Lookout Discovery – BeiTaAd プラグイン

Lookout によるお客様を保護しサポートするための脅威の発見と調査

背景と発見の経緯

2018 年後半に、Lookout の研究者は Google Play のいくつかの人気アプリに巧妙な手口で隠された広告プラグインを発見しました。このプラグインは、ユーザーのロック画面で広告を強制的に表示し、スリープ状態でも動画や音声の広告を表示させ、さらに、アプリ外広告を表示することで、ユーザーは他のアプリを使うこともできなくなります。最終的に、BeiTaAd が仕込まれたアプリは 238 本、インストール件数は合計 4 億 4000 万件に上ることが明らかになりました。

重要なポイント

1. 症状の現れ方が特殊で、存在を消すために巧妙な手口が使われている
2. アプリに隠されたファイルを復号化し、プラグインを読み込み、保存する形で機能
3. 端末自体にはインストールされないため、影響を受けたアプリを削除しない限り、取り除くことができない

機能と影響を受ける範囲

このプラグインにより、電話はほぼ使えない状態になります。広告はすぐに表示されるわけではなく、アプリを起動してから約 24 時間後に表示され始め、中にはアプリを起動してから 2 週間後から表示され始めるものもあります。2018 年にリリースされて以降、数回リファクタリングが行われていますが、最新のバージョンでは、AES を利用して暗号化された dex ファイルを無害な .renc ファイルに見せかけています。プラグインを隠すための暗号化・難読化の技術は時と共に進化しており、そのアクティビティに関わる文字列は XOR を用いて暗号化され、Base64 にエンコードされています。アプリを起動すると、SDK が初期化され、BeiTaAd のアセットのパスが取得されます。そして、端末に保存する前に、復号化され読み込まれたかどうかがチェックされます。BeiTaAd 自体は端末にインストールされないため、ユーザーがダウンロードしたアプリをアンインストールしない限り、削除できません。2019 年 5 月 23 日時点で、このプラグインによる影響を受けていた Google Play の 230 以上のアプリが、削除されたか、BeiTaAd プラグインを含まないバージョンにアップデートされています。

Lookout はどのように BeiTaAd などの脅威を検知してお客様を保護しているか

BeiTaAd の場合、いくつかのアプリを調べたところ、ホーム画面でフルスクリーン広告が表示されるものがあったため、Lookout の研究者はこのプラグインと、これを隠すための巧妙な手口を解明することができました。BeiTaAd を検出し、注意を喚起するようになってから、Lookout では数十万もの端末をアドウェアから守っています。このプラグイン ファミリーからは、モバイル アドウェアの今後の動向に関して有用な見識を得ることができました。これからも、検知されないようにするために類似の手法をとろうとするデベロッパーが現れることが予想されます。

Lookout Threat Advisory Service

急速に変化するモバイル セキュリティの世界では、実情を正確に把握するのが難しい場合があります。Lookout Threat Advisory は、数百万台の端末からなる Lookout のグローバル センサー ネットワークの膨大なデータセットを一流のセキュリティ研究者たちからの見識と組み合わせて、最新のモバイル脅威とリスクに関する実用的なインテリジェンスを提供いたします