Roaming Mantis Swarms Globally, Spawning iOS Phishing, Cryptomining

By Tara Seals

Published: 2018-05-21 · Archived: 2026-04-05 18:48:21 UTC

Analysis shows that the malware, previously a banking trojan focused on Android devices, has rapidly evolved just in the past month.

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).

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.

Its sights have become much wider, however.

"Roaming Mantis has evolved quickly," said Kaspersky Lab researcher Suguru Ishimaru, in an analysis posted on Friday. "The actors behind it have been quite active in improving their tools. The rapid growth of the campaign implies that those behind it have a strong financial motivation and are probably well-funded."

Global Infections

On the multilingual front, Roaming Mantis (a.k.a. MoqHao or XLoader) was seen this month to have significantly tweaked its landing pages and malicious APK files to support 27 languages – a serious expansion from the four languages it used in campaigns just a month ago.

In campaigns observed in April, its activity was located mostly in Bangladesh, Japan and South Korea, according to Ishimaru. Kaspersky Lab has now confirmed that several more languages have been hardcoded in the HTML source of the landing page.

These include; Arabic, Armenian, Bulgarian, Bengali, both traditional and simplified Chinese, Czech, English, Georgian, German, Hebrew, Hindi, Indonesian, Italian, Japanese, Korean, Malay, Polish, Portuguese, Russian, Serbo-Croatian, Spanish, Tagalog, Thai, Turkish, Ukrainian and Vietnamese.

The expansion is succeeding in terms of garnering more victims: "We believe the attacker made use of an easy method to potentially infect more users, by translating their initial set of languages with an automatic translator," Ishimaru said. "It's clear from [our data] that South Korea, Bangladesh and Japan are no longer the worst affected countries; instead, Russia, Ukraine and India [bear] the brunt."

New Targets and Tactics

In addition to broadening its target range, an analysis of the Roaming Mantis code reveals the criminals behind the malware have added a phishing option that targets iOS device users and a cryptomining option targeting PCs. This is a departure from the group's primary focus on the Android platform, researchers said.

"When a user connects to the landing page via iOS devices, the user is redirected to 'http://security.apple[dot]com/'," Ishimaru explained. "A legitimate DNS server wouldn't be able to resolve a domain name like that, because it simply doesn't exist. However, a user connecting via a compromised router can access the landing page because the rogue DNS service resolves this domain to the IP address 172[.]247[.]116[.]155. The final page is a phishing page mimicking the Apple website with the very reassuring domain name 'security.apple[dot]com' in the address bar of the browser."

The phishing site steals user IDs, passwords, card numbers, card expiration dates and CVVs. Here is where researchers said the HTML source of the phishing site supported 25 languages. Notably, the languages Bengali and Georgian are missing from the phishing site.

Meanwhile, the perpetrators have added a new feature such as web mining via a the CoinHive script executed in the browser. "When a user connects to the landing page from a PC, the CPU usage will drastically increase because of the cryptomining activity in the browser," Ishimaru said.

Better Evasion Techniques

"The evasion techniques used by Roaming Mantis have also become more sophisticated. Several examples of recent additions described in [the Kaspersky Lab post] include a new method of retrieving the C2 by using the email POP protocol, server-side dynamic auto-generation of changing APK file names, and the inclusion of an additional command to potentially assist in identifying research environments," researchers wrote.

The dynamic auto-generation helps avoid blacklisting, they said.

"Aside from the filename, we also observed that all the downloaded malicious APK files are unique due to package generation in real time as of May 16, 2018," explained Ishimaru. "It seems the actor added automatic generation of APK per download to avoid blacklisting by file hashes. This is a new feature."

Meanwhile, older Roaming Mantis samples connected to the C2 by accessing a "legitimate website, extracting a Chinese string from a specific part of the HTML code, and decoding it," said the researcher. In the most recent sample, instead of using HTML protocol, Roaming Mantis uses email protocol to retrieve the C2.

"The malware connects to an email inbox using hardcoded outlook.com credentials via POP3," Ishimaru said. "It then obtains the email subject (in Chinese) and extracts the real C2 address using the string 'abcd' as an anchor."

Also, the previous malicious APK from April "had 18 backdoor commands to confirm victims' environments and to control devices." It's now added a feature that calls the OS ping command with the IP address of the C2 server.

"By running this, the attackers validate the availability of the server, packet travel time or detect network filtering in the target network," he said. "This feature can also be used to detect semi-isolated research environments."

In August 2017, McAfee first identified and reported the existence of Roaming Mantis. At that time, the distribution method was SMS and South Korea was its only target. “[By] April 2018, it had already implemented DNS hijacking and expanded its targets to the wider Asian region,” Ishimaru said.

This latest expansion indicates that the actors behind the malware have no intention of slowing down their attack rate.
