RedLine Stealer Resurfaces in Fresh RIG Exploit Kit Campaign

bitdefender.com/blog/labs/redline-stealer-resurfaces-in-fresh-rig-exploit-kit-campaign/

Mihai NEAGU
April 27, 2022

At the start of the year, Bitdefender noticed a RIG Exploit Kit campaign using CVE-2021-26411 exploits found in Internet Explorer to deliver RedLine Stealer, a low-cost password stealer sold on underground forums.

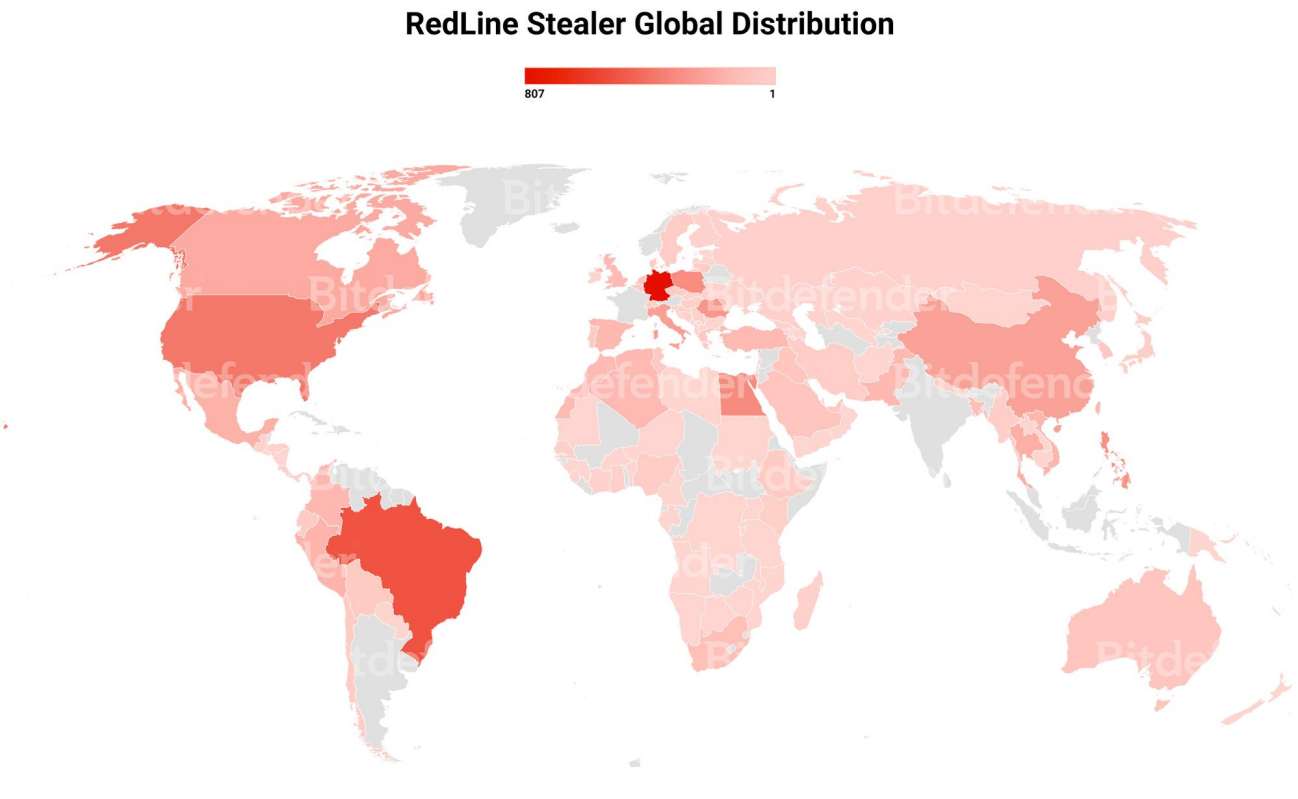
When executed, RedLine Stealer performs recon against the target system (including username, hardware, browsers installed, anti-virus software) and then exfiltrates data (including passwords, saved credit cards, crypto wallets, VPN logins) to a remote command and control server.

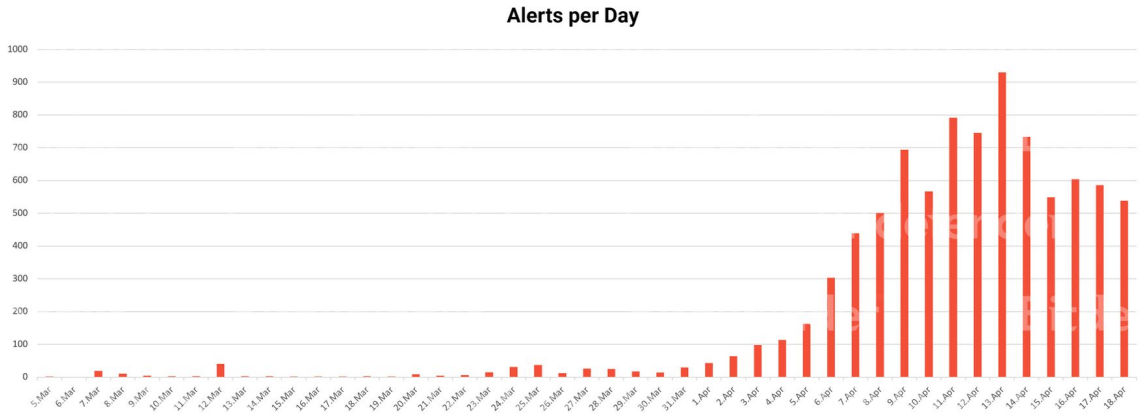
Download the RedLine Stealer whitepaper

Key Findings

- Bitdefender discovered a new RIG Exploit Kit campaign targeting an Internet Explorer vulnerability designed to distribute RedLine Stealer malware.
- If executed, the stealer exfiltrates passwords, cookies and credit card data saved in browsers, as well as crypto wallets, chat logs, VPN login credentials and text from files as per the instructions received from the C2 infrastructure.

Country distribution and daily activity





Mitigation

- Ensure anti-virus and EDR solutions have exploit detection capabilities.
- Look for the indicators of compromise (IOCs) and keep operating systems and third-party applications up to date, and prioritize security fixes.

Download the RedLine Stealer whitepaper

TAGS

whitepapers anti-malware research

AUTHOR

ion
or

Bookmarks