

Could The Smartphone Be The Weakest Link Of Your Corporate IT Network?

The theft or loss of valuable and private data from a mobile device such as laptop, USB stick or an old hard drive that hasn't been wiped and is then sold on an auction site, has gained much negative media exposure. However one of the biggest emerging threats to corporate data security is coming from unprotected smartphones.

As the popularity of smartphones grows, for both personal and business use, they have the potential to pose a similar, if not a greater risk to IT security than the laptop. In 2007 the number of smartphones shipped worldwide was approximately equal to that of laptops. However it is anticipated that it will be almost double in 2010 and the analyst group IDC predicts that within four years more than 70% of the workforce will connect to corporate networks via mobile devices.

This is perhaps unsurprising, as the cost of smartphones has come down significantly whilst functionality has massively increased. Organisations – from small business to the largest enterprise – are able to harness the capabilities of these devices to increase employee productivity through the delivery of 24x7 connectivity for always-available access to email, IM, the Internet and enterprise applications.

Yet worryingly, despite this dramatic market growth, smartphones are currently receiving a disproportionately low amount of security focus, with only 30% of visitors at a recent IT security event stating that their IT security policy covered such devices. This is of particular concern when 25% of all mobile devices in an organisation are estimated to carry mission-critical information (source: BPMF) and an astounding 30% of mobile devices are lost per year (source: SANS institute). In fact, according to The London Underground approximately 100,000 devices are found on its trains and in stations annually.

Whilst mobile phones and smartphones haven't traditionally been a primary target for Cybercriminals - apart from in Russia, which has seen a number of documented cases in the past - the rest of the world has largely managed to avoid the threat of mobile phone-based Crimeware. In recent months the appearance of malicious programs with a cybercrime aspect (including Trojans, viruses and spam) suggest that Crimecriminals have decided that 2009 is the opportune time to enter the 'market' and to start profiting from mobile Crimeware.

In January of this year we detected a Crimeware program (a Trojan known as SMS.Python.Flocker Trojan) for Symbian, one of the most common mobile phone operating systems worldwide, that targeted customers of an Indonesian mobile phone operator, which offers a money transfer service. The Trojan, written in the script language Python sends SMS messages to a specific number with instructions to transfer some of the money of the user's account to another account - belonging to the cybercriminals.

The effect on an organisation compromised by mobile Crimeware will typically be the damage or theft of mission-critical (and therefore highly valuable) business data. A smartphone can fall victim to online attacks when it's used to download information from the Internet. Infected devices can be used to penetrate the network perimeter of a corporate IT system. The loss or theft of a smartphone means that sensitive corporate information can end up in the hands of a stranger (none of us wants to be the next high profile media victim) In addition, SMS spam causes much inconvenience and stifles productivity.

Today, security vendors are one step ahead of the Cybercriminals that are trying to exploit mobile device platforms, particularly Symbian and Window Mobile. Solutions are available for enterprises to deliver comprehensive protection in the event of device loss or theft, enabling the owner to secure all data and prevent access to it until the device is recovered and, in the case of theft, automatically wipes all information remotely. Additionally, should a new SIM card be entered to the device, a hidden SMS message will be sent to the owner containing details of the new SIM card: this can be passed to the device provider and other relevant authorities. Earlier this year Kaspersky Lab

worked with Barclays to enable the bank to provide its two million online banking customers with security for their mobile devices.

The security of the corporate IT network is only ever as strong as its weakest link. Hardening every endpoint, including smartphones, is vital to ensuring the Cybercriminals do not compromise the organisation.

Author: David Emm, a member of the Global Research and Analysis Team at Kaspersky Lab (www.kaspersky.co.uk)

About Kaspersky Lab

Kaspersky Lab delivers the world's most immediate protection against IT security threats, including viruses, spyware, crimeware, hackers, phishing, and spam. Kaspersky Lab products provide superior detection rates and the industry's fastest outbreak response time for home users, SMBs, large enterprises and the mobile computing environment. Kaspersky technology is also used worldwide inside the products and services of the industry's leading IT security solution providers. For further information, please visit www.kaspersky.com. For the latest on antivirus, anti-spyware, anti-spam and other IT security issues and trends, please visit www.viruslist.com.

Editorial contact:

MCC International
Graham Thatcher / Simon Hewitt / Fiona
Brewer
kasperskylabpr@mccint.com
01962 888100

Kaspersky Lab UK
Emma Cross
emma.cross@kasperskylab.co.uk
0871 789 1634

© 2009 Kaspersky Lab. The information contained herein is subject to change without notice. The only warranties for Kaspersky Lab products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Kaspersky Lab shall not be liable for technical or editorial errors or omissions contained herein.