2013 Mid-Year Mobile Security Report

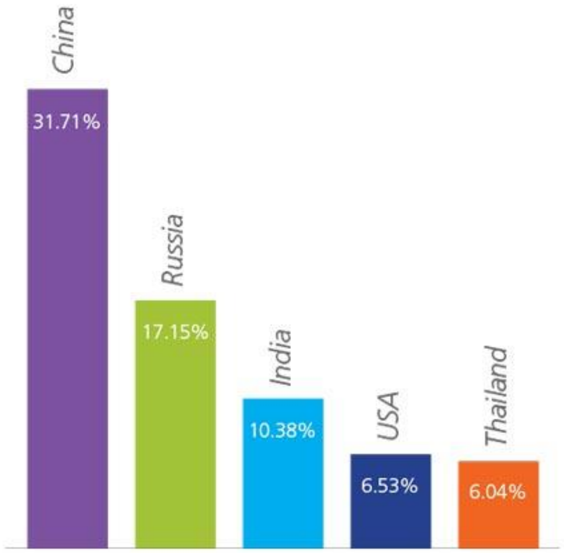
2013 NQmobile™
Mid-Year Security Report

***In the first half of 2013, NQ Mobile identified more than* 51,000 new threats*, responsible for* infecting an estimated 21 million mobile devices.**

China, Ukraine and Saudi Arabia saw the highest growth in mobile malware infections.

Malware Market Movers

- **China**: With 6.7 million devices infected in the first half of 2013, a 43 percent increase over 1Q to 2Q 2012, China continued to be the leading market for mobile infections.
- **Ukraine**: Growing 485 percent from 1Q to 2Q, Ukraine saw the most dramatic increase in mobile infections. **Russia** and Ukraine together now account for almost 20 percent of the world's mobile infections.
- **Saudi Arabia**: With infections increasing more than 28 percent, malware in Saudi Arabia now represents almost 6 percent of the world's total.
- **Southeast Asia**: With **Indonesia**, **Malaysia**, **Thailand** and **Vietnam** all making the top ten, Southeast Asia dominates the list of most infected markets. This region represents about 12 percent of the world's total mobile malware infections.
- **USA**: Although mobile infections in 2Q vs. 1Q 2013 dropped 63 percent, the USA maintained a spot in the top 10 most infected markets. At #4, the US accounts for 6.5 percent of the world's malware infections.
- **India**: The most dramatic reduction in total malware infections was seen in India, with an 88 percent decrease from Q1 to Q2, yet India remained the #3 most infected market.



Source: NQ Mobile

Inside the Numbers

51,084

threats identified during the first half of 2013.

21 million

devices infected during the first half of 2013.

43%

of malware discovered in 2013 falls into the broad category of Potentially Unwanted Programs (or PUPs). PUPs include root exploits, spyware, pervasive adware and Trojans (surveillance hacks).

32%

of mobile malware discovered in 2013 was designed to collect and profit from a user’s personal data.

23%

of malware was designed to simply make a user’s device stop working (i.e., “bricking their phones”).

Top 3 methods for delivering malware in 2013:

App Repackaging

This is the most popular 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 repackage 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.

Malware developers, 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 user's browser might then 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.

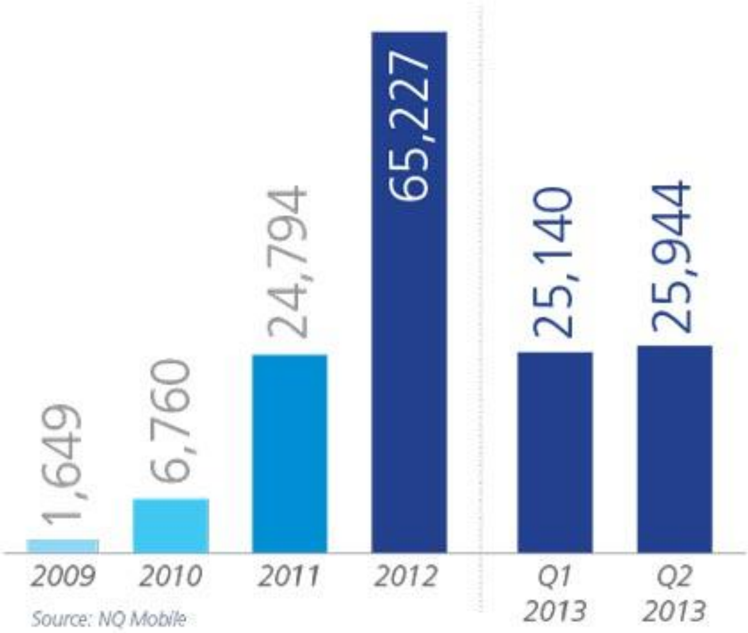
Smishing

This type of fraud uses SMS to increase the user's bill, to the profit of malware developers.

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.

Malware Discoveries, 2009 – Q2 2013

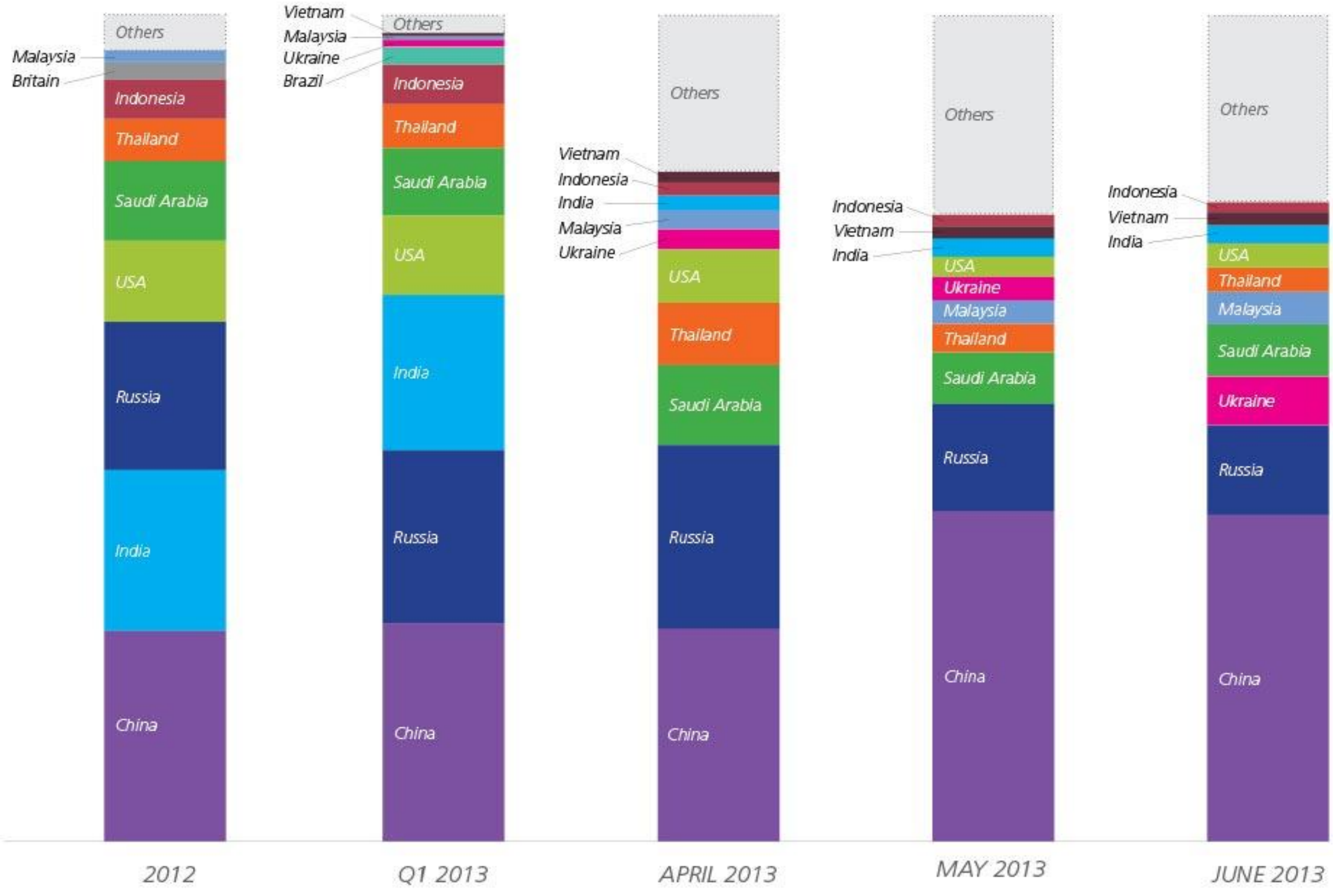
The 51,084 malware discoveries from the first half of 2013 represent **over 78% of the total from 2012.**



Source: NQ Mobile

Top 10 Infected Countries

Over the past 18 months the same 13 countries have been seen on the top ten list, but positions have changed. The US and India *have dropped, while Ukraine and China have grown significantly.*



Source: NQ Mobile

NQ Mobile’s Proprietary Tools and Resources

NQ Mobile’s 2013 Mid-Year Security Report is based on insights from NQ Mobile’s Security Lab, a team of over 250 mobile security professionals, scientists and developers around the world who proactively monitor the mobile landscape for new malware threats and mobile hacking methods. This report is also based on data collected from NQ Mobile proprietary tools and services.

NQ Sense™

372 million registered user accounts and 122 million active user accounts help provide real-time data on new malware and global infection rates.

NQ Crawler™

In 2012, our crawler scanned over 2.2 billion URLs, and discovered over 5.4 million fraudulent URLs.

NQ RiskRank™

In 2012, our RiskRank algorithm scanned 5.3M apps in 406 marketplaces around the world.