Investigation into the compromise of an infected machine

Investigating a compromised machine through a packet capture and Snort alert log.

David C

CMP416: Digital Forensics 2

2024/25

Note that Information contained in this document is for educational purposes

.

Contents

.

1 INTRODUCTION

1.1 AIM

This report aims to outline the steps taken by the investigator to assess and identify indicators of compromise (IOC) of an infected machine that was since taken over by a Command and Control (C2) server. The investigator was tasked with performing an analysis of network traffic to best identify the steps taken by the malicious actors to compromise the machine and best identify the steps that could be taken to undo the damage caused.

2 METHODOLOGY

2.1 OVERVIEW OF METHODOLOGY

The investigator is basing this report off of the OSCAR methodology (Qureshi, et al., 2021) which was presented by a group of researchers who highlight the importance of documenting steps taken before an incident may have occurred, and then providing detailed documentation to explain the impact of what had been found. This methodology has been amended due to the investigator not being able to report on the sections regarding obtaining information or strategizing.

2.2 COLLECTION

For the collection phase of this methodology the investigator intends to make use of numerous network forensics tools including Wireshark, Snort and NetworkMiner. These tools will be of particular use to the investigator for identifying a timeline of the events that occurred as the machine in the question was compromised.

Furthermore, the investigator intends to take advantage of VirusTotal to assist with analysing and triaging artefacts and IP addresses to assess the potential risks associated with servers and files that were interacted with during the compromise of the target machine.

2.3 ANALYSIS

The investigator intends to use Wireshark and Snort for analysing traffic and recovering certain artefacts from the captured data to assist with their analysis of the situation, whilst taking advantage of NetworkMiner to assist with retrieving additional artefacts to allow the investigator to gain the full picture of the events that took place.

Additionally, the investigator hopes that VirusTotal will be useful for understanding what interactions the executables downloaded throughout the captured network traffic could be interacting with on the computers side, which is not visible with the investigators current set of information.

2.4 REPORT

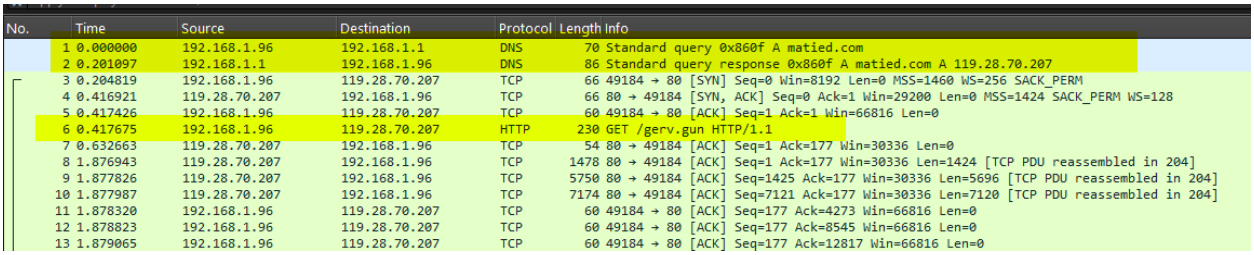
The investigator will ensure that this report is present in a manner that highlights the important information whilst remaining technically adequate for their peers, in-line with the methodology chosen for this investigation.

3 RESULTS

3.1 COLLECTION

3.1.1 Wireshark

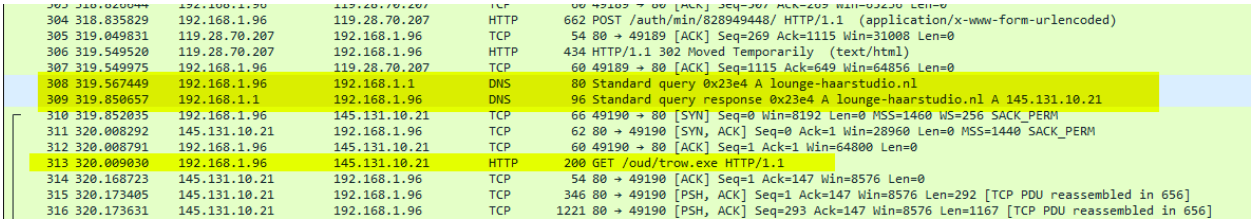
The investigator was presented with a Wireshark packet capture file which contained traffic from numerous hosts across many protocols. The first important information that was collected by the investigator was at the beginning of the capture.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.96	192.168.1.1	DNS	70	Standard query 0x860f A matied.com
2	0.201097	192.168.1.1	192.168.1.96	DNS	86	Standard query response 0x860f A matied.com A 119.28.70.207
3	0.204819	192.168.1.96	119.28.70.207	TCP	66	49184 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
4	0.416921	119.28.70.207	192.168.1.96	TCP	66	80 → 49184 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1424 SACK_PERM WS=128
5	0.417426	192.168.1.96	119.28.70.207	TCP	60	49184 → 80 [ACK] Seq=1 Ack=1 Win=66816 Len=0
6	0.417675	192.168.1.96	119.28.70.207	HTTP	230	GET /gerv.gun HTTP/1.1
7	0.632663	119.28.70.207	192.168.1.96	TCP	54	80 → 49184 [ACK] Seq=1 Ack=177 Win=30336 Len=0
8	1.876943	119.28.70.207	192.168.1.96	TCP	1478	80 → 49184 [ACK] Seq=1 Ack=177 Win=30336 Len=1424 [TCP PDU reassembled in 204]
9	1.877826	119.28.70.207	192.168.1.96	TCP	5750	80 → 49184 [ACK] Seq=1425 Ack=177 Win=30336 Len=5696 [TCP PDU reassembled in 204]
10	1.877987	119.28.70.207	192.168.1.96	TCP	7174	80 → 49184 [ACK] Seq=7121 Ack=177 Win=30336 Len=7120 [TCP PDU reassembled in 204]
11	1.878320	192.168.1.96	119.28.70.207	TCP	60	49184 → 80 [ACK] Seq=177 Ack=4273 Win=66816 Len=0
12	1.878823	192.168.1.96	119.28.70.207	TCP	60	49184 → 80 [ACK] Seq=177 Ack=8545 Win=66816 Len=0
13	1.879065	192.168.1.96	119.28.70.207	TCP	60	49184 → 80 [ACK] Seq=177 Ack=12817 Win=66816 Len=0

Figure 1 - Wireshark Capture related to gerv.gun

We can see through the highlighted packets that the host (192.168.1.96) makes a DNS query to "matied.com" and through the query, downloads a file known as "gerv.gun". This file was not recoverable through Wireshark but as will be covered later, was recovered and used in further steps of analysis. After following the file further, the investigator came across further DNS queries after a large number of packets through the TLS and TCP protocols which are commonly seen when downloading files from web servers. These DNS queries were to another domain and then followed by another executable file being downloaded.



304	318.835829	192.168.1.96	119.28.70.207	HTTP	662	POST /auth/min/828949448/ HTTP/1.1 (application/x-www-form-urlencoded)
305	319.049831	119.28.70.207	192.168.1.96	TCP	54	80 → 49189 [ACK] Seq=269 Ack=1115 Win=31008 Len=0
306	319.549520	119.28.70.207	192.168.1.96	HTTP	434	HTTP/1.1 302 Moved Temporarily (text/html)
307	319.549975	192.168.1.96	119.28.70.207	TCP	60	49189 → 80 [ACK] Seq=1115 Ack=649 Win=64856 Len=0
308	319.567449	192.168.1.96	192.168.1.1	DNS	80	Standard query 0x23e4 A lounge-haarstudio.nl
309	319.850657	192.168.1.1	192.168.1.96	DNS	96	Standard query response 0x23e4 A lounge-haarstudio.nl A 145.131.10.21
310	319.852035	192.168.1.96	145.131.10.21	TCP	66	49190 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
311	320.008292	145.131.10.21	192.168.1.96	TCP	62	80 → 49190 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1440 SACK_PERM
312	320.008791	192.168.1.96	145.131.10.21	TCP	60	49190 → 80 [ACK] Seq=1 Ack=1 Win=64800 Len=0
313	320.009030	192.168.1.96	145.131.10.21	HTTP	200	GET /oud/trow.exe HTTP/1.1
314	320.168723	145.131.10.21	192.168.1.96	TCP	54	80 → 49190 [ACK] Seq=1 Ack=147 Win=8576 Len=0
315	320.173405	145.131.10.21	192.168.1.96	TCP	346	80 → 49190 [PSH, ACK] Seq=1 Ack=147 Win=8576 Len=292 [TCP PDU reassembled in 656]
316	320.173631	145.131.10.21	192.168.1.96	TCP	1221	80 → 49190 [PSH, ACK] Seq=293 Ack=147 Win=8576 Len=1167 [TCP PDU reassembled in 656]

Figure 2- Wireshark capture related to trow.exe

The investigator was able to recover this file through the "Export HTTP Objects" feature in Wireshark and kept the file safe to perform further analysis later in their methodology.

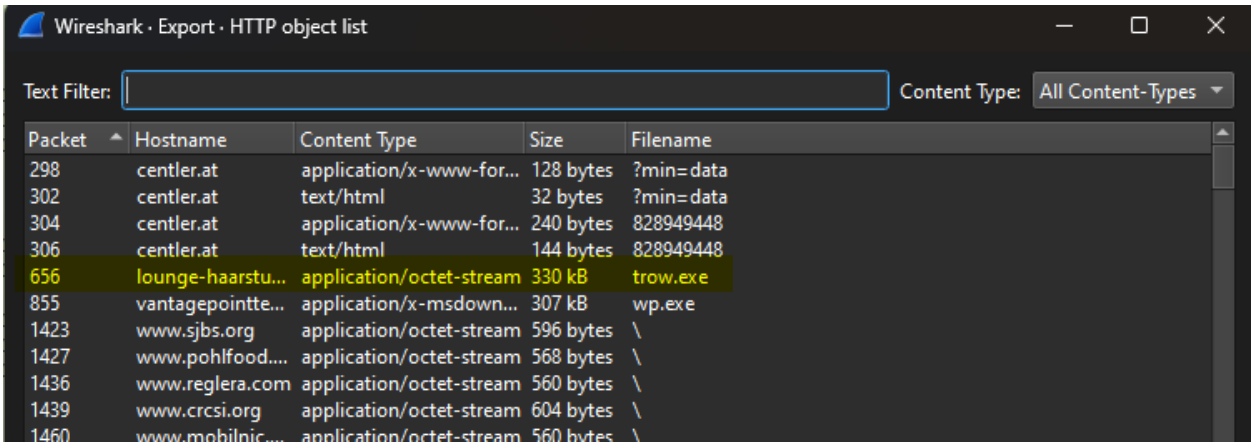


Figure 3 - Exporting trow.exe through Wireshark

This process was then repeated later on during the process after further traffic was created the process previously mentioned was completed for “t64.bin” and “wp.exe” which were both further files downloaded throughout the collection process.

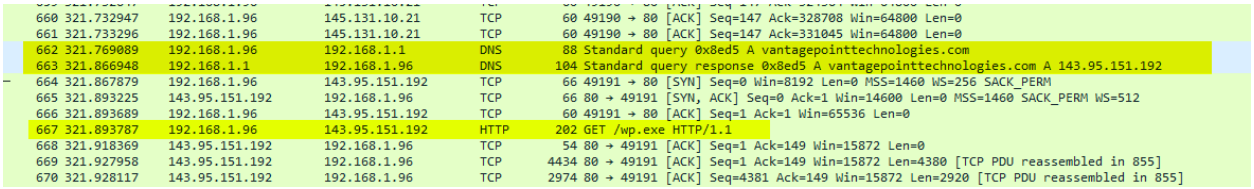


Figure 4 - Wireshark capture related to wp.exe

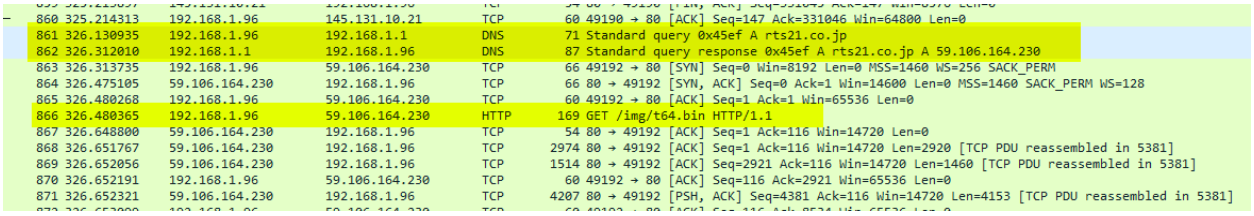


Figure 5 - Wireshark capture related to t64.bin

3.1.2 NetworkMiner

NetworkMiner was used to collect information that was otherwise unavailable through Wireshark. Of particular interest to the investigator was, “gerv.gun” as it had been irretrievable before the usage of this tool and appeared to be the first piece of the puzzle for the investigator. NetworkMiner collected and downloaded all of the IP addresses and resources accessed throughout the packet capture and sure enough for the investigator, this included the file they had been looking for. They were now able to perform necessary analysis on these files to further understand what they were doing.

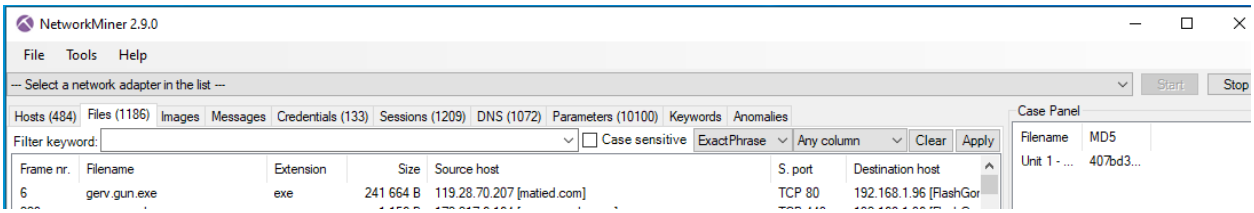


Figure 6 - NetworkMiner capturing gerv.gun

3.1.3 Snort

Snort was present and running on the machine that was infected in this situation with rules present to catch a variety of things including malware being used across the network, executable files being downloaded and sensitive data being processed. The investigator recreated a rule to imitate some of the alerts present in the alert file including the alerts regarding portable executables files being downloaded.

```
[**] [1:15306:22] FILE-EXECUTABLE Portable Executable binary file magic
detected [**]
[Classification: Potential Corporate Privacy Violation] [Priority: 1]
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
```

Figure 7 - Snort alert given to the investigator

From this alert, the investigator utilised various resources to assist with re-creating a rule to find this alert including a Snort 2 Manual (Snort Team, 2020). Through their research, they were able to recreate a rule that would successfully detect portable executable files.

```
root@machine:/etc/snort/rules# cat coursework.rules
alert tcp $EXTERNAL_NET 80 -> $HOME_NET any (msg:"FILE-EXECUTABLE Portable Executable Magic Found"; content:"|4D 5A|", offset 0; priority: 1; classtype:
 policy-violation; sid: 12351671;)
root@machine:/etc/snort/rules#
```

Figure 8 - Investigator's rule to determine Portable Executable files

```
06/27-13:44:33.928633  [**] [1:12351671:0] FILE-EXECUTABLE Portable Executable Magic Found [**] [Classification: Potential Corporate Privacy Violation]
[Priority: 1] {TCP} 208.83.223.34:80 -> 192.168.1.96:49932
06/27-13:44:33.939580  [**] [1:12351671:0] FILE-EXECUTABLE Portable Executable Magic Found [**] [Classification: Potential Corporate Privacy Violation]
[Priority: 1] {TCP} 208.83.223.34:80 -> 192.168.1.96:49932
```

Figure 9 - Output from Investigator's rule show Portable Executable files

3.2 ANALYSIS

3.2.1 Wireshark

Through the use of the Wireshark captures collected in the previous section of this report the investigator was able to create a timeline of events and make some assumptions about the situation and how it may have transpired. It appears that in the beginning of the analysis file the infected machine made a DNS query which contained a malicious record to a domain which was hosting malware, which is where “gerv.gun” was downloaded.

After the file has successfully been downloaded, there are some further queries through TLS before another query to a separate website, “lounge-haarstudio.nl” where “trow.exe” is downloaded. Purely through Wireshark, the investigator was not able to determine what this executable was doing but through later analysis, it became clear that this was performing privilege escalation on the victim’s machine.

As these files are being downloaded, the investigator felt it worth mentioning numerous requests to various websites to download javascript files and are then obfuscated and attemptedly passed through as email data across SMTP. This is consistent with the information reported to be associated with the “Malspam” malware (Duncan, 2015).

Finally, a third website is queried, “vantagepointtechnologies.com” where “wp.exe” is downloaded. Similarly to “trow.exe”, it is hard to identify through Wireshark what this executable was doing but shortly after the executable was downloaded, numerous DNS queries were made to a massive number of domains.

5508	339.652911	192.168.1.1	192.168.1.96	DNS	107	Standard query response 0x0f30 A alt4.gmail-smtp-in.l.google.com A 64.233.186.27
5509	339.658455	192.168.1.96	192.168.1.1	DNS	70	Standard query 0xac06 A cbaben.com
5510	339.658563	192.168.1.96	192.168.1.1	DNS	68	Standard query 0xa687 A umcor.am
5511	339.666327	192.168.1.1	192.168.1.96	DNS	86	Standard query response 0xda4b A oh28ya.com A 54.178.140.67
5513	339.667333	192.168.1.96	192.168.1.1	DNS	86	Standard query 0x85c7 A gmail-smtp-in.l.google.com
5514	339.667382	192.168.1.96	192.168.1.1	DNS	71	Standard query 0x9d55 A reproar.com
5515	339.667732	192.168.1.96	192.168.1.1	DNS	69	Standard query 0x284d A plaske.ua
5516	339.674324	192.168.1.96	192.168.1.1	DNS	72	Standard query 0x8741 A a-domani.com
5517	339.676020	192.168.1.96	192.168.1.1	DNS	72	Standard query 0x5718 A softizer.com
5520	339.678495	192.168.1.1	192.168.1.96	DNS	84	Standard query response 0xa687 A umcor.am A 31.7.163.133
5522	339.679564	192.168.1.96	192.168.1.1	DNS	72	Standard query 0xbab4 A yoruksut.com
5523	339.679594	192.168.1.96	192.168.1.1	DNS	72	Standard query 0x6667 A aiolos-sa.gr
5524	339.679665	192.168.1.96	192.168.1.1	DNS	71	Standard query 0xd466 A simetar.com
5525	339.679684	192.168.1.1	192.168.1.96	DNS	88	Standard query response 0xbab4 A yoruksut.com A 184.168.221.25
5527	339.680461	192.168.1.96	192.168.1.1	DNS	71	Standard query 0x08b0 A sokuwan.net
5528	339.680511	192.168.1.96	192.168.1.1	DNS	72	Standard query 0xff98 A amerifor.com
5529	339.680711	192.168.1.96	192.168.1.1	DNS	72	Standard query 0x4eed A kustnara.com
5530	339.681010	192.168.1.96	192.168.1.1	DNS	69	Standard query 0xb004 A uster.com
5531	339.685470	192.168.1.1	192.168.1.96	DNS	102	Standard query response 0xb3db A gmail-smtp-in.l.google.com A 173.194.223.27
5532	339.686153	192.168.1.96	192.168.1.1	DNS	72	Standard query 0x0269 A okashimo.com
5533	339.686274	192.168.1.1	192.168.1.96	DNS	86	Standard query response 0xac06 A cbaben.com A 173.205.126.33
5534	339.688150	192.168.1.96	192.168.1.1	DNS	72	Standard query 0xd9d6 A fogra.com.pl
5536	339.691744	192.168.1.96	192.168.1.1	DNS	72	Standard query 0xa13b A biurohera.pl
5537	339.691996	192.168.1.96	192.168.1.1	DNS	72	Standard query 0x24fa A kustnara.com
5538	339.692442	192.168.1.96	192.168.1.1	DNS	70	Standard query 0xe8cb A nekono.net
5539	339.692941	192.168.1.96	192.168.1.1	DNS	71	Standard query 0x00b7 A webband.com
5540	339.693041	192.168.1.96	192.168.1.1	DNS	69	Standard query 0xeba2 A dayvo.com
5541	339.693047	192.168.1.96	192.168.1.1	DNS	70	Standard query 0x860e A kavram.com
5543	339.698164	192.168.1.1	192.168.1.96	DNS	85	Standard query response 0x284d A plaske.ua A 91.208.115.22
5544	339.698832	192.168.1.96	192.168.1.1	DNS	69	Standard query 0xed67 A jsaps.com
5545	339.698981	192.168.1.96	192.168.1.1	DNS	72	Standard query 0x1f05 A karmy.com.pl
5546	339.699001	192.168.1.1	192.168.1.96	DNS	88	Standard query response 0x5718 A softizer.com A 46.4.194.22
5548	339.699432	192.168.1.96	192.168.1.1	DNS	69	Standard query 0xeb71 A amele.com
5549	339.701329	192.168.1.96	192.168.1.1	DNS	69	Standard query 0x47ec A slower.it
5550	339.702332	192.168.1.96	192.168.1.1	DNS	72	Standard query 0x62cf A sledsport.ru
5552	339.703878	192.168.1.96	192.168.1.1	DNS	69	Standard query 0x2c01 A akr.co.id

Figure 10 - DNS Queries after downloading wp.exe

3.2.2 VirusTotal

As mentioned in the previous section, the investigator noticed numerous files being downloaded and successfully captured them through the Collection section of their methodology. Each executable was uploaded to VirusTotal and in all three cases, were found to be highly malicious.

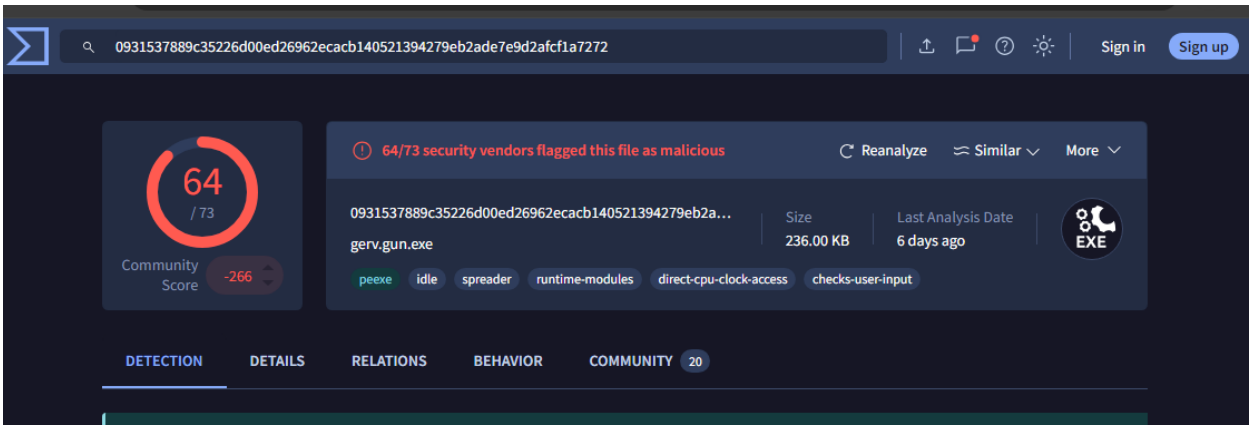


Figure 11 - VirusTotal of gerv.gun

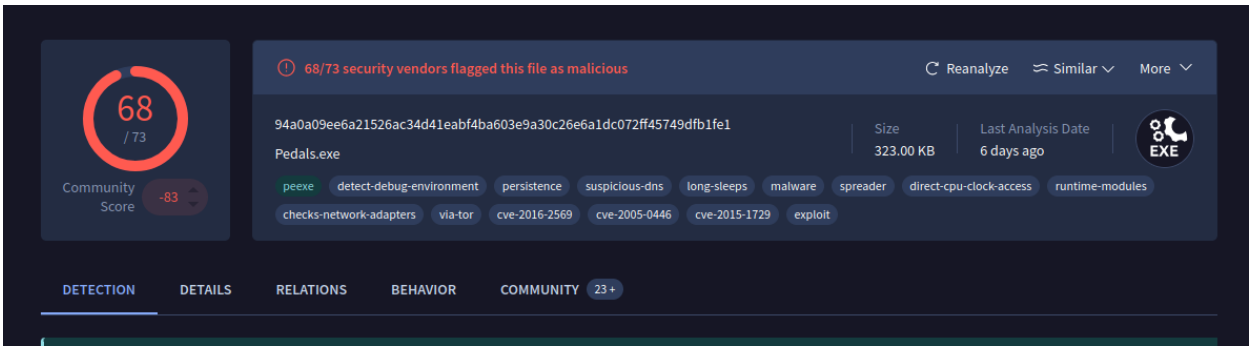


Figure 12 - VirusTotal of trow.exe

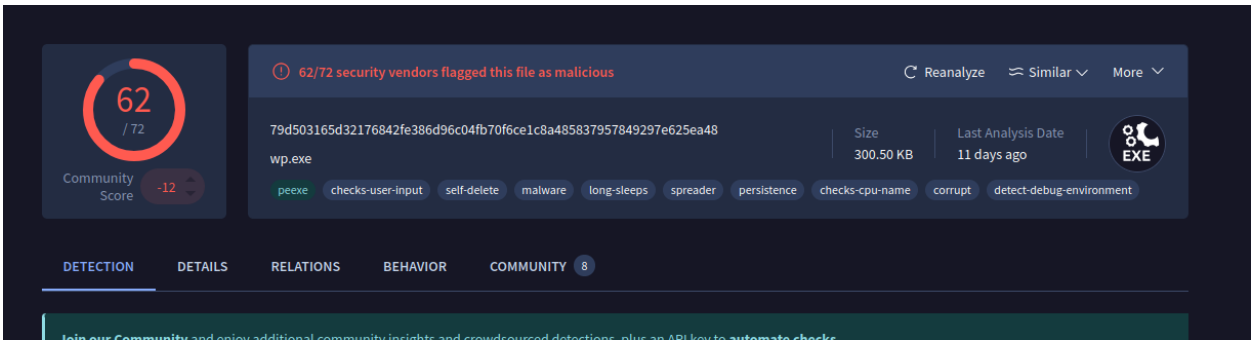


Figure 13 - VirusTotal of wp.exe

Based on the research present on VirusTotal, the investigator was able to determine that “gerv.gun” was utilised to distribute additional pieces of malware, hence “trow.exe” and “wp.exe” being downloaded after this file.

The CVE’s associated with “trow.exe” appear to be for denial-of-service attacks related to the Squid framework, which is a caching proxy used for supporting various networking protocols (squidadm, 2013).

3.2.3 Snort Alert Analysis

The first alert that was of particular interest to the investigator was further backup of the “gerv.gun” file being download and a Sensitive Data Flag (SDF) alert follows which indicates that sensitive personal information has been leaked. The investigator can be sure that these are related due to the IP and timings present in both documents.

```
[**] [1:11192:20] FILE-EXECUTABLE download of executable content [**]
[Classification: Potential Corporate Privacy Violation] [Priority: 1]
06/27-13:38:34.111294 119.28.70.207:80 -> 192.168.1.96:49184
TCP TTL:128 TOS:0x0 ID:648 IpLen:20 DgmLen:19976 DF
***A**** Seq: 0xEEED7BAB  Ack: 0xA337D497  Win: 0x500  TcpLen: 20
[Xref => http://www.microsoft.com/smallbusiness/resources/technology/security/practice_safe_computing_and_thwart_online_thugs.mspx]

[**] [139:1:1] (spp_sdf) SDF Combination Alert [**]
[Classification: Senstive Data] [Priority: 2]
06/27-13:38:34.536182 119.28.70.207 -> 192.168.1.96
PROTO:254 TTL:128 TOS:0x0 ID:661 IpLen:20 DgmLen:20 DF
```

Figure 14 - Snort alert related to gerv.gun

Based on research present on VirusTotal the investigator was able to determine that “gerv.gun” was a strain of the Kazy malware and therefore utilised for installing additional pieces of malware (F-Secure, nd). This is then further supported by a Snort alert that references this malware strain.

```
[**] [1:28406:1] MALWARE-CNC Win.Trojan.Kazy variant outbound connection [**]
[Classification: A Network Trojan was detected] [Priority: 1]
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
[Xref => http://www.virustotal.com/en/file/a064a1d3d8b9d8ab649686b7fb01e0631e569412388084f5c391722c98660763/analysis/]
```

Figure 15 - Kazy Malware mentioned by Snort alert

As the investigator continued to review the alert file, they were curious about references to various CVE's that are mentioned throughout the log and found specific references to buffer overflow vulnerabilities which can be found in greater detail in Appendix A - Snort CVE Analysis. From the investigator's analysis of the CVE's found through Snort it is assumed that the recently downloaded piece of malware was attempting attacks against targets to pivot from this machine or establish its persistence. This is further supported throughout, due to the increase in references to C2 servers through the "Pushdo" malware. Pushdo is a similar strain of malware to Kazy but in this case appears to be focusing on connecting to a C2 server, by which point, we can assume is the "wp.exe" controlling the system.

```
[**] [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

[**] [1:23832:4] INDICATOR-OBFUSCATION non-alphanumeric javascript detected [**]
[Classification: Attempted User Privilege Gain] [Priority: 1]
06/27-13:44:12.167716 104.31.81.138:80 -> 192.168.1.96:49425
TCP TTL:53 TOS:0x0 ID:51059 IpLen:20 DgmLen:2960 DF
***A**** Seq: 0xDDCE4C31  Ack: 0x16030D0B  Win: 0x1F  TcpLen: 20
[Xref => http://patriciopalladino.com/blog/2012/08/09/non-alphanumeric-javascript.html]

[**] [1:29891:7] MALWARE-CNC Win.Trojan.Pushdo variant outbound connection [**]
[Classification: A Network Trojan was detected] [Priority: 1]
06/27-13:44:12.106796 192.168.1.96:49329 -> 97.74.42.79:80
TCP TTL:113 TOS:0x0 ID:30951 IpLen:20 DgmLen:497 DF
***A**** Seq: 0xE760F116  Ack: 0xFEA133DB  Win: 0xFD5C  TcpLen: 20
```

Figure 16 - Pushdo Malware Snort alerts

4 DISCUSSION

4.1 GENERAL DISCUSSION

The investigator utilised numerous techniques to successfully attribute and document the timeline of events throughout the packet captures to the Kazy and Pushdo malware strains, followed by connections to a C2 server. Amongst the techniques used included snort analysis, file carving and packet analysis to determine not only the compromised host, (192.168.1.96) but also the cause of the compromise. The host was compromised due to a malicious DNS query which, whilst directing to the website the user had intended to load, also downloaded a malicious executable file and then downloaded additional files, consequently leading to the complete take-over of this machine.

Although the investigator was successful with their analysis of this scenario, in future situations the investigator would have set up additional logging and defensive tools to both help gather information on the victim machine such as Systems Information and Event Management (SIEM) solutions such as Microsoft Sentinel One which would have been able to provide the investigator with additional logging resources.

4.2 CONCLUSION

To conclude, the investigator was present with packet capture files from an incident which highlighted a victim machine which, through a malicious DNS query, was infected with multiple “downloader” malwares, which were responsible for downloading additional pieces of malware. As a result of these viruses, the targeted machine was converted into a “zombie” which would respond to requests from a certain machine which would be used to manage all infected devices.

5 REFERENCES

Duncan, B., 2015. *Malicious spam with zip attachments containing .js files.* [Online]
Available at: https://isc.sans.edu/diary/20153
[Accessed 5 11 2024].

F-Secure, nd. *Trojan-Downloader:W32/Kazy-17907.* [Online]
Available at: https://www.f-secure.com/v-descs/trojan-downloader-w32-kazy17907.shtml
[Accessed 1 November 2024].

Qureshi, S., Rajputt, F. A., Quershi, S. S. & Wajahat, A., 2021. *ResearchGate.* [Online]
Available at: https://www.researchgate.net/profile/Sirajuddin-Qureshi/publication/351998718_Network_Forensics_A_Comprehensive_Review_of_Tools_and_Techniques/links/60b4db2ba6fdcc1c66f57f65/Network-Forensics-A-Comprehensive-Review-of-Tools-and-Techniques.pdf?origin=publi
[Accessed 1 November 2024].

Snort Team, 2020. *Snor User Manual.* [Online]
Available at: https://snort-org-site.s3.amazonaws.com/production/document_files/files/000/000/249/original/snort_manual.pdf
[Accessed 23 October 2024].

squidadm, 2013. *squid-cache.or.* [Online]
Available at: https://www.squid-cache.org/
[Accessed 4 November 2024].

The MITRE Corporation, 2015. *CVE-2015-1729.* [Online]
Available at: https://cve.mitre.org/cgi-bin/cvename.cgi?name=2015-1729
[Accessed 3 November 2024].

6 APPENDICES

6.1 APPENDIX A - SNORT CVE ANALYSIS

CVE	Description
CVE-2015-1729	Internet Explorer buffer overflow
CVE-2014-6345	Internet Explorer buffer overflow
CVE-2013-2028	Denial of Service in Nginx function
CVE-2005-0560	Code execution in SMTP function
CVE-2002-1090	Code execution in SMTP function
CVE-2001-0260	Code execution in SMTP function

6.1.1 CVE-2015-1729

This is a vulnerability present in versions of Internet Explorer 9 and 11 which was likely to be used by the Pushdo Malware, wp.exe to try and read information from different domains or network zones through a maliciously crafted website. (The MITRE Corporation, 2015). This can be seen through the Snort analysis as requests are made via the infected machine located at 192.168.1.96.

6.1.2 CVE-2014-6345

This is a similar vulnerability to CVE-2015-1729 but instead focuses on Internet Explorer 9 and 10. It is thought that the malware was testing these vulnerabilities on various versions to see whether there was any success with installed programs on the infected machine.

6.1.3 CVE-2013-2028

This is a vulnerability present in an Nginx function whereby attackers are able to pass a large amount of data through the Transfer-Encoding header and trigger a buffer overflow vulnerability, causing a denial of service attack against the host with the possibility to be elevated into arbitrary code execution for the attacker. There are various Snort alerts found throughout the file that support this exploit being attempted.

```
[**] [120:8:2] (http_inspect) INVALID CONTENT-LENGTH OR CHUNK SIZE [**]
[Classification: Unknown Traffic] [Priority: 3]
06/27-13:44:05.882871 192.168.1.96:49260 -> 184.168.221.25:80
TCP TTL:128 TOS:0x0 ID:2489 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x7C355E51  Ack: 0x7400ED12  Win: 0xFA82  TcpLen: 20
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2013-2028]
```

Figure 17 - CVE-2013-2028 Snort alert

6.1.4 CVE-2005-0560

This CVE is related to an SMTP function where attackers are able to execute arbitrary code through an SMTP request. The investigator believes that this CVE was used in contention with the Malspam malware which attempts to send malicious JavaScript data to SMTP ports in an attempt to gain code execution over the system.

```
[**] [1:23832:4] INDICATOR-OBFUSCATION non-alphanumeric javascript detected [**]
[Classification: Attempted User Privilege Gain] [Priority: 1]
06/27-13:44:08.765489 104.27.139.76:80 -> 192.168.1.96:49292
TCP TTL:53 TOS:0x0 ID:15927 IpLen:20 DgmLen:5129 DF
***AP*** Seq: 0xCECA6E07  Ack: 0x234866D1  Win: 0x1F  TcpLen: 20
[Xref => http://patriciopalladino.com/blog/2012/08/09/non-alphanumeric-javascript.html]
```

Figure 18 - Malspam Javascript Snort Alert

```
[**] [124:1:1] (smtp) Attempted command buffer overflow: more than 512 chars [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
06/27-13:44:12.121223 192.168.1.96:49373 -> 198.54.126.63:25
TCP TTL:128 TOS:0x0 ID:6169 IpLen:20 DgmLen:836 DF
***A*R** Seq: 0xE4EE821E  Ack: 0x7046EBC9  Win: 0x4000  TcpLen: 20
[Xref => http://www.microsoft.com/technet/security/bulletin/ms05-021.mspx][Xref => ht
```

Figure 19 - CVE-2005-0560 Snort Alert

6.1.5 CVE-2002-1090

This CVE is similarly related to a previous SMTP function that would allow attackers to either execute arbitrary code or cause denial of service attacks against the target. Although the investigator cannot be sure this was used, as there seems to be a large amount of SMTP data.

6.1.6 CVE-2001-0260

Similarly to the previous CVE, this is an exploit in the Lotus Domino Mail Server 5.0.5 which can allow remote code execution or denial of service attacks through the “RCPT TO” function.