Roaming Mantis - Threat Group Cards: A Threat Actor Encyclopedia

Other threat group: Roaming Mantis

Names	Roaming Mantis *(Kaspersky)* Roaming Mantis Group *(Kaspersky)* Shaoye *(?)*
Country	[Unknown]
Motivation	Financial crime
First seen	2017
Description	(Kaspersky) In March 2018, Japanese media reported the hijacking of DNS settings on routers located in Japan, redirecting users to malicious IP addresses. The redirection led to the installation of Trojanized applications named facebook.apk and chrome.apk that contained Android Trojan-Banker. According to our telemetry data, this malware was detected more than 6,000 times, though the reports came from just 150 unique users (from February 9 to April 9, 2018). Of course, this is down to the nature of the malware distribution, but it also suggests a very painful experience for some users, who saw the same malware appear again and again in their network. More than half of the detections were observed targeting the Asian region. During our research we received some invaluable information about the true scale of this attack. There were thousands of daily connections to the command and control (C2) infrastructure, with the device locale for the majority of victims set to Korean. Since we didn't find a pre-existing name for this malware operation, we decided to assign a new one for future reference. Based on its propagation via smartphones roaming between Wi-Fi networks, potentially carrying and spreading the infection, we decided to call it 'Roaming Mantis'.
Observed	Countries: Azerbaijan, Bangladesh, Brazil, Cambodia, Canada, China, Denmark, Finland, France, Germany, Hong Kong, India, Indonesia, Iran, Ireland, Italy, Japan, Kazakhstan, Netherlands, Russia, Saudi Arabia, South Korea, Sri Lanka, Sweden, Switzerland, Taiwan, Thailand, Turkey, UK, USA, Vietnam.

Tools used	Roaming Mantis, SmsSpy.	
Operations performed	Feb 2018	Roaming Mantis malware is designed for distribution through a simple, but very efficient trick based on a technique known as DNS hijacking. When a user attempts to access any website via a compromised router, they will be redirected to a malicious website. <https://securelist.com/roaming-mantis-uses-dns-hijacking-to-infect-android-smartphones/85178/>
	May 2018	In May, while monitoring Roaming Mantis, aka MoqHao and XLoader, we observed significant changes in their M.O. The group's activity expanded geographically and they broadened their attack/evasion methods. Their landing pages and malicious apk files now support 27 languages covering Europe and the Middle East. In addition, the criminals added a phishing option for iOS devices, and crypto-mining capabilities for the PC. <https://securelist.com/roaming-mantis-dabbles-in-mining-and-phishing-multilingually/85607/>
	Sep 2018	In addition, they have started using web crypto-mining for PC, and an Apple phishing page for iOS devices. <https://securelist.com/roaming-mantis-part-3/88071/>
	Feb 2019	According to our detection data, new variants of sagawa.apk Type A (Trojan-Dropper.AndroidOS.Wroba.g) have been detected in the wild, based on our KSN data from February 25, 2019 to March 20, 2019. <https://securelist.com/roaming-mantis-part-iv/90332/>
	Jun 2019	Roaming Mantis: a new phishing method targets a Japanese MNO <https://hackmd.io/@ninoseki/Bkw66OhAN>
	Aug 2019	The McAfee mobile research team has found a new type of Android malware for the MoqHao phishing campaign (a.k.a. XLoader and Roaming Mantis) targeting Korean and Japanese users. A series of attack campaigns are still active, mainly targeting Japanese users. The new spyware has very different payloads from the existing MoqHao samples. <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/moqhao-related-android-spyware-targeting-japan-and-korea-found-on-google-play/>
	Feb 2020	The group's attack methods have improved and new targets continuously added in order to steal more funds. The attackers' focus has also shifted to techniques that avoid tracking and research:

		whitelist for distribution, analysis environment detection and so on. <https://securelist.com/roaming-mantis-part-v/96250/>
	Jun 2020	The RoamingMantis Group's Expansion to European Apple Accounts and Android Devices <https://medium.com/csis-techblog/the-roamingmantis-groups-expansion-to-european-apple-accounts-and-android-devices-e6381723c681>
	Jan 2021	Roaming Mantis Amplifies Smishing Campaign with OS-Specific Android Malware <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/roaming-mantis-amplifies-smishing-campaign-with-os-specific-android-malware/>
	2021	Roaming Mantis reaches Europe <https://securelist.com/roaming-mantis-reaches-europe/105596/>
	2022	Roaming Mantis implements new DNS changer in its malicious mobile app in 2022 <https://securelist.com/roaming-mantis-dns-changer-in-malicious-mobile-app/108464/>
	Jul 2022	Ongoing Roaming Mantis smishing campaign targeting France <https://blog.sekoia.io/ongoing-roaming-mantis-smishing-campaign-targeting-france/>
Information	<https://www.kaspersky.com/blog/roaming-mantis-malware/22427/> <https://blog.trendmicro.com/trendlabs-security-intelligence/new-version-of-xloader-that-disguises-as-android-apps-and-an-ios-profile-holds-new-links-to-fakespy/> <https://blog.threatstop.com/over-120-malicious-domains-discovered-in-analysis-on-new-roaming-mantis-campaign>	

Last change to this card: 15 February 2023

Download this actor card in PDF or JSON format
