Darknet Diaries - PCAP Threat Analysis Report: Exercise 1

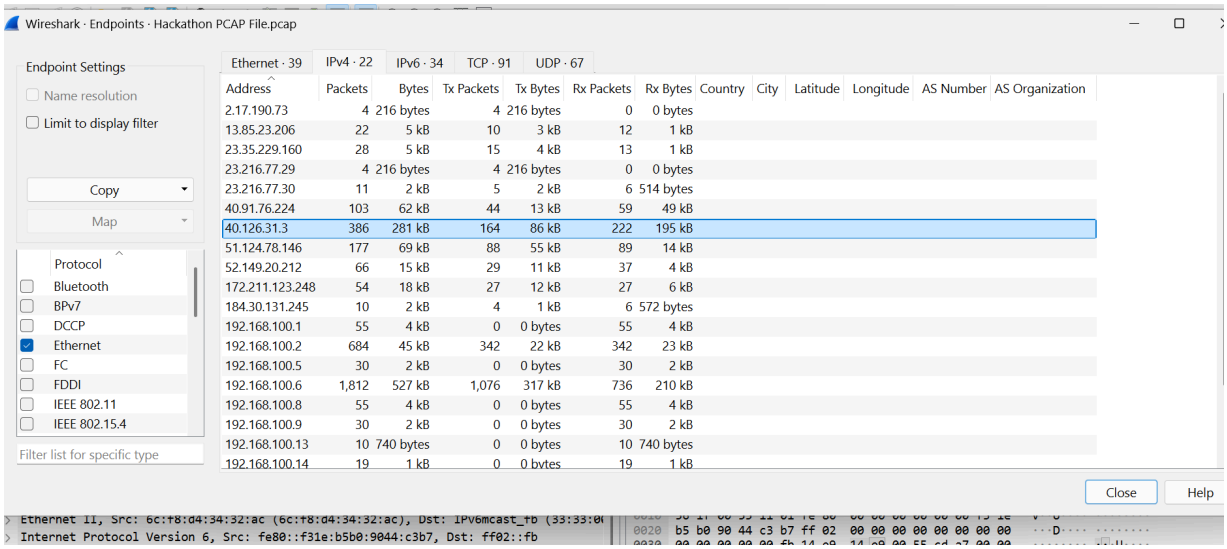
Executive Summary

This report summarizes the analysis of a PCAP file to identify a malicious IP, provide intelligence on the IP and link it back to any malicious activity.

We analyzed the PCAP file using Wireshark, and identified potential malicious IP addresses, and investigated the nature of the malicious activity associated with them using external tools like Virustotal, OTX AlienVault, IP2Location and AbuseIP.

Tools and Methods Used

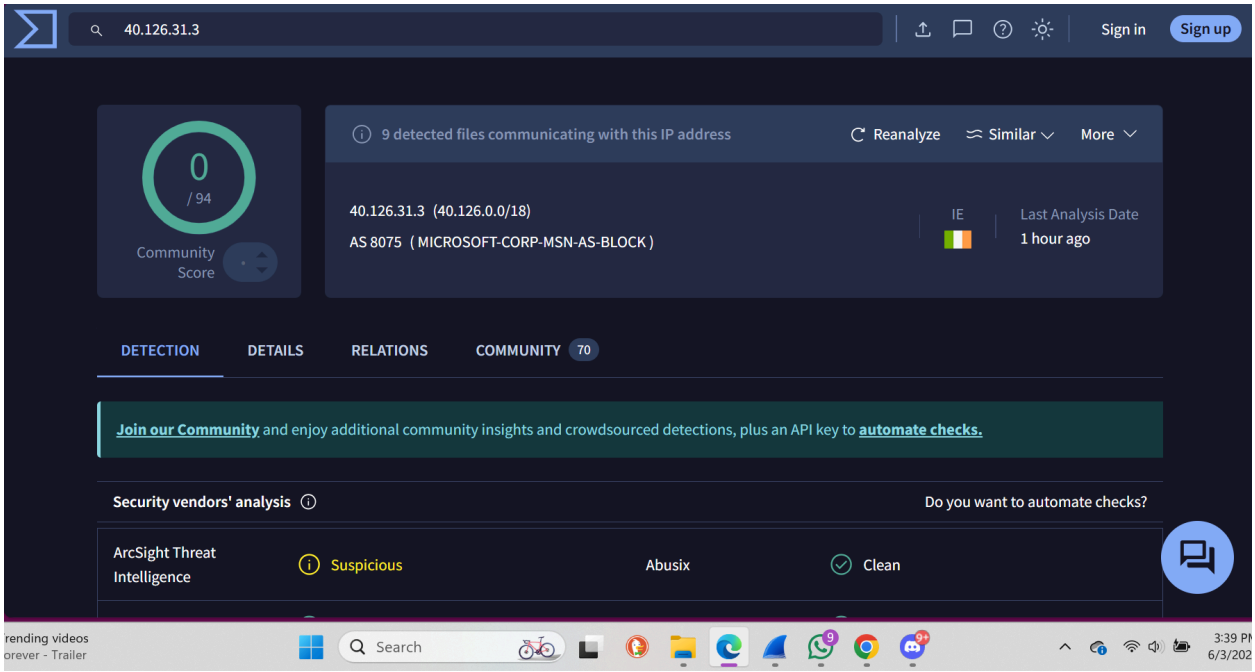
Wireshark for packet capture analysis. We use the endpoints tab `Statistics` to inspect all the IPs in the capture file, and from there we noticed one IP (40.126.31[.]3) that was transmitting a large number of packets (386) with a total of 281kB, which is the largest of the other IPs. On further inspection of this suspicious IP within the PCAP, we realised that it was opening and closing connections frequently, indicating that it could be trying to evade detection, or transmitting data in pieces.



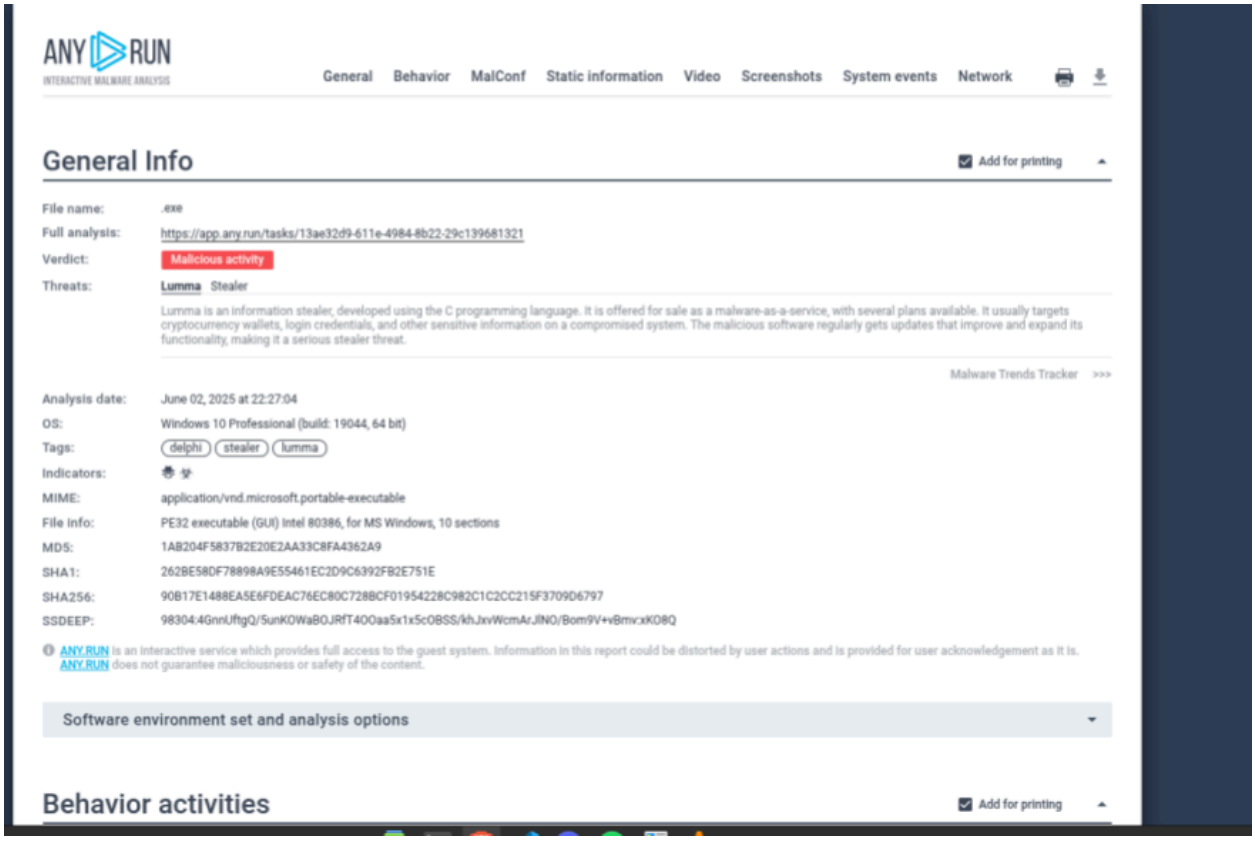
IP2Location - indicated that the IP belongs to Microsoft, and is used as a data center/web hosting, indicating that the malicious actors may be using it to hide suspicious activity and blend in with legitimate traffic.

VirusTotal - we put the highlighted IP VirusTotal for further intelligence on the IP, and although it was not explicitly marked as malicious but clean, one vendor,

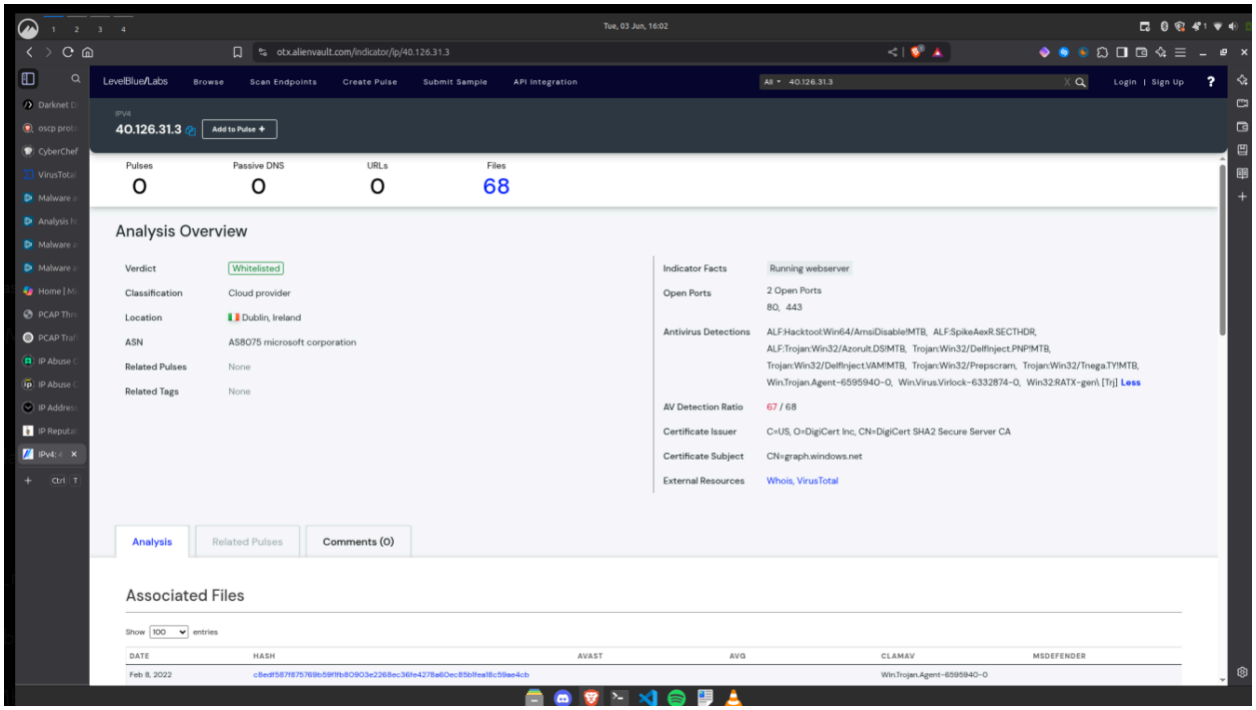
ArcSight Intelligence, marked it as being suspicious, which meant we had to dig a little bit deeper for further intelligence.

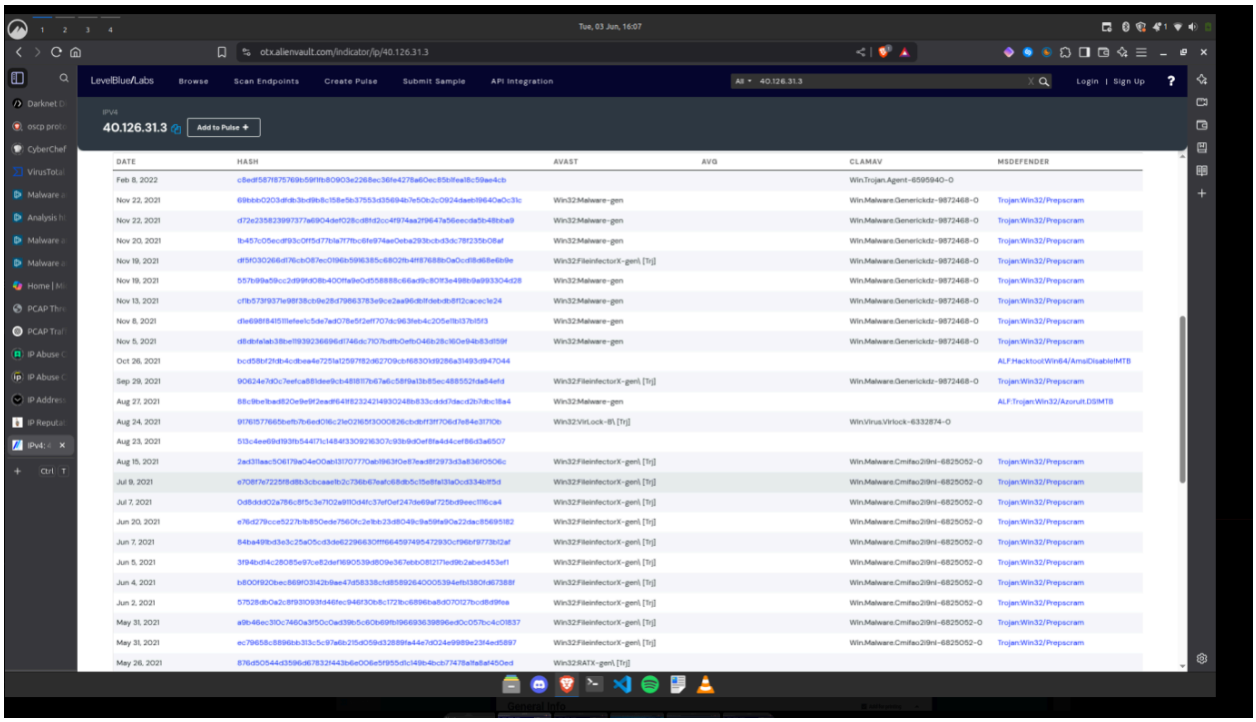


AnyRUN - the Details tab on Virustotal, under google searches led us to AnyRUN tab which indicated the IP as an IOC of phishing malicious activity.



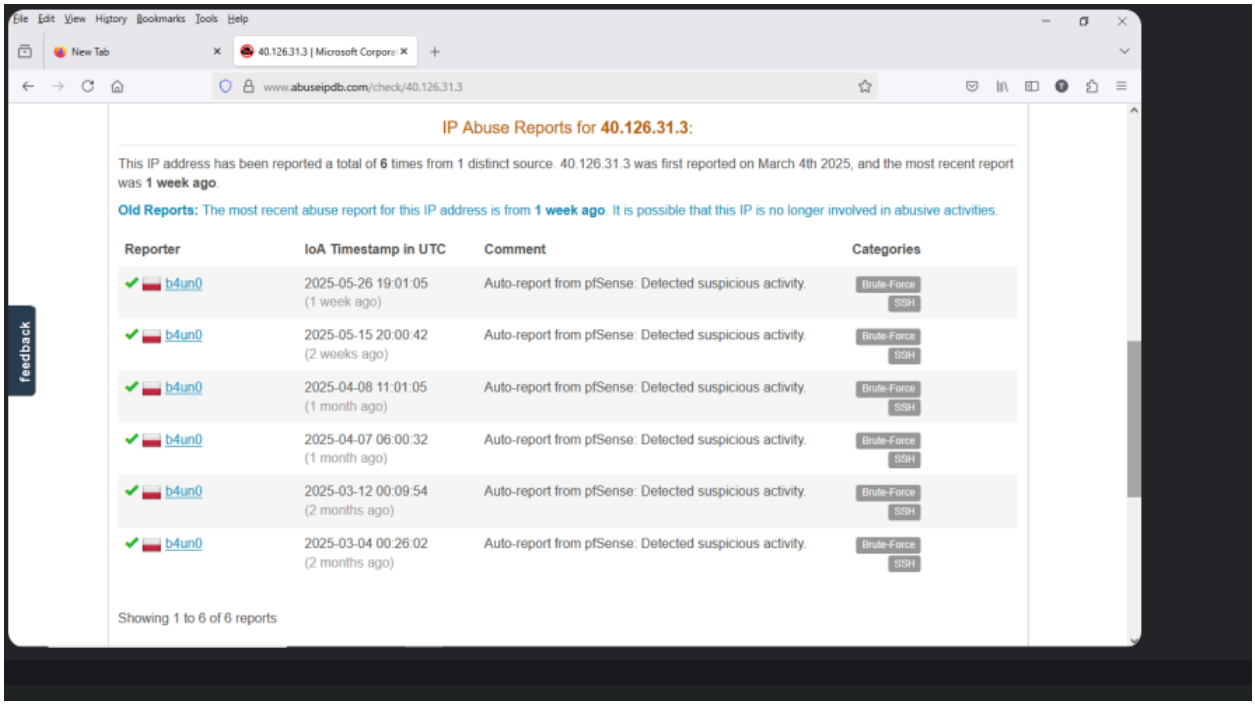
AlienVault OTX - even though AlienVault OTX shows the IP as whitelisted, VirusTotal flagged it with a *67/68* antivirus detection rate. This means the IP is very likely linked to malware or C2 activity, even if it looks safe on the surface. It's a reminder that not all legit-looking traffic is safe, and it's important to check multiple sources before trusting an IP.





AbuseIPDB -This IP address has been reported **6 times**, all by the same source. The reports are from the past **two months**, with the **latest one just a week ago**. Each time, it was flagged for trying to do a **Brute-Force SSH attack**. That means

the IP kept trying to guess usernames and passwords to break into systems.



Mitigations & Recommendation

- Block IP 40.126.31[.]3 on your firewall and monitoring tools.
- Check any systems that communicated with this IP for signs of compromise.
- Update antivirus and enable detection for related threats.
- Use strong passwords and lockout rules to stop brute-force attacks.
- Set up a SIEM like Wazuh to watch for future suspicious activity.

Conclusion

The IP address *40.126.31[.]3* is confirmed to be **malicious** based on packet behavior and external threat intelligence. The behavior includes abnormal communication patterns, likely scanning or brute force attempts. This IP should be **blocked** at the firewall level, and all endpoints communicating with it should be **reviewed for compromise**.

Task 2
Objectives for Malicious File Analysis

Summary

In this exercise we were supplied with a malicious file scan on the Intezer platform. The scan output linked the malicious file to a known threat actor, known as the Play ransomware gang.

The key port utilized by the Play ransomware group is port 135, which is a port used for the *Remote Procedure Call (**RPC**) Endpoint Mapper* service, which allows other systems to identify what services are available on a machine and on which port they can be found.
This port is essential for remote access and management, particularly in environments like *Microsoft Active Directory* where many critical services depend on it.

However, leaving port 135 open can pose significant security risks, including the potential for unauthorized access and exploitation by attackers. To mitigate these risks, strong authentication measures should be implemented, and the port should be restricted to necessary traffic only.

The main port of connections from the Play ransomware group is port 445, used for ***Server Message Block (SMB)*** protocol, which facilitates file and printer sharing within a network. Leaving this port open can serve as an entry point for malicious attackers allowing them to execute malicious code and malware through this port on the victim machines.

It is important to note that port 445 became particularly notorious after the notorious *WannaCry* ransomware attack in 2017, which exploited vulnerabilities in the SMB protocol to spread rapidly across networks. This highlights the importance of securing

port 445 against unauthorized access and potential exploits. Thus, securing access to this port should be of utmost importance to organizations.

Observed Registry Activity:

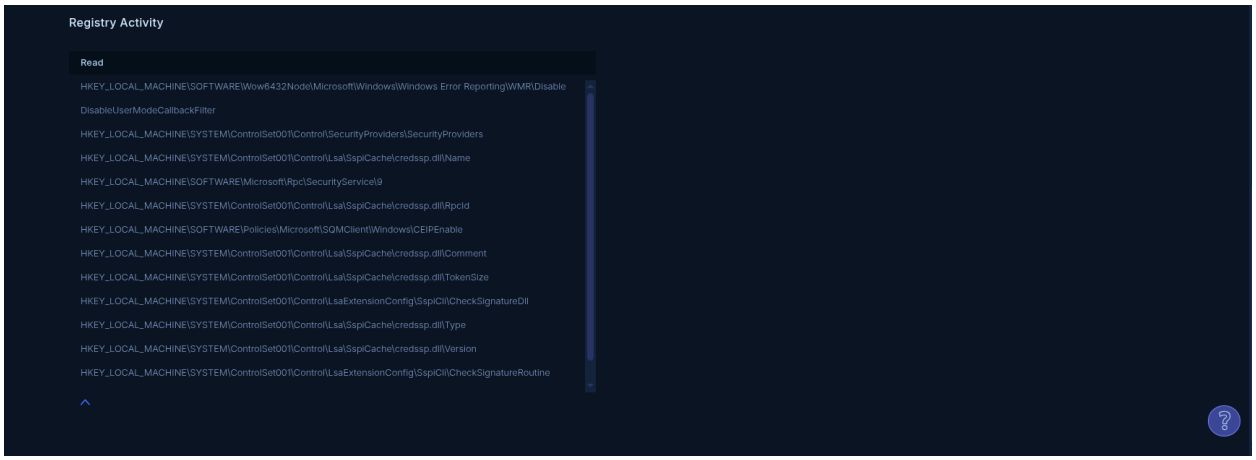
- *HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable*
  - ★ This entry is part of **Windows Error Reporting** (WER), a system that collects and sends crash reports to Microsoft when something goes wrong on a computer. The attacker is likely trying to **turn off error reporting** for some (potentially malicious) apps to stay hidden. It's like telling the computer, “Don’t tell anyone if I break something.”
- *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options*
  - ★ This setting controls how **user-mode callback filtering** works. It’s like **turning off a security camera** that watches how programs behave — so the malware can move more freely without getting caught.
- *HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SecurityProviders\SecurityProviders*
  - ★ This key lists the **security provider DLLs (dynamic-link libraries)** used by Windows to securely handle logins and secure data. This is like handing someone a list of who’s allowed to guard your house — and the attacker sneaks their own name onto it. Windows then **trusts** their malicious code as if it were a real part of the security system.
- *HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\SspiCache\credssp.dll\Name*
  - ★ This key is part of the **SSPI cache** (*SspiCache*), which stores information about **loaded security packages** (DLLs like *credssp.dll*).This entry shows that *credssp.dll* (used for logging in securely) is active. On its own, it’s **not suspicious**, but it helps confirm whether **Windows is using the expected files** — or something malicious in disguise.
- *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\SecurityService\9*
  - ★ This key is part of Windows **RPC (Remote Procedure Call)** settings.This key helps Windows know **which security system to use for secure connections**. If an attacker messes with it, they could **hijack encrypted traffic** or break security features.
- *HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\SspiCache\credssp.dll\RpcId*
  - This key belongs to the **SSPI cache** under the **LSA (Local Security Authority)** section of the registry. This is like a **tag number** that Windows

uses to keep track of who's handling secure logins. On its own, it's not dangerous — but if the file it points to (credssp.dll) has been replaced, the system might still **trust a fake**.

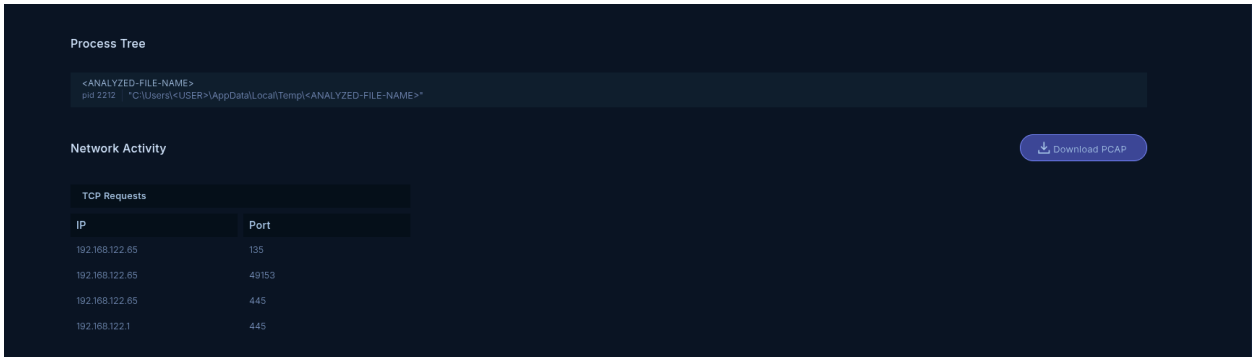
- *HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SQMClient\Windows\CEIPEnable*
    - ★ This setting controls **Windows Customer Experience Improvement Program (CEIP)**.This controls whether Windows reports how it's being used. An attacker might **turn it off** so that **no clues about their activity** get sent to Microsoft.
- *HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\SspiCache\credssp.dll\Comment*
    - ★ This entry is part of the **SSPI cache** for credssp.dll, which, as mentioned earlier, is used for **secure authentication** — especially for **Remote Desktop** and **Single Sign-On**.This is like a **label on a file** that says what it's supposed to do. Normally safe, but if a hacker puts their own fake file in place, this label might **hide the truth** or act as a cover.
- *HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\SspiCache\credssp.dll\TokenSize*
    - ★ This entry relates to *credssp.dll*, the **Credential Security Support Provider**, which handles secure logins — especially over **Remote Desktop Protocol (RDP)**.This sets the **size of the "security pass"** used during logins. If it's changed, it might help the attacker sneak in more access rights or support special tools they're using.
- *HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\LsaExtensionConfig\SspiCli\CheckSignatureDll*
    - ★ This key relates to the **LSA (Local Security Authority) extensions** that manage how Windows verifies security-related DLLs.This entry points to the system that checks if security files are legit. If an attacker messes with it, they can **sneak in fake security files** without Windows noticing.
- *HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\SspiCache\credssp.dll\Type*
    - ★ This is another entry in the **SSPI cache** for the credssp.dll security provider.This tells Windows what kind of security job credssp.dll does. It's like a job title on a security badge. If it's wrong or missing, it could mean the system has been tricked.
- *HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\SspiCache\credssp.dll\Version*
    - ★ This entry stores the **version number** of the credssp.dll security provider loaded by Windows.This tells you **which edition** of the secure login file is

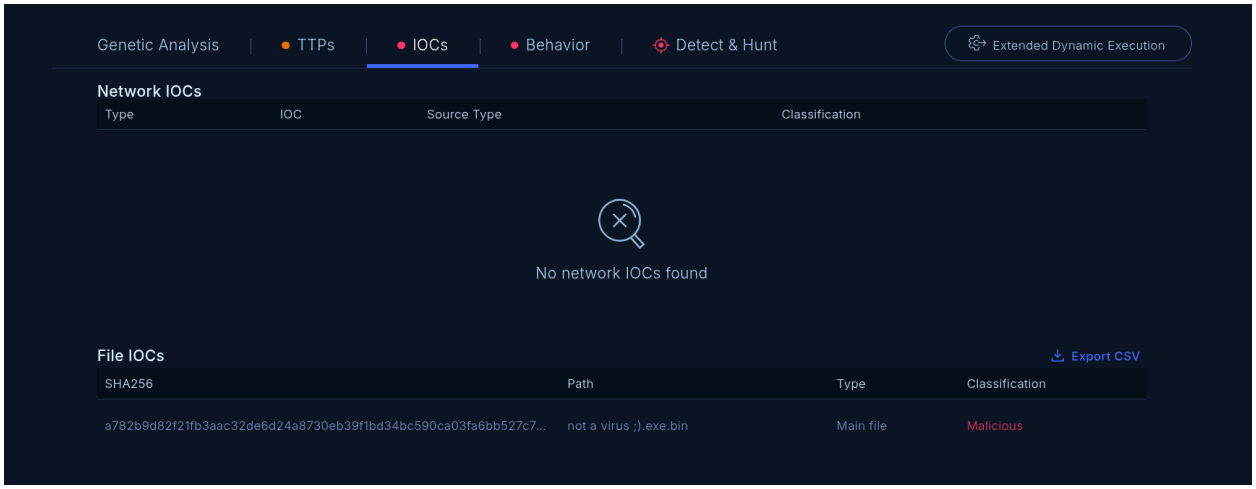
running. If it’s not what it should be, it might mean the attacker swapped it for a fake.

- *HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\LsaExtensionConfig\SspiCli\CheckSignatureRoutine*
  - ★ This key points to a **routine (function)** used by Windows to **verify digital signatures** of security-related DLLs.This is the “checker” function that confirms security files are genuine. If it’s messed with, bad files can sneak in without being caught.
- *HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\SspiCache\credssp.dll\Capabilities*
  - ★ This entry describes the **features or abilities** that the *credssp.dll* security provider supports.This lists what the secure login file can do. If it's different from what’s normal, it might be a sign the file is **not trustworthy**.



IOC	**IOC Type**
192.168.122.65	Network
192.168.122.1	Network
Port 135	Network
Port 445	Network
Port 49153	Network
a782b9d82f21fb3aac32de6d24a8730eb39f1bd34bc590ca03fa6bb527c74fec	File





Recommendations

Port 135, if not in use, should be blocked to minimize scanning of running services and their relevant ports by attackers.
To secure port 445, organizations should implement firewall rules to block unnecessary traffic on this port, especially from external networks. Additionally, keeping systems updated with the latest security patches can help prevent known vulnerabilities from being exploited.

Mitre Att&ck Mapping (Task 3)

Domain	ID	Name	Use
Enterprise	T1560 .001	Archive Collected Data: Archive via Utility	Play has used WinRAR to compress files prior to exfiltration.
Enterprise	T1059 .001	Command and Scripting Interpreter: PowerShell	Play has used Base64-encoded PowerShell scripts to disable Microsoft Defender
	.003	Command and Scripting Interpreter: Windows Command Shell	Play has used a batch script to remove indicators of its presence on compromised hosts.
Enterprise	T1030	Data Transfer Size Limits	Play has split victims' files into chunks for exfiltration.
Enterprise	T1587 .001	Develop Capabilities: Malware	Play developed and employ Playcrypt ransomware
Enterprise	T1048		
Enterprise		Exfiltration Over Alternative Protocol	Play has used WinSCP to exfiltrate data to actor-controlled accounts.

Enterprise	T1190		
Enterprise		Exploit Public-Facing Application	Play has exploited known vulnerabilities for initial access including CVE-2018-13379 and CVE-2020-12812 in FortiOS and CVE-2022-41082 and CVE-2022-41040 ("ProxyNotShell") in Microsoft Exchange
Enterprise	T1133	External Remote Services	Play has used Remote Desktop Protocol (RDP) and Virtual Private Networks (VPN) for initial access
Enterprise	T1083	File and Directory Discovery	Play has used the Grixba information stealer to list security files and processes.
Enterprise	T1657	Financial Theft	Play demands ransom payments from victims to unencrypt filesystems and to not publish sensitive data exfiltrated from victim networks.
Enterprise	T1562 .001	Impair Defenses: Disable or Modify Tools	Play has used tools including GMER, IOBit, and PowerTool to disable antivirus software

Enterprise	T1057	Process Discovery	Play has used the information stealer Grixba to check for a list of security processes.
Enterprise	T1021 .002	Remote Services: SMB/Windows Admin Shares	Play has used Cobalt Strike to move laterally via SMB.
Enterprise	T1018	Remote System Discovery	Play has used tools such as AdFind, Nltest, and BloodHound to enumerate shares and hostnames on compromised networks.
Enterprise	T1518 .001	Software Discovery: Security Software Discovery	Play has used the information-stealing tool Grixba to scan for anti-virus software
Enterprise	T1082	System Information Discovery	Play has leveraged tools to enumerate system information.
Enterprise	T1016	System Network Configuration Discovery	Play has used the information-stealing tool Grixba to enumerate network information
Enterprise	T1078 .002 .003	Valid Accounts Domain Accounts Local Accounts	Play has used valid VPN accounts to achieve initial access. Play has used valid domain accounts for access. Play has used valid local accounts to

			gain initial access.

The threat actor in question is the **Play** ransomware group, also known as ***PlayCript***. This threat actor is known to mainly target the following sectors/industries:

- Government
- Education
- Manufacturing
- Healthcare
- Financial Services
- IT Service Providers

The primary motive for this threat actor is financial gain through ransom payments, and the secondary motive is extortion. The threat actor is known for its double extortion model, whereby they exfiltrate victim organization's data after having encrypted it, and then demanding ransom.

Play (aka *PlayCrypt*) is a ransomware gang that mainly wants money. They break into companies using known software vulnerabilities or stolen credentials, then move through the system using services like *Virtual Private Networks (VPN)* and *Remote Desktop Protocol (RDP)*.

Once they're inside, they use tools like Cobalt Strike and Mimikatz to dump passwords, and they turn off antivirus, delete logs, and steal data.

They don't just encrypt files, they also threaten to leak stolen data if the victim doesn't pay.

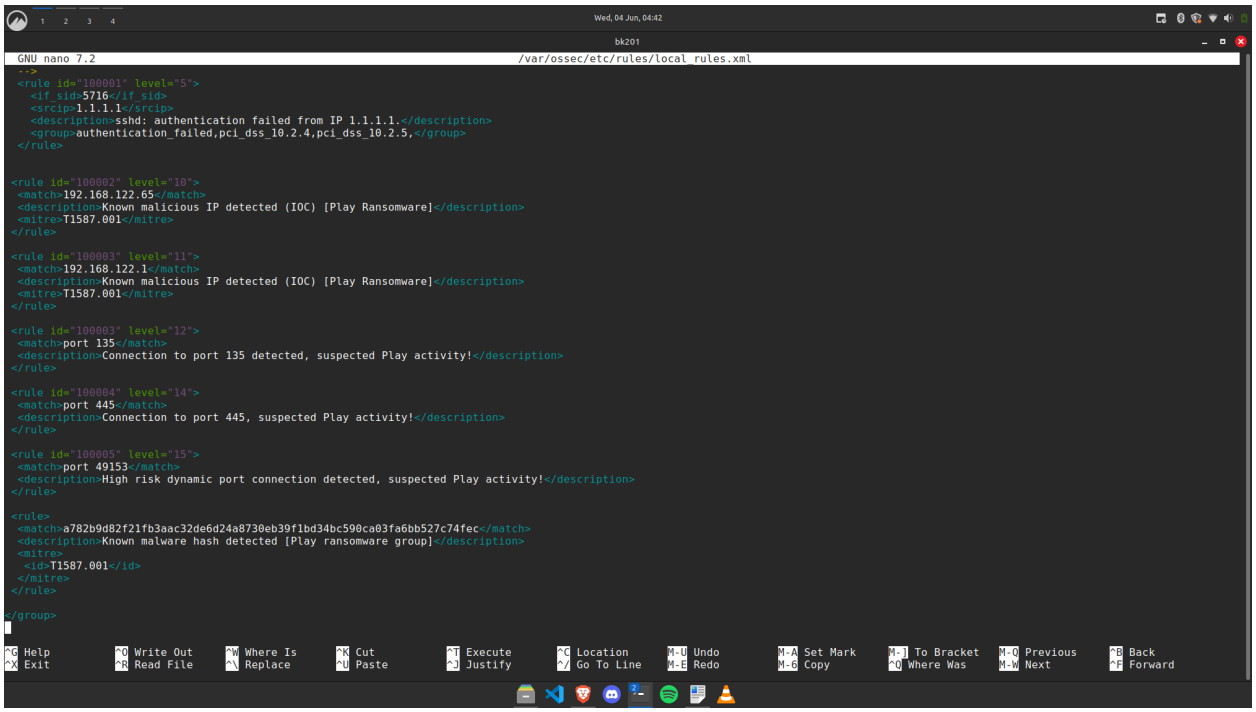
The industries they have hit include governments, schools, healthcare, banks, and tech companies, basically any place with sensitive data.

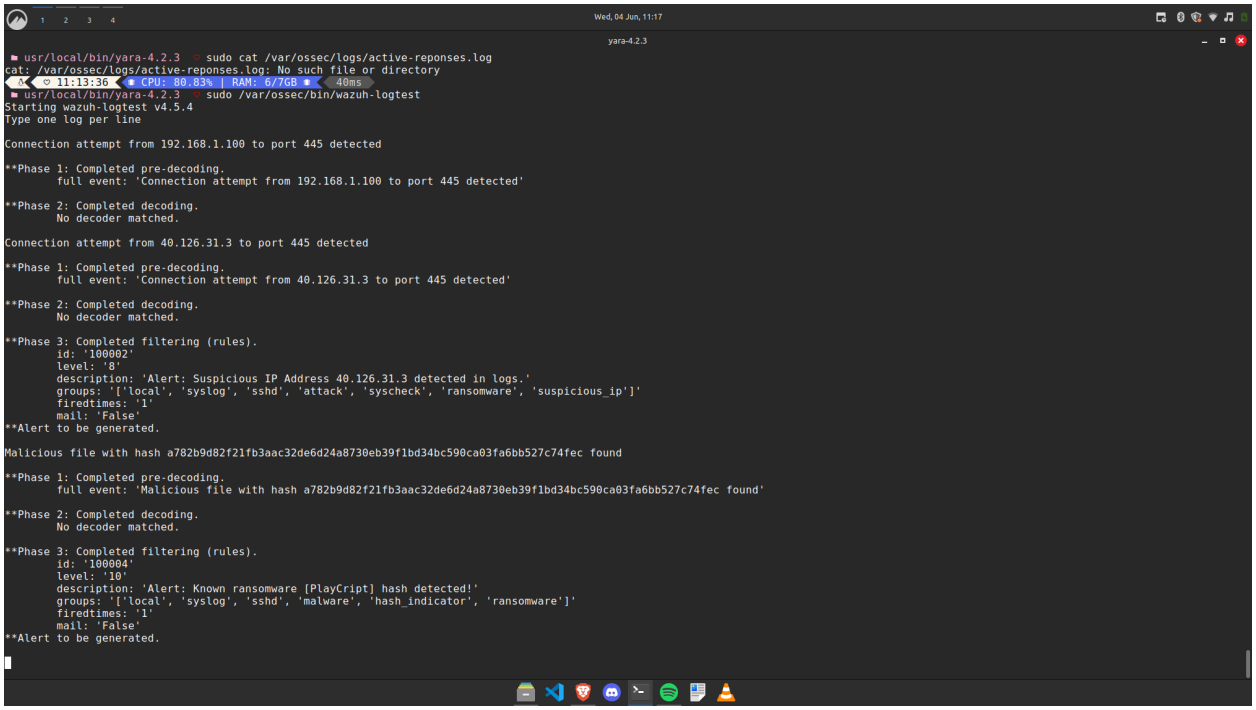
We used the **MITRE ATT&CK** framework to map out their *Tactics, Techniques and Procedures (TTPs)*. It helps show exactly how they attack, from initial access, to lateral movement, to data exfiltration and impact.

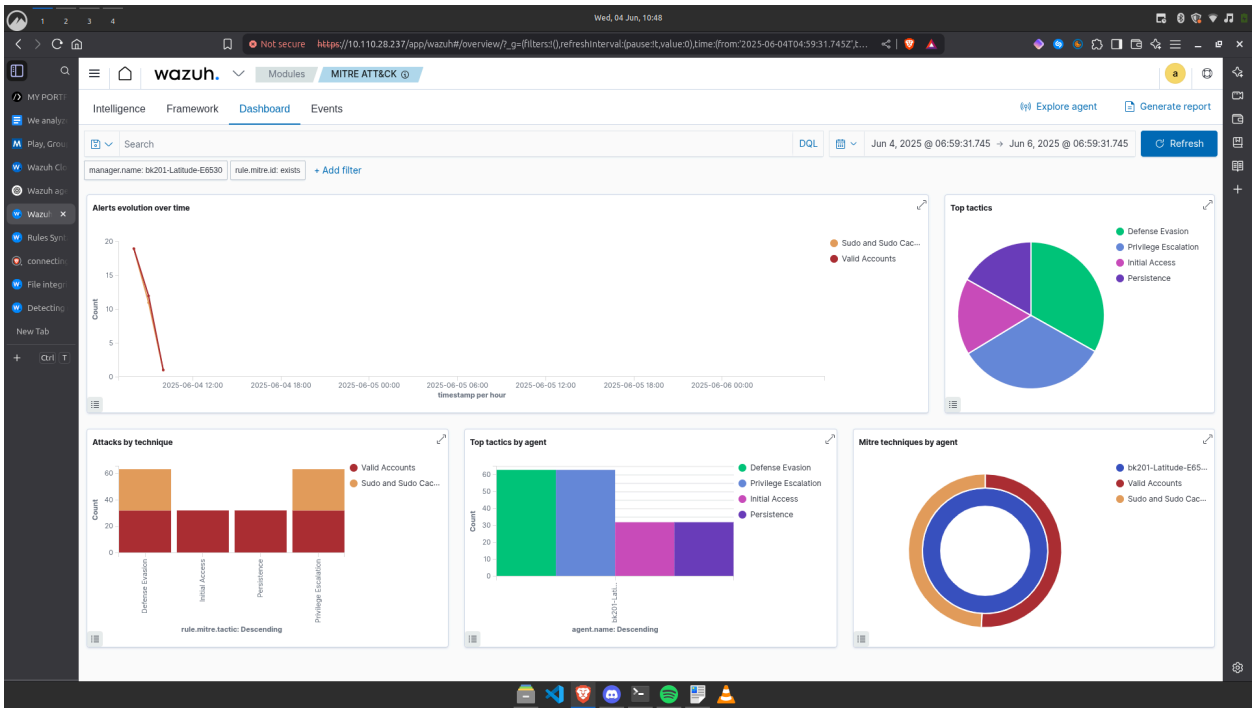
Build a Solution (Task 4)

For this task we were tasked with building a ***Security Incident and Event Management (SIEM)*** solution that can be used to protect against the threats identified in the previous tasks, namely, Play ransomware group's TTPs and keeping their IOCs locked out.

For building the SIEM tool we were supposed to use Wazuh SIEM alongside custom YARA rules for detection of the IOCs.







Getting Wazuh to use the locally defined YARA rules and display them on its GUI dashboard proved to be a challenging task, as it took more than 8 hours of troubleshooting to make it work with no luck. Thus, an optimal conclusion was to utilize the above YARA rules on every endpoint within the network, and possibly use a different SIEM tool, either Splunk, Elastic, or another.

Marketing Proposal: SIEM Tool Solution

1. Introduction

This marketing proposal outlines a strategy to promote a cybersecurity threat analysis and intelligence solution. Our solution is based on real-world threat data from a PCAP analysis and malware registry investigation, identifying active threats such as brute-force attacks, phishing campaigns, and ransomware activity (PlayCrypt group).

2. Objectives

The main goal is to raise awareness about the capabilities of our threat analysis tool and attract security-conscious clients. We position our solution as essential for any organization that wants to detect and stop threats early, especially ransomware attacks.

3. Target Audience

- IT managers and security analysts
- Small to medium businesses (SMBs)
- Government and healthcare sectors
- Educational institutions and financial services

4. Value Proposition

Our solution uses real-world packet capture (PCAP) data and threat intelligence tools to detect active threats. We help organizations understand who's attacking them, how they do it, and what to do next. We simplify complex data into clear actions: block malicious IPs, patch vulnerable services, and monitor with SIEM.

5. Marketing Strategy

We'll use the following channels:

- LinkedIn posts targeting IT professionals

- Webinars explaining how the Play ransomware works

- Blog posts breaking down the malware registry activity

- Active social media presence showing the tool in action

6. Call to Action

Encourage audiences to download the full threat report and sign up for a free 7 days threat assessment. This gives them real value while introducing them to your service.

7. Sample Marketing Content

Headline: 'A <well-known cloud> IP? Think Again.'
Body: We analyzed a clean-looking IP (40.126.31[.]3). One vendor flagged it as suspicious. Further digging revealed phishing activity and SSH brute-force attacks linked to this IP. Want to see the full investigation?

Download the full threat report now.
#CyberSecurity #ThreatIntel #PlayRansomware

8. Conclusion

This proposal shows a practical way to market our solution using a real investigation. By sharing the findings and giving useful advice, we build trust and attract clients. Our message is simple: we help you spot threats others miss.

References

Play, Group G1040 | MITRE ATT&CK®
https://attack.mitre.org/software/S1162/