Webroot® Mobile Security SDK Financial Services

OVERVIEW

The wildfire growth of mobile apps has added to the security challenges of financial institutions that provide this in-demand method of account access. The risks are substantial, but there is a way to reduce exposure while enhancing customer convenience.

The Risks

- From January 2012 to June 2015, malicious Android apps have increased over 800%.
- As of March 2015, 39 percent of all mobile phone users accessed mobile banking within the past 12 months.*
- The most common uses of mobile banking are checking account balances (94 percent); transferring money between accounts (61 percent); depositing checks (51 percent).*
- Juniper Research predicts that mobile banking users will exceed one billion in 2017, about 15 percent of all mobile users.

Individuals using smartphones and tablets tend to engage in activities that increase the risk of attacks, e.g., using social media sites to a greater degree or visiting websites that may increase vulnerabilities, such as gambling or adult entertainment sites. Mobile devices are also vulnerable to physical loss or theft, which means a person other than the account holder might gain access to account information.

*Consumers and Mobile Financial Services 2015, Board of Governors of the Federal Reserve System

The Webroot® Mobile Security SDK addresses mobile device vulnerabilities by enabling financial institutions to offer enhanced security to their customers. It features antivirus, antimalware, device and application interrogation, as well as an overall device score to easily determine the risk level.

FINANCIAL INSTITUTIONS BENEFIT

The Webroot Mobile Security SDK protects the mobile channel by performing a risk assessment of the mobile device, user and banking app. It enables organizations to manage risk by delivering data to the bank's risk engine. The score generated determines whether to allow, restrict or deny user access. The benefit: reduced risk to the device and user enabled by real-time, actionable security intelligence.

- **Increased customer convenience**
  Provide industry-leading protection against mobile threats
- **No impact on user experience**
  Powerful protection with a lightweight footprint and minimal battery drain to satisfy customers
- **Leverages Webroot BrightCloud® Threat Intelligence**
  Harnesses intelligence from millions of sources via the world's most powerful cloud security network
- **Easy integration, giving you full control**
  Simple, UI-less integration puts the financial institution's brand at the forefront of the user experience

Mobile Security SDK Benefits

- Industry-leading mobile threat protection
- Operates silently in the background and will not impact user device
- Provides real-time device health check
- Reports device and threat information directly to bank for instant analysis, interrogation and action

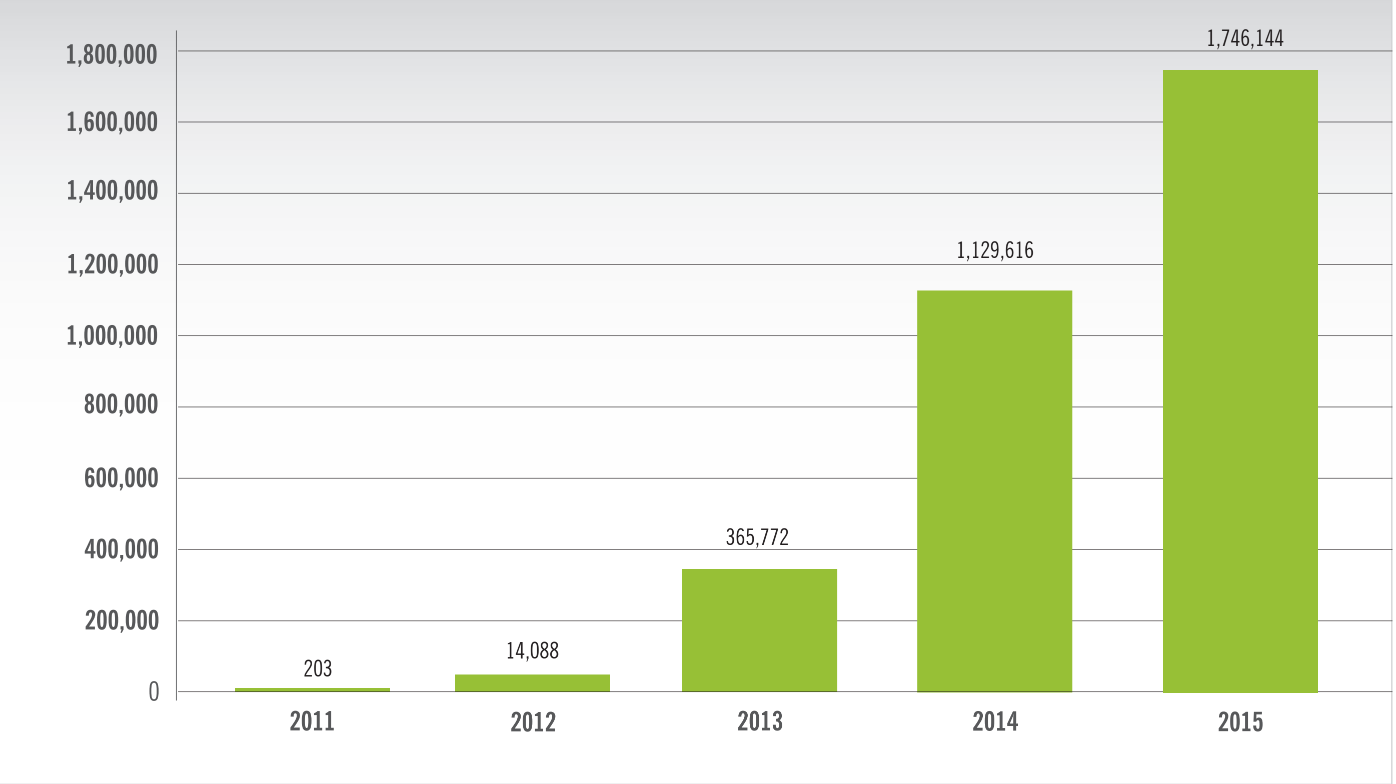


Figure 1 » Malicious Android Apps - June 2011-March 2015

WEBROOT® MOBILE SECURITY SDK IN ACTION

The Webroot® Mobile Security SDK features several modules. Financial institutions can select:

- **Monitor Service** – Background service to monitor real-time events (file downloads, package installations, application launches, etc.)
- **Scanner Service** – APIs for scanning applications (running apps, installed apps) and files
- **Application Information** – APIs for extracting all types of application information
- **Device Information** – APIs for extracting all types of device information and device snapshots
- **Device Risk Score** – The device scoring system takes into account multiple risk factors to ensure the end user information is safe and secure

All of these services may be utilized with the flexibility to leverage any permutation based on unique needs. This flexibility allows financial institutions to leverage the SDK to protect customers' mobile transactions by ensuring that devices connecting to the financial institution's applications are within acceptable risk levels.

Monitor Service

This service keeps track of device events. The service can be left running at all times or enabled while the host application is running and disabled when the host application is done. The host application has full control of the monitoring service, i.e., the service can be enabled for the duration of connection to a remote server and then terminated by the host application.

The Monitor Service can be also used to notify the host application of any files being downloaded, any applications being installed, and any applications being executed. The host application can log these events, show notifications, and take any other custom actions based on these events.

Scanner Service

This service allows the host application to run system-wide antivirus/antimalware scans of files and apps. Scans can be run silently in the background or the host application can set up scanner listeners to provide feedback to the user. Scan results are stored in a single persistent list, which can be used by the host application to interactively quarantine or remove individual files and applications.

Application Info Module

This module provides detailed information about apps installed and running on the device. The interrogated apps' data points are configurable by the host application. Some examples are different package attributes, certificate and manifest information, and various network and process related data points.

Device Info Module

This module provides detailed information about the device and operating system. The Mobile Security SDK can check whether the device is in a rooted state or is running in an emulator. It also gathers various hardware statistics and can uniquely identify the device.

Device Risk Score

This feature provides a flexible yet very powerful risk scoring mechanism to simplify the decision making process when assessing risks on a mobile device. When calculating a device score, the user, the device, and the financial institution's app are all taken into account. The system covers an endpoint and makes a simple go/no-go decision based on risk criteria, such as whether the device is rooted or jailbroken, contains high risk malware, or uses the latest definitions. The Webroot Mobile Security SDK provides the flexibility of risk scoring parameters being set by the financial institution.

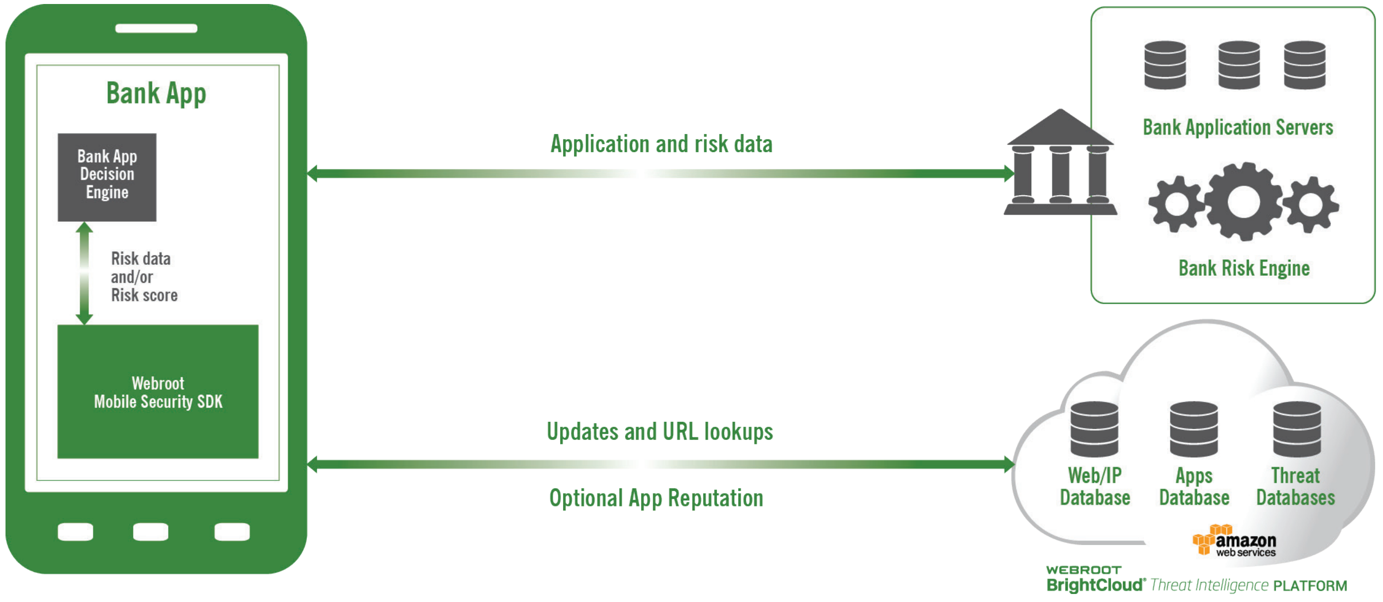
The ability to apply individual weights to malware categories allows the financial institution to add a device rooting score to other factors to balance device risk with legitimate customer access demands. Risk scoring can be as simple as a traffic light system or more complex with individual weights applied to each feature, allowing granular control over the scoring mechanism. Weights and scores can be adjusted based on risk tolerance at the financial institution's discretion.

PARTNER INTEGRATION OPTIONS

Webroot provides all the tools necessary for financial institutions to complete a simple SDK implementation into a bank's mobile banking application. Financial institutions have full control of the UI and all customer communications. The Mobile Security SDK library is modular in design, which allows for a very small memory footprint. Depending on the chosen configuration, only the necessary modules are loaded into memory.

The SDK solution consists of a Java Library, sample app, and documentation. The compiled Java Library (JAR) is embedded in the financial institution's app. The sample app enables a financial institution to view how integration of the library might be completed. Documentation includes details all of the classes and interfaces in the library that enable management.

Figure 2 » Mobile Security SDK



APIs allow for full management of all of the SDK security functions. For example, the financial institution can configure:

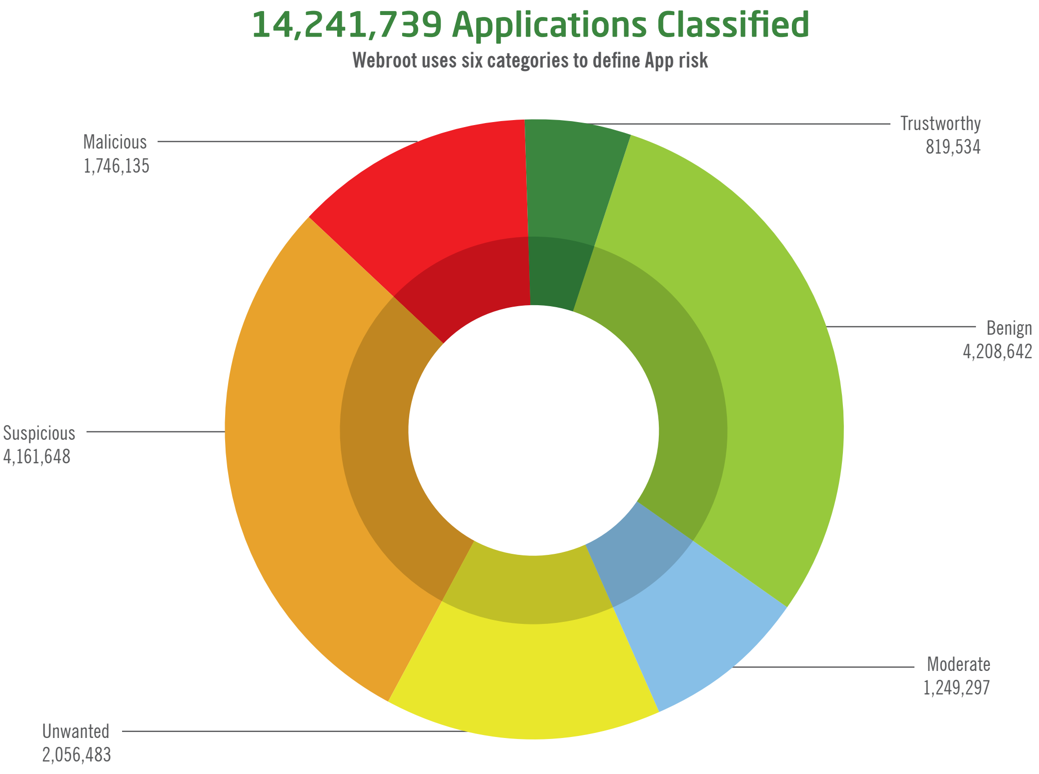
- Scan settings
- Definition update frequency
- Real-time protection settings
- Quarantine

Once deployed, security definitions are hosted by the Webroot BrightCloud® Threat Intelligence Platform. Definition updates and web lookups are queried against the Webroot servers (Figure 2).

THE COMPLETE MOBILE SECURITY SOLUTION

A major advantage of using the Webroot® Mobile Security SDK is that we are constantly monitoring, adding, and refining our security intelligence to thwart malware. As of March 2015, we have over 14 million mobile apps under research. The Webroot Mobile Threat team find that only 35 percent of all apps are truly trustworthy or benign. As the use of mobile devices increases so will the use of apps as the delivery method of choice for malware. The Webroot Mobile Security SDK ensures financial institutions are always basing their risk decisions on the most up-to-date app security intelligence.

Figure 3 » Applications Classified by Webroot - March 2015



About Webroot

Webroot provides Smarter Cybersecurity™ solutions. We provide intelligent endpoint protection and threat intelligence services to secure the Internet of Everything. By leveraging our cloud-based collective threat intelligence platform, computers, tablets, smartphones, and more are protected from malware and other cyberattacks. Our award-winning SecureAnywhere™ intelligent endpoint protection and BrightCloud® threat intelligence services protect tens of millions of consumer, business, and enterprise devices. Webroot technology is trusted and integrated into market-leading companies including Cisco, F5 Networks, HP, Microsoft, Palo Alto Networks, RSA, Aruba and many more. Webroot is headquartered in Colorado and operates globally across North America, Europe, and the Asia Pacific region. Discover Smarter Cybersecurity solutions at webroot.com.

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

DS _ 102015 _ US