Student Name: Chelsea Lyn McEachran

Final Assessment Report Submission

Case: One of Us - Secondary Malware Detection and Analysis

Date: 7/30/2025

Executive Summary

This report details an investigation conducted in response to persistent unusual system behavior observed after a primary malware infection was successfully removed. The initial local antivirus solution failed to detect any further malicious files, suggesting a gap in security coverage. To address this concern, a cloud-based antivirus scanning API (ClamAV) was employed to re-analyze suspicious files.

A Bash script was developed to automate the submission and analysis of 272 files to the ClamAV API. This identified `file176.exe` as malicious, which had been previously undetected. The MD5 hash `f48a8687e91fd9ef98cd1b7aaeeb2a4c` was extracted and verified, serving as a unique signature for future identification and blocking.

This investigation highlights the importance of layered security controls, automating threat hunting processes, and maintaining up-to-date threat intelligence for robust cybersecurity defense. The recommendations provided aim to enhance detection capabilities, prevent future infections, and improve FinancePlus's overall cybersecurity posture.

Findings and Analysis

Finding	Finding Details	Significance
Malicious File	`/home/bruce/Desktop/suspicious-files/file176.exe`	Cloud-based ClamAV API flagged this file as malicious after local antivirus failed to detect it, demonstrating the value of diverse threat intelligence sources
MD5 Hash	`f48a8687e91fd9ef98cd1b7aaeeb2a4c`	The MD5 hash provided a unique identifier for the malicious file, allowing for precise detection and prevention of future

		execution, crucial for incident response
ClamAV API Utilization	`https://clamav-ui.com/api/v1/scan`	The successful use of a cloud-based scanning service highlights the need to augment local defenses with external threat intelligence
Authentication Token	Token from `/api/v1/auth`	Secure authentication was established with the ClamAV API, demonstrating adherence to security best practices during the analysis phase
Detection Gap	Local AV failed to flag `file176.exe`	The local antivirus failing to detect the file underscores the limitations of single-layer antivirus solutions and the necessity of a layered security approach

Methodology

Tools and Technologies Used:

- **Bash:** Used to automate the scanning of hundreds of files, reducing manual errors and speeding up the analysis process.
- **curl:** Used to authenticate with the ClamAV API and submit files for scanning.
- **ClamAV API:** Employed to scan files against an external, cloud-based antivirus service, expanding the detection capabilities beyond the local antivirus.
- **grep:** Used to efficiently parse the log files, identifying detections from ClamAV's scan results.
- **md5sum:** Utilized to generate a unique cryptographic hash for the malicious file, which is critical for future detection and threat intelligence.

Investigation Process

1. **Initial Observation:** After successfully removing the primary malware, unusual system behavior persisted, leading to the hypothesis that additional malicious files had been created and executed.
2. **Authentication with ClamAV API:** Used `curl -k https://clamav-ui.com/api/v1/auth` to obtain an authentication token, saved for subsequent requests to the ClamAV API.
3. **Automated Script Creation:** A Bash script was developed to automate scanning, consisting of:
    - Looping through the directory containing suspicious files (`/home/bruce/Desktop/suspicious-files/`).
    - Submitting each file to the ClamAV API using curl.
    - Appending the scan response to a log file named `scan_results.log`.

```
bash
chmod +x scan_files.sh
./scan_files.sh
```

8. **Analysis of Scan Results:** Once completed, the scan results were parsed to identify infections. The command used was:

```
Bash

grep "infected" scan_results.log
```

This command confirmed that `file176.exe` was flagged as malicious by ClamAV.

6. **Verification and Hash Extraction:** The identified file's existence was confirmed, and its MD5 hash was extracted using:

`bash md5sum /home/bruce/Desktop/suspicious-files/file176.exe`

This hash `f48a8687e91fd9ef98cd1b7aaeeb2a4c` uniquely identifies the malicious file.

Recommendations

1. **Implement Layered Security Controls:** Adopt a multi-layered security strategy incorporating web-based AV scanning into incident response processes, catching threats missed locally.
2. **Automate Threat Hunting:** Implement automated scanning and analysis scripts into routine incident response workflows, improving speed and accuracy.
3. **Maintain and Share Threat Intelligence:** Create and maintain blocklists using malicious file hashes (e.g., MD5 here), sharing that information with security communities.

4. **File Integrity Monitoring:** Deploy File Integrity Monitoring (FIM) to detect and alert on unexpected file creations or modifications.
5. **Continuous Monitoring and Training:** Perform regular threat hunting and update defenses to combat advanced malware tactics.

Appendix A

Finding	Finding Details	Significance
Malicious File	`/home/bruce/Desktop/suspicious-files/file176.exe`	Confirms threat present and actions needed.
MD5 Hash	`f48a8687e91fd9ef98cd1b7aaeeb2a4c`	Unique identifier for effective blocking.
API URL	`https://clamav-ui.com/api/v1/scan`	Provides extra check for threats.
Authentication Token	Token from `/api/v1/auth`	Demonstrates secure data handling.
Detection Gap	Local AV didn't flag	Highlights necessity for layered defenses.