2018-10-31 TRAFFIC ANALYSIS EXERCISE - ANSWERS

https://www.malware-traffic-analysis.net/2018/10/31/index.html

Your task: Review the pcap and draft an incident report. Your report should contain:

- Date and time of the activity (in GMT or UTC)
- The account name or username from the infected Windows computer
- The host name of the infected Windows computer
- The MAC address of the infected Windows computer
- SHA256 file hashes for any malware from the pcap
- What type of infection this is

ANSWERS:

NOTE: I've rephrased the tasks as questions and tried to clarify what you should be looking for.

Q: What time in UTC does the malicious traffic start?
A: At approximately 15:34 UTC

Q: What is the Windows account name from the infected Windows computer?
A: ichabod.crane

Q:What is the host name of the infected Windows computer?
A: HEADLESS-PC

Q: What is the MAC address of the infected Windows computer?
A: 00:50:8b:2a:96:0a (HewlettP_2a:96:0a)

Q:What is the SHA256 file hash for the one malware (a Windows executable) you can extract from the pcap?
A:396223eeec49493a52dd9d8ba5348a332bf064483a358db79d8bb8d22e6eb62c

Q: What type of infection is this?
A: Trickbot

DETAILS:

As always before doing these exercises, I recommend you customize your column display in Wireshark. I've written a guide here:

- https://researchcenter.paloaltonetworks.com/2018/08/unit42-customizing-wireshark-changing-column-display/

Q: What time in UTC does the malicious traffic start?
A: At approximately 15:34 UTC

2018-10-31 TRAFFIC ANALYSIS EXERCISE - ANSWERS

Details: The first frame of the pcap starts at 2018-10-31 at 15:33:05 UTC, but this is not the date and time when the malicious activity starts. First, the machine connects to the network and the user logs in through an Active Directory (AD) Domain Controller (DC).

In recent exercises, I've provided information on the domain and LAN segment for the exercise in advance, but this time I did not. Here is the information for this active directory environment:

- LAN segment: **10.100.9.0/24** (10.100.9.0 through 10.100.9.255)
- Domain: **halloweenjob.com**
- Domain Controller: **10.100.9.4** - **HALLOWEENJOB-DC**
- Gateway: **10.100.9.1**
- Broadcast address: **10.100.9.255**
- Windows client: **10.100.9.107**

If you're just starting out, you might ask "how am I supposed to know all of this?" That's a good point. But to effectively analyze malicious network traffic, you **must** understand network fundamentals. If you investigate suspicious traffic from a corporate or workplace network, it will most likely involve an AD environment. You should also understand client/server relationships in network traffic.

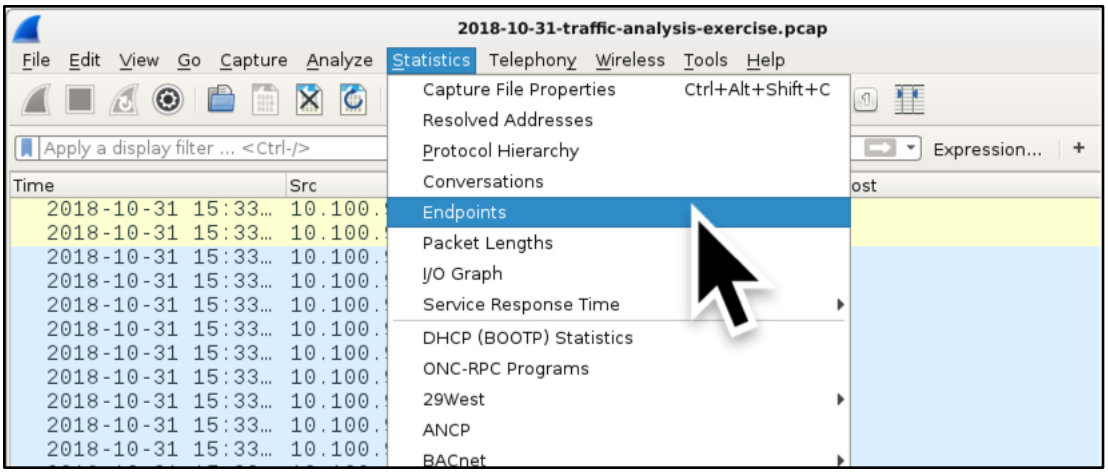
Let's tackle the first issue. How do you know what the private IP address space is for the internal network in this pcap?

First, you should know private, non-routable IP address space. There are 3 ranges: Class A, class B, and class C.

Class A private IP address space is 10.0.0.0/8 (10.0.0.0 through 10.255.255.255). Class B private IP address space is 172.16.0.0/12 (172.16.0.0 through 172.31.255.255). And class C private IP address space is 192.168.0.0/16 (192.168.0.0 through 192.168.255.255).

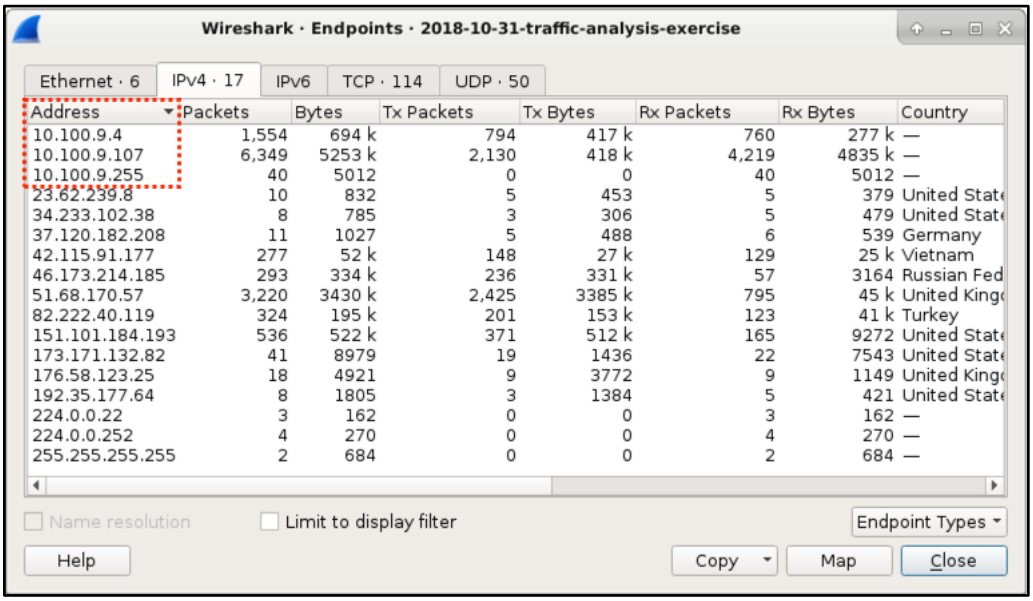
Once you understand the ranges of private (internal) IP address space, check the endpoint statistics of the pcap in Wireshark. Use the menu path: Statistics → Endpoints

2018-10-31 TRAFFIC ANALYSIS EXERCISE - ANSWERS



Shown above: Getting to the endpoint statistics in Wireshark.

When reviewing the statistics, go to the IPv4 tab. Sort on the Address column, if it's not already sorted by that column. In this case, the only private IP addresses we see are 10.100.9.4, 10.100.9.107, and 10.100.9.255.



Shown above: Wireshark's endpoints window for this pcap.

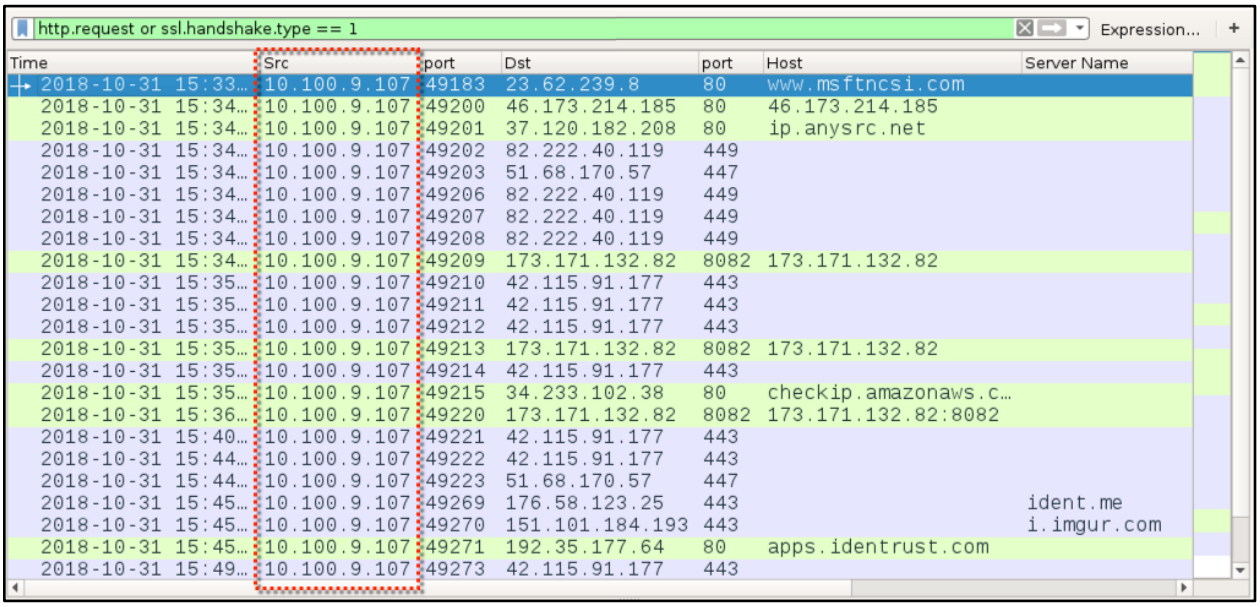
The LAN segments for these exercise pcaps range from .0 to .255 for the last octet (designated as /24 using CIDR notation). This means the private IP address ending with .255 is the broadcast address for the internal network's LAN segment. With 10.100.9.255 as the broadcast address for that LAN segment, we only have two other IP addresses in the private IP address space: 10.100.0.4 and 10.100.9.107.

One is the DC and one is the Windows client. But which is which?

In a work environment, analysts investigate alerts on suspicious activity. These alerts show the internal IP address and external IP address of the suspicious traffic. If these

analysts have access to full packet capture of network traffic, they retrieve the suspicious network traffic based on that internal IP address. In most cases, that internal IP address is the Windows client. And the traffic should contain various external IP addresses, because you want to review traffic before and after the specific alert you're investigating.

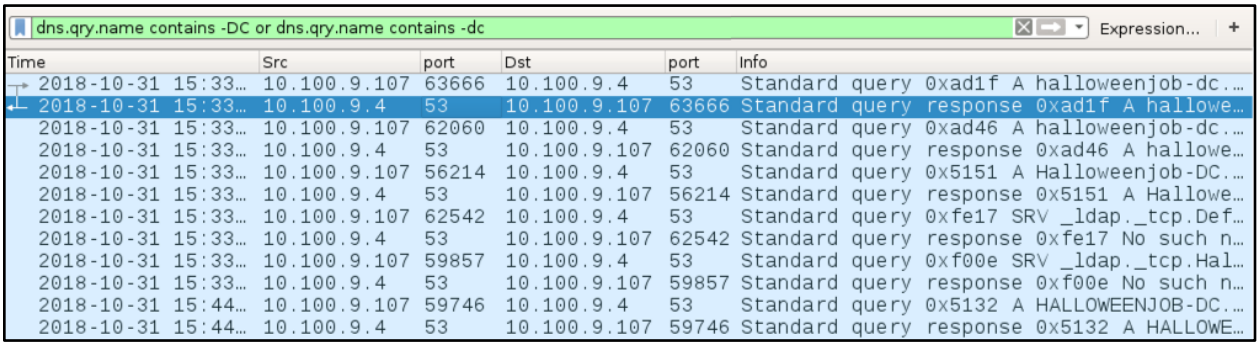
So, if we look at the pcap, we should see traffic from a single internal IP address to various external IP addresses. Using Wireshark, filter on ***http.request or ssl.handshake.type == 1*** for web-based traffic, and you'll find the source IP address is 10.100.9.107. That's the Windows client.



Shown above: Filtering on web traffic in the exercise pcap.

Understanding we're working in an AD environment, by process of elimination, 10.100.9.4 should be the domain controller. In my exercises, the hostname of the domain controller always ends with -DC. So let's filter in Wireshark on DNS queries that end with -DC or with -dc (to cover case-sensitive names). Try this Wireshark query:

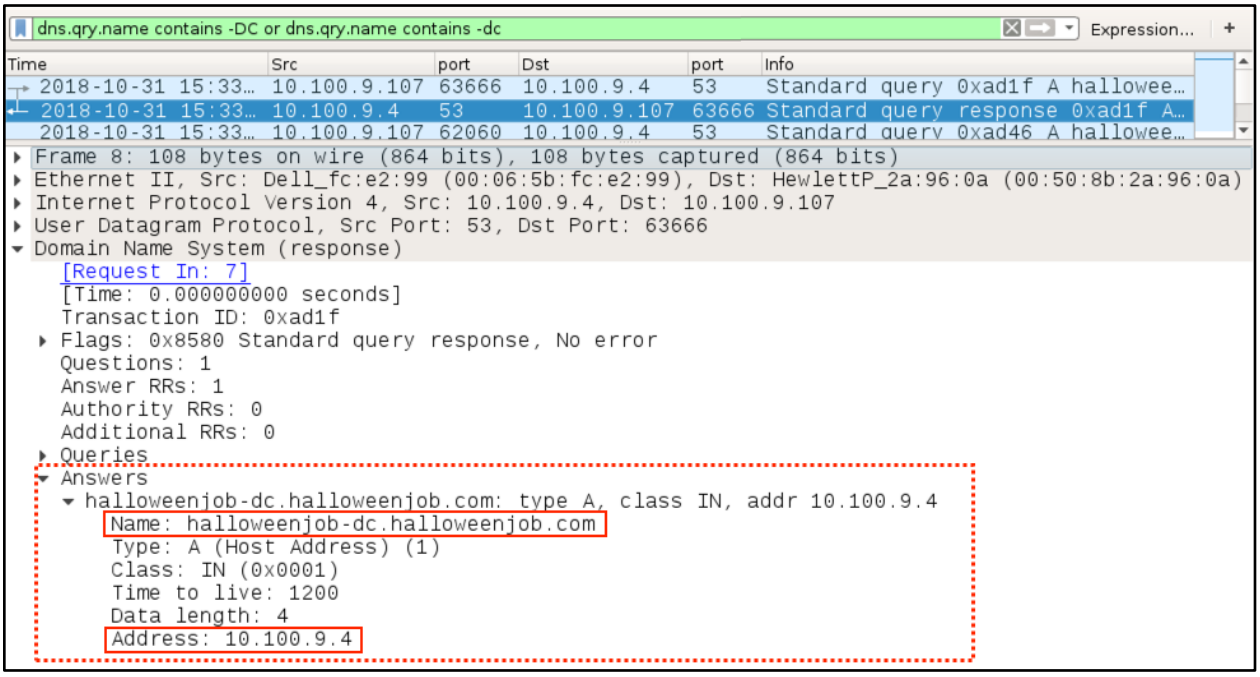
dns.qry.name contains -DC or dns.qry.name contains -dc



Shown above: Filtering in Wireshark to find the domain controller name.

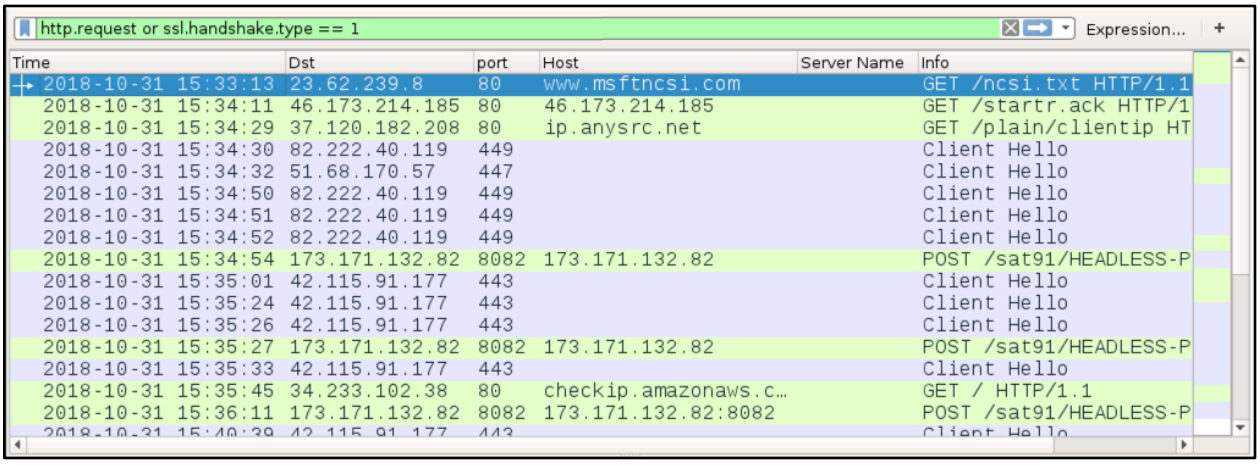
2018-10-31 TRAFFIC ANALYSIS EXERCISE - ANSWERS

Select the frame for the DNS response from the first query/response pair. Scroll down through the frame details and review the "answers" section. There, you'll find ***halloweenjob-dc.halloweenjob.com*** resolves to an IP address at ***10.100.9.4***.



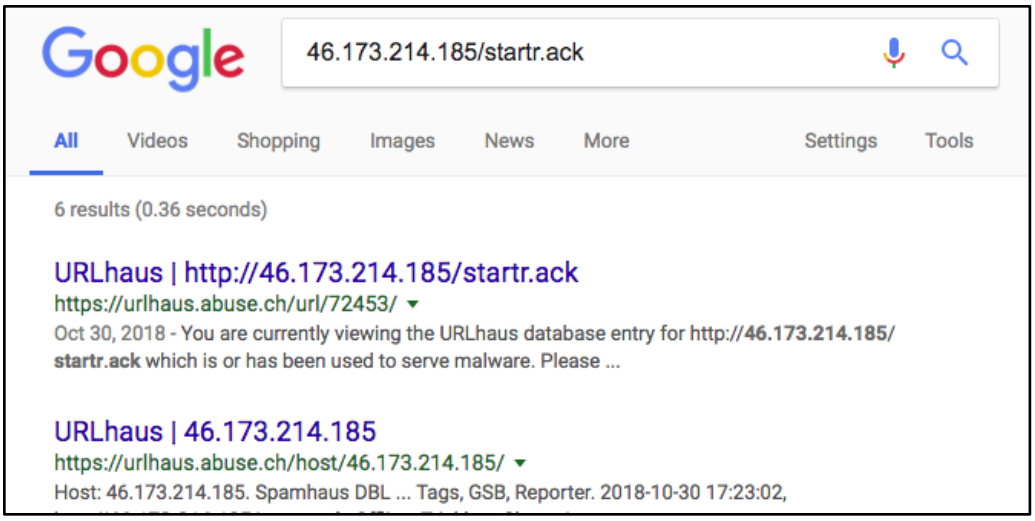
Shown above: DNS response showing the domain and domain controller name.

That just helps us understand the environment. It doesn't answer our original question: What time did the malicious traffic start? Go back to the Wireshark for web traffic: ***http.request or ssl.handshake.type == 1***

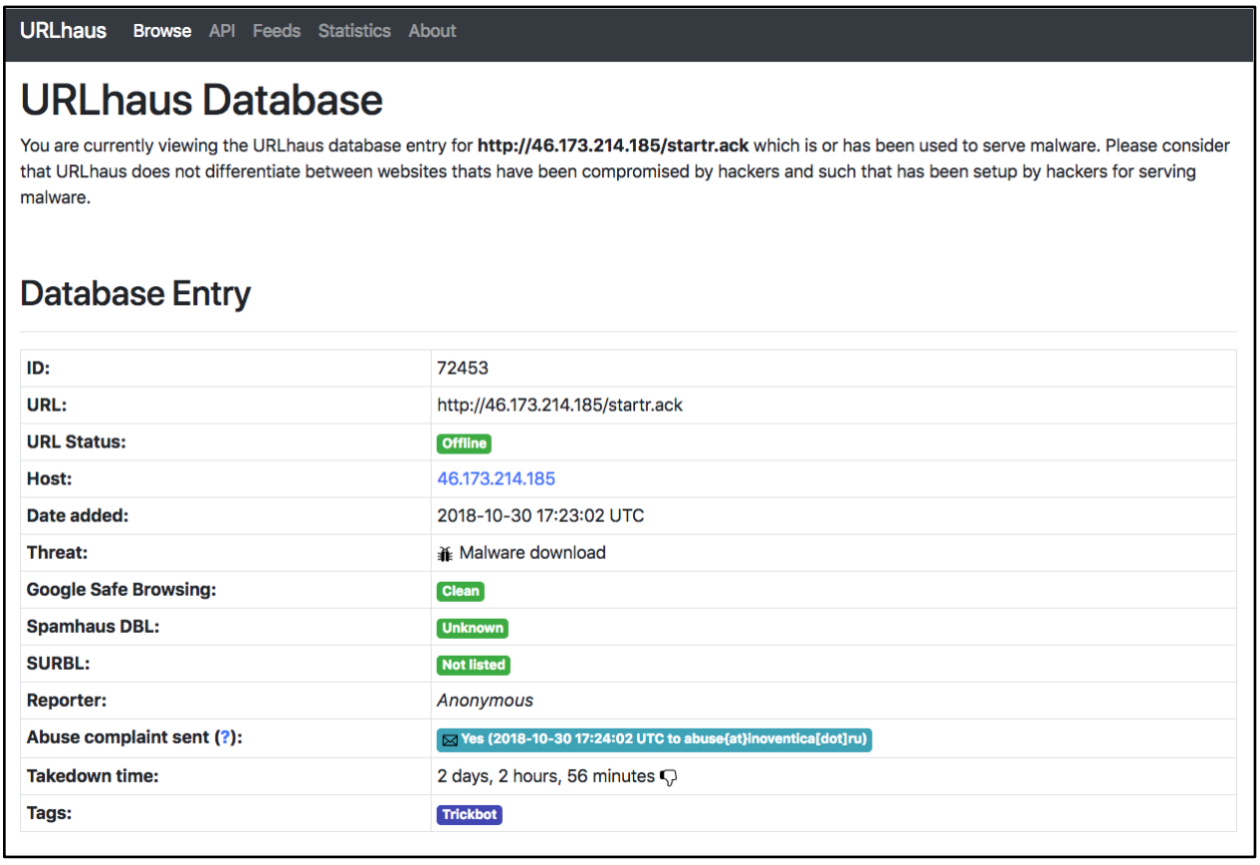


Shown above: Filtering on web traffic in the exercise pcap.

In the results, you'll see an HTTP GET request to ***www.msftncsi.com***, which is normal for Windows hosts connecting to a network. The next HTTP request on 2018-10-31 at 15:34:11 UTC is for ***46.173.214.185 - GET /startr.ack*** which is malicious. Searching for that URL on Google leads to an entry in URLhaus showing it returned Trickbot malware.



Shown above: Google search on the second URL from the pcap.



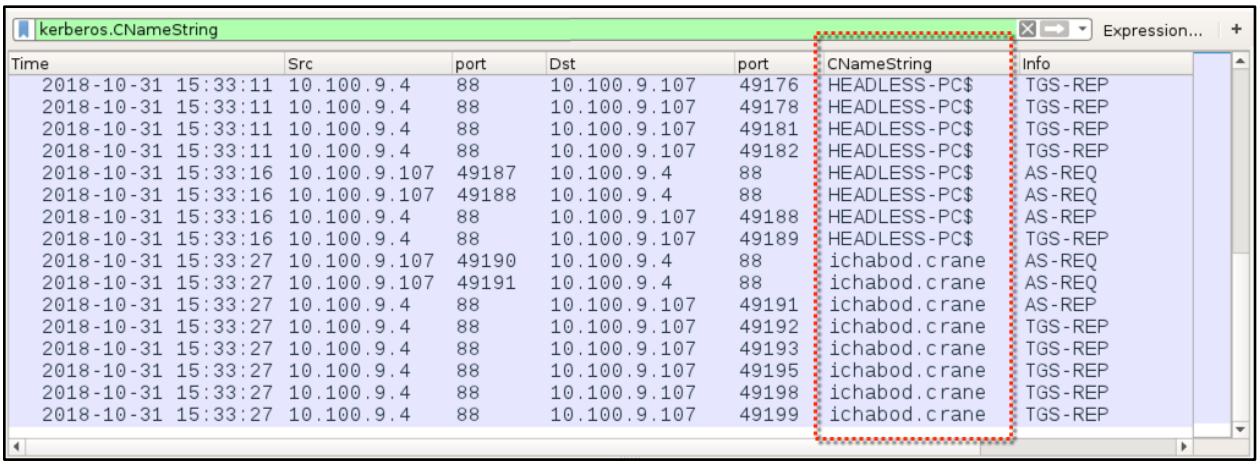
Shown above: URLhaus entry reveals that URL returned malware tagged as Trickbot.

That's a lot of details just to get the first answer, but it should help people developing their analyst skills better understand these pcaps. On to the next question…

2018-10-31 TRAFFIC ANALYSIS EXERCISE - ANSWERS

Q: What is the Windows account name from the infected Windows computer?
A: ichabod.crane

Details: If you've customized your Wireshark display as I suggested earlier, all you need to do is filter on kerberos.CNameString and show the customized CNameString column. Information in this column should include the host name of the Windows client (any name ending with a $) and the user account name ***ichabod.crane***.

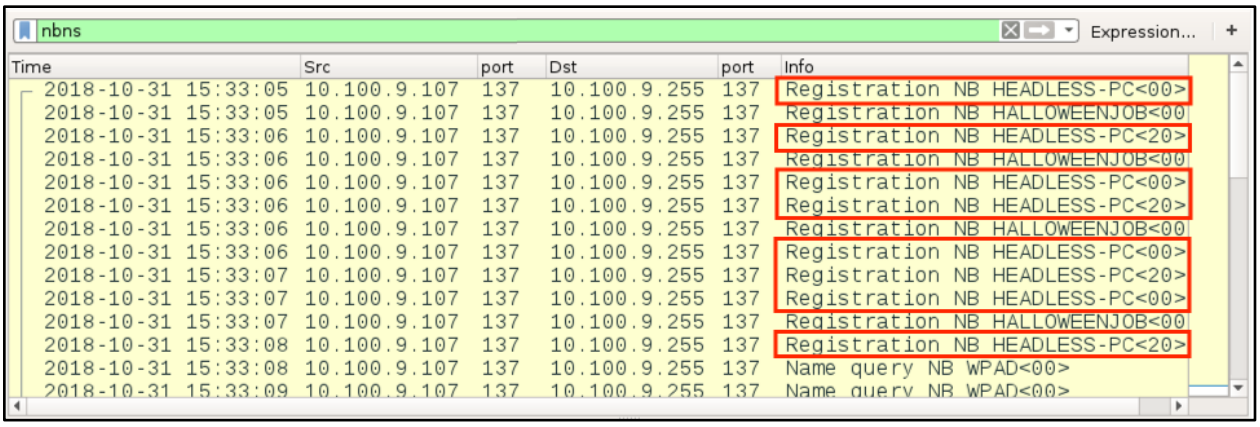


Time	Src	port	Dst	port	CNameString	Info
2018-10-31 15:33:11	10.100.9.4	88	10.100.9.107	49176	HEADLESS-PC$	TGS-REP
2018-10-31 15:33:11	10.100.9.4	88	10.100.9.107	49178	HEADLESS-PC$	TGS-REP
2018-10-31 15:33:11	10.100.9.4	88	10.100.9.107	49181	HEADLESS-PC$	TGS-REP
2018-10-31 15:33:11	10.100.9.4	88	10.100.9.107	49182	HEADLESS-PC$	TGS-REP
2018-10-31 15:33:16	10.100.9.107	49187	10.100.9.4	88	HEADLESS-PC$	AS-REQ
2018-10-31 15:33:16	10.100.9.107	49188	10.100.9.4	88	HEADLESS-PC$	AS-REQ
2018-10-31 15:33:16	10.100.9.4	88	10.100.9.107	49188	HEADLESS-PC$	AS-REP
2018-10-31 15:33:16	10.100.9.4	88	10.100.9.107	49189	HEADLESS-PC$	TGS-REP
2018-10-31 15:33:27	10.100.9.107	49190	10.100.9.4	88	ichabod.crane	AS-REQ
2018-10-31 15:33:27	10.100.9.107	49191	10.100.9.4	88	ichabod.crane	AS-REQ
2018-10-31 15:33:27	10.100.9.4	88	10.100.9.107	49191	ichabod.crane	AS-REP
2018-10-31 15:33:27	10.100.9.4	88	10.100.9.107	49192	ichabod.crane	TGS-REP
2018-10-31 15:33:27	10.100.9.4	88	10.100.9.107	49193	ichabod.crane	TGS-REP
2018-10-31 15:33:27	10.100.9.4	88	10.100.9.107	49195	ichabod.crane	TGS-REP
2018-10-31 15:33:27	10.100.9.4	88	10.100.9.107	49198	ichabod.crane	TGS-REP
2018-10-31 15:33:27	10.100.9.4	88	10.100.9.107	49199	ichabod.crane	TGS-REP

*Shown above: Filter on **Kerberos.CNameString** to find host and user account names.*

Q:What is the host name of the infected Windows computer?
A: HEADLESS-PC

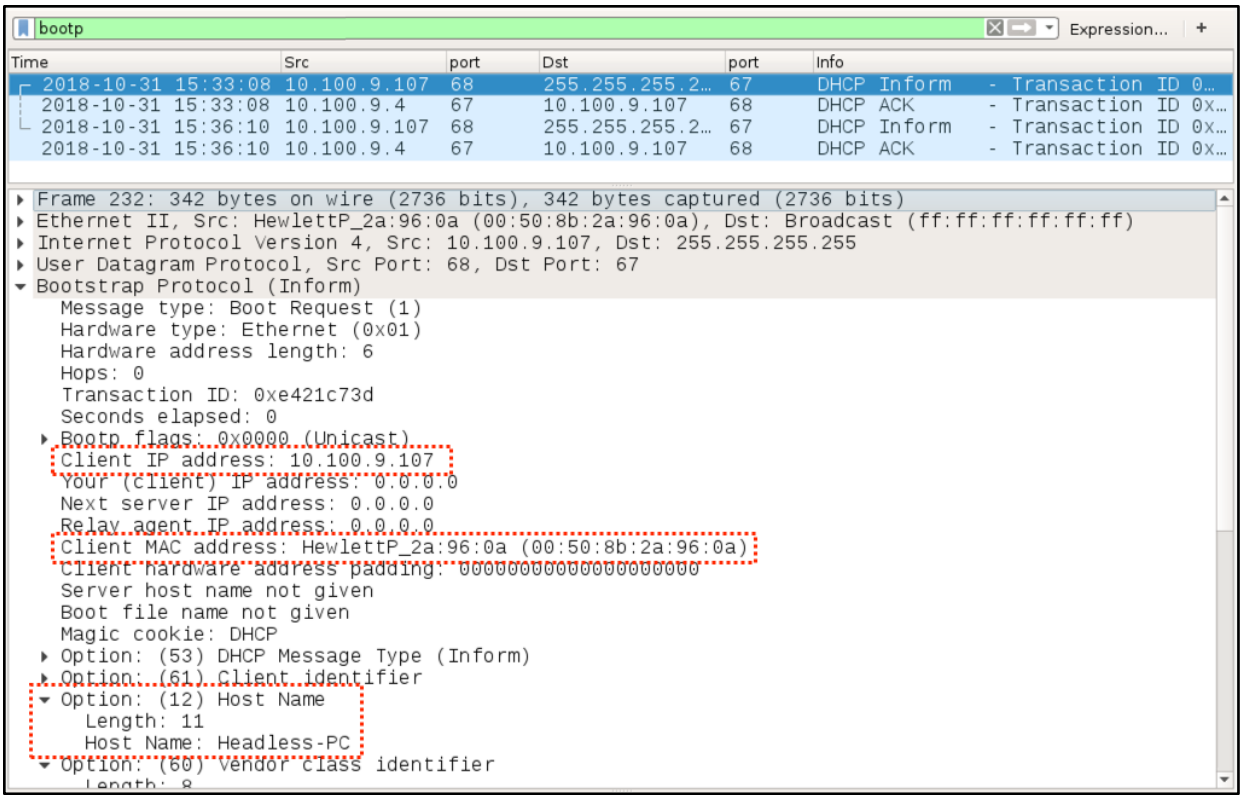
Details: This was found when searching on ***kerberos.CNameString***, but you can also find this info in DHCP traffic (filtering on ***bootp*** in Wireshark) or NetBIOS Name Service traffic (filtering on ***nbns*** in Wireshark).



Time	Src	port	Dst	port	Info
2018-10-31 15:33:05	10.100.9.107	137	10.100.9.255	137	Registration NB HEADLESS-PC<00>
2018-10-31 15:33:05	10.100.9.107	137	10.100.9.255	137	Registration NB HALLOWEENJOB<00
2018-10-31 15:33:06	10.100.9.107	137	10.100.9.255	137	Registration NB HEADLESS-PC<20>
2018-10-31 15:33:06	10.100.9.107	137	10.100.9.255	137	Registration NB HALLOWEENJOB<00
2018-10-31 15:33:06	10.100.9.107	137	10.100.9.255	137	Registration NB HEADLESS-PC<00>
2018-10-31 15:33:06	10.100.9.107	137	10.100.9.255	137	Registration NB HEADLESS-PC<20>
2018-10-31 15:33:06	10.100.9.107	137	10.100.9.255	137	Registration NB HALLOWEENJOB<00
2018-10-31 15:33:06	10.100.9.107	137	10.100.9.255	137	Registration NB HEADLESS-PC<00>
2018-10-31 15:33:07	10.100.9.107	137	10.100.9.255	137	Registration NB HEADLESS-PC<20>
2018-10-31 15:33:07	10.100.9.107	137	10.100.9.255	137	Registration NB HEADLESS-PC<00>
2018-10-31 15:33:07	10.100.9.107	137	10.100.9.255	137	Registration NB HALLOWEENJOB<00
2018-10-31 15:33:08	10.100.9.107	137	10.100.9.255	137	Registration NB HEADLESS-PC<20>
2018-10-31 15:33:08	10.100.9.107	137	10.100.9.255	137	Name query NB WPAD<00>
2018-10-31 15:33:09	10.100.9.107	137	10.100.9.255	137	Name query NB WPAD<00>

Shown above: Finding the host name in NBNS traffic.

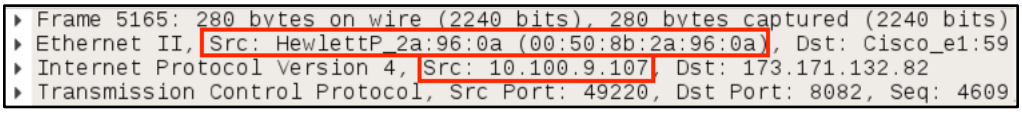
2018-10-31 TRAFFIC ANALYSIS EXERCISE - ANSWERS



Shown above: Finding the host name in DHCP traffic.

Q: What is the MAC address of the infected Windows computer?
A: 00:50:8b:2a:96:0a (HewlettP_2a:96:0a)

Details: You can easily correlate this with the IP address in the frame details window. Any frame that shows a source IP address of 10.100.9.107 should also show the associated source MAC address.

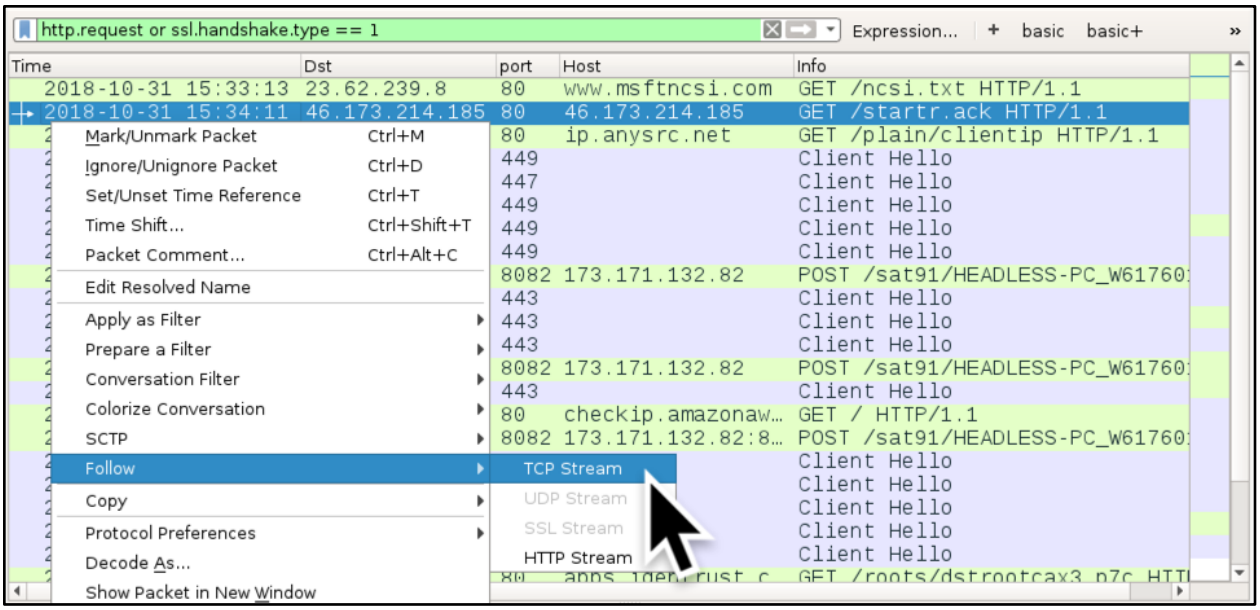


Shown above: Correlating 10.100.9.107 with its MAC address.

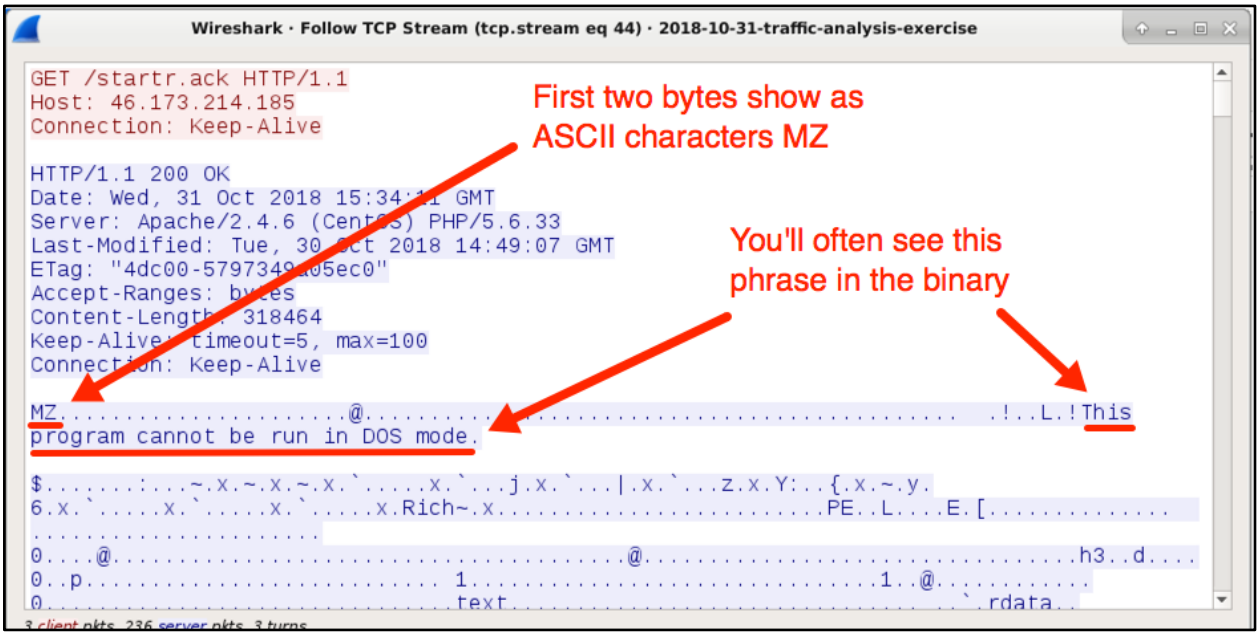
Q: What is the SHA256 file hash for the one malware (a Windows executable) you can extract from the pcap?
A: 396223eeec49493a52dd9d8ba5348a332bf064483a358db79d8bb8d22e6eb62c

Details: Reviewing the pcap, you'll find the HTTP request for ***46.173.214.185 - GET /startr.ack*** returned a Windows executable file. We already found this is Trickbot malware by reviewing the URLhaus entry for that URL, but let's review the pcap. Follow the TCP stream for that URL, and you'll find it returned a Windows executable.

2018-10-31 TRAFFIC ANALYSIS EXERCISE - ANSWERS



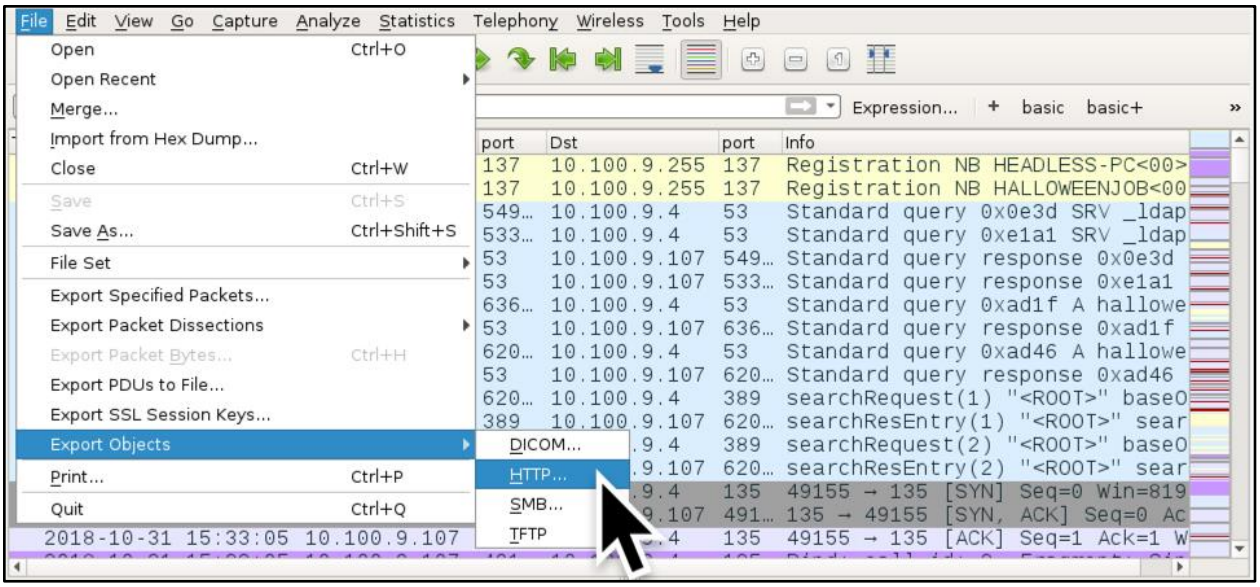
Shown above: Following the TCP stream for the HTTP GET request to 46.173.214.185.



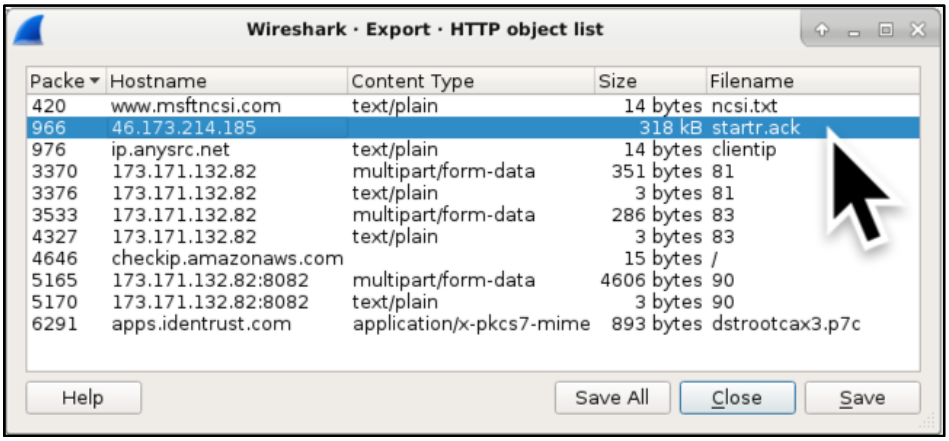
Shown above: The TCP stream for that HTTP GET request and response.

We can export this Windows executable file from the pcap. Use the following menu path:

File → Export Objects → HTTP...



Shown above: Exporting HTTP objects from the pcap.



Shown above: Selecting the startr.ack file from 46.173.214.185.

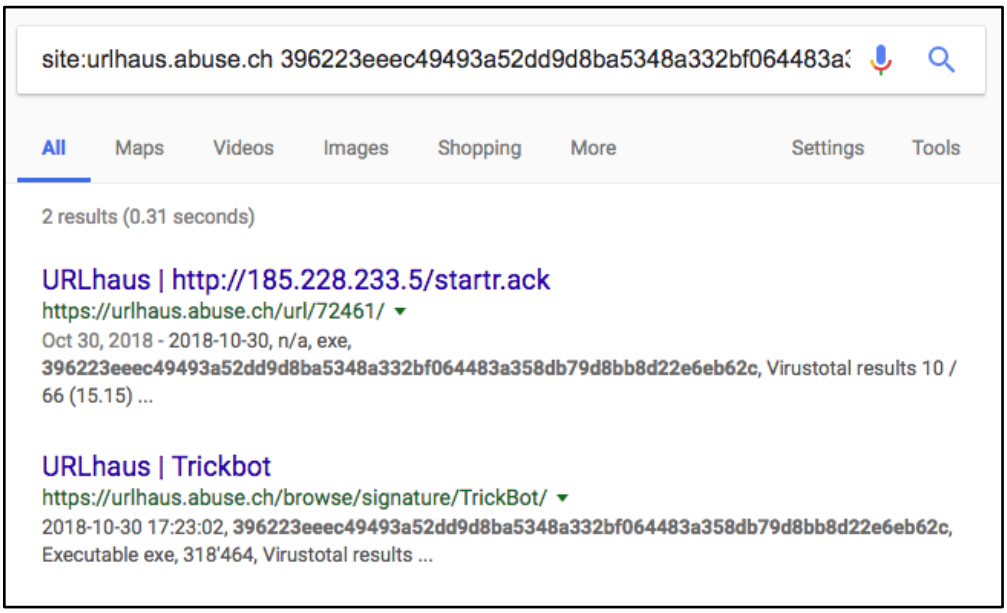
Once you export the file, in a Linux or macOS environment, you can check the file type and get the file hash.

$ file startr.ack
startr.ack: PE32 executable (GUI) Intel 80386, for MS Windows
$ shasum -a 256 startr.ack
396223eeec49493a52dd9d8ba5348a332bf064483a358db79d8bb8d22e6eb62c startr.ack

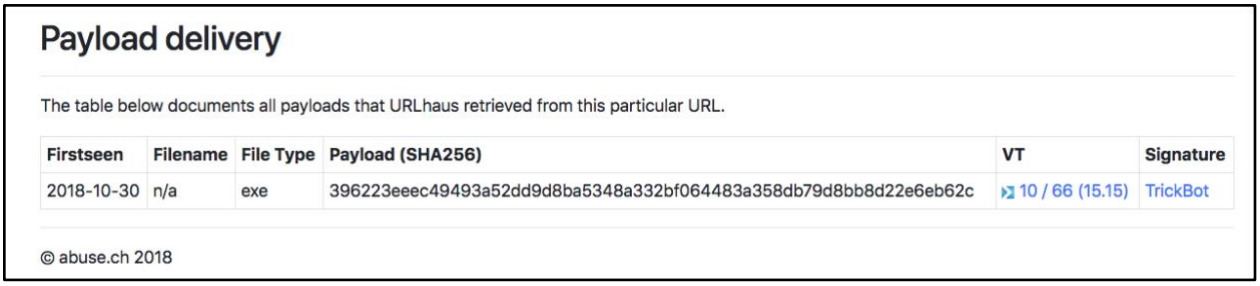
If you search for that file hash on Google, you'll find it is associated with various sandbox analysises from sites like ANY.RUN, hybrid-analysis.com, and joesandsbox.com.

Q: What type of infection is this?
A: Trickbot

Details: You might have already seen this during your Google search of the malware binary. Perhaps the quickest way to determine the malware type is the check URLhaus on the file hash. If URLhaus has it, you can easily check through the URLhaus website at ***urlhaus.abuse.ch***, or you can search on the file hash in Google and use ***site:urlhaus.abuse.ch*** as part of your search criteria.



Shown above: Using Google search to find a file hash on URLhaus.



Shown above: URLhaus showing the same file hash tagged as Trickbot.

Conclusion:

These details are primarily for the newer analysts trying to increase their skills, but some of this information might be of use to more experienced people.

As usual, there is more information about this infection from the pcap. I didn't review much of the post-infection traffic, but we've covered all the answers for this exercise.

Hope you had fun!