2020-07-31 - TRAFFIC ANALYSIS EXERCISE ANSWERS

Link to exercise: https://www.malware-traffic-analysis.net/2020/07/31/index.html

Links to some tutorials I've written that should help with this exercise:

- Customizing Wireshark - Changing Your Column Display
- Using Wireshark: Identifying Hosts and Users
- Using Wireshark - Display Filter Expressions
- Using Wireshark: Exporting Objects from a Pcap

ENVIRONMENT:

- LAN segment range: 10.07.31.0/24 (10.07.31.0 through 10.07.31.255)
- Domain: tecsolutions.info
- Domain controller: 10.07.31.7 - Tecsolutions-DC
- LAN segment gateway: 10.07.31.1
- LAN segment broadcast address: 10.07.31.255

INCIDENT REPORT:

Executive summary:

On Friday, 2020-07-31 at approximately 00:26 UTC, a Windows 10 host used by Gregory Simmons was infected with Emotet malware.

Victim details:

IP address: 10.7.31.101
MAC address: 00:0c:6e:12:af:38 (ASUSTekC_68:42:d3)
Host name: DESKTOP-PDHW305
User account name: gregory.simmons

Indicators of compromise (IOCs):

SHA256 hash: 537ceaaf4b76967b916c857bf8113e6b6ccc65dca06df2d300b66b8a61d9eedc

- File size: 176,692 bytes
- File name: INVOICE-OR85-923315.doc
- File location: http://e-dsm.com.br/www/ZdJCAB/
- File description: Word doc with macros for Emotet

SHA256 hash: 0a3aaa398a6abe7a4ba256812b8b6632fa4595b4ac5c47b459d5a6a911c2d202

- File size: 913,503 bytes
- File name: 3tknamb7298632293.exe
- File location: http://jambino.us/tv/DYsPb/
- File description: Windows executable file (EXE) for Emotet

HTTP traffic to retrieve the Word doc and Emotet EXE:

- 191.6.208.51 port 80 - e-dsm.com.br - GET /www/ZdJCAB/
- 67.20.112.81 port 80 - jambino.us - GET /tv/DYsPb/

HTTP traffic for Emotet post-infection activity:

- 201.235.10.215 port 80 - 201.235.10.215 - POST /RLVIcVHpdWjKMHfJsK/bhAzHJy/vazwovI5B9BcchWQ/d0EvU2Xl/HQ7AQetdQggMrPULmis/
- 201.235.10.215 port 80 - 201.235.10.215 - POST /M7aBEffyXE/Upa44JYc0iD8C5Co5qj/QxcEX6A0fDBvDo/
- 104.236.52.89 port 8080 - 104.236.52.89:8080 - POST /y1Oc/CRTtjoStAe/03wHuC/
- 201.235.10.215 port 80 - 201.235.10.215 - POST /2lOJG5Lepy9SF/6rmms2u4C61LmFD/hJubcUz/13vVTTA5/kRmZYIUJ67VF1I/GyiwnO6oOQatOesN4K/
- 201.235.10.215 port 80 - 201.235.10.215 - POST /qKSwAKe1Mi/y5QsEBixxmL45MPHwaD/smvp/78W7iuovnPDTvP2w/10jxRo2zF6M/
- 201.235.10.215 port 80 - 201.235.10.215 - POST /o9O08G04DzIZG8OWRp/
- 201.235.10.215 port 80 - 201.235.10.215 - POST /LCWZY47XwmugeO3/3z2TvDhczd/
- 104.236.52.89 port 8080 - 104.236.52.89:8080 - POST /rQDNZBxm3Rpz/YdX3soU3MRPD/fXFnwkKVcXuwwBkpsSq/
- 201.235.10.215 port 80 - 201.235.10.215 - POST /aNIce30YT/xzZyFctinQ3Jkn/

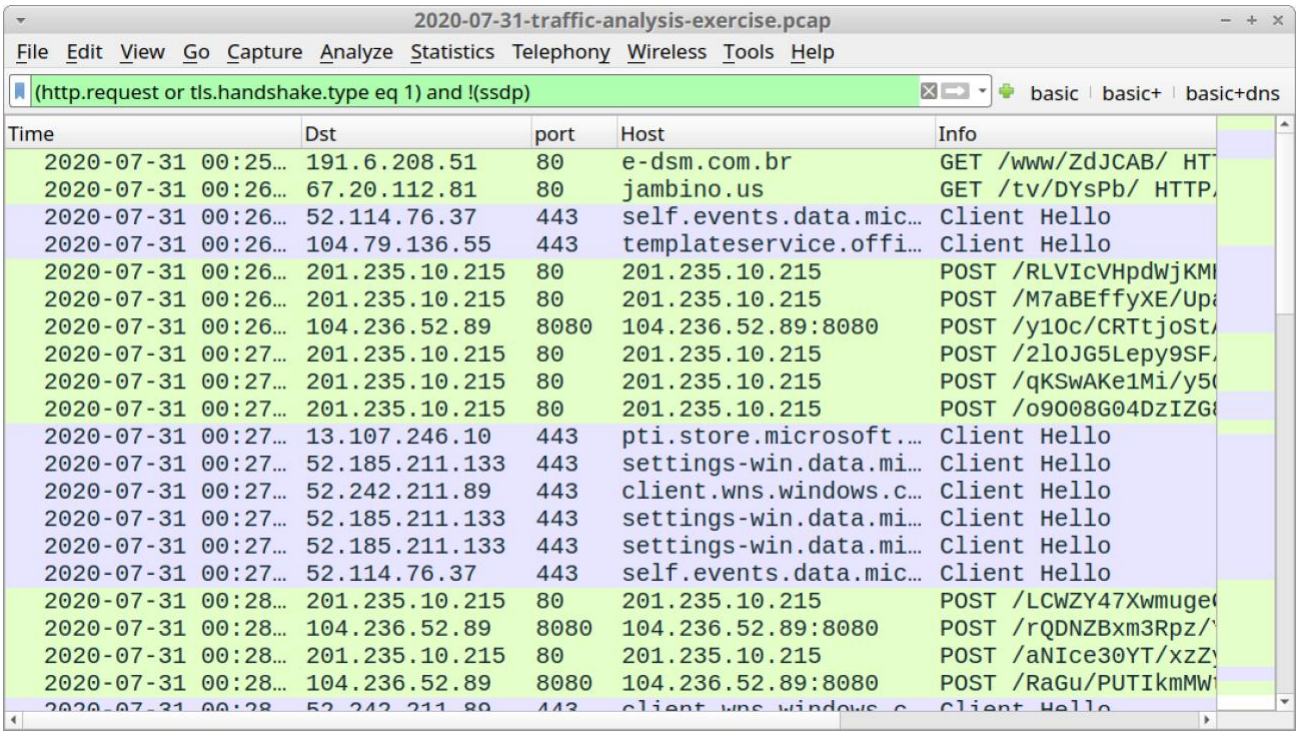
- 104.236.52.89 port 8080 - 104.236.52.89:8080 - POST /RaGu/PUTIkmMWtxHtctq/du2EPQGClXV/
- 201.235.10.215 port 80 - 201.235.10.215 - POST /4DsE/
- 201.235.10.215 port 80 - 201.235.10.215 - POST /NemVGY4zT/f6eDx8v6CbHNUXS/gjuMfPtC/j2SXoNwzJzR/
- 201.235.10.215 port 80 - 201.235.10.215 - POST /yguqyvZp1YxK083S/H5kIaZFW692xUc/HLuonj6146/
- 104.236.52.89 port 8080 - 104.236.52.89:8080 - GET /whoami.php
- 104.236.52.89 port 8080 - 104.236.52.89:8080 - POST /xian/balloon/
- 201.235.10.215 port 80 - 201.235.10.215 - POST /VmjfI/jygtnUpXR/kxLUe7h097jcjEAJPIM/u8O5/jHD8f/NiJ7CP0jmzegr/
- 201.235.10.215 port 80 - 201.235.10.215 - POST /FlpErlAFJoc1f77w3J/
- 201.235.10.215 port 80 - 201.235.10.215 - POST /RoEy0QXUh0/

INVESTIGATION:

The alerts for internal IP address 10.7.31.101 reveal the following:

- Windows EXE or DLL downloaded from 67.20.112.81 over TCP port 80
- Emotet CnC (Command & Control) traffic over 104.236.52.89 over TCP port 8080 and 201.235.10.215 over TCP port 80

Based on these alerts we're looking at an Emotet infection. We can confirm HTTP traffic on these IP addresses by reviewing the pcap.



Shown above: Basic web filter on the pcap shows HTTP traffic from all the IP addresses in the alerts.

Keep in mind that most normal web traffic is HTTPS. In regular Windows traffic, we can also find HTTP traffic from various Microsoft domains and ***windowsupdate.com***. However, HTTP POST requests to IP addresses are very suspicious. So already this is looking unusual.

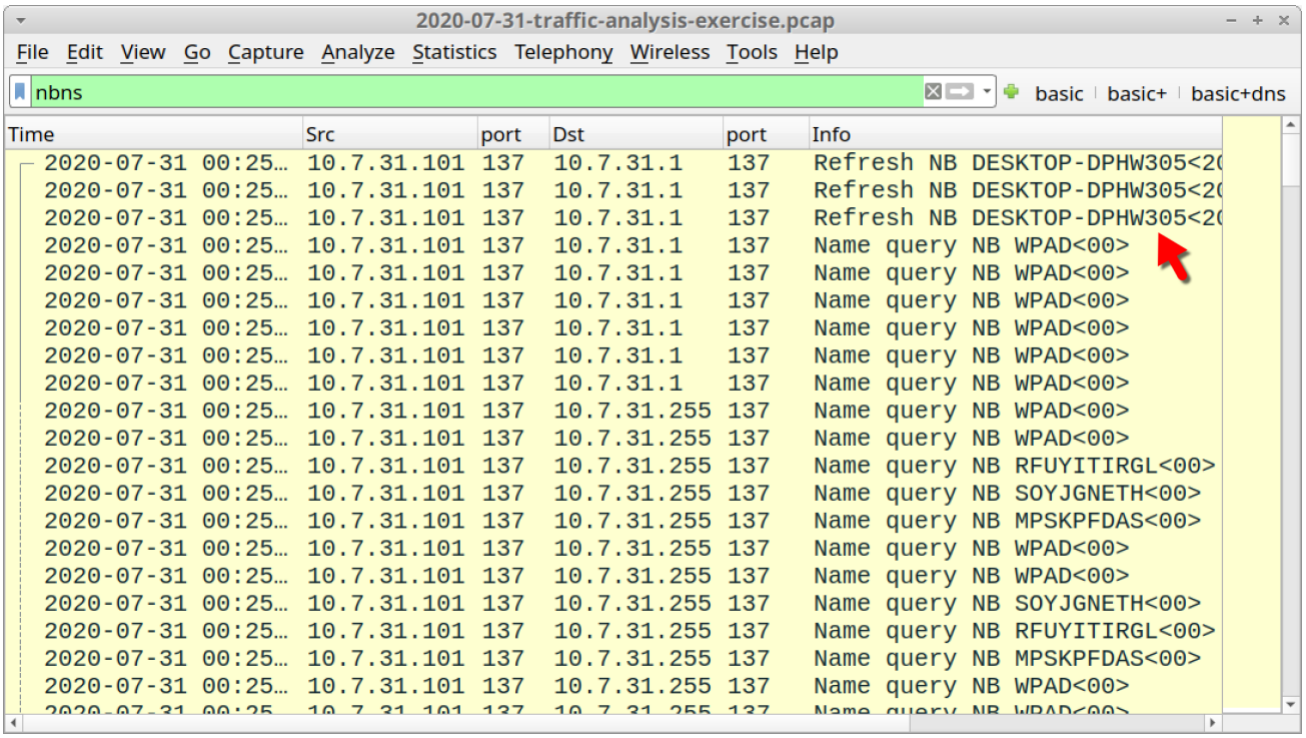
Before we investigate the infection traffic, let's get the victim details. Filter on ***nbns*** and review traffic for the hostname. In this case, you should see lines for

Refresh NB DESKTOP-DPHW305<20>

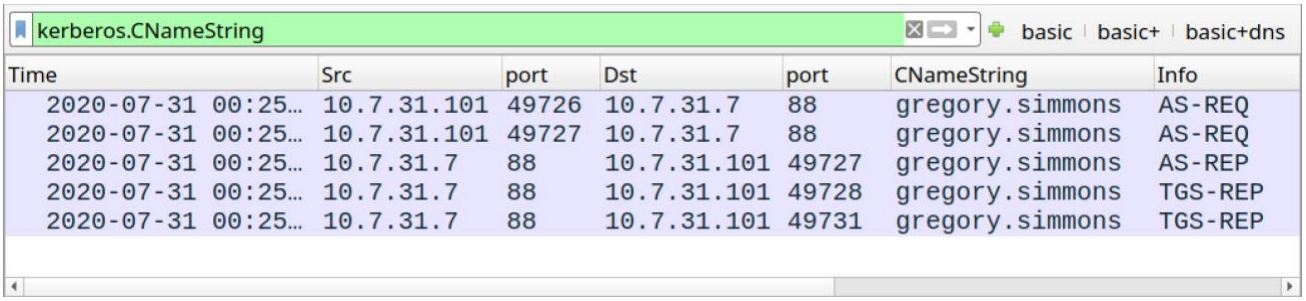
as early as 00:25 UTC.

You can easily find the Windows account name for the user by filtering on ***Kerberos.CNameString***. Of course, this assumes you've set up Wireshark according to the tutorials listed at the beginning of this document.

2020-07-31 - TRAFFIC ANALYSIS EXERCISE ANSWERS

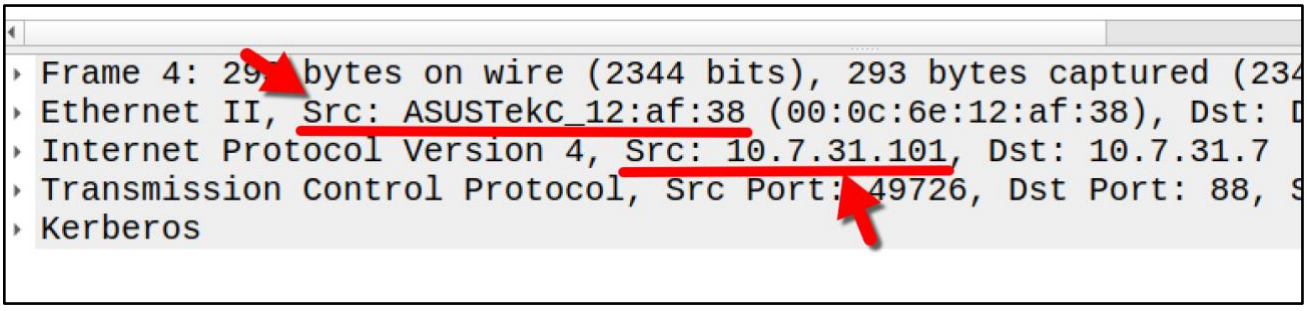


*Shown above: Filtering on **nbns** to find the Windows host name.*



*Shown above: Filter on **Kerberos.CNameString** for the user account name.*

The IP address ***10.7.31.101*** is common to all the alerts, and it's the only Windows client in this pcap. You can correlate the MAC address with the IP address in the frame details window as shown below.

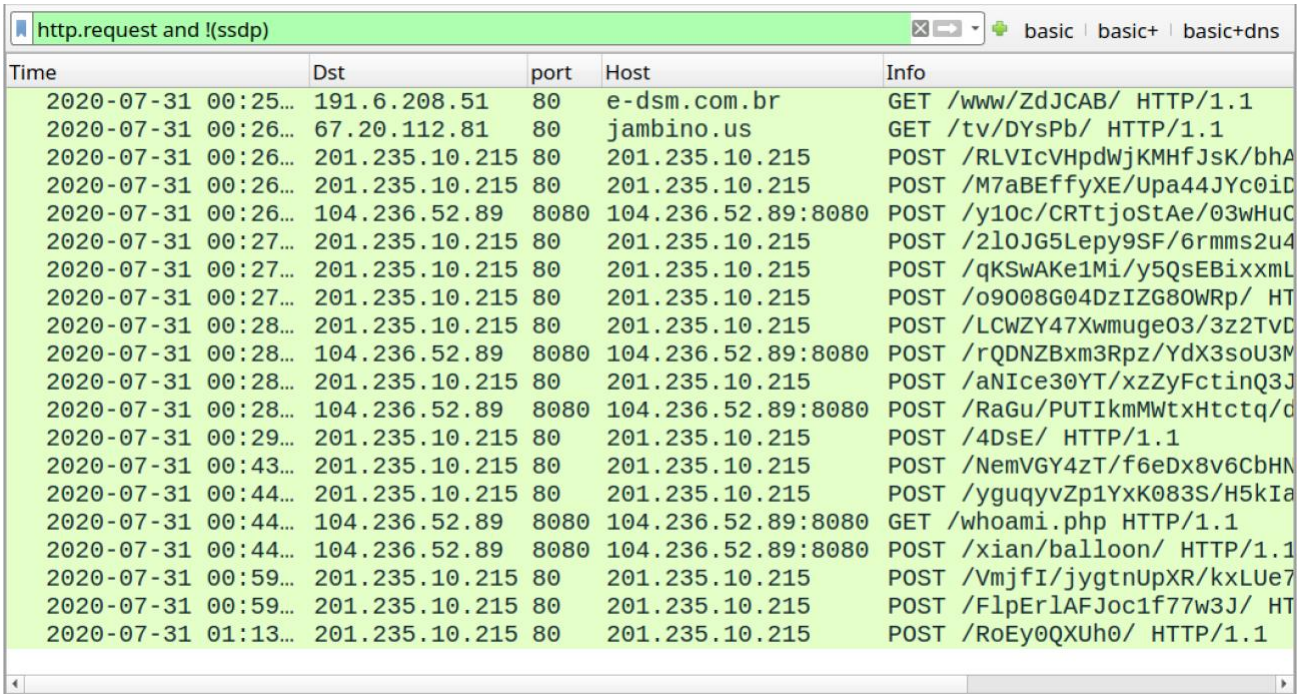


Shown above: Finding the MAC address of 10.7.31.101.

2020-07-31 - TRAFFIC ANALYSIS EXERCISE ANSWERS

Now that we have the victim details, let's get back to the infection traffic. Use the following filter to quickly review the unencrypted HTTP traffic:

http.request and !(ssdp)



Time	Dst	port	Host	Info
2020-07-31 00:25…	191.6.208.51	80	e-dsm.com.br	GET /www/ZdJCAB/ HTTP/1.1
2020-07-31 00:26…	67.20.112.81	80	jambino.us	GET /tv/DYsPb/ HTTP/1.1
2020-07-31 00:26…	201.235.10.215	80	201.235.10.215	POST /RLVIcVHpdWjKMHfJsK/bhA
2020-07-31 00:26…	201.235.10.215	80	201.235.10.215	POST /M7aBEffyXE/Upa44JYc0iD
2020-07-31 00:26…	104.236.52.89	8080	104.236.52.89:8080	POST /y1Oc/CRTtjoStAe/03wHuC
2020-07-31 00:27…	201.235.10.215	80	201.235.10.215	POST /2lOJG5Lepy9SF/6rmms2u4
2020-07-31 00:27…	201.235.10.215	80	201.235.10.215	POST /qKSwAKe1Mi/y5QsEBixxmL
2020-07-31 00:27…	201.235.10.215	80	201.235.10.215	POST /o9O08G04DzIZG8OWRp/ HT
2020-07-31 00:28…	201.235.10.215	80	201.235.10.215	POST /LCWZY47XwmugeO3/3z2TvD
2020-07-31 00:28…	104.236.52.89	8080	104.236.52.89:8080	POST /rQDNZBxm3Rpz/YdX3soU3M
2020-07-31 00:28…	201.235.10.215	80	201.235.10.215	POST /aNIce30YT/xzZyFctinQ3J
2020-07-31 00:28…	104.236.52.89	8080	104.236.52.89:8080	POST /RaGu/PUTIkmMWtxHtctq/d
2020-07-31 00:29…	201.235.10.215	80	201.235.10.215	POST /4DsE/ HTTP/1.1
2020-07-31 00:43…	201.235.10.215	80	201.235.10.215	POST /NemVGY4zT/f6eDx8v6CbHN
2020-07-31 00:44…	201.235.10.215	80	201.235.10.215	POST /yguqyvZp1YxK083S/H5kIa
2020-07-31 00:44…	104.236.52.89	8080	104.236.52.89:8080	GET /whoami.php HTTP/1.1
2020-07-31 00:44…	104.236.52.89	8080	104.236.52.89:8080	POST /xian/balloon/ HTTP/1.1
2020-07-31 00:59…	201.235.10.215	80	201.235.10.215	POST /VmjfI/jygtnUpXR/kxLUe7
2020-07-31 00:59…	201.235.10.215	80	201.235.10.215	POST /FlpErlAFJoc1f77w3J/ HT
2020-07-31 01:13…	201.235.10.215	80	201.235.10.215	POST /RoEy0QXUh0/ HTTP/1.1

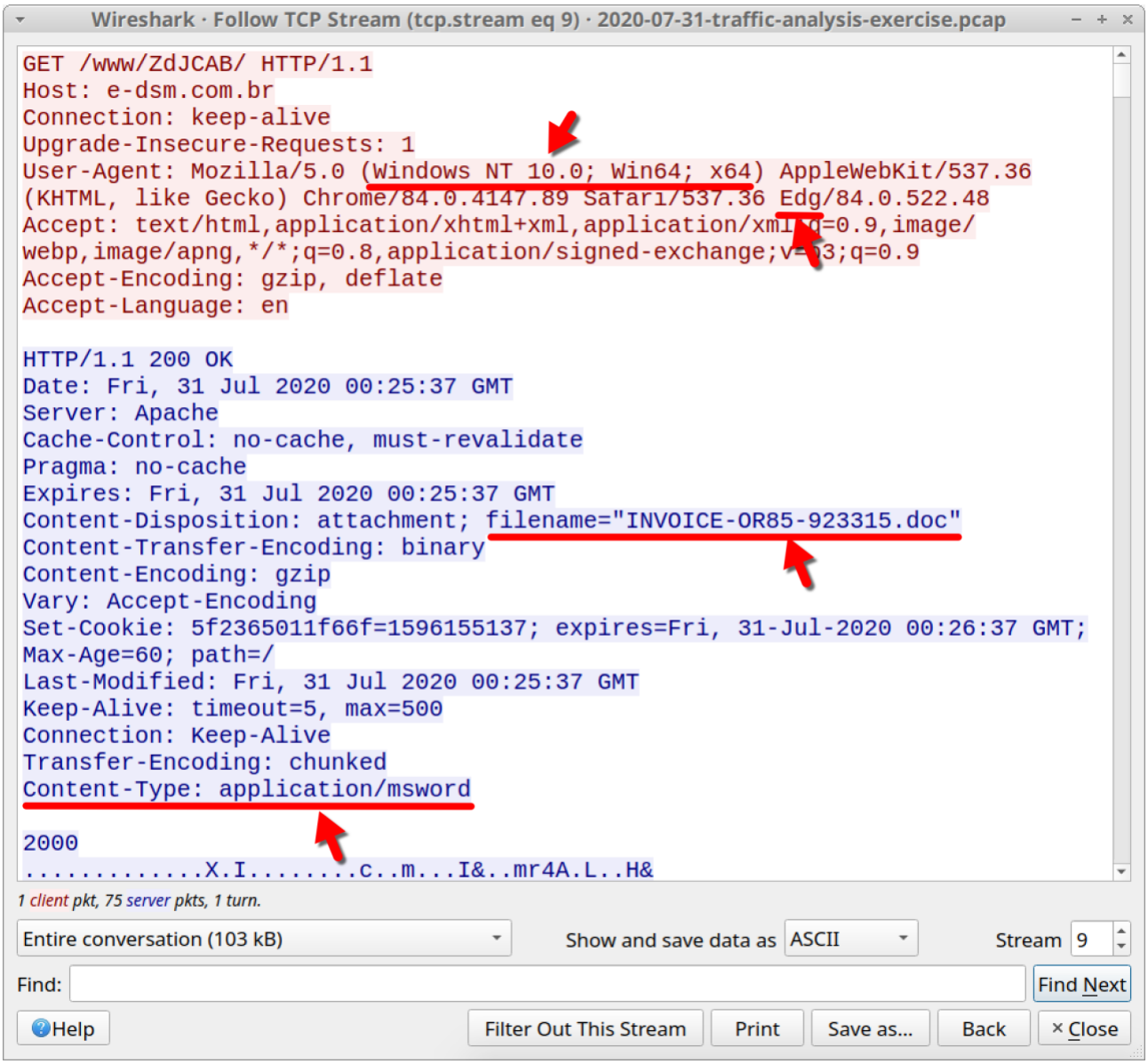
Shown above: Filtering on HTTP web traffic in this pcap.

Notice how the first HTTP GET request to ***e-dsm.com.br*** is not in the alerts. Follow the TCP stream for that request to find out more.

In the TCP stream, look at the User-Agent string in the HTTP request headers. Assuming the User-Agent hasn't been spoofed by some sort of malware, the operating system is Windows 10 64-bit, and this request was caused by the new Chromium-based Microsoft Edge browser (note "Edg" in the User-Agent sting).

You'll also see indications the file returned from the server is an "msword" file with a file name "INVOICE-OR85-923315.doc."

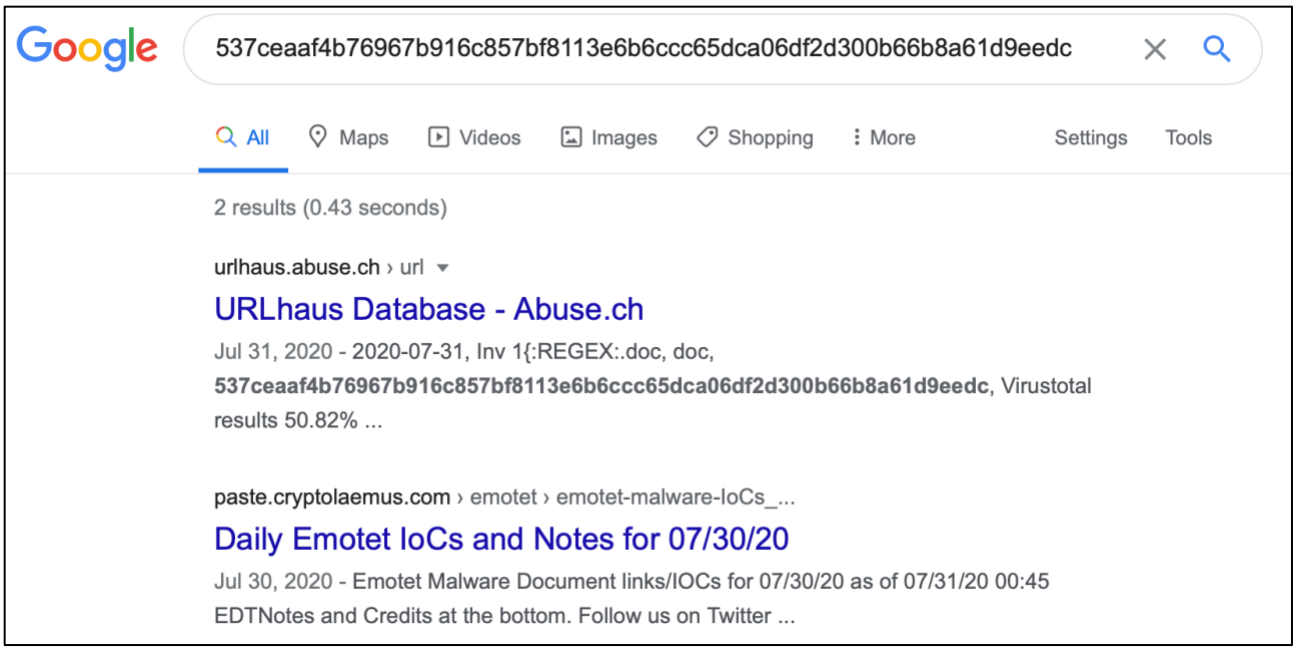
2020-07-31 - TRAFFIC ANALYSIS EXERCISE ANSWERS



Shown above: TCP stream indicating a Word doc returned for the initial HTTP GET request in our pcap.

Use the ***File --> Export Objects --> HTTP*** menu path to export this file from the pcap. When saving it, name the file ***INVOICE-OR85-923315.doc*** as shown in the HTTP request headers.

In a Linux, BSD, or mac environment, use ***shasum -a 256*** to get the SHA256 hash of this file and search the hash in Google. Your results should indicate this file is associated with Emotet.



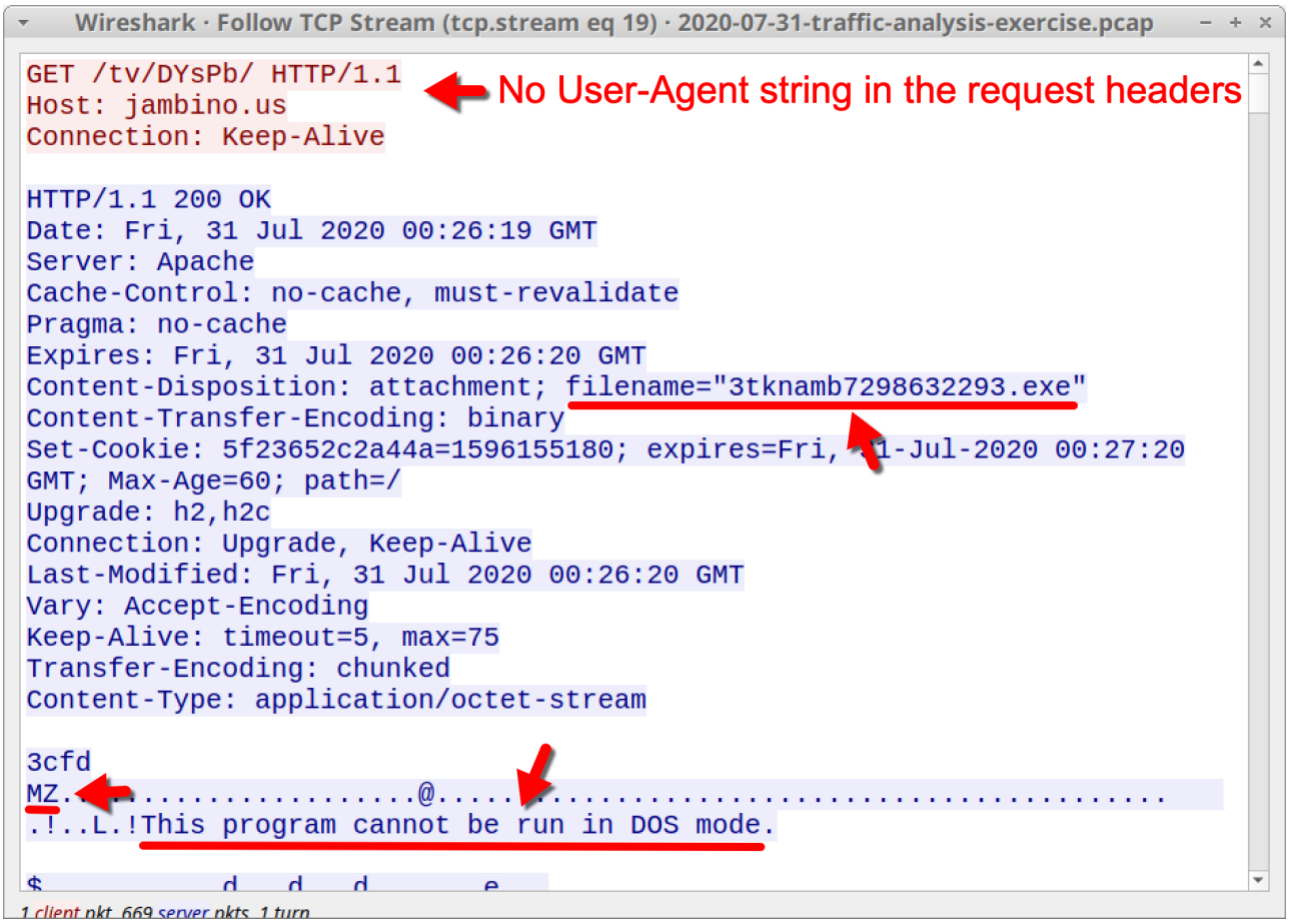
Shown above: Google search results for the Word doc file hash.

Do the ***file*** command in a Linux, BSD, or mac environment to confirm this file is a Word document. You can also search for the hash in VirusTotal to confirm this is a Word document.

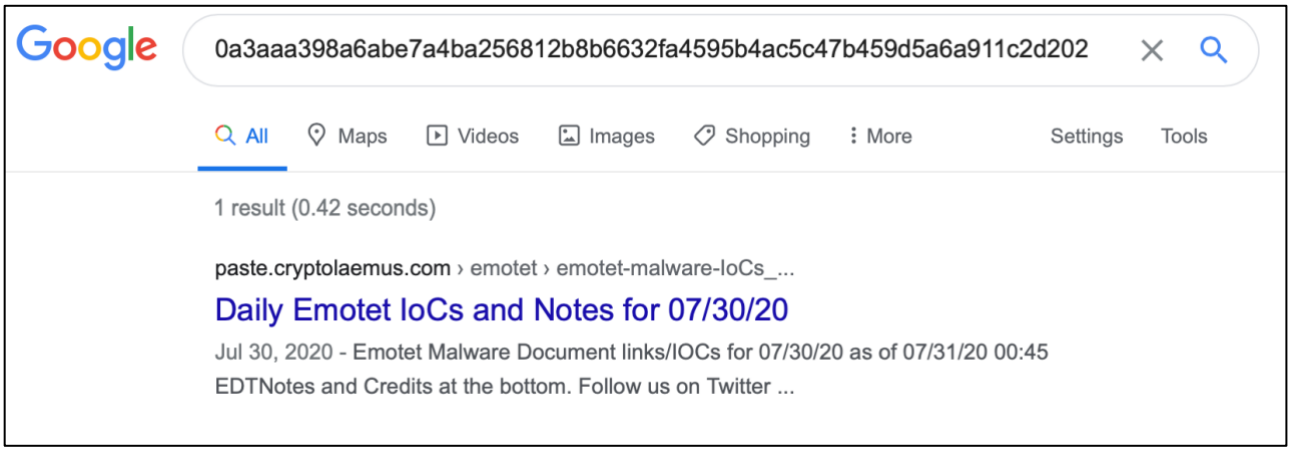
Filter on HTTP web traffic again, follow TCP stream for the second HTTP GET request, and you'll see indicators of a Windows EXE or DLL. Export that file from the pcap, get the SHA256 hash, and you'll find it's also associated with Emotet.

Do the ***file*** command in a Linux, BSD, or mac environment to confirm this file is an EXE. You can also search for the hash in VirusTotal to confirm this is an EXE.

2020-07-31 - TRAFFIC ANALYSIS EXERCISE ANSWERS



Shown above: An EXE or DLL returned from the second HTTP GET request in the pcap.

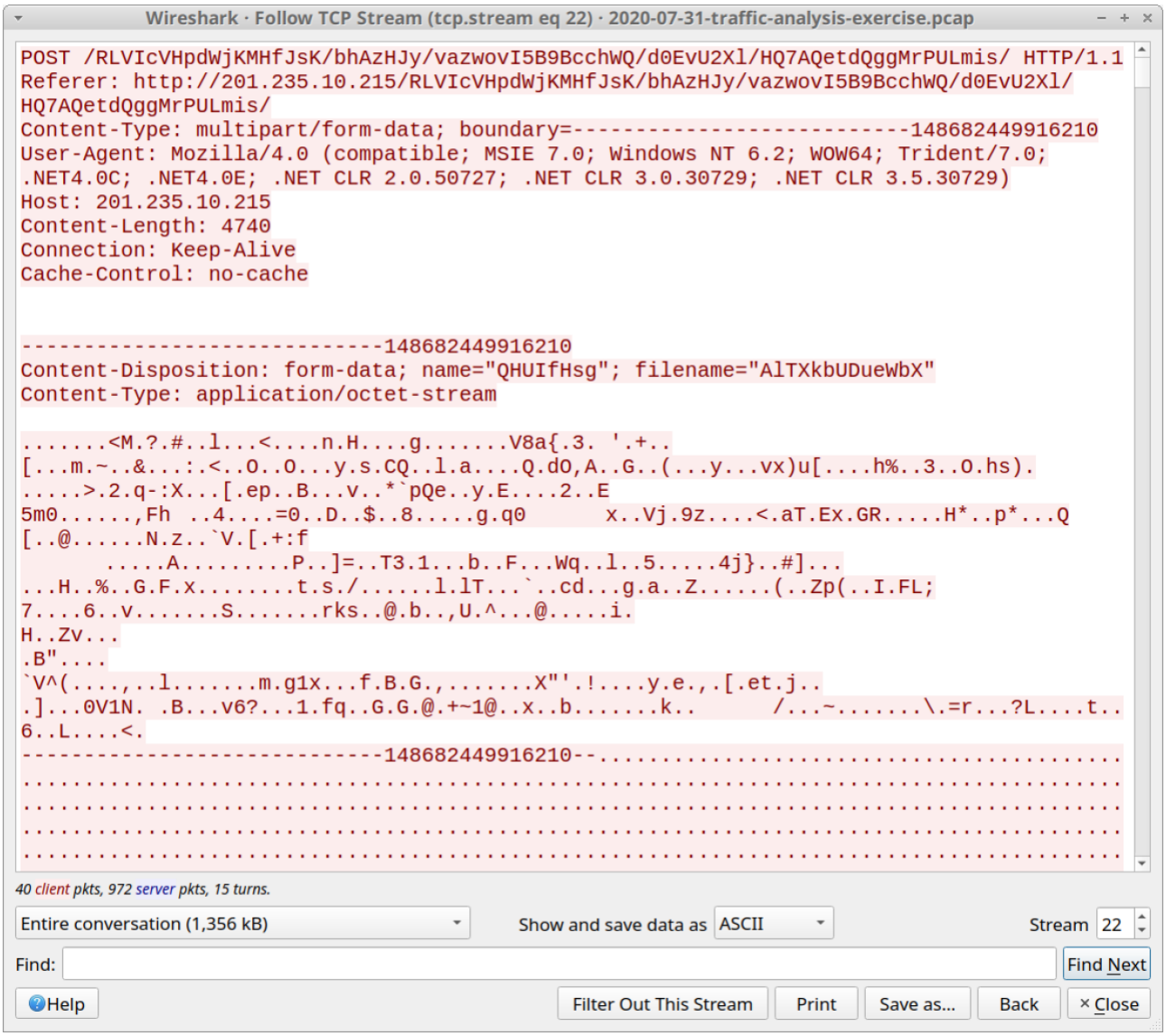


Shown above: Google search results for the EXE file hash.

2020-07-31 - TRAFFIC ANALYSIS EXERCISE ANSWERS

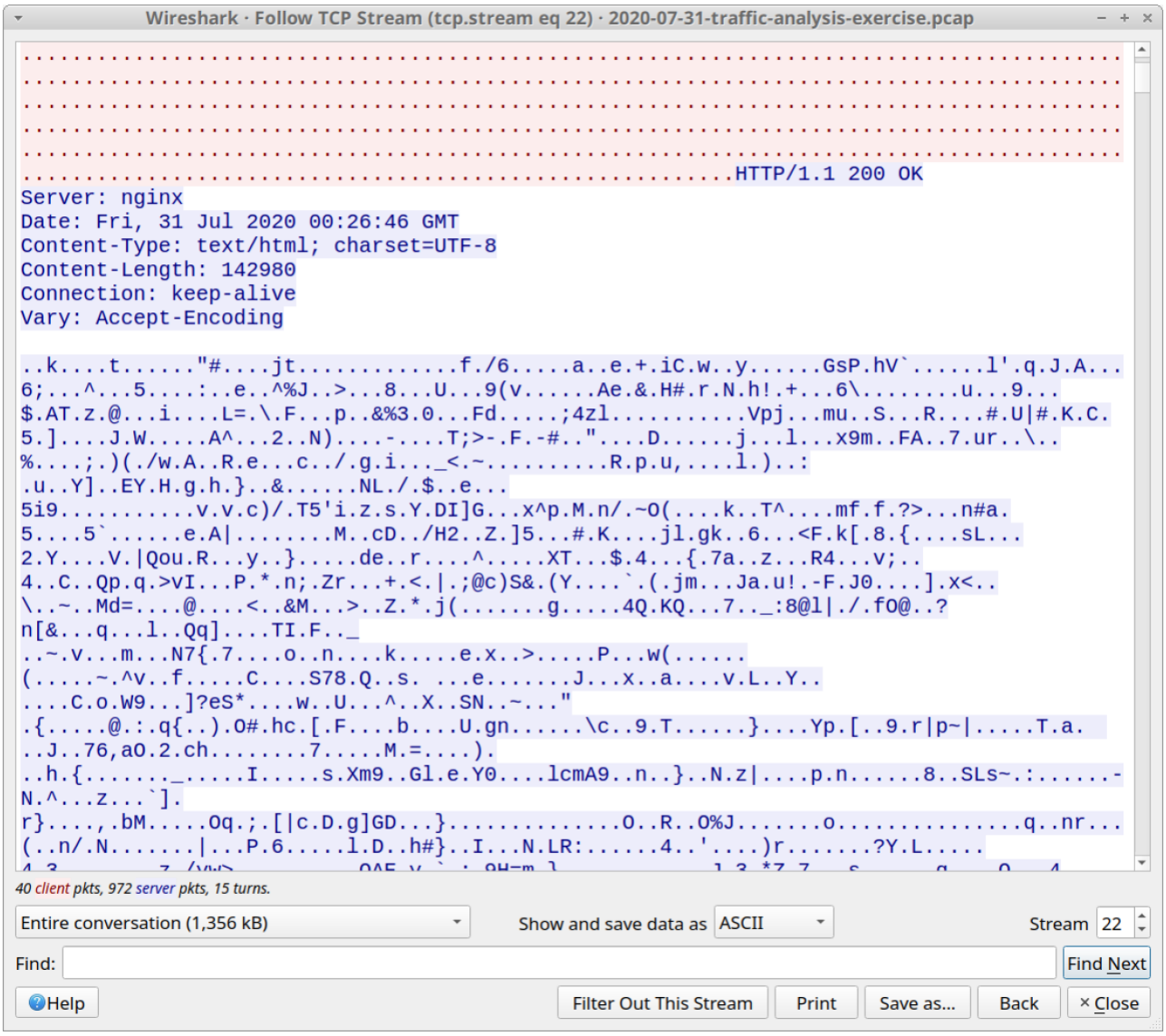
If you're curious about what Emotet CnC traffic looks like, follow one of the TCP streams for an HTTP POST request to 201.235.10.215 or 104.236.52.89:8080.

You should find form-data in the POST headers that looks like it's compress or encoded. Any data returned from the server is also encoded or encrypted.



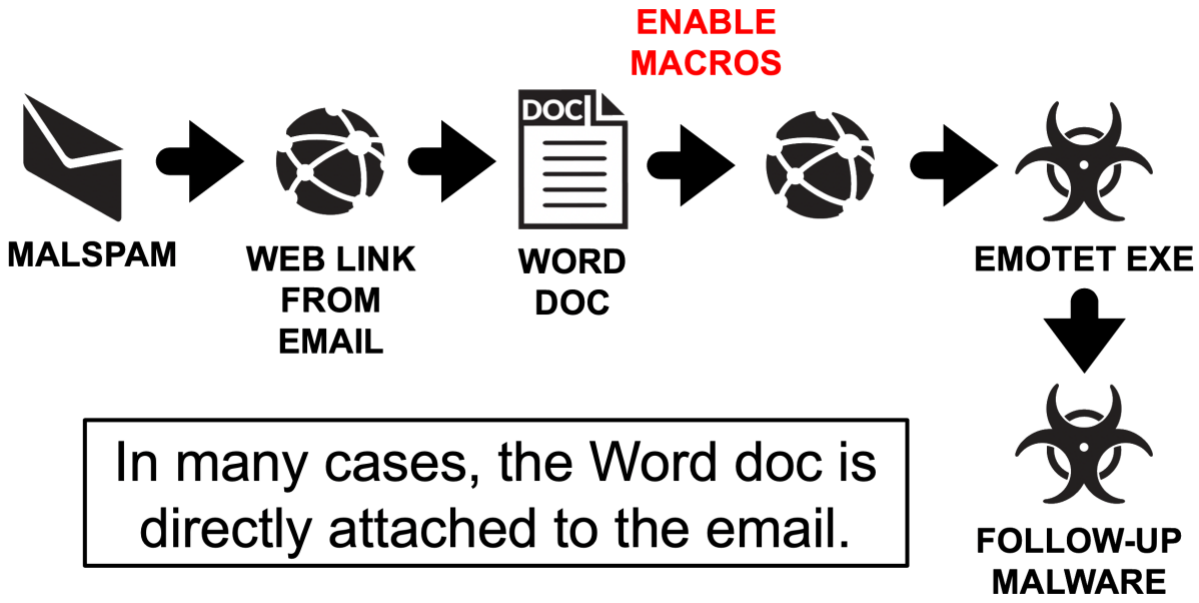
Shown above: HTTP POST request from the Emotet CnC traffic.

2020-07-31 - TRAFFIC ANALYSIS EXERCISE ANSWERS



Shown above: Encoded or encrypted data returned in response to the HTTP POST request.

This encoded data is how CnC (Command and Control, or "C2") data is returned from the Emotet servers. It's also how Emotet sends follow-up malware like Qakbot or Trickbot.



Shown above: Flow chart for most of my lab-based Emotet infections.