

Technical Analysis Report

FickerStealer

Darkside Ransomware

Teknik Analiz Raporu

Contents

[**Preview** 2](#_Toc79523819)

[**file.dll ANALYSIS** 3](#_Toc79523820)

[**7gfdg5egds.exe ANALYSIS** 6](#_Toc79523821)

[**NETWORK ANALYSIS** 12](#_Toc79523822)

[**SOLUTION PROPOSALS** 13](#_Toc79523823)

[**Yara Rules** 14](#_Toc79523824)

1

**Introduction**

FickerStealer is a infostealer threat offered as a MaaS (Malware-as-a-Service) on underground hacker forums. FickerStealer is distributed by various phishing methods. Infected computers of this malware;

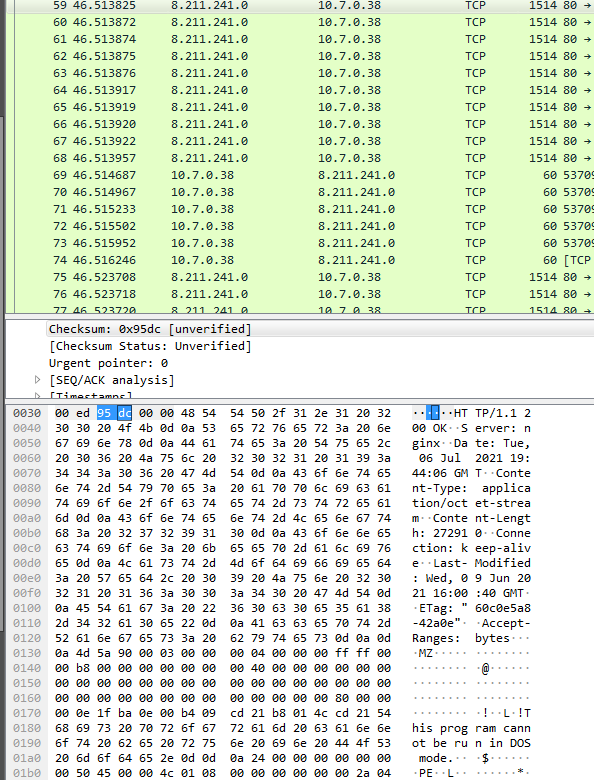
* Credentials saved in web browsers,
* Desktop messaging clients,
* To FTP clients,
* Blockchain wallets,
* It provides access to computer documents.

# **Preview**

The FickerStealer malware in the examined version continued to spread as a DLL with phishing methods. The malicious file was originally named “file.dll”. As a result of the analysis, it has been determined that this file acts as a loader to realize Stage 1.

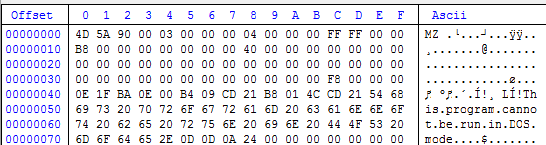
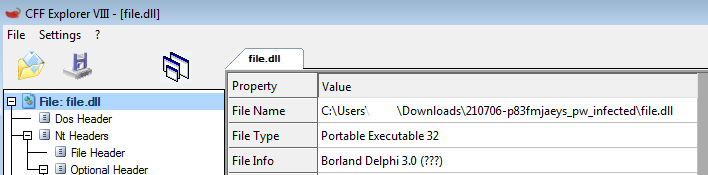
|  |  |
| --- | --- |
| File Name: | file.dll |
| MD5 | 9b59d4744ff1de8b338eeb2b85748cf2 |
| SHA1 | f3306e866bc9992c2268f204f55e88f89833a25d |
| SHA256 | fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8ad4 |

It has been observed that the file.dll malware downloads a file titled MZ when network traffic is monitored.

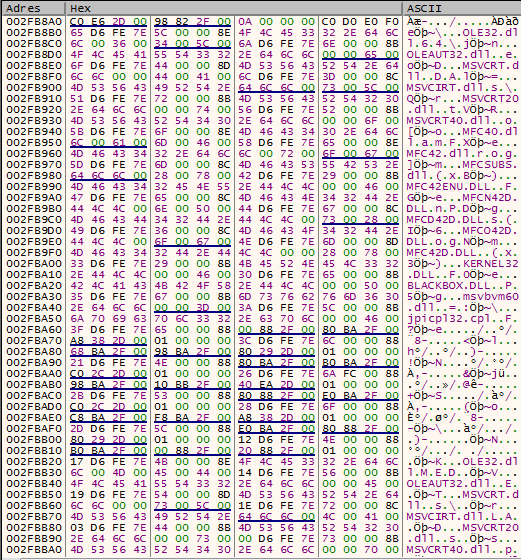


2

# **file.dll ANALYSIS**

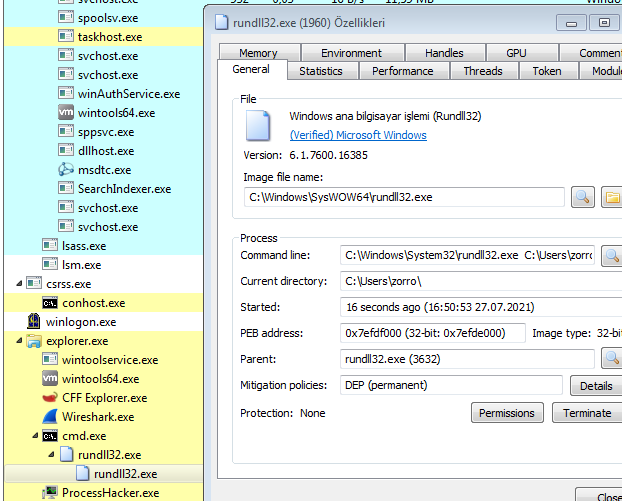
When file.dll is examined statically, it is seen that it is a 32-bit executable file.

**Dynamically loaded DLLs:**

****

|  |  |
| --- | --- |
| GDI32.dll | USP10.dll |
| MFC42.dll | msvcrt.dll |
| VERSION.dll | ADVAPI32.dll |
| MSCTF.dll | SHLWAPI.dll |
| OLEAUT32.dll | IMM32.dll |

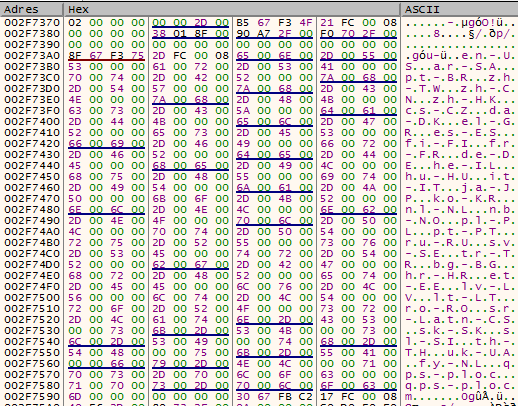
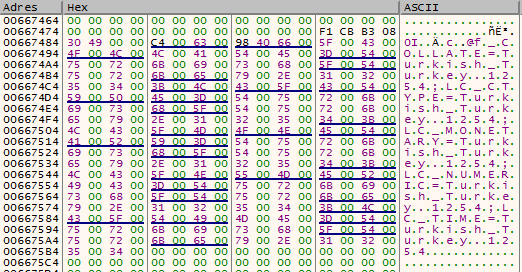
3

In general, when the behavior of file.dll is examined, it re-runs itself as suspend using the Process Hollowing technique.****

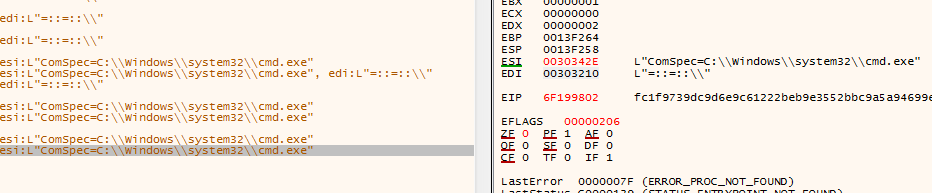
4

**Information Collected:**

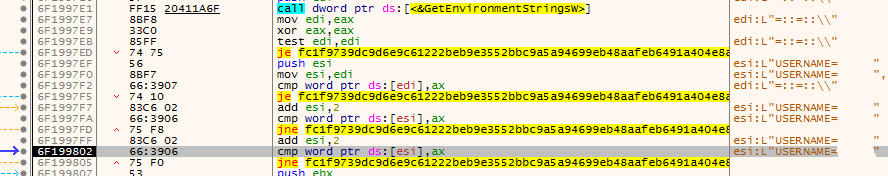
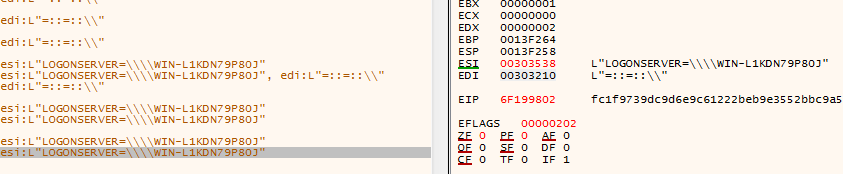
Targeted languages and countries:

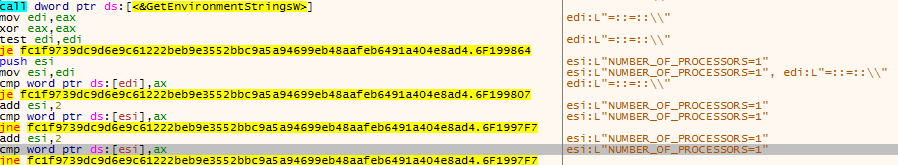


5

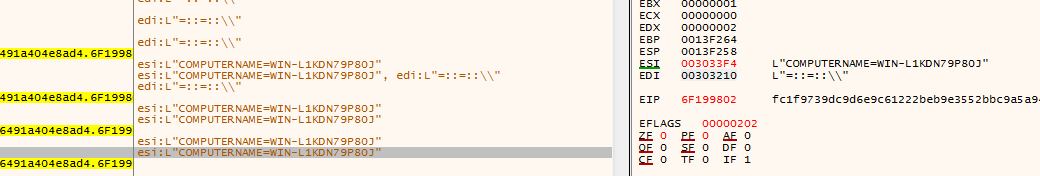
cmd.exe path:

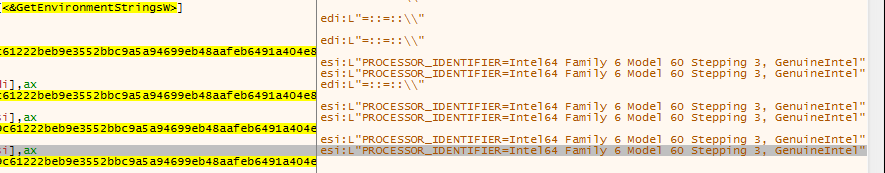
username:

LOGONSERVER:

NUMBER\_OF\_PROCESSOR:

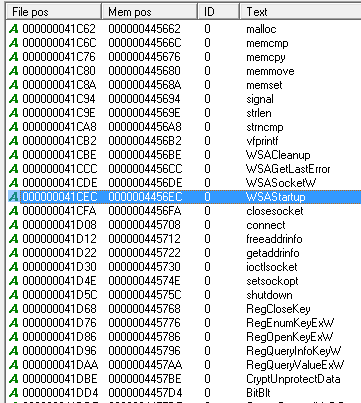
COMPUTERNAME:

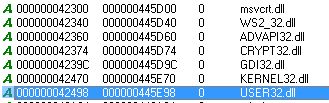


PROCESSOR:

# **7gfdg5egds.exe ANALYSIS**

|  |  |
| --- | --- |
| File Name: | 7gfdg5egds.exe |
| MD5 | 270C3859591599642BD15167765246E3 |
| SHA1 | E227A8A338166DC97E360CA9CDDDA5E007079C58 |
| SHA256 | DEE4BB7D46BBBEC6C01DC41349CB8826B27BE9A0DCF39816CA8BD6E0A39C2019 |





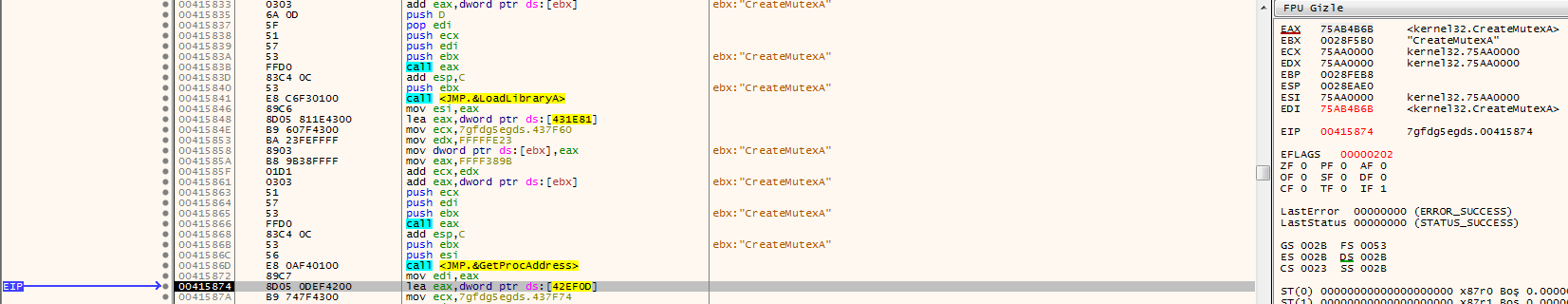
When we look at the imports of the pest, it uses important libraries such as USER32 and WS2\_32. When we look at again the WS2\_32 library, it is understood that it has the capacity to perform network operations, as can be seen from the functions it uses.

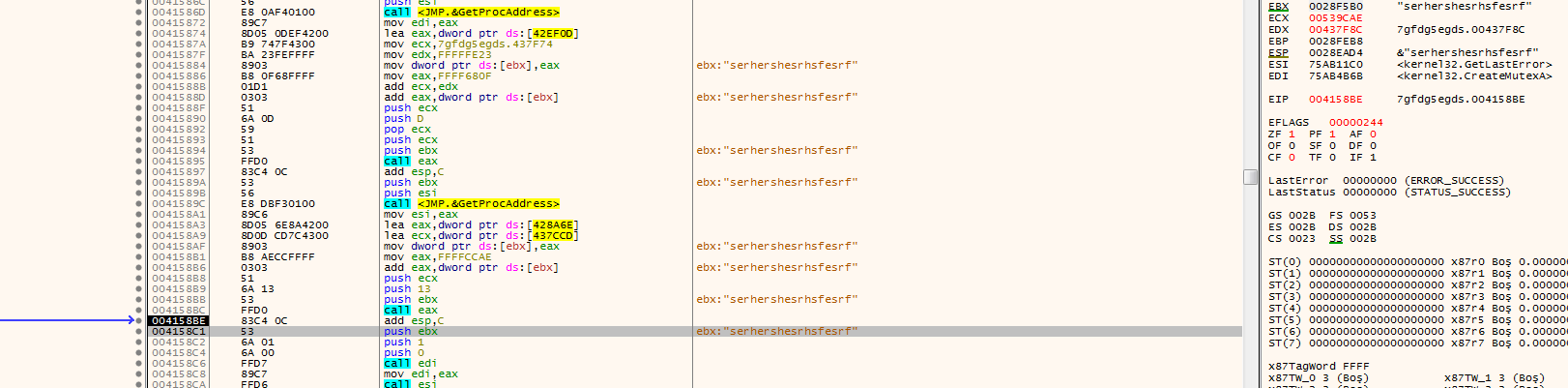
When we examine the important DLL and functions in the pest;

* CreateToolhelp32Snapshot
* WriteFile
* GetSystemInfo
* CreateMutexA

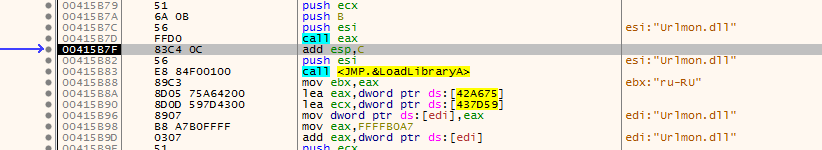
It is seen that the malware can Access system information, create a mutex object, get information about the system and files, write files, and take a snapshot of the process.

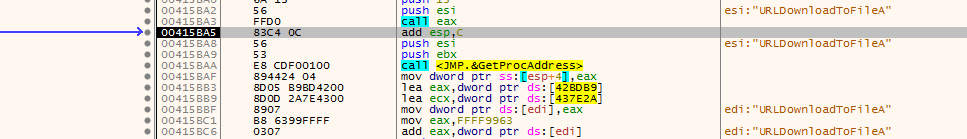
6

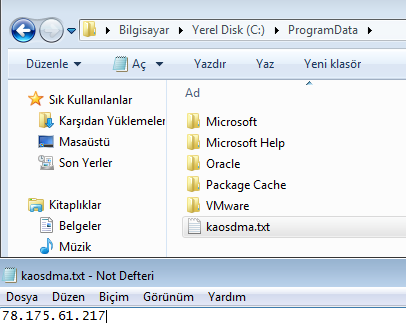
The malware first creates the mutex object with the "CreateMutexA" API that it loads dynamically.

Name of mutex object:

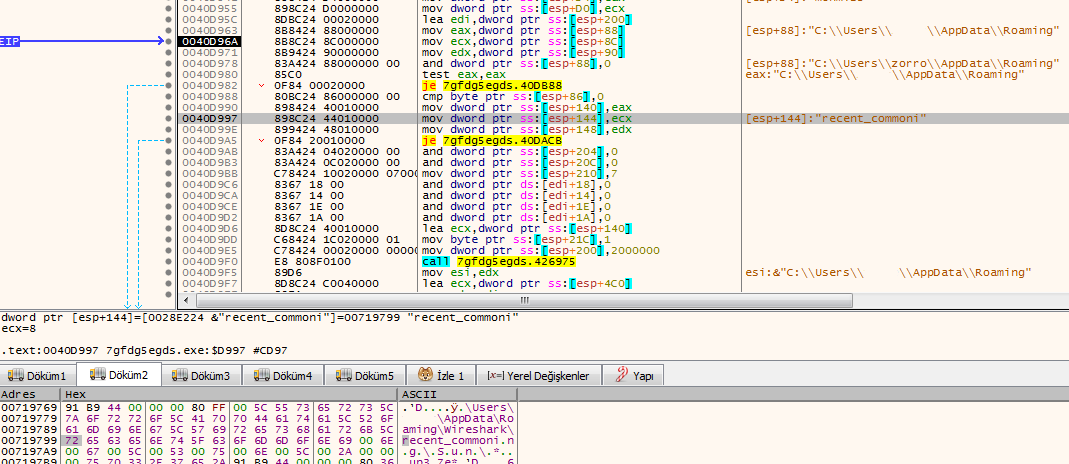


Some other DLL’s and APIs it loads dynamically:

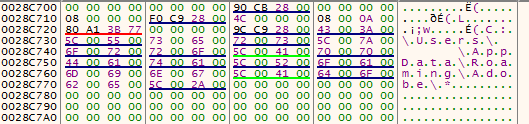


The malware then drops the .txt file with an ip address into ProgramData.

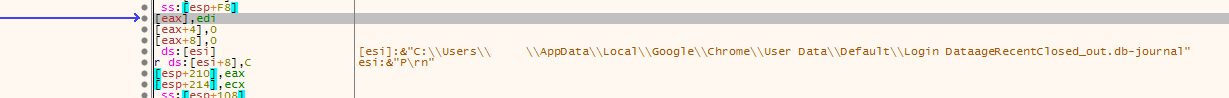
7

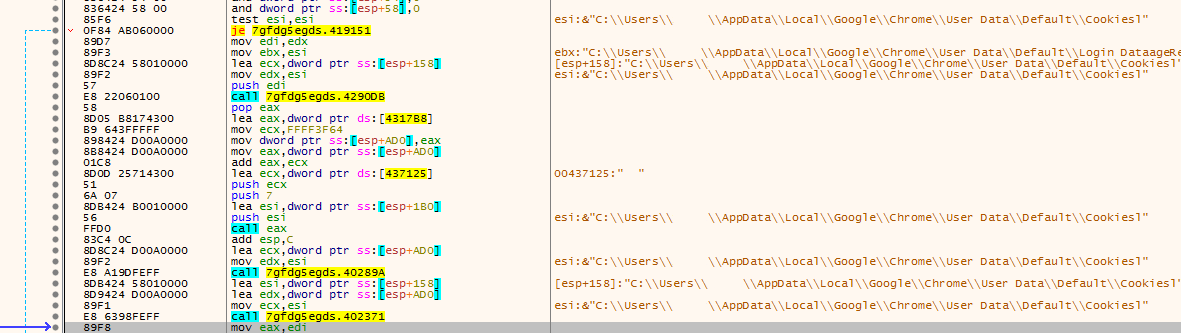
 In general, it is seen that the malware has 2 basic behaviors. First, it scans the software installed on the system.

8

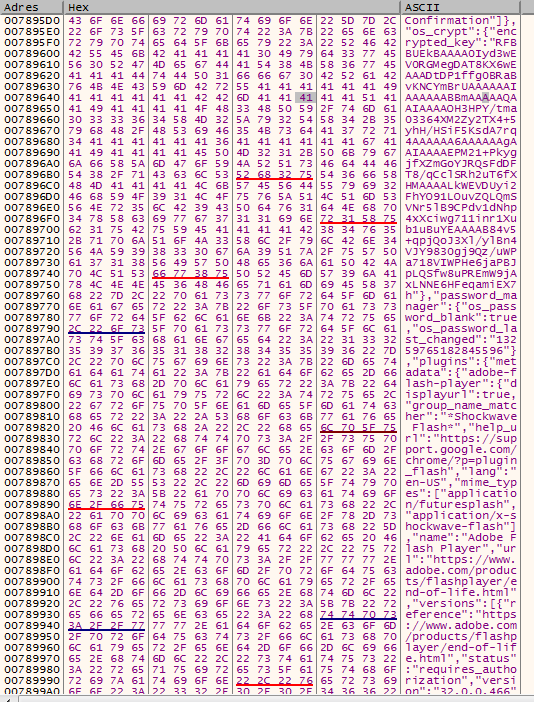
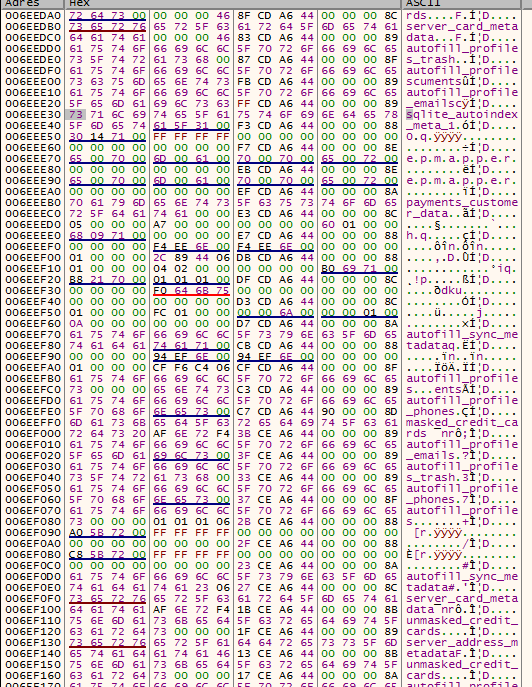


Another behavior is to steal personal data and identity information from web browsers. Since most applications are not installed, it seems that it just checks.

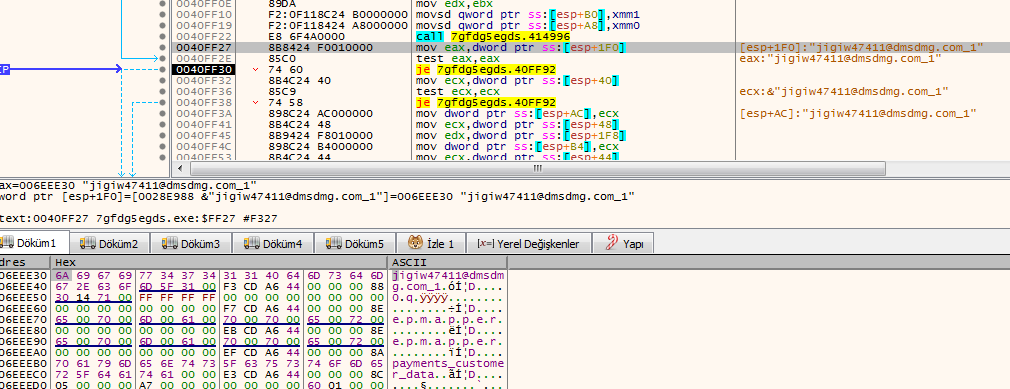
**Google Chrome:**

****

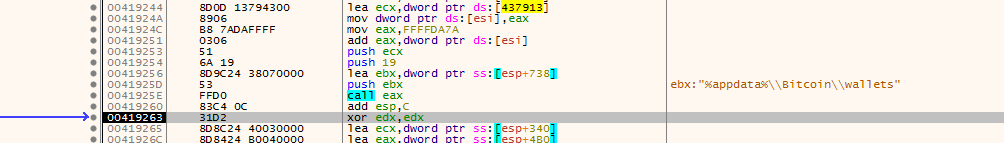
Phone number, credit card information kept in Google Chrome:

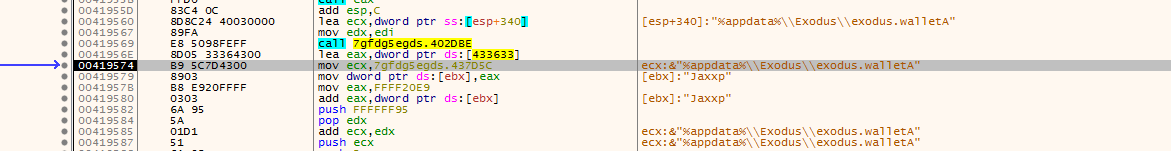


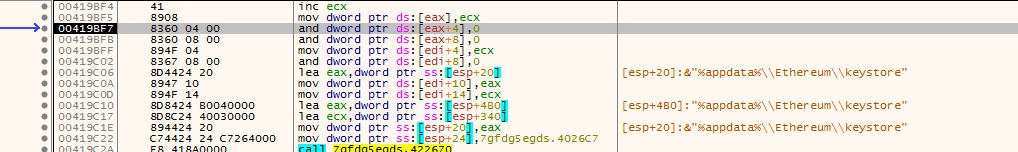
The email address that Google Chrome keeps after logging in:

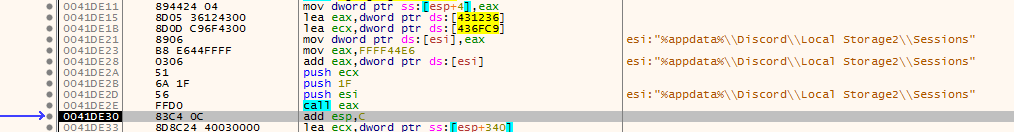


9

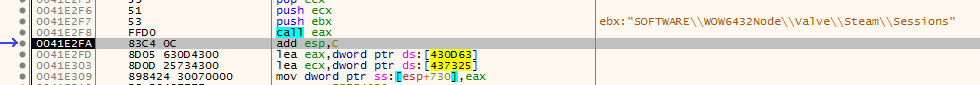
**Bitcoin wallet:**

**Exodus wallet:**

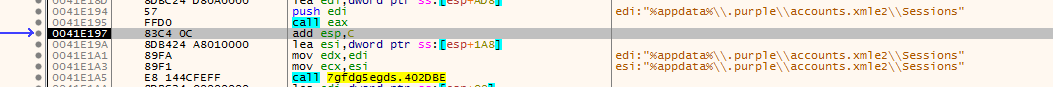
**Ethereum wallet:**

**Data from the Discord app:**

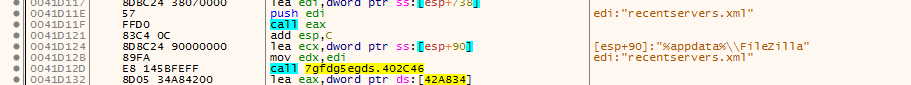
**Steam:**

****

**.purple:** It is the configuration directory in Windows. Here you can find information about the account, including chat logs, pictures from other users, passwords.

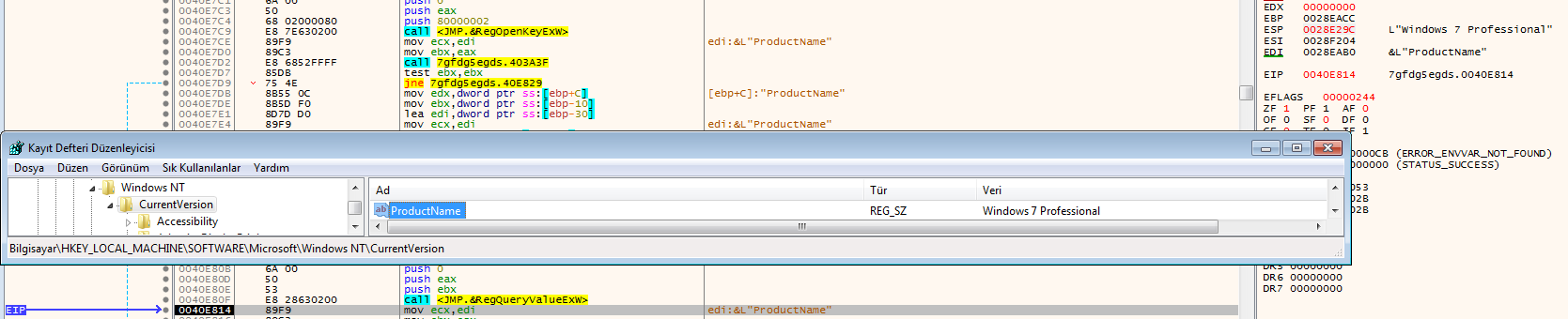


**FileZilla:**

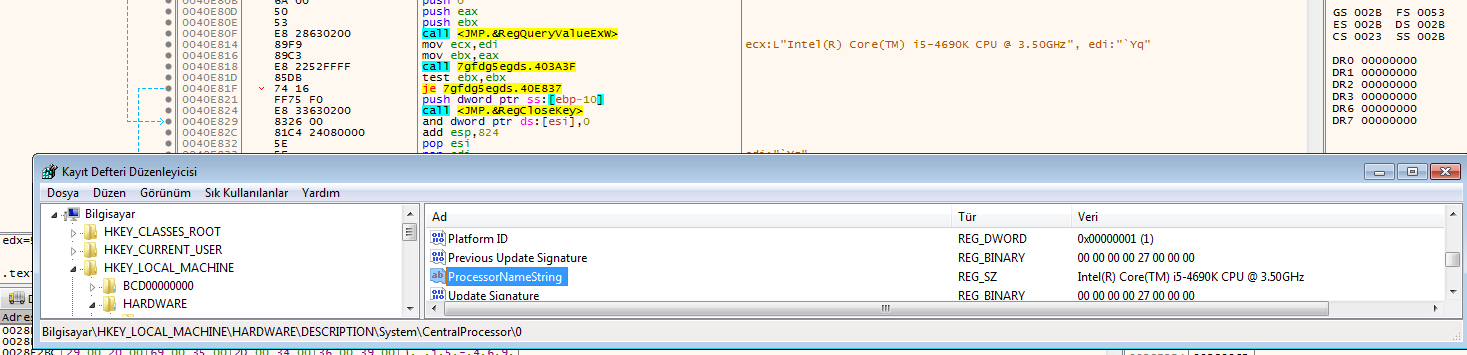
****

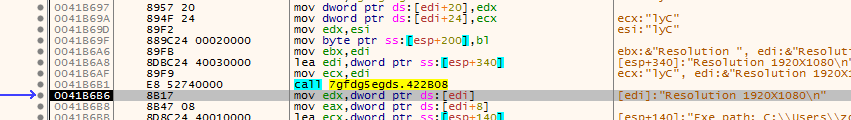
100

Here, the system information received by the malware is displayed.

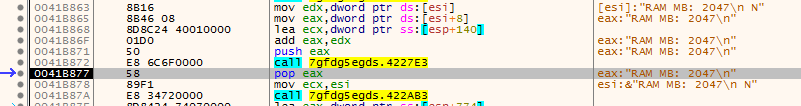
**OS:**

**Processor:**

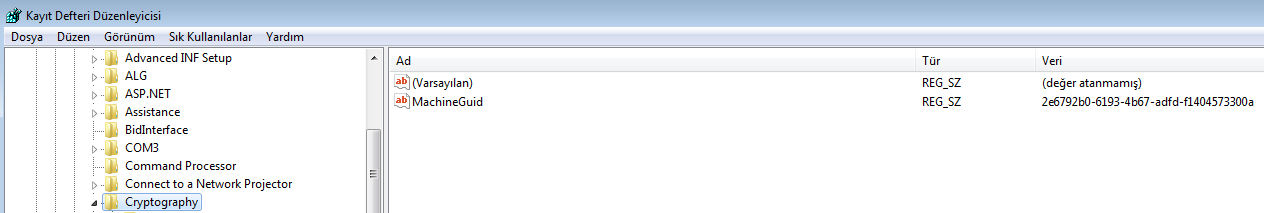
**Resolution:**

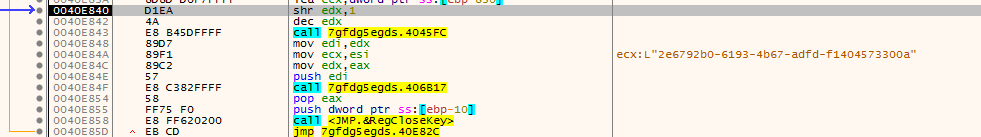
****

**Ram:**

****

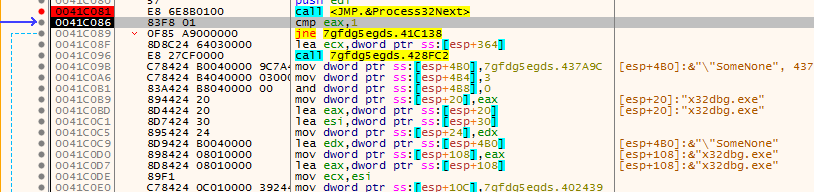
**Machine-Guid:**

****

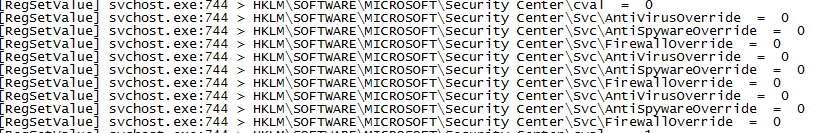
****

110

We see that the malware takes a snapshot of the operation.

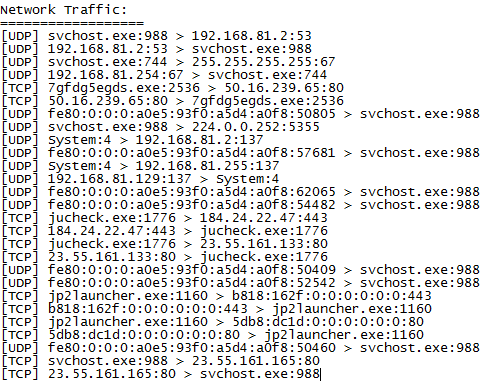
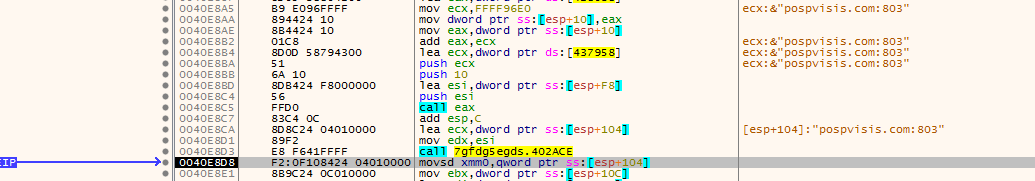


The values that the malware changes from the registry to escape antiviruses.



# **NETWORK ANALYSIS**

It has been seen that the malware tries to connect to the address 95[.]213[.]179[.]67[:]80 after stealing data. But because the server is not active, it could not establish a connection.



120

# 

# **SOLUTION PROPOSALS**

* Actual and reliable anti-virus software should be used on the systems.
* Incoming e-mails should be read carefully, e-mails and URLs from unknown sources and files should not be opened without a full scan of attachments.
* All installed software and operating system should be kept up to date.
* Train users frequently to be aware of potential phishing schemas and how to handle them in the right way.
* The network movements of the processes running on the system should be examined.

130

# **Yara Rules**

import "hash"

rule FickerStealer

{

meta:

author = "Hakan Soysal - ZAYOTEM"

description ="file.dll"

strings:

$export0 = "Closewhether"

$export1 = "Meantduck"

$export2 = "My"

$export3 = "Ropemay"

condition:

hash.md5(0,filesize) == "9b59d4744ff1de8b338eeb2b85748cf2" or all of them

}

140

import "hash"

rule FickerStealer

{

meta:

author ="Hakan Soysal - ZAYOTEM"

description ="7gfdg5egds.exe"

strings:

$a = "0x00010203040506070809101112131415161718192021222324252627282930313233343536373839404142434445464748495051525354555657585960616263646566676869707172737475767778798081828384858687888990919293949596979899[]"

$b = "\_matherr(): %s in %s(%g, %g) (retval=%g)\\n"

$c = {48 09 0A 46 45 1B 48 08 53 1D 39 81 07 46 0A 1D}

$d = {22 53 6F 6D 65 4E 6F 6E 65 00 00 00 BC 94 43 00}

condition:

hash.md5(0,filesize) == "270c3859591599642bd15167765246e3" or all of them

}

150

Hakan Soysal

<https://www.linkedin.com/in/hakansoysal/>

160