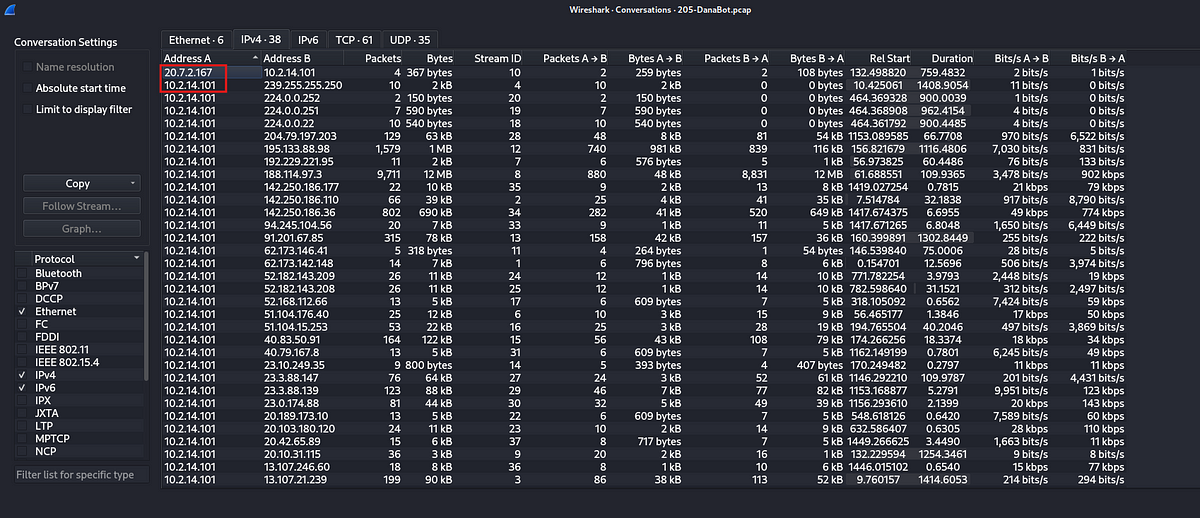
### **DANABOT — CYBERDEFENDERS**

**Scenario:** The SOC team has detected suspicious activity in the network traffic, revealing that a machine has been compromised. Sensitive company information has been stolen. Your task is to use Network Capture (PCAP) files and Threat Intelligence to investigate the incident and determine how the breach occurred.

We are given a pcap file to perform the analysis.

**Initial Analysis:**

Let us check the conversations to see the IP addresses present in this capture file.



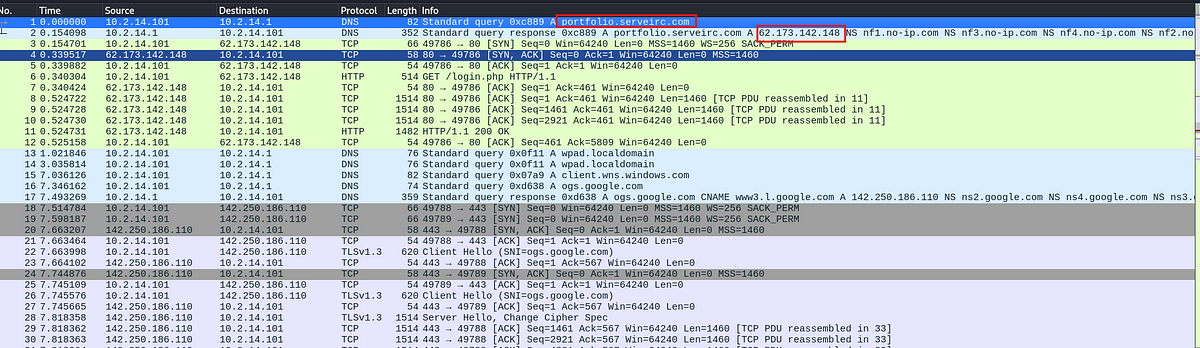
We can see above that there are only two private IP addresses in the list and most of the traffic is related to 10.2.14.101. If we look at the capture packets we can see that 10.2.14.101 is making a DNS request to 10.2.14.1 which concludes that 10.2.14.1 is the DNS server and 10.2.14.101 is the victim.

Now, let us start investigating the packets.

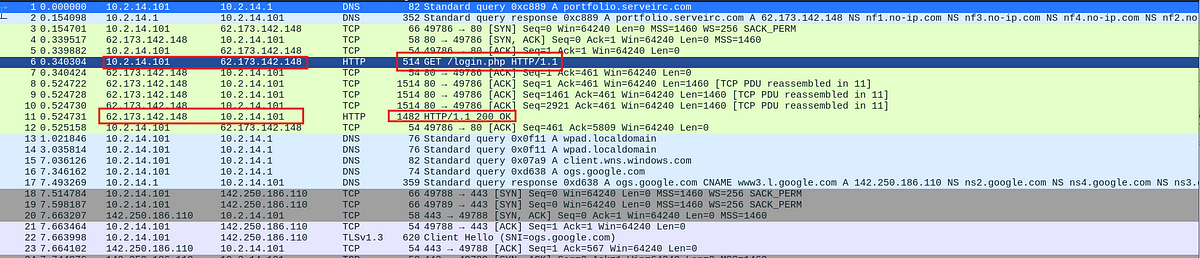
**Tasks:**

1. Which IP address was used by the attacker during the initial access?

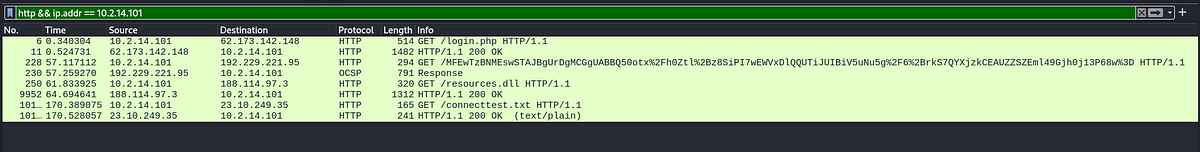
Immediately after opening the capture file, the first packet is a DNS request from the victim to the DNS server about a suspecious looking domain. portfolio[.]serveirc[.]com. The next packet we can see the resolved address for this domain which is 62[.]173[.]142[.]148.



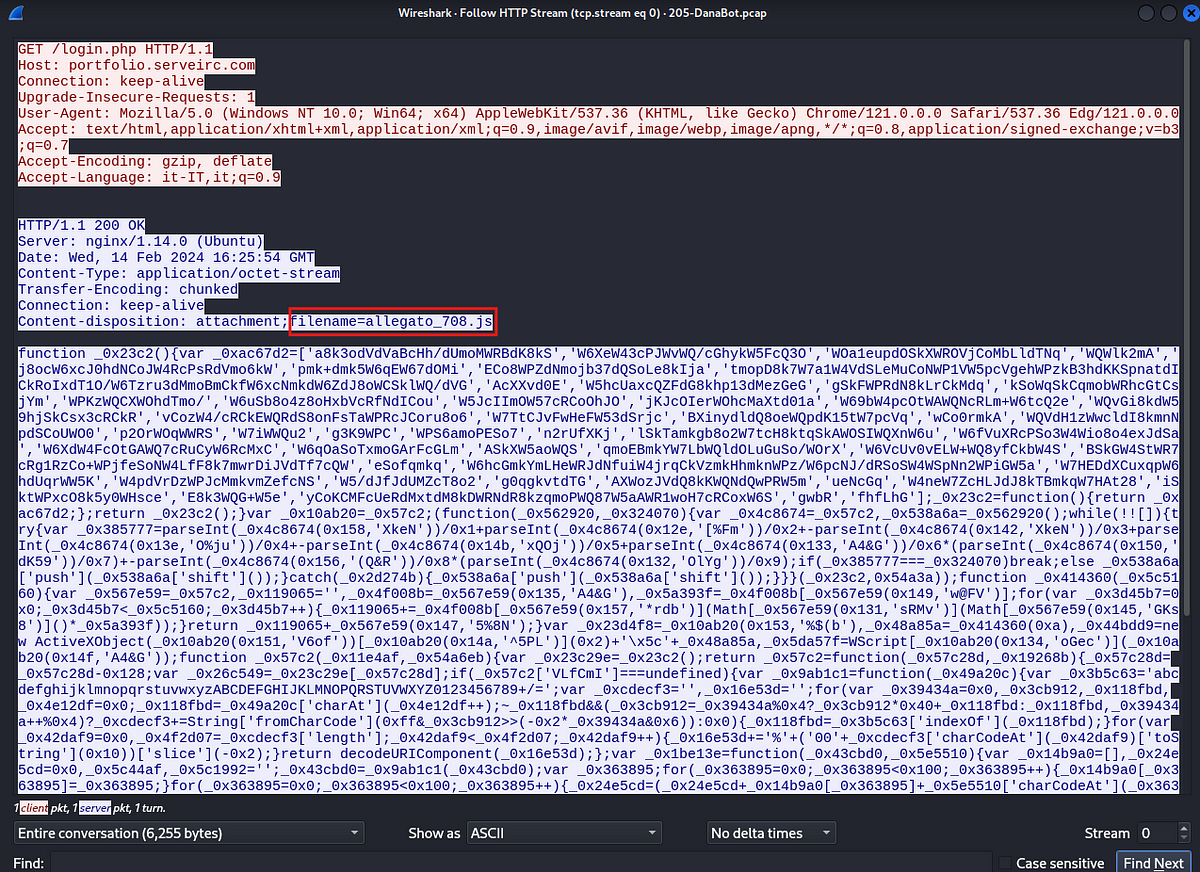
Few packets later, we can see a login request made from the victim machine to the suspicious IP. This request was successful.



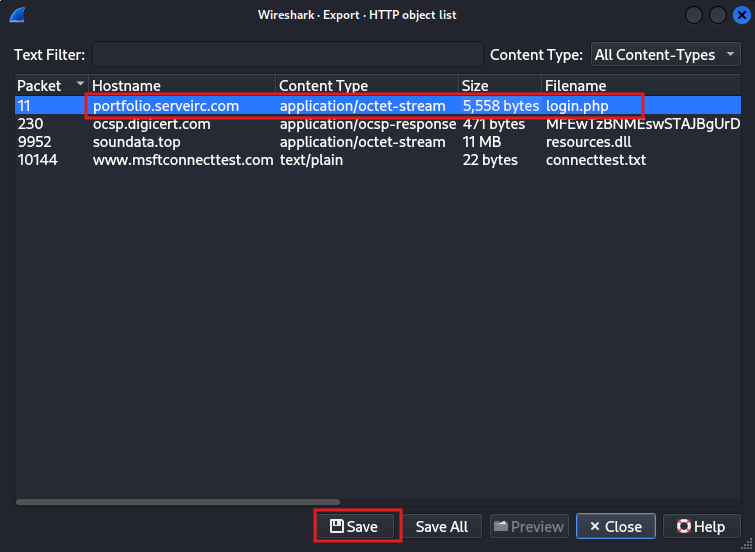
Now let us examine this. Let us first filter out the http traffic to and from the victim IP.



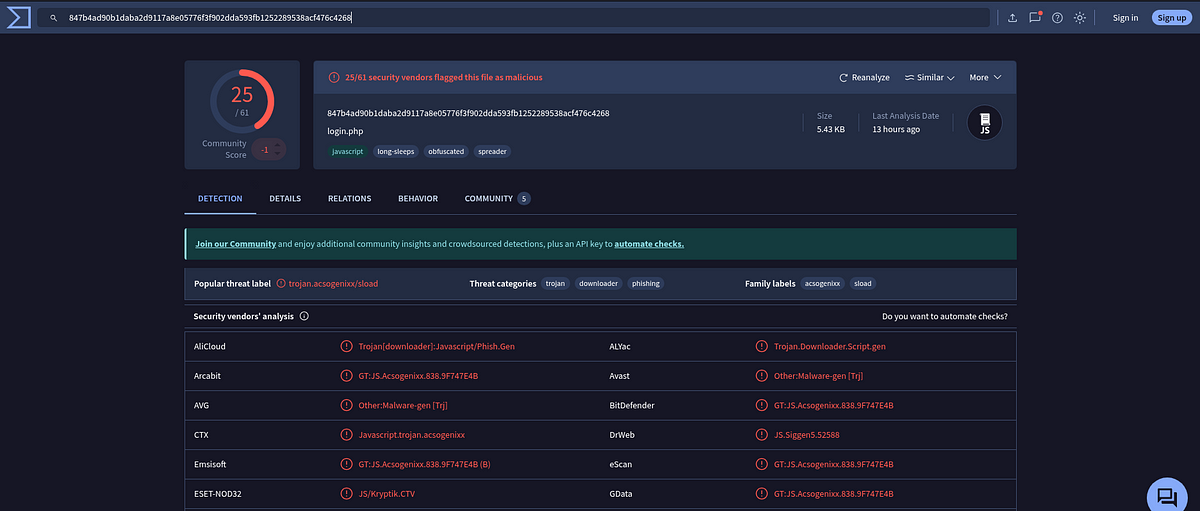
Now, let us inspect login request. Select the packet and click on follow HTTP stream.



As we can see above, a file was sent over from the suspicious IP to the victim machine. Let us export this and check if there are any known reports about this file.



Now let us calculate the hash of this file and check onVirustotal to see if it is legit or not.

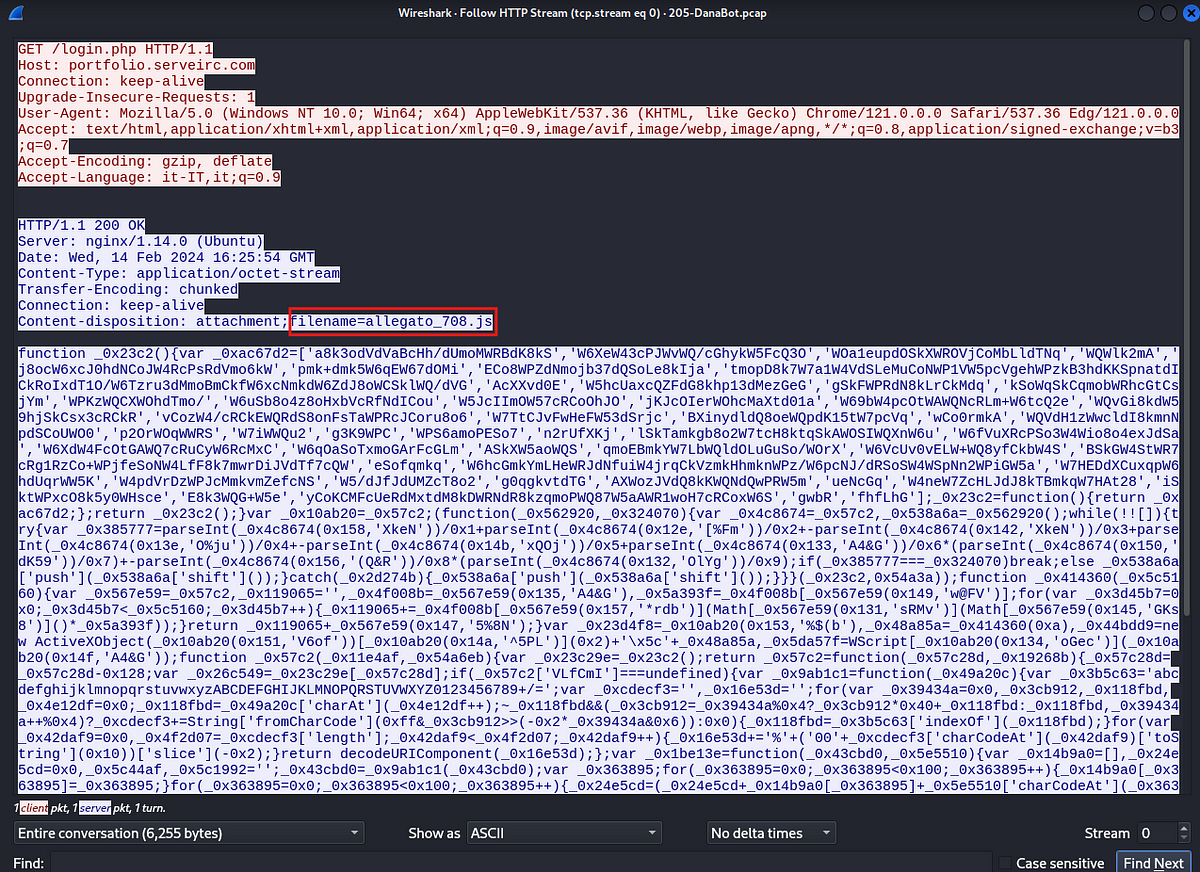


As per Virustotal, this file is a malware. So it is clear that the IP address 62[.]173[.]142[.]148 is indeed a malicious IP and was used for initial access of the victim.

Answer: 62[.]173[.]142[.]148

2. What is the name of the malicious file used for initial access?

In the above analysis, when we checked the HTTP stream, we found out the name of the file.



Answer: allegato\_708.js

3. What is the SHA-256 hash of the malicious file used for initial access?

We already calculated this previously.

Answer: 847b4ad90b1ddaba2d9117a8e05776f3f902dda593fb1252289538acf476c4268

4. Which process was used to execute the malicious file?

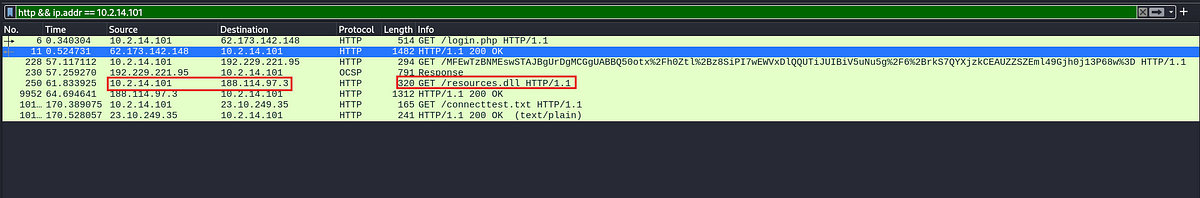
We can examine the script from the above file. Although it is heavily obfuscated, we can see that it is using WScript, which is a Windows script host used to execute scripts.



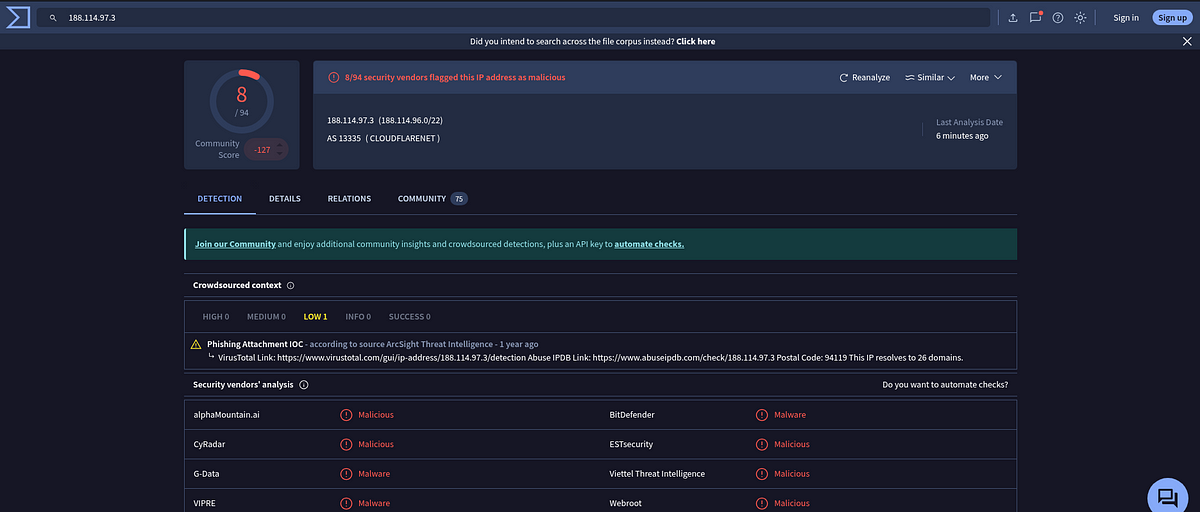
Answer: WScript.exe

5. What is the file extension of the second malicious file utilized by the attacker?

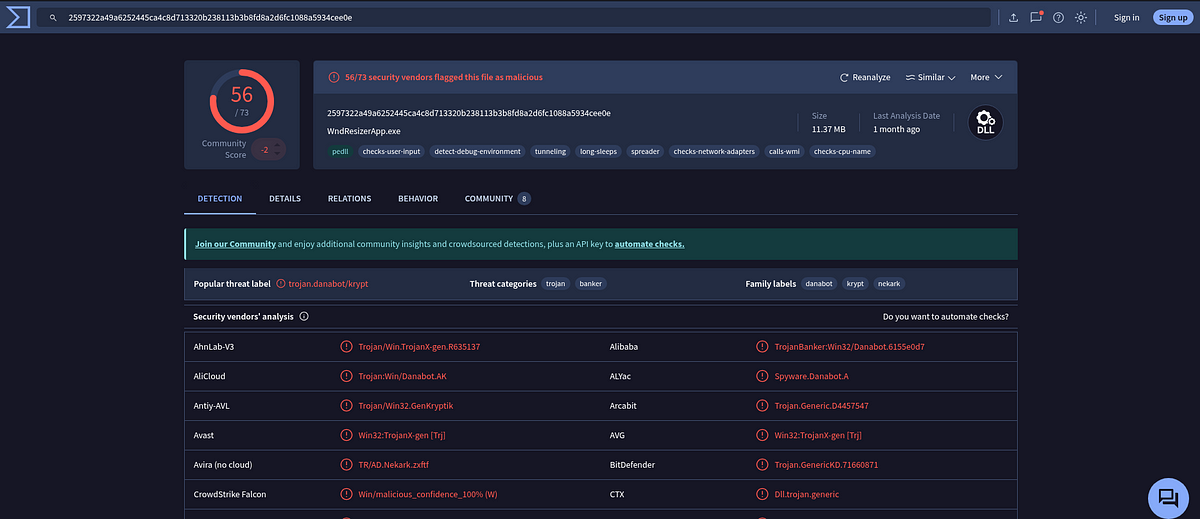
Let us look at the other http packets belonging to the vicim IP. We can see that there was another get request for a file called resources.dll.



Let us check the reputation of the IP address 188[.]114[.]97[.]3.



The IP address seems to be suspicious, let us now check the file reputation. Export the file and calculate the hash and then check it on Virustotal.



The file is definitely malicious.

Answer: .dll

6. What is the MD5 hash of the second malicious file?

Let us calculate the MD5 hash of this file.



Answer: e758e07113016aca55d9eda2b0ffeebe

This is the end of this walkthrough.