**A**

**REPORT ON**

**CLIPPER MALWARE FAMILY**

SUBMITTED BY

ARJUN ANIL

MOHAMMAD FAHEEMUDDIN

Table of Contents

[Introduction 3](#_Toc89085005)

[How it Works 3](#_Toc89085006)

[Potential Capabilities of the Malware Family 3](#_Toc89085007)

[Different Clippers Available 4](#_Toc89085008)

[Prosto Clipper 4](#_Toc89085009)

[Redline Clipper/Stealer 4](#_Toc89085010)

[Extended Clippers 5](#_Toc89085011)

[E- Clipper 5](#_Toc89085012)

[Android.C Clipper 6](#_Toc89085013)

[Masad Clipper 7](#_Toc89085014)

[Malware Families Close to Clipper Family 9](#_Toc89085015)

[Arkei 9](#_Toc89085016)

[Immortal Information Stealer 9](#_Toc89085017)

[Kpot 10](#_Toc89085018)

[Predator 11](#_Toc89085019)

[Rarog 11](#_Toc89085020)

[Revenge Malware 11](#_Toc89085021)

[Vidar Malware 12](#_Toc89085022)

[Static Analysis of E-Clipper 12](#_Toc89085023)

[Detailed Analysis of Masad Clipper 15](#_Toc89085024)

[Summary 22](#_Toc89085025)

[Detailed Analysis of Red Line Clipper Stealer 23](#_Toc89085026)

[Red Line Clipper Stealer in Action 31](#_Toc89085027)

[Summary 31](#_Toc89085028)

[Detailed Analysis Prosto Clipper 31](#_Toc89085029)

[Summary 39](#_Toc89085030)

[Yara Rule 40](#_Toc89085031)

[A Comparison of Clipper Family with other types of Malwares 42](#_Toc89085032)

[Comparison of Malware Types 42](#_Toc89085033)

[Comparison of Popularity and Sales 43](#_Toc89085034)

[Cost Comparison 43](#_Toc89085035)

[Possible Solutions 44](#_Toc89085036)

[Conclusion 45](#_Toc89085037)

[References 45](#_Toc89085038)

# Introduction

Cybercriminals have been deploying a type of malware known as “Clipper” malware, which hijacks a user’s clipboard. Clipper malware is designed to steal cryptocurrency from victims by replacing wallet addresses in the victim’s clipboard with wallet addresses that belong to the attacker. This stealthy technique is designed to silently trick the victim when making what appears to be a legitimate cryptocurrency transaction, which results in the attacker becoming the new recipient of that transaction. This attack is not especially common, but it does happen in both Bitcoin and Ethereum, and it’s important to be aware of it. Because sometimes you actually are infected, and the addresses are not the same.

The Clipper malware first started out in 2017 and was spotted on the Windows platform before appearing on underground hacking forums for sale in August 2018. Clippers are also sometimes called as Clipboard Hijackers. Some stealers like Raccoon Stealers extend and upgrade their functionality to support clipboard activities and crypto currency address changes.

There are different Clipper Malwares discovered which work mostly for windows and Android operating systems. We will analyse few samples in this paper using Static, Dynamic and Code Analysis Methods.

# How it Works

The clipboard is a buffer in operating systems used to temporarily store data while it is moved (typically, copied) from one place to another. For example, data copied from a document is stored in the clipboard so that users can then paste it to another, perhaps different, document.

In this particular case, cyber criminals use Clippers to replace the cryptocurrency wallet addresses that are copied to the clipboard with addresses of other wallets. Since the public addresses of cryptocurrencies is a hash of certain type, it is most often 128 or 256 bits. Thus, many people make transactions by entering their wallet addresses and copy them to the clipboard. Cyber criminals then use Clippers to replace it with another address so that unsuspecting victims transfer money to them and not the intended recipient.

People tend not to double-check wallet addresses entered, and cyber criminals then successfully trick them into making unintentional transactions. To prevent this, remove Clipboard malware immediately and double-check all addresses before making cryptocurrency transactions.

Many malicious programs are capable of replacing data saved to the clipboard. Other examples of Clipper Malware family include [Clipsa](https://www.pcrisk.com/removal-guides/15551-clipsa-password-stealer" \t "_self) ,[Qulab](https://www.pcrisk.com/removal-guides/15398-qulab-stealer" \t "_self), Apocalypse, Prosto, Extended Clipper, E-clipper, Red Line Clipper etc. Having malware such as Clipper installed on the system can lead to financial loss specifically loss of cryptocurrency and loss of personal information which the clipper would send using some form of mechanism. Cyber criminals might also use these programs to steal other personal information from the victim’s machine.

# Potential Capabilities of the Malware Family

The malware family could be capable of performing the following functions:

* Steals administrative credentials.
* Possible Keylogging functionality
* Mine and steal crypto currencies by replacing crypto addresses present in a clipboard via clipboard hijacking.
* Might sent web requests to malicious websites for clipboard data export.
* May use the same compromised websites as secondary command and control servers to host malicious files or upload stolen data.

# Different Clippers Available

In this section we will discuss few of the known clippers that are currently available and those which offer different or advanced functionality compared to conventional clippers.

## Prosto Clipper

Prosto Clipper malware is of Russian Origin which targets cryptocurrency wallets and is compatible with Windows Vista, 7, 8, 8.1 and 10 OS versions. Prosto Clipper has certain anti-detection capabilities such as hiding its presence from Windows Task Manager.

In a specific version which we have analysed, the clipper was written to stop the user from starting any of the administrative control applications like Task Manager, Process Hacker, Process monitor etc that can stop malicious activities. Also, the environment shutdown process was included to the list to stop the user from inadvertently shutting down the stop in case he wants to stop the activity.

Prosto Clipper can obfuscate its presence, which hinders detection. In addition, this malware is 'lightweight' at 50 KB and does not put a strain on system resources - this increases its chances of remaining hidden and avoiding user suspicion. Few of the commonly used obfuscators by Prosto is ConfuserEx Obfuscators which hides the classes and code content of the malware sample. This would help the malware to evade the AV detection capabilities.

Once a system is successfully infected with Prosto Clipper and users attempt to make transactions with certain cryptocurrencies, the malware replaces the crypto-wallet addresses entered to those held by the cyber criminals using Prosto Clipper.

Additionally, the modified cryptocurrency wallet addresses are encrypted some form of standard symmetric encryption techniques. The sample we analysed was using Triple DES technique to hide all the public addresses of the hacker and the use of such addresses was done using variable which would directly decrypt the value in place.

Furthermore, this malicious program is capable of sending status reports to the criminals via Telegram messenger. These reports are sent when Prosto Clipper is run and following each successful crypto wallet address swap/replacement.

In this paper, we have analysed a Prosto Clipper sample in detail to find out it’s functionality and attack methodology in victim’s machines using Static Analysis and Code Analysis. The detailed analysis is available in sections below.

## Redline Clipper/Stealer

In general, Red Line is a Stealer which is a malicious program which can be purchased on hacker forums for $150/$200 depending on the version.

It is capable of collecting system information such as IP addresses, usernames, keyboard layouts, UAC settings, installed security solutions, and other details. In addition to that, this malicious program can be also be used to infect computers with other malware. This property of this malware is used to deliver a payload executable which will be the clipper functionality and thus it takes access of the clipboard and performs its functions. The Redline Clipper is written and compiled in C#.

In this paper, we have analysed a Red Line Clipper sample in detail to find out it’s functionality and attack methodology in victim’s machine using Static Analysis and Code Analysis.

## Extended Clippers

Extended Clippers are clipper malwares which have extended functionality when compared to generic clippers. They can thus be used to replace other content as well. In few cases, the developers of such malicious program offer to substitute or add functionalities for an additional fee; hence, Extended Clipper infections can pose even more threats.

The primary functionality of Extended Clipper's basic build is digital wallet (e.g., crypto wallet) address replacement with those belonging to the individuals/groups behind the infection but they are also capable of replacing website links (URLs). This feature can be used to redirect victims to deceptive and malicious sites. For example, they can be redirected to phishing websites disguised as sign-in pages of legitimate accounts (e.g., online bank, social media, etc.).

Phishing scams operate by recording information entered into them, e.g., log-in credentials (IDs, email addresses, usernames, and passwords), personally identifiable details, finance-related data (credit card numbers, etc.), and other vulnerable information.

Alternatively, victims can be redirected to sites that offer malicious software disguised as genuine content or to ones that can stealthily infiltrate it into the system. Therefore, Extended Clipper could potentially cause trojan, ransomware, crypto-miner, and other infections.

This malicious program can replace regular expressions (regexes) as well. As mentioned in the introduction, developers of this malware offer some level of customization; hence, it is likely that the program may have additional harmful abilities.

To summarize, Extended Clipper infections can lead to severe privacy issues, significant financial losses, and identity theft.

**Sample SHA256: 659576f219c6f2d1cf2505f806ede15937403161d5a5bb5713bb5fd06a1cb733**

## E- Clipper

This is another variant of clipper malware family which supports a lot of cryptocurrencies and its subsequent wallets that are used today. The E-Clipper malware can obscure its presence and has certain features to ensure its persistence. To elaborate, this malicious program is light (i.e., final build is 30 KB and less than 1 MB) and hence does not strain the infected system's resources, which aids in hiding E-Clipper's presence.

E-Clipper unpacks itself in the Windows system folder. It is also run-on Windows start up and it can eliminate error-free restart. This piece of malicious software can change certain icons on the infected device, however, as mentioned, the primary purpose of E-Clipper is redirecting transfers from Fiat currency wallets and cryptocurrency wallets to those in possession of cyber criminals behind the infection.

The malware targets these Fiat currency wallets: Payeer, Qiwi, Yandex Money, and Web money, Crypto wallets E-Clipper targets include: Bitcoin, Bitcoin Gold, Byte coin, Black Coin, Dash, Dogecoin, Ethereum, Litecoin, Ripple, Stellar and Zcash.

In general, this type of malware is primarily distributed through Trojans, spam campaigns, illegal activation tools ("cracks"), fake updaters and dubious download channels.

## Android.C Clipper

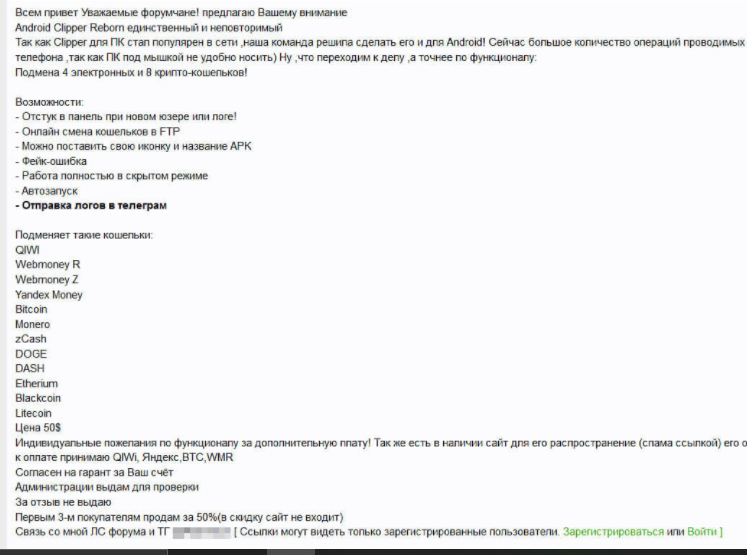
Trojans for Microsoft Windows that replace wallet numbers in the clipboard during operations involving digital money and cryptocurrencies are widespread and well known for both computer users and information security specialists. But in 2018, virus analysts examined several malicious programs with similar functions designed for the Android mobile platform.

Android.Clipper is capable of replacing the digital wallet numbers of the QIWI, WebMoney (R and Z), and Yandex.Money payment systems, as well as the Bitcoin, Monero, zCash, DOGE, DASH, Ethereum, Black coin and Litecoin cryptocurrencies.

One of the examined modifications of Android Clipper is guised as an application for Bitcoin digital wallets. The following was the process followed by the clipper:

* Once the Trojan is launched on an infected device, it displays a fake error message and continues to operate in hidden mode saying that the version is in valid and application is uninstalled to trick the user into believing that the app was deleted from the phone.
* The Trojan then hides its icon from the list of applications on the Android home screen.
* From now on, the malware can be found in the apps management section of the system preferences only.
* Both modifications of Android Clipper are then launched automatically every time an infected smartphone or tablet is turned on.
* After a successful infection, the Trojan starts to track changes in the clipboard content. Once the user copies the digital wallet number to the clipboard, Android Clipper sends the number to the command-and-control server. The malware then makes another server request waiting for the cybercriminals’ wallet number that needs to be added to the clipboard instead of the original one.

The author of Android Clipper actively sells Trojans of this family in hacking forums. At that, cybercriminals’ clients are free to use any application icon and name for every purchased copy of the malicious program.



The virus writer claims in his advertisements that the malware’s functions include sending a report on the program operation to the Telegram app and a quick change of wallet numbers embedded into the clipboard using the FTP protocol. However, these features are not implemented in the Trojan itself. All the specified functions are provided for cybercriminals by the command-and-control centre.

## Masad Clipper

This is a new Trojan-delivered spyware that uses Telegram to exfiltrate stolen information. Using Telegram as a Command and Control (C&C) channel allows the malware some anonymity, as Telegram is a legitimate messaging application with 200 million monthly active users.

The malware is being advertised on black market forums as “Masad Clipper and Stealer.” It steals browser data, which might contain usernames, passwords and credit card information. The malware also automatically replaces cryptocurrency wallets from the clipboard with its own. It sends all of the information it collects and receive commands from a Telegram bot controlled by the threat actor deploying that instance of Masad.

This malware is written using AutoIT scripts and then compiled into a Windows executable. Most samples we have seen are about 1.5 MB in size, however, Masad Stealer can be found in larger executables as it is sometimes bundled into other software.

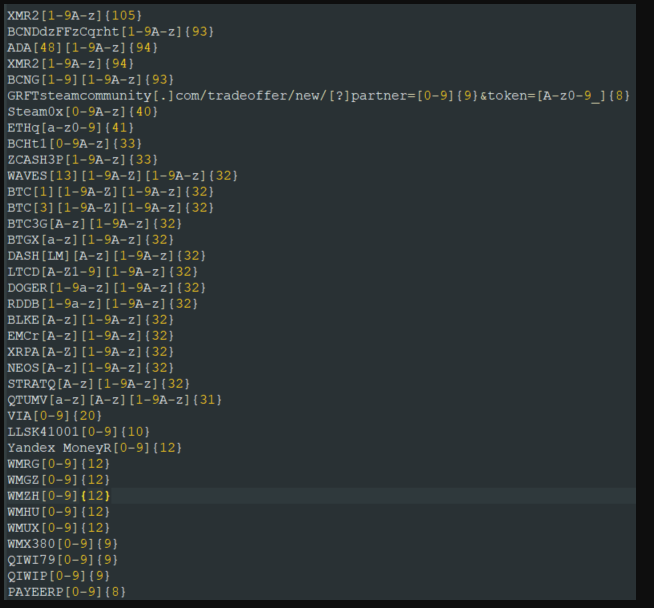
When Masad Stealer is executed, it drops itself in %APPDATA%\folder name} \{filename}, where folder name and filename are defined in the binary. Examples include amd64 usbhub3.inf.resources and ws2\_32.exe, respectively. As a persistence mechanism, Masad Stealer creates a scheduled task that will start itself every one minute.

After installing itself, Masad Stealer starts by collecting sensitive information from the system, such as:

* Cryptocurrency Wallets
* PC and system information
* Credit Card Browser Data
* Browser passwords
* Installed software and processes
* Desktop Files
* Screenshot of Desktop
* Browser cookies
* Steam files
* AutoFill browser fields
* Discord and Telegram data
* FileZilla files

It zips this information into a file using 7zip utility, which is bundled into the malware binary.

Along with all the above-mentioned functionality, this also contains functionality to copy and hijack the clipboard contents. This malware includes a function that replaces wallets on the clipboard, as soon as it matches a particular configuration. Below are the regular expressions and supported wallets that it matches against the clipboard data:



Though we have discussed few of the clippers here, there are many other clipper malwares like Qulab, Quill Clipper, Clipsa, Apocalypse Clipper which have similar functionality but different mechanisms for stealth, hiding and malicious operations.

# Malware Families Close to Clipper Family

While searching for malware samples coming under the clipper family, we came across different types of malware families. When we performed malware analysis and by searching more details on these families, we found that they were coming under ‘Information Stealer’ category. Which were used to steal credentials and even crypto currencies, but they were not using or changing anything on the clipboard. As they were also stealing the crypto currencies might have caused them to be mis identified as clipper malware. Listing some of the examples of malware families, which were misidentified as clipper.

## Arkei

ArkeiStealer is a type of malware that steals sensitive, confidential information, which cyber criminals can then use to generate revenue. Research shows that ArkeiStealer is capable of stealing login credentials and cryptocurrency wallet keys.

Cryptocurrency wallets store public and private keys, which can be used monitor balances, send money and perform other operations. ArkeiStealer can be used to steal private keys and misuse them to make fraudulent transactions. Unfortunately, there is no way to reclaim lost money (cryptocurrency) or reverse the transactions.

Furthermore, this malware is capable of stealing login credentials, and therefore cyber criminals can use it to hijack email, social networking, online payment and other accounts.

In most cases, cyber criminals use hijacked accounts to make fraudulent transactions and purchases, deceive other people into making transactions, steal identities, spread malware (such as ransomware, Trojan-type programs) and perform other malicious actions.

ArkeiStealer can be the reason behind serious online privacy issues, significant financial loss, identity theft, etc. Therefore, it must be eliminated from infected operating systems immediately.

## Immortal Information Stealer

Immortal steals data from 24 browsers. It steals stored credentials, cookies, credit card data, and autofill data from the targeted browsers.

When the user saves a username and password in the targeted browser, it stores the data in a “Login Data” file in an SQLite database format, and the browser-stored cookie information in the “Cookies” file. It also stores autofill data, credit card data, and other web information in the “Web Data” file. Below are the file paths for those files:

* “\%AppData%\Local\ {Browser}\User Data\Default\Login Data”
* “\%AppData%\Local\ {Browser}\User Data\Default\Web Data”
* “\%AppData%\Local\ {Browser}\User Data\Default\Cookies”

The autofill feature of a browser allows the user to store commonly entered information in web forms. This information might include username, email, password, address, and credit card information. So, when the user opens a web page, it will automatically fill in the information already saved by the browser. The autofill information is stored in the “Web Data” file.

Immortal fetches autofill data from the “Web Data” file and stores it in the {Autofill}\_CC.txt file.

Path: “\%AppData%\ {Random\_DirName} \Autofill\ {Browsername\_Autofill.txt}”.

The malware steals files for the Steam application. Steam is an application for playing, discussing, and creating games. The files stolen by Immortal are as follows:

* SSFN (2 files)
* VDF files from the config folder
* Config.vdf
* loginusers.vdf

Immortal steals wallet.dat files from Bitcoin-Qt, a free and open-source Bitcoin wallet software. The malware copies the wallet.dat file in “%Temp%\{Random\_DirName}\”.

Immortal also steals session-related files from Telegram and Discord. Telegram is a cloud-based instant messaging and voice over IP service. Discord is the cross-platform voice and text chat application designed to help gamers talk to each other in real time. Immortal copies those files into “%Temp%\{Random Name}\Applications\{AppName}\”.

File Path:

* %AppData%\Telegram Desktop\tdata\D877F783D5D3EF8C1\
* %AppData%\Telegram Desktop\tdata\D877F783D5D3EF8C1\map0
* %AppData%\Telegram Desktop\tdata\D877F783D5D3EF8C1\map1
* %AppData%\discord\\Local Storage\\https\_discordapp.com\_0.localstorage

## Kpot

Discovered by Jorge Mieres, KPOT is a high-risk trojan designed to steal various personal information. This malware is typically distributed using fake web browser updaters (more information), however, this trojan was previously distributed using spam email campaigns

The commands provide the following functionality:

* Steal cookies, passwords, and autofill data from Chrome
* Steal cookies, passwords, and autofill data from Firefox
* Steal cookies from Internet Explorer
* Steal various cryptocurrency files
* Steal Skype accounts
* Steal Telegram accounts
* Steal Discord accounts
* Steal Battle.net accounts
* Steal Internet Explorer passwords
* Steal Steam accounts
* Take a screenshot
* Steal various FTP client accounts
* Steal various Windows credentials
* Steal various Jabber client accounts
* Remove self

Although there aren’t specific command bits controlling the functionality, the malware also looks for and attempts to steal user accounts from various VPN providers, RDP configuration files, and Microsoft Outlook accounts.

KPOT Stealer also has the ability to search for and exfiltrate arbitrary files. “Rules” specifying what files to search for can be delivered in the above GET response. Each rule has five components delimited by "\_\_GRABBER\_\_". The components include:

* Rule name
* File mask (comma separated)
* Search path
* Minimum file size
* Maximum file size

## Predator

The Predator the Thief malware first appeared in July 2018 and is used to steal usernames, passwords, browser data and the contents of cryptocurrency wallets, as well as take photos using the infected victim's webcam. The malware is commonly sold on underground hacking forums and was also featured as part of a bundle of six different forums of malicious software.

Predator the Thief is a stealthy credential stealing malware that focuses on collecting credentials and sensitive information like usernames, passwords, browser data and payment data.

## Rarog

The Rarog malware family represents a continued trend toward the use of cryptocurrency miners and their demand on the criminal underground. While not incredibly sophisticated, Rarog provides an easy entry for many criminals into running a cryptocurrency mining botnet. The malware has remained relatively unknown for the past nine months barring a few exceptions. As the value of various cryptocurrencies continues to remain high, it is likely that we’ll continue to see additional malware families with mining functionality surface.

The malware comes equipped with a number of features. It uses multiple mechanisms to maintain persistence on the victim’s machine, including the use of the Run registry key, scheduled tasks, and shortcut links in the start-up folder. At its core, Rarog is a coin mining Trojan and gives the attackers the ability to not only download mining software but configure it with any parameters they wish. They’re also able to easily throttle the mining software based on the victim machine’s characteristics.

In addition to coin mining, Rarog also employs a number of botnet techniques. It allows the attackers to perform a number of actions, such as downloading and executing other malware, levying DDoS attacks against others, and updating the Trojan, to name a few. Throughout the malware’s execution, a number of HTTP requests are made to a remote C2 server.

## Revenge Malware

Revenge RAT, or Revenge, is a malware family used by multiple operators. It shares code and behaviour similarities, as well as tactics, techniques, and procedures (TTPs), with other publicly available RAT campaigns such as AsyncRAT, QuasarRAT, WSHRat, LimeRAT, Netwire, Cybergate, Vjw0rm, and ClipBanker, and several others that are currently unnamed.

RATs allow threat actors (cyber criminals) to manipulate infected machines remotely. Using RevengeRAT, they can manage system services/process/files, edit the Windows Registry entries and hosts file, log keystrokes, steal account credentials, access hardware (e.g., webcam), execute shell commands, and so on. Therefore, these people can cause significant damage.

Firstly, modifications performed to the system might diminish performance, and recovery could be difficult or even impossible. Additionally, by logging keystrokes and stealing account credentials, cyber criminals cause serious privacy issues. Threat actors aim to generate as much revenue as possible.

Therefore, hijacked bank, social network, email, and other accounts can be misused in various ways, such as through direct money transfers, online purchases, borrowing money from users' contacts, and so on. Victims of this trojan could lose savings, accrue significant debt, and have their identities stolen.

Revenge RAT also allows cyber criminals to execute shell commands to control the system in various ways. Be aware that shell commands are used to cause chain infections by injecting additional malware into the system. RATs such as Revenge RAT are typically used to proliferate infections that have different capabilities/purposes (e.g., ransomware, crypto miners, etc.)

## Vidar Malware

Vidar is a dangerous malware that steals information and cryptocurrency from infected users. It derives its name from the ancient Scandinavian god of Vengeance. This upgraded version of Arkei stealer has been terrorizing the internet since 2018.

The malware is capable of exfiltrating a variety of data from an infected system including system information, browser data, and credentials. The data collected from infected systems include Machine ID and GUID, operating system, computer name, current username, display resolution, keyboard language, hardware information, network information, and a list of installed software.

In addition to this, the malware generates three different files to store email credentials and browser credentials from the system.

# Static Analysis of E-Clipper

Static analysis examines a malware file without running the program. This is the safest way to analyse malware, as executing the code could infect your system. In its most basic form, static analysis gleans information from malware without even viewing the code. Metadata such as file name, type, and size can yield clues about the nature of the malware. MD5 checksums or hashes can be compared with a database to determine if the malware has been previously recognized. And scanning with antivirus software can reveal what malware you’re dealing with.

SHA256: ff93ab320749a17363f81262c5721627fb11ba13b39df725fdf75394e25859f9

**PEStudio details:**

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

A normal exe file is having different sections like, data, text, resource, etc. But here, we can see only the resource, and most of the content is under an unknown section.

Graphical user interface, application, table, Excel

Description automatically generated

Like other clipper malware samples, this one is also being detected as trojan clip banker by different antiviruses.

Graphical user interface, application, table

Description automatically generated

Here we can see some of the strings which can be used to detect the file using Yara rules. The Ethereum is a crypto currency, we can see strings related to the Clipboard and the addOnClipboardChange which can be functions making use of the clipboard in the system. Listing the strings, we have used in the Yara rule to detect this malware.

$eth1 = "ETHEREUM"

$eth2 = "SetClipboardViewer"

$eth3 = "ChangeClipboardChain"

$eth4 = "Clipper"

$eth5 = "ClipMon"

$eth6 = "add\_OnClipboardChange"

$eth7 = "remove\_OnClipboardChange"

In the Yara rule, we have used the variable $eth because Ethereum is present in its list of strings. From the list of strings here, we can infer that when the user of host system copies an Ethereum wallet address, this malware will be replacing it with the wallet address of the attacker. Thereby if the user sends any crypto currency to the copied address, without cross checking the address to which he is sending, the user may end up losing his money.

# Detailed Analysis of Masad Clipper

SHA256: e2115a42e4ef267a4484cbb5cd342ea5d12b26f93fb76f6ba92eed12129dd272

**Analysis using PEStudio**

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface

Description automatically generated

48/70 antivirus vendors are detecting this malware, but most of them are detecting it as Trojan.

Graphical user interface, application, table, Excel

Description automatically generated

Unlike the previous sample (E clipper) here we can see that the section details are showing. text, rdata and other details as well.

Graphical user interface, table

Description automatically generated with medium confidence

Some of the strings we had used to detect this clipper using Yara rules.

$clip1 = "OpenClipboard"

$clip2 = "GetClipboardData"

$clip3 = "CloseClipboard"

$clip4 = "EmptyClipboard"

$clip5 = "SetClipboardData"

$clip6 = "`vbase destructor'"

$mal1 = "FindFirstFile"

$mal2 = "DeleteFile"

$mal3 = "FindNextFile"

$mal4 = "MoveFile"

$mal5 = "CAutoIt"

$mal6 = "This is a third-party compiled AutoIt script."

$mal7 = "WinDetectHiddenText"

$mal8 = "REGEXPTITLE"

$mal9 = "AutoIt has detected the stack has become corrupt.

Stack Corruption typically occurs when either the wrong calling convention is used or when the function is called with the wrong number of arguments.

AutoIt supports the \_\_stdcall (WINAPI) and \_\_cdecl calling conventions. The \_\_stdcall (WINAPI) convention is used by default but \_\_cdecl can be used instead.

wide ascii is used for nocase.

These are the other strings we had used in the yara rule, here we can see a large number of strings, but in the detection, we may not need this much strings. We had kept this much strings so that others checking this Yara rule will also be able to understand the functionality of the malware being detected. By checking the strings $mal5 and $mal9, we can see that the malware is written using AutoIT script, which is used for automation scripting.

By analysing the Masad sample using Exeinfo PE, we came to know that the malware was packed and it has to be unpacked using Exe2Aut - AutoIt3 decompiler. But that didn’t work properly so we used MyAutToExe to decompile this sample.

Graphical user interface, text, application

Description automatically generated

We have thus used EXE2AUT for decompiling the malware sample.

As shown in the below screenshot, we can Drag and drop the files to the File/folder location and Scan File-> Automated and it will unpack the file and gives a list of files.

From the list of output files, we can analyse the file with name e2115a42e4ef267a4484cbb5cd342ea5d12b26f93fb76f6ba92eed12129dd272\_restore.au3, It will contain the AutoIT code which can be used for analysis.

Graphical user interface, application

Description automatically generated

Looking at the code, we see that so many variables are declared and used.

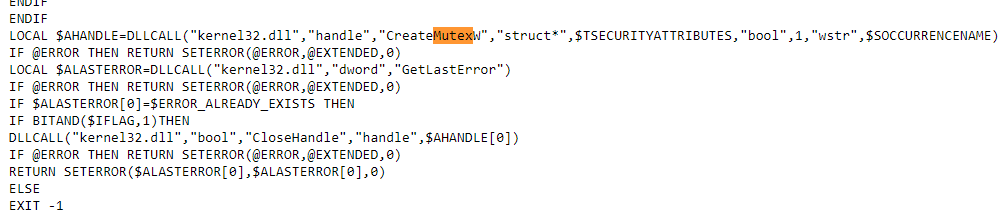
Graphical user interface, application

Description automatically generated

This part of the code shown in the below screenshot shows that the malware is accessing CreateMutexw function for creation of Mutex object.

Malware often uses a named Mutant to ensure it does not re-infect the same machine and only run a single copy of the malware. For example, consider malware which is delivered via a malicious word document. Each time the document is opened, the malware may unnecessarily reinfect the machine, increasing its chance of detection.

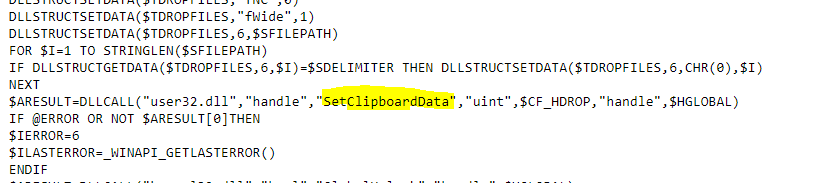
To avoid this, the malware attempts to open a named mutex with a predetermined hard coded name. If the CreateMutex call succeeds then the malware can continue to run. If the call fails it is most likely because another copy of the malware is already running, therefore the malware will exit.

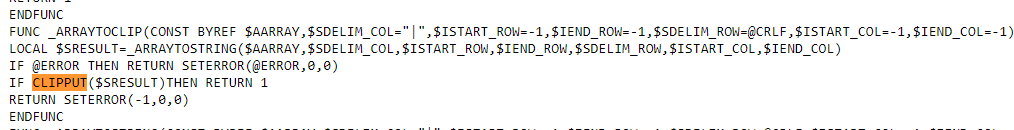


In the code below, we can see some functions using the clip functionality to check if the content is matching with another value.

The clipput function in AutoIT is used to put some data onto the clipboard.

We have also observed use of functions calls done using windows dll user32.dll which contains functions like OpenClipboard, EmptyClipboard, SetClipboarddata.





A functionality of this AutoIT script is that in the host system, the AutoIT need not be installed, it is performing the functionality by calling the dlls, which are already present in the host system, here we can see a list of dll calls.

This function is accessing the user32.dll to access the OpenClipboard and EmptyClipboard functionality.

Graphical user interface, application, Word

Description automatically generated with medium confidence

The rest of the code was found to be obfuscated as shown below.

A picture containing background pattern

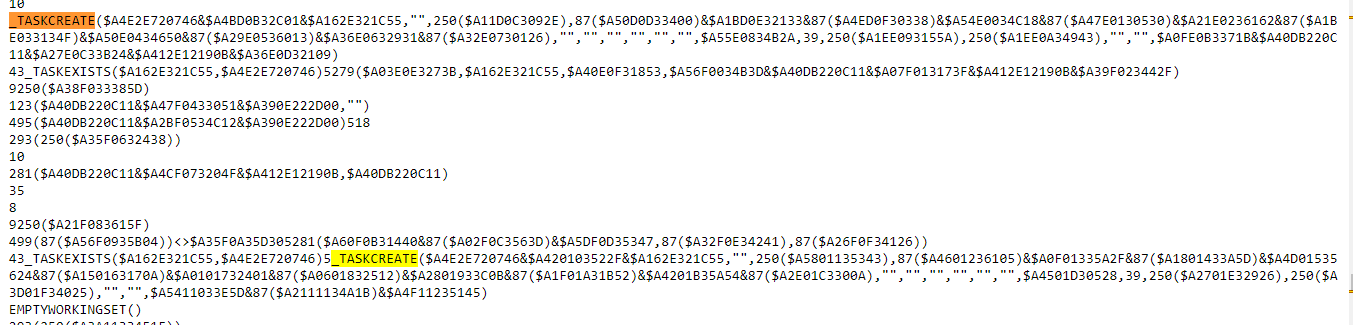
Description automatically generated

Referring online blogs and documentation provided by AutoIT, we were able to found few more things about the malware.

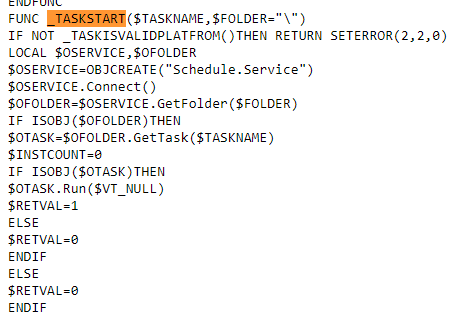
That the malware was starting Task scheduler and was creating few tasks. The \_TASKCREATE is a user defined function which is used to create the Task in scheduler.

The following are the valid parameters for the function

Func \_TaskCreate($taskname, $TaskDescription, $TriggerEvent, $StartTrigger, $EndTrigger, $DaysOfWeek, $DaysOfMonth, $MonthOfYear, $WeeksOfMonth, $DaysInterval, $Interval, $RepetitionEnabled, $LogonType, $RunLevel, $Username, $Password, $Program, $WorkingDirectory = "", $Arguments = "", $RunOnlyIfNetworkAvailable = True, $active = True, $multiinst = 0, $nobatstart = False, $stoponBat = False, $hidden = False, $idle = False, $WakeToRun = False, $timelimit = "P1D", $priority = 5, $duration="", $StartWhenAvailable = True)

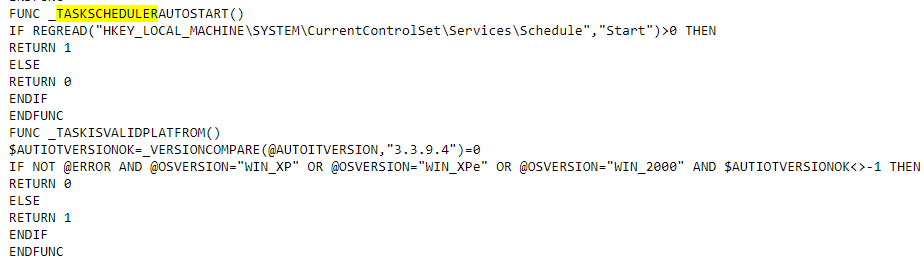


Similarly, the \_TASKSTART function is used for starting the task scheduled.

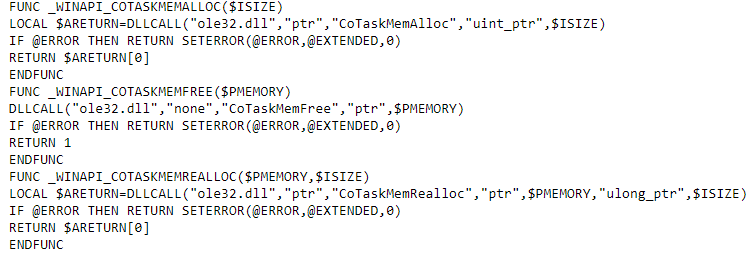


The below screenshot shows the malware code setting the scheduler to AutoStart and was confirming AUTOIT and OS versions to be used with the UDF.

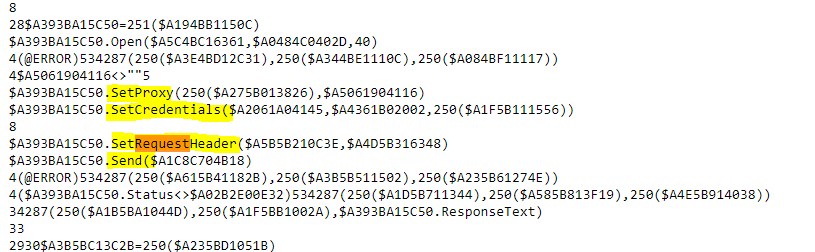
The \_TASKSCHEDULERAUTOSTART is



We also found few functions which are related to memory allocation and re-allocation which is done by the malware code.



The below screenshot shows the malware sending web request using obfuscated code. Though the URL is obfuscated, we can see the proxy, set credentials and request header functions and sending of a request. The URL cannot be decoded using the code and we have dynamic analysis has to be performed to observe network connections by the malware.



We have thus applied the sample to a dynamic analysis sandbox, we have obtained below DNS requests and network connections which show them to be malicious.



## Summary

At the end of the file, we were seeing so many obfuscated contents like shown in below screenshot and it might be because the de-obfuscator, we used to be also not able to completely de-obfuscate the code.

A picture containing background pattern

Description automatically generated

Much expertise and experience would be required in AutoIT and it subsequent tools to perform further de-compilation. Since it requires user defined decompile scripts and as complete Automated DE obfuscation is not possible.

But with the analysis performed above, we are thus able to infer below malicious activities about the malware:

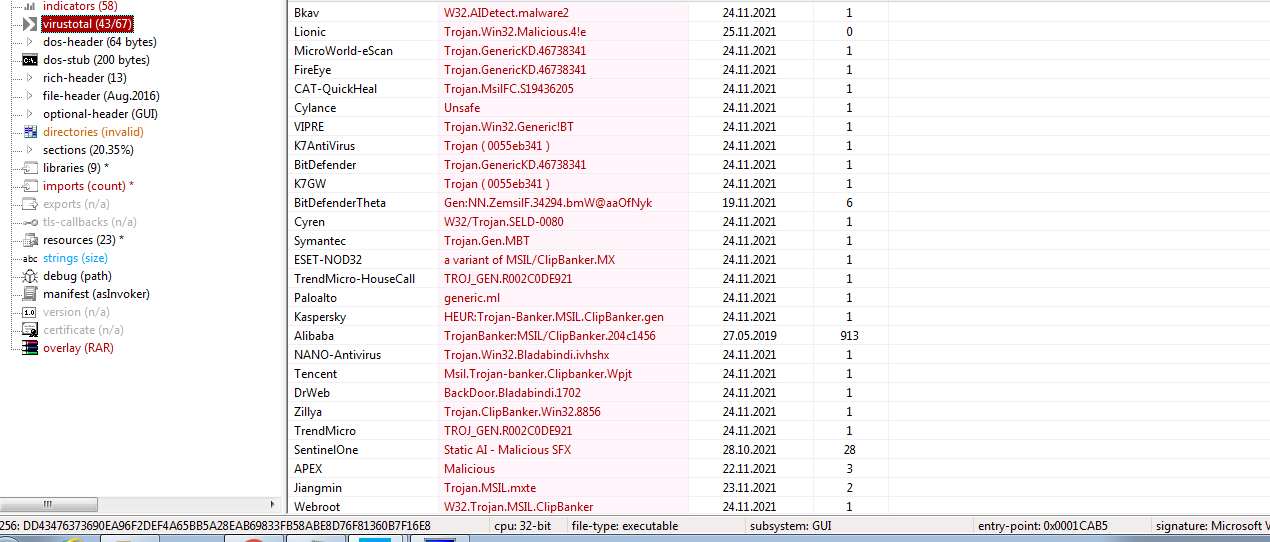
* Use of set clipboard, get clipboard, clip put, empty clipboard
* use of Mutex,
* schedule of tasks
* Memory Allocation and Re-allocation
* malicious web requests.
* API connection to telegram bot.

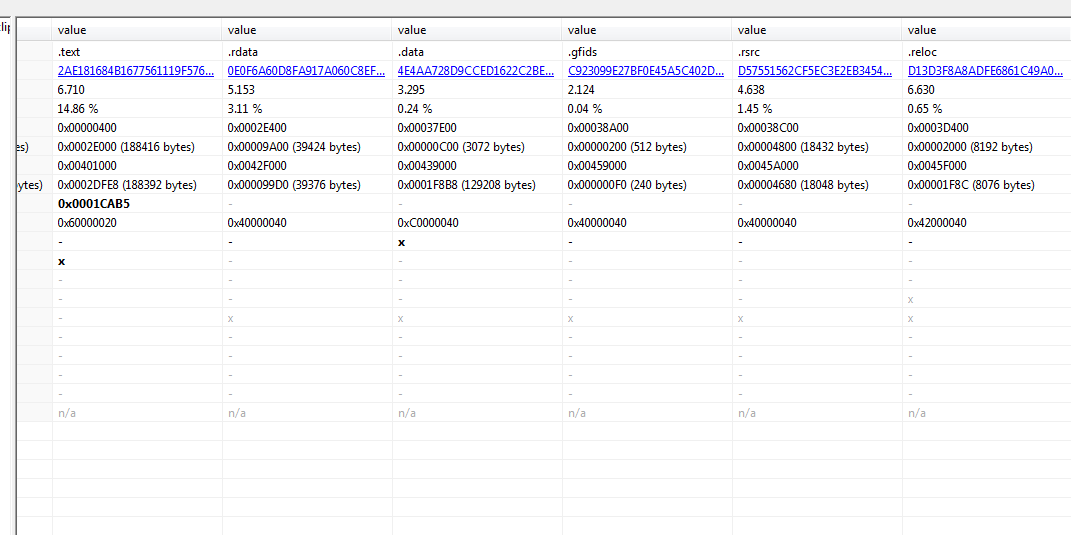
# Detailed Analysis of Red Line Clipper Stealer

­SHA256: dd43476373690ea96f2def4a65bb5a28eab69833fb58abe8d76f81360b7f16e8

**Analysis using PEStudio**

Many vendors showing it as trojan/ clip banker.

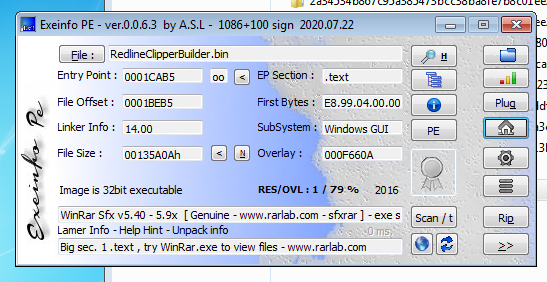




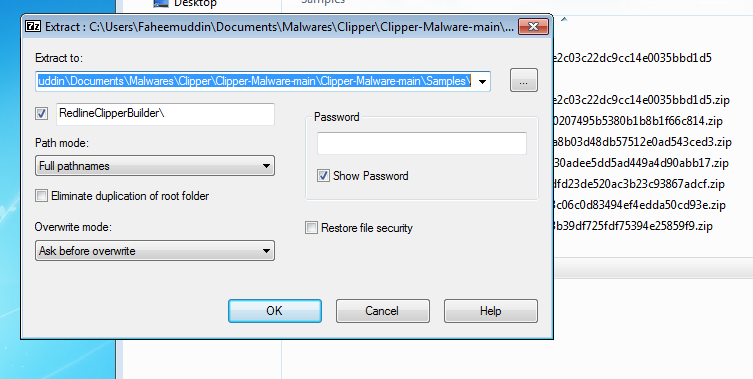
**Analysis using Exeinfope Shows that the file is SFX.**

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.

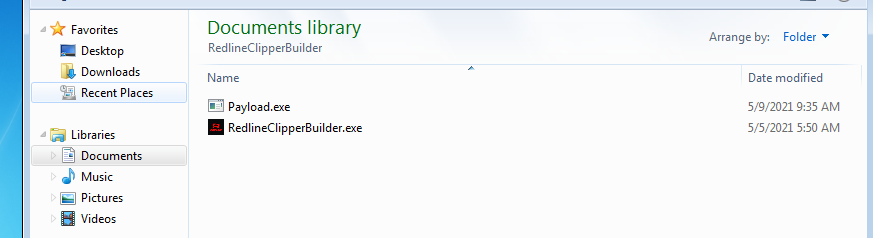
So, we can use WinRAR or 7 zip to extract its actual contents.



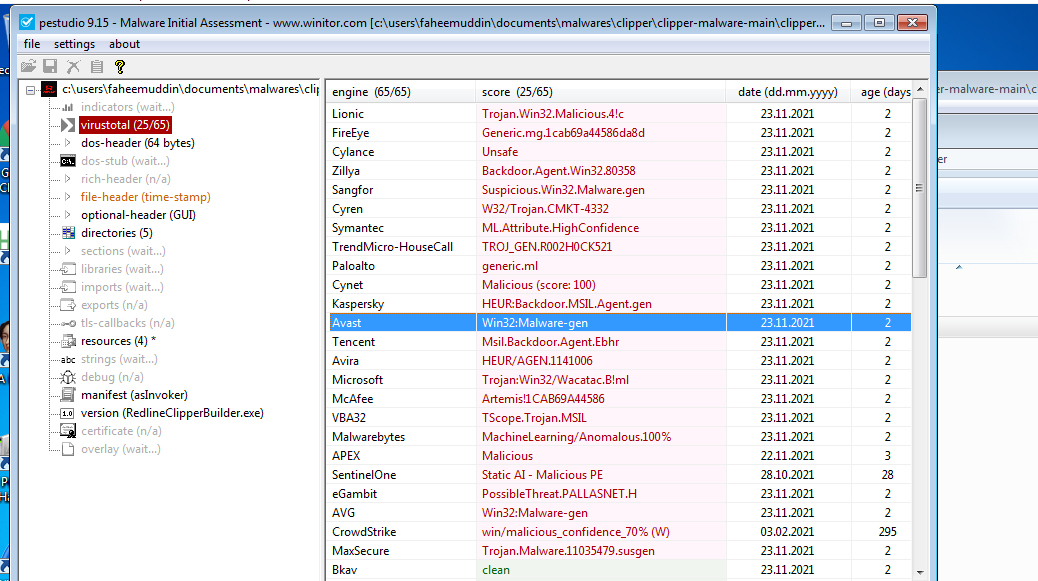
**Extracting using 7zip**



**The extracted folder has two files:**

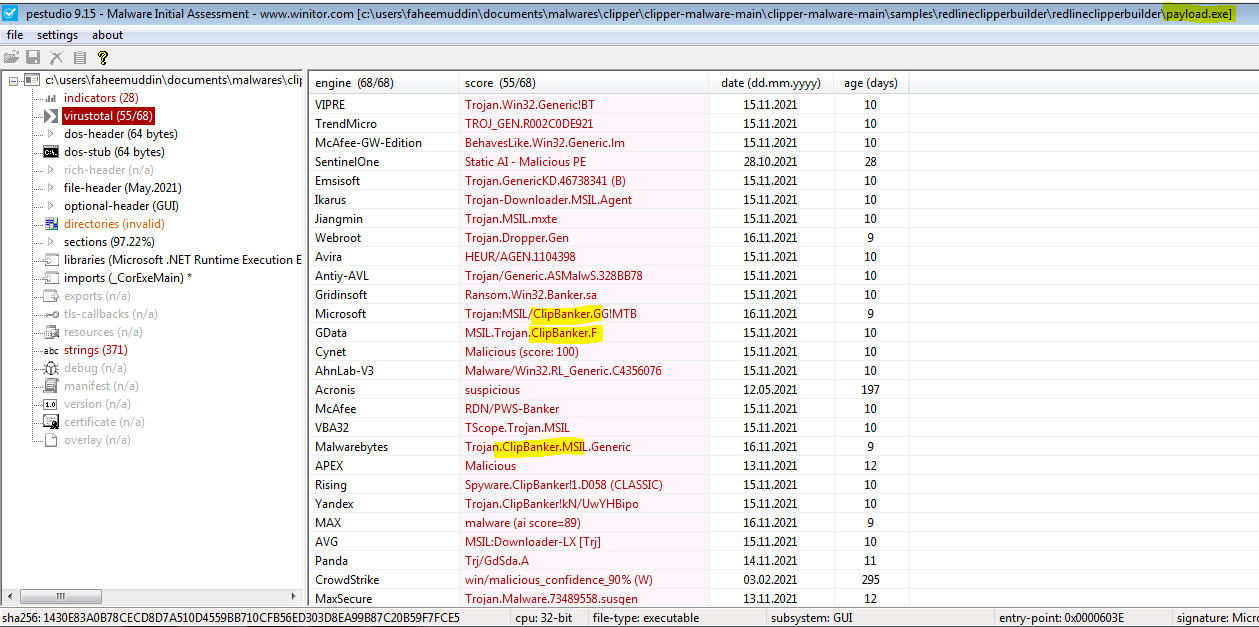


**The redlineclipperbuilder.exe is detected as trojan on virus total**

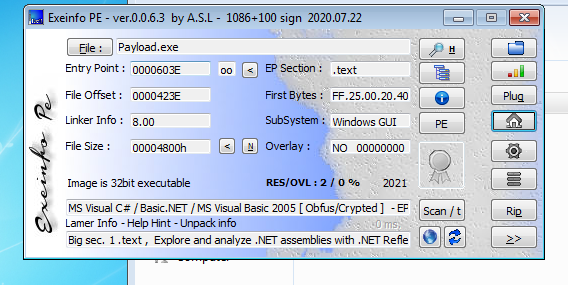


The payload.exe is detected as a Trojan/Clip banker application. We will thus use payload.exe for further analysis.

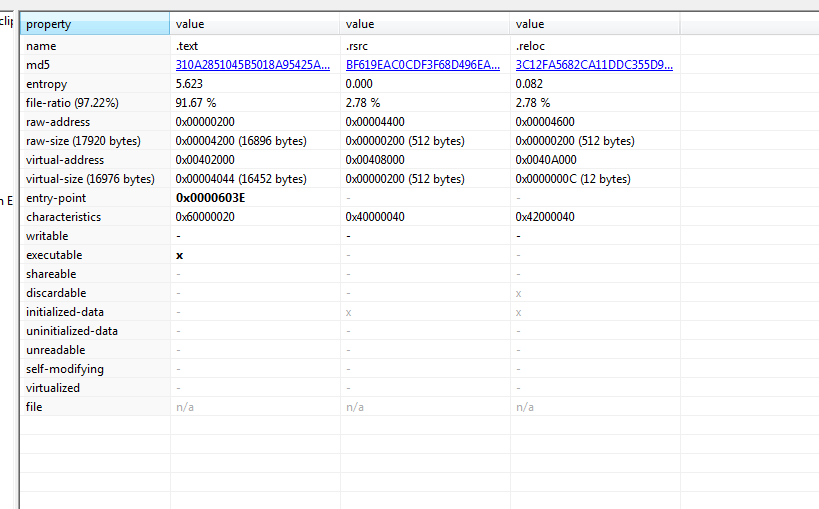
Payload.exe SHA256: 1430E83A0B78CECD8D7A510D4559BB710CFB56ED303D8EA99B87C20B59F7FCE5



The payload.exe is compiled using visual C# language

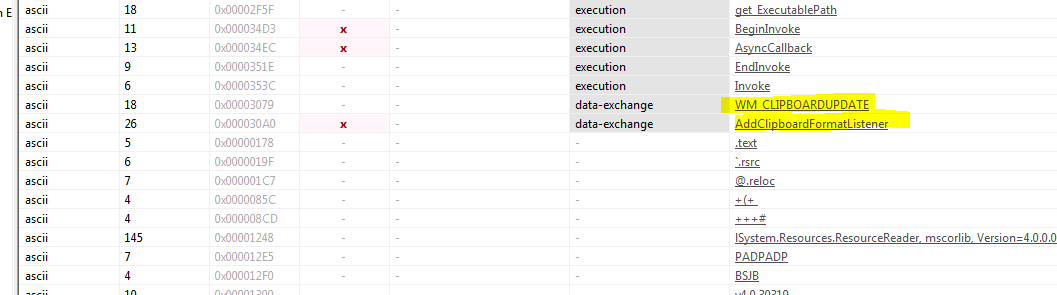


The data in the payload.exe is not obfuscated and thus can be analysed directly using dot net unpackers.

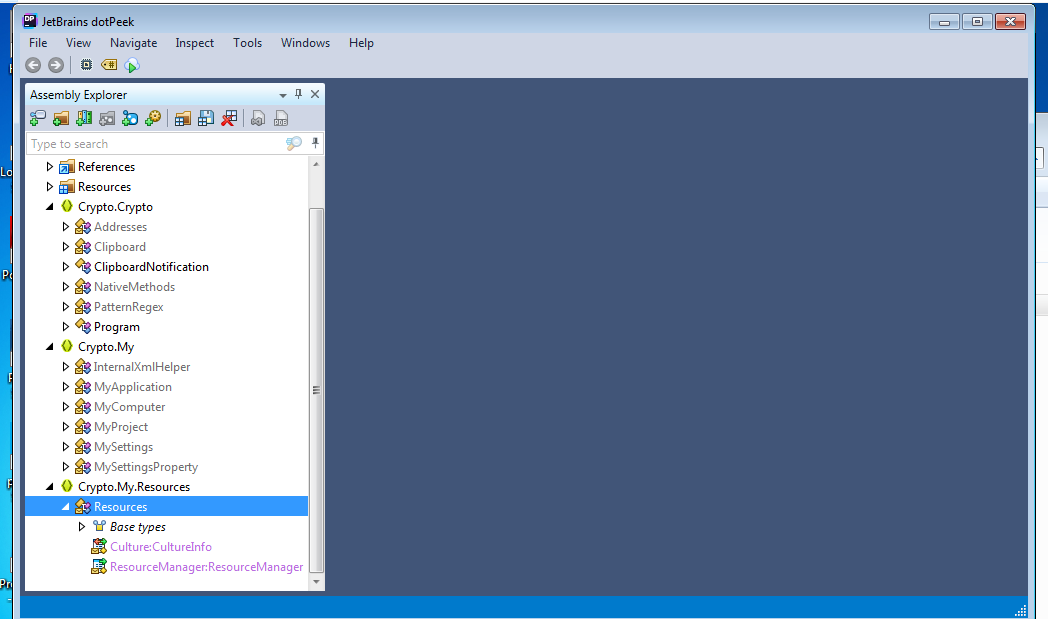


The strings in the payload.exe indicates that there is activity of clipboard update and control





Opened the payload.exe using dot net peak



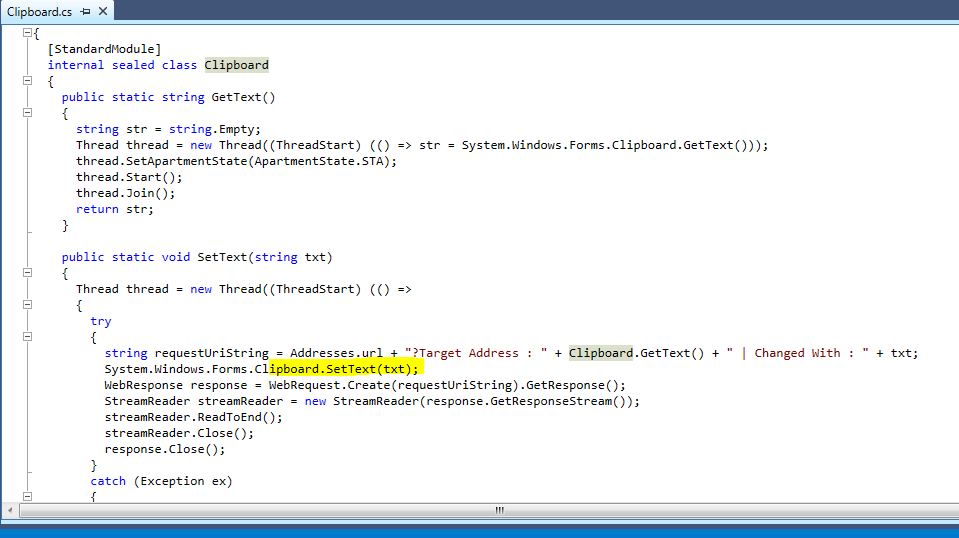
Found Class Addresses related to multiple cryptocurrencies.

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

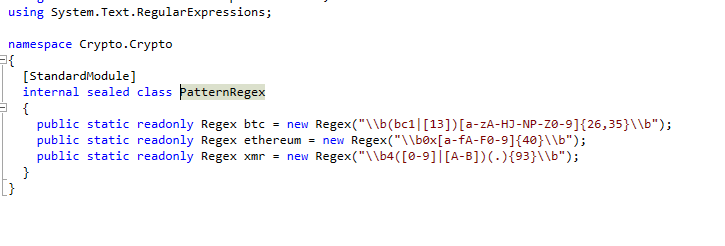


The clipboard class:

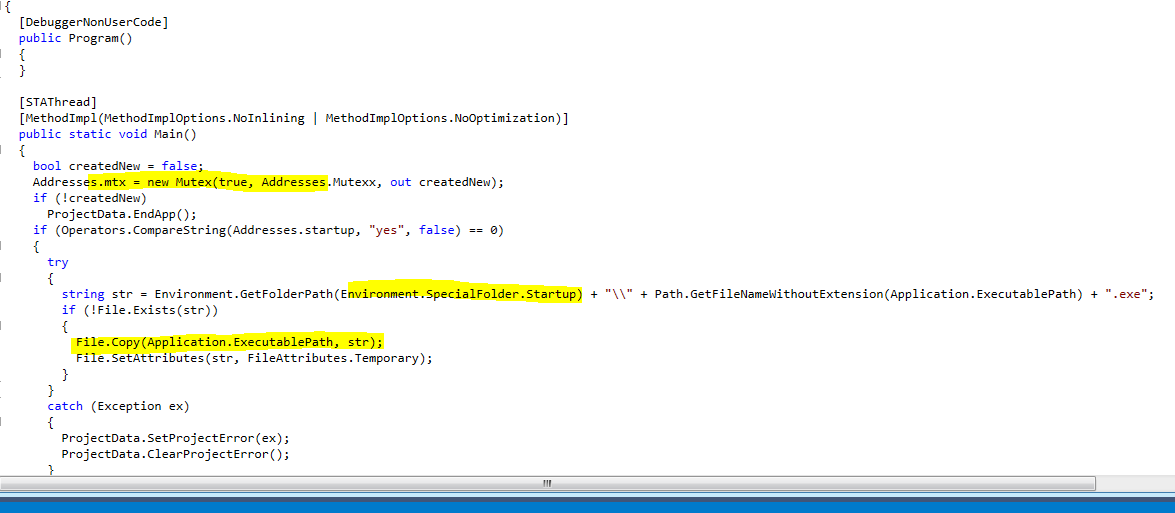
It is capturing clipboard data from victim and sending a request with its clipboard contents to compromised URL which is available in Addresses class.



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 cryptocurrency address of the attacker.



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

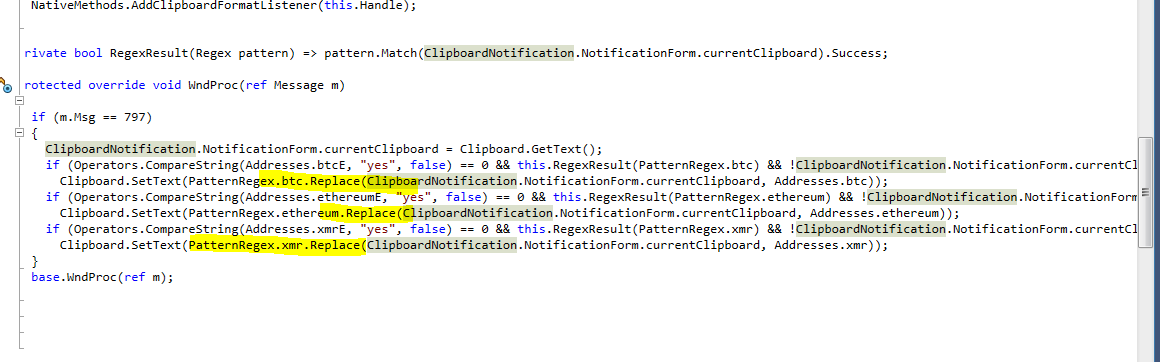


For matched patterns it is replacing the addresses with the attacker’s address using Replace function. So, if the data in clipboard matches bitcoin address. Then it is replaced with attacker’s address using the below line of code:

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

The same applies to other crypto addresses.

Attacker’s address is accessed using Addresses.btc, Address.ethereum, Addresses.xmr etc.



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

## Red Line Clipper Stealer in Action

We had executed this malware in a virtual machine and recorded its working. We have copied a list of 4 bitcoin addresses from a bitcoin donation site and copied it to a notepad. And we had copied the same addresses to another notepad and the same addresses were getting copied without any issues. Then, we ran the payload.exe of the Red Line Clipper Stealer and tried copying the same addresses. All addresses were getting copied, while posting all were showing another address. We had tested it by copying a sample “Test data” and it was getting pasted properly. Attaching below the screen recording of this demo.

<https://drive.google.com/file/d/1xHHed3aU18Z6CTX43_Cw4-fX_yq3oZQ2/view?usp=sharing>

## Summary

Based on above analysis, if the file 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 start-up 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.

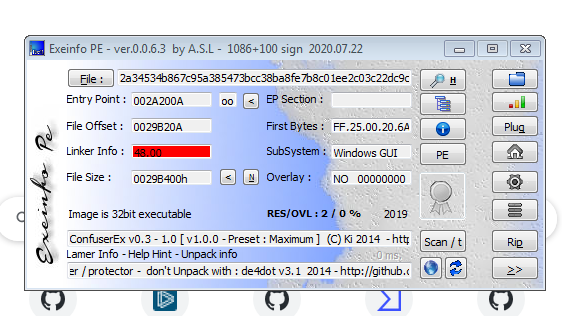
**Other Files containing the same Clipper functionality by installation of Payload.exe:**

1. 3D4165E3DE77F38DDEEDC0AC55A590A098478AFD626DA8576B44C35188C00D4C: [3d4165e3de77f38ddeedc0ac55a590a098478afd626da8576b44c35188c00d4c | ANY.RUN - Free Malware Sandbox Online](https://any.run/report/3d4165e3de77f38ddeedc0ac55a590a098478afd626da8576b44c35188c00d4c/2a3feabf-51d4-4c9e-953b-d166478d6629)
2. 5BFF05DE3BC48BF7782FF18015BE9330472EA1294C1BF0B18F5164852914C49B
3. EBCA1B997A1391234ACF2B7D0FF623028F68788529A111FE04BDFAA11DF41456
4. E5A49283D9CDA689F31B9EDC08568C6AF29CD7ED416AFCBBCB1E42FAA0BC9A55: [e5a49283d9cda689f31b9edc08568c6af29cd7ed416afcbbcb1e42faa0bc9a55 | ANY.RUN - Free Malware Sandbox Online](https://any.run/report/e5a49283d9cda689f31b9edc08568c6af29cd7ed416afcbbcb1e42faa0bc9a55/297ff3bf-6189-41e8-9029-11652fee6f1d)
5. f8209ccb1e738bc33b464ecc04980275c755bfe6be69157b6820c5be6b290112

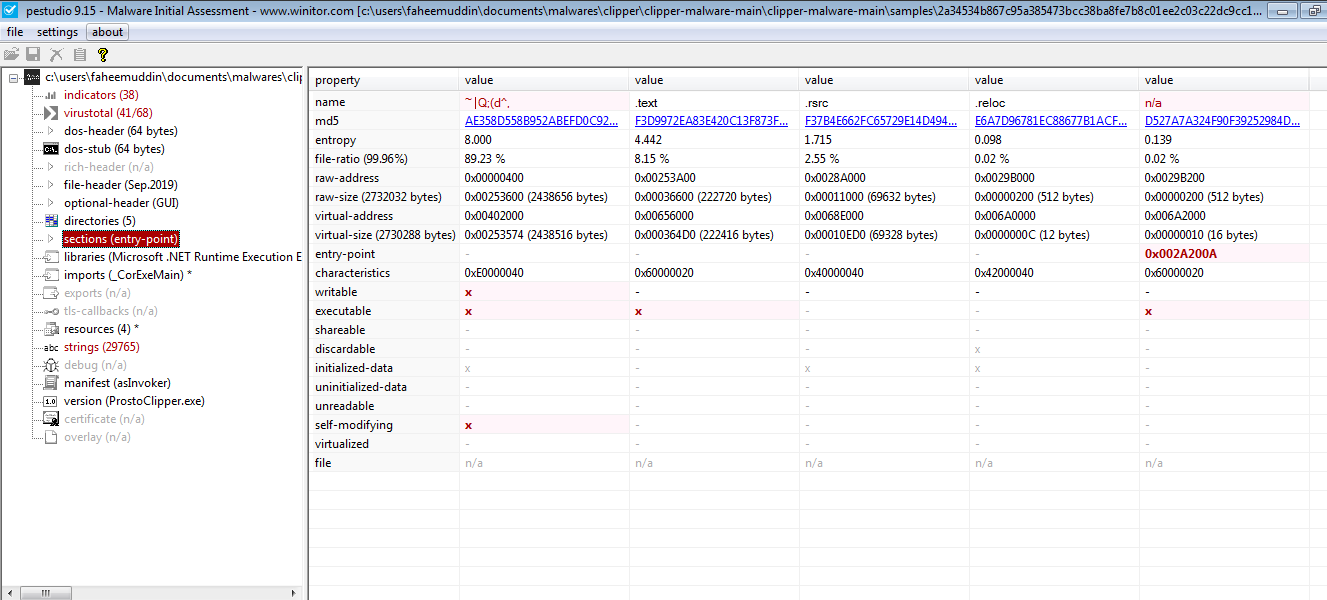
# Detailed Analysis Prosto Clipper

Analysis of Prosto clipper:

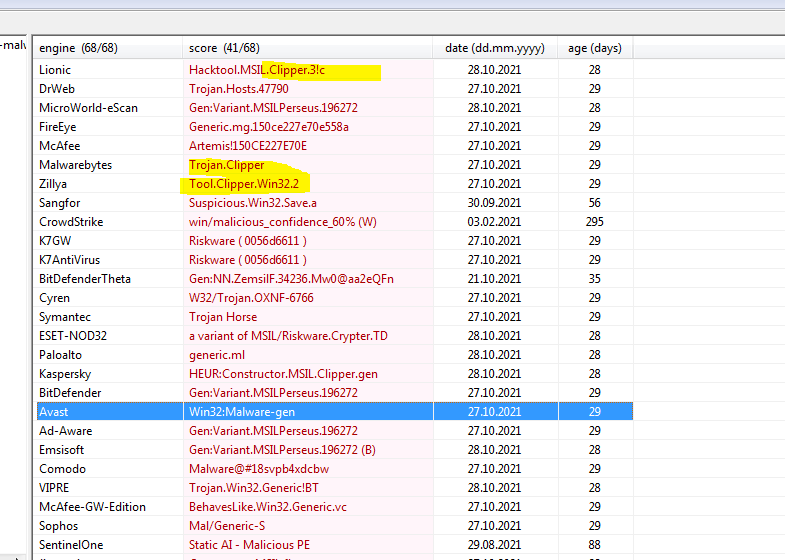
Shows that the executable is packed.



The sections indicate the same ~|Q;(d^ section is the largest and the compressed section of the file



AV Vendors on Virus Total indicate that the file is a Trojan/clipper

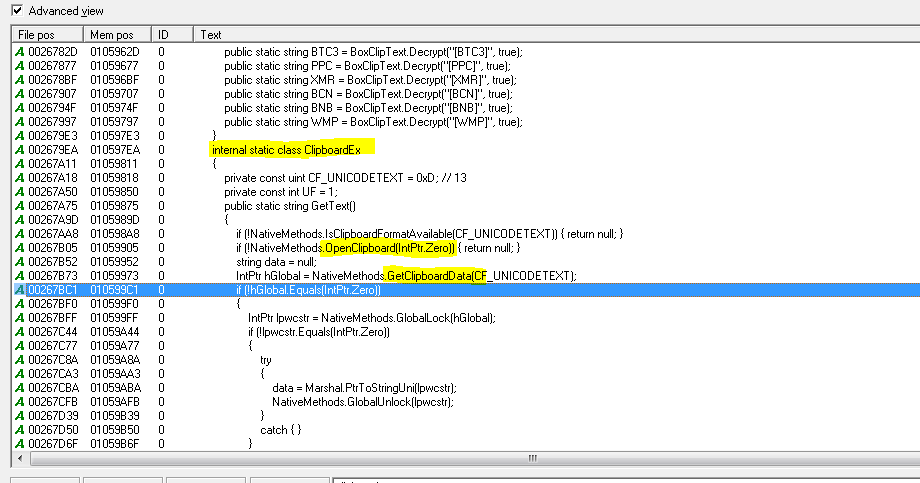


Using a ConfuserEx DE obfuscator, we can get the below unpacked file:

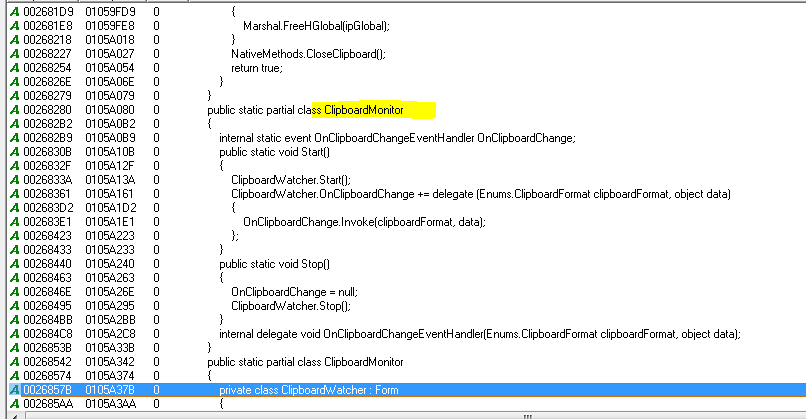
The unpacked file has SHA256 of **eb0c34e4860b696a6c8ee2040aece95083f04ddfd23de520ac3b23c93867adcf.**

Here we have pre-downloaded the deobfuscated Prosto clipper.

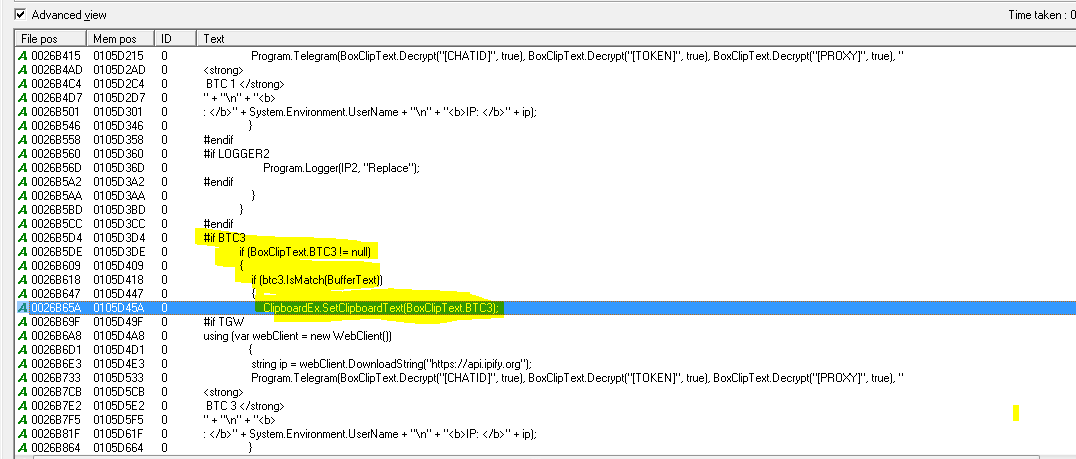
Below we can see that it is accessing clipboard and getting clipboard data.



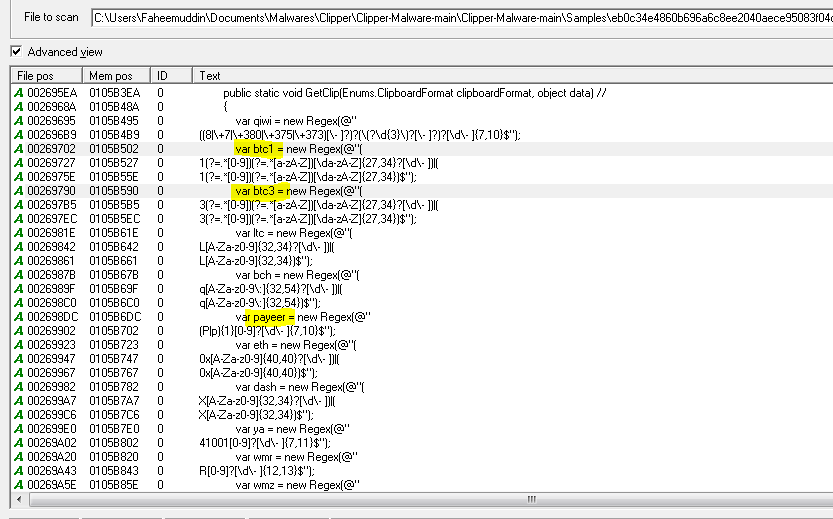
The below method clipboard Monitor provides the Prost clipper with monitoring capabilities to the changes to clipboard.



The below code is finding a match between the clipboard data in the buffer with the Bitcoin address pattern and then setting the clipboard data to new bitcoin address.



The below screenshot shows the REGEX patterns used by the Prosto clipper for matching different crypto currencies. This is the match that is checked in the above screenshot and then replaced.

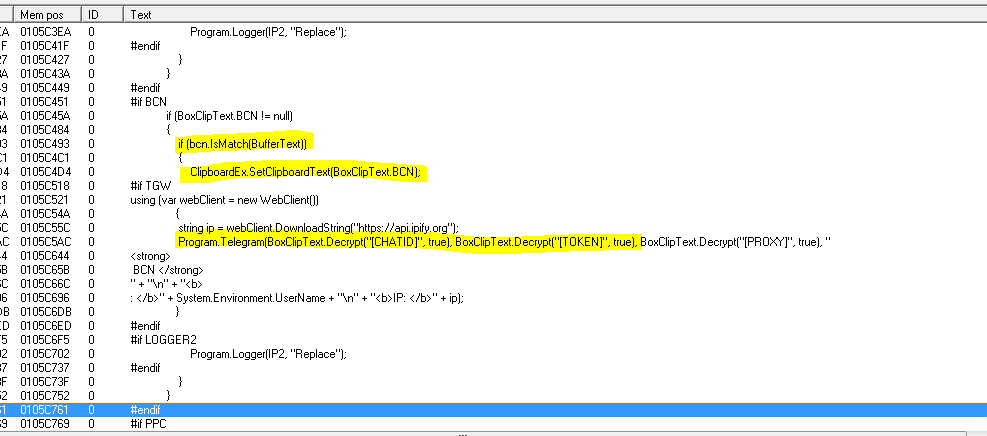


The screenshot below shows the clipper replacing one cryptocurrency data in clipboard. For each and every data replaced on the clipboard buffer, there is a call to Telegram BOT using the api.

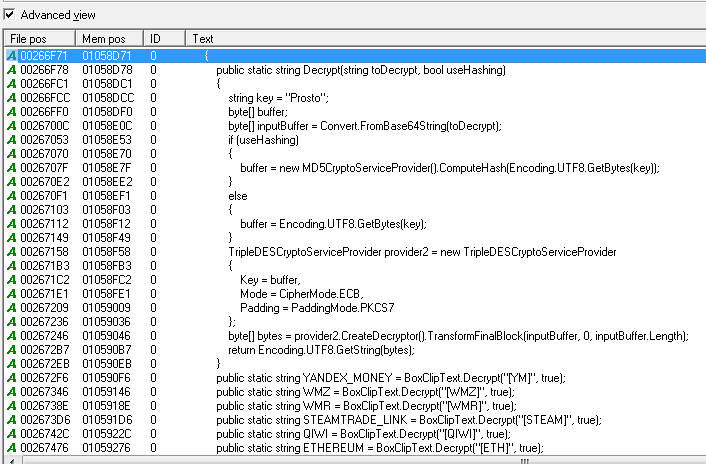
**Telegram:** Along with that, we see that the program is using Telegram BOT with specific chatID and token and possibly sending user specific data over the channel in use.

When we checked the Download String api on Microsoft documentation it mentions: “Downloads the requested resource as a String. The resource to download may be specified as either String containing the URI or a Uri.”

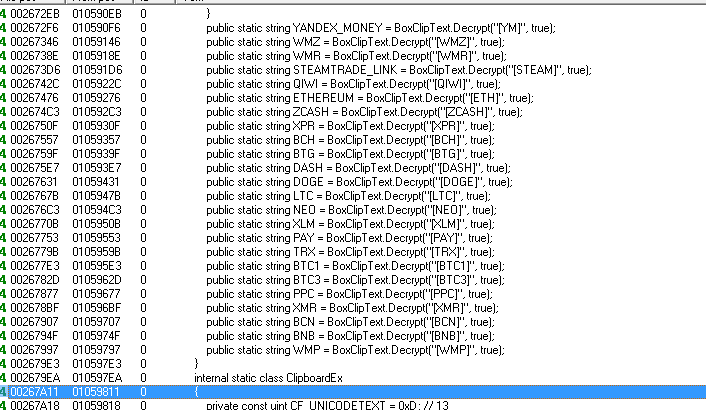
As per the code, it seems to be downloading the channel details and then sending user specific data to that particular channel.



We tried finding the public addresses in the clipper but all of them seem to be encrypted using TripleDES as we can see in below screenshots.



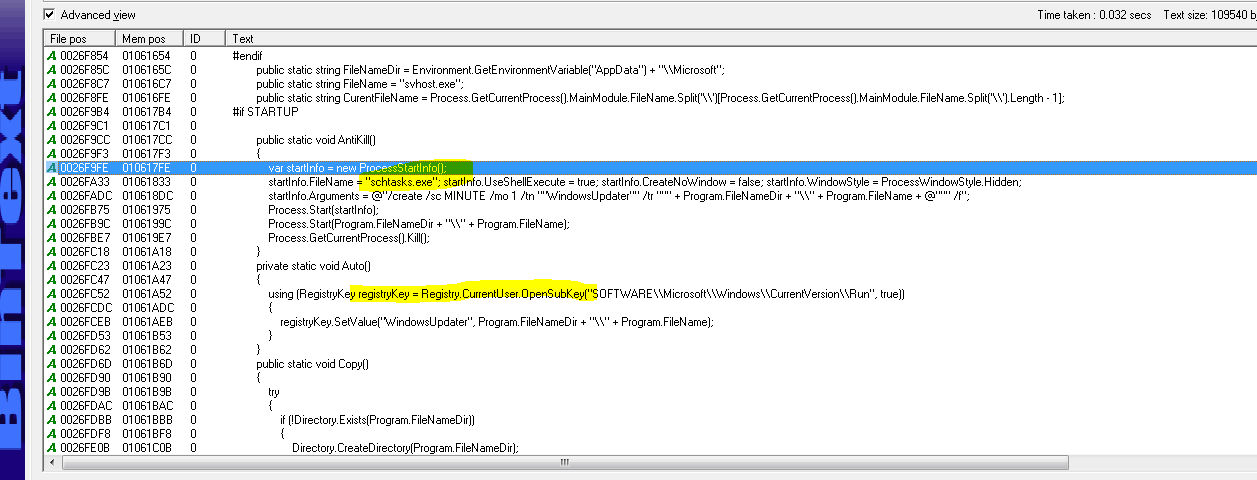
All the addresses are decrypted as shown below using the method BoxclipText.Decrypt and these public variables are directly used but no public address is revealed in the code of the executable.



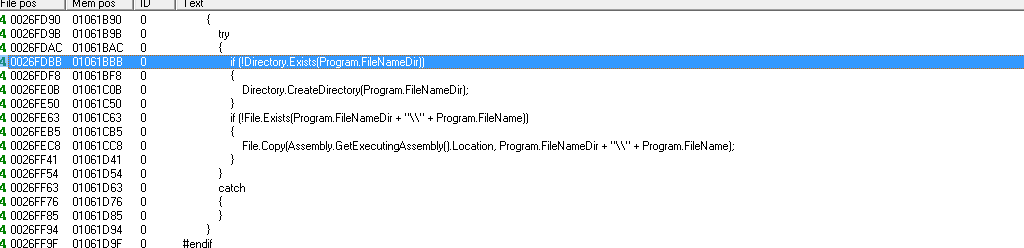
This part of the code shows, the persistence techniques used by the malware.

We can see that the malware is creating a task in task scheduler as part of AntiKill technique and naming itself as windows Updater whereas the base file location of the program is different thus tricking the user.

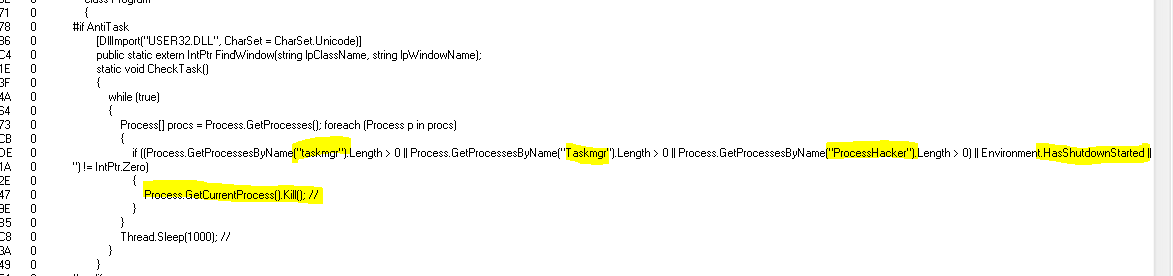
Also the code makes few changes to the registry keys in the victim’s computer for the newly scheduled task.



The malware code Indicates the malware upon execution copies itself to another directory

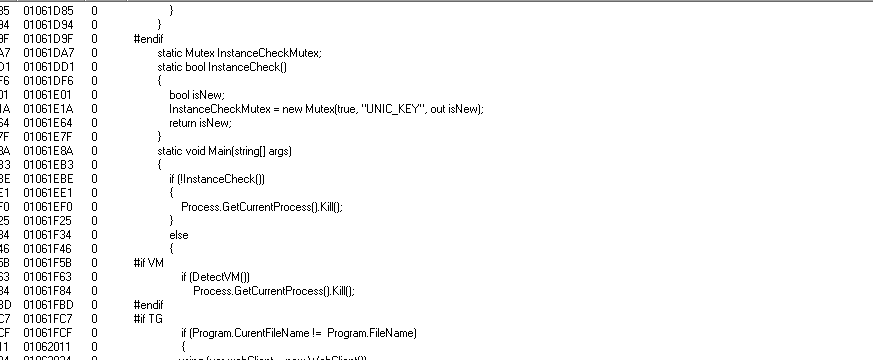


The malware is trying to detect task manager, process hacker, process explorer, shutdown process and other such tools and then trying to kill such process every 1000 seconds.



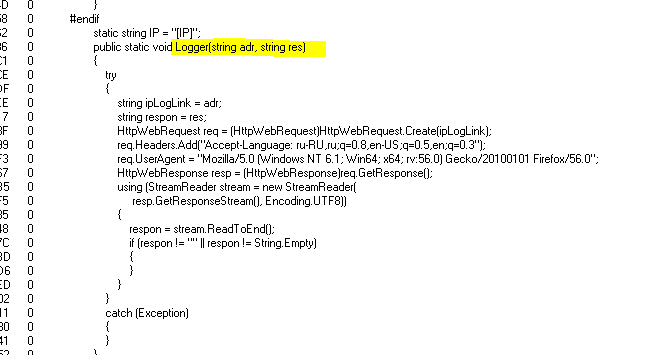
Mutex is created in the below screenshot indicating that the malware is checking for Mutex Object and creating a new object.

Also, the malware appears to be checking for a Virtual machine and killing the process if it is True.



**Logging Functionality:**

The logger function used by the malware.

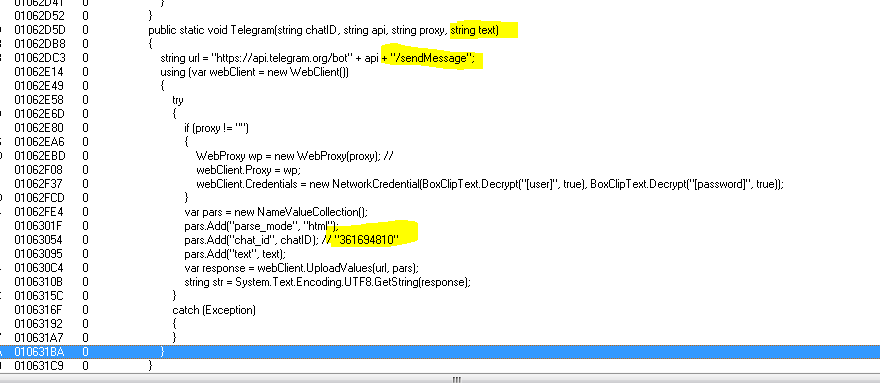


**Use of Telegram:**

The telegram method defined below is used to call the telegram api and setup specific parameters like logging into the Telegram as a user, setting the channel ID to which the communication is to be established.

It also uses proxy servers to send request without flags.

The **text parameter** sent to the method is presumed to be the user data which is then sent using the upload function.



## Summary

Based on the above analysis we can say the below Operations and capabilities are offered by the malware:

* Access to clipboard data and Replacing the Clipboard data.
* Contains a Logger Functionality.
* Replaces the cryptocurrency address with one of its own.
* Safeguards its own public address by using Triple DES encryption and using the directly decoded variables instead of the plain text values.
* Sends user confidential data to a Telegram Channel using Telegram API.
* Kills valid process like Task manager, Process hacker, shutdown process to avoid its process kill.
* Copies itself to different location
* Runs through hidden task scheduled and performs changes to the registry settings.

**SHA256 of Prosto clippers**

* eb0c34e4860b696a6c8ee2040aece95083f04ddfd23de520ac3b23c93867adcf
* 2a34534b867c95a385473bcc38ba8fe7b8c01ee2c03c22dc9cc14e0035bbd1d5

# Yara Rule

Based on the static analysis of all the clipper malware samples, we had made a yara rule to detect them.

Yara Rule:

*rule Clipper : Clipper*

*{*

*meta:*

*Description = "Rule to detect every malware coming under the Clipper Family"*

*strings:*

*$mz = { 4D 5A }*

*$clip1 = "OpenClipboard"*

*$clip2 = "GetClipboardData"*

*$clip3 = "CloseClipboard"*

*$clip4 = "EmptyClipboard"*

*$clip5 = "SetClipboardData"*

*$clip6 = "`vbase destructor'"*

*$mal1 = "FindFirstFile"*

*$mal2 = "DeleteFile"*

*$mal3 = "FindNextFile"*

*$mal4 = "MoveFile"*

*$mal5 = "CAutoIt"*

*$mal6 = "This is a third-party compiled AutoIt script."*

*$mal7 = "WinDetectHiddenText"*

*$mal8 = "REGEXPTITLE"*

*$mal9 = "AutoIt has detected the stack has become corrupt.\r\nStack corruption typically occurs when either the wrong calling convention is used or when the function is called with the wrong number of arguments.\r\nAutoIt supports the \_\_stdcall (WINAPI) and \_\_cdecl calling conventions. The \_\_stdcall (WINAPI) convention is used by default but \_\_cdecl can be used instead. See the DllCall() documentation for details on changing the calling convention." wide ascii nocase*

*$exe = "ProstoClipper.exe"*

*$red1 = "ClipboardNotification"*

*$red2 = "currentClipboard"*

*$red3 = "WM\_CLIPBOARDUPDATE"*

*$red4 = "AddClipboardFormatListener"*

*$apo1 = "CompareStringEx"*

*$apo2 = "CompareString"*

*$eth1 = "ETHEREUM"*

*$eth2 = "SetClipboardViewer"*

*$eth3 = "ChangeClipboardChain"*

*$eth4 = "Clipper"*

*$eth5 = "ClipMon"*

*$eth6 = "add\_OnClipboardChange"*

*$eth7 = "remove\_OnClipboardChange"*

*condition:*

*$mz at 0 and (all of ($clip\*) and all of ($mal\*) or $exe or all of ($red\*) or all of ($clip\*) and all of ($apo\*) or all of ($eth\*))*

*}*

In the above yara rule, we had kept these much strings because this will help in the understanding of the malware functionality. The malware would have been detected even if we reduced the number of strings used here, but the reduction in number of strings might increase the number of false positives that might get detected using this yara rule

The strings $mz is used to detect the exe files, as all the samples were exe files. We had used the strings $clip and $mal to detect the clippers Masad and Qulab, they were made using the AutoIt script so, we had used some strings to detect that feature as well.

The strings $exe is used to identify the prostoclippers, which were having string written as $prostoclipper. $red for detecting the Red Line Stealer clipper and $eth for detecting the E-clipper.

Below screenshot shows the ouput of the yara rule detecting the samples.

A picture containing background pattern

Description automatically generated

# A Comparison of Clipper Family with other types of Malwares

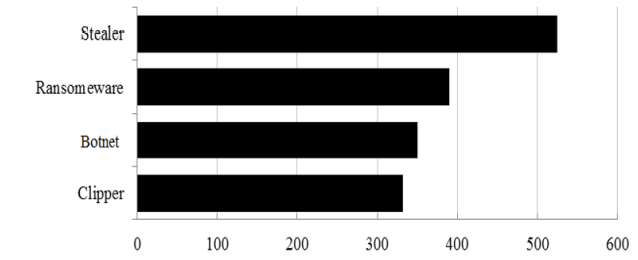
In this section, we would like to present and highlight statistical trends provided by a research paper which displayed Trends of malware influence on the integrated IT security systems and compared different types of malwares and its effects. The paper presented the analysis of modern types of malicious software. Various trends of the malware market through the anonymous segment of the Internet aka Dark web were also indicated.

The following are the various comparisons performed.

## Comparison of Malware Types

This part of the study displayed the total number of advertisements for different types of malwares on Dark web. Main trends were identified based on the assessment of fifty trading resources.

* The total number of advertisements was 2652 not taking into account duplicated ad.
* The clipper software was least represented with 332 advertisements.
* The amount of ransomware and Botnet is mostly equal and makes up 390 and 350 accordingly.
* The number of stealers advertised on the dark web is 525.

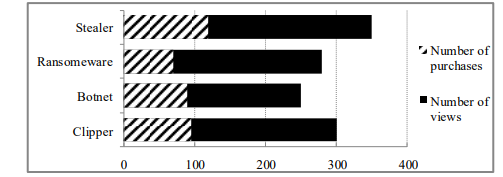


## Comparison of Popularity and Sales

The next trend was done based on the popularity of different type of malwares based on the view they received along with the number of successful purchases for the malware type. The key factors of the studied malware are its popularity, ratings and sales in the assessed information environment.

* The most popular malware is stealer (on average 350 views and 120 purchase).
* The total of 300 views and 95 purchases were registered for the clippers.
* The ad frequency on ransomware is quite diverse as such viruses are very popular and cheap. On average number of views is 280 and the number of completed purchases is 70. Also, should be noticed that more cheap versions of the ransomware are the most popular among buyers.
* The Botnet types are also quite popular and differ in specifications due to the possible number of affected nodes and number of views is 250. The number of purchases is slightly bigger than in case of ransomware and makes 90 purchases mostly for the Botnet types with the greater number of affected nodes.

The above-mentioned features are shown in below figure.

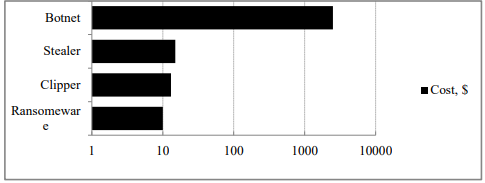


## Cost Comparison

This step performed malware cost assessment. Based on the collected information the median cost of the ransomware ranges from $0.50 to $3000 depending on the specifications. Moreover, the price varies greatly as the sellers provide not only a one-time purchase but allow the buyer to subscribe for a month or even a year.

* Ransomware could be bought for $16 (0.0003 BTC) on the Wall Street site.
* The price for the Clipper varies from $6 (0.00011 BTC) to $40 (0.00076 BTC).
* Average fee for stealer is $15 (0.00028 ВТС).
* The Botnet cost depends on the specification and number of the bots and varies from $25,75 (0.00049 BTC) to $4500 (0.085 BTC).
* The sellers declare the quick payback on their services and goods as average ransom for data encryption lays in range from 0.0037 ВТС to 0.0092 ВТС ($200 - $500). Consider the price and payback the ransomware availability is immense.

The cost ratio comparison is shown in the figure below.



# Possible Solutions

**Use of Good AV Solution**

* The first thing is going to be having a good **antivirus**. This can keep our systems safe from possible malware. But beyond that we can also make use of very varied security tools. There are browser extensions that can help us increase privacy. Also [firewall](https://itigic.com/tag/firewall/) and other tools for the same purpose.
* It is also very important to always have the **latest versions installed**.

**Be Careful while Performing Cryptocurrency Transactions**

* As we must copy and paste the wallet addresses because of its random and long nature for increasing the security, we have to be careful while doing it. Check some part of our address while copying and check if that part is available in the portion, we have pasted.

**Use of Official sources for Program Downloads**

* We need to keep in mind the importance of downloading programs from **official and reliable sources**. A major cause of malware entry is downloading software from third-party sites. This could cause us to be installing software that has been maliciously modified and may contain malware capable of hijacking the clipboard.

**Avoid falling prey to malware**

* The simplest way to avoid falling prey to such scams is to double-check every single digit of a pasted [cryptocurrency](https://coinrivet.com/dictionary/cryptocurrency/) address, no matter how tedious this may seem.
* Few analysts have also warned against using Windows software such as Cortana, as the built-in AI helper contains key-logging capabilities which could be used by hackers.

# Conclusion

* In conclusion, clipper malware modifies data saved in the victim's clipboard - it replaces copied cryptocurrency wallets with the ones owned by the attackers. When victims do not check the pasted wallet addresses, they end up paying to the attackers. Many stealers are modifying themselves with clipper functionality due to the increasing popularity and the profit that can be gained by stealing the cryptocurrency.
* Most of them are written in C# and few in AutoIT scripting languages and the country of origin of most these clippers is Russia.
* There are few steps you can take to make yourself less vulnerable like use of antivirus and being cautious while downloading any files and while using clipboard and provide the best way for safeguarding one from such malware.
* In the end, no protection is absolute. But a combination of personal awareness and well-designed protective tools can make your computer as safe as it can be.

# References

1. [MalwareBazaar | Browse malware samples (abuse.ch)](https://bazaar.abuse.ch/browse.php?search=tag%3Aclipper)
2. [Trends of malware influence on the integrated IT security system](https://www.e3s-conferences.org/articles/e3sconf/pdf/2019/61/e3sconf_itese18_04029.pdf)
3. [TAU Threat Discovery: Cryptocurrency Clipper Malware](https://blogs.vmware.com/security/2020/07/tau-threat-discovery-cryptocurrency-clipper-malware-evolves.html)
4. [First clipper malware discovered on Google Play | WeLiveSecurity](https://www.welivesecurity.com/2019/02/08/first-clipper-malware-google-play/)
5. [[Mal Series #6] AutoIT Analysis Guide | by GhouLSec | Medium](https://ghoulsec.medium.com/mal-series-6-autoit-analysis-guide-30072dda044a)