NQ Mobile
2011 Mobile Security Report

An In-Depth Look at Mobile Threats, Vulnerabilities, and Challenges

NQ Mobile examines the current state of mobile devices and the security and privacy risks that plagued these devices in 2011. We also predict future threats for mobile devices for 2012 and beyond.

Published: February 2012

About This Report

The findings in this report are based on data collected and analyzed by the NQ Mobile Security Research Team through the NQ Mobile Threat Database, which is the largest and most sophisticated mobile threat detection and monitoring database in the world.

Each of NQ Mobile's more than 120 million users are part of our mobile security cloud-based intelligence network, contributing new security knowledge to our database and helping us detect virus samples, malicious URLs and other threats. Our database includes data from approximately one million applications and one billion URLs from various sources, including the Android Market, Windows Phone Marketplace and Apple App Store, as well as third-party application markets, where many malicious applications originate.

The NQ Mobile Security Research Team, which consists of more than 250 security experts, constantly monitors and analyzes threat activity, capturing threats and attacks that provide valuable insight into malware and hacking methods. We used this data to provide an in-depth look at how cyber criminals are exploiting gaps in mobile security, as well as to predict what types of threats consumers can expect to encounter in 2012 and beyond.

2011 Mobile Security Report: General Findings

The need for safer mobile environment truly became a necessity in 2011

Executive Summary

2011 was an eventful year for mobile security. Rumors and truth over Carrier IQ and spyware concerns dominated the media for months, mobile hacking incidents endangered reputations of celebrities and politicians, and Android saw a 472% increase in mobile malware from July to November 2011. When you consider just these few major incidents, it's clear that mobile threats are taking center stage in the minds of consumers, the media and the mobile industry as a whole.

The NQ Mobile Security Research team saw two clear trends when assessing data from 2011:

1. A major increase in the number of malicious smartphone applications and related websites
2. A dramatic increase in the sophistication of the techniques used by cyber criminals to exploit vulnerabilities on smartphones

While we're still seeing the same simple, malicious malware we've seen for many years, rootkits, botnets and other advanced forms of malware are becoming more of a concern for our security experts. As a result of these trends, the number of infected phones is significantly higher, and the impact of mobile attacks is exponentially greater. This trend is expected to continue as financial gain is becoming a reality for scammers, who see tremendous value in the new wave of mobile shopping and banking.

At NQ Mobile, our number one priority is to educate smartphone users about the threats they face when using their devices and help them protect their devices (and everything on them). The 2011 Mobile Security Report provides valuable insights on what we learned from our 2011 statistics and trends.

Our key findings are highlighted below:

- By the end of 2011, mobile malware reached the highest overall growth levels in history. A total of 24,794 mobile malware threats were detected in 2011—a 1,503% increase from the 1,649 threats discovered in 2009 and a 367% rise over 6,760 threats in 2010.
- On a month-to-month basis, new Android malware threats rapidly increased on a month-to-month basis, while new Symbian malware threats steadily declined. For the first time in history, starting in October, the number of new Android pieces of malware discovered each month exceeded the number of new Symbian pieces of malware.
- Within a single year, the number of Android malware threats increased from less than 500 samples in January to more than 9,900 threats in December 2011—a staggering 1,880% increase.
- The possibility in alternative markets is two orders of magnitude higher than that in the official marketplace.
- In 2011, more than 10.8 million Android devices were infected. The top five infected countries were China (31.6%), India (13.5%), the United States (11.3%), Russia (10.5%), and the United Kingdom (7.3%).
- By the end of 2011, the possibility of a mobile user encountering a malicious application in official and alternative Android marketplaces was 0.04% and 2.20%, respectively. When you consider that these June 2011 numbers were 0.02% and 0.35% in June 2011, the risk increased dramatically in just six months.

Introduction

Adoption of smartphones and mobile devices reached an all-time high in 2011. As adoption grows, so does the need for mobile security.

The mobile industry experienced a remarkable transformation in 2011. From well-publicized debates over how personal information is collected from mobile devices to the evolution of smartphones into mobile wallets, mobile devices—and the threats to them—made many headlines. If you consider how many people are using smartphones nowadays, it's easy to see why such headlines get attention. Smartphone shipments surpassed PC shipments for the first time in 2011, according to market research firm Canalys [1], with 487 million units shipped in 2011, up from the 299 million units shipped in 2010.

In many parts of the world, smartphones are now replacing PCs, thanks to new features that make them just as (if not more) capable as computers. The release of feature-rich devices like the iPhone 4S and Galaxy Nexus S in 2011 put a spotlight on just how "smart" smartphones have become.

Unfortunately, as more people used smartphones to do more things, especially activities that involved banking or credit card details, the risks associated with using them increased as well. While mobile application developers were hard at work this year finding new ways to make mobile banking, shopping and surfing faster, easier and more convenient, cyber criminals were working just as hard to find innovative ways to steal personal and financial data and wreak havoc on smartphones. Both groups did a phenomenal job—the developers delivered phones and applications with features we couldn't have even imagined just a few years ago; and the criminals became undeniably clever, releasing malware at an unprecedented rate with increased sophistication and strength.

The need for a safer mobile environment became an absolute necessity in 2011, as mobile threats demonstrated strong capabilities in these areas:

- Escalating privileges
- Controlling infected devices (botnets)
- Incurring financial charges
- Stealing private data

For years, analysts and experts have been predicting that malware and other security threats would soon be as big a problem for mobile devices as they are for PCs. The rampant rise of malicious mobile applications and related command-and-control (C&C) websites we found in 2011, along with the sharp increase in complexity and sophistication we saw in last year's attacks, clearly show that unprotected mobile devices have now become just as risky or possibly even riskier than unprotected PCs.

To highlight an important category of risk, in 2011, the number of compromised Android devices communicating with known malicious C&C networks grew significantly. This represents a worrisome trend in the evolution of mobile malware. Until last year, mobile exploits typically didn't involve a hostile takeover of the device and active communication with a C&C botnet. This two-way online communication proves beyond a doubt that mobile devices are as susceptible to breaches and botnets as PCs.

NQ Mobile has been completely dedicated to mobile security since its inception in 2005. Our top priority is to educate consumers on the risks associated with using smartphones and make sure they can easily download necessary mobile security solutions to get complete protection for their mobile devices. To fulfill this mission, we built the world's largest and most sophisticated mobile security network, which gives us the information we need to identify and resolve emerging mobile threats (such as new malware or phishing attacks) before they have a chance to harm consumers. Specifically, our system contains more than one billion links and one million applications gathered from a variety of sources including official and alternative mobile application markets, such as the official Android Market and App Store.

The accumulated knowledge base provided by our network gives us our competitive advantage—the ability to quickly identify and resolve more than 75% of mobile threats around the world before our competitors. It also gives us the data we need to fully understand how mobile threats are evolving, which helps us stay several steps ahead of them.

Our research team collected and analyzed information from our network, using the database to identify relevant 2011 statistics; describe the evolution, functionality, and infection strategies of the top mobile threats; and predict future possibilities for mobile attacks. Along with this analysis, NQ Mobile provides a comprehensive guide for best practices for consumers to adhere to in order to protect themselves from the dangers of the current mobile security threat landscape.

2011 Mobile Threat Statistics

Just like threats to PCs, threats to mobile devices range in volume and severity, but all can potentially wreak havoc at the device and network levels. The most common mobile threats seen by NQ Mobile researchers in 2011 include phishing attacks, in which scammers use various tactics to trick users into sharing their personal or financial data, and spyware, which tracks users' activity for malicious or marketing purposes. Other threats include Trojans, which are programs that look genuine but hide malicious code, and man-in-the-middle attacks, in which scammers intercept and manipulate messages between two devices.

The threats we've discovered are similar to ones that have been plaguing PCs for many years and it's becomingly increasingly clear that mobile devices are just as vulnerable to the types of security threats that cause financial and personal loss to PC owners. However, the need for protection is not as well understood. In 2012, we hope this will change, as mobile device users learn more about the risks associated with using smartphones to do all the things they're used to doing on their PCs, such as emailing, shopping, banking, playing games and more.

Just like traditional PCs and other server platform counterparts, modern mobile platforms are subject to a variety of security threats. Among existing mainstream mobile platforms, Google's Android has become the most popular mobile platform among smartphone users, which unfortunately has also made it the most targeted mobile platform by cyber criminals. This is a recurring trend in mobile security—the more popular a platform becomes, the more targeted it is by malware authors and other cyber criminals.

In the following sections, we summarize mobile threats in four main categories: mobile malware growth, geographic distribution of malware, malware population and malicious websites in existing mobile markets.

Android has become the most popular mobile platform among smartphone users, which unfortunately has also made it the most targeted mobile platform by cyber criminals.

Mobile Malware Growth

As the popularity of mobile devices increased, the growth of mobile malware steadily grew from 1,649 threats in 2009 to 6,760 threats in 2010. However, in 2011, it jumped to 24,794 threats. The number has skyrocketed every year, and based on the current pace of smartphone use, we fully expect this trend to continue.

Mobile malware trends are greatly influenced by the popularity of mobile platforms. A closer look at the detailed monthly growth of mobile malware targeting Android and Symbian platforms shows how the popularity of Android phones caused a significant growth in malware targeting Android in 2011.

Monthly Growth of Android and Symbian Malware

Figure 2 shows the monthly growth of new pieces of Android malware cases discovered in 2011. It's not surprising that Android, which is one of the most popular mobile platforms, attracts the attention of malware writers. Specifically, the number of Android malware threats increased from less than 500 at the beginning of January 2011 to more than 9,900 at the end of December 2011, leading to a staggering 1,880% increase within a single year.

In Figure 3, we'll contrast these findings by showing the monthly growth of new malware targeting the Symbian platform. Clearly, there is a steady decline of new malware threats discovered each month that affects the Symbian platform. This shows that malware writers target the most popular mobile platforms. However, it should be noted that, due to the presence of a relatively large user base, the Symbian platform is still an attractive target for malware authors.

To better understand the malware growth trend, we re-positioned the numbers of new Android and Symbian malware in Figure 4. This graphic better illustrates the malware dynamics in the two mobile platforms. Specifically, the figure also indicates that starting in October 2011, the number of new Android malware already exceeds the number of new Symbian malware. With the continued increase of the Android platform (and the continued decline of the Symbian platform) by market share, we expect to discover more Android malware in the future.

Figure 1: Overall Mobile Malware Growth

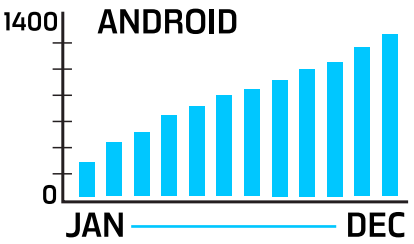


Figure 2: Month-by-month Growth of Android Malware in 2011

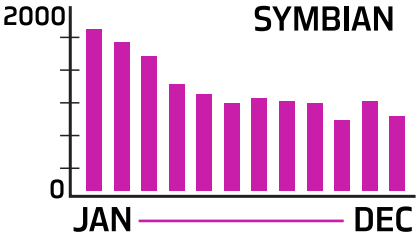


Figure 3: Month-by-month Growth of Symbian Malware in 2011

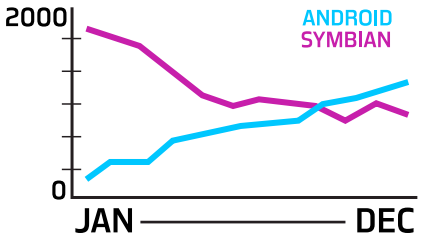
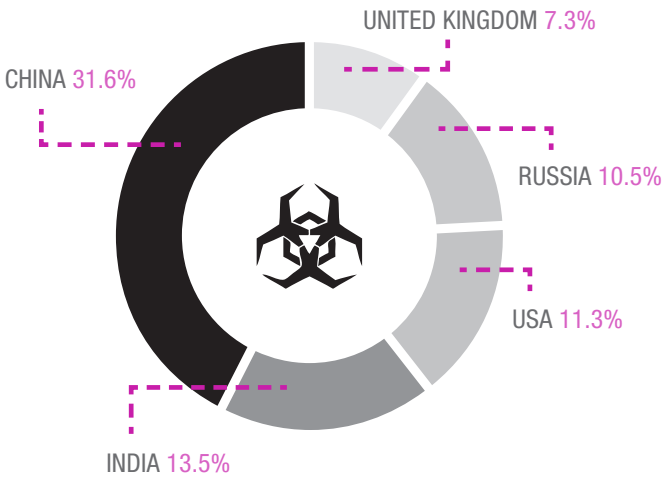


Figure 4: Month-by-month Growth of Mobile Malware Targeting Android and Symbian Platforms

Geographic Distribution of Mobile Malware

In 2011, more than 10.8 million Android devices around the world were infected. Among these infected devices, Figure 5 shows their geographic distribution.

In terms of the total number of infected Android devices, the top five countries are:



The list seems to be consistent with the popularity and user bases of smartphones and mobile devices in these countries. The more popular and widely used smartphones are in a particular region, the higher the number of infected phones in that region.

In terms of the percentage of infected Android devices within a particular country or region, the top five are: