**Malware analysis of Pony malware**

**Pony malware**, also known as Pony Stealer, Pony Loader, FareIT and a few other names is a password stealer that can decrypt or unlock passwords for over 110 different applications including VPN, FTP, email, instant messaging, web browsers and much more. Pony Stealer is very dangerous and once it infects a PC it will turn the device into a botnet, allowing it to use the PCs it infects to infect other PCs.

**Requirements:** Pony malware sample: <https://gusindia01-my.sharepoint.com/:f:/g/personal/keshavkaushik_ddn_upes_ac_in/EuctZN-vFEpNicFWH20ZD0oBMUOpzK_0TVcFizvGJ69elw?e=qnLdLd>

**Things to check for the environment you shall be working in:-**

* Updated Virtual box
* Set network configuration to host-only mode
* Do not use any USB while performing analysis
* Make sure you keep the malware in protected mode
* Open the malware only in VM
* Disable shared folders

**Tools:**

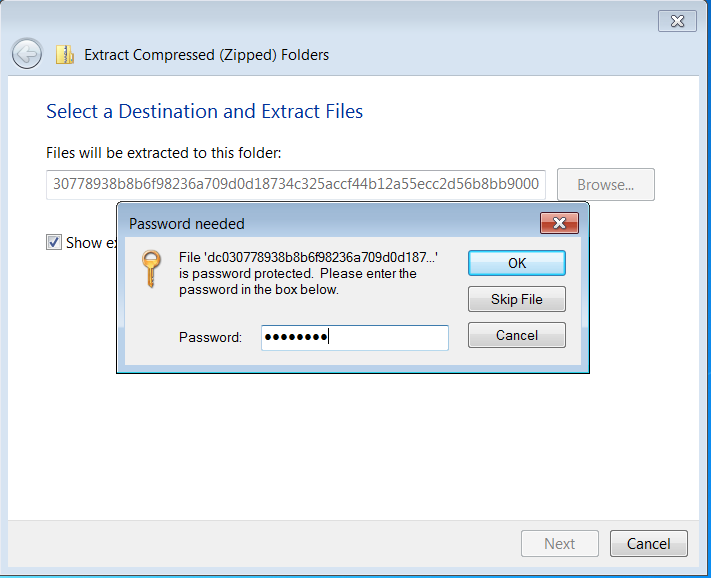
• **HxD:** HxD is a powerful Hex Editor that we will use in this experiment to analyze our Malware. HxD can be downloaded at: <https://mh-nexus.de/en/hxd/>

• **PeStudio**: PEInfois a utility to query bulk file information for researching. PeStudio can be downloaded at: <https://www.winitor.com/>

• **ExeInfo PE:** Exeinfo PEis a program that lets you verify .exe files and check out all their properties. ExeInfo PE can be downloaded at: <https://exeinfo-pe.en.uptodown.com/windows#:~:text=Exeinfo%20PE%20is%20a%20program,exe%2C%20or%20simply%20delete%20it.&text=In%20short%2C%20you%20can%20access,edit%20any%20Windows%20executable%20file>

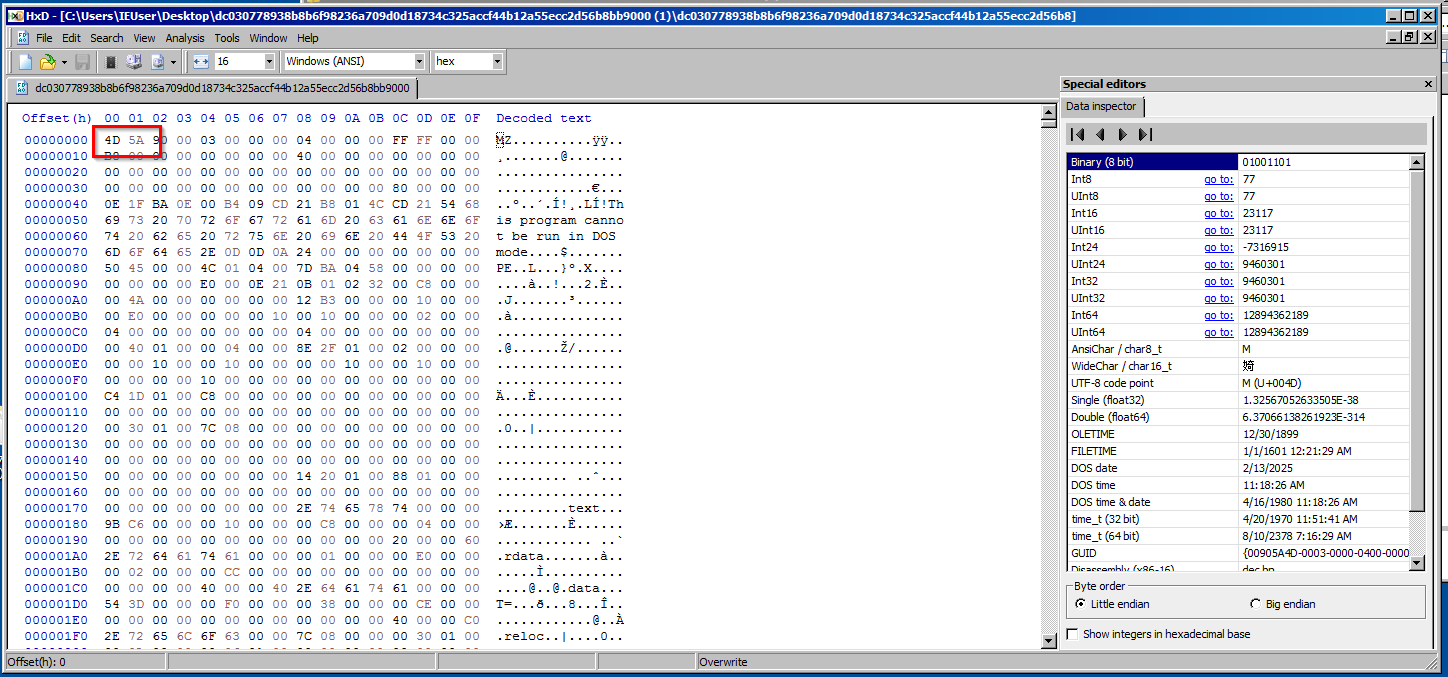
**Analysis**

**Unzip the file with password – infected**



**1** **HxD**

* Opening the malware in HxD hex editor. We will notice that at beginning of the decoded test, 4D 5A is mentioned. 4D 5A means that the file is a portable executable(PE) which is similar to windows exe files like .exe or .dl.
* We can also see there is a string in the decoded text which says that “program cannot be run in DOS mode”.

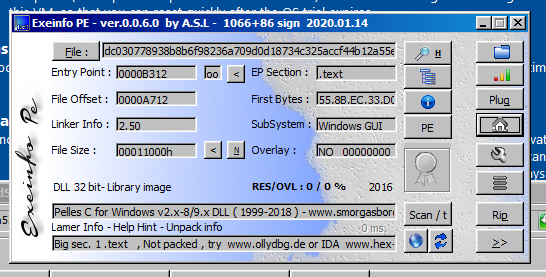




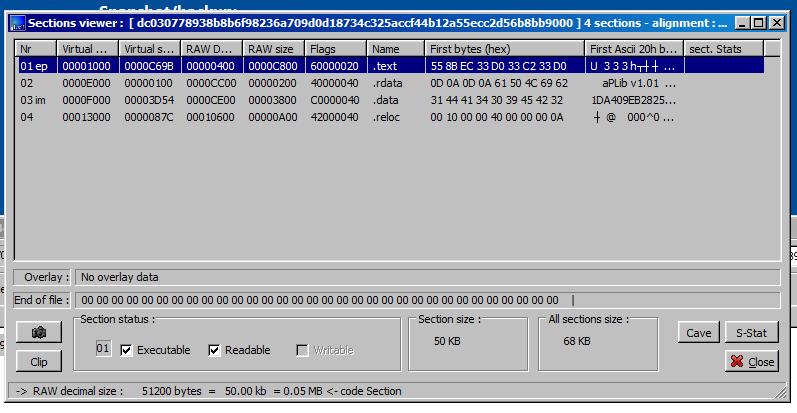
4D 5A indicates it’s a PE File along with the decoded text as the proof of it being a PE file. “This program cannot be run in DOS mode” is its property.

**2 Exeinfo PE**

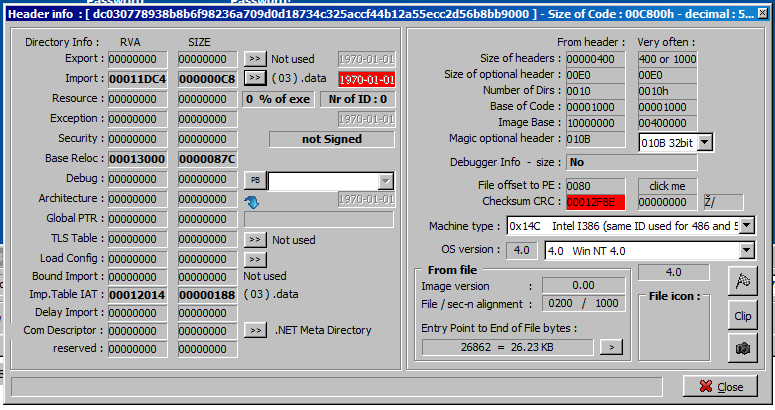
* Open the malware using ExeInfo PE.



* We observe that in the last pane of the window, packing information has been displayed and the status says “Not packed”, which means no packer has been in used on the malware to change, hide it signature.
* A more detailed look of the section viewer.

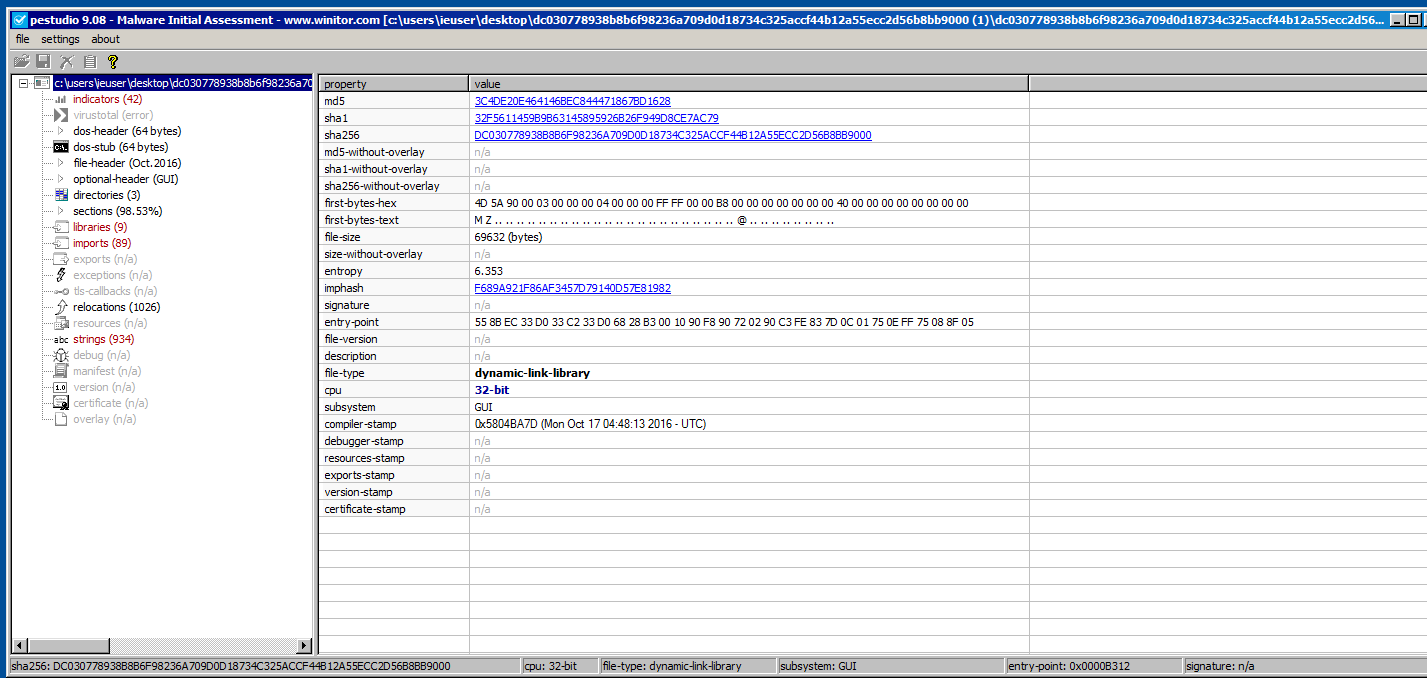


* We can navigate to the PE header section to see information like the number of directories, version, Machine type, Size of headers etc.

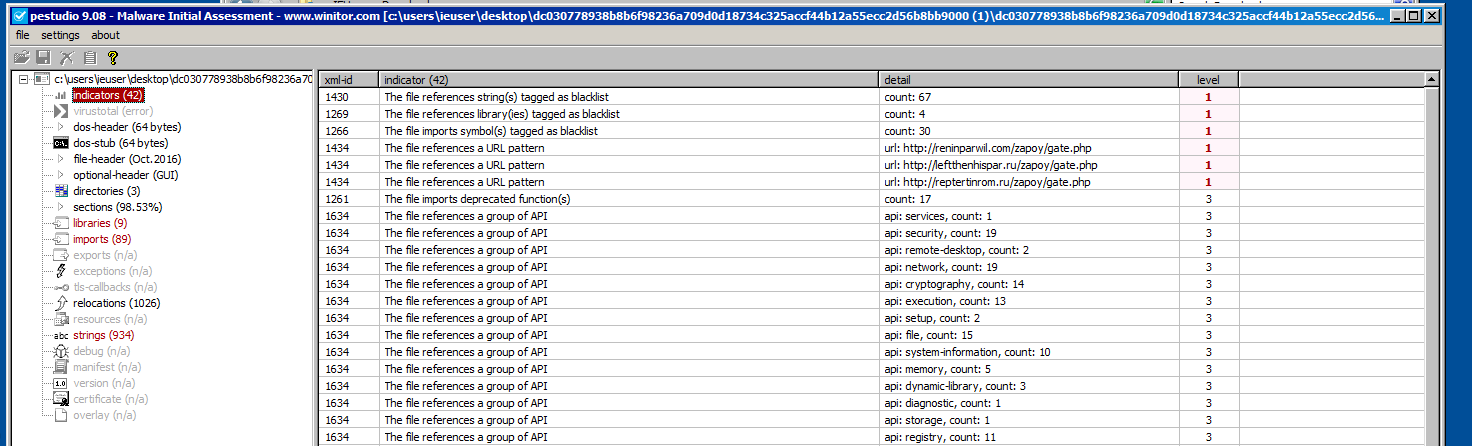


**3 PEstudio**

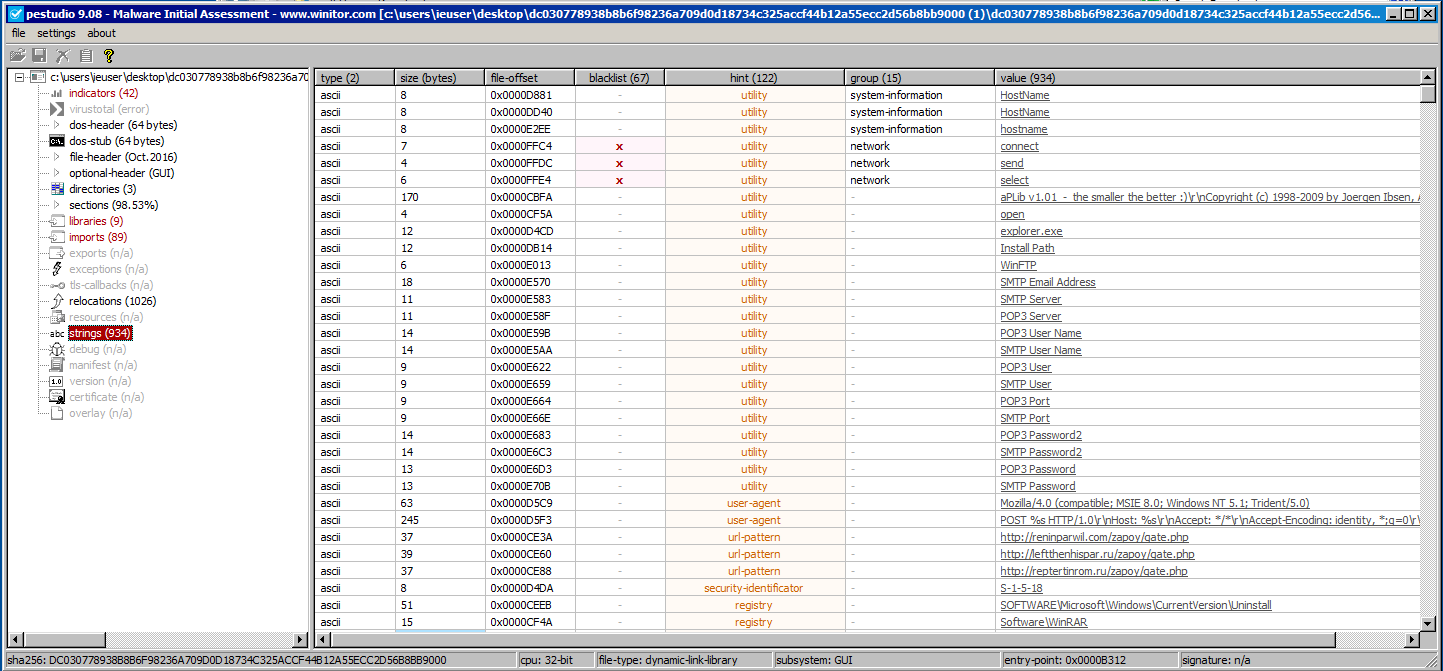
* Opening the malware using PE studio.



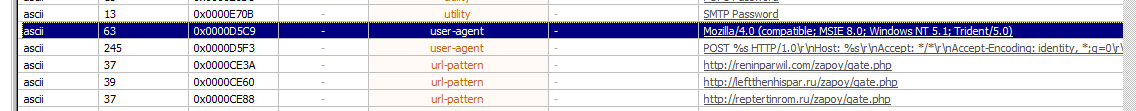
* We will navigate to all the section that are highlighted in red that contains useful info or that are suspicious.
* Navigating to the “indicators” section. Which tell us why it thinks the file is suspicious. These are some backlisted file referencing objects and accessing URLs. That could be a clue that the information collected are sent over the internet.



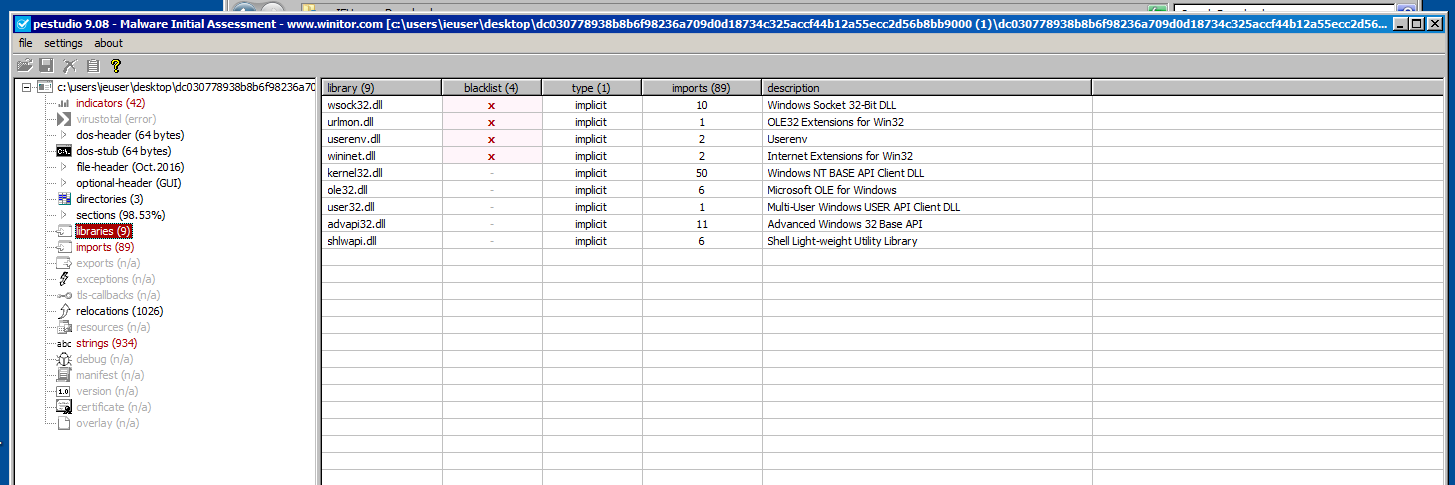
* Checking the String section which tell us all the suspicious strings detected by the tool.



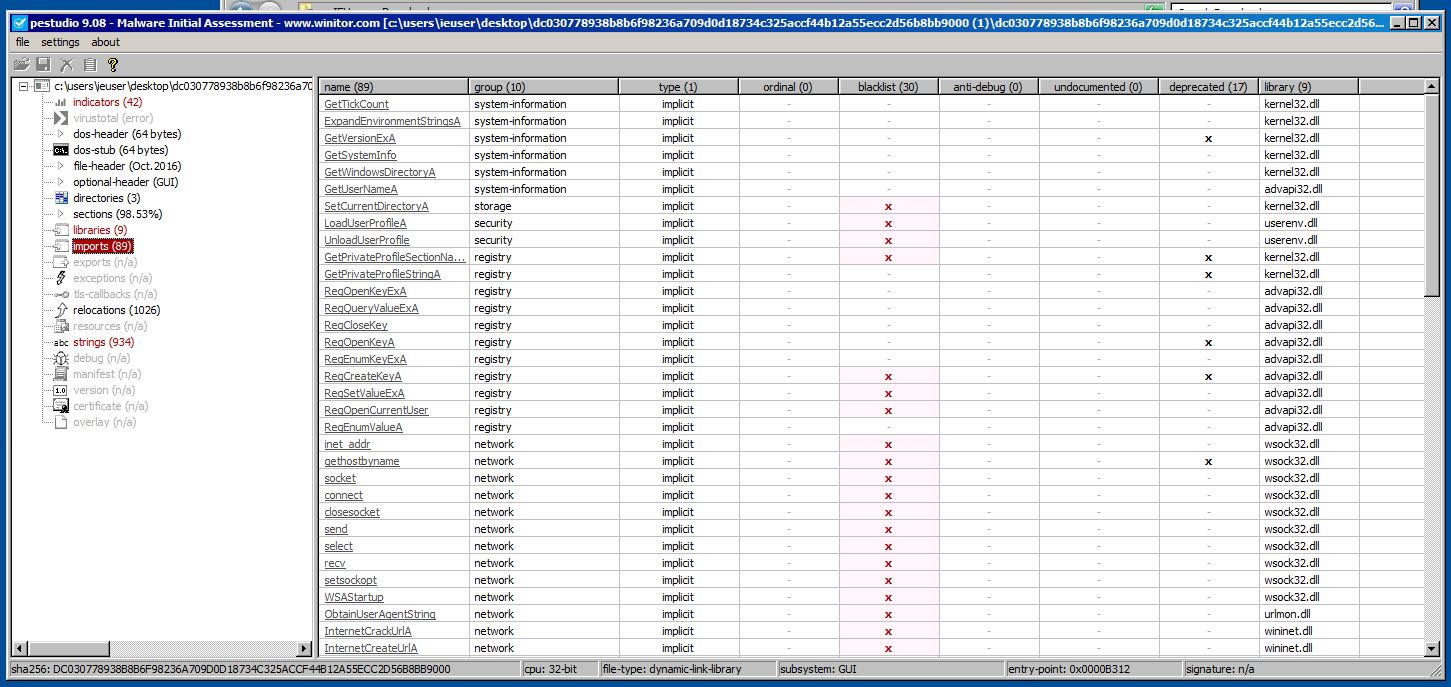
* We can see that requests had been made to access URLs with fire-fox browser.



* Navigating to the libraries section which contains the list of libraries being accessed by the file.



* Navigating to the imports section which shows a list containing some import functions that are considered malicious by the tool.



* Checking the file with virus-total at: <https://www.virustotal.com>

which shows that the malware is been detected by 63 different antiviruses.

