



Thank You for helping iSecure become Rochester's Top 100!

A sincere THANK YOU to our loyal customers, supportive partners, and dedicated staff who have made this honor possible. We are committed to another year of continued success, growth, and support to our fellow Rochester businesses.

Android Malware Up 472% Since July 2011 – Diffusing A FUD Bomb

It's been a scary past week. The landscape of mobile threats has never looked so bleak. IT administrators have already been between a rock and a hard place in deploying a management system that doesn't squash user freedoms, while protecting corporate infrastructure and data, but now, there's been a huge influx of software that aims to jeopardize any inroads we've been able to make toward gaining management approval of the efforts to not just commoditize employee device selection, but to go one step farther and consumerize it. It's absolutely true. Android malware, published to the Google Android Marketplace, is up 472% since July. This comes to us from a credible source. Juniper's Global Threat Center article from November 15th ([here](#)).



It turns out that, things may be less dire than we all feared when reading past the headline. There are very few published numbers that are not percentages and presented as growth percentages at that. What I was able to find was that, based on some reporting by Lookout, there were 55 applications found to be offenders. All of the applications under scrutiny used known exploits to do their dirty work. The majority of offending applications were repackaged legitimate, popular titles, republished by a third party. This is very basic stuff. In a separate analysis conducted by Kaspersky Labs, they determined that a single application, known as DreamDroid was acting as a Trojan backdoor for the application to download other Android malware applications for execution on the device. So, we have a couple classic attack vectors at work here. There's nothing original. All of it was preventable.



The answer to preventing attacks to our phones and tablets remains simple. It remains essentially free, but not something you can download. It is exercising common sense and keeping your eyes open. When downloading software, even from legitimate sources, look at the permissions that the application says it needs to run on your system. Look closely at the publisher. Make sure it matches the name of the company that produces the software you're after. Most companies work hard to make sure there are no typos. If something looks too good to be free, it just might be. Google for the application and read the reviews. They often contain useful gems of information, like negative reviews. There still isn't a silver bullet that magically protects against malware, but, common sense, a copy of Lookout's application and perhaps Kaspersky Mobile Edition could go a long way toward making this at least an uphill battle for those who would gladly have us download tainted applications.

Stay Vigilant, Citizens.

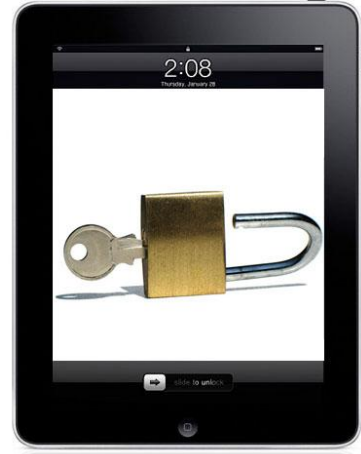
For those interested, a great analysis of mobile operating systems and their relative safety can be [found here](#), provided by Android mobile security.

New solutions that limit the vulnerability of your company's mobile devices....

Organizations spent billions over the last decade on securing their IT infrastructure in response to high profile data breaches and compliance requirements...only to be foiled by mobile devices. Smartphones and tablets in the enterprise are often unmanaged, unaudited, and unsecured and mobile data leakage is the top concern for CIOs, bar none.

Zenprise MobileManager provides customers with a triple layer of security that operates at the device, application and network tiers; thereby providing a security solution that goes everywhere the data goes, securing every point in the enterprise's mobile environment.

Palo Alto Networks Global Protect now supports Apple products such as the iPad, iPhone, and Mac OS X devices, in addition to Microsoft Windows devices to provide customers with the industry's most comprehensive security and consistent visibility and control over all of their network traffic regardless of device or location.



iSecure is now offering a free evaluation for either of these products (*through December 31, 2011*). For more information, or to schedule a free onsite consultation, please contact Mark Zane, VP Sales, at 585-419-8249 or mark.zane@isecurenet.net.



Stay informed on all current network security news, threats, solutions and more!

Stay up-to-date with the latest attacks, most harmful threats, and reviews on different solutions through our various social media sites. Whether you have a FaceBook, Twitter, or Linked-In account, follow our postings on the latest and greatest in Network Security News!



iSecure, LLC

1159 Pittsford Victor Rd., Suite 140

Pittsford, NY 14534

585-419-8200 / 800-905-8622

www.isecurenet.net

To be removed from this newsletter mailing, please send an email to support@isecurenet.net and write Newsletter Unsubscribe in the subject line.

