Hasan Md Mahadi

19-41420-3

My file No – 4 ,

What is the name of the trojan? Identify the time frame of the attack, including the date and approximate

time.

Part 2 **Gather basic information.:**

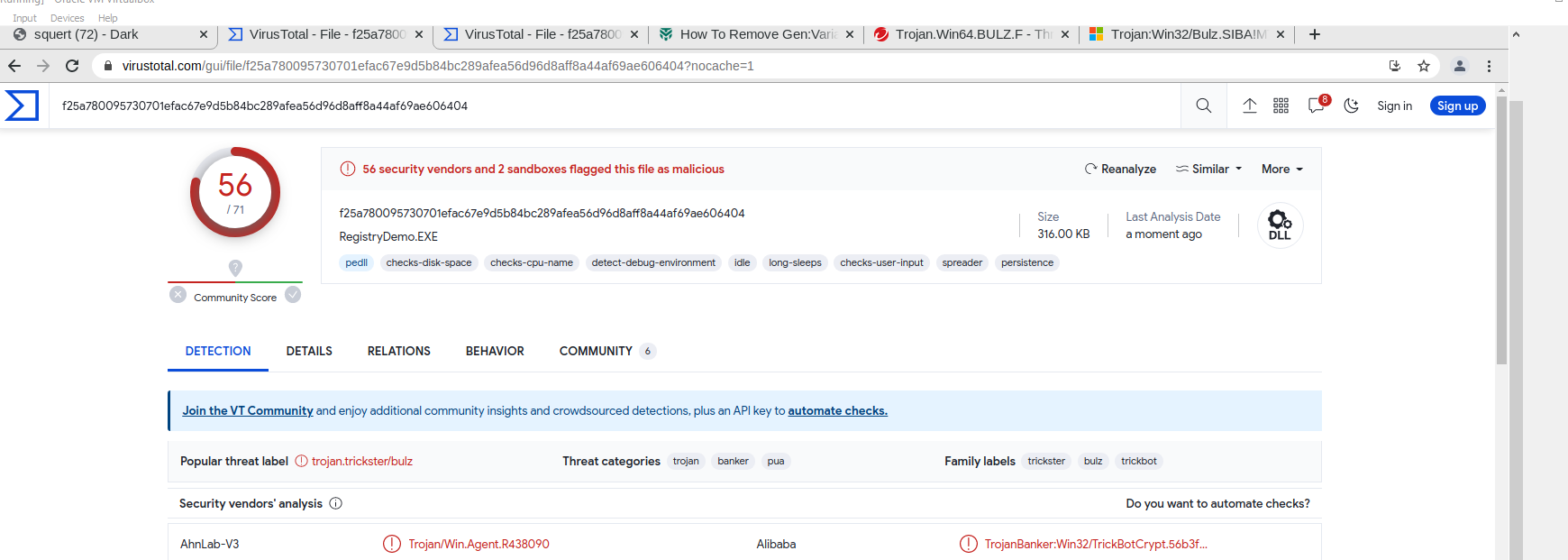
Name of the Trojan : **bulz**

**frame of the attack : Cross-frame scripting (XFS)**

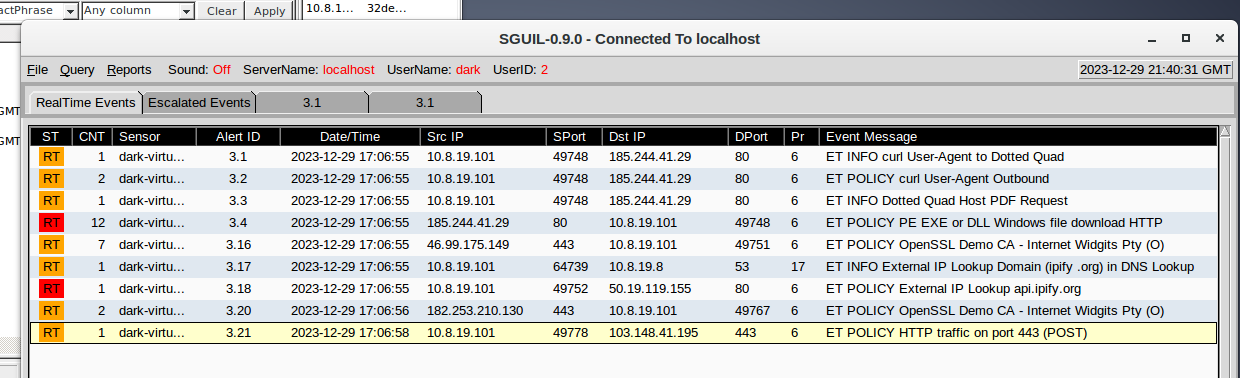
**, Actual Event time : Thu,19 Aug 2021 10:55:53 GMT**

**Server Apache/2.4.38(Debian)**

**Last Modified: Thu,19 Aug 2021 10:55:53 GMT**

****

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



Malware Traffic

c. List the internal IP addresses and external IP addresses involve

Home Network > 10.8.19.101

Destination Country and ip > Bangladesh 103.148.41.195

> US 50.19.119.155

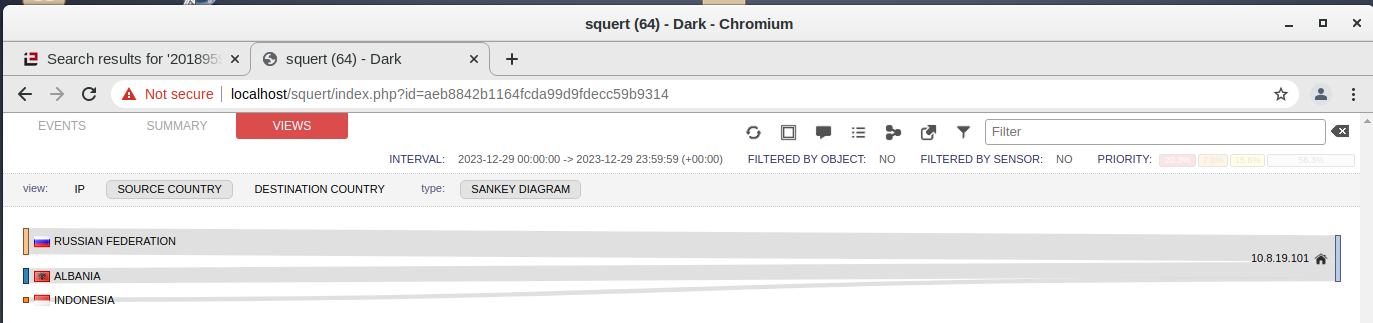
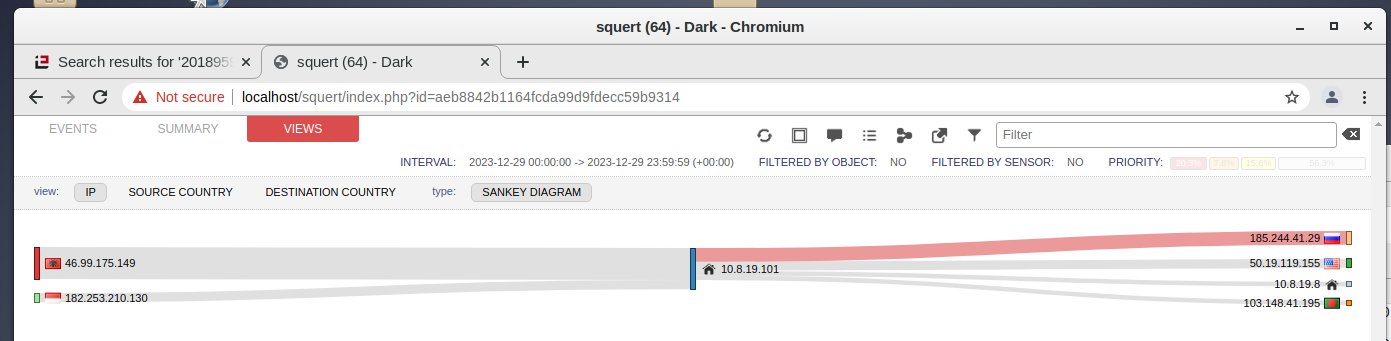
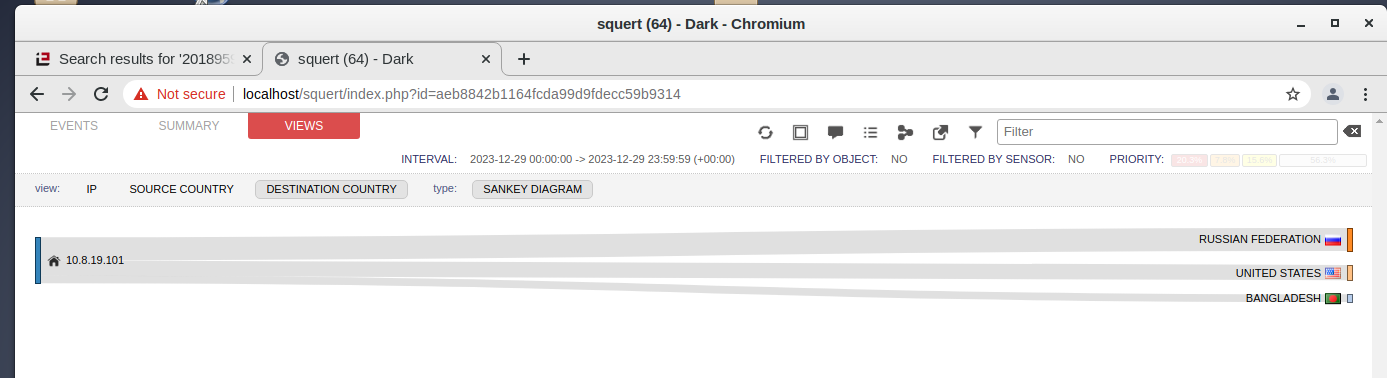
> Russia 185.244.41.29

………………………………………………………………………….

Source Country and IP > Russia Fed

> ALBANIA 46.99.175.149

> INDONESIA 182.253.210.130



**Part 2: Learn about the Exploit**

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

Step 1: Infected host

Questions:

a. 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

Infected User ip= 10.8.19.101

**Mac** : **0008021C47AE**

**NIC VENDOR** : **Hewlett Packard**

Mac Age : 10/24/2001

OS = Windows

**b. 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

Actual Event time : **Thu,19 Aug 2021 10:55:53 GMT**

Server Apache/2.4.38(Debian)

Last Modified: **Thu,19 Aug 2021 10:55:53 GMT**

Pc infacted when he or she try to Download a pdf file ,

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

Typical behavior for Trojans like Gen:Variant.Bulz is one or more of the following:

Download and install other malware.

Use your computer for click fraud.

Record your keystrokes and the sites you visit.

Send information about your PC, including usernames and browsing history, to a remote malicious hacker.

Give remote access to your PC.

So We can come up with a decision that the user download a pdf and that contains a virus . That's how user Infected ,

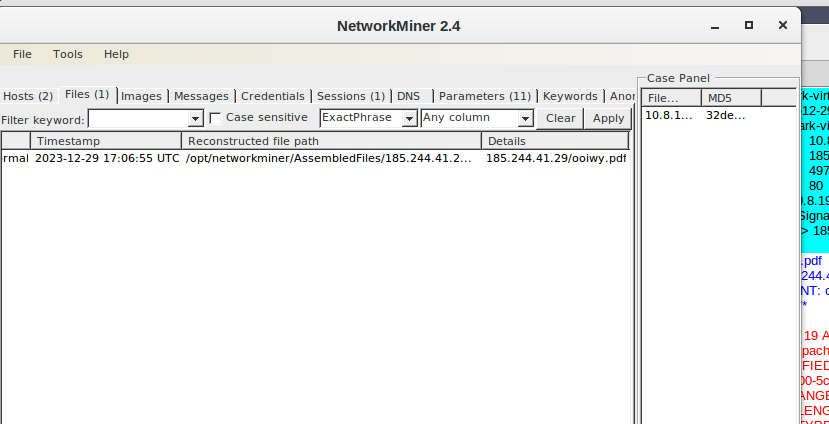
Step 2: Examine the exploit.

Questions:

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

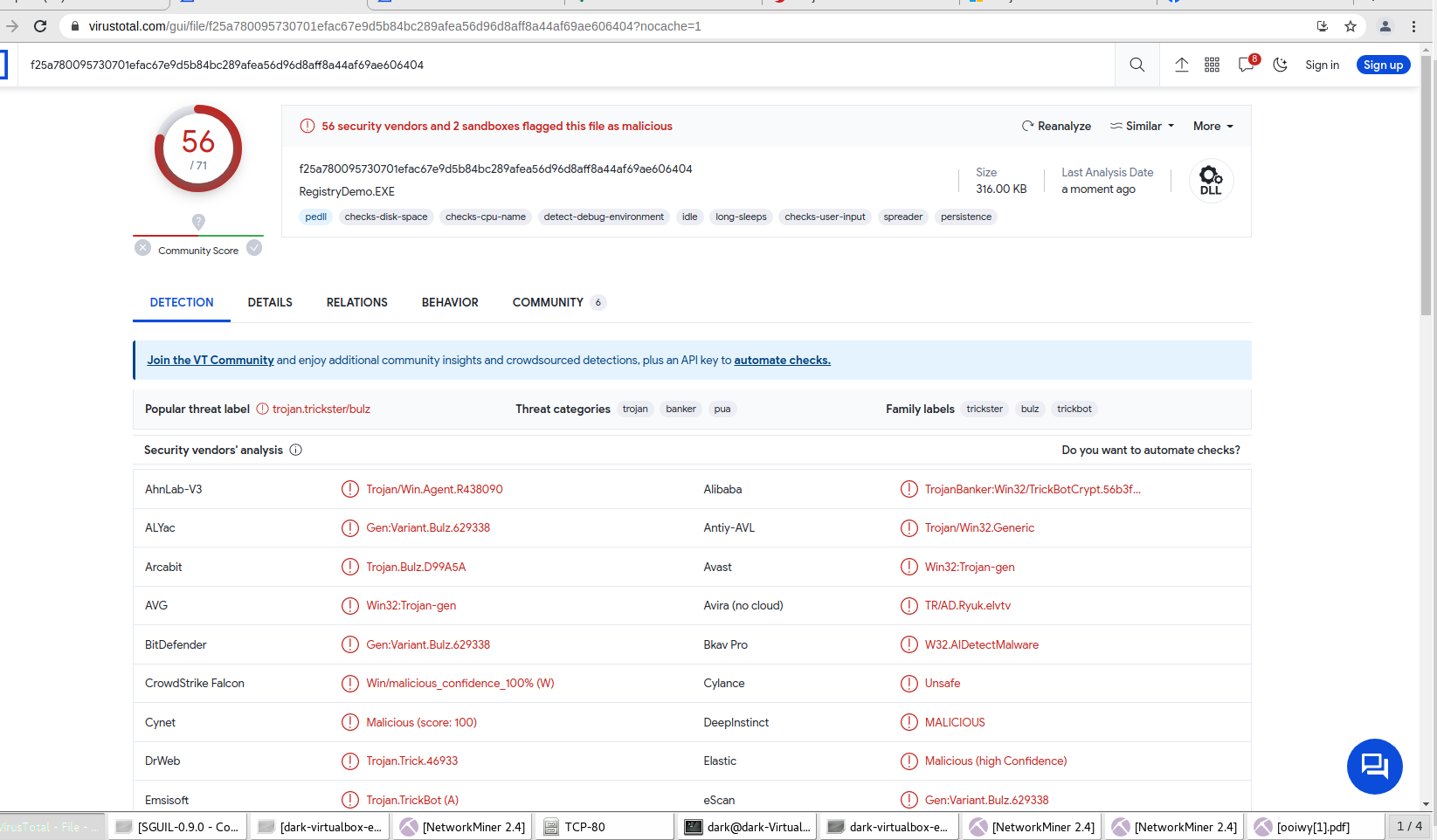
domains observed and the files downloaded

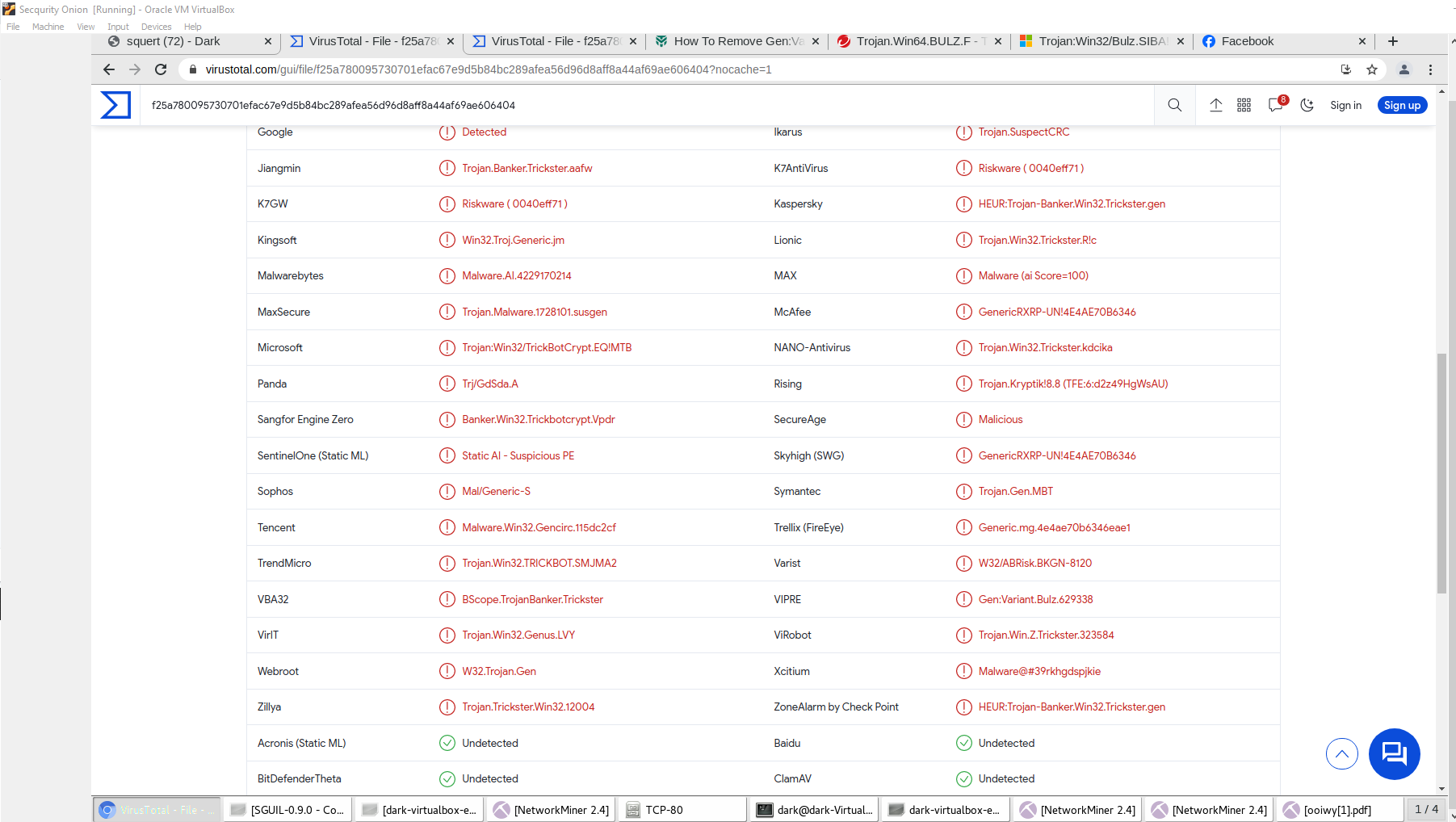
**TCP 80** , , Name of the file is **00iwy.pdf**

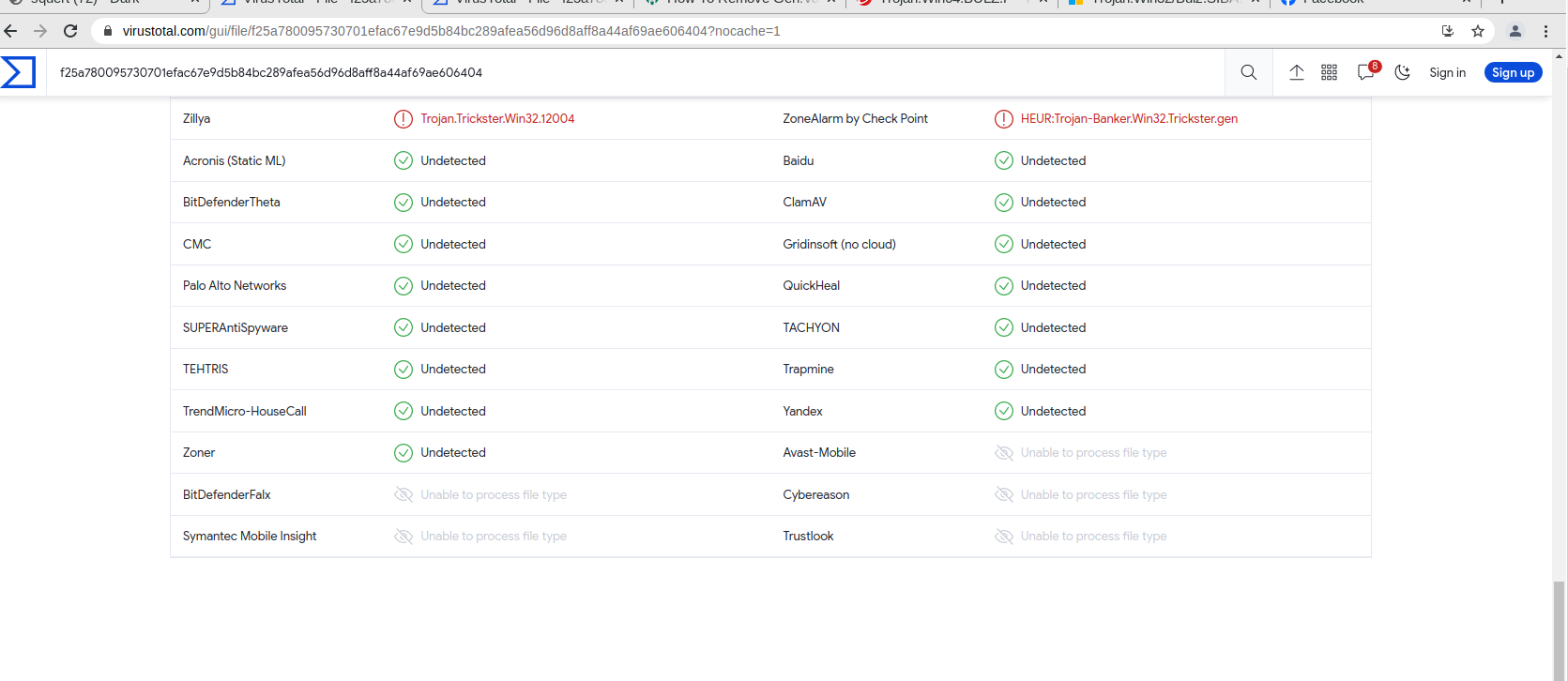


Use any available tools in Security Onion VM, determine and record the SHA256 hash for the

downloaded files that probably infected the computer



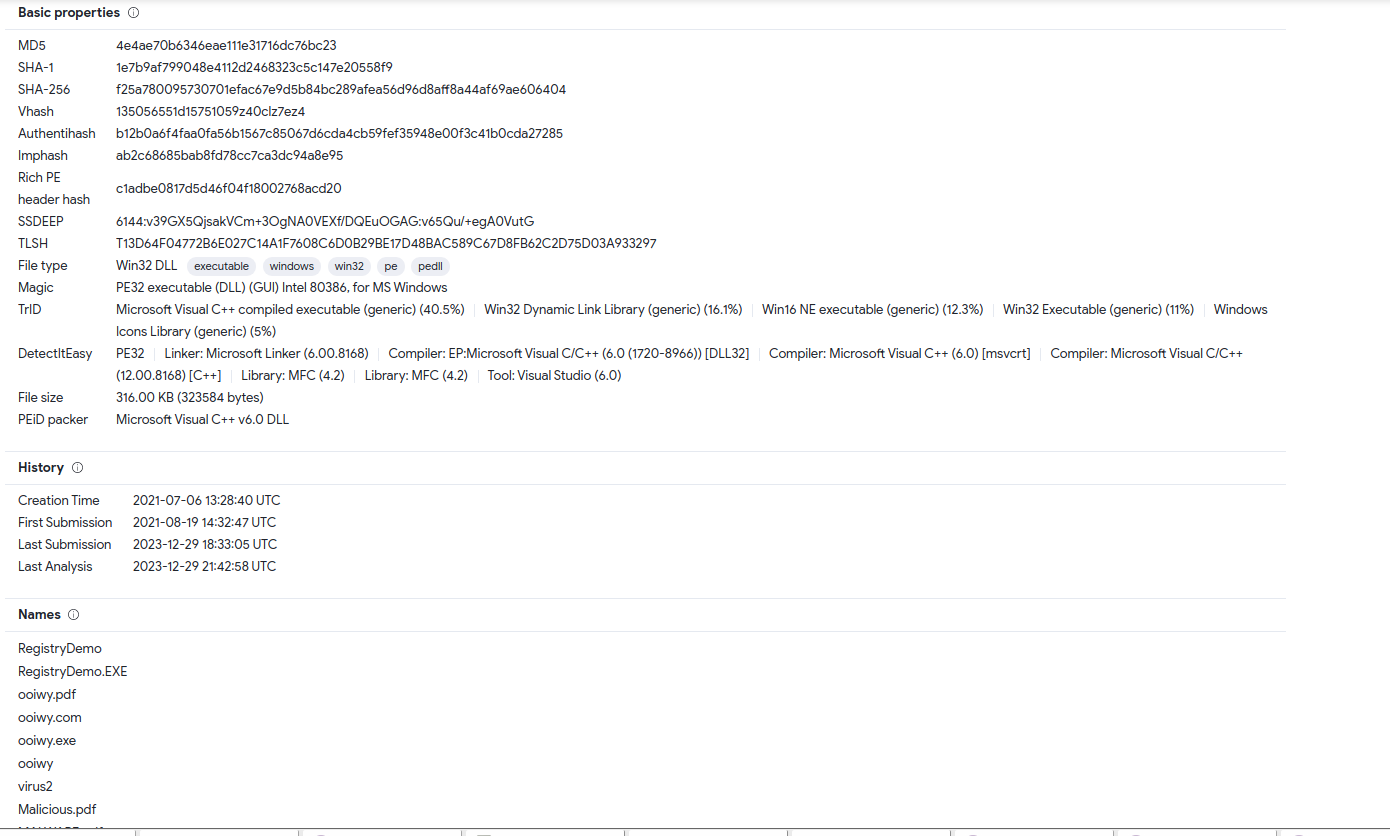




b. Navigate to www.virustotal.com input the SHA256 hash to determine if these were detected as malicious

files. Record your findings, such as file type and size, other names, and target machine. You can also

include any information that is provided by the community posted in VirusTotal



c. Examine other alerts associated with the infected host during this timeframe and record your findings

Step 3: Report Your Findings

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

your findings.

The infection was initiated through a phishing attack, facilitated by the downloading of a malicious PDF file. The trojan 'Bulz' exhibited characteristics typical of malicious software, including unauthorized data transmission and potential for further malware installation. The cross-frame scripting method indicates a sophisticated approach to exploiting vulnerabilities in web browsers or related software. The involvement of multiple international IP addresses suggests a broad scope of the attack or the use of a distributed network by the attackers.

This summary encapsulates the key aspects of the incident, focusing on the infection vector, the nature of the Trojan, and the subsequent network activities observed. Further analysis, especially with tools like VirusTotal for file hash analysis, would provide more detailed insights into the specific threats posed by the downloaded files.