BIZCOMMUNITY

Mobile malware: What is it, why should you care? (part 4)

By Justin Lee

23 Aug 2013

In this article, the fourth and last in our series of articles on mobile malware we take a look at how "malnets" (or malware networks) revolutionised the way that cyber criminals deliver malware attacks to desktops and laptop users, and are now firmly setting their sights on mobile devices.

Delivering mobile malware with malnets

Malnet infrastructures are embedded in the Internet. They are powerful tools for cyber criminals because they are always there, ready to be used in any attack, and are extremely adaptable. With these infrastructures, cyber criminals can launch ongoing attacks on users, targeting wide swaths of users with very little effort.

Cyber criminals spent 2012 tuning malnets to require low investment and deliver high-impact results.

This same strategy is now being extended to mobile devices for further financial gain. This is a significant shift that will rapidly increase attacks on mobile devices.

Prior to 2012, mobile-specific attacks launched from malnets consisted primarily of malicious Java apps. Malnet components serving malicious Android apps first appeared in October 2011. It wasn't until February 2012, though, that malnets targeting mobile users showed real activity. That month, not only did we see a significant surge in mobile malware, but also the adoption of classic evasion techniques as well. The impact of this shift has been noticeable. Since early 2012, cybercriminals have expanded their infrastructure to launch attacks on mobile devices. In 2012, mobile traffic to malnets increased to 2% of overall malnet traffic. This growth is further evidence that mobile malware is poised to make an impact in 2013.

The growth in requests to malnets from mobile devices was driven by eight unique malnets in 2012. Three of the malnets targeted mobile devices exclusively while the others simply expanded their malicious activities to include mobile devices.

It is clear that in 2012, malnets were in an experimental phase of targeting mobile devices. However, during 2013 and into 2014, they will continue to invest in their strategies, develop better tactics, and show greater success in 2013.

Anatomy of a mobile malware attack

Last September, we examined an Android attack launched by a known malnet. In this particular attack, a user was offered an Android version of Skype via a website that lived on a shared web host with many other sites. There was nothing

suspicious about the web host though the fact that the offer was delivered via a Russian website should have been an immediate red flag for users.

When a user clicked on the download button, they were relayed to a different website that was in a bad Internet "neighbourhood" - one known to be associated with suspicious and malicious activities. The user was then relayed to another known suspicious site for the actual download.

At the time of this attack, the download was recognised by only 10 of the 41 anti-virus engines. During the same week that this attack occurred, one of the mobile malware malnets used 38 domain names and another used 14 domain names for a variety of sites that were involved in attacks. Among the sites were two Flash update sites, four pornography sites, a movie site, a couple of browser sites and several general "file" and "app" sites.

The diversity of these concurrently running attacks shows that although mobile malware is in the early stages, it is clear it will continue to grow and become a problem for users as well as businesses that allow those users access to the corporate network.

Summary

These four articles clearly demonstrate that mobile users represent a complex and growing constituency for organisations today. Those that can securely manage mobile devices can gain a competitive advantage by enabling their employees to be more productive. As businesses increasingly open their networks to mobile devices, cybercriminals will be knocking at the door. As we have seen in this report, they are already arming themselves for an attack.

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 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.

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 3) 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...