**Malware Analysis Documentation**

**1. Sandbox Setup**

This section outlines the steps to create and configure accounts on Any.Run, Hybrid Analysis, and VirusTotal for malware analysis automation.

**1.1 Any.Run Account Setup**

1. **Visit Any.Run**: Go to <https://any.run> and create an account.
2. **Account Verification**: Confirm your email address and log in.
3. **API Key Access**: Once logged in, go to your profile settings to locate the API key. This key is necessary for automating submissions in Any.Run.
4. **A screenshot of a computer

   Description automatically generatedEnable API Access**: Ensure that API access is enabled in your account settings to support automated submissions.

**A screenshot of a computer

Description automatically generated**

**1.2 Hybrid Analysis Account Setup**

1. **Visit Hybrid Analysis**: Go to <https://www.hybrid-analysis.com> and create an account.
2. **API Key Access**: After logging in, locate the API Access section in profile settings to generate an API key for automated submissions.
3. **A screenshot of a computer

   Description automatically generatedEnable API Access**: Verify that API access is configured to allow automated usage.

**A screenshot of a computer

Description automatically generated**

**1.3 VirusTotal Account Setup**

1. **Visit VirusTotal**: Go to <https://www.virustotal.com> and create a free account.
2. **Generate API Key**: Once logged in, find your API key under profile settings.
3. **A screenshot of a computer

   Description automatically generatedAPI Usage Limits**: Note any usage limits in the API documentation or settings to avoid exceeding API request quotas.

**A screenshot of a computer

Description automatically generated**

**2. Script Execution Overview**

This section provides an outline of the intended execution process for each script and describes the expected results if the scripts are run successfully. It does not require actual code execution.

**2.1 Any.Run Automation Script Execution**

1. **Script Setup**: Place anyrun\_analysis.py in a designated scripts folder and ensure that config\_windows.py has the Any.Run API key configured.

A black screen with white text

Description automatically generated

1. **Expected Execution Steps**:
   * The script would ideally submit a malware file to Any.Run, receive a task ID for tracking, and poll Any.Run until the analysis is complete.
2. **Expected Output**:
   * A JSON report would be generated upon completion, containing details about the malware’s behavior, including any API calls, registry modifications, and network activity.

A screenshot of a computer

Description automatically generated

**2.2 Hybrid Analysis Automation Script Execution**

1. **Script Setup**: Place hybrid\_analysis.py in the scripts folder, with config.py containing the Hybrid Analysis API key.

A black screen with white text

Description automatically generated

1. **Expected Execution Steps**:
   * The script would submit a malware file to Hybrid Analysis, retrieve a job ID, and wait for the analysis to complete before pulling the results.
2. **Expected Output**:
   * A JSON report would be returned, ideally capturing API call usage, network connections, and file modifications. This report serves as a source for behavioral indicators.

A screenshot of a computer program

Description automatically generated

**2.3 VirusTotal Automation Script Execution**

1. **Script Setup**: Place virustotal\_analysis.py in the scripts folder, and ensure the VirusTotal API key is in config.py.

A black background with white text

Description automatically generated

1. **Expected Execution Steps**:
   * The script would submit a malware file to VirusTotal and retrieve the scan ID. It would then attempt to pull the final report for that submission.
2. **Expected Output**:
   * The report would contain metadata, such as the detection date, number of detections (positives), and scan summary.

A screen shot of a computer

Description automatically generated

**3. Sample Malware Hashes**

This section provides sample hash values for reproducibility. Using these specific hashes allows consistent analysis across other environments.

| **Sample Name** | **Hash (SHA-256)** | **Malware Type** |
| --- | --- | --- |
| Ransom1 | 2dcdf715266fb02cf258919c69f4a44e1d376131 | Ransomware |
| Trojan1 | 1b7dcb00c158bc27c2ea9cd12d9838ef7df21f2e | Trojan Horse |
| Virus1 | 6c879cb5c54af15b11bf732bbaeea3137392564 | Virus |

**4. Feature Extraction Details**

In behavioral malware analysis, key indicators provide insights into how malware interacts with the system, aiming to identify patterns or specific actions that signify malicious intent. Below are the critical behavioral indicators extracted from the JSON reports of Any.Run, Hybrid Analysis, and VirusTotal, along with their relevance to malware analysis.

**4.1 API Calls**

* **Definition**: API (Application Programming Interface) calls represent the set of commands or requests a program makes to interact with the underlying operating system or other services. Malware often relies on specific API calls to perform actions like creating files, accessing network resources, modifying the registry, and executing processes.
* **Importance in Malware Analysis**:
  + By analyzing API calls, we can identify specific functionalities of malware, such as file encryption (in ransomware) or key logging (in spyware).
  + Certain API calls are red flags in security analysis, especially those related to network communication (e.g., InternetOpenUrl) or file encryption (e.g., CryptEncrypt).
* **Tool Contributions**:
  + **Any.Run**: Provides detailed logging of API calls during real-time execution, capturing system interactions on a function-by-function basis. This data helps in observing dynamic behavior patterns, especially for malware that requires user interaction or delays its malicious actions.
  + **Hybrid Analysis**: Offers comprehensive API call tracing in its reports, categorizing calls into groups like file operations, network communication, and registry interactions. This structured data helps in quickly identifying suspicious behaviors.
  + **VirusTotal**: Although VirusTotal is more focused on file reputation, it can identify known malware based on file signatures. It may occasionally provide metadata on known API usage for specific malware families if such information is available in the collective dataset.

**4.2 Network Connections**

* **Definition**: Network connections refer to the external and internal communication attempts made by the malware. These typically involve connections to IP addresses, domain names, or ports that facilitate data exfiltration, command-and-control (C2) communication, or download of additional payloads.
* **Importance in Malware Analysis**:
  + Malicious network connections can reveal the external servers that malware communicates with, often pointing to C2 infrastructure.
  + Analyzing network activity helps in detecting malicious URLs or IP addresses, which can be blocked or monitored in network defense strategies.
* **Tool Contributions**:
  + **Any.Run**: Provides a visual map of network activity, showing connections initiated by the malware in real time. This includes details on the IP addresses, URLs, and protocols used, which are useful in identifying potential C2 servers or other malicious endpoints.
  + **Hybrid Analysis**: Captures network connections as part of its dynamic analysis and categorizes data by domains, IP addresses, and network protocols. This information is useful in understanding how malware communicates externally.
  + **VirusTotal**: While not as detailed in real-time network tracing, VirusTotal can match suspicious IP addresses or domains against its database. If the IP or domain is known for hosting malware, VirusTotal may flag it as part of the malware's network indicators.

**4.3 Registry Modifications**

* **Definition**: Registry modifications involve changes that malware makes to the Windows Registry, a hierarchical database used to store low-level settings for the operating system and applications. Malware may alter registry keys to maintain persistence, disable security features, or alter system behavior.
* **Importance in Malware Analysis**:
  + Persistent malware often uses registry changes to ensure it re-launches when the system restarts. Key registry paths are known to be modified for persistence, such as HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run.
  + Registry modifications are a common indicator of malware that operates stealthily, embedding itself within the system’s startup process or modifying security policies.
* **Tool Contributions**:
  + **Any.Run**: Logs changes made to critical registry paths, enabling analysts to identify persistence mechanisms or security modifications. Registry data from Any.Run helps in tracking how the malware ensures continued execution across system reboots.
  + **Hybrid Analysis**: Provides a comprehensive list of registry modifications in its report, with insights into which registry paths were altered and how these changes affect system configuration. This data helps in identifying specific tactics used by the malware to modify or control system behavior.
  + **VirusTotal**: Limited in registry analysis, VirusTotal does not provide direct registry monitoring but may reference registry-based signatures if they’re associated with known malware.

**4.4 File System Changes**

* **Definition**: File system changes include any modifications, deletions, or creations of files on the system. Malware often manipulates files for various purposes, such as encrypting documents (ransomware), creating new executables (worms), or modifying system files (rootkits).
* **Importance in Malware Analysis**:
  + Observing file changes can reveal the direct impact of malware on the system, such as encryption of personal files in ransomware attacks or installation of additional payloads.
  + File creation or modification in sensitive directories (e.g., system32 on Windows) often indicates malicious intent, especially if the files are hidden or protected.
* **Tool Contributions**:
  + **Any.Run**: Tracks file system changes, displaying files created, modified, or deleted by the malware. This real-time data is essential in ransomware analysis, where tracking file encryption or destruction is critical.
  + **Hybrid Analysis**: Lists file operations in its report, showing how the malware interacts with different files and directories. This data is especially useful for identifying malware that installs additional components or modifies system files.
  + **VirusTotal**: VirusTotal does not provide direct file system monitoring but may include file-related metadata from other antivirus engines or sandbox environments, giving a summary of known file actions related to the sample.

**Summary of Feature Extraction**

These indicators—API calls, network connections, registry modifications, and file system changes—form a comprehensive behavioral profile for each malware sample. By automating the extraction of these features, we can streamline the malware analysis process and focus on interpreting results rather than performing repetitive data collection tasks. Each tool in this multi-tool setup contributes unique insights, allowing for a layered approach to behavioral analysis.