### **Warzone 2 — TryHackMe**

**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.

**Tasks**

1. **What was the alert signature for A Network Trojan was Detected?**

Open the packet capture file in Brim and search with the following filter.

event\_type=="alert" alert.category=="A Network Trojan was detected"

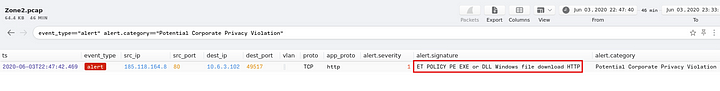


**Answer:** ET MALWARE Likely Evil EXE download from MSXMLHTTP non-exe extension M2

**2. What was the alert signature for Potential Corporate Privacy Violation?**

Search with the following filter.

event\_type=="alert" alert.category=="Potential Corporate Privacy Violation"

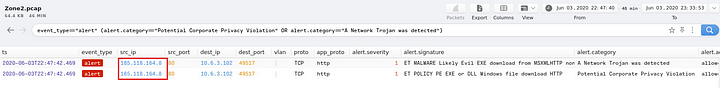


**Answer:** ET POLICY PE EXE or DLL Windows file download HTTP

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

Search with the following filter and look at the source IP address.

event\_type=="alert" (alert.category=="Potential Corporate Privacy Violation" OR alert.category=="A Network Trojan was detected")

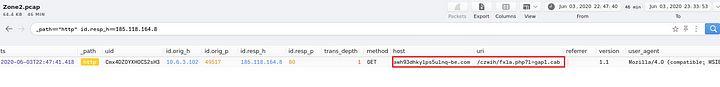


**Answer:** 185[.]118[.]164[.]8

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

Use the following filter to filter out the HTTP packets belonging to the above identified IP address.

\_path=="http" id.resp\_h==185.118.164.8



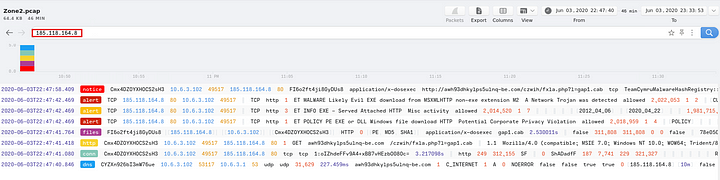
If we combine the host and uri, that would be the full URL we are looking for.

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

**5. What is the name of the payload within the cab file?**

Search with the IP address identified above.

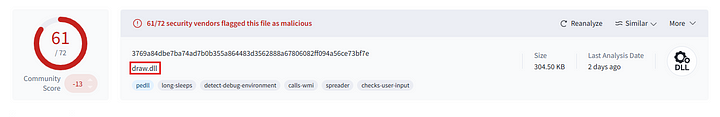
185.118.164.8



Now, check the files path, to find the hash of the gap1.cab file.



The MD5 hash is 78e05075e686397097de69fb0402263e. Now submit this hash to ViruTotal.

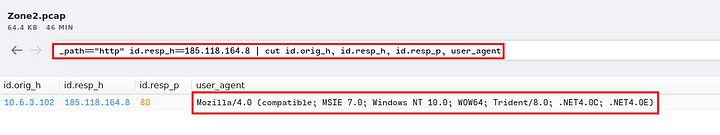


**Answer:** draw.dll

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

Apply the following filter.

\_path=="http" id.resp\_h==185.118.164.8 | cut id.orig\_h, id.resp\_h, id.resp\_p, user\_agent

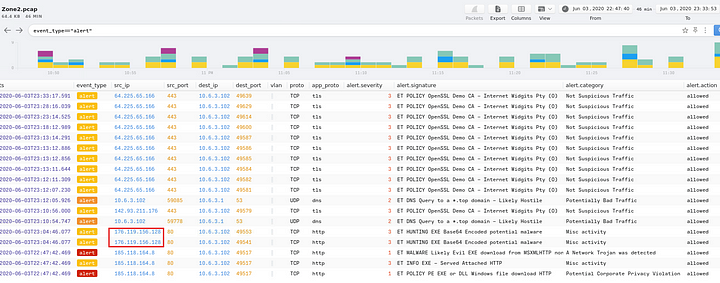


**Answer:** Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/8.0; .NET4.0C; .NET4.0E)

**7. 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. (format: domain[.]zzz,domain[.]zzz)**

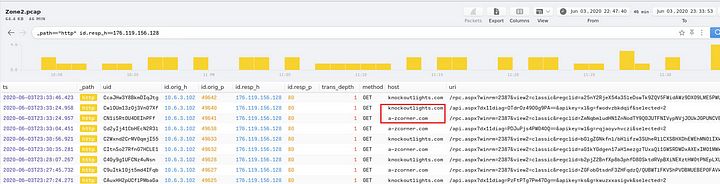
Let us check for all the alerts.

event\_type=="alert"



one of the IP addresses has Misc activity tag. Rest of the Ip addresses are marked as not malicious. So let us examine the traffic to and from this IP address, to find the domain associated with this IP.

\_path=="http" id.resp\_h==176.119.156.128



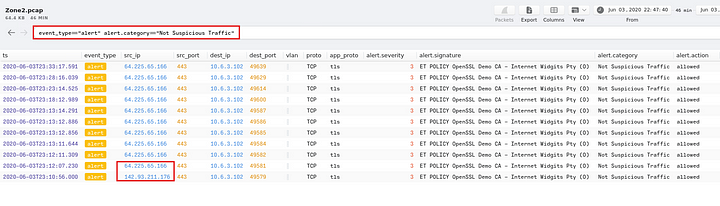
We can see above, the two domains associated with this IP address.

**Answer:** a-zcorner[.]com,knockoutlights[.]com

**8. There are IP addresses flagged as Not Suspicious Traffic. What are the IP addresses? Enter your answer in numerical order and defanged. (format: IPADDR,IPADDR)**

We looked at them in the previous question.

event\_type=="alert" event\_category=="Not Suspicious Traffic"

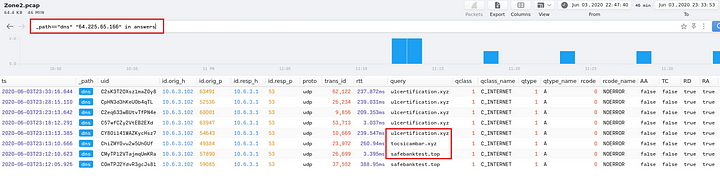


**Answer:** 64[.]225[.]65[.]166,142[.]93[.]211[.]176

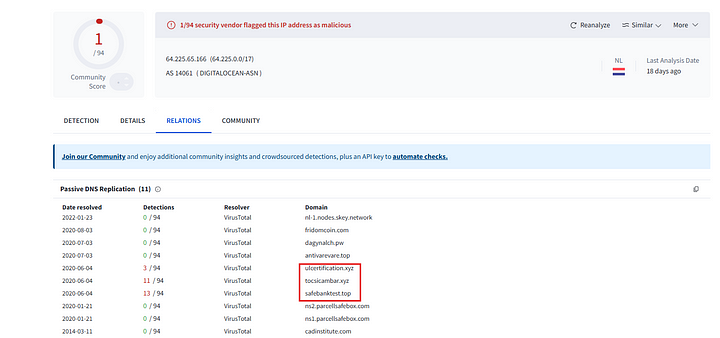
**9. For the first IP address flagged as Not Suspicious Traffic. According to VirusTotal, there are several domains associated with this one IP address that was flagged as malicious. What were the domains you spotted in the network traffic associated with this IP address? Enter your answer in a defanged format. Enter your answer in alphabetical order, in a defanged format. (format: domain[.]zzz,domain[.]zzz,etc)**

Since the traffic is tls encrypted, we cannot find much information about the traffic related to this, but we can check the dns requests related to this IP.

\_path=="dns" "64.225.65.166" in answers



We can see three domains related to this IP present in the packet capture. Now we can submit the IP to VirusTotal to check the matching domains.

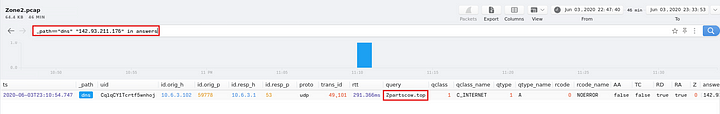


As we can see, all three domains are present in VirusTotal.

**Answer:** safebanktest[.]top,tocsicambar[.]xyz,ulcertification[.]xyz

**10. 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. (format: domain[.]zzz)**

\_path=="dns" "142.93.211.176" in answers



**Answer:** 2partscow[.]top

This is the end of this Walkthrough.