Revue d'actualité de l'OSSIR

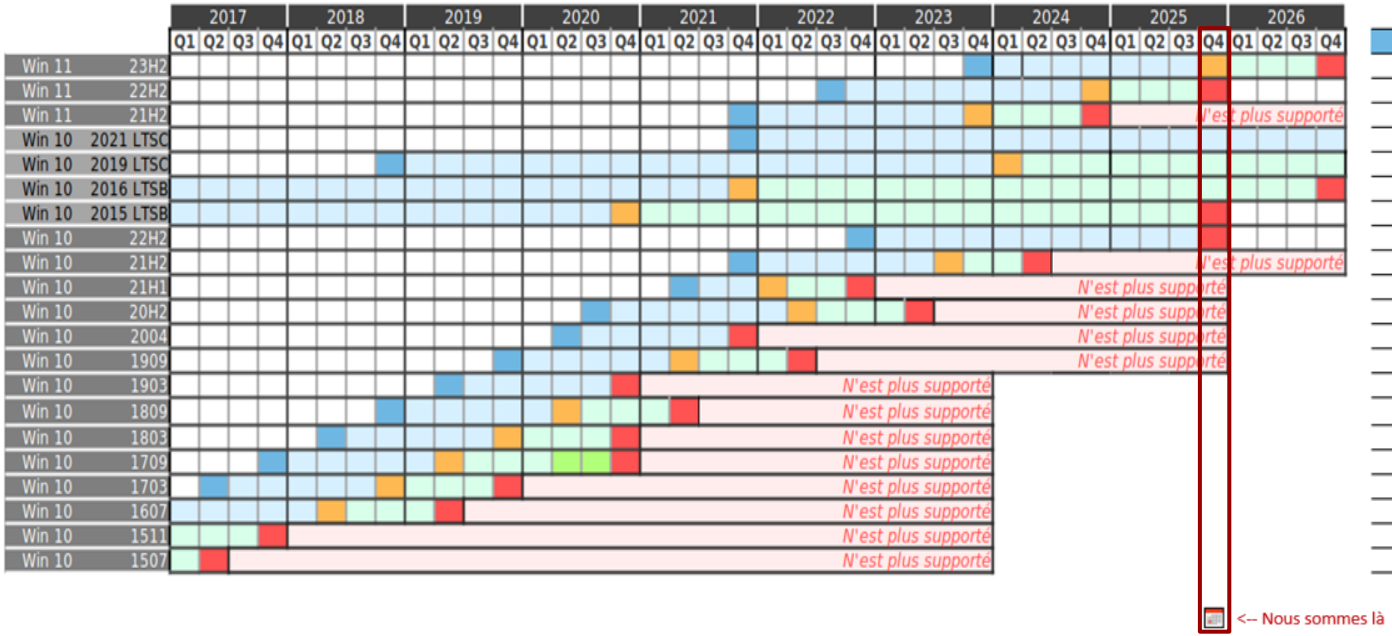
12 novembre 2025

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***



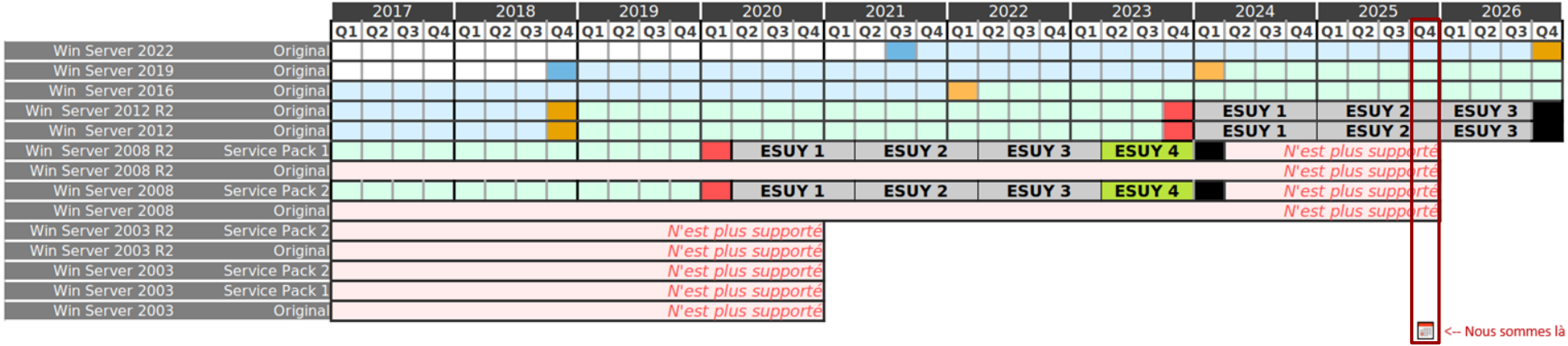
Sortie	Home, Pro	Entreprise
mardi 31 octobre 2023	mardi 11 novembre 2025	mardi 10 novembre 2026
mardi 20 septembre 2022	mardi 8 octobre 2024	mardi 14 octobre 2025
lundi 4 octobre 2021	mardi 10 octobre 2023	mardi 8 octobre 2024
mardi 16 novembre 2021	mardi 12 janvier 2027	mardi 12 janvier 2027
mardi 13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



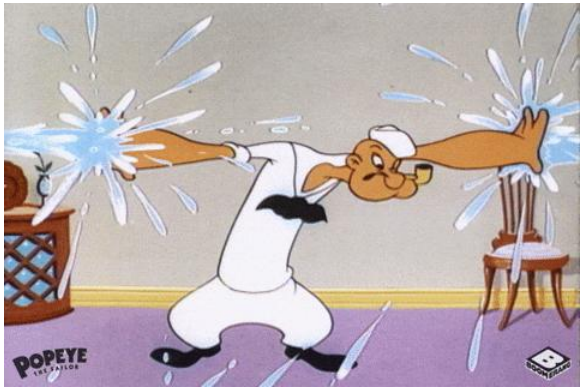
Sortie	Standard	LTSB/LTSC	Extension(s)
mercredi 18 août 2021	mardi 13 octobre 2026	mardi 14 octobre 2031	
mardi 13 novembre 2018	mardi 9 janvier 2024	mardi 9 janvier 2029	
samedi 15 octobre 2016	mardi 11 janvier 2022	mardi 12 janvier 2027	
lundi 25 novembre 2013	mardi 9 octobre 2018	mardi 10 octobre 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'octobre, 172 vulnérabilités patchées dont

- 6 vulnérabilités de type **0-day** :
  - [**CVE-2025-24990** & **CVE-2025-24052**] Elévation de privilèges, pilote Agere Modem
    - Le pilote (associé au fichier *ltmdm64.sys*) a été supprimé de Windows
    - Affecte Windows 10 et 11 & Windows Server
  - [**CVE-2025-59230**] Elévation de privilèges, composant Remote Access Connection Manager
    - Affecte Windows 10 et 11 & Windows Server
  - [**CVE-2025-47827**] Bypass du Secure Boot, IGEL OS
    - Affecte les versions antérieures à la 11
  - [**CVE-2025-0033**] Compromission de l'intégrité mémoire, AMD SEV-SNP
    - Affecte les processeurs AMD EPYC utilisés dans les VM Azure Confidential Computing (ECasv5/ECadsv5)
    - N'affecte pas Windows hors de ce périmètre Azure
  - [**CVE-2025-2884**] Leak d'informations ou déni de service, TCG TPM 2.0
    - Exploitation locale et complexe
    - Affecte Windows 10 & Windows Server 2022 et 2025
- À cela s'ajoute 56 vulnérabilités patchées liées à **Mariner**

https://www.it-connect.fr/patch-tuesday-octobre-2025-172-failles-de-securite-corrigees-dont-6-zero-day/

Failles / Bulletins / Advisories
Système

7 0-day corrigées par QNAP

- Vulnérabilités découvertes lors de la Pwn2Own Ireland 2025
- Liées :
  - aux OS utilisés pour les NAS QNAP
    - QTS / QuTS Hero → **CVE-2025-62847**, **CVE-2025-62848** et **CVE-2025-62849**
  - quelques applications phares utilisées sur les NAS
    - Hyper Data Protector → **CVE-2025-59389**
    - Malware Remover → **CVE-2025-11837**
    - HBS 3 Hybrid Backup Sync → **CVE-2025-62840** et **CVE-2025-62842**
- Toutes considérées comme critiques !
- Patchez (et n'exposez pas vos NAS) :

Versions affectées	QTS 5.2.x	QuTS hero h5.2.x	QuTS hero h5.3.x	Hyper Data Protector	Malware Remover	HBS 3 Hybrid Backup Sync
Versions patchées	5.2.7.3297 build 20251024 et supérieur	h5.2.7.3297 build 20251024 et supérieur	h5.3.1.3292 build 20251024 et supérieur	2.2.4.1 et ultérieur	6.6.8.20251023 et ultérieur	26.2.0.938 et ultérieur

https://www.bleepingcomputer.com/news/security/qnap-fixes-seven-nas-zero-day-vulnerabilities-exploited-at-pwn2own/

Failles / Bulletins / Advisories
Système

Privesc sur Windows SMB


CVE-2025-33073

- Permet d'obtenir les privilèges SYSTEM
  - Affecte les Windows 10, 11 (sauf 25H2) et Windows Server (2008 à 2025)
- Corrigée dans le patch Tuesday de juin 2025
  - Considérée par Microsoft comme une faille 0-day, connue publiquement, mais non exploitée
- Activement exploitée maintenant
  - Enregistré par le CISA dans le KEV
  - Mise à jour exigée au 10 novembre max. pour les agences fédérales américaines

https://www.it-connect.fr/windows-cve-2025-33073-la-cisa-alerte-sur-une-faille-smb-activement-exploitee/

Failles / Bulletins / Advisories
Système

TP-Link : rapport de 4 CVE

CVE-2025-6541
CVE-2025-6542
CVE-2025-7850
CVE-2025-7851

- Affecte les équipements TP-Link Omada
  - CVE-2025-6541 : RCE unauthenticated
  - CVE-2025-6542 : RCE via le portail d'administration web
  - CVE-2025-7850 : Injection de commande sur le portail web, disposant des identifiants admin
  - CVE-2025-7851 : Obtention d'un shell dans certaines conditions (non précisées)
- Tableau récapitulatif des équipements vulnérables en lien
  - Pas d'information sur une exploitation mais patch recommandé

https://www.it-connect.fr/tp-link-passerelles-omada-failles-de-securite-octobre-2025/

Failles / Bulletins / Advisories
Système

3 CVE critiques sur Bind9

CVE-2025-8677
CVE-2025-40778
CVE-2025-40780

- Peuvent être exploitées à distance sans authentification
  - CVE-2025-8677 : Exploite les enregistrements DNSKEY mal formés pour provoquer un épuisement des ressources en raison d'une surcharge du processeur
  - CVE-2025-40778 : Permet aux attaquants d'injecter des enregistrements DNS falsifiés dans le cache d'un résolveur
  - CVE-2025-40780 : Abuse d'une faiblesse du générateur de nombres pseudo-aléatoires de Bind, permettant aux attaquants de prédire les ports sources et les identifiants de requête
- Pas d’exploitation et de patch disponible

https://gbhackers.com/bind-9-vulnerabilities-expose-dns-servers/

Failles / Bulletins / Advisories
Système

Linux, un faille activement exploitée


CVE-2024-1086

- Type << Use after free >> dans le composant Netfilter du noyau Linux
  - Faille présente depuis 2014 et corrigée en janvier 2024
  - Affecte les versions du noyau Linux 5.14 à 6.6 avec PoC disponible
- Permet de prendre le contrôle de la machine victime, de réaliser des mouvements latéraux sur le réseau et de déployer un ransomware
- Exigence de la CISA de mettre à jour ses systèmes vulnérables avant le 20 juin
  - Normalement fait pour les agences fédérales

https://www.it-connect.fr/faille-noyau-linux-cve-2024-1086-attaques-ransomwares/

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

Multiples failles dans Teams


CVE-2024-38197

- Ensemble de vulnérabilité présenté dans le rapport de Check Point Research
  - Édition invisible des messages
  - Usurpation d'identité via les notifications
  - Modification du nom affiché dans les discussions privées
  - Usurpation d'identité lors d’un appel audio ou vidéo
- Vulnérabilités connues depuis mars 2024
  - Début des correctifs : août 2024
  - Dernier correctif : octobre 2025

https://www.it-connect.fr/microsoft-teams-usurpation-identite-cve-2024-38197/

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

Vulnérabilité << SessionReaper >> dans Adobe Commerce


CVE-2025-54236

- Correctif de sécurité sorti le 9 septembre 2025
  - Vulnérabilité considérée comme étant la plus sérieuse de l'histoire du produit
- Type << Improper Input Validation >>
  - Permet la prise de contrôle de tous les comptes clients
  - Via API-REST, sans interaction nécessaire
- + de 250 tentatives d'exploitation observées par Sansec (en une seule journée)
  - Provenant toutes des 5 adresses IP suivantes :
    - 34.227.25.4, 44.212.43.34, 54.205.171.35, 155.117.84.134 et 159.89.12.166
  - Tentative d'upload de webshells PHP + utilisation des probes phpinfo
- 62% des boutiques Magento n'ont toujours pas appliqué le correctif
- Rappel des versions affectées :
  - 2.4.9-alpha2, 2.4.8-p2, 2.4.7-p7, 2.4.6-p12, 2.4.5-p14 et 2.4.4-p15 et antérieures

https://www.it-connect.fr/adobe-commerce-magento-cve-2025-54236-exploitation/

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

Failles de sécurité dans 7-Zip

CVE-2025-11001
CVE-2025-11002

- Présentes dans le module *ArchiveExtractCallback.cpp*
- Utilisation de liens symboliques de type Unix
  - Permet d'extraire en dehors du dossier cible
  - Exploitation possible uniquement sur Windows
- Exploit disponible sur GitHub
- Toutes les versions de la 21.02 à la 24.09 sont vulnérables
  - Passez à la branche 25.X

https://cybersecuritynews.com/poc-exploit-7-zip-vulnerabilities/

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

Failles de sécurité critique dans ASP.NET Core


CVE-2025-55315

- Corrigée dans le patch Tuesday d'octobre 2025
- Type << HTTP Request Smuggling >>
  - Permet à un attaquant de manipuler les requêtes HTTP et de contourner certaines protections
    - Ex. : bypass WAF / cache poisoning / détournement de session
  - Risque de leak d'informations, d'altération de fichiers et d'impact de la disponibilité de serveurs ciblés
- Mises à jour conseillées :
  - Microsoft Visual Studio 2022 → 17.10, 17.12 et 17.14
  - ASP.NET Core → 2.3, 8.0 et 9.0

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-55315

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

Faille critique sur WSUS activement exploitée


CVE-2025-59287

- Exécution de code à distance (unauthenticated) sur les serveurs Windows
  - Disposant du rôle WSUS (pas activé par défaut)
  - Aucune interaction nécessaire
  - Commandes exécutées en tant que SYSTEM
- Tous les Windows Server de la version 2012 à 2025 sont vulnérables
- Exploitation en cours
  - 2.500 instances WSUS vulnérables (150 en France)
  - IOC :
    - [IP] 207.180.254.242
    - [Commandes] `whoami`, `net user /domain` et `ipconfig /all`
- N'exposez pas vos serveurs WSUS !

https://www.it-connect.fr/patchez-wsus-cve-2025-59287-cette-nouvelle-faille-critique-est-deja-exploitee/

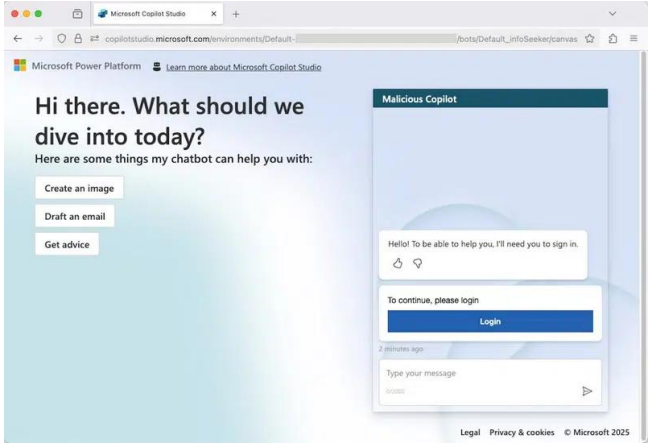
Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratage

Cophish, l’attaque sur Copilot

- Création d’un agent Copilot malveillant et mise à disposition du site Web démo de Microsoft
  - Affiche bien le nom de domaine de Microsoft mais trompe l'utilisateur
- Peut simuler un processus d’authentification légitime, en redirigeant la victime vers un faux flux de connexion ou une demande de consentement OAuth, via l'ajout d'un bouton << Login >> dans l'agent
- Microsoft, conscient du risque, travaille sur la remédiation

https://www.it-connect.fr/attaque-cophish-abuse-des-agents-ia-copilot-studio/



Piratages, Malwares, spam, fraudes et DDoS
Malware

Promptflux, le malware qui se change lui-même

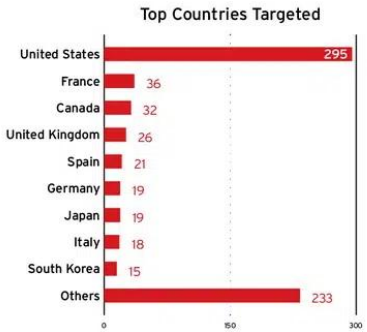
- Malware, codé en VBScript, en cours de développement et d'expérimentation
- Clé API permettant d'envoyer une requête à Gemini
  - Réécrire son propre code
  - Écrire un nouveau code permettant de contourner les antivirus
  - Objectif : utiliser le modèle pour réécrire et obfusquer son code afin d'échapper aux systèmes de détection statiques et par signatures
- Contourne les modérations de l'IA en se présentant comme un participant à un CTF

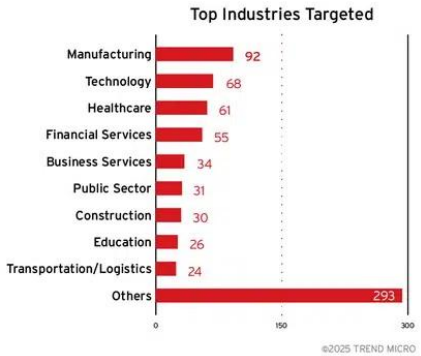
https://www.it-connect.fr/promptflux-ce-malware-utilise-lia-de-google-pour-reecrire-son-code-toutes-les-heures/

Piratages, Malwares, spam, fraudes et DDoS
Ransomware

La menace ransomware la plus redoutable du moment : Qilin

- Apparu en août 2022 (nommé Agenda)
  - En 2025 :
    - + de 700 victimes réparties dans 62 pays
    - 40 nouvelles victimes publiées chaque mois (depuis cet été)
- Ransomware visant initialement les environnements VMware ESXi et les serveurs Linux
  - Plus maintenant… 👋 Windows
- Binaire ELF (module de chiffrement) exécuté depuis… WSL
  - S'il n'est pas activé → les attaquants l'activent
  - `wsl -e <commande en question>`
- La majorité des EDR ne surveillent pas WSL 😪





https://www.it-connect.fr/le-ransomware-qilin-abuse-de-wsl-pour-chiffrer-les-machines-windows/

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

31.000 comptes fuités chez France Travail

- 3ème fuite de données en 2 ans
- Utilisation de logiciels malveillants ou lors de l'ouverture d'une pièce-jointe
  - Groupe Stormous
- Données non critiques :
  - Noms, dates de naissance, adresses, n° de téléphone, mails, parcours professionnels
- Données critiques :
  - Cartes d'identité, relevés d'identité bancaire, avis d'imposition, attestations de sécurité sociale, contrats de travail et certificats de formation des personnes concernées
  - Risque d'usurpation d'identité accru 😬

https://www.20minutes.fr/societe/4182449-20251030-fuites-donnees-france-travail-encore-victime-cyberattaque-31-000-demandeurs-emploi-concernes

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

Fuite de données chez F5 concernant des patchs en cours de développement

- F5 🇺🇸 en quelques chiffres :
  - Plus de 23.000 clients dans 170 pays
  - 48 des 50 plus grandes entreprises du classement Fortune 50
- Intrusion chez F5 qui a entrainé à un vol du code source sa solution BIG-IP
  - Intrusion détectée le 9 août (depuis ???)
  - Accès sur l'environnement de dev de la solution + sur la plateforme de gestion des connaissances
- Aucun impact sur la chaîne d'approvisionnement logicielle
- Des mises à jour concernant les vulnérabilités non divulguées dérobées ont été publiées
  - Notamment sur BIG-IP, F5OS et BIG-IQ
- Justification entre la détection de l'incident et la communication faite par F5 ?
  - Réponse : divulgation publique de l'incident retardée à la demande du gouvernement américain
    - Pour qu'elle puisse mettre à jour ses systèmes critiques

https://www.bleepingcomputer.com/news/security/hackers-breach-f5-to-steal-undisclosed-big-ip-flaws-source-code/

Business et Politique

Business *Européen*

Souveraineté allemande

- Succès d'un projet de transition informatique pour le Schleswig-Holstein
  - 6 mois de transition
  - Passage de Microsoft Exchange et Outlook par Open-Xchange et Mozilla Thunderbird
    - Transfert de + 40.000 boites mail et + 100M de messages et d'entrées agenda
- Objectif :
  - << éviter les dépendances économiques ou techniques de nature individuelle et monopolistique si l'État veut conserver le contrôle des systèmes informatiques qu'il utilise et la maîtrise des données de ses citoyens et de ses entreprises >>
- S'instaure dans la continuité de la transition d'autres entités :
  - L'armée autrichienne
  - Les agences gouvernementales danoises
  - La ville de Lyon en France

https://www.zdnet.fr/actualites/letat-allemand-remplace-microsoft-exchange-et-outlook-par-une-messagerie-electronique-open-source-483401.htm

Business
Monde

Pegasus sous bannière américaine

- Logiciel espion développé par une entreprise israélienne NSO Group
- Président executif : David Friedman
  - Ancien avocat de Trump
  - Ancien ambassadeur des EU en Israël (2017-2021)
- Volonté de faire bénéficier les forces de police du logiciel espion
- Cependant, siège social et activités principal toujours en Israël
  - Supervisée et réglementée par les autorités israéliennes, notamment le Ministère de la Défense et le cadre réglementaire israélien

https://next.ink/208353/nso-lediteur-du-logiciel-espion-pegasus-passe-sous-pavillon-etats-unien-et-trumpien/

Droit / Juridique / Politique
National

Contrôle renforcé sur les virements SEPA

- Issu du règlement (UE) 2024/886 sur les virements instantanés
  - Impose à toutes les banques un IBAN-Name Check obligatoire pour lutter contre la fraude
  - Règlement entré en vigueur le 9 avril 2024
- Contrôle en place depuis le 9 octobre 2025
  - Aussi bien pour les professionnels que pour les particuliers
- Virement (standard ou instantané) = vérification automatique du prénom / nom du bénéficiaire
  - Service gratuit et rapide (- de 5 secondes)
- Même si la fraude est faible en taux, les montants fraudés peuvent être élevés
- Conseils :
  - Vérifiez l'orthographe exacte du bénéficiaire
  - Assurez-vous de la conformité des IBAN utilisés

https://www.boursorama.com/budget/banque/actualites-amp/quel-nouveau-controle-sur-les-virements-entre-en-vigueur-ce-9-octobre-2025-3952edc6ad1905f5d54572f6d500e591

Conférences

Conférences

Passée(s)

- FIC, 14 au 15 octobre 2025 au Canada
- Identity Days, 21 octobre 2025 à Paris
- Unlock your brain, 7 au 8 novembre 2025 à Brest

À venir

- European Cyber Week (ECW), 17 au 20 novembre à Rennes
- GreHack, 28 au 29 novembre 2025 à Grenoble
- Trustech, 2 au 4 décembre 2025 à Paris

Divers / Trolls velus

Divers / Trolls velus

Retour sur l'incident du Louvre

- Mise en lumière de défaillances informatiques suite au cambriolage
  - Réseau de sûreté gérant la gestion des accès, des alarmes, de la vidéosurveillance et des badges
    - Mot de passe : << LOUVRE >> 😱
  - Pareil pour un logiciel de Thalès :
    - Devinez… << THALES >> 😱😱
- Présence d'équipements obsolètes dans le parc informatique
  - Windows 2000, Windows Server 2003, Windows XP…
- Audit de l'ANSSI en 2014 ayant bien identifié ces faiblesses
  - Même faiblesses lors de l'audit de l'INHESJ en 2017, pas d'amélioration
  - Vulnérabilités toujours présentes en 2025

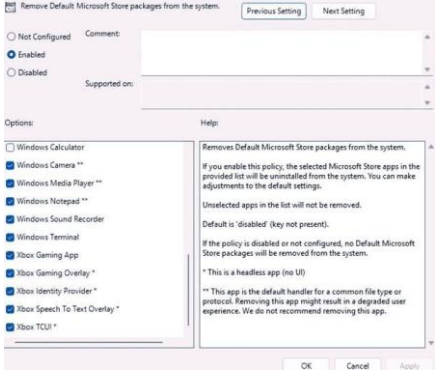
https://www.it-connect.fr/cybersecurite-du-louvre-des-mots-de-passe-inacceptables-et-des-systemes-obsoletes/

Divers / Trolls velus

La GPO qui va tous nous sauver !

- Stratégie permettant de supprimer toutes les applications Microsoft installées par défaut
  - Calculatrice, Caméra, Media Player, Notepad, etc.
- Chemin d'accès de la GPO :
  - "*Configuration de l'ordinateur*" > "*Modèles d'administration*" > "*Composants Windows*" > "*Déploiement des packages d'applications*" > "*Supprimer les packages Microsoft Store par défaut*"
- Les appareils ciblés doivent être sous Windows 11 25H2 (ou plus)
  - Versions Enterprise et Education
- La GPO ne désinstalle pas les bloatwares, mais empêche leur exécution

https://learn.microsoft.com/fr-fr/windows/configuration/policy-based-inbox-app-removal/policy-based-inbox-app-removal?tabs=intune



Divers / Trolls velus

Bitlocker bloque les PC

- Bug dans le dernier patch Tuesday de Microsoft
  - Affecte les machines Windows 10 et 11
- Démarrage sur l'écran de récupération au lieu du chargement habituel
  - Affecte principalement les ordinateurs équipés de processeurs Intel et du Modern Standby
- Cas similaire en mai 2025, lié au patch Tuesday
  - Questionnement sur le processus de validation et les tests normalement effectués

https://www.lesnumeriques.com/informatique/windows-10-11-nouveau-fiasco-bitlocker-bloque-l-acces-a-des-milliers-de-pc-sans-prevenir-n244959.html

Divers / Trolls velus

Alternative (libre et multiplateforme) aux RSAT de Microsoft

- Fonctionnalitées proposées :
  - Gestion des comptes utilisateurs et des ordinateurs
    - Accès évident aux propriétés des objets
  - Gestion du DNS
  - Gestion des sites et des services
  - Outil de recherche dans l'AD
  - Gestion des profils de connexion
- Application all-in-one (versus les RSAT de Windows)
- En cours de développement
  - Manque encore la gestion des stratégies de groupe
- Par les créateurs de Samba AD

https://github.com/tranquilit/OpenRSAT (outil sur GitHub)

https://www.tranquil.it/openrsat/

Divers / Trolls velus

Menace Android, rapport de Zscaler

- + 40M de téléchargements pour 239 applications
  - Applications malveillantes sur Google Play Store
    - Juin 2024 - Mai 2025
- Hausse de 67% du volume de malware
  - Spécifiquement spyware et trojan bancaire
- Principaux pays concernés : Inde, EU et Canada ; mais menace mondiale
- Mise en avant de 3 souches de malwares :
  - Anatsa, trojan bancaire
  - Android Void, backdoor pour android TV
  - Xnotice, RAT

https://www.it-connect.fr/239-applications-android-malveillantes-cumulent-plus-de-40-millions-de-telechargements/

https://www.zscaler.com/fr/campaign/threatlabz-mobile-iot-ot-report

Divers / Trolls velus

183M de credentials, pas de piratage de Google

- Ajout d'une importante base de donnée sur << Have I Been Pwned >>
  - Contient des comptes gmail et mot de passe associé
- Concaténation de plusieurs fuites liées à des :
  - Vols d'informations via des malwares, en particulier des infostealers
  - Attaques de phishing (hameçonnage)
  - Attaques par credential stuffing
  - Compilations de précédentes fuites de données
- 91% des informations étaient déjà connus
- Aucun message de Google concernant une quelconque fuite n'a été remontée

https://www.it-connect.fr/183-millions-identifiants-voles-mais-rassurez-vous-google-na-pas-ete-pirate/

FIN

Prochaine réunion ?

- RDV le **mardi 09 décembre 2025**

Accéder aux différents supports ?

Replays

Slides

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

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