In 2012, the Android OS continued to be the number one target for mobile malware. Overall, the number of malware attacks more than doubled from 2011 to 2012. Additionally, cybercriminals continued to expand beyond China and Eastern Europe, focusing their efforts on consumers in the United States, Saudi Arabia and other markets. One of the biggest and most profitable trends for cybercriminals in 2012 was combining mobile malware with social engineering techniques (Phishing and Smishing) to gain access to users’ financial information.
Malware Highlights

Global Infection Rates

- 163% increase in mobile malware: NQ Mobile discovered over 65,227 new pieces of mobile malware in 2012 vs. only 24,794 in 2011.
- 94.8% of malware discovered in 2012 was designed to attack Android devices vs. only 4% targeting Symbian.
- More than 32.8 million Android devices were infected in 2012 vs. 10.8 million in 2011 according to NQ Mobile estimates – an increase of over 200 percent.
- 25.5% of infected mobile devices were in China, followed by India (19.4%), Russia (17.9%), the United States (9.8%) and Saudi Arabia (9.6%).
- 65% of malware discovered in 2012 falls into the broader category of Potentially Unwanted Programs (or PUPs). PUPs include root exploits, spyware, pervasive adware and Trojans (surveillance hacks).
- 94.8% of malware discovered in 2012 was designed to attack Android devices vs. only 4% targeting Symbian.
- 28% of mobile malware discovered in 2012 was designed to collect and profit from a user’s personal data.
- 7% of malware was simply designed to make a user’s device stop working (i.e., “bricking” their phones).
- The three primary methods for delivering malware in 2012 included Smishing, Malicious URLs and App Repackaging.

2012: Top 5 Infected Markets

- China: 25.5%
- India: 19.4%
- Russia: 17.9%
- United States: 9.8%
- Saudi Arabia: 9.6%

App Repackaging

This is the most common method used by malware authors and therefore the most common way for mobile devices and user information to be compromised.

Cybercriminals add lines of malicious code into a genuine app and repackaging and reload it onto a third-party marketplace for unsuspecting mobile users to download and install. Once installed, the app works in the background to collect user data, change user settings, or remotely control the device to send SMS messages.

Malicious URLs

This type of fraud is intended to collect user’s personal information while browsing on mobile devices, especially in regard to major banking and financial institutions.

Cybercriminals, taking advantage of hard-to-see or hidden mobile web URLs, redirect users from a genuine website to a clone website. Upon visiting the malicious website the browser might initiate any number of actions including entering a username and password, downloading fake security updates, or even asking for the user’s mobile number so it can send a malicious URL link.

Smishing

This type of fraud increases the user’s bill to the profit of the malware developer via SMS.

Using social engineering (phishing) along with SMS, consumers are contacted by cybercriminals and asked to click on a malicious link. Clicking the link will trigger a malicious app download or direct the consumer to a rogue website. One of the most efficient and lucrative methods of smishing automatically downloads Premium Rate Service (PRS) images to the infected device. Also called “Toll Fraud,” this method generates as much as $4 USD per SMS for cybercriminals.
Major Malware Discoveries

Bill Shocker

The most infectious and costly mobile malware in history, Bill Shocker infected over 600,000 users in China. NQ Mobile discovered the infection, which spread through popular apps including Tencent QQ Messenger and Sohu News.

Bill Shocker silently installed itself in the background and then attempted to take remote control of the mobile device, internet connections, dialing and texting functions, and upload the contact data. It then turned the device into a “zombie” which allowed it to send PRS SMS without the user’s knowledge.

DyPusher

This malware was capable of uploading device specific information (i.e. IMSI, IMEI, mobile number, system number, etc.) as well as dynamically downloading files and apps without the user’s consent, thereby causing loss of privacy and potential bill shock. 210 users were infected by the time DyPusher was discovered by NQ Mobile.

FireLeaker

This malware was disguised as a widget and hidden from view but could collect device specific information (i.e. IMSI, IMEI, mobile number, system number, etc.) and contact data and upload it to a remote server. 13 users were infected by the time FireLeaker was discovered and eradicated by NQ Mobile.

VDloader

This malware ran as a client on an Android device and then requested interaction with a remote server.

The primary infection path was via an SMS link, using social engineering techniques to target victims. Upon clicking the link, the malware would hide inside a genuine application and only broadcast when requested.

This malware was the first to be found - by any global security vendor - with the ability to automatically upgrade itself. 1,714 users were infected by the time VDloader was discovered and innoculated by NQ Mobile.

DDSpy

DDSpy disguised itself as Gmail and ran silently in the background. It showed no icon and hid itself in the app list, communicating with its command and control server via SMS. This was discovered as a client-side Trojan malware. DDSpy included a GPS hook, whereby location-based malware can be set to activate based on a specific GPS or cell site location.

This type of location-based malware is more difficult to detect and could evade mobile anti-virus scanning engines. By hiding the malware, the authors did not have to re-engineer the malcode as often and kept their development costs down.

© 2007 - 2013 NQ Mobile™

NQ Mobile’s Security Labs discovered a number of new pieces of mobile malware, including the largest driver of SMS Toll Fraud ever discovered.

© 2007 - 2013 NQ Mobile™

NQ Mobile Discovery: Bill Shocker

© 2012 Security Report

Web Site: www.nqmobile.com | Contact Us: info@nqmobile.com | NQ Mobile | © 2012 NQ Mobile™
While instances of malware infections did not significantly increase from 2011 to 2012 in the U.S., the market is an attractive target for cybercriminals. NQ Mobile expects to see an increasing number of attacks on smartphones in the region.

Android Fragmentation

39%

Two years after its introduction, more than 39% of Android users are still using Gingerbread.¹

As a result, these mobile consumers are lacking many of the major security updates provided by Ice Cream Sandwich and Jelly Bean.

App Sideloadng

More and more Android users can now download and install mobile apps outside of Google Play.

This means that more users than ever are able to visit and download apps from third party marketplaces, where the majority of malicious apps are being hosted.

Young Smartphone Users

58%

According to Nielsen 58% of children aged 13-17 in the United States own smartphones.²

This is a demographic that not only downloads more apps (41 on average) but is also more open to downloading content and apps outside of Google Play (46%).³

Behavior Changes Needed

52%

In the US, Only 52% of consumers reported requiring a passcode or other authentication method to access their device.³

While consumers who have lost a smartphone or had one stolen in the past are significantly more likely to be taking basic protective measures with their current device, nearly one-third have still not learned their lesson.

3. This survey was conducted online within the United States on behalf of NQ Mobile from February 22-25, 2013 among 413 adults ages 18 and older. This online survey is not based on a probability sample and therefore no estimate of theoretical sampling error can be calculated.