BIZCOMMUNITY

Mobile malware: What is it, why should you care? (part 2)

By Justin Lee

22 May 2013

In this article, the second in a series of four articles where we explore how the use of mobile devices by employees in businesses represents the convergence of personal and corporate needs, we will examine the behavioural patterns of mobile users, in order to truly understand the mobile risks associated.

We observed mobile users behavioural patterns closely during 2012, which showed a stark difference from the way that people typically use their desktop. In this, we discovered a few interesting angles on how cyber criminals exploit these behavioural patterns for their own malicious benefit.

A day in the life of a mobile user

On average, mobile users spend around 72 minutes a day browsing the mobile web, using mobile browsers. It is important to note that this time does not include time spent using native applications - those apps specifically designed to run on specific devices - and thus represent the time when users are most vulnerable to threats.

Within this timeframe, just under 12 minutes are spent with content related to the Internet, while the remaining hour or so is spent looking at a variety of content, ranging from social networking, shopping and entertainment, to business and economy. The diversity of topics that comprise a user's day on the web demonstrates how important mobile devices have become for giving access to any information, at any time, from any location.

Typically, users access much more recreational content such as shopping, entertainment and personal pages/blogs, from their mobile devices than they would on their desktops or laptops. In fact, the percentage of requests for recreational content was twice as high for mobile users.

The most noticeable difference between these user behaviours occur within search engines, where desktop users make use of search engines twice as much as mobile users. This may be due to the fact that desktops and PCs simply have larger screens, and so users are able to see the complete web address, helping them realise when the site is fake.

The availability of native apps changes the dynamic on mobile devices, making it easier to access apps and features that are most important to the individual user. As the mobile ecosystem expands, cyber criminals will spend less time targeting mobile users through search engines.

Mobile killed the PC star

The uniform demand for a quality experience regardless of platform type is creating a split in the application market. Today, users will move between web, mobile web and native mobile applications, depending on which can best meet their experience expectations. For example, users are opting to use web or native mobile applications to access audio/video content, as these applications can optimise their experience better than mobile web versions.

The search for the optimal user experience continues to condition users and extends to the use of corporate applications on mobile devices. As organisations introduce corporate app stores to manage the applications on their network better, user experience will be a key driver of adoption.

From a security perspective, users will tend to go with the application that provides the best user experience even if it is not the most secure option. For example, most organisations set size limits on email attachments, however, an employee faced with these limits could split the attachment into two separate files, or upload to Dropbox and just send the link - clearly not the most secure, and might even violate compliance or regulations.

Top tips

By not paying attention to user experience, organisations can inadvertently create security gaps. It is therefore crucial that organisations close the mobile gap on the network, by ensuring a visible and consistently enforcing policy, across the following three types of apps that may be running on the network:

1. Web apps (such as desktop browsers)
2. Mobile web apps (such as mobile browsers)
3. Native mobile apps

As companies continue to adopt BYOD initiatives and allow employees to access corporate assets with their own devices, controls must be extended to those devices as well.

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 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...