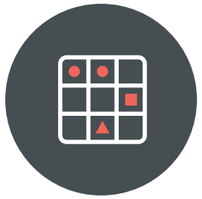
Lookout

モバイル リスクの全容

モバイル活用時に企業が把握しておくべきリスクのすべて

Lookout は、モバイル リスクの全容を構成する要素と攻撃ベクターの理解を促進し、
モバイル脅威と脆弱性の蔓延と影響について、より深く理解できるモバイル リスク マトリクスを作成しました。



モバイル リスク マトリクス

攻撃ベクター

リスクの要素

	アプリ	端末	ネットワーク	ウェブ/コンテンツ
脅威	**アプリの脅威** 1 悪意のあるアプリが情報を搾取したり、端末に損害を与え、不正なリモート アクセス権を取得する。	**端末の脅威** 攻撃者が高レベルの権限を取得し、壊滅的なデータ損失を引き起こす。	**ネットワークの脅威** 5 Wi-Fi またはセルラー ネットワーク接続を介してデータが搾取される。	**ウェブ/コンテンツの脅威** フィッシング E メールや SMS メッセージからアクセスする悪意のある URL。
SOFTWARE 脆弱性	**アプリの脆弱性** アプリに存在する脆弱性。	**端末の脆弱性** 2 OS に存在する脆弱性。	**ネットワークの脆弱性** モバイル端末はPC よりネットワーク攻撃の標的になりやすい。	**ウェブ/コンテンツの脆弱性** ビデオ、写真などの不正なコンテンツによって、端末への不正アクセスが可能になる。
ビヘイビア&設定	**アプリの ビヘイビア&設定** 3 不要に機密情報にアクセスしたり、データ漏洩のリスクが高いアプリ。	**端末の ビヘイビア&設定** 4 Android の USB デバッグや非公式のアプリ ストアからのアプリのインストール。	**ネットワークの ビヘイビア&設定** 不正な設定のルーター、不明なキャプティブ ポータル、コンテンツ フィルタリング。	**ウェブ/コンテンツの ビヘイビア&設定** 証明書を暗号化していなかったり、データを漏洩するウェブサイト

モバイル リスクの発生率

企業が支給する ANDROID 端末の 1000 台 のうち 47 台 がアプリベースの脅威に直面

2016 年第 4 四半期から 2017 年第 1 四半期の間、Lookout Mobile Endpoint Security で保護されている企業の Android 端末のうち、アプリベースの脅威に直面したのは1000 台に 47 台でした。

1

57% の IOS ユーザーが OS を 10.3 以降のバージョンにアップデートしていない

2017 年 3 月 27 日に iOS 10.3 がリリースされてから、2017 年 4 月 14 日までの間に、最新の iOS のバージョンにアップデートをしたのは全ユーザーの 43% にとどまっています。10.03.1 は、WiFi を経由したエクスプロイトを引き起こすコードに対する修正パッチであるため、この数字は大きな懸念を生みます。このデータポイントは、Lookout Personal の iOS ユーザーを基にしています。

2

アプリの 30% が端末のコンタクト情報にアクセス

企業が支給する iOS 端末にインストールされたアプリの、38% が GPS にアクセス、8% がカレンダーにアクセス、10% がマイクにアクセス、75% がカメラにアクセスしています。iOS における企業向け アプリ全体では、43% が Facebook に接続し、14% が Twitter に接続しています。

3

企業が支給する ANDROID 端末の 1000 台 のうち 5 台 がルート化されている

企業が支給する iOS 端末では 1000 台に 1 台がジェイルブレイクされています。

4

企業が支給するモバイル端末の 1% がネットワークの脅威に直面

Lookout の調査では、企業が支給するモバイル端末の 1% 弱が去年 1 年間でネットワークベースの脅威に直面しました。

5

データについて：
分析したデータは、2016 年 4 月 15 日から 2017 年 4 月 16 日にかけて、世界中で Lookout が保護する個人および企業デバイスからなるグループから収集したものです。分析した企業ユーザーのデータは、金融機関、医療機関、政府機関、その他業界で利用されている Android および iOS 端末が対象です。個人ユーザーのデータにおいては、世界各国の個人ユーザーが利用するAndroid および iOS 端末が対象となっており、その数は 1 億台以上にのぼります。すべてのデータは無記名で抽出され、この分析を実施するにあたり、企業データ、ネットワーク、システムへのアクセスは行っていません。

LOOKOUT の概要：
Lookout は、何千万もの個人、企業、政府機関にモバイル セキュリティを提供するサイバーセキュリティ企業です。Lookout Security Cloud は、世界に存在する 4 千万以上のアプリを網羅したデータセットを駆使し、簡単には検出できないつながりを特定することでモバイル攻撃を未然に防ぎます。AT&T、Deutsche Telekom、EE、KDDI、Orange、Sprint、T-Mobile、Telstra といった世界有数のモバイル ネットワーク企業が、効果的なモバイル セキュリティ ソリューションとして Lookout を選択しており、AirWatch、Ingram Micro、Microsoft、MobileIron などの大企業ともパートナーシップを結んでいます。Lookout の本社はサンフランシスコにあり、アムステルダム、ボストン、ロンドン、シドニー、東京、トロント、ワシントン D.C. にもオフィスを構えています。Lookout の詳細は弊社ホームページ (www.lookout.com/jp) をご覧ください。また、Facebook、Twitter、LinkedIn で Lookout をフォローすることも可能です。