

Severity

Medium

Analysis Summary

Mars is an information stealer that was first spotted in 2021 and advertised as a standalone version on several cybercriminal sites. It primarily targets Windows victim credentials and cryptocurrency wallets, including 2FA plugins and any other vital system information. This malware can steal information from a variety of browsers (passwords, cookies, credit cards, and so on). It can also extract browsing and file download histories, Internet cookies, and stored passwords from various browsers including Google Chrome, Chromium, and Mozilla Firefox. It steals credentials from crypto plugins and crypto-wallets.

Its code is similar to those of other information stealers such as Arkei, Oski, and Vidar. Mars stealer malware has the potential to infect multiple systems, pose serious privacy concerns, and inflict large financial losses. Passwords, banking information, and identity theft are some of the main impacts of this malware.

Impact

- Credential Theft
- Unauthorized Access

Indicators of Compromise

MD5

- 958accf13bff096146cf7403ababde87
- 14ae29a5ef95b4ce69971f452a16babe
- 6d333f6879aad330d10e6fa243bd9538

SHA-256

- 2737688ed48eec68e5d3f69515fb9ec2573dfd3a134b769e04df087ebbae827e
- 72188aa23469a7b97a95534c37c926794636aa90675bce7fce04d7402326b2bf
- 7248563d27d6963821e6e2536510681ada58cad62969cfa1f7d835ba1694ad20

SHA-1

- 4b357f88eacf4687813e40bfaa0ca4f6e1a27e5a
- d376ce5f95874b80b01f9a4436d1689560f94b52
- 3c65b90e1fd975ec17110a7e10067ae044232c36

Remediation

- Block the threat indicators at their respective controls.
- Search for IOCs in your environment.