アンラボ・セキュリティレター

Press Ahn

2023.2　Vol.110

アプリ署名証明書の流出、どれだけ危険なのか？

アプリ署名証明書の流出、どれだけ危険なのか？

Android アプリケーション（アプリ）は、開発者が自作した証明書に基づいて署名および配布される。これは Google Play ストア（Google Play Store）などマーケットにアップロードする際に開発者を区分する用途に使われ、開発者本人が開発したアプリであることを証明する重要な手段である。また、アプリのアップデートもこの署名を確認して一致する場合にのみ可能で、アプリ自体を保護する役割もある。

ポリシーの背景は、個人開発者が自由にアプリを作ってアップロードできるようにすることだ。したがって、別途の認証機関を置かずに開発者が自主的に証明書を管理するようにした。アプリ開発と配布の参入障壁を低くし、ユーザーがより幅広くアプリを体験できるという長所があるが、逆にこの要素が複合的に作用し署名証明書流出などの問題が発生することもある。

今回は公式アプリ署名証明書流出関連の攻撃タイプと事例をまとめ、不正行為に対するアンラボの複合的な対策システムを紹介する。

流出証明書取得後の攻撃者の行為タイプ

まず、攻撃者が流出した署名証明書を取得した後に行った不正行為のタイプは、大きく 2つ確認されている。

1. 証明書でマルウェアの検知を回避

公式サービスを行うアプリに署名された証明書でマルウェアを認証することである。これにより、セキュリティソリューションの検査で悪性として検知されることを回避する。

2. 証明書の公式サービスアプリのデータ共有

Android システムにおいて「コンテンツプロバイダ (Content Provider)」は、アプリケーション間のデータを共有できるようにする。公式アプリが Content Provider 設定を「署名共有」に指定した場合、その証明書で署名されたすべてのアプリが Content Provider にアクセスできる。すなわち、悪性アプリで内部のユーザーデータを取得できるようになり、実質的に公式アプリ攻撃手法として活用される。

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="com.example.myapp">
    <permission android:name="my_custom_permission_name"
                android:protectionLevel="signature" />
```

[図1] Content Provider 設定が「署名共有」に指定された場合

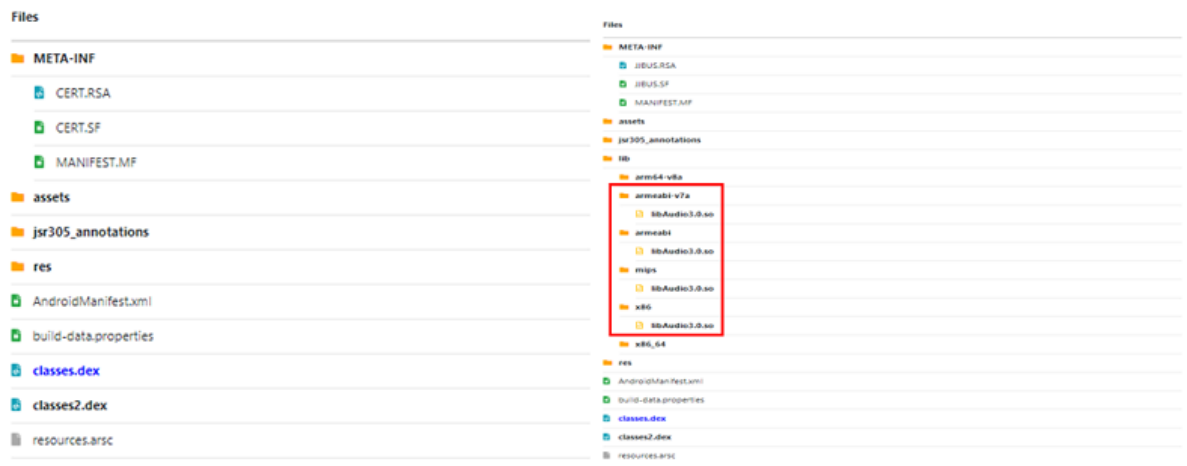
現在までは公式サービスアプリを攻撃する悪性アプリは確認されておらず、ホワイトリスト (Whitelist) 基盤セキュリティソリューションの検知を回避して不正行為を発生させる目的のサンプルのみが発見された。

次に、流出した証明書を獲得し攻撃者が不正行為を敢行した韓国国内の事例を見てみよう。

流出した証明書を活用した不正行為の敢行事例

1. 不正機能が追加されたアプリを Google Play ストアにアップロード

2019年に「光州バス」というアプリが Google Play ストアにアップデートされたが、このアプリに不正機能が含まれており、問題が発生した事例がある。ちなみに、光州バスは個人開発者が開発してサービスされていたアプリで、バスの路線図や到着予定時刻などを教えてくれる。2012年にサービスを開始して2018年に開発者が開発およびアップデートを中断したが、アプリに署名した証明書情報を廃棄しなかった。その後、証明書とコード、そして Google Play ストアにアップロードした開発者の ID およびパスワードを攻撃者が取得し、このアプリにマルウェアを追加して Google Play ストアにアップロードした。



[図2] 正常サンプルとマルウェア追加サンプルの比較

また、マルウェアが含まれたアプリが正常にアップデートされ、個人ユーザーの Google ID とパスワードを窃取した。光州バスの開発者が開発した他のアプリにも同じタイプのマルウェアを追加し、Google Play ストアにアップロードした。

*不正行為の要約: このマルウェアは *libAudio.3.0.so native* ライブラリファイルを追加し、このライブラリは追加ライブラリである *libMovie.so* ファイルをダウンロードして *Google ID* など主要情報を窃取する。

2. NHN 証明書流出

2022年 8月、NHN 証明書で署名された金融アプリが収集され、確認されたタイプだ。具体的には NHN で開発されたアプリを対象にした攻撃ではなく、セキュリティソリューションからマルウェアとして検知されることを回避するための手段として NHN 証明書を使用したことが確認された。一部 Android のホワイトリスト基盤セキュリティソリューションの場合と、比較的検証が簡単な署名情報を抽出して公式マーケットに登録されている署名情報の場合、正常なアプリで処理することができる。この場合、このアプリの不正行為は検査せずに「ホワイト (White)」として処理する現象が発生する可能性がある。

*不正行為の要約: このマルウェアは、従来の金融関連ボイスフィッシングアプリ、別名 *kaishi* マルウェアだ。受信番号操作および発信番号操作機能を作動させ、この悪性サンプルをダウンロードして強制インストールさせる「ダウンローダー *(Downloader)*」アプリだ。

3. スマホメーカーファームウェア (Firmware) 用証明書流出

2022年 11月 12日、Google は Google APVI Report を通じてプラットフォーム証明書が流出した状況が確認されたと明らかにした。ちなみに、APVI は「アンドロイドパートナー脆弱性イニシアチブ (Android Partner Vulnerability Initiative)」の略で、Google パートナー社の装備の脆弱性まで発見し対応するという趣旨から始まった。

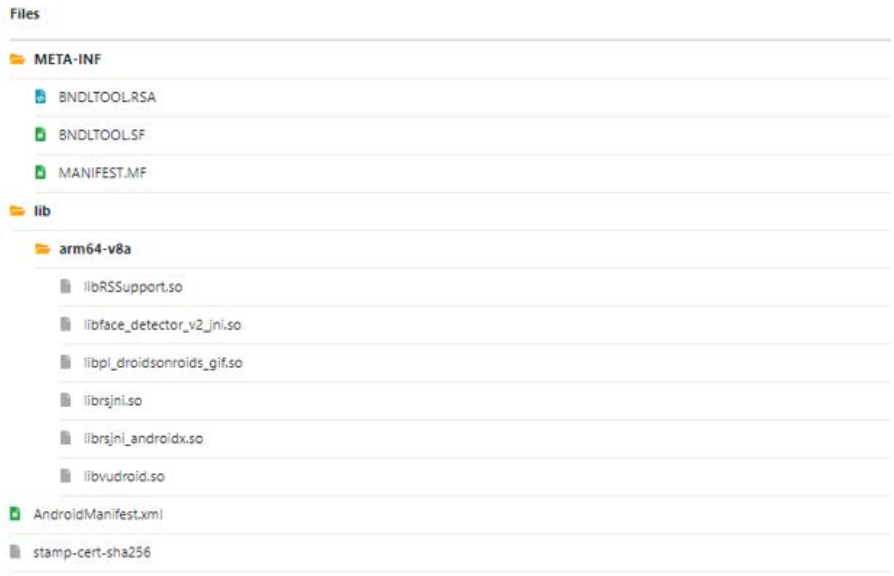
プラットフォーム証明書 (Platform Certificate) とは、システムイメージで Android アプリへ署名するのに使用なアプリ署名証明書だ。この証明書に署名されたアプリは「sharedUserId」を「android.uid.system」に指定し、システム権限を獲得することができる。すなわち、メーカー証明書で署名された悪性アプリがそのメーカーのスマホにインストールされた場合、システム権限と共にユーザーデータ (user data) 領域にアクセスできる権限が付与される。要するに、実際の OS と同じアクセス権限で作動できるようになるのである。

発見された悪性アプリは Google が認証したファームウェア証明書で署名され、そのメーカーのスマートフォンだけで不正行為を行うという点で、従来とは異なる特異な攻撃タイプに分類される。

*不正行為の要約: 悪性アプリの実行時、システム権限を獲得してユーザーの個人情報、通話内容、通話時に自動録音を行い、録音記録などを攻撃者に送信する。

4. 攻撃者の故意的な「ホワイト」証明書作成の試み

2021年 12月 7日、Google Play ストアに登録されたアプリの事例としてサンプル分析を通じ、発見された。このアプリはビットコイン関連アプリとして Google Play ストアに登録された。このアプリの特徴は、dex ファイルやその他の実行可能コードがなく単純なパッケージ (package) 名と署名情報しかないということだ。アプリ内部に dex ファイルがないため、インストールが不可能なファイルであることが確認された。



[図3] アプリの仕組み

このアプリは Google の審査を通過して正常にアップロードされ、2022年 2月 16日まで周期的にバージョンコードのみ変更してアップデートされた。アップデート時に使用した署名情報は 2022年 12月 5日から kaishi マルウェアを認証する際に使用された。

Google Play ストアにアップロードしたのは、冒頭で言及した通りホワイトリスト基盤のセキュリティソリューションを回避するための意図的な試みと見られる。Google Play ストアを通じて周期的なアップデートを提供し、その証明書を十分な期間露出させ信頼できるように誘導した後、マルウェア署名に使用したものと推測される。

アンラボの対応現況

アンラボは基本的に許可基盤の「ホワイトリスト (Whitelist)」と遮断基盤の「ブラックリスト (Blacklist)」を一緒に使用するシステムを備えている。さらに、明白な正常アプリをホワイトリストで管理する一方、悪性サンプルは機能の特徴を収集してブラックリストで管理する。ブラックリストによってホワイトサンプルで不正行為が検知された場合、アナリストが直ちにサンプルの悪性有無を詳細に分析し適切な措置を取る。

このようなシステムを基に本文で提示した事例に対応してきており、その内容は次の通りである。

#1. 不正機能が追加されたアプリを Google Play ストアにアップロード: このサンプルは従来の Google Play ストアに正

常にアップロードされるアプリで、ホワイトサンプルとして管理された。しかし、libAudio.3.0.so ファイルが「ダウンローダー」として検知され、分析専門家がサンプルを分析してこの証明書が流出したと判断し悪性に分類した。

#2. NHN 証明書流出: このサンプルは収集後すぐに典型的な kaishi マルウェアであることが確認され、直ちに NHN にその情報を共有し、不正機能サンプルに分類した。この署名情報で署名されたアプリを持続的に収集し、追加分析および悪性分類を行っている。

#3. スマホメーカーファームウェア（Firmware）用証明書流出: まず、LG はもう端末を生産していないが、この証明書で署名されたアプリが使われており「不正機能が含まれた」アプリに限り、悪性に分類した。サムスン（Samsung）、レノボ（Lenovo）、メディアテック（MediaTek）などはこの証明書を過去に廃棄し最新機器に影響を及ぼさないことが確認され、そのアプリは悪性に分類した。

結論

Android は OS およびマーケットの特性上、アプリ開発とアップロードが極めて自由だ。しかし、そのアプリ管理の重さまで軽くなったという意味ではない。認証および管理に機関が介入しないということは、そのアプリのメンテナンスとセキュリティ管理責任が全面的に開発者にあることを意味する。

これに対し、次のような改善策が必要である。

#1. 証明書の管理およびシステムに対する認識向上: アプリ開発者が所有および管理する証明書は、これまでユーザーに対し築いてきた信頼の重さと比例することを忘れてはならない。先に言及したように、別途の認証機関がないということは、それだけ個別的に管理に注意を払わなければならないという意味だ。繰り返し強調するが、アプリ署名証明書は別途の認証機関がある他の証明書よりさらに高い水準の管理が必要だ。そして、これを体系的に遂行できる方法が用意されるべきである。

#2. セキュリティソリューション改善システムの構築: セキュリティソリューションが個人および企業開発者の証明書を簡単に信頼すると、現存する脅威への対応に限界が出てくる。このような事実を認知し、悪性サンプルを機能基盤で分類する技法を複合的に活用して不正行為を防止できるようにしなければならない。

http://jp.ahnlab.com/site/main.do

http://global.ahnlab.com/site/main.do

http://www.ahnlab.com/kr/site/main.do

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315 (代)