Severity

High

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

- 86ba481bf9a90d4d2bfa52a3136e08b0

SHA-256

- 2fb2913adb95d8bac8dd7af97b5bc4e740d7ae866b0b1ee024705cbc49c6e588

SHA-1

- 1f42f592e271a378ae74950dd9404e237b1c4de0

Remediation

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