Wireshark Tutorial: Examining Trickbot Infections

unit42.paloaltonetworks.com/wireshark-tutorial-examining-trickbot-infections/

Brad Duncan

November 8, 2019

By Brad Duncan

November 8, 2019 at 6:00 AM

Category: Malware, Tutorial, Unit 42

Tags: banking, infection, pcap, Trickbot, Wireshark, Wireshark Tutorial

<pre></pre>	-setup.pcap						
File Edit View Go C	apture Analyze	Sta	tistics Telephony Wirele	ss Tools Help			
	0 9 0 0		T 🕹 📃 🗏 Q, Q, C	. 璽			
http.request or ssl.handshake	type == 1					Expression	+
Time	Dst	Port	Host	Server Name	Info		^
2018-08-03 19:06:20	192.0.79.32	80	college.usatoday.com		GET /20	17/03/01/	
2018-08-03 19:06:20	192.0.78.19	443		r-login.wordpress.com	Client	Hello	
2018-08-03 19:06:20	192.0.78.19	443		r-login.wordpress.com	Client	Hello	
2018-08-03 19:06:20	192.0.77.32	443		s2.wp.com	Client	Hello	
2018-08-03 19:06:20	1 2.0.77 32	443	гор.	s2. p.com	Client	Hello	
2018-08-03 19:06:20	1 2.0.77 31	443	I U N	s2 p.com	Client	Hello	
2018-08-03 19:06: <u>20</u>	192.0.77.32	443		s2.wp.com	Client	Hello	
2018-08-03 19:06:20	192.0.77.32	443		s1.wp.com	Client	Hello	
2018-08-03 19:06:20	192.0.77.32	443		s1.wp.com	Client	Hello	
2018-08-03 19:06:20	192.0.77.32	443		s1.wp.com	Client	Hello	
2018-08-03 19:06:20	216.58.218	443		fonts.googleapis.com	Client	Hello	
2018-08-03 19:06:20	216.58.218	443		<pre>fonts.googleapis.com</pre>	Client	Hello	
2018-08-03 19:06:20	52.84.125	80	d15krst4gi8g86.clou		GET /cs	s/usatoda	
2018-08-03 19:06:20	52.84.125	80	d15krst4gi8g86.clou		GET /js	/script.j	
2018-02-03 10-06-20	52 8/ 125	80	d15kpet/digage clou		GET /ce	chucatoda	~~
🔵 🍸 traffic-for-wireshark-c	column-setup.pcap			Packets: 4448 · Displayed:	123 (2.8%)	Profile: Defa	ault

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

Executive Summary

When a host is infected or otherwise compromised, security professionals with access to packet captures (pcaps) of the network traffic need to understand the activity and identify the type of infection.

This tutorial offers tips on how to identify Trickbot, an information stealer and banking malware that has been <u>infecting victims since 2016</u>. Trickbot is distributed through malicious spam (malspam), and it is also distributed by other malware such as <u>Emotet</u>, <u>IcedID</u>, or <u>Ursnif</u>.

Trickbot has distinct traffic patterns. This tutorial reviews pcaps of Trickbot infections caused by two different methods: a Trickbot infection from malspam and Trickbot when it is distributed through other malware.

Note: Today's tutorial requires Wireshark with a column display customized according to <u>this</u> <u>previous tutorial</u>. You should already have implemented Wireshark display filters as described <u>here</u>.

Trickbot from malspam

Trickbot is often distributed through malspam. Emails from these campaigns contain links to download malicious files disguised as invoices or documents. These files may be Windows executable files for Trickbot, or they may be some sort of downloader for the Trickbot executable. In some cases, links from these emails return a zip archive that contains a Trickbot executable or downloader.

Figure 1 shows an example from September 2019. In this example, the email contained a link that returned a zip archive. The zip archive contained a Windows shortcut file that downloaded a Trickbot executable. A pcap for the associated Trickbot infection is available <u>here</u>.



Figure 1: Flowchart from a Trickbot infection from malspam in September 2019.

Download the pcap <u>from this page</u>. The pcap is contained in a password-protected zip archive named **2019-09-25-Trickbot-gtag-ono19-infection-traffic.pcap.zip**. Extract the pcap from the zip archive using the password **infected** and open it in Wireshark. Use your

basic filter to review the web-based infection traffic as shown in Figure 2.

			2019-09-25-Tric	kbot-gta	g-ono19-infection-traffic.pcap	• - • ×	
File	<u>E</u> dit <u>V</u> iew <u>G</u> o	<u>Capture</u>	Analyze Statistics Telep	hony <u>W</u>	/ireless <u>T</u> ools <u>H</u> elp		
		🗅 🛅 🔀) 🙆 🗟 🔹 📚 🏵	k			
📕 (h	(http.request or ssl.handshake.type == 1) and !(ssdp)						
Time			Dst	port	Host	Info	
+ 2	2019-09-25	17:53	198.70.69.144	80	www.msftncsi.com	GET /ncsi.txt HTTF	
2	2019-09-25	17:53	23.229.232.193	80	www.dchristjan.com	GET /dd05ce3a-a9cs	
2	2019-09-25	17:54	72.21.81.200	443	iecvlist.microsoft.com	Client Hello	
2	2019-09-25	17:54	72.21.81.200	443	iecvlist.microsoft.com	Client Hello	
2	2019-09-25	17:54	72.21.81.200	443	iecvlist.microsoft.com	Client Hello	
2	2019-09-25	17:54	72.21.81.200	443	r20swj13mr.microsoft.com	Client Hello	
2	2019-09-25	17:54	72.21.81.200	443	r20swj13mr.microsoft.com	Client Hello	
2	2019-09-25	17:54	144.91.69.195	80	144.91.69.195	GET /solar.php HT1	
2	2019-09-25	18:05	187.58.56.26	449		Client Hello	
2	2019-09-25	18:05	176.58.123.25	443	ident.me	Client Hello	
2	2019-09-25	18:05	104.124.58.155	80	www.download.windowsupdate	GET /msdownload/up	
2	2019-09-25	18:06	195.123.220.86	447		Client Hello	
2	2019-09-25	18:06	187.58.56.26	449		Client Hello	
2	2019-09-25	18:06	187.58.56.26	449		Client Hello	
2	2019-09-25	18:07	187.58.56.26	449		Client Hello	
2	2019-09-25	18:07	170.238.117.1	8082	170.238.117.187	POST /ono19/BACHMA	
2	2019-09-25	18:07	170.238.117.1	8082	170.238.117.187	POST /ono19/BACHMA	
2	2019-09-25	18:07	170.238.117.1	8082	170.238.117.187	POST /ono19/BACHM4	
4		10 07	103 50 50 00			••••••••	

Figure 2: Pcap of the Trickbot infection viewed in Wireshark.

Review the traffic, and you will find the following activity common in recent Trickbot infections:

- An IP address check by the infected Windows host
- HTTPS/SSL/TLS traffic over TCP ports 447 and 449
- HTTP traffic over TCP port 8082
- HTTP requests ending in .png that return Windows executable files

Unique to this Trickbot infection is an HTTP request to **www.dchristjan[.]com** that returned a zip archive and an HTTP request to **144.91.69[.]195** that returned a Windows executable file. Follow the HTTP stream for the request to **www.dchristjan[.]com** as shown in Figure 3 to review the traffic. In the HTTP stream, you will find indicators that a zip archive was returned as shown in Figure 4.

		2019-09-25-Trickbot-gtag-	ono19-infection-traffic.pcap	+ _ = ×				
<u>File Edit View Go</u>	apture	Analyze Statistics Telephony Wire	eless <u>T</u> ools <u>H</u> elp					
		S 🙆 🍓 💩 🏵 🕼 😫	💻 📃 🔍 २, २, 🗉					
(http.request or ssl.ha	(http.request or ssl.handshake.type == 1) and !(ssdp)							
Dst	port	Host	nfo	<u>^</u>				
198.70.69.144	80	www.msftncsi.com	GET /ncsi.txt H	ITTP/1.1				
23.229.232.193	80	www.dchristjan.com	GET /dd05ce3a-a	9c9-4018-8252-d579eed1e				
72.21.81.200	443	iecvlist.microsoft.com	Mark/Onmark Packet					
72.21.81.200	443	iecvlist.microsoft.com	Ignore/Unignore Packet					
72.21.81.200	443	iecvlist.microsoft.com	Set/Unset Time Reference					
72.21.81.200	443	r20swj13mr.microsoft.	Time Shift					
72.21.81.200	443	r20swj13mr.microsoft.	Packet Comment					
144.91.69.195	80	144.91.69.195	Edit Resolved Name	ITTP/1.1				
187.58.56.26	449		Apply as Filter					
176.58.123.25	443	ident.me	Apply as Filter					
104.124.58.155	80	www.download.windowsu	Prepare a Filter	update/v3/static/trust				
195.123.220.86	447		Conversation Filter					
187.58.56.26	449		Colorize Conversation					
187.58.56.26	449		SCTP					
187.58.56.26	449		Follow	TCP Stream				
170.238.117.1	8082	170.238.117.187	Сору	UDP Stream				
170.238.117.1	8082	1/0.238.117.187	Protocol Preferences	SSL Stream 1617601. AC				
1/0.238.11/.1	8082	1/0.230.11/.10/	Decode As	HTTP Stream				
4			Decode As					
			Show Packet in New Window					

Figure 3: Following the HTTP stream for the request to www.dchristjan[.]com.



Figure 4: Indicators the HTTP request returned a zip archive.

In Figure 4, you can also see the name of the file contained in the zip archive,

InvoiceAndStatement.Ink. You can export the zip archive from the traffic using Wireshark as shown in Figure 5 and Figure 6 using the following path:

 $\textit{File} \rightarrow \textit{Export Objects} \rightarrow \textit{HTTP}...$

	2019-09-	25-Tric	kbot-gt	tag-ono19-infection-traffic.pcap	• - D
e <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture	Analyze Statistics	Telep	hony	<u>W</u> ireless <u>T</u> ools <u>H</u> elp	
Open	Ctrl+O	2		al 🗔 🔲 🔍 Q. Q. 11	
Open Recent	,		-		
Merge		p)		Expressio	n + basic basic+ basic+d
Import from Hex Dump			port	Host	Info
Close	Ctrl+W	44	80	www.msftncsi.com	GET /ncsi.txt HTTF
Save	Ctrl+S	193	80	www.dchristjan.com	GET /dd05ce3a-a9c9
Save As	Ctrl+Shift+S	9	443	lecvlist.microsoft.com	Client Hello
Sile Cet	carronnero	9	443	iecvlist.microsoft.com	Client Hello
File Set	,	9	443	r20cwi12mr_microsoft_com	Client Hello
Export Specified Packets		2	443	r20swj13mr microsoft com	Client Hello
Export Packet Dissections	•	95	80	144 91 69 195	GET /solar php HT]
Export Packet Bytes	Ctrl+Shift+X	50	449	144.51.65.155	Client Hello
Export PDUs to File		25	443	j ∧∵∕ .me	Client Hello
Export SSL Session Keys		155	80	Hownload.windowsupdate.	GET /msdownload/up
Export Objects		D	ICOM		Client Hello
Print	Ctrl+P	H	ТТР		Client Hello
Ouit	Ctrl+O	IM	1F		Client Hello
Z019-09-50 T0.01"	101.30.30.2	s	ИΒ		Client Hello
2019-09-25 18:07	170.238.117	TE	TP	70.238.117.187	POST /ono19/BACHM/
2019-09-25 18:07	170.238.117	·	0002	70.238.117.187	POST /ono19/BACHM4
2019-09-25 18:07	170.238.117	.1	8082	2 170.238.117.187	POST /ono19/BACHM4
		-			· · · · · · · · · · · · · · · · · · ·

Figure 5: Exporting HTTP objects from the pcap.

Packet 🔻	Hostname	Content Type	Size	Filename	-
50	www.msftncsi.com	text/plain	14 bytes	ncsi.txt	
69	www.dchristjan.com	application/zip	3,546 bytes	dd05ce3a-a9c9-4	018-825
929	144.91.69.195	application/octet-stream	679 kB	solar.php	
1188	www.download.window	application/vnd.ms-cab	58 kB	authrootstl.cab	
3425	170.238.117.187	multipart/form-data	249 bytes	81	
3427	170.238.117.187	text/plain	3 bytes	81	
3442	170.238.117.187	multipart/form-data	348 bytes	83	
3444	170.238.117.187	text/plain	3 bytes	83	
3459	170.238.117.187	multipart/form-data	260 bytes	81	
3463	170.238.117.187	text/plain	3 bytes	81	
4510	170.238.117.187:8082	multipart/form-data	269 bytes	81	
4					

Figure 6: Exporting the zip archive from the pcap.

In a BSD, Linux, or Mac environment, you can easily confirm the extracted file is a zip archive, get the SHA256 hash of the file, and extract the contents of the archive in a command line environment. In this case, the content is a Windows shortcut file, which you can also confirm and get the SHA256 hash as shown in Figure 7.

The command to identify the file type is **file** *[filename]*, while the command to find the SHA256 hash of the file is **shasum -a 256** *[filename]*.



Figure 7: Checking the extracted zip archive and its contents.

An HTTP request to **144.91.69**[.]**195** returned a Windows executable file. This is the initial Windows executable for Trickbot. You can follow the HTTP stream for this HTTP request and find indicators this is an executable file as shown in Figure 8 and Figure 9. You can extract the executable file from the pcap as shown in Figure 10.

2019-09-25-Trick	bot-gtag-ono19-infection-traffic.pca	p ×					
<u>File Edit View Go Capture Analyze Statistics Telep</u>	hony <u>W</u> ireless <u>T</u> ools <u>H</u> elp						
🥖 🔳 🖉 🕲 🚞 🗎 🗙 🖉 🙇 🔹 🥸	k 😫 📃 🗐 🔍 Q, Q, 🏢						
(http.request or ssl.handshake.type == 1) and !(ssdp)							
Time Dst	port Host	Info					
2019-09-25 17:53 198.70.69.144 2019-09-25 17:53 23.229.232.193	80 www.msftncsi.com 80 www.dchristian.com	GET /ncsi.txt HTTF					
2019-09-25 17:54 72.21.81.200	443 iecylist.microsoft.	com Client Hello					
2019-09-25 17:54 72.21.81.200	443 iecvlist.microsoft.	com Client Hello					
2019-09-25 17:54 72.21.81.200	443 A list.microsoft.	com Client Hello					
2019-09-25 17:54 72.21.81.200	443 swj13mr.microsof	t.com Client Hello					
2019-09-25 17:54 72.21.81.200	443 swj13mr.microsof	t.com Client Hello					
 → 2019-09-25 17:54 144.91.69.195 2019-09-25 18:05 187.58.56.26 2019-09-25 18:05 176.58.123.25 2019-09-25 18:05 104.124.58.155 2019-09-25 18:06 195.123.220.86 2019-09-25 18:06 187.58.56.26 2019-09-25 18:07 187.58.56.26 2019-09-25 18:07 187.58.56.26 2019-09-25 18:07 170.238.117.1 2019-09-25 18:07 170.238.117.1 2019-09-25 18:07 170.238.117.1 	80 Mark/Unmark Packet 441 Ignore/Unignore Packet 80 Set/Unset Time Reference 441 Time Shift 442 Packet Comment 443 Edit Resolved Name 444 Apply as Filter 801 Prepare a Filter 802 Conversation Filter 804 Colorize Conversation	GET /solar.php HT1 Client Hello Client Hello supdate GET /msdownload/up Client Hello Client Hello Client Hello Client Hello POST /ono19/BACHM/ POST /ono19/BACHM/ POST /ono19/BACHM/					
	SCTP >						
	Follow	TCP Stream					
	Сору	UDP Stream					
	Protocol Preferences 🕨	SSL Stream					
	Decode <u>A</u> s	HTTP Stream					
	Show Packet in New Window						

Figure 8: Following the HTTP stream for the HTTP request to 144.91.69[.]195.

🧧 Wireshark · Follow HTTP Stream (tcp.stream eq	7) · 2019-09-25-Trickbot-gtag-ono19-infection-traffic.pcap 🔶 👝 🗉 🗙
GET /solar.php HTTP/1.1	*
Connection: Keep-Alive	
Accept: */*	
Accept-Language: en-us	
User-Agent: pwtyyEKzNtGatwnJjmCcBL	boveCVpc
Host: 144.91.69.195	Content type is
HTTP/1.1 200 OK	application/octet-stream
Server: nginx/1.10.3	
Date: Wed, 25 Sep 2019 17:54:12 GM	Eilo name listed in the
Content-Type: application/octet-st	ream File fiame insteu in the
Content-Length: 679008	HTTP response headers
Connection: keep-alive	that ends in eve
Content-Description: File Transfer	
Content-Disposition: attachment; f	ilename="phn34ycjtghm.exe"
Expires: 0	
Cache-Control: must-revalidate	
Pragma: public First 2 bytes of an	EXE or DLL show as ASCII characters MZ
MZ@@	
This program cannot be run in DOS	mode.
	g{.X.g{.{.b{z{.{.;
1 client pkt, 1 server pkt, 1 turn.	
Entire conversation (679 kB) 🔹	Show and save data as ASCII 👻
Find:	Find <u>N</u> ext
₩Help	Filter Out This Stream Print Save as Back X Close

Figure 9: Indicators the returned file is a Windows executable or DLL file.

a Edit View Go Canture	Analyze Statistics T	alanhany	Wireless Tools Holp			
Open	Ctrl+0		Wireless Tools Help Wireshark · E	xport · HTTP object list		+ - O
Open Recent	•	Packet	* Hostname	Content Type	N -	Filename
Merge	p)	50	www.msftncsi.com	text/plain	res	ncsi.txt
Import from Hex Dump		69	www.dchristian.com	application/zip	3.546 bytes	dd05ce3a-a9c9-
import nom nex bump	4	929	144.91.69.195	application/octet-stream	679 kB	solar.php
Close	Ctrl+W	1188	www.download.windowsupd	application/vnd.ms-cab-co	58 kB	authrootstl.cab
Save	Ctrl+S	3425	170.238.117.187	multipart/form-data	249 bytes	81
Savo As	Ctrl+Shift+S	3427	170.238.117.187	text/plain	3 bytes	81
5ave <u>A</u> 5	curronnero o	3442	170.238.117.187	multipart/form-data	348 bytes	83
File Set	► Ð	3444	170.238.117.187	text/plain	3 bytes	83
Export Specified Packets	Э	3459	170.238.117.187	text/plain	200 bytes	81
Sweet Backet Discostions	. 9	1510	170 238 117 187 8082	multinart/form-data	260 hutes	81
Export Packet Dissections	a l	4				
Export Packet Bytes	Ctrl+Shift+X	🛛 🔀 Help		Sav	ve All XC	lose Save
Export PDUs to File						
Export SSL Session Keys		5 443	download winds		deumland	1
Export SSE Session Reys	1	55 80	download.windd	owsupdate GET /ms	download	/ up
Export Objects	•	DICOM		Client	Hello	
Print	Ctrl+P	нттр		Client	Hello	
Quit	Ctrl+O	IME		Client	Hello	
2013-03-53 TO'01"	10/,00,00.2	CMD		Client	Hello	
2019-09-25 18:07	170,238,117	SMB	70, 238, 117, 187	POST /0	no19/BAC	HMA
2010-00-25 10:07	170 220 117	TFTP	70 220 117 107	POST /o	no10/PAC	LIM/
2019-09-25 18:07	470.230.117.	1	170.230.117.107	P051 /0	TOTA/ DAC	TIP/
2019-09-25 18:07	170.238.117.	1 8082	1/0.238.11/.18/	POST /0	HO19/BAC	HMA

Figure 10: Exporting the Windows executable from the pcap.

Post infection traffic initially consists of HTTPS/SSL/TLS traffic over TCP port 443, 447, or 449 and an IP address check by the infected Windows host. In this infection, shortly after the HTTP request for the Trickbot executable, we can see several attempted TCP connections over port 443 to different IP addresses before the successful TCP connection to 187.58.56[.]26 over TCP port 449. If you use your **basic+** filter, you can see these attempted connections as shown in Figure 11 and Figure 12.

	2019-09-25-Trickbot-g	gtag-ono19-infection-traffic.pc	ap 🔿 🖉 🖉
<u>File Edit View Go Capture An</u>	alyze <u>S</u> tatistics Telephon <u>y</u>	<u>W</u> ireless <u>T</u> ools <u>H</u> elp	
🥖 🔳 🖉 💿 💼 🛅 🗙 🛛	රි 🔍 🔹 📚 🚺	🗋 📃 🔍 Q, Q, I	
(http.request or ssl.handshake.typ	e == 1 or tcp.flags eq 0x0002	2) and !(ssdp)	Expression + basic basic+ basic+dns
Time	Dst	port Host	Info
2019-09-25 17:54:11	144.91.69.195	80 144.91.69.195	GET /solar.php HTTP/1.1
2019-09-25 17:55:51	185.222.202.222	443	49166 → 443 [SYN] Seq=0 Win
2019-09-25 17:55:54	185.222.202.222	443	[TCP Retransmission] 49166
2019-09-25 17:55:57	185.222.202.222	443	[TCP Retransmission] 49166
2019-09-25 17:56:23	185.222.202.222	443	49167 → 443 [SYN] Seq=0 Win
2019-09-25 17:56:26	185.222.202.222	443	[TCP Retransmission] 49167
2019-09-25 17:56:29	185.222.202.222	443	[TCP Retransmission] 49167
2019-09-25 17:56:55	185.222.202.222	443	49168 → 443 [SYN] Seq=0 Win
2019-09-25 17:56:58	185.222.202.222	443	[TCP Retransmission] 49168
2019-09-25 17:57:00	185.222.202.222	443	[TCP Retransmission] 49168
2019-09-25 17:57:27	31.184.253.37	443	49169 → 443 [SYN] Seq=0 Win
2019-09-25 17:57:30	31.184.253.37	443	[TCP Retransmission] 49169
2019-09-25 17:57:33	31.184.253.37	443	[TCP Retransmission] 49169
2019-09-25 17:57:59	31.184.253.37	443	49170 → 443 [SYN] Seq=0 Win
2019-09-25 17:58:02	31.184.253.37	443	[TCP Retransmission] 49170
2019-09-25 17:58:04	31.184.253.37	443	[TCP Retransmission] 49170
2019-09-25 17:58:30	31.184.253.37	443	49171 → 443 [SYN] Seq=0 Win
2019-09-25 17:58:33	31.184.253.37	443	[TCP Retransmission] 49171
2019-09-25 17:58:36	31.184.253.37	443	[TCP Retransmission] 49171
2019-09-25 17:59:03	51.254.69.244	443	49172 → 443 [SYN] Seq=0 Win
2019-09-25 17:59:06	51.254.69.244	443	[TCP Retransmission] 49172
2019-09-25 17:59:08	51.254.69.244	443	[TCP Retransmission] 49172
2019-09-25 17:59:35	51.254.69.244	443	49173 → 443 [SYN] Seq=0 Win
2019-09-25 17:59:38	51.254.69.244	443	[TCP Retransmission] 49173
2019-09-25 17·59·/1	51 254 69 244	1/13	[TCP Retransmission] 49173

Figure 11: Attempted TCP connections over port 443 by the infected Windows host.

	2019-09-25-Trickbot-g	gtag-ono19-infection-tra	affic.pcap	+ _ = ×
<u>File Edit View Go Capture An</u>	alyze <u>S</u> tatistics Telephon <u>y</u>	<u>W</u> ireless <u>T</u> ools <u>H</u> elp		
	õi 🗟 🌲 📚 🍓		€ 11	
(nttp.request or ssi.nandsnake.typ	e = 1 or tcp.nags eq 0x000.	2) and !(ssdp)	Expression + basic	basic+ basic+dns
Time	Dst	port Host	Info	^
2019-09-25 18:01:47	37.44.212.216	443	[TCP Retransmission	1 49177
2019-09-25 18:02:14	203.23.128.168	443	49178 → 443 [SYN] S	Seq=0
2019-09-25 18:02:17	203.23.128.168	443	[TCP Retransmission	1 491
2019-09-25 18:02:20	203.23.128.168	443	[ICP Retransmission	1] 49178
2019-09-25 18:02:46	203.23.128.168	443	49179 → 443 [SYN] S	21 401 70
2019-09-25 18:02:49	203.23.128.108	443	TCP Retransmission	1 49179
2019-09-25 18:02:52	203.23.120.100	443		
2019-09-25 18:03:19	203.23.128.108	445	TCP Retransmission	
2019-09-25 18:03:22	203.23.120.100	443	[TCP Retransmission	1 49180
2019-09-25 18:03:51	37 228 117 146	443	49181 → 443 [SVN] 9	Seq=0 Win
2019-09-25 18:03:54	37, 228, 117, 146	443	[TCP Retransmission	1 49181
2019-09-25 18:03:57	37.228.117.146	443	TCP Retransmission	1 49181
2019-09-25 18:04:23	37,228,117,146	443	49182 → 443 [SYN] S	Seg=0 Win
2019-09-25 18:04:26	37.228.117.146	443	[TCP Retransmission	1 49182
2019-09-25 18:04:28	37.228.117.146	443	[TCP Retransmission	1 49182
2019-09-25 18:04:55	37,228,117,146	443	49183 → 443 [SYN] S	Sea=0 Win
2019-09-25 18:04:58	37.228.117.146	443	[TCP Retransmission	n] 49183
2019-09-25 18:05:00	37.228.117.146	443	[TCP Retransmission	1 49183
2019-09-25 18:05:27	187.58.56.26	449	49184 → 449 [SYN] S	Seq=0 Win
2019-09-25 18:05:28	187.58.56.26	449	Client Hello	
2019-09-25 18:05:45	176.58.123.25	443	49185 → 443 [SYN] S	Seq=0 Win
2019-09-25 18:05:46	176.58.123.25	443 ident.me	Client Hello	
2019-09-25 18:05:53	104.124.58.155	80	49186 → 80 [SYN] S€	eq=0 Win=
2019-09-25 18:05:5/	10/ 12/ 58 155	80 www.downlo	GET /msdownload/und	ate/v3/c

Figure 12: Scrolling down to see more TCP connections over port 443 before a successful connection to 187.58.56[.]26 over TCP port 449.

The HTTPS/SSL/TLS traffic to various IP addresses over TCP port 447 and TCP port 449 has unusual certificate data. We can review the certificate issuer by filtering on *ssl.handshake.type* == 11 when using Wireshark 2.x or *tls.handshake.type* == 11 when using Wireshark 3.x. Then go to the frame details section and expand the information, finding your way to the certificate issuer data as seen in Figure 13 and Figure 14.

	2019-09-25-Trickbot-g	tag-ono19	-infection-	traffic.pd	сар				+ - = ×
<u>File Edit View Go Capture Analy</u>	ze <u>S</u> tatistics Telephon <u>y</u>	<u>W</u> ireless	<u>T</u> ools <u>H</u> elp						
🧧 🔳 🖉 💿 🗎 🗎 🏅	🗟 🄹 📚 🏖 🕼			Q. Q.]	•				
ssl.handshake.type == 11				×	Т. Б	pression	+ basi	ic basic+	basic+dns
Time	Src	port	Info						^
2019-09-25 17:54:10	72.21.81.200	443	Certifi	icate	[TCP	segment	of a	reasse	emble
2019-09-25 17:54:10	72.21.81.200	443	Certifi	icate	[TCP	segment	of a	reasse	emble
2019-09-25 17:54:11	72.21.81.200	\mathbf{N}	Certifi	icate	[ТСР	segment	of a	reasse	emble
2019-09-25 17:54:11	72.21.81.200		Certifi	icate	[ТСР	segment	of a	reasse	emble
2019-09-25 17:54:11	72.21.81.200	,43	Certifi	icate	[TCP	segment	of a	reasse	emble
2019-09-25 18:05:28	187.58.56.26	449	Server	Hello	, Cer	tificat	e, Ser	ver Ke	ey Exe
2019-09-25 18:05:46	176.58.123.25	443	Certifi	icate,	Serv	er Hell	o Done	•	
2019-09-25 18:06:03	195.123.220.86	447	Server	Hello	, Cer	tificat	e, Ser	ver Ke	ey Ex
2019-09-25 18:06:22	187.58.56.26	449	Server	Hello	, Cer	tificat	e, Ser	ver Ke	EV EX
 Frame 1000: 1370 bytes Ferret II, Src: Netgenet Protocol Vers Secure Sockets Layer TLSv1 Record Layer: TLSv1 Record Layer: Content Type: Hand 	gear_b6:93:f1 (2) sion 4, Src: 187 Protocol, Src Po Handshake Protoc Ishake (22)	0:e5:2a .58.56. rt: 449 col: Se col: Ce	rver He rtifica	f1), [: 10.9 Port: 4	ost: 1 9.25.: 19184,	Hewlett 101 , Seq: :	908 D1 P_1c:4	7:ae (: 96,	00:08:02 Len: 132
Version: TLS 1.0 (Length: 878 - Handshake Protocol Handshake Type: Length: 874 Certificates Len	0x0301) .: Certificate Certificate (11) gth: 871	-							
- Certificates (87	1 bytes) 🛑								

Figure 13: Filtering for the certificate data in the HTTPS/SSL/TLS traffic, then expanding lines the frame details for the first result under TCP port 449.



Figure 14: Drilling down to the certificate issuer data on the first result over TCP port 449.

In Figure 14, we see the following certificate issuer data used in HTTPS/SSL/TLS traffic to 187.58.56[.]26 over TCP port 449:

- id-at-countryName=AU
- id-at-stateOrProvinceName=Some-State
- id-at-organizationName=Internet Widgits Pty Ltd

The state or province name (Some-State) and the organization name (Internet Widgits Pty Ltd) are not used for legitimate HTTPS/SSL/TLS traffic. This is an indicator of malicious traffic, and this type of unusual certificate issuer data is not limited to Trickbot. What does a normal certificate issuer look like in legitimate HTTPS/SSL/TLS traffic? If we look at earlier traffic to Microsoft domains at 72.21.81.200 over TCP port 443, we find the following as seen in Figure 15.

- id-at-countryName=US
- id-at-stateOrProvinceName=Washington
- id-at-localityName=Redmond
- id-at-organizationName=*Microsoft Corporation*
- id-at-organizationUnitName=Microsoft IT
- id-at-commonName=Microsoft IT TLS CA 2

	2019-09-25-Trickbot-gtag-ono19-infection-traffic.pcap 🔶 👝 🗉 🗙
<u>F</u> ile <u>E</u>	dit <u>V</u> iew <u>Go</u> <u>Capture</u> <u>A</u> nalyze <u>S</u> tatistics Telephony <u>W</u> ireless <u>T</u> ools <u>H</u> elp
	I 🖉 🐵 💼 🖺 🔀 🖾 🔹 🖢 🧏 🜬 🚽 🔜 🗐 🔍 Q Q 🎹
📕 ssl.h	handshake.type == 11 Expression + basic basic+ basic+dns
Time	Src port Info
20	019-09-25 17:54:11 72.21.81.200 443 Certificate [TCP segment of a reassemble
1 20	10_00_25 17:51:11 72 21 21 200 112 Cartificate [TCD segment of a reassemble]
	- Certificates (6599 bytes)
	Certificate Length: 4235
	- Certificate: 3082108730820e6fa003020102021320000270cc6d25336c (id-at-commonNam
	signedCertificate
	version: v3 (2)
	serialNumber: 0x20000270cc6d25336ca081b3590000000270cc
	 signature (sha256WithRSAEncryption)
	<pre>- issuer: rdnSequence (0)</pre>
	rdnSequence: 6 items (id-at-commonName=Microsoft IT TLS CA 2 id-at-organizat
	DNSequence item: 1 item (id-at-countryName=US)
	DNSequence item: 1 item (id-at-stateOrProvinceName=Washington)
	RDNSequence item: 1 item (id-at-localityName=Redmond)
	DNSequence item: 1 item (id-at-organizationName=Microsoft Corporation)
	DNSequence item: 1 item (id-at-organizationalUnitName=Microsoft IT)
	RDNSequence item: 1 item (id-at-commonName=Microsoft IT TLS CA 2)
	validity
4	subject: rdnSequence (0)

Figure 15: Certificate data from legitimate HTTPS traffic to a Microsoft domain.

The Trickbot-infected Windows host will check its IP address using a number of different IP address checking sites. These sites are *not* malicious, and the traffic is not inherently malicious. However, this type of IP address check is common with Trickbot and other families of malware. Various legitimate IP address checking services used by Trickbot include:

- api.ip[.]sb
- checkip.amazonaws[.]com
- icanhazip[.]com
- ident[.]me
- ip.anysrc[.]net
- ipecho[.]net
- ipinfo[.]io
- myexternalip[.]com
- wtfismyip[.]com

Again, an IP address check by itself is not malicious. However, this type of activity combined with other network traffic can provide indicators of an infection, like we see in this case.

	2019-09-25-Trickbot	-gtag-o	no19-infection-traffic.pcap	+ - • X
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> na	alyze <u>S</u> tatistics Telephon	<u>w</u> irel	ess <u>T</u> ools <u>H</u> elp	
	🔇 🗟 🌒 🕸 🚺		_ • • • •	
(http.request or ssl.handshake.typ	e == 1) and !(ssdp)		X 🗆 🔹	Expression + basic basic+ basic+dns
Time	Dst	port	Host	Info Add an expression to the display filter.
+ 2019-09-25 17:53:38	198.70.69.144	80	www.msftncsi.com	GET /ncsi.txt HTTP/1.1
2019-09-25 17:53:41	23.229.232.193	80	www.dchristjan.c…	GET /dd05ce3a-a9c9-4018-8
2019-09-25 17:54:10	72.21.81.200	443	iecvlist.microso…	Client Hello
2019-09-25 17:54:10	72.21.81.200	443	iecvlist.microso…	Client Hello
2019-09-25 17:54:10	72.21.81.200	443	iecvlist.microso…	Client Hello
2019-09-25 17:54:11	72.21.81.200	443	r20swj13mr.micro…	Client Hello
2019-09-25 17:54:11	72.21.81.200	443	r20swj13mr.micro…	Client Hello
2019-09-25 17:54:11	144.91.69.195	80	144.91.69.195	GET /solar.php HTTP/1.1
2019-09-25 18:05:28	187,58,56,26	449		Client Hello
2019-09-25 18:05:46	176.58.123.25	443	ident.me	Client Hello
2019-09-25 18:05:54	104.124.58.155	80	www.download.win	GET /msdownload/update/v3
2019-09-25 18:06:02	195.123.220.86	447		Client Hello
2019-09-25 18:06:22	187.58.56.26	449		Client Hello
2019-09-25 18:06:24	187.58.56.26	449		Client Hello
2019-09-25 18:07:19	187.58.56.26	449		Client Hello
Erame 46: 151 bytes	on wire (1208 hi	ts)	151 bytes cantured	(1208 hits) *
Ethernet II Src: He	wlettp 1c:47:20	(00.0	(32)	(1200 bits)
Internet Protocol Ve	rsion 4 Src: 16	9 25	101 Dst 198 70	69 144
Transmission Control	Drotocol Src D	ort.	10157 Det Dort 9	9 Seg. 1 Ack. 1 Len. 97 *
4				Þ

Figure 16: IP address check by the infected Windows host, right after HTTPS/SSL/TLS traffic over TCP port 449. Not inherently malicious, but this is part of a Trickbot infection.

A Trickbot infection currently generates HTTP traffic over TCP port 8082 this traffic sends information from the infected host like system information and passwords from the browser cache and email clients. This information is sent from the infected host to command and control servers used by Trickbot.

To review this traffic, use the following Wireshark filter:

http.request and tcp.port eq 8082

This reveals the following HTTP requests as seen in Figure 17:

- 170.238.117[.]187 port 8082 170.238.117[.]187 POST /ono19/BACHMANN-BTO-PC_W617601.AC3B679F4A22738281E6D7B0C5946 E42/81/
- 170.238.117[.]187 port 8082 170.238.117[.]187 POST /ono19/BACHMANN-BTO-PC_W617601.AC3B679F4A22738281E6D7B0C5946 E42/83/
- 170.238.117[.]187 port 8082 170.238.117[.]187 POST /ono19/BACHMANN-BTO-PC_W617601.AC3B679F4A22738281E6D7B0C5946 E42/81/
- 170.238.117[.]187 port 8082 170.238.117[.]187:8082 POST /ono19/BACHMANN-BTO-PC_W617601.AC3B679F4A22738281E6D7B0C5946 E42/81/

- 170.238.117[.]187 port 8082 170.238.117[.]187:8082 POST /ono19/BACHMANN-BTO-PC_W617601.AC3B679F4A22738281E6D7B0C5946 E42/90
- 170.238.117[.]187 port 8082 170.238.117[.]187:8082 POST /ono19/BACHMANN-BTO-PC_W617601.AC3B679F4A22738281E6D7B0C5946 E42/90

	2019-09-2	5-Trickbot-gtag-ono19-infection-traff	fic.pcap	
<u>File Edit View Go</u>	Capture Analyze Statistics	s Telephony Wireless Tools Help	ə T	
http.regu	est and tcp.port	eg 8082		
Time	Det	nort Hert	Expression + basic basic+ basic+	dns
+ 2019-09-25	18:07 170.238.117	7.187 8082 170.238.117.18	7 POST /ono19/BACHMANN-BTO-	PC_I
2019-09-25	18:07 170.238.117	7.187 8082 170.238.117.18	7 POST /ono19/BACHMANN-BTO-	
2019-09-25	18:08 170.238.117	7.187 8082 170.238.117.18	7:8082 POST /ono19/BACHMANN-BTO-	PC_I
2019-09-25	18:09 170.238.117	7.187 8082 170.238.117.18	7:8082 POST /ono19/BACHMANN-BTO-	PC_1
2019-09-25	18:20 170.238.117	7.187 8082 170.238.117.18	7:8082 POST /ono19/BACHMANN-BTO-	PC_I
				Þ

Figure 17: HTTP traffic over TCP port 8082 caused by Trickbot.

HTTP POST requests ending in 81 send cached password data from web browsers, email clients, and other applications. HTTP POST requests ending in 83 send form data submitted by applications like web browsers. We can find system information sent through HTTP POST requests ending in 90. Follow the TCP or HTTP streams for any of these HTTP POST requests to review data stolen by this infection.

Wireshark · Follow TCP Stream (tcp.stream eq 33) · 2019-09-25-Trickbot-gtag-ono19-infection-traffic.pcap	+ - • ×
POST /ono19/BACHMANN-BTO-PC_W617601.AC3B679F4A22738281E6D7B0C5946E42/81/ HTTP/1. Accept: */*	1
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Tride 7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Ce PC 6.0; .NET4.0C; .NET4.0E)	ent/ enter
Host: 170.238.117.187	
Content-Type: multipart/form-data: boundary=KMOGEEOTLOTCOMYE	
Content-Length: 249	
KMOGEEQTLQTCQMYE	
Content-Disposition: form-data; name="data"	
https://nytimes.com/ randybachman P@ssw0rd\$ - Website, username, a	and
KMOGEEQTLQTCQMYE DASSWORD	
Content-Disposition: form-data; name="source"	
chrome passwords Chrome passwords	
HTTP/1.1 200 OK	
server: Cowboy	
date: Wed, 25 Sep 2019 18:07:26 GMT	
content-length: 3	
Content-Type: text/plain	
/1/	-
2 client pkts, 1 server pkt, 1 turn.	
Entire conversation (817 bytes) Show and save data as ASCII	im 33 🌲
Find:	Find <u>N</u> ext
Filter Out This Stream Print Save as Back	X <u>C</u> lose

Figure 18: Login credentials stolen by Trickbot from the Chrome web browser. This data was sent by the Trickbot-infected host using HTTP traffic over TCP port 8082.

🚄 💿 Wireshark · Follow TCP Stream (tcp.stream eq 48) · 2019-09-25-Trickbot-gtag-ono19-infection-traffic.pcap 👘 💿 🛛
POST /ono19/BACHMANN-BTO-PC_W617601.AC3B679F4A22738281E6D7B0C5946E42/90 HTTP/1.1
Content-Type: multipart/form-data; boundary=Arasfjasu7
User-Agent: test
Host: 170.238.117.187:8082
Content-Length: 4007
Cache-Control: no-cache
Ar asi jasu/
content-Disposition. form-data, name- proclist
PROCESS LIST
[System Process]
System
Smss.exe
csrss.exe
wininit.exe
csrss.exe
winlogon.exe
services.exe
lsass.exe
lsm.exe
svchost.exe
4 client pkts, 1 server pkt, 1 turn.
Entire conversation (4,360 bytes) • Show and save data as ASCII • Stream 48 ‡
Find: Find <u>N</u> ext
Filter Out This Stream Print Save as Back X Close

Figure 19: System data sent by a Trickbot-infected host using HTTP traffic over TCP port 8082. It starts with a list of running processes.

Wireshark · Follow TCP Stream (tcp.stream eq 48)	• 2019-09-25-Trickbot-gtag-ono19-infection-traffic.pcap	• - • ×
SYSTEMINFO		*
Host Name - BACHMANN-BTO-PC OS Name - Microsoft Windows 7 Professi OS Version - Service Pack 1 OS Architecture - 64-bit Product Type - Workstation Build Type - Multiprocessor Free Registered Owner - admin Registered Organization - Serial Number - 00371-221-1925594-0617 Install Date - 30/12/1899 00.00.00 Last Boot Up Time - 30/12/1899 00.00.00 Windows Directory - C:\Windows System Directory - C:\Windows\System32 Boot Device - \Device\HarddiskVolume1	onal 8 0	
Total Physical Memory - 2593 Mb Available Physical Memory - 2593 Mb		
/c ipconfig /all		
Windows IP Configuration		
Host Name	Bachmann-BTO-PC Hybrid	*
4 client pkts, 1 server pkt, 1 turn.		
Entire conversation (4,360 bytes)	Show and save data as ASCII *	Stream 48 ‡
Find:		Find <u>N</u> ext
% Help	Filter Out This Stream Print Save as Back	X <u>C</u> lose

Figure 20: More system data sent by a Trickbot-infected host using HTTP traffic over TCP port 8082. This is later from the same HTTP stream that started in Figure 19.

Trickbot sends more Windows executable files over HTTP GET requests ending in *.png*. These follow-up Trickbot executables are used to infect a vulnerable domain controller (DC) when the infected Windows host is a client in an Active Directory environment.

You can find these URLs in the pcap by using the following Wireshark filter:

http.request and ip contains .png

2019-09-25-Tr	ickbot-gtag-ono19-infection-traffic.p	cap • _ • ×
<u>File Edit View Go Capture Analyze Statisti</u>	cs Telephony <u>W</u> ireless <u>T</u> ools <u>H</u> elp	
	<u></u> 🔁 🔛 🔍 🔍	€, ∰
http.request and ip conta	ains .png	Expression + basic basic+ basic+dns
Time Dst	port Host	Info
→ 2019-09-25 18:08… 185.98.87.	.185 80 185.98.87.185	GET /tablone.png HTTP/1.1
2019-09-25 18:08 185.98.87.	.185 80 185.98.87.185	GET /samerton.png HTTP/1.1
2019-09-25 18:29 185.98.87.	.185 80 185.98.87.185	GET /samerton.png HTTP/1.1
•	*****	Þ

Figure 21: Filtering to find follow-up Trickbot EXE files sent using URLs ending with .png.

Follow the TCP or HTTP stream in each of the three requests as shown in Figure 21. You should see indicators of windows executable files similar to what we saw in Figure 9. However, in this case, the HTTP response headers identify the returned file as image/png even though it clearly is a Windows executable or DLL file.



Figure 22: Windows executable sent through URL ending in .png.

You can export these files from Wireshark, confirm they are Windows executable files, and get the SHA256 file hashes as we covered earlier in this tutorial.

Trickbot Distributed Through Other Malware

Trickbot is frequently distributed through other malware. Trickbot is commonly seen as follow-up malware to Emotet infections, but we have also seen it as follow-up malware from IcedID and Ursnif infections

Since Emotet frequently distributes Trickbot, lets review an Emotet with Trickbot infection in September 2019 documented <u>here</u>. We already covered Emotet with Trickbot infections last year in <u>this Palo Alto Networks blog post</u>, so this tutorial will focus on the Trickbot activity.



Figure 23: Simplified flow chart for Emotet with Trickbot activity.

Download the pcap <u>from this page</u>. The pcap is contained in a password-protected zip archive named **2019-09-25-Emotet-infection-with-Trickbot-in-AD-environment.pcap.zip**. Extract the pcap from the zip archive using the password **infected** and open it in Wireshark. Use your **basic** filter to review the web-based infection traffic as shown in Figure 24.

Price Gall	Eile	2019-09-25-Emotet-infection-with-Trickbot-in-AD-environment.pcap										
Image: Interpretent of the state o												
Time Dst port Host Info -+ 2019-09-25 21:23 23.203.62.48 80 www.msftncsi.com GET /ncsi.txt HTTP/1.1 2019-09-25 21:29 172.106.75.164 80 beauty24.club GET /wp-includes/gvju6u 2019-09-25 21:30 179.62.18.56 443 179.62.18.56:443 POST /guids/usbccid/ HT 2019-09-25 21:34 178.32.255.133 443 178.32.255.133:443 GET /whoami.php HTTP/1.: 2019-09-25 21:34 179.62.18.56 443 179.62.18.56:443 POST /cab/mult/ringin/ I 2019-09-25 21:34 178.32.255.133 443 178.32.255.133:443 POST /cob/mult/ringin/ I 2019-09-25 21:34 178.32.255.133 443 178.32.255.133:443 POST /cookies/devices/ring 2019-09-25 21:34 178.32.255.133 443 178.32.255.133:443 POST /cookies/devices/ring 2019-09-25 21:34 206.21.51.38 449 Client Hello 2019-09-25 21:34 206.21.51.38 449 Client Hello		http.request or ss	l.handshake.	type ==	1) and !(ssdp)			Expression + basic basic+ basic+dns				
+ 2019-09-25 21:23 23.203.62.48 80 www.msftncsi.com GET /ncsi.txt HTTP/1.1 2019-09-25 21:29 172.106.75.164 80 beauty24.club GET /wp-includes/gvju6u 2019-09-25 21:30 179.62.18.56 443 179.62.18.56:443 POST /guids/usbccid/ HT 2019-09-25 21:34 178.32.255.133 443 178.32.255.133:443 GET /whoami.php HTTP/1.: 2019-09-25 21:34 178.32.255.133 443 178.32.255.133:443 POST /cab/mult/ringin/ (2019-09-25 21:34 200.21.51.38 449 Client Hello Client Hello 2019-09-25 21:35 216.239.32.21 80 ipecho.net GET /plain HTTP/1.1 2019-09-25 21:43 185.90.61.116 447 Client Hello Client Hello 2019-09-25 21:43 200.21.51.38 449 Client Hello Client Hello	Time	9		Dst		port	Host	Info				
2019-09-2521:29172.106.75.16480beauty24.clubGET /wp-includes/gvju6u2019-09-2521:30179.62.18.56443179.62.18.56:443POST /guids/usbccid/ HT2019-09-2521:34178.32.255.133443178.32.255.133:443GET /whoami.php HTTP/1.:2019-09-2521:34179.62.18.56443179.62.18.56:443POST /cab/mult/ringin/ I2019-09-2521:34178.32.255.133443178.32.255.133:443POST /cab/mult/ringin/ I2019-09-2521:34178.32.255.133443178.32.255.133:443POST /cob/mult/ringin/ I2019-09-2521:34178.32.255.133443178.32.255.133:443POST /cookies/devices/ring2019-09-2521:34200.21.51.38449Client Hello2019-09-2521:35216.239.32.2180ipecho.netGET /msdownload/update/2019-09-2521:35216.239.32.21443ipecho.netClient Hello2019-09-2521:34200.21.51.38449Client Hello2019-09-2521:43200.21.51.38449Client Hello2019-09-2521:43200.21.51.38449Client Hello2019-09-2521:4420.20.21.51.38449Client Hello2019-09-2521:4420.21.51.38449Client Hello2019-09-2521:4420.21.51.38449Client Hello2019-09-2521:4423.203.62.5080crl.microsoft.comGET /pki/crl/products/C<	+•	2019-09-25	21:23	23.20	3.62.48	80	www.msftncsi.com	GET /ncsi.txt HTTP/1.1				
2019-09-2521:30179.62.18.56443179.62.18.56:443POST /guids/usbccid/ HT2019-09-2521:34178.32.255.133443178.32.255.133:443GET /whoami.php HTTP/1.:2019-09-2521:34179.62.18.56443179.62.18.56:443POST /cab/mult/ringin/ I2019-09-2521:34178.32.255.133443178.32.255.133:443POST /cab/mult/ringin/ I2019-09-2521:34178.32.255.133443178.32.255.133:443POST /cob/mult/ringin/ I2019-09-2521:34178.32.255.133443178.32.255.133:443POST /cookies/devices/ring2019-09-2521:34200.21.51.38449Client Hello2019-09-2521:35216.239.32.2180ipecho.netGET /msdownload/update/2019-09-2521:35216.239.32.21443ipecho.netClient Hello2019-09-2521:35216.239.32.21443ipecho.netClient Hello2019-09-2521:43185.90.61.116447Client Hello2019-09-2521:43200.21.51.38449Client Hello2019-09-2521:43200.21.51.38449Client Hello2019-09-2521:43200.21.51.38449Client Hello2019-09-2521:4423.203.62.5080crl.microsoft.comGET /pki/crl/products/C2019-09-2521:4420.21.51.38449Client Hello2019-09-2521:4420.21.51.38449Client Hello201		2019-09-25	21:29	172.1	.06.75.164	1 80	beauty24.club	GET /wp-includes/gvju6u				
2019-09-2521:34178.32.255.133443178.32.255.133:443GET /whoami.php HTTP/1.:2019-09-2521:34179.62.18.56443179.62.18.56:443POST /cab/mult/ringin/2019-09-2521:34178.32.255.133443178.32.255.133:443POST /cab/mult/ringin/2019-09-2521:34178.32.255.133443178.32.255.133:443POST /cookies/devices/ring2019-09-2521:34200.21.51.38449Client Hello2019-09-2521:34205.185.216.4280www.download.windowsuGET /msdownload/update/2019-09-2521:35216.239.32.2180ipecho.netGET /plain HTTP/1.12019-09-2521:35216.239.32.21443ipecho.netClient Hello2019-09-2521:35200.21.51.38449Client Hello2019-09-2521:43170.238.117.1878082170.238.117.187:80822019-09-2521:43170.238.117.1878082170.238.117.187:80822019-09-2521:4423.203.62.5080crl.microsoft.comGET /pki/crl/products/C2019-09-2521:44200.21.51.38449Client Hello2019-09-2521:4420.21.51.38449Client Hello2019-09-2521:4420.21.51.38449Client Hello2019-09-2521:4420.21.51.38449Client Hello2019-09-2521:4420.21.51.38449Client Hello2019-09-2521:44200.21		2019-09-25	21:30	179.6	2.18.56	443	179.62.18.56:443	POST /guids/usbccid/ HT				
2019-09-2521:34179.62.18.56443179.62.18.56:443POST /cab/mult/ringin/2019-09-2521:34178.32.255.133443178.32.255.133:443POST /merge/devices/ring2019-09-2521:34178.32.255.133443178.32.255.133:443POST /cookies/devices/ring2019-09-2521:34200.21.51.38449Client Hello2019-09-2521:34205.185.216.4280www.download.windowsuGET /msdownload/update/2019-09-2521:35216.239.32.2180ipecho.netGET /plain HTTP/1.12019-09-2521:35216.239.32.21443ipecho.netClient Hello2019-09-2521:35200.21.51.38449Client Hello2019-09-2521:43185.90.61.116447Client Hello2019-09-2521:43200.21.51.38449Client Hello2019-09-2521:43200.21.51.38449Client Hello2019-09-2521:4420.20.3.62.5080crl.microsoft.comGET /pki/crl/products/C2019-09-2521:4420.21.51.38449Client Hello2019-09-2521:4420.21.51.38449Client Hello2019-09-2521:4420.21.51.38449Client Hello2019-09-2521:4420.21.51.38449Client Hello2019-09-2521:44200.21.51.38449Client Hello2019-09-2521:44200.21.51.38449Client Hello2019		2019-09-25	21:34	178.3	32.255.133	3 443	178.32.255.133:443	GET /whoami.php HTTP/1.:				
2019-09-2521:34178.32.255.133443178.32.255.133:443POST /merge/devices/ring2019-09-2521:34178.32.255.133443178.32.255.133:443POST /cookies/devices/ring2019-09-2521:34200.21.51.38449Client Hello2019-09-2521:34205.185.216.4280www.download.windowsuGET /msdownload/update/2019-09-2521:35216.239.32.2180ipecho.netGET /plain HTTP/1.12019-09-2521:35216.239.32.21443ipecho.netClient Hello2019-09-2521:35200.21.51.38449Client Hello2019-09-2521:43185.90.61.116447Client Hello2019-09-2521:43200.21.51.38449Client Hello2019-09-2521:43200.21.51.38449Client Hello2019-09-2521:43170.238.117.1878082170.238.117.187:80822019-09-2521:4423.203.62.5080crl.microsoft.comGET /pki/crl/products/C2019-09-2521:44200.21.51.38449Client Hello2019-09-2521:44200.21.51.38449Client Hello2019-09-2521:44200.21.51.38449Client Hello2019-09-2521:44200.21.51.38449Client Hello2019-09-2521:44200.21.51.38449Client Hello2019-09-2521:44200.21.51.38449Client Hello2019-09-2521:44		2019-09-25	21:34	179.6	2.18.56	443	179.62.18.56:443	POST /cab/mult/ringin/ I				
2019-09-25 21:34 178.32.255.133 443 178.32.255.133:443 POST /cookies/devices/r: 2019-09-25 21:34 200.21.51.38 449 Client Hello 2019-09-25 21:34 205.185.216.42 80 www.download.windowsu GET /msdownload/update/ 2019-09-25 21:35 216.239.32.21 80 ipecho.net GET /plain HTTP/1.1 2019-09-25 21:35 216.239.32.21 443 ipecho.net Client Hello 2019-09-25 21:35 216.239.32.21 443 ipecho.net Client Hello 2019-09-25 21:35 200.21.51.38 449 Client Hello 2019-09-25 21:43 185.90.61.116 447 Client Hello 2019-09-25 21:43 200.21.51.38 449 Client Hello 2019-09-25 21:43 170.238.117.187 8082 170.238.117.187:8082 POST /mor8/WARNER-WIN7-I 2019-09-25 21:44 20.21.51.38 449 Client Hello Client Hello 2019-09-25 21:44 20.21.51.38 449 Client Hello Client Hello		2019-09-25	21:34	178.3	32.255.133	3 443	178.32.255.133:443	POST /merge/devices/rin				
2019-09-25 21:34 200.21.51.38 449 Client Hello 2019-09-25 21:34 205.185.216.42 80 www.download.windowsu GET /msdownload/update/ 2019-09-25 21:35 216.239.32.21 80 ipecho.net GET /plain HTTP/1.1 2019-09-25 21:35 216.239.32.21 443 ipecho.net Client Hello 2019-09-25 21:35 200.21.51.38 449 Client Hello 2019-09-25 21:43 185.90.61.116 447 Client Hello 2019-09-25 21:43 200.21.51.38 449 Client Hello 2019-09-25 21:43 200.21.51.38 449 Client Hello 2019-09-25 21:43 170.238.117.187 8082 170.238.117.187:8082 POST /mor8/WARNER-WIN7-I 2019-09-25 21:44 23.203.62.50 80 crl.microsoft.com GET /pki/crl/products/C 2019-09-25 21:44 200.21.51.38 449 Client Hello 2019-09-25 21:44 200.21.51.38 449 Client Hello 2019-09-25 21:44 200.21.51.38		2019-09-25	21:34	178.3	2.255.133	3 443	178.32.255.133:443	POST /cookies/devices/r:				
2019-09-25 21:34 205.185.216.42 80 www.download.windowsu GET /msdownload/update/ 2019-09-25 21:35 216.239.32.21 80 ipecho.net GET /plain HTTP/1.1 2019-09-25 21:35 216.239.32.21 443 ipecho.net Client Hello 2019-09-25 21:35 200.21.51.38 449 Client Hello 2019-09-25 21:43 185.90.61.116 447 Client Hello 2019-09-25 21:43 200.21.51.38 449 Client Hello 2019-09-25 21:43 200.21.51.38 449 Client Hello 2019-09-25 21:43 170.238.117.187 8082 170.238.117.187:8082 POST /mor8/WARNER-WIN7-I 2019-09-25 21:44 23.203.62.50 80 crl.microsoft.com GET /pki/crl/products/C 2019-09-25 21:44 200.21.51.38 449 Client Hello 2019-09-25 21:44 200.21.51.38 449 Client Hello 2019-09-25 21:44 200.21.51.38 449 Client Hello 2019-09-25 21:44 200.21.51.38		2019-09-25	21:34	200.2	21.51.38	449		Client Hello				
2019-09-25 21:35 216.239.32.21 80 ipecho.net GET /plain HTTP/1.1 2019-09-25 21:35 216.239.32.21 443 ipecho.net Client Hello 2019-09-25 21:35 200.21.51.38 449 Client Hello 2019-09-25 21:43 185.90.61.116 447 Client Hello 2019-09-25 21:43 200.21.51.38 449 Client Hello 2019-09-25 21:43 200.21.51.38 449 Client Hello 2019-09-25 21:43 170.238.117.187 8082 170.238.117.187:8082 POST /mor8/WARNER-WIN7-1 2019-09-25 21:44 23.203.62.50 80 crl.microsoft.com GET /pki/crl/products/C 2019-09-25 21:44 200.21.51.38 449 Client Hello		2019-09-25	21:34	205.1	.85.216.42	2 80	www.download.windowsu	GET /msdownload/update/				
2019-09-25 21:35 216.239.32.21 443 ipecho.net Client Hello 2019-09-25 21:35 200.21.51.38 449 Client Hello 2019-09-25 21:43 185.90.61.116 447 Client Hello 2019-09-25 21:43 185.90.61.116 447 Client Hello 2019-09-25 21:43 200.21.51.38 449 Client Hello 2019-09-25 21:43 200.21.51.38 449 Client Hello 2019-09-25 21:43 170.238.117.187 8082 170.238.117.187:8082 POST /mor8/WARNER-WIN7-1 2019-09-25 21:44 23.203.62.50 80 crl.microsoft.com GET /pki/crl/products/C 2019-09-25 21:44 200.21.51.38 449 Client Hello 2019-09-25 21:44 200.21.51.38 449 Client Hello 2019-09-25 21:44 200.21.51.38 449 Client Hello		2019-09-25	21:35	216.2	39.32.21	80	ipecho.net	GET /plain HTTP/1.1				
2019-09-25 21:35 200.21.51.38 449 Client Hello 2019-09-25 21:43 185.90.61.116 447 Client Hello 2019-09-25 21:43 200.21.51.38 449 Client Hello 2019-09-25 21:43 200.21.51.38 449 Client Hello 2019-09-25 21:43 200.21.51.38 449 Client Hello 2019-09-25 21:44 23.203.62.50 80 crl.microsoft.com GET /pki/crl/products/C 2019-09-25 21:44 200.21.51.38 449 Client Hello 2019-09-25 21:44 200.21.51.38 449 Client Hello 2019-09-25 21:44 200.21.51.38 449 Client Hello		2019-09-25	21:35	216.2	39.32.21	443	ipecho.net	Client Hello				
2019-09-25 21:43 185.90.61.116 447 Client Hello 2019-09-25 21:43 200.21.51.38 449 Client Hello 2019-09-25 21:43 200.21.51.38 449 Client Hello 2019-09-25 21:43 200.21.51.38 449 Client Hello 2019-09-25 21:43 170.238.117.187 8082 170.238.117.187:8082 POST /mor8/WARNER-WIN7-I 2019-09-25 21:44 23.203.62.50 80 crl.microsoft.com GET /pki/crl/products/C 2019-09-25 21:44 200.21.51.38 449 Client Hello 2019-09-25 21:44 200.21.51.38 449 Client Hello 2019-09-25 21:44 200.21.51.38 449 Client Hello		2019-09-25	21:35	200.2	1.51.38	449		Client Hello				
2019-09-25 21:43 200.21.51.38 449 Client Hello 2019-09-25 21:43 200.21.51.38 449 Client Hello 2019-09-25 21:43 170.238.117.187 8082 170.238.117.187:8082 POST /mor8/WARNER-WIN7-1 2019-09-25 21:44 23.203.62.50 80 crl.microsoft.com GET /pki/crl/products/C 2019-09-25 21:44 200.21.51.38 449 Client Hello 2019-09-25 21:44 200.21.51.38 449 Client Hello		2019-09-25	21:43	185.9	0.61.116	447		Client Hello				
2019-09-25 21:43 200.21.51.38 449 Client Hello 2019-09-25 21:43 170.238.117.187 8082 170.238.117.187:8082 POST /mor8/WARNER-WIN7-1 2019-09-25 21:44 23.203.62.50 80 crl.microsoft.com GET /pki/crl/products/C 2019-09-25 21:44 200.21.51.38 449 Client Hello 2019-09-25 21:44 200.21.51.38 449 Client Hello		2019-09-25	21:43	200.2	1.51.38	449		Client Hello				
2019-09-25 21:43 170.238.117.187 8082 170.238.117.187:8082 POST /mor8/WARNER-WIN7-I 2019-09-25 21:44 23.203.62.50 80 crl.microsoft.com GET /pki/crl/products/C 2019-09-25 21:44 200.21.51.38 449 Client Hello 2019-09-25 21:44 200.21.51.38 449 Client Hello		2019-09-25	21:43	200.2	1.51.38	449		Client Hello				
2019-09-25 21:44 23.203.62.50 80 crl.microsoft.com GET /pki/crl/products/C 2019-09-25 21:44 200.21.51.38 449 Client Hello 2019-09-25 21:44 200.21.51.38 449 Client Hello		2019-09-25	21:43	170.2	238.117.18	37 8082	170.238.117.187:8082	POST /mor8/WARNER-WIN7-				
2019-09-25 21:44 200.21.51.38 449 Client Hello 2019-09-25 21:44 200.21.51.38 449 Client Hello		2019-09-25	21:44	23.20	3.62.50	80	crl.microsoft.com	GET /pki/crl/products/C				
2019-09-25 21:44 200.21.51.38 449 Client Hello		2019-09-25	21:44	200.2	1.51.38	449		Client Hello				
		2019-09-25	21:44	200.2	1.51.38	449		Client Hello				
	4		~ · · ·	170 0		-						

Figure 24: Filtering on web traffic in an Emotet+Trickbot infection.

Experienced analysts can usually identify the Emotet-generated traffic and the Trickbotgenerated traffic. Post-infection Emotet activity consists HTTP traffic with encoded data returned by the server. This is distinctly different than post-infection Trickbot activity which generally relies on HTTPS/SSL/TLS traffic for command and control communications. Figure 25 points out the different infection traffic between Emotet and Trickbot for this specific infection.

	2019-09-25-Emotet-infe	ection-v	with-Trickbot-in-AD-environment.p	cap 🔹 🗉 🗙
<u>File Edit View Go Capture</u>	Analyze Statistics Telep	hony <u>V</u>	<u>V</u> ireless <u>T</u> ools <u>H</u> elp	
	3 🙆 🙇 🔹 🕭		x 🔍 📃 🔍 Q, Q, 🏢	
(http.request or ssl.handshake	e.type == 1) and !(ssdp)			Expression + basic basic+ basic+dns
Time	Dst	port	Host	Info
<u> </u>	. 23.203.62.48	80	www.msftncsi.com	GET /ncsi.txt HTTP/1.1
Emotet 21:29.	172.106.75.164	80	beauty24.club	GET /wp-includes/gvju6u
21:30.	179.62.18.56	443	179.62.18.56:443	POST /guids/usbccid/ HT
2019-09-25 21:	178.32.255.133	443	178.32.255.133:443	GET /whoami.php HTTP/1.:
2019-09-25 21:34.	179.62.18.56	443	179.62.18.56:443	POST /cab/mult/ringin/ I
2019-09-25 21:34.	178.32.255.133	443	178.32.255.133:443	POST /merge/devices/rin
2019-09-25 21:34.	178.32.255.133	443	178.32.255.133:443	POST /cookies/devices/r:
2019-09-25 21:34	200.21.51.38	449		Client Hello
2019-09-25 21: 4	205.185.216.42	80	www.download.windowsu	GET /msdownload/update/
2019-09-25 21:35.	216.239.32.21	80	ipecho.net	GET /plain HTTP/1.1
2019-09-25 21:35.	216.239.32.21	443	ipecho.net	Client Hello
2019-09 25 21:35.	200.21.51.38	449		Client Hello
Trickbot 21:43.	185.90.61.116	447		Client Hello
21	200.21.51.38	449		Client Hello
2019-09-25 21:43.	200.21.51.38	449		Client Hello
2019-09-25 2.:43.	170.238.117.187	8082	170.238.117.187:8082	POST /mor8/WARNER-WIN7-I
2019-09-25 21:	. 23.203.62.50	80	crl.microsoft.com	GET /pki/crl/products/C
2019-09-25 21:44.	200.21.51.38	449		Client Hello
2019-09-25 21:44.	200.21.51.38	449		Client Hello

Figure 25: The differences in Emotet and Trickbot traffic.

This infection happened in an Active Directory environment with 10.9.25.102 as the infected Windows client and 10.9.25.9 as the DC. Later in the traffic, we see the DC exhibit signs of Trickbot infection as shown in Figure 26.

	2019-09-25-Emotet-infe	ction-with-Trickbot-in-AD)-environment.pcap	+ ×
File Edit View Go Capture An	alvze Statistics Telephony W	vireless Tools Help		(0000
	S 🗋 🏶 🕸 🕉 🛤 🕯	🛛 📃 🔍 🔍 🔍	. 11	
(http.request or ssl.handshake.typ	e == 1) and !(ssdp)		Expressio	n + basic basic+ basic+dns
Time	* Src port	Dst p	port Host	Info
2019-09-25 21:48:14	10.9.25.102 49275	195.123.220.86	447	Client Hello
2019-09-25 21:48:15	10.9.25.102 49276	200.21.51.38	449	Client Hello
Trickhot activity	10.9.25.102 49277	185.98.87.185 8	80 185.98.87.185	GET /samerton.png
HICKDOL ACTIVITY 48:41	10.9.25.102 49279	195.123.238.36	447	Client Hello
on the domain 48:43	10.9.25.102 49280	5.53.125.13	447	Client Hello
controller 48:55	10.9.25.102 49283	179.62.18.56	443 179.62.18.56:443	POST /prov/ HTTF.
49:02	10.9.25.102 49283	179.62.18.56	443 179.62.18.56:443	POST /sess/ HTTP/1
2019-09-25 21:57:05	10.9.25.102 49297	195.123.221.104 4	447	Client Hello
2019-09-25 21:57:06	10.9.25.102 49298	200.21.51.38	449	Client Hello
2019-09-25 21 57:12	10.9.25.9 63887	185.98.87.185 8	80 185.98.87.185	GET /wredneg2.png
2019-09-25 21:5:12	10.9.25.102 49344	185.98.87.185 8	80 185.98.87.185	GET /wredneg2.png
2019-09-25 21:58:	10.9.25.102 49345	200.21.51.38	449	Client Hello
2019-09-25 21:59:31	10.9.25.9 63898	190.154.203.218 4	449	Client Hello
2019-09-25 21:59:36	10.9.25.9 63901	104.124.62.48	80 www.download.wi	GET /msdownload/up
2019-09-25 21:59:38	10.9.25.9 63902	185.248.87.88	443 api.ip.sb	Client Hello
2019-09-25 21:59:43	10.9.25.9 63901	104.124.62.48	80 www.download.wi…	GET /msdownload/up
2019-09-25 22:01:56	10.9.25.9 63921	5.53.125.13	447	Client Hello
2019-09-25 22:01:57	10.9.25.9 63922	190.154.203.218 4	449	Client Hello
2019-09-25 22:02:10	10.9.25.9 63923	190.154.203.218 4	449	Client Hello
4	-			· · · · · ·

Figure 26: Trickbot activity on the DC.

How did the infection move from client to DC? Trickbot uses a version of the <u>EternalBlue</u> exploit to move laterally using Microsoft's SMB protocol. In this case, the infected Windows client sent information several times over TCP port 445 to the DC at 10.9.25.9, which then retrieved a Trickbot executable from **185.98.87[.]185/wredneg2.png**. Use the **basic+** filter to see the SYN segments for the traffic between the client at 10.9.25.102 and the DC at 10.9.25.9 right before the DC calls out to **185.98.87[.]185** as shown in Figure 27

					201	0.00.	25.Em	otot-info	ction-with-	Trickhot-in		ironment ncan				_	A
File	e Edit	View Go	Canture	Anal	ZUI:	atistic	s Tel	enhony V	Vireless Too	Is Help	-AD-env	ironment.pcap			•	A '	
-						A					0.11						
				×	2 0	-	P		× 💶	य य	Q 11						
	(http.req	uest or ssl	.handshake	e.type	== 1 or	r tcp.fl	ags eq	0x0002) a	and !(ssdp)				Expression	n ·	+ basic	basic+	basic+dns
Tim	e			*	Src			port	Dst		port	Host	Info				-
	2019	-09-25	21:57:	:06	10.9	.25.	102	49298	200.21	.51.38	449		Cl	ient	Hello)	
	2019	-09-25	21:57:	:11	10.9	.25.	102	49299	10.9.25	5.9	3268		49	299	→ 3268	B [SYN] Se
	2019	-09-25	21:57:	:11	10.9	.25.	102	49300	10.9.25	5.9	445		49	300	→ 445	[SYN]	Sec
	2019	-09-25	21:57:	:11	10.9	.25.	102	49301	10.9.25	5.9	135		49	301	→ 135	[SYN]	Sec
	2019	-09-25	21:57:	:11	10.9	.25.	102	49302	10.9.25	5.9	445		49	302	→ 445	[SYN]	Sec
	2019	-09-25	21:57:	:11	10.9	.25.	102	49303	10.9.25	5.9	445		49	303	→ 445	[SYN]	Sec=
	2019	-09-25	21:57:	:11	10.9	.25.	102	49304	10.9.25	5.9	445		49	304	→ 445	[SYN]	Sec
	2019	-09-25	21:57:	:11	10.9	.25.	102	49305	10.9.25	5.9	445		49	305	→ 445	[SYN]	Sec
	2019	-09-25	21:57:	:11	10.9	.25.	102	49306	10.9.25	5.9	445		49	306	→ 445	[SYN]	Sec
	2019	-09-25	21:57:	:11	10.9	.25.	102	49307	10.9.25	5.9	445		49	307	→ 445	[SYN]	Sec
	2019	-09-25	21:57:	:11	10.9	.25.	102	49308	10.9.25	5.9	445		49	308	→ 445	[SYN]	Sec
	2019	-09-25	21:57:	:11	10.9	.25.	102	49309	10.9.25	5.9	445		49	309	→ 445	[SYN]	
	2019	-09-25	21:57:	:11	10.9	.25.	102	49310	10.9.25	5.9	445		49	310	→ 445	[SYN]	
	2019	-09-25	21:57:	:11	10.9	.25.	102	49311	10.9.25	5.9	445		49	311	→ 445	[SYN]	Sec
	2019	-09-25	21:57:	:11	10.9	.25.	102	49312	10.9.25	5.9	445		49	312	→ 445	[SYN]	Sec
	2019	-09-25	21:57:	:11	10.9	.25.	102	49313	10.9.25	5.9	445		49	313	→ 445	[SYN]	Sec
	2019	-09-25	21:57:	:11	10.9	.25.	102	49314	10.9.25	5.9	445		49	314	→ 445	[SYN]	Sec
	2019	-09-25	21:57:	:11	10.9	.25.	102	49315	10.9.25	5.9	445		49	315	→ 445	[SYN]	Sec
	2019	-09-25	21:57:	:11	10.9	.25.	102	49316	10.9.25	5.9	445		49	316	→ 445	[SYN]	Sec
	2019	-09-25	21:57:	:11	10.9	.25.	102	49317	10.9.25	5.9	445		49	317	→ 445	[SYN]	Sec
	2019	-09-25	21:57:	:11	10.9	. 25.	102	49318	10.9.25	5.9	445		49	318	→ 445	[SYN]	Sec
	2019	-09-25	21:57:	:11	10.9	.25.	102	49319	10.9.25	5.9	445		49	319	→ 445	[SYN]	Sec
	2019	-09-25	21:57:	:11	10.9	.25.	102	49320	10.9.25	5.9	445		49	320	→ 445	[SYN]	Sec
	2019.	-09-25	21:57:	:11	10.9	.25.	102	49321	10.9.25	5.9	445		49	321	→ 445	[SYN]	Sec
	2019	-09-25	21:57:	:11	10.9	.25.	9	63887	185.98.	.87.185	80		63	887	→ 80 [[SYN]	Seq=
	2019	-09-25	21:57:	:11	10.9	.25.	102	49344	185.98.	.87.185	80		49	344	→ 80 [SYN]	Seq=
	2019	-09-25	21:57:	:12	10.9	.25.	9	63887	185.98.	.87.185	80	185.98.87.	185 GE	T /w	redneg	j2.png	HTT
	2019	-09-25	21:57:	:12	10.9	.25.	102	49344	185.98.	.87.185	80	185.98.87.	185 GE	T /w	redneg	12.png	HTT .
4																	F

Figure 27: Finding traffic from the client at 10.9.25.102) to the DC at 10.9.25.9 (shown in grey) before the DC retrieved a Trickbot EXE from 196.98.87[.]185/wredneg2.png.

Follow one of the TCP streams, for example the line with a source as 10.9.25.102 over TCP port 49321 and destination as 10.9.35.9 over TCP port 445. This is highly unusual traffic for a client to send to a DC, so it is likely related to the EternalBlue exploit. See Figure 28 for an example of this traffic



Figure 28: Example of the unusual traffic from a client to DC over TCP port 445, possibly related to an EternalBlue-based exploit.

Other than this unusual SMB traffic and the DC getting infected, any Trickbot-specific activity in this pcap is remarkably similar to our previous example.

Conclusion

This tutorial provided tips for examining Windows infections with Trickbot malware by reviewing two pcaps from September 2019. More pcaps with recent examples of Trickbot activity can be found at <u>malware-traffic-analysis.net</u>.

For more help with Wireshark, see our previous tutorials:

Get updates from Palo Alto Networks!

Sign up to receive the latest news, cyber threat intelligence and research from us

By submitting this form, you agree to our <u>Terms of Use</u> and acknowledge our <u>Privacy</u> <u>Statement</u>.