2018 年

Android 恶意软件专题报告

2019 年 2 月 14 日

摘　要

- 2018 年全年，360 互联网安全中心共截获移动端新增恶意软件样本约 434.2 万个，平均每天新增约 1.2 万个。全年相比 2017 年（757.3 万个）下降了约 42.7%。
- 2018 全年移动端新增恶意软件类型主要为资费消耗，占比高达 63.2%；其次为隐私窃取（33.7%）、恶意扣费（1.6%）、流氓行为（1.2%）、远程控制（0.3%）。
- 2018 全年，360 互联网安全中心累计监测移动端恶意软件感染量约为 1.1 亿人次，相比 2017 年（2.14 亿人次）感染量下降 48.6%，平均每日恶意软件感染量约为 29.2 万人次。
- 2018 全年从地域分布来看，恶意软件感染量最多的省份为广东省，占全国感染量的 8.2%；其次为北京（7.2%）、山东（6.5%）、河南（6.4%）江苏（6.1%）等。感染量最多的城市为北京，占全国城市的 7.2%；其次是重庆（2.2%）、广州（1.6%）、成都（1.3%）、南京（1.3%）。位居 Top10 的城市还有东莞、呼和浩特、石家庄、上海、哈尔滨。
- 2018 年恶意软件使用了多种新技术，分别是利用调试接口感染传播，首次出现 Kotlin 语言开发的恶意软件，劫持路由器设置，篡改剪切板内容，滥用 Telegram 软件协议，恶意软件适配高版本系统以及针对企业和家庭的网络代理攻击。
- 2018 年移动高级威胁方面，360 烽火实验室监测到的公开披露的 APT 报告中，涉及移动相关的 APT 报告 23 篇。被提及次数最多的被攻击国家依次是韩国、以色列、巴基斯坦、巴勒斯坦、伊朗、叙利亚和印度。
- 2018 年移动高级威胁主要围绕在亚太和中东地区，涉及朝韩半岛、克什米尔地区，巴以冲突地区。除此以外，还体现了部分国家内部动荡的政治局势。
- 2018 年移动平台黑灰产业生态，根据结构划分为流量获取分发、流量变现盈利和数据信息安全三个方面。
- 2018 年度 CVE Details 报告显示，Android 系统以 611 个漏洞位居产品漏洞数量榜前列，与 2017 年 842 个相比略有减小，下降 27.4%，与 2016 年相比增加 16.6%
- 截止 2018 年 10 月，Google 发布的 Android 系统版本分布统计，Android Nougat（Android 7.0/7.1）达到 28.2%，占比第二的是 Android Oreo（Android 8.0/8.1）总占比已达 21.5%，而最新系统版本 Android 9 Pie 不足 0.1%。
- 系统厂商自律定期更新开发者策略，政府监管处置各类违法违规应用，警企协同打击网络犯罪，共建大安全生态环境。
- 从移动威胁趋势上看，5G 时代到来物联网安全问题凸显，基于内容的诈骗活动将越来越活跃，虚拟货币价格虽然降低但攻击仍将继续，社交网络下的新型传播方式以及数据泄露推动隐私全球立法，这五个方面将成为未来的主要趋势。

关键词：移动安全、恶意软件、高级威胁、黑灰产业、威胁趋势

目　　录

第一章 总体态势

一、 恶意软件新增量与类型分布

2018 年全年，360 互联网安全中心共截获移动端新增恶意软件样本约 434.2 万个，平均每天新增约 1.2 万个。全年相比 2017 年（757.3 万）下降了约 42.7%。自 2015 年起，恶意软件新增样本量呈逐年下降趋势。

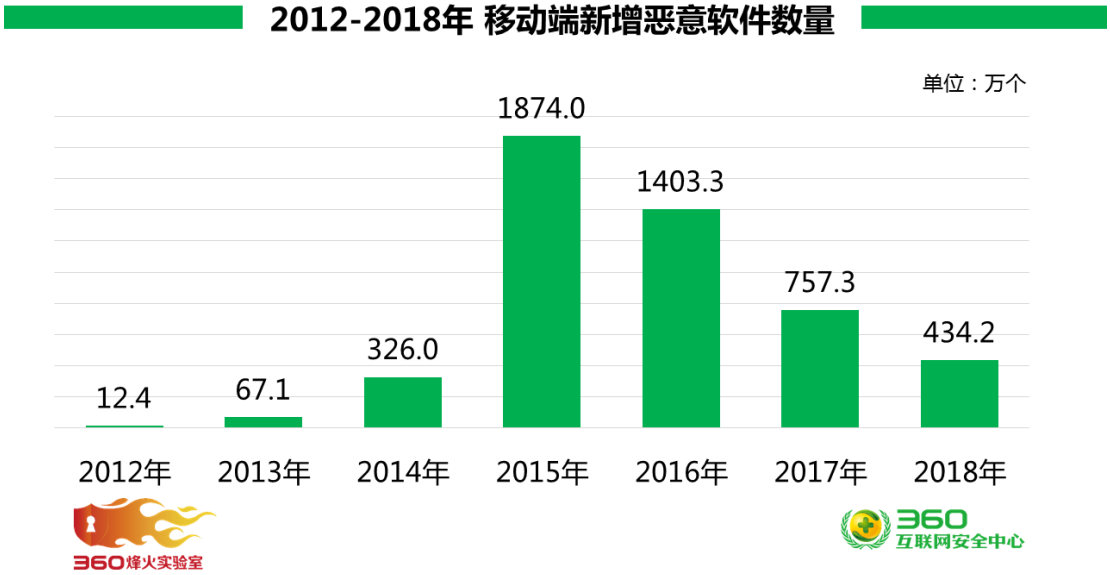


图 1.1 2012-2018 年移动端新增恶意软件数量情况

2018 年新增恶意软件整体呈现上半年、下半年较低的态势。其中 3 月份新增量最多，约 50.0 万个恶意软件，第四季度中新增样本量均较低。

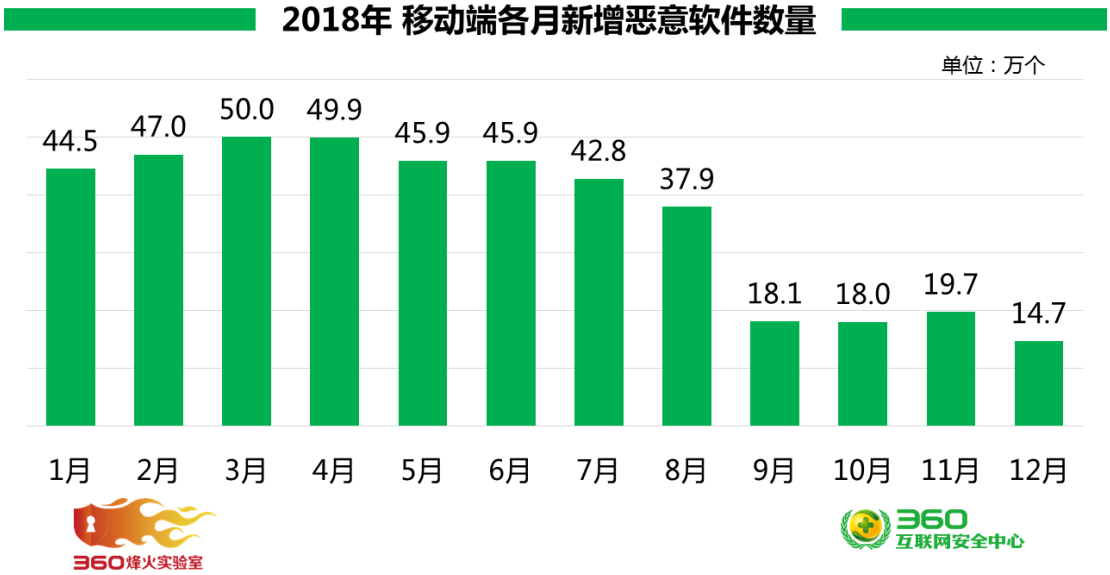


图 1.2 2018 年移动端各月新增恶意移动端样本数分布情况

2018 全年移动端新增恶意软件类型主要为资费消耗，占比高达 63.2%；其次为隐私窃取（33.7%）、恶意扣费（1.6%）、流氓行为（1.2%）、远程控制（0.3%）。

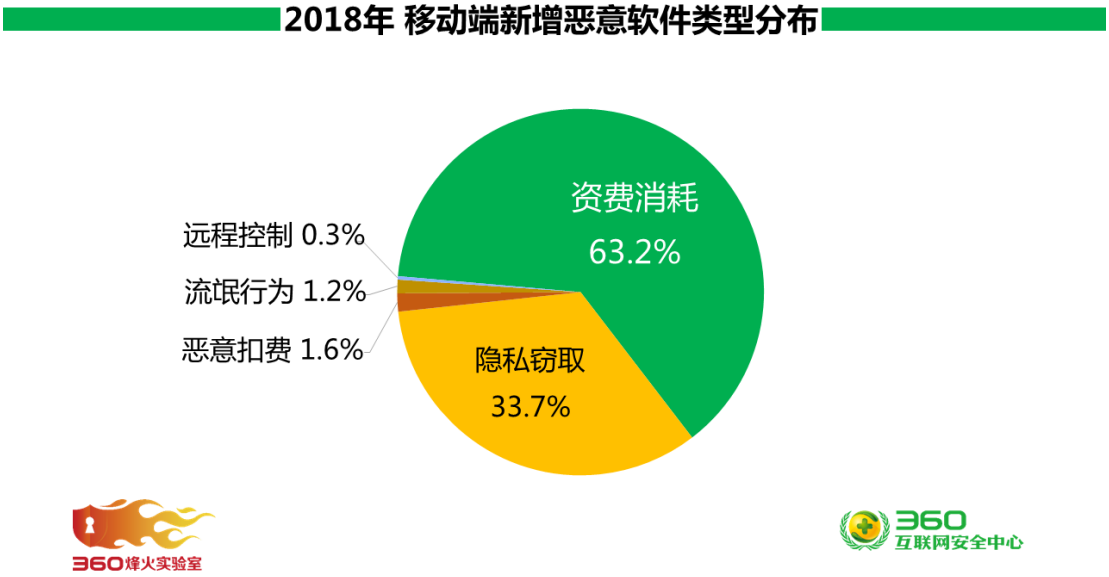


图 1.3 2018 年移动端新增恶意软件类型分布情况

二、 恶意软件感染量分析

2018 全年，360 互联网安全中心累计监测移动端恶意软件感染量约为 1.1 亿人次，相比 2017 年（2.14 亿人次）感染量下降 48.6%，平均每日恶意软件感染量约为 29.2 万人次。

从七年的移动端恶意软件感染量对比看，经过 2012-2015 年的高速增长期，2016 年起呈现逐年下降趋势，恶意软件发展逐渐平稳。

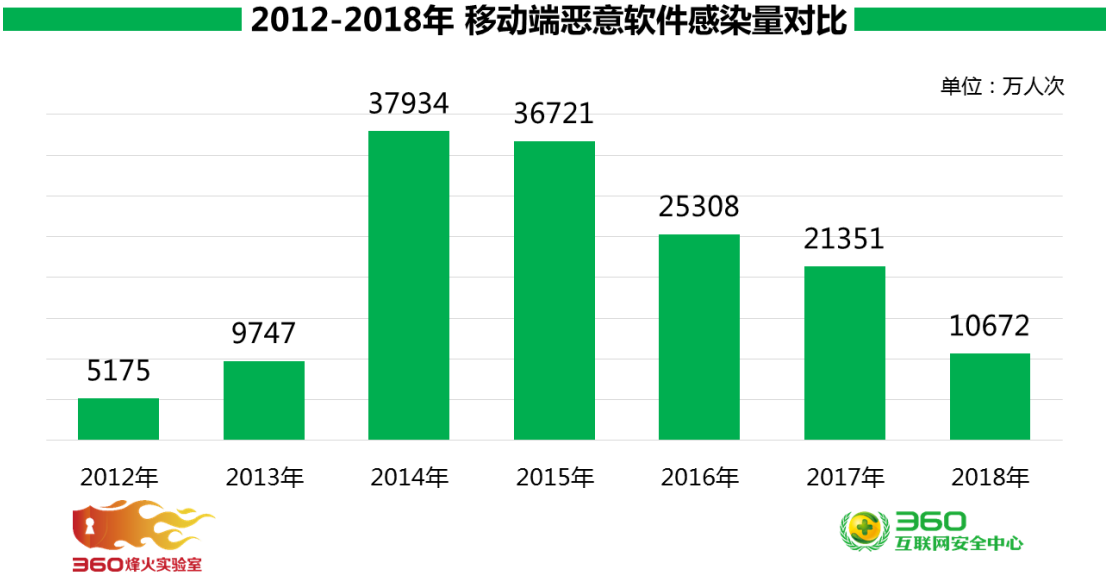


图 1.4 2012-2018 年移动端恶意软件感染量对比情况

2018 年移动端新增恶意软件感染量的按季度对比情况来看，总体呈下降趋势。四季度新增量最低，仅约 52.4 万个。

全年来看，2018 年四个季度的感染量总体呈下降趋势；其中一季度最高约为 3437.3 万人次，四季度感染量最少，仅约 2057.1 万人次。

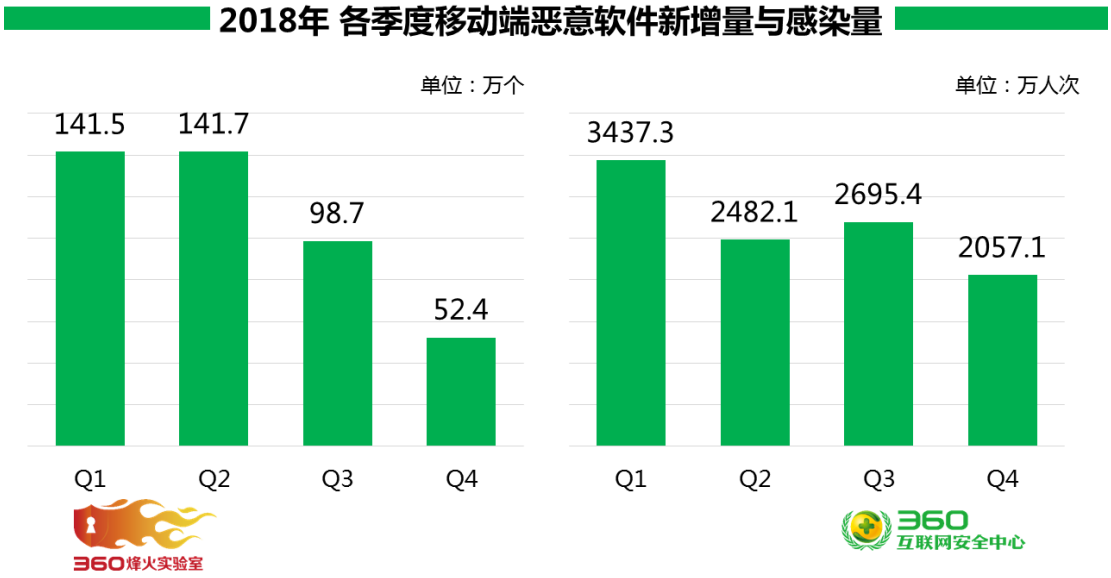


图 1.5 2018 年移动端新增恶意软件感染量按季度对比情况

三、 恶意软件感染量地域分析

2018 全年从地域分布来看，恶意软件感染量最多的省份为广东省，占全国感染量的 8.2%；其次为北京（7.2%）、山东（6.5%）、河南（6.4%）和江苏（6.1%）。此外河北、浙江、四川、黑龙江、江西的恶意软件感染量也排在前列。

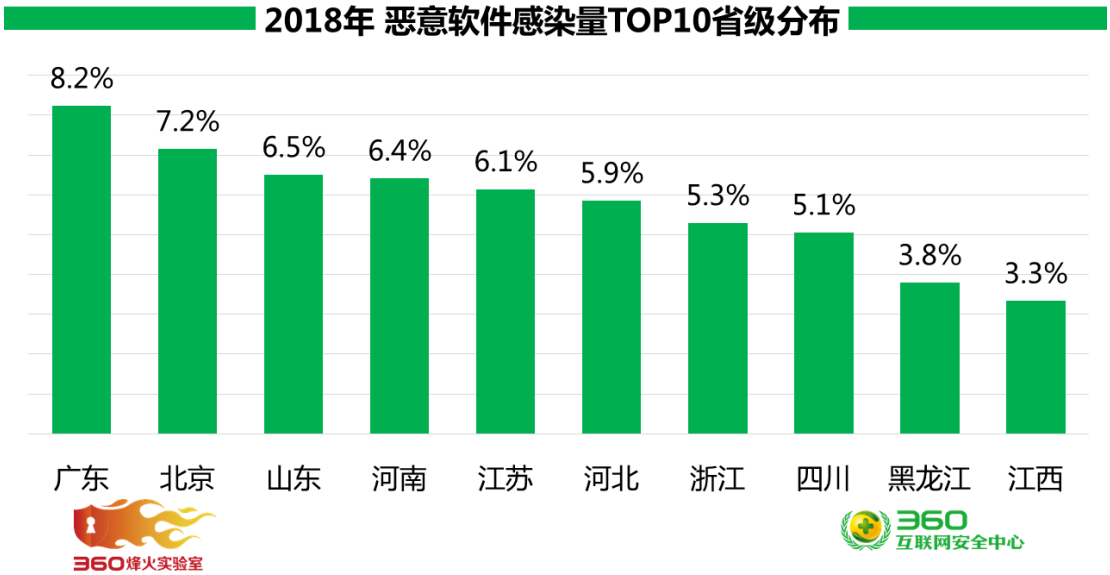


图 1.6 2018 年恶意软件感染量 TOP10 省级分布情况

恶意软件感染量最多的城市为北京，占全国城市的 7.2%；其次是重庆（2.2%）、广州（1.6%）、成都（1.3%）、南京（1.3%）。位居 Top10 的城市还有东莞、呼和浩特、石家庄、上海、哈尔滨。

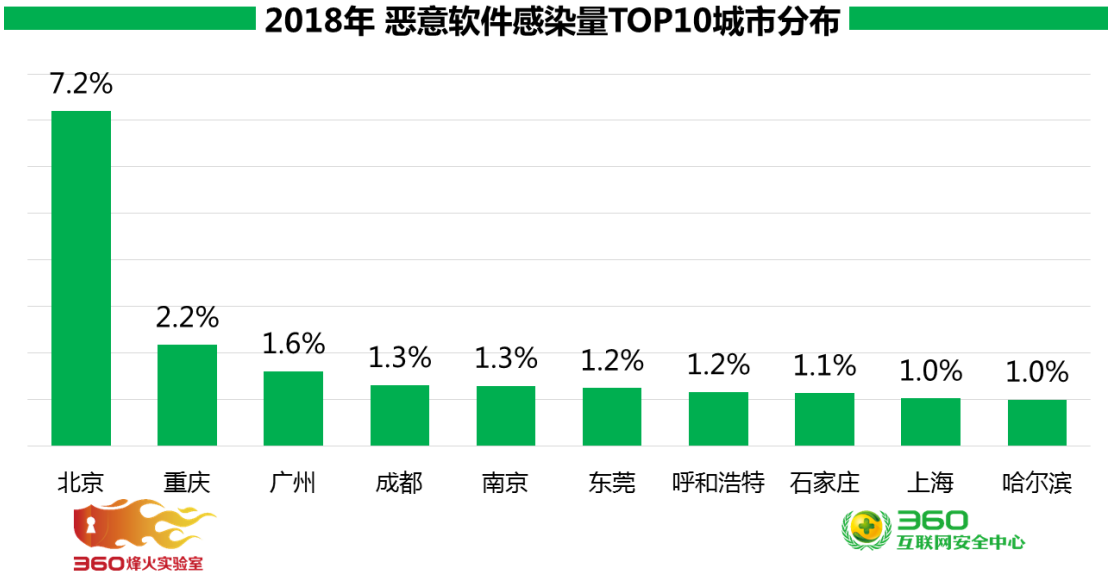


图 1.7 2018 年恶意软件感染量 TOP10 城市分布情况

第二章 盘点恶意软件的新技术

一、 利用调试接口传播

adb 是连接 Android 设备与 PC 端的桥梁，可以让用户在电脑上对设备进行全面的操作，是 Android 系统为方便软件开发者提供的一种调试接口，一般情况下软件开发人员是通过启用 USB 调试选项来使用这种接口的。但事实上，这种接口可以直接绑定到网络端口上。一旦被绑定到网络端口，攻击者就可以在不借助物理接触的前提下，远程操作 Android 设备。

今年 2 月，360 安全团队监测到全球首个 Android 平台挖矿蠕虫 ADB.Miner[1]。ADB.Miner 利用了 Android 设备上的 5555 端口，5555 端口是 Android 设备上 adb 调试接口的工作端口，正常状态下应该处于关闭状态，但未知原因导致部分设备错误打开了该端口。

ADB.Miner 蠕虫摆脱了通过短信、垃圾邮件等社交诱骗的传播方式，而是直接从 adb 接口感染和传播。另外，adb 接口功能相当丰富，其中文件上传功能及 Shell 指令为蠕虫的繁殖和运行提供了便利。在传播中，ADB.Miner 复制了 MIRAI 中 SYN 扫描模块的代码，试图加速对 5555 端口开放情况的探测过程，以便提高传播速度。

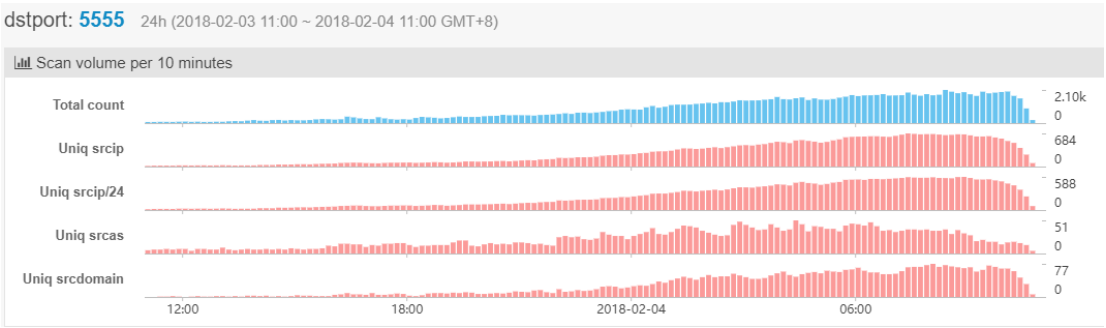


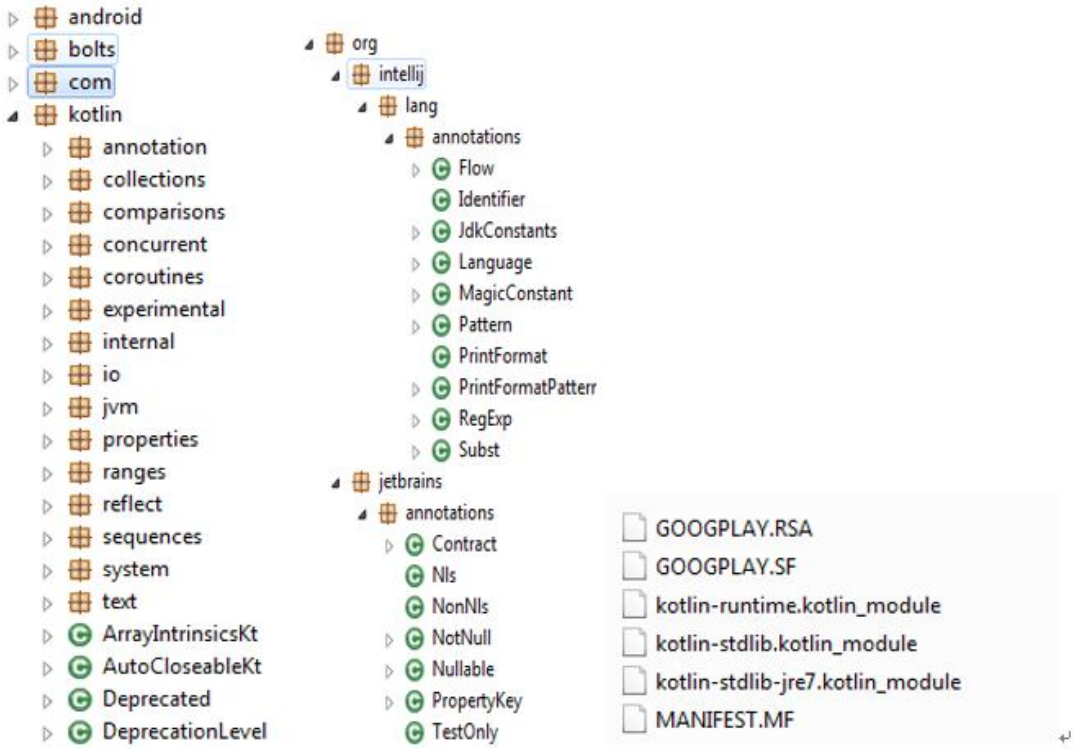
图 2.1 端口 5555 上的扫描流量正在快速增长

二、 Kotlin 语言开发的恶意软件首现

Kotlin[2]是一个用于现代多平台应用的静态编程语言, 2017 年 5 月 Google 宣布 Kotlin 正式成为 Android 官方支持开发语言。

Kotlin 特点简洁，大大减少了样板代码的数量；安全，因为它避免了诸如空指针异常之类的整个类错误；互操作性，充分利用 JVM，Android 和浏览器的现有库；并且工具友好，可用任何 Java IDE 或者使用命令行构建。

2018 年 1 月，安全厂商发现首个以 Kotlin 编程语言开发的恶意软件[3]，该恶意软件不仅能够执行远程命令，窃取信息，模拟点击广告，它还可以在未经许可的情况下为用户订阅付费短信业务。



图片来自（https://blog.trendmicro.com/trendlabs-security-intelligence/first-kotlin-developed-malicious-app-signs-users-premium-sms-services/）

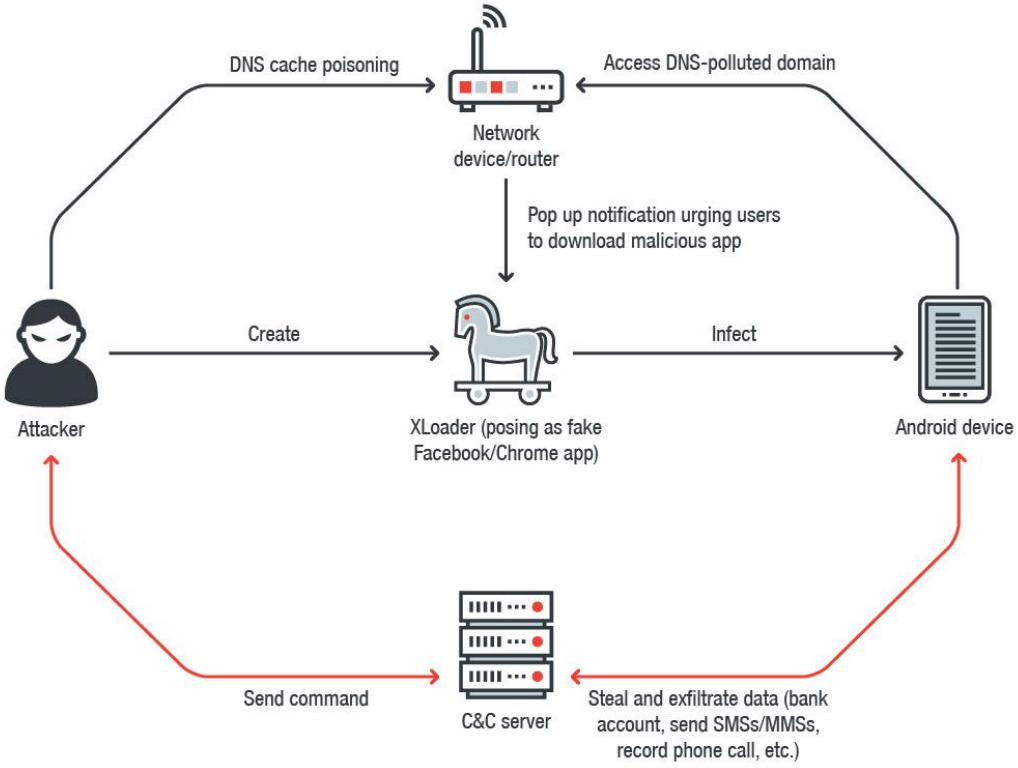
图 2.2 使用 Kotlin 开发的恶意软件的包结构

三、 劫持路由器设置

路由器被入侵的可能性大致分为两种。一种是使用路由器本身的漏洞攻击，另一种是通过路由器管理功能所设置的弱认证信息非法登录。

早在 2016 年 12 月，就曾出现了劫持路由器 DNS 设置的 Switcher[4]恶意软件家族，恶意软件即会利用一份预置好的包含 25 种默认登录名与密码的列表，在路由器的管理员 Web 界面中执行密码暴力破解。如果破解尝试成功后，木马会导航至 WAN 设置选项并设置不法犯罪分子控制的流氓 DNS 作为主 DNS 服务器。

2018 年 3 月，日本媒体报道了大量日本用户的路由器 DNS 设置被劫持，将用户重定向到恶意 IP 地址，导致用户手机下载安装了伪装成 Facebook 和 Chrome 更新的 XLoader[5]恶意软件，恶意行为包括窃取隐私、网站钓鱼、挖矿等。截至目前，攻击者已经将目标语言从 4 种扩展到 27 种，包括欧洲和中东语言，平台也从 Android 覆盖到 iOS、PC 平台。



图片来自（https://blog.trendmicro.com/trendlabs-security-intelligence/xloader-android-spyware-and-banking-trojan-distributed-via-dns-spoofing/）

图 2.3 XLoader 感染链

四、篡改剪切板内容

在使用手机时经常会用到剪切板功能，通过小小的剪贴板在各种 APP 之间传递和共享信息。我们发现由于剪切板功能简单，使用时也不需要申请额外的权限，导致被恶意利用，在复制粘贴过程中暗藏玄机。

2018 年伊始，我们发现羊毛党篡改剪贴板以非正常方式传播支付宝的吱口令，通过支付宝的红包活动赚取红包赏金。我们将信息及时反馈给支付宝，在新一期的赚取赏金活动中支付宝调整了策略，限制了邀请方式和邀请次数。

10 月，我们监控到利用剪切板盗取比特币（Bitcoin）钱包的恶意软件[6]。通过监控用户手机剪贴板中的内容来判断是否是加密数字货币的钱包地址，如果是钱包地址则替换成从服务器得到的攻击者的钱包地址。当用户把复制的钱包地址粘贴到转账地址栏的时候，原先的钱包地址已经被木马替换成了攻击者的钱包地址，造成用户的财产损失。

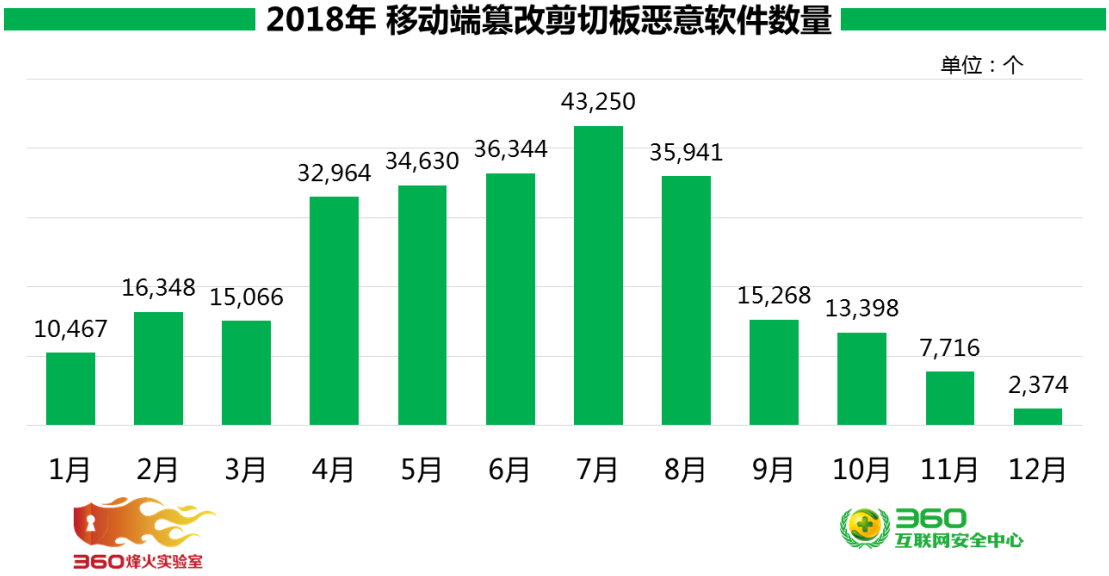


图 2.4 2018 年移动端篡改剪切板恶意软件每月新增数量

五、 滥用 Telegram 软件协议

从去年开始出现利用 Telegram 软件协议的木马，今年有更多的恶意软件作者开始滥用 Telegram 软件协议。滥用 Telegram 软件协议的 IRRAT 和 TeleRAT[7]恶意软件家族接连被曝光，并且还出现了与之前使用 Telegram Bot API 方式不同的 HeroRat[8]恶意软件家族，它使用了名为 Telesharp[9]的开源项目，它可以使用 C#语言创建 Telegram Bot，目前这个开源项目已经不再维护。

README.md

TeleSharp

TeleSharp is C# implementation of Telegram Bot API

It support most of the features of Telegram Bot API including :

- Get Bot information
- Read received messages
- Send text message
- Forward message
- Replay message
- Send location
- Send & receive sticker
- Send & receive photo
- Send & receive video
- Send & receive audio
- Send & receive document
- Set current status of bot like(Typing, Upload photo, Upload video and etc)
- Support Inline Bots
- Support ReplyKeyboardMarkup (Custom keyboards)

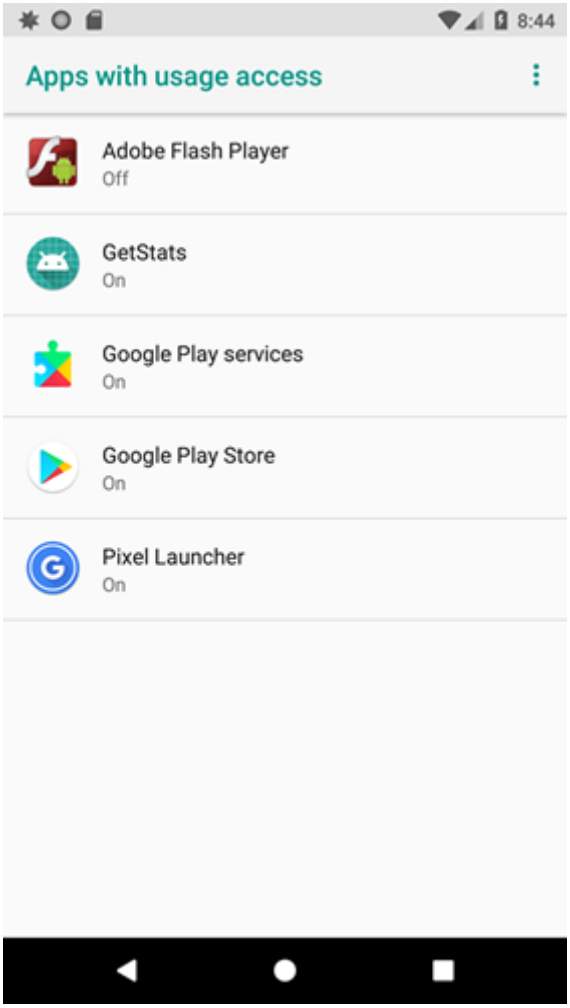
图 2.5 TeleSharp 开源项目功能介绍

六、 恶意软件适配高版本系统

在 2016 年年度报告中，我们提到界面劫持技术被大量用在钓鱼软件和勒索软件。虽然 Google 在 Android 5.0 系统及以上版本限制了获取栈顶 Activity 的获取方法，减弱了这种攻击方式。但当时由于 Android 5.0 以下版本仍然有一定的市场占有率，低版本手机仍然可能遭受到这种威胁。

2018 年 Google 已经发布了 Android 9 Pie，经过两年的发展 Android 5.0 以上系统已经占据主导地位。纵观 Google 在 Android 系统安全方面的更新，每一版本都在遏制恶意软件方面做出了积极应对，这使得界面劫持技术变得更加困难。

2018 年 6 月，我们发现 MysteryBot[10]恶意软件家族开始适配高版本系统，它通过诱导用户授予 APP Device Administrator 和 AccessibilityService 权限，而后滥用 Usage Access 权限。Usage Access 权限可以获取一个时间段内的应用统计信息，按照使用时间排列后，即可获取当前最顶层的 APP。



图片来自（https://www.threatfabric.com/blogs/mysterybot__a_new_android_banking_trojan_ready_for_android_7_and_8.html）

图 2.6 MysteryBot 请求 Usage Access 权限

七、 企业和家庭网络攻击进阶

针对企业和家庭内网的攻击，继 DressCode[11]、MilkyDoor[12]恶意软件家族后，今年又出现了利用移动设备攻击内网的新的恶意软件家族 TimpDoor[13]。TimpDoor 通过短信进行网络钓鱼，诱导用户下载安装虚假 APP，将受感染的 Android 设备转变为移动网络代理，允许不法分子加密访问内部网络，给企业和家庭内部网络带来巨大安全风险。

家族名称	DressCode	MilkyDoor	TimpDoor
曝光时间	2016 年 8 月	2017 年 4 月	2018 年 10 月
传播方式	Google Play 第三方市场	Google Play 第三方市场	钓鱼短信
数据转发	SOCKS 代理	SOCKS 代理使用 SSH 远程转发，从主控端获取 SSH 登录信息，具有广告和下载功能。	SOCKS 代理使用 SSH 远程转发，代码包含 SSH 登录信息，实现基本的代理功能。

表 1 DressCode、MilkyDoor 与 TimpDoor 恶意软件家族对比

第三章 移动高级威胁持续进化

今年 360 安全团队曝光的毒云藤（APT-C-01）[14]、蓝宝菇（APT-C-12）[15]组织对我国政府、国防、科技、教育、金融等多方面进行了长期的网络间谍活动。网络战和网络攻击成为一些热点冲突背后无硝烟的战场，可以说没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。

2018 年，我们在中国互联网安全大会（ISC）上以《APT 攻击战场升级：移动端拉响安全警报》为题，深度介绍移动端 APT 发展现状、移动端价值、植入方式、相关案例以及发展趋势。移动端的重要程度，使得成为 APT 组织转向的新目标。

一、 移动高级威胁全球研究

在 2018 年 360 烽火实验室监测到的公开披露的 APT 报告中，涉及移动相关的 APT 报告 23 篇。被提及次数最多的被攻击国家依次是韩国、以色列、巴基斯坦、巴勒斯坦、伊朗、叙利亚和印度。

从公开披露的 APT 报告数量上看，移动 APT 已经成为新兴的 APT 战场，原因在于手机中存储着人们大量重要的隐私信息，这些信息能够让攻击者发动攻击前，在攻击目标的身份辨别上更加准确，在攻击时攻击的地点和时间更加精确，在攻击后最终获得的收益更加丰厚。

从公开披露的移动高级威胁活动中涉及目标领域情况来看，政府、军事、宗教、媒体、企业是 APT 攻击者的主要目标，这也与 APT 攻击的主要意图和目的有关。

被攻击目标国家	所属地区	相关报告数量	主要被攻击领域
韩国	亚太地区	6	政府、军事、媒体、企业
以色列	中东地区	4	政府、军事
巴基斯坦	亚太地区	4	政府
巴勒斯坦	中东地区	3	政府
伊朗	中东地区	2	政府、宗教
叙利亚	中东地区	2	政府、军事
印度	亚太地区	2	政府、军事

表 2 移动高级威胁研究关注被攻击国家排行

二、 地缘政治影响日益显著

2018 年移动高级威胁主要围绕在亚太和中东地区，涉及朝韩半岛、克什米尔地区，巴以冲突地区。APT 行动与国家及地区间的政治摩擦密切相关，围绕地缘政治的影响日益显著。

2018 年围绕朝韩半岛，在移动端韩国是被公开披露次数最多的被攻击国家。主要攻击组织为 Group 123，又称 Reaper group，APT37，Geumseong121，Scarcruft，该组织被国外安全厂商认为是来自朝鲜的一个频繁活跃的 APT 攻击组织。

披露时间	披露来源	概述
2018.4.2	Cisco Talos	安全厂商对一个虚假的反病毒恶意软件 KevDroid 的分析，并且多家安全厂商对其相关分析和归属的判断[16]。
2018.4.5	Palo Alto Networks	介绍了相关联的鱼叉式网络钓鱼活动，其中伪装的应用名称为“PyeongChang Winter Games” [17]。
2018.8.22	ESTsecurity	韩国安全厂商披露 Operation Rocket Man，分析了其针对 Windows 和 Android 两个平台的攻击活动[18]。
2018.12.13	ESTsecurity	韩国安全厂商披露 Operation Blackbird，主要为该组织实施针对移动终端的攻击活动[19]。

表 3 2018 年 Group 123 组织移动端相关活动

另一个活跃的 APT 组织 Sun Team 也被频繁曝光，主要针对脱北者和媒体记者。Sun Team 和 Group 123 在移动恶意样本分发上存在一些关联，疑似归属为同一组织或使用了共同的基础服务。

披露时间	披露来源	概述
2018.1.11	McAfee	介绍利用社交网络服务发送包含恶意软件下载的链接，诱导脱北者和媒体记者安装恶意软件[20]。
2018.5.17	McAfee	安全厂商在 Google Play 上发现有针对脱北者的恶意软件[21]。

表 4 2018 年 Sun Team 组织移动端相关活动

2018 年围绕克什米尔地区，印度和巴基斯坦分别受到了多个 APT 组织攻击。印度方面，基于国外安全厂商公开的 APT 报告认为攻击印度政府的 APT 组织背后都与巴基斯坦 APT 组织有关，之前 Operation Transparent Tribe[22]和 Operation C-Major[23]的策划者也被国外安全厂商认为是巴基斯坦 APT 组织。

披露时间	披露来源	概述
2018.1.29	TrendMicro	安全厂商发现 PoriewSpy 间谍软件攻击印度 Android 用户,背后与巴基斯坦 APT 组织有关[24]。
2018.5.15	Lookout	安全厂商发现监控窃取军方和政府官员的数据的 Android 和 iOS 恶意软件[25]。

表 5 2018 年印度受到的移动端攻击相关活动

相比印度，巴基斯坦方面也遭遇了多个 APT 组织攻击，安全厂商分析发现从入侵技术和使用的工具上多个组织之间存在一定的相似性。

披露时间	披露来源	概述
2018.1.13	TrendMicro	介绍了 Confucius 组织间谍网络活动[26]。
2018.5.23	TrendMicro	介绍了 Confucius 组织新的工具和技术，以及与 Patchwork 组织的联系[27]。
2018.8.14	360 烽火实验室	肚脑虫组织（APT-C-35）移动端攻击活动主要针对巴基斯坦和克什米尔地区的目标人员[28]。
2018.8.29	TrendMicro	安全厂商发现未知组织 Urpage 与 Bahamut、Confucius 和 Patchwork 组织之间的联系[29]。

表 6 2018 年巴基斯坦受到的移动端攻击相关活动

2018 年围绕巴以冲突地区，网络攻击活动也十分频繁。从 2016 年起，双尾蝎组织（APT-C-23）对巴勒斯坦教育机构、军事机构等重要领域展开了有组织、有计划、有针对性的长时间不间断网络攻击。在 2017 年该组织更为活跃，涉及的移动端攻击中不断使用的新的恶意软件变种 VAMP[30]、FrozenCell[31]和 GnatSpy[32]相继曝光。2018 年该组织对移动恶意软件的伪装、分发、通信技术上进行了全面的升级改进，恶意行为和攻击持久性进一步增强。

披露时间	披露来源	概述
2018.4.16	Lookout	安全厂商发现 Google Play 中的监控软件与针对中东的双尾蝎（APT-C-23）组织有关[33]。
2018.8.11	Symantec	介绍了针对巴勒斯坦人的最新恶意软件的伪装、分发、通信技术[34][35]。

表 7 2018 年巴勒斯坦受到的移动端攻击相关活动

以色列方面，世界杯期间以色列国防军指责巴勒斯坦伊斯兰组织哈马斯试图通过恶意软件攻击以色列士兵的手机[36]。此前监控以色列国防军的 ViperRAT 恶意软件也被认为与哈马斯组织有关[37]。

披露时间	披露来源	概述
2018.4.16	Lookout	用于监控以色列国防军的 ViperRAT 的新变种在 Google Play 上被发现[38]。
2018.7.3	以色列国防军（IDF）	介绍世界杯期间针对以色列士兵的 Android 恶意软件相关信息，其他安全厂商进行了相继跟踪分析[39][40][41][42]。

表 8 2018 年以色列受到的移动端攻击相关活动

三、 部分国家内部局势动荡

2018 年移动 APT 攻击事件中，还体现出了部分国家内部局势动荡，主要体现在中东国家伊朗和叙利亚，针对国家内部持不同政见者和反对派力量，以及一些极端主义活动的倡导者的网络监控。

披露时间	披露来源	概述
2018.1.4	360 追日团队	介绍黄金鼠组织（APT-C-27）对叙利亚地区的攻击活动[43]。
2018.7.17	360 烽火实验室	发现黄金鼠组织（APT-C-27）Android 恶意样本携带 PE 攻击样本诱导感染 PC 平台的实例[44]。
2018.9.7	Check Point	国外安全厂商发现伊朗政府通过移动恶意软件监控内部持不同政见者和反对派力量，以及伊斯兰国的倡导者和主要在伊朗西部定居的库尔德少数民族[45]。
2018.9.7	360 烽火实验室	介绍针对伊朗长达两年的间谍活动，伪装的 Android 恶意软件带有伊朗宗教特色[46]。
2018 BlackHat	Lookout	黄金鼠组织（APT-C-27）国外安全厂商认为是中东某国电子军对反对派的监控活动[47]。

表 9 2018 年中东地区部分国家受到的移动端攻击相关活动

四、 移动端成为新的攻击入口

与传统的 PC 相比移动 APT 有更多特有的攻击入口，同时受到移动平台自身多种原因的限制，移动端保护能力弱安全性低，对于一些攻击诱饵普通用户更加难以甄别，使得移动端攻击比 PC 端受攻击面更广，攻击成功率更高。

2018 年从公开披露的 APT 报告中，攻击入口占比最大的是 Google Play（26.7%），其次是 SNS 网络（16.7%）、IM 即时通讯软件（13.3%）、钓鱼网站（13.3%）、第三方市场（6.7%）、漏洞利用（6.7%）、网盘（6.7%）、电子邮件（6.7%）和短信（3.3%）。

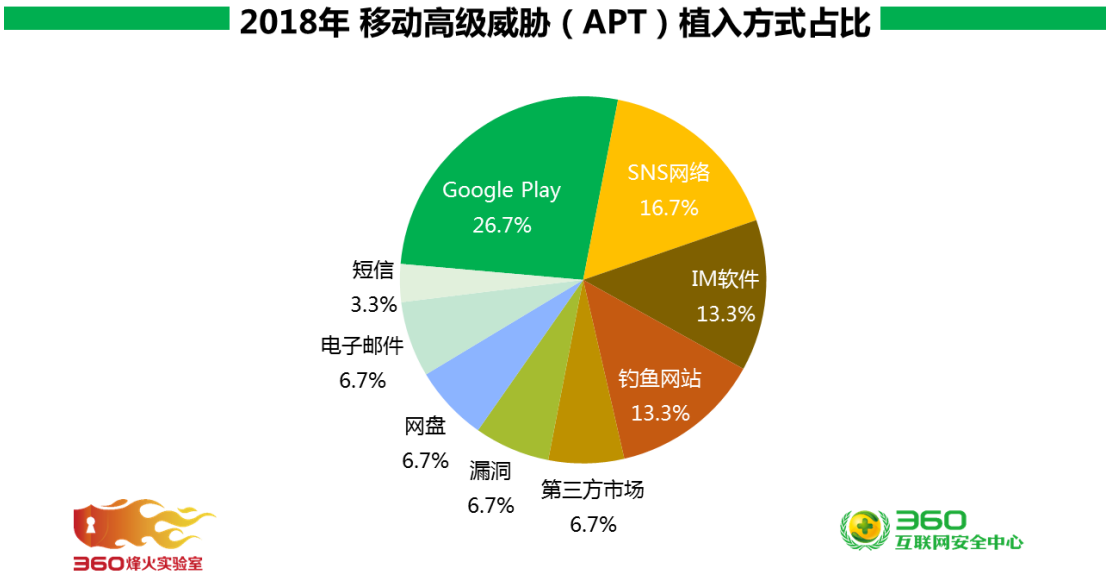


图 3.1 2018 年移动高级威胁（APT）植入方式占比

从数据可以看出，攻击者不断地寻找新的方法来为他们的恶意 APP 增加合法性。他们将恶意应用上传到 Google Play，再通过社交网络和钓鱼网站进行分发，由于用户对于 Google

Play 的信任会毫不犹豫的去下载安装，从而使攻击者钓鱼攻击变得更加成功。

另一方面，我们也可以数据看出漏洞利用也有一定占比。在今年曝光的 Operation Blackbird 攻击中，攻击者使用了三星 CVE-2015-7888 的路径遍历漏洞获取系统权限植入恶意模块。除此以外，Group 123 还在攻击中使用了 CVE-2015-6764 浏览器内核漏洞，通过 JS 去安装任意 APP。攻击者在攻击目标设备上成功植入后，通过漏洞可以进行横向移动，不仅扩大了攻击范围，同时也大大增强了持久性。

第四章 移动平台黑灰产业生态

近年来，网络安全产业步入发展的崭新阶段，产业规模快速增长。公开数据显示，2017年我国网络安全产业规模达到439.2亿元，较2016年增长27.6%，预计2018年达到545.49亿元。而黑灰产业比安全产业发展得更为野蛮。有业内人士认为，黑灰产业已达千亿元规模，网络黑灰产所带来的安全挑战愈加严峻。灰产游走在法律边缘，法无禁止即可为；黑产则触及法律的红线，利用互联网技术进行偷盗、诈骗、敲诈等各类违法犯罪案件频繁发生，围绕互联网衍生的黑灰产行业正在加速蔓延。

2018年，移动平台各种形式的黑灰产业不断浮出水面，我们对此进行了持续的跟踪和揭露。就目前移动平台移动黑灰产业生态结构而言，我们围绕流量获取分发、流量变现盈利和数据信息安全三个方面来分析目前移动平台黑灰产业生态现状。

一、流量获取分发相关产业生态

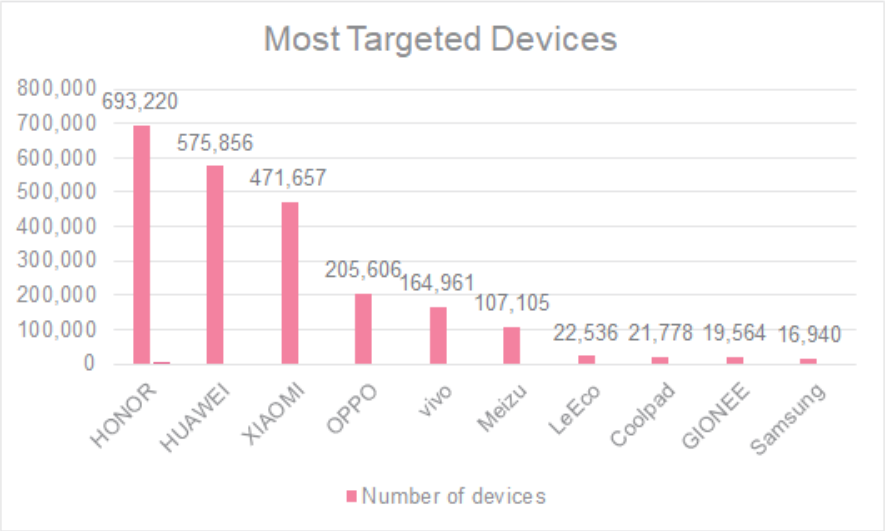
流量的获取和分发是互联网尤其是移动互联网最基本的入口，所有的业务和应用都架构在流量经济之上。流量作为一个基础性服务，采购和获取用户流量是移动黑灰产业中最重要的一环。2018年，围绕流量获取分发的黑灰产业主要体现在供应链中的手机分销渠道环节。

(一) 分销渠道预置木马感染国内多款手机

2018年3月，国外安全厂商发现国内多款手机被安装了一个被命名为“RottenSys”[48]的手机恶意推广软件，从2016年至今累计感染量达到百万级别，引起科技媒体广泛关注。

我们在进行相关技术分析后，确认“RottenSys”主要是通过一家名为“Tian Pai”的电话分销平台来进行传播的，攻击者在该环节上通过“刷机”或APP（再Root）的方式，在手机到达用户手中前，在目标上安装部分RottenSys恶意软件，从而达到感染传播的效果。

“RottenSys”在感染了国内众多Android手机后，会伪装成“系统WIFI服务”等应用，并通过不定期给用户推送广告或指定的APP来获取利益，给Android手机用户造成了一定的困扰。



图片来自（https://research.checkpoint.com/rottensys-not-secure-wi-fi-service/）

图 4.1 RottenSys 感染的手机品牌情况

(二)　小众品牌预置木马销往中小城市

2018 年 4 月，我们监测到 StealthBot[49]恶意软件家族今年一月开始出现，截止到四月中旬，短短三个多月的时间里累计感染量超过 400 万，与一般的大规模感染情况不同的是，StealthBot 感染的手机品牌多达 150 余个并且集中在小众手机品牌，感染地区避开了一、二线大城市主要集中在国内的中小城市。

在对 StealthBot 整个感染链的分析中发现，两家北京某科技公司参与制作，杭州和深圳两家公司参与传播，我们监测到主要是通过供应链攻击的方式在用户使用手机前预置到这些小众品牌的手机系统中。

小众品牌手机价格低廉，手机厂商采用多种手段收集用户流量，甚至预置恶意软件，来弥补自己小众手机品牌市场份额。此次事件影响的目标机型集中在众多中小品牌手机，具有很强的针对性；同时倾销地也指向三四线中小城市，具有很强的隐蔽性难以被发现。

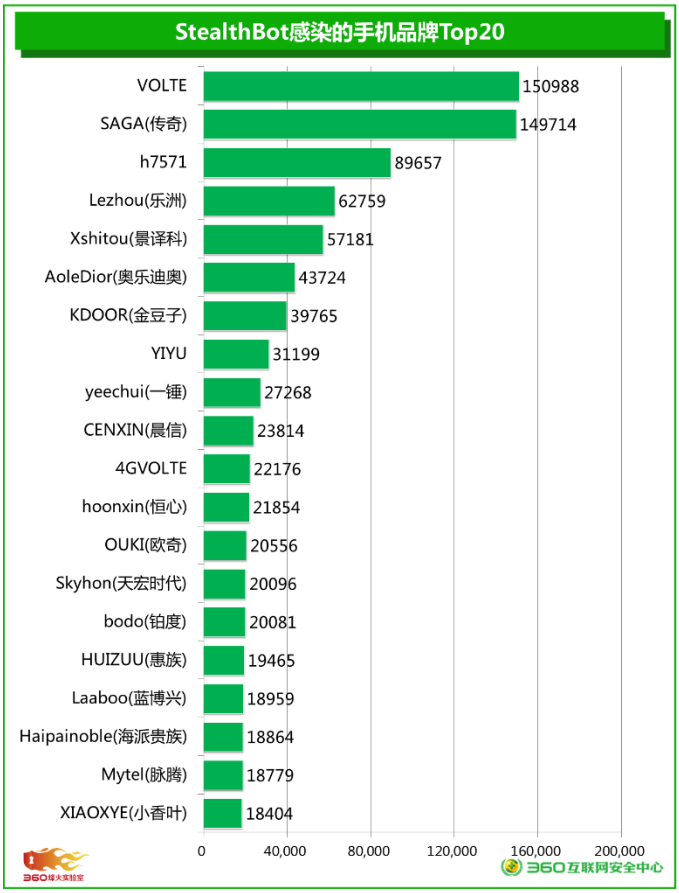


图 4.2 StealthBot 感染的手机品牌 Top20

二、流量变现盈利相关产业生态

流量变现是获取流量最终目的，移动平台几类常见的盈利模式如广告、导流网站、应用市场、佣金分成以及增值付费服务。对于黑灰产业来说，由于监管等因素一般生存周期较短，能够快速将流量变现盈利，是最根本的生存法则。

(一) 提速降费下的免流软件生态

由于国内移动数据流量并不便宜，移动互联的发展推动数据流量使用量攀升，使得部分人群开始寻求廉价甚至免费的流量获取方法，免流软件应运而生并快速传播开来。免流软件即安装后可以让用户在移动运营商网络下免流量或减少流量访问互联网的软件。一些流量巨头企业与运营商合作推出了定向流量包，与之不同的是免流的黑灰产业一般是不法分子通过技术手段，伪造网络请求欺骗运营商计费检测系统。

从我们统计的数据看，各类免流软件共计 20 余万个，使用人群高达几百万人，巨大的软件数量与使用人数进一步印证免流软件拥有着不小的市场。在一个免流 QQ 群中提供的分销、加盟价格表。

		免费代理（客户）	代理	加盟
	需要费用	0元	20元	66元
翱翔网络版				
	体验卡1G1天	0.5	0.15	0.08
	15天无限	1.8	1.2	0.4
	30天无限流量	3	1.8	0.7
至享网络版				
	体验卡1G1天	0.5	0.15	0.08
	3G30天	2	1	0.5
	6G30天	2.5	1.5	0.6
	30天无限流量	3	1.8	0.7
畅想卫士版				
	体验卡1G1天	0.5	0.1	0.03
	3G30天	2	1	0.4
	6G30天	2.5	1.5	0.5
	30天无限流量	3	1.8	0.6
	90天无限流量	8	5	1.5
	365天无限流量	26	16	5
购卡平台一次输入：3-10-20-50-100张！都会降价！买的多优惠多多！				

图 4.3 免流 QQ 群拿货价格表

围绕免流 QQ 群的免流软件生态角色分工及资金流。

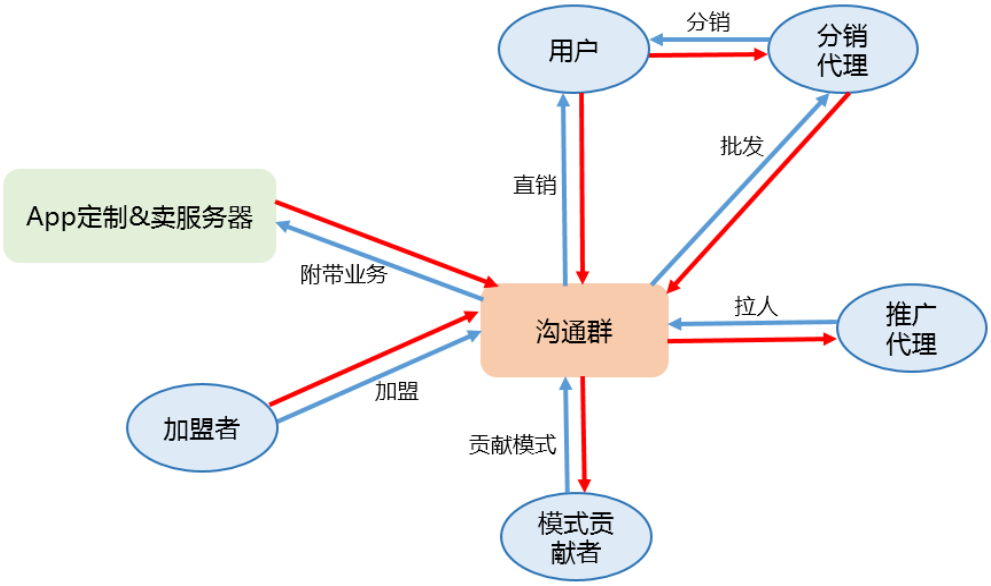


图 4.4 免流软件生态角色分工中的信息流（蓝色）与资金流（红色）

“取消流量漫游费，移动网络流量资费年内至少降低 30%”，这是 2018 年《政府工作报告》中承诺的工作重点之一。毫无疑问，在国家政策的巨大福利下，国内流量资费将进一步降低，对于免流黑灰产业将受到重创无法维持生存，免流黑灰产参与者将会分散到其他黑灰产业。

(二) 薄利多销下的代刷软件产业

围绕 UGC（User Generated Content），即用户将自己原创的内容通过互联网平台进行展示或者提供给其他用户，每个人都有了从草根到意见领袖的可能性。移动互联网流量经济下，意见领袖很大程度上存在经济收益的可能性，如微博大 V 的广告，直播平台粉丝打赏，代刷软件就是在这种背景下应运而生。代刷软件是指通过特定手段提高特定账户粉丝量、访问量或挂机时间等量化指标，或者获取特定权限的软件。常见的代刷软件可分为刷量、刷会员与代挂三种。

通过对大量 Android 代刷软件进行分析后发现，绝大多数代刷软件都是由 Web 代刷网站转化而来。代刷软件实质与 Web 代刷网站一样，都只是一个为用户提供下单购买功能的下单平台，并不包含实际的刷量逻辑。用户通过代刷软件提交订单后，代刷软件会将订单请求传递至代刷网站，代刷网站随后在后台进行统一处理，并将刷量请求传递给真正实现代刷功能的供货商代刷后台。

代刷产业是一种十分依赖于推广扩散来盈利的产业，一方面，在商家泛滥的代刷市场，推广程度会影响商家知名度，而知名度会直接影响用户数量；另一方面，主站与高级分站会从下级分站的收益中抽成，由主站与高级分站扩散出的下级分站越多，其收益越高。

代刷业务以价格低廉的特点吸引了大量用户，而实际上，代刷走的是“薄利多销”的路线，再加上代刷网站或软件的开发与维护成本极低，一个流行代刷主站的获利往往十分可观。通过长期跟进多个流行主站与分站，我们汇总出了部分代刷网站的盈利情况，主站的日平均利润在数十元至上千元不等。

主站点（一级域名）	运营天数（天）	累计成功订单总数（个）	累计交易金额（元）	平均每天订单总数（个）	平均每天交易金额（元）	平均每天利润（元，30%计）
666shua.cn	193	89390	253223.04	463	1312.04	393.61
71wl.cn	41	155383	10789.76	3790	263.16	78.95
qqdzz6.com	252	566427	1250327.21	2248	4961.62	1488.48
jibaqiu.com	3483	33948	129591.46	10	37.21	11.16
tsmzw.cn	136	5547	6628.1	41	48.74	14.62
gcdsw.54x.cc	595	5518	31507.93	9	52.95	15.89
qewei.com	88	23550	37179.39	268	422.49	126.75
myqq520.com	145	66766	109061.86	460	752.15	225.65
zzzz8.cn	42	5096	8730.31	121	207.86	62.36
hxcvb.com	134	38235	56209.06	285	419.47	125.84
nncoco.cn	119	26216	47568.49	220	399.74	119.92
hbbyd.cn	60	31048	73943.81	517	1232.40	369.72
cy198.cn	50	9688	10945.39	194	218.91	65.67
shanqianidc.com	149	14947	18752.85	100	125.86	37.76

图 4.5 部分代刷网站收益情况

下图为某代刷网站分站的内部价格表。

ID	名称	成本价格	销售价格	状态	操作
345	理论永久超级会员-质保25天-没有超级会员才可以下单哦	14.90	16.10	上架中	编辑
334	【推荐】快手直播号带锁-24小时内手工发货	75	80.00	上架中	编辑
204	看好商品名称质保与不质保等.	10.00	10.00	上架中	编辑
288	前任3在线观看高清.	0.05	0.10	上架中	编辑
76	【特慢】名片赞 (面值:1000) 日刷1W	0.2	0.2	上架中	编辑
155	【特慢】名片赞 (面值:5000) 日刷1W	0.55	0.60	上架中	编辑
185	【全民K歌】试听 (面值:100)	0.22	0.28	上架中	编辑
1	【特慢】名片赞 (面值:10000) 日刷1W	1.2	1.20	上架中	编辑
15	录音播放200丨BF200个	3.8	5.00	上架中	编辑
83	【全民K歌】试听 (面值:1000)	3	3	上架中	编辑
92	空间人气(面值:1000)	0.4	0.4	上架中	编辑
98	快手播放(面值:1000)	0.26	0.32	上架中	编辑
114	理论永久-超级会员丨自带业务请勿下单丨稳定性极强丨质保25天（推荐）	16.88	17.00	上架中	编辑
126	理论永久-超级会员丨自带业务请勿下单丨稳定性极强丨质保25天（需要密码）	17.8	17.8	上架中	编辑
135	24小时到账-QQ飞车180天雷诺	5.5	7.00	上架中	编辑
149	极客荣耀金币——周金币上限3500-4200	8.5	9.90	上架中	编辑
205	电信无限流量卡月租30.	41.00	45.00	上架中	编辑
224	【抖音】fen丝 (面值:100)	0.50	0.55	上架中	编辑

图 4.6 分站内部价格表

(三) 数据作弊下的应用推广渠道

为了保障应用的下载和使用数量，APP 厂商通常会通过第三方渠道来进行宣传推广，吸纳更多的用户。如何获取到万级、十万级甚至是百万级的用户并且还是在成本可控的范围内是 APP 推广阶段遇到的最大问题。

随着移动互联网创业成本的高涨，真正从通过市场宣传等正规渠道带来的用户越来越少，这使得传统的 APP 推广的优质渠道价格水涨船高。在这种形势下 APP 推广刷量产业链应运而生，既帮助 APP 做好面子工程，达成其想要的效果，又能赚取高额的推广费用。

2018 年 9 月，我们监测到名为“SensorService”的应用存在异常行为，分析发现其通过某广告 SDK 传播，安装后无图标，并且伪装成系统服务，利用系统漏洞进行提权，接收云端服务器控制命令进行静默安装推广应用、刷量等恶意操作[50]。其首次推广后还会在后面连续的几天里再次启动推广应用伪造推广的 APP 留存，从而获取推广收益。

图 4.7 某推广平台的应用推广价目表及规则

三、 数据信息安全相关产业生态

数据信息安全相关产业与流量获取分发、流量变现盈利产业不同，如果说流量获取分发和流量变现盈利更多的属于黑灰产中的灰产，那么数据信息安全相关产业更多的是数据窃取、敲诈勒索和网络诈骗等黑产。

(一) 利用恶意软件实施电信诈骗犯罪全球化

每年全国各地都会发生大量电信诈骗案件，使受害人蒙受大量的财产损失，电信诈骗已经成为全社会关注的信息安全焦点问题，危害极为严重。公民的个人信息泄露成为电信诈骗犯罪的基础条件，结合移动互联网的发展，电信诈骗技术和手段不断变化，诈骗目标更加精确。

手机中存储着用户的大量隐私信息，并且时常同用户的资金绑定在一起。通过植入移动恶意软件不法分子能够控制用户的手机，一方面能够对用户的隐私有完全的获取能力，

另一方面也获得了对用户资金的控制能力。

早在 2016 年，我们就深入分析了国内冒充公检法的跨平台电信诈骗活动，不法分子向受害者手机发送包含恶意软件下载链接的信息，以获取“案件号”、“单位代号”、“电子凭证”为由诱骗受害者点击链接，下载安装恶意软件以此来获得受害者手机的控制权。

2018 年我们监测到针对韩国用户的电信诈骗活动[51]，恶意软件伪装成韩国金融行业相关应用，通过窃取短信信息，拦截电话短信，伪造通话记录，并伪造拨号界面对特定的号码进行拦截转拨实施诈骗，受害者在整个过程中基本无感知。由于跨境网络电信诈骗增加了侦查取证难度，使得电信诈骗犯罪呈现全球化趋势。

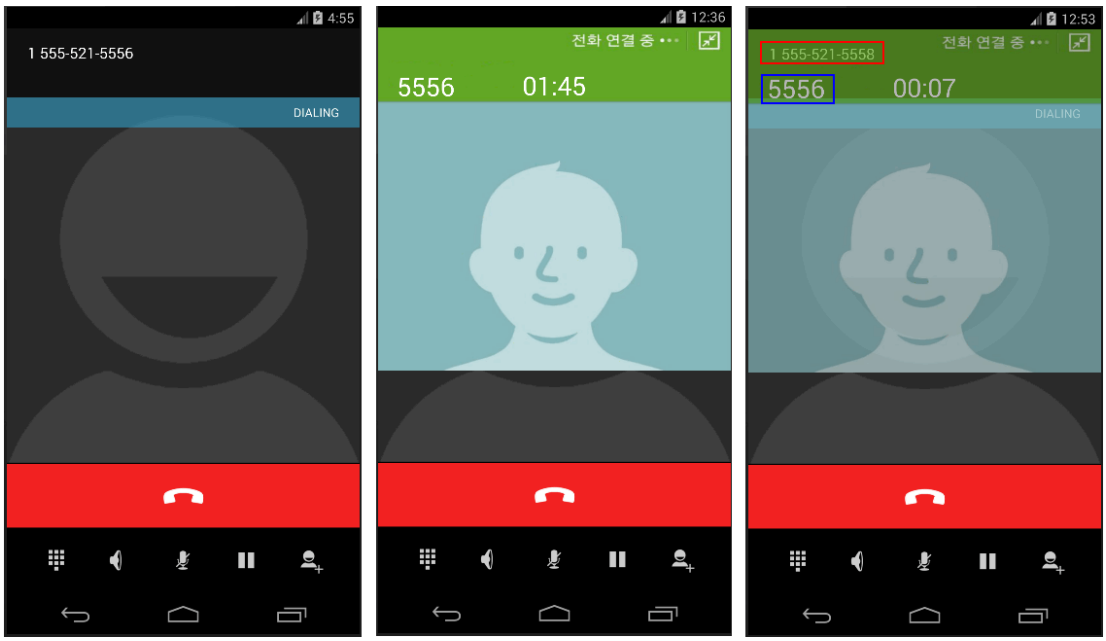


图 4.8 伪造拨号界面

(二) 社交网络下的新型钓鱼诈骗犯罪模式

近几年网贷平台数量在国内迅速增长，与传统贷款方式相比，网贷一般为无抵押贷款，门槛低，渠道成本低，交易便捷，已成为了一种潮流趋势。因此，利用贷款名目进行网络诈骗的情况也呈上升趋势。

不法分子通过电话短信等方式联系用户，通过一定的话术吸引用户，将用户引导到 QQ，微信社交软件后提供虚假贷款网站或者虚假贷款 APP，在用户提交相关信息后，常以各种理由要求用户交纳相应的贷款费用，最终以账号冻结、网站的升级等名义掩饰诈骗行为。

我们研究发现这类虚假贷款网站或者虚假贷款 APP 从代码、页面布局、访问的网址都有明显的相似性，带有明显的批量制作特征。同时，我们还发现受骗人群集中在 80 后到 90 初，一方面对于移动互联网上的新事物新思想接受较快；另一方面他们已经有一定的经济能力，但在事业家庭上又处于上升期，因此对于财富的增长需求比较强烈。

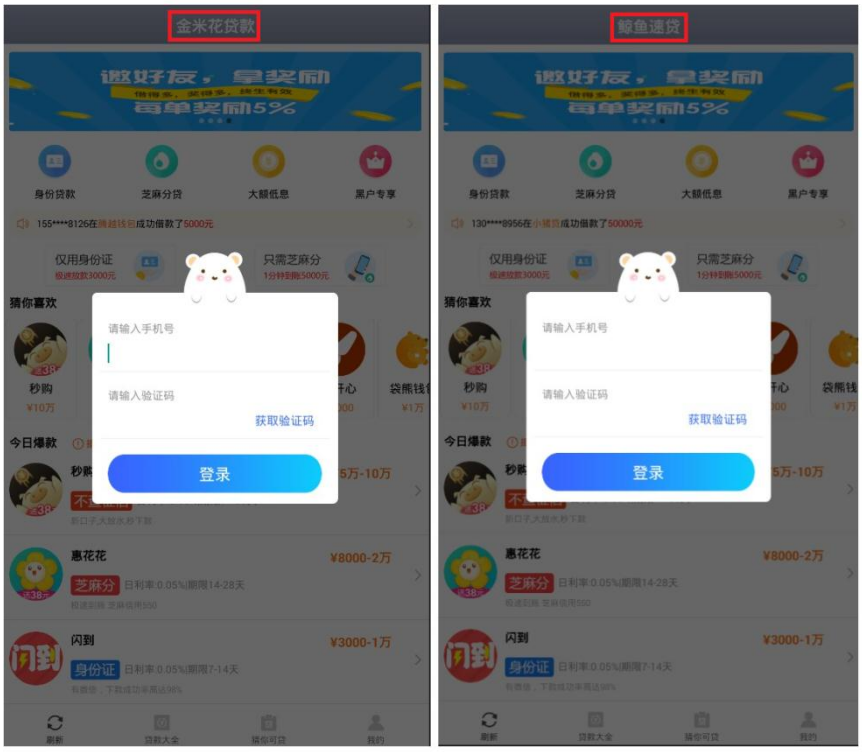


图 4.9 虚假贷款 APP 界面展示

四、 移动平台黑灰产业特征与趋势

2018 年，移动平台黑灰产业呈现一些特征，首先是依托互联网巨头的产品生态而生存；其次，黑灰产之所以如此发达且从业人员众多，就在于它非常具有互联网特色，能够精准地抓住用户的心理诉求和痛点，它会观察最新的产业热点，利用人工智能，不断更新骗术。

同时，技术灰黑产已经成为网络犯罪的技术支撑，组织方式上出现了非常明显的变化。一是黑灰产业链更清晰，各环节之间的合作更紧密。二是黑灰产业正在从粗放式的生产模式走向精加工模式开始走向大数据，走向数据挖掘，走向人工智能。三是黑灰产业逐渐呈现国际化特征，对象的选择也开始从企业到个人，被侵害对象的防范能力在降低。

第五章 协同联动共建大安全生态环境

2018 年 4 月，习主席在全国网络安全和信息化工作会议上强调指出，要提高网络综合治理能力，形成党委领导、政府管理、企业履责、社会监督、网民自律等多主体参与，经济、法律、技术等多种手段相结合的综合治网格局。要落实关键信息基础设施防护责任，行业、企业作为关键信息基础设施运营者承担主体防护责任，主管部门履行好监管责任。要依法严厉打击网络黑客、电信网络诈骗、侵犯公民个人隐私等违法犯罪行为，切断网络犯罪利益链条，持续形成高压态势，维护人民群众合法权益。要深入开展网络安全知识技能宣传普及，提高广大人民群众网络安全意识和防护技能。

一、 严峻的系统环境

(一) 系统漏洞情况

Android 系统开源就意味着在安全问题上显得更加透明，运用工具审查安全漏洞变得更容易。根据汇总 CVE 数据的网站出具的 2018 年度 CVE Details 报告显示[52]，Android 系统以 611 个漏洞位居产品漏洞数量第二名，与 2017 年 842 个相比略有减小，下降 27.4%，与 2016 年相比增加 16.6%，仍然处在漏洞榜前列。

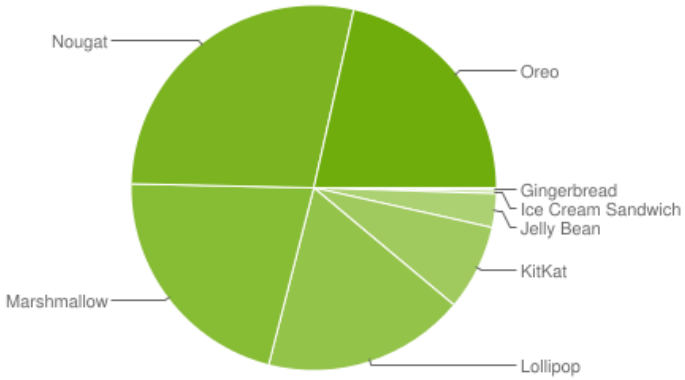
	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Debian Linux	Debian	OS	947
2	Android	Google	OS	611
3	Ubuntu Linux	Canonical	OS	492
4	Enterprise Linux Server	Redhat	OS	393
5	Enterprise Linux Workstation	Redhat	OS	377
6	Enterprise Linux Desktop	Redhat	OS	368
7	Firefox	Mozilla	Application	333
8	Acrobat Reader Dc	Adobe	Application	286
9	Acrobat Dc	Adobe	Application	286
10	Windows 10	Microsoft	OS	255

图 5.1 2018 年 CVE 网站产品漏洞数量 TOP 排名情况

(二) 系统更新情况

Google 每次发布 Android 新版本，对系统安全性都有所增强，但是由于 Android 系统碎片化严重，系统版本更新速度慢，系统安全环境整体提升受到影响。

截止 2018 年 10 月，Google 发布的 Android 系统版本分布统计[53]，Android Nougat（Android 7.0/7.1）达到 28.2%，占比第二的是 Android Oreo（Android 8.0/8.1）总占比已达 21.5%，而最新系统版本 Android 9 Pie 不足 0.1%。



图片来自（https://developer.android.com/about/dashboards/）

图 5.2：截止 2018 年 10 月 Android 系统版本分布占比情况

(三)　厂商漏洞修复情况

Android 操作系统目前仍未有非常完善的补丁机制为其修补系统漏洞，再加上 Android 系统碎片化严重，各手机厂商若要为采用 Android 系统的各种设备修复安全问题则需投入大量人力物力。受到 Android 系统的诸多特性的影响，系统版本的碎片化问题日益突出。就每一款手机而言，厂商在其维护周期内，通常会隔一段时间向用户推送一次升级版本，而用户在大多数情况下可以自主选择升级或不升级。综合这些特性，在 Android 系统的安全漏洞方面，也产生了严重的碎片化问题。

根据《2018 年安卓系统安全性生态环境研究》报告数据[54]，下图为各厂商手机中实际存在的安全补丁级别情况，该情况是将各厂商现存手机中实际补丁日期与谷歌官方最新版本（2018 年 12 月）版本对比，综合安全补丁级别最高、最新的手机品牌前 5 名。图中绿色方块面积越大，说明该厂商的手机补丁级别相对越高，漏洞修复相对越及时；相反，如果黄色和橙色面积越大，则说明补丁级别越低，漏洞修复越滞后。

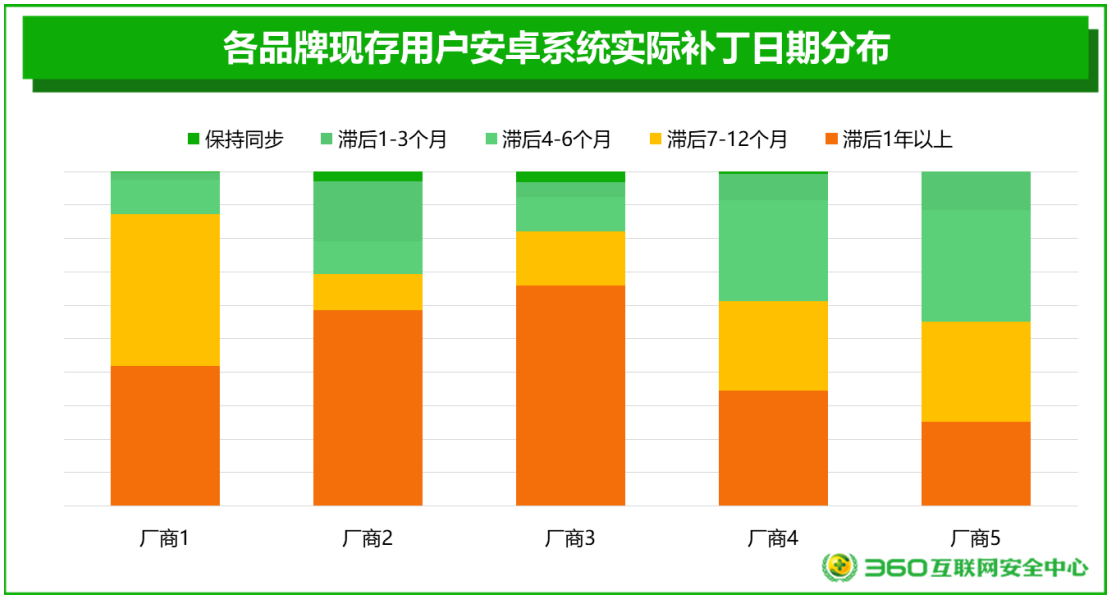


图 5.3 2018 年各品牌现存用户安卓系统实际补丁日期分布

图中我们可以看出，在及时推送安全补丁级别方面，TOP5 的厂商在本季度的检测结果显示较好，而且在本季度的调研中这五个厂商均有保持与谷歌最新安全补丁同步的更新提供，这也显示了厂商对于用户手机中安全补丁等级的逐步重视。

二、 系统厂商自我约束

作为系统厂商 Google 会定期更新开发者政策，以便为 Google Play 上的开发者和消费者保持安全和积极的体验。在最近一次更新中，Google Play 禁止使用设备计算资源挖掘加密货币的 APP 上架，但“远程管理加密货币”的 APP 仍然是允许的[55]。挖矿活动会对设备的性能产生巨大影响，在某些情况下，它还可能因过热或损坏电池而损坏设备。这一改变意味着 Google 将开始从 Google Play 中，删除任何使用设备的 CPU 或 GPU 进行加密货币挖矿操作的 APP。

安全性和性能方面，从 2018 年 11 月 1 日起，Google Play 要求对现有 APP 进行更新[56]，以达到 API 级别 26 (Android 8.0)或更高级别，确保 Google Play 上的所有 APP 都是使用最新的 APl 构建的，这些 APl 针对安全性和性能进行了优化。

在用户隐私保护方面，针对请求短信和通话记录权限的 APP，只有设置为默认呼叫或短信的应用才能访问电话和短信数据。同时 Google 也推荐了替代方案，例如，SMS Retriever API 可以执行基于短信的用户验证，SMS Intent 填充默认的短信以共享内容或邀请。对于需要访问短信和通话记录权限的开发人员需要在规定时间内填写权限声明表单，根据该表单 Google 审查其应用，以确保他们在获得用户许可后确实需要访问敏感信息。对于未提交权限声明表单的应用开发者，将从 Google Play 中删除其 APP。

三、 政府监管与信息举报

(一) 处置淫秽色情

2018 年 4 月，为切实净化网络文化环境，加大网上“扫黄打非”工作力度。全国“扫黄打非”办公室作出专门部署，深入开展“净网 2018”行动[57]。各地“扫黄打非”部门全面开展监测和清查，及时处置淫秽色情等有害信息突发传播情况，督促主要互联网企业落实主体责任加强内容审核、主动清理有害信息，从快从严查办了一大批网络行政或刑事案件。

根据 360 烽火实验室监测，仅从色情播放器 APP 数量上看，从 4 月开始出现逐渐下降，在 9 月出现了明显的大幅下降，由此可见政府相关部门的打击活动，起到了一定效果。

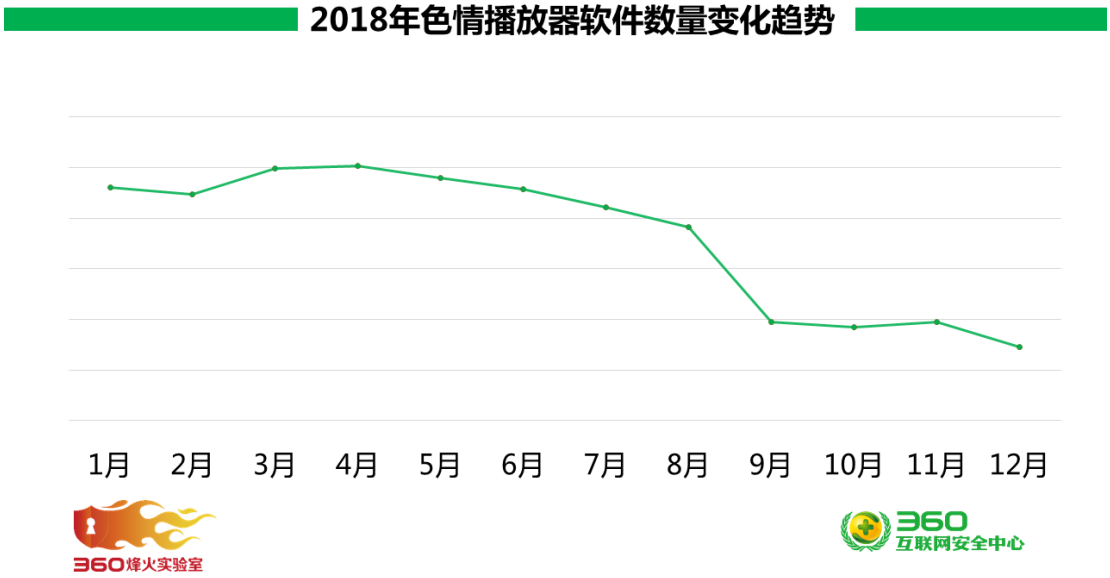


图 5.4 2018 年色情播放器软件数量变化趋势

(二) 整治骚扰电话

2018 年 7 月，工信部等 13 个国家部门联合发布《综合整治骚扰电话专项行动方案》，决定自 2018 年 7 月起到 2019 年 12 月底，在全国范围内组织开展为期一年半的综合整治骚扰电话专项行动，重点对商业营销类、恶意骚扰类和违法犯罪类骚扰电话进行整治[58]。

方案提出了五个方面的重点工作，首先是严控骚扰电话传播渠道，包括加强语音线路和码号资源管理、加强电话用户合同约束、全面规范营销外呼业务、全面清理各类骚扰软件（呼死你等）。同时，方案要求全面提升技术防范能力，包括强化主叫号码鉴权和通话溯源、提升骚扰电话拦截能力（+86 虚拟境外号码/响一声/呼死你）、增强骚扰电话提醒和预警能力、增强骚扰电话综合管控能力，并规范重点行业商业营销行为。

方案特别强调要依法惩处违法犯罪、健全法规制度保障，集中侦破一批利用电话实施诈骗、敲诈勒索、虚假广告宣传等违法犯罪案件。对明知从事违法犯罪活动，仍提供网络、技术、线路等服务的企业和人员依法严惩。集中侦破一批侵犯公民个人信息犯罪案件。依法严厉打击各行政机关和电信、金融、医疗、教育、物业、物流、寄递等重点单位工作人员非法出售或者向他人提供公民个人信息的违法犯罪行为。

(三) 关停下架违规应用

2018 年 12 月，国家网信办会同有关部门针对网民反映强烈的违法违规、低俗不良 APP 程序乱象，集中开展清理整治专项行动，依法关停下架“成人约聊”“两性私密圈”“澳门金沙”“夜色的寂寞”“全民射水果”等 3469 款涉黄涉赌、恶意扣费、窃取隐私、诱骗诈骗、违规游戏、不良学习类 APP[59]。

针对媒体重点曝光的以中小学生为用户对象的学习类 APP，屡次出现涉黄内容、网络游戏等乱象责令整改，并处以罚款。同时，教育部也印发了《关于严禁有害 APP 进入中小学校园的通知》，要求全面排查坚决杜绝有害 APP 侵蚀校园，未经备案审查的学习类 APP

禁止在校园内使用。

(四) 网络诈骗信息举报

2018 年，猎网平台共收到有效诈骗举报 21703 例，举报者被骗总金额超过 3.9 亿元，人均损失 24476 元，创近五年新高，较 2017 年人均损失增幅 69.8%。

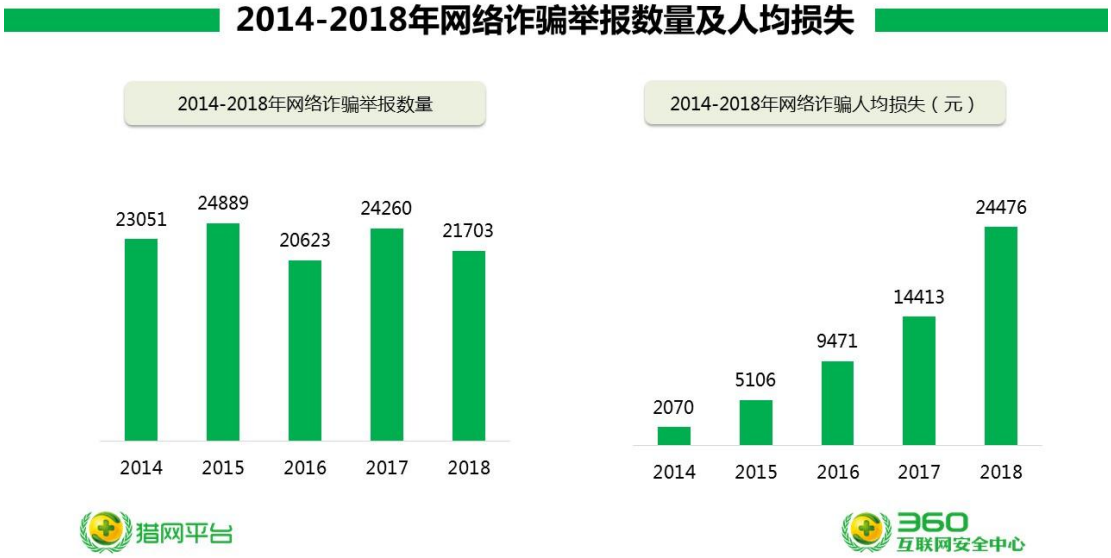


图 5.5 2014-2018 年网络诈骗举报数量及人均损失

2018 年，金融理财诈骗是举报数量最多的网络诈骗，共获得举报 2985 例，其次为虚假招聘诈骗 2570 例，网游交易诈骗 2297 例。

人均损失方面，损失最严重的也为金融理财诈骗，人均损失金额 70985 元，其次为赌博博彩诈骗，人均损失金额为 65861 元。身份冒充类诈骗人均损失 26700 元，排在第三位。

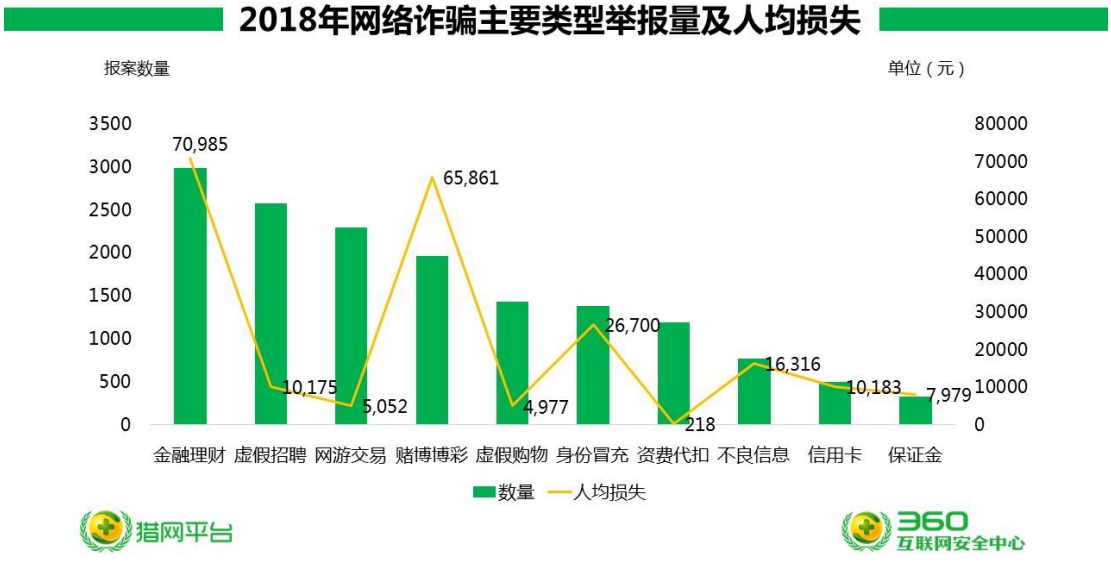


图 5.6 2018 年网络诈骗主要类型举报量及人均损失

四、 警企协同打击网络犯罪

截至目前，360 猎网平台已与全国 800 个地区的公安机关建立联系，共协助侦破、带破逾 600 余起重大网络诈骗犯罪案件，涉案金额达 3 亿元，抓获犯罪嫌疑人超过 700 人，打掉 60 余个组织严密、分工明确的大型诈骗团伙，多次获得公安机关认可和表彰致谢。

其中，仅 2018 年，360 猎网平台就协助公安机关侦破、带破 400 余起重大网络诈骗犯罪案件，涉案金额 1.2 亿元，抓获犯罪嫌疑人超过 240 余人。

截至目前，共 5 家网安和 144 余家互联网企业成员正式加入猎网联盟，360 公司一共向联盟企业推送 4289 条诈骗欺诈信息。

同时，2018 年 360 烽火实验室在涉及移动平台的网络犯罪案件侦办中，实验室通过溯源等分析手段，协助公安机关找到恶意软件作者 QQ 号 1.6 万余个，手机号及邮箱线索 1.2 万余条，案件涉及的恶意软件分析报告 15 篇以及提供 6 次溯源分析。

第六章 威胁趋势预测

一、 5G 时代到来物联网安全问题凸显

2018 年 2 月，ADB.Miner 感染了部分智能电视盒子，利用智能电视进行挖矿活动。2018 年 3 月，日本媒体报道了大量日本用户的路由器设置被劫持，将用户重定向到恶意 IP 地址，下载安装恶意软件。2018 年 5 月，亚马逊 Echo 音箱被曝“监听”用户，并将悄悄录下的对话发给了他人。2018 年 9 月，手持终端巴枪被植入恶意软件，菜鸟驿站 1000 万条快递数据被非法窃取。

多个机构预测，预计十三五期间，我国设备联网数量将突破 17 亿。物联网规模急剧扩大，其威胁因子也正急速增加。另一个不可忽视的风险因素则在于 5G 的迅速发展，毫无疑问，2019 年将成为 5G 加速发展的一年。未来，会有越来越多的 5G 物联网设备直接连接至 5G 网络，而非通过 Wi-Fi 路由器。然而，这一趋势将使设备更容易遭到攻击，以家庭用户为例，物联网设备会跳过核心路由器，从而难以进行监控。此外，在云端备份或传输数据情况也会为攻击者提供大量的新的攻击目标。

二、 基于内容的诈骗活动将成为主流趋势

2019 年 1 月，我们发布了《移动平台新型诈骗解析》报告[60]，报告对用户 2018 年在移动平台遭受诈骗的案例进行了梳理分类，我们发现基于内容的诈骗活动尤为突出。主要表现在诈骗者通过电话、短信等方式联系用户，以“贷款”、“理财”、“赌博”、“私彩”等类型的 APP 设置骗局，在 APP 页面上通过一定的虚假宣传和提示，再配以诈骗者的诱导话术，骗取用户交纳相应费用实施诈骗活动。

在传播方面，这类软件具备一定的特征，比如，通过短信方式进行推广，短信信息中的链接备案信息可能与其提供的服务内容资质不符。通常不会直接获取到 APP 或者 APP 的下载地址，需要先联系网页上所谓的客服微信或者 QQ 号。客服提供的 APP 下载地址一般为第三方应用内测分发平台。这些特征能够绕过一些自动化安全检测流程，增强迷惑性，近一步增加用户的信任度。

此外，这类软件与以往的恶意软件性质不同，由于这类软件没有恶意行为，APP 在诈骗过程中仅充当载体作用，所以依靠代码和行为的检测技术无法识别。这类诈骗活动说到底是更多的人与人之间的较量，将会成为未来移动平台诈骗的主流趋势。

三、 “币圈”降温但攻击仍将继续

“眼见他起高楼，眼见他宴宾客，眼见他楼塌了!”用来形容 2018 年的虚拟货币最为贴切。以比特币（Bitcoin）为例，年初还在 1 万美元左右，年末已经不足 4 千美元。虽然虚拟货币价格大幅下降，但是围绕虚拟货币的攻击并没有停止。

图 6.1 2018 年比特币价格变化

2018 年 10 月，我们发现利用剪卡板功能替换虚拟货币钱包地址的恶意软件，木马首先开启一个监听器，监听剪贴板的内容。然后，监控剪贴板里的内容和长度是否符合特定钱包地址格式。最后，如果符合目标格式就向服务器发送请求，获取对应的电子钱包地址进行替换。

除此以外，还发现了伪装成虚拟货币钱包的虚假 APP，大部分虚假 APP 会展现大量广告并诱导用户下载广告软件，带来额外的安全风险。

结合今年在多个虚拟货币项目中发现的安全漏洞以及虚拟货币自身匿名性的特点，虽然虚拟货币价格大幅下降，但是安全事件还是会持续发生，勒索病毒、挖矿病毒、针对交易所，公链，合约的攻击会继续，也会有新技术手段出现。

四、 社交网络下的传播链重建

近年来，除了 Google Play 以外，越来越多的手机品牌都有自己的应用市场，由于监管部门一直以来在整治应用市场方面的努力，不仅在用户体验得到明显提升，APP 安全方面也有了保障。由于应用市场在审核上越来越严格，使得一些不法分子不得不放弃借助应用市场传播，重新寻找新的传播渠道。

我们在一些 APP 中发现，要求用户必须分享到自己的 QQ 群才能使用软件功能并且对分享的 QQ 群数量和 QQ 群里的人数有明确要求，分享文字内包含了不法分子预先设置的 QQ 群号，诱导其他用户加群下载 APP。

```
public void 取号() {
        this.判断串号();
        this.判断网络串号为空改本地();
        this.号码数组 = 文本操作.分割文本(this.串号, "@");
        this.数组下标 = IntegerVariant.getIntegerVariant(数组操作.取数组成员数(ArrayVariant.getArrayVariant
        (this.号码数组)))
                .sub(ByteVariant.getByteVariant(1)).getInteger();
        this.号码 = this.号码数组[算术运算.取随机数(0, this.数组下标)];
        this.分享文字 = "|\n\n|\n\n|\n\n|\n\n特大好消息：\n\n本周最新QQ蜜码破解神器已问世
        ,只需知道QQ号就能破出密码,有需要的赶紧进群下载。\n\n注意：王者荣耀.英雄连盟.穿越火线.DNF.都是用Q号登
        录的，有些游戏号很值钱，你们千万不要盗别人的游戏号，否则后果自负。\n\n快进群"
                + this.号码 + "\n点击号码进群下载软件.免费使用
                .如果不相信,可以随便找个QQ测试一下,保证秒破密码(分享码:Hyidv
                点击统计)\n\n|\n\n|\n\n|\n\n|";
    }

    public void 按钮_分享$被单击() {
        this.取号();
        应用操作.弹出提示("必须分享到不同群内才可得到授权!");
        QQ文字分享.开始分享(this.分享文字);
        this.分享次数 = IntegerVariant.getIntegerVariant(this.分享次数).add(ByteVariant.getByteVariant(1)).
        getInteger();
    }

    public void 按钮显示$被单击() {
        if(IntegerVariant.getIntegerVariant(this.分享次数).cmp(ByteVariant.getByteVariant(10)) < 0) {
            对话框类.信息框("未授权",
            "无法显示密码,系统监测分享次数不够,请先分享到10个不同的群激活授权,再点击显示密码", "ok");
        }
        else {
            对话框类.信息框("授权未通过",
            "原因是你可能分享到了重复的Q群或者分享的群人数太少,至少要50人以上的群,请继续分享分享！只差一步了
            .加油", "ok");
        }
    }
```

图 6.2 诱导用户分享代码片段

这些 APP 名称大部分伪装成“破解”、“外挂”、“辅助”，都是使用一些简易语言开发制作。经过分析，实际上这类软件大部分并无实际功能，目的就是利用 QQ 群传播引导用户加群，恶意软件就藏在这些 QQ 群的共享文件夹里，从而达到不法分子利用社交网络传播恶意软件的新方式。这种方式传播成功率高，隐蔽性强，同时也成为一些羊毛党 QQ 群的引流方式，将会逐渐成为恶意软件传播的主要途径之一。

五、 数据泄露推动隐私立法全球化

2018 年用户数据泄露事件频发，Facebook 被曝数据泄露 8700 万用户受影响、国内某知名连锁酒店 1.3 亿用户开房记录、某快递巨头 3 亿快递收寄人信息在暗网交易、某航空公司数千万用户数据在未获授权情况下不当取览等等。

一方面，数据泄露造成用户人身财产受到威胁，不法分子通过各种途径收集到人们被泄露出去的隐私，经过筛选分析用户特征，从事电信诈骗、非法讨债甚至绑架勒索等精准犯罪活动；另一方面，数据泄露对企业和国家造成的危害则是巨大的，如果是国家重点行业、领域的数据被泄露那不仅对企业来说是致命的，还会对国家安全造成严重威胁。

欧盟在 2018 年出台了《通用数据保护条例》(GDPR)，这为欧盟以外的国家颁布各种安全和隐私举措提供了借鉴。加拿大已实施类似 GDPR 的法律；巴西最近通过类似 GDPR 的隐私法律，并将在 2020 年开始生效；受到 GDPR 的启发，澳大利亚与新加坡也已颁布了 72 小时违规通知；印度也正在考虑实施类似的法律；在 GDPR 实施后不久，美国加利福尼亚州通过的隐私法被认为是美国迄今为止最严厉的隐私法。

全球其他国家也正在讨论 GDPR 的妥善性，亚太地区以此为参考，数据立法活动也将越来越多，澳大利亚及新加坡已经开始行动，我国也颁布了《中华人民共和国网络安全法》明确要加强对个人信息保护，各国政府都会趋向于推出更加严厉的数据安全政策法规，企业将在个人数据隐私保护上投入更多力量。未来几年，黑客、黑产攻击不会停止，但数据安全保护技术将加速推出，针对不断提升的安全与隐私需求，法律与监管行动会不断升级。

附录一：参考资料

[1]ADB.Miner 安卓蠕虫的更多信息：https://blog.netlab.360.com/adb-miner-more-information/

[2]Kotlin：http://kotlinlang.org/

[3]First Kotlin-Developed Malicious App Signs Users Up for Premium SMS Services：
https://blog.trendmicro.com/trendlabs-security-intelligence/first-kotlin-developed-malicious-app-signs-users-premium-sms-services/

[4]Switcher:Android joins the‘attack-the-router’club：
https://securelist.com/blog/mobile/76969/switcher-android-joins-the-attack-the-router-club/

[5]XLoader Android Spyware and Banking Trojan Distributed via DNS Spoofing：
https://blog.trendmicro.com/trendlabs-security-intelligence/xloader-android-spyware-and-banking-trojan-distributed-via-dns-spoofing/

[6]剪贴板幽灵：币圈的神偷圣手：http://blogs.360.cn/post/analysis_of_Clipper.html

[7]TeleRAT: Another Android Trojan Leveraging Telegram’s Bot API to Target Iranian Users：
https://unit42.paloaltonetworks.com/unit42-telerat-another-android-trojan-leveraging-telegrams-bot-api-to-target-iranian-users/

[8]New Telegram-abusing Android RAT discovered in the wild：
https://www.welivesecurity.com/2018/06/18/new-telegram-abusing-android-rat/

[9]TeleSharp：https://github.com/MojtabaTajik/TeleSharp

[10]MysteryBot; a new Android banking Trojan ready for Android 7 and 8：
https://www.threatfabric.com/blogs/mysterybot__a_new_android_banking_trojan_ready_for_android_7_and_8.html

[11]内网穿透——ANDROID 木马进入高级攻击阶段：
http://blogs.360.cn/360mobile/2016/12/01/analysis_of_dresscode/

[12]内网穿透——ANDROID 木马进入高级攻击阶段（二）：
http://blogs.360.cn/360mobile/2017/05/25/analysis_of_milkydoor/

[13]Android/TimpDoor Turns Mobile Devices Into Hidden Proxies：
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/android-timpdoor-turns-mobile-devices-into-hidden-proxies/

[14]毒云藤（APT-C-01）军政情报刺探者揭露：http://blogs.360.cn/post/APT_C_01.html

[15]蓝宝菇 - 核危机行动揭秘：
http://blogs.360.cn/post/%E8%93%9D%E5%AE%9D%E8%8F%87-%E6%A0%B8%E5%8D%B1%E6%9C%BA%E8%A1%8C%E5%8A%A8%E6%8F%AD%E7%A7%98.html

[16]Fake AV Investigation Unearths KevDroid, New Android Malware：
https://blog.talosintelligence.com/2018/04/fake-av-investigation-unearths-kevdroid.html

[17]Reaper Group’s Updated Mobile Arsenal：

https://unit42.paloaltonetworks.com/unit42-reaper-groups-updated-mobile-arsenal/

[18]Operation Rocket Man：https://blog.alyac.co.kr/1853

[19]Operation Blackbird：https://blog.alyac.co.kr/2035

[20]North Korean Defectors and Journalists Targeted Using Social Networks and KakaoTalk：https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/north-korean-defectors-journalists-targeted-using-social-networks-kakaotalk/

[21]Malware on Google Play Targets North Korean Defectors：https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/malware-on-google-play-targets-north-korean-defectors/

[22]Operation Transparent Tribe：https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf

[23]Indian Military Personnel Targeted by “Operation C-Major” Information Theft Campaign：https://blog.trendmicro.com/trendlabs-security-intelligence/indian-military-personnel-targeted-by-information-theft-campaign/

[24]Hacking Group Spies on Android Users in India Using PoriewSpy：https://blog.trendmicro.com/trendlabs-security-intelligence/hacking-group-spies-android-users-india-using-poriewspy/

[25]Stealth Mango and Tangelo: Nation state mobile surveillanceware stealing data from military & government officials：https://blog.lookout.com/stealth-mango

[26]Deciphering Confucius’ Cyberespionage Operations：https://blog.trendmicro.com/trendlabs-security-intelligence/deciphering-confucius-cyberespionage-operations/

[27]Confucius Update: New Tools and Techniques, Further Connections with Patchwork：https://blog.trendmicro.com/trendlabs-security-intelligence/confucius-update-new-tools-and-techniques-further-connections-with-patchwork/

[28]肚脑虫组织（APT-C-35）移动端攻击活动揭露：http://blogs.360.cn/post/analysis-of-apt-c-35.html

[29]The Urpage Connection to Bahamut, Confucius and Patchwork ：https://blog.trendmicro.com/trendlabs-security-intelligence/the-urpage-connection-to-bahamut-confucius-and-patchwork/

[30]Targeted Attacks in the Middle East Using KASPERAGENT and MICROPSIA：https://researchcenter.paloaltonetworks.com/2017/04/unit42-targeted-attacks-middle-east-using-kasperagent-micropsia/

[31]FrozenCell: Multi-platform surveillance campaign against Palestinians：https://blog.lookout.com/frozencell-mobile-threat

[32]New GnatSpy Mobile Malware Family Discovered：

http://blog.trendmicro.com/trendlabs-security-intelligence/new-gnatspy-mobile-malware-family-discovered/

[33]Lookout finds new surveillanceware in Google Play with ties to known threat actor targeting the Middle East：https://blog.lookout.com/desert-scorpion-google-play

[34]Ongoing Android Malware Campaign Targets Palestinians - Part 1：https://www.symantec.com/blogs/expert-perspectives/ongoing-android-malware-campaign-targets-palestinians-part-1

[35]Ongoing Android Malware Campaign Targets Palestinians - Part 2：https://www.symantec.com/blogs/expert-perspectives/ongoing-android-malware-campaign-targets-palestinians-part-2

[36]Hamas' online terrorism：https://www.idf.il/en/articles/hamas/hamas-online-terrorism/

[37]Vipers, Falcons, and Droids: Apparent Link Between Arid Viper/Desert Falcons and Recent Android Malware Targeting Israeli Military：https://www.ci-project.org/blog/2017/3/4/arid-viper

[38]mAPT ViperRAT Found in Google Play：https://blog.lookout.com/viperrat-google-play

[39]Infrastructure and Samples of Hamas' Android Malware Targeting Israeli Soldiers ：https://www.clearskysec.com/glancelove/

[40]GoldenCup: New Cyber Threat Targeting World Cup Fans：https://www.symantec.com/blogs/expert-perspectives/goldencup-new-cyber-threat-targeting-world-cup-fans

[41]Google Play Users Risk a Yellow Card With Android/FoulGoal.A：https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/google-play-users-risk-a-yellow-card-with-android-foulgoal-a/

[42]GlanceLove: Spying Under the Cover of the World Cup：https://research.checkpoint.com/glancelove-spying-cover-world-cup/

[43]黄金鼠组织--叙利亚地区的定向攻击活动：https://ti.360.net/blog/articles/analysis-of-apt-c-27/

[44]移动端跨越攻击预警：新型 APT 攻击方式解析：http://blogs.360.cn/post/analysis-of-apt-c-27.html

[45]Domestic Kitten: An Iranian Surveillance Operation：https://research.checkpoint.com/domestic-kitten-an-iranian-surveillance-operation/

[46]ArmaRat：针对伊朗用户长达两年的间谍活动：http://blogs.360.cn/post/analysis_of_ArmaRat.html

[47]Under the SEA:A Look at the Syrian Electronic Army's Mobile Tooling：https://i.blackhat.com/eu-18/Wed-Dec-5/eu-18-DelRosso-Under-the-SEA.pdf

[48]RottenSys: Not a Secure Wi-Fi Service At All：https://research.checkpoint.com/rottensys-not-secure-wi-fi-service/

[49]StealthBot：150 余个小众手机品牌预置刷量木马销往中小城市：
http://blogs.360.cn/post/analysis_of_stealthbot.html

[50]SensorBot：利益驱动下的病毒营销：http://blogs.360.cn/post/analysis_of_SensorBot.html

[51]针对韩国长达 5 年的跨境网络电信诈骗：
http://blogs.360.cn/post/telecom_fraud_network_for_Korea.html

[52]Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2018：
https://www.cvedetails.com/top-50-products.php?year=2018

[53] Android 平台版本：https://developer.android.com/about/dashboards/

[54] 2018 年度安卓系统安全性生态环境研究：
http://zt.360.cn/1101061855.php?dtid=1101061451&did=610082749

[55]开发者政策中心：
https://play.google.com/intl/zh-CN_ALL/about/restricted-content/financial-instruments/cryptocurrencies/

[56]Providing a safe and secure experience for our users ：
https://android-developers.googleblog.com/2018/10/providing-safe-and-secure-experience.html

[57]全国“扫黄打非”办推进开展“净网 2018”等三大专项行动：
http://www.xinhuanet.com/legal/2018-04/09/c_129846373.htm

[58]十三部门关于印发《综合整治骚扰电话专项行动方案》的通知：
http://www.miit.gov.cn/n1146290/n4388791/c6283131/content.html

[59]国家网信办集中开展 APP 乱象专项整治行动 全环节治理将成为常态：
http://www.12377.cn/txt/2018-12/29/content_40629818.htm

[60]移动平台新型诈骗解析：http://blogs.360.cn/post/the_new_telecom_fraud.html

360 烽火实验室

360 烽火实验室，致力于 Android 病毒分析、移动黑产研究、移动威胁预警以及 Android 漏洞挖掘等移动安全领域及 Android 安全生态的深度研究。作为全球顶级移动安全生态研究实验室，360 烽火实验室在全球范围内首发了多篇具备国际影响力的 Android 木马分析报告和 Android 木马黑色产业链研究报告。实验室在为 360 手机卫士、360 手机急救箱、360 手机助手等提供核心安全数据和顽固木马清除解决方案的同时，也为上百家国内外厂商、应用商店等合作伙伴提供了移动应用安全检测服务，全方位守护移动安全。