Vidar Stealer

TEKNİK ANALİZ RAPORU

ZAYOTEM

ZARARLI YAZILIM ÖNLEME VE TERSİNE MÜHENDİSLİK

İçindekiler

Ön Bakış

Vidar ailesinden olan zararlı karşımıza EXE uzantılı olarak çıkmaktadır. Bu zararlı yazılım bulaşmış olduğu bilgisayarlarda kişisel bilgi, kripto cüzdanı verilerini ve tarayıcılardaki cookie bilgilerine ulaşmaktadır. İlk olarak 2018'in sonlarında keşfedildi ve o zamandan beri düzenli olarak güncellendi ve geliştirildi. Zararlı e-posta yolu ile gönderilen kötü amaçlı bağlantılar veya ekler, indirilmiş sahte dosyalar veya uygulamalar, kötü amaçlı reklamlar ve sosyal mühendislik saldırılarıyla yayılabilir.

Sample.exe Analizi

Adı	sample.exe
MD5	701477F861BDE9756D5FC3ACE9D2F019
SHA256	2E0F06DF176B574CD8F629F8E0D32FDEDC72DD20
Dosya Türü	PE32/EXE

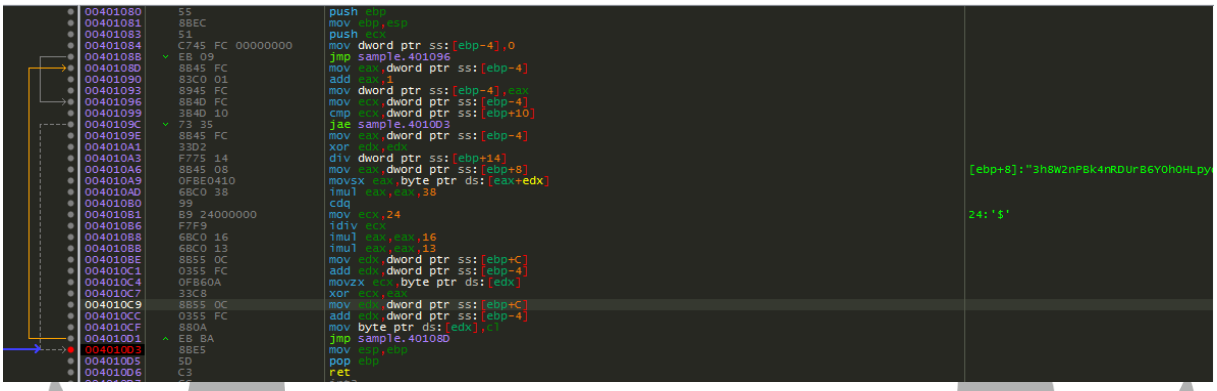
Zararlının MD5, SHA-1 ve SHA-256 bilgileri tabloda yer almaktadır. Orijinal ismi 48aa1381548b2590a3ae1d740852fdefdf51c46666ee2d86e50aeae66afbda60.exe fakat analiz ederken kolaylık olması açısından sample.exe olarak adlandırılmıştır.

Dinamik Analiz

```
mov     dword ptr [ebp+var_820+4], edx
push    42h ; 'B'
push    77Eh
lea     eax, [ebp+var_7B0]
push    eax
push    offset a3h8w2npbk4nrdu ; "3h8W2nPBk4nRDUrB6Y0h0HLpyqaFdsG77R2qmHs"...
call    sub_401080
```

Şekil 1. Zararlının kullandığı string

Zararlı incelendiğinde **3h8W2nOBk4nRDUrB6Y0HLpyqaFdsG77R2qmHs** isimli string dikkat çekmektedir. Çağrıldığı fonksiyon incelendiğinde, memory'de atlama işlemleri yapan zararsız bir Shellcode olduğu görülmektedir. Bu stringin kafa karıştırmak amacıyla koyulduğu anlaşılmaktadır.

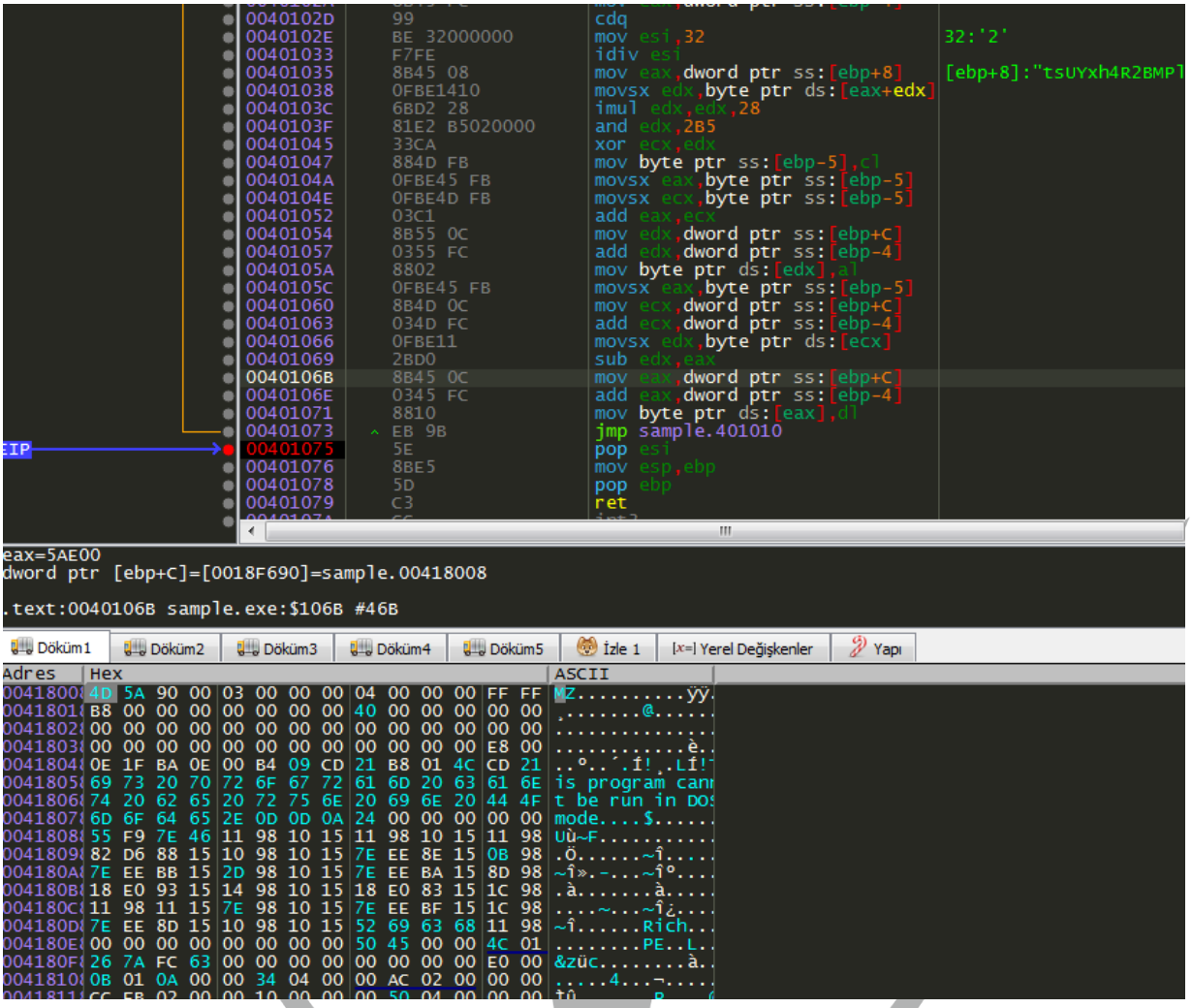


Şekil 2. Memory'de yapılan atlama işlemleri

```
push    42h ; 'B'
push    5AE00h
push    offset unk_418008
push    offset aTsuyxh4r2bmpl6 ; "tsUYxh4R2BMPl6IVK7msKOJi8MeYnj3B4ogS6KP"...
call    sub_401000
```

Şekil 3. Zararlının kullandığı string

Zararlı incelendiğinde, dikkat çeken **tsUYxh4R2BMPl6IVK7msKOJi8MeYnj3B4ogS6KP** isimli diğer string görülmektedir. Bu string **sub_401000** isimli fonksiyona atanmaktadır.



Şekil 4. Enjekte edilen PE dosyası

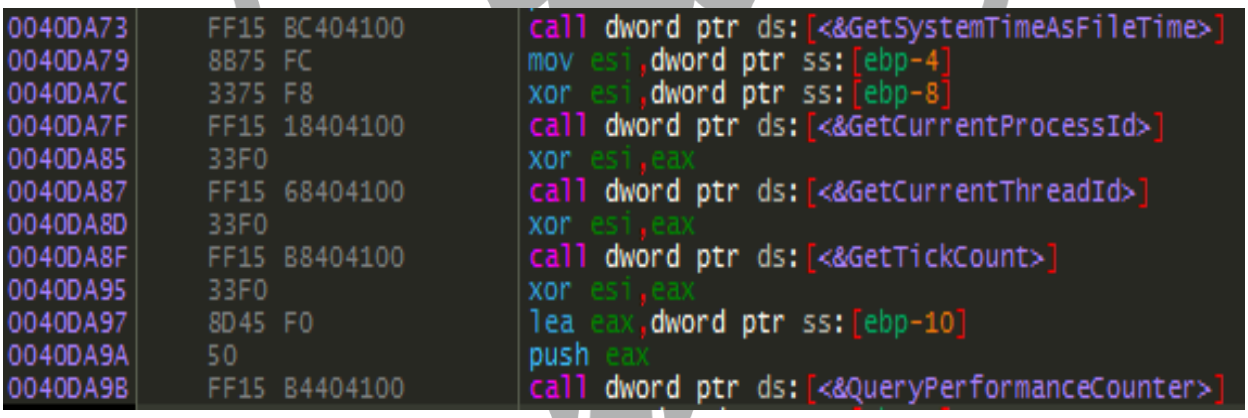
sub_401000 fonksiyonuna girilip incelendiğinde, pop esi talimatıyla sample.exe'nin içine bir **PE** dosyası enjekte edildiği anlaşılmaktadır. Döküm, hafıza haritasında takip edilip daha sonra SAMPLE_00418000.EXE olarak kaydedildi. Kaydedilen .exe dosyası statik ve dinamik olarak incelenmiştir.

SAMPLE_00418000.EXE Analizi

Adı	sample_00418000.exe
MD5	35EBCE61CD83460135893269B991E740
SHA256	DA39750642B84880BD1E882E3EF53C7E72C42366
Dosya Türü	PE32/EXE

Droplanan .exe dosyasının MD5 ve SHA-256 bilgileri tabloda yer almaktadır. Analiz ederken kolaylık olması açısından sample_00418000.exe olarak adlandırılmıştır.

Dinamik Analiz

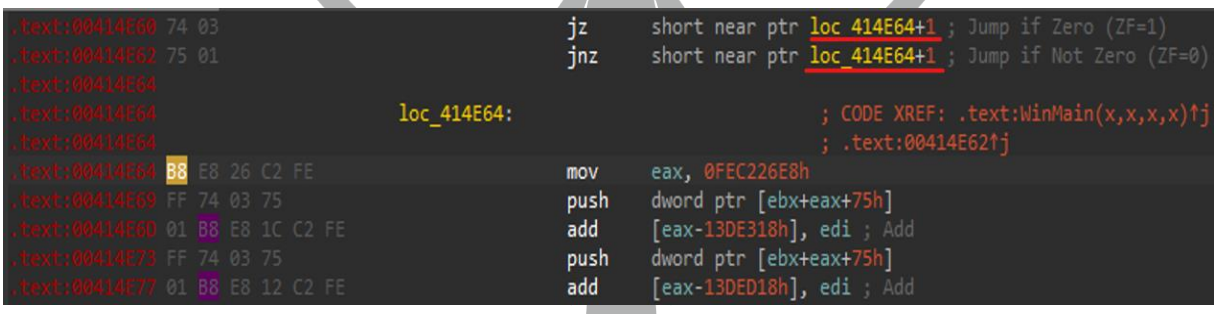


Şekil 5. Zararlının kullandığı API'ler

Zararlının ilk aşamada sistem hakkında genel bilgiler topladığı görülmektedir. Kullandığı API'ler aşağıdaki tabloda verilmiştir.

GetSystemTimeAsFileTime	Geçerli sistem tarihini ve saatini alır. Bilgiler Koordineli Evrensel Zaman (UTC) formatındadır.

GetCurrentProccessId	Çağıran sürecin süreç tanımlayıcısını alır
GetCurrentThreadId	Çağıran iş parçacığının iş parçacığı tanımlayıcısını alır
GetTickCount	Sistemin başlatılmasından bu yana geçen milisaniye sayısını (49,7 güne kadar) alır.
QueryPerformanceCounter	Zaman aralığı ölçümleri için kullanılabilecek yüksek çözünürlüklü (<1us) zaman damgası olan performans sayacının geçerli değerini alır.



Şekil 6. Impossible Disassembly Tekniği

Droplanan .exe dosyası Disassembler programında incelendiğinde, Impossible Disassembly tekniği kullanıldığı anlaşılmaktadır. Bu teknik tersine mühendislik işlemini zorlaştırmayı amaçlayan bir Anti-Disassembly tekniğidir. Şekilde görüldüğü gibi koşullu atlama yönergesine veri baytı eklenmiştir. Bu veri baytları, disassembly algoritmasının atlama yönergesinden sonra gerçek yönergeyi disassembly etmesini engellemek için tasarlanmıştır. Şekilde görülen B8 opcode'u atlandığı için hiç kullanılmamaktadır.

Disassambler bu kısımları anlamlandıramadığı için yanlış yorumlama yapmaktadır. Bu teknik genellikle kötü amaçlı yazılımlarda ve diğer güvenli olmayan yazılımlarda kullanılmaktadır.

```
.text:00414E60 74 03                    jz      short near ptr loc_414E64+1 ; Jump if Zero (ZF=1)
.text:00414E62 75 01                    jnz     short near ptr loc_414E64+1 ; Jump if Not Zero (ZF=0)
.text:00414E64
.text:00414E64                  loc_414E64:                                 ; CODE XREF: .text:WinMain(x,x,x,x)↑j
.text:00414E64                                                              ; .text:00414E62↑j
.text:00414E64 B8 E8 26 C2 FE           mov     eax, 0FEC226E8h
.text:00414E69 FF 74 03 75              push    dword ptr [ebx+eax+75h]
.text:00414E6D 01 B8 E8 1C C2 FE        add     [eax-13DE318h], edi ; Add
.text:00414E73 FF 74 03 75              push    dword ptr [ebx+eax+75h]
.text:00414E77 01 B8 E8 12 C2 FE        add     [eax-13DED18h], edi ; Add
```

Şekil 7. Impossible Disassembly tekniği çözümlenmeden önce

Şekilde görülen B8 opcode'unu 90 ile değiştirerek yani NOP ile doldurarak, impossible disassembly tekniğinin çözümlemesini yapıyoruz.

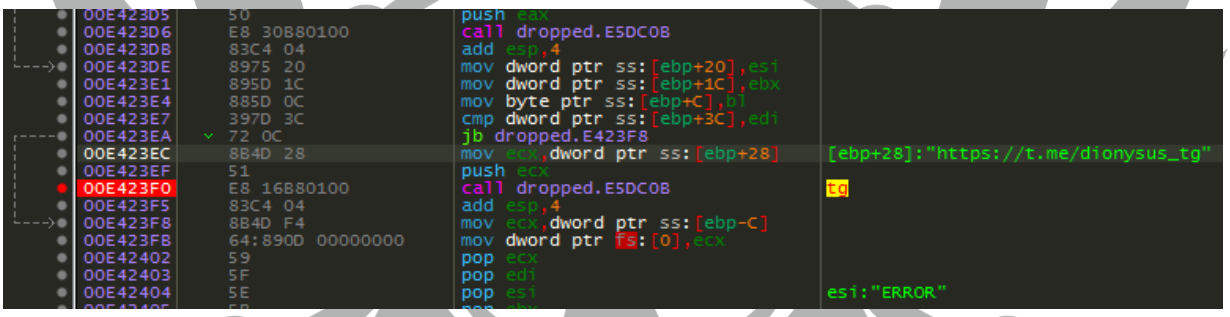
```
.text:00414E60
.text:00414E60                  ; int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nShowCmd)
.text:00414E60                  _WinMain@16:                            ; CODE XREF: ___tmainCRTStartup+115↓p
.text:00414E60 74 03                    jz      short loc_414E65 ; Jump if Zero (ZF=1)
.text:00414E62 75 01                    jnz     short loc_414E65 ; Jump if Not Zero (ZF=0)
.text:00414E64 90                       nop                     ; No Operation
.text:00414E65
.text:00414E65                  loc_414E65:                             ; CODE XREF: .text:WinMain(x,x,x,x)↑j
.text:00414E65                                                          ; .text:00414E62↑j
.text:00414E65 E8 26 C2 FE FF           call    sub_401090      ; Call Procedure
.text:00414E6A 74 03                    jz      short near ptr unk_414E6F ; Jump if Zero (ZF=1)
.text:00414E6C 75 01                    jnz     short near ptr unk_414E6F ; Jump if Not Zero (ZF=0)
.text:00414E6E 90                       nop                     ; No Operation
```

Şekil 8. Impossible Disassembly tekniği çözümlendikten sonra

Böylelikle zararlı Disassembler'a takılmadan analiz edilebilir hale gelmektedir.

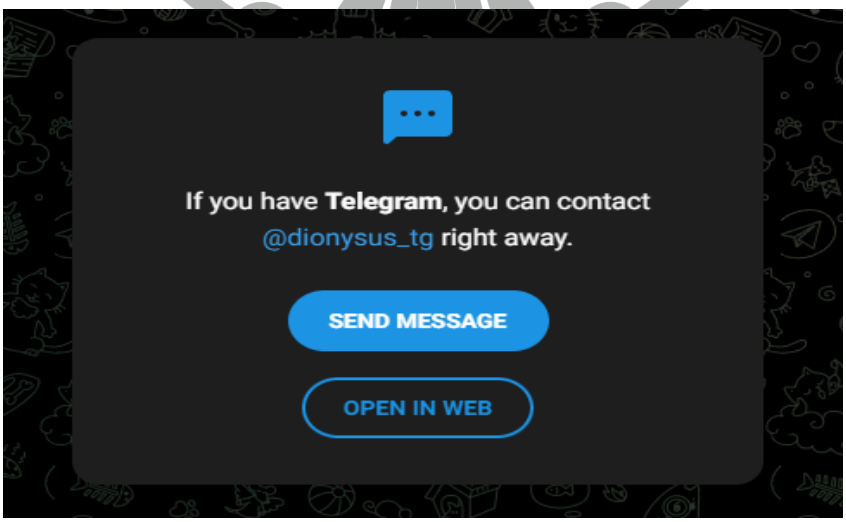
Impossible Disassembly tekniği kullanan zararlı yazılımlardan korunmak için:

- Güvenilir kaynaklardan yazılım indirin.
- Yazılımı güncel tutun.
- Bir antivirüs programı kullanın.
- Bilgisayarınızın yazılımını tersine mühendislik için tasarlanmış özel araçlarla analiz edin.



Şekil 9. Telegram botu URL adresi

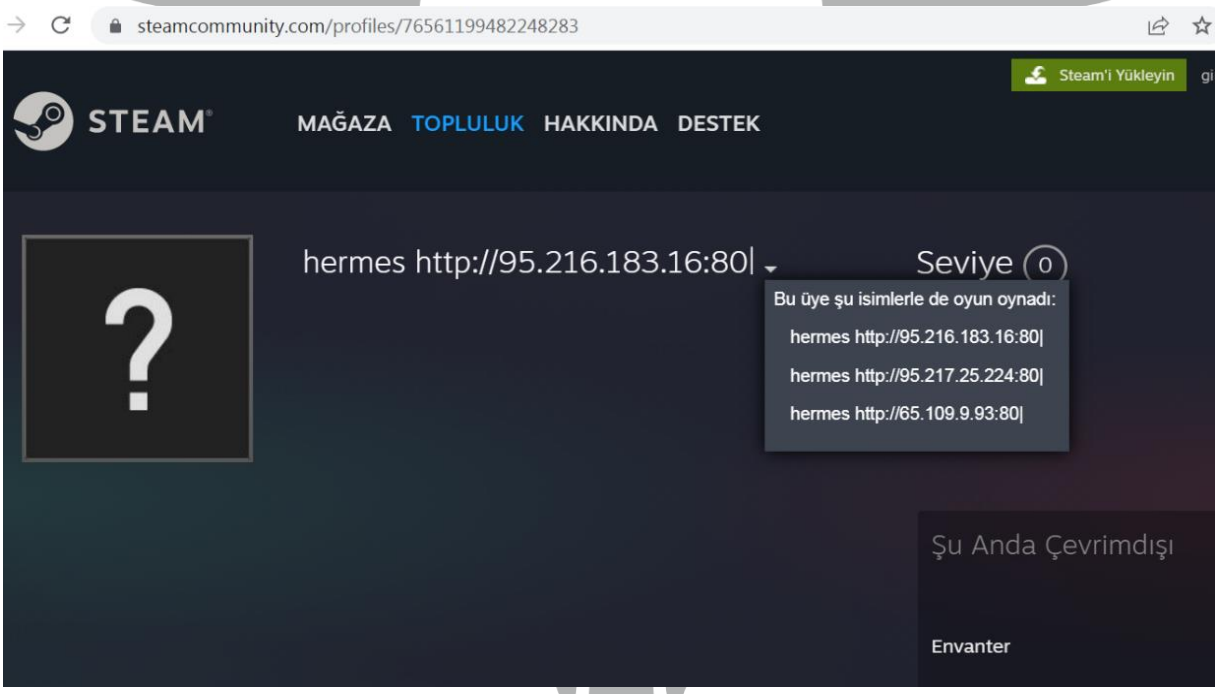
Drop edilen .exe dosyası içerisinde C&C server için kullanılan telegram botunun URL adresi bulunmaktadır.



Şekil 10. Telegram botu

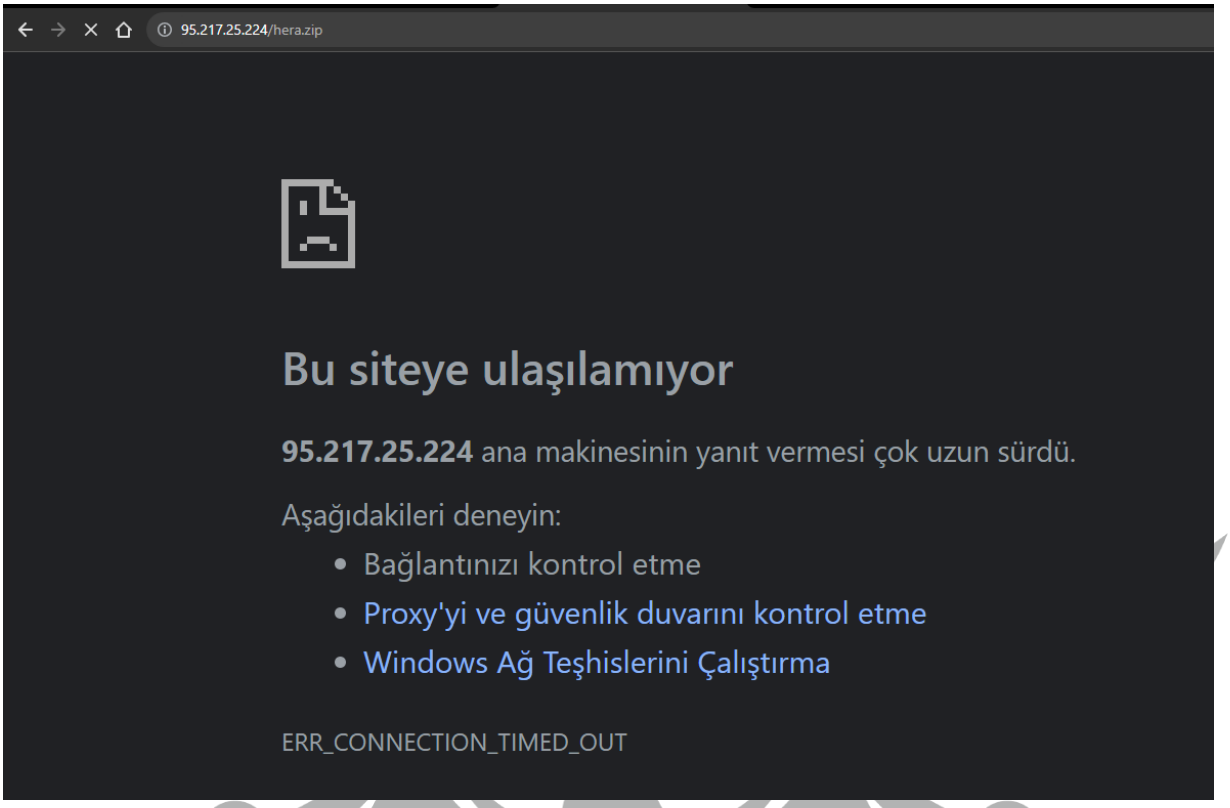
Şekil 11. steam URL adresi

Drop edilen .exe dosyası içerisinde steamcommunity URL adresi bulunmaktadır.



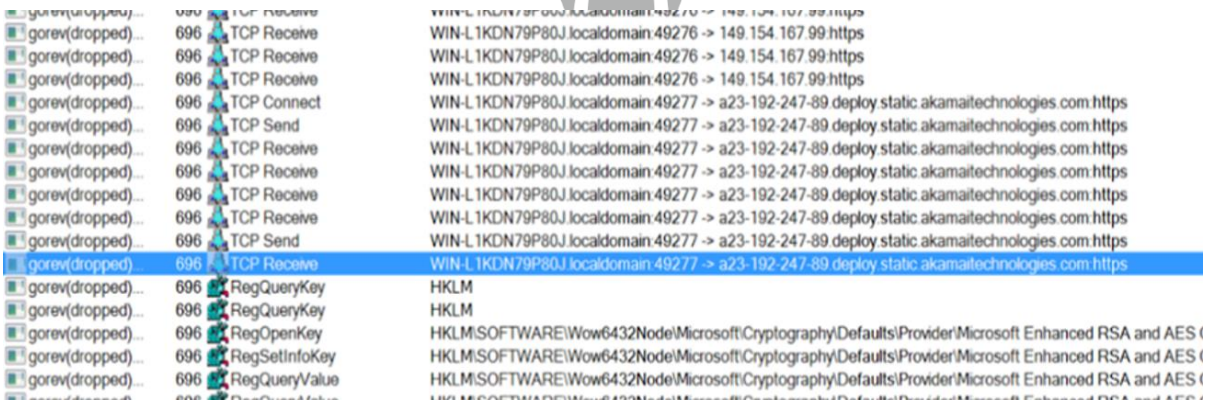
Şekil 12. steam ekranı

Zararlı, steamcommunity URL adresini kullanarak **hermes http[:]//95[.]216[.]183[.]16[:]80, hermes http[:]//95[.]217[.]25[.]224[:]80, hermes http[:]//65[.]109[.]9[.]93[:]80** adreslerine HTTP GET isteği atmaktadır. Zararlı bu istek ile sunucudan **hera.zip** isimli bir dosya çekmeye çalışmaktadır.



Şekil 13. hera.zip'in çekileceği web server

hera.zip isimli dosyanın çekileceği sunucunun kapalı durumda olduğu görülmektedir.



Şekil 14. Yerel makinadan atılan istek

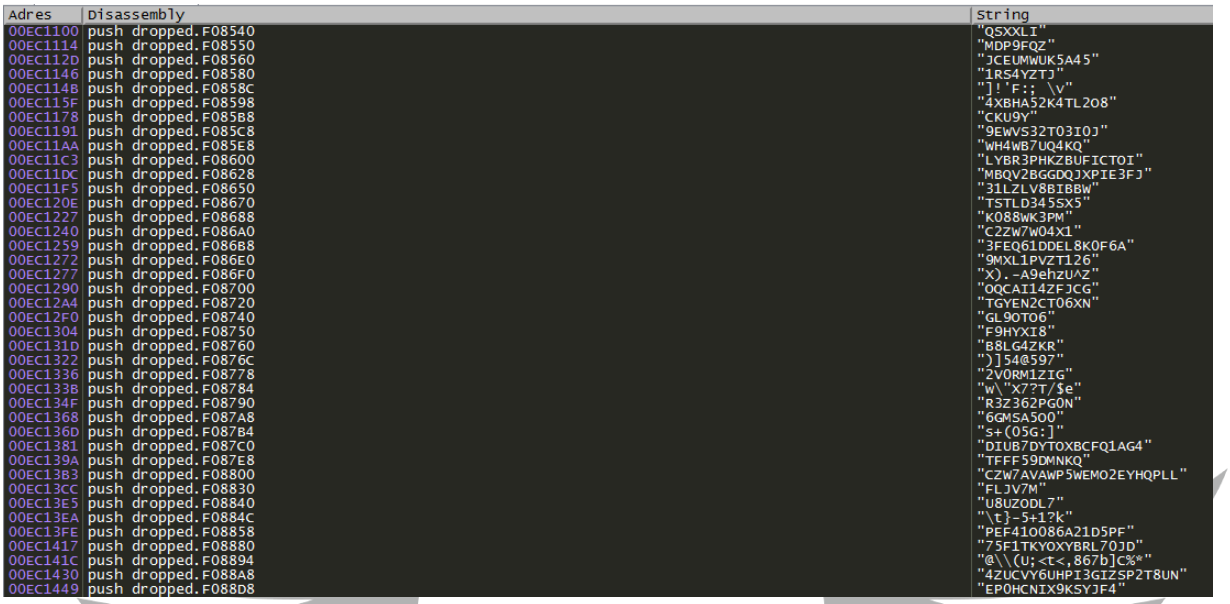
829	646.855253	23.192.247.89	192.168.213.128	TLSv1.2	85 Encrypted Alert
830	646.855305	192.168.213.128	23.192.247.89	TCP	54 49181 → 443 [RST, ACK] Seq=674 Ack=39916 Win=0 Len=0
831	646.856503	23.192.247.89	192.168.213.128	TCP	60 443 → 49185 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
832	646.856553	192.168.213.128	23.192.247.89	TCP	54 49185 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
833	646.856921	192.168.213.128	23.192.247.89	TLSv1.2	275 Client Hello
834	646.857097	23.192.247.89	192.168.213.128	TCP	60 443 → 49185 [ACK] Seq=1 Ack=222 Win=64240 Len=0
835	646.916788	23.192.247.89	192.168.213.128	TLSv1.2	1514 Server Hello
836	646.916788	23.192.247.89	192.168.213.128	TCP	1498 443 → 49185 [PSH, ACK] Seq=1461 Ack=222 Win=64240 Len=1444 [TCP segm…
837	646.916858	192.168.213.128	23.192.247.89	TCP	54 49185 → 443 [ACK] Seq=222 Ack=2905 Win=64240 Len=0
838	646.917070	23.192.247.89	192.168.213.128	TLSv1.2	995 Certificate, Certificate Status, Server Key Exchange, Server Hello D…
839	646.917092	192.168.213.128	23.192.247.89	TCP	54 49185 → 443 [ACK] Seq=222 Ack=3846 Win=63299 Len=0
840	646.927153	192.168.213.128	23.192.247.89	TLSv1.2	180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
841	646.927426	23.192.247.89	192.168.213.128	TCP	60 443 → 49185 [ACK] Seq=3846 Ack=348 Win=64240 Len=0
842	646.982192	23.192.247.89	192.168.213.128	TLSv1.2	105 Change Cipher Spec, Encrypted Handshake Message
843	646.982246	192.168.213.128	23.192.247.89	TCP	54 49185 → 443 [ACK] Seq=348 Ack=3897 Win=63248 Len=0
844	646.987164	192.168.213.128	23.192.247.89	TLSv1.2	379 Application Data
845	646.987544	23.192.247.89	192.168.213.128	TCP	60 443 → 49185 [ACK] Seq=3897 Ack=673 Win=64240 Len=0

Şekil 15. Wireshark ekran görüntüsü

Aynı zamanda zararlının yerel makineden **23[.]192[.]247[.]89** ip adresine de istek attığı görülmektedir.

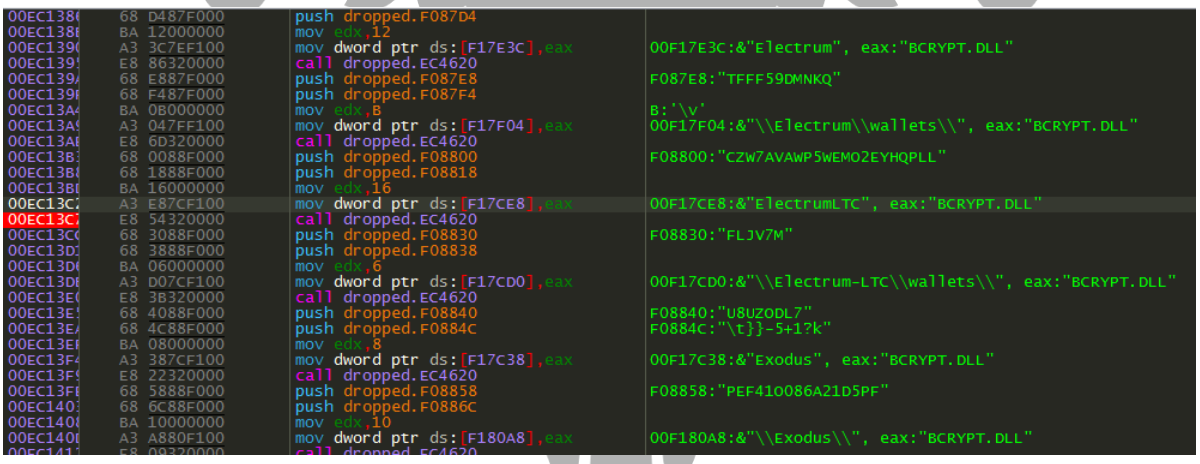
Şekil 16. Geçersiz IP adresi

23[.]192[.]247[.]89 ip adresine bakıldığında geçersiz olduğu görülmektedir.



Adres	Disassembly	string
00EC1100	push dropped.F08540	"QSXXLI"
00EC1114	push dropped.F08550	"MDP9FQZ"
00EC112D	push dropped.F08560	"JCEUMWUK5A45"
00EC1146	push dropped.F08580	"1RS4YZTJ"
00EC114B	push dropped.F0858C	"]!'F:; \v"
00EC115F	push dropped.F08598	"4XBHA52K4TL2O8"
00EC1178	push dropped.F085B8	"CKU9Y"
00EC1191	push dropped.F085C8	"9EWVS32TO3I0J"
00EC11AA	push dropped.F085E8	"WH4WB7UQ4KQ"
00EC11C3	push dropped.F08600	"LYBR3PHKZBUFICTOI"
00EC11DC	push dropped.F08628	"MBQV2BGGDQJXPIE3FJ"
00EC11F5	push dropped.F08650	"31LZLV8BIBBW"
00EC120E	push dropped.F08670	"TSTLD345SX5"
00EC1227	push dropped.F08688	"KO88WK3PM"
00EC1240	push dropped.F086A0	"C2ZW7WO4X1"
00EC1259	push dropped.F086B8	"3FEQ61DDEL8K0F6A"
00EC1272	push dropped.F086E0	"QMXL1PVZT126"
00EC1277	push dropped.F086F0	"X).-A9ehzU^Z"
00EC1290	push dropped.F08700	"OQCAI14ZFJCG"
00EC12A4	push dropped.F08720	"TGYEN2CTO6XN"
00EC12F0	push dropped.F08740	"GL9OTO6"
00EC1304	push dropped.F08750	"F9HYXI8"
00EC131D	push dropped.F08760	"B8LG4ZKR"
00EC1322	push dropped.F0876C	")]54@597"
00EC1336	push dropped.F08778	"2V0RM1ZIG"
00EC133B	push dropped.F08784	"W\"X7?T/$e"
00EC134F	push dropped.F08790	"R3Z362PG0N"
00EC1368	push dropped.F087A8	"6GMSA5OO"
00EC136D	push dropped.F087B4	"s+(O5G:]"
00EC1381	push dropped.F087C0	"DIUB7DYTOXBCFQ1AG4"
00EC139A	push dropped.F087E8	"TFFF59DMNKQ"
00EC13B3	push dropped.F08800	"CZW7AVAWP5WEMO2EYHQPLL"
00EC13CC	push dropped.F08830	"FLJV7M"
00EC13E5	push dropped.F08840	"U8UZODL7"
00EC13EA	push dropped.F0884C	"\t}-5+1?k"
00EC13FE	push dropped.F08858	"PEF41OO86A21D5PF"
00EC1417	push dropped.F08880	"75F1TKYOXYBRL7OJD"
00EC141C	push dropped.F08894	"@\\(U;<t<,867b]C%*"
00EC1430	push dropped.F088A8	"4ZUCVY6UHPI3GIZSP2T8UN"
00EC1449	push dropped.F088D8	"EPOHCNIX9KSYJF4"

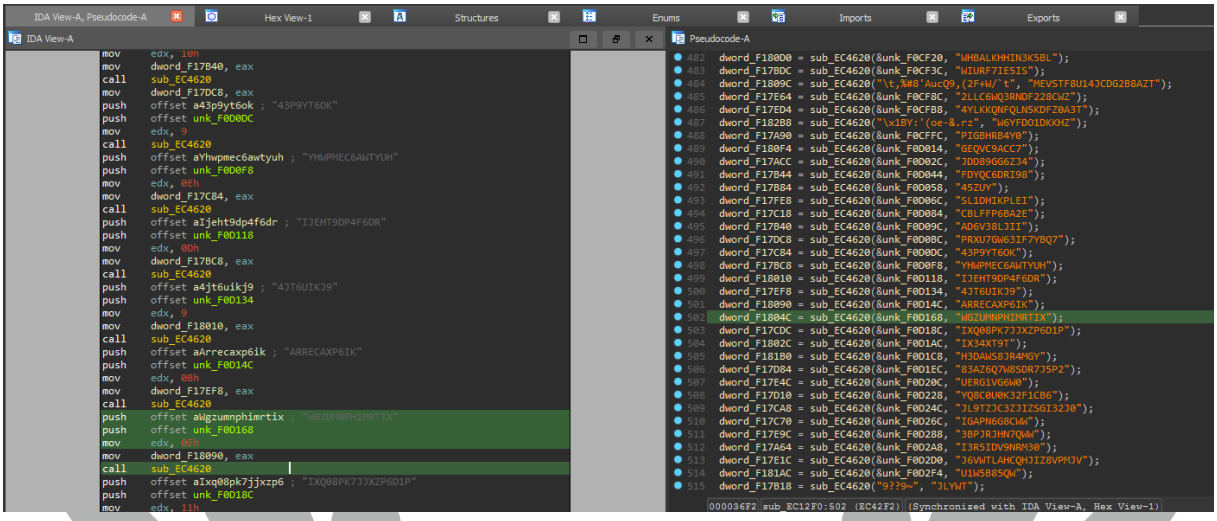
Şekil 17. modül içindeki string referansları



```
00EC138(    68 D487F000     push dropped.F087D4
00EC138[    BA 12000000     mov edx,12
00EC139(    A3 3C7EF100     mov dword ptr ds:[F17E3C],eax     00F17E3C:&"Electrum", eax:"BCRYPT.DLL"
00EC139!    E8 86320000     call dropped.EC4620
00EC139A    68 E887F000     push dropped.F087E8               F087E8:"TFFF59DMNKQ"
00EC139[    68 F487F000     push dropped.F087F4
00EC13A4    BA 0B000000     mov edx,B                         B:'\v'
00EC13A9    A3 047FF100     mov dword ptr ds:[F17F04],eax     00F17F04:&"\\Electrum\\wallets\\", eax:"BCRYPT.DLL"
00EC13AE    E8 6D320000     call dropped.EC4620
00EC13B3    68 0088F000     push dropped.F08800               F08800:"CZW7AVAWP5WEMO2EYHQPLL"
00EC13B8    68 1888F000     push dropped.F08818
00EC13BD    BA 16000000     mov edx,16
00EC13C2    A3 E87CF100     mov dword ptr ds:[F17CE8],eax     00F17CE8:&"ElectrumLTC", eax:"BCRYPT.DLL"
00EC13C7    E8 54320000     call dropped.EC4620
00EC13CC    68 3088F000     push dropped.F08830               F08830:"FLJV7M"
00EC13D1    68 3888F000     push dropped.F08838
00EC13D6    BA 06000000     mov edx,6
00EC13DB    A3 D07CF100     mov dword ptr ds:[F17CD0],eax     00F17CD0:&"\\Electrum-LTC\\wallets\\", eax:"BCRYPT.DLL"
00EC13E0    E8 3B320000     call dropped.EC4620
00EC13E5    68 4088F000     push dropped.F08840               F08840:"U8UZODL7"
00EC13EA    68 4C88F000     push dropped.F0884C               F0884C:"\t}-5+1?k"
00EC13EF    BA 08000000     mov edx,8
00EC13F4    A3 387CF100     mov dword ptr ds:[F17C38],eax     00F17C38:&"Exodus", eax:"BCRYPT.DLL"
00EC13F9    E8 22320000     call dropped.EC4620
00EC13FE    68 5888F000     push dropped.F08858               F08858:"PEF41OO86A21D5PF"
00EC1403    68 6C88F000     push dropped.F0886C
00EC1408    BA 10000000     mov edx,10
00EC140D    A3 A880F100     mov dword ptr ds:[F180A8],eax     00F180A8:&"\\Exodus\\", eax:"BCRYPT.DLL"
00EC1412    E8 09320000     call dropped.EC4620
```

Şekil 18. assembly görünümü

Zararlıda stringlerin ve cüzdan adreslerinin şifrelenmesi için ortak bir fonksiyon bulunmaktadır.



Şekil 19. ida ve pseudo code görünümü

Bunlardan birçoğu cüzdan işlemlerinde kullanılan stringler iken, şifrelemeyi çözen fonksiyon (EC4620) zararlının birçok yerinde kullanılmıştır.

```
_BYTE *__fastcall sub_EC4620(int a1, unsigned int a2, int a3, const char *a4)
{
  int v4; // ecx
  char *v5; // eax
  _WORD *v6; // edi
  __int16 v7; // ax
  _BYTE *v8; // ebx
  unsigned int v9; // eax
  unsigned int v10; // ecx
  unsigned int v11; // edx
  _BYTE *v12; // esi
  unsigned int v14; // [esp+4h] [ebp-210h] BYREF
  char v15; // [esp+8h] [ebp-20Ch] BYREF

  v14 = a2;
  v4 = 520;
  v5 = &v15;
  do
  {
    *v5++ = 0;
    --v4;
  }
  while ( v4 );
  v6 = (_WORD *)&v14 + 1;
  do
  {
    v7 = v6[1];
    ++v6;
  }
  while ( v7 );
  qmemcpy(
    v6,
    L"Nor again is there anyone who loves or pursues or desires to obtain pain of itself, because it
    0xCEu);
```

Şekil 20. decryption fonksiyonu

Fonksiyonun genel yapısı resimdeki gibi olmakla beraber, memory'ye de bir mesaj bırakmaktadır.

Zararlı yazılımın hedeflediği tarayıcı eklentileri:

Eklenti Kimliği	Eklenti Adı
gojhcdgcpbpfigcaejpfhfegekdgiblk	Opera Wallet
pnndplcbkakcplkjnolgbkdgjikjednm	Tronium
egjidjbpglichdcondbcbdnbeeppgdph	Trust Wallet
aholpfdialjgjfhomihkjbmgjidlcdno	Exodus Web3 Wallet
jnlgamecbpmbajjfhmmmlhejkemejdma	Braavos
kkpllkodjeloidieedojogacfhpaihoh	Enkrypt
mcohilncbfahbmgdjkbpemcciiolgcge	OKX Web3 Wallet
epapihdplajcdnnkdeiahlgigofloibg	Sender
gjagmgiddbbciopjhllkdnddhcglnemk	Hashpack
kmhcihpebfmpgmihbkipmjlmmioameka	Eternl
bgpipimickeadkjlklgciifhnalhdjhe	GeroWallet
phkbamefinggmakgklpkljjmgibohnba	Pontem Wallet
ejjladinnckdgjemekebdpeokbikhfci	Petra Wallet
efbglgofoippbgcjepnhiblaibcnclgk	Martian Wallet
cjmkndjhnagcfbpiemnkdpomccnjblmj	Finnie
aijcbedoijmgnlmjeegjaglmepbmpkpi	Leap Terra

YARA Kuralı

```
import "hash"

rule sample{

meta:

        author="Team3"

        description="Vidar Stealer"

        first date="16.09.2023"

        report date="16.10.2023"

        file name="sample.exe"

strings:

        $dnm_a="3h8W2nPBk4nRDUrB6Y0h0HLpyqaFdsG77R2qmHs6N8ItqBhW4SbYsSYEyutCXGUpq"

        $dnm_b="http://ocsp.entrust.net00"

        $dnm_c="tsUYxh4R2BMPl6IVK7msKOJi8MeYnj3B4ogS6KPyHbGwtYiJEr9efHvkNOaoLGqUp"

        $dnm_d="http://ocsp.digicert.com0X"

        $dnm_e="http://pki.eset.com/csp0"

Condition:

        Hash.md5(0,filesize)=="701477F861BDE9756D5FC3ACE9D2F019" or all of them

}
```

MITRE ATTACK TABLE

Execution	Persistence	Defense Evasion	Credential Access	C&C
Windows Management Instrumentation	Account Manipulation	Deobfuscate/Decode Files or Information	OS Credential Dumping	Encrypted Channel
Native API		Obfuscated Files or Information	Input Capture	Ingress Tool Transfer
		Virtualization/Sandbox Evasion	Credentials in Registry	Non-Application Layer Protocol
		Process Injection		Application Layer Protocol

Çözüm Önerileri

1. Sistemlerde güncel, güvenilir bir anti-virüs yazılımı kullanılmalıdır,

2.Ağ paketlerinin filtrelenmesi ve takibi yapılmalıdır,

3.Tıklanılan bağlantıların doğru ve güvenilir olduğundan emin olunmalıdır,

4.Soğuk cüzdan gibi daha güvenilir kripto para saklama yöntemleri tercih edilmelidir,

5. Kripto hesaplarınızda çift faktörlü doğrulama kullanılmalıdır,

6.Şüphenilen bir durumda ağın izlenmesi ve duruma göre müdahale edilmesi gerekmektedir.

HAZIRLAYAN

Elif ÇAĞLAR

https://www.linkedin.com/in/elif-%C3%A7a%C4%9Flar-27902b214/

Ömer Faruk SÖNMEZ

https://www.linkedin.com/in/omertheroot

Melike TAŞDELEN

https://www.linkedin.com/in/melike-taşdelen-90345926a/