**TZFM862 CyberOps Associate**

**Question 3: The Cyber Security Investigation**

ã 2020 - 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Adapted by the Open University with permission – for sole use on TZFM862

**Introduction**

To complete this activity, you have to explore the Security Onion VM, you have been working on during your microcredential studies and determine any potential malicious activity associated with the Pushdo trojan. The module team advise you to consider reimporting the virtual machine image, to ensure that you have not created any unintentional false positives during your practical studies on the microcredential.

You should use internet research to learn more about the events, you may also use websites, such as VirusTotal to verify threat existence.

Content for this assessment was obtained from http://www.malware-traffic-analysis.net/ and is used with permission.

Step one is preparatory, marks will be available for Steps Two thru Four only.

**Submission guidance:**

• When submitting your EMA, please copy/paste this entire document into your main EMA submission, using it as a template for the investigation you must complete for question three.

• The word count is notional – please do not become fixated by this, word counts for practical activities tend to have little meaning. We will not adjust your marks for over, under or accurate.

• Evidence can either be copy/pasted or screenshots – however, you must also briefly write how you ‘found’ the evidence and cite any considered sources.

**Required Resources**

• Host computer with at least 8GB of RAM and 45GB of free disk space

• Latest version of Oracle VirtualBox

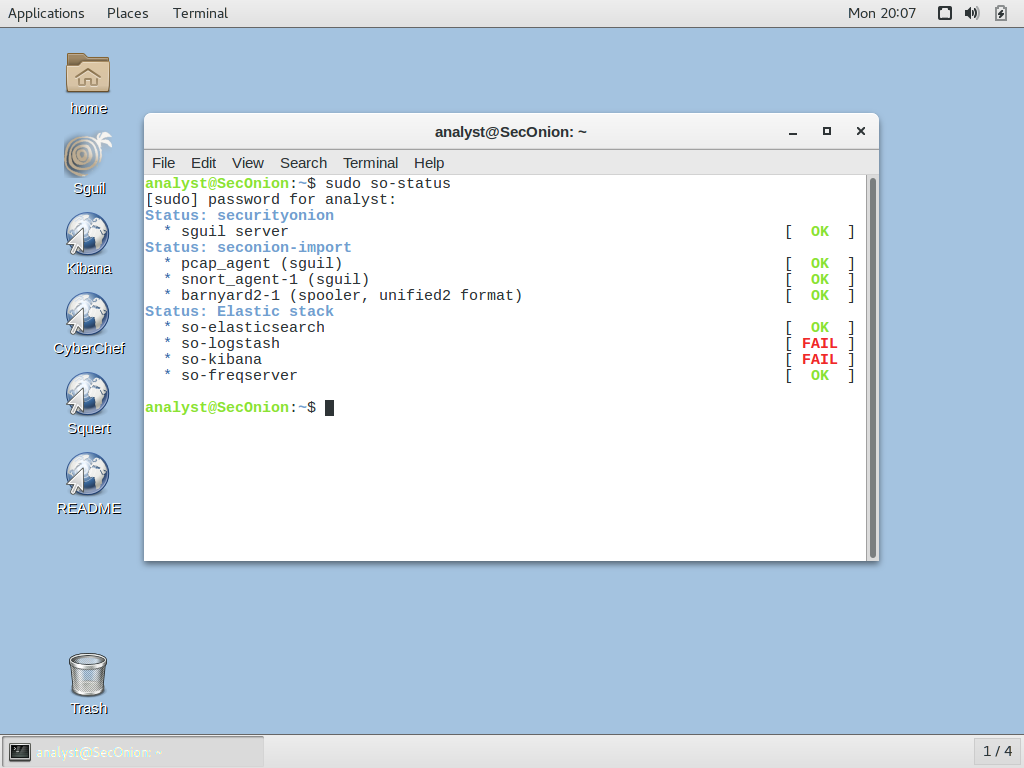
• The provided Security Onion virtual machine requires 4GB of RAM using 25GB disk space

• Internet access

**Step 1: Verify the status of services (unmarked)**

1. Log into Security Onion VM using with the username analyst and password cyberops.

b. Open a terminal window. Enter the sudo so-status command to verify that all the services are ready.

****

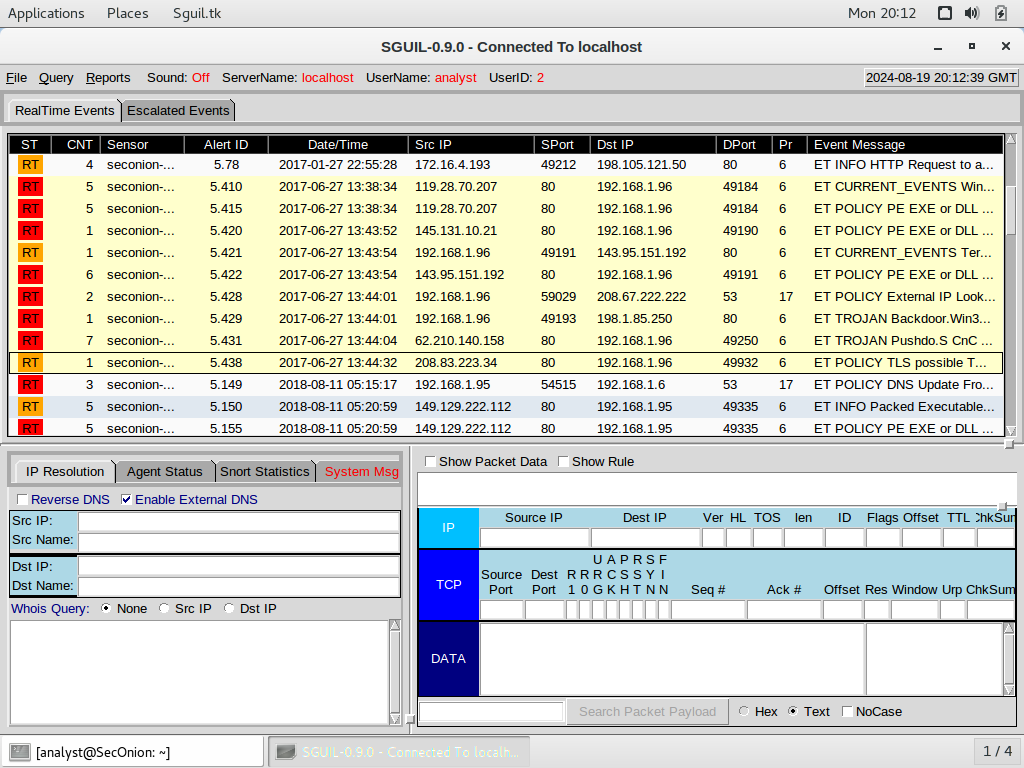
\* The screenshot shows kibana and logstash failed, I did not need to access these tools to complete the assessment\*

c. When the nsm service is ready, log into Sguil or Kibana with the username analyst and password cyberops.

**Step 2: Gather basic information (marked)**

Questions:

1. Identify the time frame of the Pushdo trojan attack, including the date and approximate timespan.

****

**The time frame for the attack was 2017-06-27 from 13:38:34 to 13:44:32**

1. List the alerts noted during the time frame associated with this trojan:

ET CURRENT\_EVENTS WinHttpRequest Downloading EXE

ET POLICY PE EXE or DLL Windows file download HTTP

ET POLICY PE EXE or DLL Windows file download HTTP

ET CURRENT\_EVENTS Terse alphanumeric executable downloader high likelihood of being hostile

ET POLICY PE EXE or DLL Windows file download HTTP

ET POLICY External IP Lookup Domain (myip.opendns .com in DNS lookup)

ET TROJAN Backdoor.Win32.Pushdo.s Checkin

ET TROJAN Pushdo.S CnC response

ET POLICY TLS possible TOR SSL traffic

1. List the range of internal IP addresses and external IP addresses involved.

IP addresses are displayed on the above sguil screenshot under src IP and dst IP columns:

**Internal IP address:**

* 192.168.1.96 – this is internal as it falls within the 192.168.x.x private address range

**External IP addresses:**

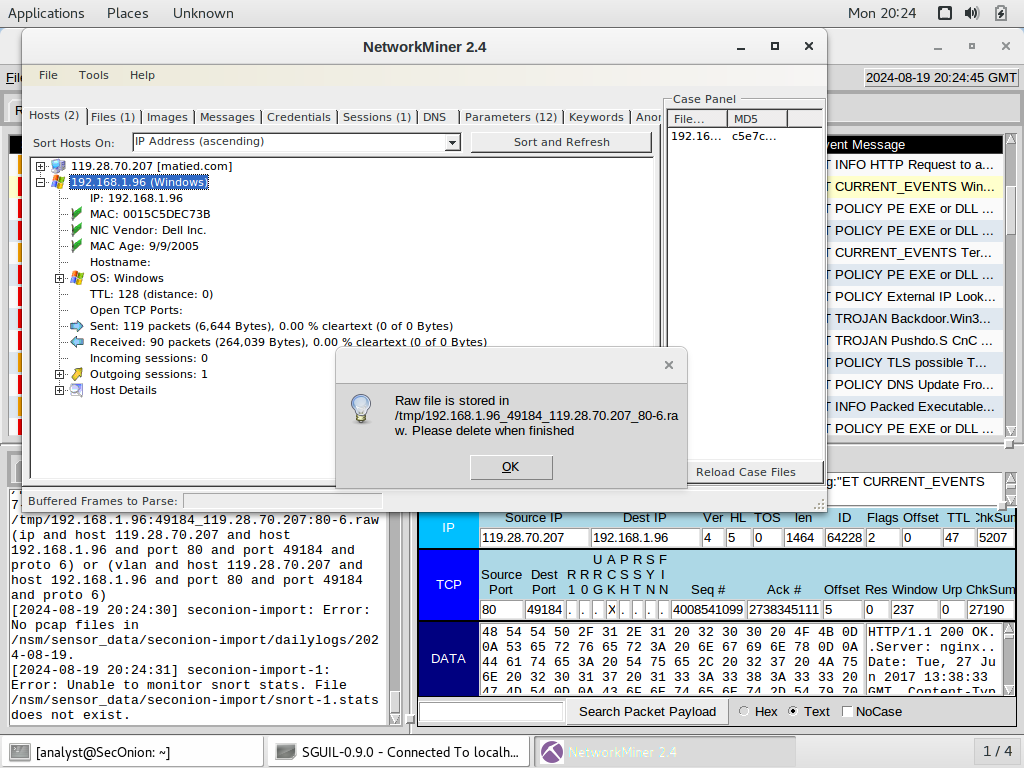
* 143.95.151.192
* 119.28.70.207
* 145.131.10.21
* 62.210.140.158
* 119.28.70.207
* 208.67.222.222
* 208.83.223.34
* 198.1.85.250
* These are external as they are public IP addresses

**Step 3: Infected host (marked)**

Questions:

1. Based on the alerts, what is the IP and MAC addresses of the infected computer? Based on the MAC address, what is the vendor of the NIC chipset?

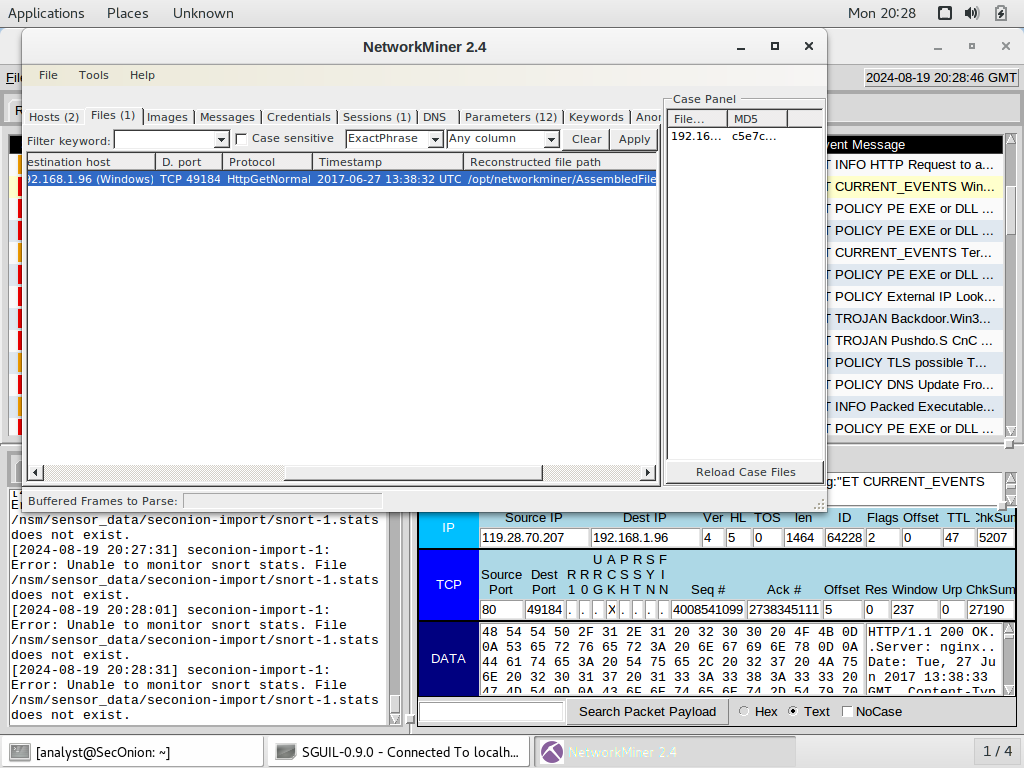
**Right click on alert ID 5410, select NetworkMiner**

****

**IP address: 192.168.1.96 MAC: 00-15-C5-DE-C7-3B NIC VENDOR: DELL INC**

1. Based on the alerts, when (date and time in UTC) and how was the system infected?

**Click Files in NetworkMiner, to view the timestamp:**

****

**The PC was infected at 2017-06-27 13:38:32 UTC, malware named gerv.gun was executed via the Pushdo trojan**

1. How did the malware infect the system?

The PC with IP address 192.168.1.96 connected to a malicious domain. Malware was installed using the Pushdo trojan. Pushdo is often referred to as a ‘downloader’ trojan – its intention is to download and install malware.

<https://www.secureworks.com/research/pushdo>

**Step 4: Examine the exploit (marked)**

Questions:

1. Based on the alerts associated with HTTP GET request, what files were downloaded?

**gerv.gun trow.exe wp.exe**

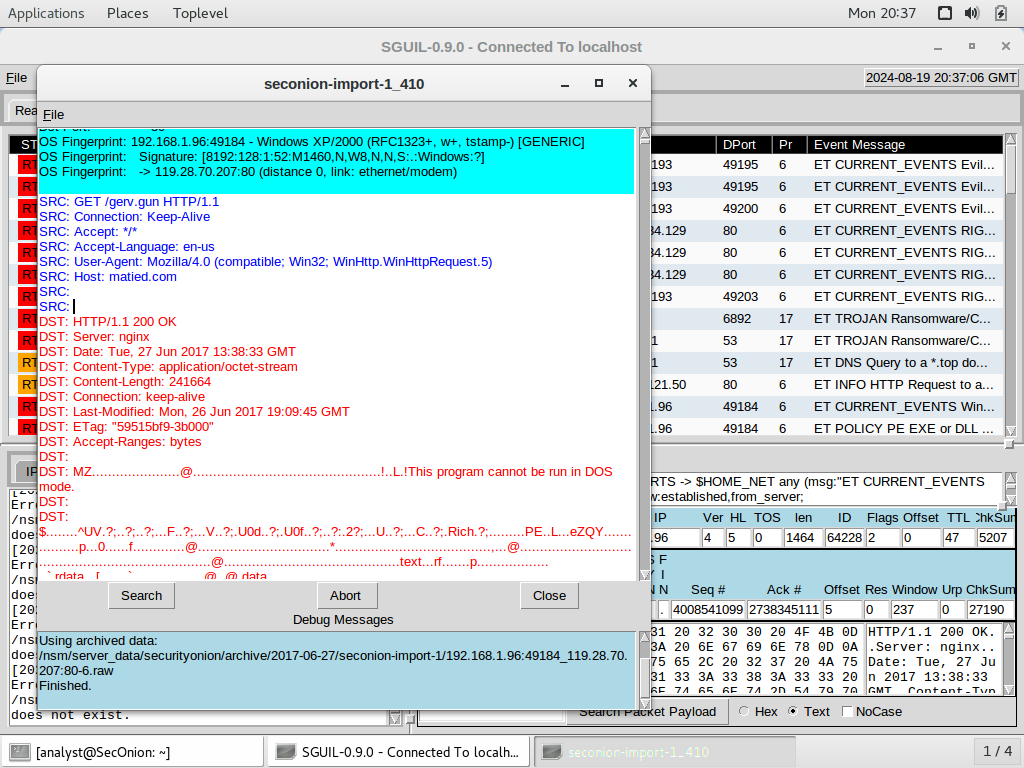
1. List the malicious domains observed and the files downloaded.

**matied.com/gerv.gun**

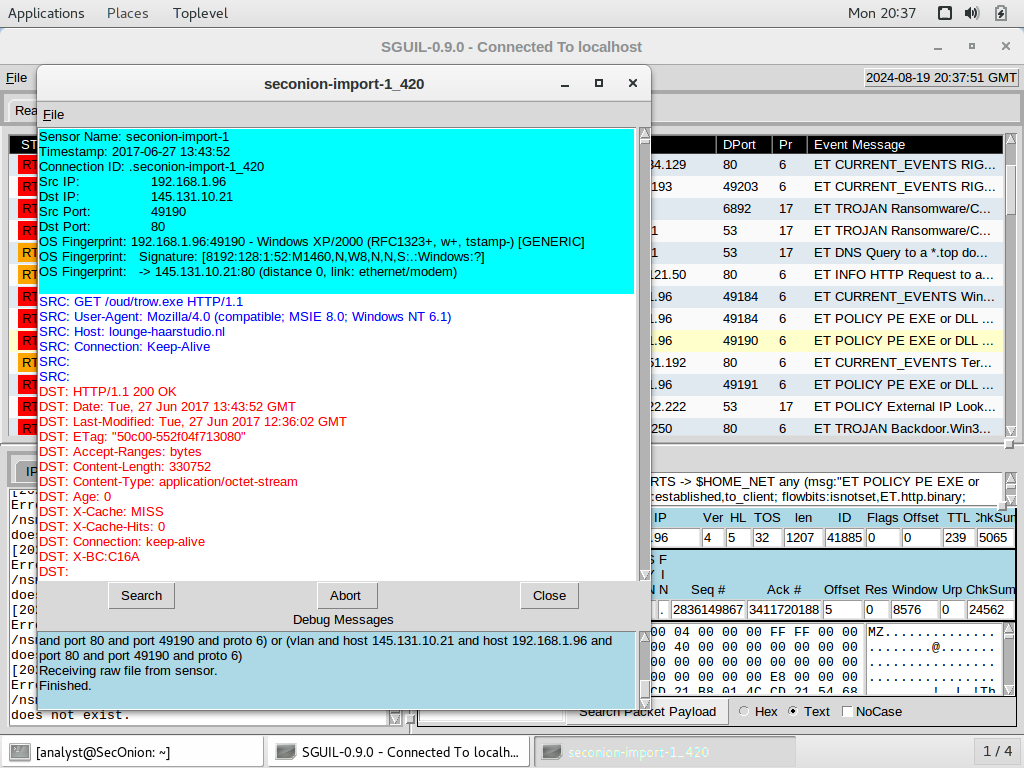
**lounge-haarstudio.nl/oud/trow.exe**

**vantagepointtechnologies.com/wp.exe**

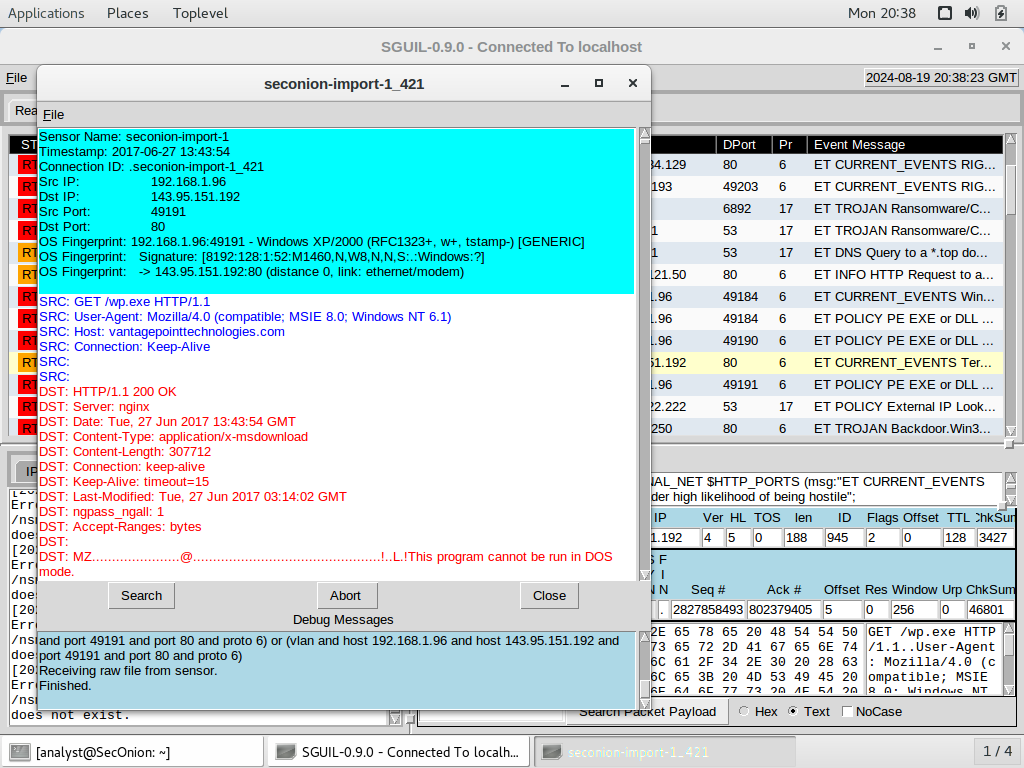
**Right click on alert ID 5410, select transcript**

****

**Right click alert ID 5420, select transcript**

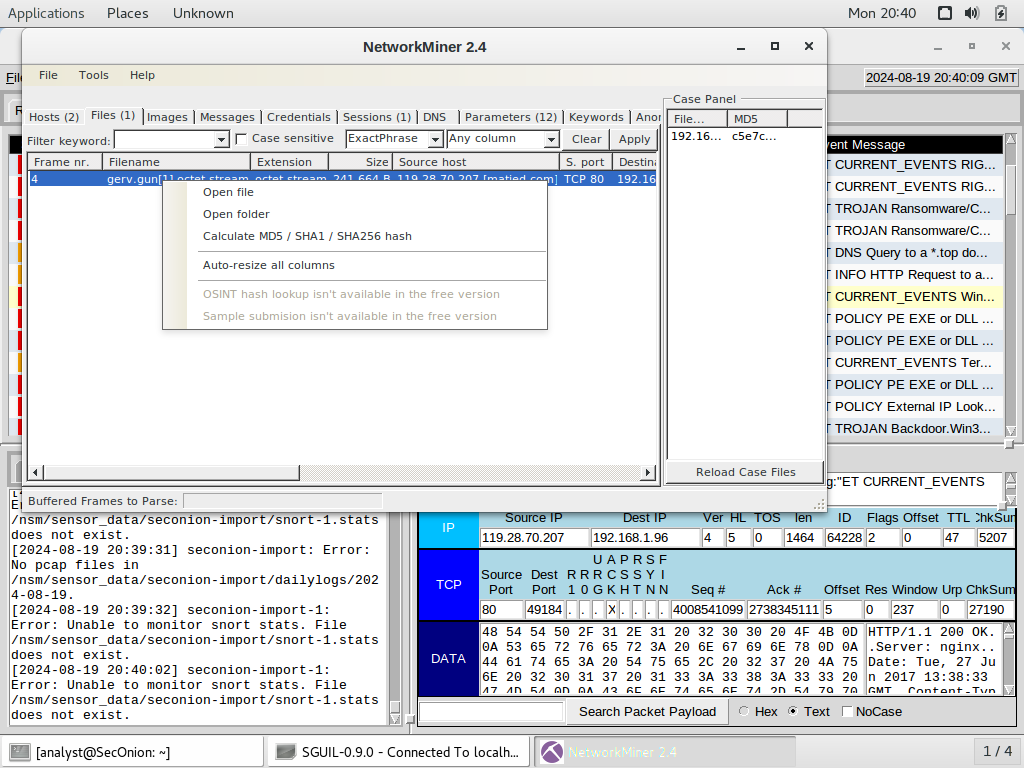
****

**Right click alert ID 5421, select transcript**

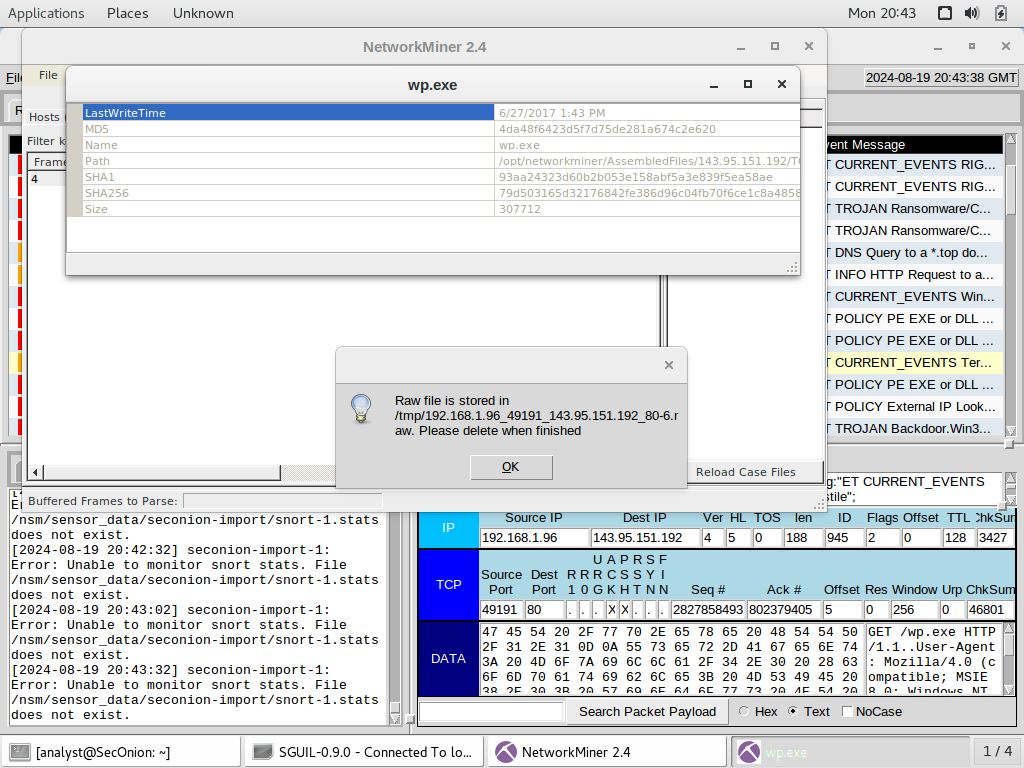
****

1. Use any available tools in Security Onion VM, determine and record the SHA256 hash for the downloaded files that probably infected the computer?

**Using the NetworkMiner utility, right click on alert ID 5410, choose NetworkMiner, click Files tab. On the first line, right click, select Calculate MD5/SHA1/SHA256 hash**

****

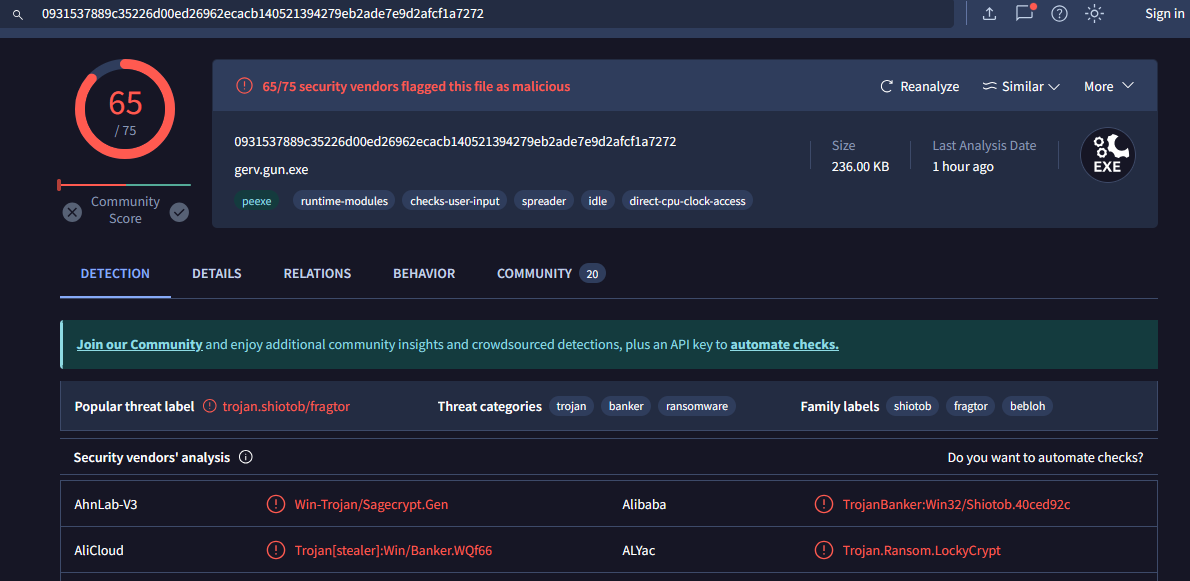
**Below shows the hash information for the wp.exe file**

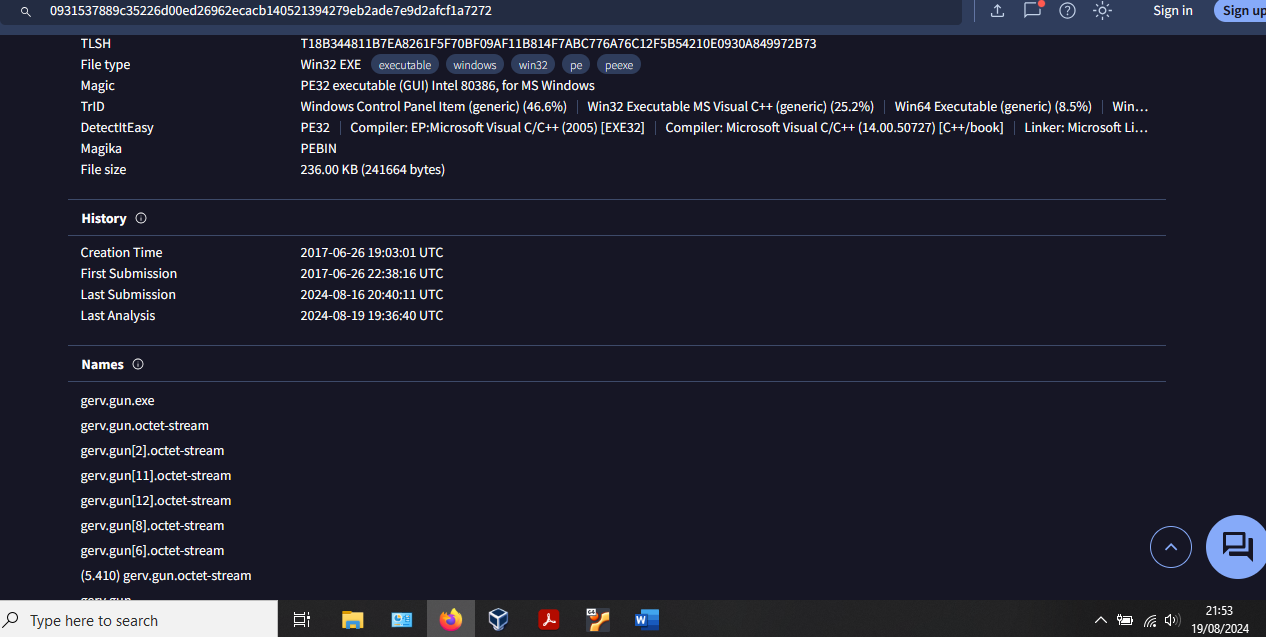
****

**The process was repeated for alerts 5420 and 5421.**

1. Navigate to www.virustotal.com input the SHA256 hash to determine if these were detected as malicious files. Record your findings, such as file type and size, other names, and target machine. You may also include any relevant information provided by the community as posted in VirusTotal.

**Opened firefox and entered virustotal.com into address bar. In the search bar, each hash was entered to display the following results:**

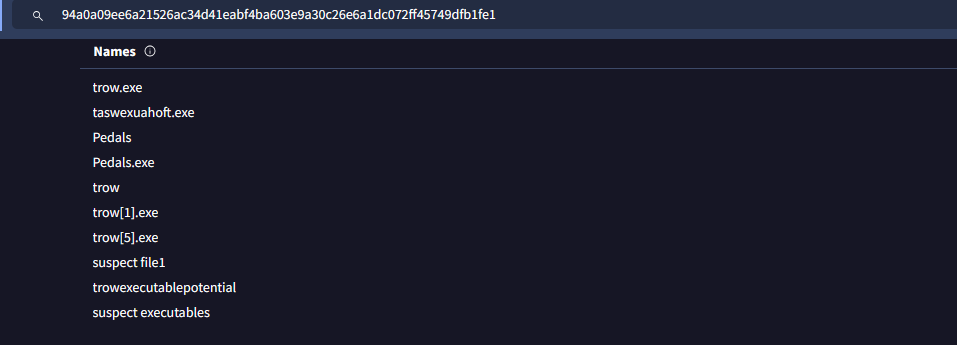
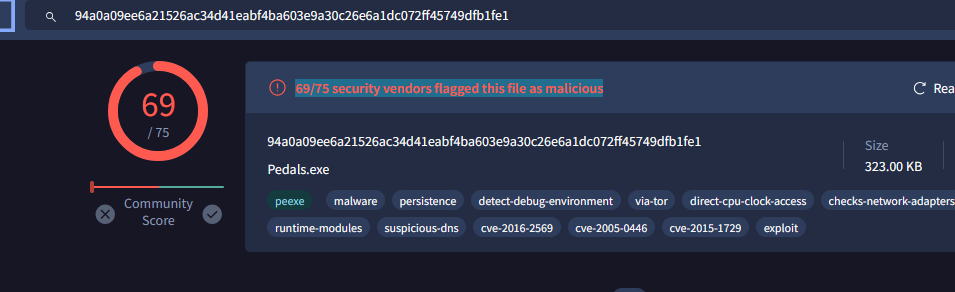
****

****

gerv.gun. = 0931537889c35226d00ed26962ecacb140521394279eb2ade7e9d2afcf1a7272

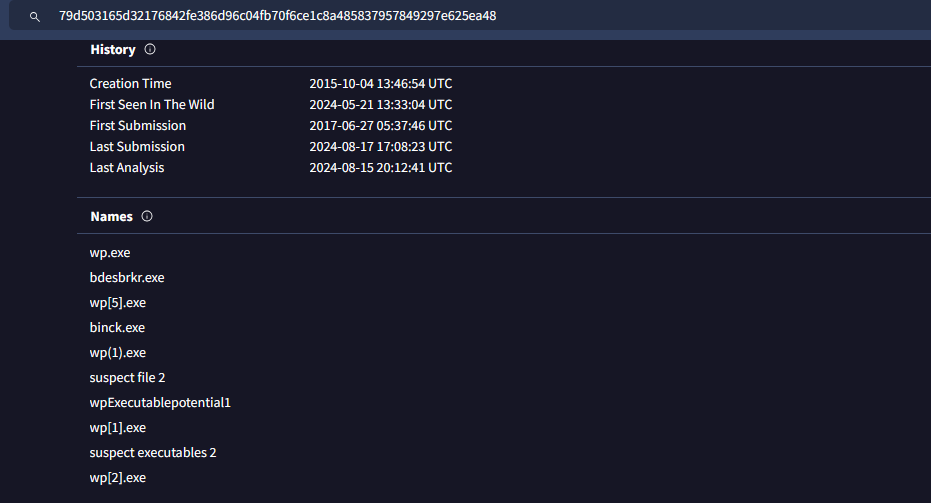
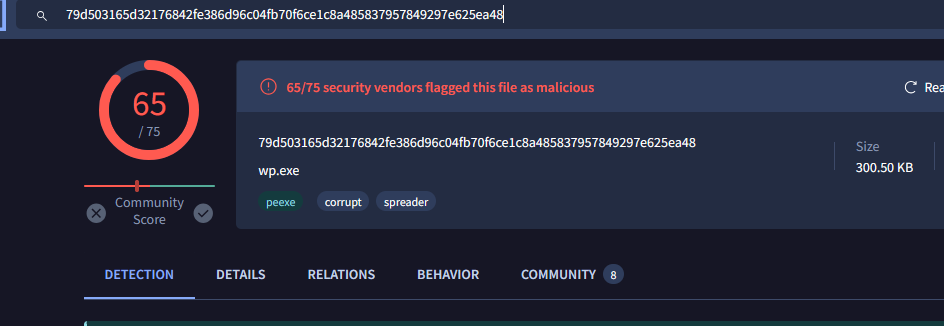
**gerv.gun**

* 65/75 vendors flagged as malicious
* File type Win32.EXE
* File size 236KB
* Threat categories: trojan, banker, ransomware
* Target machine: intel 386 or later processor and compatible processors
* Other names:
* gerv.gun.exe
* gerv.gun.octet-stream
* gerv.gun[2].octet-stream
* gerv.gun[11].octet-stream
* gerv.gun[12].octet-stream
* gerv.gun[8].octet-stream

****

**trow.exe** = 94a0a09ee6a21526ac34d41eabf4ba603e9a30c26e6a1dc072ff45749dfb1fe1

* threat categories: trojan, dropper
* 69/75 security vendors flagged this file as malicious
* Size 323KB
* Other names:
* Pedals
* Pedals.exe
* trow.exe
* test3
* 2017-06-28\_18-18-14.exe
* bma2beo4.exe
* Target Machine: Intel 386 or later processors and compatible processors

****

**wp.exe** = 79d503165d32176842fe386d96c04fb70f6ce1c8a485837957849297e625ea48

* 65/75 security vendors flagged this file as malicious
* Threat category: corrupt, spreader
* File type: Win32 EXE
* File size: 300.50 KB
* Other names:
* wp.exe
* test2
* test\_3
* 4da48f6423d5f7d75de281a674c2e620.virobj
* wp.exe.x-msdownload
* Target Machine: Intel 386 or later processors and compatible processors

**e. Evaluate other significant alerts associated with the infected host during this timeframe and record these**

In the event message column of Sguil, the ET POLICY External IP Lookup Domain (myip.opendns .com in DNS lookup) – reveals the infection began when host 192.168.1.96 performed a DNS lookup through a malicious domain with the destination IP address of 208.67.222.222

**Step 3: Report Your Findings**

Summarizes your findings based on the information you have gathered from the previous parts, summarize your findings.

The host with IP 192.168.1.96, connected to a malicious domain for a DNS query, and was infected with the Pushdo trojan. The Pushdo trojan masquerades as an Apache server, listening on port 80. Once infected, the Pushdo trojan downloads malware to the victim PC. Further investigation revealed the malware that was downloaded and installed – gerv.gun, trow.exe and wp.exe. After examining these files in virustotal.com, using their SHA256 hashes, the files were listed as malicious by most vendors and member comments.

References:

<https://www.secureworks.com/research/pushdo>

<https://www.securityweek.com/how-pushdo-malware-hides-cc-traffic/>

https://www.bitdefender.com/blog/labs/in-depth-analysis-of-pushdo-botnet/