Malicious apps infect 25 million Android devices with 'Agent Smith' malware

July 11 2019, by Cat Ferguson

Credit: CC0 Public Domain

Malicious apps from a campaign called "Agent Smith" have been downloaded to 25 million Android devices, according to new research by cyber-security firm Check Point.

The apps, most of them games, were distributed through third-party app stores by a Chinese group with a legitimate business helping Chinese developers promote their apps on outside platforms. Check Point is not identifying the company, because they are working with local law enforcement. About 300,000 devices were infected in the U.S.

The malware was able to copy popular apps on the phone, including WhatsApp and the web browser Opera, inject its own malicious code and replace the original app with the weaponized version, using a vulnerability in the way Google apps are updated. The hijacked apps would still work just fine, which hid the malware from users.

Armed with all the permissions users had granted to the real apps, "Agent Smith" was able to hijack other apps on the phone to display unwanted ads to users. That might not seem like a significant problem, but the same security flaws could be used to hijack banking, shopping and other sensitive apps, according to Aviran Hazum, head of Check Point's analysis and response team for mobile devices.

"Hypothetically, nothing is stopping them from targeting bank apps, changing the functionality to send your bank credentials" to a third party, Hazum said. "The user wouldn't be able to see any difference, but the attacker could connect to your bank account remotely."

The group also had 11 apps in the official Google Play store with a "dormant" version of "Agent Smith," which could have been triggered into action by a banner ad containing the keyword "infect." The apps, which have been removed from the Google Play store, had been downloaded over 10 million times.

It's important for users to understand that ads aren't always just ads, according to Dustin Childs, the communications manager for cybersecurity company Trend Micro's Zero Day Initiative, a so-called

'bug bounty' program that pays rewards to hackers and researchers who tip them off about software security flaws.

"We've seen malicious ads that can install apps when you browse to a webpage from your Android device. They could be installing ransomware, they could be copying your contacts," he said, referring to prior research. "Ad blockers aren't just to block ads."

Childs recommends Android users use ad blocker software, always update their devices when prompted, and only download apps from the Google Play Store.

"The app developer can do nothing to prevent this," said Hazum. "The fix has to come from the operating system."

Google already fixed at least one of the Android exploits used by "Agent Smith," nicknamed Janus, in 2017 but the fix hasn't made its way onto every Android phone. It's a potent reminder that millions of phones around the world are being used without the latest security measures.

"The sheer numbers infected by this campaign shows how many devices are not updated," Hazum said. "It takes quite a lot of time for an update to reach every phone."

A big part of the problem is how fragmented the Android ecosystem is, especially compared to the iPhone ecosystem, Childs said.

"Google is very good about releasing fixes for the vulnerabilities they know about, but getting it to all the devices is a very difficult problem."

Whenever Google issues a new security fix, or "patch," every device maker such as Samsung or LG has make sure all their own apps still work with the new system, which can take time. Manufacturers usually

stop offering security updates to phone models after a few years, or even a few months, a significant problem given how long people tend to keep smartphones.

If manufacturers push out an update for the device, all the carriers such as Verizon and AT&T then have to authorize the update.

The final step, of course, is getting people to actually update their phones.

"People see they have an update and know it will take their phone 30 minutes to download it, apply it, and restart the device," Hazum said. "A lot of people ignore it."

Whether or not users have updated security on their phones, one of the biggest risks to Android devices comes from third-party app stores, which aren't well-vetted, said Daniel Thomas, a research associate and lecturer at University of Cambridge.

Thomas was part of a research team that found 87% of Android devices in 2015 were using out-of-date versions of the operating system. The team's Android Vulnerabilities program distributes data about historical and current risks for the devices.

But iPhone users shouldn't get comfortable. Even though the Apple ecosystem is more controlled than Android, hackers have found plenty of ways to exploit devices using iOS, not to mention Apple is set to stop offering security updates to many iPhone models that are still widely used.

"In any large body of code, there will always be vulnerabilities we haven't found yet," Thomas said.