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

- 9e7ac86863937758e29d82e03d09b84f
- 5fc658881ab1a3b2bb18c3b23b6d1549
- d750a3a9b6206f8d9a5c928b629b2785
- ed64f06e1980a703b470450a284cbbc6

SHA-256

- 9cb4a7dd8876f5db191c7e99fc434b948b4f86cb78b445faba0d032801c832c0
- 2a736fb2cb9df92ac3030cb5c122ba7636d4deed93ba10cc32769e469bfd0db5
- 4834b94e7534aecde98d41efcae093a81c0597006bd3a0e0cda8ffc4593bd210
- 296f6f3725ca757cddbb4237d6563d780c69e57298a3e1dc04d741bf5ff201af

SHA-1

- 9cb4a7dd8876f5db191c7e99fc434b948b4f86cb78b445faba0d032801c832c0
- 2a736fb2cb9df92ac3030cb5c122ba7636d4deed93ba10cc32769e469bfd0db5
- 4834b94e7534aecde98d41efcae093a81c0597006bd3a0e0cda8ffc4593bd210
- 296f6f3725ca757cddbb4237d6563d780c69e57298a3e1dc04d741bf5ff201af

URL

- http[:]//www[.]sdrclm[.]cn/vendor/phpdocumentor/P800/P90GT_Invoice_Related_Property_Tax_P800[.]exe

Remediation

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