Warzone-1 THM(Medium)

1. Summary

As a Tier 1 Security Analyst (L1) at an MSSP, I investigated an alert indicating **Potentially Bad Traffic and Malware Command-and-Control (C2) Activity**. My task was to validate whether the alert represented a legitimate threat by analyzing the associated PCAP file and extracting malicious artifacts.

During the investigation, I reviewed network flows, identified suspicious outbound connections, inspected payloads, and parsed potential malware communication patterns. By correlating traffic behavior, endpoint indicators, and protocol anomalies, I confirmed that the alert was a **true positive**. The PCAP revealed active C2 communication consistent with malware beaconing, unauthorized outbound traffic to a suspicious external host, and identifiable malicious indicators. These findings validated the escalation and supported further response actions.

2. Investigation Overview

Objective:

The investigation focused on analyzing network traffic logs and a PCAP file to identify indicators of compromise, malicious communication patterns, and associated threat intelligence. Tools such as **Brim**, **Wireshark**, **CyberChef**, and **VirusTotal** were used to trace the activity, profile the threat actor, and correlate data across alerts, IPs, domains, and downloaded files.

Data / Tools Used:

- Brim
- VirusTotal
- PCAPs / Wireshark
- CyberChef
- MITRE ATT&CK

3. What I Did

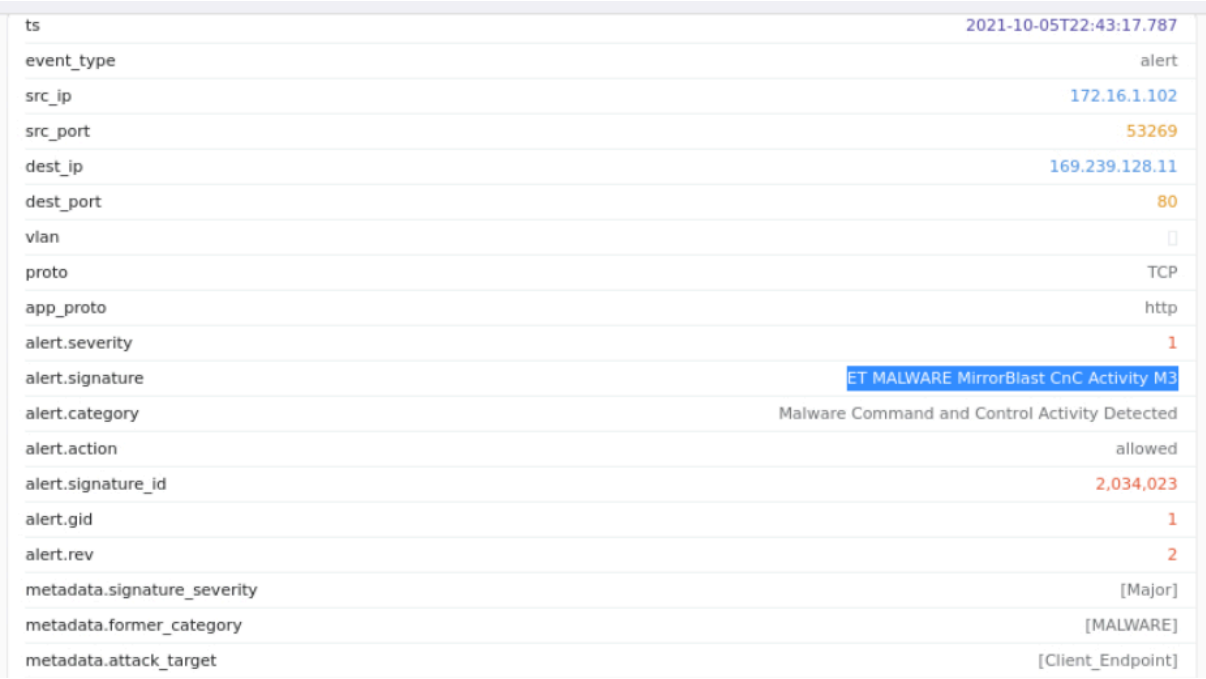
Lets start the machine and analyze the pcap file.

Task-1 Analyzing the pcap files and answering the questions.

Q1) What was the alert signature for Malware Command and Control Activity Detected?

By opening brim and filtering for the alert of **Malware Command and Control Activity Detected**

We can see the alert signature the brim log detail.



ts	2021-10-05T22:43:17.787
event_type	alert
src_ip	172.16.1.102
src_port	53269
dest_ip	169.239.128.11
dest_port	80
vlan	
proto	TCP
app_proto	http
alert.severity	1
alert.signature	ET MALWARE MirrorBlast CnC Activity M3
alert.category	Malware Command and Control Activity Detected
alert.action	allowed
alert.signature_id	2,034,023
alert.gid	1
alert.rev	2
metadata.signature_severity	[Major]
metadata.former_category	[MALWARE]
metadata.attack_target	[Client_Endpoint]

Q2)What is the source IP address? Enter your answer in a defanged format.

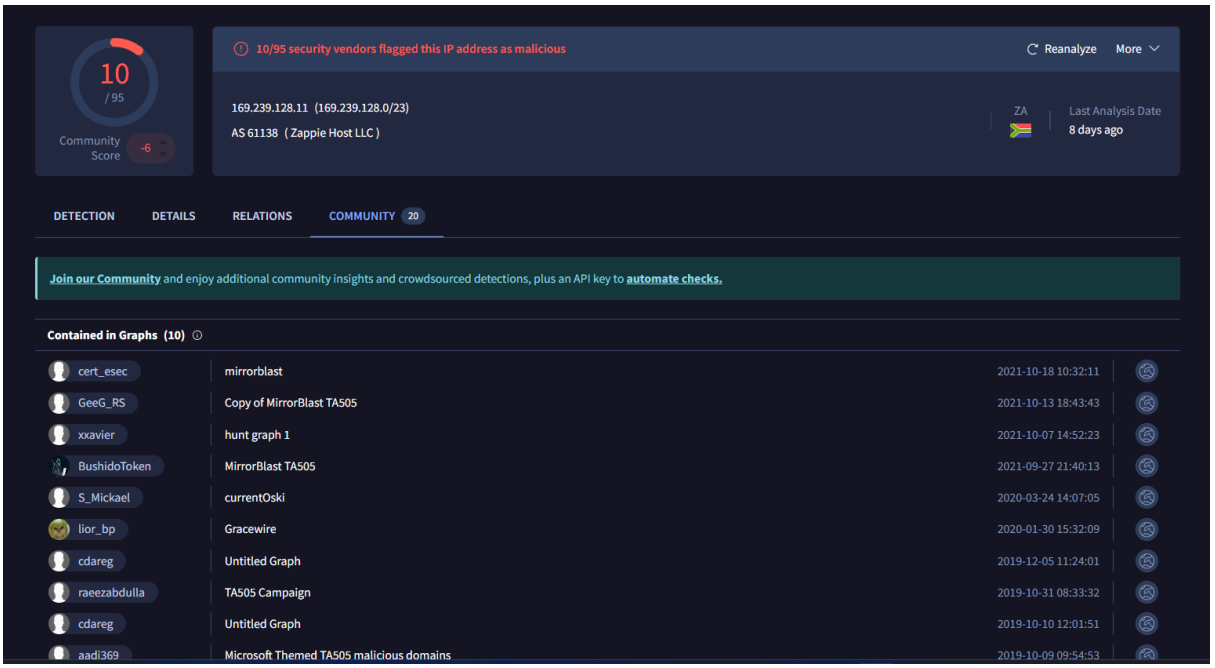
In the log we can see the source ip and we can defang this IP using cyberchef

Q3) What IP address was the destination IP in the alert? Enter your answer in a defanged format.

Following the same log we have the destination IP address.

Q4)Still in VirusTotal, under Community, what threat group is attributed to this IP address?

Virus total findings-



Q5)What is the malware family?

Again searching the log used in Q1 and Q2 we can see the malware family is mirrorblast.

Q6)Do a search in VirusTotal for the domain from question 4. What was the majority file type listed under Communicating Files?

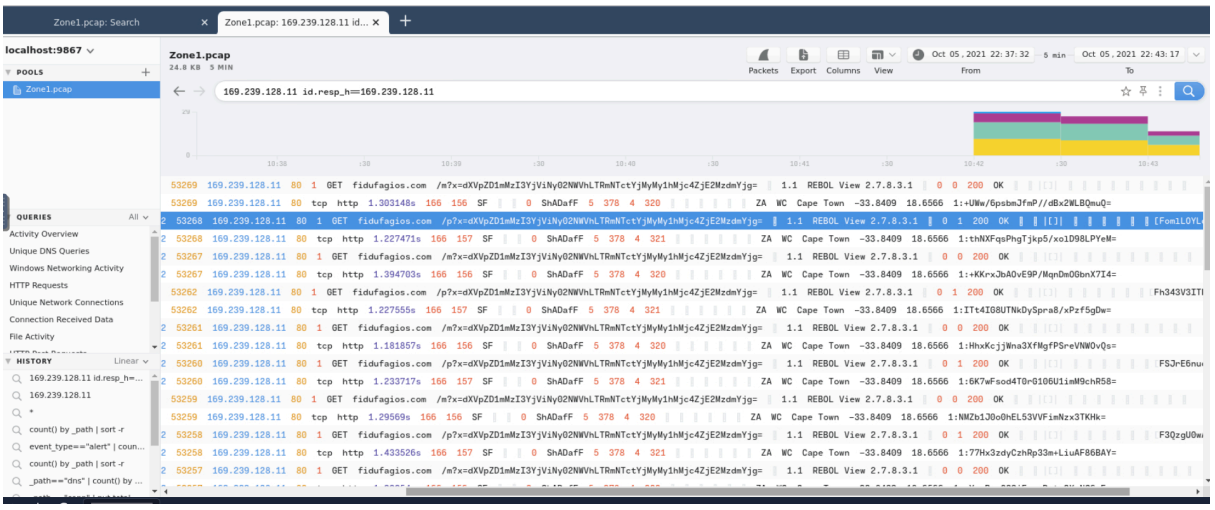
In virus total under relations tab we can see the majority file type but it was a bit tricky to figure out the exact file.

Communicating Files (188)

Scanned	Detections	Type	Name
2020-08-30	20 / 60	Office Open XML Spreadsheet	result.xlsm
2021-03-02	55 / 71	Win32 EXE	wotsuper3.exe
2020-08-07	43 / 73	Win32 EXE	wotsuper.exe
2020-08-28	53 / 68	Win32 EXE	bb62edbc434c9c35b8151035475f9a66.virus
2020-08-21	64 / 68	Win32 EXE	06c0c9101e4d3685a427.pe32
2021-04-12	53 / 70	Win32 EXE	tau111.exe
2020-02-27	33 / 72	Win32 EXE	Vidar.exe
2025-11-13	37 / 63	Windows Installer	10opd3r_load.msi
2025-03-24	62 / 73	Win32 EXE	FSTIME.EXE
2020-08-16	38 / 68	Win32 EXE	Vidar.exe

Q7)Inspect the web traffic for the flagged IP address; what is the user-agent in the traffic?

In the brim dashboard we can filter the flagged IP and the suer agent field is at the end of the query.



Q8)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.

Filtering the http requests in the brim dashboard we can see a few ip addresses at the bottom.

172.16.1.102	169.239.128.11	80	GET	fidufagios.com	/p?x=dXVpZD1mMzI3YjViNy02NWVhLTRmNTctYjMyMy1hMjc4ZjE2MzdmYjg=	1
172.16.1.102	169.239.128.11	80	GET	fidufagios.com	/m?x=dXVpZD1mMzI3YjViNy02NWVhLTRmNTctYjMyMy1hMjc4ZjE2MzdmYjg=	1
172.16.1.102	169.239.128.11	80	GET	fidufagios.com	/p?x=dXVpZD1mMzI3YjViNy02NWVhLTRmNTctYjMyMy1hMjc4ZjE2MzdmYjg=	1
172.16.1.102	169.239.128.11	80	GET	fidufagios.com	/m?x=dXVpZD1mMzI3YjViNy02NWVhLTRmNTctYjMyMy1hMjc4ZjE2MzdmYjg=	1
172.16.1.102	169.239.128.11	80	GET	fidufagios.com	/p?x=dXVpZD1mMzI3YjViNy02NWVhLTRmNTctYjMyMy1hMjc4ZjE2MzdmYjg=	1
172.16.1.102	169.239.128.11	80	GET	fidufagios.com	/m?x=dXVpZD1mMzI3YjViNy02NWVhLTRmNTctYjMyMy1hMjc4ZjE2MzdmYjg=	1
172.16.1.102	169.239.128.11	80	GET	fidufagios.com	/p?x=dXVpZD1mMzI3YjViNy02NWVhLTRmNTctYjMyMy1hMjc4ZjE2MzdmYjg=	1
172.16.1.102	169.239.128.11	80	GET	fidufagios.com	/m?x=dXVpZD1mMzI3YjViNy02NWVhLTRmNTctYjMyMy1hMjc4ZjE2MzdmYjg=	1
172.16.1.102	169.239.128.11	80	GET	fidufagios.com	/p?x=dXVpZD1mMzI3YjViNy02NWVhLTRmNTctYjMyMy1hMjc4ZjE2MzdmYjg=	1
172.16.1.102	169.239.128.11	80	GET	fidufagios.com	/m?x=dXVpZD1mMzI3YjViNy02NWVhLTRmNTctYjMyMy1hMjc4ZjE2MzdmYjg=	1
172.16.1.102	169.239.128.11	80	GET	fidufagios.com	/p?x=dXVpZD1mMzI3YjViNy02NWVhLTRmNTctYjMyMy1hMjc4ZjE2MzdmYjg=	1
172.16.1.102	169.239.128.11	80	GET	fidufagios.com	/m?x=dXVpZD1mMzI3YjViNy02NWVhLTRmNTctYjMyMy1hMjc4ZjE2MzdmYjg=	1
172.16.1.102	169.239.128.11	80	GET	fidufagios.com	/r?x=bmFtZT1TVE9DS01URk9SVVNcZHdpZ2h0Lm1vcmFsZXMmb3M9MTAuMCZhcmNoPX	1
172.16.1.102	192.36.27.92	80	GET	192.36.27.92	/10opd3r_load.msi	1
172.16.1.102	185.183.96.147	80	GET	185.183.96.147	/?data=STOCKITFORUS:DESKTOP-6RXUZ74.stockitforus.net:dwight.morales	1
172.16.1.102	185.10.68.235	80	GET	185.10.68.235	/	1
172.16.1.102	142.250.74.110	80	GET	feedproxy.google.com	/~r/x1i/~3/L_o0vlHoK84	1

Q9)What were the file names of the downloaded files? Enter the answer in the order to the IP addresses from the previous question.

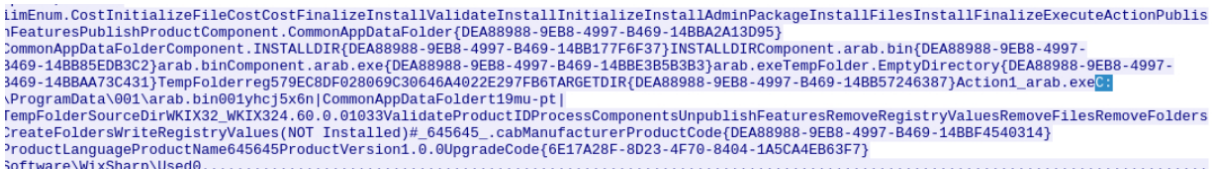
In the file activity section we can see the file which has been downloaded by the first IP and the file which has been downloaded by the second IP can be figured from the http request filter.

172.16.1.102	169.239.128.11	80	GET	fidufagios.com	/p?x=dXVpZD1mMzI3YjViNy02NWVhLTRmNTctYjMyMy1hMjc4ZjE2MzdmYjg=	1
172.16.1.102	169.239.128.11	80	GET	fidufagios.com	/m?x=dXVpZD1mMzI3YjViNy02NWVhLTRmNTctYjMyMy1hMjc4ZjE2MzdmYjg=	1
172.16.1.102	169.239.128.11	80	GET	fidufagios.com	/p?x=dXVpZD1mMzI3YjViNy02NWVhLTRmNTctYjMyMy1hMjc4ZjE2MzdmYjg=	1
172.16.1.102	169.239.128.11	80	GET	fidufagios.com	/m?x=dXVpZD1mMzI3YjViNy02NWVhLTRmNTctYjMyMy1hMjc4ZjE2MzdmYjg=	1
172.16.1.102	169.239.128.11	80	GET	fidufagios.com	/p?x=dXVpZD1mMzI3YjViNy02NWVhLTRmNTctYjMyMy1hMjc4ZjE2MzdmYjg=	1
172.16.1.102	169.239.128.11	80	GET	fidufagios.com	/m?x=dXVpZD1mMzI3YjViNy02NWVhLTRmNTctYjMyMy1hMjc4ZjE2MzdmYjg=	1
172.16.1.102	169.239.128.11	80	GET	fidufagios.com	/p?x=dXVpZD1mMzI3YjViNy02NWVhLTRmNTctYjMyMy1hMjc4ZjE2MzdmYjg=	1
172.16.1.102	169.239.128.11	80	GET	fidufagios.com	/m?x=dXVpZD1mMzI3YjViNy02NWVhLTRmNTctYjMyMy1hMjc4ZjE2MzdmYjg=	1
172.16.1.102	169.239.128.11	80	GET	fidufagios.com	/p?x=dXVpZD1mMzI3YjViNy02NWVhLTRmNTctYjMyMy1hMjc4ZjE2MzdmYjg=	1
172.16.1.102	169.239.128.11	80	GET	fidufagios.com	/m?x=dXVpZD1mMzI3YjViNy02NWVhLTRmNTctYjMyMy1hMjc4ZjE2MzdmYjg=	1
172.16.1.102	169.239.128.11	80	GET	fidufagios.com	/p?x=dXVpZD1mMzI3YjViNy02NWVhLTRmNTctYjMyMy1hMjc4ZjE2MzdmYjg=	1
172.16.1.102	169.239.128.11	80	GET	fidufagios.com	/m?x=dXVpZD1mMzI3YjViNy02NWVhLTRmNTctYjMyMy1hMjc4ZjE2MzdmYjg=	1
172.16.1.102	169.239.128.11	80	GET	fidufagios.com	/r?x=bmFtZT1TVE9DS01URk9SVVNcZHdpZ2h0Lm1vcmFsZXMmb3M9MTAuMCZhcmNoPX	1
172.16.1.102	192.36.27.92	80	GET	192.36.27.92	/10opd3r_load.msi	1
172.16.1.102	185.183.96.147	80	GET	185.183.96.147	/?data=STOCKITFORUS:DESKTOP-6RXUZ74.stockitforus.net:dwight.morales	1
172.16.1.102	185.10.68.235	80	GET	185.10.68.235	/	1
172.16.1.102	142.250.74.110	80	GET	feedproxy.google.com	/~r/x1i/~3/L_o0vlHoK84	1

Q10)**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?**

For this task we have to open the pcap file in wireshark and follow the TCP streams which we have loaded through brim.

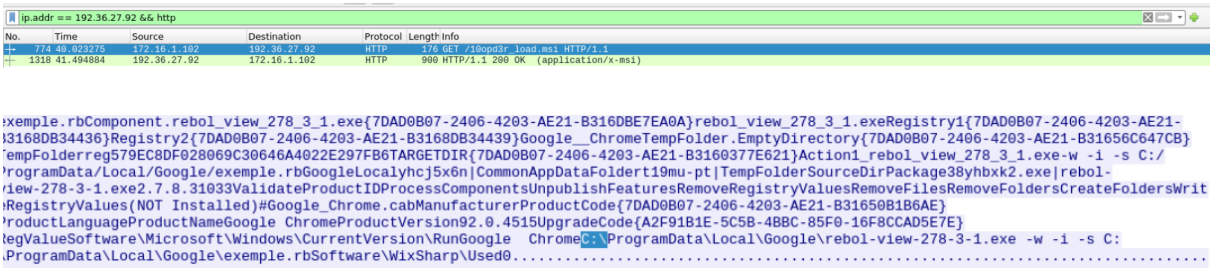
We search for the C: word in tcp stream



We have two files one with .exe entension and one with .bin extension which is our answer.

Q11) 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?

We follow the same steps we have taken in Q10.



THANK YOU!

4. Key Findings

1. Malware C2 Activity Detected

- Brim flagged an alert for **“Malware Command and Control Activity Detected”**, revealing suspicious external communication consistent with known malware beaconing patterns.

2. Source & Destination Hosts Identified

- The **source IP** and **destination C2 IP** involved in the alert were extracted and defanged for safe handling.
- These IPs were later correlated with threat intelligence from VirusTotal.

3. Threat Group Attribution

- VirusTotal’s Community section linked the destination IP to a **known threat group**, confirming this was not random malicious traffic but part of a larger campaign.

4. Malware Family: MirrorBlast

- The alert logs indicated the malware family **MirrorBlast**, a malware strain known for leveraging malicious documents and multi-stage payload deliveries.

5. Associated Domain & File Types

- The domain tied to the threat group showed several communicating files in VT.
- The majority file type was identified through analyzing the **Relations → Communicating Files** section.

6. User-Agent Analysis

- HTTP traffic associated with the flagged IP showed a distinct **user-agent string**, helping identify the tool or exploit kit interacting with the C2 server.

7. Lateral Indicator Expansion

- Retracing traffic revealed **multiple additional IP addresses** tied to the attack chain.
- These IPs were defanged and documented in numeric order.

8. Payload Retrieval

- Two downloaded files were identified for each malicious IP.
- File names were captured from Brim's file activity view and correlated with HTTP requests.

9. File Path Discovery in Wireshark

- By following TCP streams and searching for "C:" strings, full **file paths** and **payload names** (.exe and .bin) were extracted.
- For both malicious downloads, two files were saved in the same directory each time, highlighting the dropper behavior.

10. Full Attack Chain Mapped

- From initial alert → suspicious IPs → download requests → payload paths → threat actor attribution.
- The end-to-end infection flow was reconstructed successfully, showing how MirrorBlast delivered multiple payloads from different remote hosts.

---

8. What I Learned

1. Handling PCAP Files Efficiently

I learned how to load, filter, and analyze large PCAP files using **Brim** and **Wireshark**, allowing me to quickly isolate suspicious activity, correlate logs, and follow TCP streams to extract meaningful forensic information.

2. Identifying Command-and-Control (C2) Activity

Through log analysis and filtering, I gained hands-on experience recognizing patterns associated with **malware C2 communication**, including beaconing behavior, suspicious user-agent strings, and consistent connections to known malicious IPs.

3. Using Threat Intelligence for Attribution

By integrating **VirusTotal** into the investigation, I understood how to:

- Attribute malicious infrastructure to **known threat groups**
- Identify malware families (e.g., **MirrorBlast**)
- Analyze communicating files, domains, and file types

This helped strengthen my threat attribution and intelligence correlation skills.

4. Tracing Multi-Stage Attack Chains

I learned how to retrace attacker steps by following:

- Initial alert logs
- Related IPs
- HTTP download requests
- Associated payloads
- Final file paths on the victim system

This gave me a deeper understanding of how distributed infrastructure is used in real-world malware campaigns.

5. Extracting Payloads & File Paths

By following TCP streams in Wireshark, I learned how attackers deliver multiple payloads (.exe, .bin) and how to identify where these files would land on the victim system. This improved my forensic skills in reconstructing malware delivery paths.

---

9. Conclusion

The investigation confirmed that the network activity was part of a coordinated malware campaign attributed to a known threat group associated with **MirrorBlast**. Through structured analysis using Brim, VirusTotal, and Wireshark, I successfully traced the entire attack chain—from initial C2 alerts to multiple malicious IPs, payload downloads, and local file paths.