2019 年 Android 恶意软件专题报告

摘 要

- 2019 年全年，360 安全大脑共截获移动端新增恶意程序样本约 180.9 万个，平均每天截获新增手机恶意程序样本约 0.5 万个。新增恶意程序类型主要为资费消耗，占比 46.8%；其次为隐私窃取（41.9%）、远程控制（5.0%）、流氓行为（4.6%）、恶意扣费（1.5%）、欺诈软件（0.1%）。

- 2019 年全年，360 安全大脑累计为全国手机用户拦截恶意程序攻击约 9.5 亿次，平均每天拦截手机恶意程序攻击约 259.2 万次。

- 从省级分布来看，2019 年全年遭受手机恶意程序攻击最多的地区为广东省，占全国拦截量的 9.8%；其次为山东（7.7%）、江苏（7.3%）、河南（6.9%）、浙江（5.8%）等。

- 从城市分布来看，2019 年全年遭受手机恶意程序攻击最多的城市为北京市，占全国拦截量的 2.2%；其次为重庆（2.0%）、上海（1.9%）、广州（1.9%）、成都（1.8%）等。

- 2019 年移动金融行业、移动流量产业和移动社交领域均遭受了移动恶意软件的攻击。对移动金融行业的攻击，主要表现为窃取大量银行账号密码信息，这类事件大多针对国外银行；而在国内，大量冒充以及虚假金融借贷服务，其本身并无真实借贷业务，仅用于骗取用户隐私和钱财；对移动流量产业的攻击，表现为移动广告商使用不同的欺诈技术获得广告主的报酬；对移动社交领域的攻击，则是利用揣摩特殊人群心里需求特点，使用虚假身份在社交过程中推送虚假信息，诱导充值进行诈骗。

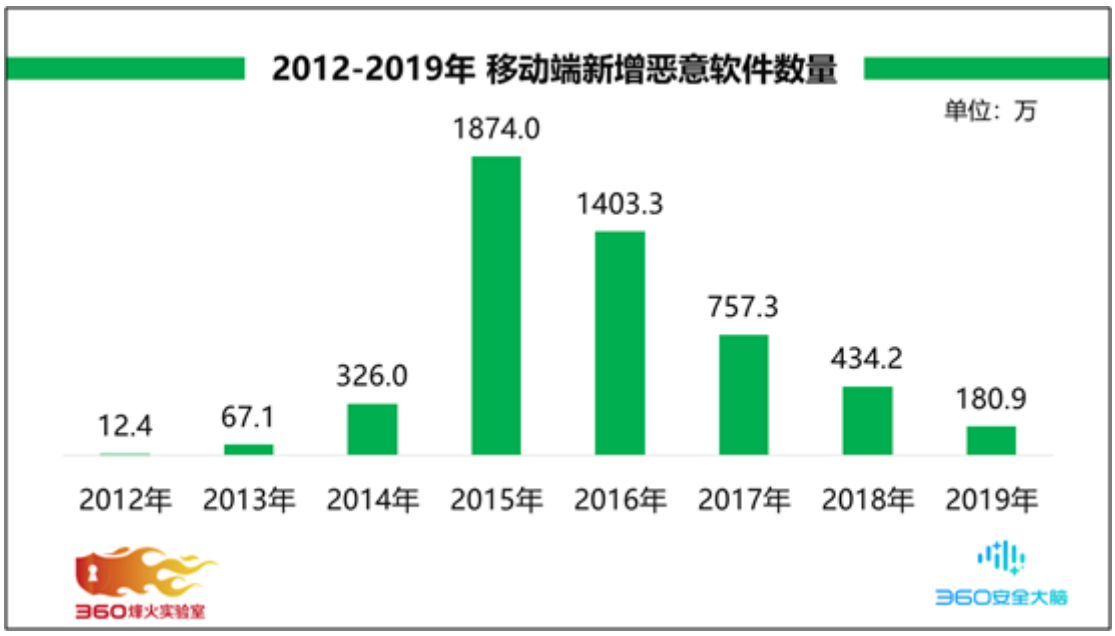
- 2019 全年从漏洞数量看，Android 系统以 414 个漏洞位居产品漏洞数量榜首。从系统更新情况看，截至 2019 年 5 月，Google 发布的 Android 系统版本分布统计，Android Oreo（Android 8.0/8.1）达到 28.3%，占比第二的是 Android Nougat（Android 7.0/7.1）总占比已达 19.2%。从漏洞在野利用情况看，使用 Janus 和 Strandhogg 漏洞的恶意软件较为活跃。
- 2019 年移动端 APT 方面，360 烽火实验室监测到的公开披露的 APT 报告中，涉及移动相关的 APT 报告 14 篇。被提及受到移动 APT 组织攻击的受害者所属国家主要有中国、朝鲜、韩国、印度、巴基斯坦、以色列、叙利亚、伊朗、埃及等东亚、西亚、中东多个国家。移动端 APT 组织活动针对的目标和领域来看，涉及政治、经济、情报等多个重要板块。
- 2019 年围绕 5G、重点领域的钓鱼攻击、生物信息安全以及企业对数据的使用等方面暴露出多种安全风险及问题，将成为未来几年攻防对抗发展的的主要趋势，需要加强治理和战略部署。

关键词：移动安全、恶意软件、移动端 APT、金融、流量、社交

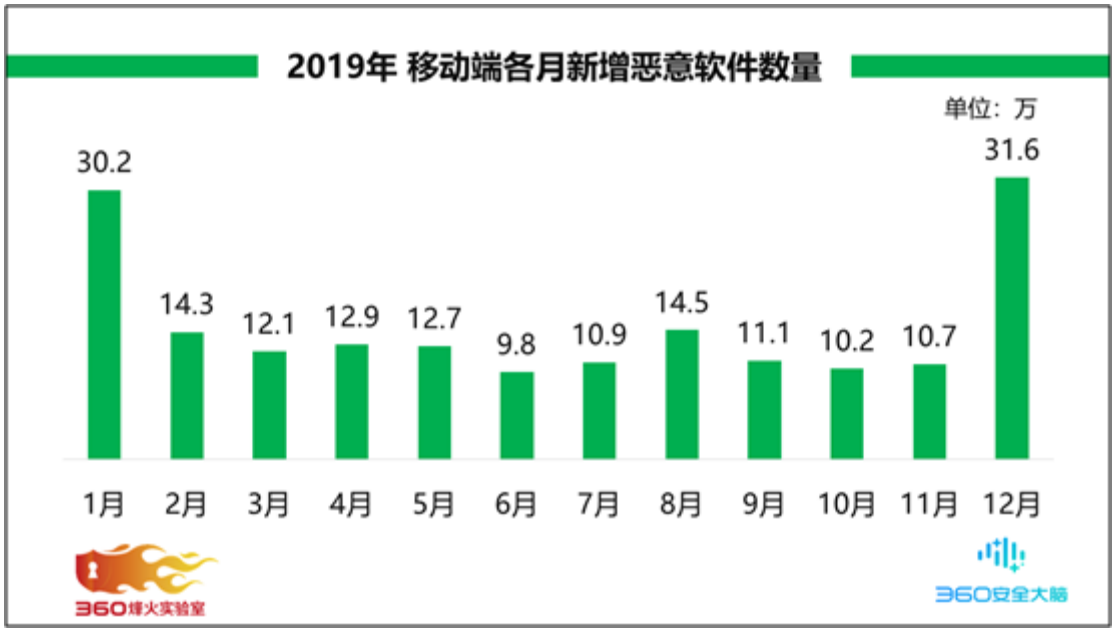
第一章 总体态势

一、 恶意软件新增量与类型分布

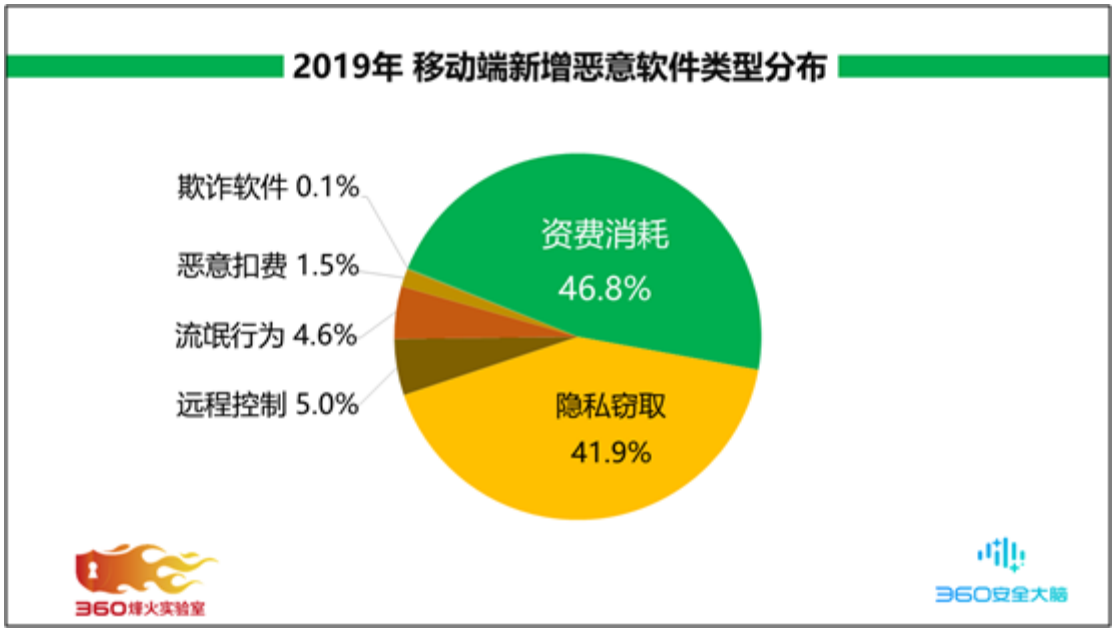
2019 年全年，360 安全大脑共截获移动端新增恶意软件样本约 180.9 万个，环比 2018 年（434.2 万个）下降了 58.3%，平均每天截获新增手机恶意软件样本约 0.5 万个。自 2015 年起，恶意软件新增样本呈逐年下降趋势。下图给出了 2012 年-2019 年移动端新增恶意软件样本量统计：



纵观 2019 年全年恶意样本增长情况，在 1 月与 12 月出现新增样本量峰值，其余月份新增样本趋势较平稳。观察新增样本类型，主要体现在恶意扣费、资费消耗、隐私窃取。由于春节假期前后，大众的社交娱乐活动增多，棋牌游戏、抢红包已成为大众假期娱乐必选项。不法分子正是利用这一敏感时间段，大肆传播恶意软件，实现不良获利。具体分布如下图所示：

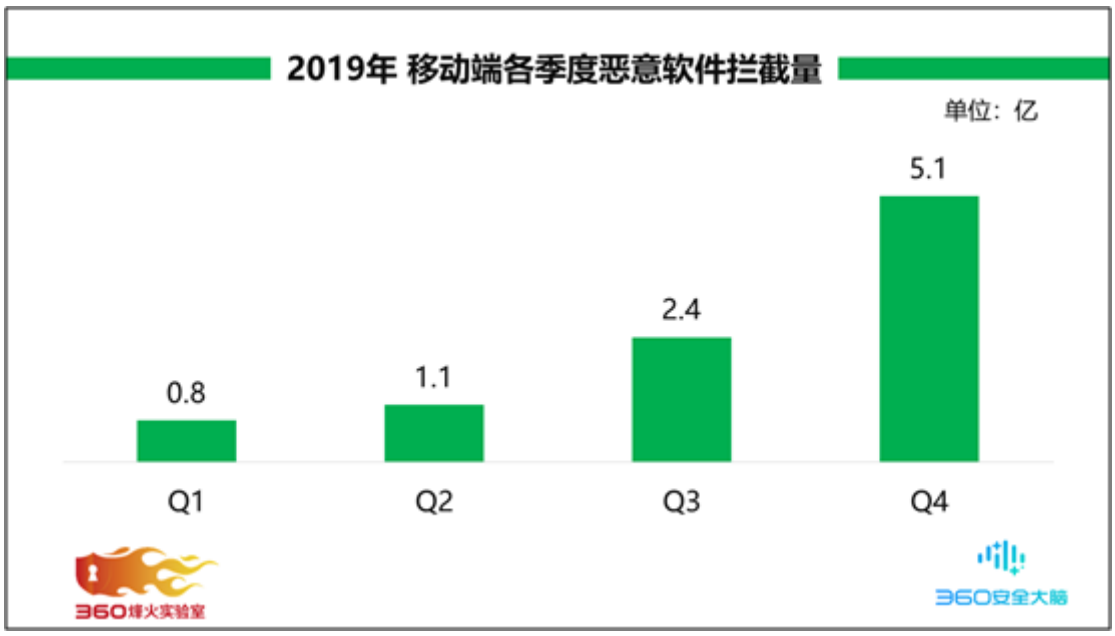


2019 年全年移动端新增恶意软件类型主要为资费消耗，占比 46.8%；其次为隐私窃取（41.9%）、远程控制（5.0%）、流氓行为（4.6%）、恶意扣费（1.5%）、欺诈软件（0.1%）。



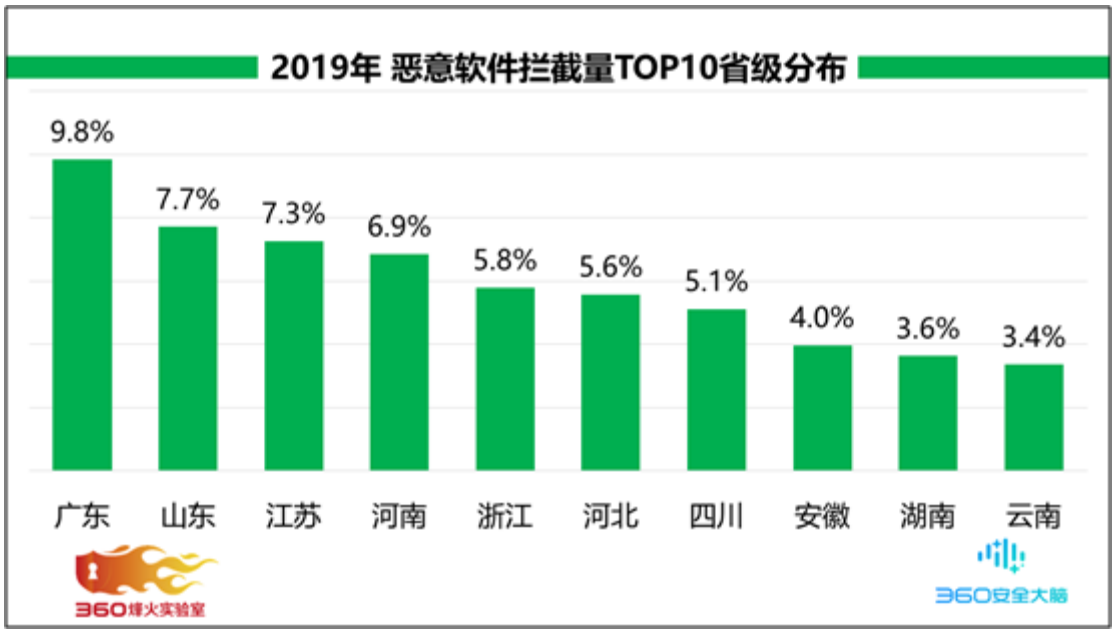
二、 恶意软件拦截量分析

2019 年全年，360 安全大脑累计为全国手机用户拦截恶意软件攻击约 9.5 亿次，平均每天拦截手机恶意软件攻击约 259.2 万次。通过统计 2019 年 Q4 季度样本数量 TOP500 的恶意软件发现，赌博棋牌与色情视频类软件呈现增长态势，致使拦截量直线上升。下图给出了 2019 年移动端各季度恶意软件拦截量统计：

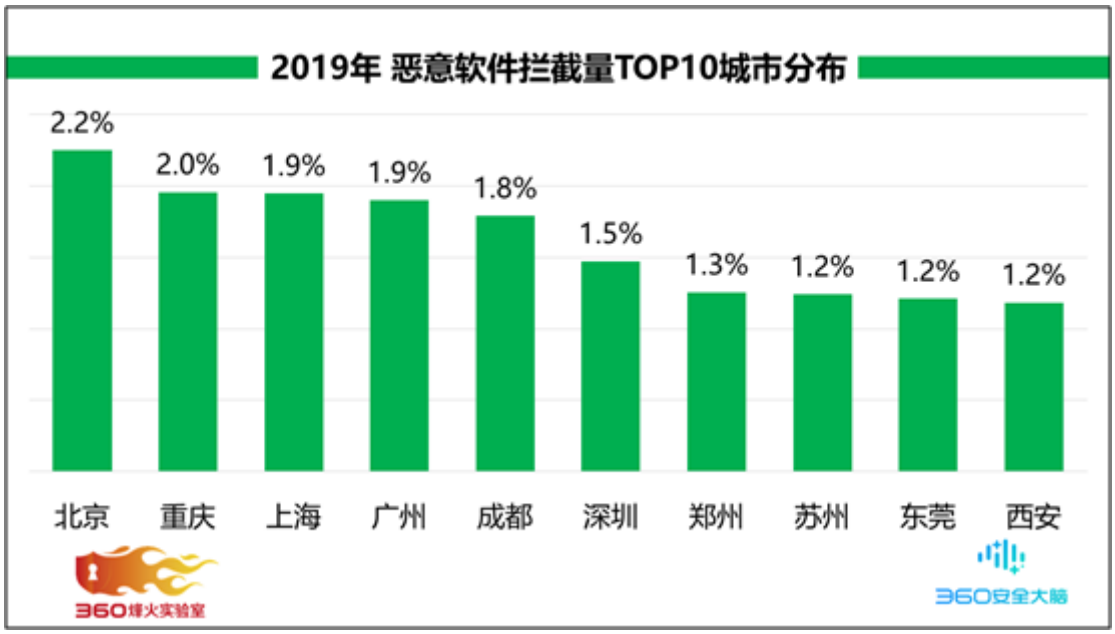


三、 恶意软件拦截量地域分析

2019 年全年，从省级分布来看，遭受手机恶意软件攻击最多的地区为广东省，占全国拦截量的 9.8%；其次为山东（7.7%）、江苏（7.3%）、河南（6.9%）、浙江（5.8%），此外河北、四川、安徽、湖南、云南的恶意软件拦截量也排在前列。



从城市分布来看，遭受手机恶意软件攻击最多的城市为北京市，占全国拦截量的 2.2%；其次为重庆（2.0%）、上海（1.9%）、广州（1.9%）、成都（1.8%），此外深圳、郑州、苏州、东莞、西安的恶意软件拦截量也排在前列。



第二章 多个领域遭受移动恶意软件攻击现状

据中国互联网信息中心发布的第 44 次《中国互联网发展状况统计报告》报告统计，截止 2019 年 6 月，我国移动互联网网民数量突破 8.47 亿，占我国网民总数量的 99.2%[1]。金融服务、生活服务以及社交娱乐等全面面向移动互联网迁移。一方面这些行业领域给我们带来了生活的便利，物质和精神需求的满足；另一方面这些行业也遭受到移动恶意软件的攻击，不仅侵害了移动用户的合法利益，同时破坏了正常的行业领域发展。

2019 年移动金融行业、移动流量产业和移动社交领域均遭受了移动恶意软件的攻击。对移动金融行业的攻击，主要表现为窃取大量银行账号密码信息，这类

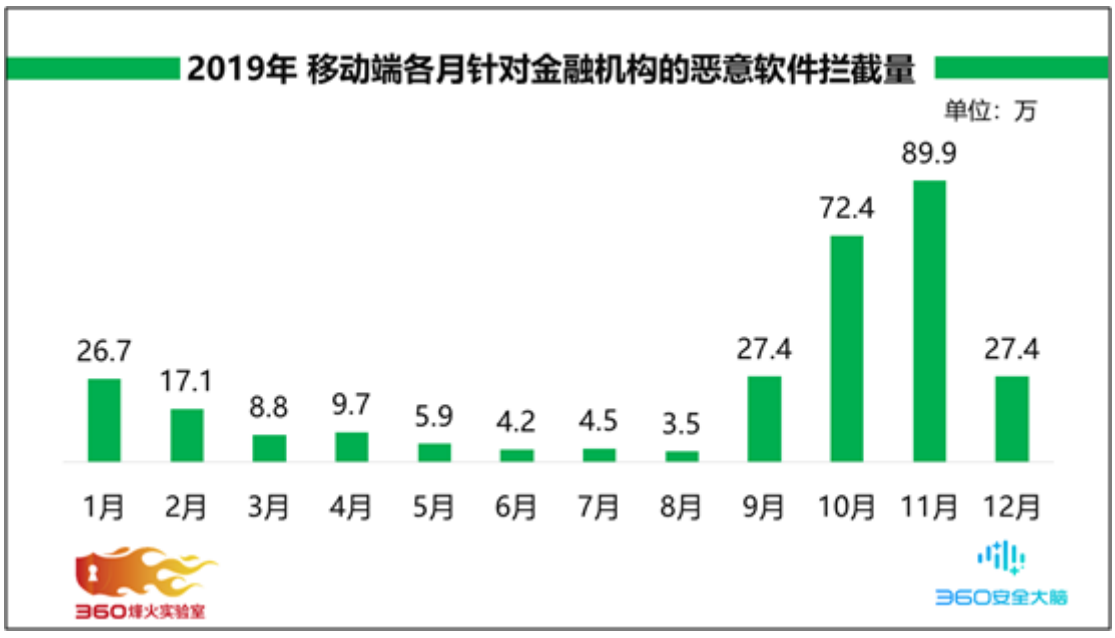
事件大多针对国外银行；而在国内，大量冒充以及虚假金融借贷服务，其本身并无真实借贷业务，仅用于骗取用户隐私和钱财；对移动流量产业的攻击，表现为移动广告商使用不同的欺诈技术获得广告主的报酬；对移动社交领域的攻击，则是利用揣摩特殊人群心里需求特点，使用虚假身份在社交过程中推送虚假信息，诱导充值进行诈骗。

一、 针对移动金融行业攻击

(一) 全球金融机构遭受移动钓鱼攻击

有数据显示 2019 年第三季度，43.19%的网络钓鱼攻击针对在线金融机构，包括银行、在线商城及电子支付系统[2]。

从移动端平台看，2019 年 360 安全大脑拦截针对金融机构的钓鱼类银行恶意软件近 300 万次，月均拦截 25 万次。从全年拦截次数看，其中 6 月至 8 月拦截量最低月均约 4 万次，10 月和 11 月拦截量最高月均 81 万次，呈现年中低，年末高的活跃趋势。究其原因，我们认为是与年末银行等金融机构为了达成年度商业目标，揽储等活动更加频繁有关，从而针对移动金融机构攻击也出现强势增长。

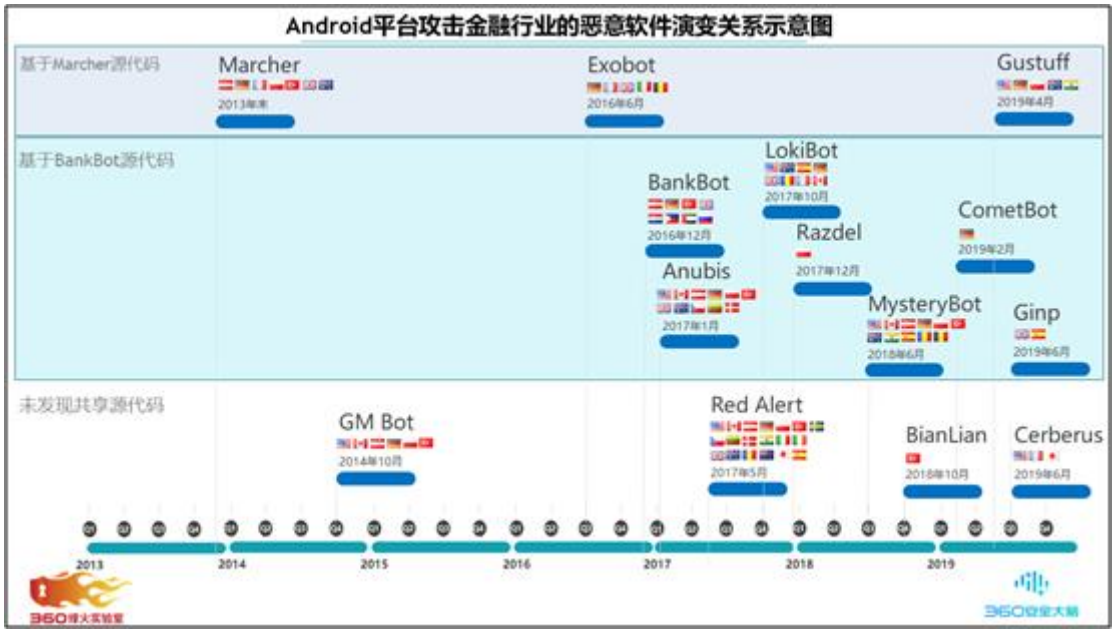


在 2019 年，遭受移动钓鱼攻击的金融机构所在国家主要有美国，加拿大，奥地利，德国，法国，波兰，土耳其，英国，澳大利亚，捷克，丹麦，立陶宛，印度，意大利，爱尔兰，日本，西班牙，罗马尼亚，瑞典，新西兰，巴西，比利时，俄罗斯等等，集中在西亚、欧洲、北美和澳洲。

(二) 国外金融账户信息遭受持续攻击

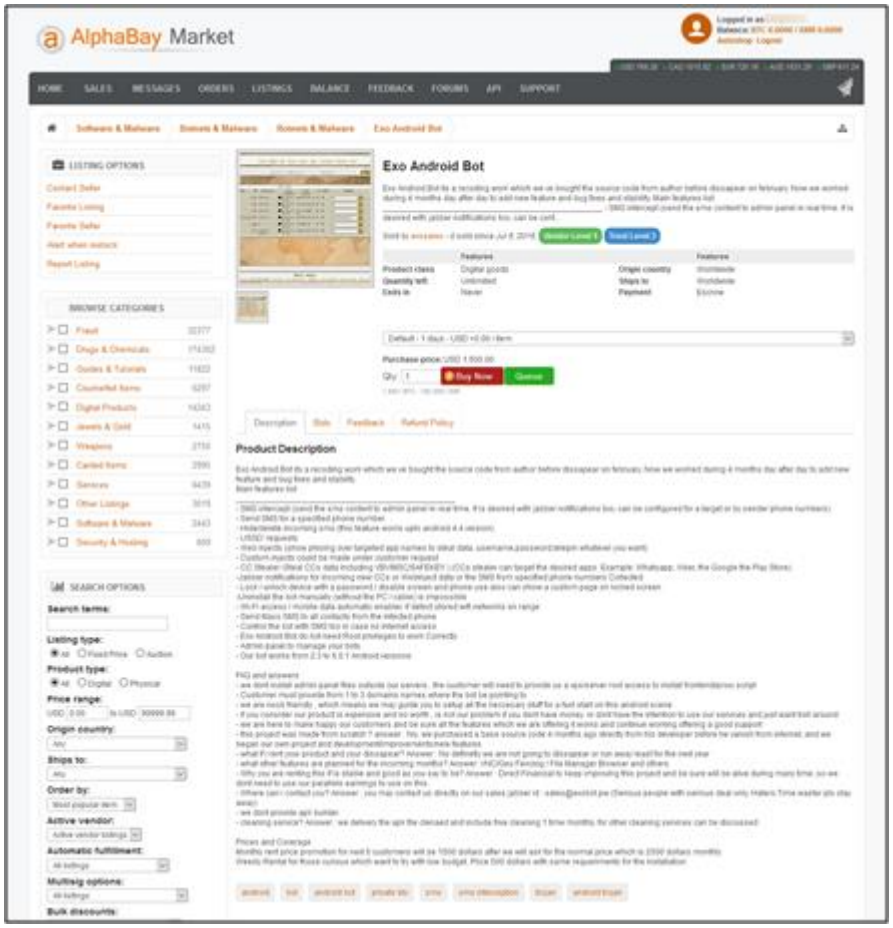
由于国内外金融行业发展以及支付习惯的差异，恶意软件作者通常会精心伪造国外银行页面，有针对性的对全球指定的金融机构进行网络钓鱼，以获取银行客户的账户信息，最终从银行账户中窃取金钱。

根据 360 安全大脑所监测到的信息，对攻击国外金融机构的钓鱼类银行恶意软件家族进行了梳理，由于这类家族数量众多且各个厂商的命名不同，在此我们仅列举出一些有影响力的恶意家族来说明各个家族之间的演变关系及特点。



Marcher 于 2013 年底首次出现。该恶意家族最初窃取俄罗斯用户的 Google Play 凭据和支付卡数据。2014 年 3 月，采用相同策略的新版本已发展成为银行类恶意家族，并且以德国的金融机构为主要目标，并且此后攻击者将攻击的金融机构清单不断扩大。截至 2016 年 5 月，Marcher 已经针对包括英国，德国，奥地利，波兰，法国，澳大利亚和土耳其银行。基于 Marcher 源代码派生出新的恶意软件变种 Exobot 和 Gustuff。

Exobot 最早出现在 2016 年 6 月，其最初是基于 Marcher 恶意家族源代码，是 Marcher 恶意家族的一种变种，同样具有窃取银行凭据的恶意行为。2017 年 5 月 ExoBot2.0 版的发布并且通过官网销售。2018 年 1 月 Exobot 作者在网络犯罪地下论坛称其退出并出售 Exobot 源代码，2018 年 5 月，ExoBot 的源代码泄漏。下图为 Exobot 在网络犯罪地下论坛出售的页面：



BankBot 最早出现在 2016 年 12 月俄语的网络犯罪地下论坛，在 2017 年 1 月被安全厂商捕获并命名为 BankBot，此后 BankBot 成为了共享源代码派生的银行类恶意家族通用名称。基于 BankBot 源代码派生的新的恶意家族有 Anubis、LokiBot、Razdel、MysteryBot 和 CometBot 等。

其中以 Anubis 最为流行，Anubis 源于 2016 年 12 月俄语的网络犯罪地下论坛名为 maza-in 的用户 ID 制作的银行恶意软件源代码改进而来。主要目标是从受害者的设备中窃取银行凭据。它通常冒充 Flash Player 更新软件，Android 系统工具或其他合法应用软件。Anubis 通常由下载器和有效载荷两部分组成，目前很多恶意家族仍然在使用 Anubis 的下载器进行自我保护和伪装。maza-in 于 2018 年 12 月宣布发布 Anubis 2.5 版本，但是有人质疑新版本只是重新设计了后端 Web 界面，并没有重写整个代码。2019 年 1 月 Anubis 源代码在一个地下论坛中泄露。2019 年 3 月已经停止支持和更新。截止 2019 年 3 月 Anubis 针对来自 100 多个不同国家/地区的约 370 个金融机构的应用软件，主要活跃

在欧洲，西亚，北美和澳大利亚。下图为 maza-in 在俄语的网络犯罪地下论坛中的发布的帖子：

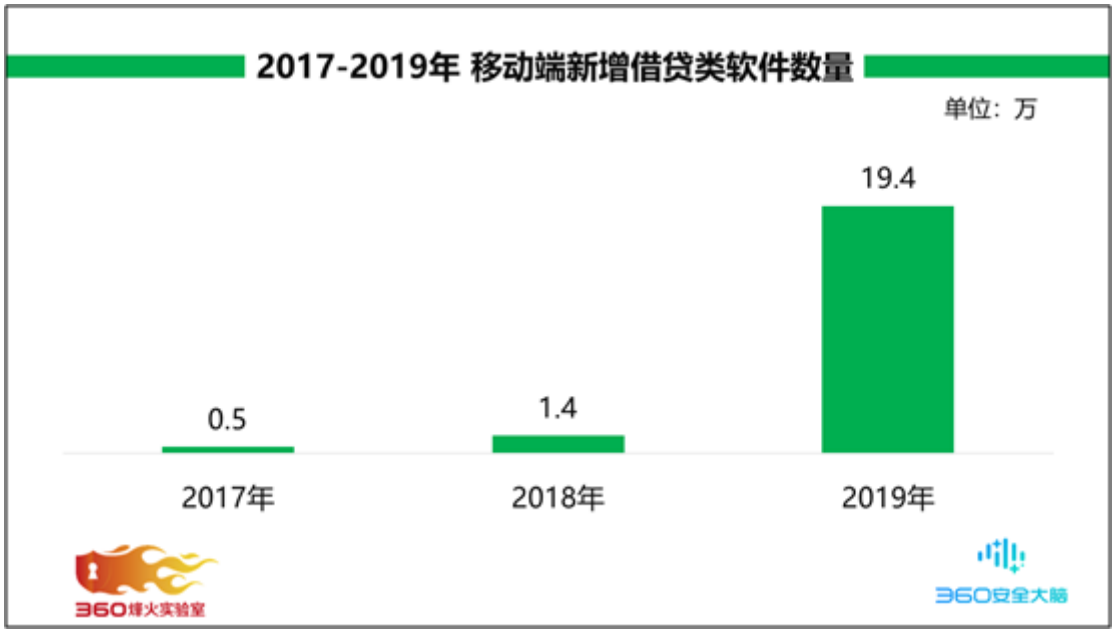
以上这些攻击金融机构的恶意软件家族都具备一些显著的特点，首先都是从网络犯罪地下论坛以租售的形式开始传播，增加了自身的隐蔽性。其次，在这些恶意软件源码遭到泄露后，在接下来的时间里立马会出现新的恶意软件家族，新的恶意软件作者起初会根据泄漏的代码构建自己的恶意软件版本或者变种。最后，会基于泄露的代码进行功能上的改进，比如引入了勒索功能、代理功能及键盘记录等。另外，在 2019 年最新发现的银行类恶意家族如 Cerberus 和 Ginp，也都符合这一特点，它们目前仍然处在积极开发中。

(三) 国内仿冒金融借贷诈骗屡见不鲜

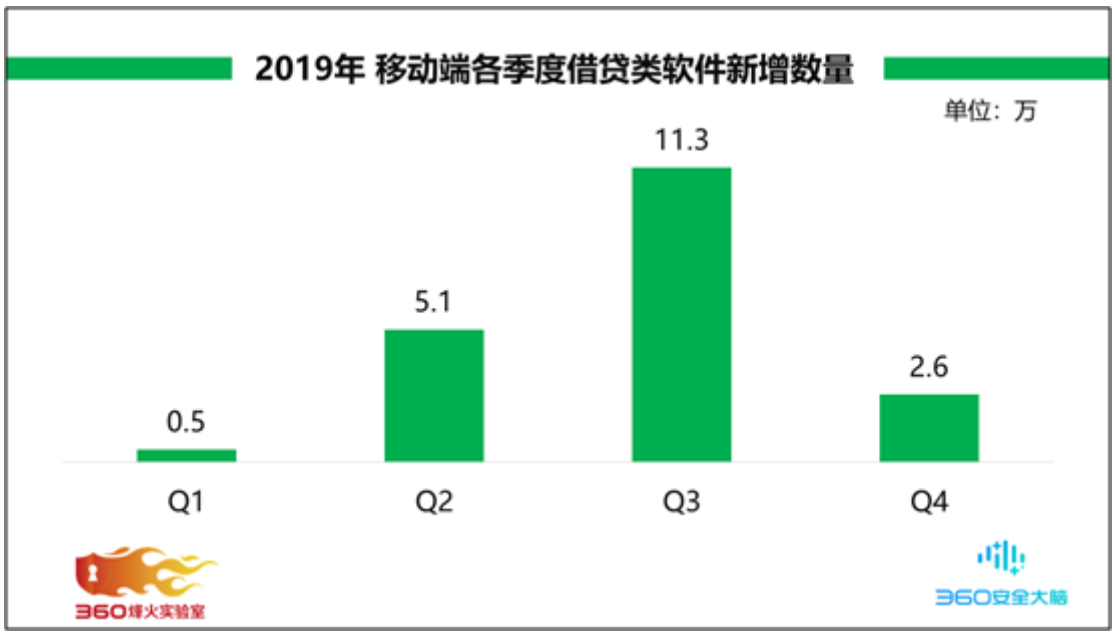
我们调查发现，针对移动金融行业的攻击，国内与国外有明显的不同，国外主要遭受恶意软件的钓鱼攻击，而国内则是通过仿冒金融借贷类应用软件，以短信、网页广告和社交网络等形式广撒网，通过放款前收取工本费、解冻费、保

证金、担保金等名目诈骗用户钱财，不仅给借贷人带来财产损失，还损害了正规金融机构的借贷服务的口碑。

2019 年，360 安全大脑共发现金融借贷类应用软件约 19.4 万个。全年新增借贷类应用软件相比 2017 年（约 0.5 万个）增长了约 37.8 倍。相比 2018 年（约 1.4 万个）增长了约 12.9 倍，呈现爆发式增长。



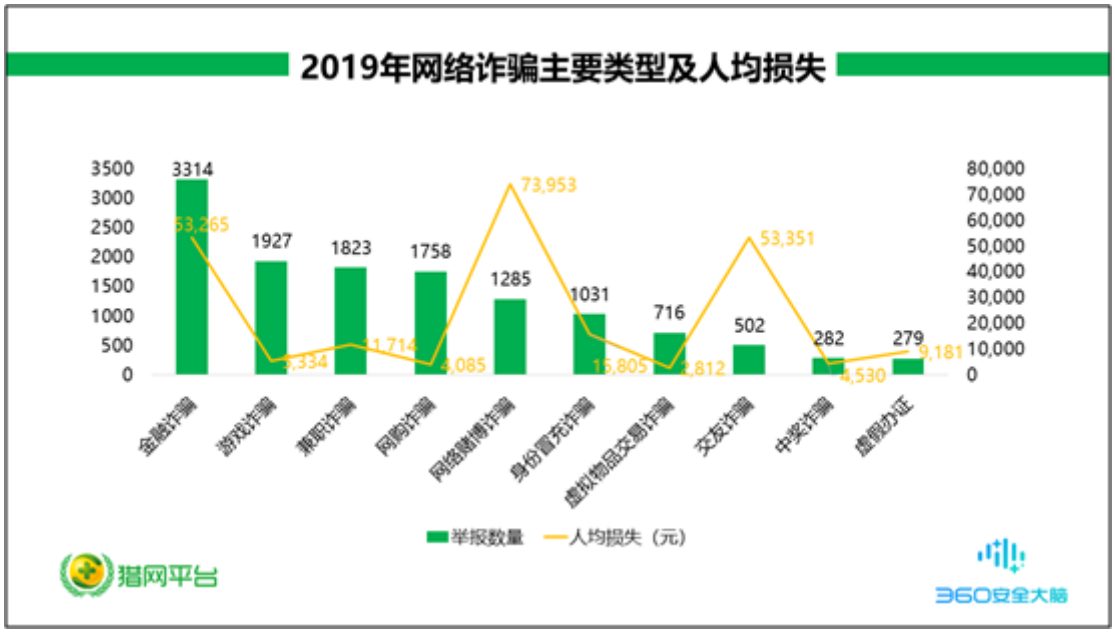
从每月新增借贷类应用软件数据看，第一季度最低约 0.5 万个，第三季度最高约 11.3 万个，第一季度到第三季度呈现增长趋势，然而第四季度出现大幅下降仅约 2.6 万个。究其原因，我们注意到 2019 年 10 月，央行下发《个人金融信息（数据）保护试行办法（初稿）》征求意见（以下简称《办法》），重点涉及完善征信机制体制建设，将对金融机构与第三方之间征信业务活动等进一步作出明确规定，加大对违规采集、使用个人征信信息的惩处力度。这一《办法》对一些违法违规的借贷类应用软件得到有效治理，从而影响到第四季度的新增借贷类应用软件数量。



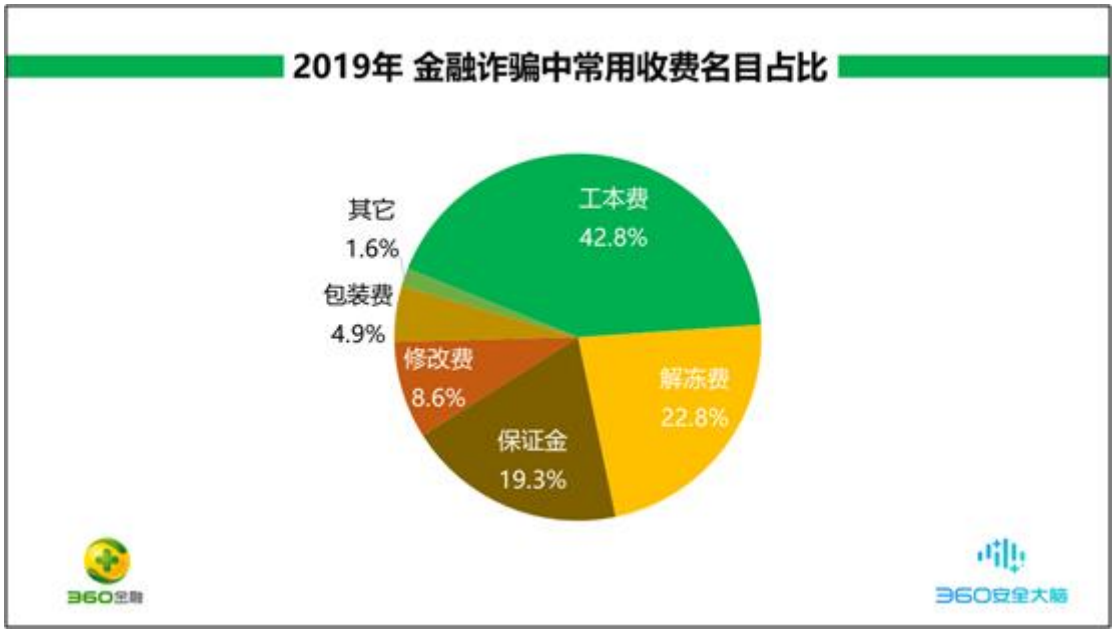
随着金融借贷类应用软件快速增长，出现了大量仿冒金融借贷类的应用软件，这些仿冒的软件并无真实借贷业务，不仅骗取借贷人钱财，而且部分仿冒金融借贷类要求借贷人提交姓名、身份证照片、个人资产证明、银行账户、家庭住址等骗取用户隐私信息。

2019 年猎网平台发布的网络诈骗趋势研究报告显示，金融诈骗是举报量最高的诈骗，高达 3314 例。其次为游戏诈骗举报量 1927 例，兼职诈骗 1823 例。

从人均损失上看，人均损失最高的诈骗为博彩诈骗，人均损失高达 73953 元。其次为交友诈骗人均损失 53351 元；金融诈骗人均损失 53265 元，是人均损失第三高的诈骗类型。



在对金融借贷软件诈骗骗术和接触渠道的研究方面，根据 360 金融反诈实验室联合 360 手机卫士发布的报告显示，放款前收费是金融诈骗团伙常用的骗术，金融诈骗常用的收费名目如下



数据显示，借贷人接触仿冒金融借贷类应用软件渠道占比，电话（52.1%），短信（24.6%），微信（7.0%），搜索（5.6%），QQ（5.6%），网址

（1.4%），其他（3.5%）,有超过一半的受害者通过电话渠道接触仿冒的金融借贷类应用软件。

通过对大量用户举报的金融借贷诈骗案例中发现，第三方分发平台是这些仿冒金融借贷类的应用软件的主要传播源，主要原因是这些第三方分发平台对于分发软件审核不严，造成了这些仿冒的应用软件大肆泛滥，下图所示是第三方分发平台分发的仿冒的金融借贷类应用软件：

除了第三方分发平台，2019 年我们研究发现仿冒金融借贷类应用软件的一个新分发渠道，其依靠服务器指令替换软件内容，应用市场中的软件介绍与实际运行内容不符，从而绕过应用市场审核， 应用市场成为仿冒金融借贷类应用软件的传播新渠道[3]。值得注意的是，在金融借贷诈骗的大量举报案例中，一些诈骗分子通过假冒知名金融借贷类应用软件的形式实施诈骗，更容易骗取用户信任实施诈骗，大大提高了诈骗成功的可能，损害了正规金融借贷服务行业的形象。

二、 针对移动流量产业攻击

(一) 流量是企业商业模式的基因

流量是互联网尤其是移动互联网商业模式的重中之重，流量的获取和分发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。企业变现的核心在于流量转化，基于流量转化的商业模式可以决定一个企业的成败。然而，流量转化离不开广告营销公司，它们能够通过广告投放帮助企业建立品牌形象，从而建立自己的产品或服务矩阵。

一般而言，广告投放过程包含这样几个环节：

第一步，广告主选择投放哪种广告，常见的形式包括 SEM、DSP、信息流、开屏广告等；

第二步，确认广告的付费形式，常见的广告付费形式有 CPM、CPC、CPA、CPS 为主要的结算方式，分别按照展示量、点击量、 转化量、销售额结算；

第三步，跟踪广告的投放数据，常见的投放数据有展现量、点击量、点击率、消费、下载量、成功注册量等。

一方面由于广告服务商在广告投放过程中存在各级代理，各种渠道流量获取的透明度不高；另一方面广告主一般会制定点击率、点击成本、互动率、转化成本等各种各样得指标，多方面因素催生了流量作弊黑灰产业。

(二) 流量的评判性催生虚假流量

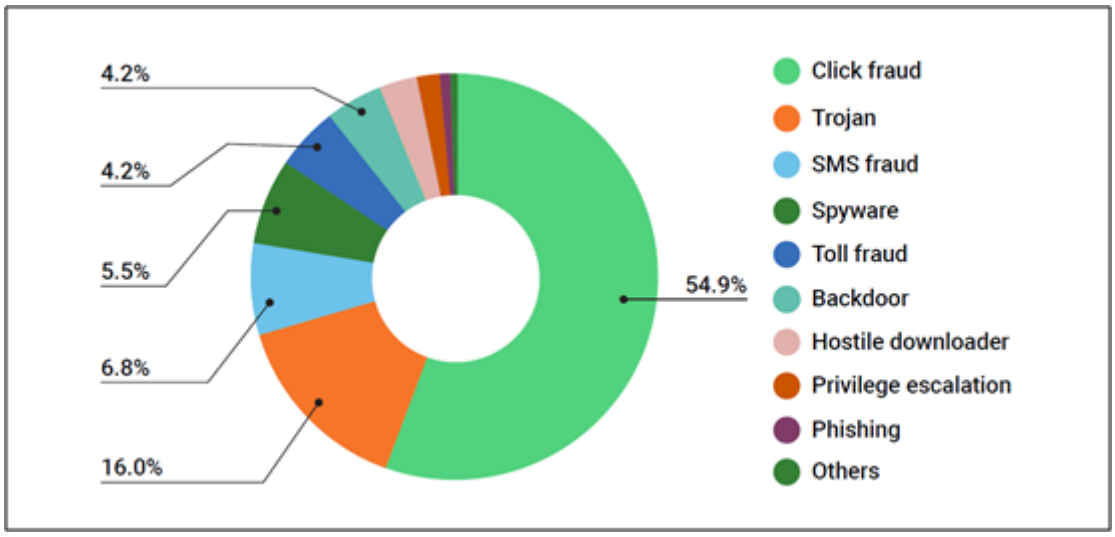
企业在追求商业利益的背景下，不断强调“流量变现”“流量即王道”，流量的重要性在移动互联网中得到了进一步的放大。比如购物网站中对商品的评价，文章的阅读量，视频的播放量都是依靠流量来判定产品、文章、视频的质量，流量的评判性成为消费者决策的重要依据。

数据显示，2019 年第三季度，全球超过四分之一（26%）的 Android 系统应用软件内广告包含欺诈性质的虚假流量内容，其中在中国注册的应用软件内程序化广告的虚假流量率最高为 33%[4]。

流量的评判性催生虚假流量，不论是在电商、支付平台、还是 O2O、自媒体、广告等行业，都有着它的身影。不同行业的流量作弊形式不同，移动端常见刷量方式已经被我们多次曝光，比如感染恶意软件实现刷量、脚本代替人模拟点击、篡改 API 执行结果以及破解 SDK 代码等等。

(三) 移动广告流量欺诈手段剖析

2019 年 3 月，Google 发布的 2018 年 Android 安全报告显示，点击欺诈应用软件占 PHA 总安装率的 54.9%[5]，如下图所示：



2019 年我们发现移动广告欺诈手段更加激进和复杂，采取多种手段规避检测，例如代码被大量混淆，使用自定义加密算法，伪装成流行的浏览器图标诱导点击，注册为前台服务保持活动状态，延长触发时间，检测 Google 沙箱 IP，在打开最近的屏幕设置标题和图标不可见，以及仿冒知名应用进行嫁祸等多种手段。

常见的移动广告欺诈主要有模拟点击、点击劫持、移动设备劫持、移动设备仿真和 IP 地址仿真等多种形式。

模拟点击是使用受恶意软件感染的设备进行虚假访问和广告点击。欺诈者使用各种技巧来绕过广告商的监测技术。经过特殊设计的恶意软件可以使用延迟触发和模拟人点击来更好地模拟真实的人类点击广告。通常，广告商是点击欺诈的主要受害者，但一些犯罪分子也会采用该技术来针对使用设备用户，这可能包括订阅付费服务。

2019 年 10 月，Ai.type 键盘应用软件中发现可疑移动交易记录，在用户未知的情况下私自模拟点击行为，进行广告刷量和订阅付费服务操作[6]。该软件嵌入看似正常的 SDK，但是包含了应用开发者可能不知道的行为和功能。该 SDK 功能将设备连接到广告分发平台，使用 JavaScript 下载广告并在未经用户同意的情况下执行自动点击操作。

点击劫持是用户点击有意义或看上去真实的按钮、链接的地方，但实际上，他们单击的是隐藏在网页上不可见元素中的链接。欺诈者必须在浏览器和移动操作系统开发方面保持技术领先，才能不断寻找隐藏元素而不被阻止或泄露的新方法。他们还使用精心设计的文字和图像来诱使用户单击页面的特定部分。欺诈者还利用点击可能会将其重定向到令人迷惑的网页载满广告的网站并向广告商索取收入，或是吸引或诱使他们进行付费服务订阅，或者他们可能只是使用不可见的链接来触发恶意软件下载。

移动设备劫持是欺诈者将恶意软件植入手机。这可以包括伪装或加密应用软件中的代码，以使它们在进入正式的 Google Play 商店之前可以逃避安全检查。让看起来无辜的应用软件秘密下载并安装其他造成实际损害的应用软件。该恶意软件反复加载广告，从而使欺诈者从广告商那里获取分成。

移动设备仿真主要分为机器作弊和人工作弊，机器作弊主要使用群控系统，通常通过改机工具冒充特定的手机或平板电脑型号，从而使流量显示来自移动设备。机器作弊成本较低，离不开代码程序，但这类型流量容易被监测到；人工作弊即通过雇佣、激励的方式雇佣大批人员去生成的流量，这类作弊带来的虚假流量较难屏蔽，但成本相对较高。

IP 地址仿真主要涉及使用各种技术来更改报告的 IP 地址发出请求，例如点击次数和广告展示次数。这可以用来使假定的人类用户看起来在一个利润更高的市场中，但是通常这样做是为了避免从同一 IP 地址报告过多的虚假点击并引起怀疑。

三、 针对移动社交领域攻击

中国移动社交市场格局虽然稳定，却不乏竞争。当下社交呈现较强的刚需特征，市场空间巨大，与此同时新技术、新形式、新需求等多重因素的叠加让后来者看到希望，因此互联网势力纷纷推出新型社交产品试图瓜分变革红利。

2019 年初，以多闪、马桶 MT、聊天宝为代表的新型社交产品率先吹响移动社交市场冲锋号，但效果平平，后续又有多款新型产品相继上线，持续搅动移动社交市场战争。

在中国移动互联网加速渗透的过程中，移动社交用户也出现了大规模增长。有数据显示，2019 年中国移动社交用户规模为 7.77 亿，预计 2020 年有望突破 8 亿人[7]。其中，中国陌生人社交用户预计增至 6.22 亿人[8]。

(一) 借社交名义频繁触碰监管底线

2019 年第一季度，多款陌生人社交应用软件先后被分发渠道以及监管部门封杀和勒令关停，涉事原因多为应用软件内出现涉黄内容，行业风气整顿刻不容缓。

2019 年 2 月，音遇、Hello 语音、微光等语音社交类应用软件遭到了苹果应用商店的下架[9]。

2019 年 4 月，音遇由于涉黄和大面积出现不发分子的广告，而遭到全网的下架[10]。

2019 年 4 月，国家网信办启动小众即时通信工具专项整治，比邻、聊聊、密语、等 9 款陌生人社交应用软件因为涉嫌淫秽色情而被国家网信办关停[11]。

2019 年 4 月 16 日，探探出现在国家网信办启动的小众即时通信工具专项整治榜单中。4 月 28 日，业内人士普遍认为探探由于涉嫌传播淫秽色情等违法违规信息，在安卓应用市场遭遇下架；5 月 1 日，探探亦被苹果应用商店下架[12]。

(二) 同城交友陪聊美女多为虚假用户

从数据看似移动社交领域一片繁荣商机潜力无限，实则不然，大量的同城交友类应用软件中充斥着的桃色陷阱和内幕，很多陪聊的美女都是虚假用户。这类交友应用，通常起的名字大多很直白，比如：夜约、成人约爱、同城陌陌约、缘分、激情约爱、同城单身约、闪约等。让人看到名称怦然心动，立马下载安装。安装过后，不需要注册选一下性别位置就可以了。进入后，不一会就可以得到一大堆的美女等你来搭讪，真是让人激动万分。

我们以一款名为“约聊”的应用软件为例，注册之后会在短时间收到很多陌生美女头像向你打招呼的消息，当回复第一条聊天信息之后，第二条聊天信息需要充值付费，价格显示 69 元一个月，138 元六个月以及 139 元终身，并且下方还提示其他用户充值消费的信息，但购买之后，原先热情发来招呼的美女们全部噤声，与之前的热情主动判若两人，不管发出多少消息都得不到回复。

另外，我们还尝试在不同地点进行注册登录，发现这些陌生陪聊美女的话术一模一样，由此可见这个软件所谓的同城交友，实际上都是骗局，陪聊美女都是程序控制的虚假用户，她们的头像，相册均来自网络。这些聊天机器人自动发

送文字、语音信息搭讪新注册及在线用户，然后引诱用户充值陷入骗局。这类应用的开发成本很低，甚至可以直接购买然后换个应用名，换个启动时的开屏图片，进而开始大肆骗钱。

目前 5G、人工智能、VR 等技术的发展与变迁让声音、图片、视频等新型社交方式加快落地。社交需求呈现出新变化，在行业变革的重要窗口期，这类软件真假难辨，取证也是困难重重，给移动社交领域的良性发展带来不利影响。

第三章 第五维空间面临的高级威胁和挑战

随着信息和网络技术的飞速发展，互联网已渗透到人类生活的方方面面，并对国家安全、军事斗争以及战争形态产生了重大而深远的影响，网络空间已成为与陆、海、空、天并列的第五维空间领域。

第五维空间作为网络空间，是连接其他四维空间的纽带，第五维空间的优劣势将决定在其它物理维空间的优劣势，将成为多维作战空间争夺的关键领域，第五维空间的力量也将成为主导全维作战行动的重要力量。

一、 第五维空间安全将成为各国政治、经济、军事安全的重大挑战

军事战近忧，网络战远忧。作为不分军民的网络战争，攻击发起者早已从业余团队演进成具有国家背景的黑客组织和网络部队。在全域交织渗透的同时，数以百亿计的物联网设备、新技术、芯片、云端都会成为攻击的切入点，漏洞无处不在。近年来漏洞问题带来的第五维空间安全问题与国家政治、经济、军事等紧密相关, 国内与国外对于漏洞的管控政策相继出台。

在网络安全漏洞的披露方面[13]，美国制定了各种法律并结合政策手段加以规范。2001 年出台的《爱国者法案》、《2002 年关键基础设施信息法》及 2013 年发布的《提高关键基础设施的网络安全》鼓励个人和组织向政府披露漏洞信息，以减少网络入侵事件，提高网络安全的信息共享并为用户营造可信赖的网络环境。美国国防部 2004 年 1 月发布的漏洞披露政策，允许自由安全研究人员通过合法途径披露国防部公众系统存在的任何漏洞。2017 年 7 月，美国司法部犯罪科网络安全部门发布《在线系统漏洞披露计划框架》，帮助组织机构制定正规的漏洞披露计划。美国已从政策、立法和程序上，构建了国家层面统一的网络安全漏洞披露协调和决策机制。

2019 年 11 月，为有效落实我国《网络安全法》，确保信息发布有利于防范网络安全威胁和风险，推动政企机构和公众了解威胁和风险并进行处置响应，同时又要避免不当发布引发消极后果。国家网信办发布《网络安全威胁信息发布管理办法（征求意见稿）》（以下简称《办法》）[14]。《办法》对发布涉及计算机病毒、网络攻击、网络侵入、网络安全事件等可能威胁网络正常运行活动的相关安全威胁信息，以及包括系统漏洞、网络风险等在内的可能暴露网络脆弱性的安全威胁信息，从发布内容、发布流程、发布方法等方面，对研究机构、网络安全厂商、个人研究者，以及信息发布平台运营单位做出了较为具体的规范。

随着网络争端的络续，网络战已成为国与国对抗的核心战场。人类已经迈向网络战时代，网络战争时刻都在发生。没有网络安全，就没有国家安全。

(一) 严峻的系统环境

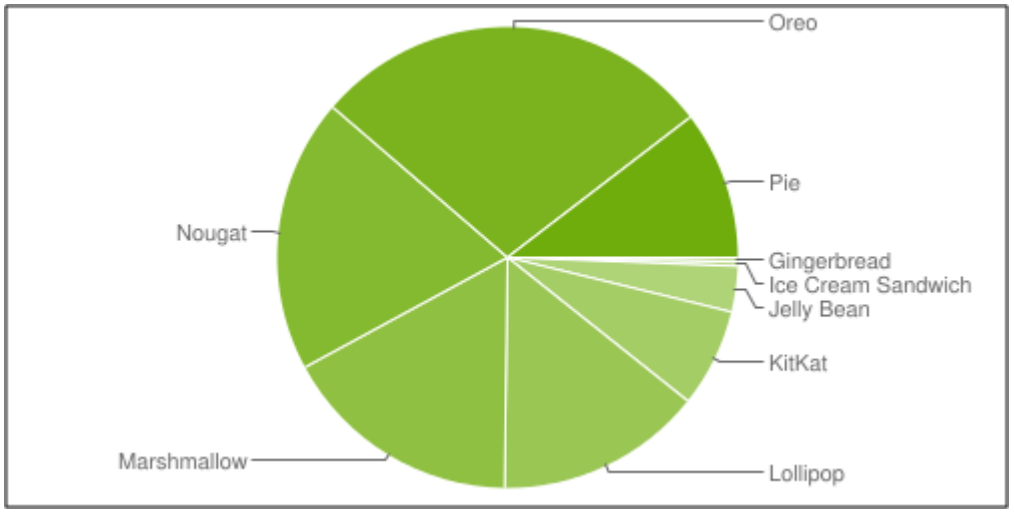
Android 系统开源就意味着在安全问题上显得更加透明，运用工具审查安全漏洞变得更容易。根据汇总 CVE 数据的网站出具的 2019 年度 CVE Details 报告显示[15]，Android 系统以 414 个漏洞位居产品漏洞数量榜首，虽然与 2018 年 611 个相比下降 32.2%有所减小，但是仍然处在漏洞榜前列。

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Android	Google	OS	414
2	Debian Linux	Debian	OS	360
3	Windows Server 2016	Microsoft	OS	357
4	Windows 10	Microsoft	OS	357
5	Windows Server 2019	Microsoft	OS	351
6	Acrobat Reader Dc	Adobe	Application	342
7	Acrobat Dc	Adobe	Application	342
8	Cpanel	Cpanel	Application	321
9	Windows 7	Microsoft	OS	250
10	Windows Server 2008	Microsoft	OS	248

(二) 系统更新情况

从 Android 系统更新情况看，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。

截至 2019 年 5 月，Google 发布的 Android 系统版本分布统计[16]，Android Oreo（Android 8.0/8.1）达到 28.3%，占比第二的是 Android Nougat（Android 7.0/7.1）总占比已达 19.2%，自 2019 年 5 月起谷歌就未再更新过这份数据，所以最新版本 Android 10 占比还仍然未知。



综合上述对 Android 系统环境的介绍，我们可以看出仍然存在大量未升级至新版本系统正在被使用，这些与安全更新脱节的现象直接导致用户手机暴露于各种漏洞的威胁之下，可造成用户的隐私、财产安全。

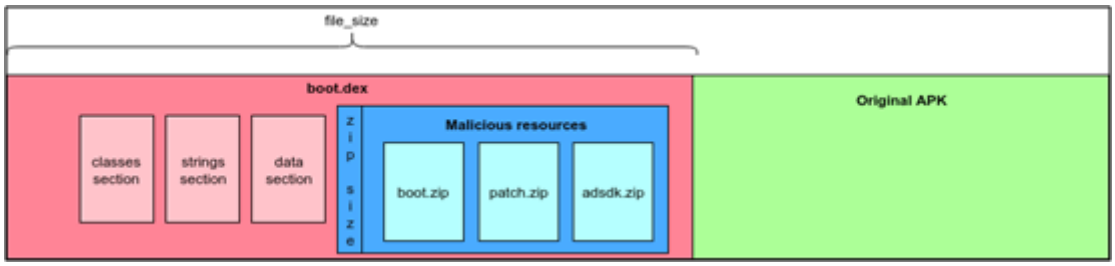
(三) 漏洞利用情况

2019 年开始不断曝出 Android 漏洞在现实环境中被恶意软件利用，其中比较有代表性 Janus 漏洞（CVE-2017-13156）[17]和 Strandhogg 漏洞[18]。

Janus 漏洞（CVE-2017-13156），可以让攻击者向任何 APK 中插入代码，绕过 Android 系统的签名校验机制，直接安装到 Android 系统中，如果作为其他应用软件的更新包安装，可以继承该应用软件的所有权限，对应用软件进行完全控制。如果被控制的应用软件是一个具有很高权限的应用软件，比如系统应用，甚至可以完全接管系统。该漏洞影响使用 JAR 签名方案（v1 方案）签名的应用软件，不影响 APK 签名方案 v2 签名的应用软件。

2019 年 7 月，国外安全公司发现 Agent Smith 恶意软件家族[19]，Agent Smith 伪装成与 Google 相关的应用软件，恶意软件的核心部分利用各种已知的 Android 漏洞，并自动将设备上已安装的应用软件替换为恶意版本，而无需用户干预，感染了大约 2500 万个设备。

Agent Smith 在核心模块中使用一系列 Bundle 漏洞，用于在受害者不知情的情况下安装应用软件。使用 Janus 漏洞（CVE-2017-13156），使攻击者可以用受感染的版本替换任何正常的应用软件。使用 SHAREit 和 Xender 的 Man-in-the-Disk 漏洞来安装恶意更新。



Strandhogg 最早在 2015 年 USENIX 安全研讨会上发布了此漏洞。是一个存在于 Android 多任务系统中的应用漏洞。该漏洞利用则是基于一个名为“taskAffinity”的 Android 控件设置，允许包括恶意应用在内的任意程序，随意采用多任务处理系统中的任何身份。该漏洞影响所有 Android 版本，包括最新的版本 Android 10。

2019 年 12 月，我们发现数十个利用此漏洞的 Bankbot 恶意家族变种，其针对近 20 个国外银行。

二、 第五维空间将成为多维作战空间争夺的关键领域

2019 年 7 月，国务院新闻办公室发布的《新时代的中国国防》[20]指出，网络空间是国家安全和经济社会发展的关键领域。网络安全是全球性挑战，也是中国面临的严峻安全威胁。中国军队加快网络空间力量建设，大力发展网络安全

防御手段，建设与中国国际地位相称、与网络强国相适应的网络空间防护力量，筑牢国家网络边防，及时发现和抵御网络入侵，保障信息网络安全，坚决捍卫国家网络主权、信息安全和社会稳定。

(一) 移动端 APT 全球研究

2019 年，360 烽火实验室监测到的公开披露的 APT 组织活动报告中，涉及移动端相关的 APT 组织活动报告 14 篇。

被提及受到移动 APT 组织攻击的受害者所属国家主要有中国、朝鲜、韩国、印度、巴基斯坦、以色列、叙利亚、伊朗、埃及等东亚、西亚、中东多个国家。

APT 组织活动归根到底其实是利益冲突，从公开披露的移动端 APT 组织活动针对的目标和领域来看，涉及政治、经济、情报等多个重要板块。

(二) 政治目标的刺探

2019 年，移动端以对政治目标刺探为目的 APT 攻击活动，从地理位置上看主要围绕在亚太和中东地区，涉及朝鲜半岛、克什米尔地区、巴以冲突地区、海

湾地区。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。

2019 年围绕朝鲜半岛，国外安全厂商认为来自朝鲜的多个活跃 APT 组织对包括韩国在内的多个亚洲国家进行攻击，攻击目标和领域包括政府、军事、外交、人权、外贸等。

披露时间	组织行动	披露来源	概述
2019.2.4	Lazarus Group（APT-C-26）	McAfee	安全厂商发现伪装成由韩国开发人员开发的交通应用，它能够下载恶意插件、接收控制指令进行远控、伪装 Google 进行钓鱼、搜索用户手机与军事政治有关的文件等[21]。
2019.6.26	黑格莎（Higaisa）	腾讯	安全厂商发现来自朝鲜半岛的一个具有政府背景的黑格莎（Higaisa）APT 攻击组织，常利用节假日、朝鲜国庆等朝鲜重要时间节点来进行钓鱼活动。该攻击组织具有移动端的攻击能力，伪装成韩国检察厅。被攻击的对象还包括跟朝鲜相关的外交实体（如驻各地大使馆官员）、政府官员、人权组织、朝鲜海外居民、贸易往来人员等。目前监测到的受害国家包括中国、朝鲜、日本、尼泊尔、新加坡、俄罗斯、波

披露时间	组织行动	披露来源	概述
			兰、瑞士等。[22]
2019.8.5	ScarCruft（APT-C-28）	ESTsecurity	安全厂商发现 ScarCruft 在 PC 端使用隐写术并且配合移动端进行双平台攻击活动,与 Blackbird 行动使用的代码相似。[23]

2019 年围绕克什米尔地区，国外安全厂商认为来自印度的 APT 组织对中国、巴基斯坦等国家进行攻击，攻击目标和领域包括政府、军工、外交、企业等。

披露时间	组织行动	披露来源	概述
2019.12.19	蔓灵花（APT-C-08）	360 烽火实验室	2016 年 6 月开始，蔓灵花组织开始使用定制木马针对中国和巴基斯坦展开了长期有组织、有计划的攻击活动。根据已有数据，发现该组织在攻击活动中常用的载荷投递方式包括水坑、钓鱼、短信、社交工具，受害者包括中国军工行业人员、中国党政干部、企业客服人员以及其他中国群众，也包括巴基斯坦和印度克什米尔区域群体[24]。

2019 年围绕巴以冲突地区，国外安全厂商认为来自中东的 APT 组织尤为活跃。据披露的信息显示，Operation ViceLeaker 是 2018 年 5 月发现的攻击活动，与当时以色列安全机构宣布哈马斯在以色列士兵的智能手机上安装间谍软件事件可能存在关联。

披露时间	组织行动	披露来源	概述
2019.3.20	双尾蝎（APT-C-23）	Check Point	安全厂商发现双尾蝎（APT-C-23）最新移动端活动，伪装成 Adobe 软件并显示带有政治主题的欺骗性 PDF 文档[25]。
2019.6.26	Operation ViceLeaker	Kaspersky	安全厂商发现针对以色列的攻击活动，首次开发始于 2016 年底，但其主要活动开始于 2017 年底到 2018 年初。同时介绍了，攻击者使用两种方法将恶意代码植入到正常应用中[26]。

2019 年海湾地区局势动荡，国外安全厂商认为来自伊朗的 APT 组织利用短信传播恶意软件下载链接，受攻击国家可能包括土耳其、巴基斯坦、阿富汗。

披露时间	组织行动	披露来源	概述
2019.6.10	MuddyWater	Trend Micro	安全厂商发现 MuddyWater 在移动端的活动，通过向所有联系人发送包含指向该联系人的链接的 SMS 来传播恶意应用恶意 APK。链接指向土耳其的非营利研究机构的合法网站，该网站可能是遭到入侵[27]。

与此同时，美国与伊朗之间的政治紧张持续加剧。据《纽约时报》报道，美国在 2019 年 6 月份，使用网络武器，摧毁了伊朗准军事部门使用的一个关键数

据库，该数据库具备定位油轮及策划袭击的能力。受到该网络攻击的影响，暂时降低了伊朗秘密针对波斯湾航运的控制能力。

2019 年 7 月 18 日，据美联社媒体报道声称，美国纽约疑似遭到网络攻击，三十多个电力控制中心被入侵，最终导致纽约大城市停电 4 个小时，随后美国中情局（CIA）公布调查结果，这场网络攻击疑似来自伊朗革命卫队信息战部队。

2020 年 1 月 3 日，美国对伊朗发动“斩首行动”，美军空袭巴格达机场，伊朗“二号人物”——圣城旅指挥官卡西姆•苏莱曼尼(Qasem Soleimani)遇袭身亡。“斩首行动”背后与美国国家安全局 NSA 长期的网络监控、情报获取能力有着必然的联系。正当就在多名美国官员和安全专家，警告要注意来自伊朗方面发动的网络攻击之时，1 月 4 号美国政府网站和塞拉利昂商业银行网站遭到破坏。

(三) 经济利益的驱使

2019 年移动端高级威胁以经济利益为目的，国外安全厂商认识来自东亚的 APT 组织 Konni，冒充虚拟加密货币交易所向攻击目标发送鱼叉式钓鱼邮件，用于窃取被攻击目标的虚拟货币账户信息。

国外安全厂商认识来自东亚的 APT 组织海莲花（APT-C-00），一直针对中国的敏感目标进行攻击活动，是近几年来针对中国大陆进行攻击活动的最活跃的 APT 攻击组织之一。2019 年该组织在移动端的活动首次曝光，使用了著名的网络军火商 HackingTeam 提供的商业间谍软件。

披露时间	组织行动	披露来源	概述
2019.8.24	Konni	ESTsecurity	安全厂商发现 Konni 通过鱼叉式网络钓鱼邮件冒充加密货币交易通知，以保护加密货币交换账户

披露时间	组织行动	披露来源	概述
			的名义诱导下载移动端恶意软件，并称其与 APT 组织 Kimsuky 存在关联[28]。
2019.5.24	海莲花（APT-C-00）	安天	安全厂商发现海莲花在移动端的活动，使用的攻击样本签名中包含 HackingTeam 字样，可能是由 HackingTeam 提供的商业间谍软件[29]。

同时，据外媒报道，海莲花（APT-C-00）组织可能在 2019 年春季渗透到德国汽车巨头宝马公司的网络系统中，其活跃的目的可能是收集更多信息，例如各地汽车销量的报告。另外，在 2019 年 2 月该组织还对对包括丰田东京销售控股有限公司、东京丰田汽车公司、丰田东京卡罗拉等多家丰田在东京的公司展开攻击，最终导致约 310 万丰田客户的个人信息被泄露。该组织相继攻击德、日、韩多国汽车巨头企业的行为，被外媒认为是替自己国家汽车制造企业发展开辟道路。

(四) 特殊人群的监控

2019 年移动端 APT 攻击事件中，还体现出了部分国家内部局势动荡，主要体现在中东地区，针对国家内部持不同政见异见人群、反对派力量，以及一些极端主义活动的倡导者的网络监控。监控内容包括，这些特殊人群的活动范围，预谋的破坏行动，以及控制舆论导向。

披露时间	组织行动	披露来源	概述
2019.03.11	拍拍熊（APT-C-37）	360 烽火实验室	拍拍熊（APT-C-37）是西亚地区某国电子军背景的 APT 组织，其同时拥有针对 Windows 和 Android 的攻击平台，并且在过去主要针对极端组织“伊斯兰国”实施攻击活动[30]。
2019.05.23	军刀狮（APT-C-38）	360 烽火实验室	军刀狮（APT-C-38）针对中东地区展开攻击活动，其主要通过 Telegram 和水坑攻击分发恶意软件，该组织以库尔德人为攻击目标。其攻击平台为 Windows 和 Android[31]。
2019.06.18	Bouncing Golf	Trend Micro	安全厂商发现以窃取军事信息为目的的中东的间谍活动 Bouncing Golf，与 Domestic Kitten 在代码结构及窃取的数据格式有相似的地方[32]。
2019.07.01	Operation Tripoli	Check Point	安全厂商发现针对利比亚的攻击活动，攻击者通过在 Facebook 冒充利比亚国民军指挥官传播恶意样本，窃取了包括属于利比亚政府的秘密文件，电子邮件，官员的电话号码及官员护照照片等敏感信息[33]。

披露时间	组织行动	披露来源	概述
2019.10.3	未知	Check Point	安全厂商发现针对埃及记者和人权活动分子的针对性攻击，攻击者通过一种新的网络钓鱼技术，使攻击者获得了对受害者电子邮件的完全访问权限。同时，利用移动应用软件窃取受害者位置信息、通讯录和通话记录。该攻击活动背后被认为是由该国政府支持，对其本国异见人群或组织的监控活动[34]。

(五) 网络军火的进化

网络军火是由网络军火商制造，是在网络空间战中使用的武器，网络军火具备震慑、侦察、破坏、欺骗和防护作用。网络军火是国与国之间在第五维空间高科技技术的对抗，是掌控第五维空间主动权的重要因素。今年以来，安全厂商披露的网络军火出现功能多样化、漏洞利用常态化等特征。

2019 年 3 月，安全厂商发现在 Google Play 商店发现新型 Android 监控软件 Exodus[35]，Exodus 由一家名为 eSurv 的意大利公司开发的，该公司主要从事视频监控业务。Exodus 具有广泛的收集和拦截功能。根据公开信息，似乎 eSurv 自 2016 年开始开发间谍软件。

2019 年 5 月 WhatsApp 的爆出零日漏洞[36]。该漏洞被攻击者用于将以色列间谍软件注入到 1400 台手机中，这些恶意代码由以色列公司 NSO 集团开发，可以通过 iOS 和 Android 版 WhatsApp 呼叫其他用户来传播。黑客通过 WhatsApp 给用户打电话，即使用户没接听，黑客仍能在用户的手机上安装监

控软件，来电记录会自动消失，用户无法察觉手机出现异样。并且监控软件能远程控制手机的摄像头和麦克风，并收集个人信息和位置数据。

2019 年 7 月，安全厂商披露了一个有史以来最先进、功能最全面的移动 Android 监控软件 Monokle[37]，报告指出 Monokle 能够在没有 ROOT 访问权限的情况下，使用了 Android Accessibility 服务从第三方应用软件中窃取数据；将攻击者指定的证书安装到受感染设备上的受信任证书上，以允许中间人（MITM）攻击;使用预测文本字典了解目标所感兴趣的主题。能够在屏幕解锁事件期间记录设备的屏幕，从而使其能够泄露用户的 PIN，图案或密码。该监控软件由俄罗斯国防承包商 STC 开发，该公司因干预 2016 年美国总统大选而受到美国政府的制裁。

2019 年 9 月，SIM 卡被发现存在严重漏洞[38]，远程攻击者可利用漏洞在用户不知情的情况下发送短消息、设置调用、启动浏览器、提供本地数据、按命令运行和发送数据。攻击者只需通过向设备发送 SMS 即可触发攻击，通过软件提供的执行环境，在手机上运行恶意命令，监控跟踪目标用户。据悉，全球或有超 10 亿手机用户会受危害。早在 2015 年，就已有媒体曝出，美国国家安全局（NSA）已入侵全球手机 SIM 卡。

2019 年 11 月，360 高级威胁应对团队披露黄金雕（APT-C-34）组织活动[39]，其中移动端使用了著名的网络军火商 Hacking Team 泄露的网络攻击武器，其包括多达 17 种窃取隐私信息的功能模块。

三、 第五维空间将成为主导全维作战行动的重要力量

近年来，发生在第五维空间的攻击已成为争夺全球话语权的主流战争形态。网络空间威胁格局不断变化，但隐藏在其背后的，是国家间的博弈与较量。鉴于第五维空间在国家安全中的重要地位，第五维空间的作战力量将成为未来夺取主导全维作战行动的重要力量。

2018 年 12 月，俄罗斯与乌克兰因刻赤海峡冲突剑拔弩张，乌克兰宣布进入备战状态。英国率第 77 旅网络战部队从网络舆论到信息对抗的角度，火速支援

乌克兰并扬言让莫斯科停电，最终俄罗斯决定向乌克兰转交扣押的 3 艘乌克兰船只。

2019 年 3 月，委内瑞拉遭遇美国国家级黑客攻击，前所未有的至暗时刻来临，全国 23 个州中有 22 个遭遇断电，首都加拉加斯亦未能幸免一度陷入黑暗。

2019 年 5 月，以色列在成功防御来自哈马斯的国家级网络攻击后，通过更高级的网络攻击进行溯源并精确定位，用物理攻击的方式一颗导弹炸毁黑客组织据点。

2019 年 7 月，巴西司法部宣布总统博尔索纳罗使用的手机成黑客攻击的目标。据悉，该组织通过手机语音信箱入侵 1000 多个 Telegram 账号，其中就包括巴西总统、司法部长及经济部长所使用的账户。该团伙直接曝光了前巴西总统涉嫌参与洗钱、挪用款项、行贿受贿等行为，以及利用非法手段制造了多起政治黑幕，引发了一场政治风暴。

2019 年 10 月，360 烽火实验室首度揭秘叙利亚网络部队在叙利亚内战中的作用与影响[40]。在叙利亚电子军（SEA）后期的攻击活动中，可以发现其攻击目标为叙利亚政府军的各种敌对势力，利用网络战争获取真实战场情报先机。并且在利用网络攻击的同时，叙利亚政府军同时对相应敌对势力进行真实世界的军事打击。

从公开披露信息看，发生在第五维空间的攻击尤其是 PC 端发起的 APT 攻击从以前严格的政治、军事、外交目标，转向工控产业化和关键基础设施领域。主要攻击效果在于破坏和控制。而移动端发起的 APT 攻击则侧重在对于特定目标人群的定位和情报窃取。原因在于手机中存储着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。

由此可见，当网络战与实战走向融合时，其杀伤力无人能挡、无人能及；此外，我们还必须看到，当军事对抗力量不对等时，第五领域空间无疑将是大国博弈的最终战场。

第四章 聚焦第五维空间威胁趋势，加强治理和战略部署

一、 5G 或将对未来战场产生深远影响

2019 年“5G”这个字眼已经变得炙手可热，俨然已成为全球的热门话题。5G 是第 5 代移动网络技术的简称。5G 将拥有更高数据速传输速率，超大容量，超低延时，以及更低的成本和更加节省能源等方面的优势，并具有大规模连接终端的能力，进而加速推动物联网技术的发展，5G 成为万物互联的新型关键基础设施。工业互联网、车联网、智能电网、智慧城市、军事网络等都将构架在 5G 网络上裂变发展。

然而，就在我们享受 5G 所带来的巨大赋能时，另一端，前所未有的安全风险也随之而来。尤其网络切片技术使边界变得模糊，网络空间与物理空间紧密相连时，黑客也凭借“5G 东风”乘势发动攻击，物联网、车联网、工控等关键基础设施首当其冲，成为重点攻击对象。可以说，在 5G 浪潮之下，网络安全问题也成为百年未有的难题。

根据 360 发布的《5G 网络安全研究报告》报告指出[41]，从目前的分析来看，5G 安全仍面临着前所未有的更大挑战。短期内 5G 的安全特性难以发挥，并且伪基站问题将长期存在。另一方面，新技术带来新的安全挑战。比如，网络切片技术使得网络边界模糊，5G 对用户位置隐私的保护提出更高要求，低时延业务扩大了网络安全的攻击面，5G 在促进物联网发展的同时，也会成为黑客攻击的重点目标。

二、 围绕重要领域的钓鱼攻击不断增多

近年来，网络钓鱼攻击在不断地发展，特别是围绕重要领域的网络钓鱼攻击正在崛起。由于攻击依赖的是任何可利用的人为因素，因此，攻击者对这类攻击十分青睐。

最近，微软起诉了一个国外安全厂商认为是朝鲜背景的某个黑客组织，指控其从美国计算机上窃取“高度敏感信息”。理由就是 Thallium 组织向美、日、韩三国，包括政府雇员、智囊团、大学工作人员、关注世界和平与人权组织成员以及从事核扩散人员，发送大批量鱼叉式网络钓鱼邮件，将字母 r 和 n 组合在一起“microsoft”变成“rnicrosoft”，从而冒充的微软域名，借用这样的障眼法，迷惑攻击目标。

美国 MITRE 组织早在 2013 年推出了 ATT&CK 框架，一套根据现实的观察数据试图描述、分类攻击者的行动，基于攻防视角，试图让行业、设备用一种通用的语言去交流。ATT&CK 框架尽量将看不见、摸不着的攻击抽象成相对精准的信息矩阵，试图解决以往企业防护产品难以评估有效性的问题，同时提供了攻击映射到具体行为的防护思路。虽然行业对 ATT&CK 框架有着各自不同的理解，但是在 2019 年 ATT&CK 框架已然成为业内聚焦争论的热点话题。

在 ATT&CK 框架中将网络钓鱼划分到攻击者的初始访问阶段，这也就意味着未来钓鱼攻击将成为攻击者发起攻击的最初的攻击入口，网络攻击技术正在由简单粗暴向复杂精细转变，在与泄露的大量的数据信息相结合，针对特定个人，企业或重要基础设施的发起的钓鱼攻击将不断增多。

三、 人脸、指纹过度采集，生物信息安全建设需加强

随着银行电子化程度的不断提升，以及支付宝、微信等第三方移动支付的不断崛起，人脸、指纹识别的应用已经不再局限于手机解锁，而是将拓展至各种金融应用场景。

2019 年 2 月深圳某人脸识别企业被证实发生数据泄露事件，超过 250 万人的核心数据可被获取，680 万条记录泄露，其中包括身份证信息、人脸识别图像及 GPS 位置记录等。

2019 年 9 月某款 AI 换脸应用软件迅速走红，然而只用了短短一天，就从爆火刷屏到成为风暴中心。根据该应用软件的用户协议，其除了可免费使用并修改用户的肖像外，还可以将它任意授权给自己想授权的第三方。该条款引发公众对于自己的隐私信息尤其是人脸图像泄露的担忧。

有媒体调查发现在互联网某平台上，有商家公开兜售“人脸数据”，数量约 17 万条。在商家发布的商品信息中可以看到，这些“人脸数据”涵盖 2000 人的肖像，每个人约有 50 到 100 张照片。此外，每张照片搭配有一份数据文件，除了人脸位置的信息外，还有人脸的 106 处关键点，如眼睛、耳朵、鼻子、嘴、眉毛等的轮廓信息等。

中国消费者协会曾发布报告，报告显示多款应用软件涉嫌过度收集个人生物特征信息。2019 年 1 月，安全厂商调查发现多款具有美颜相机功能的应用软件，以需要用户将照片上传到指定的服务器来“美化”他们的图片的名义，收集用户上传的照片，用于恶意目的。

生物特征数据具有唯一性，但生物特征一旦被非法窃取利用，基于生物特征的身份认证系统均可被轻易绕过，进而引发一系列安全事件。目前，生物信息安全存在收集主体多、安全保障弱的突出问题，仍需加快推进个人信息保护法立法进程。

四、 企业采集、存储和使用数据规范亟待增强

目前企业对网络安全和数据信息保护不够重视，存在很大的安全隐患。一方面，很多企业都想着如何收集到更多的用户信息获取最大的利益，但数据在采集、储存、分析、计算、使用的过程中缺乏安全保护；另一方面，在一些非法网站或暗网中，用户数据交易已成常态，数据信息的交易泛滥，也是导致网络犯罪频发的重要原因之一。

2019 年央视“3•15”晚会上，曝光了某款社保查询应用软件利用授权窃取用户信息黑幕。因其未明示收集用户的社会保障号、社保查询密码等个人敏感信息的目的，并在用户注册时、查询社保时将以上信息传送至第三方服务器。除了应用软件利用授权窃取用户信息，我们还发现部分金融软件使用的数据采集 SDK，在没有隐私声明的情况下，违规采集用户通讯录和通话记录等隐私信息。

2019 年，为规范企业采集、存储和使用数据，首先从系统层面对采集源头加以限制，Android 10 引入了大量隐私权变更，比如，针对访问设备硬件标识符实施了访问限制，限制第三方应用软件获取设备硬件唯一标识；增强了用户对位置权限的控制力，限制在后台时请求访问用户位置信息的应用等，目的是保护隐私权并赋予用户控制权。

其次，监管层面文件密集发布，包括《数据安全管理办法（征求意见稿）》、《APP 违法违规收集使用个人信息行为认定方法（征求意见稿）》、《个人信息安全规范（征求意见稿）》、《信息安全技术、移动互联网应用 (APP) 收集个人信息基本规范（草案）》、《关于发布金融行业标准加强移动金融客户端应用软件安全管理的通知》、《信息安全技术网络安全等级保护基本要求》等。同时进一步完善相关政策法律法规，2019 年 10 月，最高人民法院、最高人民检察院发布《最高人民法院最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》，对拒不履行信息网络安全管理义务罪，非法利用信息网络罪和帮助信息网络犯罪活动罪的定罪量刑标准和有关法律适用问题作了全面、系统的规定。

与此同时，为配合政策法规的发布，展开了多个专项打击和治理活动。2019 年 01 月，中央网信办、工业和信息化部、公安部、市场监管总局联合发布“关于开展 APP 违法违规收集使用个人信息专项治理的公告”，在全国范围组织开展 APP 违法违规收集使用个人信息专项治理。2019 年 11 月，针对 APP 违规收集个人信息、过度索权、频繁骚扰、侵害用户权益等问题突出，群众反映强烈，社会关注度高。工业和信息化部决定组织开展 APP 侵害用户权益专项整治

行动工作，分别通报了两批侵害用户权益 APP，要求厂商在限期内完成整改落实工作，对于逾期不整改的依法下架处理。

在互联互通的全球数字经济背景下，数据是企业最重要的战略资产。只有提升对数据价值的认识，对数据存储、使用和管理的方式予以高度重视并将其置于企业战略的核心，同时建立有效的数据保护策略，方能保障企业安全。

附录一：参考资料

[1] 第 44 次《中国互联网络发展状况统计报告》：http://www.cac.gov.cn/2019-08/30/c_1124938750.htm

[2] Spam and phishing in Q3 2019：https://securelist.com/spam-report-q3-2019/95177/

[3] 安全预警：借贷软件变脸绕过应用市场审核：http://blogs.360.cn/post/analysis_of_bianlian.html

[4] 2019 Mobile Ad Supply Chain Safety Report：http://info.pixalate.com/mobile-advertising-supply-chain-safety-report-2019

[5] Android Security & Privacy 2018 Year In Review：https://source.android.com/security/reports/Google_Android_Security_2018_Report_Final.pdf

[6] Secure-D uncovers suspicious mobile transactions from Android Keyboard app ai.type generating non-human clicks and making unwanted purchases：https://www.upstreamsystems.com/secure-d-uncovers-suspicious-mobile-transactions-android-keyboard-app-ai-type-generating-non-human-clicks-making-unwanted-purchases/

[7] 2019 中国移动社交行业规模、投融资情况及发展趋势分析：https://www.iimedia.cn/c1020/66304.html

[8] 陌生人社交市场报告：2019 年用户规模将超 6 亿，“色交约炮 APP”凸显监管漏洞：https://www.iimedia.cn/c460/64707.html

[9] 大批社交和语音类软件从苹果 App Store 下架 数量或达 700 个：http://www.sohu.com/a/294375036_728306

[10] 音乐社交 APP 音遇全网下架：http://www.techweb.com.cn/it/2019-04-26/2733674.shtml

[11] 国家网信办启动小众即时通信工具专项整治 首批清理关停 9 款违法违规 APP：http://www.cac.gov.cn/2019-04/16/c_1124373996.htm

[12] 即时通讯整治继续探探因违规被下架：https://baijiahao.baidu.com/s?id=1632067888319591047&wfr=spider&for=pc

[13] 有关网络安全漏洞披露管理的现状分析与建议：https://www.freebuf.com/articles/neopoints/209224.html

[14] 国家互联网信息办公室关于《网络安全威胁信息发布管理办法（征求意见稿）》公开征求意见的通知：http://www.cac.gov.cn/2019-11/20/c_1575785387932969.htm

[15] CVE Details：https://www.cvedetails.com/top-50-products.php?year=2019

[16] 平台版本：https://developer.android.google.cn/about/dashboards

[17] CVE-2017-13156：https://source.android.google.cn/security/bulletin/2017-12-01

[18] The StrandHogg vulnerability：https://promon.co/security-news/strandhogg/

[19] Agent Smith: A New Species of Mobile Malware：https://research.checkpoint.com/2019/agent-smith-a-new-species-of-mobile-malware/

[20] 新时代的中国国防：http://www.gov.cn/zhengce/2019-07/24/content_5414325.htm

[21] MalBus: Popular South Korean Bus App Series in Google Play Found Dropping Malware After 5 Years of Development：https://www.mcafee.com/blogs/other-blogs/mcafee-labs/malbus-popular-south-korean-bus-app-series-in-google-play-found-dropping-malware-after-5-years-of-development/

[22] 警惕来自节假日的祝福 APT 攻击组织“黑格莎（Higaisa）”攻击活动披露 https://dlied6.qq.com/invc/qqpcmgr/skin/1572851347.pdf

[23] 금성 121 APT 조직, 스테가노그래피 기법과 스마트폰 노린 퓨전 공격 수행：https://blog.alyac.co.kr/2452

[24] 蔓灵花（APT-C-08）移动平台攻击活动揭露：http://blogs.360.cn/post/analysis_of_APT_C_08.html

[25] New #APT_C_23 sighting, this time for mobile devices： https://twitter.com/_CPResearch_/status/1108402662960177153

[26] ViceLeaker Operation: mobile espionage targeting Middle East：https://securelist.com/fanning-the-flames-viceleaker-operation/90877/

[27] MuddyWater Resurfaces, Uses Multi-Stage Backdoor POWERSTATS V3 and New Post-Exploitation Tools：https://blog.trendmicro.com/trendlabs-security-intelligence/muddywater-resurfaces-uses-multi-stage-backdoor-powerstats-v3-and-new-post-exploitation-tools/

[28] 코니(Konni) APT 조직, 모바일 스파이 활동을 통한 스마트 위협 증가：https://blog.alyac.co.kr/2486

[29] 关于海莲花组织针对移动设备攻击的分析报告：https://www.antiy.com/response/20190524.html

[30] 拍拍熊（APT-C-37）：持续针对某武装组织的攻击活动揭露: http://blogs.360.cn/post/analysis-of-apt-c-37.html

[31] 军刀狮组织（APT-C-38）攻击活动揭露：http://blogs.360.cn/post/analysis-of-APT-C-38.html

[32] Mobile Cyberespionage Campaign ‘Bouncing Golf’ Affects Middle East：https://blog.trendmicro.com/trendlabs-security-intelligence/mobile-cyberespionage-campaign-bouncing-golf-affects-middle-east/

[33] Operation Tripoli：https://research.checkpoint.com/2019/operation-tripoli/

[34] The Eye on the Nile：https://research.checkpoint.com/2019/the-eye-on-the-nile/

[35] Exodus: New Android Spyware Made in Italy：https://securitywithoutborders.org/blog/2019/03/29/exodus.html

[36] The NSO WhatsApp Vulnerability – This is How It Happened：https://research.checkpoint.com/2019/the-nso-whatsapp-vulnerability-this-is-how-it-happened/

[37] Lookout discovers new mobile surveillanceware developed by Russian defense contractor Special Technology Center：
https://blog.lookout.com/monokle

[38] Simjacker – Next Generation Spying Over Mobile ：
https://www.adaptivemobile.com/blog/simjacker-next-generation-spying-over-mobile_

[39] 盘旋在中亚上空的阴影-黄金雕（APT-C-34）组织攻击活动揭露：
http://blogs.360.cn/post/APT-C-34_Golden_Falcon.html

[40] 叙利亚电子军揭秘：管窥网络攻击在叙利亚内战中的作用与影响：
http://blogs.360.cn/post/Syrian_Electronic_Army.html

[41] 5G 网络安全研究报告：
http://zt.360.cn/1101061855.php?dtid=1101062370&did=210884514

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。