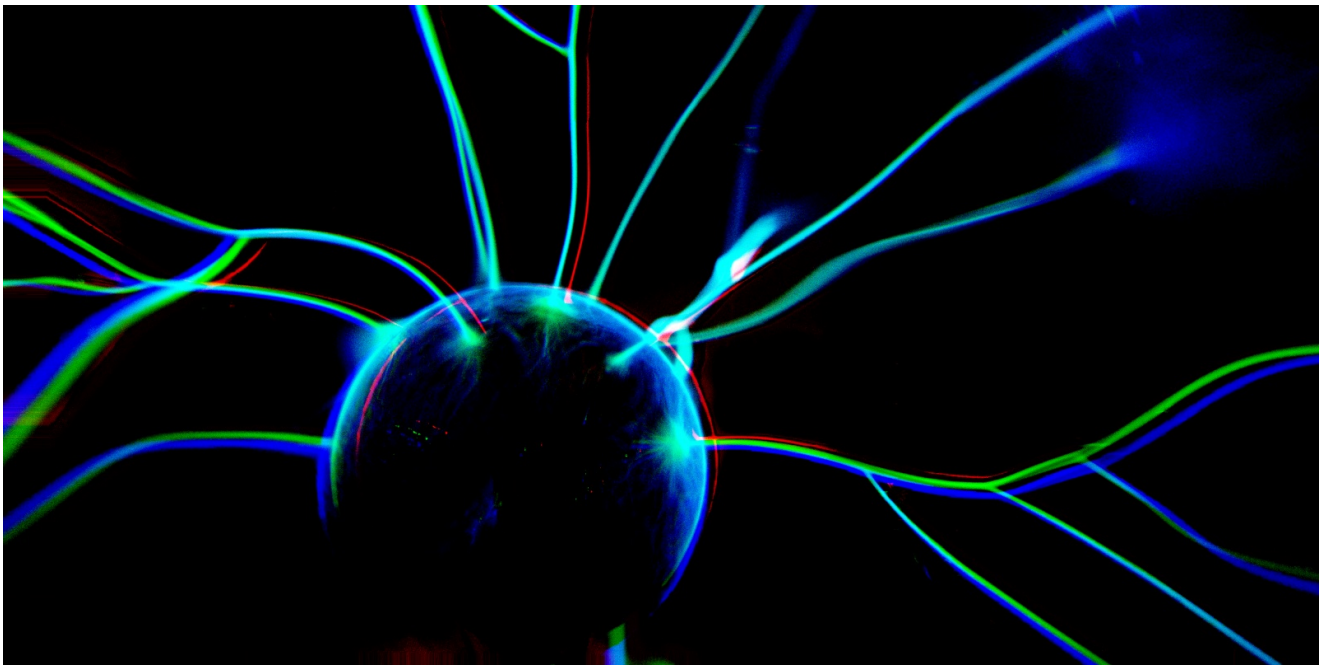
New Golang botnet empties Windows users' cryptocurrency wallets

bleepingcomputer.com/news/security/new-golang-botnet-empties-windows-users-cryptocurrency-wallets/

Sergiu Gatlan

By
Sergiu Gatlan

- February 18, 2022
- 03:27 PM
- 0



A new Golang-based botnet under active development has been ensnaring hundreds of Windows devices each time its operators deploy a new command and control (C2) server.

First spotted in October 2021 by ZeroFox researchers who dubbed it **Kraken**, this previously unknown botnet uses the SmokeLoader backdoor and malware downloader to spread to new Windows systems.

After infecting a new Windows device, the botnet adds a new Registry key to achieve persistence between system restarts. It will also add a Microsoft Defender exclusion to ensure that its installation directory is never scanned and hides its binary in Window Explorer using the hidden attribute.

Kraken has a limited and simplistic feature set, allowing attackers to download and execute additional malicious payloads on compromised devices, including the RedLine Stealer malware.

RedLine is currently the most widely deployed information stealer capable of harvesting victims' passwords, browser cookies, credit card info, and cryptocurrency wallet info.

"Monitoring commands sent to Kraken victims from October 2021 through December 2021 revealed that the operator had focused entirely on pushing information stealers – specifically RedLine Stealer," ZeroFox said.

"It is currently unknown what the operator intends to do with the stolen credentials that have been collected or what the end goal is for creating this new botnet."

Built-in crypto wallet theft capabilities

However, the botnet also features built-in information theft capabilities and can also steal crypto wallets before dropping other info stealers and cryptocurrency miners.

According to ZeroFox, Kraken can steal info from Zcash, Armory, Bytecoin, Electrum, Ethereum, Exodus, Guarda, Atomic, and Jaxx Liberty crypto wallets.

Based on info collected from the Ethermine cryptocurrency mining pool, this botnet seems to be adding roughly USD 3,000 every month to its masters' wallets.

"While in development, Kraken C2s seem to disappear often. ZeroFox has observed dwindling activity for a server on multiple occasions, only for another to appear a short time later using either a new port or a completely new IP," the researchers added.

Nevertheless, "by using SmokeLoader to spread, Kraken quickly gains hundreds of new bots each time the operator changes the C2."

Related Articles:

New cryptomining malware builds an army of Windows, Linux bots

Microsoft: Sysrv botnet targets Windows, Linux servers with new exploits

Qbot malware switches to new Windows Installer infection vector

New ERMAC 2.0 Android malware steals accounts, wallets from 467 apps

Microsoft detects massive surge in Linux XorDDoS malware activity