UBNETDEF Network Activity Report

# Executive Summary

UBNetDef investigated network traffic that took place between 13:38:32 UTC and 13:44:42 UTC on June 27, 2017. That traffic showed that at least 3 pieces of malware infected the computer using Windows under the name **FlashGordon-PC** during that time frame. As a result, any credentials for the user for this computer are likely compromised. Along with user credentials for this pc, user’s email credentials and bank credentials are possibly compromised. In addition, it’s possible the malware spread to other computers in the domain, and therefore other computers on the same network are vulnerable. In this incident, the 3 malware executables focus on getting credentials, system and network information and can lead to possible financial loss along with few system’s compromised. In order to fix the problem, the first step is utilizing a good rated security tool to remove these malicious files and then all the computers in the network should perform regular system wide security scans and keep their Windows security updates on and update regularly. Keeping **Windows Defender** **ON** on the victim’s computer could have prevented and mitigated at least 2 out of 3 malicious files. Further mitigation strategies are in the “Recommended Clean Up and Mitigation Strategies” section.

UBNetDef investigated network traffic that took place between 13:38:32 UTC and 13:44:42 UTC on June 27, 2017. That traffic showed that at least 3 pieces of malware-infected the computer using Windows under the name FlashGordon-PC during that time frame. As a result, any credentials for the user for this computer are likely compromised. Along with user credentials for this pc, these can compromise the user’s email credentials and bank credentials. Also, it is possible the malware spread to other computers in the domain, and therefore other computers on the same network are vulnerable. In this incident, the 3 malware executables focus on getting credentials, system, and network information, leading to possible financial loss and a few systems compromised. To fix the problem, the first step is utilizing a well-rated security tool to remove these malicious files, and then all the computers in the network should perform regular system-wide security scans and keep their Windows security updates on and update regularly. Keeping Windows Defender ON on the victim’s computer could have prevented and mitigated at least 2 out of 3 malicious files. Further mitigation strategies are in the “Recommended Clean Up and Mitigation Strategies” section.

Contents

[Executive Summary 1](#_Toc475906041)

[Technical Analysis 3](#_Toc475906042)

[Recommended Clean Up and Mtitigation Strategies 23](#_Toc475906043)

[Contributing Analysts 24](#_Toc475906044)

[Appendix: Analysis Cheat Sheet 25](#_Toc475906045)

# 

# Technical Analysis

**UBNetDef** started the investigation of pcap file containing potential malicious traffic downloaded from https://www[.]malware-traffic-analysis[.]net/2017/06/28/index[.]html . According to basic file properties as shown below, the most recent modification date on the file is June 27, 2017 at 23:59:26 UTC. The file titled “2017-06-28-traffic-analysis-exercise.pcap” has a listed size of 12.4 MB according to file properties.

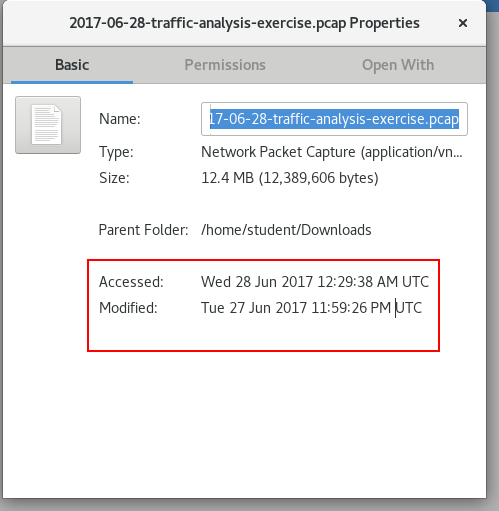


Figure - File Properties

**UBNetDef** started the analysis by first gathering the basic information about the pcap. **UBNetDef** utilized the Wireshark summary option under Statistics > Summary to gather file’s statistic information. The image below shows time of the first and last packet captured and the total duration of the capture. The first packet was captured at 13:38:32 UTC on June 27, 2017 and the last packet was captured on 13:44:42 UTC on the same day and time elapsed between them was 6 minutes and 10 seconds as shown in the image.

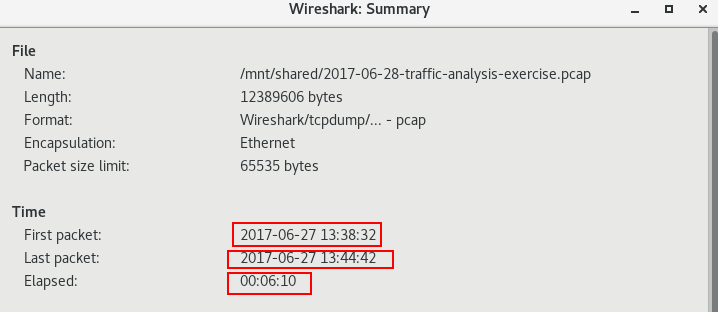


Figure - Wireshark Summary 1

Within the same window, **UBNetDef** also found the bytes of data captured and the number of packets captured. The image below shows these statistics.

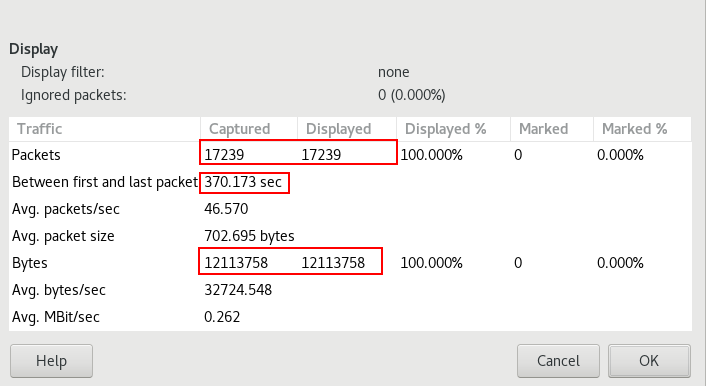


Figure - Wireshark Summary 2

The nest step was to find the ip address of the host computer. Using Wireshark, **UBNetDef** was able to determine the host’s ip as shown in the figure below.

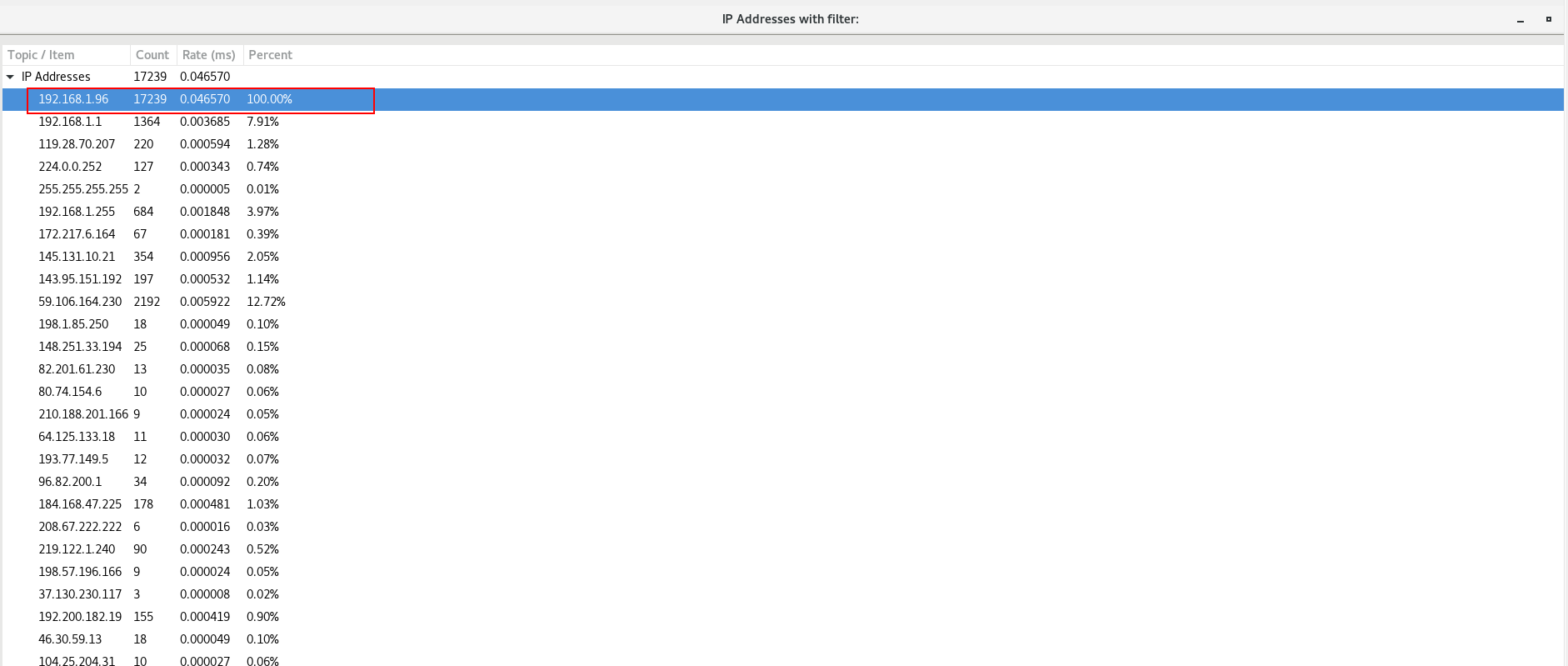


Figure - Wireshark IP List

Furthermore, **UBNetDef** was able to determine the MAC address of the host using packet details of communication by host’s ip as shown in the image.

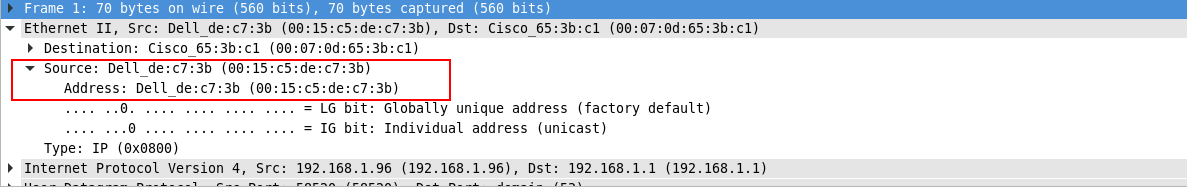


Figure - MAC Address for 192.168.1.96

**UBNetDef** verified this mac address by using zeek logs as shown in the image below.



Figure - MAC Address using Zeek

The Natural next step was to determine the Hostname of the infected Machine. For this purpose, **UBNetDef** utilized the Network Miner tool which analysis the pcap and gives useful inform about the network traffic, similar to Wireshark, but more detailed information. The image below shows the Network Miner screen with the host Ip with it’s hostname highlighted.

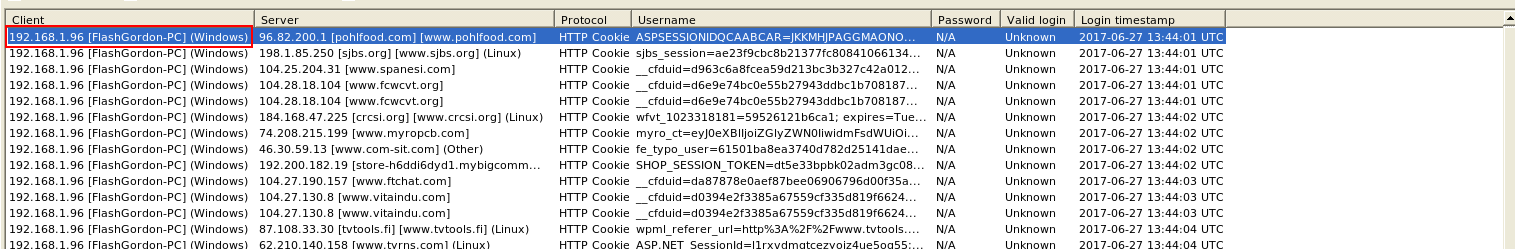


Figure - Hostname (Network Miner)

**UBNetDef** verified this hostname by using zeek logs as shown in the image below.



Figure - Hostname (Zeek)

Next, UBNetDef used Wireshark to export http objects to find any malicious files downloaded during the communication.

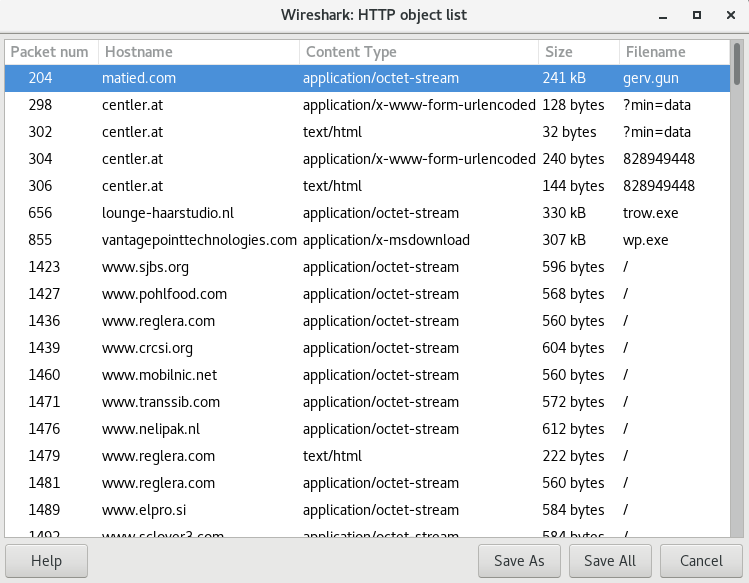


Figure - Exporting HTTP Objects

The next step was to analyze these files captured during http communication, and after analyzing all of these files, **UBNetDef** found 3 malicious executable files which needed further investigation. The following images show the Virustotal scan results for all three malicious files found.

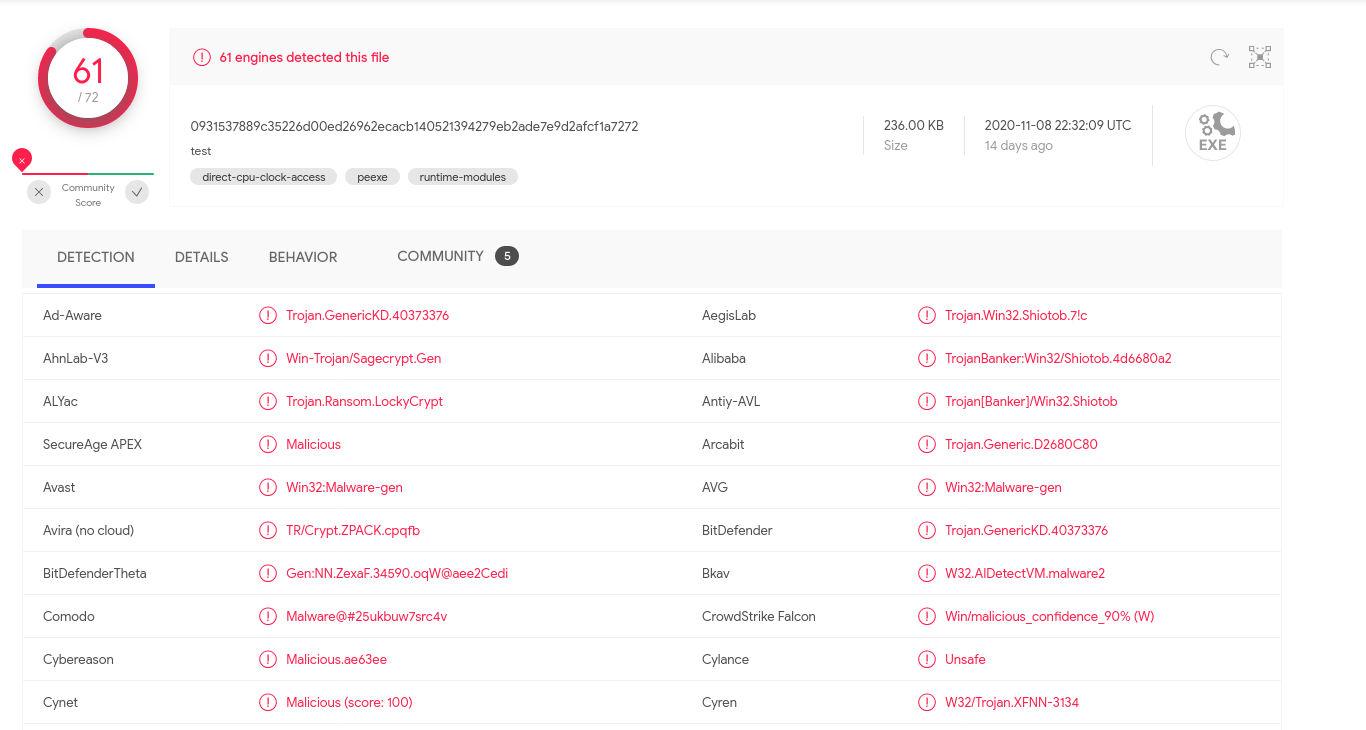


Figure - Virustotal Scan - gerv.gun

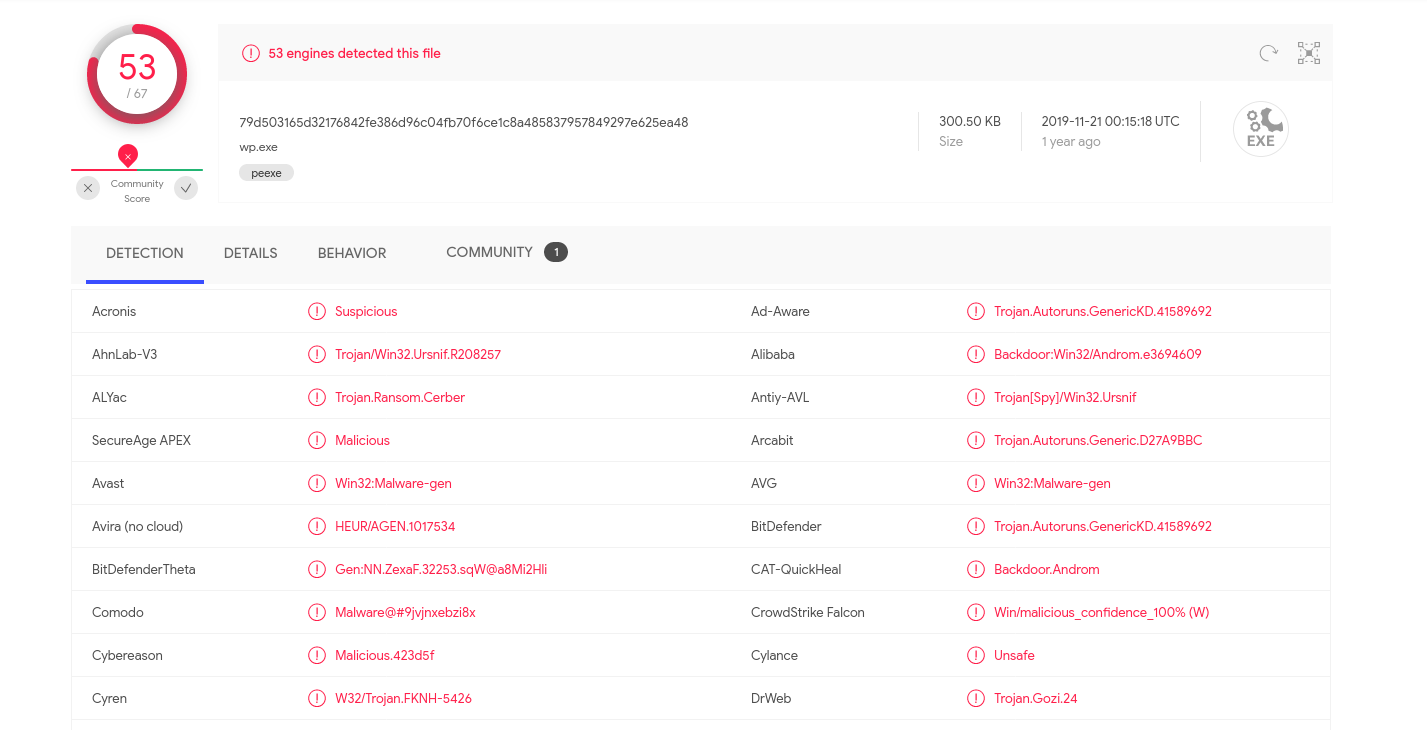


Figure - Virustotal Scan - wp.exe

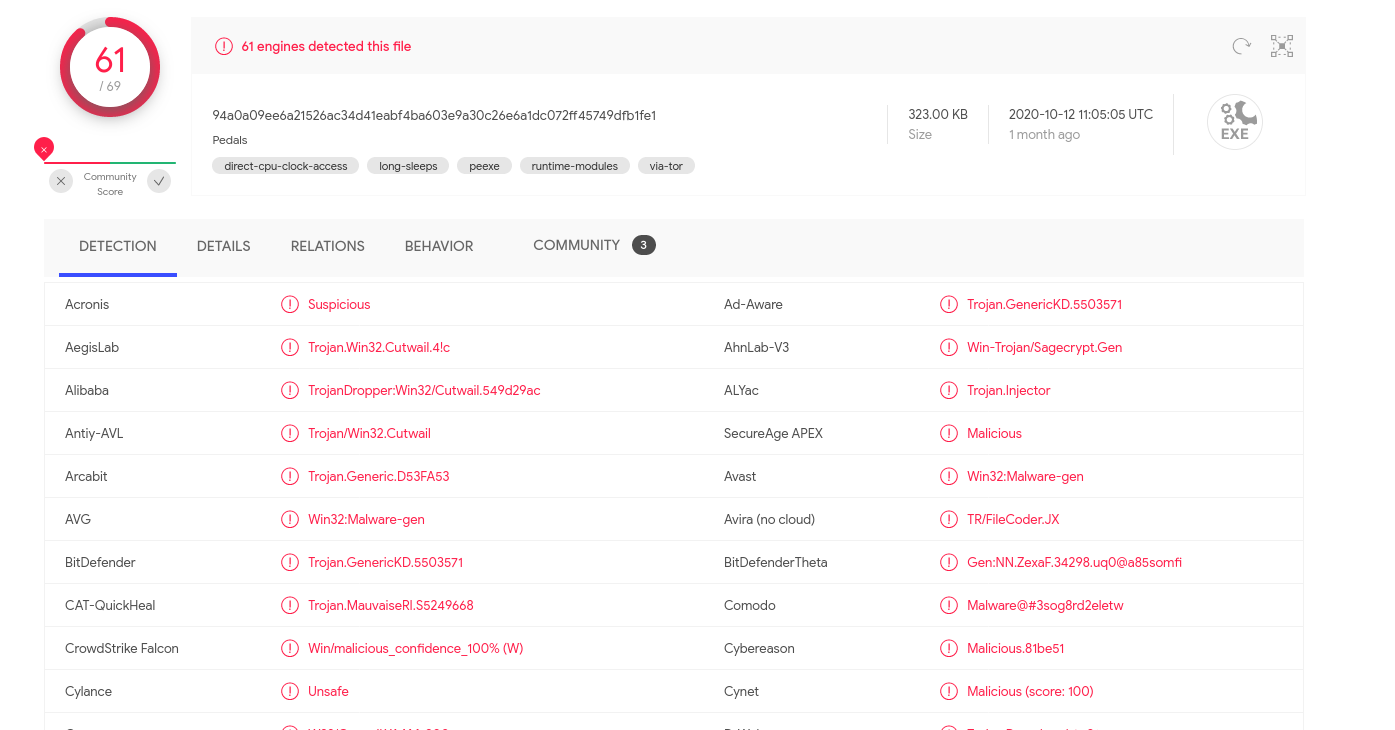


Figure - Virustotal Scan - trow.exe

**UBNetDef** utilized zeek logs to get the ip addresses of the sources of these malicious files.

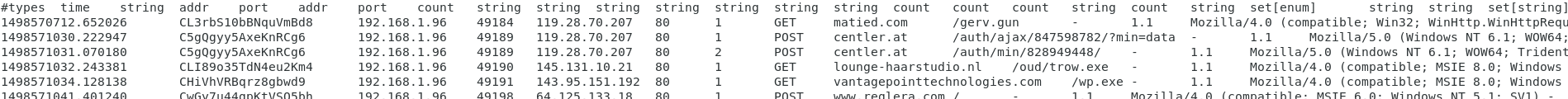


Figure - Source IP's of Malicious Files ( Zeek)

For further detail, **UBNetDef** also used https://ipstack[.]com/ to get location information using the ip addresses of source of these malicious files.

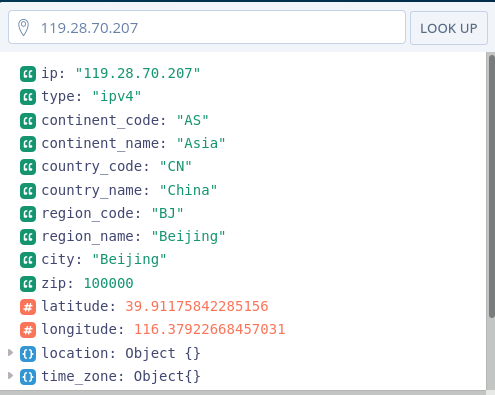


Figure - Source Location - gerv.gun

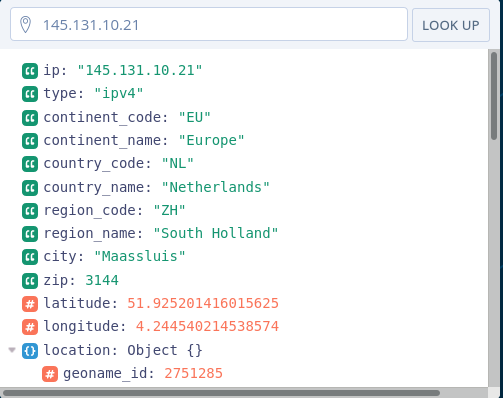


Figure - Source Location - trow.exe

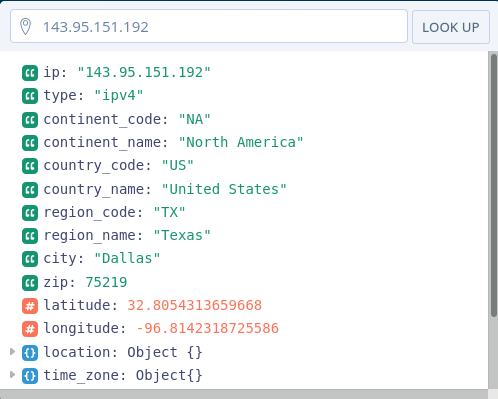


Figure - Source Location - wp.exe

Now, before getting into more depth, **UBNetDef** utilized zeek dns logs and Virustotal to get further information about any other malicious traffic in the pcap.

The following is a refined dns list generated from dns logs of zeek scan of the pcap with all unique dns requests, sorted by their frequency.



Figure - DNS list (Zeek)

On analyzing the most frequent dns requests, we found the following 8 suspicious dns requests, which can lead us to more malicious activity.

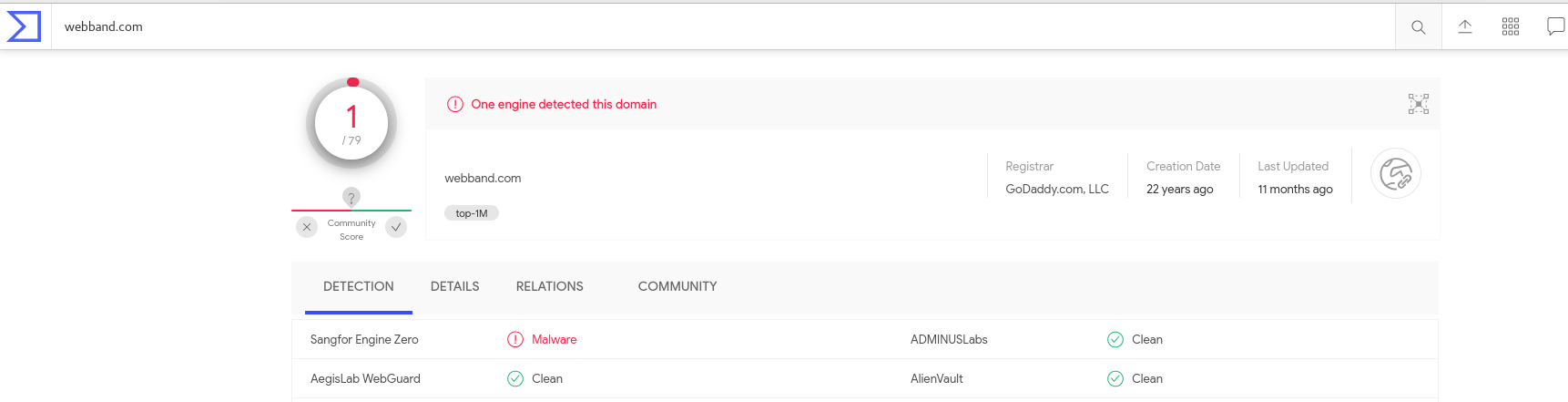


Figure - Malicious DNS Request 1

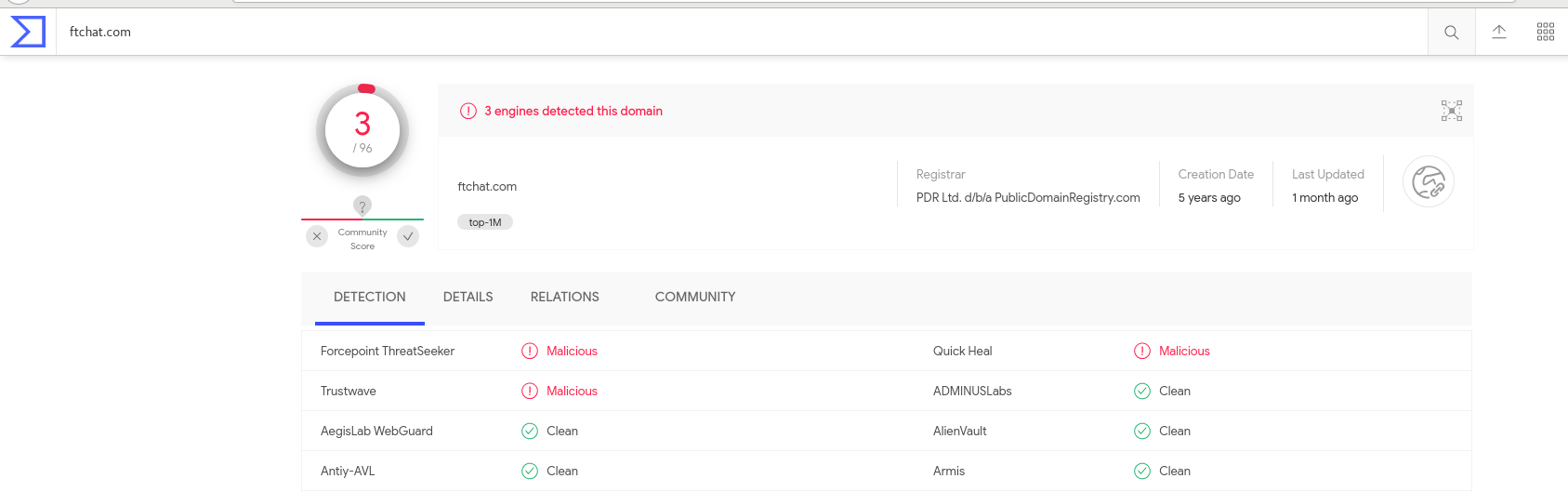


Figure - Malicious DNS Request 2

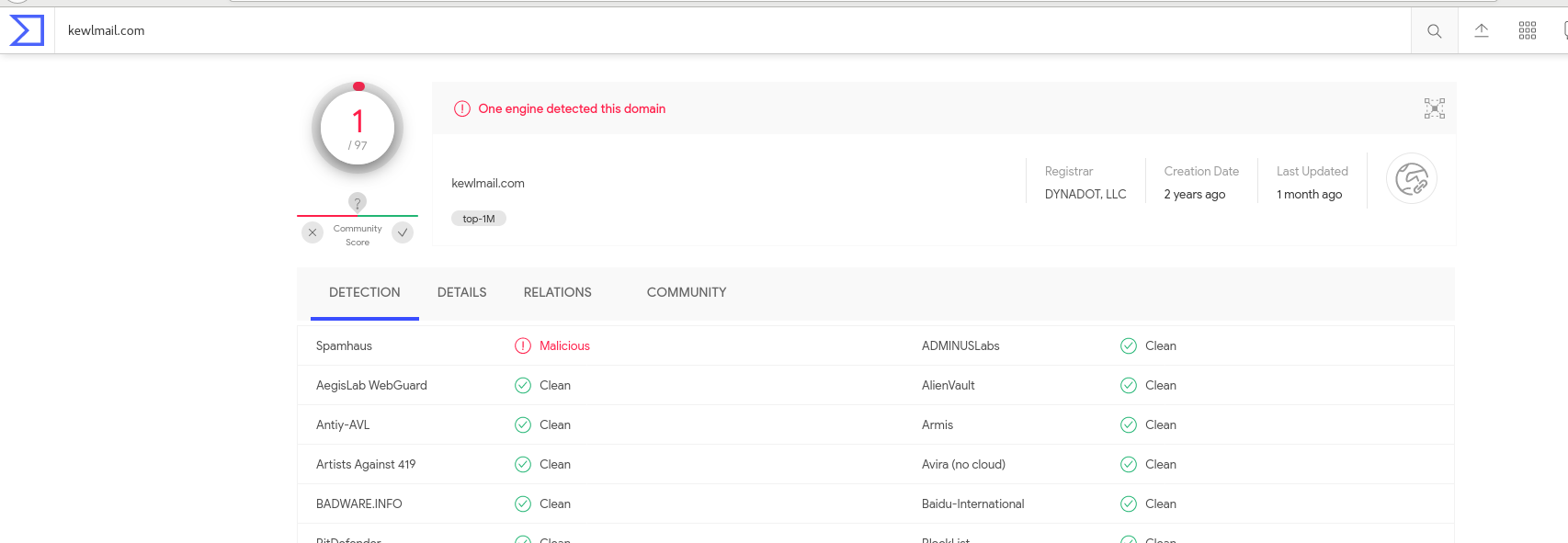


Figure - Malicious DNS Request 3

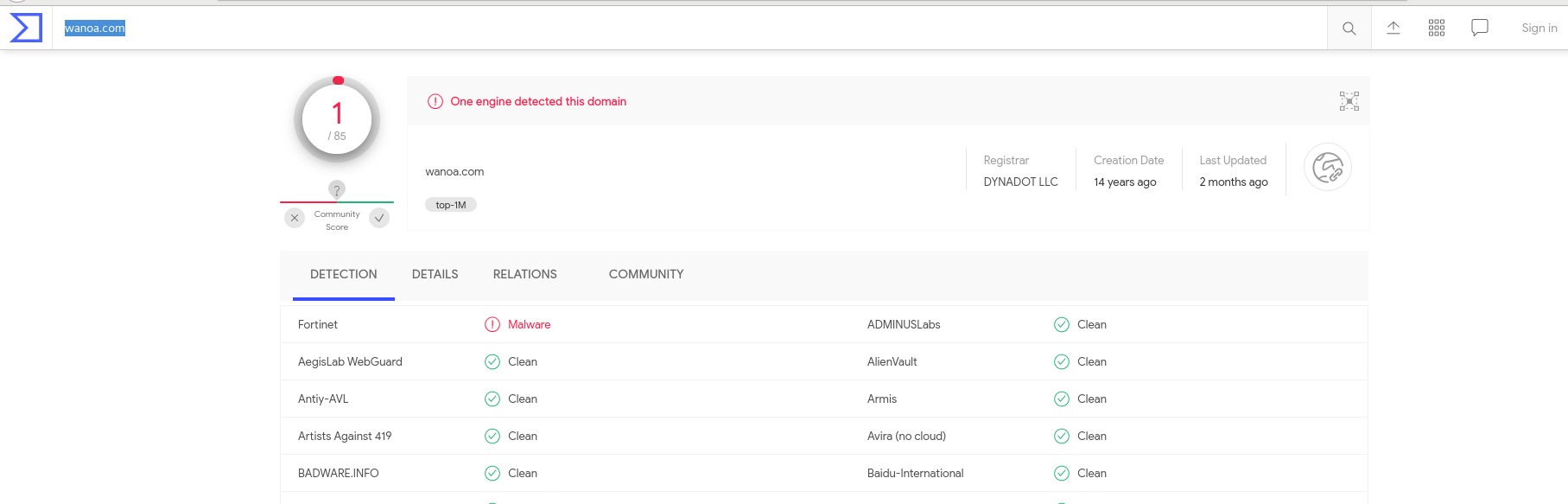


Figure - Malicious DNS Request 4

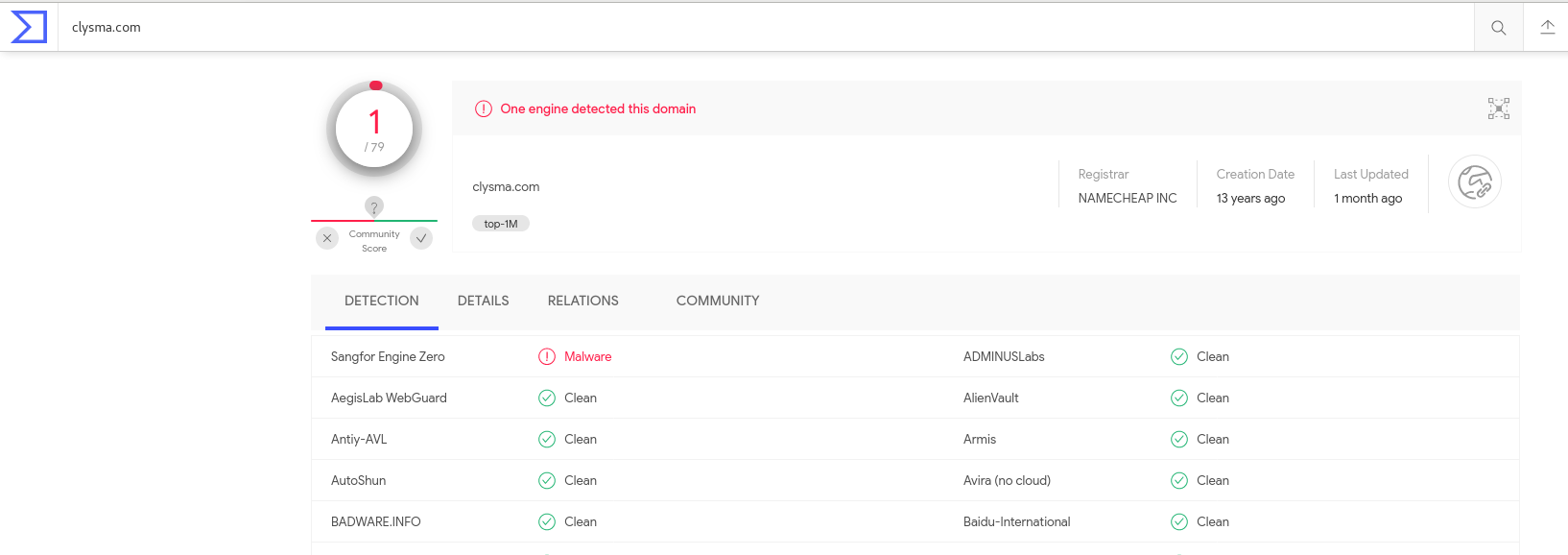


Figure - Malicious DNS Request 5

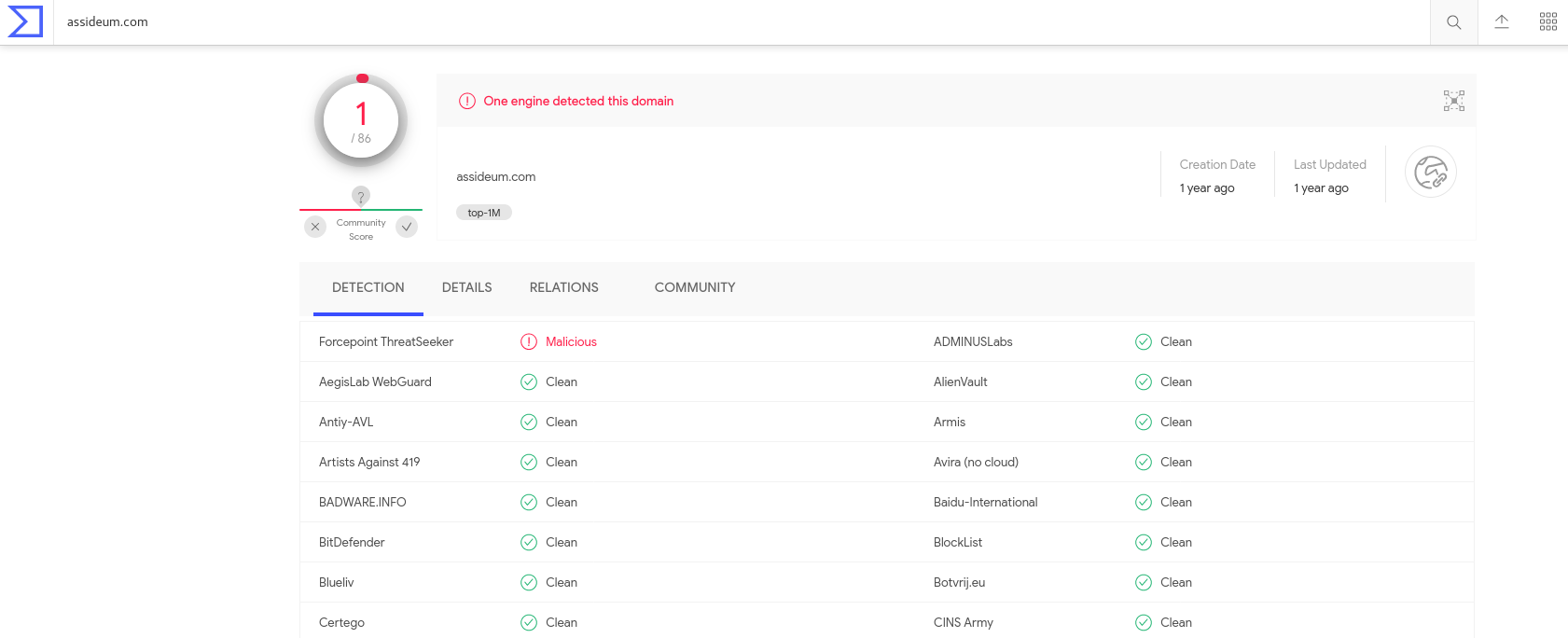


Figure - Malicious DNS Request 6

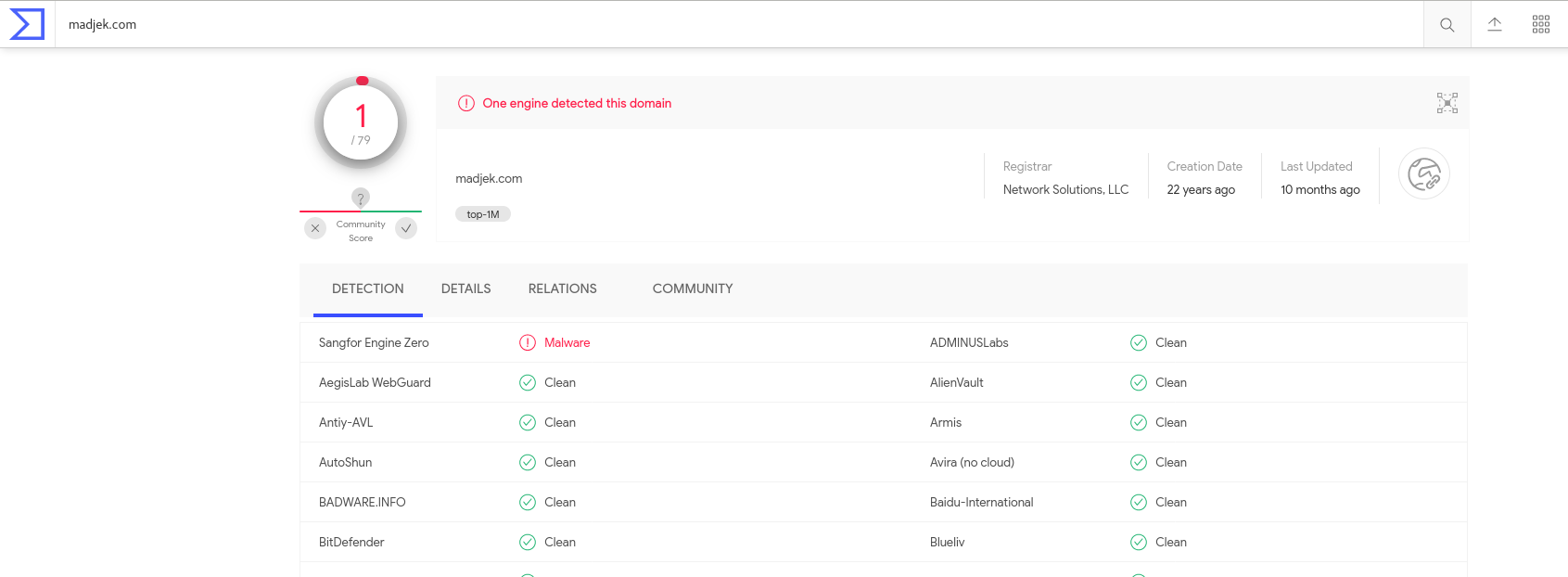


Figure - Malicious DNS Request 7

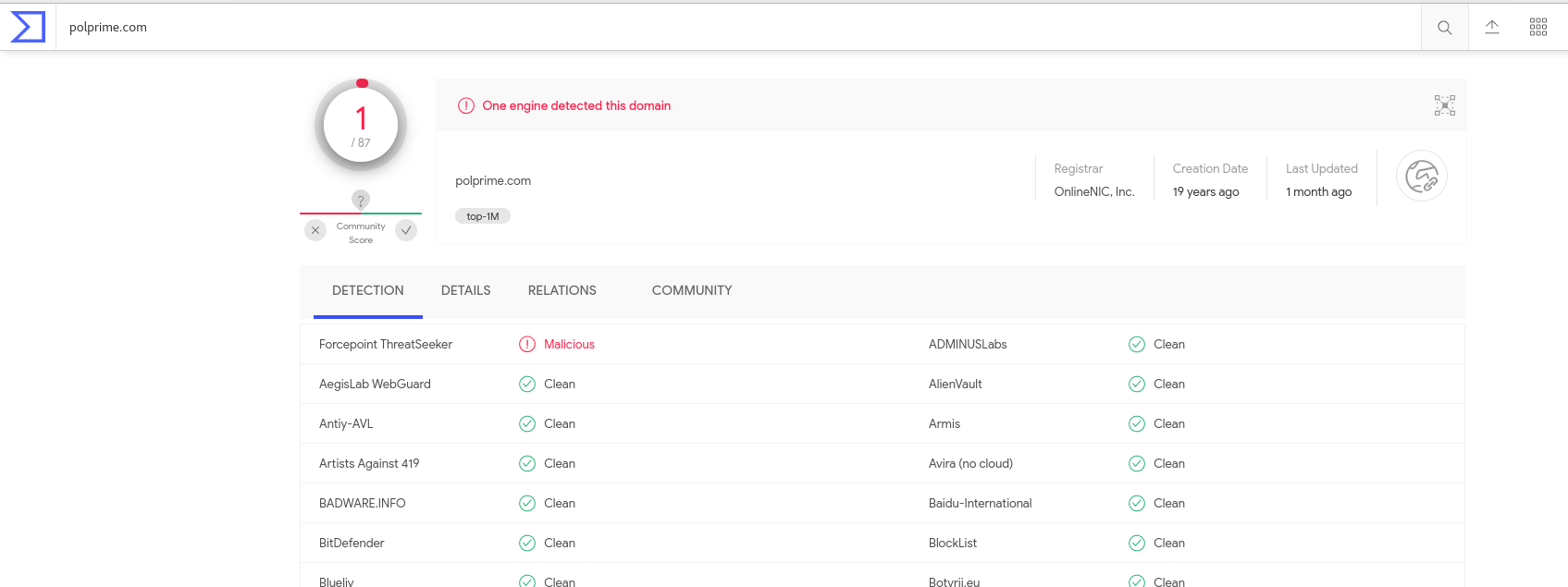


Figure - Malicious DNS Request 8

The Virustotal Scan of the pcap generated several Snort and Suricata alerts indicating that multiple Network Trojan’s might be infecting the host computer. The following images show the Virustotal results.

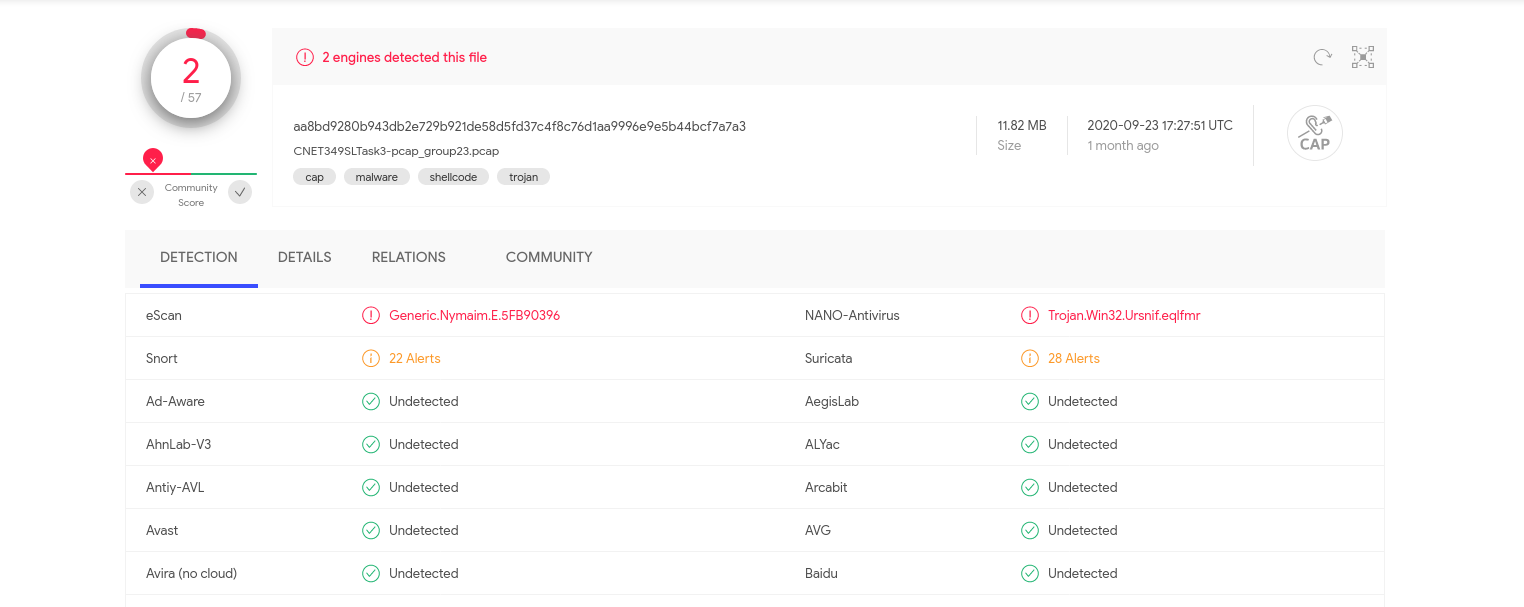


Figure - Virustotal Scan PCAP

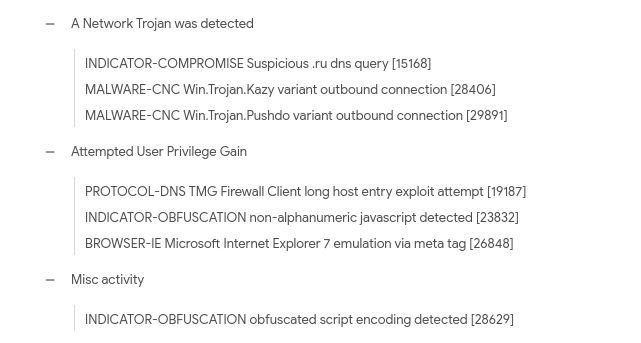


Figure - Virustotal Snort Alerts

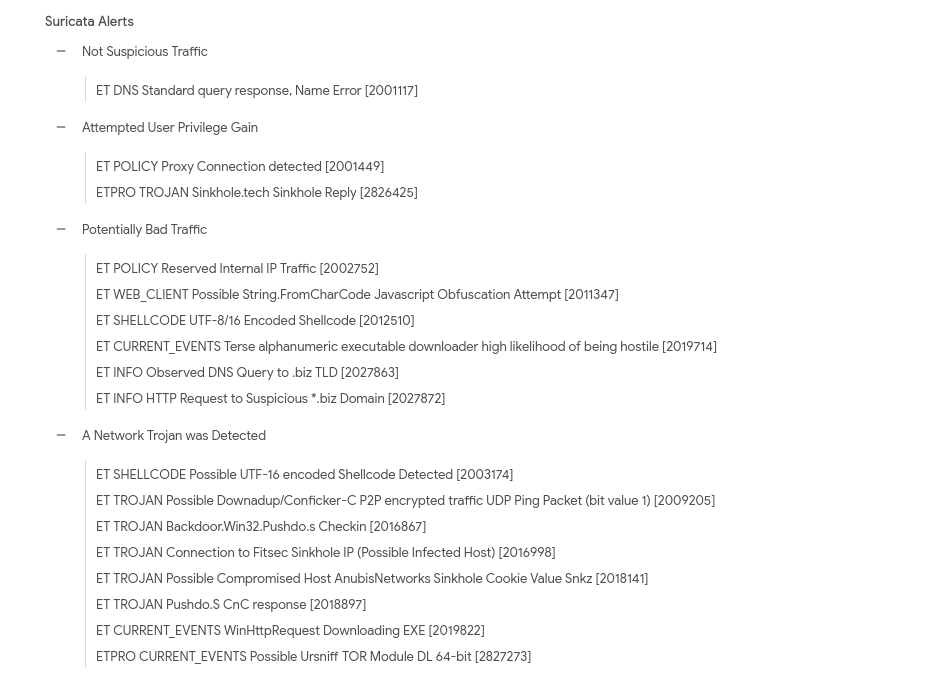


Figure - Virustotal Suricata Alerts

Now, **UBNetDef** proceeded with further investigating the executables found in the http traffic and used Wireshark and Snort to locate and confirm the threats they offer. Further, **UBNetDef** used google search engine to get some useful details regarding the discovered malicious files.

The first packet of the pcap sends a dns request for **matied[.]com**, and as soon as it get’s it’s ip and visits this site by sending an http GET request, it gets it’s first malicious file coupled along the http response packet.



Figure - DNS Query matied[.]com



Figure - Whois Lookup matied[.]com



Figure - HTTP GET request gerv.gun

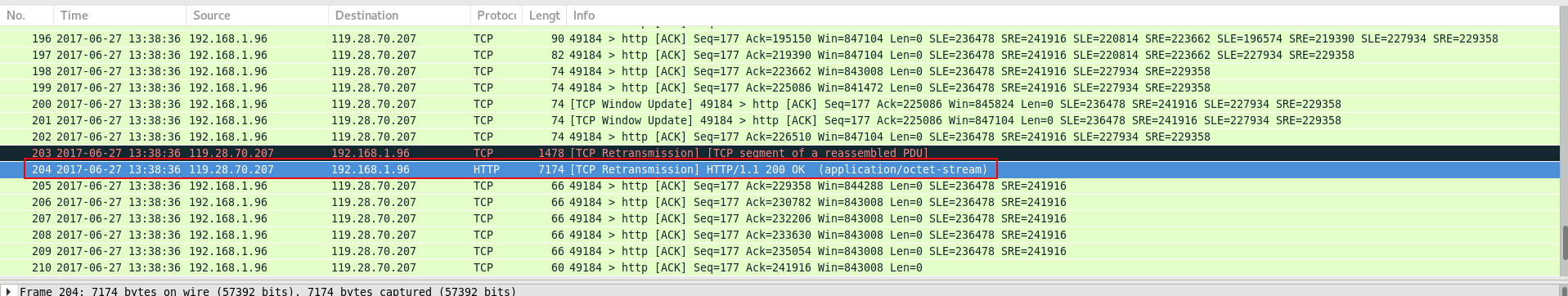


Figure - First Malicious packet - gerv.gun

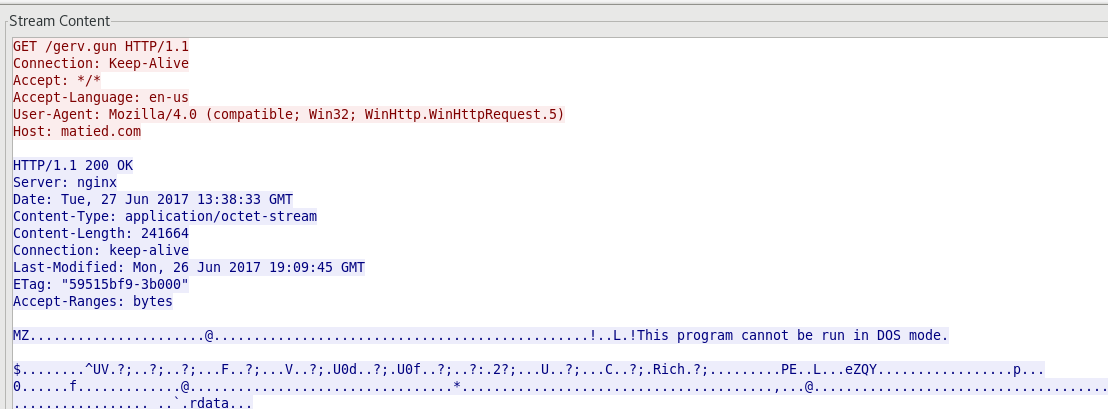


Figure - TCP stream - gerv.gun

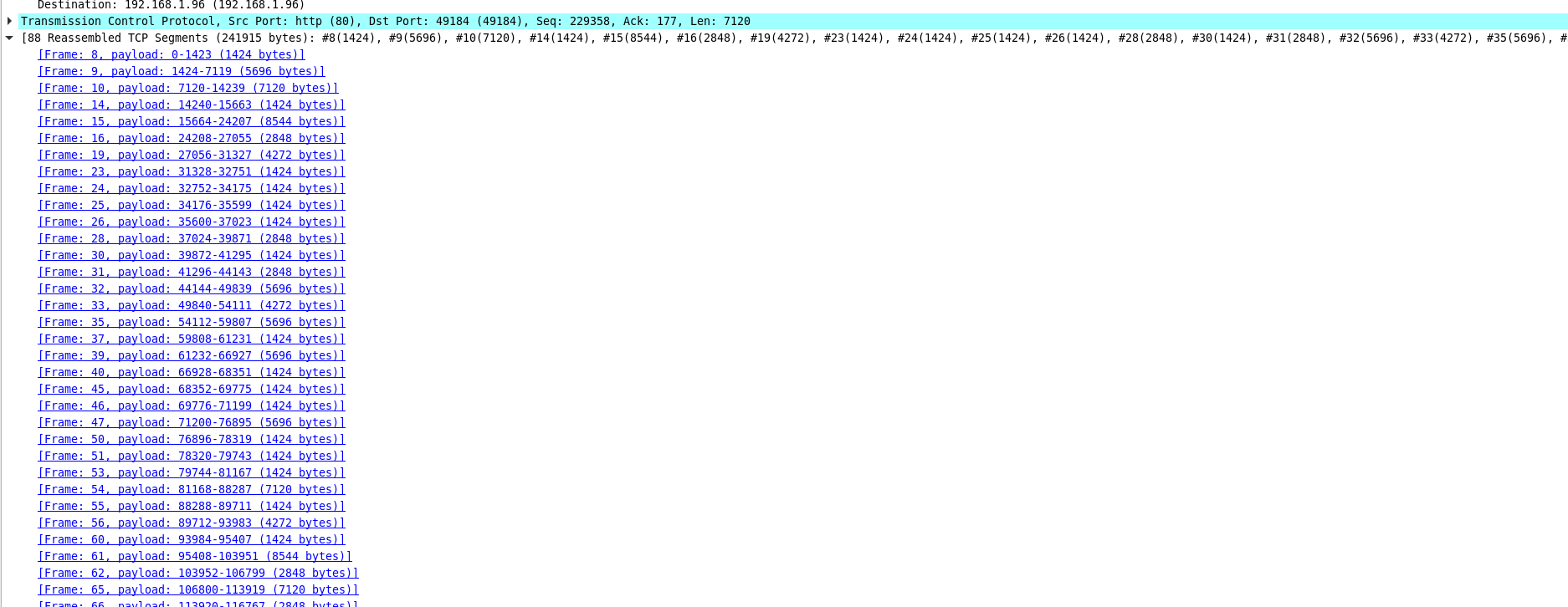


Figure - HTTP response packet containing payload

The snort alerts verify and indicate the malicious activity from 119.28.70.207.

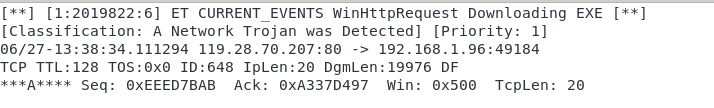


Figure - Snort Alert - gerv.gun

On further investigation of results gathered from Wireshark, snort and Virustotal, **UBNetDef** was able to determine that the Trojan was a Spy banking Trojan **Shiotob.**

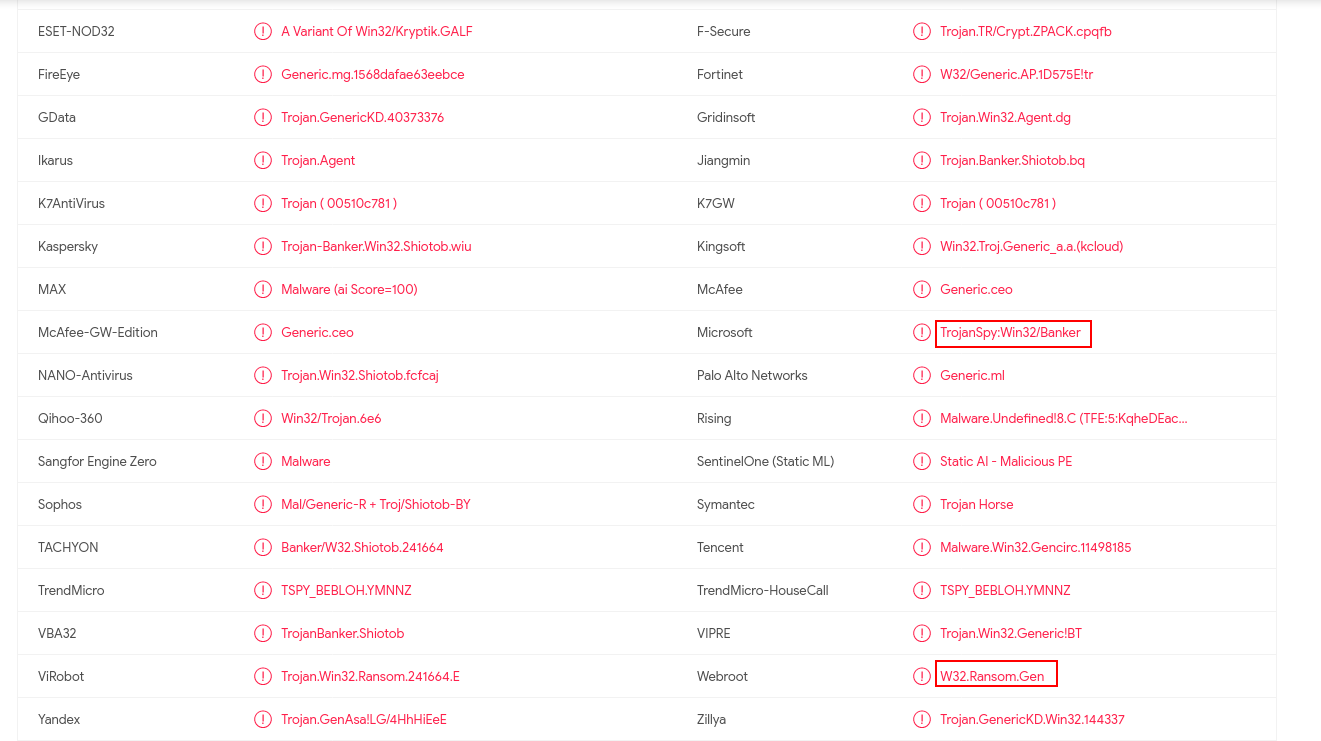
****

Figure - Trojan Shiotob (Virustotal)

With google search it was discovered that this trojan monitors and steals user’s login credentials for online banking. It also forces the use of Internet Explorer if tried to use another browser.

When it’s run, it drops a copy of itself with a random name in the windows system folder and changes the registry so that it’s copy runs every time the Windows system file “userinit.exe’ runs, which happens when Windows starts. To hide itself in the victim’s computer, it runs it’s payload in the context of the system process “csrss.exe”. It disables use of Internet proxy by changing registry data.

It gather’s information like OS version, Network configuration, Windows address book and captured user credentials.

To detect and remove this threat from victim’s pc, run a full system scan with a appropriate, up to date, security solution.

The second executable was detected in HTTP response packet of HTTP get request to **lounge-haarstudio[.]nl** and using Wireshark , UBNetDef was able to determine that the name ip address was used for another malicious http activity later on the victim’s PC.



Figure - HTTP traffic - trow.exe



Figure - Another Malicious packet from same IP

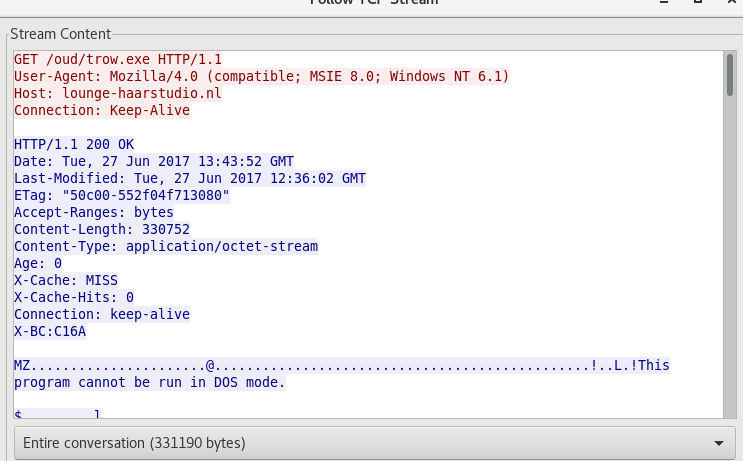


Figure - TCP Stream of the Later Packet

The snort alerts indicate that the traffic from this source is potentially malicious and as we verified earlier, it is indeed a malicious traffic source.

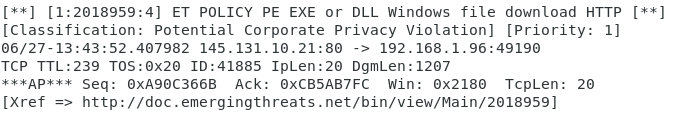


Figure - Snort Alert - trow.exe

On a quick google search along with previous results, **UBNetDef** were able to determine the malware was a Network trojan **Cutwail**.

This threat downloads and runs files on victim’s PC including a trojan that sends spam emails. It can also steal email usernames and passwords as well as FTP credentials. This threat also uses a advanced stealth rootkit and other defensive techniques to avoid detection and removal.

Cutwail tries to overwrite the original device driver on victim’s pc and restore various system hooks to their original unhooked state to circumvent any security application and any other detection.

**Windows Defender** detects and removes this threat.

The third executable was analyzed using similar techniques in Wireshark and snort as follows.



Figure - HTTP request - wp.exe



Figure - HTTP response - wp.exe

The snort alerts show that the traffic violates the corporate privacy policy and is potentially dangerous, but from our earlier analysis we already now that this file is part of malicious activity captured in the pcap.

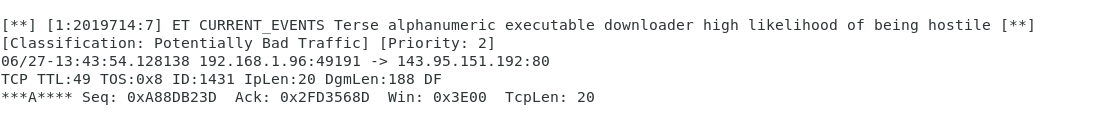


Figure - Snort Alert 1 - wp.exe

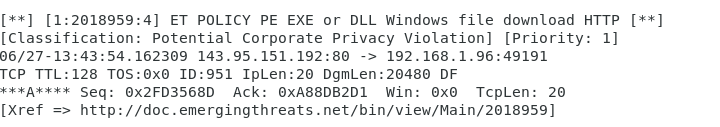


Figure - Snort Alert 2 - wp.exe

With above results and some research on google, **UBNetDef** was able to determine this trojan as **Ursnif** Trojan.

It can steal personal information and information about the victim’s pc to the adversary. It can also run commands from malicious hackers and spread through an infected remote or removable drive.

**Windows defender** detects and removes this threat and family of this threat.

Now apart from the above detections, **UBNetDef** was also able to determine some other malicious activity in the network traffic captured.

One of the snort alerts indicated the presence of a **Backdoor Pushdo** which on some further research found to be related to **Cutwail** Trojan. The following images show the Wireshark and snort results of this analysis.

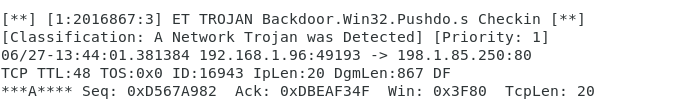


Figure - Snort Alert Backdoor Pushdo.s



Figure - Backdoor packet info

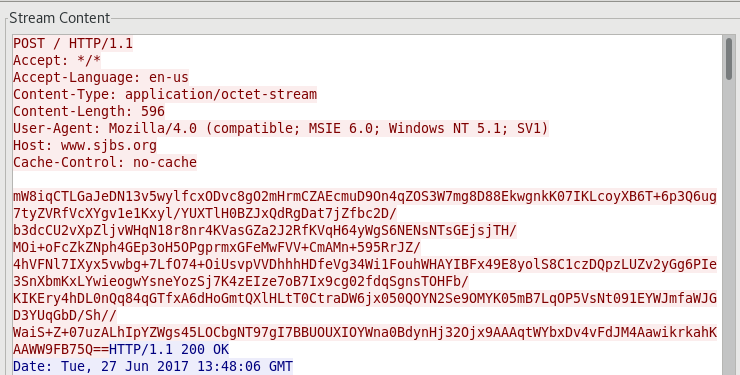


Figure - TCP Stream - Backdoor

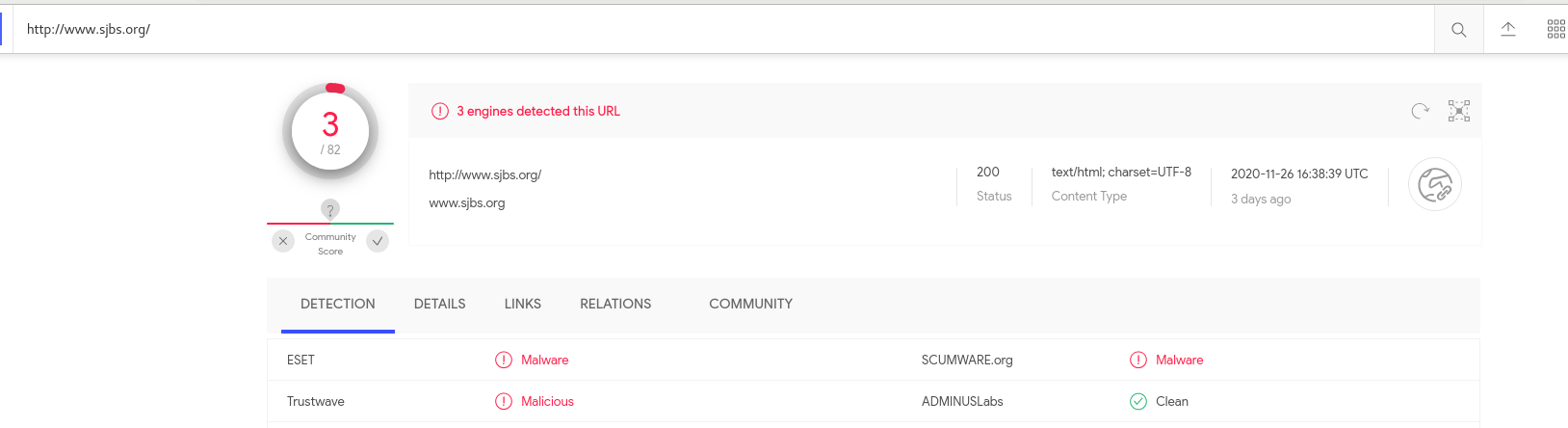


Figure - Virustotal Scan - Backdoor

Another interesting discovery in the snort alerts was a **CnC response** alert as shown below.

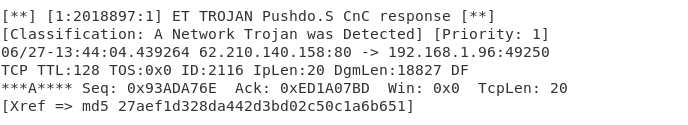


Figure - CnC Snort Alert

Using Wireshark, **UBNetDef** was able to get an indication of a possible Command and Control communication with victim’s machine.



Figure - CnC Trojan packet

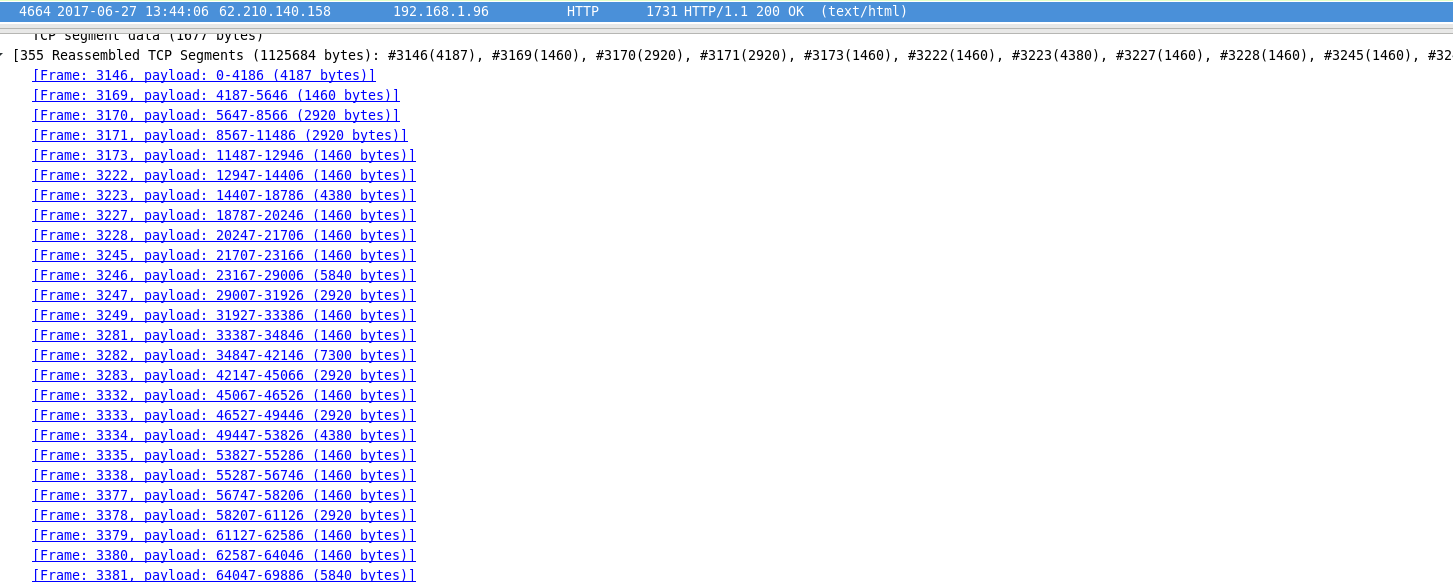


Figure - CnC response packet info

On further investigation, **UBNetDef** found an indicator from a snort alert, which on further investigation verified the idea of command and control communication from victim’s machine to **208.83.223.34** over port **80**. The following screenshots show the investigation results.

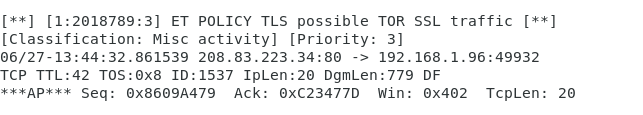


Figure - Snort Alert Indicator

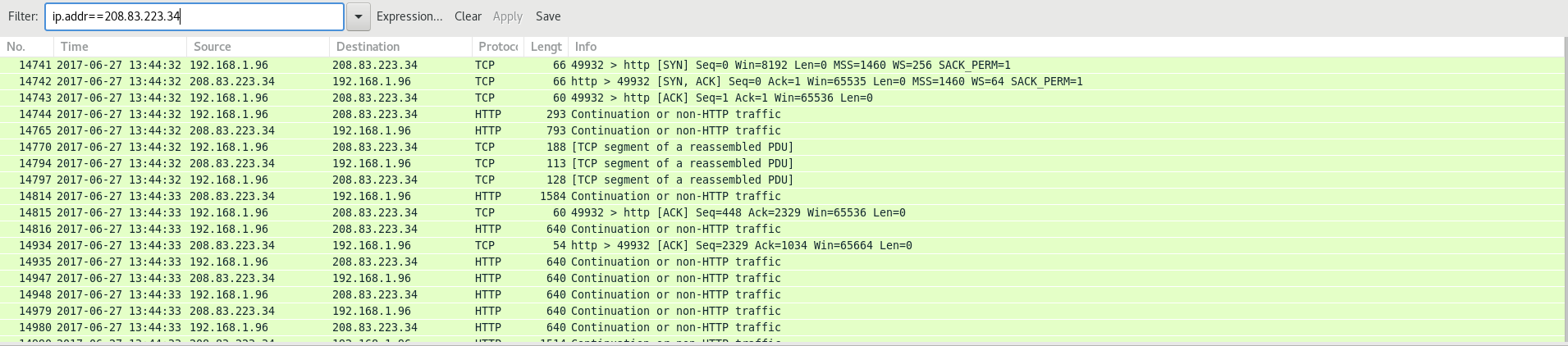


Figure - Maintaining HTTP Connection - Indicator



Figure - Indicator details

In addition to above there were some other malicious activities in the network traffic which can be investigated to get more details or possible links to already available information. The following screenshots show a malicious **URL** and protocols encountered on non-standard ports.

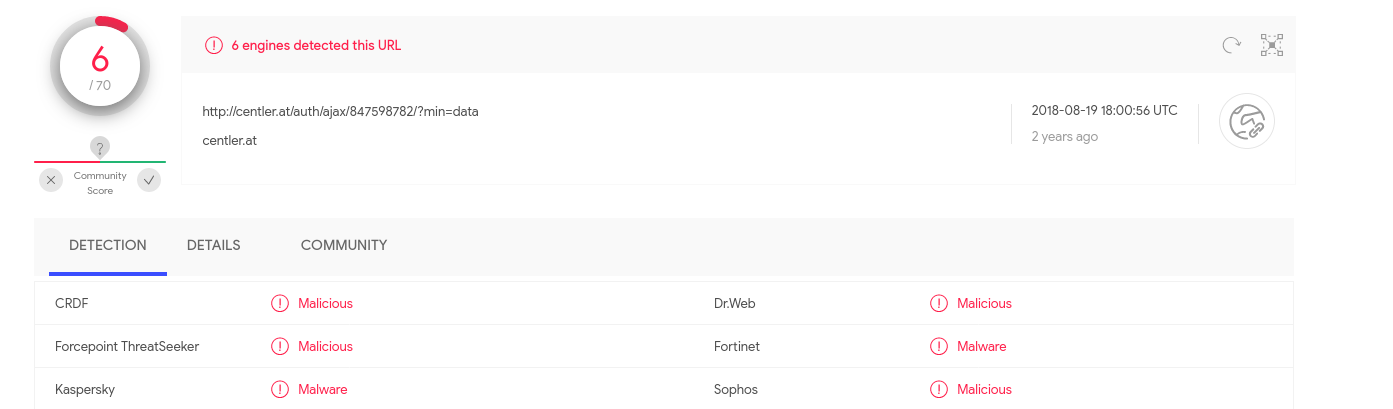


Figure - Malicious URL 1

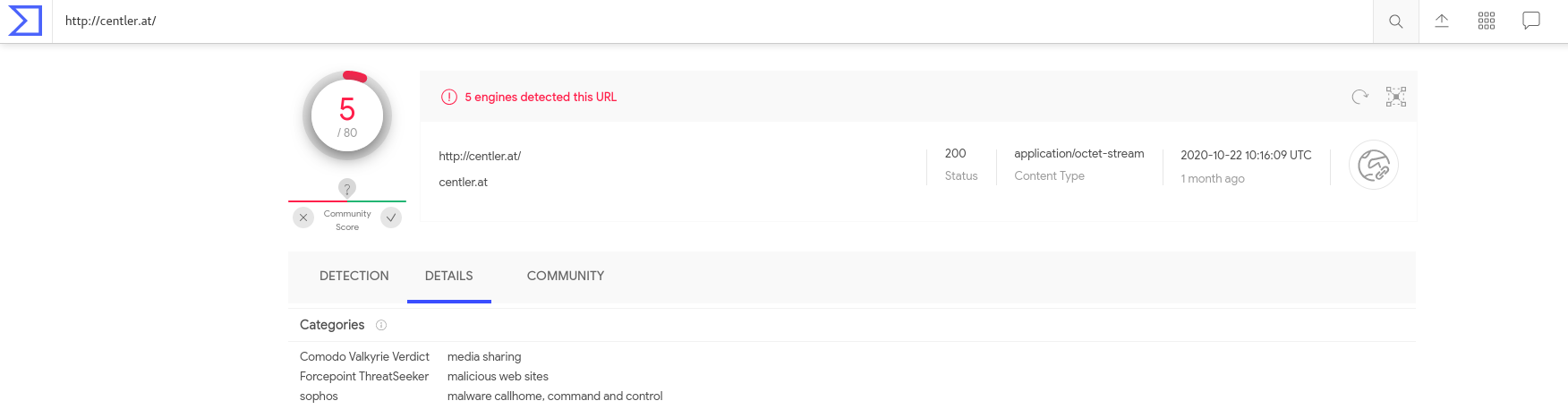


Figure - Malicious URL 2



Figure - Malicious URL TCP Stream

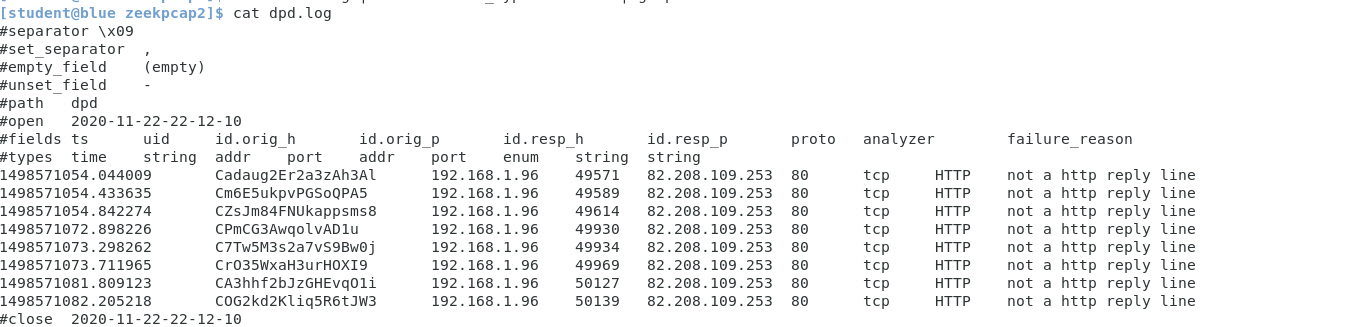


Figure - Protocols encountered on non-standard ports (Zeek)

The following table shows the malicious traffic discovered during our investigation that matches to corresponding phases in **Cyber Kill Chain**.

|  |  |
| --- | --- |
| Phase | Activity |
| Reconnaissance | - |
| Weaponization | Coupling malicious info with a document/webpage |
| Delivery | Sending a spam email with malicious link **matied[.]com**, possibly relevant to victim’s interest, this indicate possible reconnaissance that was not captured. |
| Exploitation | There were 3 executables **gerv.gun** , **trow.exe** and **wp.exe**, which were delivered and contained payloads.  In context of csrss.exe – **gerv.gun** |
| Installation | **Backdoor.Pushdo** was discovered – possible source Cutwail Trojan (trow.exe) |
| Command and Control(C2) | **Pushdo.S CnC** - to **208.83.223.34:80 (using indicator)** |

# Recommended Clean Up and Mtitigation Strategies

For preventing this type of attack in the future, **UBNetDef** recommends the following:

* Turn on Windows Defender on your PC and keep it updated.
* Install a reliable security tools/antivirus with good rating and perform regular system wide security scans.
* Use a firewall to block all incoming connections from the Internet to services that should not be publicly available. By default, you should deny all incoming connections and only allow services you explicitly want to offer to the outside world.
* Enforce a password policy. Complex passwords make it difficult to crack password files on compromised computers. This helps to prevent or limit damage when malware compromises a computer.
* Disable AutoPlay to prevent the automatic launching of executable files on network and removable drives, and disconnect the drives when not required. If there is no need for write access, enable read-only mode if the option is available.
* Do not open emails/click any links from unknown domains.

# Contributing Analysts

Lead Analyst: **Gursimran Singh**

# Appendix: Analysis Cheat Sheet

* zeek -r 2019-12-03-traffic-analysis-exercise.pcap
* less -S dns.log
* cat dns.log | zeek-cut query | sort | uniq -c | sort -rn > dnslist
* sudo snort -c ../../etc/snort.conf -r /home/student/Downloads/2017-06-28-traffic-analysis-exercise.pcap -A full
* sudo cat /var/log/snort/alert | less -S
* cat dhcp.log | bro-cut mac client\_addr
* cat dhcp.log | bro-cut client\_addr host\_name | sort | uniq