Machine Learning Malware Battle - Gotta Evade 'em All User Manual

Emily J Chaffey, Daniele Sgandurra

July 16, 2020

Contents

Chapter 1

Requirements

The recommended system requirements are:

1. Microsoft Windows 10 (64-bit)

2. 8gb RAM

3. Approximately 25GB free space (due to using virtual machines)

If you cannot meet the above requirements, you can run a lite version, where the virtual machines are not used, as it will use already generated data. For more information on this option see 1.2.2.

In order to successfully run my program, you must have the following installed:

1. Python 3.6 or above
   The following can be installed with the command 'pip install' followed by the name of the library:

   arcade

   numpy

   scikitlearn

   win32api

   autopy

   Pygame

2. Oracle VirtualBox (not needed for lite version)

In order to open the virtual environment, you must download the virtual box file from here[1].

For setup instructions see Chapter 1.1

---

[1]The password to download the VM is 'CuckooPass1920'

1.1 Setup

In this chapter we will cover how to successfully setup the system.

1.1.1 Virtual Environment

This section explores how to import the virtual environment.

1. First, open Oracle VM VirtualBox Manager.

2. Then, select the file option and click on the option 'Import Appliance'.

3. Next, under the File section, browse your file directory to locate and select the OVA file (downloadable from here[2]).

4. Then, click 'Next' followed by 'Import'.

5. Wait for the appliance to finish importing and then you are ready to go!

1.2 Running the Main Software

For an alternative explanation of how to run the final deliverable, please watch the videos in the folder 'Gotta_Evade_'em_All_Videos'.

1.2.1 Running the Virtual Environment

This section can be skipped if you are going to use the lite version.

In order to run the final deliverable using the virtual environment, you should use the command:

'python main.py'

The agent should then automatically start Oracle VirtualBox.

Troubleshooting

In this section troubleshooting solutions will be covered.

How to import the virtual machine?

1. First, open Oracle VM VirtualBox Manager.

---

[2]The password to download the VM is 'CuckooPass1920'

2. Then, select the file option and click on the option 'Import Appliance'.

3. Next, under the File section, browse your file directory to locate and select the OVA file (downloadable from here[3]).

4. Then, click 'Next' followed by 'Import'.

5. Wait for the appliance to finish importing and then you are ready to go!

Which Username to Use? If the Ubuntu virtual machine requires you to log in, you must use the user 'Gotta Evade 'em All'.

What Password to Use? If a password is required, the password is 'CuckooPass1920'.

1.2.2   Lite Version

The lite version should only be used when the virtual environment cannot be used. This means that only the visualisation software and the machine learning aspects of my project will be used.

In order to run the visualisation software, open the command prompt and use the command:

'python main.py lite'

This will then proceed to run the parser engine and then the visualisation software (see 1.2.3 for instructions on how to use the visualisation software).

1.2.3   Visualisation Software

In order to run the visualisation software, you must have run either the command 'python main.py' or 'python main.py lite'.

The first screen you will encounter is the start screen (see Figure 1.1). In order to proceed, you must click within the window to begin the animation of the 'battle'.

---

[3]The password to download the VM is 'CuckooPass1920'

Figure 1.1: Visualisation Start Screen

The animation of the 'battle' will then be displayed. Once the 'battle' has finished, the victor screen will appear (see Figure 1.2). In order to progress to the next screen, the user must click within the window.
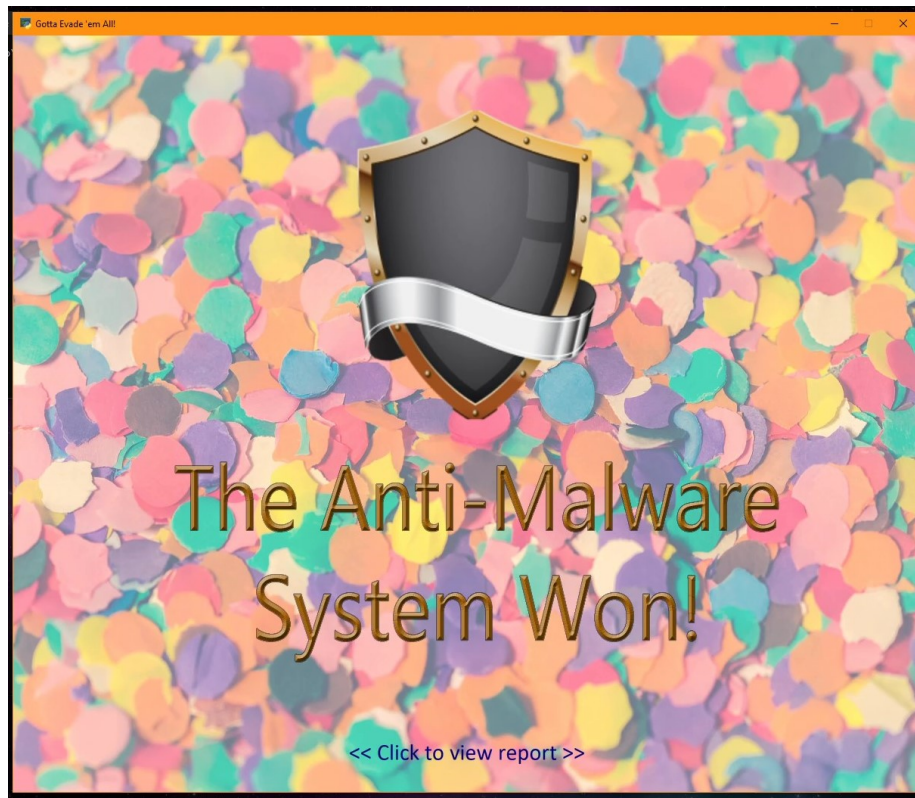
Figure 1.2: Visualisation Winner Screen

The next screen that will be displayed is the first page of the report. This screen informs the user of how dangerous the AMS deems the sample to be (see Figure 1.3). In order to view the next page of the report, the user must click within the window.
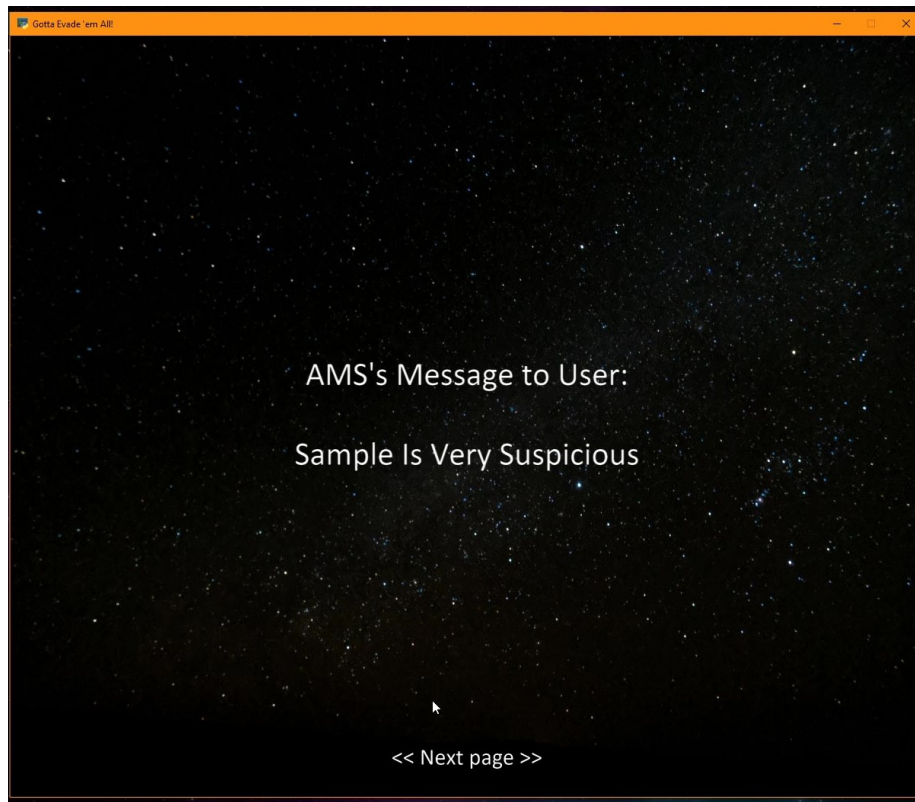
Figure 1.3: Visualisation First Report Page

Now the user will be viewing the second screen of the report, which displays the machine learning results (see Figure 1.4). In order to close the visualisation program and the rest of the system, the user simply needs to click within the window.
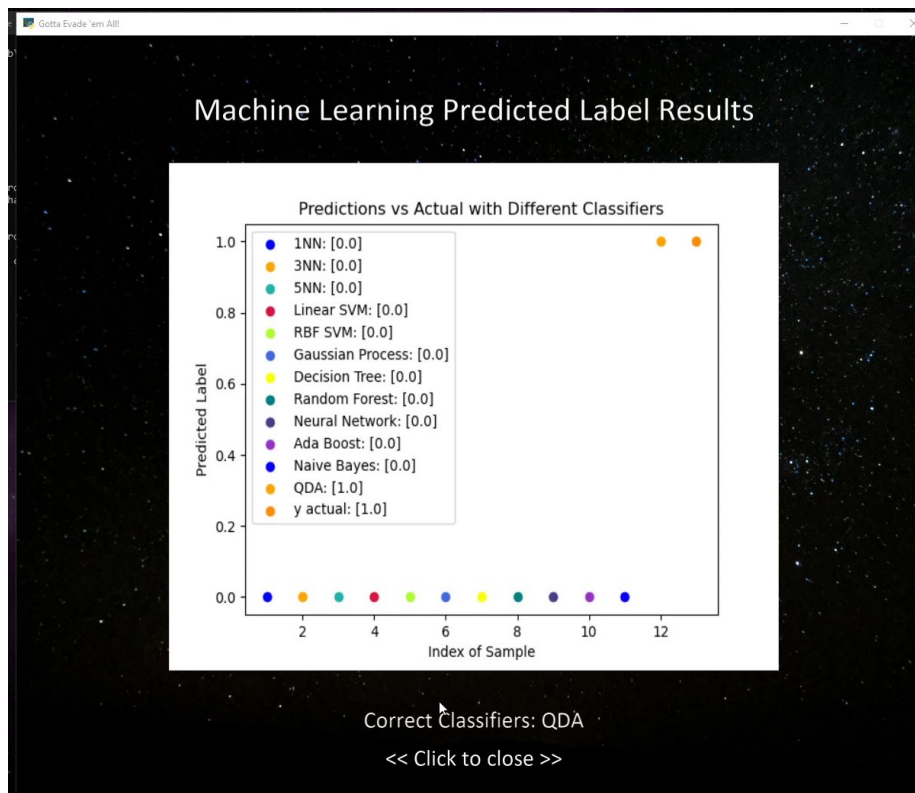
Figure 1.4: Visualisation Second Report Page (Machine Learning Results)