## PCAP-1

Sadir Ahmed Zidan

20-43263-1

## 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.

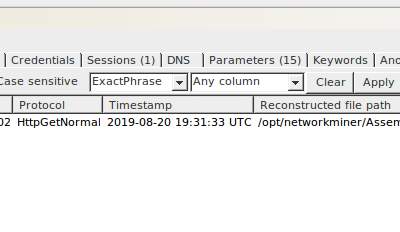
### Verify the status of services

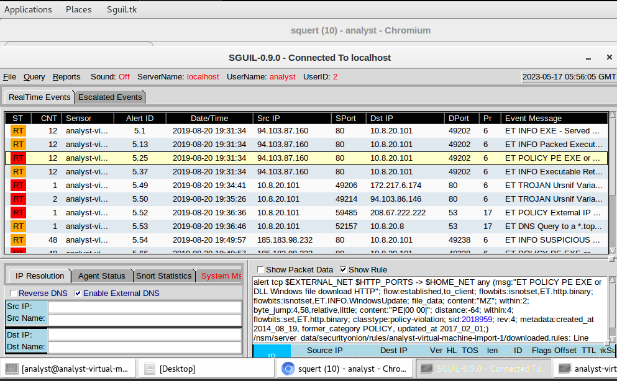
* + - 1. Log into Security Onion VM.
      2. Open a terminal window. Enter the **sudo so-status** command to verify that all the services are ready.
      3. When the nsm service is ready, log into Sguil.sud
      4. Download the .pcap file of yours and replay the malware packet capture. Before replaying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

### Gather basic information.

#### Questions:

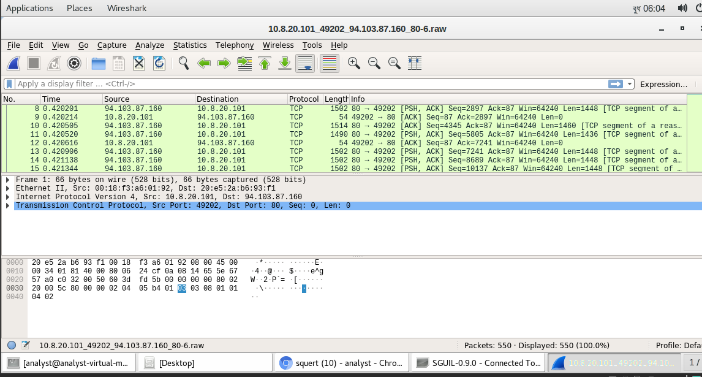
* + - 1. What is the name of the trojan? Identify the time frame of the attack, including the date and approximate time.
* Trojan Name: Trojan.Gozi
* Time frame: 08/20/2019 7:31 PM



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

.

* + - 1. List the internal IP addresses and external IP addresses involve
* Internal IP: 10.8.20.101
* External Ip: 94.103.87.160



Type your answers here.

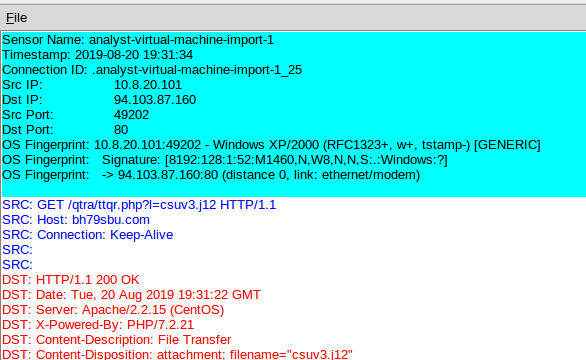
## Learn about the Exploit

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

### Infected host

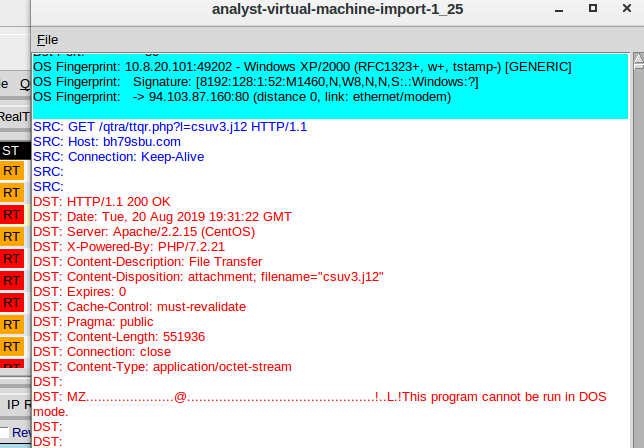
#### Questions:

* + - 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



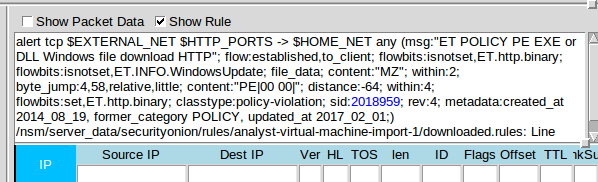
Type your answers heggre

* + - 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



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

The Gozi malware is usually spread by malicious websites, phishing emails, and opening a Word or Excel document, and requires macro to run.According to this pcap , the user had downloaded a file , by which the gozi malware infected the pc.

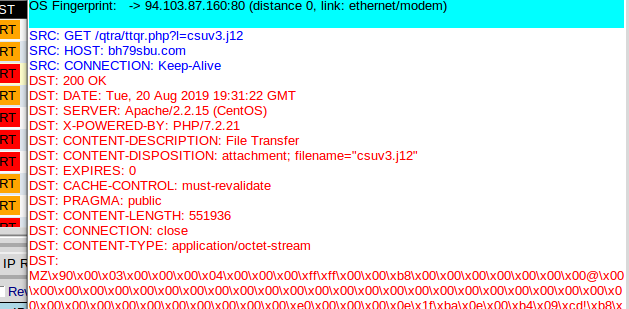


### Examine the exploit.

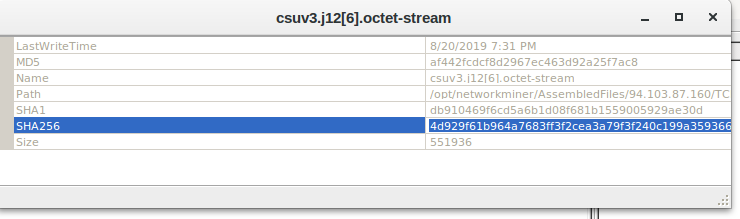
#### Questions:

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

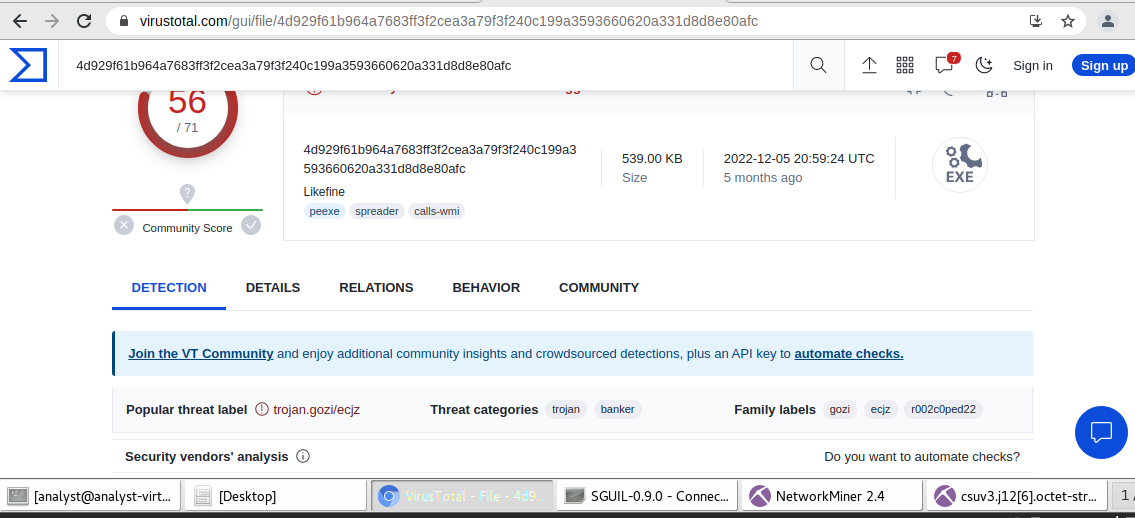
Here we can see a file name “csuv3.j12”



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



* + - 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.

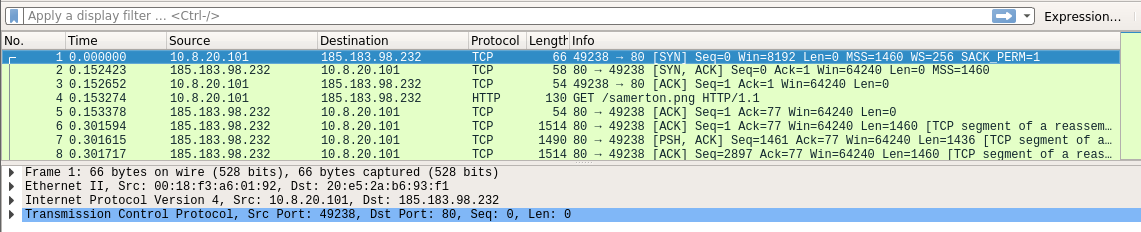




Trojan.Gozi is operated by several groups and can be dropped on the affected system by an Initial Acces Broker or be download by the user under false pretences.

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

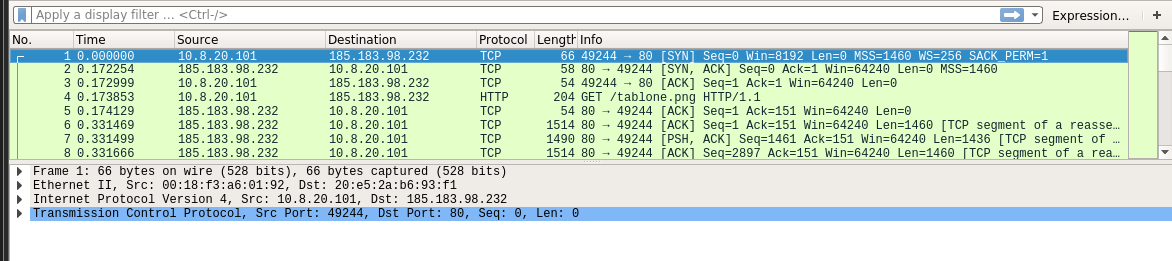
Another infected found at



And the time frame was 19:49





Type your answers here. 

### Report Your Findings

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

Find trojan gozi and 2 other infected. Got through a downloaded file and got a file also as infected.

Type your answers here.

End of document