BIZCOMMUNITY

Mobile malware: What is it, why should you care? (part 1)

By Justin Lee

27 Mar 2013

In this article, the first of a series of four articles, we will explore how the use of mobile devices by employees in businesses represents the convergence of personal and corporate needs.

Today, with increasing initiatives such as Bring Your Own Device (BYOD), businesses are not only challenged to keep up to date with the wide variety of mobile devices brought onto the corporate network, but also the mammoth task to maintain control over these devices from a security perspective, as the growth of mobility has created an alluring opportunity for cyber criminals to generate profits through mobile malware.

The mobile threat landscape

In 2012, there were only a small percentage of malicious threats on mobile devices, most of which were classic scams attempting to convince users to enter sensitive information into a website that replicates a bank's website, for instance. However, this will certainly change in 2013 as the adoption of mobile devices continues to grow at a rapid pace.

According to analyst house IDG's most recent "Global Mobility Study", 70% of those employees surveyed, access the corporate network and business-critical apps, using a personally owned mobile device, including phones and tablets, and 80% access email from their personal devices.

In the "traditional" desktop world, cybercriminals today can purchase exploit kits on the underground market and utilise malware networks (or "malnets") to continually launch malware attacks on users, but to date, exploits that target mobile devices have not yet appeared. However, established techniques such as pornography, spam and phishing that have worked well in the desktop world are now successfully migrating to the mobile world.

As many of these tactics are device agnostic, expanding the attack to target mobile devices to convince users to provide credentials or other confidential information, such as credit card information, is relatively simple.

Another important and significant difference between desktop and mobile environments is the fact that mobile versions of websites are often crafted and hosted by third parties. This means that the URL might not be a good indicator of the relative safety of the site, as is often the case on desktop PCs where users have larger screens and viewing the full web address normally could be a good indicator whether a site is safe or not. When trying to access certain sites on a mobile device, users are redirected to a different site, and this practice essentially conditions customers to be comfortable with going to a strange URL to find an official site and thus gives attackers an edge that they can potentially leverage to deceive mobile users.

What can be done?

Mobile devices have empowered users, giving them access to a wealth of information and corporate assets from anywhere. Yet, many businesses have not yet put tools and practices in place to allow users make good, safe choices.

When we think about security under the lens of mobile devices, some risks decrease, some increase and some stay the same. For example, consider the increased risk of your password being exposed to an onlooker, as mobile phones often reverse the years-long practice of instantly masking passwords when you type them in - these devices typically expose the password, character by character, to ensure that your entry is correct.

It is also often harder to make good choices about the links you visit on a mobile device. Many times these links are truncated or shortened via a service such as bitly, which impedes a user's ability to make a good decision about their destination.

Lastly, a recent phishing attack from "PayPal" demonstrates how easy it is to be tricked into providing your credentials on a mobile device. In this attack, users received a perfectly formatted, grammatically correct phishing email informing them that PayPal had detected suspicious activity during the user's last transaction. The email goes on to say that PayPal has temporarily blocked the account until the user verified the account by clicking on a link.

Extending an enterprise-class web security solution to include mobile devices is a good first step towards protecting your employees. By closing the mobile security gap and enabling controlled access to corporate assets with appropriate policy controls, businesses can proactively protect themselves against this evolving mobile threat landscape while capitalising on the innovation and productivity of a mobile workforce.

Our next article will examine the behavioural patterns of mobile users - stay tuned.

For more:

- Bizcommunity: Mobile malware: What is it, why should you care? (part 2) by Justin Lee
- Bizcommunity: Mobile malware: What is it, why should you care? (part 3) by Justin Lee
- Bizcommunity: Mobile malware: What is it, why should you care? (part 4) by Justin Lee

ABOUT JUSTIN LEE

Justin Lee has over 15 years of IT experience specialising in Network and Security. He is currently the Regional Sales Manager for Blue Coat Systems in South Africa, and is responsible for leading sales and channel initiatives for Sub-Saharan Africa. He has extensive experience in working with numerous service providers, mobile operators and enterprise's across Africa. Contact details: website www.bluecoat.com

- Mobile malware: What is it, why should you care? (part 4) - 23 Aug 2013
- Mobile malware: What is it, why should you care? (part 3) - 21 Jun 2013
- Mobile malware: What is it, why should you care? (part 2) - 22 May 2013
- Mobile malware: What is it, why should you care? (part 1) - 27 Mar 2013

View my profile and articles...