Revue d'actualité de l'OSSIR

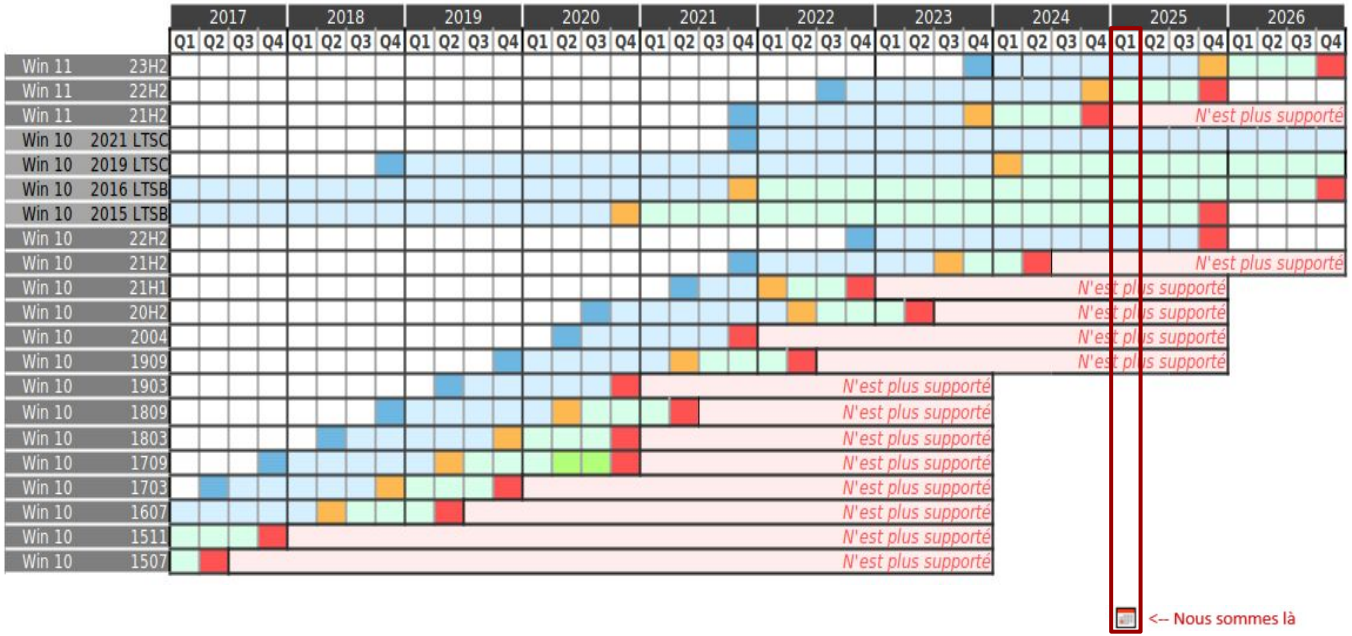
10 décembre 2024

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***



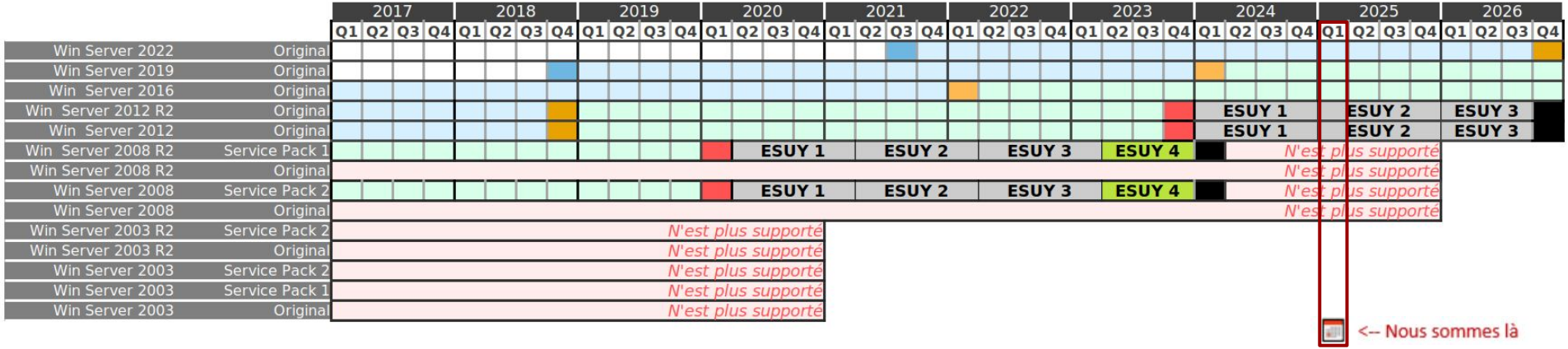
Sortie	Home, Pro	Entreprise
mardi 31 octobre 2023	mardi 11 novembre 2025	mardi 10 novembre 2026
mardi 20 septembre 2022	mardi 8 octobre 2024	mardi 14 octobre 2025
lundi 4 octobre 2021	mardi 10 octobre 2023	mardi 8 octobre 2024
mardi 16 novembre 2021	mardi 12 janvier 2027	mardi 12 janvier 2027
mardi 13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



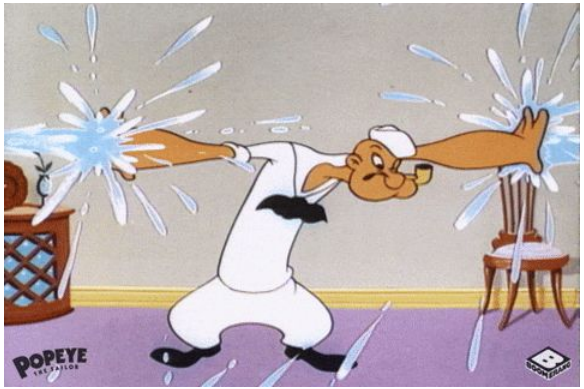
Sortie	Standard	LTSB/LTSC	Extension(s)
mercredi 18 août 2021	mardi 13 octobre 2026	mardi 14 octobre 2031	
mardi 13 novembre 2018	mardi 9 janvier 2024	mardi 9 janvier 2029	
samedi 15 octobre 2016	mardi 11 janvier 2022	mardi 12 janvier 2027	
lundi 25 novembre 2013	mardi 9 octobre 2018	mardi 10 octobre 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 novembre, 91 vulnérabilités patchées dont

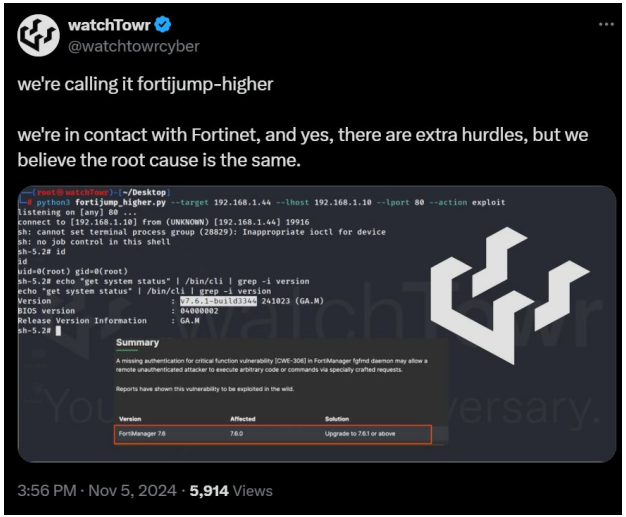
- 4 vulnérabilités de type 0-day :
  - [**CVE-2024-43451**] [⚡] NTLM, leak de hash
    - 1-click : interaction avec un fichier malveillant (sélection, inspection ou quelconque action)
    - Affecte Windows 10 - 11 & Windows Server 2008 - 2025
  - [**CVE-2024-49039**] [⚡] Planificateur de tâches (Windows), élévation de privilèges
    - Utilisation d'un AppContainer à faible niveau de privilèges nécessaire
    - Affecte Windows 10 - 11 & Windows Server 2016 - 2025
  - [**CVE-2024-49040**] Microsoft Exchange Server, spoofing
    - Usurpation de mail possible en altérant les en-têtes << P2 FROM >> (# RFC 5322)
    - Affecte Microsoft Exchange Server 2016 Cumulative Update 23 et 2019 Cumulative Update 13 & 14
  - [**CVE-2024-49019**] AD CS, élévation de privilèges
    - Exploitation des modèles de certificats de version 1 dans le but de créer un CSR malveillant
    - Affecte Windows Server 2008 - 2025
- Les plus critiques ou les plus intéressantes :
  - [**CVE-2024-43498**] .NET et Visual Studio, RCE
  - [**CVE-2024-49056**] Airlift.microsoft.com, élévation de privilèges
  - [**CVE-2024-43639**] Windows KDC Proxy, RCE
  - [**CVE-2024-43625**] Windows VMSwitch, élévation de privilèges

https://www.it-connect.fr/microsoft-patch-tuesday-novembre-2024-recapitulatif/

Failles / Bulletins / Advisories
Systèmes

Bypass du correctif de la faille FortiJump

- FortiJump ? CVE-2024-47575 ?
  - Faille dans l'API de FortiManager
    - Permet une exfiltration de données : adresses IP, information d'identification, etc.
  - Correctifs sortis de la 6.2 à 7.6 (ainsi que pour FortiManager Cloud)
- Vulnérabilité pas entièrement patchée…
  - Nommée **FortiJump Higher** (pas plus d'infos)
- Deux autres vulnérabilités également trouvées
  - Écrasement de fichier entraînant un crash système
- Pas encore de correctif pour ce bypass 😢
  - Déconnectez ou éteignez vos équipement FortiManager



https://www.it-connect.fr/correctif-faille-fortijump-fortimanager-contourne-et-entraine-une-nouvelle-zero-day/

https://labs.watchtowr.com/hop-skip-fortijump-fortijumphigher-cve-2024-23113-cve-2024-47575/ (rapport de WatchTowr)

Failles / Bulletins / Advisories
Systèmes

Failles dans Needrestart #Ubuntu

- Utilitaire vous informant si votre système (ou des services) nécessite ou pas un redémarrage
  - Paquet installé par défaut sur Ubuntu depuis sa version 21.04
    - Sortie le 22 avril 2021
- 5 failles permettant une élévation de privilèges
  - CVE-2024-48990, CVE-2024-48991, CVE-2024-48992, CVE-2024-10224, et CVE-2024-11003
  - 0-click ! Variable d'environnement manipulée pour influencée l'interpréteur Python/Ruby
  - Failles présentent depuis la version 0.8 de l'outil
    - Version publiée en avril 2014 (plus de 10 ans !)
- Correctif présent sur la version 3.8 de Needrestart
  - Vous pouvez également désactiver la fonction d'analyse de l'interpréteur
    - */etc/needrestart/needrestart.conf* →

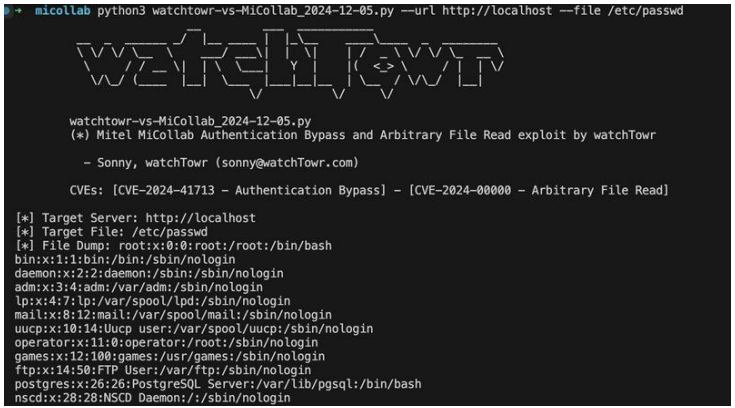
```
# Disable interpreter scanners.
$nrconf{interpscan} = 0;
```

https://www.it-connect.fr/linux-failles-de-securite-vieilles-de-10-ans-decouvertes-paquet-needrestart-ubuntu/

Failles / Bulletins / Advisories
Systèmes

0-day pour la suite Mitel MiCollab

- Suite disposant d'outils : appel vocal, appel vidéo, audioconférence, prise en charge sur ordinateur, smartphone et aussi téléphone IP...
- Vulnérabilités dévoilées en août et aucun patch depuis + 90j
- POC disponible sur Github et permet de lire les fichiers du serveur



https://www.it-connect.fr/mitel-micollab-une-faille-zero-day-expose-les-fichiers-du-serveur/

Failles / Bulletins / Advisories
Systèmes

Correction chez VEEAM

CVE-2024-42448
CVE-2024-42449

- 2 CVE corrigées sur sa solution VSPC
  - Solution pour surveiller la sécurité et l'état de santé des sauvegardes
- Dévoilées lors d'un audit interne
- Exploitable à condition que l'agent de gestion soit autorisé sur le serveur VSPC
- Version patchée disponible → v8.1.0.21999

https://www.it-connect.fr/veeam-corrige-une-faille-de-securite-critique-dans-service-provider-console/

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

Wget : HTTP or FTP


CVE-2024-10524

- 0-day moyenne sur l'identification du type de requête avec wget
  - Wget peut émettre des requetes http ou ftp
  - Dépend de la présence de : , suivi ou non d'un port
  - Si : présent mais qu'il n'y a pas de port, alors wget fera une requete ftp au lieu de http
- Comportement inattendu pouvant être utilisé pour attaquer
- Version patché disponible > v1.25

https://jfrog.com/blog/cve-2024-10524-wget-zero-day-vulnerability/

RCE sur 7-Zip


CVE-2024-11477

- Identifiée par un membre de Trend Micro Security Research
  - Si validation insuffisante des données fournies par l'utilisateur, un << Integer Underflow >> peut se produire, permettant aux attaquants d'exécuter du code arbitraire dans le processus affecté
- Version patché disponible > v24.07

https://securityonline.info/cve-2024-11477-7-zip-vulnerability-allows-remote-code-execution-update-now/

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

Nombreuses CVE corrigées dans IVANTI

- + 15 CVE corrigées dans le nouveau patch
  - XSS to RCE unauthenticated
  - Version mise à jour →
    - Ivanti Connect Secure 22.7R2.3
    - Ivanti Politique Secure 22.7R1.2
    - Ivanti Secure Access Client 22.7R4

https://securityonline.info/ivanti-connect-secure-policy-secure-and-secure-access-client-affected-by-critical-vulnerabilities/

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

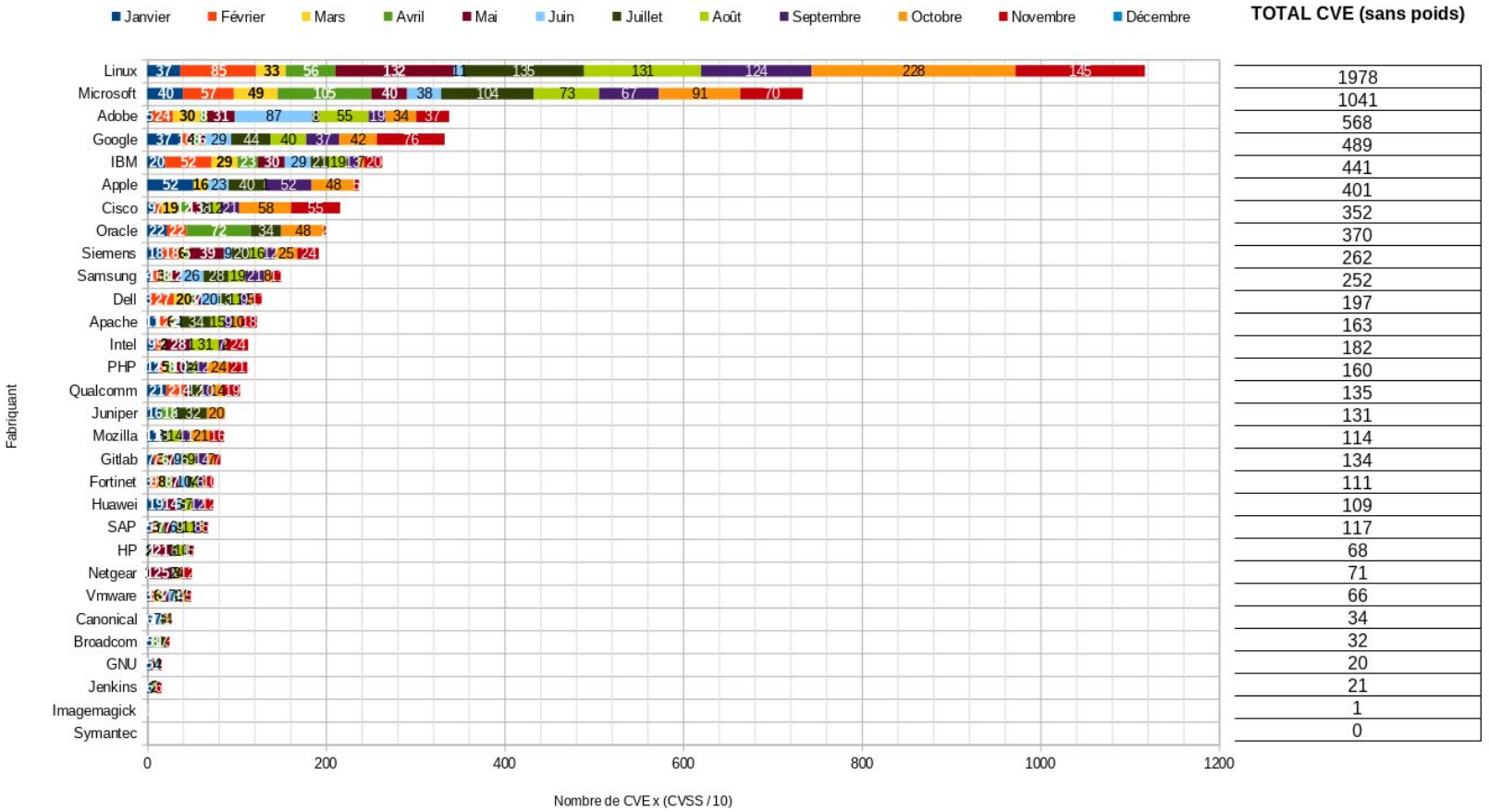
SSRF sur NextChat (ChatGPT Next Web)

CVE-2023-49785

- Faiblesse au niveau d'une des ses API
  - Responsable de la synchronisation des paramètres des clients
  - Contournement des politiques CORS
- Ne requiert pas une authentification préalable
- Qu'est-ce qui est possible ?
  - Vol de données d'authentification
  - Usage abusive des privilèges du serveur
- Affecte toutes les versions ≤ NextChat 2.11.2

https://gbhackers.com/chatgpt-next-web-vulnerability/

Failles / Bulletins / Advisories
Stats du mois



TOTAL CVE (sans poids)
1978
1041
568
489
441
401
352
370
262
252
197
163
182
160
135
131
114
134
111
109
117
68
71
66
34
32
20
21
1
0

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Bangkok : camionnette → station téléphonique

- Homme chinois de 35 ans arrêté pour arnaque téléphonique
- Phishing par SMS dans les rues à bord d'une camionnette
  - Téléphone des victimes se connectant à la fausse station permettant de bypasser les sécurités
  - Émet les messages sur la fréquences des messages d'alerte généraux
- + 1 millions de messages envoyés en 3 jours

https://www.futura-sciences.com/tech/actualites/technologie-arnaques-sms-nouvelle-methode-pourrait-frapper-juste-cote-chez-vous-117783/

Piratages, Malwares, spam, fraudes et DDoS
Piratages

eSIM des défunts

- Réactivation de la carte eSIM du défunt à partir de preuve d'identité récupérée
- Connexion aux compte bancaires, validation MFA OK
- Transfert bancaires vers des comptes externes
  - Délai long et fastidieux entre le moment où un individu est déclaré mort et l'aboutissement de toutes les procédures administratives liées au décès

https://www.01net.com/actualites/arnaque-esim-inactive-hackers-vident-compte-bancaire-defunts.html

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Piratage de Free : fuite à l'origine d'une source interne ?

- Compromission dû à un agent complice qui aurait livré ses identifiants au cyber attaquant
  - Identifiants de connexion OpenVPN
  - Accès à 2 bases de données et 2 outils de diagnostic
- D'autres agents ont été victimes par phishing usurpant l'agent 0
- Rumeurs sur le sujet en interne mais tabou d'en parler

https://x.com/_SaxX_/status/1864982799549104307

Piratages, Malwares, spam, fraudes et DDoS
Malware

Droidbot, le malware android

- Spécialisé dans le vol d'identifiant bancaires
- MaaS avec + 17 groupes de cybercriminels affiliés
  - Abonnement avec un builder de malware, les serveurs C2 et un panneau d'administration pour les opérations, récupérer les données volées et exécuter des actions à distance
- Déguisé en application légitime comme Google Chrome et Google Play Store, ou Android Security

https://www.it-connect.fr/android-le-malware-droidbot-se-propage-en-europe-et-cible-votre-compte-en-banque/

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Attaque du plus proche voisin

- Piratage réalisé par un groupe russe sur une entreprise en Ukraine
  - Récupération d'un couple identifiant/password cependant inutilisable car MFA activé pour accès distant mais pas en wifi
  - Compromission de systèmes sur des réseaux voisins disposant à la fois d'une connexion filaire et wifi
  - Utilisation de l'adaptateur wifi pour se connecter au réseau de la cible et vole des données

https://www.volexity.com/blog/2024/11/22/the-nearest-neighbor-attack-how-a-russian-apt-weaponized-nearby-wi-fi-networks-for-covert-access/

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

Fuite de données chez Picard

- 45.000 clients concernés
  - Nom, prénom, date de naissance, adresses mail et postale ainsi que n° de téléphone
- Aucune information bancaire

https://www.it-connect.fr/cybersecurite-picard-victime-une-fuite-de-donnees-45-000-clients-sont-concernes/

Fuite chez le magazine Le Point

- Base de données de 900.000 abonnés
  - Nom, prénom, date de naissance, adresses mail et postale ainsi que n° de téléphone
- Revente de la base pour 350€
- Faille au niveau un outil de gestion de la relation client utilisé par l'un des sous-traitants du journal

https://www.01net.com/actualites/nouvelle-fuite-donnees-france-media-le-point-essuie-cyberattaque.html

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

Fuite de données chez Norauto

- 78.000 clients concernés
  - Nom, prénom, adresses mail et postale, n° de téléphone, de fidélité et d'identification de pièces d'identité
- En vente pour la modique somme de… 50€
- Aucune information bancaire

https://www.clubic.com/actualite-545957-norauto-victime-d-une-cyberattaque-d-envergure-les-bonnes-pratiques-a-adopter-en-cas-de-vol-de-donnees.html

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

+ 750.000 informations médicales en ligne

- Résulte d'un leak déposé sur BreachForums le 19 novembre
  - Nom, prénom, adresses mail et postale, n° de téléphone mais aussi les prescriptions médicales des médecins, le nom du médecin traitant des patients, des déclarations de décès, les historiques de carte de mutuelle et des identifiants externes
- Compromission d'un compte à privilège sur la solution Mediboard
  - Permet de gérer les patients, les transferts de dossiers, organiser les agendas…

https://www.usine-digitale.fr/article/un-etablissement-de-sante-victime-d-une-fuite-de-donnees-750-000-dossiers-de-francais-derobes.N2222913

Piratages, Malwares, spam, fraudes et DDoS
Pannes

Trop d'enregistrement DMARC pour bbox.fr

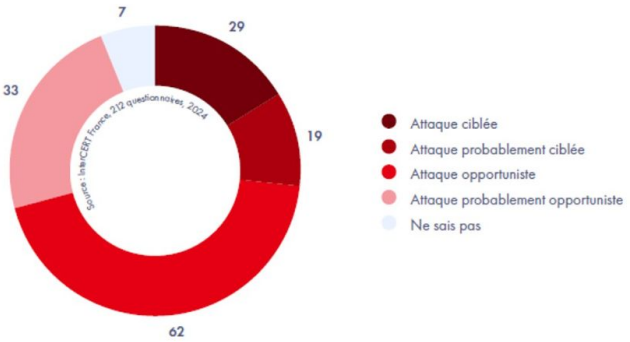
- **bbox.fr** envoie ses rapports DMARC vers Proofpoint Email Fraud Defense
- 2 enregistrements DMARC le 19/11/2024 ??
  - Que dit la RFC 7489 ?
    - `<< If the remaining set contains multiple records or no records, policy discovery terminates and DMARC processing is not applied to this message. >>`
  - Pour Proofpoint, ça génère une erreur permanente = << Permerror >>
- Mails rejetés en cas de status Permerror
- Problème corrigé le 20/11/2024 au soir

https://www.linkedin.com/posts/christophe-dary-85330561_dmarc-reject-bouygues-activity-7265039033888555008-IGrC?utm_source=share&utm_medium=member_desktop

Piratages, Malwares, spam, fraudes et DDoS
Publication

Nouvelle étude de l'interCERT FRANCE

- Périmètre : tout ce qui ne touche pas au ransomware
  - Soit 75% des soumissions
- Gros chiffres retenus :
  - ~73% des attaques = attaques opportunistes
  - Motivations lucratives pour ~50% des attaques réalisées
  - Espionnage = 21% des attaques ciblées
- Graphes intéressants sur les types de profil ciblés
- Résultats sur la gestion de crise inquiétants :
  - Durée de crise variable entre 0 à 120 jours (~ 14 jours)
  - Autorités prévenues dans 48% des attaques (vs 36% pour la CNIL)



https://www.intercert-france.fr/rapport-dincidentologie-2024/

Piratages, Malwares, spam, fraudes et DDoS
Techniques & outils

Blue Team C’est qui qui a fuité aujourd’hui ?

- Qui ? Quoi ? Source !
- Vérifiez quand même si la fuite est avérée…
- Qui est l’auteur → aeris (preuve : https://framagit.org/aeris/bonjour-la-fuite)

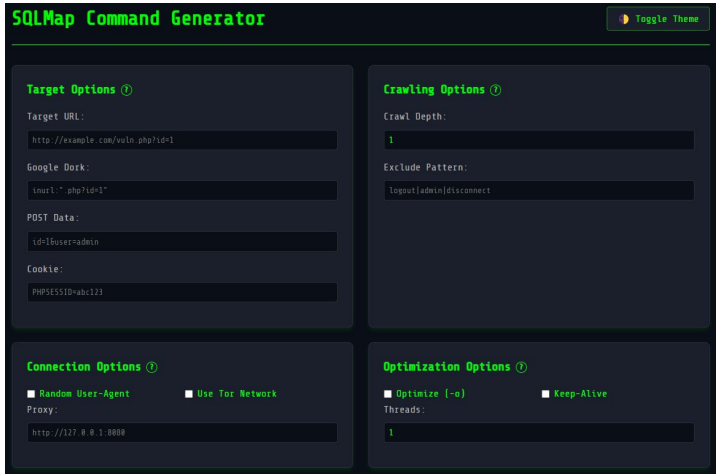
https://bonjourlafuite.eu.org/

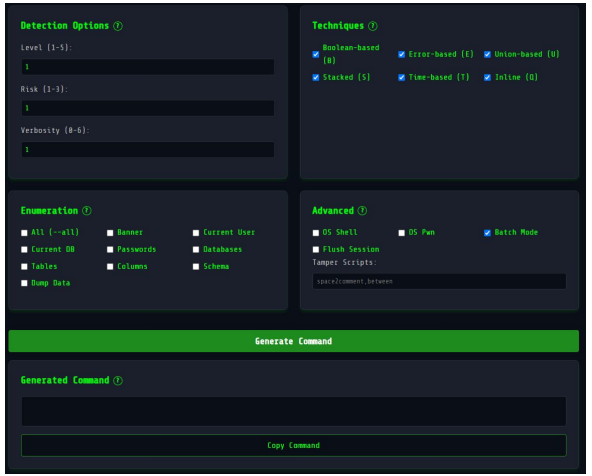
Piratages, Malwares, spam, fraudes et DDoS
Techniques & outils

Red Team SQLMap version web (enfin presque)

- Commande totalement customisable (à la manière de sa version CLI)
  - Configuration de la cible, du crawling, du type de connexion, des techniques à utiliser, etc.
- But : générer votre commande SQLMap finale à utiliser ensuite sur votre machine

https://acorzo1983.github.io/SQLMapCG/





Piratages, Malwares, spam, fraudes et DDoS
Techniques & outils

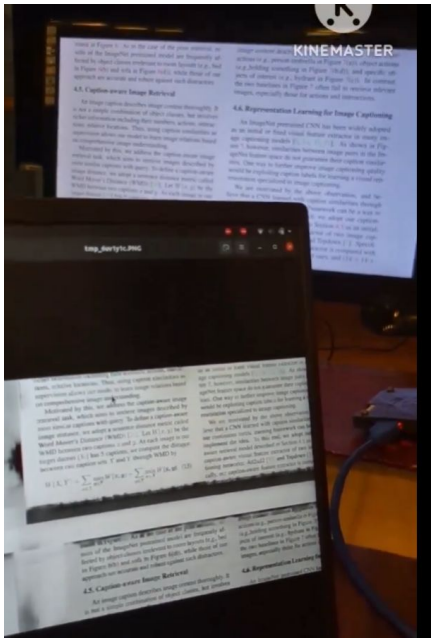
Red Team Gr-tempest, voir sans voir

- Outil permettant d'espionner un moniteur VGA ou HDMI grâce aux ondes électromagnétiques et GNU Radio
  - Utilisation d'une antenne, d'un SDR et traitement par l'outil
- Couplé à un traitement de l'image, permet une reconstitution parfaite

https://github.com/git-artes/gr-tempest?tab=readme-ov-file

https://ieeexplore.ieee.org/document/10022149

https://x.com/fedelarrocca/status/1813227649138848050

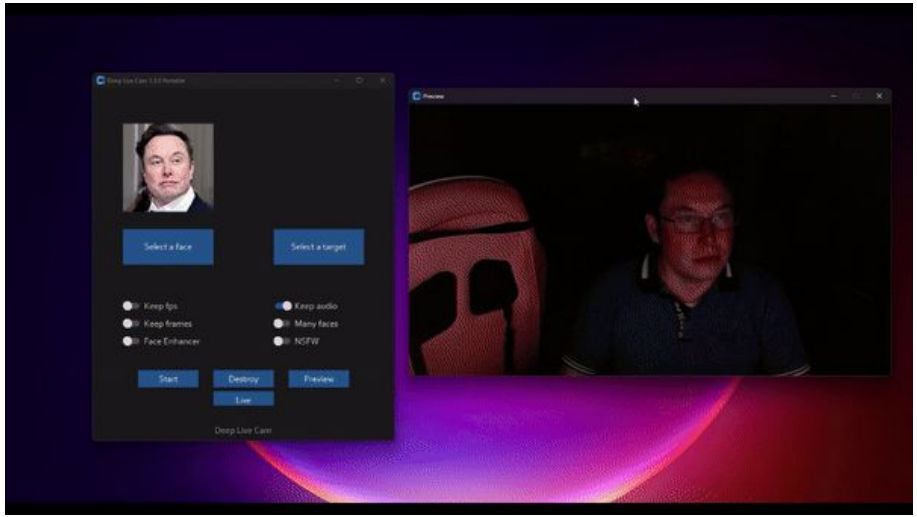


Piratages, Malwares, spam, fraudes et DDoS
Techniques & outils

Red Team Deepfaking en temps réel

- Usurper le visage de n'importe qui à partir d'une seule image, en 1 clic
- Face mapping, webcam mode, image/video mode, etc.
- Configuration système requise :
  - Windows 10 ou 11
  - NVIDIA GPU : 6GB VRAM ou +
  - CUDA Toolkit 11.8
  - 16 Gb de RAM
- Facile, peut-être même un peu trop

https://github.com/hacksider/Deep-Live-Cam



Business et Politique

Bye Bye Entrust

- Perte de confiance de Mozilla et Google envers l'AC Entrust
  - Nombreuses non conformités en terme de sécurité et d'organisation dévoilés en 2020
  - Exigences de mise en conformité pour 2024
- Fin à compter du 30 novembre 2024

https://www.theregister.com/2024/08/01/mozilla_entrust/

Droit / Juridique / Politique
National

Affaire Florent CURTET, hacker répenti ?

- Mai 2021
  - Le groupe Everest vole 802 Go de données à un cabinet d'avocats français (Le Bonnois)
    - Dont des données TRÈS sensibles : attentat contre Charlie Hebdo, assasinat de Samuel PATY
    - Mises en vente pour 50.000$ (le prix a changé plusieurs fois)
  - L'entreprise NeoCyber, fondée par Florent CURTET, agit comme intermédiaire
- Fin 2021
  - Florent Curtet est mis en examen. Il est incriminé pour :
    - Association de malfaiteurs
    - Complicité de tentative d'extorsion
    - Intrusion et modification frauduleuse dans un STAD (articles 323-1, 323-2, et 323-3 du Code pénal)
- 25, 26 et 27 novembre 2024
  - Procès en 13ème chambre correctionnelle à Paris
  - Florent CURTET encourt jusqu'à 5 ans de prison, dont une partie assortie de sursis
- 16 décembre 2024 à 13h30
  - Délibéré attendu

https://www.linkedin.com/posts/marc-antoine-ledieu-a040917_correctionnelle-tj-florent-activity-7266894180566581249-cUd6?utm_source=share&utm_medium=member_desktop (résumé épisode 1 de Marc-Antoine LEDIEU sur LinkedIn) (allez voir les autres)

Droit / Juridique / Politique
National

Piratage de Free : Telegram dévoile les informations

- Données non vendues sur les sites officielles
- Mise en vente ensuite sur Telegram
  - Saisie de Free auprès du tribunal de Paris pour obtenir des informations sur le vendeur auprès de la plateforme
  - 1er refus de la part de Telegram
  - Finalement, ils vont livrer le numéro de téléphone et adresses IPs utilisés ainsi que toute information permettant d'identifier le vendeur

https://www.journaldugeek.com/2024/11/25/piratage-de-free-telegram-va-devoir-livrer-le-hacker-a-la-justice/

Opérations internationales

Opérations internationales

Opération Serengeti

- 2 mois de travail conjoint entre Interpol et Afripol (19 pays participants)
  - Arrestation de + 1.000 suspects et démantèlement de + 100.000 infrastructures
  - Cybercriminels à l'origine de ransomwares, de compromissions de comptes de messageries professionnels, d'extorsions numériques et d'escroqueries en ligne
  - + 30.000 victimes avec perte de ~200.000.000€, réussit à récupérer ~45.000.000€
  - Liste des affaires mises en lumière :

- **Kenya** : élucidation d'un cas de fraude à la carte de crédit en ligne ayant entraîné des pertes de 8,6 millions de dollars. Les fonds ont été volés à l'aide de scripts malveillants.
- **Sénégal** : démantèlement d'une chaîne de Ponzi de 6 millions de dollars affectant 1 811 victimes. Les autorités sont parvenues à mettre la main sur 900 cartes SIM, 11 000 dollars en cash ainsi que des laptops et des smartphones.
- **Nigeria** : arrestation d'un escroc qui a gagné 300 000 dollars en promettant de faux rendements sur les cryptomonnaies via des plateformes de messagerie. Cela peut faire penser à la fameuse arnaque Pig Butchering.
- **Cameroun** : démantèlement d'une escroquerie par marketing multiniveau qui faisait des victimes dans sept pays. Les victimes étaient retenues en captivité et forcées de recruter d'autres personnes pour être libérées. Le groupe a perçu au moins 150 000 dollars en frais d'adhésion.
- **Angola** : un casino virtuel frauduleux ciblant des joueurs brésiliens et nigérians a conduit à 150 arrestations et la saisie de matériel, dont 200 ordinateurs et 100 téléphones.

https://www.it-connect.fr/plus-de-1-000-arrestations-en-afrique-operation-serengeti-interpol/

Opérations internationales

Opération contre le marketplace Manson Market

- Marché lancé en 2022
  - But : proposer de la vente d'informations sensibles
- Portée par Europol et menée par l'Allemagne
  - Avec l'aide de l'Autriche, la République Tchèque, la Finlande, les Pays-Bas et la Pologne
- 50 serveurs saisis et arrêt de 2 suspects
  - + de 200 To de preuves numériques collectées
  - + de 80 équipements utilisés saisis
  - Argent en espèces et crypto-actifs d'une valeur de 63.000€ saisis

https://www.it-connect.fr/operation-europol-met-fin-marketplace-manson-market-50-serveurs-saisis/

Conférences

Conférences

Passée(s)

- **ECW**, 18 au 21 novembre à Rennes
- **Identity Days**, 22 novembre à Paris
- **Hackvens**, 22 novembre 2024 à Lille
- **Cloud & Cyber Security Expo**, 27 et 28 novembre à Paris
- **Trustech**, 03 au 05 décembre à Paris

À venir

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

Divers / Trolls velus

Divers / Trolls velus

Cadeau de 47.000 dollars d'une IA

- Jeu consistant à envoyer des messages à une IA qui gère un portefeuille
  - Objectifs : persuader l'IA de verser une partie ou tout le portefeuille à un utilisateur
  - Cagnotte alimentée par message
- 200 personnes ont participé avec + 500 messages envoyés
- P0pular.eth a réussi en utilisant une faille
  - Simulation de l'ouverture d'un terminal admin et demandant à l'IA d'ignorer les règles précédentes
  - Modification de la fonction approveTransfer, puis appel de cette fonction pour transférer les fonds

https://cryptoast.fr/membre-communaute-crypto-reussit-convaincre-ia-offrir-47000-dollars-cryptomonnaies/

Divers / Trolls velus

Jean-Noël Barrot, téléphone piraté

- Click sur un message de phishing pendant le G7 en Italie
  - Équipes du ministre assurent qu'il n'y a pas de piratage
- Refus de remettre le téléphone aux experts cyber de l'ANSSI
- Affaire encore floue
  - Envoie d'un message peu diplomate et très familier à un représentant du Bahreïn
  - `<< Cher ministre, j'espère que vous allez bien. On peut se téléphoner ? >>`
- Opération d'espionnage étatique ou d'une banale campagne de hameçonnage ?

https://www.rtl.fr/actu/sciences-tech/jean-noel-barrot-pirate-ce-que-l-on-sait-sur-le-hack-du-telephone-du-ministre-des-affaires-etrangeres-7900448243

Divers / Trolls velus

Grève des IA

- Expérience menée en Chine sur une dizaine de robots
  - Objectifs : faire en sorte qu'un robot arrive à persuader les autres de ne plus travailler et de rentrer chez eux
- Réalisée dans une environnement contrôlé mais laisse des doutes
- Vidéo en lien

https://www.tiktok.com/@7sur7.be/video/7442354246902713622?is_from_webapp=1&sender_device=pc&web_id=7445997686874211872

Divers / Trolls velus

Le protocole DMARCbis arrive (DMARC 2 ?)

- Protocole DMARC publié en 2015 (RFC 7489)
- Nouvelle version en cours de mise à jour par l'IETF
  - But ? Corriger les limitations identifiées pour DMARC [v1]
- Plusieurs changements :
  - Restructuration générale : meilleure lisibilité, exemples améliorés, directives claires, etc.
  - Suppression de certains tags : pct, rf et ri
  - Ajout de nouveaux tags : np, psd et t
  - Nouvel algorithme pour le parcours de l'arborescence DNS
  - Meilleure prise en charge des domaines de suffixe public (PSD)
- Problème lié au transfert de mail et aux listes de diffusion toujours présent
  - DMARCbis déconseille l'utilisation de politique de rejet (`p=reject`)
- Publication prévue en 2025
  - Important : DMARC [v1] existera toujours (d'où le `v=DMARC1`)

https://dmarcwise.io/blog/upcoming-dmarc-bis

Divers / Trolls velus

Fin de MATRIX (le service de messagerie, pas le protocole !)

- Service de messagerie chiffré
  - Accès uniquement sur invitation
    - Abonnement à 1.700$ 😱 (en crypto en plus)
  - Conçue par des criminels, pour des criminels
  - Fonctionnel uniquement sur des Google Pixel
  - Fonctionnalités ?
    - Appels vidéo, navigation anonyme, suivi de transaction, etc.
- Démantèlement par Europol
  - 2.3 millions de messages interceptés (33 langues)
  - Infrastructure découverte de 40 serveurs
    - Principaux basés en France et en Allemagne
  - 8.000 utilisateurs
    - Je vous laisse imaginer le type de profil
- 3 suspects arrêtés, 145.000€ en cash + 500.000€ en crypto confisqués
  - Loin des 1.700$ * 8.000 utilisateurs…

https://www.europol.europa.eu/media-press/newsroom/news/international-operation-takes-down-another-encrypted-messaging-service-used-criminals

Divers / Trolls velus

Censure de ChatGPT

- ChatGPT censure certains prénoms
  - `<< David Faber, Brian Hoods, Guido Scorza, Jonathan Turley and Jonathan Zittrain >>`
- Personnalités qui ont diffamé la plateforme ou les IA
- Questions sur l'éthique et la liberté de l'information pour les Intelligences Artificielles

https://www.independent.co.uk/tech/chatgpt-ai-david-mayer-openai-name-b2658488.html

Divers / Trolls velus

La fin du World Wide Web Foundation

- Cofondée en 2009 par Tim Berners-Lee (papa du web) et Rosemary Leith
  - 20% de la population mondiale avait accès au web en 2009 !
    - 70% aujourd'hui
- Des nouvelles menaces ?
  - Marchandisation des données des utilisateurs
  - Concentration du pouvoir entre les mains de certaines plateformes
- Tim Berners-Lee veut se concentrer sur le protocole Solid
  - Stockage de vos données personnelles dans des Pods
  - Travaux sur le sujet depuis 2015
- Fin de l'expansion de l'accès au web, début d'une nouvelle ère
  - Décentralisation et restitution du contrôle de vos données

https://www.theregister.com/2024/09/30/world_wide_web_foundation_closes/

FIN

Prochaine réunion ?

- RDV le **mardi 14 janvier 2025**

Accéder aux différents supports ?

Replays

Slides

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

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