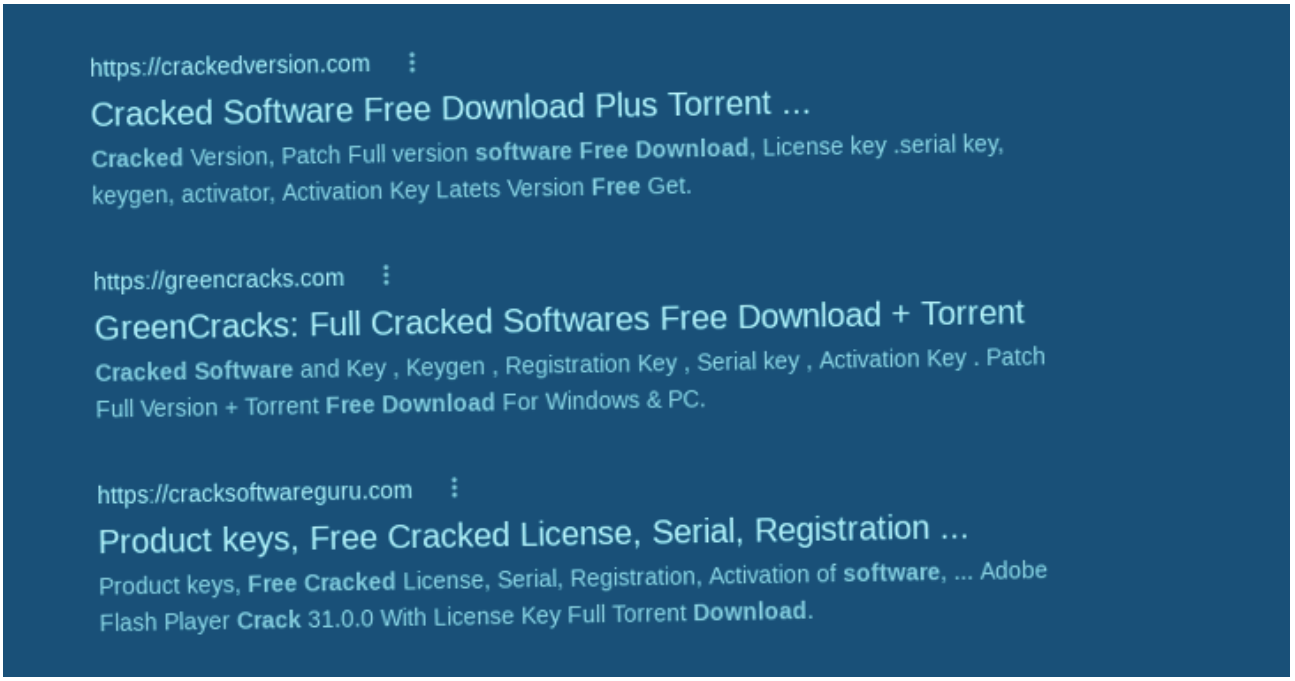
Raccoon and Vidar Stealers Spreading via Massive Network of Fake Cracked Software

By The Hacker News

Published: 2023-01-16 · Archived: 2026-04-05 21:31:55 UTC



A "large and resilient infrastructure" comprising over 250 domains is being used to distribute information-stealing malware such as Raccoon and Vidar since early 2020.

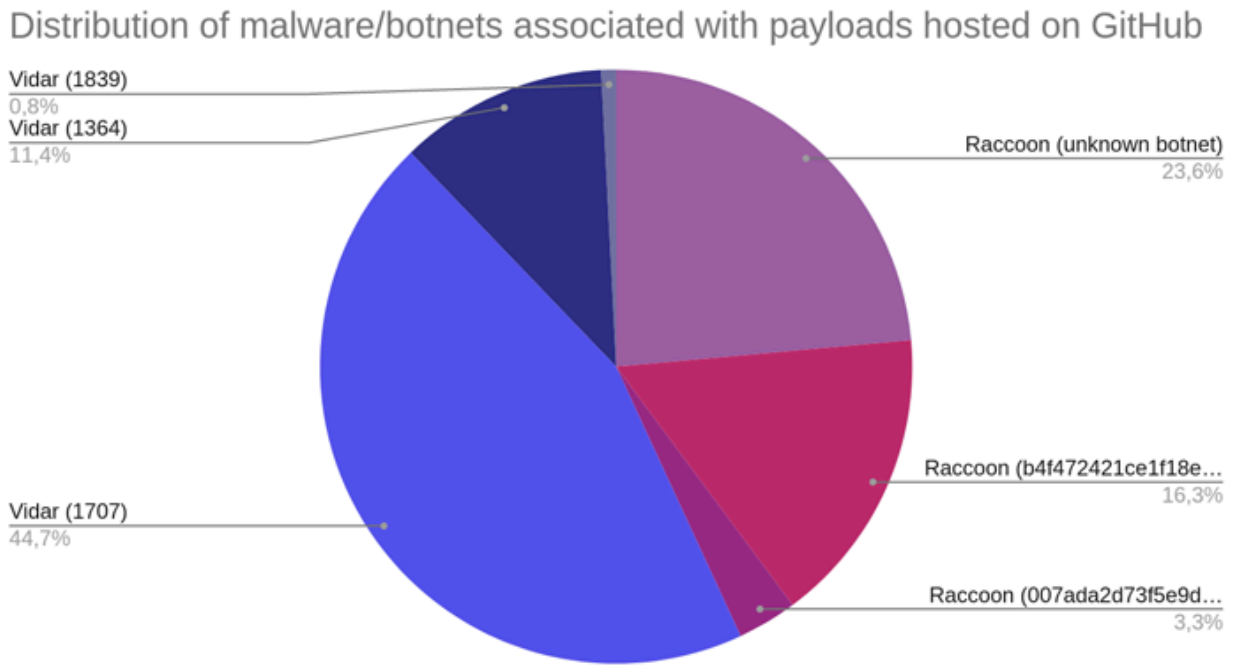
The infection chain "uses about a hundred of fake cracked software catalogue websites that redirect to several links before downloading the payload hosted on file share platforms, such as GitHub," cybersecurity firm SEKOIA said in an analysis published earlier this month.

The French cybersecurity company assessed the domains to be operated by a threat actor running a traffic direction system (TDS), which allows other cybercriminals to rent the service to distribute their malware.

The attacks target users searching for cracked versions of software and games on search engines like Google, surfacing fraudulent websites on top by leveraging a technique called search engine optimization (SEO) poisoning to lure victims into downloading and executing the malicious payloads.

The poisoned result comes with a download link to the promised software that, upon clicking, triggers a five-stage URL redirection sequence to take the user to a web page displaying a shortened link, which points to a password-protected RAR archive file hosted on GitHub, along with its password.

"Using several redirections complicates automated analysis by security solutions," the researchers said. "Carving the infrastructure as such is almost certainly designed to ensure resilience, making it easier and quicker to update or change a step."



Should the victim uncompress the RAR archive and run the purported setup executable contained within it, either of the two malware families, Raccoon or Vidar, are installed on the system.

The development comes as Cyble detailed a rogue Google Ads campaign that employs widely-used software such as AnyDesk, Bluestacks, Notepad++, and Zoom as lures to deliver a feature-rich stealer known as Rhadamanthys Stealer.

An alternate variant of the attack chain has been observed taking advantage of phishing emails masquerading as bank statements to dupe unwitting users into clicking on booby-trapped links.

Fabricated websites impersonating the popular remote desktop solution have also been put to use in the past to propagate a Python-based information stealer dubbed Mitsu Stealer.

Both pieces of malware are equipped to siphon a wide range of personal information from compromised machines, harvest credentials from web browsers, and steal data from various cryptocurrency wallets.

Users are advised to refrain from downloading pirated software and enforce multi-factor authentication wherever possible to harden accounts.

"It is crucial for users to exercise caution when receiving spam emails or to visit phishing websites and to verify the source before downloading any applications," the researchers said.

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.
