Lookout®

WHITEPAPER

Why Embedded AppDefense for mobile is a must-have for financial services

Consumer financial institutions are in the midst of a digital transformation that includes moving traditional face-to-face customer interactions to mobile devices. According to a global study by Deloitte, which surveyed 17,000 respondents across 17 countries, 72 percent of consumers use a mobile app to access their primary bank.[1] Mobile banking creates unprecedented conveniences for customers, such as mobile check deposits, near-instant person-to-person transfers, and access to personal financial accounts in real time.

The key benefits banks and other financial firms see from customer-facing mobile apps include:

- Increasing customer engagement. As customers are more engaged, they realize the value firms are delivering. A J.D. Power and associates study shows an 84-point lift in customer satisfaction from mobile banking.
- Building brand and recognition. The average user spends more than four hours per day on a mobile phone. Even if a firm's app is not open and running, its brand and logo are still visible as one of the apps installed
- on a user's device, staying top of mind for the customer.
- Reducing the cost of service. By automating face-to-face interactions, financial services firms can reduce customer support costs and redirect the savings into revenue-producing initiatives.

As new features for mobile apps continue to be developed, security must stay top of mind for app developers, to protect customer credentials from being stolen by malicious actors.

Threats to customer-facing banking apps

There are four main ways in which a malicious actor can compromise customer credentials and data in a mobile app:

1. **Compromised Device.** Through a compromised (jailbroken or rooted) device, attackers can turn off security features of the device that normally prevent access to private app data; modify the processes running on the device that interact with the app and subsequently gain access to the app's data; and install malicious code to do all of the above and more.
2. **Malware.** Via a malicious app that's installed on a device, attackers can access all apps running on the device, including enterprise apps. This allows access to data by being overly permissive or by using an exploit to compromise the device.
3. **Trojanized version of legitimate app.** Attackers can take a legitimate version of an app from Google Play or Apple App Store, modify the app and then upload it to a third party app store that has an easier app vetting process. Attackers can also send the app directly to a customer via phishing. A fake version of the app would then be available for download by customers, directing credentials and data to the attacker rather than the firm.
4. **Network attack.** Attackers can decrypt, view, or modify traffic including customer credentials after exploiting vulnerabilities in encrypted communications systems. This kind of exploit is known as a man-in-the-middle attack.

[1] Deloitte Insights, "Accelerating digital transformation in banking ", p.7, 2019

Banking trojans are active on customer devices

Leveraging data from our unique sensor network of nearly 200 million mobile devices worldwide, Lookout has analyzed 30,000 mobile devices with one or more major customer-facing banking apps installed. The mobile threat histories of these devices during a one-year study showed that ten percent of mobile banking customers encountered a mobile threat or risk.

Figure 1.1 : Customer Threat Encounters

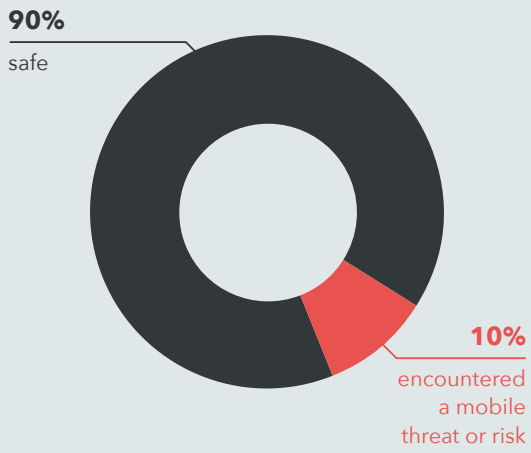
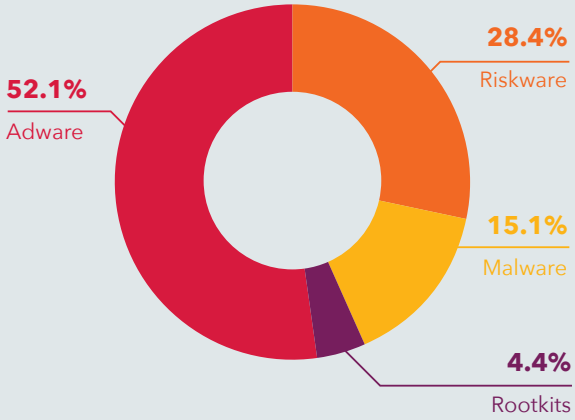


Figure 1.2: Threat Types Encountered



During this study, Lookout detected devices that encountered one or more of targeted banking trojans such as BancaMarStealer, PlayBanker, Shunbad, SvPeng, and TauSpy.

Table 1: Banking Trojans Encountered

Trojan Family	Description
BancaMarStealer	A basic login credential stealer that functions as an SMS receiver to intercept mobile transaction authentication number (mTAN) messages.
PlayBanker	A trojan that generates push notifications to encourage the victim to download rogue versions of legitimate banking apps.
Shunbad	A trojan that impersonates banking apps and steals SMS and contact data.
SvPeng	A trojan that waits in the background and monitors for the use of legitimate banking apps and then overlays a fake login screen to capture a victim's banking credentials.
TauSpy	A basic login credential stealer that functions as an SMS receiver to intercept mobile transaction authentication number (mTAN) messages.

In order to proactively decrease account takeover, increase customer trust, and protect against mobile threats, financial institutions need to protect customer-facing apps using an app defense solution.

Internal app development sometimes overlooks security

App developers are likely to be more concerned about user experience and optimizing functionality than building in security measures to protect against mobile threats. Developers might focus on making sure there are no vulnerabilities in the app code, but often they don't consider the security of the device itself.

A breach of customer credentials or data leads to a series of negative consequences for firms, including loss in revenue from fraud or as customers opt to no longer do business with the firm; erosion in brand equity due to negative publicity; and financial penalties due to non-compliance with regulations.

An app defense solution you can count on

Lookout Embedded AppDefense provides financial services firms with proactive mobile app security by preventing data compromise of customer-facing mobile apps. It does this by delivering comprehensive visibility into the spectrum of mobile risk, and provides advanced security against these risks.

Lookout has developed the Mobile Risk Matrix to help organizations understand the components and vectors that make up the spectrum of mobile risk — and to provide data that will help enterprises gain a deeper understanding of the prevalence and impact of mobile threats and vulnerabilities.

Lookout Embedded AppDefense leverages the power of the Lookout Security Graph to deliver an easy-to-deploy solution to protect individuals from data compromise when conducting transactions via mobile apps.

Specifically, Lookout Embedded AppDefense includes four unique capabilities:

The Lookout global device network. Millions of mobile devices are running Lookout Personal in more than 150 countries, and it is the same underlying technology shared by Lookout Embedded AppDefense. This massive footprint gives Lookout early and exclusive visibility into new and existing mobile threats. This device network allows Lookout to better track existing threat actors and discover zero-day threats to protect customers and minimize exposure of sensitive data.

The Lookout dataset and machine learning (ML) technology. Many security vendors claim they have machine learning capabilities, but it's not the machine learning algorithms that really matter but the data. Without a sufficiently large dataset to train ML models, a solution is not going to be effective at scale. Lookout has the dataset required and has implemented ML at scale.

A cloud-first, device-assisted architecture. Lookout designed and optimized its platform for the mobile environment. Its security approach is to leverage its cloud for deep threat analysis and implement efficient on-device scans when the mobile app is launched.

Rapid, frictionless deployment. Lookout Embedded AppDefense has been optimized to make it easy for non-security personnel to deploy the SDK into customer-facing apps in minutes. App developers are not required to be security experts in order to secure the data and functionality of customer-facing mobile apps.