Roaming Mantis infects smartphones through Wi-Fi routers

By Alex Drozhzhin

Published: 2018-05-18 · Archived: 2026-04-06 00:57:57 UTC

Some time ago our experts investigated a piece of malware that they dubbed Roaming Mantis. Back then, the people affected were mainly users from Japan, Korea, China, India, and Bangladesh, so we didn't discuss the malware in the context of other regions; it seemed to be a local threat.

However, in the month since the report was published, Roaming Mantis has added two dozen more languages and is rapidly spreading around the world.

The malware uses compromised routers to infect Android-based smartphones and tablets. It then redirects iOS devices to a phishing site and runs the CoinHive cryptomining script on desktops and laptops. It does so by means of DNS hijacking, making it hard for targeted users to detect that something's amiss.

What is DNS hijacking

When you enter a site name in your browser address bar, the browser doesn't actually send a request to that site. It can't; the Internet operates on IP addresses, which are sets of numbers, whereas domain names with words are easier for people to remember and input.

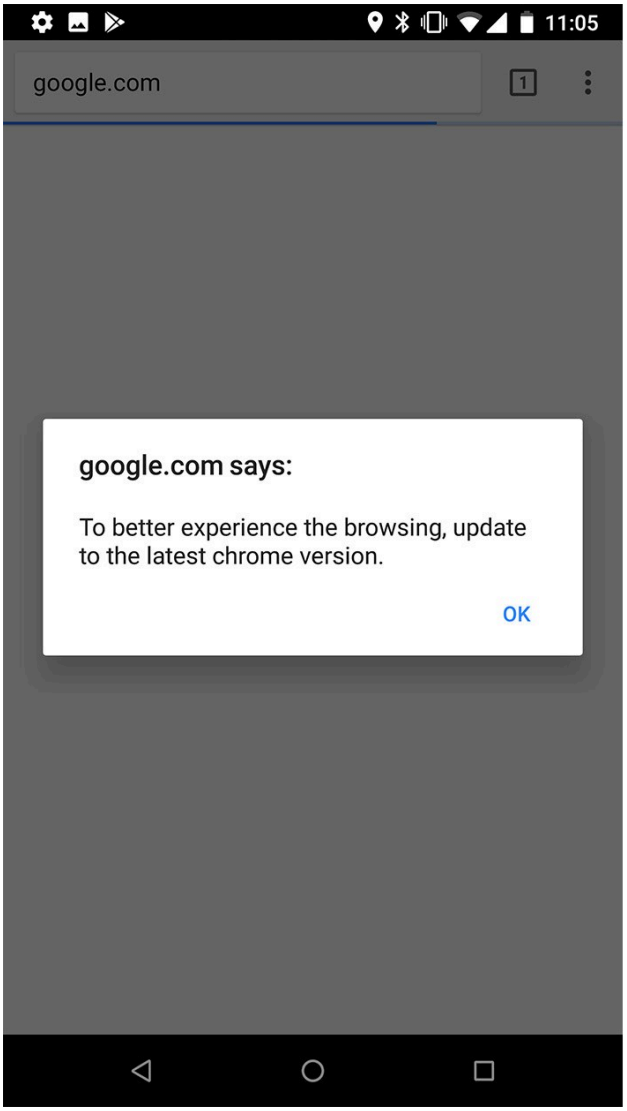
When you enter a URL, your browser sends a request to a DNS-server (DNS is Domain Name System), which translates the human-friendly name into the IP address of the corresponding website. It is this IP address that the browser uses to locate and open the site.

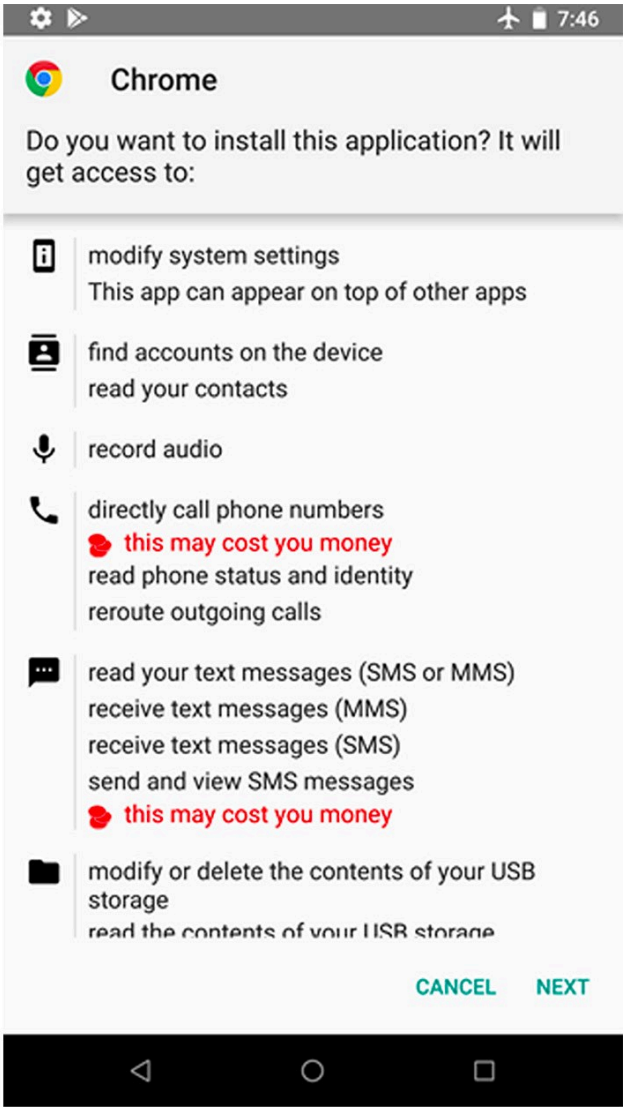
DNS hijacking is a way of fooling the browser into thinking it has matched the domain name to the correct IP address when in fact it hasn't. Although the IP address is wrong, the original URL entered by the user is displayed in the browser address bar, so nothing looks suspicious.

There are many DNS-hijacking techniques, but the creators of Roaming Mantis have chosen perhaps the simplest and most effective: They hijack the settings of compromised routers, forcing them to use their own rogue DNS servers. That means regardless of what is typed into the browser address bar of a device connected to this router, the user is redirected to a malicious site.

Roaming Mantis on Android

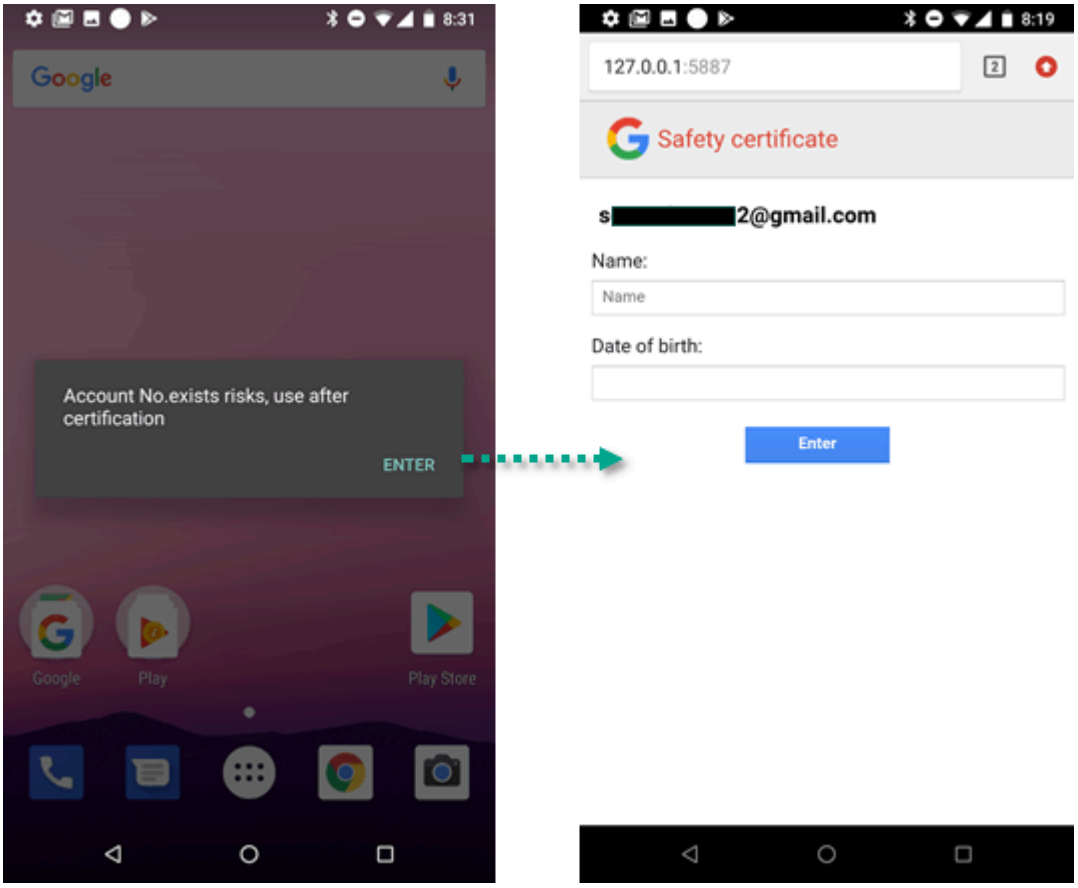
After the user is redirected to the malicious site, they are prompted to update the browser. That leads to the download of a malicious app named **chrome.apk** (there was another version as well, named **facebook.apk**).





The malware requests a bunch of permissions during the installation process, including rights to access account information, send and receive SMS messages, process voice calls, record audio, access files, display its own window on top of others, and so on. For a trusted application such as Google Chrome, the list doesn't seem too suspicious — if the user considers this "browser update" legit, they are sure to grant permissions without even reading the list.

After the application is installed, the malware uses the right to access the list of accounts to find out which Google account is used on the device. Next, the user is shown a message (it appears on top of all other open windows, another permission the malware requested) saying that something is wrong with their account and that they need to sign in again. A page then opens and prompts the user to enter their name and date of birth.



It appears that this data, together with the SMS permissions that grant access to the one-time codes needed for two-factor authentication, is then used by the creators of Roaming Mantis to steal Google accounts.

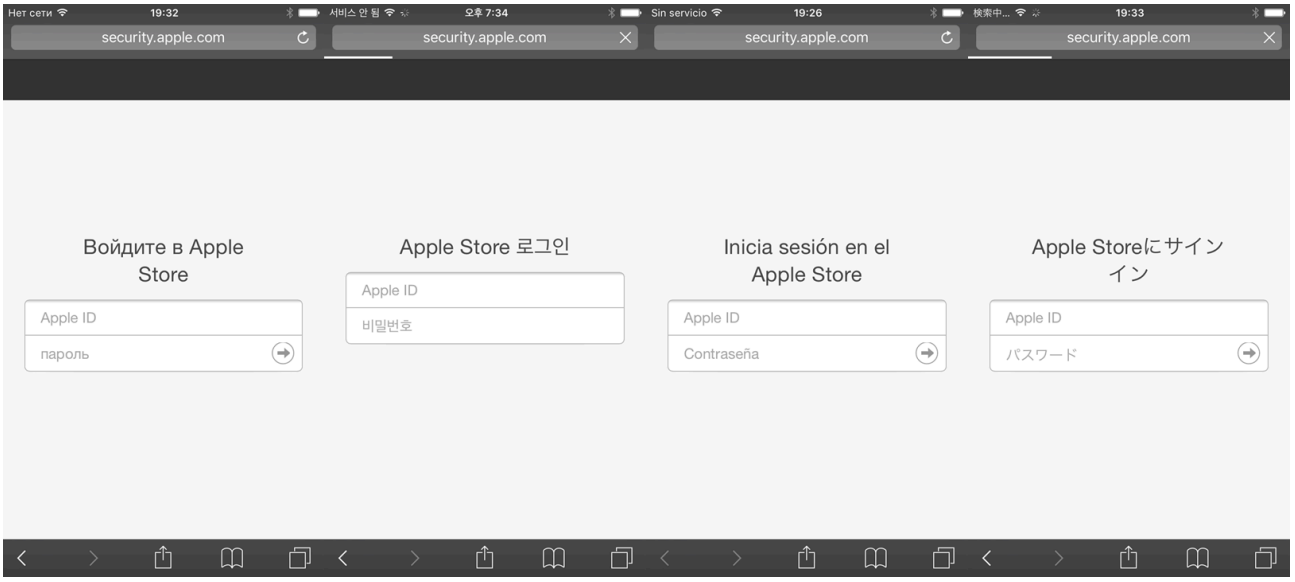
Roaming Mantis: World tour, iOS debut, and mining

In the beginning, Roaming Mantis could display messages in four languages: English, Korean, Chinese, and Japanese. But somewhere along the line, its creators decided to expand and add another two dozen languages to their polyglot malware:

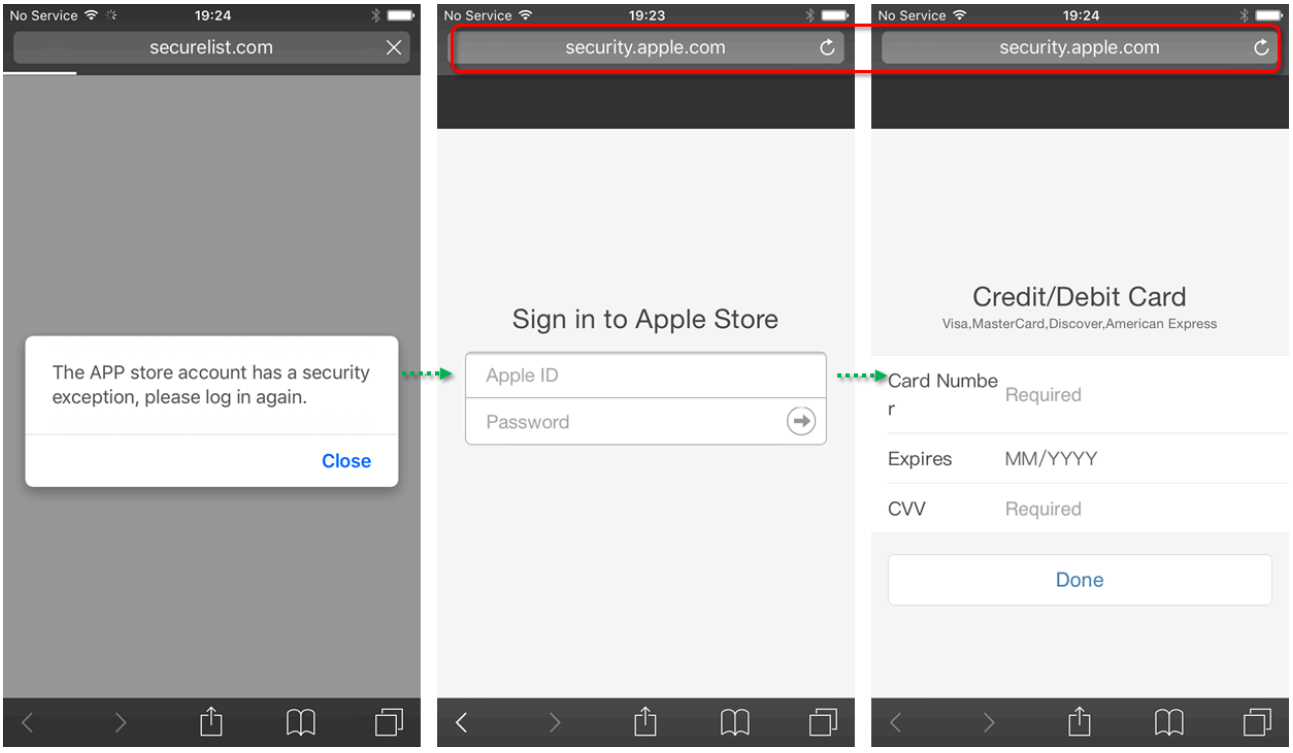
- Arabic
- Armenian
- Bulgarian
- Bengali
- Czech
- Georgian
- German
- Hebrew
- Hindi
- Indonesian
- Italian
- Malay
- Polish
- Portuguese

- Russian
- Serbo-Croat
- Spanish
- Tagalog
- Thai
- Turkish
- Ukrainian
- Vietnamese

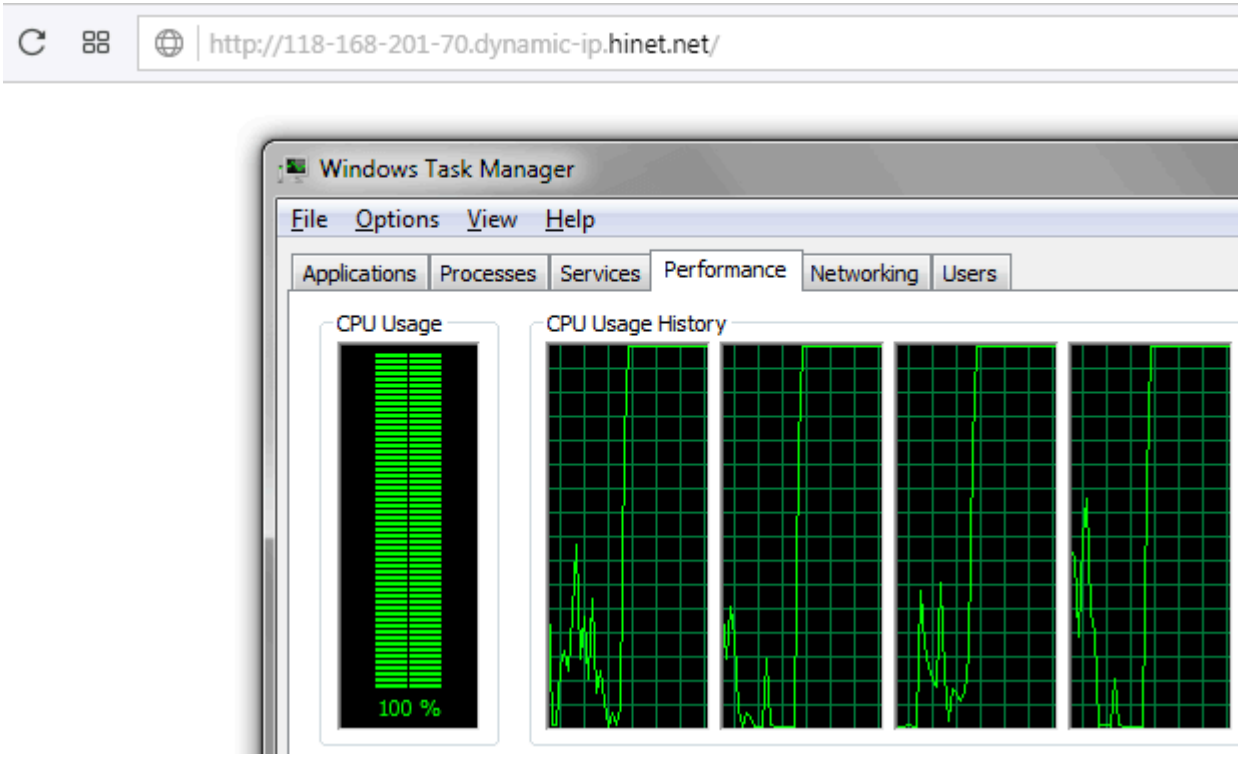
While they were at it, the creators also improved Roaming Mantis, teaching it to attack devices running iOS. It's a different scenario from the Android attacks. On iOS, Roaming Mantis skips downloading the application; instead, the malicious site displays a phishing page prompting the user to log back in to the App Store right away. To add credibility, the address bar shows the reassuring URL **security.apple.com**:



The cybercriminals do not confine their theft to Apple ID credentials; immediately after entering this data, the user is asked for a bank card number:



The third innovation our experts uncovered concerns desktop computers and laptops. On these devices, Roaming Mantis runs the CoinHive mining script, which mines cryptocurrency and dumps it straight into the pockets of the malware makers. The victim's computer processor is loaded to the max, forcing the system to slow down and consume vast amounts of power.



You can find more details about Roaming Mantis in the original report and a fresh Securelist post with updated information about the malware.

How to protect from Roaming Mantis

- Use antivirus protection on all devices: not just computers and laptops, but smartphones and tablets too.
- Regularly update all installed software on your devices.
- On Android devices, disable the installation of applications from unknown sources. You'll find this option under *Settings -> Security -> Unknown sources*.

- Update your router firmware (check your router's manual to find out how) as often as possible. Don't use unofficial firmware downloaded from shady sites.
- Always change the default administrator password on the router.

What to do if infected by Roaming Mantis

Kaspersky security products detect and remove Roaming Mantis, so your first step is to install antivirus on all of your devices and run a system scan. After you scrub Roaming Mantis from your computers and devices, you'll need to do a bit of cleanup to avoid reinfection:

- Change all passwords for accounts compromised by the malware. Cancel all bank cards for which you entered details on the Roaming Mantis phishing site.
- Change the router administrator password and update the firmware. In doing so, be sure to download it only from the official website of the router manufacturer.
- Navigate to your router's settings and check the DNS server address. If it doesn't match the one issued by your provider — you can find that on your ISP's website (check it from a safe system!) or call them to find out — change it back to the right one.

Source: https://www.kaspersky.com/blog/roaming-mantis-malware/22427/