Severity

Medium

Analysis Summary

Redline is an info stealer malware that steals information from web browsers and has the ability to corrupt operating systems by installing harmful software.

It steals user information from browsers, instant messaging applications, and file transfer protocol clients. According to the Proofpoint analysis, the malware first appeared in March 2020. Redline expanded throughout several nations during the COVID-19 epidemic and is still active today. Passwords, credit card information, cookies, usernames, locations, autofill data, and even hardware configuration such as keyboard layout, UAC settings can be stolen by RedLine. RedLine is also capable of stealing cryptocurrency. This malware is a live campaign that is aimed at a variety of Asian organizations.

Impact

- Data Exfiltration
- Credential Theft
- Information Theft
- Financial Loss

Indicators of Compromise

MD5

- 3bf923f6caabfbb7ff460413b814e40b

SHA-256

- 70af158d463ddd5fb50e5b74b9b4711846b18985a5afb9a684359fc29a077b11

SHA-1

- 56036068fe2f4c6af3f250c760adcfd9f33df571

Remediation

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