移动安全十年形势发展白皮书

360手机卫士 10周年

前言

万物互联时代，移动互联网伴随着移动网络通信基础设施的更新换代，得到极速发展。近十年中，智能终端设备的普及、移动电子商务的崛起、移动支付的全民化，为移动互联网的发展成功助力。与此同时，移动安全问题也更加突出。恶意程序入侵、电信骚扰加剧、个人隐私信息透明化、黑灰产业“蓬勃发展”已成为移动互联网所面临的新一级“挑战”。

应对移动互联网中暴露的各项安全问题，360 应时进入移动安全“主战场”，360 手机卫士应声而出。秉承 360 母品牌“安全第一”的基因，经过多年的持续发展，累计用户超过 10 亿人，成为国内用户量最多的手机安全管理软件。同时，360 手机卫士的市场占有率也始终保持在领先地位。

安全是每一个手机用户最关注的问题。360 手机卫士上线以来，共识别拦截骚扰电话 1768.5 亿个；为全国用户拦截各类垃圾短信约 2993.7 亿条；拦截各类钓鱼网站攻击 138.8 亿次；截获手机恶意程序超过 4966.3 万个；平均每天截获新增手机恶意程序样本近 1.8 万个；日识别拦截骚扰电话约 0.88 亿次；日拦截垃圾短信条 1.09 亿条。（数据来源于 360 报告中心，统计截止到 2019 年 6 月 30 日）有效保护了用户设备安全与个人信息安全。

2018 年，360 手机卫士应对高发网络欺诈现象，推出“应龙反诈平台”。通过建立线索关联、预警识别机制、丰富的拦截策略和针对性劝阻的全面反制诈骗的措施，实现发案率的持续回落、破案率提升，弥补现有治理工作对诈骗电话准确性、隐蔽性、发现及处置能力的不足，实现提升整体通信反诈环境的和谐发展，降低电信诈骗的社会危害性。目前，“应龙反诈平台”已成功帮助公安降低报案率，帮助运营商减少投诉率，提升业务排名。

针对日益复杂化的安全威胁，以及电信诈骗高发态势，360 手机卫士发起 “全民守卫”计划。综合多种技术手段全面升级安全风险提醒机制、联合公安、运营商、高校、媒体共同一起，向电信诈骗“Say No!”，让每一个手机用户都能安心地享受手机带来的便捷生活。

目录

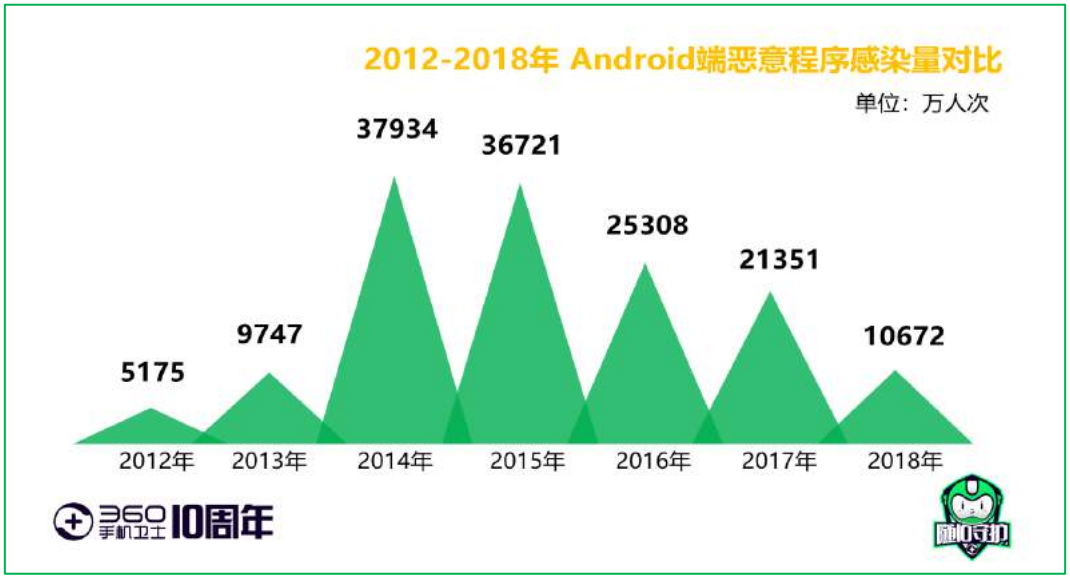
移动端近十年内安全态势发展

1. 恶意程序转战新兴战场

随着智能手机的功能越来越强大，手机应用体系的日益完善，用户使用手机联通网络的行为日益增多，手机病毒的行为开始向多元化，层次化方向倾斜。新兴手机病毒紧随移动互联网的发展而演进，并开始出现程序“自我保护”机制，多个威胁进程互相守护，用户安装后，无法利用系统自带卸载功能进行手工清除。

转入 2011 年，基于移动操作系统平台，以各类手机应用软件为标志的移动互联网进入井喷式增长。Symbian 系统市场占有率的持续下降，安卓平台在手机系统市场的占有率持续提升。由于几乎没有入驻门槛，木马制作者可以通过篡改正常软件的方式，随意将捆绑了木马的软件应用在 Android 平台发布。于是，恶意程序开始转战安卓，（360 数据） 2011 年下半年 Symbian 平台被感染人数为 1049 万人次，比上半年的 1206 万人次下降 13%。从 2011 年 8 月起，Android 平台每月新增木马连续 4 个月超过 Symbian 平台，安卓平台在新增安全威胁的增速与增量上全面居首，成为新的移动互联网安全攻防主战场。同时，随着 Android 平台“千元智能机”的迅速普及，安全问题“大爆发”也随之而来。手机病毒在此前主要针对塞班平台的基础上，开始将对更多手机系统平台构成威胁。移动端病毒紧随移动互联网的应用而广泛发展，植入方式更灵活、多变，增加了安全防护的难度。

如下图，从近七年的 Android 端恶意程序感染人次看，经过 2012-2015 年的高速增长期，2016-2018 年呈现下降趋势，说明手机恶意程序发展进入平稳期。



2. 电信骚扰成为新一级安全问题

随着我国移动互联网用户数量的增加，移动互联网的应用水平，终端普及，市场规模呈现迅猛增长态势。但在一系列热潮背后，智能手机的安全问题也愈发凸显，手机木马、恶意广告严重威胁着用户的隐私、话费、流量安全；垃圾短信、骚扰电话直接影响着用户的正常生活和信息安全。

手机用户频繁遭到电信骚扰的原因主要分为两点：一是用户主动填写给商户的个人信息导致骚扰不断，如商场会办理会员卡、买房时给中介电话、在网站上进行实名注册等等。二是，某些不法分子为充分挖掘资源，垃圾短信、骚扰电话的相关产业，形成了一条完整的黑色产业链。从上游的电话号码及个人信息的买卖，中游的经营垃圾短信群发、语音电话推销服务的公司，到下游广告主为垃圾产业持续提供大量资金支持，使得用户的智能手机时刻处于险恶的安全威胁之中。鉴于此，工信部等行业主管部门从 2013 年年末开始实施的垃圾短信严格治理政策；各大电信运营商也开始越来越重视用户体验，对于垃圾短信的过滤技术也得到了不断的提升。

360 等手机安全厂商通过不断的技术进步，使得垃圾短信绕过手机安全软件防护的 机会越来越低，从而使发送垃圾短信的商业价值越来越低。工信部等行业主管部门从 2013 年年末开始实施的垃圾短信严格治理政策逐步取得了一定的成效。各大电信运营商也开始越来越中是用户体验，对于垃圾短信的过滤技术也得到了不端的提升。

如下图，从近五年的骚扰电话标记与拦截统计看，随着骚扰号码标记库的样本积累，越来越多的骚扰号码在用户接听时已经有了标记提示，也是用户对号码标记数降低的原因。

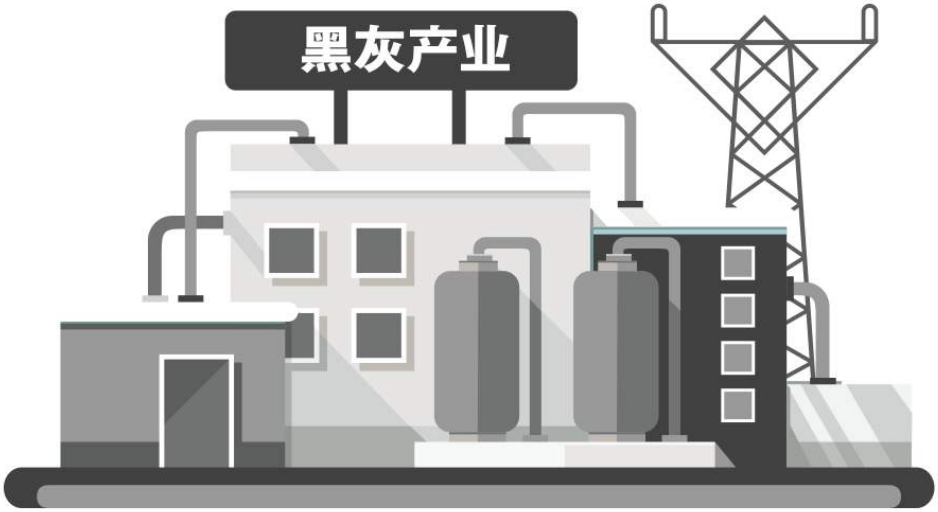
3. 全行业围栏打击黑灰产初见成效

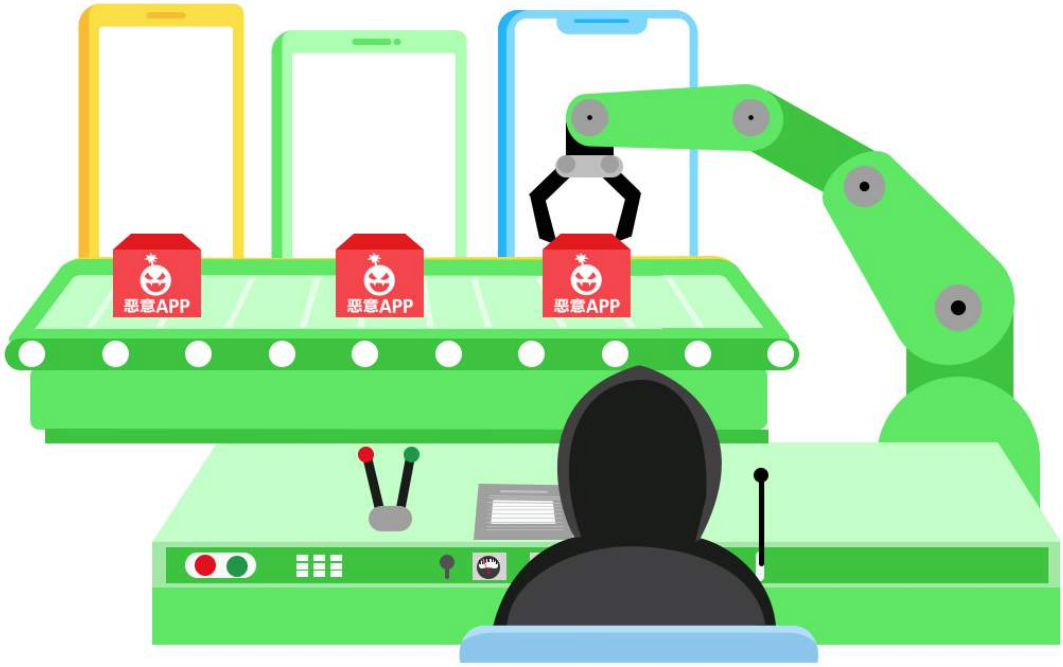
安全是互联网发展的基础，没有健全的网络安全环境，互联网就没有办法长久持续地发展。互联网黑灰产业的链条化已严重影响了互联网的正常发展与进步。鉴于此，互联网各行各业开始抱团，联合抵制黑灰产，打造政府+行业+用户的网络安全治理模式。党中央、国务院高度重视打击治理电信网络新型违法犯罪，各地、各有关部门，持续开展打击治理专项行动，侦破了一大批重大案件，捣毁了一大批犯罪窝点，抓获了一大批犯罪分子，为人民群众挽回了大量经济损失。互联网行业根据网络安全等级保护制度的标准，借助网络安全厂商的安全赋能，通过安全监测、态势感知等方式健全并提升自己的网络安全能力。互联网用户借助安全厂商的安全产品和安全知识播报，提升自身的网络安全识别和抵御能力。

4. 恶意样本制作实现规模化

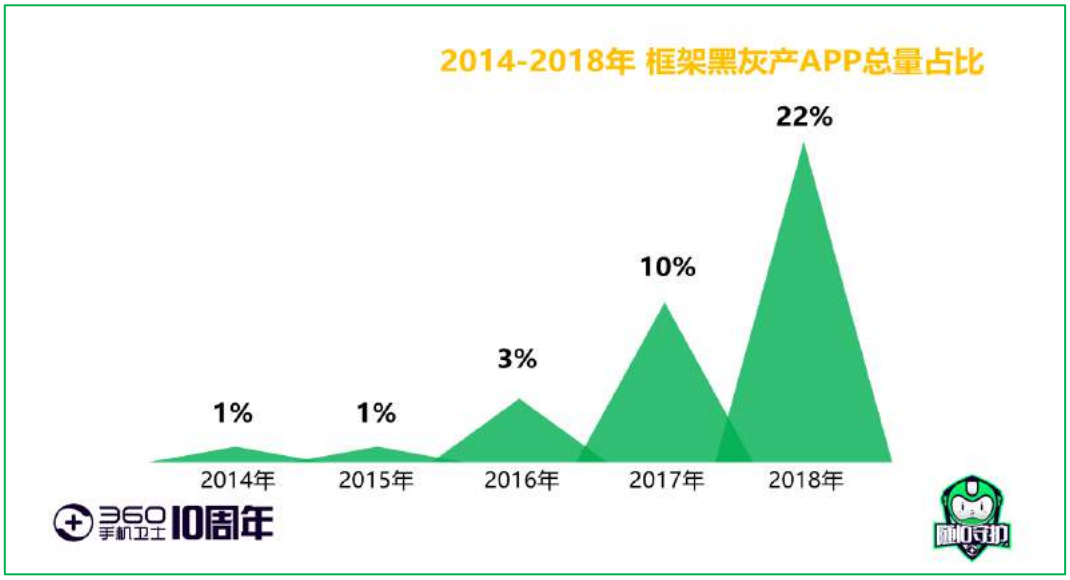
随着技术的发展，Android 平台的恶意程序制作成本逐渐降低，并且可以批量生成恶意程序，部分虚假购物类钓鱼网站，仅允许手机端访问，在 PC 上无法打开，钓鱼网站已经开始向移动端精准投放，针对移动端的攻击行为逐渐规模化。

APP 生成框架即是无需复杂技术编程即可实现 APP 开发的一种框架。使用 APP 生成框架开发 APP 能极大简化开发步骤、缩短开发周期并在一定程度上节约开发成本，因此越来越多有开发需求的人成为 APP 生成框架的用户。360 烽火实验室在对 Android 黑灰产的持续监测中发现，越来越多黑灰产开发者倾向于使用 APP 生成框架来开发黑灰产 APP。





如下图，从近五年全年黑灰产 APP 总量中框架开发黑灰产 APP 的占比情况看，自 2016 年开始，框架开发黑灰产 APP 数量与占比开始激增，到 2018 年，全年黑灰产 APP 总量中 22%均由框架开发。从框架开发黑灰产 APP 占比变化来看，黑灰产 APP 整体呈现框架化趋势，APP 生成框架在帮助众多用户实现开发梦的同时也给黑灰产提供了一种成本低廉的 APP 生产途径。



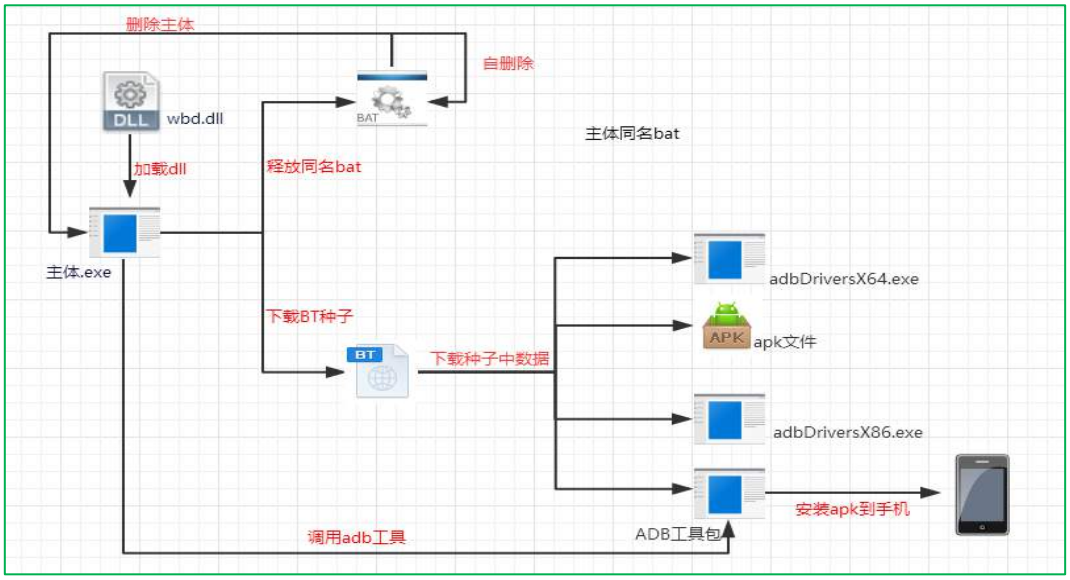
5. 恶意软件试图躲避安全厂商拦截

恶意程序不论是在技术手法，还是传播技法上，一直呈现花样翻新的势头。并且会利用知名的软件在人们心中的熟悉度，以假充真，骗取用户下载安装。

在技术上，黑客借助 Android6.0 系统版本的无障碍模式 Accessibility 和动态权限模型，通过社工技巧突破用户手法防线。此两个功能都需要用户主动授权后才可以使用，于是

Android 木马开始借助社工学，通过诱导性的图标和文字，引导用户授予相应的功能的权限，从而保证恶意行为的正常运行。黑客还应用界面劫持手法，在金融支付和主流的社交应用软件上，使用 Activity 劫持手段，弹出虚假的登录提示框，骗取用户的账号、密码等重要的隐私信息。

在传播渠道上，在采用“伪基站+钓鱼网站+手机木马”的传统方式进行网络诈骗活动时，仍开拓新的传播渠道。在手机通过 USB 方式连接到电脑时，恶意程序通过 PE 文件释放 adb 工具包，在手机上静默安装恶意的 apk 进行传播。



6. 移动平台成为勒索软件的重灾区

受系统的影响，敲诈者木马在 PC 平台肆虐，给用户造成巨大损失。同样在移动平台，勒索软件也逐渐形成规模，尽管相比之下的移动平台损失相对较轻，但同样带来的是用户“花钱消灾”的心态以及立案条件的不足。导致勒索软件的作者仍会肆无忌惮。360 烽火实验室发现勒索软件在勒索页面的设计和文字上都有很多相似的地方，其中最为典型的特征是勒索页面中都留有制马人联系方式，方便中招的受害者与制马人联系，以便制马人对受害者进行敲诈勒索，这些联系方式几乎都是 QQ 号或者是 QQ 群。制马人肆无忌惮制作、传播勒索软件进行勒索敲诈，并且大胆留下自己的 QQ、微信以及支付宝账号等个人联系方式，主要是因为他们年龄小，法律意识淡薄，认为涉案金额少，并没有意识到触犯法律。甚至以此作为赚钱手段，并作为向他人进行炫耀的资本，加速了手机勒索软件的演变。

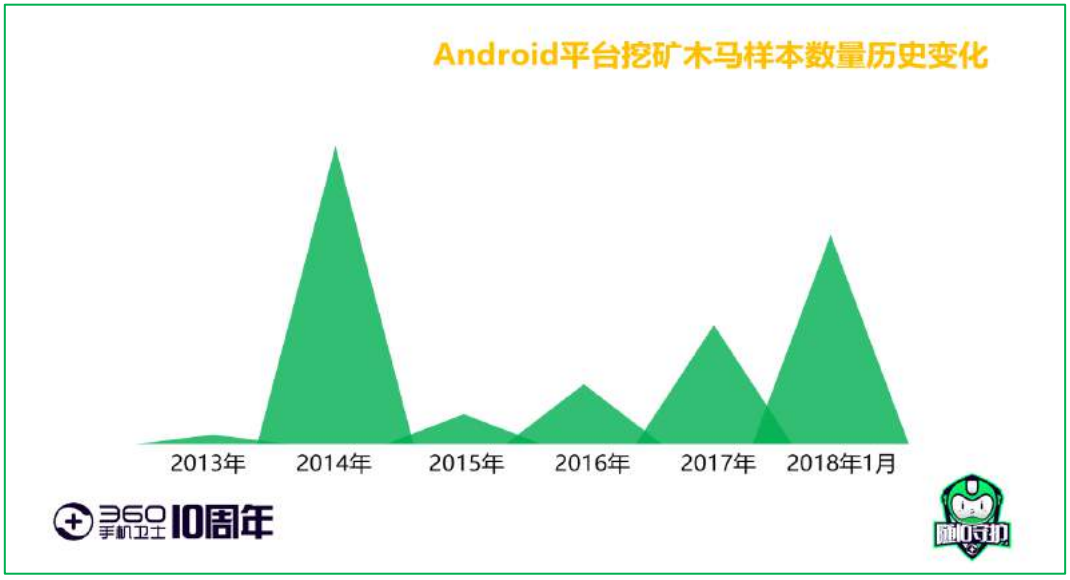
自 2016 年起，360 烽火实验室在勒索软件黑产研究中就发现了大量使用 Android 易语言（E4A）一键生成的勒索 APP，而事实上，E4A 只是市场上众多 APP 生成框架中的一种，近几年 360 烽火实验室陆续收集了数万种 APP 生成框架，同时更是捕获到了上百万利用这些 APP 生成框架开发的黑灰产 APP。

7. 智能设备爆发式增长，移动端的攻击越发明显

随着智能设备爆发式增长,存储着的个人核心隐私信息越来越多，设备及信息所带来的价值也越来越高，针对移动端的攻击也越发明显。2017 年最疯狂的莫属电子货币，以比特币为代表的电子货币，年内单价突破了 2 万美元，随着电子货币价格暴涨，种类增多，针对电子货币相关的攻击事件也越来越频繁。在移动平台上，从 2013 年开始至 2018 年 1 月，360 烽火实验室共捕获 Android 平台挖矿木马 1200 余个，其中仅 2018 年 1 月 Android 平台挖矿木马接近 400 个，占全部 Android 平台挖矿类木马近三分之一。

如下图，从 Android 平台挖矿木马样本数量历史变化看，2014 年 Android 挖矿木马经过短暂的爆发后，于 2015，2016 年逐渐归于平静。主要原因是受到当时移动平台技术等限制，以及电子货币价格影响，木马作者的投入和产出比不高。但随着 2017 年年底电子货币

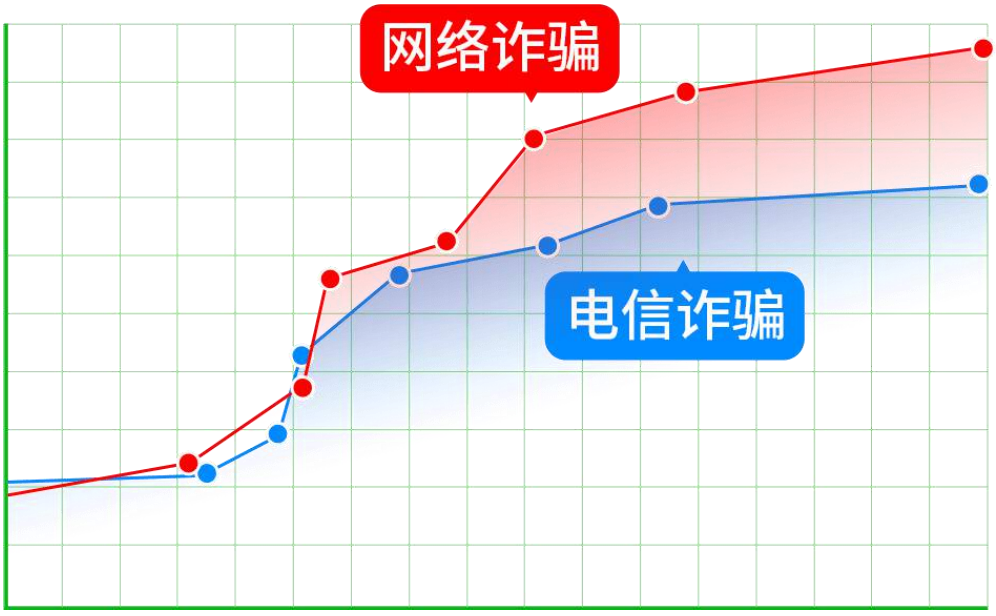
价格的一路高涨，挖矿技术的成熟，再次成为木马作者的目标，手机挖矿木马在也呈爆发式增长。



8. 移动互联网衍生黑灰产业成熟致网络诈骗案件频发

移动互联网的技术进步，智能设备的性能增强，带动了关联产业的演变与成长。各家企业借助移动互联网的东风，开展各种线上营销活动，提升了企业的“美好”形象。各类互联网黑灰产业借助移动互联网的“红利”，打造出自身的生态体系。上游售卖各类基础资源，如手机号、银行卡、IP、域名、猫池，社交软件账号；中游黑灰产运营人员通过群控系统、代刷脚本、CDKEY 工具批量薅取企业营销活动的羊毛；通过群控系统，代刷广告，短视频等产品的流量，伪造产品及产业的真实情况；通过冒充身份，虚假网站，虚假应用等手法实施欺诈活动。下游资金转移人员，通过伪造、套取身份等方式，使用第三方、第四方支付渠道批量转移资金。

黑灰产业的成熟，导致网络诈骗案件频发。2019 年上半年 360 手机先赔共接到手机诈骗举报 2508 起。其中诈骗申请为 1095 起， 涉案总金额高达 638.0 万元，人均损失 5826 元。 从涉案总金额来看，赌博博彩类诈骗总金额最高，达 248.0 万元，占比 38.9%；其次是 金融理财诈骗，涉案总金额 160.1 万元，占比 25.1%；身份冒充诈骗排第三，涉案总金额为 109.6 万元，占比 17.2%。


网络诈骗
电信诈骗

移动端近十年安全大事件

1. 隐私安全危机爆发

✧ Carrier IQ（简称 CIQ）事件

2011 年 12 月，一款名为 Carrier IQ（简称 CIQ）的内核级间谍软件被曝光，该软件会暗中收集用户隐私信息，甚至每按下一次键盘都会秘密地记录在案。CIQ 原本是一款用来监测手机使用情况的应用程序，它会根据手机使用情况提供具体数据，以指导手机用户，方便手机生产商提高产品质量和服务水平。包括苹果、HTC、三星在内的手机制造商，以及 AT&T、Sprint、T-Mobile 等运营商都在手机上预装 CIQ 软件，已被预装在全球 1.41 亿部手机中。中国不少智能手机用户，尤其是水货手机用户也受到影响。

对此，360 安全中心紧急推出了国内首个 CIQ 查杀工具，并率先实现了全平台查杀，不仅可对手机系统进行深度扫描，精准识别隐藏在系统深处的 CIQ 程序，更能彻底并永久禁用其服务，保证隐私安全，有数千万手机用户通过 360 手机卫士进行 CIQ 间谍软件的查杀。

✧ 快递单信息泄露事件

电商网购的兴起带动了快递行业的迅速发展，但自 2012 年起，由于快递单信息泄露引发的恶性案件屡屡发生，引起了社会各界的广泛关注。通过调研发现，在一些平台网站内，快递单号被明码标价进行销售，售价从 0.4 元到 2 元不等，并附带“底单”等配套服务。该平台内发布的单号信息中，包含了快递单号、发货地址、收货地点、是否扫描等内容，根据各个单号的不同情况，售卖的底单价格也不同。除了这类专业网站，在各大社交平台中，销售快递单号的现象也十分火热，网络中充斥着各类“售快递单”的社交群，群成员人数多达 500 人。销售更累快递单信息、单号生成器，甚至有人直接出售物流系统，可供客户新建快递单号与物流信息。这类“地下产业”的发展，致使电商平台内商家“刷信誉”作弊行为得到支持。

内容截选：

人民网——《快递单号成泄密条摇钱树 私营公司泄露最多》

报道链接：http://finance.people.com.cn/n/2012/1116/c70846-19606097.html

2. 签名漏洞是手机沦为“肉鸡”

2013 年，据业内专家了解，国外研究人员声称发现了一个 Android 严重漏洞，此漏洞从 Android1.6 开始就一直存在，影响过去 4 年间发布的 99%的 Android 手机。业内专家将该漏洞定义为“安卓系统 Master Key 签名漏洞”。

业内专家介绍，数字签名可以保证每个应用程序来源于合法的开发商，这是整个安卓操作系统得以控制风险的一种至关重要的安全校验机制。由于此漏洞允许攻击者修改应用程序的代码，但不会改变其加密签名，使得绝大多数安卓设备面临巨大风险：不法分子可在不破坏 APP 数字签名的情况下，篡改任何正常手机应用，并进而控制中招手机，实现偷账号、窃隐私、打电话或发短信等任意行为，使手机瞬间沦为“肉鸡”。

当前已经有大量热门软件被“安卓系统 Master Key 签名漏洞”感染，不法分子可以在某个软件客户端中植入带盗号、偷隐私、后台发短信的恶意程序，告诉用户，这是一个升级版本。如果签名不同，这个升级版本安装时，系统会报错，提示签名有异常。然而，利用漏洞构造的恶意程序却有和正版软件完全一样的签名，安装时系统就不会报错，用户会把这个盗版的软件误认为这是一个完全正常的官方软件。

安卓系统之所以成为信息安全问题频发的重灾区，一方面由于安卓系统的开放性，使得众多手机应用厂商参差不齐，另一方面受巨额利益的驱使，一些不良厂商在正规应用中捆绑恶意软件，更有一些不法分子利用恶意软件肆无忌惮窃取用户本机号码、通讯录等隐私数据，然后将其贩卖至一些营销机构，从而导致用户受到越来越多的骚扰。

同年 7 月下旬，360 互联网安全中心截获了一批利用该漏洞实施攻击的手机木马，这类使用了合法签名的木马会导致手机隐私被窃、自动向通讯录联系人群发诈骗短信及私自发送扣费短信。这类木马涉及游戏、壁纸及网银等多种软件，并且绝大多数都是来自应用商店，危害性和传播性不容小觑。

内容截选：

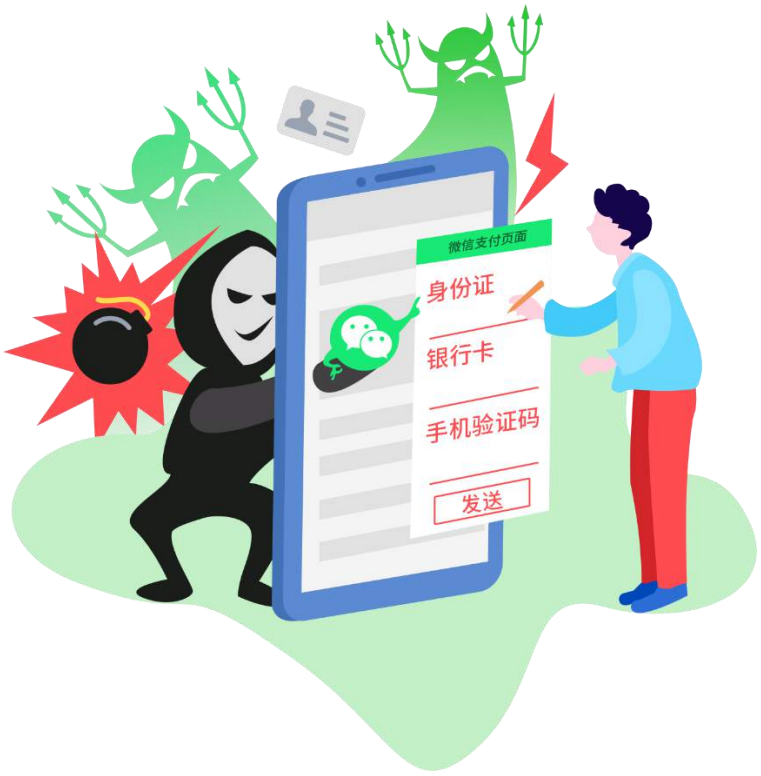
工控网——Android 又爆高危漏洞 加密软件封堵泄密源头

报道链接：http://www.gongkong.com/news/201307/61328.html

3. 移动支付安全日益严峻

✧ 微信变“威信”窃隐私木马

2014 年春节期间，最为火爆的新年活动莫过于微信抢红包，据统计，从除夕开始，截止大年初一 16 点，参与抢微信红包的用户超过 500 万，总计抢红包 7500 万次以上。假红包也伺机出现，不少网友反映，收到了 802 元的“巨款”红包，但“拆开”后却发现钱并没有进到自己的口袋，抢不到红包其实是小事，如果骗子发来的是钓鱼网站，或者木马下载链接，根本无法辨别，不留心输入了密码等信息，微信关联的银行卡存款将面临极大风险。



恶意篡改以及伪装成微信的手机木马也越来越多。2014 年 6 月，伪装成微信支付界面的手机木马“鬼脸银贼”，通过诱骗手机用户在加微信支付界面输入身份证、银行卡号等敏感信息并偷偷发送到黑客邮箱，以此大窃钱财。同年 11 月初，“微信鬼面”手机木马，伪装成“微信支付功能”，接收木马作者的短信指令使中招手机向外发送短信，还能将中招手机新收到的短信转发给木马坐着。双十一期间，一款恶意篡改“微信电话本”的手机木马会通过中招手机的通讯录向所有联系人群发短信，还能在后台私自发送扣费信息，甚至还能判断手机中是否安装了安全软件逃避查杀。

微信的功能越来越多，微信支付已成为人们日常中便捷支付的常用工具。但一些不法分子也借机利用钓鱼网址、手机木马大肆作恶，微信安全已经成为手机用户不可忽视的移动安全问题。

✧ “套牌木马”劫持支付宝偷钱

2014 年 10 月 24 日，360 互联网安全中心截获一个利用（Activity）安卓系统组件的“套牌木马”家族，能够修改中招手机中“爸”“妈”“哥”“姐”等家人的手机号码，更为危险的是，这一家族的木马还会使用 Activity 劫持方法将正版支付宝付款页面替换为钓鱼页面，窃取支付宝账号和密码。

“套牌木马”会在中招手机中执行三类恶意行为，一是劫持支付宝骗取手机用户的支付宝账号和密码，二是修改手机中“爸”“妈”“哥”“姐”等类型家人昵称存储的联系人号码，三是窃取手机中全部短信、通话记录以及联系人等隐私信息。

4. 电信诈骗——账户资金异常变动诈骗爆发

2015 年 7 月以来，360 互联网安全中心突然接到大量用户反馈，称自己的网银账户无故接到账户资金支出的通知短信，随后接到客服人员的“理财产品购买确认”电话。用户为了找回自己的资金，将收到的验证码告知给对方后，账户资金全部损失。7-10 月间，全国各地均出现类似骗局，用户损失从几千元到几万元不等。

实际上，这是一种综合利用用户个人信息实施的新型网络诈骗，识别和防御难度极高。骗子们受限盗取了受害者的网银账号和密码。但由于没有 U 盾或验证码，骗子们无法真正完成网银盗刷。于是，骗子们再登陆受害者网银账户后，使用受害者网银内的存款，执行购买贵金属或活期转定期等账户内部资金操作（此类操作一般不需要使用 U 盾或验证码），从而造成受害者网银账户有欠款流出的假象。之后骗子再假冒电商客服联系受害者，以帮助受害者退回钱款为由，骗取受害者手机验证码，并最终完成对受害者网银的盗刷。

此类新型诈骗手法的出现，是对传统网银账户安全体系的一次重大挑战，不仅引起了媒体的高度关注，同时也引起了各大银行的高度关注。9 月以后，各大银行都纷纷出台了各种新的账号保护措施。进入 11 月以后，这类诈骗的报案量大幅减少。

5. 史上最严手机“实名制”实施

2015 年 9 月 1 日，史上最严手机卡实名制将开始实施，工信部出台实名制政策的主要目的在遏制电信诈骗问题。电信专家表示，实名制实施后将提高犯罪分子作案的成本，但并不会彻底解决电信诈骗问题，对于手机用户来说，还需提高防范意识。

据悉，为缓解频发的电信诈骗问题，工信部也将推出“电话黑卡治理专项活动”，全面推进未实名老用户补等级工作，未实名用户在未来办理业务是将会收到一定程度的限制，甚至有被停机的风险。

6. 微信支付宝不实名认证支付受限

《非银行支付机构网络支付业务管理办法》（以下简称《办法》）将于 2016 年 7 月 1 日正式生效，支付机构将对客户实行实名制管理。根据《办法》要求，7 月 1 日之前，各支付机构实名率需满足 95%。届时未进行实名登记，支付宝、微信账户将受限。《办法》要求，支付账户将严格实行实名管理，并按照三类支付账户分级管理。如果用户身份验证情况未达到《办法》所规定标准，会影响支付账户部分功能使用。

7. 徐玉玉被骗不幸离世案件引发广泛关注

即将踏入大学的 18 岁山东女孩徐玉玉，2016 年 8 月 19 日接到了一通诈骗电话，结果被骗走了上大学的费用 9900 元。得知被骗后，徐玉玉伤心欲绝，郁结于心，最终导致心脏骤停，虽经医院全力抢救，但仍不幸于 21 日离世，让人扼腕。

随后，在公安部统一指挥下，涉案的 8 名犯罪嫌疑人悉数归案。据报道，此次精准诈骗案中至关重要的“窃取个人信息”环节，竟然出自一个同样只有 18 岁的四川宜宾少年杜天禹之手。而其他几位犯罪嫌疑人中，也有三人为 90 后，一人年仅 19 岁，都是与受害人徐玉玉年龄相仿的年轻人。

8 月，除了徐玉玉案件，山东临沂考生遇电信诈骗后心脏骤停不幸离世、清华大学教师被骗 1760 万、女大学生被骗 3 万后遭骗子嘲讽、广东大学女生被骗后投海自尽……一起起电信诈骗案件，敲响了整个社会的安全警钟。

8. 不法分子借势世界杯传播恶意程序

世界杯激战正酣，全世界的球迷也开启了一个多月的狂欢。然而，今年的世界杯却爆冷结果频出，继梅西、C 罗之后，夺冠大热门西班牙也悲情出局，不少球迷戏称俄罗斯世界杯为最“冷”的一届世界杯。但是，再“冷”的世界杯也抵不住不法分子的借势热度。今日，有用户反馈，一些恶意程序在世界杯期间顶上了球迷手机，非法侵入造成用户隐私泄露。

由于安卓系统自身的开放性，安卓手机往往会成为恶意软件的目标。据相关用户反馈，世界杯期间，游戏类恶意软件大多会通过垃圾短信、不正规应用商店等渠道进行传播。其中，垃圾短信里经常会附有不明链接。如有不明真相的用户下载并安装此类软件，手机便会在用户不知情的情况下发生“悄然转变”。比如，一些恶意软件会强行捆绑推广其他恶意软件，并自动下载和安装到用户手机，或是更改用户手机导航和浏览器主页等。

除此，不法分子还会假借世界杯的名义肆意传播木马病毒，此类恶意软件的危害性更是不容小觑。这类恶意软件借由“预测比赛结果”类诈骗短信、“销售虚假世界杯门票”类钓鱼网站等渠道传播，一些禁不住诱惑的球迷朋友变回下载安装到木马软件。

这类恶意软件不仅会暗中捆绑下载其他应用软件，导致用户手机资费、流量、性能等出现损耗，用户手机内的个人信息等重要隐私也存在泄漏风险。一旦用户隐私遭泄漏，转瞬就会流入个人信息贩卖黑色产业链，被不法分子用来实施精准诈骗，由此可能产生的损失更为严重。据相关统计数据显示，在一周内短信内容中包含“世界杯”关键词且成功拦截的短信数量高达 2.4 万条，其中，大多数为赌博短信，并附有赌博网址。

9. P2P 网贷“爆雷”潮

2018 年 6 月以来，全国范围内集中出现了百余起 P2P 网贷平台清盘、停业、实际控制人失联、停止兑付本息等风险事件。进入 7 月后，网贷平台的“爆雷”愈演愈烈，我过 P2P 行业面临着前所未有的流动性危机和生存发展的挑战。

网贷平台“爆雷”的一个突出特点是，出问题的不少是规模较大的 P2P 平台，其中不乏拥有国资背景和运营多年的知名网贷机构。从风险性质看，此次 P2P 平台的倒闭大致分为两种类型：一是直接关停，由于资金链断裂、实际控制人失联或因涉嫌非法吸收公众存款被警方立案侦查等原因，平台停止运营或不在兑付本息。另一种是良性清盘，即因流动性枯竭等原因，P2P 平台主动决定良性退出网贷行业，并承诺不跑路，不失联，及时追回欠款，未来几年内分批次兑付所有资金。

整体而言，此阶段 P2P 贷款平台良莠不齐，“跑路”风险随时都有可能爆发。一方面平台对于借款人是否有偿还能力、“一户多贷”等资质调查和审核不过关，导致逾期率和坏账率上升；另一方面也不乏一些不法分子打着贷款平台的幌子实施违法、诈骗行为或在贷款时就没想还的“骗子”。

内容截选：

一财网——《频频爆雷，P2P 网贷行业走向何方》

报道链接：https://finance.sina.cn/2018-08-05/detail-ihhhczfc0730430.d.html

10. 半夜收到白条验证短信的“GSM 劫持+短信嗅探”

用户反馈出现了一种新的诈骗行为，一觉醒来后发现手机收到数条验证码和银行扣款短信，甚至还有的因此莫名“被网贷”，蒙受了极为严重的经济损失。李女士(化名)便是此类诈骗案件中的一名受害者，她在凌晨接收到来自银行、京东和支付宝平台的 100 多条验证码后，发现自己钱款全部被转走，京东平台还开通了金条、白条功能，被借走一万多元。

上述案件，不法分子通过利用“GSM 劫持+短信嗅探”技术，可实时获取用户手机短信内容，从而利用银行、网站、移动支付 APP 的技术漏洞和缺陷，最终实现信息窃取、钱款盗刷、私自借贷等诈骗犯罪的目的，这是一种最新型的网络电信诈骗手法。虽然对于普通民众来说，“GSM 劫持”还属于较为陌生的词汇，但是“伪基站”却早已被人们熟知，大致来说，“GSM 劫持”便是“伪基站 2.0 版本”，属于伪基站的技术再升级。不法分子通过伪基站劫持的方式将用户的手机降为 2G，然后利用技术手段获取到一定范围内潜在的手机号码后，再利用“GSM 嗅探”技术来窥探用户短信中的验证码信息，以便他们完成密码重置、身份验证等步骤。据悉，不法分子的劫持对象主要针对那些处于 GSM 网络中的手机，有时也会干扰附近的手机信号使之降级到 2G 信号后，窃取用户短信信息，然后通过登录其他网站，试图掌握用户更多隐私信息，继而盗刷用户的钱款、冒充受害者进行消费或套现。整个过程中，不法分子无需直接与受害者接触，只需利用“GSM 劫持+嗅探技术”就可以窃取用户的短信信息，因此用户毫无知觉。它就像是一条经过专业训练的狗，悄无声息地辨别事物，所以也被专业人士叫做“短信嗅探”技术。

GSM 协议的问题早已经被关注到，目前该方面的系统也在换代升级中。通过近期出现的各种利用截获短信验证码等方式实施的网络诈骗行为来看，未来确实有必要提出多项加强身

份验证安全性的措施。除常用的短信验证码外，还可以考虑新增图片验证、语音验证、人脸验证、指纹验证等等诸多二次验证机制。

11. 流量造假，明星应援 APP

走过 2018 的偶像元年，一茬又一茬的偶像新星们从节目中诞生偶像数量增长，各家粉丝为了打榜、轮博、集资、反黑粉更是忙的不可开交。追星 App 便是为粉丝提供高效追星服务的平台，帮助粉丝在错综复杂的环境中更加迅速的对偶像的一切动向了如指掌。某明星一亿微博转发量幕后推手“星援 APP”被查封，撕开了流量造假产业链的一角。

此类用户流量造假产业的明星应援类 APP，通过月租费或功能收费等方式收取费用，包含很多关注明星动态功能，如时刻提醒所关注明星的社交动态，一键查看明星行程动向。监控微博、贴吧平台上出现所关注明星的黑帖，实时生成举报链接。微博、贴吧、爱奇艺等平台实现一键签到，各种投票类榜单的一键投票打榜。

互联网科技公司或艺人经纪公司开发应援类 APP。粉丝自发或艺人经纪公司给粉丝安排刷榜任务，帮助粉丝组建刷量数据组，应援群。粉丝通过内部圈、微信公众号、应用商店等方式下载应援 APP。粉丝为完成各种任务（明星转发量，热搜），纷纷利用各种应援 APP，轮播，刷榜，帮助“心爱” 的明星刷出大量的虚假流量。为获得与所追明星见面或者获得粉丝周边的产品，利用各种应援 APP，抢占所追明星的热评。为帮助所追明星完成线上或线下的活动，在应援类应用充值开展众筹活动。

从粉丝角度看，虽然这是一种粉丝自愿行为，但属于数据造假，违反了《中华人民共和国电信条例》和《北京市微博客发展管理若干规定》中关于实名制注册，不得以虚假身份办理入网手续，实施扰乱网络传播秩序的法律规定，应予以禁止。

从平台角度看：平台作为网络服务提供者，有审核及监督义务。“根据《侵权责任法》第三十六条规定，平台需在未履行网络服务提供者义务的情况下，承担侵权责任。”另外，根据《网络安全法》《电子商务法》相关规定，平台有义务核实应援项目真实性，监管资金去向，以保证网络安全，保障电子商务交易安全。

12. 走路就能赚钱的“趣步 APP”

“走路赚钱”在近期一跃成为大众热点话题，随着趣步 APP 的话题性日渐深入，区块链又一次进入大众视野。“立足运动健康领域，以区块链技术为支撑，开发并运营趣步及网络

商城，鼓励全民关注自身健康，参与快乐运动的创新型科技公司”这是趣步的宣传口号，看似简单快捷的赚钱方式，实则是一家利用区块链实施诈骗的非法企业。

1） 以区块链的旗号吸引眼球

区块链，通俗来讲是由一组技术实现的大规模、去中心化的经济组织模式。对于区块链，人们通过比特币了解了这项技术，比特币作为最早的虚拟货币，在中国虽得到禁售，但比特币的价值也获得了人们的认可。无形中，一些运用区块链技术的企业得到了更多人的关注。

而趣步在运营期间声称有国家颁发的区块链牌照，这使更多用户相信平台的真实性，并放心大胆的进行投资。实际上，国家并没有任何部门颁发虚拟货币运营牌照，平台属于虚假宣传，利用国家认可的噱头获得更多曝光度。

“用趣步每天走路 4000 步”=“月入十几万元”+“饭店、旅游、健身、宾馆甚至买房服务”“零投入，走路就赚钱，这样的好事是真的吗？”“趣步每天 4000 步，手机变成摇钱树！”。这些是趣步运营期间，网络上流传的宣传话语，走路赚钱确实是一种新鲜方式，再加上趣步洗脑式的宣传，更多的人愿意接受这一形式去进行尝试。

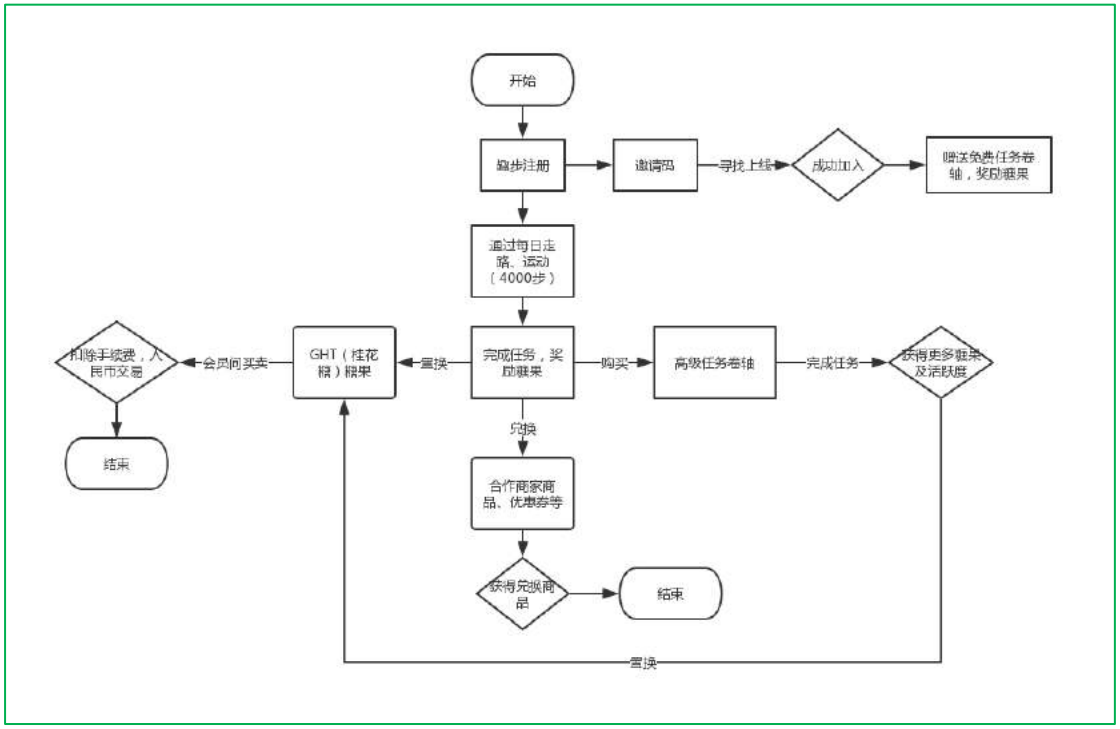
2） 趣步“传销式”的运营模式

在趣步平台流通的是一种叫做“糖果”的虚拟货币，平台声称利用“区块链”技术以人体运动计步来计算“糖果”的产量，参与者的每一步都能够产出“糖果”。号称不出售糖果，只能通过运动的方式获取，并且有数量上限，总量为 10 亿枚、永不增发，糖果不具备货币功能，只是为了奖励爱运动的人们，可以利用糖果在商城中兑换商品。但同时，趣步 APP 中又支持糖果兑换成 GHT（桂花糖），这种糖果支持用户间交易，而价格每日间有浮动。交易就需要扣除手续费，由平台收取。这种否认糖果价值又支持糖果交易的“双标”举动，可见其中蕴含猫腻。

在趣步中，通过每日任务可获得少数糖果。如果想要积攒更多的糖果，则需要购买任务卷轴，购买卷轴的同时，需要花费现有糖果。但后续完成卷轴任务后，每日可获得更多上限的糖果，每日步数要求也随之增长，并可获得活跃度。玩法简称，想获得更多的糖果，就需要完成更高级的任务。利用这种手法，带动更多的用户进行活动。

那么问题来了，要获得更多的糖果，需要用一定数量的糖果换卷轴，可换卷轴的钱从哪来？如果想依靠每日系统赠送的糖果，确实需要很长一段时间，于是，拉新成为一种主要方式。通过趣步内推荐码拉拢身边的人参与，即自己的下线。如果通过“直推”形成团队，成

为星级达人，则给予更高的奖励。可获得全球手续费分红。前期想进入趣步，同样需要寻找上线，才可加入，高息返佣、发展下线，属于明显的“传销”手段。



3) 趣步“糖果”交易运用形式

在趣步注册期间，要求用户以个人真实信息绑定，并使用与支付宝类似的刷脸。此要求成为硬性要求，向用户表达了，趣步是一款正规化、流程化的可持续发展平台。在交易时，用户可在平台通过低价买入桂花糖，寻找机会高价卖出的方式达到获得收益的目的。但收益是需要建立在糖果有价值的基础上，通过以上分析可得知，如果用户花费资金“囤”糖果，只会造成资产亏空。这种形式，糖果为一种虚拟货币的现象就更加明显。官方承诺的 10 亿固定数量并没有在此得到体现，更像是要多少则有多少，趣步作为“资金盘”的特性越见明显。

由于趣步不承认糖果含有货币价值，建立了交易平台，但并不支持平台交易。用户间交易需要通过私下转账方式进行，交易完成再由糖果的卖方支付给买方糖果。再回头看，趣步用户间存在多个交流群，每个群都有领导者、运营者，并有人在群里喊话卖糖果。猜测这些卖方都是诈骗平台的非法人员，通过这种交易方式，用户将得不到任何担保，直接导致损失。

总结：

趣步所依靠的区块链技术实际是一个噱头，并不真实存在。而“糖果”，是不法分子所运用的非法产物，可以人为地操控其数量、价格等信息。我国目前还没有任何机构承认虚拟币的合法性，已属于违法。分析其运营模式，是常见“传销”模式，通过高返佣、拉下线实现新用户的增长。同时建立多个非法组织群，群内不法分子对群内人员进行洗脑，诱导用户拉新，从中获利。

手机卫士十周年里程碑事件

1. 360 手机卫士诞生，全平台保护

- 2009 年，奇虎 360 推出 360 手机卫士塞班版 1.0 版与安卓版 1.0 版；
- 2010 年 10 月，推出 360 手机卫士 IOS 版 1.0 版；
- 2013 年 8 月，推出 360 手机卫士 WP 版 1.0 版；

360 手机卫士集防垃圾短信，防骚扰电话，防隐私泄漏，对手机进行安全扫描，联网云查杀恶意软件，软件安装实时检测，流量使用全掌握，系统清理手机加速，归属地显示及查询等功能于一身，实现移动端全平台保护。

2. 工具矩阵，全方位保护手机

- 360 省电王

2012 年 4 月，360 手机卫士推出 360 省电王，主要用于解决智能手机待机时间短的问题。该软件可以精准预估电池可用时间，并提供个性化的节电模式，最大程度延长电池使用时间。在节省电量的同时，360 电池医生提供每月完全循环充电提醒、完善的充电阶段展示、充满提醒以及专业的电池保养知识。

- 360 隐私保险箱

2012 年 5 月，360 手机卫士推出 360 隐私保险箱，帮助用户记录微博、邮箱、网银、游戏、银行账号等密码信息，再不用为忘记各种各样的账号密码烦恼。用密码保护用户个人隐私程序，并具备防暴力破解保护功能。自动锁定，时刻保护用户隐私不被窥视。

- 360 优化大师

同 2012 年，360 手机卫士推出 360 优化大师，该软件是一款针对 Android 系统工具软件，主要用于提供全面有效的系统优化清理、系统增强管理量大基础功能模块及多个实用小工具，并且操作使用简单、高效、安全。其宗旨是专业优化清理， 使手机运行如飞。

- 360 手机卫士（极客版）

360 手机杀毒于 2014 年 4 月更名 360 手机卫士极客版，是一款手机安全防御软件。360 手机卫士极客版拥有全新广告扫描引擎，一键过滤，极致清爽界面；防隐私泄露，位置伪装，

百变由你；智能接管通知栏消息，无用信息不打扰；新增智能休眠模式，告别反复清理，省电省内存等功能。

- 360 清理大师

2014 年 3 月，360 手机卫士推出 360 清理大师，360 清理大师，是一款免费手机清理软件，主要为用户解决手机卡慢和空间不足问题。专注手机清理 8 年，服务 6 亿用户，拥有国内外海量的垃圾清理数据库，覆盖 90%以上的手机垃圾，共累计为用户清理手机垃圾 1.2 亿 G。

360 清理大师首创毫秒加速技术，超强智能一键清理，给用户带来内存秒速释放的卓越体验。首创并保持了多项领先功能：

微信专清，全面扫描和管理微信空间占用，采用新一代 KDD（数据挖掘）技术，瞬间搞定微信垃圾，轻松腾出 1G 空间。

照片清理，独创 PR（模式识别）技术，智能筛选照片，多角度对照片进行整理和分类删除。

短信清理，创造性的将人工智能运用在短信分类识别中，解决大量垃圾短信的分类和整理删除工作，月帮助用户删除垃圾短信过 2 亿条。

视频压缩，利用先进的压缩算法，在保证视频质量的前提下，为视频瘦身，节约大量空间。

- 360 流量卫士

2014 年 6 月，360 手机卫士推出 360 流量卫士，是一款集流量节省、防止流量后台偷跑、流量实时查询等三大功能的软件。使用 360 流量卫士不仅可以帮助用户节省手机流量，达到省钱目的;也可以让用户了解使用后台流量的应用详情，及时禁止后台偷跑流量，以避免流量在未知的情况下被偷偷消耗。同时 360 流量卫士提供的流量实时查询功能可以让用户了解到自己的流量还剩多少，帮助用户明明白白使用流量。

3. 反骚扰反诈骗，保障支付和网购安全

- 手机支付保镖

2014 年，360 手机卫士发布国内独创手机支付保镖，三重保护，让用户安心完成网购交易：

第一重防护，是当用户下载网银、网购客户端时，360 支付保镖将自动检测客户端是否遭到恶意篡改，抑制威胁源头。

第二重防护，指 360 支付保镖针对盗号木马和钓鱼信息，提供了联网云查杀功能，保障帐号、帐户的安全。

第三重防护，则是在手机支付行为发生时，360 支付保镖会立即自动运行，阻止未知程序运行，实时检测支付环境的安全与否。

- 手机先赔

“手机先赔”是 360 手机卫士 2014 年全球首家推出的手机电信诈骗先赔服务。360 手机卫士设有“先赔功能”，能够对用户在进行手机支付、网址访问或者在接收短信时，自动识别钓鱼网址和密码，有效的保护用户的个人隐私安全。如果开启手机先赔功能的用户因为收到钓鱼网址或者木马短信诈骗遭受损失，能够通过 360 手机卫士来申请理赔，符合理赔条件的用户会获得金额最高上限单笔 6000 元，全年 72000 元的保险金额。目前，360 手机卫士手机先赔累积开启量超过 1000 万。

- 成立反骚扰反诈骗联盟

2014 年 5 月，360 手机卫士联合晶报、法制晚报、新闻晨报、海峡都市报等国内五十余家主流媒体，正式宣布成立中国手机反骚扰反欺诈联盟，向骚扰电话宣战，同时正式启动 519 手机公益行动。该公益行动通过手机反骚扰反欺诈联盟、手机诈骗先赔服务等两大保障，360 手机卫士专版升级、400 个城市 10 万家门店免费修手机、在线专家门诊随时响应等三大举措，帮助中国手机用户彻底解决手机安全问题。

4. 与手机厂商运营商密切合作，覆盖国内外 10 亿用户

2014 年，360 手机卫士在手机杀毒、垃圾清理、防骚扰反诈骗中，与手机厂商、运营商密切合作。截止到 2019 年，TOP 厂商使用骚扰拦截、杀毒、清理等 SDK，SDK MAU 突破 10 亿。

5. 360 手机卫士用户超过 10 亿

2017 年，360 手机卫士业内率先完成 10 亿用户积累，稳居手机安全行业第一。

6. 开源安卓插件化框架 RePlugin，体现技术能力

2017年7月,安卓进入“全面插件化”时代,360手机卫士开源安卓插件化框架RePlugin，已被百度、京东、58 等公司采用，体现技术能力。

7. 360 安全大脑极智赋能，360 手机卫士 8.0 重磅上线

360 安全大脑是 360 公司旗下的分布式智能安全系统，综合利用人工智能、大数据、云计算、IoT 智能感知、区块链等新技术，保护国家、国防、关键基础设施、社会、城市及个人的网络安全。 2018 年，360 手机卫士推出版本 8.0 并引入 360 安全大脑,杀毒引擎技术革新，骚扰拦截能力提升，AI 智能清理推出。

8. 助力政企，迈入下一个十年反诈新纪元—应龙综合反诈平台

在所有的成就中，我们尤其为投身反诈的使命感、为执法部门带来的业务保障、能挫败犯罪分子的诡计而倍感荣耀。这些为社会、为群众、为公安、为运营商乃至于为企业带来的安全保障，使我们广受赞誉。

2018 年，360 手机卫士推出“应龙反诈平台”，在工信部、公安部、信通院、运营商以及公安局相关领导及业务专家的引领下，运用互联网数据运营的思想，配合现有业务流程实现通信反诈机制的优化和升级。依靠卓越的业务基础、智能的数据算法，建立“预警-拦截-劝阻-关联”的反诈机制。协助部署系统的区域，降低报案率、减少用户投诉量，进一步保障群众财产安全。

360 手机卫士也凭借十年以来对反诈业务的敏锐洞察力，紧跟反诈新形势新要求，不断创新思路举措，积极加强防范治理电信网络诈骗技术能力建设，成为电信网络诈骗治理支撑与服务单位中的一员。

2019 年 6 月，“应龙综合反诈平台”荣获“2019 年度防范治理电信网络诈骗创新实践示范项目”。

360 手机卫士的应龙综合反诈平台，可以帮助我们的客户应对关键行业挑战，为他们建立并优化预警、拦截、劝阻的全面反制诈骗的措施，从而实现提升整体通信环境和谐发展，降低因诈骗为群众带来的巨额经济损失。未来运营商与公安反诈机关开展反诈行动，将会和应龙反诈平台这样的技术多多结合，将诈骗分子拦截在门外，或者提高他们的参与诈骗的门槛。让运营商、公安以及企业掌握实实在在反诈的主动权。

功能点

- 2012 年——首发摇一摇清理
- 2012 年——来电秀上线，快速推出快速迭代，支持标记、归属地、形象展示等
- 2014 年——伪基站检测和拦截，保护通信安全
- 2014 年——防吸费功能，查杀吸费、偷跑流量软件，查杀盗版软件
- 2016 年——家人防护，帮家人防骗，时刻守护更安心
- 2017 年——iOS 首发骚扰短信

附录 1 社会贡献

维护网络安全需要让每个人都成为参与者。在手机安全问题日益严峻、电信诈骗产业化的今天，360 手机卫士联合社会各界力量，重拳出击，打击电信诈骗。

1. 联合公安&运营商反欺诈

打击手机诈骗犯罪，协同公安共同破案。360 手机卫士联合新疆、吉林、哈尔滨、天津等各地公安部门，已成功破获多起特大型典型诈骗案，有效的打击了手机诈骗犯罪，维护了手机用户的合法权益。

360 手机卫士推出的“应龙反诈骗平台”，帮助公安建立预警、拦截、劝阻的全面反制诈骗的措施，使某地公安通信诈骗报案量下降 47%；帮助运营商更精准的识别和拦截高危号码，有效降低误判，减少投诉率，使合作运营商骚扰治理集团排名跃升至前三名。

2. 高校安全讲座

网络安全防骗公益讲座走进社区。由网信办、北青网联合指导，360 手机卫士承办的“安全用网 健康成长”互联护苗 • 2019 科普知识进社区活动，引导青少年安全上网、绿色上网，普及网络安全知识，提升广大青少年及家庭的网络安全防范意识，使网络安全意识深入人心。

致力提升高校学生群体的网络安全意识，全面阻击诈骗！防范针对学生群体的电信诈骗犯罪，360 手机卫士走进高校，开展了以“青少年 大学习”为主题的校园防骗宣传活动。截止目前，360 手机卫士已与贵州、吉林、辽宁、甘肃四个省市的高校确立合作试点，共计举办安全教育公益讲座十余场，单场学生人数最高 800 人，媒体曝光覆盖电视台、报纸、校媒以及 360 官微矩阵等，得到校方、警方的一致好评，充分建立“警、企、师生”全面联动的范防诈骗联盟。

附录 2 所获奖项

奖项年份	奖项名称	颁奖机构 （以下机构排名不分先后）
2010 年	年度最佳手机安全软件	2010 移动互联网与终端应用市场年会组委会
	第二届移动互联网创新服务提供商奖	易观国际
	中国手机产业手机安全杰出表现奖	2010 中国手机产业发展大会
	2010 中国互联网最具价值项目奖	计世网
	2010 年度 IT 产品编辑推荐奖	驱动中国
	2012 年度优秀产品奖	计算机世界
	2010 年度最受欢迎手机安全软件	中国科学院《互联网周刊》
	最佳手机应用服务奖	艾瑞咨询集团
2011 年	成功之作奖	中国电脑教育报
	2011 年度最佳移动互联网应用	速途网
	2011 年度最佳手机安全软件	中国科学院《互联网周刊》、中国社会科学院信息化研究中心
	2011 年度最佳手机安全软件	川报集团全媒体中心
	最具影响力产品奖	比特网
	2011 年度最佳手机安全软件	手机之家
	最受关注的十大移动互联网应用	TechWeb
	网民眼中 2011 最靠谱产品	2011 中国互联网产业年会组委会
	2011 移动互联网最佳应用奖	移动互联网产业发展论坛组委会
	最受用户喜欢安卓应用奖	木蚂蚁应用市场
	移动互联网应用类最受欢迎产品奖	2011 移动互联网终端及应用创新大赛组委会

	IMEA 年度最佳应用软件奖	CIE 第二届两岸互动数字内容设计大赛组委会
2012 年	系统安全年度 APP	Pconline 软件频道
	中国反网络病毒联盟白名单	中国反网络病毒联盟
	2012 年度中国网络技术最值得推荐手机安全软件	CCID 赛迪
	中国互联网十大价值产品	2012 中国互联网产业年会组委会
	2012 年度十大手机应用软件企业	2012 中国手机行业年度盛典组委会
	2012 领秀榜最佳手机安全软件	川报集团全媒体中心
	年度最受欢迎应用奖	安智
	最佳安全应用奖	中华网
2013 年	2013 最受用户信赖移动安全品牌	南京日报社
	2013 年度最受用户信赖手机安全软件	硅谷动力
	2013 年最佳移动安全奖	2013 易观互联网创新大会
	最佳应用工具奖	中国手机应用开发者大会组委会
	中国国际软件博览会金奖	第十七届中国国际软件博览会组委会
	2013-2014 年度中国移动互联网应用类最具影响力安全应用奖	艾瑞咨询集团
2014 年	Best android security 2014	av-test.org
	2104 年最佳工具应用奖	人民网&艾媒咨询集团
	TopDigital 2014 数字创新方案奖	TopDigital
2015 年	最佳工具应用奖	艾媒咨询集团
2016 年	2016 手机安全管理领域最具领导力品牌奖	中国科学院《互联网周刊》、中国社会科学院信息化研究中心
	年度无线城市运营商	2016 第三节中国好 WIFI 组委会
	年度最佳工具应用奖	广东省互联网协会举办，广东互联网大会组委会、艾媒咨询集团

	Global Tech 2016 年度产品奖	环球网
	年度值得推荐安全管理 App 奖	人民邮电报
2017 年	“年度最佳创新科技”	
	2017 年软博会金奖	
	信息时报 2017 年度产业突出贡献奖	信息时报
2018 年	2018 大数据产业峰会可信应用分发模块奖	
	“码号卫士奖”	
2019 年	“年度隐私政策透明奖”	南都个人信息保护研究中心
	“众志护网”2019 年度防范治理电信网络诈骗创新示范项目	中国互联网协会、中国信息通信研究院