Challenge Writeup: Warzone 2

This writeup details the approach to solving the Warzone 2 challenge hosted on TryHackMe. This room involves the use of various network forensics tools, including Brim, Wireshark, and NetworkMiner, to analyse a PCAP file.

Scenario: You work as a Tier 1 Security Analyst L1 for a Managed Security Service Provider (MSSP). Again, you're tasked with monitoring network alerts. An Alert triggered: Misc Activity, A Network Trojan was Detected, and Potential Corporate Privacy Violation. The case was assigned to you. Inspect the PCAP and retrieve the artifacts to confirm this alert is a true positive.

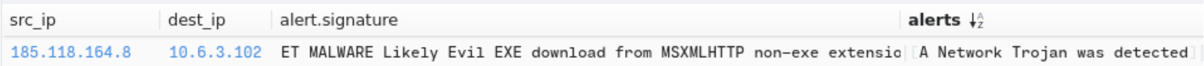
Your tools:

- Brim
- Network Miner
- Wireshark

What was the alert signature for a Network Trojan Was Detected?

We are able to find the alert signature for A Network Trojan Was Detected through using Brim and investigating the Suricata alerts. We can use the following query to do this:

- event_type=="alert" | alerts := union(alert.category) by src_ip, dest_ip, alert.signature | sort alerts

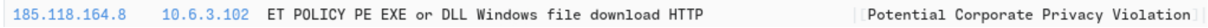


src_ip	dest_ip	alert.signature	alerts
185.118.164.8	10.6.3.102	ET MALWARE Likely Evil EXE download from MSXMLHTTP non-exe extensio	[A Network Trojan was detected]

The text in the alert.signature field is the answer. Note, I simply modified the predefined Suricata Alerts by Source and Destination query to include the alert.signature column.

What was the alert signature for Potential Corporate Privacy Violation?

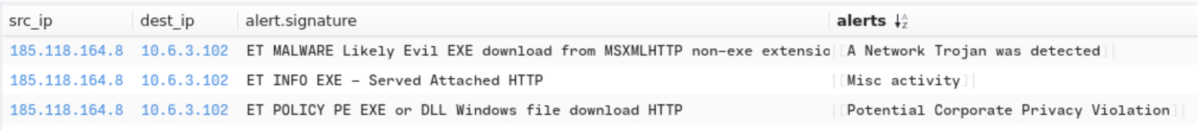
The query entered previously allows us to find this alert produced by Suricata along with its alert signature:



185.118.164.8	10.6.3.102	ET POLICY PE EXE or DLL Windows file download HTTP	[Potential Corporate Privacy Violation]

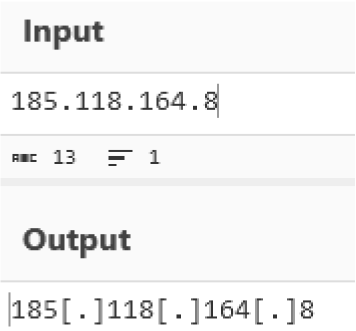
What was the IP to trigger either alert? Enter your answer in a defanged format.

As can be seen in the query used for question 1 and 2, the source IP address for both triggered alerts are 185.118.164.8:



src_ip	dest_ip	alert.signature	alerts
185.118.164.8	10.6.3.102	ET MALWARE Likely Evil EXE download from MSXMLHTTP non-exe extensio	[A Network Trojan was detected]
185.118.164.8	10.6.3.102	ET INFO EXE - Served Attached HTTP	[Misc activity]
185.118.164.8	10.6.3.102	ET POLICY PE EXE or DLL Windows file download HTTP	[Potential Corporate Privacy Violation]

We can use cyberchef in conjunction with the Defang IP Addresses recipe to defang the IP address like as follows:



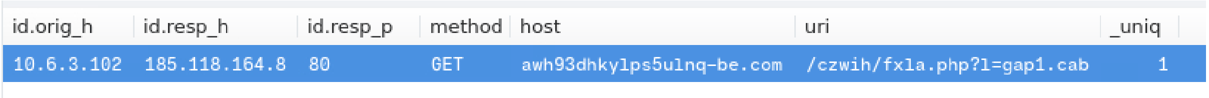
```
185.118.164.8
```

```
185[.]118[.]164[.]8
```

Provide the full URI for the malicious downloaded file. In your answer, defang the URI.

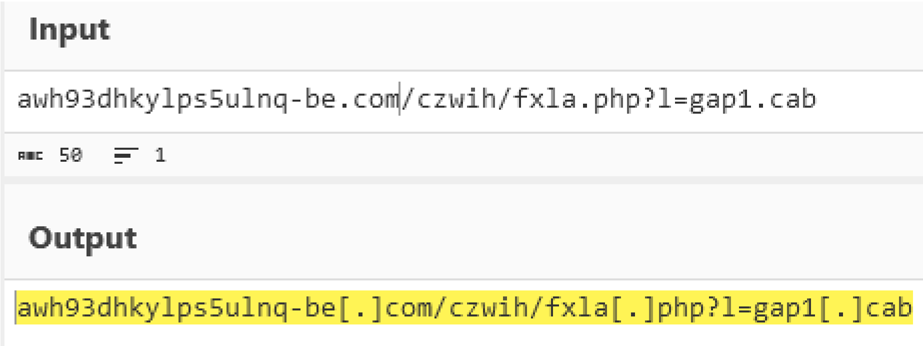
The Suricata alert generated for the malicious download indicates that the source of the alert (where the file was downloaded) is 185.118.164.8. Therefore, to identify the full URI for the malicious downloaded file, I used the following query:

- _path=="http" 185.118.164.8 | cut id.orig_h, id.resp_h, id.resp_p, method,host, uri | uniq -c



id.orig_h	id.resp_h	id.resp_p	method	host	uri	_uniq
10.6.3.102	185.118.164.8	80	GET	awh93dhkylps5ulnq-be.com	/czwih/fxla.php?l=gap1.cab	1

Then, all we need to do is navigate back to cyberchef and use the Defang URL recipe like as follows:

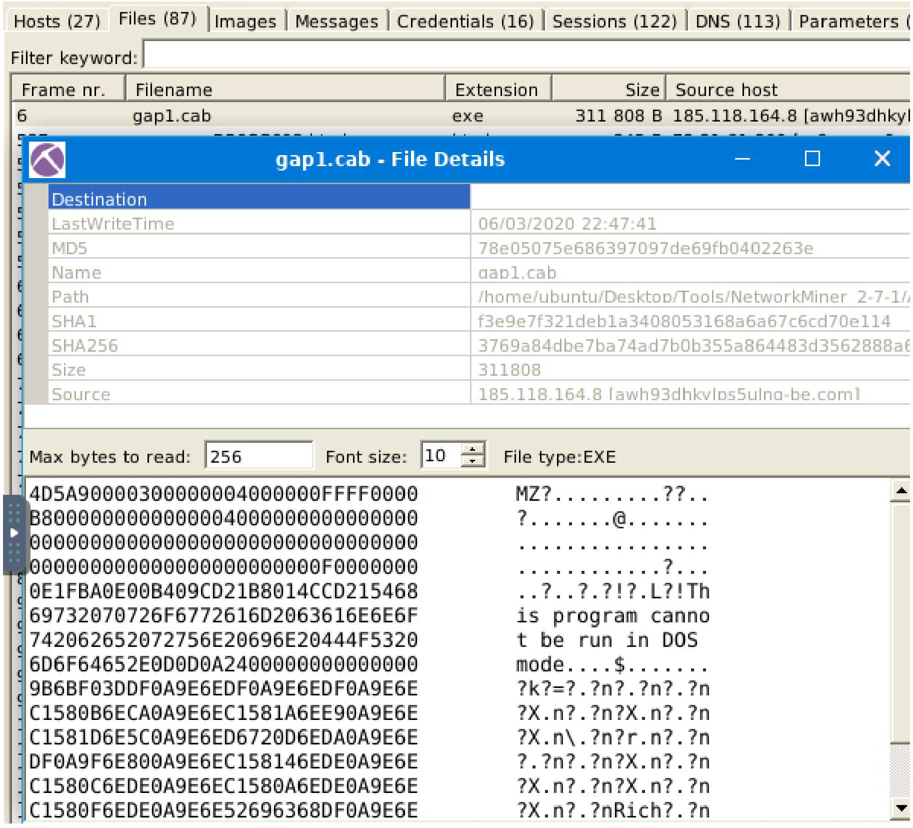


```
awh93dhkylps5ulnq-be.com/czwih/fxla.php?l=gap1.cab
```

```
awh93dhkylps5ulnq-be[.]com/czwih/fxla[.]php?l=gap1[.]cab
```

What is the name of the payload within the cab file?

To find the name of the payload file, we first need to get a hash of the file and search it in VirusTotal as directed to in the hint. To do this, I am going to use NetworkMiner and navigate to the file section:



Filter keyword:

Frame nr.	Filename	Extension	Size	Source host
6	gap1.cab	exe	311 808 B	185.118.164.8 [awh93dhkyl

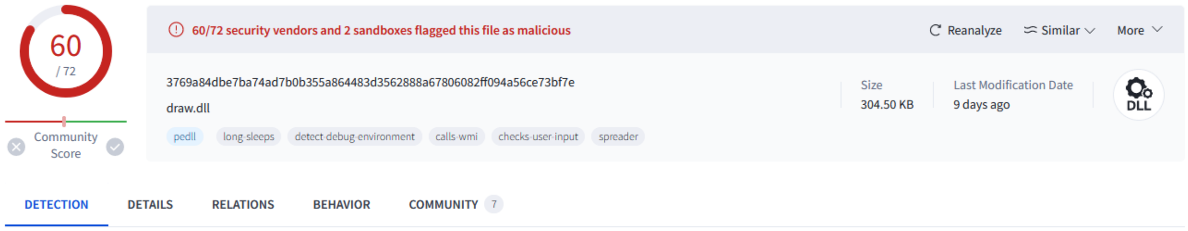
gap1.cab - File Details

Destination	
LastWriteTime	06/03/2020 22:47:41
MD5	78e05075e686397097de69fb0402263e
Name	gap1.cab
Path	/home/ubuntu/Desktop/Tools/NetworkMiner_2-7-1/
SHA1	f3e9e7f321deb1a3408053168a6a67c6cd70e114
SHA256	3769a84dbe7ba74ad7b0b355a864483d3562888a6
Size	311808
Source	185.118.164.8 [awh93dhkylps5ulnq-be.com]

Max bytes to read: 256 Font size: 10 File type:EXE

```
4D5A90000300000004000000FFFF0000    MZ?.........??..
B8000000000000004000000000000000    ?.......@.......
00000000000000000000000000000000    ................
000000000000000000000000F0000000    ............?...
0E1FBA0E00B409CD21B8014CCD215468    ..?..?.?!?.L?!Th
69732070726F6772616D2063616E6E6F    is program canno
742062652072756E20696E20444F5320    t be run in DOS 
6D6F64652E0D0D0A2400000000000000    mode....$.......
9B6BF03DDF0A9E6EDF0A9E6EDF0A9E6E    ?k?=?.?n?.?n?.?n
C1580B6ECA0A9E6EC1581A6EE90A9E6E    ?X.n?.?n?X.n?.?n
C1581D6E5C0A9E6ED6720D6EDA0A9E6E    ?X.n\.?n?r.n?.?n
DF0A9F6E800A9E6EC158146EDE0A9E6E    ?.?n?.?n?X.n?.?n
C1580C6EDE0A9E6EC1580A6EDE0A9E6E    ?X.n?.?n?X.n?.?n
C1580F6EDE0A9E6E52696368DF0A9E6E    ?X.n?.?nRich?.?n
```

Here we can find the file and its corresponding hash (in this case I will use the SHA256 hash). Let's now enter it into VirusTotal:



60/72 security vendors and 2 sandboxes flagged this file as malicious

3769a84dbe7ba74ad7b0b355a864483d3562888a67806082ff094a56ce73bf7e

draw.dll

pedll long-sleeps detect-debug-environment calls-wmi checks-user-input spreader

Size 304.50 KB

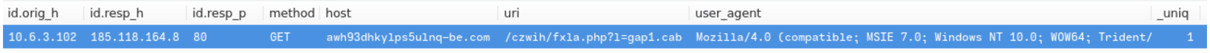
Last Modification Date 9 days ago

draw.dll is the answer.

What is the user-agent associated with this network traffic?

To find the user-agent associated with this traffic I simply included the user_agent field to the http query used earlier:

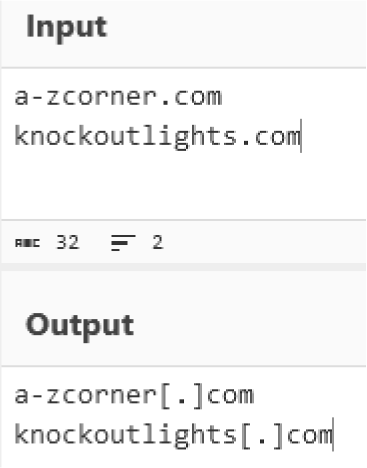
- _path=="http" 185.118.164.8 | cut id.orig_h, id.resp_h, id.resp_p, method,host, uri, user_agent | uniq -c



id.orig_h	id.resp_h	id.resp_p	method	host	uri	user_agent	_uniq
10.6.3.102	185.118.164.8	80	GET	awh93dhkylps5ulnq-be.com	/czwih/fxla.php?l=gap1.cab	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/	1

What other domains do you see in the network traffic that are labelled as malicious by VirusTotal? Enter the domains defanged and in alphabetical order.

If you investigate the HTTP logs, you can determine that there are only 6 unique domains visited. If you use the following query and start investigating each domain using VirusTotal, you can determine that a-zcorner.com and knockoutlights.com are malicious domains (az361816.vo.msecnd.net was also flagged by one vendor but its not the answer for the question). You then need to enter these domains into cyberchef like as follows:



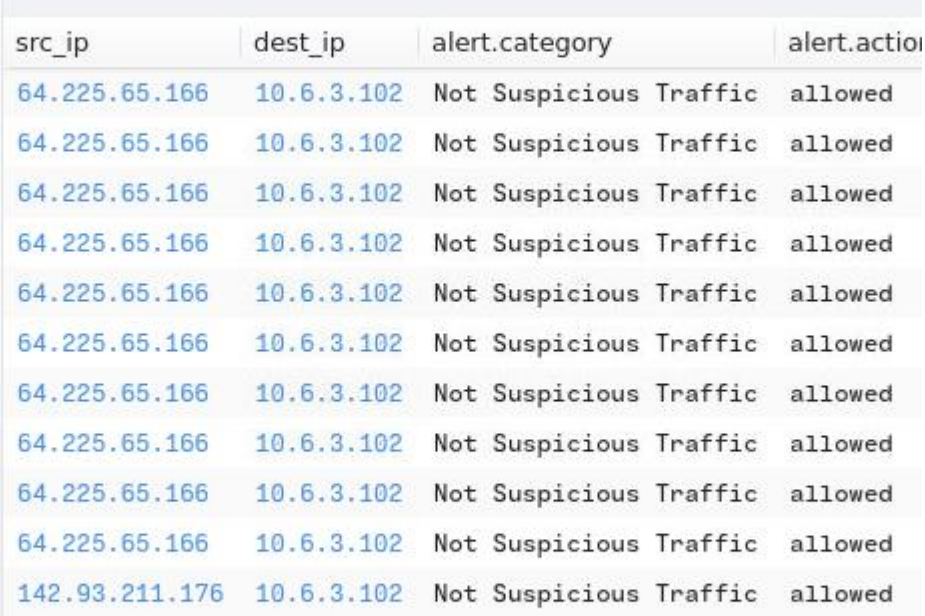
```
a-zcorner.com
knockoutlights.com
```

```
a-zcorner[.]com
knockoutlights[.]com
```

There are IP addresses flagged as Not Suspicious Traffic. What are the IP addresses? Enter your answer in numerical order and defanged.

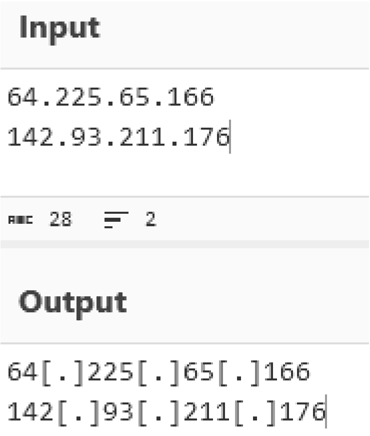
First, we need to investigate the Suricata alerts to identify the IP addresses associated with Not Suspicious Traffic, we can do this by using the following query:

- event_type=="alert" "Not Suspicious Traffic" | cut src_ip, dest_ip, alert.category, alert.action



src_ip	dest_ip	alert.category	alert.actio
64.225.65.166	10.6.3.102	Not Suspicious Traffic	allowed
64.225.65.166	10.6.3.102	Not Suspicious Traffic	allowed
64.225.65.166	10.6.3.102	Not Suspicious Traffic	allowed
64.225.65.166	10.6.3.102	Not Suspicious Traffic	allowed
64.225.65.166	10.6.3.102	Not Suspicious Traffic	allowed
64.225.65.166	10.6.3.102	Not Suspicious Traffic	allowed
64.225.65.166	10.6.3.102	Not Suspicious Traffic	allowed
64.225.65.166	10.6.3.102	Not Suspicious Traffic	allowed
64.225.65.166	10.6.3.102	Not Suspicious Traffic	allowed
64.225.65.166	10.6.3.102	Not Suspicious Traffic	allowed
142.93.211.176	10.6.3.102	Not Suspicious Traffic	allowed

Now simply enter both identified source IP addresses into cyberchef to defang them:



Input

```
64.225.65.166
142.93.211.176
```

28 2

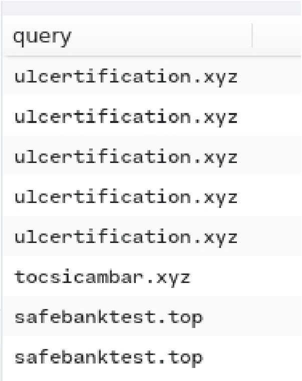
Output

```
64[.]225[.]65[.]166
142[.]93[.]211[.]176
```

For the first IP address flagged as Not Suspicious Traffic. According to VirusTotal, there are several domains associated with this one IP address that was flagged as malicious. What were the domains you spotted in the network traffic associated with this IP address? Enter your answer in defanged format and in alphabetical order.

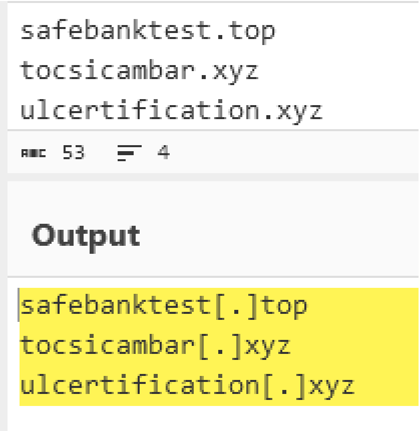
Let's start off by finding domains associated with the first IP, to do this we can enter the following query:

- 64.225.65.166 | cut query



query
ulcertification.xyz
ulcertification.xyz
ulcertification.xyz
ulcertification.xyz
ulcertification.xyz
tocsicambar.xyz
safebanktest.top
safebanktest.top

Now all we need to do is enter every domain into VirusTotal and determine what gets flagged as malicious. All three are flagged as malicious, so let's enter them into cyberchef to defang each URL:



```
safebanktest.top
tocsicambar.xyz
ulcertification.xyz
```

53 4

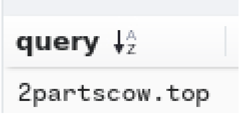
Output

```
safebanktest[.]top
tocsicambar[.]xyz
ulcertification[.]xyz
```

Now for the second IP marked as Not Suspicious Traffic. What was the domain you spotted in the network traffic associated with this IP address? Enter your answer in a defanged format.

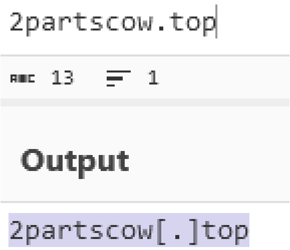
To answer this question all we need to do is change the IP address from the above query to the second IP marked as Not Suspicious Traffic like as follows:

- 142.93.211.176 | cut query



query
2partscow.top

Once you defang the URL, you are presented with:



```
2partscow.top
```

```
2partscow[.]top
```

In this challenge we successfully utilised network forensics tools like Brim and NetworkMiner to analyse a PCAP file and validate alerts triggered by Suricata. By following a systematic approach, we were able to:

- Identify the alert signatures for both a Network Trojan and a Potential Corporate Privacy Violation
- Extract and defang the IP addresses and URIs involved in the malicious activity
- Determine the name of the payload within the CAB file and the associated user-agent.
- Identify additional malicious domains and IP addresses flagged as not suspicious, providing comprehensive details through the analysis of network traffic

In my opinion the first challenge (Warzone 1) was much harder and required the use of all three tools (Wireshark, Brim, and NetworkMiner).