ThreatMon

RHADAMANTHYS STEALER ANALYSIS

@threatmon

@MonThreat

ThreatMon

Rhadamanthys Stealer Analysis Report

Table of Contents

Executive Summary

What Is Malware?

Malware, short for "**Malicious Software**", is software developed by cybercriminals to steal information and damage devices connected to the Internet. Common examples of malware are traditionally viruses, worms, trojans, and ransomware. However, stealer pests have also come to the fore in recent years.

What is Stealer Malware?

Stealer, as a term, completes itself as an information thief. This type of malware infects the device and then collects data from the device to send the information to the attacker. Typical targets are credentials used in online banking services, emails, or FTP accounts.

Stealer pests use multiple data collection methods. The most common ones are;

- Autofill username and password information
- computer name,
- RAM capacity,
- CPU Cores,
- Timezone,
- GEOIP,
- Wallet,
- History.

What is Rhadamanthys Stealer?

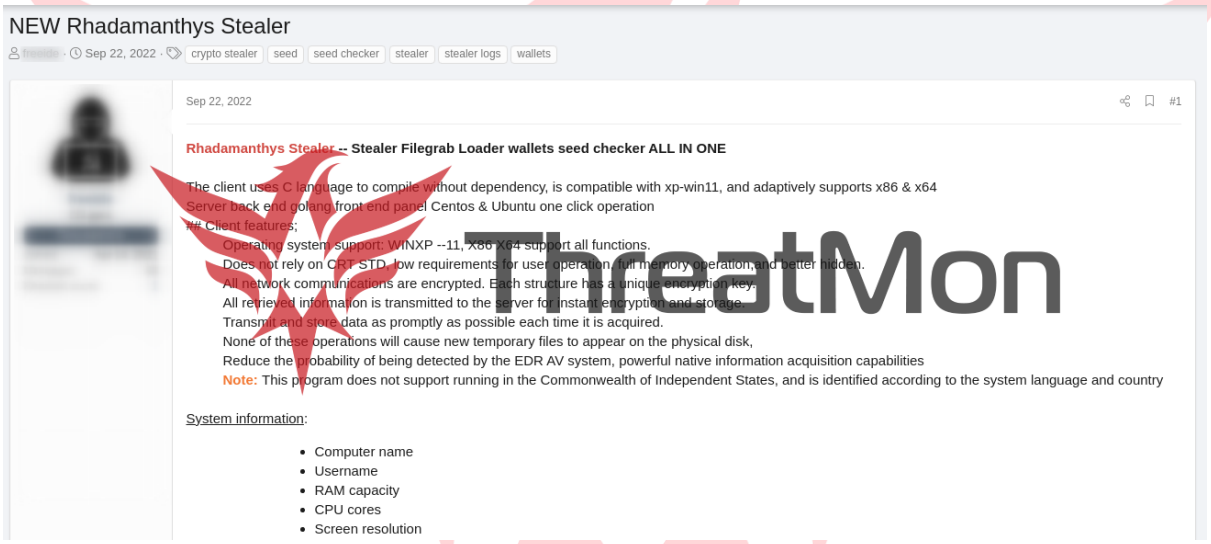
Rhadamanthys is a stealer trojan that is written in **C++** and compiled on **2022-08-22**, according to the information received from the hacker, Stealer is still under development.

Rhadamanthys reads your Registry, Computer Information, Browser Data and sends it to Hacker's C&C Server over encrypted WebSocket protocol.

Cyber Threat Intelligence Process

Rhadamanthys malware is a stealer variant developed by adopting MaaS structure, Malware as a Service. This malware, which was detected by the ThreatMon team during the Darkweb Forum activity check on September 26, 2022, was put into service in a global forum that is frequently used among Russian hackers. At ThreatMon, we have prepared a report on this new stealer malware.

How Was Rhadamanthys Detected?



NEW Rhadamanthys Stealer

Sep 22, 2022 · crypto stealer | seed | seed checker | stealer | stealer logs | wallets

Sep 22, 2022 #1

Rhadamanthys Stealer -- Stealer Filegrab Loader wallets seed checker ALL IN ONE

The client uses C language to compile without dependency, is compatible with xp-win11, and adaptively supports x86 & x64
Server back end golang front end panel Centos & Ubuntu one click operation
Client features;
Operating system support: WINXP --11, X86 X64 support all functions.
Does not rely on CRT STD, low requirements for user operation, full memory operation, and better hidden.
All network communications are encrypted. Each structure has a unique encryption key.
All retrieved information is transmitted to the server for instant encryption and storage.
Transmit and store data as promptly as possible each time it is acquired.
None of these operations will cause new temporary files to appear on the physical disk,
Reduce the probability of being detected by the EDR AV system, powerful native information acquisition capabilities
Note: This program does not support running in the Commonwealth of Independent States, and is identified according to the system language and country

System information:

- Computer name
- Username
- RAM capacity
- CPU cores
- Screen resolution

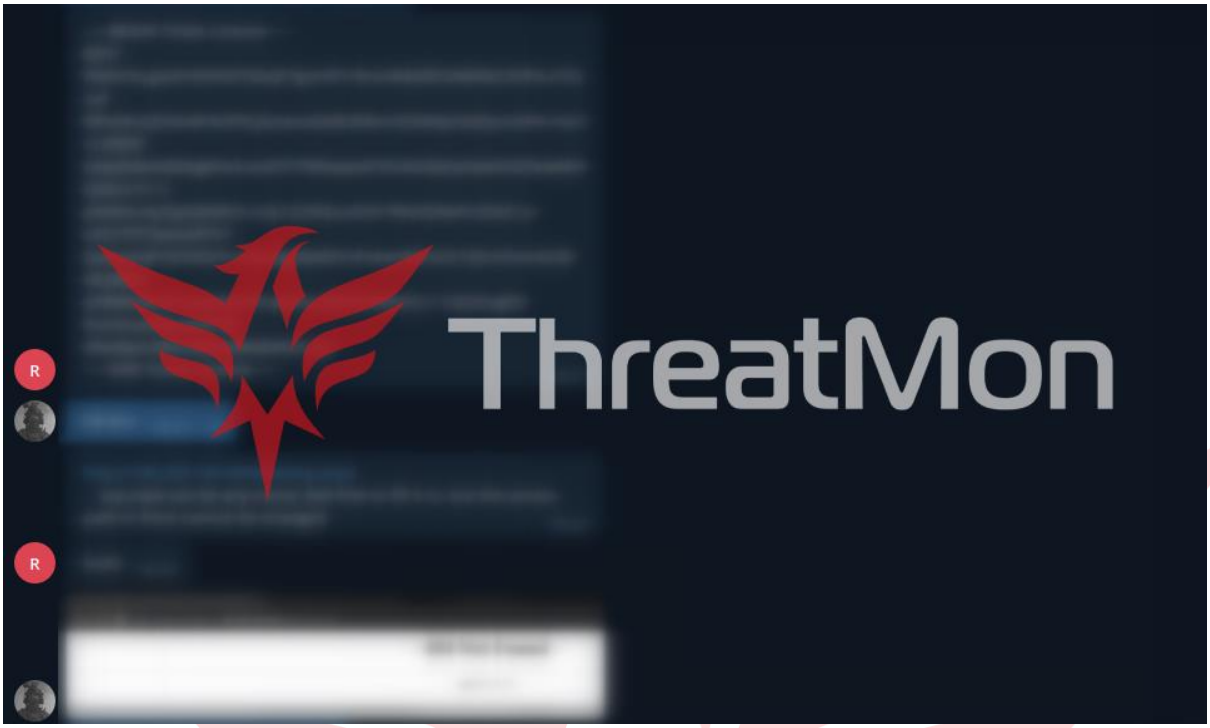
Rhadamanthys malware is a stealer variant developed by adopting MaaS structure, Malware as a Service. This malware, which was detected by the ThreatMon team during the routine Darkweb Forum activity check on September 26, 2022, was put into service in a global forum that is frequently used among Russian hackers.

As ThreatMon, we started working on this new stealer malware based on our professional experience in this regard.

Within the agreements made with the vendor, we searched for traces of a previous trace of this malware or whether it could be a version of a different variant using various methods, and we came to the conclusion that this malware is a completely independent and new type of stealer malware.

As a result of the studies carried out by ThreatMon analysts, we obtained a sample stealer panel and license from the vendor and started to examine the features and offerings of this new stealer.

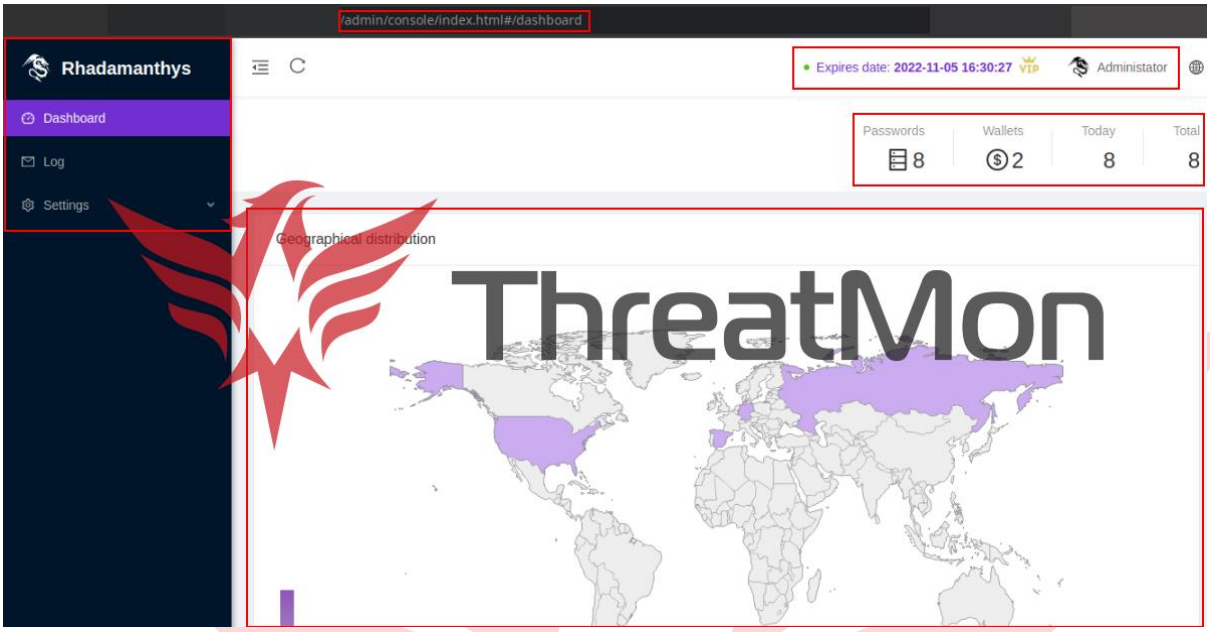
Rhadamanthys Stealer Analysis



The image you see above belongs to the access panel obtained as a result of the social engineering techniques applied by contacting the seller.

Rhadamanthys Stealer Analysis

What Are the Characteristics and Abilities of Rhadamanthys?



Here is a Dashboard image of the Rhadamanthys Stealer software.

Rhadamanthys malware is written in C++, as can be seen in many malware types and variants. According to the information detected by ThreatMon analysts in their analysis, this malware has an architecture that can be executed on all Windows-based operating systems from Windows XP to Windows 11. Malware can carry out malicious activities on two architectures, x64 and x86.

The malware demands minimum requirements to operate and has full memory and network encryption on all systems.

It also has completely independent and unique encryption keys for each stealer malicious file. Another stealer feature detected makes it impossible to see and detect temporary files created on the system in order to carry out malicious activities.

For this reason, stealer can avoid being caught by Anti-virus and EDR systems. The fact that Rhadamanthys carries out these malicious activities completely confidentially also poses a great risk to users.

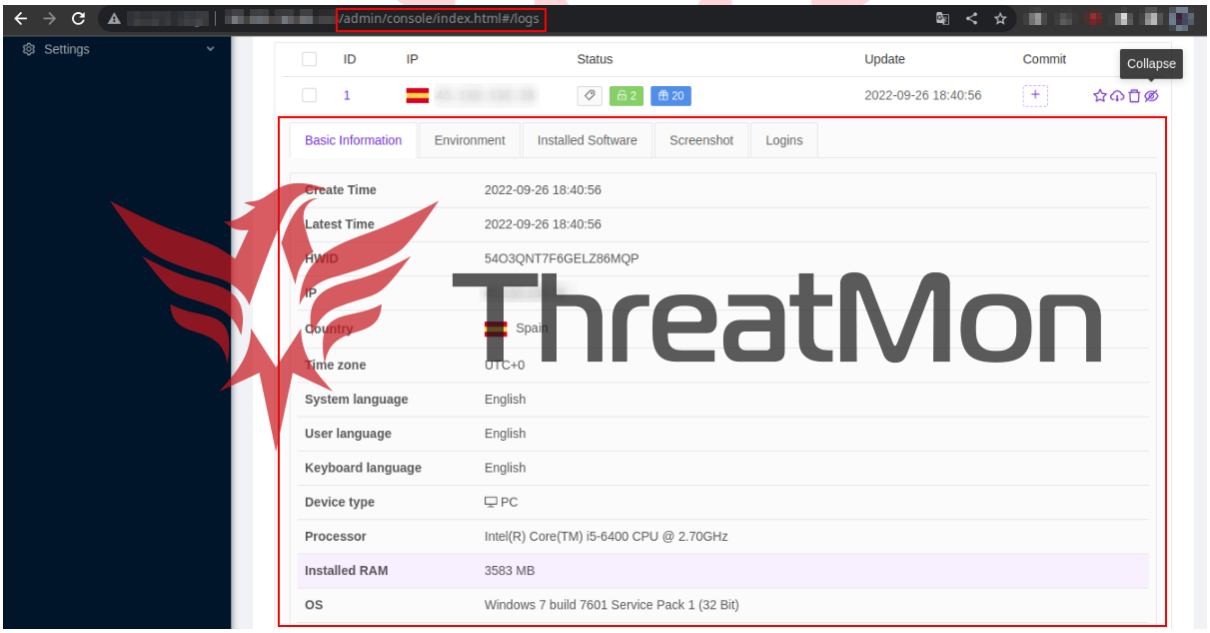
Also, according to the information obtained, the malware producer does not work on the Commonwealth of Independent States. For this reason, it prevents the attacks of the people who produce the malware against these countries.

Harmful Activities Executed on the System

As a result of the analysis made by ThreatMon analysts, the information leaked by the Rhadamanthys malware in order to carry out its malicious activities is listed.

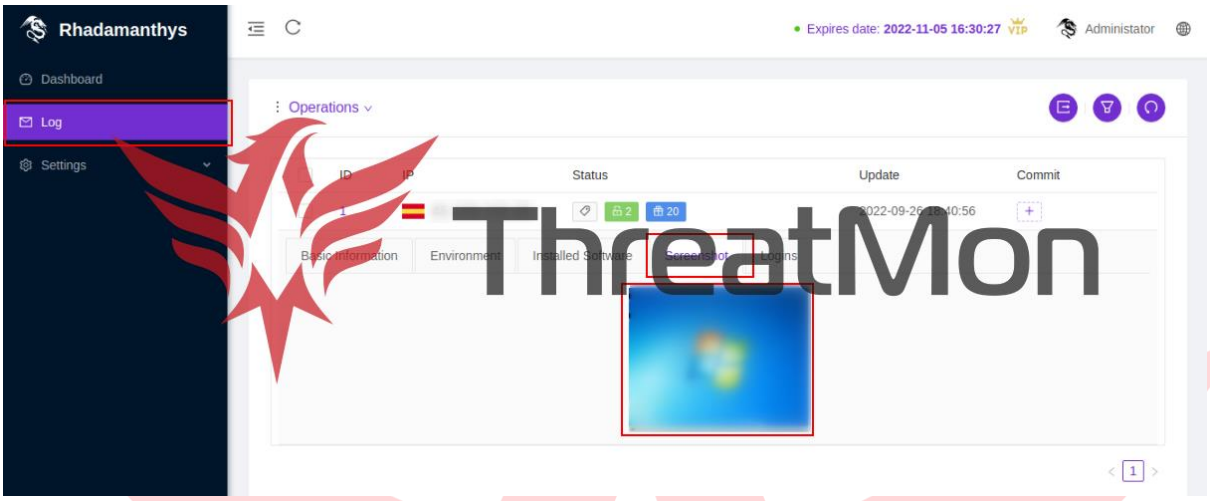
- Computer Name
- Username
- RAM Information
- CPU Information
- Screen resolution
- Time Zone
- GEO Information and IP Address
- programs on the computer
- Screenshot

Below is the display of the leaked information on the side of leaking system information of the Rhadamanthys malware, which was accessed by ThreatMon analysts, on the panel.



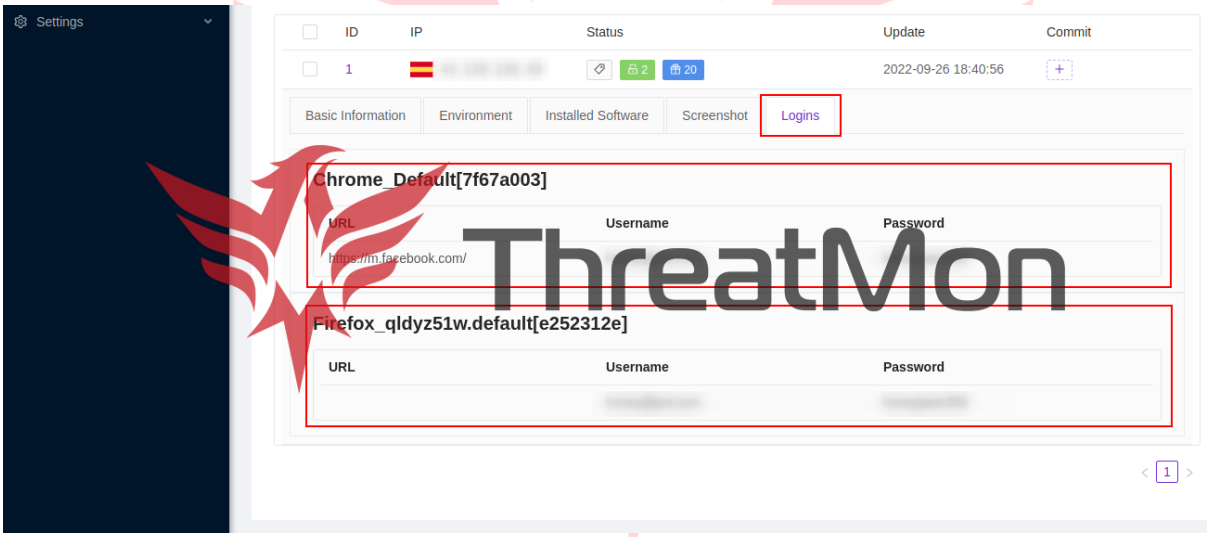
Rhadamanthys Stealer Analysis

In addition, the image you see below includes the screenshot taken on the infected system and then the image of the leaked data on the system before it was exported.



Browser Activities

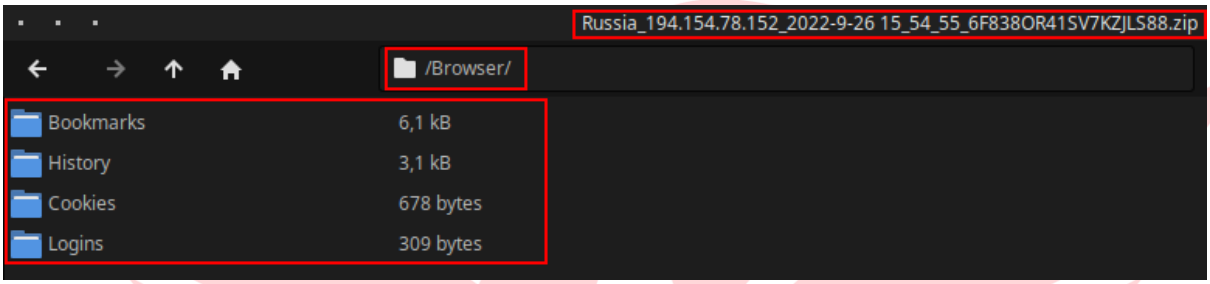
As a result of the analyzes made by ThreatMon analysts, it has been observed that Rhadamanthys malware can work on browser engines such as Gecko, Chromium and Trident and leak data.



Rhadamanthys Stealer Analysis

Browser information leaked by Rhadamanthys Stealer malware on infected systems is listed below.

- Cookies
- history
- autofil
- credits
- Downloads
- Favorites
- Extension



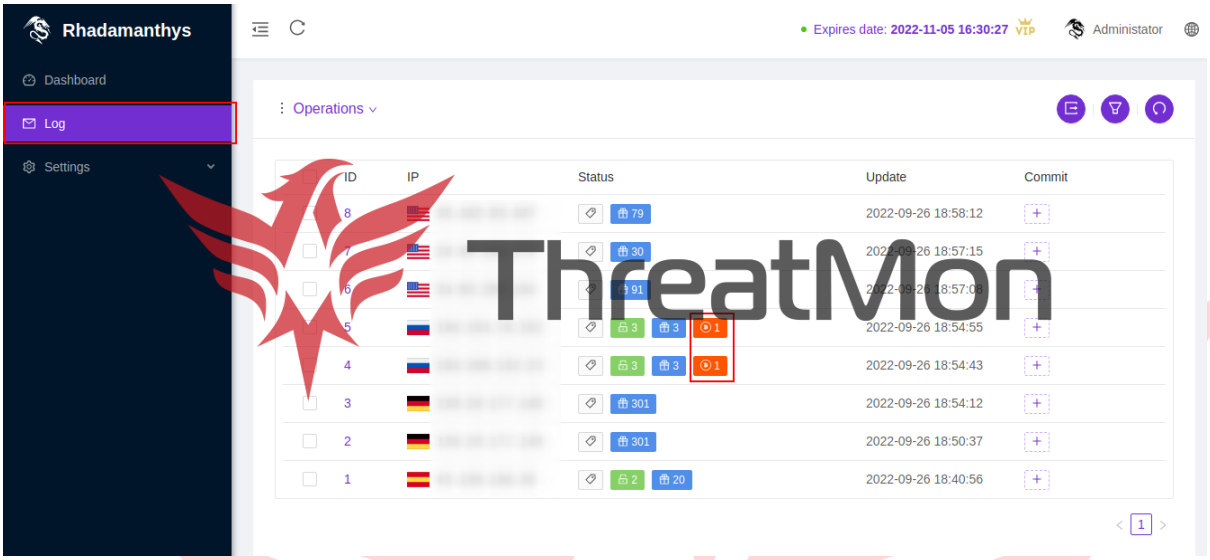
In addition, popular internet browsers that users may be affected by are listed below.

- Brave
- Opera
- Firefox
- Google Chrome
- Opera GX Opera
- AVG Browser
- AVAST Browser
- Avant Browser

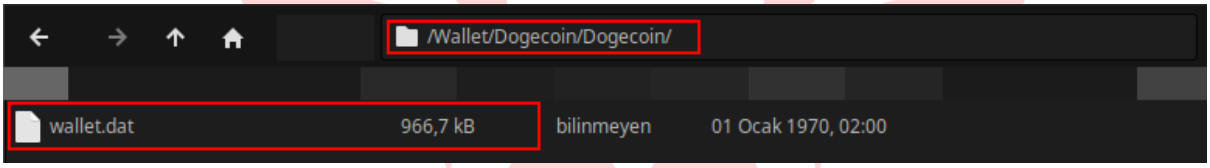
Rhadamanthys Stealer Analysis

Coin Wallets

It has also been detected by ThreatMon analysts that this new type of stealer, Rhadamanthys, has also leaked crypto wallet data.



Above, there is information on how the data of Crypto Wallets leaked by ThreatMon analysts are listed in Rhadamanthys Stealer's panel. In addition, when the leaked data is exported, the information in the stealer file is given below visually.



Below are the Crypto wallets and information that Rhadamanthys can leak among the activities that Rhadamanthys can run on the system.

Rhadamanthys Stealer Analysis

Leakable Wallets on the System | NAME – SYSTEM

Armory	System	Exodus	System
AtomicWallet	System	Frame	System
Atomicdex	System	Guarda	System
Binance Wallet	System	Jaxx	System
Bisq	System	LitecoinCore	System
BitcoinCore	System	Monero	System
BitcoinGold	System	MyCrypto	System
Bytecoin	System	MyMonero	System
Coinomi wallets	System	Safepay	System
DashCore	System	Solar wallet	System
DeFi-Wallet	System	Tokenpocket	System
Defichain-electrum	System	WalletWasabi	System
Dogecoin	System	Zap	System
Electron Cash	System	Zcash	System
Electrum	System	Zecwallet Lite	System
Electrum-LTC	System	Ethereum Wallet	System

Rhadamanthys Stealer Analysis

Browser Leakable Wallets | NAME – ID

Auvitas Wallet	klbgaboailigngkiifaglicepkfckppa	Phantom	bfnaelmomeimhlpmgjnjophhpkkoljpa
BitApp	fihkakfobkmkjojpchpfgcmhfjnmnfpi	Rabet Wallet	hgmoaheomcjnaheggkfafnjilfcefbmo
Crocobit	pnlfjmlcjdjgkddecgincndfgegkecke	Ronin Wallet	fnjhmkhhmkbjkkabndcnnogagogbneec
Exodus	aholpfdialjgjfhomihkjbmgjidlcdno	Slope Wallet	pocmplpaccanhmnllbbkpgfliimjljgo
Finnie	cjmkndjhnagcfbpiemnkdpomccnjblmj	Sollet	fhmfendgdocmcbmfikdcogofphimnkno
GuildWallet	nanjmdknhkinifnkgdcggcfnhdaammmj	Starcoin	mfhbebgoclkghebffdldpobeajmbecfk
ICONex	flpiciilemghbmfalicajoolhkkenfel	Swash	cmndjbecilbocjfkibfbifhngkdmjgog
Jaxx	cjelfplplebdjjenllpjcblmjkfcffne	Terra Station	aiifbnbfobpmeekipheeijimdpnlpgpp
Keplr	dmkamcknogkgcdfhhbddcghachkejeap	Tron	ibnejdfjmmkpcnlpebklmnkoeoihofec
Liquality	kpfopkelmapcoipemfendmdcghnegimn	XinPay	bocpokimicclpaiekenaeelehdjllofo
MTV Wallet	aeachknmefphepccionboohckonoeemg	Yoroi Wallet	ffnbelfdoeiohenkjibnmadjiehjhajb
Math	afbcbjpbpfadlkmhmclhkeeodmamcflc	ZilPay Wallet	klnaejjgbibmhlephnhpmaofohgkpgkd
Metamask	nkbihfbeogaeaoehlefnkodbefgpgknn	binance	fhbohimaelbohpjbbldcngcnapndodjp
Mobox	fcckkdbjnoikooededlapcalpionmalo	coin98	aeachknmefphepccionboohckonoeemg
Nifty	Hhjbhnchjifpkchbcccnkeccabelmkcm		
Oxygen	fhilaheimglignddkjgofkcbgekhenbh		

Rhadamanthys Stealer Analysis

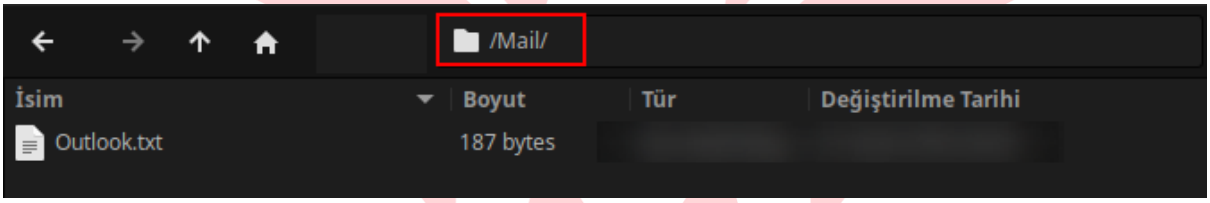
FTP Activities

In the attacks on the FTP Protocol, which was detected and tested by the ThreatMon team, it was determined that the Rhadamanthys software was able to attack the protocols listed below and leak information.

- Cyberduck
- FTP Navigator
- FTPRush
- FlashFXP
- Smartftp
- TotalCommander
- Winscp
- Ws_ftp
- Coreftp

Mail Activities

According to another detection and test by the ThreatMon team, Rhadamanthys software can attack FTP service applications and leak data, as well as attack Mail applications and leak data.



As stated in the image above, the malware can leak sensitive data of the Outlook service on the system.

- Mail Applications:
- CheckMail
- Claws-mail
- GmailNotifierPro
- Mailbird
- Outlook
- PostboxApp
- Thebat
- Thunderbird
- TrulyMail
- EM Client
- Foxmail

Rhadamanthys Stealer Analysis

Also, other Protocols and Applications that can leak data with proven accuracy tested by Rhadamanthys' ThreatMon analysts are as follows.

2FA & Pass:

- RoboForm
- WinAuth
- Authy Desktop
- KeePass (Memory interception password key DAT)

VPN:

- AzireVPN
- NordVPN
- OpenVPN
- PrivateVPN_Global_AB
- ProtonVPN
- WindscribeVPN

NOTE:

- NoteFly
- Notezilla
- Simple Sticky Notes
- Windows Sticky Notes of win7 10

Messaging:

- Discord
- Telegram
- Psi+
- Pidgin
- Tox

As an extra, this malware has the capacity to leak files. It can leak all your documents, including files with special characters.

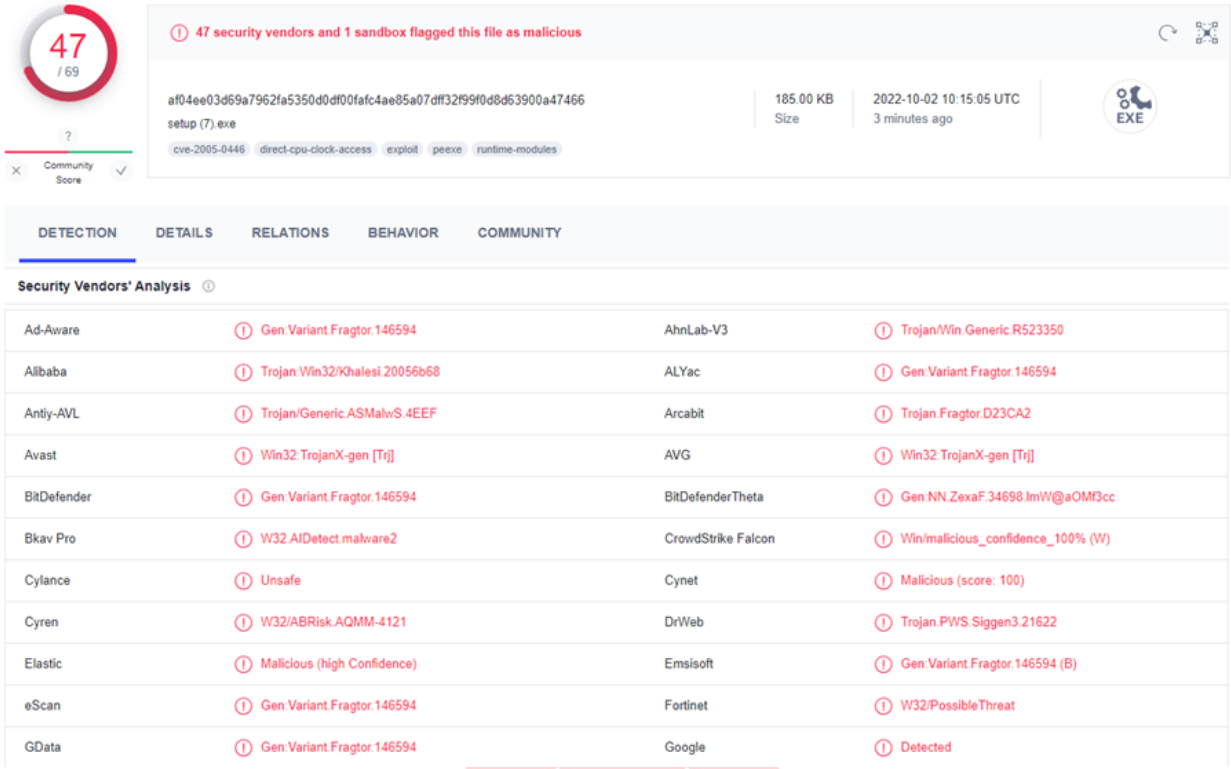
Now we will move on to the static and dynamic analysis of this stealer.

Analysis and Findings

Analysis of Rhadamanthys Stealer

The malware that received from the attacker was first analyzed through **Virustotal**.

"**47** security vendors and 1 sandbox flagged this file as malicious."



Rhadamanthys Stealer Analysis

Secondly, the header of the PE (Portable Executable) file is analyzed. The compilation date of the file is **22 August 2022**.

- setup (7).exe
  - IMAGE_DOS_HEADER
  - MS-DOS Stub Program
  - IMAGE_NT_HEADERS
    - Signature
    - IMAGE_FILE_HEADER
    - IMAGE_OPTIONAL_HEADER
  - IMAGE_SECTION_HEADER .text
  - IMAGE_SECTION_HEADER .rdata
  - IMAGE_SECTION_HEADER .data
  - SECTION .text
  - SECTION .rdata
  - SECTION .data

pFile	Data	Description	Value
00000084	014C	Machine	IMAGE_FILE_MACHINE_I386
00000086	0003	Number of Sections	
00000088	63038F42	Time Date Stamp	2022/08/22 Mon 14:14:26 UTC
0000008C	00000000	Pointer to Symbol Table	
00000090	00000000	Number of Symbols	
00000094	00E0	Size of Optional Header	
00000096	0103	Characteristics	
		0001	IMAGE_FILE_RELOCS_STRIPPED
		0002	IMAGE_FILE_EXECUTABLE_IMAGE
		0100	IMAGE_FILE_32BIT_MACHINE

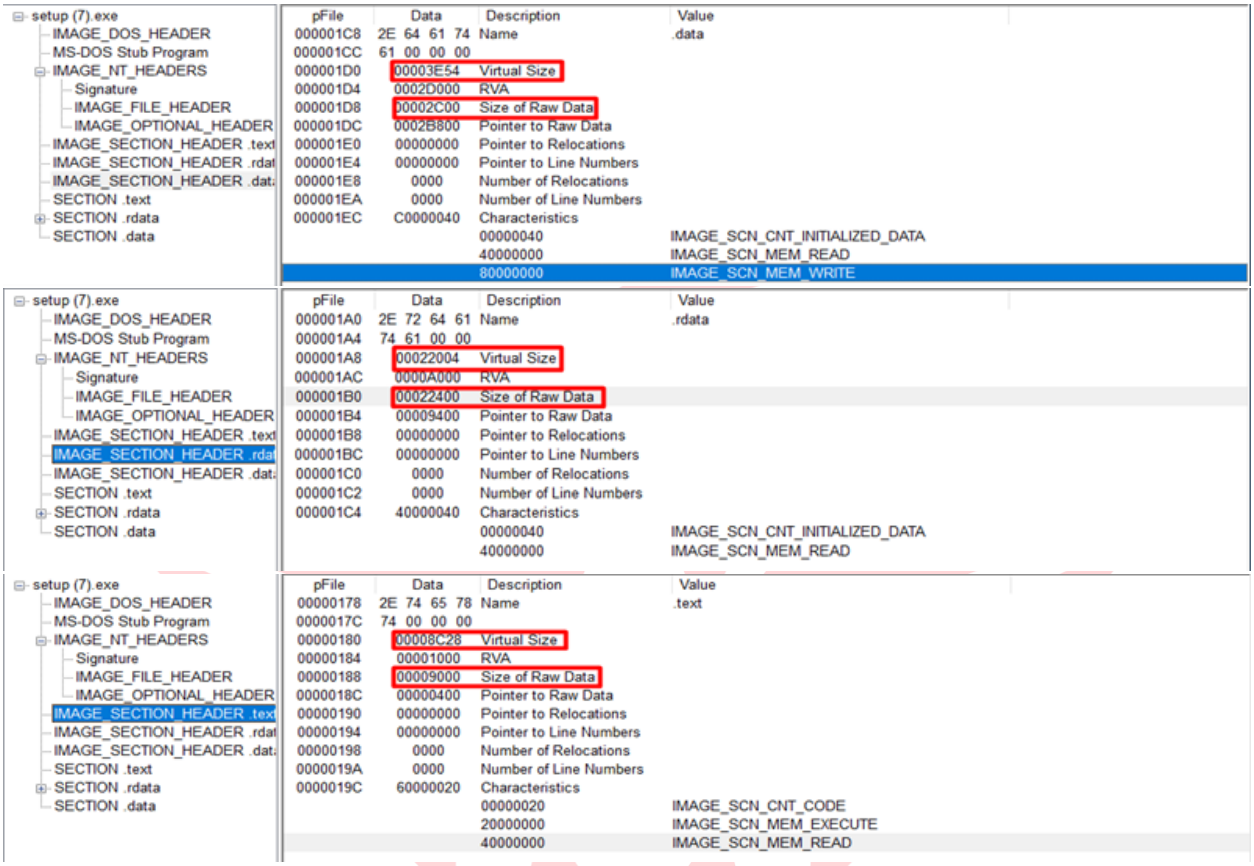
IMAGE_SUBSYSTEM_WINDOWS_GUI value shows us there can be a Graphical Interface of the file.

- setup (7).exe
  - IMAGE_DOS_HEADER
  - MS-DOS Stub Program
  - IMAGE_NT_HEADERS
    - Signature
    - IMAGE_FILE_HEADER
    - IMAGE_OPTIONAL_HEADER
  - IMAGE_SECTION_HEADER .text
  - IMAGE_SECTION_HEADER .rdata
  - IMAGE_SECTION_HEADER .data
  - SECTION .text
  - SECTION .rdata
  - SECTION .data

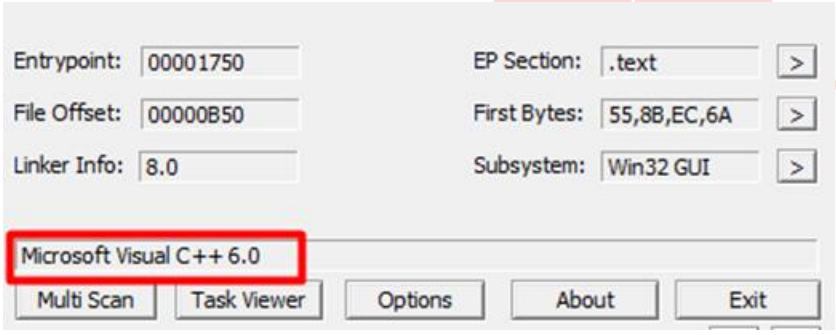
pFile	Data	Description	Value
00000084	014C	Machine	IMAGE_FILE_MACHINE_I386
00000086	0003	Number of Sections	
00000088	63038F42	Time Date Stamp	2022/08/22 Mon 14:14:26 UTC
0000008C	00000000	Pointer to Symbol Table	
00000090	00000000	Number of Symbols	
00000094	00E0	Size of Optional Header	
00000096	0103	Characteristics	
		0001	IMAGE_FILE_RELOCS_STRIPPED
		0002	IMAGE_FILE_EXECUTABLE_IMAGE
		0100	IMAGE_FILE_32BIT_MACHINE

Rhadamanthys Stealer Analysis

The Virtual and Disk Sizes of the sections look normal. If the virtual size was larger than the disk size, it would be an indicator that there is packaging here.

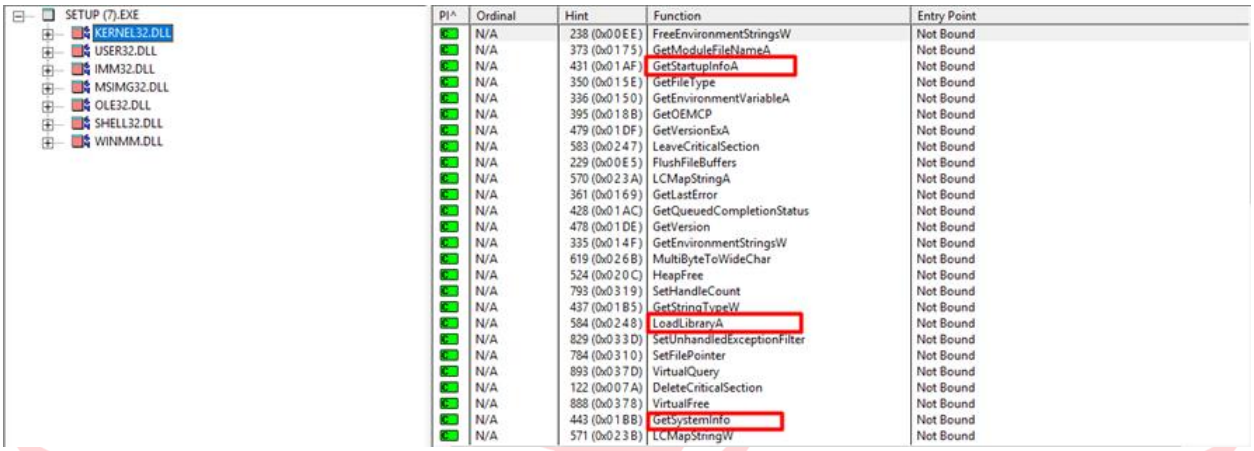


Stealer was written in **C++** and there is no packaging.



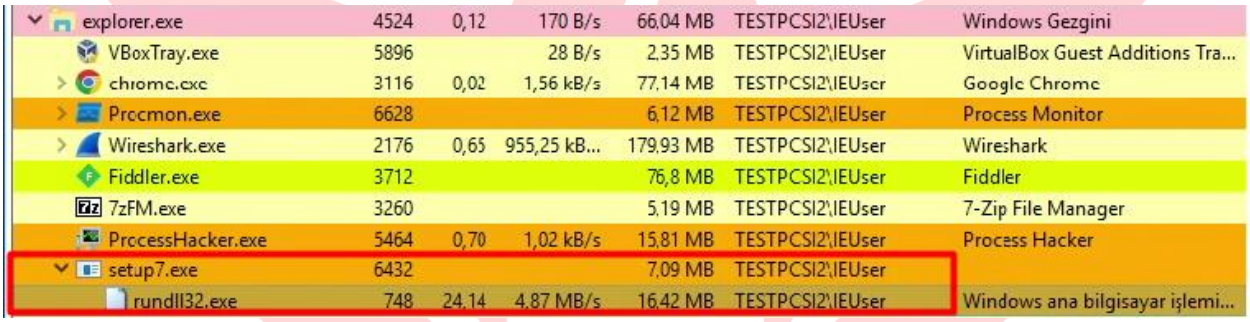
There are some functions imported by stealer that look suspicious like **GetStartupInfo** and **LoadLibrary**. **LoadLibrary** function often used by malwares to be stealthy.

Rhadamanthys Stealer Analysis



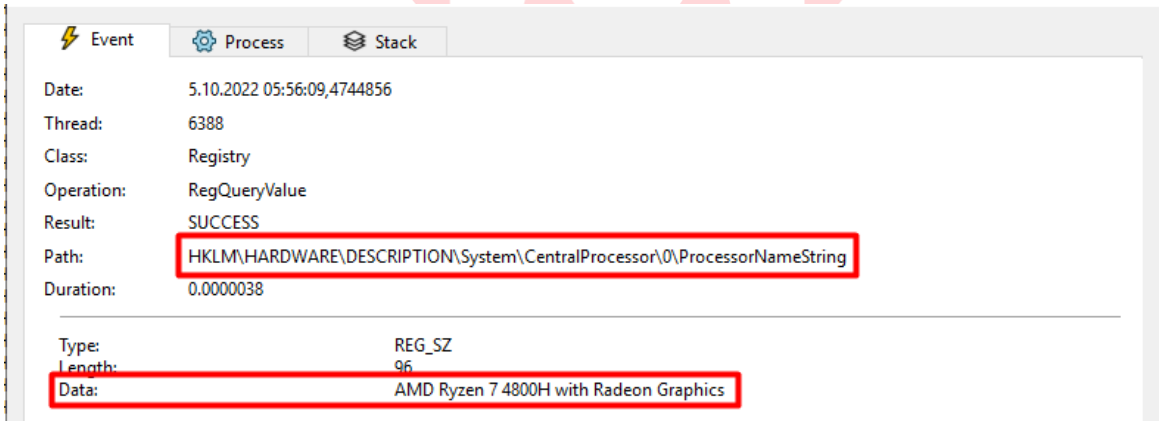
PI^	Ordinal	Hint	Function	Entry Point
	N/A	238 (0x00EE)	FreeEnvironmentStringsW	Not Bound
	N/A	373 (0x0175)	GetModuleFileNameA	Not Bound
	N/A	431 (0x01AF)	GetStartupInfoA	Not Bound
	N/A	350 (0x015E)	GetFileType	Not Bound
	N/A	336 (0x0150)	GetEnvironmentVariableA	Not Bound
	N/A	395 (0x018B)	GetOEMCP	Not Bound
	N/A	479 (0x01DF)	GetVersionExA	Not Bound
	N/A	583 (0x0247)	LeaveCriticalSection	Not Bound
	N/A	229 (0x00E5)	FlushFileBuffers	Not Bound
	N/A	570 (0x023A)	LCMapStringA	Not Bound
	N/A	361 (0x0169)	GetLastError	Not Bound
	N/A	428 (0x01AC)	GetQueuedCompletionStatus	Not Bound
	N/A	478 (0x01DE)	GetVersion	Not Bound
	N/A	335 (0x014F)	GetEnvironmentStringsW	Not Bound
	N/A	619 (0x026B)	MultiByteToWideChar	Not Bound
	N/A	524 (0x020C)	HeapFree	Not Bound
	N/A	793 (0x0319)	SetHandleCount	Not Bound
	N/A	437 (0x01B5)	GetStringTypeW	Not Bound
	N/A	584 (0x0248)	LoadLibraryA	Not Bound
	N/A	829 (0x033D)	SetUnhandledExceptionFilter	Not Bound
	N/A	784 (0x0310)	SetFilePointer	Not Bound
	N/A	893 (0x037D)	VirtualQuery	Not Bound
	N/A	122 (0x007A)	DeleteCriticalSection	Not Bound
	N/A	888 (0x0378)	VirtualFree	Not Bound
	N/A	443 (0x01BB)	GetSystemInfo	Not Bound
	N/A	571 (0x023B)	LCMapStringW	Not Bound

After execution of the setup.exe (Stealer) there is no significant operation was found. It is determined that **rundll32.exe** is executed by setup.exe and performs the actual operations.



explorer.exe	4524	0,12	170 B/s	66,04 MB	TESTPCSI2\IEUser	Windows Gezgini
VBoxTray.exe	5896		28 B/s	2,35 MB	TESTPCSI2\IEUser	VirtualBox Guest Additions Tra...
chrome.exe	3116	0,02	1,56 kB/s	77,14 MB	TESTPCSI2\IEUser	Google Chrome
Procmon.exe	6628			6,12 MB	TESTPCSI2\IEUser	Process Monitor
Wireshark.exe	2176	0,65	955,25 kB...	179,93 MB	TESTPCSI2\IEUser	Wireshark
Fiddler.exe	3712			76,8 MB	TESTPCSI2\IEUser	Fiddler
7zFM.exe	3260			5,19 MB	TESTPCSI2\IEUser	7-Zip File Manager
ProcessHacker.exe	5464	0,70	1,02 kB/s	15,81 MB	TESTPCSI2\IEUser	Process Hacker
setup7.exe	6432			7,09 MB	TESTPCSI2\IEUser	
rundll32.exe	748	24,14	4,87 MB/s	16,42 MB	TESTPCSI2\IEUser	Windows ana bilgisayar işlemi...

the CPU Information was read:



Event | Process | Stack

Date:	5.10.2022 05:56:09,4744856
Thread:	6388
Class:	Registry
Operation:	RegQueryValue
Result:	SUCCESS
Path:	HKLM\HARDWARE\DESCRIPTION\System\CentralProcessor\0\ProcessorNameString
Duration:	0.0000038

Type:	REG_SZ
Length:	96
Data:	AMD Ryzen 7 4800H with Radeon Graphics

Rhadamanthys Stealer Analysis

The Computer Name Information was read:

Event | Process | Stack

Date:	5.10.2022 05:56:09,3968772
Thread:	6388
Class:	Registry
Operation:	RegOpenKey
Result:	REPARSE
Path:	HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName
Duration:	0.0000031
Desired Access:	Read

Browser Database, Cookies, Credentials, SSH Hosts were also read by Stealer.

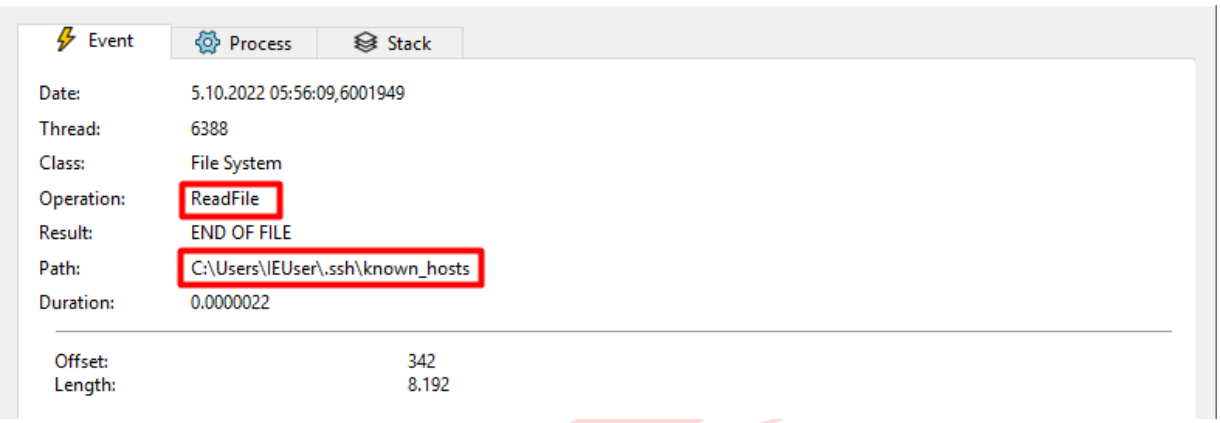
Event | Process | Stack

Date:	5.10.2022 05:56:09,3997943
Thread:	6388
Class:	File System
Operation:	ReadFile
Result:	SUCCESS
Path:	C:\Users\IEUser\AppData\Local\Google\Chrome\User Data\Default\Login Data
Duration:	0.0000306
Offset:	0
Length:	47.104
Priority:	Normal

Event | Process | Stack

Date:	5.10.2022 05:56:09,5868449
Thread:	6388
Class:	File System
Operation:	ReadFile
Result:	SUCCESS
Path:	C:\Users\IEUser\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000005.ldb
Duration:	0.0000106
Offset:	0
Length:	28.782
Priority:	Normal

Rhadamanthys Stealer Analysis



Event | Process | Stack

Date:	5.10.2022 05:56:09,6001949
Thread:	6388
Class:	File System
Operation:	ReadFile
Result:	END OF FILE
Path:	C:\Users\IEUser\.ssh\known_hosts
Duration:	0.0000022
Offset:	342
Length:	8.192

After reading operations, **stealer** sent our data to Hacker's C&C Channel over encrypted **Websocket** Protocol.

1809	66.512173	192.168.100.168	185.209.160.99	HTTP	232	GET /blob/top.mp4 HTTP/1.1
1812	66.903909	185.209.160.99	192.168.100.168	HTTP	183	HTTP/1.1 101 Switching Protocols
1813	66.914744	192.168.100.168	185.209.160.99	TCP	62	62548 → 80 [PSH, ACK] Seq=179 Ack=130 Win=66048 Len=8 [TCP segment of a reassembled PDU]
1814	66.951740	185.209.160.99	192.168.100.168	TCP	54	80 → 62548 [ACK] Seq=130 Ack=187 Win=64256 Len=0
1815	66.951922	192.168.100.168	185.209.160.99	WebSoc…	187	WebSocket Binary [FIN] [MASKED]
1816	66.990876	185.209.160.99	192.168.100.168	TCP	54	80 → 62548 [ACK] Seq=130 Ack=320 Win=64256 Len=0
1817	67.050292	185.209.160.99	192.168.100.168	WebSoc…	152	WebSocket Binary [FIN]
1818	67.061573	192.168.100.168	185.209.160.99	TCP	60	62548 → 80 [PSH, ACK] Seq=320 Ack=228 Win=66048 Len=6 [TCP segment of a reassembled PDU]
1819	67.099236	185.209.160.99	192.168.100.168	TCP	54	80 → 62548 [ACK] Seq=228 Ack=326 Win=64256 Len=0
1820	67.099416	192.168.100.168	185.209.160.99	WebSoc…	62	WebSocket Binary [FIN] [MASKED]
1824	67.137863	185.209.160.99	192.168.100.168	TCP	54	80 → 62548 [ACK] Seq=228 Ack=334 Win=64256 Len=0
1825	67.196849	185.209.160.99	192.168.100.168	WebSoc…	202	WebSocket Binary [FIN]
1826	67.222487	192.168.100.168	185.209.160.99	TCP	60	62548 → 80 [PSH, ACK] Seq=334 Ack=376 Win=65792 Len=6 [TCP segment of a reassembled PDU]
1827	67.222590	192.168.100.168	185.209.160.99	WebSoc…	1260	WebSocket Binary [FIN] [MASKED] [TCP segment of a reassembled PDU]
1828	67.222602	192.168.100.168	185.209.160.99	TCP	1260	62548 → 80 [PSH, ACK] Seq=1546 Ack=376 Win=65792 Len=1206 [TCP segment of a reassembled PDU]

Indicator of Compromise (IOC)

MD5 HASH
89ec4405e9b2cab987f2e4f7e4b1666e

URL / IP
185[.]209[.]160[.]99
http://185[.]209[.]160[.]99/blob/top.mp4

MITRE ATT&CK

Technic	ID
Steal Web Session Cookie	T1539
Credentials from Password Stores	T1555
Unsecured Credentials	T1552
Query Registry	T1012
Software Discovery	T1518
System Information Discovery	T1082

45305 Catalina cs St 150, Sterling VA 20166