SvcStealer Malware Targeting Users to Extract Sensitive Data from Browsers and Applications - Active IOCs - Rewterz

Published: 2025-03-24 · Archived: 2026-04-05 13:30:52 UTC

Severity

High

Analysis Summary

SvcStealer 2025 is a newly identified information stealer that primarily spreads through spear phishing email attachments. First observed in January 2025, this malware is designed to harvest extensive sensitive data, including machine details, installed software, user credentials, cryptocurrency wallets, and browser information. It systematically extracts this data before compressing and transmitting it to its command-and-control (C2) servers. Additionally, the malware has the capability to download further malicious payloads, increasing its overall impact beyond initial data theft.

Identified by Researchers, SvcStealer is written in Microsoft Visual C++ and employs various evasion techniques to bypass security tools. It terminates monitoring processes and deletes traces of its activity to avoid detection. Upon infecting a system, the malware generates a unique 11-byte alphanumeric identifier derived from the victim's volume serial and communicates with its C2 infrastructure using the IP address **176.113.115.149** over port 80. The stolen data is sent through HTTP POST requests with a **multipart/form-data** content type, disguising it as normal web traffic to avoid raising suspicion.

In terms of persistence, SvcStealer continuously beacons to its C2 server, awaiting further instructions from threat actors. These commands may include downloading additional malware families, expanding the attack's scope. By maintaining constant communication with the C2 infrastructure, the malware remains an active threat even after initial data exfiltration.

Security experts strongly advise users to remain cautious of suspicious email attachments, as phishing remains the primary infection vector. Implementing advanced endpoint protection, network monitoring, and behavioral analysis can help detect and prevent infections. Organizations must enhance their security awareness and deploy proactive defenses to mitigate the risks posed by this evolving threat.

Impact

- Sensitive Data Theft
- Crypto Theft
- Gain Access
- Security Bypass

Indicators of Compromise

IP

- 185.81.68.156
- 176.113.115.149

MD5

- 0535262fe0f5413494a58aca9ce939b2
- ee0fd4d6a722a848f31c55beaf0d0385
- 05ef958a79150795d43e84277c455f5d
- 4868a5a4c8e0ab56fa3be8469dd4bc75

SHA-256

- 0e545c02f20c83526f7f7f424f527e3faa103017cfe046c1f3b7e4ccd842829b
- 9f77bbcdd38b75f6ec62bc84ff8adcf7be6c9c184a61941af75a2b8f93091fb8
- 4254de273cf58a956855203549ce4c6ffa2e0eba107d4a11e884f4ea064821d5
- b1e889002d9174c58dd9d8b20758516a3ff6e636ff14e00793da3ff9a09a7e9e

SHA-1

- c680c17065c5dbc6ee633f81e02c5d91b2539edc
- a377b72cc04fcb676d5e9671337fd950b5e5d3a9
- 4ac97823e2107ed5cee77f63f197d2897d910dff
- 881efd7b368cd566dff7210fa2278f1627817002

Remediation

- Block all threat indicators at your respective controls.
- Search for indicators of compromise (IOCs) in your environment utilizing your respective security controls.
- Avoid opening email attachments or links from unknown or suspicious sources. Deploy advanced email filtering solutions to detect and block phishing attempts.
- Use next-generation antivirus (NGAV) and endpoint detection and response (EDR) solutions to detect and block malicious activities in real time.

- Implement network traffic analysis to identify unusual HTTP POST requests or suspicious communication with known malicious IPs, such as **176.113.115.149**.
- **Process and Behavior Monitoring:** Continuously monitor running processes for suspicious activities, such as unauthorized process termination or attempts to delete system logs.
- Ensure operating systems, security tools, and installed software are up to date with the latest security patches to prevent exploitation.
- Apply the principle of least privilege (PoLP) to limit user permissions, reducing the impact of potential infections.
- Use dynamic malware analysis tools to analyze and block suspicious files before execution in the network.
- Establish a well-defined incident response strategy to quickly contain and mitigate infections if a system is compromised.
- Regularly back up critical data and store it securely offline to ensure recovery in case of data theft or ransomware deployment.
- Educate employees about phishing techniques and social engineering tactics to minimize the risk of falling victim to email-based attacks.
