Firm warns of hacker threat to mobile gadgets

February 29 2012, by Glenn Chapman

Cyber security veterans behind startup CrowdStrike will demonstrate at the RSA conference on Wednesday that the types of attacks used against computers are heading for smartphones.

Cyber security veterans behind startup CrowdStrike will demonstrate at the RSA conference on Wednesday that the types of attacks used against computers are heading for smartphones.

Former McAfee chief technical officer George Kurtz and Dmitri Alperovitch, who has researched major cyberespionage operations, have figured out how to take over smartphones using booby-trapped text messages.

"The reality is that those attacks are probably already in the wild and no one has discovered them," Alperovitch, the author of reports on

cyberespionage operations Aurora, Night Dragon, and Shady Rat, told AFP.

Hackers could send a text message worded like a warning from the telecom service provider that the account will be canceled if the smartphone user doesn't click an enclosed link to resolve the matter.

Clicking the link then triggers the installation of malicious software that lets a hacker control the smartphone remotely.

"We can monitor and record all calls, get all inbound and outbound SMS messages... basically take over the phone," Kurtz said.

"Imagine sitting in a board meeting and someone accesses your phone and listens remotely."

A hacker could even track a smartphone user's whereabouts using a handset's location-sensing capabilities.

Tricking computer users to click on links or to open rigged email attachments has been a longtime technique used to infect computers.

When it comes to smartphones, experts have mainly focused on the potential for makers of "apps" to program in nefarious tasks such as stealing data.

"When we look around we see people worried about malicious apps," Kurtz said. "We think the real issue is vulnerability in those phones."

Kurtz and Alperovitch have been operating freshly-launched CrowdStrike in "stealth mode," but it has gotten $26 million in backing from global private equity firm Warburg Pincus.

Relentless waves of cyber attacks that appeared to be the work of states inspired the researchers come up with a different way of taking on the threat.

"Most companies are focused on detecting malware, and there are millions of pieces of that, with new ones coming all the time," Kurtz said.

"It really is akin to focusing on the bullets in the gun as opposed to the shooter... We think most companies have an adversary problem, not a malware problem."

CrowdStrike is building tools to figure out who is behind attacks, how they move after invading systems and what they are out to steal or accomplish, according to the researchers.

"You can't know how best to fight a war without knowing who the enemy is, and it is the same thing in cyber space," Alperovitch said, describing China and Russia as the most prominent threats.

CrowdStrike plans to have a security product to market in the second half of this year.

"At the end of the day it is another guy sitting at a keyboard somewhere going after your data," Alperovitch said. "You don't have a malware problem, you have a people problem."