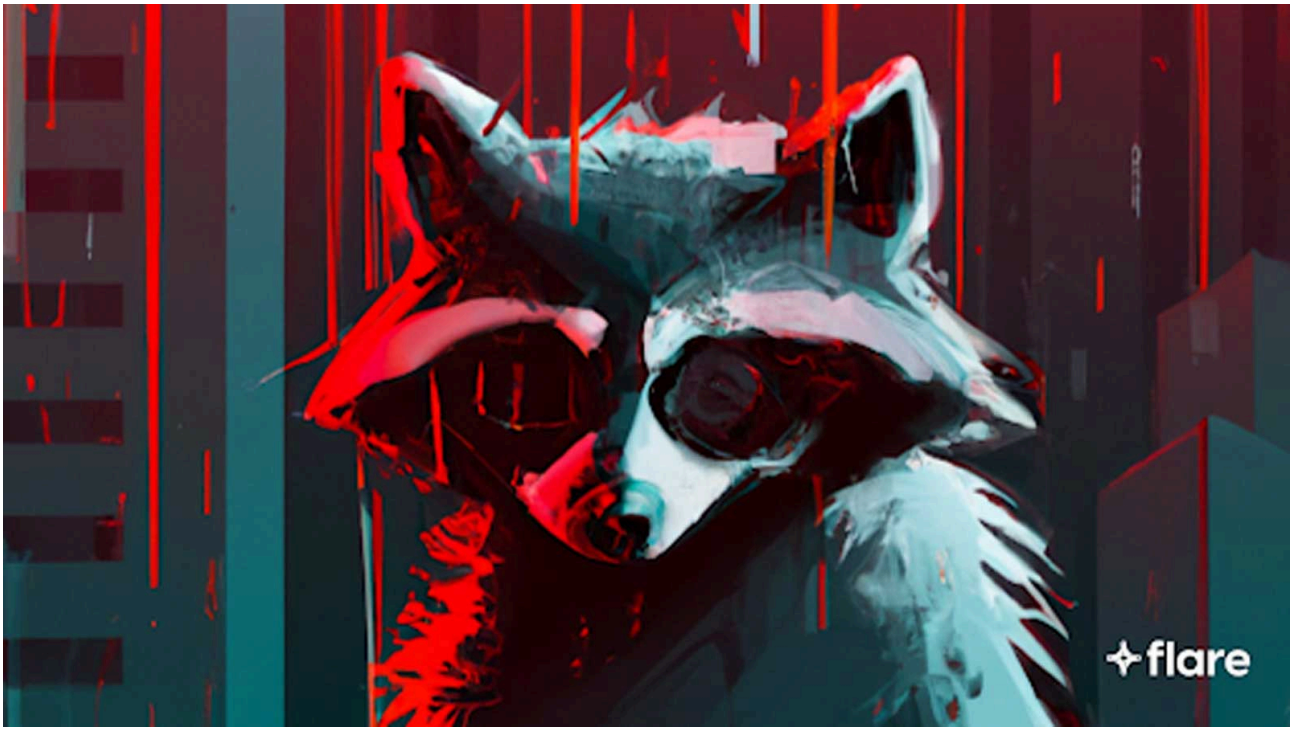
Dissecting the Dark Web Supply Chain: Stealer Logs in Context

By Flare

Published: 2023-06-06 · Archived: 2026-04-05 14:40:13 UTC



Stealer logs represent one of the primary threat vectors for modern companies. However, many security teams are still focused on leaked credentials and remain unaware of the significant threat posed by devices infected with infostealer malware.

This Flare explainer article will delve into the lifecycle of stealer malware and provide tips for detection and remediation.

What is a Stealer Log? Several variants of infostealer malware exist, but the primary groups we often encounter are Redline, Raccoon, Vidar, and Titan. This malware infects victim computers and exports passwords saved within the browser, alongside host data such as OS version, IP address, clipboard data, browser history, saved credit cards, and cryptocurrency wallet data.

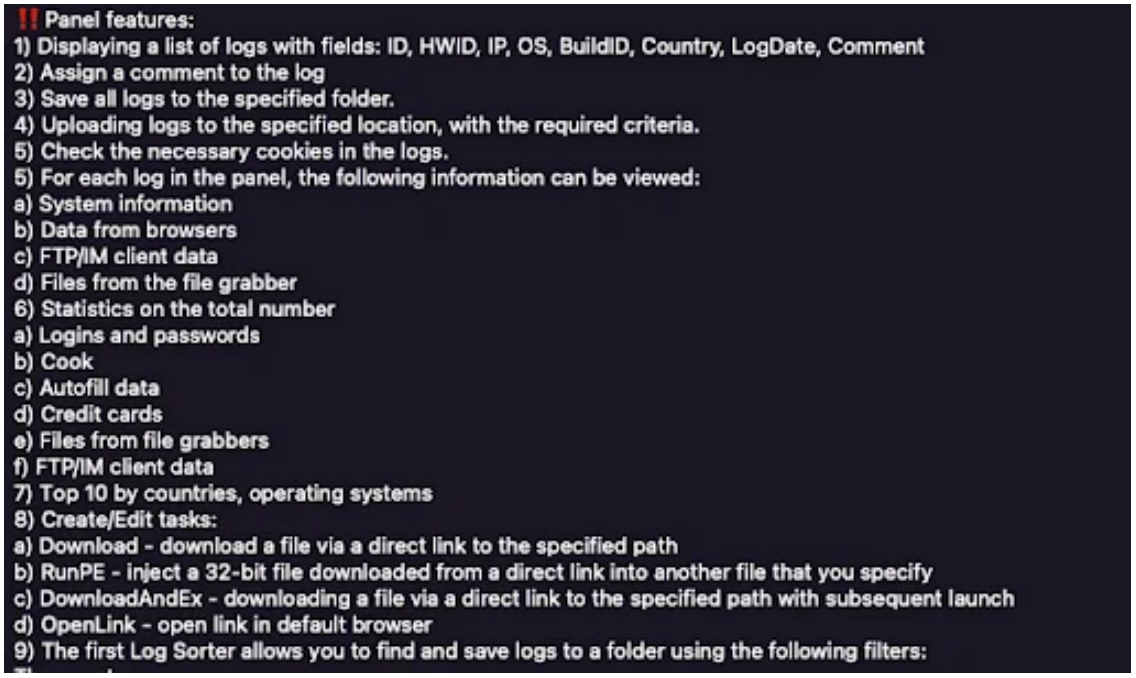
The malware then sends this data back to the threat actor's command-and-control infrastructure. It is subsequently sold as individual listings on dedicated dark web marketplaces or distributed through specialized cybercrime Telegram channels.

The Stealer Malware Lifecycle - Malware as a Service Vendors

The cybercrime ecosystem's growth has seen an increasing tendency towards the commoditization of malware, and infostealer malware is no exception.

Malware as a service vendors sell access to the primary infostealer variants on specialized Telegram channels for a fixed monthly price, typically ranging from $100 to $300, depending on the malware's age; and with lifetime subscriptions available.

Buyers also gain access to a web portal linked to command-and-control infrastructure, which can be used to collect logs from victims in a centralized location.



Description of stealer web panel features
Source: Flare

The Stealer Malware Lifecycle - Distribution

Threat actors who purchase stealer logs have the responsibility of distributing the malware to victims. This distribution typically occurs through three principal vectors: cracked software downloads, illegitimate ads, and spear-phishing emails for targeted attacks against organizations.

Once the infostealer malware is downloaded onto a victim's computer, it automatically executes and attempts to establish communication with the C2 infrastructure. Upon successful communication, credentials and host data are sent back to the threat actor.

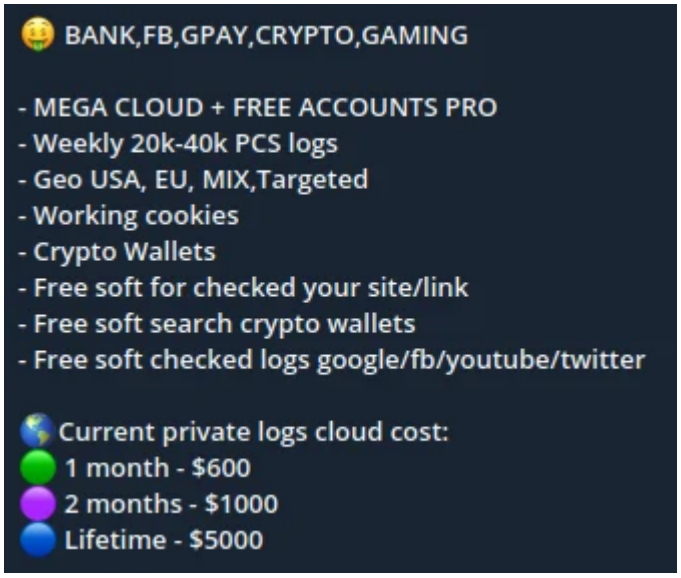
The Stealer Malware Lifecycle - Reselling

The Vast majority stealer logs originate from home computers without access to corporate IT environments. In many instances, threat actors utilize stealer logs to access VPN environments, streaming services, and other basic consumer applications. However, logs that do provide access to corporate IT environments are highly prized.

At Flare we process more than 1 million stealer logs per week, and estimate that a minimum of 1% contain access to corporate IT environments. Stealer logs are typically distributed through one of four major channels:

Russian Market Genesis Marketplace Public Telegram Rooms Private "VIP" Telegram Rooms

Using Flare's SaaS cyber-intel platform, we found logs sold on the Russian and Genesis marketplaces come with a basic list of saved credentials that were saved in the browser. Full information about the victim's machine and the passwords are provided upon purchase.



Threat actor promoting private info-stealer logs
Source: Flare

These marketplaces are designed for threat actors who are "shopping" for specific credentials and credentials often vary in price dramatically based on the type of information being sold. For example the average price of an infected device listed on Genesis market is $14.39 however with a healthcare domain listed the price jumps to $93.91 and access to banking services brings the price north of $110 per device.

Private Log Channel Ad on Telegram

Logs distributed through Telegram are wholly different, they typically appear in large zip files containing hundreds or thousands of individual logs. They are often distributed in public Telegram rooms, but a significant number are also shared in private VIP "paid access" Telegram channels.

These typically cost between $300-$900 per month and are limited to 10-15 users. This provides exclusivity to the threat actors in the channel, allowing them to pick over and exploit the most valuable logs before they are likely given away on a public Telegram room later.

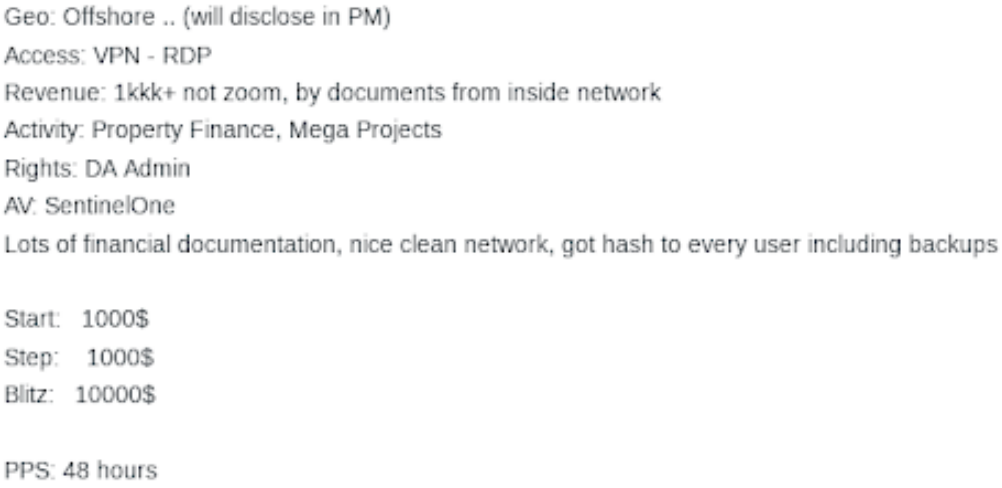
Redline Stealer logs shared on Telegram
Source: Flare

Logs being given away for free in a public Telegram channel.

The Stealer Malware Lifecycle - Initial Access Brokers

We believe that many initial access brokers, who are active on dark web forums such as exploit.in and xss.is, sift through millions of stealer logs found in VIP Telegram channels and on the Russian and Genesis markets.

Their aim is to identify logs containing corporate access, which can then be used to establish and expand corporate access. Buying logs that already have multiple sets of corporate credentials significantly simplifies the process of compromising a company.



Selling logs with corporate credentials
Source: Flare

It allows the threat actor to focus on validating and expanding initial access rather than initially establishing it. Once access has been validated, initial access brokers (IAB's) auction off the established access for prices ranging from thousands to tens of thousands of dollars, depending on the victim organization and level of access established.

A post from Exploit.in selling access to a corporate environment. Note that the threat actor lists notable information about the company affected in addition to the AV the victim is using. The bidding starts at $1,000 with increments of an additional $1,000 and a "buy it now" price of $10,000.

Detect & Remediate Stealer Logs with Flare

Flare's SaaS platform delivers high-value, tailored threat exposure management to organizations. Flare detects threats across hundreds of dark web markets & forums, thousands of illicit Telegram channels & clear web sources of risk.

Our SaaS platform integrates into your existing security program in 30-minutes with native integrations that enable you to build a threat led cybersecurity program. Request a product demo today to learn more.

Sponsored and written by Flare.

Source: https://www.bleepingcomputer.com/news/security/dissecting-the-dark-web-supply-chain-stealer-logs-in-context/