DATASHEET

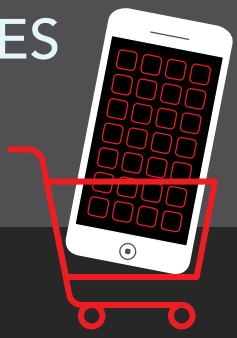
EXTERNAL THREATS—MOBILE

Detect and Respond to Mobile App Threats

RISKIQ®

THERE ARE MORE THAN 150 MOBILE APP STORES WITH MORE THAN 2.5 MILLION MOBILE APPS IN EACH

Monitor mobile apps to protect your customers and brand



MOBILE APP THREATS CAN IMPACT ALL DIGITAL ORGANIZATIONS

Many organizations with a digital presence have one or many mobile apps to help customers and employees interact with your organization on a day to day basis. Even organizations without an online presence or mobile app can unwittingly have their brand appear in app stores around the world.

Hackers increasingly use mobile as a new attack vector, leveraging gaps in organizations' visibility of their mobile assets to attack their brand and customers via expired versions of apps, third-party modifications of legitimate apps, and rogue or unsanctioned apps. These threat actors use trusted brands with a high-profile public presence or association with valuable data as lures to deceive end-users and steal sensitive information.

MOBILE THREATS TAKE MANY FORMS

RiskIQ's advanced mobile reconnaissance, inspection, and analytics technologies offer unique coverage and detection capabilities to actively identify and track legitimate and unauthorized applications across mobile platforms and sources. RiskIQ dynamically monitors the mobile app ecosystem to detect:

Credential Harvesting

Apps that target an organization's customers by stealing login credentials to take over accounts. These apps are a new form of phishing, which impersonates targeted brands with fake, look-alike applications. Organizations are now forced to address resulting fraud costs and loss of customer trust.

Malware

Malicious apps use brand affiliation to covertly install malware disguised as legitimate applications on users' devices. These apps flood users with unwanted ads, broadcast sensitive data to third parties, lock devices until a ransom is paid, inflate users' phone bills with premium SMS charges, and other malicious activities.

Download Diversion

Lost downloads translate to lost revenue for paid apps and apps with in-app purchases or ads. Other parties may offer free or cracked versions without the original authors' knowledge or consent.

User Experience Damage

Poor-quality apps created by fans and other third parties damage brand perception and interfere with the organization's engagement with customers. This leads to user dissatisfaction and confusion, even if the apps are not malicious or don't involve sensitive data.

Non-Compliant Official Apps

Expired and modified app versions may contain security flaws or performance issues that expose customers to risk. Apps that are not updated or removed from third-party app stores when a newer version is released and apps that are modified for compatibility with jailbroken or rooted devices also pose security risks.

RISKIQ PROVIDES COMPREHENSIVE MANAGEMENT OF MOBILE APPS

RiskIQ Mobile Threats provides discovery across all major app stores as well as more than 150 less common stores, including focused coverage of high-risk stores and regions for brand impersonation, malware, and fraud. In addition to unparalleled coverage of third-party app stores worldwide, RiskIQ incorporates a unique source of "feral app" binaries, or mobile apps collected outside of dedicated mobile app stores. With this comprehensive mobile presence knowledge, organizations have the unparalleled ability to:

- Monitor Google Play, Apple App Store, and more than 150 other app stores around the world to uncover official, unknown, or rogue mobile apps
- Intelligently sort legitimate apps from modified versions, unauthorized fakes, and lookalikes
- Go beyond just the title and description, automatically analyzing all app content and code to discover logos, brand references, and malicious code hidden in-app files
- Track app versions and correlate apps across stores for efficient management and enforcement of related incidents

ADVANCED MOBILE THREAT DETECTION TECHNOLOGY

Native-level integrations with each app store's particular layout and download procedures allow RiskIQ to gather the full set of app metadata and download mobile binaries for analysis automatically. Access to the binary enables RiskIQ to offer superior detection capabilities when compared to other solutions that use simple scraping and generic keyword searches for detection. Advantages include:

- Ability to automatically track app versions
- Identification of brand references and policy violations inside the application code
- Logo and image detection inside the mobile application code
- App permissions analysis
- Automatic sorting of legitimate apps, brand abuse, and fraudulent/malicious applications
- Granular policy controls based on specific app fields and contents
- Ability to correlate apps across all stores, based on md5 hash, title, developer, malicious code contained, or other shared attributes for efficient management and enforcement of related apps

EASILY MITIGATE MOBILE THREATS

RiskIQ provides an easy-to-access online dashboard for security teams to investigate mobile threats and determine the appropriate response. With full details in a quick snapshot, RiskIQ enables rapid app assessment with integrated language translation for international apps or app stores. It also offers the option to view and search all app code and files for in-depth analysis.

RiskIQ enables customers to quickly respond to actionable alerts and minimize organizational and customer impact by providing in-app workflows to contact apps stores and developers for app removal or app metadata updates.

Continuous monitoring lets customers know about successful threat remediation, and RiskIQ's post-resolution monitoring re-opens events and informs customers of any threats posing recurring risks to their organization.

MOBILE APP TELEMETRY

For advanced mobile app investigations, RiskIQ can provide mobile app install telemetry data, including install statistics and details about devices running fake, modified, or malicious mobile applications. Using information from over 300 million mobile devices, RiskIQ can extract data about the distribution and presence of rogue apps on end-users' devices and provide access to this data via JSON files.

REPORT ON MOBILE THREAT POSTURE

RiskIQ provides an intuitive dashboard and reporting options for monitoring and investigating mobile app threats and enforcement, which includes:

- Executive summary reports and a snapshot of the current state of an organization's global mobile presence
- Trends and benchmarks of mobile security improvements over time
- Custom reports and data drill-down include:
    - Policy violation type
    - Event generation time period
    - Current review status and change history
    - Event uptime until resolution
    - Event source and app store
    - Brands associated with events
    - Geographic distribution of apps