GHAMBAR (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 14:36:23 UTC

win.ghambar (Back to overview)

GHAMBAR

According to Mandiant, GHAMBAR is a remote administration tool (RAT) that communicates with its C2 server using SOAP requests over HTTP. Its capabilities include filesystem manipulation, file upload and download, shell command execution, keylogging, screen capture, clipboard monitoring, and additional plugin execution.

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.
