Lookout App Defense

Proactively reduce risk and prevent customer data compromise in your mobile apps

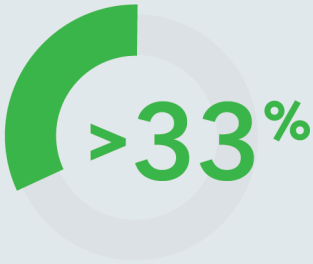
Mobile apps – the new hacker battleground

Smartphone apps have become an integral part of everyday life to manage everything from booking travel to handling finances, so enterprises have shifted to rely on apps to deliver innovative consumer experiences and increase brand engagement. However, the rise in adoption of mobile apps brings an accompanying rise in cyber threats. Malicious attackers are now primarily targeting mobile devices to steal login credentials and customer data for financial gain or committing fraud on other digital channels. One of the primary threat vectors leveraged by attackers on mobile is to go after the apps themselves.

11,500

increase in mobile banking malware kits between Q4 of 2018 and Q1 of 2019[1]

global increase in app downloads from 2016 – 2018[2]



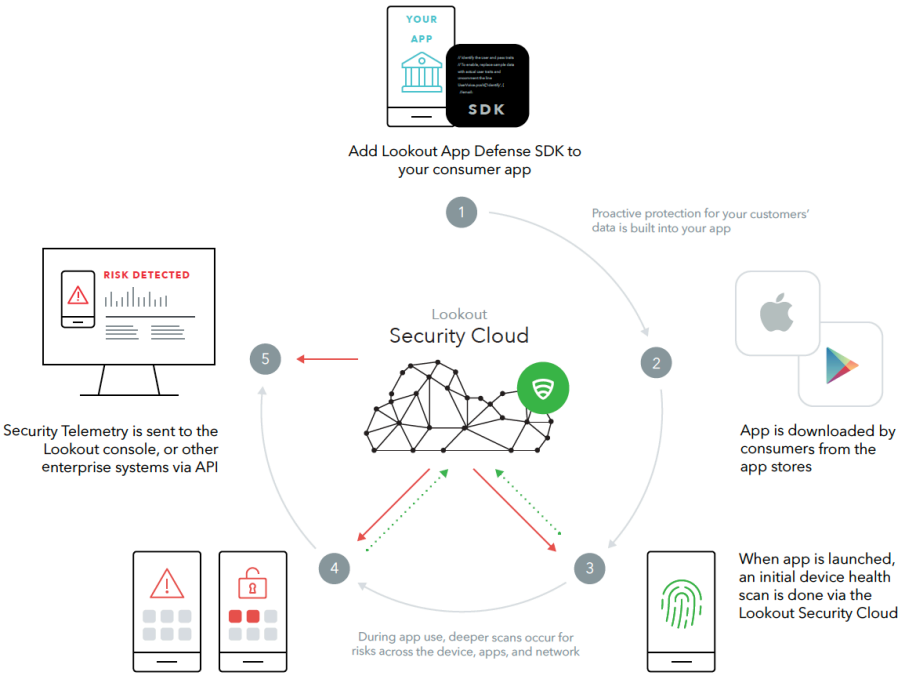
of fraudulent banking transactions now take place on mobile[3]

[1] Kaspersky Labs. "Phantom Menace: Mobile Banking Trojan Modifications Reach All-Time High.„ Kaspersky.com, Kaspersky Labs, 2018, www.kaspersky.com/about/press-releases/2018_phantom-menace.
[1] The State of Mobile 2019: Banking and Finance. App Annie, 2019, The State of Mobile 2019: Banking and Finance, www.appannie.com/en/go/state-of-mobile-2019/
[1] RSA Quarterly Fraud Report. RSA, 2019, RSA Quarterly Fraud Report, www.rsa.com/en-us/products/fraud-prevention/fraud-prevention.

Lookout app defense SDK

Lookout App Defense solution protects mobile apps via an embeddable lightweight SDK for both Android and iOS. Once the SDK is embedded, the app can leverage the Lookout Security Cloud, which contains data from over 170M devices and 70M apps, to protect individuals and organizations from cyberthreats and malware that potentially leads to data compromise.

Enterprises can access the security telemetry generated by Lookout App Defense by utilizing the SDK to mitigate within the app based on the severity and type of threat. To integrate with existing security tools such as SIEM and risk rating models, the Lookout Event Feed API provides a feed of raw security event telemetry. Overall, the SDK can help you reduce the risk of fraud and data compromise, comply with standards such as GDPR and PSD2, and protect unaware consumers by identifying potential issues on their device when using the app itself



In-app protection for detection and remediation

The key to the efficacy of the SDK is making mobile apps self-protecting through various remediation workflows without being intrusive or damaging the user experience. Below are some examples of likely detections and the mitigation steps that the app could take after being alerted by Lookout's App Defense policies:

Detection (Severity)		Remediation
Jailbroken/rooted device and privilege escalation (High)	→	Block authentication or terminate session
Zero Day exploits and man-in-the-middle attacks (High)	→	Terminate the session and clear the cache
Devices with root enablers, trojans, etc (Medium)	→	Limit transaction size or enable MFA
Malware such as adware, spyware, etc (Low)	→	No immediate remediation – monitor threats

Lookout App Risk Posture

Lookout provides visibility with App Risk Posture by breaking down the threat vectors stemming from all the consumer devices using an organization's mobile app. This includes the breakdown of devices that have unpatched operating systems, have been rooted or jailbroken, or are infected with malware along with the classification of malware families based on threat severity. Below is a sample snapshot of the data derived from the SDK telemetry and Lookout security cloud that is invaluable and actionable for a security, fraud, or mobile team as they continuously refine their risk models and strengthen their defenses against cyber threats.