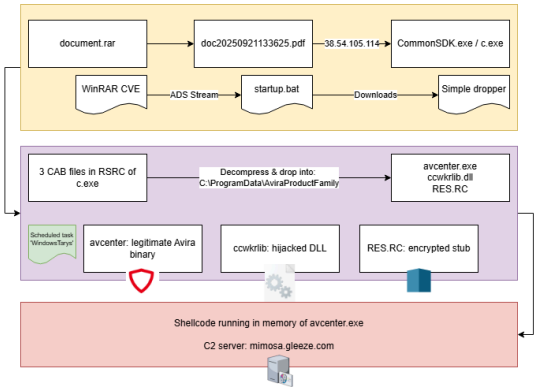
Earth Estries alive and kicking

Earth Estries, also known as Salt Typhoon and a few other names, is a China-nexus APT actor, and is known to have used multiple implants such as Snappybee (Deed RAT), ShadowPad, and several more.

In their latest campaign, the actor leverages one of the latest WinRAR vulnerabilities that will ultimately lead to running shellcode.

The execution flow is as follows:



That is all. Find below indicators of compromise and Yara rules.

Indicator	Type	Purpose
f8c119bfc057dc027e6c54b966d168ee1ef38c790e581fb44cf965ca0408db1d	SHA256 Hash	CAB file storing ccwkrlib.dll
94aa6619c61d434e96ca8d128731eb7ee81e399a59a17f751a31b564a7f3a722	SHA256 Hash	Encrypted stub
3c84a5255e0c08e96278dea9021e52c276b4a6c73af9fa81520aefb4a8040a8b	SHA256 Hash	CAB file storing RES.RC
3822207529127eb7bdf2abc41073f6bbe4cd6e9b95d78b6d7dd04f42d643d2c3	SHA256 Hash	Dropper
64ca55137ba9fc5d005304bea5adf804b045ec10c940f6c633ffde43bc36ff3f	SHA256 Hash	Fake PDF with ADS stream
6c6af015e0bfec69f7867f8c957958aa25a13443df1de26fa88d56a240bdd5ad	SHA256 Hash	Hijacked DLL, bloated
5e062fee5b8ff41b7dd0824f0b93467359ad849ecf47312e62c9501b4096ccda	SHA256 Hash	Hijacked DLL
3b47df790abb4eb3ac570b50bf96bb1943d4b46851430ebf3fc36f645061491b	SHA256 Hash	Downloads CommonSDK.exe
ccwkrlib.dll	Filename	Hijacked DLL
RES.RC	Filename	Encrypted stub
CommonSDK.exe	Filename	Fake PDF with ADS stream

doc20250921133625.pdf	Filename	Fake PDF with ADS stream
startup.bat	Filename	Downloads CommonSDK.exe
WindowsTarys	Filename	Scheduled task
38[.]54[.]105[.]114	IP Address	Download server
mimosa[.]gleeze[.]com	Domain	C2 Server

Associated Yara rules are available on my Github:

https://github.com/bartblaze/Yara-rules

Rule names:

- EE_Loader
- EE_Dropper
- WinRAR_ADS_Traversal

References / Resources:

WinRAR CVE:

https://nvd.nist.gov/vuln/detail/CVE-2025-8088

https://www.welivesecurity.com/en/eset-research/update-winrar-tools-now-romcom-and-others-exploiting-zero-day-vulnerability/

Earth Estries:

https://jsac.jpcert.or.jp/archive/2025/pdf/JSAC2025_1_5_leon-chang_theo-chen_en.pdf

https://www.trendmicro.com/en_us/research/25/j/premier-pass-as-a-service.html

https://malpedia.caad.fkie.fraunhofer.de/actor/earth_estries

https://malpedia.caad.fkie.fraunhofer.de/actor/ghostemperor