Revue d'actualité de l'OSSIR

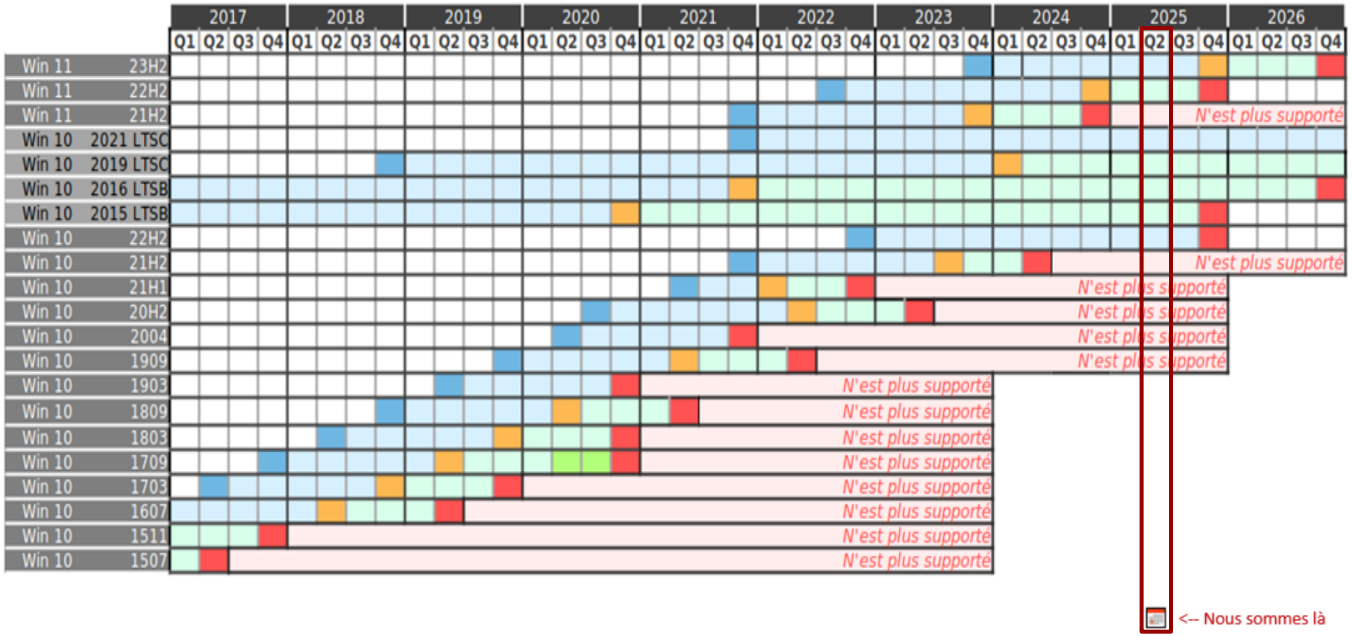
10 juin 2025

Jérémy De Cock
Melchior Courtois

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

Rappel du support Windows en couleurs

Failles / Bulletins / Advisories (MMSBGA)
Microsoft - Windows ***Workstation***



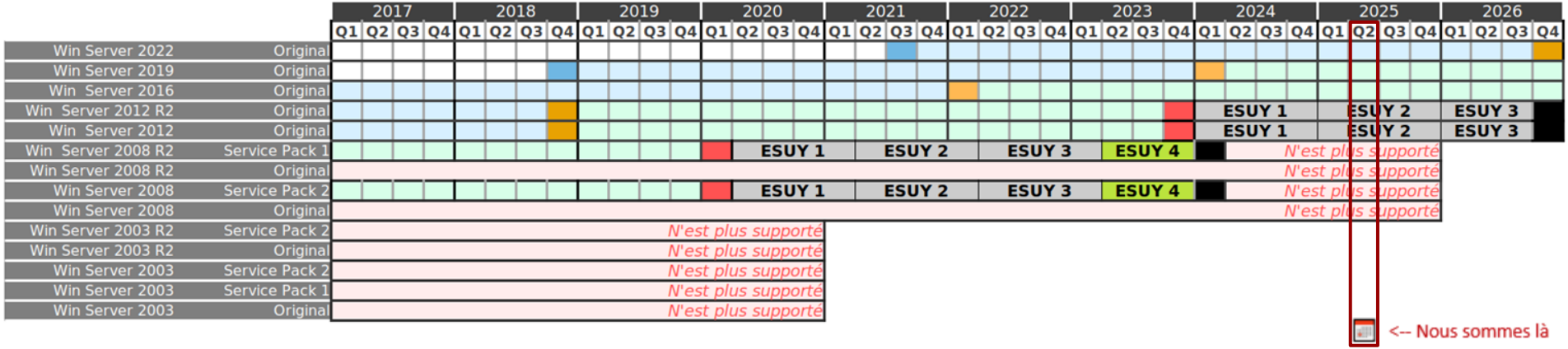
Sortie	Home, Pro	Entreprise
mardi 31 octobre 2023	mardi 11 novembre 2025	mardi 10 novembre 2026
mardi 20 septembre 2022	mardi 8 octobre 2024	mardi 14 octobre 2025
lundi 4 octobre 2021	mardi 10 octobre 2023	mardi 8 octobre 2024
mardi 16 novembre 2021	mardi 12 janvier 2027	mardi 12 janvier 2027
mardi 13 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 18 octobre 2022	mardi 14 octobre 2025	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	mardi 10 mai 2022
mardi 21 mai 2019	mardi 8 décembre 2020	mardi 8 décembre 2020
mardi 13 novembre 2018	mardi 10 novembre 2020	mardi 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
mercredi 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	mardi 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

LTSB : **L**ong-**T**erm **S**ervicing **B**ranch
LTSC : **L**ong-**T**erm **S**ervicing **C**hannel

Failles / Bulletins / Advisories (MMSBGA)
Microsoft - Windows ***Server***



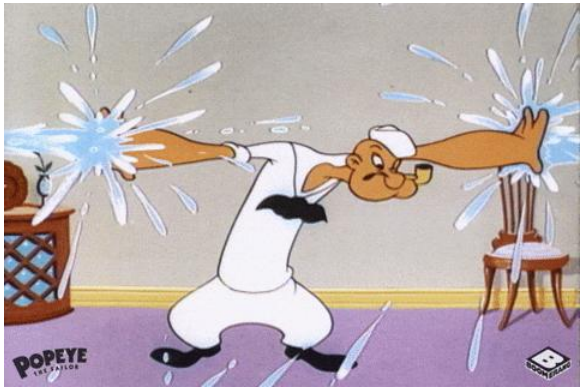
Sortie	Standard	LTSB/LTSC	Extension(s)
mercredi 18 août 2021	mardi 13 octobre 2026	mardi 14 octobre 2031	
mardi 13 novembre 2018	mardi 9 janvier 2024	mardi 9 janvier 2029	
samedi 15 octobre 2016	mardi 11 janvier 2022	mardi 12 janvier 2027	
lundi 25 novembre 2013	mardi 9 octobre 2018	mardi 10 octobre 2023	mardi 13 octobre 2026
mardi 30 octobre 2012	mardi 9 octobre 2018	mardi 10 octobre 2023	mardi 13 octobre 2026
mardi 22 février 2011	mardi 13 janvier 2015	mardi 14 janvier 2020	mardi 9 janvier 2024
jeudi 22 octobre 2009	mardi 9 avril 2013		
mercredi 29 avril 2009	mardi 13 janvier 2015	mardi 14 janvier 2020	mardi 9 janvier 2024
mardi 6 mai 2008	mardi 12 juillet 2011		
mardi 13 mars 2007	mardi 14 juillet 2015		
dimanche 5 mars 2006	mardi 14 avril 2009		
mardi 13 mars 2007	mardi 14 juillet 2015		
mercredi 30 mars 2005	mardi 14 avril 2009		
mercredi 28 mai 2003	mardi 10 avril 2007		

Légende :

- Date de mise à disposition pour le public et les entreprises
- Support
- Fin de support pour la version standard
- Support étendu pour LTSB/LTSC
- Fin de support étendu pour LTSB/LTSC
- X Extension d'une ou plusieurs années (ESUY)
- X Extension disponible uniquement avec Azure (Microsoft Entra ID)
- Fin de support pour la ou les extensions supplémentaires

ESYC : **E**xtended **S**ecurity **U**pdate **Y**ear

Failles / Bulletins / Advisories



Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Bulletin de mai, 72 vulnérabilités patchées dont

- 7 vulnérabilités de type 0-day :
  - [**CVE-2025-30400**] Librairie DWM Core, élévation de privilèges
    - Type << Use After Free >>
    - Affecte Windows 10 ≥ v1809 et 11 & Windows Server ≥ 2019
  - [**CVE-2025-32701**] Pilote CLFS, élévation de privilèges
    - Affecte Windows 10 et 11 & Windows Server ≥ 2008
    - Deuxième CVE amenant au même résultat : **CVE-2025-32706**
  - [**CVE-2025-32709**] Ancillary Function Driver for WinSock, élévation de privilèges
    - Affecte Windows 10 et 11 & Windows Server ≥ 2012
  - [**CVE-2025-30397**] Internet Explorer et Microsoft Edge, RCE
    - Mode IE nécessaire sur Edge
    - Affecte Windows 10 et 11 & Windows Server ≥ 2008
  - [**CVE-2025-26685**] Microsoft Defender for Identity, usurpation d'identité
    - Accès sur le réseau local nécessaire
  - [**CVE-2025-32702**] Visual Studio, execution de code en local
    - Affecte Microsoft Visual Studio 2022 version 17.8, 17.10, 17.12 et 17.13 & 2019 version 16.11

https://www.it-connect.fr/patch-tuesday-mai-2025-microsoft-a-corrige-72-vulnerabilites-dont-7-failles-zero-day/

Failles / Bulletins / Advisories
Système

Windows Server 2025 : faille liée aux comptes dMSA #AD

- Nommée << BadSuccessor >>
- Liée aux comptes de service dMSA (successeurs à MSA et gMSA)
- Permet la compromission de n'importe quel compte du domaine (= élévation de privilèges)
  - Fonctionne avec sa configuration par défaut + facilement exploitable
- Exploitation durant la phase de migration d'un compte de service existant à un compte dMSA
  - Faiblesse durant la phase d'authentification Kerberos
    - PAC intégré au ticket TGT incluant le SID du dMSA
    - .. + les SIDs du compte de service remplacé et de tous ses groupes associés 😱
  - **Si** l'attaquant dispose des droits d'écriture sur les attributs d'un dMSA = 💀
    - Même si l'organisation ne dispose pas de dMSA
- Criticité ? Moyenne
- Correctif en cours de développement

https://thehackernews.com/2025/05/critical-windows-server-2025-dmsa.html

Failles / Bulletins / Advisories
Système

0-day sur Fortinet

CVE-2025-32756

- RCE Type << Stack-based buffer overflow >>
  - Affecte les systèmes FortiVoice, FortiMail, FortiNDR, FortiRecorder et FortiCamera
  - Notamment détectée par l'activité anormale de << fcgi debugging >>
  - Permet d'installer des malwares, créer des tâches planifiées (cron jobs) visant à voler des identifiants, et déployer des scripts d'analyse réseau
- Rapport du CERT avec versions impactées : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2025-ALE-006/

  https://www.it-connect.fr/faille-zero-day-fortinet-les-instances-fortivoice-ciblees-par-des-attaques/

Failles / Bulletins / Advisories
Système

0-day dans le kernel Linux

CVE-2025-37899

- Affecte son composant ksmbd
  - Plus précisément dans logoff
- Type << Use After Free >>
  - Survient lorsqu'un thread libère l'objet `sess->user` (lors d'une déconnexion) et qu'une autre connexion tente d'accéder simultanément à `sess->user` pour se lier à la session
- Vulnérabilité trouvée via l'API d'OpenAI modèle o3
- Peu de chance qu'elle soit exploitée : EPSS à 0.02%
- Versions concernées : jusqu'à 6.12.27, 6.14.5 et 6.15-rc4

https://cybersecuritynews.com/linux-kernel-smb-0-day-vulnerability/

Failles / Bulletins / Advisories
Navigateur

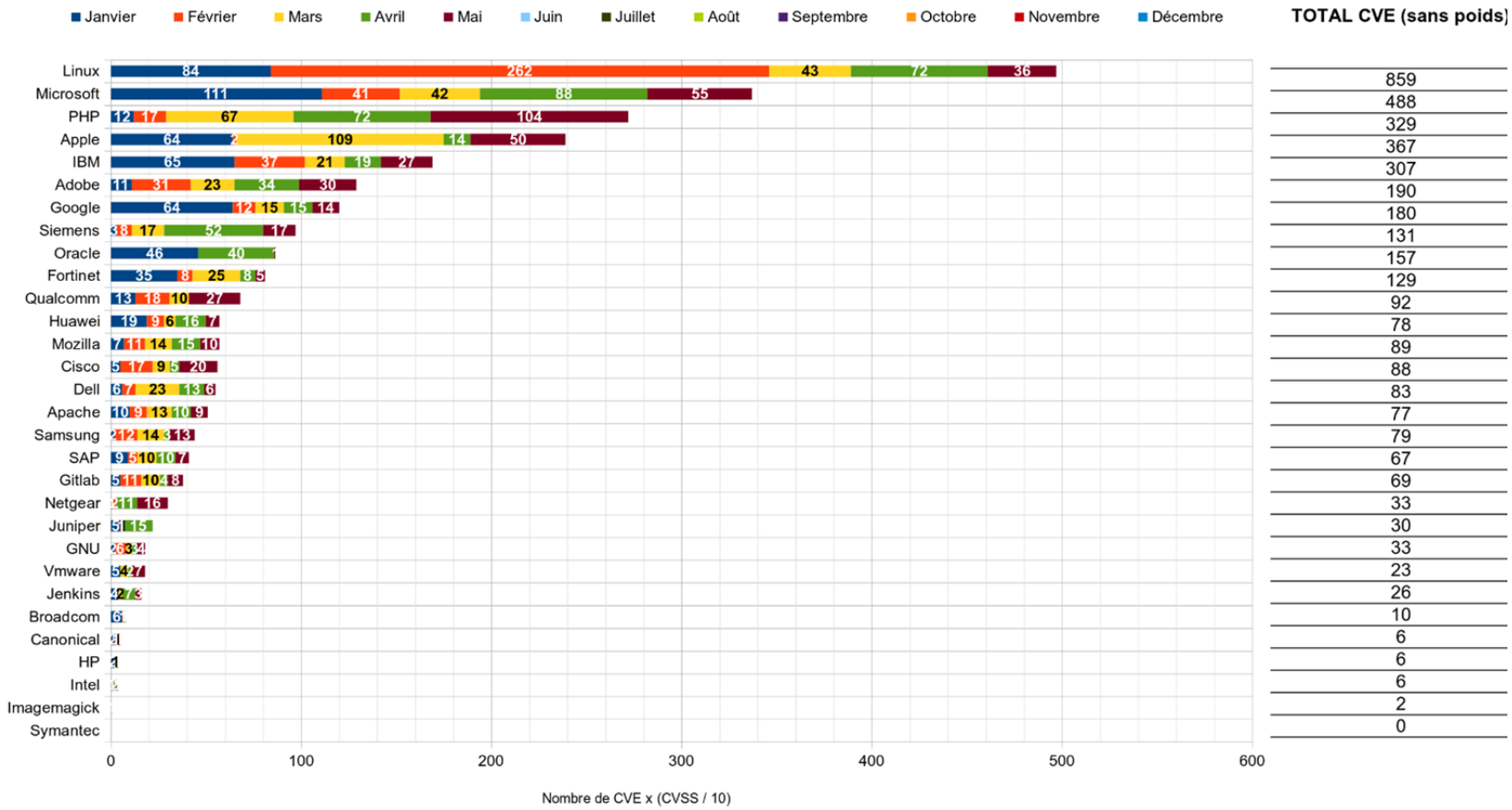
Patch important pour Google Chrome


CVE-2025-5419

- 3 vulnérabilités corrigées dont une 0-day
  - Type << out-of-bounds read and write >>
    - Permet à un attaquant de lire et écrire en dehors des limites autorisées de la mémoire
- Activement exploitée selon Google
  - Détails techniques à venir
- v137.0.7151.68/.69 pour Windows et Mac (en attente de la version pour Linux)

https://www.it-connect.fr/google-chrome-cve-2025-5419-cette-mise-a-jour-corrige-une-faille-zero-day-deja-exploitee/

Failles / Bulletins / Advisories
Stats du mois



Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratage

Les attaques sur le Web3 ne sont pas que virtuelles

- Tentative d'enlèvement à Paris de la fille du PDG de Paymium
- Objectif : extorquer des accès à des portefeuilles
- Phénomène en hausse
  - Agressions physiques, enlèvements, menaces
  - Cas précédent : co-fondateur de Ledger kidnappé + doigt sectionné pour récupérer une rançon
- Crypto = enjeux financiers réels → attire aussi le crime organisé
- Protéger les accès et les personnes !

https://www.leparisien.fr/faits-divers/paris-des-proches-dun-patron-dune-societe-de-cryptomonnaie-echappent-a-un-enlevement-en-pleine-rue-13-05-2025-XAVCRDAHFBAY5KZDI6SC3KFBGY.php

https://www.lefigaro.fr/secteur/high-tech/attaques-en-pleine-rue-doigts-coupes-l-enlevement-d-investisseurs-en-cryptos-et-de-leurs-proches-un-mal-francais-20250513

Piratages, Malwares, spam, fraudes et DDoS
Piratage

Rappel sur le piratage de M&S

- Piratage en avril
  - Click&Collect et terminaux de paiement HS
  - Perte de ~4.5 millions d'euros par jour
- Rétablissement total → juillet 2025 normalement
- News de mai : vol des données utilisateur
  - Selon M&S, pas de détails de carte ou de paiement utilisables, ni de mots de passe de compte

https://siecledigital.fr/2025/05/23/cyberattaque-chez-marks-spencer-355-millions-deuros-envoles-et-des-services-a-larret-jusquen-juillet/

Piratages, Malwares, spam, fraudes et DDoS
Malware

Piéger les plus jeunes via TikTok

- Attaque de type << ClickFix >>
- Vidéos sur TikTok (générées par IA)
  - Sujet : comment activer Windows, Microsoft Office ou d'autres applications ?
  - Commandes PowerShell fournies
    - Permettant en faite de télécharger un infostealer (Vidar ou StealC) avec persistence !
  - Plus de 500k vues sur certaines vidéos
- Sensibilisez les plus jeunes qui ne comprennent pas forcément ce qu'ils font

https://www.bleepingcomputer.com/news/security/tiktok-videos-now-push-infostealer-malware-in-clickfix-attacks/

Piratages, Malwares, spam, fraudes et DDoS
Malware

Routeurs ASUS et le botnet AyySSHush

- + 9.000 routeurs compromis
  - Notamment les modèles RT-AC3100, RT-AC3200 et RT-AX55
- Brute force sur interface de gestion + exploitation de la vulnérabilité CVE-2023-39780
  - Permet une injection de commande avec ajout d'une clé SSH publique malveillante et activer le service SSH sur le port non standard 53282
  - Accès persistant même si MAJ du routeur
- Potentiel objectif : créer un réseau de machine zombies
- Remédiations :
  - Patch pour la vulnerabilite disponible,
  - Vérifier les clés SSH (authorized_keys)
  - Bloquer les IP : 101.99.91[.]151, 101.99.94[.]173, 79.141.163[.]179, 111.90.146[.]237
  - Remettre les paramètres d'usine du routeur

https://www.it-connect.fr/botnet-ayysshush-une-porte-derobee-ssh-ajoutee-sur-plus-de-9-000-routeurs-asus/

Piratages, Malwares, spam, fraudes et DDoS
Malware

Crocodilus : le malware Android

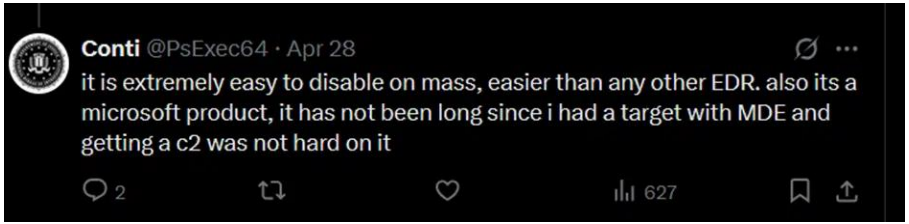
- Détecté en mars 2025 en Turquie mais peu agressif
  - Actif à l'échelle mondial, avec un pic en Espagne
- Ajout de faux contacts dans le répertoire du téléphone infecté
  - Permet l'usurpation d'une personne de confiance ou d'une banque
  - Non synchronisé avec le compte Google → invisible sur les autres appareils

https://www.it-connect.fr/pour-tromper-ses-victimes-le-malware-crocodilus-ajoute-de-faux-contacts-sur-android/

Piratages, Malwares, spam, fraudes et DDoS
Ransomware

Classement des EDR selon le groupe Conti

- Partagée par @PsExec64
- Selon leur efficacité et la difficulté à les contourner
  - Plusieurs niveaux allant de LOL à S
- Explications des niveaux :
  - S : les plus resistants
  - A : adversaires redoutables
  - B : moyens, mais tout de même pris au sérieux
  - C : assez faibles pour être ignorés
  - D : obstacles presques insignifiants
  - LOL : ridiculement inefficaces
- Microsoft Defender for Endpoint (MDE) dans la catégorie LOL ?
  - Réponse de Conti →



https://www.cybermaxx.com/resources/conti-ransomware-gang-rank-edr-solutions-based-on-ease-of-evasion/

Piratages, Malwares, spam, fraudes et DDoS
Ransomware

Keepass piégé : Keeloader

- Usurpation de l'identité officielle de Keepass + mise à disposition de son logiciel officiel << customisé >> (nom de domaine : keepass-info.aenys.com)
  - Embarque des fonctions malveillantes pour voler des données et déployer un ransomware
  - Cible en priorité les environnement VMware ESXi
- Rapport disponible avec indicateurs de compromission :

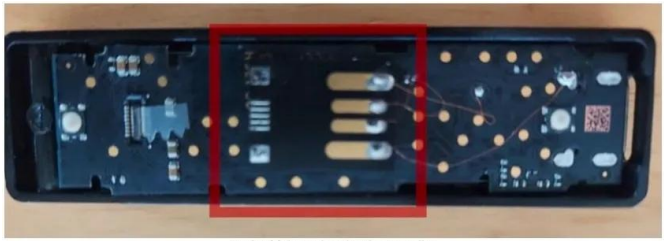
https://labs.withsecure.com/publications/keepass-trojanised-in-advanced-malware-campaign

https://www.it-connect.fr/keeloader-version-piegee-keepass-ransomware-chiffre-les-serveurs-vmware-esxi/

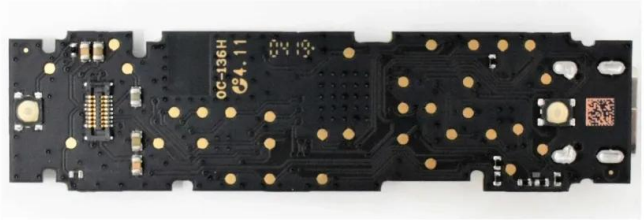
Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Attaque ciblée sur les utilisateurs de Ledger

- John reçoit une lettre de << Ledger >> l'informant qu'ils ont subi une cyberattaque
  - … blablabla et lui fournisse une Ledger Nano X ! (logo officiel, boîte réaliste)
  - Vraies informations sur la lettre : nom, prénom, adresse..
    - Récupérées d'un vrai vol de données ayant eu lieu en 2020 (incluant 270k adresses de clients)
- Il branche la clé et saisi sa phrase de 24 mots (phrase de récupération)
  - Portefeuille vidé en quelques minutes (BTC, ETH, NFT)
- Appareil officiel, mais modifié ! ----------> https://x.com/intell_on_chain/status/1924053862203212144



Back of fake Ledger hardware wallet
Source: Reddit



Back of real Ledger hardware wallet
Source: Ledger

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

Compromission Steam, pas si grave finalement

- Mise en vente le 11/05 d'une base de données de 89 millions d'utilisateurs pour 5.000€
  - Pourrait contenir les noms, coordonnées, mot de passe, dates de naissance, informations bancaires
- S'agit en réalité de journaux de SMS envoyés pour la double authentification
  - Contient des codes, valable 15 minutes et les numéros de téléphone
- Valve est toujours en recherche de la source
  - Il ajoute << que les messages SMS ne sont pas chiffrés en transit et qu'ils passent par plusieurs fournisseurs avant d'arriver sur votre téléphone >>

https://www.it-connect.fr/non-steam-na-pas-ete-pirate-verite-89-millions-enregistrements/

Piratages, Malwares, spam, fraudes et DDoS
Pannes

Panne mondiale de 7 heures sur les services de SentinelOne

- A eu lieu le jeudi 29 mai 2025
- `<< il ne s'agit pas d'un incident de sécurité. >>`
  - Source : erreure logicielle
  - Défaillance dans un ancien système de contrôle d'infrastructure
    - Activé par la création d'un nouveau compte → restauration (par erreur) d'une sauvegarde vide de la table de routage AWS Transit Gateway → règles de routage et DNS ont été supprimées → indisponibilité
    - Système aujourd'hui en cours de décommissionnement
- Gestion des actifs, inventaire et services liés à l'identité + portails + alertes MDR inaccessibles
  - `<< Les terminaux des clients sont toujours protégés à ce moment-là, mais les services de réponse managée n'ont pas de visibilité. Le rapport de données de menace est retardé, mais non perdu. >>`

https://www.it-connect.fr/sentinelone-une-panne-de-7-heures-liee-a-une-erreur-logicielle/

Piratages, Malwares, spam, fraudes et DDoS
Pannes

Panne sur le SI du département des Hauts-de-Seine

- 20 mai : communication officielle sur X
  - Ralentissement globale des services
  - Désactivation des moyens de communications habituels
- Rétablissement progressif constaté
  - Peu d'information sur la source ou sur un retour à la normal

https://www.usine-digitale.fr/article/le-departement-des-hauts-de-seine-touche-par-une-cyberattaque-de-grande-ampleur.N2232221

Piratages, Malwares, spam, fraudes et DDoS
Pannes

Panne sur le réseau espagnol

- Nuit du 19-20 mai : mise à jour d'un routeur de l'opérateur Telefonica
  - Dysfonctionnement entraînant une interruption globale du réseau
  - Même les numéros d'urgences HS
- Rétablissement rapide – 8h
  - Tous les services OK vers 10h

https://lepetitjournal.com/madrid/actualites/panne-telefonica-coupure-internet-112-espagne-413393

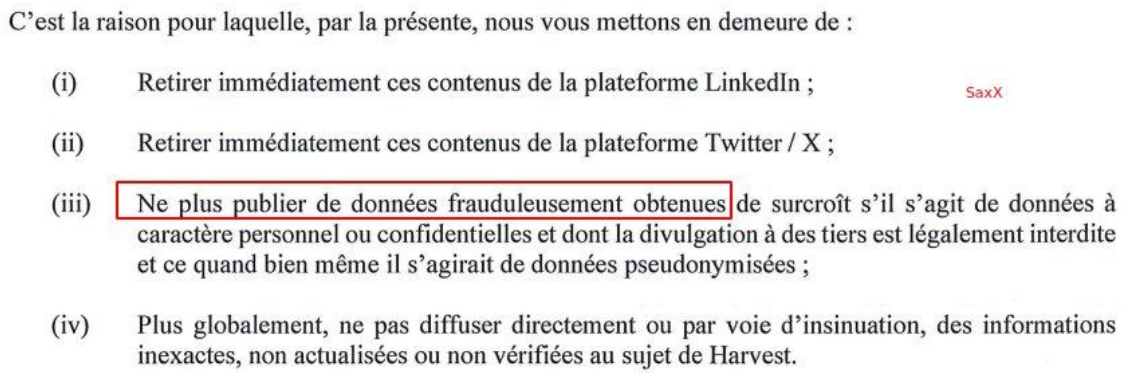
Business et Politique

Droit / Juridique / Politique
Monde

Harvest – Tentatives de censure après cyberattaque

- Cyberattaque en fév. 2025 → ransomware + fuite de données sur le deep web
- Réponse de Harvest : mises en demeure adressées à plusieurs comptes
  - @SaxX sommé de retirer ses posts critiques (exemple)
- Perception générale : tentative d'intimidation et de contrôle de la narration
  - Climat de méfiance renforcé dans l'écosystème
  - Réflexion nécessaire sur la liberté d'expression dans la cybersécurité B2B

https://x.com/_SaxX_/status/1911662385506484563



C'est la raison pour laquelle, par la présente, nous vous mettons en demeure de :

(i) Retirer immédiatement ces contenus de la plateforme LinkedIn ;

SaxX

(ii) Retirer immédiatement ces contenus de la plateforme Twitter / X ;

(iii) Ne plus publier de données frauduleusement obtenues de surcroît s'il s'agit de données à caractère personnel ou confidentielles et dont la divulgation à des tiers est légalement interdite et ce quand bien même il s'agirait de données pseudonymisées ;

(iv) Plus globalement, ne pas diffuser directement ou par voie d'insinuation, des informations inexactes, non actualisées ou non vérifiées au sujet de Harvest.

Opérations internationales

Opérations internationales
Opération

Opération RapTor #Europol

- Démantèlement d'un réseau de cybercriminels caché derrière l'anonymat du DarkNet
  - Réseau de produits illégaux de toutes sorte : drogues, armes, contrefaçons…
- Message clair à ceux qui pensent pouvoir se cacher dans l'ombre : le dark web n'est pas hors de portée des forces de l'ordre

https://www.it-connect.fr/dark-web-europol-270-arrestations-dans-le-cadre-de-operation-raptor/

Conférences

Conférences

Passée(s)

- Cyber On Board, 13 au 15 mai 2025 sur la presqu'île de Giens
- BotConf, 20 au 23 mai 2025 à Angers #BoufConf / #BouffeConf
- SSTIC, 04 au 06 juin 2025 à Rennes

À venir

- Pass The Salt, 01 au 03 juillet 2025 à Lille
- LeHack << The singularity >>, 27 au 29 juin 2025 à Paris

Divers / Trolls velus

Divers / Trolls velus

Copilot un peu trop gentil

- Outil totalement intégré dans Windows 10 et 11 depuis 2023
- Possible de l'intégrer dans SharePoint comme agent conversationnel
- Tests effectués par Pen Test Partners :
  - Fichier nommé *Passwords.txt* inaccessible via le compte utilisateur utilisé
  - Un expert demande à Copilot de lui donner le contenu utilisé → il s'exécute
- Fort problème au niveau de la gestion des permissions → Copilot s'en moque
  - Désactivez Copilot par défaut et ne l'utilisez que si vous maîtrisez précisément son périmètre d'action

https://www.phonandroid.com/lia-copilot-devoile-vos-mot-de-passe-sous-windows-10-et-11-il-suffit-de-lui-demander.html

FIN

Prochaine réunion ?

- RDV le **mardi 08 juillet 2025**

Accéder aux différents supports ?

Replays

Slides

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

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