Lindsay Anson
Final Assessment Report Submission

Final Assessment Report Submission
Case: One of Us
Date: 2024-11-27

Executive Summary

This report analyzes a set of suspicious files to identify potentially malicious activity. The investigation revealed that file176.exe is malicious. The analysis involved running a Python script that calculated the MD5, SHA-1, and SHA-256 hashes for each file and cross-referencing these hashes with known malware databases. This process pinpointed file176.exe as a potential threat.

The report provides a detailed step-by-step methodology, including the tools used and the rationale for their selection. It also presents a comprehensive analysis of the findings, explaining their significance within the cybersecurity context. Finally, the report offers actionable recommendations to mitigate the identified risks, secure systems, and prevent future similar incidents.

Findings and Analysis

- Malicious File: File176.exe
- Hash: f48a8687e91fd9ef98cd1b7aaeeb2a4c
- File Attribute 224k

Methodology

Tools and Technologies Used

- Python Scripting: Python was used to automate the process of hash calculation and analysis.
- Hashing Algorithms: MD5, SHA-1, and SHA-256 were used to generate unique file signatures for comparison.

Investigation Process

- The investigation began with a comprehensive analysis of the provided files. An initial assessment using the ls -l and -h flags revealed that all files had the same privileges and were approximately the same size. To delve deeper into the contents of each file without directly executing them, a Python script was employed to generate MD5, SHA-1, and SHA-256 hashes. These hashes served as unique fingerprints for each file, allowing for safe evaluation. Several files with

suspicious hash characteristics were then scrutinized further using ClamAV and VirusTotal. This analysis ultimately led to the identification of file176.exe as the potentially malicious file.

Recommendations

- **Quarantine and Delete**: Immediately isolate file176.exe to prevent further damage. Delete the file once it has been investigated.
- **Update Antivirus**: Ensure your antivirus software is up-to-date to detect and prevent future infections.
- **Regular Scans**: Regularly scan your system for malicious files to catch any threats early.