보안 이슈

AhnLab 보안 전문가의 심층분석! 보안 이슈 정보를 전해드립니다.

앱 서명 인증서 유출, 얼마나 위험할까?

AhnLab 2023-02-06

안드로이드 애플리케이션(앱)은 개발자가 자가 생성한 인증서를 기반으로 서명 및 배포된다. 이는 구글 플레이스토어(Google Play Store) 등 마켓에 업로드 할 때 개발자를 구분하는 용도로 사용되며, 개발자가 자신이 개발한 앱이라는 것을 증명하는 중요한 수단이다. 또한, 앱 업데이트도 해당 서명을 확인하여 일치할 경우에만 가능해 앱 자체를 보호하는 역할도 한다.

정책의 배경은 개인 개발자가 자유롭게 앱을 만들어 업로드 할 수 있도록 하는 것이다. 따라서, 별도의 인증 기관을 두지 않고 개발자가 자체적으로 인증서를 관리하도록 했다. 앱 개발과 배포의 진입 장벽을 낮추고 사용자들이 더 폭 넓게 앱을 경험할 수 있다는 장점이 있지만, 반대로 해당 요소들이 복합적으로 작용해 서명 인증서 유출 등의 문제가 발생하기도 한다.

이번 글에서는 공식 앱 서명 인증서 유출 관련 공격 유형과 사례를 정리하고, 악성 행위에 대한 안랩의 복합적인 대응 체계를 소개한다.

유출 인증서 취득 후 공격자 행위 유형

우선, 공격자가 유출된 서명 인증서를 취득한 후 수행한 악성 행위 유형은 크게 2가지가 확인되었다.

1. 인증서로 악성코드 탐지 회피

공식 서비스를 수행하는 앱에 서명된 인증서로 악성코드를 서명하는 것이다. 이를 통해 보안 솔루션의 검사에서 악성으로 탐지되는 것을 회피한다.

2. 인증서의 공식 서비스 앱 데이터 공유

안드로이드 시스템에서 '콘텐트 프로바이더(Content Provider)'는 애플리케이션 간 데이터를 공유할 수 있도록 한다. 공식 앱이 Content Provider 설정을 '서명 공유'로 지정한 경우, 해당 인증서로 서명된 모든 앱이 Content Provider에 접근할 수 있다. 즉, 악성 앱으로 내부 사용자 데이터를 취득할 수 있게 되며, 실질적으로 공식 앱 공격 기법으로 활용된다.

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

[그림 1] Content Provider 설정이 '서명 공유'로 지정된 경우

현재까지는 공식 서비스 앱을 공격하는 악성 앱은 확인되지 않았으며, 화이트리스트(Whitelist) 기반 보안 솔루션의 탐지를 회피해 악성 행위를 발현시킬 목적의 샘플만 발견되었다.

다음으로 유출된 인증서를 획득해 공격자가 악성 행위를 감행한 국내 사례들을 살펴본다.

유출된 인증서 활용 악성 행위 감행 사례

1. 악성 기능이 추가된 앱을 플레이스토어에 업로드

2019년 '광주버스'라는 앱이 플레이스토어에 업데이트 되었는데, 해당 앱이 악성 기능을 포함해 문제가 발생했던 사례가 있다. 참고로, 광주버스는 개인 개발자가 개발해 서비스하던 앱으로, 버스 노선도, 도착 예정 시각 등을 알려준다. 2012년 서비스를 시작했으며 2018년 개발자가 개발 및 업데이트를 중단했는데, 앱을 서명하는 인증서 정보를 폐기하지 않았다. 이후, 인증서와 코드 그리고 플레이스토어에 업로드한 개발자의 아이디 및 패스워드를 공격자가 취득했으며, 해당 앱에 악성코드를 추가하여 플레이스토어에 업로드했다.

[그림 2] 정상 샘플과 악성코드 추가 샘플 비교

또한, 악성코드가 포함된 앱이 정상적으로 업데이트 되어 개인 사용자의 구글 아이디와 비밀번호를 탈취했다. 광주버스 개발자가 개발했던 다른 앱 역시 같은 유형의 악성코드를 추가해 플레이스토어에 업로드하기도 했다.

*악성 행위 요약: 해당 악성코드는 libAudio.3.0.so native 라이브러리 파일을 추가하고 해당 라이브러리는 추가 라이브러리인 libMovie.so 파일을 다운로드하여 구글 아이디 등 주요 정보를 탈취한다.

2. NHN 인증서 유출

2022년 8월, NHN 인증서로 서명된 금융 앱이 수집되면서 확인된 유형이다. 구체적으로는 NHN에서 개발된 앱을 대상으로 한 공격이 아닌, 보안 솔루션으로부터 악성코드로 탐지되는 것을 회피하기 위한 수단으로 NHN 인증서를 사용한 것으로 확인되었다. 일부 안드로이드의 화이트리스트 기반 보안 솔루션의 경우, 비교적 검증이 간단한 서명 정보를 추출하여 공식 마켓에 등록되어 있는 서명 정보인 경우 정상적인 앱으로 처리할 수 있다. 이 때, 해당 앱의 악성 행위는 검사하지 않고 '화이트(White)'로 처리하는 현상이 발생할 수 있다.

*악성 행위 요약: 해당 악성코드는 기존 금융 관련 보이스 피싱앱, 일명 kaishi 악성코드다. 수신 번호 조작 및 발신 번호 조작 기능을 수행하며, 이 악성 샘플을 다운로드하여 강제 설치하도록 하는 '다운로더(Downloader)' 앱이다.

3. 스마트폰 제조사 펌웨어(Firmware)용 인증서 유출

2022년 11월 12일, 구글은 Google APVI Report를 통해 플랫폼 인증서가 유출된 정황이 확인되었다고 밝혔다. 참고로, APVI는 '안드로이드 파트너 취약점 이니셔티브(Android Partner Vulnerability Initiative)'의 약자로 구글 파트너사 장비의 취약점까지 발견하고 대응하겠다는 취지에서 시작됐다.

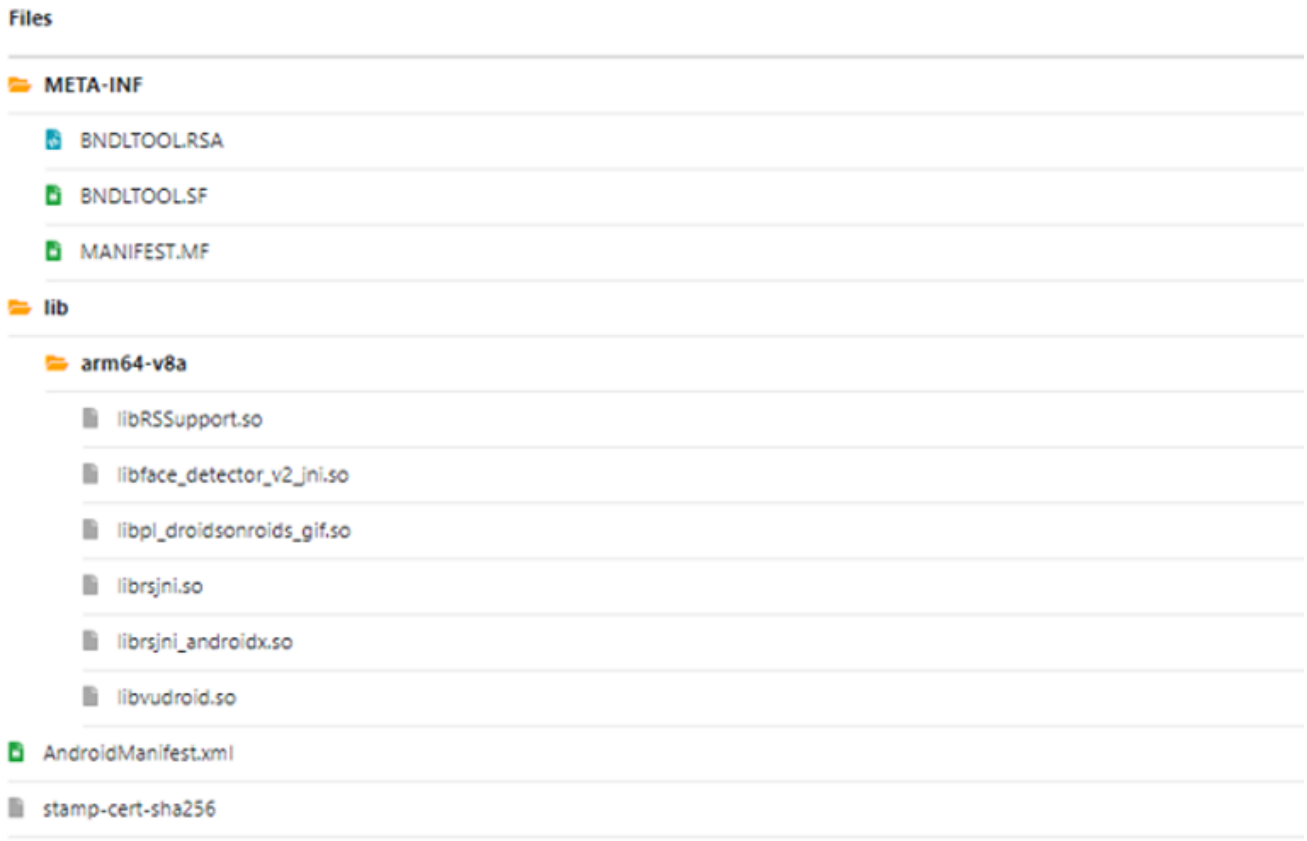
플랫폼 인증서(Platform Certificate)란 시스템 이미지에서 안드로이드 앱에 서명하는데 사용하는 앱 서명 인증서다. 해당 인증서로 서명된 앱은 'sharedUserId'를 'android.uid.system'으로 지정하여 시스템 권한을 획득할 수 있다. 즉 제조사 인증서로 서명된 악성 앱이 해당 제조사의 휴대폰에 설치될 경우, 시스템 권한과 함께 사용자 데이터(user data) 영역에 접근할 수 있는 권한이 부여된다. 한 마디로, 실제 OS와 같은 접근 권한으로 동작할 수 있게 되는 것이다.

발견된 악성앱은 구글이 인증한 펌웨어 인증서로 서명되었으며, 해당 제조사 스마트폰에서만 악성 행위를 수행한다는 점에서, 기존과는 다른 특이한 공격 유형으로 분류된다.

*악성 행위 요약: 악성앱 실행 시, 시스템 권한을 획득하여 사용자의 개인정보, 통화 내용, 통화 시 자동 녹음을 수행하고 녹음 기록 등을 공격자에게 전송한다.

4. 공격자의 고의적인 '화이트' 인증서 생성 시도

2021년 12월 7 일, 플레이스토어에 등록된 앱의 사례로 샘플 분석을 통해 발견되었다. 해당 앱은 비트코인 관련 앱으로 플레이스토어에 등록되었다. 해당 앱의 특징은 dex 파일이나 여타 실행 가능 코드 없이 단순 패키지(package) 이름과 서명 정보만 있다는 것이다. 앱 내부에 dex 파일이 없어 설치가 불가능한 파일로 확인되었다.



[그림 3] 앱 구조

해당 앱은 구글의 심사를 통과해 정상적으로 업로드 되었고, 2022년 2월 16일까지 주기적으로 버전 코드만 변경하여 업데이트 되었다. 업데이트 시 사용한 서명 정보는 2022년 12월 5 일부터 kaishi 악성코드를 서명할 때 사용되었다.

플레이스토어에 업로드 한 것은 서두에 언급한대로 화이트리스트 기반 보안 솔루션을 회피하기 위한 의도적인 시도로 보인다. 플레이스토어를 통해 주기적인 업데이트를 제공하고, 해당 인증서를 충분한 기간 동안 노출시켜 신뢰할 수 있도록 유도한 후, 악성코드 서명에 사용한 것으로 추측된다.

안랩 대응 현황

안랩은 기본적으로 허용 기반의 '화이트리스트(Whitelist)'와 차단 기반의 '블랙리스트(Blacklist)'를 함께 사용하는 체계를 갖추고 있다. 부연하면, 명백한 정상 앱을 화이트리스트로 관리하는 한편, 악성 샘플은 기능의 특징을 수집해 블랙리스트로 관리한다. 블랙리스트로 인해 화이트 샘플에서 악성 행위가 탐지될 경우, 분석가가 즉각 샘플의 악성 여부를 상세 분석해 적절한 조치를 취한다.

이러한 체계를 바탕으로 본문에서 제시한 사례들을 대응해 왔으며, 그 내용은 다음과 같다.

#1. 악성 기능이 추가된 앱을 플레이스토어에 업로드: 해당 샘플은 기존 플레이스토어에 정상 업로드되는 앱으로 화이트 샘플로 관리되었다. 하지만, libAudio.3.0.so 파일이 '다운로더'로 탐지되었고, 분석가가 샘플을 분석해 해당 인증서가 유출된 것으로 판단하고 악성으로 분류했다.

#2. NHN 인증서 유출: 해당 샘플은 수집 즉시 전형적인 kaishi 악성코드로 확인되어 즉각 NHN에 해당 정보를 공유하고 악성 기능 샘플로 분류했다. 해당 서명 정보로 서명된 앱을 지속적으로 수집하여 추가 분석 및 악성 분류를 수행 중이다.

3. 스마트폰 제조사 펌웨어(Firmware)용 인증서 유출: 우선, LG는 더 이상 단말을 생산하지 않지만, 해당 인증서로 서명된 앱이 사용되고 있어 '악성 기능이 포함된' 앱에 한해 악성으로 분류했다. 삼성, 레노보(Lenovo), 미디어텍(MediaTek) 등은 해당 인증서를 과거에 폐기해 최신 기기에 영향을 미치지 않는 것으로 확인되었으며, 해당 앱은 악성으로 분류하였다.

결론

안드로이드는 운영체제 및 마켓의 특성 상 앱 개발과 업로드가 지극히 자유롭다. 하지만, 해당 앱 관리의 무게까지 가벼워졌다는 의미는 아니다. 인증 및 관리에 기관이 개입하지 않는다는 것은 해당 앱의 유지보수와 보안 관리 책임이 전적으로 개발자에게 있음을 뜻한다.

이에 대해 다음과 같은 개선책이 필요하다.

#1. 인증서 관리 및 체계 대한 인식 제고: 앱 개발자가 소유 및 관리하는 인증서는 지금까지 사용자에게 쌓은 신뢰의 무게와 비례한다는 것은 안된다. 앞서 언급했듯, 별도 인증 기관이 없다는 것은 그만큼 개별적으로 관리에 주의를 기울여야 한다는 뜻이다. 거듭 강조하지만, 앱 서명 인증서는 별도 인증 기관이 있는 다른 인증서보다 더 높은 수준의 관리가 필요하다. 그리고, 이를 체계적으로 수행할 수 있는 방안이 마련되어야 한다.

#2. 보안 솔루션 개선 체계 마련: 보안 솔루션이 개인 및 기업 개발자의 인증서를 쉽게 신뢰하면 현존하는 위협을 대응하는데 한계가 있다. 이와 같은 사실을 인지하고, 악성 샘플을 기능 기반으로 분류하는 기법을 복합적으로 활용하여 악성 행위를 방지할 수 있도록 해야 한다.

AhnLab 엔진개발팀 김우진 책임연구원