AYI NEDJIMI Consultants

Infostealers : La Menace Silencieuse qui Alimente le

Catégorie : Techniques de Hacking Lecture : 12 min Publié le : 08/03/2026 Auteur : Ayi NEDJIMI

Analyse complète des infostealers en 2026 : Raccoon, RedLine, Lumma, techniques d'infection, données ciblées, marché des logs, lien avec le.

Avertissement : Les techniques présentées dans cet article sont destinées exclusivement à des fins éducatives et de tests autorisés. Toute utilisation malveillante est illégale et contraire à l'éthique professionnelle.

Le marché des infostealers est dominé par une poignée de familles qui se disputent les parts de marché du cybercrime. Chacune présente des caractéristiques techniques distinctes, mais toutes partagent un objectif commun : extraire le maximum de données exploitables d'un système compromis en un minimum de temps, généralement en moins de 30 secondes. Analyse complète des infostealers en 2026 : Raccoon, RedLine, Lumma, techniques d'infection, données ciblées, marché des logs, lien avec le. Les techniques offensives évoluent rapidement : infostealers menace silencieuse cybercrime fait partie des compétences essentielles que tout pentester et red teamer doit maîtriser pour mener des missions réalistes. Nous abordons notamment : prévention de l'exfiltration, questions frequentes et conclusion : une menace systémique qui exige une réponse globale. Les professionnels y trouveront des recommandations actionnables, des commandes prêtes à l'emploi et des stratégies de mise en œuvre adaptées aux environnements d'entreprise.

RedLine Stealer

RedLine reste l'un des infostealers les plus répandus depuis son apparition en 2020. Distribué principalement comme MaaS sur des forums russophones, il est vendu sous forme d'abonnement mensuel (environ 150 USD/mois) ou en licence à vie (environ 800 USD). Son panel d'administration web permet aux opérateurs de configurer les paramètres de collecte, de gérer les bots infectés et de télécharger les logs extraits.

Du point de vue technique, RedLine cible un éventail impressionnant de données. Il extrait les credentials stockés dans les navigateurs Chromium et Firefox, les cookies de session (y compris les cookies protégés par les mécanismes DPAPI de Windows), les données de remplissage automatique, l'historique de navigation, les données de portefeuilles crypto (extensions de navigateurs comme MetaMask, Phantom, ainsi que les clients desktop comme Exodus et Electrum), les informations système complètes (processeur, GPU, RAM, logiciels installés, solutions antivirus détectées), les tokens Discord, les fichiers ciblés par extension (`.txt`, `.doc`, `.key`, `.kdbx`), et réalise des captures d'écran du bureau de la victime.

La communication avec le serveur de commande et contrôle (C2) s'effectue via des requêtes SOAP/XML ou des API REST sur HTTP/HTTPS. Les données volées sont compressées puis exfiltrées en une seule transmission, ce qui rend la détection difficile car l'activité réseau est brève. Malgré le démantèlement de certaines infrastructures par les forces de l'ordre en 2023, de nouvelles variantes continuent d'apparaître, témoignant de la résilience de son écosystème.

Raccoon Stealer v2

Raccoon Stealer a connu un développement mouvementé. Après l'arrestation de son développeur principal, un ressortissant ukrainien, en mars 2022, l'équipe restante a lancé la version 2 (également appelée RecordBreaker) entièrement réécrite en C/C++ (la v1 était en C++). Cette réécriture a considérablement amélioré les performances et réduit la taille du binaire, facilitant son intégration dans des chaînes de distribution polymorphiques.

Le modèle commercial de Raccoon v2 repose sur un abonnement de 200 USD par mois, ce qui le place dans le segment milieu de gamme. Il se distingue par sa simplicité d'utilisation : le panel de gestion est intuitif, et les logs sont automatiquement structurés et classés par pays, navigateur et type de données volées. Les fonctionnalités couvrent l'extraction de credentials navigateur, les cookies, les données de remplissage automatique, les portefeuilles crypto, et les informations système. Le stealer collecte également les fichiers présents sur le bureau de la victime selon des filtres configurables (extension, taille maximale).

Lumma Stealer (LummaC2)

Votre surface d'attaque externe est-elle réellement celle que vous imaginez ?

Lumma Stealer, apparu fin 2022, s'est rapidement imposé comme l'un des infostealers les plus aboutis du marché. Vendu entre 250 et 1000 USD selon le plan choisi (Basic, Professional, Corporate), il se distingue par ses capacités d'évasion avancées. Lumma utilise des techniques d'anti-analyse comme la détection de machines virtuelles (VMware, VirtualBox, Hyper-V), la vérification du nombre de processeurs et de la mémoire disponible, l'inspection des noms de processus pour détecter les sandboxes (WireShark, Process Monitor, x64dbg), et le chiffrement des chaînes de caractères pour compliquer la rétro-ingénierie statique.

L'une des innovations de Lumma est sa capacité à **restaurer les cookies Google expirés**. En exploitant des mécanismes liés aux tokens de rafraîchissement OAuth, certaines versions de Lumma ont démontré la capacité de régénérer des cookies de session Google même après leur expiration ou leur invalidation par l'utilisateur. Cette fonctionnalité, si elle est confirmée dans sa pleine portée, représente une escalade significative dans les capacités des stealers, car elle pourrait permettre un accès persistant aux comptes Google des victimes, contournant ainsi les procédures de réinitialisation de mot de passe et de révocation de session.

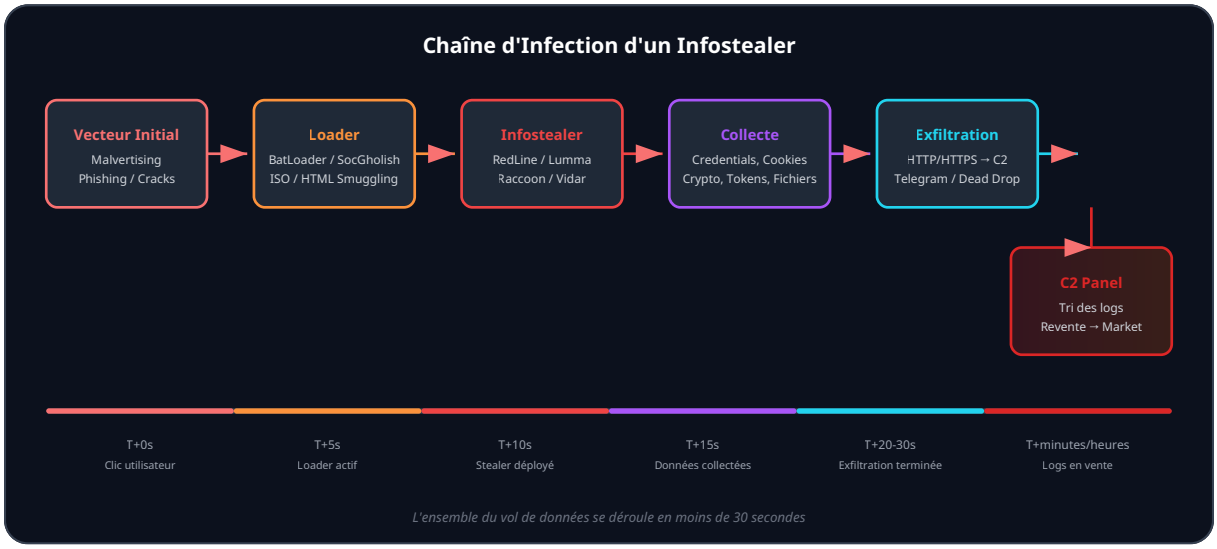
Lumma utilise également des techniques de contournement d'EDR comme le unhooking de DLL ntdll.dll, la résolution dynamique d'API via des hachages, et l'injection de code dans des processus légitimes. Son infrastructure C2 s'appuie sur des domaines générés algorithmiquement (DGA) et des communications chiffrées, rendant le blocage par indicateurs de compromission particulièrement difficile.

Notre avis d'expert
L'automatisation des tests d'intrusion ne remplacera jamais la créativité d'un pentester expérimenté. Les outils accélèrent la phase de reconnaissance, mais c'est l'intuition humaine qui identifie les chaînes d'exploitation complexes permettant d'atteindre les actifs critiques.

ISO/VHD Mounting : les fichiers image disque (`.iso`, `.vhd`, `.img`) sont montés automatiquement par Windows lors d'un double-clic. Les fichiers contenus à l'intérieur ne portent pas le Mark-of-the-Web, ce qui permet de contourner les avertissements de sécurité SmartScreen. L'image disque contient typiquement un raccourci `.lnk` pointant vers un script PowerShell ou un binaire malveillant caché dans un sous-dossier.

HTML Smuggling : cette technique consiste à encoder le payload malveillant directement dans du code JavaScript intégré à une page HTML ou à un email HTML. Lorsque l'utilisateur ouvre le fichier, le JavaScript reconstruit le binaire malveillant en mémoire et déclenche son téléchargement automatique. Cette approche contourne efficacement les passerelles de messagerie et les proxys web qui n'analysent que les fichiers joints classiques.

Loader Chains : les infostealers sont rarement délivrés directement. Ils passent par une chaîne de loaders intermédiaires : **BatLoader** utilise des scripts batch obfusqués qui téléchargent et exécutent le payload via PowerShell ou `mshta.exe`. **SocGholish** (FakeUpdates) se présente sous forme de fausses mises à jour de navigateur et utilise des frameworks JavaScript obfusqués pour déployer le stealer. **PrivateLoader** fonctionne comme un service de distribution pay-per-install, installant simultanément plusieurs malwares (infostealer + cryptominer + botnet). **SmokeLoader**, vétéran du marché, agit comme un loader modulaire capable de télécharger et d'exécuter n'importe quel payload, y compris des infostealers.



Point clé : la rapidité de l'attaque
Un infostealer typique complète l'intégralité de sa mission -- de l'exécution à l'exfiltration -- en **moins de 30 secondes**. Cette fenêtre d'exécution extrêmement courte rend la détection en temps réel très difficile, même pour les solutions EDR les plus avancées. Le malware s'auto-supprime fréquemment après l'exfiltration, ne laissant que peu de traces forensiques.

Le vol de cryptomonnaies représente la source de revenu direct la plus lucrative pour les opérateurs d'infostealers. Les cibles incluent les **extensions de navigateur** (MetaMask, Phantom, Coinbase Wallet, Trust Wallet -- les stealers extraient les fichiers de configuration

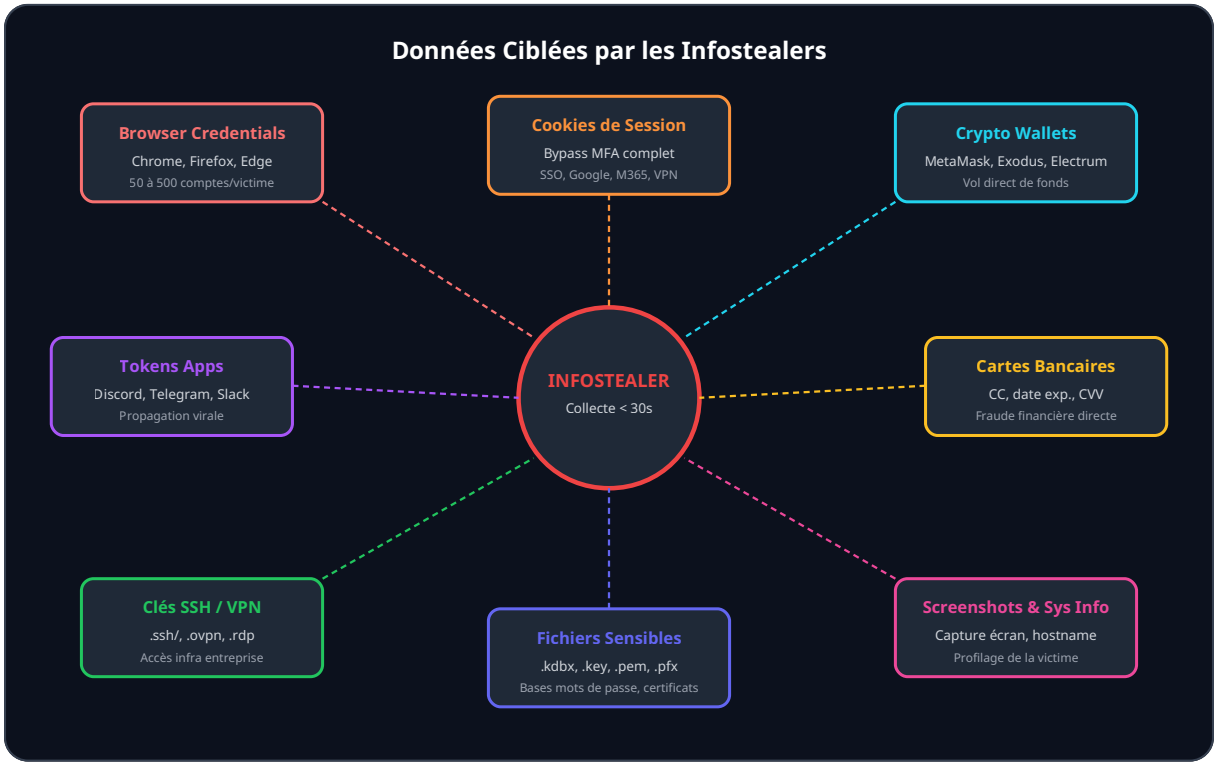
contenant les clés chiffrées et les mnémoniques), les **clients desktop** (Exodus, Electrum, Atomic Wallet, Bitcoin Core -- les répertoires de données sont directement copiés), et les **fichiers wallet** (`wallet.dat`, `keystore/`, seed phrases stockées dans des fichiers texte). Certains stealers poussés surveillent même le presse-papiers pour détecter et remplacer les adresses de portefeuilles copiées par l'utilisateur (technique du clipboard hijacking), redirigeant ainsi les transactions vers des portefeuilles contrôlés par l'attaquant.

Tokens Discord, Telegram et applications

Les **tokens d'authentification** des applications de messagerie constituent des cibles de grande valeur. Un token Discord volé permet de prendre le contrôle total du compte : accès aux messages privés, aux serveurs, possibilité de disséminer des liens malveillants aux contacts de la victime. Les tokens Telegram offrent un accès similaire. Ces comptes compromis sont ensuite utilisés comme vecteurs de distribution secondaires pour propager l'infostealer de manière virale au sein des cercles de confiance de la victime.

Données bancaires, clés SSH/VPN et fichiers sensibles

Les **données de cartes bancaires** stockées dans les navigateurs (numéro, date d'expiration, CVV lorsqu'il est enregistré) sont systématiquement extraites. Les **clés SSH** (typiquement dans `~/.ssh/`) et les **configurations VPN** (fichiers `.ovpn`, profils Cisco AnyConnect) sont également collectées car elles fournissent un accès direct aux infrastructures d'entreprise. Les stealers recherchent des fichiers sensibles par extension : `.kdbx` (bases KeePass), `.key`, `.pem`, `.pfx` (certificats), `.rdp` (connexions Bureau à distance). Les **captures d'écran** prises au moment de l'infection et les **données système** complètes (nom d'hôte, domaine, IP, processus, logiciels installés, solutions de sécurité présentes) enrichissent le profil de la victime et aident les acheteurs de logs à évaluer la valeur de la cible.



```
LOG_FR_Chrome_2026-02-10/
├── Browsers/
│   ├── Chrome_Default_Passwords.txt      # URL | Login | Password
│   ├── Chrome_Default_Cookies.txt        # Host | Cookie | Value | Expiry
│   ├── Chrome_Default_Autofill.txt       # Nom, adresse, téléphone
│   ├── Chrome_Default_CreditCards.txt    # Numéro | Exp | Nom
│   ├── Firefox_default_Passwords.txt
│   └── Edge_Default_Passwords.txt
├── Crypto/
│   ├── MetaMask/                         # Vault data
│   ├── Exodus/                           # seed, conf
│   └── wallet_addresses.txt
├── Files/
│   ├── Desktop_files.txt                 # Fichiers bureau ciblés
│   └── Documents/                        # .kdbx, .key, .pem
├── Tokens/
│   ├── Discord_tokens.txt
│   └── Telegram_tdata/
├── System/
│   ├── SystemInfo.txt                    # OS, CPU, GPU, RAM, AV
│   ├── InstalledSoftware.txt
│   ├── ProcessList.txt
│   └── Screenshot.png
├── SSH/
│   └── id_rsa, known_hosts
└── VPN/
    └── profiles.ovpn
```

Ce format standardisé permet aux acheteurs de parcourir et d'analyser rapidement les logs à l'aide d'outils automatisés. Des scripts spécialisés extraient automatiquement les credentials par service, identifient les logs contenant des accès d'entreprise, et évaluent la valeur financière de chaque log en fonction des données qu'il contient.

Les Initial Access Brokers (IAB) : le chaînon vers le ransomware

Les **Initial Access Brokers** représentent un maillon critique de la chaîne cybercriminelle. Ces acteurs spécialisés achètent massivement des logs d'infostealers et les analysent pour identifier les accès d'entreprise exploitables. Un IAB typique va filtrer les millions de logs disponibles pour trouver ceux qui contiennent des credentials VPN d'entreprise (Cisco AnyConnect, Pulse Secure, Fortinet), des cookies de session SSO (Okta, Azure AD), des accès RDP (Remote Desktop Protocol) à des serveurs exposés, ou des credentials pour des interfaces d'administration (Citrix, VMware vCenter, panneaux de gestion cloud).

Une fois un accès viable identifié, l'IAB le valide (s'assure que les credentials fonctionnent encore et que l'accès est exploitable), puis le met en vente sur des forums spécialisés (Exploit, XSS, RAMP) ou le propose directement à des groupes de ransomware via des canaux privés. Les prix des accès IAB varient considérablement selon la taille de l'entreprise cible et le type d'accès : de 500 USD pour un accès VPN à une PME, jusqu'à 50 000 USD ou plus pour un accès administrateur de domaine à une grande entreprise ou une infrastructure critique. Le retour sur investissement est spectaculaire pour les opérateurs de ransomware, qui peuvent transformer un accès acheté quelques milliers de dollars en une rançon de plusieurs millions.

Le **renforcement des tokens de session** vise à réduire l'exploitabilité des cookies volés. Les mesures incluent la liaison des tokens de session à l'empreinte TLS du client (token binding), la réduction de la durée de validité des sessions (8 heures maximum pour les accès sensibles), la ré-authentification obligatoire pour les actions critiques (changement de mot de passe, accès aux données sensibles, téléchargement en masse), la validation de l'adresse IP et du user-agent dans le contexte de session (en tenant compte du BYOD et de la mobilité), et l'implémentation de Device Trust (certificats client, conformité posture). Google a introduit en 2024 les **Device Bound Session Credentials (DBSC)**, qui lient les cookies de session au TPM (Trusted Platform Module) du dispositif, rendant les cookies inexploitables sur un autre appareil. Cette approche, si elle est généralisée, pourrait considérablement réduire l'impact du vol de cookies.

Monitoring des credentials compromis

La **surveillance proactive des fuites de credentials** permet de détecter rapidement si des identifiants d'entreprise apparaissent dans des logs d'infostealers. Les services spécialisés incluent **Hudson Rock**, qui surveille en temps réel les marchés de logs et les canaux Telegram pour détecter les credentials d'entreprise compromis. **Flare** et **KELA** offrent des plateformes de surveillance du dark web avec des alertes automatisées. **Have I Been Pwned** (HIBP) reste une ressource gratuite essentielle pour vérifier si des adresses email ont été compromises. **SpyCloud** propose une base de données exhaustive de credentials issus de stealers avec des API d'intégration pour les SIEM. L'intégration de ces services dans les workflows de réponse aux incidents permet de réagir rapidement en forçant la réinitialisation des mots de passe compromis, en révoquant les sessions actives, et en investiguant l'étendue de la compromission.

Protection DPAPI et surveillance réseau

La **protection DPAPI** peut être renforcée en utilisant Windows Credential Guard, qui isole les secrets DPAPI dans un hyperviseur sécurisé (VBS - Virtualization Based Security). Cette mesure empêche les infostealers d'accéder aux clés de déchiffrement DPAPI même s'ils s'exécutent avec des privilèges élevés sur le système d'exploitation.

Prévention de l'exfiltration

La **surveillance réseau** doit intégrer des règles de détection spécifiques à l'exfiltration des stealers. Les indicateurs réseau comprennent des connexions HTTP/HTTPS inhabituelles depuis des postes de travail vers des domaines récemment créés, des uploads importants peu après le téléchargement d'un exécutable, des communications avec des adresses IP connues de C2 d'infostealers (threat intelligence feeds), des résolutions DNS vers des domaines générés algorithmiquement (DGA), et des connexions à l'API Telegram depuis des processus non-Telegram (exfiltration via bot Telegram). Les solutions NDR (Network Detection and Response) comme Vectra, Darktrace ou ExtraHop peuvent identifier ces patterns comportementaux au niveau du trafic réseau.

Sensibilisation des utilisateurs

La **sensibilisation** reste un pilier incontournable. Les utilisateurs doivent comprendre les risques spécifiques liés aux infostealers : le danger des logiciels piratés et des "cracks" (premier vecteur de distribution), la nécessité de vérifier l'URL des sites de téléchargement (ne pas cliquer sur les annonces sponsorisées pour télécharger des logiciels), l'importance de ne pas sauvegarder les mots de passe dans les navigateurs, la vigilance face aux emails et messages contenant des liens suspects. Les programmes de sensibilisation doivent inclure des scénarios réalistes montrant comment un simple téléchargement peut mener à une compromission complète de l'entreprise. Les exercices de simulation de phishing doivent intégrer des scénarios de type malvertising et faux logiciels. Il est également crucial de créer une culture où les employés signalent rapidement toute activité suspecte ou téléchargement accidentel, sans crainte de sanctions, car la rapidité de la réponse est critique pour limiter l'impact.

Checklist prioritaire anti-infostealer

- **Désactiver** la sauvegarde de mots de passe dans les navigateurs (GPO)
- **Déployer** un gestionnaire de mots de passe entreprise (Bitwarden, 1Password)
- **Implémenter** des durées de session courtes et la ré-authentification contextuelle
- **Activer** Windows Credential Guard sur tous les postes
- **Surveiller** les accès aux fichiers de profils navigateurs via EDR
- **Souscrire** à un service de monitoring de credentials compromis
- **Bloquer** l'exécution d'archives ISO/VHD montées automatiquement
- **Former** les utilisateurs sur les risques des logiciels piratés et du malvertising
- **Segmenter** le réseau pour limiter le pivotement post-compromission
- **Imposer** le MFA résistant au phishing (FIDO2/Passkeys) sur les accès critiques

Pour approfondir ce sujet, consultez notre outil open-source burpsuite-automation qui facilite l'automatisation des tests d'intrusion web.

Questions frequentes

Comment mettre en place Infostealers dans un environnement de production ?

La mise en œuvre de Infostealers en production necessite une planification rigoureuse, incluant l'evaluation des prerequis techniques, la definition d'une architecture cible, des tests de validation approfondis et un plan de deploiement progressif avec des points de controle a chaque etape.

Pourquoi Infostealers est-il essentiel pour la securite des systemes d'information ?

Infostealers constitue un element fondamental de la securite des systemes d'information car il permet de reduire significativement la surface d'attaque, d'ameliorer la detection des menaces et de renforcer la posture globale de securite de l'organisation face aux cybermenaces actuelles.

Quelles sont les bonnes pratiques pour Infostealers en 2026 ?

Les bonnes pratiques pour Infostealers en 2026 incluent l'adoption d'une approche Zero Trust, l'automatisation des controles de securite, la mise en œuvre d'une veille continue sur les vulnerabilites et l'integration des recommandations des organismes de reference comme l'ANSSI et le NIST.

Sources et références : MITRE ATT&CK · OWASP Testing Guide

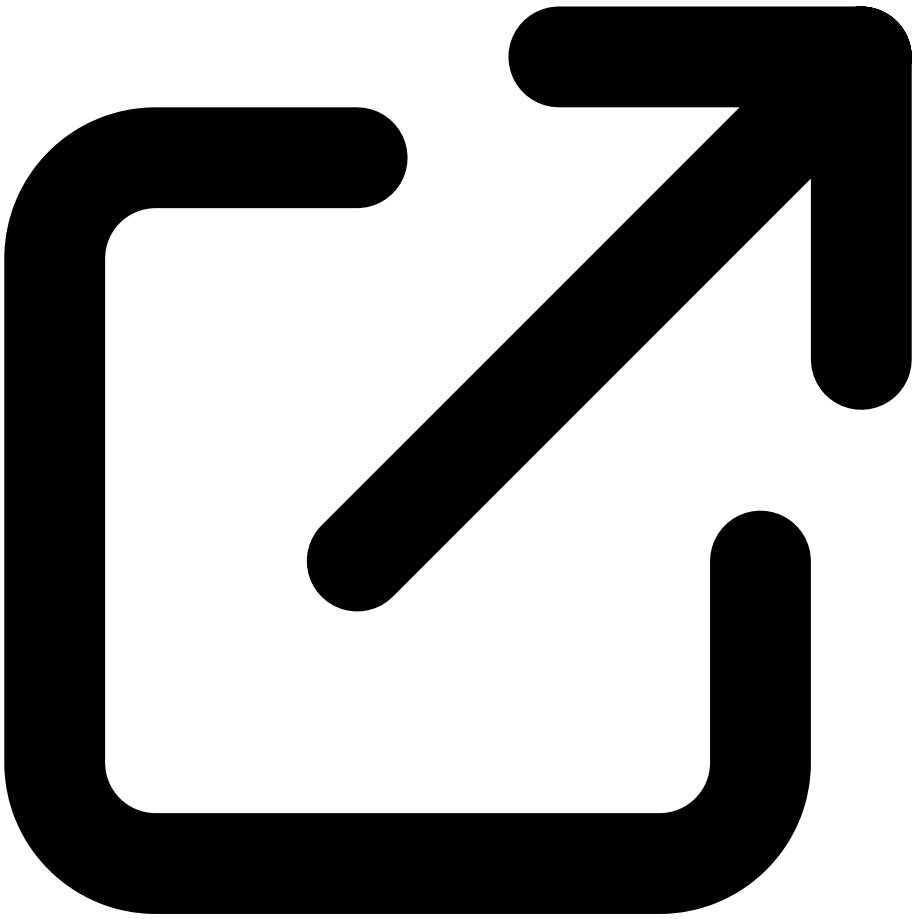
> Points clés à retenir
>
> - Prévention de l'exfiltration
> - Questions frequentes
> - Conclusion : une menace systémique qui exige une réponse globale

Conclusion : une menace systémique qui exige une réponse globale

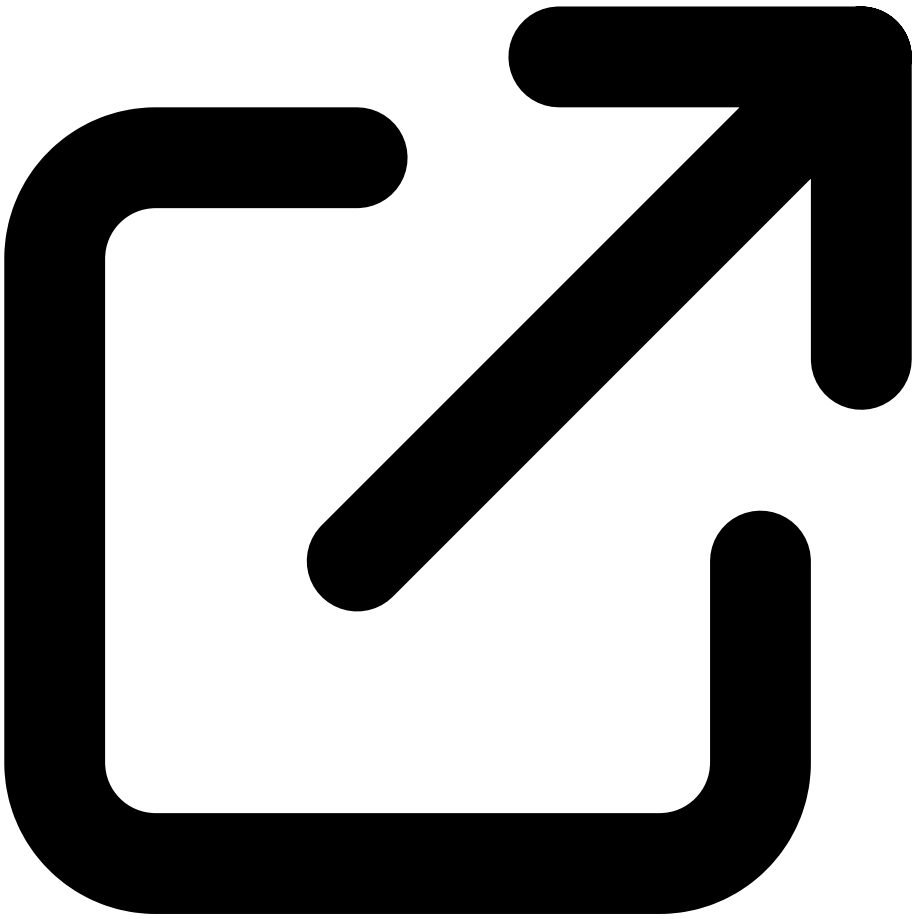
Les infostealers ont profondément transformé le paysage de la cybercriminalité en industrialisant le vol d'identifiants et en créant une chaîne d'approvisionnement fluide pour les opérateurs de ransomware. Leur modèle économique -- le MaaS -- a démocratisé l'accès à des outils de vol de données élaborés, permettant à un nombre croissant d'acteurs malveillants de participer à cet écosystème. La rapidité d'exécution des stealers (moins de 30 secondes), la diversité des données ciblées, et l'efficacité des marchés de revente rendent cette menace particulièrement insidieuse.

Face à cette menace systémique, les organisations doivent adopter une posture de sécurité qui intègre la réalité du marché des logs. Il ne suffit plus de protéger le périmètre ; il faut partir du principe que des credentials seront compromis et construire des défenses qui limitent l'impact de cette compromission. Le session token hardening, la surveillance proactive des fuites, la segmentation réseau rigoureuse, et la sensibilisation ciblée des utilisateurs constituent les piliers d'une défense efficace. Les technologies émergentes comme les Device Bound Session Credentials (DBSC) et les Passkeys FIDO2 offrent des perspectives encourageantes pour rendre les données volées par les stealers inexploitables, mais leur adoption généralisée prendra encore plusieurs années.

En définitive, la lutte contre les infostealers ne peut se gagner qu'en comprenant l'intégralité de la chaîne de valeur cybercriminelle : du développeur de malware au groupe de ransomware, en passant par les opérateurs, les marchés de logs et les courtiers d'accès. C'est cette compréhension globale qui permet de installer des contre-mesures pertinentes à chaque maillon de la chaîne, et de réduire significativement la surface d'attaque exposée aux conséquences critiques de cette menace silencieuse.



SEKOIA.IO - Threat Intelligence Blog
sekoia.io



Hudson Rock - Infostealer Intelligence
hudsonrock.com

Ayi NEDJIMI

Expert en Cybersécurité & Intelligence Artificielle

Consultant senior avec plus de 15 ans d'expérience en sécurité offensive, audit d'infrastructure et développement de solutions IA. Certifié OSCP, CISSP, ISO 27001 Lead Auditor et ISO 42001 Lead Implementer. Intervient sur des missions de pentest Active Directory, sécurité Cloud et conformité réglementaire pour des grands comptes et ETI.

LinkedIn Profil complet Tous ses articles

Références et ressources externes

- MITRE ATT&CK T1555 -- Credentials from Password Stores
- MITRE ATT&CK - RedLine Stealer -- Fiche technique RedLine
- CISA Cybersecurity Advisories -- Alertes et recommandations de la CISA
- CERT-FR (ANSSI) -- Centre de veille et d'alerte français
- Have I Been Pwned -- Vérification de compromission de comptes

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr