Lookout App Defense

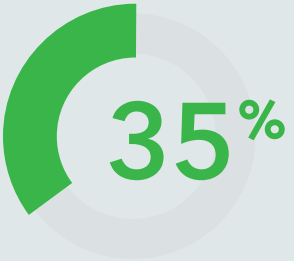
モバイル アプリで積極的にリスクを軽減して顧客データの侵害を防止する

モバイル アプリ - ハッカーの新たな戦場

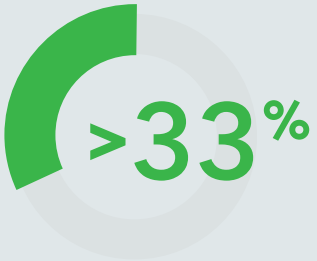
スマートフォン アプリは、旅行の予約から財務処理に至るまであらゆるものを管理し、毎日の生活に欠かせないものになっています。そのため企業は、革新的な顧客エクスペリエンスの実現やブランド拡大を、アプリを利用して行う方向にシフトしてきました。ただし、モバイル アプリの導入に伴い、サイバー脅威も生じています。悪意のある攻撃者は現在、主にモバイル端末をターゲットにして、ログイン認証情報や顧客データを盗んで金銭的利益を得ようとしたり、他のデジタル チャネルで不正行為を働いたりしています。モバイルで攻撃者が利用する主要な脅威ベクターの 1 つには、アプリ自体を狙う脅威があります。

11,500

2018 年第 4 四半期から 2019 年第 1 四半期における
モバイル バンキング マルウェア キットの増加数[1]



2016 年から 2018 年にかけて
世界中で増加したアプリ内
ダウンロード数の割合[2]



現時点でモバイルにおいて
行われているバンキング取引のうち
不正な取引の割合[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.

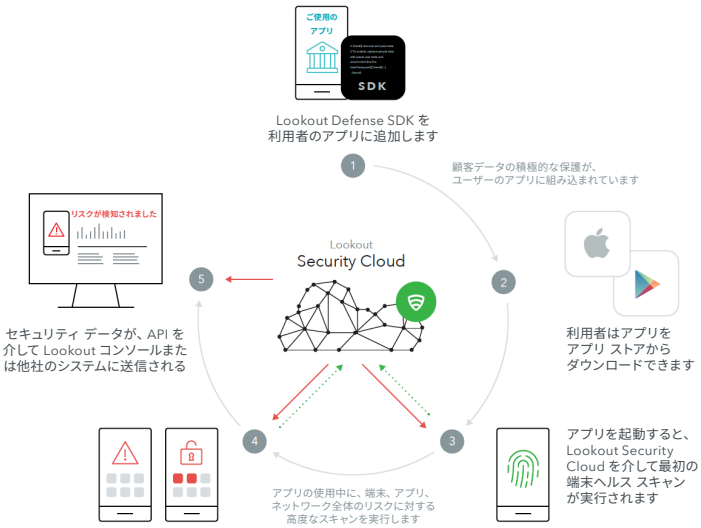
[1] The State of Mobile 2019:Banking and Finance.App Annie, 2019, The State of Mobile 2019:Banking and Finance, www.appannie.com/en/go/state-of-mobile-2019/.

[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 ソリューションは、Android と iOS のどちらにも組み込み可能で軽量な SDK を使用してモバイル アプリを保護します。この SDK が組み込まれると、アプリは Lookout Security Cloud (1 億 7 千万以上の端末と 7 千万以上のアプリからのデータが含まれます) を利用して、データ侵害に至りかねないサイバー脅威とマルウェアから個人と組織を保護できます。

企業はこの SDK を使用して Lookout App Defense が生成したセキュリティ テレメトリーにアクセスし、脅威の重大度とタイプに基づいてアプリ内で対処できます。SIEM などの既存のセキュリティ ツールやリスク評価モデルと統合するため、Lookout Event Feed API には生のセキュリティ イベント テレメトリーをフィードする機能が備わっています。一般にこの SDK を使用すると、不正行為やデータ侵害のリスクを低減し、GDPR や PSD2 などの規準に準拠できます。また、このアプリの使用時に不用意なユーザーの端末上に存在する可能性がある問題を識別して保護することもできます。



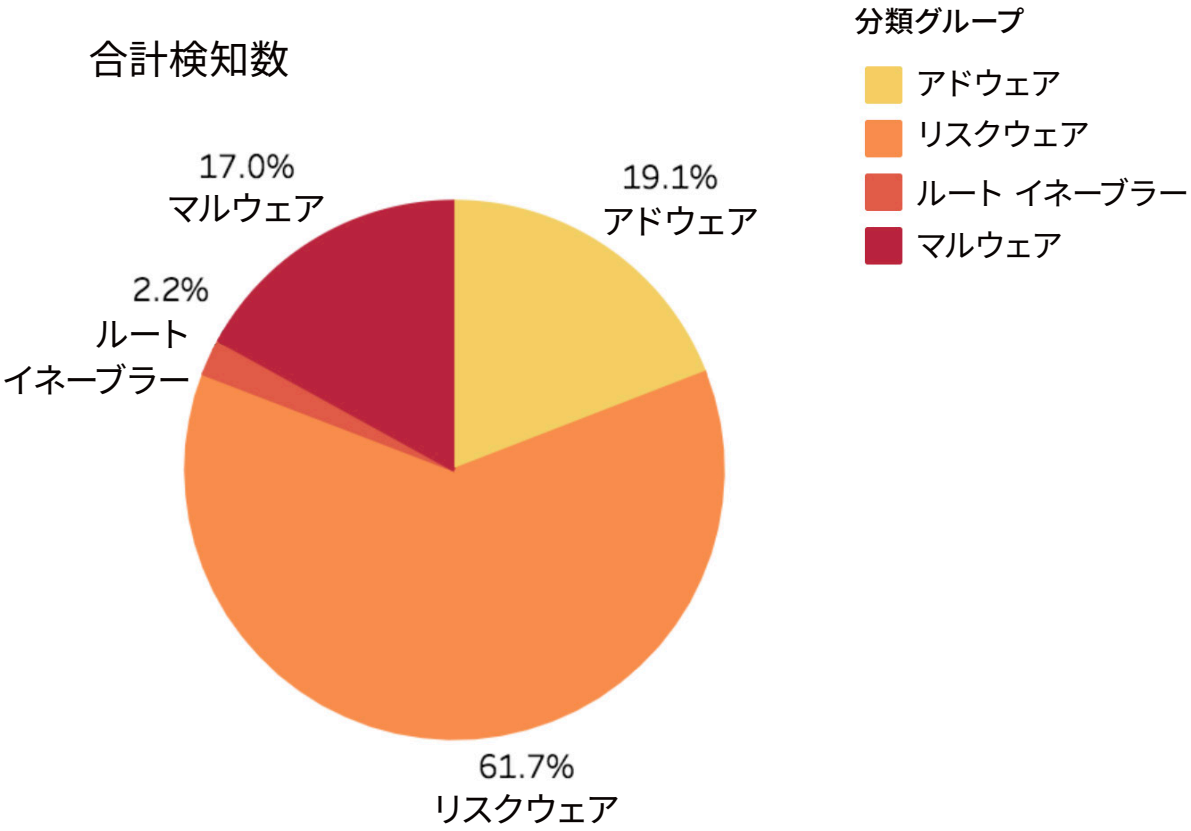
検知と修復のためのアプリ内の保護

この SDK が効率性の鍵は、モバイル アプリ自体が過度に割り込んだりユーザー エクスペリエンスを損ねたりすることなく、各種の修復ワークフローによって自ら保護できるようになるという点にあります。Lookout の App Defense ポリシーによってアラートが出された後にアプリが実行できる検知と修復のステップの例を以下に示します。

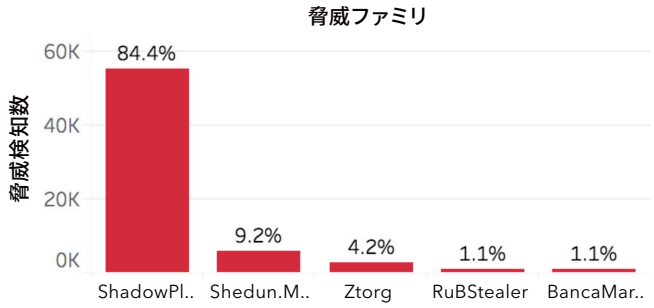
検知 (重大度)	修復
ジェイルブレイク/ルート化された端末および特権エスカレーション (高)	認証をブロックするか、セッションを終了します
ゼロデイ エクスプロイトおよび中間者攻撃 (高)	セッションを終了して、キャッシュをクリアします
ルート イネーブラーやトロイの木馬などが含まれる端末 (中)	トランザクション サイズを制限するか、MFA を有効にします
アドウェア、スパイウェアなどのマルウェア (低)	すぐに修復せず、脅威を監視します

Lookout App Risk Posture

Lookout では App Risk Posture による可視性が確保されています。組織のモバイル アプリを使用しているすべてのユーザー端末から取り出された脅威ベクターを詳細に調べて可視化されます。これには、パッチが適用されていないオペレーティング システムを使用している端末、ルート化またはジェイルブレイクされた端末、マルウェアに感染した端末、脅威の重大度に基づいてマルウェア ファミリとして分類されたマルウェアに感染した端末の詳細情報が含まれます。以下に SDK テレメトリーと Lookout Security Cloud からのデータのサンプル スナップショットを示します。これらは、セキュリティ、不正行為対策、またはモバイルのチームがリスク モデルを強化したり、サイバー脅威に対する保護を強めたりするために継続的に実行できる重要な情報となります。



トロイの木馬 - トップ 5



マルウェア検知数