Mphasis
The Next Applied

The RedLine Stealer Malware

Date: 21st April 2024 | Severity: High

Summary

RedLine is a stealer malware that aims primarily at banking credentials and collects information such as saved credentials, autofill data, and credit card details, as well as usernames, location data, hardware configuration, and information about installed security software. RedLine may also steal cryptocurrency.

Attack Vectors

Attackers initially delivered the RedLine malware in an email campaign, attackers to collect credentials from web browsers, cryptocurrency wallets, and applications, including:

- Chromium browsers
- Gecko-based browser, like Mozilla Firefox
- FTP clients.
- Instant messaging applications
- VPN applications

Indicator of compromise

INDICATOR TYPE	INDICATORS
Domain	• ofth546ebr.cfd • adsharedwi897th.cfd • crackplaced.com • psestwotothr.cfd • anydesk-vip.com • istanmove.cfd
URLs	• https[:]//github.com/microsoft/STL/files/14432565/Cheater.Pro.1.6.0.zip • https[:]//31.210.21.158:43975 • https[:]//privatlab.com/s/s/3Qa0YRMaVaij07Z8BqzZ/7ca69d4c-c5bb-4ab3-b5a9-87c17b7167b5-86yYgEGqbQMnoszgm0OmgGb6g • http[:]//ivcgroup.in/temp/Citrix-x64.msix

File Hash	• ff77b3faead625a06b88799a3c68d56f60a4bece30c70c37cdfd5591b283976e • 8556ced6ff3186ddbcb3f4612ff96a6f088871907810f243bc370907cf86bce2 • aef765b0a188ccf547e620748caa34f33f455efc0ebc13d3e3e948a87c635c75 • a74bd4fb84febbb2021f611ffdd6c74f
IP	• 185.215.113.121 • 213.248.43.58 • 77.91.103.31 • 45.150.67.175 • 146.70.124.71 • 193.43.146.26 • 94.131.111.240

Recommendation

- Detect and report phishing attacks, including a reminder not to click on any suspicious links or documents
- Store passwords securely, such as in an encrypted password manager rather than their browser
- Implement and use MFA
- Download apps only from trusted sources, like the App Store or Google Play
- Install anti-virus software on all devices

Reference Links

- https://flare.io/learn/resources/blog/redline-stealer-malware/
- https://thehackernews.com/2024/04/new-redline-stealer-variant-disguised.html