technology review
Published by MIT

Thursday, February 9, 2012

Attacks on Android Devices Intensify

Rising security incidents and poorly defended phones suggest 2012 could be a risky year for smart-phone users.

By David Talbot

A recent rise in Android malware—combined with increased efforts to combat the threat—highlight the fact that, just like tech companies, app makers, and users, hackers are fast turning their attention to mobile devices. What's more, experts say, such devices are often configured in ways that make it easier for malware to thrive.

Several new types of Android malware have been spotted "in the wild" in recent weeks, and they demonstrate growing sophistication. One specimen, dubbed Opfake, is a bogus Web browser that automatically makes calls to premium phone lines. Opfake exhibits a powerful trick previously seen only in desktop malware, whereby the code repeatedly mutates to make anti-virus detection more difficult.

To counter the rising tide of threats, Google last week announced it had launched an app prescreening tool called Bouncer that runs a server-based simulation to check apps for malicious behavior—such as attempts to access or send personal data, or simply send out pricey text messages. Google blocks them before they get into the official Android Market.

Bouncer has been used quietly for several months; in the second half of 2011, the Android market saw a 40 percent decrease in malware apps identified as potentially malicious, compared to the first half of the year, wrote Hiroshi Lockheimer, Google's Android engineering vice president, in a blog post.

In a similar move, the mobile security firm Lookout says it is testing new methods for Android users that quarantine and scan downloaded apps. Whereas many existing tools screen the phone for already installed malware, a new tool would allow users to delay installation of a downloaded app until a check was complete. "For many users who install apps outside of Android Market, there is a need for pre-installation detection," says Derek Halliday, senior security manager at Lookout.

Lookout found, at the end of 2011, that 4 percent of Android users were likely to encounter malware over the course of the year—up from 1 percent of users a year ago, though part of the increase may be a function of improved detection, Halliday says.

Android is the most popular smart-phone operating system in the world, with 52.5 percent of the global market at the end of 2011, according to Gartner.

Google and Lookout's moves are a reaction to the relatively recent trend of malware writers intensively focusing on the official Android Market, and not just third-party app-dealing sites. "Since the vast majority of users rely on the official Android Market, it's understandable that there's increased focus there. At the same time, there are all kinds of other places where users can potentially acquire malware," says Halliday.

Meanwhile, new research is finding that Android phones themselves are often vulnerable out of the box. At the Network and Distributed System Security Symposium in San Diego this week, one research paper painted a bleak picture, reporting that many major brands come with factory settings that amount to a preweakened immune system, with various settings fixed to allow apps to access personal data, such as GPS position or stored contacts.

Xuxian Jiang, a computer scientist at North Carolina State University, said that his group studied eight mass-market phones—the HTC Legend, Evo 4G and Wildfire S, the Motorola Droid and Droid X, the Samsung Epic 4G, and the Google Nexus One and Nexus 4S. All but the two Google phones came out of the box with permissions pregranted for apps to access data that isn't needed for those apps to function, undercutting a pillar of Android's permission-based security model. The researchers say they

have notified the phone makers about the findings.

"There is a trend where malware is going to grow, and is going to evolve," Jiang says. "Google's Bouncer will be helpful to move in the right direction, but more work needs to be done to contain the malware growth." And part of that should include making phones more conservative in what they allow apps to do by default, he adds. The effort also requires more and better screening tools; his group is working on one tool called Droid Ranger.

Permissive factory settings on phones are no accident, says Radu Sion, a computer scientist and security researcher at Stony Brook University. The hotly competitive commercial landscape rewards makers of devices that are easiest for average consumers to use. "The usability of devices becomes more and more important. Most vendors will err on the side of usability—then they will sell more."

But creating an easy plug-and-play experience means not making the user individually authorize various data releases—which makes the devices more vulnerable to malware.

So far, the malware problem has been an annoyance rather than a major threat, but the pieces are in place for the situation to grow worse quickly, Sion says: "Android is not going to be safe anytime soon until we have some high-profile attacks. Right now, the malware is not a huge problem. Guys in Ukraine have not zoomed in on Android yet, but it's very easy to come in there. It's going to become a big problem."