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

- 1a2d6f0ad70ea9aa913a668fff2255fb
- dc979e040f4d9aa2ded05f4f71973495
- eafd2f1a2af41de6ad0a9ef4db0b2b99
- 0e9db60ad1bf774e9cee7b52cc145b4e
- bc9964b04c2c38eb8fab28aae525071e
- bb76d8e38cef6a561efe8a09a65d45d2
- 841ffed489bd0256296c0b9059405b10

SHA-256

- 3ee9814c18b0d55b57844adc047e61f7c94283904788e03d1a02e2941bd01058
- 6bfa63da8cff003557071b7077726c15b5da21ff8001fbffb208b198ade14654
- d2fa024a4dc4c0f41baf5e6caf426315c05eb2cd8db6061472a4c1e6421da194
- af573246f95b5eab9ae520005e00fd4e3f35e3488b2681e1a196d3e24eeb8c02
- deceeec4d99e6b4b70de57d6ee732b1f70e6cbb9ea27d0bb7304fd51b1ca0b2d
- 08994ca3543a247a9cde09070f355673d46bb13134349d0c34b008f0391634ed
- a767e7176c4418bfa362d2cc38c6668ddc1f4cb9c37a0f793e351415ef410f20

SHA-1

- c1e58c5de0bd41118300de219dffcb77a51df531
- bb9007431d60557066f31f7a9ada52e766ac0a2b
- 9ddc822030a475988361ca72e3acc7d080b675c3
- 322187dd46fc28a2727faac47b1efea50505a89a
- 62599cf43426898880b02997370780db75a157bf
- 2f1e437d1d863d1208edfa50f2e5156d8802717f
- e3011ddc3563328e6caa8def6efa22a3fcde48e5

Remediation

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