

Wireshark Tutorial: Examining Emotet Infection Traffic

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

Brad Duncan

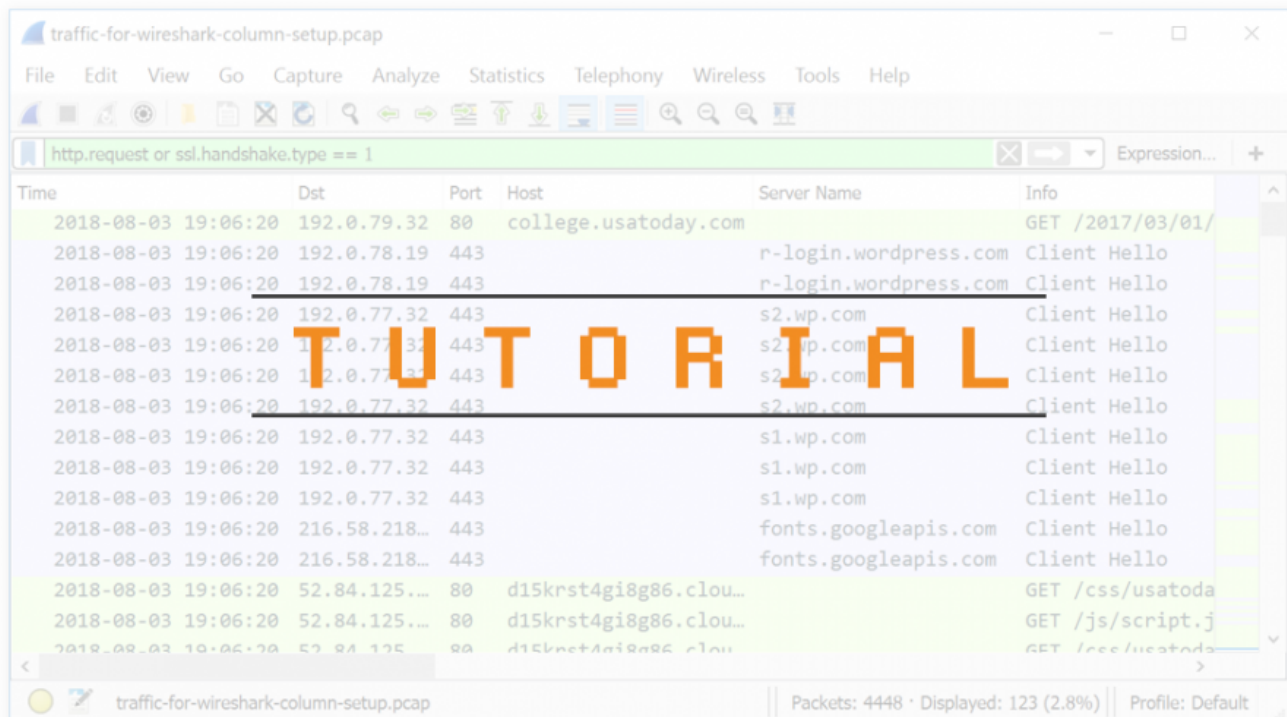
January 19, 2021

By [Brad Duncan](#)

January 19, 2021 at 6:00 AM

Category: [Tutorial](#), [Unit 42](#)

Tags: [Wireshark Tutorial](#)



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 [Wireshark](#) is necessary to understand this tutorial, which focuses on Wireshark version 3.x.

[Emotet](#) is an information-stealer first reported in 2014 as banking malware. It has since evolved with additional functions such as a dropper, distributing other malware families like [Gootkit](#), [IcedID](#), [Qakbot](#) and [Trickbot](#).

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 [our previous Wireshark tutorial about customizing the column display](#).

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.

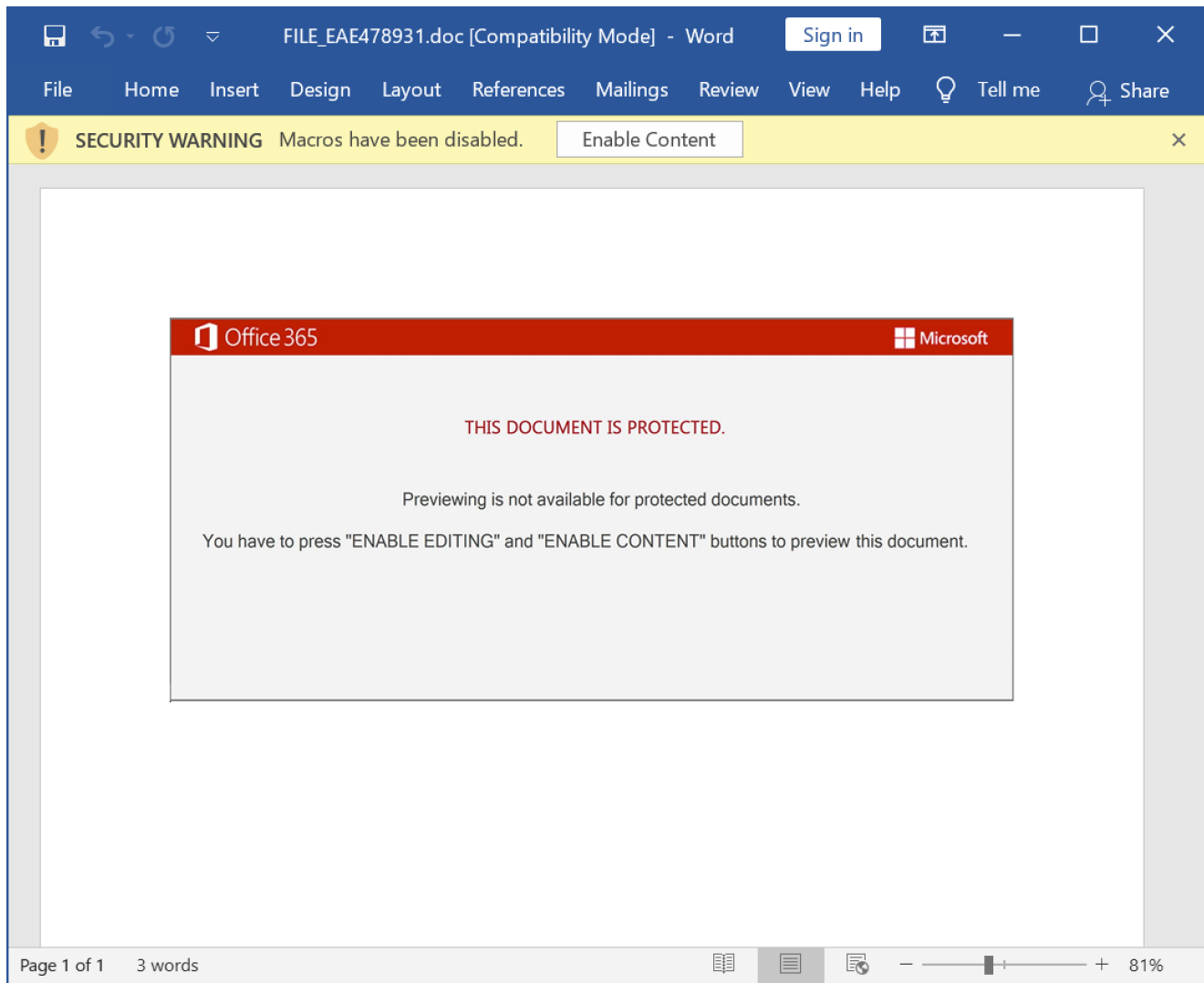


Figure 1. Screenshot of a Word document used to cause an Emotet infection in January 2021.

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.

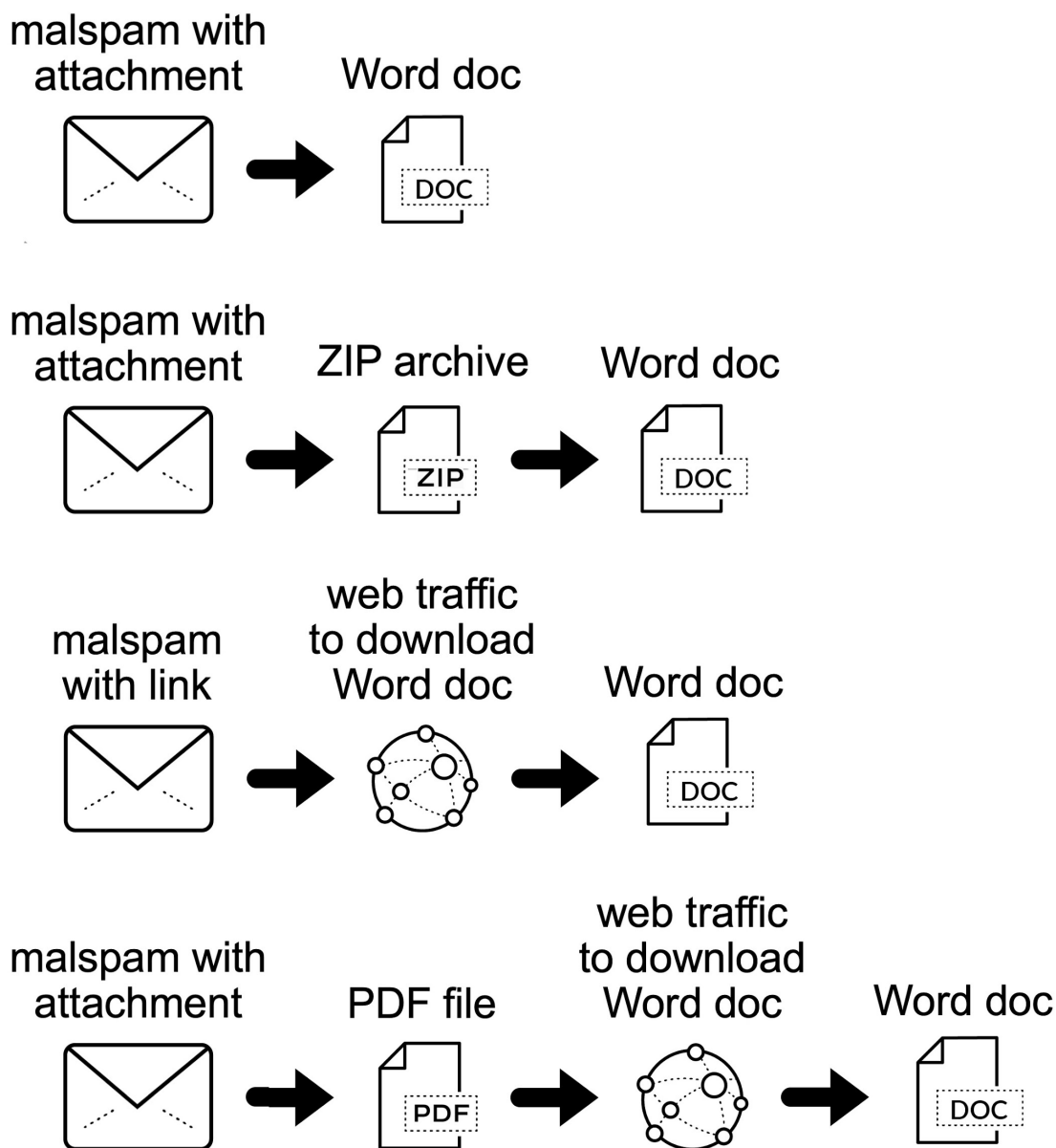


Figure 2. Various distribution paths for an Emotet Word document.

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.

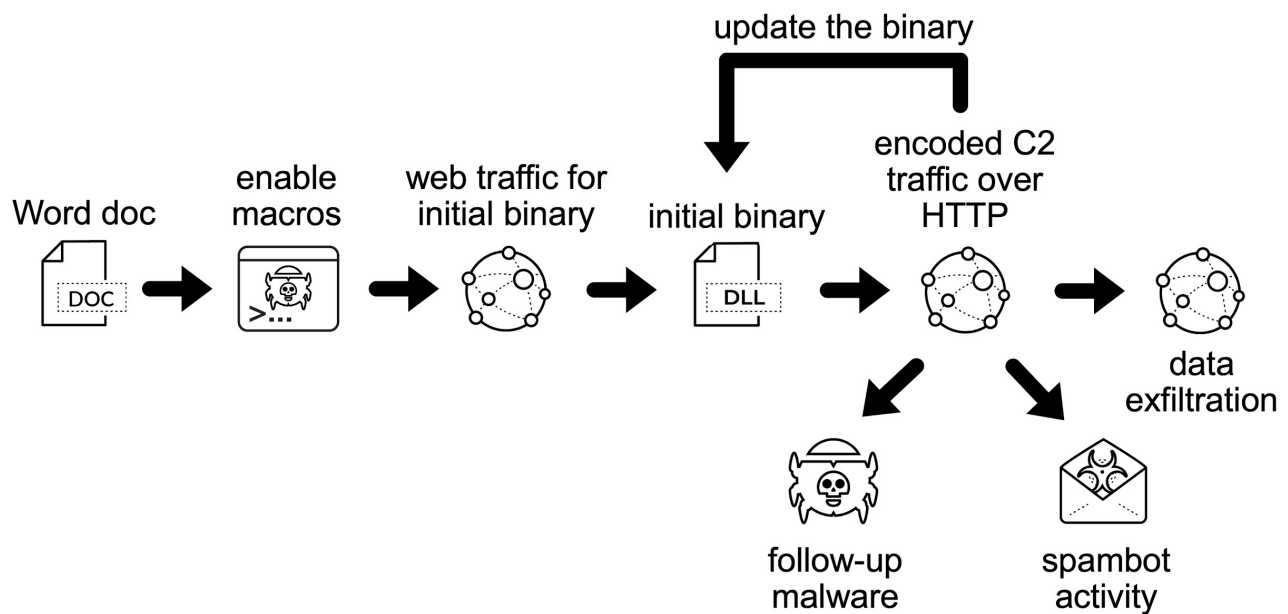


Figure 3. Flowchart for an Emotet infection.

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 [this GitHub repository](#). Once on the GitHub page, click on each of the ZIP archive entries and download them, as shown in Figures 4 and 5.

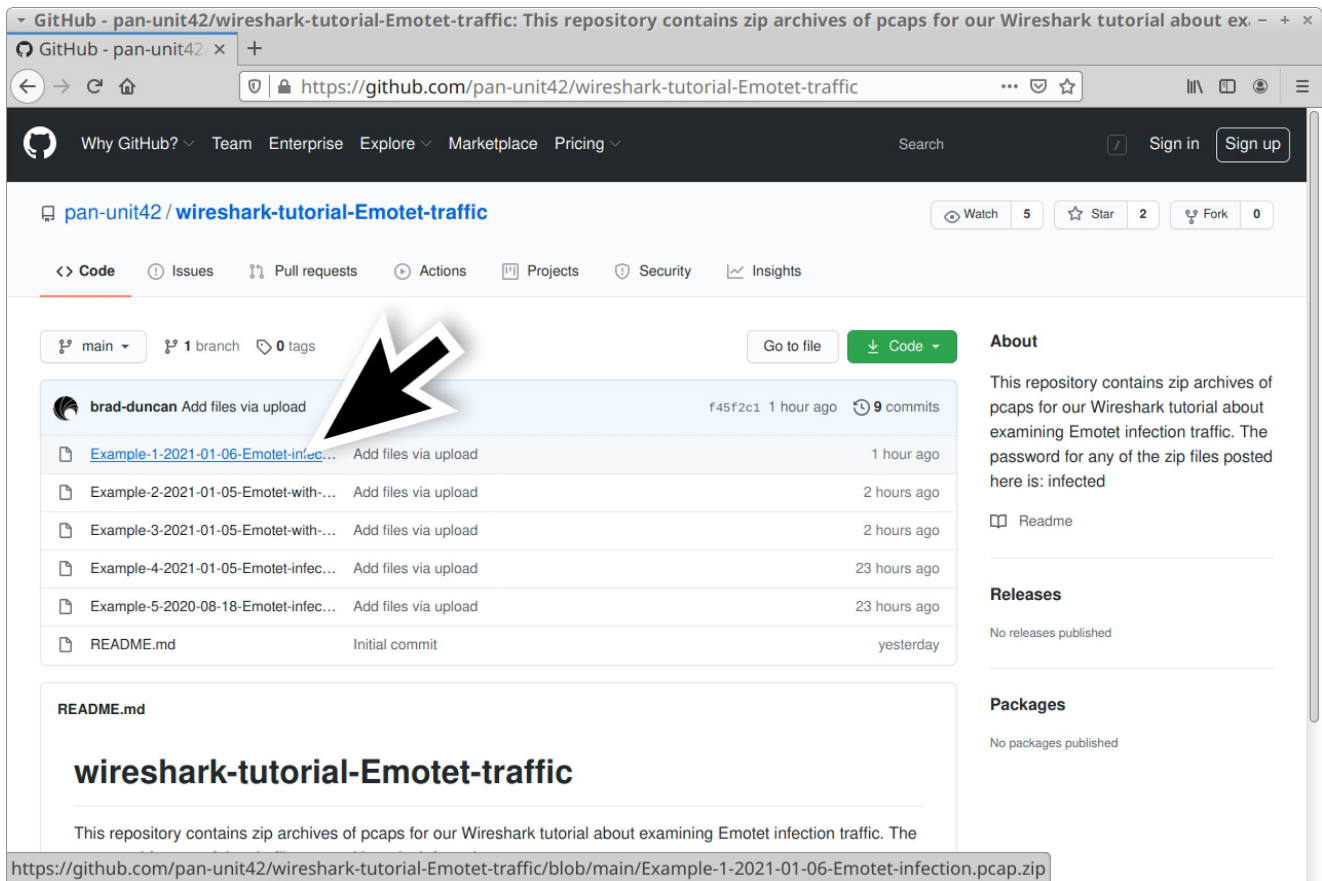


Figure 4. GitHub repository with links to ZIP archives used for this tutorial.

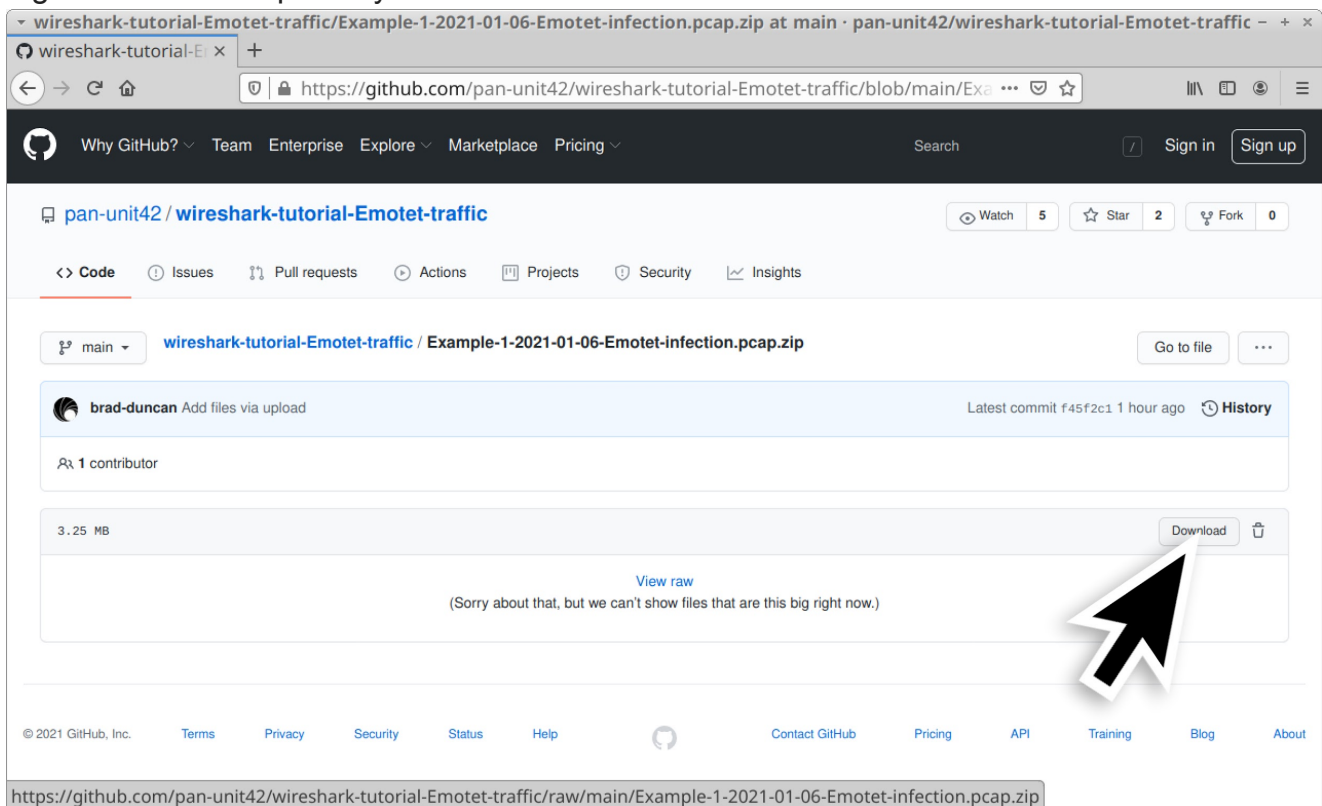


Figure 5. Downloading one of the ZIP archives for this tutorial.

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 [tutorial about Wireshark filters](#). 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 [tutorial about customizing Wireshark displays](#), your display should look similar to Figure 6.

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/1.1
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 /7u0e9j2avwlvnuyny/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/8l
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 /ves4up2v2n5qjq5r1/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
2021-01-06 16:47:11	104.05.04.118	443	stereocableprovcoti...	Client Hello

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/0I/

- 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.

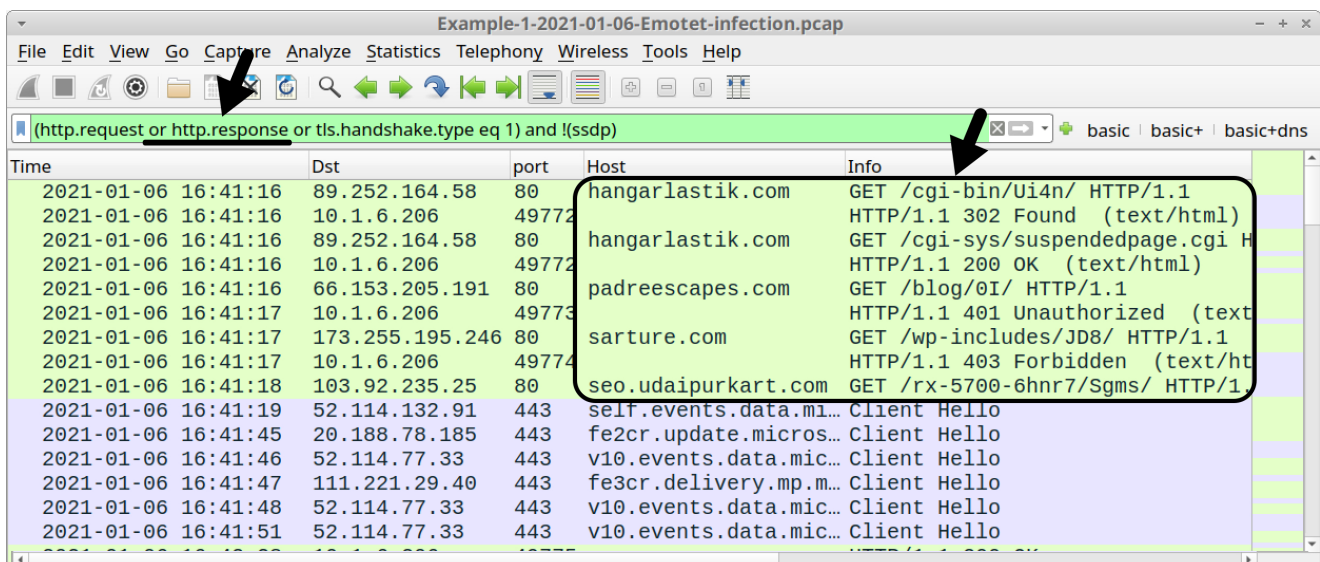


Figure 7. Adding HTTP responses to the Wireshark display filter.

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/0I/
- 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.

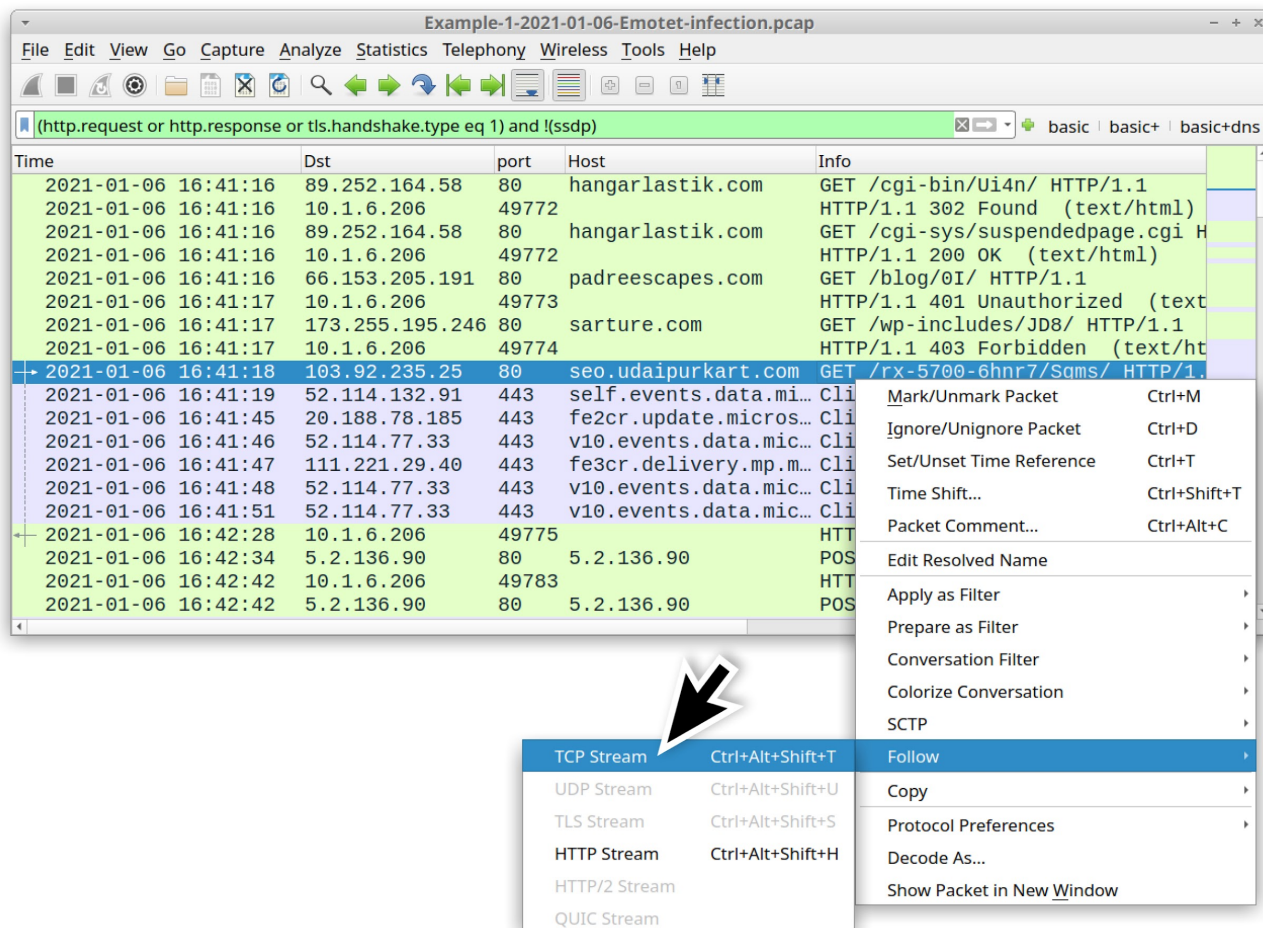


Figure 8. Following TCP stream for the HTTP request to seo.udaipurkart[.]com. The TCP stream shows indicators that seo.udaipurkart[.]com returned a Windows DLL file, as shown in Figure 9.

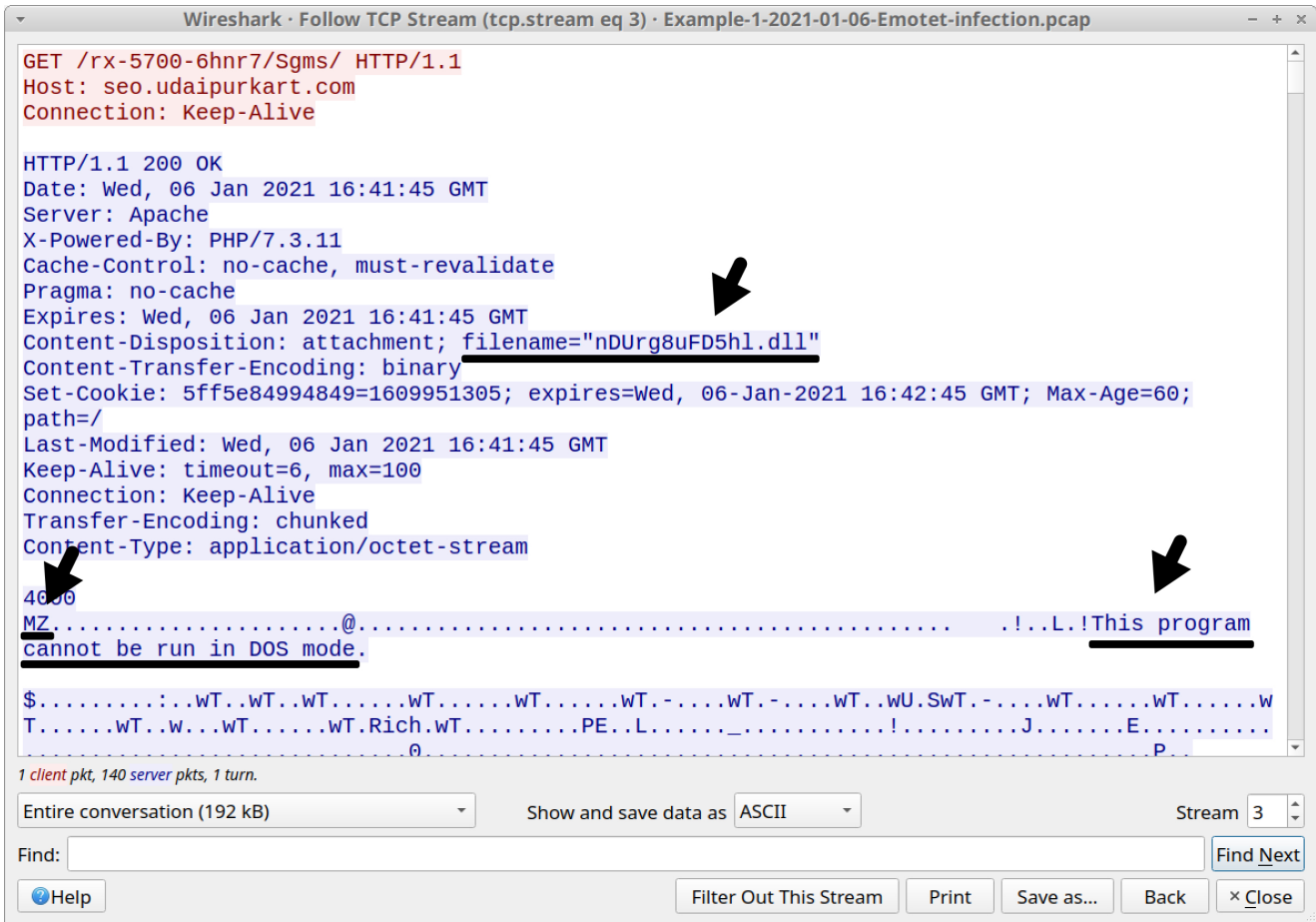


Figure 9. Indicators of a DLL file returned from seo.udaipurkart[.]com. Export this DLL from the pcap by using the menu path: **File --> Export Objects --> HTTP**, as shown in Figure 10. As always, we recommend you do not export this file in a Windows environment, since the DLL is Windows-based malware.

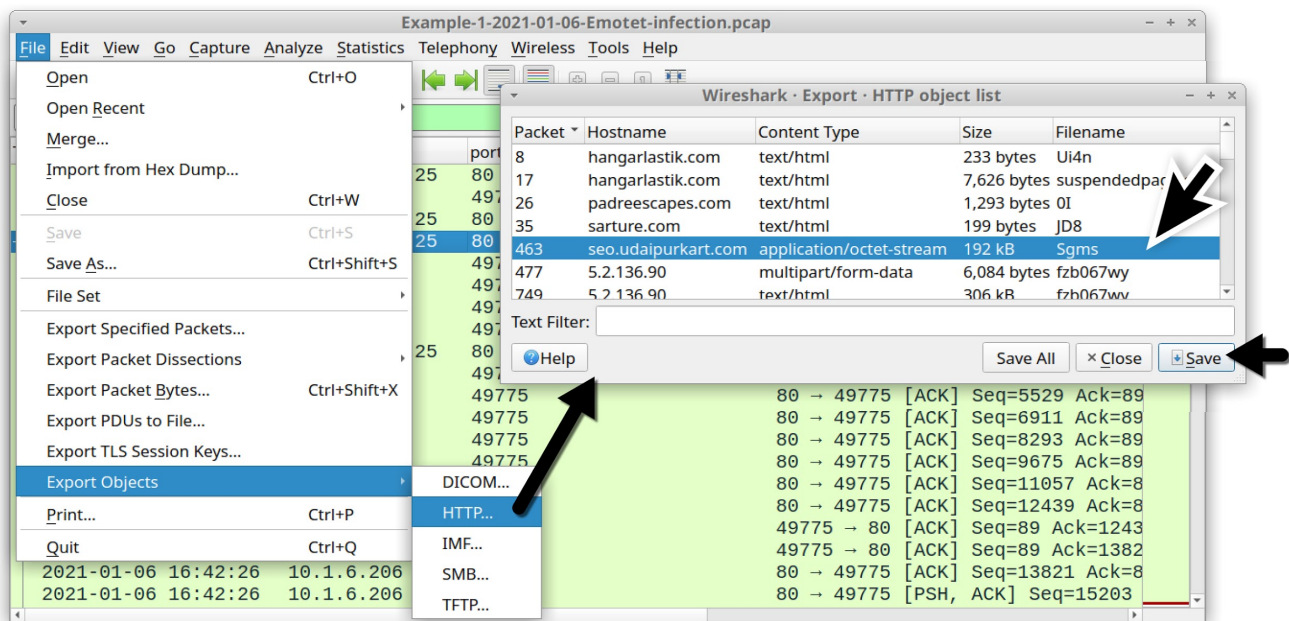


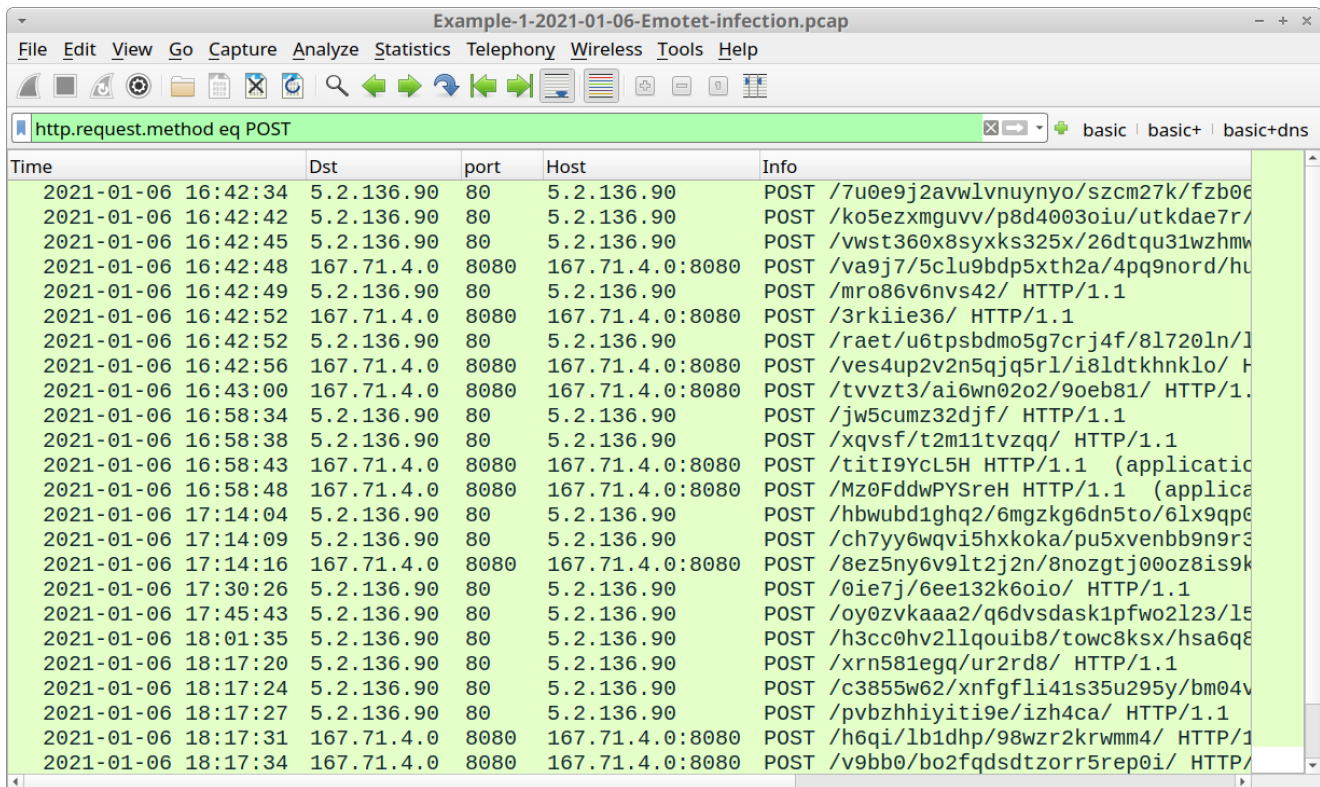
Figure 10. Exporting the Emotet DLL from our first pcap. The SHA256 hash for this extracted DLL is:

8e37a82ff94c03a5be3f9dd76b9dfc335a0f70efc0d8fd3dca9ca34dd287de1b

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.



Time	Dst	port	Host	Info
2021-01-06 16:42:34	5.2.136.90	80	5.2.136.90	POST /7u0e9j2avwlvnuyny/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/1
2021-01-06 16:42:56	167.71.4.0	8080	167.71.4.0:8080	POST /ves4up2v2n5qjq5r1/i8ldtkhnlklo/ H
2021-01-06 16:43:00	167.71.4.0	8080	167.71.4.0:8080	POST /tvvzt3/ai6wn0202/9oeb81/ 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 (applicat
2021-01-06 17:14:04	5.2.136.90	80	5.2.136.90	POST /hbwubd1ghq2/6mgzk6dn5to/6lx9qp6
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/q6dvsdask1pfw02l23/15
2021-01-06 18:01:35	5.2.136.90	80	5.2.136.90	POST /h3cc0hv2llqouib8/towc8ksx/hsa6q6
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/xnfgfli41s35u295y/bm04v
2021-01-06 18:17:27	5.2.136.90	80	5.2.136.90	POST /pvbzhhiyiti9e/izh4ca/ HTTP/1.1
2021-01-06 18:17:31	167.71.4.0	8080	167.71.4.0:8080	POST /h6qi/lb1dhp/98wzr2krwmm4/ HTTP/1
2021-01-06 18:17:34	167.71.4.0	8080	167.71.4.0:8080	POST /v9bb0/bo2fqdsdtzorr5rep0i/ 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.

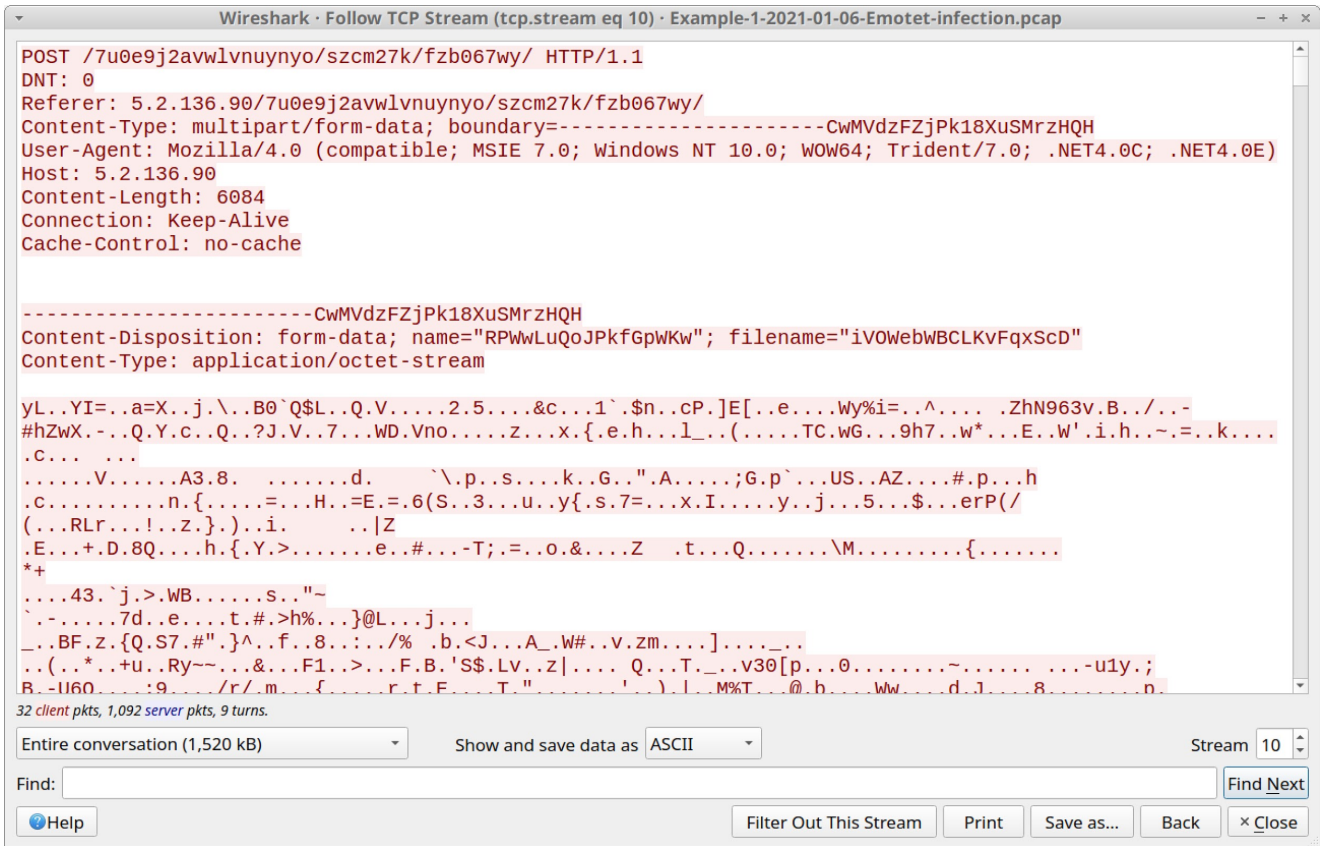


Figure 12. The first type of HTTP POST request for Emotet C2 traffic.

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.

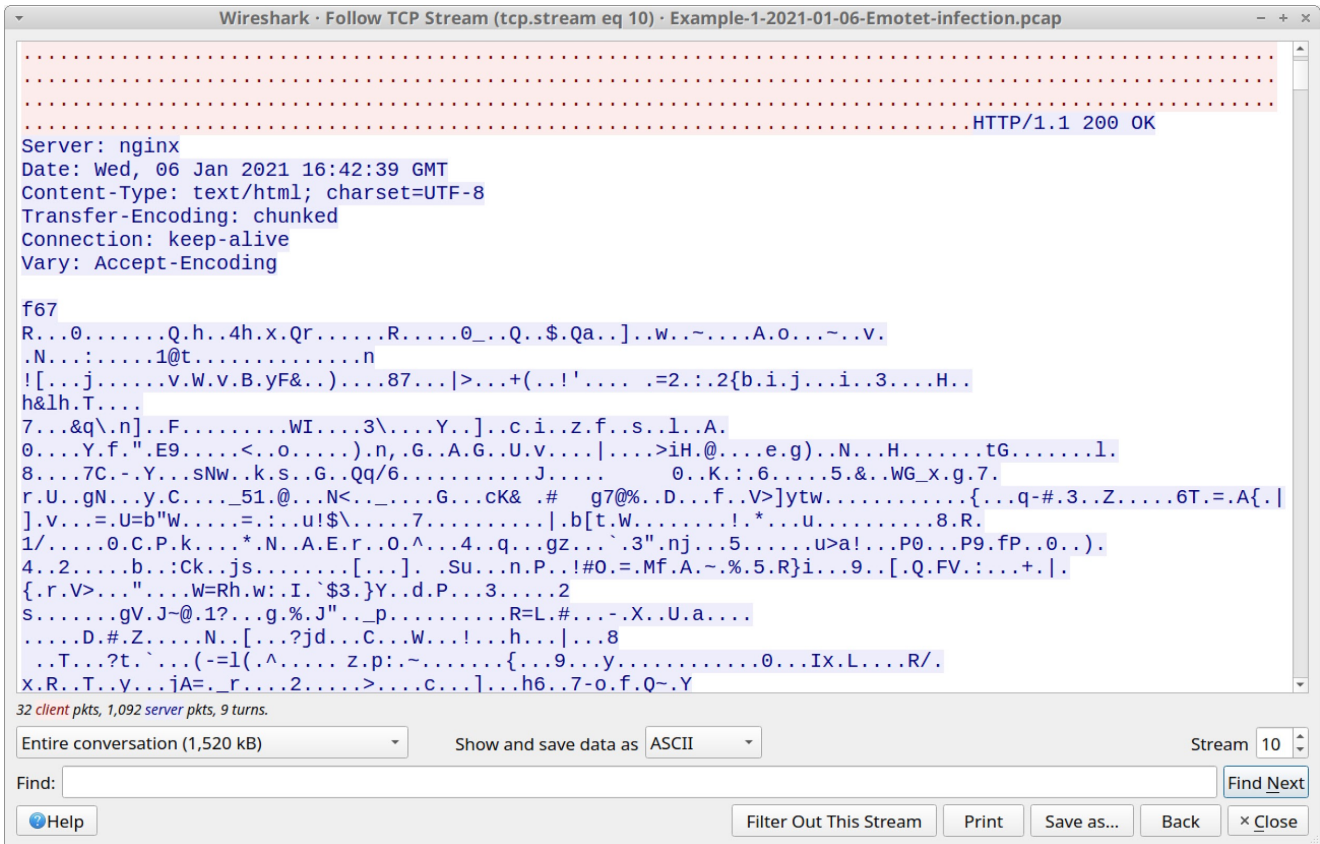


Figure 13. Encoded data returned from the server in response to the HTTP POST request. This type of encoded or encrypted data is how Emotet botnet servers exchange data with an infected Windows host. This is also the channel Emotet uses to update the Emotet DLL and drop follow-up malware.

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.

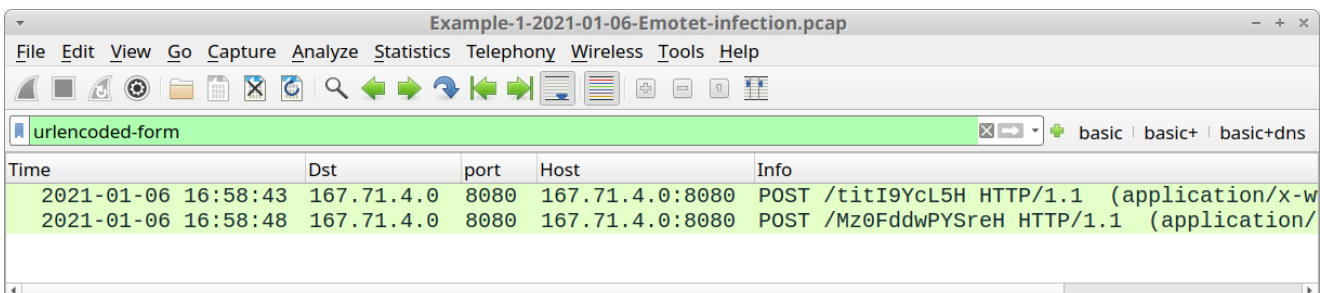


Figure 14. Filtering for the second type of HTTP POST request in Emotet C2 traffic. Follow the TCP stream for the first of these two HTTP POST requests at 16:58:43 UTC. Review the traffic. The results are shown in Figure 15.

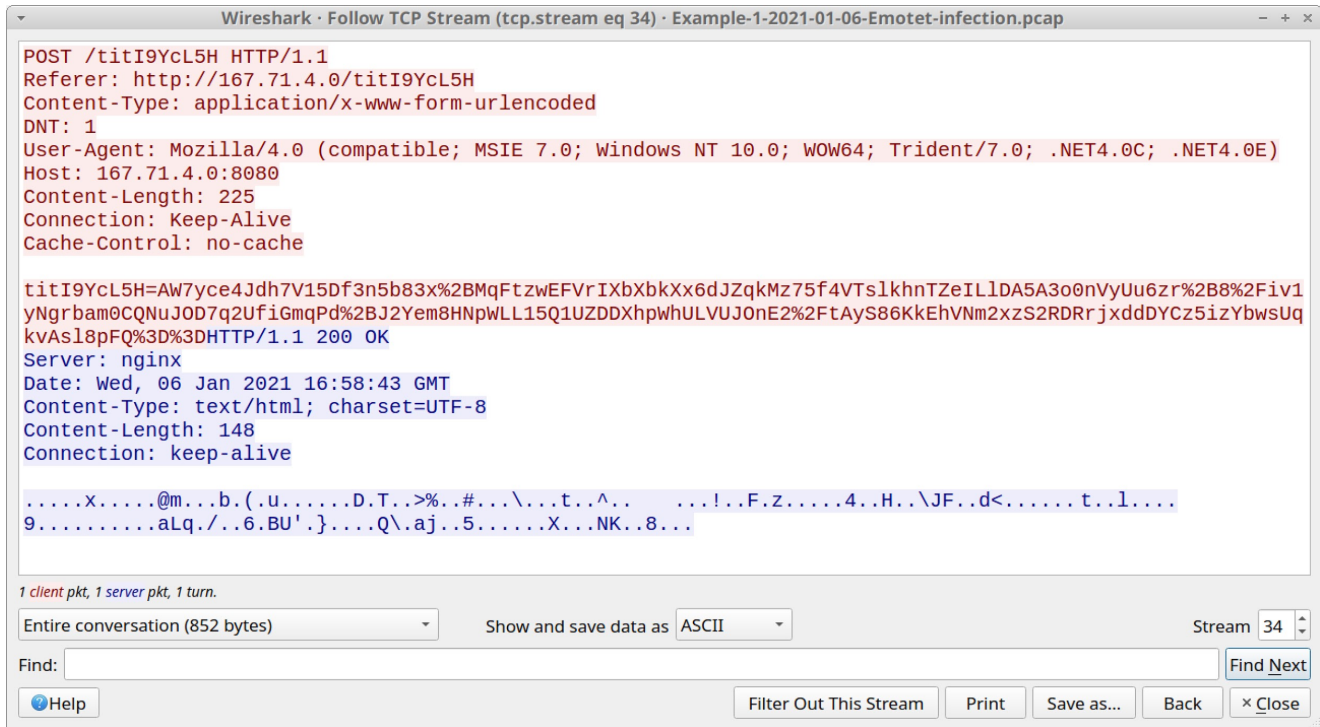


Figure 15. TCP stream for the second type of HTTP POST request in Emotet C2 traffic.

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.

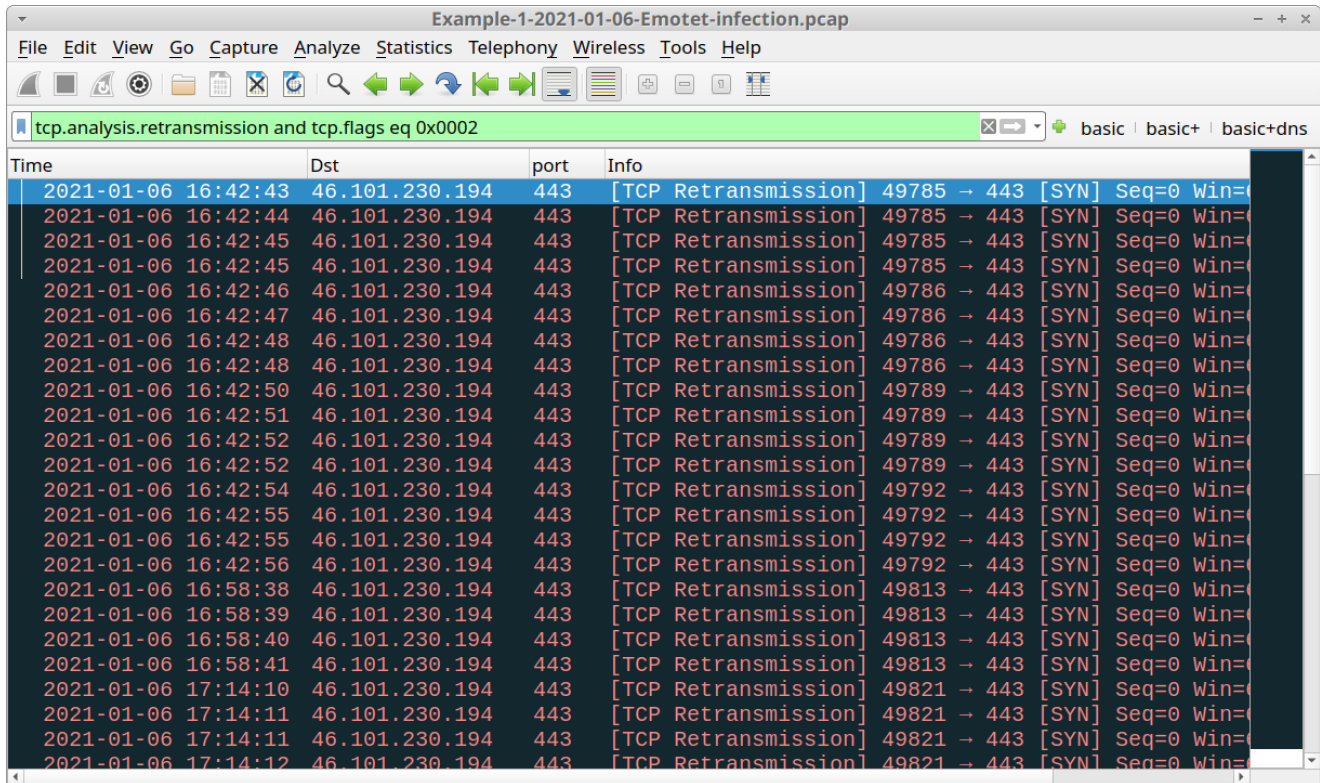


Figure 16. Filtering on retransmissions of TCP SYN segments in Wireshark.

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.

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/h9gu0nw8r
2021-01-05 19:49:25	104.236.52.89	8080	104.236.52.89:8080	POST /z1x928hdy3f92jatt/dytq2c
2021-01-05 19:49:38	125.0.215.60	80	125.0.215.60	POST /yajtvsgexg08cw/ 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	nti.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 this domain was reported as hosting an Emotet binary on Jan. 5, 2021, 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.

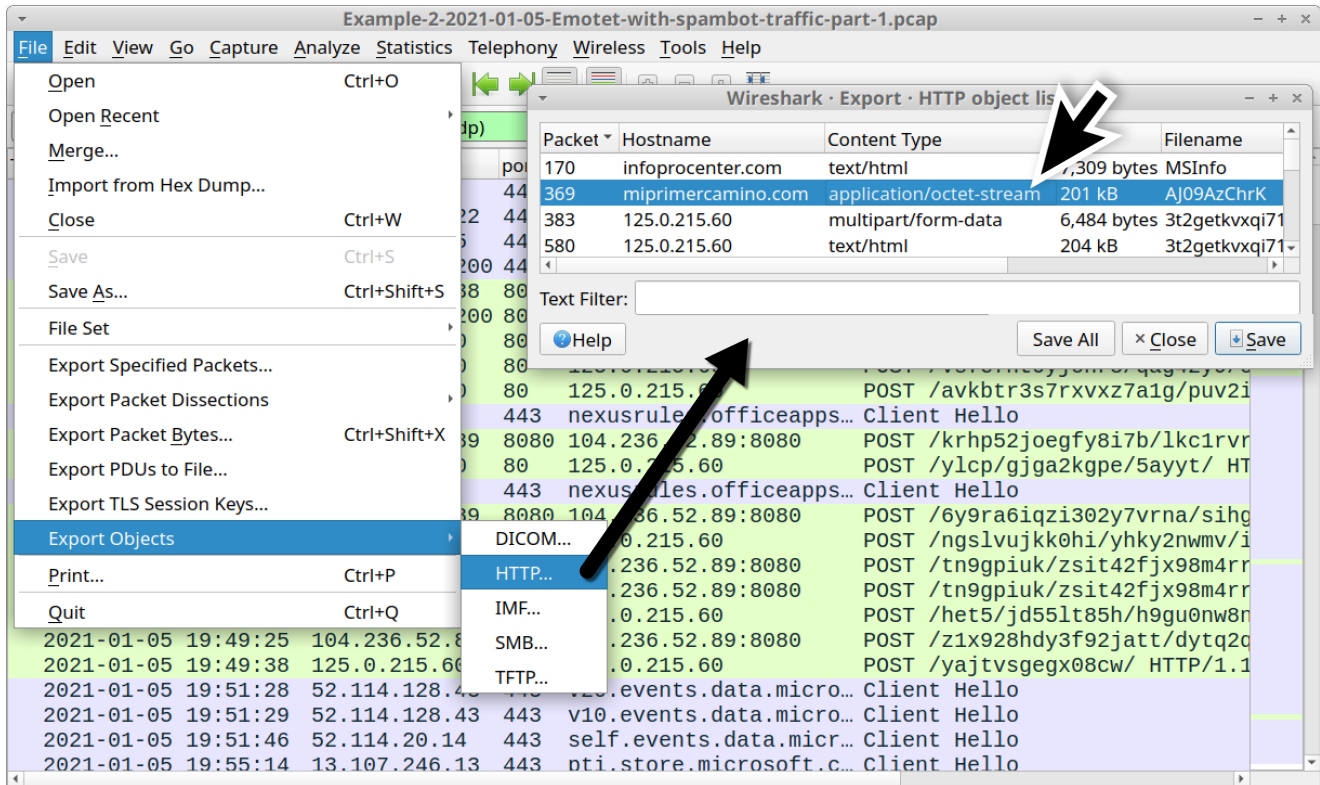


Figure 18. Exporting the Emotet DLL from the pcap.

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

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

(http.request or tls.handshake.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	194.25.134.110	465		Client Hello
2021-01-05 20:06:22	172.217.195.109	465		Client Hello
2021-01-05 20:06:22	172.217.195.109	465		Client Hello
2021-01-05 20:06:22	172.217.195.109	465		Client Hello
2021-01-05 20:06:22	172.217.195.109	465		Client Hello
2021-01-05 20:06:22	172.217.195.109	465		Client Hello
2021-01-05 20:06:22	172.217.195.109	465		Client Hello
2021-01-05 20:06:23	178.238.37.174	25		Client Hello
2021-01-05 20:06:23	202.168.255.44	25		Client Hello
2021-01-05 20:06:26	195.22.8.84	587		Client Hello
2021-01-05 20:06:28	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	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	198.71.240.9	587		Client Hello
2021-01-05 20:06:39	85.13.141.102	25		Client Hello
2021-01-05 20:06:40	65.99.248.136	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.

Time	Dst	port	Host	Info
2021-01-05 20:16:01	172.217.195.108	587		Client Hello
2021-01-05 20:16:01	172.217.195.108	587		Client Hello
2021-01-05 20:16:02	98.136.96.80	465		Client Hello
2021-01-05 20:16:02	173.231.241.171	465		Client Hello
2021-01-05 20:16:09	46.18.134.131	587		Client Hello
2021-01-05 20:16:09	162.214.70.141	465		Client Hello
2021-01-05 20:16:09	213.209.1.144	587		Client Hello
2021-01-05 20:16:10	195.3.96.71	25		Client Hello
2021-01-05 20:16:12	43.225.55.182	25		Client Hello
2021-01-05 20:16:15	108.167.137.28	25		Client Hello
2021-01-05 20:16:25	164.160.91.17	25		Client Hello
2021-01-05 20:16:31	162.219.249.113	25		Client Hello
2021-01-05 20:16:35	162.214.68.171	8080	162.214.68.171:8080	POST /vNcfHx0yDM
2021-01-05 20:16:36	162.214.70.141	465		Client Hello
2021-01-05 20:16:42	108.167.137.28	25		Client Hello
2021-01-05 20:16:45	103.21.59.169	25		Client Hello
2021-01-05 20:16:57	107.180.108.7	25		Client Hello
2021-01-05 20:17:00	162.214.68.171	8080	162.214.68.171:8080	POST /oefPeUB4q5
2021-01-05 20:17:02	162.214.70.141	465		Client Hello
2021-01-05 20:17:03	82.118.225.196	7080	82.118.225.196:7080	POST /J8JVUHb6J9
2021-01-05 20:17:04	52.185.211.133	443	settings-win.data.microsoft.com	Client Hello
2021-01-05 20:17:04	13.107.5.88	443	evoke-windowservices-tas.msedge...	Client Hello
2021-01-05 20:17:12	103.21.59.169	25		Client Hello
2021-01-05 20:17:22	213.94.78.178	465		Client Hello
2021-01-05 20:17:23	64.233.169.109	25		Client Hello
2021-01-05 20:17:23	213.227.17.168	587		Client Hello

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.

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
2021-01-05 20:19:38	193.252.22.84	25	from: "Juan Diaz <JDIAZ@THY.COM>" <ozdemir.nuran@orange.f
2021-01-05 20:19:47	193.252.22.84	25	from: "Green Mountains Laboratory Inc <office@gml-v.com>'
2021-01-05 20:19:51	193.252.22.84	25	from: "Green Mountains Laboratory Inc <office@gml-v.com>'
2021-01-05 20:19:54	193.252.22.84	25	from: "Gladisbel Miranda <gmiranda@randgeng.com>" <ozdemir

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

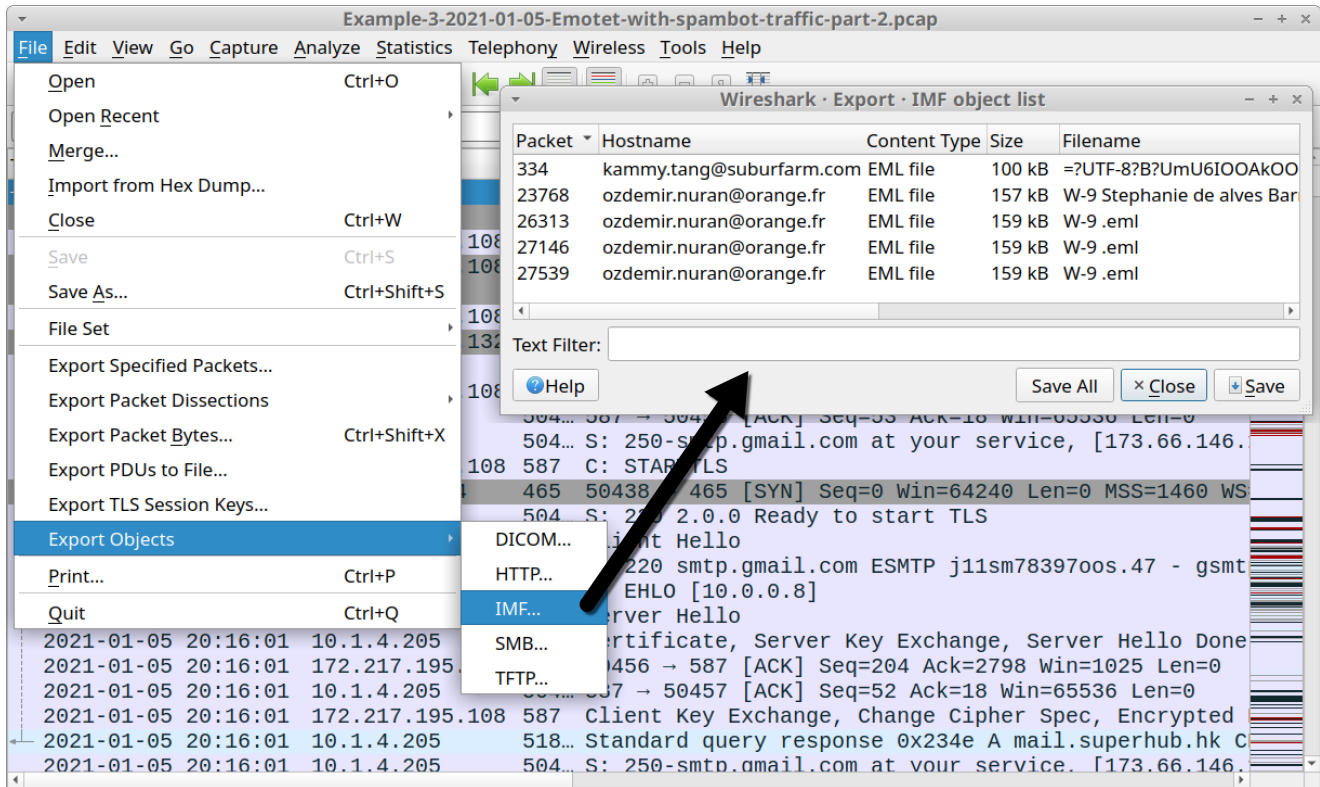


Figure 24. Exporting Emotet malspam from our third pcap.

Export these emails and examine them. Ideally, we recommend doing this in a non-Windows environment. [Thunderbird](#) 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.

Time	Dst	port	Host	Info
2021-01-05 17:15:55	173.254.250.226	443	fathekarim.com	Client Hello
2021-01-05 17:15:56	52.242.211.89	443	client.wns.windows.com	Client Hello
2021-01-05 17:15:56	40.91.76.238	443	licensing.mp.microsoft.com	Client Hello
2021-01-05 17:16:04	90.160.138.175	80	90.160.138.175	POST /agyjkoxblu/ HTTP/1
2021-01-05 17:16:45	23.3.86.10	443	storeedgefd.dsx.mp.micros...	Client Hello
2021-01-05 17:16:45	23.3.86.10	443	storeedgefd.dsx.mp.micros...	Client Hello
2021-01-05 17:16:46	23.48.32.27	443	img-prod-cms-rt-microsoft...	Client Hello
2021-01-05 17:16:56	23.3.86.10	443	livetileedge.dsx.mp.micro...	Client Hello
2021-01-05 17:20:57	23.66.131.11	443	storecatalogrevocation.st...	Client Hello
2021-01-05 17:21:55	52.114.159.34	443	v10.events.data.microsoft...	Client Hello
2021-01-05 17:22:58	52.114.75.79	443	v10.events.data.microsoft...	Client Hello
2021-01-05 17:29:19	52.137.106.217	443	settings-win.data.microso...	Client Hello
2021-01-05 17:29:20	13.107.5.88	443	evoke-windowsservices-tas...	Client Hello
2021-01-05 17:30:19	52.109.12.19	443	nexusrules.officeapps.liv...	Client Hello
2021-01-05 17:31:10	90.160.138.175	80	90.160.138.175	POST /t8yph1u/khoa190/hjy...
2021-01-05 17:37:57	52.114.159.112	443	v10.events.data.microsoft...	Client Hello
2021-01-05 17:46:39	90.160.138.175	80	90.160.138.175	POST /9c8b/h2psftp4eiyv/...
2021-01-05 17:51:25	13.107.43.23	443	config.edge.skype.com	Client Hello
2021-01-05 18:02:56	90.160.138.175	80	90.160.138.175	POST /a4rspfrvf/atfj6ouc...
2021-01-05 18:03:00	90.160.138.175	80	90.160.138.175	POST /h6jk7r5fx0/azyhusr...
2021-01-05 18:03:00	167.99.105.11	8080	167.99.105.11:8080	POST /mVfIeEcm8a HTTP/1.1
2021-01-05 18:03:02	167.99.105.11	8080	167.99.105.11:8080	POST /eUCxd691 HTTP/1.1
2021-01-05 18:03:05	90.160.138.175	80	90.160.138.175	POST /2dhrftruljndz4cjt/...
2021-01-05 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.

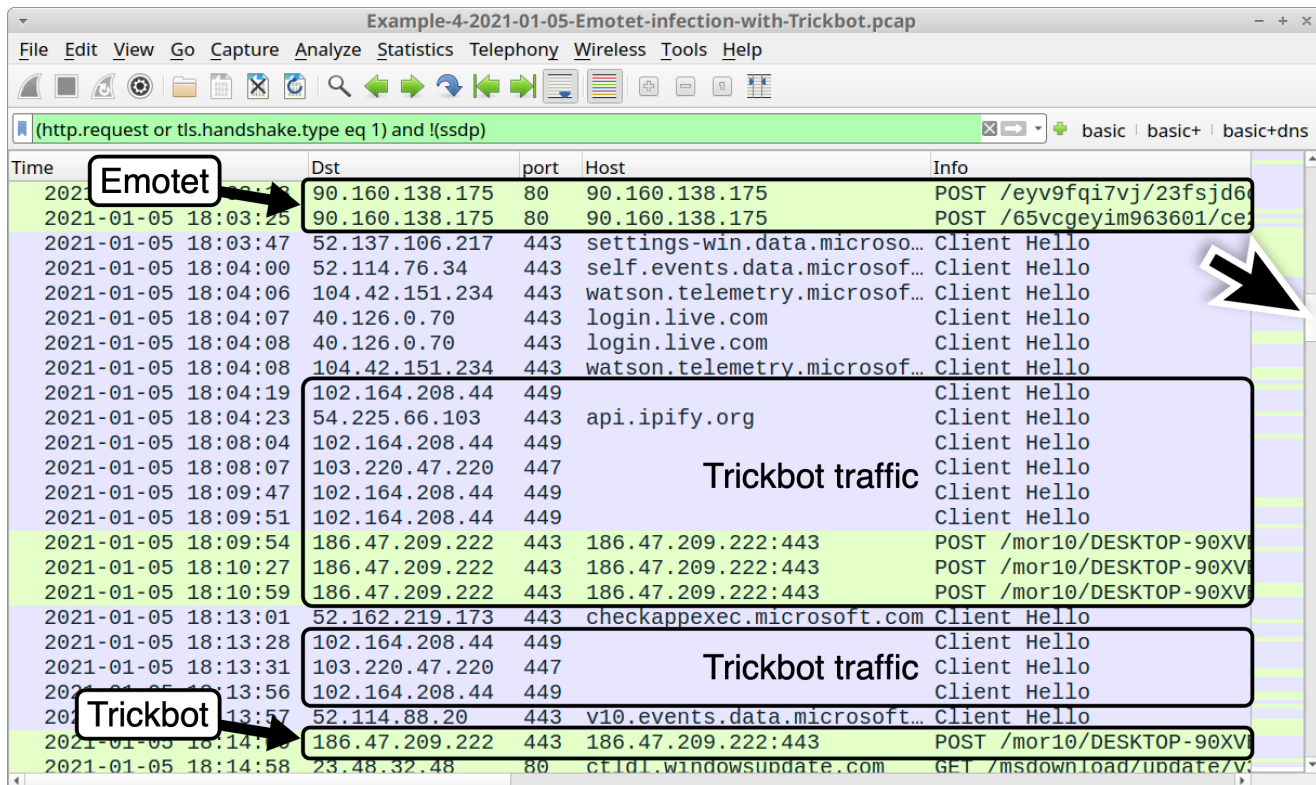


Figure 26. Scrolling down the column display to find Trickbot indicators in our fourth pcap using a basic web filter.

We've reviewed Trickbot in [our previous Wireshark tutorial on examining Trickbot infections](#), 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.

Time	Dst	port	Host	Info
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 18:13:56	102.164.208.44	449		Client Hello
2021-01-05 18:19:09	102.164.208.44	449		Client Hello
2021-01-05 18:22:40	102.164.208.44	449		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 traffic over TCP port 447 or TCP port 449.

Time	Dst	port	Host	Info
2021-01-05 18:09:54	186.47.209.222	443	186.47.209.222:443	POST /mor10/DESKTOP-90XVB7Q
2021-01-05 18:10:27	186.47.209.222	443	186.47.209.222:443	POST /mor10/DESKTOP-90XVB7Q
2021-01-05 18:10:59	186.47.209.222	443	186.47.209.222:443	POST /mor10/DESKTOP-90XVB7Q
2021-01-05 18:14:09	186.47.209.222	443	186.47.209.222:443	POST /mor10/DESKTOP-90XVB7Q

Figure 28. Filtering for HTTP POST requests associated with Trickbot data exfiltration.

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.

Time	Dst	port	Host	Info
2021-01-05 19:56:32	192.119.162.87	80	192.119.162.87	GET /images/saved.png HTTP/1.1
2021-01-05 20:17:28	192.119.162.87	80	192.119.162.87	GET /images/mingup.png HTTP/1.1
2021-01-05 20:18:39	192.119.162.87	80	192.119.162.87	GET /images/mingup.png HTTP/1.1
2021-01-05 20:18:54	192.119.162.87	80	192.119.162.87	GET /images/saved.png HTTP/1.1

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.

Time	Dst	port	Host	Info
2020-08-18 21:23:38	198.70.69.144	80	www.msftncsi.com	GET /ncsi.txt HT
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 /UwjHXosfee
2020-08-18 21:25:01	82.163.245.38	80	82.163.245.38	POST /tLJcyWZ/Cc
2020-08-18 21:25:02	45.55.82.2	8080	45.55.82.2:8080	POST /YWXhUDN/Fp
2020-08-18 21:25:07	82.163.245.38	80	82.163.245.38	POST /lZjGtKXueE
2020-08-18 21:25:07	45.55.82.2	8080	45.55.82.2:8080	POST /bfd2SwL/OV
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 /JrvH5PyKht
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 /iwak1vp47V
2020-08-18 21:25:32	82.163.245.38	80	82.163.245.38	POST /X2IXP07A0K
2020-08-18 21:26:28	13.107.246.10	443	nti.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 a URL reported as hosting an Emotet Word document on the same date. 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. This domain was 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.

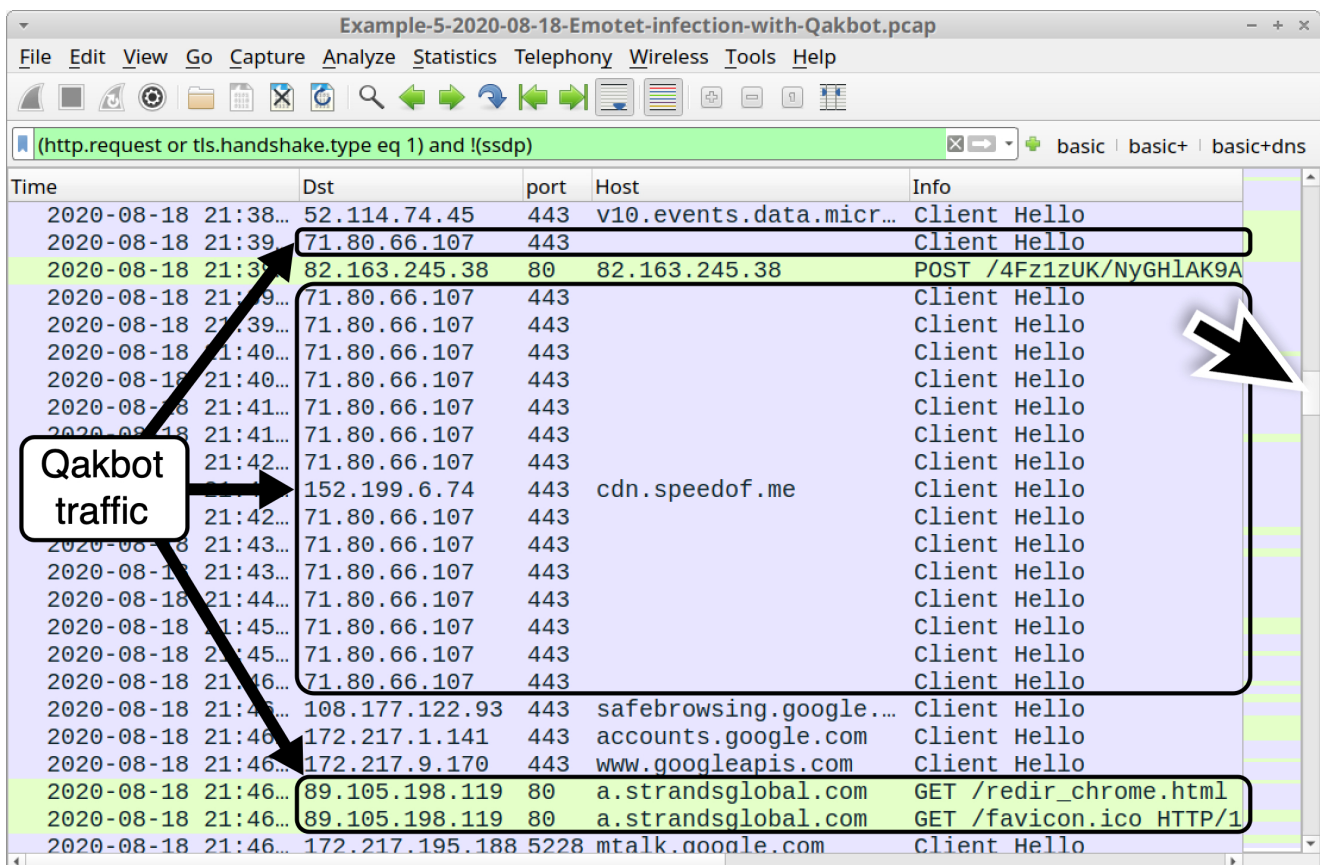


Figure 31. Scrolling down the column display to find Qakbot indicators in our fifth pcap using a basic web filter.

We've reviewed Qakbot in our previous Wireshark tutorial on examining Qakbot infections, 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.

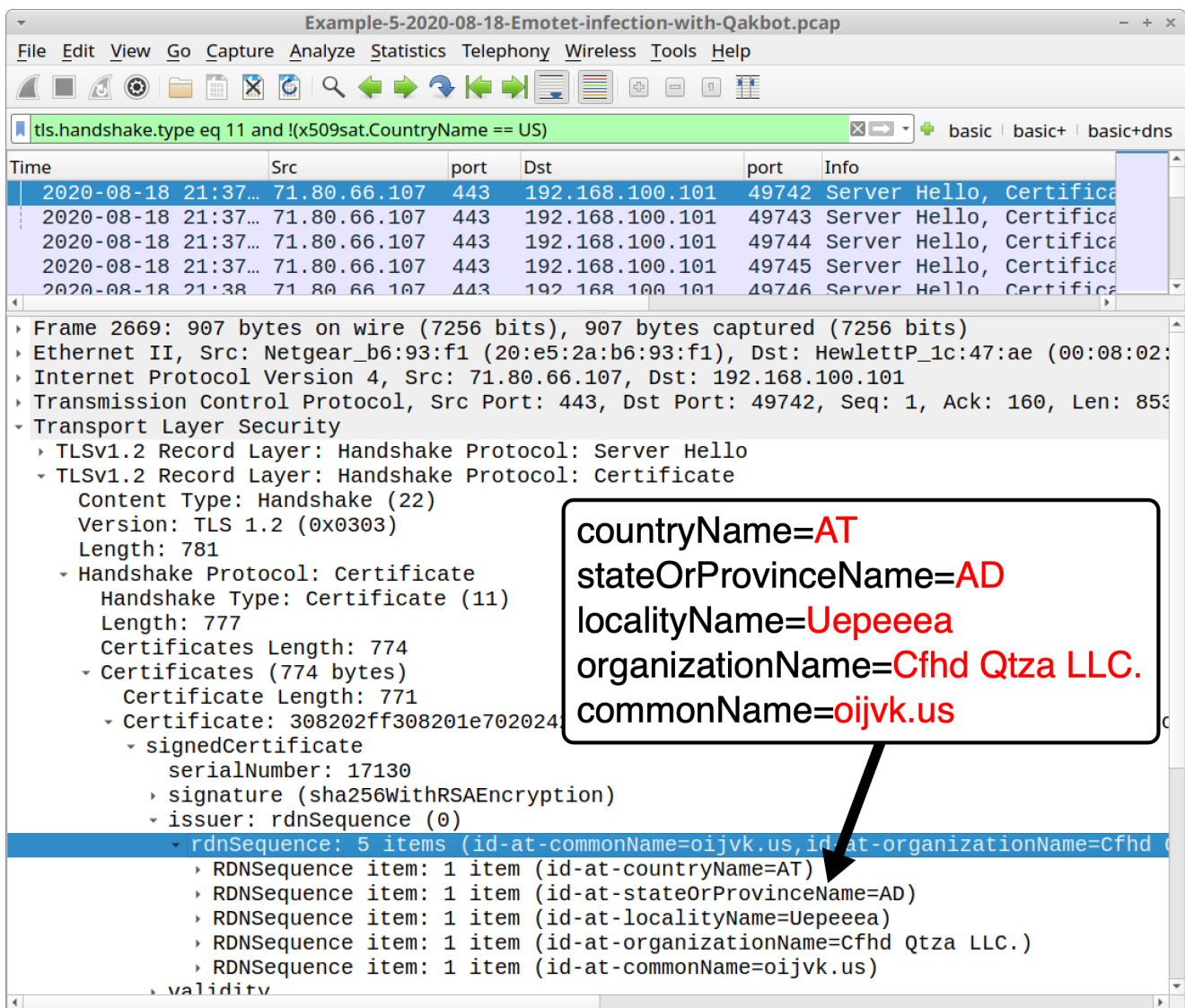


Figure 32. Filtering and searching for unusual certificate issuer data in HTTPS traffic generated by Qakbot.

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.

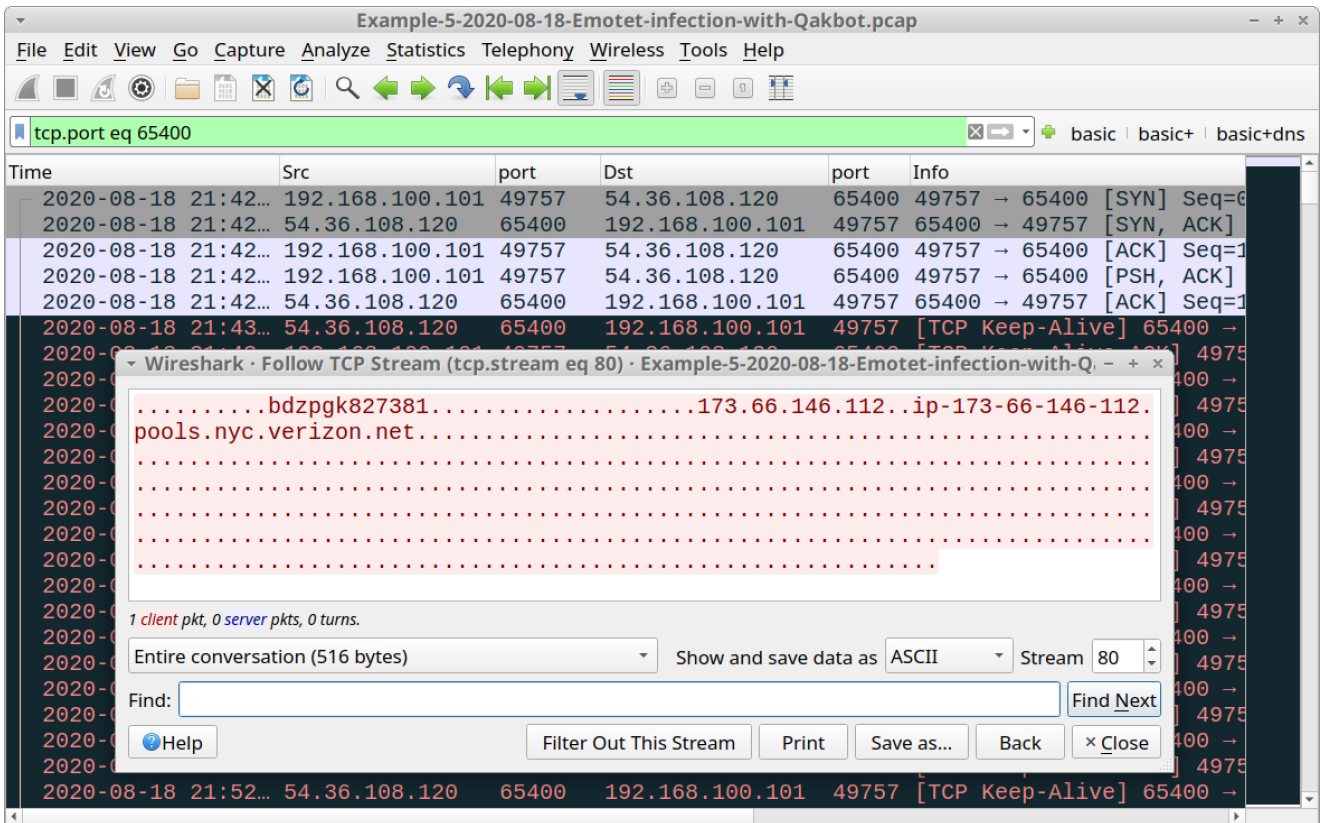


Figure 33. Filtering for Qakbot traffic over TCP port 65400.

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.

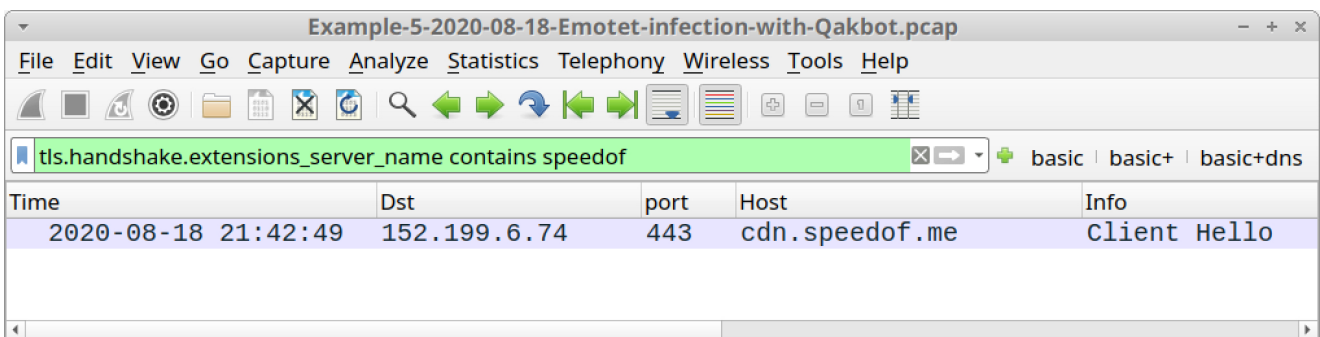


Figure 34. Filtering for traffic to cdn.speedof[.]me, which is not inherently malicious, but a connectivity check caused by Qakbot prior to late November 2020.

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.strandsglobal[.]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 [Terms of Use](#) and acknowledge our [Privacy Statement](#).