

TDX ARENA

Certification Report

Araseli Serrano

Final Assessment Report Submission

Case: One of Us

12.18.2024

Executive Summary

A cyber rese

Findings and Analysis

Finding	Finding Details	Description
User	Bruce	The name of the end user is Bruce.
Process	ClamAV scan	The file was identified malicious by ClamAV
File Attribute	Size: 223.19 KB	MimeType: application/x-ms-dos-executable
Hash	f48a8687e91fd9ef 98cd1b7aaeeb2a4 c	The MD5 of the malicious executable file.
Malicious File	file176.exe	A probable malicious file with the potential to exploit vulnerabilities of the system, have access to sensitive data, and install additional malware. This malicious file seems to be bundled into the files by an attacker.

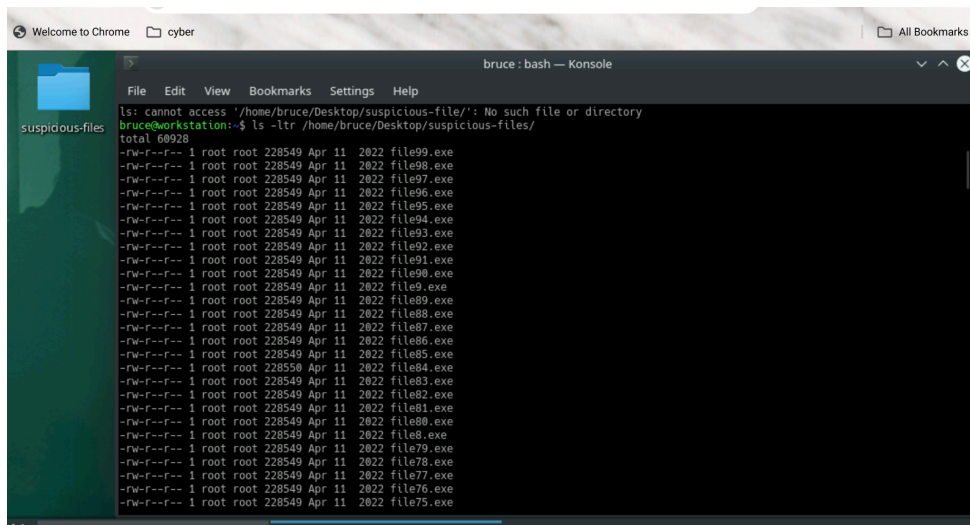
Methodology

Tools and Technologies Used

- **ls:** ls listed all the files that were in the folder 'suspicious-files'
- **find . -type f -exec file {} \;** - This was used to identify all executable files in the folder.
- **file:** File command was used to determine the type of files were in the folder to find the one that was malicious.

Investigation Process

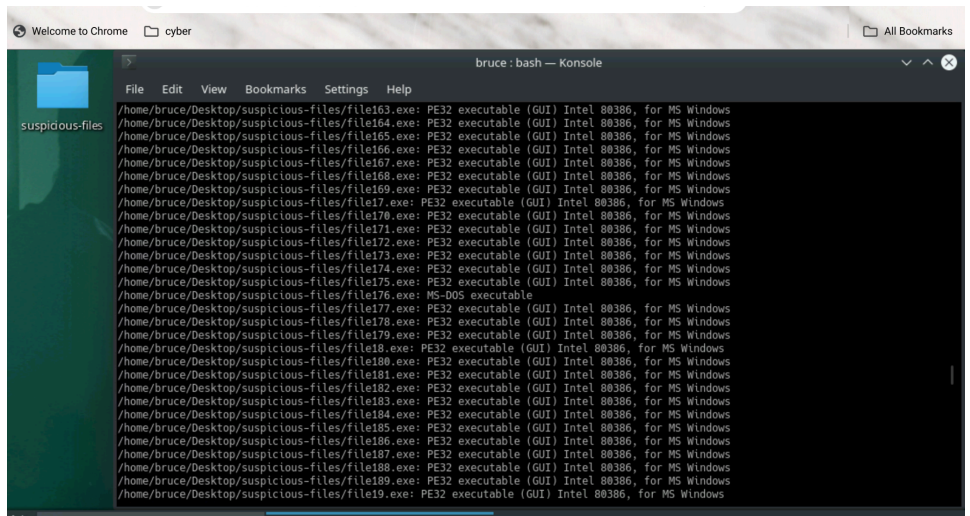
1. I started by listing all the files that were in the folder.



A screenshot of a terminal window titled "bruce : bash — Konsole". The terminal shows the command `ls: cannot access '/home/bruce/Desktop/suspicious-file/': No such file or directory` and then `bruce@workstation:~$ ls -ltr /home/bruce/Desktop/suspicious-files/`. The output lists 20 files in the directory `/home/bruce/Desktop/suspicious-files/`, all with permissions `-rw-r--r--`, owned by `root`, and dated `Apr 11 2022`. The files are `file99.exe` through `file75.exe`.

```
ls: cannot access '/home/bruce/Desktop/suspicious-file/': No such file or directory
bruce@workstation:~$ ls -ltr /home/bruce/Desktop/suspicious-files/
total 60928
-rw-r--r-- 1 root root 228549 Apr 11 2022 file99.exe
-rw-r--r-- 1 root root 228549 Apr 11 2022 file98.exe
-rw-r--r-- 1 root root 228549 Apr 11 2022 file97.exe
-rw-r--r-- 1 root root 228549 Apr 11 2022 file96.exe
-rw-r--r-- 1 root root 228549 Apr 11 2022 file95.exe
-rw-r--r-- 1 root root 228549 Apr 11 2022 file94.exe
-rw-r--r-- 1 root root 228549 Apr 11 2022 file93.exe
-rw-r--r-- 1 root root 228549 Apr 11 2022 file92.exe
-rw-r--r-- 1 root root 228549 Apr 11 2022 file91.exe
-rw-r--r-- 1 root root 228549 Apr 11 2022 file90.exe
-rw-r--r-- 1 root root 228549 Apr 11 2022 file89.exe
-rw-r--r-- 1 root root 228549 Apr 11 2022 file88.exe
-rw-r--r-- 1 root root 228549 Apr 11 2022 file87.exe
-rw-r--r-- 1 root root 228549 Apr 11 2022 file86.exe
-rw-r--r-- 1 root root 228549 Apr 11 2022 file85.exe
-rw-r--r-- 1 root root 228550 Apr 11 2022 file84.exe
-rw-r--r-- 1 root root 228549 Apr 11 2022 file83.exe
-rw-r--r-- 1 root root 228549 Apr 11 2022 file82.exe
-rw-r--r-- 1 root root 228549 Apr 11 2022 file81.exe
-rw-r--r-- 1 root root 228549 Apr 11 2022 file80.exe
-rw-r--r-- 1 root root 228549 Apr 11 2022 file79.exe
-rw-r--r-- 1 root root 228549 Apr 11 2022 file78.exe
-rw-r--r-- 1 root root 228549 Apr 11 2022 file77.exe
-rw-r--r-- 1 root root 228549 Apr 11 2022 file76.exe
-rw-r--r-- 1 root root 228549 Apr 11 2022 file75.exe
```

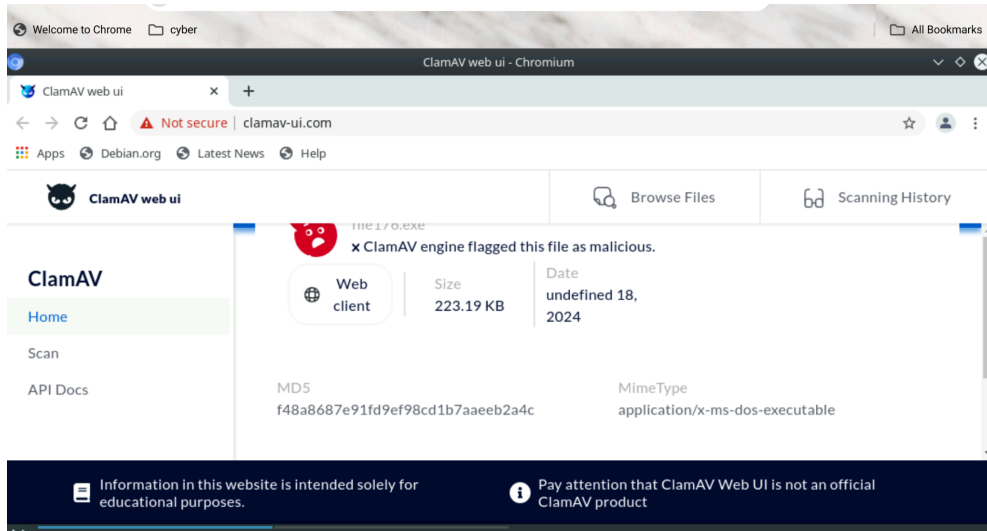
2. Next, I check the data and file type for each file in the folder. I found one that was very different from the others.



A screenshot of a terminal window titled "bruce : bash — Konsole". The terminal shows the command `file` being run on each file in the directory `/home/bruce/Desktop/suspicious-files/`. The output shows that most files are `PE32 executable (GUI) Intel 80386, for MS Windows`, but `file176.exe` is `MS-DOS executable`.

```
/home/bruce/Desktop/suspicious-files/file163.exe: PE32 executable (GUI) Intel 80386, for MS Windows
/home/bruce/Desktop/suspicious-files/file164.exe: PE32 executable (GUI) Intel 80386, for MS Windows
/home/bruce/Desktop/suspicious-files/file165.exe: PE32 executable (GUI) Intel 80386, for MS Windows
/home/bruce/Desktop/suspicious-files/file166.exe: PE32 executable (GUI) Intel 80386, for MS Windows
/home/bruce/Desktop/suspicious-files/file167.exe: PE32 executable (GUI) Intel 80386, for MS Windows
/home/bruce/Desktop/suspicious-files/file168.exe: PE32 executable (GUI) Intel 80386, for MS Windows
/home/bruce/Desktop/suspicious-files/file169.exe: PE32 executable (GUI) Intel 80386, for MS Windows
/home/bruce/Desktop/suspicious-files/file17.exe: PE32 executable (GUI) Intel 80386, for MS Windows
/home/bruce/Desktop/suspicious-files/file170.exe: PE32 executable (GUI) Intel 80386, for MS Windows
/home/bruce/Desktop/suspicious-files/file171.exe: PE32 executable (GUI) Intel 80386, for MS Windows
/home/bruce/Desktop/suspicious-files/file172.exe: PE32 executable (GUI) Intel 80386, for MS Windows
/home/bruce/Desktop/suspicious-files/file173.exe: PE32 executable (GUI) Intel 80386, for MS Windows
/home/bruce/Desktop/suspicious-files/file174.exe: PE32 executable (GUI) Intel 80386, for MS Windows
/home/bruce/Desktop/suspicious-files/file175.exe: PE32 executable (GUI) Intel 80386, for MS Windows
/home/bruce/Desktop/suspicious-files/file176.exe: MS-DOS executable
/home/bruce/Desktop/suspicious-files/file177.exe: PE32 executable (GUI) Intel 80386, for MS Windows
/home/bruce/Desktop/suspicious-files/file178.exe: PE32 executable (GUI) Intel 80386, for MS Windows
/home/bruce/Desktop/suspicious-files/file179.exe: PE32 executable (GUI) Intel 80386, for MS Windows
/home/bruce/Desktop/suspicious-files/file18.exe: PE32 executable (GUI) Intel 80386, for MS Windows
/home/bruce/Desktop/suspicious-files/file180.exe: PE32 executable (GUI) Intel 80386, for MS Windows
/home/bruce/Desktop/suspicious-files/file181.exe: PE32 executable (GUI) Intel 80386, for MS Windows
/home/bruce/Desktop/suspicious-files/file182.exe: PE32 executable (GUI) Intel 80386, for MS Windows
/home/bruce/Desktop/suspicious-files/file183.exe: PE32 executable (GUI) Intel 80386, for MS Windows
/home/bruce/Desktop/suspicious-files/file184.exe: PE32 executable (GUI) Intel 80386, for MS Windows
/home/bruce/Desktop/suspicious-files/file185.exe: PE32 executable (GUI) Intel 80386, for MS Windows
/home/bruce/Desktop/suspicious-files/file186.exe: PE32 executable (GUI) Intel 80386, for MS Windows
/home/bruce/Desktop/suspicious-files/file187.exe: PE32 executable (GUI) Intel 80386, for MS Windows
/home/bruce/Desktop/suspicious-files/file188.exe: PE32 executable (GUI) Intel 80386, for MS Windows
/home/bruce/Desktop/suspicious-files/file189.exe: PE32 executable (GUI) Intel 80386, for MS Windows
/home/bruce/Desktop/suspicious-files/file19.exe: PE32 executable (GUI) Intel 80386, for MS Windows
```

3. I decided to scan that particular file onto ClamAV and was identified as malicious.



Recommendations

Based on the findings, it is recommended to:

1. Implement regular scanning and monitoring of files to identify any discrepancies.
2. Continue educating or conducting regular training to inform users the importance of verifying files.
3. Keep antivirus software up to date and find ways to enhance ClamAV detection rates.

Methodology

The investigation involved a systematic approach to analyze and solve the Thrive DX challenge. This methodology ensured comprehensive exploration of the provided data and facilitated the identification of key insights. The steps undertaken include:

1. **Data Extraction:**
 - Examined the provided virtual memory file (**emperor.vmem**) for potential evidence using extraction and string analysis tools.
 - Utilized Visual Studio Code to parse through data segments and locate relevant information within the file.
2. **Password Analysis:**
 - Analyzed file contents for potential passwords or encrypted files.
 - Leveraged password-cracking tools to attempt decryption when necessary.
3. **Artifact Identification:**
 - Identified key artifacts, such as the **gift.7z** archive, and analyzed its contents using the extracted strings and any accompanying metadata.

Tools and Technologies Used

1. Strings Command

- **Purpose:** Extracted readable text strings from binary files to identify potential hints, passwords, or filenames.
- **Reason for Use:** The `strings` command is highly effective in processing large binary files and extracting human-readable content quickly.

2. Visual Studio Code

- **Purpose:** Used to analyze extracted data and manually inspect files for relevant details.
- **Reason for Use:** Visual Studio Code offers robust search functionality, syntax highlighting, and an organized interface to navigate large datasets effectively.

3. 7-Zip Command Line Tool

- **Purpose:** Attempted to extract the contents of the `gift.7z` archive with and without known passwords.
- **Reason for Use:** The 7-Zip utility supports strong encryption formats and is essential for working with `.7z` archives.

4. John the Ripper

- **Purpose:** Performed brute-force password cracking on encrypted files, leveraging known hash values.
- **Reason for Use:** John the Ripper is a powerful, open-source password-cracking tool capable of handling various encryption schemes.

5. Ubuntu Command Line Environment

- **Purpose:** Used for executing tools, scripting, and interacting with files within the provided virtual environment.
- **Reason for Use:** Ubuntu provides a versatile command-line environment suitable for forensic and investigative workflows.

By combining these tools and methodologies, a comprehensive analysis of the challenge was achieved, enabling us to uncover and document critical findings.
