Wireshark Tutorial: Examining Qakbot Infections

unit42.paloaltonetworks.com/tutorial-qakbot-infection/

Brad Duncan

February 13, 2020

traffic-for-wireshark-column-setup.pcap			- 🗆 X
File Edit View Go Capture Analyze	Statistics Telephony Wirele	ess Tools Help	
_ ■ 2 ◎ ■ 🖹 🖄 🙆 ۹ ⇔ ⇔	🖻 🚯 📃 📃 🔍 Q 🖲	2. 壅	
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. p.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	fonts.googleapis.com	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	20 d15kpst/di2026 clou		GET / cee/usatoda V
🔵 🌋 traffic-for-wireshark-column-setup.pcap		Packets: 4448 · Displayed:	123 (2.8%) Profile: Default

By Brad Duncan

February 13, 2020 at 6:00 AM

Category: <u>Tutorial</u>, <u>Unit 42</u>

Tags: Cybercrime, pcap, Qakbot, Wireshark, Wireshark Tutorial

traffic-for-wireshark-column	-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 /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	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		fonts.googleapis.com	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 84 125	80	d15kpet/di8d86 clou		GET /rec/usatoda	- ×
🔵 🍸 traffic-for-wireshark-c	column-setup.pcap			Packets: 4448 · Displayed:	123 (2.8%) Profile: Defa	ult

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

Overview

<u>Qakbot</u> is an information stealer also known as Qbot. This family of malware has been active for years, and Qakbot generates distinct traffic patterns. This <u>Wireshark</u> tutorial reviews a recent packet capture (pcap) from a Qakbot infection. Understanding these traffic patterns can be critical for security professionals when detecting and investigating Qakbot infections.

Note: This tutorial assumes you have a basic knowledge of network traffic and Wireshark. We use a customized column display shown in <u>this tutorial</u>. You should also have experience with Wireshark display filters as described in <u>this additional tutorial</u>.

Please also note that the pcap used for this tutorial contains malware. You should review this pcap in a non-Windows environment. If you are limited to a Windows computer, we suggest reviewing the pcap within a virtual machine (VM) running any of the popular recent Linux distros.

This tutorial will cover the following:

- Qakbot distribution methods
- Initial zip archive from link in an malspam
- Windows executable for Qakbot
- Post-infection HTTPS activity
- Other post-infection traffic

The pcap used for this tutorial is located <u>here</u>. Download the zip archive named **2020-01-29**-**Qbot-infection-traffic.pcap.zip** and extract the pcap. Figure 1 shows our pcap open in Wireshark, ready to review.

	2	2020	-01-29-Qbot-	infection-traffic.pcap		+ - E ×					
E	le <u>E</u> dit <u>V</u> iew	<u>Go</u> <u>Capture</u> <u>A</u> nalyze <u>St</u>	atistics T	elephony <u>W</u> ireless	s <u>T</u> ools	Help					
(🗎 🖺 🔀 🗔 🧔	* * 10	🗋 📃 🔍		X X					
	Apply a display filter <ctrl-></ctrl-> Expression + basic basic+ basic+DNS										
Tir	ne	Src	Src port	Dst	Dst port	i Info					
	2020-01-29	15:40 10.1.29.101	137	10.1.29.255	137	Registration NB DESKTC					
	2020-01-29	15:40 10.1.29.101	137	10.1.29.255	137	Registration NB WORKGR					
	2020-01-29	15:40 10.1.29.101	51955	10.1.29.1	53	Standard query 0xf4c0					
	2020-01-29	9 15:40 10.1.29.101	5353	224.0.0.251	5353	Standard query 0x0000					
	2020-01-29	9 15:40 10.1.29.101	5353	224.0.0.251	5353	Standard query respons					
	2020-01-29	9 15:40 10.1.29.1	53	10.1.29.101	62540	Standard query respons					
	2020-01-29	9 15:40 10.1.29.1	53	10.1.29.101	51955	Standard query respons					
	2020-01-29	9 15:40 10.1.29.101	57281	224.0.0.252	5355	Standard query 0x29af					
	2020-01-29	9 15:40 10.1.29.101	51876	10.1.29.1	53	Standard query 0xde09					
	2020-01-29	9 15:40 10.1.29.1	53	10.1.29.101	51876	Standard query respons					
	2020-01-29	9 15:40 10.1.29.101	61365	10.1.29.1	53	Standard query 0xcb44					
	2020-01-29	9 15:40 10.1.29.101	65053	10.1.29.1	53	Standard query 0x68a1					
	2020-01-29	9 15:40 10.1.29.1	53	10.1.29.101	65053	Standard query respons					
	2020-01-29	9 15:40 10.1.29.1	53	10.1.29.101	61365	Standard query respons					
	2020-01-29	15:40 10.1.29.101	49671	13.107.4.52	80	49671 → 80 [SYN] Seq=0					
	2020-01-29	15:40 10.1.29.101		224.0.0.22		Membership Report / Jo					
	2020-01-29	15:40 13.107.4.52	80	10.1.29.101	49671	80 → 49671 [SYN, ACK]					
	2020-01-29	9 15:40 10.1.29.101	49671	13.107.4.52	80	49671 → 80 [ACK] Seq=1					
	2020-01-29	15:40 10.1.29.101	49671	13.107.4.52	80	GET /connecttest.txt H					
4	2020-01-20	15.40 13 107 4 52	80	10 1 29 101	49671	80 → 49671 [ACK] Seg=1					

Figure 1. The pcap for this tutorial.

Qakbot Distribution Methods

Qakbot is most often distributed through malicious spam (malspam), but it also has been distributed through exploit kits <u>as recently as November 2019</u>. In some cases, Qakbot is a follow-up infection caused by different malware like <u>Emotet</u> as reported in <u>this example from March 2019</u>.

Recent malspam-based distribution campaigns for Qakbot follow a chain of events shown in Figure 2.



Figure 2. Flow chart from recent Qakbot distribution campaigns.

Initial Zip Archive from Link in Malspam

Recent malspam distributing Qakbot uses fake email chains that spoof legitimate email addresses. One such example is shown in Figure 3.

	cident with the Porsche	- Mozilla Thunderbird	d				- 0	>
le <u>E</u> dit	<u>V</u> iew <u>G</u> o <u>M</u> essage	<u>I</u> ools <u>H</u> elp						
From					5 Reply	Seply All ▼	→ Forward	More
ubject R	e: Accident with the P	orsche				Date Mon, 03 F	eb 2020 21:51	:53 +00
То		<		>☆				
ello.								
,								
o atta	ched the report hele	w just pood you	to confirm that it'		loaso tako	a look and got h	ack to mo	
e alla	ched the report beit	ow, just need you	to comminat it	s good to go. F	riease lake	a look and get b	back to me.	
-		-						
IACH	IMENT DOCUMEN							
ank v	ou							
				10.1				
		Link poi	ints to: ht	p://bhat	ner.co	m/wp-co	ontent/	
			10000101					
		uploads	S/2020/01	/ahead/	9312.z	ID		
	,							
	,							
Yes, it	, was the William's F	Porsche. The accid	dent was entirely	my fault, thoug	gh. I didn't c	heck my blind s	pot before	
Yes, it changi	, was the William's F ing lanes.	Porsche. The accid	dent was entirely	my fault, thoug	gh. <mark>I d</mark> idn't c	heck my blind s	pot before	
Yes, it changi	, was the William's F ing lanes.	Porsche. The accid	dent was entirely	my fault, thoug	gh. I didn't c	heck my blind s	pot before	
Yes, it changi - Rona	, was the William's F ing lanes. Id	Porsche. The accid	dent was entirely	my fault, thoug	gh. I didn't c	heck my blind s	pot before	
Yes, it changi - Rona	, was the William's F ing lanes. Id	Porsche. The accic	dent was entirely	my fault, thoug	gh. I didn't c	heck my blind sj	pot before	
Yes, it changi - Rona	, was the William's F ing lanes. Ild	Porsche. The accid	dent was entirely	my fault, thou <u>c</u>	gh. I didn't c	heck my blind sj	pot before	
Yes, it chang - Rona > On J	, was the William's F ing lanes. Ild lun 26, 2019, at 12:	Porsche. The accid	dent was entirely wrote:	my fault, thouថຼ	gh. I didn't c	heck my blind sj	pot before	
Yes, it changi - Rona > On J >	, was the William's F ing lanes. Ild lun 26, 2019, at 12:	Porsche. The accid	dent was entirely wrote:	my fault, thoug	gh. I didn't c	heck my blind s	pot before	
Yes, it changi - Rona > On J > > Rona	, was the William's F ing lanes. Ild lun 26, 2019, at 12: ald,	Porsche. The accid	dent was entirely wrote:	my fault, thoug	gh. I didn't c	heck my blind s	pot before	
Yes, it changi - Rona > On J > Rona >	, was the William's F ing lanes. Ild lun 26, 2019, at 12: ald,	Porsche. The accid	dent was entirely wrote:	my fault, thoug	gh. I didn't c	heck my blind s	pot before	
Yes, it chang - Rona > On J > Rona > Rona > Rum	, was the William's F ing lanes. Ild lun 26, 2019, at 12: ald, or has it your Nissa	Porsche. The accid 26 PM, an was involved in	dent was entirely wrote:	my fault, thoug	gh. I didn't c	heck my blind s	pot before	
Yes, it chang - Rona > On J > Rona > Rona > Rona > Pors	, was the William's F ing lanes. Ild lun 26, 2019, at 12: ald, or has it your Nissa che. And the Porsc	Porsche. The accid 26 PM, an was involved in be was driven by 1	dent was entirely wrote:	my fault, thoug with the	gh. I didn't c	heck my blind s	pot before	
Yes, it chang - Rona > On J > Rona > Rona > Rona > Pors	, was the William's F ing lanes. Ild lun 26, 2019, at 12: ald, lor has it your Nissa che. And the Porsc true?	Porsche. The accid 26 PM, an was involved in he was driven by '	dent was entirely wrote: n a traffic accident William in accourt	my fault, thoug with the hting. Was	gh. I didn't c	heck my blind s	pot before	
Yes, it chang - Rona > On J > Rona > Rona > Rum > Pors > this t	, was the William's F ing lanes. Ild lun 26, 2019, at 12: ald, lor has it your Nissa che. And the Porsc true?	Porsche. The accid 26 PM, an was involved in he was driven by '	dent was entirely wrote: n a traffic accident William in accourt	my fault, thoug with the hting. Was	gh. I didn't c	heck my blind s	pot before	

Figure 3. Recent malspam example pushing Qakbot.

URLs from these emails end with a short series of numbers followed by *.zip*. See Table 1 for a few examples of URLs from Qakbot malspam recently reported on <u>URLhaus</u> and <u>Twitter</u>.

First reported	URL for initial zip archive
2019-12-27	hxxps://prajoon.000webhostapp[.]com/wp- content/uploads/2019/12/last/033/033.zip
2019-12-27	hxxps://psi-uae[.]com/wp-content/uploads/2019/12/last/870853.zip
2019-12-27	hxxps://re365[.]com/wp- content/uploads/2019/12/last/85944289/85944289.zip
2019-12-27	hxxps://liputanforex.web[.]id/wp-content/uploads/2019/12/last/794/794.zip
2020-01-06	hxxp://eps.icothanglong.edu[.]vn/forward/13078.zip
2020-01-22	hxxp://hitechrobo[.]com/wp- content/uploads/2020/01/ahead/84296848/84296848.zip

2020-01-22	hxxp://faithoasis.000webhostapp.com/wp- content/uploads/2020/01/ahead/550889.zip
2020-01-27	hxxps://madisonclubbar[.]com/fast/invoice049740.zip
2020-01-29	hxxp://zhinengbao[.]wang/wp-content/uploads/2020/01/lane/00571.zip
2020-01-29	hxxp://bhatner[.]com/wp-content/uploads/2020/01/ahead/9312.zip
2020-02-03	hxxp://santedeplus[.]info/wp- content/uploads/2020/02/ending/1582820/1582820.zip

Table 1. URLs for the initial zip archive to kick off a Qakbot infection chain.

In our pcap, you can find the HTTP request for a zip archive using *http.request.uri contains .zip* in the Wireshark filter as shown in Figure 4.



Figure 4. Finding the URL for the initial zip archive.

Follow the TCP stream to confirm this is a zip archive as shown in Figure 5 and Figure 6, then try to export the zip archive from the pcap as shown in Figure 7.

		2020-01-	29-Qbot-infe	ction-tra	ffic.pcap		• • • •
<u>File Edit View</u>	<u>Go</u> <u>C</u> aptu	re <u>A</u> nalyze <u>S</u> ta	atistics Te	lephony	<u>Wireless</u> Tools <u>H</u> elp	1	
) 🙆 🙇 🜲 🕯	> - K		● ④ ④ ④ Ⅲ		
http.request.ur	ri contains	zip		× =	Expression + t	basic ba	asic+ basic+DNS
Гime		Dst	Dst port	Host	Info		
2020-01-29	15:41	103.91.92.1	80	bhatn	Mark/Unmark Packet	ontent	/uploads/2020/
				<u>1</u>	gnore/Unignore Packet		
					Set/Unset Time Reference	e	
					lime Shift	-	
				F	Packet Comment		
				E	Edit Resolved Name		
				1	Apply as Filter	•	
				F	Prepare a Filter		
				(Conversation Filter	•	N
				(Colorize Conversation	•	
				9	SCTP	•	
				F	ollow	•	TCP Stream
				(Сору	•	UDP Stream
				F	Protocol Preferences	•	SSL Stream
				[Decode <u>A</u> s		HTTP Stream
				9	Show Packet in New Win	dow	

Figure 5. Following the TCP stream for the HTTP request from our filter results.



2020-01-29-Qbot-infection-traffic.pcap File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help Open Ctrl+O **Open Recent** basic | basic+ | basic+DNS Expression... + Merge... ort Host Info Import from Hex Dump... 49679 → 80 [SYN] Close Ctrl+W 9 80 → 49679 [SYN, Save Ctrl+S 49679 → 80 [ACK] bhatner.com GET /wp-content/u Ctrl+Shift+S Save As... '9 80 → 49679 [ACK] File Set 9 [TCP Previous sed Export Specified Packets... [TCP Out-Of-Order '9 Export Packet Dissections [TCP Previous seg 9 Continuation Export Packet Bytes... Ctrl+Shift+X 9 ontinuation Export PDUs to File... 9 [TCP Out-Of-Order Export SSL Session Keys... 9 ICP Out-Of-Order DICOM... Export Objects Continuation Continuation HTTP... Print... Ctrl+P Continuation IMF... Quit Ctrl+Q • SMB... TFTP...

Figure 6. Indicators this URL returned a zip archive.

Figure 7. Exporting objects from HTTP traffic in the pcap.

In most cases, the menu for *File* \rightarrow *Export Objects* \rightarrow *HTTP* should export a zip archive sent over HTTP. Unfortunately, as shown in Figure 8, we cannot export this file named *9312.zip* because it is separated into hundreds of smaller parts within the export HTTP objects list.

	Wireshark •	Export · HTTP obje	ect list		• - •
Packet •	Hostname	Content Type	Size	Filename	4
21	www.msftconnecttest.com	text/plain	22 bytes	connecttest.tx	t
322	bhatner.com		1,358 bytes	9312.zip	
325	bhatner.com		1,358 bytes	9312.zip	
335	bhatner.com		1,358 bytes	9312.zip	
343	bhatner.com		1,358 bytes	9312.zip	
348	bhatner.com		1,358 bytes	9312.zip	
350	bhatner.com		1,358 bytes	9312.zip	
354	bhatner.com		1,358 bytes	9312.zip	
360	bhatner.com		1,358 bytes	9312.zip	
362	bhatner.com		1,358 bytes	9312.zip	
363	bhatner.com		1,358 bytes	9312.zip	
366	bhatner.com		1,358 bytes	9312.zip	
371	bhatner.com		1,358 bytes	9312.zip	
382	bhatner.com		1,358 bytes	9312.zip	
387	bhatner.com		1,358 bytes	9312.zip	
390	bhatner.com		1,358 bytes	9312.zip	
391	bhatner.com		1,358 bytes	9312.zip	
392	bhatner.com		1,358 bytes	9312.zip	
394	bhatner.com		1,358 bytes	9312.zip	
395	bhatner.com		1,358 bytes	9312.zip	
409	bhatner.com		1,358 bytes	9312.zip	
411	bhatner.com		1,358 bytes	9312.zip	_
112	hhatnar cam		1 250 butos	0212 -in	•
;;; Help			Save	All X <u>C</u> lose	≧ <u>S</u> ave

Figure 8. 9312.zip is broken up into hundreds of objects within the list, so we cannot export it this way.

Fortunately, we can export data from a TCP stream window and edit the binary in a hex editor to remove any hxxP response headers. Use the following steps to extract the zip archive from this pcap:

1.

- 1. Follow TCP stream for the HTTP request for 9312.zip.
- 2. Show only the response traffic in the TCP stream Window.
- 3. Change "Show and save data as" from ASCII to Raw.
- 4. Save the data as a binary (I chose to save it as: 9312.zip.bin)
- 5. Open the binary in a hex editor and remove the HTTP request headers before the first two bytes of the zip archive (which show as PK in ASCII).
- 6. Save the file as a zip archive (I chose to save it as 9312.zip)
- 7. Check the file to make sure it's a zip archive.

See Figures 9 through 14 for a visual guide of this process.



Figure 9. Step 2 - When viewing the TCP stream, switch from viewing the entire conversation to viewing only data returned from the server.



Figure 10. Step 3 - Show and save data as Raw instead of ASCII.



Figure 11. Step 4 - Save this raw data from the TCP stream as a binary.

													931	L2.zij	p.bir	- Bl	ess											÷		×
<u>File</u> <u>E</u> dit	<u>File Edit View Search Tools Help</u>																													
	21	5	¢	*	Ē			à	2																					
9312.zip.b	oin ×																													
00000000	48	54	54	50	2F	31	2E	31	20	32	30	30	20	4F	4B	0D	0A	44	61	74	65	ЗA	20	НТТ	P/1.1	200	9 OK.	.Dat	e:	*
00000017	57	65	64	20	20	32	39	20	4A	61	6E	20	32	30	32	30	20	31	35	3A	34	33	3A	Wed	1, 29	Jan	2020	15:	43:	
0000002e	33	39	20	47	4D	54	OD	0A	53	65	72	76	65	72	3A	20	41	70	61	63	68	65	2F	39	GMT	Ser	ver:	Apad	:he/	
00000045	32	2E	32	2E	31	35	20	28	12	65	AE	71	1E	52	29	20	44	41	56	2F	32	20	50	2.2	2.15 (Cent	tOS)	DAV	2 P	
0000005c	48	50	2F	37	2E	30	2E	33	488	Peri	orm	Op	era	tion		V	55	72	65	64	2D	42	79	HP/	7.0.3	33)	X-Pov	vered	I-By	
00000073	3A	20	50	48	50	2F	35	2E	ð	Cuţ							6E	74	65	6E	74	2D	40	: F	HP/5.	4.10	6Co	onter	it-L	
0000008a	65	6E	67	74	68	3A	20	32	0	Cop	У						13	6F	6E	6E	65	63	74	eng	ith: 2	184	158	Conr	lect	
000000a1	69	61	6E	3A	20	6B	65	65		Past	e					20	20	63	60	61	73	65	OD	101	I: Kee	ep-a	live,	CLO	ose.	
000000008	UA 42	41	63	03	65	10	74	20		Dele	ete				1	20	62	79	14	05	13	OD 61	UA	. AC	cept-	Rang	ges:	byte	·S	
00000000	43	61	62	69	60	0E	65	20	20	20	66	60	60	GE	6E	61	60	OF 6E	OE	34	20	22	21	tor	hmont	DIS	ilon	mo-!	aL	
00000000000000000000000000000000000000	22	25	74	60	70	22	OE	04	12	20	65	74	65	65	74	20	54	70	70	65	39	20	61	2 7	in"	Cont	tent	Type	931	
00000010	70	70	60	60	63	61	74	60	45 6E	6F	25	74	60	70	00	OA.	00	04	50	4B	03	04	14	nnl	icati	on/	zin	- i y pe	. a	
00000114	00	00	00	0.9	00	25	58	36	50	40	B1	23	32	36	53	21	00	68	DB	41	00	OD.	00	PP I	Xe	DT	#2>51	h 4		
00000120	00	00	44	56	43	SE	36	30	33	37	32	2E	76	62	73	64	ED	69	57	DB	54	03	20		IVC 66	372	vhsr	i iW	7 -	
00000142	100		-14		40		00		00		02	~~		02				00			UN		20		vo_00		. • • • • •			•
Signe	d 8	bit:	72					Sig	gneo	32	bit:	12	134	861	60						He	kade	ecim	nal:	48 54	54 5	0		>	c
Unsigne	d 8	bit:	72				U	nsig	gneo	1 32	bit:	12	134	861	60							De	ecim	nal:	072 08	84 08	34 08	0		
Signed	16	bit:	185	516				F	loat	t 32	bit:	21	742	5.3									Oct	tal:	110 12	24 12	24 12	0		
Unsigned	16	bit:	185	516	3			F	loa	t 64	bit:	2.7	7670	0875	5323	3932	24E-	+40				1	Bina	ary: [01001	000	0101	0100	010	
Show	littl	e er	dia	n de	ecod	ing			C	Sh	ow	unsi	gne	d as	s he	xad	ecin	nal				ASC	II Te	ext:	HTTP					
												0	Offs	et: C)x0	/ 0x	215	503			5	Sele	ctio	n: 0)	(0 to 0	x125	6 (0×1	26	INS	///

Figure 12. Step 5 - Open your saved binary in a hex editor and remove any HTTP response data before the first two bytes of the zip archive (that show as PK in ASCII).

						9312.zi	p.bin	* - Ble	55							•	
File Edit View S	earch Tools	s <u>H</u> elp															
<u>▶</u> ew <u>▶</u> open	0	trl+N trl+O	d 22														
Save	C	trl+S	00 09	00	25 59	26 50	40	D1	10 00	25	6.2	21 00	60	DK	VEDT	#250	I b 4
Save <u>A</u> s	Shift+C	tres	4A 56	43	2E 58	30 33	37	32	23 32 2E 76	3E	73	64 FD	69	A	JVC 60372	#2>5	d.i
e <u>R</u> evert			56 F9	15	CA OB	E4 09	0E	06	DB 72	23	25	61 40	E8	W.Z		.r#%	a@.
Export			Bz 94 27 6	6		13 80	8D	10	13 DE	Save	GA File A	55 32 Is	na	L KOB			U2. .\$
<u>1</u> . 9312.zip.bin		1	8D 33	F	Namo		03	12 -	n								
× <u>C</u> lose	Ct	rl+W	BC FC	7	<u>N</u> ame.		93	12.2	М								:0
Quit 000000cf 27 61 000000e6 48 46	CI 6A E8 6C A6 9C 8C	trl+Q : 14 44 9F 29	BE EF B1 F2 8F 87	056	Save ir	n <u>f</u> older	•	Dov	nloa	ds					Create Fo	lder	Y.
000000fd C3 D0	33 6E 55	11 EA	74 E2	F	Name								•	Size	Modified	-	. N
00000114 98 E8 00000012b CA B4 00000142 33 AE	34 F2 27 31 51 89 29 9F 1E	FC 6B A7 87 4B 25	11 3D F4 17 45 94	4 1 7	♦ 931	2.zip.bir	n							2.2 MB	21:04		y. (#
Signed 8 bit:	80		Signe	d 3													
Unsigned 8 bit:	80	Ur	nsigne	d 3													5
Signed 16 bit:	20555		Floa	at 3													1
Unsigned 16 bit:	20555		Floa	nt 6										S Car	ncel	ave	00
Show little en	dian decodi	ing		Sh	iow uns	igned a	s he	kade	imal	_	-	ASC	II Te	xt: PK	0 0 0 4		
						Offset:	0x0 /	0x2	153dc	i		Sele	ctior	n: None			INS

Figure 13. Step 6 - Save your edited binary as a zip archive.

Terminal: ~/Downloads	• - • ×
File Edit View Terminal Tabs Help	
~\$ cd Downloads/	1
~/Downloads\$ file 9312.zip	
9312.zip: Zip archive data, at least v2.0 to extract	
<pre>~/Downloads\$ unzip 9312.zip</pre>	
Archive: 9312.zip	
inflating: JVC_60372.vbs	
<pre>~/Downloads\$ file JVC_60372.vbs</pre>	
JVC_60372.vbs: ASCII text, with very long lines	
<pre>~/Downloads\$ shasum -a 256 9312.zip JVC_60372.vbs</pre>	
5121c89e898eadeff9eeef660d92f3cff75700c7f017b33c913a951018a3df9a	9312.zip
51758a9ddf92d19be7c69a60125fb3dfc303152e9bbc77478dfff497422f3d25	JVC_60372.vbs
~/Downloads\$	

Figure 14. Step 7 - Confirm the edited file is a zip archive, then extract the VBS file and check the file hashes.

Figure 14 shows how to use a terminal window from a Debian-based Linux distro to check the files. From our pcap, the zip archive should be the same as <u>this file submitted to</u> <u>VirusTotal</u>. Our extracted VBS file should be the same as <u>this file also submitted to</u> <u>VirusTotal</u>.

A public sandbox analysis of <u>our extracted VBS file</u> indicates it generates the next Qakbotrelated URL in our infection chain: a URL that returned a Windows executable for Qakbot.

Windows Executable for Qakbot

These extracted VBS files generate URLs that return Windows executables for Qakbot. Since December 2019, URLs for Qakbot executables have ended with 44444.png or 444444.png. See Table 2 for some recent examples of these Qakbot URLs we found using our <u>AutoFocus</u> Threat Intelligence service.

First Seen	URL for Qakbot executable
2019-12- 27	hxxp://centre-de-conduite-roannais[.]com/wp- content/uploads/2019/12/last/444444.png
2020-01- 06	hxxp://newsinside[.]info/wp-content/uploads/2020/01/forward/44444.png
2020-01- 15	hxxp://iike.xolva[.]com/wp-content/themes/keenshot/fast/444444.png
2020-01- 17	hxxp://deccolab[.]com/fast/444444.png

2020-01-	hxxp://myrestaurant.coupoly[.]com/wp-
21	content/uploads/2020/01/along/444444.png
2020-01- 22	hxxp://alphaenergyeng[.]com/wp-content/uploads/2020/01/ahead/444444.png
2020-01-	hxxp://claramohammedschoolstl[.]org/wp-
23	content/uploads/2020/01/upwards/444444.png
2020-01- 23	hxxp://creationzerodechet[.]com/choice/444444.png
2020-01-	hxxp://productsphotostudio[.]com/wp-
26	content/uploads/2020/01/lane/444444.png
2020-01-	hxxp://sophistproduction[.]com/wp-
27	content/uploads/2020/01/choice/444444.png
2020-01- 30	hxxp://uofnpress[.]ch/wp-content/uploads/2020/01/side/444444.png
2020-02- 03	hxxp://csrkanjiza[.]rs/wp-content/uploads/2020/02/ending/444444.png

Table 2. URLs for Qakbot executables.

In our pcap, find the HTTP GET request for our Qakbot executable using *hxxp.request.uri contains .png* in the Wireshark filter as shown in Figure 15.

	:	2020-01-29-Qbot-infection-traffic	.pcap	+ ×
<u>F</u> ile <u>E</u> dit <u>V</u> iew	<u>Go</u> <u>Capture</u> <u>Analyze</u> <u>Stat</u>	istics Telephony <u>W</u> ireless	s <u>T</u> ools <u>H</u> elp	
	🗎 🗎 🕅 🙆 💩 🔶	③ I III III III III III III III	Q, Q, 🎹	
http.request.ur	i contains .png		Expression + b	asic basic+ basic+DNS
Time	Dst	Dst port Host	Info	
+ 2020-01-29	15:42 5.61.27.159	80 alphaenergye	ng.com GET /wp-conter	nt/uploads/2020/01/ah
4				Þ

Figure 15. Finding the URL for our Qakbot executable.

Export this object from the pcap using the *File* \rightarrow *Export Objects* \rightarrow *HTTP* menu path as shown in Figure 16 and check the results as shown in Figure 17.

<u>Edit View Go</u> Capture Open	Analyze Statistics Ctrl+O	Telephony	Wireless	Tools Help			
Open Recent	,			Wireshark · Exp	ort · HTTP object li	st	• - E
Merge Import from Hex Dump	Child W	ort Host alpha	Packet * 2370 2371	Hostname bhatner.com bhatner.com	Content Type	Size 1,358 bytes 1,358 bytes	Filename 9312.zip 9312.zip
Save As	Ctrl+S Ctrl+Shift+S		2376 2378 2380	bhatner.com bhatner.com bhatner.com		1,358 bytes 1,358 bytes 1,358 bytes	9312.zip 9312.zip 9312.zip
File Set Export Specified Packets	•		2385 2387 2391	bhatner.com bhatner.com bhatner.com	imagolong	1,358 bytes 1,358 bytes 788 bytes	9312.zip 9312.zip 9312.zip
Export Packet Dissections Export Packet Bytes Export PDUs to File Export SSL Session Keys	، Ctrl+Shift+X		14850 14897 15172 1549 3021	store.nvprivateoffice.com store.nvprivateoffice.com store.nvprivateoffice.com store.nvprivateoffice.com crt.usertrust.com	text/html text/html text/html text/html application/	97 bytes 169 bytes 97 bytes 571 bytes 983 bytes	redir_ie.html favicon.ico redir_ie.html favicon.ico USERTrustECCA
Export Objects		DICOM	30	ts-ocsp.ws.symantec.com	application/	1,589 bytes	MFEWTzBNMEsw MFEWTzBNMEsw
Print	Ctrl+P	HTTP	337	ocsp.verisign.com	application/	83 bytes	sta
Quit	Ctrl+Q	IMF SMB	346 129 149	ocsp.verisign.com go.microsoft.com dmd.metaservices.micr	application/ text/xml text/xml	5 bytes 1,242 bytes 1,242 bytes	stat. ?L metal vc

Figure 16. Exporting our Qakbot executable from the pcap.



Figure 17. Checking the exported file in a Debian-based Linux terminal window. From our pcap, the Qakbot executable should be <u>this file submitted to VirusTotal</u>. A <u>public</u> <u>sandbox analysis of this file</u> generated several Qakbot indicators (identified as Qbot).

Post-infection HTTPS Activity

Use your basic filter (covered in <u>this previous WIreshark tutorial</u>) for a quick view of web traffic in our pcap. Scroll down to activity after the HTTP GET request to alphaenergyeng[.]com that returned our Qakbot executable. You should see several indicators of HTTPS or SSL/TLS traffic to 68.1.115[.]106 with no associated domain as noted in Figure 18.

🚄 2020-01-29-Qbot-infection-traffic.pcap 🔷 👵 🗉 🛠						
File Edit View Go Capt	ture <u>A</u> nalyze <u>S</u> tatisti	cs Telep	hony <u>W</u> ireless <u>T</u> ools <u>H</u> elp			
	3 🙆 🙇 💩 3		💶 🔍 २, २, 🎹			
(http.request or ssl.hand	Ishake.type == 1) and	!(ssdp)	Expression.	+ basic basic+ basic	+DNS	
Time	Dst	Dst port	Host	Info	-	
2020-01-29 15:42	. 5.61.27.159	80	alphaenergyeng.com	GET /wp-content/uploa	a	
2020-01-29 15:48	. 204.79.197.200	443	www.bing.com	Client Hello		
2020-01-29 15:48	. 204.79.197.222	443	fp.msedge.net	Client Hello		
	. 13.107.42.254	443	l-ring.msedge.net	Client Hello		
	. 104.114.164.71	443	ow1.res.office365.com	Client Hello		
SSL/TLS traffic 8.	. 13.107.246.10	443	pti.store.microsoft.com	Client Hello		
generated by	. 68.1.115.106	443		Client Hello		
generated by	. 68.1.115.106	443		Client Hello		
Qakbot ^{9.}	. 68.1.115.106	443		Client Hello		
.9	. 68.1.115.106	443		Client Hello		
2020-01 29 13 5.	. 68.1.115.106	443		Client Hello		
2020-01-19 15:50	. 68.1.115.106	443		Client Hello		
2020-01-29 15:50	. 68.1.115.106	443		Client Hello		
2020-01-29 1:50	. 68.1.115.106	443	.	Client Hello		
2020-01-29 15. 0.	. 52.242.231.32	443	fe2cr.update.microsoft.c	Client Hello	_	
2020-01-29 15:	65.52.108.90	443	Te3cr.delivery.mp.micros	Client Hello		
2020-01-29 15:51	68.1.115.106	443		Client Hello		
2020-01-29 15:51	. 68.1.115.106	443		Client Hello		
2020-01-29 15:52	. 68.1.115.106	443		Client Hello		
2020-01-29 15:52	. 68.1.115.106	443		Client Hello		
2020-01-29 15:54.	68.1.115.106	443		Client Hello		

Figure 18. HTTPS or SSL/TLS traffic caused by Qakbot.

This traffic has unusual certificate issuer data commonly noted during Qakbot infections. We reviewed unusual certificate issuer data in our <u>previous WIreshark tutorial about Ursnif</u>, so this should be easy to find.

Let's review our Qakbot certificate issuer data using the following Wireshark filter:

Ip.addr eq 68.1.115.186 and ssl.handshake.type eq 11

For Wireshark 3.0 or newer, use *tls.handshake.type* instead of *ssl.handshake.type*. Select the first frame in your results and expand the frame details window until you find the certificate issuer data as shown in Figure 19.



Figure 19. Reviewing certificate issuer data from Qakbot traffic.

Patterns for the locality name, organization name, and common name are highly-unusual, not normally found in certificates from legitimate HTTPS, SSL, or TLS traffic. Our example of this issuer data is listed below:

- id-at-countryName=ES
- id-at-stateOrProvinceName=IA
- id-at-localityName=Uorh Ofwa
- id-at-organizationName=Coejdut Mavmtko Qxyemk Dxsjie LLC.
- id-at-commonName=gaevietovp.mobi

Other Post-infection Traffic

Our pcap contains other activity associated with a Qakbot infection. Each activity is not inherently malicious on its own, but taken together with our previous findings, we can assume a full Qakbot infection.

Another indicator of a Qakbot infection is HTTPS traffic to cdn.speedof[.]me. The domain speedof[.]me is used by a legitimate Internet speed test service. Although this is not malicious traffic, we frequently see traffic to cdn.speedof[.]me during Qakbot infections. Figure 20 shows this activity from our pcap.

	2020-01-29-Qbot-infection-traffic.pcap							
<u>File Edit View Go Capt</u>	ture <u>A</u> nalyze <u>S</u> tatis	tics Tele	phony <u>W</u> ireless <u>T</u> ools <u>H</u> elp					
	🗙 🙆 🔯 📚	3 16 6	l 📃 📃 Q, Q, Q, 🎹					
(http.request or ssl.handshake.type == 1) and !(ssdp)								
Time	Dst	Dst port	Host	Info				
HTTPS or	. 52.242.231.32	443	fe2cr.update.microsoft.c	Client Hello				
	65.52.108.90	443	fe3cr.delivery.mp.micros	Client Hello				
SSL/ILS traffic	. 68.1.115.106	443		Client Hello				
Idenerated by	. 68.1.115.106	443		Client Hello				
generated by	. 68.1.115.106	443		Client Hello				
Qakbot	. 68.1.115.106	443		Client Hello				
2020-01-1 13.34.	. 68.1.115.106	443		Client Hello				
2020-01-29 1. 54	. 72.21.81.189	443	cdn.speedof.me	Client Hello				
2020-01-29 15:5	68.1.115.106	443		Client Hello				
2020-01-29 15:54.	. 68.1.115.106	443		Client Hello				
2020-01-29 15:54.	. 68.1.115.106	443		Client Hello				
2020-01-29 15:55.	. 68.1.115.106	443		Client Hello				
2020-01-29 15:55.	. 68.1.115.106	443		Client Hello				
2020-01-29 15:55.	. 68.1.115.106	443		Client Hello				
2020-01-29 15:55	. 72.21.81.189	443	cdn.speedof.me	Client Hello				
2020-01-29 15:55.	. 68.1.115.106	443		Client Hello				
2020-01-29 15:56.	. 72.21.81.200	443	iecvlist.microsoft.com	Client Hello				
2020-01-29 15:56.	. 52.109.20.3	443	officeclient.microsoft.c	Client Hello				
2020-01-29 15:56.	. 52.109.20.3	443	officeclient.microsoft.c	Client Hello				
2020-01-29 15:56	89 105 198 1	80	store nunrivateoffice com	GET /redir ie h				

Figure 20. The domain cdn.speedof[.]me within the Qakbot traffic.Qakbot also opens windows from all browsers on an infected Windows host. At approximately 13 minutes and 5 seconds into <u>this sandbox analysis</u>, the video playback shows Qakbot opening Chrome, then Firefox, then Internet Explorer on a Windows 7 host. This analysis shows Qakbot generated traffic to the following URLs:

- hxxp://store.nvprivateoffice[.]com/redir_chrome.html
- hxxp://store.nvprivateoffice[.]com/redir_ff.html
- hxxp://store.nvprivateoffice[.]com/redir_ie.html

The domain nvprivateoffice[.]com has been registered through GoDaddy since 2012, and store.nvprivateoffice[.]com shows a default web page for nginx on a Fedora server.

Our pcap for this tutorial is from a Qakbot infection on a Windows 10 host without Chrome or Firefox installed. Our pcap only shows web traffic for Internet Explorer and the new Chromium-based Microsoft Edge. Both times, the URL generated by Qakbot was hxxp://store.nvprivateoffice[.]com/redir_ie.html.

To find this traffic, use the following Wireshark filter as shown in Figure 21:

http.request.full_uri contains store.nvprivateoffice

File Edit View	2020-01-29-Qbot-infection-traffic.pcap File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
http.request.fu	ll_uri contains store.nvpriv	ateoffice.com	X 🗆 🔹	Expression +	basic basic+	basic+DNS	
Time	Dst	Dst port	Host		Info		
+ 2020-01-29	15:56 89.105.198.	119 80	store.nvpr	ivateoffice.c	om GET /redir	_ie.html	
2020-01-29	15:56 89.105.198.	119 80	store.nvpr	ivateoffice.c	om GET /favic	on.ico HT	
2020-01-29	15:56 89.105.198.	119 80	store.nvpr	ivateoffice.c	om GET /redir	_ie.html	
2020-01-29	15:56 89.105.198.	119 80	store.nvpr	ivateoffice.c	om GET /favic	on.ico HT	
4						•	

Figure 21. Finding Qakbot traffic that opens web browsers on an infected Windows host. Follow the TCP stream for each of the two HTTP GET requests ending in redir_ie.html. The first request has a User-Agent in the HTTP headers for Internet Explorer as shown in Figure 22. The second request for the same URL has a User-Agent in the HTTP headers for the new Chromium-based Microsoft Edge as noted in Figure 23.



Figure 22. Qakbot traffic to store.nvprivateoffice[.]com using Internet Explorer 11.

Wireshark · Follow TCP Stream (tcp.stream)	eq 62) · 2020-01-29-Qbot-infection-traffic.pcap
<pre>GET /redir_ie.html HTTP/1.1 Host: store.nvprivateoffice.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0 Gecko) Chrome/79.0.3945.130 Safari/537.3 Accept: text/ntml,application/xntml+xml, apng,*/*;q=0.8,application/signed-exchan Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 HTTP/1.1 200 OK Server: nginx/1.12.2 Date: Wed, 29 Jan 2020 15:56:14 GMT Content-Type: text/html Content-Length: 97 Last-Modified: Fri, 09 Aug 2019 06:59:46 Connection: keep-alive ETag: "5d4d19e2-61" Accept-Ranges: bytes</pre>	; Win64; x64) AppleWebKit/537.36 (KHTML, like 6 Edg/79.0.309.71 application/xm; q=0.9, image/webp, image/ ge;v=b3;q=0.9 User-Agent string for the new Chromium-based Microsoft Edge browser on a Windows 10 host GMT
<html> <head> <meta content="4; U
</head>
</html></td><td>RL='https://www.msn.com'" http-equiv="refresh"/></head></html>	
2 client pkts, 3 server pkts, 3 turns.	
Entire conversation (1,923 bytes) -	Show and save data as ASCII - Stream 62 🗘
Find:	Find <u>N</u> ext
Filt	er Out This Stream Print Save as Back X <u>C</u> lose

Figure 23. Qakbot traffic to store.nvprivateoffice[.]com using the new Chromium-based Microsoft Edge.Finally, our pcap from the Qakbot-infected host also has email-related TCP traffic to various ports for various email protocols like SMTP, IMAP, and POP3. To get an idea of this non-web-related traffic, use the following Wireshark filter as shown in Figure 25: *tcp.flags eq 0x0002 and !(tcp.port eq 80) and !(tcp.port eq 443)*

		2020)-01-29-Qb	ot-infection-traffic.pcap		+ - • ×
<u>F</u> ile <u>E</u> dit <u>V</u> iew	<u>Go</u> <u>C</u> aptu	ure <u>A</u> nalyze <u>S</u> ta	tistics T	elephony <u>W</u> ireless <u>T</u>	ools <u>H</u> elp	0
		🕻 🎑 💩 📦	* 1	🗋 📃 🔍 Q	Q 👖	
tcp.flags eg 0x	0002 and !	(tcp.port eq 80) a	nd !(tcp.	port eg 443)	xpression	+ basic basic+ basic+DNS
Time		Src	Src port	Dst	Dst nort	Info
- 2020-01-29	15:54	10.1.29.101	49712	54.36.108.120	65400	49712 → 65400 [SYN] SE
2020-01-29	15:55	10.1.29.101	49720	54.36.108.120	65400	49720 → 65400 [SYN] St
2020-01-29	16:25	10.1.29.101	49915	69.49.109.87	25	49915 → 25 [SYN] Seg=(
2020-01-29	16:25	10.1.29.101	49916	208.47.185.20	110	49916 → 110 [SYN] Seq:
2020-01-29	16:25	10.1.29.101	49917	38.111.141.32	143	49917 → 143 [SYN] Seq:
2020-01-29	16:25	10.1.29.101	49918	69.49.109.87	465	49918 → 465 [SYN] Seq:
2020-01-29	16:25	10.1.29.101	49919	208.68.152.4	587	49919 → 587 [SYN] Seq:
2020-01-29	16:25	10.1.29.101	49920	208.50.94.55	25	49920 → 25 [SYN] Seq=(
2020-01-29	16:25	10.1.29.101	49921	38.111.141.32	993	49921 → 993 [SYN] Seq:
2020-01-29	16:25	10.1.29.101	49922	108.167.181.241	110	49922 → 110 [SYN] Seq:
2020-01-29	16:25	10.1.29.101	49923	38.111.141.32	995	49923 → 995 [SYN] Seq:
2020-01-29	16:25	10.1.29.101	49924	38.111.141.32	143	49924 → 143 [SYN] Seq:
2020-01-29	16:25	10.1.29.101	49925	66.102.1.28	465	49925 → 465 [SYN] Seq:
2020-01-29	16:25	10.1.29.101	49926	208.50.94.55	587	49926 → 587 [SYN] Seq=
2020-01-29	16:25	10.1.29.101	49927	208.47.185.20	993	49927 → 993 [SYN] Seq=
2020-01-29	16:25	10.1.29.101	49928	108.167.181.241	995	49928 → 995 [SYN] Seq=
2020-01-29	16:36	10.1.29.101	49931	208.68.152.4	25	49931 → 25 [SYN] Seq=(
2020-01-29	16:36	10.1.29.101	49932	108.167.181.241	110	49932 → 110 [SYN] Seq=
2020-01-29	16:36	10.1.29.101	49933	208.50.94.55	143	49933 → 143 [SYN] Seq:
2020-01-29	16:36	10.1.29.101	49934	66.102.1.28	465	49934 → 465 [SYN] Seq:
2020-01-29	16:36	10.1.29.101	49935	216.55.149.9	587	49935 → 587 [SYN] Seq:
2020-01-29	16:36	10.1.29.101	49935	216.55.149.9	587	[TCP Retransmission] 4
2020-01-29	16:36	10.1.29.101	49936	208.50.94.55	993	49936 → 993 [SYN] Seq=
2020-01-29	16:36	10.1.29.101	49935	216.55.149.9	587	[TCP Retransmission] 4
2020-01-29	16:36	10.1.29.101	49937	216.155.194.54	995	49937 → 995 [SYN] Seq=
2020-01-29	16:36	10.1.29.101	49935	216.55.149.9	587	[TCP Retransmission] 4
2020-01-29	16:40	10.1.29.101	49939	153.92.65.114	995	49939 → 995 [SYN] Seq:
2020-01-29	16:51	10.1.29.101	49946	153.92.65.114	995	49946 → 995 [SYN] Seq
2020-01-29	17:11	10.1.29.101	49950	153.92.65.114	995	49950 → 995 [SYN] Seq=
2020-01-29	17:31	10.1.29.101	49956	153.92.65.114	995	49956 → 995 [SYN] Seq:
1 2020 01 20	17:07	10 1 00 101	10050	153 00 65 114	005	ADDED . DOE LOVNI COT
				3334		

Figure 25. Getting an idea of the non-web-related traffic from this Qakbot infection. Figure 25 shows TCP connections and attempted TCP connections to various ports like 25, 110,143, 465, 587, 993, and 995 commonly used by different email protocols. The first two lines in the results show traffic to TCP port 65400, but reviewing the associated TCP streams indicates this also email-related traffic.

Use the following Wireshark filter to get a better idea of email-related traffic from the infected host as shown in Figure 26:

smtp or imap or pop

	2020-01-2	9-Qbot-infection	on-traffic.pcap • _ • ×
<u>File Edit View Go Capt</u>	ure <u>A</u> nalyze <u>S</u> tatistic	s Telephon	y <u>W</u> ireless <u>T</u> ools <u>H</u> elp
	3 🙆 🔍 🔹 📚 🥱	· 🕪 🌒 📃	
smtp or imap or pop			Expression + basic basic+ basic+DNS
Time	Src	Src port Inf	0
2020-01-29 16:25	69.49.109.87	25 S:	220 mail125c7.megamailservers.com ESMTP Sen
2020-01-29 16:25	208.47.185.20	110 S:	+OK POP3 ready
2020-01-29 16:25	38.111.141.32	143 Re	sponse: * OK CommuniGate Pro IMAP Server rea
2020-01-29 16:25	208.50.94.55	25 S:	220-mail.stratuswave.net ESMTP
2020-01-29 16:25	208.50.94.55	25 S:	220-MagicMail Daemon with Built-In Anti-Spa
2020-01-29 16:25	108.167.181.241	110 S:	+OK Dovecot ready.
2020-01-29 16:25	38.111.141.32	143 Re	sponse: * OK CommuniGate Pro IMAP Server rea
2020-01-29 16:25	208.68.152.4	587 S:	220 BCEX.BROOKSCOUNTYISD.NET Microsoft ESMT
2020-01-29 16:25	208.50.94.55	587 S:	220-mail.stratuswave.net ESMTP
2020-01-29 16:25	208.50.94.55	587 S:	220-MagicMail Daemon with Built-In Anti-Spa
2020-01-29 16:36	208.68.152.4	25 S:	220 barracuda.esc2.net ESMTP (b8f05b8c395c8
2020-01-29 16:36	108.167.181.241	110 S:	+OK Dovecot ready.
2020-01-29 16:36	208.50.94.55	143 Re	<pre>sponse: * OK [CAPABILITY IMAP4rev1 LITERAL+</pre>
2020-01-29 18:22	208.47.185.20	25 S:	220 mail.insightbb.com ESMTP
2020-01-29 18:22	208.47.185.20	25 S:	421 esmtp: protocol deviation
2020-01-29 18:22	209.86.93.204	110 S:	+OK NGPopper vEL_0_1_42_P at earthlink.net
2020-01-29 18:22	69.89.27.216	143 Re	sponse: * OK [CAPABILITY IMAP4rev1 SASL-IR L
4			

Figure 26. Finding email-related traffic caused by Qakbot in this pcap.

Follow some of the TCP streams to get a better idea for this type of email traffic. We do not normally see such unencrypted email traffic originating from a Windows client to public IP addresses. Along with other indicators, this *smtp or imap or pop* filter may reveal Qakbot activity.

Conclusion

This tutorial provided tips for examining Windows infections with Qakbot malware. More pcaps with examples of Qakbot 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>.