Smartphones tempting new targets for hackers

July 30 2010, by Glenn Chapman

A shopper looks at a smartphone at a shop in Taipei on July 19. Software security experts warn that mobile phones are tempting targets for hackers in a world where people eagerly invite strange applications onto handsets packed with personal data.

Software security experts warn that mobile phones are tempting targets for hackers in a world where people eagerly invite strange applications onto handsets packed with personal data.

Briefings on Thursday at a Black Hat computer security conference were devoted to threats to smartphones, mobile personal computers used for anything from banking and shopping to pinpointing people's whereabouts.

"Right now, it is one of the hottest topics there is," said John Hering,

founder and chief executive of Lookout Mobile Security.

Smartphone owners are seldom far from their handsets, which they trust with passwords, telephone numbers, Internet browsing, banking, shopping, navigating, and more.

The online App Store run by iPhone maker Apple kicked off blazing trend of developers making mini-programs that add fun, hip or functional features to mobile phones of all types.

"Users are downloading apps at a furious pace and, generally, have not been thinking about security," Hering said.

"If you download an app you are trusting the developers so it is important to be careful."

Lookout studied approximately 300,000 mobile phone applications and found that some programs accessed more data than users might expect.

One application for changing the pictures set as background "wallpaper" on mobile telephone screens fed telephone numbers from smartphones to a computer server owned by a Chinese software developer, according to Lookout.

"If you want to put a picture of your kid, your dog, or Star Wars as background, it doesn't make sense that the application needs your phone number," Hering said.

Some data grabs by applications could be unintended side effects of developers hastily cranking out software in a rush to be the next must-have app for smartphones.

"Everyone is trying to write an app to make the next million dollars at

the App Store," Hering said.

"They may be whipping something out without being careful."

Apps offer hackers Trojan Horses in which to slip malicious code, said F-Secure chief resource officer Mikko Hypponen.

F-Secure recently followed a trail that led to malicious code hidden in an anti-terrorist shooter game program for smartphones.

A Russian hacker had cracked a legitimate game, planted a virus in it and then offered the tainted app for free at a copycat website, according to Hypponen.

"It is actually a very good game that suddenly was free," the security researcher explained. "Download sites thought it was the real deal."

The game software was modified to wait a while after being downloaded before having smartphones call eight telephone numbers that charged premium rates and funneled the bulk of the charges back to the hacker.

The calls added a total of 12 dollars to a smartphone owner's monthly bill, and the software was programmed to repeat the calls once per billing cycle.

While the calls appeared to be international, to places such as the South Pole, a tactic called "short-stopping" was used to route them only a fraction of the way but bill the full rate.

"It didn't call the South Pole, but you paid for the call to the South Pole and the virus writer got the money," Hypponen said, displaying a list of operators that sell such shady numbers.

"Hacking mobile phones to make international calls to get money, that is where I believe the future of mobile phone malware will be.

Hackers still prefer to attack personal computers, the researcher said.

F-Secure reported that there are approximately 40 million known pieces of malicious code targeting PCs and just 500 designed to attack mobile phones.

"Eventually, virus writers will realize it is easier to make money by infecting phones than it is by infecting computers," Hypponen said.

"And, of course, there are more phones on this planet than there are computers."

People were advised to set strong passwords and install anti-virus software on smartphones, and to be wary of apps.