### **Warzone 1 — TryHackMe**

**Scenario:** You work as a Tier 1 Security Analyst L1 for a Managed Security Service Provider (MSSP). Today you’re tasked with monitoring network alerts.

A few minutes into your shift, you get your first network case: **Potentially Bad Traffic** and **Malware Command and Control Activity detected**. Your race against the clock starts. Inspect the PCAP and retrieve the artifacts to confirm this alert is a true positive.

**Your tools**:

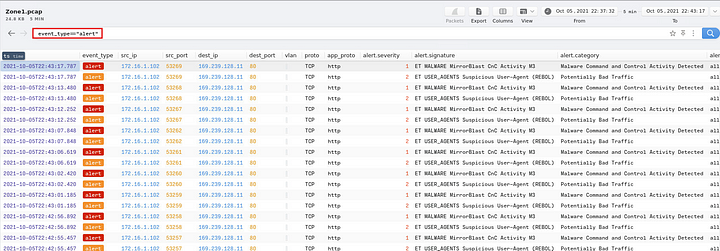
* Brim
* Network Miner
* Wireshark

#### **Tasks**

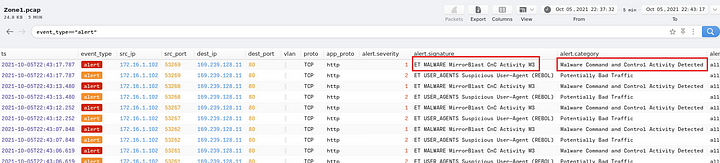
1. **What was the alert signature for Malware Command and Control Activity Detected?**

Open the given pcaket capture file in brim and filter to view all the alerts.

event\_type=="alert"



We can see the alert signature for Malware Command and Control Activity.

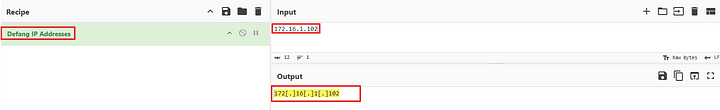


**Answer:** ET Malware MirrorBlast CnC Activity M3

**2. What is the source IP address? Enter your answer in a defanged format.**

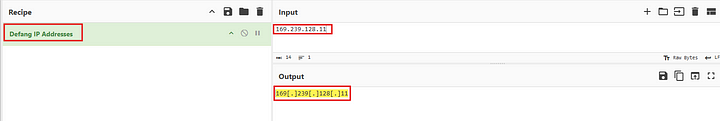
****

We can see the IP address above, we can defand this by adding ‘[]’ around the dots or simply by pasting it to cyberchef and defang it.



**Answer:** 172[.]16[.]1[.]102

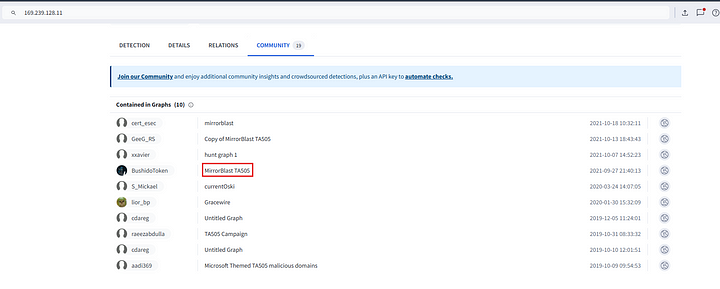
**3. What IP address was the destination IP in the alert? Enter your answer in a defanged format.**

****

**Answer:** 169[.]239[.]128[.]11

**4. Still in VirusTotal, under Community, what threat group is attributed to this IP address?**

Paste the above IP address into VirusTotal and navigate to the community section.

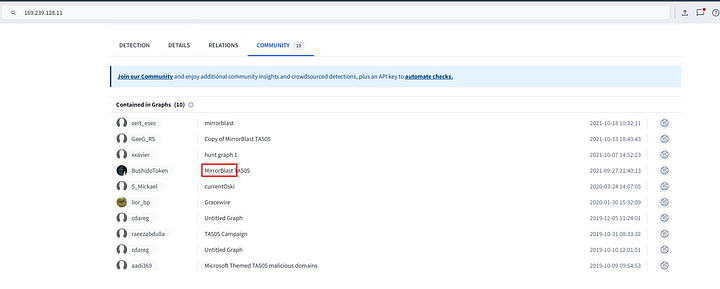


As we can see above the threat actor is TA505.

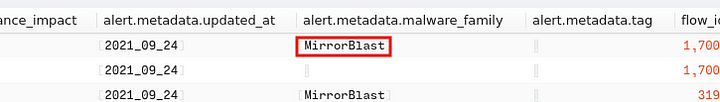
**Answer:** TA505

**5. What is the malware family?**

This is also evident from the above image.



We can also confirm this from the alert.

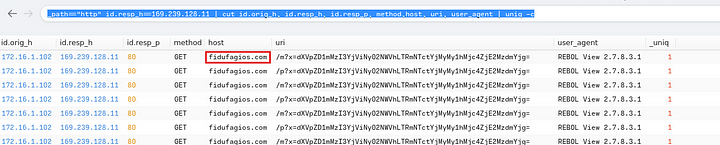


**Answer:** Mirrorblast.

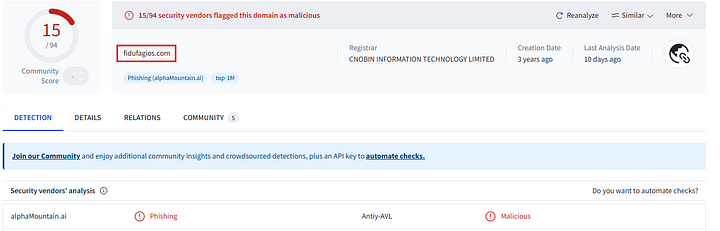
**6. Do a search in VirusTotal for the domain from question 4. What was the majority file type listed under Communicating Files?**

Let us filter the HTTP traffic from the IP address in question 4.

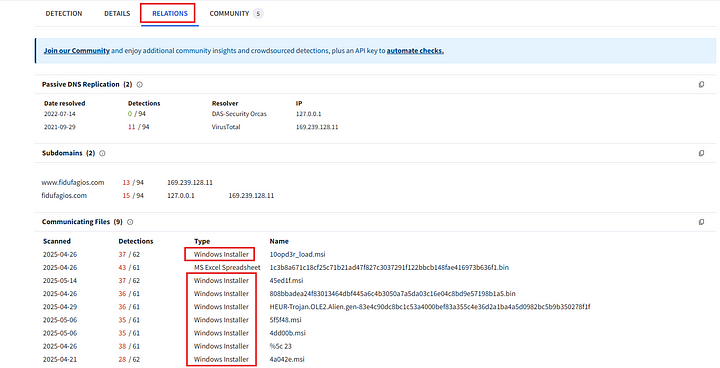
\_path=="http" id.resp\_h==169.239.128.11 | cut id.orig\_h, id.resp\_h, id.resp\_p, method,host, uri, user\_agent | uniq -c



Above, we can see the domain related to this IP address. Now we can submit this to VirusTotal.



Now, under Relations tab we can find the majority filetype associated with this domain.

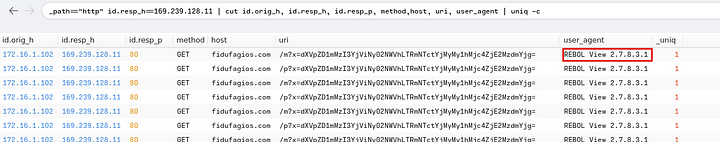


**Answer:** Windows Installer

**7. Inspect the web traffic for the flagged IP address; what is the user-agent in the traffic?**

This is also visible from the above filter.

\_path=="http" id.resp\_h==169.239.128.11 | cut id.orig\_h, id.resp\_h, id.resp\_p, method,host, uri, user\_agent | uniq -c



**Answer:** REBOL View 2.7.8.3.1

**8. Retrace the attack; there were multiple IP addresses associated with this attack. What were two other IP addresses? Enter the IP addressed defanged and in numerical order. (format: IPADDR,IPADDR)**

In the above filtered results, we have four more IP addresses other than the already identified malicious IP and the victim IP.



Two of these Ip addresses sent GET requests to download Windows Installer files, which we already found out from the above that were related to the attack. This can also be confirmed by submitting them to VirusTotal.

**Answer:** 185[.]10[.]68[.]235,192[.]36[.]27[.]92

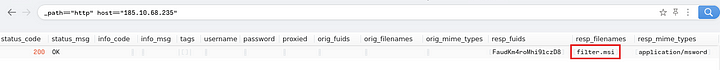
**9. What were the file names of the downloaded files? Enter the answer in the order to the IP addresses from the previous question. (format: file.xyz,file.xyz)**

****

We can clearly see one of the file names. To find the other filre name, we need to expand our results.

\_path=="http" host=="185.10.68.235"

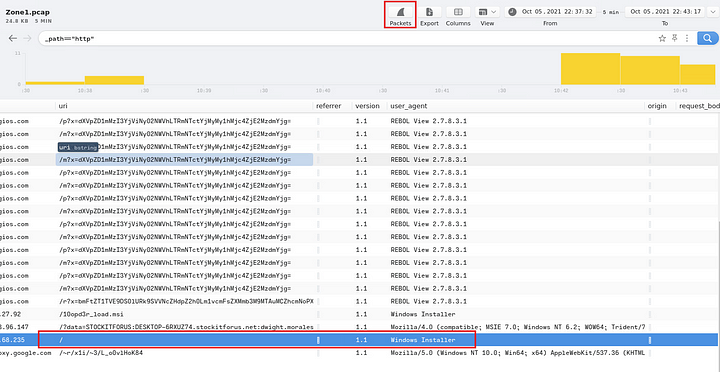
The above search will give us all the details relating to the http packet from the IP address.



**Answer:** filter.msi, 10opd3r\_load.msi

**10. Inspect the traffic for the first downloaded file from the previous question. Two files will be saved to the same directory. What is the full file path of the directory and the name of the two files? (format: C:\path\file.xyz,C:\path\file.xyz)**

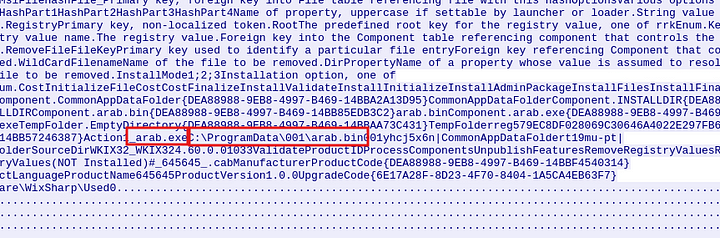
In brim select the packet related to filter.msi and click on the Packets option at the top.



This will open Wireshark with the related packet already selected.



Now right click on this and select follow TCP stream.

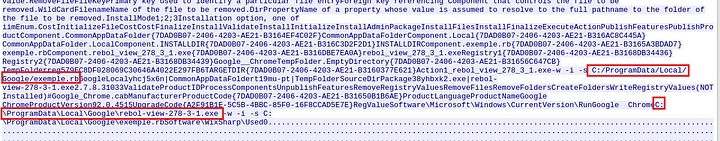
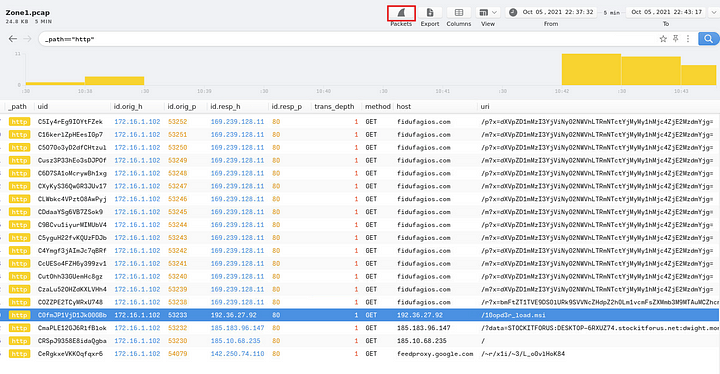


Now we can see the files related to the Windows Installer. Since they are saved to the same path the path for arab.exe will be the same.

**Answer:** C:\ProgramData\001\arab.bin, C:\ProgramData\001\arab.exe

**11. Now do the same and inspect the traffic from the second downloaded file. Two files will be saved to the same directory. What is the full file path of the directory and the name of the two files? (format: C:\path\file.xyz,C:\path\file.xyz)**

We can follow the same procedure as in the previous question.



**Answer:** C:\ProgramData\Local\Google\rebol-view-278–3–1.exe, C:/ProgramData/Local/Google/exemple.rb

This is the end of this walkthrough.