BROKEYOLK (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 21:37:07 UTC

win.brokeyolk (Back to overview)

BROKEYOLK

According to Mandiant, BROKEYOLK is a .NET downloader that downloads and executes a file from a hard-coded command and control (C2) server. The malware communicates via SOAP (Simple Object Access Protocol) requests using HTTP.

References

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.
