

Speculoos (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 15:45:50 UTC

elf.speculoos ([Back to overview](#))

Speculoos

Actor(s): [APT17](#)

There is no description at this point.

References

2020-04-13 · [Palo Alto Networks Unit 42](#) · [Bryan Lee](#), [Jen Miller-Osborn](#), [Robert Falcone](#)
APT41 Using New Speculoos Backdoor to Target Organizations Globally
[Speculoos APT41](#)

2020-03-25 · [FireEye](#) · [Christopher Glycer](#), [Dan Perez](#), [Sarah Jones](#), [Steve Miller](#)
This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits
[Speculoos Cobalt Strike](#)

2020-01-01 · [Secureworks](#) · [SecureWorks](#)
BRONZE ATLAS
[Speculoos Winnti ACEHASH CCleaner Backdoor CHINACHOPPER Empire Downloader HTran MimiKatz PlugX Winnti APT41](#)

There is no Yara-Signature yet.

Source: <https://malpedia.caad.fkie.fraunhofer.de/details/elf.speculoos>