**MALWARE ANALYSIS TOOLS and TECHNIQUES**

**PRACTICAL TEST 1**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | Tan Jia Shun | **Date** | Week 4 (9 -13 Nov) |
| **Student ID** | S10198161 | **Duration** | 1.5 hours |

**Instructions**

1. Copy the malware malware.zip from the desktop to the virtual machine.

The password for the malware is ‘Infected2020’ (without the quotes)

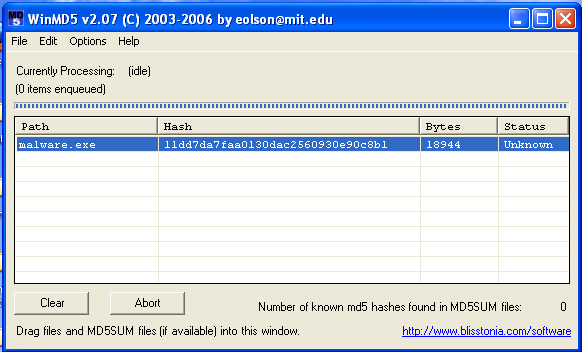
The malware is called malware.exe

1. You are to answer the questions below by performing basic static analysis and basis dynamic analysis on the malware. Upload your answers on MeL.
2. The total marks for this paper is **50 Marks**.

**Questions**

1. What is the hash of the malware? Provide the screenshot.

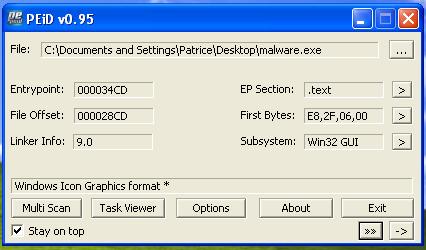
(2 marks)



11dd7da7faa0130dac2560930e90c8b1

1. Is the malware packed? What compiler/packer was used? Provide the screenshot and justify your answer.

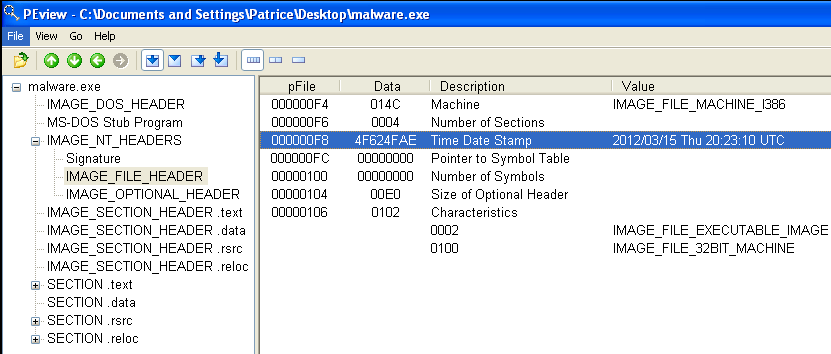
(4 marks)



The malware is not pack. It use windows icon graphics format \*

1. When was this malware created? Provide the screenshot.

(2 marks)



1. State TWO important DLLs that the malware imports. For each 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)

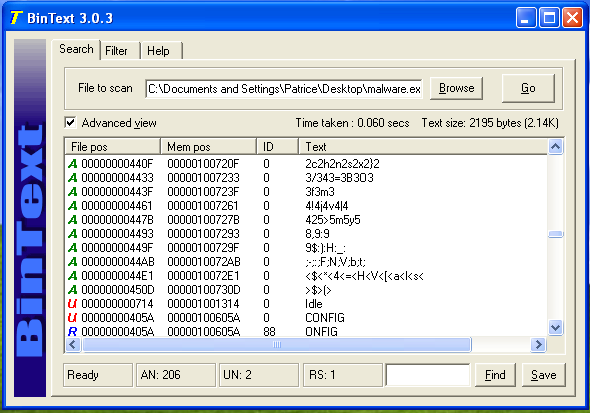
|  |  |  |  |
| --- | --- | --- | --- |
| **DLL Name** | KERNEL32.dll | | |
| **Function 1** | | | |
| **Name** | CopyFilaA | **Ordinal Number** | 63 |
| **Function 2** | | | |
| **Name** | CreateFilaA | **Ordinal Number** | 79 |
| **Purpose of DLL** | | | |
| The dll is use to create a file and move of file | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **DLL Name** | WININET.dll | | |
| **Function 1** | | | |
| **Name** | HttpOpenRequestA | **Ordinal Number** | 85 |
| **Function 2** | | | |
| **Name** | InternetConnectA | **Ordinal Number** | 111 |
| **Purpose of DLL** | | | |
| The dll is use to allow the application to access the internet | | | |

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)



String 1:

Software\Microsoft\Windows\CurrentVersion\Run

This string tell us that the malware may try to open Run or trying to override Run

String 2:

POST

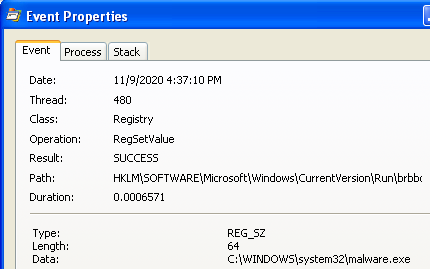
This string tell us that the malware may do a post request to a website

**Basic Dynamic Analysis**

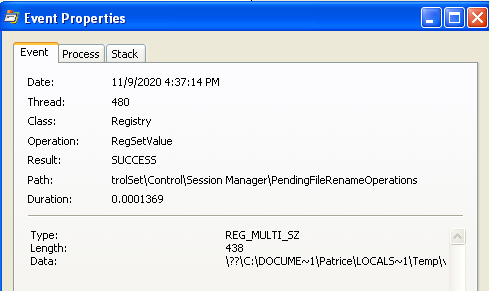
To answer the following questions, you will need to prepare the necessary tools and execute the malware.

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

(4 marks)



This registry change so that Run will know the path to the new malware.exe path

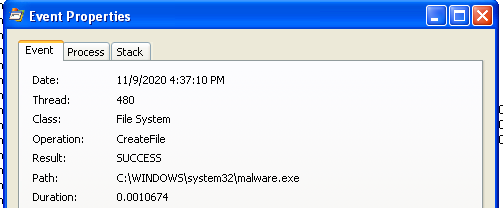


This registry change show that the malware set a filename operation in the session manager so

That everytime the device is on, it will do a file rename operation for the malware

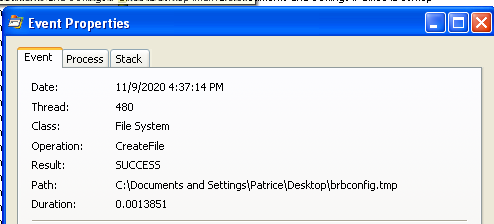
1. Was any file created on the system? If so, what is the filename? Provide the screenshot.

(2 marks)



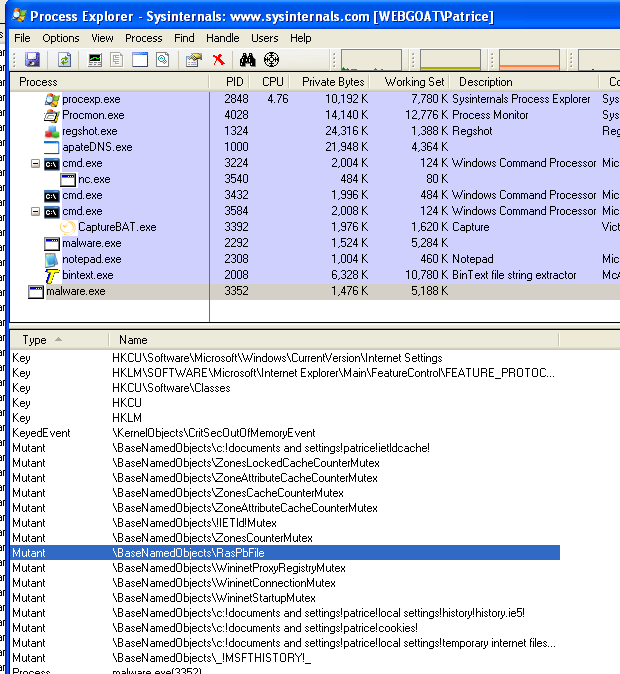
Yes, malware.exe is created in system32 folder

Brbconfig.tmp is also created



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

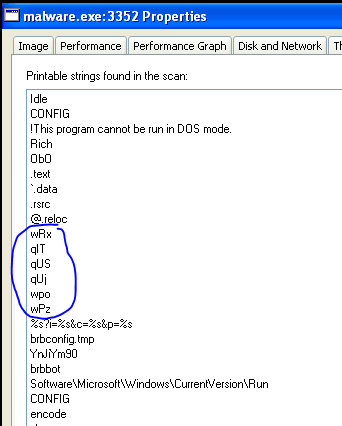
(2 marks)



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

(4 marks)

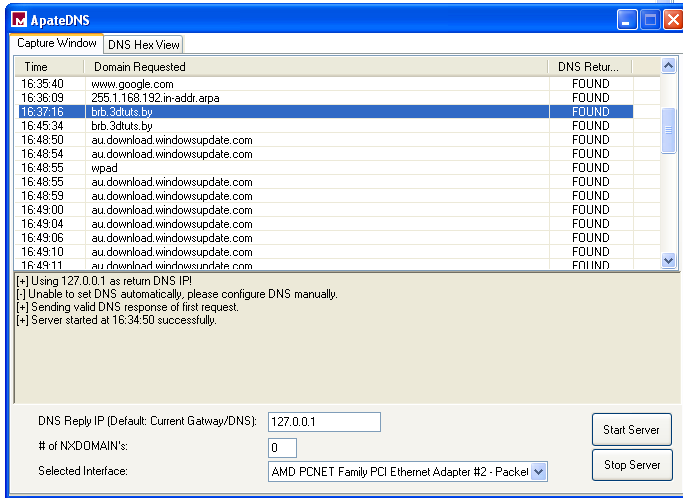
There is some change in the string as shown in the image



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

(2 marks)

It try to connect to brb.3dtuts.by



1. Based on basic static and basic dynamic analysis performed, what are some network-based indicators of this malware? Screenshot not required.

(6 marks)

brb.3dtuts.by

Mozilla/4.0 (compatible; MSIE 8.0; Wimdows NT 6.1; Tident/4.0)

HTTP/1.1

GET

POST

1. Based on basic static and basic dynamic analysis performed, what are some host-based indicators of this malware? Screenshot not required.

(6 marks)

WININET.dll

KERNEL32.dll

Brbconfig.tmp

Software\Microsoft\Windows\CurrentVersion\Run

HttpOpenRequestA

Sleep

1. What do you think is the purpose of the malware?

(4 marks)

The malware is a malware that check where is your location and send the information to a website.

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