Abertay University

CMP416 Advanced Digital Forensics - Unit 1

Michael Awoyemi

2024/25

Contents

Introduction

Background

In today's digital landscape, organisations face significant threats from cyberattacks that could disrupt operations and compromise sensitive data. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are critical components of cybersecurity, serving to monitor network traffic for suspicious activity and responding to potential threats. Firewalls act as a barrier, controlling incoming and outgoing traffic based on predetermined security rules, while system monitoring tools provide real-time insights into system health and performance.

Despite their importance, these technologies are not without challenges. Some organisations struggle with the volume of alerts generated, leading to alert fatigue and the potential for genuine threats to be overlooked. Additionally, improperly configured firewall rules can create vulnerabilities, allowing unauthorised access to sensitive information. The integration of IDS, IPS, and monitoring solutions requires a strategic approach to ensure comprehensive coverage without overwhelming security teams.

This report explores the pressing issues within these security technologies, emphasising the need for improved management, streamlined alert systems, and effective rule configuration. By addressing these challenges, organisations can enhance their cybersecurity posture, reduce risks, and ensure the integrity of their digital environments.

Aim

The objective of this project is to successfully create multiple snort alert rules to examine a network traffic capture file and identify the compromised computer, to conclude when, where, how and what happened.

METHODOLOGY

OVERVIEW OF PROCEDURE

To investigate the network traffic for signs of malicious activity, a Wireshark packet capture (pcap) file was generated, encompassing a comprehensive range of both inbound and outbound traffic. This pcap capture serves as a critical resource for identifying who was involved, when the activity occurred, where it took place, and what actions were taken.

To thoroughly analyse this network traffic data, a variety of specialized tools were employed, including Snort, Wireshark, T-shark, and TCPdump. Each of these tools offers unique functionalities that help in dissecting the pcap file. For example, Wireshark provides a graphical interface for visualizing packet details, while TCPdump allows for command-line packet analysis. Snort acts as an intrusion detection system, applying network rules to recognize unwanted threats within the network traffic. Deploying all these tools helped to gain a clear understanding of the network's behaviour and pinpoint any irregularities that may indicate malicious activity.

SNORT

Various alerts were created to effectively identify and monitor malicious traffic within the network using the open-source intrusion detection system, Snort.

One particular alert was configured to detect traffic from any port of any IP going to any port of any IP that contained .exe files downloaded over HTTP, capturing the HTTP URI or looking for a specific MIME type. As illustrated in Figures 2 and 3, the alerts showed that at 13:43:52, the IP address 192.168.1.96, through port 49190, successfully downloaded an executable file from the IP address 145.131.10.21, which is associated with the domain vantagpointtechnologie.com. This was followed closely by another alert triggered at 13:43:54, where a second executable file was downloaded. This time, the transaction occurred on port 49191 from the IP address 143.95.151.192, linked to the domain lounge-haarstudio.nl.

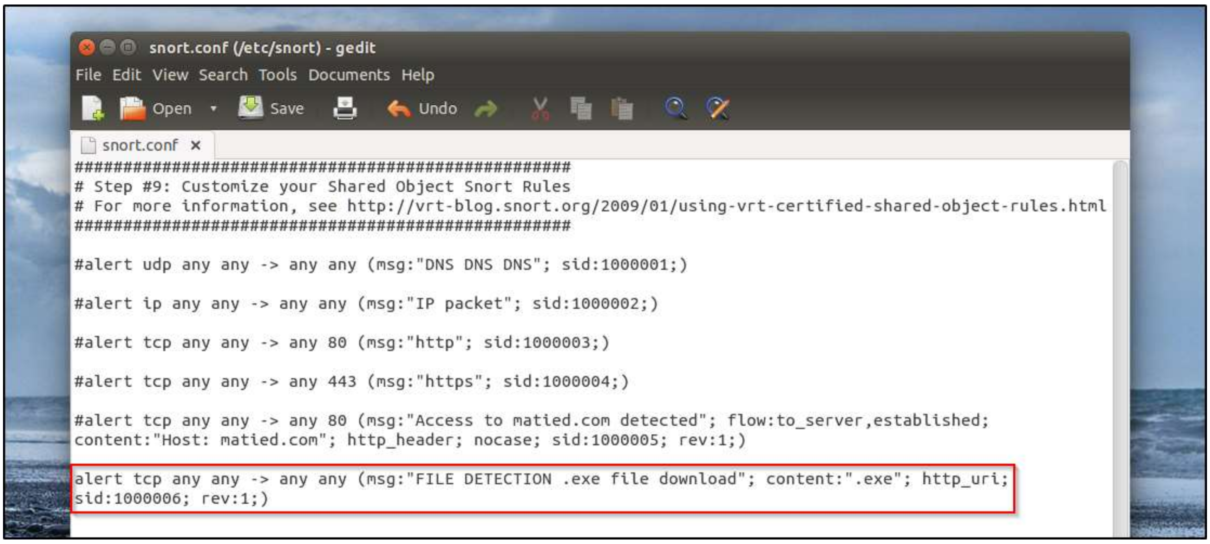


Figure 1: snort alert creation.

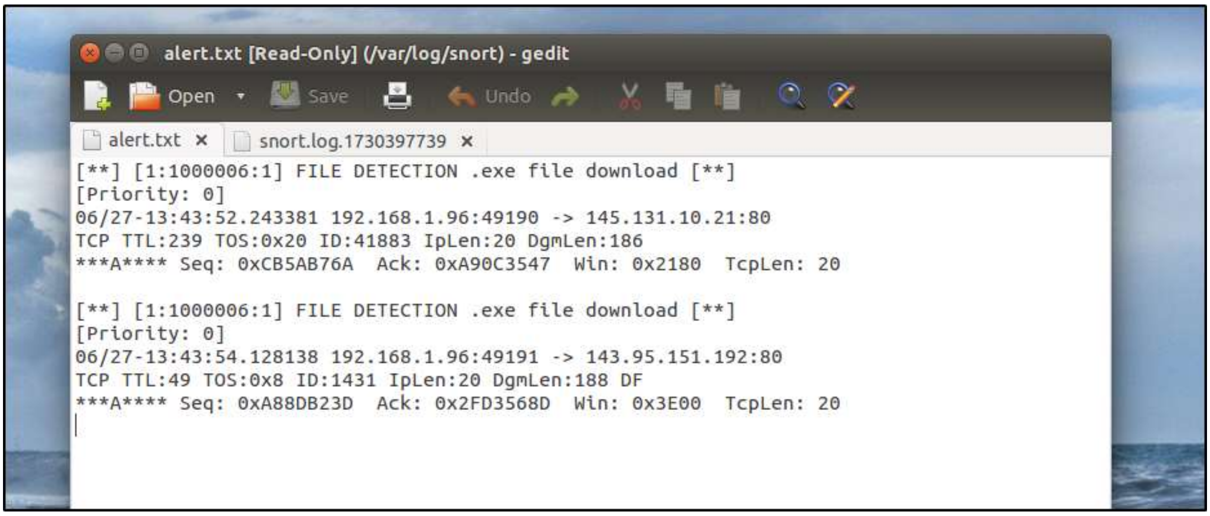


Figure 2: snort alert output detecting .exe downloaded files.

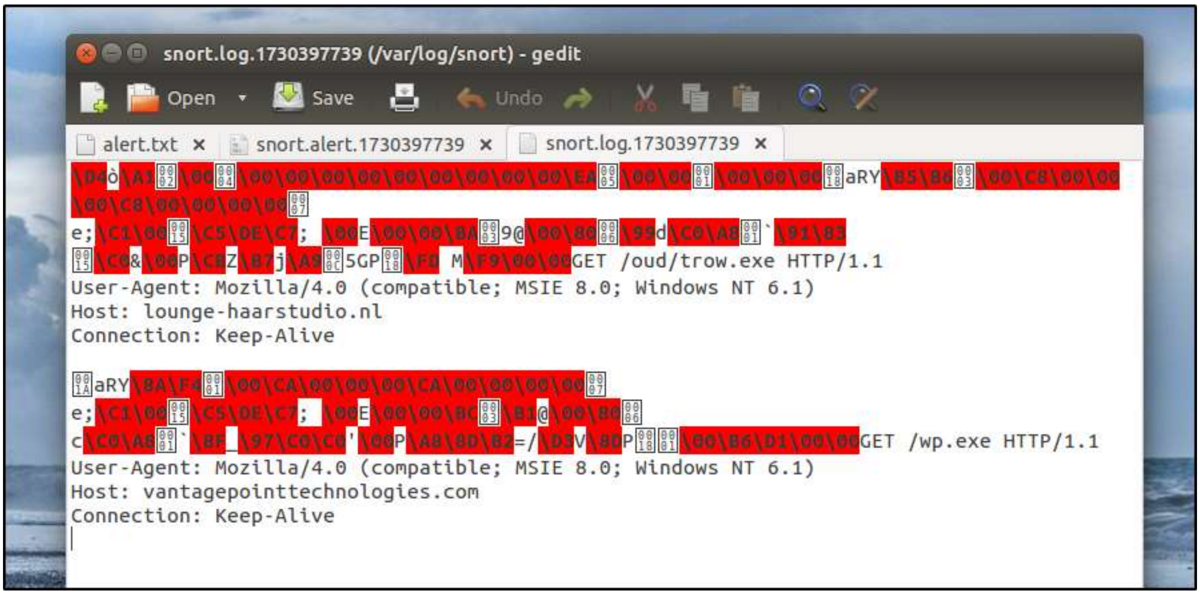


Figure 3: output of snort's log file showing the URLs.

WIRESHARK

From the snort alerts and the Wireshark pcap file, IP 192.168.1.96 was found to be accessing various websites and downloading files from unknown websites. A quick DHCP search helped determine the MAC address of the device alongside the owner of the device. This came to be a Dell computer with the hostname FlashGordon-PC. This detailed information not only confirmed the specific device involved but also permitted the identification of the owner for possible follow-up actions regarding the unusual network activity.

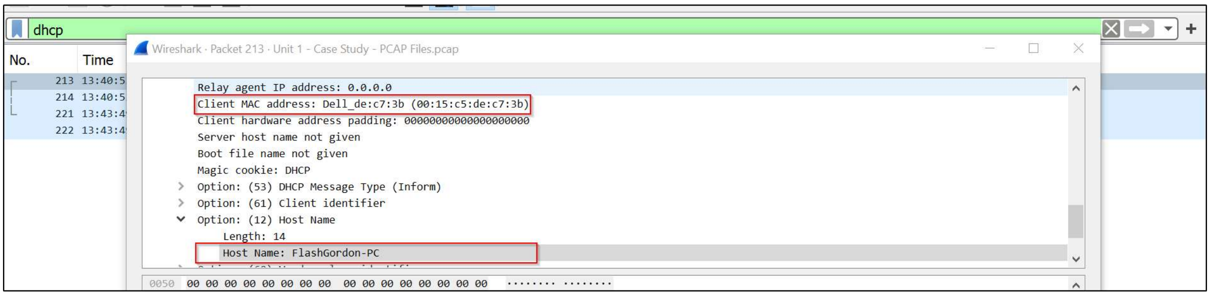
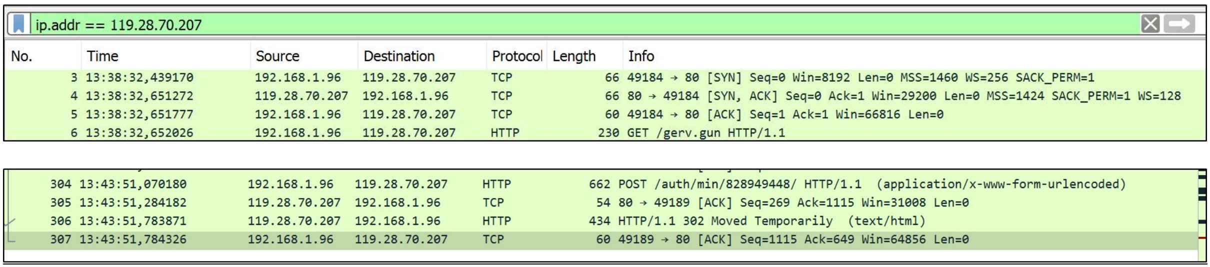


Figure 4: DHCP information of suspicious address.

When checking the traffic, the first 6 packets were between the same host (...96) and a web server 119.28.70.207 (matied.com). Once the TCP connection was established following the 3-way handshake SYN//SYN-ACK//ACK, the first download of an unknown file was found. The file downloaded via a GET request was named gerv.gun and lasted from 13:38:32 to 13:43:51.



Figures 5 & 6: beginning of gerv.gun and end.

Analysing the following traffic after the gerv.gun, another 2 DNS queries led to the download of files: trow.exe from 145.131.10.21 (lounge-haarstudio.nl) and wp.exe from 143.95.151.192 (vantagepointtechnologies.com).

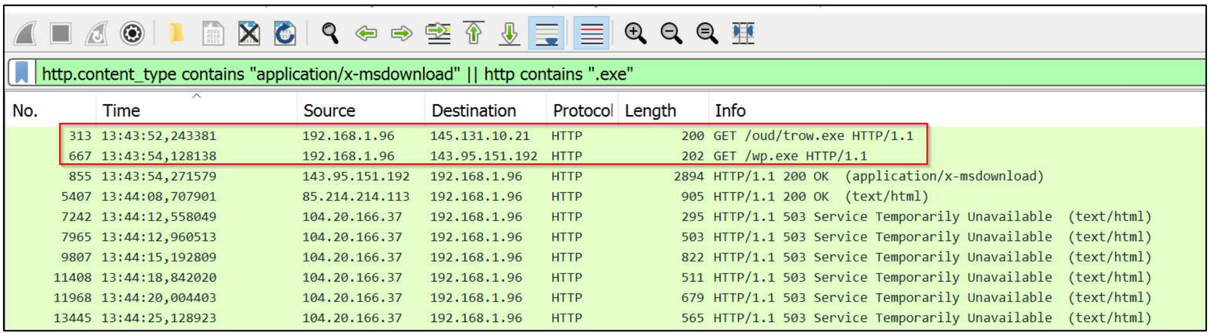


Figure 7: http.content_type contains "application/x-msdownload" || http contains ".exe".

The Wireshark option to export the http object was then used to download the 2 files (wp.exe and trow.exe).

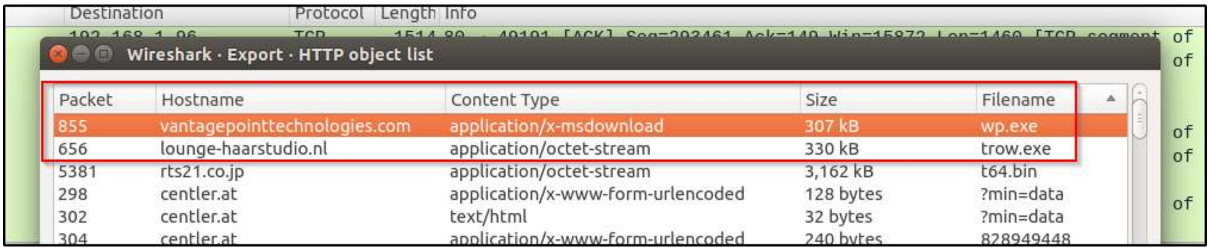


Figure 8: Wireshark export object http.

TCPdump

When analysing the pcap file using TCPdump, the output revealed indications of potential payload obfuscation. Normally, SMTP (Simple Mail Transfer Protocol) traffic is characterized by human-readable text, making it easier to interpret the content of email communications. However, upon closer examination of one output, an unusual repeated pattern can be observed. This anomaly indicates that the data being transmitted may have undergone a process of obfuscation or encoding, which obscures its true content. Such repeated sequences are not typically observed in regular SMTP traffic, which suggests there was an attempt to mask the actual payload. Here is an example of the possible obfuscation due to the repetition of HcyJe0Lg2Ni4Pk6Rm8T and CXtEZvGbxIdzKf1Mh3Oj5Q. This output can be found below and in Appendix A.

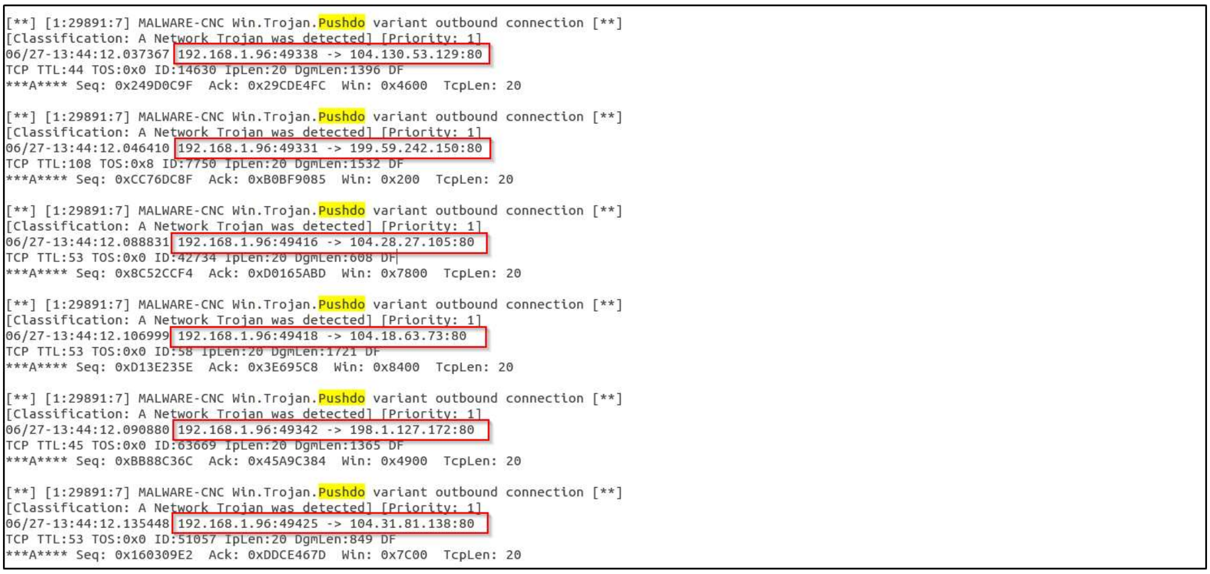
uFawHcyJe0Lg2Ni4Pk6Rm8TwHcyJe0Lg2Ni4Pk6Rm8TpAVrCXtEZvGbxIdzKf1Mh3Oj5QtEZvGbxIdzKf1Mh3
Oj5Ql7So9UqBWsDYuFawHcyJe0Lg2UqBWsDYuFawHcyJe0Lg2Ni4Pk6Rm8TpAVrCXtEZvGbxPk6Rm8TpA
VrCXtEZvGbxIdzKf1Mh3Oj5Ql7ZvGbxIdzKf1Mh3OjCXtEZvGbxIdzKf1Mh3Oj5Ql7So9UqBWsDYuFawHc5Ql
7So9UqBWsDYuFawHcyJe0Lg2Ni4Pk6Rm8TpAVrCe0Lg2Ni4Pk6Rm8TpAVrCXtEZvGbxIdzKf1Mh3Oj5Ql7S
oGbxIdzKf1Mh3Oj5Ql7So9UqBWsDYuFawHcyJe0Lg2NiBWsDYuFawHcyJe0Lg2Ni4Pk6Rm8TpAVrCXtEZvG
i4Pk6Rm8TpAVrCXtEZvGbxIdzKf1Mh3Oj5Ql7So9UqBdzKf1Mh3Oj5Ql7So9UqBWsDYuFawHcyJe0Lg2Ni4P
k6YuFawHcyJe0Lg2Ni4Pk6Rm8TpAVrCXtEZvGbxIdzKf1TpAVrCXtEZvGbxIdzKf1Mh3Oj5Ql7So9UqBWsDYu
FawOj5Ql7So9UqBWsDYuFawHcyJe0Lg2Ni4Pk6Rm8TpAcyJe0Lg2Ni4Pk6Rm8TpAVrCXtEZvGbxIdzKf1Mh3
Oj5QtEZvGbxIdzKf1Mh3Oj5Ql7So9UqBWsDYuFawHcyJe0Lo9UqBWsDYuFawHcyJe0Lg2Ni4Pk6Rm8TpAVr
CXtEg2Ni4Pk6Rm8TpAVrCXtEZvGbxIdzKf1Mh3Oj5Ql7So9bxIdzKf1Mh3Oj5Ql7So9UqBWsDYuFawHcyJe0L
g2Ni4PsDYuFawHcyJe0Lg2Ni4PkDYuFawHcyJe0Lg2Ni4Pk6Rm8TpAVrCXtEZ2Ni4Pk6Rm8TpAVrCXtEZvGb
xIdzKf1Mh3Oj5Q

DISCUSSION

RESULTS

An expanded set of Snort rules enabled a more comprehensive analysis, which ultimately led to the identification of multiple outbound connections originating from 192.168.1.96 to a range of external IP addresses, as illustrated in Figure 9. The intrusion detection system flagged these connections as being associated with the malware classified as Win.Trojan.Pushdo. This particular strain of malware typically functions as a downloader, responsible for retrieving additional malicious software components from the internet.

The recurring outbound connections to various external IP addresses strongly indicate that the malware is attempting to establish communication with its command-and-control (C&C) servers. These servers serve as centralized hubs for malicious actors, allowing them to send instructions to the infected systems. The pattern of repeated connections suggests that the malware is either seeking to download more malicious payloads to further compromise the system or is engaged in data exfiltration activities, where sensitive information could be sent back to the attackers.



```
[**] [1:29891:7] MALWARE-CNC Win.Trojan.Pushdo variant outbound connection [**]
[Classification: A Network Trojan was detected] [Priority: 1]
06/27-13:44:12.037367 192.168.1.96:49338 -> 104.130.53.129:80
TCP TTL:44 TOS:0x0 ID:14630 IpLen:20 DgmLen:1396 DF
***A**** Seq: 0x249D0C9F  Ack: 0x29CDE4FC  Win: 0x4600  TcpLen: 20

[**] [1:29891:7] MALWARE-CNC Win.Trojan.Pushdo variant outbound connection [**]
[Classification: A Network Trojan was detected] [Priority: 1]
06/27-13:44:12.046410 192.168.1.96:49331 -> 199.59.242.150:80
TCP TTL:108 TOS:0x8 ID:7750 IpLen:20 DgmLen:1532 DF
***A**** Seq: 0xCC76DC8F  Ack: 0xB0BF9085  Win: 0x200  TcpLen: 20

[**] [1:29891:7] MALWARE-CNC Win.Trojan.Pushdo variant outbound connection [**]
[Classification: A Network Trojan was detected] [Priority: 1]
06/27-13:44:12.088831 192.168.1.96:49416 -> 104.28.27.105:80
TCP TTL:53 TOS:0x0 ID:42734 IpLen:20 DgmLen:608 DF
***A**** Seq: 0x8C52CCF4  Ack: 0xD0165ABD  Win: 0x7800  TcpLen: 20

[**] [1:29891:7] MALWARE-CNC Win.Trojan.Pushdo variant outbound connection [**]
[Classification: A Network Trojan was detected] [Priority: 1]
06/27-13:44:12.106999 192.168.1.96:49418 -> 104.18.63.73:80
TCP TTL:53 TOS:0x0 ID:58 IpLen:20 DgmLen:1721 DF
***A**** Seq: 0xD13E235E  Ack: 0x3E695C8  Win: 0x8400  TcpLen: 20

[**] [1:29891:7] MALWARE-CNC Win.Trojan.Pushdo variant outbound connection [**]
[Classification: A Network Trojan was detected] [Priority: 1]
06/27-13:44:12.090880 192.168.1.96:49342 -> 198.1.127.172:80
TCP TTL:45 TOS:0x0 ID:63669 IpLen:20 DgmLen:1365 DF
***A**** Seq: 0xBB88C36C  Ack: 0x45A9C384  Win: 0x4900  TcpLen: 20

[**] [1:29891:7] MALWARE-CNC Win.Trojan.Pushdo variant outbound connection [**]
[Classification: A Network Trojan was detected] [Priority: 1]
06/27-13:44:12.135448 192.168.1.96:49425 -> 104.31.81.138:80
TCP TTL:53 TOS:0x0 ID:51057 IpLen:20 DgmLen:849 DF
***A**** Seq: 0x160309E2  Ack: 0xDDCE467D  Win: 0x7C00  TcpLen: 20
```

Figure 9: Pushdo outbound connections detected by snort.

Based on the analysis of the Snort alerts and the subsequent examination conducted with Wireshark, it became evident that a series of files were downloaded during the incident. Among these files, two notable executables, named Wp.exe and trow.exe, were identified. These files were extracted using Wireshark's capabilities for capturing network traffic. Following the extraction, a hash value for each file was generated employing the command “shasum”, which is a widely used method for creating secure checksums to verify file integrity.

Once the hash values were obtained, a thorough search was performed on the internet to determine their reputation. The results revealed that both Wp.exe and trow.exe are well-known malware, as confirmed by their listings on VirusTotal, a platform that aggregates antivirus detection results and file analysis. This information is clearly depicted in Figures 10, 11, and 12, which illustrate the specific details and threats associated with these malicious files.

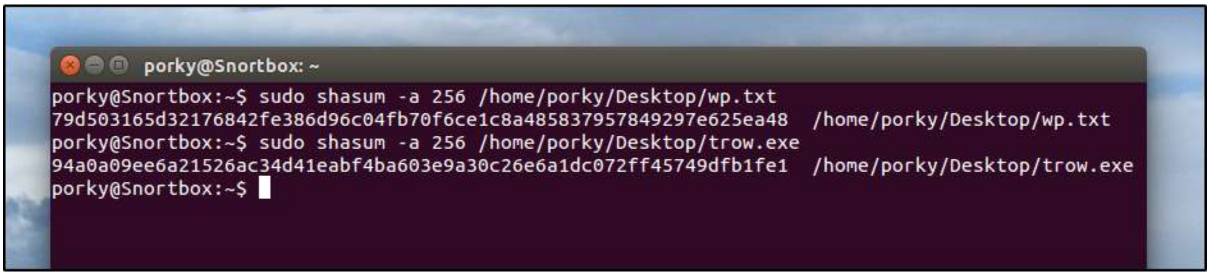


Figure 10: wp.exe and trow.exe shasum.

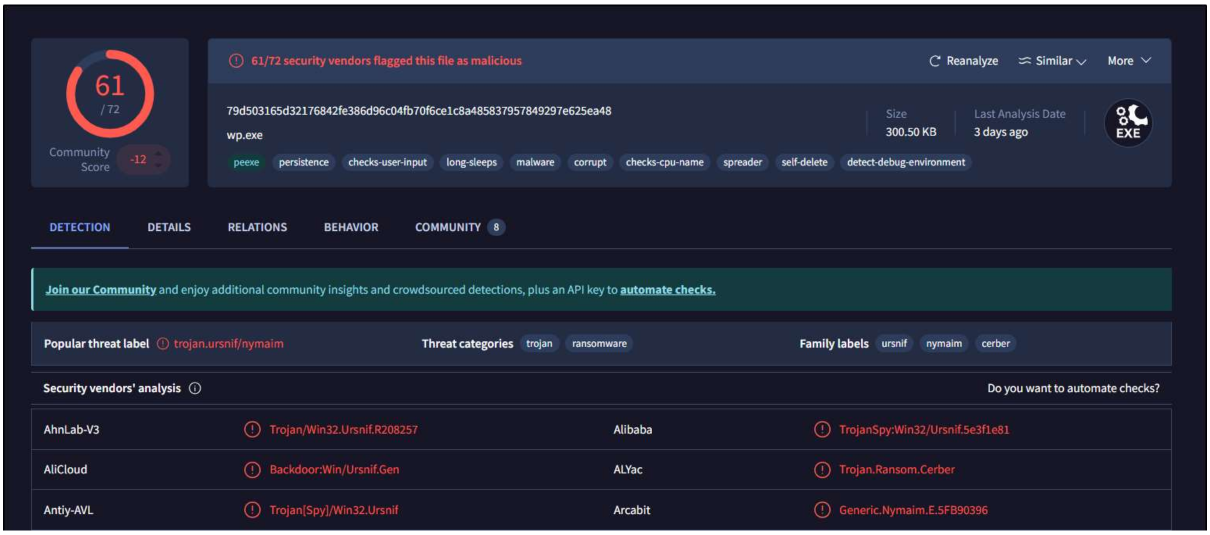


Figure 11: wp.exe hash on VirusTotal.

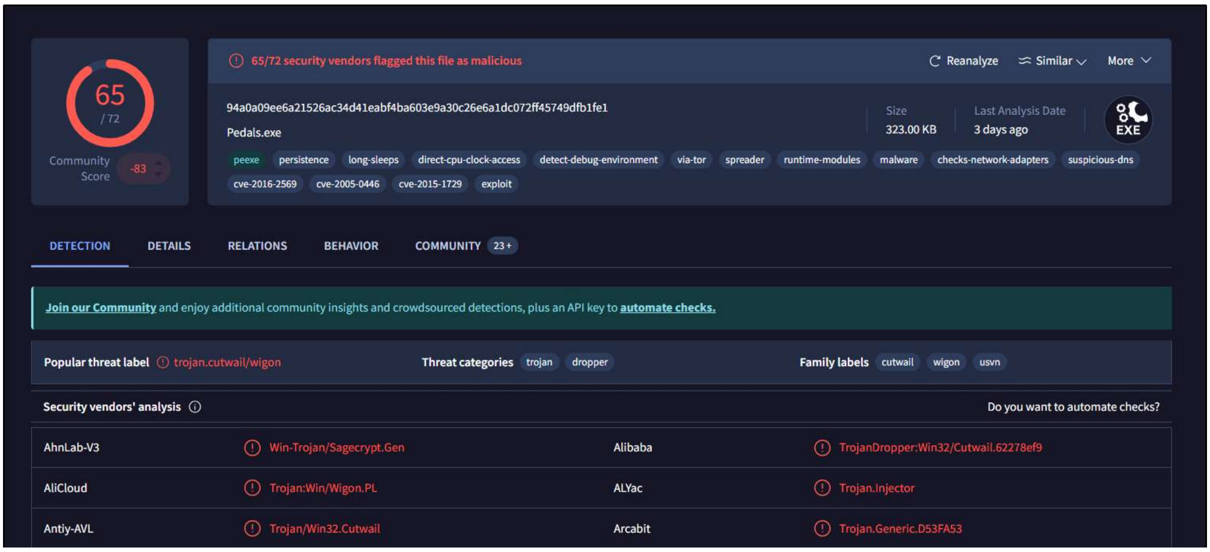


Figure 12: trow.exe hash on VirusTotal.

CONCLUSION

This forensic investigation effectively identified and analysed malicious activity within the captured network traffic, with detailed evidence pinpointing IP 192.168.1.96 as the compromised device. Early in the analysis, unusual patterns emerged as the device repeatedly communicated with external, untrusted domains—behaviour that raised red flags. This device's persistent connections with previously unknown IP addresses suggested potential command-and-control (C2) communication, a common tactic employed by malware to maintain contact with remote servers for further instructions or data exfiltration.

To confirm the presence of malicious activity, custom Snort rules were created and applied to the .pcap file to detect suspicious .exe file downloads. These Snort alerts flagged several outbound HTTP requests from IP 192.168.1.96 to external servers, specifically requesting .exe files, which were highly indicative of malware distribution. By examining these alerts more in-depth, a clear pattern of suspicious downloads was identified, where the compromised device accessed multiple domains linked to malware-hosting infrastructure. The analysis in Wireshark further validated these findings, confirming each download event and detailing their associated DNS queries and GET requests from vantagpointtechnologie.com and lounge-haarstudio.nl

Further inspection and verification were conducted using VirusTotal to analyse the downloaded files, which included wp.exe and trow.exe. The hashing and upload of these files to VirusTotal returned positive identifications of known malware variants, linking the files directly to Win.Trojan.Pushdo. Pushdo is a notorious Trojan, recognized for its ability to establish and maintain C2 connections, download additional malware payloads, and facilitate data exfiltration. This malware's signature capabilities aligned with the observed behaviour, where 192.168.1.96 made regular outbound connections to unfamiliar domains, potentially in an attempt to exfiltrate data or receive further commands.

References

VirusTotal (n.d.) *File Details for 94a0a09ee6a21526ac34d41eabf4ba603e9a30c26e6a1dc072ff45749dfb1fe1*. Available at: https://www.virustotal.com/gui/file/94a0a09ee6a21526ac34d41eabf4ba603e9a30c26e6a1dc072ff45749dfb1fe1/details (Accessed: 5 November 2024).

VirusTotal (n.d.) *File Details for 79d503165d32176842fe386d96c04fb70f6ce1c8a485837957849297e625ea48*. Available at: https://www.virustotal.com/gui/file/79d503165d32176842fe386d96c04fb70f6ce1c8a485837957849297e625ea48/details (Accessed: 4 November 2024).

CyberChef. Available at: https://gchq.github.io/CyberChef/ (Accessed: 04 November 2024).

APPENDICES

APPENDIX A