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

Use WinMD5.

Table

Description automatically generated

Ans: 11dd7da7faa0130dac2560930e90c8b1

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

Use PEiD

Graphical user interface, application

Description automatically generated

The malware is not packed. The compiler used was Windows Icon Graphics Format \*. The file is not packed because the EP section is “.text” and the compiler Windows Icon Graphics format is not a packer.

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

Use PEView

Graphical user interface, text, application, email

Description automatically generated

This malware was created on 2012/03/15 Thu 20:23:10 UTC

4. 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.

Use Dependency Walker

Table

Description automatically generated

One imporant DLL that the malware imports is the KERNEL32.DLL. Two significant functions that the malware imports include CreateProcessA (Ordinal No: 99) and CreateFileA (Ordinal No: 80). The DLL is being used to create or open files and processes on the host system.

Table

Description automatically generated

One important DLL that the malware imports is the WININET.DLL. Two significant functions that the DLL imports are InternetConnectA (Ordinal Number: 231) and InternetReadFile (Ordinal Number: 277). The purpose of the malware is to connect to the internet and read/use files from it.

5. 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.

Use BinText

Graphical user interface, application, Word

Description automatically generated

1. Software\Microsoft\Windows\CurrentVersion\Run. It shows that the malware is trying to install itself into this directory which will make the malware run everytime the computer is turned on.
2. Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0). It shows that the malware is trying to connect to the intenet using a web browser which is Mozilla in this case.

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

Text, letter

Description automatically generated

The malware installed brbbot into the CurrentVersion\Run\ directory which indicates that the malware wants to be persistent and ran every time the system is booted up.

Text

Description automatically generated

The malware also manipulates the PendingFileRenameOperations which indicates the possibility that the malware wants to rename itself everytime the system boots up to make it even more persistant as it will be more difficult to find.

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

Graphical user interface, text

Description automatically generated

Yes, there were files created on the system. The filenames are brbconfig.tmp, MALWARE.EXE-009EA6F4.pf, and malware.exe

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

A picture containing table

Description automatically generated

Yes there is a mutex created. The mutex’s name is RasPbFile, \BaseNamedObjects\RasPbFile.

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

Graphical user interface, application

Description automatically generated

There a changes in the string after running the malware, the changes start below the line @.reloc in the image.

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

Graphical user interface

Description automatically generated with medium confidence

Text

Description automatically generated

The malware tries to connect to the network. It attempts to connect to the domain brb.3dults.by.

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

Brb.3dults.by

Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0)

HTTP/1.1

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

CreateFileA

CreateProcessA

Software\Microsoft\Windows\CurrentVersion\Run  
HKLM\SYSTEM\ControlSet001\Control\Session Manager\PendingFileRenameOperations

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

The malware upon infection of a system will install itself into the directory Software\Microsoft\Windows\CurrentVersion\Run as well as change the registry HKLM\SYSTEM\ControlSet001\Control\Session Manager\PendingFileRenameOperations to make itself persistent. It also connects to the internet and creates a backdoor to a domain brb.3dults.by