

Forum: [Hack Forums](#)

Thread: [\[Malware Analysis\] ZeroTrace Stealer packed via SFX, dropping multiple payloads](#)

Bastille - May 17, 2025, 8:35 am

Tool shared : ZeroTrace Stealer ([BroadCom Article](#))

Quote: April 14, 2025

ZeroTrace Stealer is a new infostealing malware that recently emerged on the threat landscape. The malware builder has been distributed via various underground forums and file-sharing platforms while advertised as being created for educational and research purposes only. ZeroTrace is a C#-based variant with functionality to exfiltrate various confidential data from the infected machines. The targeted data includes credentials, cryptocurrency wallets, cookies, browser history, user files, Discord and Telegram data, among others. The collected information might be exfiltrated back to the attackers with help of Discord or Telegram.

File downloaded : "ZeroTrace Stealer Official.zip"

Size of the archive : 90.7MB

MD5 Hash : 8c7c006e2800ff9ca09e4b7a108621a3

SHA256 Hash : 9b3313fef14fd3897ce17cb6b2b54d275fda8042b683c589527abda90842869f

VirusTotal Report :

<https://www.virustotal.com/gui/file/9b3313fef14fd3897ce17cb6b2b54d275fda8042b683c589527abda90842869f>

Detection : 10/63

1. STATIC ANALYSIS

Unzipped archive : Password.txt : adrikadi

"ZeroTrace Stealer Official.sfx.exe" [size : 90.8MB]*

VirusTotal report of "ZeroTrace Stealer Official.sfx.exe" :

<https://www.virustotal.com/gui/file/cfc156f45fe0018b10d78ea572f21f236fd065b4fc79bec9d0803de47209c8c7>

? File size

"ZeroTrace Stealer Official.zip" is 90.7Mb

"ZeroTrace Stealer Official.sfx.exe" is 90.8Mb

This is way too big for a stealer builder. We can assume that there are other things than just a builder inside.

?Double Extension

"ZeroTrace Stealer Official.sfx.exe". Author probably added SFX to make it less "suspicious" because of the .EXE extension.

?SFX extension

SFX or SEA, for "Self-Extracting Archive" are archive files working as a PE files (Portable

Executable), that's why they get the .EXE extension. These archive file can contain scripts to automatically execute tasks when unarchived. For example :

- "Path= ..." Custom extraction location, files will be saved at this location
- "Setup=..." Execution of executables

? How .SFX files work?

Windows executes it as a regular .exe file, because it's a valid Portable Executable (PE).

The embedded SFX (self-extracting archive) module kicks in — usually from WinRAR or 7-Zip.

It reads the SFX script stored in the comment section

It extracts the files, often silently into a temporary folder (%TEMP% or %APPDATA%).

Then, it executes each file listed with Setup=, in the order they appear.

Using ? Strings we can find the script which starts with "CMT", here is the content :

The script will execute each file (.vbs, .exe) in the order displayed. To take a look at each of these I've used the following website : <https://www.ezyzip.com> to extract the files online. Each of these will execute a .bat file :

The .bat files are droppers that will download executables from a website. 4 files will be downloaded from the same website based on the bat file below :

- setup.exe
- clip.exe
- update.exe
- svchost.exe

When browsing the website, it looks "closed" :

But the payloads can still be downloaded, I'll not take a look it depth here to stay focused on the main malware, but it will be possible to conduct analysis on them, or define them as exercises for beginners :clip.exe, VirusTotal report :

<https://www.virustotal.com/gui/file/78d513d80e7273a5fbace44a52bac6751628d36e02eafacbe6a289931e6a5344>

setup.exe, VirusTotal report :

<https://www.virustotal.com/gui/file/5138ca2a5f362bb67bd6e485f34149c39b30b2363da04784e4f5a7e71a7604b6>

svchost.exe, VirusTotal report :

<https://www.virustotal.com/gui/file/36d2731a3b140a6cd2197f9f89fff65df6b2633b07f9b765c82432db79219754>

update.exe, VirusTotal report :

<https://www.virustotal.com/gui/file/5138ca2a5f362bb67bd6e485f34149c39b30b2363da04784e4f5a7e71a7604b6>

Going back to the SFX script, some .exe files are also executed :conhost.exe, VirusTotal report :

<https://www.virustotal.com/gui/file/6353b1218561a746bb3e009b611a1945bc2367b4d3ffef7849d4af>

[4d369f184c](#)

crack.exe, VirusTotal report : [wasn't able to upload on VT]

svchost.exe, VirusTotal report :

<https://www.virustotal.com/gui/file/710c10e169bc8d0bb92be5750aa7de0faf1a0cc89d64fa6c9a4e44f0c87e6479>

sass.exe, VirusTotal report :

<https://www.virustotal.com/gui/file/78d513d80e7273a5fbace44a52bac6751628d36e02eafacbe6a289931e6a5344>

After getting all those shits dropped and ran on our computer, we'll focus on the "main files" :
zeroTrace Stealer Official.exe
crack.exe

zeroTrace Stealer Official.exe

I've ran the tool on a VM and so far nothing suspicious. I didn't go in depth, only ran the tool.
The tool seems to be executed normally, few features are disabled and require "to be member", but the tool is supposed to be free.

crack.exe

It's supposed to be the activator, but ZeroTrace is announced to be free. Crack.exe drops clppth.exe which is a clipper.

ZeroTrace Stealer has been available on Github, but the repos have been taken down.

ZrNoxb - May 17, 2025, 8:49 am

Very good report, thanks for letting us know.

Bastille - May 17, 2025, 8:57 am

(May 17, 2025 08:49 AM)ZrNoxb Wrote: [\[CITE\]](#) Very good report, thanks for letting us know.

Thanks ! I'm making these threads for people interested to learn malware analysis, and to warn the community that this new stealer is used with SFX files to spread malware. I've seen different SFX files on different websites while I was doing my researches for this thread

r00t34 - May 17, 2025, 11:43 am

It's good to see someone is making malware analysis. Good job @Bastille!

Bastille - May 18, 2025, 1:28 am

(May 17, 2025 11:43 AM)r00t34 Wrote: [\[CITE\]](#) It's good to see someone is making malware analysis. Good job @Bastille!

Thanks man, are you into it too ? I've seen more and more cybersecurity people joining the forum lately

r00t34 - May 19, 2025, 9:22 pm

(May 18, 2025 01:28 AM)Bastille Wrote: [\[CITE\]](#) Thanks man, are you into it too ? I've seen more and more cybersecurity people joining the forum lately

You're welcome. Yeah i am into too. For a long time i was thinking to join and now i decided to join and share what i know but my time is limited. For this reason i am preparing to make one and release soon.

Bastille - May 19, 2025, 9:49 pm

(May 19, 2025 09:22 PM)r00t34 Wrote: [CITE](#) You're welcome. Yeah i am into too. For a long time i was thinking to join and now i decided to join and share what i know but my time is limited. For this reason i am preparing to make one and release soon.

I will be glad to read your thread, feel free to let me know when it's out :)

SIM-5600039 - May 21, 2025, 1:59 pm

Thank you for the analysis of the tool.