JhoneRAT (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 17:21:18 UTC

win.jhone_rat (Back to overview)

JhoneRAT

Cisco Talos identified JhoneRAT in January 2020. The RAT is delivered through cloud services (Google Drive) and also submits stolen data to them (Google Drive, Twitter, ImgBB, GoogleForms). The actors using JhoneRAT target Saudi Arabia, Iraq, Egypt, Libya, Algeria, Morocco, Tunisia, Oman, Yemen, Syria, UAE, Kuwait, Bahrain and Lebanon.

References

2020-12-21 · Cisco Talos · JON MUNSHAW
2020: The year in malware
WolfRAT Prometei Poet RAT Agent Tesla Astaroth Ave Maria CRAT Emotet Gozi IndigoDrop JhoneRAT Nanocore RAT NjRAT Oblique RAT SmokeLoader StrongPity WastedLocker Zloader

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

2020-03-03 · Palo Alto Networks Unit 42 · Alex Hinchliffe, Bryan Lee, Robert Falcone
Molerats Delivers Spark Backdoor to Government and Telecommunications Organizations
Downeks JhoneRAT Molerat Loader Spark

2020-01-16 · Cisco Talos · Eric Kuhla, Paul Rascagnères, Vitor Ventura, Warren Mercer
JhoneRAT: Cloud based python RAT targeting Middle Eastern countries
JhoneRAT

There is no Yara-Signature yet.
