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, while new Symbian malware threats steadily declined.

  For the first time in history, starting in October 2011, the total 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.
- 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%).
- The possibility of finding Android malware in alternative markets is two orders of magnitude higher than it is in the official marketplace.
- 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

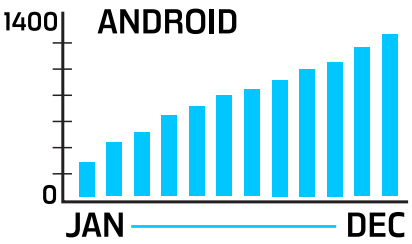


Figure 2: Month-by-month Growth of Android Malware in 2011

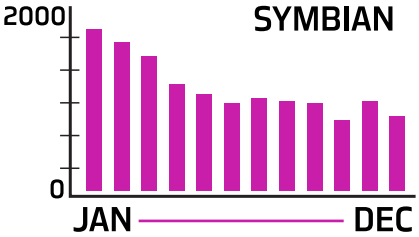


Figure 3: Month-by-month Growth of Symbian Malware in 2011

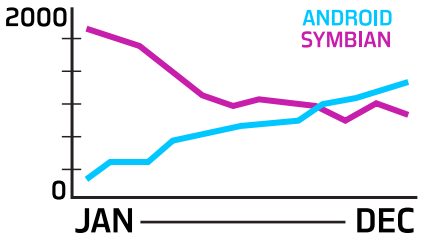
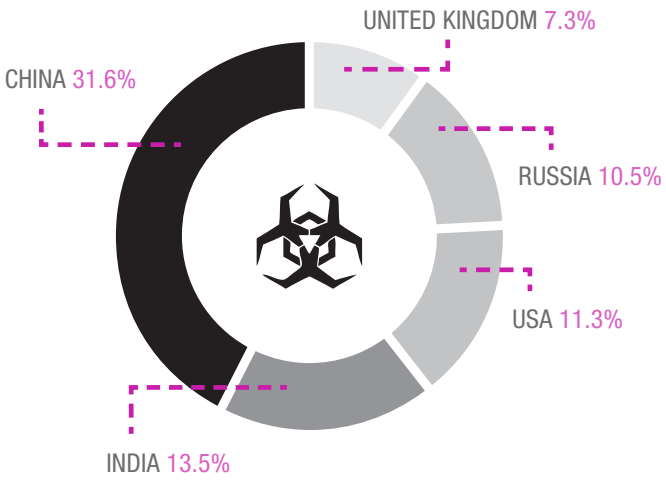


Figure 4: Month-by-month Growth of Mobile Malware Targeting Android and Symbian Platforms

Geographic Distribution of Mobile Malware

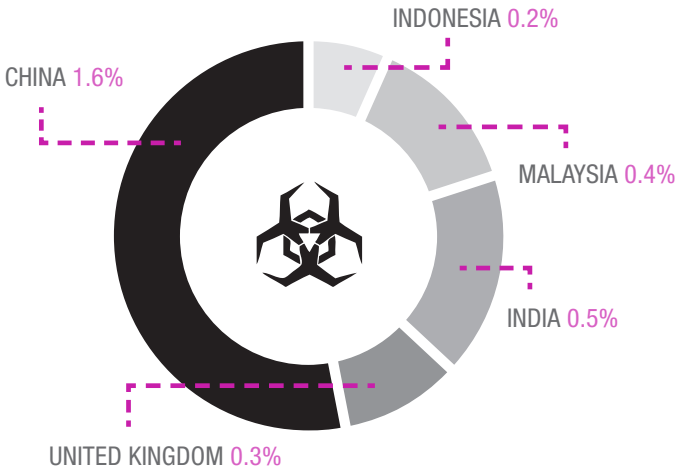
In 2011, more than 10.8 million Android devices around the world were infected. Among these infected devices, Figure 5 shows their geographic distribution.

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:



Immediately following the list, the United States of America is ranked sixth, with 0.2% of Android devices being infected at least once in 2011.

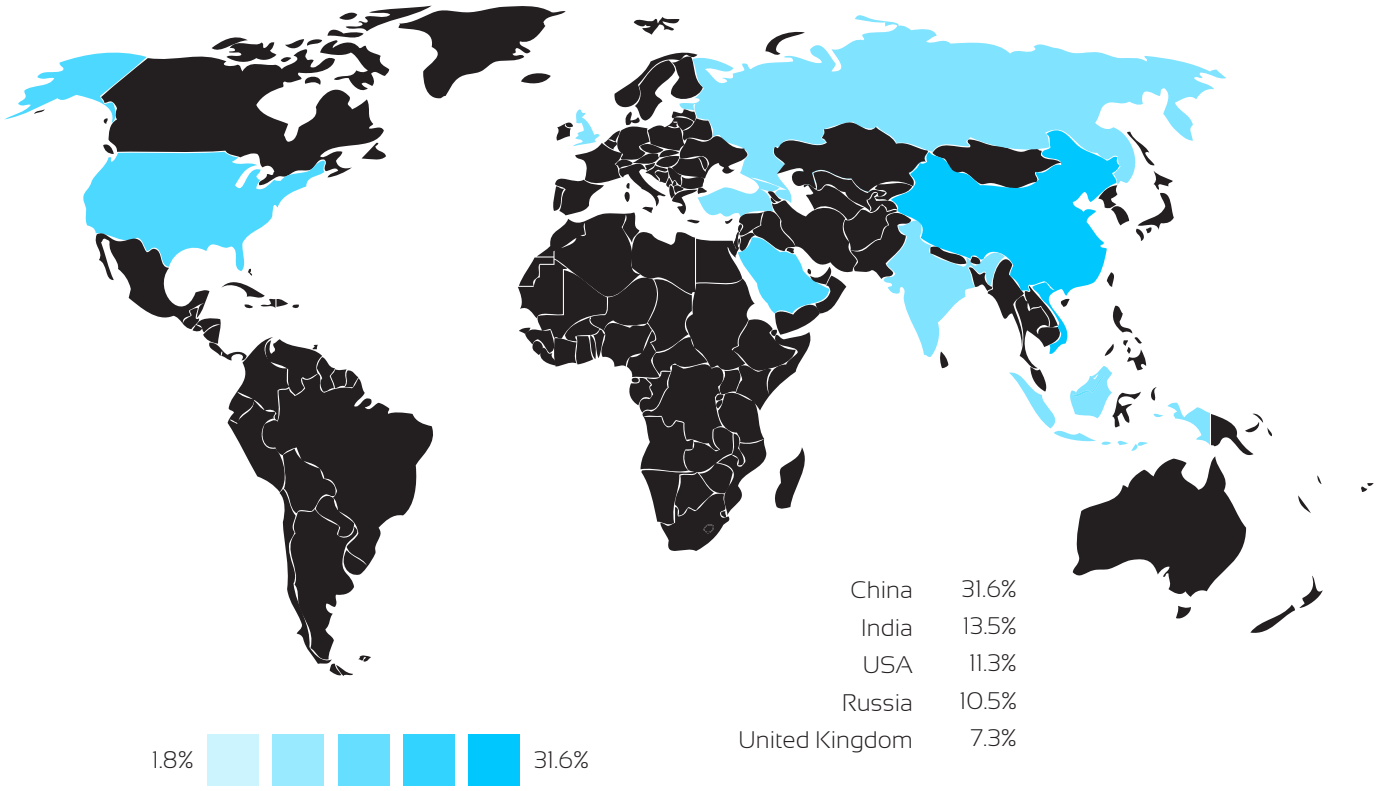


Figure 5: Geographic Distribution of Infected Android Devices

Likelihood of Infection in Android Markets

The presence of various mobile application markets and centralized models of mobile application distribution provide convenience for both application developers and mobile users. While mobile users enjoy the convenience to browse, search and install mobile applications, this same centralized model of mobile distribution also provides the "convenience" for malware writers to distribute malware. In addition, the presence of mostly unregulated third-party mobile markets significantly contributes to the likelihood that mobile users will encounter a malicious application.

Our statistics show that, by the end of 2011, the possibility of a mobile user encountering a malicious application in official and alternative Android markets was 0.04% and 2.20%, respectively. In June 2011, the possibilities were 0.02% and 0.35%, respectively. The possibility of encountering malicious applications in alternative Android markets was two orders of magnitude higher than the same possibility in the official marketplace.

Likelihood of Infection in Web Browsing

Web browsing presents another avenue for malware infection. Figure 6 shows the monthly growth of malicious URLs, in terms of the percentage of traversed URLs that are malicious. Overall, the infection likelihood of clicking a malicious URL nearly doubled from 0.18% to 0.31%. This statistic is alarming, as users are relying on mobile devices for Web surfing more than ever.

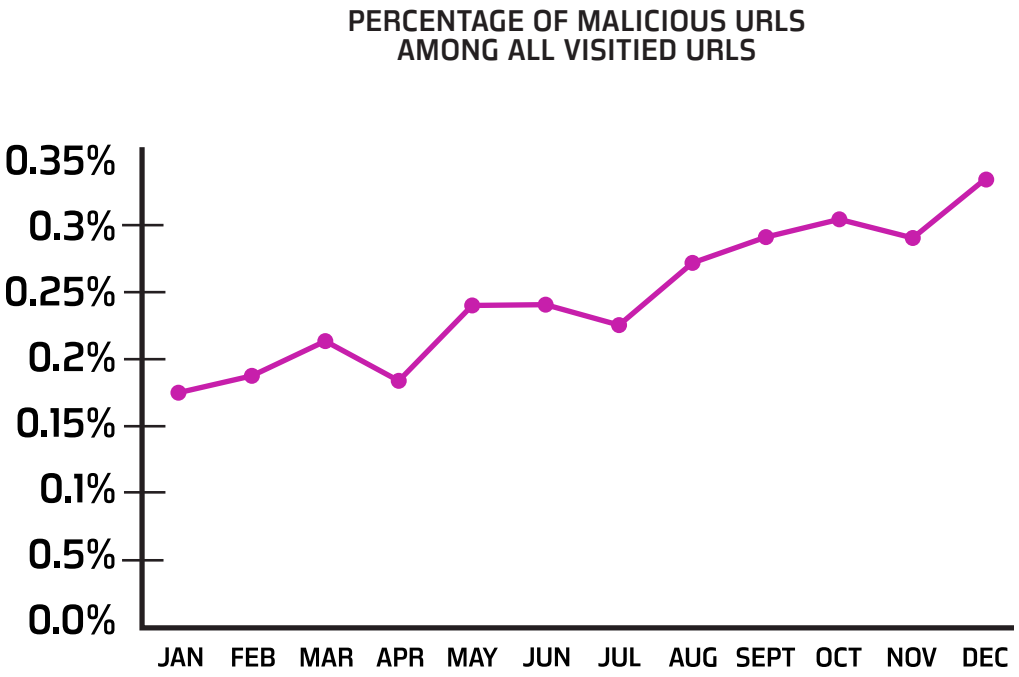


Figure 6: Month-by-Month Growth of Malicious URLs

How Malware Authors Infect Smartphones

The growing popularity of the open Android platform and the accompanying rampant growth of Android malware warrant an in-depth investigation. To better understand this constantly evolving category of malware, the NQ Mobile Security Research Team investigated the evolution of Android malware, the most common methods used by malware authors to infect users' devices and the built-in functionalities in their payloads.

The Evolution of Malware Families

In 2011, mobile malware demonstrated impressive growth and posed significant technical challenges. Specifically, mobile malware authors are not only actively applying advanced malware infection techniques from the traditional (and relatively mature) PC arena, but are also developing new exploits and attacks unique to the mobile industry.

In Figure 7, we show the evolution of 83 Android malware families that were discovered last year. The growth sharply escalated in the second half of 2011, with more than 71% new malware families.

Among existing malware families, several are significant in size. For example, PJapps [18] is a large family with several hundred threats. DroidKungFu [4][6] is another large family with more than 1,000 threats in different variants to bypass the detection from existing mobile anti-virus software. AnserverBot [3] also has several hundred threats that evolved from the earlier BaseBridge [2] family by borrowing infection techniques from Plankton [5].

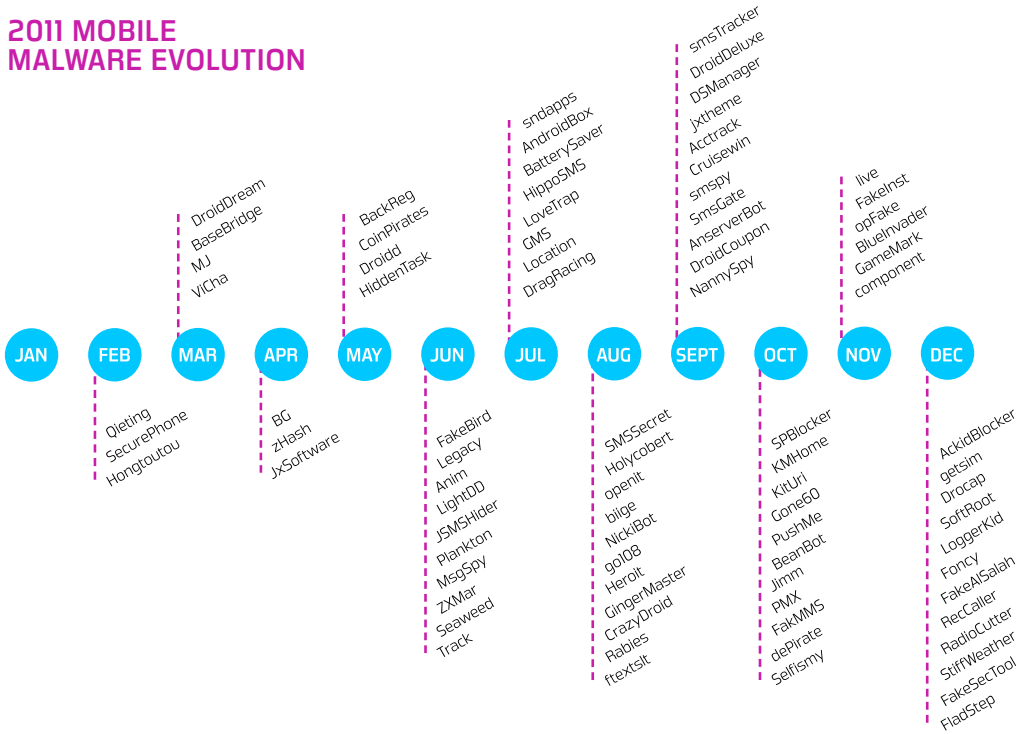


Figure 7: The Evolution of 83 Android Malware Families Reported in 2011

Malware Infection

Mobile malware uses a variety of techniques to infect mobile devices. To gain a better understanding of these techniques, we systematically analyze existing malware in our database and categorize their installation techniques. In the following section, we elaborate on three of them. These techniques aren't mutually exclusive, as different variants of the same malware family might use different techniques to entice users to download.

#1: Piggybacking on Legitimate Apps

One of the most common techniques used by malware authors in 2011 was "piggybacking" malicious payloads into popular mobile applications (such as Angry Birds). Piggybacking allows malware authors to find popular applications; download and disassemble them; add additional malicious payloads; re-assemble them; and submit the reassembled applications to various Android markets. Malware authors then use a variety of techniques to get users to download and install their infected applications. Our researchers found that 80% of existing malicious applications on Android markets are repackaged. The most popular types of malicious applications for repackaging include popular game applications, powerful utility applications (including security updates) and pornography-related applications.

In the piggybacking process, possibly because they're trying to hide piggybacked malicious payloads, malware authors tend to use common names that look legitimate and benign. For example, AnserverBot [3] malware uses the package name com.sec.android.provider.drm as its payload, which looks like a module that provides legitimate DRM functionality. DroidKungFu [4] originally chose to use com.google.ssearch to disguise itself as the Google search module but a later version [6] used com.google.update to pose as an official Google update.

#2: Upgrading Legitimate Apps to Malicious Ones

Piggybacking typically encloses the entire malicious payload into original legitimate applications, which could potentially expose their presence. This second technique makes detection difficult. While it may still repackage popular applications, rather than enclosing the payload as a whole, it only includes an upgrade component that will fetch or download the malicious payloads at runtime. As a result, a static scanning of host applications may fail to capture the malicious payloads. In our dataset, there are several such types of malware, including BaseBridge [2], AnserverBot [3], and Plankton [5].

For example, Figure 7-1 shows the upgrade attack from a BaseBridge variant [2] that was first discovered by NQ Mobile. In particular, when this type of infected application runs, it will check whether an upgrade dialogue needs to be displayed. If the answer is yes, the user is given the option to install the updated version. The new version can be stored in the host application as a resource or asset file or dynamically downloaded from an attacker-controlled server. If the user accepts the update request, an "updated" version with the malicious payload is installed (Figure 7-2). Because the malicious payload is in the "updated" app, not the original application itself, this method is stealthier than the first technique that piggybacks the entire malicious payload within the original application.

Besides installing a new version of the mobile application, some sophisticated variants of upgrade attacks may stealthily upgrade certain components in the host application, not the entire application. As a result, it does not require user approval. For example, Plankton [5] directly fetches and runs additional code maintained in a remote server while AnserverBot retrieves a public (encrypted) blog entry, which contains the actual payloads for update! In Figure 8, we show the actual network traffic to download the AnserverBot payload from the remote command and control (C&C) server. The stealthy nature of these upgrade attacks poses significant challenges for their detection.

Figure 7-1: The Upgrade Attack from the BaseBridge Malware

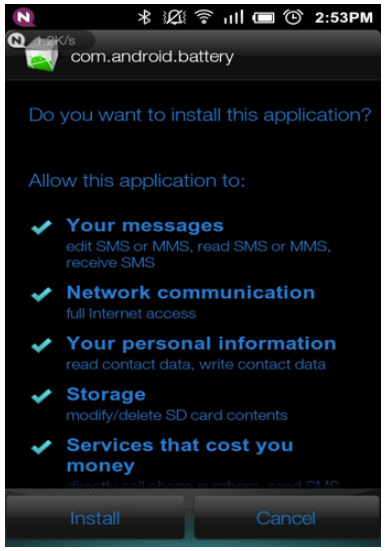


Figure 7-2: The Upgrade Attack from the BaseBridge Malware

```
GET /s/blog_8440ab780100t0nf.html HTTP/1.1
User-Agent: Dalvik/1.2.0 (Linux; U; Android 2.2.1;
        generic Build/MASTER)
Host: blog.sina.com.cn
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/0.7.62
Date: Wed, 21 Sep 2011 01:44:16 GMT
...
v____:yjEJTT1SvSSVSGRp9NASSSSS<wbr>SSSSSSSSSSSkSSSS7WB5
rthy<wbr>0V3JeJ4q96sSrc50s7g6Wsz8<wbr>hJn99P606UaRgkSZsu
...
```

Figure 8: The Upgrade Attack from the AnserverBot Malware

#3: Enticing Users for Downloads

The third technique applies the traditional drive-by download attacks to the mobile space. Though they aren't directly exploiting mobile browser vulnerabilities, they're enticing users to download "interesting" or "feature-rich" apps. Some representative examples are Jifake [7], Spitmo [8], ZitMo [9], and GGTracker [10].

Specifically, the Jifake malware is downloaded when a mobile user is redirected to a malicious website. Instead of using in-application advertisements to attract and redirect users, the malware is based on malicious QR code, which, when scanned, redirects the user to another URL that contains the malware. The malware itself is a repackaged mobile ICQ client that sends short SMS messages to a hardcoded premium rate number.

The Spitmo and ZitMo examples are also worth mentioning. In essence, they're ported versions of nefarious desktop PC malware, such as SpyEye and Zeus. The two work in a similar manner: when a user is conducting online banking activities with a compromised PC, the user is redirected to download a smartphone application, which promises better online banking protection. However, the downloaded application is really malware, which collects mTANs or SMS messages to a remote server. These two malware families rely on the compromised desktop browsers to launch the attack. While it is difficult to infect users this way, the fact that criminals can steal sensitive bank information this way is a major concern.

In addition to the three installation techniques listed above, malware authors also create fake applications and masquerade them as original legitimate ones. Behind the scenes, they can stealthily perform malicious actions, such as stealing user credentials or sending SMS messages in the background. For example, FakeNetflix [11] steals a user's Netflix account and password. FakePlayer [12] masquerades as a movie player but doesn't play movies at all. Instead, it sends premium SMS messages without the user's knowledge. Similarly, Walkinwat [13] pretends to be a popular paid application -- Walk and Text -- on the official Android Market. However, after it's installed, it does nothing but steal the user's information and send unauthorized SMS messages to all the contacts stored on the phone.

Malware Capabilities

In addition to the various malware infection methods, we also investigated the various functionalities in the carried payloads. We partitioned the payload functionalities into four representative categories. They aren't mutually exclusive, as malware variants often have payloads with different functionalities.

Escalating Privileges (e.g., Root Exploits)

The Android platform is a complicated system that consists of not only the Linux kernel, but also the entire Android framework, which includes more than 90 open-source libraries. Its complexity naturally introduces software vulnerabilities that can be potentially exploited for privilege escalation. Overall, there are a small number of platform-level vulnerabilities that are being actively exploited in the wild. These exploits include exploid [21], RageAgainstTheCage [22], and Zimperlich [23].

Our analysis resulted in one particularly alarming result: approximately one-third of our studied dataset contained a root exploit to escalate privileges and bypass the built-in security mechanism in Android. Also, it's common for malware to have two or more root exploits to maximize its chances of successful exploitations on multiple platform versions.

A further investigation on how these exploits are used revealed that many earlier malware examples simply copied verbatim the publicly available root exploits without modifying them. Some didn't even remove the original debug output strings or change the file names of associated root exploits. For example, DroidDream [20] contained the exploid file name, which was exactly the same as the publicly available one. However, things have changed recently. For example, DroidKungFu [6] doesn't directly embed these root exploits. Instead, it first encrypts these root exploits and then stores them as a resource or asset file. At runtime, it dynamically uncovers these encrypted root exploits and then executes them properly, which makes it very challenging to detect them. Other recent malware examples, such as DroidCoupon [14] and GingerMaster [15], obfuscate the file names of the associated root exploits (for instance, by posing as picture files with the .png suffix). These recent changes reflect the evolving nature of malware development and the ongoing arms race for malware defense.

Controlling Infected Devices (e.g., Botnets)

While investigating the remote control functionality among the malware payloads, we were surprised to find that more than 90% of them have server-side components, which can be used to turn the compromised phones into botnets and control them through a network or short messages. Specifically, the majority of them use HTTP-based traffic to receive bot commands from their own C&C servers. To hide them from detection, existing malware typically encrypts the URLs of remote C&C servers, as well as the related communication with them. For example, Pjapps [18] uses its own encoding scheme to encrypt the C&C server addresses. DroidKungFu [6] employs the standard AES encryption scheme and Geinimi [19] similarly applies DES encryption scheme to encrypt its communication with remote C&C servers.

Using remote controlled infected devices, malware authors can flexibly push down or install additional payloads. For instance, FakeBird [25] reported by NQ Mobile in June 2011, disguised itself as the popular Angry Birds application and used the remote C&C server to fetch browser bookmarks and payload applications for installation. DroidLive [26], also reported by NQ Mobile in November 2011, connected to the remote server for an instruction file, which was used to control which premium numbers would be used in SMS scams.

Our investigation revealed that most C&C servers are registered in domains controlled by the attackers themselves. However, we also identified threats where the C&C servers are hosted in public clouds. For instance, the Plankton spyware [5] dynamically fetches and runs its payload from a server hosted on the Amazon cloud. Most recently, attackers are even turning to public blog servers as their C&C servers. AnserverBot [2] is one sample that uses two popular public blog services, Sina.com and Baidu.com, as its C&C servers to retrieve the latest payloads and new C&C URLs.

Incurring Financial Charges (such as SMS Scams)

In addition to using malware payloads to escalate privileges or remotely control infected devices, additional motives for installing malware are tied to financial gain.

One profitable malware method is surreptitiously subscribing to (attacker-controlled) premium-rate services. Sending SMS messages from an infected device is the most common way to do this. On Android, there's a permission-guarded function (sendTextMessage) that allows cyber criminals to send an SMS message in the background without the victim's awareness. Our database showed this type of attack in Russia, the United States, Singapore and China:

- The very first Android malware FakePlayer [12] sent the SMS message "798657" to multiple premium-rate numbers in Russia.
- GGTracker [10] automatically subscribed infected users to premium services in the U.S. without the user's knowledge.
- Similarly, HippoSMS [16] and MJ [29] send SMS messages to premium-rate numbers in China without the user's consent.

Some malware authors don't use hard-coded premium-rate numbers. Instead, they leverage the flexible remote control to push down the numbers at runtime. These malware families are stealthier than earlier ones because the destination number can't be revealed by statically analyzing the infected applications. For example, BatterySaver [30] sends SMS messages according to whatever the C&C server instructs in Singapore.

To automatically subscribe to premium services, these malware families need to reply to certain SMS messages. Specifically, in China, to sign up for a premium service, the user must reply to a confirmation SMS message sent from the service provider to finalize or activate the service subscription. To keep users from being notified, the malware will simply reply to these confirmation messages themselves. For example, RogueSPPush [17] will automatically reply "Y" to such incoming messages; GGTracker [10] will reply "YES" to one premium number, 99735, to activate the premium service. Similarly, to prevent users from seeing subsequent billing-related messages, incoming SMS messages are filtered. This behavior is present in a number of malware threats, including RogueSPPush [17] and GGTracker [10].

Stealing Private Information (Aggressive Adware)

In addition to the above payloads, malware are actively harvesting data on the infected phones, including victims' SMS messages, phone numbers, contacts, call logs and other personal information. For example, MsgSpy [27], which was discovered by NQ Mobile in June 2011, can sniff phone calls, record GPS locations and upload SMS messages. Track [31], which was reported by NQ Mobile in May 2011, automatically replies to incoming SMS messages (using the keyword "TRACK") with the current GPS location. Also, similarly, SndApps [24] collects the victims' email addresses and sends them to a remote server. FakeNetflix [11] gathers its victims' Netflix account numbers and passwords by directing them to a fake but seeming identical Netflix user interface.

To monetize their applications, most application developers include third-party ad libraries. However, some existing ad libraries aggressively abuse permissions granted to the host applications so they can gather personal information stored on the phones. For example, some particular ad libraries upload the list of installed applications on the devices to remote servers. Other ad libraries attempt to collect users' call logs or upload the users' phone numbers or SMS messages. Additional ad libraries might even dynamically fetch and execute code stored on remote servers, which opens up many opportunities for exploitation and abuse and makes it impossible to ensure the integrity of the host applications. Unfortunately, existing defense mechanisms aren't sufficiently fine-tuned to clearly delineate the boundary between intended or unintended ad functionalities. One illustrative example is the recent incident of so-called Counterclank malware, which isn't malicious but comes from an aggressive ad network [28].

In summary, when analyzing the carried payloads, we found numerous alarming statistics:

- Around one-third of the studied malware samples leverage root-level exploits to fully compromise the Android devices' security, posing the highest level of threat to users' security and privacy;
- More than 90% of malware threats have server-side components, which can be used to turn the compromised phones into botnets and control them through a network or short messages;
- About one-half of studied malware samples have built-in support to send short messages to premium-rate numbers or make background phone calls without the victims knowledge; and
- Approximately one-half of studied malware threats harvest user's information, including user accounts, phone numbers and short messages stored on the phone.

A Look into the Future: Predictions for 2012

Mobile platforms are constantly evolving. In 2011, Android gained notoriety as the most popular platform and, as a result, became very popular with malware authors. Based on the current trend of700,000 activations of Android devices per day, we fully expect that the Android malware growth will continue over the next few years.

While platform popularity has a major impact on mobile security trends, we found that most mobile malware threats stem from a desire for personal data or financial gain. As people increasingly use their mobile devices to shop and bank, malware authors know that financial data will be even more easily accessible. For this reason, we expect financial gain to remain the primary driver for most new malware threats in 2012.

Several types of mobile malware that matured in 2011, such as SMS fraud scams and mobile botnets, will continue to evolve in 2012, despite efforts by platform vendors to fight them with advanced defense mechanisms. In particular, we expect to see more attempts by cyber criminals to install malicious rootkits on mobile devices this year. They'll likely use social engineering tactics to trick users into installing the rootkits or piggyback them on repackaged applications. Once installed, rootkits allow scammers to control the phone remotely, steal private data, or drain the device's battery without the user's knowledge.

We also expect to see malvertising and mobile payment-related attacks to surface more frequently and to a more serious degree than they have in previous years, mainly because people have become more comfortable downloading applications by clicking on advertisements. Scammers are aware of this level of comfort and familiarity with mobile advertisements and are now taking advantage of it. We've already seen cases where malware authors purchase mobile advertisements, which they use to coerce people into downloading malicious applications from phony websites that mimic the Android Market and automatically launch drive-by downloads.

Similarly, mobile payment-related attacks are inevitable as more people jump on the mobile payments bandwagon. Many people already check balances, transfer funds and use other financial services on their mobile phones. This trend opens up many opportunities for mobile payment-related attacks and highlights the need for mobile security.

To counter these negative trends, the mobile industry needs to make a stronger effort to educate consumers about the risks associated with using smartphones to text, make calls, email, shop, bank, share photos and more, and teach them how to protect themselves from these risks.

While mobile security companies are working hard to combat the next wave of malware, the masses of unprotected smartphones offer a goldmine of opportunities for cybercriminals. Even if we don't see many new configurations of malware, it's highly likely that we'll see an even higher level of sophistication in the scams already out there. For this reason, it's critical that consumers understand the risks and know how to protect themselves.

2012 HOT TARGETS FOR MOBILE MALWARE

OUR SECURITY EXPERTS SEE THESE AREAS AS HOTBEDS FOR MOBILE MALWARE

1 MOBILE THREAT

PIGGYBACKING

CURRENT USE:

Crafty malware authors are already wrapping malicious code inside the legitimate looking skin of mobile applications like Angry Birds.

WHAT IT DOES:

When the infected application is downloaded, it launches its payload into the heart of your mobile system. Scammers will increasingly find ways to automate this process so they can quickly generate "new" games and service applications.

2 MOBILE THREAT

SMS FRAUD

CURRENT USE:

We saw a major increase in SMS scams in 2011 and expect it to evolve in 2012.

WHAT IT DOES:

Malware authors set up premium texting services that charge users high rates to send SMS messages to specified numbers or collect personal data from infected phones that scammers can use to execute phishing or identity theft scams.

3 MOBILE THREAT

BOTNETS

CURRENT USE:

Popular on PCs but just starting to surface in the mobile world.

WHAT IT DOES:

Mobile botnets take advantage of security gaps to gain root permissions over a mobile device allowing hackers to send messages, make phone calls, access contacts and photos and more. Botnets spread by sending copies of themselves from compromised devices to other devices via SMS or email.

The New Rules of Mobile Protection

Malware authors are getting more sophisticated in their craft, but threats are also coming from users who increasingly use their smartphones to do all the things they do on their PCs but fail to give their smartphones the same protection as their PCs. There's no time like the present to take steps to protect your mobile device.

NQ Mobile recommends a few simple tips that will help keep your phone safe from mobile threats:

- ☐ Be careful when downloading applications or clicking URLs. Only use trusted application markets to download applications, and make sure you check an app's reviews and ratings before you download it. Never click on unknown URLs or respond to requests for your personal information.

- ☐ Make protecting your mobile device as much of a priority as protecting your PC: You wouldn't use your PC without security protection, so why would you take chances with your mobile device? Use an app like NQ Mobile Security to prevent viruses, malware, hacking, eavesdropping and other mobile threats, and protect your data if your phone is lost or stolen.

- ☐ Download the latest software updates for your phone. Make sure your phone is protected by the newest security patches.

- ☐ Disable geo-tagging. When there's no specific need for it, keep your phone's geo-tagging feature turned to the off position. No one needs to know where you are unless there's an agreed-upon plan to track you.

- ☐ Only window-shop when using public Wi-Fi. Don't make purchases or do other financially-related transactions at public Wi-Fi hotspots.

.

About NQ Mobile

NQ Mobile Inc. is a leading global provider of consumer-centric mobile Internet services focusing on security and productivity. NQ is one of the first companies to recognize the growing security threats targeting smartphone users and is now a leading Software-as-a-Service (SaaS) provider with over 120 million registered user accounts worldwide. As a market leader in mobile security, NQ's innovation and global significance have been widely recognized through distinctions, such as the 2011 Technology Pioneer Award from the World Economic Forum.
For more information on NQ, visit www.nq.com

Increases in the number of mobile threats and the sophistication of mobile attacks are scary. However, hopefully these statistics will encourage smartphone users to increase their understanding of mobile security issues and take action to protect their mobile devices, just as they protect their PCs.

References

[1] Canalys. "Smart phones overtake client PCs in 2011,"
http://www.canalys.com/newsroom/smart-phones-overtake-client-pcs-2011, January, 2012

[2] NQ Mobile, "A Technical Analysis of the Anserverbot Trojan,"
http://research.nq.com/?p=145, September 2011

[3] SecurityWeek News, "`Fee-Deduction' Malware Targeting Android Devices Spotted in the Wild ,"
http://www.securityweek.com/fee-deduction-malware-targeting-android-devices-spotted-wild, , May 2011

[4] Xuxian Jiang, "Security Alert: New Sophisticated Android Malware – DroidKungFu – Found in Alternative App Markets,"
http://www.csc.ncsu.edu/faculty/jiang/DroidKungFu.html, June 2011

[5] Wired, "Android Malware Found in Angry Birds Add-on Apps,"
http://www.wired.com/gadgetlab/2011/06/android-malware-angry-birds/, June 2011

[6] NQ Mobile Security Research Blog, "DriodKungFu is Back: Bigger and Badder,"
http://research.nq.com/?p=15#more-15, August 2011

[7] SecureList, "Malicious QR Codes Pushing Android Malware,"
https://www.securelist.com/en/blog/208193145/Its_time_for_malicious_QR_codes, September 2011

[8] Fortinet, "Spitmo Gets on Android: mini-FAQ,"
http://blog.fortinet.com/spitmo-gets-on-android-mini-faq/, September 2011

[9] Fortinet, "Zitmo Hits Android,"
http://blog.fortinet.com/zitmo-hits-android/, July 2011

[10] CNN, "Mobile Malware Alert: Beware of Fake Android Market,"
http://articles.cnn.com/2011-06-21/tech/android.malware.fake.market.gahran_1_android-app-android-users-android-phones, June 2011

[11] PC Magazine, "Fake Netflix Android App Steals Your Data,"
http://www.pcmag.com/article2/0,2817,2394621,00.asp, October 2011

[12] ReadWriteWeb, "First Trojan for Android Phones Goes Wild,"
http://www.readwriteweb.com/archives/first_trojan_for_android_phones_goes_wild.php, August 2010

[13] MSNBC.com, "Fake 'Walk and Text' App Slaps Buyer for Being Cheap,"
http://www.msnbc.msn.com/id/42361788/ns/technology_and_science-security/t/fake-walk-text-app-slaps-buyer-being-cheap/, March 2011

[14] NQ Mobile, "Security Alert: DroidCoupon Masquerades as Coupon App,"
http://research.nq.com/?p=112, September 2011

[15] NQ Mobile, "Security Alert: GingerMaster Virus: First on Android 2.3!"
http://research.nq.com/?p=4, August 2011

[16] Xuxian Jiang, "Security Alert: New Android Malware – HippoSMS -- Found in Alternative Android Markets,"
http://www.csc.ncsu.edu/faculty/jiang/HippoSMS, July 2011

[17] Xuxian Jiang, "Security Alert: New Android Malware – RogueSPPush -- Found in Alternative Android Markets,"
http://www.csc.ncsu.edu/faculty/jiang/RogueSPPush, August 2011

[18] NQ Mobile, "Android Virus: MSO.PJApps.I,"
http://virus.netqin.com/en/android/MSO.PJApps.I/, December 2010

[19] NQ Mobile, "A New Geinimi Variant Captured in the Wild,"
http://blog.netqin.com/en/?p=530, April 2011

[20] PC World, "DroidDream Becomes Android Market Nightmare,"
http://www.pcworld.com/businesscenter/article/221247/droiddream_becomes_android_market_nightmare.html, March 2011

[21] http://c-skills.blogspot.com/2010/07/android-trickery.html

[22] http://c-skills.blogspot.com/2010/08/droid2.html

[23] http://c-skills.blogspot.com/2011/02/zimperlich-sources.html

[24] Xuxian Jiang, "Security Alert: Questionable Android Apps – SndApps -- Found and Removed from Official Android Market,"
http://www.csc.ncsu.edu/faculty/jiang/SndApps, July 2011

[25] NQ Mobile, "Android Virus: BD.FakeBird.A,"
http://virus.netqin.com/android/BD.FakeBird.A/, June 2011

[26] NQ Mobile, "Security Alert: new SMS Android Trojan – DroidLive – Being Disguised as a Google Library,"
http://blog.netqin.com/en/?p=224, November 2011

[27] NQ Mobile, "Android Virus: SW.Msgspy.A,"
http://virus.netqin.com/en/android/SW.Msgspy.A/, June 2011

[28] Computer World, "Symantec recants Android malware claims,"
http://www.computerworld.com/s/article/9223893/Symantec_recants_Android_malware_claims?taxonomyId=77, January 2012

[29] NQ Mobile, "Android Virus: MSO.MJ.A,"
http://virus.netqin.com/android/MSO.MJ.A/, March 2011

[30] NQ Mobile, "Android Virus: MSO.BatterySaver.A,"
http://virus.netqin.com/android/MSO.BatterySaver.A/, July 2011

[31] NQ Mobile, "Android Virus: BD.TRACK.A,"
http://virus.netqin.com/android/BD.TRACK.A/, June 2011

[32] NQ Mobile, "Android Virus: MSO.BatterySaver.A,"
http://virus.netqin.com/android/MSO.BatterySaver.A/, July 2011

[33] NQ Mobile, "Android Virus: BD.TRACK.A,"
http://virus.netqin.com/android/BD.TRACK.A/, June 2011