Traffic data Example steps (these will vary depending on systems and how data was moved)

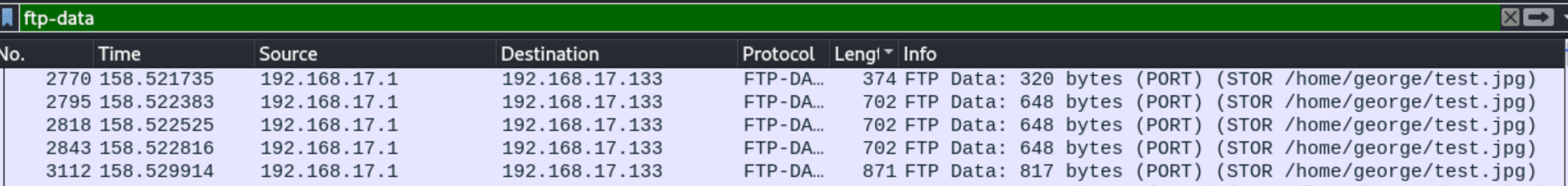
Set parameters to FTP

Calendar

Description automatically generated with medium confidence

This was because of how this protocol sends files across the network so it would be the first one to look for any files being sent across as user account is shown to be george but we need the actual data.

Set parameters to FTP-DATA



To focus into FTP data that actually contains the data

Right click ftp-data and look into the tcp streams using follow.

NOTE (important tool to remember): We do not have to use binwalker to find files embedded within the binaries as jpeg was found without the use of it

Text

Description automatically generated

To look into the information

Show data as raw in order to convert the plausible file test.jpg into something readable

Save as jpeg as we are looking into a test.jpg as shown in info.

Graphical user interface, text, application, chat or text message

Description automatically generated

Open it up and we can see the exfiltrated file.

Basic analysis:



The Source IP Address: is 192.168.17.1. This is because of how the source from wireshark stated sent the FTP-DATA Stream which contained the jpeg file that was exfiltrated across.

The Destination IP address: is 192.168.7.133. This is because of how the destination was the location shown in wireshark where the exfiltrated file test.jpg was heading towards.

The exfiltration method was the exfiltration of data over FTP using the tcp protocol.

A picture containing text, sky, outdoor

Description automatically generated

These steps are now for finding a malware hidden withing the network traffic using Wireshark (may vary depending on type of malware and the attackers goal)

How it was accomplished.

Assigned parameters to http.

Graphical user interface, application

Description automatically generated

            Due to the protocol being less secured so it is more open to attacks.

Sorted the length information to decrease.

            Due to malware traffic usually having a lot of redirects to infected urls or interactions to other malicious code in order to execute properly and spread to neighbouring devices.

Graphical user interface, text, application

Description automatically generated

Noticed that source IP addresses were relatively common. Looked into the information with get methods.

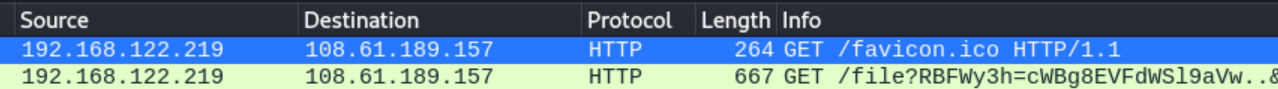
            A lot of malicious code interacting through the network would most likely have the reason to get the victim's computer to install more malicious code and to do a large amount of damage as it is easily noticeable if it was all in one piece of code. This means that the malicious code would be sending several get messages to download even more malware.

Finally looked into the previous and next requests.



^This would reveal all the possible hostnames and destination IP Addresses that the malware traffic might be trying to communicate on. This would also reveal the name of the malware as we could google the hostname to reveal the analysis on the related code as shown in the last few screenshots where after searching the hostname up it would reveal all the possible other hostnames that the malware goes into and what each of the sites accomplish.

Analysis:

The source IP Address is 192.168.122.219 

This is because of how multiple get requests are happening in the same computer which is considered the victim as the person downloaded the malware into the pc itself. This is proven as there are multiple get requests that allow the malware to obtain and download urls and malicious codes to harm the source -which is the victims pc-.

The destination IP Address are 108.61.189.157 and 192.68.122.219.



A screenshot of a computer

Description automatically generated

This is proven to be the case with the next request when clicked showed 192.168.122.219

A screenshot of a computer

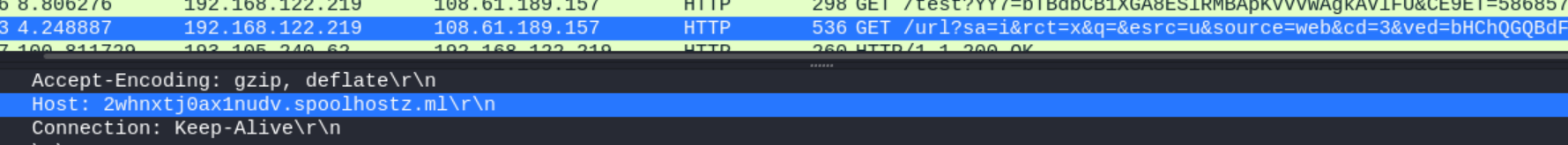
Description automatically generated

^Shifting throughout the requests to find next possible destination addresses.

Because the third http request showed it going back to the same destination address (108.61.189.157), this means that the main destination ip address is 108.61.189.157.

In terms of providing proof on what the malware is while also understanding on what the attacker was trying to accomplish with this malicious code

One possible hostname is 2whnxtj0ax1nudv.spoolhostz.m1\r\n



Text

Description automatically generated

^List of all possible hostnames in the website (nuclear)

From the website (nuclear) as well in terms of going indepth, this means that throughout following the related domains The possible hostnames are alphameioambiente.com.br, and the third one is film24hd.us. while The final compromised website being the randomremodeling.com

The malware used to generate this nuclear EK

Text

Description automatically generated

Obtained when searching up the hostname from the malware traffic in wireshark. This is because of how it is related to the spoolhostz url that was being obtained by the get method in the malware traffic.

This malware called nuclear ek is also known as a nuclear exploit kit.(nuclearDef) Victims or websites hacked by the nuclear EK malicious code are basically injected with rogue code that redirects the user to other domains that appear to be hosting ads. (nuclearDef) This is designed as a distraction as well as the fraud as these ads for the websites were designed to send visitors to the malware as well allowing it to propagate. (nuclearDef)

Graphical user interface, text, application

Description automatically generated

^An inDepth overview on the nuclear exploit kit malware by malwarebyte (nuclearDef).

[Reference]

<https://www.malware-traffic-analysis.net/2015/10/05/index.html> (nuclear)

<https://blog.malwarebytes.com/threat-analysis/2016/02/nuclear-ek-leveraged-in-large-wordpress-compromise-campaign/> (nuclearDef)