CyberDefenders: DanaBot Lab

The following writeup is for DanaBot on CyberDefenders, it involves investigating a pcap file.

Scenario: Our SOC team detected suspicious activity in the network traffic. A machine has been compromised, and company information that should not have been there has now been stolen. It's up to you to determine what happened and what data was taken.

What is the malicious file name used for initial access?

Start off by extracting the zip file and opening the pcap file in Wireshark. I started off by navigating to Statistics > Protocol hierarchy to get an understanding of what packets were captured:

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	13900	100.0	15010280	82 k	0	0	0	13900
Ethernet	100.0	13900	1.3	194600	1063	0	0	0	13900
Internet Protocol Version 4	99.9	13889	1.9	277820	1518	0	0	0	13889
User Datagram Protocol	1.9	268	0.0	2144	11	0	0	0	268
Simple Service Discovery Protocol	0.1	10	0.0	1526	8	10	1526	8	10
QUIC IETF	0.5	64	0.2	35139	192	64	34970	191	65
NetBIOS Name Service	0.3	39	0.0	2652	14	39	2652	14	39
NetBIOS Datagram Service	0.0	2	0.0	402	2	0	0	0	2
SMB (Server Message Block Protocol)	0.0	2	0.0	238	1	0	0	0	2
SMB MailSlot Protocol	0.0	2	0.0	50	0	0	0	0	2
Microsoft Windows Browser Protocol	0.0	2	0.0	66	0	2	66	0	2
Multicast Domain Name System	0.1	7	0.0	296	1	7	296	1	7
Link-local Multicast Name Resolution	0.0	2	0.0	66	0	2	66	0	2
Domain Name System	1.0	144	0.1	20420	111	144	20420	111	144
Transmission Control Protocol	97.9	13611	96.4	14474821	79 k	12638	13473570	73 k	13611
Transport Layer Security	6.8	940	15.0	2256718	12 k	940	1993311	10 k	1005
Hypertext Transfer Protocol	0.1	8	79.5	11930909	65 k	4	1077	5	8
Online Certificate Status Protocol	0.0	1	0.0	471	2	1	471	2	1
Line-based text data	0.0	1	0.0	22	0	1	22	0	1
Data	0.0	2	79.5	11927990	65 k	2	11927990	65 k	2
Data	0.2	25	0.0	4402	24	25	4402	24	25
Internet Group Management Protocol	0.1	10	0.0	160	0	10	160	0	10
Address Resolution Protocol	0.1	11	0.0	308	1	11	308	1	11

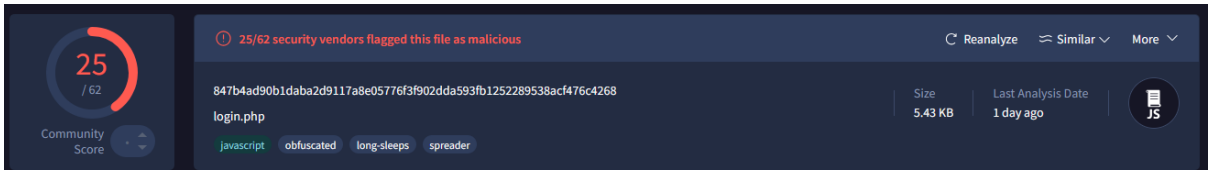
I started by looking at HTTP requests, specifically GET requests to see what the user was accessing:

Source	Destination	Destination Port	Protocol	Host	User-Agent	Info
10.2.14.101	62.173.142.148	80	HTTP	portfolio.s…	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko…	GET /login.php HTTP/1.1
10.2.14.101	192.229.221.95	80	HTTP	ocsp.digice…	Microsoft-CryptoAPI/10.0	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUA
10.2.14.101	188.114.97.3	80	HTTP	soundata.top	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .N…	GET /resources.dll HTTP/1.1
10.2.14.101	23.10.249.35	80	HTTP	www.msftcon…	Microsoft NCSI	GET /connecttest.txt HTTP/1.1

Both resources.dll and login.php appear to be interesting. If we select the GET request to /login.php and right click > Follow TCP stream, we can find the name of the file used for initial access:

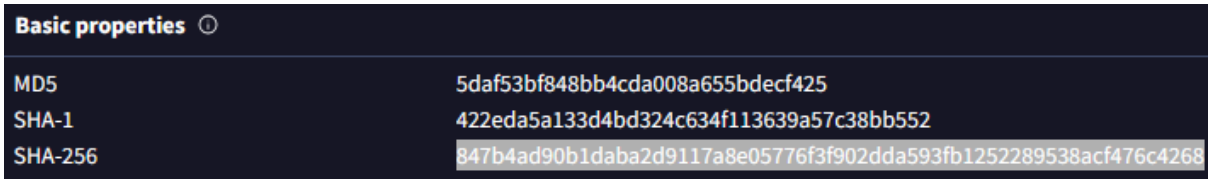
```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Wed, 14 Feb 2024 16:25:54 GMT
Content-Type: application/octet-stream
Transfer-Encoding: chunked
Connection: keep-alive
Content-disposition: attachment;filename=allegato_708.js
```

To verify that the file is malicious, you can also go to File > Export Objects > HTTP, download the file in a sandboxed environment, and check it on VirusTotal:



What is the sha256 hash of the file used for initial access?

We can find the sha256 hash of the file found previously in VirusTotal:



Alternatively, you can use the Get-FileHash cmdlet:

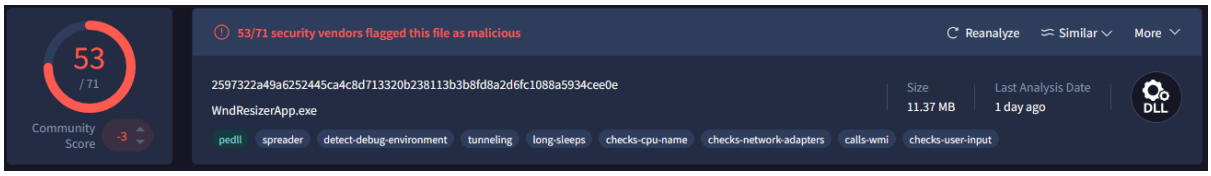
```
PS C:\Users\timba\Downloads> Get-FileHash -Algorithm SHA256 .\login.php

Algorithm       Hash
---------       ----
SHA256          847B4AD90B1DABA2D9117A8E05776F3F902DDA593FB1252289538ACF476C4268
```

What is the process used to execute the malicious file?

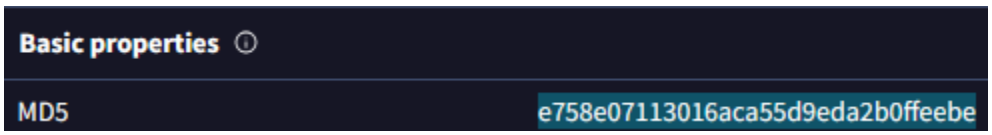
Based on the behaviour section in VirusTotal, we can determine that wscript.exe was used to execute the malware. Windows Script (wscript) enables users to execute scripts in various languages.

What is the extension of the second malicious file used by the attacker?

Previously, we found a .dll file that looked suspicious (resources.dll). After exporting this file and entering it in VirusTotal, it has 53 detections:



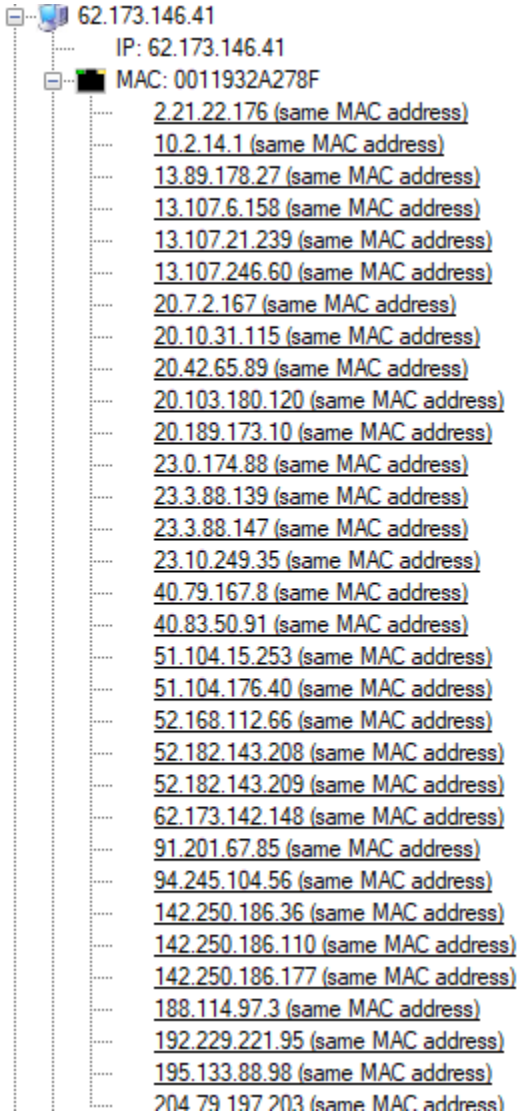
What is the MD5 hash of the second malicious file?



```
PS C:\Users\timba\Downloads> Get-FileHash -Algorithm MD5 .\resources.dll

Algorithm       Hash
---------       ----
MD5             E758E07113016ACA55D9EDA2B0FFEEBE
```

What is the IP address used by the attacker in initial access?

Using VirusTotal, we can determine the IP addressed used by the attacker in initial access to be 62.173.146.41. However, a better way to determine the attackers IP is to investigate the Hosts tab in NetworkMiner:



We can see that this IP address is spoofing a different MAC address.

What is the last malicious IP address in the PCAP that is known to be used as CnC by DanaBot?

Using the IP traffic section in VirusTotal (found in the behaviour tab) we can determine (by checking the presence of the IP addresses in the pcap) that 91.201.67.85 is the last malicious IP address in the PCAP.