WEBROOT
Smarter Cybersecurity

BrightCloud®
Mobile Security SDK

Simple, flexible, powerful detection and protection for Android® devices

Overview

» In 2018, on average 2% of Android apps analyzed by Webroot were malicious or potentially unwanted apps (PUAs)

» Malicious apps and PUAs are a threat to personal and corporate data, and can compromise financial transactions

» The BrightCloud® Mobile Security SDK offers enhanced mobile security, including antivirus, antimalware, application scanning and interrogation, device root detection, and device risk scoring

Individuals using smartphones and tablets tend to engage in activities that increase the risk of attacks on themselves and networks. For instance, using unsecured public WiFi or downloading apps from untrustworthy third-party sites can infect a device with mobile malware. These could lead to unwanted consequences, including data exfiltration, camera and microphone hijacking, financial extortion, or acting as a Trojan horse into the WiFi network it connects to.

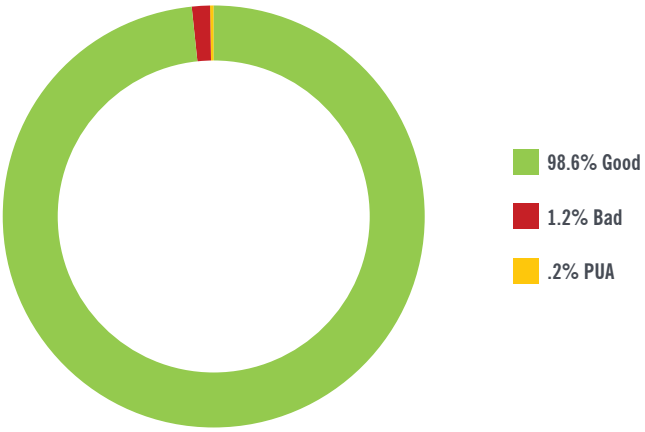

Figure 1: Distribution of Android™ app reputations in 2018

Webroot detects a variety of malicious apps, including malware, spyware, and trojans. PUAs include commercial rooting tools, hacking tools, aggressive advertising, and data leakage apps. Security administrators may consider eliminating PUAs, as they have the potential to impact data loss or incur unwanted mobile usage fees.

The BrightCloud Mobile Security SDK addresses mobile device threats by enabling technology partners to offer enhanced mobile security for their customers within their solutions. It features antivirus, antimalware, application scanning and interrogation, device root detection, and device risk scoring, all while utilizing very little memory, bandwidth, or battery life. As a fully functional mobile security solution, it offers significantly better protection than a simple, static blacklist approach and is designed to stay ahead of today's mobile threats.

Partner Benefits

» **Differentiate yourself from your competition**
Offer your customers industry-leading detection and protection against mobile threats

» **Leverage Webroot BrightCloud Threat Intelligence**
Harness collective threat intelligence from millions of sources via the world's most powerful cloud-based security network

» **Easy integration gives you full control**
Simple, UI-less integration puts your brand at the forefront of the user experience

» **No impact on user experience**
Powerful protection with a tiny footprint and minimal battery drain to satisfy your customers

Mobile Security SDK Benefits:

① Industry-leading mobile threat protection

② Does not slow devices or hinder user productivity

③ Simple, flexible development options for partners

BrightCloud® Mobile Security SDK in Action

The BrightCloud® Mobile Security SDK enables our technology partners to monitor Android devices, check for malicious apps, act on threats, and check overall device status.

Device Scanning

The SDK scans the device to detect threats when either initiated by the user or triggered by events occurring on the device. Additionally, the SDK proactively scans at set intervals to ensure changes do not go unnoticed. This multi-pronged approach offers optimal protection for the user from viruses and malware, while not impacting their experience using the device. Results can be integrated into the host application for visibility of overall protection status, and extended detection details can be requested for suggested remediation actions.

Root Detection

Rooted devices can try to bypass security and may be more vulnerable to malicious apps. The SDK uses a multitude of detections to determine the status of the device, and checks for root management applications, potentially dangerous applications, and root cloaking applications.

Device Risk Score

The service provides a simple, flexible, and powerful risk scoring mechanism to ensure Webroot partners and end users are secure. When calculating a device score that partners can use to make a simple go/no-go decision, various attributes including whether the device is rooted, contains high-risk malware, and other criteria are taken into consideration.

Runtime Permissions

When using the mobile SDK in Android OS API level 23 (Marshmallow) or higher, runtime permissions must be accepted by a user. With this feature, partners can retrieve a list of required permissions and present any permissions that have not yet been accepted by the user.

Partners have access to all of these features, with the flexibility to adjust their configuration based on their unique needs. This flexibility allows partners to leverage the SDK in various scenarios, such as:

» Mobile device management providers can bolster their customers' mobile security through enhanced protection

» Smartphone manufacturers, mobile network operators, and communications service providers can differentiate through pre-loaded security for their users, featuring their own brand

» Financial institutions and anti-fraud providers can protect their customers' mobile transactions by ensuring that devices transacting with their systems are within acceptable risk levels

Partner Integration Options

Webroot follows established Android app development standards to help make SDK implementation simple in partners' solutions. Webroot partners are responsible for developing all UI components (both client and management interface) using the SDK and leveraging only the functionality needed for their use case.

The SDK solution consists of access to an online Gradle repository and actively maintained documentation that includes details all of the classes and interfaces in the library. In addition to Android-native integration into the apps, developers can quickly access the latest changes and choose whether to accept cutting-edge features or stay with well-established components. Webroot follows a lifecycle model in alignment with Google to ensure actively supported Android OS versions remain compatible as Android continues to tighten compliance and security requirements.

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

» Scan settings

» Real-time protection settings

» Quarantine

In 2018, Android users who enabled installations from "Unknown Sources" were over 8 times more likely to have an infected phone versus those who only used the Google Play Store.[1]

About Webroot

Webroot was the first to harness the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide the number one security solution for managed service providers and small businesses, who rely on Webroot for endpoint protection, network protection, and security awareness training. Webroot BrightCloud® Threat Intelligence Services are used by market leading companies like Cisco, F5 Networks, Citrix, Aruba, Palo Alto Networks, A10 Networks, and more. Leveraging the power of machine learning to protect millions of businesses and individuals, Webroot secures the connected world. Headquartered in Colorado, Webroot operates globally across North America, Europe, and Asia. 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

[1] 2019 Webroot Annual Threat Report