



TDX ARENA

Certification Report

Case: One of Us

8/2/2024

Executive Summary

I began a new job as a threat hunter in Sea-Snail Security. During a routine IR day at my client's office, I discovered a malicious connection to my client's computer. After detecting and deleting malicious files, the client still complained about odd behavior from an employee computer. Upon further inspection, additional files were created when the original malware was executed which were not recognized by anti-virus software as malicious.

A folder was created on the Desktop of a Linux based machine containing the 272 suspicious files. Going through the files one by one would be a daunting task which would consume a significant amount of time, making automation of significant importance. Using the Linux Konsole, I was able to obtain an api token from clamav-ui.com and utilized that in a bash script created to run with clamav-ui.com to scan all the suspicious files in the directory.

The bash script ran all the suspicious files through clamav-ui.com, and created a log file containing data on all the files in the directory. After using keywords to search the large document, I was able to find (1) additional malicious file.

Findings and Analysis

Finding	Finding Details	Description
Malicious File	file176.exe	Backdoor Trojan

This file appears to be a trojan installed by an attacker through a back door which was more than likely accessed through a malicious attachment or link in a phishing email.

Finding	Finding Details	Description
Phishing	Social engineering attack	A cyber attack where an attacker impersonates a trustworthy entity to deceive individuals into providing sensitive information, such as login credentials or financial details.
More than likely how the malicious files came to be on the device. Though a fraudulent email or message, someone may have downloaded a file or clicked a link that gave a nefarious individual access to their device.		
Finding	Finding Details	Description
Hash	Md5 of malicious file	Unique fixed-size string of numbers generated from input data.
This hash helped determine the nature of the malicious file through the use of virustotal.com.		
Finding	Finding Details	Description
API Key	Authentication Token	Used as a unique identifier to authenticate a client when making API request to a server.
Utilized the API Key to communicate with clamav-ui.com to automate a scan of multiple files though the web service instead of one at a time.		

Methodology

Tools and Technologies Used

Clamav-ui.com: Open-source web-based antivirus tool that allowed us to scan multiple files utilizing it's API.

ChatGPT: Open source artificial intelligence tool that can help with scripting and coding.

Bash Scripting: The process of writing scripts in the Bash (Bourne Again Shell) language to automate tasks in Unix-like operating systems.

Virustotal.com: An online service that analyzes files and URLs to detect malware and other types of malicious content. It aggregates results from various antivirus engines and tools to provide a comprehensive assessment of the submitted items.

Investigation Process

- 1) Upon opening the machine, we could see a directory on our desktop named "suspicious-files." Knowing that somewhere in that directory is a persistent malicious file. A web browser was also opened to clamav-ui.com giving me a hint I needed to use this to scan the files in the directory.
- 2) After reading the clamav-ui.com API docs page, I used curl command in Linux Konsole to get an API key for clamav-ui.com as it was necessary in order to automate a mass scan of the files in /home/bruce/Desktop/suspicious-files.

```
bruce@workstation:~$ curl https://clamav-ui.com/api/v1/auth -k
{"status":"success","data":{"token":"eyJhbGciOiJIUzUxMiIsInR5cCI6IkpXVCJ9.eyJpcCI6IjE3Mi4xNy4wLjkwIiwiaG9zdG5hbWUiOiJjbGFTYXZtdWkuY29tIiwiaWF0IjoxNzIyNDc5NjEzLCJleHAiOiE3MjI0ODMyMTMsImZcyI6IHNsYW1BViJ9.pJ41XPTFYp8DQZKzbfSvwYUr0PF4xGBDrAvT3WYqLJ-9ckkkqyvLydWwMBaA36WlOM6GMKhLuo3B8Pct1rgNQ"}}bruce@workstation:~$ ^C
```

- 3) After obtaining the API key, I was able to utilize ChatGPT to help me generate a bash script to run. I created a bash file on the desktop and saved my script there with updated fields for the API key, directory, logfile and the API URL. I wanted the script to output a log file to examine the data provided from clamav-ui.com.

```
#!/bin/bash

# Configuration
API_KEY="eyJhbGciOiJIUzUxMiIsInR5cCI6IkpXVCJ9.eyJpcCI6IjE3Mi4xNy4wLjkwIiwiaG9zdG5hbWUiOiJjbGFTYXZtdWkuY29tIiwiaWF0IjoxNzIyNDc5NjEzLCJleHAiOiE3MjI0ODMyMTMsImZcyI6IHNsYW1BViJ9.pJ41XPTFYp8DQZKzbfSvwYUr0PF4xGBDrAvT3WYqLJ-9ckkkqyvLydWwMBaA36WlOM6GMKhLuo3B8Pct1rgNQ" # Replace with your ClamAV API key
SCAN_DIR="/home/bruce/Desktop/suspicious-files"
LOG_FILE="/home/bruce/Desktop/scan_results.log"
API_URL="https://clamav-ui.com/api/v1/scan" # Replace with the correct API URL if different

# Function to scan a file
scan_file() {
    local file=$1
    local response

    echo "Scanning $file..."

    # Perform the scan
    response=$(curl -s -k -X POST "$API_URL" \
        -H "Authorization: Bearer $API_KEY" \
        -F "file=@$file")

    # Extract result
    echo "$response" >> "$LOG_FILE"
}

# Ensure log file is empty before starting
echo "Scan Report - $(date)" > "$LOG_FILE"

# Scan each file in the directory
for file in "$SCAN_DIR"/*; do
    if [ -f "$file" ]; then
        scan_file "$file"
    fi
done

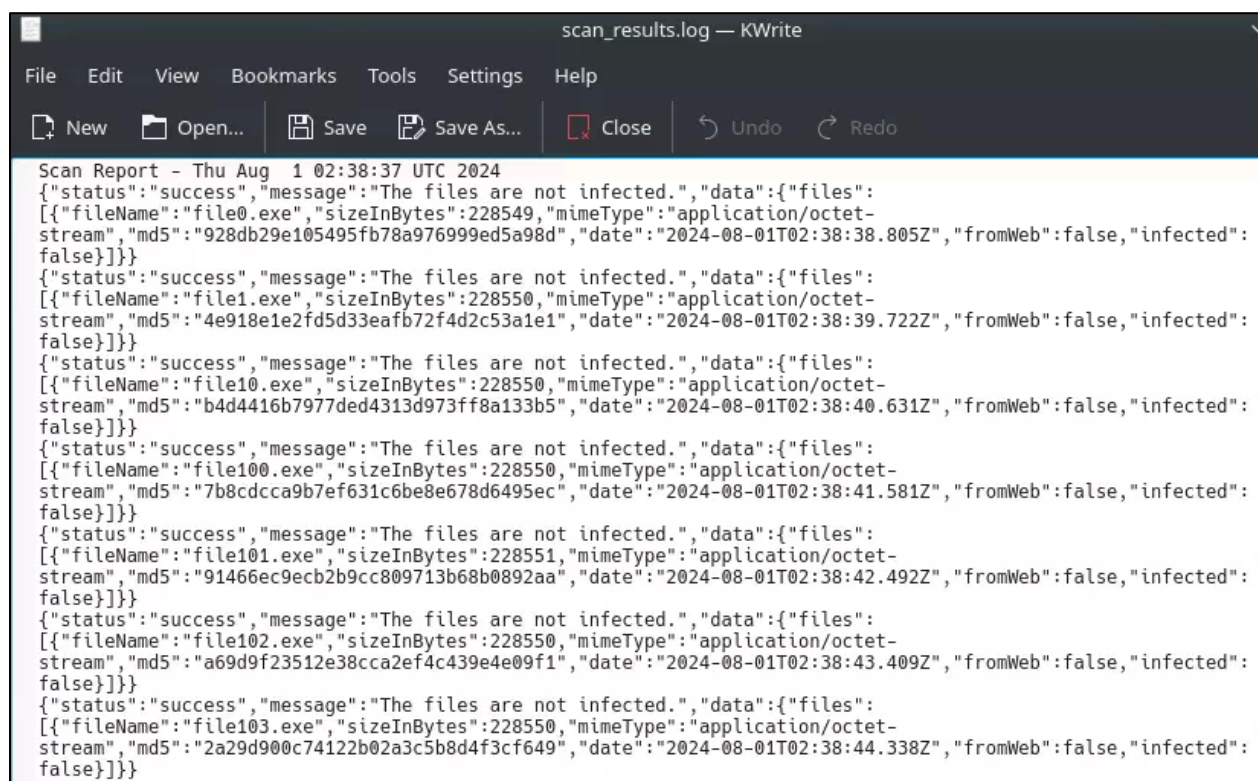
echo "Scan complete. Results have been saved to $LOG_FILE."
```

```

bruce@workstation:~/Desktop$ ./scanfiles.sh
Scanning /home/bruce/Desktop/suspicious-files/file0.exe...
Scanning /home/bruce/Desktop/suspicious-files/file1.exe...
Scanning /home/bruce/Desktop/suspicious-files/file10.exe...
Scanning /home/bruce/Desktop/suspicious-files/file100.exe...
Scanning /home/bruce/Desktop/suspicious-files/file101.exe...
Scanning /home/bruce/Desktop/suspicious-files/file102.exe...
Scanning /home/bruce/Desktop/suspicious-files/file103.exe...
Scanning /home/bruce/Desktop/suspicious-files/file104.exe...
Scanning /home/bruce/Desktop/suspicious-files/file105.exe...
Scanning /home/bruce/Desktop/suspicious-files/file106.exe...
Scanning /home/bruce/Desktop/suspicious-files/file107.exe...
Scanning /home/bruce/Desktop/suspicious-files/file108.exe...
Scanning /home/bruce/Desktop/suspicious-files/file109.exe...
Scanning /home/bruce/Desktop/suspicious-files/file11.exe...

```

- 4) After running the script, it took a few minutes for a full report to process, and the log file had a lot of information regarding the scan of the files.



```

scan_results.log — KWrite
File Edit View Bookmarks Tools Settings Help
New Open... Save Save As... Close Undo Redo

Scan Report - Thu Aug 1 02:38:37 UTC 2024
{"status":"success","message":"The files are not infected.,"data":{"files":
[{"fileName":"file0.exe","sizeInBytes":228549,"mimeType":"application/octet-
stream","md5":"928db29e105495fb78a976999ed5a98d","date":"2024-08-01T02:38:38.805Z","fromWeb":false,"infected":
false}]}}
{"status":"success","message":"The files are not infected.,"data":{"files":
[{"fileName":"file1.exe","sizeInBytes":228550,"mimeType":"application/octet-
stream","md5":"4e918e1e2fd5d33eafb72f4d2c53a1e1","date":"2024-08-01T02:38:39.722Z","fromWeb":false,"infected":
false}]}}
{"status":"success","message":"The files are not infected.,"data":{"files":
[{"fileName":"file10.exe","sizeInBytes":228550,"mimeType":"application/octet-
stream","md5":"b4d4416b7977ded4313d973ff8a133b5","date":"2024-08-01T02:38:40.631Z","fromWeb":false,"infected":
false}]}}
{"status":"success","message":"The files are not infected.,"data":{"files":
[{"fileName":"file100.exe","sizeInBytes":228550,"mimeType":"application/octet-
stream","md5":"7b8cdcca9b7ef631c6be8e678d6495ec","date":"2024-08-01T02:38:41.581Z","fromWeb":false,"infected":
false}]}}
{"status":"success","message":"The files are not infected.,"data":{"files":
[{"fileName":"file101.exe","sizeInBytes":228551,"mimeType":"application/octet-
stream","md5":"91466ec9ecb2b9cc809713b68b0892aa","date":"2024-08-01T02:38:42.492Z","fromWeb":false,"infected":
false}]}}
{"status":"success","message":"The files are not infected.,"data":{"files":
[{"fileName":"file102.exe","sizeInBytes":228550,"mimeType":"application/octet-
stream","md5":"a69d9f23512e38cca2ef4c439e4e09f1","date":"2024-08-01T02:38:43.409Z","fromWeb":false,"infected":
false}]}}
{"status":"success","message":"The files are not infected.,"data":{"files":
[{"fileName":"file103.exe","sizeInBytes":228550,"mimeType":"application/octet-
stream","md5":"2a29d900c74122b02a3c5b8d4f3cf649","date":"2024-08-01T02:38:44.338Z","fromWeb":false,"infected":
false}]}}

```


Based on the information in the file, we could see toward the end of each file, an indicator of “false” next to “infected”, and this lead me to search for “true” providing me with the infected file, and it’s md5 hash.

```

{"status":"success","message":"The files are infected.,"data":{"infectedFiles":["file176.exe"],"files":
[{"fileName":"file176.exe","sizeInBytes":228550,"mimeType":"application/octet-
stream","md5":"f48a8687e91fd9ef98cd1b7aaeeb2a4c","date":"2024-08-01T02:39:58.143Z","fromWeb":false,"infected":
true}]}}

```

- 5) I ran md5 hash f48a8687e91fd9ef98cd1b7aaeeb2a4c through virustotal to see it was a backdoor trojan.



SUMMARY
DETECTION
DETAILS
RELATIONS
COMMUNITY 1

Join our **Community** and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks**.

Popular threat label
trojan.shikataganai

Threat categories
trojan

Family labels
shikataganai

Security vendors' analysis ⓘ
Do you want to automate checks?

AliCloud	Backdoor:Win/meterpreter.A
Avast	Win32:ShikataGaNai-A [Trj]
AVG	Win32:ShikataGaNai-A [Trj]
Bkav Pro	W32.Common.A122632F
ClamAV	Win.Trojan.MSShellcode-6360728-0
Fortinet	W32/Swrort.Cltr
GData	DOS.Trojan.Agent.Y5U7QM
Google	Detected
MaxSecure	Trojan.Malware.121218.susgen
Avira (Static ML)	Undetected

Recommendations

Based on the findings, my recommendations to mitigate the identified risks, secure the systems, and prevent future incidents include:

- 1) Update Antivirus software regularly.
- 2) Add malicious file signature to current AV.
- 3) Employee cybersecurity training/refresher.