

Forum: [Hack Forums](#)

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

Bastille - May 18, 2025, 8:03 am

Tool shared : Arkei Stealer ([Malpedia](#))

Quote:Arkei is a stealer that appeared around May 2018. It collects data about browsers (saved passwords and autofill forms), cryptocurrency wallets, and steal files matching an attacker-defined pattern. It then exfiltrates everything in a zip file uploaded to the attacker's panel. Later, it was forked and used as a base to create Vidar stealer.

File downloaded : "Arkei_Stealer_2025_Cracked.zip"

Size of the archive : 22.3MB

MD5 Hash : 18c309390a124c296b076ab54aaa1bd6

SHA256 Hash : 4b956a683fecda0454db6d6eb519a625e262b68c232dacfa1edef95f302e3797

VirusTotal Report : [unable to upload]

Detection : unable to upload

Unzipped archive : Password.txt : adrikadi

"Arkei Stealer 2025 Cracked..exe" [size :22.4MB]

VirusTotal report of "Arkei Stealer 2025 Cracked.exe" : unable to upload

Based on the icon, we can assume this is an .SFX archive. I've used the following online tool : <https://www.ezyzip.com/> , to get a look at the content (with the password provided in the .txt file), and they are similar to another .SFX file shared by the same member. We can find the same SFX script that will run every .vbs and .exe files :

acledit.bat
pnpuibat
rasdiag.bat
xpssvcs.bat
Arkei Stealer.exe
conhost.exe
crack.exe
sass.exe
svchost.exe
nhac.vbs
pots.vbs
rundll32.vbs
zipfldr.vbs

Here is the thread about the .SFX file I've already conducted a malware analysis on : <https://hackforums.net/showthread.php?tid=6298353>

I'll not do the same thing here, feel free to check the previous thread for this part.

Now we'll focus on the Arkei Stealer.exe file :

Size of the file : 2.4MB

MD5 Hash : 7692c4d6193386adfcf6f391764c64f3

SHA256 Hash : 71c316924f3821c63cba855b72a6f1e603890b114f7e1c9171b0583daf557ffb

VirusTotal Report :

<https://www.virustotal.com/gui/file/71c316924f3821c63cba855b72a6f1e603890b114f7e1c9171b0583daf557ffb/detection>

Old Detection : 54/68

i Last time this file has been analyzed was 2 years ago, I'm running a new analyze. It's a good practice when you use VirusTotal, between in the meantime AV engines have probably been improved.

New Detection : 56/72

Running it through TRIA.GE : <https://tria.ge/250518-p9sm8sdq5z> , the file is flagged as Quasar RAT. As we can see below, Arkei Stealer drops 2 files : "build1.exe", which creates a task "driver.exe", which also creates a task

As there not seem to be downloads from external sources, these executables have probably been embedded in the main executable. Taking a look at the file with PE-Bear we can see it has been protected with VMProtect, which can obfuscate code, add anti-debug, anti-dump, anti-VM protections. This software is often used for malware because it can hide malicious payload (such as here), make the analysis harder, or bypass antivirus and sandboxes.

.vmp sections are related to VMProtect :

I've been able to retrieve build1.exe and driver.exe and they seem to be the same file, not sure why they have different names, here is the VirusTotal Report :

<https://www.virustotal.com/gui/file/2288da6767af6f614225e8c4694f7e07c83df7a2b53a222506cdd37d330f5520?nocache=1> . The location of the files are different, maybe as a "redundancy".

The C2 server seems down now, besides "Arkei Stealer" does nothing when executed, it's just used to lure people.

We can see in Ghidra that there are many namespaces related to xClient, which is associated to Quasar and its forks :

GOLLUM - May 18, 2025, 8:08 am

thanks for the analysis

Bastille - May 18, 2025, 8:10 am

(May 18, 2025 08:08 AM)GOLLUM Wrote: [\[CITE\]](#) thanks for the analysis

You're welcome, always glad to remove infected links on the forum to protect members; feel free to report any suspicious link.

Besides, it provides content for people who want to learn malware analysis.

GOLLUM - *May 18, 2025, 8:11 am*

(May 18, 2025 08:10 AM) Bastille Wrote: [\[CITE\]](#) You're welcome, always glad to remove infected links on the forum to protect members; feel free to report any suspicious link.

Besides, it provides content for people who want to learn malware analysis.

will be glad to learn