Hackers turning smartphones into slave armies

November 19 2014

An Android-powered smartphone is seen at a promotional event in New Delhi on July 30, 2014

Mobile security firm Lookout on Wednesday warned that Android-powered smartphones or tablets are being targeted with malicious software that puts them at the mercy of hacker overlords.

The persistence and sophistication of malware dubbed NotCompatible is another sign that cyber criminals are hitting smartphones and tablets with

tactics and tenacity once reserved for desktop computers, according to Lookout security researcher Jeremy Linden.

"Mobile is becoming the dominant computing platform and, because it is so ubiquitous, we are seeing heightened malware targeting it," Linden told AFP.

"Mobile malware is becoming very advanced and rapidly reaching parity with PC malware."

Information that can be mined from hacked smartphones includes where people have been, pictures taken and call logs.

"It is the jackpot when it comes to valuable data, so obviously bad guys are doing a lot of work to get at it," Linden said.

So far, it appears to Lookout that control of smartphones and not pilfering what they hold is the primary use of NotCompatible.

Armies of enslaved mobile devices are used for sending spam hawking goods such as diet pills, or snatching up hot concert tickets when they go on sale so they can be scalped later at higher prices, according to Lookout.

Hackers operating networks of infected mobile devices likely rent out the "botnets" for uses such as unleashing barrages of email ads and attacking websites.

The most common way for the virus to get on a smartphone is by visiting legitimate websites that have been hacked and then booby-trapped to secretly infect visitors, Linden said.

NotCompatible typically introduces itself as an Android system update

and asks for permission to install in mobile devices. One way to safeguard against infection is to decline such prompts and go through smartphone settings to check for system updates.

The malware has grown in sophistication since it was first detected in 2012, adopting measures to elude detection by researchers and adding the ability to endure even if servers being used by hackers to control it are taken down, according to Lookout.

Those behind NotCompatible were said to be running it like a savvy business operation, and are doing well enough to invest heavily in beefing up the back-end on which the malware relies.

"While it is true we haven't seen any data stealing, you don't want anything like this on your device," Linden said.

"You are adding to the general danger of the Internet by letting an attacker use your network for something unsavory, and you could be responsible for any data plan charges."

If people use infected smartphones on the job, there is risk the virus could provide openings for hackers to slip into company networks.