

<http://mobileworld.com.my/blogs/gomobile/2459-mobile-under-attack.html>

Mobile Under Attack

Kashminder Singh Wednesday, 18 January 2012 18:48

Last month I was at a press summit that was organised by NetEvents. The topics at the summit were squarely enterprise centric. I had to suffer an immense overdose of topics like datacentres, virtualisation, enterprise cloud solutions and networking but one topic made me attend and that was cyber security.

A large number of security solutions providers were there. Companies like Palo Alto Networks, Fortinet, Sourcefire, Blue Coat and Niometrics. Of course, the speakers who spoke on cyber security issues also focussed on enterprise issues but the background information I gained was invaluable.

In essence, everyone who uses a smart mobile device and his or her employers should take cyber security very seriously.

Firstly, the profile of the attacker has changed. Malware makers are no longer hacker kids out for some mischief and bragging rights. These days, malware threats are more likely to come from organised crime out to make as much money as possible.

Also, these attacks are not just coming from traditional means such as infected files sent by emails. They can come from anywhere actually. For instance; Facebook. Yes, the social network we visit everyday has up to 600,000 breaches a day. Click on the link shared by your friend purporting to show you a hot video and you could end up with a compromised PC or mobile device.

That was the most frightening part for me; to learn that mobile devices are becoming prime targets for malware attackers. That and the fact that there is little that can be done about it by the end user.

Here's something you may not know. The mobile security solutions sold by end user antivirus vendors are all but useless. This was confirmed by quite a few of the experts I spoke to at the event. The reason why antivirus vendors cannot build effective solutions for mobile devices is quite simple. I was told that this was because they don't have access to key portions of the operating system; these are blocked by the OS companies.

If that is the case, it brings up an important question. Who then is responsible for ensuring that my data and my device are safe from a cyber attack? It can't be me if there are no good solutions to get from vendors. Logically speaking, it has to be the OS maker, the telcos and ISPs. Companies like Google and Apple have to make sure that the OS is safe if they lock up portions of their platform. Telcos and ISPs have the responsibility because all traffic passes through them. I have always believed if ISPs put in good security systems at the network level, end users will have much less to worry about. When we travel on highways, we expect that exit and entry areas will be lighted up and safety measures will be in place all along the highway. Shouldn't ISPs (telcos are ISPs too) then work on the same principles? Especially if it is a known fact that proper security is not possible at the device level?

Another worrying thing I learnt is that the attackers have gotten personal. These cyber criminals have learnt that it is easier to get into an organisation's network by walking in through a compromised mobile device in the hands of an unsuspecting employee than to launch attacks on the perimeters of the network. They do not depend on generic viruses for the attack. Instead they will carefully study the potential victim and build specific malware for him or her. For example, an avid fisherman could receive on Facebook a link to a fishing video which would have a trojan inserted in it.

As Nir Zuk, the founder and CTO of Palo Alto

Networks puts it; "... today's desktop anti-virus software is not very good at protecting against the targeted attacks And then the second challenge with the desktop anti-virus is that it doesn't run on things that are not desktop and we need to find a good solution for that as well, for the iPhones, the iPads, the Androids and even the Macs of the world."

But for now, that sort of attack is almost impossible to stop and this is why mobile security will be one of the trends that I will be watching very closely next year.