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

- 2b7ff665165866036cbf842e8c2efb8f

SHA-256

- 0e703d45075ec9b49302d7555df1a873c5a708a4a3461af65166616aba72d4a4

SHA-1

- 662371d36b4152a327cd13673e846340bf65d4e4

Remediation

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