ECHO

CYBER THREAT INTELLIGENCE

RHADAMANTHYS

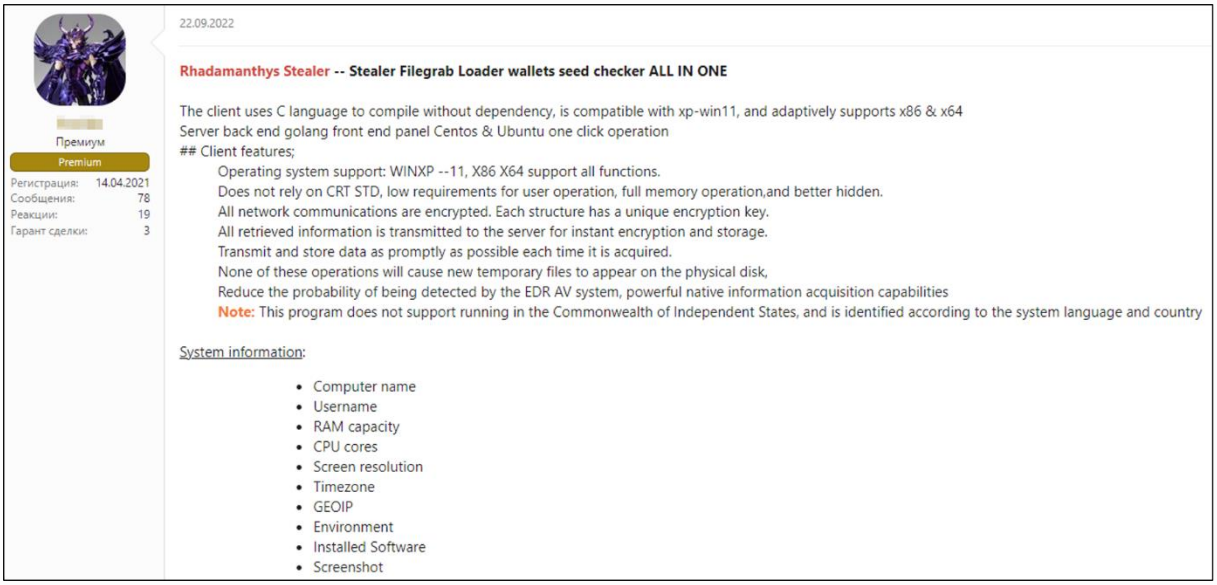
TECHNICAL ANALYSIS REPORT

Content

Introduction 3
Rhadamanthys Technical Analysis 4
ATTODiskBenchmark.exe 4
Process BlackList 5
Time-Based Side-Channel Attack Detection 6
API Hashing 7
Hashing of APIs 8
Network 12
Some of the collected cryptocurrency wallet extensions include: 13
Targeted browsers include: 13
FTP 14
YARA RULE 15
SIGMA RULE 16
Mittre Att&ck 17

Introduction

This report provides a technical analysis of the Rhadamanthys malware family, which has been active since October 2022. This stealer family demonstrates its effectiveness regardless of the country it targets. To gain insights into this stealer family and its activities, it is recommended to thoroughly read the report. Furthermore, to enhance your system's security, we suggest integrating the rules provided at the end of the report.



Şekil 1 Rhamadanthys Stealer for sale

As depicted in Figure 1, the distribution of this particular malware family is observed to be conducted through online forums in the described manner. Notably, it possesses distinctive characteristics that set it apart from other prevalent stealer malware families. These differences include:

- Implementation of Anti-Analysis Techniques
- Network Communication Patterns
- Utilization of APIs at the Kernel Level

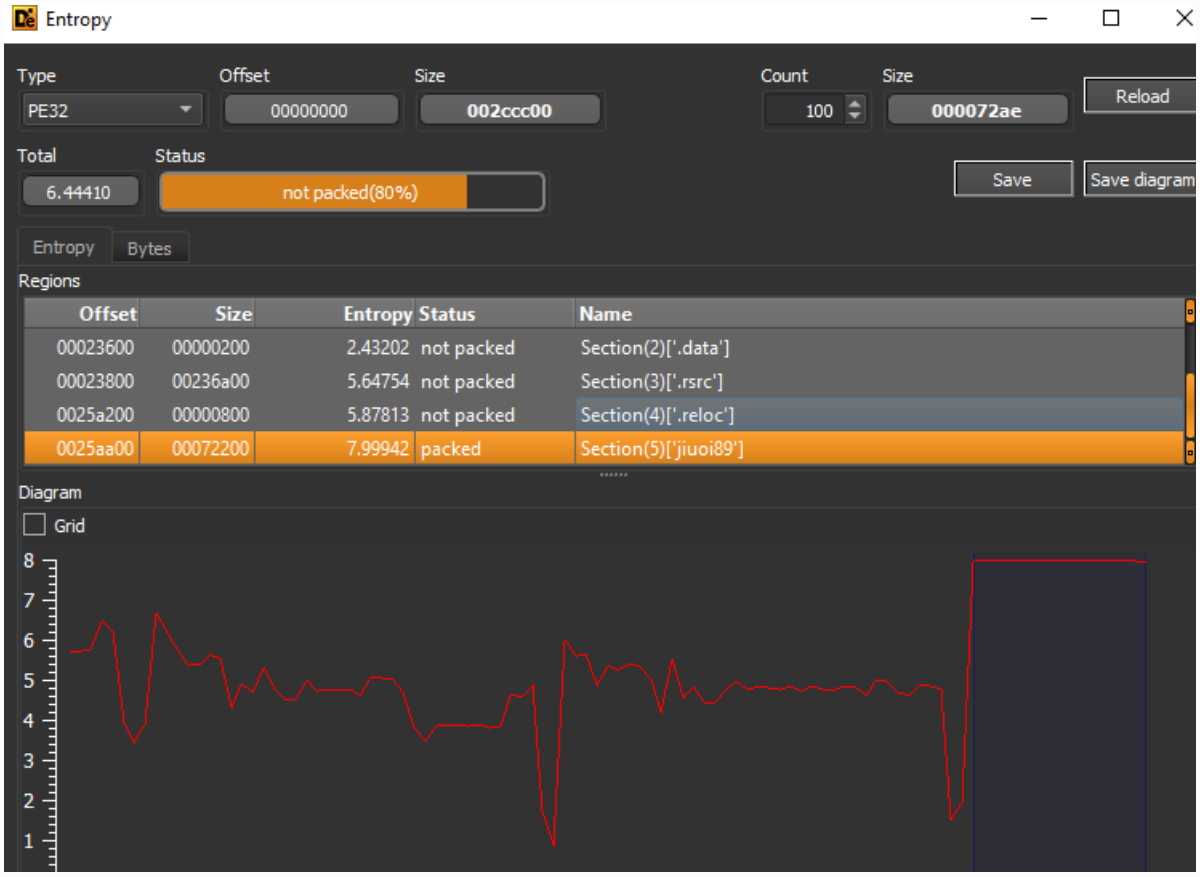
Furthermore, the Rhadamanthys family often employs mimicry of legitimate applications. Through Search Engine Optimization (SEO), it strategically positions itself ahead of authentic websites in browser searches, effectively imitating legitimate entities. Consequently, vigilance is recommended when accessing sites during searches for lawful applications to ensure their authenticity.

The examined Rhadamanthys malware, as detailed in this report, has been identified to impersonate the legitimate application **ATTO Disk Benchmark**.

Rhadamanthys Technical Analysis

ATTODiskBenchmark.exe

File Name	ATTODiskBenchmark.exe
SHA-1	fcb82785c04b3b805c58ca20d24e83c28dc73fc8
SHA-256	8e77cf490e5027b35fb25df886b991f9c63f7ecbca64aff34cd599a5ad9c63fd
File Type	PE32 - EXE

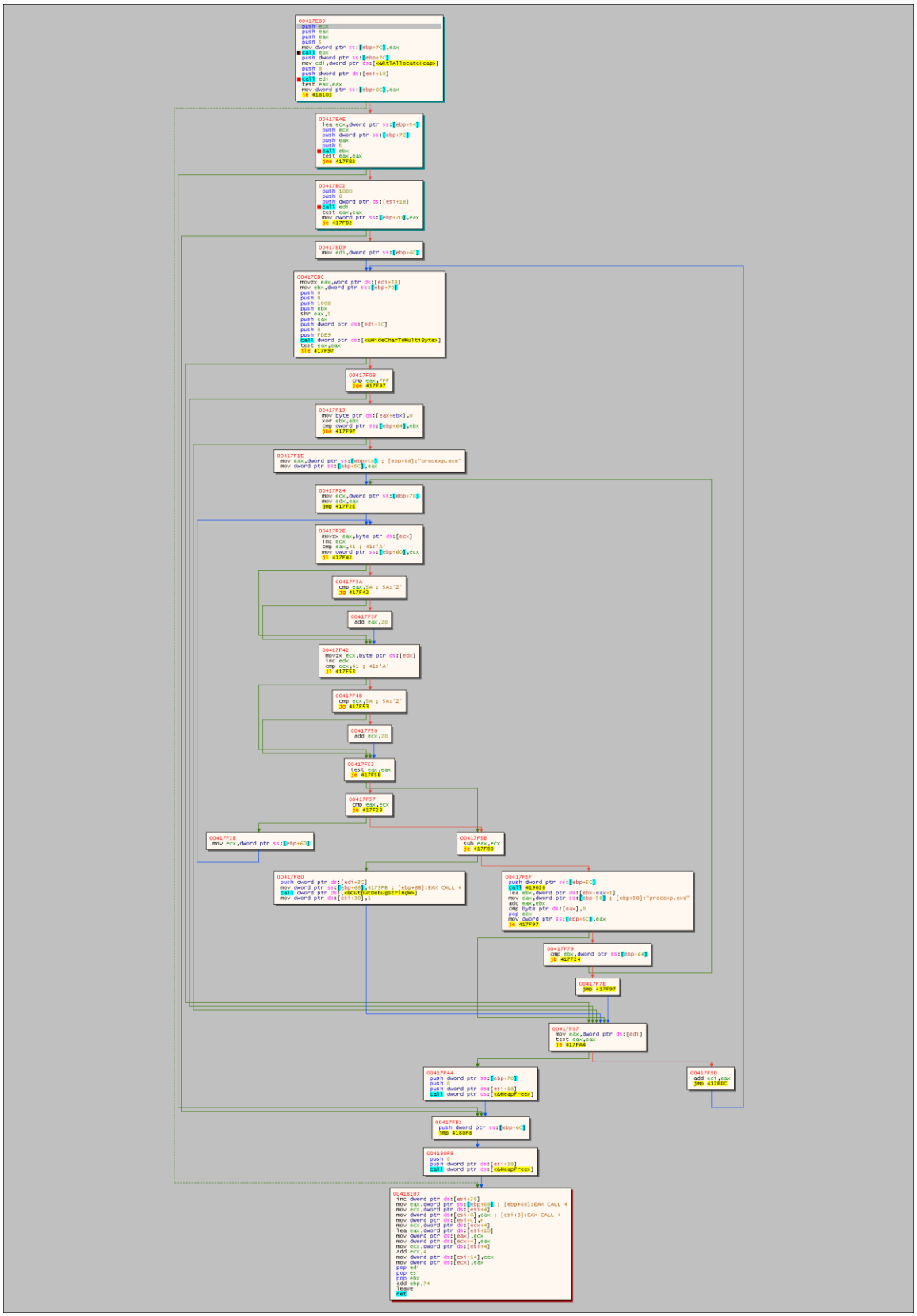


Upon initial analysis, it was observed that the malicious entity appeared to be packed, prompting the decision to unpack it. After successful unpacking, the malware generates a new thread to execute the deciphered code.

The identified malware employs certain anti-analysis techniques, including:

- Process BlackList
- API Hashing
- Time-Based Side-Channel Attack Detection
- Heaven's Gate

Process BlackList

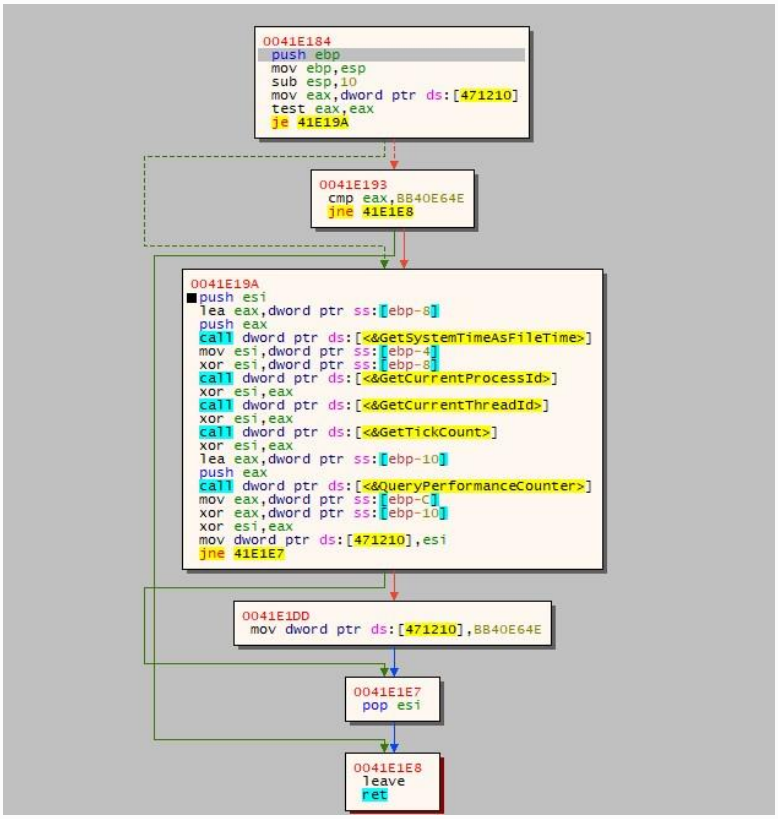


Şekil 2 ProcessBlackList Algorithm

The malware checks the following process names to determine if it is running in the background:

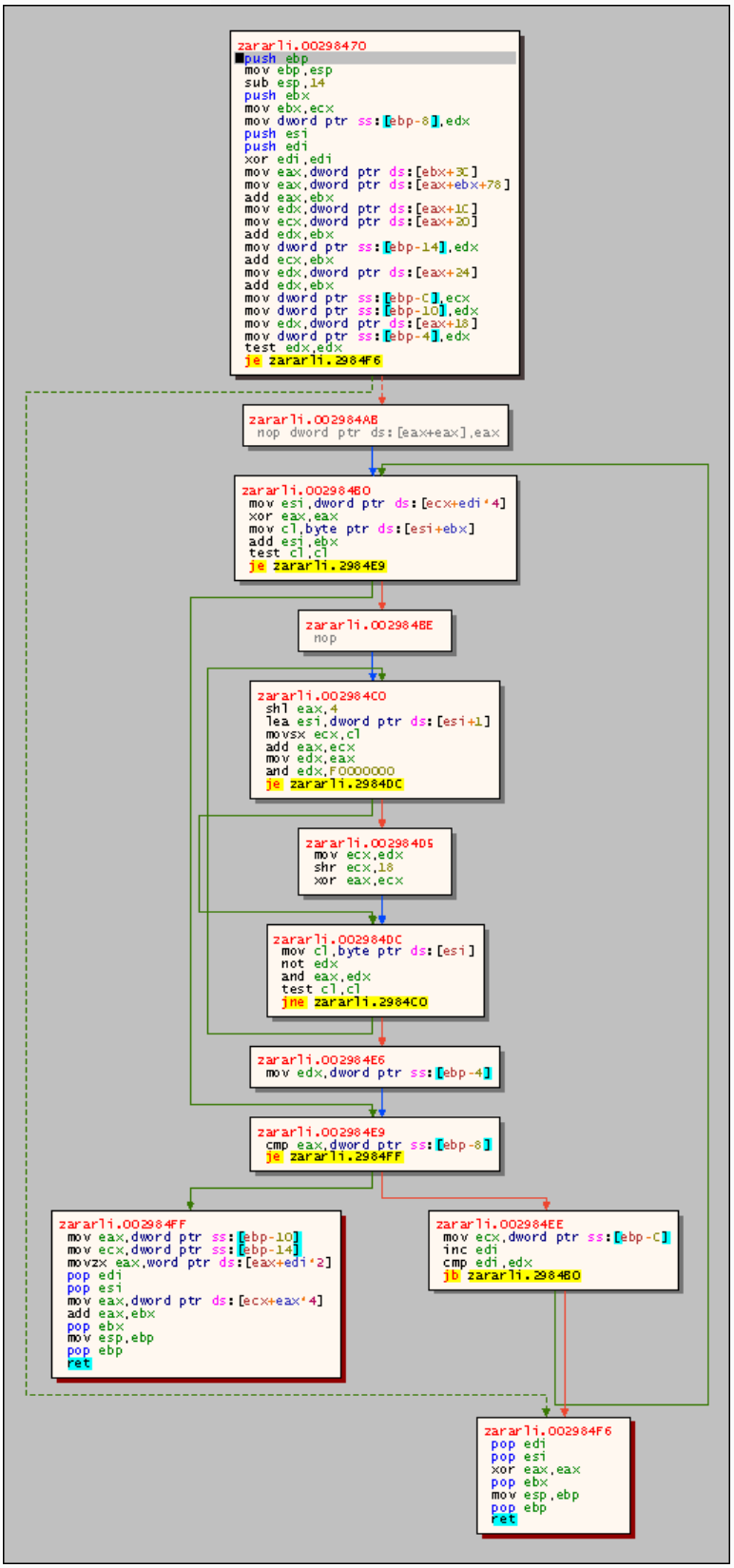
ImmunityDebugger.exe	hookexplorer.exe
WinDump.exe	ilspy.exe
x64dbg.exe	lordpe.exe
x32ddbg.exe	dnspy.exe
OllyDbg.exe	aoutorunsc.exe
ProcessHacker.exe	resourcehacker.exe
idaq64.exe	regmon.exe
autoruns.exe	windanr.exe
dumpcap.exe	procexp.exe
de4dot.exe	Fiddler Everwhere.exe
procexp64.exe	Fiddler.exe
tcpview.exe	ida.exe
tcpview64.exe	ida64.exe
Procmon.exe	portmon.exe
Procmon64.exe	processlasso.exe
vmmap.exe	Wireshark.exe
vmmap64.exe	

Time-Based Side-Channel Attack Detection



Şekil 3 Time-Based Side-Channel Attack Detection Algorithm

API Hashing



Şekil 4 API Hashing Algorithm

Hashing of APIs

```
function(char* apiname,int key){
        int result=key;
        for(i=0;i<strlen(apiname);i++){

                result=result*result* 0x1000193;
                result=result^apiname[i];
        }
        return result;
}
```

Şekil 5 Hashing of an API

The deciphered list of APIs is as follows:

VirtualProtect	VirtualProtect	GetModuleHandleW
HeapSize	GetSystemInfo	MultiByteToWideChar
GetStringTypeW	OutputDebugStringA	GetCurrentProcess
GetStringTypeA	HeapAlloc	CloseHandle
GetCurrentProcessId	GetProcessHeap	ReadFile
GetSystemTimeAsFileTime	MulDiv	CreateFileW
GetLocaleInfoA	HeapFree	OutputDebugStringW
GetStringTypeA	lstrlenW	WideCharToMultiByte
GetStringTypeW	GetModuleFileNameW	ExitProcess
HeapSize	InterlockedIncrement	CreateEventW
GetModuleHandleW	HeapDestroy	DeleteMenu
MultiByteToWideChar	WaitForSingleObject	SetTimer
GetCurrentProcess	VirtualQuery	CreateAcce
CloseHandle	HeapCreate	leratorTableW
ReadFile	FrameRect	GetSystemMenu
CreateFileW	GetClassInfoW	DrawMenuBar
OutputDebugStringW	CharUpperBuffW	SetMenuItemInfoW
WideCharToMultiByte	IsIconic	GetWindowTextW
ExitProcess	EnableWindow	GetDCEx
CreateEventW	DrawIcon	RegisterClassW
GetMenuItemInfoW	LoadCursorW	LoadBitmapW
SetScrollPos	BeginPaint	DrawFocusRect
FillRect	CreateWindowExW	LoadIconW
CreateMenu	PostMessageW	ShowCaret
GetScrollInfo	EndPaint	CopyImage
KillTimer	ShowWindow	PeekMessageW

DestroyWindow	DestroyIcon	GetMenuStringW
CreateIcon	GetClassInfoExW	DefMDIChildProcW
InsertMenuW	LoadStringW	GetScrollRange
GetClientRect	GetDlgCtrlID	IsDialogMessageW
ReleaseDC	GetDC	GetTextMetricsW
DestroyMenu	GetSystemMetrics	MoveToEx
DefFrameProcW	RegCloseKey	CreateCompatibleBitmap
DispatchMessageW	RegQueryValueExW	GetWindowOrgEx
GetScrollPos	RegOpenKeyExW	SetRectRgn
GetCursor	StretchBlt	RoundRect
IsZoomed	SetBkMode	PolyBezierTo
DestroyCursor	SetAbortProc	CreatePalette
EndMenu	SetTextColor	CreateICW
MsgWaitForMultipleObjectsEx	GetStockObject	RectVisible
CreateSolidBrush	CoUninitialize	DocumentPropertiesW
Polygon	OleInitialize	ClosePrinter
AngleArc	OleUninitialize	OpenPrinterW
Piet	CoCreateInstance	EnumPrintersW
GetEnhMetaFileHeader	CoInitialize	GetModuleHandleA
RestoreDC	IsEqualGUID	GetSta
CreateDCW	CoTaskMemAlloc	rtupInfoA
GetDeviceCaps	GetFileVersionInfoW	GetCommandLineA
GDI32	VerQueryValueW	GetVersionExA
CoTaskMemFree	GetFileVersionInfoSizeW	GetProcAddress
TlsAlloc	GetModuleFileNameA	LeaveCriticalSection
SetLastError	UnhandledExceptionFilter	EnterCriticalSection
GetCurrentThreadId	FreeEnvironmentStringsA	GetACP
GetLastError	GetEnvironmentStrings	GetOEMCP
TlsFree	FreeEnvironmentStringsW	GetCPInfo
TlsSetValue	GetEnvironmentStringsW	LoadLibraryA
TlsGetValue	SetHandleCount	InitializeCriticalSection
TerminateProcess	GetFileType	VirtualAlloc
WriteFile	DeleteCriticalSection	HeapReAlloc
GetStdHandle	VirtualFree	RtlUnwind
InterlockedExchange	LCMapStringW	QueryPerformanceCounter
LCMapStringA	GetTickCount	

The decrypted User-Agent information is as follows:

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36\r\n
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36\r\n
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36\r\n
Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0\r\n
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36\r\n
Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108.0\r\n
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML,like Gecko) Version/16.2 Safari/605.1.15\r\n
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36\r\n
Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/109.0\r\n
Mozilla/5.0 (X11; Linux x86_64; rv:108.0) Gecko/20100101 Firefox/108.0\r\n
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36\r\n
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0)Gecko/20100101 Firefox/109.0\r\n
Mozilla/5.0 (Macintosh; Intel MacOS X 10.15; rv:108.0) Gecko/20100101 Firefox/108.0\r\n
Mozilla/5.0(Windows NT 10.0; rv:109.0) Gecko/20100101 Firefox/109.0\r\n
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,like Gecko)Chrome/108.0.0.0 Safari/537.36 Edg/108.0.1462.76\r\n
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/109.0\r\n
Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0\r\n
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36 dg/109.0.1518.61\r\n
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 OPR/94.0.0.0\r\n
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/16.1 Safari/605.1.15\r\n
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36 Edg/109.0.1518.70\r\n
Mozilla/5.0 (Windows NT 10.0; rv:108.0) Gecko/20100101 Firefox/108.0\r\n
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:108.0) Gecko/20100101 Firefox/108.0\r\n
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36 Edg/109.0.1518.55\r\n
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/16.3 Safari/605.1.15\r\n
Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36\r\n
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36Edg/109.0.1518.78\r\n
Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0\r\n
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36\r\n
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 YaBrowser/22.11.5.715 Yowser/2.5 Safari/537.36\r\n

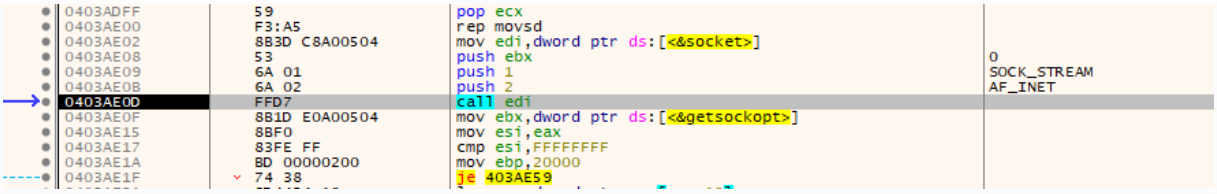
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36\r\n
Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36\r\n
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36\r\n
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 Edg/108.0.1462.54\r\n
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.6.1 Safari/605.1.15\r\n
Mozilla/5.0 (Windows NT 10.0; rv:102.0) Gecko/20100101 Firefox/102.0\r\n
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36 OPR/93.0.0.0\r\n
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36\r\n
Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) Gecko/20100101 Firefox/1

Additionally, the malware has been found to monitor certain registry entries and files. These include:

Registry	File Name
31aPGJK9Lv	2yVLZrH
io74s	TY8kzx7
kyOs	kjdhM
kCnbOl	LndDr
c0g8G8rUSNM	b8svY
9nQmIB	Q7vc
LNU2W	Z3VTlyR
YpykW	QY9YVW
Ktcgpm	lK8pUeed2QM
MuIbGLO4	5XS2X1w6e
W1PGm	hTXjSJFrPa
GXhINinN	HHLSOv8m3
qd7cvBMA	xcYUv0IK
XF4J3D3	1R0Ny
tC342j	qFK88
jPY5BaNS	BvoNid
Uizj	MOgIUGJ1u
tDcVDhL8S	BcHXV3Cxa
msad0fkKex	aKt8EUt2pch
Q2dw5Ro4cO	cVVx8
WcZrCaG	ADYrwg5
AUU9sR3blYO	XiOujq9ex8B
4I05TZ	1v5L
HWS1JyNedYh	
bLV9jACrGH	

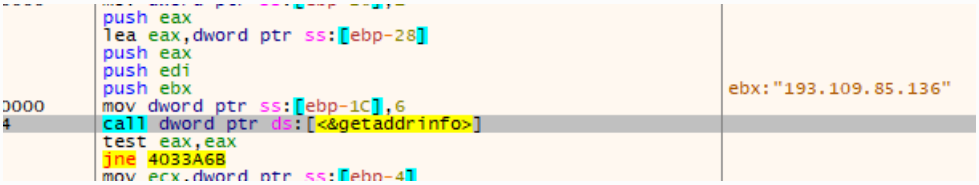
Network

It has been identified that the malware establishes communication with an unconventional Command and Control (C2) server.



Şekil 6 SOCKET Create

The malware has been observed to create sockets.



Şekil 7 getaddrinfo

193[.]109[.]85[.]139 It has been determined that the IP address is specified as the socket address.

Upon execution, the Rhadamanthys malware initiates communication with the IP address 193[.]109[.]85[.]139, progressing to the next stage.

In the subsequent stages, the stolen information encompasses:

- System details
- Screenshots
- Browser credentials and cookies
- Cryptocurrency wallets
- FTP credentials
- Email clients
- Two-Factor Authentication applications (RoboForm, WinAuth, Authy Desktop)
- Password managers (KeePass)
- VPN information
- Messenger data (Psi+, Pidgin, TOX)
- Discord
- Telegram
- Steam
- TeamViewer, SecureCRT, and also NoteFly
- Notezilla
- Simple Sticky Notes

Some of the collected cryptocurrency wallet extensions include:

Auvitas Wallet	BitApp	Crocobit
Exodus	Finnie	GuildWallet
ICONex	Jaxx	Keplr
Liquality	MTV Wallet	Math
Metamask	Mobox	Nifty
Oxygen	Phantom	Rabet Wallet
Ronin Wallet	Slope Wallet	Sollet
Starcoin	Swash	Terra Station
Tron	XinPay	Yoroi Wallet
ZilPay Wallet	binance	coin98

Targeted browsers include:

360ChromeX	360 Secure Browser	7Star
AVAST Browser	AVG Browser	Atom
Avant Browser	BlackHawk	Blisk
Brave	CCleaner Browser	CentBrowser
Chedot	CocCoc	Coowon
Cyberfox	Dragon	Element Browser
Epic Privacy Browser	Falkon	Firefox
Firefox Nightly	GhostBrowser	Google Chrome
Hummingbird	IceDragon	Iridium
K-Meleont	Kinza	Kometa Browser
SLBrowser	MapleStudio	Maxthon
Naver Whale	Opera	Opera GX
Opera Neon	QQBrowser	SRWare Iron
SeaMonkey	Sleipnir5	Slimjet
Superbird	Twinkstar	UCBrowser
Xvast	citrio	Pale Moon
Torch Web Browser	UR Browser	Vivaldi

FTP

Cyberduck	FTP Navigator
FTPRush	FlashFXP
Smartftp	TotalCommander
Winscp	Ws_ftp
Coreftp	

YARA RULE

```
rule Rhadamanthys {
    meta:
        date = "2023-08-23"
        description = "Detects Rhadamanthys malware"
        author = "Bilal BAKARTEPE"
        hash1 = "3798E6DAE3DF606799111B63BF54AAD9"
        verdict = "dangerous"
        platform = "windows"

    strings:
        $hashedAPI_1={F1 F0 AD 0A} //LoadLibraryA hash
        $hashedAPI_2={64 18 2D 07} //VirtualProtect hash
        $hashedAPI_3={B5 3D 2C 06} //WideCharToMultiByte hash
        $hashedAPI_4={17 8B FA 0D} //GetModuleFileNameW hash
        $hashedAPI_5={27 89 D6 0A} //CreateFile hash
        $hashedAPI_6={D5 69 67 00} //GetFileSize hash
        $hashedAPI_7={A5 CB 78 0B} //ReadFile hash

        $algorithm_1={8B 34 B9 33 C0 8A 0C 1E 03 F3 84 C9 74 2B 66 90 C1 E0 04 8D 76 01 0F BE C9 03 C1 8B D0 81 E2 00 00 00 F0 74 07 8B CA C1 E9 18 33 C1 8A 0E F7 D2 23 C2 84 C9 75 DA 8B 55 FC 3B 45 F8 74 11 8B 4D F4 47 3B FA 72 BA} // API hashing Algorithm
        $algorithm_2={8A 04 0E 8D 49 01 88 41 FF 83 EA 01 75 F2} //Copy itself a memory block
        $algorithm_3={8A 02 8D 49 01 88 41 FF 8D 52 01 83 EE 01 75 F0} // Copy itself a memory block
        $algorithm_4={8B 4C 24 04 8A 01 84 C0 74 16 8B 54 24 08 69 D2 93 01 00 01 0F B6 C0 33 D0 41 89 54 24 08 EB E4 8B 44 24 08} //hashing APIs algorithm
        $algorithm_5={7E 29 8B 45 10 8B 4D 08 2B C8 8A 14 01 32 55 14 88 10 8B 55 14 66 D1 6D 14 83 E2 01 85 D2 74 07 81 75 14 00 B4 00 00 40 4E 75 DF 5E } //Decrypt algorithm for User-Agent informations

    condition:

            (all of ($hashedAPI_*)and(any of ($algorithm_*)) or (any of ($algorithm_*))

}
```

SIGMA RULE

```
title: Detects Outbound Socket Communication by Rhadamarthys
description: Detects processes communicating over a specific port using by Rhadamarthys.
status: experimental
author: Bilal BAKARTEPE
logsource:
    category: network
    type: firewall
detection:
    selection_1:
        field: destination.port
        values:
            - 7825
    selection_2:
        field: destination.ip
        values:
            - 193.109.85.136
    condition: all of selection_*
    fields:
        - process.name
        - process.path
        - source.ip
        - destination.port
    falsepositives:
        - unknown
level: high
```

Mittre Att&ck

Discovery	Defense Evasion	Credential Access	Initial Access	Execution	Collection	Command and Control
T1082 System Information Discovery	T1622 Debugger Evasion	T1003 OS Credential Dumping	T1199 Trusted Relationship	T1106 Native API	T1005 Data from Local System	T1071 Application Layer Protocol: Web Protocols
T1033 System Owner/User Discovery	T1140 Deobfuscate/Decode Files or Information	T1110.001 Brute Force: Password Guessing	T1566 Phishing	T1053 Scheduled Task/Job	T1560 Archive Collected Data	T1571 Non-Standard Port
T1217 Browser Information Discovery	T1600 Weaken Encryption	T1155 Credentials from Password Stores				
T1057 Process Discovery						
T1012 Query Registry						
T1614 System Location Discovery						
T1124 System Time Discovery						
T1497 Virtualization/Sandbox Evasion						

ECHO

CYBER THREAT INTELLIGENCE