CTF Walkthrough: Cyber Defenders - DanaBot

By: Tyreese Evans

Date: 2/7/2025

CyberSecurity and DFIR

LinkedIn: Tyreese Evans

GitHub:TEvans-Developer

Introduction

In this walkthrough, I will be tackling the Network Forensics challenge known as ***DanaBot*** from Cyber Defenders. DanaBot, is a well know sophisticated RAT trojan used in phishing campaigns and allows remote access to compromised systems for exfiltration of sensitive data. The challenge is designed to test and develop the network forensics skills of Blue Team professionals such as **Security Operation Center (SOC)** analyst and **Digital Forensics and Incident Response (DFIR)** by analyzing **Malware**, **Packet Captures (PCAP)**, gathering information with **Threat Intelligence** tools.

About the Author

Tyreese Evans is a passionate cybersecurity enthusiast and budding professional with a strong interest in cybersecurity, network security and digital forensics. Utilizing experience in participating in various Capture The Flag (CTF) challenges and a focus on malicious behavior detection, Tyreese Evanshas developed a keen understanding of advanced attack tactics and techniques.

Through hands-on experience in identifying the tactics, techniques and procedures (TTPs) used by malware such as DanaBot, a sophisticated banking Trojan and remote access tool (RAT). In this project, Tyreese Evans will focus on investigating and analyzing the malware's behavior, from initial access through to exfiltration and impact, while also applying industry best practices for mitigation and defense.

Participating in CTF Challenges has help Tyreese Evans in deepen his knowledge in reverse engineering, network traffics analysis and incident response, aiming to contribute to the cybersecurity community with insights into real-world cyber threats and defenses.

When not working on CTFs, Tyreese Evans enjoys learning about new technologies, contributing to open-source projects and keeping up-to-date with latest trends in cybersecurity research.

CTF Information

Platform: Cyber Defenders

Challenge: DanaBot

Category: Network Forensics

Difficulty: Easy

References (Link): Blue team CTF Challenges | DanaBot - CyberDefenders

Purpose of the Walkthrough

The purpose of this walkthrough will be to provide a step-by-step guide to solving the DanaBot lab from Cyber Defenders. This lab focuses on identifying, analyzing and mitigating a **botnet** that has been compromised with malware. The challenge is designed to help participants improve their skills in **network analysis**, **malware identification** and **incident response**.

In the walkthrough I will break down the different tasks that are involved in the lab, demonstrating how to:

- Analyze network traffic to detect malicious botnet communication
- Decompile malware samples to understand how the botnet operates.
- Extract valuable information, such as **Command –and-Control (C&C or C2)** servers and botnet functionality.
- Mitigate the threat by implementing defensive measures and security best practices.

The underlying goal is to provide a clear understanding of how botnets work and how to approach malware analysis which all are essential skills for anyone interested in **cybersecurity** and **threat hunting**.

Tools and Setup

Tools:

- Wireshark
- VirusTotal
- ANY.RUN (optional)
- Kali Linux

What is Wireshark?

Wireshark is an open-source networking tool that can be utilized in examining / analyzing detailed packet data from endpoints to better understand what is happening within network cabling. It can be used to troubleshoot network problems, examine security problems, debug protocol implementations and much more (Wireshark, 2019).

What is VirusTotal?

VirusTotal a free online service that allows user to upload and scan files, URLs and other types of content for potential malware or viruses. VirusTotal utilizes over 70 antivirus scanners and

URL/domain blocklisting services in addition to its myriads of tools to extract signals from studied content (VirusTotal, n.d.).

What is ANY.RUN?

ANY.RUN is an interactive malware analysis and dynamic analysis tool designed to examine suspicious files, URLS and network activity within a sandbox environment. It aids users in analyzing the behavior of potentially malicious files in real-time to help give a deeper understanding of how the malware operates and interacts with the system (a.bespalova, 2020).

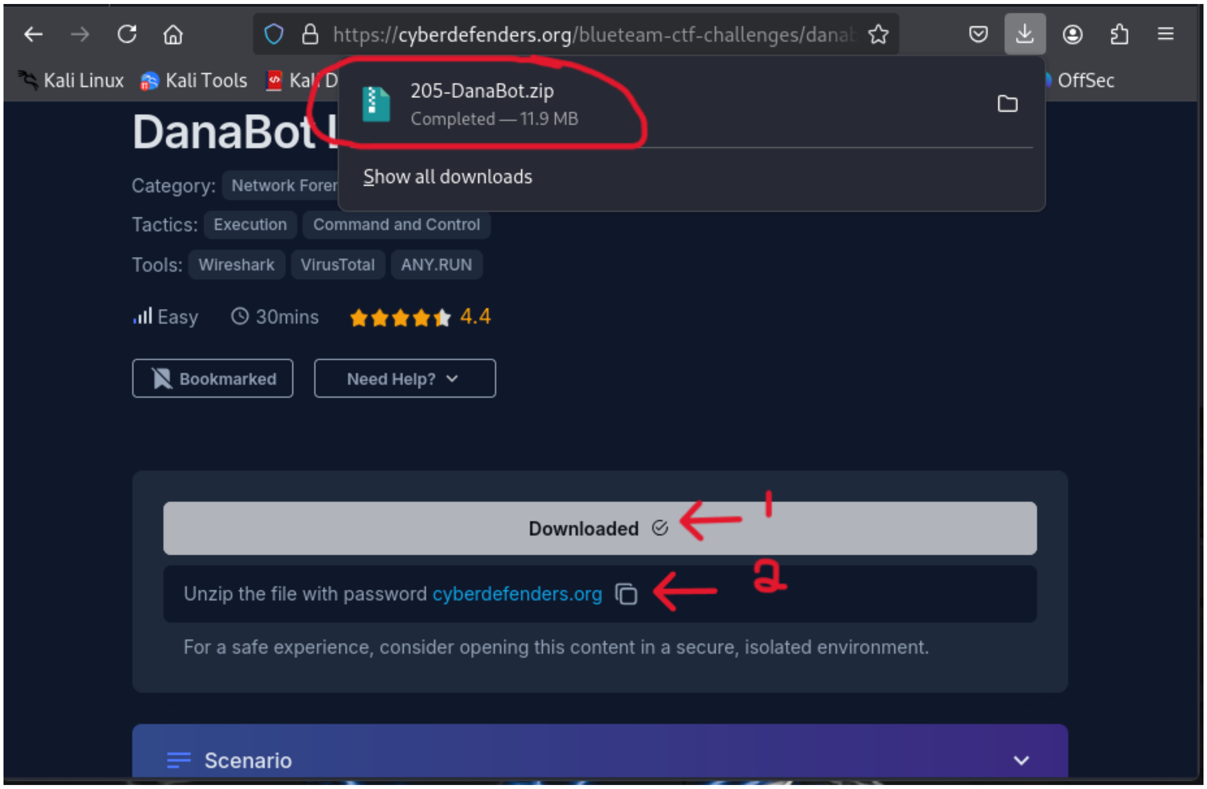
What is Kali Linux?

Kali Linux is a Debian-based Linux distribution that is designed for cyber security professionals and their needs. Kali Linux can be utilized for penetration testing, security auditing and ethical hacking. Kali Linux comes with a wide variety of tools for task such as vulnerability assessment, network analysis, digital forensics, reverse engineering and web application testing (What is Kali Linux? | Kali Linux Documentation, 2023).

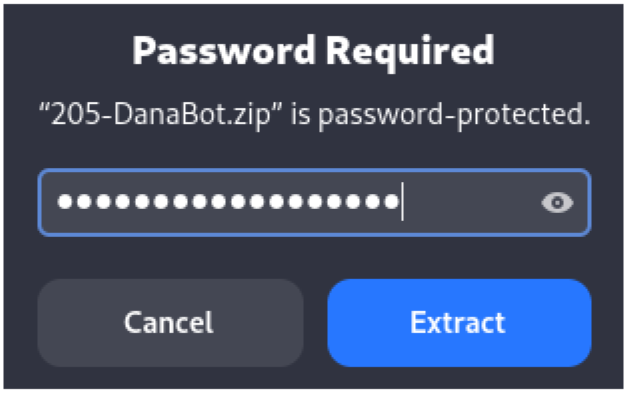
Setup:

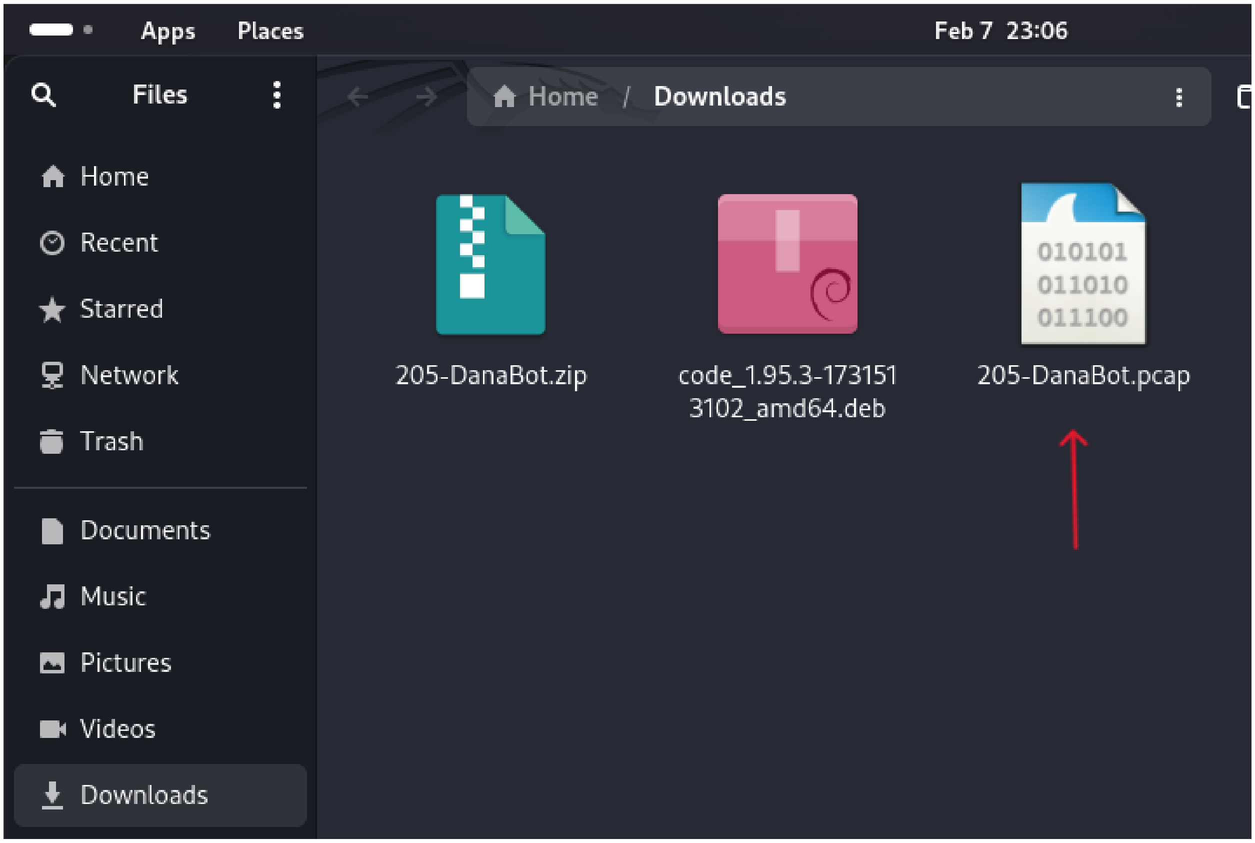
The initial setup for this CTF was done in a Kali Linux machine with the appropriate tools, updates and upgrades.

1. You need to navigate to the CyberDefenders platform for the DanaBot CTF (reference), here you will need to Download the Zip files.


https://cyberdefenders.org/blueteam-ctf-challenges/danab
Kali Linux
Kali Tools
Kali D
OffSec
205-DanaBot.zip
Completed — 11.9 MB
Show all downloads
DanaBot
Category: Network Foren
Tactics: Execution Command and Control
Tools: Wireshark VirusTotal ANY.RUN
Easy
30mins
4.4
Bookmarked
Need Help?
Downloaded
1
Unzip the file with password cyberdefenders.org
2
For a safe experience, consider opening this content in a secure, isolated environment.
Scenario

2. The provided password from CyberDefenders was used to unzip the files for analysis. A **.pcap** file should appear in the Download directory.





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*" (CyberDefenders, 2024)

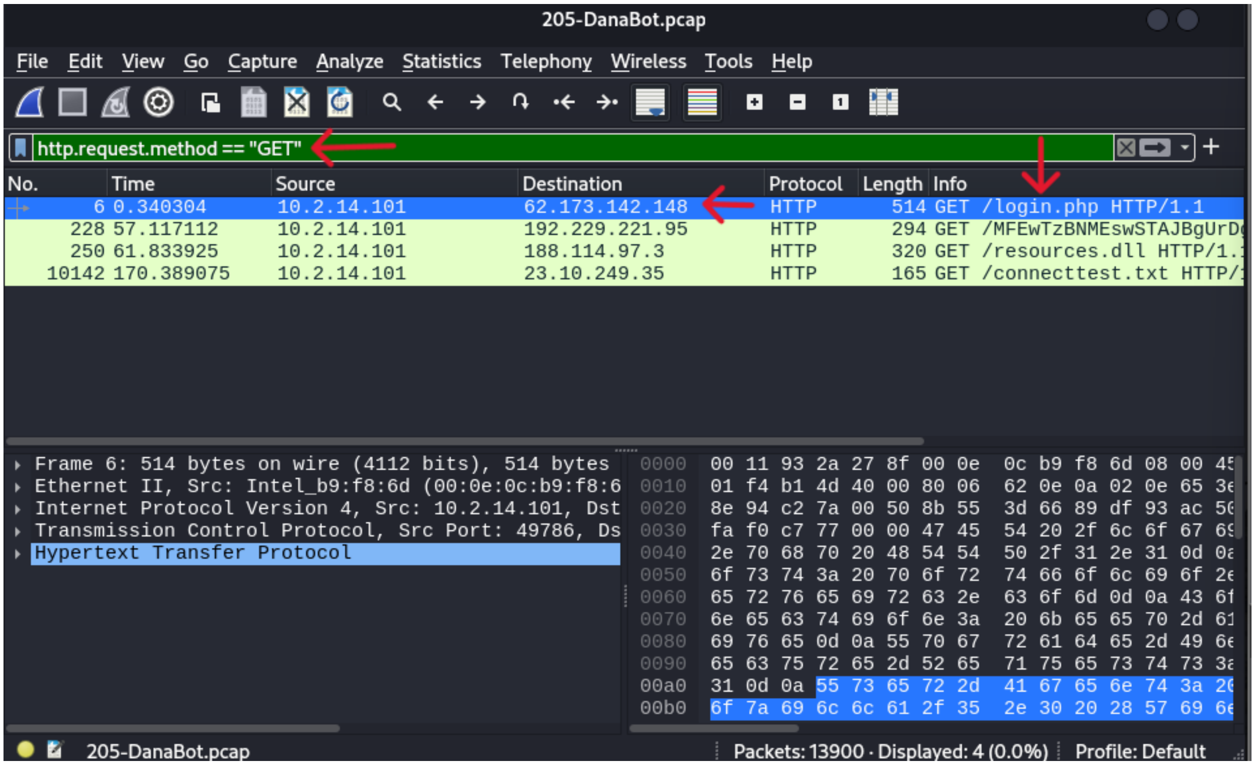
Questions Answers and Walkthrough

Q1. Which IP address was used by the attacker during the initial access?

Approach: Discovering the IP address is a critical part of discovering the type of target we are dealing with. This information allows us to understand where the target is, the IP to block, the potential TTP they could have made on our system. Having this information is important because it could be associate with other potential attacks made on our system or other organizations that have been attacked. Lastly, this information can help take legal action against the attackers.

Step 1: We utilize the Wireshark tool in this particular question. We open the Wireshark tool and then navigate to the file button on the top left of the window. Click open and we will then find the packet capture file "***205-DanaBot.pcap***" from the directory it was saved in.

Step 2: In the filter bar, we will use the "***http.request.method* == *"GET*"" to find possible signs of GET request made to retrieve a login attempts. The GET method is asking the backend to receive data relevant to the specific account the attacker is logging into. Here we can see there is a destination IP address where a GET request was made.



```
http.request.method == "GET"
```

```
No.   Time        Source       Destination      Protocol Length Info
    6 0.340304    10.2.14.101  62.173.142.148   HTTP        514 GET /login.php HTTP/1.1
  228 57.117112   10.2.14.101  192.229.221.95   HTTP        294 GET /MFEwTzBNMEswSTAJBgUrDg
  250 61.833925   10.2.14.101  188.114.97.3     HTTP        320 GET /resources.dll HTTP/1.1
10142 170.389075  10.2.14.101  23.10.249.35     HTTP        165 GET /connecttest.txt HTTP/1
```

```
▸ Frame 6: 514 bytes on wire (4112 bits), 514 bytes
▸ Ethernet II, Src: Intel_b9:f8:6d (00:0e:0c:b9:f8:6
▸ Internet Protocol Version 4, Src: 10.2.14.101, Dst
▸ Transmission Control Protocol, Src Port: 49786, Ds
▸ Hypertext Transfer Protocol
```

```
0000  00 11 93 2a 27 8f 00 0e  0c b9 f8 6d 08 00 45
0010  01 f4 b1 4d 40 00 80 06  62 0e 0a 02 0e 65 3e
0020  8e 94 c2 7a 00 50 8b 55  3d 66 89 df 93 ac 50
0030  fa f0 c7 77 00 00 47 45  54 20 2f 6c 6f 67 69
0040  2e 70 68 70 20 48 54 54  50 2f 31 2e 31 0d 0a
0050  6f 73 74 3a 20 70 6f 72  74 66 6f 6c 69 6f 2e
0060  65 72 76 65 69 72 63 2e  63 6f 6d 0d 0a 43 6f
0070  6e 65 63 74 69 6f 6e 3a  20 6b 65 65 70 2d 61
0080  69 76 65 0d 0a 55 70 67  72 61 64 65 2d 49 6e
0090  65 63 75 72 65 2d 52 65  71 75 65 73 74 73 3a
00a0  31 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20
00b0  6f 7a 69 6c 6c 61 2f 35  2e 30 20 28 57 69 6e
```

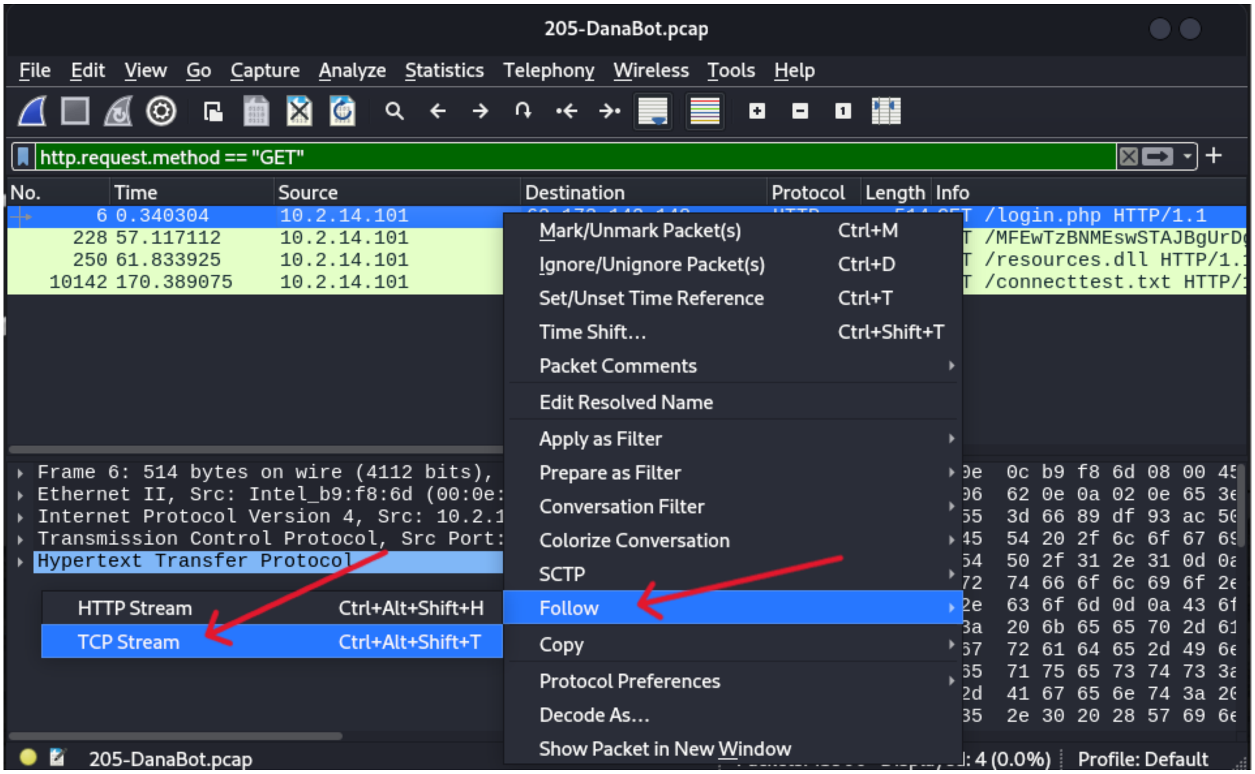
205-DanaBot.pcap | Packets: 13900 · Displayed: 4 (0.0%) | Profile: Default

Q1. Answer: **62.173.142.148**

Q2. What is the name of the malicious file used for initial access?

Approach: Being able to understand the method in which the attacker gains their initial access in the system could help guide us in understanding other possible tactics, techniques and procedures our attack may use. This could help us as analyst perform better forensics and look into specific locations in detail to find other possible compromises, lateral movements and more. We will be able to also create alerts and block similar methods in the near future.

Step 1: We need to find to methods in which the attacker gained their initial access. In order to do so we will right click the highlighted line where we discovered our malicious IP. Here we then navigate and hover over tab "***Follow***" tab and then navigate and click "***TCP Stream***".



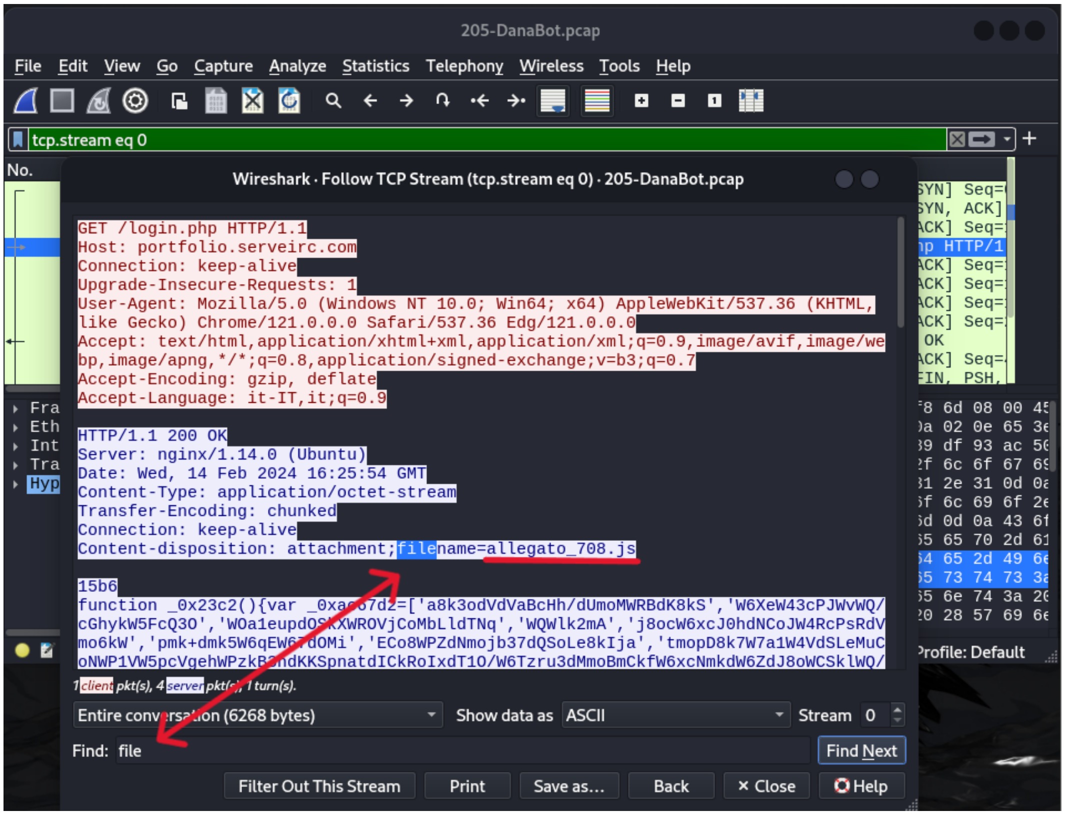
http.request.method == "GET"

```
No.    Time        Source        Destination    Protocol  Length  Info
     6 0.340304    10.2.14.101                                   T /login.php HTTP/1.1
   228 57.117112   10.2.14.101                                   T /MFEwTzBNMEswSTAJBgUrD
   250 61.833925   10.2.14.101                                   T /resources.dll HTTP/1.
 10142 170.389075  10.2.14.101                                   T /connecttest.txt HTTP/
```

```
› Frame 6: 514 bytes on wire (4112 bits),
› Ethernet II, Src: Intel_b9:f8:6d (00:0e:
› Internet Protocol Version 4, Src: 10.2.1
› Transmission Control Protocol, Src Port:
› Hypertext Transfer Protocol
```

```
0e  0c b9 f8 6d 08 00 45
06  62 0e 0a 02 0e 65 3e
55  3d 66 89 df 93 ac 50
45  54 20 2f 6c 6f 67 69
54  50 2f 31 2e 31 0d 0a
72  74 66 6f 6c 69 6f 2e
2e  63 6f 6d 0d 0a 43 6f
3a  20 6b 65 65 70 2d 61
57  72 61 64 65 2d 49 6e
55  71 75 65 73 74 73 3a
2d  41 67 65 6e 74 3a 20
35  2e 30 20 28 57 69 6e
```

Step 2: Now presented with the TCP stream between the source and destination IP (attacker) we now have more in-depth information to help us discover how the attacker gained their foothold. We can manually navigate to see the HTTP response from our server (Blue) to see the status code 200 OK sent to the attacker. We can type in "***File***" in the **Find** search bar and see in the **Content-disposition** there was a file name "***allgato_708.js***", a JavaScript file.


205-DanaBot.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 0
Wireshark · Follow TCP Stream (tcp.stream eq 0) · 205-DanaBot.pcap
Entire conversation (6268 bytes)
Show data as ASCII
Stream 0
Find: file
Find Next
Filter Out This Stream
Print
Save as…
Back
✕ Close
Help
Profile: Default

```
GET /login.php HTTP/1.1
Host: portfolio.serveirc.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/121.0.0.0 Safari/537.36 Edg/121.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: it-IT,it;q=0.9

HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Wed, 14 Feb 2024 16:25:54 GMT
Content-Type: application/octet-stream
Transfer-Encoding: chunked
Connection: keep-alive
Content-disposition: attachment;filename=allegato_708.js

15b6
function _0x23c2(){var _0xa667d2=['a8k3odVdVaBcHh/dUmoMWRBdK8kS','W6XeW43cPJWvWQ/
cGhykW5FcQ3O','WOa1eupdOSkXWROVjCoMbLldTNq','WQWlk2mA','j8ocW6xcJ0hdNCoJW4RcPsRdV
mo6kW','pmk+dmk5W6qEW67dOMi','ECo8WPZdNmojb37dQSoLe8kIja','tmopD8k7W7a1W4VdSLeMuC
oNWP1VW5pcVgehWPzkB3ndKKSpnatdICkRoIxdT1O/W6Tzru3dMmoBmCkfW6xcNmkdW6ZdJ8oWCSklWQ/
```

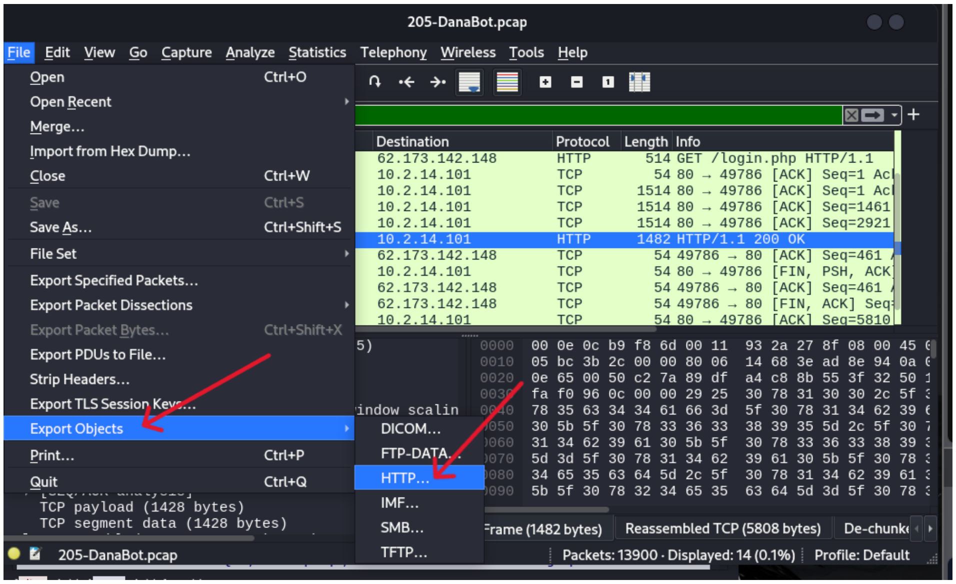
1 client pkt(s), 4 server pkt(s), 1 turn(s).

Q2. Answer: **allegato_708.js**

Q3. What is the SHA-256 has of the malicious file used for initial access?

Approach: The reason we find SHA-256 hash extracted from .pcaps are to help detect malicious payloads delivered via HTTP, FTP, SMB, E-mail attachments etc. and to compare those files hash against known malware databases like Virus Total.

Step 1: In Wireshark we will navigate to the **File** tab on the top of the application. We then hover over **Export Objects** and click **HTTP**.

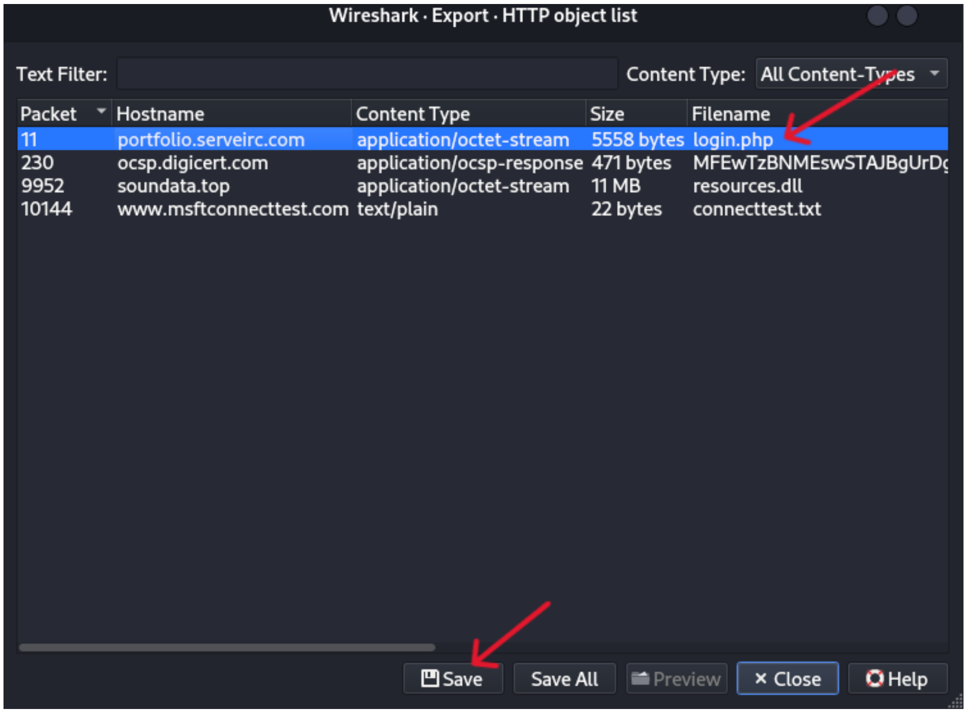


```
Destination       Protocol  Length Info
62.173.142.148    HTTP      514 GET /login.php HTTP/1.1
10.2.14.101       TCP        54 80 → 49786 [ACK] Seq=1 Ac
10.2.14.101       TCP      1514 80 → 49786 [ACK] Seq=1 Ac
10.2.14.101       TCP      1514 80 → 49786 [ACK] Seq=1461
10.2.14.101       TCP      1514 80 → 49786 [ACK] Seq=2921
10.2.14.101       HTTP     1482 HTTP/1.1 200 OK
62.173.142.148    TCP        54 49786 → 80 [ACK] Seq=461
10.2.14.101       TCP        54 80 → 49786 [FIN, PSH, ACK
62.173.142.148    TCP        54 49786 → 80 [ACK] Seq=461
62.173.142.148    TCP        54 49786 → 80 [FIN, ACK] Seq
10.2.14.101       TCP        54 80 → 49786 [ACK] Seq=5810
```

```
5)
indow scalin
  TCP payload (1428 bytes)
  TCP segment data (1428 bytes)
```

```
0000  00 0e 0c b9 f8 6d 00 11  93 2a 27 8f 08 00 45
0010  05 bc 3b 2c 00 00 80 06  14 68 3e ad 8e 94 0a
0020  0e 65 00 50 c2 7a 89 df  a4 c8 8b 55 3f 32 50
0030  fa f0 96 0c 00 00 29 25  30 78 31 30 30 2c 5f
0040  78 35 63 34 34 61 66 3d  5f 30 78 31 34 62 39
0050  30 5b 5f 30 78 33 36 33  38 39 35 5d 2c 5f 30
0060  31 34 62 39 61 30 5b 5f  30 78 33 36 33 38 39
0070  5d 3d 5f 30 78 31 34 62  39 61 30 5b 5f 30 78
0080  34 65 35 63 64 5d 2c 5f  30 78 31 34 62 39 61
0090  5b 5f 30 78 32 34 65 35  63 64 5d 3d 5f 30 78
```

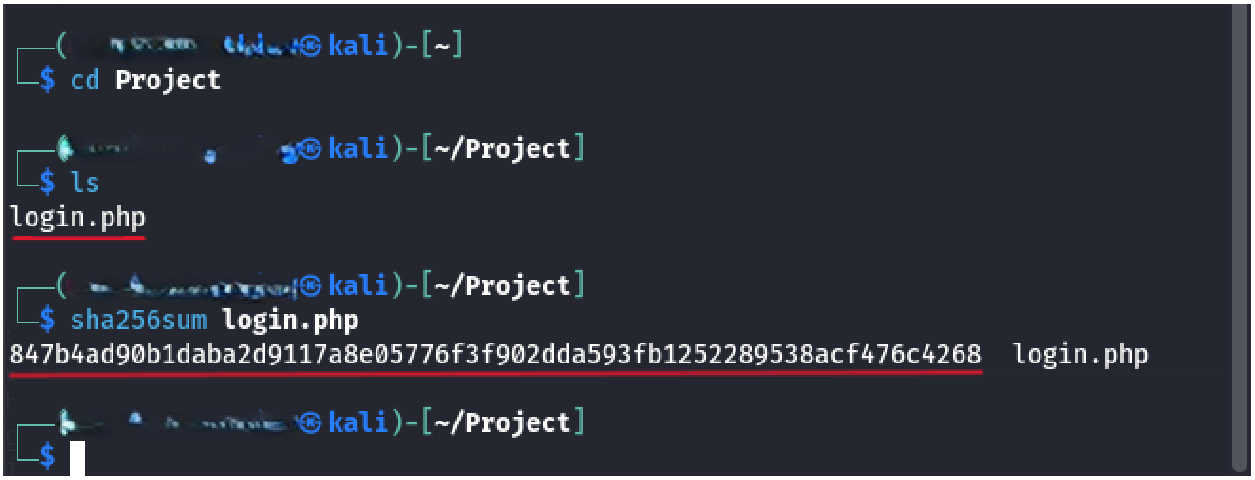
Step 2: We use packet 11 which has the file name "***login.php***". Click "**Save**" to save the file to a directory in the machine.


Wireshark · Export · HTTP object list
Text Filter:
Content Type: All Content-Types
Save
Save All
Preview
× Close
Help

Packet	Hostname	Content Type	Size	Filename
11	portfolio.serveirc.com	application/octet-stream	5558 bytes	login.php
230	ocsp.digicert.com	application/ocsp-response	471 bytes	MFEwTzBNMEswSTAJBgUrDg
9952	soundata.top	application/octet-stream	11 MB	resources.dll
10144	www.msftconnecttest.com	text/plain	22 bytes	connecttest.txt

Step 3: Opening a command terminal and change to the directory where the export file is being held, we checked the hash of the file by typing in the following command (below). Afterwards, a SHA256 hash appears.

sha256sum login.php



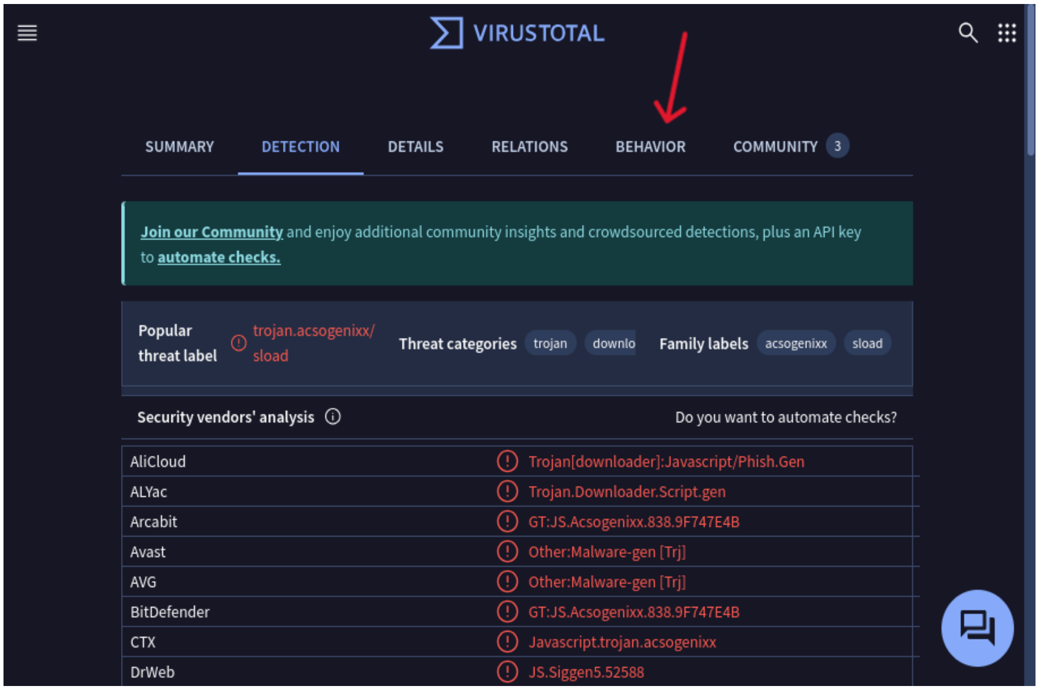
```
┌──([redacted]㉿kali)-[~]
└─$ cd Project

┌──([redacted]㉿kali)-[~/Project]
└─$ ls
login.php

┌──([redacted]㉿kali)-[~/Project]
└─$ sha256sum login.php
847b4ad90b1daba2d9117a8e05776f3f902dda593fb1252289538acf476c4268  login.php

┌──([redacted]㉿kali)-[~/Project]
└─$ 
```

Q3. Answer: **847b4ad90b1daba2d9117a8e05776f3f902dda593fb1252289538acf476c4268**

Q4. What process was used to execute the malicious file?

Approach: Comparing the file hash against VirusTotal is an important step in the forensics process because it provides a plethora of information that can be used to further understand the attack, the attacker and the malware on the endpoint or in the systems. VirusTotal can provide the different MITRE ATT&CK Tactics and Techniques associated with the malicious file, its behavior, network communication, rules and much more.

Step 1: We open up our web browser and navigate to VirusTotal's website (https://www.virustotal.com/gui/). We click on the **Choose File** icon and select the exported file from the packet capture. Virus total will then provide information about the malicious file.



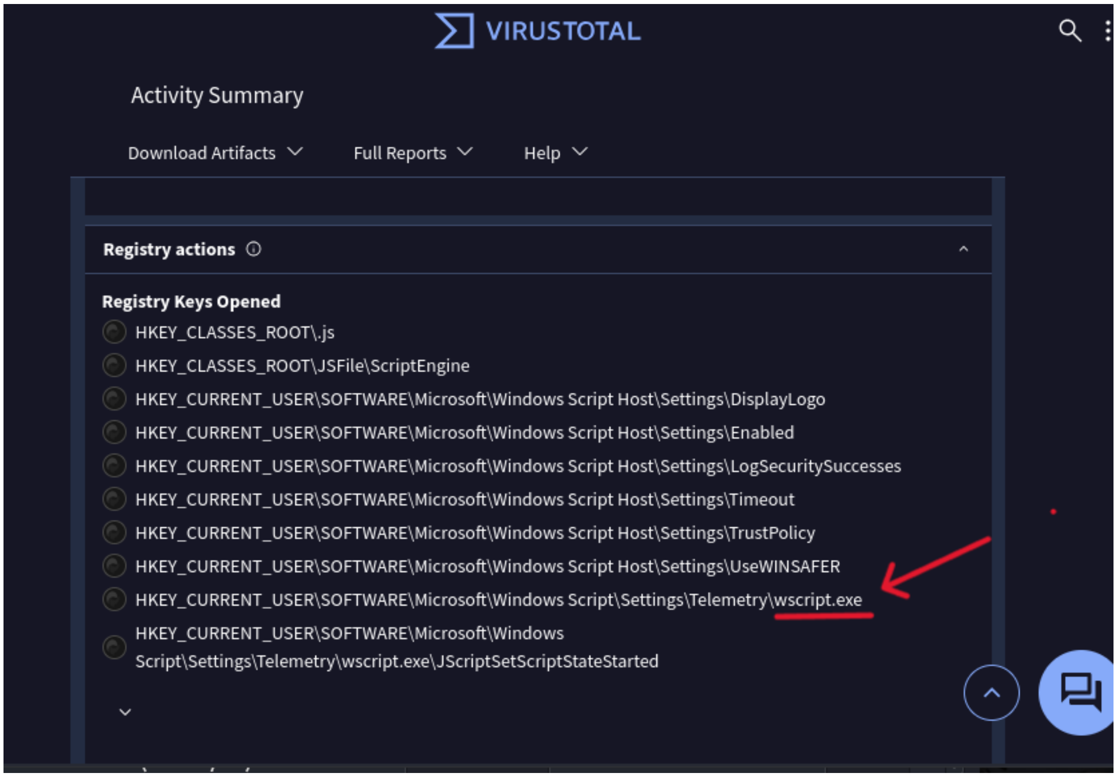
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.acsogenixx/sload — Threat categories: trojan, downlo — Family labels: acsogenixx, sload

Security vendors' analysis — Do you want to automate checks?

AliCloud	Trojan[downloader]:Javascript/Phish.Gen
ALYac	Trojan.Downloader.Script.gen
Arcabit	GT:JS.Acsogenixx.838.9F747E4B
Avast	Other:Malware-gen [Trj]
AVG	Other:Malware-gen [Trj]
BitDefender	GT:JS.Acsogenixx.838.9F747E4B
CTX	Javascript.trojan.acsogenixx
DrWeb	JS.Siggen5.52588

Step 2: We then navigate to the **BEHAVIOR** tab and scroll down to the **Registry actions** section. Here we will find our executable file. This is important because the registry actions provide insights into how a file or executable interacts with the Windows Registry, which is a hierarchical database that stores configuration settings and system information for Windows OS, application services and hardware devices.



Registry actions

Registry Keys Opened

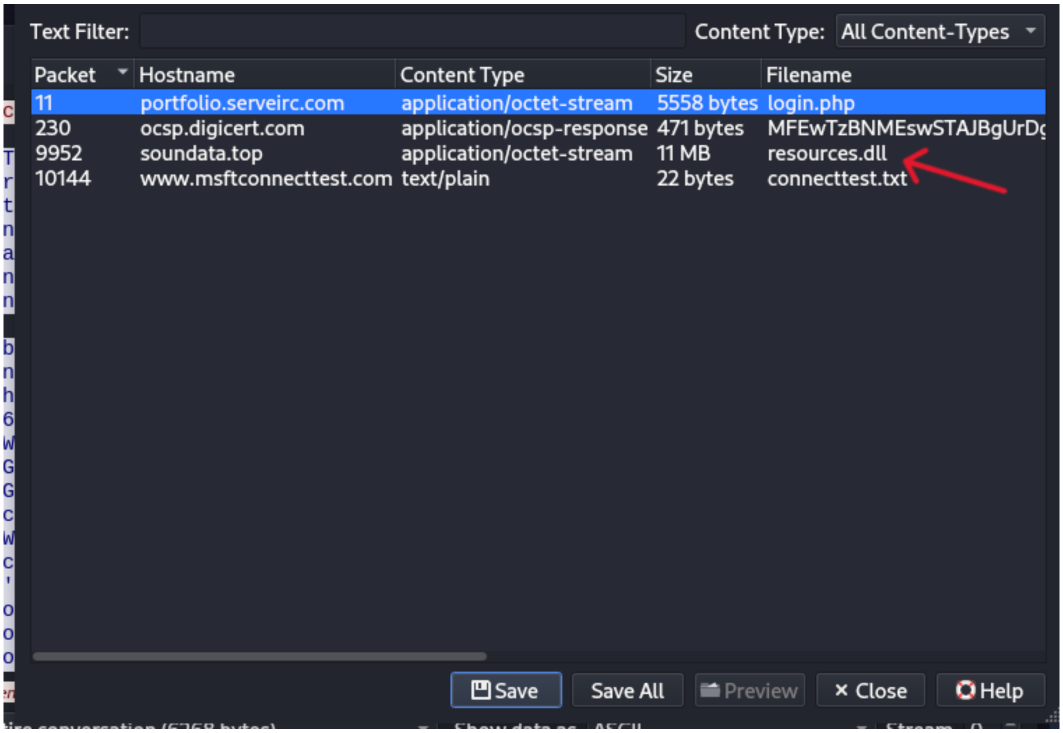
```
HKEY_CLASSES_ROOT\.js
HKEY_CLASSES_ROOT\JSFile\ScriptEngine
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows Script Host\Settings\DisplayLogo
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows Script Host\Settings\Enabled
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows Script Host\Settings\LogSecuritySuccesses
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows Script Host\Settings\Timeout
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows Script Host\Settings\TrustPolicy
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows Script Host\Settings\UseWINSAFER
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows Script\Settings\Telemetry\wscript.exe
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows
Script\Settings\Telemetry\wscript.exe\JScriptSetScriptStateStarted
```

Q4. Answer: **wscript.exe**

Q5. What is the file extension of the second malicious file utilized by the attacker?

Approach: Attackers often have different tactics and techniques they use to exploit and maintain persistence in an endpoint or network. As SOC analyst and DFIR analyst it is important identify all the footholds/ initial access, processes, privilege escalations and more to ensure that the threat actor does not maintain that persistence or create more.

Step 1: During the analysis we exported the login.php file from the pcap. On the same window of the application there was another file that the attacker uploaded with the extension of .dll.



Text Filter:

Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
11	portfolio.serveirc.com	application/octet-stream	5558 bytes	login.php
230	ocsp.digicert.com	application/ocsp-response	471 bytes	MFEwTzBNMEswSTAJBgUrDg
9952	soundata.top	application/octet-stream	11 MB	resources.dll
10144	www.msftconnecttest.com	text/plain	22 bytes	connecttest.txt

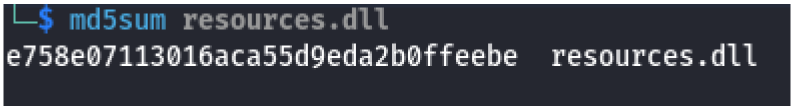
Q5. Answer: **.dll**

Q6. What is the MD5 has of the second malicious file?

Approach: As previously state the purpose of gaining hash information is beneficial to analyst because it provides a multitude of information regarding the type of malicious file we are dealing with, its behavior and how it compares to other files found using VirusTotal.

Step 1: We navigate to the file tab in Wireshark and export the object called, "**resources.dll**". This process is similar to what we did with the "**login.php**" file. We will change directories to where the export file is and check its MD5 hash using the following command.

md5sum resources.dll



```
└─$ md5sum resources.dll
e758e07113016aca55d9eda2b0ffeebe  resources.dll
```

Q6. Answer: **e758e07113016aca55d9eda2b0ffeebe**

Conclusion

After careful forensic analysis it was discovered that there was evidence of a breach in the network. Wireshark, a tool used to analyze network traffic was used to capture packets that were being sent from the attacker to the organization system. The attacker was able to gain access to a user with advanced privileges through a possible phishing campaign, in which the **Remote Access Trojan (RAT), DanaBot** was installed onto the machine. **DanaBot, a banking Trojan / RAT generally used with phishing campaigns, social engineering and malicious downloads. The RAT is able to communicate with Command-and-Control(C2) servers to forward malicious commands**.

The attacker was given remote access and control over the victim's machine after a file was installed on the endpoint which allowed them to run commands remotely from the attackers C&C. We were able to discover the attackers initial IP address (**62.173.142.14)** and the files in which they uploaded into the compromised endpoint (**allgato_708.js, resources.dll**). Utilizing our Kali Linux machine, we were able to discover the SHA256 hash for the exported file named **Login.php (**as well as that MD5 has for **resources.dll)** and compare it to VirusTotal's database of malwares.

VirusTotal validated that the file was indeed a trojan of the **acsogenixx/sload** family, a type of malware associated with cybercrime campaigns, often used to facilitate further attacks on infected systems. It is known to distribute through malicious Microsoft Word documents or malicious email attachments. The file opens a key registry (**HKEY_CURRENT_USER**) in the Windows OS which contains configuration settings and preferences specific to the currently logged-in user. The malware misused **wscript.exe** , a legitimate **Windows Script Host (WSH)** which is the executable used to run script files in the Windows OS. This allowed the attacker to upload the **resources.dll** file and steal sensitive data.

Tactics, Techniques and Procedures (TTPs)

1. Initial Access

-**Tactic**: Gaining initial access to the target system.

-**Techniques**:

- **Phishing**: Attackers use malicious email attachments or links to trick the user into downloading and running the malware.

2. Execution

-**Tactic**: Execution of malicious code to install the malware.

-**Techniques**:

- **Malicious Attachments**: The malware is delivered as an attachment (script / executable file). It is executed when the user opens it.
- **Exploitation of Vulnerabilities**: The malware exploits unpatched vulnerabilities in the system to gain execution.

3. Persistence

-**Tactic**: Ensuring the malware remains active after reboots and system changes.

-**Techniques**:

- **Registry Modifications**: The malware adds or modify registry keys to ensure it runs on system start up.
- **Scheduled Tasks**: Scheduled task can be created by the malware to run at specific intervals, ensuring continuous execution.

4. Privilege Escalation

-**Tactic**: Elevating privileges to gain greater access to the system.

- **Techniques**:

- **Credential Dumping**: The malware can dump user credentials from the system to escalate privileges and move laterally across the network.

5. Defense Evasion

-**Tactic**: Avoiding detection by security software and system defenses

-**Techniques**:

- **Obfuscation**: The malware uses various obfuscation techniques to hide presence and avoid detection by antivirus or security tools.

6. Credential Access

-**Tactic**: Collecting user credentials to access sensitive information.

-**Techniques**:

- **Keylogging**: The malware can include a keylogger to record keystrokes, capturing sensitive information such as passwords and user name.
- **Credential Dumping**: Extracts stored credentials from the system, potentially allowing attackers to gain unauthorized access to other systems.

7. Lateral Movement

- **Tactic**: Moving within the network to gain access to additional systems or resources.

-**Techniques**:

- **Remote Services**: The malware is capable of exploiting compromised credentials to move laterally via services like RDP (Remote Desktop Protocol) or SMB (Server Message Block)

8. Collection

-**Tactic**: Collecting valuable data for exfiltration or exploitation.

-Techniques:

- **Data Staged**: The malware collects sensitive information and stage it for later exfiltration.

9. Exfiltration

-Tactic: Sending stolen data from the target system to an external attack-controlled location.

-Techniques:

- **Exfiltration Over Command-and-Control Channel**: The collected data is transmitted back to the attacker's command and control (C2) server using encrypted or obfuscated channels to avoid detection.

Mitigation

There are several methods in which we can prevent attacks and others similar to this:

- **User Education**: Training users to avoid phishing scams.
- **Patch Management**: Regularly update and patching vulnerabilities as soon as they are available.
- **Endpoint Protection**: Use strong antivirus and EDR solutions.
- **Network Segmentation**: Limit lateral movement by dividing networks.
- **Access Controls**: Enforce least privilege and multi-factor authentication (MFA).
- **Incident Response**: Develop and maintain and incident response plan.
- **Compliance**: Use compliance / security frameworks such as (NIST, SOC 2) to create a base line to prepare and prevent future incidents. These frameworks can also act as baselines to handling incident responses (e.g., NIST SP 800-61 Rev.2).
- **Convert HTTP to HTTPS**: changing the protocol from HTTP to HTTPS can help secure the information being forwarded and not being transferred in plain text.
- **Restrict File Types and Implement Sanitization**: Block or filter unsafe file types (e.g., .js, .exe and etc.)
- **Implement Content Security Policy (CSP)**: limit where scripts can be loaded from and what resources can be executed on sites / networks.

Reference

CyberDefenders. (2024, September 30). *DanaBot*. CyberDefenders. https://cyberdefenders.org/blueteam-ctf-challenges/danabot/

Wireshark. (2019). *Chapter 1. Introduction*. Wireshark.org. https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html#ChIntroWhatIs

a.bespalova. (2020, October 29). *How to Use a Malware Sandbox*. ANY.RUN Blog. https://any.run/cybersecurity-blog/how-to-use-anyrun/

What is Kali Linux? | Kali Linux Documentation. (2023, November 4). Kali.org. https://www.kali.org/docs/introduction/what-is-kali-linux/