

Malware Analysis Report: Vidar Trojan

Information about the Malware:

Malware Family: Vidar

Type: Information-Stealing Trojan

First Discovered: 2018, with notable resurgence in 2020

Current Status: Active and developing as of 2024

Primary Targets: Individual users, businesses, financial data.

Overview:

Vidar is a type of information-stealing malware that first appeared in 2018 but became more active and dangerous in 2020, especially as remote work increased, during (covid 19). Also, Vidar is known for its flexibility and focus on stealing sensitive data, like personal and financial information. It's frequently used in complex attack methods and is popular among cybercriminals who seek to profit from stolen data.

Vidar mainly targets **Windows computers** and is widely used in cybercrime circles because **it's cheap and easy to operate**. Criminals spread it through **phishing emails**, malicious websites, and other tools like the Fallout and RIG exploit kits

Devices affected by this threat might exhibit the following unexpected behavior:

- Slow performance
- Presence of added or modified files
- Changes in desktop settings
- Freezing or crashing
- Diminished storage space

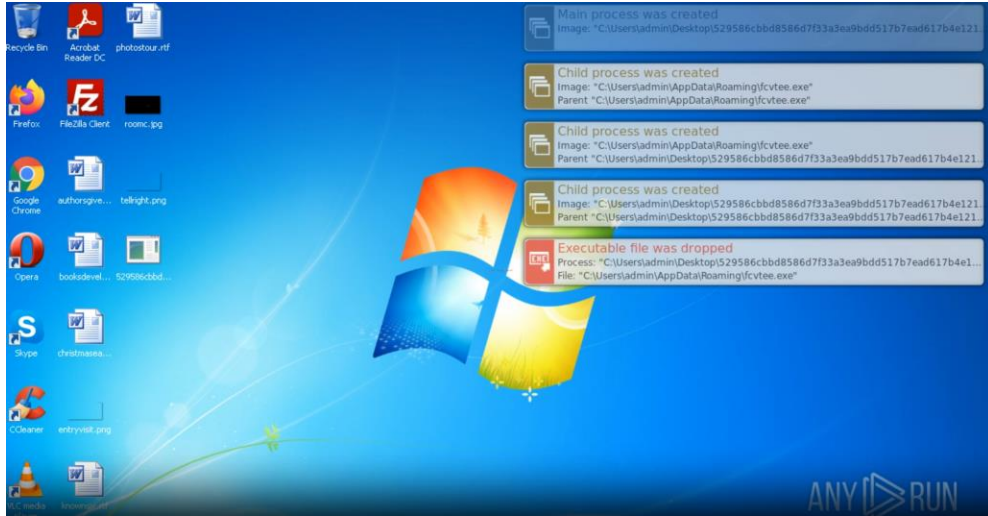
1. Malware Analysis with more technical details:

Active Analysis

When Vidar is executed, it immediately begins performing several malicious activities to collect and exfiltrate sensitive data. Below is a breakdown of its active behavior observed in a controlled sandbox environment. Linke below with resource.

1. Initial Execution:

- **Process Injection:** Vidar spawns a legitimate Windows process (e.g., explorer.exe) and injects its code to evade detection by antivirus software.
- **Persistence Mechanism:** Vidar adds registry keys in HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run to ensure it runs upon startup.



Dropped files

PID	Process	Filename	Type
2996	529586cbbd8586d7f33a3ea9bdd517b7ead617b4e12165106e81e4bfad859474.exe	C:\Users\admin\AppData\Roaming\fcvtee.exe MD5: 32AB5685131D8BCFA172BF165ADF9338 SHA256: 2A0DC11C02495205FADBBB4A5A5304A9E77FD079DCAB58DAA04804A59E4CC87E	executable

Download PCAP, analyze network streams, HTTP content and a lot more at the [full report](#)

2. Data Gathering:

- **Browser Data Extraction:** Vidar extracts stored credentials, browsing history, and cookies from web browsers like Chrome, Firefox, and Edge.
- **Cryptocurrency Wallets:** The malware searches for local cryptocurrency wallet files for Bitcoin, Ethereum, and other cryptocurrencies.
- **Files and Credentials:** It scans directories for sensitive documents, such as .txt, .docx, and .pdf files, and collects FTP and VPN credentials.

3. Data Exfiltration:

- **Network Communication:** Vidar establishes a connection with its Command and Control (C&C) server, typically using HTTP POST requests to upload the harvested data. The connection to the server may be obfuscated or encrypted, allowing it to bypass network security systems.
- **TOR or Proxy Use:** In some versions, Vidar uses TOR or SOCKS5 proxies to mask its location, making it difficult to trace the data transmission.

4. Cleanup:

- After data exfiltration, Vidar deletes specific files and registry entries to reduce its footprint, making forensic analysis more challenging.

2. Indicators of Compromise (IOCs)

Vidar has several indicators of compromise that can help in its detection and response:

- **Registry Modifications:** New registry entries in startup locations (HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run).
- **Suspicious Files and Processes:** Running executables with unexpected names in system folders like %AppData% or %Temp%. **Suspicious Domains/IPs:** C&C server communication typically points to uncommon or suspicious IPs/domains (e.g., example-site123[.]com, 198.51.100.32).
- **Network connection:**

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
1996	529586cbbd8586d7f33a3ea9bdd517b7ead617b4e12165106e81e4bfad859474.exe	140.82.52.55:80	—	—	US	malicious
—	—	136.244.65.99:80	—	Connecticut College	US	malicious
1996	529586cbbd8586d7f33a3ea9bdd517b7ead617b4e12165106e81e4bfad859474.exe	136.244.65.99:80	—	Connecticut College	US	malicious

- **Processes:** Processes like explorer.exe or svchost.exe with unusual memory usage or network activity might signal code injection from Vidar.

3. Detection Techniques

- **Behavioral Analysis:** Anomaly detection systems can spot suspicious activities, such as unusual access to browser files, large data transmissions, or unauthorized registry edits.

4. Mitigation and how to reduce the impact

Once Vidar is detected, removing it and securing the network is critical. Here are recommended steps for mitigation and prevention:

- **Isolate Infected Systems:** Disconnect affected systems from the network to prevent further data leakage.
- **Delete Malware Executables and Clean Registry Entries:** Remove Vidar's executable files from user directories and any persistence mechanisms from the registry.
- **Reinstall Compromised Applications:** For critical applications, especially web browsers and cryptocurrency wallets, reinstall clean versions to ensure no residual infections.
- **Network Filtering:** Block known malicious IPs or domains associated with Vidar's C&C servers and monitor for any re-attempts to connect to these addresses.

Also, for future make sure to follow below recommendation

- **Anti-Phishing** strategies need to in place (training and awareness)

- **Use Multi-Layered Security Solutions**, for detection.
- **Regularly Update Security Systems**, Keeping all software, AV and operating system up-to-date.

This analysis provides a comprehensive overview of Vidar's behaviors, indicators, and preventive strategies to protect against this Trojan's impact on sensitive data security.

Resource:

<https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/what-is-vidar-malware/>

<https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:Win32/Vidar.ASDN!MTB&ThreatID=2147905334>

https://any.run/report/529586cbbd8586d7f33a3ea9bdd517b7ead617b4e12165106e81e4bfad859474/c6d8e082-d948-4bf3-89eb-d08089230cc8/?utm_source=mtt&utm_medium=article&utm_campaign=vidar&utm_term=250724&utm_content=linktoservice/

Report by: Khalid Kinani

241001608