UBNETDEF Network Activity Report

Date: 2019-12-03

# Executive Summary

UBNetDef investigated network traffic that took place between 22:44:56

UTC and 23:13:28 UTC on December 03, 2019. That traffic showed that some

pieces of malware infected the computer using Windows under the name

**JUANITA-WORK-PC** during that time frame. As a result, any

credentials for the user for this computer are likely compromised. In addition, it’s

very possible the malware spread to other computers in the domain, and therefore other computers on the same network are

vulnerable. In this incident, the specific piece of malware is responsible for

millions of dollars in damages to victim businesses. In order to fix the problem, IT

staff should use the removal tools provided by Symantec to remove the malware

from the **JUANITA-WORK-PC** computer, and if not successful, will need to reinstall

Windows. All computers on the network will need to install a Microsoft security

update and follow best practices detailed in the “Recommended Clean Up and

Mitigation Strategies” section in order to prevent an attack of this kind from

happening in the future.

Contents

[Executive Summary 1](#_Toc475903980)

[Technical Analysis 2](#_Toc475903981)

[Recommended Clean Up and Mtitigation Strategies 19](#_Toc475903982)

[Contributing Analysts 19](#_Toc475903983)

[Appendix: Analysis Cheat Sheet 20](#_Toc475903984)

# Technical Analysis

UBNetDef investigated a PCAP file containing potentially malicious network traffic,

downloaded from https://www.malware-traffic-analysis.net/2019/12/03/. According to the basic file properties, the most recent modification date on the file is December 03, 2019 at 23:45:51 UTC. The file, titled “ 2019-12-03-traffic-analysis-exercise.pcap” has a listed size of 11.1 MB, according to the file’s basic information.

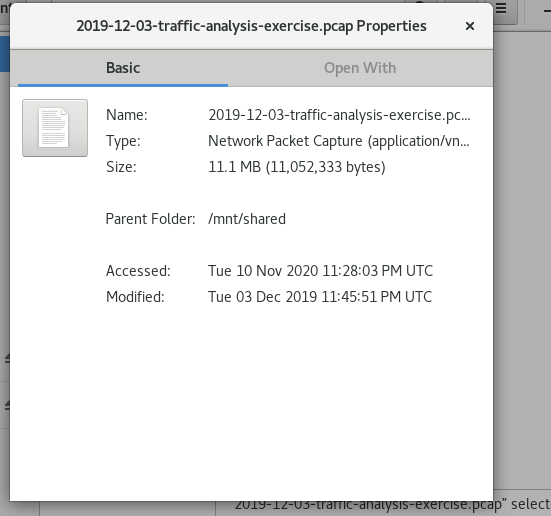


Figure :File Properties

UBNetDef opened “Capture File Properties” within Wireshark to find that the file has a listed capture size of 10.7 MB.

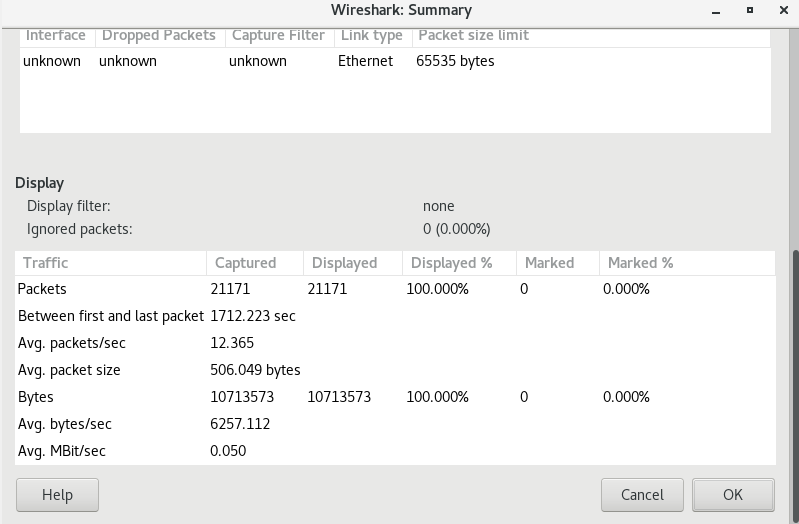


Figure :Capture File Properties - Capture Size

According to Wireshark, all network traffic captured within the file took place between 22:44:56 UTC and 23:13:28 UTC on December 03, 2019. According to the website from which UBNetDef downloaded the file, the LAN segment range is 10.2.23.0/24.

UBNetDef opened the PCAP file in Wireshark on CentOS 7 Linux and found that the first

packet took place 22:44:56 UTC on December 03, 2019, and the last packet took place at

23:13:28 UTC on the same day, making the entire exchange 28 minutes and 32 seconds.

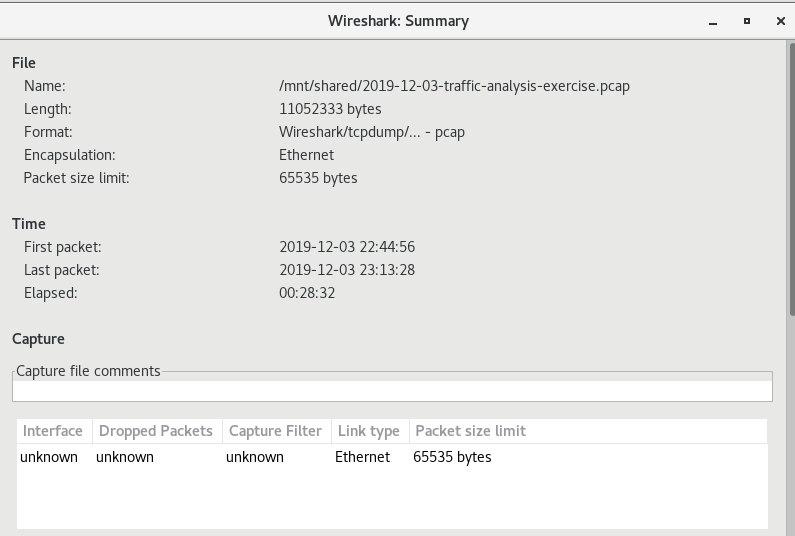


Figure :Capture File Properties - Time Duration

The above information is verified using the “capinfos” command on CentOS machine as shown.

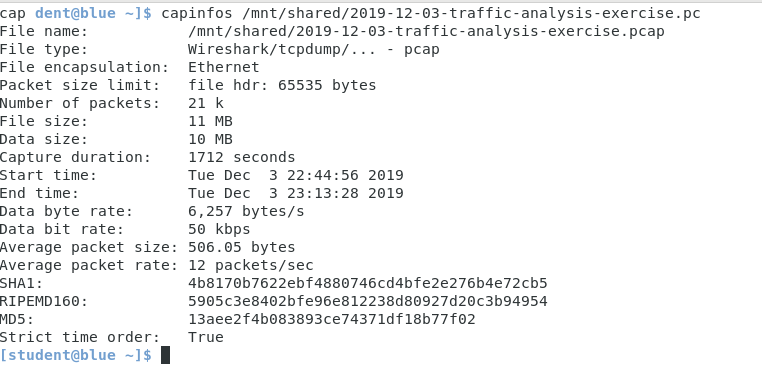


Figure :Capinfos Output

Then UBNetDef used Protocol Hierarchy in Wireshark to determine the most frequently used protocols in the packet capture. The image below shows the same.

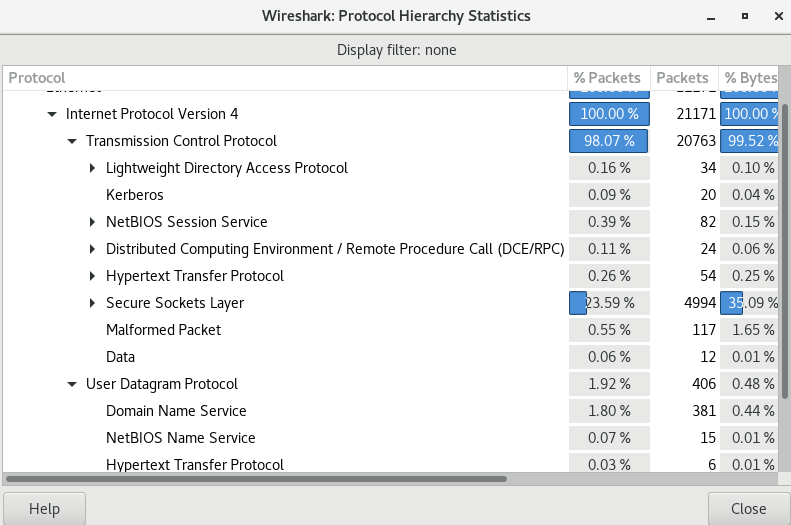


Figure :Protocol Hierarchy

Next, UBNetDef used Wireshark to get the list of IP address used and their frequency, through which the victim’s/host’s IP was identified as shown.

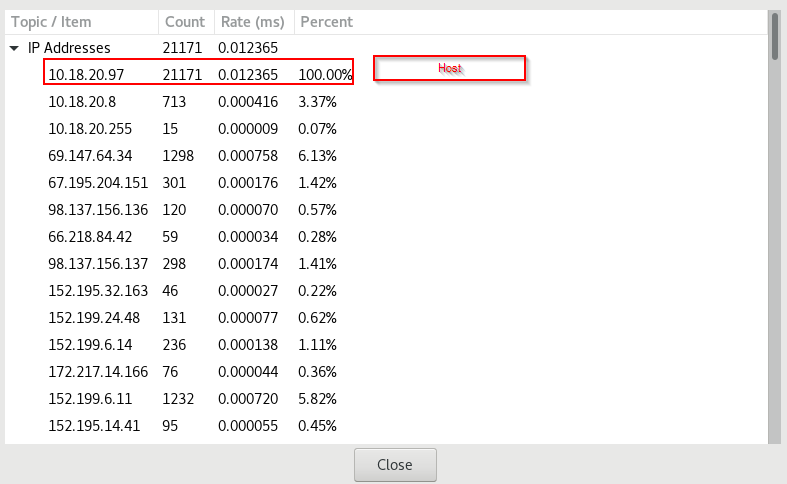


Figure : Host IP Address (IP Address List)

Using the host’s IP, UBNetDef were able to determine the MAC address of the host’s machine as shown using Wireshark.

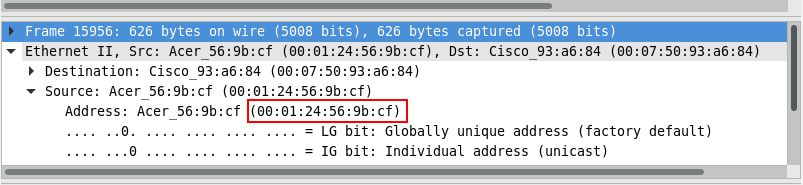


Figure : MAC Address of the Host

Next Using Wireshark, Vulnerable TCP ports such as ldap, Microsoft-ds, etc and UDP ports such as netbios-ns, ssdp, etc used during the communication were identified. The following Images show the same.

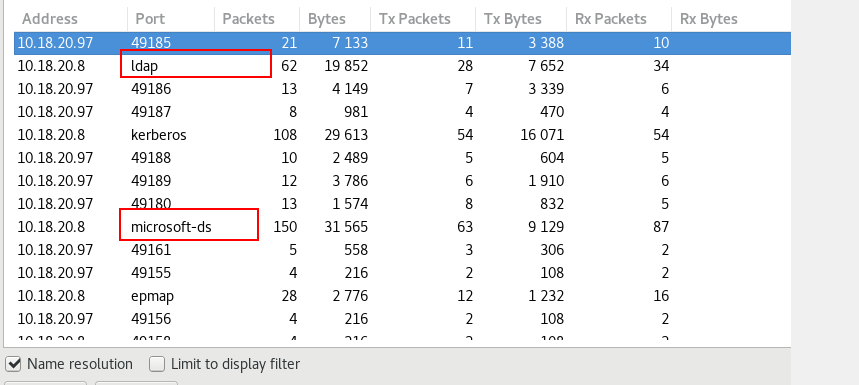


Figure : TCP Vulnerable Open Ports

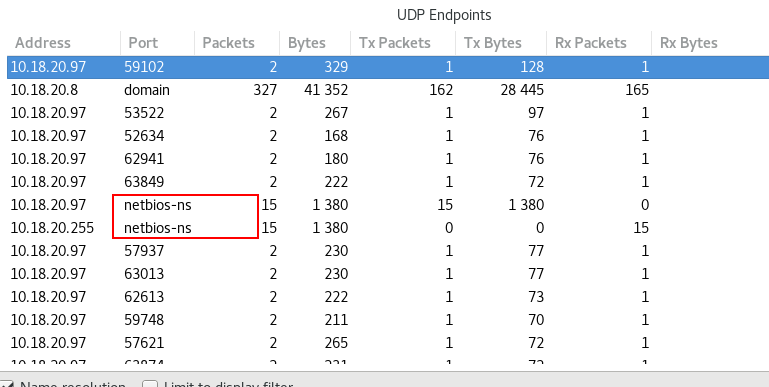


Figure : UDP Vulnerable Open Ports – 1

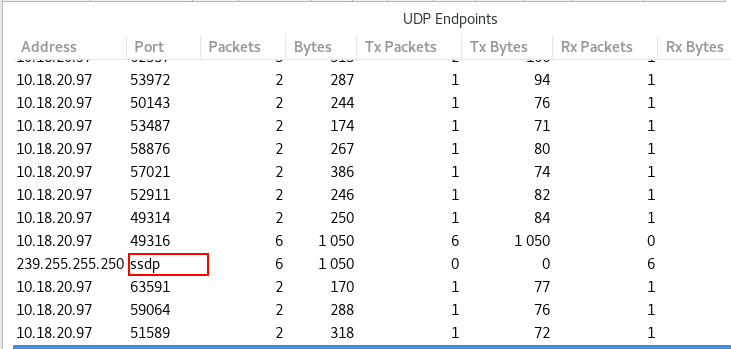


Figure : UDP Vulnerable Open Ports – 2

Then UBNetDef extracted files from HTTP stream using HTTP Objects in Wireshark and scanned each of those files on Virustotal. Although the files seems suspicious, the scan cleared all these files from containing any known malicious information.

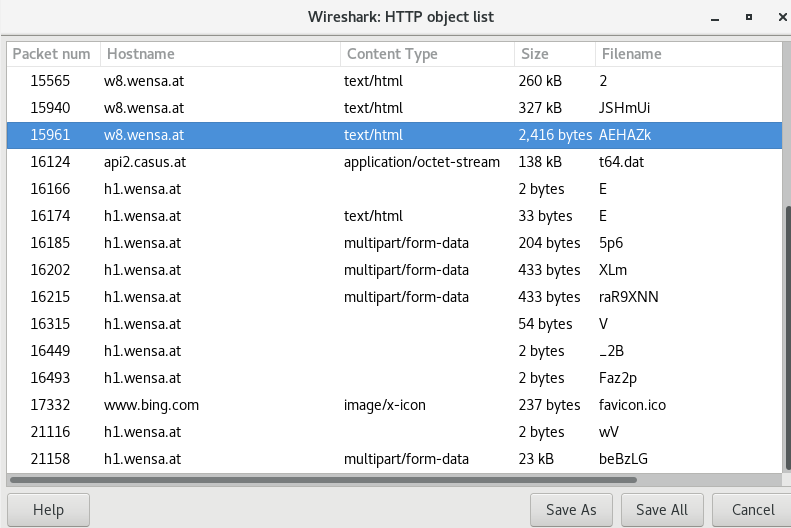


Figure : Extracted HTTP Objects using Wireshark

UBNetDef used the zeek/bro to generate a DNS log, and found the most commonly used domains within the DNS traffic within the PCAP file as shown in Figure 1 below:



Figure : DNS List

Using VirusTotal, UBNetDef scanned the top queried dns servers in the packet capture and found 4 malicious dns servers as follows:

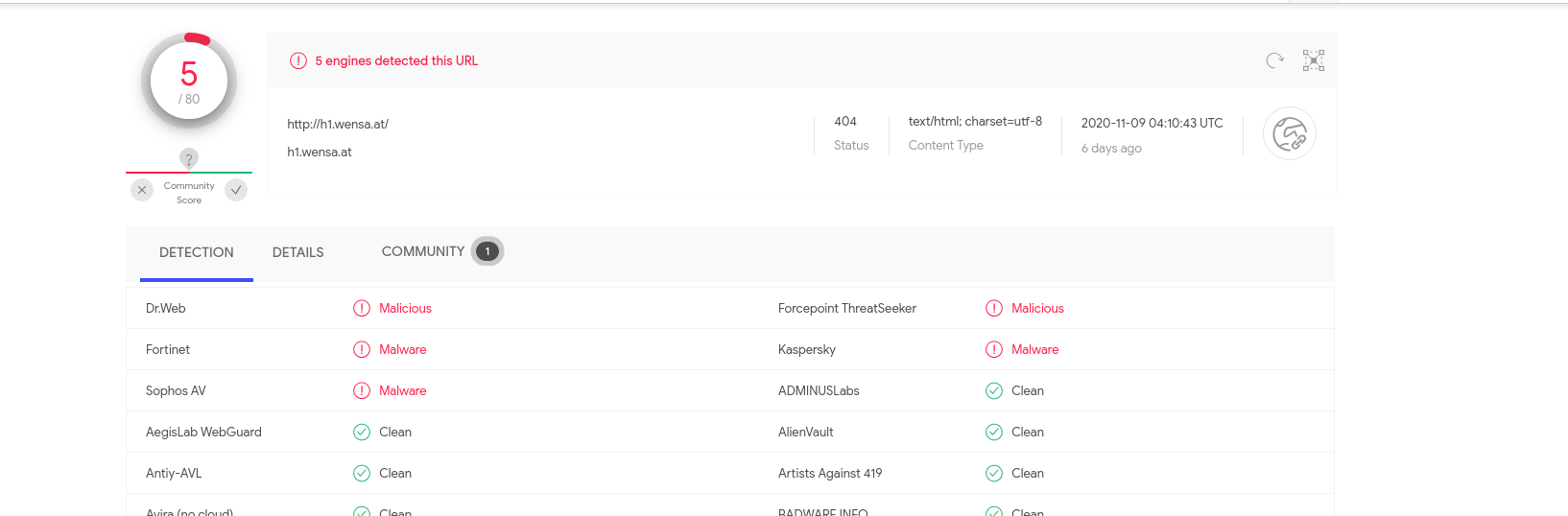


Figure : h1.wensa.at

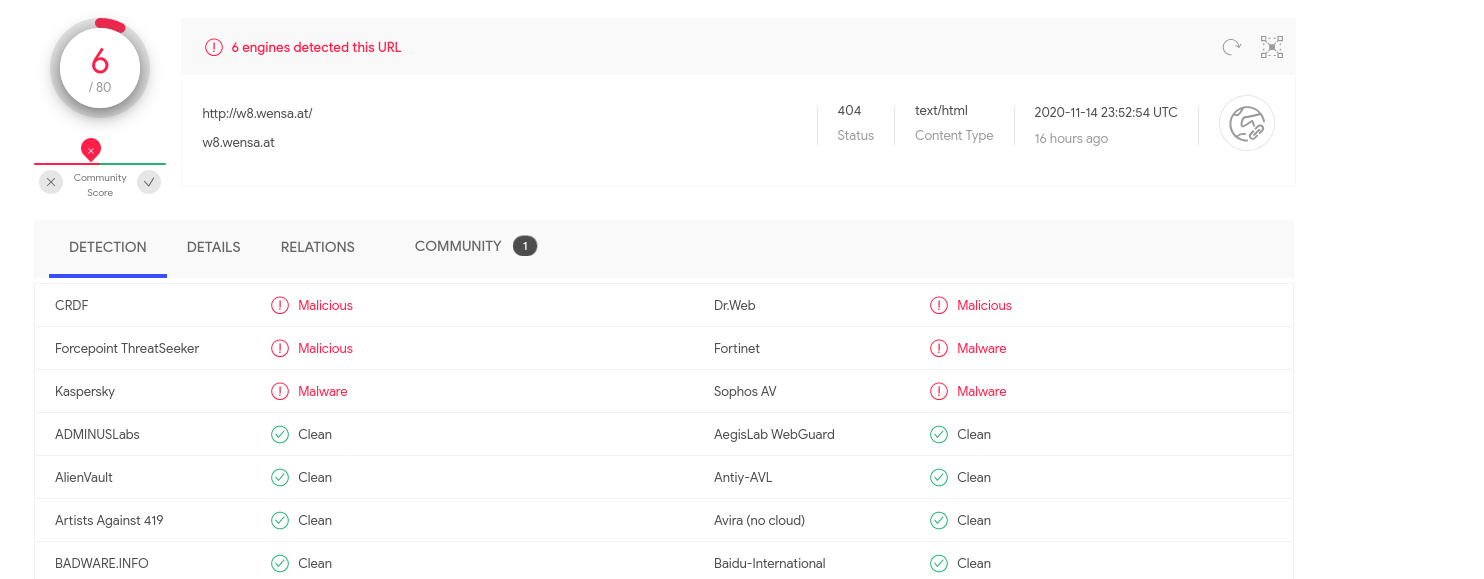


Figure : w8.wensa.at

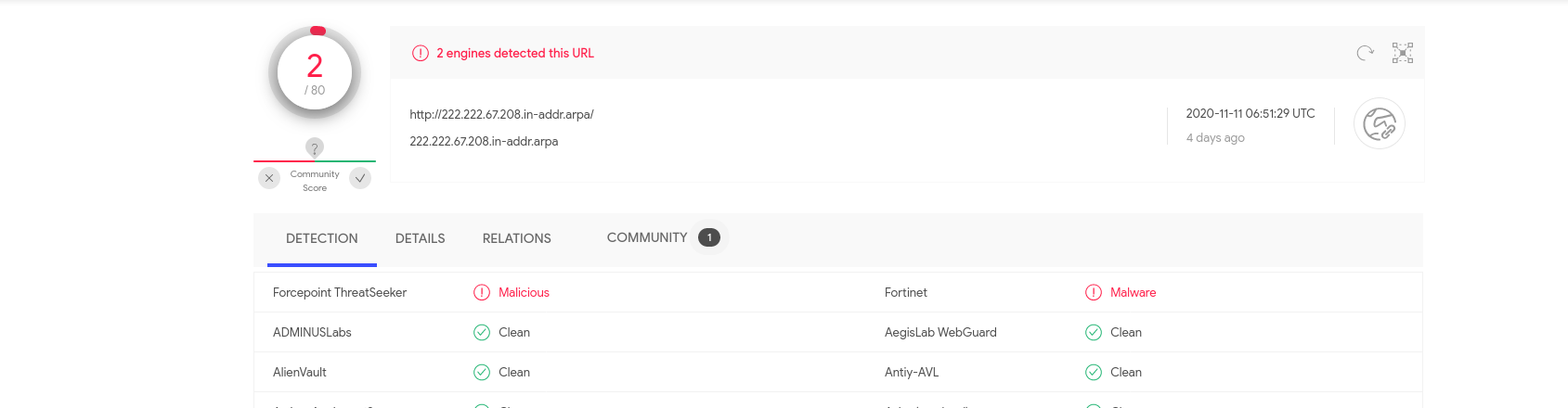


Figure : 222.222.67.208.in-addr.arpa

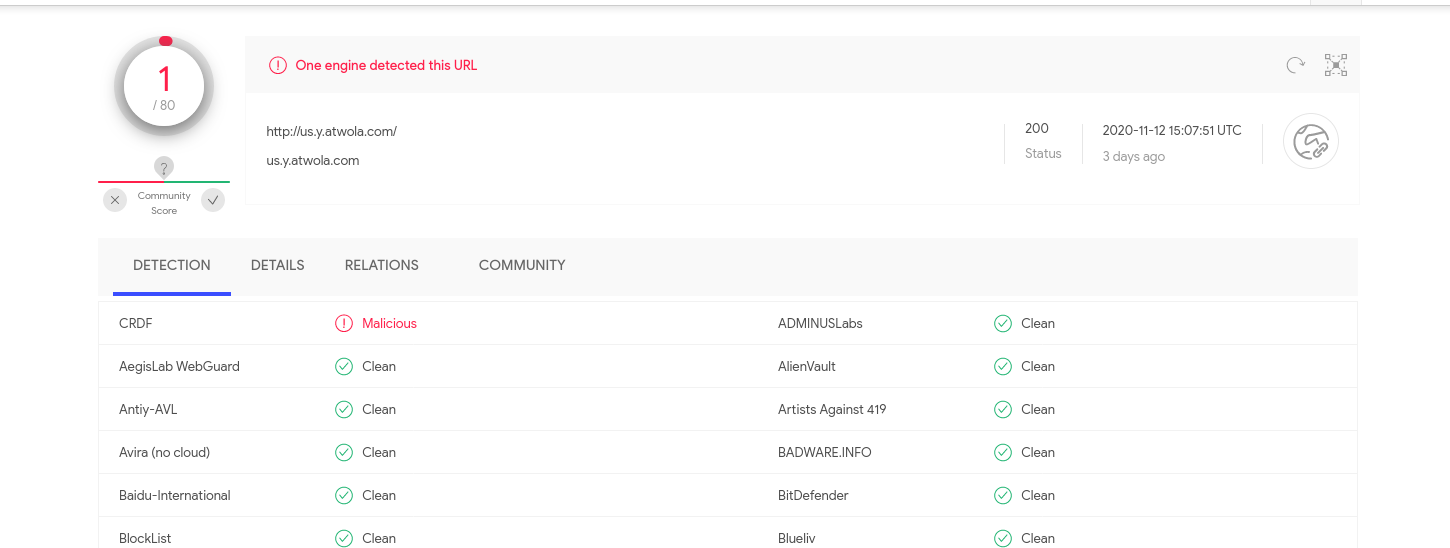


Figure :us.y.atwola.com

UBNetDef used dns logs created by zeek to get more information regarding these malicious dns servers as shown.

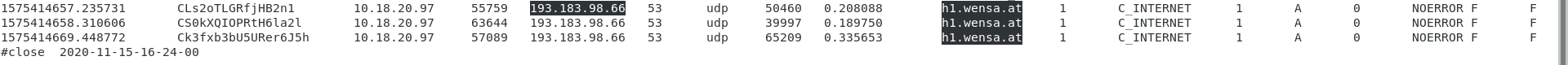


Figure : Malicious DNS 1

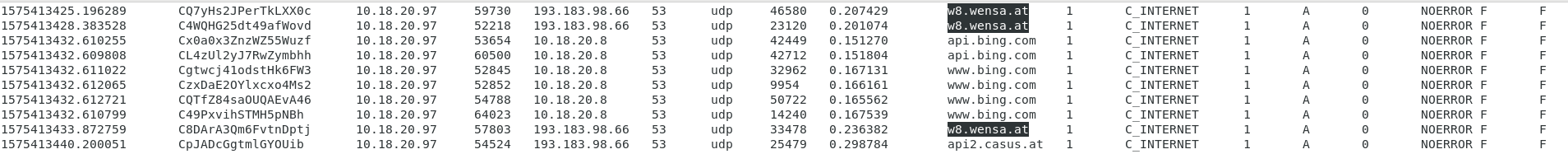


Figure : Malicious DNS 2



Figure : Malicious DNS 3

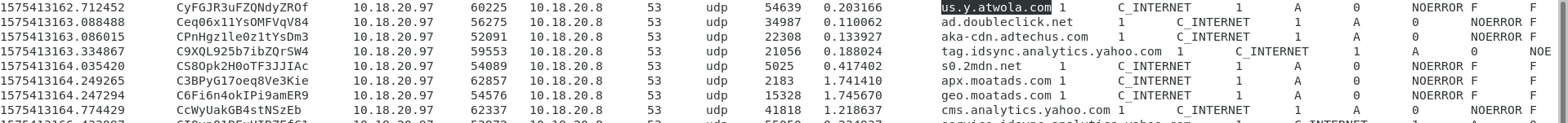


Figure : Malicious DNS 4

Next, UBNetDef used Network Miner tool to determine the Host Name - **JUANITA-WORK-PC** , Host Username - **momia.juanita** and Password (not revealed here to maintain confidentiality) as shown in the following image.

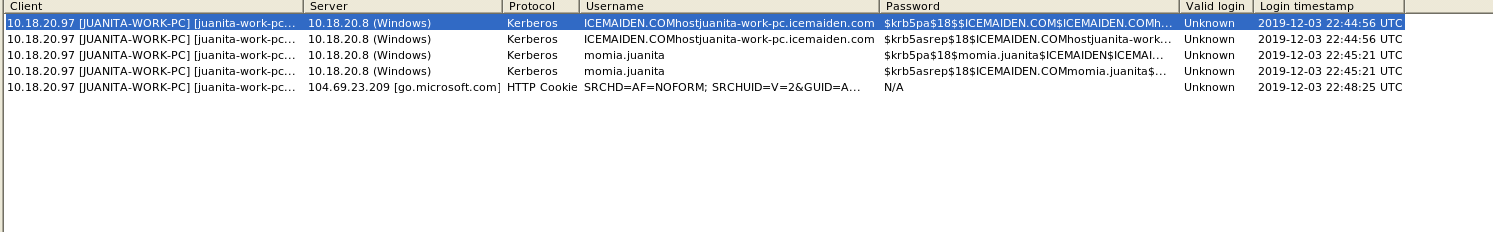


Figure : Host Info Revealed

UBNetDef used Virustotal to generate snort alerts for the pcap file. There were total 22 Snort alert for the pcap file out of which the outstanding one were Detection of a Denial of Service Attack, Attempted user Privilege Gain, Detection of Network Scan, Potentially Bad Traffic and Attempted Information Leak. The following images show more details.

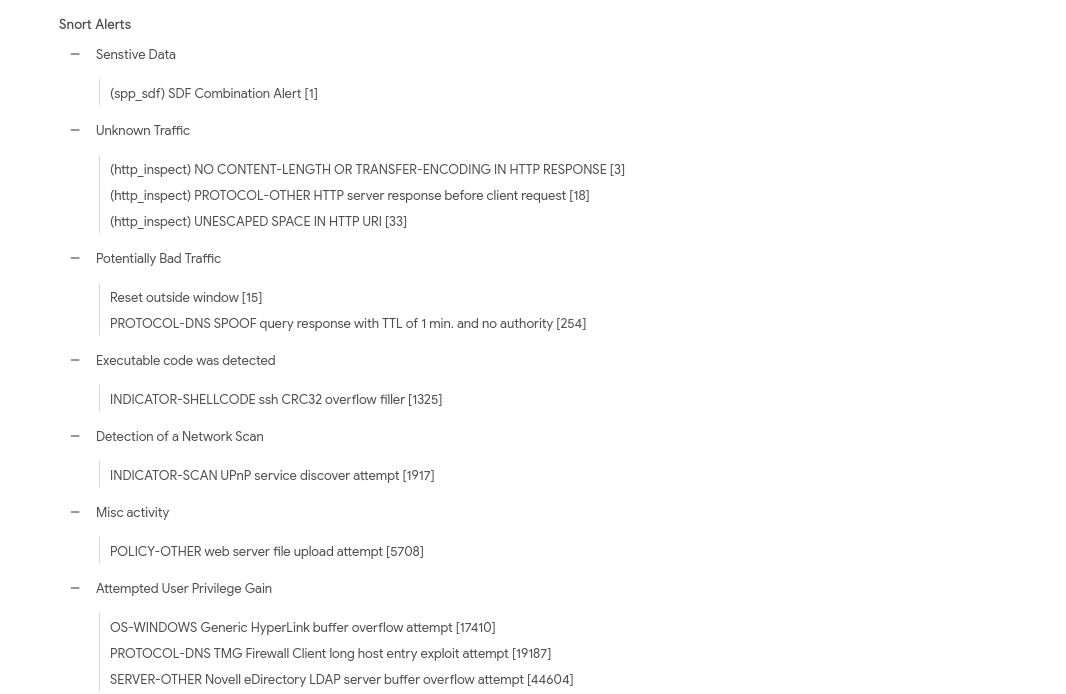


Figure : Snort Alerts 1

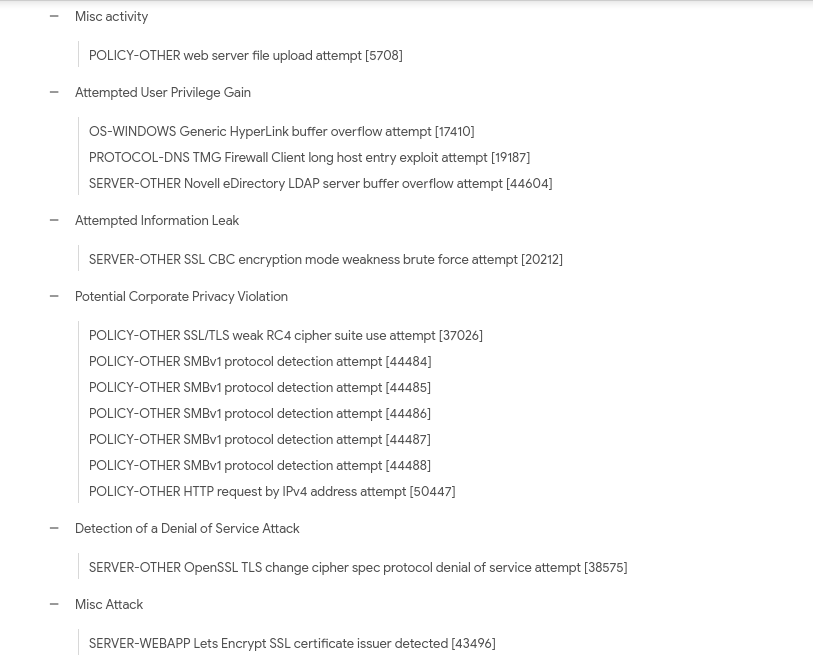


Figure : Snort Alerts 2

The Virustotal Scan also disclosed some crucial information like malicious http traffic, malicious ip’s and malicious dns servers as shown below.



Figure : Virustotal 1



Figure : Virustotal 2

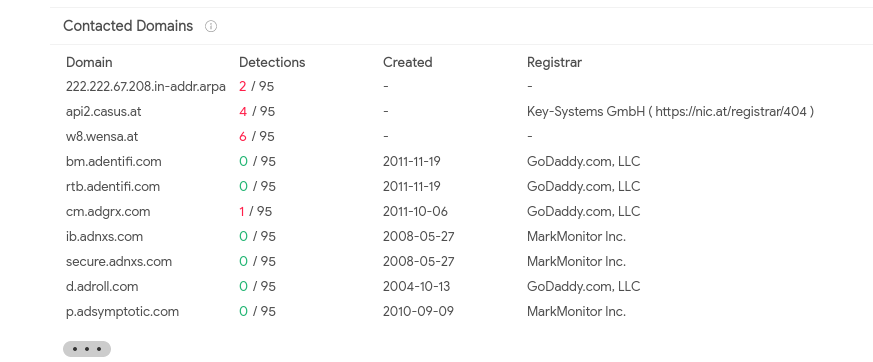


Figure : Virustotal 3

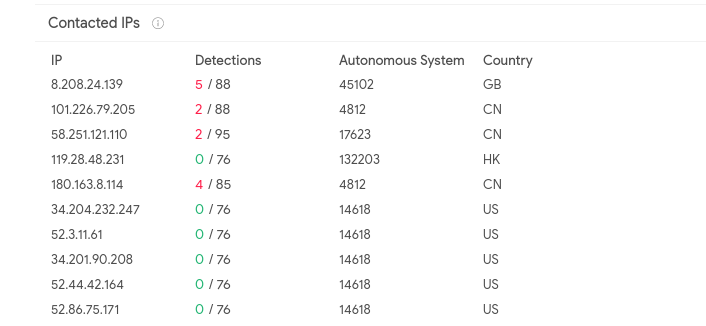


Figure : Virustotal 4

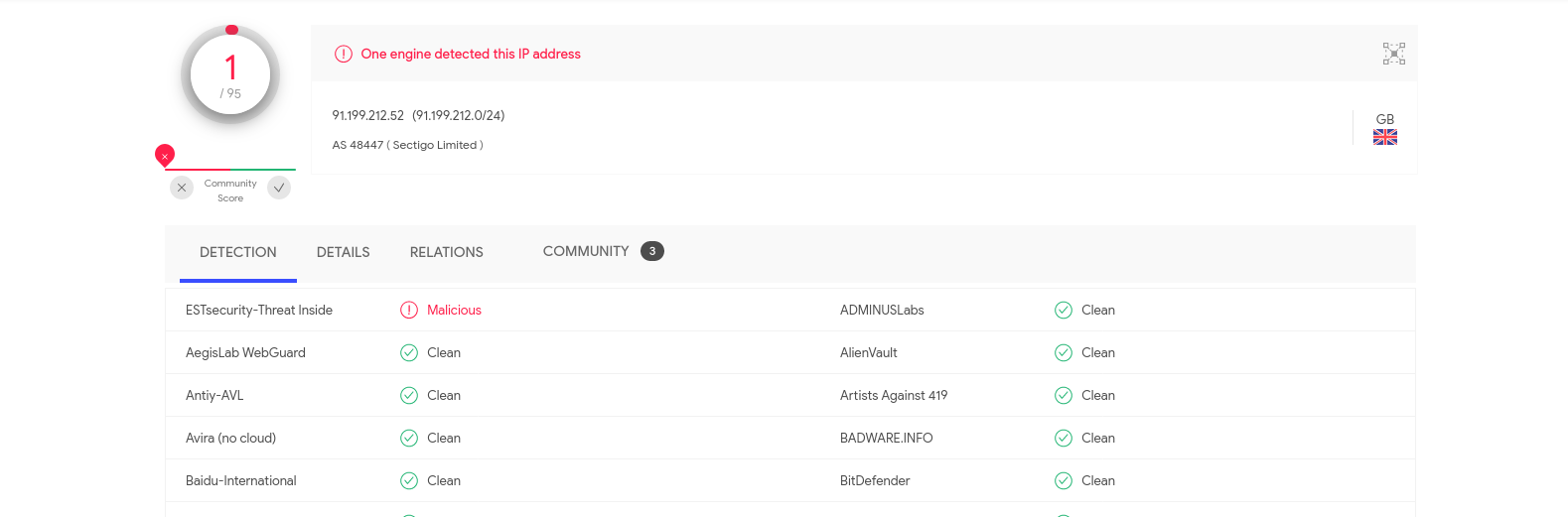


Figure : Virustotal 5

UBNetDef used Virustotal to generate Suricata alerts as well, which revealed a lot of crucial information including a Network Trojan used for Command and Control, Network Scan, Bad Traffic and Privilege escalation attempt. The following image show further details.



Figure : Suricata Alerts showing a Network Trojan

Upon execution, Ursnif checks for the presence of any virtual or debugging environments; if found, it will show a fake alert message box with the text, "Error Initializing Client App!". It also performs process hollowing on svchost.exe or explorer.exe and injects a dll file (client.dll) based on the system environment (whether it is 32- or 64-bit).

Afterwards, it tries to steal multiple pieces of information from the system and store them in a file. It then connects to a malicious command and control (C&C) server.

Ursnif is typically encountered when the user inadvertently opens a malicious file attachment that arrives via a spam email message.

# 

# Recommended Clean Up and Mtitigation Strategies

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

* 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.
* Ensure that programs and users of the computer use the lowest level of privileges necessary to complete a task. When prompted for a root or UAC password, ensure that the program asking for administration-level access is a legitimate application.
* 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.
* Turn off and remove unnecessary services. By default, many operating systems install auxiliary services that are not critical. These services are avenues of attack. By removing them, threats have less avenues of attack.
* Always keep your patch levels up-to-date, especially on computers that host public

services and are accessible through the firewall, such as HTTP, FTP, mail, and DNS

services.

* Isolate compromised computers quickly to prevent threats from spreading further.
* Perform a forensic analysis and restore the computers using trusted media.
* Train employees not to open attachments unless they are expecting them. Also, do not

execute software that they download from the Internet unless they scan it for viruses.

* Simply visiting a compromised Web site can cause infection if users don’t patch certain

browser vulnerabilities.

# practices:Contributing Analysts

Lead Analyst: Gursimran Singh

Contributing Analysts: 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