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

- b2cde2b7f52a07cab9eafb342c356ca0

SHA-256

- 24c19a1636d3587279d55be4fe5ff2921f8caf3698d6214fe4110bc3ca76fc16

SHA-1

- 0ea31f1aa973672a08c52949efa3e52c7b874727

Remediation

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