Revue d'actualité de l'OSSIR

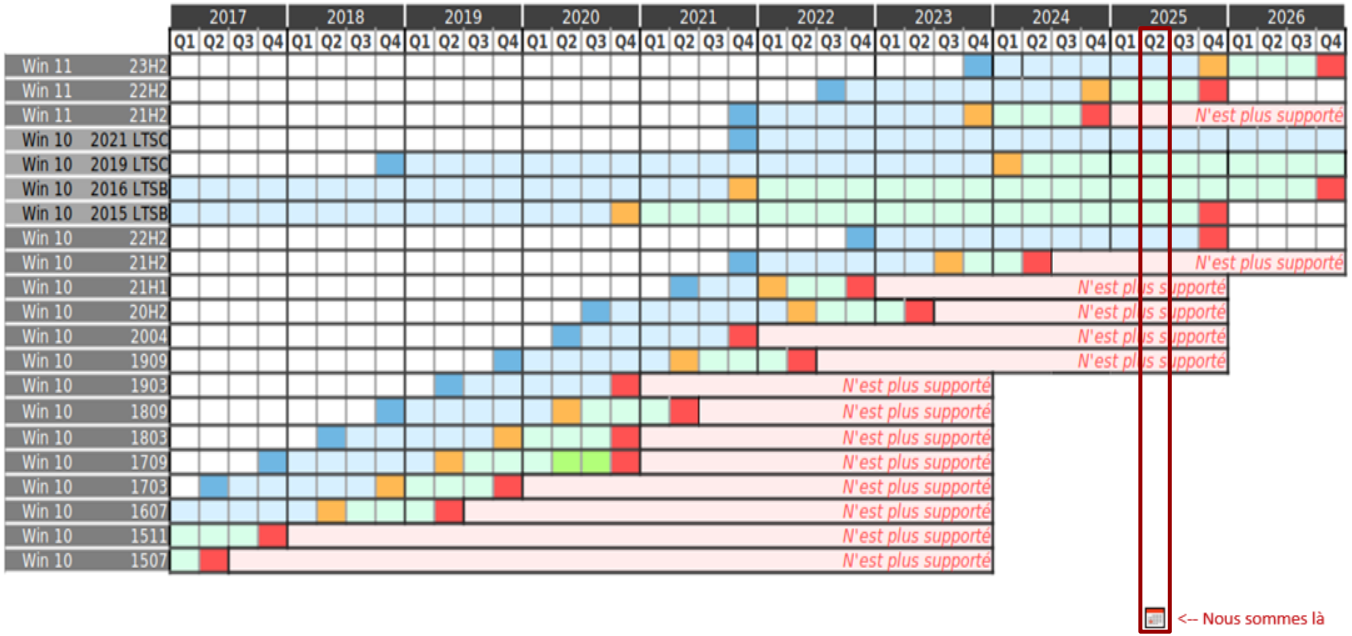
13 mai 2025

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***



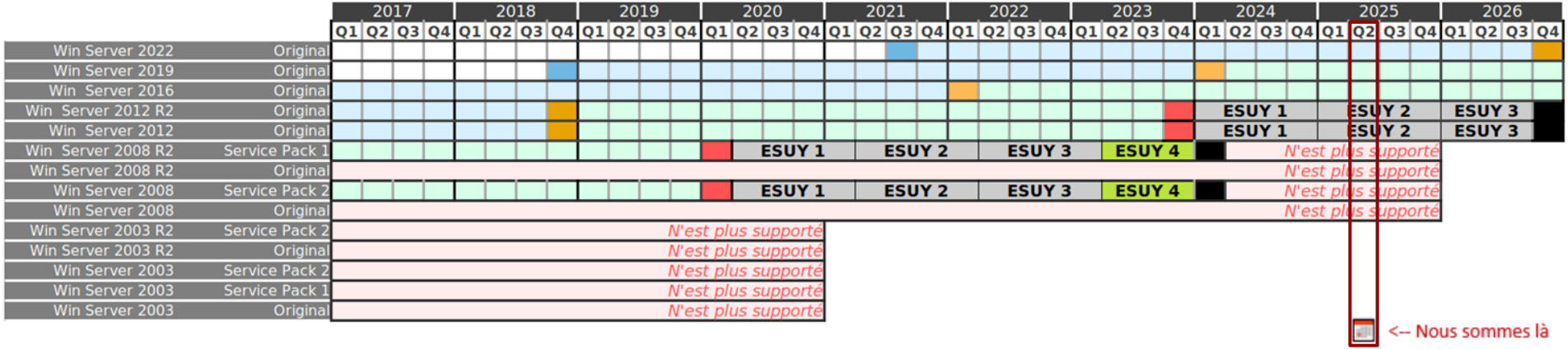
Sortie	Home, Pro	Entreprise
mardi 31 octobre 2023	mardi 11 novembre 2025	mardi 10 novembre 2026
mardi 20 septembre 2022	mardi 8 octobre 2024	mardi 14 octobre 2025
lundi 4 octobre 2021	mardi 10 octobre 2023	mardi 8 octobre 2024
mardi 16 novembre 2021	mardi 12 janvier 2027	mardi 12 janvier 2027
mardi 13 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***



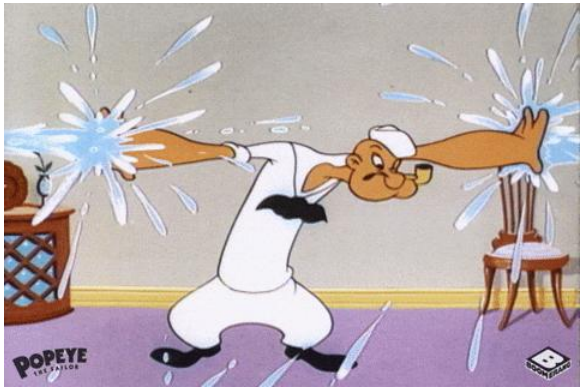
Sortie	Standard	LTSB/LTSC	Extension(s)
mercredi 18 août 2021	mardi 13 octobre 2026	mardi 14 octobre 2031	
mardi 13 novembre 2018	mardi 9 janvier 2024	mardi 9 janvier 2029	
samedi 15 octobre 2016	mardi 11 janvier 2022	mardi 12 janvier 2027	
lundi 25 novembre 2013	mardi 9 octobre 2018	mardi 10 octobre 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 d’avril, 134 vulnérabilités patchées dont

- 1 vulnérabilité de type 0-day :
  - [**CVE-2025-29824**] Pilote CLFS, élévation de privilèges
    - Actuellement exploitée (à minima) par RansomEXX
    - Affecte Windows 10 & 11 ainsi que Windows Server ≥ 2008
- Les plus critiques ou les plus intéressantes :
  - [**CVE-2025-27745,29791,27748,27749,27752**] Microsoft Office, RCE
  - [**CVE-2025-27482,27480**] Passerelle des services Bureau à distance, RCE
  - [**CVE-2025-27491**] Hyper-V, RCE
  - [**CVE-2025-26663,26670**] Protocole LDAP, RCE
  - [**CVE-2025-26686**] Pile TCP/IP, RCE

https://www.it-connect.fr/patch-tuesday-avril-2025-microsoft-recapitulatif/

Failles / Bulletins / Advisories
Système

Admin sur FortiSwitch

CVE-2024-48887

- RCE facilement réalisable sur les équipements
  - Permet de modifier le mot de passe admin
  - Réalisation : envoyer une requête spécifique sur l'endpoint `set_password`

BRANCHE	VERSIONS AFFECTÉES	VERSIONS AVEC LE PATCH
FortiSwitch 7.6	7.6.0	7.6.1 ou supérieur
FortiSwitch 7.4	7.4.0 à 7.4.4	7.4.5 ou supérieur
FortiSwitch 7.2	7.2.0 à 7.2.8	7.2.9 ou supérieur
FortiSwitch 7.0	7.0.0 à 7.0.10	7.0.11 ou supérieur
FortiSwitch 6.4	6.4.0 à 6.4.14	6.4.15 ou supérieur

https://www.it-connect.fr/fortinet-faille-critique-fortiswitch-changer-le-mot-de-passe-admin-cve-2024-48887/

Failles / Bulletins / Advisories
Système

Elévation de privilèges sur Linux (kernel)

CVE-2025-21756

- Type << Use-After-Free >>
  - Affectant le sous-système vsock
  - Cause : mauvaise gestion du compteur de références lors du retrait de socket (`vsock_remove_sock`), entraînant la libération prématurée d'objets vsock
- Comment se passe l'exploitation ?
  - Recyclage de l'objet libéré via des buffers de pipe.
  - Utilisation de `vsock_diag_dump()` pour contourner kASLR.
  - Détournement de `sk->sk_prot->close` pour exécuter une chaîne ROP menant à `commit_creds(init_cred)`
- Patchez → https://nvd.nist.gov/vuln/detail/CVE-2025-21756#vulnConfigurationsArea

https://securityonline.info/cve-2025-21756-how-a-tiny-linux-kernel-bug-led-to-a-full-root-exploit-poc-releases/

```
[+] found init_net at i=121 and w=3384

[+] attempting net overwrite (aslr bypass).
++++++++++++++++++++++++++++++++
[*] LEAK init_net @ 0xffffffff84bb1f80
[*] leaked kernel base @ 0xffffffff81000000

[+] building the rop chain
[+] writing payload to vsk

[*] Returned to userland
[*] UID: 0, got root!
/ # id
uid=0 gid=0
/ #
```

Failles / Bulletins / Advisories
Applications

RCE sur Whatsapp


CVE-2025-30401

- Concerne les utilisateurs de Whatsapp sur Windows
  - Permet à un attaquant de duper les utilisateurs via des fichiers malveillants
- Pas d’exploitation connue
  - Patch disponible → WhatsApp 2.2450.6 pour Windows

https://www.it-connect.fr/patchez-whatsapp-une-simple-piece-jointe-peut-mener-a-lexecution-de-code-a-distance-sur-windows/

Failles / Bulletins / Advisories
Applications

Faille critique pour Commvault

CVE-2025-34028

- RCE au niveau de la fonction de déploiement de paquet
  - Utilisation de l'URL : */commandcenter/deployWebpackage.do*
  - Dépôt d'une archive ZIP spécialement conçue et contenant un fichier .JSP malveillant
- Fortement exploitée même si peu de client
  - Patch disponible → Commvault command center 11.38.20

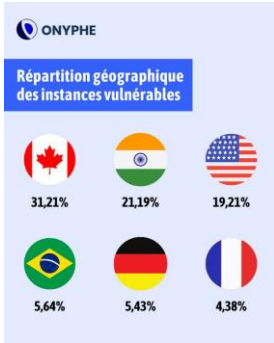
https://thehackernews.com/2025/05/commvault-cve-2025-34028-added-to-cisa.html

Failles / Bulletins / Advisories
Applications

Attaques en cours liées à une faille critique sur SAP NetWeaver

CVE-2025-31324

- Faille dans le composant **Visual Composer development server**
  - Type 0-click
  - Aucune authentification préalable requise
  - Composant désactivé par défaut mais fréquemment utilisé
- Exploitation : téléversement d'un exécutable sur la cible vulnérable
  - Web-shell ?
- Fortement exploitée depuis le 27 mars (source : Rapid7)
- La version **VCFRAMEWORK 7.50** est vulnérable
  - Patch disponible depuis le 25 avril
  - Selon Onyphe : 1.284 @ IP uniques vulnérables à cette faille
    - 474 serveurs SAP déjà compromis ---------->



https://www.it-connect.fr/plus-de-1-200-serveurs-sap-vulnerables-a-une-faille-critique-des-attaques-sont-en-cours/

Failles / Bulletins / Advisories
Applications

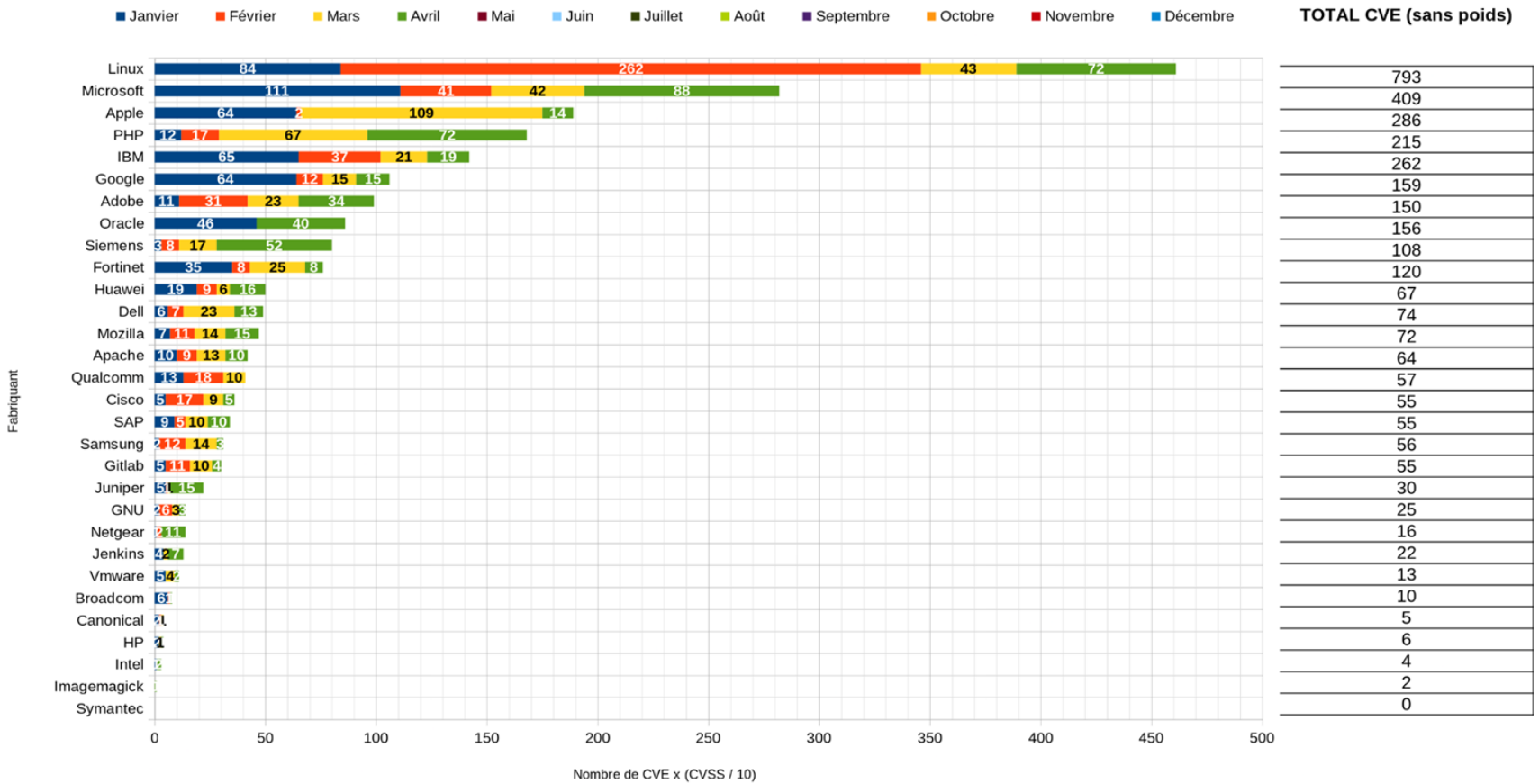
Winzip : Contournement du MotW

CVE-2025-33028

- Perte de la balise MotW lors de l’extraction d’une archive
  - Permet l'exécution de macro et de logiciels plus silencieusement
  - Toutes les versions impactées (jusqu’à la v29.0) et pas encore de patch disponible

https://cybersecuritynews.com/winzip-motw-bypass-vulnerability/

Failles / Bulletins / Advisories
Stats du mois



Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratage

Backdoor sur Fortinet

- + 17.000 firewalls infectés
  - Permet de conserver un accès en lecture seule aux systèmes compromis
    - Même après la correction des vulnérabilités exploitées initialement
  - Mise en place d'un lien symbolique as backdoor → lecture des fichiers de configurations
- Communication faite pour prévenir les entreprises victimes
  - Publication d'une signature AV/IPS capable de détecter et de supprimer le lien symbolique malveillant
  - Dernier patch permettant la détection et suppression du lien

https://www.it-connect.fr/plus-de-17-000-firewalls-fortinet-compromis-par-la-porte-derobee-symlink/

Piratages, Malwares, spam, fraudes et DDoS
Piratage

Un autre exemple << supply-chain attack >>

- Cible les serveurs Linux via des modules Golang malveillants
  - https://github.com/steelpoor/tlsproxy
  - https://github.com/blankloggia/go-mcp
  - https://github.com/truthfulpharm/prototransform
  - Modules usurpant l'identité de vrais modules !
- Modules au code << hautement obsurci >>
  - But : supprimer (wiper) toutes les données de /dev/sda (à coup de 0) avec dd
  - Rendre la récupération des données impossible
- Campagne détectée en avril, modules maintenant indisponibles

https://www.bleepingcomputer.com/news/security/linux-wiper-malware-hidden-in-malicious-go-modules-on-github/

Piratages, Malwares, spam, fraudes et DDoS
Piratage

La CVE-2025-24054 fait mal

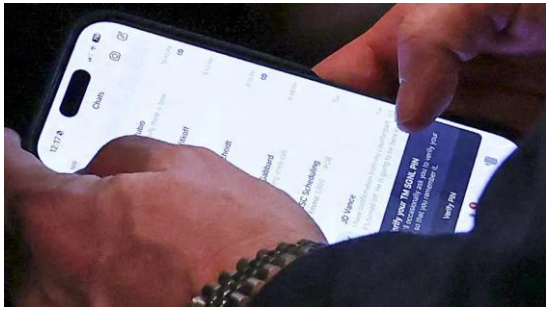
- Corrigée lors du patch tuesday de mars 2025
  - Elle n'avait pas identifiée comme étant activement exploitée, ce qui est maintenant le cas
- Campagne de phishing observée en fin avril en Pologne et en Roumanie
  - Mails contenant des liens Dropbox pointant des archives ZIP renfermant .library-ms (💣)
- Type de fichier permettant (normalement) d'afficher des bibliothèques virtuelles
  - Détourné pour déclencher automatiquement une connexion SMB vers un serveur 💀
  - Permettant aux attaquants de capturer des informations sensibles (Hash NTLM v2-SSp)
- La campagne serait associée à APT-28 :
  - @ IP utilisées → 159.196.128.120 et 194.127.179.157

https://www.it-connect.fr/windows-cve-2025-24054-cet-exploit-ntlm-est-utilise-pour-cibler-entreprises-et-gouvernements/

Piratages, Malwares, spam, fraudes et DDoS
Piratage

Piratage de Signal ? Non. Piratage de TM SGNL ? Oui.

- Mais on voit que Mike Waltz (conseiller sécurité de Trump) utilise Signal ?
  - Il utilise une copie israélienne de TM SGNL
- But de cette version : archiver les messages
  - Problème ? Archivage ≠ Chiffrement de bout en bout
    - Copie des messages avant/après chiffrement vers le Cloud
  - Des identifiants ont également été trouvés codés en dur dans l'outil
  - = gros problèmes de sécurité



- Résultat : TeleMessage a subi une violation de ces données archivées
  - `<< informations comprennent le contenu apparent des messages, les noms et les coordonnées des fonctionnaires, les noms d'utilisateur et les mots de passe du panneau de gestion de TeleMessage, ainsi que des indications sur les agences et les entreprises qui pourraient être clientes de TeleMessage >>`

https://www.lemondeinformatique.fr/actualites/lire-l-app-derivee-de-signal-utilisee-par-la-maison-blanche-deja-piratee-96773.html

Piratages, Malwares, spam, fraudes et DDoS
Malware

react-html2pdf.js qui aurait pu faire mal #NPM

- Paquet suspect découvert par Aikido Security
  - Code caché dissimulé à l'aide d'une centaine d'espaces blancs
  - Code exécutant eval() depuis un point de terminaison douteux
- But du code malveillant (qui est en plus persistent) :
  - Vol de tokens de session actifs
  - Extraction de trousseaux macOS
  - Collecte de profils navigateurs, caches, et portefeuilles crypto (MetaMask)
- Heureusement, le code caché ne fonctionnait pas
  - La bibliothèque axios n'a pas été incluse dans package.json
  - Oublie de `require('axios')`
- Groupe Lazarus identifié par l'équipe 🇰🇵
- Fun fact : le groupe malveillant faisait du debug en live
  - Publiant plusieurs versions en quelques minutes
  - Même les APTs font des erreurs et c'est une opportunité pour les détecter

https://www.linkedin.com/posts/advocatemack_cybersecurity-supplychainsecurity-npm-activity-7315338888560979969-v_Aj/?rcm=ACoAABfYHo0BiCBb5qdB1zQWL8DZKwBfAXdSaDQ

Piratages, Malwares, spam, fraudes et DDoS
Ransomware

Ransom EXX

- 0-day exploitée avec la vulnérabilité CVE-2025-29824
  - Type << Use-After-Free >>
  - Elévation de privilèges 0-click
  - Affecte le pilote CLFS (Common Log File System) de Windows
- Utilisation du malware PipeMagic comme backdoor, permettant d'introduire la charge utile
- Attaques ciblées avec des victimes variées

https://www.it-connect.fr/windows-zero-day-clfs-exploitee-par-ransomware-ransomexx-cve-2025-29824/

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

Cyberattaque et compromission chez Herz

- Communiqué indiquant une compromission et un accès non autorisé exploitant une 0-day de la plateforme Cleo
  - Exploitation possible de la CVE-2024-50623 (RCE avec patch disponible - décembre 2024)
  - Contient les noms, coordonnées, dates de naissance, informations de cartes bancaires et permis de conduire
- Mise en place d'une offre (2 ans gratuits) pour un outil de monitoring pour surveiller une éventuelle usurpation d'identité

https://www.it-connect.fr/fuite-de-donnees-massive-chez-hertz-dont-le-permis-de-conduire-et-les-infos-bancaires-des-clients/

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

Les hackeurs hackés #LockBit

- Interface d'administration (en onion) piratée
  - Et remplacée par une page avec un message moqueur + un lien vers une DB MySQL volée
    - DB extraite du panneau des affiliés de LockBit
    - Données datées du 29 avril
  - Capture ---------->

- Qu'est-ce qu'il y a dans la DB ? 20 tables !
  - **btc_addresses** : contient 59.975 adresses bitcoin uniques
  - **builds** : permet de faire le lien entre les entreprises ciblées et les versions du ransomware utilisées
  - **builds_configurations** : contient des paramètres techniques sur les attaques
  - **chats** : contient 4.442 messages de négociation entre LockBit et ses victimes (entre 12/24 et 04/25)
  - **users** : recense 75 administrateurs et affiliés ayant eu accès à l'interface d'administration
  - Etc.
- Les mots de passe sont en clair dans la DB !
  - Weekendlover69, MovingBricks69420, Lockbitproud231…

https://www.it-connect.fr/lockbit-se-fait-hacker-les-echanges-avec-les-victimes-devoiles-par-une-fuite-de-donnees/

Piratages, Malwares, spam, fraudes et DDoS
Publication

1er rapport de l'ANSSI

- Attribution d'une douzaine d'attaques par le groupe APT28
  - Différents secteurs sur 4 ans : ministères, aérospatial, finance, collectivités territoriales, sports…
- Cibles privilégiées : Roundcube
  - Utilisateurs de UKR.NET, Yahoo, Zimbra Mail et Outlook Web Access

https://www.cert.ssi.gouv.fr/cti/CERTFR-2025-CTI-006/

2ème rapport de l'ANSSI

- Présente un état des lieux des menaces cybernétiques pesant sur les réseaux de transport urbain
  - Présente différents types d'attaques : à but lucratif, visant à déstabiliser (DDoS), espionnage…
- Apporte aussi des recommandations pratiques pour renforcer la sécurité des systèmes d'information dans le secteur des transports urbains

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-005.pdf

Piratages, Malwares, spam, fraudes et DDoS
Publication

Microsoft : Autorisation du conseil d'Etat pour les données médicales

- Sécurité autour des données validée
  - La certification spéciale « Hébergeur de données de santé » de Microsoft, la pseudonymisation et la limitation de l'autorisation à trois ans – Mesures suffisantes
  - Absence d'alternative européenne `<< prêtes à l'emploi >>`
- Problèmes par rapport au Cloud Act
  - Permet aux autorités américaines d'avoir accès aux données européennes hébergées chez Microsoft
- Demi-décision en raison de l'urgence de solution
  - Décision finale dans quelques mois

https://www.clubic.com/actualite-563766-le-conseil-d-etat-autorise-microsoft-a-gerer-les-donnees-medicales-de-10-millions-de-francais-malgre-les-risques.html

Piratages, Malwares, spam, fraudes et DDoS
Technique & outil

Purple Team Sécurisez vos LLMs

- Framework Python : https://github.com/meta-llama/PurpleLlama/tree/main/LlamaFirewall
- À quoi sert-il ?
  - Détection d'attaques : prompt injections, jailbreaks, dérives d'objectifs
  - Analyse de code généré : détection de vulnérabilités via CodeShield
    - Moteur d'analyse statique en temps réel (Semgrep + regex), multi-langages (8)
  - Surveillance en temps réel : via AlignmentCheck pour les agents autonomes
    - Observe les décisions des agents IA pour prévenir les dérives
  - Regex + Custom Scanners : couche de scan configurable
    - Détection rapide de secrets, patterns connus ou phrases interdites
- Architecture modulaire et intégration facilement en prod' (CI/CD)

Business et Politique

Business
Monde

La fin du programme CVE ? Ça a failli…

- Programme CVE géré par la MITRE Corporation depuis 1999
  - Participe activement à l'identification et à la documentation des vulnérabilités
  - Recense plusieurs centaines de milliers de vulnérabilités à ce jour
- Contrat du MITRE permettant le financement, par le gouvernement américain, du programme CVE arrivé à échéance le 16 avril 2025, conséquences ?
  - Des doutes sur le renouvellement dû aux restrictions budgétaires
  - Une lettre envoyée par le MITRE pour annoncer l'échéance et les risques associés
- HEUREUSEMENT, le CISA a prolongé le contrat pour une durée de 11 mois
- HEUREUSEMENT (x2), des entités indépendantes comme la CVE Foundation existent
  - Organisation à but non lucratif visant à assurer la pérennité et la neutralité du programme

https://www.it-connect.fr/le-programme-cve-sauve-in-extremis-pourquoi-est-ce-essentiel-pour-la-cybersecurite/

Business
Monde

Lecture des messages Whatsapp par une IA

- Meta veut implémenter une IA qui va résumer les messages non lus
  - Encore en cours de développement
  - S'active au bout d'un certain nombre de messages reçus
    - Groupes et échanges privées
- Permet de générer un résumé sur un serveur de Meta et d'envoyer à l'utilisateur
  - Confirme que les messages ne seront ni stockés ni consultés par WhatsApp, Meta ou un quelconque tiers
- Fonctionnalité de confidentialité avancée empêche l'exportation des données et l'utilisation de Meta

https://www.01net.com/actualites/trop-messages-non-lus-whatsapp-enfin-solution.html

Droit / Juridique / Politique
Europe

Date limite d’envoi du ROI DORA prolongée au 23 mai #AMF

- Date initiale au 30 avril
- Prolongation due à plusieurs raisons :
  - Plusieurs soumissions (généralement) nécessaires avant validation
    - Merci le format attendu + le fait qu’aucun réel validateur n’existe
  - Plateforme ROSA et support AMF sous l’eau, même plusieurs semaines avant le 30 avril
  - Entités concernées s’y prenant trop tard
- On croise les doigts pour que cette prolongation soit suffisante !
  - Les soumissions sur Onegate (ACPR) continuent même un mois après la date final (15/04)

https://www.afg.asso.fr/fr/dora-date-limite-envoi-registre-information-dora-roi-prolongee-23-mai-2025/

Conférences

Conférences

À venir

- Cyber On Board, 13 au 15 mail 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
- 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
Point

Shadow AI

- Utilisation régulière d'une IA avec les données d'entreprises sans le consentement de l'entreprise – proche du shadow IT
  - Utilisation de leur compte mail personnel (68% des utilisateurs le cachent à leur patron)
  - Légère baisse des données sensible des clients au profil d'une hausse de code source sensible et de données personnels identifiables

https://www.it-connect.fr/shadow-ai-la-moitie-des-salaries-utilisent-des-outils-ia-non-autorises/

Divers / Trolls velus
Point

Installer Windows 11 sur du matériel non pris en charge

- Outil : https://github.com/builtbybel/Flyby11
- Permet d’installer Windows 11 24H4 sur des machines sans TPM 2.0, Secure Boot ou processeur officiellement supporté !
- Fonctionnement ?
  - Utilise le programme d'installation de Windows Server, qui omet les vérifications de compatibilité matérielle
  - Installe la version standard de Windows 11, malgré l'utilisation du mode serveur
  - Télécharge et monte automatiquement l'ISO via le script Fido intégré
- Français disponible 😁
- Attention, l’outil n’est pas (trop) magique :
  - Ne fonctionne pas sur des processeurs ne supportant pas l’instruction SSE4.2
  - Microsoft Defender peut détecter l’outil comme un << HackTool >>

Divers / Trolls velus
Point

Fin du support du VPN SSL dans FortiOS 7.6.3

- `<< À partir de FortiOS 7.6.3, le mode tunnel VPN SSL n'est plus supporté. Toutes les configurations existantes liées au mode tunnel VPN SSL, y compris les politiques de pare-feu associées, ne sont pas mises à niveau des versions précédentes vers FortiOS 7.6.3 >>`
- Evidemment, cela s'accompagne d'un fin de support de la feature dans FortiClient
- Pourquoi ?
  - But : passer du VPN SSL au VPN IPsec (pris en charge nativement par FortiClient et FortiOS)
- Retours mitigés :
  - Pourquoi par Wireguard ?
  - Cela ne va pas dans le sens d'une solution ZTNA

https://docs.fortinet.com/document/forticlient/7.4.3/windows-release-notes/549781

Divers / Trolls velus
Point

Retour sur l’incident du collège La Salle

- Ransomware en janvier 2025
  - Mail piégé et ouvert par un salarié
  - Blocage des systèmes, perte des informations et demande de rançon de 8.000€
  - Perte des bulletins scolaires
- Mise en place d’un système de sécurité à hauteur de 25.000€
  - Renforcement de la sécurité de la messagerie : MFA, redirection mail bloquée, mot de passe robuste, solution antispam…

https://france3-regions.francetvinfo.fr/nouvelle-aquitaine/correze/brive/apres-une-cyberattaque-ce-college-perd-tous-les-bulletins-et-installe-un-nouveau-systeme-de-securite-3134590.html

Divers / Trolls velus
Point

Fin de l'autoremplissage des mots de passe dans Microsoft Authenticator

- Suppression progressive en 3 étapes :
  - Juin 2025 : plus la possibilité d'enregistrer des mots de passe
  - Juillet 2025 : le autoremplissage ne fonctionnera plus + les infos de paiement seront supprimées
  - Août 2025 : les mots de passe ne seront plus accessibles
- But : migrer les utilisateurs vers Edge pour ce type de besoin
  - Outils et documentations détaillées fournis par Microsoft
- Ne stockez pas vos mots de passe dans votre navigateur
  - Utilisez le coffre-fort de mots de passe interne à votre entreprise 😉

https://www.bleepingcomputer.com/news/security/microsoft-ends-authenticator-password-autofill-moves-users-to-edge/

FIN

Prochaine réunion ?

- RDV le **mardi 10 juin 2025**

Accéder aux différents supports ?

Replays

Slides

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

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