Vidar Stealer an Info Stealing Malwre

Date: 05th June 2024 | Severity: High

Summary

Vidar Stealer, a potent malware written in C++, capable of stealing a wide range of data from the compromised system. Vidar Stealer targets user's personal data, web-browser data, cryptocurrency wallets, financial data, sensitive files within user directories, communication applications, process explorer data, network communications, and more. This customizable malware is being sold on the dark web and underground forums as a malware-as-a-service and leveraging the social media platforms as their part of C2 infrastructure to get details such as IP address, instructions, updates, and downloads. Understanding the operation and impact of Vidar Stealer is crucial for cybersecurity professionals to develop effective defense strategies against such sophisticated threats.

Attack Vectors

- Vidar is an information-stealing malware that targets a wide range of data.
- It is being sold as a malware-as-a-service on the dark web and underground forums.
- It comes with customizable functionality.
- The malware hides the core malicious code in an obfuscated form and decodes after analyzing the environment for debugger/analysis tools.
- Injects the malicious code into the legitimate Windows process.
- Use social media platforms to get C2 details.
- Downloads additional binaries from C2 to support its operation.
- Checks for the use of self-signed certificates to detect the potential network interception between malware and C2.
- Collects a wide range of data from the compromised system including personal and financial data, application data, system activity, and more.
- Harvests all the targeted data into the Program Data folder under a randomly generated file name.
- Exfiltrates all the collected data to the C2 server and subsequently deletes them from the Program Data folder to eliminate potential traces of data exfiltration.
- The analyzed sample exhibits no signs of a persistence mechanism.
- The threat actor appears to be of Russian origin based on the language used to promote and sell the malware across the dark web and Telegram channel.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• 7e74918f0790056546b862fa3e114c2a • fed19121e9d547d9762e7aa6dd53e0756c414bd0a0650e38d6b0c01b000ad2fc • 90e744829865d57082a7f452edc90de5 • 036a57102385d7f0d7b2deacf932c1c372ae30d924365b7a88f8a26657dd7550 • 3c67ddeb2426bfd91144dd8ca4ec06ee20578105514ad629c830e194bfd65893 • 0bbdda44330f983208041c1422e52759e87de6c4438b152d6dc36e17f07f9765 • 3bae8ea58db5926584007d715d1f47fc60cc8e219b564ef5dddc5c7dbc70f9be
URL	• https[:]//steamcommunity[.]com/profiles/76561199686524322 • https[:]//t[.]me/k0mono • https[:]//65.108.55.55[:]9000 • https[:]//91.107.221.88[:]9000
IP	• 65[.]108[.]55[.]55 • 91[.]107[.]221[.]88

Recommendation

- Submit the File Hash to the Antivirus team to update their database with the file hashes.
- Submit the Domains to the Network team to update their database with the Domains.
- Secure RDP ports to prevent threat actors from abusing and leveraging RDP tools.
- Prioritize remediating known exploited vulnerabilities.
- Implement EDR solutions to disrupt threat actor memory allocation techniques.
- Make regular backups of important and critical files.
- Avoid browsing the unsafe websites, clicking on suspicious links, or opening unknown email attachments.
- Update and Patch operating system, applications, and security software's up to date with latest patches.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Link

- https://www.cyfirma.com/research/vidar-stealer-an-in-depth-analysis-of-an-information-stealing-malware/