

TDX ARENA

Certification Report

Brett Reich

Final Assessment Report Submission

Case: One of Us

6/3/24

Executive Summary

The client's computer still had malicious files on their machine. After going through the suspicious files one of them was able to be identified through the ClamAV web-based anti-virus as evidence of leftover malicious software after the initial detection and deletion. There was an attempt at building a script to allow all the files to be uploaded at once to the anti-virus. However, it didn't work as intended, so for efficiency's sake the files were all uploaded individually. The culprit was found in file176.exe, which means that the first attempt at fortifying the system was not fully successful.

At this point, the client's machine needs to be disconnected from the rest of the network. Either a restore or wipe and install would probably be the best approach to mitigate any more potential damage to the company. An intense scanning of the rest of the network and tracing of how the initial malware was introduced would also need to be conducted to protect the system.

Findings and Analysis

One malicious exe file still found on bruce workstation.

Finding	Finding Details	Description
file176.exe	Malicious File	A malicious file found through a scan on ClamAV web browser.

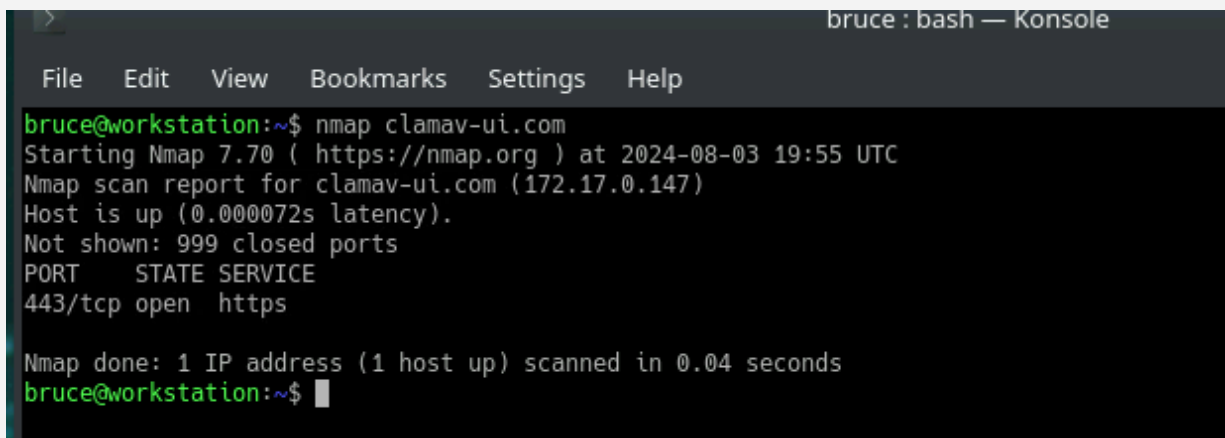
Methodology

Tools and Technologies Used

- **Linux CLI:** Created a sh file to execute multiple uploads into the web-based ClamAV anti-virus.
- **Nmap:** To scan the ClamAV website to determine if HTTPS was the only way to upload all files at risk.

Investigation Process

1. I started by running nmap to see if there were any other open ports just as a base to see the best option to upload the files, potentially through FTP.

A screenshot of a terminal window titled "bruce : bash — Konsole". The terminal shows the output of an nmap scan. The user enters the command "nmap clamav-ui.com". The output indicates that the host is up and that port 443/tcp is open and serving https. The terminal text is as follows:

```
bruce@workstation:~$ nmap clamav-ui.com
Starting Nmap 7.70 ( https://nmap.org ) at 2024-08-03 19:55 UTC
Nmap scan report for clamav-ui.com (172.17.0.147)
Host is up (0.000072s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
443/tcp   open  https
Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
bruce@workstation:~$
```

2. Next, I attempted to produce an "sh" file with a script that would automatically upload the entire contents of the suspicious-files folder to ClamAV's website.

```
bruce: bash — Konsole
File Edit View Bookmarks Settings Help
GNU nano 3.2 upload_files.sh

#!/bin/bash

# Configuration
AUTH_URL="https://{clamav-ui.com}/api/v1/auth"
SCAN_URL="https://{clamav-ui.com}/api/v1/scan"
DIRECTORY="bruce@workstation/Desktop/upload_files.sh"

# Function to generate token
generate_token() {
    echo "Generating authentication token..."
    TOKEN=$(curl -s $AUTH_URL)
    if [[ $TOKEN == *"Unauthorized"* ]]; then
        echo "Authentication failed"
        exit 1
    fi
    echo "Token generated: $TOKEN"
}

# Function to upload a single file
upload_file() {
    local file_path="$1"
    echo "Uploading $file_path..."

    response=$(curl -s -w "\nHTTP_STATUS_CODE:%{http_code}" -X POST "$SCAN_URL" \
        -H "Authorization: $TOKEN" \
        -H "Content-Type: multipart/form-data" \
        -F "fileinput=@${file_path}")

    http_status=$(echo "$response" | grep "HTTP_STATUS_CODE" | awk -F':' '{print $2}')
    result=$(echo "$response" | sed -e 's/HTTP_STATUS_CODE:.*//g')

    if [ "$http_status" -eq 200 ]; then
        echo "Scan result for $(basename "$file_path"): $result"
    else
        echo "Failed to upload $(basename "$file_path"): $result"
    fi
}
```

```
fi
}

# Function to scan all files in the directory
scan_directory() {
    for file in "$DIRECTORY"/*; do
        if [ -f "$file" ]; then
            upload_file "$file"
        fi
    done
}

# Main execution
generate_token
scan_directory
```

3. This did not end up working, so for efficiency I was able to individually upload each file to the website and found one malicious file still on the machine.
4. File176.exe file in suspicious-files folder was found to be malicious.


ClamAV web ui


← → ↻ 🏠


⚠ Not secure | clamav-ui.com

☆ 👤 ⋮

🌐 Apps 🌐 Debian.org 🌐 Latest News 🌐 Help

 **ClamAV web ui**

 Browse Files

 Scanning History


ClamAV


Home

Scan

API Docs

Scan log

 file176.exe
x ClamAV engine flagged this file as malicious.

 Web client

Size
223.19 KB

Date
Sep 2, 2024

MD5

f48a8687e91fd9ef98cd1b7aaeeb2a4c

MimeType

application/x-ms-dos-executable

Scan another

Recommendations

1. Update the AV that is currently being used on the client's machines.
2. Add the malicious file signature to the AV.
3. Ensure bruce workstation is completely restored or wiped and reinstalled.
4. Ensure the rest of the client's network is protected from lateral movement from attackers from bruce workstation.

Appendix A

File-related Findings	
Malicious File	/home/Bruce/desktop/suspicious-files/file176.exe
Hash	f48a8687e91fd9ef98cd1b7aaeeb2a4c
File Attribute	223.2 KiB (228,549) Monday, 11 April 2022 09:49:42 UTC
Endpoint-related Findings	
Host	bruce@workstation
User	bruce