Symantec

# SECURITY RESPONSE

# Mobile Adware and Malware Analysis

**Bartlomiej Uscilowski**

Version 1.0 – October, 2013

*“The percentage of madware on Google Play is steadily increasing, reaching over 23 percent in the first half of 2013.”*

Follow us on Twitter
@threatintel

Visit our Blog
http://www.symantec.com/connect/symantec-blogs/sr

Symantec

# CONTENTS

# OVERVIEW

Madware and malware are two types of Android security risks that have had a consistent presence over the past few years. They have been found in apps hosted both on Google Play and on third-party app stores.

Madware refers to apps that use aggressive ad libraries. There are at least 65 known ad libraries and over 50 percent of them are classified as aggressive libraries. The percentage of madware on Google Play is steadily increasing, reaching over 23 percent in the first half of 2013. On average, apps were trending towards using two ad libraries, regardless of how aggressive the ad libraries are.

The presence of malware in each app category varies on Google Play and on third-party app stores, as certain categories contain more than others. The growth of the number of known malicious samples is much higher than the linear growth of the number of malware families. Apps from the Personalization and Libraries & Demos categories contain the most madware. Most third-party app stores host more security risks than Google Play does. However, the level of security risks on 11 percent of known third-party app stores is lower than on Google Play.

Symantec

# AGGRESSIVE AD LIBRARIES IN FREE ANDROID APPS

> “Developers can monetize mobile apps by displaying advertisements on them.”

# Aggressive ad libraries in free Android apps

## Ad library aggressiveness

Developers can monetize mobile apps by displaying advertisements on them. They can use at least 65 ad libraries that we know of for this purpose. These libraries have the ability to collect information about the app's user in order to serve targeted advertisements. However, that can be abused and depending on which ad library features the developer chooses to use, personal data can be leaked through an ad library. Additionally, an ad library can exhibit annoying behaviors such as displaying ads in the notification bar, creating ad icons or changing Web browser bookmarks.

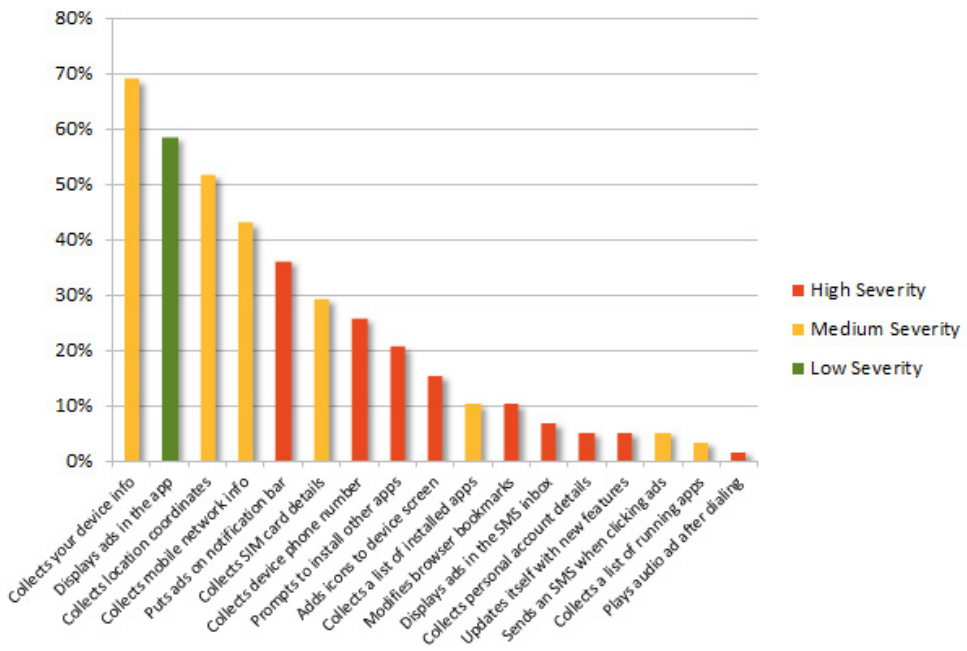


*Figure 1. Ad libraries' behaviors and their levels of severity*

There are 17 groups of behaviors that we associate with ad libraries. Figure 1 presents the usage of different behaviors among all of the ad libraries.

We can see that more than two thirds of ad libraries collect device information, such as its IMEI number or phone producer and model. This is not too intrusive and many other apps collect the same information. However, a third of ad libraries display ads in the notification bar, which may annoy the user.

Because some behaviors are more intrusive or annoying to the user than others, we defined three severity levels to describe how aggressive the ad library behavior is:

- Low severity behaviors (green bar): No leakage of any data, just displays ads in the app window
- Medium severity behaviors (yellow bars): Leaks some data that is not considered to cause much harm (such as location information, mobile network information). Also, most users do not find them annoying.
- High severity behaviors or madware behaviors (red bars): The most aggressive behaviors. Leaks private data (phone numbers or user account information) or annoys the user (shows ads in the notification bar or plays a voice ad when making a phone call).

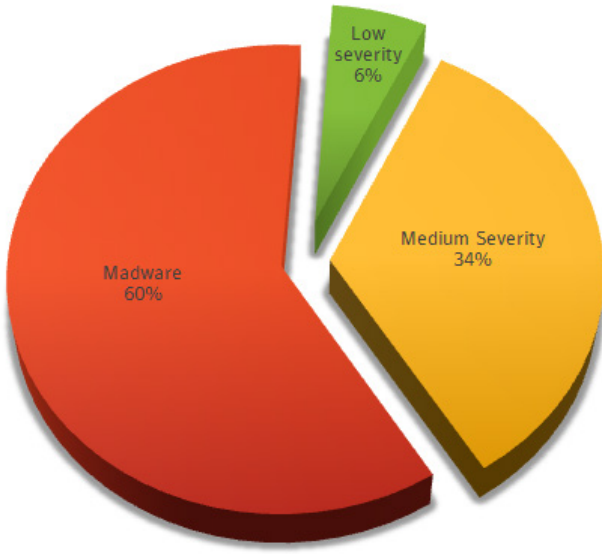


*Figure 2. Percentages of ad libraries' aggressiveness*

Based on how aggressive their behaviors are, we

classified ad libraries into one of three groups: low severity, medium severity and high severity. Any app containing high severity ad libraries is called madware and 55 percent of all known ad libraries are classified as such (see Figure 2).

It is important to stress that this is based on the capability to use certain behaviors. An app developer can decide to use only a subset of behaviors available for a given ad library. However, we consider it would have negligible impact on the analysis, so we assume all available behaviors are used.

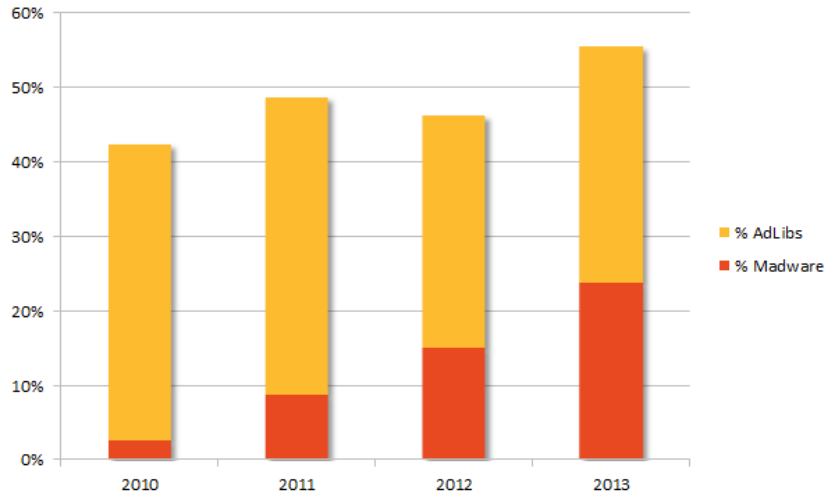


*Figure 3. Percentage of apps on Google Play containing aggressive and/or any ad library seen each year*

## Aggressive ad libraries on Google Play

The percentage of apps containing aggressive ad libraries (madware) on Google Play goes up each year (Figure 3). About half of all apps are supported by ad libraries and this has been consistent over the years, with a slight increase to 55 percent so far this year. However, in general, the percentage of madware grows at constant rate. In 2012, 15 percent of apps seen on Google Play included madware, while in 2013 up to the end of June, we have seen that 23.8 percent of apps contain madware.

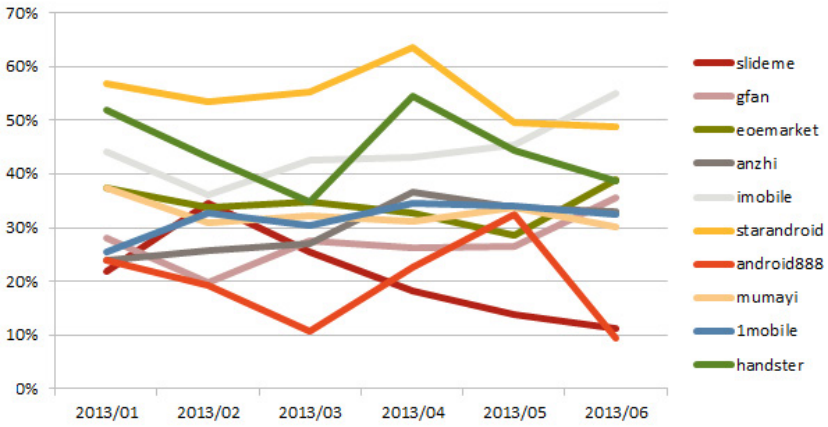


*Figure 4. Percentage of madware in new or updated free apps on the oldest third-party stores in 2013*

## Third-party app stores versus Google Play

The presence of madware on third-party app stores is different than on Google Play. Figures 4 and 5 show the trend in the percentage of madware in the oldest app stores and the largest app stores. We can see that:

- The majority of third-party stores have a higher percentage of madware than Google Play.
- The percentage of madware

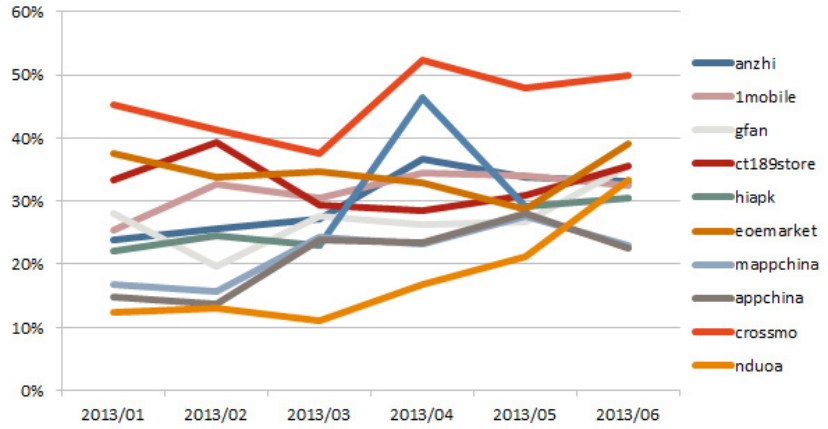


*Figure 5. Percentage of madware in new or updated free apps on the largest third-party stores in 2013*

does not show clear signs of increasing or decreasing.
- The oldest app stores have a higher percentage of madware.

In Figure 6, we compare the levels of security risks on Google Play with third-party stores hosting more than 1,000 free apps. There are 175 such third-party stores in total and only 19 (11 percent) of them meet up to the Google Play standard (Google Play is regarded as a trusted source). That is, the percentage of security risks in those stores is lower or equal to Google Play.

Figure 7 shows the third-party app stores with the largest proportion of madware, among apps added or updated in the first half of 2013. In these 'madware stores', over 40 percent of newly published (or updated) apps were madware. We recommend users avoid downloading apps from them.

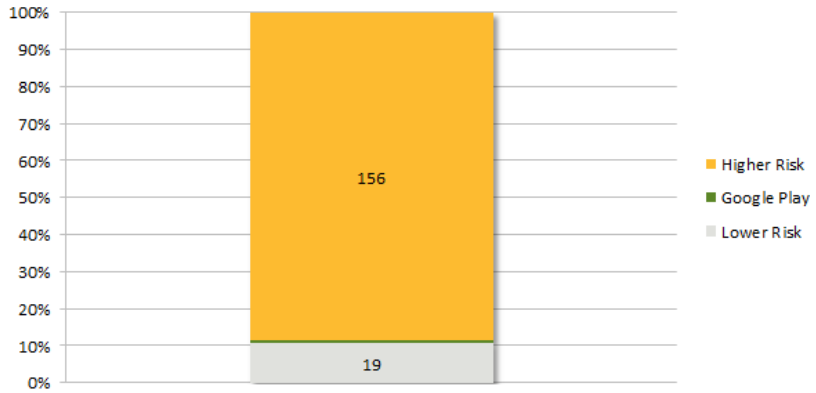


*Figure 6. Insecure versus secure third-party stores based on the Google Play standard from January to June 2013*

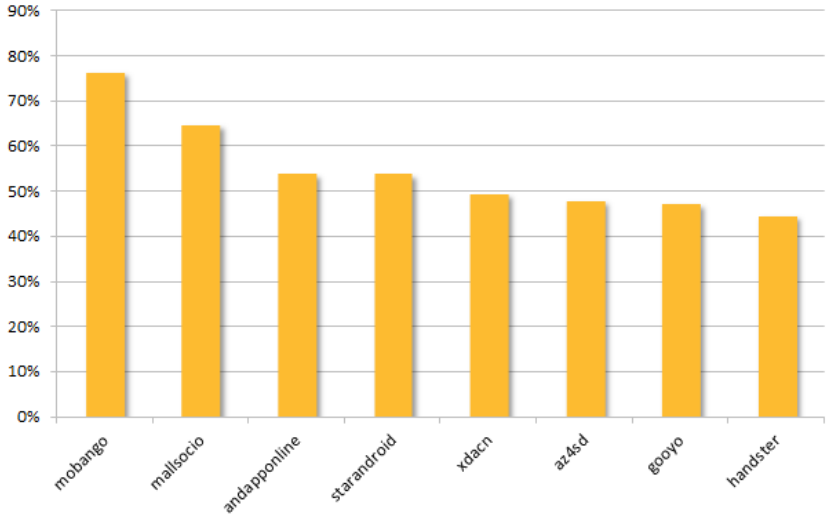


*Figure 7. Major third-party madware stores from January to June 2013*

## Number of ad libraries per app

The average number of ad libraries used in ad-supported apps has grown from 1.6 in 2011 to 1.8 in 2012. This figure dropped to 1.7 in 2013 so far. However, when aggressive ad libraries are used, the average number of ad libraries per app is higher: 2.75 in 2011, 2.79 in 2012 and 2.2 in 2013. There is a strong shift towards using two ad libraries per app when it comes to madware observed this year.

When we looked at the distribution by the number of ad libraries used, we can see that when developers use aggressive ad libraries, they are more eager to use a higher number of ad libraries (Figure 8 and Figure 9).

We can also see a general trend in the use of more ad libraries per app in 2012 than in 2011.That trend continues in 2013 with the largest increase seen in apps containing two ad libraries. This is more pronounced among apps using aggressive ad

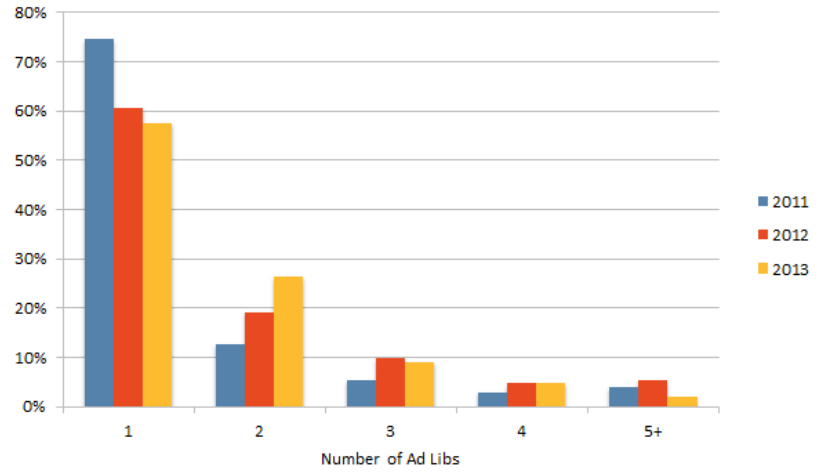


*Figure 8. Distribution of the number of ad libraries used per app for all ad supported apps*

libraries – the use of two ad libraries increased from 32.2 percent in 2011 to 35.5 percent in 2012 and it grew further to 43 percent in 2013 (Figure 9). Interestingly, there is a drop in apps using more than four ad libraries when it comes to apps using aggressive ad libraries in 2012 and 2013 (Figure 9) while in general, the percentage of free apps supported by more than four ad libraries increased in 2012 (Figure 8).

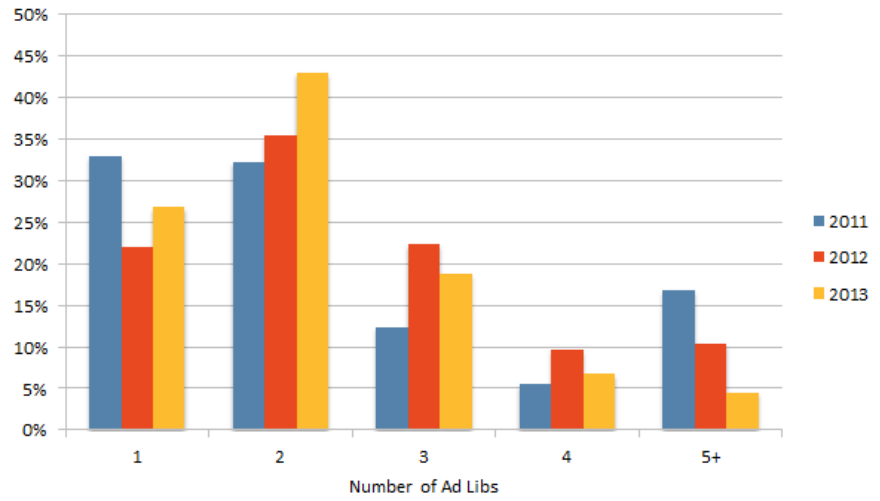


*Figure 9. Distribution of the number of ad libraries used per app for apps using aggressive ad libraries*

## Madware trends in app categories

The madware usage differs between app categories. There are 25 app categories in total and most of them have seen an increase in the usage of madware in 2012 compared with 2011, and a further increase in 2013. The highest increase can be observed in the Personalization category, while the Libraries & Demo category recorded a high increase in 2012 and a slight drop in 2013. It is worth mentioning that a lot of live wallpapers and widgets fall into the Personalization category, which explains such a huge increase of madware, although we cannot provide the breakdown for that category. The bar chart in Figure 10 shows the categories with the highest increase in the percentage of madware.

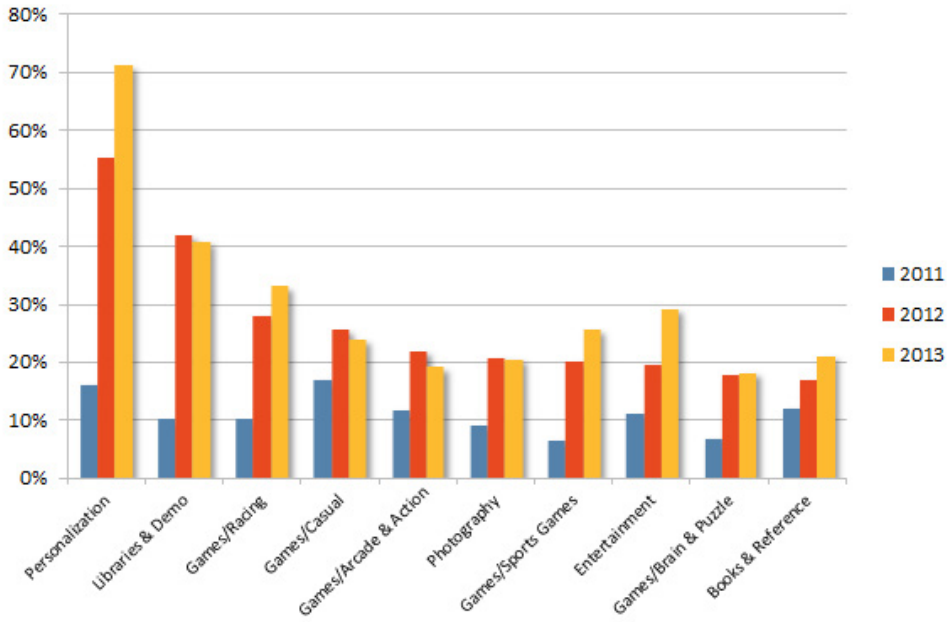


*Figure 10. Madware usage in Google Play based on app categories*

Symantec

# ANDROID MALWARE


> “There is a massive growth in the volume of malware families and samples...”

# Android malware

## Android malware trend

The trend in the volume of malware threats, variants and samples is presented in Figure 11. There is a massive growth in the volume of malware families and samples:

- The number of known malware families increased by 69 percent between June 2012 (121 threat families) and June 2013 (204 threat families).
- The number of known malware samples increased almost four times between June 2012 (about 32,000 samples) and June 2013 (about 273,000 samples).

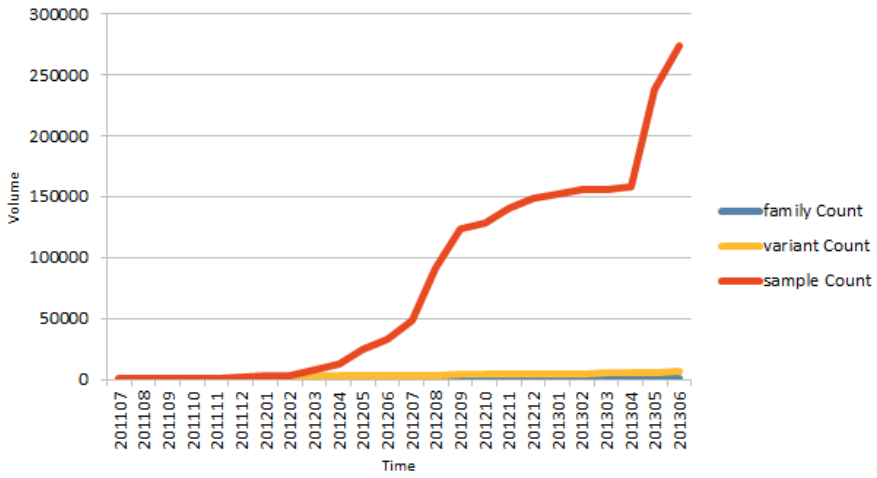


*Figure 11. Android malware growth*

## Malware trends by category

The percentage of malware in each app category is presented in Figure 12. The values have been gathered on all apps available since 2010. On third-party app stores, the most dangerous is the Games/Arcade & Action category followed by the Photography category.

However, when we just look at Google Play and how the ten most dangerous categories have changed in 2011, 2012 and so far in 2013 (Table 1), we can see that the Photography category is no longer that dangerous. Currently, users should be cautious when downloading apps in the Multimedia category. It is worth noting that the Entertainment category always makes it into the top three most dangerous categories.

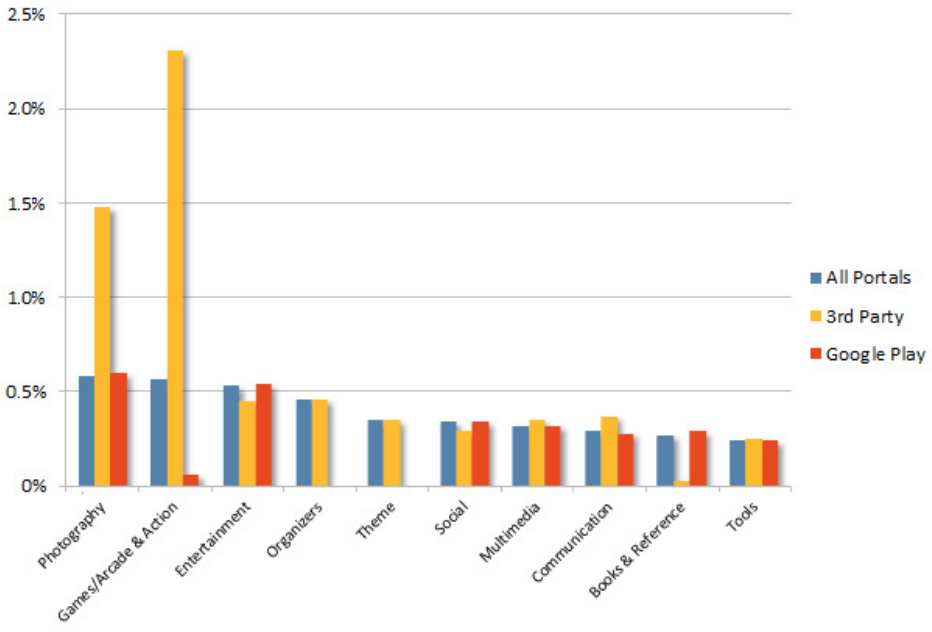


*Figure 12. Top ten app categories with the highest percentage of malware*

*Table 1. App categories on Google Play with the most malware between 2011 and 2013*

| 2011 Category | 2011 Malware Percentage | 2012 Category | 2012 Malware Percentage | 2013 Category | 2013 Malware Percentage |
|---|---|---|---|---|---|
| Photography | 1.77 | Books & Reference | 0.56 | Multimedia | 0.72 |
| Entertainment | 1.01 | Entertainment | 0.36 | Social | 0.37 |
| Communication | 0.47 | Games/Racing | 0.35 | Entertainment | 0.3 |
| Tools | 0.45 | Multimedia | 0.29 | Lifestyle | 0.23 |
| Social | 0.31 | Personalization | 0.24 | Communication | 0.19 |
| Personalization | 0.19 | Social | 0.2 | Tools | 0.16 |
| Travel | 0.18 | Communication | 0.18 | Games/Sports Games | 0.14 |
| Games/Casual | 0.13 | Games/Cards & Casino | 0.15 | Games/Racing | 0.08 |
| Productivity | 0.12 | Games/Casual | 0.15 | Games/Cards & Casino | 0.05 |
| Transportation | 0.12 | Travel | 0.14 | Games/Casual | 0.05 |

## Third-party app stores hosting malware in 2013

Although malware slips into Google Play, most malware is hosted on third-party app stores. There are also stores that only host malware. However, such stores do not live long or they offer very few apps, with less than 1,000 apps added in first six months of this year.

When it comes to more active third-party app stores, the percentage of malware apps added in the first half of 2013 can be as high as 10 percent. Figure 13 shows the percentage of malware added to third-party app stores in the first half of 2013. In the case of Anzhi portal, almost one out of ten apps added this year is malicious.

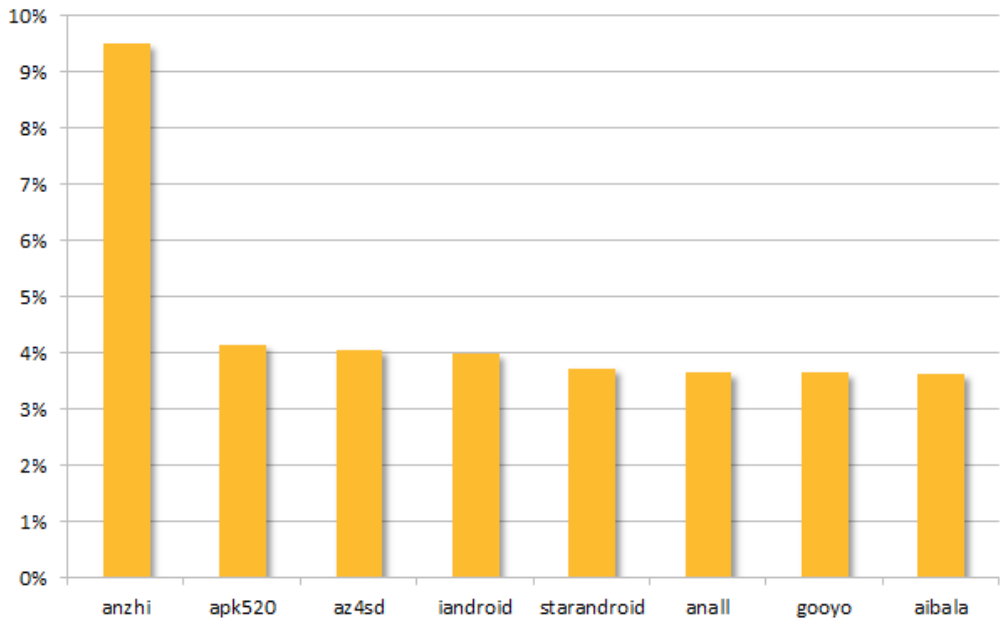


*Figure 13. Third-party app stores hosting the most malware from January to June 2013*

# CONCLUSION

> “There was a large increase in the number of malicious APKs in the middle of 2012 and again in the second quarter of 2013.”

# Conclusion

We see a constant growth in the presence of security risks among Android applications, be it malware or madware. There was a large increase in the number of malicious APKs in the middle of 2012 and again in the second quarter of 2013. The presence of madware on Google Play has grown from 2011 to 2012 and again in the first half of 2013, while the vast majority of third-party app stores host an even greater presence of madware and malware. By the end of this year, we can expect one in four free apps available on Google Play to contain madware.

# Resources


- http://www.symantec.com/connect/blogs/spyware-and-adware-mobile-devices
- http://www.symantec.com/connect/blogs/new-symantec-research-motivations-recent-android-malware
- http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/motivations_of_recent_android_malware.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Oct__androidmalwarewhitepaper
- http://www.symantec.com/connect/blogs/top-5-security-predictions-2013-symantec-0
- http://www.mobilesecurity.com/articles/269-making-madware-a-choice-for-everyone
- http://www.mobilesecurity.com/articles/270-how-annoying-is-that-app
- http://www.mobilesecurity.com/articles/271-the-state-of-madware
- http://www.mobilesecurity.com/articles/274-madware-infographic
- http://www.mobilesecurity.com/articles/285-madware-makers-mixing-up-their-code
- http://www.mobilesecurity.com/articles/312-how-to-avoid-mobile-adware
- http://www.networkworld.com/news/2012/102212-trendmicro-android-malware-263542.html
- http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-3q-2012-security-roundup-android-under-siege-popularity-comes-at-a-price.pdf
- http://blog.trendmicro.com/trendlabs-security-intelligence/164-unique-android-adware-still-online/


## Author

**Bartlomiej Uscilowski**

Principle SQA Engineer


## About Symantec

Symantec protects the world's information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment—from the smallest mobile device to the enterprise data center to cloud-based systems.

Our industry-leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

Follow us on Twitter
@threatintel

Visit our Blog
http://www.symantec.com/connect/symantec-blogs/sr

For specific country offices and contact numbers, please visit our website.


Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527-8000
1 (800) 721-3934
www.symantec.com