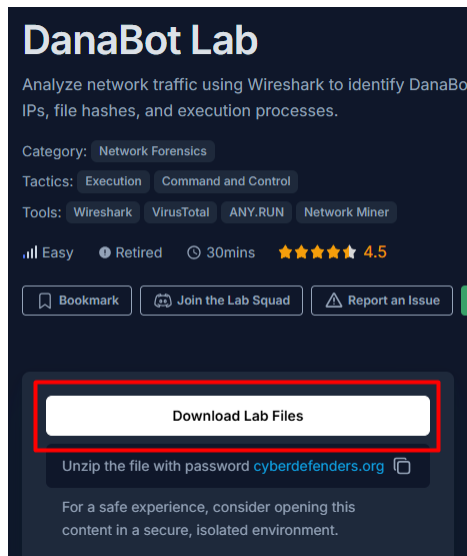


Reference: <https://cyberdefenders.org/blueteam-ctf-challenges/danabot/#>

Download the PCAP from the above link



In Linux with tcpdump

```
saf-1x@Saf-Ubuntu:~/Desktop/CyberDefenders/temp_extract_dir/temp_extract_dir$ tcpdump -tttt -r 205-DanaBot.pcap --count
reading from file 205-DanaBot.pcap, link-type EN10MB (Ethernet), snapshot length 65535
13900 packets
saf-1x@Saf-Ubuntu:~/Desktop/CyberDefenders/temp_extract_dir/temp_extract_dir$

saf-1x@Saf-Ubuntu:~/Desktop/CyberDefenders/temp_extract_dir/temp_extract_dir$ tcpdump -tttt -r 205-DanaBot.pcap -n | awk '{print $4}' | cut -d "." -f 1-4 | sort | uniq -c | sort -nr
reading from file 205-DanaBot.pcap, link-type EN10MB (Ethernet), snapshot length 65535
 8831 188.114.97.3
 2735 10.2.14.101
 839 10.2.14.101
 520 142.250.186.36
 157 91.201.67.85
 113 13.107.21.239
 108 40.83.50.91
 81 204.79.197.203
 77 23.3.88.139
 61 10.2.14.1
 52 23.3.88.147
 49 23.0.174.88
 41 142.250.186.110
 28 51.104.15.253
 24 13.107.6.158
 16 20.19.31.115
 15 51.104.176.40
 14 52.182.143.209
 14 52.182.143.208
 14 20.103.180.120
 13 142.250.186.177
 11 94.245.104.56
 11 2.21.22.176
 10 13.107.246.60
 8 Reply
 8 62.173.142.148
 7 52.168.112.66
 7 40.79.167.8
 7 20.42.65.89
 7 20.189.173.10
 7 13.89.170.27
```

Source side

```

saf-lx8Saf-Ubuntu: ~/Desktop/CyberDefenders/temp_extract_dir/temp_extract_dir$ tcpdump -tttt -r 205-DanaBot.pcap -n | awk '{print $6}' | cut -d "." -f 1-4 | sort | uniq -c | sort -nr
reading from file 205-DanaBot.pcap, link-type EN10MB (Ethernet), snapshot length 65535
11154 10.2.14.101
880 188.114.97.3
740 195.133.88.98
282 142.250.186.36
150 91.201.67.85
133 10.2.14.1
86 13.107.21.239
56 40.83.50.91
48 204.79.197.203
46 23.3.88.139
32 23.0.174.88
25 51.104.15.253
25 142.250.186.110
24 23.3.88.147
20 20.10.31.115
17 13.107.6.158
12 52.102.143.209
12 52.102.143.208
10 51.104.176.40
10 239.255.255.250
10 224.0.0.22
10 2.21.22.176
10 20.103.180.120

```

## Destination side

```

saf-lx8Saf-Ubuntu: ~/Desktop/CyberDefenders/temp_extract_dir/temp_extract_dir$ tcpdump -tttt -r 205-DanaBot.pcap -n src 10.2.14.101 -A | grep "GET"
reading from file 205-DanaBot.pcap, link-type EN10MB (Ethernet), snapshot length 65535
2024-02-14 18:25:54.190791 IP 10.2.14.101.49786 > 62.173.142.148.80: Flags [P.], seq 0:460, ack 1, win 64240, length 460: HTTP: GET /login.php HTTP/1.1
..e>...z.P.U=f...P...w..GET /login.php HTTP/1.1
2024-02-14 18:26:50.967599 IP 10.2.14.101.49798 > 192.229.221.95.80: Flags [P.], seq 0:240, ack 1, win 64240, length 240: HTTP: GET /MFewTzBNMEswSTA3BgUrDgMCGGUABQ50otxk2Fh0ztLk2Bz85IPi7wEw
VxDLQUTL3UIB1V5uNu5gK2F6x2BrK57QVXjzkCEAUZZSZEml49Gjh0j13P68wK3D HTTP/1.1
..e>...P...b..yP.....GET /MFewTzBNMEswSTA3BgUrDgMCGGUABQ50otxk2Fh0ztLk2Bz85IPi7wEwVxDLQUTL3UIB1V5uNu5gK2F6x2BrK57QVXjzkCEAUZZSZEml49Gjh0j13P68wK3D HTTP/1.1
2024-02-14 18:26:55.684412 IP 10.2.14.101.49799 > 188.114.97.3.80: Flags [P.], seq 0:266, ack 1, win 65535, length 266: HTTP: GET /resources.dll HTTP/1.1
..e>...P...z1.8.P.....GET /resources.dll HTTP/1.1
2024-02-14 18:28:44.239052 IP 10.2.14.101.49803 > 23.10.249.35.80: Flags [P.], seq 0:111, ack 1, win 64240, length 111: HTTP: GET /connecttest.txt HTTP/1.1
0P...e>...GET /connecttest.txt HTTP/1.1

```

## Suspicious IP address.

1

/95

Community Score

1/95 security vendor flagged this IP address as malicious

62.173.142.148 (62.173.128.0/19)

AS 34300 (Internet-Cosmos LLC)

RU

Last Analysis Date

21 hours ago

DETECTION

DETAILS

RELATIONS

COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Basic Properties

Network	62.173.128.0/19
Autonomous System Number	34300
Autonomous System Label	Internet-Cosmos LLC
Regional Internet Registry	RIPE NCC
Country	RU
Continent	EU

Last HTTPS Certificate

JARM Fingerprint

IP address was used by the attacker during the initial access.

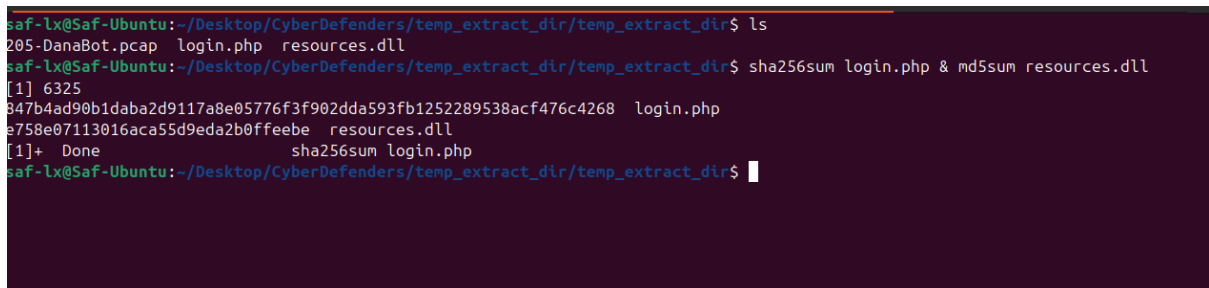
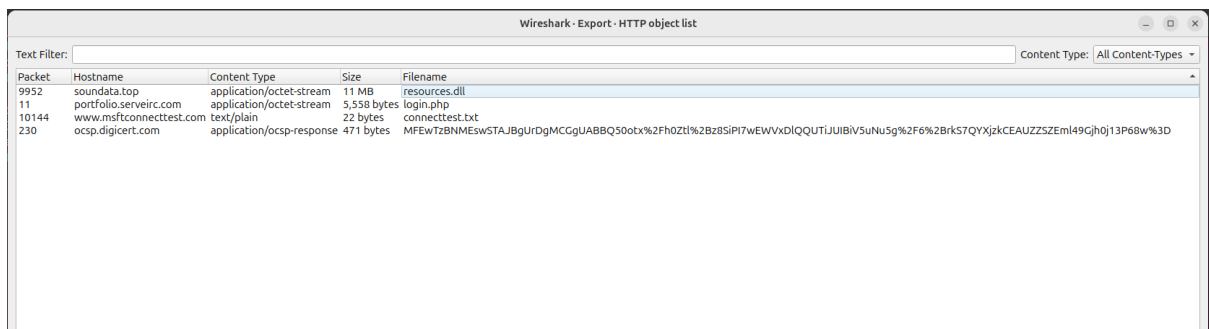
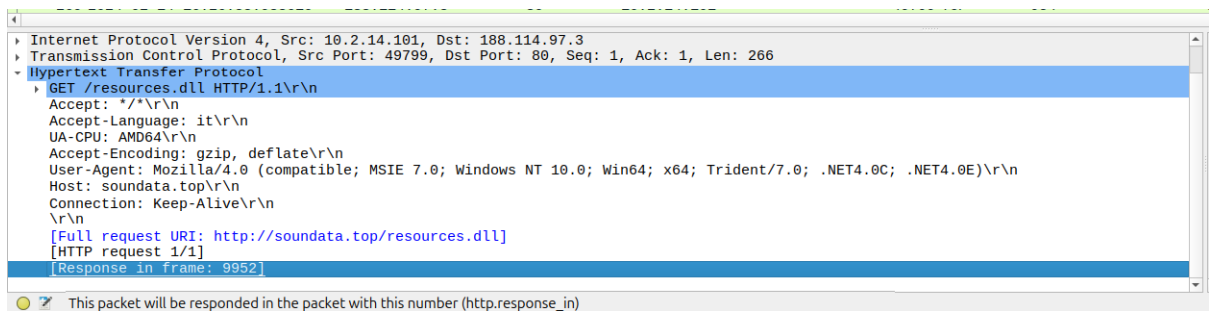
```

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/webp,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_768.js

```

Name of the malicious file used for initial access



Hashes of malicious file.

Javascript obfuscated script, most likely string array. It is clear that it uses the LOLbin wscript.exe to execute a malicious file. Process was used to execute the malicious file.

