MoqHao (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 17:52:07 UTC

MoqHao

aka: Shaoye, Wroba, XLoader

Actor(s): Yanbian Gang

MoqHao, also called Wroba and XLoader (not to be confused with the malware of the same name for Windows and macOS), is an Android-based mobile threat that is associated with a financially motivated Chinese group called Roaming Mantis. The malware claims to be the default SMS application and has dropper and banker capabilities.

References

2023-03-31 · Telekom ·
Moqhao masters new tricks
MoqHao

2023-03-16 · Team Cymru · S2 Research Team
MoqHao Part 3: Recent Global Targeting Trends
MoqHao

2023-01-19 · Kaspersky Labs · GReAT
Roaming Mantis implements new DNS changer in its malicious mobile app in 2022
MoqHao

2022-08-11 · xanhacks' infosec blog · xanhacks
MoqHao Android malware analysis and phishing campaign
MoqHao

2022-07-18 · Sekoia · Quentin Bourgue, Threat & Detection Research Team
Ongoing Roaming Mantis smishing campaign targeting France
MoqHao

2022-04-12 · Broadcom · Broadcom
MoqHao malware continues to target mobile users in Europe
MoqHao

2022-04-07 · Team Cymru · Josh Hopkins
MoqHao Part 2: Continued European Expansion
MoqHao

2021-08-11 · Team Cymru · Josh Hopkins
MoqHao Part 1.5: High-Level Trends of Recent Campaigns Targeting Japan
MoqHao

2021-05-18 · Medium (Cryptax) · Axelle Apvrille
A native packer for Android/MoqHao
MoqHao

2021-05-05 · Kashif Ali Surfeit and Blasé Security · Kashif Ali
Roaming Mantis Amplifies Smishing Campaign with OS-Specific Android Malware
MoqHao Roaming Mantis

2021-01-20 · Team Cymru · Andy Kraus
MoqHao Part 1: Identifying Phishing Infrastructure
MoqHao

2020-06-25 · Medium CSIS Techblog · Aleksejs Kuprins
The RoamingMantis Group’s Expansion to European Apple Accounts and Android Devices
FakeSpy FunkyBot MoqHao

2020-02-27 · Kaspersky Labs · Suguru Ishimaru
Roaming Mantis, part V: Distributed in 2019 using SMiShing and enhanced anti-researcher techniques
FunkyBot MoqHao Roaming Mantis

2020-01-17 · Hiroaki Ogawa, Manabu Niseki
100 more behind cockroaches?
MoqHao Emotet Predator The Thief

2019-01-01 · Kaspersky Labs · Hiroaki Ogawa, Manabu Niseki, Suguru Ishimaru
Roaming Mantis: an Anatomy of a DNS Hijacking Campaign
MoqHao Roaming Mantis

2018-11-26 · Trend Micro · Ecular Xu, Lorin Wu
Examining XLoader, FakeSpy, and the Yanbian Gang
FakeSpy MoqHao Yanbian Gang

2018-11-26 · Trend Micro · Ecular Xu, Lorin Wu
A Look into the Connection Between XLoader and FakeSpy, and Their Possible Ties With the Yanbian Gang
FakeSpy MoqHao

2018-04-20 · Trend Micro · Trend Micro

XLoader Android Spyware and Banking Trojan Distributed via DNS Spoofing

MoqHao Yanbian Gang

There is no Yara-Signature yet.
