Mobile Security: It's Time to Get Serious

By Terry Cutler on Dec 16, 2010

More people are flocking to their smartphones and tablets, leaving their notebooks behind. Attackers are certain to try to profit from this trend.

There's seemingly no end to the productivity gains from smartphones and tablets. With the anywhere access to email, applications, and data, workers are using their devices to do everything from staying in touch with co-workers on social networks to accessing and adding data to their CRM applications.

Although none of this may sound entirely new, it's not just about the technology, but also the rate of its adoption. Mobile has hit its inflection point. In the third quarter of 2010, according to the research firm Gartner, smartphone sales were up 96 percent from the same period a year ago.

Where people go, attackers follow. The trouble is that these devices are not exactly secure. We're already seeing malware specifically designed to attack mobile devices. Although such malware is not a dire threat now, in the months and years ahead it most certainly will be. Consider the rootkit designed by scientists at Rutgers University that burrows into the heart of the smartphone to access its microphone, GPS, and battery. This malware was a proof-of-concept and was not designed to be used on real-world attacks, but it showed just how easy it is to turn on the phone's microphone to snoop, send the location of the phone, and perform other undesirable shenanigans.

Traditional viruses have also been knocking on the keyboards of mobile phones for some time. Consider this 2008 **report**, when viruses such as the SymbOS/Beselo and the WinCE/InfoJack.A struck. That was also when the first Trojan aimed at the iPhone was unleashed. Although none of these viruses have hit critical mass, remember that after the Morris worm struck the Internet in 1988, it wasn't until 1999 that mass e-mail viruses received any attention as a risk to mainstream users.

As our dependence on mobile technology is growing, I doubt it will take that long this time around.

Experts expect other types of malware to proliferate as well. For instance, there's the threat of rogue applications being installed on mobile devices in order to steal data at a later point. Mobile devices can also be turned into spy devices. For example, software bugs can be installed on mobile devices and used to snoop on telephone conversations, grab text messages, and listen to conversations occurring within a room anywhere in the world, such as the proof-of-concept mentioned above.

These attacks are just as straightforward as other attacks we see today. First, the attack software is installed on the target's phone. To this end, users may be lured to a malicious website were the attack software is downloaded, perhaps by a link in a text message. Once the target opens what seems to be a message, the

Most Read | Most Recent

» Survey Reveals How Stupid People are With Their Passwords

» New Tool Reveals Internet Passwords

» Hacker Uses XSS and Google Street View Data to Determine Physical Location

» Snoop Dogg Joins the War on Cybercrime

» Study Reveals 75 Percent of Individuals Use Same Password for Social Networking and Email

» The Rise of the Small Botnet

» An Inside Look at Hacker Business Models

» IT Salary Guide Shows Increase in Salaries for IT Security Professionals

» Defense Department's Cyberwar Credibility Gap

» Nevercookie Eats Evercookie With New Firefox Plugin

» Veracode Expands Mobile App Verification Service to Android and iOS

» IBM Launches Initiatives to Help Secure the Exploding World of Connected Devices

» Sourcefire Unveils Immunet 3.0 with Ability to Create Custom Anti-Malware Signatures

software stealthily installs itself. In either case, once installed, the eavesdropper can actively monitor all incoming and outgoing calls, read all text messages, and listen in to any ambient conversations by remotely activating the microphone at any time.

While such attacks are specific to mobile phones and some tablets, expect the same types of attacks that have plagued PCs for years to also hit mobile devices—namely, viruses, spyware, worms, and Trojans—designed to snoop, steal, or destroy data.

So how do enterprises protect themselves?

The first line of defense does not have much to with technology, but everything to do with training and awareness. Enterprises can have the most elaborate defenses in place and still be humiliated by a single user’s mistake. The first step is to educate your end users to:

1. Never leave their phone unattended. It only takes a few minutes for someone to install the software on and taint a phone with malware. It doesn't take long for an attacker to copy the data on the phone either.

2. Don’t allow others to make phone calls from their phone. If they do, make sure they never leave sight of their phone. Remember, most often the person installing the spy software on a target's phone is not some shady character wearing a black trench coat, but someone very close to them.

3. If your phone has a feature to automatically password protect it during any inactivity, enable it.

4. Keep current with your phone’s security updates and firmware.

In the year ahead, as employees not only leave their notebooks behind to work on their mobile phones and even tablets, it’s important to ensure that users know the same security rules apply: Beware where one surfs and where one downloads software and always keep in mind that smartphones are powerful computers in their own right. Remind them that the data on their mobile devices is just as sensitive as that held on their PCs and that viruses, worms, spyware, and rootkits can do the same damage whether they hit a system within a datacenter, on a desk, or within their palm.

More Mobile Security News & Insights

Like Buzz Tweet 15 0 Digg Share 5 RSS

Terry Cutler is a co-founder of Digital Locksmiths, Inc., an IT security and data defense firm based in Montreal and serves as the company's Chief Security Evangelist and Certified Ethical Hacker. Prior to joining Digital Locksmiths, he was a Premium Support Engineer for Novell in Canada where he analyzed network vulnerabilities and transitioned security technologies into production. In addition to being a licensed private investigator in Canada, Terry is an internationally known author, trainer, speaker, and security consultant, Terry has appeared in numerous national television and radio programs and is very active on the conference circuit. Follow Terry on Twitter at @TerryPCutler

Previous Columns by Terry Cutler:

- Beating Back the Botnets
- Enterprise Security Priorities for 2011
- Mobile Security: It's Time to Get Serious
- The Anatomy of an Advanced Persistent Threat

Tags: INDUSTRY INSIGHTS Mobile Security Mobile & Wireless

- VASCO's DIGIPASS Technology to be Embedded Into Intel Identity Protection Technology
- 'Internet Kill Switch' - Is this Technically Feasible in the US?
- Organizations Struggle with Data and Application Security Budgets & Strategies
- Dell Completes Acquisition of SecureWorks
- Agiliance Launches Cloud-Based PCI Compliance Service
- One in Three Experience Mobile Device Loss or Theft. Do People in 'Party Cities' Lose More Phones?
- Mobile Threats Trending Upward, More Connected Devices Mean More Threats

Recent Activity

You need to be logged into Facebook to see your friends' activity

Like

DISQUS

Showing 0 comments

Sort by Best rating Subscribe by email Subscribe by RSS

Add New Comment

Type your comment here.

Post as ...

Trackback URL http://disqus.com/forums/securityweek/mobile

No recent activity to display.

http://www.securityweek.com/The%20I
40 people shared this.

'Internet Kill Switch' - Is this Technically Feasible in the US? | Information Security News, IT S
10 people shared this.

Man Pleads Guilty to Hacking Neighbor's Wireless, Sending Threats against Vice President | Informati
116 people shared this.

Cybercriminals Attack EFTPS.gov Users, Businesses Targeted in Another Massive ZeuS Attack | Informat
47 people shared this.

Facebook social plugin

Popular Topics

- Information Security News
- IT Security News
- Cloud Security
- Security Whitepapers
- Compliance
- Application Security

Security Community

- IT Security Newsletters
- Events
- Comments
- Most Read

Stay Intouch

- Twitter
- Facebook
- LinkedIn Group
- Stuxnet Group on LinkedIn
- RSS Feed
- Submit Tip

About SecurityWeek

- Team
- Advertising
- Events
- Writing Opportunities
- Feedback
- Contact Us

Wired Business Media