TRIAL and ERROR: Kaspersky Lab unearths iOS cryptomining attacks, careless mistakes by Roaming Mantis

Just five months after Kaspersky Lab's first report on the DNS hijacking operation to infect Android smartphones in Asia, the attack dubbed 'Roaming Mantis' remains highly active, exploring new tricks and techniques to extend its reach.

Close monitoring by Kaspersky Lab experts discovered Roaming Mantis attempting to web mine iOS devices used for legitimate cryptomining. The malware banked on the popular CoinHive miner, the tool it first used to infect PCs.
Malicious cryptocurrency mining refers to hackers infecting a cryptomining platform to mine cryptocurrency from unaware victims.

"In our first report, we warned that Roaming Mantis is clearly designed to attack and reach more users. True to its name, it has been extending its malicious arms rapidly since April, in terms of its location and attack and evasion methods. From infecting Android devices, it engaged in phishing activities and is now trying to mine iOS gadgets used for cryptomining. From the initial four languages in Asia, this malware is now using a further 27, covering Europe and the Middle East. We are pretty much looking at cybercriminals who show no traces of stopping anytime soon," warns Suguru Ishimaru, security researcher at Kaspersky Lab's Global Research and Analysis Team (GReAT) Asia Pacific.

Researchers also noticed that the hackers have adopted a trial and error approach to testing which technique would get them more money faster. For instance, the attacker modified the infected landing page of the malware, alternately using an Apple phishing site and a web coin-mining page.

Roaming Mantis has also boosted its attack and evasion tools. The group initially hijacked DNS systems of rogue Wi-Fi routers to infect Android users in Japan, Korea, India, and Bangladesh with Trojanized applications named facebook.apk and chrome.apk.

The latest updates reveal that facebook.apk has been changed to sagawa.apk and has been spread via a rented SMS message spoofing delivery service. This technique was first used last year by another cybergang.

Kaspersky Lab also uncovered that the attacker spreads its malware via Prezi, cloud-based presentation software that allows free user accounts, making it harder for security products to detect phishing or malicious activities as this site is considered legitimate. In addition, the redirected SCAM content shows that Roaming Mantis uses templates, which suggests that Prezi is an established delivery system for malicious content, too.

Aside from the updated tools and techniques, researchers at Kaspersky Lab spotted careless mistakes committed by the hacking group as they try to dabble in additional types of attacks as fast as possible.

Roaming Mantis, also known as MoqHao and XLoader, was launched in four languages and in two

months quickly added two dozen more, including Asian languages — Bengali, both traditional and simplified Chinese, Hindi, Indonesian, Japanese, Korean, Malay, Tagalog, Thai, and Vietnamese.

After this update, researchers detected mixed-ups in the language environment. For instance, Japanese users will get a pop-up message written in Korean.

The group also used HTML instead of URL to redirect users to their malicious content, contrary to how Prezi as a delivery system really works. As a result, the tweaked landing page was not able to infect its target victims.

“The intense financial motivation of this group is undoubtedly fueling it to try different attack and evasion tricks to widen its reach in a short period of time. In its haste to jump on different platforms, languages, and territories, Roaming Mantis is leaving crumbs of clues that guide us in understanding and predicting its next moves. While this group seems rich in manpower, time, and resources, Kaspersky Lab researchers tracking the minutest details will continue to dig up further forensic information to keep track of their movements,” adds Ishimaru.

To protect your devices against Roaming Mantis attacks, Kaspersky Lab suggests users do the following:
• Check your router’s settings
• Change the default login and password for admin of your devices, especially when used in cryptomining
• Use robust security solutions for all your devices
• Do not allow “Install unknown apps”

Kaspersky Lab security solutions detect malware used by Roaming Mantis as HEUR: Trojan-Banker and AndroidOS.Wroba.e and HEUR: Trojan-Banker and AndroidOS.Wroba.al.