JUMPALL (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 14:04:34 UTC

win.jumpall (Back to overview)

JUMPALL

Actor(s): APT41

According to FireEye, JUMPALL is a malware dropper that has been observed dropping HIGHNOON/ZXSHELL/SOGU.

References

2019-08-09 · FireEye · FireEye
Double Dragon APT41, a dual espionage and cyber crime operation
CLASSFON crackshot CROSSWALK GEARSHIFT HIGHNOON HIGHNOON.BIN JUMPALL POISONPLUG Winnti

There is no Yara-Signature yet.
