bizcommunity

Mobile malware: What is it, why should you care? (part 3)

This article, the third in a series of four articles where we explore how the use of mobile device by employees in businesses represents the convergence of personal and corporate needs, will examine the mobile threat vectors, and how use behaviour can become the Achilles Heel.

By Justin Lee 21 Jun 2013

Mobile user behaviour creates opportunities for cyber criminals to lure users to malware by leveraging popular categories of content. Protecting users that are vulnerable to manipulation or behavioural exploitat can be challenging without understanding where they are most at risk.

These threat vectors are driven by user choices or behaviour, and are designed to lead mobile users to malware. During 2012, the most dangerous place for mobile users was pornography. More than 20% of th time that a user went to a pornography site, it led to a threat, and they have a one in five chance of finding a threat than when compared to other sites.

The prevalence of porn on mobiles

Interestingly, when malware first moved to the Internet, pornography was one of the leading sources of malware for desktop users. The prevalence of pornography as leading threat vector has ebbed, giving way to attacks that target much larger user populations, such as search engine poisoning.

With users spending the most amount of their mobile web browsing time accessing computers/Internet content, it's not surprising that this content is also a leading threat vector, responsible for more than 7% of malicious requests from mobile devices. Many of the early successful mobile malware attacks offered use free Angry Birds apps, an Android version of Skype or an Opera browser.

Web ads and malvertisting

Further, web advertisements are an interesting case. They rank as both the fourth most requested categor of content as well as the fourth ranked threat vector for mobile users, demonstrating that both the ad-based revenue model and malvertising attack methodology have transitioned to the mobile web nicely.

Mobile users who shop or conduct online banking on their smartphones are important targets for both commercial businesses and malware operators. The volume of web advertisements that are delivered through these mobile applications creates an effective entry point for cybercriminals to inject ads that lead malicious downloads. A recent example was a fake Angry Birds download that delivered an SMS Trojan th made premium SMS calls (texts) to the malware host, which then billed users without their knowledge.

Other similar tactics involve presenting fake downloads such as PDFs, browser updates or executable file that then deliver malicious payloads designed to steal personal information and other assets.

Best practices

Given the success of the model in desktop environments and the seemingly successful transition to mobil environments, it is reasonable to expect malvertising will continue to be a key threat vector.

We would advice businesses to:
• Block all content to mobile and desktop devices from dangerous categories, including pornography, phishing and spam.
• Block executable content from un-rated domains and categories that typically host malware, such as Dynamic DNS hosts.

For more:

- Bizcommunity: Mobile malware: What is it, why should you care? (part 1) by Justin Lee
- 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 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 responsit 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
View my profile and articles...