KPMG GLD & Associés Monaco

L'Écosystème des Infostealers ou le Rôle des Intermédiaires du Cybercrime

■ **ADVISORY** ■ CYBER

■ *Newsletter N°7*

Introduction : le paysage actuel du Cybercrime

Le cybercrime contemporain ne se résume plus à des attaques isolées ; il s'est transformé en une **chaîne d'approvisionnement industrialisée** et hautement spécialisée. Aujourd'hui, les attaquants ont intégré un paradigme fondamental : « le vol d'identifiants est plus facile que de forcer un pare-feu ».

Cette évolution a donné naissance à une économie souterraine où **l'infostealer est devenu le moteur principal de l'accès initial, alimentant une machine criminelle globale**.

Quelle différence entre Infostealers et Ransomwares ?

Bien que ces deux menaces collaborent souvent, les infostealers et les ransomwares poursuivent des objectifs fondamentalement différents et se distinguent par leur mode opératoire.

L'infostealer a pour objectif principal la **récolte furtive d'identifiants**, de secrets techniques ainsi que de jetons de session, tandis que le ransomware vise avant tout le **chiffrement des données** afin d'exiger une rançon dans une logique d'extorsion.

En termes de visibilité, l'infostealer se caractérise par un fonctionnement **silencieux**. Il opère en arrière plan afin de maximiser la durée de vie de l'accès compromis, sans alerter l'utilisateur ou l'organisation victime. À l'inverse, le ransomware agit de manière **immédiate et visible**, affichant une demande de rançon et provoquant une paralysie rapide des opérations.

La vitesse d'action constitue une autre différence majeure entre ces deux menaces. L'infostealer procède à une **exfiltration ultra rapide** des données, souvent quelques minutes seulement après l'infection initiale. Le ransomware, quant à lui, s'inscrit dans un **processus long**, comprenant des phases de mouvement latéral, d'exfiltration progressive, puis de chiffrement des systèmes ciblés.

Pour résumer de façon imagée : l'infostealer est le prédateur furtif, tandis que le ransomware est l'agresseur bruyant.

Rôle et tendance des Infostealers dans l'Écosystème Criminel

Ce type de menace est en croissance explosive : IBM X-Force, dans son rapport annuel sorti en 2025, a observé une augmentation de 84 % des emails délivrant des « infostealer » par rapport à l'année précédente.

Une fois les identifiants volés à l'aide des logiciels infostealers, ils sont triés par des **Initial Access Brokers** (courtiers d'accès). Ces intermédiaires filtrent ce qu'ils ont récolté pour identifier les accès à haute valeur (VPN, RDP, SSO) **et les revendent** sur des forums spécialisés tels que **Ramp, Breach, XSS** ou **Exploit**. Ces données volées sont des marchandises dont le prix dépend de l'usage criminel potentiel.

Comment s'en protéger ?

De façon générales, plusieurs sources techniques s'accordent pour **briser deux idées reçues :** i) ces codes malveillants sont capables de contourner l'authentification à 2 Facteurs (par exemple mot de passe + Code sur téléphone) et ii) les antivirus traditionnels peinent à détecter cette « nouvelle » menace.

En conséquence, une stratégie multi-niveau est nécessaire pour se protéger efficacement. Techniquement tout d'abord : il peut être intéressant **d'Interdire l'enregistrement des mots de passe dans le navigateur** et **d'imposer un gestionnaire de mots de passe d'entreprise**.

Des mesures organisationnelles peuvent aussi aider à se sécuriser, comme **l'interdiction stricte du BYOD**. Selon certaines sources, 70 % des infections proviendraient de ces terminaux. Notez que **faire appel à des professionnels de la sécurité informatique** pour sensibiliser les utilisateurs, aider à définir des mesures techniques pertinentes ou contrôler la bonne application de configurations de durcissement, patchs de sécurité, etc. permet de s'assurer du bon fonctionnement de son dispositif.

Conclusion : une réaction en chaîne

La détection d'un infostealer, ou un vol d'identifiant n'est pas un incident isolé, c'est le **premier maillon** d'une réaction en chaîne.

Ignorer une alerte de vol d'identifiant, c'est accepter par avance un futur ransomware ou une exfiltration massive de données. La vigilance est donc de mise pour assurer la sécurité de ses données, en appliquant toujours les basiques du moindre privilège, du besoin d'en connaître, et dans la bonne gestion des actifs informatiques (mises à jour, limitation de l'exposition des actifs, etc.) en matière de sécurité.

Sources :

- https://fr.newsroom.ibm.com/IBM-annonce-aujourdhui-les-resultats-de-ledition-2025-de-son-rapport-annuel-IBM-X-Force-Threat-Intelligence-Index-sur-le-paysage-mondial-des-menaces
- https://fr.flare.io/learn/resources/blog/redline-stealer-malware/
- https://ankura.com/insights/the-silent-epidemic-infostealers-and-the-evolution-of-cybercrime-in-2025
- https://www.eset.com/fr/about/newsroom/press-releases/recherche/operation-magnus-demantelement-redline-stealer/
- https://cyber.gouv.fr/nous-connaitre/publications/panoramas-de-la-cybermenace/panorama-de-la-cybermenace-2024/

Auteurs

Sabina DEBUSSY
Directeur Associé • Advisory • KPMG Monaco
sdebussy@kpmg.mc

Clément MAILLIOUX
Directeur • Advisory • KPMG Monaco
cmaillioux@kpmg.mc

Contactez-nous

Bettina RAGAZZONI
Associé
bragazzoni@kpmg.mc

Stéphane GARINO
Associé Principal
sgarino@kpmg.mc

Xavier CARPINELLI
Directeur Associé Expertise
xaviercarpinelli@kpmg.mc

Anne Marie FELDEN
Directeur Associé Audit
afelden@kpmg.mc

Cécile BOZANO-BODIN
Directeur Associé Advisory
cbozanobodin@kpmg.mc

Sabina DEBUSSY
Directeur Associé Advisory
sdebussy@kpmg.mc

Sylvie ROTI
Directeur Associé Expertise
sroti@kpmg.mc

Patrice DARMON
Directeur Associé Expertise
pdarmon@kpmg.mc

Mélanie LE MOIGN
Directeur Associé Audit
mlemoign@kpmg.mc

Alain CHARPENTIER
Directeur Associé Audit
acharpentier@kpmg.mc

KPMG GLD & Associés Monaco

2, rue de la Lüjerneta • "Athos Palace" • 98000, Monaco

mc-news@kpmg.mc
www.KPMG.mc
@KPMG_Monaco
+377 977 777 00
@kpmg-monaco
@KPMGMonaco