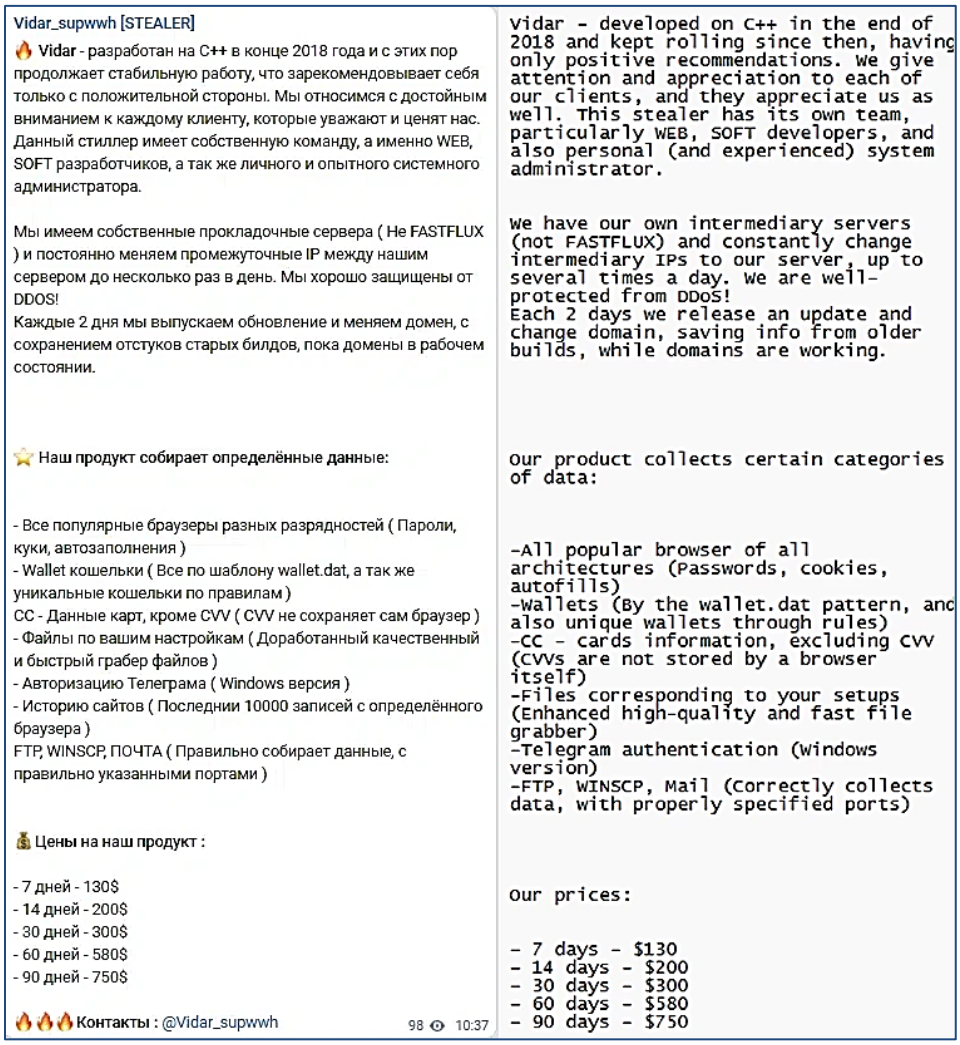
HC3: Analyst Note
July 2, 2024 TLP:CLEAR Report: 202407021700

Vidar Malware

Executive Summary

Vidar (also known as Vidar Stealer) is an infostealer malware operating as malware-as-a-service, which was first discovered in late 2018 and is likely a direct evolution of the Arkei trojan. Sold on the dark web for anywhere between $130 and $750 (depending on the license), the malware runs on Windows and can collect a wide range of sensitive data from browsers and digital wallets. Additionally, the malware is used as a downloader for ransomware. Since its emergence, Vidar has grown to be one of the most successful infostealers.



Vidar_supwwh [STEALER]

🔥 Vidar - разработан на C++ в конце 2018 года и с этих пор продолжает стабильную работу, что зарекомендовывает себя только с положительной стороны. Мы относимся с достойным вниманием к каждому клиенту, которые уважают и ценят нас. Данный стиллер имеет собственную команду, а именно WEB, SOFT разработчиков, а так же личного и опытного системного администратора.

Мы имеем собственные прокладочные сервера (Не FASTFLUX) и постоянно меняем промежуточные IP между нашим сервером до несколько раз в день. Мы хорошо защищены от DDOS!
Каждые 2 дня мы выпускаем обновление и меняем домен, с сохранением отстуков старых билдов, пока домены в рабочем состоянии.

⭐ Наш продукт собирает определённые данные:

- Все популярные браузеры разных разрядностей (Пароли, куки, автозаполнения)
- Wallet кошельки (Все по шаблону wallet.dat, а так же уникальные кошельки по правилам)
CC - Данные карт, кроме CVV (CVV не сохраняет сам браузер)
- Файлы по вашим настройкам (Доработанный качественный и быстрый грабер файлов)
- Авторизацию Телеграма (Windows версия)
- Историю сайтов (Последних 10000 записей с определённого браузера)
FTP, WINSCP, ПОЧТА (Правильно собирает данные, с правильно указанными портами)

💰 Цены на наш продукт :

- 7 дней - 130$
- 14 дней - 200$
- 30 дней - 300$
- 60 дней - 580$
- 90 дней - 750$

🔥🔥🔥 Контакты : @Vidar_supwwh 98 10:37

vidar - developed on C++ in the end of 2018 and kept rolling since then, having only positive recommendations. We give attention and appreciation to each of our clients, and they appreciate us as well. This stealer has its own team, particularly WEB, SOFT developers, and also personal (and experienced) system administrator.

We have our own intermediary servers (not FASTFLUX) and constantly change intermediary IPs to our server, up to several times a day. We are well-protected from DDoS!
Each 2 days we release an update and change domain, saving info from older builds, while domains are working.

our product collects certain categories of data:

-All popular browser of all architectures (Passwords, cookies, autofills)
-Wallets (By the wallet.dat pattern, and also unique wallets through rules)
-CC - cards information, excluding CVV (CVVs are not stored by a browser itself)
-Files corresponding to your setups (Enhanced high-quality and fast file grabber)
-Telegram authentication (Windows version)
-FTP, WINSCP, Mail (Correctly collects data, with properly specified ports)

our prices:

- 7 days - $130
- 14 days - $200
- 30 days - $300
- 60 days - $580
- 90 days - $750

Vidar promotion post in a Telegram chat. *Source: Gridinsoft*

Report

Vidar is primarily an infostealer, meaning that it is designed to collect a variety of sensitive information from an infected computer and exfiltrate this data to an attacker. Some examples of the information that Vidar collects from infected computers, browsers, and digital wallets include:

- OS data

- Account credentials
- Credit card data
- Browser history

Throughout its history, Vidar typically uses email as its primary means of delivery, but recently it has also utilized an ISO file (a disk image file format commonly used by malware authors to package their malware). In Vidar's case, the malicious ISO has been embedded in fake installers for legitimate software such as Adobe Photoshop and Microsoft Teams, delivered via the Fallout exploit hit, and sent as an attachment to phishing emails. Once the malware reaches an infected machine, it uses a few different techniques to protect against detection. Among these are the use of a large executable file — designed to defeat antivirus scanners — and files digitally signed with an expired and potentially breached Avast digital certificate.

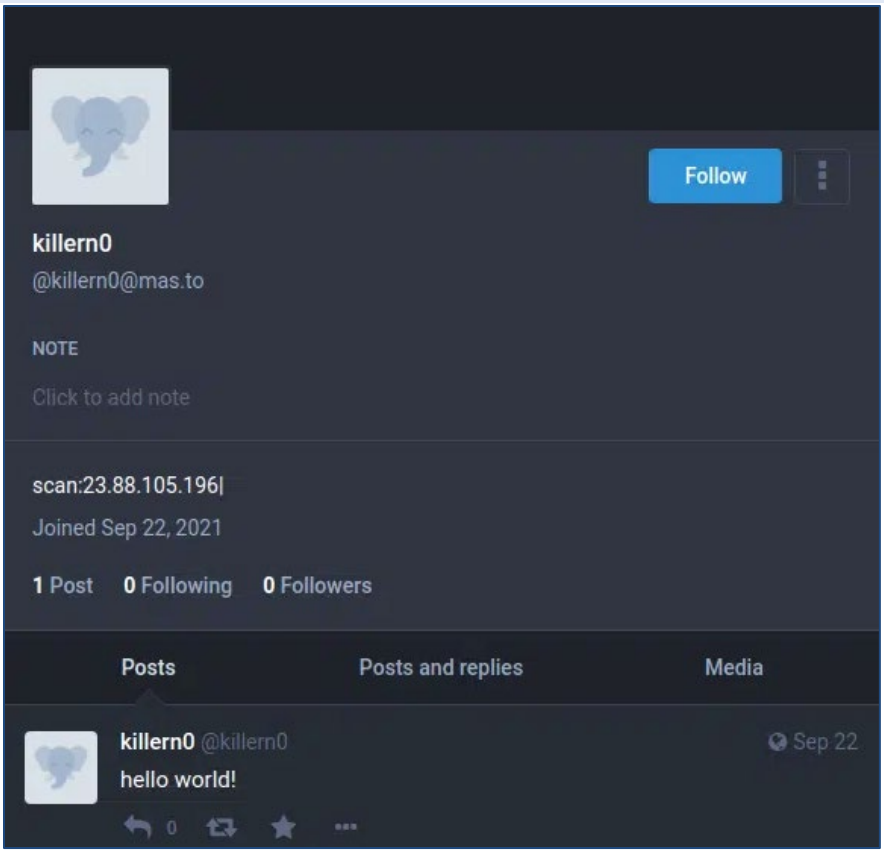
Vidar frequently uses social media as part of its command and control (C2) infrastructure. The IP address of the C2 infrastructure will be embedded in a user profile on platforms like Mastodon, Telegram, etc. The malware can access this profile, contact the indicated IP address, and download configuration files, instructions, and other malware. Considering the fact that Vidar—like other stealers—also defaults to performing self-destruction after gathering all the information from the system, it is a rather prolific malware.

Analysis

Vidar uses tricks to avoid instant detection by both in-system antivirus software and analysis sites like VirusTotal. It contains a row of null bytes at the beginning of the file to bloat its size up to around 700 MB, which exceeds file size limits of anti-malware software—thus the file is skipped—but this tactic is applied only in cases when Vidar arrives within the library, i.e., via a search result malvertising campaign or email with the library attached.

This malware does not require tricking the user into running it, as macros do everything. Since 2021, Vidar has used the same loader—DerpLoader—for its attack. It is the first part of the malware to run, and it is in charge of creating a dedicated memory area, preparing the binary, and injecting it into that area. The 18-bit decryption key is supplied inside of the loader. (Note: It is different in each analyzed sample of Vidar.) After that, using the *VirtualAlloc* function, the loader creates a memory area and injects the results of decoding/decryption, simultaneously passing the execution to that area. At that moment, the malware is ready to run, and the first thing it does after launching is contact the C2 server. The IP address of the C2 server is not present within the Vidar sample. Instead, the malware carries an address of a social network page, which contains the C2 IP in its name or description. The most widely used social media Vidar uses are Telegram and Mastodon.

HC3: Analyst Note
July 2, 2024 TLP:CLEAR Report: 202407021700



Mastodon account used to route the C2 connection. *Source: Gridinsoft*

First contact with the C2 server contains only a bot ID within a standard GET request. The server in turn replies with a configuration package that contains guidances upon behavior, as well as the DLL the malware needs for running. It uses certain native Windows libraries, but most of the required ones arrive only after the C2 communication. It is worth noting that the malware supposes different behavior patterns, and thus different DLL lineups that suit each case. The most commonly used DLLs are:

- vcruntime140.dll
- msvcp140.dll
- freebl3.dll
- sqlite3.dll
- softokn3.dll
- mozglue.dll
- libcurl.dll
- nss3.dll

The body of a C2 response contains a specification that points at the features to be used, as well as a list of specific directories and names to look for.

After receiving the configuration file from the server, Vidar moves to its next step: data stealing. Overall, Vidar may collect the following categories of data from the target system:

- List of installed software
- Last downloaded files (in the Downloads folder)
- Cryptocurrency wallets
- Autofill files
- Browser cookies
- Browsing history
- Files of specific formats

It also checks the mentioned directory for files that contain the following words in naming:

- Passwords
- Information
- Outlook
- Screenshot
- Cookie
- List

To the web browsers present in the system, malware applies a specific string of actions. The two main groups Vidar targets are Chrome and Chromium-based browsers, and Firefox with Quantum-based analogs. In the root directory of Chrome, it extracts account information, passwords, and usernames. Considering that people often use their Google account to log into Chrome, this could be incredibly detrimental. Direct extraction of login credentials is not possible in late Chrome versions (80.0+), but the malware has its own way to circumvent this. It creates a query to a database file that keeps this information and receives what it needs. Firefox and related browsers receive nearly the same treatment—an SQL request that extracts credentials from a database. However, some of the last Firefox versions keep credentials in a logins.json file in the encrypted form. To deal with that problem, Vidar uses the nss3.dll library previously mentioned. Browsers developed by Microsoft (Internet Explorer and Edge) are attacked with the use of Vault functionality, which is a third-party identity management system. Vidar has an embedded solution based on this program that helps it to extract credentials from these browsers, which use a different way to store login information.

Aside from grabbing account credentials, Vidar is also capable of messing with browser cookies. The way it extracts information from cookie files depends on the browser, as in the case of personal data decryption. IE and Microsoft Edge store cookies in a regular .txt file, thus malware succeeds in stealing them by just scanning these browsers' directories. Chrome and Firefox are a different story; these two browsers use SQL databases to keep all the cookies in less accessible forms. It is also worth noting that they are kept away from a root directory, particularly in the corresponding folder in the *App/Data/Roaming* or */Local* directory. A SQL query (unique for each browser type) will extract cookies in a similar fashion, as with login credentials.

Next, Vidar checks if there are any FTP clients present in the system. Earlier versions of Vidar could attack only WinSCP and FileZilla clients, along with Pidgin messenger, but that has changed. Now, this malware is able to steal credentials from both autofill form and currently active sessions. Vidar also pays additional attention to two email clients—MS Outlook and Mozilla Thunderbird—and it tries to steal login credentials from these services. Additionally, it carries the ability to steal information about cryptocurrency wallets

kept in the system going for the most popular wallets such as Exodus, ElectronCash, Ethereum, Electrum/ElectrumLTC, MultiDoge, Atomic, and JAXX.

Finally—to keep the collected information in one place—before sending it to the command server, Vidar stealer keeps it in a directory in the *ProgramData* folder. It is already hidden; thus, malware does not worry about the user noticing it during routine browsing. In the directory with a randomized name, it creates folders that correspond to the categories of extracted data, as well as unsorted data and screenshots that lay at the directory root. After finishing the data collection, Vidar stealer packs it into a ZIP archive, and sends it to a command server. Once done, the malware initiates a self-destruct process, but before doing so, it deletes all the files it managed to collect and bring to its root directory. As it leaves no straightforward evidence, investigating what happened to the system is difficult.

Vidar Malware Indicators of Compromise (IOCs)

Malware Taxonony Hashes	
Malware Taxonomy	**SHA256**
Spy.Win64.Vidar.tr	- 3c67ddeb2426bfd91144dd8ca4ec06ee20578105514ad629c830e194bfd65893
Spy.Win32.Vidar.tr	- 8fce32ef6687aeb691c1a9427cfbf11fd6e9c0407bb8dcbab1f839d88077172e - 55575cb7f0ced9114e7c8b6ffe8081bed842d8dc9ac1b57cc69ca66534c7aac6
Spy.U.Vidar.tr	- 0bbdda44330f983208041c1422e52759e87de6c4438b152d6dc36e17f07f9765 - 3bae8ea58db5926584007d715d1f47fc60cc8e219b564ef5dddc5c7dbc70f9be - 1ccfce02fe1c6407fdcbbd93f8d234ef7ec7d4fbdf8a09e594302a7757d6b463 - 141625c898ccd820bfde15265079fff595417ab13f95e139a376642e956c3727 - b6b8c9103f43ea8a354fbaab763b84b2718142181a482ee5e1b7065f266ae451
Spy.Win32.Vidar.bot	- a58eb00dc23a5b23214a1e4db215cd00fe6ed77aeda1537ea4fd76aa3ef749fd
IP Addresses	
	- 162[.]241[.]225[.]237 - 5[.]79[.]66[.]145 - 104[.]21[.]45[.]70 - 193[.]29[.]187[.]162 - 104[.]18[.]5[.]149 - 45[.]151[.]144[.]128 - 18[.]205[.]93[.]2 - 141[.]8[.]194[.]149 - 95[.]217[.]16[.]127 - 157[.]90[.]148[.]112

	- 116[.]203[.]6[.]107 - 37[.]140[.]192[.]11 - 185[.]163[.]204[.]10
Domains	
	- notepadplusplus[.]site - download-notepad-plus-plus[.]duckdns[.]org - download-obsstudio[.]duckdns[.]org - dowbload-notepadd[.]duckdns[.]org - dowbload-notepad1[.]duckdns[.]org - download-davinci-resolve[.]duckdns[.]org - download-davinci[.]duckdns[.]org - download-sqlite[.]duckdns[.]org - download-davinci17[.]duckdns[.]org - download-rufus[.]duckdns[.]org - download-kritapaint[.]duckdns[.]org
URLs	
	- hxxps://t[.]me/litlebey - hxxps://steamcommunity[.]com/profiles/76561199472399815
Social Media Addresses	
	- hxxp://www[.]tiktok[.]com/@user6068972597711 - hxxps://t[.]me/mantarlars - mas[.]to/@zara99 - ioc[.]exchange/@zebra54 - nerdculture[.]de/@yoxhyp - hxxp://www[.]ultimate-guitar[.]com/u/smbfupkuhrgc1 - mas[.]to/@kyriazhs1975 - mastodon[.]online/@olegf9844g - steamcommunity[.]com/profiles/76561199436777531 - ioc[.]exchange/@xiteb15011 - hxxps://t[.]me/larsenup - c[.]im/@xinibin420 - nerdculture[.]de/@yixehi33 - mas[.]to/@ofadex - t[.]me/asifrazatg - steamcommunity[.]com/profiles/76561199441933804 - c[.]im/@xiteb15011 - nerdculture[.]de/@tiaga00 - steamcommunity[.]com/profiles/76561199439929669
Filename Hashes	
Filename	**SHA256**
npp.Installer.x64.zip	- 7DFD1D4FE925F802513FEA5556DE53706D9D8172BFA207D0F8AAB3CEF46424E8

HC3: Analyst Note

July 2, 2024 TLP:CLEAR Report: 202407021700

Filename Hashes	
npp.Installer.x64.exe	- 368008b450397c837f0b9c260093935c5cef56646e16a375ba7c47fea5562bfd
rufus-3.21.zip	- 75db4f8187abf49376a6ff3de0163b2d708d72948ea4b3d5645b86a0e41af084
rufus-3.21.exe | krita-x64-5.1.5-setup.exe | DaVinci_Resolve_18.1.2_Windows.exe	- 169603a5b5d23dc2f02dc0f88a73dcdd08a5c62d12203fb53a3f43998c04bb41
DaVinci_Resolve_18.1.2_Windows.zip	- 73f00e3b3ab01f4d5de42790f9ab12474114abe10cd5104f623aef9029c15b1e
krita-x64-5.1.5-setup.zip	- 85eb4b0e3922312d88ca046d89909fba078943aea3b469d82655a253e0d3ac67

Vidar Malware MITRE ATT&CK Tactics, Techniques, & Procedures (TTPs)

Technique ID	Description
T1204	User Execution
T1555	Credentials from Password Stores
T1539	Steal Web Session Cookie
T1614	System Location Discovery
T1518	Software Discovery
T1007	System Service Discovery
T1095	Non-Application Layer Protocol
T1566	Phishing
T1552	Unsecured Credentials
T1113	Screen Capture
T1057	Process Discovery
T1087	Account Discovery
T1041	Exfiltration Over C&C Channel

Protecting Against Vidar

- **Anti-Malware Software:** Being confident an employee is doing everything right is not enough to protect an organization's system from malware invasion. It sometimes may come from unexpected places, and to cover these blind spots, an organization should consider an anti-malware program.
- **Employee Training:** Vidar is commonly distributed via phishing emails or fake downloads of legitimate software, which actually deliver the malware. Training employees to recognize and respond properly to malicious attachments, and to avoid cracked copies of legitimate software, can reduce the threat of a Vidar infection.
- **Email Security:** Many Vidar campaigns deliver the malicious ISO file as an attachment to a phishing email. Email security solutions that inspect email attachments for malicious content can identify and block the Vidar malware before it reaches a user's inbox.
- **Web Security:** Vidar malware can be distributed as part of a malicious download where the malware masquerades as a free version of legitimate software. Web security solutions can identify and block malicious downloads and visits to dangerous sites before malware can reach a user's computer.

- **Strong Passwords**: Vidar steals credentials from various locations, but some of this data may be password hashes rather than plaintext passwords. Use of strong, long, and random passwords can make them more difficult for an attacker to crack.
- **Multi-Factor Authentication (MFA):** As an infostealer, user credentials are a major target of the Vidar malware. Deploying MFA wherever possible can make it more difficult for an attacker to use the credentials that they have stolen.

References

Information-Stealing Malware Malvertises on Google
https://darktrace.com/blog/vidar-info-stealer-malware-distributed-via-malvertising-on-google

Vidar Stealer Malware
https://gridinsoft.com/spyware/vidar

What is Vidar Malware?
https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/what-is-vidar-malware/

Data Exfiltration Trends in Healthcare
data-exfiltration-in-healthcare-tlpclear.pdf (hhs.gov)

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback