WEBROOT®

The Wild, Wild West of Mobile Apps

How MDM vendors, carriers, service providers and app stores can protect users from malicious mobile apps

Contents

Brought to you compliments of
WEBROOT®

Business Opportunities Jeopardized by Security Issues

Mobile applications are providing exciting new business opportunities for service providers and technology companies. Innovative firms are thriving by offering apps in app stores and app markets, by supporting apps with mobile services and infrastructure, and by managing apps through mobile device management (MDM) and mobile application management (MAM) products. Enterprises are providing mobile apps to their employees and customers through corporate app catalogs.

But these business opportunities could be jeopardized by information security issues.

Attacks on mobile devices are growing at exponential rates. Security firms have estimated that:

- Mobile threats grew from 7,000 in 2010, to 25,000 in 2011, to more than 65,000 in 2012.
- The number of Android malware threats, including variants, could reach 1 million by the end of 2013.[1]
- The number of infected Android devices grew more than 200% in 2012, from 10.8 million at the beginning of the year to 32.8 million at the end of the year. [2]

[1] "Predictions for 2013 and Beyond," Trend Micro, Dec. 13, 2012.
[2] "2012 Security Report," NQ Mobile.

Service providers and technology companies that fail to address these trends risk losing customers. Firms that respond well have an opportunity to gain market share.

In this white paper, we will look at:

1. Why mobile attacks are exploding.
2. Options for protecting against malicious mobile apps.
3. The newest defense: mobile app reputation services.
4. The Webroot Mobile App Reputation Service.

Why Mobile Attacks Are Exploding

Why are mobile attacks exploding now, after remaining just over the horizon for several years? The reasons include increasing opportunities for mobile app-related attacks, the increasing sophistication and ingenuity of cybercriminals, and end-user ignorance of the risks.

A torrent of apps. A Nielsen survey showed that the average U.S. smartphone user installs 41 apps per year.[3] According to ABI Research estimates, 56 billion smartphone apps plus another 14 billion tablet apps will be downloaded worldwide in 2013.[4] These figures dwarf the equivalent statistics for conventional applications installed on PCs and laptops. Such high volumes provide plentiful opportunities for cybercriminals to find weak spots. They also make mobile device users less attentive to the security implications of each individual download.[5]

Proliferation of unpoliced app storefronts. Application storefronts managed by major vendors and service providers like Apple, Google, Microsoft, Samsung, Nokia, Cisco, Verizon and Vodafone tend to be well policed. However, there are now dozens of other large and highly visible Android and cross-platform storefronts, hundreds of smaller ones, and a vast number of websites offering mobile apps. Many of these have little or no ability to identify and block apps that contain malware. Dubious business people and cybercriminals have gone even further by setting up websites for the purpose of offering pirated apps and apps containing malware.[6]

Sophisticated and ingenious cybercriminals. Until recently, most malicious mobile apps were focused on adware and generating text messages and calls to high-cost services (toll fraud or premium number fraud). These attacks continue, but more dangerous campaigns are becoming more common. By the end of 2012, approximately one quarter of threats were "data stealers" designed to capture confidential data from devices — typically contact lists, text messages, passwords and authentication keys and location data.[7]

[3] "Nielsen: U.S. Consumers Avg App Downloads Up 28% To 41," *TechCrunch*, May 16, 2012.

[4] "Android Will Account for 58% of Smartphone App Downloads in 2013," ABI Research, March 4, 2013.

[5] "Chinese iOS pirate Kuaiyong launches web app store," *The Register*, April 17, 2013.

[6] "Fake apps and the lure of alternative sources," Microsoft, July 17, 2012.

[7] "TrendLabs 2012 Mobile Threat and Security Roundup: Repeating History," Trend Micro.

Hackers have learned how to counterfeit popular apps and to "repackage" them by adding malicious code to legitimate apps. Examples include fake versions of Pinterest, Skype, Angry Birds, Instagram and games like Plants vs. Zombies and Grand Theft Auto III. The fake and altered applications take actions like:

- Sending users to survey or games websites that generate unneeded or exorbitant charges.
- Downloading malware that takes control of SMS send-and-receive capabilities to send concealed messages and generate charges without the user being aware.
- Retrieving from devices information such as email addresses and phone numbers.[8]

Cybercriminals are also adapting phishing and social engineering techniques learned from PC-based attacks. Variants include "smishing" (SMS-based phishing attacks) and hidden or misleading URLs designed to take users to bogus banking websites in order to capture account numbers and passwords.

Examples of sophisticated, targeted advanced persistent threats are starting to appear in the mobile world. The University of Toronto documented one such targeted attack on a Tibetan human rights organization. The attackers used a repackaged version of Kakao Talk, a popular Android mobile messaging client, to change permissions on smartphones and extract contacts, call histories and SMS messages.[9] While this attack was aimed at a human rights group, it suggests mobile apps are likely to be employed soon in attacks targeting corporations and government agencies.

Finally, researchers have shown how compromised mobile devices can be used to spy on workplaces, by secretly snapping pictures, listening to conversations and capturing GPS data. Computer scientists at the Georgia Institute of Technology even demonstrated how a phone on a desk could use its accelerometer to detect vibrations from a nearby keyboard and capture words with up to 80% accuracy.[10]

Long-lasting vulnerabilities. With mobile apps, just like with PCs, vulnerabilities in installed software can give malware an avenue to take control of devices. Unfortunately, the infrastructure for patching software on mobile systems is not very well developed. For example, when Google finds a vulnerability in the Android operating system, each individual manufacturer has to create a patch for its own devices. It can take months before all smartphone manufacturers provide patches for their versions of Android.

Uninformed end users. Most people have been exposed to press coverage of phishing, malware and social engineering attacks against laptops and desktop PCs. However, far fewer users are aware that threats against mobile devices even exist. Most are also ignorant of how malicious apps manifest themselves on mobile devices — for example, through fast battery drain, slow performance and spikes in data usage.[11]

[8] "Pinterest Plagued by More Scams, Fake Android Apps," *PC Magazine*, April 30, 2012; "Children run up huge mobile bills on fake Angry Birds game," *MailOnline.com*, Jan. 15, 2013; "Fake game apps flood Google Play," *Help Net Security*, Jan. 21, 2013; "Fake apps and the lure of alternative sources," Microsoft, July 17, 2012.

[9] "Permission to Spy: An Analysis of Android Malware Targeting Tibetans," University of Toronto, The Citizen Lab, April 18, 2013.

[10] "Innovative Attacks Treat Mobile Phones as Sensors," *Dark Reading*, Oct. 27, 2011; "Mobile Trojans Can Give Attackers An Inside Look," *Dark Reading*, Oct. 8, 2012.

[11] "Five Signs Your Android Device Is Infected With Malware," *PC Magazine*, April 3, 2013.

Cavalier attitudes toward security. Individuals are accustomed to regarding smartphones and tablets as personal devices used for entertainment and personal communication, even when they contain business information. Therefore, many do not take the precautions understood to be appropriate for company PCs and laptops.

Options for Protecting Against Malicious Mobile Apps

Most service providers and enterprises have adopted some form of "defense in depth" against mobile malware. Technologies and practices commonly used include:

- **Mobile antivirus software** to detect malware in mobile apps.
- **MDM and MAM** solutions to help systems administrators monitor mobile devices, lock settings and wipe confidential data if devices are lost.
- **User education** to equip mobile device users with the knowledge to avoid suspicious mobile apps and to recognize and report symptoms of attacks.
- **Company policies** that prohibit employees from installing non-business applications on mobile devices that contain business information, and that mandate the use of approved app storefronts.
- **Corporate app catalogs** that give employees access to apps that have been tested and approved by the company.

However, these defenses are unlikely to prove sufficient. Mobile antivirus products do a good job of blocking known malware, but they can't recognize all variants of malicious and repackaged mobile apps. MDM and MAM products help keep devices patched so malicious apps have fewer vulnerabilities to exploit — but as noted earlier, often patches are not available for long periods. And unless an organization can lock down devices and completely control user behavior, some employees inevitably ignore security education, company policies and approved app catalogs.

The Newest Defense: Mobile App Reputation Services

Mobile app reputation services represent an innovative new approach for defending against malicious apps. They can be deployed by:

- App storefronts, telecom carriers, mobile service providers and mobile device manufacturers, to protect their customers.
- MDM, MAM and other security vendors, to improve the effectiveness of their offerings.
- Enterprises and government agencies, to improve the security of enterprise app catalogs.

Mobile app reputation services operate in four stages: *collection*, *analysis*, *classification* and *sharing* (see Figure 1 on the following page).

In the **collection** phase, the service gathers millions of apps from app storefronts and websites, as well as from customers, security information clearinghouses and other security vendors.

In the **analysis** phase, the apps are studied rigorously using a variety of techniques, including:

- Static analysis of the structure and content of the file.
- Runtime analysis of the behavior of the app, to detect potentially malicious actions.
- Market analysis, to detect similarities with malware previous identified by security vendors and enterprises.

In the **classification and scoring** phase, the data gathered in the analysis phase is compiled and weighted, and reputation scores are assigned to the apps.

In the **sharing** phase, the scores and fingerprints of the apps are shared with app storefronts, service providers, security vendors, enterprises and other subscribers of the service.

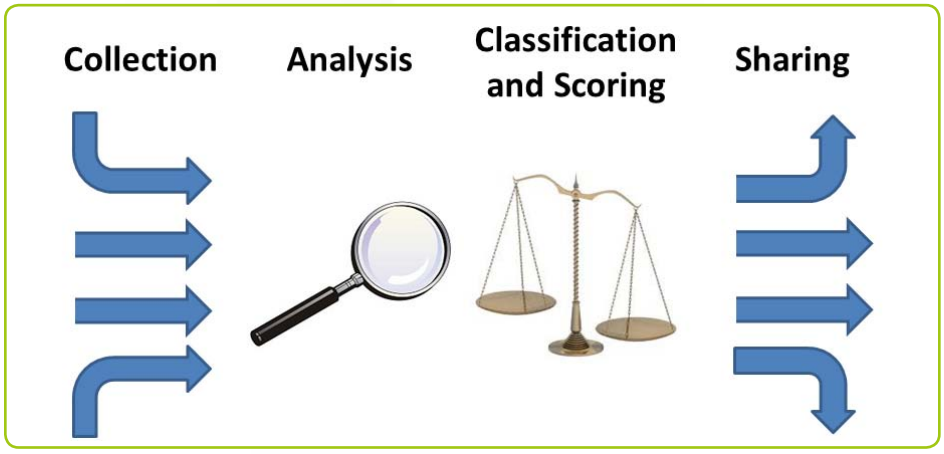

Figure 1: Mobile app reputation services operate in four phases.

The subscribing organizations use the scores and fingerprints to create blacklists and whitelists, or to enable graded responses (such as block, quarantine for review, warn and allow) based on levels of risk.

While mobile app reputation services are now available from several providers, they are not all equal. The effectiveness of each depends on factors such as:

- The breadth of the collection effort.
- The size of the threat database.
- The quality and extent of the analysis.
- The sophistication of the classification.
- The range of information provided, along with the overall reputation score.

We will now look at Webroot's Mobile App Reputation Service to see how it performs in these areas.

The Webroot Mobile App Reputation Service

The Webroot Mobile App Reputation Service is a sophisticated, flexible tool that gives app storefronts, telecom carriers, mobile service providers, MDM vendors, enterprises and others accurate, nuanced information on the risk associated with mobile applications in the wild.

Webroot's service was not created from scratch. Rather, it is built on the Webroot Intelligence Network (WIN), one of the largest and most comprehensive threat databases in the world, and on Webroot's highly sophisticated anti-malware analysis technology, which has been proven over many years in the PC and laptop anti-malware market.

Here we will look briefly at how the Webroot Mobile App Reputation Service operates in the four phases outlined above (see Figure 2).

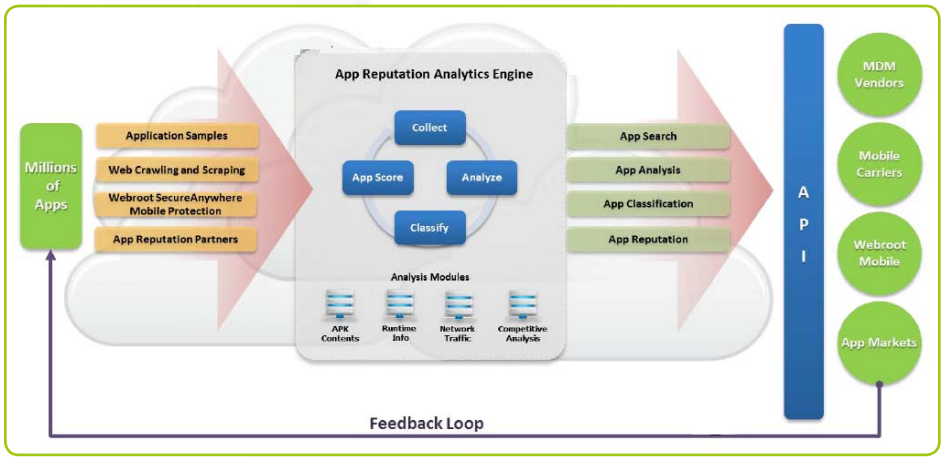

Figure 2: Overview of the Webroot Mobile App Reputation Service.

Collection

The Webroot Mobile App Reputation Service collects millions of mobile applications from a wide range of sources.

It downloads applications from major app marketplaces like Google Play as well as from many lesser-known app markets, and monitors these sites for new apps and new versions of known apps.

Webroot also uses Web crawling and scraping technologies to scan for user ratings and feedback on mobile apps, application categorization on app market websites, and data that reflects on the risk of mobile apps.

Webroot utilizes application information gathered from millions of customers — consumer and enterprise users of its endpoint and mobile protection services who opt in to provide security and application data. It also participates in file-sharing programs with other security vendors.

Mobile app data is stored in WIN, a cloud-based database with more than 100 terabytes of threat data.

Analysis

After the Webroot Mobile App Reputation Service collects data on a new application, it performs a detailed analysis of information, including:

- Details of the APK (application package file), such as its manifest, certificate and binary files.
- Heuristic and statistical analysis of the code to identify repackaged and recompiled versions of known malicious software.
- Suspicious behaviors captured by running the app in a secure sandbox, such as attempts to capture phone numbers and email addresses, changes in permissions, attempts to enable additional features, and modifications to browsers and bookmarks.
- Runtime attempts to contact known bad and questionable IP addresses and URLs (based on IP and URL reputation databases in WIN).
- Comparison of the app name and a fingerprint (an MD5 hash) with malware data provided by other security vendors.
- Correlation with feedback and application metadata gathered from app marketplaces and other websites.

The comprehensive analysis of 3.7 million Android and iOS apps to date has found that 12% were infected with malicious code — a confirmation that mobile threats have already reached a dangerous threshold.

Classification and Scoring

After the Webroot Mobile App Reputation Service completes the analysis phase, it uses a neural-network-based classifier to aggregate the analysis results into a combined reputation score.

The raw reputation scores are then grouped in classification bands:

- Malicious: Known malware, such as a Trojan or rootkit.
- Unwanted: Not known malware, but unwanted characteristics.
- Suspicious: No malware definitions triggered, but malicious or unwanted scores from some analysis module.
- Moderate: Seemingly benign, but contains dangerous permissions (e.g., SEND SMS).
- Benign: Non-whitelisted, but no dangerous permissions.
- Trustworthy: Whitelisted.

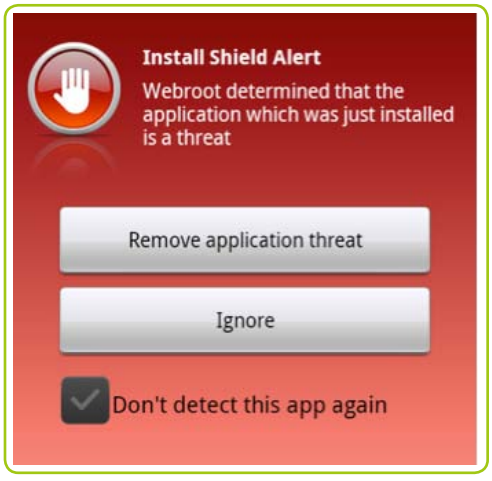

Figure 3: Subscribers can use reputation data to align responses with risks.

These classification bands make it easy for organizations subscribing to the service to create blacklists and whitelists, or to enable a spectrum of responses tuned to the app risk level — responses such as block, quarantine for review, warn the end user and await a response (Figure 3), and allow.

Sharing

The Webroot Mobile App Reputation Service shares risk classifications with subscribing organizations through a RESTful Web service application programming interface.

For each app, subscribers can access not only the simple classification band, but also more detailed information on the files, the manifest, the digital certificate, permission requests, phone feature requests, recent files added, Google Play information and market prevalence.

This detail gives subscribers the ability to modify risk rankings based on issues important to a given audience. For example, if a service provider is working with enterprises or government agencies where location information is confidential, it could bump up the risk classification of all apps that attempt to access GPS data on devices.

Business Value for Service Providers and Enterprises

As security becomes a major issue for mobile app users:

- Consumers will hold app market vendors and websites to high standards for screening and checking the apps they provide.
- Customers will expect carriers, mobile service providers and equipment manufacturers to build meaningful safeguards into their offerings.
- Enterprises will demand effective mobile security from MDM vendors and other security companies.
- Employees will count on enterprise IT departments to protect them from malicious mobile apps in the same way they are protected from conventional PC malware.

In this environment, mobile app reputation services will be a key tool to retain credibility to increase competitiveness.

The Webroot Mobile App Reputation Service is one of the most sophisticated and powerful mobile app reputation services on the market, deployed as a high-performance, reliable and secure cloud service, and backed by a vendor with an outstanding record of providing easy-to-use, industry-leading endpoint and mobile device protection.

For more information, please visit
www.webroot.com/En_US/business/security-solutions/mobile-app-reputation**.**

