Anaisy Garcia

PID: 5734454

Fake FBI Attack

The malware presented here is a small python script which was turned into an executable to hide as another program within windows. The program can do multiple things such as write multiple files secretly to the C drive, change the wallpaper, show an image that bounces around the screen, and emit noise. The program will write 100,000 files with 50 lines of writing in each after this it will open them and it will play a song and display pop ups, then finally an image will bounce on screen. The purpose of this code is to make the victim believe they’re being watched by the FBI while flooding their computer with worthless files. The malware was obtained originally from one website then changes were made using other small sections of code online.

This program can take a long time to fully run wait until the bouncing picture is shown. To run the program, extract the final project zip file to the C drive, turn up computer volume, and double click the Fortnite shortcut. After this check the bin folder to see everything being written and wait till image bounces on screen. If nothing shows up, go to the install folder and double click the Fortnite application and install to the C drive then double click the Fortnite shortcut. After the run start trying to X out of all notepads/pop-ups. To remove, stop the process called Final\_Project in task manager.

The malware was originally from Stack Exchange under Code Review where someone uploaded their code to receive feedback a year ago. The code was just supposed to function as a picture bouncing around the screen that was hard to avoid or get rid of and was done using tkinter import (Code Review Stack Exchange, 2018). This code was taken and then the first change made was adding a pop-up that would continue to appear even when exited from it and was done using easygui import. The code for this section of the program was taken from a Stack Overflow comment (Ginstorm, 2010). The next change made was the ability to change the desktop wallpaper as well as check for with bit OS is being used. This code was taken from a comment on a Stack Overflow question and was done using the ctypes import (Smith and Tolonen, 2018). The final change made was the ability to create and write files to the C drive. This code was taken from Guru99 and Stack Overflow where the explanation for writing, creating, and reading files can be found (Guru, 2019)(Stack Exchange, 2019). All codes can be found at the end of the report.

This is the original code:

|  |  |
| --- | --- |
| import tkinter  from random import randint  from pygame import mixer  from time import sleep  # Create a window:  window = tkinter.Tk()  # Setup the image:  img\_obj = tkinter.PhotoImage(file='jake.png')  img\_label = tkinter.Label(window, image=img\_obj)  img\_label.image = 'jake.png'  img\_label.pack()  width, height = img\_obj.width(), img\_obj.height()  # Setup the windows:  screen\_width = window.winfo\_screenwidth()  screen\_height = window.winfo\_screenheight()  window.title('JAKE.EXE')  window.resizable(False, False)  window.overrideredirect(True)  def random\_x():  return randint(0, screen\_width - width)  def random\_y():  return randint(0, screen\_height - height)  def random\_vel():  speed = 10  vel = randint(-speed, speed)  if vel == 0:  return random\_vel() | return vel  x = random\_x()  y = random\_y()  x\_vel = random\_vel()  y\_vel = random\_vel()  # Setup the sound:  mixer.init()  sound = 'walmart30mins.mp3'  mixer.music.load(sound)  mixer.music.play()  # Main loop:  while True:  sleep(0.01)  if x >= (screen\_width - width) and x\_vel > 0:  x\_vel = -x\_vel  elif x <= 0 and x\_vel < 0:  x\_vel = -x\_vel  if y >= (screen\_height - height) and y\_vel > 0:  y\_vel = -y\_vel  elif y <= 0 and y\_vel < 0:  y\_vel = -y\_vel  x += x\_vel  y += y\_vel  if randint(1, 100) == 100:  x\_vel = random\_vel()  y\_vel = random\_vel()  window\_string = str(width) + 'x' + str(height) + '+' + str(x) + '+' + str(y)  window.geometry(window\_string)  window.update() |

Taken from:

Code Review Stack Exchange. (2018). Tkinter prank to display a bouncing picture. [online] Available at: <https://codereview.stackexchange.com/questions/202169/tkinter-prank-to-display-a-bouncing-picture> [Accessed 27 Nov. 2019].

The code for pop-ups:

import easygui

easygui.msgbox("This is a message!", title="simple gui")

Taken from:

Ginstorm, R. (2010). How can I create a simple message box in Python?. [online] Stack Overflow. Available at: <https://stackoverflow.com/questions/2963263/how-can-i-create-a-simple-message-box-in-python> [Accessed 27 Nov. 2019].

The code for changing desktop wallpaper:

import struct

import ctypes

PATH = 'C:\\Users\\Patrick\\Desktop\\0200200220.jpg'

SPI\_SETDESKWALLPAPER = 20

def is\_64bit\_windows():

"""Check if 64 bit Windows OS"""

return struct.calcsize('P') \* 8 == 64

def changeBG(path):

"""Change background depending on bit size"""

if is\_64bit\_windows():

ctypes.windll.user32.SystemParametersInfoW(SPI\_SETDESKWALLPAPER, 0, PATH, 3)

else:

ctypes.windll.user32.SystemParametersInfoA(SPI\_SETDESKWALLPAPER, 0, PATH, 3)

changeBG(PATH)

Taken from:

Smith, J. and Tolonen, M. (2018). Change Windows 10 background in Python 3. [online] Stack Overflow. Available at: <https://stackoverflow.com/questions/53878508/change-windows-10-background-in-python-3> [Accessed 27 Nov. 2019].

The code for writing and creating files in a loop:

f= open("guru99.txt","w+")

for i in range(10):

f.write("This is line %d\r\n" % (i+1))

Taken from:

"Python File Handling: Create, Open, Append, Read, Write", Guru99.com, 2019. [Online]. Available: <https://www.guru99.com/reading-and-writing-files-in-python.html> [Accessed: 09- Dec- 2019]

The code for opening notepad:

import os

os.system("notepad.exe file.txt")

Taken from:

"Open a text file window using Python", Stack Overflow, 2019. [Online]. Available: <https://stackoverflow.com/questions/26205275/open-a-text-file-window-using-python> [Accessed: 09- Dec- 2019]