Issued 7/10/17

CopyCat malware infected 14 million outdated Android devices

A new strain of a malware called CopyCat has infected more than 14 million Android devices around the world, rooting phones and hijacking apps to make millions in fraudulent ad revenue, researchers at Check Point said Thursday. While the majority of victims are in Asia, more than 280,000 Android devices in the US were hit by the massive hack. Google had been tracking the malware for the last two years and has updated Play Protect to block CopyCat, but millions of victims are getting hit through third-party app downloads and phishing attacks.

There was no evidence that CopyCat was distributed on Google Play, according to Check Point. "Play Protect secures users from the family, and any apps that may have been infected with CopyCat were not distributed via Play," Google said in a statement. Keeping true to its name, CopyCat pretends to be a popular app that people on third-party stores, like SimSimi, which had more than 50 million downloads on the Google Play store.

Once downloaded, it collects data about the infected device and downloads rootkits to help root the phone, essentially cutting off its security system. From there, CopyCat can download fake apps, as well as hijack your device's Zygote -- the launcher for every app on your phone. Once it has control of the Zygote, it knows every new app that you've downloaded, as

well as every app that you open. CopyCat is able to replace the Referrer ID on your apps with its own, so every ad that pops up on the app will send revenue to the hackers instead of the app's creators. Every now and then, CopyCat will also throw in its own ads for an extra buck.

There's been nearly 4.9 million fake apps installed on infected devices, displaying up to 100 million ads. In just two months, CopyCat helped hackers make more than $1.5 million, Check Point estimated. The malware also checks to see if the infected device is in China. Victims in China are spared from the cyberattack, and Check Point's researchers believe it's because the cybercriminals are Chinese and are trying to avoid any police investigations. While there hasn't been any direct evidence on who is behind the attack, there has been several connections between CopyCat and the Chinese ad network MobiSummer. The malware and the ad company operate on the same server, and several lines in the virus's code is signed by MobiSummer. The two also use the same remote services.

The majority of victims were in India, Pakistan, Bangladesh, Indonesia and Myanmar. More than 381,000 devices in Canada were infected with CopyCat. The mobile malware spread through five exploits that hit devices running Android 5.0 and earlier and had been discovered and patched more than two years ago. Android users on older devices are still vulnerable to the attack, if they're downloading apps off third-party markets.

The attack hit its highest number of victims between April and May of 2016 and has slowed down since Google blacklisted it on Play Protect, but Check Point believes infected devices could still be suffering from the malware.