The Suspicious Chocolate.exe

Overview

Room URL: https://tryhackme.com/room/adventofcyberpreptrack

Difficulty: Easy

Category: Prep

Date Completed: 12/1/2025

Objectives

Determine if `chocolate.exe` is safe or infected.

Table of Contents

Introduction

A suspicious USB labeled "SOCMAS Party Playlist" containing `chocolate.exe` arrives on your desk. You must use a simulated VirusTotal tool to scan the file and determine if it's safe or malicious—a critical skill for identifying threats before they compromise systems.

Walk Through

1. Click the view site button on THM
    1. This brings up a simulated virustotal website preloaded with `chocolate.exe`

2. Clicking scan to scan the `.exe` file on virtustotal
3. After clicking scan, the website scans the file and loads the results
    1. The website loaded results from 48 vendors
        1. Clean Vendor A
        2. Clean Vendor B
        3. Malhare Labs
        4. +45 other vendors marked this file as clean
    2. Malhare labs is classified as `MalhareTorjan` with `ref:ML-2025-011
4. This file is not free from viruses. suspiciouschocolate.png

---

Lessons Learned

In this activity, I learned how to use VirusTotal to scan files for viruses and identify malicious threats across multiple security vendors.

Resources

TryHackMe

Virus Total

Revision #5
Created 2025-12-01 16:25:31 UTC by David Rizzo
Updated 2025-12-01 17:18:31 UTC by David Rizzo