## Introduction

You have been hired as a security analyst. You were tasked to determine any malicious activity associated with a malware attack.

You will have access to the internet to learn more about the events. You can use websites, such as VirusTotal, to upload and verify threat existence.

The tasks below are designed to provide some guidance through the analysis process.

You will practice and be assessed on the following skills:

* Evaluate event alerts using Squil.
* Use Google search as a tool to obtain intelligence on a potential exploit.
* Use VirusTotal to upload and verify threat existence.

# Instructions

## Gather the Basic Information

In this part, you will review the alerts listed in Security Onion VM and gather basic information for the interested time frame.

### Verify the status of services

* + - 1. Log into Security Onion VM.
      2. Open a terminal window. Enter the **sudo so-status** command to verify that all the services are ready.
      3. When the nsm service is ready, log into Sguil.sud
      4. Download the .pcap file of yours and replay the malware packet capture. Before replaying the packet capture, update IDS rules using the command **sudo rule-update**.

### Gather basic information.

#### Questions:

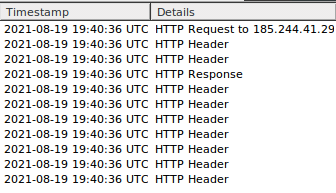
* + - 1. What is the name of the trojan? Identify the time frame of the attack, including the date and approximate time.

Ans:

Name: trojan.trickster/bulz

Also can be said as trickster / bulz / trickbot

Date and Approx time:

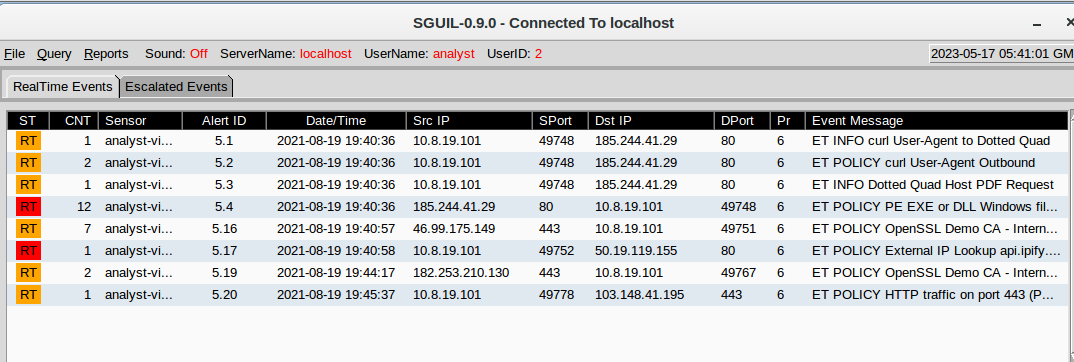


Or

19 Aug 2021 19:40:36 GMT

Type your answers here.

* + - 1. List the alerts noted during this time frame associated with the trojan.



Type your answers here.

* + - 1. List the internal IP addresses and external IP addresses involve

Internal :

10.8.19.101

External :

185.244.41.29

50.19.119.155

103.148.41.195

Type your answers here.

## Learn about the Exploit

In this part, you will learn more about the exploit.

### Infected host

#### 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? (**Hint**: NetworkMiner or internet search

ANS:

IP : 10.8.19.101

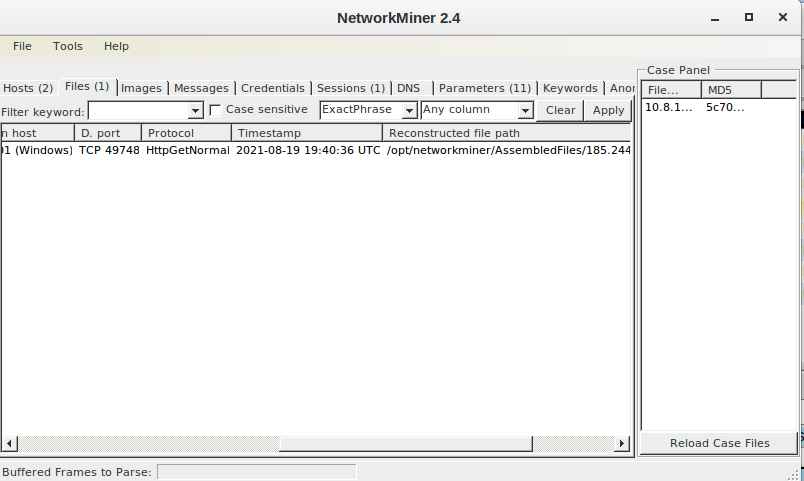
MAC : 00:08:02:1C:47:AE

NIC VENDOR : Hewlett Packard

Type your answers heggre

* + - 1. Based on the alerts, when (date and time in UTC) and how was the PC infected? (**Hint**: Enter the command **date** in the terminal to determine the time zone for the displayed time

Ans:



Ooiwy.pdf an executable file was executed by Trickster torjan

Type your answers here.

c. How did the malware infect the PC? Use an internet search as necessary.

Ans:

The user accessed a malicious ip address. Then the trickster malware was downloaded.

Then it looked up the external ip. There was HTTP traffic on port 443.

Trojan.Win32.Trickster (also known as TrickLoader and TrickBot) is capable of infecting 32- and 64-bit versions of Windows. The Trojan is generally small in size (less than 500 KB) and does not use additional packaging or encryption for the main body. Judging by the protocol used to communicate with the command-and-control server, the malware was rewritten from the source code for Dyre (Dyreza) but, unlike Dyre, is able to perform web injects.

The main body of Trojan.Win32.Trickster contains the following characteristic strings in Unicode format:  
• TrickLoader  
• Global\TrickBot  
• BotLoader

A characteristic and easily identifiable trait of the malware is the presence of the “TrickLoader” string in the User-Agent field of network packets.

A file with the list of command-and-control servers for Trojan.Win32.Trickster is stored in encrypted form in resources. The AES encryption algorithm is used for decrypting the list as well as modules received from command-and-control servers. The key consists of a hash in RSA-256 format.

Type your answers here.

### Examine the exploit.

#### Questions:

* + - 1. Based on the alerts associated with HTTP GET request, what files were downloaded? List the malicious domains observed and the files downloaded.

Ans:





GET /ooiwy.pdf

File Name: ooiwy.pdf

File Size : 316.00

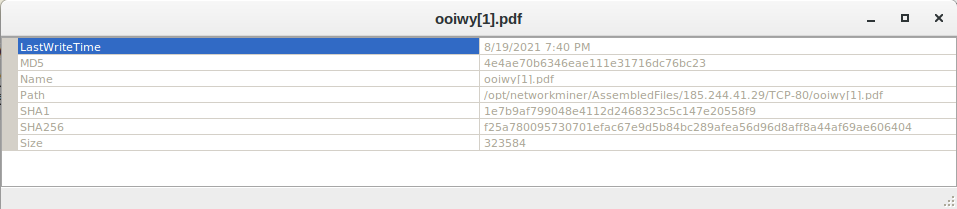
File Type : PE32 executable (DLL) (GUI) Intell 80386, for Ms Windows

Malicious Domain for DNS look up : api.ipify.org

Type your answers here.

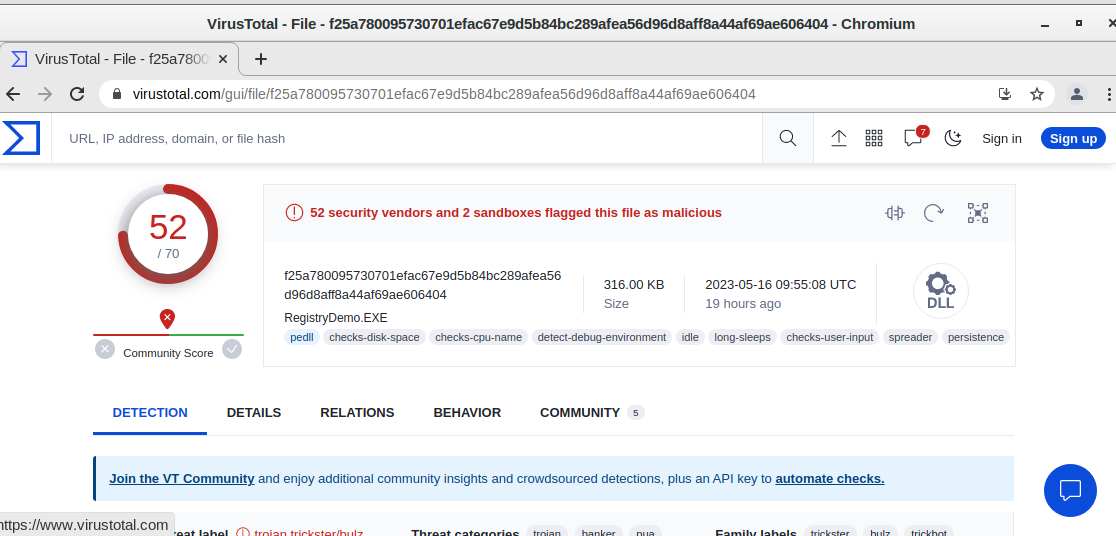
Use any available tools in Security Onion VM, determine and record the SHA256 hash for the downloaded files that probably infected the computer?

Ans:



Type your answers here.

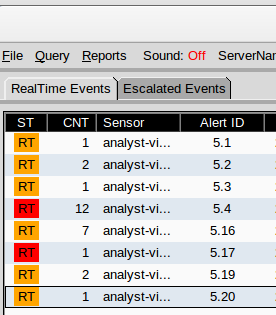
* + - 1. Navigate to [www.virustotal.com](http://www.virustotal.com) input the SHA256 hash to determine if these were detected as malicious files. Record your findings, such as file type and size, other names, and target machine. You can also include any information that is provided by the community posted in VirusTotal.

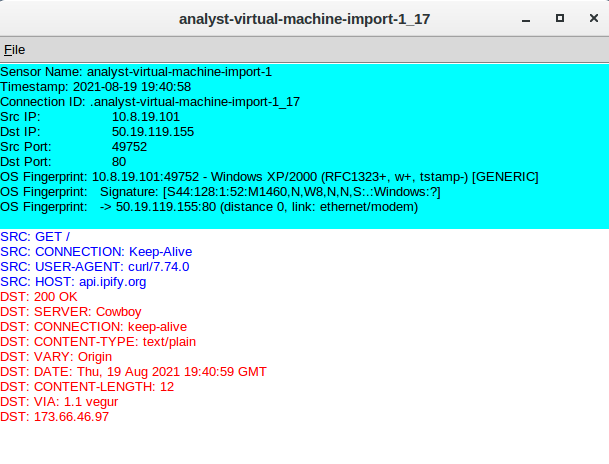


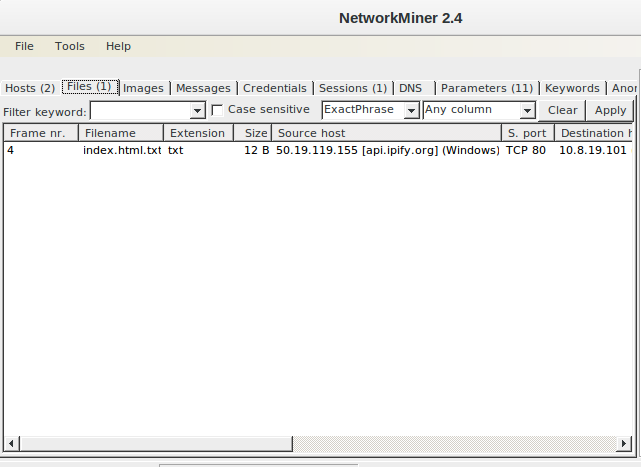
Type your answers here.

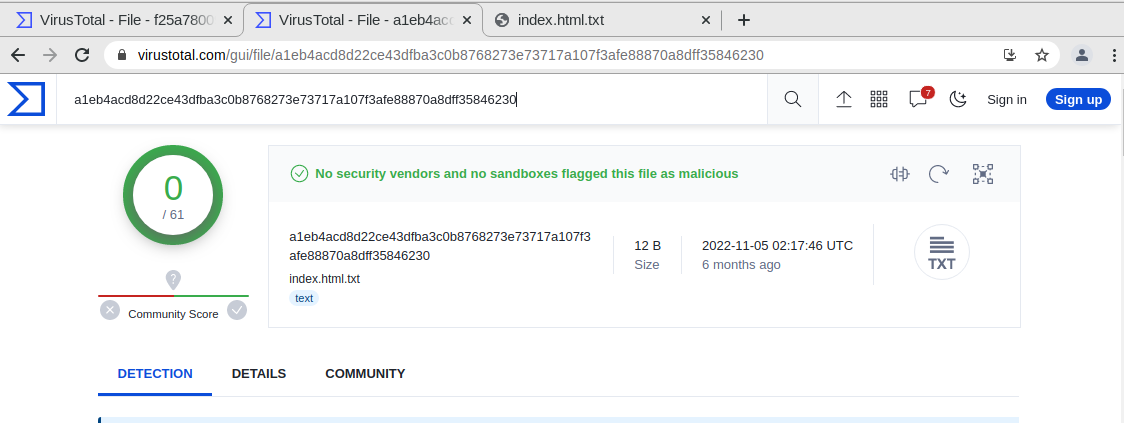
* + - 1. Examine other alerts associated with the infected host during this timeframe and record your findings

ANS:









We check the alert id 5.17. Here, index.htm.txt file is downloaded. The file seems to be virus free in the virus total but it contains the ip address that is 173.66.46.97. Here the host did an DNS Look up through a malicious domain which is

api.ipify.org

Alerts from 5.1, 5.2, 5.3 also download the same file ooiwy.pdf that is downloaded through get request.

Type your answers here.

### Report Your Findings

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

Ans:

The Host ip 10.8.19.101 a pc running on windows accessed malicious domain through DNS query and Trickster trojan file ooiwy.pdf file was downloaded. This malware was downloaded multiple times. The SHA256 of this file was calculated and run through virus total which resulted that it was a trojan trickster verified by 52/70 sources.

Type your answers here.

End of document