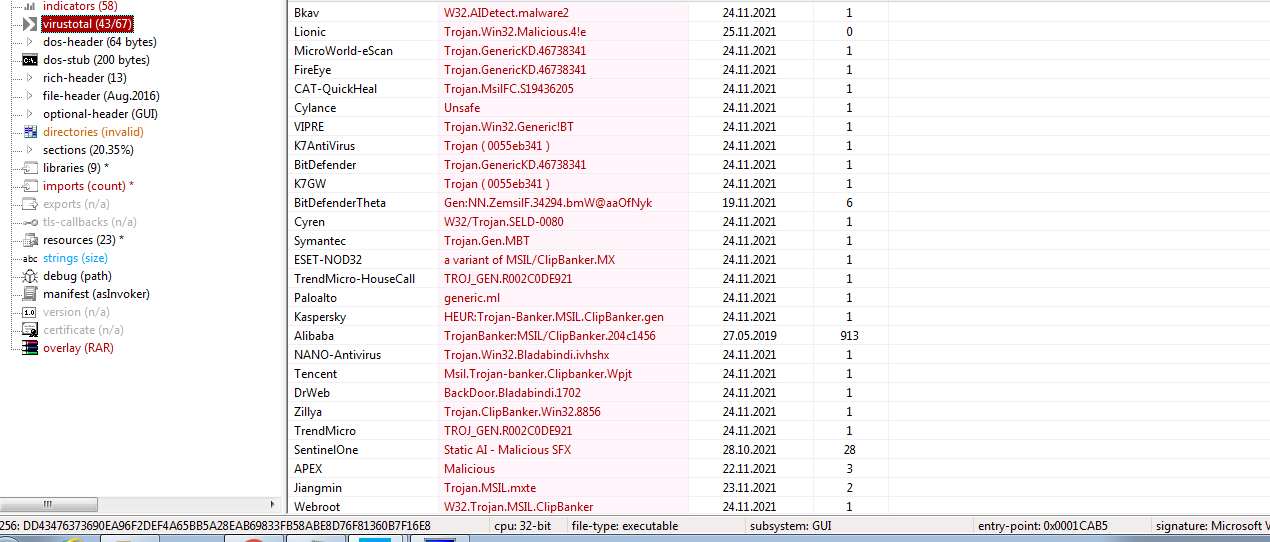
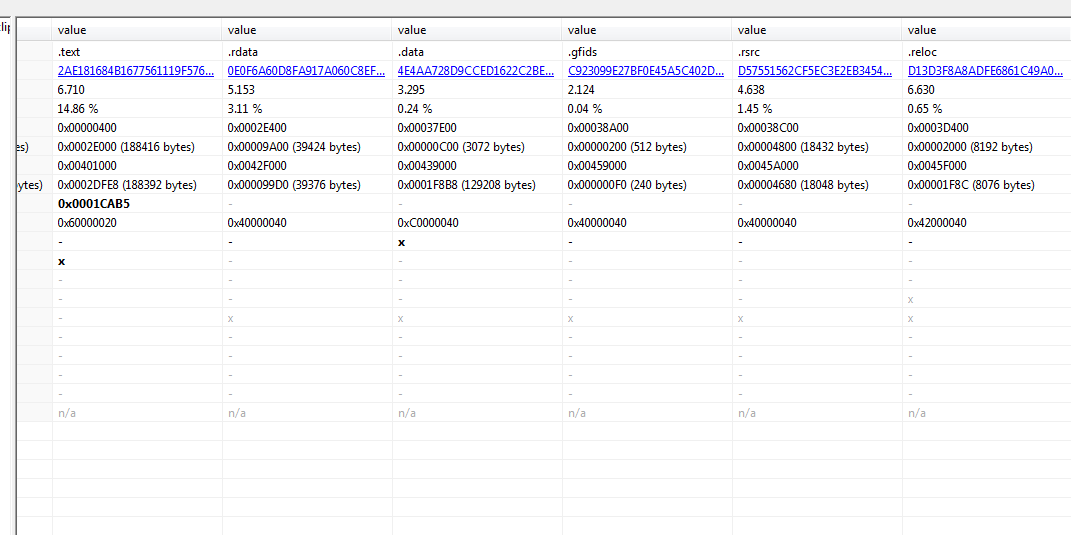
­SHA256: dd43476373690ea96f2def4a65bb5a28eab69833fb58abe8d76f81360b7f16e8

Sample report link: [dd43476373690ea96f2def4a65bb5a28eab69833fb58abe8d76f81360b7f16e8 | ANY.RUN - Free Malware Sandbox Online](https://any.run/report/dd43476373690ea96f2def4a65bb5a28eab69833fb58abe8d76f81360b7f16e8/825b9e75-e715-4b66-895f-296622c8a855)

Analysis using pestudio:

Many vendors showing it as trojan/ clip banker.

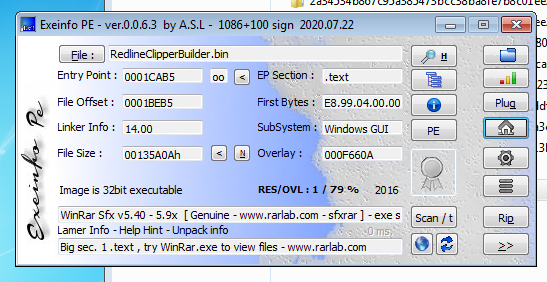




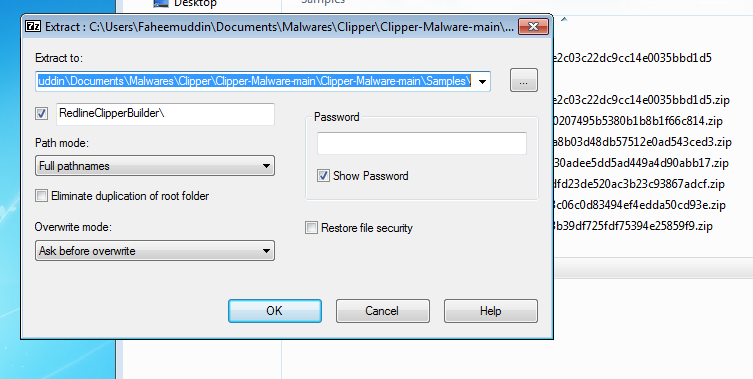
**Analysis using Exeinfope Shows that the file is SFX.**

A **self-extracting archive** (**SFX/SEA**) is a [computer](https://en.wikipedia.org/wiki/Computer) [executable program](https://en.wikipedia.org/wiki/Application_software) which contains compressed data in an [archive file](https://en.wikipedia.org/wiki/Archive_file) combined with machine-executable program instructions to extract this information on a compatible operating system and without the necessity for a suitable extractor to be already installed on the target computer.

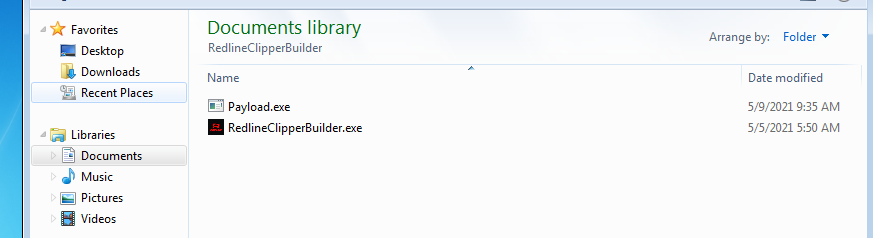
So we can use winrar or 7 zip to extract it’s actual contents.



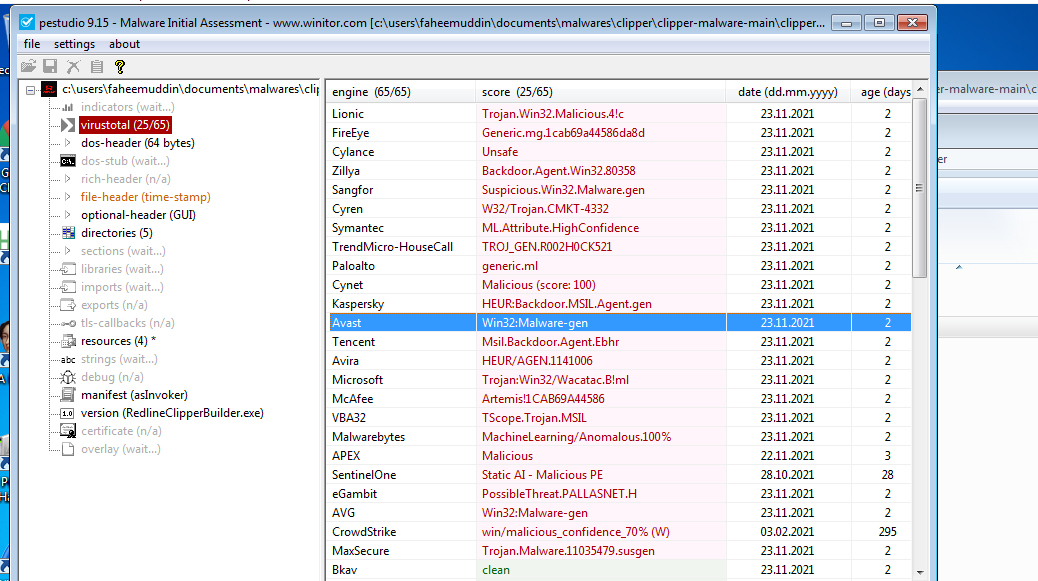
**Extracting using 7zip**



**The extracted folder has two files:**

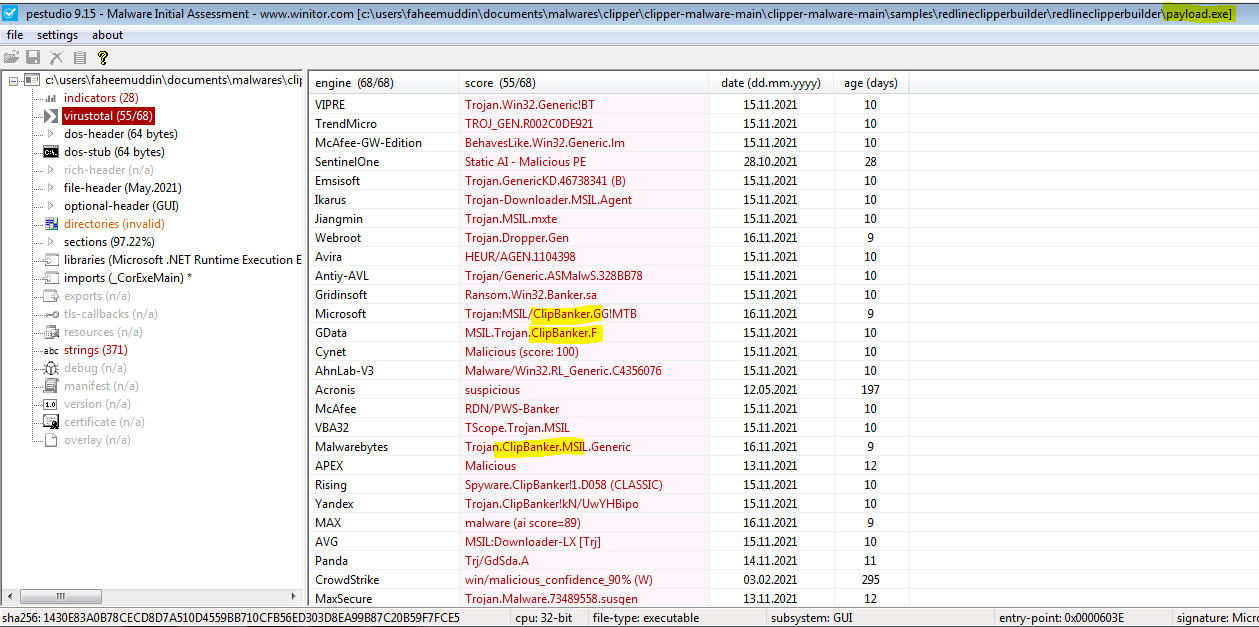


**The redlineclipperbuilder.exe is detected as trojan on virustotal**

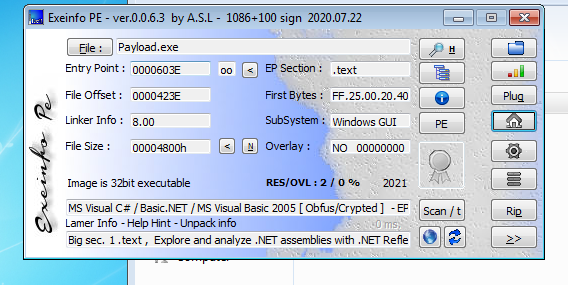


The payload.exe is detected as a Trojan/Clipbanker application. We will thus use payload.exe for further analysis.

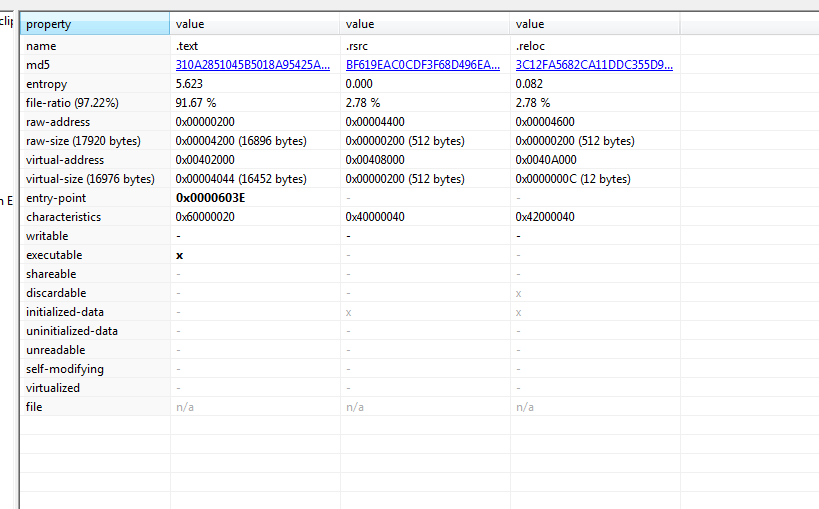
Payload.exe SHA256: 1430E83A0B78CECD8D7A510D4559BB710CFB56ED303D8EA99B87C20B59F7FCE5



The payload.exe is compiled using visual C# language

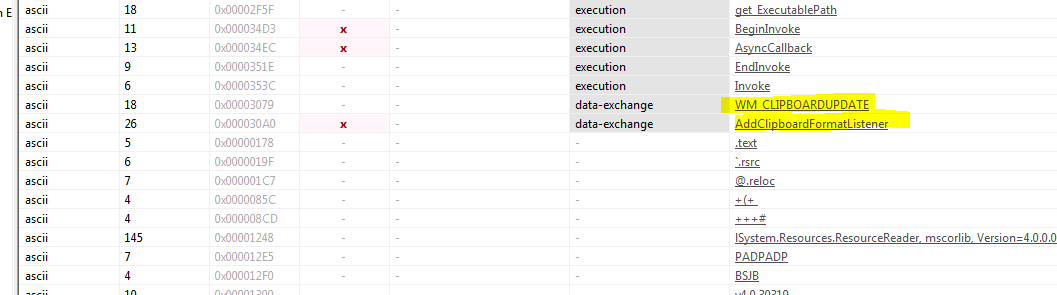


The data in the payload.exe is not obfuscated and thus can be analyzed directly using dot net unpackers.

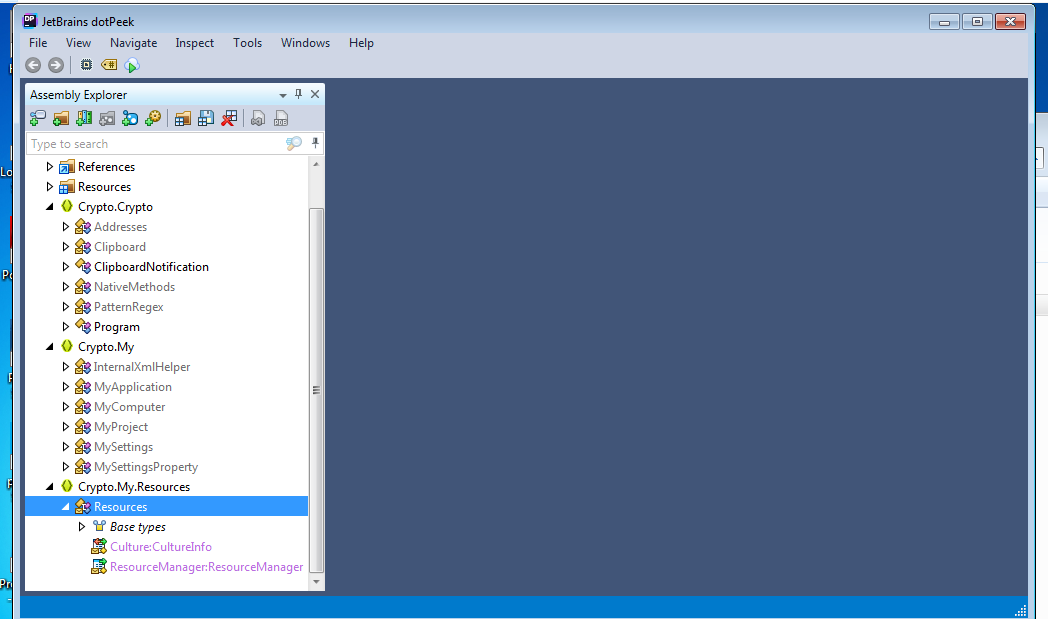


The strings in the payload.exe indicates that there is activity of clipboard update and control





Opened the payload.exe using dot net peak



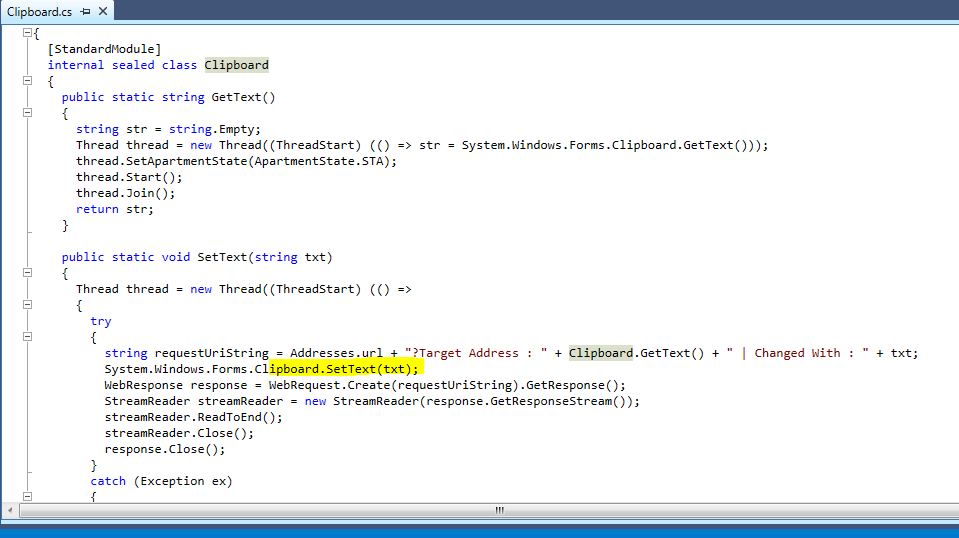
Found Class Addresses related to multiple cryptocurrencies.

This is used to declare public address which can be called and used to replace the clipboard content.

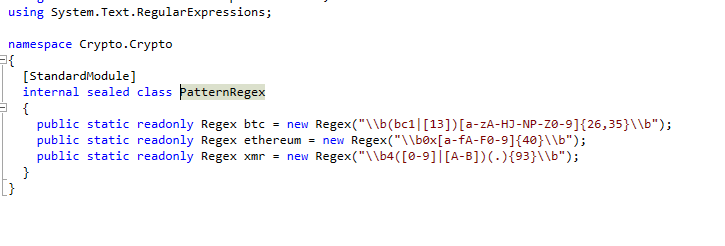


The clipboard class:

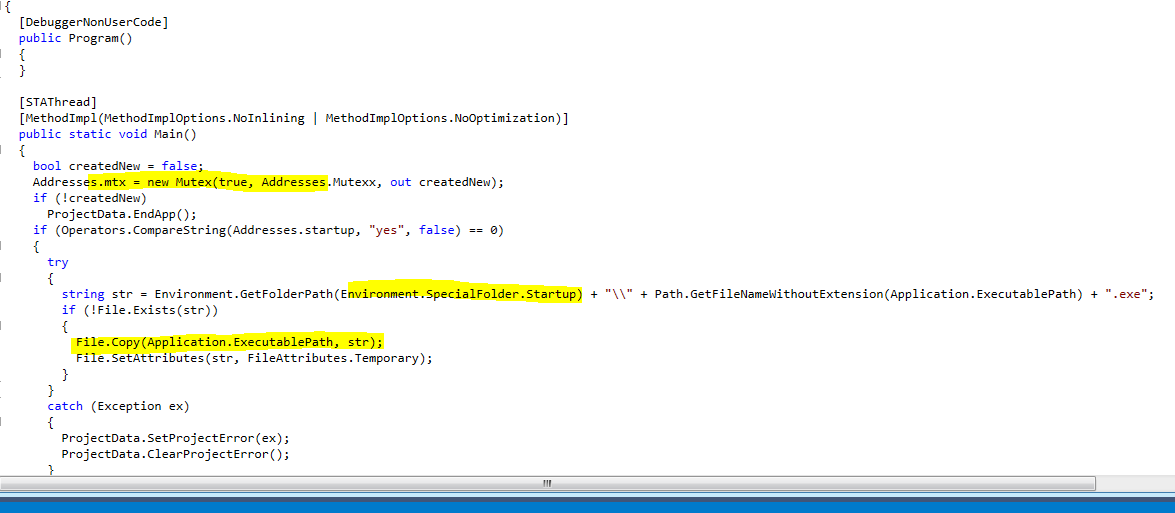
It is capturing clipboard data from victim and sending a request with it’s clipboard contents to compromised url which is available in Addresses class.



This part of the code is used to match Regex patterns to detect which type of crypto currency address was copied to clipboard. Once matched, it can then use address in Addresses class to replace it with matched cryptocurreny address of the attacker.



The program.cs class shows that the payload is creating a mutex object and then copying application to startup folder

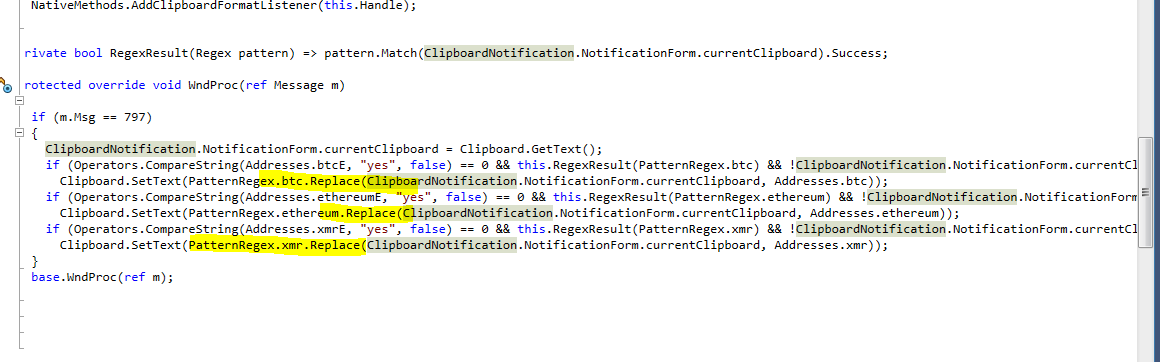


For matched patterns it is replacing the addresses with the attackers address using Replace function. So if the data in clipboard matches bitcoin address. Then it is replaced with attackers address using the below line of code:

Clipboard.SetText(PatternRegex.btc.Replace(ClipboardNotification.NotificationForm.currentClipboard, Addresses.btc));

The same applies to other crypto addresses.

Attackers address are accessed using Addresses.btc, Address.ethereum, Addresses.xmr etc.



# Summary:

Based on above analysis:

The file if executed will:

1. Will Self-Extract itself and install a different application name payload.exe and Redlineclipperbuilder.exe.
2. The payload.exe will create a mutex and copy itself to startup folder so that it can execute itself after system restarts/shutdowns.
3. Controls the contents of the clipboards
4. Sends the contents of the clipboard to a url.
5. Tries to match clipboard contents to known list of crypto currency addresses.
6. Replaces the cryptocurrency addresses with its own addresses.