DanaBot Lab

Created	@August 18, 2025 3:19 PM

Scenario

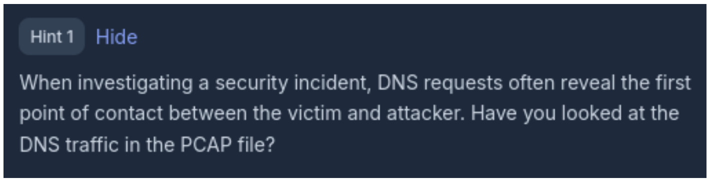
The SOC team has detected suspicious activity in the network traffic, revealing that a machine has been compromised. Sensitive company information has been stolen. Your task is to use Network Capture (PCAP) files and Threat Intelligence to investigate the incident and determine how the breach occurred.

Introduction

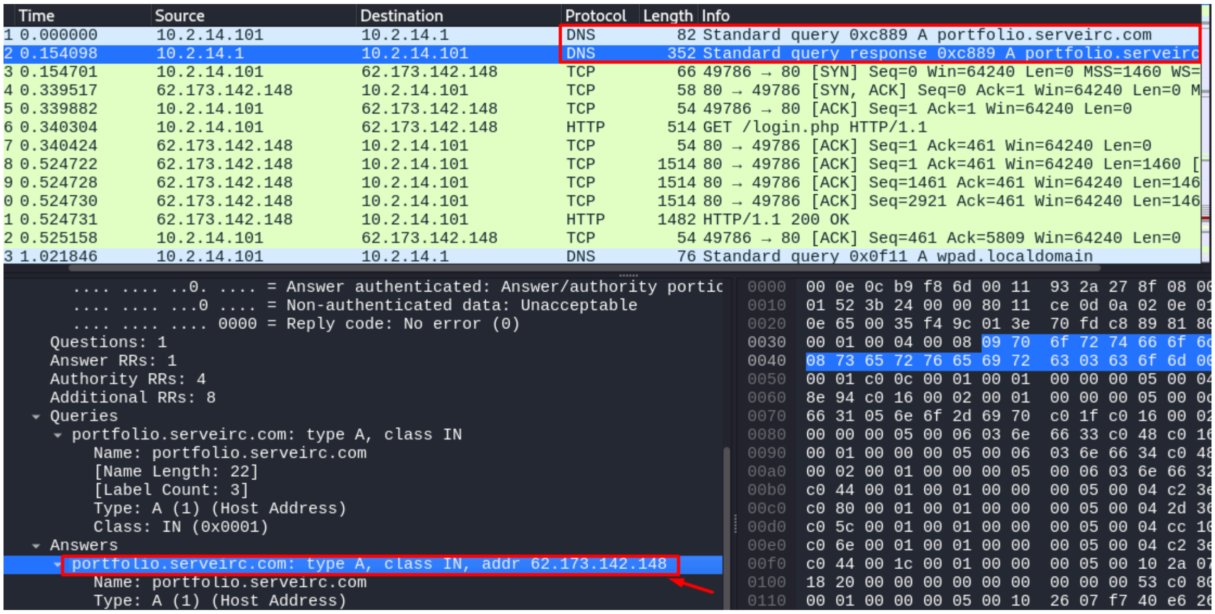
In this lab, we delve into a network forensics investigation to analyze a cyber attack involving the `Dana Bot` malware. The `SOC` (Security Operations Center) team has identified suspicious activity within network traffic, which reveals that a machine in the network has been compromised. This breach has led to the exfiltration of sensitive company data. As a cybersecurity analyst, your objective is to investigate the incident using a `PCAP` (Packet Capture) file and associated threat intelligence to uncover how the compromise occurred and to identify key details about the attack.The lab focuses on dissecting the tactics, techniques, and procedures (TTPs) used by the attacker,including reconnaissance, initial access, execution, and persistence. You will utilize `Wireshark` to extract and analyze critical network artifacts, such as malicious files and communication with external servers. By deobfuscating JavaScript code and examining related artifacts, you will uncover how the malware gained a foothold in the network, executed additional payloads, and maintained its presence. This lab provides a comprehensive opportunity to practice real-world forensic skills and gain deeper insights into detecting and responding to sophisticated malware attacks.

Initial Analysis

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



When investigating a security incident, DNS requests often reveal the first point of contact between the victim and attacker. Have you looked at the DNS traffic in the PCAP file?

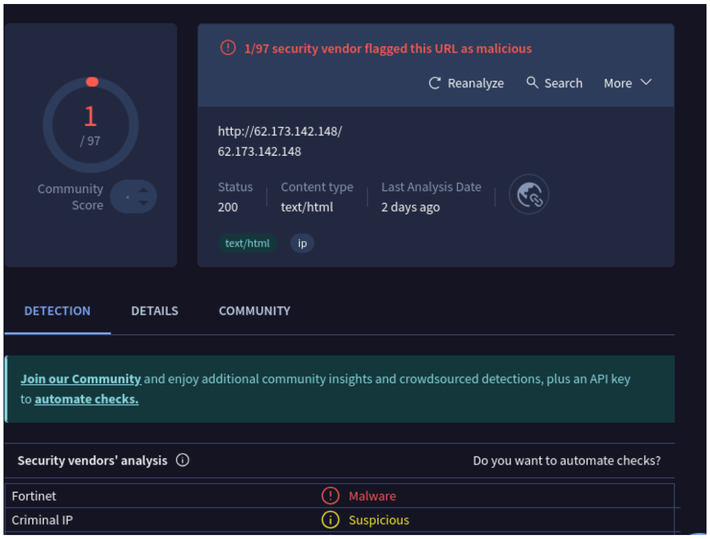


```
  Time       Source          Destination      Protocol Length Info
1 0.000000   10.2.14.101     10.2.14.1        DNS        82 Standard query 0xc889 A portfolio.serveirc.com
2 0.154098   10.2.14.1       10.2.14.101      DNS       352 Standard query response 0xc889 A portfolio.serveirc
3 0.154701   10.2.14.101     62.173.142.148   TCP        66 49786 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=
4 0.339517   62.173.142.148  10.2.14.101      TCP        58 80 → 49786 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M
5 0.339882   10.2.14.101     62.173.142.148   TCP        54 49786 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
6 0.340304   10.2.14.101     62.173.142.148   HTTP      514 GET /login.php HTTP/1.1
7 0.340424   62.173.142.148  10.2.14.101      TCP        54 80 → 49786 [ACK] Seq=1 Ack=461 Win=64240 Len=0
8 0.524722   62.173.142.148  10.2.14.101      TCP      1514 80 → 49786 [ACK] Seq=1 Ack=461 Win=64240 Len=1460 [
9 0.524728   62.173.142.148  10.2.14.101      TCP      1514 80 → 49786 [ACK] Seq=1461 Ack=461 Win=64240 Len=146
0 0.524730   62.173.142.148  10.2.14.101      TCP      1514 80 → 49786 [ACK] Seq=2921 Ack=461 Win=64240 Len=146
1 0.524731   62.173.142.148  10.2.14.101      HTTP     1482 HTTP/1.1 200 OK
2 0.525158   10.2.14.101     62.173.142.148   TCP        54 49786 → 80 [ACK] Seq=461 Ack=5809 Win=64240 Len=0
3 1.021846   10.2.14.101     10.2.14.1        DNS        76 Standard query 0x0f11 A wpad.localdomain
```

```
    .... .... ..0. .... = Answer authenticated: Answer/authority portic
    .... .... ...0 .... = Non-authenticated data: Unacceptable
    .... .... .... 0000 = Reply code: No error (0)
  Questions: 1
  Answer RRs: 1
  Authority RRs: 4
  Additional RRs: 8
▾ Queries
  ▾ portfolio.serveirc.com: type A, class IN
      Name: portfolio.serveirc.com
      [Name Length: 22]
      [Label Count: 3]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
▾ Answers
  ▾ portfolio.serveirc.com: type A, class IN, addr 62.173.142.148
      Name: portfolio.serveirc.com
      Type: A (1) (Host Address)
```

```
0000  00 0e 0c b9 f8 6d 00 11  93 2a 27 8f 08 00
0010  01 52 3b 24 00 00 80 11  ce 0d 0a 02 0e 01
0020  0e 65 00 35 f4 9c 01 3e  70 fd c8 89 81 80
0030  00 01 00 04 00 08 09 70  6f 72 74 66 6f 6c
0040  08 73 65 72 76 65 69 72  63 03 63 6f 6d 00
0050  00 01 c0 0c 00 01 00 01  00 00 00 05 00 04
0060  8e 94 c0 16 00 02 00 01  00 00 00 05 00 0c
0070  66 31 05 6e 6f 2d 69 70  c0 1f c0 16 00 02
0080  00 00 00 05 00 06 03 6e  66 33 c0 48 c0 16
0090  00 01 00 00 00 05 00 06  03 6e 66 34 c0 48
00a0  00 02 00 01 00 00 00 05  00 06 03 6e 66 32
00b0  c0 44 00 01 00 01 00 00  00 05 00 04 c2 3e
00c0  c0 80 00 01 00 01 00 00  00 05 00 04 2d 36
00d0  c0 5c 00 01 00 01 00 00  00 05 00 04 cc 10
00e0  c0 6e 00 01 00 01 00 00  00 05 00 04 c2 3e
00f0  c0 44 00 1c 00 01 00 00  00 05 00 10 2a 07
0100  18 20 00 00 00 00 00 00  00 00 00 53 c0 80
0110  00 01 00 00 00 05 00 10  26 07 f7 40 e6 26
```

By analyzing the PCAP file, we see a DNS request made to `portfolio.serveirc.com`.In fact paste dns ip into Virustotal to verifies if its a malicious vendor



1/97 security vendor flagged this URL as malicious

http://62.173.142.148/
62.173.142.148

Status: 200
Content type: text/html
Last Analysis Date: 2 days ago

text/html ip

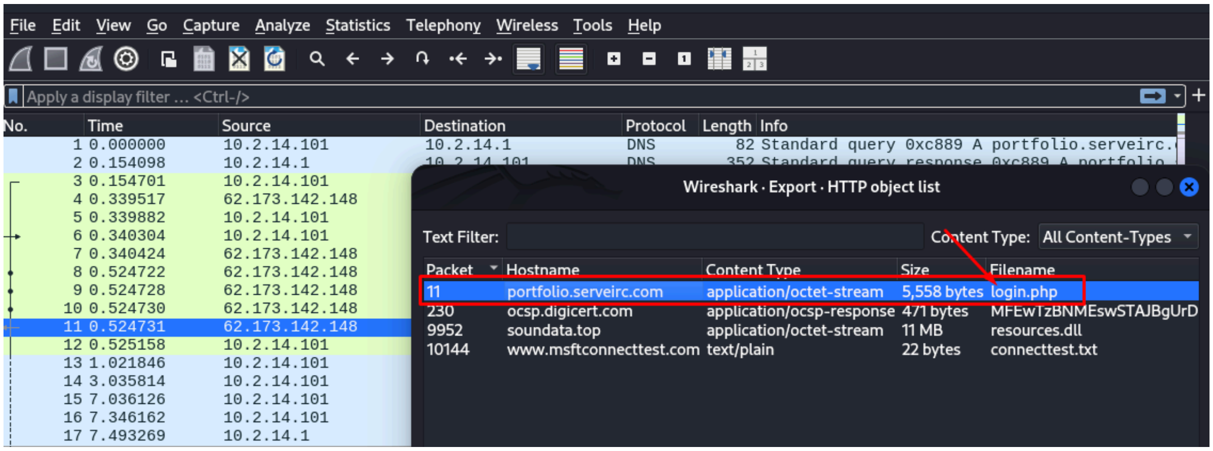
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

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

Fortinet	Malware
Criminal IP	Suspicious

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

To begin investigating the incident involving the Dana Bot malware, we start by analyzing the network capture file using Wireshark. The main goal is to identify the malicious file used for initial access. We first start by examining the files in Wireshark's HTTP object export feature. This is accessible by navigating to `File → Export Objects → HTTP`.



```
No.   Time      Source          Destination   Protocol Length Info
    1 0.000000  10.2.14.101     10.2.14.1     DNS          82 Standard query 0xc889 A portfolio.serveirc.
    2 0.154098  10.2.14.1       10.2.14.101   DNS         352 Standard query response 0xc889 A portfolio.
    3 0.154701  10.2.14.101
    4 0.339517  62.173.142.148
    5 0.339882  10.2.14.101
    6 0.340304  10.2.14.101
    7 0.340424  62.173.142.148
    8 0.524722  62.173.142.148
    9 0.524728  62.173.142.148
   10 0.524730  62.173.142.148
   11 0.524731  62.173.142.148
   12 0.525158  10.2.14.101
   13 1.021846  10.2.14.101
   14 3.035814  10.2.14.101
   15 7.036126  10.2.14.101
   16 7.346162  10.2.14.101
   17 7.493269  10.2.14.1
```

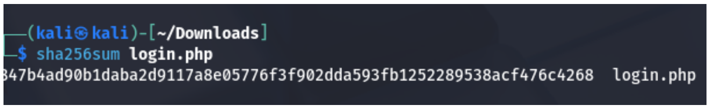
Wireshark · Export · HTTP object list

Text Filter:

Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
11	portfolio.serveirc.com	application/octet-stream	5,558 bytes	login.php
230	ocsp.digicert.com	application/ocsp-response	471 bytes	MFEwTzBNMEswSTAJBgUrD
9952	soundata.top	application/octet-stream	11 MB	resources.dll
10144	www.msftconnecttest.com	text/plain	22 bytes	connecttest.txt

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

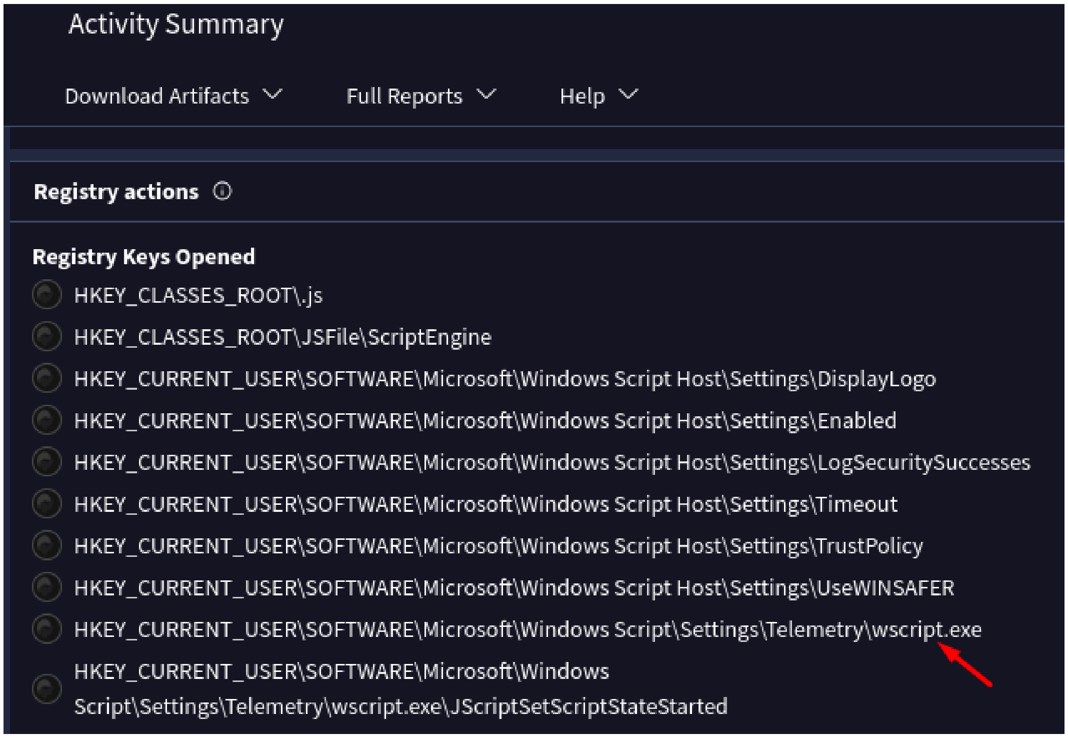


```
┌──(kali㉿kali)-[~/Downloads]
└─$ sha256sum login.php
347b4ad90b1daba2d9117a8e05776f3f902dda593fb1252289538acf476c4268  login.php
```

The SHA-256 hash of the malicious file used for initial access can be computed using the following bash command.

```
sha256sum login.php
```

Resulting in the hashvalue: `847b4ad90b1bda2d9117ae05776f3f902dda593fb15222895938acf476c4268`.
Use this filehash to check in VirusTotal: Click on Behaviour and scroll down to registry actions section



Registry actions

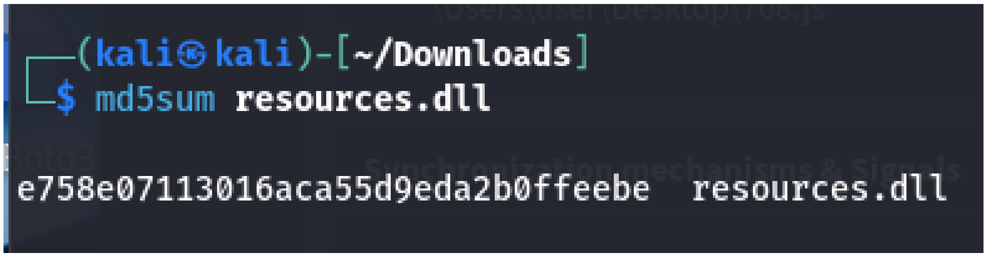
Registry Keys Opened

- 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

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

As can be seen from the previous analysis, the second file which was downloaded by the obfuscated script is `resources.dll` and has a `.dll` extension

Q6 What is the MD5 hash of the second malicious file?



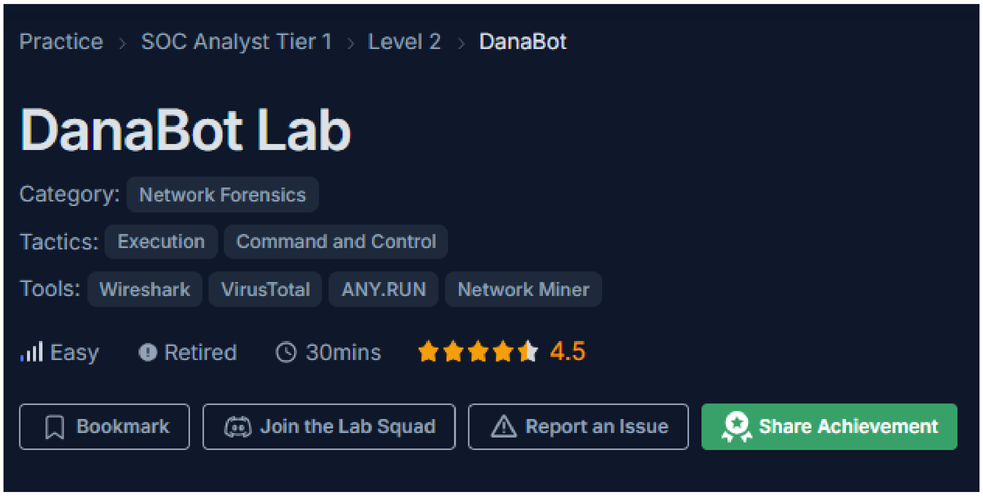
```
┌──(kali㉿kali)-[~/Downloads]
└─$ md5sum resources.dll

e758e07113016aca55d9eda2b0ffeebe  resources.dll
```

extract file from wireshark then use command md5sum t

Conclusion

This is one of a very useful Challenge that I get to refresh my skills using Wireshark tool pcap analysis, Hashing understanding and Virustotal Research in findings IoCs.

Simply the website was already infected with trojan to spread to other devices.



Practice › SOC Analyst Tier 1 › Level 2 › DanaBot

DanaBot Lab

Category: Network Forensics

Tactics: Execution Command and Control

Tools: Wireshark VirusTotal ANY.RUN Network Miner

Easy Retired 30mins ★★★★★ 4.5