ANTIYINNOVATION

安天创造

305期

2023年5月 试行

安天移动安全专刊

主办：安天 400-840-9234 antiynews@antiy.cn

移动互联网应用生态的“良赢治理”

本期焦点

上期回顾

执行体全量识别与精细管控——网络空间威胁对抗与防御技术研讨会

本期《安天创造》为第十届安天网络安全冬训营系列文章专刊，共分六个章节。前三个章节，分别围绕 2022 年网络安全威胁回顾、支撑执行体全量识别与精细管控的基础能力与赋能应用场景，选取了 14 个技术报告撰文精编，希望能与业界同仁和客户共同探讨更有效的安全运营变革，打造坚实厚重的网空防御力量；“聚合 效能 闭环”章节，介绍了安天最新发布的六款助力提升客户在数字化转型等新场景安全运营效能的创新产品；“安天党建文化与青春风采”章节，分享了具有“安天特色冰雪符号”的“2023 年安天雪雕大赛”部分作品。

➤ 《安天创造》是安天面向客户的品牌刊物，按照安天达成客户有效安全价值的企业使命，汇聚发布安天长期从事威胁对抗工作的分析报告，分享安天在与客户并肩战斗中形成的安全理念与认知理解，总结保障和服务客户的实践经验，传递以创造性思维和工程化能力为客户解决问题的安天工程师文化，展示安天团队的创造力与青春风采。

刊首语

移动终端用户侧威胁泛化，风控为核心的体系化应对是关键

自 2014 年首次对外发布安卓恶意代码编年史以来，安天移动安全一直致力于发现、识别和监测移动安全问题和移动终端用户安全威胁的变化形态和发展趋势，随着国内反病毒技术的逐渐成熟，移动终端侧的新增恶意程序数量呈逐渐下降趋势。但移动终端用户的安全威胁并未随之递减，反而呈现出威胁泛化的趋势。早在 2017 年，安天移动安全就在年报中提出了威胁全面迁徙的观点，并持续围绕移动终端应用程序（App）进行安全性检测和判定体系的建设。

当前，App 逐步渗透到衣、食、住、行等与人们生活息息相关的各个领域，移动互联网在促进产业升级并为人们生活带来极大便利的同时也滋生了不可忽视的风险，本应服务用户的 App 正在成为用户安全最主要的威胁来源之一。移动终端用户威胁虽以 App 为中心，但不应将用户威胁归结为应用自身问题，而要从 App 开发制作、分发、安装、运行及卸载等全生命周期的全局性视角关注可能产生的潜在用户威胁。

作为网络健康生态的助推者和用户安全的守护者，安天移动安全基于移动用户安全威胁以 App 为主要承载的客观现状，一直致力于解决当前移动智能终端用户所面临的应用威胁和风险问题。2020 年，安天移动安全从移动应用生态可持续发展和用户权益保护的视角出发，首次提出“风险应用”的概念，将风险问题进行了标准化定义、分类，形成了细粒度的移动互联网应用问题取证标准和科学评估办法，并对应用威胁的识别发现、分析判定和检测治理的工程化体系进行了进一步的设计和调整，逐步建立了核心为风控的风险应用体系。

安天移动安全在长期持续关注移动终端用户安全威胁的过程中，深刻思考并认识到，当前移动终端应用风险问题与产业链发展现状是高度绑定的关系，因此也带来了应用治理的难度和挑战。我们认为，移动生态治理只是作为一种手段，最终目的是基于“良赢治理”的安全发展理念，保障用户权益并促进移动互联网生态良性发展，形成围绕移动互联网产品和服务质量的良性竞争生态，达成个人用户、企业、社会等多方共赢目的，最终实现安全普惠。

移动互联网良性竞争生态的形成，离不开监管部门、手机厂商、安全厂商、互联网平台等生态多方共同的努力和协作。未来，安天移动安全将一如既往配合并支撑监管部门开展 App 侵害用户权益专项整治行动，并与手机厂商等产业链各方共同建立安全联运体系并进行生态治理，提供多维度、全方位的移动安全风控能力，促进移动互联网产业安全有序发展。

本 | 期 | 导 | 读

一直以来，在移动互联网 App、小程序、快应用等应用程序中出现的各类乱象，如借虚假免费试用、特惠活动或异性聊天等诱导用户付费的行为，以赚钱为幌子欺骗用户下载使用、设置多种提现障碍的行为，诱导未成年人充值消费、强制自动续费等严重侵害用户权益的行为等，都是安天移动安全重点关注和产业链联合治理的对象。

2022 年 12 月 12 日，中央网信办部署开展“清朗·移动互联网应用程序领域乱象整治”专项行动，着力解决损害用户合法权益的突出问题，保障用户合法权益。安天移动安全积极响应，并依托“安鉴”风险检测预警平台对 App 相关问题针对性的进行深度公开曝光，同时配合监管部门、终端厂商等产业链各方进行了生态治理，取得了阶段性积极成果。

本期《安天创造》为近两年安天移动安全在移动互联网应用生态中海量发现的研究成果，以及联合产业链共同协作的治理成果分享专刊，全刊共分 5 个章节。前三个章节，分别围绕 2022 年移动互联网风险应用重点问题披露、移动互联网风险应用典型问题解析以及安天移动安全配合产业链各方积极治理的阶段性工作成果进行了分享，重点选取了 16 篇文章，详细介绍了相关案例分析与实战经验，希望能与监管部门、终端厂商、业界同仁等产业链各方探讨更有效的移动互联网应用生态治理方案，共同抬升行业底线，保障广大用户的合法权益；“安天党建文化与青春风采”章节，分享了一系列安天组织多方学习主题党课的精彩记录。

目录

CONTENTS

PAGE

01 2022 移动互联网风险应用白皮书

引言

近年来，安天移动安全 -OPPO 安全联合实验室（下称：联合实验室）一直致力于发现、识别和监测移动安全问题和移动终端用户安全威胁的变化形态和发展趋势，持续围绕移动终端侧的 App 实现了应用的安全性判定和检测体系建设；并且基于此，以历年的移动安全年报对外披露当年的移动应用威胁变化态势情况（详见图 1）。

近年来，国家监管针对移动互联网 App 的一系列专项治理行动，包括个人信息保护、用户权益、未成年人权益、不良应用 / 快应用 / 小程序 /SDK、数据安全等等。这也促使我们从更广泛的用户安全视角重新思考。

因此，安天移动安全 -OPPO 安全联合实验室结合从移动终端用户权益保护、移动互联网产业链生态良性发展的视角出发，重新审视和评估移动互联网应用的安全问题。我们发现，整个移动智能终端下的应用威胁呈现泛化趋势，其中包括应用威胁形态的隐蔽化和多样化，并且从 App 到 Hybrid App/ 快应用 / 应用 SDK/WAP 站 / Web 应用等泛应用形式。此外，这些潜在的应用风险问题一定程度上与移动互联网生态发展中出现的野蛮生长、黑暗森林模式有关，其最终将导致用户权益受损，形成“劣币驱逐良币”不健康的生态发展导向等诸多问题。

联合实验室对移动互联网应用的风险性问题进行了标准化的定义、分类，以及建立了科学的评估方法，基于此在过去两年间针对移动互联网生态下部分垂直行业的应用进行了分析评估，发现了大量的问题及案例（详见图 2）。

上述的部分应用风险问题也在近两年的 3.15 晚会上作为热点问题向公众曝光，例如诱导老人下载 App 的广告弹窗属于应用存在用户权益风险问题；直播平台男运营冒充女主播过度索取礼物属于应用存在支付和用户资产风险问题并涉及诱导付费和欺诈。这些问题随着近两年国家监管的治理、媒体的曝光以及生态各方的协作呈现出一定的缓解趋势。

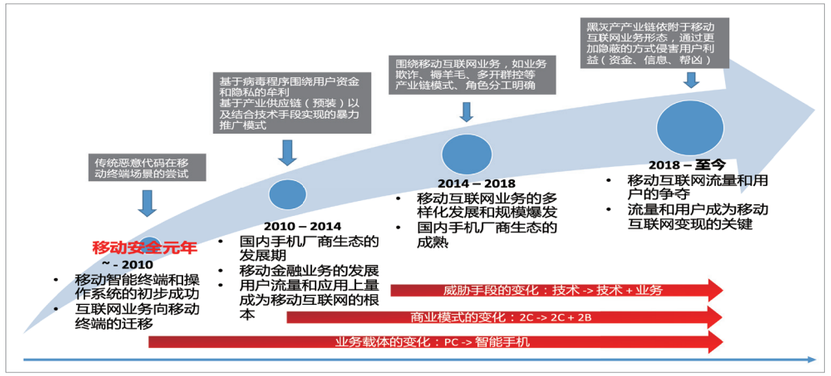


图 1 移动互联网生态和安全威胁发展概览

图 2 应用风险分类和风险问题示例

应用风险问题的变化

《移动互联网风险应用白皮书（2021）》[1] 中安天移动安全总结了当前移动互联网生态中一些普遍存在的行业共性风险问题以及部分垂直品类生态中特有的风险问题，并在 2022 年间协同各方监管部门对这些风险问题进行了一系列专项治理行动。本章节将着重介绍 2022 年联合实验室在广告弹窗问题、应用内容问题、应用功能及服务规范问题以及应用内支付和用户资产风险问题这四类较严峻的风险问题上的工作情况以及这些问题的发展变化。

1. 广告弹窗问题

广告流量变现是移动互联网行业一种常见的变现模式，尤其在工具和网赚品类中，这种盈利模式更为普遍，相应地广告弹窗问题在这两类应用中也最为突出。继 2021 年“央视 3·15 晚会”曝垃圾清理类 App 针对终端用户频繁推送广告的现象后，2022 年“央视 3·15 晚会”特别报道了“免费 WIFI”类应用弹窗广告、误触下载等问题，2022 年监管相关发文中，也多次提及要加强对应用弹窗问题的治理，足以看出监管部门治理广告弹窗问题的决心。

以下是安天移动安全总结的四类常见广告弹窗问题：

(1) 应用外广告弹窗问题

(2) 应用的广告弹窗存在欺骗、误导和强迫形式

(3) 应用推送的广告存在误触下载行为

(4) 应用频繁弹出广告

安天移动安全通过研究这类风险问题的实现原理，监控其技术衍变，形成一套高效精准的广告问题发现体系。支撑手机厂商终端部门加强终端识别及管控能力，推进应用市场优化该类风险问题的审核机制。

2022 年年中，应用市场审核规范中首次提出不再收录清理类应用，各大手机厂商从年初开始逐步加强终端应用外广告弹窗的管控。清理类应用的应用外广告弹窗整体呈下降趋势。回顾 2022 年，安天移动安全发现有部分开发者通过对 App 代码进行混淆加固，利用云控归因策略企图绕过终端管控限制、安天发现体系和应用市场审核机制。随着安天移动安全、手机厂商和有关监管部门的持续努力，2022 年 9 月之后，清理品类中的应用外广告弹窗问题得到明显遏制（详见图 1）。

图 1 2022 年清理品类新增用户量

清理品类主要风险问题为应用外广告弹窗问题，其他三类广告弹窗问题相对较少。但该三类问题在移动互联网中更为普遍，网赚品类中也存在类似风险问题。随着今年安天移动安全联合监管、手机厂商和安全厂商等相关单位开展基于清理品类广告弹窗风险问题的治理专项行动，在 App 侧该类风险问题得到明显改善，在包括清理品类等各类应用中广告弹窗风险行为都有显著减少。

在关注到 App 侧广告弹窗问题减少的同时，安天移动安全也留意到泛应用中的广告问题在逐步显露。部分开发者意识到 App 侧的管控加强后，转向其他监管目前比较薄弱的应用形态，导致泛应用中的风险问题增多。在新应用形态风险问题一章中安天移动安全将详细介绍快应用中出现的风险问题。

2. 应用内容问题

应用内容问题分为两类，一是应用运营方主动提供违反法律法规的模块功能，二是应用运营主体内容审核工作不到位，导致应用内存在违反相关法规要求或给对用户身心造成不良影响的内容。从落实责任主体的角度来看，此二类问题的管控仍然为应用运营方的责任。在《移动互联网风险应用白皮书（2021）》中安天移动安全提到过的风险问题中，属于应用内容问题的有以下几类：

(1) 应用内提供博彩模块

(2) 应用内提供色情模块

(3) 应用内存在低俗色情内容

(4) 应用广告内容问题

应用内容问题长期以来都是监管部门关注的重中之重，但在暴利面前，仍有不少开发者不断试探监管红线。安天移动安全发现交友类用中关于低俗色情内容的风险问题呈现快速发展的态势。部分陌生人交友类应用为了提高男用户留存率以及充值付费率，主动降低内容审核要求，导致应用内充斥低俗色情内容，给移动互联网应用生态造成极大负面影响。

除了应用开发者主动提供博彩色情模块以及内容审核要求不严谨导致应用内存在低俗色情内容的风险问题外，安天移动安全在持续监控分析应用内容风险问题发展变化过程中发现应用内容问题广告问题与某些商业广告 SDK 有关。

如（图 2-1、图 2-2、图 2-3）所示，示例中网赚应用展示的广告由某商业 SDK 下发，添加广告中的微信号后，会被引流到某博彩平台。

图 2-1 网赚应用

图 2-2 添加网赚微信号

图 2-3 引流到某博彩平台

如（图 2-4、图 2-5）所示，示例中清理工具类应用中的色情应用广告由某商业广告 SDK 下发。

图 2-4 色情广告示例 1

图 2-5 色情广告示例 2

在应用广告内容问题上，安天移动安全还发现网赚品类中出现大量有诱导欺诈性内的广告内容问题，这类广告以“中奖”、“抽奖”、“红包”等带有诱导性的文字或图片吸引用户点击，用户进入后随即跳转到第三方网站，通常为盲盒或话费券抽奖，存在极大的欺诈风险。这些问题安天移动安全将在品类风险问题深度解析一章进行详细分析介绍。

3. 应用功能及服务规范问题

出于对用户知情权的保障，应用应该在用户第一次进入使用时如实告知用户应用提供的功能和服务细则。在对应用风险问题的发现和界定过程中，安天移动安全定义了以下三类应用功能及服务不规范的风险问题：

(1) 应用在桌面隐藏图标入口

(2) 应用提供的功能是虚假的

(3) 应用设置提现障碍问题

在对这类问题的跟踪过程中安天移动安全发现，这类问题往往出自 IAA 品类。流量品类应用具备变现周期短，留存率低，应用开发门槛低等特点，因此这类应用的开发

运营者最终目的在于提高短期收益，不在乎应用是否能长期发展，在这种背景下应用功能及服务不规范的问题屡禁不止。2022 年网信办开展的“清朗”活动中，明确强调要严格规范功能设置，从严查处应用程序恶意隐藏相关功能的行为，如设置透明图标等，同时要求打击各类应用程序以赚钱为幌子欺骗用户下载使用，设置多种提现障碍。同年工信部发布的《工业和信息化部关于进一步提升移动互联网应用服务能力的通知（征求意见稿）》中也对应用功能及服务规范提出了类似要求。

根据对风险问题边界的界定和违规代码特征的分析，安天移动安全的特征代码检测工程体系从审核取证和应用检出两个层面，对隐藏图标入口和提供虚假功能的应用进行了治理。2022 年上半年，工具品类应用屡次被曝光存在隐藏图标问题，9 月份以后随着监管及厂商管控力度的缩紧，工具品类行业审核门槛的提高，行业逐渐走向健康发展，依赖这些风险问题进行暴力变现的开发者正逐渐减少，这类违规问题也随即淡出了安天移动安全的视线。

应用设置提现障碍问题则主要出现在网赚应用品类，网赚品类作为一种极具特色的 IAA 品类，不仅应用广告弹窗问题频发，还存在其独特的应用功能及服务不规范的风险问题。安天移动安全在第三章品类风险问题深度解析中将会详细介绍。

4. 应用支付和用户资产风险问题

应用支付和用户资产风险是指应用使用诱导、欺诈、迷惑、操纵等手段，或者内置非法的支付平台，令用户暴露在财产安全风险之下。在安天移动安全提到的风险问题中，有以下问题归纳在应用支付和用户资产风险问题中：

（1）应用存在诱导付费行为

（2）虚假宣传并欺骗诱导用户消费

（3）应用内存在擦边博彩的游戏玩法

作为与用户切身利益紧密相关的问题，用户资产安全问题一直是联合实验室关注的核心风险问题之一，同时也是各监管部门和终端厂商密切关注的问题。2022 年 12 月“清朗”行动中明确提到要严厉打击诱导充值，坚决打击部分应用程序恶意借虚假免费试用、特惠活动或异性聊天等诱导用户付费的行为。

《移动互联网风险应用白皮书（2021）》中提及的诱导付费问题主要指社交交友品类中存在大量诱导用户充值付费的现象。在对这类问题的持续跟踪监测中，安天移动安全发现这种诱导付费行为可以细分为两类：一类是社交交友应用内存在女性用户有组织地诱导男性用户充值付费的行为，这类行为跟社交交友行业中“公会”这一角色密不可分；另一类是社交交友应用开发者在设计平台运营策略和推送机制时，有意地通过一些手段诱导用户进行充值付费，这种诱导付费问题安天移动安全将在接下来的品类风险问题深度解析章节中分享。

除了在下沉交友上的诱导付费问题外，安天移动安全还发现了更多的 IAP 品类应用中付费功能不规范的问题。同样将在在接下来的品类风险问题深度解析章节作具体分析。

参考文献

[1]《移动互联网风险应用白皮书（2021）》
https://mp.weixin.qq.com/s/0CcAOm_7aGJzZ1hslG3oFA

新风险问题的发现

当前移动互联网生态中除 App 外，小程序、快应用等泛应用以及 SDK、插件等互联网信息服务提供主体也存在不少风险问题。在 2022 年的监管部门发文和通报中也多次提及要规范包括 App、小程序、快应用以及 SDK 和插件等在内的服务提供主体的行为。

本章节将介绍 2022 年安天移动安全新关注到的，在当前移动互联网生态中频发的一些风险问题，这些风险问题包括 App 侧新风险问题以及新的应用形态 --- 快应用相关的风险问题。

1. App 侧新风险问题

1.1 线下分发渠道应用存在的风险问题

《移动互联网风险应用白皮书（2021）》中提到部分开发者针对生态治理使用渠道分发对抗手段，利用线上和线下分发渠道的应用审核及管控力度存在差异性这一特点，实现只在线下分发不合规版本、套户等一系列违规行为。可见，不受应用市场上架审核规范限制的线下分发渠道给部分非良性开发者更多的可乘之机。在今年的检测治理工作中，安天移动安全发现一类线下分发渠道应用，存在严重的应用内广告内容问题。

在网赚品类中，有一类应用要求用户分享应用内容到社交平台并获取到有效阅读后才能获得奖励并提现，安天移动安全将这类应用称为分裂式网赚。这类应用有两种特点：一是这类应用不在主流渠道分发，包括各大应用市场和广告平台，而是通过线下 App 网站分发。这类应用由网站站长收集并提供应用下载二维码或下载链接，通过这种渠道下载下来的用户及由这些用户分享裂变出去的用户都将是二维码或下载链接提供者的下级用户，其收益都将被抽成一部分给站长。二是这类应用不像普通网赚应用使用大量广告位，通过用户观看点击广告来获取收益并分润给用户，而是通过分享链接的广告盈利。因为使用站长渠道下载出来的这类应用内的文章内容都是正常资讯，但是分享之后的链接会呈现黑五类广告。

这类分裂式网赚分发网站截图及下载页面（详见图 1-1、图 1-2），应用下载完成后打开界面（详见图 1-3），可以看到这里的应用界面没有广告，组成模块也很简单，主要分为“文章内容模块”“搜索模块”“邀请奖励模块”“提现模块”。当其他用户点击该应用的用户分享到社交平台的文章链接后展示页面，可以看到出现了黑五类广告（详见图 1-4）。

图 1-1 分裂式网赚分发网站截图

图 1-2 分裂式网赚分发网站下载截图

图 1-3
应用下载完成后打开截图

图 1-4
应用下载完成后打开截图

1.2 应用为绕过审核上架使用不实描述

由于网赚应用侵害用户权益的风险问题频发，多家应用市场不断缩紧对此类应用的审核规范。OPPO、vivo、华为、百度等应用市场规范中明确提到了多条针对网赚类应用的要求。安天移动安全发现部分网赚应用开发者为了绕过应用市场审核上架，使用了不实的应用描述和应用标签，并结合云控归因针对不同渠道下载的用户展示不同形式的应用。

如（图 1-5、图 1-6、图 1-7、图 1-8）所示，案例中的应用的文字介绍和内容图片均显示这是一款与农业相关的知识工具类 App，直接通过应用市场下载的应用是与描述相符的产品。通过点击头条广告跳转应用市场下载的应用则变成了一款模拟经营类的网赚应用。背后的实现原理是开发者在用户首次运行时上传用户下载渠道、机型等信息，通过云控归因来决定要给用户展示什么样的应用界面。

2. 新应用形态风险问题

在《移动互联网风险应用白皮书（2021）》中，安天移动安全提到随着泛应用的发展以及监管和厂商对应用侧的管控加强，移动互联网中除 App 外其他应用形态的风险问题也值得关注。

2022 年安天移动安全注意到当前移动互联网中另一种应用形态 -- 快应用正处于快速发展阶段。快应用是一种基于行业标准开发的新型免安装应用，具有免安装、即点即用、节省空间等优势。得益于用户触达链路短、开发成本低、市场大力扶持等特点，快应用用户规模和开发者正处于高速增长中。

当前快应用的用户、服务、内容三大生态均已形成一定规模，随之而来的是快应用中出现了诸多风险行为问题，严重侵害用户权益，阻碍行业生态健康发展。

图 1-5 农业相关的知识工具类 App 示例 1

图 1-6 农业相关的知识工具类 App 示例 2

图 1-7 农业相关的知识工具类 App 示例 3

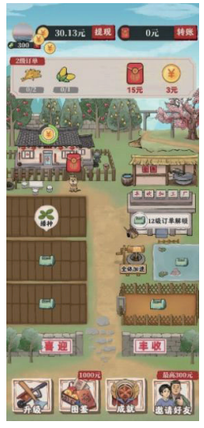


图 1-8 农业相关的知识工具类 App 示例 4

图 2-1 快应用“玩趣挑战”

下面安天移动安全将介绍快应用中存在的风险问题。

2.1 快应用拉起行为问题

快应用在用户不知情或无提示情况下被拉起主要包括两种形式：

第一种形式，用户访问 Web 链接时拉起快应用。

如（图 2-1）所示，用户在浏览器中访问某网页链接时，自动打开一款名为“玩趣挑战”的快应用。

第二种形式，App 内的广告自动跳转到快应用。

如（图 2-2）所示，用户在第三方 App 内查看广告时未做任何操作自动跳转到广告推送的快应用 。

2.2 快应用退出行为问题

指用户尝试退出快应用时，如点击回退键或 Home 键，快应用无法关闭（详见图 2-3）。

2.3 快应用广告行为问题

在对快应用风险问题进行分析检测的过程中，安天移动安全总结了以下四类广告问题：

(1) 快应用广告自动跳转

应用弹出的红包页会自动展示广告，具体表现为进入福利页时会弹出红包弹窗，在红包上方出现关闭图标后，自动跳转展示广告落地页（详见图 2-4）。

(2) 快应用广告误触下载

用户通过广告落地页拉起快应用后，进入小说阅读页面，然后自动触发广告点击，在未经用户同意的情况下跳转到应用市场下载安装目标 App（详见图 2-5）。

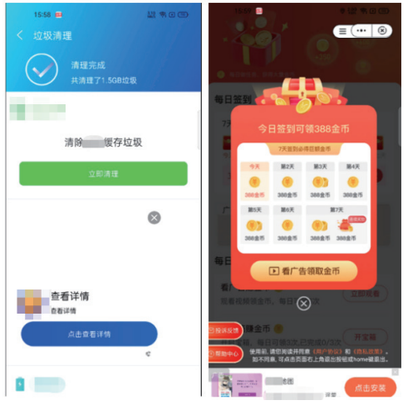


图 2-2 自动跳转到广告推送截图

图 2-3 快应用无法关闭截图

图 2-4 快应用广告自动跳转截图

图 2-5 快应用误触下载截图

(3) 快应用广告窗口无法关闭

该应用通过外部链接拉起后直接弹出红包插屏，点击右上角返回按键或者手机的返回按键都无法退出快应用（详见图 2-6）。

(4) 快应用广告诱导问题

开发者通过红包、福利奖励的方式诱导用户点击领取奖励按钮，触发广告点击跳转应用市场下载推广 App。

如（图 2-7）所示，链接拉起快应用后弹出红包弹窗，以金币奖励诱导用户点击领取，当用户点击“开”按钮或者点击红包弹框后触发广告点击，自动跳转到应用市场下载推广 App。

图 2-6 快应用广告窗口无法关闭截图

图 2-7 快应用中广告诱导问题截图

开发者通过频繁弹窗并放大广告点击按钮，或修改广告点击按钮描述引导用户点击广告。用户退出快应用时，快应用频繁弹窗，并将其中的“确认”、“点击领取”、“是”等按钮绑定为广告点击，当用户点击上述按钮后，跳转到广告推广页面。

2.4 快应用隐藏自身关闭菜单入口问题

指用户从外部网页跳转进入快应用后，应用界面中的菜单栏被隐藏。（详见图 2-8、图 2-9）

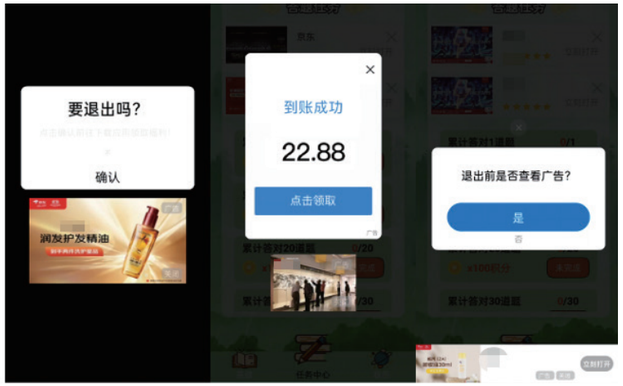


图 2-8 快应用隐藏自身关闭菜单入口

图 2-9 快应用隐藏自身关闭菜单入口

品类风险问题深度解析

联合实验室除了关注移动互联网中存在的通用性风险问题外，还针对一些品类特有的风险问题进行深入的跟踪监测和研究。在这个过程中安天移动安全发现品类应用的风险问题与该品类特有的商业变现和业务模式存在一定的关联性。

本章安天移动安全从品类视角出发，基于深入理解技术实现、产品功能、商业变现、行业产业生态的背景，对下沉交友品类、IAP 品类及网赚品类典型风险问题进行深度解析。

1. 下沉交友品类主要风险问题

下沉交友应用指的是面向三四线及以下群体的以男用户付费聊天为主要产品核心的陌生人交友应用。该品类的特点是男用户需要花钱才能和女用户交流，而女用户不需要花钱，其中文字信息按条收费，语音和视频按分钟或者秒收费。

1.1 公会诱导付费问题

对下沉交友应用而言，他们需要优质的女用户来留住男用户，并刺激男用户在平台多加充值消费。对黑灰产工作者而言，下沉交友行业这种在消费上的男女不平等性，让他们看到了商机，衍生出一类专门在该类应用中通过聊天、索要礼物来获利的职业 ---- 聊天员，以及大量招聘、培训女性“聊天员”以话术诱导男性用户付费或者送礼物的组织 ---- 公会。

对这类包含重度社交属性的平台来说，公会的存在本身就涉嫌欺诈用户，既促使男用户在“聊天员”的专业话术诱导下非理性处理个人财产，又根本无法满足其交友需求和期待。公会雇佣的聊天员还会以交换联系方式、线下见面为由不断向用户索要礼物，而因为其身份的特殊性非但不能满足用户的实际需求，还会对用户的感情和财产构成双重欺诈，因此这类应用经常收到大量用户投诉。

安天移动安全在长期持续关注婚恋交友应用侵害用户权益行为的过程中发现，诱导消费、色情低俗等问题的出现与公会有着直接的关系，行业内公会渗透度越高，侵害用户权益的问题越普遍，公会是下沉交友应用侵害用户权益问题滋生的根源。由于不良公会的加入可以带来 ARPU（每用户平均收入）的大幅提升，平台也会因此获益。在利益的驱使下，平台直接或间接与公会合作，雇佣女聊天员、使用聊天辅助工具，以“真实交友”之名，行欺诈获利之实，利用诱导用户充值、刷礼物等手段骗取男性用户的钱财，下沉交友平台诱导消费、低俗问题频发的背后是下沉交友公会的算计和套路。

与直播不同，交友通常是以一对一的形式出现，用户之间私密性更强，同时迫于监管的压力，下沉交友应用的公会一般没有专职的运营人员，直接由公会长负责女聊天员、代理的招募和培训。代理还可以发展二级代理，但受约定提成比例的限制，为了防止自身利润被稀释，

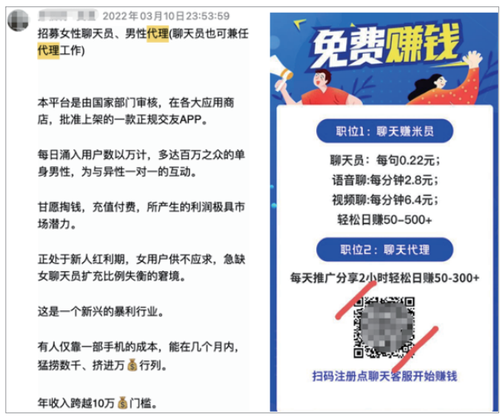


图 1-1 一对一交友方式截图

鲜少有代理会招收多个下级，因此一般不会出现多层代理的情况。（详见图 1-1）

在利益分配、结算方式上，直播与下沉交友的公会也存在明显区别。直播行业的公会是合理合规的存在，直播平台可以直接与公会按照协议和流水数据进行结算，公会再对公会长、主播完成内部结算。据了解，直播的公会通常可以分配 60%～70% 的的利润，经过最终测算，主播收益基本维持在所有结算收入的 40%～50%。而在本应为用户解决真实交友需求的下沉交友平台上，公会的存在并不合理，对于平台的用户来说也不具备价值。下沉交友平台为了规避监管风险，通常以线下的方式与公会、代理进行结算，为了让交友更“真实”，女聊天员则直接通过平台提现，从而实现财务上的“物理隔离”。在分配方面，平台、公会、代理以及聊天员分成比例一般维持在 5：1：1：3。（详见图 1-2）

1v1私聊（偏重做1V1私聊）扶持政策

享受政策要求：公会主播人数≥10人

分成	板块	主播	公会长		特殊扶持	
		40%	15%	5%	奖励/周结	500/1000/3000元
结算方式	1V1私聊	自提日结算	周结算	满足周流水5w元周结算	要求	公会一周达标流水300元+消息回复率75%的主播需10人 公会周流水达3000元，奖励500元 公会周流水达5000元，奖励1000元 公会周流水达10000元，奖励3000元
分成	家族派对	40%	10%			
结算方式		自提日结算（包含家族+派对流水）	自提日结算（包含家族+派对流水）			

图 1-2 1V1 私聊（偏重做 1V1 私聊）扶持政策

对于中小型平台来说，引入公会可以极大缓解供给和需求两端的压力，公会借助自身资源优势统一招募、培训、管理旗下聊天员，快速提升平台 ARPU 值的同时也缩短了平台买量回收周期，平台则得以聚焦在平台功能开发和买量推广上。一般情况下，在中小型平台上，公会往往拥有更高权重和话语权，同时也会得到一些平台给予的“特权”，比如账号解封、功能权限、流量扶持等，甚至还有部分平台帮助公会 “筛选” 大哥，就像“3·15”报道的案例中，用户成为平台和公会待收割的“韭菜”。

1.2 应用推送机制具有明显诱导用户付费的目的

除了公会问题外，安天移动安全在持续检测和分析中发现，部分平台通过向用户频繁推送大量模板化消息，诱导用户回复或使用聊天功能，进而促进付费。这些行为有时候与应用内用户无关，并非女用户主动发起的消

息搭讪或视频通话，而是开发者为了促使男用户充值付费，通过推送机制营造一种平台内大量女用户积极主动的假象。

下面是安天移动安全总结的一些推送机制有诱导用户付费目的的风险行为。

(1) 使用提前录制好的视频文件，向用户发起视频邀请

在部分平台上，视频通话功能也需要按分钟计费，且一般由男用户向女用户支付，应用向男用户主动推送一些提前录制好的视频通话邀请，邀请人往往是男用户从未交流过的对象，邀请页面利用女性用户的视频诱导用户付费进行接听。

以下图视频通话需要付费的交友应用为例，应用在用户使用过程中会主动弹出视频通话邀请，同时会展示录制好的女性视频，诱导用户付费接听，更有些应用在后台时也会频繁弹出视频通话邀请。

如（图 1-3）所示应用为例，用户在正常浏览时，会收到提前录制的视频发起的视频通话邀请。

(2) 向用户推送的消息具有相同或高度相似的消息内容和形式，或者明显基于模板生成

部分交友类应用在用户注册、登录时推送大量的“交友信息”，这类信息发送频次高且有固定话术的痕迹，疑似平台为新注册用户“量身定制”并基于模板生成的自动化消息推送，以达到增加用户留存和诱导用户付费的目的。

如（图 1-4）所示为例，用户进入应用后短时间内收到大量打招呼消息，应用以非正常方式向用户发送陌生人打招呼消息，且回复消息需要收费。

如（图 1-5）所示为例，应用给用户发送的消息形式高度相似，有模板化痕迹。

2. IAP 品类付费功能不规范问题

IAP 品类指的是以应用内购买服务为主要收益来源的应用类型。这类应用主要通过其功能吸引用户，并设置付费功能，用户可以选择充值付费购买更多服务。涉及到用户资产的 App 支付问题直接关系到用户的切身利益，该类风险问题也是联合实验室重点关注的问题之一。

在长期持续关注 App 支付环节侵害用户权益问题的过程中安天移动安全发现，移动应用程序诱导付费、强制自动续费等严重侵害用户权益的行为曲解了产品付费

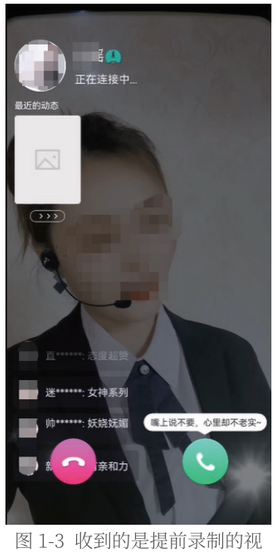


图 1-3 收到的是提前录制的视频发起的视频通话邀请

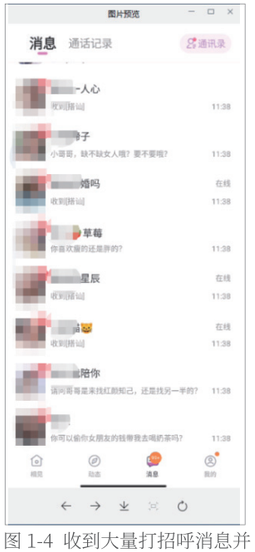


图 1-4 收到大量打招呼消息并向陌生人自动回复收费消息

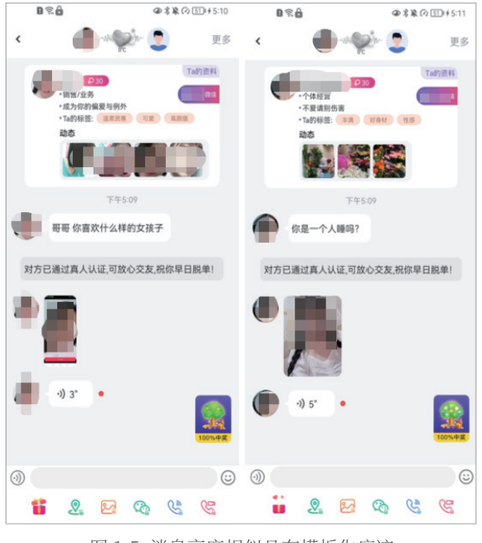


图 1-5 消息高度相似且有模板化痕迹

的应有意义，造成用户财产受损，干扰了移动互联网生态健康发展。下面安天移动安全将分享 IAP 品类中付费功能不规范的问题。

2.1 虚假特惠活动等宣传诱导付费

虚假宣传诱导付费一般指应用以低价试用或免费试用作为噱头，吸引用户进行试用体验，实际是为了捆绑销售其他付费服务。具体表现形式有：

(1) 低价捆绑

以低价试用或免费试用诱导用户进行付费，但暗自捆绑了其他付费项目。

如（图 2-1）所示，案例为某小说 App，包含多款“会员试用套餐”均捆绑自动续费连续包月服务，如 7 天试用仅需 1 元，想要体验试用服务必须同意自动续费条款。

图 2-1 某小说 App 中“会员试用套餐”均捆绑自动续费连续包月服务

(2) 虚假特惠活动

一般指应用通过突出宣传引人误解的优惠信息，模糊或隐藏关键信息，引起用户对优惠活动的误解，诱导用户进行付费购买（详见图 2-2）。具体有：

虚假限时：在活动期间，用户并未享受到实际的优惠价格，常见为倒计时促销等；

虚假限额：宣传限量获得，但名额实际不受限。

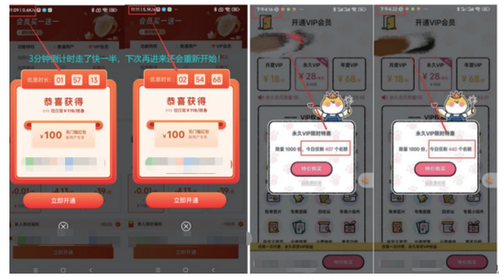


图 2-2 虚假特惠活动

2.2 红包、提现等福利诱导用户订阅自动续费服务

安天移动安全发现有些应用会以提现、领取现金、领取红包或优惠福利等词条来诱导用户并通过精心设计的福利页面来降低用户警惕，诱导用户订阅自动续费服务。

这种风险问题表现方式如下：

(1) 提现诱导：应用以红包提现诱导用户授权订阅第三方支付平台自动续费服务。

(2) 优惠福利诱导：应用提供虚假的优惠福利并设置倒计时，来诱导用户授权订阅第三方支付平台自动续费服务。

如（图 2-3）所示案例的网赚应用以自动提现诱导用户授权第三方支付平台，用户同意后跳转到伪造的第三方支付平台自动续费签约页面，然后使用虚假的红包奖励和优惠福利作为诱饵，设置倒计时诱导用户点击。当用户点击同意签约，跳转到真正的第三方支付平台自动续费签约页面，此页面中的服务介绍只有扣款内容，并没有福利相关说明，但因为上一步的伪造页面与当前页面极为相似，容易导致用户信以为真，或疏忽了扣款内容，签订了自动续费服务。

首次进入该应用会有红包弹窗，每次通关游戏后也会有红包奖励弹窗。

点击应用内的任何红包或提现按钮会有提现弹窗提示，要求授权第三方支付平台后才能自动提现（详见图

2-4）。

点击确认按钮后会先跳转到应用内自建的伪装第三方支付平台签约的页面，在该页面的服务详情中会显示应用内设置好的福利说明，但该福利实为虚假福利。此外，该页面还会设置倒计时和高亮显示，用户点击后跳转真正的第三方支付平台签约页面。若用户没有点击行为，倒计时结束后也会进行自动跳转（详见图 2-5）。

2.3 自动续费设置不规范

在长期持续关注 App 支付环节侵害用户权益行为的过程中安天移动安全发现，应用为提高用户的付费率、续费率，利用低价或免费使用的噱头，捆绑用户开通自动续费服务，续费前无提醒且难以取消，严重侵害用户权益，造成用户财产受损，遭到用户大量投诉。具体表现形式有：

(1) 续费前无提醒

该问题指的是部分应用续费扣款前 5 日，无明确的续费提示信息。据媒体报道和用户投诉情况，大量用户在 App 自动续费、扣款前没有收到任何通知或提醒，在不知不觉中就被扣了款，造成财产损失。安天移动安全在对 App 抽样检测、调研中发现，大量 App 无论是在支付购买页面还是相关协议中均未提到扣费提醒相关信息。

(2) 续费取消难

该问题指部分应用未提供独立的自动续费管理或取消功能，或虽提供该功能但是位置隐蔽。App 自动续费取消难也是用户投诉主要问题之一，安天移动安全发现 App 未提供独立的自动续费管理入口或取消功能的情况较为普遍，有些 App 虽然提供该功能但是位置非常隐蔽，取消方式复杂，操作难度大。

如（图 2-6）所示案例为某漫画 App 页面上，没有向用户提供取消订阅（续费）模块，取消订阅需查看自动续费协议，且隐藏较深，用户需进行大量复杂的操作才能取消。据用户投诉情况，即使按照提示顺利取消，仍然被扣费。

图 2-6 没有向用户提供取消订阅（续费）模块

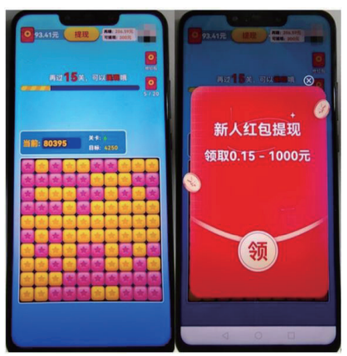


图 2-3 新人红包提现弹出页面

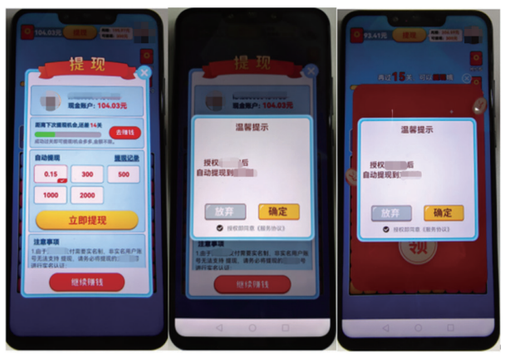


图 2-4 要求授权第三方支付平台界面

图 2-5 伪造签约页面

2.4 价格欺诈

安天移动安全发现，部分应用开发者为提高用户的付费率收益，在产品服务购买、支付阶段，利用云控算法区别定价、低价诱导高价结算等价格欺诈手段诱导用户付费，严重侵害用户权益，造成用户财产受损，遭到用户大量投诉。

应用价格欺诈行为常见形态主要有以下两类：

(1) 云控算法，区别定价

应用在未标明交易条件的前提下，通过云控算法等技术手段，同一功能或服务对不同用户制定不同的价格，导致用户权益受损。

在某节拍器 App 中，未标明交易条件的前提下，就同一会员服务，在同一时间，对不同的用户实行区别定价。同样是“永久会员”，向不同用户分别定价 162 元和 110 元（详见图 2-7）。

经过分析发现，该应用在本地存在定价配置文件，该配置文件也可随时通过云端更新，里面包含了共 13 种价格组合。云端还会更新定价配置逻辑，每次新用户安装，会随机选择一种定价组合（详见图 2-8、图 2-9）。

(2) 低价诱导，高价结算

应用不标示或者显著弱化标示实际价格，以低价诱骗消费者，以高价进行结算。

某扫描 App 会员购买界面上，以 0.01 元 / 月的价格诱导用户进行付费，弱化实际结算价格，用户在付款时稍不注意就会支出超出预期的费用（详见图 2-10）。

图 2-7 不同用户区别定价

图 2-8 应用在本地存在定价配置文件并随时通过云端更新

图 2-9 随机选择一种定价组合

3. 网赚品类主要风险问题

网赚应用指的是用户通过完成指定的任务获取现金回报，而应用运营者则主要通过流量投放实现变现的一类应用。这类应用“提现”来吸引用户进行任务，比如让用户看数条视频后可提现等等。无论网赚应用的任务是玩游戏还是看视频又或者是充电、走路等，用户在完成这些任务过程中都是要看广告的，广告收益就是这类应用的主要收益来源。

安天移动安全发现部分网赚应用为了快速回本、增大收益，试图在各个环节增加用户提现难度，如设置假

图 2-10 低价诱导 高价结算

提现、不一次性明示提现规则，甚至部分应用还会使用欺诈性的广告素材，在用户身上获取更高的收益，更有甚者，还会出现上文中提及的诱导用户订阅自动续费服务问题。

3.1 假提现

“假提现”指的是某些做任务赚钱类 App 在用户达到其宣称的提现标准时却告知还需完成其他任务方可提现，以不断增加提现条件，设置提现门槛等方式迫使用户投入更多时间使用其 App 的现象。在应用商店根据提现相关的关键词进行检索得出数据，此类 App 在架的有 908 款，负面评价用户数量多达 20033 人。

此类应用最初以小额提现秒到账的方式吸引用户使用，但在大额提现时通过屡次设置虚假条件欺骗用户，给用户营造一种很快就能提现的错觉，这样即使难度增加，用户也不想放弃现有的奖励，之后在提现阶段通过各种不合理途径拒绝给用户支付。实际上，App 运营商只需以最初支付的小额提现的成本即可获得高于该成本几十倍的利润，然而用户却白白耗费时间和精力做任务、看广告，沦为其营利工具。

以下为“假提现”的示例：

(1) 达到提现门槛之前，提现页面截图如（图 3-1）所示，提现界面宣称“满多少提多少”，当选择提现 300 元时，页面下方显示提现条件为“余额满足 300 元”，并未提示其他附加条件；

(2) 达到门槛后，提现页面截图如（图 3-2）所示，当用户余额达到 300 元后，提现条件变为“连续签到 5 天”；

即使用户完成签到任务，提现条件可能还会增加“邀请好友”等其他任务，以此类推，层层加码，不断为用户设置更多的提现门槛。

图 3-1 达到提现门槛之前截图

图 3-2 到达门槛后截图

3.2 未一次性明示提现规则

“未一次性明示提现规则”指的是应用未在提现界面直接告知用户完整的提现规则，用户需要去其它地方才能查看完整的提现规则。此类应用一般只在提现页面展示较为容易实现的提现条件，而实际用户提现还有其它的条件需要达到。

以下为相关示例：

(1) 提现页面只展示金额达成条件（详见图 3-3），但是实际在用户协议中还有其它条件未展示（详见图 3-4）。

图 3-3 显示金额达成条件

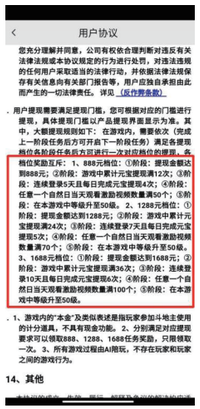


图 3-4 其它附加条件

(2) 有些应用的提现页面虽然为用户提供了查看完整提现规则的快捷入口，但提示形式依然不够显著。用户不一定会去点击或者去其它地方查看相关的规则，并没有对用户造成很好的明示作用（详见图 3-5、图 3-6）。

3.3 欺诈性广告素材

(1) 话费券广告

此处的话费券广告指的是应用内出现以【充值 19.9 元得 100 元话费】为噱头吸引用户付费的广告，然而用户实际获得的并非“话费”，而是碎片化的“话费券”

图 3-5 查看完整提现规则入口不显著案例 1

图 3-6 查看完整提现规则入口不显著案例 2

图 3-7 弹出“充值 19.9 元得 100 元话费”的广告

图 3-8 弹出手机话费券领取页面

图 3-9 抽奖池显示奖品均为手机

（可能是 20 张 5 元充值券），并且充值时有严格的限制条件，如：必须下载特定应用，在该应用内进行充值才能使用优惠券、每次充值必须达到 100 元才能使用一张 5 元优惠券。且整个充值流程对用户权益没有保障，当用户反悔想要退还已充值钱款时无法找到退还渠道，申诉无门。在违规投诉平台使用关键词“话费券”进行检索，得到 13908 条投诉结果， 其中大部分投诉问题为“话费券并未到账”。

以下为相关示例：

1) 应用内完成签到时弹出“充值 19.9 元得 100 元话费”的广告（详见图 3-7）。

2) 点击进入后却显示获得的是“话费券”（详见图 3-8）。

(2) 盲盒广告

某互动广告页面，无论抽到哪个奖品均显示【恭喜砸出大奖】，让用户误以为自己中奖，只需支付 39 元即可领取价值几千元的手机。然而实际上，用户支付的 39 元获取到的仅为一次抽奖机会，奖品形式为随机盲盒，并非广告引导的手机类奖品，且盲盒不支持退换。

以下为相关示例：

1) 抽奖池显示奖品均为手机；由广告页面可知供应商名为“XX 盒子”（详见图 3-9）。

2) 只要点击“免费抽奖”就会出现【恭喜中奖】界面，提示【付款 39 元即可提货】，奖品页面的手机图片具有误导性（详见图 3-10、图 3-11）。

图 3-10 点击“免费抽奖”后弹出界面

图 3-11 奖品页面手机与实际奖品不符

总结

2022 年，安天移动安全 -OPPO 联合实验室在坚持安全普惠原则，协同移动互联网中多方共同构建移动互联网风险应用体系。凭借十余年的技术积累和实战经验，与监管部门、手机厂商等产业伙伴一同深度配合，积极参与到产业安全洞察、终端应用检测、应用市场上架审核等多个重要环节，最终通过应用安全治理为终端消费者使用 App 时的自身权益保驾护航。但是应用治理只是作为一种手段，而不是目的，最终目的是通过建立基于“良赢治理”，促进产业良性发展并在保障用户利益、增强用户体验的前提下，形成围绕移动互联网产品和服务质量的良性竞争生态，达成个人用户、企业、社会和国家机构的多方共赢目的。本报告最终目的是期望以此引发生态各方对现今的移动终端用户权益和应用安全风险现状的讨论，共同推进移动互联网应用生态的净化发展。

02 移动互联网风险应用典型问题解析

引言

数字经济时代，如何合法合规地使用数据，保障用户的隐私和权益已成为政府监管部门关注的重要问题。为净化网络环境，营造清朗网络空间，2022 年 12 月 12 日，中央网信办开展“清朗·移动互联网应用程序领域乱象整治”专项行动，深入治理 App、小程序、快应用等应用程序乱象。其中明确提到严厉打击各类借虚假免费试用、特惠活动或异性聊天等诱导用户付费的行为；坚决打击各类以赚钱为幌子欺骗用户下载使用，设置多种提现障碍的行为；从严惩处各类诱导未成年人充值消费，强制自动续费等严重侵害用户权益的行为。着力解决损害用户合法权益的突出问题，保障用户合法权益。

一直以来，上述各类移动互联网应用程序领域乱象都是安天移动安全重点关注和治理的对象，同时依托“安鉴”风险检测预警平台就曾针对性地进行过多轮公开曝光，并配合监管部门、终端厂商等产业链各方进行了生态治理，取得了阶段性积极成果。

为积极配合中央网信办开展“清朗·移动互联网应用程序领域乱象整治”专项行动，安天移动安全不仅在“安鉴”风险检测预警平台积极上线了相关的违规应用曝光、问题定义和解读、监管政策与媒体动态等功能；同时，还特别精选摘编了各类问题典型案例，进行集中披露与深度解析。未来，安天移动安全仍将继续加大对各类侵害用户权益问题的检测力度，并积极与产业链各方配合，共同抬升行业底线，保障广大用户的合法权益。

快应用生态下的用户安全问题亟待重视和规范

近年来，得益于用户触达链路短、开发成本低、市场大力扶持等优势，即点即用、免安装的快应用及其用户规模实现高速增长，但随之而来的诸多风险行为、违规问题严重侵害用户权益。

在长期持续关注当前移动智能终端安全态势过程中，安天移动安全“安鉴”风险检测预警平台发现，部分快应用中存在启动及退出问题、广告行为问题、归因差异化触发和展示等诸多风险行为，破坏用户使用体验的同时严重侵害了用户权益。

现将部分快应用风险问题披露如下：

1．快应用启动和退出行为问题

“安鉴”风险检测预警平台在持续关注快应用生态潜在风险问题的过程中发现，部分快应用存在无法退出或关闭的问题。当用户尝试通过“返回键”、“Home 键”退出快应用时无法完成，破坏了用户的正常使用体验。

在某砍价快应用中，进入砍价的详情页面后，右上角返回按钮和手机系统返回按钮失灵导致无法退出快应用。

“安鉴”风险检测预警平台在对该快应用分析中发现，该快应用隐藏了系统退出菜单栏，同时“劫持”了

图 1 强制跳转广告页面

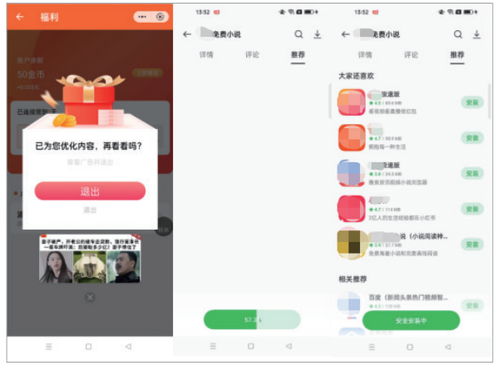


图 2-1 广告及自动下载安装推广应用

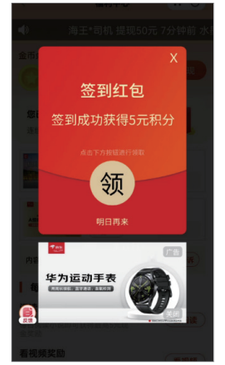


图 2-2 签到红包及虚假关闭按钮

页面左上方的返回和系统返回按钮并绑定广告跳转行为，导致快应用无法正常退出且强制跳转广告页面。(详见图 1)

2．快应用广告行为问题

“安鉴”风险检测预警平台在对快应用检测分析中发现，快应用商业变现主要模式仍然是流量变现，在流量利益的驱动下，快应用中滋生了误导点击和自动下载安装、虚假关闭诱导用户点击、快应用自行跳转至其它链接等诸多广告问题。

案例一：误导点击和自动下载安装

某辅助睡眠快应用在用户退出时通过容易引起误解的内容，诱导用户点击退出按钮从而触发广告，广告触发后未经用户同意自动下载安装推广应用。(详见图 2-1)

案例二：设置虚假关闭诱导用户点击

用户进入快应用签到时弹出签到红包页面，点击红包右上角的“X”会跳转广告。经检测发现，该弹窗并未设置关闭按钮，“X”为虚假关闭按钮。(详见图 2-2)

案例三：快应用自行跳转至其它链接

在进入福利页时该快应用弹出红包弹窗，在红包上方出现关闭图标后，自动触发广告点击事件跳转应用下载页面（已安装故显示“打开”）。(详见图 2-3)

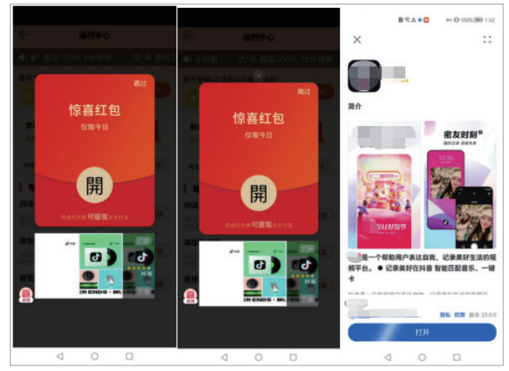


图 2-3 红包弹窗及跳转应用下载页面

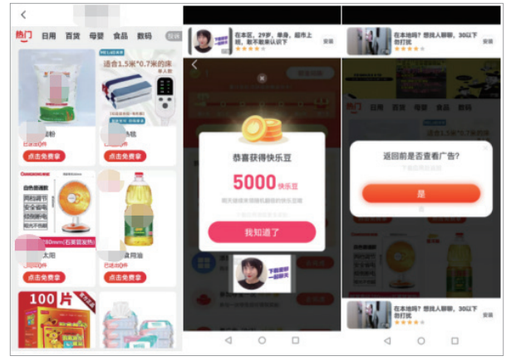


图 3-1 通过地理位置对用户进行差异化显示

3．快应用运行时归因问题

“安鉴”风险检测预警平台在对快应用运行行为的分析检测中发现，快应用存在基于用户渠道归因，实现风险内容的用户差异化展示和风险行为的差异化触发，从而规避监管和审核。

案例一：该快应用通过当前地理位置信息对用户做归因实现问题行为的差异化，下发不同的云控参数来控制广告行为，从而逃避审核和监管。（详见图 3-1）

案例二：快应用通过对分发渠道的归因实现内容的差异化显示，通过某头部广告平台下发的链接跳转拉起进入该应用后，发现该快应用下有较多的色情小说内容。（详见图 3-2）

图 3-2 通过分发渠道对用户进行差异化显示

图 3-3 快应用中心显示内容无问题

但在应用市场内的快应用中心进入该应用，内容无问题。（详见图 3-3）

除此之外，“安鉴”风险检测预警平台在长期持续关注快应用生态潜在风险问题的过程中发现，还存在快应用在用户不知情或者无提示的情况下被拉起、虚假提现等诸多威胁用户安全的风险问题，在用户规模高速增长的今天，快应用侵害用户权益问题亟待重视。

中央网信办在“清朗·移动互联网应用程序领域乱象整治”专项行动中明确指出，**要深入治理包括快应用在内的应用程序乱象问题，其中重点提到了无法关闭等快应用启动和退出问题**，以及诱导点击捆绑下载、自行跳转等快应用广告行为问题，保障广大用户的合法权益。

作为网络健康生态的助推者，为保障广大用户的合法权益，促进快应用生态良性发展，一方面，“安鉴”风险检测预警平台上线快应用相关的违规应用曝光、问题定义和解读、监管政策与媒体动态等功能，帮助开发者及时了解相关政策、法规并自查自纠。

另一方面，**安天移动安全针对快应用违规问题已建立系统性发现能力，接下来将加大对快应用违规问题的分析和检测力度，并配合监管部门、手机厂商及产业链各方进行生态治理**，助力移动应用生态健康有序发展。

安天移动安全多举措助力婚恋社交应用用户权益保障和开发者安全赋能

随着移动互联网技术的快速发展和智能终端的广泛普及，网络社交的重心逐渐从以往的 PC 端向移动端迁移，移动社交凭借更加便捷有效的互动沟通优势，吸引了众多用户的使用，各类婚恋社交应用或平台如雨后春笋般涌现，但与此同时，诱导用户消费、低俗色情等用户安全问题频发，严重侵害了广大用户的合法权益。

1. 安天移动安全对婚恋社交应用的风险判定逐渐成为行业共识

在市场和用户规模高速增长的背景下，部分婚恋社交应用开发者在商业利益的驱使下，利用诱导付费、色情引流等违规手段给用户带来不可预知的风险，严重侵害了广大用户的合法权益。早在 2020 年，安天移动安全立足用户安全，就开始关注婚恋社交类平台侵害用户权益的问题，一方面不断加大技术发现与取证的力度，另一方面对其典型问题进行了多次公开曝光披露。

自 2022 年央视 315 曝光直播交友平台诱骗用户刷礼物、打赏乱象以来，监管部门开展了一系列专项整治行动，安天移动安全公开曝光的婚恋社交应用诱导消费、低俗色情等多个问题都成为重点治理对象。中央网信办“清朗·移动互联网应用程序领域乱象整治”专项行动中提到的异性聊天等诱导用户付费行为，安天移动安全就曾在《移动互联网风险应用白皮书（2021）》中进行了重点介绍和取证分析。

安天移动安全现已初步建立针对婚恋社交应用的系统性发现能力，伴随对婚恋社交应用产业上下游认识的不断加深，对婚恋社交类应用侵害用户权益问题的判定正逐渐成为监管部门、终端厂商等产业链上下游各方进行生态治理的共识。

2. 下沉交友公会渗透是侵害用户权益问题频发的根源

下沉交友是婚恋社交的一个细分品类，在长期持续关注下沉交友应用侵害用户权益行为的过程中，“安鉴”风险检测预警平台发现，诱导用户消费、色情低俗等问题的出现与下沉交友公会有直接的关系。公会渗透越高，侵害用户权益的问题越普遍，诱导消费、低俗问题频发的背后是下沉交友公会的算计和套路，下沉交友公会的存在扭曲了产品本应服务大众的初衷，成为下沉交友应用侵害用户权益问题滋生的根源。

所谓下沉交友公会一般是指以高回报、低成本、零门槛为诱饵招聘聊天员，聊天员借助平台相关打赏、消费功能，以相亲、交友的名义，通过文字聊天、视频语音互动等方式诱导用户消费，最终根据约定比例与聊天员、甚至下沉交友平台进行分成的组织。

由于下沉交友公会的存在与否，直接关系到广大用户的权益保障和财产安全，安天移动安全基于对下沉交友应用的全量发现和实时分析能力，再结合线下情报研判和加权算法，形成了“公会侵入度”动态检测标准，实现了针对下沉交友公会渗透情况的量化，今后将基于安天移动安全高频高覆盖的动态取证，对下沉交友应用进行持续跟踪检测。（详见图 1）

3. 安天移动安全多举措助力婚恋社交应用用户权益保障和开发者安全赋能

为保障广大用户的合法权益，同时帮助开发者规避合规风险，筑牢快速、可持续增长的安全能力防线，安天移动安全基于十余年的攻防实战经验和技术积累，结合婚恋社交开发者自查自纠能力不足的痛点和风险防范

公会侵入度测评

违规点TOP10

典型案例分析

图标	应用名称	上架企业名称	公会侵入度排名	公会侵入度趋势	公会侵入度监测	检测详情
	她悦	杭州梨鸣网络技术有限公司	前8%		突增	详情
	甜伴交友	太方科技（深圳）有限公司	前1%		持续高	详情
	期伴	杭州梨鸣网络技术有限公司	前5%		持续高	详情
	佳偶成双	杭州追一网络技术有限公司	前6%		持续高	详情
	伊糖	太方科技（深圳）有限公司	前6%		持续高	详情
	月话	广西心娱科技有限公司	前13%		持续高	详情
	心享	海南黄蜂科技有限公司	前13%		持续高	详情
	同城来聊	深圳聊欢网络科技有限公司 深圳市诚兴嘉业科技有限公司	前2%		上升 持续高	详情
	蜜遇	深圳市艾森互动科技有限公司	前4%		上升 持续高	详情
	聊伴交友	昊韵晟世（大连）网络科技有限公司 广州凯帽网络科技有限公司	前9%		上升 持续高	详情

图 1 公会侵入度详情：https://dev.avlsec.com/public-pages/show-page

诉求，创新研发了针对婚恋社交应用的风控体系 SaaS 产品，高效识别公会高危女用户及其风险设备，为开发者进行安全赋能，促进婚恋交友行业良币驱逐劣币的良性生态的形成。

同时“安鉴”风险检测预警平台还上线了违规问题定义和解读、监管政策等功能，帮助开发者了解监管及合规政策，并提供整改申诉、复测入口，保障用户权益的同时为开发者降低风控管理成本。

接下来，安天移动安全立足用户安全，将继续加大对婚恋社交类应用的检测力度，对公会侵入度居高不下且严重侵害用户权益的应用进行公开曝光，同时向终端用户发送风险预警，并配合监管部门、手机厂商及产业链各方进行行业生态治理，助力婚恋交友生态良性、有序健康发展。

诱导付费、强制自动续费，部分移动应用程序（App）仍在“收割”用户

自 2022 年起，安天移动安全“安鉴”风险检测预警平台就曾对应用诱导用户付费等侵害用户权益行为进行了多轮公开曝光，并配合监管部门、终端厂商等产业链各方进行了生态治理，取得了阶段性积极成果，但虚假免费试用、虚假特惠活动等诱导用户付费问题仍然广泛存在。

在长期持续关注当前移动生态侵害用户权益问题的过程中，“安鉴”风险检测预警平台发现，虚假免费试用、虚假特惠活动问题主要表现为以下几类：

(1) 虚假免费试用

一般指应用以低价试用或免费试用作为噱头，诱导用户进行试用体验，实际是为了捆绑销售其他付费服务。具体表现形式有：

1) 低价捆绑：以低价试用或免费试用诱导用户进行付费，但暗自捆绑了其他付费项目。

2) 强制自动续费：在低价或免费试用结束后，应用在未告知用户的情况下进行强制自动续费。

(2) 虚假特惠活动

一般指应用通过突出宣传引人误解的优惠信息，模糊或隐藏关键信息，引起用户对优惠活动的误解，诱导用户进行付费购买。具体表现形式有：

1) 虚假限时：在活动期间，用户并未享受到实际的优惠价格，常见为倒计时促销等。

2) 虚假限额：宣传限量获得，但名额实际不受限。

3) 虚假折价：活动折扣并没有实际起到优惠的效果，甚至高于原价。

其中部分典型问题解析如下：

1. 虚假免费试用

在某头部扫描类应用中，存在低价试用、捆绑自动续费问题。应用声称的所谓 1 元 7 天试用，实际是为了推广自动续费服务。而该自动续费服务，用户却难以在应用设置中进行取消，进而进一步造成了强制自动续费的问题。（详见图 1-1）

上述开发者开发的另一款名片应用中，还存在通过虚假的用户购买记录，诱导用户开通自动续费功能的问题。经技术检测发现，所谓的购买记录实际上是由云控下发 js 代码中控制生成，购买用户名称和时间都是虚假的，并非真实的用户购买记录。（详见图 1-2）

图 1-1 应用付费界面

图 1-2 购买记录界面

2. 虚假特惠活动

应用虚假特惠活动问题以虚假限时和虚假折价最为常见。

2.1 虚假限时

虚假限时一般表现为应用通过设置虚假的优惠倒计时信息，引起用户的紧迫感，诱导用户进行付费，实际倒计时并不能影响优惠结果。

在某扫描类应用中，应用内优惠活动在限时倒计时结束后，优惠券依然存在，所谓的限时优惠实则是个幌子。（详见图 2-1）

图 2-1 某扫类描应用优惠券

图 2-2 某学习类应用优惠券

同样的，在一款学习类应用中，应用所谓的优惠活动倒计时结束后，倒计时重新开始，优惠有名无实。（详见图 2-2）

2.2 虚假折价

此类问题主要表现为应用不标示或者显著弱化标示实际价格，以低价诱骗消费者，以高价进行结算，严重侵害用户合法权益。

在两款识别、扫描类应用中都出现了低价诱导、高价结算的问题。在这两款应用中，突出显示“0.01 元”、“永久”等字样，弱化实际需要支付的金额，很容易引起用户误解，诱导用户付费。（详见图 2-3）

图 2-3 付费界面

同样的情况也出现在一款盲盒应用中，应用突出显示“首抽 0 元”，最终支付显示必须购买 5 连抽。通过引起用户误解的方式，诱导用户进行购买。（详见图 2-4）

移动应用程序诱导付费、强制自动续费等侵害用户权益行为曲解了产品付费的应有意义，应用开发者应该通过不断提升产品、服务质量来提高付费率，而不是利用诱导付费、强制自动续费等算计和套路用户的方式，应用开发者侵害用户权益提升付费率的行为无疑是饮鸩

图 2-4 某盲盒应用付费界面

止渴之举，与产品服务大众的初衷相悖，最终造成用户的反感和流失。

中央网信办在“清朗·移动互联网应用程序领域乱象整治”专项行动中重点提到了，要严厉打击借虚假免费试用、特惠活动或异性聊天等诱导用户付费行为。作为网络健康生态的助推者，安天移动安全基于对违规应用的系统性发现能力，将加大对虚假特惠活动、虚假免费试用等诱导用户付费行为的检测力度，配合监管部门、手机厂商及产业链各方进行生态治理，同时向终端用户发送风险预警，保护用户权益。

同时，“安鉴”风险检测预警平台将在“安鉴披露”上线应用付费侵害用户权益问题的相关功能，对相关风险应用及其开发者进行公开曝光。伴随安天移动安全对移动应用风险的判定逐渐成为行业的共识，“安鉴”风险检测预警平台公开披露、曝光的违规问题及相关应用也成为监管、厂商等产业链上下游进行生态治理的重要依据。

虚假优惠、涉嫌变相赌博风险，盲盒类应用衍生问题亟待规范

早在 2021 年，安天移动安全就关注到了盲盒类应用侵害用户权益行为及问题，在《移动互联网风险应用白皮书（2021）》中对盲盒应用风险进行重点介绍和取证分析。2022 年以来，安天移动安全基于对盲盒应用风险的系统性发现能力，并配合监管部门、终端厂商等产业链各方进行了生态治理，取得了阶段性成果。

在持续关注盲盒类应用侵害用户权益问题的过程中，安天移动安全“安鉴”风险检测预警平台发现，盲盒类应用衍生出了新的问题，且侵害用户权益的手段更加隐蔽，主要表现为以下两类：

(1) 虚假优惠活动

除常见的虚假低价优惠问题外，盲盒应用中出现验证夸大中奖概率诱导用户付费抽取的行为：

1) N 抽必中：使用“ 百分百”、“必中”等绝对话语进行营销推广，实际中奖概率无法保证，诱导用户付费。

2) 虚假中奖提示：推广宣传中刻意突出“中奖信息”，但弱化或隐藏其盲盒属性。

(2) 涉嫌变相赌博风险

盲盒应用奖品回收、变现存在现金博弈风险，同时宣传以小博大诱导投机，存在变相赌博风险：

1) 回收变现存在现金博弈风险：盲盒回收构成随

机玩法的定向转移，形成消费资金再变现的交易闭环，导致产生现金博弈的风险。

2） 宣传以小博大诱导投机，存在变相赌博风险：通过设置高价差对比机制或刻意凸显原本极低或本不存在的高收益机会，诱导用户进行投机炒作。

图 1-1 应用宣传素材中出现的绝对话语

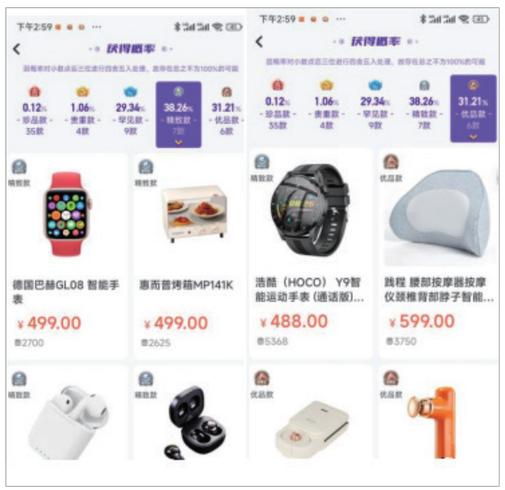


图 1-2 公布概率

1. 虚假优惠活动

除常见的“新人首抽0.01元”等虚假低价优惠问题外，盲盒应用还存在严重的夸大中奖概率的问题。夸大中奖概率主要表现为将概率事件描述为必然结果，诱导用户付费。

1.1 N 抽必中

应用在宣传素材中使用“ 百分百”、“必中”等绝对话语进行营销推广，实际中奖概率无法保证。

某盲盒 App 内宣传 N 连抽必中，但是根据实际公布的概率进行测算，发现存在至少 20% 的概率无法达成（详见图 1-1）：

公布概率（详见图 1-2）：

1.2 虚假中奖提示

虚假中奖提示是指应用在推广宣传内容中突出显示“中奖信息”，但弱化或隐藏其盲盒属性（详见图 1-3）：

实际支付界面（详见图 1-4）：

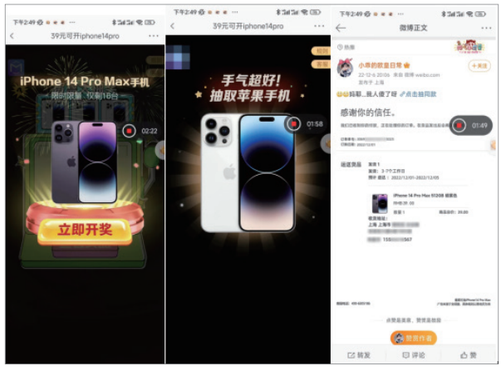


图 1-3 中奖信息界面

图 1-4 实际支付界面

2. 涉嫌变相赌博风险

盲盒目前主要有两种较为严重的涉嫌变相赌博风险，其一，回收变现存在现金博弈风险，其二，宣传以小博大诱导投机，存在变相赌博风险。

2.1 回收变现存在现金博弈风险

回收变现存在现金博弈风险一般指盲盒回收构成随机玩法的定向转移，形成消费资金再变现的交易闭环，导致产生现金博弈的风险。

目前盲盒应用中回收变现现金博弈风险主要有以下两类：

（1） 官方直接或间接利用寄售、转赠或其他形式在应用内实施盲盒回收；

（2） 官方支持、引导或默许黄牛在线下进行盲盒回收炒作。

案例 1：

某小程序官方通过寄售功能对盲盒开出的商品进行回收，形成实际意义上的“钱进钱出”（详见图 2-1）。

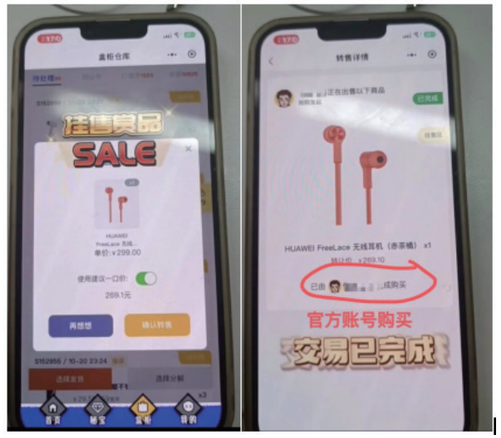


图 2-1 某官方账号对盲盒商品回收

案例 2：

某盲盒开发者官方用户群中，客服默许黄牛进行回收，且该黄牛和官方有极大可能存在关联关系（详见图 2-2）。

图 2-2 某盲盒开发者官方用户群

案例 3：

某盲盒官方通过 steam 对盲盒开出的虚拟道具进行回收（详见图 2-3）。

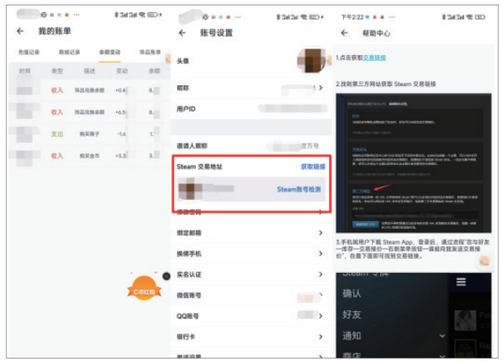


图 2-3 某盲盒官方 steam 回收界面

2.2 宣传以小博大诱导投机，存在变相赌博风险

通过设置高价差对比机制或刻意凸显原本极低或本不存在的高收益机会，诱导用户进行投机炒作。

其中主要有两类典型问题：

（1） 官方或其关联者在宣传中故意突出稀有商品远远高出盲盒价格或存在价值兜底，以此引导用户过度关注价差带来的高回报，营造稳赚不赔的变相赌博氛围。

（2） 官方或其关联者在宣传推广中故意散布高价值中奖者的信息或诱导鼓吹冲榜获得概率累加效果，以此造成用户陷入幸存者效应或蒙特卡洛效应。

在问题一中，开发者往往通过以下两种方式达成目的：

1） 官方或其关联者在营销推广中只着重对比单次机会的低价与稀有商品的高价。

图 2-4 某盲盒 App 宣传内容和物品价格

2） 官方或官方关联者在营销推广中显著提示存在与购买价格相等或略高的物品以此营造稳赚不赔的感觉。

某盲盒 App 宣传“保底”必出，并配合超高价金条，营造稳赚不赔的错觉（详见图 2-4）。

在问题二中开发者常见手法：

1） 官方或者官方关联者在应用内或官方群内显著频繁提示用户中奖者名单。

2） 官方或官方关联者在应用内或官方群内频繁提示引导用户已消费额度与中奖概率正相关。

某盲盒私域的大 R 群中，官方通过以上两种方式刺激用户冲动消费（详见图 2-5）。

盲盒作为当前流行的产品模式，因其独有的新鲜性、刺激性及社交属性而深受广大年轻人的喜爱，在年轻消费者中拥有巨大的市场，作为一种新消费体验有其存在的合理性。但开发者和经营者在利益的驱动下，罔顾广大消费者尤其是年轻用户合法权益，不仅不进行合理消费引导，反而过度营销消费者的猎奇心理，诱导、误导消费者冲动消费，严重侵害了用户的合法权益。

作为网络健康生态的助推者，为切实保障用户合法权益，安天移动安全基于对违规应用的系统性发现能力，“安鉴”风险检测预警平台“安鉴披露”上线盲盒类应用侵害用户权益问题的相关功能，对相关风险应用及其开发者进行公开曝光，并以此为依据配合监管部门、手机厂商及产业链各方进行生态治理，同时向终端用户发送风险预警，保护用户权益的同时助力生态净化。

图 2-5 某盲盒私域群和中奖名单

共同抬升行业底线，安天移动安全将加大对赚钱提现应用侵害用户权益问题的检测力度

当前，越来越多的 App 通过“赚钱提现”吸引用户来达到其商业化目标。这些 App 利用人们想要“赚钱”的心态，以“无提现门槛”为噱头，吸引了大量用户下载注册及使用，从而创造流量入口进行商业化变现。安天移动安全“安鉴”风险检测预警平台在检测中发现，以赚钱为噱头欺骗用户下载，设置多种提现障碍的问题广泛存在于头部短视频、走路赚钱、玩游戏赚钱、免费小说、WIFI 工具、来电秀等各类应用程序中。

安天移动安全对 App 侵害用户权益问题的判定正逐渐成为监管部门、终端厂商等产业链上下游各方进行生态治理的共识。在中央网信办开展的“清朗·移动互联网应用程序领域乱象整治”专项行动中，安天移动安全对赚钱提现类应用风险的判定再次成为重点治理对象。过去一年，安天移动安全曾对赚钱提现类应用风险进行过多轮公开曝光，并配合监管部门、终端厂商等产业链各方进行了生态治理，接下来，将继续加大对赚钱提现类应用部分侵害用户权益问题的检测力度，与产业链各方共同抬升行业底线，保障用户权益。

1. 立足用户安全，赚钱提现应用部分违规问题得到明显改善

2022 年，安天移动安全就针对赚钱提现侵害用户权益问题，配合监管部门、终端厂商等产业链各方进行了生态治理，在赚钱提现应用中，常见的“未明示用户完整提现规则”套路用户的部分典型问题得到明显改善，侵害用户权益问题大幅减少，现将典型问题分享如下。

(1) 在某些应用中，提现页面只显示赢满 XX 元即可提现，实则在用户协议中隐藏大量提现要求，设置多种提现障碍，用户误以为金额达标即可提现，在不知情的情况下投入大量时间和精力，权益无法保障。

(2) 某些应用内活动满 XX 元可提现，提现页面类似“立即赚钱”的提示让用户误以为参与即可达标提现，实则参与后仍然不能达到 XX 提现金额，开发者利用信息不对称和模糊性导致用户投入大量的时间和精力，设置多种提现障碍套路用户。

(3) 某些应用在用户提现时显示满 XX 元即可提现，实则页面上所谓的“注意事项”中要求用户通过查看用户协议获取其他提现要求，设置多种提现障碍。由于用户协议入口隐藏较深，且用户通常没有查看用户协议的习惯，导致用户投入大量时间和精力后仍然不能顺利提现。

(4) 抽奖式提现，在某些应用的抽奖式提现中，应用告知用户玩游戏即可获得提现机会，实则用户按要求参与后并未直接获得宣传中所谓的提现机会，而是获得概率无法保证的转盘抽奖，应用设置多种提现障碍，导致用户不能顺利提现，遭到用户的大量投诉。

2. 共同抬升行业底线，安天移动安全将加大对赚钱提现应用部分侵害用户权益问题的检测力度

安天移动安全“安鉴”风险检测预警平台在持续对赚钱提现类应用检测中发现，虽然未明示用户完整的提现规则相关问题得到明显改善，但诸如提现页面无任何提现规则说明、非一次性完整告知用户提现条件等问题依然广泛存在，接下来，安天移动安全将加大对以下部分赚钱提现类应用侵害用户权益典型问题的检测力度，不断抬升行业底线，保障用户合法权益。

(1) 在某些应用中，提现页面只有可以提现的金额，没有任何跟提现规则相关的提示，用户完全不知道怎样才算达到提现条件。

(2) 在某些应用中，用户在进行提现时，尽管提现条件告知用户需要满足“注意事项的要求”，但未能使用户直接获知完整提现规则，用户仍需去其他地方查看提现规则，此类方式不仅繁琐且容易被用户忽视造成无法顺利提现。

赚钱提现类应用作为颇受广大用户尤其是年轻用户喜爱的应用类型之一，拥有非常可观的用户和市场规模，据相关数据显示，仅 2021 年赚钱提现类 App 影响用户量已高达 4 亿。另外，该类 App 在下沉城市更受欢迎，其中 00 后用户占比为 24%，无论是用户规模还是用户构成都决定了规范赚钱提现类应用侵害用户权益行为的必要性。

作为网络健康生态的助推者，安天移动安全将基于对赚钱提现类应用系统性发现能力，继续加大对赚钱提现类 App 侵害用户权益行为的分析和检测力度，一方面在“安鉴”风险检测预警平台上线违规问题定义和解读、监管政策等功能，帮助开发者了解监管及合规政策，并提供整改申诉、复测入口；另一方面，配合监管部门、手机厂商及产业链各方进行生态治理，共同抬升行业底线，保障用户权益的同时助力生态净化。

全方位、多维度的安全检测和综合评估，护航数字安全

移动安全应用公益检测平台（安鉴），由当地网信办指导，基于安天移动安全数字安全核心技术优势，从行业规范、隐私规范、第三方组件安全、用户权益保护等多维度对APK包进行全方位检测，并智能化生成分析报告，帮助开发者深度挖掘潜在风险及源头，力争快速完成合规整改；同时出众的数字安全技术检测体系实现了对当前移动应用生态中的超范围收集信息、滥用权限等热点难点问题的精准检测，基于每天产生的海量安全大数据，为监管快速全面掌握开发者信息，发现App背后隐匿的开发者关联关系，从而实现快速追踪违法、违规开发者团伙，守护移动智能终端安全和用户权益保障，助力数字时代移动生态治理。

全量应用统一管控

- 技术手段收录相关App，登记备案
- 支持开发者主动提交App检测备案
- 支持与地方应用商店分发平台接口对接
- 支持管理人员上传补录App

违规应用检测发现

- App隐私合规检测
- App违规取证检查
- 广告内容违规/色情问题取证
- 大数据杀熟取证

影响力较大应用长效监测

- 头部重点App新老版本持续监测
- 存在历史污点App启用自动化策略“回头看”
- 持续对线上线下App跟踪监测，快速发现隐患

应用安全态势综合图谱

- 全量应用的综合态势感知
- 根据开发者、应用类型、传播渠道、传播量等多维度分类管理
- 检测、监测App数据一目了然
- App整改进度清晰明了

03 配合产业链各方的阶段性积极成果

武汉安天信息技术有限责任公司简介

武汉安天信息技术有限责任公司（简称“安天移动安全”）成立于 2010 年，是安天科技集团旗下专注于移动智能终端及用户安全防护的科技公司。

2013 年，公司自主研发的移动反病毒引擎产品，实现了中国安全厂商在全球顶级安全测评领域重量级奖项零的突破，目前该产品已累计为全球超 30 亿移动智能终端设备提供全维度、全生命周期安全防护。

经过多年发展与积累，公司与全球近百家知名芯片厂商、移动终端厂商、移动应用开发者、运营商等移动设备产业链上下游企业形成良好的移动产业生态合作，并为政府、监管部门及权威机构提供强有力的技术支撑。

安天移动安全始终秉承安全普惠理念，坚持自主创新，基于公司移动安全领域核心技术储备的优势，与产业链各方共同打造移动终端安全的绿色生态链，为新时代用户打造国民级安全产品，在万物互联时代营造更安全和可持续的全场景健康数字体验。

官方网站：www.avlsec.com

安天移动安全获评 2022 vivo “最佳安全技术伙伴”

图 1 2022 vivo 最佳安全技术伙伴评选结果

2022 年 11 月 8 日，以“MORE，近你所想”为主题的 2022 vivo 开发者大会在线上如期举行，安天移动安全凭借过去一年在 vivo 隐私安全保护及生态安全解决方案建设中提供的多项关键技术、创新服务，获评 2022 年 vivo“最佳安全技术伙伴”。（详见图 1）

过去一年，安天移动安全基于十余年的反恶意代码数据体系能力，围绕应用隐私和生态安全能力建设与 vivo 开展了深度密切的合作。在移动应用安全防护领域，安天移动安全在 vivo 应用隐私和生态安全解决方案建设中提供了多项关键技术支撑，落地了恶意软件和风险软件的识别、判定与分析等相关技术合作，有效提升了终端对应用流氓行为的防控能力，在共同治理应用广告乱象等方面取得显著成效。

此次获颁“最佳安全技术伙伴”（详见图 2），不仅是 vivo 对安天移动安全技术实力的认可，更表明 OEM 厂商携手安全厂商共建移动安全数字世界已步入常态化发展方向。

图 2 2022 vivo 最佳安全技术伙伴奖杯

当前，无论是监管部门、手机厂商还是安全厂商都在持续关注侵害用户权益的问题，移动互联网生态良性有序发展除了行业规范的引导、专业的技术支撑，也离不开终端厂商、开发者等各方的共同努力。安天移动安全拥有十余年移动安全技术积累，能对风险应用侵害用户权益的行为进行准确有效地追踪溯源，精准定位恶意代码、模块、SDK 等。安天移动安全愿和各方一道助力移动生态健康、有序发展，还用户一个安全纯净的网络环境。

安天移动安全与荣耀成立联合实验室，携手构建安全联合运营和防护体系

2022 年 11 月 22 日，荣耀 MagicOS 发布会暨首届开发者大会在深圳举办，在隐私安全分论坛上，“荣耀与安天移动安全联合实验室”宣布正式成立（以下简称“联合实验室”）。双方将开放创新能力，联合构筑终端安全风控能力体系，以应对当前日益复杂、泛化的移动应用生态新威胁。

安天移动安全副总经理何淼、荣耀 MagicOS 解决方案设计与开发部副部长赵珅出席了签约及揭牌仪式（详见图 1）。安天移动安全凭借过去一年在荣耀生态安全建设中提供的多项关键技术和支撑获颁“荣耀安全联合创新最佳合作伙伴”奖项。

在隐私安全分论坛现场，安天移动安全副总经理彭智俊在主题为《移动应用生态的新威胁和应对》的演讲中提到，移动 App 种类和数量呈爆发式增长，渗透到人们工作和生活的各个领域，同时侵害用户权益的事件也层出不穷。以往基于单个应用的网络诈骗威胁向跨应用、平台的多场景威胁演变，威胁手段也不再局限于仿冒应用盗刷、漏洞利用盗刷，逐渐多样化和复杂化，因此，

图 1 “荣耀与安天移动安全联合实验室”揭牌仪式

图 2 安天移动安全副总经理彭智俊

多方参与、联防联控是应对当前移动生态新威胁的“钥匙”。（详见图 2）

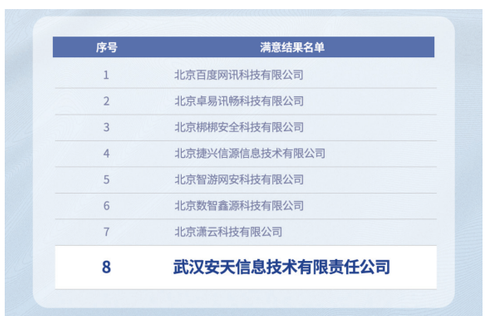
安天移动安全认为，建立全生态参与的安全联运体系是应对移动应用生态新威胁的关键。针对虚假价格优惠、虚假功能等移动应用生态新威胁，联合实验室将在技术预研、能力共建、联合安全运营等方面开展深度合作，联合构筑终端安全风控能力体系，开放创新能力并面向行业联合赋能，提供多维度、全方位的移动安全风控能力，致力于打造更加纯净、安全的终端生态。

荣耀与安天移动安全联合实验室的成立，不仅是荣耀对安天移动安全技术实力的认可，更表明智能终端厂商携手安全厂商联合打造产业生态，共建移动安全数字世界，为消费者提供更加纯净、安全的使用体验成为趋势。

基于对终端生态安全的共同愿景，双方将在终端安全风控领域作深入研究，致力于为全球用户提供纯净、安全、可靠的服务体验，同时通过共同协作努力，开放创新能力，为行业发展助力和赋能。

安天移动安全成为八家通过中国信通院“能力验证计划”的企业之一

2022 年 12 月 26 日，中国信息通信研究院（以下简称“中国信通院”）泰尔终端实验室，依据 ISO/IEC 17043：2010《能力验证提供者能力的要求》（CNAS-CL03《能力验证提供者认可准则》）对全国主要 App 个人信息保护检测机构的检测能力进行了考核评估，安天移动安全成为八家通过中国信通院评测的企业之一。（详见图 1）



序号	满意结果名单
1	北京百度网讯科技有限公司
2	北京卓易讯畅科技有限公司
3	北京梆梆安全科技有限公司
4	北京捷兴信源信息技术有限公司
5	北京智游网安科技有限公司
6	北京数智鑫源科技有限公司
7	北京潘云科技有限公司
8	武汉安天信息技术有限责任公司

（排名不分先后，按照笔划排序）

图 1 安天移动安全成为八家通过中国信通院评测的企业之一

为切实提升机构检测技术和服务水平，提高行业个人信息保护水平，2022 年 11 月，中国信通院泰尔终端实验室开展了“移动互联网应用程序（APP）用户权益保护测试能力验证计划”。参加本次能力验证计划检测机构以《移动互联网应用程序（APP）用户权益保护测评规范》《信息安全技术移动互联网应用程序（APP）收集个人信息基本要求》等标准为依据对样品 App 进行测试。

图 2 移动互联网应用程序（APP）用户权益保护测试能力验证结果证书

基于十余年的技术积累和实战经验，目前，安天移动安全针对当前移动应用风险问题已初步形成系统性发现能力，建立了细粒度的移动互联网应用问题取证标准，采用终端侧本地规则引擎和云端检测引擎的双引擎战略，实现终端用户侧真实威胁态势的感知能力和实时的威胁处置能力，能够精准定位恶意代码、模块、SDK 及各类小程序、快应用等侵害用户权益问题，并最终通过中国信通院本次测试评估。（详见图 2）

在此次能力验证测试中，安天移动安全仅展示了部分检测技术和能力，本次获得中国信通院的认可，既是安天移动安全在移动应用风险检测技术方面综合能力的体现，也是对安天移动安全在移动生态个人信息保护领域核心技术优势的肯定。

作为网络安全的助推者，为保障广大用户合法权益，一方面，安天移动安全“安鉴”风险检测预警平台将及时跟进政策法规和检测细则的更新并进行专业解读，帮助开发者了解监管及合规政策，并提供整改申诉、复测入口，实现检出规则和政策同步迭代。

另一方面，安天移动安全将持续加大研发投入和技术人员能力提升，精准定位恶意代码、模块、SDK 及各类小程序、快应用等侵害用户权益问题，提前布局技术趋势的前沿领域安全。并积极配合工信部、中国信通院、泰尔终端实验室等监管部门开展 App 用户权益保护检测技术支持和相关保障工作，与移动产业链各方一同保障用户权益，共建纯净健康的移动互联网生态。

安天移动安全收到湖北省通信管理局的感谢信

2023 年 1 月，湖北省通信管理局向安天移动安全发来了感谢信，对过去一年，安天移动安全为湖北省信息通信行业网络安全与信息化建设提供的技术支撑和突出贡献表达了感谢。（详见图 1）

当前，移动互联网应用程序（App）已经渗透到衣、食、住、行等人们生活中的各个领域，侵害用户权益问题及风险应用出现大规模扩张，保障用户安全并做好数据安全工作意义重大，刻不容缓。安天移动安全积极发挥自身技术优势，为湖北省信息通信行业网络安全与信息化建设做出了突出的贡献，得到一致肯定和感谢。

本次收到湖北省通信管理局的感谢信，既是对安天移动安全在湖北省网络和数据安全工作中所作努力的认

湖北省通信管理局处室简函

感谢信

武汉安天信息技术有限责任公司：

2022 年是党的二十大召开之年，是我们党进入全面建设社会主义现代化国家、向第二个百年奋斗目标进军新征程的重要时刻召开的一次十分重要的大会。在此期间，得到了贵单位的大力支持和帮助，为湖北省信息通信行业网络安全与信息化建设做出了突出的贡献，在此表示衷心感谢！

2023 年是全面贯彻落实党的二十大精神的开局之年，也是把握数聚叠加发展机遇，加快建设网络强国，数字中国的关键之年。

希望贵单位一如既往地支持我局各项工作，进一步推动湖北省信息通信行业网络和数据安全工作迈上新台阶。新年将至，祝贵单位事业蒸蒸日上，全体干部职工新年快乐，事事顺遂！

湖北省通信管理局网络安全管理处

2022 年 12 月 29 日

◀ 图 1 湖北省通信管理局的感谢信

可，也是对安天移动安全在该领域核心技术优势的肯定。

当前，无论是监管部门、手机厂商还是安全厂商都在持续关注侵害用户权益的问题，移动互联网生态良性有序发展除了行业规范的引导、专业的技术支撑，也离不开终端厂商、开发者等各方的共同努力。安天移动安全拥有十余年移动安全技术积累，能对风险应用侵害用户权益的行为进行准确有效地追踪溯源，精准定位恶意代码、模块、SDK 等。安天移动安全愿和各方一道助力移动生态健康、有序发展，还用户一个安全纯净的网络环境。

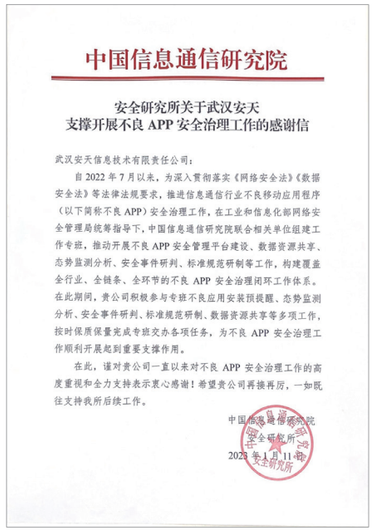
安天移动安全收到中国信息通信研究院安全研究所感谢信

2023 年 1 月 11 日，中国信息通信研究院安全研究所向安天移动安全发来了感谢信，对自 2022 年 7 月份以来，安天移动安全积极参与中国信通院开展的不良应用程序安全治理工作，并起到重要支撑作用表达了感谢。（详见图 1）

当前，App 已经渗透到衣、食、住、行等人们生活中的各个领域，诱导付费、强制自动续费、虚假优惠等侵害用户权益的风险应用出现大规模扩张，构建覆盖全行业、全链条、全环节的不良 App 安全治理体系对保障用户安全具有重要意义。安天移动安全发挥自身核心技术优势，积极参与到不良 App 安全治理体系建设中，并在态势分析、实践研判、标准规范研制等方面提供了重要支撑，得到中国信通院安全研究所的认可和肯定。

本次收到中国信通院安全研究所的感谢信，既是对安天移动安全在不良应用程序安全治理工作中所做努力的认可，也是对安天移动安全在该领域核心技术优势的肯定。

作为网络安全的助推者，为保障广大用户合法权益，安天移动安全



中国信息通信研究院

安全研究所关于武汉安天
支撑开展不良 APP 安全治理工作的感谢信

武汉安天信息技术有限责任公司：

自 2022 年 7 月以来，为深入贯彻落实《网络安全法》《数据安全法》等法律法规要求，推进信息通信行业不良移动应用程序（以下简称不良 APP）安全治理工作，在工业和信息化部网络安全管理局统筹指导下，中国信息通信研究院联合相关单位组建工作专班，推动开展不良 APP 安全管理平台建设、数据资源共享、态势监测分析、安全事件研判、标准规范研制等工作，构建覆盖全行业、全链条、全环节的不良 APP 安全治理闭环工作体系。在此期间，贵公司积极参与专班不良应用安装预提醒、态势监测分析、安全事件研判、标准规范研制、数据资源共享等多项工作，按时保质保量完成专班交办各项任务，为不良 APP 安全治理工作顺利开展起到重要支撑作用。

在此，谨对贵公司一直以来对不良 APP 安全治理工作的高度重视和全力支持表示衷心感谢！希望贵公司再接再厉，一如既往支持我所后续工作。

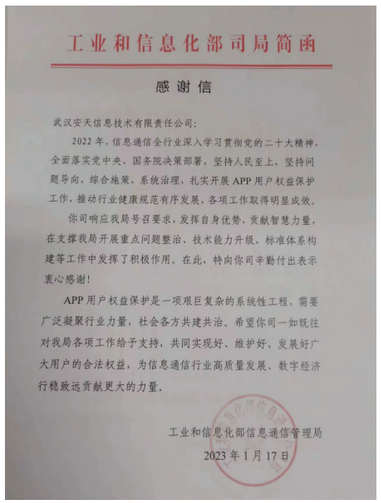
中国信息通信研究院
安全研究所
2023 年 1 月 11 日

图 1 中国信息通信研究院安全研究所感谢信

一方面在安鉴风险检测预警平台上线违规问题定义和解读、监管政策等功能，帮助开发者了解监管及合规政策，并提供整改申诉、复测入口；另一方面，还将积极配合中国信通院等监管部门开展 App 用户权益保护工作并提供相关技术支持和保障，与移动产业链各方一同保障用户权益，共建纯净健康的移动互联网生态。

安天移动安全收到工业和信息化部信息通信管理局的感谢信

2023 年 1 月 17 日，工业和信息化部信息通信管理局（以下简称“工信部信息通信管理局”）向安天移动安全发来了感谢信，对 2022 年，安天移动安全支撑工信部信息通信管理局开展重点问题整治、技术能力升级、标准体系构建等工作中发挥的积极作用表达了衷心感谢。（详见图 1）



工业和信息化部司局简函

感谢信

武汉安天信息技术有限责任公司：

2022 年，信息通信全行业深入学习贯彻党的二十大精神，全面落实党中央、国务院决策部署，坚持人民至上，坚持问题导向，综合施策，系统治理，扎实开展 APP 用户权益保护工作，推动行业健康规范有序发展，各项工作取得明显成效。

你司响应我局号召要求，发挥自身优势，贡献智慧力量，在支撑我局开展重点问题整治、技术能力升级、标准体系构建等工作中发挥了积极作用。在此，特向你司辛勤付出表示衷心感谢！

APP 用户权益保护是一项艰巨复杂的系统性工程，需要广泛凝聚行业力量，社会各方共建共治。希望你司一如既往对我局各项工作给予支持，共同实现好、维护好、发展好广大用户的合法权益，为信息通信行业高质量发展、数字经济行稳致远贡献更大的力量。

工业和信息化部信息通信管理局

2023 年 1 月 17 日

图 1 中国信息通信研究院安全研究所感谢信

当前，App 已经渗透到衣、食、住、行等人们生活中的各个领域，诱导付费、强制自动续费、虚假优惠等侵害用户权益的风险应用出现大规模扩张。坚持人民至上，坚持问题导向，系统治理，扎实开展 App 用户权益保护工作，推动行业健康规范有序发展，具有重大意义并取得明显成效。

安天移动安全发挥自身核心技术优势，积极参与到 App 用户权益保护工作中，并在重点问题整治、技术能力升级、标准体系构建等方面提供了重要支撑，得到工信部信息通信管理局的认可和感谢。

作为移动安全的助推者，为保障广大用户合法权益，安天移动安全将一如既往对工信部信息通信管理局各项工作给予支持，与移动产业链各方共同实现好、维护好、发展好广大用户的的合法权益，共建纯净健康的移动互联网生态，为信息通信行业高质量发展、数字经济行稳致远贡献更大的力量。

安天移动安全入选工业和信息化部 2023 年度 CAPPVD 漏洞库技术支撑单位

2023 年 1 月，工业和信息化部移动互联网 App 产品安全漏洞专业库（以下简称“CAPPVD 漏洞库”）公布了 2023 年度 CAPPVD 漏洞库技术支撑单位名单，安天移动安全成功入选。（详见图 1）

2023 年 1 月，工业和信息化部 CAPPVD 漏洞库根据《CAPPVD 漏洞库支撑单位能力评定办法》，经过对各支撑单位在 2021-2022 年度的支撑情况开展能力评定，安天移动安全凭借在 2021 ～ 2022 年协助做好网络产品安全漏洞管理、消控国内 App 产品安全隐患等方面的优秀表现和积极作用，成功入选 2023 年度 CAPPVD 漏洞库技术支撑单位名单。

本次入选工信部移动互联网 App 产品安全漏洞库技术支撑单位，不仅是对安天移动安全重大漏洞、安全事件发现、防范及应对能力的认可，同时也是安天移动安全在移动生态安全领域综合实力的体现。

未来，安天移动安全将一如既往地全力支撑国家移动互联网 App 产品安全漏洞管理工作，持续提升重大漏洞和重要安全事件的发现、分析、处置能力，安全漏洞研究、事件披露能力，与产业链各方一同构建移动安全感知协同的防御体系，共建漏洞防御切面，全面提升移动应用安全漏洞、事件的研究水平和预警能力，提高威胁应对与风险管理能力，促进移动互联网产业安全有序发展，为我国移动互联网 App 安全防护提供有力支撑。

2023 年度 CAPPVD 漏洞库技术支撑单位名单	
1	深圳海云安网络安全技术有限公司
2	天翼安全科技有限公司
3	北京山石网科信息技术有限公司
4	西北工业大学软件学院
5	深圳市博通智能技术有限公司
6	深圳市能信安科技股份有限公司
7	北京鸿腾智能科技有限公司
8	上海斗象信息科技有限公司
9	远江盛邦(北京)网络安全科技股份有限公司
10	北京梆梆安全科技有限公司
11	北京小米科技有限责任公司
12	浙江大华技术股份有限公司
13	山东新潮信息技术有限公司
14	中国联合网络通信有限公司软件研究院
15	浙江御安信息技术有限公司
16	北京众安天下科技有限公司
17	奇安信科技集团股份有限公司
18	北京智游网安科技有限公司
19	北京神州绿盟科技有限公司
20	北京天融信网络安全技术有限公司
21	武汉安天信息技术有限责任公司
23	北京安普诺信息技术有限公司
24	深圳市网安计算机安全检测技术有限公司
25	北京时代新威信息技术有限公司
26	江苏骏安信息测评认证有限公司
27	江苏通付盾信息安全技术有限公司
28	新疆量子通信技术有限公司
29	郑州云智信安安全技术有限公司
30	深圳市腾讯计算机系统有限公司
31	北京云测信息技术有限公司

图 1 安天移动安全入选 2023 年度 CAPPVD 漏洞库技术支撑单位名单

04 安天党建文化与青春风采

由安天承办的“学习二十大 奋进新征程 – 网安书记讲党课”系列活动上线

为深入学习领会党的二十大精神，进一步贯彻落实网络强国战略思想，扎实推进网络安全和信息化工作，由中国网络安全产业联盟主办，安天科技集团、光明网网络安全频道协办的“学习二十大 奋进新征程——网安书记讲党课”线上活动于近日在光明网、中国网络安全产业联盟公众号等端口上线。目前该活动已登陆光明网网络安全频道首页（https://wlaq.gmw.cn/）。

活动由中国电子技术标准化研究院党委书记、副院长，中国网络安全产业联盟秘书长杨建军宣布启动。

中国电子技术标准化研究院党委书记、副院长，中国网络安全产业联盟秘书长杨建军

首期“网安书记讲党课”由全国政协委员、中国网络安全产业联盟理事长、安天科技集团党委书记肖新光作题为“学习贯彻党的二十大精神 以总体国家安全观为根本遵循 全面加速网络安全产业发展”的专题报告。报告重点围绕“对二十大报告中国家安全相关内容与结构的学习理解”“关于‘国家安全’‘总体’的界定”“坚定不移贯彻总体国家安全观”“推进国家安全体系和能力现代化”四个方面，结合网络安全实际工作及深入学习贯彻党的二十大精神中关于推进国家安全体系和能力现代化相关要求，探讨网络安全行业如何做好重大基础设施、网络等安全保障体系建设。

二十大报告中提出“构建全域联动、立体高效的国家安全防护体系。增强维护国家安全能力。”“筑牢国家安全人民防线。提高公共安全治理水平，坚持安全第一、预防为主，完善公共安全体系，提高防灾减灾救灾和急难险重突发公共事件处置保障能力，加强个人信息保护”，吹响了网络安全产业人的冲锋号角，对网络安全工作提出了更高的要求。

全国政协委员、中国网络安全产业联盟理事长、安天科技集团党委书记肖新光

肖新光同志表示，“作为网络安全工作者，我们要以习近平总书记总体国家安全观为根本遵循，以网络强国重要思想为工作指引，强化自主创新，增强有效安全能力供给，全力保障国家网络空间安全。”

4·19 | 安天六地党支部学习党课，收获满满畅谈学习体会

为了深入学习贯彻习近平总书记关于总体国家安全观和网络强国战略思想，增强国家安全意识和法治意识，践行网络安全国家队的使命责任，4 月 19 日，在安天集团党委的统一组织下，各地支部组织观看安天集团党委书记肖新光同志《以总体国家安全观为根本遵循，全面加速网络安全产业发展》的党课视频，学习领会党的二十大精神和“总体国家安全观”的重要精神。

2014 年，习总书记在中央国家安全委员会第一次全体会议上强调指出，要准确把握国家安全形势变化新特点新趋势，坚持总体国家安全观。2016 年 4 月，习总书记在网络安全和信息化工作座谈会上发表了重要讲话，为网络强国战略目标构建了方法论工作指引。

安天在集团党委的统一组织下，形成了每年 4 月组织主题学习活动的传统，并取得一定的工作成效。今年是纪念习总书记“4·19”重要讲话发表七周年，更是落实党的二十大精神的开局之年。党的二十大报告中，首次将国家安全方面的内容形成单独章节，以“推进国家安全体系和能力现代化，坚决维护国家安全和社会稳定”为主题对国家安全内容做了全面系统阐述。在党和国家发展的新要求下，对网络安全从业者又提出了新的历史使命和要求。安天集团今年开展和组织“总体国家安全观主题学习月”活动，是深刻学习理解总体国家安全观、坚定践行初心使命、广泛凝聚全体党员和员工力量的重要举措。在观看党课视频后，党员同志们收获满满，纷纷畅谈学习体会。

安天各地开展“总体国家安全观主题学习月”活动

主题学习月期间，安天集团党委还将组织开展国家安全观和安全保密知识竞赛答题、“高级威胁分析技能大赛”等多种形式的活动。

安天集团组织召开“纪念习总书记视察安天七周年暨主题教育空中党课”活动

2016 年 5 月 25 日，习近平总书记在黑龙江调研期间来到安天总部视察。在听取汇报后，总书记对安天人说，“你们也是国家队，虽然你们是民营企业。”自此，每年这一天，安天都会举行空中党课等主题活动，统一思想认知，凝聚集体意志、将习近平总书记的嘱托转化为安天人坚定的使命信念和砥砺前行的持久动力。

今天，安天集团党委组织召开 “纪念习总书记视察安天七周年暨主题教育空中党课”活动，邀请北京航空航天大学张文木研究员、中央党校孙东方教授，为安天集团全体员工讲授了专题党课。张文木研究员授课内容为《世界大变局和中华民族伟大复兴》，孙东方教授的授课内容为《全面贯彻总体国家安全观》。

安天集团哈尔滨、北京、武汉、上海、成都、深圳等地一千多名员工通过现场和线上方式收看授课内容。后续还会继续以支部为单位，组织党员干部、积极分子按照学习贯彻习近平新时代中国特色社会主义思想主题教育活动的部署进一步交流研讨。

七年来，安天人一直把＂网络安全国家队＂作为自身的定位和导向。始终坚持战略驱动、自主创新，达成有效安全价值，向具有鲜明网络空间防务特色和网络安全基础设施特点的网络安全一流企业这一发展目标扎实迈进。

北京航空航天大学张文木研究员

中央党校孙东方教授

安天各地支部通过现场和线上方式收看党课

安天移动安全&武汉软件新城丨红色引擎·党建引领人才服务主题党日活动

为进一步丰富“党建+理论学习实践”，提升支部党建引领力，3月16日下午，在现代服务业园综合党委指导下，安天移动安全与武汉软件新城联合开展“红色引擎·引领人才服务”党建融合主题活动。现代服务业园党委代表、亿达集团副总裁、武汉软件新城党委代表莅临活动，安天移动安全党支部书记、总经理和卓越学院高研班骨干及10余名党员参与活动。

1. 重温入党誓词

安天移动安全党支部书记首先带领大家重温入党誓词，大家一起高举右手，面对鲜红党旗庄严宣誓。一字一句铿锵恢宏的誓词，神圣而豪迈，体现了党员同志们对中国共产党的无限忠诚。

2. 党史学习

党史学习环节，邀请到亿达中国股份有限公司执行董事、副总裁袁文胜讲授主题为《从解放战争看毛泽东的战略思维》的党课，通过对国共两党战争形势的对比，及领导人不同的战略思维和战略布局的博弈分析，突显中国共产党“存地失人，人地皆失；存人失地，人地皆存”的战略思想，和以“人”为中心的战略选择是取得解放战争全面胜利的关键，进而从战争中看现代企业战略布局，点明企业中人与人才的重要性、战略选择的重要性，并深入交流企业“以党建引领人才”的创新做法，感慨“党建是办好企业的一大重要法宝。”

3. 分享交流

公司总经理、卓越学院院长陈家林听完袁总生动党课后感慨：所谓战略，即是通过创新搭建起的一种可持续的、差异化竞争。安天作为武汉本土成长，一步一步壮大起来的网络安全领军企业应充分发挥自身技术、人才优势和技术创新主体作用，在激烈的市场竞争中主动将党的先进理论与公司战略“挂钩”，现阶段正带领卓越学院骨干研习先进的管理模式，从公司实际出发，进一步完善和强化公司的流程、组织和人才建设，在“扬弃”中系统搭建好自身特色的经营管理模式，抢占市场战略控制点。若把中国共产党比作一家百年企业，它期间面临的艰难险阻远比我们当下要大得多，公司广大员工要树立信心，从中国共产党的成功经验中汲取力量，坚定理想信念，砥砺前进初心！

此次党建引领人才交流主题党日活动圆满结束，后期支部将着力在“党建+理论学习”中结合业务侧紧紧围绕“五史”时间线开展党史学习教育活动，营造一级带着一级的学习风气。从根上加强意识形态正向引导，从质上提升大家分析问题和解决问题的能力，通过党建引领赋能公司战略目标实现。

安天资讯 INFORMATION

No.1 ▌安天总分第二获“首届工业信息安全应急大赛”二等奖

近日，第四届国际工业信息安全应急大会在北京举办。本届大会同期举办了“首届工业信息安全应急大赛”，安天在 19 支参赛队伍中以总分第二的成绩，荣获“首届工业信息安全应急大赛”二等奖，展示了在工业场景的应急处置和安全运维能力。安天再次入选国家工业信息安全漏洞库（CICSVD）技术组成员单位并被评为 2022 年度漏洞治理合作最具贡献单位。

No.2 ▌安天参加第二十一届中国 IT 用户满意度大会并发表演讲

2 月 10 日，由国家工业信息安全发展研究中心、中国电子质量管理协会指导，计世资讯（CCWResearch）主办的第二十一届中国 IT 用户满意度大会在北京召开。安天出席本次会议并发表《端点执行体采集和全量识别》的主题演讲。

No.3 ▌安天获“第一批网络安全产品互联互通联盟技术规范试点单位”授牌

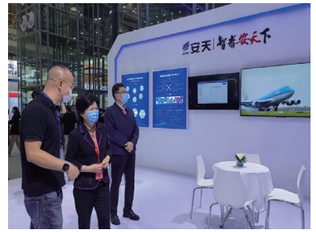
3 月 28 日，在中国网络安全产业联盟主办的 2023 年 CCIA 网络安全技术应用专题研讨会 - 网络安全产品互联互通专题会上，安天获得“第一批网络安全产品互联互通联盟技术规范试点单位”授牌。安天自主研发的“威胁对抗运营 XDR 平台”作为首批典型安全产品接受验证，完成《信息安全技术网络安全产品互联互通告警信息格式》、《信息安全技术 网络安全产品互联互通资产信息格式》两项联盟技术规范试点验证工作。

No.4 ▌安天再度入选工信部 2022 年工业互联网试点示范名单

近日，工业和信息化部公布了 2022 年工业互联网试点示范名单，安天申报的“面向工业互联网多场景的恶意代码检测技术”入选安全类“新技术融合创新应用”试点示范名单。

No.5 ▌安天参展第十一届中国电子信息博览会 守卫数字时代网络安全

4 月 7 日至 9 日，以“创新引领，协同发展”为主题的第十一届中国电子信息博览会在深圳会展中心（福田）举办。安天作为网络安全领军企业，积极参与并重点展示了在执行体治理、供应链安全、云安全、移动安全、威胁对抗等领域的技术体系、创新产品和解决方案，以及能力型安全产品为用户的终端安全、流量安全、Web 防护等层面提供的安全保障，解决用户在数字化发展中面临的各种复杂安全问题。黑龙江省副省长王岚莅临安天展台参观指导，在听取了安天的业务发展、核心技术创新等相关汇报后，对安天的企业定位、产品和服务能力给予高度认可。



No.6 ▌安天牵头编写多个章节 |《2022 网信自主创新调研报告》发布

4 月 19 日，安天参编的《2022 网信自主创新调研报告》在“第六届关键信息基础设施自主安全创新论坛暨纪念‘4.19’讲话发表七周年活动”上正式发布。在报告 25 个章节中，安天牵头编写了“反恶意代码引擎”“高级威胁检测”“终端安全”章节，并参与“工控安全”“数据安全”章节的编写工作。报告得到中国工程院倪光南院士、沈昌祥院士推荐及业界众多专家的关注和支持。安天在编写工作中提出了大量的建设性意见与观点，撰写了高质量的专业素材，获得编委会专家的高度肯定及感谢信。

No.7 ▌安天参研项目获广东省科技进步一等奖

近日，广东省科学技术厅发布了《2022 年度广东省科学技术奖拟奖公示》，安天与鹏城实验室、哈尔滨工业大学（深圳）、广州大学等联合申报的“大规模网络仿真验证平台（鹏城靶场）关键技术与系统”项目通过评审，获广东省科技进步一等奖。

No.8 ▌安天入选《CCSIP 2022 中国网络安全产业全景册（第五版）》

近日，FreeBuf 咨询正式发布《CCSIP（China Cyber Security Industry Panorama）2022 中国网络安全行业全景册（第五版）》。安天入选本次全景册 15 个一级分类 32 个细分领域，涵盖通信网络安全、云安全、安全开发、应用防护、身份识别与访问管理、边界访问控制、数据安全、威胁检测与捕获、漏洞检测与管理、安全情报、事件管理 & 响应、安全服务、工控安全、物联网安全、移动安全领域。

前沿动态 INFORMATION

一、网络安全战略与政策动态

No.1 ▌工业和信息化部等五部门发布《关于调整网络安全专用产品安全管理有关事项的公告》

2023 年 4 月 12 日，工业和信息化部等五部门发布《关于调整网络安全专用产品安全管理有关事项的公告》[1]，旨在加强网络安全专用产品安全管理，推动安全认证和安全检测结果互认，避免重复认证、检测。《公告》指出，自 2023 年 7 月 1 日起，列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品应当按照《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求，停止颁发《计算机信息系统安全专用产品销售许可证》，停止执行《关于调整信息安全产品强制性认证实施要求的公告》和《财政部 工业和信息化部 质检总局 认监委关于信息安全产品实施政府采购的通知》，工业和信息化部等五部门统一公布和更新符合要求的网络关键设备和网络安全专用产品清单，供社会查询和使用。

No.2 ▌中央网信办等五部门印发《2023 年数字乡村发展工作要点》

2023 年 4 月 13 日，中央网信办等五部门印发《2023 年数字乡村发展工作要点》[2]，旨在以数字化赋能乡村产业发展、乡村建设和乡村治理，推动农业强国建设取得新进展、数字中国建设迈上新台阶。《要点》明确了到 2023 年底，数字乡村发展取得阶段性进展的工作目标，对 10 个方面 26 项重点任务进行了部署，包括夯实乡村数字化发展基础、强化粮食安全数字化保障、提升网络帮扶成色成效、因地制宜发展智慧农业、多措并举发展县域数字经济、创新发展乡村数字文化、提升乡村治理数字化水平、深化乡村数字普惠服务、加快建设智慧绿色乡村、保障数字乡村高质量发展等。

No.3 ▌全国信息安全标准化技术委员会发布《2023 年度第一批网络安全国家标准需求的通知》

2023 年 4 月 13 日，全国信息安全标准化技术委员会发布《2023 年度第一批网络安全国家标准需求的通知》[3]，旨在加强网络安全全国家标准在国家网络安全保障工作中的基础性、规范性、引领性作用。《通知》中包括通知正文，以及 2023 年度第一批网络安全国家标准需求清单、申报工作要求、申报操作指南等六个附件内容。标准需求清单中包括《信息安全技术 生成式人工智能预训练和优化训练数据安全规范》等 23 项制定标准，以及信息安全技术 信息系统灾难恢复规范等 7 项修订标准，全国信息安全标准化技术委员会要求有关部门围绕需求做好申报工作，并于 2023 年 5 月 12 日前进行申报。

No.4 ▌最高人民检察院发布《关于加强新时代检察机关网络法治工作的意见》

2023 年 4 月 18 日，最高人民检察院发布《关于加强新时代检察机关网络法治工作的意见》[4]，旨在认真学习贯彻党的二十大精神，依法能动履行法律监督职责，以检察工作现代化融入和助力网络法治工作现代化，更好服务保障网络强国、数字中国建设。《意见》包括 6 个方面 21 条，强调了要深入贯彻网络强国的重要思想，指出要充分发挥司法办案职能，依法严厉打击利用网络实施的危害国家安全犯罪，明确统筹运用检察监督，强化一体履职数据赋能，要求要积极参与网络立法制定修订工作，推动制定修订法律法规。

No.5 ▌美网络安全和基础设施安全局发布《零信任成熟度模型 V 2.0》

4 月 11 日，网络安全和基础设施安全局（CISA）发布《零信任成熟度模型 V 2.0》（Zero Trust Maturity Model）[5]，旨在协助用户制定零信任战略和实施计划，并展示 CISA 跨机构支持零信任解决方案的方式。《模型》包含了身份、网络、数据与应用程序以及工作负载五大支柱，并提供了零信任架构的具体示例。在传统、初始、高级、最佳四个成熟度阶段基础上，CISA 不仅对现有功能进行了更新而且添加了部分新功能。《模型》指出零信任架构应具备持续验证功能、风险分析功能、覆盖整个机构的身份整合功能，以及按需自动访问特定系统和应用程序的定制功能等。此外，零信任架构网络应具有分布式微边界，并对安全访问控制措施和配置定期进行监控和更新。《模型》的发布进一步推动了联邦政府在网络安全零信任方法实施的持续进展，以支持国家网络安全战略。

No.6 ▌美国家安全局等联合发布《改变网络安全平衡：设计安全与默认安全的原则和方法》

4 月 13 日，美国家安全局等联合发布《改变网络安全平衡：设计安全与默认安全的原则和方法》（Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by Design and Default）[6]，旨在提高认识并促进关于关键优先事项、投资和必要决策的国际对话制造安全、可靠和有弹性的技术。《原则和方法》的发布方除美国家安全局、美网络安全和基础设施安全局等以外，还包括澳大利亚网络安全中心、加拿大网络安全中心、英国国家网络安全中心等多国网络安全机构。《原则和方法》将确保技术产品的构建和配置方式能够防止恶意网络行为者访问设备、数据、连接基础设施，敦促技术和软件制造商修改其设计和开发程序，将具备设计安全和默认安全的产品交付客户。《原则和方法》还概述了开发过程中使用定制的威胁模型、披露产品的安全漏洞时最大限度地确保信息透明和问责、使用内存安全类编程语言等相关措施。

No.7 ▌欧盟通过《网络团结法案》提案

4 月 18 日，欧盟通过《网络团结法案》提案（EU Cyber Solidarity Act）[7]，旨在加强欧盟的网络安全能力。《法案》将加强联盟层面的团结，通过创建欧洲网络安全盾和全面的网络应急机制，更好地发现、准备和应对重大网络安全事件。欧洲网络盾牌是一个泛欧基础设施，由遍布欧盟的国家和跨境安全运营中心组成，这些中心可能将在 2024 年初投入运营。网络应急机制能够加强欧盟的网络事件响应能力，支持准备行动、创建新的欧盟网络安全储备、互相提供财政支持等。同时，建立网络安全事件审查机制，通过在重大网络安全事件发生后审查、评估并吸取经验教训，在适当时发布改善联盟网络态势的建议。《法案》下所有行动的总预算为 11 亿欧元，其中约 2/3 资金将由欧盟通过数字欧洲计划提供。该法案发布，不仅能够强化了各成员国之间的团结，而且增强了成员国的危机管理和响应能力。

二、网络安全产业动态

No.1 ▌嘶吼安全产业研究院发布《2023 Q1 网络安全产业重点洞察》

4 月 3 日，嘶吼安全产业研究院发布《2023 Q1 网络安全产业重点洞察》[8]，旨在对 2023 Q1 网络安全产业重点进行分析。《洞察》报告围绕网络安全政策动向、网络安全投融资、网络安全厂商、网络安全大事件、网络安全技术等五方面进行分析解读。《洞察》报告显示 2023 年两会网络安全相关的提案主要聚焦于数据安全、车联网安全等领域，在网络安全投融资领域呈现“倒春寒”现象，指出未来投资者将会更注重专精型、创新型赛道的投资力度，认为未来网络安全厂商的重点技术研发集中在云主机安全、终端威胁、数字边界等方面。

No.2 ▌Gartner 发布《新兴技术：安全—网络威胁检测与响应（NDR）采用增长洞察》

4 月 5 日，Gartner 发布《新兴技术：安全—网络威胁检测与响应（NDR）采用增长洞察》（Emerging Tech: Top Use Cases for Network Detection and Response）[9]，旨在帮助用户负责人了解 NDR 产品并提供相关建议。《洞察》指出 NDR 市场基于用户采用率，由检测、事件响应、响应用例三个核心驱动，为最大限度提高收入，应该将产品路线图集中在三个核心驱动上。《洞察》显示政府和金融行业客户对 NDR 更感兴趣，原来 NDR 更多的是吸引大型组织用户的注意，但现在中型组织用户对其也越来越来感兴趣。《洞察》还提出通过将 NDR 响应集成投资集中在端点保护平台供应商上来扩大响应功能、通过投资非网络检测源与不断用户需求保持相关性等建议。

No.3 ▌安全牛发布《网络安全行业全景图》

4 月 7 日，安全牛发布第十版《网络安全行业全景图》[10]，旨在真实、全面、客观的展现我国网络安全行业整体状况，帮助了解当前产业发展特征。新版《全景图》中，共收录 456 家国内网络安全企业和相关行业机构，较第九版增加 23 家；细分领域共收录 3180 项，较第九版增加 571 项。《全景图》对细分安全领域的划分进行了优化调整，共分为 15 个一级安全分类，107 个二级细分领域。《全景图》推算我国网络安全企业 2022 年度整体收入约为 1014 亿元，相比 2021 年度整体增长率为 20%，且预计 2023 年将重回到 30% 以上。

No.4 ▌中国信通院发布《中国数字经济发展研究报告（2023 年）》

4 月 27 日，中国信通院发布《中国数字经济发展研究报告（2023 年）》[11]，该报告首次研究了我国数字经济发展效率水平，并得出如下核心观点：（1）我国数字经济进一步实现量的合理增长，数字经济规模达到 50.2 万亿元，同比名义增长 10.3%，增速连续 11 年高于同期 GDP 水平。（2）我国数字经济结构优化促进质的有效提升，数字产业化规模与产业数字化规模分别达到 9.2 万亿元和 41 万亿元，占数字经济比重分别为 18.3% 和 81.7%，数字经济的二八比例结构较为稳定。（3）我国数字经济全要素生产率进一步提升，数字经济全要素生产率为 1.75，数字经济生产率水平和同比增幅均高于整体国民经济生产效率。（4）我国数据生产要素价值进一步释放，加快数据产权、流通交易等基础制度建设，解决数据价值释放过程的系列难题；同时，数据产业体系得到进一步健全。

No.5 ▌中国网络安全产业联盟发布《美国情报机构网络攻击的历史回顾》

4 月 11 日，中国网络安全产业联盟发布由安天撰写的报告《美国情报机构网络攻击的历史回顾》[12]，旨在系统梳理美情报机构对全球各国开展的网络攻击活动，揭露美方网络霸权对全球网络空间秩序构成的重大破坏及严重威胁。《历史回顾》按照时间和事件脉络，共分为 13 篇，主要包括美国情报机构网络攻击他国关键基础设施，进行无差别网络窃密与监控，植入后门污染标准及供应链源头，开发网络攻击武器并造成泄露，纵容渗透测试平台成为黑客工具，干扰和打压正常的国际技术交流与合作，破坏网络空间国际秩序和市场规则，阻碍全球信息技术发展，制造网络空间的分裂与对抗等。

注：以上内容由安天前瞻研究中心搜集整理。

参考资料

[1]《关于调整网络安全专用产品安全管理有关事项的公告》
http://www.gov.cn/zhengce/zhengceku/2023-04/18/content_5751982.htm
[2]《2023 年数字乡村发展工作要点》
http://www.cac.gov.cn/2023-04/13/c_1683027266482224.htm
[3]《2023 年度第一批网络安全国家标准需求的通知》
https://www.tc260.org.cn/front/postDetail.html?id=20230413185511
[4]《关于加强新时代检察机关网络法治工作的意见》
https://www.spp.gov.cn/spp/xwfbh/wsfbt/202304/t20230418_611553.shtml#1
[5]《零信任成熟度模型 V 2.0》
https://www.cisa.gov/news-events/alerts/2023/04/11/cisa-releases-zero-trust-maturity-model-version-2
[6]《改变网络安全平衡：设计安全与默认安全的原则和方法》
https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3361073/nsa-us-and-international-partners-issue-guidance-on-securing-technology-by-desi/
[7]《网络团结法案》
https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2243
[8]《2023 Q1 网络安全产业重点洞察》
http://www.myzaker.com/article/642a4fb38e9f090ff245df9a
[9]《新兴技术：安全—网络威胁检测与响应（NDR）采用增长洞察》
https://www.gartner.com/document/4244799
[10]《网络安全行业全景图》
https://www.aqniu.com/focus/jiaodiantua/95236.html
[11]《中国数字经济发展研究报告（2023 年）》
http://www.caict.ac.cn/kxyj/qwfb/bps/202304/t20230427_419051.htm
[12]《美国情报机构网络攻击的历史回顾》
http://www.china-cia.org.cn/home/WorkDetail?id=643368b50200340e00ff4fc7

安天官方微信

安天开放资料平台

北京运营总部
地址:北京市海淀区闵庄路3号
清华科技园玉泉慧谷一期1号楼
邮编:100195

哈尔滨总部基地
地址:哈尔滨市松北区世坤路838号
科技创新城7号楼
邮编:150028

北京、成都、武汉、深圳、上海、沈阳、南京七地研发中心

内部资料 赠阅参考