Unit 1

[Redacted]

CMP416: Advanced Digital Forensics

2024/25

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

.

Contents

.

1 INTRODUCTION

1.1 BACKGROUND

Digital forensics is the process through which electronically stored data is collected and analyzed. Within this is the domain of network forensics, covering data transmitted using elements such as wireless and mobile networks. Network forensic data can be gathered through a variety of means, such as capturing all network traffic passively and filtering it after the fact, or setting up systems which automatically detect and alert administrators when potential problems/areas of interest may arise. Network forensics is typically considered a form of “active” or “proactive” forensics, in that if systems are not configured to collect data as a problem arises, native systems are unlikely to retain much information in relation to a breach which speaks to the need for solid configuration of data collection systems and rulesets to allow for post-exploitation analysis.

1.2 AIM

The four aims of this project are:

- Understand a Snort alert and re-create the rules therein
- Identify the compromised computer
- Investigate the cause of the compromise
- Determine what the computer was compromised with

2 PROCEDURE

2.1 TOOLS

Tool	Version	Usage
Wireshark	3.6.8	Network traffic monitoring and analysis
SNORT	2.9.17GRE	Alert rules reconstruction and testing
Notepad++	8.6	Data interpretation
NetworkMiner	2.9.0.0	File extraction

2.2 METHODOLOGY

The examiner was provided with a .pcap file and a snort alert text file.

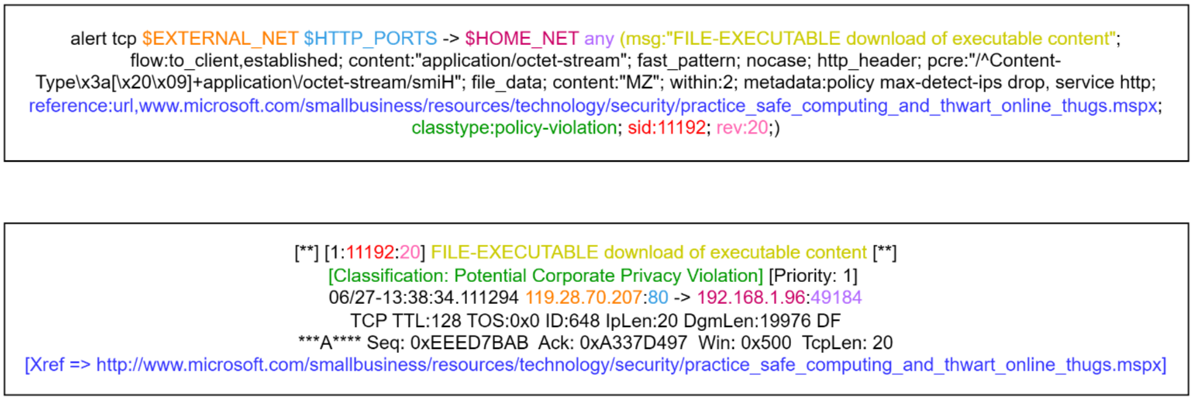
2.2.1 Snort Alert File and Reconstruction

To begin with, the snort file was examined using Notepad++ with the intent of reconstructing the ruleset based on the alerts present based on the tester's knowledge of SNORT and the relevant documentation for SNORT 2 (Team Snort, n.d.). It also provided a cursory impression of the incident through simply observing the alerts present. Some areas of immediate note were alerts titled the following:

- "FILE-EXECUTABLE download of executable content"
- "MALWARE-CNC Win.Trojan.Kazy variant outbound connection"
- "MALWARE-CNC Win.Trojan.Pushdo variant outbound connection"

which provided a strong indication of a malware-based infection, likely from a file download.

To begin with reconstruction, unique rule names were obtained as shown in Appendix A (Source and destination addresses can vary, but rule names cannot, nor can SID's). Then identifiable information was worked out, with Appendix B detailing the brief deconstruction of the unique alerts into a more usable format and another example of this translation can also be seen in Figure 1**Error! Reference source not found.**. Appendix C provides the ruleset constructed.



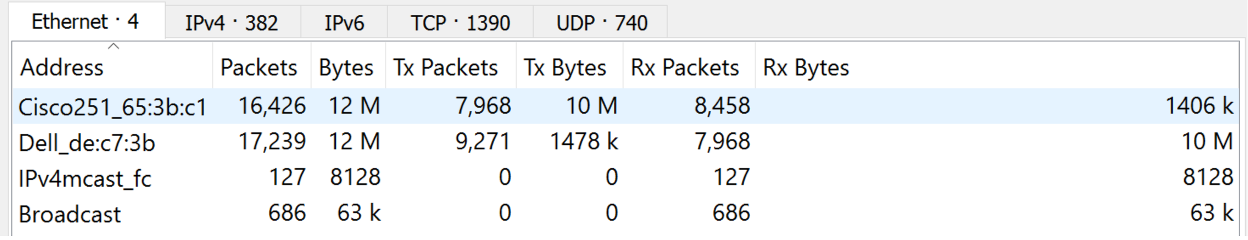
```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"FILE-EXECUTABLE download of executable content";
flow:to_client,established; content:"application/octet-stream"; fast_pattern; nocase; http_header; pcre:"/^Content-
Type\x3a[\x20\x09]+application\/octet-stream/smiH"; file_data; content:"MZ"; within:2; metadata:policy max-detect-ips drop, service http;
reference:url,www.microsoft.com/smallbusiness/resources/technology/security/practice_safe_computing_and_thwart_online_thugs.mspx;
classtype:policy-violation; sid:11192; rev:20;)
```

```
[**] [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]
```

Figure 1 - Snort Rule elements present in alerts

2.2.2 Device Compromise Analysis

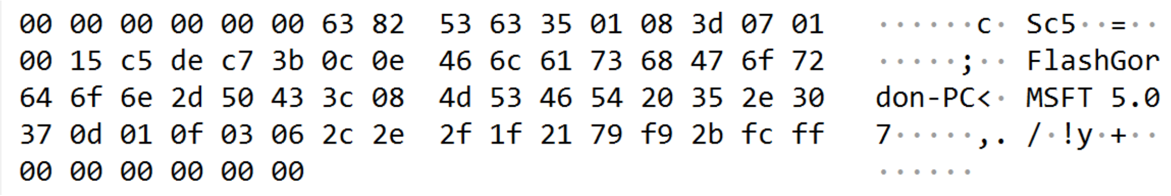
Device and exploit analysis was performed initially through Wireshark. To establish the possible infected devices, the examiner navigated to Statistics > Endpoints > Ethernet - this listed all of the unique MAC addresses and thus all possible infected devices, significantly narrowing the scope of the search (see Figure 2).



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
Cisco251_65:3b:c1	16,426	12 M	7,968	10 M	8,458	1406 k
Dell_de:c7:3b	17,239	12 M	9,271	1478 k	7,968	10 M
IPv4mcast_fc	127	8128	0	0	127	8128
Broadcast	686	63 k	0	0	686	63 k

Figure 2 - Ethernet endpoints

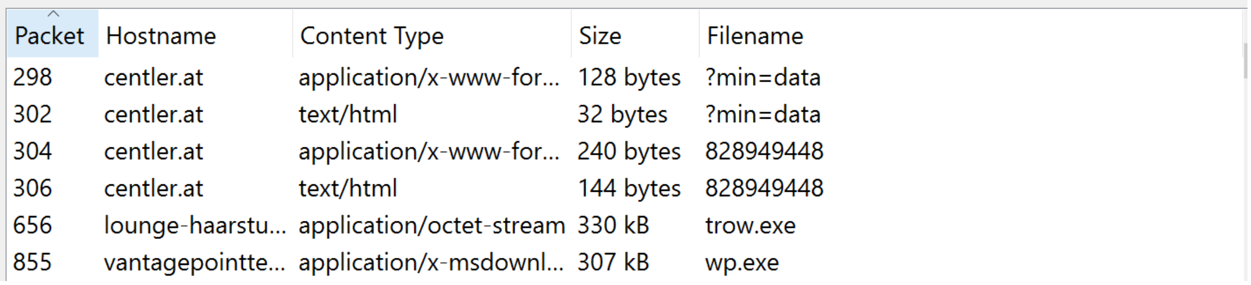
Subsequently ordering the protocols alphabetically showed a DHCP connection, which can be used to obtain device information. In this case, it indicated the PC name as “FlashGordon-PC” (see Figure 3)



```
00 00 00 00 00 00 63 82  53 63 35 01 08 3d 07 01   ······c· Sc5··=··
00 15 c5 de c7 3b 0c 0e  46 6c 61 73 68 47 6f 72   ·····;·· FlashGor
64 6f 6e 2d 50 43 3c 08  4d 53 46 54 20 35 2e 30   don-PC<· MSFT 5.0
37 0d 01 0f 03 06 2c 2e  2f 1f 21 79 f9 2b fc ff   7·····,. /·!y·+··
00 00 00 00 00 00                                  ······
```

Figure 3- FlashGordon-PC PC shown in Option: Host Name

After this in order to quickly ascertain possible malware vectors, file > export objects > http was used which automatically showed files downloaded using the specified protocol. Two items of note were “trow.exe” and “wp.exe” (see Figure 4)

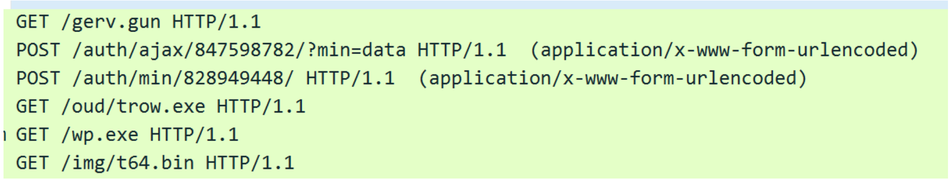


Packet	Hostname	Content Type	Size	Filename
298	centler.at	application/x-www-for...	128 bytes	?min=data
302	centler.at	text/html	32 bytes	?min=data
304	centler.at	application/x-www-for...	240 bytes	828949448
306	centler.at	text/html	144 bytes	828949448
656	lounge-haarstu...	application/octet-stream	330 kB	trow.exe
855	vantagepointte...	application/x-msdownl...	307 kB	wp.exe

Figure 4 - Relevant Exported Objects

These were both http GET requests, and a third relevant element gerv.gun was shown by examining that type of request through packet filtering within the pcap using the filter:

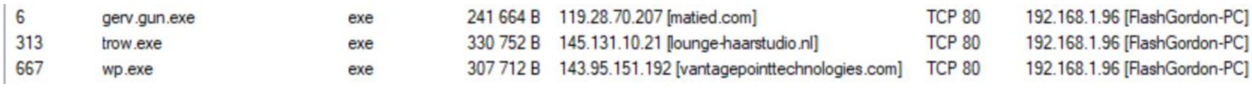
(http.request)



```
GET /gerv.gun HTTP/1.1
POST /auth/ajax/847598782/?min=data HTTP/1.1  (application/x-www-form-urlencoded)
POST /auth/min/828949448/ HTTP/1.1  (application/x-www-form-urlencoded)
GET /oud/trow.exe HTTP/1.1
GET /wp.exe HTTP/1.1
GET /img/t64.bin HTTP/1.1
```

Figure 5 - Get request to /gerv.gun

This was then cross referenced with the SNORT Alert to see if it triggered anything based on the timecode. This was not the case as the first snort alert begins at 13:38:34 whereas the /gerv.gun file was obtained at 13:38:32, meaning 2 seconds before the snort alerts began. /gerv.gun did not show up for extraction within wireshark, so automatic file carving was performed with NetworkMiner instead, which also served to automatically confirm the hostname.



6	gerv.gun.exe	exe	241 664 B	119.28.70.207 [matied.com]	TCP 80	192.168.1.96 [FlashGordon-PC]
313	trow.exe	exe	330 752 B	145.131.10.21 [lounge-haarstudio.nl]	TCP 80	192.168.1.96 [FlashGordon-PC]
667	wp.exe	exe	307 712 B	143.95.151.192 [vantagepointtechnologies.com]	TCP 80	192.168.1.96 [FlashGordon-PC]

Figure 6 - gerv.gun.exe as shown in NetworkMiner

These files were then placed into to Virustotal for analysis.

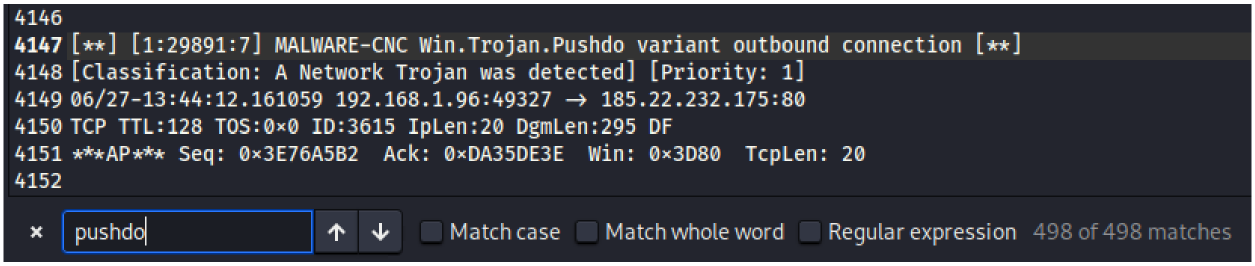
Additionally, Virustotal has an inbuilt PCAP analyzer which the examiner employed in order identify malicious external connections, files and other elements that had been previously found as a verification measure.

3 RESULTS

As part of understanding and recreating snort rules, the snort.alert file given alongside the submission shows sample output from running the PCAP against the recreated rules. Appendix E features a measurement of the accuracy of these rules by comparing the newly obtained alerts to the provided alert file, demonstrating approximately 99.1% accuracy in recreating **ALL** alerts from the provided file with this ruleset.

The compromised computer was Dell_de aka FlashGordon-PC - likely a Dell Desktop running Windows based on the resolved name, hostname and user agent packets. From the downloaded files, specifically Gerv.gun, an exe downloaded after a DNS query to “Matied.com”, it was suggested the compromise was due to malware spam emails (My Online Security, n.d.) as indicated by online searching.

The computer was likely compromised with a Pushdo trojan, based on the 498 SNORT alerts in relation to those connections (see Figure 7)



```

[**] [1:29891:7] MALWARE-CNC Win.Trojan.Pushdo variant outbound connection [**]
[Classification: A Network Trojan was detected] [Priority: 1]
06/27-13:44:12.161059 192.168.1.96:49327 -> 185.22.232.175:80
TCP TTL:128 TOS:0x0 ID:3615 IpLen:20 DgmLen:295 DF
***AP*** Seq: 0x3E76A5B2  Ack: 0xDA35DE3E  Win: 0x3D80  TcpLen: 20

```

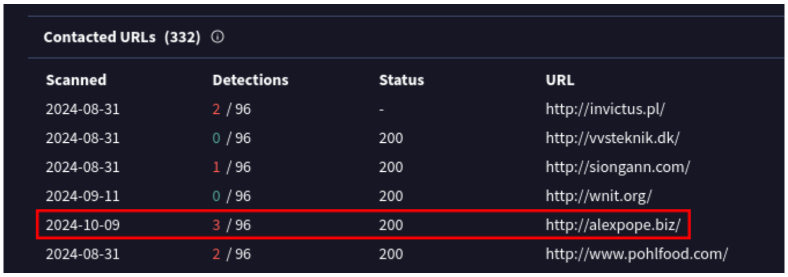
Figure 7 - Pushdo connection alert and count

Furthermore, this trojan downloaded 3 malicious files.

- WP.exe
- trow.exe
- Gerv.gun

This aligned with how this trojan typically operates (Stewart, 2007). Appendix E showed the virustotal scans indicating all of the files were malicious. Notably, Trow.exe was of type “trojan.cutwail/wigon” which is believed to come from the same group as Pushdo (Stewart, 2007) further indicating the likelihood of pushdo being used.

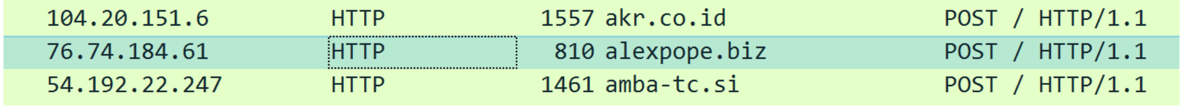
These files then began contacting external addresses, which could be shown by comparing the hosts contacted in Virustotal and the hosts within the pcap. For example when examining trow.exe, alexpope.biz was present in both, indicating subsequent host contacts (see Figure 8 and Figure 9)



Contacted URLs (332)

Scanned	Detections	Status	URL
2024-08-31	2 / 96	-	http://invictus.pl/
2024-08-31	0 / 96	200	http://vvsteknik.dk/
2024-08-31	1 / 96	200	http://siongann.com/
2024-09-11	0 / 96	200	http://wnit.org/
2024-10-09	3 / 96	200	http://alexpope.biz/
2024-08-31	2 / 96	200	http://www.pohlfood.com/

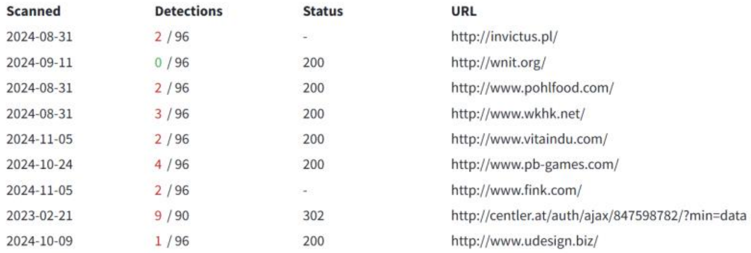
Figure 8 - Virustotal contacted URL's showing alexpope.biz



104.20.151.6	HTTP	1557 akr.co.id	POST / HTTP/1.1
76.74.184.61	HTTP	810 alexpope.biz	POST / HTTP/1.1
54.192.22.247	HTTP	1461 amba-tc.si	POST / HTTP/1.1

Figure 9 - alexpope.biz shown in pcap

This was only one example of external malicious addresses contacted, multiple others were easily visible by placing the pcap file within virustotal as seen below in Figure 10.



Scanned	Detections	Status	URL
2024-08-31	2 / 96	-	http://invictus.pl/
2024-09-11	0 / 96	200	http://wnit.org/
2024-08-31	2 / 96	200	http://www.pohlfood.com/
2024-08-31	3 / 96	200	http://www.wkhk.net/
2024-11-05	2 / 96	200	http://www.vitaindu.com/
2024-10-24	4 / 96	200	http://www.pb-games.com/
2024-11-05	2 / 96	-	http://www.fink.com/
2023-02-21	9 / 90	302	http://centler.at/auth/ajax/847598782/?min=data
2024-10-09	1 / 96	200	http://www.udesign.biz/

Figure 10 - Virustotal analysis of PCAP file indicating multiple malicious URLs

4 DISCUSSION

4.1 GENERAL DISCUSSION

Understanding the Snort alerts presented some difficulty, with significant time being occupied with pcre (Perl Compatible Regular Expressions) which essentially is regex for perl to produce similar output. Elements such as SID and Revision number were easy to replicate based on alert parsing, with some regex elements matching existing rules that could be found online. In terms of technical decisions, Snort 2 was used as it was recommended, the rule output matched it, and the documentation for Snort 3 is lacking in regards to syntax. Overall this was immensely time consuming but proved to be successful in producing similar output. One additional element of note is that the provided Snort alert file was likely cut short or failed to identify the initial point of breach, meaning a new rule should be implemented to catch downloads of Gerv.gun if this is the case.

Identifying the compromised computer presented little problem on account of the fact that there was only one valid device that represented an infection vector. The method of assessment took very little time owing to wireshark's easy to use GUI. Then determining what the computer was compromised with was already strongly signaled through reading the Snort alert file, with the majority of it being made of PushDo network trojans (498 alerts), with wireshark providing clear indications of the malicious executables. NetworkMiner proved to exceed wireshark's usefulness and would form the backbone of analysis if this project was repeated due to it's better file extraction capabilities and OS recognition.

Something to note is that virustotal when analyzing the pcap provided the same snort alerts as within the file provided, and virustotal makes use of the sourcefile VRT ruleset (Virustotal, n.d.) – meaning identifying the ruleset being employed was not significantly difficult.

The overall implication of these findings indicates that the network was likely compromised due to human error in relation to email attachments, and either more stringent policies should be implemented preventing the download of external files, or internal training should be conducted to prevent this.

5 CONCLUSION

In conclusion, the examiner was able to essentially fully recreate the snort file purely from the provided alert capture, with an accuracy of over 99%. The examiner succeeded in identifying all information relevant to the breach by employing modern digital forensic techniques, up to and including the PC name, original cause of compromise, and what the compromise entailed. This indicated that post-exploitation analysis was effective and served to provide a detailed recollection of the incident, strongly providing justification for intrusion detection systems and networking logging.

6 REFERENCES

My Online Security, n.d. *Japanese Language Invoice Malspam Using Js Files Inside Zips Today.* [Online]
Available at: https://myonlinesecurity.co.uk/japanese-language-invoice-malspam-using-js-files-inside-zips-today/
[Accessed 5 November 2024].

Stewart, J., 2007. *Pushdo - Analysis of a Modern Malware Distribution System.* [Online]
Available at: https://www.secureworks.com/research/pushdo
[Accessed 5 November 2024].

Team Snort, n.d. *Writing Snort Rules.* [Online]
Available at: http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node27.html
[Accessed 5 November 2024].

Virustotal, n.d. *Snort.* [Online]
Available at: https://docs.virustotal.com/reference/files-snort
[Accessed 6 November 2024].

APPENDICES

APPENDIX A - UNIQUE ALERT TITLES

```
FILE-EXECUTABLE download of executable content
(spp_sdf) SDF Combination Alert
FILE-EXECUTABLE Portable Executable binary file magic detected
MALWARE-CNC Win.Trojan.Kazy variant outbound connection
(http_inspect) INVALID CONTENT-LENGTH OR CHUNK SIZE
INDICATOR-OBFUSCATION obfuscated script encoding detected
(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE
INDICATOR-OBFUSCATION non-alphanumeric javascript detected
INDICATOR-OBFUSCATION potential javascript unescape obfuscation attempt detected
POLICY-OTHER Remote non-JavaScript file found in script tag src attribute
BROWSER-IE Microsoft Internet Explorer 7 emulation via meta tag
INDICATOR-COMPROMISE Suspicious .ru dns query
MALWARE-CNC Win.Trojan.Pushdo variant outbound connection
Consecutive TCP small segments exceeding threshold
(http_inspect) UNESCAPED SPACE IN HTTP URI
(smtp) Attempted command buffer overflow: more than 512 chars
BROWSER-OTHER local loopback address in html
SENSITIVE-DATA Email Addresses
```

APPENDIX B – DECONSTRUCTION OF UNIQUE ALERTS FOR RULE RECOMPILATION

Name	FILE-EXECUTABLE Portable Executable binary file magic detected
Classification	Classification: Potential Corporate Privacy Violation
Source	119.28.70.207:80 (External Net)
Dest	192.168.1.96:49184 (Home Net)
Reference	http://www.microsoft.com/smallbusiness/resources/technology/security/practice_safe_computing_and_thwart_online_thugs.mspx
Name	FILE-EXECUTABLE download of executable content
Classification	Potential Corporate Privacy Violation
Source	119.28.70.207:80 (External Net)
Dest	192.168.1.96:49184 (Home Net)
Reference	
Name	SDF Combination
Classification	Senstive Data
Source	145.131.10.21 (External Net)
Dest	192.168.1.96 (Home Net)
Reference	
Name	MALWARE-CNC Win.Trojan.Kazy variant outbound connection
Classification	A Network Trojan was detected
Source	192.168.1.96:49191 (Home Net)

Dest	143.95.151.192:80 (External Net)
Reference	
Name	(http_inspect) INVALID CONTENT-LENGTH OR CHUNK SIZE
Classification	Unknown Traffic
Source	192.168.1.96:49200 (Home Net)
Dest	96.82.200.1:80 (External Net)
Reference	
Name	INDICATOR-OBFUSCATION obfuscated script encoding detected
Classification	Misc activity
Source	148.251.33.194:80 (External Net)
Dest	192.168.1.96:49194 (Home Net)
Reference	
Name	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE
Classification	Unknown Traffic
Source	96.82.200.1:80 (External Net)
Dest	192.168.1.96:49200 (Home Net)
Reference	
Name	INDICATOR-OBFUSCATION non-alphanumeric javascript detected
Classification	Attempted User Privilege Gain
Source	104.28.18.104:80 (External Net)
Dest	192.168.1.96:49210 (Home Net)
Reference	http://patriciopalladino.com/blog/2012/08/09/non-alphanumeric-javascript.html
Name	INDICATOR-OBFUSCATION potential javascript unescape obfuscation attempt detected
Classification	Potential Corporate Privacy Violation
Source	74.208.215.199:80 (External Net)
Dest	192.168.1.96:49212 (Home Net)
Reference	
Name	POLICY-OTHER Remote non-JavaScript file found in script tag src attribute
Classification	Potential Corporate Privacy Violation
Source	184.168.47.225:80 (External Net)
Dest	192.168.1.96:49201 (Home Net)
Reference	http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6345
Name	BROWSER-IE Microsoft Internet Explorer 7 emulation via meta tag
Classification	Attempted User Privilege Gain
Source	211.1.226.69:80 (External Net)
Dest	192.168.1.96:49225 (Home Net)
Reference	
Name	INDICATOR-COMPROMISE Suspicious .ru dns query

Classification	A Network Trojan was detected
Source	192.168.1.96:51688 (Home Net)
Dest	192.168.1.1:53 (External Net)
Reference	
Name	MALWARE-CNC Win.Trojan.Pushdo variant outbound connection
Classification	A Network Trojan was detected
Source	192.168.1.96:49322 (Home Net)
Dest	104.27.158.125:80 (External Net)
Reference	
Name	Consecutive TCP small segments exceeding threshold
Classification	Potentially Bad Traffic
Source	192.154.109.132:80 (External Net)
Dest	192.168.1.96:49312 (Home Net)
Reference	
Name	BROWSER-OTHER local loopback address in html
Classification	Unknown Traffic
Source	88.86.118.82:80 (External Net)
Dest	192.168.1.96:49422 (Home Net)
Reference	http://tools.ietf.org/html/rfc990
Name	(smtp) Attempted command buffer overflow: more than 512 chars
Classification	Attempted Administrator Privilege Gain
Source	192.168.1.96:49299 (Home Net)
Dest	50.28.8.201:25 (External Net)
Reference	http://www.microsoft.com/technet/security/bulletin/ms05-021.mspx http://cve.mitre.org/cgi-bin/cvename.cgi?name=2005-0560 http://cve.mitre.org/cgi-bin/cvename.cgi?name=2001-0260
Name	(http_inspect) UNESCAPED SPACE IN HTTP URI
Classification	Unknown Traffic
Source	192.168.1.96:49932 (Home Net)
Dest	208.83.223.34:80 (External Net)
Reference	
Name	SENSITIVE-DATA Email Addresses
Classification	Senstive Data
Source	208.83.223.34:80 (External Net)
Dest	192.168.1.96:49932 (Home Net)
Reference	

APPENDIX C – RULES FILE

```
#SENSITIVE-DATA Email Addresses
alert tcp $HOME_NET any -> $EXTERNAL_NET [80,20,25,143,110]
(msg:"SENSITIVE-DATA Email Addresses";  sd_pattern:20,email;
classtype:sdf; sid:5; gid:138; rev:1;)


#FILE-EXECUTABLE Portable Executable binary file magic detected
alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any
(msg:"FILE-EXECUTABLE Portable Executable binary file magic
detected"; flow:to_client,established; file_data; content:"MZ";
byte_jump:4,58,relative,little; content:"PE|00 00|"; within:4;
distance:-64; classtype:policy-violation; sid:15306; rev:22;)


#INDICATOR-COMPROMISE Suspicious .ru dns query
alert udp $HOME_NET any -> $HOME_NET 53 (msg:"INDICATOR-COMPROMISE
Suspicious .ru dns query"; flow:to_server; content:"|01 00 00 01 00
00 00 00 00 00|"; depth:10; offset:2; content:"|02|ru|00|";
distance:0; pcre:"/[\x05-
\x20][bcdfghjklmnpqrstvwxyz]{5,32}[^\x00]*?\x02ru\x00/i";
classtype:trojan-activity; sid:15168; rev:13;)


#POLICY-OTHER Remote non-JavaScript file found in script tag src
attribute
alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any
(msg:"POLICY-OTHER Remote non-JavaScript file found in script tag
src attribute"; flow:to_client,established; file_data;
content:"<script"; content:"src="; within:30;
isdataat:100,relative; content:!"|2E|js"; within:100;
reference:cve,2014-6345; reference:url,technet.microsoft.com/en-
us/security/bulletin/MS14-065; classtype:policy-violation;
sid:32481; rev:2;)

alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any
(msg:"POLICY-OTHER Remote non-JavaScript file found in script tag
src attribute"; flow:to_client,established; file_data;
content:"<script"; content:"src="; within:30; isdataat:50,relative;
isdataat:!100,relative; content:!"|2E|js"; within:50;
reference:cve,2015-1729; reference:url,technet.microsoft.com/en-
us/security/bulletin/MS15-065; classtype:policy-violation;
sid:35180; rev:1;)


#BROWSER-IE Microsoft Internet Explorer 7 emulation via meta tag
alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any
(msg:"BROWSER-IE Microsoft Internet Explorer 7 emulation via meta
tag"; flow:to_client,established; file_data; content:"<meta ";
content:"content=|22|IE=EmulateIE7|22|"; within:200;
classtype:attempted-user; sid:26848; rev:7;)


#FILE-EXECUTABLE download of executable content
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"FILE-
EXECUTABLE download of executable content";
flow:to_client,established; content:"application/octet-stream";
fast_pattern; nocase; http_header; pcre:"/^Content-
Type\x3a[\x20\x09]+application\/octet-stream/smiH"; file_data;
content:"MZ"; within:2;
reference:url,www.microsoft.com/smallbusiness/resources/technology/
security/practice_safe_computing_and_thwart_online_thugs.mspx;
classtype:policy-violation; sid:11192; rev:20;)


#BROWSER-OTHER local loopback address in html
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"BROWSER-
OTHER local loopback address in html"; flow:to_client,established;
file_data; content:"http|3A 2F 2F|127."; fast_pattern:only;
reference:url,tools.ietf.org/html/rfc990; classtype:unknown;
sid:26879; rev:6;)


#MALWARE-CNC Win.Trojan.Kazy variant outbound connection
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"MALWARE-
CNC Win.Trojan.Kazy variant outbound connection";
flow:to_server,established; content:".exe HTTP/1.1|0D 0A|User-
Agent: Mozilla/"; fast_pattern:only; content:"|3B| MSIE ";
http_header; content:!"Accept"; http_header; content:"|29 0D
0A|Host: "; distance:0; http_header; pcre:"/^GET\x20\x2f[a-
z]{1,12}\.exe\x20HTTP\x2f1\.1\r\nUser\x2dAgent\x3a\x20Mozilla\x2f[\
x20-\x7e]{10,100}\)\r\nHost\x3a\x20[a-z0-
9\x2e\x2d]{6,32}\r\nConnection\x3a\x20Keep\x2dAlive\r\n\r\n$/";
reference:url,www.virustotal.com/en/file/a064a1d3d8b9d8ab649686b7fb
01e0631e569412388084f5c391722c98660763/analysis/; classtype:trojan-
activity; sid:28406; rev:1;)


#MALWARE-CNC Win.Trojan.Pushdo variant outbound connection
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"MALWARE-
CNC Win.Trojan.Pushdo variant outbound connection";
flow:to_server,established; content:"POST"; http_method;
content:!"Referer|3A 20|"; http_header; content:"Accept|3A| */*|0D
0A|Accept-Language|3A| en-us|0D 0A|Content-Type|3A|
application/octet-stream|0D 0A|Content-Length|3A| "; depth:93;
http_header; content:"User-Agent|3A| Mozilla/4.0 (compatible|3B|
MSIE 6.0|3B| Windows NT 5.1|3B| SV1)|0D 0A|Host|3A|"; distance:0;
fast_pattern:34,20; http_header; content:"Connection|3A| Keep-
Alive|0D 0A|Cache-Control|3A| no-cache|0D 0A|"; distance:0;
http_header; classtype:trojan-activity; sid:29891; rev:7;)


#INDICATOR-OBFUSCATION non-alphanumeric javascript detected
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any
(msg:"INDICATOR-OBFUSCATION non-alphanumeric javascript detected";
flow:to_client,established; file_data; content:"+!![]";
content:"+!![]"; distance:0; content:"+!![]"; distance:0;
content:"+!![]"; distance:0;
reference:url,patriciopalladino.com/blog/2012/08/09/non-
alphanumeric-javascript.html; classtype:attempted-user; sid:23832;
rev:4;)
```

```
#INDICATOR-OBFUSCATION potential javascript unescape obfuscation
attempt detected
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any
(msg:"INDICATOR-OBFUSCATION obfuscated script encoding detected";
flow:to_client,established; file_data; content:"script"; nocase;
content:"language"; within:50; nocase; content:"JScript.Encode";
within:50; nocase; classtype:misc-activity; sid:28629; rev:6;)

alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any
(msg:"INDICATOR-OBFUSCATION potential javascript unescape
obfuscation attempt detected"; flow:to_client,established;
file_data; content:".write"; content:"unescape"; fast_pattern:only;
pcre:"/var\s+([^\s]+)\s*=\s*unescape\s*\x28.*?\x2ewrite\s*\x28\s*\1
/smi";  sid:19888; rev:8;)

alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any
(msg:"INDICATOR-OBFUSCATION potential javascript unescape
obfuscation attempt detected"; flow:to_client,established;
file_data; content:".write"; content:"unescape";
pcre:"/\x2ewrite\s*\x28\s*unescape\s*\x28/smi";  classtype:policy-
violation; sid:19887; rev:7;)
```

APPENDIX D – ACCURACY METRICS

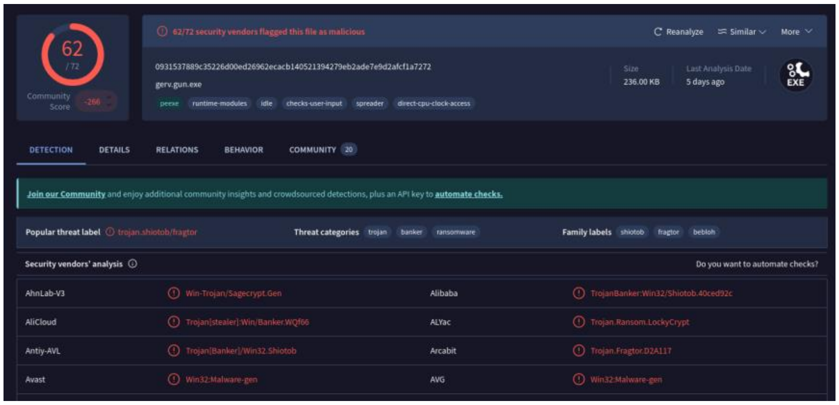
Below is the comparison between the number of alerts in the provided snort file and the alerts in the examiner created snort file.

Alerts	Examiner alerts	Provided Alerts
BROWSER-IE Microsoft Internet Explorer 7 emulation via meta tag	2	2
BROWSER-OTHER local loopback address in html	3	3
Consecutive TCP small segments exceeding threshold	8	3
FILE-EXECUTABLE download of executable content	2	2
FILE-EXECUTABLE Portable Executable binary file magic detected	6	6
(http_inspect) INVALID CONTENT-LENGTH OR CHUNK SIZE	9	9
(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE	15	16
(http_inspect) UNESCAPED SPACE IN HTTP URI	0	1
INDICATOR-COMPROMISE Suspicious .ru dns query	3	3
INDICATOR-OBFUSCATION non-alphanumeric javascript detected	47	47
INDICATOR-OBFUSCATION obfuscated script encoding detected	1	1
INDICATOR-OBFUSCATION potential javascript unescape obfuscation attempt detected	10	10
MALWARE-CNC Win.Trojan.Kazy variant outbound connection	1	1
MALWARE-CNC Win.Trojan.Pushdo variant outbound connection	498	498
POLICY-OTHER Remote non-JavaScript file found in script tag src attribute	18	18
SENSITIVE-DATA Email Addresses	1	1
(smtp) Attempted command buffer overflow: more than 512 chars	41	41
(smtp) Attempted response buffer overflow: 611 chars	1	1
(smtp) Attempted response buffer overflow: 856 chars	1	1
(spp_sdf) SDF Combination Alert	5	9

Total	672	673

When subtracting in excess alerts (such as in the case of “Consecutive TCP small segments exceeding threshold”, wherein all of the provided alerts WERE obtained, but additional alerts were too) This leads to the following comparison: 667 vs 673 alerts,

APPENDIX E – VIRUSTOTAL SCANS



62/72 security vendors flagged this file as malicious

0931537889c35226d00ed26962ecacb140521394279eb2ade7e9d2afcf1a7272

gerv.gun.exe

peexe · runtime-modules · idle · checks-user-input · spreader · direct-cpu-clock-access

Size: 236.00 KB

Last Analysis Date: 5 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.shiotob/fragtor

Threat categories: trojan · banker · ransomware

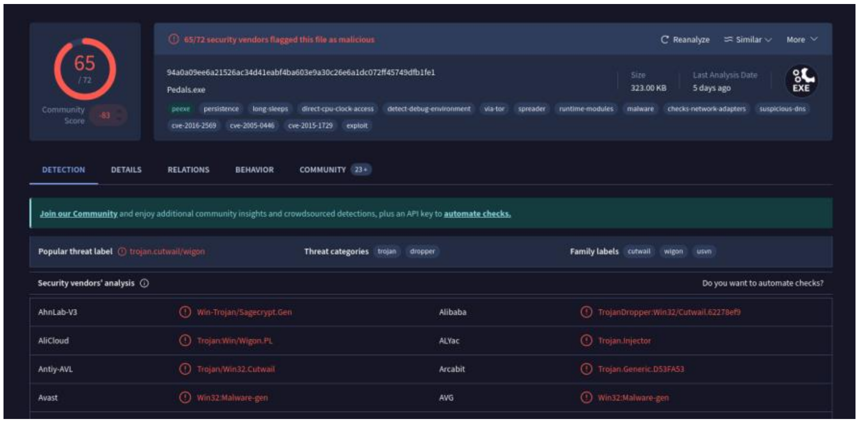
Family labels: shiotob · fragtor · bebloh

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Win-Trojan/Sagecrypt.Gen	Alibaba	TrojanBanker:Win32/Shiotob.40ced92c
AliCloud	Trojan[stealer]:Win/Banker.WQf66	ALYac	Trojan.Ransom.LockyCrypt
Antiy-AVL	Trojan[Banker]/Win32.Shiotob	Arcabit	Trojan.Fragtor.D2A117
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen

gerv.gun.exe



65/72 security vendors flagged this file as malicious

94a0a09ee6a21526ac34d41eabf4ba603e9a30c26e6a1dc072ff45749dfb1fe1

Pedals.exe

peexe · persistence · long-sleeps · direct-cpu-clock-access · detect-debug-environment · via-tor · spreader · runtime-modules · malware · checks-network-adapters · suspicious-dns · cve-2016-2569 · cve-2005-0446 · cve-2015-1729 · exploit

Size: 323.00 KB

Last Analysis Date: 5 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.cutwail/wigon

Threat categories: trojan · dropper

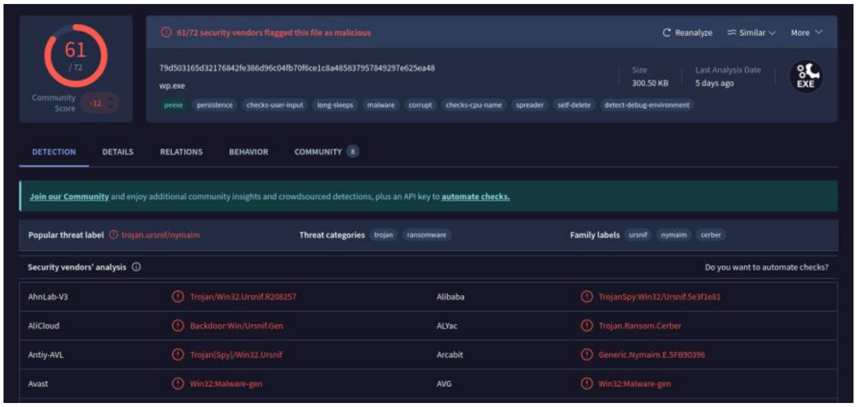
Family labels: cutwail · wigon · usvn

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Win-Trojan/Sagecrypt.Gen	Alibaba	TrojanDropper:Win32/Cutwail.62278ef9
AliCloud	Trojan:Win/Wigon.PL	ALYac	Trojan.Injector
Antiy-AVL	Trojan/Win32.Cutwail	Arcabit	Trojan.Generic.D53FA53
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen

Trow.exe



61 / 72

Community Score -12

61/72 security vendors flagged this file as malicious

79d503165d32176842fe386d96c04fb70f6ce1c8a485837957849297e625ea48

wp.exe

peexe persistence checks-user-input long-sleeps malware corrupt checks-cpu-name spreader self-delete detect-debug-environment

Size 300.50 KB

Last Analysis Date 5 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.ursnif/nymaim

Threat categories trojan ransomware

Family labels ursnif nymaim cerber

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan/Win32.Ursnif.R208257	Alibaba	TrojanSpy:Win32/Ursnif.5e3f1e81
AliCloud	Backdoor:Win/Ursnif.Gen	ALYac	Trojan.Ransom.Cerber
Antiy-AVL	Trojan[Spy]/Win32.Ursnif	Arcabit	Generic.Nymaim.E.5FB90396
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen

Wp.exe