

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PPER、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 等に基づき、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、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。