# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:13:50 UTC



## Tool: Roaming Mantis

| | |
|---|---|
| Names | Roaming Mantis<br>MoqHao<br>XLoader<br>Wroba |
| Category | Malware |
| Type | Banking trojan, Info stealer, Miner |
| Description | (Kaspersky) The Roaming Mantis mobile banking trojan is roaming further afield than it ever has before. Recent analysis shows that the malware has rapidly evolved just in the past month. It's now targeting Europe and the Middle East in addition to Asian countries. According to researchers, it's following the cyber-zeitgeist by expanding its capabilities to include cryptomining (and iOS phishing).<br><br>Roaming Mantis is a mostly-mobile malware which this year has been spreading via DNS hijacking. Potential victims are typically redirected to a malicious webpage that distributes a trojanized application that pretends to be either Facebook or Chrome. Once installed manually by users, a trojan banker will execute. |
| Information | <https://threatpost.com/roaming-mantis-swarms-globally-spawning-ios-phishing-cryptomining/132149/><br><https://blog.trendmicro.com/trendlabs-security-intelligence/xloader-android-spyware-and-banking-trojan-distributed-via-dns-spoofing/><br><https://blog.trendmicro.com/trendlabs-security-intelligence/a-look-into-the-connection-between-xloader-and-fakespy-and-their-possible-ties-with-the-yanbian-gang/><br><https://research.checkpoint.com/2021/top-prevalent-malware-with-a-thousand-campaigns-migrates-to-macos/><br><https://blog.malwarebytes.com/mac/2021/07/osx-xloader-hides-little-except-its-main-purpose-what-we-learned-in-the-installation-process/><br><https://securelist.com/roaming-mantis-reaches-europe/105596/><br><https://securelist.com/roaming-mantis-dns-changer-in-malicious-mobile-app/108464/><br><https://www.mcafee.com/blogs/other-blogs/mcafee-labs/moqhao-evolution-new-variants-start-automatically-right-after-installation/> |

| | |
|---|---|
| MITRE ATT&CK | <https://attack.mitre.org/software/S0318/> |
| Malpedia | <https://malpedia.caad.fkie.fraunhofer.de/details/apk.roaming_mantis><br><https://malpedia.caad.fkie.fraunhofer.de/details/apk.moqhao><br><https://malpedia.caad.fkie.fraunhofer.de/details/apk.xloader> |
| AlienVault OTX | <https://otx.alienvault.com/browse/pulses?q=tag:Roaming%20Mantis> |

Last change to this tool card: 06 March 2024

Download this tool card in JSON format

### All groups using tool Roaming Mantis

| Changed | Name | Country | Observed | |
|---|---|---|---|---|
| **Other groups** | | | | |
| | Roaming Mantis | [Unknown] | 2017-Jul 2022 | |

*1 group listed (0 APT, 1 other, 0 unknown)*

---

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=aa243282-d977-4d61-81a2-b81c17ac47f3