DropBook (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 12:42:41 UTC

win.dropbook (Back to overview)

DropBook

Actor(s): Molerats

DropBook is a backdoor developed by the Molerats group and first appeared in late 2020. The backdoor abuses Facebook and Dropbox platforms for C2 purposes, where fake Facebook accounts are used by the operators to control the backdoor by posting commands on the accounts.

References

2020-12-09 · Cybereason · Cybereason Nocturnus
New Malware Arsenal Abusing Cloud Platforms in Middle East Espionage Campaign
DropBook MoleNet Quasar RAT SharpStage Spark

2020-12-09 · Cybereason · Cybereason Nocturnus Team
MOLERATS IN THE CLOUD: New Malware Arsenal Abuses Cloud Platforms in Middle East Espionage Campaign
DropBook JhoneRAT Molerat Loader Pierogi Quasar RAT SharpStage Spark

There is no Yara-Signature yet.
