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

- 8da17a030beb96b93f58e938afe5be7a

SHA-256

- 2948e0568dd511b296781352a128f748c1969e47d9c684d798c9294f0feae3d1

SHA-1

- 353d7c63820d4e8205f508b248e2b59e987a1d2b

Remediation

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