Published on *The National Law Review* https://natlawreview.com

Privacy Tip #436 – Microsoft Warns of Crypto Wallet Scanning Malware StilachiRAT

Article By:

Linn F. Freedman

A Microsoft blog post reported that incident response researchers uncovered a remote access trojan in November 2024 (dubbed StilachiRAT) that “demonstrates sophisticated techniques to evade detection, persist in the target environment, and exfiltrate sensitive data.”

According to Microsoft, the StilachiRAT threat actors use different methods to steal information from the victim, including credentials stored in the browser, scans for digital wallet information, system information, and data stored on the clipboard.

Once inside the victim’s system, StilachiRAT scans the configuration data of 20 cryptocurrency wallet extensions for the Google Chrome browser, extracting and decrypting saved credentials from Google Chrome. The 20 cryptocurrency wallet extensions targeted are listed in the blog article. The article also lists recommended mitigations.

One takeaway from the article is to not store critical credentials in Chrome, a common and simple security measure. If a threat actor gains access to these credentials, multiple applications could be at risk. You may wish to consider which passwords you are saving in Chrome and refrain from saving the credentials for any banking or cryptocurrency platforms, as well as for access to your employer’s system. These are credentials worth memorizing.

Copyright © 2025 Robinson & Cole LLP. All rights reserved.

National Law Review, Volume XV, Number 79

Source URL:https://natlawreview.com/article/privacy-tip-436-microsoft-warns-crypto-wallet-scanning-malware-stilachirat