Anaisy Garcia

PID 5734454

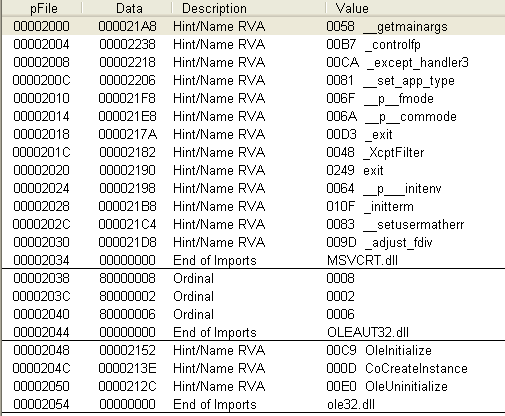
**Lab 7-2**

Analyze the malware found in the file *Lab07-02.exe*.

***Questions***

1. How does this program achieve persistence?

This program will not achieve persistence because it will only run once then exit.

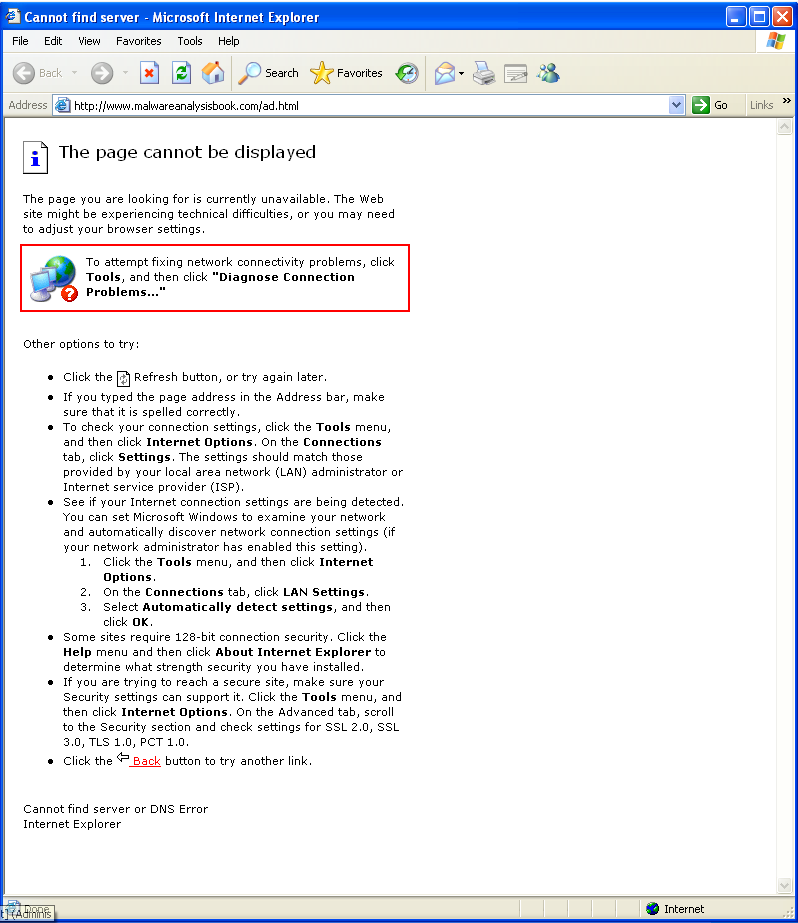


The imports include an exit as well as initialize and then uninitialize.

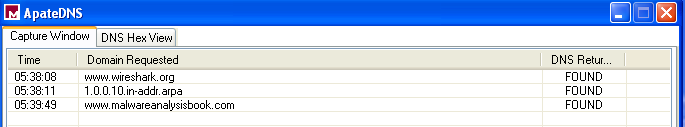
1. What is the purpose of this program?

The purpose of this program is to show an advertisement to the victim. 

Here we can see the website where the ad is located.



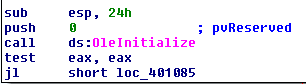
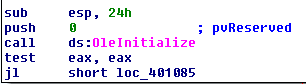
The ad would not show on this computer due to no access to the internet.

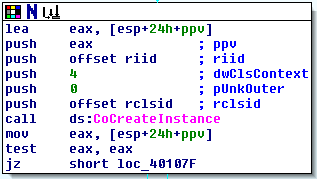


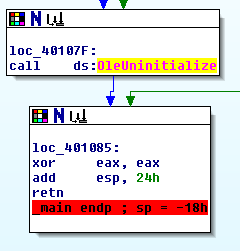
Here we see the program connecting to the website.

1. When will this program finish executing?

The program exits once it is done showing the victim the ad.







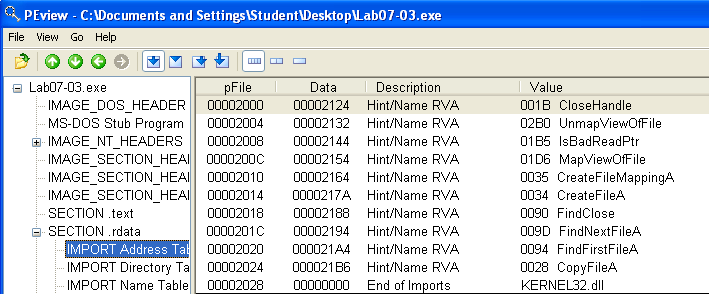
Here we see that the program called OleUninitialize which act as a cleanup function.

**Lab 7-3**

***Questions***

1. How does this program achieve persistence to ensure that it continues running when the computer is restarted?

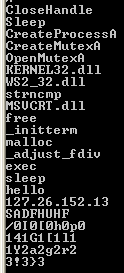
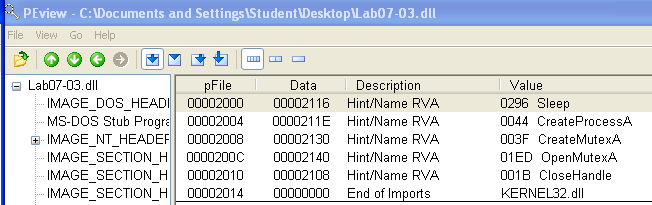
The program writes a DLL to a path in the computer (C:\Windows\System32). It then modifies every .exe file on the system to import the DLL it created.



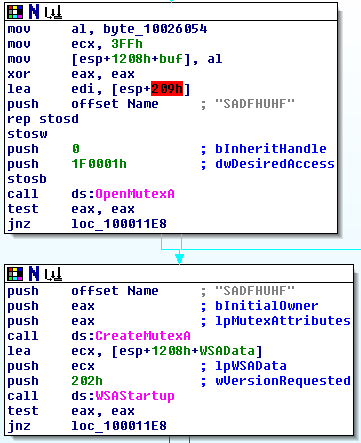
Here we can see the imports for writing the files and looking for files.

1. What are two good host-based signatures for this malware?

The program creates a mutex on the computer named SADFHUHF and uses a hard-coded file named kerne132.dll rather than the original kernel32.dll.



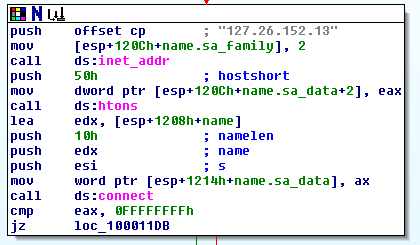
Here we see the imports for the mutex as well as the name of it on the strings program.



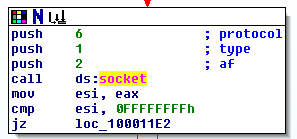
IDA pro also shows us the mutex being created and named.

1. What is the purpose of this program?

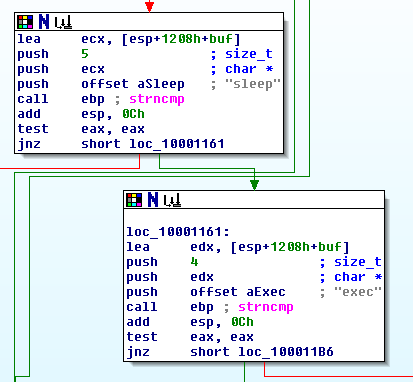
This program creates a back door on a victim’s computer which either runs a command or sleeps.



Here we see the connection to the ip address.



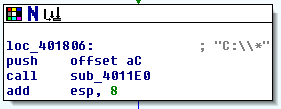
Here we can see a connection to a socket or port which was 80.



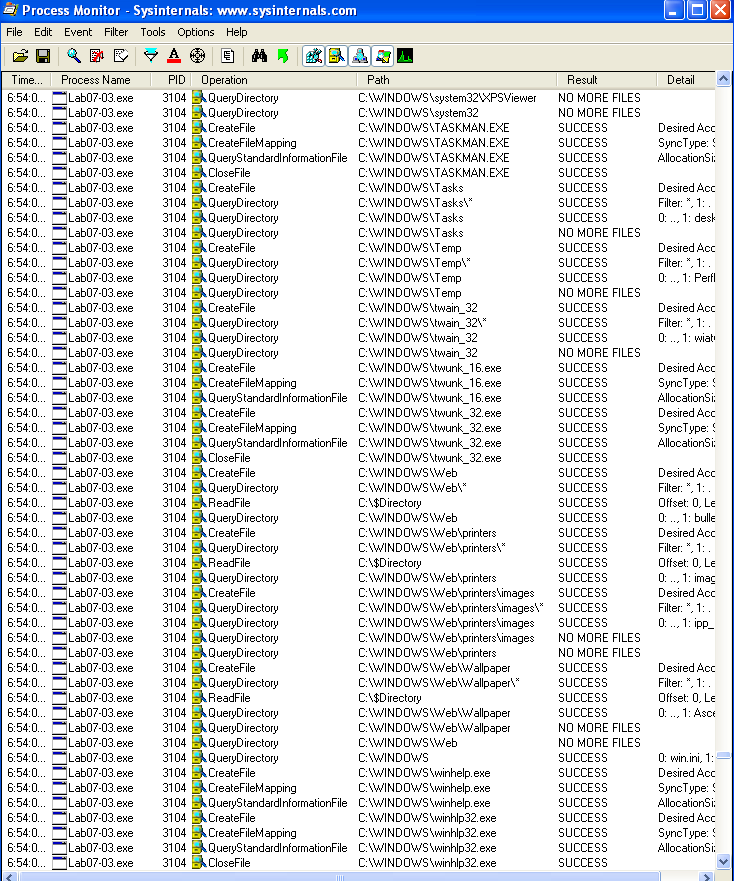
Here we see the program will either sleep or execute.

1. How could you remove this malware once it is installed?

It is difficult to remove this virus due to it infecting all exe files on the system. The best course of action would be a system restore.



Here we an see it does search the C drive here what it will due is look for all exe files and infect them.



This was further checked when running the exe, in process mon we can see it searching for any exe file then mapping to the dll.