INTRINSEC

Innovative by design

“Chaos is a ladder”: Vidar’s recent rise to the top

Cyber Threat Intelligence

April 2026

@Intrinsec @Intrinsec Blog Website

2026 Intrinsec, Inc. All rights reserved.

Table of contents

1. Key findings

Detailed in this report:

- The state of Vidar in the beginning of 2026. Following major takedowns affecting Lumma and Rhadamanthys, Vidar profited from the generated chaos to rise to the top of the stealer ecosystem. We assess that this rise was made available due to the release of version 2.0 of the malware, and to the collaboration with "Cloud" Telegram channels.
- Details on a kill-chain that infected corporate employees. We were able to analyse the whole kill-chain starting from the download of a fake software advertised on YouTube, unpacking of the Vidar stealer and selling of credentials on Russian Market.
- Analysis of the Vidar sample. While the new version of the malware was already recently analysed by other editors, we gave details on the C2 recovery mechanism using dead drop resolvers, control flow flattening to slow down analysis. The discovery of an unpacked sample potentially uploaded by a Russian threat actor on VirusTotal reveals the classic stealing capabilities.
- Details on the infrastructure used by Vidar. This infrastructure was previously identified in our Acreed analysis; however, we were able to determine the use of some of the domains for the generation of built payloads by clients of Vidar.

2. Introduction

Infostealer is still an important threat. The year 2025 saw many shifts in the ecosystem, mainly due to international police operations leading to the takedowns of stealer infrastructure. Lumma and Rhadamanthys were the main ones affected, but the chaos resulting from their downfall created more opportunities for their competitors.

Lumma was the number one stealer in the market since the end of 2024 and at the beginning of 2025. However, a takedown operation announced in May 2025 by Europol and its partners[1] resulted in a continuous slowdown of its use by threat actors and visible activity. At first, the takedown had a limited impact on the market. But as time continued, more threat actors abandoned the project and shifted to other stealers, due to concerns on the security of the project and operational continuity. Even though, the project is not discontinued, and some threat actors are still leveraging it[2] mainly in ClickFix campaigns.

From the disruptions, the newly born Acreed (which we previously analysed, see ***Analysis of Acreed, a rising infostealer***) [3] saw a surge in use, followed by Vidar and Stealc.

Around mid-2025, Rhadamanthys started to become used more, and we analysed the shift from Lumma to Rhadamanthys in another analysis. However, only a few months after its rising popularity, Rhadamanthys was also subject to a takedown operation in November 2025[4].

Around all this instability, Vidar's operator(s) probably saw an opportunity for greater success and announced the release of the version 2 of its malware in October 2025[5]. Following this announced, we noted a steady rise of its popularity amongst threat actors. In this analysis, we wanted to explain why Vidar (which we previously analysed in 2022 and in a campaign analysis in the beginning of 2025, is now the top infostealer and understand its current distribution channels and TTPs, as we came across a kill-chain used to compromise corporate and non-corporate users.

[1] https://www.europol.europa.eu/media-press/newsroom/news/europol-and-microsoft-disrupt-world%E2%80%99s-largest-infostealer-lumma
[2] https://www.bitdefender.com/en-us/blog/labs/lummastealer-second-life-castleloader
[3] https://www.intrinsec.com/analysis-of-acreed-a-rising-infostealer/
[4] https://www.europol.europa.eu/media-press/newsroom/news/end-of-game-for-cybercrime-infrastructure-1025-servers-taken-down
[5] https://www.trendmicro.com/en_us/research/25/j/how-vidar-stealer-2-upgrades-infostealer-capabilities.html

3. Vidar's recent rise

3.1 The top stealer since November 2025

After reviewing the infostealer ecosystem for our annual threat reporting, we noticed that Vidar was the top stealer on the Russian Market marketplace. We assess that this is mainly in response to the takedowns which affected infrastructures of Lumma and Rhadamanthys. Acreed tried to take a significant portion of the market share but ultimately since November 2025, Vidar is the most used stealer on the marketplace.

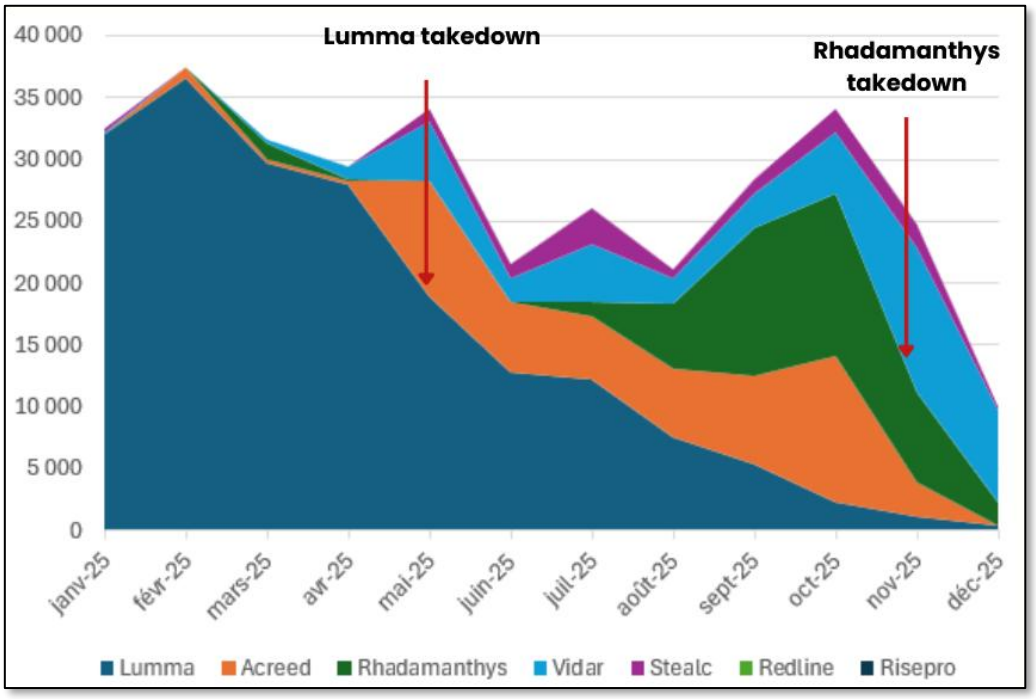


Figure 1: Number of logs uploaded on Russian Market per stealer by months. Source: Intrinsec.

Initially this surprised us as this was a rather "old" stealer compared to other participants. Our team previously wrote a first analysis of this stealer back in 2022. However, after a thorough review we observed Vidar in recent ClickFix campaigns in January 2025, and we were alerted on instances of compromise of some of our client's employees by the Vidar stealer.

Furthermore, we noticed that several recent public reports mentioned the use of Vidar in attack campaigns. CISA published a security advisory on 29 July 2025 on Scattered Spider, indicating that Vidar was amongst the malware and tools used by the threat group[6]. On 6

[6] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a

November 2025, Datadog by Security Labs published a report on the delivery of Vidar by leveraging trojanized npm packages[7].

[7] https://securitylabs.datadoghq.com/articles/mut-4831-trojanized-npm-packages-vidar/

3.2 Release of version 2.0 of the malware

The user “Loadbaks” on Exploit is the main user advertising the Vidar malware on the forum, since 3 November 2018. After few announcements made during the first half of 2025, “Loadbaks” released Vidar 2.0 on 6 October 2025.

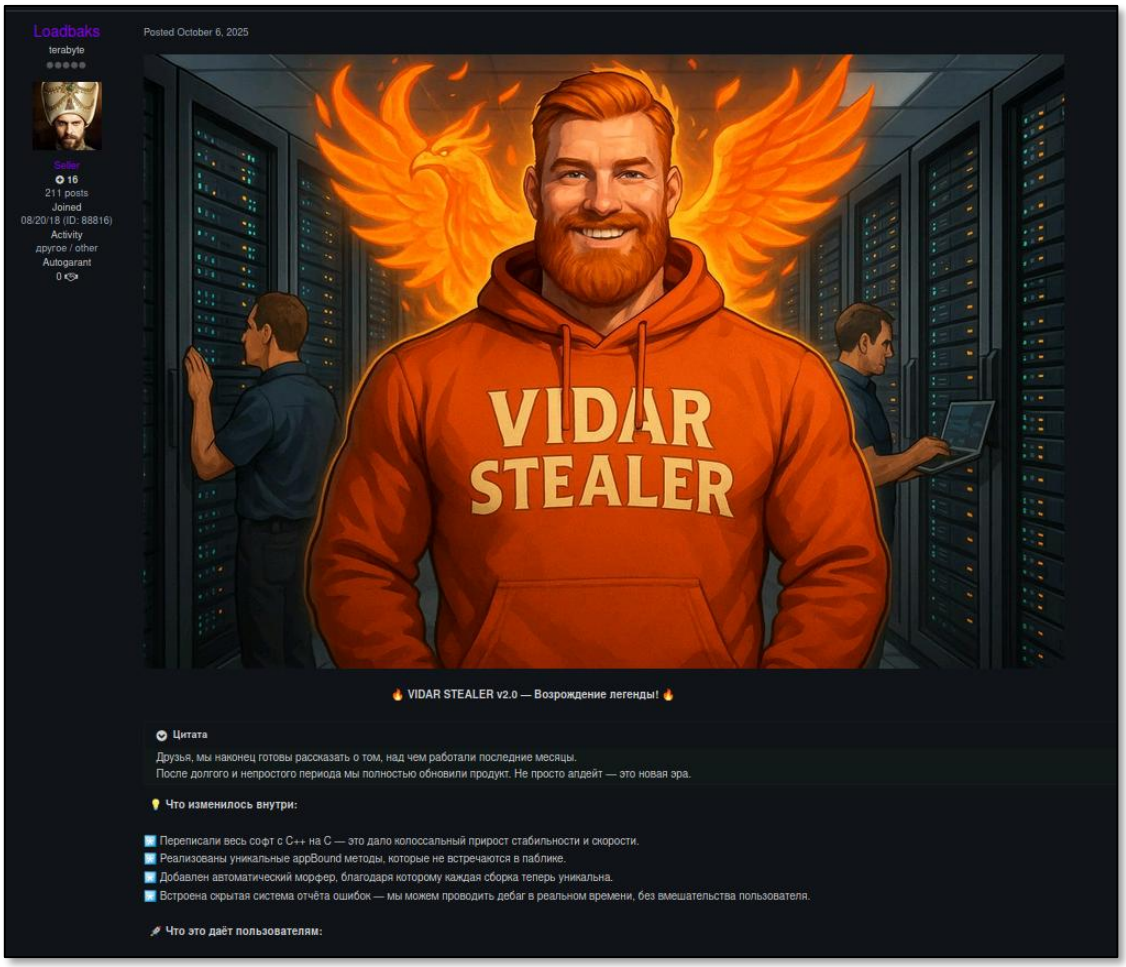


Figure 2: Vidar advertising on Exploit.

The developer behind the Vidar stealer has an extensive online presence, used to advertise its product and maintain a steady client base. Inside logs collected by Vidar, the file “information.txt” reveals the domain used to advertise Vidar, which is now **vidars[.su**.

information.txt

```
1  -- VIDAR STEALER - ЛУЧШИЙ STEALER НА РЫНКЕ!!!!
2  -- Контакты для связи: https://reg.vidars.su/
3
```

Figure 3: Vidar main domain inside “information.txt”.

The specific “reg” subdomain is a login and registration panel for clients of the stealer.

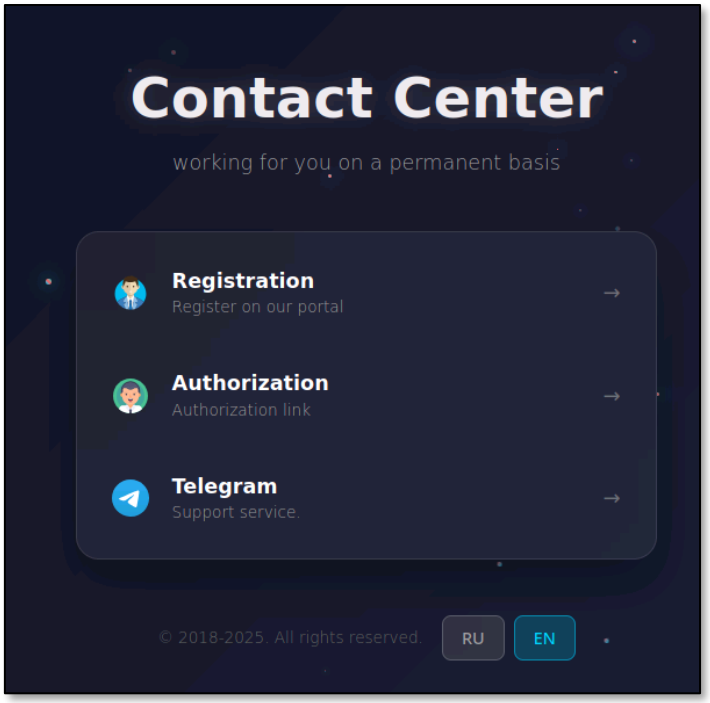


Figure 4: Content of the registration panel.

3.3 Telegram Cloud collaboration

The registration page asks for an invite code so we could not create an account. However, we can still extract relevant information from it. This page shows a list of forums and channels where Vidar's operator probably advertised the malware. The "cloud" channels refer to Telegram channels where stolen logs are shared freely or available for sale. As such, we can suspect that **KATANACLOUD, POLTERGEIST CLOUD, CRON CLOUD** and **0MEGA CLOUD** shared Vidar logs and probably cooperate with Vidar's operator.

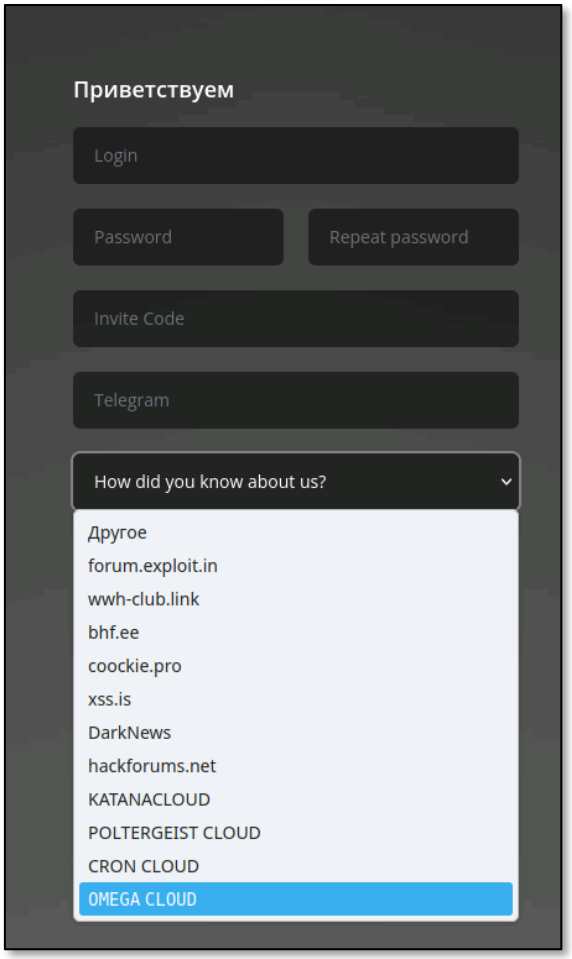


Figure 5: Telegram “Cloud” channels mentioned in the panel.

If we look inside the **KATANACLOUD** channel, we can confirm that the channel advertises Vidar stealer as its main stealer.

Figure 6: Mention of Vidar inside KatanaCloud's channel. Source: https://t.me/KATANACLOUD_NEWS/20

Inside one of the free logs shared in the channel, we can also consult the "information.txt" file which directly mentions Vidar, further confirming the proof that the owner of this channel shares logs stolen by Vidar, either as a direct client of the malware or as a promotion channel for other threat actors.

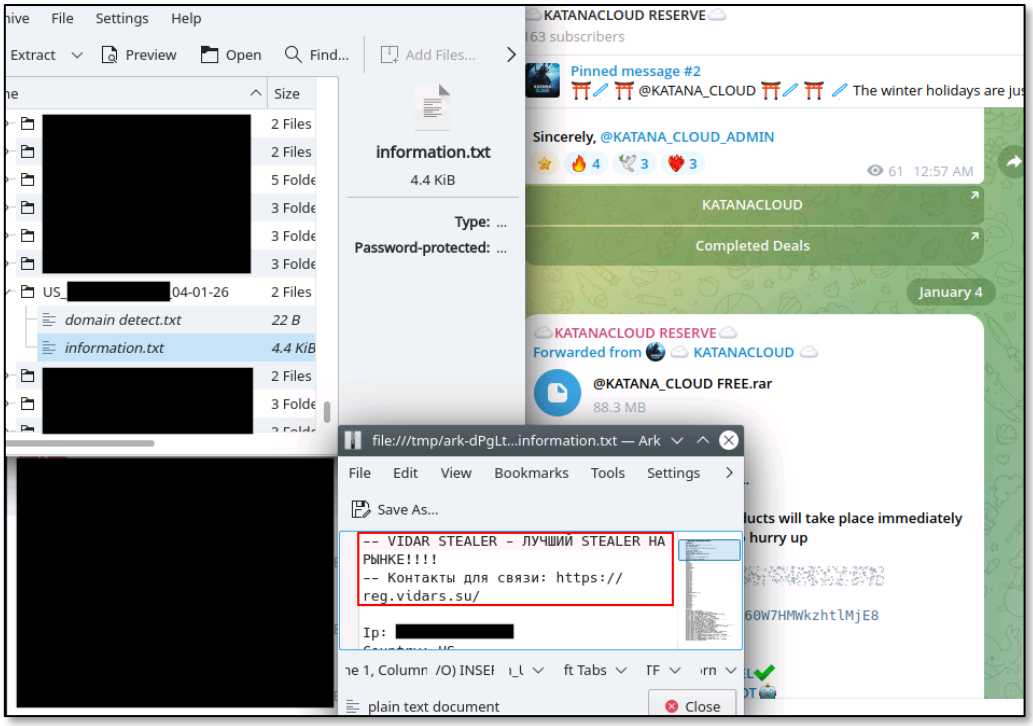


Figure 7: Vidar log inside a free archive shared by KatanaCloud. Source: https://t.me/KATANACLOUD_RESERVE/28

We also noticed on 12 January 2026 that the **BradMax Cloud** started advertising the Vidar stealer.

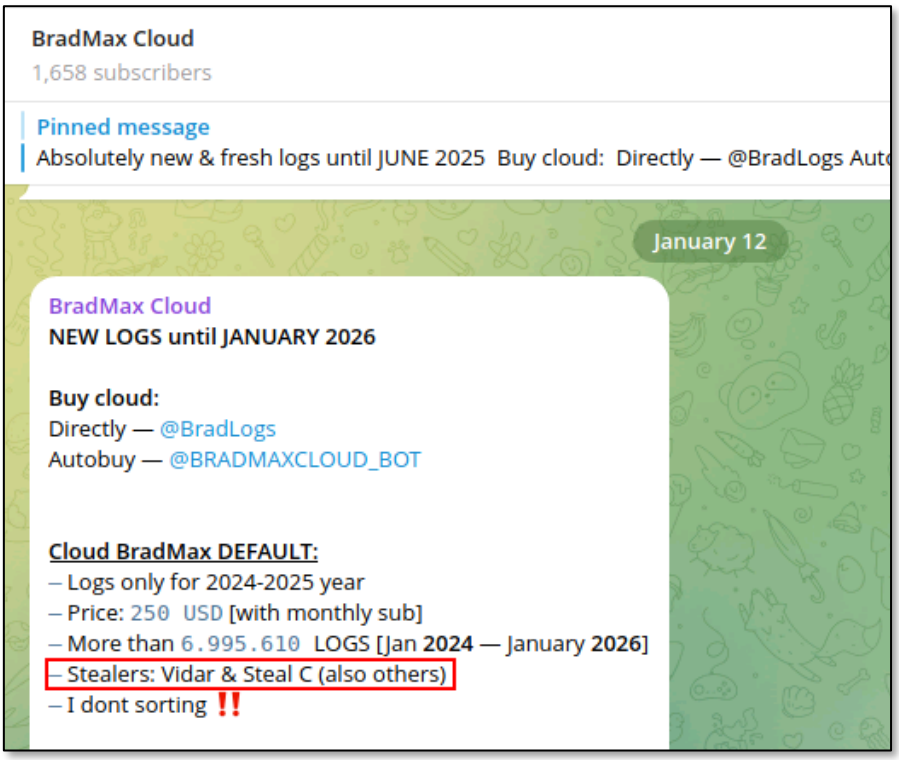


Figure 8: Vidar mentioned inside BradMax Cloud's channel. Source: https://t.me/c/2380538610/267

These elements may help in explaining why Vidar is now the number one stealer on Russian Market. Telegram “cloud” channels fuels the ecosystem of stolen logs and help advertise the stealers behind the stolen data. Subscribers to these channels may notice that more channels are now using Vidar and therefore think that this is a useful program to steal data. This in returns helps Vidar grow its client base by catering to individual threat actors looking for financial gains.

4. Infecting corporate users: kill-chain illustration

As we explained earlier, we were notified of a Vidar compromise affecting one of our client's employees. We were able to obtain data on this compromise, which helps detail almost all the aspects of the kill-chain that led to the exfiltration of sensitive data.

Find below a schematic breakdown of the analysed kill-chain.

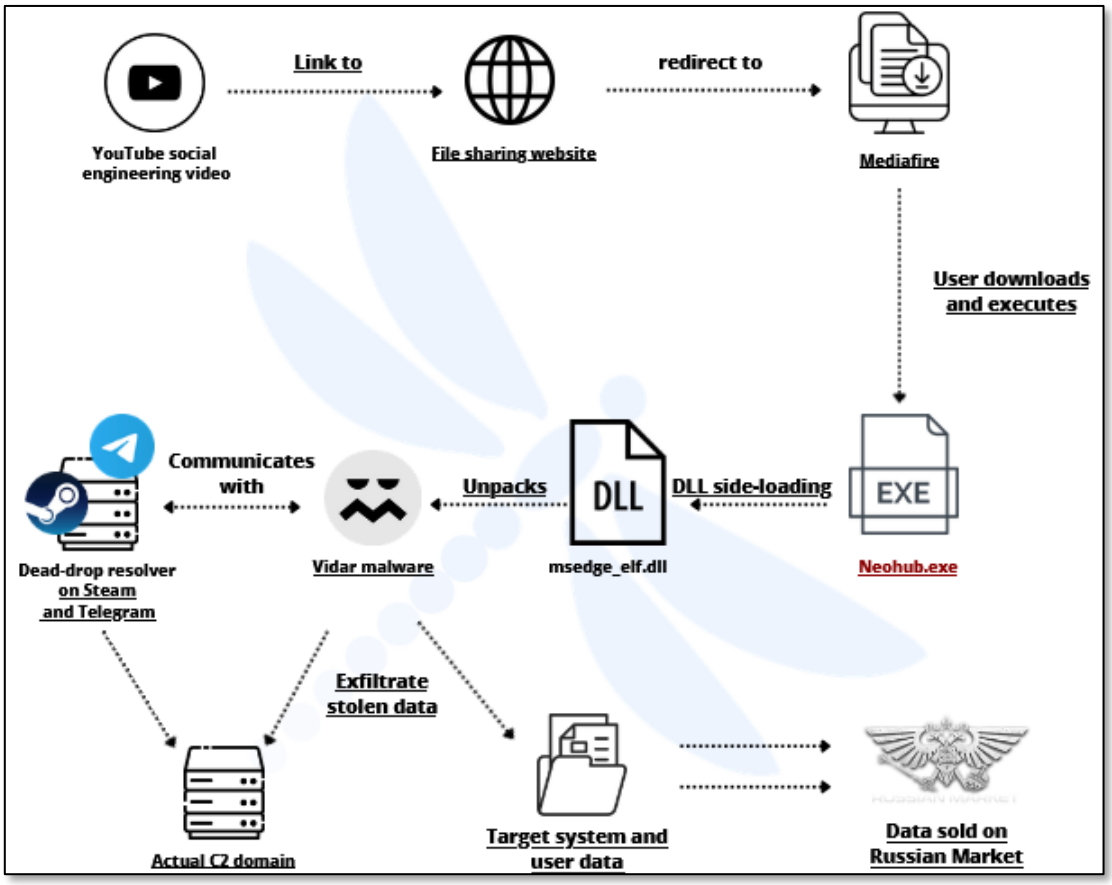


Figure 9: Kill-chain execution flow.

4.1 Delivering the archive

The victim was compromised by downloading a file masquerading as NeoHub, from the website Mediafire. We are not sure how the victim came across this URL but by reviewing content inside the stolen log, we can hypothesize that it came from YouTube, as the victim visited YouTube and was then probably redirected to the filesharing website filefa[.st, before landing on Mediafire.

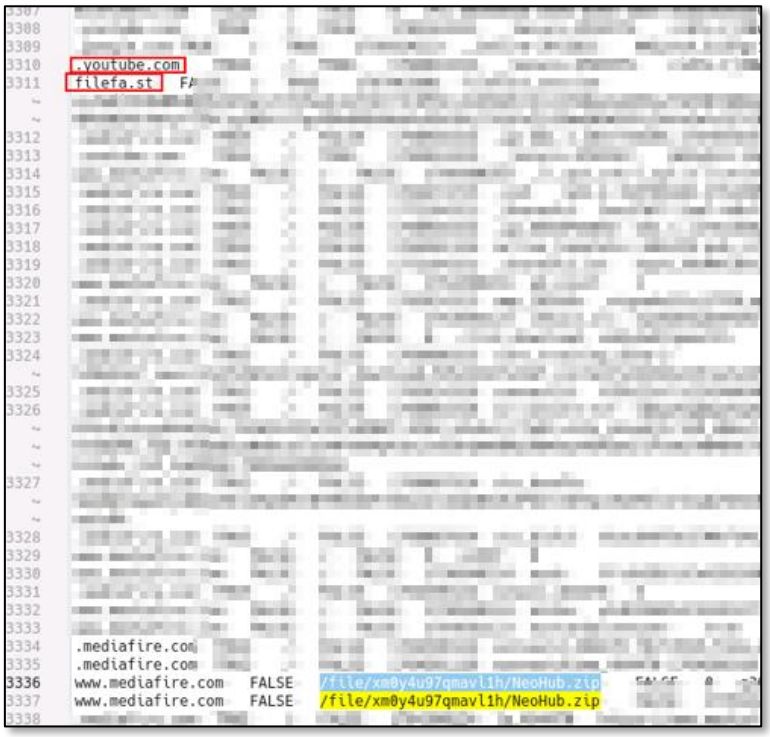


Figure 10: Websites visited before downloading the malicious archive.

At the time of writing of this report, the malicious archive was still available on Mediafire[8]. As such, we were able to download and analyse it.

8 https://www.virustotal.com/gui/url/cc0440fcfa3210939f032721fa90b90604a75c3602c09fa4d5ea29826baeb5b1/relations

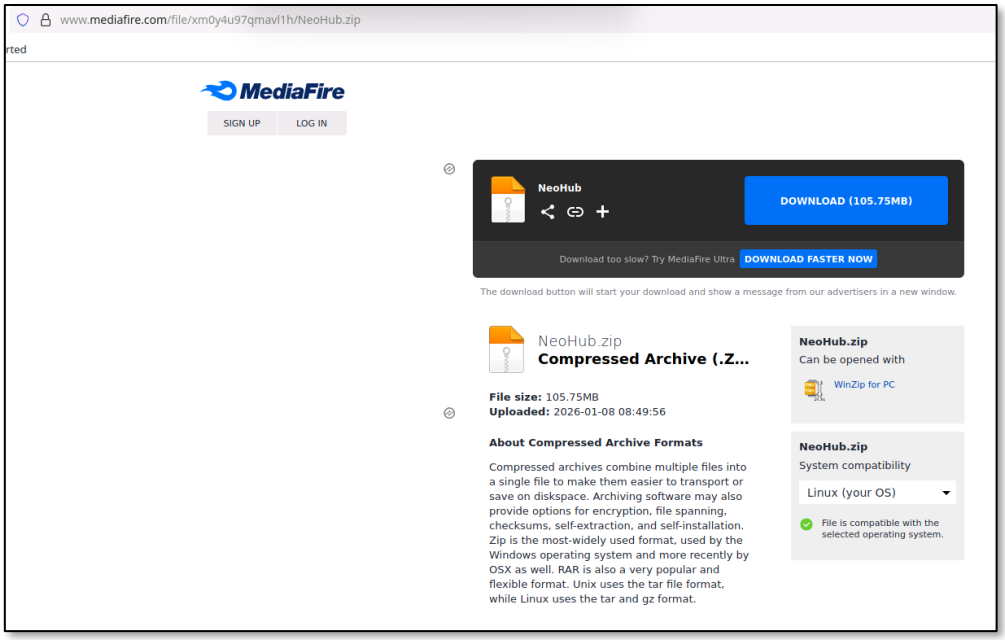


Figure 11: Malicious archive found on Mediafire.

The archive contains the following files, which were created on 16 October 2025. To note, the archive's hash was not found on VirusTotal[9].

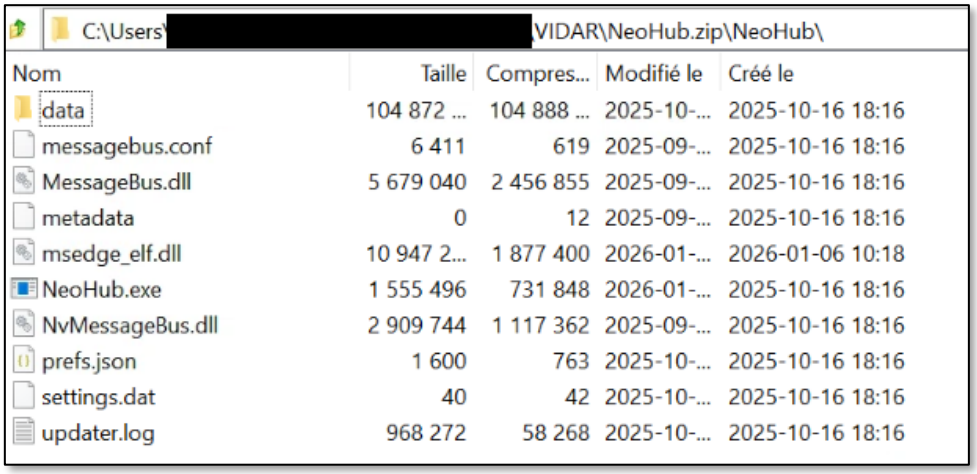


Figure 12: Content of the archive.

9 https://www.virustotal.com/gui/file/737cf993fb3e372a775378904012a88e5ae9cde437a713ec7e85f001994dca15

4.2 NeoHub.exe

Naturally, victims would first click on the file "**NeoHub.exe**" as it is an executable for what they could suspect is the program they are trying to install. By looking at it, we can notice that it imports two functions from the file "msedge_elf.dll" named "**GetInstallDetailsPayload**" and "**SignalInitializeCrashReporting**".

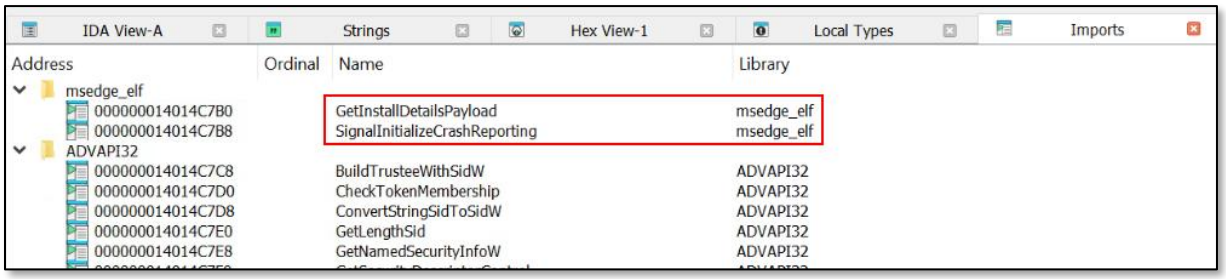


Figure 13: Imports of the malicious EXE.

The file "msedge_elf.dll"[10] is in fact detected on VirusTotal as a malicious Vidar sample. It masquerades as a legitimate DLL of the Microsoft Edge Browser, responsible for rendering and core functionalities[11].

[10] https://www.virustotal.com/gui/file/b21638e6dc0d08386d9ef2fe8f7a0e2dcfcdbbad5ab2cc7c2f773f4d96e9a3e4/relations

[11] https://www.dllme.com/dll/files/msedge_elf

4.3 Msedge_elf.dll

The file "msedge_elf.dll" is a 64-bit DLL of 10.44MB in size, compiled in GO.

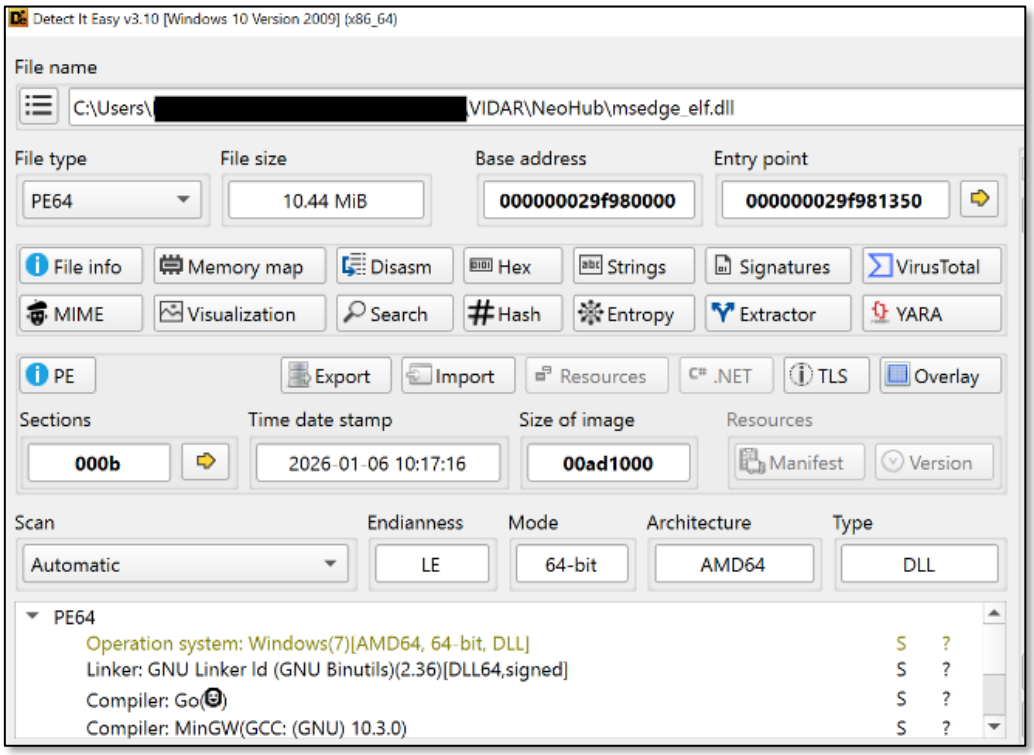


Figure 14: Details on the malicious DLL.

4.3.1 Fake certificate

The DLL was signed using a fake certificate named "**github.com**", masquerading as GitHub. The certificate was valid from 16 October 2025, which corresponds to the creation date of the files inside the downloaded archive.

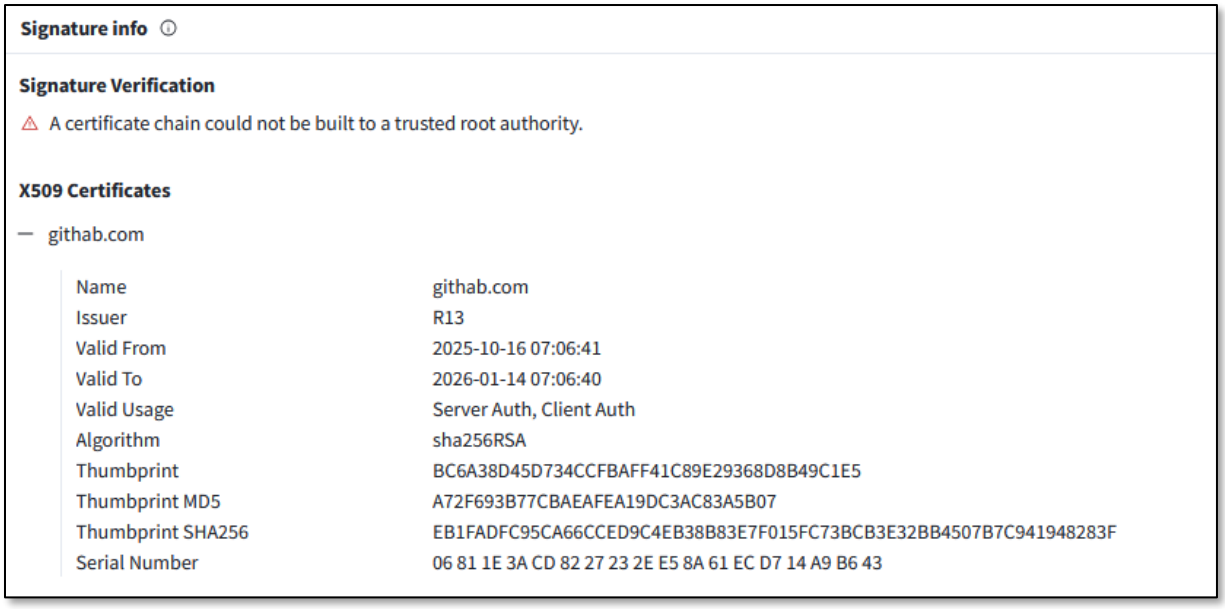


Figure 15: Fake certificate. Source: https://www.virustotal.com/gui/file/b21638e6dc0d08386d9ef2fe8f7a0e2dcfcdbbad5ab2cc7c2f773f4d96e9a3e4/details

The certificate's serial number "**06 81 1E 3A CD 82 27 23 2E E5 8A 61 EC D7 14 A9 B6 43**" is interesting as it is linked to many malicious files on VirusTotal, most of them being stealers (Vidar, Stealc). This could indicate that it is either used by a single threat actor or is a third-party fake certificate generation service used by various threat actors.

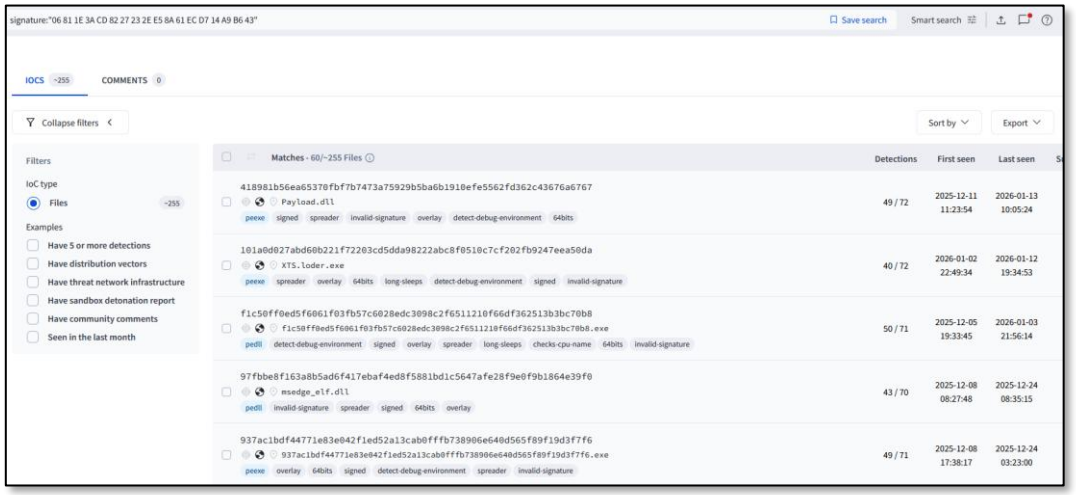


Figure 16: Malicious files sharing the same certificate. Source: https://www.virustotal.com/gui/search/signature%253A%252206%252081%25201E%25203A%2520CD%252082%252027%252023%25202E%2520E5%25208A%252061%2520EC%2520D7%252014%2520A9%2520B6%252043%2522?type=files

When we downloaded the file from Mediafire, the certificate was now changed to usurp "**grow.com**" with the serial number "**00 a0 c0 68 0c 19 15 30 8b 0d fa ab f8 f6 94 5f f3**".

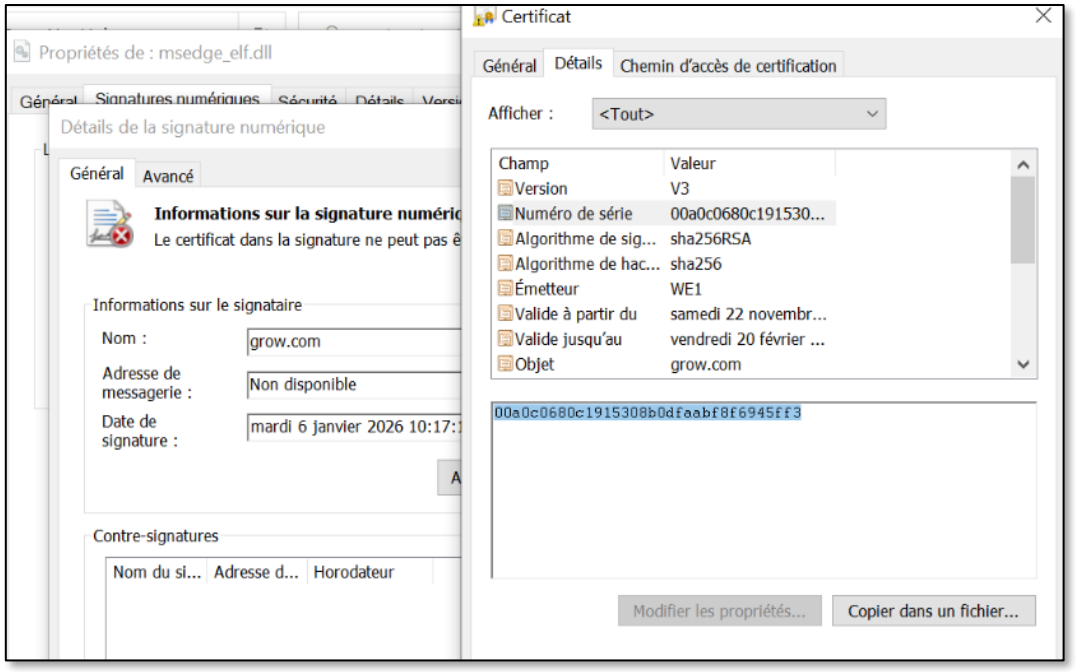


Figure 17: Another fake certificate.

This certificate is currently only linked to one other Vidar sample on VirusTotal[12].

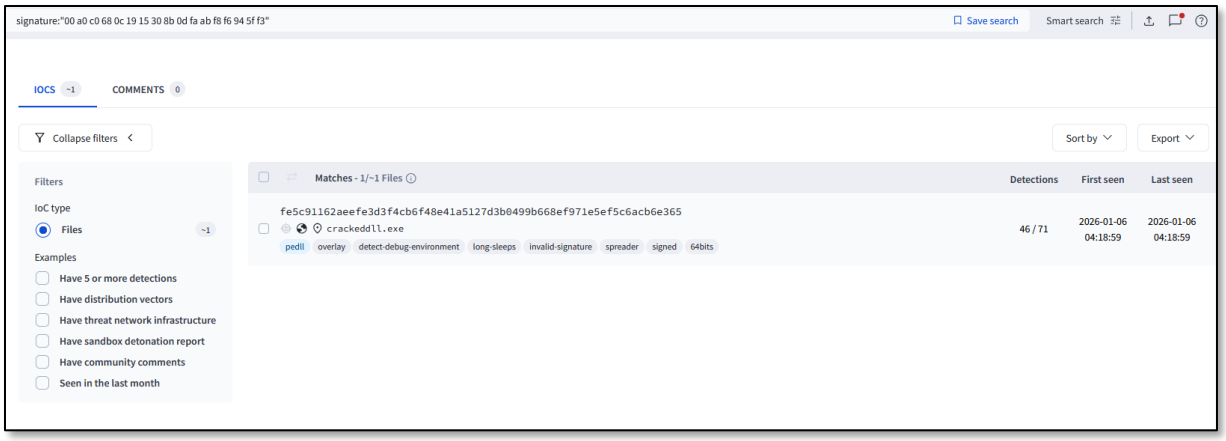


Figure 18: Malicious file sharing the same certificate. Source: https://www.virustotal.com/gui/search/signature%253A%252200%2520a0%2520c0%252068%25200c%252019%252015%252030%25208b%25200d%2520fa%2520ab%2520f8%2520f6%252094%25205f%2520f3%2522?type=files

12 https://www.virustotal.com/gui/file/fe5c91162aeefe3d3f4cb6f48e41a5127d3b0499b668ef971e5ef5c6acb6e365/relations

4.3.2 GO Packer

When viewing the details of the DLL, it appears that it is packed with a GO packer. The file has eight sections with unconventional names, which may suggest packing. The sections are: "**/4**", "**/19**", "**/31**", "**/45**", "**/57**", "**/70**", "**/81**", "**/92**". Some of the imports could also be linked to packer functionalities, such as "**LoadLibrary**", "**GetProcAddress**".

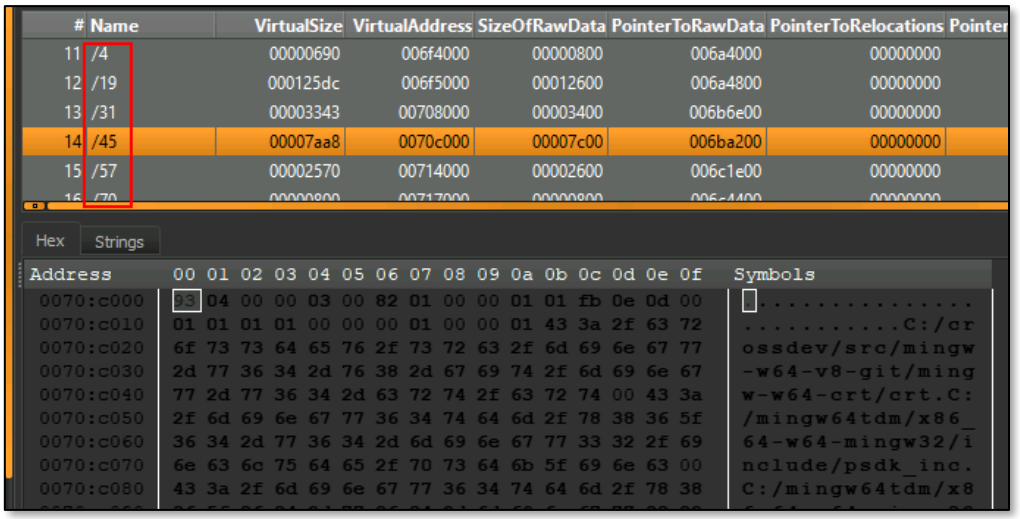


Figure 19: Unusual section names.

The entrypoint of the DLL is at the offset **F981350**, while the entrypoint of the calls from NeoHub.exe ("**GetInstallDetailsPayload**" and "**SignalInitializeCrashReporting**") are respectively at the offsets FC3FE30 and FC3FE70.

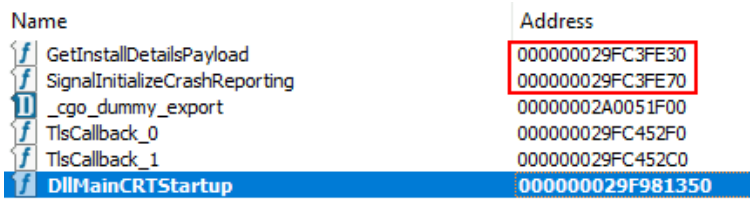
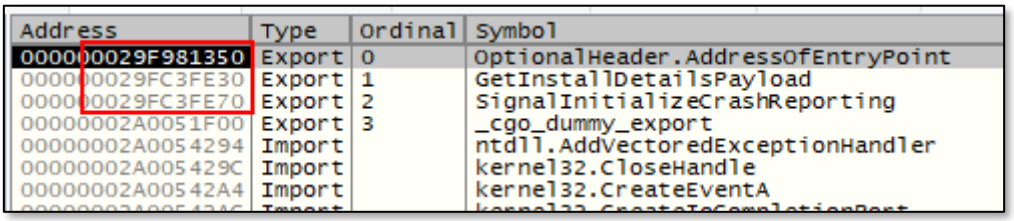


Figure 20: Address of the calls from NeoHub.exe.

For this analysis readability, we will not detail the debugging process that can be used to unpack the malware. However, we noted that analysts need to manually patch the file to get corresponding exports offset when using x64dbg so that the malware can be properly debugged. Deleting the "DLL characteristics" from the "optional header" is the way to go as exposed in this video by OALabs[13]. This is a problem specific when using the built-in loader from x64dbg, that can be circumvented using other means. Still, the packer functions

[13] https://www.youtube.com/watch?v=bkj8wSVEDR4

properly and the offsets are properly rendered when viewing them using IDA or PE bear for example.



Address	Type	Ordinal	Symbol
00000029F981350	Export	0	OptionalHeader.AddressOfEntryPoint
00000029FC3FE30	Export	1	GetInstallDetailsPayload
00000029FC3FE70	Export	2	SignalInitializeCrashReporting
00000002A0051F00	Export	3	_cgo_dummy_export
00000002A0054294	Import		ntdll.AddVectoredExceptionHandler
00000002A005429C	Import		kernel32.CloseHandle
00000002A00542A4	Import		kernel32.CreateEventA

Figure 21: Correcting the address' offset.

5. Vidar infrastructure

5.1 Current and old domains

Using DomainTools on the current main Vidar domain (vidars[.su), we were able to map some of the infrastructure composed of IP addresses and domain names. Most of this infrastructure was previously identified in our Acreed analysis[14], where we identified overlap between Vidar and Acreed infrastructures. Still, we were able to find additional IP addresses and domain names since then. Find below the details by IP addresses.

- 116.202.186[.230:
  - vidar[.su
  - vidas[.su
  - vidars[.su
  - tech-v[.top
  - v-new[.cloud
  - true-v[.top

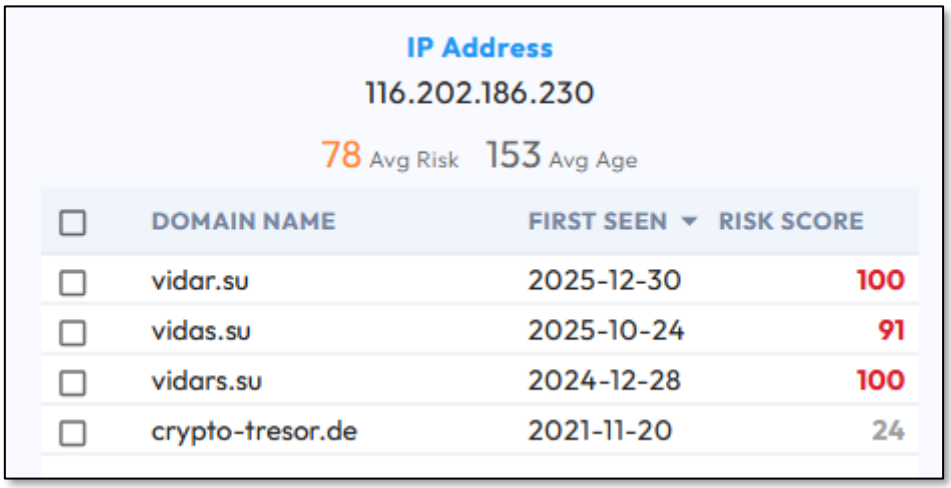
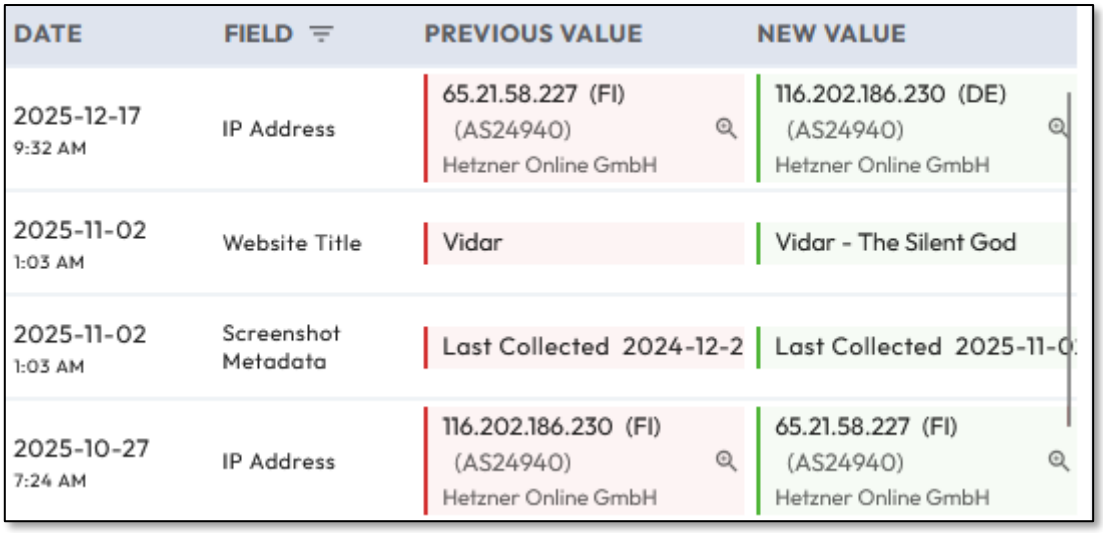


Figure 22: Vidar domains associated with the IP address.

- 65.21.58.227:
  - tech-v[.top
  - vidars[.su
  - SSH fingerprint: 33dcb98ec7bb3fba6171139cd8939049869d1c8ea04ee773afa60e400b9cbc68 -> links to 159.69.103[.251

[14] https://www.intrinsec.com/analysis-of-acreed-a-rising-infostealer/



DATE	FIELD	PREVIOUS VALUE	NEW VALUE
2025-12-17 9:32 AM	IP Address	65.21.58.227 (FI) (AS24940) Hetzner Online GmbH	116.202.186.230 (DE) (AS24940) Hetzner Online GmbH
2025-11-02 1:03 AM	Website Title	Vidar	Vidar - The Silent God
2025-11-02 1:03 AM	Screenshot Metadata	Last Collected 2024-12-2	Last Collected 2025-11-0
2025-10-27 7:24 AM	IP Address	116.202.186.230 (FI) (AS24940) Hetzner Online GmbH	65.21.58.227 (FI) (AS24940) Hetzner Online GmbH

Figure 23: Vidar domains associated with the IP address.

- 159.69.103[.251 :
  - tech-v[.top
  - Vidars[.su since 13 January 2026 https://www.virustotal.com/gui/ip-address/159.69.103.251/relations

- 65.109.242[.143:
  - vidars[.su
  - my-vidar[.ru
  - vidmn[.top
  - v-tamin[.lol

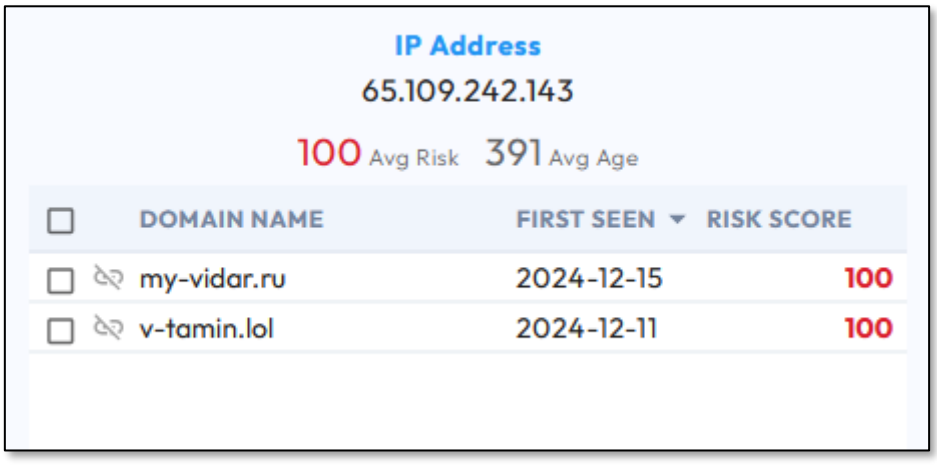
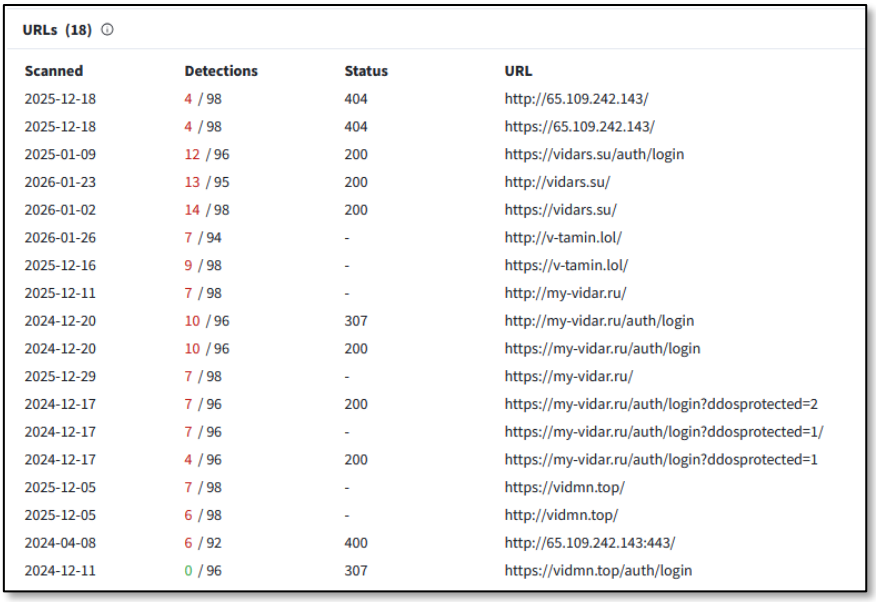


Figure 24: Vidar domains associated with the IP address.



URLs (18)

Scanned	Detections	Status	URL
2025-12-18	4 / 98	404	http://65.109.242.143/
2025-12-18	4 / 98	404	https://65.109.242.143/
2025-01-09	12 / 96	200	https://vidars.su/auth/login
2026-01-23	13 / 95	200	http://vidars.su/
2026-01-02	14 / 98	200	https://vidars.su/
2026-01-26	7 / 94	-	http://v-tamin.lol/
2025-12-16	9 / 98	-	https://v-tamin.lol/
2025-12-11	7 / 98	-	http://my-vidar.ru/
2024-12-20	10 / 96	307	http://my-vidar.ru/auth/login
2024-12-20	10 / 96	200	https://my-vidar.ru/auth/login
2025-12-29	7 / 98	-	https://my-vidar.ru/
2024-12-17	7 / 96	200	https://my-vidar.ru/auth/login?ddosprotected=2
2024-12-17	7 / 96	-	https://my-vidar.ru/auth/login?ddosprotected=1/
2024-12-17	4 / 96	200	https://my-vidar.ru/auth/login?ddosprotected=1
2025-12-05	7 / 98	-	https://vidmn.top/
2025-12-05	6 / 98	-	http://vidmn.top/
2024-04-08	6 / 92	400	http://65.109.242.143:443/
2024-12-11	0 / 96	307	https://vidmn.top/auth/login

Figure 25: Vidar domains associated with the IP address. Source: https://www.virustotal.com/gui/ip-address/65.109.242.143/relations

- 116.203.13[.215:
  - true-v[.top
  - v-new[.cloud
  - vidars[.su
- 95.216.181[.234
  - vidars[.su
- 95.217.233[.214
  - vidars[.su

Apart from the naming convention, we can confirm that the previously found domains are related to Vidar as they share a similar icon dhash.

v-tamin.lol 65.109.242.143 4.5.6.7	-	6 / 92	WEBCC	2024-12-11 19:03:32	2026-01-20 18:30:55	
v-new.cloud 216.120.147.200 116.202.186.230 116.203.13.215	-	16 / 92	-	2024-12-21 00:00:00	2025-12-21 00:00:00	
vidars.su 116.202.184.103 159.69.103.251 65.21.58.227 top-1M	-	13 / 92	-	2024-12-28 00:00:00	-	
vidar.su 116.202.184.103 178.156.164.66 116.202.186.230	-	9 / 92	-	2025-12-30 00:00:00	-	
vidar.cc 216.120.147.200 88.198.89.252 80.66.81.168	-	11 / 92	Web Commerce Commu...	2024-11-26 10:27:13	2025-11-27 08:05:25	

Figure 26: Vidar domains sharing the same icon dhash. Source: https://www.virustotal.com/gui/search/entity%253Adomain%2520main_icon_dhash%253A423c1c9938321008?type=domains

5.2 Additional infrastructure

Additionally, the email address denis[@otmail[.top is linked to three confirmed Vidar domains. This domain name otmail[.top appears to masquerade as "Hotmail" and is linked to the IP address 138[.199.168.93, associated with various domains usurping known email providers (Gmail, protonmail).

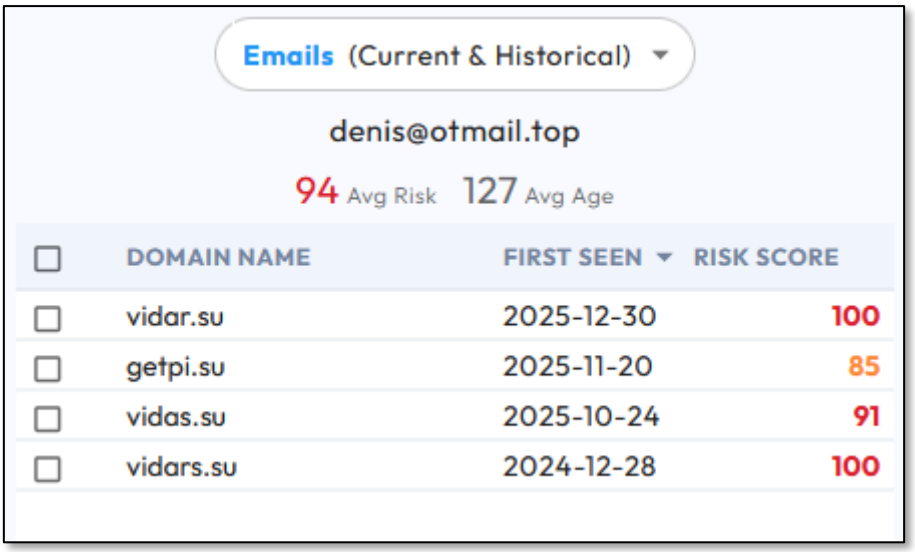


Figure 27: Vidar domains associated with the email address.

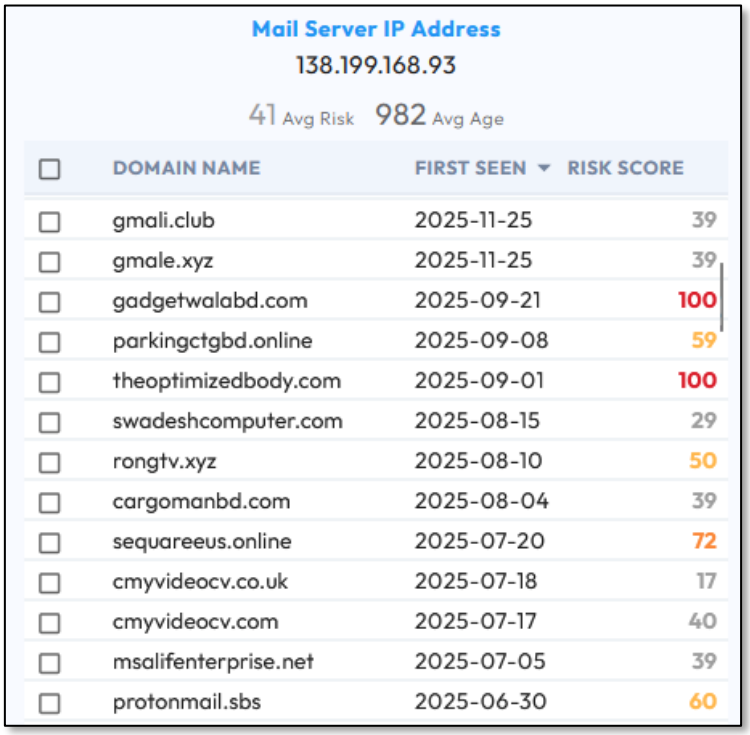


Figure 28: Domains associated with the IP address.

The domain getpi[.su does not evoke anything so we decide to further investigate it. On VirusTotal this domain returns nothing, but by using passive DNS tools, we can see that the subdomain v.getpi[.su was active.

Domain	Rank	Hosting Provider
getpi.su		-
v.getpi.su		Hosting technology LTD

Figure 29: Subdomain of getpi.

This subdomain was linked to the IP addresses 91[.142[.72[.234 and 213.159.75[.95.

v.getpi.su historical A data

A | AAAA

IP Addresses	Organization	First Seen	Last Seen	Duration Seen
91.142.72.234	Hosting technology LTD	2025-12-04 (2 months)	2026-01-29 (today)	2 months
213.159.75.95	Intercom LLC	2025-11-22 (2 months)	2025-12-04 (2 months)	12 days

Figure 30: IP addresses associated with the subdomain.

91.142.72[.234 is linked to some of the Vidar domains we previously encountered and the domains get-p[.buzz and mgt.bbproject[.ru as seen on VirusTotal[15].

[15] https://www.virustotal.com/gui/ip-address/91.142.72.234/relations

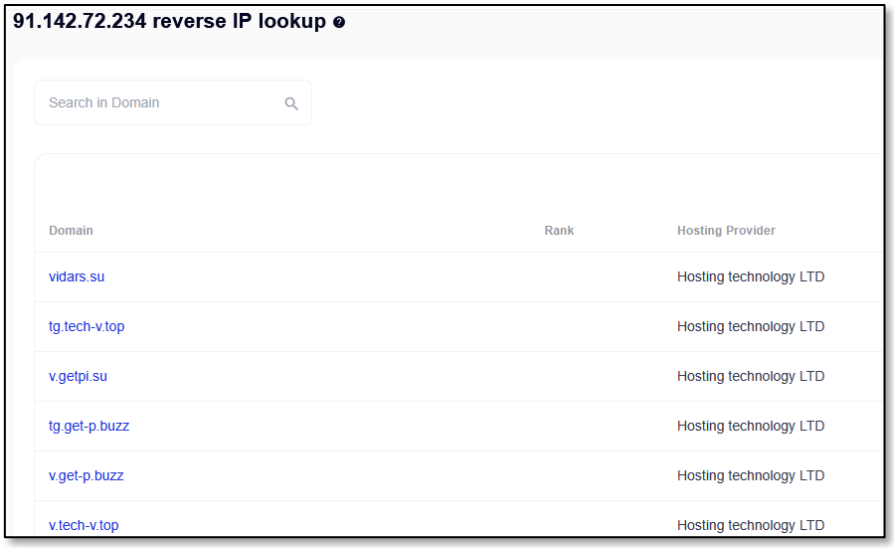


Figure 31: Vidar domains associated with the IP address.

213.159.75[.95 is also linked to some of the previously seen Vidar domains and the domain get-p[.buzz. We also saw this IP address in our Acreed analysis but at the time, it was only linked to the domains vidar[.su and true-v[.top. As such, we can suspect with high confidence that these two IP addresses are related to the infrastructure.

Passive DNS Replication (5)

Date resolved	Detections	Resolver	Domain
2025-12-03	0 / 93	VirusTotal	v.get-p.buzz
2024-12-11	9 / 93	Georgia Institute of Technology	vidar.su
2024-12-07	0 / 93	VirusTotal	v.true-v.top
2024-11-18	0 / 93	VirusTotal	v.getpacks.online
2024-11-13	0 / 93	VirusTotal	v.truedom.icu

URLs (9)

Scanned	Detections	Status	URL
2024-11-19	1 / 96	200	https://v.getpacks.online/
2024-11-19	1 / 96	200	http://v.getpacks.online/
2025-12-30	0 / 98	-	http://213.159.75.95/
2025-10-22	0 / 98	200	https://v.true-v.top/uFJrXt/builder?hash=443_d29f5f7c045713f2ddc1bb1b43faa920&download=1
2025-10-22	0 / 98	200	https://v.true-v.top/uFJrXt/builder?hash=443_d29f5f7c045713f2ddc1bb1b43faa920
2025-10-02	0 / 98	403	https://213.159.75.95/
2025-01-11	0 / 96	404	https://v.true-v.top/uFJrXt
2025-01-09	0 / 96	200	https://v.true-v.top/uFJrXt/profile?hash=2400_3d28ee12b525a340e0530024e89431c7

Figure 32: Vidar domains associated with the IP address. Source: https://www.virustotal.com/gui/ip-address/213.159.75.95/relations

Here is a graphic representation of the shared infrastructure.

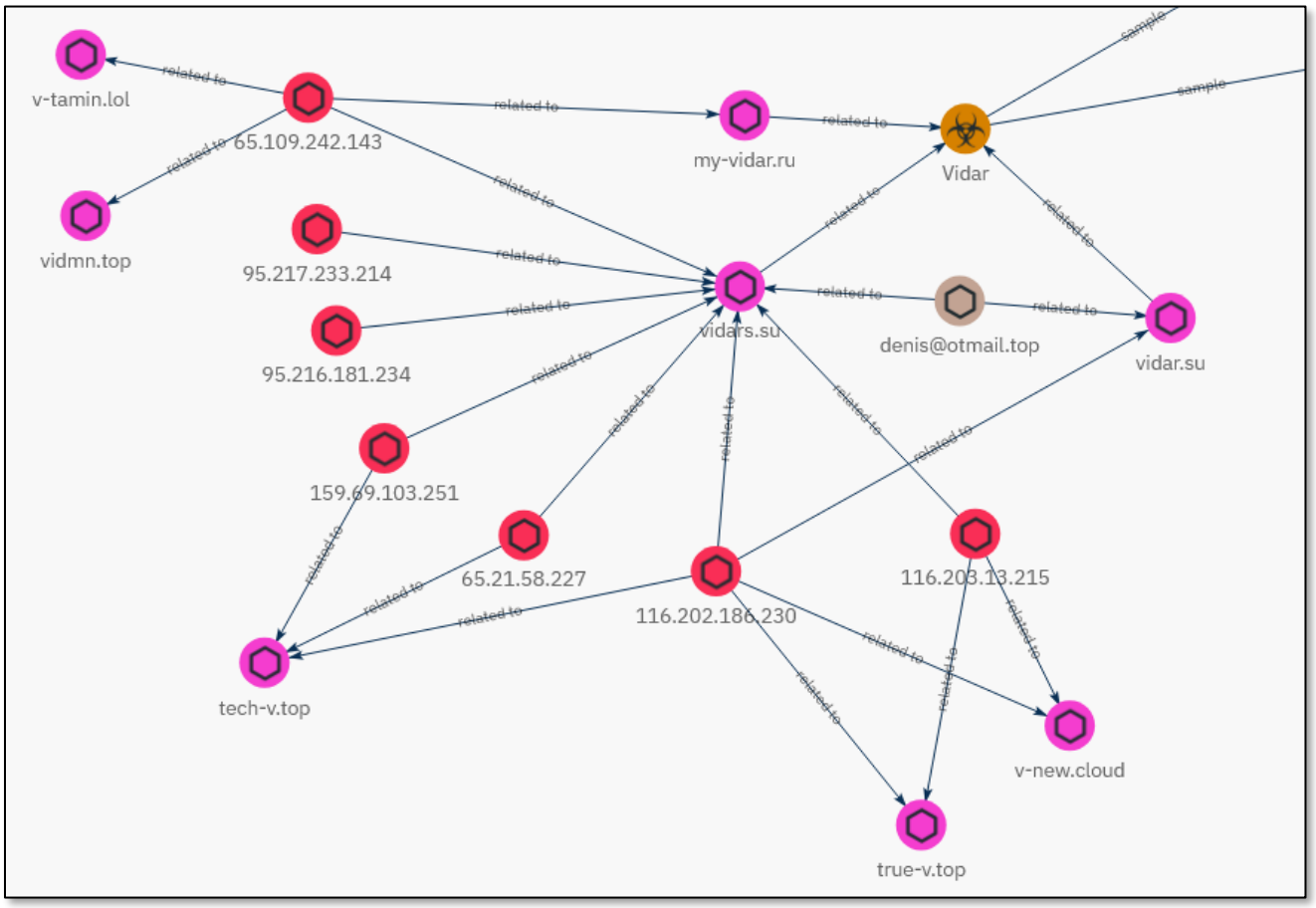


Figure 33: Schematic representation of the shared infrastructure.

5.3 Builder download

One user from Russia uploaded the content of a downloaded archive from one of the previously found domains (v.true-v[.top). The file "builder.zip" was downloaded from the URL

hxxps://v.true-v.top/uFJrXt/builder?hash=443_d29f5f7c045713f2ddc1bb1b43faa920&download=1

We can therefore suspect that the domains we previously exposed as related to the Vidar infrastructure are used by clients of the stealer for various purposes, including to build payloads.

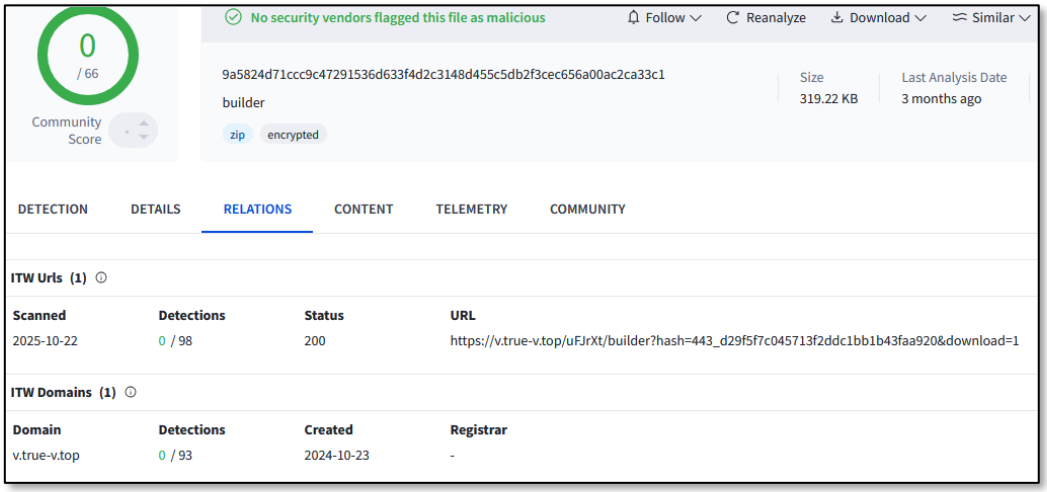


Figure 34: URL exposed on VirusTotal.

The archive's password was exposed in another URL (*SsGWEZIA*).

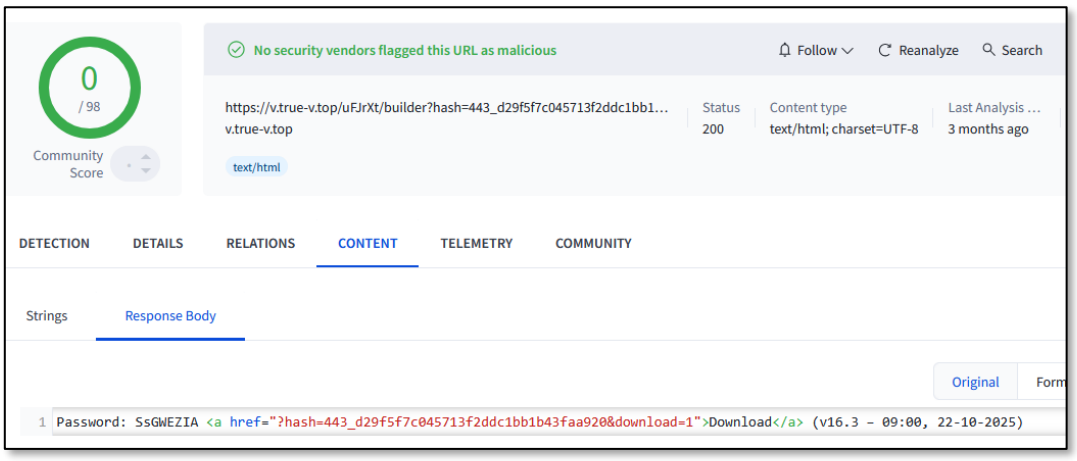


Figure 35: Content returned by the URL. Source: https://www.virustotal.com/gui/url/12af668e3b6428d03a392b14185ee95314784087417a97b2f8b15ed3c0e94c71/content/source

We can then extract the file using the provided password.

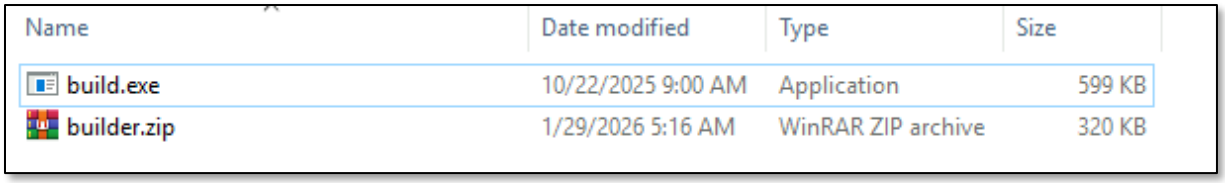


Figure 36: Extracting the content of the archive.

6. Vidar unpacked malware analysis

Interestingly, the sandbox analysis available on VirusTotal shows a warning message indicating that the malware should be packed to avoid detection. This message may be directed to threat actors that use the file for testing purposes.

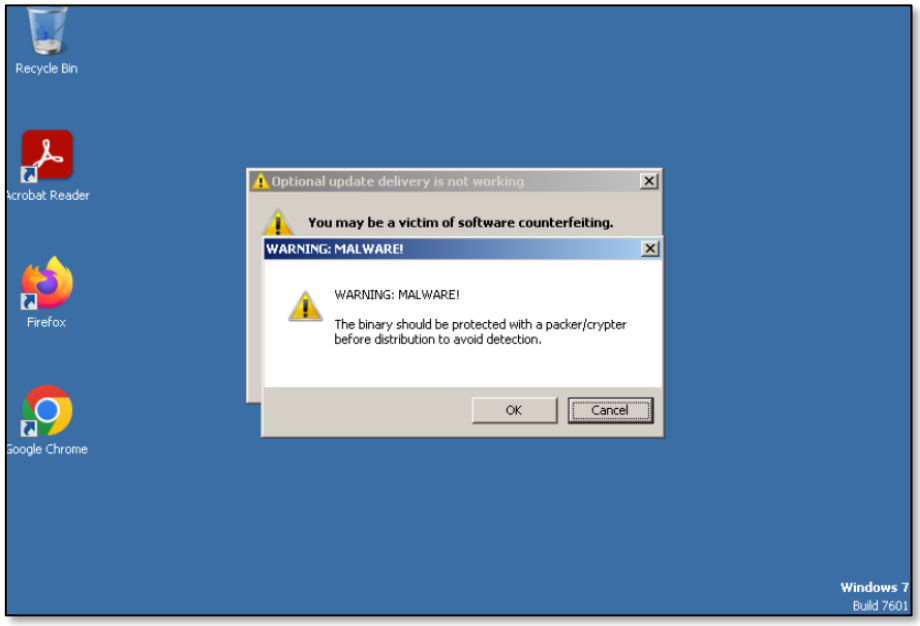


Figure 37: Message showed when executing the file. Source: https://www.virustotal.com/gui/file/03acfc321b897deee78c9a103e7921334fc97d9fdac944523ae3e95e5e867676/behavior

The malware is effectively not packed, but there is a lot of control flow flattening to slow-down analysis.

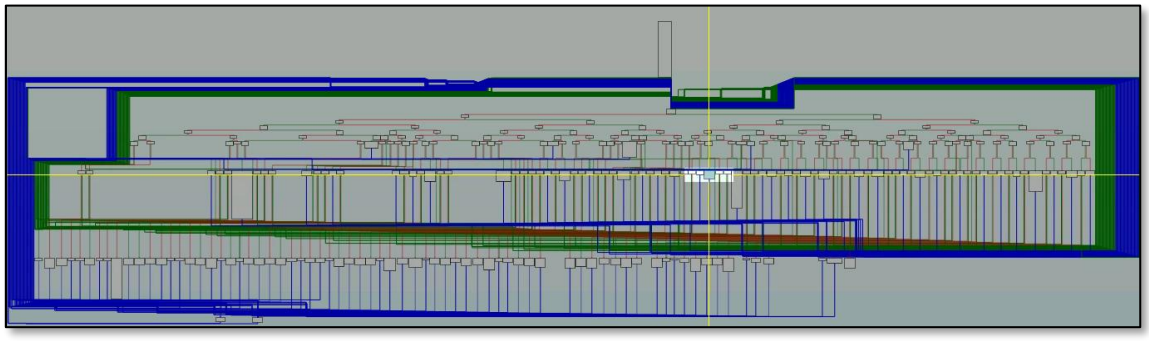


Figure 38: Control flow flattening.

Control Flow Flattening

Control Flow Flattening (CFF) is an advanced code obfuscation technique that transforms the natural hierarchical structure of a function's Control Flow Graph (CFG) into a flat, non-hierarchical state machine controlled by a single switch statement. This transformation

breaks the semantic relationship between basic blocks, making it extremely difficult to reconstruct the original program logic through static analysis.

6.1 Stealer capabilities

Vidar, just like other stealers, can target a variety of credentials stored internally, other browser files (history, credit cards, autofills) and cryptocurrency wallets. We identified the targeting of Chrome, Firefox, Edge, Opera, Vivaldi, Waterfox, Palemoon.

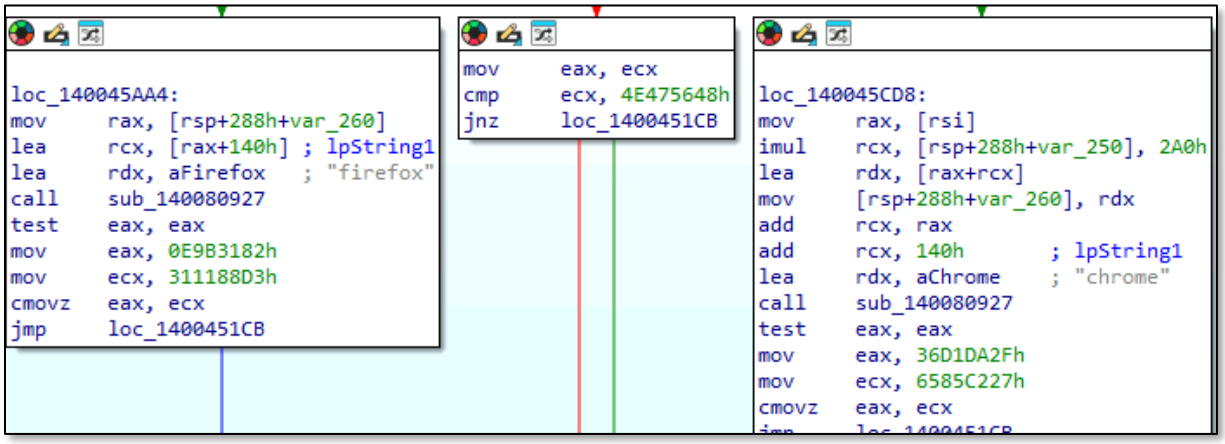


Figure 39: Targeting Web Browsers.

To steal credentials, it targets local files stores and decrypt them. For instance, concerning Firefox, it targets the file "key4.db".

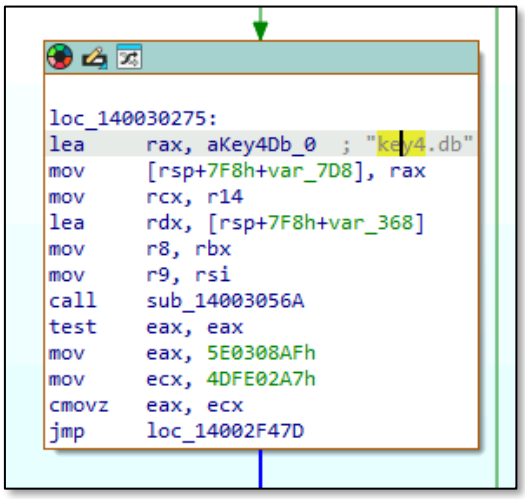


Figure 40: Targeting Firefox DB.

6.2 Dead Drop Resolver

Vidar is known for using dead drop resolvers to recover its C2 domain. This technique was previously documented in a Vidar analysis from 21 March 2025 by Aviab1[16].

Dead Drop Resolver

Adversaries may post content, known as a dead drop resolver, on Web services with embedded (and often obfuscated/encoded) domains or IP addresses. Once infected, victims will reach out to and be redirected by these resolvers. Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Use of a dead drop resolver may also protect back-end C2 infrastructure from discovery through malware binary analysis while also enabling operational resiliency (since this infrastructure may be dynamically changed).[17]

By reviewing various samples, we noticed that the Telegram and Steam dead drop resolvers were contacted by many samples and were regularly changed. For instance, this Steam profile[18], linked to "**wto.azl[.one**" and this Telegram channel[19], linked to "**wto.mir-massage[.kiev-ua**" are related to several hundred malicious files. As such, we suspect that this C2 mechanism is directly included and provided by Vidar, instead of being set up by individual threat actors. If this was the contrary, we would see more variety in how Vidar recovers and communicates with its C2. This potential centralization by Vidar's operators allows for a rapid C2 infrastructure rotation, a resilience against takedowns for individual threat actors, a reduced operator workload and consistent operational security.

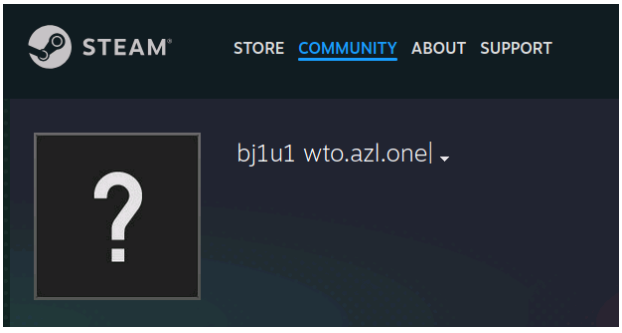


Figure 41: Steam dead drop resolver.

[16] https://aviab1.github.io/blog/vidar-stealer/

[17] https://attack.mitre.org/techniques/T1102/001/
[18] https://steamcommunity.com/profiles/76561198754004827
[19] https://t.me/g2trbox

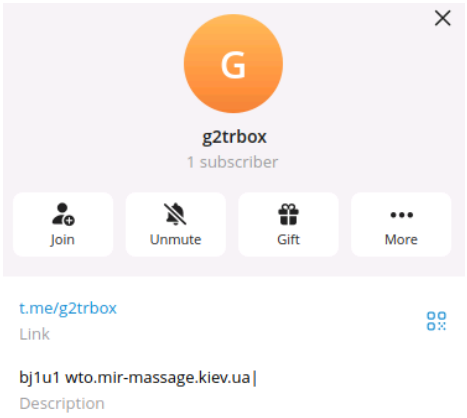


Figure 42: Telegram dead drop resolver.

In our sample, we identified the following Steam dead-drop resolver (*hxxps://steamcommunity.com/profiles/76561198777118079*) and Telegram (*hxxps://telegram.me/sre22qe*).

```
D8                dq 1Fh dup(0)
D0 aMozilla50Windo db 'Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:145.0) Gecko/2010010'
D0                                  ; DATA XREF: sub_1400124BA+238↓o
11                db '1 Firefox/145.0',0
21                align 8
28                dq 15h dup(0)
D0 aHttpsSteamcomm db 'https://steamcommunity.com/profiles/76561198777118079',0
D0                                  ; DATA XREF: sub_1400124BA+251↓o
06                align 8
08                dq 19h dup(0)
D0 aBM4_0         db 'b_m4',0       ; DATA XREF: sub_1400124BA+26A↓o
D5                align 8
D8                dq 1Fh dup(0)
D0 aMozilla50Windo_0 db 'Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:145.0) Gecko/2010010'
D0                                  ; DATA XREF: sub_1400124BA+283↓o
11                db '1 Firefox/145.0',0
```

Figure 43: Steam dead drop resolver hardcoded.

This dead drop is linked to the subdomain gz.technicalprorj[.xyz. It is associated with multiple malicious files on VirusTotal[20].

[20] https://www.virustotal.com/gui/domain/gz.technicalprorj.xyz/relations

Figure 44: Steam dead drop resolver.

The dead-drop resolves to the real C2 domain gpu.orca-trade[.com[21], associated with the IP address 78.47.238[.183[22].

[21] https://www.virustotal.com/gui/domain/gpu.orca-trade.com/relations
[22] https://www.virustotal.com/gui/ip-address/78.47.238.183

6.3 Browser extension ID

We identified that information related to crypto wallet extensions is Base64 encoded. The content below is decoded into "MetaMask", associated with its browser extension identifier.

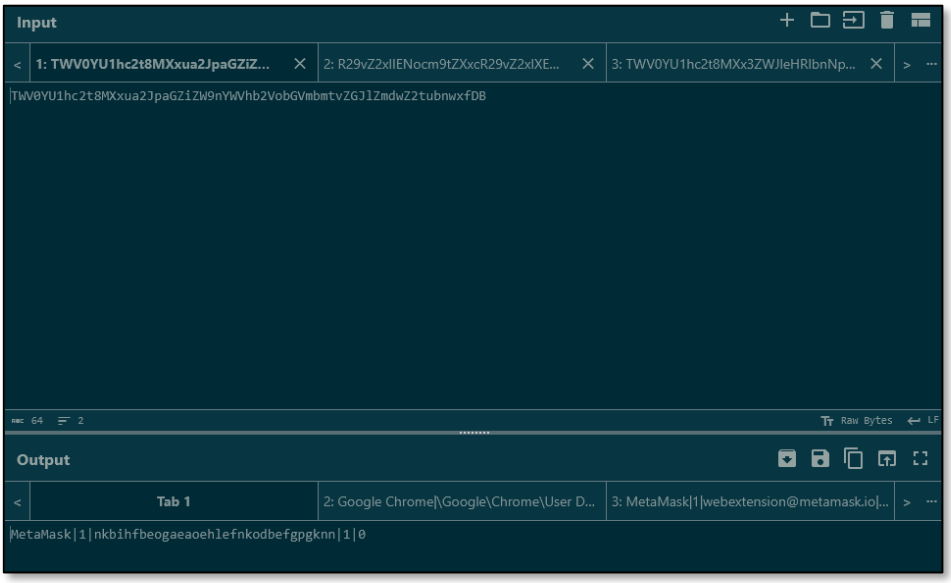
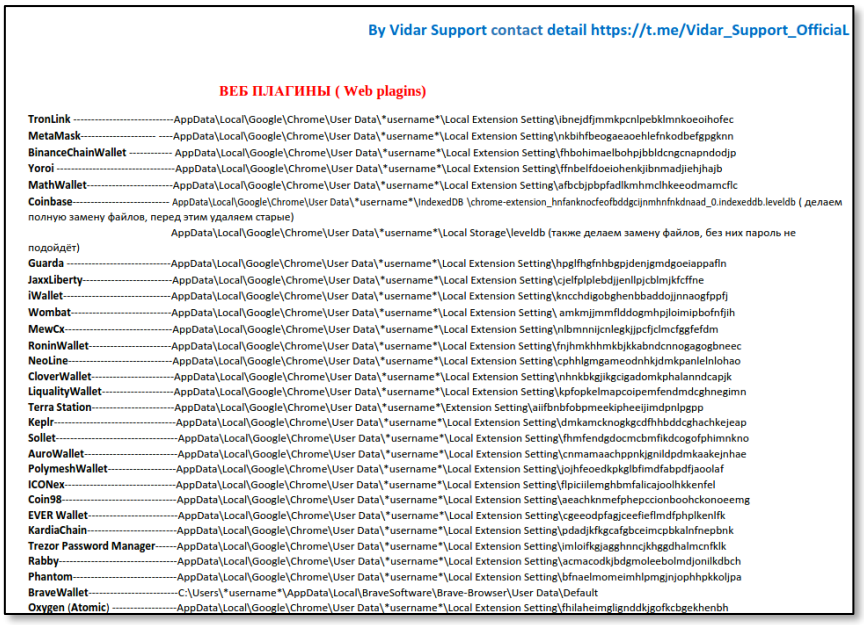


Figure 45: Targeting crypto browser extension.

Interestingly, a .pdf list of extension ID was found hosted on the domain vidars[.su. The file named "crypto_en.pdf" shows a list of paths of "*web plagins*" (i.e browser extensions) associated with cryptocurrency wallets.



By Vidar Support contact detail https://t.me/Vidar_Support_OfficiaL

ВЕБ ПЛАГИНЫ (Web plagins)

TronLink ----------AppData\Local\Google\Chrome\User Data*username*\Local Extension Setting\ibnejdfjmmkpcnlpebklmnkoeoihofec
MetaMask---------- ----AppData\Local\Google\Chrome\User Data*username*\Local Extension Setting\nkbihfbeogaeaoehlefnkodbefgpgknn
BinanceChainWallet ---------- AppData\Local\Google\Chrome\User Data*username*\Local Extension Setting\fhbohimaelbohpjbbldcngcnapndodjp
Yoroi ----------AppData\Local\Google\Chrome\User Data*username*\Local Extension Setting\ffnbelfdoeiohenkjibnmadjiehjhajb
MathWallet----------AppData\Local\Google\Chrome\User Data*username*\Local Extension Setting\afbcbjpbpfadlkmhmclhkeeodmamcflc
Coinbase---------- AppData\Local\Google\Chrome\User Data*username*\IndexedDB \chrome-extension_hnfanknocfeofbddgcijnmhnfnkdnaad_0.indexeddb.leveldb (делаем полную замену файлов, перед этим удаляем старые)
AppData\Local\Google\Chrome\User Data*username*\Local Storage\leveldb (также делаем замену файлов, без них пароль не подойдёт)
Guarda ----------AppData\Local\Google\Chrome\User Data*username*\Local Extension Setting\hpglfhgfnhbgpjdenjgmdgoeiappafln
JaxxLiberty----------AppData\Local\Google\Chrome\User Data*username*\Local Extension Setting\cjelfplplebdjjenllpjcblmjkfcffne
iWallet----------AppData\Local\Google\Chrome\User Data*username*\Local Extension Setting\kncchdigobghenbbaddojjnnaogfppfj
Wombat----------AppData\Local\Google\Chrome\User Data*username*\Local Extension Setting\ amkmjjmmflddogmhpjloimipbofnfjih
MewCx----------AppData\Local\Google\Chrome\User Data*username*\Local Extension Setting\nlbmnnijcnlegkjjpcfjclmcfggfefdm
RoninWallet----------AppData\Local\Google\Chrome\User Data*username*\Local Extension Setting\fnjhmkhhmkbjkkabndcnnogagogbneec
NeoLine----------AppData\Local\Google\Chrome\User Data*username*\Local Extension Setting\cphhlgmgameodnhkjdmkpanlelnlohao
CloverWallet----------AppData\Local\Google\Chrome\User Data*username*\Local Extension Setting\nhnkbkgjikgcigadomkphalanndcapjk
LiqualityWallet----------AppData\Local\Google\Chrome\User Data*username*\Local Extension Setting\kpfopkelmapcoipemfendmdcghnegimn
Terra Station----------AppData\Local\Google\Chrome\User Data*username*\Extension Setting\aiifbnbfobpmeekipheeijimdpnlpgpp
Keplr----------AppData\Local\Google\Chrome\User Data*username*\Local Extension Setting\dmkamcknogkgcdfhhbddcghachkejeap
Sollet----------AppData\Local\Google\Chrome\User Data*username*\Local Extension Setting\fhmfendgdocmcbmfikdcogofphimnkno
AuroWallet----------AppData\Local\Google\Chrome\User Data*username*\Local Extension Setting\cnmamaachppnkjgnildpdmkaakejnhae
PolymeshWallet----------AppData\Local\Google\Chrome\User Data*username*\Local Extension Setting\jojhfeoedkpkglbfimdfabpdfjaoolaf
ICONex----------AppData\Local\Google\Chrome\User Data*username*\Local Extension Setting\flpiciilemghbmfalicajoolhkkenfel
Coin98----------AppData\Local\Google\Chrome\User Data*username*\Local Extension Setting\aeachknmefphepccionboohckonoeemg
EVER Wallet----------AppData\Local\Google\Chrome\User Data*username*\Local Extension Setting\cgeeodpfagjceefieflmdfphplkenlfk
KardiaChain----------AppData\Local\Google\Chrome\User Data*username*\Local Extension Setting\pdadjkfkgcafgbceimcpbkalnfnepbnk
Trezor Password Manager----------AppData\Local\Google\Chrome\User Data*username*\Local Extension Setting\imloifkgjagghnncjkhggdhalmcnfklk
Rabby----------AppData\Local\Google\Chrome\User Data*username*\Local Extension Setting\acmacodkjbdgmoleebolmdjonilkdbch
Phantom----------AppData\Local\Google\Chrome\User Data*username*\Local Extension Setting\bfnaelmomeimhlpmgjnjophhpkkoljpa
BraveWallet----------C:\Users*username*\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default
Oxygen (Atomic) ----------AppData\Local\Google\Chrome\User Data*username*\Local Extension Setting\fhilaheimglignddkjgofkcbgekhenbh

Figure 46: Path to crypto wallets browser extensions.

7. Conclusion

"*Chaos is a ladder*", and Vidar successfully profited of the instability resulting from the takedowns of Lumma and Rhadamanthys, to rise to the top of the infostealer ecosystem. Despite being an old player in the market, we assess that this rise was made possible by the combination of multiple factors: the shakeout from international police operations; the development of the capabilities of the malware made visible by the release of Vidar 2.0; and the collaboration with known actors of the stealer ecosystem mainly in the form of "Cloud" Telegram channels.

The malware is weaponised by a variety of threat actors, either opportunistic individuals or threat groups (such as Scattered Spider). Due to the high volume of sample and indiscriminate campaigns targeting users worldwide, we can expect to continue seeing several compromise attempts against corporate networks using this malware. As such, enterprise should implement measures to protect against this threat and apply the recommendations found in this document.

8. Actionable content

8.1 Indicators of compromise

Value	Type	Description
chi.botick[.top	Domain-name	Vidar dead-drop resolver found on Steam
https://steamcommunity[.com/profiles/76561198761022496	URL	Chi.botick.top
https://steamcommunity.[com/profiles/76561198763098204	URL	Pre.automanpk.com
https://steamcommunity[.com/profiles/76561198754004827	URL	Wto.azl.one
Pre.automanpk[.com	Domain-name	Vidar dead-drop resolver found on Steam
wto.azl[.one	Domain-name	Vidar dead-drop resolver found on Steam
wto.mir-massage.kiev[.ua	Domain-name	Vidar dead-drop resolver found on Telegram
t[.me/g2trbox	URL	Telegram channel with dead-drop resolver in description
v-new[.cloud	Domain-name	Vidar infrastructure
Vidars[.su	Domain-name	Vidar infrastructure
my-vidar[.ru	Domain-name	Vidar infrastructure
Vidmn[.top	Domain-name	Vidar infrastructure
true-v[.top	Domain-name	Vidar infrastructure
v-tamin[.lol	Domain-name	Vidar infrastructure
Vidar[.su	Domain-name	Vidar infrastructure
tech-v[.top	Domain-name	Vidar infrastructure
Getpi[.su	Domain-name	Vidar infrastructure
get-p[.buzz	Domain-name	Vidar infrastructure
denis@otmail[.top	Email-Addr	Mail address used to register some Vidar domains
fe5c91162aeefe3d3f4cb6f48e41a5127d3b0499b668ef971e5ef5c6acb6e365	Sha-256	Vidar stealer
9a5824d71ccc9c47291536d633f4d2c3148d455c5db2f3cec656a00ac2ca33c1	Sha-256	Vidar build recovered from the C2 URL

b21638e6dc0d08386d9ef2fe8f7a0e2dcfcdbbad5ab2cc7c2f773f4d96e9a3e4	Sha-256	Fake msedge_elf.dll
a8dd417fdac8c47b8c4b0630c3dca337ce4f873cddfbe0d86576734a6bef545b	Sha-256	Vidar stealer
03acfc321b897deee78c9a103e7921334fc97d9fdac944523ae3e95e5e867676	Sha-256	Vidar stealer
116.203.13[.215	IPv4	Vidar infrastructure
65.21.58[.227	IPv4	Vidar infrastructure
159.69.103[.251	IPv4	Vidar infrastructure
95.217.233[.214	IPv4	Vidar infrastructure
213.159.75[.95	IPv4	Vidar infrastructure
116.202.186[.230	IPv4	Vidar infrastructure
91.142.72[.234	IPv4	Vidar infrastructure
193.233.198[.22	IPv4	Vidar C2
65.109.242[.143	IPv4	Vidar infrastructure
95.216.181[.234	IPv4	Vidar infrastructure
d586d192b0d5c050a03698753d9754ec0f5ce0b0791e0c2919a46284bf3b3c14	Sha-256	Grow[.com certificate hash
a72f693b77cbaeafea19dc3ac83a5b07	md5	githab[.com certificate hash
gpu.orca-trade[.com	Domain-Name	Vidar C2
hxxps://vidars[.su/files/instructions/cripto_en.pdf	URL	Instruction file

8.2 Recommendations

- **Block the IOCs** provided in the "Indicators of compromise" section of this analysis and subscribe to a CTI feed to obtain fresh IOCs related to stealer-malware and cracking websites. Intrinsec offers its own **CTI feed** to enhance your detection and response capabilities: https://www.intrinsec.com/en/cyber-threat-intelligence-feeds/
- **Regularly train employees** to recognize phishing attempts, especially those involving malicious attachments or suspicious links. Conduct internal phishing tests to assess and improve employee awareness.
- **Block suspicious URLs and domains:** Use firewall rules, Secure Web Gateways (SWG), and DNS filtering to block known malicious URLs, domains, and IP addresses associated with the ransomware's C2 infrastructure.
- **Implement file integrity monitoring**: Continuously monitor for unauthorized changes to critical files or system configurations.
- **Use advanced email security gateways** to detect and block phishing emails, particularly those containing malicious attachments or links.
- **Employ sandboxing solutions** to analyse email attachments and URLs before they reach users.
- **Enable multi-factor authentication** (MFA) for browser-related accounts to mitigate credential theft.
- **Set up network monitoring** to identify unusual or unauthorized outbound connections, particularly to known Command and Control (C2) servers.

8.3 Tactics, Techniques, and Procedures

ID	Tactic	Comment
T1566.001	Phishing: Spearphishing Attachment	Malicious archives disguised as legitimate software. Distribution via file-sharing platforms (MediaFire)
T1566.002	Phishing: Spearphishing Link	Social engineering via YouTube. Redirection chains through file-sharing services
T1189	Drive-by Compromise	Potential compromise through malicious advertisements. Fake software download pages
T1204.002	User Execution: Malicious File	User-initiated execution of NeoHub.exe. Requires user interaction to trigger infection chain
T1129	Shared Modules	Loading of malicious msedge_elf.dll. Exploitation of DLL search order
T1574.002	Hijack Execution Flow: DLL Side-Loading	Use of legitimate-appearing executable to load malicious DLL. Masquerading as Microsoft Edge component
T1027.002	Software Packing	GO-based packer with control-flow flattening
T1027.005	Indicator Removal from Tools	Polymorphic packer removes static signatures
T1027.009	Embedded Payloads	Payload embedded within oversized DLL
T1036.001	Invalid Code Signature	Fake certificates: github.com, grow.com
T1036.005	Match Legitimate Name or Location	msedge_elf.dll mimics Microsoft Edge DLL
T1036.008	Masquerade File Type	NeoHub installer masquerades as legitimate software
T1140	Deobfuscate/Decode Files or Information	Base64 encoding of exfiltrated data. Runtime unpacking of compressed payload
T1112	Modify Registry	Standard Vidar behavior for persistence
T1555.003	Credentials from Web Browsers	Chrome, Firefox, Edge, Opera credentials
T1555.005	Password Managers	Browser-integrated password managers
T1539	Steal Web Session Cookie	Extraction of session cookies for account hijacking. Targeting of authenticated sessions
T1552.001	Unsecured Credentials: Credentials In Files	Scanning for configuration files. Wallet files (cryptocurrency)
T1083	File and Directory Discovery	Enumeration of user directories. Targeting of specific file types
T1082	System Information Discovery	Collection of system metadata. Generation of information.txt file with system details
T1518.001	Security Software Discovery	Detection of AV/EDR for evasion
T1010	Application Window Discovery	Identification of running browser processes. Targeting of cryptocurrency wallet applications
T1217	Browser Information Discovery	Enumeration of installed browsers. Discovery of browser extensions (particularly crypto wallets like MetaMask)
T1005	Data from Local System	Credential databases, cryptocurrency wallets, configuration files
T1113	Screen Capture	Screenshot capability
T1114	Email Collection	Email client data theft
T1071.001	Application Layer Protocol: Web Protocols	HTTP-based C2 communication, GET and POST requests for data exfiltration
T1132.001	Data Encoding: Standard Encoding	Base64 encoding of stolen data, example: MetaMask extension data

T1568.003	DNS Calculation	Dead-drop resolver mechanism using Steam profiles and Telegram channels containing C2 domains
T1102.002	Bidirectional Communication	Steam Community dead-drop, Telegram dead-drop and log distribution
T1573	Encrypted Channel	HTTPS for some C2 communications, encryption of exfiltrated data
T1041	Exfiltration Over C2 Channel	Primary exfiltration mechanism, HTTP POST to C2 servers
T1020	Automated Exfiltration	Automated collection and transmission, no user interaction required post-infection
T1030	Data Transfer Size Limits	Chunked transmission of large data sets, optimized for stealth
T1565	Data Manipulation	Modification of system configurations. Potential clipboard manipulation for cryptocurrency theft

9. Sources

- https://www.trendmicro.com/en_us/research/25/j/how-vidar-stealer-2-upgrades-infostealer-capabilities.html
- https://www.ontinue.com/resource/blog-vidar-stealer-malware-analysis/
- https://www.broadcom.com/support/security-center/protection-bulletin/vidar-stealer-2-0
- https://securitylabs.datadoghq.com/articles/mut-4831-trojanized-npm-packages-vidar/
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a
- https://aviab1.github.io/blog/vidar-stealer/