Smartphones under growing threat from hackers

February 17 2010, by Laurent Thomet

A man looks at his mobile phone during the Mobile World Congress in Barcelona on February 16, 2010. Smartphones are under a growing menace from cyber-criminals seeking to hack into web-connected handsets, but the mobile industry has contained the threat so far, security experts said.

Smartphones are under a growing menace from cyber-criminals seeking to hack into web-connected handsets, but the mobile industry has contained the threat so far, security experts said.

Software security firms warned at the Mobile World Congress in Barcelona, Spain, that the increasingly popular smartphones could face an explosion of virus attacks in the coming years.

"Tomorrow we could see a worm on phones which would go around the world in five minutes," said Mikko Hyppoenen, chief research officer at

F-Secure, which makes anti-virus software for mobile phones.

"It could have happened already. It hasn't, but it could happen. And I do think that sooner or later it will happen, but when? Well that I cannot tell you," he told AFP.

But security companies, mobile operators and makers of operating systems have found solutions to limit the attacks so far and delay an onslaught of spam and viruses, he said.

"It won't work forever, eventually we will see the first global outbreak. But we have been able to delay it by more than five years, at least," he said.

The first mobile virus appeared six years ago, and so far F-Secure has detected only 430 mobile worms. This compares to millions of computer viruses.

Much like the first computer hackers of two decades ago, the people attacking mobile phones have been doing it as a hobby, Hyppoenen said.

"It seems that on any new platform, the first years, the first viruses are done by hobbyists just to show off and then later more professional money-making criminals move in," he said.

One of the first viruses was called Skulls. Spreading through wireless bluetooth systems, a skull would appear on a phone's screen and delete all its data, Hyppoenen said.

The few money-making "trojan" viruses that have been seen infiltrate a person's phone and send text messages to premium numbers controlled by the hacker, he said.

Security companies have developped anti-spam and anti-virus software for mobile phones as well as anti-theft features that allow a phone's owner to remotely block the device and even map its location.

But smartphones, with their email and Internet capabilities, will invite more break-ins, especially with the growth of mobile banking -- financial transactions that can be done through applications, experts said.

"It is all about money," said Eugene Kaspersky, founder and chief executive of software protection firm Kaspersky Lab.

"Malware is developed to make more money. It doesn't matter if it's computers or smartphones," he said.

His company has detected an average of 30 mobile viruses per month over the past year, and believes that a wave of financial assaults are just around the corner.

It took more than 20 years for computer viruses to become a money-making industry, Kaspersky said.

"We expect that in mobiles it will take much less time," he said. "This year and next year we expect to see the industrialisation of smartphone malware."

Adam Leach, a mobile device expert at Ovum research firm, played down the threat, saying that the industry is staying on top of the problem.

"The threat hasn't been as high as expected," he said, adding that companies have learned from past experiences and have found ways to "minimise the threat."

But he warned that the mobile industry should not let its guard down.

"I think it is something companies need to take seriously," Leach said. "If it is not taken seriously, it has the potential to have a big impact on (mobile phone) users."

(c) 2010 AFP