2014

WEBROOT®

INTRODUCTION

The Webroot® Mobile Threat Report for January 2014 provides an overview of the risks and trends of the mobile space, based on research and analysis conducted by the Webroot Mobile Threat Research team. This report includes:

- Year-over-year comparisons, demonstrating the sharp rise in malicious attacks on mobile devices
- An examination of mobile application categories, organized by their likelihood of causing SMS infections
- Infection risk comparison between the iOS and Android platforms
- A detailed breakdown of Lost Device Protection services and their activation rates by Webroot users

Webroot believes that users and system administrations should be armed with the most up-to-date information on the risks and security issues currently facing the deployment and use of mobile devices. As employees continue to employ their own devices for work purposes, greater threats are introduced into the workplace leaving company data, and the networks these devices access, at risk. Users and system administrators must be educated on the threats currently facing their enterprises, and the security solutions that can be put into place to defend against them.

TESTING METHODOLOGY

The Webroot Threat Research team has analyzed more than 5.9 million mobile applications, hundreds-of-thousands of infections, nearly 125 thousand Lost Device Protection (LDP) activations, and infection rates from millions of customers between 2011 through 2013.

APP REPUTATION BY VOLUME AND DEVICE

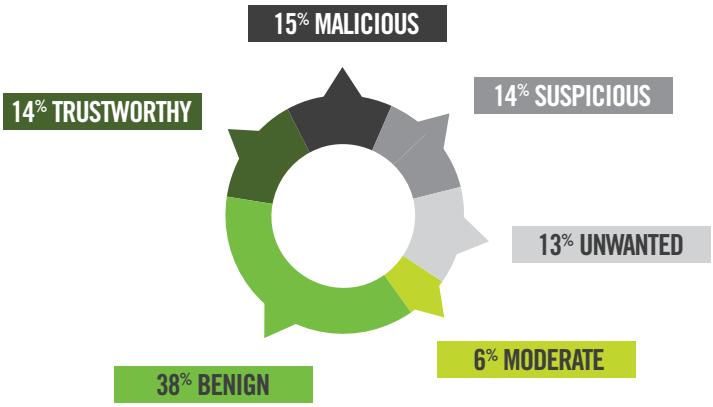
Detecting and removing malicious apps is essential to any mobile security solution; however, taking steps to understand the fine details and granular nature of these attacks is key to preventing future incursions. Most app reputation services take a standard good vs. bad, binary approach, which leave a majority of apps in a 'gray area.' Companies who allow their employee to download 'gray' apps may risk exposing their employees and networks to unwanted risk, such as accessing a phone's microphone, location data, camera, or other elements that may not be deemed malicious at first pass by other services.

The Webroot® Mobile App Reputation Service categorizes mobile apps into six risk-based groups; malicious, unwanted, suspicious, moderate, benign, and trustworthy. By understanding the associated risk of installing a new app, vendors who offer mobile device management and corporations who support BYOD can set user policies to stay secure, such as only allowing benign or trustworthy apps, or defining different levels of allowed risk based on groups or roles (e.g. stricter for finance executives vs. temporary interns using the network).

The following pie charts illustrate that the platform for Android™ may pose a greater security threat than the platform for iOS®. 42% of applications analyzed for Android between 2011 and 2013 were classified as either malicious, unwanted, or suspicious. Notably, applications were analyzed based on the likelihood of a threat being present.

CUMULATIVE BREAKDOWN OF ANDROID™ APPS

This chart represents an analysis of nearly 4 million applications for Android. Total threats to Android devices detected by Webroot rose 384% in comparison to 2012 data.



[1] Webroot treats updated apps the same way it treats new apps, as malicious code may be introduced later in the app development cycle. Overall 1,677,914 unique applications for Android and 843,735 unique applications for iOS were analyzed for this report.

The Webroot® Threat Research Team was able to break these threats down into separate threat categories. Over the course of 2013, the majority of potentially dangerous apps were primarily represented by:

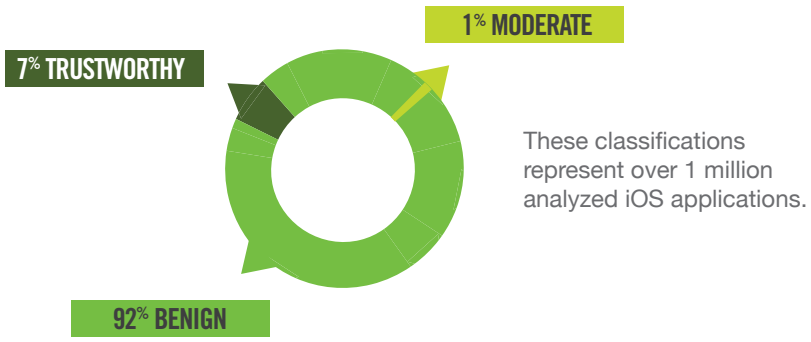
38.7% SMS Malware

39.8% Ad-SDK PUAs

8.9% Malware using obfuscation

SMS Malware is more common in regions which have fee-based SMS text services to participate in lotteries, purchase services, or perform some other activity by which sending a text message from your phone triggers a payment through your carrier. Through malicious apps, cybercriminals have figured out different ways to monetize their activities by making unsuspecting users' phones covertly send messaging to premium-rate SMS services. PUAs, or potentially unwanted applications, often contain aggressive advertising and/or try to access parts of your phone that users may not want them to, such as a flashlight app accessing the phone's contact list or camera. Malware using obfuscation is similar in that the malicious code is hidden so well in the app that it is difficult for the code to be caught without deep-level, advanced analysis, and could slip through basic security screenings.

By comparison, iOS® devices were primarily assigned the 'Benign' tag at a rate of 92%. (This is because iTunes® has historically put applications through a rigorous vetting methodology, whereas third party Android™ marketplaces, and to a certain extent Google Play have not.) The full breakdown can be found in the pie chart below. Although this breakdown indicates that suspicious, unwanted, and malicious applications were significantly rarer on the platform for iOS, the number of applications deemed entirely trustworthy was rated at 7%, exactly half the amount of the platform for Android. This is primarily due to ad-based apps which users have come to expect with low/no cost applications.



APP REPUTATION BY CATEGORY

Based on previous data reports, Webroot® estimates an average smartphone user downloads over 100 applications for a variety of different services. These apps can be carriers for malicious attacks, rendering users unknowing participants in their own vulnerabilities. Given the large percentage of SMS-related infections, Webroot tracks SMS infections by app category, giving their researchers complete insight into the most common source of infections – and the safest offerings. A recent analysis of more than 31,000 sample infections of Android™ devices revealed startling results.

Arcade and Action Games: 7,211 infections

Communication: 4,428 infections

Entertainment: 3,397 infections

Health and Fitness: 2,752 infections

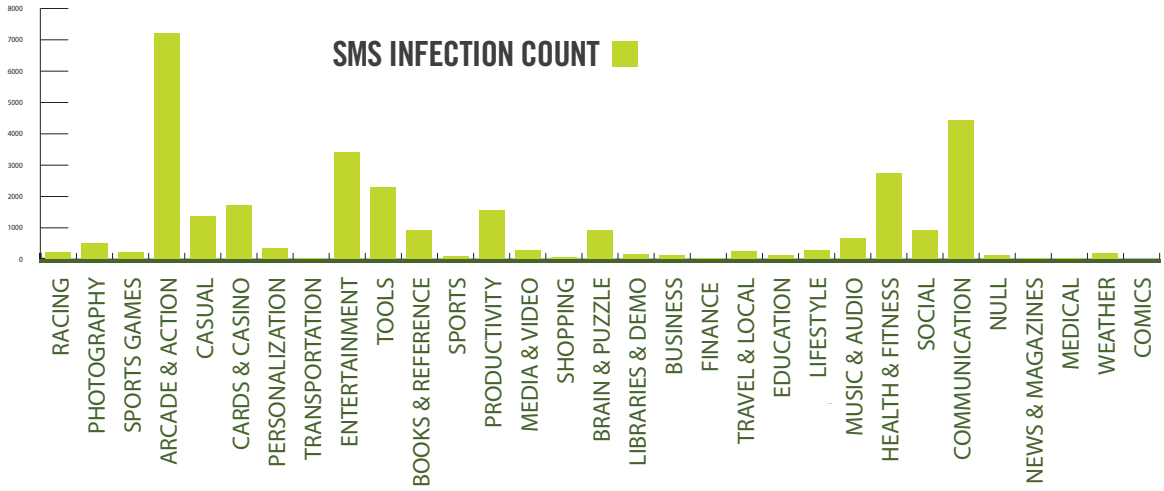
Music and Audio: 669 infections

News, Magazines, and Comics: 33 total infections

Shopping: 24 infections

Sports: 15 infections

The complete analyzed list is shown in the chart below.

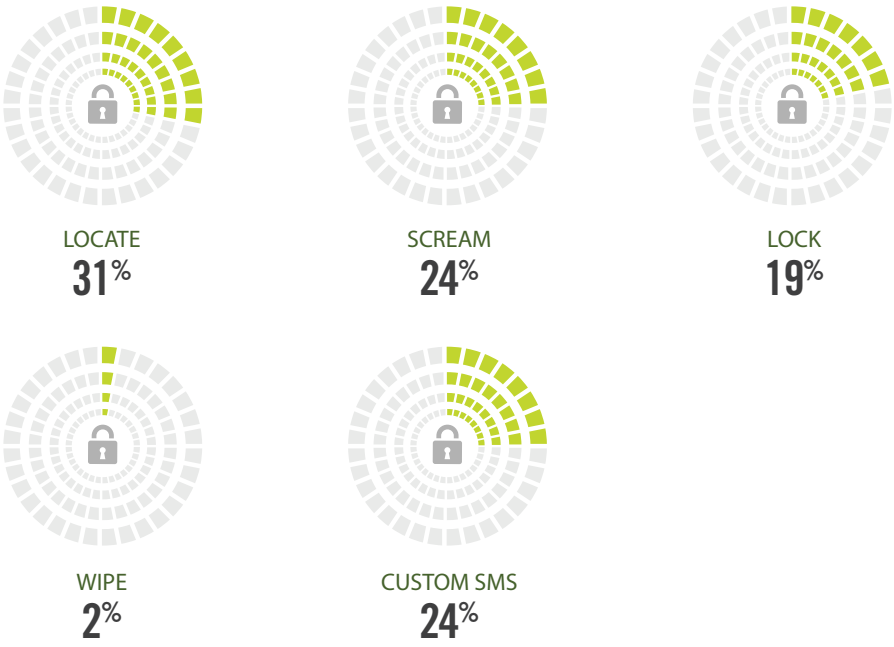


Gaming applications and entertainment updates are responsible for the highest rates of infection. Users who frequently employ gaming services on their work-related devices may wish to download instead a book, news app, or magazine; Webroot® data reveal that these apps were responsible for only 33 total infections (less than one percent of the total analysis), compared to the 29.3% represented by gaming applications. Although the data suggests that game related apps are the common source of mobile device infection, no category was entirely risk free.

DEVICE PROTECTION

The Webroot Lost Device Protection (LDP) services are a key component of its mobile security services. While data protection is a priority for any user, the same careful consideration must be given to devices themselves. Employing LDP can greatly reduce the impact of a misplaced or stolen device. Users are offered an array of options to resolve any misplaced (or potentially stolen) mobile devices, broken down into five separate functions: a GPS location service, a high-pitched 'scream,' remote lockdown of phone functionality, a complete wipe of all personal data, and finally an on-screen display of a custom message (often including 'return to user' language).

Knowing that each of these functions serves a unique purpose, the Webroot Threat Research Team examined data from August 2011 to November of 2013 to shed light on the most frequently employed service, and associated trends. The results are represented by the chart below.



Over the course of this study, the basic location service was employed the most frequently, representing 31% of all LDP services. Serving as a practical and unobtrusive method of determining if your device has been lost or stolen, the location function is often the first step taken by users.

The SMS message display represents 24% of total activity. Displaying a helpful message or phone number prominently onscreen allows anyone who stumbles upon a lost device to take action without requiring the type of research or outreach that might prevent its safe return. Activation of the 'scream' feature also makes up 24% of total LDP activity. Notably, the high-pitched scream feature, a function notable for both location assistance as well as stolen device scenarios, also locks the phone.

Subsequently, the 'lock' function could be construed as a more precautionary method: the mobile's location may be unknown, but the information is entirely safe while it is recovered or replaced. This option is employed less frequently than the 'scream' function, at a rate of only 19% of total LDP activations.

Analysis of nearly 125,000 actions by Webroot® users has resulted in a surprisingly well-distributed spread of activity. With the exception of the necessary, but sporadically used, complete wipe of personal data (2% of total actions), each of these tools was employed at least 19% of the time by users.

CONCLUSION

Mobile users must take additional precautionary steps to protect their data in order to keep up with evolving and opportunistic presence of hostile programs and hackers. New exploits, ransomware and app obfuscation techniques will continue to arise, yet many smartphone users are unaware of the steps they should take to protect the data on their personal devices.

Other methods and best practices to protect your mobile device include:

- Only installing applications from trusted sources such as Google Play and iTunes.
- Paying very close attention to permission requests from new app installations.
- Both corporate-owned and personal devices should use lock screens. 8 digit PINs are much better than swipe locks or 4 digit PINs.
- Using a mobile device security app to protect against malicious apps, web threats, and to deploy LDP services.

Further mobile security education will result in safer application usage, better security-related decisions, and ensure that the reliability and convenience of mobile devices is not compromised.

About Webroot

Webroot is bringing the power of software-as-a-service (SaaS) to Internet security with its suite of Webroot SecureAnywhere® offerings for consumers and businesses, as well as offering its security intelligence solutions to cybersecurity organizations, such as Palo Alto Networks, F5 Networks, Corero, Juniper, and others. Founded in 1997 and headquartered in Colorado, Webroot is the largest privately held security organization based in the United States – operating globally across North America, Europe and the Asia Pacific region. For more information on our products, services and security visit: www.webroot.com, the **Webroot Threat Blog:** http://blog.webroot.com or **Webroot on Twitter:** http://twitter.com/webroot.

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
+1 800 772 9383

Webroot EMEA
6th floor, Block A
1 George's Quay Plaza
George's Quay, Dublin 2, Ireland
+44 (0) 870 1417 070

Webroot APAC
Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australia
+61 (0) 2 8071 1900