ECHO

CYBER THREAT INTELLIGENCE

StealC Technical Analysis Report

Prepared By ECHOCTI

Content

Tables

Request Content

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.

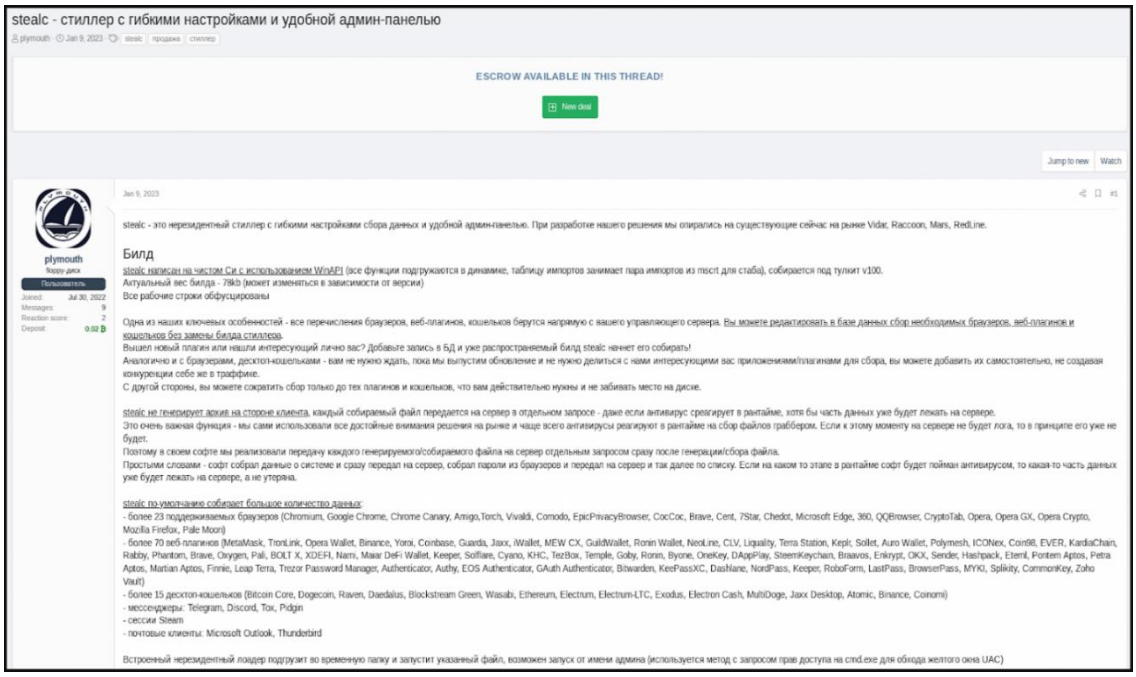
Based on our analysis conducted by the EchoCTI Analyst Team, we have identified that the distinctive features of the StealC family could potentially pose a significant and persistent threat in the near future. Therefore, by sharing this technical analysis report, our aim is to assist in enhancing your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

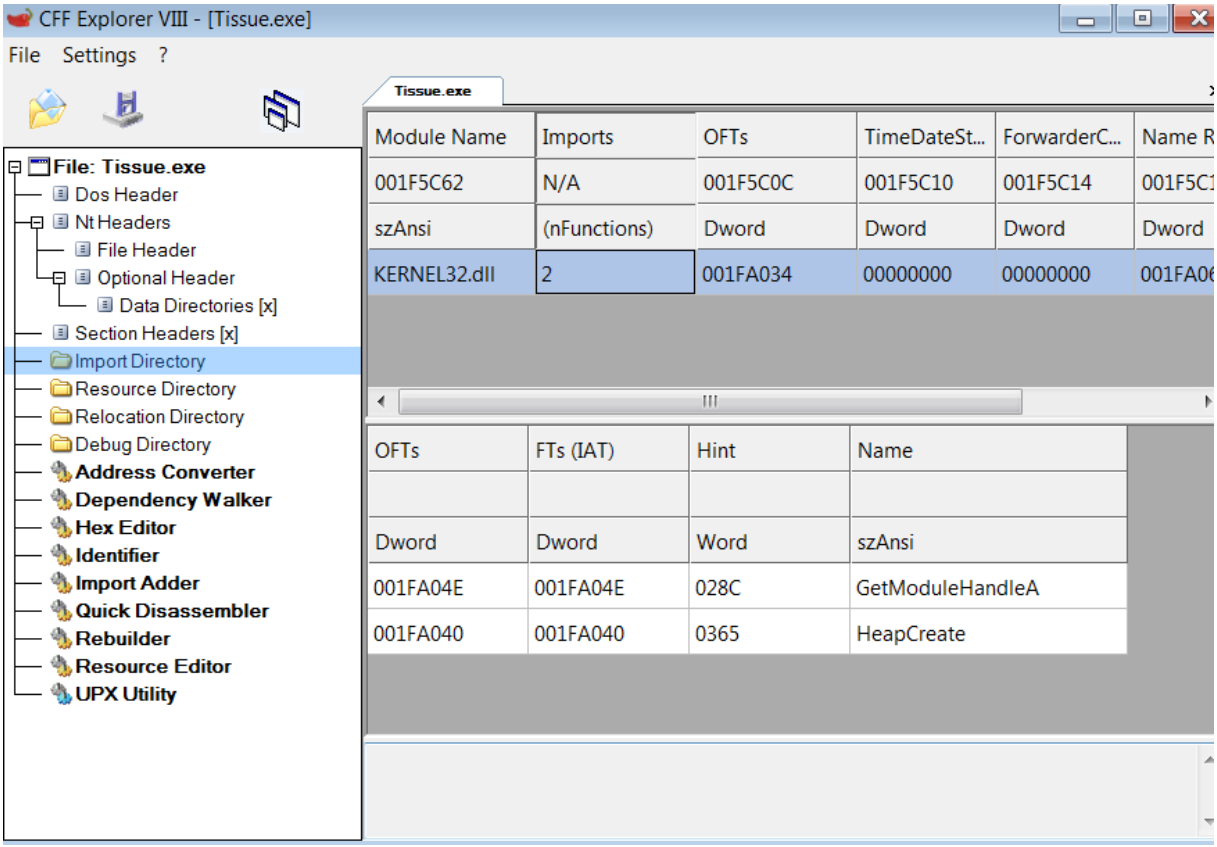


Şekil 1 Stealc Malware Family Advertisement

Tissue.exe Technical Analysis

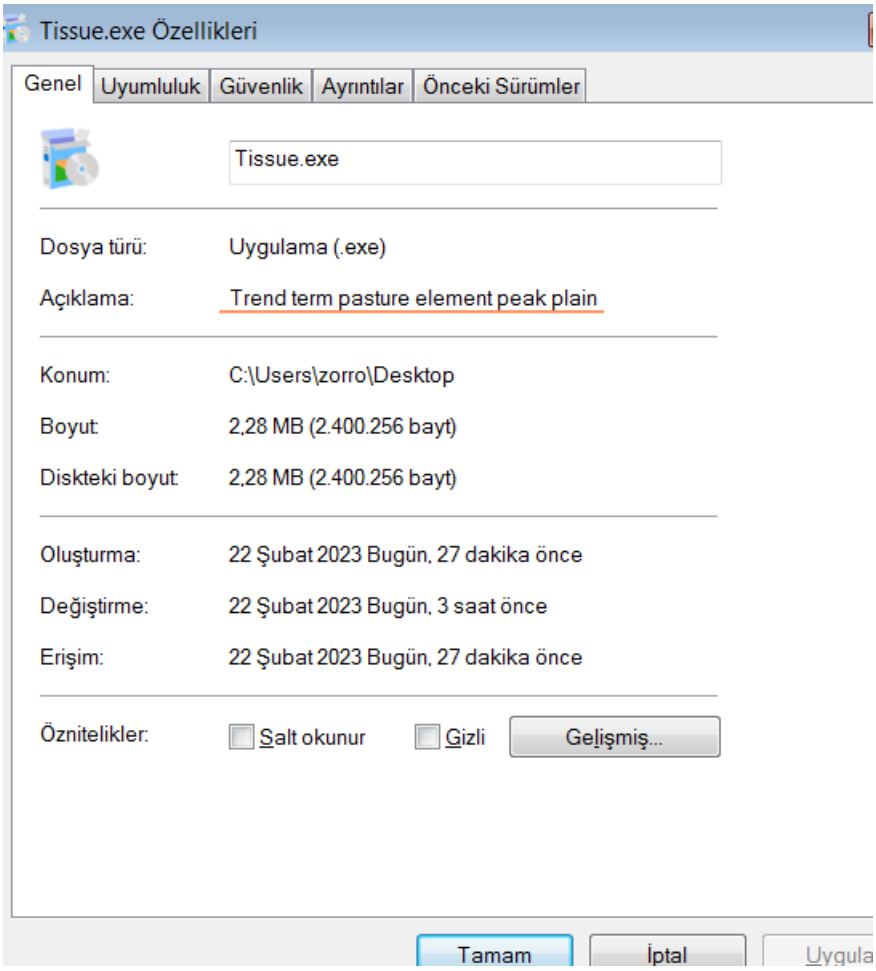
File Name	Tissue.exe
SHA256	1587857AD744C322A2B32731CDD48D98EAC13F8AA8FF2F2AFB01EBBA88D15359
File Type	PE32-EXE

Tablo 1 Tissue.exe File Informations



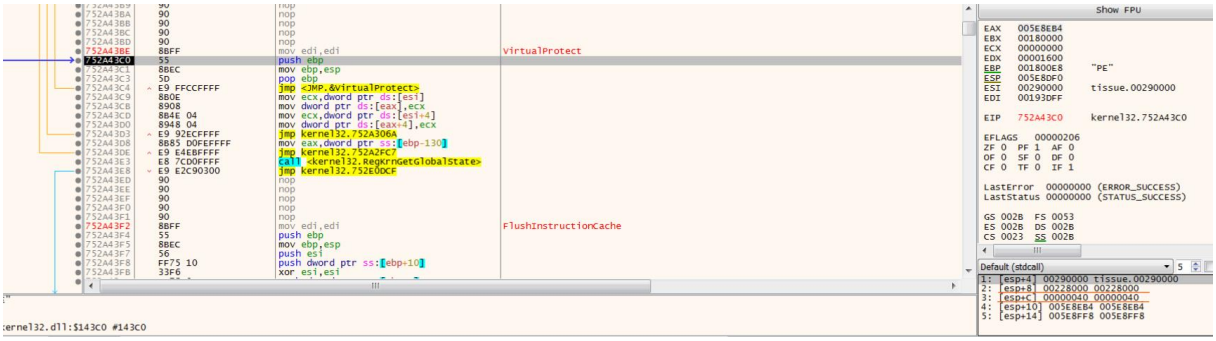
Şekil 2 Malware Import Address Table

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



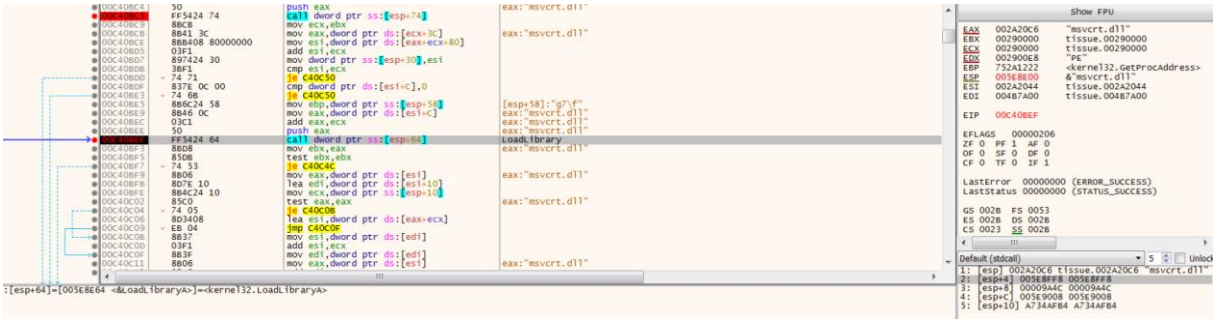
Şekil 3 Explanation Information of the Malicious Application

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



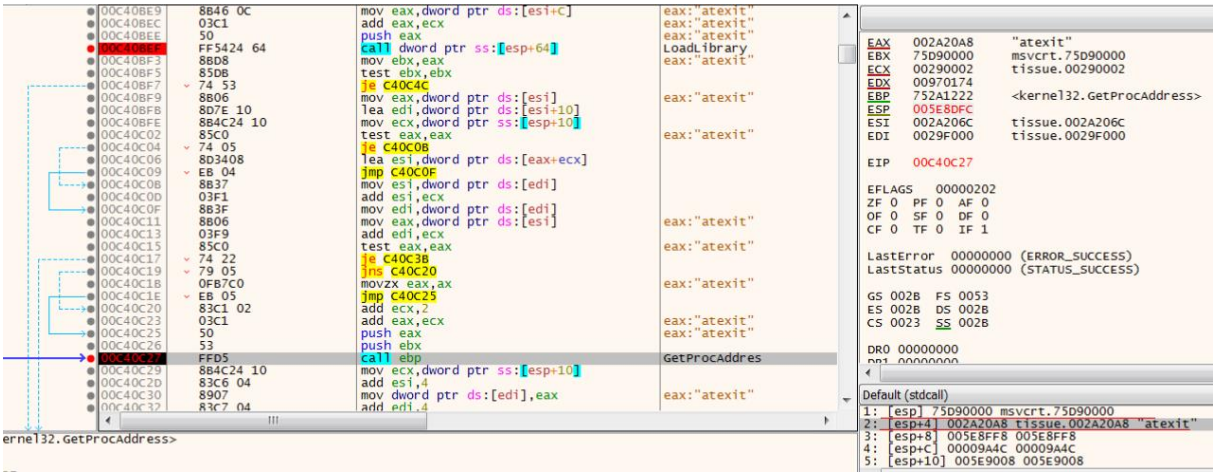
Şekil 4 Virtual Protect

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

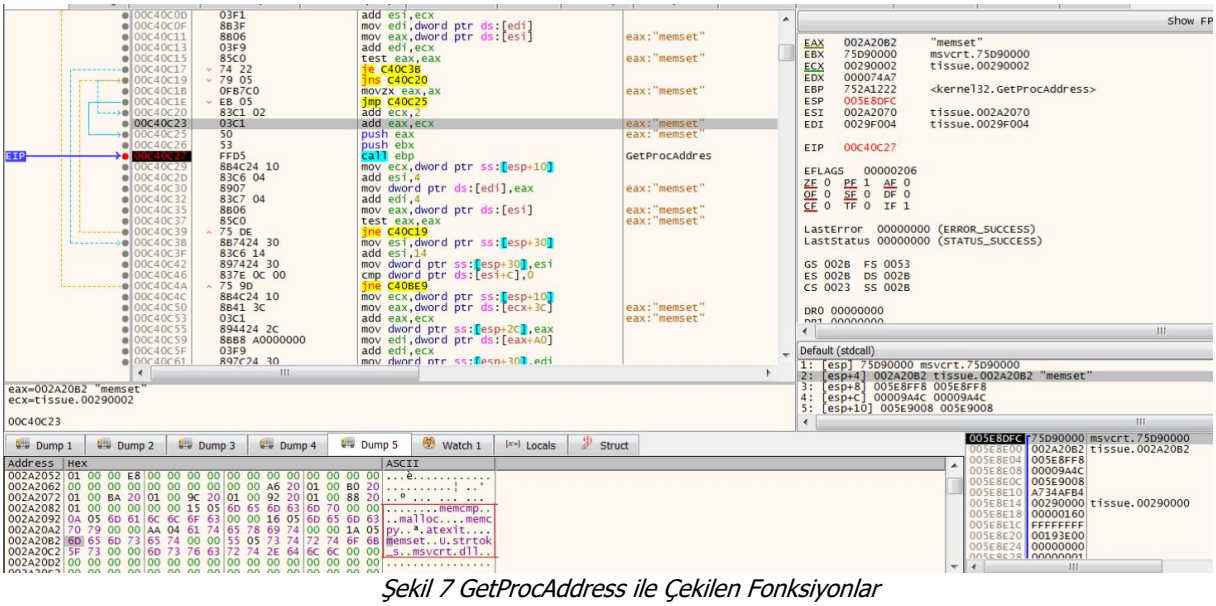


Şekil 5 LoadLibraryA

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.

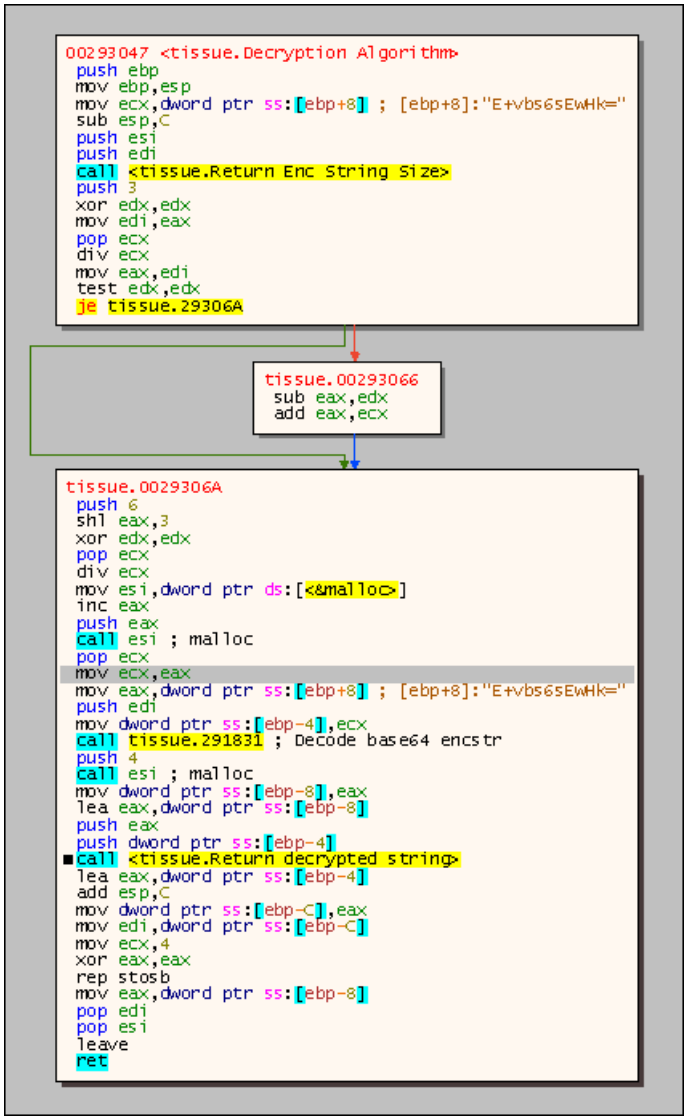


Şekil 6 GetProcAddress



Şekil 7 GetProcAddress ile Çekilen Fonksiyonlar

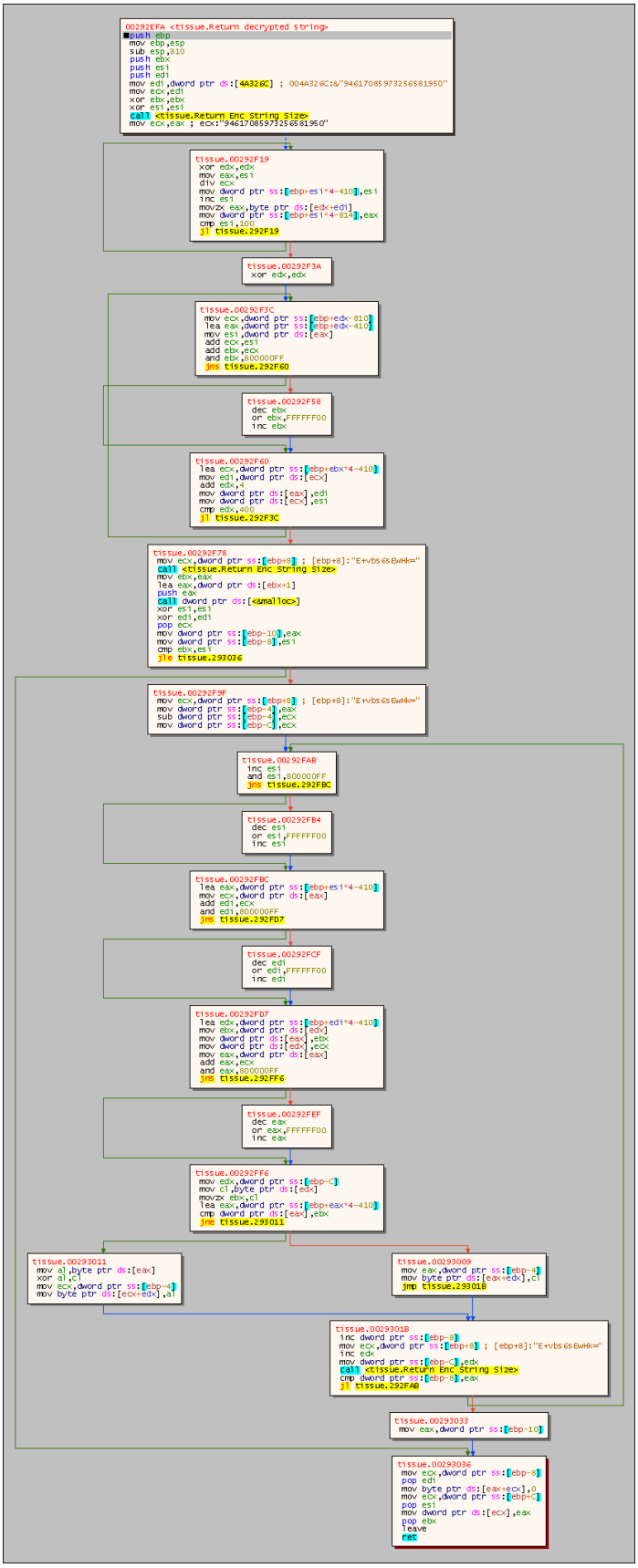
It was observed that certain functions from the dynamic library msvcrt.dll were loaded (such as memset, malloc, atexit, etc.).



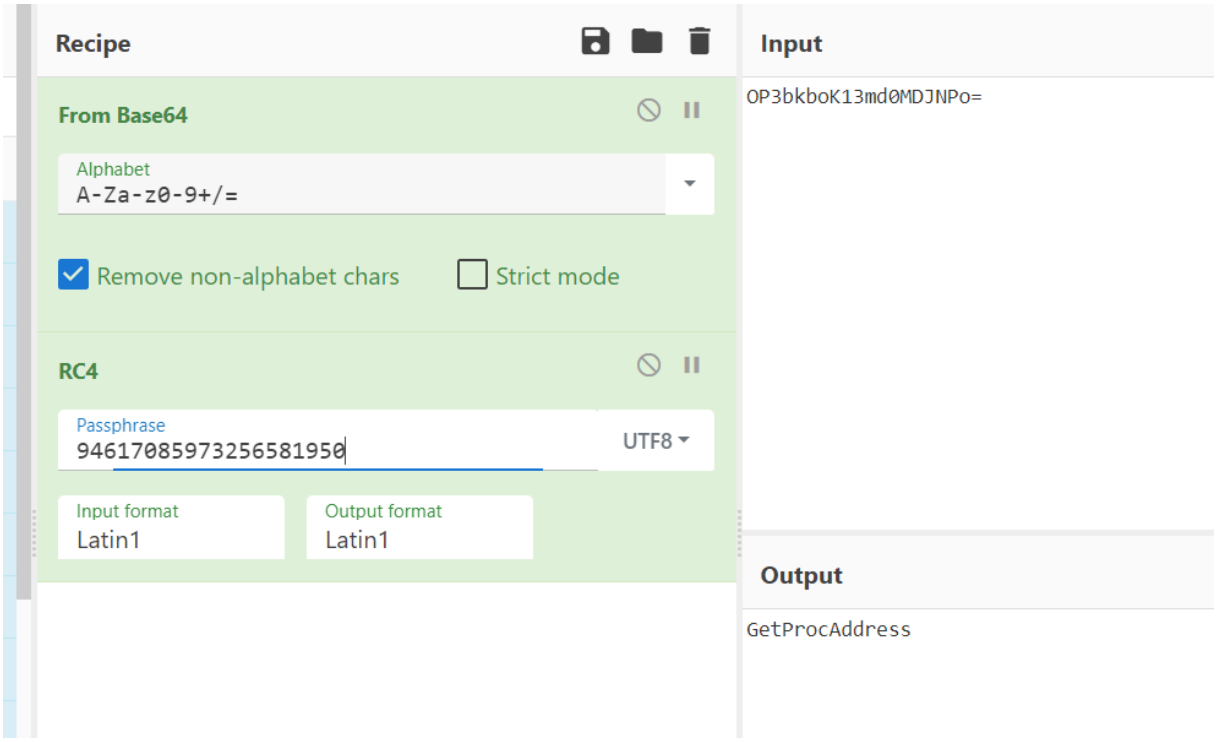
Şekil 8 String Decryption Algorithm

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.

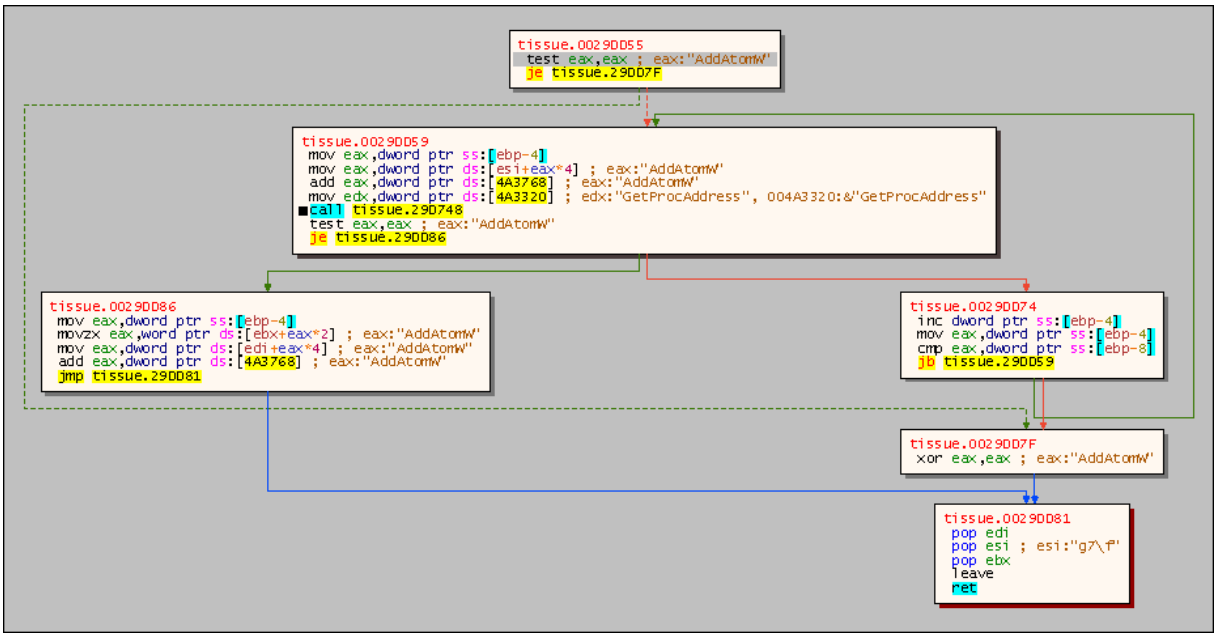


Şekil 9 String Decryption Function RC4 Algorithm



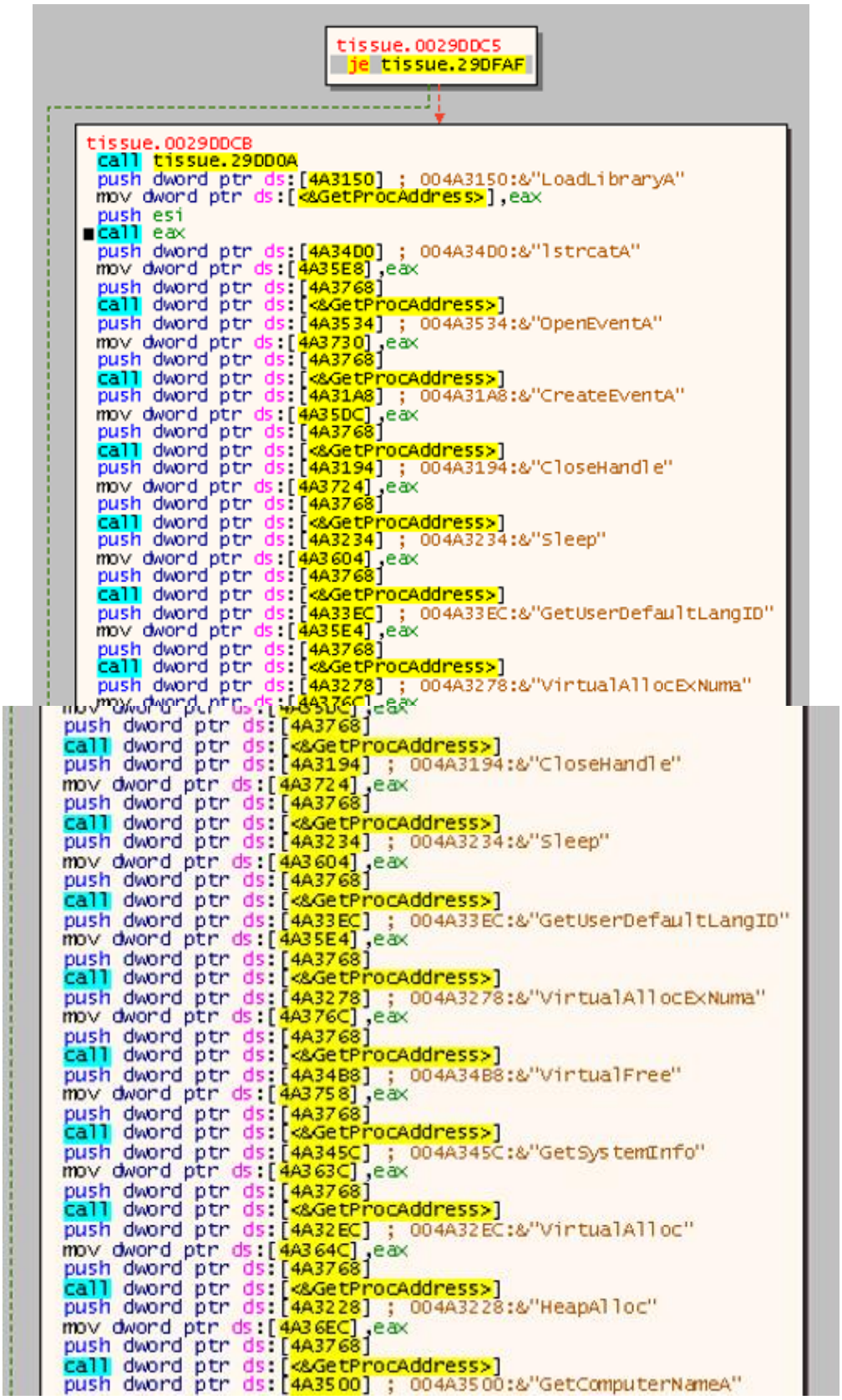
Şekil 10 An Example of String Decryption

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.

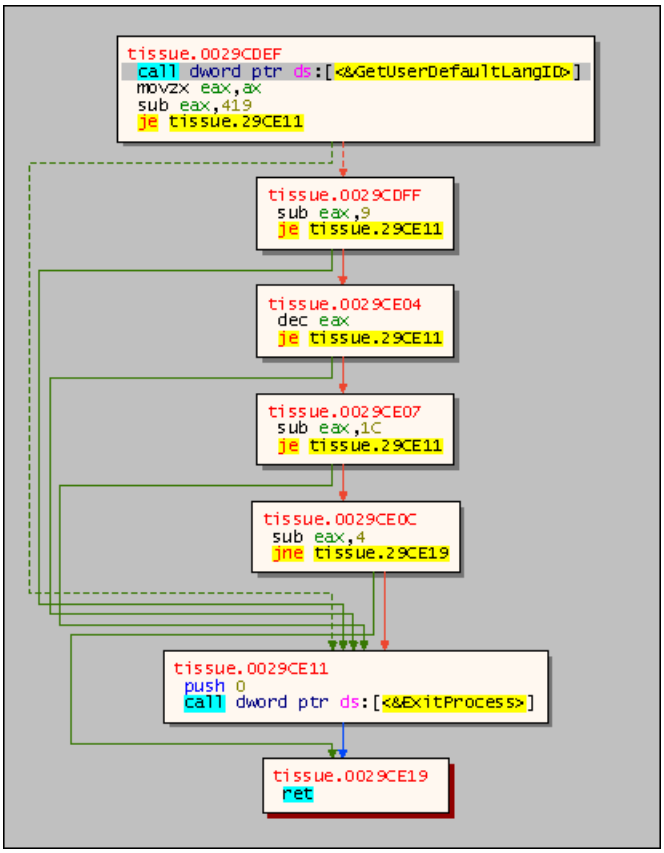


Şekil 11 Searching kernel32.dll APIs for GetProcAddress

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.



Şekil 12 Loads Decrypted APIs and Dlls



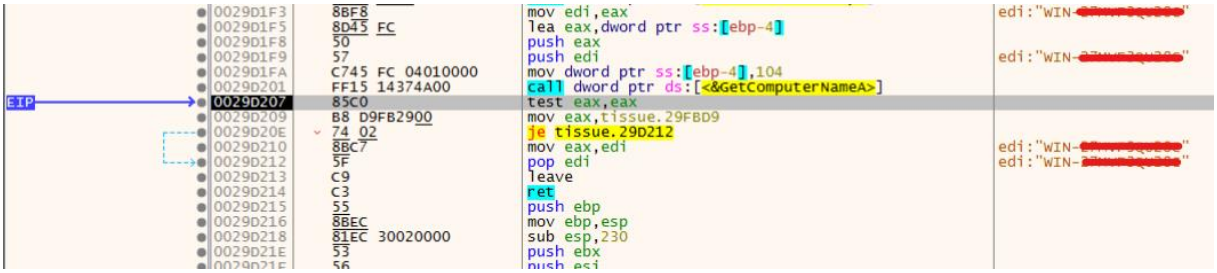
Şekil 13 Checking User Country

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

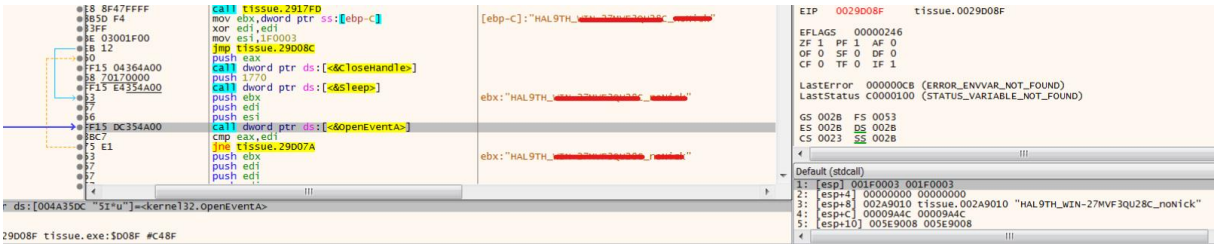
Tablo 2 White List for Countries

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



Şekil 14 Getting Computer Name

Şekil 15 Getting Username

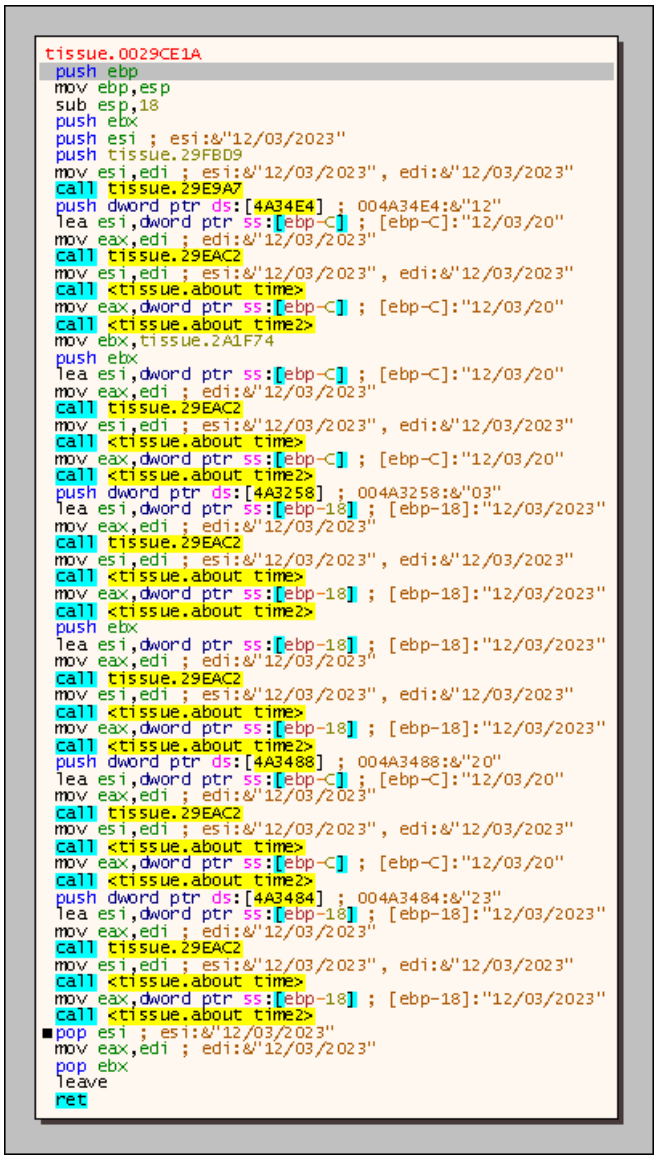


Şekil 16 Try to Open an Event

Şekil 17 Create an Event

It has been identified that an event is generated in the format of HAL9TH_computername _username.

Şekil 18 Getting System Time



Şekil 19 Time Resolution 12/03/2023

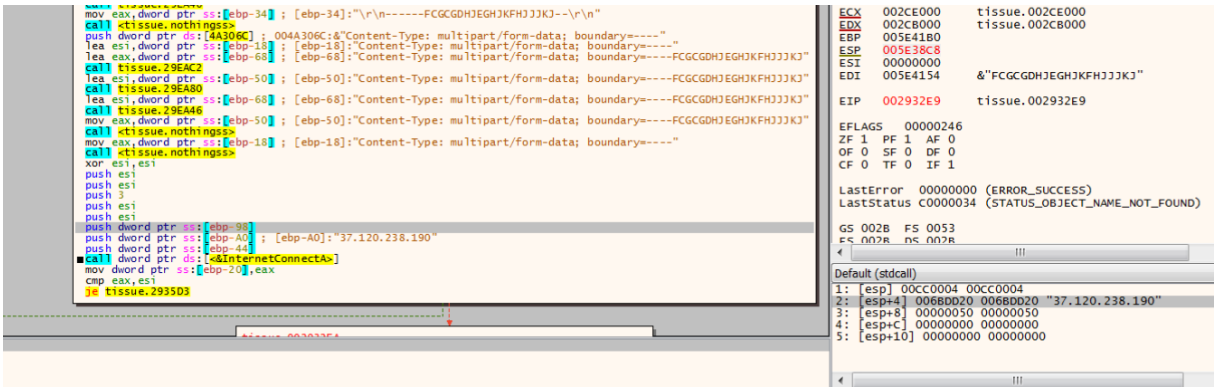
It has been observed that this malicious software has a deadline, and if this time elapses, it will cease to function. This feature is believed to be related to the licensing aspect of the malware's sale.

Şekil 20 Loads Decrypted API and DLLs via GetProcAddress

Network

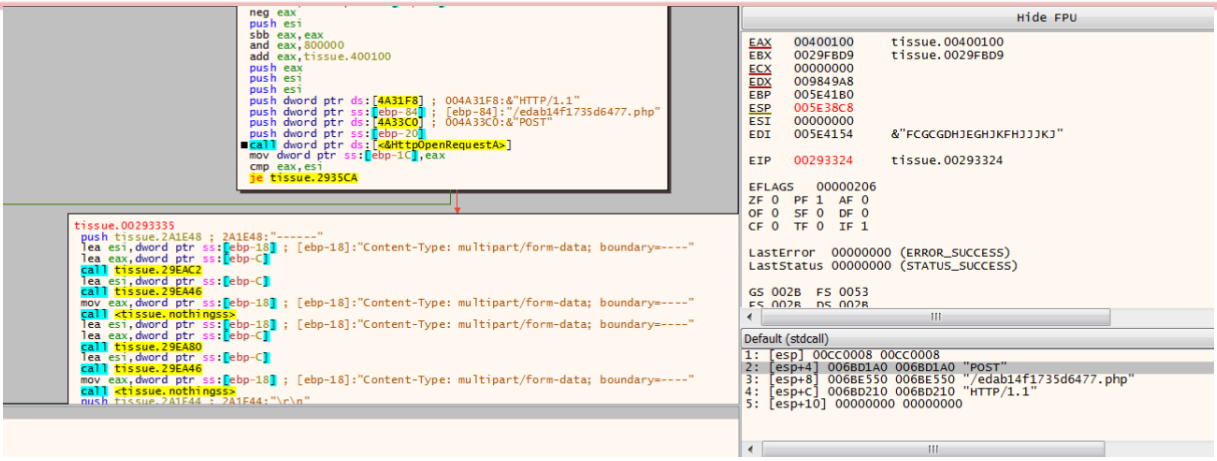
The identified network findings related to the malware are as follows:

- 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

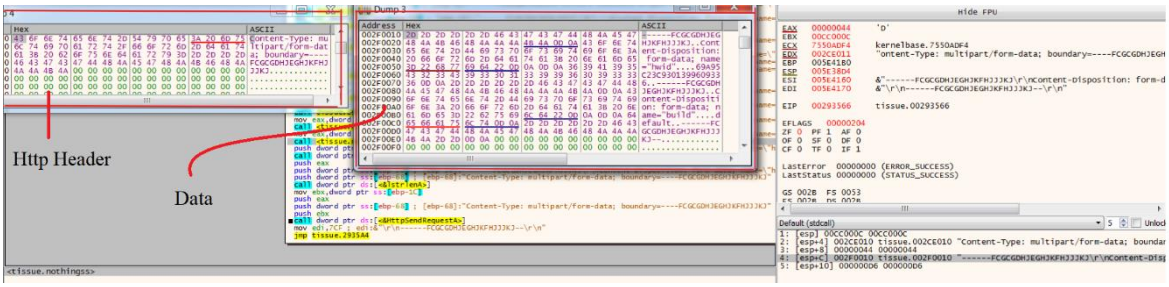


Şekil 21 Internet Connection to Decrypted IP Address

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



Şekil 22 HttpOpenRequest



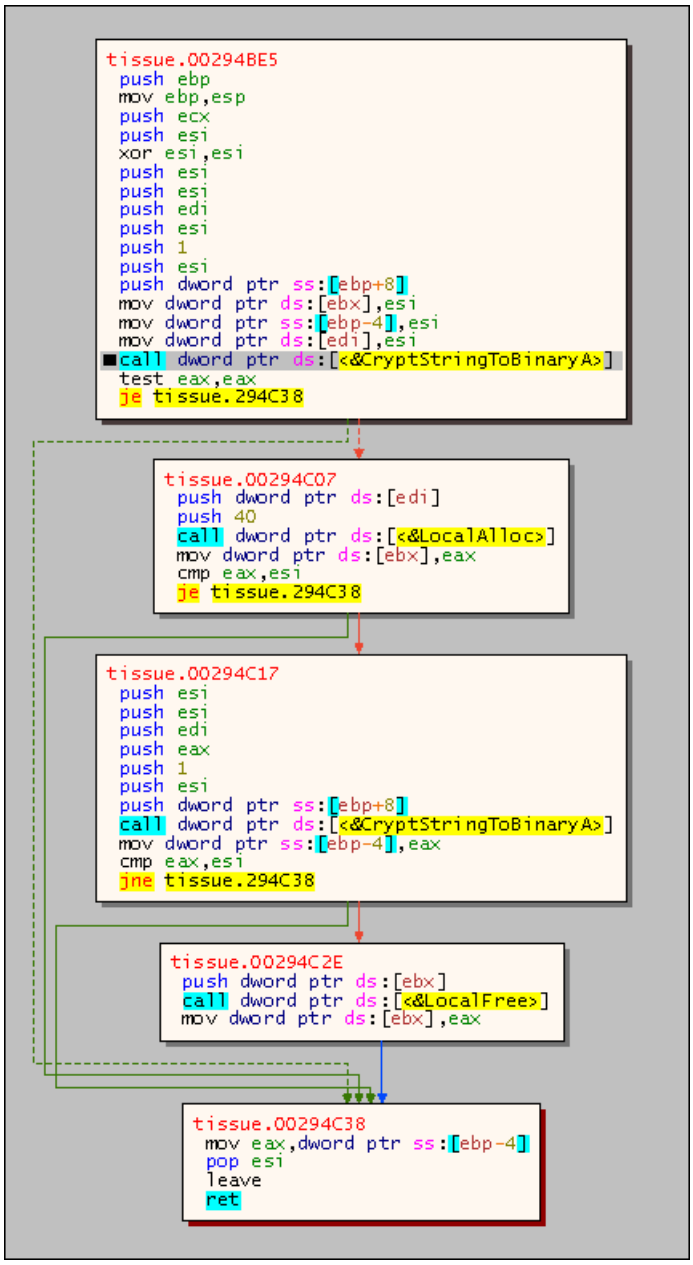
Şekil 23 HttpSendRequest

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\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

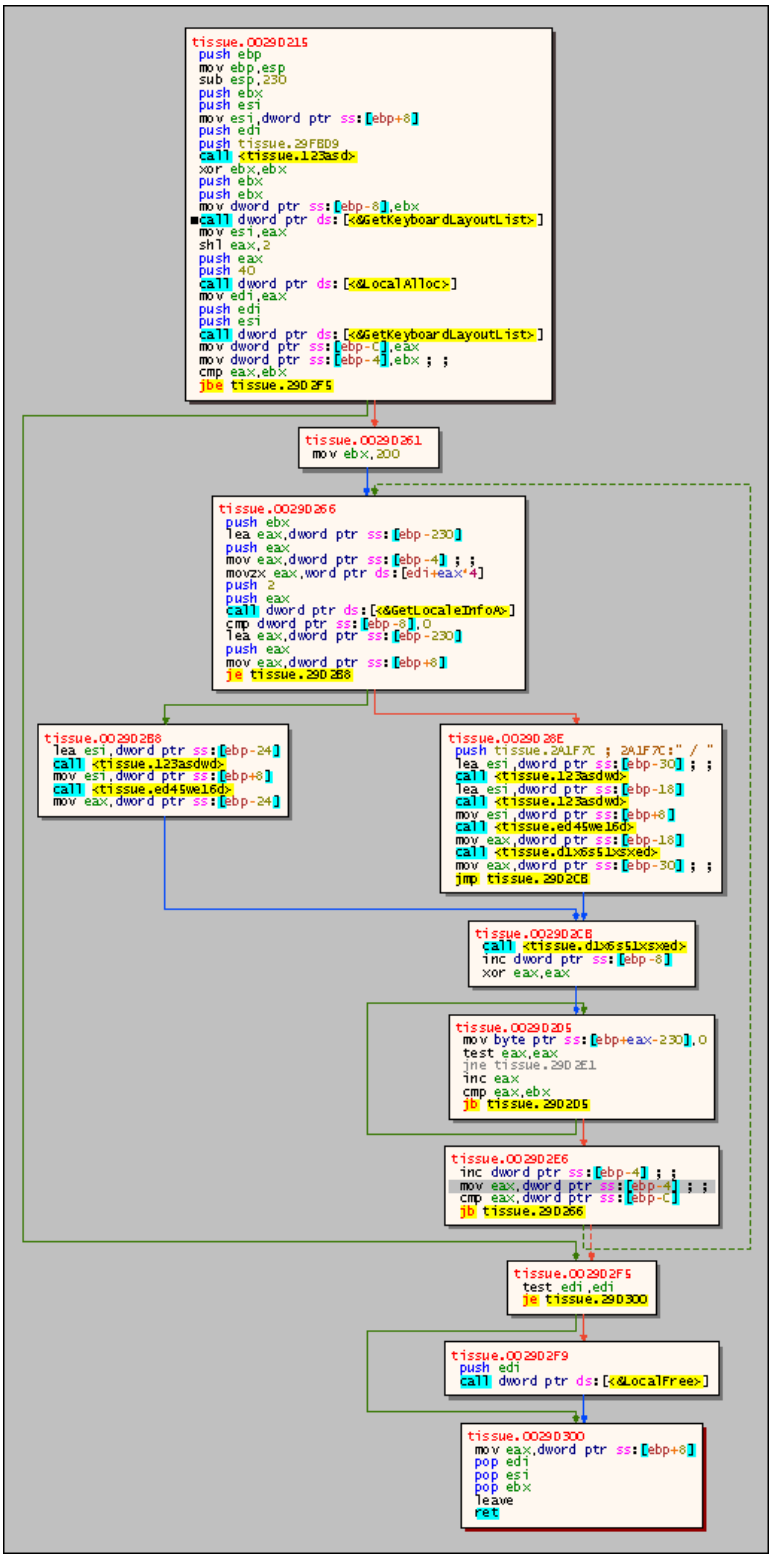
It was determined that the malware sent two more HTTP POST requests.

```
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

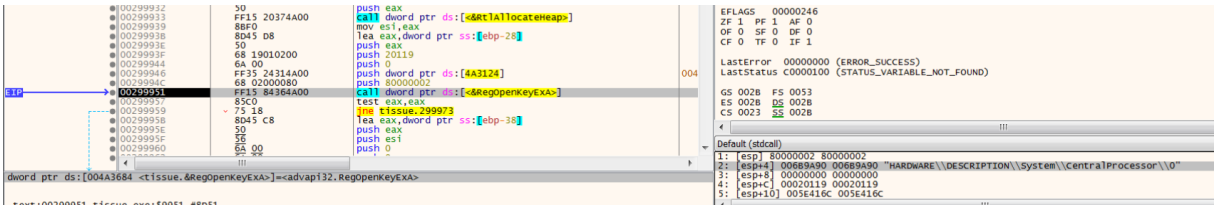
```
Header
"Content-Type: multipart/form-data; boundary=----EGIIJDHCGCBKECBFIJKK"
Content
"------EGIIJDHCGCBKECBFIJKK\r\nContent-Disposition: form-data;
name=\"token\"\r\n\r\nEchoCTI\r\n------EGIIJDHCGCBKECBFIJKK\r\nContent-Disposition: form-
data; name=\"message\"\r\n\r\nplugins"
```

Request Content 3 Request 3

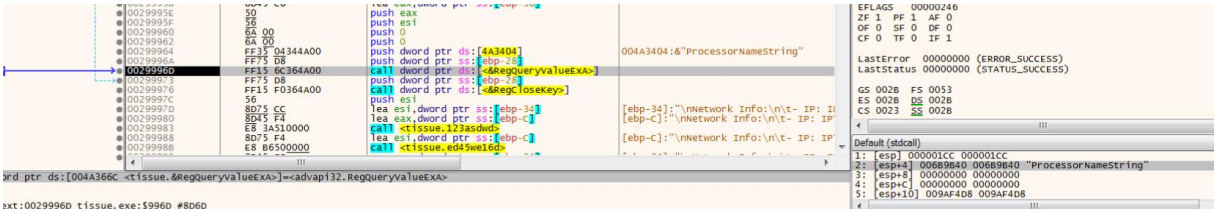


Şekil 25 GetKeyboarLayoutList

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



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

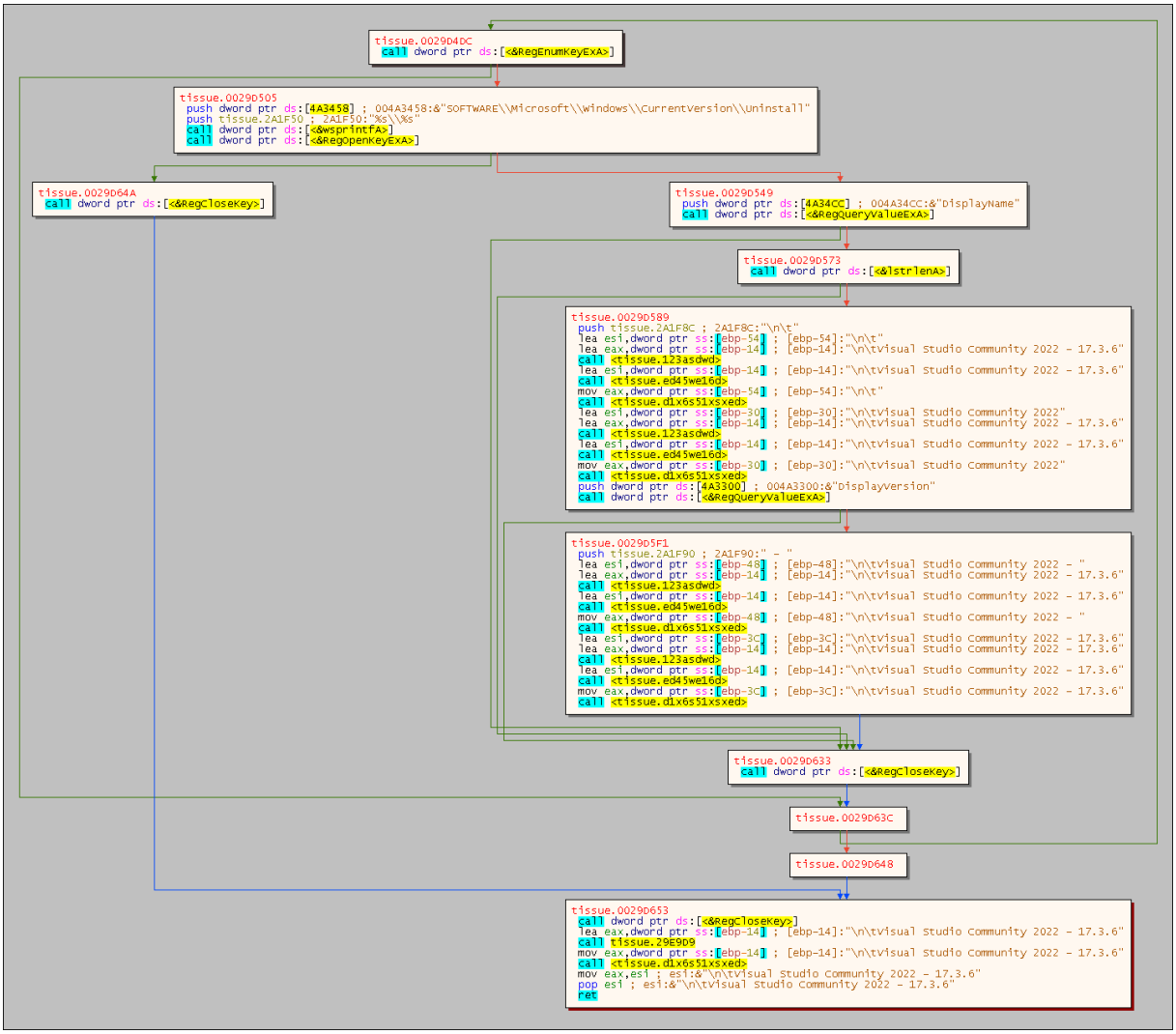


Şekil 27 RegQueryValue for ProcessorNameString

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:

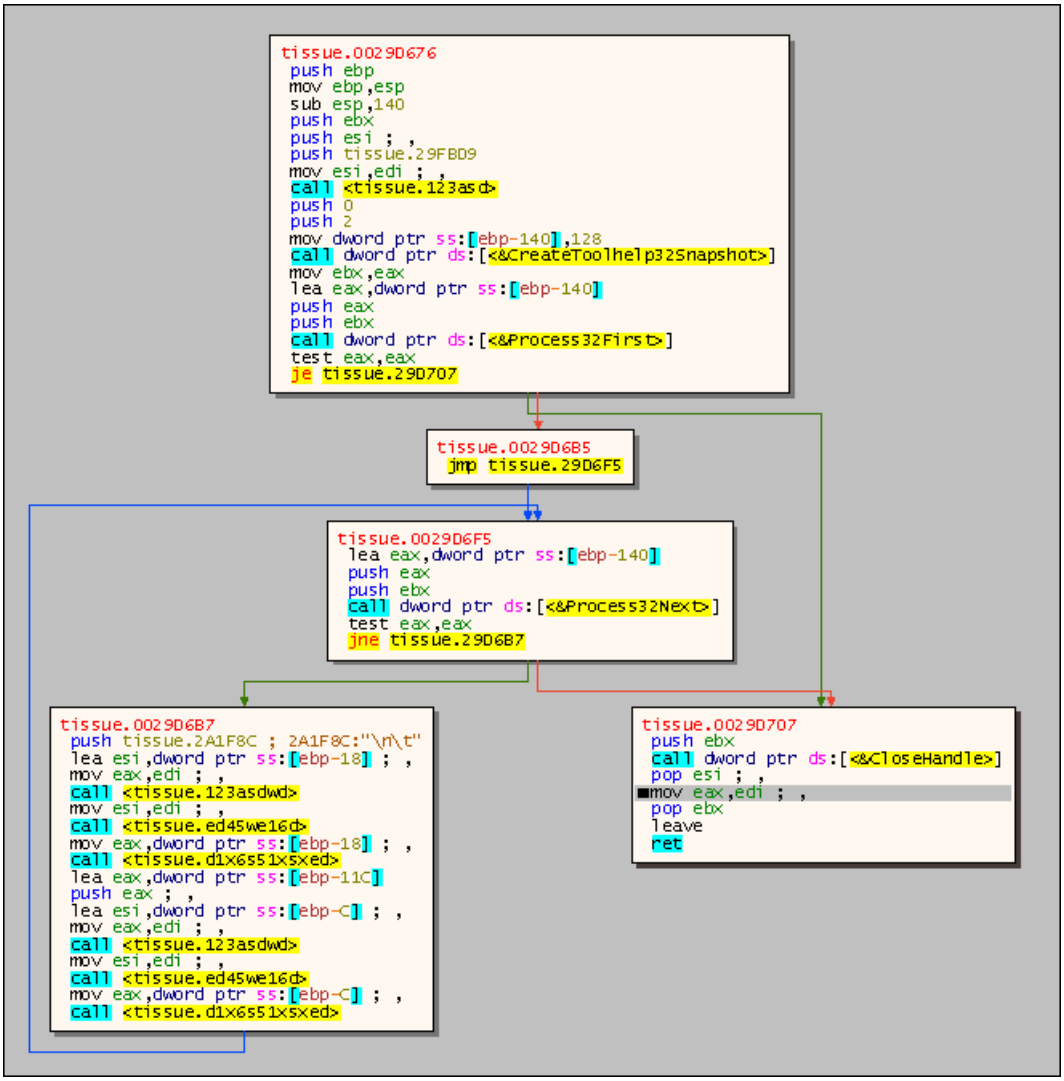
1. SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion
2. HARDWARE\\DESCRIPTION\\System\\CentralProcessor\\0
3. HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall



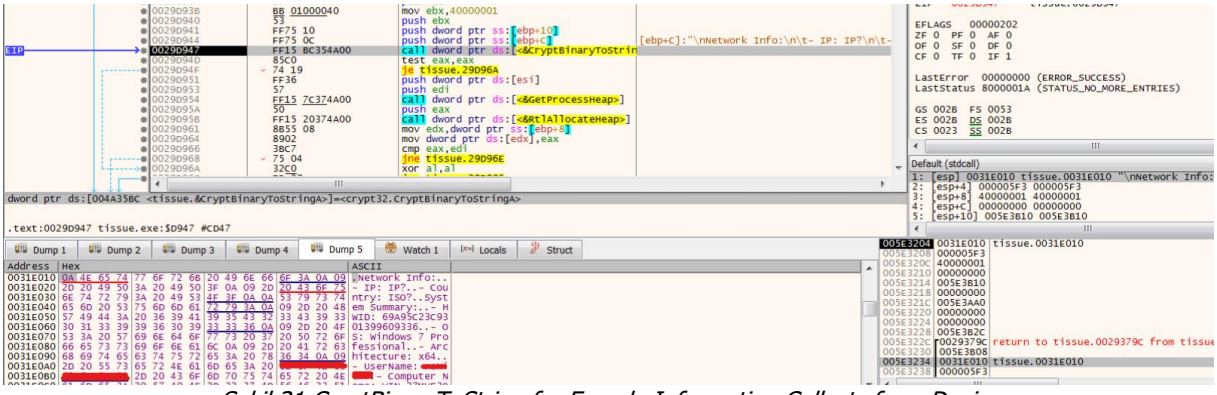
Şekil 29 Collecting Names and Version Information of Certain Software Products

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. Bilgisyar Mimarisi
6. RAM Depolama Alanı
7. Ekran Boyutu Bilgisi
8. Arka Planda Çalışan Process Listesi

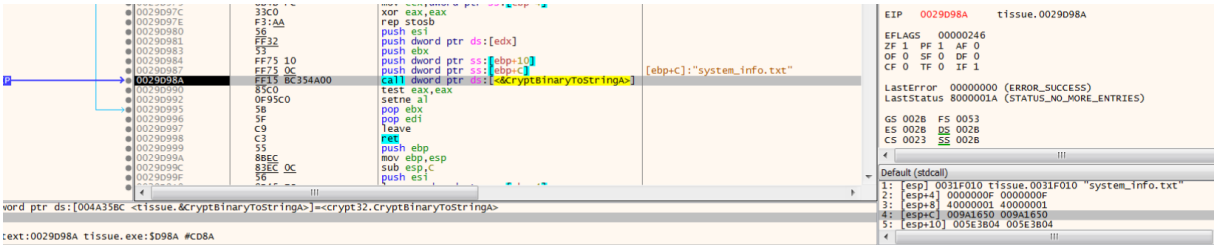


Şekil 30 The Algorithm of Collection Processes that Running Background



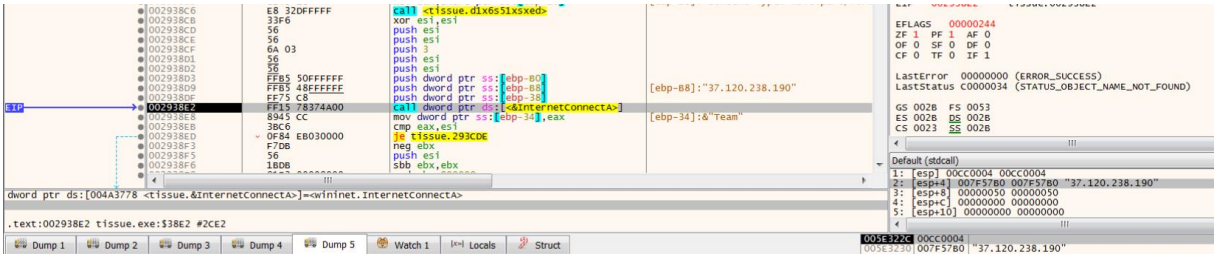
Şekil 31 CryptBinaryToString for Encode Information Collects from Device

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



Şekil 32 Encodes system_info.txt file name

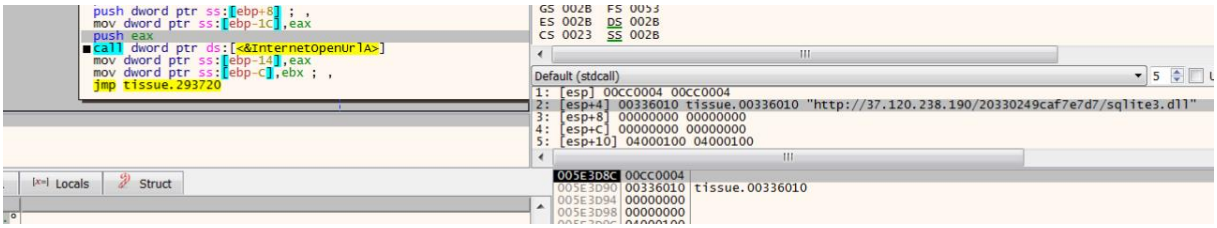
It has been observed that a string expression named 'system_info.txt' is also converted into Base64 encoding format. It has been determined that this string expression represents a file name.



Şekil 33 InternetConnect for Send Information

Şekil 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.



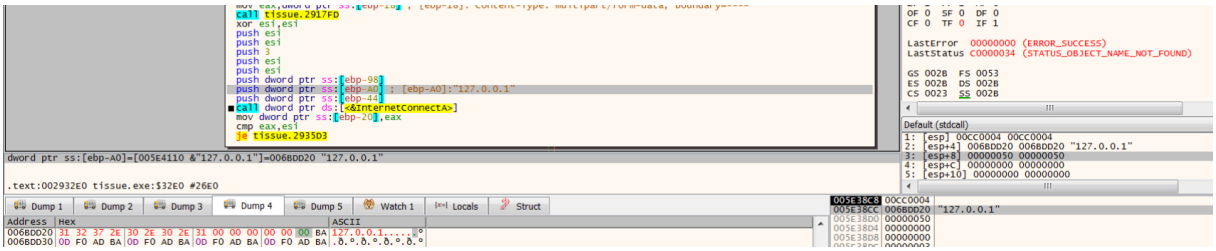
Şekil 35 Drope sqlite3.dll: InternetOpenUrl

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\n{Collects Info Base64 form}”

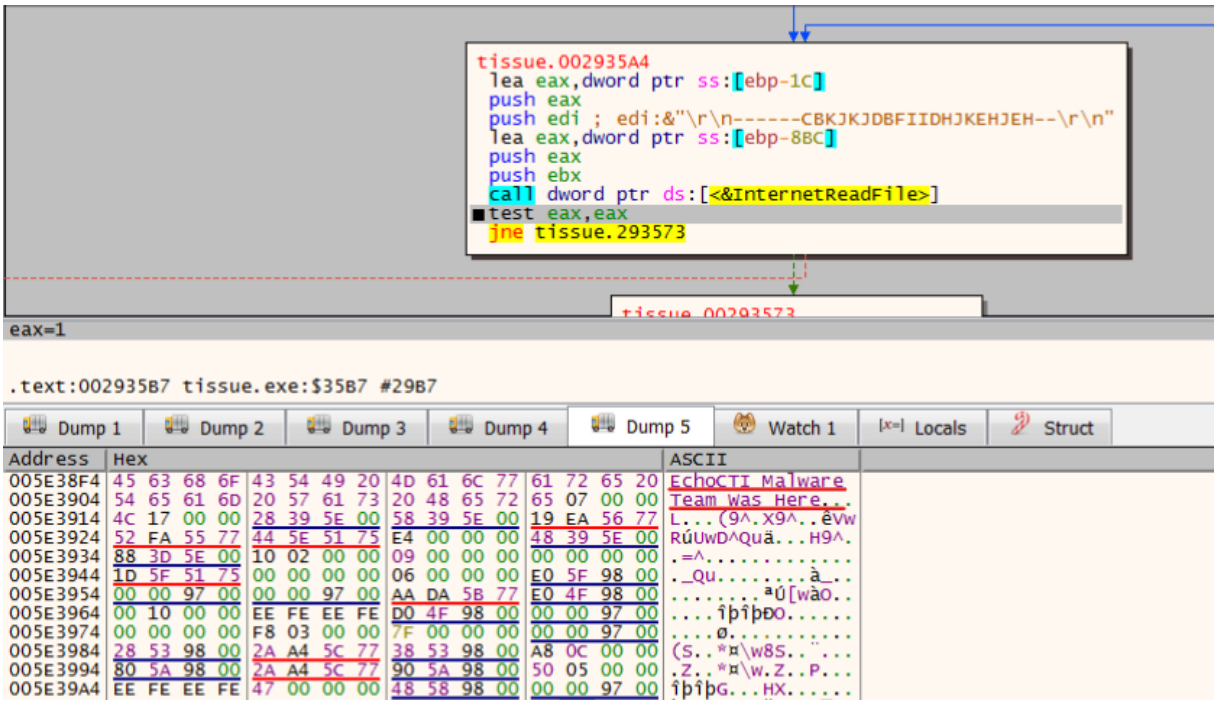
Request Content 4 Request 4: Sending Collects Information

Reversing Network Protocol

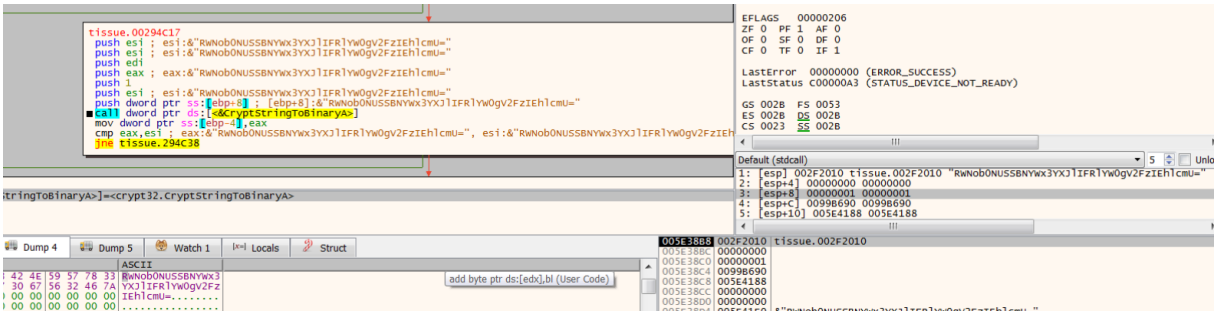


Şekil 36 Reversing Network Protocol: InternetConnectA

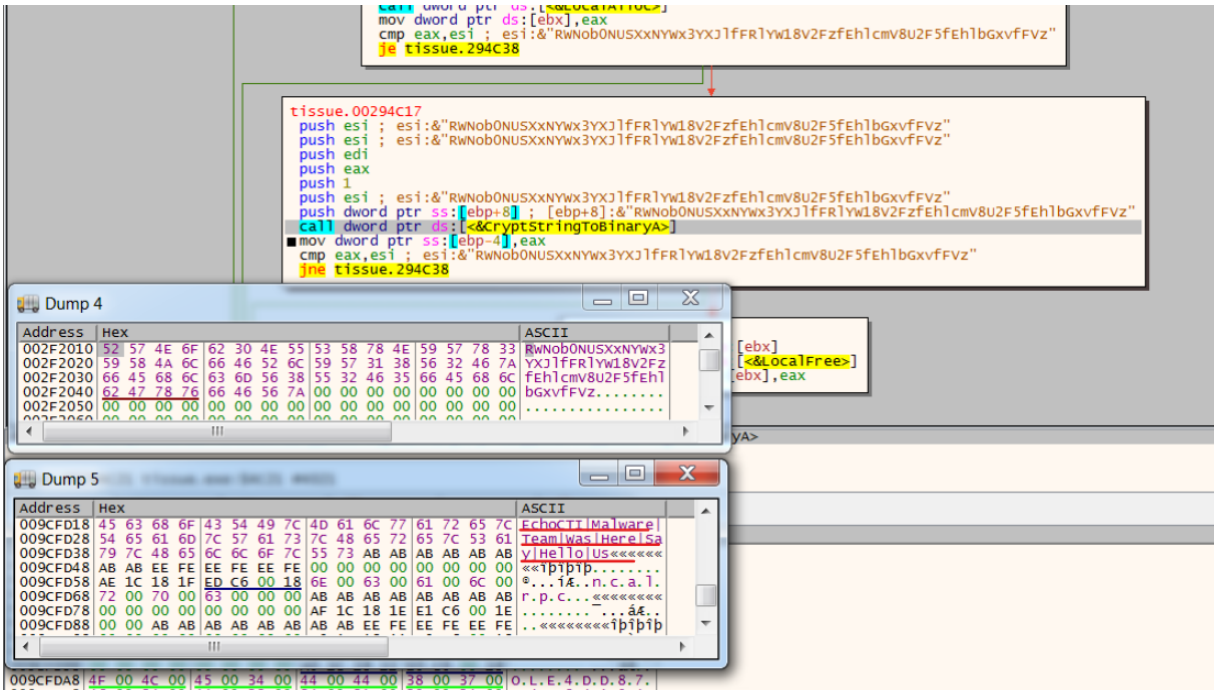
Şekil 37 Reversing Network Protocol: HttpOpenRequest



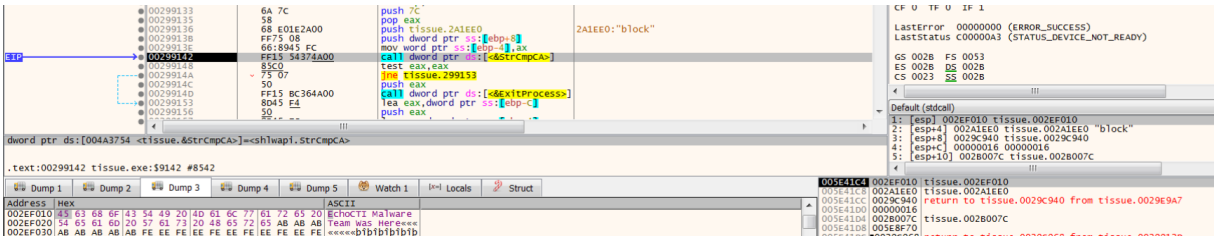
Şekil 38 Reversing Network Protocol: InternetReadFile



Şekil 39 Reversing Network Protocol: Decode Base64 Response



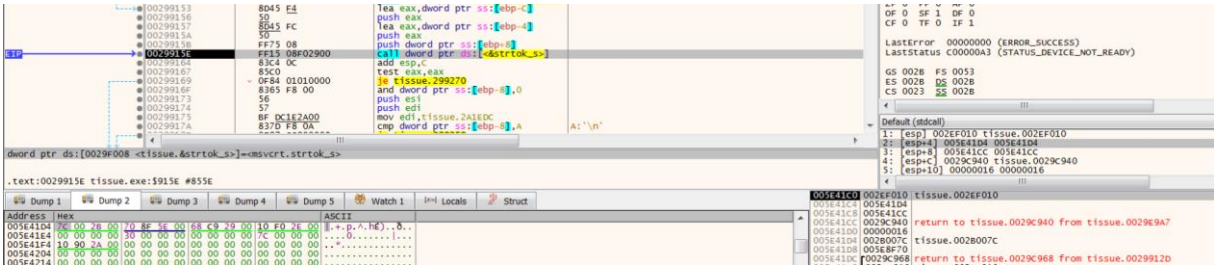
Şekil 40 Reversing Network Protocol: Decoded form of Response



Şekil 41 Reversing Network Protocol: Control Blocking

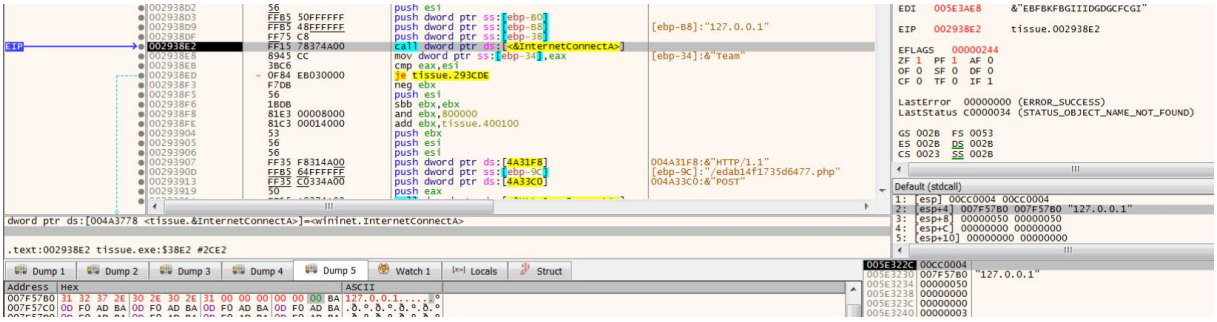
It has been observed that the malware performs blocking control based on the request sent. Possible checks performed on the server side could be as follows:

- 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.

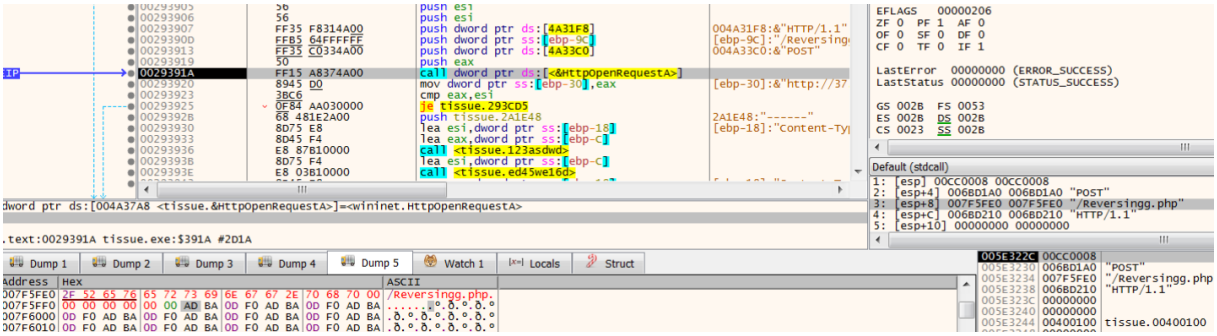


Şekil 42 Reversing Network Protocol: Differentiating the content of the Response.

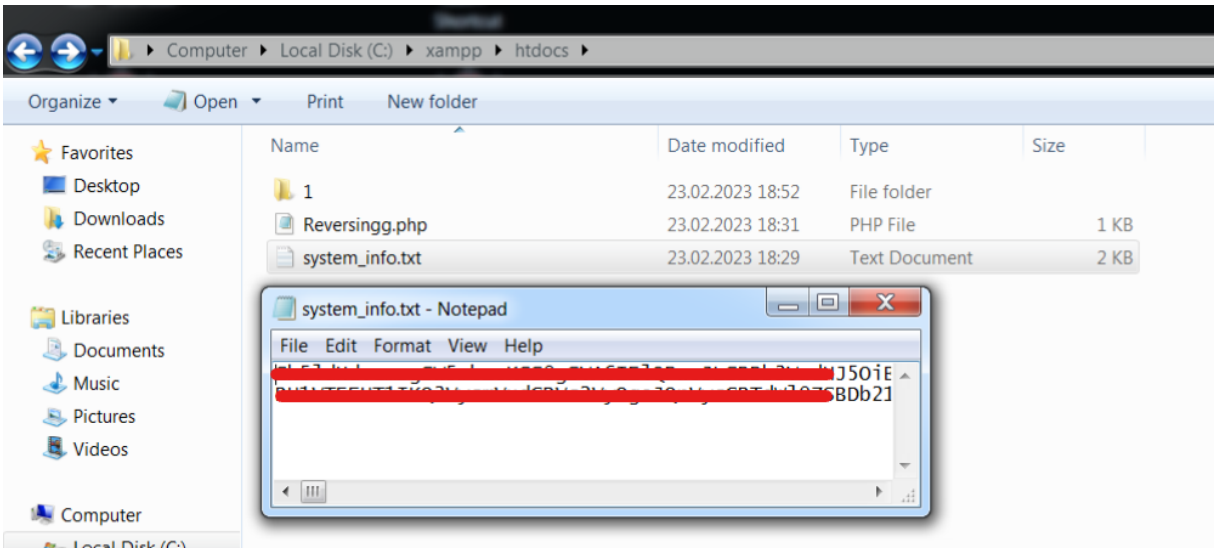
It was observed that values separated by '|' should be present in the Response



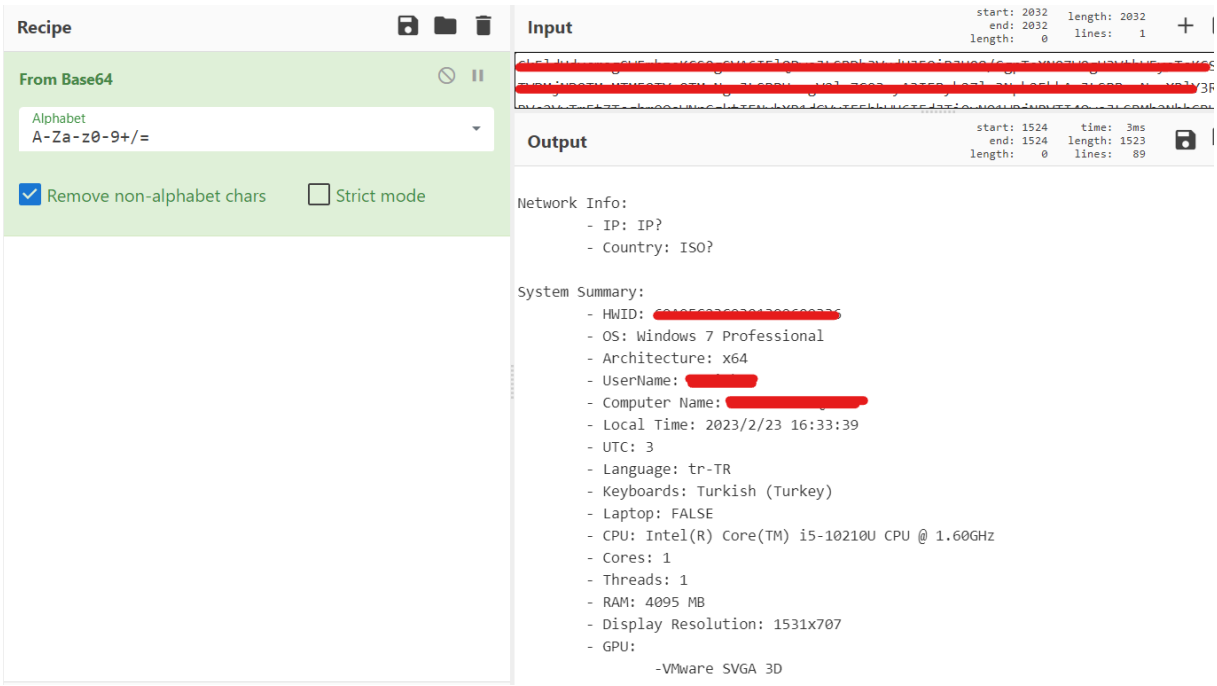
Şekil 43 Network Protocol Reversing: InternetConnect for Send Information Collects from Device



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

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	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	oeljdldpnmdbchonielidgobddfffla l
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 Targeted Browser Extention

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/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	Exfliration
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 Exfliration 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					

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

CYBER THREAT INTELLIGENCE