# **CTF Topic: Malware Analysis**

**Introduction**

In this CTF challenge, you'll be conducting a malware analysis to understand the behavior and characteristics of a suspicious executable file. Your goal is to reverse-decode the malware, identify its components, and retrieve specific flags hidden within the code or its activities.

# **Tools and requirements**

* NotPad
* [VirusTotal](https://www.virustotal.com/gui/home/upload)

# **Link**

* Download the suspicious executable file from the provided link: [Sample](https://www.mediafire.com/file/cnq4m5ngu251ohk/Start.bat/file)
* <https://www.mediafire.com/file/cnq4m5ngu251ohk/Start.bat/file>

# **Scenario**

You have been provided with a suspicious executable file that is believed to be malware. Your task is to analyze the file, understand its behavior, and retrieve specific flags hidden within the malware. This process will involve static and dynamic analysis techniques.

# **Process to Perform**

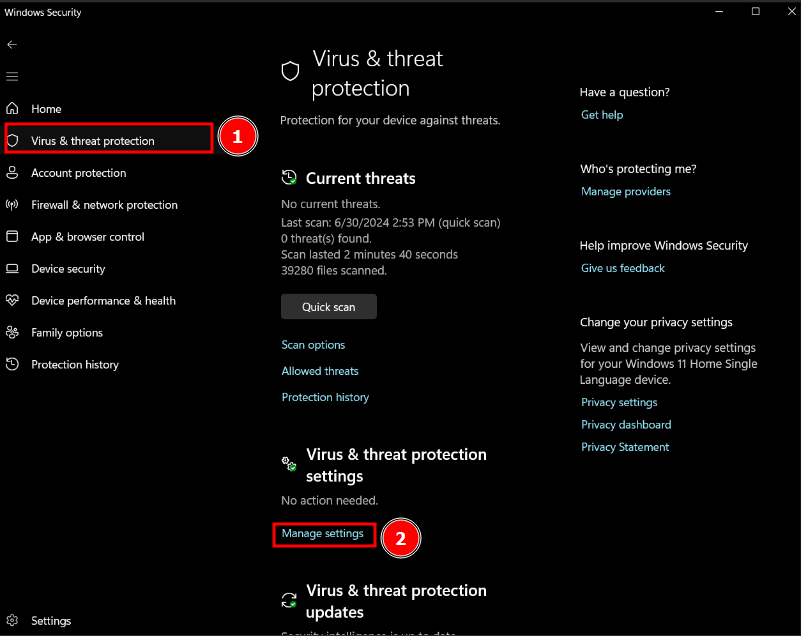
1. Go to the Link\_1 and download the file.
2. Edit the file in the notepad and capture the flag.
3. Check the malicious file details to capture the more flag by scanning on virus total given on the Link\_2.

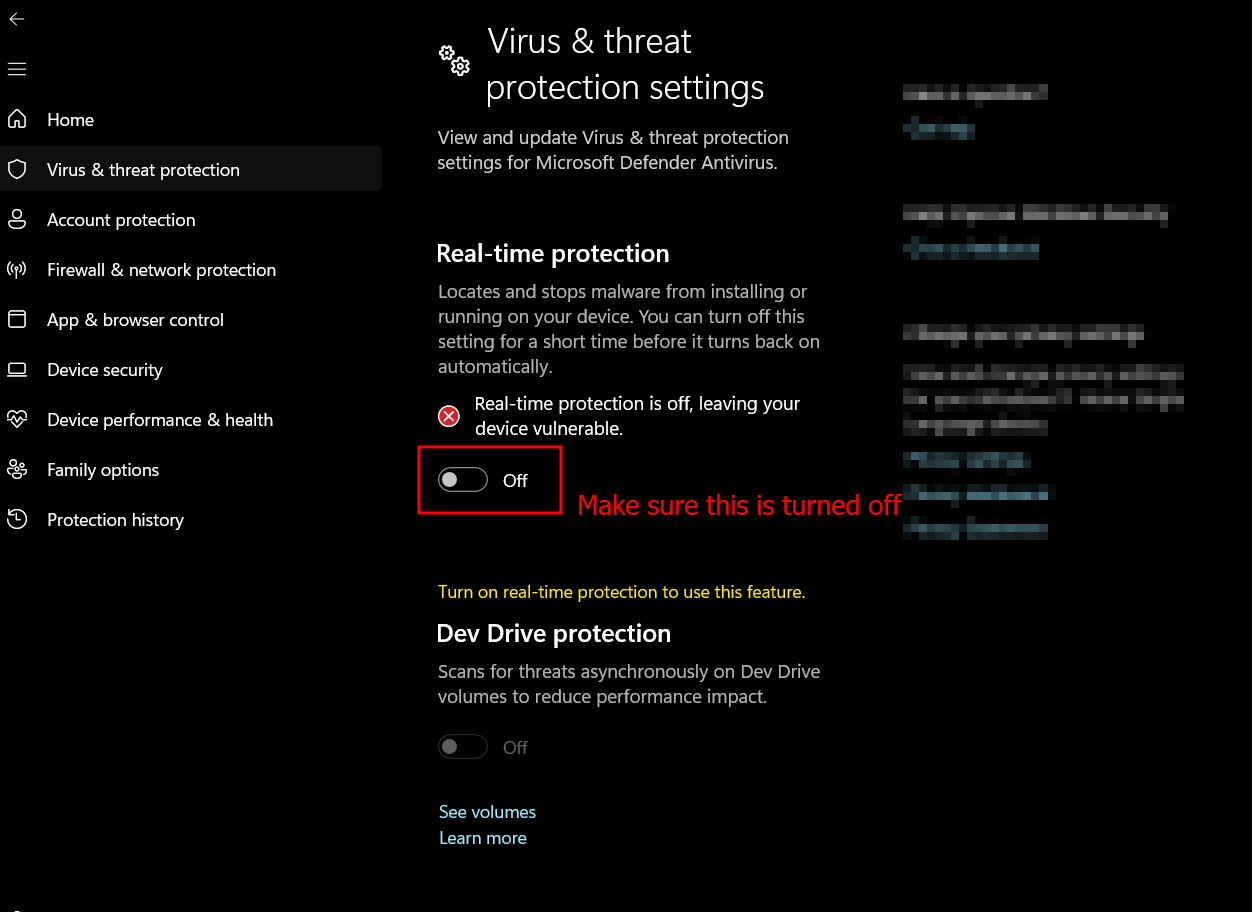
Link\_1: <https://www.mediafire.com/file/cnq4m5ngu251ohk/Start.bat/file>

Link\_2: <https://www.virustotal.com/gui/home/upload>

***In case your system does not allow you to download the corrupt file make sure you turn off the Window virus & threat protection.***

***Search for Windows Security > VIrus & threat protection > Manage settings > Real-Time protection (make sure this is turned off)***

****

****

# **Let’s start the Challenge**

# **Question**

Flag1: What is the flag you got after decoding the file?

Answer: ING{Skill\_Academy.flag}

Flag Captured

Flag 2: How many viruses were detected by the virus Total software?

Answer: 7

Flag Captured

Flag3: What is the SHA-256 value of that malicious File?

Answer: e6d078b426676d52deb9965cf0b6a3b9bb6102271c61f9051801ce684a2a04e1

Flag Captured

# **Hint**

