crackshot (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 20:42:36 UTC

crackshot

Actor(s): APT41

CRACKSHOT is a downloader that can download files, including binaries, and run them from the hard disk or execute them directly in memory. It is also capable of placing itself into a dormant state.

References

Yara Rules

▶ [TLP:WHITE] win_crackshot_w0 (20190812 | Detects APT41 malware CRACKSHOT)

Download all Yara Rules

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.crackshot