Lookout Discovery - eSurvAgent

Lookoutによるお客様の保護とサポートのための脅威の発見と調査

背景と発見の経緯

2018 年の初めに、Lookout は eSurvAgent を調査しました。eSurv というイタリアの会社 (以前の Connexxa) が関連する高度な Android 監視ウェア エージェントです。Exodus としても知られるこのエージェントは、少なくとも 5 年間にわたって開発されていたようです。これは、ドロッパー、大きな第 2 ステージ ペイロード、端末へのルート アクセスを取得する最終ステージを備えた、マルチステージの脅威となっています。最近、Lookout の研究者は、同じ脅威の iOS コンポーネントを発見しました。その脅威は、カスタマー サポート サイトを模倣したフィッシング サイトを通じてユーザーに配信されました。さらに、Apple の企業プロビジョニング システムが悪用され、eSurv アプリケーションは正式な Apple 発行の証明書で署名されていました。

重要なポイント

1. 合法的インターセプト市場向けに作成されたと思われる
2. Apple の企業アプリ プロビジョニング システムを悪用することで機能する
3. 機能はプッシュ ペイロードによって制御されるため、攻撃者は取得するデータを指定できる

機能と影響を受ける範囲

iOS の亜種には、Android リリースが提供する機能のサブセットが含まれており、端末のOSを改ざんすることはできませんでした。とはいえ、このバージョンでは、Apple の認証プロセスを利用して正当に表示されていたため、iOS 端末にインストールされると、以下のタイプのデータを盗み出すことができました。

連絡先情報 | 写真 | GPS 位置情報 | オーディオ | ビデオ | 端末情報

このソフトウェアは、イタリアとトルクメニスタンのモバイル キャリアを模したフィッシング サイト、およびイタリアの Play ストアで発見されました。その後、公式の Play ストアから削除され、Apple はその証明書を失効させました。

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

Lookout Security Intelligence チームは、静的および動的分析と機械学習エンジンを組み合わせることにより、新しい脅威の発見と調査を継続的に行い、お客様を保護しサポートしています。HTTPS ピニング、HTTPS を介してトンネリングされる C2 トラフィックに使用される非対称暗号化、API エンドポイント URL とディレクトリ パスのすべての部分に使用される GUID 等に基き、eSurvAgent を監視ウェアとして分類しました。Lookout がインストールされた端末は、2018 年 3 月以降、eSurvAgent を検知して警告が出されています。Lookout は、検出されにくい他の高度な監視ウェアからも保護します。

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。