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

- b23a4794f36589ad6ccdc7283013c8ae
- 5fea51478a01f10a78d428751e973aba

SHA-256

- 309122794db2c8fd2ffd82c9770988297860a56116ce184be08da75b64d361f8
- 0f63b4b4659449eee766610af817b786e9cd7622743851cf7b71430613d7521b

SHA-1

- ad73edc33406d2a5d080a5adfa967927c9c3f9df
- cb7f1e3acc3636a6f890edb8c44d0abe2674ec1c

URL

- http[:]//62[.]204[.]41[.]69/p8jG9WvgbE[.]php

Remediation

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