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.

Researchers discovered newly registered domains created by a threat actor to spoof Microsoft's official Windows 11 OS download portal in April 2022. The fake sites were set up to spread malicious ISO files that infect endpoints with the Vidar infostealer. These Vidar malware variants fetch their C2 configuration via attacker-controlled Telegram and Mastodon social media channels.

Impact

- Data Exfiltration
- Information Theft
- Exposure of Sensitive Data

Indicators of Compromise

Domain Name

- ms-win11[.]com
- ms-win11[.]midlandscancer[.]com
- win11-serv4[.]com
- win11-serv[.]com
- win11install[.]com
- ms-teams-app[.]net

IP

- 195[.]201[.]250[.]209
- 107[.]189[.]11[.]124
- 5[.]252[.]178[.]50
- 107[.]189[.]11[.]124

MD5

- 52c47fdda399b011b163812c46ea94a6
- da82d43043c101f25633c258f527c9d5
- e9a3562f3851dd2dba27f90b5b2d15c0
- 6ae17cb76cdf097d4dc4fcccfb5abd8a

SHA-256

- cfd4b9db2d6b999ee3de514a5418575a0c6e89a2e6e1a3f29b908022b8c87c5a
- 8a2a200ae56ff80f9d861d72f9ad8f5d3d57bf8ae600e5b376a6e2bb89996dfd
- e600b8ef36477ed37d924b1ba8deaadeab3275392ba0accd6329a11542adbaad
- b7981244c7c3d79872799387efa6656ba1dd82055d6ae59c2f788690fca357b0

SHA-1

- 446742810f5e31c61e8d0346c59ae36b083d6960
- 75c80701c253990fd6bd60a76c96315be9c30b6a
- 98be930c6674cc31c9cf7efb656f7fadb320a273
- 93ff6dadfeb9711ae0e1abfaaaf2310283648048

URL

- https[:]//t[.]me/btc20220425
- https[:]//ieji[.]de/@ronxik213
- https[:]//koyu[.]space/@ronxik123
- https[:]//t[.]me/mm20220428

Remediation

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