

Vidar Stealer

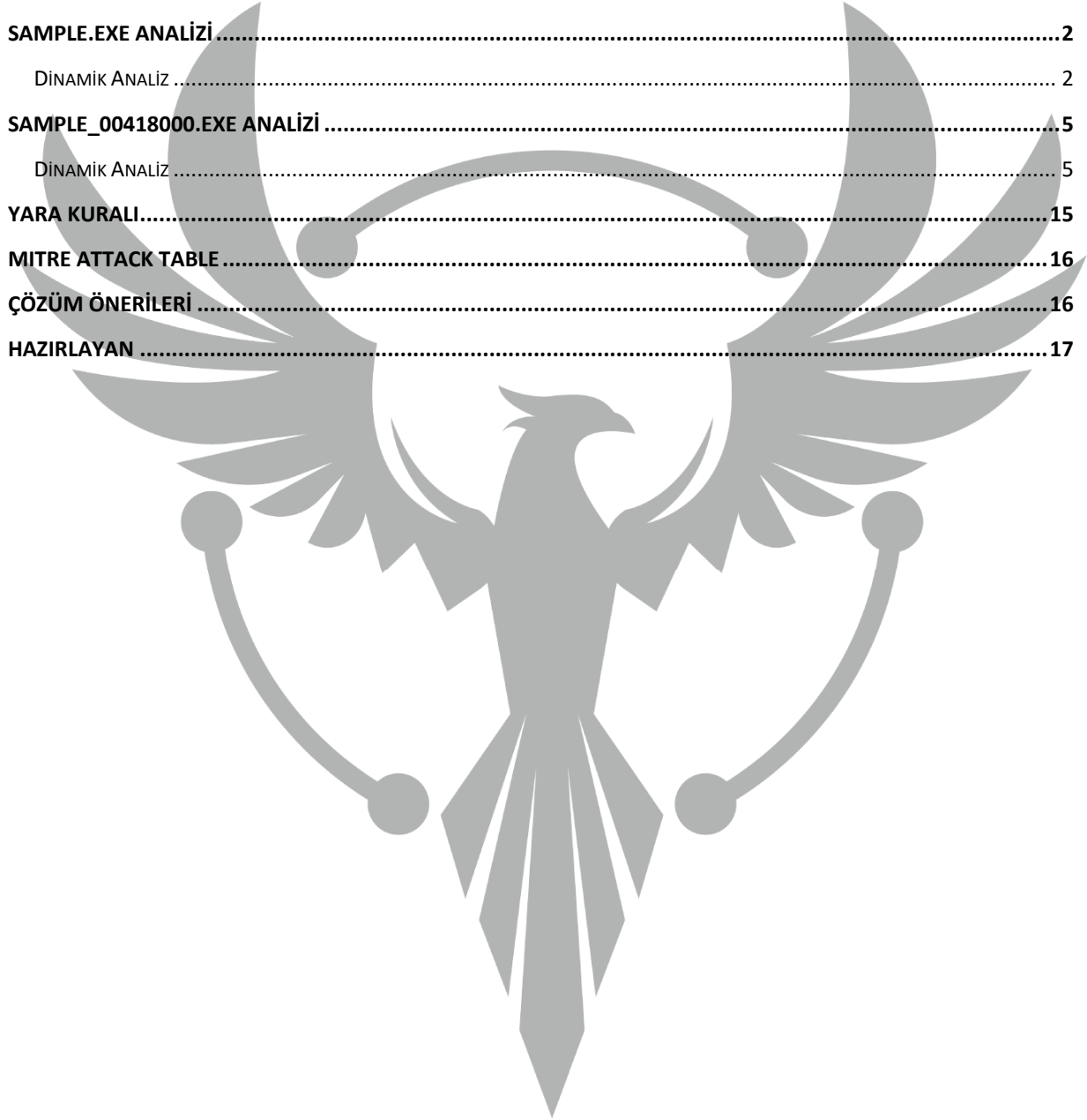
TEKNİK ANALİZ RAPORU

ZAYOTEM

ZARARLI YAZILIM ÖNLEME VE TERSİNE MÜHENDİSLİK

İçindekiler

İÇİNDEKİLER	i
ÖN BAKIŞ	1
SAMPLE.EXE ANALİZİ	2
DİNAMİK ANALİZ	2
SAMPLE_00418000.EXE ANALİZİ	5
DİNAMİK ANALİZ	5
YARA KURALI	15
MITRE ATTACK TABLE	16
ÇÖZÜM ÖNERİLERİ	16
HAZIRLAYAN	17



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.

```

00401080 55      push    ebp
00401081 8BEC   mov     ebp,esp
00401083 51     push    esi
00401084 C745 FC 00000000 mov     dword ptr ss:[ebp-4],0
00401088 EB 09  jmp     sample.401096
00401089 8B45 FC mov     ecx,dword ptr ss:[ebp-4]
00401090 8340 01 add     ecx,1
00401093 8945 FC mov     dword ptr ss:[ebp-4],eax
00401096 8B4D FC mov     ecx,dword ptr ss:[ebp-4]
00401099 3B40 10 cmp     ecx,dword ptr ss:[ebp+10]
0040109C 73 35  jae     sample.4010D3
0040109E 8B45 FC mov     ecx,dword ptr ss:[ebp-4]
004010A1 33D2   xor     ecx,ecx
004010A3 F775 14 div     dword ptr ss:[ebp+14]
004010A6 8B45 08 mov     ecx,dword ptr ss:[ebp+8]
004010A9 0FB80410 movsx   ecx,byte ptr ds:[eax+edx]
004010AD 6600 38 imul   ecx,ecx,38
004010B0 99     cdq
004010B1 B9 24000000 mov     ecx,24
004010B6 F7F9   idiv   ecx
004010B8 66C0 16 imul   eax,ecx,16
004010BB 66C0 13 imul   ecx,ecx,13
004010BE 8B55 0C mov     esi,dword ptr ss:[ebp+C]
004010C1 0355 FC add     esi,dword ptr ss:[ebp-4]
004010C4 0FB60A movzx   edi,byte ptr ds:[eax]
004010C7 33C8   xor     ecx,ecx
004010C9 8B55 0C mov     esi,dword ptr ss:[ebp+C]
004010CC 0355 FC add     esi,dword ptr ss:[ebp-4]
004010CF 8B0A   mov     byte ptr ds:[edx],al
004010D0 E9 BA  jmp     sample.401080
004010D3 BBE5   mov     esi,ebp
004010D5 5D     pop     esi
004010D6 C3     ret

```

Şekil 2. Memory'de yapılan atlama işlemleri

```

push    42h ; 'B'
push    5AE00h
push    offset unk_418008
push    offset aTsuyxh4r2bmp16 ; "tsUYxh4R2BMP16IVK7msKOJi8MeYnj3B4ogS6KP"...
call    sub_401000

```

Şekil 3. Zararlının kullandığı string

Zararlı incelendiğinde, dikkat çeken **tsUYxh4R2BMP16IVK7msKOJi8MeYnj3B4ogS6KP** isimli diğer string görülmektedir. Bu string **sub_401000** isimli fonksiyona atanmaktadır.

```

0040102D 99 cdq
0040102E BE 32000000 mov esi,32 32:'2'
00401033 F7FE idiv esi
00401035 8B45 08 mov eax,dword ptr ss:[ebp+8] [ebp+8]:"tsuyxh4R2BMP1
00401038 0FBE1410 movsx edx,byte ptr ds:[eax+edx]
0040103C 6BD2 28 imul edx,edx,28
0040103F 81E2 B5020000 and edx,2B5
00401045 33CA xor ecx,edx
00401047 884D FB mov byte ptr ss:[ebp-5],cl
0040104A 0FBE45 FB movsx eax,byte ptr ss:[ebp-5]
0040104E 0FBE4D FB movsx ecx,byte ptr ss:[ebp-5]
00401052 03C1 add eax,ecx
00401054 8B55 0C mov edx,dword ptr ss:[ebp+C]
00401057 0355 FC add edx,dword ptr ss:[ebp-4]
0040105A 8802 mov byte ptr ds:[edx],al
0040105C 0FBE45 FB movsx eax,byte ptr ss:[ebp-5]
00401060 8B4D 0C mov ecx,dword ptr ss:[ebp+C]
00401063 034D FC add ecx,dword ptr ss:[ebp-4]
00401066 0FBE11 movsx edx,byte ptr ds:[ecx]
00401069 2BD0 sub edx,eax
0040106B 8B45 0C mov eax,dword ptr ss:[ebp+C]
0040106E 0345 FC add eax,dword ptr ss:[ebp-4]
00401071 8810 mov byte ptr ds:[eax],dl
00401073 ^ EB 9B jmp sample.401010
00401075 5E pop esi
00401076 8BE5 mov esp,ebp
00401078 5D pop ebp
00401079 C3 ret

```

eax=5AE00
dword ptr [ebp+C]=[0018F690]=sample.00418008
.text:0040106B sample.exe:\$106B #46B

Adres	Hex	ASCII
00418000	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF	MZ.....yy
00418014	B8 00 00 00 00 00 00 00 40 00 00 00 00 00@.....
00418024	00 00 00 00 00 00 00 00 00 00 00 00 00 00
00418034	00 00 00 00 00 00 00 00 00 00 00 00 E8 00ë.....
00418044	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21	...!i!Li!
00418054	69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E	is program can
00418064	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F	t be run in DOS
00418074	6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00	mode...\$....
00418084	55 F9 7E 46 11 98 10 15 11 98 10 15 11 98	Uü~F.....
00418094	82 D6 88 15 10 98 10 15 7E EE 8E 15 0B 98	.Ö.....~i...
004180A4	7E EE BB 15 2D 98 10 15 7E EE BA 15 8D 98	~i».....~i°...
004180B4	18 E0 93 15 14 98 10 15 18 E0 83 15 1C 98	.à.....à.....
004180C4	11 98 11 15 7E 98 10 15 7E EE BF 15 1C 98	.~.....~i°...
004180D4	7E EE 8D 15 10 98 10 15 52 69 63 68 11 98	~i.....Rich...
004180E4	00 00 00 00 00 00 00 00 50 45 00 00 4C 01PE..L...
004180F4	26 7A FC 63 00 00 00 00 00 00 00 00 E0 00	&züc.....ä...
00418104	0B 01 0A 00 00 34 04 00 00 AC 02 00 00 00	+...4...-....
00418114	CC FB 02 00 00 10 00 00 00 50 04 00 00 00	...P...

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

0040DA73	FF15 BC404100	call dword ptr ds: [<&GetSystemTimeAsFileTime>]
0040DA79	8B75 FC	mov esi, dword ptr ss: [ebp-4]
0040DA7C	3375 F8	xor esi, dword ptr ss: [ebp-8]
0040DA7F	FF15 18404100	call dword ptr ds: [<&GetCurrentProcessId>]
0040DA85	33F0	xor esi, eax
0040DA87	FF15 68404100	call dword ptr ds: [<&GetCurrentThreadId>]
0040DA8D	33F0	xor esi, eax
0040DA8F	FF15 B8404100	call dword ptr ds: [<&GetTickCount>]
0040DA95	33F0	xor esi, eax
0040DA97	8D45 F0	lea eax, dword ptr ss: [ebp-10]
0040DA9A	50	push eax
0040DA9B	FF15 B4404100	call dword ptr ds: [<&QueryPerformanceCounter>]

Şekil 5. Zararlıının kullandığı API'ler

Zararlıının 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.
-------------------------	---

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

```

.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 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'ü atlandığı için hiç kullanılmamaktadır.

Disassembler 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'ünü 90 ile değiştirerek yani NOP ile doldurarak, impossible disassembly tekniğinin çözümlenmesini 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.

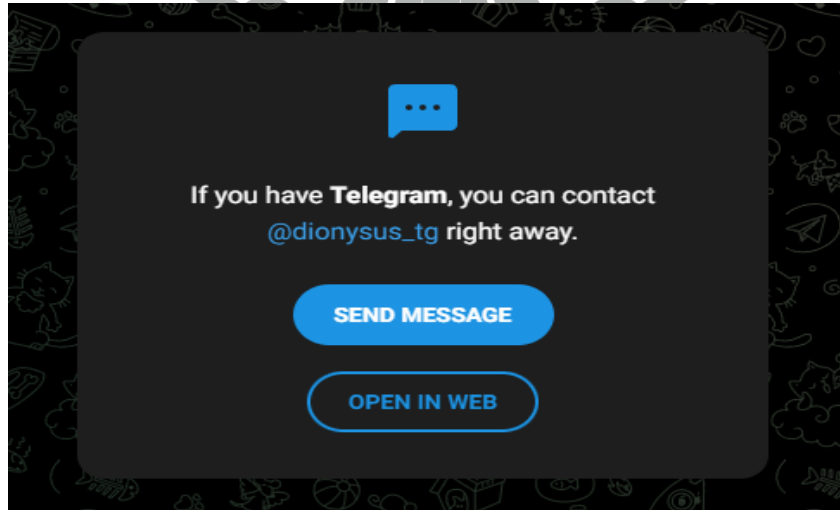
Impossible Disassembly tekniği kullanan zararlı yazılımlardan korunmak için:

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

```
00E423D5 50          push ebx
00E423D6 E8 30B80100 call dropped.E5DC0B
00E423D8 83C4 04     add esp,4
00E423DE 8975 20     mov dword ptr ss:[ebp+20],esi
00E423E1 895D 1C     mov dword ptr ss:[ebp+1C],ebx
00E423E4 885D 0C     mov byte ptr ss:[ebp+C],bl
00E423E7 397D 3C     cmp dword ptr ss:[ebp+3C],edi
00E423EA 72 0C     jb dropped.E423F8
00E423EC 8B4D 28     mov ecx,dword ptr ss:[ebp+28] [ebp+28]:"https://t.me/dionysus_tg"
00E423EF 51         push ecx
00E423F0 E8 16B80100 call dropped.E5DC0B [C]
00E423F5 83C4 04     add esp,4
00E423F8 8B4D F4     mov ecx,dword ptr ss:[ebp-C]
00E423FB 64:890D 00000000 mov dword ptr fs:[0],ecx
00E42402 59         pop ecx
00E42403 5F         pop edi
00E42404 5E         pop esi
esi:"ERROR"
```

Şekil 9. Telegram botu URL adresi

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

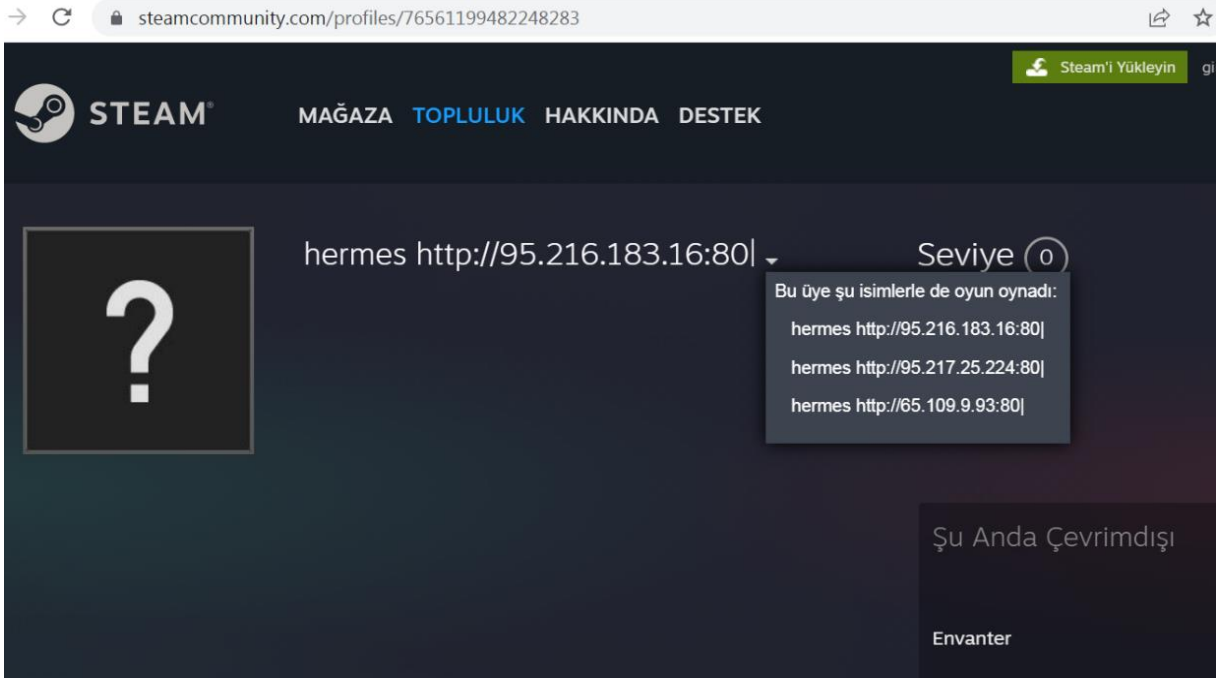


Şekil 10. Telegram botu

```
00E3E7C0 55 push esp
00E3E7C1 8BEC mov ebp,esp
00E3E7C3 51 push ecx
00E3E7C4 33C0 xor eax,ecx
00E3E7C6 6A 35 push 35
00E3E7C8 C746 14 0F000000 mov dword ptr ds:[esi+14],F
00E3E7CF 8946 10 mov dword ptr ds:[esi+10],eax
00E3E7D2 68 60FAE700 push dropped.E7FA60
00E3E7D7 8BCE mov ecx,esi
00E3E7D9 8945 FC mov dword ptr ss:[ebp-4],eax
00E3E7DC 8806 mov byte ptr ds:[esi],al
00E3E7DE E8 0DA9FFFF call dropped.E390F0
00E3E7E3 8BC6 mov eax,esi
00E3E7E5 8BE5 mov esi,ebp
00E3E7E7 5D pop ebp
00E3E7E8 C3 ret
E7FA60:"https://steamcommunity.com/profiles/76561199482248283"
esi:"ERROR"
esi:"ERROR"
esi:"ERROR"
```

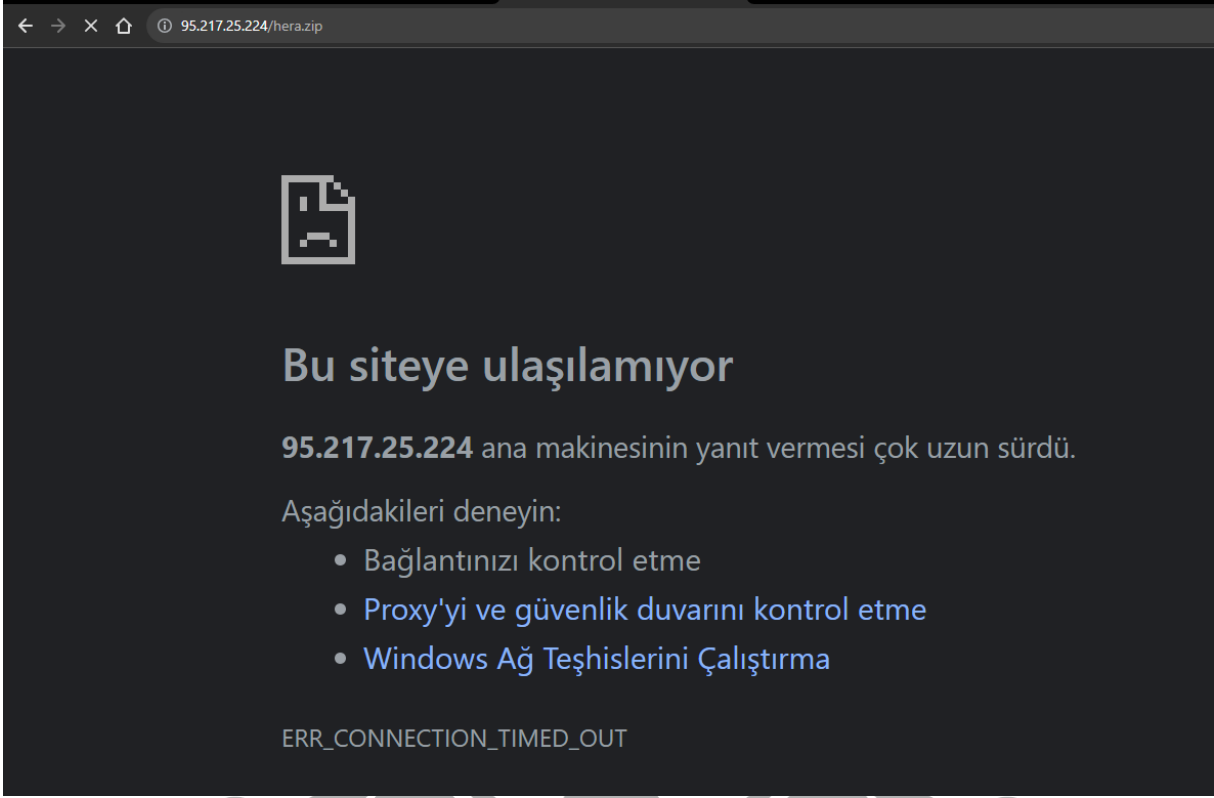
Şekil 11. steam URL adresi

Drop edilen .exe dosyası içerisinde steamcommunity URL adresi bulunmaktadır.



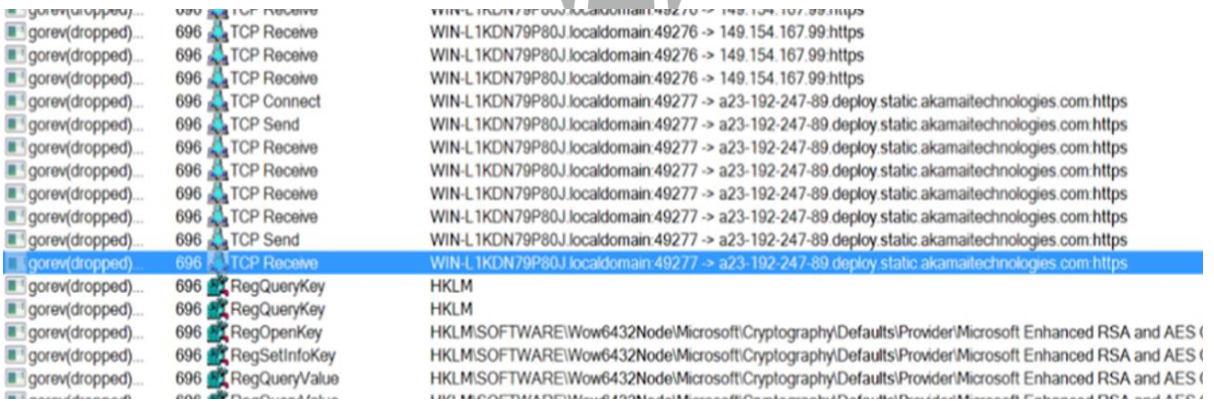
Şekil 12. steam ekranı

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.

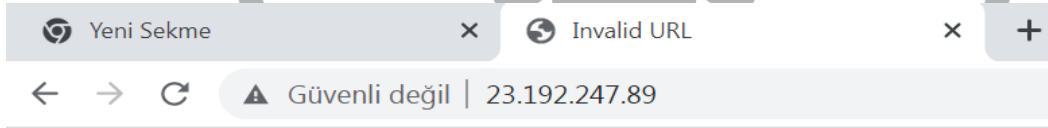


Şekil 14. Yerel makinedan atılan istek

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.



Invalid URL

The requested URL "[no URL]", is invalid.

Reference #9.5d161102.1697050990.e66b895

Şekil 16. Geçersiz IP adresi

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

Adres	Disassembly	String
00EC1100	push dropped.F08540	"Q5XXLI"
00EC1114	push dropped.F08550	"MDP9FQZ"
00EC112D	push dropped.F08560	"JCEUMWUK5A45"
00EC1146	push dropped.F08580	"1R54YZTJ"
00EC114B	push dropped.F0858C	"! F;; \v"
00EC115F	push dropped.F08598	"4XBHA52K4TL2o8"
00EC1178	push dropped.F08588	"CKU9Y"
00EC1191	push dropped.F085C8	"9E1W532T03I0J"
00EC11AA	push dropped.F085E8	"WH4W87U04KQ"
00EC11C3	push dropped.F08600	"LYBR3PHKZBUFICTOI"
00EC11DC	push dropped.F08628	"MBQV2BGGDQJXPIE3FJ"
00EC11F5	push dropped.F08650	"31LZLV88IBBW"
00EC120E	push dropped.F08670	"TSTLD3455X5"
00EC1227	push dropped.F08688	"K088Wk3PM"
00EC1240	push dropped.F086A0	"C2Zw7w04x1"
00EC1259	push dropped.F08688	"3FEQ61DDEL8K0F6A"
00EC1272	push dropped.F086E0	"9MXL1PZT126"
00EC1277	push dropped.F086F0	"X) -A9eRZUAZ"
00EC1290	push dropped.F08700	"OQCA14ZFJCG"
00EC12A4	push dropped.F08720	"TGVEN2CT06XN"
00EC12F0	push dropped.F08740	"GL90T06"
00EC1304	push dropped.F08750	"F9HYX18"
00EC131D	push dropped.F08760	"B8L64ZKR"
00EC1322	push dropped.F0876C	"J]54@597"
00EC1336	push dropped.F08778	"2VORMIZIG"
00EC133B	push dropped.F08784	"W X7?T/\$e"
00EC134F	push dropped.F08790	"R3Z36PG0N"
00EC1368	push dropped.F087A8	"6GMSA500"
00EC136D	push dropped.F087B4	"s+ (05g;]"
00EC1381	push dropped.F087C0	"DIUB7DYTOXBFCF1AG4"
00EC139A	push dropped.F087E8	"TFFF59DMNKQ"
00EC13B3	push dropped.F08800	"CZW7AVAWP5WEMO2EYHQPLL"
00EC13CC	push dropped.F08830	"FL3V7M"
00EC13E5	push dropped.F08840	"U8UZODL7"
00EC13EA	push dropped.F0884C	"\E]-5+1?k"
00EC13FE	push dropped.F08858	"PEF410086A21D5PF"
00EC1417	push dropped.F08880	"75F1TKY0XYBRL70JD"
00EC141C	push dropped.F08894	"@ (U; <<< 867b]C%*"
00EC1430	push dropped.F088A8	"4ZUCVY6UHP13GIZSP2T8UN"
00EC1449	push dropped.F088D8	"EP0HCNIX9K5YJF4"

Şekil 17. modül içindeki string referansları

00EC1381	68 D487F000	push dropped.F087D4	
00EC1381	BA 12000000	mov edi, 12	
00EC1391	A3 3E7EF100	mov dword ptr ds:[F17E3C], eax	00F17E3C:&"Electrum", eax:"BCRYPT.DLL"
00EC1391	E8 8E320000	call dropped.EC4620	
00EC1391	E8 E887F000	push dropped.F087E8	F087E8:"TFFF59DMNKQ"
00EC1391	68 F487F000	push dropped.F087F4	
00EC13A4	BA 0B000000	mov edi, 8	
00EC13A1	A3 047FF100	mov dword ptr ds:[F17F04], eax	B:'\v'
00EC13A1	E8 6D320000	call dropped.EC4620	00F17F04:&"\Electrum\wallets\\", eax:"BCRYPT.DLL"
00EC13B1	68 0088F000	push dropped.F08800	F08800:"CZW7AVAWP5WEMO2EYHQPLL"
00EC13B1	68 1888F000	push dropped.F08818	
00EC13B1	BA 16000000	mov edi, 16	
00EC13C1	A3 E87CF100	mov dword ptr ds:[F17CE8], eax	00F17CE8:&"ElectrumLTC", eax:"BCRYPT.DLL"
00EC13C1	E8 54320000	call dropped.EC4620	
00EC13C1	68 3088F000	push dropped.F08830	F08830:"FL3V7M"
00EC13D1	68 3888F000	push dropped.F08838	
00EC13D1	BA 06000000	mov edi, 6	
00EC13D1	A3 D07CF100	mov dword ptr ds:[F17CD0], eax	00F17CD0:&"\Electrum-LTC\wallets\\", eax:"BCRYPT.DLL"
00EC13E1	E8 3B320000	call dropped.EC4620	
00EC13E1	68 4088F000	push dropped.F08840	F08840:"U8UZODL7"
00EC13E1	68 4C88F000	push dropped.F0884C	F0884C:"\t]-5+1?k"
00EC13E1	BA 08000000	mov edi, 8	
00EC13F1	A3 387CF100	mov dword ptr ds:[F17C38], eax	00F17C38:&"Exodus", eax:"BCRYPT.DLL"
00EC13F1	E8 22320000	call dropped.EC4620	
00EC13F1	68 5888F000	push dropped.F08858	F08858:"PEF410086A21D5PF"
00EC1401	68 6C88F000	push dropped.F0886C	
00EC1401	BA 10000000	mov edi, 10	
00EC1401	A3 A880F100	mov dword ptr ds:[F180A8], eax	00F180A8:&"\Exodus\\", eax:"BCRYPT.DLL"
00EC1411	E8 00320000	call dropped.EC4620	

Şekil 18. assembly görünümü

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

```

IDA View-A, Pseudocode-A | Hex View-1 | Structures | Enums | Imports | Exports
IDA View-A
mov     edx, 10h
mov     dword_17B80, eax
call    sub_EC4620
mov     dword_17DC8, eax
push   offset a43p9y760k ; "43P9YT60K"
push   edx, 9
call    sub_EC4620
push   offset aYhmpmec6awtyuh ; "YHMPMEC6AWTYUH"
push   offset unk_F0D0F8
mov     edx, 0Eh
mov     dword_17C84, eax
call    sub_EC4620
push   offset a1jeht9dp4f6dr ; "1JEHT9DP4F6DR"
push   offset unk_F0D118
mov     edx, 0Dh
mov     dword_17B84, eax
call    sub_EC4620
push   offset a41t6uikj9 ; "41T6UIKJ9"
push   offset unk_F0D134
mov     edx, 9
mov     dword_18010, eax
call    sub_EC4620
push   offset aArrecaxp61k ; "ARRECAP61K"
push   offset unk_F0D14C
mov     edx, 0Bh
mov     dword_17FE8, eax
call    sub_EC4620
push   offset aIgzumpphmtix ; "IGZUMPPHMTIX"
push   offset unk_F0D168
mov     edx, 0Eh
mov     dword_18090, eax
call    sub_EC4620
push   offset a1xq08pk7jixzp6 ; "1XQ08PK7JIXZP6"
push   offset unk_F0D18C
mov     edx, 11h

Pseudocode-A
482 dword_18000 = sub_EC4620(&unk_F0CF20, "HMBALKHHIN3K58L");
483 dword_17BDC = sub_EC4620(&unk_F0CF3C, "N1UR7IE515");
484 dword_1809C = sub_EC4620("Yhmpmec6awtyuh", "43P9YT60K");
485 dword_17FE4 = sub_EC4620(&unk_F0CF8C, "1LCLGQ3RNDP228CZM");
486 dword_17ED4 = sub_EC4620(&unk_F0CF88, "4VLLKQKQFNQNSKDFZ0A3T");
487 dword_182B8 = sub_EC4620("x1Bv:(oe-&.rz", "M6YFD01DKKHZ");
488 dword_17A90 = sub_EC4620(&unk_F0CFFC, "P1GBHRB4Y0");
489 dword_180F4 = sub_EC4620(&unk_F0D014, "6EQVC9C7C");
490 dword_179AC = sub_EC4620(&unk_F0D02C, "DD8S6G6CZ4");
491 dword_17844 = sub_EC4620(&unk_F0D044, "FDVOCDD190");
492 dword_17B84 = sub_EC4620(&unk_F0D058, "45ZUV");
493 dword_17FE8 = sub_EC4620(&unk_F0D06C, "SLIDIKPLEI");
494 dword_17C18 = sub_EC4620(&unk_F0D084, "CBLFFP6A2E");
495 dword_17B40 = sub_EC4620(&unk_F0D09C, "ADDV3BL3I1");
496 dword_17DC8 = sub_EC4620(&unk_F0D09C, "PRKU7GM631F7BQ7");
497 dword_17C84 = sub_EC4620(&unk_F0D0DC, "43P9YT60K");
498 dword_17B84 = sub_EC4620(&unk_F0D0F8, "YHMPMEC6AWTYUH");
499 dword_18010 = sub_EC4620(&unk_F0D118, "1JEHT9DP4F6DR");
500 dword_17FE8 = sub_EC4620(&unk_F0D134, "41T6UIKJ9");
501 dword_18090 = sub_EC4620(&unk_F0D14C, "ARRECAP61K");
502 dword_1804C = sub_EC4620(&unk_F0D168, "IGZUMPPHMTIX");
503 dword_17DC8 = sub_EC4620(&unk_F0D18C, "IXQ08PK7JIXZP6D1P");
504 dword_1802C = sub_EC4620(&unk_F0D1AC, "IX34X19");
505 dword_181B0 = sub_EC4620(&unk_F0D1C8, "H3DAH53R3R9V");
506 dword_17D84 = sub_EC4620(&unk_F0D1EC, "83A26Q7N5DR735P2");
507 dword_17E4C = sub_EC4620(&unk_F0D20C, "UERGI5V6L0");
508 dword_17D10 = sub_EC4620(&unk_F0D228, "YQ8CB0K32F1CB6");
509 dword_17C88 = sub_EC4620(&unk_F0D24C, "1819T3C3Z1Z5G13210");
510 dword_17C70 = sub_EC4620(&unk_F0D26C, "IGH6R6R6L");
511 dword_17E9C = sub_EC4620(&unk_F0D288, "8BP3R3H7QW");
512 dword_17A64 = sub_EC4620(&unk_F0D2A8, "13R51DV9NRH30");
513 dword_17E1C = sub_EC4620(&unk_F0D2D8, "3GWT1LHQC0H1Z8VPH1V");
514 dword_181AC = sub_EC4620(&unk_F0D2F4, "U1N5B850M");
515 dword_18118 = sub_EC4620("979", "JLYM");
000034F2 sub_EC4620 sub_EC4620 (EC42F2) | (Synchronised with IDA View-A, Hex View-1)

```

Şekil 19. ida ve pseudo code görünümü

Bunlardan birçoğu cüzdan işlemlerinde kullanılan stringler iken, şifrelemeyi çözen fonksiyon (EC4620) zararlıının 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
pnndplcbkakcplkjnlgbkdggjikjednm	Tronium
egjidjbpiglichdcondcbdbdnbeppgdph	Trust Wallet
aholpfdialjgjfhomihkjbmjjidlcno	Exodus Web3 Wallet
jnlgamecbpmbajjfhmmmlhejkemejdma	Braavos
kkpllkodjeloidieedojojgacfhpaihoh	Enkrypt
mcohilncbfahbmgdjkbpemcciolgcge	OKX Web3 Wallet
epapihdplajcdnnkdeiahlgigofloibg	Sender
gjagmgiddbbciopjhllkdnddhcglnemk	Hashpack
kmhcihpebfmpgmihbkipmjlmioameka	Eternl
bgpipimickeadkjlklgciifhnalhdjhe	GeroWallet
phkbamefinggmakgklpljjmgibohnba	Pontem Wallet
ejjladinnckdgjemekebdpeokbikhfci	Petra Wallet
efbglgofoippbgcjepnhiblaibcncglk	Martian Wallet
cjmkndjhnagcfbpiemnkdpomccnjbmlj	Finnie
aijcbedoijmgnlmjeegjaglmepbmkpi	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="3h8W2nPBk4nRDUrB6Y0h0HLpyqaFdsG77R2qmHs6N8ltqBhW4SbYsSYEyutCXGUpq"

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

    $dnm_c="tsUYxh4R2BMPI6IVK7msKOJi8MeYnj3B4ogS6KPyHbGwtYiJEr9efHvkNOaoLGqUp"

    $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. Şüphelenilen bir durumda ağın izlenmesi ve duruma göre müdahale edilmesi gerekmektedir.

HAZIRLAYAN

Elif AĐLAR

<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/>