Wireshark Tutorial: Examining Emotet Infection Traffic

unit42.paloaltonetworks.com/wireshark-tutorial-emotet-infection/

Brad Duncan

January 19, 2021

By Brad Duncan

January 19, 2021 at 6:00 AM

Category: Tutorial, Unit 42

Tags: Wireshark Tutorial

traffic-for-wireshark-column-setup.pcap			
File Edit View Go Capture Analyze	e Statistics Telephony Wireles	ss Tools Help	
		噩	
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 /2017/03/01/
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	s2.vp.com	Client Hello
2018-08-03 19:06:20 1 2.0.77 31	443	s2 p.com	Client Hello
2018-08-03 19:06:20 192.0.77.32	443	s2.wp.com	Client Hello
2018-08-03 19:06:20 192.0.77.32	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 /css/usatoda
2018-08-03 19:06:20 52.84.125	80 d15krst4gi8g86.clou		GET /js/script.j
2018_08_03 10+06+20 52 8/ 125	RA disknet/aiRaRE clou		GET /rec/licatoda
🔵 🍸 traffic-for-wireshark-column-setup.pcap		Packets: 4448 · Displayed: 1	23 (2.8%) Profile: Default

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

Executive Summary

This tutorial is designed for security professionals who investigate suspicious network activity and review packet captures (pcaps). Familiarity with <u>Wireshark</u> is necessary to understand this tutorial, which focuses on Wireshark version 3.x.

<u>Emotet</u> is an information-stealer <u>first reported in 2014</u> as banking malware. It has since evolved with additional functions such as a dropper, distributing other malware families like <u>Gootkit</u>, <u>IcedID</u>, <u>Qakbot</u> and <u>Trickbot</u>.

Today's Wireshark tutorial reviews recent Emotet activity and provides some helpful tips on identifying this malware based on traffic analysis.

Note: These instructions assume you have customized Wireshark as described in <u>our</u> <u>previous Wireshark tutorial about customizing the column display</u>.

You will need to access a GitHub repository with ZIP archives containing the pcaps used for this tutorial.

Warning: Some of the pcaps used for this tutorial contain Windows-based malware. There is a risk of infection if using a Windows computer. If possible, we recommend you review these pcaps in a non-Windows environment like BSD, Linux or macOS.

Chain of Events for an Emotet Infection

To understand network traffic caused by Emotet, you must first understand the chain of events leading to an infection. Emotet is commonly distributed through malicious spam (malspam) emails. The critical step in an Emotet infection chain is a Microsoft Word document with macros designed to infect a vulnerable Windows host.



Figure 1. Screenshot of a Word document used to cause an Emotet infection in January 2021.

Malspam spreading Emotet uses different techniques to distribute these Word documents.

The malspam may contain an attached Microsoft Word document or have an attached ZIP archive containing the Word document. In recent months, we have seen several examples where these ZIP archives are password-protected. Some emails distributing Emotet do not have any attachments. Instead, they contain a link to download the Word document.

In previous years, malspam pushing Emotet has also used PDF attachments with embedded links to deliver these Emotet Word documents.

Figure 2 illustrates these four distribution techniques.



Figure 2. Various distribution paths for an Emotet Word document.

After the Word document is delivered, if a victim opens the document and enables macros on a vulnerable Windows host, the host is infected with Emotet.

From a traffic perspective, we see the following steps from an Emotet Word document to an Emotet infection:

- Web traffic to retrieve the initial binary.
- Encoded/encrypted command and control (C2) traffic over HTTP.
- Additional infection traffic if Emotet drops follow-up malware.
- SMTP traffic if Emotet uses the infected host as a spambot.

Figure 3 shows a flowchart of network activity we might find during an Emotet infection.



Figure 3. Flowchart for an Emotet infection.

Since Dec. 21, 2020, the initial binary for Emotet has been a Windows DLL file. Previously, this binary had been a Windows EXE file.

Emotet C2 traffic consists of encoded or otherwise encrypted data sent over HTTP. This C2 activity can use either standard or non-standard TCP ports associated with HTTP traffic. This C2 activity also consists of data exfiltration and traffic to update the initial Emotet binary.

Since Emotet is also a malware dropper, the victim may become infected with other malware. Analysts should search for traffic from other malware when investigating traffic from an Emotet-infected host.

Finally, an Emotet-infected host may also become a spambot generating large amounts of traffic over TCP ports associated with SMTP like TCP ports 25, 465 and 587.

Pcaps of Emotet Infection Activity

Five password-protected ZIP archives containing pcaps of recent Emotet infection traffic are available at <u>this GitHub repository</u>. Once on the GitHub page, click on each of the ZIP archive entries and download them, as shown in Figures 4 and 5.

O GitHub - pan-unit42/ × +		Jui Wileshark Lucoria	
← → C ŵ 🔽 🖉 ♠ https://github.com/pan-unit42/wireshar	<-tutorial-Emotet-traffic	ເ ☆	II\
Why GitHub? V Team Enterprise Explore V Marketplace Pricing V	Search	/ S	ign in Sign up
pan-unit42 / wireshark-tutorial-Emotet-traffic	\odot	Vatch 5 🖧 Star 2	eg Fork 0
<> Code () Issues 1 Pull requests () Actions () Projects () Se	curity 🗠 Insights		
🐉 main 👻 🐉 1 branch 💿 0 tags	Go to file	About	
brad-duncan Add files via upload	f45f2c1 1 hour ago 🕚 9 commits	This repository contains pcaps for our Wireshard	s zip archives of k tutorial about
Example-1-2021-01-06-Emotet-inf-ec Add files via upload	1 hour ago	password for any of the	zip files posted
Example-2-2021-01-05-Emotet-with Add files via upload	2 hours ago	here is: infected	
Example-3-2021-01-05-Emotet-with Add files via upload	2 hours ago	C Readme	
Example-4-2021-01-05-Emotet-infec Add files via upload	23 hours ago		
Example-5-2020-08-18-Emotet-infec Add files via upload	23 hours ago	Releases	
README.md Initial commit	yesterday	No releases published	
README.md		Packages	l
wireshark tutorial Emotot traffic		No packages published	
witeshark-tutonal-Emotet-traffic			
This repository contains zip archives of pcaps for our Wireshark tutorial about ex	amining Emotet infection traffic. The		
https://github.com/pan-unit42/wireshark-tutorial-Emotet-traffic/blob/main/E	kample-1-2021-01-06-Emotet-infection	.pcap.zip	
Figure 4. GitHub repository with links to ZIP ar	chives used for this tu	torial.	
wireshark-tutorial-Emotet-traffic/Example-1-2021-01-06-Emotet-infect	tion.pcap.zip at main · pan-unit42/w	ireshark-tutorial-Emo	otet-traffic – + ×
O wireshark-tutorial-ELX +			
$\leftarrow \rightarrow \mathbb{C}$ (a) $\mathbb{O} \mid \mathbb{A}$ https://github.com/pan-unit42/wireshar	k-tutorial-Emotet-traffic/blob/main/E	xa ••• 🖻 ✿	
Why GitHub? V Team Enterprise Explore V Marketplace Pricing V	Search		Sign in Sign up
pan-unit42/wireshark-tutorial-Emotet-traffic		Watch 5	2 & Fork 0
<> Code () Issues () Pull requests () Actions () Projects () Se	curity 🗠 Insights		
2* main - wireshark-tutorial-Emotet-traffic / Example-1-2021-01-06-Emote			
	t-infection.pcap.zip		Go to file
brad-duncan Add files via upload	t-infection.pcap.zip	Latest commit f45f2c1 1 hour	Go to file
brad-duncan Add files via upload As 1 contributor	t-infection.pcap.zip	Latest commit f45f2c1 1 hour	ago 🕤 History
brad-duncan Add files via upload At 1 contributor 3.25 MB	t-infection.pcap.zip	Latest commit f45f2c1 1 hour	So to file ago 🕥 History Download
brad-duncan Add files via upload At 1 contributor 3.25 MB Vie (Sorry about that, but we can't st	t-infection.pcap.zip w raw now files that are this big right now.)	Latest commit f45f2c1 1 hour	Go to file ago ③ History Download ①
brad-duncan Add files via upload A: 1 contributor 3.25 MB Vie (Sorry about that, but we can't st	t-infection.pcap.zip w raw now files that are this big right now.)	Latest commit f45f2c1 1 hour	Go to file ago ③ History Download ①
brad-duncan Add files via upload At 1 contributor 3.25 MB Vie (Sorry about that, but we can't si (Sorry about that, but we can't si	t-infection.pcap.zip	Latest commit f45f2c1 1 hour	Biog About

Figure 5. Downloading one of the ZIP archives for this tutorial.

Use *infected* as the password to extract pcaps from these ZIP archives. This should give you the following five pcap files:

- Example-1-2021-01-06-Emotet-infection.pcap
- Example-2-2021-01-05-Emotet-with-spambot-traffic-part-1.pcap
- Example-3-2021-01-05-Emotet-with-spambot-traffic-part-2.pcap
- Example-4-2021-01-05-Emotet-infection-with-Trickbot.pcap
- Example-5-2020-08-18-Emotet-infection-with-Qakbot.pcap

Example 1: Emotet Infection Traffic

Open *Example-1-2021-01-06-Emotet-infection.pcap* in Wireshark and use a basic web filter as described in our previous <u>tutorial about Wireshark filters</u>. The basic filter for Wireshark 3.x is:

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

If you've set up Wireshark according to our initial <u>tutorial about customizing Wireshark</u> <u>displays</u>, your display should look similar to Figure 6.

*	Example-1-2021-01-06-Emotet-infection.pcap							
<u>F</u> ile <u>E</u> dit <u>V</u> iev	<u>File Edit View Go Capture Analyze Statistics Telephony Wireless Tools H</u> elp							
/ = / · · · · · · · · · · · · · · · · ·								
🖡 (http.request or tls.handshake.type eq 1) and !(ssdp)								
Time		Dst	port	Host	Info	-		
2021-01-	06 16:41:16	89.252.164.58	80	hangarlastik.com	GET /cgi-bin/Ui4n/ HTTP/1.1			
2021-01-	06 16:41:16	89.252.164.58	80	hangarlastik.com	GET /cgi-sys/suspendedpage.cgi			
2021-01-	06 16:41:16	66.153.205.191	80	padreescapes.com	GET /blog/0I/ HTTP/1.1			
2021-01-	06 16:41:17	173.255.195.246	80	sarture.com	GET /wp-includes/JD8/ HTTP/1.1			
2021-01-	06 16:41:18	103.92.235.25	80	seo.udaipurkart.com	GET /rx-5700-6hnr7/Sgms/ HTTP/1			
2021-01-	06 16:41:19	52.114.132.91	443	self.events.data.mic	Client Hello			
2021-01-	06 16:41:45	20.188.78.185	443	fe2cr.update.microso	Client Hello			
2021-01-	06 16:41:46	52.114.77.33	443	v10.events.data.micr	Client Hello			
2021-01-	06 16:41:47	111.221.29.40	443	fe3cr.delivery.mp.mi	Client Hello			
2021-01-	06 16:41:48	52.114.77.33	443	v10.events.data.micr	Client Hello			
2021-01-	06 16:41:51	52.114.77.33	443	v10.events.data.micr	Client Hello			
2021-01-	06 16:42:34	5.2.136.90	80	5.2.136.90	POST /7u0e9j2avwlvnuynyo/szcm27			
2021-01-	06 16:42:42	5.2.136.90	80	5.2.136.90	POST /ko5ezxmguvv/p8d4003oiu/ut			
2021-01-	06 16:42:42	52.109.8.21	443	nexusrules.officeapp	Client Hello			
2021-01-	06 16:42:45	5.2.136.90	80	5.2.136.90	POST /vwst360x8syxks325x/26dtqu			
2021-01-	06 16:42:48	52.114.132.91	443	self.events.data.mic	Client Hello			
2021-01-	06 16:42:48	167.71.4.0	8080	167.71.4.0:8080	POST /va9j7/5clu9bdp5xth2a/4pq9			
2021-01-	06 16:42:49	5.2.136.90	80	5.2.136.90	POST /mro86v6nvs42/ HTTP/1.1			
2021-01-	06 16:42:52	167.71.4.0	8080	167.71.4.0:8080	POST /3rkiie36/ HTTP/1.1			
2021-01-	06 16:42:52	5.2.136.90	80	5.2.136.90	POST /raet/u6tpsbdmo5g7crj4f/81			
2021-01-	06 16:42:53	52.109.8.21	443	nexusrules.officeapp	Client Hello			
2021-01-	06 16:42:56	167.71.4.0	8080	167.71.4.0:8080	POST /ves4up2v2n5qjq5rl/i8ldtkh			
2021-01-	06 16:43:00	167.71.4.0	8080	167.71.4.0:8080	POST /tvvzt3/ai6wn02o2/9oeb81/			
2021-01-	06 16:46:42	52.114.88.21	443	v10.events.data.micr	Client Hello			
2021-01-	06 16:47:07	40.126.5.36	443	login.live.com	Client Hello			
2021-01-	06 16:47:07	40.91.76.238	443	licensing.mp.microso	Client Hello			
2021-01-	06 16:47:07	52.183.220.149	443	settings-win.data.mi	Client Hello			
1 2021 01	06 16.17.11	10/ 05 0/ 110	110	atorocotologrovocoti	Client Helle			

Figure 6. Our first pcap in this tutorial filtered in Wireshark.

As shown in Figure 6, the first five HTTP GET requests represent four URLs used to retrieve the initial Emotet DLL. The traffic is:

- hangarlastik[.]com GET /cgi-bin/Ui4n/
- hangarlastik[.]com GET /cgi-sys/suspendedpage.cgi
- padreescapes[.]com GET /blog/0l/

- sarture[.]com GET /wp-includes/JD8/
- seo.udaipurkart[.]com GET /rx-5700-6hnr7/Sgms/

The first two URLs indicate hangarlastik[.]com no longer had the Emotet DLL file it had been hosting. Follow TCP streams for each of these requests to see replies to each of the HTTP GET requests.

An easier way to see the HTTP responses is to update your Wireshark basic web filter to include HTTP responses:

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

This will show HTTP responses in the *Info* column, as illustrated in Figure 7.



Figure 7. Adding HTTP responses to the Wireshark display filter.

Now we have a clearer picture of what happened when the Word macro tried to retrieve an Emotet DLL:

- hangarlastik[.]com GET /cgi-bin/Ui4n/
- HTTP/1.1 302 Found
- hangarlastik[.]com GET /cgi-sys/suspendedpage.cgi
- HTTP/1.1 200 OK
- padreescapes[.]com GET /blog/0l/
- HTTP/1.1 401 Unauthorized
- sarture[.]com GET /wp-includes/JD8/
- HTTP/1.1 403 Forbidden
- seo.udaipurkart[.]com GET /rx-5700-6hnr7/Sgms/

The only 200 OK was a reply for a suspended page notification from hangarlastik[.]com.

The HTTP GET request to seo.udaipurkart[.]com does not show a response, so follow the TCP stream for this request, as shown in Figure 8.

• Example-1-2021-01-06-Emotet-infection.pcap - + ×							
<u>File Edit View Go Capture Analyze Statistics Telephony Wireless Tools H</u> elp							
/ I () () () () () () () () () (
(http.request or http.response or tls.handshake.type eq 1) and !(ssdp)							
Time	Dst	port	Host		Info		<u>^</u>
2021-01-06 16:41:16	89.252.164.58	80	hangarlastik.com	1	GET	/cgi-bin/Ui4n/ HTTP/1	.1
2021-01-06 16:41:16	10.1.6.206	49772			HTTP	/1.1 302 Found (text	/html)
2021-01-06 16:41:16	89.252.164.58	80	hangarlastik.com	1	GET	/cgi-sys/suspendedpag	e.cgi H
2021-01-06 16:41:16	10.1.6.206	49772	nedween en en		HTTP	/1.1 200 OK (text/ht	m1)
2021-01-06 16:41:16	66.153.205.191	80	padreescapes.com	1	GEI	/DIOG/01/ HITP/1.1	(toyt
2021-01-00 10.41.17	173 255 105 246	49//3	sarture com		CET	/un_includes/108/ HTT	
2021-01-06 16:41:17	10 1 6 206	49774	sar cure.com		HTTP	/1 1 403 Forbidden (text/ht
$\rightarrow 2021 \cdot 01 \cdot 00 \cdot 10.41.17$	103.92.235.25	80	seo.udaipurkart.	com	GET	/rx-5700-6hnr7/Sams/	HTTP/1.
2021-01-06 16:41:19	52.114.132.91	443	self.events.data	.mi	Cli	Mark/Unmark Packet	Ctrl+M
2021-01-06 16:41:45	20.188.78.185	443	fe2cr.update.mic	ros	Cli		Ctrl+D
2021-01-06 16:41:46	52.114.77.33	443	v10.events.data.	mic	Cli	Ignore/Onignore Packet	CUITD
2021-01-06 16:41:47	111.221.29.40	443	fe3cr.delivery.m	р . т	Cli	Set/Unset Time Reference	Ctrl+T
2021-01-06 16:41:48	52.114.77.33	443	v10.events.data.	mic	Cli	Time Shift	Ctrl+Shift+T
2021-01-06 16:41:51	52.114.77.33	443	v10.events.data.	m1C	CLI	Packet Comment	Ctrl+Alt+C
+ 2021 - 01 - 06 16:42:28 2021 - 01 - 06 16:42:34	10.1.6.206	49775	5.2.136.90		POS	Edit Resolved Name	
2021-01-06 16:42:42	10.1.6.206	49783	0121200100		HTT	Luit Resolved Name	
2021-01-06 16:42:42	5.2.136.90	80	5.2.136.90		POS	Apply as Filter	×
4						Prepare as Filter	+
						Conversation Filter	+
						Colorize Conversation	•
						SCTP	•
		1	CP Stream Ctrl+A	lt+Shift	+T	Follow	•
		- U	JDP Stream Ctrl+A	lt+Shift	+U	Сору	•
		Т	LS Stream Ctrl+A	lt+Shift	+S	Protocol Preferences	•
		H	HTTP Stream Ctrl+A	lt+Shift	+H	Decode As	
		H	HTTP/2 Stream			Show Packet in New <u>W</u> indow	
		(OUIC Stream				

Figure 8. Following TCP stream for the HTTP request to seo.udaipurkart[.]com.

The TCP stream shows indicators that seo.udaipurkart[.]com returned a Windows DLL file, as shown in Figure 9.

Wireshark · Follow TCP Stream (tcp.stream eq	3) · Example-1-2021-01-06-Emotet-infection.pcap –	+ ×
GET /rx-5700-6hnr7/Sgms/ HTTP/1.1 Host: seo.udaipurkart.com Connection: Keep-Alive		
HTTP/1.1 200 OK Date: Wed, 06 Jan 2021 16:41:45 GMT Server: Apache		
X-Powered-By: PHP/7.3.11 Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Wed, 06 Jan 2021 16:41:45 GMT	¥	
Content-Disposition: attachment; filename="nDU Content-Transfer-Encoding: binary Set-Cookie: 5ff5e84994849=1609951305; expires:	Jrg8uFD5hl.dll" =Wed, 06-Jan-2021 16:42:45 GMT; Max-Age=60;	
path=/ Last-Modified: Wed, 06 Jan 2021 16:41:45 GMT Keep-Alive: timeout=6, max=100 Connection: Keep-Alive		
Transfer-Encoding: chunked Content-Type: application/octet-stream	¥	
MZ@@@@@@		
\$WTWTWTWTWTWT TWTWWTWT	wTwTwTwU.SwTwTwTwT. .LJE Р	W •
1 <mark>client</mark> pkt, 140 server pkts, 1 turn.		
Entire conversation (192 kB) • Show and s	ave data as ASCII The Stream 3	3
Find:	Find	<u>N</u> ext
⊘ Help	Filter Out This Stream Print Save as Back × C	ose

Figure 9. Indicators of a DLL file returned from seo.udaipurkart[.]com.Export this DLL from the pcap by using the menu path: *File --> Export Objects --> HTTP,* as shown in Figure 10. As always, we recommend you do not export this file in a Windows environment, since the DLL is Windows-based malware.



Figure 10. Exporting the Emotet DLL from our first pcap. The SHA256 hash for this extracted DLL is: Emotet C2 traffic is encoded data sent using HTTP POST requests. You can easily find these requests in Wireshark using the following filter:

http.request.method eq POST

The results are shown in Figure 11.

• Example-1-2021-01-06-Emotet-infection.pcap - + ×									
File <u>E</u> dit <u>View Go</u> <u>Capture A</u> nalyze <u>Statistics</u> Telephony <u>Wireless</u> <u>T</u> ools <u>H</u> elp									
$\blacksquare \blacksquare \boxtimes \odot \models \blacksquare \blacksquare \blacksquare \blacksquare \blacksquare \blacksquare \blacksquare \blacksquare \blacksquare \blacksquare$									
http.request.method eq POST									
Time	Dst	port	Host	Info		^			
2021-01-06 16:42:34	5.2.136.90	80	5.2.136.90	POST	/7u0e9j2avwlvnuynyo/szcm27k/fzb06				
2021-01-06 16:42:42	5.2.136.90	80	5.2.136.90	POST	/ko5ezxmguvv/p8d4003oiu/utkdae7r/				
2021-01-06 16:42:45	5.2.136.90	80	5.2.136.90	POST	/vwst360x8syxks325x/26dtqu31wzhmw				
2021-01-06 16:42:48	167.71.4.0	8080	167.71.4.0:8080	POST	/va9j7/5clu9bdp5xth2a/4pq9nord/hu				
2021-01-06 16:42:49	5.2.136.90	80	5.2.136.90	POST	/mro86v6nvs42/ HTTP/1.1				
2021-01-06 16:42:52	167.71.4.0	8080	167.71.4.0:8080	POST	/3rkiie36/ HTTP/1.1				
2021-01-06 16:42:52	5.2.136.90	80	5.2.136.90	POST	/raet/u6tpsbdmo5g7crj4f/8l720ln/l				
2021-01-06 16:42:56	167.71.4.0	8080	167.71.4.0:8080	POST	/ves4up2v2n5qjq5rl/i8ldtkhnklo/ H				
2021-01-06 16:43:00	167.71.4.0	8080	167.71.4.0:8080	POST	/tvvzt3/ai6wn02o2/9oeb81/ HTTP/1.				
2021-01-06 16:58:34	5.2.136.90	80	5.2.136.90	POST	/jw5cumz32djf/ HTTP/1.1				
2021-01-06 16:58:38	5.2.136.90	80	5.2.136.90	POST	/xqvsf/t2m11tvzqq/ HTTP/1.1				
2021-01-06 16:58:43	167.71.4.0	8080	167.71.4.0:8080	POST	/titI9YcL5H HTTP/1.1 (applicatio				
2021-01-06 16:58:48	167.71.4.0	8080	167.71.4.0:8080	POST	/Mz0FddwPYSreH HTTP/1.1 (applica				
2021-01-06 17:14:04	5.2.136.90	80	5.2.136.90	POST	/hbwubd1ghq2/6mgzkg6dn5to/6lx9qp0				
2021-01-06 17:14:09	5.2.136.90	80	5.2.136.90	POST	/ch7yy6wqvi5hxkoka/pu5xvenbb9n9r3				
2021-01-06 17:14:16	167.71.4.0	8080	167.71.4.0:8080	POST	/8ez5ny6v9lt2j2n/8nozgtj00oz8is9k				
2021-01-06 17:30:26	5.2.136.90	80	5.2.136.90	POST	/0ie7j/6ee132k6oio/ HTTP/1.1				
2021-01-06 17:45:43	5.2.136.90	80	5.2.136.90	POST	/oy0zvkaaa2/q6dvsdask1ptwo2123/15				
2021-01-06 18:01:35	5.2.136.90	80	5.2.136.90	POST	/h3cc0hv2llqou1b8/towc8ksx/hsa6q8				
2021-01-06 18:17:20	5.2.136.90	80	5.2.136.90	POST	/xrn581egq/ur2rd8/ HTTP/1.1				
2021-01-06 18:17:24	5.2.136.90	80	5.2.136.90	POST	/c3855W62/xnTgT1141s35u295y/bm04v				
2021-01-06 18:17:27	5.2.136.90	80	5.2.136.90	POST	/pvbznniyiti9e/izh4ca/ HTTP/1.1				
2021-01-06 18:17:31	167.71.4.0	8080	167.71.4.0:8080	POST	/n6q1/1D1anp/98wZr2Krwmm4/ HTTP/1				
2021-01-06 18:17:34	167.71.4.0	8080	167.71.4.0:8080	POST	/v9bb0/b02tqasatzorr5rep01/ HTTP/	-			

Figure 11. Filtering for HTTP POST requests in our first pcap. In our first pcap, Emotet C2 traffic consists of HTTP POST requests to:

- 5.2.136[.]90 over TCP port 80
- 167.71.4[.]0 over TCP port 8080

Emotet generates two types of HTTP POST requests for its C2 traffic. The first type of POST request ends with HTTP/1.1. The second type of POST request ends with HTTP/1.1 (application/x-www-form-urlencoded).

Follow the TCP stream for the initial HTTP request to 5.2.136[.]90 at 16:42:34 UTC to see an example of the first type of C2 POST request, as shown in Figure 12.



Figure 12. The first type of HTTP POST request for Emotet C2 traffic.

Figure 12 shows this POST request sends approximately 6 KB of form-data that appears to be an encoded or encrypted binary. Scroll down to the HTTP response to see encoded data returned from the server. Figure 13 shows the start of this encoded data.

Wireshark · Follow TCP Stream (tcp.stream eq 10) · Example-1-2021-01-06-Emotet-infection.pcapHTTP/1.1 200 OK Server: nginx Date: Wed, 06 Jan 2021 16:42:39 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding f67 R...0.....Q.h..4h.x.Qr.....R....0_..Q..\$.Qa..].w..~...A.o...~..v. ![...j....v.W.v.B.yF&..)....87...|>...+(..!'.....=2.:.2{b.i.j...i..3....H.. h&lh.T... 7...&q\.n]..F.....WI....3\....Y..]..c.i..z.f..s..l..A. 0....Y.f.".E9.....<..o....).n,.G..A.Ğ..U.v....|....>iH.@....e.g)..N...H.....tG.....l. 8....7C.-.Y...sNw..k.s..G..Qq/6.....J..... 0..K.:.6....5.&..WG_x.g.7.].v...=.U=b"W.....=.:..u!\$\.....7......|.b[t.W......!.*...u..........8.R. 1/....0.C.P.k....*.N..A.E.r..0.^...4..q...gz...`.3".nj...5.....u>a!...P0...P9.fP..0..). 4..2....b..:Ck..js.....[...]. .Su..n.P..!#0.=.Mf.A.~.%.5.R}i...9..[.Q.FV.:...+.|. {.r.V>..."....W=Rh.w:.I.`\$3.}Y..d.P...3....2 s.....gV.J~@.1?...g.%.J".._p......R=L.#...-.X..U.a....D.#.Z....N..[...?jd...C...W...!...h...|...8 x.R..T..y...jA=._r....2.....>....c...]...h6..7-o.f.Q~.Y 32 client pkts, 1,092 server pkts, 9 turns. Entire conversation (1,520 kB) Show and save data as ASCII -Stream 10 ‡ Find Next Find: Help Filter Out This Stream Print Save as... Back × Close

Figure 13. Encoded data returned from the server in response to the HTTP POST request. This type of encoded or encrypted data is how Emotet botnet servers exchange data with an infected Windows host. This is also the channel Emotet uses to update the Emotet DLL and drop follow-up malware.

The second type of HTTP POST request for Emotet C2 traffic looks noticeably different than the first type. Use the following filter in Wireshark to easily find the second type of HTTP POST request:

urlencoded-form

This should return two HTTP POST requests to 167.71.4[.]0 over TCP port 8080, as shown in Figure 14.

+ Example-1-2021-01-06-Emotet-infection.pcap - + ×						
<u>File Edit View Go</u> Capture	<u>A</u> nalyze <u>S</u> tatistics	Telepho	ony <u>W</u> ireless <u>T</u> ools <u>H</u> el	р		
$\blacksquare \blacksquare \boxtimes \odot \models \blacksquare \blacksquare \boxtimes \boxtimes \land \Leftrightarrow \Rightarrow \diamondsuit \models \clubsuit \models \blacksquare \blacksquare \blacksquare \blacksquare$						
urlencoded-form					🛛 🖃 🔹 basic	basic+ basic+dns
Time	Dst	port	Host	Info		
2021-01-06 16:58:43	167.71.4.0	8080	167.71.4.0:8080	POST /titI9YcL5	H HTTP/1.1 (a	application/x-w
2021-01-06 16:58:48	167.71.4.0	8080	167.71.4.0:8080	POST /MZ0FddwPY	SreH HTTP/1.1	(application/
4						►.

Figure 14. Filtering for the second type of HTTP POST request in Emotet C2 traffic. Follow the TCP stream for the first of these two HTTP POST requests at 16:58:43 UTC. Review the traffic. The results are shown in Figure 15.

Wireshark · Follow TCP St	ream (tcp.stream eq 34) · Exampl	e-1-2021-01-06-Emotet-i	nfection.pcap	- + ×
POST /titI9YcL5H HTTP/1.1 Referer: http://167.71.4.0/titI9Yc Content-Type: application/x-www-fo DNT: 1 User-Agent: Mozilla/4.0 (compatibl Host: 167.71.4.0:8080 Content-Length: 225 Connection: Keep-Alive Cache-Control: no-cache titI9YcL5H=AW7yce4Jdh7V15Df3n5b83x yNgrbam0CQNuJ0D7q2UfiGmqPd%2BJ2Yem kvAsl8pFQ%3D%3DHTTP/1.1 200 OK	-5H 'm-urlencoded 2; MSIE 7.0; Windows NT : 62BMqFtzwEFVrIXbXbkXx6dJJ 3HNpWLL15Q1UZDDXhpWhULVU	10.0; WOW64; Tride ZqkMz75f4VTslkhnTZ JOnE2%2FtAyS86KkEh	ent/7.0; .NET4.0C; ZeILlDA5A3o0nVyUu6 iVNm2xzS2RDRrjxddD	.NET4.0E) zr%2B8%2Fiv1 YCz5izYbwsUq
Date: Wed, 06 Jan 2021 16:58:43 GM Content-Type: text/html; charset=U Content-Length: 148 Connection: keep-alive	r FF-8			
0D.T>% 9aLq./6.BU'.}Q\.aj	#\t^!. 5XNK8	.F.z4H\JI	Fd <t.l< th=""><td></td></t.l<>	
1 <mark>client</mark> pkt, 1 server pkt, 1 turn.				
Entire conversation (852 bytes)	Show and save data as ASCII	•		Stream 34 ‡
Find:				Find <u>N</u> ext
€ Help		Filter Out This Stream	Print Save as	Back × <u>C</u> lose

Figure 15. TCP stream for the second type of HTTP POST request in Emotet C2 traffic. As shown in Figure 15, some of the data sent in the POST request is encoded as a base64 string with some URL encoding. For example, %2B is used for a + symbol, %2F represents / and %3D is used for =.

Data sent in response from the server is encoded or otherwise encrypted.

Our first pcap has no follow-up malware or other significant activity.

The only other activity is repeated connection attempts to 46.101.230[.]194 over TCP port 443. You can easily spot this activity by filtering on TCP SYN segments that are retransmissions. Use the following Wireshark filter:

tcp.analysis.retransmission and tcp.flags eq 0x0002

The results are shown in Figure 16.

• Example-1-2021-01-06-Emotet-infection.pcap - + ×									
<u>File Edit View Go Capture Analyze Statistics Telephony Wireless Tools H</u> elp									
	/ = / © = 1 × 0 + + + + + = = = 0 = 1								
tcp.analysis.retransmission an	d tcp.flags eq 0x0002			🛛 🗔 🔹 🔶 basic 🗆 basic+ 🗆 basic+dns					
Time	Dst	port	Info	<u> </u>					
2021-01-06 16:42:43	46.101.230.194	443	[TCP Retransmission]	49785 → 443 [SYN] Seq=0 Win=0					
2021-01-06 16:42:44	46.101.230.194	443	[TCP Retransmission]	49785 → 443 [SYN] Seq=0 Win=0					
2021-01-06 16:42:45	46.101.230.194	443	[TCP Retransmission]	49785 → 443 [SYN] Seq=0 Win=0					
2021-01-06 16:42:45	46.101.230.194	443	[TCP Retransmission]	49785 → 443 [SYN] Seq=0 Win=0					
2021-01-06 16:42:46	46.101.230.194	443	[TCP Retransmission]	49786 → 443 [SYN] Seq=0 Win=0					
2021-01-06 16:42:47	46.101.230.194	443	[TCP Retransmission]	49786 → 443 [SYN] Seq=0 Win=0					
2021-01-06 16:42:48	46.101.230.194	443	[TCP Retransmission]	49786 → 443 [SYN] Seq=0 Win=0					
2021-01-06 16:42:48	46.101.230.194	443	[TCP Retransmission]	49786 → 443 [SYN] Seq=0 Win=0					
2021-01-06 16:42:50	46.101.230.194	443	[TCP Retransmission]	49789 → 443 [SYN] Seq=0 Win=0					
2021-01-06 16:42:51	46.101.230.194	443	[TCP Retransmission]	49789 → 443 [SYN] Seq=0 Win=0					
2021-01-06 16:42:52	46.101.230.194	443	[TCP Retransmission]	49789 → 443 [SYN] Seq=0 Win=0					
2021-01-06 16:42:52	46.101.230.194	443	[TCP Retransmission]	49789 → 443 [SYN] Seq=0 Win=0					
2021-01-06 16:42:54	46.101.230.194	443	[TCP Retransmission]	49792 → 443 [SYN] Seq=0 Win=0					
2021-01-06 16:42:55	46.101.230.194	443	[TCP Retransmission]	49792 → 443 [SYN] Seq=0 Win=0					
2021-01-06 16:42:55	46.101.230.194	443	[TCP Retransmission]	49792 → 443 [SYN] Seq=0 Win=0					
2021-01-06 16:42:56	46.101.230.194	443	[TCP Retransmission]	49792 → 443 [SYN] Seq=0 Win=0					
2021-01-06 16:58:38	46.101.230.194	443	[TCP Retransmission]	49813 → 443 [SYN] Seq=0 Win=0					
2021-01-06 16:58:39	46.101.230.194	443	[TCP Retransmission]	49813 → 443 [SYN] Seq=0 Win=(
2021-01-06 16:58:40	46.101.230.194	443	[TCP Retransmission]	49813 → 443 [SYN] Seq=0 Win=0					
2021-01-06 16:58:41	46.101.230.194	443	[TCP Retransmission]	49813 → 443 [SYN] Seq=0 Win=0					
2021-01-06 17:14:10	46.101.230.194	443	[TCP Retransmission]	49821 → 443 [SYN] Seq=0 Win=0					
2021-01-06 17:14:11	46.101.230.194	443	[TCP Retransmission]	49821 → 443 [SYN] Seq=0 Win=0					
2021-01-06 17:14:11	46.101.230.194	443	[TCP Retransmission]	49821 → 443 [SYN] Seq=0 Win=0					
2021-01-06 17:14:12	46.101.230.194	443	ITCP Retransmission1	49821 → 443 [SYN] Seg=0 Win=					

Figure 16. Filtering on retransmissions of TCP SYN segments in Wireshark. An Internet search on 46.101.230[.]194 should reveal this IP address has been used for Emotet C2 activity.

The remaining traffic in the pcap is system traffic generated by a Microsoft Windows 10 host.

In our next pcap, we examine an Emotet infection with spambot activity.

Example 2: Emotet With Spambot Traffic, Part 1

Open *Example-2-2021-01-05-Emotet-with-spambot-traffic-part-1.pcap* in Wireshark and use a basic web filter, as shown in Figure 17.

Example-2-2021-01-05-Emotet-with-spambot-traffic-part-1.pcap - + ×								
<u>File Edit View Go</u> Capture	<u>File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help</u>							
	/ I () () () () () () () () () (
http.request or tls.handshake.type eq 1) and !(ssdp)								
Time	Dst	port	Host	Info				
2021-01-05 19:47:13	5.45.114.71	443	obob.tv	Client Hello				
2021-01-05 19:47:15	52.114.132.22	443	self.events.data.micr	Client Hello				
2021-01-05 19:47:16	52.109.88.35	443	nexusrules.officeapps	Client Hello				
2021-01-05 19:47:53	204.79.197.200	443	www.bing.com	Client Hello				
2021-01-05 19:48:48	185.225.36.38	80	infoprocenter.com	GET /wp-admin/MSInfo/ HTTP/1.1				
2021-01-05 19:48:48	144.217.79.200	80	miprimercamino.com	GET /cgi-bin/AJ09AzChrK/ HTTP/				
2021-01-05 19:48:58	125.0.215.60	80	125.0.215.60	POST /bgi93n6v5xtgj/k3i3a/u46l				
2021-01-05 19:49:06	125.0.215.60	80	125.0.215.60	POST /vs7e7ht0yjohr8/qag42y9/c				
2021-01-05 19:49:10	125.0.215.60	80	125.0.215.60	POST /avkbtr3s7rxvxz7a1g/puv2i				
2021-01-05 19:49:11	52.109.8.20	443	nexusrules.officeapps	Client Hello				
2021-01-05 19:49:11	104.236.52.89	8080	104.236.52.89:8080	POST /krhp52joegfy8i7b/lkc1rvr				
2021-01-05 19:49:14	125.0.215.60	80	125.0.215.60	POST /ylcp/gjga2kgpe/5ayyt/ HT				
2021-01-05 19:49:15	52.109.8.20	443	nexusrules.officeapps	Client Hello				
2021-01-05 19:49:15	104.236.52.89	8080	104.236.52.89:8080	POST /6y9ra6iqzi302y7vrna/sihg				
2021-01-05 19:49:19	125.0.215.60	80	125.0.215.60	POST /ngslvujkk0hi/yhky2nwmv/i				
2021-01-05 19:49:19	104.236.52.89	8080	104.236.52.89:8080	POST /tn9gpiuk/zsit42fjx98m4rr				
2021-01-05 19:49:19	104.236.52.89	8080	104.236.52.89:8080	POST /tn9gpiuk/zsit42fjx98m4rr				
2021-01-05 19:49:25	125.0.215.60	80	125.0.215.60	POST /het5/jd55lt85h/h9gu0nw8n				
2021-01-05 19:49:25	104.236.52.89	8080	104.236.52.89:8080	POST /z1x928hdy3f92jatt/dytq2q				
2021-01-05 19:49:38	125.0.215.60	80	125.0.215.60	POST /yajtvsgegx08cw/ HTTP/1.1				
2021-01-05 19:51:28	52.114.128.43	443	v20.events.data.micro	Client Hello				
2021-01-05 19:51:29	52.114.128.43	443	v10.events.data.micro	Client Hello				
2021-01-05 19:51:46	52.114.20.14	443	self.events.data.micr	Client Hello				
2021-01-05 19:55:14	13.107.246.13	443	pt1.store.microsoft.c	Client Hello				

Figure 17. Traffic from the second pcap filtered in Wireshark using our basic web filter. Similar to our first example, we receive some HTTP GET requests before Emotet C2 traffic. These GET requests are attempts to download the initial Emotet DLL over web traffic. The first frame in the column display shows HTTPS traffic to obob[.]tv, which was probably a web request for the initial Emotet DLL, because <u>this domain was reported as hosting an Emotet</u> <u>binary on Jan. 5, 2021</u>, the same date as the traffic in our pcap.

Follow the TCP stream for the HTTP GET request to miprimercamino[.]com to confirm it returned an Emotet DLL. You should see indicators similar to Figure 9 from our first pcap. We can export the Emotet DLL returned from miprimercamino[.]com, as shown in Figure 18.

·	Example-2-20	021-0	01-0	5-Emote	t-with-spambot-traffi	c-part-1.pcap	- + ×
<u>File</u> <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture	<u>Analyze</u> <u>Statistics</u>	Tele	epho	n <u>y W</u> ire	less <u>T</u> ools <u>H</u> elp		
<u>O</u> pen	Ctrl+O		-			· Export · UTTD obj	at lie
Open <u>R</u> ecent	•		-	•	WITESTIATE	C · Export · HITP obje	
Merge		(qr		Packet *	Hostname	Content Type	Filename
Import from Hoy Dump			роі	170	infoprocenter.com	text/html	,309 bytes MSInfo
Import from Hex Dump			44	369	miprimercamino.com	application/octet-str	eam 201 kB AJ09AzChrK
Close	Ctrl+W	12	44	383	125.0.215.60	multipart/form-data	6,484 bytes 3t2getkvxqi71
Save	Ctrl+S	, 200	44	580 ∢	125.0.215.60	text/html	204 kB 3t2getkvxqi71~
Save <u>A</u> s	Ctrl+Shift+S	38	80	Text Filte	er:		
File Set	Þ	200	80	@Help			Save All × Close Save
Export Specified Packets		5	80		UILLUIU,		
Export Packet Dissections	•)	80	125	.0.215.6	POST /avkbt	r3s7rxvxz7a1g/puv2i
Export Packet Bytes	Ctrl+Shift+X	20	443	3 nexi		ps Client Hell	0 2joegfy8j7b/lkc1ryr
Export PDUs to File)	80	125	.0.7.5.60	POST /ylcp/	gjga2kgpe/5ayyt/ HT
			443	B nexi	us les.officeap	ps… Client Hell	0
Export TLS Session Keys		39	808	30 104	86.52.89:8080	POST /6y9ra	6iqzi302y7vrna/sihg
Export Objects	•	1	DICC	ом	0.215.60	POST /ngslv	ujkkOhi/yhky2nwmv/i
<u>P</u> rint	Ctrl+P	ł	нттр	P	236.52.89:8080	POST /tn9gp	iuk/zsit42fjx98m4rr
Quit	Ctrl+Q	I	MF		.0.215.60	POST /het5/	jd55lt85h/h9gu0nw8n
2021-01-05 19:49:25	104.236.52.8	9	SMB		.236.52.89:8080	POST /z1x92	8hdy3f92jatt/dytq2q
2021-01-05 19:49:38	125.0.215.60	1	IFTP		.0.215.60	POST /yajtv	sgegx08cw/ HTTP/1.1
2021-01-05 19:51:28	52.114.128.4				.events.data.mic	ro… Client Hell	0
2021-01-05 19:51:29	52.114.128.4	43	443		events.data.mic	ro… Client Hell	0
2021-01-05 19:51:40	13 107 246 1	+ 1 3	443	s sell	store microsoft	c Client Hell	0
4	10.107.240.1	10	44.	, nrt	STOLE HITCLOSULE	. C CITCHE HEIT	•

Figure 18. Exporting the Emotet DLL from the pcap. The SHA256 hash for the extracted DLL from our second pcap is:

963b00584d8d63ea84585f7457e6ddcac9eda54428a432f388a1ffee21137316

Again, we find two types of HTTP POST requests for Emotet C2 traffic. To filter for each type of Emotet C2 HTTP POST request, use the following Wireshark filters:

- First type: http.request method eq POST and !(urlencoded-form)
- Second type: urlencoded-form

Follow TCP streams for the HTTP POST requests returned by these filters and confirm they follow the same patterns seen in our first pcap.

After reviewing some examples of Emotet C2 traffic from this pcap, let's move on to the spambot activity.

In this example, our infected host was turned into a spambot, so we also have SMTP traffic. The spambot SMTP traffic is encrypted, but we can easily find it by using our basic web filter and scrolling down the column display.

At 20:06:20 UTC, the pcap starts showing SSL/TLS traffic to TCP ports associated with the SMTP email protocol, like TCP ports 25, 465 and 587, as shown in Figure 19.

•	Example-2-2021-01	-05-Emotet-with-spambot-traffic-part-	-1.pcap – + ×
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture	Analyze Statistics Telepl	nony <u>W</u> ireless <u>T</u> ools <u>H</u> elp	
	🙆 l 🔍 🔶 🌩 象 🖗 🖷		
(http.request or tls.handshak	e.type eq 1) and !(ssdp)		🛛 📼 🝷 🔶 basic 🗆 basic+ 🗆 basic+dns
Time	Dst	port Host	Info
2021-01-05 20:06:14	104.236.52.89	8080 104.236.52.89:8080	POST /kSiN3pL7eYh HTTP/1.1
2021-01-05 20:06:20	172.217.195.109	465	Client Hello
2021-01-05 20:06:20	108.177.9.109	465	Client Hello
2021-01-05 20:06:20	212.127.35.17	465	Client Hello
2021-01-05 20:06:20) 194.25.134.110	465	Client Hello
2021-01-05 20:06:20	67.195.228.95	587	Client Hello
2021-01-05 20:06:21	212.227.15.142	25	Client Hello
2021-01-05 20:06:21	213.165.67.124	587	Client Hello
2021-01-05 20:06:21	195.235.200.178	587	Client Hello
2021-01-05 20:06:22	2 194.25.134.110	465	Client Hello
2021-01-05 20:06:22	2 172.217.195.109	465	Client Hello
2021-01-05 20:06:22	2 172.217.195.109	465	Client Hello
2021-01-05 20:06:22	2 172.217.195.109	465	Client Hello
2021-01-05 20:06:22	2 172.217.195.109	465	Client Hello
2021-01-05 20:06:22	2 172.217.195.109	465	Client Hello
2021-01-05 20:06:22	2 172.217.195.109	465	Client Hello
2021-01-05 20:06:23	3 178.238.37.174	25	Client Hello
2021-01-05 20:06:23	3 202.168.255.44	25	Client Hello
2021-01-05 20:06:20	b 195.22.8.84	587	Client Hello
2021-01-05 20:06:28	3 172.217.195.109	587	Client Hello
2021-01-05 20:06:29	81.95.97.100	587	Client Hello
2021-01-05 20:06:29	23.29.122.187	465	Client Hello
2021-01-05 20:06:29	9 192.185.131.139	465	Client Hello
2021-01-05 20:06:30	212.227.17.168	587	Client Hello
2021-01-05 20:06:30) 103.74.54.6	465	Client Hello
2021-01-05 20:06:30) 173.201.192.101	25	Client Hello
2021-01-05 20:06:33	3 198.71.240.9	587	Client Hello
2021-01-05 20:06:39	85.13.141.102	25	Client Hello
<u>2021_01_05_20+06+40</u>	65 00 2/8 136	25	Client Hello

Figure 19. Using the basic web filter and scrolling through the column display to find spambot traffic.

We can filter on smtp to find some of the SMTP commands before encrypted SMTP tunnels are established. Figure 20 shows the results.

▼	Example-2-2021-0	1-05-Emotet-v	vith-spambot-traffic-part-1.pcap – + ×
<u>File Edit View Go</u> Captu	e <u>A</u> nalyze <u>S</u> tatistics Tele	ohon <u>y</u> <u>W</u> ireles	is <u>T</u> ools <u>H</u> elp
	। 🙆 🔍 🔶 🌩 ≽		ē = 1 🏥
smtp			🛛 🗔 🔹 🔶 basic 🗆 basic+ 🗆 basic+dns
Time	Dst	port Ir	nfo 💳
2021-01-05 20:06:	20 10.1.5.101	49735 S	: 220 DM5PR16CA0045.outlook.office365.com Micro
2021-01-05 20:06:	20 40.97.128.210	587 C	: EHLO [10.0.0.3]
2021-01-05 20:06:	20 10.1.5.101	49728 S	: 220 smtp.mail.yahoo.com ESMTP ready
2021-01-05 20:06:	20 67.195.228.95	587 C	: EHLO [10.0.0.3]
2021-01-05 20:06:	20 10.1.5.101	49735 [TCP Spurious Retransmission] S: 220 DM5PR16CA00
2021-01-05 20:06:	20 10.1.5.101	49735 [TCP Spurious Retransmission] S: 220 DM5PR16CA00
2021-01-05 20:06:	20 10.1.5.101	49735 S	: 250-DM5PR16CA0045.outlook.office365.com Hello
2021-01-05 20:06:	20 40.97.128.210	587 C	: STARTTLS
2021-01-05 20:06:	20 10.1.5.101	49728 S	: 250-smtp404.mail.gq1.yahoo.com Hello [10.0.0.
2021-01-05 20:06:	20 67.195.228.95	587 C	: STARTTLS
2021-01-05 20:06:	20 10.1.5.101	49735 [TCP Spurious Retransmission] S: 250-DM5PR16CA004
2021-01-05 20:06:	20 10.1.5.101	49735 S	: 220 2.0.0 SMTP server ready
2021-01-05 20:06:	20 40.97.128.210	587 C	: \026\003\001\000\$\001\000\000\$\003\003\$~\$\031
2021-01-05 20:06:	20 10.1.5.101	49732 S	: 220 web.de (mrweb101) Nemesis ESMTP Service re
2021-01-05 20:06:	20 213.165.67.124	587 C	: EHLO [10.0.0.3]
2021-01-05 20:06:	20 10.1.5.101	49733 S	: 220 kundenserver.de (mreue010) Nemesis ESMTP 🔙
2021-01-05 20:06:	20 212.227.15.142	25 C	: EHLO [10.0.0.3]
2021-01-05 20:06:	20 10.1.5.101	49735 [TCP Spurious Retransmission] S: 220 2.0.0 SMTP
2021-01-05 20:06:	20 10.1.5.101	49728 S	: 220 2.0.0 Ready to start TLS
2021-01-05 20:06:	20 10.1.5.101	49723 S	: 220 mail.notin.net ESMTP MSA MDaemon 20.0.3; 💻
2021-01-05 20:06:	20 195.235.200.178	587 C	: EHLO [10.0.0.3]
2021-01-05 20:06:	20 10.1.5.101	49735 [TCP Spurious Retransmission] S: 220 2.0.0 SMTP :
2021-01-05 20:06:	20 10.1.5.101	49735 S	: 200813231849Z\027 2208142
2021-01-05 20:06:	20 10.1.5.101	49735 [TCP Spurious Retransmission] S:
2021-01-05 20:06:	20 10.1.5.101	49735 S	
1 2021 01 0E 201061	00 10 1 E 101	40705 0	

Figure 20. Filtering for SMTP traffic in our second pcap.

We can sometimes find unencrypted SMTP from spambot traffic generated by an Emotetinfected Windows host. Unencrypted SMTP will reveal its message content, but the volume of encrypted SMTP from a spambot host is far greater than the volume of unencrypted SMTP. Therefore, most of the spambot messages from an Emotet-infected host are hidden within the encrypted traffic.

In this example, you should only see encrypted SMTP traffic.

But our next example is later from this same infection, when we finally saw some unencrypted SMTP.

Example 3: Emotet With Spambot Traffic, Part 2

Open *Example-3-2021-01-05-Emotet-with-spambot-traffic-part-2.pcap* in Wireshark and use a basic web filter, as shown in Figure 21.

-	• Example-3-2021-01-05-Emotet-with-spambot-traffic-part-2.pcap - + ×							
<u>F</u> ile <u>E</u> dit <u>V</u> iew	<u>Go</u> <u>C</u> apture <u>/</u>	<u>A</u> nalyze <u>S</u> tatistics Telep	hony <u>N</u>	(ireless <u>T</u> ools <u>H</u> elp				
	/ I () () () () () () () () () (
📕 (http.request or tls.handshake.type eq 1) and !(ssdp)								
Time		Dst	port	Host	Info	^		
2021-01-05	5 20:16:01	172.217.195.108	587		Client Hello			
2021-01-05	5 20:16:01	172.217.195.108	587		Client Hello			
2021-01-05	5 20:16:02	98.136.96.80	465		Client Hello			
2021-01-05	5 20:16:02	173.231.241.171	465		Client Hello			
2021-01-05	5 20:16:09	46.18.134.131	587		Client Hello			
2021-01-05	5 20:16:09	162.214.70.141	465		Client Hello			
2021-01-05	5 20:16:09	213.209.1.144	587		Client Hello			
2021-01-05	5 20:16:10	195.3.96.71	25		Client Hello			
2021-01-05	5 20:16:12	43.225.55.182	25		Client Hello			
2021-01-05	5 20:16:15	108.167.137.28	25		Client Hello			
2021-01-05	5 20:16:25	164.160.91.17	25		Client Hello			
2021-01-05	5 20:16:31	162.219.249.113	25		Client Hello			
2021-01-05	5 20:16:35	162.214.68.171	8080	162.214.68.171:8080	POST /vNcfHx0yD	M		
2021-01-05	5 20:16:36	162.214.70.141	465		Client Hello			
2021-01-05	5 20:16:42	108.167.137.28	25		Client Hello			
2021-01-05	5 20:16:45	103.21.59.169	25		Client Hello			
2021-01-05	5 20:16:57	107.180.108.7	25		Client Hello			
2021-01-05	5 20:17:00	162.214.68.171	8080	162.214.68.171:8080	POST /oefPeUB4q	5		
2021-01-05	5 20:17:02	162.214.70.141	465		Client Hello			
2021-01-05	5 20:17:03	82.118.225.196	7080	82.118.225.196:7080	POST /J8JVUHb6J	9		
2021-01-05	5 20:17:04	52.185.211.133	443	settings-win.data.microsoft.co	m Client Hello			
2021-01-05	5 20:17:04	13.107.5.88	443	evoke-windowsservices-tas.msed	ge… Client Hello			
2021-01-05	5 20:17:12	103.21.59.169	25		Client Hello			
2021-01-05	5 20:17:22	213.94.78.178	465		Client Hello			
2021-01-05	5 20:17:23	64.233.169.109	25		Client Hello			
1 1001 01 05		010 007 17 160	E07		Client Helle	• •		

Figure 21. Traffic from the third pcap filtered in Wireshark using our basic web filter. In this pcap, we still see HTTP POST requests for Emotet C2 traffic, at least twice each minute. We can also find encrypted spambot activity similar to our previous pcap.

Spambot activity frequently generates a large amount of traffic. This pcap consists of 4 minutes and 42 seconds of spambot activity from the infected Windows host, and it's over 21 MB of traffic.

We can quickly identify any unencrypted SMTP traffic by using the following Wireshark filter:

smtp.data.fragment

Figure 22 shows the results of this filter for our third pcap. The filter reveals five examples of Emotet malspam generated by the infected Windows host.

-	Example-3-2021-0	1-05-En	motet-with-spambot-traffic-part-2.pcap – + ×				
<u>File E</u> dit <u>V</u> iew <u>Go</u> <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Telephony <u>W</u> ireless <u>T</u> ools <u>H</u> elp							
/ = / ® = * × * < + + * * * * = = = * *							
smtp.data.fragment			🛛 🗔 🔹 🍦 basic 🗆 basic+ 🗆 basic+dns				
Time	Dst	port	Info				
2021-01-05 20:16:05	202.134.60.178	587	from: "daikei-koumuten@gaia.eonet.ne.jp" <kammy.tang@subu< td=""></kammy.tang@subu<>				
2021-01-05 20:19:38	193.252.22.84	25	from: "Juan Diaz <jdiaz@thy.com>" <ozdemir.nuran@orange.f< td=""></ozdemir.nuran@orange.f<></jdiaz@thy.com>				
2021-01-05 20:19:47	193.252.22.84	25	from: "Green Mountains Laboratory Inc <office@gml-v.com>'</office@gml-v.com>				
2021-01-05 20:19:51	193.252.22.84	25	from: "Green Mountains Laboratory Inc <office@gml-v.com>'</office@gml-v.com>				
2021-01-05 20:19:54	193.252.22.84	25	from: "Gladisbel Miranda <gmiranda@randgeng.com>" <ozdemi< td=""></ozdemi<></gmiranda@randgeng.com>				
•			•				

Figure 22. Filtering for indicators of unencrypted SMTP from spambot traffic.

Follow the TCP stream for the last email from: "Gladisbel Miranda at 20:19:54 UTC. Examine what these messages look like, as shown in Figure 23.

```
Wireshark · Follow TCP Stream (tcp.stream eq 266) · Example-3-2021-01-05-Emotet-with-spambot-traffic-part-2.pcap - + ×
220 mwinf5d09 ME ESMTP server ready
EHLO [10.0.0.3]
250-mwinf5d09 hello [173.66.146.112], pleased to meet you
250-HELP
250-AUTH LOGIN PLAIN
250-SIZE 44000000
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 OK
AUTH PLAIN AG96ZGVtaXIubnVyYW5Ab3JhbmdlLmZyAExlbWVzbGU20CE=
235 2.7.0 ... authentication succeeded
MAIL FROM: <ozdemir.nuran@orange.fr>
250 2.1.0 <ozdemir.nuran@orange.fr> sender ok
RCPT TO: <SBARROS@THY.COM>
250 2.1.5 <sbarros@thy.com> recipient ok
DATA
354 enter mail, end with "." on a line by itself
Date: Tue, 05 Jan 2021 20:19:35 +0000
From: "Juan Diaz <JDIAZ@THY.COM>" <ozdemir.nuran@orange.fr>
To: "Stephanie de alves Barros" <SBARROS@THY.COM>
Subject: W-9 Stephanie de alves Barros
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="---=_NextPart_006_9169_385159614.3532224132"
-----= NextPart 006 9169 385159614.3532224132
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: quoted-printable
<html>
<head>
<meta http-equiv=3DContent-Type content=3D"text/html; charset=3Dutf-8">
</head>
<bodv>
Morning Stephanie de alves Barros, <br>
<br>
w-9<br>
<br>
<br>
<br>
THY<br>>=0Dwww,THY,COM
</body>
</html>
-----= NextPart 006 9169 385159614.3532224132
Content-Type: application/msword; name="W-9 Form.doc"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="W-9 Form.doc"
486 client pkts, 22 server pkts, 42 turns.
Entire conversation (638 kB)
                               -
                                                         Ŧ
                                                                       Stream 266 🗘
                                    Show and save data as ASCII
Find:
                                                                           Find Next
                                       Filter Out This Stream
 Help
                                                       Print
                                                             Save as...
                                                                      Back
                                                                            × Close
```

Figure 23. TCP stream for an example of Emotet malspam from our third pcap.

We can export these five items of Emotet malspam by using the menu path *File --> Export Objects --> IMF,* as shown in Figure 24.

	Example-3-2021-01-05-Emotet-with-spambot-traffic-part-2.pcap – + 2							- + ×				
F	ile <u>E</u> dit <u>V</u> iew	<u>G</u> o <u>C</u> apture	<u>A</u> nalyze	<u>S</u> tatistics	Telep	ohony <u>V</u>	<u>V</u> ireless <u>T</u> ools <u>H</u> elp					
Г	Open		Ctr	rl+O								
ſ	Open Recent			•		*	Wireshar	·k · Ехроі	rt · IMF obj	ect list		- + ×
4	Merge					Packet	 Hostname 	Co	ontent Type	Size	Filename	
1	<u></u>	D.				334	kammy.tang@suburfar	m.com El	ML file	100 kB	=?UTF-8?B?UmU6I	OOAkOO
-	Import from H	ex Dump				23768	ozdemir.nuran@orange	e.fr El	ML file	157 kB	W-9 Stephanie de	alves Bar
	<u>C</u> lose		Ctr	rl+W	100	26313	ozdemir.nuran@orange	e.fr El	ML file	159 kB	W-9 .eml	
	Save		Ctr	rl+S	100	27146	ozdemir.nuran@orange	e.fr El	ML file	159 kB	W-9 .eml	
	Save As		Ctr	rl+Shift+S	TOC	27539	ozdemir.nuran@orange	e.fr El	ML file	159 kB	W-9 .eml	
	 File Set			,	108	•						•
ŀ	Export Specific	d Dackata			132	Text Filte	er:					
	Export Specifie	ed Packets			1.05	(2) Help				Sa	ve All × Close	Save
	Export Packet	Dissections		•	TOC	:1074		050-0				
	Export Packet	Bytes	Ctr	rl+Shift+X		504	S: 250-sr.p.gmail	.com a	t your s	servic	e, [173.66.14	6.
	Export PDUs to	o File			108	587	C: STAP TLS				, 2	
	Export TLS Ses	sion Keys			t	465	50438 465 [SYN]	Seq=0	Win=642	240 Le	n=0 MSS=1460	WS:
h	Export Objects	,		•	D	504 ICOM	i ot Hello	iy to s	tart iLs	5		
Ŀ	Export objects	,	-			TTD	220 smtp.gmail	.com E	SMTP i11	Lsm783	9700s.47 - as	mt =
Ŀ	<u>P</u> rint		Ctr	rl+P	н	TTP	EHL0 [10.0.0.8	3]	j		ge	
	<u>Q</u> uit		Ctr	rl+Q	II	MF	rver Hello	-				
	2021-01-05	20:16:0	L 10.1	.4.205	S	MB	rtificate, Serv	ver Key	Exchang	ge, Se	rver Hello Do	ne —
	2021-01-05	20:16:0	L 172.	217.195	т	FTP	0456 → 587 [ACK]	Seq=2	04 Ack=2	2798 W	in=1025	
	2021-01-05	20:16:0	L 10.1	.4.205	100	507	J7 → 50457 [ACK]	Seq=5	2 ACK=18	3 Win=	65536 Len=0	
	2021-01-05	20:16:0	1 10 1	4 205	. 108	507 518	Standard query re	ige, ch	ange C1p	A mai	pec, Encrypte	u_
	2021-01-05	20.10.0		4.205		504	S: 250-smtn amail	com a	t vour s	servic	e [173 66 14	6
•	2021-01-00	20.10.0	0.1	200		004	G. 200 Shieb. undil		it vour s		0. 11/0.00.14	×

Figure 24. Exporting Emotet malspam from our third pcap.

Export these emails and examine them. Ideally, we recommend doing this in a non-Windows environment. <u>Thunderbird</u> is a free email client you can use to see how a potential victim might view these emails.

As mentioned earlier, Emotet is also a malware downloader. Perhaps the most common malware distributed through Emotet is Trickbot.

Example 4: Emotet Infection with Trickbot

Open *Example-4-2021-01-05-Emotet-infection-with-Trickbot.pcap* in Wireshark and use a basic web filter, as shown in Figure 25.

-	Example-4-2021-01-05-Emotet-infection-with-Trickbot.pcap							
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o	<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Telephony <u>W</u> ireless <u>T</u> ools <u>H</u> elp							
	/ • · · · · · · · · · · · · · · · · · ·							
(http.request or tis	🖡 (http.request or tls.handshake.type eq 1) and !(ssdp)							
Time		Dst	port	Host	Info			
2021-01-05 1	17:15:55	173.254.250.226	443	fathekarim.com	Client Hello			
2021-01-05 1	17:15:56	52.242.211.89	443	client.wns.windows.com	Client Hello			
2021-01-05 1	17:15:56	40.91.76.238	443	licensing.mp.microsoft.com	Client Hello			
2021-01-05 1	17:16:04	90.160.138.175	80	90.160.138.175	POST /agyjkoxblu/ HTTP/1			
2021-01-05 1	17:16:45	23.3.86.10	443	<pre>storeedgefd.dsx.mp.micros</pre>	Client Hello			
2021-01-05 1	17:16:45	23.3.86.10	443	<pre>storeedgefd.dsx.mp.micros</pre>	Client Hello			
2021-01-05 1	17:16:46	23.48.32.27	443	<pre>img-prod-cms-rt-microsoft</pre>	Client Hello			
2021-01-05 1	17:16:56	23.3.86.10	443	livetileedge.dsx.mp.micro	Client Hello			
2021-01-05 1	17:20:57	23.66.131.11	443	storecatalogrevocation.st	Client Hello			
2021-01-05 1	17:21:55	52.114.159.34	443	v10.events.data.microsoft	Client Hello			
2021-01-05 1	17:22:58	52.114.75.79	443	v10.events.data.microsoft	Client Hello			
2021-01-05 1	17:29:19	52.137.106.217	443	settings-win.data.microso	Client Hello ——			
2021-01-05 1	17:29:20	13.107.5.88	443	evoke-windowsservices-tas	Client Hello			
2021-01-05 1	17:30:19	52.109.12.19	443	nexusrules.officeapps.liv	Client Hello			
2021-01-05 1	17:31:10	90.160.138.175	80	90.160.138.175	POST /t8yph1u/khoal90/hjy			
2021-01-05 1	17:37:57	52.114.159.112	443	v10.events.data.microsoft	Client Hello			
2021-01-05 1	17:46:39	90.160.138.175	80	90.160.138.175	POST /9c8b/h2psftp4eiyv/			
2021-01-05 1	17:51:25	13.107.43.23	443	config.edge.skype.com	Client Hello			
2021-01-05 1	18:02:56	90.160.138.175	80	90.160.138.175	POST /a4rspfrvf/atfj6ouc:			
2021-01-05 1	18:03:00	90.160.138.175	80	90.160.138.175	POST /h6jk7r5fx0/azyhusr			
2021-01-05 1	18:03:00	167.99.105.11	8080	167.99.105.11:8080	POST /mVfIeEcm8a HTTP/1.:			
2021-01-05 1	18:03:02	167.99.105.11	8080	167.99.105.11:8080	POST /eUCxd691 HTTP/1.1			
2021-01-05 1	18:03:05	90.160.138.175	80	90.160.138.175	POST /2dhrftruljndz4cjt/2			
2021-01-05 1	18:03:05	167.99.105.11	8080	167.99.105.11:8080	POST /oli6a7u1mvvoib/ HT			

Figure 25. Traffic from the fourth pcap filtered in Wireshark using our basic web filter. This pcap does not have an HTTP GET request for an initial Emotet DLL. However, the first frame in our column display shows HTTPS traffic to fathekarim[.]com. This was probably a web request for the Emotet DLL, because this domain was reported as hosting an Emotet binary on Jan. 5, 2021, the same date as the traffic in our pcap.

You should find the same two types of HTTP POST requests associated with Emotet C2, as described in our previous two pcaps.

This pcap also contains indicators of a Trickbot infection. Use your basic web filter and scroll down to find Trickbot traffic, as shown in Figure 26.

-	Example-4-2021-01-05-Emotet-infection-with-Trickbot.pcap							
<u>File Edit View Go</u> Capture	<u>File Edit View Go Capture Analyze Statistics Telephony Wireless Tools H</u> elp							
/ • • • • • • • • • • • • • • • • • • •								
(http.request or tls.handshake.type eq 1) and !(ssdp)								
Time [Freedat]	Dst	port	Host	Info				
	90.160.138.175	80	90.160.138.175	POST /eyv9fqi7vj/23fsjd6				
2021-01-05 18:03:25	90.160.138.175	80	90.160.138.175	POST /65vcgeyim963601/ce:				
2021-01-05 18:03:47	52.137.106.217	443	settings-win.data.microso	Client Hello				
2021-01-05 18:04:00	52.114.76.34	443	self.events.data.microsof	Client Hello				
2021-01-05 18:04:06	104.42.151.234	443	watson.telemetry.microsof	Client Hello				
2021-01-05 18:04:07	40.126.0.70	443	login.live.com	Client Hello				
2021-01-05 18:04:08	40.126.0.70	443	login.live.com	Client Hello				
2021-01-05 18:04:08	104.42.151.234	443	watson.telemetry.microsof	Client Hello				
2021-01-05 18:04:19	102.164.208.44	449		Client Hello				
2021-01-05 18:04:23	54.225.66.103	443	api.ipify.org	Client Hello				
2021-01-05 18:08:04	102.164.208.44	449		Client Hello				
2021-01-05 18:08:07	103.220.47.220	447	Trickhot traffic	Client Hello				
2021-01-05 18:09:47	102.164.208.44	449		Client Hello				
2021-01-05 18:09:51	102.164.208.44	449		Client Hello				
2021-01-05 18:09:54	186.47.209.222	443	186.47.209.222:443	POST /mor10/DESKTOP-90XVI				
2021-01-05 18:10:27	186.47.209.222	443	186.47.209.222:443	POST /mor10/DESKTOP-90XVI				
2021-01-05 18:10:59	186.47.209.222	443	186.47.209.222:443	POST /mor10/DESKTOP-90XV				
2021-01-05 18:13:01	52.162.219.173	443	checkappexec.microsoft.com	Client Hello				
2021-01-05 18:13:28	102.164.208.44	449		Client Hello				
2021-01-05 18:13:31	103.220.47.220	447	Trickbot traffic	Client Hello				
202 13:56	102.164.208.44	449		Client Hello				
201 I rickbot 13:57	52.114.88.20	443	v10.events.data.microsoft	Client Hello				
2021-01-05 10:14:15	186.47.209.222	443	186.47.209.222:443	POST /mor10/DESKTOP-90XVI				
2021-01-05 18:14:58	23.48.32.48	80	ctldl.windowsupdate.com	GET /msdownload/update/v:				

Figure 26. Scrolling down the column display to find Trickbot indicators in our fourth pcap using a basic web filter.

We've reviewed Trickbot in <u>our previous Wireshark tutorial on examining Trickbot infections</u>, but here is a quick refresher. The following are common indicators for Trickbot:

- HTTPS traffic over TCP ports 447 or 449 without an associated domain or hostname.
- HTTP POST requests over standard or non-standard TCP ports for HTTP traffic that end with /81/, /83/ or /90, which are associated with data exfiltration.
- With Trickbot from Emotet infections, the above HTTP POST requests start with /mor followed by a number (only one or two digits seen so far).
- HTTP GET requests for URLs that end in .png that return additional Trickbot binaries.

We can easily find these indicators using the following Wireshark filters:

- tls.handshake.type eq 1 and (tcp.port eq 447 or tcp.port eq 449)
- (http.request.uri contains /81 or http.request.uri contains /83 or http.request.uri contains /90) and http.request.uri contains mor
- http.request.uri contains .png

Figures 27-29 show the results from each of the above filters.

Example-4-2021-01-05-Emotet-infection-with-Trickbot.pcap							
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture	<u>A</u> nalyze <u>S</u> tatistics Tele	phony	<u>W</u> ireless <u>T</u> ools <u>H</u> elp				
/ · · · · · · · · · · · · · · · · · · ·							
Itls.handshake.type eq 1 and (t	cp.port eq 447 or tcp.po	rt eq 44	9)	🛛 🗖 🛉 basic 🗉 basic+	basic+dns		
Time	Dst	port	Host	Info	A		
2021-01-05 18:04:19	102.164.208.44	449		Client Hello			
2021-01-05 18:08:04	102.164.208.44	449		Client Hello			
2021-01-05 18:08:07	103.220.47.220	447		Client Hello			
2021-01-05 18:09:47	102.164.208.44	449		Client Hello			
2021-01-05 18:09:51	102.164.208.44	449		Client Hello			
2021-01-05 18:13:28	102.164.208.44	449		Client Hello			
2021-01-05 18:13:31	103.220.47.220	447		Client Hello			
2021-01-05 18:10:00	102.104.200.44 102.164.208.44	449		Client Hello			
2021-01-05 18:22:40	102.104.200.44 102.164.208.44	119		Client Hello			
2021-01-05 18:26:09	102.164.208.44	449		Client Hello			
2021-01-05 18:29:39	102.164.208.44	449		Client Hello			
2021-01-05 18:33:07	102.164.208.44	449		Client Hello			
2021-01-05 18:36:34	102.164.208.44	449		Client Hello			
2021-01-05 18:40:18	102.164.208.44	449		Client Hello			
2021-01-05 18:40:21	103.220.47.220	447		Client Hello			
2021-01-05 18:50:47	110.39.160.66	447		Client Hello			
2021-01-05 18:52:29	102.164.208.44	449		Client Hello			
2021-01-05 18:52:42	102.164.208.44	449		Client Hello	¥		
Figure 27.: Filtering for	Trickbot HTTPS	S traff	ic over TCP port 447	or TCP port 449.			
-	Example-4-2021-01-05	-Emote	et-infection-with-Trickbot.pca	ар	- + x		
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture	<u>Analyze</u> <u>S</u> tatistics Tele	phony	<u>Wireless</u> <u>T</u> ools <u>H</u> elp				
	ै। ९ 🔶 🔶 🍋	•	0 0 1				
http.request.uri contains /83 o	or http.request.uri conta	ns /90)	and http.request.uri contains m	nor 🛛 🖃 🍨 basic 🗉 basic+	basic+dns		
Time	Dst	port	Host	Info			
2021-01-05 18:09:54	186.47.209.222	443	186.47.209.222:443	POST /mor10/DESKTO	P-90XVB7Q		
2021-01-05 18:10:27	186.47.209.222	443	186.47.209.222:443	POST /mor10/DESKTO	P-90XVB7Q		
2021-01-05 18:10:59	186.47.209.222	443	186.47.209.222:443	POST /mor10/DESKTO	P-90XVB7Q		
2021-01-05 18:14:09	186.47.209.222	443	186.47.209.222:443	POST /mor10/DESKT0	P-90XVB7Q		
4				-	Þ		
igure 28. Filtering for HTTP POST requests associated with Trickbot data exfiltration.							

Figure 28. Filtering for HTTP POST requests associated with Trickbot data extititation. Follow TCP streams for each of the HTTP POST requests shown in Figure 28 to see if any password data was exfiltrated. The last HTTP POST request ending with /90 contains data about the infected Windows host and its environment.



Figure 29. Filtering for HTTP GET requests ending in .png associated with additional Trickbot binaries.

Follow TCP streams for each of the HTTP POST requests shown in Figure 29 to see if any Windows binaries were returned. Doing so should reveal two Windows executable files. You can then export these binaries from the pcap using *File --> Export Objects --> HTTP*, as discussed in our previous examples.

SHA256 hashes for these two Windows binaries (both EXE files) are:

- 59e1711d6e4323da2dc22cdee30ba8876def991f6e476f29a0d3f983368ab461 for mingup.png
- ed8dea5381a7f6c78108a04344dc73d5669690b7ecfe6e44b2c61687a2306785 for saved.png

Trickbot is the most common malware distributed by Emotet, but it is not the only one. Qakbot is another type of malware frequently dropped on Emotet-infected Windows hosts.

Example 5: Emotet Infection With Qakbot

Open *Example-5-2020-08-18-Emotet-infection-with-Qakbot.pcap* in Wireshark and use a basic web filter, as shown in Figure 30.

• Example-5-2020-08-18-Emotet-infection-with-Qakbot.pcap - + ×							
<u>File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help</u>							
$ \blacksquare \blacksquare \boxtimes \otimes \models \models \boxtimes \boxtimes 4 \Leftrightarrow \Rightarrow \textcircled{lag} \models \textcircled{lag} \blacksquare \textcircled{lag} \models \textcircled{lag} \models \textcircled{lag} \models \textcircled{lag} \blacksquare \textcircled{lag} \models \textcircled{lag} \blacksquare lag$							
(http.request or tls.handshake.type eq 1) and !(ssdp)							
Time	Dst	port	Host	Info	^		
2020-08-18 21:23:38	198.70.69.144	80	www.msftncsi.com	GET /ncsi.txt H1			
2020-08-18 21:23:38	204.79.197.200	443	www.bing.com	Client Hello			
2020-08-18 21:23:40	52.242.211.89	443	client.wns.windows.com	Client Hello			
2020-08-18 21:23:50	166.62.28.83	80	saketpranamam.mysquare.in	GET /temp/y32sa·			
2020-08-18 21:23:51	13.107.42.23	443	config.edge.skype.com	Client Hello			
2020-08-18 21:24:28	204.79.197.200	443	www.bing.com	Client Hello			
2020-08-18 21:24:31	52.109.20.3	443	office15client.microsoft	Client Hello			
2020-08-18 21:24:32	52.109.8.23	443	nexus.officeapps.live.com	Client Hello			
2020-08-18 21:24:32	52.109.8.20	443	nexusrules.officeapps.li	Client Hello			
2020-08-18 21:24:34	23.76.192.84	443	gameplayapi.intel.com	Client Hello			
2020-08-18 21:24:40	43.255.154.32	443	samaritantec.com	Client Hello			
2020-08-18 21:24:54	82.163.245.38	80	82.163.245.38	POST ∕UWjHXosfe€			
2020-08-18 21:25:01	82.163.245.38	80	82.163.245.38	POST /tLJcyWZ/Co			
2020-08-18 21:25:02	45.55.82.2	8080	45.55.82.2:8080	POST /YWXhUDN/Fr			
2020-08-18 21:25:07	82.163.245.38	80	82.163.245.38	POST /lZjGtKXue			
2020-08-18 21:25:07	45.55.82.2	8080	45.55.82.2:8080	POST /bfd2SwL/O\			
2020-08-18 21:25:08	82.163.245.38	80	82.163.245.38	POST /W40YnrfP77			
2020-08-18 21:25:13	82.163.245.38	80	82.163.245.38	POST /cqwZCV0Siz			
2020-08-18 21:25:19	82.163.245.38	80	82.163.245.38	POST /JrVH5PyKhl			
2020-08-18 21:25:19	45.55.82.2	8080	45.55.82.2:8080	POST /jj6ilnCS/			
2020-08-18 21:25:22	82.163.245.38	80	82.163.245.38	POST /I8sW0Er2ME			
2020-08-18 21:25:22	45.55.82.2	8080	45.55.82.2:8080	POST /iwak1vp47\			
2020-08-18 21:25:32	82.163.245.38	80	82.163.245.38	POST /X2IXP07A0			
2020-08-18 21:26:28	13.107.246.10	443	pti.store.microsoft.com	Client Hello	~		

Figure 30. Traffic from the fifth pcap filtered in Wireshark using our basic web filter. In our fifth pcap, an Emotet Word document was retrieved from saketpranamam.mysquare[.]in at 21:23:50 UTC, which matches <u>a URL reported as hosting</u> <u>an Emotet Word document on the same date</u>. Export this Word document from the pcap using *File --> Export Objects --> HTTP*, as discussed in our previous examples.

The SHA256 hash for this extracted Word document is:

```
c7f429dde8986a1b2fc51a9b3f4a78a92311677a01790682120ab603fd3c2fcb
```

We also see HTTPS traffic to samaritantec[.]com at 21:24:40 UTC. <u>This domain was</u> reported as hosting an Emotet binary on the same date.

As in our previous examples, you should find the same two types of HTTP POST requests associated with Emotet C2 traffic.

Additionally, this pcap contains indicators of a Qakbot infection. Use your basic web filter and scroll down to find Qakbot traffic, as shown in Figure 31.

•		Examp	le-5-2020-0	8-18-Er	notet-infection-with-Qakbot.p	сар	- + ×	
<u>F</u> ile <u>E</u> dit <u>V</u> iew	<u>G</u> o <u>C</u> aptu	re <u>A</u> nalyze	Statistics	Felepho	ny <u>W</u> ireless <u>T</u> ools <u>H</u> elp			
		🖉 Q	🔶 🔶 🗣	(→				
(http.request or tls.handshake.type eq 1) and !(ssdp) Image: Section 1 and interval an								
Time		Dst		port	Host	Info	^	
2020-08-1	L8 21:38	52.114.	74.45	443	v10.events.data.micr	Client Hello		
2020-08-1	18 21:39	71.80.6	6.107	443		Client Hello)	
2020-08-1	18 21:3	82.163.	245.38	80	82.163.245.38	POST /4Fz1zUK/NyGH1AK9A		
2020-08-1	18 21: 9	71.80.6	6.107	443		Client Hello		
2020-08-1	18 21 . 39	71.80.6	6.107	443		Client Hello		
2020-08-1	18 1:40	71.80.6	6.107	443		Client Hello		
2020-08-1	18 21:40	71.80.6	6.107	443		Client Hello		
2020-08-	8 21:41	71.80.6	6.107	443		Client Hello		
2020-08/1	18 21:41	71.80.6	6.107	443		Client Hello		
Qakbot	21:42	71.80.6	6.107	443		Client Hello		
1		152.199	.6.74	443	cdn.speedof.me	Client Hello		
[traπic	21:42	71.80.6	6.107	443		Client Hello		
2020-00-	8 21:43	71.80.6	6.107	443		Client Hello		
2020-08-1	21:43	71.80.6	6.107	443		Client Hello		
2020-08-1	18 21:44	71.80.6	6.107	443		Client Hello		
2020-08-1	18 .1:45	71.80.6	6.107	443		Client Hello		
2020-08-1	18 2 1 · 45	71.80.6	6.107	443		Client Hello		
2020-08-1	18 21.46	71.80.6	6.107	443		Client Hello	,	
2020-08-1	18 21:46	108.177	.122.93	443	safebrowsing.google	Client Hello		
2020-08-1	18 21:46	172.217	.1.141	443	accounts.google.com	Client Hello		
2020-08-1	18 21:46	172.217	.9.170	443	www.googleapis.com	Client Hello		
2020-08-1	18 21:46	89.105.	198.119	80	a.strandsglobal.com	GET /redir_chrome.html		
2020-08-1	18 21:46	89.105.3	198.119	80	a.strandsglobal.com	GET /favicon.ico HTTP/1		
2020-08-1	18 21:46	172.217	.195.188	5228	mtalk.google.com	Client Hello	-	

Figure 31. Scrolling down the column display to find Qakbot indicators in our fifth pcap using a basic web filter.

We've reviewed Qakbot in <u>our previous Wireshark tutorial on examining Qakbot infections</u>, but here is a quick refresher. The following are common indicators for Qakbot:

- HTTPS traffic over standard and non-standard TCP ports for HTTPS.
- Certificate data for Qakbot HTTPS traffic has unusual values for the issuer fields, and the certificate is not issued by an authority based in the United States.
- TCP traffic over TCP port 65400.

- Prior to late November 2020, Qakbot commonly generated HTTPS traffic to cdn.speedof[.]me.
- Prior to late November 2020, Qakbot commonly generated HTTP GET requests to a.strandsglobal[.]com.

We can easily find these indicators by using the following Wireshark filters:

- tls.handshake.type eq 11 and !(x509sat.CountryName == US)
- tcp.port eq 65400
- tls.handshake.extensions_server_name contains speedof
- http.host contains strandsglobal

Figures 32-35 show the results from each of the above filters.



Figure 32. Filtering and searching for unusual certificate issuer data in HTTPS traffic generated by Qakbot.

In Figure 32, the results of our first filter show several frames in the column display for traffic from 71.80.66[.]107. Search through the frame details and find unusual certificate issuer data, as shown above.

Example-5-2020-08-18-Emotet-infection-with-Qakbot.pcap							
<u>File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help</u>							
	⊭ 🏓 📃						
tcp.port eq 65400 🛛 🖾 🔮 basic basic+ basic+dns							
Time Src	port	Dst	port	Info			^
- 2020-08-18 21:42 192.168.100.101	49757	54.36.108.120	65400	49757 →	65400 [[SYN] S	Seq=0
2020-08-18 21:42 54.36.108.120	65400	192.168.100.101	49757	65400 →	49757 [SYN, /	ACK]
2020-08-18 21:42 192.168.100.101	49757	54.36.108.120	65400	49757 →	65400 [ACK]	Seq=1
2020-08-18 21:42 192.168.100.101	49757	54.36.108.120	65400	49757 →	65400 [PSH, /	ACK]
2020-08-18 21:42 54.36.108.120	65400	192.168.100.101	49757	65400 →	49757 [ACK]	Seq=1
2020-08-18 21:43 54.36.108.120	65400	192.168.100.101	49757	[TCP Ke	ep-Alive	e] 6540	00 →
2020 - C Wiresbark · Follow TCP Stream (tcp	stream eq	80) · Example-5-2020-08	-18-Emot	et-infectio	n-with-O		4975
2020-0	isti cuili cq	00) Indinpie 0 1010 00	10 11100			4	00 →
2020-(bdzpgk827381			6.112	ip-173-	66-146-1	.12.	4975
2020-(pools.nyc.verizon.net						4	00 →
2020-(4975
2020-(• • • • • • •			00 →
2020-(• • • • • • •			4975
2020-(• • • • • • •		40	00 →
2020-(• •			4975
2020-0						1	00 →
2020 - C 1 client pkt, 0 server pkts, 0 turns.							4975
2020-(Entire conversation (516 bytes)		Show and save of	A se steb	scii -	Stream 8		00 → 4075
		Show and save c		,cii			4975
2020 Find:					Find	Next	407E
	F IK	Out This Character					4970
2020-0 VHeip	Filter	Out This Stream Prin	t Save	e as E	sack $\times \underline{C}$	lose	407F
	65400	192 168 100 101	10757	TOD KA	en_Alive) 1 6540	
₹	00400	192.100.100.101	43737	LICE KE	ch-YTTAG	J 054	·

Figure 33. Filtering for Qakbot traffic over TCP port 65400.

In the above image, we find a single TCP stream of Qakbot traffic over TCP port 65400. This stream contains the public IP address and a botnet identification string for the Qakbot-infected Windows host.

Example-5-2020-08-18-Emotet-infection-with-Qakbot.pcap							
<u>File Edit View Go</u> Capture Analyze Statistics Telephony <u>W</u> ireless Tools <u>H</u> elp							
◢ ■ ∅ ◎ ⊨ 🖺 🕅 < 🔶 🔶 🔷 🔶 🚽 📃 📃 🛛 = я ፤							
📕 tls.handshake.extensions_server_name contains speedof							
Time	Dst	port	Host	Info			
2020-08-18 21:42:49	152.199.6.74	443	cdn.speedof.me	Client Hello			
4				•			

Figure 34. Filtering for traffic to cdn.speedof[.]me, which is not inherently malicious, but a connectivity check caused by Qakbot prior to late November 2020.

-	Example-5-2020-08-18-Emotet-infection-with-Qakbot.pcap						
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u>	<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>Go</u> <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Telephony <u>W</u> ireless <u>T</u> ools <u>H</u> elp						
	$\blacksquare \blacksquare \boxtimes \boxtimes \square \blacksquare $						
http.host contains strandsglob	al			🛛 🗔 🔹 basic 🗆 basic+ 🗆 basic+dns			
Time	Dst	port	Host	Info			
2020-08-18 21:46:24	89.105.198.119	80	a.strandsglobal.com	GET /redir_chrome.html HTTP/1.1			
2020-08-18 21:46:25	89.105.198.119	80	a.strandsglobal.com	GET /favicon.ico HTTP/1.1			
2020-08-18 21:47:12	89.105.198.119	80	a.strandsglobal.com	GET /redir_ie.html HTTP/1.1			
2020-08-18 21:47:12	89.105.198.119	80	a.strandsglobal.com	GET /favicon.ico HTTP/1.1			
2020-08-18 21:47:16	89.105.198.119	80	a.strandsglobal.com	GET /redir_ie.html HTTP/1.1			
2020-08-18 21:47:17	89.105.198.119	80	a.strandsglobal.com	GET /favicon.ico HTTP/1.1			
•				•			

Figure 35. Filtering for traffic to a.stransglobal[.]com, typically generated by Qakbot prior to late November 2020.While Emotet has commonly dropped Trickbot and Qakbot, be aware that Emotet has also dropped other types of malware such as Gootkit and IcedID.

Conclusion

This tutorial reviewed how to identify Emotet activity from pcaps of its infection traffic. We reviewed five recent pcaps and found similarities in HTTP POST requests caused by Emotet C2 traffic. The patterns are fairly unique and can be used to identify an Emotet infection within your network. We also reviewed other post-infection activities associated with Emotet, such as spambot traffic and different families of malware dropped on an infected host.

This knowledge can help security professionals better detect and catch an Emotet infection when reviewing suspicious network activity.

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>.