CYBERSECURITY SEMINARS Google.org, 1st Cycle

Exercise 4

Fullname: Klajdi Cami

Activity 1: Virus Identification -- Scenario 1

Objective: To determine whether the protection software detects malicious files and, if so, how.

Steps:

1. Creating a "Virus"

• Open Notepad.

• Copy and paste the following string (EICAR Test File).

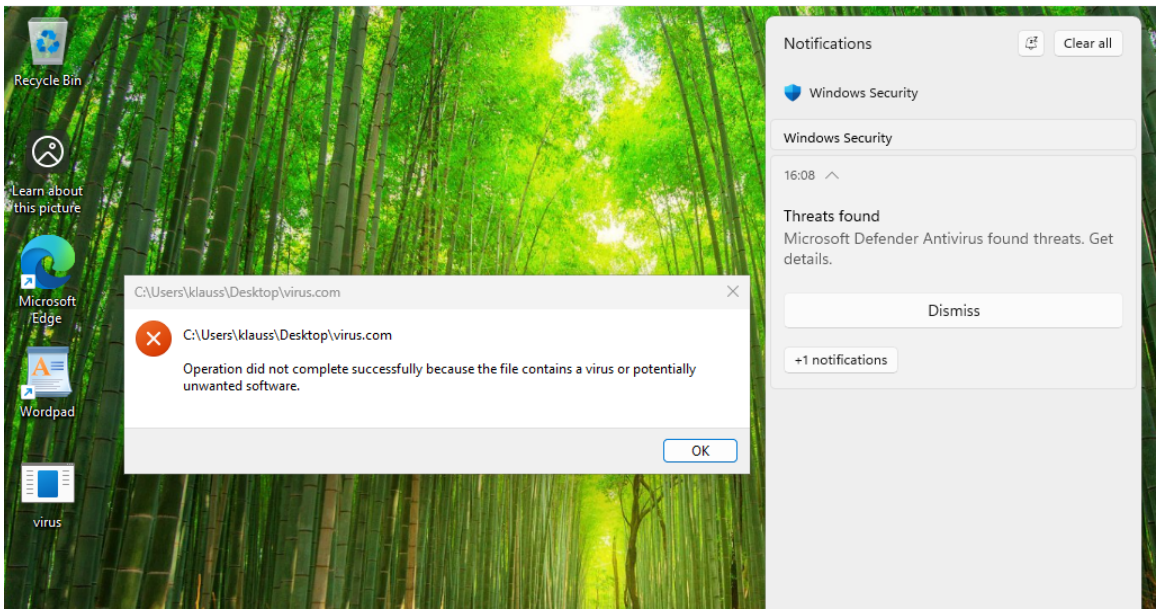
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

• Save the file as virus.com (select "All Files" instead of ".txt").

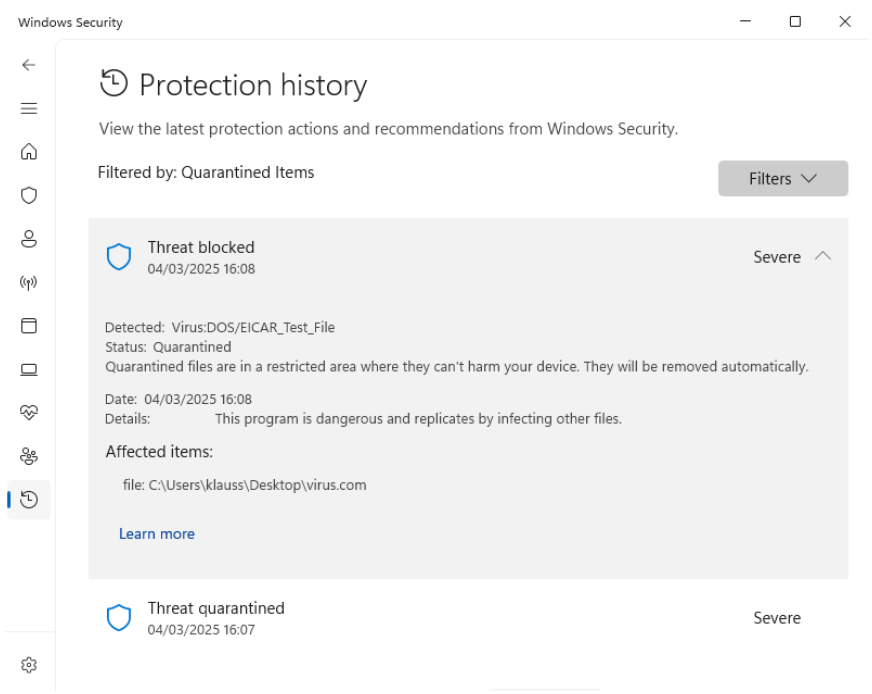
2. Observing Defender Antivirus Response

Answer:

Windows Defender immediately blocked the file, meaning it did not allow the file to be saved because it considered it to contain a virus or unwanted software. Specifically, it displayed a notification that threats were found in the virus.com file. The method most likely used for virus detection is the Dictionary Approach, meaning Defender recognized it as a virus through signature-based detection.



In the protection history for detection logs, we observe that the file has been quarantined, which means Defender does not allow us to run it or affect other files, thus keeping the system safe.



3. Experimenting with File Variations

A)

• You will need to shut down the Virtual Machine by selecting File->Close->Power off the Machine, enabling the Restore Current Snapshot option with the snapshot name, before the next startup.

• Open Notepad.

• Copy and paste the following string (EICAR Test File).

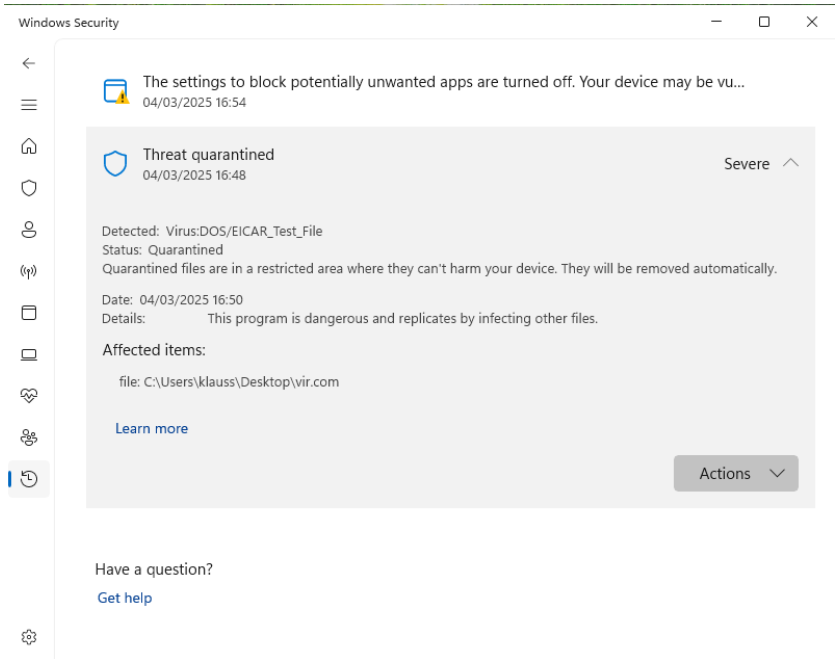
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

• Try renaming the file. Save the file as vir.com (select "All Files" instead of ".txt").

• Try scanning it again.

Answer:

Similarly, Defender immediately blocked the file and placed it in quarantine, meaning that even with a different file name (vir.com instead of virus.com), Defender does the same job. This happens because, as mentioned, Defender recognized it as a virus through signature-based detection and not based on the file name.



B)

• You will need to shut down the Virtual Machine by selecting File->Close->Power off the Machine, enabling the Restore Current Snapshot option with the snapshot name, before the next startup.

• Open Notepad.

• Copy and paste the following string (EICAR Test File).

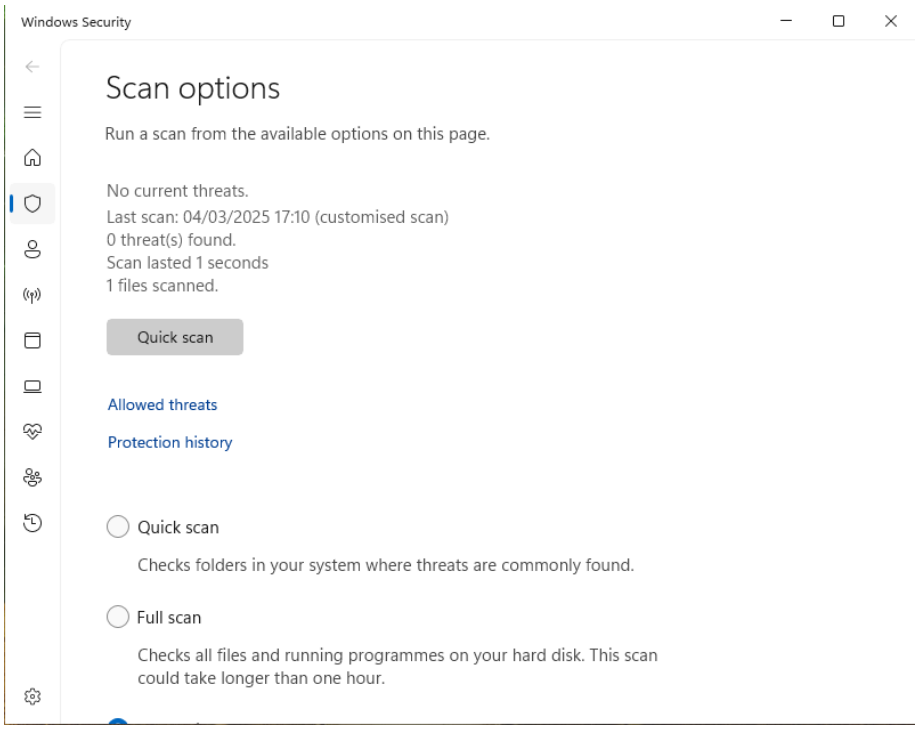
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

• Try changing some letters in the file. Save the file as virus.com (select "All Files" instead of ".txt").

• Try scanning it again.

Answer:

In this case, the file was saved normally. After scanning, we observe that no threats were detected in the system, meaning that the virus.com file does not contain malicious code. This happened because Windows Defender performed signature-based detection. However, due to the modification we made to the file, it failed to recognize it as a virus.



Activity 2: Virus Identification -- Scenario 2

Objective: To determine whether the protection software detects malicious files and, if so, how.

Steps:

1. Creating the Malicious Script

• Open Notepad.

• Copy and paste the following code:

```
# Fake Malicious Script

Set-MpPreference -DisableRealtimeMonitoring $true # Attempt to disable Defender

New-Item -Path "C:\Windows\System32\malware.txt" -ItemType File # Fake system modification

Add-MpPreference -ExclusionPath "C:" # Attempt to exclude all files from Defender's scan

Start-Process notepad.exe # Run a program
```

2. Save the file as: fake_malware.ps1. Make sure the "Save as type" is set to "All Files".

3. Executing the Malicious Script

• Open PowerShell as Administrator. To do this, type "powershell" in the program search in the Start Menu, select PowerShell, right-click, and choose "Run as Administrator".

• Navigate to the folder where the file is saved:

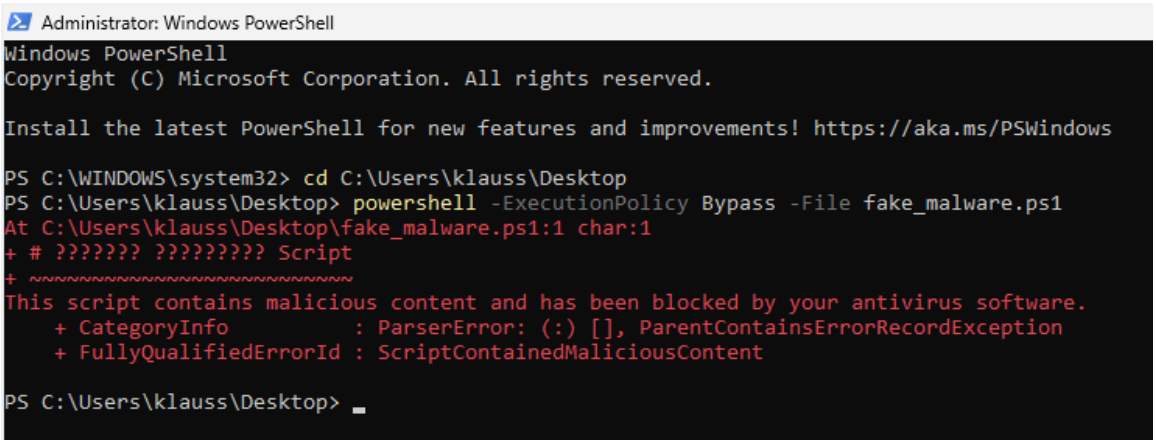
```
cd C:\Users\Public\

Execute the script: powershell -ExecutionPolicy Bypass -File fake_malware.ps1
```

4. **Observing Defender Antivirus Response**

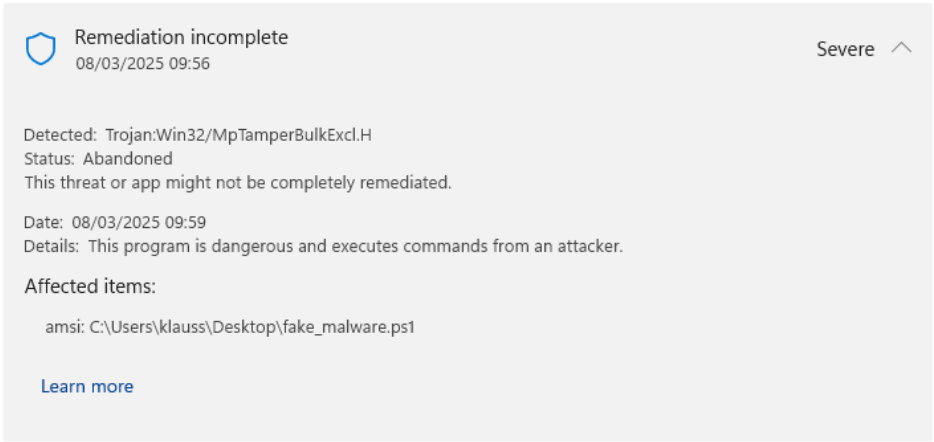
Answer:

First, we create the file and save it, observing that when saving it, no notification from Defender appears. If we execute the file via PowerShell with the command: powershell -ExecutionPolicy Bypass -File fake_malware.ps1, then the following message appears:



The above message says that the file contains malicious content and has been blocked by the antivirus software. The detection method most likely used is Behavior-Based Detection, and this is because when we ran the file, even with -ExecutionPolicy Bypass, it recognized the behavior and blocked it.

If we go to Windows Security > Protection History, we will notice that for this file, it is reported that "This program is dangerous and contains commands from an attacker," meaning that Defender indeed performed behavior-based detection through the file's commands.



Activity 3: Observing Virus Behavior

Objective: Observing virus behavior.

Steps:

1. Preparing the Initial Code of the "Malicious File"

• Create a .bat file with the following code.

```
@echo off
:: Version 1
:: This version will copy itself and create a harmless file
:: Copy the virus to a new location copy %0 C:\Users\Public\virus.bat
:: Write a harmless message to the system folder echo This file was infected by a virus. > C:\Windows\System32\harmless.txt
Exit
```

2. Observing the Behavior

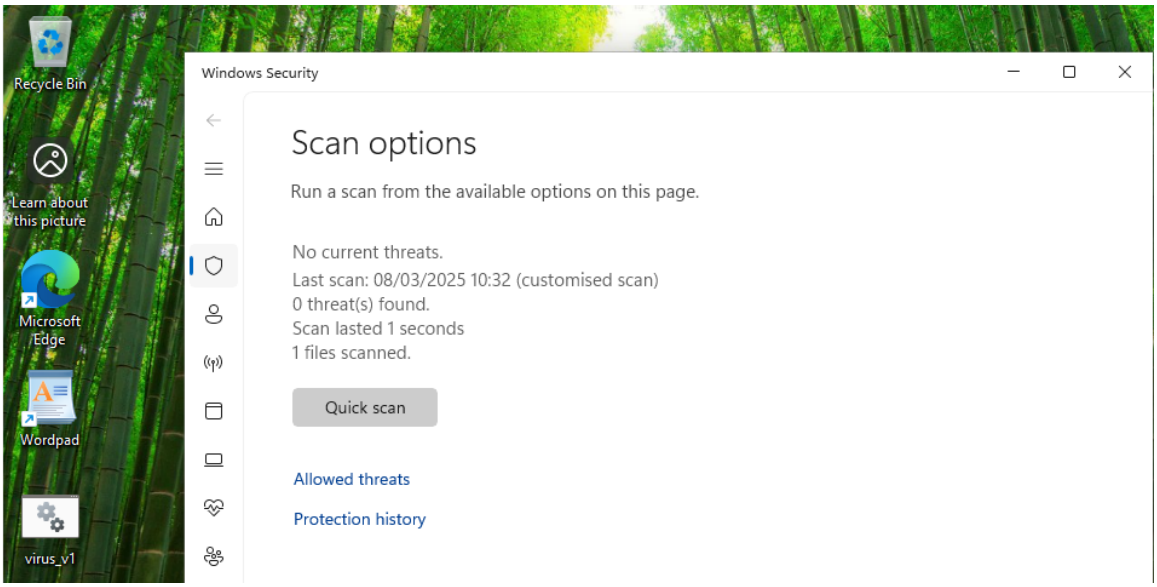
• Save the file as virus_v1.bat on the Desktop or any folder.

• Scan the file with Windows Defender to show that it is not detected as malicious. This is important because it is just a harmless script.

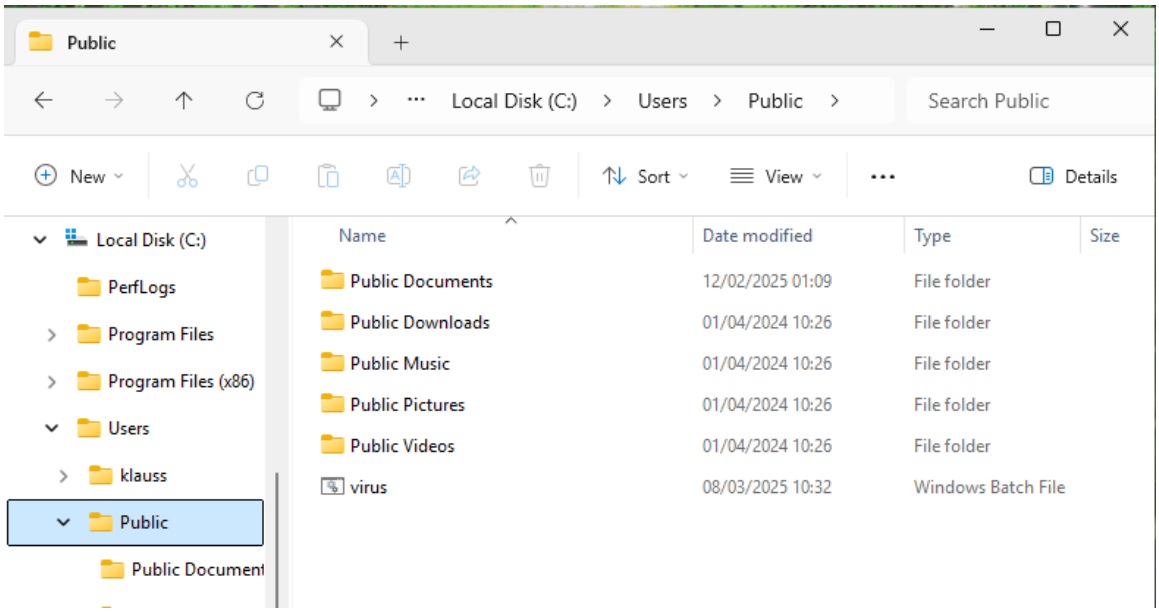
• Execute the file: When virus_v1.bat is executed, it will copy itself to the C:\Users\Public\ folder and write the message to System32\harmless.txt.

Answer:

First, after scanning the file, we observe that the file is not flagged as malicious.



Additionally, after execution, the file was indeed copied to the Public folder.



3. Modifying the "Malicious File"

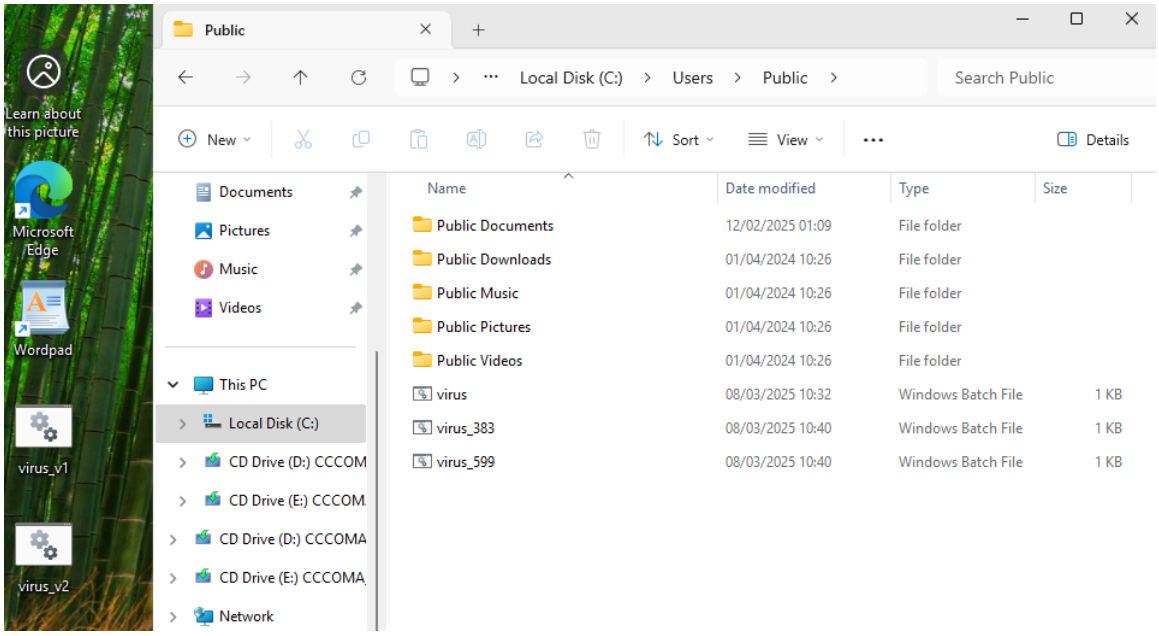
• Modify the behavior using the following code:

```
@echo off
:: Version 2
set /a num=%random%
:: Copy the file
copy %0 C:\Users\Public\virus_%num%.bat
:: Write a harmless message to the same system file (without causing harm)
echo This file was infected by a virus. >C:\Windows\System32\harmless_%num%.txt
exit
```

4. Observing the Behavior

Answer:

If we check the folder (C:\Users\Public), we observe that files with the name virus_(random number) have been created.



The behavior of the above program resembles the operation of a self-replicating virus. It is a basic technique used by viruses to survive and spread across a system or network.

Activity 4: DOS Attack on YouTube Client

• Add the two Kali Linux Virtual Machines to Virtual Box, which you can find at link 1 and link 2.

• The Linux VMs come pre-installed with Mozilla Firefox and netwox, which is a suite of tools for carrying out attacks.

• The IP addresses of the two VMs are 10.0.2.8 and 10.0.2.10.

• The goal of the exercise is to implement a sniff and spoof attack on a client watching a video on YouTube, terminating their connection.

• For both VMs, select the NAT Network option for their network connectivity. This is done by selecting the VM, right-clicking, and then selecting Settings->Network, setting the NAT Network option in the Attached to field.

Steps:

1. Starting VMs

• The username and password for a user with administrator rights on the VMs are kali/kali. Use these to log in to the VMs.

2. Initializing Victim and Attacker

• Open Firefox on the VM with IP 10.0.2.8 (victim) from the toolbar at the top of the screen and connect to YouTube, playing a video.

• On the second VM (10.0.2.10, attacker), open a terminal by selecting terminal emulator from the toolbar at the top of the screen and start the sniff and spoof attack on the first VM.

• To do this, use option 78 (sniff and spoof tool) of netwox, giving the following command:

sudo netwox 78 --filter "src host xxx.xxx.xxx.xxx"

where xxx.xxx.xxx.xxx is the IP address of VM1.

3. Observing the Behavior

Answer:

The general behavior of the client after the attack is that the connection to YouTube will stop, and the user will not be able to continue playing the video. There are also network delays and issues with internet connectivity. If the attack continues, the client may experience a complete loss of connection or inability to refresh the page.