lookout™
MOBILE SECURITY

STATE OF MOBILE SECURITY

COMPUTEL

Table of Contents

INTRODUCTION

The number of smartphone and tablet owners in the world will skyrocket to one billion in the next few years, according to Forrester. As the mobile economy gains momentum, it continues to capture the attention of malware writers.

Mobile security continues to be a global issue, with 'Toll Fraud,' a type of malware designed for profit, emerging as the lead threat. Over the past year, Lookout estimates that millions of people were affected by malware worldwide with millions of dollars stolen from consumers.

But numbers don't tell the full story. The *State of Mobile Security 2012* report also dives into the sophistication and new distribution mechanisms being explored by malware writers and fraudsters.

1. HIGHLIGHTS

- **Mobile malware is a profitable business.** The mobile malware industry has matured and become a viable business model for attackers.

- **One type of malware designed for profit — Toll Fraud — is the most prevalent type of malware.** Primarily impacting Eastern Europe and Russia, Toll Fraud has successfully stolen millions from consumers.

- **As the mobile industry evolves so do mobile threats.** Fraudsters are tampering with legitimate mobile tools and advertising systems to achieve broader distribution and make more money.

- **Mobile privacy is a growing issue.** Five percent of free Android mobile applications contain one or more aggressive ad networks, which can access personal information or display confusing ads. In addition, a number of high-profile iOS applications raised red flags about privacy issues this year.

- **The likelihood of encountering mobile malware greatly depends on your geographic location and user behavior.** Android malware likelihood is much higher in Russia, Ukraine and China than elsewhere. In terms of user behavior, people who download apps outside of trusted sources like Google Play have a higher likelihood of encountering malware.

- **Mobile malware distribution techniques are diversifying.** Attackers are using a combination of new and existing distribution techniques, including email spam, hacked websites that enable drive-by-downloads and affiliate-based marketing.

2. METHODOLOGY

The *State of Mobile Security 2012* findings are based on data collected and analyzed by Lookout's Mobile Threat Network, which includes application data from a variety of global sources including official application markets, alternative application sources, and mobile devices to form the largest mobile application dataset in the world.

To estimate the overall financial impact of malware, Lookout used detection data gathered from Lookout's global user base along with Android user estimates based on Canalys data 2012 (the Global Smartphone Installed Base Forecasts, June, 2012 Report) to infer broader rates of user infection.

2.1 Likelihood Methodology

This year Lookout made changes to how the likelihood of encountering a mobile threat is calculated. In past reports, Lookout analyzed threat detection rates for Lookout users over a given 12 month period, excluding data from inactive and new customers over the sampled time frame.

Lookout now evaluates likelihood month-by-month and considers data from users that remain active for seven days. Lookout determines the likelihood of encountering application-based mobile threats by summing distinct user detections for new Lookout users over their first seven days of usage. Lookout then divides the total distinct user detections for a given month by the total users registered and active for at least seven days in that month. In addition, recent likelihood figures include detection events from File System Monitoring and Install Monitoring, two features launched in April 2012 that detect malware prior to installation and activation. Through this new methodology, Lookout gleans a monthly likelihood metric that more closely reflects a snapshot of malware prevalence within a population. Because of these differences, the likelihood figures in this report should not be compared one-to-one with those from previous reports.

Lookout uses a different technique to estimate the likelihood of encountering a web-based threat due to their nature. Whereas mobile malware can be present on a device prior to installation, for web-based threats Lookout relies on a period of browsing in order to build an accurate model. Likelihood of encountering web-based threats is determined by analyzing active Lookout users, with the Safe Browsing functionality active, across the 12 month period from July 2011 to July 2012. Lookout totaled distinct user detections for web threats in this population and divided this by the total number of users in the population.

New Lookout users are defined as those who have remained active for at least seven days. Distinct user detections are calculated by only counting the first detection for any given user, which removes multiple detections from consideration.

3. MOBILE THREAT TRENDS

3.1 Definitions: Families, Instances and Variants

Without proper context, malware statistics often appear overblown or exaggerated. The discovery of a single malware family with thousands of individual samples, each varying only slightly from one another can suggest astronomical growth of malware; however the impact could be quite small. In order to understand how threats relate to each other and evolve over time, one must first understand the definitions and lexicon of threats. Simple biology analogies are used to illustrate important distinctions and relationships.

A FAMILY is best thought of as a distinct species of malware or spyware. Like a species, a family is made up of a number of individuals that share important common elements that together define the group as a whole. For malware families, these common elements are often particular sections of code or associated data that define how it executes key functional behaviors and can include distinct communications protocols, Command and Control servers, certain images or other application assets, or unique methods chosen to escalated privileges.

AN INSTANCE is an individual sample within a particular family. Within a biological species, individuals have distinguishing traits that make them identifiable such as eye color, height or weight. Similarly, while malware or spyware instances can often include very minor differences that distinguish them within a group, they are inherently cut from the same cloth.

VARIANTS. If two malware instances are different enough in construction to stretch the boundary of an instance, they may be defined as separate variants.

Malware families can differ greatly in the number of instances or variants they contain. Some families may be composed of only a handful of samples while others may include thousands. When malware writers distribute thousands of samples that feature only extremely minor differences between one another, they may be trying to evade detection. Even the smallest difference can be enough to defeat simple methods of detection such as file hash identification.

3.2 Application-Based Threats

This section explores some of the prevalent and emerging trends related to application-based threats, including evolution in mobile malware motivations, distribution methods and capabilities. For a full glossary of different types of application-based threats, please visit Lookout's mobile security glossary.

PREVALENCE: MALWARE AND SPYWARE

Detection rates of malware continue to outpace those of spyware, a trend observed since

Without proper context, malware statistics often appear overblown or exaggerated.

Detection rates of malware continue to outpace those of spyware, a trend observed since last year's report.

last year's report. Lookout has seen a significant increase in the number of individual malware instances detected in the last six months, with Toll Fraud malware emerging as the most significant threat category. In Q1 2012, detections of Toll Fraud malware alone started to surpass those of spyware. In **Figure 1** below, 'Spyware' incorporates both untargeted and targeted ('Surveillanceware') samples.

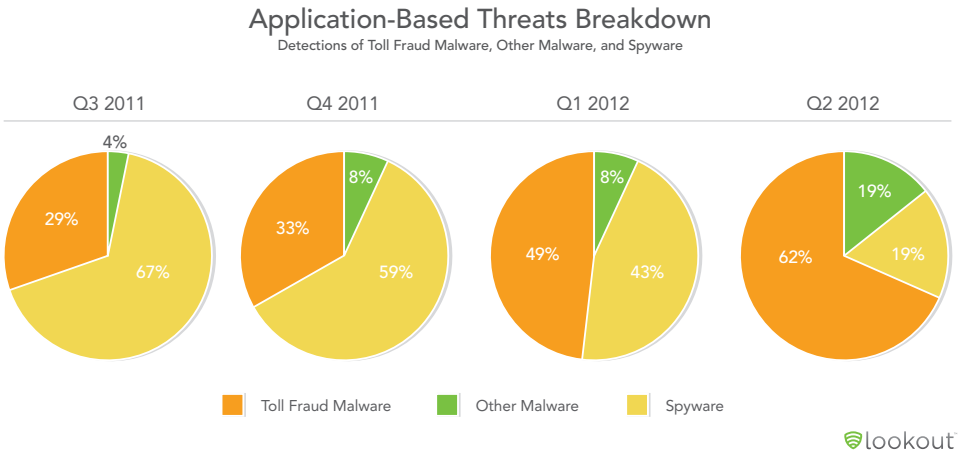

FIGURE 1: APPLICATION-BASED THREATS BREAKDOWN

NOTABLE MALWARE TYPE: TOLL FRAUD

As mentioned, there has been a notable rise in the prevalence of Toll Fraud malware (malware designed for profit that works by billing an unsuspecting victim through premium SMS services). Inspecting this data one layer closer reveals that this massive increase can be attributed primarily to a single Toll Fraud family type dubbed 'FakeInst'.

FAKEINST

FakeInst, also referred to as RuSMSMarket, OpFake, Fakebrows, and FakeWAM, is by far the most prevalent malware detected to date (reference Figure 3). Classified as a Fake Installer, FakeInst pretends to act as an installer for legitimate popular apps such as the Opera Browser (hence the names 'OpFake' and 'Fakebrows') or WhatsApp Messenger. In most cases, Fake Installer malware doesn't perform installations. In fact, in most cases it doesn't contain much user-facing functional code at all.

Figure 3 shows how the proliferation of FakeInst Toll Fraud compares to other common malware families. In 2011, GGTracker and RuFraud were two high-profile Toll Fraud families that caused significant financial damage to users in 2011 in the US and Europe, respectively. Comparatively, FakeInst is almost exclusively directed at Eastern Europe and Russian users.

FakeInst is by far the most prevalent malware detected to date.

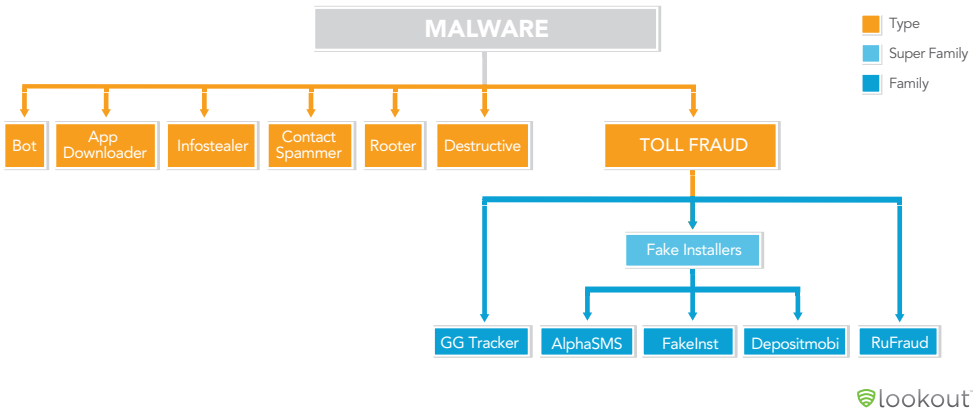

FIGURE 2: FAKEINST AND TOLL FRAUD AS RELATED TO OTHER COMMON MALWARE CLASSIFICATIONS

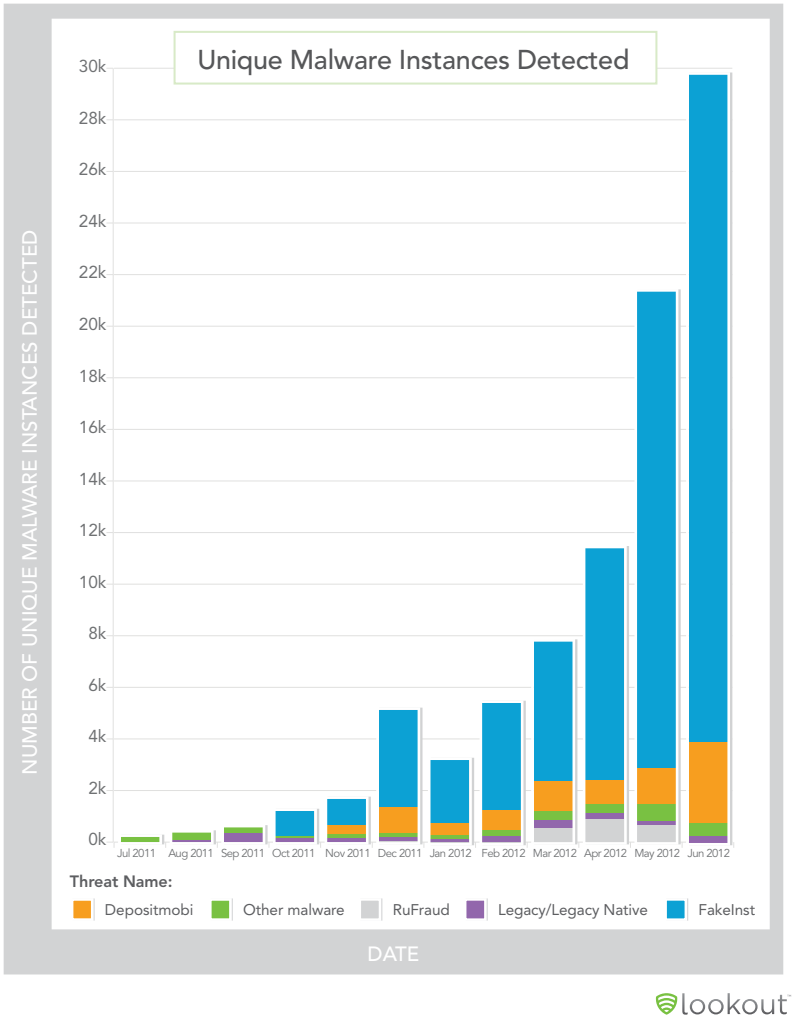

FIGURE 3: UNIQUE MALWARE INSTANCES DETECTED, BY FAMILY

The FakeInst family dominates both the increase in overall month-to-month malware detection events across the Lookout user base as well as the sharp increase in unique binaries (instances) observed and reported in the last year.

The emergence of FakeInst as the dominant family in overall detection events (reference **Figure 4** below) can be attributed to a number of factors:

- Lax premium SMS regulation in certain geographies, including Eastern Europe and Russia, creates an environment in which toll fraud can be a viable business. Safeguards such as double-confirmation subscriptions are not standardized across geographies.

- Similarly, the lack of closely monitored mobile app distribution sites in such regions provides a reliable distribution mechanism for malware. By using third-party markets, file sharing sites and forums, individuals become more likely to encounter malware.

- Malware increasingly leverages affiliate-based promotion networks to mirror the widespread distribution of legitimate applications. For more information on this distribution approach, refer to section 3.5, Distribution Methods.

The increase in unique instances (reference Figure 3) is explained by multiple configuration options available in the distribution system that result in a unique instance of the malware, as well as chosen/random assets generated by the distribution system itself. Executable code occasionally — but rarely — changes. Simply put, the way FakeInst is distributed enables promoters to slightly modify or customize their app for distribution, resulting in a completely unique instance of malware, while the executable code remains identical. Though simple, this technique yields a massive growth in the number of unique identifiable samples in the wild that vastly outstrips the growth of new malware families.

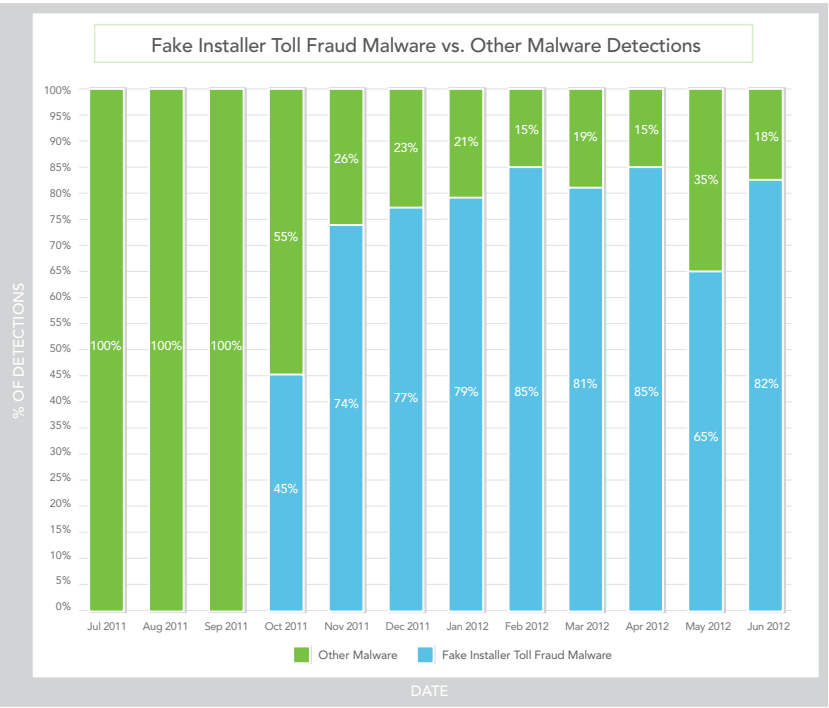

FIGURE 4: RELATIVE MONTHLY DETECTION PREVALENCE OF FAKEINST VS. ALL OTHER DETECTED MALWARE

It should be noted that although AlphaSMS, FakeInst and Deposimobi have distinct code bases, they target the same set of country-specific short codes for fraudulent transactions. This indicates a potential relationship between families, at least in the ultimate beneficiaries of any successful charges.

LIKELIHOOD OF ENCOUNTERING MALICIOUS APPLICATIONS

As noted in Section 2, Methodology, Lookout's method of calculating application-based likelihood has changed from previous years and thus should not be compared year-over-year.

The likelihood that a given device contains malware or spyware is heavily dependent on geographic location, varying from .04% in Japan to 41.6% in Russia. This provides the closest proxy currently available for the current global percentage of devices affected by malicious application-based threats.

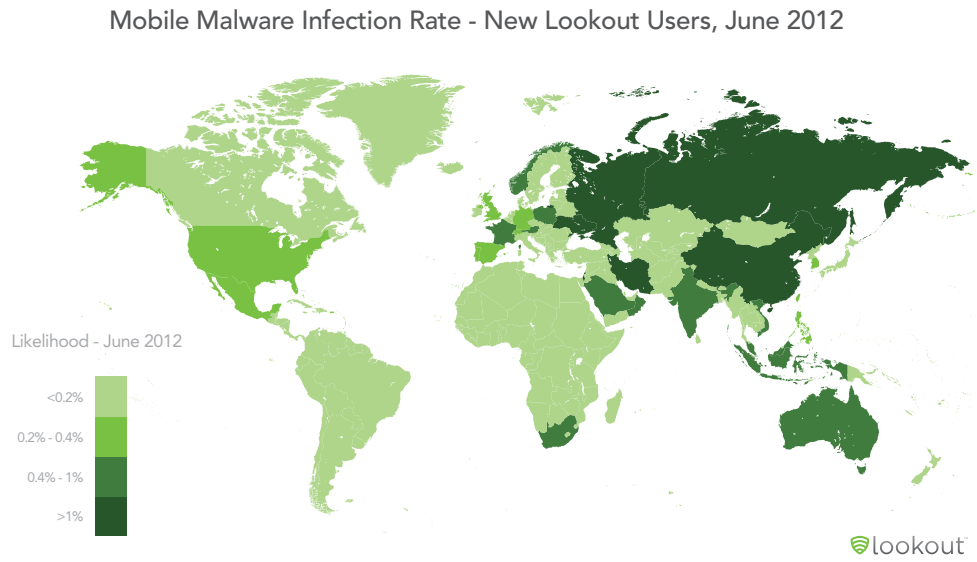

FIGURE 5: MOBILE MALWARE INFECTION RATE – NEW LOOKOUT USERS, JUNE 2012

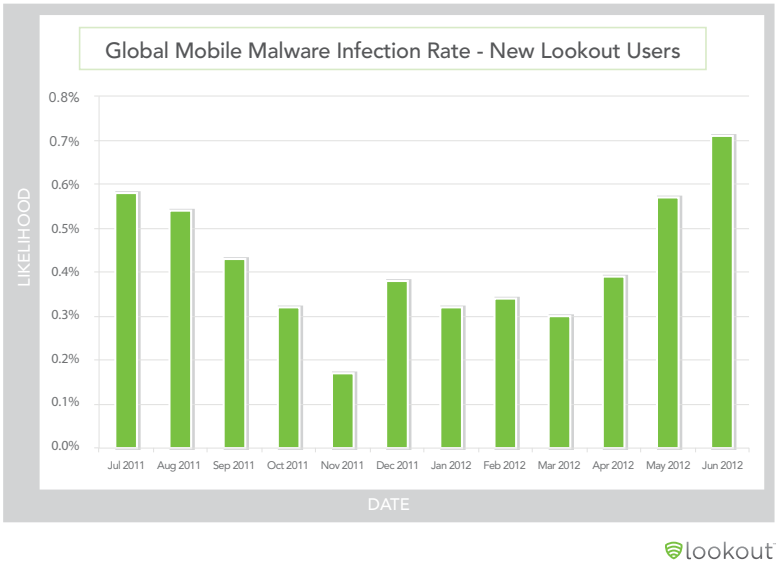

FIGURE 6: GLOBAL MOBILE MALWARE INFECTION RATE – NEW LOOKOUT USERS

The likelihood that a given device contains malware or spyware is heavily dependent on geographic location, varying from .04% in Japan to 41.6% in Russia.

The recent prevalence of Eastern European and Russian targeted malware such as FakeInst is reflected by the extraordinary fact that roughly 42% of new Lookout users in Russia have malware on their Android device (June 2012). This estimate is based on the monthly likelihood that a new Lookout user will have malware on their device in the first seven days (reference Likelihood methodology, Section 2.1).

To estimate the total number of mobile users that have encountered malware within the past 12 months, the raw detection rate is determined amongst all Lookout users in countries with highest statistical significance. By extrapolating this detection rate across the Android user base (reference Canalys) of each of these regions, Lookout estimates that as many as six million people have encountered malware during the 12 month timeframe.

3.3 Malware Motivations

Mobile malware developers create malware for any number of reasons, but the primary incentive is financial return. Malware writers have achieved profit by leveraging the built-in phone billing system (Premium SMS), gaming the app ecosystem incentive structure and devising malware that enables Bank Fraud. Beyond the financial incentive, some malware is designed simply to gain control of or harvest information from a device. This section explores the different types of behaviors that malware exhibits.

TOLL FRAUD MONETIZATION

Premium-rate text messages (premium SMS messages) allow people to charge a variety of mobile services, like ringtones or wallpapers, to their phone bill directly, and the implementation differs country by country slightly. In general, when someone texts a specific number (or "short code") to order a service, the content is delivered, and a fee appears on their phone bill. Because of its ease of use as a phone payment mechanism, SMS billing is used by many legitimate services.

Malware writers can exploit the premium-rate SMS process to steal money. In fact, unique instances of Toll Fraud, malware that manipulate the premium-rate SMS process, are now the most prevalent type of malware, accounting for 91% of malware. In the past year, 78.5% of Lookout's malware detections were classified as Toll Fraud malware.

Regulation over premium SMS services varies greatly from country to country. Some countries, such as the US, require a "double opt-in" — the exchange of multiple confirmation messages before a user is charged for any service and require that mobile operators keep funds from being transferred to a premium service provider until after the user has paid their phone bill. Other countries, such as Russia, do not enforce such regulatory practices, making them more lucrative locations for malware.

Mobile malware developers create malware for any number of reasons, but the primary incentive is financial return.

78.5% of Lookout's malware detections were classified as Toll Fraud malware.

Premium SMS can involve a number of key players, including:

- The wireless provider (e.g., a mobile operator or carrier) runs the network and supplies shortcodes to facilitate premium SMS billing.

- Aggregators act as "middlemen" between content providers (companies that want to interact with end users through their mobile devices) and wireless providers. Aggregators manage billing transactions and maintain the technical and service level requirements of each wireless network.

- Content providers (e.g., a ringtone company) create and sell mobile content that consumers purchase.

Figure 7 shows how the legitimate premium SMS text message process works. And Figure 8 illustrates how malware writers take advantage of this system, silently sending and intercepting premium SMS text messages from an infected device without the user's knowledge or consent.

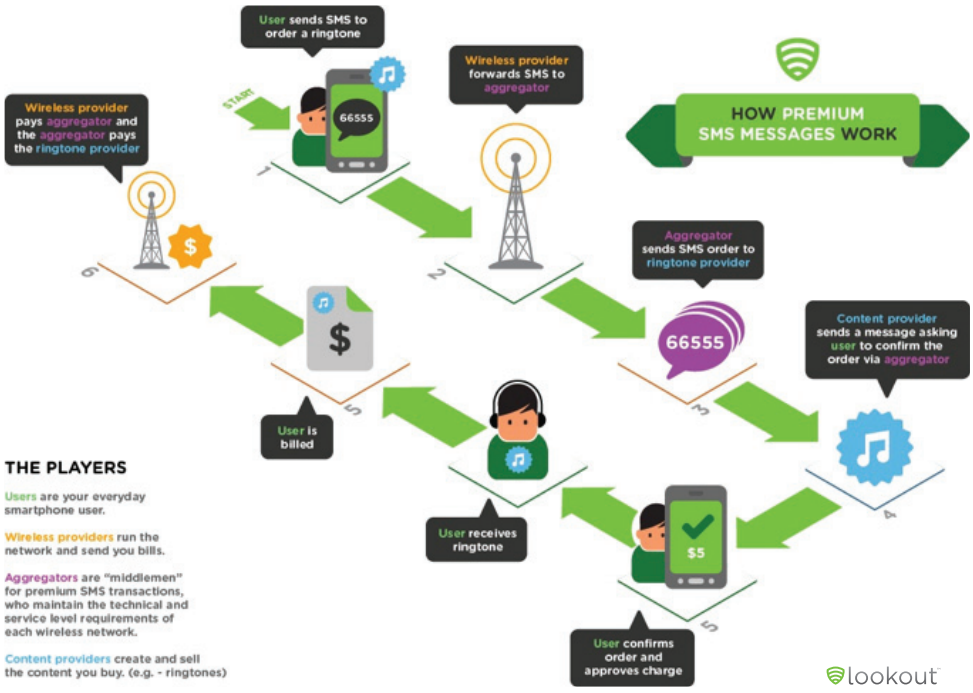

FIGURE 7: HOW PREMIUM SMS WORKS

Other countries, such as Russia, do not enforce strict regulatory practices, making them more lucrative locations for malware.

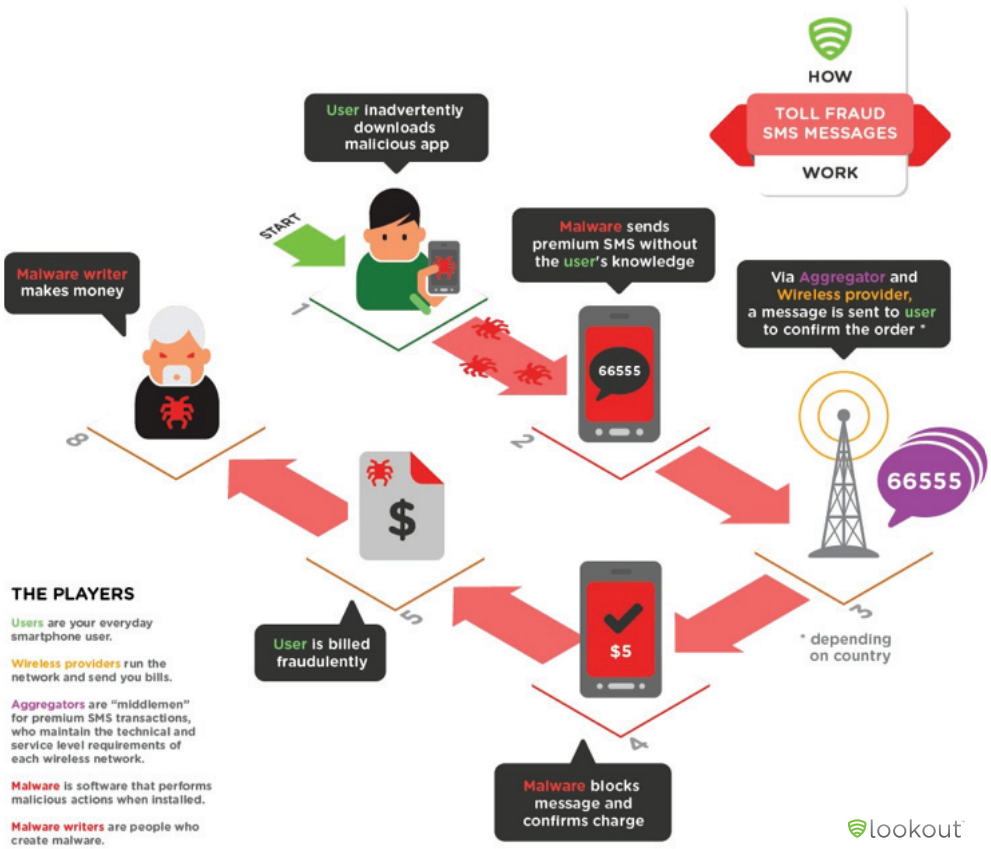

FIGURE 8: HOW TOLL FRAUD MALWARE WORKS

AD NETWORK HIJACKING

As profiled in the 2011 Mobile Threat Report, repackaging is a very common tactic by which a fraudster takes a legitimate application and modifies it by injecting malicious code. Lookout has also seen repackaged apps that aren't necessarily malicious, but are modified to redirect ad traffic to a different affiliate ID or add additional ad networks. This tactic is especially effective at fooling end users because it is often difficult to tell the difference between a legitimate app and its repackaged twin.

We continue to observe cases of targeted repackaging that make specific changes to an application to modify the embedded ad networks so that someone other than the legitimate developer is compensated for ad impressions. It's important to note that this isn't necessarily malware, since they aren't adding malicious capabilities to the tampered application.

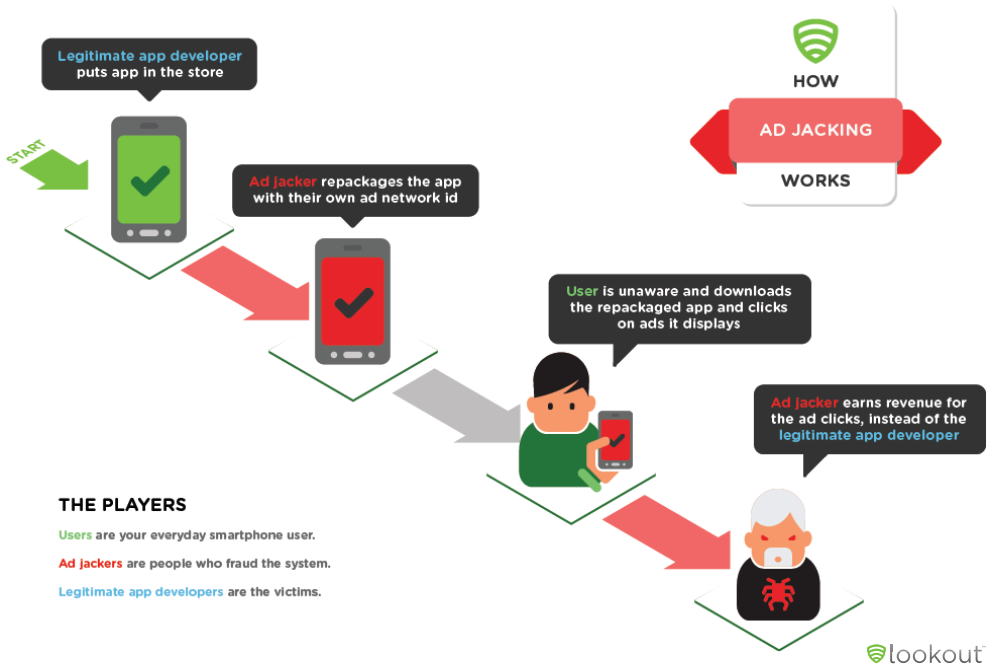

FIGURE 9: HOW ADJACKING WORKS

GAMING THE APP ECOSYSTEM

App marketers (promoters) are often incentivized based on how well they are able to drive metrics that correlate to app popularity, including app downloads, installs and activations. While the incentive structures may vary, the general rule of thumb is that the more times an app is downloaded, installed or run, the bigger the reward. App promoters will use malware capable of one or more of the following malicious tactics to boost metrics without the user's knowledge:

- Download applications from alternative app market sources to storage locations that do not alert the end user. These apps may or may not be installed, depending on the type of malware.
- Masquerade as an application that requires root permissions to gain escalated privileges on a device, which can then be used to install subsequent applications.
- Install third party app stores onto the device in an effort to convince the user to download specific apps.
- Silently run applications while the device screen is off to register "active app" events.

This is an increasing trend in China; Lookout has identified several different families of malware that promote Chinese applications or Chinese third party app stores. The Gamex malware family is capable of rooting a phone and subsequently installs additional apps. This type of malware is not new; iLegacy, LeNa and Geinimi are other malware families that exhibit capabilities that enable app promoters to "game the system".

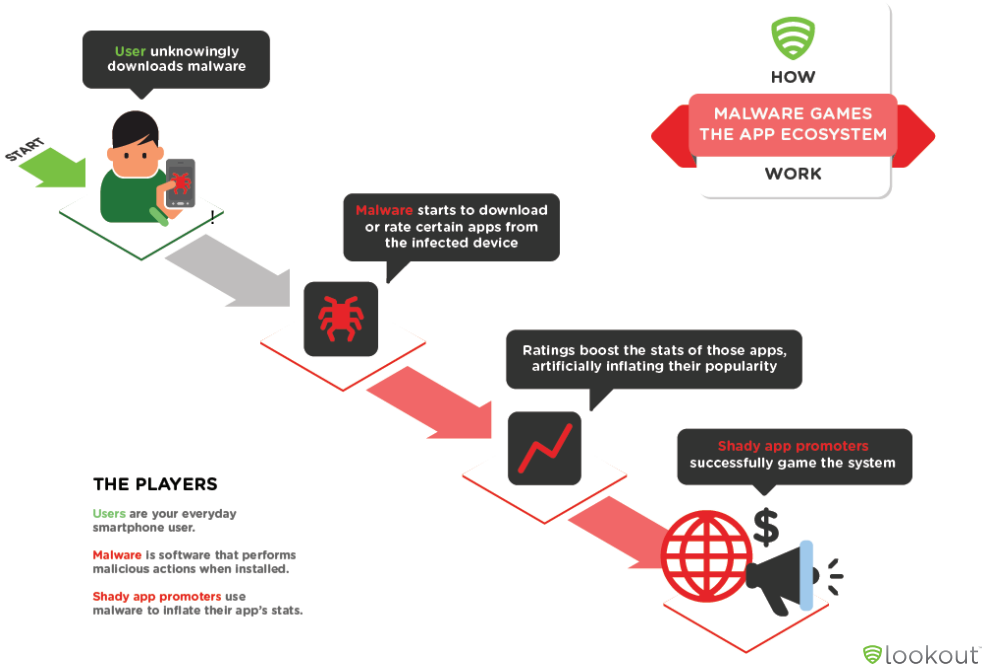

FIGURE 10: HOW MALWARE THAT GAMES THE APP ECOSYSTEM WORKS

Beyond the financial incentive, some malware is designed simply to gain control of or harvest information from a device.

MAN-IN-THE-MOBILE AND BANK FRAUD

Secondary authentication factors such as mobile Transaction Authentication Numbers (mTAN) provide an out-of-band component that can help to mitigate the impact of Man-in-the-Browser fraud techniques employed on the desktop by Zeus, SpyEye, and Tatanga. Man-in-the-Mobile interceptors have been discovered in the wild than can intercept mTANs to help gain full control of a victim's bank account.

REMOTE CONTROL

Beyond monetization, mobile malware presents an opportunity to establish additional methods of access or control over a user.

These include:

- Network Access
  - Although we do not believe that it was built specifically for such a purpose, NotCompatible's design as a simple TCP relay means that it could be used to gain illicit access to private networks — and any sensitive data on such a network — by turning an infected Android device into a proxy.
- Targeted Surveillance
  - Commercial Surveillanceware provides a means to gain extremely sensitive information. Comprehensive access to communications' records and location data has the potential to violate significant user privacy restrictions and put businesses and organizations at similarly broad risk.

3.4 Estimated Impact

Lookout estimates that more than six million people were affected by Android malware from June 2011 to June 2012, most were affected by Toll Fraud applications. As shown in Figure 1, the prevalence of Toll Fraud grew explosively from 29% of the application-based threats in Q3 2011 to more than 62% in Q2 2012.

Lookout estimates that one sub-family of FakeInst, the most prevalent Toll Fraud malware family, has netted an approximate $10 million for its makers over the past nine months, mostly from Eastern European and Russian Android users. As criminals continue to experiment with Toll Fraud, we expect the financial impact to increase and the geographical reach to broaden.

3.5 Distribution Methods

Malware developers use a variety of techniques to establish the broadest possible distribution across devices. In this section we review some of the most notable new distribution trends we've seen over the past 12 months.

Lookout estimates that more than six million people were affected by Android malware from June 2011 to June 2012, most were affected by Toll Fraud applications.

AFFILIATE NETWORK-BASED DISTRIBUTION FOR TOLL FRAUD

Legitimate application developers often use affiliate distribution techniques to promote their applications and services, drive downloads and generate revenue. Traditional affiliate networks enable app developers to increase app downloads and website visits by offering promoters a share of revenue generated by such actions or a specific fee per action.

Lookout found that shady affiliate networks even provide a set of customization tools that allow app promoters to create unique instances of Toll Fraud malware. On one affiliate network, app promoters can choose the type of app they would like to promote (e.g. fake Opera browser, fake WhatsApp Messenger, or fake Facebook app), target geographies, and the specific SMS bill rates to charge end users. FakeInst malware, profiled in section 3.2 uses affiliate networks to secure widespread distribution of its malicious applications.

Promoters distribute applications through various channels, including in-app ads, links, web-based pop-ups or third-party application markets. When a mobile user taps on the promotion, the malicious app is downloaded. If a user then installs and activates the downloaded application, the app can begin sending silent SMS messages off the phone to a premium short code.

It is often difficult to identify the source of malware due to the fact that fraudsters often use multiple connection aggregators or affiliate networks in sequence. By hiding fraudulent behavior behind a number of business entities or actors, it becomes unclear whether or not a given affiliate network (or the promoters themselves) are aware of the fact that they are distributing malicious software.

Figure 11 shows how malware writers use affiliate-based techniques to distribute Toll Fraud malware and generate revenue from unsuspecting users.

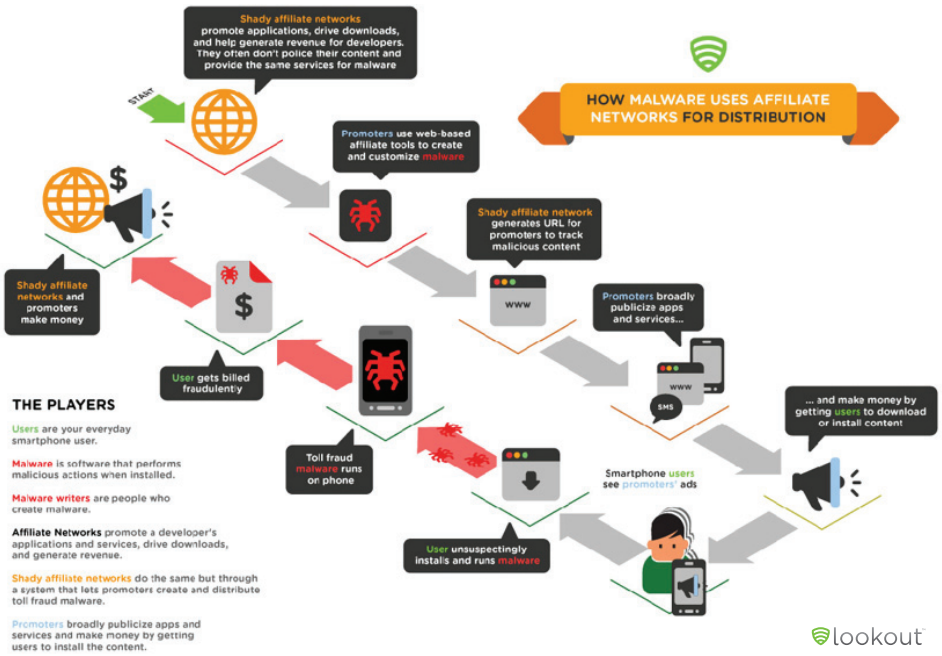

FIGURE 11: MALWARE DISTRIBUTION ON 'SHADY' AFFILIATE NETWORKS

Lookout found that shady affiliate networks even provide a set of customization tools that allow app promoters to create unique instances of Toll Fraud malware.

DRIVE-BY DOWNLOADS

A drive-by download is a distribution technique where a webpage automatically starts downloading an application when a user visits it. Drive-by downloads can be combined with clever social engineering tactics to appear as if they are legitimate. Because the Android browser does not automatically install downloaded applications, an attacker also needs to convince the user to download the app in order to successfully infect the device with malware.

Figure 12 shows how misleading file names are a common social engineering tactic for drive-by downloads. The NotCompatible drive-by-download is named 'com.Security. Update' to trick users to manually installing it.

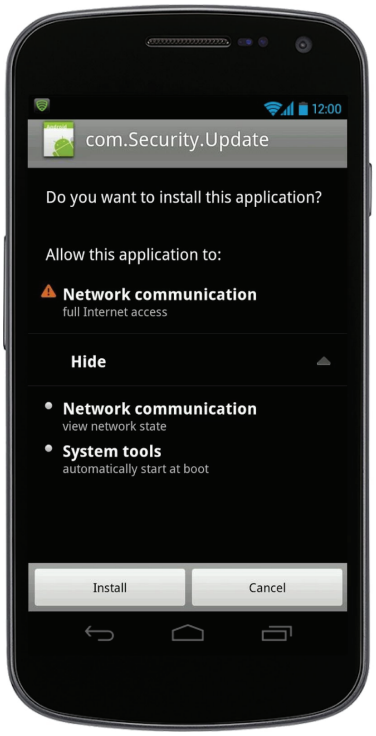

FIGURE 12: DRIVE-BY DOWNLOAD NOTCOMPATIBLE DISGUISED AS A SYSTEM UPDATE

MALVERTISING

Also known as "malicious advertising," malvertising leverages mobile advertising as a distribution technique. Because legitimate developers commonly run advertisements in other apps to attract new users, it's not uncommon to download apps through advertisements. In the case of malvertising, a malware writer buys legitimate mobile ads and directs users to download malware on legitimate markets or from a fake site designed to imitate legitimate markets. For an example of malvertising, visit our 2011 Mobile Threat Report.

3.6 Web-Based Threats

Web-based threats have remained a significant threat for mobile users, particularly because users on mobile devices can encounter threats targeting PCs. This category includes phishing scams that use email or social networks as distribution mechanisms, as well as mobile-specific tactics such as SMS-based spam and phishing. Some web-based threats, such as phishing attacks, do not discriminate based on mobile platform; they affect Android, iOS and PCs in the same way.

Lookout found that the likelihood of encountering a web-based threat within a given year varied from an estimated 10% to 40% globally. In the United States, 4 in 10 users will click on an unsafe link on a mobile device this year.

In the United States, 4 in 10 users will click on an unsafe link on a mobile device this year.

PHISHING, MALICIOUS AND COMPROMISED WEBSITES

PHISHING sites are designed to mimic trusted sites, such as financial institutions, in order to trick users into divulging account or personal information. The small form factor of mobile devices, coupled with trends such as the use of URL shorteners or QR codes, often makes it more difficult for users to evaluate the reputability of a given website.

COMPROMISED websites are legitimate websites that have been infected by a bad actor to scam or defraud visitors, while MALICIOUS websites are often distribution points for malicious applications. Websites infected by the NotCompatible trojan (reference NotCompatible in the appendix) are an example of compromised websites that served Android-targeted drive-by downloads.

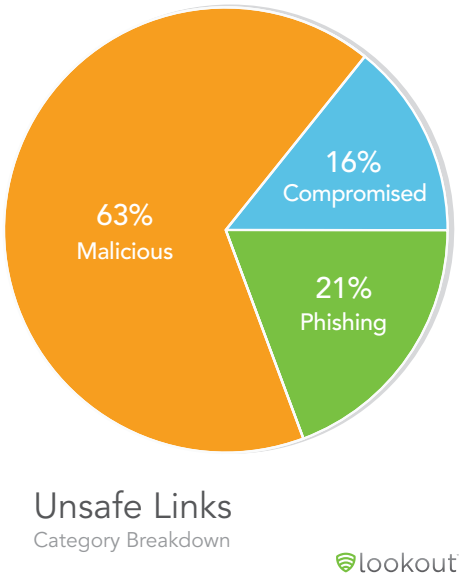

FIGURE 13: CATEGORY BREAKDOWN OF UNSAFE LINKS

3.7 Adware

2012 saw the emergence of a number of aggressive mobile advertising practices, which include pushing out-of-app ads, changing browser and desktop settings, and accessing personally identifiable information without suitable notification or transparency. For these reasons, Lookout released the Mobile App Advertising Guidelines in July 2012, which provides a framework to help app developers and ad providers understand how they can explore new mobile advertising techniques while adhering to strong privacy and user choice principles. Moving forward, applications that do not comply with this framework are characterized as 'Adware.'

The next section, Privacy Threats, provides an in-depth view into mobile privacy issues related to aggressive advertising techniques.

4. PRIVACY THREATS

Privacy is a significant concern for consumers when using mobile applications. This is unsurprising, given that our mobile devices are a veritable treasure trove of personal information, including location, browsing history, call history, text messages, contact lists, email, Facebook messages, the device's phone number and unique identifiers that can be used for tracking.

4.1 Aggressive vs. Acceptable Behavior

Legitimate apps can use personal information to provide powerful features and benefits. However, the opportunity to misuse that information exists as well. Because they have the potential to access so much data on devices, it's common for applications to gather data without properly notifying users of its collection.

4.2 Adware and Aggressive Mobile Ad Behavior

The presence of aggressive ad providers in mobile apps is a prevalent mobile privacy issue today. Aggressive ad behavior includes pushing out-of-app ads, changing browser and desktop settings and accessing personally identifiable information without suitable notification or transparency to the user. Based on Lookout's analysis, more than five percent of free applications on Google Play contain ad networks that practice aggressive practices. While most ad providers aren't aggressive in nature, the few that are could have a negative impact for the industry as a whole.

AGGRESSIVE AD PROVIDER DISTRIBUTION

As shown in **Figure 14**, the prevalence of aggressive ad providers can vary greatly across third party app stores globally.

COUNTRY OF ORIGIN	% OF APPS W/ AGGRESSIVE ADS
China	4.41%
US	5.37%
Russia	6.12%

lookout

FIGURE 14: AGGRESSIVE AD PROVIDER DISTRIBUTION AMONGST GOOGLE PLAY AND ALTERNATIVE APP STORES

On Google Play, apps in the personalization category have the highest percentage of aggressive ad networks at 17%.

ALTERNATIVE APP STORES

On Google Play, apps in the personalization category have the highest percentage of aggressive ad networks (17%). **Figure 15** shows prevalence across a number of app categories.

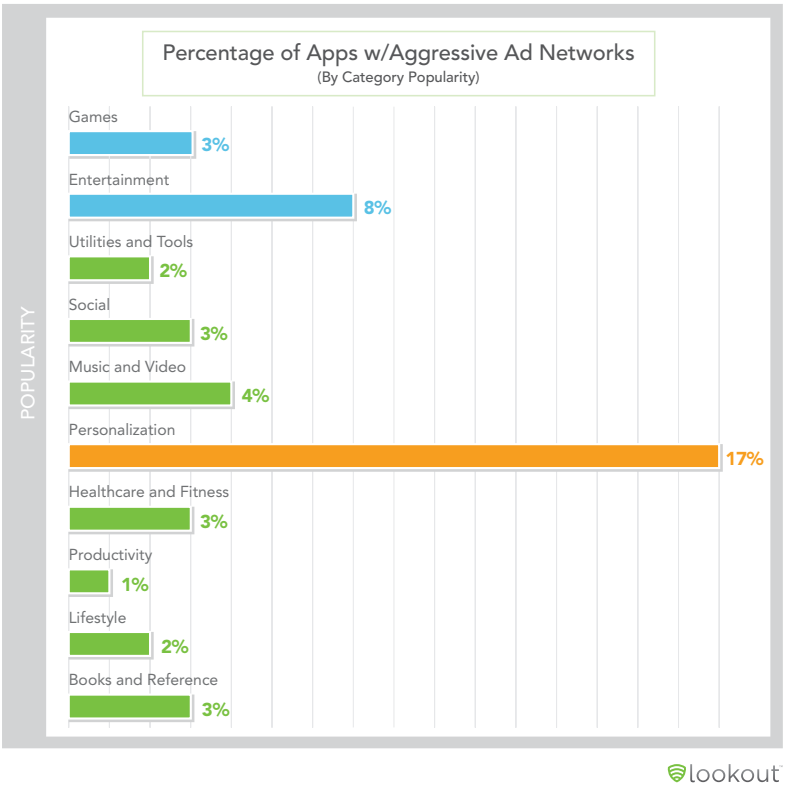

FIGURE 15: AGGRESSIVE AD PROVIDER DISTRIBUTION AMONGST FREE GOOGLE PLAY APPS BY CATEGORY (AS OF JUNE 2012)

Each of these distribution estimates has been determined by analyzing Lookout's Mobile Threat Network, which is composed of applications acquired from official and third party markets globally. It should be noted that this data does not take into account.

5. MOBILE PLATFORM UPDATES

In any software system, there are bound to be flaws and security vulnerabilities, mobile device operating systems are no exception. In past years, mobile platforms have been repeatedly exploited through operating system-level vulnerabilities, allowing attackers (as well as phone enthusiasts) to gain access to and control a device. Both iOS and Android have adopted increasingly sophisticated methods to protect their platforms from attack.

In any software system, there are bound to be flaws and security vulnerabilities, mobile device operating systems are no exception.

5.1 Android

PLATFORM

Google has released a number of new features recently that improve the security of the platform as a whole. The latest versions of the Android operating system have implemented progressively stricter forms of Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP), which together make the exploitation of memory corruption vulnerabilities probabilistically difficult:

- ASLR helps protect against some security attacks by making it more difficult for an attacker to predict target memory addresses of key data areas in a process's address space that can be the target of an attack.

- DEP helps protect against exploits such as buffer overflows by limiting the surface of executable memory regions to those expected to contain code rather than allowing execution in regions used only for data.

Previous versions of Android have featured a number of security mitigations, including DEP in Android 2.3+ (Gingerbread). Android 4.0 (Ice Cream Sandwich) was the first to make use of ASLR, however the implementation was shown to be relatively limited, leaving substantial segments of process address space predictable. Android 4.1 (Jelly Bean), released in July 2012, includes a more comprehensive and secure implementation.

A new keychain API and underlying encrypted storage let applications store and retrieve private keys and their corresponding certificate chains. Any application can use the keychain API to install and store user certificates and CAs securely. Ice Cream Sandwich also includes Full Disk Encryption, a feature initially released for tablets in Android 3.0, which allows devices to perform boot-time, on-the-fly encryption / decryption of the application storage area. Lastly, Google announced future plans for paid app encryption designed to prevent piracy at I|O 2012.

GOOGLE PLAY & BOUNCER

In early February 2012, Google announced Bouncer, a system to automatically analyze submissions to Google Play for potentially malicious behavior. Bouncer provides developers and the greater security community an alternative to the manual curation process. Developers

can still innovate quickly while Bouncer increases the baseline level of security for Android users. Recent research has uncovered methods to profile Bouncer's execution environment, which could be used to sneak malicious applications past Google Play's "velvet rope." Similar to system-level vulnerabilities, we expect that there will always be a way for determined malware developers to sneak malicious applications past safeguards such as Bouncer, but it is a great step in raising the bar to attacking Android devices.

5.2 iOS

PLATFORM

In May of 2012 Apple released its first report on iOS Security, covering current capabilities related to System Architecture, Encryption and Data Protection, Network Security, and Device Access. iOS 5.1, was released on March 7, 2012, and was jailbroken just days later. While the iOS 6 release included kernel ASLR and was not as easy to jailbreak dedicated hackers were still able to develop workarounds for their jailbreak solutions. Meanwhile, Apple has had its own experience with malicious applications on its App Store.

APP STORE

In September of 2011, security researcher Charlie Miller published research demonstrating a method to bypass iOS code verification, the process by which compiled iOS applications are sealed and attributed to a specific developer. This flaw allowed applications in the App Store to download new, unsigned code that was not vetted by App Store curated review process. Charlie Miller demonstrated the ability for an attacker to gain remote access and control of a device, even going so far as to trigger physical responses such as vibrations, or to download a personal address book without the user's knowledge. Although Apple shipped a fix for this vulnerability quickly with iOS 5.0.1, it clearly demonstrated that no platform is immune to security vulnerabilities or risks.

Although Apple shipped a fix for this vulnerability quickly with iOS 5.0.1, it clearly demonstrated that no platform is immune to security vulnerabilities or risks.

6. WHAT'S NEXT?

The past 12 months have clearly demonstrated that mobile malware creators have found a business model that works. Malware authors have largely forsaken the development of sophisticated new fraud techniques in favor of large-scale distribution of basic Toll Fraud malware, with FakeInst leading the way. With Toll Fraud malware taking millions of dollars for malicious developers and very little in the way of Premium SMS regulation in Russia and Eastern Europe, it's difficult to imagine malware authors changing their strategy any time in the near future barring a significant change. Instead, we expect that those behind FakeInst and similar scams will continue to explore new and effective means of app distribution such as affiliate-based promotion.

The majority of technical malware innovation in the past 12 months has largely come from Asian sources, and includes greater sophistication in embedding of exploit payloads (LeNa v2) and two-stage malware that remotely fetches an exploit (**RootSmart**). While Toll Fraud malware has the potential to defraud users of significant funds, exploit-enabled malware has the potential to do far greater damage to devices since it can be used to gain and maintain full control over an infected device. Some root-enabled malware has been largely focused on enabling app marketers to game the ecosystem (see Section 3.3), and the functionality and has not yet been used to enable large-scale mobile botnets. Creating such a network may well be the next step in technical mobile malware innovations. As the mobile ecosystem continues to evolve, it is expected that malware writers will continue to experiment with new ways to trick existing marketing tools and processes.

The likelihood of encountering malware is highly dependent on a person's geographic location, in addition to their user behavior. The chance of encountering malware is much higher in Russia, Ukraine and China than elsewhere. People who decide to download apps outside of trusted sources like Google Play also have a higher likelihood of encountering malware.

7. HOW TO STAY SAFE

While threats are growing in sophistication and frequency, people everywhere can take measures to stay safe while using their smartphones.

- **Passcode.** Set a password on your mobile device so that if it is lost or stolen, your data is more difficult to access.
- **Trusted sources.** Only download apps from trusted sources, such as reputable app stores and download sites. Remember to look at the developer name, reviews, and ratings.
- **Pirated app? Use caution.** Be wary of apps that offer a typically paid app for free, or an app that claims to install or download other apps for you.
- **Clicking on web links.** After clicking on a web link, pay close attention to the address to make sure it matches the website it claims to be, especially if you are asked to enter account or login information.
- **Security app.** Download a mobile security app that scans every app you download for malware and spyware and can help you locate a lost or stolen device. For extra protection, make sure your security app can also protect from unsafe websites.
- **Check your phone bill.** Be alert for unusual behaviors on your phone, which could be a sign that it is infected. These behaviors may include unusual text messages, suspicious charges to the phone bill or suddenly decreased battery life.
- **Firmware updates.** Make sure to download and install firmware updates as soon as they are available for your device.

APPENDIX

New Threat Profiles

NOTCOMPATIBLE

In April 2012, Lookout discovered NotCompatible, the first example of mobile malware that used compromised websites as a targeted distribution method. NotCompatible is automatically downloaded when an Android browser visits an infected website. The downloaded application is disguised as a security update in an attempt to convince the user to install it.

If successfully installed, NotCompatible does not cause direct harm to a target device, but can potentially be used to gain illicit access to private networks by turning an infected Android device into a network proxy. This feature could be significant for system IT administrators. A device infected with NotCompatible could potentially be used to gain access to protected information or systems, such as those maintained by enterprise or government.

Based on Lookout's research, it appears that NotCompatible's authors are using infected Android devices to assist in fraudulent online purchases, such as buying tickets to a Red Hot Chili Peppers concert via TicketMaster and shopping on the Apple App Store. A dispersed proxy network can be used to evade IP or region-oriented reputation or transaction velocity models used to detect fraudulent transactions. In the case of ticket purchases, such techniques might be designed to identify and limit high volume ticket purchases by scalpers.

NotCompatible has shown one of the highest rates of detection amongst Lookout users of any malware family in 2012, second only to FakeInst.

CI4

In June 2012 Lookout identified CI4, one of the first SMS bot distributed via email spam campaigns (a SMS Bot can put SMS capabilities under remote control for the purpose of SMS spamming). If a user follows through with the download and installation process, CI4 is installed without a launcher icon, making it difficult for users to recognize that their system is affected. Instead of relying on a user to open the app, CI4 is activated by system events broadcast when the device is powered on or woken up. The malware then sends identifying information off of the infected device to a remote server.

CI4's most unique trait is that it employs Twitter to obfuscate the data transmission channel as it acquires its Command and Control host address from algorithmically generated Twitter accounts.

NotCompatible has shown one of the highest rates of detection amongst Lookout users of any malware family in 2012, second only to FakeInst.

Figure 16 shows one such Twitter account that has since been taken down.

FIGURE 16: ALGORITHMICALLY-GENERATED CI4 TWITTER ACCOUNT

RUFRAUD

In December 2011, Lookout discovered over 27 malicious Android apps posted on Google Play targeting users in Europe and Russia. The malware, named RuFraud, posed as popular wallpaper, movie and game apps, but were actually bundled with malicious Toll Fraud code. RuFraud buried a disclosure deep within the permissions' fine print specifying that SMS messages may result in user charges.

When a smartphone user opened the app, the malware would send premium rate text messages without the user's knowledge. In the UK alone, nearly 1,400 Android smartphone users downloaded RuFraud; costing each user an average of £15, roughly equivalent to $23.50. RuFraud sparked an international investigation spearheaded by regulatory firm PayPhonePlus, who was able to shut down the maliciously used UK shortcodes employed by RuFraud. Beyond the UK, the RuFraud scam targeted over 18 countries including the UK, Italy, France, Germany, and Russia.

Lookout identified CI4, one of the first SMS bot distributed via email spam campaigns.

Figure 17 shows the user consent screen from a December 2011 instance of RuFraud. The inconspicuous link to "The Rules" in the bottom right of the screen leads to a set of lengthy, unclear terms of service that describe the premium SMS message changes.

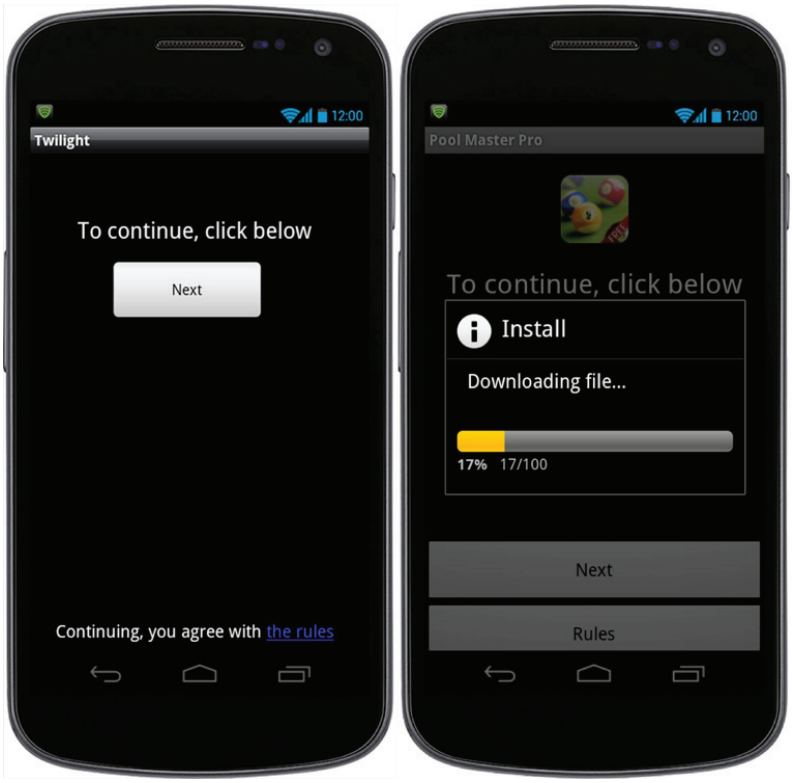

FIGURE 17: MISLEADING RUFRAUD USER CONSENT AND INSTALL SCREENS

LENA V2

In April 2012, Lookout discovered a new variant of Legacy Native (LeNa), a malware family originally discovered in October 2011 that masquerades as a legitimate application and attempts to trick a user into activating its malicious payload by invoking the SU utility on rooted devices used to selectively grant superuser privileges to applications that request them. LeNa's repackaged application functionality works properly after gaining root access while simultaneously installing a native binary file that is capable of installing additional software without user notification.

LeNa v2 uses the Gingerbreak exploit payload hidden at the end of an otherwise functional JPEG to gain root permissions on a device. By employing an exploit, this variant of LeNa doesn't depend on user interaction to gain root access to a device. Like its predecessor, LeNa v2 also drops a secondary payload that is capable of installing additional packages and push URLs to be displayed in the browser. LeNa v2's Command and Control appears to focus on pushing a single package to the device: com.the9.gamechannel, a Chinese-language alternative market that publishes Android games. This

package is installed without the user's knowledge and is then launched. The alternative market may be front and center on a device after a user leaves it unattended for a prolonged period of time.

GAMEX

In April 2012 Lookout discovered Gamex, a new trojan most notable for piggybacking on repackaged versions of applications that require root access, such as file managers, ad blockers and device performance boosters. After Gamex gains root privileges, it communicates with a remote server and installs another application to the target device's system partition. The new app in turn installs additional apps (reference Gaming the Ecosystem).

ROOTSMART

Discovered in February 2012 by security researchers at NC State, 'RootSmart' is the first known malware sample that remotely fetches an exploit payload. While RootSmart uses the same root exploit that other malware (such as Gingerbreak) has used in the past, RootSmart is unique because it does not directly embed the exploit payload inside the app. Instead it dynamically fetches the root exploit from a remote server before using it to escalate its privileges. After obtaining root privileges, RootSmart behaves like many other malware samples; it downloads additional malicious applications from a remote Command and Control server and installs them to the system partition of a device without user knowledge.