Advanced Digital Forensics

An investigation into a compromised network

Casey Donaldson

2203162

CMP416: Advanced Digital Forensics

2024/25

Note that the Information contained in this document is for educational purposes.

.

Contents

.

1 INTRODUCTION

1.1 BACKGROUND

A company was infected with malware and this paper investigates the causes of the breach and attempts to identify the malicious files and the host which is compromised. The investigation will analyse a PCAP file which contains a record of the network traffic at the time of the incident.

Additionally, a text file was provided which contained Snort alerts. The investigation will start by analysing these alerts to identify where to start the analysis on the PCAP file.

1.2 AIMS

The aims of this investigation are listed below.

- Create snort rules and run them through the PCAP file.
- Identify the compromised host and the cause of the breach.
- Determine what malware is present.
- Identify IPs which are responsible for infecting the network.

2 METHODOLOGY

2.1 SNORT ANALYSIS

The first step was the analysis of the provided Snort alerts text file. After thoroughly analysing the alerts, it was concluded that host 192.168.1.96 was infected after downloading a malicious file. This is due to the sheer mass of traffic from this host which has been alerted as “MALWARE-CNC Win.Trojan/Pushdo”. This suggests that the infected host was sending malware to additional hosts (propagation). Furthermore, below is a list of additional alerts which has been set off.

- File executable binary file magic detected.
- SDF combination alerts (sensitive data).
- Download an executable (PE) Detected.
- Invalid content length or chunk size.
- Obfuscated script encoding.
- Microsoft Explorer 7 emulation via meta tag.
- Non-alphanumeric JavaScript detected.
- Remote JavaScript file found in script-tag
- Indicator-compromise suspicious “.RU” DNS query.#

These alerts reveal that a file was downloaded which then downloaded additional malware. The host 192.168.1.96 appears to be consistently accessing malicious websites revealing possible violations of corporate policies.

2.2 CONSTRUCTION OF SNORT ALERTS

As this investigation was given a list of recorded Snort alerts the investigator only created 5 rules to enforce the current alerts and attempt to find where the malware came from. The first rule detects files being downloaded if the payload contains MZ at the start, see below.

```
#this alert should detect any protable executable file
alert tcp any any -> any any (msg: "PE file detected being downloaded - Detected"; flow:from_server,established; content:"MZ"; depth:2; sid:1000050;
rev:1;)
```

Figure 1 First Snort rule.

The second, third, fourth and fifth rules attempt to detect any HTTP download which contains “.exe”, “.zip”, “.JS”, or “.BIN”, see below.

```
#this rules is used to detect suspicious HTTP files being downloaded.
alert tcp any any -> any 80 (msg:"Suspicious HTTP File Download .EXE - Potential Malware"; content:".exe"; http_uri; nocase; sid:1000005; rev:1;)
alert tcp any any -> any 80 (msg:"Suspicious HTTP File Download .ZIP - Potential Malware"; content:".zip"; http_uri; nocase; sid:1000006; rev:1;)
alert tcp any any -> any 80 (msg:"Suspicious HTTP File Download .JS - Potential Malware"; content:".js"; http_uri; nocase; sid:1000007; rev:1;)
alert tcp any any -> any 80 (msg:"Suspicious HTTP File Download .BIN - Potential Malware"; content:".bin"; http_uri; nocase; sid:1000007; rev:1;)
```

Figure 2 Second to Fifth Snort rules.

The last rule attempts to detect any GET request, this was achieved by using content with “GET” and “Connection|3A|”, see below.

```
#this alert attempts to detect suspicious GET requests
alert tcp any any -> any 80 (msg:"Suspicious HTTP GET Request Detected"; content:"GET"; http_method; content:"Connection|3A| Keep-Alive"; distance:0;
distance:0; sid:1000015; rev:1;)
```

Figure 3 Sixth Snort rule.

Once the custom Snort rules were in place the Snort application was executed using the command shown below. The program executed rapidly, and the alert file was found in the directory provided below.

```
porky@Snortbox:/etc/snort$ sudo snort -c snort.conf -r /home/porky/Desktop/Unit\ 1\ -\ Case\ Study\ -\ Source\ Files/Unit\ 1\ -\ Case\ Study\ -\ PCAP\ File
s.pcap -l /var/log/snort/
```

Figure 4 Snort command.

Evidence of the Snort alerts can be found in Appendix B – Snort alerts. Upon analysing the alerts there were four unusual files. These included a download of an EXE and BIN file and additional suspicious GET requests. Below is a summary of what was found due to the customs rules ordered in ascending order based on time.

- HTTP GET request was triggered on 06/27 at 13:38:32.652026
    - IPs involved: Src-192.168.1.96:49184, Des-119.28.70.207:80
- HTTP GET request was triggered on 06/27 at 13:43:52.243381
    - IPs involved: Src-192.168.1.96:49190, Des-145.131.10.21:80
- A suspicious HTTP file download alert for an EXE file was triggered on 06/27 at 13:43:52.243381
    - IPs involved: Src-192.168.1.96:49190, Des-145.131.10.21:80
- A Suspicious PE file detected being downloaded on 06/27 at 13:43:52.407982
    - IPs involved: Src-145.131.10.21:80, Des-192.168.1.96:49190
- HTTP GET request was triggered on 06/27 at 13:43:54.128138
    - IPs involved: Src-192.168.1.96:49191, Des-143.95.151.192:80
- A suspicious HTTP file download alert for an EXE file was triggered on 06/27 at 13:43:54.128138
    - IPs involved: Src-192.168.1.96:49191, Des-143.95.151.192:80
- HTTP GET request was triggered on 06/27 at 13:43:58.714716
    - IPs involved: Src-192.168.1.96:49192, Des-59.106.164.230:80
- A suspicious HTTP file download alert for a BIN file was on 06/27 at 13:43:58.714716
    - IPs involved: Src-192.168.1.96:49192, Des-59.106.164.230:80

Snort has helped in identifying interesting packets and IPs that need to be investigated. According to the Alerts given and the Alerts created it appears that malware was installed onto the IP 192.168.1.96 with some Trojan. This hypothesis will be further examined in the next section, Analysis of PCAP with Wireshark.

2.3 ANALYSIS OF PCAP WITH WIRESHARK

The first packet to be examined is the packet which was sent on 06/27 at 13:38:32.652026. The packet appears to be a GET request to a “gerv.gun” file. This came from “matied.com” which has the IP address 119.28.70.207, see below.

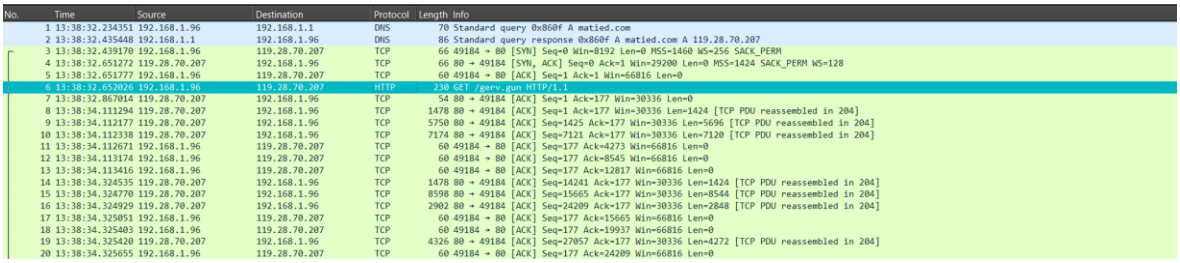

Figure 5 Wireshark first packet.

The TCP stream was followed and the data containing the file was saved into a raw binary file. This aimed to carve out the file and test if it was malicious. This was achieved by uploading the binary file to HxD. Once the file was uploaded it was identified to be a portable executable(PE) as per the “MZ” hexadecimal. The data before the MZ was removed and the file SHA-256 was then captured, Figure 10. The hash was identified as “0931537889c35226d00ed26962ecacb140521394279eb2ade7e9d2afcf1a7272”, the hash was then uploaded to Virustotal.com which identified the file as malware, Figure 13. This proved that the host was infected during this time and proved that the malware was a Trojan installer, this could indicate that further malicious files are to come.

The next packet which was identified during the Alerts was sent at 13:43:52.243381. This shows another GET request for “trow.exe”, this was downloaded from “lounge-haarstudio.nl” which has the IP address 145.131.10.21, Figure 6. The same process as before was conducted, this time following the HTTP stream.

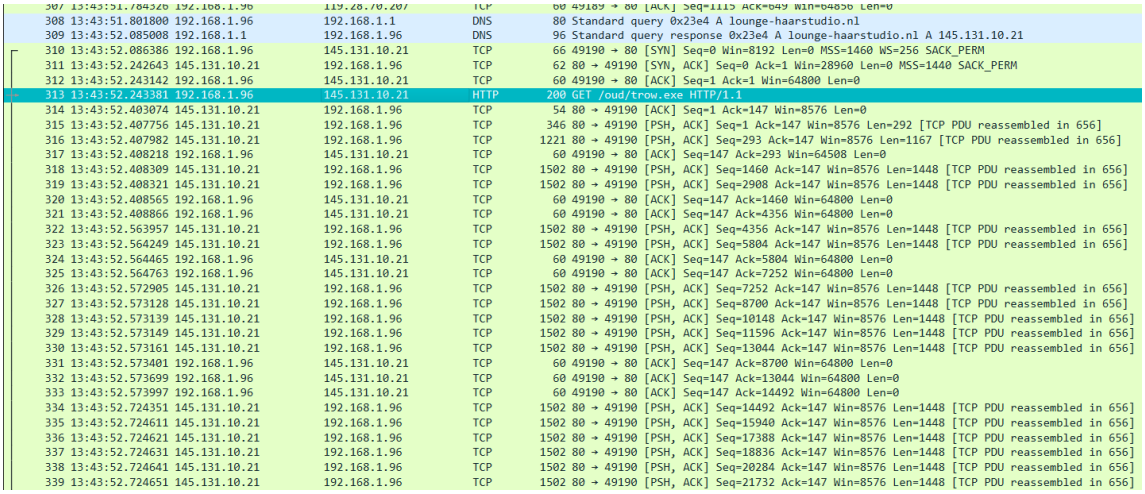

Figure 6 Wireshark second packet.

Once the HTTP stream was saved and uploaded to HxD. This revealed that the file was an executable. The SHA-256 hash was identified as "94a0a09ee6a21526ac34d41eabf4ba603e9a30c26e6a1dc072ff45749dfb1fe1" Once uploaded to Virustotal.com it was revealed to be malware, Figure 14.

The third packet which is to be analysed was sent at 13:43:54.128138. This packet was another GET request from the domain "vantagepointtechnologies.com", which has the IP 143.95.151.192, Figure 7.

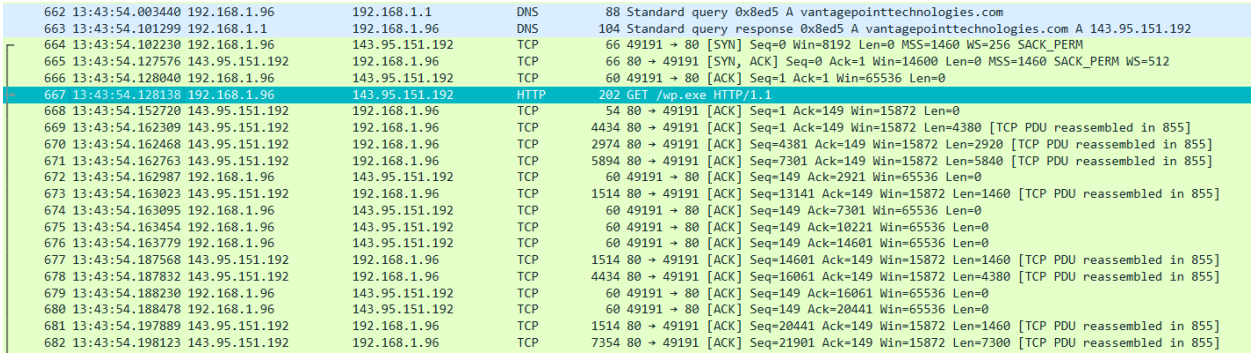

Figure 7 Wireshark third packet.

This TCP stream was then followed and the data related to the file was uploaded into HxD, Figure 12. The file was identified to be another PE file and the data before the MZ was removed, the data from MZ up to the padding was then saved and the SHA-256 was identified to be "79d503165d32176842fe386d96c04fb70f6ce1c8a485837957849297e625ea48". The hash was uploaded to Virustotal.com and this was then identified as malware, Figure 15.

The final packet stream which is to be analysed was sent at 13:43:58.714716. This revealed that the stream was another GET request from the URL "rts21.co.jp", with the IP address 59.106.164.230.

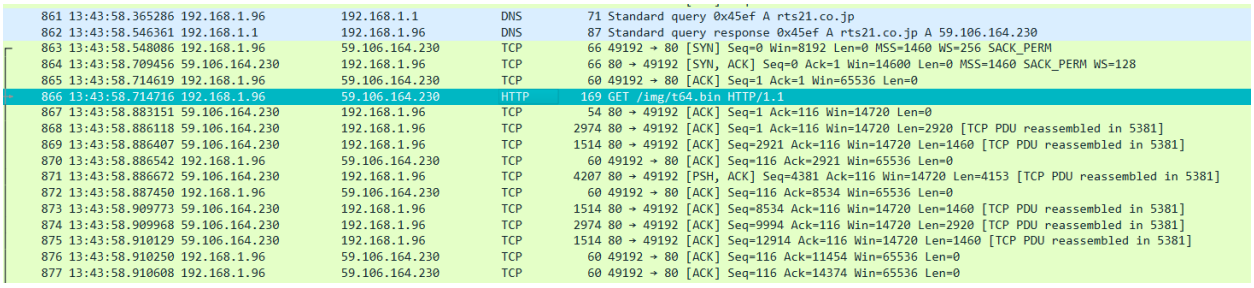

Figure 8 Wireshark fourth packet.

Upon viewing this packet, it was identified that the request is attempting to get a t64.bin file from an "img" folder at the above URL. The contents of the TCP stream are unreadable and could indicate some obfuscation or the use of a ZIP file. The contents within the TCP stream show that there could be an executable file and could additionally contain an image file. The reason this packet raises suspicion is due to the details section of Virustotal.com which reveals t64.bin as a possible name for the malware "gerv.gun", Figure 16.

3 DISCUSSION

3.1 RESULTS

The infection occurred on 06/27 at 13:38:32. The host computer, which was infected had the IP 192.168.1.96, and the host name was “FlashGordon – PC”. The resolved MAC address of this computer is “Dell_de:c7:3b”, this suggests that the PC is a Dell PC, Figure 9.

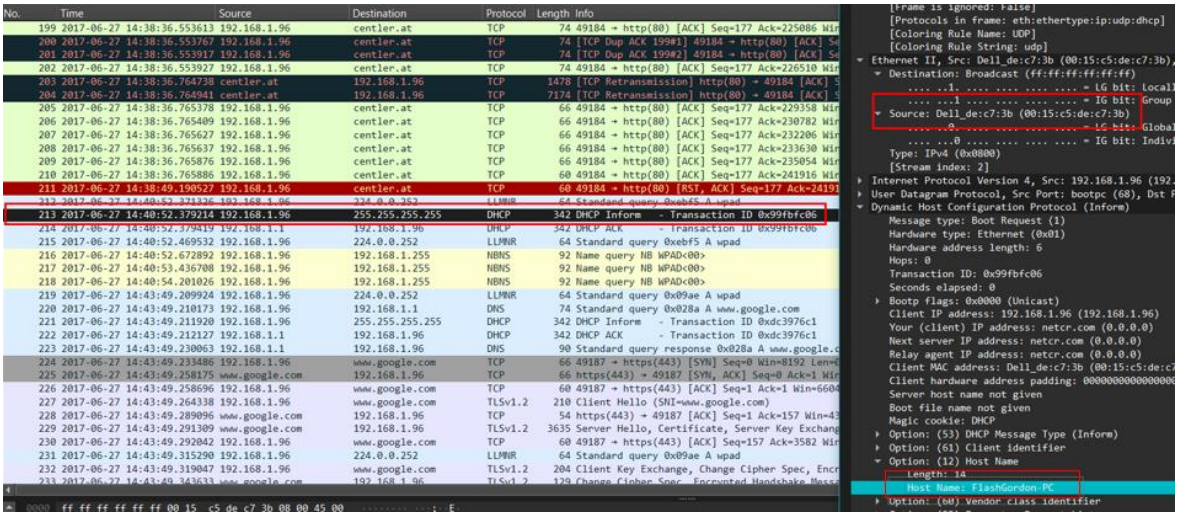

Figure 9 Infected host's DHCP configuration.

The PCAP file is confirmed to have 3 executables within. These 3 executables are identified as malicious by Virustotal.com. The website also mentioned that the trojan is installed using the downloader “gerv.gun”, which is why 3 separate downloads were made. The timing of these downloads was seconds apart and from different URLs making this more likely to be related to malware.

A report mentions a similar attack in Japan which involves the 3 executables found. The report also mentions a zip file which contains “.JS” files. These were not found but are likely to be contained within the obfuscated “/img/t64.bin” file, (My Security Online, 2022).

The primary IPs which were involved are listed below, not including IPs which were not involved in the transmission of malicious files.

- 192.168.1.96 (Infected host)
- 143.95.151.192
- 145.131.10.21
- 119.28.70.207
- 59.106.164.230

Finally, several “.RU” domains were accessed this raises alarms as in the past it has shown a lot of malware comes from these domains. The best practice is to deny all “.RU” domains and allow-list only legitimate “.RU” domains

3.2 CONCLUSION

In conclusion, the host 192.168.1.96 was infected with trojan malware, which used gerv gun to download the actual malware, trow.exe and wp.exe. After the downloads, the malware then attempted to propagate to further networks according to snort alerts given at the start of the investigation.

Further analysis of this PCAP should be taken as 17 thousand packets were detected and given the timescale a thorough analysis was not possible. Further analysis could identify other areas which show where the infection spread, moreover, malware analysis could be done to analyse what the actual executables did, the behaviour of the programs and how to implement better defences.

4 REFERENCE LIST

Kessler, G. (2019). *File Signatures*. [online] Garykessler.net. Available at: https://www.garykessler.net/library/file_sigs.html [Accessed 3 Nov. 2024].

My Security Online (2022). *Japanese Language Invoice Malspam Using Js Files Inside Zips Today*. [online] myonlinesecurity.co.uk. Available at: https://myonlinesecurity.co.uk/japanese-language-invoice-malspam-using-js-files-inside-zips-today/ [Accessed 2 Nov. 2024].

Poisel, R. and Tjoa, S. (2013). *A Comprehensive Literature Review of File Carving*. [online] IEEE Xplore. doi:https://doi.org/10.1109/ARES.2013.62.

Wireshark (2019). *Chapter 1. Introduction*. [online] Wireshark.org. Available at: https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html [Accessed 3 Nov. 2024].

5 APPENDICES

APPENDIX A – PHOTOS OF ANALYSIS

Get_garv.gun_file

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ.....ÿÿ..
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	¸.......@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	D8	00	00	00	.....Ø...
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	..º..´.Í!¸.LÍ!Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode....$.....
00000080	D2	5E	55	56	96	3F	3B	05	96	3F	3B	05	96	3F	3B	05	Ò^UV–?;.–?;.–?;.
00000090	B1	F9	46	05	B3	3F	3B	05	B1	F9	56	05	F3	3F	3B	05	±ùF.³?;.±ùV.ó?;.
000000A0	55	30	64	05	97	3F	3B	05	55	30	66	05	89	3F	3B	05	U0d.—?;.U0f.‰?;.
000000B0	96	3F	3A	05	32	3F	3B	05	B1	F9	55	05	BF	3F	3B	05	–?:.2?;.±ùU.¿?;.
000000C0	B1	F9	43	05	97	3F	3B	05	52	69	63	68	96	3F	3B	05	±ùC.—?;.Rich–?;.
000000D0	00	00	00	00	00	00	00	00	50	45	00	00	4C	01	04	00	........PE..L...
000000E0	65	5A	51	59	00	00	00	00	00	00	00	00	E0	00	03	01	eZQY........à...
000000F0	0B	01	08	00	00	70	01	00	00	30	02	00	00	00	00	00	.....p...0.....
00000100	66	A8	00	00	00	10	00	00	00	80	01	00	00	00	40	00	f¨.......€....@.
00000110	00	10	00	00	00	10	00	00	04	00	00	00	00	00	00	00	.....
00000120	04	00	00	00	00	00	00	00	00	C0	03	00	00	10	00	00	.........À.....
00000130	2A	8F	02	00	02	00	00	00	00	00	10	00	00	10	00	00	*.....
00000140	00	00	10	00	00	10	00	00	00	00	00	00	10	00	00	00	.....
00000150	00	00	00	00	00	00	00	00	2C	CC	01	00	40	01	00	00	........,Ì..@...
00000160	00	10	02	00	9C	A0	01	00	00	00	00	00	00	00	00	00	....œ .....
00000170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000001A0	80	C2	01	00	40	00	00	00	00	00	00	00	00	00	00	00	€Â..@.....
000001B0	00	80	01	00	90	02	00	00	00	00	00	00	00	00	00	00	.€.....
000001C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000001D0	2E	74	65	78	74	00	00	00	72	66	01	00	00	10	00	00	.text...rf.....
000001E0	00	70	01	00	00	10	00	00	00	00	00	00	00	00	00	00	.p

Figure 10 HxD Gerv.gun file.

thow-exe-http-file-hex

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ.....ÿÿ..
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	¸.......@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	E8	00	00	00	.....è...
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	..º..´.Í!¸.LÍ!Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode....$.....
00000080	F7	C1	6C	0D	B3	A0	02	5E	B3	A0	02	5E	B3	A0	02	5E	÷Ál.³ .^³ .^³ .^
00000090	BA	D8	97	5E	A5	A0	02	5E	BA	D8	86	5E	8A	A0	02	5E	ºؗ^¥ .^º؆^Š .^
000000A0	BA	D8	81	5E	3D	A0	02	5E	94	66	79	5E	AE	A0	02	5E	º؁^= .^”fy^® .^
000000B0	B3	A0	03	5E	0B	A0	02	5E	BA	D8	88	5E	B2	A0	02	5E	³ .^. .^º؈^² .^
000000C0	AD	F2	96	5E	B2	A0	02	5E	BA	D8	93	5E	B2	A0	02	5E	.ò–^² .^ºؓ^² .^
000000D0	52	69	63	68	B3	A0	02	5E	00	00	00	00	00	00	00	00	Rich³ .^.....
000000E0	00	00	00	00	00	00	00	00	50	45	00	00	4C	01	04	00	.....PE..L...
000000F0	7C	15	52	59	00	00	00	00	00	00	00	00	E0	00	03	01	|.RY.....à...
00000100	0B	01	09	00	00	0C	02	00	00	FC	02	00	00	00	00	00	.....ü.....
00000110	09	CF	00	00	00	10	00	00	00	20	02	00	00	00	20	14	.Ï..... .... .
00000120	00	10	00	00	00	02	00	00	05	00	00	00	00	00	00	00	.....
00000130	05	00	00	00	00	00	00	00	00	50	05	00	00	04	00	00	.....P.....
00000140	91	C2	03	00	02	00	00	80	00	00	10	00	00	10	00	00	‘Â.....€.....
00000150	00	00	10	00	00	10	00	00	00	00	00	00	10	00	00	00	.....
00000160	00	00	00	00	00	00	00	00	7C	60	02	00	2C	01	00	00	.....|`..,...
00000170	00	C0	02	00	C8	8D	02	00	00	00	00	00	00	00	00	00	.À..È.....
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000190	20	23	02	00	1C	00	00	00	00	00	00	00	00	00	00	00	#.....
000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000001B0	38	4A	02	00	40	00	00	00	00	00	00	00	00	00	00	00	8J..@.....
000001C0	00	20	02	00	D0	02	00	00	00	00	00	00	00	00	00	00	. ..Ð.....
000001D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000001E0	2E	74	65	78	74	00	00	00	02	0B	02	00	00	10	00	00	.text

Figure 11 HxD trow.exe file.

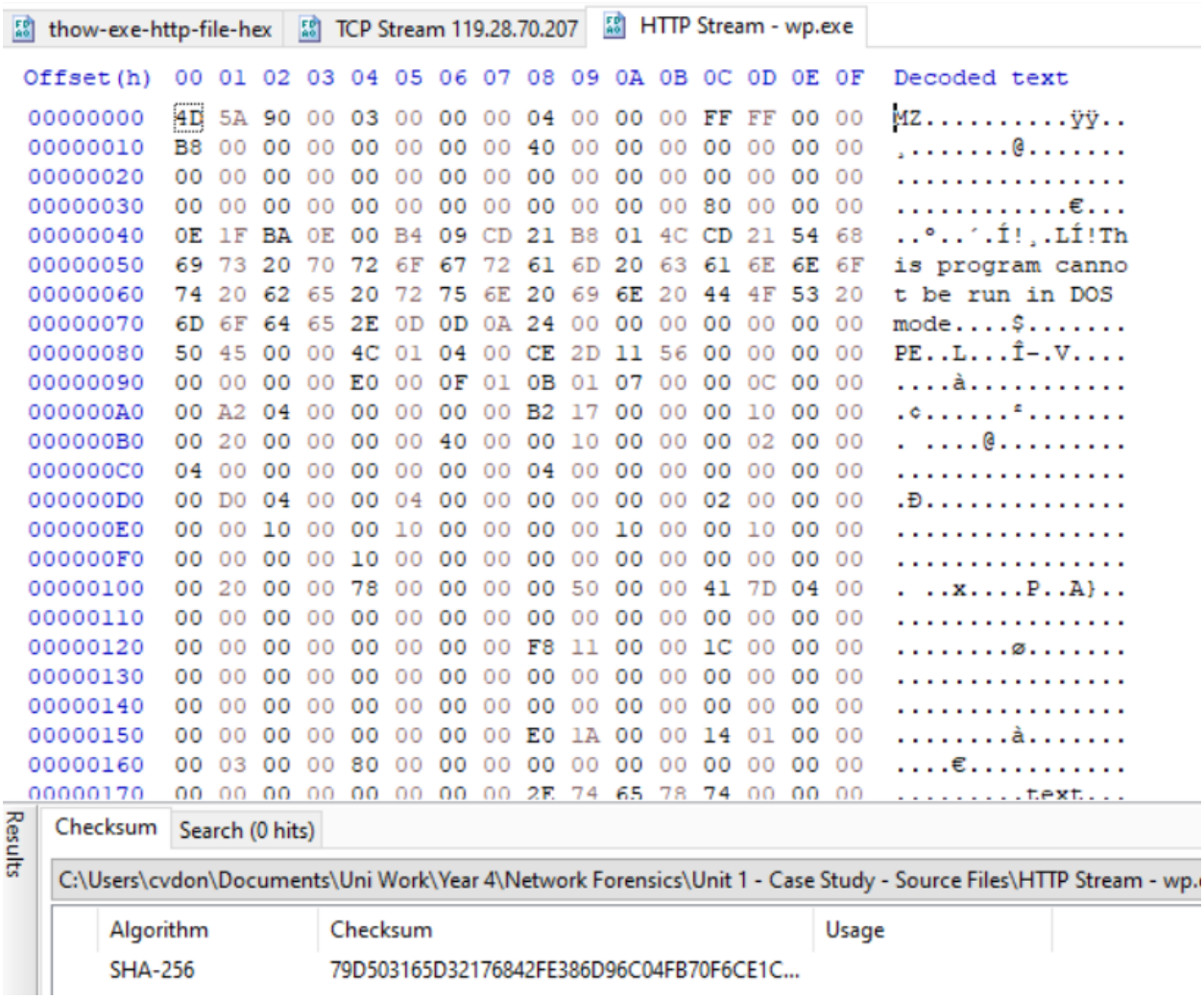

Figure 12 HxD wp.exe file.

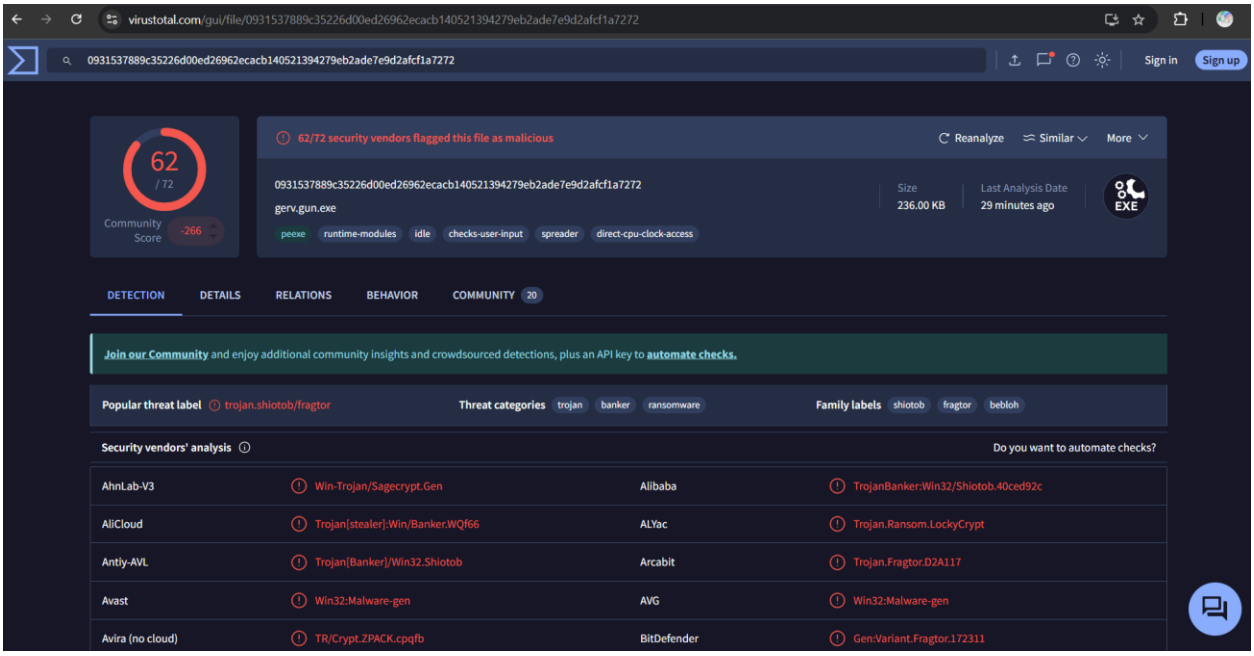

Figure 13 Virustotal - 0931537889c35226d00ed26962ecacb140521394279eb2ade7e9d2afcf1a7272

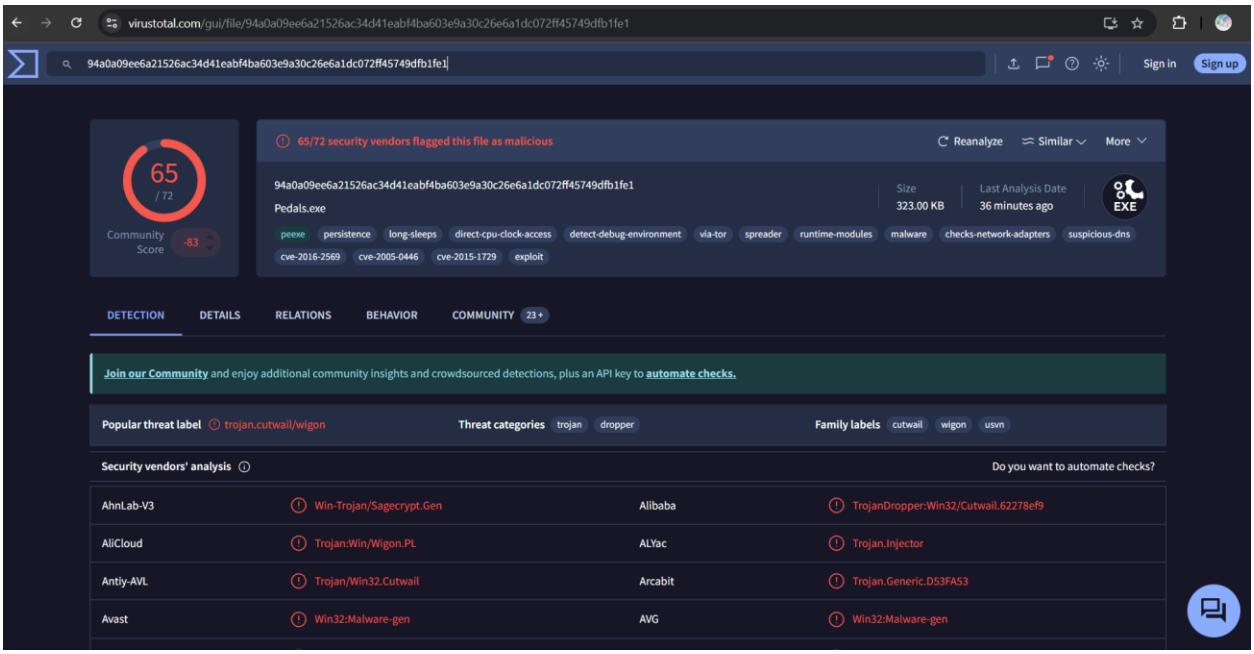

Figure 14 Virustotal - 94a0a09ee6a21526ac34d41eabf4ba603e9a30c26e6a1dc072ff45749dfb1fe1

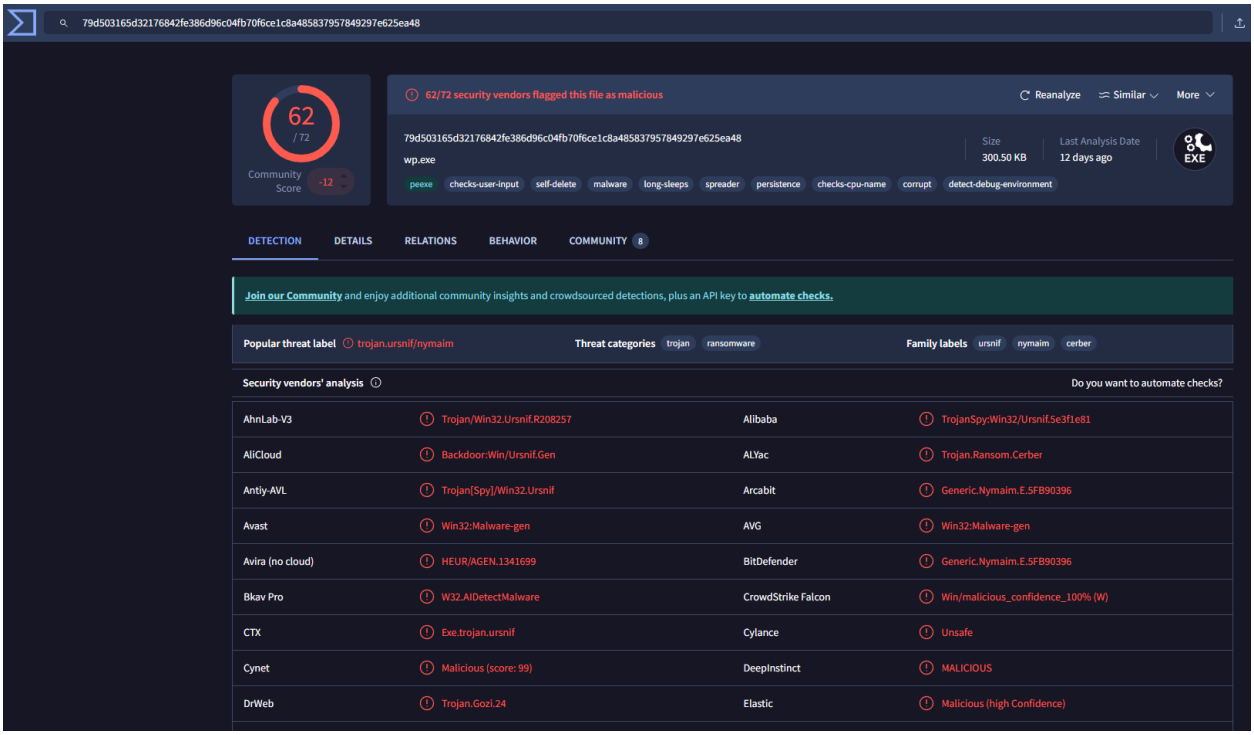

Figure 15 Virus total - 79d503165d32176842fe386d96c04fb70f6ce1c8a485837957849297e625ea48

Figure 16 Virus total gerv.gun detail section.

APPENDIX B – SNORT ALERTS

```
[**] [1:1000015:1] Suspicious HTTP GET Request Detected [**]
[Priority: 0]
06/27-13:38:32.652026 192.168.1.96:49184 -> 119.28.70.207:80
TCP TTL:47 TOS:0x0 ID:64227 IpLen:20 DgmLen:216 DF
***A**** Seq: 0xA337D3E7  Ack: 0xEEED7BAB  Win: 0x7680  TcpLen: 20

[**] [1:1000015:1] Suspicious HTTP GET Request Detected [**]
[Priority: 0]
06/27-13:43:52.243381 192.168.1.96:49190 -> 145.131.10.21:80
TCP TTL:239 TOS:0x20 ID:41883 IpLen:20 DgmLen:186
***A**** Seq: 0xCB5AB76A  Ack: 0xA90C3547  Win: 0x2180  TcpLen: 20

[**] [1:1000005:1] Suspicious HTTP File Download .EXE - Potential Malware [**]
[Priority: 0]
06/27-13:43:52.243381 192.168.1.96:49190 -> 145.131.10.21:80
TCP TTL:239 TOS:0x20 ID:41883 IpLen:20 DgmLen:186
***A**** Seq: 0xCB5AB76A  Ack: 0xA90C3547  Win: 0x2180  TcpLen: 20

[**] [1:1000050:1] PE file detected being downloaded - Detected [**]
[Priority: 0]
06/27-13:43:52.407982 145.131.10.21:80 -> 192.168.1.96:49190
TCP TTL:239 TOS:0x20 ID:41885 IpLen:20 DgmLen:1207
***AP*** Seq: 0xA90C366B  Ack: 0xCB5AB7FC  Win: 0x2180  TcpLen: 20

[**] [1:1000015:1] Suspicious HTTP GET Request Detected [**]
[Priority: 0]
06/27-13:43:54.128138 192.168.1.96:49191 -> 143.95.151.192:80
TCP TTL:49 TOS:0x8 ID:1431 IpLen:20 DgmLen:188 DF
***A**** Seq: 0xA88DB23D  Ack: 0x2FD3568D  Win: 0x3E00  TcpLen: 20

[**] [1:1000005:1] Suspicious HTTP File Download .EXE - Potential Malware [**]
[Priority: 0]
06/27-13:43:54.128138 192.168.1.96:49191 -> 143.95.151.192:80
TCP TTL:49 TOS:0x8 ID:1431 IpLen:20 DgmLen:188 DF
***A**** Seq: 0xA88DB23D  Ack: 0x2FD3568D  Win: 0x3E00  TcpLen: 20
```

Figure 17 Custom Snort alert 1.

```
[**] [1:1000015:1] Suspicious HTTP GET Request Detected [**]
[Priority: 0]
06/27-13:43:58.714716 192.168.1.96:49192 -> 59.106.164.230:80
TCP TTL:44 TOS:0x0 ID:43236 IpLen:20 DgmLen:155 DF
***A**** Seq: 0x709F8625  Ack: 0xDFE26F51  Win: 0x3980  TcpLen: 20
_ws.col.protocol == "HTTP"
[**] [1:1000007:1] Suspicious HTTP File Download .BIN - Potential Malware [**]
[Priority: 0]
06/27-13:43:58.714716 192.168.1.96:49192 -> 59.106.164.230:80
TCP TTL:44 TOS:0x0 ID:43236 IpLen:20 DgmLen:155 DF
***A**** Seq: 0x709F8625  Ack: 0xDFE26F51  Win: 0x3980  TcpLen: 20
```

Figure 18 Custom Snort alert 2.