Mobile App Reputation

A Webroot Security Intelligence Service

Timur Kovalev and Darren Niller
April 2013
Contents

Rise of the Malicious App Machine .......................................................... 3
Webroot App Reputation Service .............................................................. 3
Detailed Mobile Application Lifecycle and Webroot Analysis Methodology ............... 5
Summary ........................................................................................................ 9
About Webroot ............................................................................................ 9
The Rise of the Malicious App Machine

The exploding popularity of smartphones and tablets has created a major new threat vector — the mobile application. With the large volume of apps now available, hackers can easily disguise and distribute malicious code to unwitting victims. In fact, apps have become the primary vehicle to distribute mobile malware, and the exponential growth of apps is compounding the problem. As of September 2012, for example, mobile users had downloaded 25 billion apps from the Google Play Store.

Attacks by cybercriminals on mobile devices have become increasingly sophisticated. The behavior of these malicious applications ranges from stealing confidential data to performing remote control activities like sending spam or calling premium numbers for cash. Through social engineering tactics, they easily distribute Trojan, Spyware and Backdoor malware.

In particular, the openness of the Android platform makes it easy for hackers to create and distribute malware quickly, which explains why it has become the biggest target. In the first half of 2012 alone, Webroot Research has seen a 900% growth in Android malware samples, and this rapid growth shows no sign of slowing.

While mobile malware still represents only a fraction of the millions of threats targeting PCs, the number of new mobile threats has shown a more aggressive growth trajectory. Nonetheless, individuals and businesses remain largely unaware of the risks of applications. Most mobile malware is delivered via mobile apps cleverly disguised as “good” and distributed through mobile app markets. Unsuspecting individuals install these applications on their mobile devices without doing any research on the application or its developers, opening the door to an attack with precious data as the target. And with BYOD becoming a reality, this presents a security threat to individuals and businesses alike.

The large volumes of existing apps, a constant stream of new apps, and a growing number of third-party app distribution markets combine to present a significant security challenge. How do you determine which apps are malicious and which apps are safe? Vendors that provide mobile management and security solutions need to ensure their customers are protected from malicious applications, have the ability to filter out unwanted or non-compliant apps and allow access to reputable applications.

Webroot App Reputation Service

In response to the increasing threat presented by mobile applications, Webroot has developed the Webroot® App Reputation Service. Utilizing data collected and analyzed by the Webroot Intelligence Network (WIN), the App Reputation Service gives Webroot partners and customers the ability to manage the delivery of mobile applications that are safe and compliant.

How Webroot App Reputation Service Works

Figure 1 presents a process flow showing how the App Reputation Service collects, analyzes and distributes app data to partners and customers.

1. **Collection.** The App Reputation Service collects millions of applications from app markets, third-party sites, app sharing services, strategic partners, and Webroot SecureAnywhere™ Business – Mobile Protection users.
2. **Analysis.** After the applications are fed into the App Reputation Analytics Engine, an automated, multi-staged analysis process collects detailed data on each application.

3. **Classification and Scoring.** Each app is categorized and assigned a score based on algorithms using detailed analysis data. Compared to simply looking at the permissions that the apps request, this approach allows for granular detail on what the app actually does once installed, enabling Webroot to better determine if an app is trustworthy, neutral, malicious, or suspicious.

4. **Partner API.** The Classification and Scoring results allow Webroot partners to analyze apps or analyze app data via a web service API.

5. **Feedback Loop.** Information collected by Webroot partners is then gathered and looped back into the App Reputation analytics engine.

Using the data and analysis results provided by the Webroot App Reputation Service, MDM vendors, mobile carriers, app developers and application marketplaces can develop solutions that incorporate app reputation to ensure their customers are free from malicious or unwanted mobile apps.

**Webroot Intelligence Network**

The Webroot Intelligence Network (Figure 2) powers the Webroot Mobile App Reputation solution. WIN collects billions of pieces of information from multiple sources—including data from customers, test laboratories, and intelligence shared between partners and other security vendors—to create one of the world’s largest malware detection networks. At 75+ terabytes of threat data and growing every day, WIN is always up to date and ready to detect new malware threats. All Webroot security products—Endpoint, Mobile and Web—utilize this threat database.
The App Reputation Service utilizes other WIN databases such as URL and IP Reputation to analyze and classify applications.

**Figure 2: Webroot Intelligence Network**

**Detailed Mobile Application Lifecycle and Webroot Analysis Methodology**

**Collection**

**Application Samples**

Application samples provide the most thorough and reliable data for the App Reputation Service. Samples are harvested in a number of ways, including direct download from Google Play and other markets and monitoring app markets for new applications as well as new versions of known applications. Webroot also collaborates and participates in file sharing programs with other security vendors and receives daily feeds of suspicious and malicious applications. Webroot conducts proactive research for suspicious applications.

**Webroot SecureAnywhere Business – Mobile Protection Users**

In addition to actual application samples, Webroot leverages application information collected from SecureAnywhere Business – Mobile Protection users who opt-in to participate in providing security and application data. At present, over 200,000 users from more than 100 countries contribute to WIN.

Application information is collected directly from users’ endpoint devices, uploaded, and then processed by App Reputation Analytics Engine. The collected information drives sample
acquisition by establishing priority based on real-time market information pertaining to application popularity and prevalence in the market.

The provided signature is correlated with the application attributes, which are extracted from the manifest and digital certificate. This information is used to generate application classification and reputation even without the application sample being available.

*Web-Scraped Metadata*

Webroot employs web crawling and scraping technologies to collect additional information on applications when available. This information includes user ratings and feedback, application categorization in mobile markets, and other data points as available. The data are juxtaposed with other information available on a particular application in the system.

The samples collected have allowed us to analyze and classify over 1.8M apps to date, with over a million apps analyzed and classified over the last half of 2012 (Figure 3). Out of 1.8M apps analyzed, 12% were found to be infected with malicious code.

![Figure 3: Number of Mobile Apps Analyzed](image)

**Analysis**

Once information on a new application is in the Webroot database, automated modules process these data to extrapolate additional data points for that specific application. Application undergo a thorough analysis to extract information such as: applications contents, runtime information,
network traffic, source code, app market information, and data provided by SecureAnywhere Business – Mobile Protection users. (Figure 4)

![Diagram of Analysis and Classification Modules]

**Figure 4: Analysis and Classification Modules**

Samples of the detailed information include:

- **APK Contents** – Application archive is mined for manifest, digital certificate, and DEX (Dalvik Executable) binary data.
- **Runtime Information** – Applications are executed in a device simulator while capturing network traffic and device log information.
- **Network Traffic** – Captured network traffic is analyzed and cross-referenced against Webroot IP and URL reputation and classification services leveraging WIN.
- **Market Analysis Information** – All applications and application metadata are cross-referenced with other third-party virus comparison services.

All the collected information is filed and catalogued for future reference. Market statistics for a given app are calculated and recorded.

**Classification and Score**

Once the data collection modules complete their tasks, Webroot machine classifiers process the collected data and assign a reputation score to each application.

To classify an application, the App Reputation Engine analyzes the data using various classification modules including, Heuristic-based Analysis, Definitions-based Analysis, Statistical Classifiers, Active Learning, and Manual Classification. All applications start with a score of 100 (clean), which is subsequently adjusted based on presence of characteristics such as dangerous permissions, suspicious network traffic, source of application information, etc.

Webroot uses a proprietary, statistically backed variant analysis system to analyze the executable code of every application in the system. The system is very effective in detecting variants (re-packaged and re-compiled versions) of known malicious software. The Support Vector Machine technology generates a score with underlying statistical distribution that allows application classification. Every application that enters the system is scanned with the SecureAnywhere Business – Mobile Protection engine and is re-scanned whenever new rules become available.

A neural-network based classifier is used to aggregate the classification results of other analysis modules into a combined classification score. The score is subsequently used to generate a reputation for that specific application.
App Reputation Service API

Webroot has streamlined the analysis to provide a concise reputation band and other information on mobile apps in the database. The information collected is exposed via a RESTful web service API and can be used by MDM or other applications that enable mobile app usage policies. Webroot provides several application lookup mechanisms, including package name and md5. A simple banding classification provides an easy-to-implement solution for Webroot partners. This is the main advantage of the App Reputation Solution — either allowing or blocking the mobile apps based on the policy designed to safeguard the interest of business and its users.

App Reputation Band Classification

To simplify interpretation of the numeric reputation score, application reputation is placed in one of the following bands:

- **Malicious** – The application was detected as a non-PUA (Potentially Unwanted Application) threat (i.e., Trojan, Rootkit, etc.) by Webroot definitions. Figure 5 shows the distribution of Malicious Threats by type classified by the App Reputation Service

- **Unwanted** – The application was detected as a PUA by Webroot definitions. PUA is not malware but has unwanted characteristics. Some unwanted characteristics include aggressive ads and popups, intrusive privacy policies, marketing to contacts, etc.

- **Suspicious** – The application has not triggered any definitions, but Webroot machine classifiers scored the application in the malicious and unwanted range

- **Moderate** – Seemingly benign application that contains dangerous permissions (e.g., SEND SMS, CALL PHONE, etc.)

- **Benign** – Non-whitelisted application that contains no dangerous permissions

- **Trustworthy** – Whitelisted applications that is safe to use

Other information exposed via the APIs includes but is not limited to:

- Application reputation
- Blacklist
- Whitelist
- Basic file and package information
- Digital certificate information
- Manifest data
- Permission requests
- Requested phone features
- Runtime captures
- Source code files
- Top number of malicious applications
- Most recent files added
- Google Play information
- Market prevalence information

Developers using the API have flexibility to set permissions beyond the banding classification and use other data points exposed via the API to determine application policy compliance. For example, an app may be classified as moderate, yet it might have other undesirable characteristics such as GPS location or access to user’s phone contact list.
Summary

The Webroot App Reputation service allows MDM vendors, mobile carriers, and application distributors to deliver mobile applications safely to their customers. Built on the Webroot Intelligent Network, it harnesses data and inputs from millions of sources, making it one of the most powerful application reputation services on the market.

The App Reputation Service is simple and easy to integrate. It provides flexibility for MDM providers, mobile carriers and app market providers to decide how to use the mobile app information and adapt it for specific management requirements.

With millions of mobile applications available and new apps introduced everyday, Webroot partners will have the assurance that their customers are protected from the potential threats hidden in mobile applications and are using only safe apps.

About Webroot

Webroot is committed to taking the misery out of Internet security for businesses and consumers. Founded in 1997, privately held Webroot is headquartered in Colorado and employs approximately 350 people globally in operations across North America, Europe and the Asia Pacific region.

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, CO 80021
USA
800 870 8102

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

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