Severity

High

Analysis Summary

Racoon gathers private data such as credit card numbers, cryptocurrency wallet addresses, login passwords, and browser information like cookies and history. It was discovered in the wild for the first time in April 2019. This malware is a C++ program that allows you to steal data from common browsers and cryptocurrency wallets. Exploit kits are used to deploy the virus, which employs browser-based vulnerabilities to lead users to landing sites containing exploit codes. It’s also propagated through phishing efforts that persuade victims to run the malicious payload or macros. This info stealer collects related to the machine, such as the OS arch and version, hardware information, and installed apps.

Impact

- Data exfiltration
- Credential theft
- Financial loss

Indicators of Compromise

MD5

- 800f1fbfda6fa368cd469f5bdff644b0

SHA-256

- 5da3db74eee74412c1290393a0a0487c63b2c022e57aebcd632f0c3caf23d8bc

SHA-1

- fa1db6808d4b4d58de6f7798a807dd4bea5b9bf7

Remediation

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