AhnLab

安全月刊

2023.02 Vol.123

App 签名证书的泄露

App 签名证书的泄露，有何风险?

安卓应用程序（App）是根据程序开发者自生成的证书进行签名和分发的。这用于在将 App 上传到 Google Play Store 等市场时识别程序开发者，是开发者证明自己开发的 App 的重要手段。此外， App 只有在验证匹配相应签名后才能进行更新，这也起到了保护 App 本身的作用。

该政策的背景是为了让个人开发者自由创建和上传 App。因此，程序开发者可以自行管理证书，并不需要权威的数字证书签名机构认证。其优点是降低了 App 开发和分发的准入门槛，让用户可以更广泛地体验 App ，但恰恰相反，由于这些因素共同作用，可能会出现签名证书泄露等问题。

本文总结了官方 App 签名证书泄露相关的攻击类型和案例，并介绍了 AhnLab 针对恶意行为的多重响应系统。

在安卓系统中，允许“内容提供者（Content Provider）”实现App之间的数据共享。如果官方App将Content Provider设置为“签名共享”，则所有使用该证书签名的App都可以访问Content Provider。换句话说，攻击者可以通过恶意App获取内部用户数据，并将其用作针对官方App的攻击手段。

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

【图1】Content Provider设置为“签名共享”

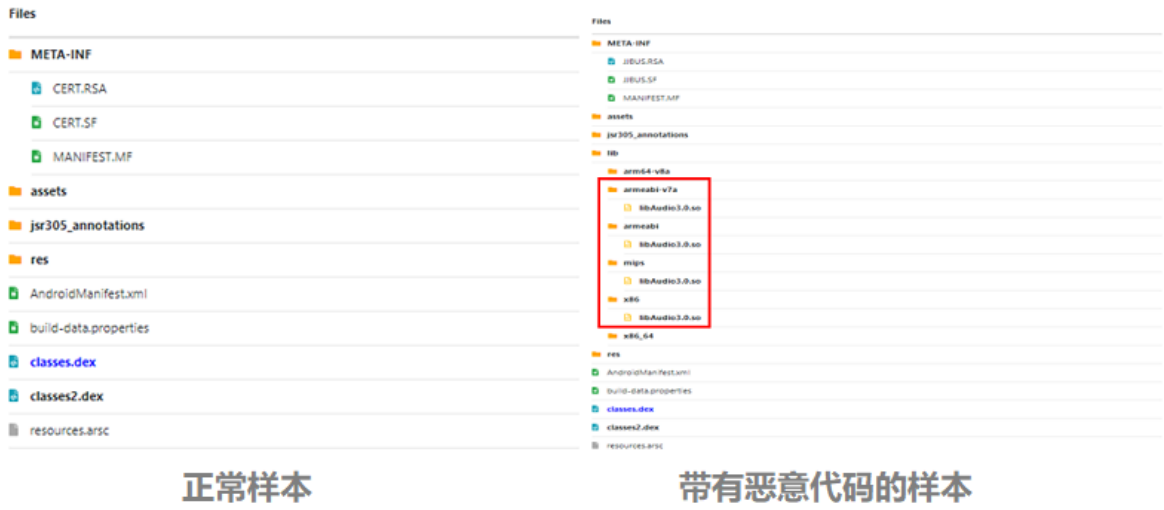
到目前为止，尚未发现攻击官方App的恶意App，仅发现了试图通过绕过基于白名单（Whitelist）的安全解决方案的检测来执行恶意行为的样本。

下面我们来看一下韩国的攻击者通过获取泄露的证书执行恶意行为的案例。

利用泄露的证书执行恶意行为的案例

1. 将带有恶意功能的App上传到Google Play Store

2019年，Google Play Store更新了一款名为“Gwangju Bus”的App，由于该App包含恶意功能而出现了问题。作为参考，Gwangju Bus是由个人开发者开发和提供服务的App，它通知用户公交路线图和预计到达时间等信息。该App于2012年开始提供服务，其后开发者于2018年停止了开发和更新，但并未撤销该App的证书签名信息。之后，攻击者获取到了证书、代码以及开发者上传到Google Play Store的ID和密码，并在App中添加恶意代码后，再次上传到了Google Play Store。



【图2】正常样本与添加恶意代码的样本比较

此外，包含恶意代码的 App 通过正常的更新流程，窃取了个人用户的谷歌ID和密码。Gwangju Bus 开发者开发的另一个 App 也被添加了相同类型的恶意代码并上传至 Google Play Store 。

※ ***恶意行为总结：该恶意代码添加了 libAudio.3.0.so 原生库文件，其后该库下载了附加库 libMovie.so 文件，从而窃取谷歌ID等关键信息。***

2.NHN证书泄露

2022 年 8 月，在收集使用 NHN 证书签名的金融 App 时，确认了此案例。经证实，NHN 证书用作避免被安全解决方案检测为恶意代码的手段，而不是针对 NHN 开发的 App 进行攻击。对于一些基于安卓白名单的安全方案，提取验证相对简单的签名信息，如果签名信息是注册到官方市场的，则可以将其视为正常 App 进行处理。此时，该 App 的恶意行可能会在未经检查的情况下被视为“白名单”。

※ ***恶意行为总结：该恶意代码是现有的金融类语音钓鱼 App，又名 kaishi 恶意代码。它是一个 “下载器（Downloader）” App，可以篡改来电和去电号码，并下载和强制安装该恶意样本。***

3.智能手机制造商固件（Firmware）证书泄露

2022年11月12日，谷歌通过 Google APVI Report 披露了部分安卓原始设备制造商的平台证书发生了泄露。作为参考，APVI是“安卓合作伙伴漏洞倡议计划（Android Partner Vulnerability Initiative）”的简称，最初旨在发现和响应谷歌合作伙伴公司设备中的漏洞。

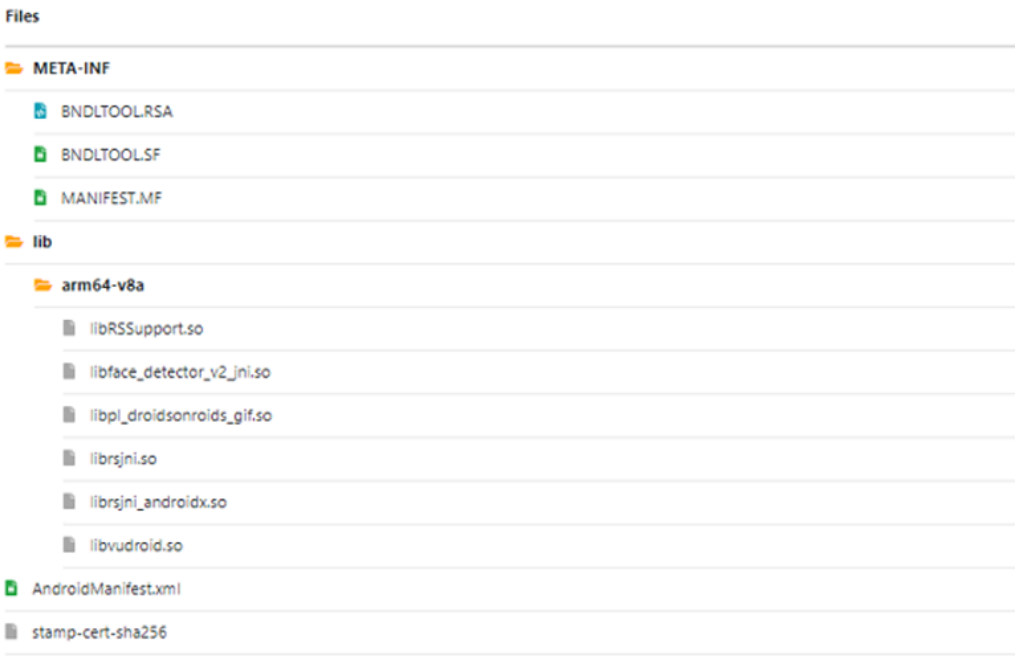
平台证书（Platform Certificate）是一种 App 签名证书，主要用于对系统映像上的安卓 App 进行签名。使用该证书签名的 App 可以通过将“sharedUserId”指定为“android.uid.system”来获取系统权限。换句话说，当使用制造商证书签名的恶意 App 被安装到相应制造商的手机上时，它会被授予可访问用户数据（user data）区域的权限以及系统权限。也就是可以使用与实际操作系统相同的访问权限运行。

被发现的恶意 App 是由谷歌认证的固件证书签名，它只在制造商的智能手机上执行恶意行为，从这一角度来看它与现有恶意 App 不同，可以被视为一种独特的攻击类型。

※ ***恶意行为总结：当运行恶意 App 时，它会获取系统权限，并将用户个人信息、通话内容，在通话时录音记录等信息发送给攻击者。***

4.攻击者蓄意试图创建“白名单”证书

2021年12月7日，通过对发布在 Google Play Store 的一个 App 进行样本分析发现。该 App 在 Google Play Store 注册为比特币相关的应用程序。它的特点是只有简单的包（package）名称和签名信息，没有 dex 文件或其他可执行代码。它被识别为无法安装的文件，因为 App 内部没有 dex 文件。



【图3】App 结构

该 App 通过了谷歌审核后成功上传到商城。直到2022年2月16日，仅通过定期更改版本代码来进行更新。更新时使用的签名信息从2022年12月5日开始用于签名 kaishi 恶意代码。

蓄意上传到 Google Play Store 似乎是为了绕过基于白名单的安全解决方案。据推测，在通过 Google Play Store 提供定期更新并将证书暴露足够长的时间以诱导信任后，它被用于签名恶意代码。

AhnLab 响应情况

AhnLab 具备了同时使用基于允许的“白名单（Whitelist）”和基于阻止的“黑名单（Blacklist）”的系统。详细来说，AhnLab 将确定为正常的 App 列入白名单进行管理，而恶意样本会收集功能特征并将其列入黑名单进行管理。当由于黑名单而在白样本中检测到恶意行为时，分析人员会立即分析样本是否含有恶意并采取相应措施。

基于此系统，我们对本文中介绍的案例进行了响应，内容如下。

案例 1. 上传到 Google Play Store 的带有恶意功能的 App

该样本为正常上传到当前 Google Play Store 的 App ，AhnLab 曾将其列入白样本进行管理。然而，随着 libAudio.3.0.so 文件被检测为“下载器”，分析人员分析了样本并确定该证书已被泄露后，将其归类为恶意文件。

案例 2.NHN 证书泄露

该样本一经收集，即被识别为典型的 kaishi 恶意代码，并立即将信息分享给NHN后，归类为恶意功能样本。目前我们还在持续收集使用该签名信息签名的 App，并进一步分析并将其归类为恶意应用。

案例 3.智能手机制造商固件（Firmware）证书泄露

首先，LG虽然不再生产终端，但目前仍有使用该证书进行签名的 App，因此只将“包含恶意功能”的 App 归类为恶意应用。三星、联想、联发科（MediaTek）过去撤销了该证书，经确认不会影响到最新设备，该 App 已经归类为恶意应用。

结论

由于安卓操作系统和商店的性质，App 开发和上传极为自由。然而，这并不意味着管理 App 的负担减轻。机构不介入认证和管理，意味着开发者需要全权负责 App 的维护和安全管理。

对此，需要采取如下改进措施。

1. 提高对证书管理和系统的认识

不应忘记，App 开发者拥有和管理证书与他们到目前为止与用户建立的信任权重成正比。如前所述，没有独立认证机构意味着必须对管理给予特别关注。同样，与具有独立认证机构的其他证书相比，App 签名证书需要具备更高级别的管理。此外，必须制定可以系统地执行管理的方案。

2. 建立安全解决方案改进体系

如果安全解决方案轻易信任个人和企业开发者的证书，那么响应现有威胁的能力就会受到限制。认识到这一事实，有必要通过使用基于功能对恶意样本进行分类的技术来防止恶意行为。

AhnLab

安全月刊

https:// cn. AhnLab .com

https://global. AhnLab .com

https://www. AhnLab .com

关于AhnLab

Ahnlab的尖端技术和服务不断满足当今世界日新月异的安全需求，
确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。
我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、
移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。
AhnLab已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室
电话：+86 10 8260 0932（北京） / +86 21 6095 6780（上海） | cn.sales@ AhnLab .com