Malicious programmers focus on smartphones, tablets

May 4 2011, By Brandon Bailey

Malicious programmers are always looking for new targets. While smartphones and tablets replace PCs as the gadgets we use for messaging, Web surfing and even doing business, some shady characters are starting to target these devices with new forms of viruses, Trojans and spyware.

Researchers at several security software companies say that in recent months they've identified a handful of malicious programs hidden in seemingly innocuous applications, including games and video players, that could make Android phones send information and receive commands without the owners' knowledge.

In some cases the purpose was unclear. But one app used a phone's locating software to transmit the owners' whereabouts without permission. Another was designed to quietly send repeated text messages, while charging hefty fees to the owner's wireless account.

The number of threats is tiny compared with the vast array of malware targeting PCs. And at this stage, some experts say it's more important for smartphone users to follow common-sense precautions than to purchase one of the commercial antivirus products now offered for mobile devices. But even though the most popular smartphone operating systems may be less vulnerable than PCs, experts say the growing popularity of mobile gadgets means malicious coders will inevitably target them more often in the future.

"There hasn't been an example of malware affecting thousands or millions of devices yet, but that doesn't mean it's not possible or it won't happen," said analyst Chris Hazelton, who tracks mobile technology for the 451 Group, a tech research firm.

"We don't want to be the scaremongers," added Lyle Frink, a spokesman for security software company Avast. "But the development curve for these things is accelerating."

Researchers at another security company, McAfee, say the bulk of the smartphone malware they detected last year was written to target the Symbian operating software used by Nokia, long an international leader in the smartphone industry. But they and other experts have noted an uptick in malicious applications written for Google's Android, which late last year overtook Symbian as the most popular smartphone operating system, according to Canalys, a tech research firm.

"There's a growing installed base of Android users. And it's a very open platform - you can do a lot of good things with it, but if you want, you can also be more nefarious," said Mark Kanok, a spokesman for security software maker Symantec.

Historically, smartphones have used a variety of operating systems. And since a virus written for one platform wouldn't necessarily work on another, the pool of potential targets for any particular virus was small. Also, operating systems and mobile Web browsers have technical features that make it difficult to transfer files or data onto a device without the user's permission.

"They're much more locked down," said Andrew Jaquith, a former mobile industry analyst who is now chief technology officer at Perimeter E-Security.

But as smartphones become ubiquitous, the Android platform has become a prominent target. And experts say another reason they're seeing more Android malware is because Google, seeking to encourage independent developers, makes it relatively easy for anyone to offer an app through the official Android Market.

While Apple is known for closely screening every program offered through its App Store, analysts say Google does virtually no pre-testing or screening of apps in the Android Market. And Android apps can be downloaded from a variety of other sites, which increases the opportunity for bad guys to create a seemingly harmless app that contains malicious code, and then distribute it to an unwitting pool of Android device users.

A Google spokesman declined to comment on the issue of pre-screening apps, but the company said in a statement that it takes security very seriously and has numerous safeguards.

Android's design includes a "sandboxing" feature that prevents individual applications from reading or changing information in other applications or the underlying operating system, without first getting permission. That's why users who download an Android app typically get a message asking permission to access other services or software on the device.

Experts say smartphone users should not agree to anything that seems suspicious, although less savvy users may not understand what they're allowing.

The Android Market also displays user ratings and reviews, and Google encourages users to consider those before downloading any app. When the company has learned of a problem, it has yanked apps from the Android Market. And twice in the last year, Google has used its ability to

remotely remove certain apps from any device that had downloaded them, under the "terms of service" that Android Market users agree to accept.

In the most recent incident, Google disclosed last month that it had remotely killed several malicious apps that were transmitting information about the host device and its location. The company also used its ability to automatically install a security update on the affected devices to prevent further unauthorized transmissions.

"We are adding a number of measures" that would prevent similar apps from being distributed in the future, the company said in a blog post.

While crediting Google with reacting quickly, Hazelton noted that Google only learned of the malware from an independent developer after it had been downloaded an estimated 250,000 times. And as more users download more kinds of apps from a variety of sources, he said there's an increasing risk of malware getting past the security safeguards.

"We're seeing these things come almost in development cycles, where people are putting out different versions, testing their capabilities and incorporating new methodologies," added Symantec's Kanok.

Symantec, McAfee and several other software companies sell products that combine mobile antivirus software with features that allow consumers to back up their data, locate a missing phone and lock or "wipe" personal data if the device gets lost or stolen. Experts say these can be useful, but several said the most important thing owners can do is lock their device with a password.

While not every smartphone user currently needs antivirus software, Hazelton said the need likely will increase as banks and financial institutions offer more apps and online services for mobile devices.

"It comes down to each user and what they do with that device," he added.