



Revue d'actualité de l'OSSIR

09 avril 2024

*Jérémy De Cock
Melchior Courtois*



Failles / Bulletins / Advisories

■ Bulletin de février, 73 vulnérabilités patchées dont

- 2 failles 0-day :
 - [CVE-2024-21351] Bypass de **SmartScreen**, RCE via un 1-click
 - Affecte toutes les versions >= Windows 10 v1607 et >= Windows Server 2016
 - [CVE-2024-21412] Bypass de **Mark of the Web** (fichier provenant d'Internet ou non ?)
 - Exploitée par le groupe APT DarkCasino
 - Affecte toutes les versions >= Windows 10 v1809 et >= Windows Server 2019
- Les plus critiques ou les plus intéressantes :
 - [CVE-2024-21380] Microsoft Dynamics, leak de données
 - [CVE-2024-21410] Microsoft Exchange Server, relai NTLM
 - Nécessaire d'activer Exchange Extended Protection for Authentication (EPA)
 - HealthChecker (outil pour checker l'état d'EPA) disponible sur le GitHub de Microsoft
 - [CVE-2024-21413] Microsoft Office, RCE via un 1-click (nommée Moniker Link)
 - Bypass l'ouverture en mode protégé
 - [CVE-2024-20684] Hyper-V, DoS de l'hôte
 - [CVE-2024-21357] Windows Pragmatic General Multicast (PGM), RCE

<https://www.it-connect.fr/patch-tuesday-fevrier-2024-73-vulnerabilites-corrigees-et-2-faille-de-securite-zero-day/>

Failles / Bulletins / Advisories (MMSBGA)

Microsoft

■ Bulletin de mars, 60 vulnérabilités patchées dont

- Aucune faille 0-day ! 🤖
- Les plus critiques ou les plus intéressantes :
 - [CVE-2024-21407] & [CVE-2024-21408] Hyper-V, RCE & DoS
 - [CVE-2024-26199] Microsoft Office, élévation de privilèges
 - [CVE-2024-20671] Faille permettant de ne pas démarrer Defender
 - [CVE-2024-21411] Skype for Consumer, RCE
 - [CVE-2024-21390] Microsoft Authenticator, élévation de privilèges
- MAJ qui a provoqué le redémarrage de quelques contrôleurs de domaine
 - Fuite de mémoire faisant planter le processus LSASS
 - Impacte uniquement les Windows Server
 - Correctifs uniquement disponibles via le Catalogue Microsoft Update
 - <https://www.catalog.update.microsoft.com/Search.aspx?q=2024-03%20Cumulative%20Update>

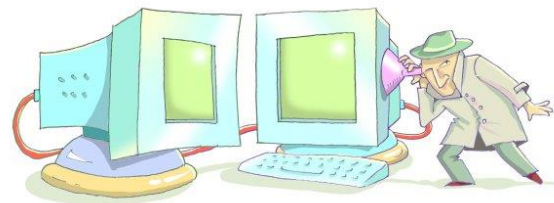
<https://www.it-connect.fr/patch-tuesday-mars-2024-60-vulnerabilites-corrigees/>

Faillles / Bulletins / Advisories Systèmes

■ Vulnérabilité matérielle du côté des puces Apple, GoFetch

- M1, M2 et même M3
- Type “side-channel” ciblant le DMP
 - Dans le but de lui faire leaker des données
- Elle ne peut pas être corrigée...
 - Enfin, du côté matériel
 - Mais attention, vos puces vont avoir mal

<https://gofetch.fail/>



■ Patchez vos NAS QNAP (CVE-2024-21899, CVE-2024-21900 et CVE-2024-21901)

- 3 vulnérabilités découvertes
 - Permettent la compromission des données du NAS
 - La première est très critique car elle ne nécessite aucune authentification
- Remédiation :
 - Patchez, Patchez et encore Patchez !

<https://www.it-connect.fr/faillles-securite-critiques-nas-qnap-mars-2024/>

~~QTS 5.1.x et QTS 4.5.x
QuTS hero h5.1.x et QuTS hero h4.5.x
QuTScloud c5.x
myQNAPcloud 1.0.x~~

■ RCE sur FortiClient EMS (CVE-2023-48788)

- Injection SQL qui ne requiert pas d'être authentifié
 - Exécution de code en tant que SYSTEM
 - Injection SQL -> xp_cmdshell -> RCE
- Fortement exploitée
 - 446 serveurs FortiClient EMS exposés selon Shodan
- Passez sur les versions patchées
 - 7.2.3 pour la branche 7.2
 - 7.0.11 pour la branche 7.0

<https://github.com/horizon3ai/CVE-2023-48788> (PoC)

<https://www.bleepingcomputer.com/news/security/exploit-released-for-fortinet-rce-bug-used-in-attacks-patch-now/>

Failles / Bulletins / Advisories

Navigateurs (principales failles)

■ 7 failles du côté de Chrome, dont des 0-day 🚨

- [CVE-2024-2886] Use-after-free dans WebCodecs
- [CVE-2024-2887] Type “Confusion” dans WebAssembly
- Montez de version !
 - Windows & Mac : 123.0.6312.86/.87
 - Linux : 123.0.6312.86

https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_26.html

Failles / Bulletins / Advisories

Applications / Framework / ... (principales failles)

■ Faille dans la librairie “Aiohttp” exploitée par ShadowSyndicate (CVE-2024-23334)

- Librairie Python permettant la gestion de requêtes HTTP asynchrones
 - Elle-même basée sur le framework Python d’E/S AsyncIO
- Faille de type “Path transversal” pour une personne non authentifiée
 - Permettant l’accès à des ressources sensibles sur le serveur 🕸
- Toutes les versions < 3.9.2 sont affectées
- Le groupe ShadowSyndicate (ransomware) à la recherche de serveurs vulnérable
 - = scans + tentatives d’exploitations
- Selon ODIN : +44.500 serveurs exposés ont une en-tête HTTP correspondant à Aiohttp

<https://www.youtube.com/watch?v=DhRQVjspH6I> (vidéo)

<https://www.it-connect.fr/aile-de-securite-aiohttp-cve-2024-23334-exploitee-ransomware-shadowsyndicate/>

```
81[.]19[.]136[.]251
157[.]230[.]143[.]100
170[.]64[.]174[.]95
103[.]151[.]172[.]28
143[.]244[.]188[.]172
```

Failles / Bulletins / Advisories

Applications / Framework / ... (principales failles)

■ Multiples failles sur GLPI (CVE-2024-27096)

- 5 vulnérabilités moyennes et 1 élevée
 - Moyennes : **CVE-2024-27098** (SSRF), **CVE-2024-27104** & **CVE-2024-27914** (XSS), **CVE-2024-27930** (accès à des données sensibles) et **CVE-2024-27937** (énumération des emails)
 - Élevée : **CVE-2024-27096** (injection SQL via le moteur de recherche)
- Pour exploiter ces vulnérabilités, il est nécessaire que l'attaquant soit authentifié
 - Mais ne vous reposez pas sur cette spécificité 😊
- Passez à la version 10.0.13
 - Surtout que GLPI enchaîne les vulnérabilités critiques (RCE en 10/2023, injections SQL en 12/23)

<https://glpi-project.org/fr/sortie-de-glpi-10-0-13/>

Failles / Bulletins / Advisories

Applications / Framework / ... (principales failles)

■ Faille critique sur ScreenConnect (CVE-2024-1709)

- Partie serveur vulnérable (on-premise et SaaS)
 - RCE unauthenticated
- Exploitée en masse
 - Black Basta et Bl00dy en profite
- 10.000 serveurs exposés sur Internet selon Shodan
 - Et 85% sont vulnérables
- Passez à la version 23.9.9 ou +
 - Upgrade path : 2.1 → 2.5 → 3.1 → 4.4 → 5.4 → 19.2 → 22.8 → 23.3 → 23.9

<https://www.it-connect.fr/patchez-screenconnect-faille-critique-exploitee-ransomware-black-basta-et-bl00dy/>



Failles / Bulletins / Advisories

Applications / Framework / ... (principales failles)

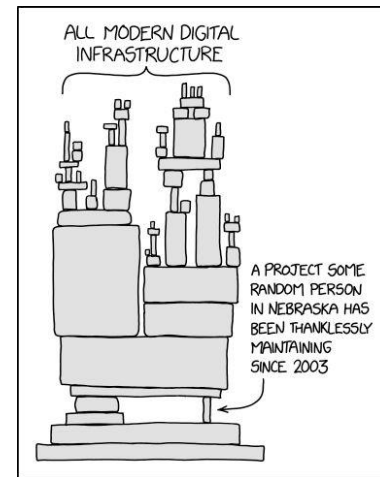
Porte dérobée sur XZ Utils, on a évité le pire ! (CVE-2024-3094)

- 2 versions impactées par une supply chain : 5.6.0 et 5.6.1
 - Code malveillant poussé dans des fichiers m4 obfusqués (jeux de tests)
 - Porte dérobée activée en mars 2024 (un mois après l'avoir déployée)
- Que fait-elle ?
 - Détournement de l'authentification en hardcodant une clé ED448
- Provient d'un contributeur sur le projet actif depuis 3 ans... #JiaT75
- Trouvée par Andres Freund (ingénieur Microsoft) 🙌🙌🙌
 - Suite à des latences sur ses connexions SSH
 - Fun fact : OpenSSH n'utilise même pas XZ
 - Il utilise Libsystemd qui lui dépend de Liblzma
- Affecte :
 - Version unstable et testing de Debian (ouffff)
 - Fedora 41 et Rawhide
 - Arch Linux

<https://linuxfr.org/users/ytterbium/journaux/xz-liblzma-compromis>

<https://www.openwall.com/lists/oss-security/2024/03/29/4>

<https://github.com/amlweems/xzbot> (PoC)



When a girl
flirts



notice a
library
running 0.2s
slower

Failles / Bulletins / Advisories

Applications / Framework / ... (principales failles)

■ **N'exposez pas votre framework IA Ray !**

- Framework d'intelligence artificielle : Ray
 - Exécute des charges de travail qui servent à former, déployer et affiner des modèles d'IA machine learning
- 5 vulnérabilités découvertes en 2023
 - 4 corrigées car la dernière n'est pas considérée comme une faille :
 - Absence d'authentification
 - << Ray s'attend à fonctionner dans un environnement réseau sûr et à agir sur un code fiable >>

<https://docs.ray.io/en/latest/ray-security/index.html#best-practices> (documentation de l'outil)

<https://www.lemondeinformatique.fr/actualites/lire-un-mauvais-deploiement-du-framework-ia-ray-fragilise-des-milliers-de-serveurs-93386.html>

Failles / Bulletins / Advisories

Applications / Framework / ... (principales failles)

■ Plusieurs XSS sur Joomla

- 5 failles XSS pouvant entraînées une RCE
 - **CVE-2024-21722 -> CVE-2024-21726**
 - Lien malveillant envoyé à un admin du site + son clic = RCE
- Patchez !
 - Joomla 4.4.3 et 5.0.3 disponibles

<https://www.bleepingcomputer.com/news/security/joomla-fixes-xss-flaws-that-could-expose-sites-to-rce-attacks/>

Failles / Bulletins / Advisories

Applications / Framework / ... (principales failles)

■ Grosse(s) faille(s) sur Firefox (CVE-2024-2615)

- 12 failles de sécurité
 - 5 importantes et 1 critique liées à la **CVE-2024-2615**
 - Problème de sécurité dans la mémoire entraînant une exécution de code
- Passez sur Firefox 124
 - Et à la 115.9 pour Firefox ESR
 - Et à la 115.9 pour Thunderbird

<https://www.mozilla.org/en-US/security/advisories/mfsa2024-12/>

Failles / Bulletins / Advisories

Applications / Framework / ... (principales failles)

■ **Élévation de privilèges dans le sous-système Nftables (CVE-2023-0179)**

- Réside dans le stockage des en-têtes VLAN
 - Qui peut entraîner un buffer overflow (et une réécriture des registres au passage 😊)
- Affecte toutes les versions Linux entre la 5.5 et la 6.2-rc3
 - Si vous ne pouvez pas mettre à jour nftables, vous pouvez désactiver les chaînes concernées

<https://github.com/TurtleARM/CVE-2023-0179-PoC?tab=readme-ov-file> (PoC)

<https://ethicalhacking.uk/cve-2023-0179-a-buffer-overflow-vulnerability-in-the-linux-kernel/#gsc.tab=0>

■ **Faible SQL critique dans le connecteur JDBC de PostgreSQL (CVE-2024-1597)**

- Permet d'accéder aux données stockées dans les BDD et de les manipuler
- Prérequis : le mode "PreferQueryMode=SIMPLE" doit être actif
- Les versions antérieures aux versions suivantes sont concernées :
 - 42.7.2, 42.6.1, 42.5.5, 42.4.4, 42.3.9 et 42.2.8

<https://www.it-connect.fr/connecteur-jdbc-postgresql-affecte-faible-securite-critique-cve-2024-1597/>

Failles / Bulletins / Advisories

Applications / Framework / ... (principales failles)

■ **Faille critique sur Zoom (CVE-2024-24691)**

- RCE via un 1-click
 - Lien malveillant ou ouverture d'un fichier malveillant ?
 - Pas plus d'informations
- Affecte plusieurs produits Zoom, mettez à jour :
 - Zoom Desktop Client : 5.16.5
 - Zoom VDI Client : 5.16.10
 - Zoom Rooms Client : 5.17.0
 - Zoom Meeting SDK : 5.16.5

<https://www.zoom.com/en/trust/security-bulletin/>

Failles / Bulletins / Advisories

Applications / Framework / ... (principales failles)

Failles critiques sur VMware ESXi, Workstation, Fusion et Cloud

- Jail escape (possibilité d'accéder à l'hôte physique à partir d'une VM)
 - CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, CVE-2024-22255 (1 par solution)
- Nécessitent les droits administrateurs sur la VM
- Use-after-free présent dans les contrôleurs XHCI et UHCI USB
 - Permettant d'exécuter du code sur l'hyperviseur (au nom du processus VMX)
- Mettez à jour ou retirez le contrôleur USB des VM

<https://www.it-connect.fr/vmware-esxi-workstation-fusion-vulnerabilites-critiques-mars-2024/>

Response Matrix:

Product	Version	Running On	CVE Identifier	CVSSv3	Severity	Fixed Version (1)	Workarounds
ESXi	8.0	Any	CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, CVE-2024-22255	8.4, 8.4, 7.9, 7.1	Critical 	ESXi80U2sb- 23305545	KB96682
ESXi	8.0 [2]	Any	CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, CVE-2024-22255	8.4, 8.4, 7.9, 7.1	Critical 	ESXi80U1d- 23299997	KB96682
ESXi	7.0	Any	CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, CVE-2024-22255	8.4, 8.4, 7.9, 7.1	Critical 	ESXi70U3p- 23307199	KB96682
Workstation	17.x	Any	CVE-2024-22252, CVE-2024-22253, CVE-2024-22255	9.3, 9.3, 7.1	Critical 	17.5.1	KB96682
Fusion	13.x	MacOS	CVE-2024-22252, CVE-2024-22253, CVE-2024-22255	9.3, 9.3, 7.1	Critical 	13.5.1	KB96682

Failles / Bulletins / Advisories

Réseau (principales failles)

La requête DNS qui va coûter chère, Keytrap (CVE-2023-50387)

- Vulnérabilité dans DNSSEC
 - Et dans son traitement des signatures
- Un seul paquet = entre **56 secondes et 16 heures** pour le traiter ! 🤖
- Affecte les services DNS les plus connus
 - Bind9, dnsmasq, PowerDNS, le DNS sur Windows Server, etc.
- Serait exploitable depuis 1999...
 - 30% des utilisateurs 🌐 utiliseraient des résolveurs DNS vulnérables
- Patchez si possible !
 - Déjà fait du côté de Windows (Patch Tuesday 02/24)
 - Egalement du côté de Google et CloudFlare
 - Ou désactivez DNSSEC

	Name	Vuln.	Comment
Server Software	Akamai CacheServe BIND9	●	Still answers to cached entries
	Knot Resolver	●	Bigger impact due to inefficient key selection
	PowerDNS Recursor Unbound	●	Limited DNS key buffer size only allows for 126 DNSSEC keys
	Windows Server 2022	●	Retries increase attack duration
	Windows Server 2019	●	Algorithm 15 not supported
	unwind (from OpenBSD7.3)	●	Algorithm 15 not supported
	Technitium dnsmasq 2.80	●	Limited msg-buffer size only allows for 15625 validations
	stubby 0.4.3	●	Limited msg-buffer size only allows for 2500 validations
	Cloudflare	●	-
	Google	●	-
Service	OpenDNS Quad9	●	Confirmed by Developers
	Quad9	●	Confirmed by Developers
Tool	dig 9.16.1	○	No DNSSEC validation
	kdig 2.7.8	○	No DNSSEC validation
	dely 9.16.1	●	Validation logic from Bind9
	DNSViz 0.9.4 (latest)	●	Throws exception after attack
	ldns-verify-zone kzonecheck	●	uses vulnerable ldns library shipped with Knot DNS authoritative server
Libs	named-checkzone	○	does not validate signatures
	dnspython	●	-
	getdns	●	used by stubby
	ldns libunbound	●	used by Unbound

TABLE I: Vulnerable DNS implementations.

<https://www.bleepingcomputer.com/news/security/keytrap-attack-internet-access-disrupted-with-one-dns-packet/>

Failles / Bulletins / Advisories

Réseau (principales failles)

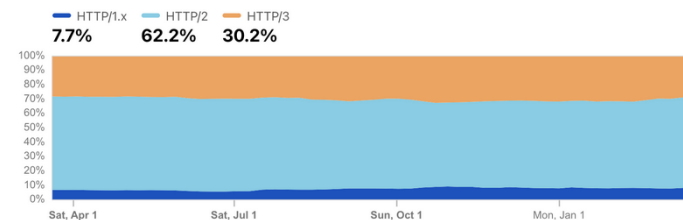
Après Rapid Reset sur HTTP/2, CONTINUATION Flood

- Ensemble de 9 failles de sécurité (1 par implémentation)

Nhttp2	AMPHP	Apache HTTP	Arista Networks	Red Hat	SUSE Linux	Node.js	Envoy	Go
CVE-2024-27983	CVE-2024-27919	CVE-2024-2758	CVE-2024-2653	CVE-2023-45288	CVE-2024-28182	CVE-2024-27316	CVE-2024-31309	CVE-2024-30255
?	?	< 2.4.59	?	?	?	?	< 1.29.2	?

- Un seul paquet TPC extrêmement long sans “END_HEADERS” = DoS 🤖

<https://www.it-connect.fr/vulnerabilite-continuation-flood-dans-http2-expose-serveurs-web-attaques-dos/>



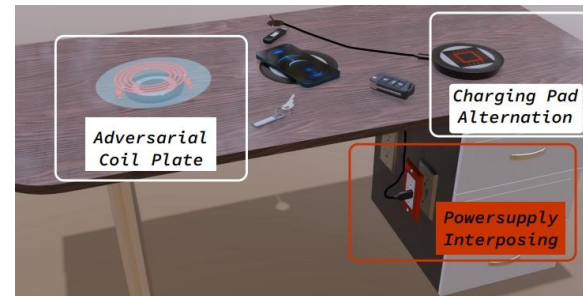
Failles / Bulletins / Advisories Smartphones (principales failles)

■ Hack explosif ✨

- Attaque VoltSchemer
 - Cible les chargeurs sans-fil
 - Injection d'IEMI via un émetteur externe
- Conséquences ?
 - Prise de contrôle d'assistance vocale
 - Contournement du mécanisme de protection de la norme Qi
 - Destruction de l'appareil rechargé et des appareils / objets aux alentours
- 9 appareils testés = 9 appareils vulnérables
 - Marques Anker, Philips, Renesas, WaiWaiBear
 - Il y en a sûrement d'autres...

<https://arxiv.org/pdf/2402.11423.pdf> (travaux des chercheurs)

<https://www.it-connect.fr/attaque-voltschemer-cible-les-chargeurs-sans-fil-et-peut-faire-exploser-votre-smartphone/>



Failles / Bulletins / Advisories *Smartphones (principales failles)*

■ **Passez à iOS 17.4 ! (ou iPad 17.4)**

- 2 vulnérabilités 0-day dans le Kernel et dans RTKit
 - CVE-2024-23225 & CVE-2024-23296
 - Permettent de contourner les protections kernel
- Pas plus d'informations techniques
- Profitez au passage de la conformité d'Apple avec le DMA 
 - Prise en charge des magasins d'applications tiers
 - Possibilité de choisir son navigateur web par défaut

<https://www.bleepingcomputer.com/news/apple/apple-fixes-two-new-ios-zero-days-exploited-in-attacks-on-iphones/>



Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Piratages

La CISA victime des failles Ivanti

- Vulnérabilités sur les solutions Ivanti X Secure énormément exploitées début 2024...
 - Cf. revue OSSIR <https://www.ossir.org/paris/supports/2024/2024-02-13/2024-02-13.pdf> 😊
- 2 systèmes du CISA impactés par ces failles
 - Système permettant le partage d'outils d'évaluations cyber entre entités
 - + Système hébergeant les informations sur l'évaluation de la sécurité des installations chimiques
 - = Informations sensibles...
- Aucun impact opérationnel selon la CISA
 - Cela leur permet de se << mettre à niveau et de moderniser nos [ses] systèmes >>

<https://www.it-connect.fr/cyberattaque-cisa-americaine-victime-des-failles-ivanti/>



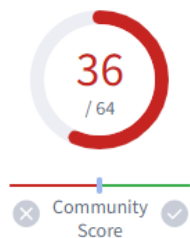
Piratages, Malwares, spam, fraudes et DDoS

Malware


AcidPour, le malware qui cible Linux

- Variante du malware AcidRain
 - Type “data wiper”
 - 30% de code source en commun
- Utilisé contre Viasat début mars
- Ennemi de l’IoT (Linux x86) et des équipements réseaux
 - Tout ce qui contient des chemins types `/dev/dm-XX` (LVM), `/dev/ubiXX`, etc.

<https://www.bleepingcomputer.com/news/security/new-acidpour-data-wiper-targets-linux-x86-network-devices/>



! 36/64 security vendors and no sandboxes flagged this file as malicious Reanalyze Similar More

6a8824048417abe156a16455b8e29170f8347312894fde2aabe644c4995d7728	Size	Last Modification Date	
6a8824048417abe156a16455b8e29170f8347312894fde2aabe644c4995d7728.elf	16.98 KB	14 minutes ago	

elf self delete

Piratages, Malwares, spam, fraudes et DDoS

Malware

Anatsa, le malware Android

- De + en + actif depuis novembre 2023 en Europe
 - 5 campagnes pour 5 zones géographiques ciblées
 - UK, Allemagne, Espagne, Slovaquie, Slovénie et Rep. Tchèque (oui ça fait 6 🤪)
 - + de 150 000 appareils infectés
- Type info-stealer (vole les identifiants bancaires)
- Se cache dans des applis présentes sur le Google Store
 - Phone Cleaner, PDF Viewer, PDF Reader...

<https://www.threatfabric.com/blogs/anatsa-trojan-returns-targeting-europe-and-expanding-its-reach>

Piratages, Malwares, spam, fraudes et DDoS

Malware

Info Stealer sur les PC AceMagik

- Mini-PCs performants au prix attractif
- Mais malheureusement...
 - Fournis avec des infos-stealer pour le même prix ! (sans demander votre avis)
- Marque chinoise
 - Coïncidence ?!

<https://hothardware.com/news/acemagic-ends-spyware-preinstalled-on-pcs>



Piratages, Malwares, spam, fraudes et DDoS

Malware

■ Backdoor du moment pour MAC : RustDoor

- Faite en Rust ce qui permet d'affecter toutes les puces utilisées par MAC
 - Intel (architecture x86_64) + Apple Silicon (architecture ARM)
- Cachée dans un outil de mise à jour Visual Studio
 - Rappel : Visual Studio pour MAC sera abandonnée à partir du 31 août 2024
- Connectée à 4 serveurs C2
 - Supporte un ensemble de commandes : shell, botkill, taskkill, download, upload ainsi que l'ajout de jobs Cron pour la persistance
 - Prend le contrôle des systèmes compromis et exfiltre ses données
- Distribuée furtivement pendant 3 mois avant d'être repérée
 - Nombre de systèmes compromis = ~ utilisateurs de VS sur MAC x86 et ARM 🙈

<https://securityaffairs.com/158942/malware/macOS-backdoor-rustdoor.html>

Piratages, Malwares, spam, fraudes et DDoS

Fuites de données

■ Fuite de données massive chez France Travail

- 43 millions de personnes impactées (2/3 tiers des français 🤖)
 - N'oublions pas la précédente fuite de données chez Pôle Emploi en août 2023...
- Qui est concerné ?
 - Personnes actuellement inscrites
 - Personnes précédemment inscrites au cours des **20 dernières années** *
 - Personnes non inscrites sur la liste de demandeurs d'emploi ayant un compte sur franetravail.fr
- * Historique sur 20 ans ? On est loin des 10 ans renseignés sur leur site 🤖
- Données concernées : nom, prénom, date de naissance, n° de sécurité sociale, identifiant France Travail, email, n° de téléphone, adresse postale
- 3 jeunes suspects (~ 20 ans) mis en examen
 - Accès aux données via une usurpation de l'identité d'un agent de Cap Emploi par téléphone 🤖
- Impossible maintenant de s'authentifier sur le site via son compte Ameli (car id = n° de secu)

https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/france-travail-annonce-avoir-ete-la-cible-d-une-cyberattaque-43-millions-de-personnes-potentiellement-concernees_6422023.html

Piratages, Malwares, spam, fraudes et DDoS

Fuites de données

■ Fuite de données chez YX International menaçant votre 2FA

- Entreprise asiatique spécialisée dans la fabrication d'équipements de réseau cellulaire
 - Et fournissant des services de routage de SMS !
- Base de données interne exposée sur Internet (sans mot de passe)
 - Contenu des messages texte envoyés compris dans la base..
 - Codes de sécurité à usage unique
 - Liens de réinitialisation de mot de passe (Google, Meta, TikTok, etc.)
 - Espérons qu'ils aient tous expiré...
- Aucun log d'accès sur le serveur = impossible d'évaluer le nombre d'accès à la base

<https://techcrunch.com/2024/02/29/leaky-database-two-factor-codes/>

Piratages, Malwares, spam, fraudes et DDoS

Fuites de données

3 chercheurs à la recherche d'instances Firebase mal configurées

- 20 millions de mots de passe trouvés
 - 98% sont enregistrés en clair
- 916 sites web vulnérables trouvés en 1 mois
- 125 millions d'enregistrements liés à des données utilisateur
- Toutes les entreprises concernées ont été contactées
 - 842 mails ont été envoyés
 - Aucune réponse
 - 25% des entreprises notifiées ont corrigé le problème
- On stocke ses secrets en base de manière chiffrée !
 - Argon2, PBKDF2, bcrypt... et pas en MD5 ou en SHA-1 😊



<https://www.it-connect.fr/19-millions-de-mots-de-passe-en-clair-exposes-dans-des-instances-firebase-mal-configurees/>

Piratages, Malwares, spam, fraudes et DDoS

Fuites de données

■ L'administration française : à 4 mois des JO, les temps sont durs !

- Rappel : vol de PC dans un train le 26 février
 - Condamnation : 7 mois d'emprisonnement
- 2ème vol le 1 mars
 - Infraction physique sur la voiture de la secrétaire générale de l'hôpital Avicienne
 - Vol du PC contenant les plans d'accès et de circulation des hôpitaux pendant les JO

https://www.bfmtv.com/paris/jo-de-paris-2024-un-ordinateur-contenant-des-documents-confidentiels-vole-a-drancy_AN-202403040788.html

Piratages, Malwares, spam, fraudes et DDoS

Fuites de données

CAF: 4 comptes → des milliers de comptes

- Le groupe *Lulsec* revendique le piratage de 600 000 comptes de la CAF en février
 - Photo avec 4 comptes piratés
 - CAF confirme le piratages de ces 4 comptes mais assure que ce sont les seuls
- En réalité, des milliers de comptes piratés !
 - Les accès aux comptes compromis ont pu être dérobés par phishing / vishing et info stealers ?
 - Changement de mot de passe obligatoire pour les comptes concernés

<https://www.rtl.fr/actu/sciences-tech/allocations-familiales-les-donnees-de-600-000-allocataires-de-la-caf-ont-elles-ete-piratees-7900352438> (1ère version de la news)

<https://www.rtl.fr/actu/sciences-tech/piratage-de-la-caf-des-milliers-de-comptes-finalement-touchees-changement-de-mot-de-passe-obligatoire-7900356943> (2ème version)

Piratages, Malwares, spam, fraudes et DDoS

Fuites de données

■ Attention à ne pas push vos secrets !

- 12.8 millions de secrets d'authentification disponibles sur GitHub
 - Augmentation de 28% par rapport à 2022
 - France en 5ème position 😬
 - Mots de passe de comptes, clés d'API, certificats SSL/TLS, clés de chiffrement, jetons OAuth...
 - Mise en place d'une protection par défaut, pour éviter cette exposition, par GitHub
 - Solution alternative : "Has My Secret Leaked" # GitGardians 🇫🇷
 - Cf. revue OSSIR https://www.ossir.org/paris/supports/2023/2023-12-12/2023-12-12_OSSIR-20231212-v0.1.pdf 😊
- <https://www.gitguardian.com/hasmysecretleaked#how-to-create-hash> (solution de GitGardians)
- <https://www.it-connect.fr/2023-plus-de-12-millions-secrets-authentification-divulgues-github/>

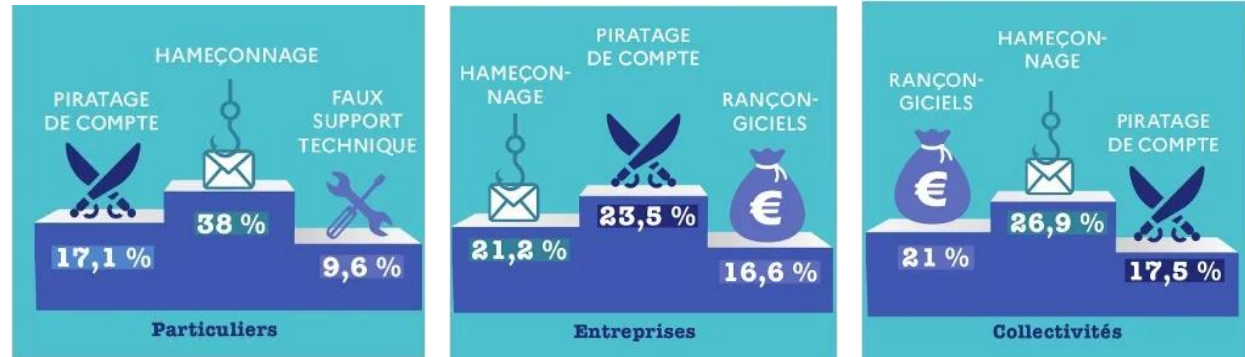
Piratages, Malwares, spam, fraudes et DDoS

Publication

Rapport d'activité 2023 de Cybermalveillance.gouv.fr

- Inclus des chiffres clé liés à la plateforme
 - 280.000 demandes d'assistance (+15% vs 2022)
- Et les tendances de l'année (tout public)
 - Principale menace tout public : **hameçonnage** (50.000 demandes d'assistance)
 - Puis le piratage de compte et les attaques par rançongiciel
 - Phénomène de 2023 : escroquerie au faux conseiller bancaire

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/rapport-activite-2023#~:text=Entreprises,toujours%20en%20augmentation%20en%20volume>



Piratages, Malwares, spam, fraudes et DDoS

Publication

Panorama de la cybermenace 2023 #ANSSI

- Attaques par ransomware toujours au TOP 😞
 - +30% d'attaques par rapport à 2022
 - Sources majeures : LockBit puis ALPHV/Black Hat, Akira...
 - Cibles principales :
 - TPE, PME, ETI (34%)
 - Collectivités locales et territoriales (24%)
 - Etablissements de santé (1/10)
 - Comment ? Exploitation de vulnérabilité, 0-day, 1-day...
- La France pourrait être la cible de DDoS à l'occasion des JO ?
- Top 5 des vulnérabilités exploitées ----->
 - On retrouve les vulns sur VMware ESXI, MoveITet Citrix (sans surprise)
- Menace des JO prises au sérieux
 - Audits et accompagnements techniques prévus pour les entités impliquées

Avertissement: ce classement ne comptabilise que les événements pour lesquels l'ANSSI ou un prestataire d'investigation a pu confirmer avec un haut degré de certitude l'exploitation d'une vulnérabilité.

CVE	ÉDITEUR	CVSS SCORE ²⁰	RÉFÉRENCE CERT-FR
CVE-2021-21974	VMWARE	8.8	CERTFR-2023-ALE-015 CERTFR-2021-AVI-145
CVE-2023-20198	CISCO	10.0	CERTFR-2023-ALE-011 CERTFR-2023-AVI-0878
CVE-2023-3519	CITRIX	9.8	CERTFR-2023-ALE-008 CERTFR-2023-AVI-0568
CVE-2023-22518	ATLASSIAN	9.8	CERTFR-2023-AVI-0899 CERTFR-2023-ACT-048
CVE-2023-34362	PROGRESS SOFTWARE	9.8	CERTFR-2023-ALE-005

<https://www.cert.ssi.gouv.fr/cti/CERTFR-2024-CTI-001/> (document de l'ANSSI)

<https://www.it-connect.fr/lanssi-a-publie-son-panorama-de-la-cybermenace-2023-les-ransomwares-toujours-au-top/>

Piratages, Malwares, spam, fraudes et DDoS

Techniques & outils

Red Team Espionner des appareils via leur Bluetooth, BlueSpy

- Automatisation de la chaîne d'infection
 - Identification de l'appareil + appairage (utilisant la feature "JustWorks")
- Le son généré sur l'appareil cible et sauvegardé puis exporté
- Recommandations de Tarlogic
 - Forcer la demande d'appairage auprès de l'utilisateur
 - Notifier l'utilisateur de l'appairage
 - Pouvoir activer/désactiver l'état de découvrabilité et d'appairage de l'appareil

<https://www.tarlogic.com/bsam/controls/bluetooth-pairing-without-interaction/> (plus d'infos sur la vuln exploitée)

<https://github.com/TarlogicSecurity/BlueSpy> (outil)

Piratages, Malwares, spam, fraudes et DDoS

Techniques & outils

■ Outil de déchiffrement pour le ransomware Rhysida

- 1er apparition du ransomware en mai 2023
 - Victimes connues : British Library + hôpitaux et cliniques
- Vulnérabilité dans le schéma de chiffrement du ransomware
 - Utilise l'heure du système afin de générer la clé de chiffrement
- Equipe coréen de 5 chercheurs de l'université Kookmin en collaboration avec la KISA

<https://seed.kisa.or.kr/kisa/Board/166/detailView.do> (outil + documentation)

<https://www.bleepingcomputer.com/news/security/free-rhysida-ransomware-decryptor-for-windows-exploits-rng-flaw/>



Conférences

Conférences

Passée(s)

- Defcon, 12 février 2024 à Paris
- JSSI, 12 mars 2024 à Paris
 - Thème : « Intelligence artificielle et [in]sécurité »
- CoRIIN, 26 mars 2024 à Lille
 - En parallèle du FIC
- FIC, 26 au 28 mars 2024 à Lille

À venir

- sambaXP, 17 au 18 avril 2024 via Zoom
- BotConf, 24 au 26 avril 2024 à Nice #BoufConf / #BouffeConf
- SSTIC, 05 au 07 juin 2024 à Rennes
- Pass The Salt, 03 au 05 juillet 2024 à Lille
- LeHack « Compile », 05 au 07 juillet 2024 à Paris (20ème édition !)



Divers / Trolls velus

Divers / Trolls velus

■ (Presque) N'importe qui sur X peut vous appeler 📞

- Nouvelle fonctionnalité (cachée) sur X activée par défaut
 - → “Activer les appels audio et vidéo”
 - Désactivée si vous DM sont fermés !
- Uniquement les abonnés **Premium** peuvent vous appeler (bon, 3\$)
 - Mais peuvent appeler n'importe quel type de compte (premium ou non)
- Prérequis ?
 - Uniquement les personnes que vous suivez peuvent vous appeler (par défaut)
 - Il faut que vous ayez envoyé au moins un message privé à la personne voulant vous appeler
 - Pas forcément une grande mesure de sécurité
- Risque de recevoir un appel (même sans répondre) ? Donner votre IP gratuitement 🗨️
 - Peut-être utile pour faire de l'OSINT !

<https://help.twitter.com/en/using-x/direct-messages/audio-video-calls>

Divers / Trolls velus

■ Vainqueur (encore) du concours Pwn2Own : Synacktiv 🇫🇷

- Thème : automobile
 - Mise en évidence de multiples vulnérabilités permettant de prendre le contrôle du véhicule
- 8 failles exploitées !
 - Chargeurs de véhicules (4 vulns - remote)
 - Autoradio (1 vuln - USB)
 - OS (1 vuln - USB)
 - Tesla ✂️ (co-sponsor) (2 vulns - remote)



https://www.synacktiv.com/sites/default/files/2023-11/tesla_codeblue.pdf (RETEX Pwn2Own 2023)

<https://www.solutions-numeriques.com/pwn2own-2024-synacktiv-remporte-lepreuve-en-prenant-le-controle-dune-tesla/>

Divers / Trolls velus

■ Copilot for Security #MICROSOFT

- Date de sortie : 1er avril 2024 (not a joke)
- IA générative << for cybersecurity >>
- Nativement intégrable aux outils Microsoft (365, Defender, XDR...)
 - Gain de temps & traitement des incidents ++
 - Quid de nos données ?

<https://www.microsoft.com/en-us/security/business/ai-machine-learning/microsoft-copilot-security#modal-41>



Divers / Trolls velus

La fin de LockBit, vraiment ? Vous êtes sûr ?

- Opération Cronos ✂
 - Lancée en 2022 par Eurojust
 - Coordonnée par Europol et la NCA
 - 11 pays : UK, USA, Allemagne, France, Japon, Australie...
 - But ? Mettre fin aux activités de LockBit (3.0)
- Résultats ?
 - 34 serveurs stoppés 🌐
 - 200 comptes de cryptomonnaie gelés
 - 14.000 comptes en ligne fermés
 - 1.000 clés de déchiffrement récupérés
 - Outil développé par la suite et disponible sur No More Ransom 🙌
 - 2 arrestations 🇷🇺 🇺🇦
- RCE liée à la CVE-2023-3824 (PHP) à l'origine de cette histoire ?
 - LockBitSupp en rigole << parce que, après avoir nagé dans l'argent pendant cinq ans, je suis devenu très paresseux >>
 - Et le FBI profite de sa victoire (qui aura été courte) (cf. image)
- Perspectives de changement de carrière ?
 - Le FBI propose 15 millions de \$ en échange d'informations (utiles) sur LockBitSupp (#TOCRP)



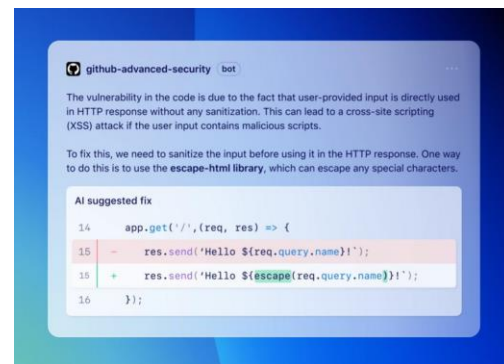
<https://www.lemagit.fr/actualites/366573933/Ransomware-un-mois-de-fevrier-marque-par-loperation-Cronos-contre-LockBit>

Divers / Trolls velus

Automatiser la correction de vulns sur GitHub avec l'IA

- “Code Scanning Autofix” = GitHub Copilot + CodeQL
- Actuellement en beta publique
 - Activé sur tous les dépôts privés des utilisateurs de GitHub Advanced Security
- Correction automatique du code + explications des améliorations
 - Le développeur peut accepter, modifier ou rejeter les propositions de l'IA
- Prend en charge : JS, TypeScript, Java et Python
 - Et également C# et Go d'ici quelques mois

<https://docs.github.com/en/code-security/code-scanning/managing-code-scanning-alerts/about-autofix-for-codeql-code-scanning>



Divers / Trolls velus

■ Identification de fichier avec Magika (#Google)

- Types de fichiers binaires et textuels
- Paquet Python (`$ pip install magika`) ou version en ligne (<https://google.github.io/magika/>)
- Déjà utilisé sur Gmail, Drive, Safe Browsing et sur VirusTotal !

<https://github.com/google/magika> (outil)

<https://www.it-connect.fr/magika-outil-open-source-google-identifier-fichiers-grace-a-ia/>

```
$ magika -r examples/  
examples/README.md: Markdown document (text)  
examples/bmp.bmp: BMP image data (image)  
examples/code.asm: Assembly (code)  
examples/code.py: Python source (code)  
examples/doc.docx: Microsoft Word 2007+ document (document)  
examples/doc.ini: INI configuration file (text)  
examples/elf64.elf: ELF executable (executable)  
examples/flac.flac: FLAC audio bitstream data (audio)  
examples/java.class: Java compiled bytecode (executable)  
examples/jpg.jpg: JPEG image data (image)  
examples/pdf.pdf: PDF document (document)  
examples/pe32.exe: PE executable (executable)  
examples/png.png: PNG image data (image)  
examples/tar.tar: POSIX tar archive (archive)  
examples/webm.webm: WebM data (video)
```

Content type	File magic		File Mime		Exif Tool		TrID		Guess Lang		Magika	
	Prec	Recall	Prec	Recall	Prec	Recall	Prec	Recall	Prec	Recall	Prec	Recall
APK	90%	72%	90%	72%	n/a	n/a	99%	72%	n/a	n/a	99%	99%
Jar	70%	60%	70%	60%	n/a	n/a	67%	81%	n/a	n/a	99%	97%
C	43%	97%	43%	97%	n/a	n/a	n/a	n/a	96%	87%	99%	99%
Java	93%	72%	93%	72%	n/a	n/a	n/a	n/a	82%	93%	99%	99%
JavaScript	90%	74%	90%	74%	n/a	n/a	n/a	n/a	93%	83%	99%	99%
Python	94%	94%	94%	82%	99%	13%	n/a	n/a	87%	94%	99%	99%
Powershell	100%	0.6%	n/a	n/a	n/a	n/a	n/a	n/a	89%	93%	99%	99%
VBA	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	88%	36%	99%	99%
CSV	91%	64%	91%	64%	n/a	n/a	n/a	n/a	49%	66%	99%	98%
HTML	44%	84%	44%	84%	86%	77%	75%	71%	46%	86%	99%	89%
YAML	n/a	n/a	n/a	n/a	n/a	n/a	100%	0.1%	62%	91%	99%	99%
INI	13%	1%	6%	1%	n/a	n/a	60%	38%	17%	90%	99%	98%
Overall	92%	72%	92%	71%	91%	41%	93%	67%	73%	22%	99%	99%

■ Vos cookies de session enfin protégés ?

- Cookies de session stockés sur votre machine = risque (info stealer 😊)
- Nouvelle feature from Google : **Device Bound Session Credentials (DBSC)**
 - Vos cookies seront chiffrés par une bi-clé stocké sur votre puce TPM
 - 1 bi-clé par cookie de session !
 - Vos cookies volés, seuls, deviendront donc inutiles
 - Taux d'erreur de l'ordre de 0,001%
- Actuellement en cours de développement
 - Première version experimentable activable sur Chrome via "chrome://flags" (enable-bound-session-credentials)

<https://github.com/WICG/dbsc> (feature open-source)

<https://www.bleepingcomputer.com/news/security/new-chrome-feature-aims-to-stop-hackers-from-using-stolen-cookies/>

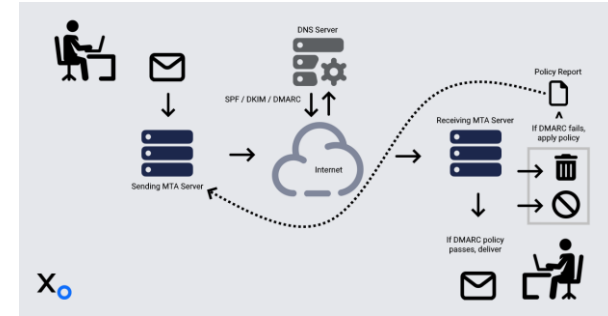
Divers / Trolls velus

SPF, DKIM et DMARC sinon 📧 🗑️

- Normes demandées pour être un SENDER de confiance
 - Sinon vos mails seront rejetés par Google et Yahoo
- Blocage effectif par ces ESP depuis avril 2024
- But : bloquer les spams & phishing

<https://www.xomedia.io/blog/a-deep-dive-into-email-deliverability/>

<https://www.mail-tester.com/> (testez le niveau d'indésirabilité de vos mails)



Et maintenant ?

Prochaine réunion ?

RDV le mardi 14 mai 2024

Des questions ?

- C'est le moment !

Des idées d'illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous



OSSIR