**Bonfire Security Anti-Malware Program**

User Manual

Version 1.0 – 2/21/2024

**Table of Contents:**

1 - Introduction:

1.1 Software Overview 3

2 - Setup / Getting Started:

2.1 Warnings 4

2.2 Program Setup 4

2.3 Menu Overview 4

3 - Using the system:

3.1 - Path Scan 5

3.2 - File Scan

3.3 - Folder Scan

3.4 - Full System Scan

3.5 - Add to Whitelist

3.6 - Get All Process IDs

3.7 - Scan System Using YARA Rules

3.8 – Network Scan

3.9 – Quarantine and Restore Files

1. Introduction

1.1 – Software Overview

Bonfire Security is an anti-malware application that can perform hash signature or YARA rule-based file scans.

2. Setup/Getting Started

2.1 – Warnings

This software may not find all malicious files on your system. This software may not be able to scan all files on a system.

2.2 – Software Setup

For file scans to run correctly, the software requires access to the virus signature data dump from <https://bazaar.abuse.ch/export/>. This file, named full.csv, needs to be included inside the signature\_based folder, as pictured below.

A screen shot of a computer

Description automatically generated

A screenshot of a computer

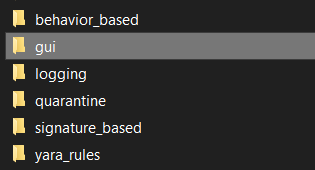
Description automatically generated

If the full.csv file is in the correct location, you can start the program by running the signature\_based.py file, pictured below.

A screenshot of a computer screen

Description automatically generated

You can also start the program from the mainGUI.py file found in the gui folder.

A screenshot of a computer

Description automatically generated

After running signature\_based.py or mainGUI.py, you should see the main menu, pictured below.

A screenshot of a computer

Description automatically generated

2.3 – Menu Overview

In the bottom half of the screen is the system output. This will display the progress and results of any scans you run. Above, there is a text box to type a file path to scan, and buttons for various system actions, described in the following section.

3. Using the System

3.1 – Path Scan

A grey rectangular sign with white text

Description automatically generated

Near the top of the main menu, there is a text box (pictured above) that prompts the user for a file path to scan. After entering the path to a file, the program will run a scan on it if it exists. If it doesn’t an error will be displayed in the system output.

3.2 – File Scan

A blue and black sign with white text

Description automatically generated

3.3 – Folder Scan



3.4 - Full System Scan



3.5 - Add to Whitelist

A blue rectangle with white text

Description automatically generated

3.6 - Get All Process IDs



3.7 - Scan System Using YARA Rules



3.8 – Network Scan

A blue rectangle with white text

Description automatically generated

3.9 – Quarantine and Restore Files

A blue rectangle with white text

Description automatically generated

This button will open a separate window for quarantining files and folders, as well as for restoring quarantined files.

This is what the menu looks like:

A screenshot of a computer

Description automatically generated

The “Quarantine File” button will open a dialog box for the user to select a file. Once a file is selected, the program will immediately quarantine that file.

“Quarantine Folder” works the same way with the user selecting a folder.

From the drop-down menu, the user can select a previously quarantined file. When the user clicks “Restore File”, the selected file will be restored to its original location.

There is currently no display about the results of these actions.