DIGITAL FORENSICS - INVESTIGATON OF A PCAP

Cybersecurity DFIR

2025

MICHAEL MUSOKE

Contents

PCAP Investigation using Security Onion

Objectives

1. Import .pcap file into Security Onion
2. Investigate .pcap file
3. Provide an analysis of what probably occurred

Introduction

Security Onion is a free open-source Linux distribution for network security monitoring, intrusion detection, and log management. It integrated powerful like Suricata, Zeek, Wazuh and the ELK stack to capture and analyse network traffic.
In the security industry, Security Onion plays a critical role by providing SOCs, incident responders and threat hunters with a comprehensive platform for real-time monitoring and forensic analysis. Its ability to correlate data from multiple sources enables organisations to quickly identify, investigate and mitigate potential threats, thereby enhancing their overall security posture.

In this demonstration, a. pcap will be ingested into security onion and an investigation will be done to determine the nature of the captured network traffic.

Log on to the security onion console. Create a directory into which the pcap will be downloaded using mkdir command e.g. **mkdir Malware**

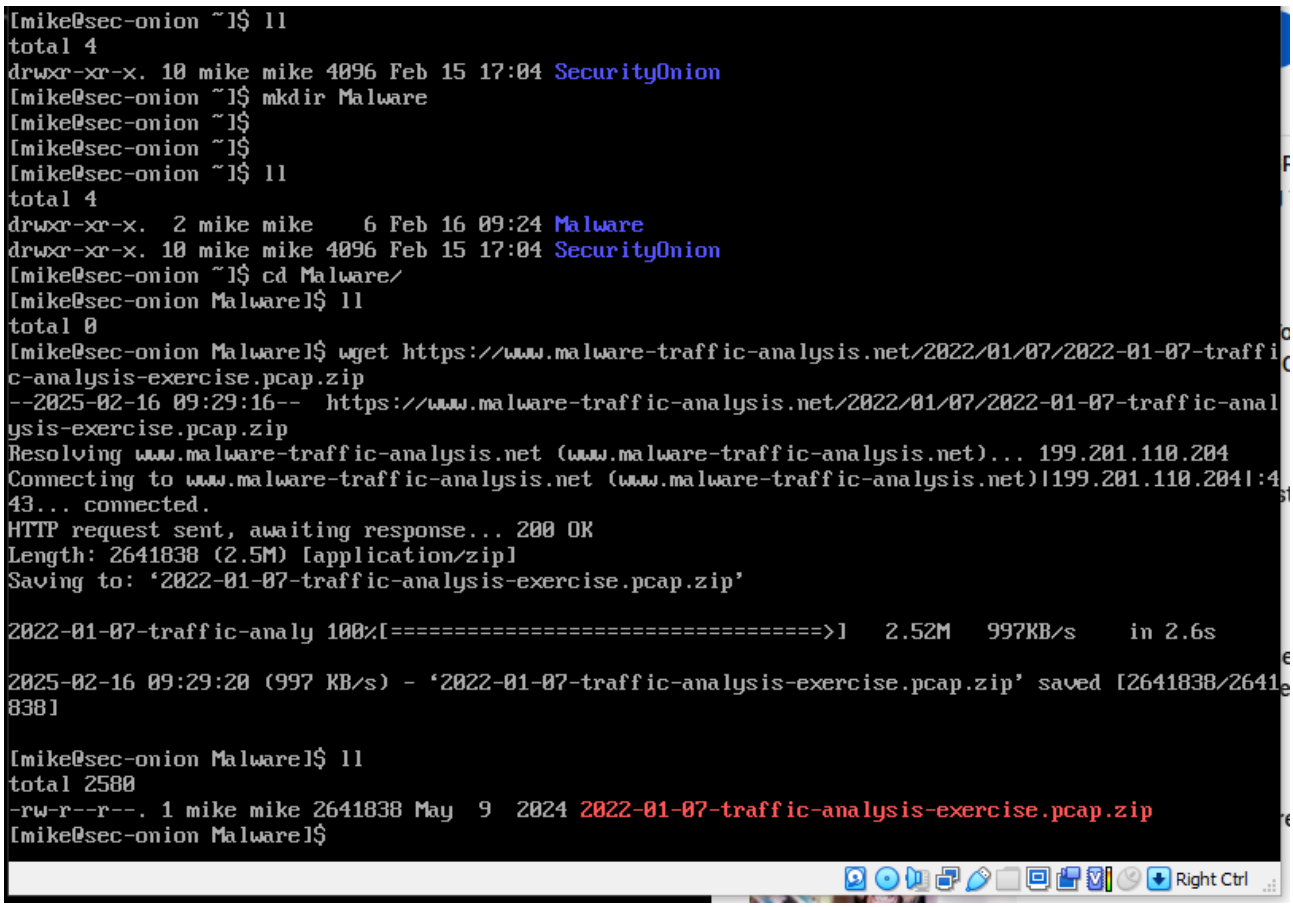


Figure 1

use the command wget to download an infected pcap from the website as shown in figure 1
https://www.malware-traffic-analysis.net/2022/01/07/2022-01-07-traffice-analysis-exercise.pcap.zip

When the zipped pcap is downloaded use the unzip command to decompress the pcap. Visit the about page of Traffic analysis to obtain the password

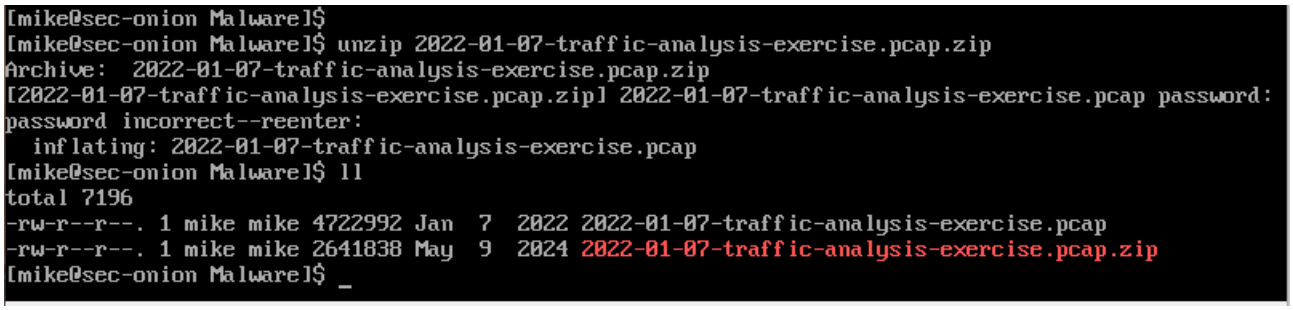


Figure 2

Next is to import the pcap using the command **so-import-pcap <name of pcap>**

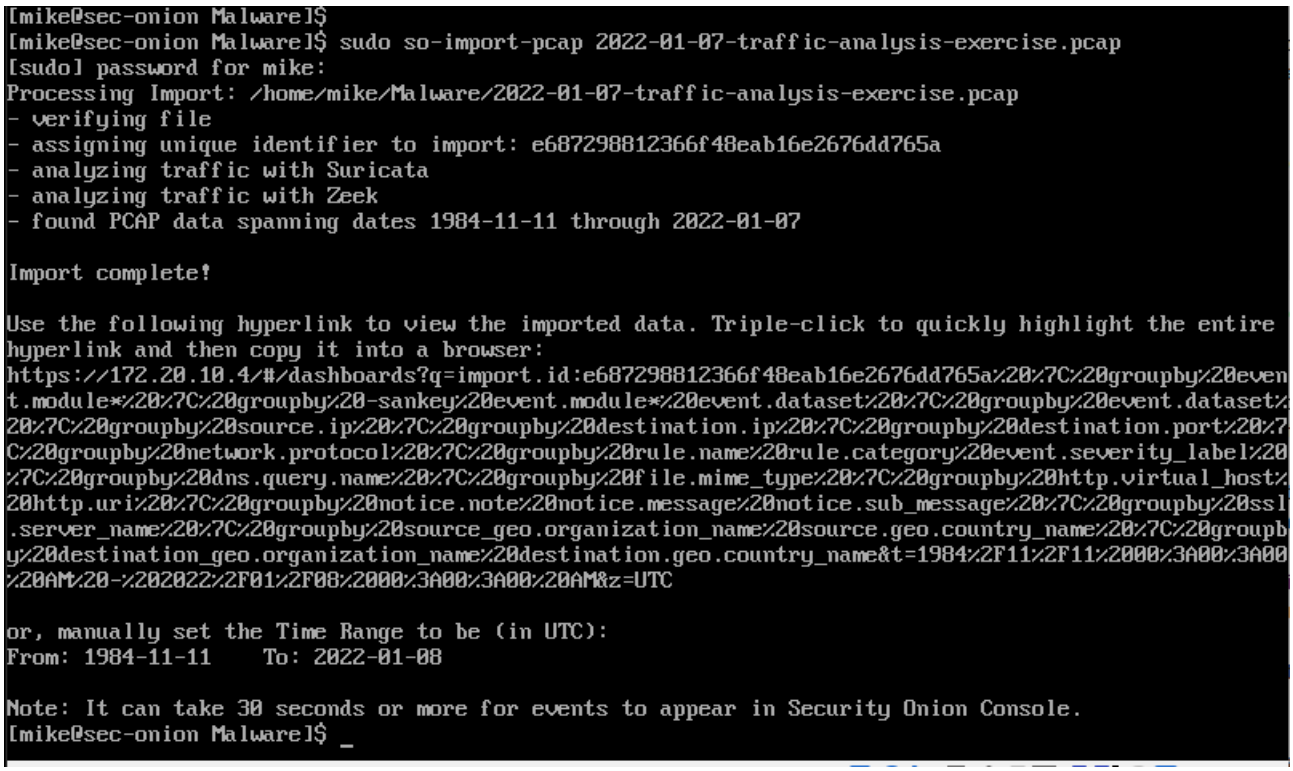


Figure 3

With the import complete log on the web console. To examine the pcap change time to a period the pcap was captured in this case 2022-01-07-2022-01-31

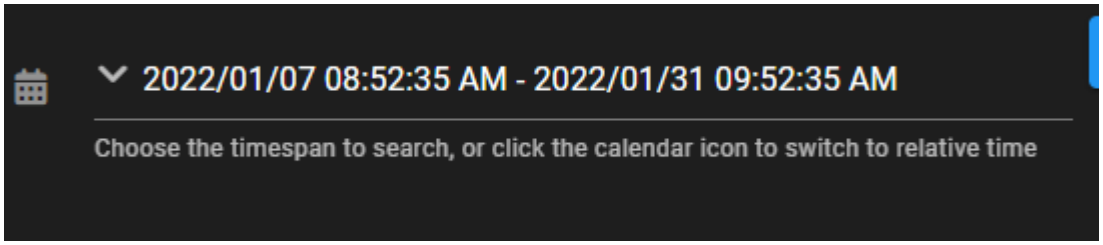


Figure 4

Take note of the query that was generated by changing the time. The wildcard * to select everything grouped by the different options

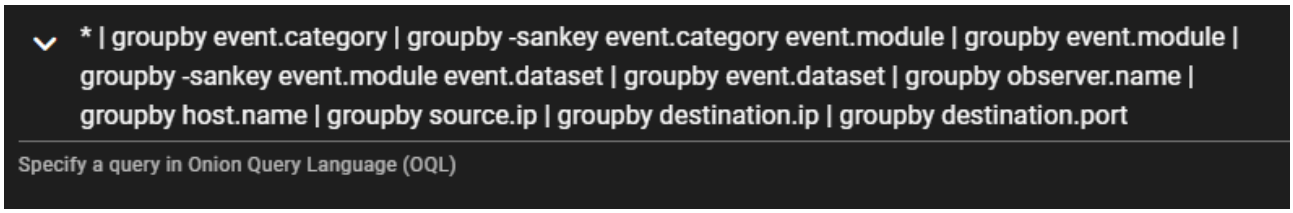
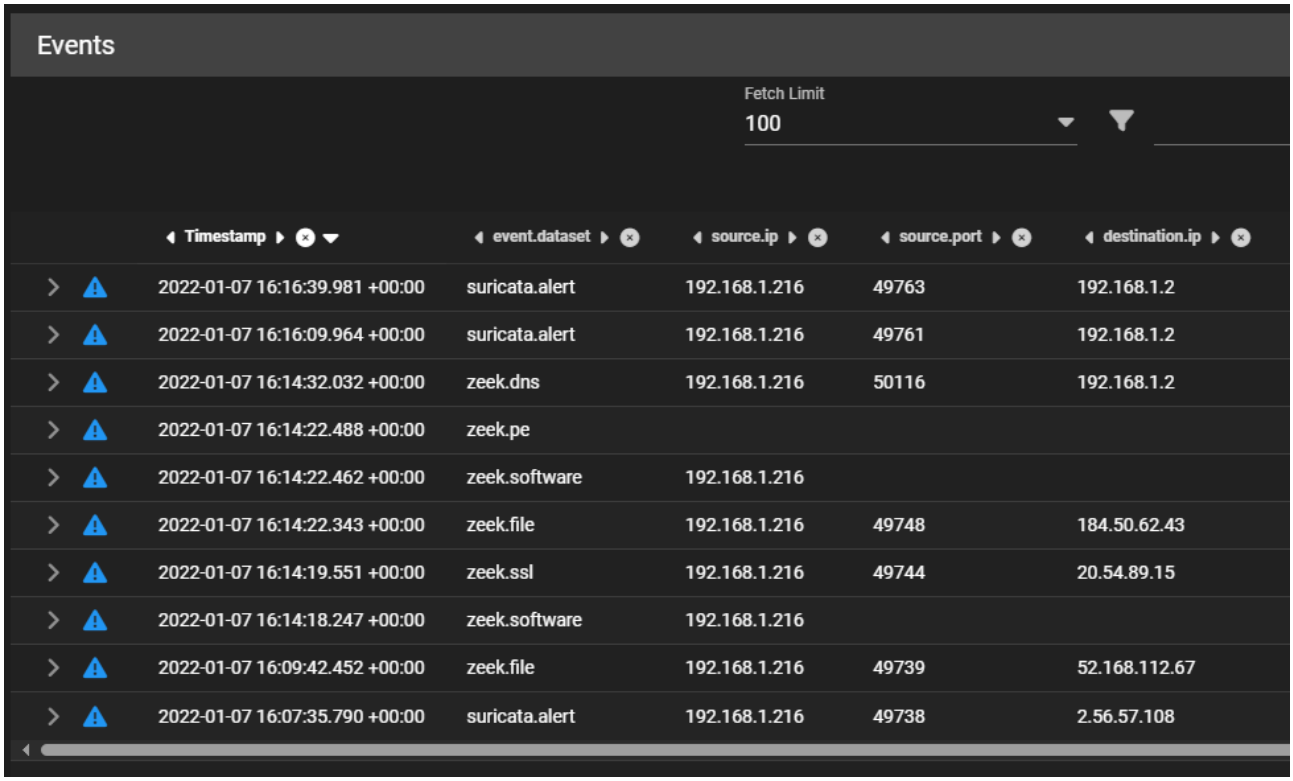


Figure 5

Scrolling to the Event alerts by Suricata and Zeek at the time. Under event dataset Suricata and Zeek flagged some packets



Timestamp	event.dataset	source.ip	source.port	destination.ip
2022-01-07 16:16:39.981 +00:00	suricata.alert	192.168.1.216	49763	192.168.1.2
2022-01-07 16:16:09.964 +00:00	suricata.alert	192.168.1.216	49761	192.168.1.2
2022-01-07 16:14:32.032 +00:00	zeek.dns	192.168.1.216	50116	192.168.1.2
2022-01-07 16:14:22.488 +00:00	zeek.pe			
2022-01-07 16:14:22.462 +00:00	zeek.software	192.168.1.216		
2022-01-07 16:14:22.343 +00:00	zeek.file	192.168.1.216	49748	184.50.62.43
2022-01-07 16:14:19.551 +00:00	zeek.ssl	192.168.1.216	49744	20.54.89.15
2022-01-07 16:14:18.247 +00:00	zeek.software	192.168.1.216		
2022-01-07 16:09:42.452 +00:00	zeek.file	192.168.1.216	49739	52.168.112.67
2022-01-07 16:07:35.790 +00:00	suricata.alert	192.168.1.216	49738	2.56.57.108

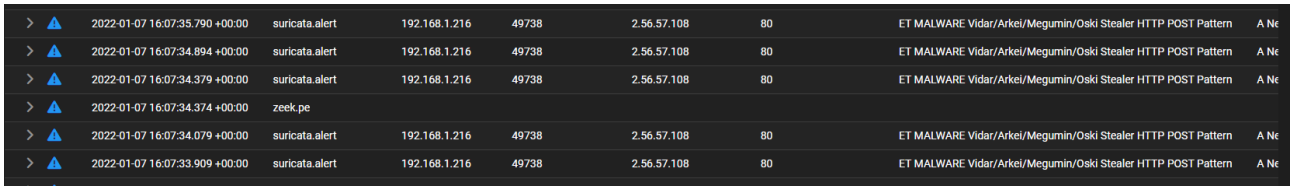
Figure 6

In the Alerts tab 9 counts Malware Vider are shown

Count	rule.name	event.module	event.severity_label	rule.uuid
9	ET MALWARE Vidar/Arkei/Megumin/Oski Stealer HTTP POST Pattern	suricata	high	2034813
3	ET HUNTING SUSPICIOUS Dotted Quad Host MZ Response	suricata	medium	2021076
2	GPL NETBIOS SMB IPC$ unicode share access	suricata	low	2100538
1	ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Chrome_Default.txt)	suricata	medium	2033886
1	ET INFO PE EXE or DLL Windows file download HTTP	suricata	high	2018959

Items per page: 50 1-5 of 5

Figure 7



2022-01-07 16:07:35.790 +00:00	suricata.alert	192.168.1.216	49738	2.56.57.108	80	ET MALWARE Vidar/Arkei/Megumin/Oski Stealer HTTP POST Pattern	A Ne
2022-01-07 16:07:34.894 +00:00	suricata.alert	192.168.1.216	49738	2.56.57.108	80	ET MALWARE Vidar/Arkei/Megumin/Oski Stealer HTTP POST Pattern	A Ne
2022-01-07 16:07:34.379 +00:00	suricata.alert	192.168.1.216	49738	2.56.57.108	80	ET MALWARE Vidar/Arkei/Megumin/Oski Stealer HTTP POST Pattern	A Ne
2022-01-07 16:07:34.374 +00:00	zeek.pe						
2022-01-07 16:07:34.079 +00:00	suricata.alert	192.168.1.216	49738	2.56.57.108	80	ET MALWARE Vidar/Arkei/Megumin/Oski Stealer HTTP POST Pattern	A Ne
2022-01-07 16:07:33.909 +00:00	suricata.alert	192.168.1.216	49738	2.56.57.108	80	ET MALWARE Vidar/Arkei/Megumin/Oski Stealer HTTP POST Pattern	A Ne

Figure 8

The source IP address 2.56.57.108 could give some more information. Using OSINT tools to find out more about the source IP address.

Using AbuseIP.com, the source IP based in Singapore was reported several times. It was associated with multiple cases of misuse.

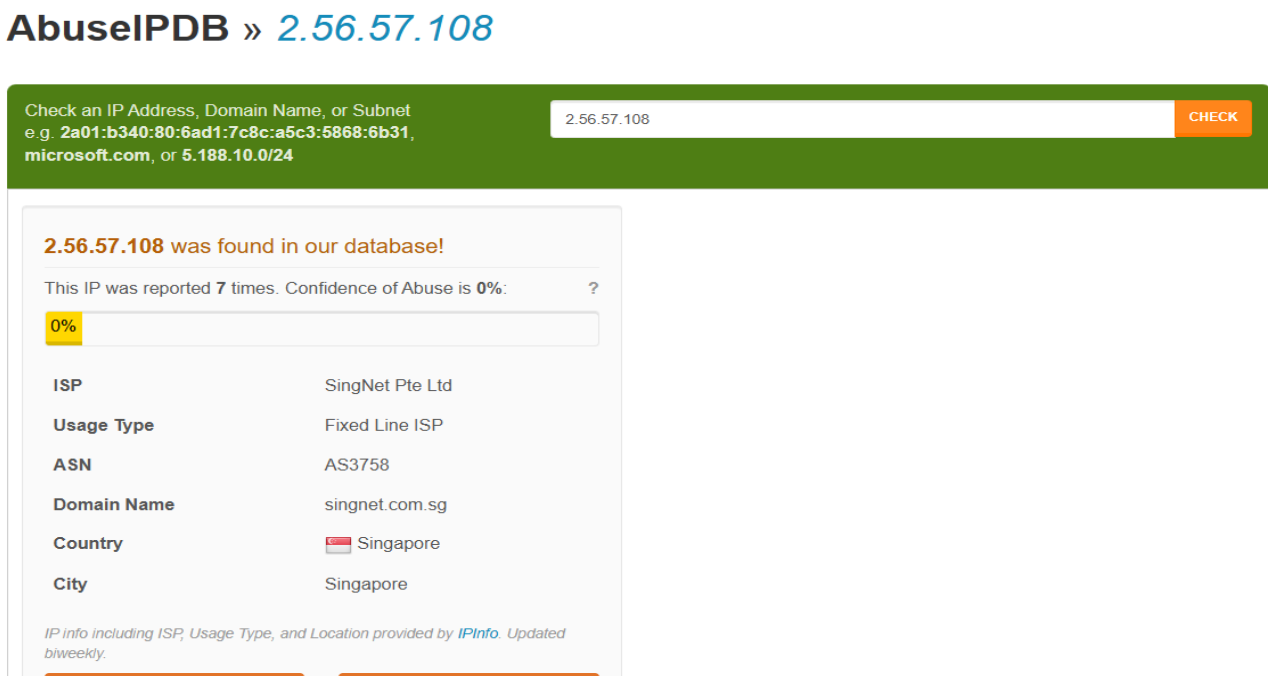


Figure 9

Checking on Virus Total, 4 security vendors flagged the IP address.

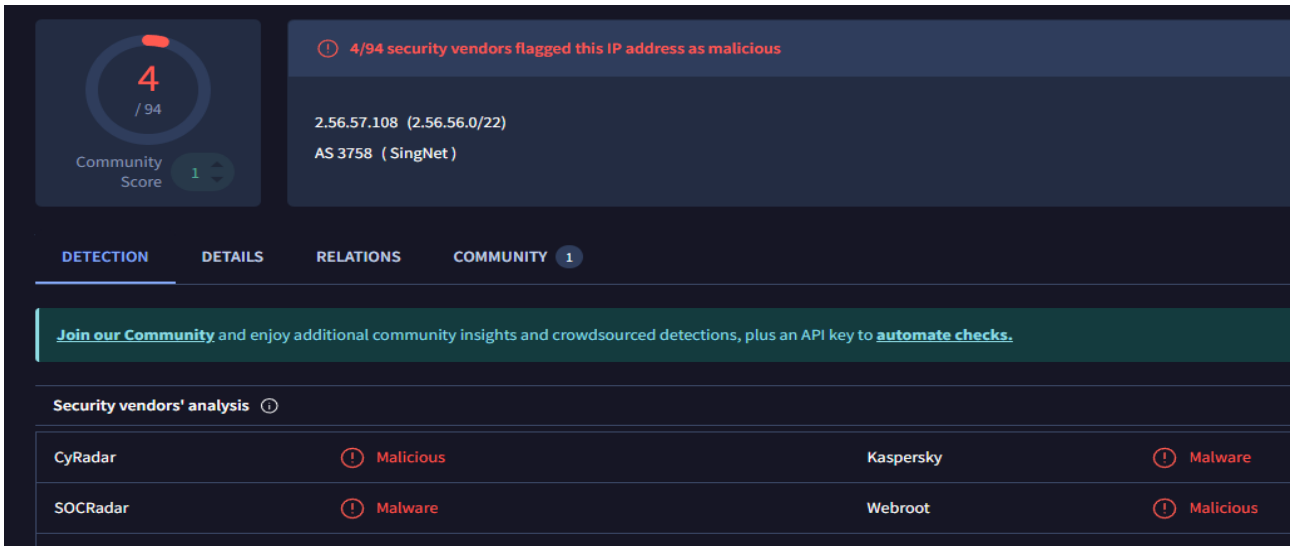


Figure 10

Expanding the event. Under network data decoded. Notice content Type jpeg

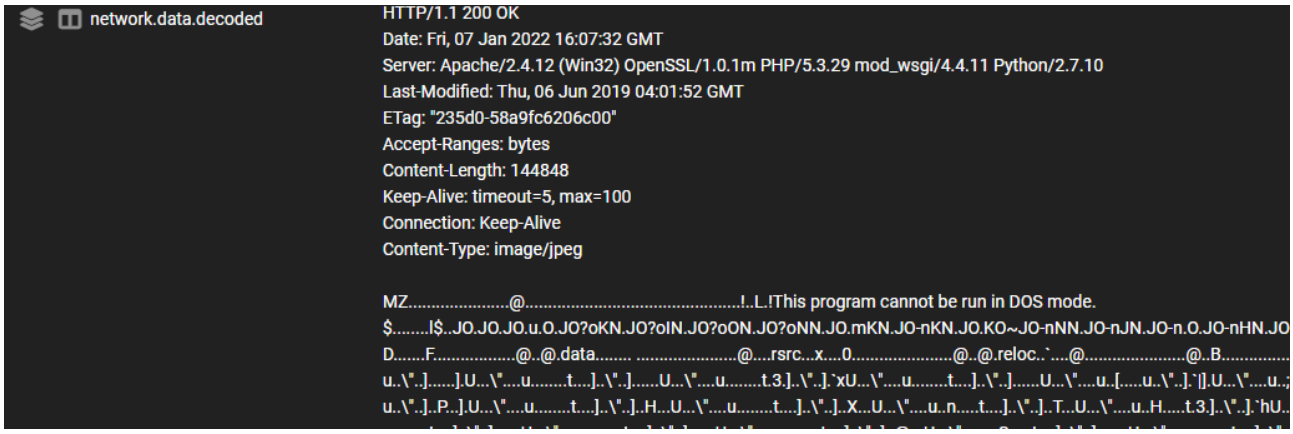


Figure 11

But compared to Gary Kessler Magic number MZ are associated with .exe or DLLs.
Jpegs are as shown in figure 12.

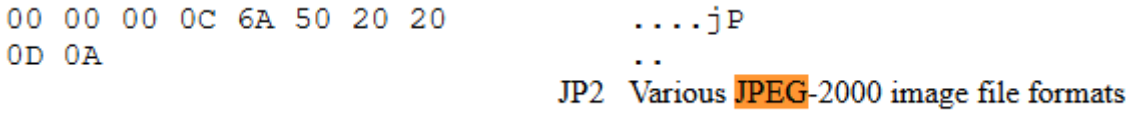


Figure 12

Further scrutiny shows that Suricata flagged a Privacy Violation, and this would warrant further investigation.

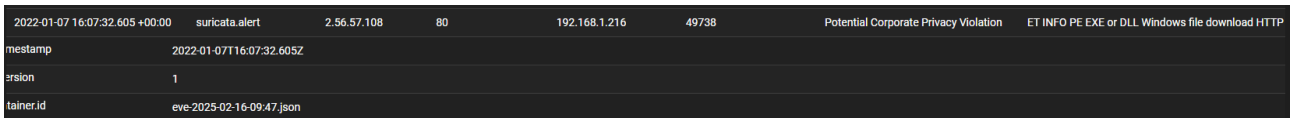


Figure 13

From the brief analysis, it would seem that the source IP address had access and was able to download a file.

Conclusion.

Multiple tools installed in Security Onion make the investigation of cases easier, enabling the security team to identify anomalies in the traffic flow, ultimately confirming the presence of suspicious behaviour. The Security team can have a comprehensive analysis of network traffic and underscores the importance of continuous network monitoring and reinforces the need for proactive threat detection and response measures

Lessons Learned

1. Importing a pcap into Security Onion
2. Searching for anomalies
3. Using OSINT tools to get more details
4. Using Gary Kessler Magic number to identify discrepancies in file extensions
5. Using Online tools e.g. Virus Total, AbuseIP