SUBMISSION TO THE COMMONWEALTH CONSUMER AFFAIRS ADVISORY COUNCIL INQUIRY INTO

App purchases by Australian consumers on mobile and handheld devices

BY

TREND MICRO ANZ

31 JANUARY 2013

MOBILE APPS - A SECURITY PERSPECTIVE

PREFACE

Trend Micro, a global security vendor and one of the leading security brands in Australia, welcomes the opportunity to make this submission to the CAAC inquiry on the app market.

Trend Micro has a core focus on mobile security and this submission analyses the topic from a security perspective. With more than 1500 global threat researchers and a development centre based in Australia, Trend Micro has drawn on the latest research from TrendLabs to analyse the current state of mobile apps and user safety.

OVERVIEW

Mobile devices have transformed our lives and opened up endless possibilities in communications, productivity, and entertainment. However, our digital lifestyle has also unleashed new vulnerabilities that are being exploited by cyber criminals around the world. The Android mobile operating system is particularly vulnerable, with apps – which form a central part of this ecosystem – especially so.

2012 saw the exponential boom in Android malware and high-risk apps. Trend Micro’s 2012 Annual Security Roundup noted that the number of Android malware grew to 350,000 – which was a significant leap from the 1,000 mobile malware we saw in 2011. If this trend continues this year, we predict that the volume of malicious and high-risk Android apps will hit 1 million in 2013.

To protect their devices, users must be extra careful with downloading apps, especially those hosted on third-party app providers. Reviewing the app’s description and developer reputation is also a commendable way to prevent installing programs that can compromise the device’s security. For better protection, users should install antivirus programs which detect these malicious apps.

INTRODUCTION

App use has become the cornerstone for smartphone ownership. A Nielsen study showed that the number of apps U.S. smartphone users install increased from 32 in 2011 to 41 in 2012. Research from Flurry revealed that the average amount of time spent on apps grew 35% in 2012.

Smartphone users in Australia are able to download a wide variety of apps, many of which are either inexpensive or free. Not all of these actually meet what users expect in terms of features, and some of these even introduce risks that users may not fully understand.

For older or "feature" phones, the security issues are generally limited to issues such as losing the device itself, or perhaps to sending spammed text messages. For smartphones, the security risk is greater as users can easily install various third-party apps, which may not be provided by the legitimate developers and telecommunication companies. The distribution channels of various third-party apps may be used by cybercriminals as well. Users should understand that the increased power of mobile devices also increases the risk.

It is becoming increasingly clear that the mobile space is the next great frontier for malicious activity in cyberspace. The cybercriminals are clearly favoring Android as their preferred target in this area. It is also clear that mobile devices need active protection just like PCs do.

Some apps have unwanted routines which we consider high-risk; for example, some violate the user's privacy by accessing the user's personal information. Frequently, this is done by apps which display ads (i.e., adware). Examples of routines that may cause an app to be classified as such include:

- Consuming system resources
- Displaying pop-up advertising
- Violating the user's privacy

Users who continue to use these apps may encounter unexpected behaviour, and may suffer problems without any notice.

Aside from the above apps which are clearly fraudulent, there are also more subtle cases where smartphone users encounter certain privacy threats a bit differently. In such cases, while the "extracted" user information was considered as "necessary" to install the app, users may not have been fully informed of the privacy consequences.

GROWTH OF ANDROID

Android's popularity is making it a prime target for cybercriminals and attackers. The platform's growing dominance in the mobile landscape echoes that of Windows in the desktop and laptop space, albeit at a much faster pace.

All mobile ecosystems and devices are increasingly at risk from threats. The fact that the Android ecosystem allows users to install apps from independent sources means that businesses who offer these download services have a duty of care to ensure their product is as risk free as possible.

At first glance, the headline prediction may sound surprising; the volume of malicious and high-risk Android apps will hit 1 million in 2013. However, when you consider that our prediction for total Android malware by the end of 2012 has been constantly revised up throughout the year and now stands at over 350,000, maybe it no longer sounds so fanciful.

THE PROBLEM WITH ANDROID

Typically, malware is hidden in legitimate looking applications and often designed to look like cheaper or free versions of popular paid-for software, including mobile games, in order to lure the victim into downloading them. The problem with Android is that anyone, anywhere can make an app available for download, even if it is not via the official Google Play app store.

To make matters worse, unlike Apple's tightly-controlled App Store, an app can be uploaded to Google Play with minimal checks, so malware also frequently appears on this main site, although Google will usually take down anything it finds suspicious.

Google Android is fast becoming the mobile equivalent of Windows in the 1990s – incredibly popular with users but also number one with cyber crooks. Unfortunately, every day TrendLabs researchers uncover new strains of malware designed to steal, spy and extract money from unsuspecting users.

Android devices can of course get infected by traditional means – if users click on malicious links in emails and on social networking sites, open dodgy attachments or visit infected web pages, for example – but it is malicious applications where the criminals have focussed most of their efforts. In just one month in 2012, Trend Micro saw the number of malicious apps double from 10K to 20K.

THE GROWTH OF MALICIOUS APPS

In 2012, Trend Micro detected 350,000 malicious and high-risk Android app samples, showing a significant increase from the 1,000 samples seen in 2011. It took less than three years for malicious and high-risk Android apps to reach this number—a feat that took Windows malware 14 years.

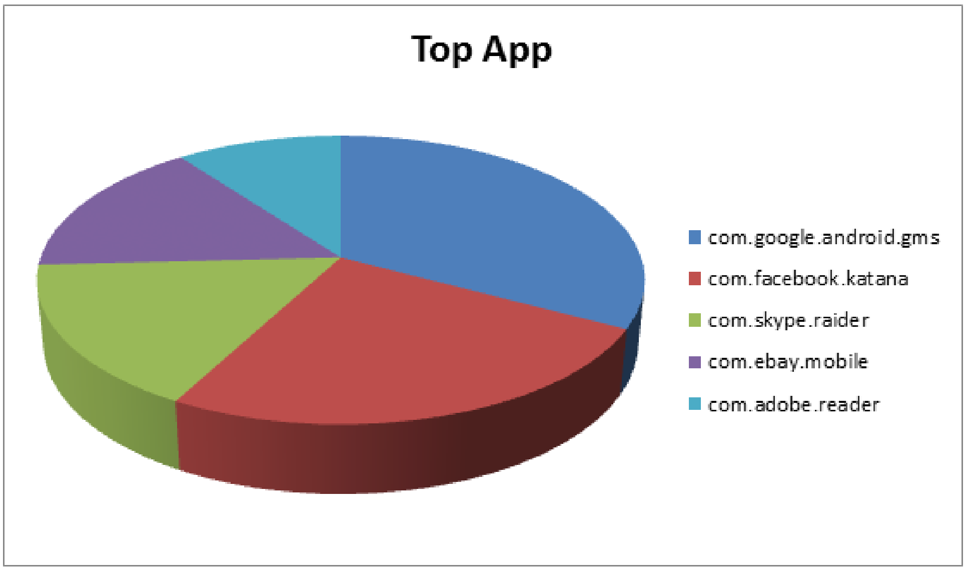
Just as Windows malware varied, so did Android malware—around 605 new malicious families were detected in 2012. Premium service abusers, which charge users for sending text messages to a premium-rate number, comprised the top mobile threat type, with transactions typically costing users US$9.99 a month. And victims of mobile threats didn't just lose money, they also lost their privacy. The issue of data leakage continued to grow as more ad networks accessed and gathered personal information via aggressive adware.

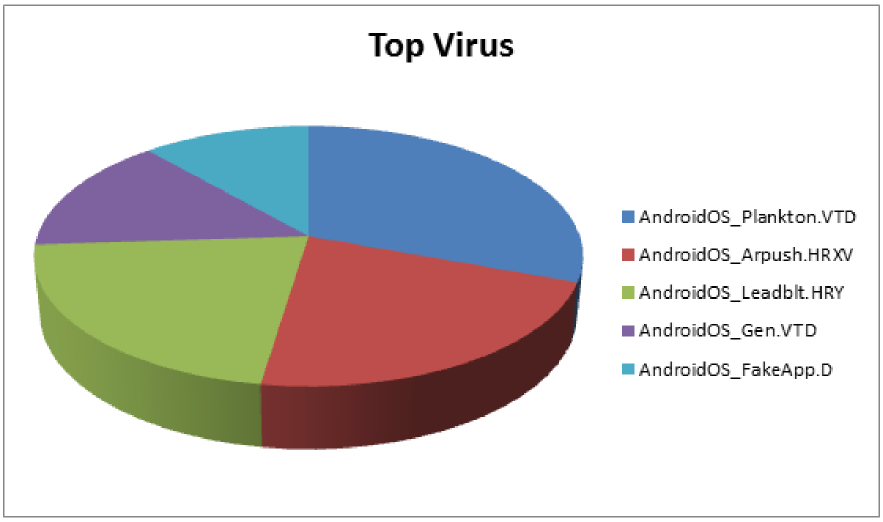
Aggressive adware in mobile devices are now similar to the notorious spyware, adware, and click-fraud malware rampant in the early days of the PC malware era. They, like PC malware, generate profit by selling user data. PC malware took advantage of loopholes in legitimate ads and affiliate networks, while today's aggressive adware can cause data leakages that aren't always limited to malicious apps. Even popular and legitimate apps can disclose data.

AUSTRALIAN APP ANALYSIS

Out of a sample of 2,052,131 Android apps scanned in Australia during January 2013, a total of 15,058 (or 0.7%) were found to be malicious or high risk. The top 5 malware variants in terms of volume of downloads in Australia during the period were:

1. AndroidOS_Plankton.VTD
2. AndrooidOS_Arpush.HRXV
3. AndroidOS_Leadblt.HRY
4. AndroidOS_Gen.VTD
5. AndroidOS_FakeApp.D





These malware variants display the following malicious behaviour:

Arpush and **Leadblt** are aggressive adware. These are apps that may actually be legitimate (or marketed as legitimate), but they are integrated with ad libraries that may be intrusive and compromise the user experience (for example, adding shortcuts in a smartphone, pushing ads even outside the app, etc.)

Plankton is a family of data stealers. These are apps that steal device information like IMEI and so on. Some variants also have backdoor capabilities, so a malicious user not only gets the stolen info the app gathers, but they can also send commands such as installing bookmarks, etc.

Fakeapp, as the name implies, are “Trojanized” or spoofed versions of legitimate popular applications. Routines vary, but these apps exhibit adware and data stealing capabilities.

Gen implies a generic or blanket detection. These are apps that may be asking for too many permissions and are deemed malicious.

Globally, in 2012 Nigeria was the country with the most malicious apps downloaded, followed by Peru and India. Other countries in the top 30 include New Zealand (17), Germany (24), and the U.S. (26). The ranking was based on the percentage of apps rated as malicious over the total number of apps scanned per country.

THE MOBILE THREAT LANDSCAPE

2012 saw an exponential increase in the number of detected Android malware, with 350,000 malicious samples by yearend. The number of detections spiked in the third quarter from 41,000 to 156,000 samples. The significant increase was due to the swell in aggressive adware.

The growth of Android malware also indicates the speed by which cybercriminals are targeting multiple platforms.

Premium service abusers topped this year’s list of most common malicious and high-risk **Android app** detections. They behave like the dialers of the desktop environment. Dialers call premium numbers and leave users with charges for calls to long-distance numbers or pay-per-call sites.

Cybercriminals may have favoured premium service abusers because they are simpler to create and less risky to use compared with committing credit card fraud or distributing fake antivirus.

Premium service abusers also topped the list of most commonly seen Android malware in 2012. Often disguised as **popular apps**, they are designed to trick users into installing them. Trend Micro spotted a rogue version of the game “Bad Piggies,” which was actually a FAKEINST variant. SMSBOXER variants spoof several best-selling Android apps, including “Angry Birds Space” and Instagram. GAPPUSIN variants, meanwhile, download other malicious apps and steal information from infected devices.

TOP MOBILE MALWARE THREATS

The main mobile malware threats to users tracked by TrendLabs include:

Premium service abuser – will automatically and secretly subscribe a user’s phone to premium rate services owned by the cybercriminals, then will text or call these premium rate numbers to make them money.

Click fraudster – will force user’s device to generate fraudulent clicks on search engine ads, generating money for the hacker.

Data stealer – will steal and then send information on the user’s phone, perhaps from the address book or calendar, back to the cybercriminal. They could then choose to use this to commit ID fraud, or sell it on the black market to others.

Spying – May track the user’s GPS data, or allow the hacker to turn on the phone’s mic or camera to eavesdrop on conversations.

Remote access tool/rooter – allows hacker to take complete control of the user’s device, with the aim of stealing financially lucrative data, spying, or forcing the phone to carry out other tasks unknown to the victim.

Adware – forces intrusive ads to appear on the user’s phone, thus generating money for the developer.

TYPES OF DATA COMMONLY STOLEN

The information stolen by data stealers—one of the top threats in 2012 —may be used by cybercriminals for malicious schemes. They can, for instance, take advantage of a user’s contact list for SMS phishing or sell stolen information in the underground market. Some frequently stolen data include:

- Application Programming Interface (API) key—a value that authenticates service users
- Application ID
- Contact list
- International Mobile Station Equipment Identity (IMEI)—a number used to identify mobile devices
- International Mobile Subscriber Identity (IMSI)—a number used to identify subscribers in a network

- Location
- Network operator
- Phone ID and model
- Phone number
- Text messages

MOBILE VULNERABILITIES

Software vulnerabilities have long been exploited by cybercriminals and attackers for their malicious schemes. For instance, zero-day vulnerabilities were exploited in attacks using the Blackhole Exploit Kit and remote access Trojans (RATs). But such vulnerabilities are no longer just limited to the desktop environment.

Android vulnerabilities were also discovered in 2012, making affected devices possible new infection vectors. Patching mobile vulnerabilities may be difficult as some carriers or phone manufacturers are slow to release updates. Older OS versions may not even receive updates—an issue similar to some Windows™ legacy systems.

Dialpad App Vulnerability

This vulnerability was found in the dialer app of certain smartphones. A vulnerable dialer app can directly execute Unstructured Supplementary Service Data (USSD) codes, including malicious ones, without prompting the user.17 Cybercriminals can use this to remotely wipe data from a device.

SMS Phishing Vulnerability

This vulnerability can allow a running app to send fake text messages to the user.18 Attackers or cybercriminals can exploit this vulnerability to bypass user permissions. They can simply use fake text messages to solicit sensitive user information.

Android Debug Bridge (ADB) Vulnerability

The ADB was created to allow developers to communicate with connected Android devices for debugging purposes. However, its implementation contained a vulnerability that can allow a malicious app to gain full control of a targeted app. Malicious apps can take advantage of this vulnerability to steal data and control the run-time behaviour of its targeted app.

Samsung Exynos Vulnerability

This vulnerability was found in a driver of certain Samsung devices. It allows any installed app to access the phone’s memory. Attackers can use this vulnerability to gain complete control of a device.

AGGRESSIVE MOBILE ADWARE AND OTHER HIGH-RISK TOOLS

App developers integrate advertising libraries to their apps to generate revenue. According to Trend Micro research, over 90% of the free apps we found contained ad libraries—modules used by ad networks to push ads.

Though ad libraries are not inherently malicious, we found apps with ad libraries that try to gather data without explicitly notifying users. They also aggressively display ads, even via notifications. The aggressive display of ads is reminiscent of Windows adware, which have been plaguing desktops and laptops and annoying users with pop-up messages.

The prevalence of aggressive adware brought three major issues to light:

Fraudulent text messages: Ad networks sometimes send out ads in the form of fake text messages. This method tricks users to click ads.

User annoyance: Some apps send out constant notifications or announcements. Not only does this annoy users, it also contributes to battery drainage.

Data leakage: Ad libraries can collect sensitive data like GPS location, call logs, phone numbers, and device information. One study found that some ad libraries even made personal information directly accessible to advertisers. Ad libraries expanded the number of parties privy to private information, which can lead to misuse.

However, efforts have been made to remedy these issues. Some of the top mobile ad networks enforced compliance measures in line with Google's revised developer policy. Their new software developer kits (SDKs) had opt-in mechanisms, giving users the ability to either allow or forbid ad networks to collect data and display ads outside apps.

Aside from aggressive adware, other high-risk tools also became prominent this year. While not inherently malicious, these apps can be exploited by malicious individuals for their own gain. High-risk tools may be viewed as the mobile equivalent of PC grayware. They can track user data like device location, phone calls, and messages. One particular app, Spy Phone PRO+, gained notoriety because despite clearly stating its purpose, it was downloaded more than 100,000 times from Google Play.

ANALYSIS: The Ad Delivery Cycle for "Free" Apps

As mentioned previously, we define those apps that demonstrate the following routines without user consent as high-risk apps:

- Displaying pop-up ads
- Getting the user's private information

One reason these apps are increasing that ads are sold. Ad agents/networks provide software development kits (SDKs) for app developers. By inserting the SDK-provided code into their apps, app developers can have ads appear inside their apps.

They would then earn money from how many ads are viewed and/or clicked. This revenue allows the developer to charge little or no money for his app.

However, users put their personal information at risk when they download these apps. Users may be able to afford many free or cheap apps, but they may fall victim to ad networks that may not show a EULA (End User Licence Agreement) or even get their private information without consent. If these privacy-violating apps increase in number, users would be at increased risk of information theft.

How to Make the Ads Safer

One benefit of ads in mobile apps is that it allows independent app developers to earn money. In addition, it also allows what would normally be expensive apps to be sold with a low (or no) price at all. Imposing a blanket ban of advertising and acquiring user information may be harmful to the mobile sector as a whole.

How can we make ad-supported apps safer for everyone? First, users should know that it is a good idea to check if the app they are downloading is reputable. To do this, users can check the comments of the app they want to download, as well as other apps offered by the developer.

App developers may also want to make it easier for users to find and read their EULA, their privacy policy, and the permissions their apps require. Aside from making these documents easier to find, the content should also be similarly easy to read and understand.

OTHER MOBILITY ISSUES - PRIVACY AND BATTERY LIFE

Just as desktop and laptop users have concerns beyond malware, so do mobile users. Privacy is a concern for both platform users, given the amount of data sent online. Desktop and laptop users often worry about the speed and performance of their computers. Mobile users, meanwhile, are concerned with device battery consumption.

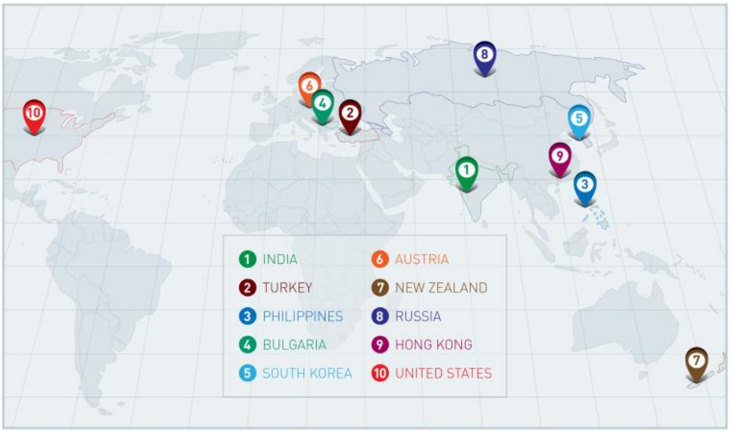
Early desktop users were rarely concerned with OS version updates as these often came several years in-between. Mobile users now face the task of regularly updating their devices as platform refreshes come in at a much faster rate.

App Use and Privacy

While apps continue to rise in popularity, users may not be aware that they can put personal data at risk. Apps like “Angry Birds” and “Angry Birds Space” can access data like a phone’s IMEI number and a user’s location.

The issue of data access is made more difficult because each user has a different definition of privacy. What may seem invasive to one user may be viewed as routine by another. It is up to users to decide the how much information they are willing to disclose to their apps.

Top 10 Countries at Risk of Privacy Exposure



India topped the list, followed by Turkey and the Philippines. Other countries in the top 30 include Germany (15), Australia (16), and the U.K. (19).

The ranking was based on the percentage of apps rated as high-risk over the total number of apps scanned per country. The ranking was limited to countries with at least 10,000 scans. The rating was based on the yearly analysis of real-time threat detection via Trend Micro™ Mobile Security Personal Edition.

Managing Battery Life

Privacy is not the only concern of users. A Trend Micro study found that battery drainage was the biggest smartphone concern of more than 60% of the respondents. While users can tweak their device settings to lower power consumption, they fail to realize that app use also causes battery drainage.

A study by Purdue University and Microsoft stated that more energy is consumed by third-party ads in free apps than the apps themselves. Recent findings from Trend Micro Longevity for Android™ app showed that 18% of the apps users downloaded rated ”poor” in battery utilisation.

SECURITY BY MOBILE PLATFORM

Performance and ease of use are not the only things now considered when buying a smartphone. Security has also become a major factor to consider, especially in the presence of mobile threats. In 2012, mobile OS vendors released platform refreshes with upgraded or new security and privacy features.

Apple has long taken an aggressive stance when it comes to securing its iOS platform. Its most recent version, iOS 6, gives users more control over their privacy. The new privacy settings let users decide which apps can access data like user location, contacts, photos, Bluetooth-shared files, Tweets, and Facebook posts. iOS 6 used Identifier for Advertisers (IFA) tracking technology, which allows users to switch off mobile tracking and be marked as unwilling participants in advertisers' data-gathering process. IFA only kept track of online habits, a marked difference from the previously used Unique Device Identifiers (UDIDs), which paired devices to users' personal information.

Jelly Bean 4.2, the latest version of the Android OS, offers users control over app access rights and access to files on a shared device. Jelly Bean had an improved setup that divided permissions into two categories—privacy and device access. It also came with real-time malicious app scanning that complemented Bouncer, a service that scans Google Play for potentially malicious apps.30

Windows 8 boasts of multiple layers of security, including three key security features—extended Information Rights Management (IRM) and automatic device encryption, real-time phishing filtering, and Kids Corner. Extended IRM and device encryption control the amount of access allowed to specific emails and documents hosted on a Windows server. Real-time phishing filtering uses Microsoft's SmartScreen URL reputation system to notify users every time they land on phishing sites. Kids Corner allows children access to only the apps and media content a parent selects.

A CASE STUDY IN APP LAW ENFORCEMENT - JAPAN

On October 30, 2012, several police agencies in Japan arrested a number of suspects for violating the newly implemented cybercrime law. Five suspects were arrested, including an IT company executive for creating malicious apps known as "the movie virus." In another case, a company executive was arrested who allegedly created the malicious apps Longer Battery Life, Signal Improvement, Sma Solar, Power Charge, or Solar Charge.

In both of these incidents, the suspects targeted smartphone users in Japan. The apps were installed by smartphone users due to their enticing names and descriptions. Some are named in Japanese as Video Reply, Battery Longevity or Solar Power Generation and the like. Users tend to install them expecting the functionality their names imply. These apps, however, could hardly deliver on their claims but instead executed their harmful routines.

In this information theft routine, the cybercriminals focus on the user’s phone book. The names, phone numbers, and email addresses of the people listed in the phone book were extracted and sent out to the external server. Because of this, the user information of the device’s owner and his/her friends and acquaintances are stolen by the attackers.

THE FUTURE OF ANDROID MALWARE

As the popularity of Android continues to grow, there will be more third party app stores and people will become more mobile and more social. There will, however, be more risk and an increase in the number of threats. Every device and every service is becoming so deeply interlinked with every other and with the cloud, that any computing environment is no longer discrete. Changes and insecurities in any part of the user experience chain can and do have amplified effects elsewhere.

The volume of malicious and high-risk Android apps will reach 1 million in 2013. Aside from increasing in number, here are additional predictions about Android malware:

New delivery methods: Social networking apps now allow users to sync various social networking accounts. Malicious individuals will take advantage this feature to simultaneously post mobile malware links to different social networks.

QR codes will also be exploited by malicious individuals to spread Android malware.

Combined mobile-desktop threats: Android malware will also become part of attack chains involving desktop threats, particularly for attacks targeting online banking transactions.

More devices (and more threats) in the workplace: Bring your own device (BYOD) is fast becoming a norm for many organizations. But rather than having uniform devices, users will opt to bring multiple devices that run on different platforms. Cybercriminals and attackers will take advantage of the multiple devices and platforms at work to spread malware.

More sophisticated malware: Android malware will continue to evolve to avoid detection by security apps and bypass platform security measures. This evolution will come in the form of rootkits. Security researchers have published a proof-of-concept (POC) rootkit, which shows how rootkits can be used by malware authors to gain full control of a mobile device without being detected.

New targets: More malware attacks will focus on new payment methods like near-field communications (NFC) to steal financial information.

HOW TO PROTECT YOUR MOBILE DEVICES

With the constant changes in the mobile threat landscape, smartphone owners should secure their devices. Here are some steps to protect devices against mobile threats:

Use your device's built-in security features. Opt for phones that have security features and use them. Built-in security features like password, pattern, or PIN lock options prevent outsiders from accessing your data should your phone get misplaced or stolen.

Do research on apps before downloading them even from trusted sources. Cybercriminals often disguise malware by spoofing popular apps. Familiarize yourself with details of popular apps (e.g., the name of the developer) to ensure that you download the legitimate version. It is advisable to download from reputable app stores like Google Play than third-party ones.

Read permissions before installing apps. Malicious apps usually seek access to various kinds of data stored in a mobile device. Read permissions to check what type of actions an app will perform once installed. Be wary of apps that require more permissions than necessary (e.g., a calendar app that seeks access to your call logs).

Regularly check for software updates. Software updates are usually released to address issues like vulnerabilities or improve software performance.

Invest in a security app. Security apps can inform you if an app has malicious or suspicious behaviours. Some apps even protect data with features like remote wipe or privacy scanner.

Set BYOD policies at work. Organisations should decide which employees will only be allowed to bring devices and what types of devices they will support. Set up procedures to take if a device is stolen, lost, or damaged.

Summary: Security Advice To Mobile Users

- Use your smartphone's built-in security features.
- Avoid using free but unsecured Wi-Fi access.
- Scrutinize every app you download regardless of source.
- Understand permissions before accepting them.
- Consider investing in a mobile security app

MAKING APPS SAFER: THE JAPANESE APPROACH

The Japanese Ministry of Internal Affairs and Communication (MIC) has issued guidelines for Japanese app stores and developers that list the eight items that should be included in privacy policies. Seeing if all eight are present would be a good way to know whether or not the privacy policy of user's app is really legitimate. MIC is not alone in these types of efforts; telecom trade groups like the GSM Association and governments such as the United States have released similar guidelines.

Items	Remarks

The Developer ‘s Name	Indicate the full name of the app developer and contact address.
User Information Type	Enumerate all types and contents of the user information extracted.
Method	Indicate how to extract the information — if it is through user’s own input or if it is automatically acquired.
Purpose	Indicate if it is used for further services to users or for other purposes. If it is used for the ad-delivery or marketing purposes, indicate this.
Notice / User Involvement	Indicate how to release the notice, how to get the agreement, how and where to post the privacy policy, who are the target users to get the agreement, and when these are conducted.
The Third-Party Providers, External Senders, and Info-gathering Modules	Indicate if it contains such items as the third-party providers, external senders, and info-gathering modules.
Contact Details	Indicate the contact details such as phone numbers, email addresses, etc.
Change Procedure	Indicate the procedure when the privacy policy is changed.

Table: MIC Guidelines for Privacy Policy

ANALYSIS: APPS IN THE ENTERPRISE - THE RISKS OF BYOD

When we talk about consumerisation trends these days we often concentrate on the device, the ‘D’ in BYOD (Bring Your Own Device). But enterprise employees have been using consumer-grade applications in the workplace for a lot longer, such as the popular Instant Messaging or email clients provided by Yahoo, Google and others.

Thanks to the ubiquity of cloud computing and powerful smartphones and tablets this trend of Bring Your Own Apps (BYOA) is gaining pace, and needs to be understood and managed better by IT staff.

Popular consumer-grade online apps now exist to serve a huge range of needs including online storage and file sharing (eg Dropbox); blogging (WordPress, Blogger); telephony (Skype); social media and engagement (Twitter, Facebook, Hootsuite); and collaboration (Huddle, Yammer).

The problem is that, just as with the BYOD trend, these unsanctioned tools have largely crept into the enterprise in an ad hoc, piecemeal manner. Yes, they’re great time-savers and allow users to work in the way they have become accustomed at home, with intuitive, productivity-enhancing tools, but they also bring extra risk into an organisation.

The risks mainly stem from the fact that the majority of these apps were not designed to be used in an enterprise environment, with all its associated security policies and controls. They were built primarily with consumers in mind, which can raise issues of data privacy if sensitive corporate information ends up on the servers of a third party company.

While many web firms have strict auditing and data centre security controls of their own, the vetting of such providers is something IT managers ideally need to be involved in from the start. Similarly, there are risks around what happens if a cloud provider goes bust or is bought, or even if a member of staff leaves along with their private web account – what happens to the corporate data then?

IT also faces a potential security disaster if users are allowed to download whatever applications they wish from online app stores. While official iOS and Window Phone channels offer certain protections, Android's open ecosystem makes it easy for cyber criminals to upload malware-ridden apps masquerading as legitimate software.

The exponential rise in the volume of Android malware is proof that IT teams need to carefully manage the downloading of apps onto corporate or BYOD devices.

Some BYOA tips

IT teams have to realize that BYOA is happening because users find consumer tools much easier to use and more readily available than their enterprise equivalents. IT therefore needs to harness the obvious benefits of continued use of consumer-grade apps while putting in place the practices and policies to manage them securely.

The following steps should help start the process:

- Draw up clear policies on the use of consumer applications in the workplace and detail the process for reviewing new tools.

- Once agreed upon, communicate the policies to employees. Remind employees of these policies regularly, alongside other ongoing communications on IT policies.

- Audit existing tools in use in the organisation, then decide which ones can be kept and managed securely.

- Establish platform owners for each that are responsible for keeping infosecurity teams updated of any changes.

- Suggest logical points of consolidation between teams – i.e.: all social teams on TweetDeck or Hootsuite, not both – or upgrade to an enterprise grade equivalent.

- Consider client security and mobile device management for all BYOD and corporate devices to ensure only safe and pre-approved apps can be downloaded.

APPENDIX A: Technical Analysis: Investigation into Japanese Apps

To evaluate the risk to user privacy, Trend Micro analysed the 200 most popular free apps (both general apps and gaming apps) in the Google Play app store in Japan as of August 31, 2012.

Trend Micro evaluated the risk of privacy violation on these sample apps. The details of the sampled data are indicated in the following tables.

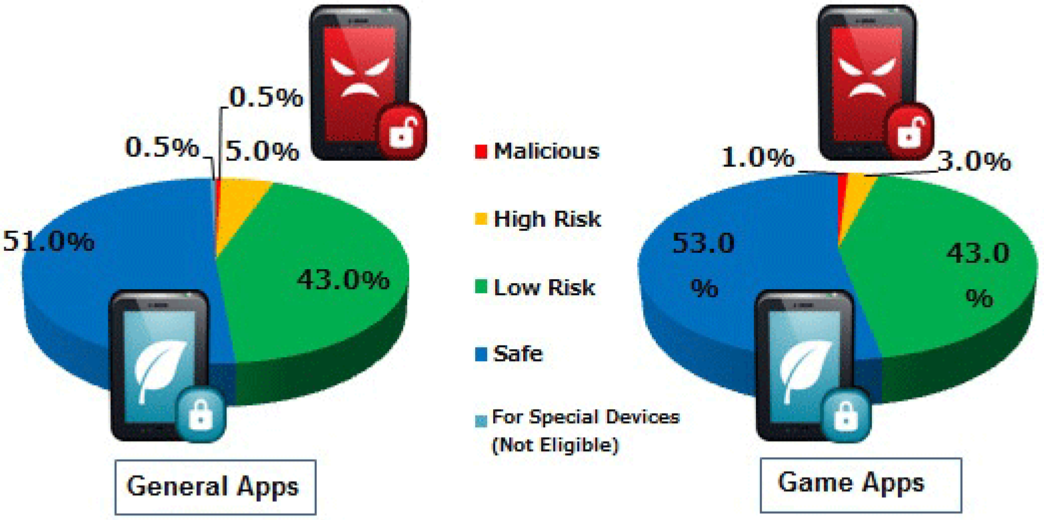
Location	Google Play – Japan
# of APK Files	400
Targeted Categories	Google Play－Applications, FreeGoogle Play – Games, Free
Date Covered	August 31, 2012
Sampling Criteria	Top 200 of the most popular apps (respectively both general apps and game apps) out of all free apps in Google Play Japan according to Google's announcement as of August 31, 2012

Table: Details of the Examined Apps

We used Trend Micro Mobile App Reputation (MAR) to examine these apps, looking at three areas in particular:

- unwanted routines
- information leakage (focusing on privacy violations)
- high memory usage

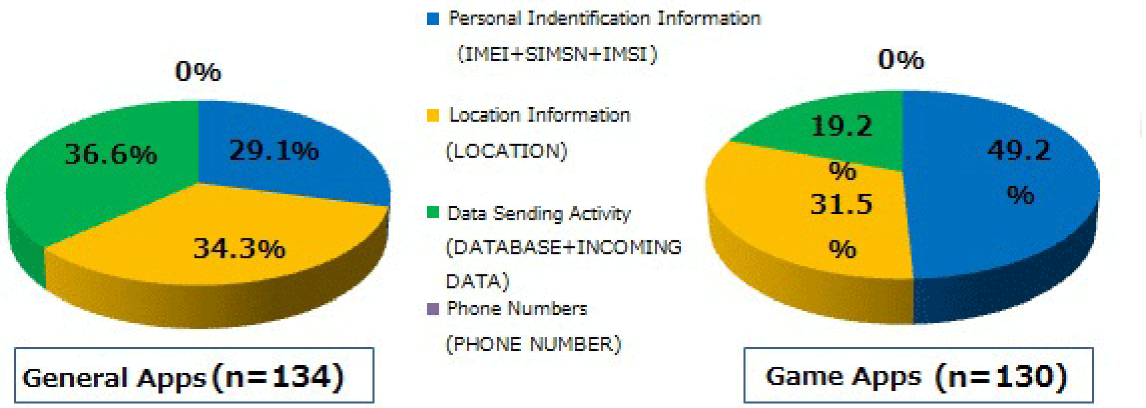
Based on our analysis, we grouped the apps into four categories, from highest to lowest risk, namely: "Malicious", "High Risk", "Low Risk", and "Safe".



App Ratings

As you can see, 0.5% (one app) of all general apps and 1% (two apps) of all game apps are considered “malicious”. 5% of all general apps and 3% of all game apps are considered as “high risk”. More “high risk” apps are present among general apps than gaming apps.

Apps considered as “Malicious” have unwanted routines like delivering malicious ads. App developers should be careful about which ad network they use, as if their apps is found to contain malicious apps, their reputation may be damaged. The same is true if their app leaks personal information.



Type of private information disclosed

The above chart shows the types of personal information that is acquired by the studied apps. This information was also used in rating the risk level of apps.

Trend Micro Mobile Security has a function known as “Privacy Scan”. With this, users can easily check the privacy risks of their installed apps. It can also scan apps as they are being installed; users can also check the already-installed-apps manually to check their privacy risks.)

If the scan results make you feel suspicious about the possibility of a privacy leak, check the comments on its download page, as well as its EULA and privacy policy. If these convince you that the app is legitimate, continue – but if in doubt, uninstall.

APPENDIX B: Pirated App Stores on iOS

During the first weeks of January 2013 there were news stories about how iOS users could now install pirated apps without having to jailbreak their phones. This was made possible by certain Chinese app store-like services.

The same features which allow enterprises to deploy their own custom apps have now been abused to deliver pirated apps to users.

This “newly discovered” method represents one of the methods to get malicious/fake apps onto iOS devices. However, because the iOS sandbox has not been compromised, what each app can and can’t do is rather limited. The iOS app may try to send out some personal privacy information to external server which creates privacy data leakage problem.

At this point in time it is not likely to be much of a security threat, as the number of users who would actually use these “pirated” app stores is rather limited. However, it does represent an interesting avenue for targeted attacks in enterprise settings. It would not take much effort to refine this into something that could more seamlessly get users to install apps on their own iOS devices via a link they receive on their desktop or laptop and connecting their phone via USB. Expect Apple to fix this in future.

What should users learn from this? It's a lesson that Android users have known for a while now – yes, you can install bad apps onto your device. Attackers have to work harder to do so, but it's still possible. As users, we need to be careful not to install any app from unknown sources. Mobile private information leaks always start from installing malicious apps on the device, and even iOS users aren't spared the risk of bad apps.

APPENDIX C: Technical Analysis: Android Malware Found to Send Remote Commands

Apart from those apps that register users for unwanted services and those that aggressively push ads, Android users should also worry about apps with backdoor capabilities.

While premium service abusers and adware accounted for the majority of malicious apps in 2012, they are, however, not the only threats to Android. Reports of a botnet running on more than a million smartphones recently made the headlines, which goes to show that attacks aimed at Android devices are varied and far from over.

Prior to these reports, we have been seeing these malware since July 2012 and have so far detected 4,282 in the wild. The related samples we analysed (detected by Trend Micro as ANDROIDOS_KSAPP.A, ANDROIDOS_KSAPP.VTD, ANDROIDOS_KSAPP.CTA, ANDROIDOS_KSAPP.CTB, and AndroidOS_KSAPP.HRX) were from a certain third-party app store, though we suspect there are other available several sites. Typically, these apps are marketed as gaming apps, some of them bearing or are repackaged versions of popular gaming titles.

The first batch of samples we analysed was packaged using the same app title, purportedly from the same company.

Once any of these malicious apps is installed in a device, it communicates to the following remotes sites to acquire compressed script then parses the said script:

- http://{BLOCKED}y.{BLOCKED}i.com:5222/kspp/do?imei=xxxx&wid=yyyy&type=&step=0

- http://{BLOCKED}n.{BLOCKED}1302.com:5222/kspp/do?imei=xxxx&wid=yyyy&type=&step=0

- http://{BLOCKED}1.com:5101/ks/do?imei=xxxx&wid=yyyy&type=&step=0

This parsing of the downloaded script makes it more complicated than a typical botnet-related malware found on Android since the malware can equip itself with a new script.

The malware also updates the running script, to avoid being detected by antivirus (AV) software, as highlighted above. This updating mechanism enables the malware to download a new variant of itself. This remote script also contains customized commands that a remote attacker can execute onto the infected device. For example, the app can execute a test call function (code seen below):

After parsing the remote script, new Java object e.g. variables and functions can be instantiated using Java reflections, thus dynamic remote code can be executed on local device, which may lead to download other possible malicious files.

To prompt users to install these files, the app will show notification bar or pop-up windows. Users who download these file are unfortunately making their devices vulnerable to further malware infection. Not to mention that by installing ANDROIDOS_KSAPP variants, users are allowing their devices to be controlled by a remote user who can execute more sinister commands.

APPENDIX D: GLOSSARY OF TERMS

App store	App stores are sites where users browse, download, and buy computing programs or "apps", mostly for mobile devices. Though Apple claims copyright to the phrase "App Store," many still refer to it when discussing apps across operating systems and brands. Device manufacturers and OS developers have native app stores built into their devices. These include Google Play, Blackberry App World, Samsung Apps, and iOS App Store. Third party app stores also exist for users who seek specific apps not available on native app stores. GetJar, MobiHand, and Handango belong to this category. The mobile app market offer apps free, on trial, or for a fee. Cybercriminals leverage this by tricking users to download bogus apps that steal credential data off mobile devices.
Application/Apps	Applications are software programs developed for end-users to accomplish specific computing tasks. Apps, on the other hand, mostly refer to programs developed for mobile devices. Both depend on the platform and operating system they were designed for. Most applications are used to process documents and are bundled with other applications to form a suite, just like Microsoft Office. This is also the same for mobile apps. Both applications and apps are popular for their various uses in entertainment, novelty, education, reference, and others. However, mobile apps are patronized more for entertainment and communication purposes. Applications are bought with the operating system or individually from physical stores or websites. Apps are usually downloaded from mobile app stores.
Click fraud	Click fraud is a type of internet crime that occurs in pay-per-click online advertising when a person, automated script, or computer program imitates a legitimate user of a web browser clicking on an ad, for the purpose of generating a charge per click without having actual interest in the target of the ad's link.
Crimeware	Crimeware is a general term for software used to perpetrate crime, such as stealing personal identities, money or proprietary information. Crimeware can spread by way of viruses, Trojan horse programs, worms, spyware, or adware.
Cybercriminals	Cybercriminals are hackers and other malicious users that use the Internet to commit crimes such as identity theft, spamming, phishing and other types of fraud. Cybercriminals often work together forming cyber gangs.
Dialers	Dialers are software that change modem configurations to dial high cost toll numbers or request payment for access to specific content. Many users run

	dialers without knowing that some of these programs actually dial long distance numbers or connect to pay-per-call sites; and that they are being charged for the calls. Dialers are often offered as programs for accessing adult sites.
fake app(s)	These are apps in mobile devices that trick users into downloading them by using legitimate companies or popular references. They may also pose as quirky and attractive apps, providing interesting services like live wallpapers or real-time spying tools. Once installed on a mobile device, fake apps can perform a variety of malicious routines. They can persistently push ads, track and report location and other sensitive information, or subscribe users to premium services without consent. These can all lead to loss of data and privacy and waste of device resources.
Malware	Malware is a general category of malicious code that includes viruses, worms and Trojan horse programs.
Spyware	Spyware is a program that monitors and gathers personal information and sends to a third party without the user’s knowledge or consent. Many users inadvertently install spyware when accepting the End User License Agreement (EULA) for certain free software.
Threat	Threats are security issues that include the following: malware, grayware/adware, spyware, spam, phishing, and bots/botnets.
Virus	A virus is a computer program that can copy itself and infect a computer without a user’s permission or knowledge.
Vulnerability	A vulnerability is a security weakness typically found in programs and operating systems leaving computing systems open to malware and hacker attack. When vulnerabilities are exposed, software vendors will provide fixes or patches for their products.
Zero-day exploits	Zero-day exploits refer to software vulnerabilities that have been found in-the-wild before security researchers and software developers become aware of the threat. Because of this, they pose a higher risk to users than other vulnerabilities.

- END OF SUBMISSION -

Supporting information:

TrendLabs 2012 Mobile Threat and Security Roundup
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-repeating-history.pdf

TrendLabs Digital Life E-guides:
The 4Ws and 1H of Mobile Privacy
When Android Apps Want More Than They Need
5 Simple Steps to Secure Your Android-based Smartphone
http://about-threats.trendmicro.com/ebooks/

Trend Micro Infographic: Behind the Android Menace: Malicious Apps
https://blog.trendmicro.com/trendlabs-security-intelligence/infographic-behind-the-android-menace-malicious-apps/
http://www.trendmicro.ae/infographics/android-threats/index.html
http://www.trendmicro.ae/infographics/android-threats/index.html

Trend Micro infographic: Unwrapping Mobile Security During the Holidays
http://blog.trendmicro.com/trendlabs-security-intelligence/unwrapping-mobile-security-during-the-holidays/

CCAAC INQUIRY SUBMISSION FROM TREND MICRO ANZ

Authors:

Greg Boyle	Sr Global Product Marketing Manager, Consumer Mobility Solutions, Trend Micro
Adam Biviano	Senior Manager, Strategic Products, Trend Micro ANZ
John Papanidis	PR Manager, Trend Micro ANZ

with additional information from Trend Micro research reports, blogs, and contributors.

Contact:
John Papanidis
Public Relations Manager
Office: +61 2 9870-4888
Mobile: 0401 237 854
Email: john_papanidis@trendmicro.com.au

Trend Micro ANZ

Level 3
2-4 Lyon Park Rd
North Ryde, NSW 2113
Australia