New hacks strike at heart of mobile innovations

August 7 2015

Smartphones have become increasingly targets for cyber criminals as people cram the gadgets with troves of personal information

As fierce competition leads to rapid innovation in the smartphone market, hackers have pounced on cracks in defenses of developments on devices at the heart of modern lifestyles, experts say.

Smartphones have become increasingly targets for cyber criminals as

people cram the gadgets with troves of personal information and go on to use them for work.

"Mobile devices are taking a bigger place in businesses and in our lives," Avi Bashan of Tel Aviv based cyber defense firm Check Point Software Technologies told AFP on Thursday at a Black Hat computer security conference in Las Vegas.

"As more people use them for more things, attackers gain interest."

Check Point has seen attacks rise during the past three years on the world's leading mobile operating systems - Apple iOS and Google-backed Android, according to Bashan.

Check Point researchers at Black Hat revealed a vulnerability that allows hackers take over Android smartphones by taking advantage of a tool pre-installed that was intended to give tech support workers remote access to devices.

"It effects every version of Android," Check Point mobile threat prevention director Ohad Bobrov said.

The hack can be triggered by tricking a smartphone user into installing an application rigged to reach out and connect with the pre-installed support tool, Bobrov explained.

In some cases the hack can be accomplished by sending a text message that a recipient doesn't even have to open, he warned.

The text message tricks a smartphone into thinking it is connecting with a legitimate support technician remotely when it is actually linking to an online server commanded by a hacker.

"I need your phone number and that is it," Bashan told AFP.

Bobrov said the flaw in Android software architecture has been disclosed to Google and smartphone makers.

Attacks have risen during the past three years on the world's leading mobile operating systems - Apple iOS and Google-backed Android, says Check Point

Dealing with Stagefright

The Check Point revelation came a week after cyber security firm Zimperium warned of a "Stagefright" vulnerability in the world's most popular smartphone operating system that also lets hackers take control with a text message.

Zimperium research senior director Joshua Drake took a stage at Black Hat to discuss Android code at the heart of the problem.

Stagefright automatically pre-loads video snippets attached to text messages to spare recipients from the annoyance of waiting to view clips.

Hackers can hide malicious code in video files and it will be unleashed even if the smartphone user never opens it or reads the message, according to Drake.

Stagefright imperils some 95 percent, or an estimated 950 million, of Android phones, according to the security firm.

Zimperium reported the problem to Google and provided the California Internet firm with patches to prevent breaches. Updates have started hitting Android devices, according to Drake.

Computer security firm Secunia on Thursday said about 80 vulnerabilities were discovered in Apple mobile operating software so far this year and about 10 were found in Android.

"There has been a big boom in mobile," Drake said.

"When there is a big boom, people take a lot of shortcuts, when you take shortcuts you build up a lot of technical debt."

Mobile operating system makers who raced ahead now have to backtrack to squash bugs, some of which are exposed by good-guy hackers.

Check Point's Bashan sees it as a case of smartphone rivals moving so fast to add features and improvements that innovation trumped security at times in the process.

"The operating systems developed so quickly," Bashan said.

"And when you develop quickly, some things get developed badly."