**Questions & Answers**

**for**

**Malware Analysts**



**Presented By,**

Bashetty Arun Kumar

Master of Computer Security

EPITA-2018

**Questions for Malware Analysts:**

1.what are the characteristics of the sample?

* + PEiD,
  + CFFExplorer,
  + Strings,
  + sha256sum,
  + md5sum

2- how does the sample survive to reboot?

3- what is the CnC IP/domain name?

4- what are the create/dropped files on disk?

5- what does it do?

6- how to clean the system?

=>After research I found that the given file is netmon.exe.

**What is netmon.exe?**

1. netmon.exe is a process which is registered mass-mailing worm.
2. Non-system processes like netmon.exe originate from software you installed on your system.
3. Since most applications store data on your hard disk and in your system's registry, it is likely that your computer has suffered fragmentation and accumulated invalid entries which can affect your PC's performance.
4. The netmon.exe is an executable file on your computer's hard drive. This file contains machine code. If you start the software Trojan.W32.MIMAIL on your PC, the commands contained in netmon.exe will be executed on your PC
5. For this purpose, the file is loaded into the main memory (RAM) and runs there as a Trojan.W32.MIMAIL process (also called a task).

**Is netmon.exe harmful?**

**Warning!** netmon.exe is considered to be a dangerous process and should be removed. Running issues with this process can increase the risk of malware infection if bugs are present.

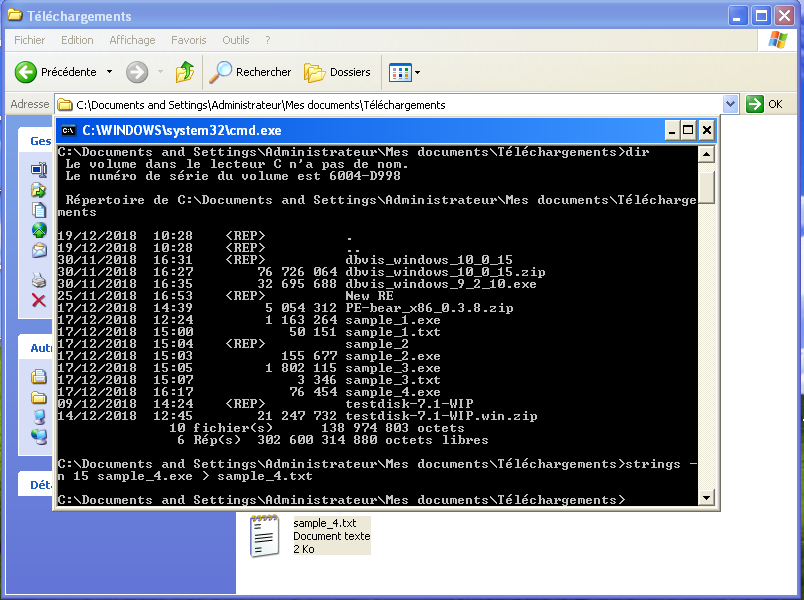
**Process name:** Trojan.W32.MIMAIL

**What are the characteristics of the sample?**

**Strings:**

Before converting to strings, you have to download application from <http://www.adeleda.com/epita/malwares/exercises/>

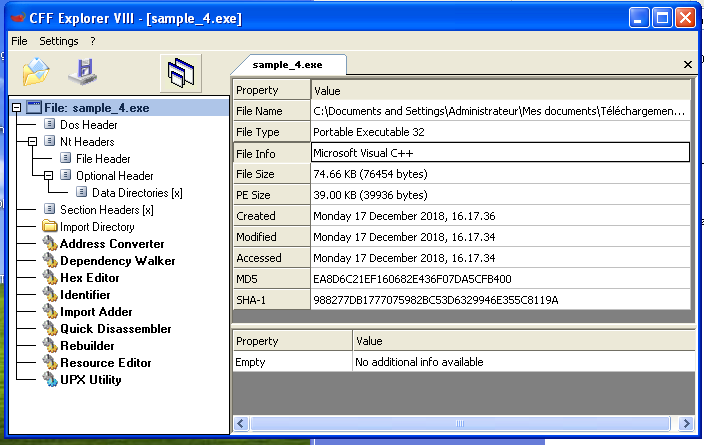
and change the extension to .exe

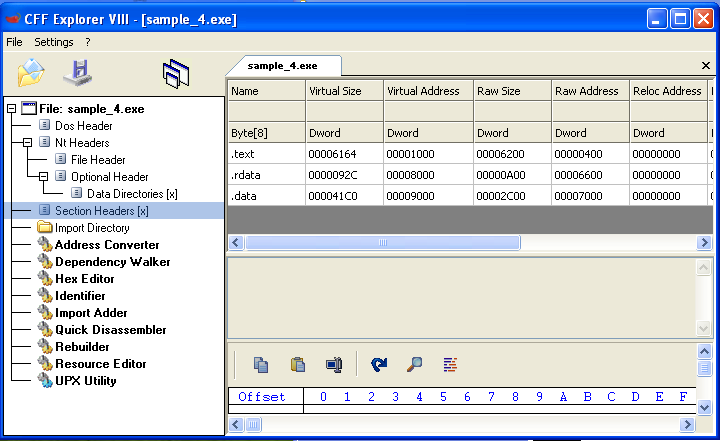


After changing the extension, open the cmd from windows option and give a path, that where you downloaded your file.

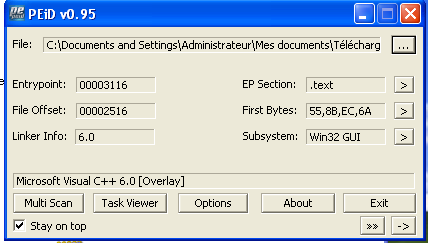
After that use strings command and create a new file name and save the strings.

**CFF Explorer:**

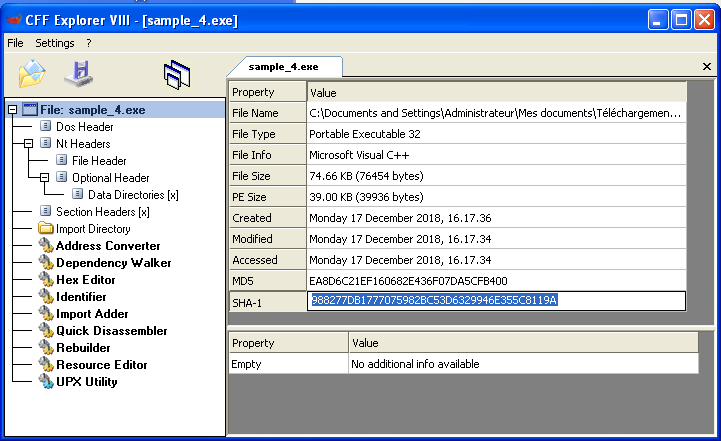




**PEiD:**



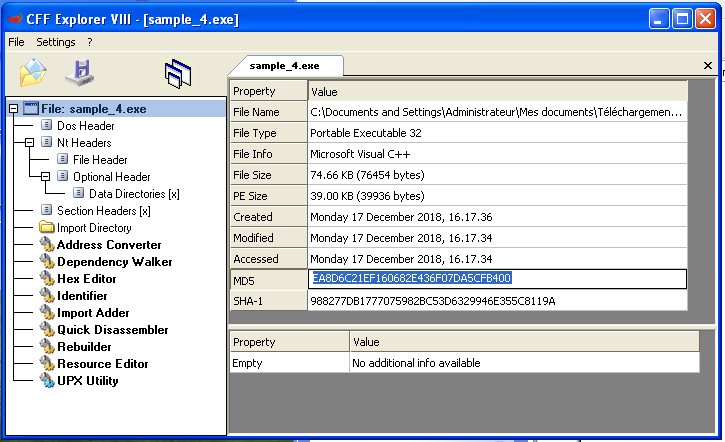
**Sha256sum:**



After importing the file in CFF explorer, you can see MD5 and SHA-1 passwords.

**Md5:**

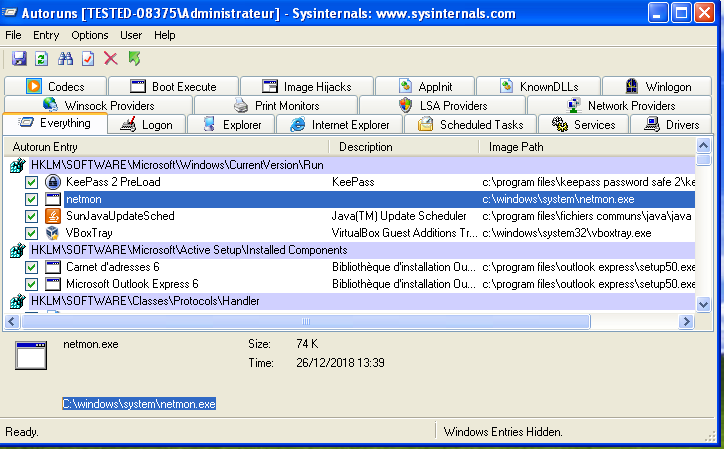
MD5hashis contain 32 bits and it will display above on SHA-1.



**What are the create/dropped files on disk?**

=>After downloading file from website, I changed the extension to .exe,

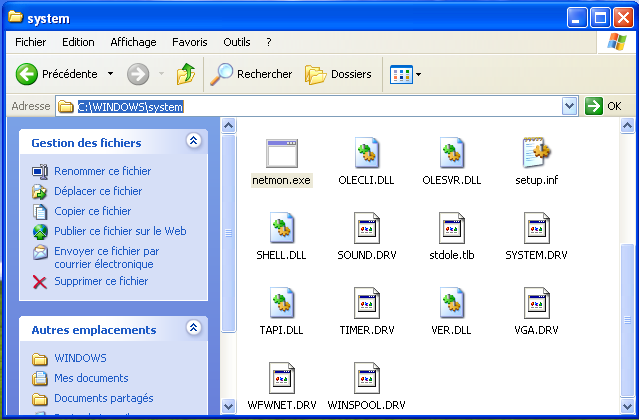
=>When I clicked on malware application, it automatically hides from download folder



=>I opened autorun and checked the location.

We can see the netmon.exe file inside the below path.

C: WINDOWS/system/netmon.exe

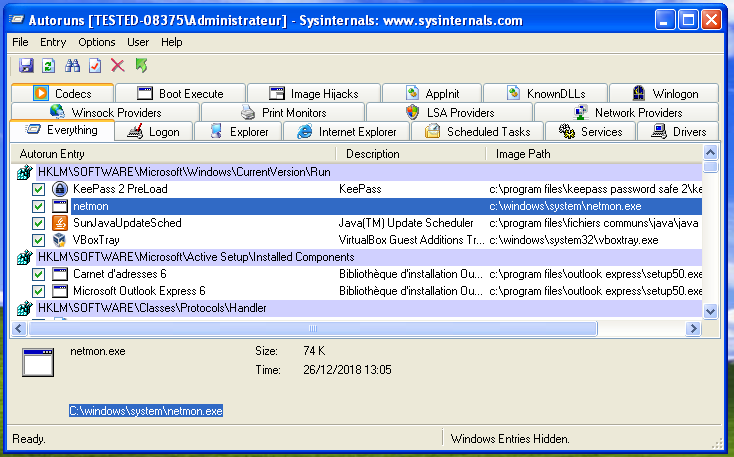


**How to clean the system?**

netmon.exe is most likely a virus or Trojan, in which case it should be stopped or removed immediately.

To remove this malware from your system, you have to use Autorun software.

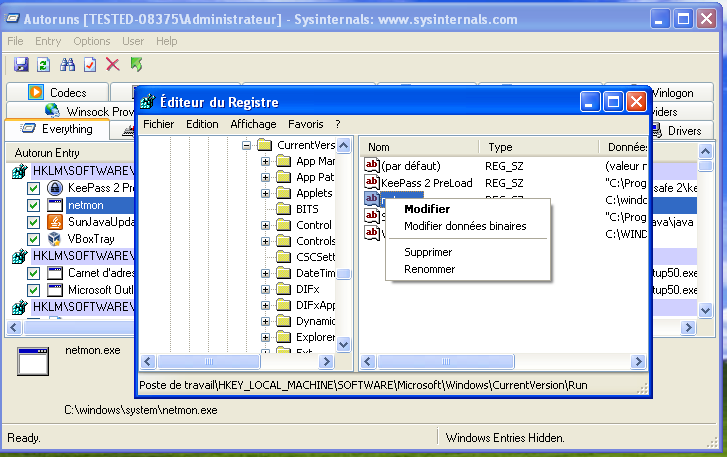
After opening this application, you can see the file that look different to you, here I found NetMon file is looks like different and I must delete it.



You can remove this file by using 2 steps,

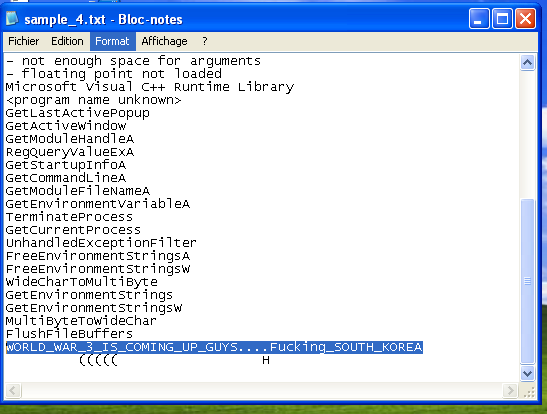
First one, you can right click on malware file and you can see the options for delete, click on delete and the malware is deleted from your system

Second one, you can double click on malware and it will display below screenshot.



Right click on netmon folder and it will display some option, click on supprimer, this malware will remove from your system.

Finally, I Found for this netmon.exe file contain secret information,



***This is the end of the report***