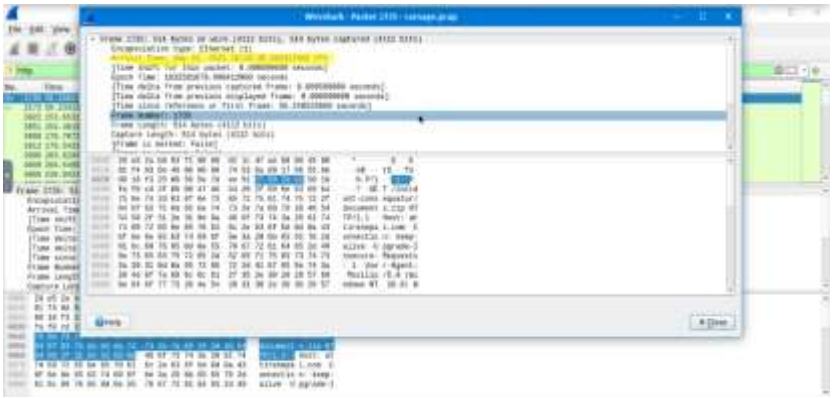
A walkthrough on the TryHackMe Carnage Room for pcap traffic analysis using Wireshark.

First, I opened the file on the Analysis Folder in the Virtual Machine using Wireshark attempted the questions as follows:

1.What was the date and time for the first HTTP connection to the malicious IP? (**answer format:** yyyy-mm-dd hh:mm:ss)

The packet info on the first packet revealed the required date and time of the first HTTP connection to the malicious IP. The time is indicated as Sep 24, 2021 16:44:38 but you can manually change it to fit the format specified in the question. Ans: **2021-09-24 16:44:38**

Note that you can also change the time format by selecting the "View" tab then navigating to "Time Display Format" and selecting the format you prefer.

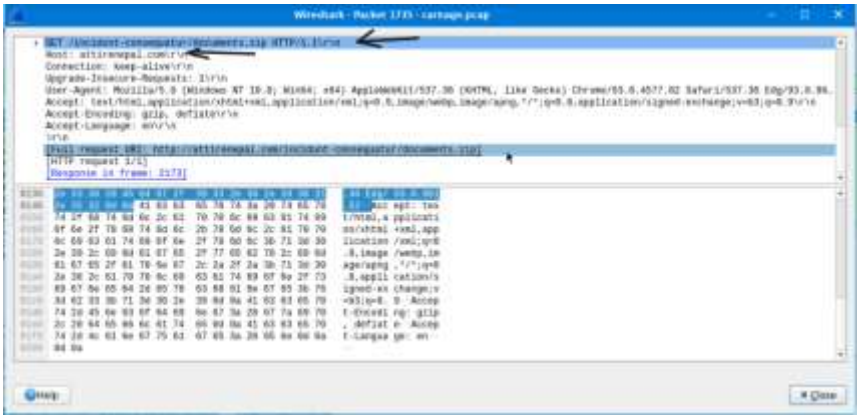


2. What is the name of the zip file that was downloaded?

On further investigation of the displayed information of the packet we see a GET request of the downloaded file as well as the domain hosting the malicious file. Ans: **documents.zip**

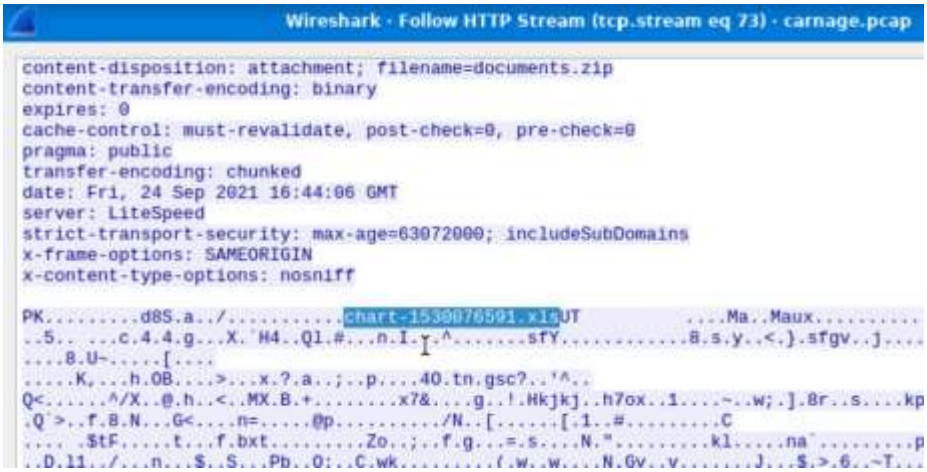
3. What was the domain hosting the malicious zip file?

The domain hosting the malicious file is also displayed on the same window. Ans: **attirenepal.com**



4. Without downloading the file, what is the name of the file in the zip file?

To get more information on the packet we have to follow the TCP Stream and that is accomplished by first right-clicking on the packet and selecting the “Follow” option then “TCP Stream”. A new window will be displayed showing the full stream conversation where we can also get the GET request of the file downloaded and the domain where the file is being hosted.
The name of the malicious file is displayed in the same stream as an .xls file (Microsoft Excel).
Ans: **chart-1530076591.xls**



5. What is the name of the webserver of the malicious IP from which the zip file was downloaded?

The webserver and version as also displayed on the same stream window. Ans: **LiteSpeed**

6. What is the version of the webserver from the previous question?

Ans: **PHP/7.2.34**

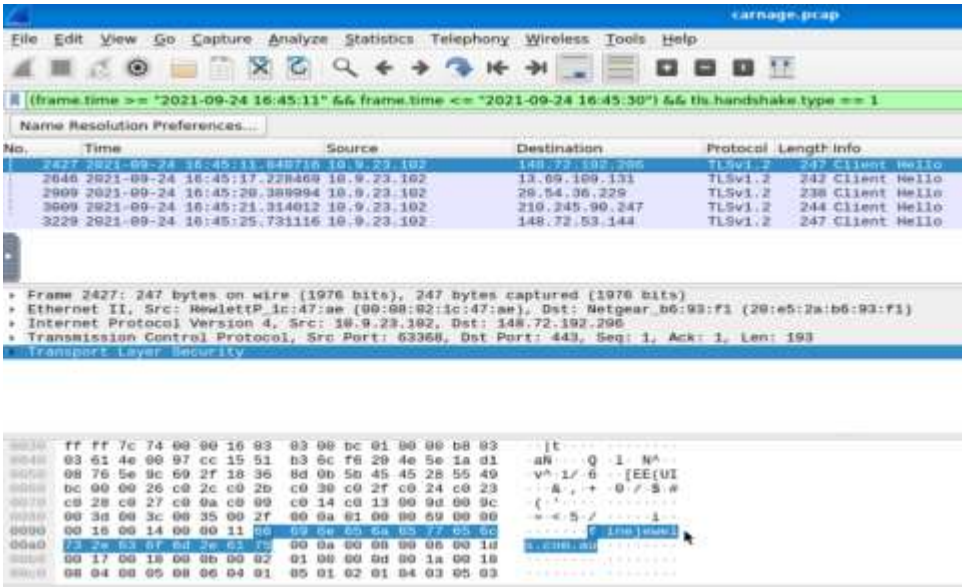
7. Malicious files were downloaded to the victim host from multiple domains. What were the three domains involved with this activity?

The hint specifies that we check HTTPS traffic and narrow down the timeframe from 16:45:11 to 16:45:30. To make the search easier for us we can use the following filter:

(frame.time >= "2021-09-24 16:45:11" && frame.time <= "2021-09-24 16:45:30") && tls.handshake.type == 1

The filter is broken down as follows:
- First we use ***frame.time*** to specify a specific time in the pcap as specified by THM. The operators >= and <= specify that we are interested in the time in between.
- ***tls.handshake.type == 1*** is used to specify the beginning of a tls handshake where the client sends a "hello" to the server. Note that HTTPS uses TLS/SSL encryption.

Applying the filter will bring up 5 packets displayed and by examining each you will be able to come up with 3 domain names from the. A search through Virus Total will help you pick out the malicious ones.
Ans: **finejewels.com.au, thietbiagt.com, new.americold.com**

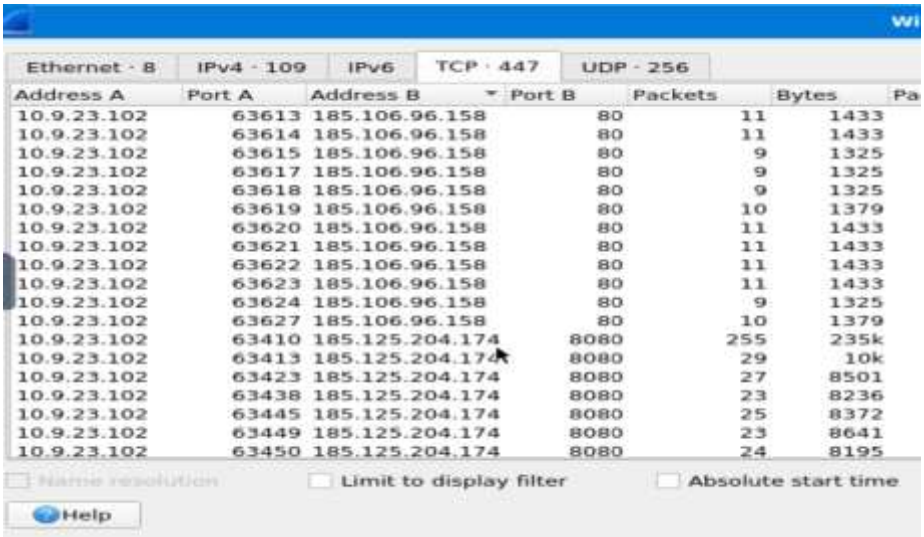


8. Which certificate authority issued the SSL certificate to the first domain from the previous question?

We have already identified the first domain to be "**finejewels.com.au**" which we got from the first packet of our previous filter. To view the certificate, we will follow the TCP stream conversation. From the resulting window we will find the Certificate Authority as it has been highlighted in several instances.
Ans: **GoDaddy**

9. What are the two IP addresses of the Cobalt Strike servers? Use VirusTotal (the Community tab) to confirm if IPs are identified as Cobalt Strike C2 servers. (answer format: enter the IP addresses in sequential order)

THM have hinted that we check the Conversations menu for the IP addresses. For that we select the "Statistics" tab on the file and choose the "Conversations" menu which will show us the IPs that are constant communicating and with the help of Virus Total we can figure out the malicious IPs. Ans: **185.106.96.158, 185.125.204.174**



10. What is the Host header for the first Cobalt Strike IP address from the previous question?

This information can be obtained by a quick search of the domain in Virus Total. Ans: **ocsp.verisign.com**

11. What is the domain name of the first Cobalt Strike server IP? You may use VirusTotal to confirm if it's the Cobalt Strike server (check the Community tab).

This information can be obtained by a quick search of the IP in Virus Total. Ans: **survmeter.live**

drb_ra
2 years ago

Cobalt Strike Server Found
C2: HTTPS @ 185[.]106[.]96[.]158:8888
C2 Server: survmeter[.]live,/gscp[.]R/,185[.]106[.]96[.]158,/gscp[.]R/
POST URI: /supprq/sa/
Country: United States
ASN: DediPath
Host Header: ocsp[.]verisign[.]com

#c2 #cobaltstrike

Note: The domain name and Host Header are defanged and can be resolved into to their original state using CyberChef.

12. What is the domain name of the second Cobalt Strike server IP? You may use VirusTotal to confirm if it's the Cobalt Strike server (check the Community tab).

As was with the first IP address, information on the second can be obtained from Virus Total and the domain name resolved with CyberChef. Ans: **securitybusinpuff.com**

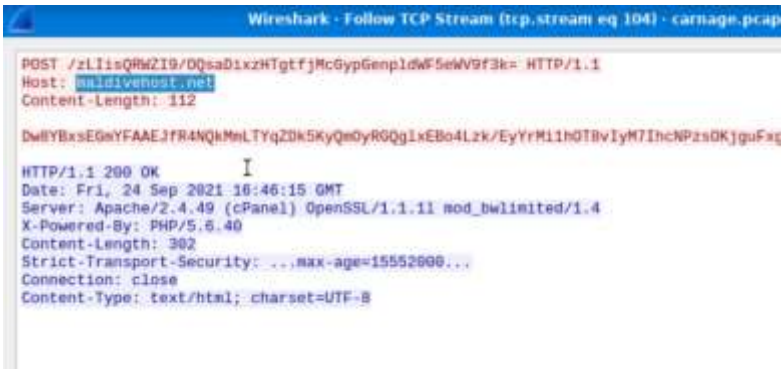
drb_ra
2 years ago

Cobalt Strike Server Found
C2: HTTPS @ 185[.]125[.]204[.]174:4444
C2 Server: securitybusinpuff[.]com,/jquery-3[.]
POST URI: /jquery-3[.]3[.]2[.]min[.]js
Country: N/A
ASN: Hydra Communications Ltd

#c2 #cobaltstrike

13. What is the domain name of the post-infection traffic?

The hint specifies that we look into the POST traffic so we shall use the following filter to achieve that: ***http:request:method == POST*** then we will follow the TCP stream conversation and that will reveal the host/domain name. Ans: **maldivehost.net**



Wireshark · Follow TCP Stream (tcp.stream eq 104) · carnage.pcap

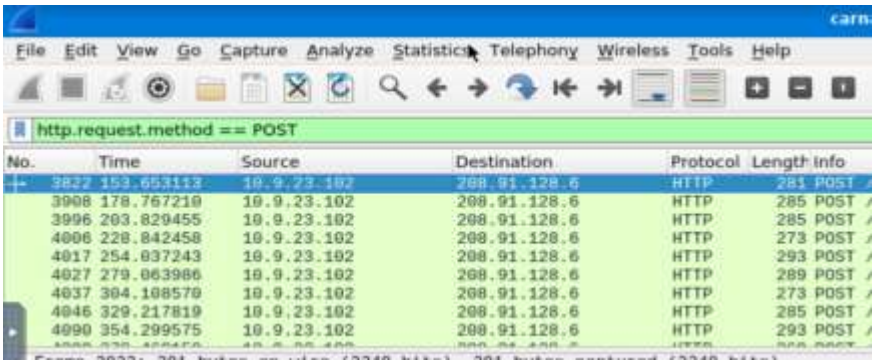
```
POST /zLIisQRWZI9/DQsaDixzHTgtfjMcGypGenpldWF5eWV9f3k= HTTP/1.1
Host: maldivehost.net
Content-Length: 112

DwEYBxsEGmYFAAEJfR4NQkMmLTYqZDk5KyQmOyRGQglxEBo4Lzk/EyYrMi1hOTBvIyM7IhcNPzsOKjguFxg

HTTP/1.1 200 OK
Date: Fri, 24 Sep 2021 16:46:15 GMT
Server: Apache/2.4.49 (cPanel) OpenSSL/1.1.11 mod_bwlimited/1.4
X-Powered-By: PHP/5.6.40
Content-Length: 302
Strict-Transport-Security: ...max-age=15552000...
Connection: close
Content-Type: text/html; charset=UTF-8
```

14. What are the first eleven characters that the victim host sends out to the malicious domain involved in the post-infection traffic?

The same stream conversation will also reveal the first eleven characters of the POST request. Ans: **zLIisQRWZI9**

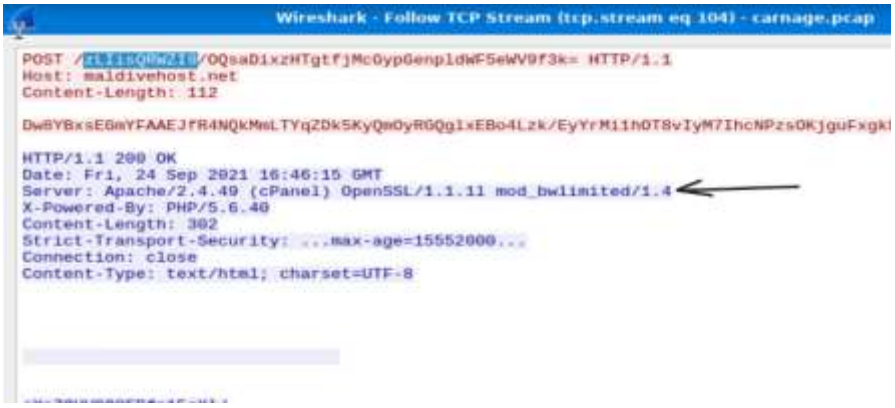
15. What was the length for the first packet sent out to the C2 server?

From the earlier POST filter, the packet length is shown in the Length column. Ans: **281**



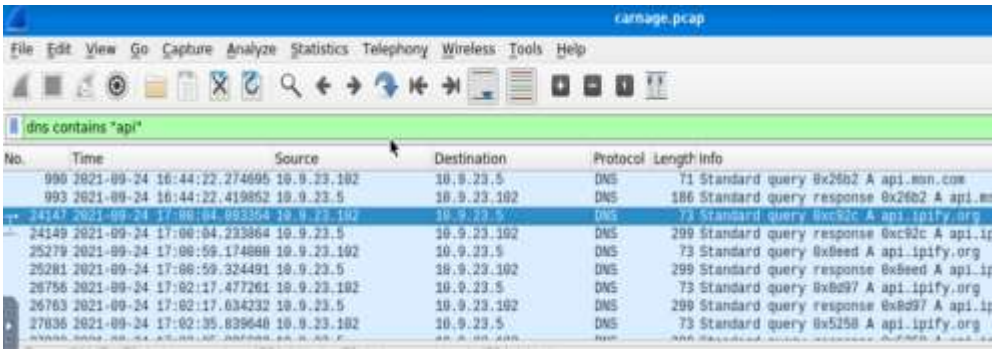
16. What was the Server header for the malicious domain from the previous question?

We can get this from the earlier TCP stream conversation window. Ans: **Apache/2.4.49 (cPanel) OpenSSL/1.1.1l mod_bwlimited/1.4**



17. The malware used an API to check for the IP address of the victim's machine. What was the date and time when the DNS query for the IP check domain occurred? (**answer format**: yyyy-mm-dd hh:mm:ss UTC)

We are requested to look for at DNS queries that use "api" to check for IP addresses, we can tailor our filter our packets to display DNS and anything containing "api". Our filter will be as follows: ***dns contains "api".*** Applying that filter will display DNS packets with the word "api". Ans: **2021-09-24 17:00:04**

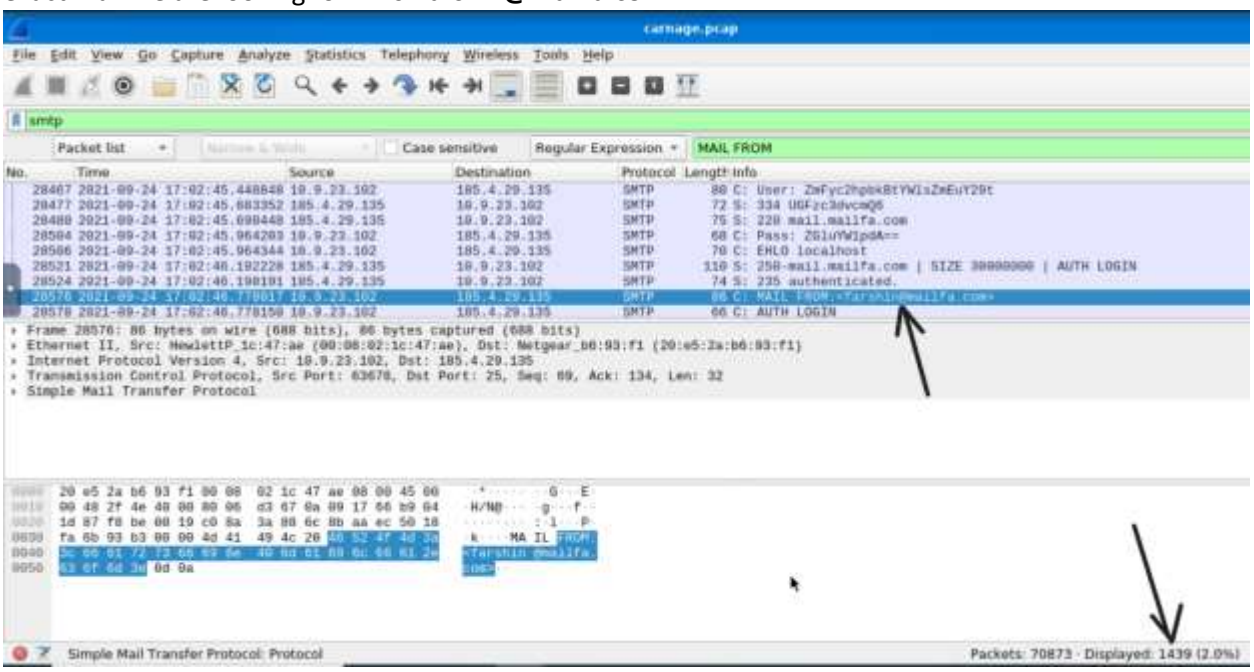


18. What was the domain in the DNS query from the previous question?

Looking at the packet, the domain is displayed. Ans: **api.ipify.org**

19. Looks like there was some malicious spam (malspam) activity going on. What was the first MAIL FROM address observed in the traffic?

SMTP (Simple Mail Transfer Protocol) is used when sending/receiving mail so a global SMTP search will reveal all packets related to SMTP. A further "find" search (Ctrl + F) for "MAIL FROM" will reveal the exact mail we are looking for. Ans: **farshin@mailfa.com**



20. How many packets were observed for the SMTP traffic?
Ans: **1439**