Ostorlab

2026 移动银行应用安全报告

64 个国家和地区前 500 家银行的 2,686 款银行应用在 Android、iOS 和 HarmonyOS 上包含哪些内容，以及这对欺诈防范意味着什么。

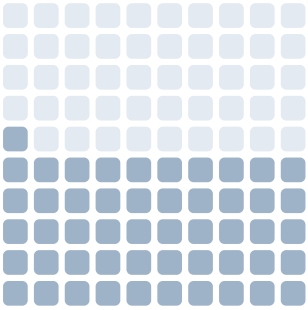


核心发现

独立数字银行的高危及以上发现项最多。

数字银行应用的扫描结果被评为高危或严重的比例高于传统银行应用，分别为 61.1% 和 51.2%，而差距完全来自独立数字银行。传统银行旗下的数字银行与其母行表现相近。

51.2%

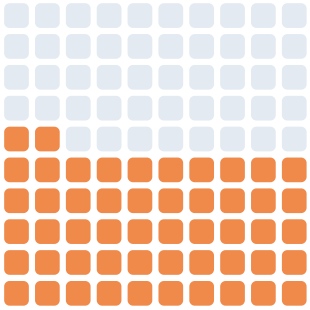


传统银行

商业银行、零售银行和公司银行

2,596 款应用

52.5%

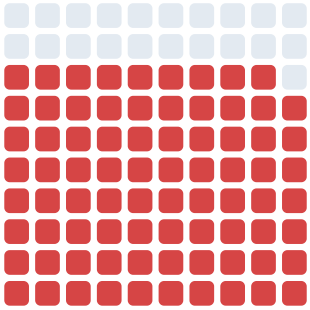


银行旗下数字银行

传统银行的数字化品牌

61 款应用

79.3%



独立数字银行

无传统银行背景的纯数字银行

29 款应用

差距从何而来

OAuth 账户接管，评级为高危或严重

6.1%
24.1%

不安全的序列化，评级为高危或严重

6.4%
17.2%

Google API 密钥以外的内嵌凭据

19.8%
48.3%

但它们在现代防御措施上领先

已集成通行密钥 API

4.6%
37.9%

应用或设备证明

19.9%
48.3%

与密钥绑定的生物识别

74.0%
100.0%

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

目录

2,686 款应用，十一个章节。

每一行均链接至对应页面。

核心发现：独立数字银行 02
摘要 04
九个数字读懂本报告 05

01 研究方法 06
覆盖各地区的2,686 款应用 07
三类证据，每个数字遵循五条规则 08

02 银行应用如何构建 09
混合 Web 应用风险最高 10
一个平台，众多银行 11
更新频繁，却仍支持旧手机 12
每6 至9 周发布一个新版本 13

03 应用内含什么 14
分析 SDK 无处不在，反欺诈 SDK 寥寥无几 15
AI 银行尚未进入应用 16

04 扫描发现 17
半数应用存在高危及以上发现项 18
代码与隐私类发现项波及多数应用 19
五分之一的应用内嵌了本应保密的凭据 20
四成应用含有已知漏洞 21
各平台的问题各不相同 22

05 身份认证与支付 23
通行密钥代码已内置，通行密钥却未上线 24
银行网站是否声明了其应用？ 25
生物识别多与密钥绑定，但三分之一可被绕过 26

06 运行时防护：应用内置了什么 27
代码中发现的防护措施 28
许多检测由 SDK 提供 29
很少有应用实施多层防御 30

07 应用之外 31
银行域名：已具备抗量子能力，却难以报告漏洞 32
与应用不符的隐私标签 33
部分银行服务器开放了 Web 以外的服务 34
六分之一的银行有公开的数据泄露记录 35
银行须遵守的规则及其自我声明 36

08 威胁态势 37
四成银行上了木马目标名单 38
2026 年：攻击者让银行自己的应用为其所用 39
银行能否察觉其应用已被调包？ 40
资金流向何处 41

09 按地区、银行类型和国家 42
没有哪个地区面面俱到 43
各国结果 44
各地区最安全的银行应用 45

10 案例研究 46
CyberDakait：七种木马，一通电话 47
WindRelay：用受害者自己的应用办理贷款 48
Hirudo：替换银行应用的木马 49
在仿冒副本中，每项检测都可被伪造 50
变成 AI 凭据的 Google API 密钥 51

11 下一步行动 52
2026 年银行应采取的10 项首要行动 52

A 定义与数据说明 53

能够阻止现代欺诈的控制措施依然少见。

今年，我们分析了 64 个国家和地区前 500 家银行的 2,686 款移动银行应用。银行更新频繁，大多数应用具备基本防护。但应对当今攻击真正关键的防护措施，如通行密钥、应用证明和运行时防护，仍只出现在少数应用中。

半数应用存在高危及以上发现项

51.5% 的应用在我们的自动化扫描中至少有一个高危或严重发现项，仅 11.8% 的应用没有低危以上的发现项。最常见的原因是应用中内嵌的凭据（Google API 密钥以外的占 20.3%）以及含有已知漏洞的组件（41.1%）。

强身份认证仍处于起步阶段

仅 4.9% 的应用集成了通行密钥 API，20.2% 使用了应用或设备证明。在 Android 上，35.1% 的应用存在可被我们的扫描器绕过的生物识别流程，尽管多数绑定生物识别的应用都将其与密钥绑定。

攻击者如今直接针对应用本身

前 500 家银行中，有 192 家银行的应用出现在公开的银行木马目标名单上。2026 年，Hirudo 和 Gigabud 等攻击活动更进一步，在受害者手机上替换或克隆正版银行应用。在英国，2025 年授权推送支付诈骗损失中有 52% 经由移动银行发生。

防护措施零散常见，完整体系罕见

在 Android 上，69.9% 的应用会检测 root，但仅 26.9% 内置了商业或平台级防护产品。我们的数据反映的是应用包含哪些内容，而非其实际防护效果；后者需要真机测试。

扫描得出的三项发现

51.5%



的应用至少有一个高危或严重发现项

2,686 款应用中的 1,384 款

35.1%



的 Android 应用存在可被我们的扫描器绕过的生物识别流程

Android 应用

4.9%



的应用集成了通行密钥 API，这一控制措施可使被钓鱼窃取的密码失去作用

九个数字读懂本报告。

组件 01

41.1%

的应用含有存在已知漏洞的组件

2,686 款应用中的 1,103 款

第 04 章 · 第 17 页 →

密钥 02

20.3%

的应用内嵌了 API 密钥、访问令牌或私钥等机密信息

2,686 款应用中的 544 款；不含 Google API 密钥

第 04 章 · 第 17 页 →

旧手机 03

96%

的应用可安装在已不再获得安全补丁的系统版本上

Android 99% · HarmonyOS 100% · iOS 72%

第 02 章 · 第 12 页 →

应用证明 04

20.2%

的应用使用了应用或设备证明

2,602 款代码可读的应用中的 525 款

第 05 章 · 第 23 页 →

运行时防护 05

26.9%

的 Android 应用内置了运行时防护产品

商业或平台级产品，Android 应用

第 06 章 · 第 27 页 →

AI 06

2 款应用

引用了大语言模型 API；没有应用内置 LLM SDK，而 28.3% 使用了端侧 ML

共 2,686 款应用；条码、文字和人脸模型居多

第 03 章 · 第 14 页 →

木马 07

38%

的银行有应用出现在公开的银行木马目标名单上

前 500 家银行中的 192 家；名单大多发布于 2021 至 2023 年

第 08 章 · 第 37 页 →

后量子 08

71%

的可访问银行 Web 主机协商使用后量子 TLS

1,038 次完成的握手中的 732 次

第 07 章 · 第 31 页 →

诈骗损失 09

52%

的英国 2025 年诈骗损失经由移动银行发生

授权推送支付诈骗损失 576.4 百万英镑中的 301.8 百万英镑（UK Finance）

第 08 章 · 第 37 页 →

第 01 章

01

研究方法

我们下载了 64 个国家和地区前 500 家银行的 2,686 款银行应用，并在 Android、iOS 和 HarmonyOS 上逐一通过 Ostorlab 的自动化安全分析。



图示：按国家和地区划分的样本。

2,686

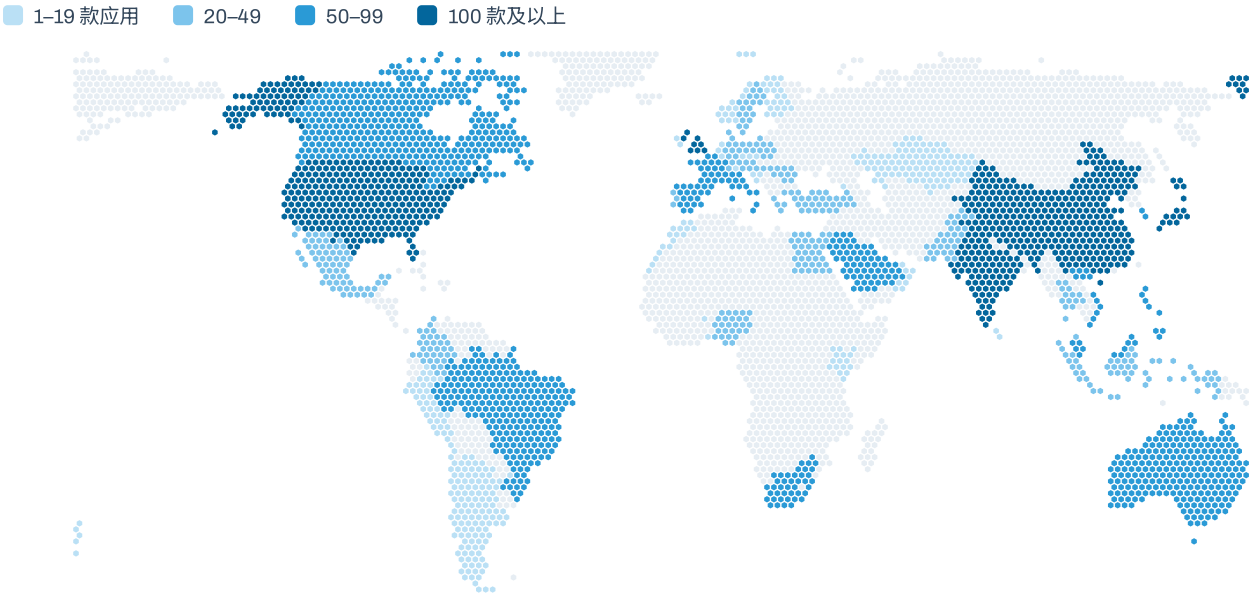
款应用，来自 64 个国家和地区的前 500 家银行

覆盖各地区的 2,686 款应用。

样本涵盖前 500 家银行的 2,686 款应用，其中包括 29 家全球系统重要性银行，覆盖 Android、iOS 和 HarmonyOS。

银行来自 64 个国家和地区，遍及各大洲

图 1.1

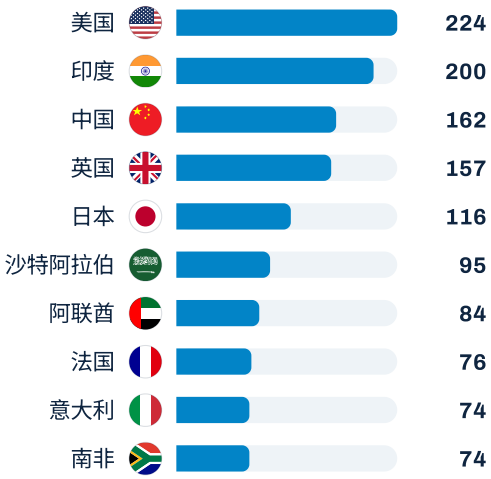


按银行本国市场统计的各国分析应用数量。共收集 2,841 个应用商店条目，其中 155 个无法下载。

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

十大市场

图 1.2

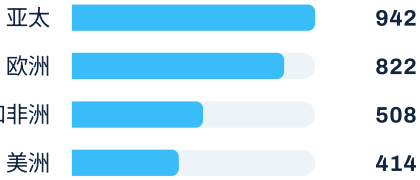


应用数量，按银行所在国家统计。

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

亚太是最大的地区

图 1.3



应用数量，按银行所在地区统计。

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

三类证据，每个数字遵循五条规则。

本报告中的每项数据均来自 Ostorlab 对应用的分析，且每个数字都遵循相同的五条规则，确保图表、正文和图注一致。

应用清单

列出每款应用的构建要素：框架、SDK、权限、防护措施及其通信的主机。覆盖全部 2,686 款应用。

自动化安全扫描

Ostorlab 的扫描器规则发现漏洞、评定其严重程度，并将其映射到 OWASP MASVS。规则因平台而异。覆盖全部 2,686 款应用。

控制信号

十六项针对身份认证、支付和隐私控制的检查，每项均附有触发它的代码证据。覆盖全部 2,686 款应用。

如何解读每个数字

01 每个占比都注明分母

每个百分比都在图表下方的图注中注明其统计所依据的应用范围。

02 平台专属规则只在本平台统计

仅存在于 Android 的规则按其在 Android 应用中的占比报告，绝不按全部应用计算。

03 未知项计数，不做推测

加壳或无法读取的代码不计入相应检查的分母，并注明被排除的数量。

04 Google API 密钥单独报告

Google 预期这类密钥会出现在应用中，因此凭据的总体数据不包含它们。

05 不点名任何银行

证据来自真实应用，展示时隐去银行名称，所有机密信息均已遮盖。

解读数字

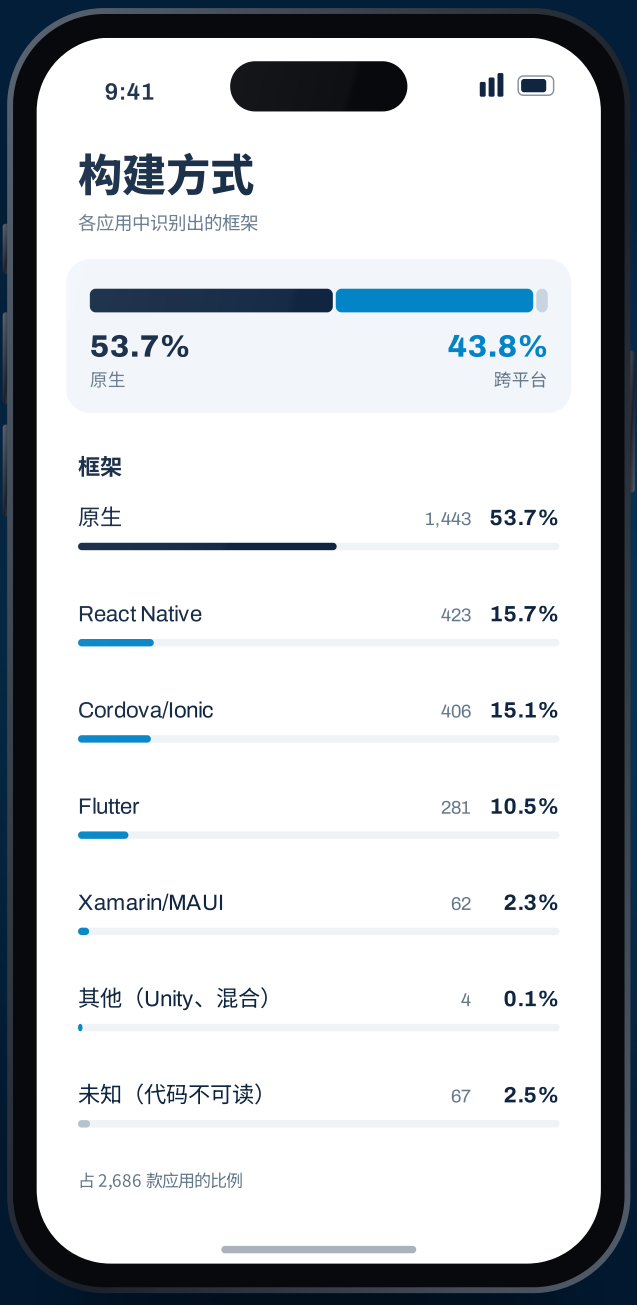
发现项表示我们的扫描器在发布的安装包中匹配到了一条规则。它是问题存在的证据，而非该问题可在生产环境中被利用的证明。严重程度沿用扫描器的评级：严重、高危、中危和低危。扫描器还使用两个更低的评级。“潜在风险”表示某种模式可能是真实漏洞，但需要人工确认，例如形似密钥的字符串。“加固建议”表示缺少某项安全防护。应用按其最严重的严重、高危、中危或低危发现项评级；“潜在风险”和“加固建议”发现项不影响该评级。图表若将其计入，会另行注明。

第 02 章

02

银行应用如何构建

大多数银行仍采用原生开发，但如今四成应用运行在跨平台框架上。这一选择会体现在安全结果中。



图示：各应用中识别出的框架。

43.8%

的应用基于跨平台框架构建

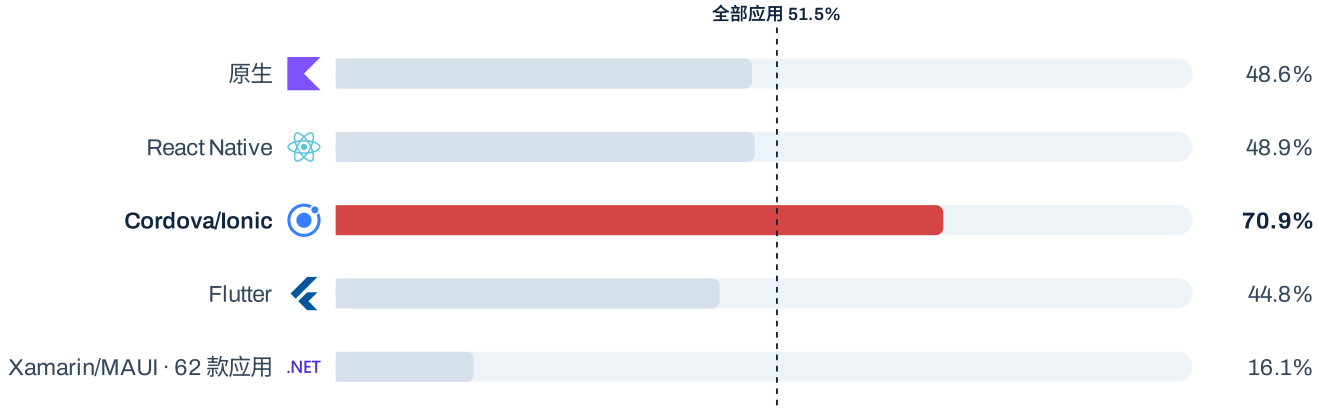
2,686 款应用中的 1,176 款

混合 Web 应用风险最高。

Cordova 和 Ionic 应用将 Web 应用封装在原生外壳中。它们占样本的 15.1%，其中 70.9% 存在高危或严重发现项，而原生应用为 48.6%。

70.9% 的 Cordova 和 Ionic 应用存在高危及以上发现项

图 2.1

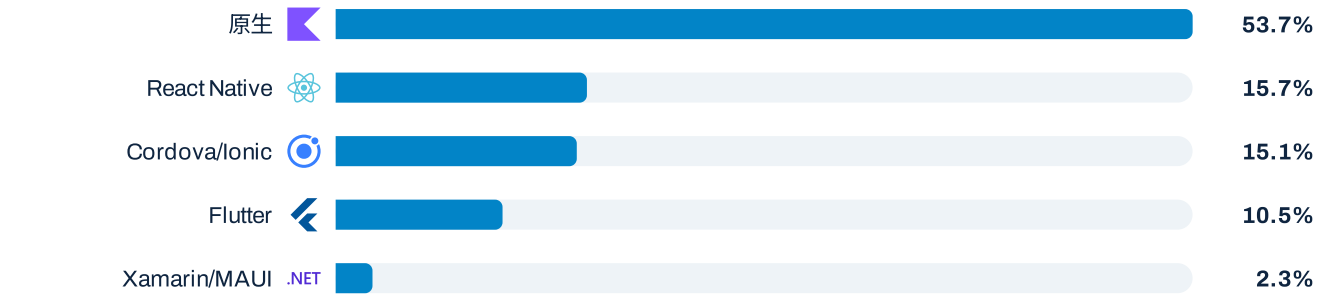


各框架应用中至少有一个高危或严重发现项的占比。虚线：全部 2,686 款应用。

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

大多数银行应用仍采用原生开发

图 2.2



按框架划分的 2,686 款应用占比；67 款代码不可读的应用未显示。

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

Cordova 和 Ionic 应用在存在漏洞的组件方面同样居首（72.2%），主要是打包进 Web 层的过时 JavaScript 库。

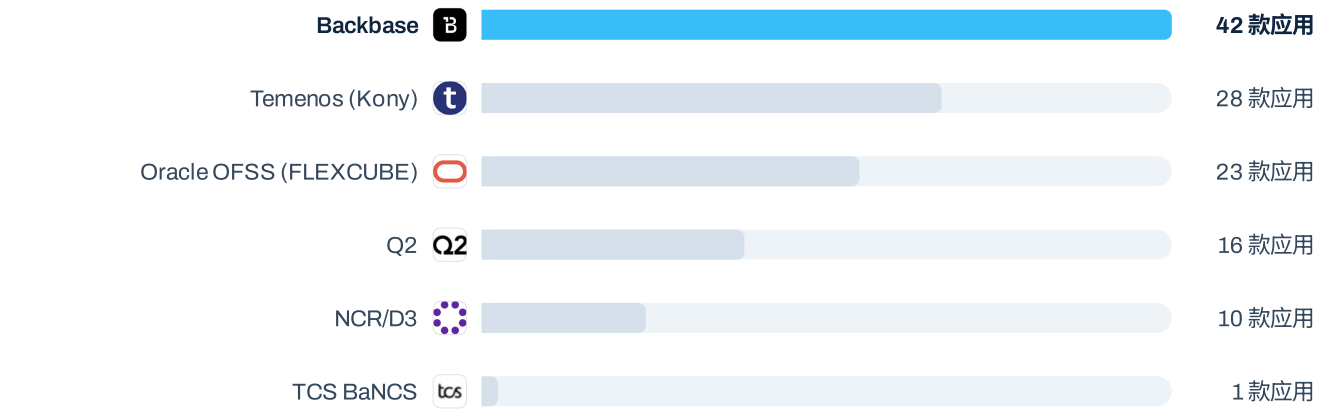
原生（48.6%）、React Native（48.9%）和 Flutter（44.8%）应用之间没有明显差异。Xamarin 和 MAUI 应用表现最好，但样本仅有 62 款，而且它们内嵌凭据的比例最高（43.5%）。

一个平台，众多银行。

许多银行并不从零开发应用，而是授权使用数字银行平台并贴上自有品牌。样本中有 120 款应用带有 6 个此类平台之一的代码特征。

Backbase 是检测到最多的银行平台

图 2.3



应用数量。2,602 款应用中有 120 款匹配已知平台特征。匹配需要可识别的平台代码，因此这些数字是下限。

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

平台一旦共享，其中的一个漏洞就可能波及所有使用它的银行。

为何重要

共享平台代码中的缺陷就是基于它构建的每款应用中的缺陷，而修复取决于供应商的发布，再取决于每家银行的上线。一次漏洞披露就可能同时让许多银行暴露于风险之中。

良好实践

要求平台供应商提供软件物料清单、安全测试结果和约定的补丁修复时限。像关注自身公告一样密切跟踪供应商的安全公告。

更新频繁，却仍支持旧手机。

银行使应用紧跟平台更新：72.1% 的 Android 应用以最新的 Android API 为目标。但在所有平台上，大多数应用仍可安装在已不再获得安全补丁的操作系统版本上。

在所有平台上，大多数应用可安装在未打补丁的系统版本上

图 2.4



各平台中最低系统版本可读的应用占比。若应用声明的最低系统版本早于仍在获得安全补丁的最旧版本（Android 14，iOS 18；HarmonyOS 应用声明的是 Android 版本），则计入。这反映的是应用允许运行的范围，而非客户实际使用的版本。

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

支持旧手机是一项业务选择：客户会继续使用旧手机。风险在于应用运行在存在已知且未修补漏洞的系统上。仅 0.5% 的 Android 应用拒绝未打补丁的版本；在 iOS 上，28.5% 的应用要求 iOS 18 或更高版本。银行可以在登录时检查补丁级别，并在不再获得更新的设备上限制高风险操作。

各应用可安装的最旧版本

图 2.5

Android 和 HarmonyOS · Android 版本

	Android	HarmonyOS
4 及更早	0.8%	4.0%
5	4.4%	12.8%
6	5.3%	7.8%
7	17.4%	24.3%
8	19.5%	19.5%
9	13.1%	13.0%
10	16.5%	12.4%
11	7.0%	3.4%
12	12.8%	2.9%
13	2.7%	0.0%
14 及更新	0.5%	0.0%

iOS · iOS 版本

	iOS
11 及更早	1.8%
12	2.1%
13	5.0%
14	6.5%
15	27.0%
16	23.1%
17	5.9%
18 及更新	28.5%

各平台应用按可安装的最旧版本划分的占比。每根柱条恰好对应该版本；此类应用也可安装在所有更新的版本上。Android 14 和 iOS 18 是仍在获得补丁的最旧版本。

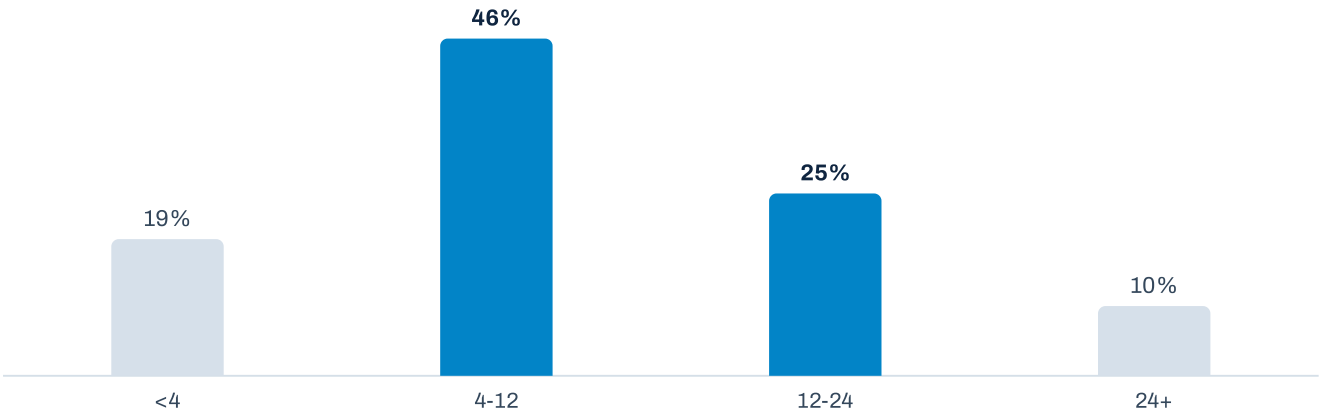
来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

每 6 至 9 周发布一个新版本。

Android 应用的中位数每年至少发布 8.9 个版本（根据 Google Play 评论重建），iOS 应用的中位数为 6.0 个（根据 App Store 版本历史）。HarmonyOS 应用商店仅列出当前版本，因此无法统计 HarmonyOS。频繁发布是一项优势：本报告中的发现项正是借此得到修复并送达客户。

大多数应用每年发布 4 至 24 个版本

图 2.6



可根据 Google Play 评论重建发布历史的 Android 应用，按每年发布次数划分的占比；中位数 8.9，由于无人评论的版本会被遗漏，此为下限。iOS：中位数 6.0，来自 App Store 版本历史。

来源 为本报告收集的 Google Play 和 App Store 商店条目及评论。

75.1%
的 Android 应用（有 Play 更新日期）在过去 90 天内有更新

6.8%
一年以上未更新

38 亿
Android 应用在 Google Play 上的总安装量下限

体积

下载体积中位数为：Android 68 MB，iOS 38 MB，HarmonyOS 129 MB。这些应用中半数原生库来自已知的第三方 SDK，仅 4% 可确认属于银行自身。第三方代码是下一章的主题。

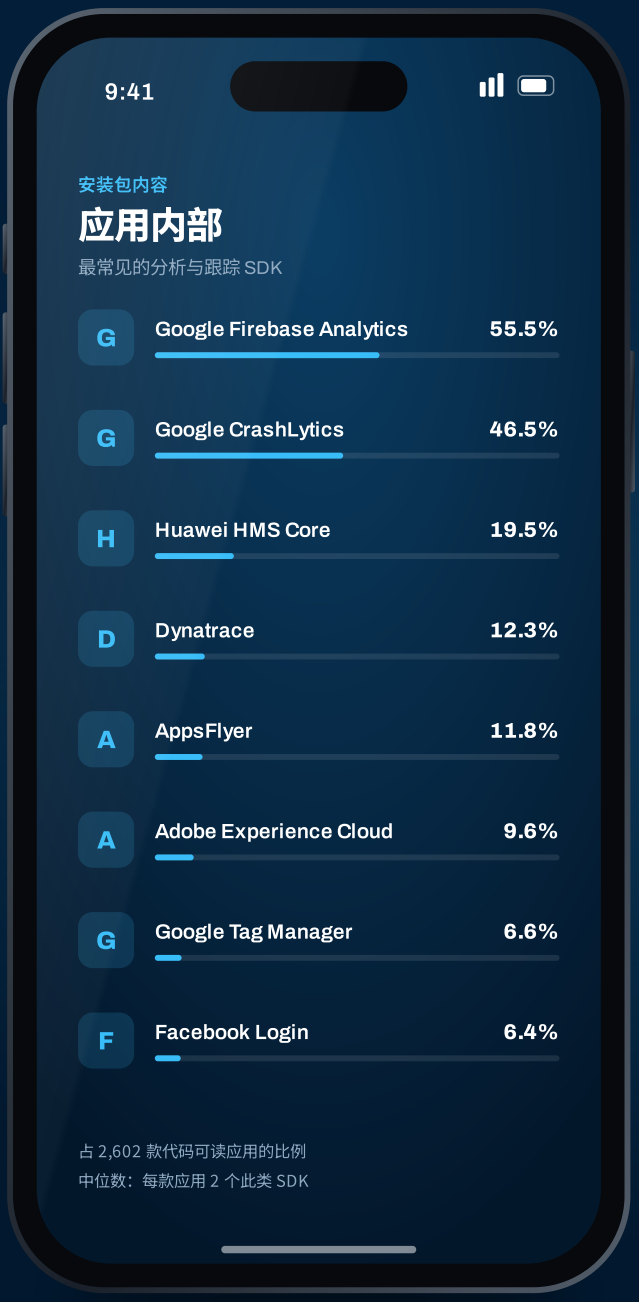
发布频繁，组件陈旧

频繁发布并不能让每个部分都保持最新。如第 4 章所示，41.1% 的应用仍打包了含有已知漏洞的组件。

03

应用内含什么

银行应用的大部分代码出自他人之手：分析、崩溃报告、欺诈检测、地图、扫码。每个 SDK 都带来自己的数据流和自己的漏洞。



图示：最常见的分析与跟踪 SDK。

80.6%

的代码可读应用至少内置了一个分析或跟踪 SDK

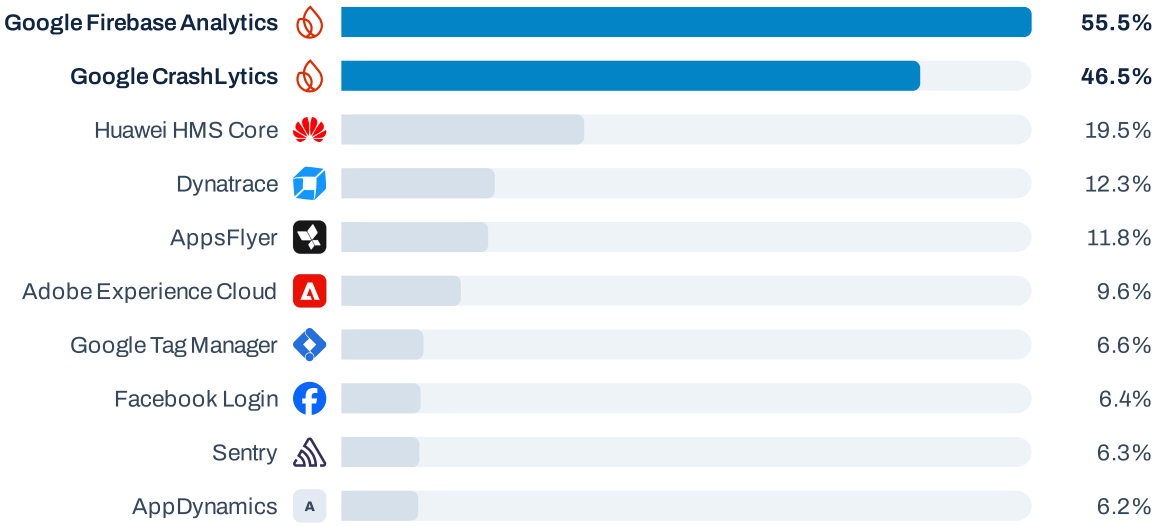
2,602 款应用中的 2,096 款

分析 SDK 无处不在，反欺诈 SDK 寥寥无几。

Google 的 Firebase Analytics 出现在 55.5% 的应用中。银行用于实时识别账户接管的专用欺诈与设备风险 SDK 仅出现在 12.1% 的应用中。

Google 的 Firebase Analytics 和 Crashlytics 在跟踪器中居首

图 3.1

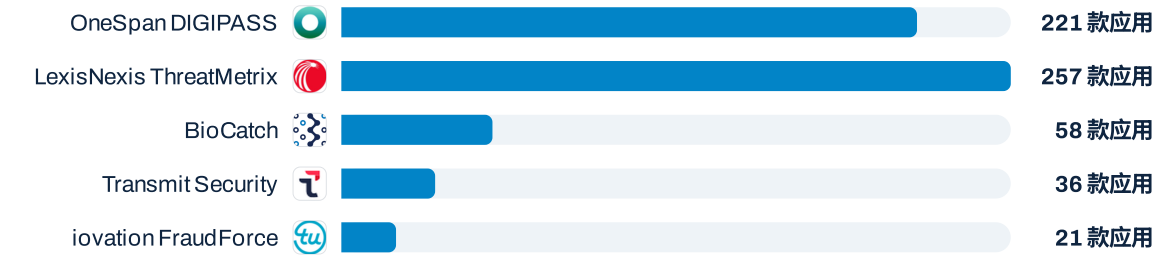


占 2,602 款代码可读应用的比例。跟踪器特征来自 Exodus Privacy 数据库。Huawei HMS Core 出现在 64% 的 HarmonyOS 应用中，涵盖华为推送、定位和分析服务。

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

专业安全 SDK 覆盖的应用很少

图 3.2



应用数量。身份认证 SDK：9.3% 的应用。欺诈与设备风险 SDK：12.1%。

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

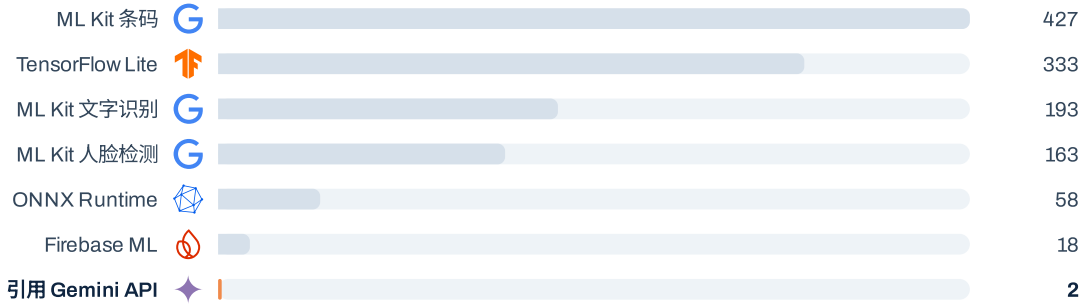
专业 SDK 集中在 iOS 应用中：35.3% 的 iOS 应用内置了欺诈或设备风险 SDK，而 Android 为 8.8%。多家供应商服务于众多银行，因此其安全性的影响远超任何单一应用。

AI 银行尚未进入应用。

28.3% 的应用内置了端侧机器学习，几乎全部用于识别条码、证件和人脸。没有应用内置大语言模型 SDK：2,686 款应用中有 2 款引用了 LLM API，且我们未在任何应用中发现内嵌的 AI 服务商密钥。

端侧 ML 用于识别条码、文字和人脸

图 3.3

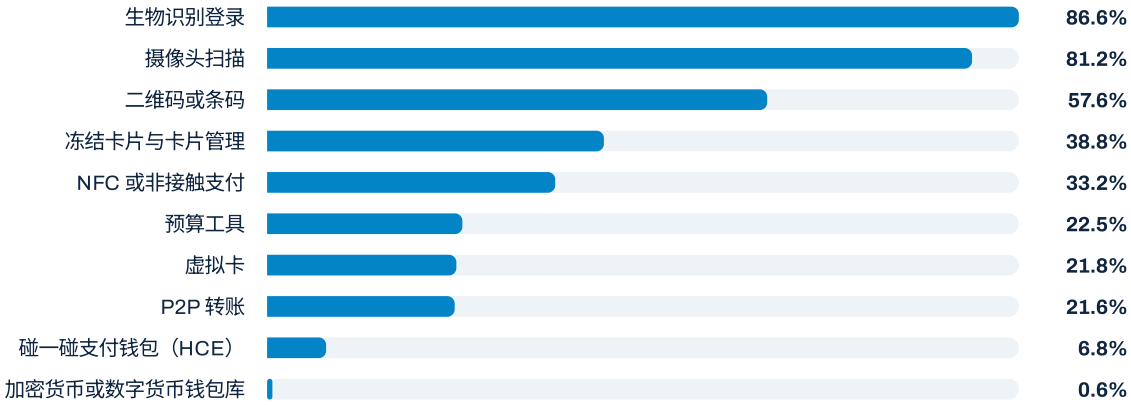


应用数量。引用 Gemini API：应用中出现 Gemini API 端点；没有应用内置 LLM SDK。LLM 功能可能完全运行在银行服务器上，不会体现在应用中。

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

生物识别登录和摄像头扫描几乎普及

图 3.4

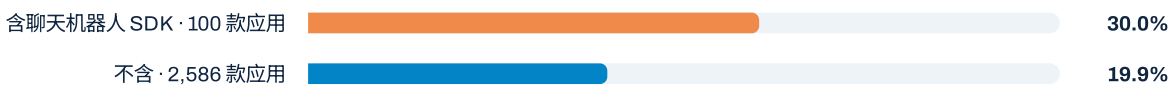


占 2,686 款应用的比例。根据代码、资源和权限检测；代码中存在的功能可能已被关闭。加密货币或数字货币钱包库：应用代码中包含钱包或区块链库即计入；这并不表示该应用提供加密货币交易。

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

内置聊天机器人或虚拟助手 SDK 的应用更常内嵌凭据

图 3.5



至少有一个 Google API 密钥以外内嵌凭据的应用占比。聊天机器人 SDK 指 Dialogflow、Kore.ai、Kasisto 或 Watson Assistant 等供应商的聊天机器人或虚拟助手库，而非大语言模型；仅 2 款应用引用了 Gemini API，且两者均未内置聊天机器人 SDK。规模较大的银行更常部署聊天机器人，也内置更多 SDK：这是相关性，而非因果关系。

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

第 04 章

04

扫描发现

Ostorlab 的自动化扫描在半数应用中发现了至少一个高危或严重问题。内嵌凭据和过时组件居首，其后是各平台特有的问题。



图示：样本中一款真实应用的扫描报告。

18.4%

的应用至少有一个严重发现项

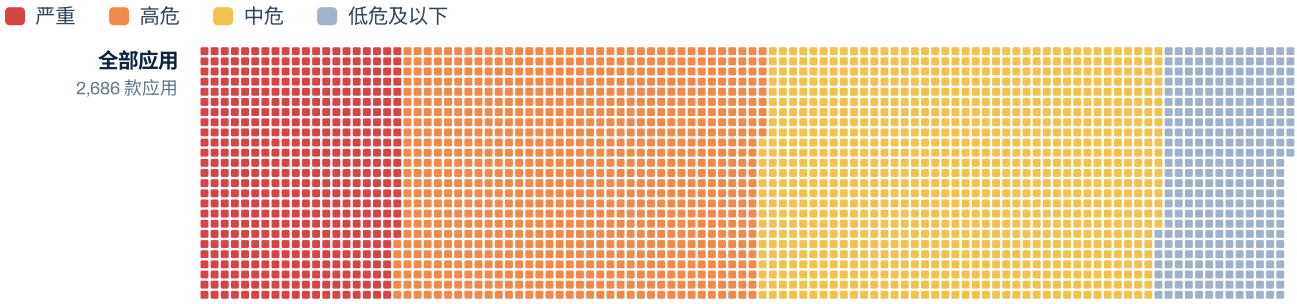
2,686 款应用中的 494 款

半数应用存在高危及以上发现项。

我们按最严重的发现项为每款应用评级。在 Android 上，54.2% 的应用至少有一个高危或严重问题；在 iOS 上为 36.2%。HarmonyOS 应用的严重发现项最多，达 31.6%，主要源于过时组件。

全部 2,686 款应用，按最严重发现项划分

图 4.1

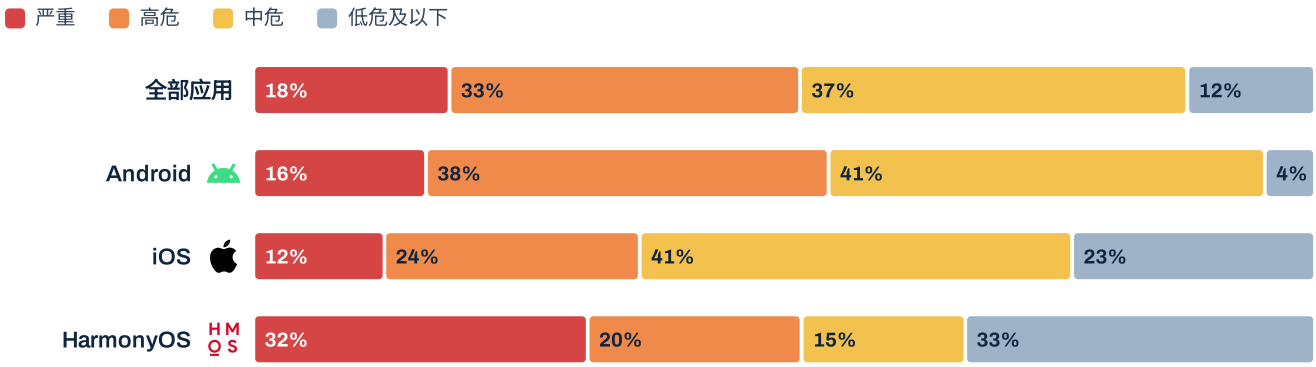


每个方块代表一款应用，按严重程度排序。低危及以下包括最严重发现项为低危、“潜在风险”或“加固建议”的应用，以及没有发现项的应用。

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

HarmonyOS 应用的严重发现项最多

图 4.2



按最严重发现项划分的应用占比。全部 2,686 款应用。低危及以下包括最严重发现项为低危、“潜在风险”或“加固建议”的应用，以及没有发现项的应用。iOS 和 HarmonyOS 上低危及以下的占比较高，部分原因是这些平台的扫描器规则较少。

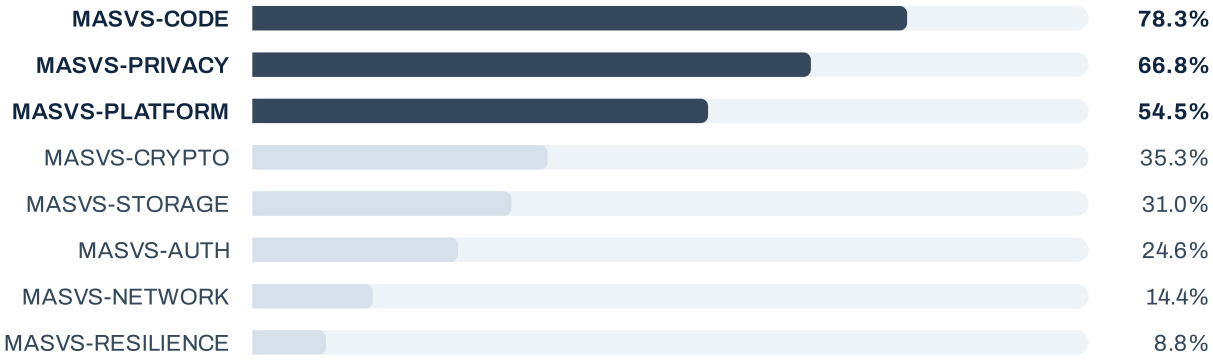
来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

代码与隐私类发现项波及多数应用。

大多数发现项可映射到 OWASP MASVS 的某个控制组，该标准是移动应用安全的行业标准。计入严重、高危、中危和低危发现项时，代码类发现项出现在 78.3% 的应用中，隐私类发现项出现在 66.8% 的应用中。iOS 和 HarmonyOS 应用没有加密或身份认证类发现项，拉低了这两组的数值。

在各 OWASP MASVS 控制组中存在发现项的应用占比

图 4.3



在各组中至少有一个严重、高危、中危或低危发现项的应用占 2,686 款应用的比例。“潜在风险”和“加固建议”发现项不计入。15% 的 Android 发现项未映射到任何组。

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。



样本中一款真实应用的扫描

扫描器报告中的一款应用

766 个发现项，一个评级

样本中的这款 Android 应用有 2 个严重、2 个高危、757 个中危和 5 个低危发现项。与本报告中的所有应用一样，它按最严重的发现项评级：严重。

一条规则可在一款应用中多次触发。中危数量之所以很大，是因为一条序列化规则匹配了数百个调用点；但它仍只是一个需要修复的问题。

扫描器还报告了 98 个“潜在风险”项和 2 个“加固建议”项。“潜在风险”表示某种模式可能是真实漏洞，但需要人工确认；“加固建议”表示缺少某项安全防护。两者均不影响应用的评级。

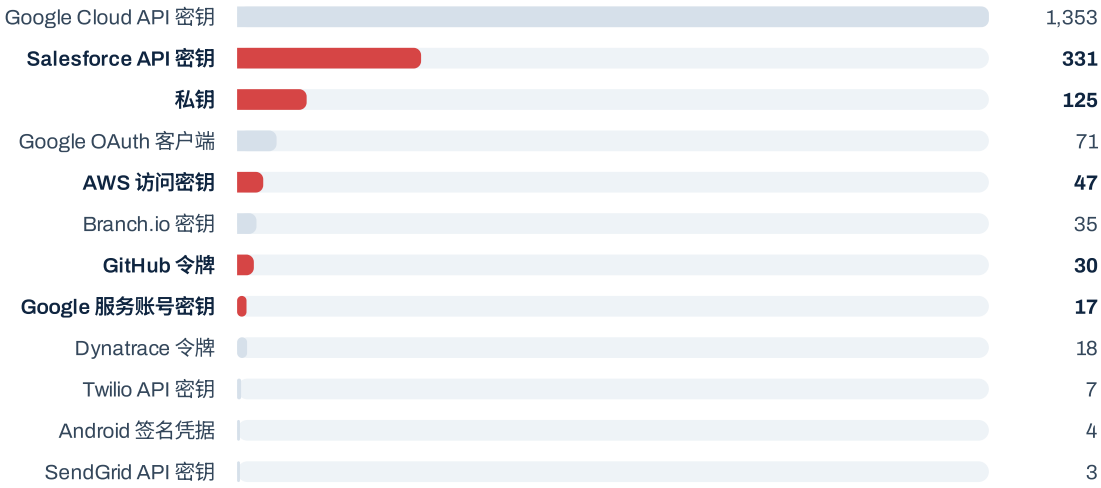
MASVS-AUTH-2 MASVS-CODE-1 MASVS-CODE-3 MASVS-CODE-4
MASVS-NETWORK-1 MASVS-PRIVACY-1 MASVS-PRIVACY-3 MASVS-PRIVACY-4
MASVS-STORAGE-1 MASVS-STORAGE-2

五分之一的应用内嵌了本应保密的凭据。

59.8% 的应用至少包含一个格式可识别的凭据。其中大多数是 Google API 密钥，Google 的设计本就允许其随应用发布：它们用于为 Maps 和 Firebase 等服务标识项目，依靠云项目中设置的限制（应用签名、指定 API）而非保密来保护。我们未测试任何密钥是否受到限制。排除这些密钥后，仍有 20.3% 的应用内置了私钥、云服务密钥和访问令牌（Android 18%，iOS 21%，HarmonyOS 28%）。

除 Google API 密钥外，Salesforce 密钥和私钥居多

图 4.4



扫描器凭据规则标记出各类凭据的应用数量；一款应用可能包含多种。采用另一种方法对整个安装包进行搜索，在 80% 的 Android 应用、71% 的 HarmonyOS 应用和 31% 的 iOS 应用中发现了 Google API 密钥（第 51 页）。

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。



来自样本中一款真实应用的扫描；值已遮盖

任何人都能下载银行应用并读取其中的内容。

一款应用的安装包

这款 Android 应用内置了 4 类疑似机密信息，包括 Google API 密钥、Sentry DSN、Firebase 数据库地址和签名令牌。任何下载该应用的人都能读取它们。

Google API 密钥在应用发布后可能获得新的访问权限：参见第 51 页的案例研究。

良好实践

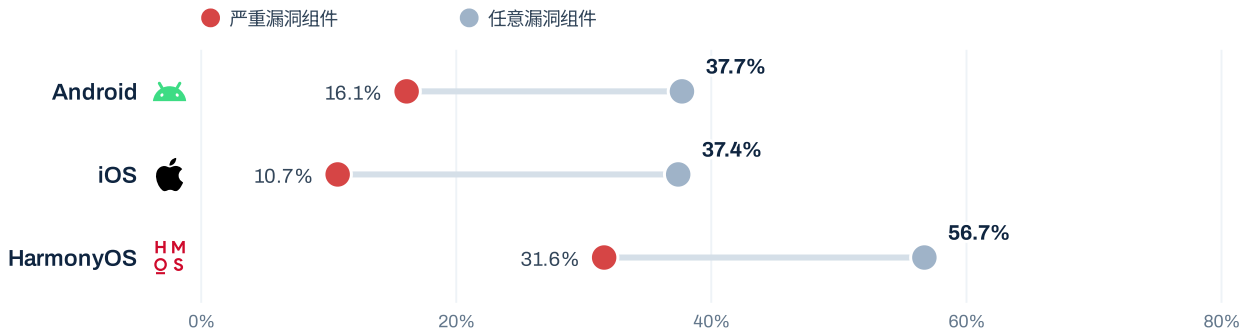
将机密信息保存在服务器上，并向应用签发短期令牌。如果密钥必须随应用发布（如 Google Maps），应将其限制为应用签名和所需的 API，并监控其使用情况。

四成应用含有已知漏洞。

41.1% 的应用包含存在已公开漏洞的第三方组件，18.2% 包含评级为严重的此类组件。HarmonyOS 应用情况最差。

HarmonyOS 应用含有存在漏洞的组件最多

图 4.5

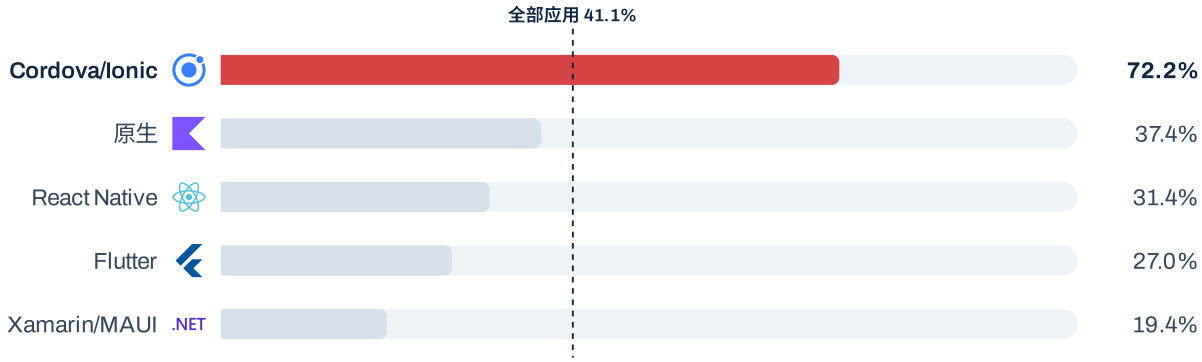


各平台应用占比。标签显示含有任意漏洞组件的占比。

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

72.2% 的 Cordova 和 Ionic 应用含有存在漏洞的组件

图 4.6



各框架应用占比。虚线：全部 2,686 款应用。

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

为何久治不愈

组件会被其他组件引入。银行可以每月更新自己的代码，却仍在一个自己无法控制的 SDK 中带着多年前的旧库。

良好实践

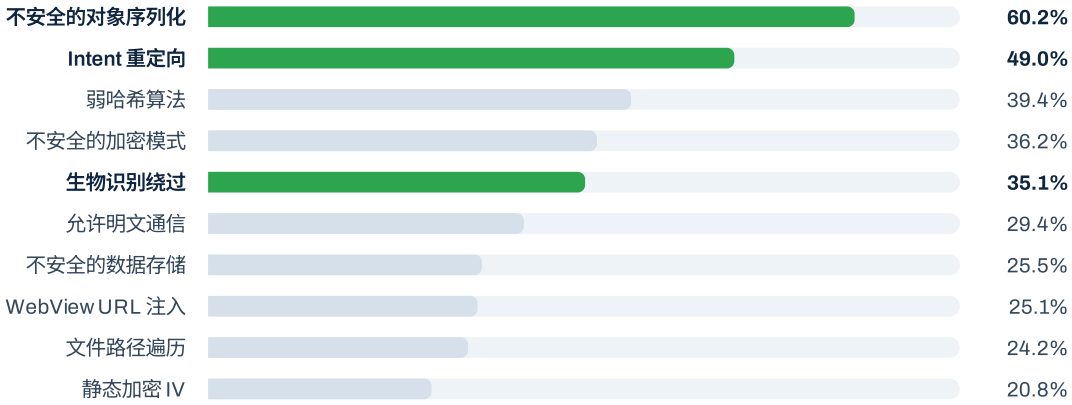
为每个版本维护软件物料清单，据此跟踪安全公告，并为修复严重组件设定期限。对 SDK 供应商提出同样的要求。

各平台的问题各不相同。

许多扫描规则只针对单一平台，因此我们在同一平台内比较应用。在 Android 上，代码层面的问题占主导；在 iOS 上，首要问题是配置；在 HarmonyOS 上，旧组件和 Web 代码问题居首。

Android：序列化和 Intent 重定向居首

图 4.7



Android 应用占比。仅限 Android 的规则。

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

iOS：配置问题居首

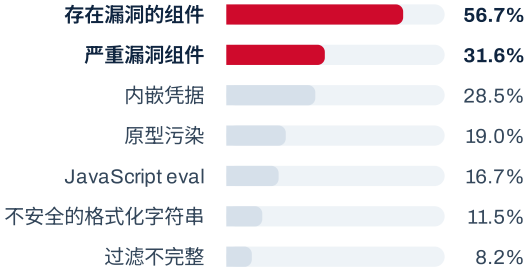
图 4.8



iOS 应用占比。通用链接可防止 OAuth 账户接管，即另一款应用抢占登录重定向。

HarmonyOS：旧组件和 Web 代码居首

图 4.9



HarmonyOS 应用占比。

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

第 05 章

05

身份认证与支付

通行密钥、应用证明和与密钥绑定的生物识别，能让被盗密码和被篡改的应用大大失去用处。它们正在普及，但速度缓慢。



图示：通行密钥提示的示意图，并非真实应用。

4.9%

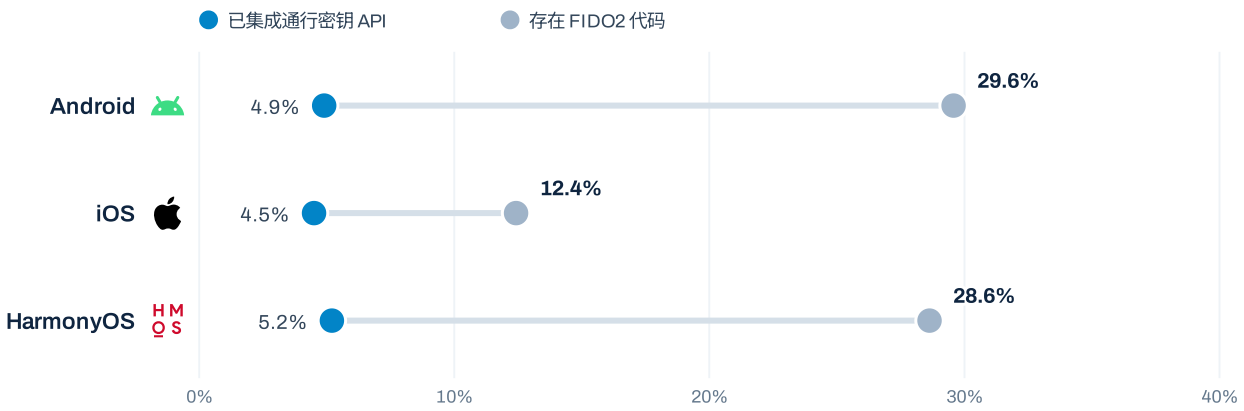
的应用集成了通行密钥 API

通行密钥代码已内置，通行密钥却未上线。

近三分之一的 Android 应用包含 FIDO2 或 WebAuthn 代码，但仅 4.9% 调用了通行密钥 API；iOS 上为 4.5%。代码可能随其他库一同引入，而相应功能并未启用。

FIDO2 代码常见，通行密钥 API 罕见

图 5.1



各平台应用占比。已集成通行密钥 API：应用调用了 Credential Manager、Google FIDO2 API 或 Apple 的通行密钥 API。

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

79.8% 的应用完全未使用证明机制

图 5.2

	强	仅弱	无
Android 强：Play Integrity · 弱：仅 SafetyNet（已弃用）	16.0%	2.8%	81.2%
iOS 强：App Attest · 弱：DeviceCheck，未确认使用 App Attest	3.6%	17.2%	79.2%
HarmonyOS 强：Play Integrity 13.4%，HMS Safety Detect 7.5% · 弱：仅 SafetyNet（已弃用）	20.9%	4.5%	74.5%

各平台代码可读应用的占比。强：银行服务器可以验证应用和设备。仅弱：较旧的或仅针对设备的检查，且没有强证明配合。App Attest 和 DeviceCheck 是 Apple 的服务；Play Integrity 和 SafetyNet 是 Google 的服务；HMS Safety Detect 是华为的服务。

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

证明机制让银行服务器能够核实请求来自正版设备上的正版应用。它是抵御 Hirudo 这类重打包应用的主要防线，但仍有 79.8% 的应用未使用。服务器是否强制校验证明结果，无法从应用中看出。

银行网站是否声明了其应用?

只有当银行网站声明了应用时，通行密钥和应用链接才能生效。我们读取了每家银行公开的关联文件，检查其中是否列出了该应用。

很少有银行网站为保存的登录信息和通行密钥声明其应用

图 5.3



各平台应用中，其银行网站声明该应用可共享已保存登录信息和通行密钥的占比。读取自银行域名下的 apple-app-site-association 和 assetlinks.json 文件。

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

16%

的 iOS 应用所属银行的关联文件中还列出了测试版应用 ID

92

的银行域名（共 226 个有 Apple 关联文件）列出了非生产环境应用 ID

88

的银行域名（共 217 个有 Android asset-links 文件）列出了非生产环境的包



我们的检查所读取的一家银行的文件

一家银行的关联文件

该银行的文件为通用链接声明了其 iOS 应用，因此指向银行网站的链接会打开该应用。但文件未为 Web 凭据声明该应用，因此应用无法提供银行的通行密钥。文件还在生产版应用旁列出了 4 个测试版应用 ID。

属于安全卫生问题，而非漏洞

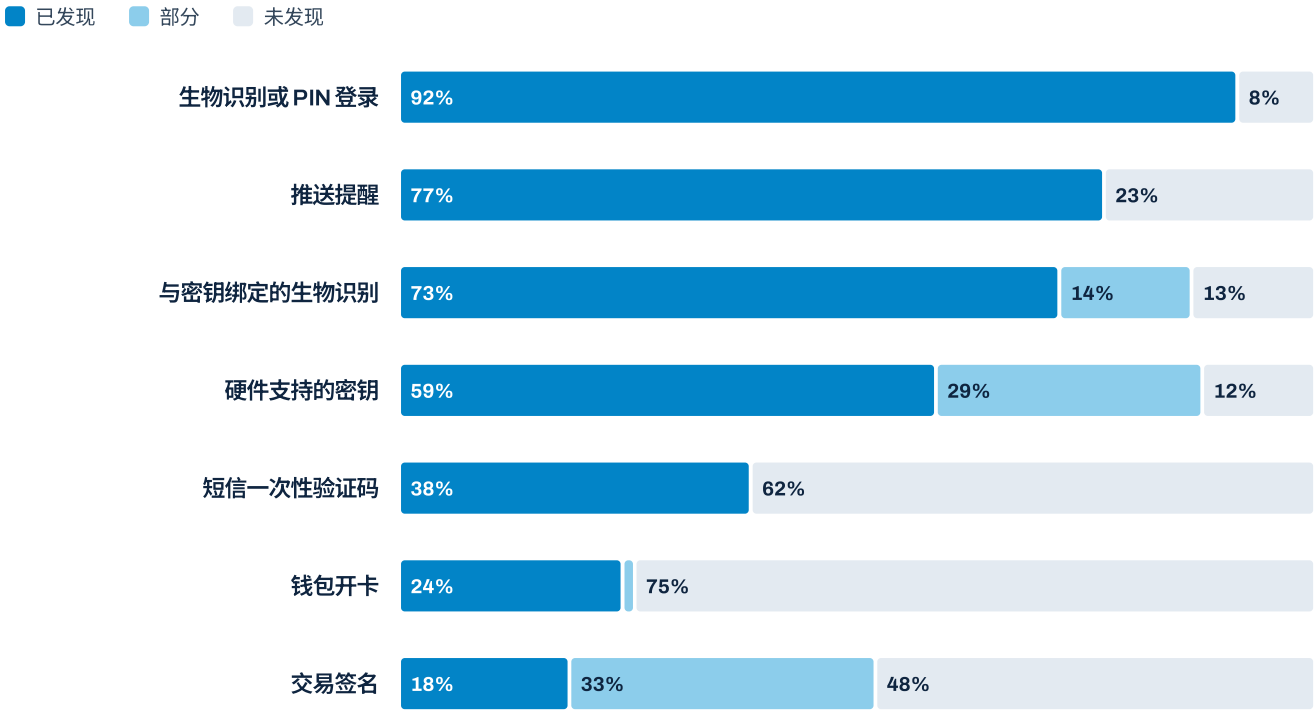
只有银行签名的应用才能使用这些条目。但在生产文件中列出测试版本，等于向任何人透露银行的内部构建标识符，并使链接和凭据在客户本不应运行的版本上继续有效。更大的缺口是缺失的条目：没有它，应用根本无法提供通行密钥。

生物识别多与密钥绑定，但三分之一可被绕过。

在我们能判断 Android 应用如何使用生物识别的情况下，73.2% 将该检查与加密密钥绑定，11.4% 将其视为恶意软件可伪造的“是或否”判断。我们的扫描器还在 35.1% 的 Android 应用中发现了可被绕过的生物识别流程。与此同时，三分之一的 Android 应用和大多数 iOS 应用支持短信一次性验证码，而这正是 SIM 卡调换攻击的目标。

应用如何进行用户登录和支付审批

图 5.4



跨平台 2,686 款应用的占比。已发现：有明确的代码证据。部分：有部分而非全部证据。证明机制和反欺诈 SDK 分别见第 24 页和第 15 页。

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

可被绕过的生物识别

可被绕过的流程可能存在于在其他地方使用了密钥绑定生物识别的应用中。每项敏感操作都应走密钥绑定路径，这样伪造的“是”也解锁不了任何东西。

短信验证码与 SIM 卡调换

在 SIM 卡调换攻击中，欺诈者说服移动运营商将受害者的号码转移到其控制的 SIM 卡上。此后每条短信一次性验证码都会发给攻击者，而不是客户。与设备和交易绑定的验证码不通过短信传输。

第 06 章

06

运行时防护：应用内置了什么

运行时防护可检测已 root 的手机、调试器、Hook 工具和被篡改的应用副本。我们在三个平台上逐一检查了每款应用的代码中是否存在这些防护措施。



图示：已 root 手机上一款受防护应用的示意图。

26.9%

的 Android 应用内置了商业或平台级防护产品

Android 应用

代码中发现的防护措施。

在各平台上，大多数应用至少会检测已 root 或越狱的手机。能检测 Hook 工具、篡改或远程控制的应用要少得多：22.3% 的 Android 应用和 36.2% 的 iOS 应用含有检测屏幕共享或远程控制的代码，而木马正是借此在受害者自己的手机上实施欺诈。

Root 检测常见，Hook 和远程控制检测罕见

图 6.1

	Android	iOS	HarmonyOS
Root 或越狱检测	69.0%	47.2%	67.4%
防截屏	53.9%	45.4%	45.0%
模拟器检测	51.6%	32.6%	49.8%
覆盖层防护	44.1%	不适用	40.0%
重打包检测	43.3%	21.1%	45.2%
调试器检测	35.4%	18.1%	38.5%
证书锁定	34.6%	51.9%	33.3%
Hook 检测	33.7%	28.8%	44.8%
防篡改	29.0%	26.7%	31.4%
远程控制检测	22.3%	36.2%	18.0%

各平台中，由银行自有代码或无法归属的代码调用该检测的应用占比。按 Android 占比排序。不适用：覆盖层防护不适用于 iOS，因为 iOS 上任何应用都无法在其他应用之上绘制界面。

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

存在不等于有效

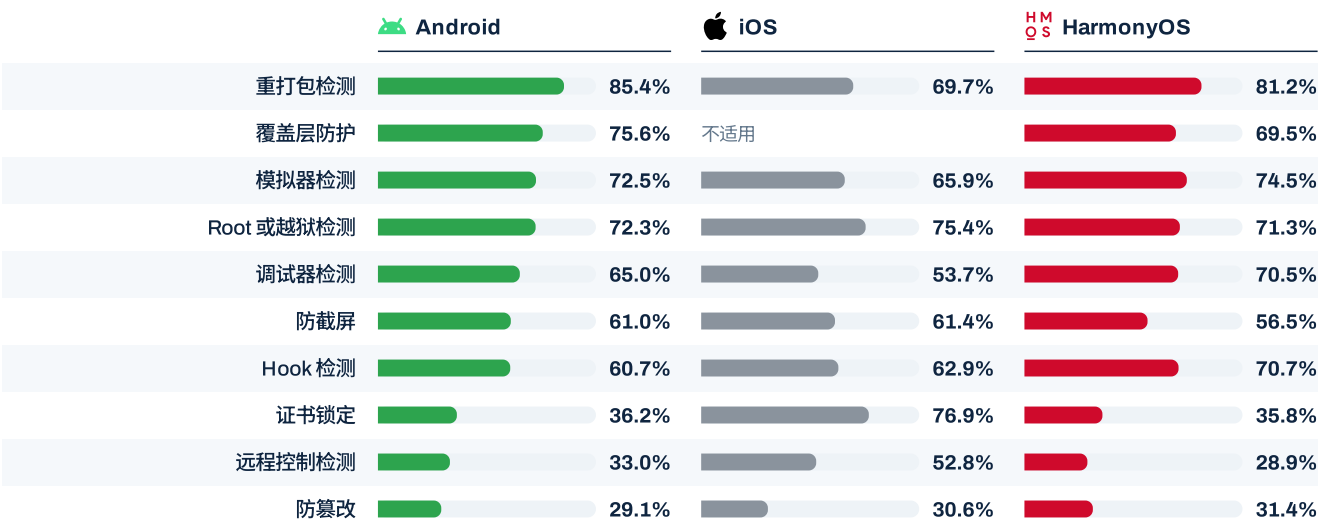
这些结果表明应用中存在某项防护，但不能说明它能否抵御知道其存在的攻击者。检验这一点需要真机测试，计划在后续版本中进行。请将这些数据视为防护水平的上限。

许多检测由 SDK 提供。

若将内置 SDK 中的检测与银行自有代码一并计入，85.4% 的 Android 应用具备重打包检测，但仅 33% 具备远程控制检测，而后者正是抵御远程访问木马最关键的检测。

重打包检测普遍，防篡改检测在各平台都很少见

图 6.2



各平台应用占比。已发现：检测存在于应用中，位于银行自有代码或内置 SDK 中。不适用：覆盖层攻击不适用于 iOS。SDK 中的检测只有在银行启用后才能保护应用。

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

很少有应用实施多层防御。

运行时防护分层部署时效果最佳，这样绕过一项检测不会使其余检测失效。在我们检查的 10 项防护措施中，Android 应用的中位数有 4 项有明确证据；10.7% 的应用有 8 项或更多。

我们检查的 10 项防护措施

01 **Root 检测**
察觉已 root 的手机，此类手机上的应用数据处于暴露状态。

02 **模拟器检测**
察觉应用运行在模拟器中，而非真实手机上。

03 **调试器检测**
察觉运行中的应用附加了调试器。

04 **Hook 检测**
察觉 Frida 等在运行时修改应用的工具。

05 **重打包检测**
察觉由他人签名的应用修改副本。

06 **防篡改**
检查应用自身代码未被修改。

07 **证书锁定**
只接受银行自己的服务器证书。

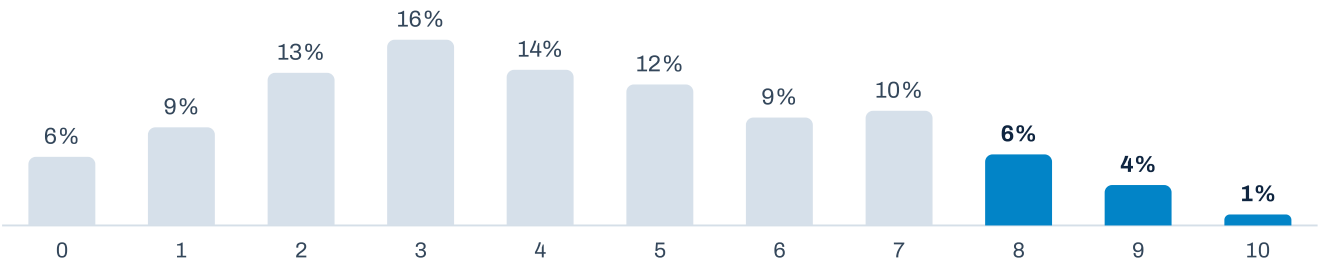
08 **覆盖层防护**
阻止其他应用在银行应用上绘制虚假界面。

09 **防截屏**
阻止对敏感界面截屏和录屏。

10 **远程控制检测**
察觉屏幕共享或远程访问工具。

Android 应用的中位数具备 10 项防护中的 4 项

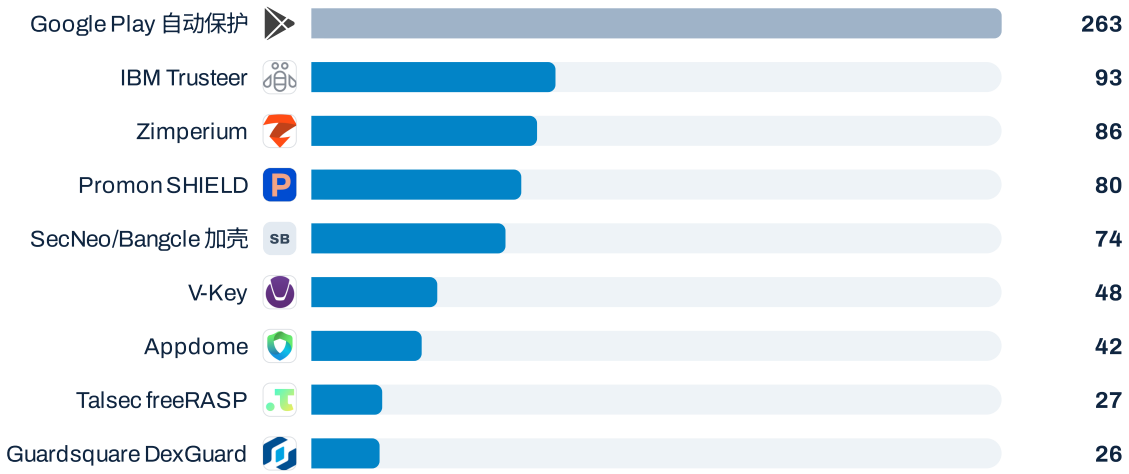
图 6.3



按有明确证据的防护项数（共 10 项）划分的 Android 应用占比。突出显示：8 项或更多。

Google 的 Play 自动保护是最常见的防护

图 6.4



使用各产品的应用数量，覆盖所有平台。Google 的 Play 自动保护（pairip）由应用商店施加，而非在代码中选择。

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

第 07 章

07

应用之外

应用的可信程度取决于其背后的域名、服务器和机构。我们检查了银行的 Web 和邮件域名、应用通信的服务器、隐私标签、公开的数据泄露记录，以及每家银行须遵守的规则。



图示：一个典型的标签，以及我们的扫描最常发现的不一致之处。

67%

的 Android 应用在 Google Play 上的隐私标签与其自身权限或 SDK 相矛盾

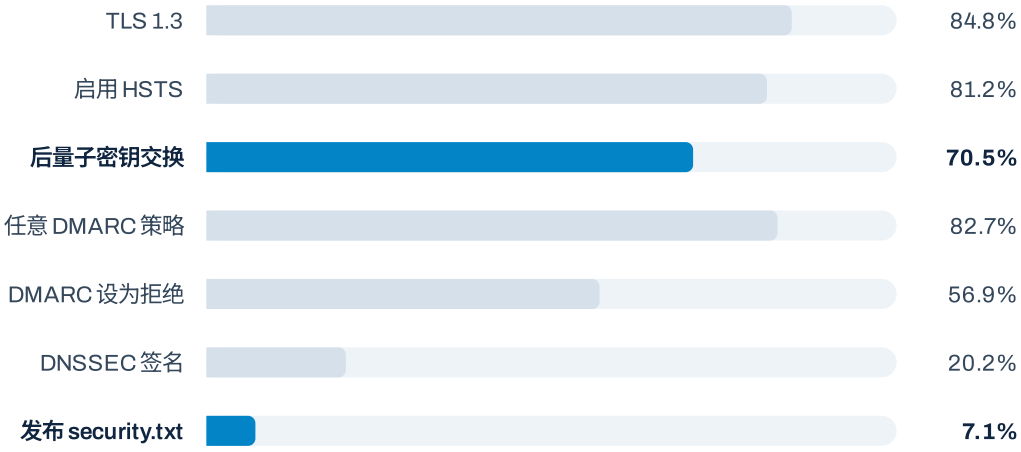
有 Google Play 隐私标签的 Android 应用

银行域名：已具备抗量子能力，却难以报告漏洞。

在我们访问到的银行 Web 主机中，70.5% 已协商使用后量子密钥交换。基础安全卫生却相对滞后：仅 7.1% 的域名发布了 security.txt 文件，告知研究人员在何处报告漏洞。

后量子 TLS 领先于 security.txt

图 7.1

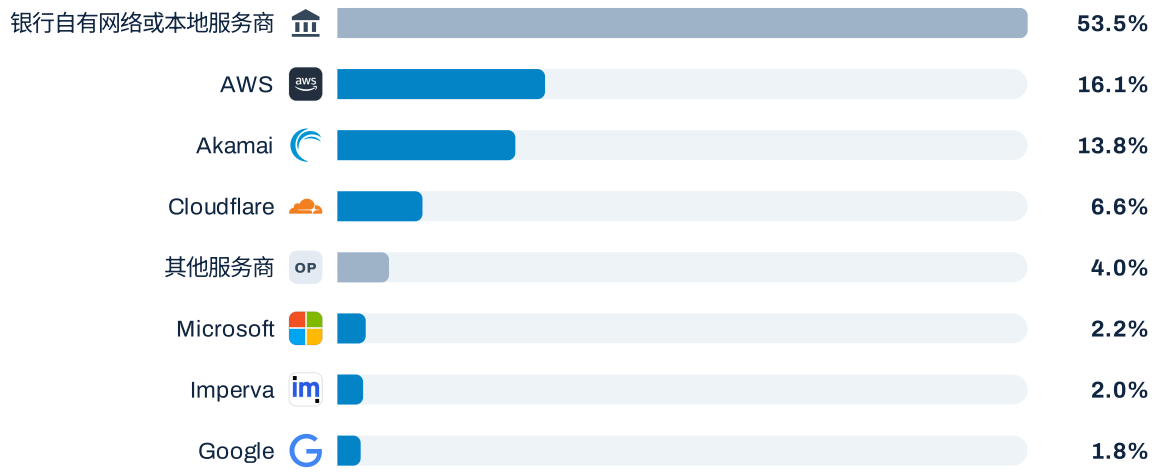


TLS 和 HSTS：占 1,140 个可访问 Web 主机的比例。后量子：1,038 次完成的握手。DNS 检查：1,252 个域名。

来源 Ostorlab 对银行域名的 TLS 握手及公开 DNS 记录。

大多数后端运行在银行自有网络上；云服务商中 AWS 居首

图 7.2



三个平台的应用所引用的 5,101 个银行自有后端 IP 地址的占比，通过公共 DNS 解析。

来源 应用中引用的主机，通过公共 DNS 解析；IP 归属登记数据。

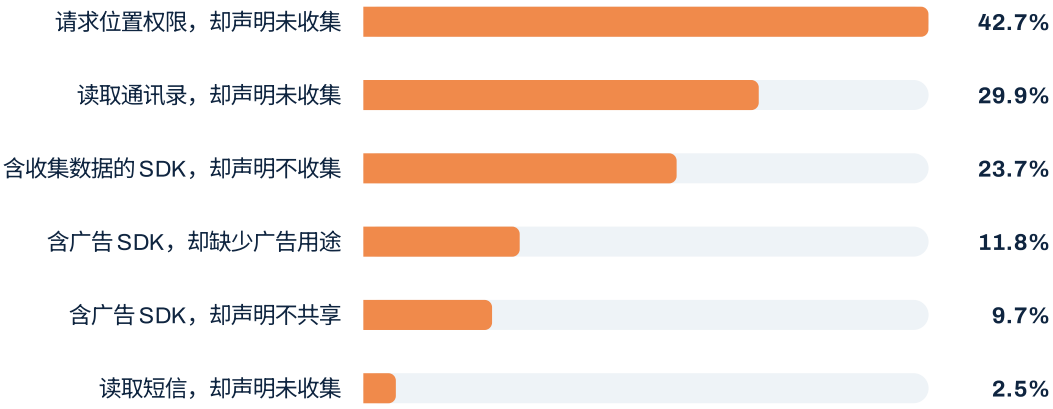
AWS、Akamai、Cloudflare 和 Microsoft 承载了 38.7% 的后端地址。其中任何一家发生中断或数据泄露，都会同时波及许多银行。欧盟 DORA 恰恰要求银行在签约前权衡这一点，包括是否属于“与不易替代的 ICT 第三方服务提供商订立合同”（非官方译文）（条例（EU）2022/2554 第 29 条第 1 款）。

与应用不符的隐私标签。

应用商店要求开发者声明其应用收集哪些数据。在 67% 的 Android 银行应用中，声明与应用自身权限或 SDK 所显示的情况相矛盾。

未声明位置信息是最常见的标签不一致

图 7.3



有 Google Play 数据安全标签的 Android 应用占比。一款应用可能存在多处不一致。

来源 Google Play 数据安全标签，与应用的权限和 SDK 进行比对。

为何重要

清单中的权限并不证明应用实际使用了它，因此部分不一致源于过于保守的清单声明。但监管机构把标签视为承诺。低报数据收集的标签是一项合规风险，也会误导比较应用的客户。

iOS 标签

在有隐私标签的 iOS 银行应用中，19% 声明了用于跨其他公司应用跟踪用户的数据，最常见的是标识符和使用数据。

部分银行服务器开放了 Web 以外的服务。

在应用指向的 5,101 个银行自有服务器地址中，有 4,113 个出现在公开的全网观测数据中。其中 251 个在 Web 和 CDN 流量以外的端口上有响应，涉及 113 家银行；79 个运行的软件版本与已知漏洞相匹配。

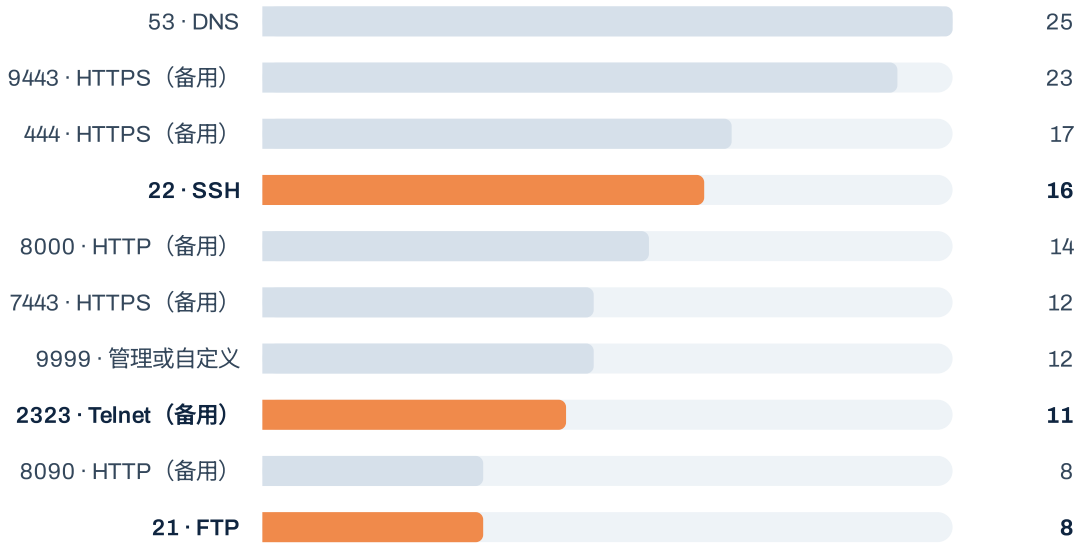
251
个银行 IP 开放了 Web 和 CDN 以外的端口，涉及 113 家银行

79
个银行 IP 根据软件版本推断存在 CVE，涉及 74 家银行

25
个银行 IP 运行着已终止支持的产品

DNS 和备用 HTTPS 端口在额外开放的端口中居首

图 7.4



在 Shodan InternetDB 收录的 4,113 个银行自有 IP 中，在各端口上有响应的 IP 数量。不含端口 80、443 及 CDN 代理端口；151 个在超过 40 个端口上响应的 IP（防火墙和蜜罐的典型特征）不计入。

来源 Shodan InternetDB 被动索引；未向任何银行服务器发送请求。

我们未扫描任何银行服务器

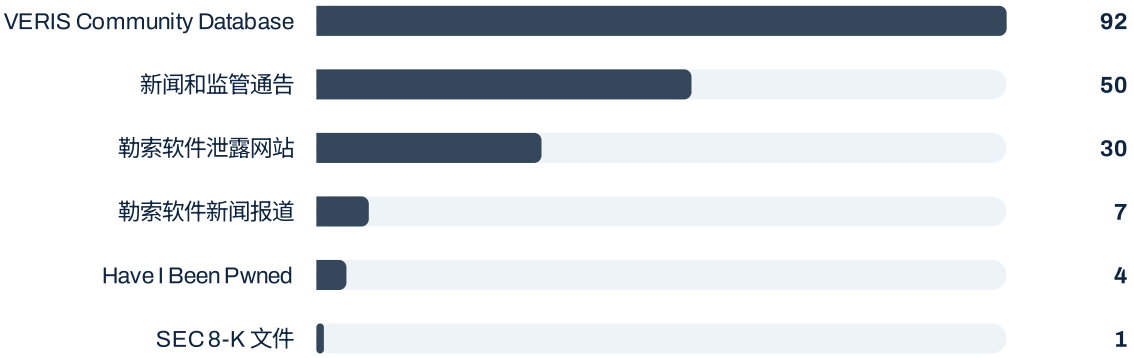
开放端口和软件版本来自公开的全网观测数据（Shodan InternetDB），因此未触及任何银行系统。其余 988 个地址不在该数据中：状态未知，并非已关闭。CVE 是根据观察到的软件版本匹配的，因此每一项都是需由银行确认的线索。

六分之一的银行有公开的数据泄露记录。

通过检索数据泄露数据库、勒索软件泄露网站、监管通告和 SEC 文件，我们发现前 500 家银行中有 83 家（16.6%）至少有一条公开的数据泄露记录，其中 55 家有 2020 年或之后的记录。

大多数数据泄露记录来自 VERIS 数据库

图 7.5



前 500 家银行的记录数量；一家银行可能有多条记录。每条匹配均经人工复核。新闻和监管检查仅覆盖 29 家 G-SIB。

来源 VCDB、Have I Been Pwned、ransomware.live、SEC 8-K 文件、新闻和监管通告。

何为记录

记录指公开报道的事件：一次攻击、内部人员滥用访问权限、导致数据泄露的错误，或勒索软件组织的声称。它并不是关于银行应用的发现项，而且许多记录年代久远：VERIS 数据库可追溯至十多年前。

涉及银行名称的 CVE

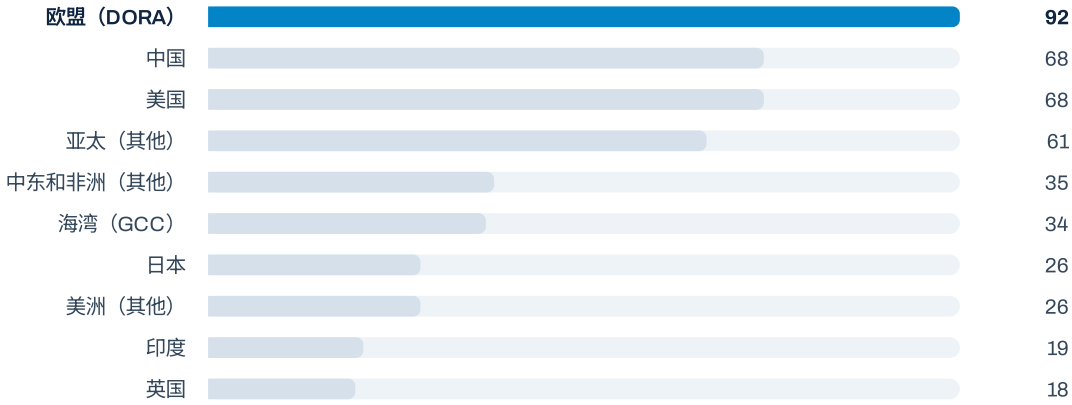
51 条已发布的 CVE 记录与 37 家银行的品牌相匹配，其中 14 条发布于 2025 年之后。大多数描述的是旧版移动应用，且品牌匹配存在误报，因此我们将其视为线索而非发现项。

银行须遵守的规则及其自我声明。

样本中的每家银行都受某一国家或地区的 ICT 风险监管制度约束。前 500 家银行中有 95 家受欧盟《数字运营韧性法案》（DORA）约束，该法案自 2025 年1月起适用，并将第 32 页所述托管服务商等依赖关系列为管理层职责。

欧盟 DORA 覆盖的银行群体最大

图 7.6



前 500 家银行的数量，按其所在国家的监管制度划分。显示十个最大的群组；另有 40 家银行属于较小的群组。

来源 监管机构登记信息及银行所在市场。

332

的前 500 家银行是 Apple Pay 发卡行

44

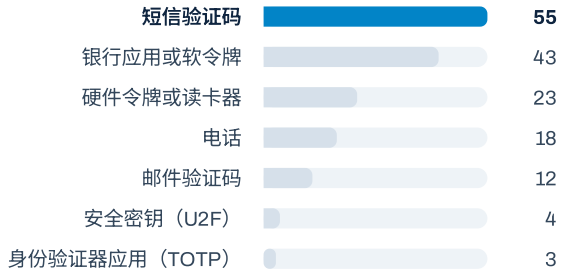
家银行在其网站上声明持有认证，最常见的是 ISO 27001

19

家银行设有公开的漏洞披露计划，其中 5 家设有漏洞赏金

短信是宣传最多的第二因素

图 7.7



网站描述了登录方式的 73 家银行的数量；一家银行可能列出多种。8 家宣传支持通行密钥。

来源 银行网站及 2fa.directory 列表。

声明，而非证书

认证情况依据的是银行网站的声明，而非经核实的证书。62 家银行在至少一个域名上发布了 security.txt 文件，19 家公布了漏洞披露计划。短信仍是宣传最多的第二因素，尽管阿联酋央行等监管机构正在逐步淘汰短信一次性验证码。

第 08 章

08

威胁态势

银行木马会维护其攻击的应用名单。钓鱼工具包仿冒银行的登录页面。过去一年，攻击者还用篡改后的副本替换正版银行应用。



图示：已公开目标名单的格式，应用名称已遮盖。

15%

的已分析 Android 应用出现在至少一份公开的银行木马目标名单上

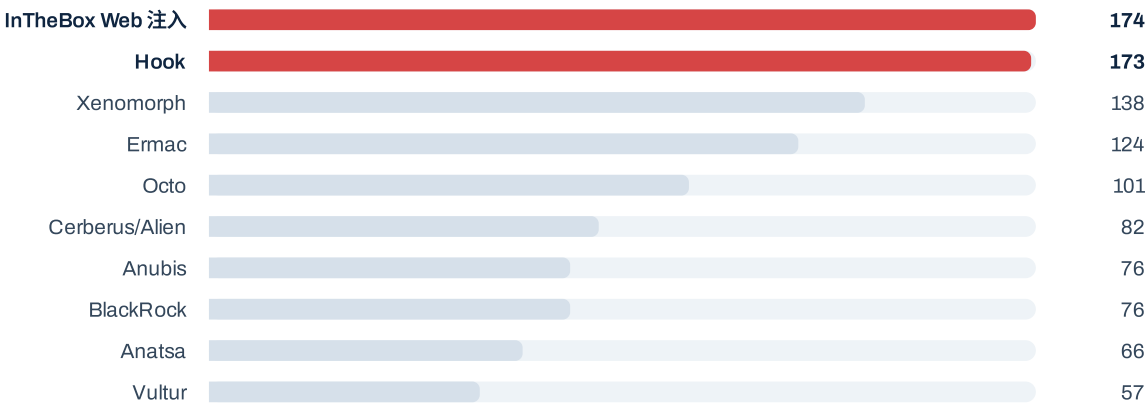
Android 应用

四成银行上了木马目标名单。

研究人员会公开银行木马中发现的目标名单。将其与我们样本中的 Android 应用比对后，192 家银行（38.4%）的 280 款应用被 29 个家族中的至少一个列入名单。

Hook 和 InTheBox 针对样本中的应用最多

图 8.1



我们样本中出现在各家族已公开目标名单上的应用数量：共 47 份名单，大多由 ThreatFabric、Cleafy、Zimperium 等于 2021 至 2023 年发布。仅限 Android，因为名单列出的是 Android 包名。

来源 已公开的银行木马目标名单（ThreatFabric、Cleafy、Zimperium 等），2021–2023 年。

欧洲和美洲吸引了 93% 的钓鱼主机，以及全部九家最常被仿冒的银行

图 8.2

54%
欧洲
9 家最常被仿冒银行中的 5 家

39%
美洲
9 家最常被仿冒银行中的 4 家

5%
亚太
9 家最常被仿冒的银行均不在此地区

1%
中东和非洲
9 家最常被仿冒的银行均不在此地区



颜色：各地区在冒用银行名义的活跃钓鱼主机中所占的比例。图钉：该国总部所在的九家最常被仿冒银行的数量；这九家银行合计吸引了全部主机的 57%。灰色：不在样本中。不点名银行。

来源 PhishTank、OpenPhish、Phishing.Database 和 URLhaus。

2026 年：攻击者让银行自己的应用为其所用。

十年来，银行木马一直在真实应用之上绘制虚假界面。过去一年的攻击活动更进一步：它们篡改、克隆或替换正版应用，让银行自己的代码最终为攻击者服务。

自 2016 年起
覆盖
在上层绘制

木马在真实应用之上绘制虚假的登录或支付界面，读取客户输入的内容。

为何奏效
正版应用未被改动；木马只需获得无障碍权限。

防御手段
覆盖层防护、无障碍服务检查

GOLDFACTORY，2025 年
篡改
修改应用

攻击者获取正版应用，注入 Hook 代码并重新签名，使银行自己的界面运行攻击者的代码。

为何奏效
副本的外观和行为与真实应用一致，包括其完整性检查，而这些检查已被 Hook 关闭。

防御手段
对照银行密钥的签名检查、服务器端证明

GIGABUD，2026 年
克隆
运行第二个副本

攻击者在其控制的隐藏工作资料或虚拟空间中运行正版应用。

为何奏效
反欺诈工具看到的是已知设备上的真实应用，因此会话看似正常。

防御手段
工作资料和虚拟空间检测、设备绑定

HIRUDO，2026 年
替换
调包应用

投放器卸载正版应用，并安装一个名称、图标和版本号都相同的篡改副本。

为何奏效
客户看不到任何变化。只有签名密钥不同，而只有银行服务器能够检查它。

防御手段
检查签名密钥的服务器端证明

应用调包如何逐步实施

1. 虚假更新
受害者通过链接或虚假商店页面安装投放器。

2. 真实应用被移除
投放器卸载正版银行应用。

3. 副本取而代之
它安装一个篡改副本：名称、图标和版本相同，签名密钥不同。

4. 凭据泄露
副本在看似正常的同时窃取密码和一次性验证码。

5. 由服务器裁决
只有银行服务器上的证明机制才能区分副本与正版应用。

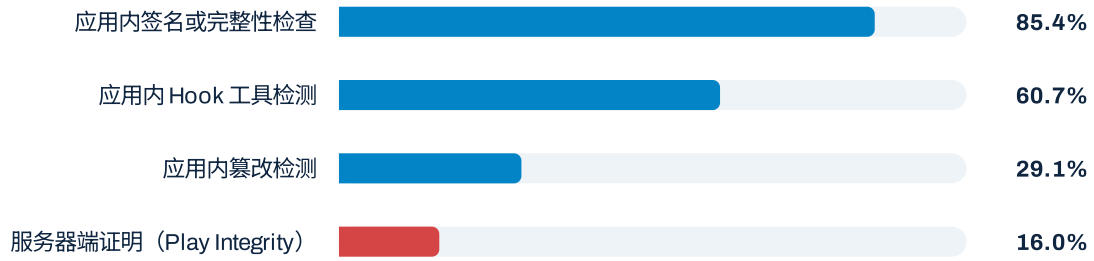
来源 Group-IB（GoldFactory、Gigabud）、ThreatFabric（Hirudo）；Ostorlab 分析。

银行能否察觉其应用已被调包？

篡改后的副本可以关闭在手机上运行的任何检测。服务器则能做得更好：它可以拒绝未携带由 Google 或 Apple 签名、证明应用为银行正版构建的最新凭证的请求。仅 16% 的 Android 应用包含请求该证明的代码，而我们无法看到其服务器是否强制校验。

应用内检测常见，服务器端检测罕见

图 8.3



Android 应用占比。应用内：在银行自有代码或内置 SDK 中发现。服务器端证明：应用包含请求证明的代码；服务器是否强制校验无法从应用中看出，且正版但已被攻陷的设备仍可能通过。

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

2026 起攻击活动

时间	攻击活动	类型	经过	报告方
2025 年12月	**GoldFactory**	篡改	泰国、越南和印度尼西亚的正版银行应用被注入可绕过其完整性检查的 Hook 代码：27 款被修改的应用，报告感染超过 11,000 次。	Group-IB
2026 年2月至7月	**Gigabud**	克隆	银行应用在 Android 工作资料中运行以规避欺诈检测；报告约 1,469 台设备被攻陷。	Group-IB
2026 年5月	**实验室测试**	篡改	在八个市场测试的银行应用中，58% 可被重打包。	Promon
2026	**覆盖类家族**	覆盖	34 个活跃的银行恶意软件家族，针对 90 个国家和地区的 1,243 个金融品牌。	Zimperium
2026 年8月至10月	**Hirudo**	替换	投放器将一款真实的印度尼西亚银行应用替换为用公开测试密钥签名的篡改副本；七家银行的八款应用已有现成的替换版本。案例研究见第 49 页。	ThreatFabric

应对措施

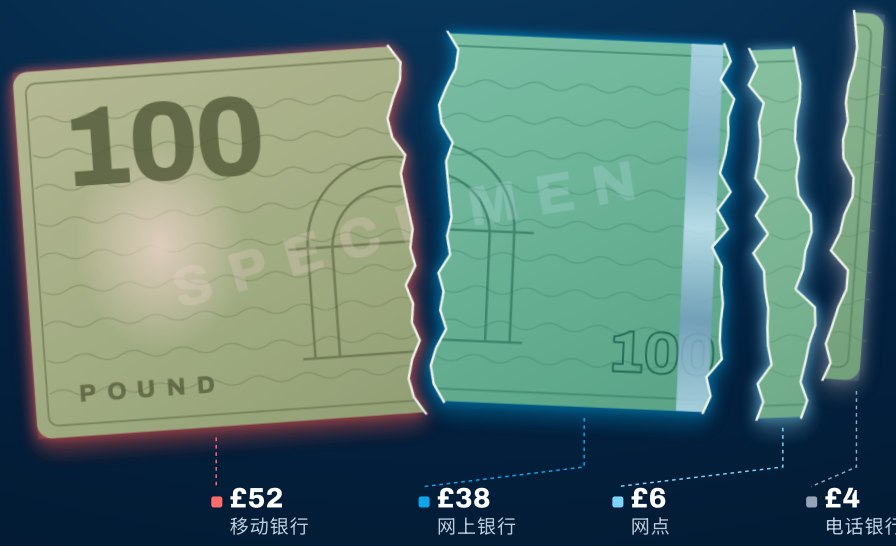
将手机上运行的任何检测都视为减速带。让服务器做决定：登录和支付必须经过证明，拒绝来自银行自有密钥以外任何密钥签名的应用的请求，并将客户会话绑定到发起会话的设备。

资金流向何处。

公开的欺诈数据零散不全：在我们检查的 101 个市场中，仅 83 个发布了可比较的数据。在有数据的地方，趋势一致：欺诈已转向客户受骗而主动发起的支付，并转向手机。

图 8.4

在英国，每 100 英镑诈骗损失中，有 52 英镑经由移动银行应用流出



576.4 百万英镑
为英国 2025 年授权推送支付诈骗造成的损失

79%
的诈骗支付（按笔数计）通过移动银行完成

88%
的已报告诈骗损失根据英国退款规则获得赔付

一张 100 英镑纸币按诈骗支付所用渠道撕开；每一片的宽度等于该渠道在损失金额中的占比。在授权推送支付（APP）诈骗中，客户受骗主动转出资金。当年授权类损失上升 19%，而非授权类损失下降 5%。

来源：UK Finance《Annual Fraud Report 2026》；英国支付系统监管机构（PSR）

欧洲

2024 年，欧盟欺诈性贷记转账金额中有 74% 源于操纵付款人授权付款。按金额计，卡不在场时的银行卡欺诈发生率是卡在场时的 13 倍。来源：ECB 和 EBA 支付欺诈报告，2024 年数据。

赔付机制见效

自英国于 2024 年10月实行强制赔付以来，在随后 18 个月内，银行按金额返还了已报告 APP 诈骗损失的 88%。责任正在转向银行，这提升了在应用内阻止诈骗的控制措施的价值。来源：英国支付系统监管机构（PSR）。

背景，而非成因

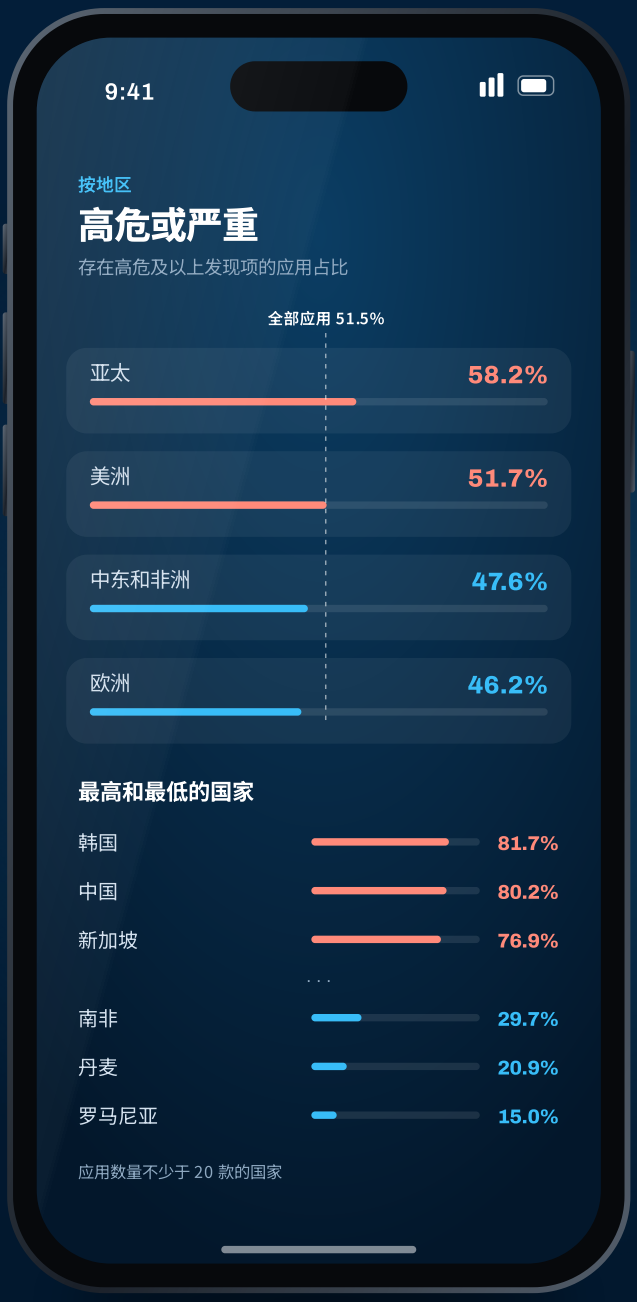
这些统计数据描述的是各市场的欺诈情况，并不表明本报告中的应用弱点导致了这些损失。

第 09 章

09

按地区、银行类型和国家

结果因国家而异的程度大于因平台而异。有些市场在运行时防护上领先，有些在应用证明上领先，没有一个市场在所有方面都领先。



图示：按地区和国家划分的存在高危或严重发现项的应用。

64

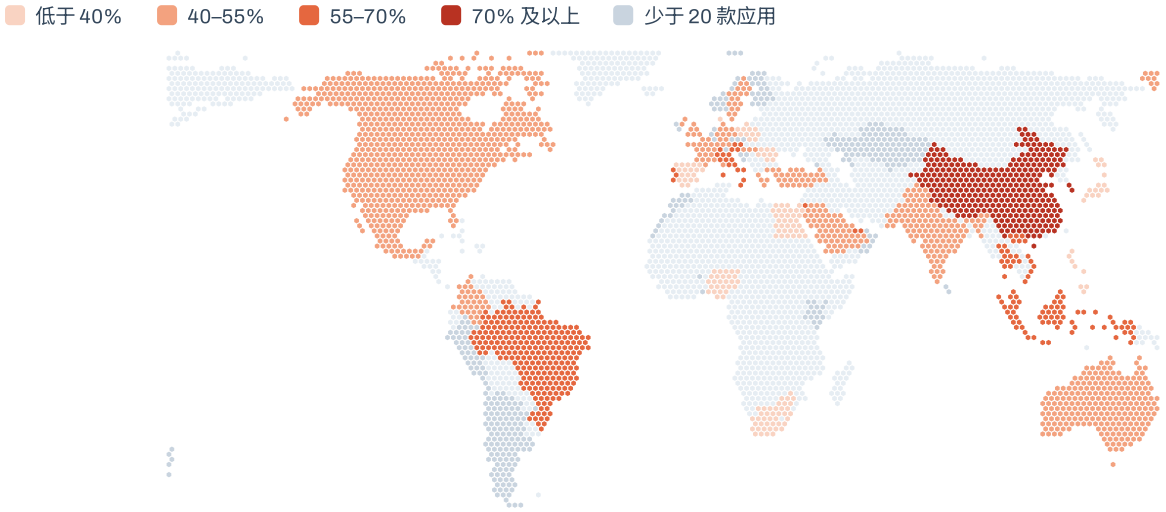
个国家和地区纳入样本，从美国、中国到多哥和列支敦士登

没有哪个地区面面俱到。

亚太应用的高危及以上发现项最多，同时运行时防护也最多。欧洲应用的高危或严重发现项最少。美洲应用在通行密钥上领先，达 9.9%。

高危及以上发现项在不同国家之间差异很大

图 9.1



各国应用占比，涵盖至少有 20 款应用的 40 个国家和地区；灰色：在样本中但应用少于 20 款。

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

没有哪个地区或银行类型在所有指标上领先

图 9.2

群组	应用	高危或严重	存在漏洞的组件	内嵌凭据	防护产品	应用证明	通行密钥 API
亚太	942	58.2%	46.3%	24.5%	33.7%	20.0%	2.8%
欧洲	822	46.2%	40.0%	15.7%	21.3%	16.9%	4.7%
中东和非洲	508	47.6%	39.0%	23.0%	19.9%	19.9%	4.3%
美洲	414	51.7%	33.8%	16.2%	29.5%	23.4%	9.9%
按银行类型							
传统银行	2,596	51.2%	40.9%	19.8%	26.4%	19.3%	4.4%
银行旗下数字银行	61	52.5%	47.5%	24.6%	37.7%	16.4%	4.9%
独立数字银行	29	**79.3%**	44.8%	**48.3%**	24.1%	**48.3%**	**37.9%**
全部应用	*2,686*	*51.5%*	*41.1%*	*20.2%*	*26.6%*	*19.6%*	*4.8%*

各群组的应用占比。独立数字银行存在高危或严重发现项的比例远高于其他应用（79.3% 对 51.2%；Fisher 精确检验，$p = 0.002$），而银行旗下数字银行与其余应用相近。独立数字银行在应用证明和通行密钥 API 上也领先。它们只有 29 款应用，其中三分之一来自同一家银行，因此差距的大小仅供参考。单元格着色方式与下一页相同。内嵌凭据不含 Google API 密钥。由于各地区的平台构成不同，仅比较跨平台规则。

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

各国结果。

样本中应用最多的 18 个国家和地区。每个单元格按其高出全部应用占比的幅度着色：红色表示风险，蓝色表示防御。未着色的单元格等于或低于全部应用占比。

每个国家都有各自的风险与防御格局

图 9.3

高于全部应用占比： 风险 +5 个百分点 +12 +20 防御 +5 个百分点 +12 +20

国家	应用	高危或严重	存在漏洞的组件	内嵌凭据	防护产品	应用证明	通行密钥 API
美国	224	52.2%	35.3%	12.9%	33.9%	28.1%	12.9%
印度	200	50.0%	30.5%	21.0%	**43.0%**	**32.5%**	0.5%
中国	162	**80.2%**	**77.8%**	**43.8%**	**51.9%**	15.4%	5.6%
英国	157	47.1%	**57.3%**	31.2%	**43.9%**	18.5%	14.0%
日本	116	38.8%	33.6%	13.8%	6.9%	4.3%	3.4%
沙特阿拉伯	95	47.4%	32.6%	31.6%	17.9%	13.7%	6.3%
阿联酋	84	**64.3%**	**59.5%**	25.0%	23.8%	28.6%	0.0%
法国	76	43.4%	35.5%	3.9%	21.1%	9.2%	0.0%
意大利	74	58.1%	**58.1%**	21.6%	5.4%	29.7%	2.7%
南非	74	29.7%	17.6%	**37.8%**	20.3%	**54.1%**	9.5%
马来西亚	71	57.7%	42.3%	25.4%	31.0%	25.4%	1.4%
西班牙	69	37.7%	24.6%	8.7%	**42.0%**	27.5%	7.2%
巴西	66	60.6%	31.8%	22.7%	27.3%	21.2%	10.6%
澳大利亚	63	54.0%	33.3%	19.0%	4.8%	23.8%	3.2%
韩国	60	**81.7%**	**71.7%**	21.7%	3.3%	3.3%	0.0%
越南	56	**64.3%**	51.8%	**33.9%**	**41.1%**	25.0%	3.6%
卡塔尔	55	41.8%	40.0%	21.8%	10.9%	25.5%	0.0%
加拿大	50	48.0%	26.0%	14.0%	12.0%	14.0%	4.0%
全部应用	*2,686*	*51.5%*	*41.1%*	*20.2%*	*26.6%*	*19.6%*	*4.8%*

各国应用占比。着色：高出全部应用占比 5、12 和 20 个百分点及以上。中国的应用中有许多 HarmonyOS 应用，拉高了其组件和严重级别数据。

来源 Ostorlab 对 2,686 款银行应用的自动化安全分析。

各地区最安全的银行应用。

每个地区选出三家银行，其应用的弱点比同行更少、严重程度更低，按字母顺序排列。不显示分数。

北美

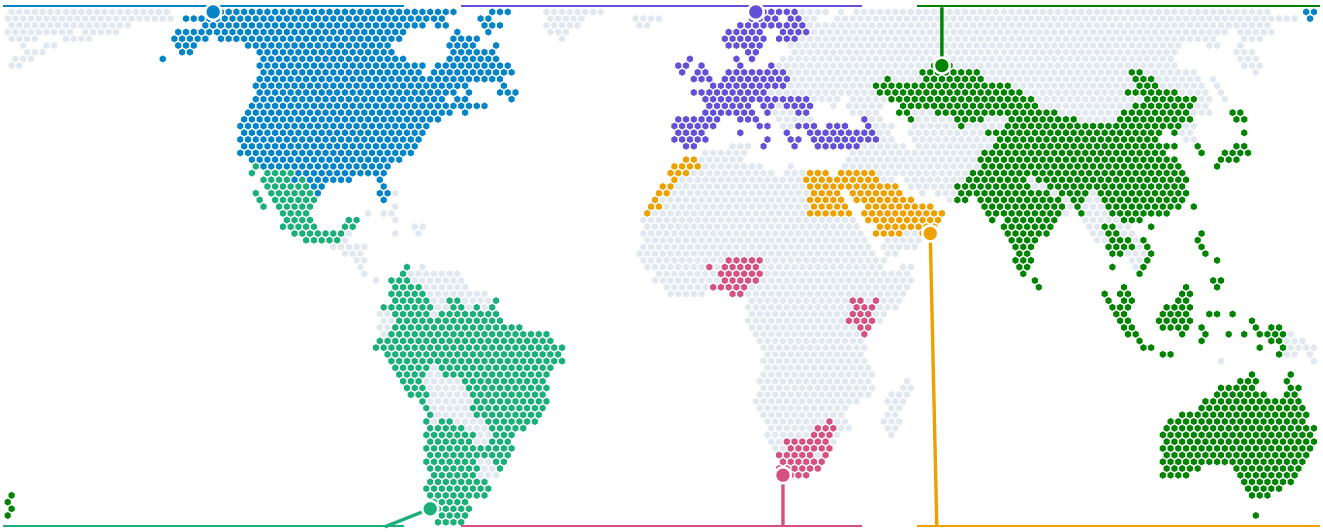
- **Scotiabank** — 加拿大
- **WaFD Bank** — 美国
- **Zions Bancorporation** — 美国

欧洲

- **Ibercaja** — 西班牙
- **Komerční banka** — 捷克
- **TSB** — 英国

亚太

- **Bandhan Bank** — 印度
- **HBL** — 巴基斯坦
- **RCBC** — 菲律宾



拉丁美洲

- **Banorte** — 墨西哥
- **BCP** — 秘鲁
- **Itaú** — 巴西

撒哈拉以南非洲

- **Absa** — 南非
- **Co-Operative Bank of Kenya** — 肯尼亚
- **Rand Merchant Bank** — 南非

中东和北非

- **Gulf Bank** — 科威特
- **Qatar Islamic Bank** — 卡塔尔
- **Saudi Investment Bank** — 沙特阿拉伯

颜色：参与比较的银行所在国家，每个地区一种颜色　灰色：未参与比较

银行如何比较

比较的是银行，而非单个应用。每款经扫描的应用根据其扫描评级（70%）以及代码中发现的防御措施和弱点（30%）获得一个分值，并在同一应用商店的应用中排位。银行的应用得分是其所有经扫描应用的平均值，应用较少时向中间值收缩。

安全历史也计入

随后，过去三年中银行每发生一起公开报道的安全事件，其应用得分就会相应降低：严重事件扣分多，轻微事件扣分少。针对客户的诈骗不计入。历史记录为空表示未发现事件，而不是没有发生事件。

入选的含义

在至少有两款经扫描应用的银行中，各地区排名前三的银行。入选表示其发现项比同行更少、严重程度更低，并不表示其应用没有发现项。

来源 Ostorlab 对前 500 家银行应用的扫描评级与安全控制；公开的事件报告。徽标为银行网站图标，是其所有者的商标，仅用于识别。

第 10 章

10

案例研究

2026 年的四起公开攻击，每起都与我们的扫描在其目标应用中的发现相对照。从在通话期间安装的虚假应用，到正版应用被替换，再到在应用发布后获得新权限的云服务密钥。



图示：四个案例及各自的起始页。

4

起 2026 年的公开攻击，每起都与我们的扫描在其目标应用中的发现相对照

案例研究 1/4 • 虚假应用

CyberDakait：七种木马，一通电话。

七个针对印度银行客户的 Android 木马家族。恶意软件本身并不特别，真正奏效的是事先的那通电话：冒充银行的诈骗者诱导受害者安装它。

7
个木马家族属于该集群

17,960+
台受感染设备，根据攻击者自己的服务器统计

7.6 百万
条短信从受害者手机上被拦截

Group-IB 报告，2026年10月28日

攻击如何实施

1 **电话**
冒充银行的来电者推销“信用卡保护计划”或奖励。

告知客户：银行绝不会在通话期间发送应用

2 **链接**
受害者收到一个冒充 11 家印度银行之一或 2 个政府项目的应用文件。

3 **虚假更新**
仿 Google Play 风格的“更新”界面诱使用户安装应用并授予权限。

4 **覆盖层**
仿冒的银行界面索要卡片信息、登录凭据和 PIN。

5 **短信**
木马读取收到的短信，并将一次性验证码转发给攻击者。

将验证码与设备和交易绑定，而非使用普通短信

6 **盗取**
攻击者凭借凭据和验证码清空账户。报告的损失超过 30,500 美元。

我们的扫描发现

应用内覆盖层防护 **75.6%**

支持短信一次性验证码 **33.7%**

Android 应用占比。覆盖层防护只保护正版应用：通话期间发送的虚假应用根本不会运行它。当银行接受短信验证码作为身份证明时，攻击就会得逞。

本可阻止攻击的措施

- 在应用内及所有渠道告知客户：银行绝不会在通话期间发送应用或要求安装应用。
- 以与设备和交易绑定的审批取代短信验证码。
- 对通话期间出现的新设备和新收款人暂缓处理并进行审核。

Group-IB，*False Protection, Emptied Accounts: The Seven Android Trojan Families Targeting Indian Banking Apps*，2026年10月28日。
不点名任何银行：Group-IB 未公布被冒充银行的名称。

案例研究 2/4 • 被劫持的应用

WindRelay：用受害者自己的银行应用办理贷款。

在中欧被组合使用的两种工具：SpyNote，一种让攻击者掌控受害者手机的远程访问木马；以及 WindRelay，它通过 NFC 将受害者的支付卡中继到钱骡持有的手机上。

2
种工具组合使用：远程访问木马和 NFC 中继

3
个目标国家：捷克、斯洛伐克和斯洛文尼亚

23
个样本，采集于 2025 年11月至 2026 年7月

Group-IB 报告，2026年8月12日

攻击如何实施

1 **电话**
语音诈骗者冒充银行或其他可信方联系受害者。

2 **安装**
受害者安装一款应用；每个 SpyNote 构建版本都标注了受害者的姓名。

3 **刷卡**
中继应用让受害者将银行卡贴近手机并输入 PIN，然后转发给钱骡。

4 **取现**
钱骡使用被中继的银行卡付款或取现。

5 **接管**
攻击者通过 SpyNote 操控手机，并打开正版银行应用。

检测屏幕是否被共享或远程控制

6 **贷款**
在至少一个案例中，攻击者通过该应用以受害者名义办理了贷款。

在服务器端对贷款、收款人和限额实施加强验证

我们的扫描发现

应用内远程控制检测 **33.0%**

服务器端证明（Play Integrity） **16.0%**

Android 应用占比。接管发生在受害者真实设备上的真实应用内，因此设备绑定和 SIM 卡检查都会通过。只有应用本身能察觉其界面正被远程操控。

本可阻止攻击的措施

- 检测屏幕共享和远程控制，并将信号发送至银行的风险引擎。
- 对贷款、新增收款人和提高限额，要求进行新的、与密钥绑定的审批。
- 将应用内先刷卡后要求输入 PIN 的行为视为欺诈模式。

Group-IB，*WindRelay and SpyNote: an NFC and RAT combination in fraud*，2026年8月12日。
不点名任何银行：Group-IB 未公布受影响银行的名称。

案例研究 3/4 • 被替换的应用

Hirudo：替换银行应用的木马。

一种不满足于绘制虚假界面的 Android 银行木马。它卸载真实应用，并安装一个篡改副本，副本中隐藏的 Hook 会向应用自身的安全检测返回伪造的结果。

42
款金融应用在 Hirudo 的目标名单上

8
款银行应用（来自 7 家印度尼西亚银行）已有现成的篡改副本

1
行代码被添加到每个副本中，用于加载 Hook 引擎

ThreatFabric 报告，2026年10月14日

攻击如何实施

1 **诱饵**
一款可正常使用的购物、短剧、足球或成人视频应用。

2 **虚假更新**
诱饵应用安装木马，木马随即申请无障碍和通知访问权限。

3 **窃密**
虚假的结账、银行和钱包提示框收集 PIN 和密码；虚假的图案解锁界面骗取解锁码。

4 **目标**
木马找到八款目标银行应用之一，并检查其签名证书。

5 **调包**
虚假的更新提示打开卸载程序，随后木马自行安装篡改副本。

6 **接管**
副本在伪造的安全信号下运行，同时攻击者实时查看屏幕。

对每项受保护操作，在服务器端检查 Play Integrity 判定结果

篡改应用的内部

副本保留原有的名称和版本号，但使用公开的 Android 测试密钥签名，因此必须先移除正版应用。新增的一行代码加载一个 Hook 引擎，该引擎仅在木马写入的某个文件存在时才会启用。

远程访问与数据收集

实时屏幕查看和摄像头会话、对 90 天内短信的扫描，以及位于中国、印度、墨西哥、摩洛哥和泰国的凭据窃取目标。一台未加防护的攻击者服务器存有数千条被盗凭据和金融档案。

ThreatFabric，*Hirudo: from fake updates to patched banking apps*，2026年10月14日。
BleepingComputer，*Hirudo Android malware replaces banking apps to evade security checks*，2026年10月14日。
不点名任何银行：ThreatFabric 未公布这些印度尼西亚银行的名称。我们的扫描发现：见下页。

在仿冒副本中，每项检测都可被伪造。

Hirudo 在攻击者控制的进程中运行银行自己的检测，并自行作答。61% 至 85.4% 的 Android 银行应用具备它所伪造的应用内检测。

应用提出的问题		HIRUDO 的回答	提出该问题的 ANDROID 应用
签名证书 “这是银行的签名密钥吗？”	→	HIRUDO 的伪造回答 返回正版证书，隐藏测试密钥签名。	签名或重打包检测 **85.4%**
无障碍服务 “是否有其他应用在控制屏幕？”	→	HIRUDO 的伪造回答 返回空列表，隐藏木马的控制服务。	覆盖层或无障碍滥用防护 **75.6%**
防截屏 “此界面能否被录制？”	→	HIRUDO 的伪造回答 去除该标志，使银行界面可被远程查看和录制。	截屏防护 **61.0%**
硬件密钥证明 “密钥是否位于安全硬件中？”	→	HIRUDO 的伪造回答 使用一个已泄露的硬件 keybox 作答，其证书已被 Google 吊销。	未计入：无法与其他证明调用区分
Play Integrity “这是正版手机上的正版应用吗？”	→	HIRUDO 的伪造回答 将请求发送到攻击者的服务器，由其返回应用会接受的通过判定。	Play Integrity 调用 **16.0%**

Hook：ThreatFabric。占比：在银行自有代码或内置 SDK 中具备该检测的 Android 应用；Play Integrity：代码可读的应用。存在检测不等于能抵御 Hook。

依然有效的措施：由银行服务器自行核验的答案

- 在服务器端验证 Play Integrity，并与会话和受保护操作绑定。
- 对照 Google 的吊销列表检查密钥证明证书。
- 在登录、凭据找回、新增收款人和支付审批环节，将交易风险控制保留在服务器端。
- 将无障碍和屏幕捕获信号纳入风险评分，而不是将其作为独立的拦截条件。

来源：ThreatFabric（Hook）；Ostorlab 分析（应用）。

案例研究 4/4 • 泄露的密钥

变成 AI 凭据的 Google API 密钥。

Google 长期告诉开发者，其 API 密钥（以 AIza 开头的字符串）不属于机密信息：它们用于为 Maps 或 Firebase 标识项目，本就应随应用发布。但密钥能访问什么，是在云项目中设置的，往往由另一个团队在应用发布很久之后设置。

2,863
个具有 Gemini 访问权限的有效 Google API 密钥在公开网络数据中被发现

32
个具有 Gemini 访问权限的有效密钥存在于 22 款热门 Android 应用中

82,314 美元
一名密钥被滥用的受害者报告的 Gemini 账单

Truffle Security 报告（2026 年2月）及 CloudSEK 报告（2026 年4月）

无害的密钥如何变成 AI 凭据

1 **密钥随应用发布**
应用携带用于 Maps 或 Firebase 的 Google API 密钥，这是 Google 文档所允许的。

将每个随应用发布的密钥限制为所需的 API 和应用签名

2 **Gemini 被启用**
另一个团队在同一云项目中启用了 Generative Language API。

将 AI API 放在其密钥绝不下发到设备的项目中

3 **密钥获得 AI 访问权限**
该项目现有的每个密钥现在都能调用 Gemini，而应用本身没有任何变化。

4 **滥用**
攻击者从应用中提取密钥，读取上传到 Gemini 的文件并刷高账单：一名受害者被收取了 82,314 美元。

我们的扫描发现

Android 应用 **80.3%**

iOS 应用 **30.6%**

HarmonyOS 应用 **71.4%**

安装包中任意位置至少含有一个 Google API 密钥的应用占比；占全部应用的 72.5%。密钥未经测试：大多数可能仅限于 Maps 或 Firebase，而应用团队无法从密钥本身判断。

本可阻止攻击的措施

- 将每个密钥限制为其所需的 API 和应用的签名证书。
- 将 Gemini 及其他 AI API 放在单独的云项目中。
- 在启用新 API 之前，轮换所有曾随应用发布的密钥。

Truffle Security，*Google API keys weren't secrets, but then Gemini changed the rules*，2026年2月25日。
CloudSEK，*Hardcoded Google API keys in top Android apps now expose Gemini AI*，2026年4月7日。
不点名任何银行：两个来源均未公布密钥遭泄露的金融机构名称。

2026 年银行应采取的 10 项首要行动。

十项行动，每项都对应本报告中的一项发现和一个 OWASP MASVS 控制组，并按其减少欺诈的直接程度排序。

01 在服务器端验证应用

使用 Play Integrity 和 App Attest，在服务器端检查判定结果并拒绝未通过的请求。这是篡改或调包的应用唯一无法关闭的防御措施。

79.8% 的应用未使用证明机制

MASVS-RESILIENCE

02 将每项敏感操作与密钥绑定

让登录和支付审批通过与硬件支持密钥绑定的生物识别完成，绝不使用“是或否”式的检查。

35.1% 的 Android 应用存在生物识别绕过

MASVS-AUTH MASVS-CRYPTO

03 提供通行密钥

增加通行密钥登录，并发布相应的 asset links 和关联域名，使被钓鱼窃取的密码不再足以登录。

4.9% 集成了通行密钥 API

MASVS-AUTH

04 将机密信息移出应用

将私钥、云服务密钥和服务令牌移至服务器，并签发短期令牌。将必须随应用发布的密钥限制为您的应用签名及其所需的 API。

20.3% 内嵌了 Google API 密钥以外的凭据

MASVS-STORAGE MASVS-CRYPTO

05 封堵登录重定向

通过只有您的应用才能认领的通用链接和应用链接返回登录结果，绝不使用其他应用可注册的自定义 URL scheme。

21.1% 的 iOS 应用可能遭受 OAuth 账户接管

MASVS-PLATFORM MASVS-AUTH

06 检测远程控制和覆盖层

组合使用 root、Hook、篡改、覆盖层和屏幕共享检测，启用 SDK 中已具备的检测，并在真机上进行测试。

33% 的 Android 应用具备远程控制检测

MASVS-RESILIENCE

07 掌握所发布的内容

为每个版本维护软件物料清单，包括 SDK 和供应商平台，并在规定期限内修复严重组件。

41.1% 含有存在漏洞的组件

MASVS-CODE

08 加密每一条连接

关闭明文通信，为自有 API 锁定证书，并将 WebView 限制在自有页面。

29.4% 的 Android 应用允许明文通信

MASVS-NETWORK MASVS-PLATFORM

09 关注旧设备

在登录时检查操作系统的补丁级别，并在不再获得更新的设备上限制高风险操作。

99.5% 的 Android 应用可在未打补丁的 Android 上运行

MASVS-CODE

10 让标签和联系方式真实可信

使应用商店隐私标签与应用的实际行为一致，并发布 security.txt，以便研究人员能联系到您。

7.1% 的银行域名发布了 security.txt

MASVS-PRIVACY

定义与数据说明。

样本

本研究涵盖前 500 家银行的移动应用。共收集 2,841 个应用商店条目，下载并分析了其中 2,686 款，覆盖 Android、iOS 和 HarmonyOS。国家和地区按银行所在市场划分。

严重程度

应用的严重程度取其最严重的严重、高危、中危或低危发现项。“潜在风险”（需要人工确认的模式）和“加固建议”（缺少某项安全防护）不影响该评级；若图表将其计入，会另行注明。高危或严重表示至少有一个这两个级别之一的发现项；低危及以下表示没有严重、高危或中危发现项。

平台专属规则

生物识别绕过、Intent 重定向、序列化、密码学、明文通信和存储类规则仅在 Android 上运行；App Transport Security 和隐私清单规则仅在 iOS 上运行。其占比以该平台的应用数为分母。

未知值

当应用代码经过加壳或无法读取时，检查结果为未知。这些应用不计入该检查的分母，其数量在数据旁注明。运行时防护图表将未知单独显示为一段。

内嵌凭据

格式可识别的机密信息，如 API 密钥、访问令牌或私钥。Google Cloud API 密钥单独报告。未测试密钥的有效性。

通行密钥与证明机制

已集成通行密钥 API 指应用调用了 Android Credential Manager、Google FIDO2 API 或 Apple 的 AuthenticationServices 通行密钥 API。由其他库打包引入的 FIDO2 类不计入。证明机制指 Play Integrity、SafetyNet、HMS Safety Detect、App Attest 或 DeviceCheck。

运行时防护

在代码或内置产品中发现的防护措施，覆盖全部三个平台。在 iOS 上，以越狱检测替代 root 检测，覆盖层防护不适用。未在设备上测试其存在情况。

未打补丁的系统版本

Android 和 HarmonyOS：低于 API level 34（Android 14），自 2026 年3月起不再获得 Android 安全公告补丁。iOS：低于 iOS 18，即 Apple 仍提供完整补丁的最旧主版本。

银行侧数据

后端暴露面和 CVE 来自 Shodan 的 InternetDB 被动索引，系根据版本推断，未经测试。数据泄露记录来自 VCDB、Have I Been Pwned、ransomware.live、SEC 8-K 文件，对 G-SIB 还包括新闻和监管机构信息；每条匹配均经人工复核。认证情况依据网站声明。

外部数据

Web 和邮件检查覆盖 1,252 个银行域名。后量子支持情况读取自记录的 TLS 握手。木马目标名单来自 47 份已公开名单。钓鱼主机取自四个公开情报源的单次快照。隐私标签来自 Google Play 和 App Store。对于无法打开的 142 个银行网站，我们读取了 2025 年或之后最新的公开存档副本（Internet Archive）；存档副本可能早于实时网站。

欺诈统计

来自监管机构、央行和行业组织的 536 项已公布数据，每项均保留其统计期间和统计范围。它们描述的是各市场的欺诈情况，而非本报告中的弱点所造成的损失。

案例研究

公开研究的摘要，出处已在各页注明。与之并列的扫描数据来自我们。

Ostorlab

2026 移动银行应用安全报告

版本 3 · 2026年11月12日