



Revue d'actualité de l'OSSIR

11 juin 2024

*Jérémy De Cock
Melchior Courtois*



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)

Microsoft

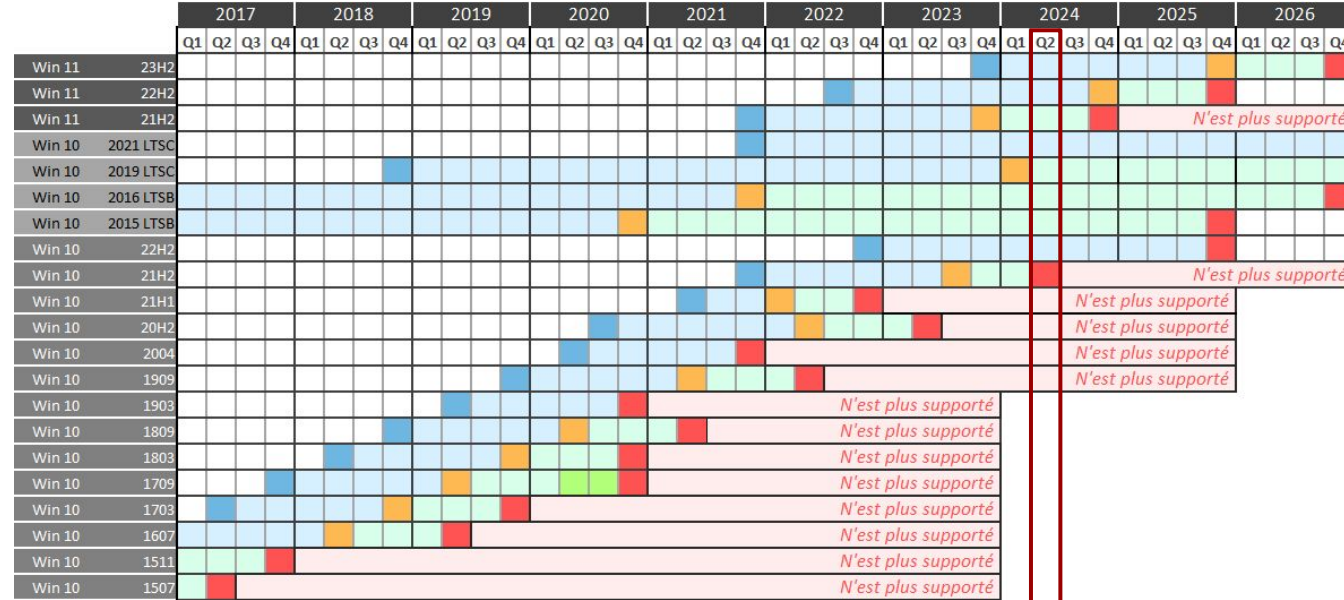
■ Bulletin de mai, 61 vulnérabilités patchées dont

- **3 vulnérabilités 0-day :**
 - **[CVE-2024-30040]** Bypass OLE dans **Microsoft 365 & Microsoft Office**
 - Toutes les versions \geq Windows 10 et Windows Server 2016 sont affectées
 - **[CVE-2024-30046]** Elévation de privilèges dans **DWM**
 - En tant que SYSTEM sinon c'est pas drôle (hein Qakbot)
 - Périmètre vulnérable semblable à la CVE-2024-30040
 - **[CVE-2024-30051]** Dénier de service dans **Microsoft Visual Studio 2022**
 - Affecte toutes les versions comprises entre la 17.4 et la 17.9
 - Difficile à exploiter selon Microsoft
- **1 autre vulnérabilité critique :**
 - **[CVE-2024-30044]** RCE dans **SharePoint Server**
 - Autorisation << Site Owner >> nécessaire

<https://www.bleepingcomputer.com/news/microsoft/microsoft-may-2024-patch-tuesday-fixes-3-zero-days-61-flaws/>

Faibles / Bulletins / Advisories (MMSBGA) Microsoft

Rappel du support Windows 10 / 11 en couleurs 🔄



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 2023
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

<-- Nous sommes là

Faibles / Bulletins / Advisories

Navigateurs (principales faibles)

■ Nouvelle 0-day sur Chrome (CVE-2024-5274)

- Présente dans le moteur JavaScript V8
 - << Type confusion >>
- Patchez !
 - Version 125.0.6422.112/.113 pour Windows & MacOS
 - Version 125.0.6422.112 pour Linux

<https://www.it-connect.fr/cve-2024-5274-la-8eme-faible-zero-day-de-2024-corrigee-dans-google-chrome/>

Failles / Bulletins / Advisories

Applications / Framework / ... (principales failles)

■ Target : Firewall Check Point

- Rapport de Check Point du 24 mai sur une mauvaise configuration de l'authentification VPN
- Compromission de plusieurs firewalls depuis 1 mois
 - Présence de comptes locaux par défaut sur les équipements avec mot de passe simple
- Recommandation : désactiver ses comptes locaux ou ajouter une couche de protection
- Check Point a publié récemment un Hotfix pour bloquer l'utilisation de ces comptes

<https://www.it-connect.fr/cyberattaques-vpn-check-point-mai-2024/>

Failles / Bulletins / Advisories

Applications / Framework / ... (principales failles)

■ 2 ème coup de marteau sur Check Point (CVE-2024-24919)

- Vulnérabilité permettant de lire les informations sur les passerelles exposées dont l'accès à distance ou mobile est activé
 - Produits vulnérables : CloudGuard Network, Quantum Maestro, Quantum Scalable Chassis, Quantum Security Gateways, Quantum Spark Appliances
- Check Point a fait une article d'installation du correctif contre cette CVE
 - Exploitée depuis le 30 avril selon le rapport de l'entreprise
 - Détails du rapport : "permet à un attaquant d'énumérer et d'extraire des hashes de mots de passe pour tous les comptes locaux, y compris le compte utilisé pour se connecter à Active Directory."
Les mots de passe faibles peuvent être compromis, ce qui entraîne d'autres abus et des mouvements latéraux potentiels au sein du réseau."

<https://www.it-connect.fr/check-point-cve-2024-24919-zero-day-vpn/>

■ Vulnérabilité dans glibc qui impacte PHP (CVE-2024-2961)

- Fonction **iconv** affectée
 - Plus précisément dans le plugin **ISO-2022-CN-EXT**
 - Survient lors du processus de conversion de caractères UCS4
- Type << out-of-bounds memory write >>
 - Contrôles insuffisants des caractères d'échappement fournis
- L'API iconv() de PHP est donc également affectée

<https://securityonline.info/cve-2024-2961-glibc-vulnerability-opens-door-to-php-attacks-patch-immediately/>

<https://www.ambionics.io/blog/iconv-cve-2024-2961-p1> (démonstration avec PHP)

■ **Vulnérabilité by design sur Foxit Reader**

- Campagne active par le groupe APT-C-35 ciblant les utilisateurs de l'application
- Vulnérabilité de conception
 - Si détection de malware : une alerte est remontée à l'utilisateur dont l'action par défaut est d'exécuter l'exploit (à valider 2 fois)
 - L'exploit va télécharger et charger des malwares comme VenomRAT, Agent-Tesla, Remcos, NjRAT, NanoCore RAT, Pony, Xworm, AsyncRAT, et DCRat
- Correction de cette vulnérabilité dans la prochaines version de Foxy Reader – non disponible encore

<https://www.it-connect.fr/cet-exploit-foxit-reader-pdf-infecter-pc-malwares/>

Failles / Bulletins / Advisories

Applications / Framework / ... (principales failles)

■ **Faille critique dans PHP (CVE-2024-4577)**

- RCE unauthenticated
 - Bypass du correctif de la **CVE-2012-1823** via des séquences de caractères
 - Liée à PHP-CGI, les exécutable PHP doivent être accessibles
 - Bypass dû à **Best-Fit Mapping**
- Affecte toutes les versions PHP sur Windows (à partir de 5.X)
 - PHP 8.3 (avant la 8.3.8)
 - PHP 8.2 (avant la 8.2.20)
 - PHP 8.1 (avant la 8.1.29)
- Autres mesures correctives
 - Bloquer les attaques avec des << Rewrite Rules >>
 - Commenter les directives dans XAMP liées aux << ScriptAlias >>

<https://securityonline.info/cve-2024-4577-critical-php-vulnerability-exposes-millions-of-servers-to-rce/>

Failles / Bulletins / Advisories

Applications / Framework / ... (principales failles)

■ **Bypass de l'authentification sur Veeam Backup (CVE-2024-29849)**

- Présente dans Veeam Backup Enterprise Manager
 - Permet de gérer plusieurs instances de Veeam
 - Non activé par défaut
- Passez à la version 12.1.2.172 de l'outil
 - Sinon, désactivez temporairement le service (ainsi que VeeamRESTSvc)
 - Cette version corrige aussi 3 autres CVE critiques (relais NTLM, etc.)

<https://www.it-connect.fr/faille-critique-veeam-backup-enterprise-manager-cve-2024-29849/>

Failles / Bulletins / Advisories

Réseau (principales failles)

■ **Routeur TP-Link Archer C5400X (CVE-2024-5035)**

- Routeur populaire pour son utilisation dans le domaine du gaming
- Faille critique avec un score CVSS4 de 10 sur 10 :
 - Permet à un attaquant d'exécuter des commandes à distance sans authentification
- Cause : binaire "rftest" exposant un service réseau vulnérable à l'injection de commande sur les ports 8888, 8889 et 8890
- Version vulnérable : 1_1.1.6 ou antérieur
- Correctif déjà en ligne

<https://www.it-connect.fr/routeur-tp-link-archer-c5400x-faille-critique-cve-2024-5035/>

Failles / Bulletins / Advisories

Applications / Framework / ... (principales failles)

■ **Faible critique côté GitHub (CVE-2024-4985)**

- Bypass de l'authentification SAML
 - Le SSO via SAML est utilisée **avec** la fonction **optionnelle** d'assertions chiffrées
- Affecte GitHub Enterprise Server
 - Plus précisément les versions antérieures à 3.13.0

<https://www.bleepingcomputer.com/news/security/github-warns-of-saml-auth-bypass-flaw-in-enterprise-server/>

■ **Et une autre côté GitLab (CVE-2024-4835)**

- XSS 1-click via le Web IDE (éditeur de code VS)
 - Leak d'informations sensibles possible (secrets, clés d'API, etc.)
- Affecte GitLab Community Edition (CE) et Enterprise Edition (EE)
 - Passez sur les versions 17.0.1, 16.11.3 ou 16.10.6

<https://www.bleepingcomputer.com/news/security/high-severity-gitlab-flaw-lets-attackers-take-over-accounts/>

Failles / Bulletins / Advisories

Autre (principales failles)

■ RCE présentes dans + de 6000 modèles #IA

- Faille présente dans la bibliothèque llama-cpp-python (**CVE-2024-34359**)
- Le package utilise Jinja2 pour des rendus dynamiques du HTML
 - Traitement des métadonnées du modèle (.gguf) hors sandbox !
 - Template malicieuse = RCE
- Passez à la version 0.2.72 de la lib
 - Validation des entrées + sandbox

<https://korben.info/faille-rce-critique-llama-cpp-python-affecte-6000-modeles-ia.html>



Piratages, Malwares, spam, fraudes et DDoS

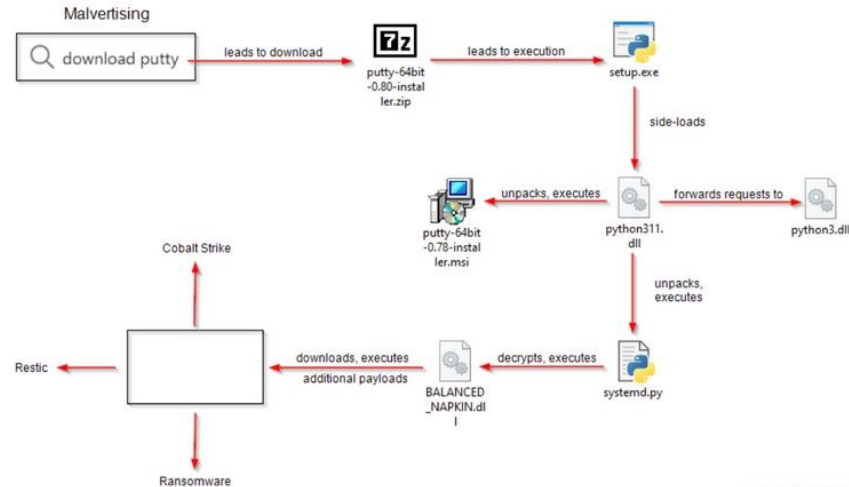
Piratages, Malwares, spam, fraudes et DDoS

Malware

Admin SYS, soyez au aguets

- Ransomware non identifié
- Cheval de Troie caché dans des publicités malveillantes pour Putty et WinSCP
 - Chargement d'une dll (malware loader) qui va aller chercher le ransomware

<https://www.it-connect.fr/malvertising-un-gang-de-ransomware-cible-les-administrateurs-systemes-sous-windows-grace-a-putty-et-winscp/>



Piratages, Malwares, spam, fraudes et DDoS

Malware

Microsoft Office, l'appât de luxe

- Diffusion en masse d'une version piratée de Microsoft Office
- Malware Loader connecté à un canal de diffusion Télégram ou Mastodon afin de récupérer un lien Drive ou GitHub pour les malwares
 - Malwares identifiés : orcus RAT, XMRig, AntiAV, PureCrypter
- Si un malware est détecté et supprimé, il est réintroduit par module Updater, exécuté au démarrage



<https://www.it-connect.fr/alerte-versions-piratees-microsoft-office-utilisees-pour-distribuer-malwares/>

Piratages, Malwares, spam, fraudes et DDoS

Ransomwares

■ Ransomware du mois : ShrinkLocker

- Utilise l'outil Bitlocker de Microsoft afin de chiffrer la victime et bloque les options de récupération
- Script VBS :
 - Vérification des prérequis avec WMI (Windows Management Instrumental)
 - Redimensionne chaque partition locale (-100Mo) et crée de nouvelles partitions
 - Réinstalle les fichiers de démarrage sur les nouvelles partitions
 - Ajoute des entrées de registre puis change le nom des partitions avec l'email de l'attaquant
 - Désactive les protections de LockBit
 - Définit une nouvelle clé de chiffrement pour les partitions à l'aide de Bitlocker puis crée une requête POST envoyant les informations à l'attaquant
 - Efface ses traces, les journaux et effectue un arrêt forcé du système

<https://securelist.com/ransomware-abuses-bitlocker/112643/>

Piratages, Malwares, spam, fraudes et DDoS

Ransomwares

■ Monti 1, Monti 2, Monti 3

- 3 victimes du malware Monti dans la nuit du 12 au 13 mai dans la ville de Pau : l'aéroport de Pau-Pyrénées, l'école de commerce et le campus numérique
- Rancon non payée mais informations volées mise en ligne donc prudence
 - Type de document fuités : des documents administratifs, des factures, des bilans RH ainsi que des informations personnelles relatives aux salariés et aux étudiants

<https://www.it-connect.fr/cyberattaques-ransomware-monti-trois-victimes-en-france-a-pau-mai-2024/>

Piratages, Malwares, spam, fraudes et DDoS

Fuites de données

■ **Zadig & Voltaire : 600 000 comptes fuités**

- Données volées en novembre 2023, et mise en ligne sur BreachForums
 - Pas d'informations sur la technique de l'obtention de cette base de données
- Informations diffusées : noms, prénoms, adresses e-mails, numéros de téléphone, adresses postales, et dates de naissance.
- Recommandation : Changer son mot de passe !!

<https://www.it-connect.fr/cyberattaque-zadig-et-voltaire-fuite-de-donnees-600000-clients/>

Piratages, Malwares, spam, fraudes et DDoS

Fuites de données

Telegram : 361 000 000 comptes fuités

- Troy Hunt, responsable de “Have I been Pwned”, a reçu une base de données de 122 Go de la part d'un acteur inconnu
 - Contient + de 1700 fichiers provenant de + de 500 canaux Telegram (scraping)
 - 361 millions d'adresses e-mails uniques, dont 151 millions ajoutées pour la première fois
- Il a indiqué avoir passé du temps à vérifier la véracité des informations et indique qu'elles semblent avérées.

```
1 https://accounts.nike.com/challenge: [redacted]@libero.it
2 https://www.toweroffantasy-global.com/: [redacted]:Alexandru2708
3 https://rafrettur.is/account/register: [redacted]@gmail.com:Gaggi2
4 https://www.footlocker.co.uk/product/yeet-1/315346047202.html:er
5 https://accounts.google.com/AddSession: [redacted]@gmail.com:To
6 https://portal1.globalautomotive.it/[redacted]:260128
7 android://nPFfHIRoyECqL0nXCFzNtgLWJ3BIwgsELe9h-roxVnhdCXE8SyP_hT
8 https://www.alnkhel.com/ar/login:[redacted]:alsafari123
9 https://www.scholarships.punjab.gov.in/sLogin.aspx:32625:[redacted]@9
10 https://www.euroimportpneumatici.com/admin.html:[redacted]@gmail.c
```

<https://www.it-connect.fr/361-millions-de-comptes-voles-divulgues-sur-telegram-etes-vous-concerne/>

Piratages, Malwares, spam, fraudes et DDoS

Fuites de données

■ Ticketmaster : 500 000 000 comptes fuités

- Violation d'accès le 20 mai et mise en vente des données le 27 mai selon Live Nation, propriétaire de Ticketmaster
- Revendication par le groupe ShinyHunters et demande de rançon
- Ticketmaster ne confirme pas la violation et indique mener l'enquête avec les autorités australiennes pour identifier le problème

<https://mashable.com/article/ticketmaster-breach-confirmed>

Piratages, Malwares, spam, fraudes et DDoS

Pannes

■ Cyberbombe de Nouvelle-Calédonie

- Cyberattaque d'ampleur "inédit" réalisé le 22 mai
- Attaque de type DDOS avec e-mail bombing entraînant le crash du serveur
- Attaque non revendiqué mais les IP pointent vers la Russie. Kremlin ?
 - effet spectaculaire, mais bref et sans conséquences à moyen terme

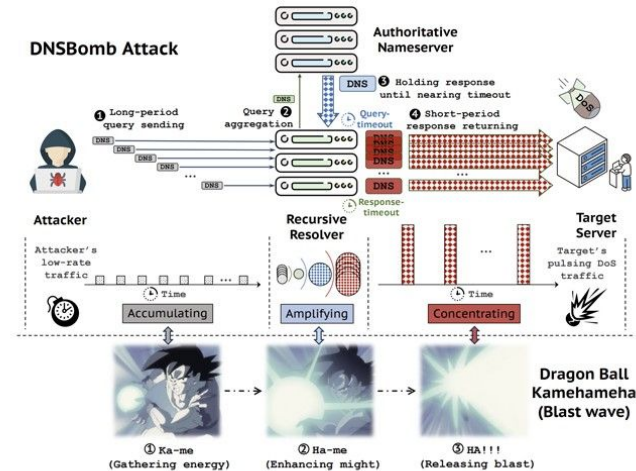
<https://incyber.org/article/une-cyberattaque-dune-ampleur-inedite-frappe-la-nouvelle-caledonie/>

Piratages, Malwares, spam, fraudes et DDoS Pannes

■ DNSBomb : Nouveau DDOS DNS (CVE-2024-33655)

- Attaque de type PDOS (**P**ulsing **D**enial-**o**f-**S**ervice)
 - Accumuler les réponses DNS pour les libérer simultanément vers une cible : ce qui fait l'effet d'une bombe
 - Facteur d'amplification X 20 000
- Services vulnérables : les services DNS et les services CDN (réseau de diffusion de contenu)
- Recommandation : Implémenter des limites comme le nombre de requêtes maximale par client

<https://www.it-connect.fr/attaque-dnsbomb-deni-de-service-dns-2024>



Threat Model of the DNSBOMB Attack.

Piratages, Malwares, spam, fraudes et DDoS

Techniques & outils

Blue Team Réécriture de YARA en Rust

- 11 ans après, toujours par VirusTotal
- Tend à remplacer YARA sur le temps
 - << YARA-X is already better than YARA in many aspects, but it's still very young and therefore some features are not implemented yet >>

<https://virustotal.github.io/yara-x/docs/intro/yara-x-vs-yara/> (YARA vs YARA-X)

<https://github.com/VirusTotal/yara-x> (outil)

Piratages, Malwares, spam, fraudes et DDoS

Techniques & outils

Blue Team Détecter des machines virtuelles cachées sur ESXI

- Il est possible de créer des machines virtuelles cachées
 - Invisibles côté UI de VMware ESXi & vCenter 🤖
 - Opération effectuée via CLI
- Pour les détecter : VirtualGHOST #CrowdStrike #PowerShell
 - Compare la liste des VM dans l'inventaire avec celles actuellement allumées
 - Retourne des infos sur les machines suspectes (config réseau, etc.)
- Module VMware PowerCLI nécessaire

<https://github.com/CrowdStrike/VirtualGHOST> (outil)

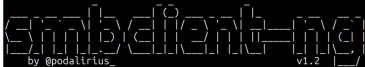
Divers / Trolls velus

Red Team Client SMB pour les pentesteurs

- Développé en Python
 - Installable via PIP
- Modulable, il inclus déjà quelques features :
 - Récupération des mots de passe inclus dans les GPP (merci Microsoft)
 - Alternative au << find >> sur Linux
- Ensemble de commandes connues :)
 - Cat, ls, cd, pwd, rm, tree, mkdir, rm, put, get...

<https://github.com/p0dalirius/smbclient-ng>

```
[smbclient-ng]$ ./smbclient-ng.py -d LAB -u Administrator -p 'Admin123!' --target 10.0.0.101
```



```
[*] Successfully authenticated to '10.0.0.101' as 'LAB\Administrator'!
```

```
•[\\10.0.0.101]> shares
```

Share	Hidden	Type	Description
admin\$	True	DISKTREE, SPECIAL	Remote Admin
c\$	True	DISKTREE, SPECIAL	Default share
ipc\$	True	IPC, SPECIAL	Remote IPC
netlogon	False	DISKTREE	Logon server share
sysvol	False	DISKTREE	Logon server share

```
•[\\10.0.0.101]> use c$
```

```
•[\\10.0.0.101(c$)]> dir
```

File Name	Size	Attributes	Creation Time	Modification Time	Access
\$Recycle.Bin\	0.00 B		2023-10-04 16:32		
Documents and Settings\	0.00 B		2023-10-05 01:29		
inetpub\	0.00 B		2023-10-04 17:01		
pagefile.sys	704.00 MB		2024-06-02 19:20		
PerfLogs\	0.00 B		2022-11-05 20:03		
Program Files\	0.00 B		2024-02-07 07:42		
Program Files (x86)\	0.00 B		2023-10-05 10:05		
ProgramData\	0.00 B		2023-11-29 16:54		
Recovery\	0.00 B		2023-10-05 01:29		
System Volume Information\	0.00 B		2024-06-02 20:11		
Users\	0.00 B		2023-10-04 16:32		
Windows\	0.00 B		2024-05-31 05:05		

```
•[\\10.0.0.101(c$)]>
```

```
•[\\10.0.0.101(c$)]>
```

Piratages, Malwares, spam, fraudes et DDoS

Techniques & outils

■ RansomLord, l'anti-ransomware

- Développé par John Page alias "hyp3rlinx"
- Outil capable de détecter et mettre aux ransomwares avant exécution de leur charge
 - Créer ses propres DLL que le ransomware va utiliser pour chiffrée le système et va ainsi pouvoir mettre fin au processus grâce à un code présent dans cette DLL
 - Lien de l'outil : <https://github.com/malvuln/RansomLord>
- Fonctionne sur de nombreux ransomware : LockBit, Wannacry, HelloGoukie, BlackCat...
 - Résultat non garanti car peut dépendre de plusieurs facteurs : version OS, emplacement du ransomware...
 - Test effectué sur machine virtuelle Windows 10 et un client mince OS intégré Win-7

<https://www.it-connect.fr/ransomlord-outil-open-source-anti-ransomware/>

Piratages, Malwares, spam, fraudes et DDoS

Techniques & outils

■ **Kaspersky Virus Removal Tool arrive sur Linux !**

- Analyse votre machine à la recherche d'artefacts ou de logiciels malveillants
 - Propose également un nettoyage des menaces détectées
 - N'effectue pas de surveillance en temps réel !
- Fonctionne sur Debian, Ubuntu, Red Hat Enterprise Linux, etc.
- Version portable only sans auto-update
- CLI ou GUI

<https://www.kaspersky.fr/downloads/free-virus-removal-tool> (outil)

<https://www.it-connect.fr/kaspersky-virus-removal-tool-linux-outil-gratuit/>



Business et Politique

■ Apple refuse de rémunérer un bug bounty à Kaspersky Lab

- 4 vulnérabilités découvertes dans l'iPhone (type 0-day)
 - Utilisées, entre autres, pour espionner les employés de Kaspersky 😂
 - Cf. opération triangulation (2023)
- Choix motivé par le contexte géopolitique actuel
 - Judicieux ou pas de se mettre des bounty hunters à dos ?

<https://therecord.media/kaspersky-apple-bug-bounty-declined>



Conférences

Conférences

Passée(s)

- SSTIC, 05 au 07 juin 2024 à Rennes
- Cyber Show Paris, 29 au 30 mai 2024 à Paris
- DEFCON Paris, 10 juin 2024 à Paris

À venir

- 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

■ Un outil qui vérifie les liens que vous recevez

- Orange Cybersecure
 - Corps de mail, site, lien, SMS
- Vérification auto (dans sa BDD) sinon par manuelle par un expert

<https://cybersecurite.orange.fr/> (outil)

<https://www.it-connect.fr/phishing-verifier-lien-suspect-avec-orange-cybersecure/>



<https://www.ticketmaster.com/>

Ce lien n'est pas identifié dans notre base de données

→ Vérification manuelle nécessaire

■ Après Cronos, opération Endgame

- Menée fin **mai 2024** et coordonnée par **Europol**
 - + France, l'Allemagne, les Pays-Bas, le Danemark, le Royaume-Uni et les Etats-Unis
- But : neutraliser les serveurs utilisés par des cybercriminels
 - Ex : BumbleBee, IcedID, Smokeloder, Pikabot, Trickbot et SystemBCT
- Résultat ?
 - Une **centaine de serveurs** & plus de **2000 noms de domaine** saisis 🙌

<https://www.europol.europa.eu/media-press/newsroom/news/largest-ever-operation-against-botnets-hits-dropper-malware-eco-system> (rapport d'Europol)

<https://www.it-connect.fr/operation-endgame-action-internationale-contre-les-cybercriminels-et-malwares/>



■ Canal+ vs les DNS alternatifs

- DNS alternatifs ?
 - Google (8.8.8.8), CloudFlare (1.1.1.1) et Cisco (OpenDNS, 208.67.222.222)
- Le but étant de les faire bloquer la résolution de noms de sites illicites
 - Sites de streaming, IPTV, etc.
 - Procédure visant également les DNS des FAI
- Canal+ veut protéger ses droits sur la F1
 - Décision de justice fin juillet
 - 30 sites diffusant illégalement des matchs du TOP 14 déjà impactés

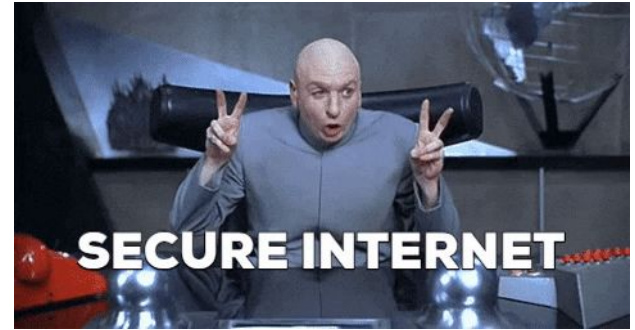
<https://www.01net.com/actualites/canal-cran-plus-loin-attaquer-iptv-illegale.html>

Divers / Trolls velus

■ Cherchez dans plus de 75 milliards de lignes de code

- Représentent plus de 40 millions de projets
 - Bitbucket, CodePlex, Fedora Project, GitLab, GitHub, etc.
 - 243+ languages
- Regex fonctionnelles + filtres
- API disponible
- Par curiosité, cherchez “password”, “key”, etc. 🤨

<https://searchcode.com/>



Et maintenant ?

Prochaine réunion ?

RDV le mardi 09 juillet 2024

Des questions ?

- C'est le moment !

Des idées d'illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous



OSSIR