Personal Specialization Project

Table of Content

Project Definition

Introduction

This project is all about researching and developing my own idea for couple of weeks. I have full freedom for what I want to choose and go in full depths for the specific topic. My idea was to have two things, one connected with the infrastructure and the other is about the cyber security field. Talking about my idea connected with the infrastructure is to create monitoring/supporting tool, which could measure the CPU and RAM in real-time. Another thing that I would like to have in this monitoring tool is to be able to see system information and private, MAC addresses. My other idea for cyber security is to create malware, which will allow me to execute commands in victim's computer. Both of my ideas were quite interesting for me due to I have always wanted to try to create my own simple monitoring system and about the malware, in the courses we did not really saw any specifics malwares only brief description about what is exactly. So, I decided to do research for myself for how I could me such a program, which will allow to execute malicious activities without the knowledge of the victim.

Research

During my research I wrote for myself some questions, which were quite useful in order to go in the right direction. For me is very import before starting something to have some planning and helpful question, which will hold me in the right direction.

- What are the different types of monitoring tools?
- Which programming language is the best for monitoring tool and why?
- What packages do I need for this application?
- What should I measure and show ?
- How to create undetectable malware ?
- Which programming language is the best for malware and why?
- How to establish connection between server and client ?
- What things do I want to execute in victim's system?

With all the questions, I wanted to prepare myself due to if I could answer them, I will definitely complete the work. In the previous semesters, I was always taught to be prepared for the future problems, which will occur in one moment. That why I wanted to be ready for any kind of challenge that I will go through. Throughout my research I used three different, which were workshop, lab and library. Talking about the workshop research, in order to gain the needed information, I explored different things, which are similar to my assignment. Regarding the workshop research, certainly I tried prototyping and sketching in order to gain more insights what is possible and how could work. Last, but not least, I used lab research, where did a lot of test towards my application in order to see if the things work out the way I wanted.

Project Goal

The aim of this project is to create perfectly functional monitoring tool and malware. I want my monitoring tool to be user-friendly and easy to use. Another aim for this tool is to be able to show the CPU and RAM in real-time. The goal for my malware is once again to be easy to use, which will allow me to execute malicious activities more easier. In general, I would like to improve my researching, python programming and planning skills.

.

Planning

I really like to have a plan in my head, which allows to hold on the correct path for specific project. My planning is quite useful and makes the separate tasks easier for me in order to do them. Immediately, after choosing both assignments, I started working on the plan. I knew, I had a lot of time in order to finish the whole project. My first step of my plan was to spent a whole week just researching about the specific topics, which I chose and go in details about everything connected with my assignments. This week allowed to have a good idea of what I needed to do, how could be done and to have crystal clear idea for everything. During my research, I also started writing the documentation for the project, which included introduction and planning. After, whole week spending for researching and writing, my plan was to start working on the technical part. I wanted to spent two weeks in creating my monitoring tool and I believe that was the best solution in order to able to finish the fully the application. After finishing the design and functionality for the application, I needed to start working on the other task, which was the malware. There, I also wanted to spent two weeks, which in my personal opinion was enough time to finish and test it. Everything was done and the last parts, which I needed to was to write and document everything that I did during these weeks. I even had to time spend if I wanted to improve the design or functionality of my tool and malware.

Preparation

Monitoring tool(python)

My preparation for creating the application was quite long due to I needed a to setup correct environment for it and install couple of packages needed for correct functionality and design. Basically, I needed to install visual studio code, where I needed to install python, but this part was skipped due to I already had such setup and moved immediately to the next part. Next part, was to install and use the following packages:

- Sys - This module provides various functions and variables that are used to manipulate different parts of the Python runtime environment. It allows operating on the interpreter as it provides access to the variables and functions that interact strongly with the interpreter
- Platform – This module is used to access the underlying platform's data, such as, hardware, operating system, and interpreter version information.
- PyQt5 - cross-platform GUI toolkit, a set of python bindings for Qt v5. With it you can develop an interactive desktop application with so much ease because of the tools and simplicity provided by this library.
- Psutil - cross-platform library used to access system details and process utilities. It is used to keep track of various resources utilization in the system. Usage of resources like CPU, memory, disks, network, sensors can be monitored
- Pathlib - provides various classes representing file system paths with semantics appropriate for different operating systems.
- NumPy - is a library consisting of multidimensional array objects and a collection of routines for processing those arrays. Using NumPy, mathematical and logical operations on arrays can be performed.
- Collections - are containers used for storing data and are commonly known as data structures, such as lists, tuples, arrays, dictionaries, etc.
- Time - provides many ways of representing time in code, such as objects, numbers, and strings
- Socket - provides various objects, constants, functions and related exceptions for building full-fledged network applications including client and server programs
- Uuid - library which helps in generating random objects of 128 bits as ids. It provides the uniqueness as it generates ids on the basis of time, Computer hardware.

Malware(python)

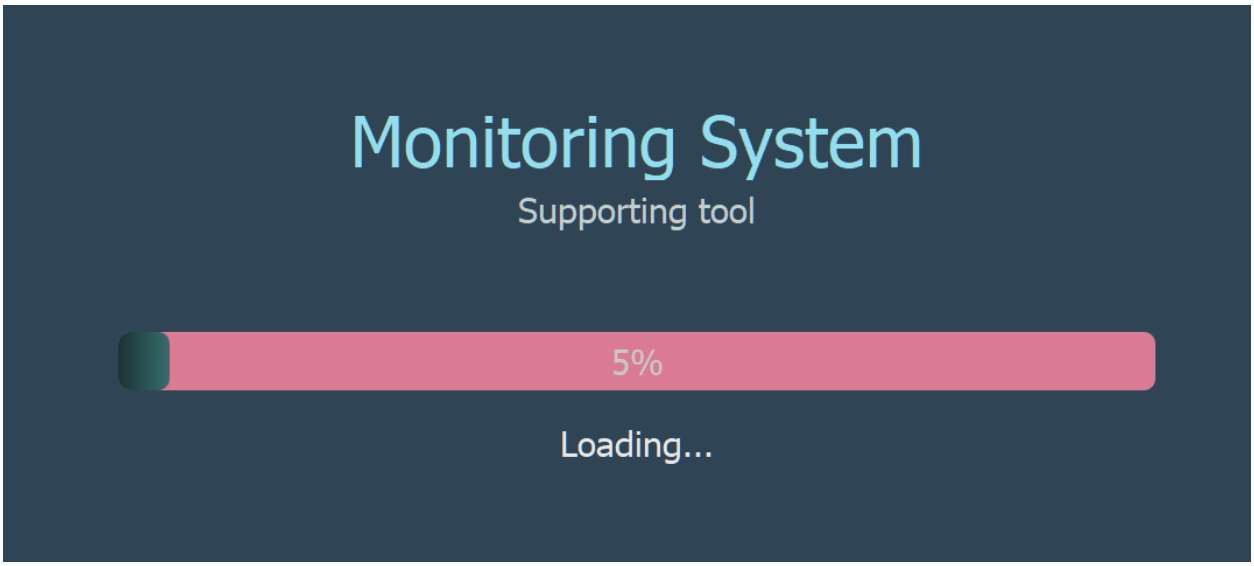
My preparation for malware was once again very long due to this time l needed to setup 1 Virtual machine with Linux, there to install Visual Studio code, python and the needed packages. The reason for creating VM is that my local laptop will be used as client and the Virtual machine will be used as server side. As l said before my setup on my local computer was ready, so l just needed to everything in the VM, which took quite a while. Next part, was to install and use the following packages:

- Sys
- Platform
- Time
- Socket
- OS - provides functions for interacting with the operating system and a portable way of using operating system-dependent functionality
- Zipfile - provides tools to create, read, write, append, and list a ZIP file.
- Pyautogui - allows for the running script to control mouse and keyboard, providing input much like how a user on the system would, allowing for interactions between applications on the system.
- Shutil - offers several functions to deal with operations on files and their collections. It provides the ability to copy and removal of files
- Winreg – This module offers functions expose the Windows registry API to Python. Instead of using an integer as the registry handle, a handle object is used to ensure that the handles are closed correctly

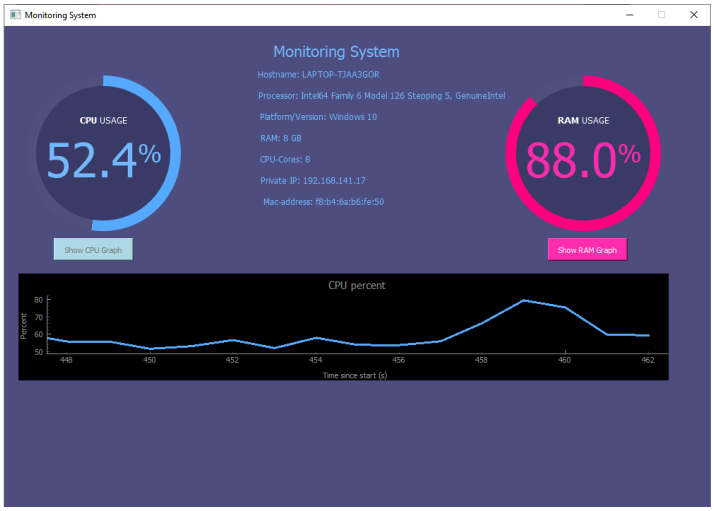
Description and general overview

Monitoring tool

My monitoring tool is written in python language and there are used packages, which allowed me to complete the functionality and design. The could be run in two ways, the first way is to run in through the command console with command “py systemMonitor.py”. The second and probably the option is to just click the .exe file, which I specifically created for this application. This was possible with package named “pyinstaller”, which also allowed me to put icon for the file. After running the program, it will pop up loading screen, which was designed by me and I was pleased with the design.



When the program load, it will show the main screen, where everything could be seen. This is the main screen, where it has graph, which measure the CPU and RAM over time. You can switch between seeing the real-time graph between the CPU and RAM. Both widgets show all the time, what are the percentage of CPU and RAM. There also, you can see some system information like Hostname, Platform, Platform/Version, RAM, CPU-cores and other things that are available to display are the Private IP and MAC-address



Malware

My malware is written in python language and there are used packages, which allowed me to complete the functionality. I have server and client side, in my scenario my Virtual machine is the server, who are waiting for connection and my local laptop is the client, who is connecting to the server. I have wrote filles in both side, which allow them to establish connection and execute things. Firstly, I ran the server side and then the client, which establish connect.

```
┌──(nightmare㉿nightmare)-[~/Server Side]
└─$ python3 main_server.py
                [+] Connection established with 192.168.1.185 on port 57413
[+] Handling connection
```

```
(venv) C:\Users\alexd\OneDrive\Desktop\Client Side>py main_client.py
[+] Handling connection
```

After the connection is successfully, in the server side I could see options, which I could execute. These are the available possibilities:

- Running system commands
- Upload file
- Download file
- Change Dir
- Capture Screenshot
- Become Persistent

```
┌──(nightmare㉿nightmare)-[~/Server Side]
└─$ python3 main_server.py
                [+] Connection established with 192.168.1.185 on port 57413
[+] Handling connection


                [ 01 ] Run Command on victim OS
                [ 02 ] Upload file to the victim's machine
                [ 03 ] Download File folders
                [ 04 ] Change Dir
                [ 05 ] Capture Screenshot
                [ 06 ] Become Persistant
                [ 99 ] Exit Program
[+] Select your options:
```

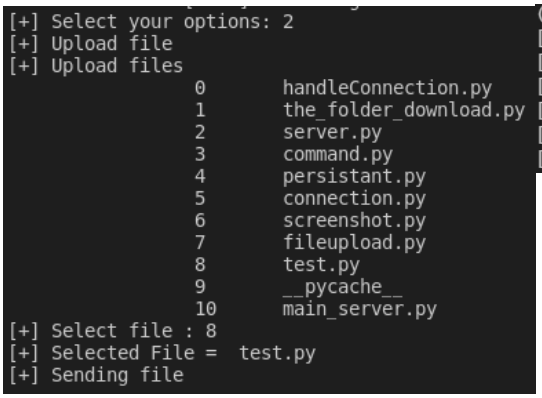
When I choose the first options, it allows me to execute commands in the Victim's machine. Basically, executing the command systeminfo, let me see everything regarding the system's victim.

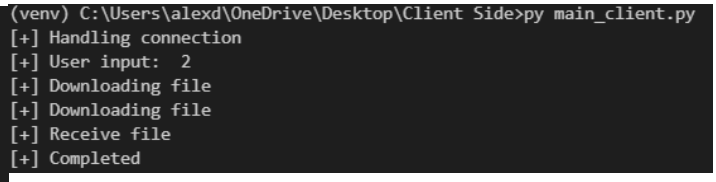
```
[+] Select your options: 1
[+] Running the system commands on victim
[+] Running commands
>> systeminfo

Host Name:                 LAPTOP-TJAA3GOR
OS Name:                   Microsoft Windows 10 Home
OS Version:                10.0.18363 N/A Build 18363
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          alex.dobrev.bg@gmail.com
Registered Organization:   HP
Product ID:                00325-96591-05728-AAOEM
Original Install Date:     10/8/2019, 9:03:44 AM
System Boot Time:          12/3/2021, 10:44:05 AM
System Manufacturer:       HP
System Model:              HP Pavilion Laptop 14-ce3xxx
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 126 Stepping 5 GenuineIntel ~1298 Mhz
BIOS Version:              Insyde F.15, 9/3/2021
Windows Directory:         C:\windows
System Directory:          C:\windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-gb;English (United Kingdom)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
Total Physical Memory:     7,970 MB
Available Physical Memory: 43 MB
Virtual Memory: Max Size:  19,794 MB
Virtual Memory: Available: 2,851 MB
Virtual Memory: In Use:    16,943 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\LAPTOP-TJAA3GOR
```

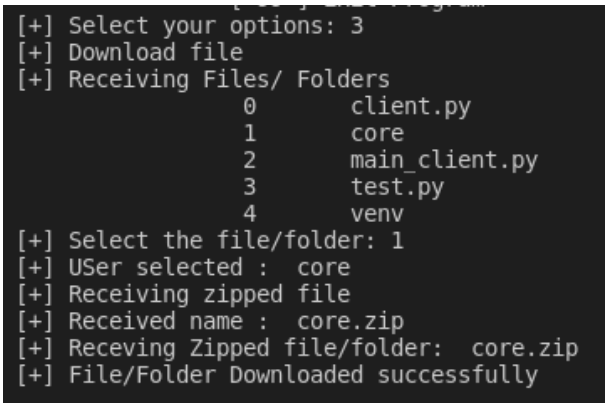
```
(venv) C:\Users\alexd\OneDrive\Desktop\Client Side>py main_client.py
[+] Handling connection
[+] User input:  1
[+] Running system commands
[+] Executing commands
systeminfo
```

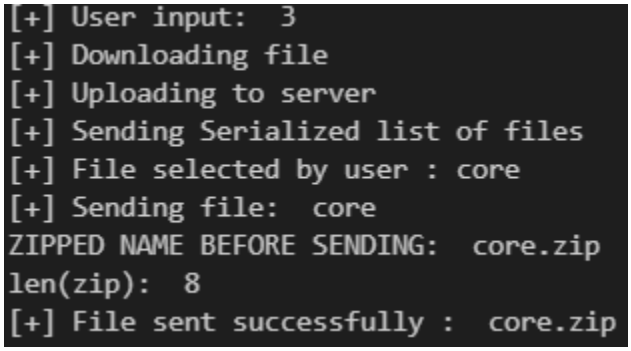
With the second option, I can upload whatever a file into victim's system. After, selecting this option, I could see what available files can uploaded. Whatever file is sent to the target's computer, it is received as ZIP file.



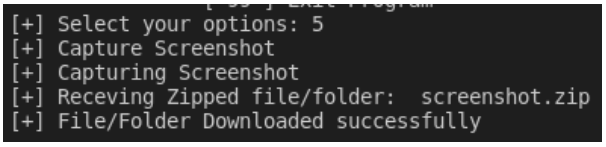


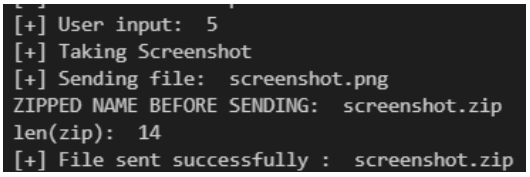
The third option is for downloading file/folder from the victim's machine. After choosing it, I could see what are the available files for downloading. I receive them as ZIP file.



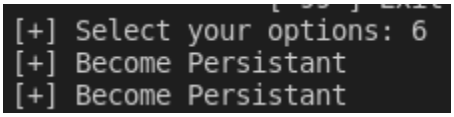


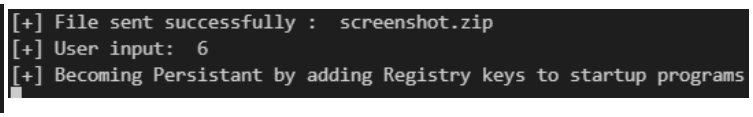
One of last option is to take screenshot of the victim's desktop and then receiving in the server side. Once again, I receive the photo as a ZIP file.

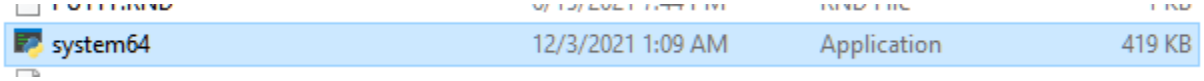




The last option allows me to become persistant by adding Registry keys to startup programs in victim's system. It could be backdoor file or whatever I want to put. In the example, I am just putting file, which do not harm the system.







Conclusion, Reflection & Findings

During this whole project, I managed to explore different packages regarding the application that I created. I was able to create complete application with a lot of effort and research. I was pleased with my work due to I managed to complete my main goals for the application, which were to measure CPU and RAM, showing some system information as well Private/Mac address. I was able to improve my python programming and get better understanding of some used packages. Talking about the assignment regarding the malware, there are I also managed to reach my goals, which I planned. Got better understating of what is actually malware and some things that you could possible do with it. My main goals for functionality were to run command, upload, download, capture pictures and to add registry keys to startup programs in the victim's machine. It was quite fun and exciting to work on both assignments, which allowed to gain more experience and understanding.

To be honest, I believe my overall project was on a decent level with different types of things. I managed to create and to follow my planning and also did some good researching in order to be able to hold the correct path. Another thing that I improved was my organization skills, which allowed to finish everything in the right time. Also, I am proud of this project and how much hours I managed to put in it. The main key that I was able to do was separate the tasks, which included planning, researching, preparation and testing. I was very interested in doing this kind of project, where my responsibility was to choose topic and go in full details about it. I was able to develop my research skills even more and also to be more patient. This whole project was quite a challenge for me, but I like challenging myself and I truly believe this project learnt different skills and things, which will be useful for my future projects.