blackpoint

THREAT PROFILE:

Vidar Stealer

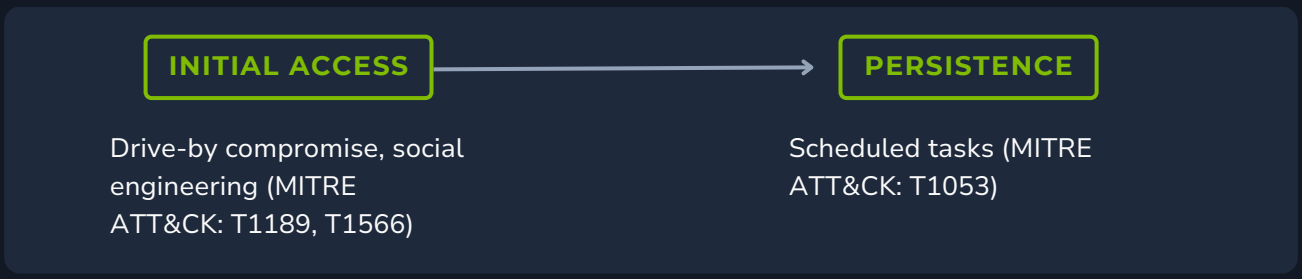
Table of Contents

Executive Summary

First Identified:
2018

Malware Type:
- Information Stealer

Known Associates:
- Arkei Malware
- BatLoader
- RisePro Malware
- Scattered Spider
- Bebra Malware
- Cyclops/Knight Ransomware
- Hive Ransomware
- Laplas Clipper
- LockBit Ransomware
- SmokeLoader
- STOP/Djvu Ransomware
- XMRig Miner



Description

Vidar Stealer is a malware that has been active since November 2018 and is used to steal personal information from compromised machines. The malware is sold as a Malware-as-a-Service (MaaS) from the developer's website. The price ranges from $130 to $750 depending on the model. The malware is often advertised on hacking forums and Telegram groups.

Vidar Stealer is often deployed via social engineering attacks – phishing emails with malicious attachments and links – and drive-by downloads. Vidar Stealer has also been observed using malicious Google ads to spread the malware variant. Vidar Stealer has been observed impersonating legitimate software such as Advanced IP Scanner, Adobe Photoshop, Microsoft Teams, and Adobe Illustrator.

Vidar Stealer has been previously assessed to be a variant of the Arkei malware family; however, an interview with purported Vidar Stealer staff indicated that that source code was purchased from the Arkei developer but is a completely separate operation.

The name Vidar is likely in relation to the god Vidar. Vidar is the god of vengeance, silence, and resilience. Vidar is the son of Odin, the chief of the Aesir gods, and the giantess Gríðr. Additionally, text on the Vidar developer's site supports this with the "Hail to the Silent One! Hail to Leathershod! Hail to the Wolf Ripper! Hail to the Far-Seer!" text visible on the home page.

Vidar Stealer sells for $130 to $750 depending on the model.

Vidar Stealer is written in C++ programming language. Vidar Stealer samples have been observed including a row of null bytes at the beginning of the file in order to bloat its size up to nearly 700MB. The size limits of anti-malware software, which results in the file often being skipped. Researchers have reported that this method has only been observed when the malware is delivered via an archive – either via search result malvertising campaign or emails with archive attachments.

Vidar Stealer uses social media as its C2, including Telegram, Mastadon, Steam, Twitter, and TikTok. The first contact with the C2 includes only a bot ID. The server then returns with a configuration package that contains guidance upon behavior, and the DLL the malware needs to run. The body of the C2 response contains a specification that points at the features to be used; a sequence of 0 and 1 corresponds to the "modules" that will be used. Security researchers with GridinSoft identified the following module functionalities:

- Grabbing AutoFill data, cookies and credit card information.
- Collecting history of web views and downloads
- Stealing cryptocurrency wallet addresses
- Hijacking messages history from Telegram
- Taking a screenshot
- Stealing specific files

Previous Targets: Vidar Stealer

Previous Industry Targets

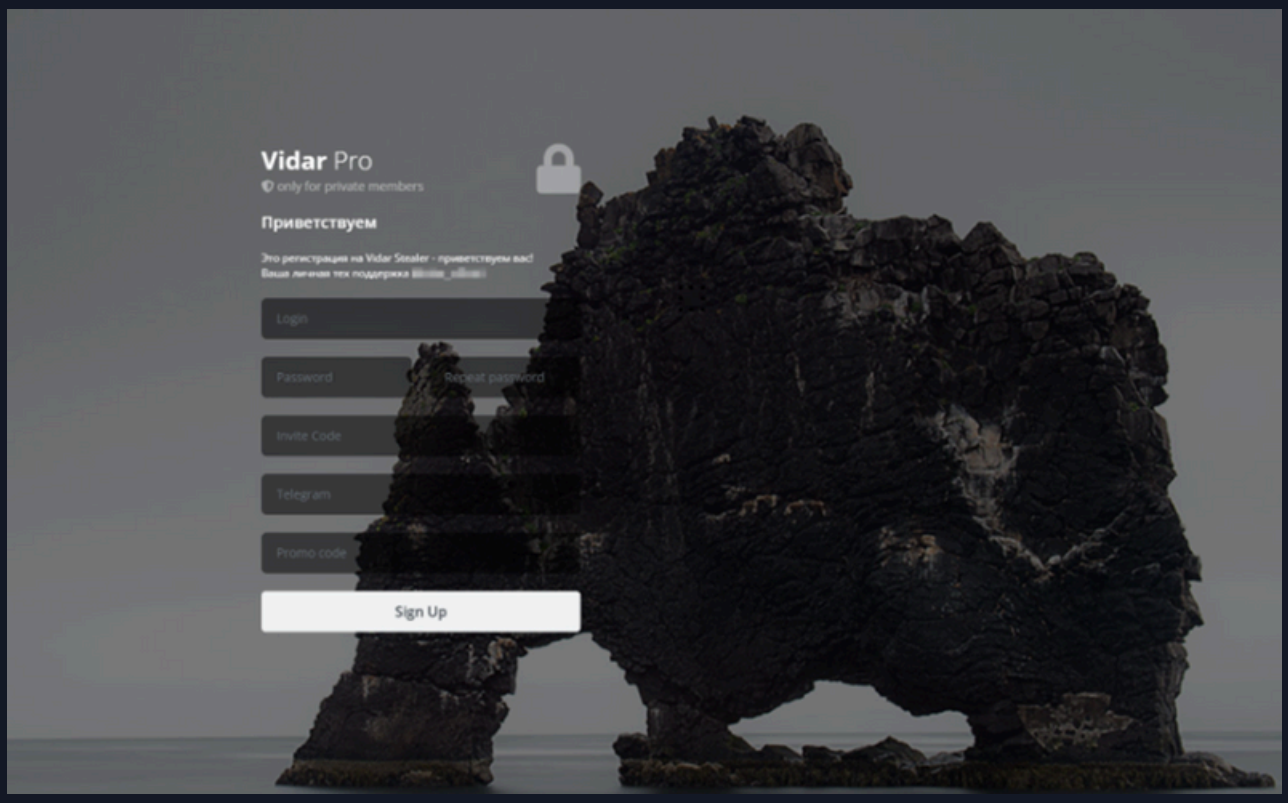
- **Academics**
- **Basic Materials**
- **Consumer Cyclicals**
  - Hotels & Entertainment
  - Retail
- **Consumer Non-Cyclicals**
- **Energy**
- **Financials**
  - Insurance
- **Government**
- **Healthcare**
- **Industrials**
  - Construction & Engineering
  - Manufacturing
  - Transportation
- **Institutions & Organizations**
- **Professional & Commercial Services**
  - Business Services
  - Legal Services
- **Real Estate**
- **Technology**
  - MSPs
  - Telecommunications
- **Utilities**

Previous Targets: Vidar Stealer

Previous Victim HQ Regions

- Vidar Stealer is a MaaS and is likely deployed worldwide; however, the operators prohibit the deployment of the malware in Belarus, Russia, Kazakhstan, and other CIS countries.

Malware Panel: Vidar Stealer



Information Gathered

Browsers

Brave, Chrome, Internet Explorer, Microsoft Edge, Mozilla Firefox, Opera

Credentials

CCleaner, FileZilla, WinSCP

Email

Microsoft Outlook, Mozilla Thunderbird

Other

Authy Desktop, EOS Authenticator, GAuth Authenticator, Google Authenticator

Wallets

Atomic, AuroWallet, BinanceChainWallet, BitAppWallet, Blockstream, BoltX, Brave Wallet, CloverWallet, Coin98, Coinbcase, CyanoWallet, Daedalus Mainnet, Dogecoin, ElectronCash, Electrum/ElectrumLTC, EQUALWallet, Ethereum, EVERWallet, Exodus, Goby, Guarda, GuildWallet, Harmony, ICONex, iWallet, JAXX, KardiaChain, Keplr, KHC, Ledger Live, LiqualityWallet, MaiarDefiWallet, MathWallet, MetaMask, MewCx/Enkrypt, MultiDoge, NeoLine, NiftyWallet, NomiWallet, Oxygen, PaliWallet, Phantom, PolyMeshWallet, Rabby, RavenCoin, RoninWallet, RoninWalletEdge, Solflare, Sollet, Temple, Terra Station, TezBox, Toroi, TronLink, Wasabi, WavesKeeper, Wombat, XdefiWallet

Associations: Vidar Stealer

Arkei Malware

Vidar Stealer has been previously linked to the Arkei malware family; however, Vidar Stealer staff has indicated that it is not of the same family but built from purchased source code.

BatLoader

Vidar Stealer has been observed as a final payload in a Batloader campaign. As Vidar Stealer is a MaaS, it is likely this was a campaign of an affiliate rather than a coordinated campaign between the two developer groups.

RisePro Malware

Security researchers have assessed that RisePro malware is a new version of the Vidar Stealer due to the similar characteristics, operates as a similar MaaS structure, and use of the same DLL dependencies.

Scattered Spider

Scattered Spider has been observed using the Vidar Stealer as part of their toolkit during attributed cyberattacks.

Bebra Malware

Vidar Stealer has been detected alongside the Bebra malware payload.

Cyclops/Knight Ransomware

Vidar Stealer has been observed as an initial payload prior to the deployment of the Cyclops ransomware variant.

Hive Ransomware

Vidar Stealer has been observed as an initial payload prior to the deployment of the Hive ransomware variant.

Laplas Clipper

Vidar Stealer has been detected alongside the Laplas Clipper payload.

Associations: Vidar Stealer

LockBit Ransomware

Vidar Stealer has been observed as an initial payload prior to the deployment of the LockBit ransomware variant.

SmokeLoader

Vidar Stealer has been detected alongside the SmokeLoader malware payload.

STOP/Djvu Ransomware

Vidar Stealer has been observed as an initial payload prior to the deployment of the STOP/Djvu ransomware variant.

XMRig Miner

Vidar Stealer has been detected alongside the XMRig Miner malware payload

Known Tools: Vidar Stealer

Applaunch	A part of the Microsoft .NET ClickOnce Launch Utility that has been used to inject and deploy malware variants.
cmd	A program used to execute commands on a Windows computer.
DerpLoader	A loader malware that has been observed in a majority of Vidar Stealer malware cyberattacks.
dllhost.exe	Vidar Stealer uses this process to execute its own code and evade detection.
explorer.exe	Vidar Stealer can inject code into this process, which is responsible for managing the Windows desktop and file manager. It allows the malware to capture screenshots and monitor user activity.
Fallout EK	An EK variant used to install malware onto a victims' computer by targeting software vulnerabilities, typically in browsers or plugins such as Adobe Flash.
GitHub	An internet hosting service for software development and version control that has been used by threat actors to host malware.
Mastadon	A free and open-source software for running self-hosted social networking services. It has been used as C2 by some threat actors.
Steam	A video game digital distribution service that can be used to play, discuss, and create games. It has been used by some threat actors for C2.
svchost.exe	Vidar Stealer uses this process to hide its presence and evade detection by security software. The process is a generic process that hosts multiple Windows services.
taskhost.exe	Vidar Stealer can hijack this process to perform malicious activities without being detected. This process manages background tasks in Windows.
Taskkill	A legitimate Windows file that is used by malware to terminate processes on the victims' computer.

Known Tools: Vidar Stealer

Telegram	A freemium, cross-platform, encrypted, cloud-based and centralized instant messaging service. Threat actors often use Telegram to communicate with other threat actors, post targets, and host malware.
TikTok	A short-form video hosting service. It has been used by threat actors as a C2.
Twitter	A social media platform often used by threat actors to post about activities, attacks, and has been previously used to leak information about a group or malware variant.
wininet.exe	Vidar Stealer can abuse this process to exfiltrate stolen data to its C2 servers.

Observed Vidar Stealer Behaviors: Windows

API/Functions	CryptUnprotectData() VirtualAlloc() CreateDirectoryA() SetCurrentDirectoryA() NSS_Init() BCryptDecrypt() GetCurrentHwProfileA() GetVolumeInformationA()
Defense Evasion	C:\Windows\System32\cmd.exe" /c taskkill /im Devil.exe /f & timeout /t 6 & del /f /q "C:\Users\MalWorkstation\Desktop\Malware.exe" & del C:\ProgramData*.dll & exit
Credential Access	%appdata%\mozilla\firefox\profiles\ (Mozilla Firefox) %appdata%\Moonchild Productions\Pale Moon\Profiles\ (Pale Moon) %appdata%\Thunderbird\Profiles\ (Thunderbird) Google\Chrome\User Data\Local State HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Sessions (Vidar Stealer is not able to decrypt the passwords if WinSCP is protected with a master password and will then only be able to extract usernames).
Discovery	SOFTWARE\Microsoft\Cryptography\MachineGuid HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\WPAD\52-54-00-36-3E-FF and HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\INTERNET EXPLORER\SECURITY SELECT HOST_KEY, is_httponly, path, is_secure, (expires_utc/1000000)-11644480800, name, encrypted_value from cookies SELECT host, isHttpOnly, path, isSecure, expiry, name, value FROM moz_cookies
Collection	\AppData\Local\Google\Chrome\User Data\Default\Web Data SELECT name_on_card, expiration_month, expiration_year, card_number_encrypted FROM credit_cards, %appdatalocal%\Google\Chrome\User Data\Default\Local Extension Settings\<extension_name>

Observed Vidar Stealer Behaviors: Windows

Command and Control	AppData\Roaming\discord\Local Storage\leveldb AppData\Roaming\discord\Session Storage\leveldb HKEY_CURRENT_USER\Software\Valve\Steam AppData\Roaming\Telegram Desktop\tdata
Other	AppData\Roaming\Authy Desktop\Local Storage\leveldb

MITRE ATT&CK® Mappings: Vidar Stealer

Initial Access	
T1189: Drive-by Compromise	
T1566: Phishing	.001: Spearphishing Attachment .002: Spearphishing Link
Execution	
T1129: Shared Modules	
T1204: User Execution	.002: Malicious File
Persistence	
T1053: Scheduled Task/Job	.005: Scheduled Task
Privilege Escalation	
T1055: Process Injection	
T1574: Hijack Execution Flow	.010: Services File Permissions Weakness
Defense Evasion	
T1027: Obfuscated Files or Information	.001: Binary Padding .002: Software Packing .005: Indicator Removal from Tools
T1036: Masquerading	.004: Masquerade Task or Service
T1070: Indicator Removal	.004: File Deletion .006: Timestomp

MITRE ATT&CK® Mappings: Vidar Stealer

Defense Evasion	
T1574: Hijack Execution Flow	.010: Services File Permissions Weakness
Credential Access	
T1539: Steal Web Session Cookie	
T1552: Unsecured Credentials	
T1555: Credentials from Password Stores	.003: Credentials from Web Browsers
Discovery	
T1007: System Service Discovery	
T1033: System Owner/User Discovery	
T1057: Process Discovery	
T1082: System Information Discovery	
T1083: File and Directory Discovery	
T1087: Account Discovery	
T1497: Virtualization/Sandbox Evasion	.001: System Checks
T1518: Software Discovery	.001: Security Software Discovery
T1614: System Location Discovery	.001: System Language Discovery

MITRE ATT&CK® Mappings: Vidar Stealer

Collection	
T1005: Data from Local System	
T1113: Screen Capture	
T1115: Clipboard Data	
T1119: Automated Collection	
Command and Control	
T1071: Application Layer Protocol	.001: Web protocols
T1095: Non-Application Layer Protocol	
T1102: Web Service	.001: Dead Drop Resolver
T1105: Ingress Tool Transfer	
Exfiltration	
T1020: Automated Exfiltration	
T1041: Exfiltration Over C2 Channel	

References

- BalaGanesh (2023, February 24) Security Investigation: “Vidar Infostealer Malware Returns with new TTPS – Detection & Response.” https://www.socinvestigation.com/vidar-infostealer-malware-returns-with-new-ttps-detection-response/
- Check Point (n.d.) “What is Vidar Malware?” https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/what-is-vidar-malware/
- Counter Threat Unit Research Team (2023, November 30) SecureWorks: “Vidar Infostealer Steals Booking.com Credentials in Fraud Scam.” https://www.secureworks.com/blog/vidar-infostealer-steals-booking-com-credentials-in-fraud-scam
- Cyble (2021, October 26) “Vidar Stealer Under the Lens: A Deep-dive Analysis.” https://cyble.com/blog/vidar-stealer-under-the-lens-a-deep-dive-analysis/
- eSentire TRU (2023, May 09) “eSentire Threat Intelligence Malware Analysis: Vidar Stealer.” https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-vidar-stealer
- Farghaly, Mostafa (n.d.) GitHub: “Deep Analysis of Vidar Stealer.” https://m4lcode.github.io/malware%20analysis/vidar/
- g0njxa (2023, November 30) Medium: “Approaching stealers devs: a brief interview with Vidar.” https://g0njxa.medium.com/approaching-stealers-devs-a-brief-interview-with-vidar-2c0a62a73087
- GridinSoft (2024, February 15) “Vidar Stealer Malware.” https://gridinsoft.com/spyware/vidar
- Holland, Aidan (2023, November 21) Censys: “Tracking Vidar Infrastructure with Censys.” https://censys.com/tracking-vidar-infrastructure/
- Quorum Cyber (2023, January) “Malware Analysis Report Vidar – Stealerware.” https://www.quorumcyber.com/wp-content/uploads/2023/01/Malware-Analysis-Vidar.pdf

Adversary Pursuit Group

blackpoint