VBREVSHELL (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 14:53:54 UTC

vbs.vbrevshell (Back to overview)

VBREVSHELL

According to Mandiant, VBREVSHELL is a VBA macro that spawns a reverse shell relying exclusively on Windows API calls.

References

2023-12-02 · openhunting.io · openhunting.io
Threat Hunting Malware Infrastructure
VBREVSHELL AsyncRAT

2022-12-12 · SOCRadar · SOCRadar
Dark Web Profile: APT42 – Iranian Cyber Espionage Group
PINEFLOWER VINETHORN VBREVSHELL BROKEYOLK CHAIRSMACK DOSTEALER GHAMBAR SILENTUPLOADER TAG-56

2022-09-07 · Mandiant · Mandiant Intelligence
APT42: Crooked Charms, Cons and Compromises
PINEFLOWER VINETHORN VBREVSHELL BROKEYOLK DOSTEALER GHAMBAR SILENTUPLOADER

There is no Yara-Signature yet.
