges (et énumération ?)
 - [CVE-2023-36563] Microsoft WordPad : vol des hashes NTLM à l'ouverture d'une doc avec WordPad
 - [CVE-2023-44487] HTTP/2 Rapid Reset : DDoS (records 🦋)
- 12 failles critiques de type "RCE" :
 - Windows - Protocole L2TP : 9 CVEs
 - Windows Message Queuing : 2 CVEs
 - Windows-vTPM : 1 CVE

<https://patchalooza.com/>

Faibles / Bulletins / Advisories

Systemes

■ Faible 0-day dans Cisco IOS XE (CVE-2023-20198)

- Nécessite un accès à l'interface web
 - En HTTP ou HTTPS
 - [+] Sans authentification
 - [=] Privilèges administrateurs = contrôle total de l'équipement !
- Un implant malveillant est injecté sur chaque appareil compromis
 - Peut être détecté par le scanner mis au point par VulnCheck
- Des dizaines de milliers d'appareils compromis
 - Dont 1000 en France
- Que faire ?
 - Désactivez l'accès HTTP/HTTPS depuis l'extérieur !!!!!
 - Et mettez à jour : 17.9.4a (IOS XE 17.9), 17.6.6a (IOS XE 17.6) et 17.3.8a (IOS XE 17.3)

<https://vulncheck.com/blog/cisco-implants> (scanner)


<https://www.horizon3.ai/cisco-ios-xe-cve-2023-20198-deep-dive-and-poc/> (+ détails techniques par Horizon3.ai)

<https://www.bleepingcomputer.com/news/security/over-10-000-cisco-devices-hacked-in-ios-xe-zero-day-attacks/>

Failles / Bulletins / Advisories

Applications / Framework / ... (principales failles)

■ Faille 0-day dans SysAid (CVE-2023-47246)

- Solution de type ITSM
- Faille de type “path traversal”
 - Permet d’exécuter du code sur le serveur
 - Utilisé pour déployer un webshell à la racine du Tomcat et ... déployer Clop 
- Patchez → version SysAid 23.3.36 (ou plus)

<https://www.it-connect.fr/une-faille-zero-day-dans-sysaid-est-exploitee-au-sein-dattaques-avec-le-ransomware-clop/>

■ 2 vulnérabilités critiques sur Veeam ONE (CVE-2023-38547 & CVE-2023-38548)

- 1x RCE sur le SQL Server qui héberge la base de données de Veeam ONE
- 1x faille permettant de récupérer le hash NTLM du compte utilisé par le Reporting Service
- Mettez à jour !
 - Veeam ONE 12 P20230314 (12.0.1.2591), Veeam ONE 11a (11.0.1.1880) et Veeam ONE 11 (11.0.0.1379)
 - Permet de corriger 2 autres vulnérabilités intermédiaire au passage

<https://www.it-connect.fr/patchez-veeam-one-pour-vous-protger-de-4-vulnerabilites-dont-2-critiques/>

Failles / Bulletins / Advisories

Applications / Framework / ... (principales failles)

■ Faille dans Apache ActiveMQ (CVE-2023-46604)

- Exploiter pour déployer le ransomware Hello Kitty
 - RCE sur la machine
 - Déploiement du ransomware à la volée
- 3k instances ActiveMQ accessibles et vulnérables

<https://github.com/X1r0z/ActiveMQ-RCE> (POC)

<https://thehackernews.com/2023/11/hellokitty-ransomware-group-exploiting.html> (liste des versions patchées)



■ Vulnérabilité dans DSM (CVE-2023-2729)

- Mot de passe du compte admin généré avec Math.Random()
 - Aléatoire fourni par les bibliothèques mathématiques **0**
 - Aléatoire fourni par les bibliothèques cryptographiques **1** → `window.crypto.getRandomValues()`
- Cassage du mot de passe difficile
 - Prérequis 1 : récupérer certains GUIDs générés lors de l'installation (pour obtenir le seed PRNG)
 - Prérequis 2 : accéder au NAS
 - Sachant que : le compte admin est désactivé par défaut

<https://thehackernews.com/2023/10/new-admin-takeover-vulnerability.html>

Failles / Bulletins / Advisories

Réseau (principales failles)

■ Faille dans le protocole SLP (CVE-2023-29552)

- Ajoutée par le CISA dans son catalogue de vulnérabilités connues et exploitées
- Protocole permettant la découverte automatique de services sur un réseau local
 - En écoute sur le port 427/udp
 - Disponible sur les serveurs VMware ESXI, l'IMM des serveurs IBM, etc.
- Faille de type “dénier de service”
 - Pas besoin d'être authentifié
 - Facteur d'amplification pouvant atteindre x2200
- Service désactivé par défaut sur VMware ESXI

<https://thehackernews.com/2023/11/cisa-alerts-high-severity-slp.html>

Failles / Bulletins / Advisories

Smartphones (principales failles)

■ Génial, depuis iOS 14, Apple anonymise l'adresse MAC... (CVE-2023-42846)

- Ah bah non en fait 😞
- Broadcast d'une requête mDNS à chaque connexion à un WiFi
 - Avec la MAC réelle dans le champ des "option data"

<https://arstechnica.com/security/2023/10/iphone-privacy-feature-hiding-wi-fi-macs-has-failed-to-work-for-3-years/>



Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Piratages

■ Piratage chez Okta

- Vol de fichiers contenant des cookies et des jetons de session
 - Correspondant à des environnements de clients (134 clients impactés) !
 - Utilisés lors de cas d'assistance
- Possible grâce à un vol d'identifiants d'un employé d'Okta
 - Donnant accès à la solution d'Help Desk d'Okta (pour gérer les tickets)
- Liste non exhaustive de clients affectés : BeyondTrust, CloudFlare, 1Password, etc.
 - L'alerte est venue d'une tentative de connexion venant d'un compte admin Okta chez BeyondTrust

<https://www.bleepingcomputer.com/news/security/okta-says-its-support-system-was-breached-using-stolen-credentials/>

Piratages, Malwares, spam, fraudes et DDoS

Piratages

■ **Attaques de logiciels malveillants contre le secteur technologique israélien**

- **Campagne d'Imperial Kitten**
 - Cible : Israël - entreprises de transport, de logistique et de technologie
 - Corps des gardiens de la révolution islamique (IRGC)

<https://www.bleepingcomputer.com/news/security/iranian-hackers-launch-malware-attacks-on-israels-tech-sector/>

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

■ Une brèche chez ... Facebook

- les comptes d'utilisateurs interdits restaurés
 - l'IA en cause ??

<https://planetzuda.com/concealed-breach-revealed-planet-zuda-uncovers-facebooks-hidden-hack-banned-user-accounts-now-being-restored/2023/10/30/>

Piratages, Malwares, spam, fraudes et DDoS

Ransomwares

■ ASVEL victime de NoEscape

- Vol de 32 Go de données
 - Informations sur les joueurs : passeports, cartes d'identités, documents de finance, etc.
 - Documents contractuels entre les joueurs et le club de l'ASVEL
- Les données n'ont finalement pas été publiées...
 - Négociations effectuées entre le club et le groupe NoEscape ?

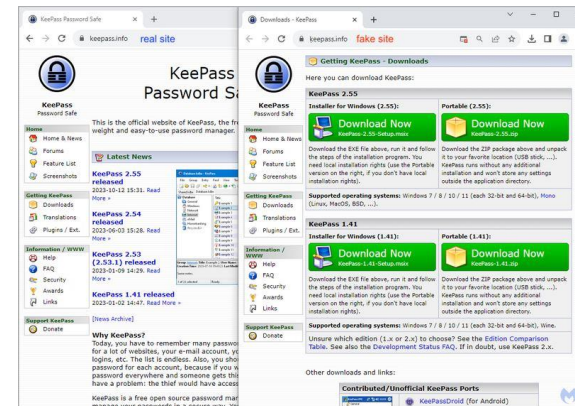
<https://www.it-connect.fr/cyberattaque-lasvel-club-de-basket-professionnel-victime-du-ransomware-noescape/>

Piratages, Malwares, spam, fraudes et DDoS Hack 2.0

Fake du site de KeePass avec Punycode

- “keepass” → site fake en 1ère position puisqu’il est sponsorisé
 - Nom du site = www.keepass.info
 - Ou plutôt xn--eepass-vbb[.]info avec l’encodage des caractères
- Copie du site officiel à une différence près
 - KeePass-2.55-Setup.msix (signé avec un certificat) infecté par un script PS #FakeBat
 - Utilisé pour établir une connexion avec un C2
- Site supprimé entre temps

<https://www.bleepingcomputer.com/news/security/fake-keepass-site-uses-google-ads-and-punycode-to-push-malware/>

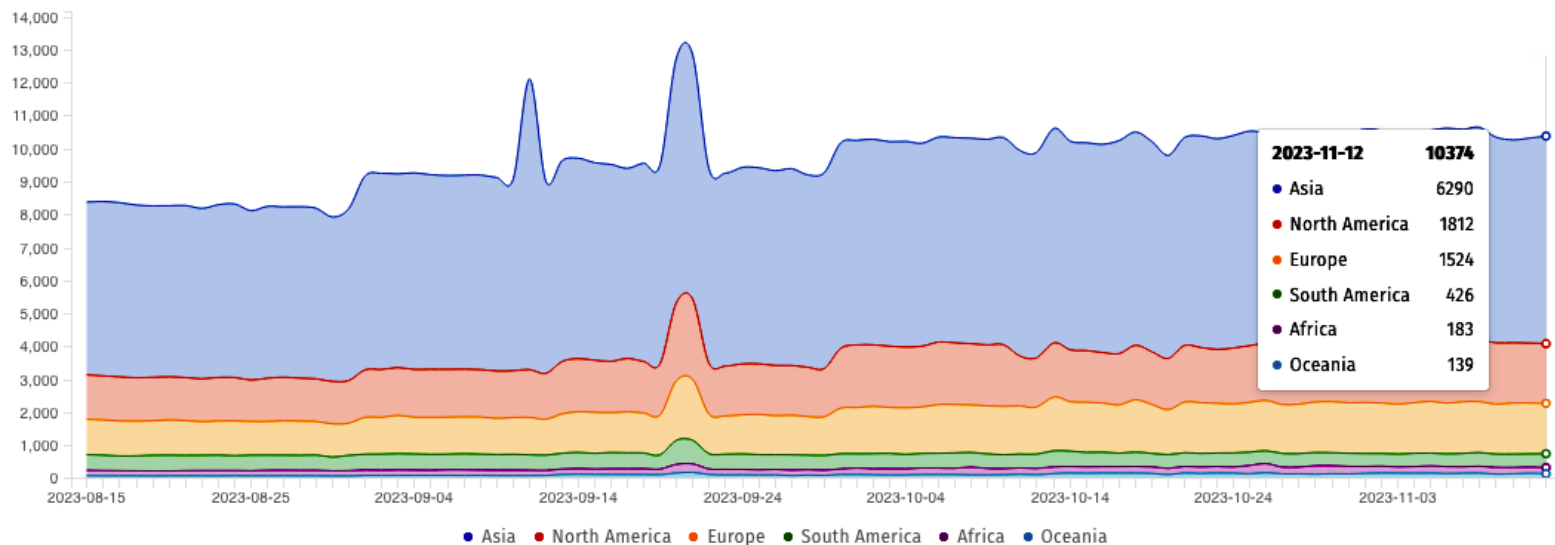


Piratages, Malwares, spam, fraudes et DDoS Hack 2.0

Chaîne d'exploitation RCE préauth de Juniper

- Juniper J-Web
 - CVE-2023-36844, CVE-2023-36845, CVE-2023-36846 et CVE-2023-36847
 - Shodan voit plus de 13 600 appareils Juniper exposés

https://www.bleepingcomputer.com/news/security/cisa-warns-of-actively-exploited-juniper-pre-auth-rce-exploit-chain/?traffic_source=Connatix



Piratages, Malwares, spam, fraudes et DDoS

Fuites de données

■ Fuite de données chez Casio (126k utilisateurs impactés)

- Accès à la base de données du service ClassPad.net
 - 91k clients japonais
 - 35k clients situés dans 148 pays
- Nom, prénom, adresse mail, pays de résidence, clés de licence, commandes, etc.
 - Aucune information de paiement
- Recommandé de changer de mot de passe sur leur site

<https://www.bleepingcomputer.com/news/security/casio-discloses-data-breach-impacting-customers-in-149-countries/>

■ Fuite de données chez Ile-de-France Mobilités

- Collecte de 4k utilisateurs et mots de passe
- Recommandé de changer de mot de passe sur leur site

<https://www.tf1info.fr/transports/pass-navigo-passe-ile-de-france-mobilite-porte-plainte-apres-le-piratage-de-milliers-de-comptes-d-usagers-donnees-personnelles-2272211.html>

Piratages, Malwares, spam, fraudes et DDoS

Fuites de données

■ Lockbit vs Boeing

- Depuis octobre 2023
 - Cible : activité de pièces détachées et de distribution
 - Ultimatum : 02/10/2023
 - Publication : 10/10/2023
 - Volume : 500 Go de données

<https://www.linformaticien.com/magazine/cybersecurite/61337-lockbit-boeing-confirme-un-cyberincident.html>

<https://incyber.org/boeing-confirme-attaque-par-rancongiel-lockbit/>

<https://www.usine-digitale.fr/article/les-hackers-de-lockbit-commencent-a-publier-des-donnees-de-boeing.N2194448>

<https://www.boursorama.com/bourse/actualites/donnees-de-boeing-publiees-par-la-bande-de-pirates-lockbit-fca77758f5175305796169ffdec9ac73>



Piratages, Malwares, spam, fraudes et DDoS

Fuites de données

■ Gros leak du côté de LinkedIn

- 35 millions de comptes concernés (dont 200k français)
 - Noms complets, adresses mail, etc.
 - Aucun mot de passe !
- Aucune compromission, juste du web scraping
- Ce n'est pas leur premier leak (#500m2021 #827m2021again)

<https://www.hackread.com/hacker-leaks-scraped-linkedin-user-records/>

Piratages, Malwares, spam, fraudes et DDoS

Publication

Rapport de l'ANSSI sur MOA

- Opération d'APT28 ciblant des entités françaises depuis 2021
 - Odays + phishing + relais par des routeurs compromis + outils "classiques"

<https://www.cert.ssi.gouv.fr/cti/CERTFR-2023-CTI-009/>

Nouveau guide de sécurisation AD (#ANSSI)

- Fait suite aux "*Recommandations de sécurité relatives à Active Directory*"
 - Qui commence à dater (septembre 2014)
- Insiste particulièrement sur l'importance du cloisonnement (tiering)

<https://cyber.gouv.fr/publications/recommandations-pour-ladministration-securisee-des-si-reposant-sur-ad>

Tier 0

- forte sensibilité (l'objectif est de réduire son exposition aux menaces)
- peu de ressources

Tier 1

- essentiel aux valeurs métier
- grande hétérogénéité

Tier 2

- moindre sensibilité (mais les usages conduisent à une forte exposition aux menaces)
- beaucoup de ressources



Piratages, Malwares, spam, fraudes et DDoS

Techniques & outils

Blue Team Scan de drivers Windows malveillants

- Liste de pilotes Windows malveillants utilisés (ex : mimidrv.sys)
- Scanner disponible sur leur Github (en PS)

<https://github.com/magicword-io/LOLDrivers>

<https://www.loldrivers.io/>



Business et Politique

■ Atos pourrait être nationalisé !!?

- Temporairement ?
- Concernant ses activités stratégiques
- Pour éviter un rachat étranger

https://www.francetvinfo.fr/economie/entreprises/atos-le-geant-francais-de-la-cybersecurite-que-des-deputes-veulent-nationaliser-temporairement_6142020.html

■ Un alternant d'OCD à Rennes, condamné à 4 ans dont 2 avec sursis

- Développeur de Frenchy Shellcode

<https://www.zdnet.fr/actualites/alternant-chez-orange-cyberdefense-le-jour-developpeur-de-programmes-malveillants-la-nuit-39962084.htm>

SentinelOne acquiert le cabinet de conseil en cybersécurité Krebs Stamos Group

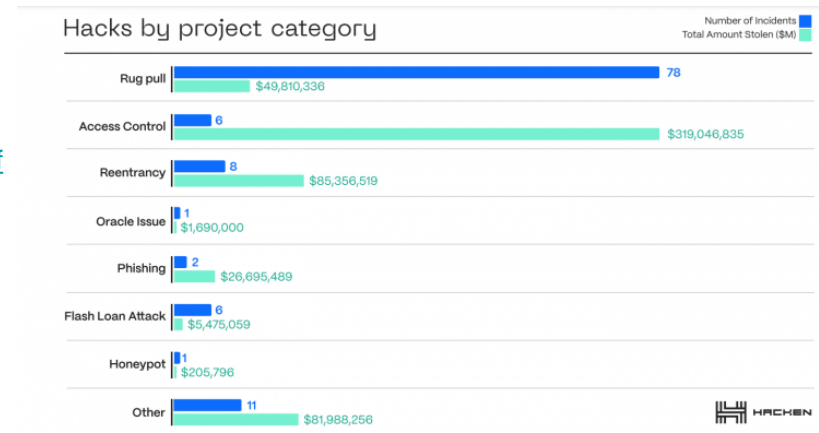
- Krebs Stamos
 - Christopher Krebs, premier directeur de l'Agence américaine de cybersécurité et de sécurité des infrastructures (CISA, équivalent de l'Anssi)
 - Alex Stamos, ancien responsable de la sécurité de Facebook.

<https://therecord.media/sentinelone-to-acquire-krebs-stamos-group>

680 million d'euros ...

- Haken Web3 Report
 - Le facteur humain et les "Rug Pull"

<https://wp.hacken.io/wp-content/uploads/2023/10/Protecting-WEB3-Q3-report.pdf>



Clearview gagne

- Au Royaume-Uni
 - Société étrangère

<https://techcrunch.com/2023/10/18/clearview-wins-ico-appeal/>

SolarWinds

- Securities and Exchange Commission
 - Affaire SUNBURST
 - poursuites à l'encontre de SolarWinds

<https://www.sec.gov/news/press-release/2023-227>

Meta et TikTok

- Union Européenne
 - visés par une procédure de l'UE ?
 - paiement d'astreintes périodiques ?

<https://www.rfi.fr/europe/20231020-d%C3%A9sinformation-meta-et-tiktok-dans-le-collimateur-de-la-commission-europ%C3%A9enne>

Intel

- Bug DownFall
 - plainte en recours collectif déposée
 - 5 ans avant de sortir un correctif !

<https://www.darkreading.com/vulnerabilities-threats/intel-downfall-lawsuit-10k-plaintiff-ignoring-chip-bug>

■ Apple ouvre les portes de son SEAR parisien

- Centre SEAR (Security Engineering & Architecture)
 - Ivan Krstic dirige une équipe internationale d'ingénieurs
 - Objectif : prévoir d'éventuelles failles matérielles
 - En août 2023 : sollicité par ... Google pour \$15 000

<https://www.macg.co/aapl/2023/11/ivan-krstic-directeur-des-systemes-de-securite-dapple-le-mode-isollement-na-toujours-pas-ete-pris-en-defaut-140445>

<https://www.forbes.com/sites/daveywinder/2023/08/03/google-pays-apple-15000-for-hacking-chrome-security/>

<https://yourstory.com/2023/08/google-apple-chrome-bug-bounty-collaboration>

<https://www.helpnetsecurity.com/2023/09/22/cve-2023-41992-cve-2023-41991-cve-2023-41993/>

■ **Intégration de backdoor dans les services de messagerie comme Signal ?**

- Souhaité par Gérald Darmanin (ministre de l'intérieur)
 - WhatsApp, Telegram, Signal, etc. = messageries protégées par le chiffrement P2P
 - Afin de faciliter les enquêtes (écouter les appels téléphoniques, lire les SMS)
- Peu de chance que les éditeurs acceptent...
- Alternative ? Logiciel espion ? Pegasus ?

<https://www.it-connect.fr/le-gouvernement-veut-pouvoir-acceder-aux-conversations-whatsapp-telegram-signal-etc/>

■ Microsoft, il y a 40 ans

- Annoncée le 10 novembre 1983, la première version de Windows sortira deux ans plus tard

<https://www.clubic.com/actualite-508486-il-y-a-40-ans-microsoft-annoncait-la-sortie-de-windows.html>

<https://www.01net.com/actualites/microsoft-fete-les-40-ans-de-word-et-evoque-les-nouveautes-a-venir.html>





Conférences

Conférences

Passée(s)

- Les assises de la cybersécurité, 11-14 octobre à Monaco
- Hackvens, 13 octobre à Lyon
- SecSea, 13 au 14 octobre à La Ciotat
 - Belle conférence tech
- Hexacon, 14-15 octobre à Paris
- Identity Days, 24 octobre à Paris
- DevSecOps World Tour, 17 octobre à Paris
- Unlock your Brain, 4 au 5 novembre à Brest

À venir

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



Divers / Trolls velus

Divers / Trolls velus

Log4Shell ...

- Log4.sh
 - Hummm

<https://log4.sh/>



Ce site ne peut pas fournir de connexion sécurisée

log4.sh utilise un protocole incompatible.

ERR_SSL_VERSION_OR_CIPHER_MISMATCH

Masquer les détails

Protocole incompatible

Le client et le serveur ne sont pas compatibles avec une version de protocole ou une méthode de chiffrement SSL commune.

log4.sh

Updated 1 second ago

Domain Information

Domain:	log4.sh
Registrar:	Porkbun LLC
Registered On:	2021-12-18
Expires On:	2023-12-18
Updated On:	2023-09-01
Status:	clientDeleteProhibited clientTransferProhibited
Name Servers:	maceio.ns.porkbun.com curitiba.ns.porkbun.com salvador.ns.porkbun.com fortaleza.ns.porkbun.com

Qualys. SSL Labs

[Home](#) [Projects](#) [Qualys Free Trial](#) [Contact](#)

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > log4.sh

SSL Report: log4.sh

Assessed on: Sat, 11 Nov 2023 16:40:27 UTC | [Hide](#) | [Clear cache](#)

[Scan Another >>](#)

	Server	Test time	Grade
1	44.227.76.166 ec2-44-227-76-166.us-west-2.compute.amazonaws.com Failed to communicate with the secure server	Sat, 11 Nov 2023 16:39:51 UTC Duration: 7.839 sec	-
2	44.227.65.245 ec2-44-227-65-245.us-west-2.compute.amazonaws.com Failed to communicate with the secure server	Sat, 11 Nov 2023 16:39:59 UTC Duration: 28.483 sec	-

Divers / Trolls velus

AMAZON s'installe en prison

- Amazon s'est installé dans une ancienne prison dans la prison Koepel dans Haarlem (Pays-Bas)

<https://twitter.com/cullend/status/1722797579128185161>

<https://twitter.com/eastdakota/status/1723088114288103899>



https://ca.finance.yahoo.com/news/amazon-office-former-prison-netherlands-215831018.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xiLmNvbS8&guce_referrer_sig=AQAAAMYLZ94_CWtrrGLzDEqEIQ37fZke_dlvx7_JOq00U2oQ49Qdv78FyM3JcG3ldtpyhDzJINkaj_iaHw5eW0A83ClbHhGyOXuCVLLzBWB3N2aQggN-gjiBwtJZnOk_cGQs_Qa3pod-YMWkO22xQ3_zb5jyNDUKVlxlvjIX0gx43emd

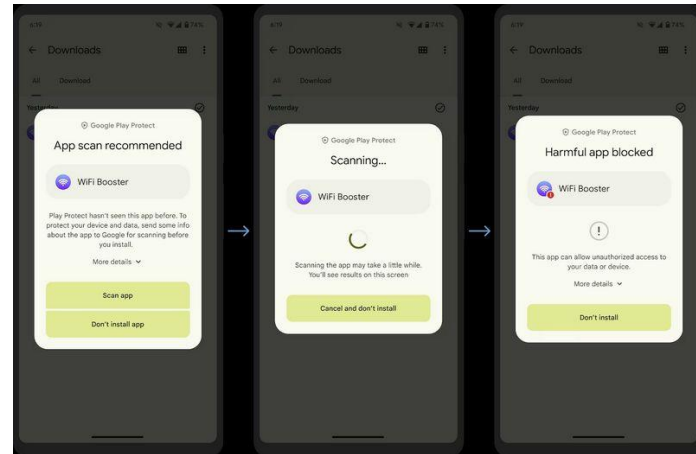


Divers / Trolls velus

Google Play Protect v2 ?

- Présent depuis plusieurs années
 - Contré par les malwares polymorphes
- Analyse maintenant en temps réel le code des applications téléchargées
 - Utilise des algorithmes de machine learning
 - Possibilité d'analyser les applications déjà téléchargées
- Déploiement step by step (en commençant par l'Inde)

<https://www.it-connect.fr/pour-lutter-contre-les-malwares-google-play-protect-va-analyser-le-code-des-apps-en-temps-reel/>

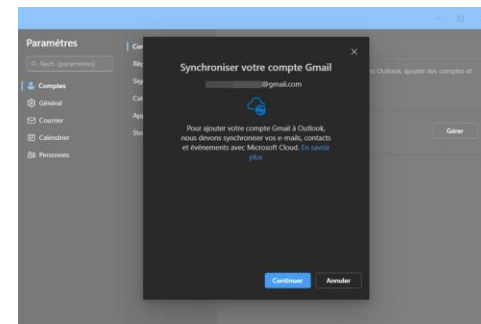


Divers / Trolls velus

■ Qui aime le nouveau look d'Outlook ?

- Qui dit nouvel Outlook...
 - Nouvelle interface
 - Prise en charge des comptes Microsoft, Gmail, Yahoo, iCloud, etc.
- ... dit quelques libertés
 - << La synchronisation de votre compte avec Microsoft Cloud signifie qu'une **copie de votre courrier électronique, de votre calendrier et de vos contacts** sera synchronisée entre votre **fournisseur de messagerie** et les **centres de données Microsoft**. >>
 - Également la synchronisation du nom d'utilisateur, du mot de passe ainsi que le serveur de destination

<https://www.it-connect.fr/le-nouvel-outlook-copie-vos-donnees-vers-les-serveurs-microsoft-y-compris-pour-les-comptes-gmail/>



■ Est-ce que NTLM disparaîtra un jour ? Microsoft tente...

- IAKerb
 - **Problématique** : l'authentification Kerberos requiert de pouvoir joindre le DC (KDC)
 - **Solution** : utilisation de serveur relais pour l'authentification (🤖)
- Local KDC for Kerberos
 - **Problématique** : c'est le contrôleur de domaine qui joue le rôle de KDC (= authentification en local compliquée)
 - **Solution** : ajout d'un surcouche au niveau de la base SAM afin de réaliser une authentification via Kerberos
- Réponse : c'est compliqué.

<https://www.it-connect.fr/microsoft-kerberos-va-evoluer-pour-preparer-la-desactivation-de-ntlm-dans-windows-11/>

■ “Protection IP” sur Chrome

- Nouvelle fonctionnalité permettant de masquer votre adresse IP
 - À l'aide de serveurs Proxy...
 - ... à deux sauts : 1st Google & 2nd CDN externe
- Seuls les adresses IP basées aux USA pourront en profiter (pour l'instant)
- Quelques issues...
 - Rend le blocage des DDoS compliqué
 - Si un Proxy est compromis, le trafic traversant sur ce dernier pourra être manipulé
- Quelques solutions
 - Limitation de débit
 - Authentification auprès du Proxy

<https://www.bleepingcomputer.com/news/google/google-chromes-new-ip-protection-will-hide-users-ip-addresses/>

■ Enfin le support natif des formats d'archive sur Windows

- Formats supportés : .rar, .7z, .tar, .tar.gz, .tar.bz2, .tar.zst, .tar.xz, .tgz, .tbz2, .tzst et .txz
 - La prise en charge des fichiers chiffrés par mot de passe n'est pas encore disponible
- Uniquement sur Windows 11 22H2
 - Via une mise à jour optionnelle

<https://www.bleepingcomputer.com/news/microsoft/windows-11-adds-support-for-11-file-archives-including-7-zip-and-rar/>

Divers / Trolls velus

■ Inondez de notifs les appareils à proximité 🐼

- Possible sur Android, Windows et iOS
 - Grâce au BLE (Bluetooth Low Energy)
- “Bluetooth-LE-Spam” + Flipper Zero = "Spam Attack"
 - Diffuser des demandes de connexion via BLE toutes les secondes
 - Puissance d'émission pouvant être réglée
- Contre-mesure ?
 - Désactiver les notifications liées au partage à proximité

<https://github.com/simondankelmann/Bluetooth-LE-Spam> (outil)

Prochaine réunion ?

RDV le mardi 12 décembre

Questions ?

Des questions ?

- C'est le moment !

Des idées d'illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous



OSSIR