**MALWARE ANALYSIS TOOLS and TECHNIQUES**

**PRACTICAL TEST 1**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | Dominic Lee | **Date** | 10 Nov 2022 |
| **Student ID** | S10222894 | **Duration** | 1.5 hours |

**Instructions**

1. Download the malware “VirusShare\_b0ce348674920ebf69e4cfd335a42d7e.zip” from  <https://drive.google.com/file/d/1BTgvx3WbGC3uzYNr2N6wLFfymUUaJW9W/view?usp=sharing>
2. Password will be shared by the tutor.
3. Copy and paste (or Drag n Drop) the malware.zip into your XP VM and then unzip it.
4. Rename the file as malware.exe.
5. You are to answer the questions below by performing basic static analysis and basis dynamic analysis on the malware.
6. Make sure you **save your work regularly** on your host machine.
7. Upload the file to BrightSpace.
8. The total marks for this paper is **50 Marks**.

**Questions**

1. The malware is packed. Which packer was used? How do you unpack this malware?

(2 marks)

The packer used is UPX 0.89.6 - 1.02 / 1.05 - 2.90 -> Markus & Laszlo [Overlay]. To unpack the malware, click on Plugins in PeiD and then use the UPX unpacker to unpack the malware.

1. State ONE important DLL that the malware imports. For the DLL, state TWO significant functions that the malware imports (Function Name, Ordinal Number). Explain what the DLL is being used for. Provide the screenshot of the tool used.

(8 marks)

Graphical user interface

Description automatically generated

|  |  |  |  |
| --- | --- | --- | --- |
| **DLL Name** | KERNEL32.DLL | | |
| **Function 1** | | | |
| **Name** | CreateFileA | **Ordinal Number** | 80 |
| **Function 2** | | | |
| **Name** | CreateEventA | **Ordinal Number** | 76 |
| **Purpose of DLL** | | | |
| The DLL is used for file and event manipulation. The above two functions either creates a new or opens an existing file or event on the host system. | | | |

1. Use an appropriate tool to view some strings in the malware. Find TWO strings that could reveal

some information. Justify your answer. Note: The identified strings should not be related to imported DLLs or imported Windows functions. Provide the screenshot of the tool used.

(4 marks)

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application

Description automatically generated

String 1:

String 1: “DOMAIN error”

Indicates that the malware is trying to connect to a domain

String 2:

String 2: “7zS.sfx.exe”

This is an executable that the malware might be trying to disguise as a .sfx file. Otherwise, it is still an executable file that is installed upon installion of the malware and could be used to attack the host system.

**Basic Dynamic Analysis**

To answer the following questions, you will need to prepare the necessary tools and execute the unpacked malware.

1. What happens when you execute the unpacked malware? Provide the screenshot and explain why this happens.

Graphical user interface

Description automatically generated

(4 marks)

This could happene because the unpacker which was used was (UPX unpacker) in PeID was not fully

Suitable to unpack the file as such, some of the contents of the unpacked malware was corrupted and the unpacked.exe is unable to be ran.

1. What are the two important registry changes observed? Provide the screenshot and explain the purpose of this change.

(4 marks)

**A picture containing calendar

Description automatically generated**

Here, the executable C:\Program Files\AdwareAlert\AdwareAlert.exe was put into the Run directory. This means that the malware is trying to gain persistence by executing AdwareAlert.exe on boot.

A picture containing text

Description automatically generated

The malware also changes the host’s cache to be filled with random data. This could indicate that the malware is aiming to slow the host’s processing speed by filling the host’s cache with useless data.

1. Was any file created on the system? If so, what is the filename? Provide the screenshot.

(2 marks)

Text

Description automatically generated

The filenames include 2994e3.msi, Icon.exe, AdwareAlert Scheduled Scan.job

1. Is there any Mutex created by the malware? If so, what is the name of the Mutex? Provide the screenshot.

(2 marks)

A screenshot of a computer

Description automatically generated with medium confidence

Yes, there are mutexes created by the malware. There are many names of the mutex as there are many mutants created. E.g. (WininetStartupMutex)

1. Are there any changes in the Strings after the malware is executed? If so identify the changes. Provide the screenshot.

(4 marks)

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application

Description automatically generated

At the bottom of the strings, the strings in memory were HTML code and or different to the strings in the image.

1. Does the malware try to connect to the network? If so, what address does it try to connect to? Provide the screenshot.

(2 marks)

Yes, the malware tries to connect to the network. It tries to connect to the domain spywaredb3.2squared.com

Application

Description automatically generated with medium confidence

1. Based on basic static and basic dynamic analysis performed, identify TWO important network-based indicators of this malware? Screenshot not required.

(6 marks)

1. spywaredb3.2squared.com
2. virusscan.antispyware.com

Graphical user interface, text, application, email

Description automatically generated

1. Based on basic static and basic dynamic analysis performed, identify TWO important host-based indicators of this malware? Screenshot not required.

(6 marks)

1. HKU\S-1-5-21-1123561945-492894223-1957994488-1003\Software\Microsoft\Windows\CurrentVersion\Run\AdwareAlert: "C:\Program Files\AdwareAlert\AdwareAlert.exe -boot"
2. CreateFileA
3. What do you think is the purpose of the malware?

(6 marks)

The purpose of the malware is to disguise as an AdwareAlert executable and after it is downloaded on the computer it maintains persistence by manipulating the registry and running every time the host system boots. Furthermore, it also creates an internet connection to spywaredb.2squared.com most likely, receiving code or instructions from that domain to spy on the host system. As such, it is more probably a trojan program that wants to spy on the use by disguising itself as an Adware alert programme.

**\*\* End of paper \*\***