The Risks and Rewards of Mobile Banking Apps

The market demand for mobile banking technology and its rapidly increasing adoption rate means that many banks have been managing the security risk of mobile apps almost entirely on their own. The reward for success is improved customer convenience and retention and substantial operational cost savings.

This paper looks at the risk to reward ratio as it exists today and how new security technology from Webroot can help financial institutions become more adept and efficient at managing their app risk to reward calculations.

MOBILE APP USE INCREASES

The wildfire growth of mobile apps has added to financial institutions security challenges. ABI Research estimates that over 56 billion smartphone apps, plus another 14 billion tablet apps, were downloaded worldwide in 2013.[1]

During 2014, the Webroot Mobile Threat Research team has seen an exponential increase in Android-based malware to over 3 million malicious or potential unwanted applications (PUAs). Meanwhile, the percentage of apps that are trustworthy or benign has dropped from 45 to 39% in the same timeframe.

Such high volumes of app creation and downloads provide numerous opportunities for cybercriminals to find weak spots and infect customer devices.

WHY ARE MOBILE DEVICES A GREATER SECURITY RISK THAN OTHER PLATFORMS?

Mobile devices present a far greater security risk when compared to a laptop or desktop for a variety of factors, such as:

- Less user authentication, QR Codes, data sharing, SMS, NFC, etc
- More focus on user convenience over user security
- Easier access to data on compromised mobile devices than computers
- Higher risk of identity theft due to ease of account and document access via email or cloud storage, etc
- Unsafe data transmission over wireless connections, often unsecured public Wi-Fi
- Unsafe data storage as mobile apps often save sensitive data, such as banking PINs, card numbers, and passwords
- Sensitive data leakage due to poor app coding or authentication, exposing sensitive data to third parties

WHAT TYPES OF THREATS TARGET MOBILE BANKING USERS SPECIFICALLY?

While the general security risk is getting much higher, particularly for Android device users, there are many mobile device attacks that present severe risks for financial institutions. Recent examples include:

Trojans

- **Zitmo** – steals mTAN codes sent by banks in text messages
- **Banker** – steals passwords and other sensitive information
- **Perkel/Hesperbot** – uses JS injection on PC to request mobile number, delivers Trojan via SMS, Trojan poses as a security app
- **Wrob** – poses as the Google Play app and replaces installed banking apps with Trojan clones
- **Bankum** – replaces legitimate versions of banking apps with fake ones
- **ZertSecurity** – impersonates bank login, steals credentials

Rootkits

- **DroidDream** – uses rageagainstthecage exploit to root the device, steal data, install additional apps, execute remote commands

Spyware

- **Keyloggers** – pose as third party keyboards that send keystroke and contextual information

Users of Mobile Apps Worldwide by Region 2012-2017

	2012	2013	2017
App Users Worldwide	1.2 billion	N/A	4.4 billion
Asia Pacific	30%	32%	47%
Europe	29%	28%	21%
North America	18%	17%	10%
Middle East & Africa	14%	13%	12%
Latin America	9%	10%	10%
App Revenues	$12 billion	$20.4 billion	$63.5 billion

Users Set to Grow to 4.4BN by 2017

Source: Portio Research (March 2013) via: mobiThinking

---

[1] The Wild, Wild West of Mobile Apps, TechTarget, 2013

Other Trends Relating to Banking

» **Data Mining and Theft**

- Mobile devices contain increasing amounts of data and means to access data about individuals
- Criminals understand big data and can leverage analysis for targeted attacks

» **SIM Swap Fraud and Device Impersonation**

- Targets vulnerabilities in carrier infrastructure
- Requires off-device risk-assessment techniques

» **Spear Phishing and Social Engineering**

- Occurs via email, SMS, Twitter and other social networking, blogs, and news feeds
- Commercial phishing kits, such as Rock Phish, make it easy for even the inexperienced to launch a relatively sophisticated attack
- Modern phishing site lifespan is measured in hours, rendering even regularly updated blacklists virtually ineffective

THE APP DELIVERY CHANNEL

App-based mobile banking is now the fastest growing delivery channel.[2] Growth is driven by several factors, including customer convenience and operational cost savings for the financial institution. The cost of processing a transaction via mobile phone can be as much as 10 times lower than via ATM, and as much as 50 times lower than via physical branch.[3] Mobile deposits are especially cost-effective. JP Morgan Chase & Co. recently said mobile check deposits cost the bank three cents per transaction, versus 65 cents for deposits made with a teller.[4]

The financial rewards and customer convenience are substantial, but the potential that mobile banking customers might access a banking network with a rooted device is one of many risks. As with PCs, vulnerabilities in software installed on mobile devices can give malware an avenue to take control. 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 devices. It can take months before all smartphone manufacturers provide patches for their Android versions.

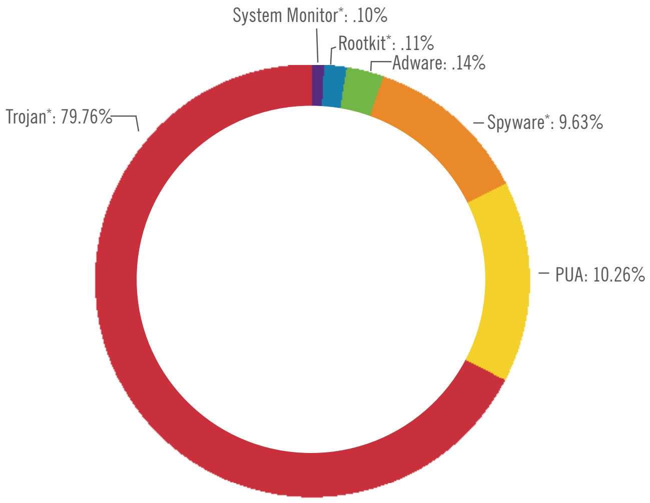
Financial institutions can leave device security management in the hands of their account holders and hope for the best or evaluate the security of the devices that access their banking systems. Device level security management does not require intrusion into account holders' personal information. Instead, it provides a health check of the device to determine the risk of malware and fraudulent activity. Fortunately, risk scoring for mobile devices assists when making an informed security decision without slowing the device or hindering productivity.

WEBROOT MOBILE RISK SCORING CATEGORIES:

The list below includes the primary criteria a financial organization can use to determine the risk each individual mobile banking user may present.

2014 Mobile Malware Status

Detected Malware Categories (Android)



*Categories focused on banking customers

Webroot Mobile Threat Research data, January 2015

Malware Detection Criteria

» Trojan

» System monitor

» Worm

» Rootkit

» Spyware

» Keylogger

» Adware

» PUA

Device State Criteria

» Device Rooted

» Up-to-date Webroot configuration

» Host application in debug-able state

» Host application is run in an emulator

» Allow side-loading/unknown sources option detected

» USB debugging option detected

» Up-to-date OS version

---

[2] FDIC Supervisory Insight, Winter 2011

[3] Tower Group – from Deloitte report: Mobile Banking: A Catalyst for Improving Banking Performance

[4] Wall Street Journal – April 9, 2014

THE ADVANTAGES OF SELF-DEFINED RISK SCORING

Self-defined risk scoring allows banks to address geo-specific circumstances and score based on the unique profiles of individual account holders. For example, rooted devices are common in Asia. In some geographies a rooted device may present an immediate red flag, blocking the device from account access. But in Asia, such a policy decision could cause customer service and retention issues. The ability to apply customized weights to malware detection categories and device state criteria allows the bank to alter a device rooting score above or below 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 on each feature allowing granular control over the scoring mechanism.

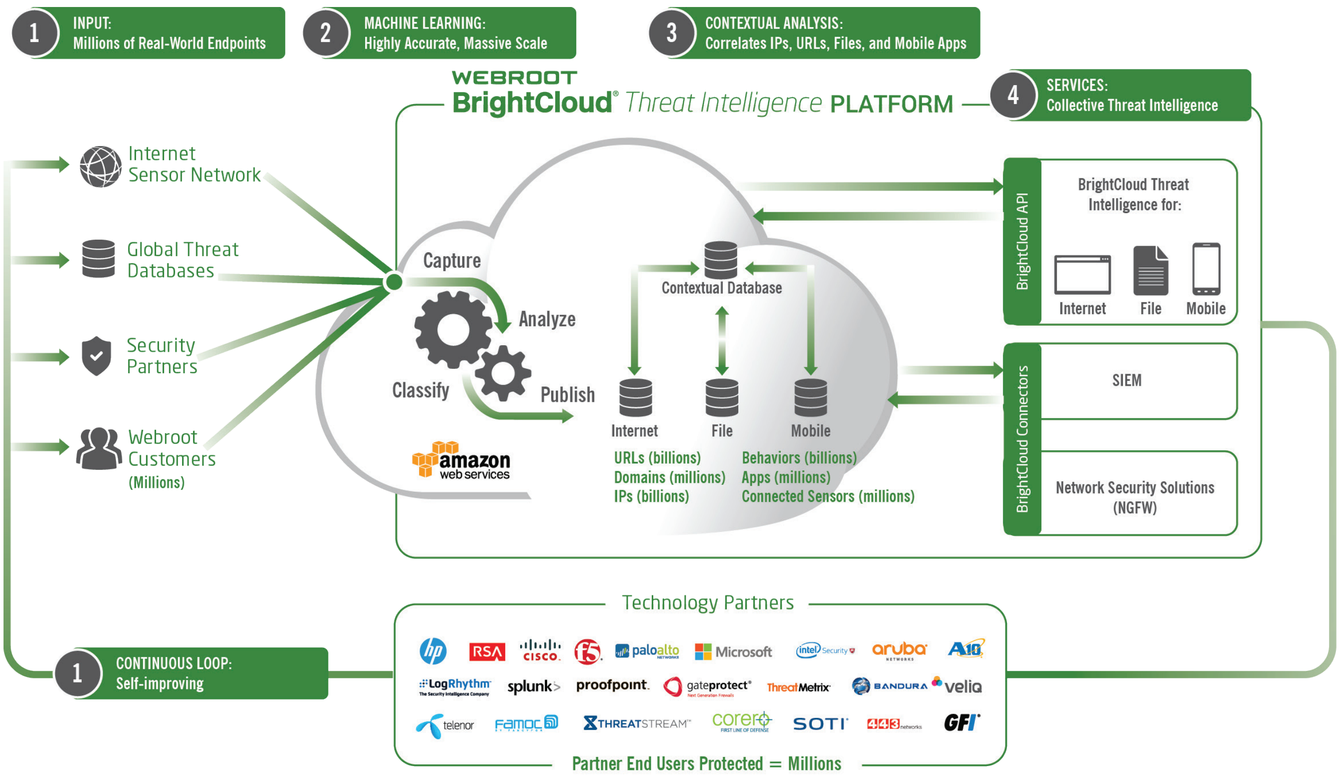
Risk scoring is one element of a security management strategy, but quality of threat risk information is equally important.

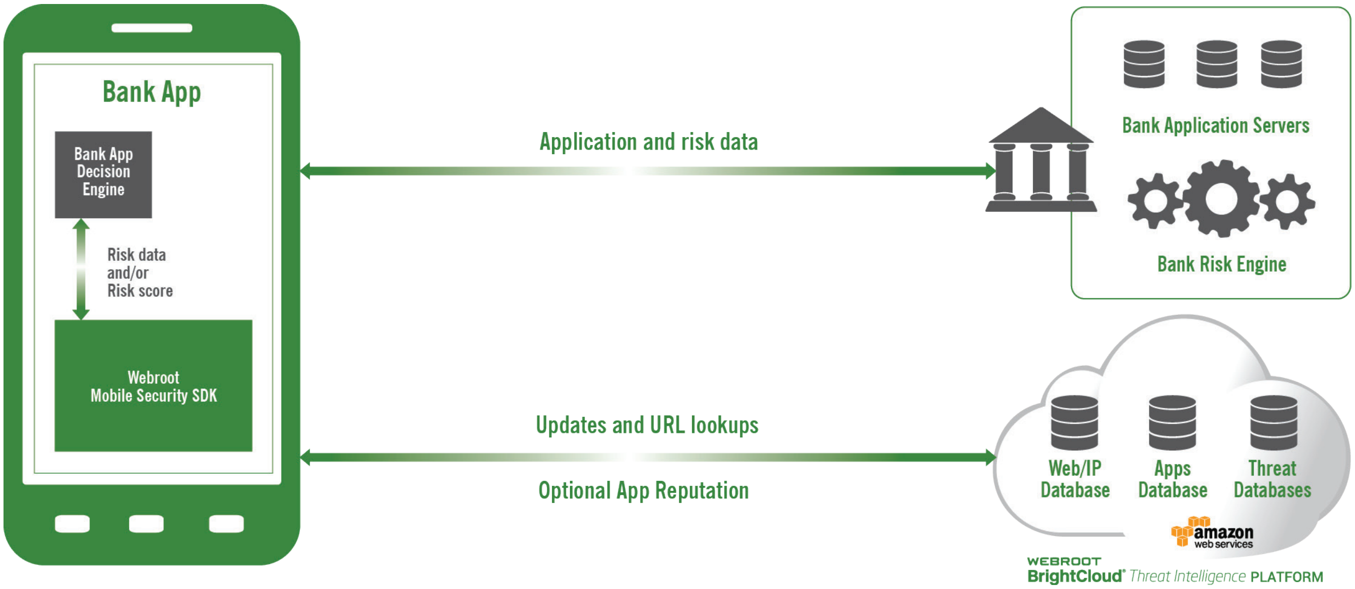
THE BRIGHTCLOUD THREAT INTELLIGENCE PLATFORM

The Webroot Mobile Security SDK accesses the Webroot BrightCloud® Threat Intelligence Platform to provide next generation threat intelligence that is highly accurate and always up to date. This architecture incorporates the patented Webroot threat processing and malicious code identification system which has intimate knowledge of more than 300 million executables, including their runtime behavioral characteristics.

BrightCloud® Threat Intelligence Services categorize files and their interactions with other files, and use the Webroot® Brightcloud® IP Reputation Service to track malicious IP addresses and provide accurate content classification, threat reputation, and threat vector data. These systems, along with another 150+ terabytes of threat data, ensure that Webroot security solutions are ready to detect new threats. As this collective intelligence delivers comprehensive real-time protection, endpoints collect over 200 gigabytes of behavioral execution data each day. Unique URL and IP data feeds from strategic partners further enrich Webroot malware intelligence.

Overview of the Webroot BrightCloud® Threat Intelligence Platform


1 INPUT: Millions of Real-World Endpoints
2 MACHINE LEARNING: Highly Accurate, Massive Scale
3 CONTEXTUAL ANALYSIS: Correlates IPs, URLs, Files, and Mobile Apps
WEBROOT BrightCloud® Threat Intelligence PLATFORM
4 SERVICES: Collective Threat Intelligence
Internet Sensor Network
Global Threat Databases
Security Partners
Webroot Customers (Millions)
Capture
Analyze
Classify
Publish
amazon web services
Contextual Database
Internet
File
Mobile
URLs (billions)
Domains (millions)
IPs (billions)
Behaviors (billions)
Apps (millions)
Connected Sensors (millions)
BrightCloud API
BrightCloud Threat Intelligence for:
Internet
File
Mobile
BrightCloud Connectors
SIEM
Network Security Solutions (NGFW)
Technology Partners
hp RSA cisco f5 paloalto Microsoft intel Security aruba A10
LogRhythm splunk> proofpoint gateprotect ThreatMetrix BANDURA velia
telenor Famoc THREATSTREAM corero SOTI 443 networks GFI
Partner End Users Protected = Millions
1 CONTINUOUS LOOP: Self-improving



Webroot Mobile Security SDK

HOW THE BRIGHTCLOUD THREAT INTELLIGENCE PLATFORM INTERACTS WITH A MOBILE APP AND THE CUSTOMER DEVICE

The Webroot® Mobile Security SDKs for Android™ and iOS® devices are designed to be embedded within a bank's mobile banking app, working behind the scenes without interfering, changing, or modifying the customer experience or transaction processes. The device scan and collection of security data will occur within two seconds of the app launching, completely invisible to the user. Customer-specific data is not captured or stored by Webroot. The user interface is under the full control of the bank, with all user interaction configured and controlled by the bank.

- The customer engages with the bank via the mobile banking app
- The Mobile Security SDK scans and collects security data within two seconds of the app launching
- The SDK provides the bank's risk engine with the risk data for instant analysis, interrogation, and action
- The risk score takes into account risks to the end user, the device, and the banking app
- Based on the risk score, decisions can be made locally or fed into a bank's risk engine to deny action that poses a threat to the bank—reducing risk, or simply flagging an issue

FLEXIBLE SECURITY MODULE DEPLOYMENT

The Webroot Security Mobile SDK is modular in design, allowing financial institutions the flexibility to load the modules into memory however best suits their needs.

Modules include:

- **Active Protection Service** – Monitor Service, which keeps track of device events. It can be left running at all times or enabled only while the host application is running.
- **Scanner Service** – This service allows the host application to run system-wide antivirus/antimalware scans of files and apps. Scans can run silently in the background or the host application can set up scanner listeners to provide feedback to the user. The host application can interactively quarantine or remove individual files and applications, if necessary.
- **Application Info Module** – This module provides information about apps installed and running on the device. Examples of different package attributes include certificate and manifest information, various network, and process-related data points.
- **Device Info Module** – Detailed information about the device and operating system is gathered to check if the device is rooted or running in an emulator. Various hardware statistics and unique device identification are included.

SUMMARY

Delivering financial services access via a mobile banking app exposes a bank to the increasing variety of mobile malware, malicious apps, data leakage, and, ultimately, financial loss. Maintaining and enhancing app security is critical to meet the demand and adoption of mobile banking. The Webroot® Mobile Security SDK allows financial institutions that offer the convenience of mobile banking to measure, manage, and minimize their security risks.

The benefits of implementing a Mobile Security SDK include:

» Invisible to the customer and doesn't require customer involvement to install or operate
» No interference or impact to customer devices
» Captures only device-specific data, not customer specific
» Increases customer retention
» Measured/managed control of each customer's device access
» Confidence that mobile banking remains secure, increasing the number of mobile banking users
» Reduction in threats presented by customer devices
» Reduction in fraud and associated costs
» Increased operational savings over non-mobile transaction methods
» No complex back end integration and can be implemented within weeks

To learn more, contact:

Lisa Grimshaw, Global Director for Financial Services Security Solutions, at lgrimshaw@webroot.com, +44 7598 538 374

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
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

WP_102015_A4