Monitoring and Detection Documentation by Amish Gadhia (group 8)

For monitoring we are running an infinite loop which checks the files of the directory. First, we check the hash signatures of the files using sha256. If a signature of the file got changed then we check the content of the file. If any changes look suspicious then we are raising alerts for the user. There are two kinds of alerts.

1. Low priority alert – This will be shown to the user when the user made changes on the file by himself/herself. At that time the mitigation won’t start
2. High Priority alert – This will be shown to user when some changes made inside the file and those changes are not human readable. Which means content changes are not in English. There will be high probability that the file is encrypted. So immediately after detection we will start the mitigation.

NOTE – To run the code, you need to install a python library.

#pip install googletrans==3.1.0a0

You need to change the your target directory path according to your file path.

rootdir = '/home/sec-lab/Desktop/projectfiles'

Here is the Example simulation –

First the program will initially check all the files of the target directory and store their signature and path inside the dictionaries.

Text

Description automatically generated

“document1.txt” is one of the file inside the target directory.

Graphical user interface, text, application

Description automatically generated

If we as a user change the content inside the document1.txt (here we appended word edited) then it will raise an low priority alert showing changes are made inside the file. But it won’t start the mitigation as these changes as made by a normal user.

Graphical user interface

Description automatically generated

But when an evil person tries to encrypt the file of the target directory then the program immediately raises a high priority alert and start the mitigation process.

Text

Description automatically generated

Here is the content inside file after the encryption.

Graphical user interface, application, website

Description automatically generated