Rilide: A New Malicious Browser Extension for Stealing Cryptocurrencies

Date: 13th January 2024 | Severity: Medium

Summary

The Rilide information-stealing malware was first reported by cybersecurity researchers in April 2023. The infostealer targets the users of Chromium-based web browsers, such as Google Chrome, Brave, Opera, and Microsoft Edge.

Attack Vectors

- Once executed, Rilide disables the Content Security Policy (CSP) feature, designed to prevent cross-site scripting (XSS) attacks, and runs a script to attach a listener that monitors the user's activity, such as switching tabs and visiting a website. In case the visited domain matches a predefined list of targets, designated scripts are injected into the webpage to steal user information (for example, credentials and cryptocurrency data).
- In August 2023, cybersecurity researchers reported an updated Rilide version that overrides the Chrome Extension Manifest V3 to install malicious extensions on Chromium browsers. The novel malware version employed additional features, such as the ability to exfiltrate data to a Telegram channel and to take screenshots every time interval according to predefined URL rules.
- The malware was observed being distributed as P2E (Play To Earn) games that were promoted on Twitter and as a fake Palo Alto GlobalProtect plugin. One of the newly-observed campaigns specifically targeted the banking credentials of users in the United Kingdom and Australia. In these campaigns, the malware also used a PowerShell loader to modify the browser's Secure Preferences file so the browser would always be launched with the malicious extension.
- In April 2024, cybersecurity researchers reported a phishing campaign that leveraged malicious Facebook pages to trick victims, primarily based in Europe, into downloading fake desktop versions of popular AI software (for example, Midjourney, Sora AI, DALL-E 3, Evoto, and ChatGPT). These fake installers led to the deployment of infostealers, such as a new variant of Rilide (V4). The novel malware version, masqueraded as a Google Translate extension, was enhanced to target Facebook cookies and also employed improved obfuscation techniques to evade detection.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• 32a097b510ae830626209206c815bbbed1c36c0d2df7a9d8252909c604a9c1f1 • a7c07d2c8893c30d766f383be0dd78bc6a5fd578efaea4afc3229cd0610ab0cf • e394f4192c2a3e01e6c1165ed1a483603b411fd12d417bfb0dc72bd6e18e9e9d • 027268c51892ca07c36b66ae31dbe33c2afeb789 • d504505d18408343a5f1225a0d0f3c1b • f2348f98a71afcc241c6e3d5777b300e5602a4e5 • 92751fd15f4d0b495e2b83d14461d22d6b74beaf51d73d9ae2b86e2232894d7b • e89971bfb8375d748cc233157537856c5598fcd513ed42e862261a99843f40d0 • f5dc1259e5300b8d4711ca7bf51c6e9f
URLs	• https[:]//download.hdoki[.]org/yzxdhdxsqkmvcayrtevs/RiotRevelry1[.]0.2[.]exe • https[:]//nch-software[.]info/1/2.exe
Domains	• proyectopatentadomxapostol[.]com • ashgrrwt[.]click • pupkalazalupka[.]com • extensionsupdate[.]com • nightpredators[.]com • assets[.]bnbcoinstatic[.]com • extension-login[.]com • nvidia-graphics[.]top • blackfox[.]lol • tes123123t[.]com • nch-software[.]info • web-lox[.]com
IP Address	• 45.15.156[.]210

Recommendation

- Enable 2FA: Always use two-factor authentication where possible.
- Update Software: Ensure your software, including browsers, is up to date.
- Exercise Caution: Be wary of suspicious extensions and files.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https[:]//www.bleepingcomputer.com/news/security/hackers-use-rilide-browser-extension-to-bypass-2fa-steal-crypto/
- https[:]//www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/rilide-a-new-malicious-browser-extension-for-stealing-cryptocurrencies/