**Malware Analysis Automation Project: Comprehensive Source Code and Configuration Documentation**

**Abstract**

**This document provides an overview of the source code and configuration settings used in the malware analysis automation project. The project uses Any.Run, Hybrid Analysis, and VirusTotal for malware behavior analysis. The document includes explanations of each script, detailed configuration files, and instructions for setting up and running the code on other systems. The provided scripts are designed for flexibility and scalability, supporting reproducible analysis across multiple datasets.**

**1. Project Overview**

**The objective of this project is to automate the analysis of malware samples using three sandboxing environments: Any.Run, Hybrid Analysis, and VirusTotal. The automation includes file submission, status monitoring, report retrieval, and feature extraction for indicators such as API calls, network connections, registry modifications, and file system changes.**

**2. Directory Structure and Configuration Files**

**Project Structure**

**A screenshot of a computer

Description automatically generated**

**Configuration Files**

Each configuration file stores the API keys, endpoints, and sample paths for each platform, making it easy to adapt the project to different environments.

**1. Configuration for Any.Run (config\_anyrun.py)**

**A screenshot of a computer code

Description automatically generated**

**2. Configuration for Hybrid Analysis (config\_hybrid.py)**

**A screenshot of a computer code

Description automatically generated**

**3. Configuration for VirusTotal (config\_virustotal.py)**

**A computer code with black text

Description automatically generated**

**3. Code Breakdown**

**3.1 Any.Run Automation Script (anyrun\_analysis.py)**

The anyrun\_analysis.py script automates malware file submissions to Any.Run, retrieves the analysis status, and parses JSON reports for API calls, network connections, registry changes, and file changes.

**A screenshot of a computer program

Description automatically generated**

**3.2 Hybrid Analysis Automation Script (hybrid\_analysis.py)**

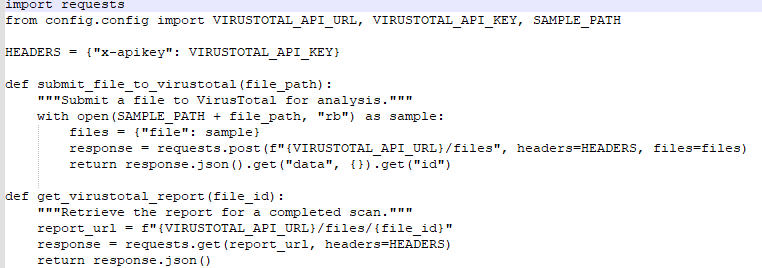
The hybrid\_analysis.py script submits malware samples to Hybrid Analysis, checks the job status, and extracts information from the JSON report.

A screenshot of a computer code

Description automatically generated

**3.3 VirusTotal Automation Script (virustotal\_analysis.py)**

The virustotal\_analysis.py script submits files to VirusTotal, monitors the status, and retrieves detection results.

****

**3.4 Report Parsing and Feature Extraction (report\_parser.py)**

The report\_parser.py script parses JSON reports to extract behavioral indicators: API calls, network connections, registry modifications, and file system changes.

**A screenshot of a computer program

Description automatically generated**

**4. Instructions for Running on a Different System**

1. **Set up the directory structure** on the new system as shown above.
2. **Install dependencies** with:

“pip install requests “

1. **Configure API keys** in each configuration file (config\_anyrun.py, config\_hybrid.py, config\_virustotal.py).
2. **Place malware samples** in the data/samples/ folder.
3. **Run each script** independently or use main.py to orchestrate all analyses.

**5. Applying to New Datasets**

To analyze new datasets:

Replace samples in the data/samples/ folder.

Update configuration files with any required changes.

Run the relevant scripts, adjusting parameters as needed.