Severity

High

Analysis Summary

Vidar, which first appeared in late 2018, is a malware family that primarily acts as an information stealer and is frequently seen as a prelude to ransomware distribution. This malware takes data and distributes it as spam email, cracked commercial software, and keygen programs.

Vidar can scrape a wide range of digital wallets in addition to credit card data and passwords. Various campaigns can be used to propagate this malware. It allows data such as system information, browser data, and passwords to be captured and exfiltrated from a system. Vidar has also been seen as a secondary payload in ransomware attacks like STOP/DJVU.

Impact

- Data Exfiltration
- Information Theft
- Exposure of Sensitive Data

Indicators of Compromise

MD5

- 27a8a630c04ebf28745d4ae773a7ddac

SHA-256

- 3da2b7b3db8644140e7f0f832ce30ada1009b24b8b29883b05df978d5d64d23f

SHA-1

- 627c6af2bbc95a0d1a31161e9f66dbd92d20dace

Remediation

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