

【注意喚起】相次ぐ情報漏えい、その原因の一つは「アプリ解析からのサーバ攻撃」

～AI で高度化する脆弱性探索、Android アプリを手掛かりにした A2B 攻撃に注意～

【ポイント】

- 国内で相次ぐ情報漏えい事案の原因の一つとして、公開アプリを悪用した「A2B 攻撃」を特定
- 攻撃者は公開 Android アプリを解析し、得られた情報をもとに接続先のサーバを狙い撃ち
- Android アプリを提供する事業者に向け、3 種の推奨対策をまとめた注意喚起を公表

国立研究開発法人情報通信研究機構（^{エヌアイシーティ}NICT、理事長：大野 英男）の脅威情報分析チーム^{レティース}LETTICE は、国内で相次ぐ情報漏えい事案の原因の一つとして、一般に公開されている Android アプリを解析し、その情報を悪用してアプリの接続先であるバックエンドサーバ[※]を攻撃する手法を特定しました。

LETTICE は、この攻撃手法を「A2B 攻撃（App-to-Backend Attack）」と名付け、その仕組みと、Android アプリを公開する事業者に推奨する 3 種の対策をまとめた注意喚起を公表しました。注意喚起の詳細は CYNEX Library をご覧ください（<https://cynex.nict.go.jp/library/261013-01.html>）。

※バックエンドサーバ: Web サイトやアプリの裏側で、ログイン認証や利用者情報の管理などを行うサーバ。脆弱性が悪用されると、不正アクセスや個人情報の漏えいにつながるおそれがある。

【背景】

国内で個人情報などの大量漏えい事案が相次いでいます。一方、その攻撃手法には不明な点も多く、被害の発生や拡大を防ぐためには、攻撃の実態を明らかにすることが急務となっています。

【今回の成果】

NICT の脅威情報分析チーム LETTICE は、独自の調査・分析により、国内で相次ぐ情報漏えい事案の原因の一つとして、公開 Android アプリの解析結果を悪用し、アプリの接続先サーバの仕様に合わせた攻撃を行う「A2B 攻撃（App-to-Backend Attack）」を特定しました。

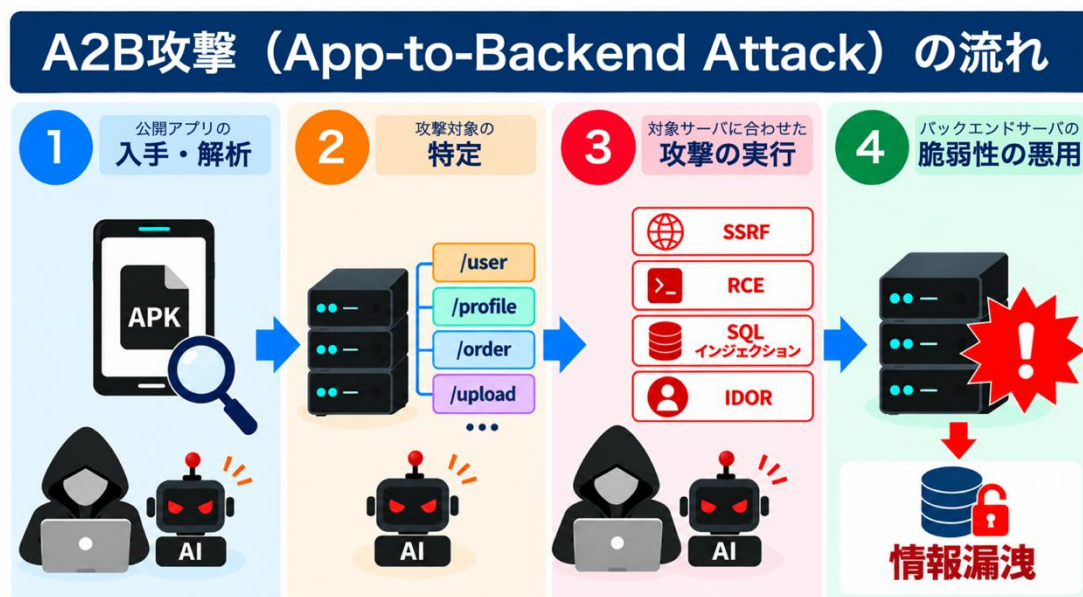


図 A2B 攻撃の流れ

A2B 攻撃では、攻撃者が一般に公開されている Android アプリを入手・解析し、アプリが通信するサーバの接続先や通信の仕組み(API)などを調べます。そして、得られた情報をもとに、攻撃対象のサーバに合わせた攻撃を実行します。

アプリを提供する事業者から見ると、一般には公開していないつもりでもサーバの内部仕様が攻撃者に知られ、自社のシステムの弱点をピンポイントで狙った攻撃を受けることになります。その結果、サーバに脆弱性が存在する場合には、個人情報などの漏えいにつながるおそれがあります。

同様の問題は Android アプリに限らず、iOS アプリや Web サービスのバックエンド API でも発生する可能性があるため、これらを提供する事業者においても注意が必要です。さらに、AI の活用によってアプリの解析や脆弱性の発見が効率化され、こうした攻撃がより多くのシステムに広がる可能性にも注意が必要です。

今回公表した注意喚起では、A2B 攻撃の具体的な手法や主に狙われている脆弱性を解説するとともに、Android アプリを公開する事業者に推奨する「侵害の確認」「脆弱性の点検」「暫定的な緩和策」の 3 種の対策を紹介しています。また、攻撃に関連する IoC(侵害指標)も掲載しています。

注意喚起の詳細は CYNEX Library をご覧ください。

<https://cynex.nict.go.jp/library/261013-01.html>

【LETTICE について】

LETTICE(Leading Expert Team for Threat Intelligence Collection and Evaluation)は NICT のサイバーセキュリティネクサス(CYNEX)において、2024 年 2 月に発足した脅威情報の共同分析チームです。CYNEX に参画する組織の有志によって構成され、様々なサイバー脅威に関する情報を共同で分析し、得られた知見の共有に取り組んでいます。

【本注意喚起に関するお問い合わせ】

本注意喚起の内容に関するご質問は、下記「本件に関する問合せ先」まで電子メールでお寄せください。

個々のシステムの診断や改修には、システムの構成や運用状況に応じた専門的な確認が必要です。NICT では個別のシステムに関する診断や技術的なご相談には対応しておりませんので、本注意喚起を点検の手がかりとして、社内のセキュリティ担当者や開発・運用の委託先、セキュリティ専門事業者などにご相談の上、対応を進めていただくようお願いいたします。

< 本件に関する問合せ先 >

国立研究開発法人情報通信研究機構
サイバーセキュリティ研究所
サイバーセキュリティネクサス
CYNEX アライアンス事務局
E-mail: cynex@ml.nict.go.jp

< 広報（取材受付） >

広報部 報道室
E-mail: publicity@nict.go.jp