REDLINESTEALER Malware Driving the Initial Access Broker Market

By Laurie Iacono, Keith Wojcieszek, George Glass

Published: 2024-08-14 · Archived: 2026-04-05 15:06:23 UTC

Kroll frequently sees threat actors, particularly ransomware gangs, leveraging valid accounts to gain a foothold in corporate networks. Many of these gangs rely on information stealing malware as a means to obtain such credentials. REDLINESTEALER is one of the most common varieties of infostealer that Kroll currently encounters. Infostealer logs are a significant factor in the initial access broker market. Threat actors sell access they have gained to corporate environments, to ransomware operators who then complete the attack chain and extort the victim.

Infostealers are most commonly deployed via phishing, malvertising and fake or misleading posts on social media. Threat actors aim to infect as many individuals as possible to collect their credentials. This presents an unseen risk to corporate environments as employees' personal machines can become infected. These might contain credentials that provide access to corporate credentials or present a threat through reuse, enabling threat actors to test them against edge services such as VPN, email platforms or application gateways.

Characteristics of REDLINESTEALER

First seen in around 2020, REDLINESTEALER is available on underground forums as a monthly subscription service. This gives attackers access to the REDLINESTEALER panel and the ability to pack the malware and collect the logs of stolen information. Its main functionality is to steal data such as passwords, credit card information, usernames, locations, cookies and hardware configuration from infected systems.

REDLINESTEALER collects this data from a number of sources, including:

- Installed browsers, such as SQLite databases
- VPN credentials
- Crypto wallets (such as files containing *.wallet)
- Chat messages
- FileZilla credentials

REDLINESTEALER can gather detailed information about victims’ systems, such as IP address, city and country, operating system, administrator privileges and information about infected PC hardware and graphic cards, as well as identifying any installed antivirus software on the system.

If REDLINESTEALER is found to have been executed on a device, it is safe to consider that any credentials stored locally on that device have been compromised. REDLINESTEALER can also download files, making it likely that further payloads could be deployed to a victim device, should a threat actor require more functionality depending on their objectives, such as high bandwidth data exfiltration or ransomware.

Cybercriminals deliver REDLINESTEALER in a number of ways. They have been found posting sponsored adverts on hijacked Facebook business and community pages. These offer free downloads of AI chatbots such as ChatGPT and Google Bard but lead users to download REDLINESTEALER. In November 2023, a new version of the ScrubCrypt obfuscation tool was identified as being available for sale on dark web marketplaces and used to launch account takeover and fraud attacks with REDLINESTEALER.

In Q4 2023, Kroll investigated a surge in cases in which users downloaded a file associated with REDLINESTEALER. In these instances, the lure was a PDF converter software, on the URL “pdfconvertercompare[.]com. It is likely that users accessing the page were searching for a legitimate copy of a tool or searching innocuous phrases such as 'printable calendars' or 'business models' and being presented with the malicious URL at the top of their search results. Once on the site, it contained a description of the alleged tool above a download button. The subsequently downloaded file was "PdfConverters.exe", which Kroll identified as REDLINE. The file had a low anti-virus detection rate at eight vendors detecting out of 69. Within Kroll cases, interaction with the file caused it to be quarantined at the point where the process "WmiPrvSE.exe" interacted with the file to either execute or delete the file.

Kroll has previously reported on similar tactics used by other infostealers such as VIDAR, leveraging Google Ads to masquerade as a legitimate site to download popular software.
