腾讯安全2017年度
互联网安全报告

腾讯安全　腾讯安全联合实验室

腾讯安全2017年度互联网安全报告

目录

前言

据中国信息通信研究院发布的《2017 中国数字经济发展白皮书》指出，2016 年中国数字经济总量达到 22.6 万亿元，占 GDP 的比重超过 30%。毫无疑问，随着中国数字化进程逐步推进，各个行业的价值链都将经历着彻底变革。“中国数字经济发展将进入快车道”,习近平总书记在致第四届世界互联网大会的贺信中表示。

但与此同时 ,以信息技术为代表的新一轮科技和产业革命也给世界各国主权、安全、发展利益带来许多新的挑战。近年来，国家级网络武器及其相关工具和技术的扩散，使得新型勒索病毒对各国关键基础设施造成了极大的挑战。全球互联网治理体系变革进入关键时期，构建网络空间命运共同体日益成为国际社会的广泛共识。

早在中央网络安全和信息化领导小组第一次会议上，习总书记就提出“网络强国”战略。“家门就是国门”，安全问题刻不容缓，作为发展基础的安全人才建设问题成为重中之重。然而当前我国安全人才缺口问题较为突出，据数据显示，截止 2017 年上半年我国网络安全人才总需求量超过 70 万人，相关行业每年还以 1.5 万人的速度递增，但我国高校教育近年培养的信息安全专业人才仅 3 万余人 ,远不能满足网络安全行业的需要。

网络空间的竞争，归根到底是人才的竞争。中国需加紧计算机信息安全人才体系建设，推动我国尽快从网络大国走向网络强国，这也是确保中国未来取得国际空间话语权与规则制定权的关键。

一、 网络安全整体现状扫描

1.1 国际格局下中国网络安全形势复杂化、多元化和新型化

1.1.1 网络威胁全球化特征日益明显，中国加速迈向网络强国

近年来，全球网络空间安全威胁呈现新的变化，一些新型网络威胁正呈现全球蔓延的态势。例如今年影响最恶劣的“WannaCry”勒索病毒，攻击范围遍及全球，100 多个国家和地区遭受攻击，包括政府部门、教育、医院、能源、通信、制造业等多个行业的数十万台电脑受到攻击感染。

面对严峻的安全形势，中国亟需提升网络安全实力，加速从网络大国向网络强国的迈进。今年以来，中国安全产品与安全人才屡屡在国际舞台中展露身手，使中国安全能力受到国际瞩目。在产品方面，腾讯电脑管家(英文版)OEM 版和 TAV 版连续 26 次通过 VB100 评测；并且在 AV-C 11 月评测报告中，腾讯电脑管家(英文版)以 96 分的全球最高分列居榜首，累计斩获 AV-C 测试 20 个“A+”最高评级，这一成绩已与卡巴斯基、小红伞、Bitdefender 等老牌杀毒厂商旗鼓相当，也意味着国产杀软已跻身国际杀毒软件第一阵营。此外，在今年的 Mobile Pwn2Own 2017 黑客大赛中，代表中国的腾讯安全团队第三次拿下“世界破解大师”称号，成为该赛事中全球首个“三冠王”。这场赛事有来自北美、欧洲、亚洲地区的全球顶尖安全战队参加，也可以看出中国安全实力正在加速赶超。

1.1.2 经济新发展带来网络安全新焦点

1.1.2.1 物联网安全

2017 年以来，重大物联网安全事件呈现出增长态势，有调查数据显示，2017 年上半年物联网攻击增加了 280%。9 月，物联网安全研究公司 Armis 在蓝牙协议中发现了 8 个 0day 漏洞，预计影响全球超过 53 亿设备；10 月，WiFi 设备 WAP2 安全协议又爆出安全漏洞，几乎所有手机系统受到影响。而 8 月央视紧急曝光的家庭摄像头入侵事件，更是让广大用户从日常生活层面切实感知到物联网带来的安全隐患，造成了消费者对隐私安全问题的极大担忧。

物联网安全目前存在的隐患，极大程度上与安全标准滞后、智能设备商缺乏安全意识和投入有关。安全行业如果不能提供有效的安全防御解决方案，将直接影响这些新兴领域的未来发展。

1.1.2.2 网络黑产挑战加剧

2017 年，网络黑产所带来的安全挑战愈加严峻。各种利用互联网技术进行偷盗、诈骗、敲诈等案件不断发生，围绕互联网的黑灰产业正以极快的速度蔓延。从各个主要国家的统计数据看，利用互联网技术实施偷盗、诈骗、敲诈的案件数每年以超过 30% 的增速在增长。据测算，仅中国“网络黑产从业人员”就已超过 150 万，“市场规模”也已高达千亿级别。

面对网络黑产愈发严峻的挑战，各行业、企业之间，必须要具备更加开放、合作、共享的心态。互联网科技公司、安全厂商、白帽黑客个体及团体也需针对上游的漏洞挖掘、病毒防御等方面更加积极主动，才能遏制黑产的发展势头。

1.1.2.3 互联网金融诈骗

2017 年年底，钱宝网实际控制人张小雷因涉嫌违法犯罪，向南京市公安机关投案自首，又一起互联网金融诈骗案件崩盘。据了解，钱多宝以做任务获高额收益为诱饵，吸引用户注册为会员 ,并缴纳一定保证金。当用户缴纳 10 万保证金后 ,可获得最低 4000 元、最高过万元的高收益，吸引了无数人投资。

近年来互联网金融诈骗频发，这类涉众型、风险型经济犯罪案件，处置不当，极易发生群体性事件，造成较大社会影响。这要求相关部门加强民众宣传引导，从源头上防止案件发生，另一方面需加强审核把关，严格防范利用注册公司进行违法犯罪，并进一步提升自身金融反欺诈的能力。

1.1.2.4 数据隐私泄漏现象日益严重

随着互联网+的日益深入，数据隐私现象正变得越来越严重。据数据显示，2017 年上半年全球泄露或被盗的数据达 19 亿条，这一数字已经超过了 2016 年全年被盗数据总量，其中，仅雅虎一家就达到了 30 亿条。

信息泄漏现象严重主要有几下几方面原因：一是缺少个人信息保护的细致规则；二是消费者个人信息保护意识不强；三是经营者管理不规范；四是行政监管和行业监督尚待完善；五是行业自律规则和行业标准尚不健全，对企业监督未能发挥充分作用。随着云计算、大数据、物联网的加速普及，数据泄露不仅需要更加严格的监管措施，同时也

需要借助技术创新，进一步防止因外部攻击而导致数据被盗取、泄露等风险。

1.1.2.5 共享经济监管薄弱 产品存在明显安全隐患

有数据显示，2016 年中国共享经济市场规模达 39450 亿元，增长率为 76.4%，未来几年将继续保持高速增长。共享产品的商业模式决定了服务商很难对其进行严格的管控，这就给了不法分子巨大的作案空间。一方面，不法分子可以通过更改二维码的方式挟持服务分发的渠道，将用户访问导入到非法的网络内容之中；另一方面，不法分子还可以直接对产品进行修改，以控制用户的个人信息设备。

1.1.2.6 食药安全涉及民生，成网络安全领域关注焦点

随着我国互联网经济蓬勃发展，“互联网 + 食品”新业态乘势而上，但其中也存在一定的不规范问题。业内人士指出，当前食药监管存在几个主要问题：1、网络食品经营第三方平台食品安全责任落实不到位；2、部分入网食品经营者安全意识不高，食品安全存在隐患；3、网络食品的虚拟市场交易，涉及信息发布、第三方平台、线上线下结算、商品配送等多方面，法律关系更为复杂，4、网络食品的虚拟性和跨地域特点为监管带来难度。

1.2 《中华人民共和国网络安全法》正式施行，网络安全进入法制化时代

6 月 1 日，我国第一部全面规范网络空间安全管理的基础性法律——《中华人民共

和国网络安全法》正式施行，共有七章七十九条，内容十分丰富，具有六大突出亮点。一是明确了网络空间主权的原则；二是明确了网络产品和服务提供者的安全义务；三是明确了网络运营者的安全义务；四是进一步完善了个人信息保护规则；五是建立了关键信息基础设施安全保护制度；六是确立了关键信息基础设施重要数据跨境传输的规则。

新法的施行标志着我国网络安全从此有法可依，网络空间治理、网络信息传播秩序规范、网络犯罪惩治等即将翻开崭新的一页，对保障我国网络安全、维护国家总体安全具有深远而重大的意义。

同时，今年 12 月 4 日上午，由中国网络空间研究院编写的《世界互联网发展报告 2017》和《中国互联网发展报告 2017》蓝皮书在第四届世界互联网大会上正式发布。这是世界互联网大会举办以来，首次面向全球发布互联网领域最新学术研究成果。两份蓝皮书不仅全面展现世界各国和中国互联网发展现状及未来趋势,同时把网络安全纳入互联网发展程度的评价维度指标,提升到了新的高度。

1.3 2017 年度安全大事件盘点

1.3.1 跨国名企信息泄漏，波及全球超两亿用户

2017 年年初，国际上连续爆出多家知名企业用户信息泄露事件，其中包括全球四大会计师事务所之一的 Deloitte（德勤）、加拿大电信巨头贝尔公司、知名教育平台 Edmodo 与知名云服务商 Cloudflare 等。泄漏的信息主要为用户的隐私信息、私人账户信息、企业内部敏感文件与公司内往来邮件内容等，总计影响全球超两亿用户。

1.3.2 美国中央情报机关被“闯入”，“最高机密”泄漏

2017 年 3 月，美国中央情报局数千份“最高机密”文档泄露，不仅暴露了全球窃听计划，还包括一个可入侵全球网络节点和智能设备的庞大黑客工具库。

4 月，黑客组织 Shadow Brokers 公布了其盗取的 NSA 的机密文件，其中包括可以远程攻破全球约 70% Windows 机器的漏洞利用工具。

1.3.3 勒索病毒“WannaCry“全球爆发，规模史无前例

2017 年 5 月 12 日，一款名为“WannaCry”的蠕虫勒索软件袭击全球网络，通过加密电脑文档向用户勒索比特币。

这被认为是迄今为止最巨大的勒索病毒事件 ,至少 150 个国家、30 万名用户中招，造成损失达 80 亿美元。中国部分 Windows 操作系统用户遭受感染，某些大型企业的应用系统和数据库文件被加密勒索，影响巨大。

1.3.4 中国首部《网络安全法》颁布，实行“全民实名制”

2017 年 6 月 1 日，网络安全领域首部《中华人民共和国网络安全法》正式施行，新法的颁布将让广大网络用户在虚拟的世界中有法可依。

《网安法》在时下最热门的个人信息保护等领域均有新规，更以法律的形式对“网

络实名制”作出规定 :用户在使用信息发布、即时通讯等服务时 ,应提供真实身份信息。

1.3.5 “暗云Ⅲ”突袭全国，百万机器帮不法黑客“赚黑钱”

2017 年 6 月 9 日下午，腾讯电脑管家监控到目前已知复杂度最高、感染用户数量最大的木马之一——“暗云 Ⅲ”大量传播，并实现开机启动，数百万用户电脑沦为不法黑客发起的 DDoS 攻击的“傀儡机”。本次受影响机器覆盖极广，几乎涵盖所有省市运营商的骨干网络。

1.3.6 家用摄像头遭入侵，你的生活正在被“直播”

2017 年 6 月 ,国家质检总局对市场上的智能摄像头进行了监测 ,在 40 批样品中，32 批存在安全隐患，28 批数据传输没有加密，20 批初始密码是“弱口令”。此后国家国家互联网应急中心的调查中 ,随机挑选的两个摄像头品牌就存在十几万个弱口令漏洞，极易受攻击。之后，央视曝光了一起家用摄像头遭破解的案例，用户家庭隐私被公开贩卖，用户真实生活被“直播”。

1.3.7 “善心汇”不善心，传销诈骗数百亿元

2017 年 7 月，“善心汇”特大网络传销组织遭到了公安机关的打击查处。该组织打着“扶贫济困、均富共生”旗号发布虚假宣传，采取“拉人头”方式大肆发展会员，为头目谋取不法高额收益。截止查处当日，善心汇已发展 500 多万会员，遍布全国 31 个

省区市，涉案金额数百亿元，是近年来较为罕见的特大涉嫌传销组织。

1.3.8 加密协议被破解，WiFi 不再安全？！

2017 年 10 月，用于保护 WiFi 网络安全的 WPA2 安全加密协议被不法黑客破解。这意味着用户连接的绝大多数 WiFi 处于易受攻击的状态，信用卡、密码、聊天记录、照片、电子邮件等重要信息随时有可能被不法黑客窃取。涉及平台包括安卓系统、iOS 系统以及 Windows 操作系统。

1.3.9 恶意病毒“Bad Rabbit”席卷东欧

2017 年 10 月 24 日，一款名为“BadRabbit”（坏兔子）的勒索软件导致“东欧陷落”。“BadRabbit”伪装成 Adobe flash player 升级的对话框，主要靠弱密码连环攻击来勒索比特币。同时在局域网内扩散，形成“一台感染、一片瘫痪”的局面。包括乌克兰与俄罗斯在内的东欧公司受灾严重。

1.3.10 高危漏洞“潜伏”17 年，Office 文档或带毒

2017 年 11 月，潜伏长达 17 年之久的 Office 远程代码执行漏洞（CVE-2017-11882）的攻击代码被公开，影响范围包括任意版本的 Office 软件。这意味着任何人都可以利用此漏洞发起攻击，例如通过钓鱼邮件或网络共享的办公文档诱骗人们点击。如果不慎打开恶意文档，电脑就会被黑客远程控制。

二、2017 病毒形势整体好转，漏洞威胁呈上升势头

2.1 PC 端病毒拦截近 30 亿，新增病毒数量 6 年来首次下降

2.1.1 PC 端平均每月木马病毒拦截 2.45 亿次

2017 年腾讯电脑管家统计数据显示，PC 端总计已拦截病毒近 30 亿次，相较 2016 年同比下降 36.2%；平均每月拦截木马病毒近 2.45 亿次，同比下降 38.7%。

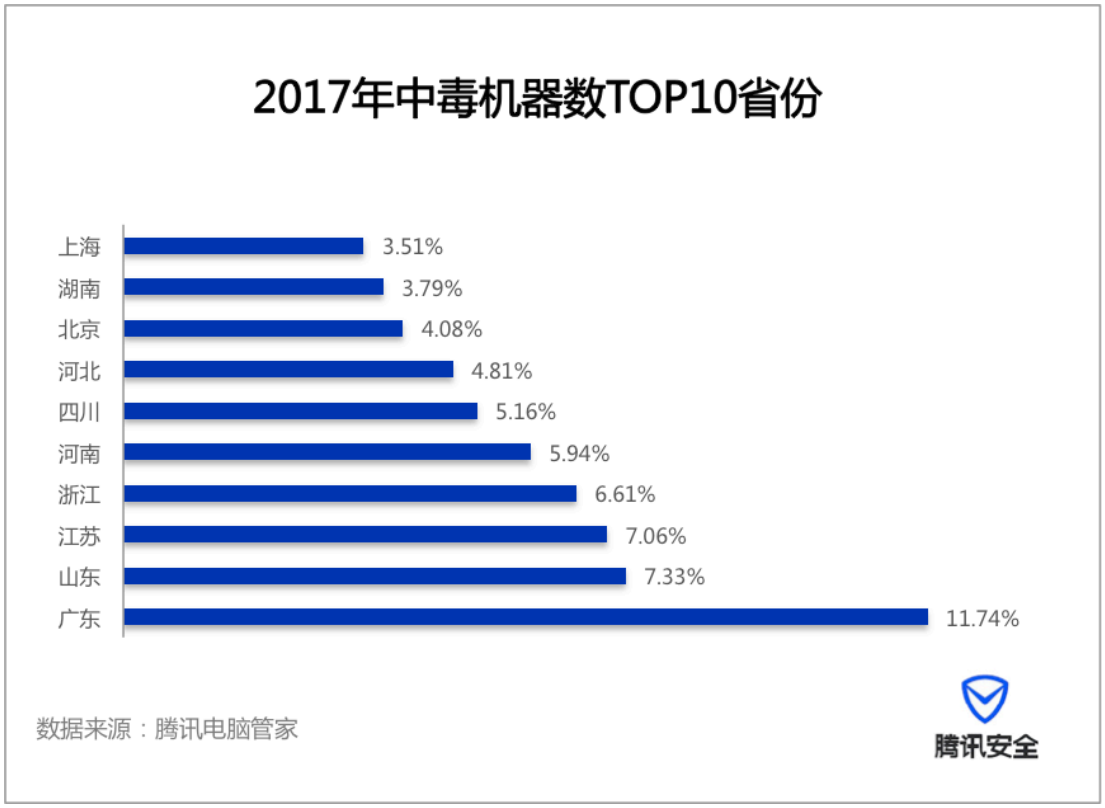
2017 年相较于 2016 年新发现病毒数量同比下降 8.6%。从 2012 年到 2016 年，新发现病毒量始终呈逐年递增状态，2017 年是量近 6 年来的首次下降。

2.1.2 2017 年共发现 6.3 亿台用户机器中病毒或木马

2017 年腾讯电脑管家共发现 6.3 亿台用户机器中病毒或木马，相比 2016 年同比下降 23.2%。其中 7 月是全年用户机器染毒量最低点，为 4339 万。

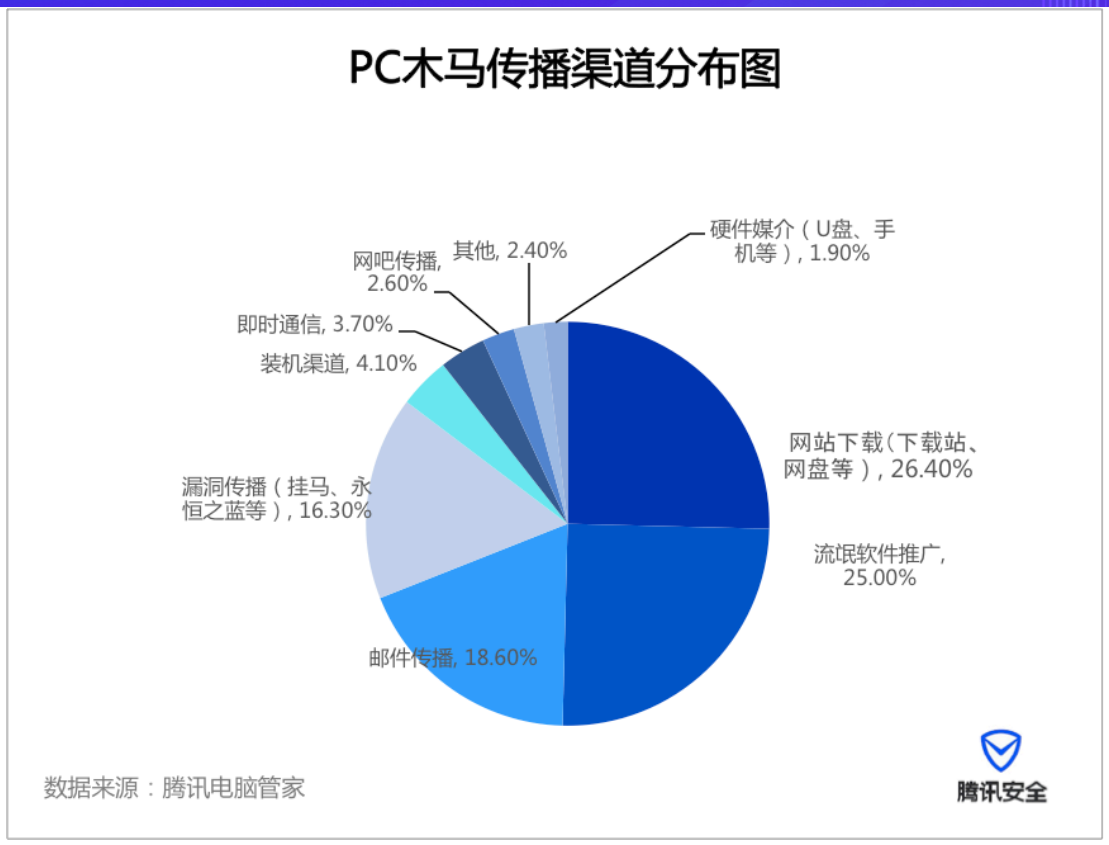
2.1.3 PC 端中毒用户省份最多为广东，占全部拦截量的 11.74%

根据腾讯电脑管家监测到的中毒 PC 数量统计，从省份分布来看，全国拦截病毒排名第一省份为广东省，占全部拦截量的 11.74%%，第二名为山东省，占全部拦截量的 7.33%，第三名为江苏省，占全部拦截量的 7.06%。



2.1.4 网站下载、流氓软件推广占木马传播渠道 5 成以上

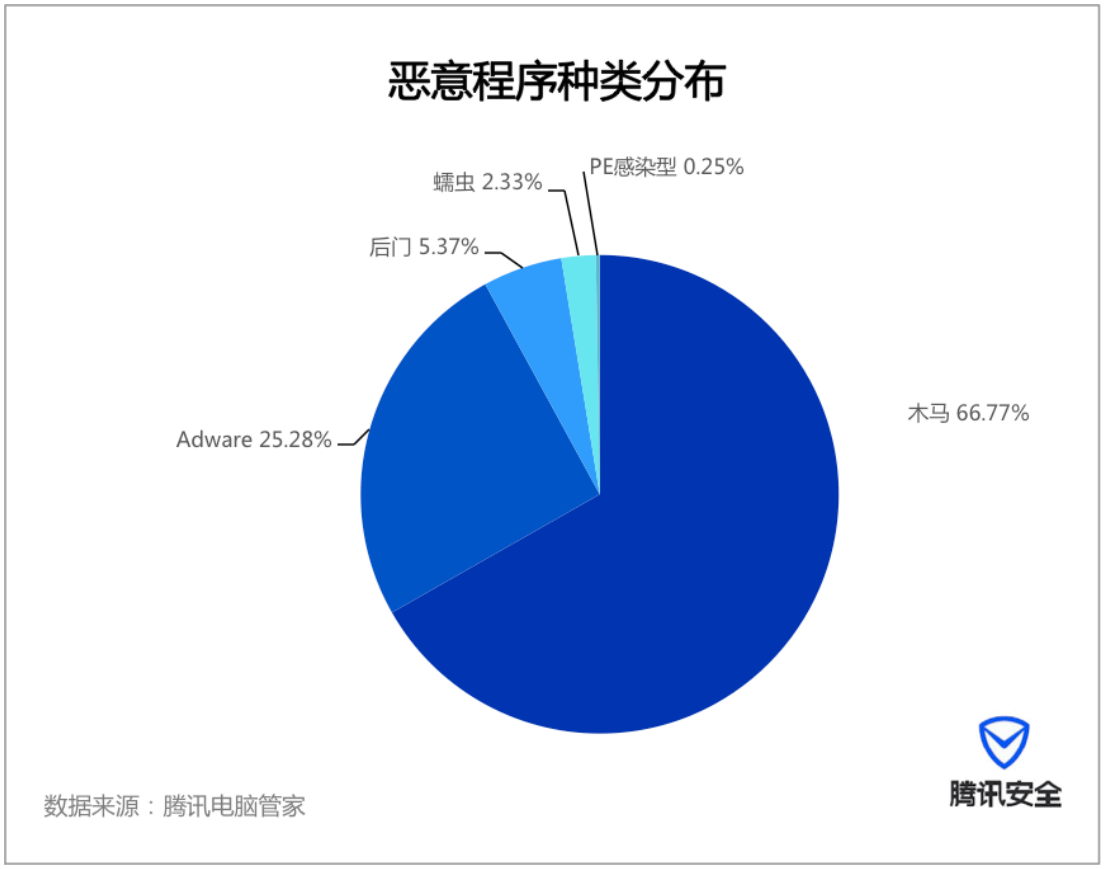
在木马传播渠道中，网站下载占比 25.4%，流氓软件推广占比 25%，邮件传播占比 18.6%，漏洞传播占比 16.3%。用户应尽可能减少从非安全站点下载软件、文件、视频、图片等，特别是一些号称破解版的软件。



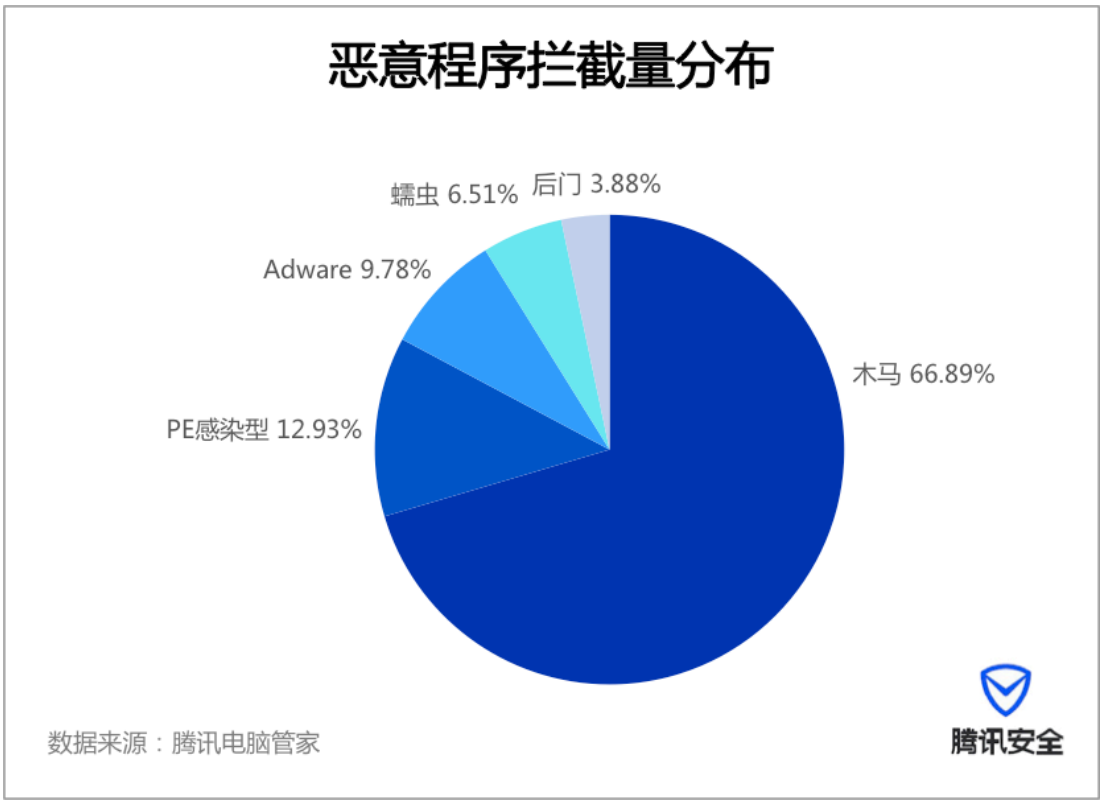
2.2 近六成恶意程序为木马，已成网络黑产首选攻击方式

2.2.1 木马仍然为年度第一大恶意程序种类，占总体数量的 59.22%

根据腾讯电脑管家 2017 年获取到的恶意程序样本分析，恶意程序种类上，木马类占总体数量的 59.22%，占据全年第一大种类恶意程序。Adware 类（广告软件、强制安装、收集用户隐私、弹垃圾信息等）为第二大恶意程序种类，占总体数量的 31.47%。后门类为第三大恶意程序种类，占总体数量的 6.09%。

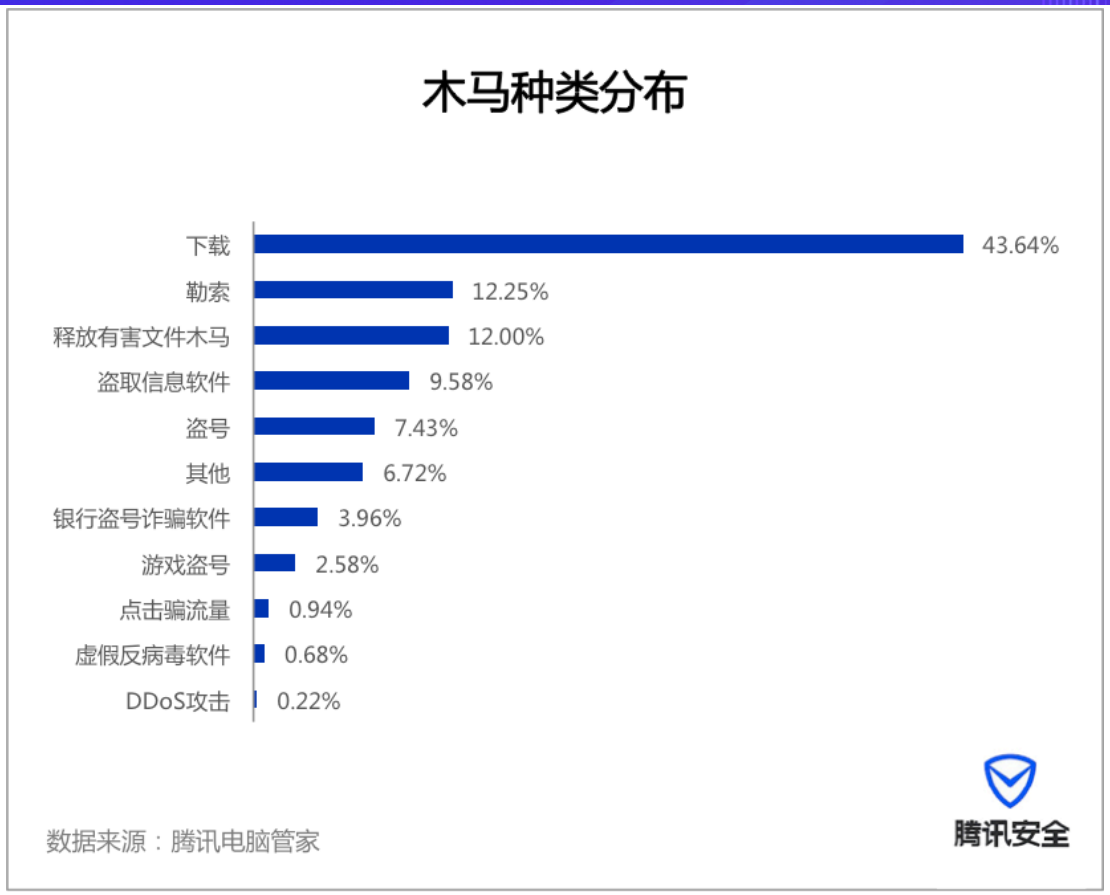


从拦截恶意程序样本的数量上来划分，排在第一位仍然是木马类，占了总量的66.89%。排在第二位的是 PE 感染型，占总体数量的 12.93%。Adware 排在第三位，占总体数量的 9.78%。

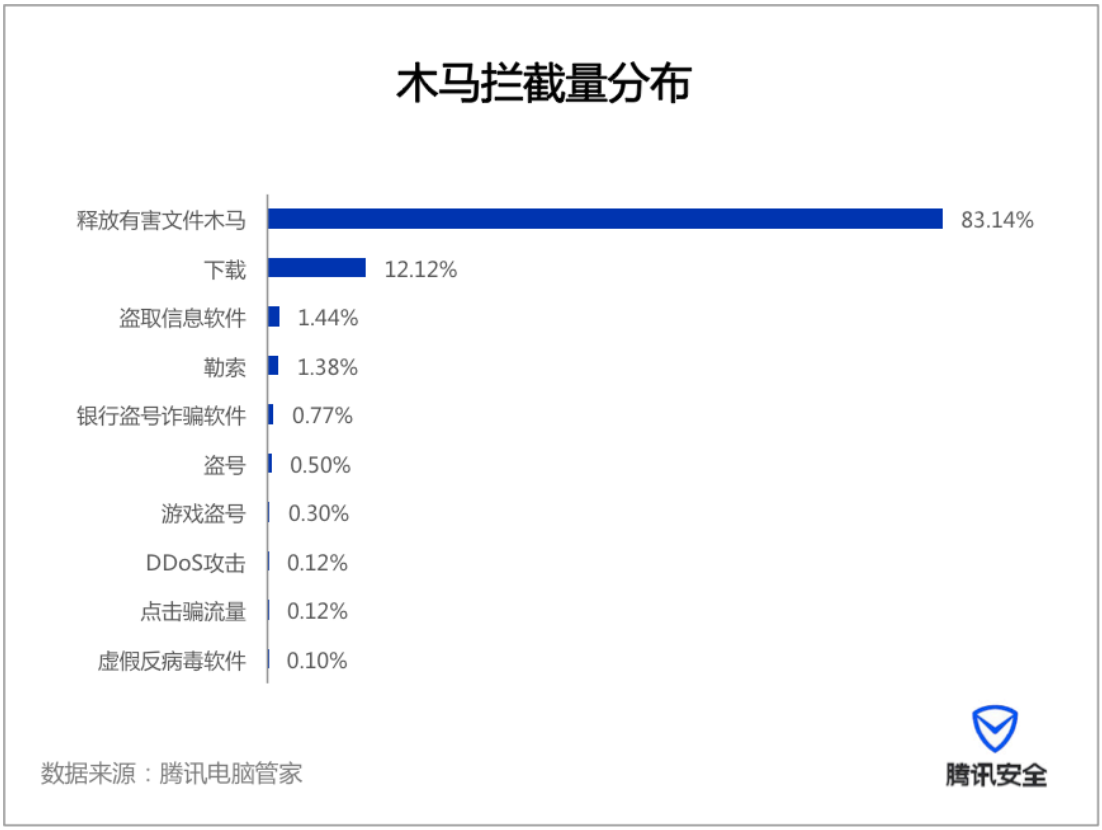


2.2.2 勒索病毒仅为年度第二大木马种类，Dropper 类木马拦截量最多

在第一大病毒类木马类中，可以详细划分为多种类型的木马病毒。其中排名第一位的是下载类木马，占全部种类的 43.64%。排在第二位的勒索病毒种类占到了 12.25%。



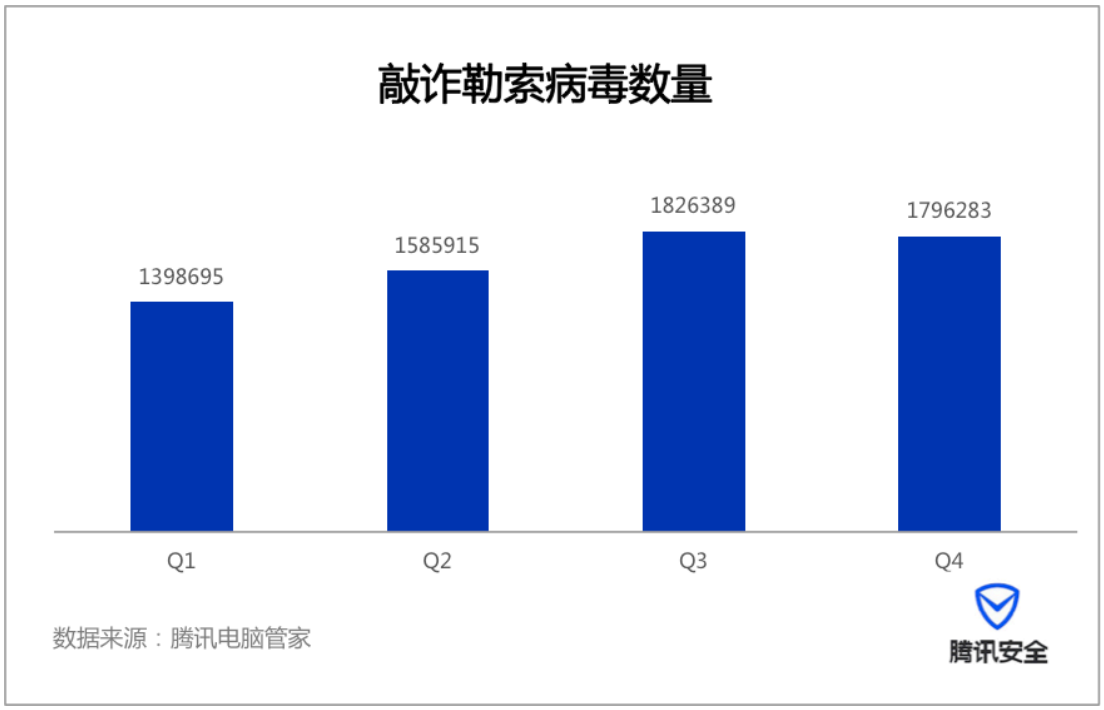
但如果从木马病毒样本的数量上来划分，可以看到排在第一位是 Dropper 类木马病毒（释放有害文件木马），占全部拦截量的 83.14%。Dropper 类虽然在病毒种类上没有下载类种类多，但在数量级上远远超过了下载类，这说明此类木马传播的最广泛，数量最多，受害的用户也最多。勒索类病毒并不太多，但今年较活跃，占全部拦截量的 1.38%。



2.3 勒索病毒爆发性增长，办公人群成主要“敲诈”对象

2.3.1 2017 全年总计发现敲诈勒索病毒样本数量 660 万

根据检测到的敲诈勒索病毒显示，2017 全年总计已发现敲诈勒索病毒样本数量在 660 万个，平均每月检测到敲诈勒索病毒数量近 55 万个。Q3 季度为 4 个季度中检测病毒的高峰，检测量为 180 万个。



2.3.2 敲诈勒索病毒传播方式

目前的敲诈勒索病毒主要采用以下几种传播方式：

敲诈勒索病毒传播方式
1. 文件感染传播
2. 网站挂马传播
3. 利用系统漏洞传播
4. 邮件附件传播
5. 网络共享文件传播
6. 软件供应链传播

1、文件感染传播

利用感染型病毒的特点进行传播，如 PolyRansom 就是利用感染型病毒的特点，加密用户所有文档后再弹出勒索信息，而由于 PE 类文件被感染后具有了感染其他文件的能力，因此如果此文件被用户携带（U 盘、网络上传等）到其他电脑上后运行，就会使得该电脑的文件也被全部感染加密。

2、网站挂马传播

网站挂马通过是在获取网站或者网站服务器的部分或全部权限后，在网页文件中插入一段恶意代码，这些恶意代码主要是一些包括 IE 等浏览器漏洞利用代码，用户访问被挂马的页面时，如果系统没有更新恶意代码中利用的漏洞补丁，则会执行恶意代码。

3、利用系统漏洞传播

5 月爆发的 WannaCry 就是利用 Windows 系统漏洞进行传播，利用系统漏洞传播的特点是被动式中毒，即用户没有去访问恶意站点，没有打开未知文件也会中毒，因为病毒会扫描同网络中存在漏洞的其他 PC 主机，只要主机没有打上补丁，就会被攻击。

腾讯安全反病毒实验室提醒大家，及时更新第三方软件补丁，及时更新操作系统补丁，以防被已知漏洞攻击。

4、邮件附件传播

通过邮件附件进行传播的敲诈勒索病毒通常会伪装成用户需要查看的文档，如信用卡消费清单、产品订单等。附件中会隐藏恶意代码，当用户打开后恶意代码便会开始执

行，释放病毒。这类伪装病毒通过会批量发送给企业、高校、医院机构等单位，这些单位中的电脑中通常保存较重要的文件，一旦被恶意加密，支付赎金的可能性远远超过普通个人用户。

5、网络共享文件传播

一些小范围传播的敲诈勒索病毒会通过共享文件的方式进行传播，病毒作者会将病毒上传到网络共享空间、云盘、QQ 群、BBS 论坛等地方，以分享的方式发送给特定人群诱骗下载安装。

腾讯安全反病毒实验室提醒大家，下载软件请到官方正规渠道下载安装，切勿下载未知程序，如需要使用未知来源的程序，可提前安装腾讯电脑管家进行安全扫描。

6、软件供应链传播

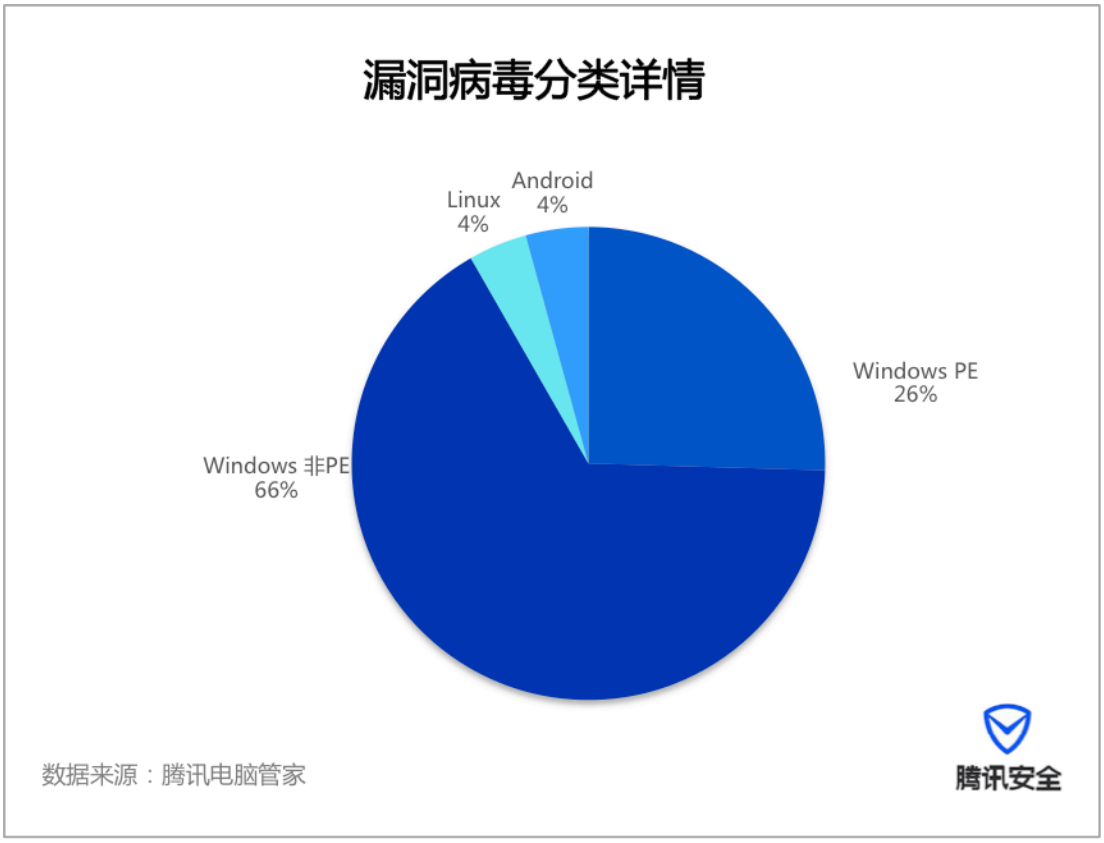
病毒制作者通过劫持正常软件的安装、升级，在用户进行正常软件安装、升级时达到病毒传播的目的。这种传播方式利用了用户与软件供应商之间的信任关系，成功绕开传统安全产品的围追堵截，因此传播方式更加隐蔽。

2.4 漏洞危害日趋严重，亟需重视移动安全新思维

2.4.1 Windows 平台漏洞病毒占比最多，非 PE 类型的漏洞样本达到 65.60%

漏洞病毒样本主要分布在 Windows、Linux、Android 平台上，通过对获取到的漏洞类型样本统计，可以看到 Windows 平台占比最多，其中非 PE 类型的漏洞样本达到 65.60%，PE 类型漏洞样本达到 25.21%，Windows 平台漏洞样本总量可达到所有

平台全部漏洞样本总量的 90.81%。



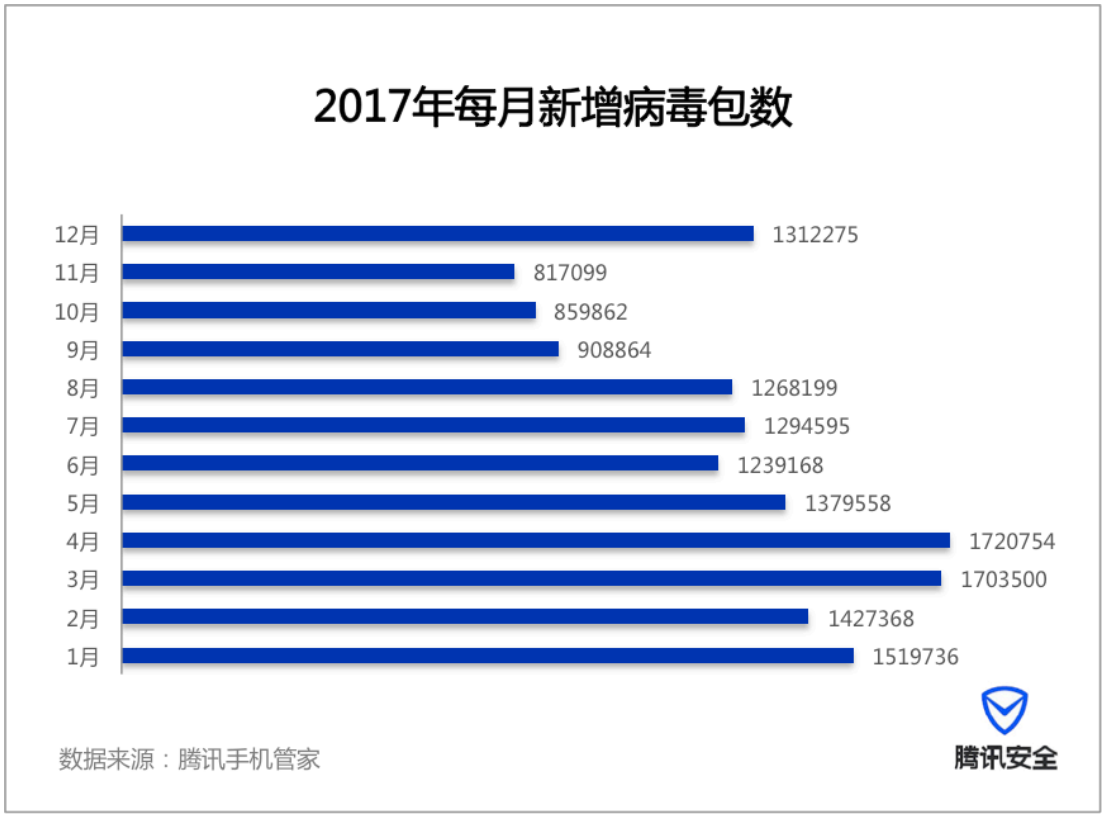
2017 年 12 月，腾讯安全反病毒实验室安全团队率先在全球范围内捕获了一例病毒样本，并顺藤摸瓜捕获了一个潜伏了 17 年之久的 0day 漏洞——该病毒利用 Office 公式编辑器中的 0day 漏洞发动攻击，潜伏期长达 17 年之久，威胁大量 Office 版本，一旦用户打开恶意文档，无需其他操作，就会被植入后门木马，被不法分子完全控制电脑。

在移动安全快速变化的当下，一些看似影响不大的单个漏洞耦合在一起也会产生新的风险。2017 年 12 月 7 日，腾讯安全玄武实验就基于此发现“应用克隆”攻击威胁模型，可以轻松“克隆”用户账户，窃取隐私信息，盗取账号及资金等。对此，腾讯玄武实验室第一时间向 CNCERT（国家互联网应急中心）报送了相关的漏洞，并与 2018 年 1 月 9 日联合知道创宇召开技术研究发布会，提醒大家注意移动安全风险。

2.5 全年查杀 Android 病毒 12.4 亿次，手机支付类病毒下降近八成

2.5.1 移动端病毒包增长呈波动下降趋势，新增病毒总数达 1545 万

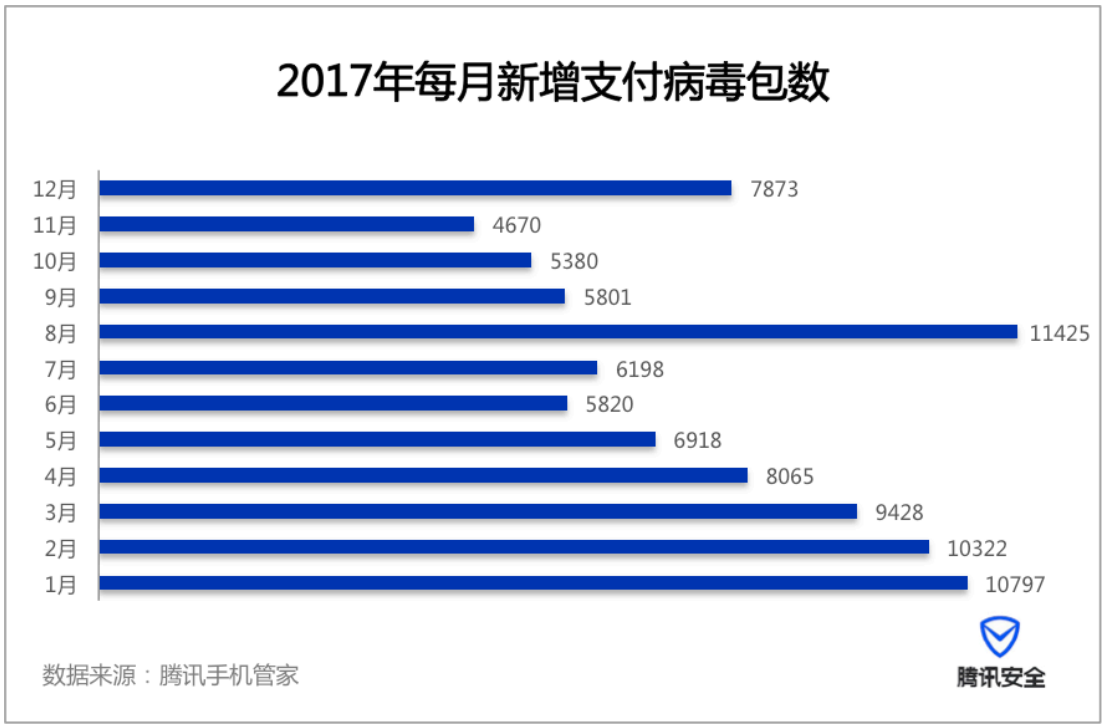
2017 年腾讯手机管家截获 Android 新增病毒包总数达 1545 万，相较 2016 年下降近二成。



基于全年来看，新增病毒包数整体呈现波动下降趋势，但 12 月大幅激增到 130 万，达到下半年峰值。

2.5.2 全年新增手机支付类病毒包总数 92697，占总新增病毒包 0.6%

2017 年全年共新增支付类病毒包总数为 92697，同比下降 79.6%，占总新增病毒包数的 0.6%。



2.5.3 2017 年染毒手机用户数超 1.88 亿

2017 年手机病毒感染用户量整体呈下降趋势，总数为 1.88 亿，相较 2016 年同比下降 62.4%。

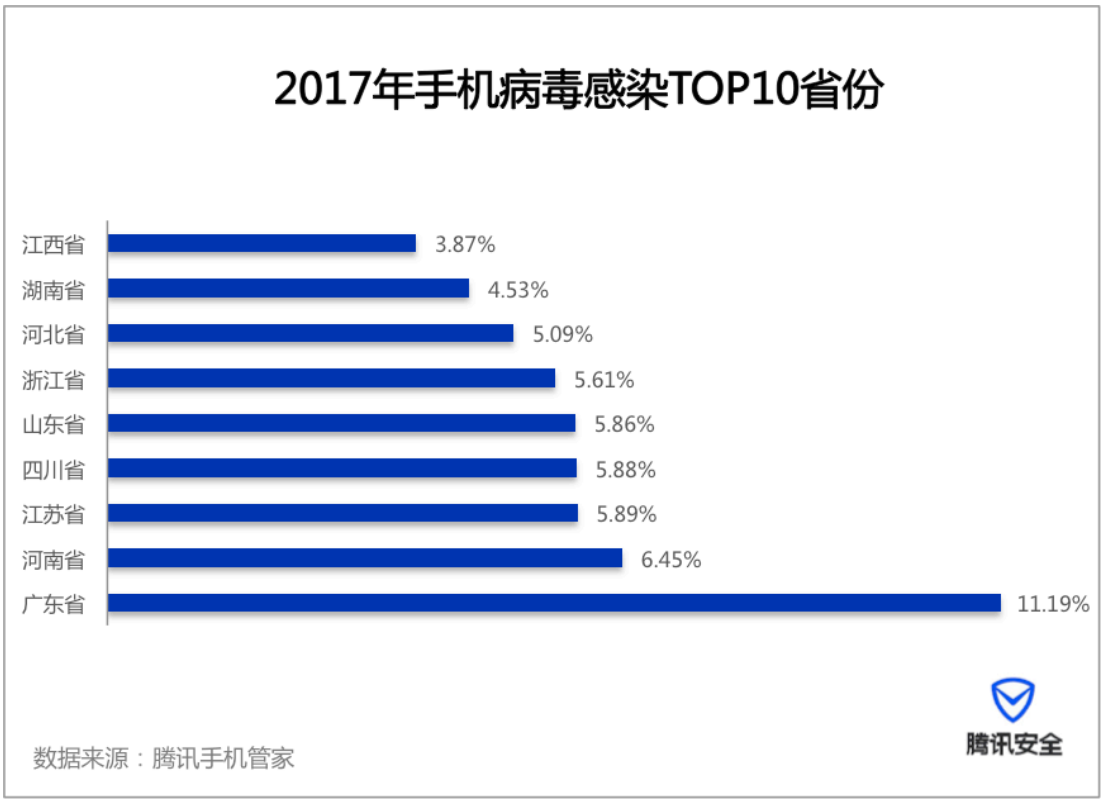
2017 年 1 月单月感染用户数达到 2166 万，为全年最高纪录；下半年用户病毒感染情况整体优于上半年，但 7 月和 12 月出现了两个染毒高峰。

2.5.4 2017 年腾讯手机管家共查杀 Android 病毒 12.4 亿次

在病毒感染用户数大幅下降的情况下，2017 年腾讯手机管家查杀病毒次数达到 12.4 亿次，基于全年来看手机病毒查杀次数呈现降低趋势。

2.5.5 移动端中毒用户数量广东居首

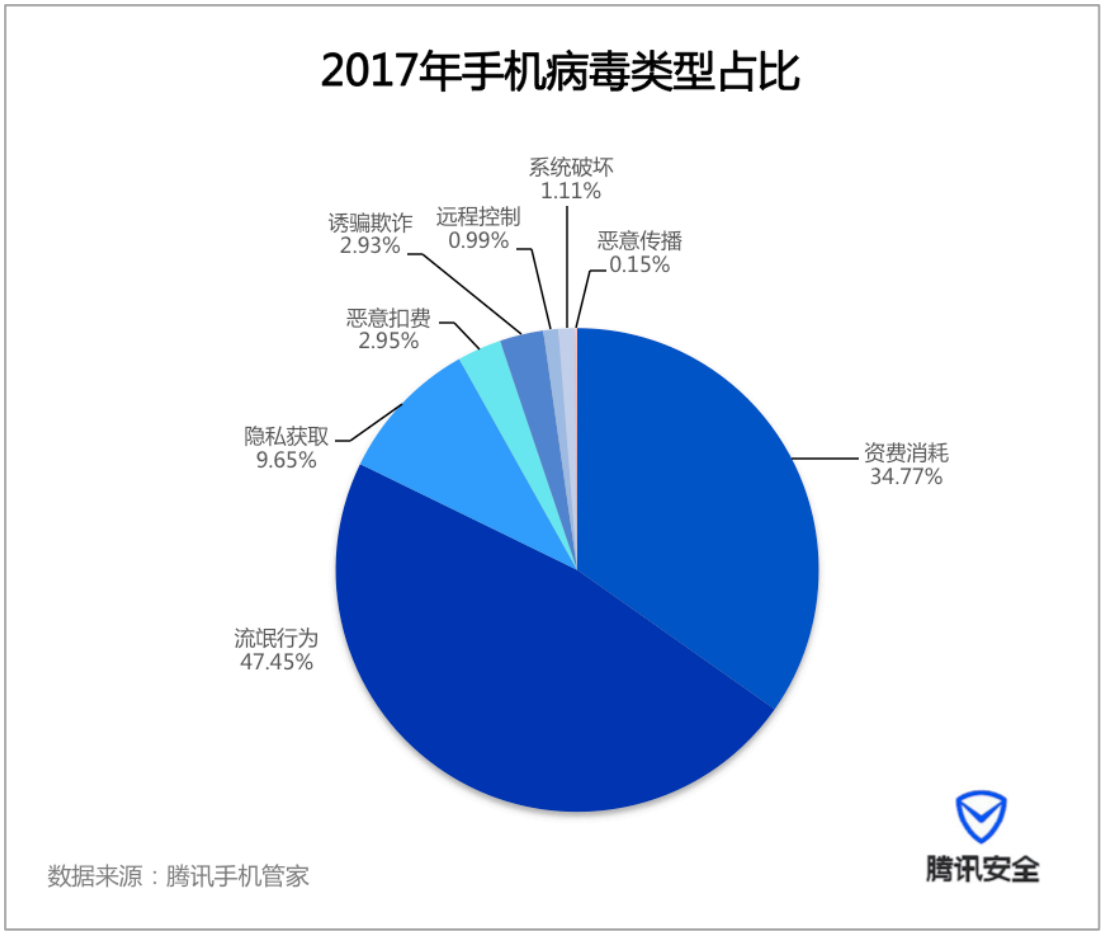
在感染手机病毒的用户地域分布方面，广东排名第一，占比高达 11.19%。



2.5.6 流氓行为和资源占比超 80%，手机资源站为病毒主要渠道来源

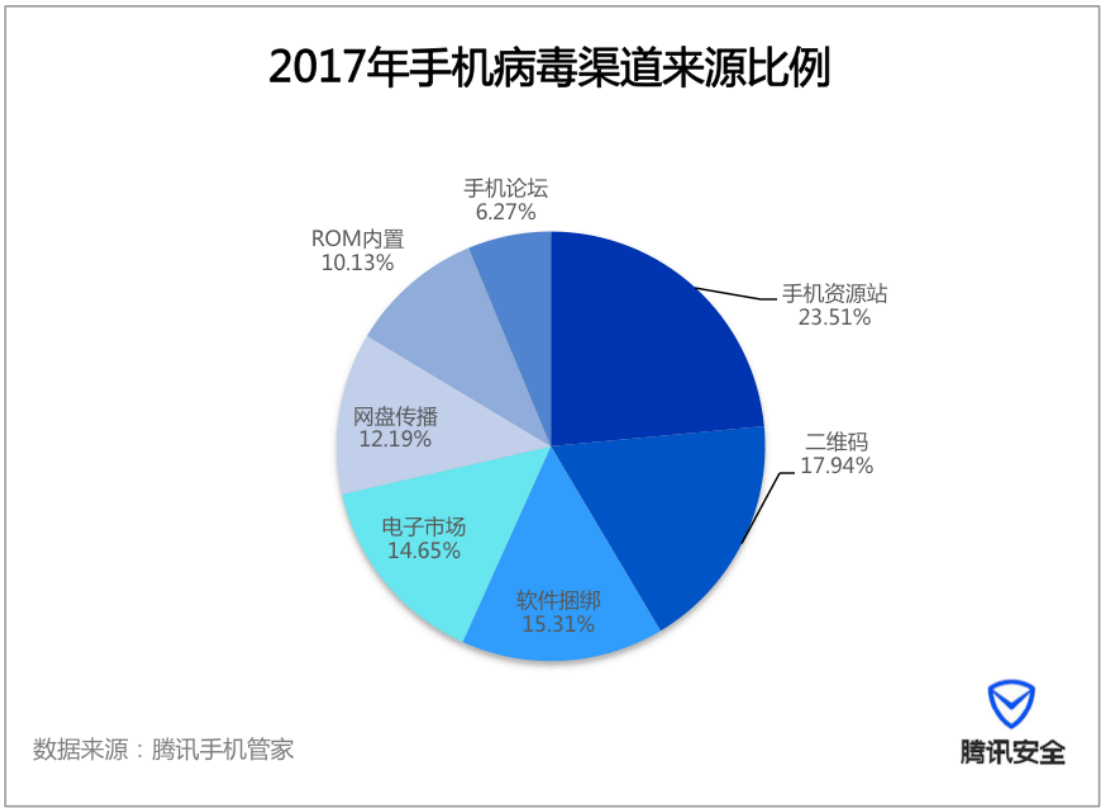
2.5.6.1 移动端病毒中流氓行为和资费消耗占比超 80%

2017 年手机病毒类型比例中 ,流氓行为和资费消耗占比最高 ,以 47.45%和 34.77%的比例分列一、二位。排名第三的隐私获取同样占据了 9.65%，恶意扣费、诱骗欺诈、远程控制、系统破坏和恶意传播占比分别为 2.95%、2.93%、0.99%、1.11%和 0.15%。



2.5.6.2 手机资源站、二维码是手机病毒主要渠道来源

手机病毒渠道来源主要有七大类，分别是手机资源站、二维码、软件捆绑、电子市场、网盘传播、ROM 内置和手机论坛。病毒渠道入口的分散化与多元化，也进一步增加了用户染毒的几率与风险。



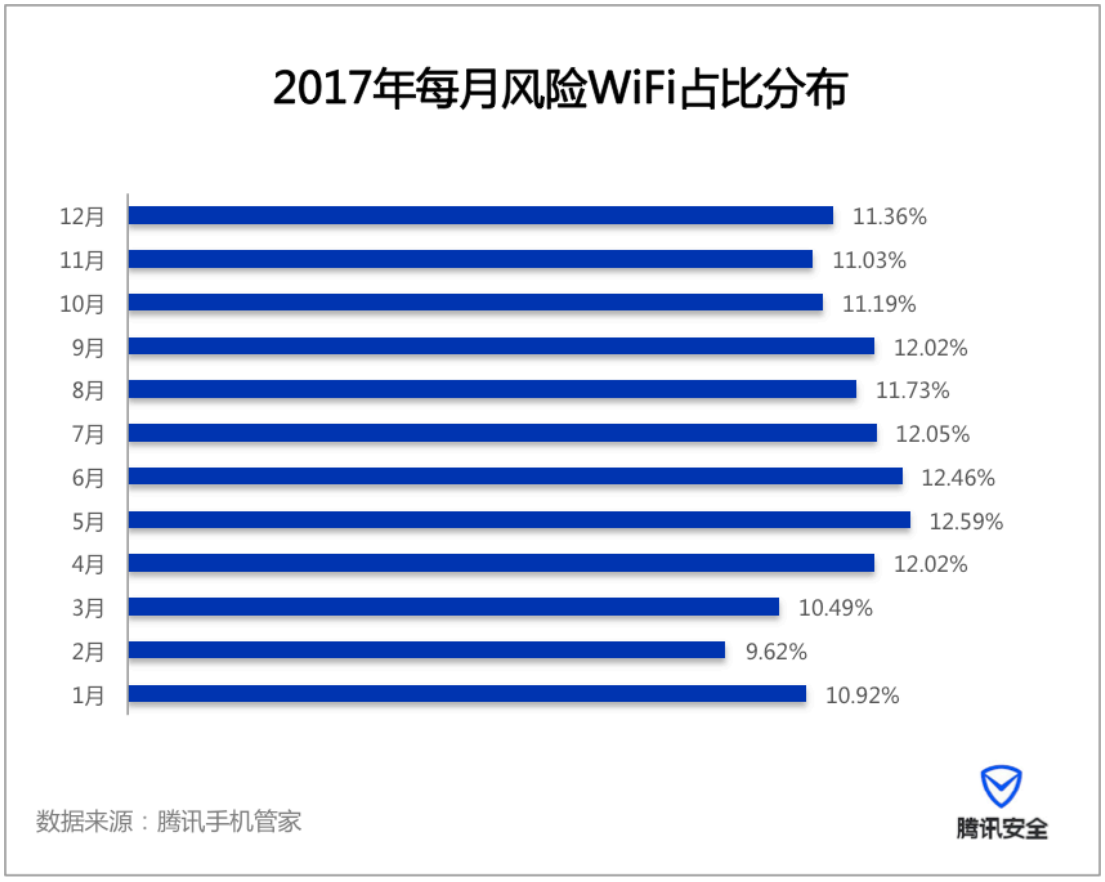
值得注意的是，手机资源站由上半年的第五上升为第一大手机病毒传播渠道。手机资源站一般为非官方型应用下载网站，这些下载站无任何安全检测措施，甚至主动内置手机病毒和木马，以情色 App 诱惑用户下载安装。

2.6 公共 WiFi 建设井喷：总数已超 3.36 亿成为用户基本需求

2.6.1 2017 年公共 WiFi 总数超过 3.36 亿

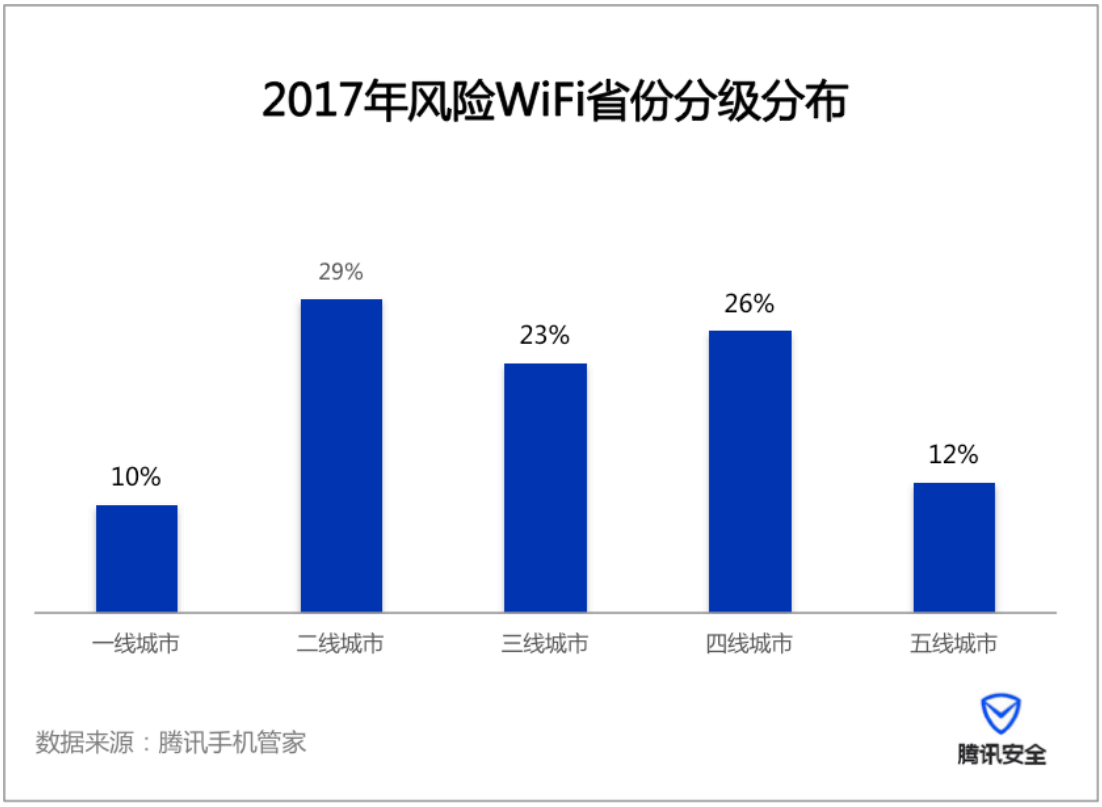
随着移动互联网的迅猛发展、智能终端的深入渗透，WiFi覆盖率进一步深入各大城市，用户对于WiFi的使用率进一步提升。与此同时，WiFi的风险形势不容忽视。根据腾讯安全移动安全实验室数据显示，从整体趋势来看，2017年我国风险WiFi数呈现缓慢

增长趋势，2月风险WiFi占整体比例为9.62%，是全年最低占比，5月占比达12.59%，为全年最高占比，二者相差不大。风险WiFi平均每月占总体的11.46%。



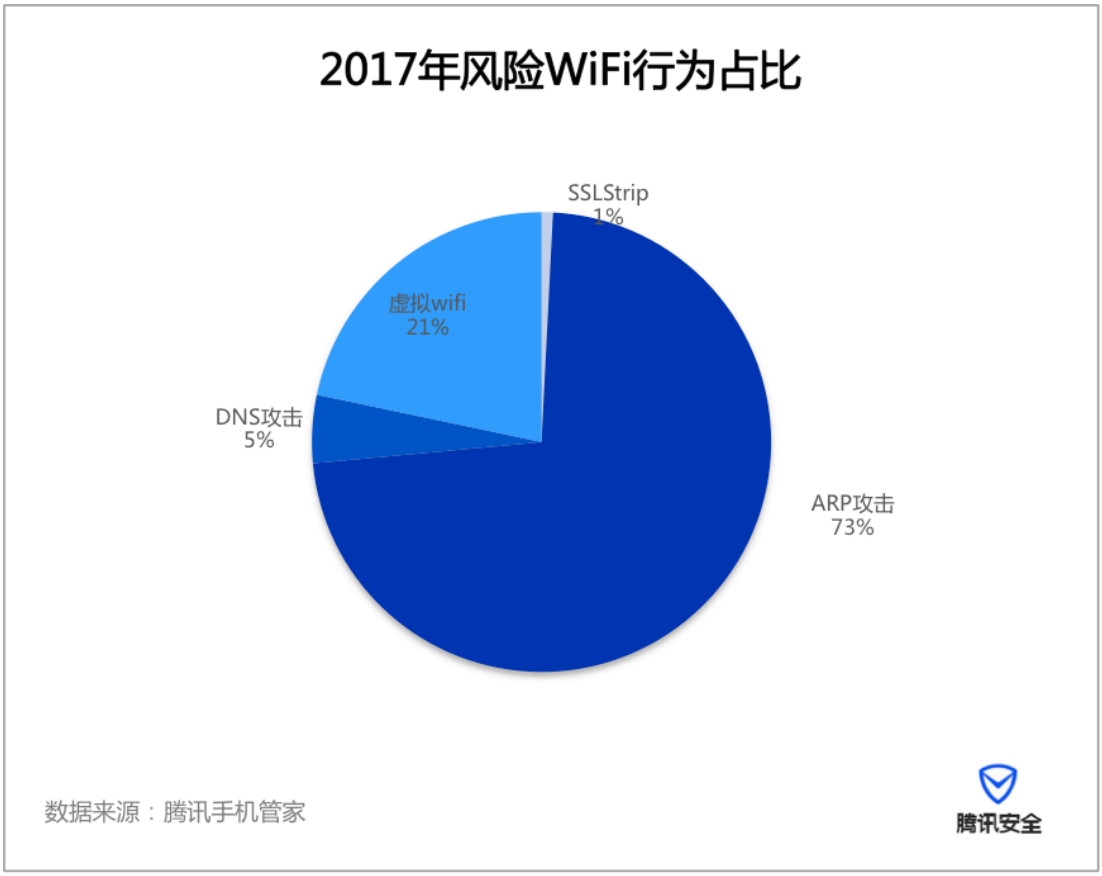
2.6.2 风险 WiFi 中一线城市占比 10%，二、三、四线城市 WiFi 风险更高

在风险 WiFi 的城市分布占比调查中，一线城市占比为 10%，而二线、三线、四线城市占比分别达到 29%、23%、26%，WiFi 使用风险均超过一线城市。



2.6.3 APR 攻击为第一大风险 WiFi 行为，占比达到 73%

根据数据统计，风险WiFi主要类别分为ARP中间人攻击、DNS攻击、ARP攻击、SSLStrip。其中，ARP中间人攻击是主流，占风险WiFi类型比例达到73%，另外，虚拟WiFi占比21%，DNS攻击占比5%。


2017年风险WiFi行为占比
SSLStrip
1%
虚拟wifi
21%
DNS攻击
5%
ARP攻击
73%
数据来源：腾讯手机管家
腾讯安全

三、2017 反网络黑产诈骗初具成效，网络传销形势依旧严峻

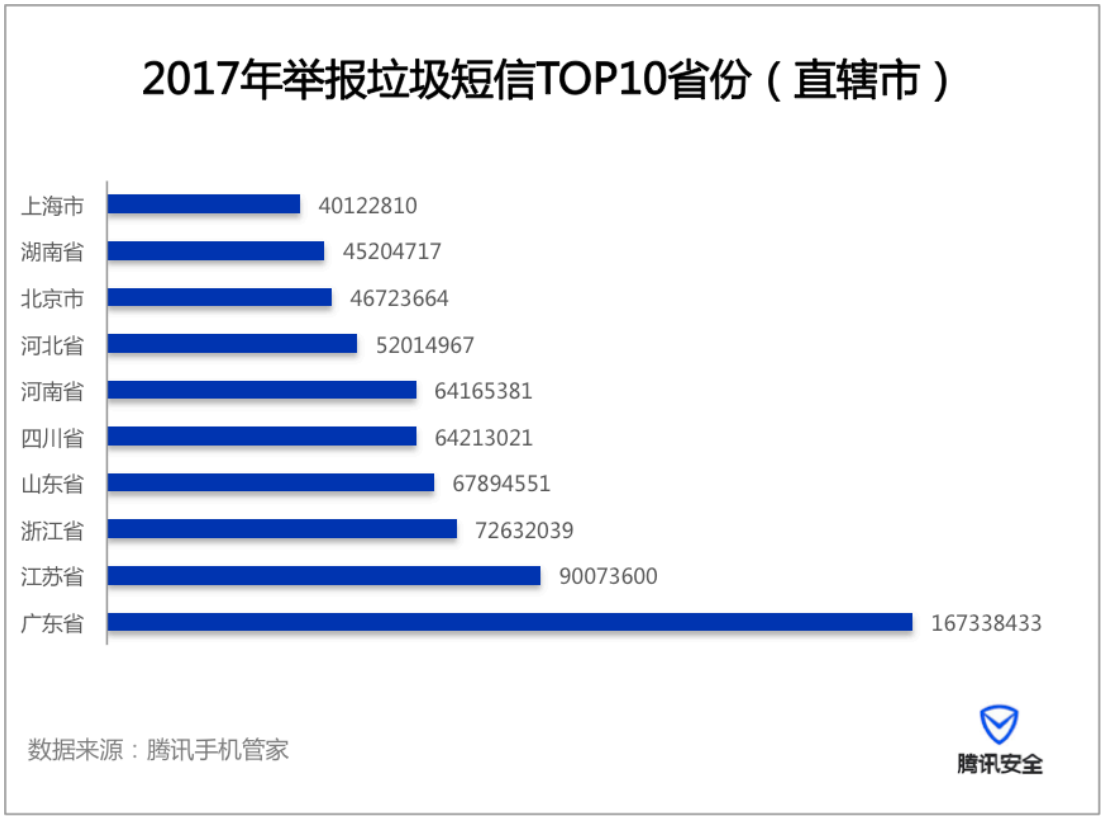
3.1 举报垃圾短信超 13.8 亿条，非法诈骗类短信一家独大

3.1.1 2017 年用户举报垃圾短信数达 13.8 亿条，同比增长近 30%

较低的传播成本及其背后存在的巨大利益链，导致垃圾短信一直难以得到有效整治，用户举报数也是有增无减。2017 年，腾讯手机管家共收到用户举报垃圾短信数 13.8 亿条，同比增长近 30%；其中诈骗类短信总数为 4433 万。

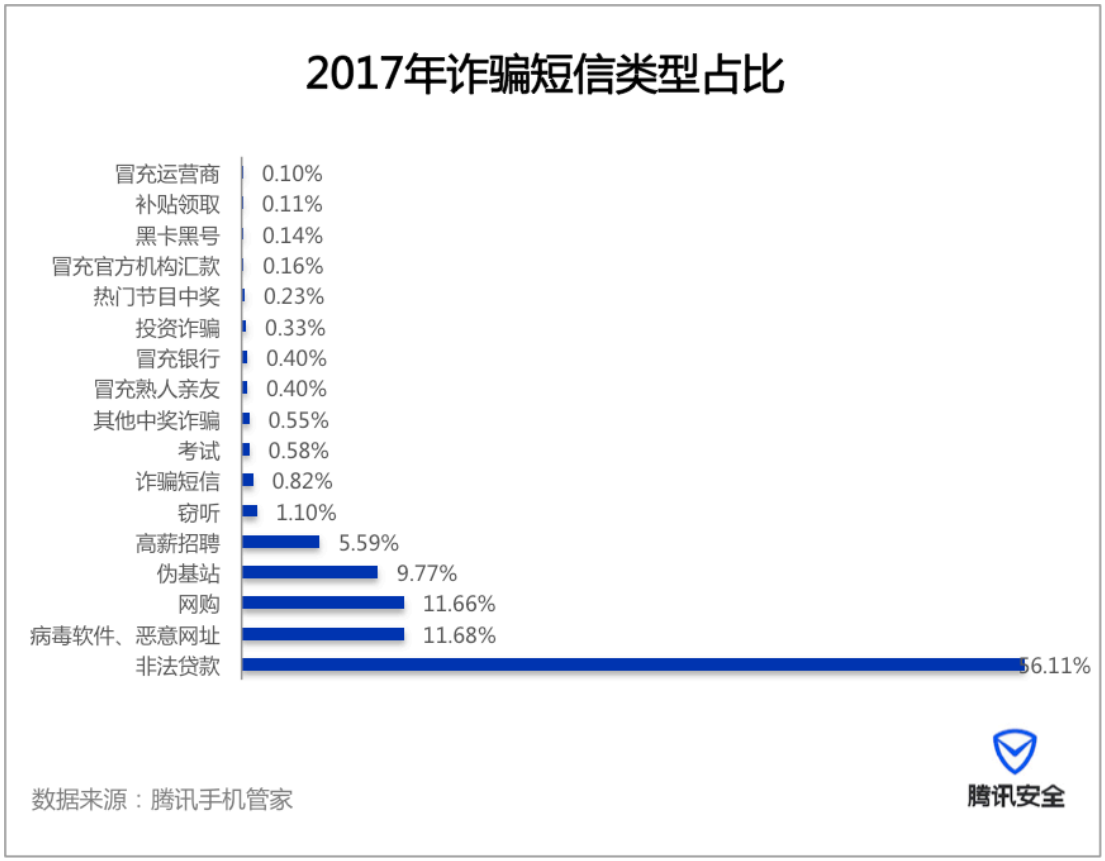
3.1.2 用户举报垃圾短信最多的省份为广东，最多的城市为深圳

在垃圾短信的地域省份分布方面，用户举报垃圾短信最多的前三省份分别为广东、江苏和浙江，其中广东省举报垃圾短信数达 1.67 亿。此外山东、四川、河南、河北、北京和湖南同样位列前十。这些省份或直辖市普遍分布在东部沿海和中部地区，人口密集和经济发达是它们最大的共同点，这也为诈骗分子批量发送垃圾短信并牟取利益创造了有利条件。



3.1.3 非法贷款是最常见的诈骗短信类型

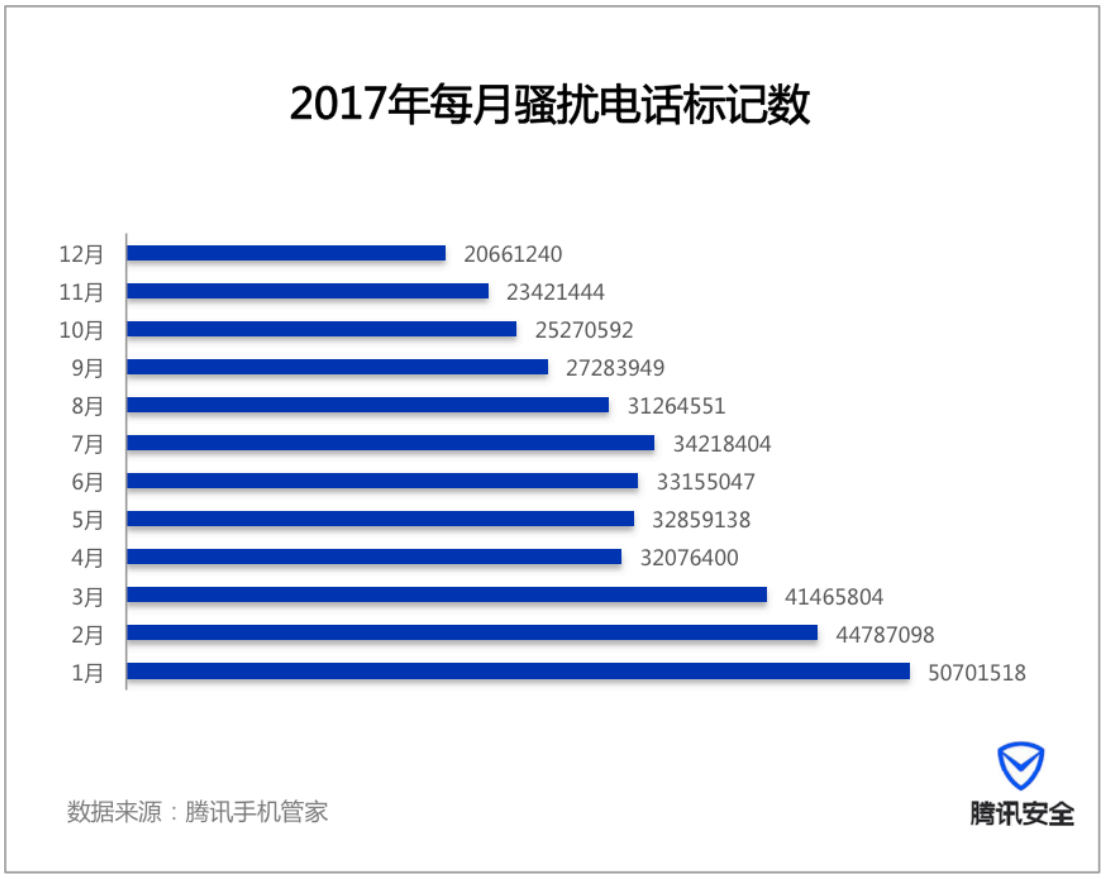
诈骗短信的手段多样化和隐秘性强使其危害性始终高居不下。据腾讯手机管家监测到的 4246 万条诈骗短信显示，非法贷款、病毒软件及恶意网址、网购和伪基站是占比最高的几大诈骗短信类型。



3.2 骚扰电话用户标记量达 3.97 亿次，同比下降 33.4%

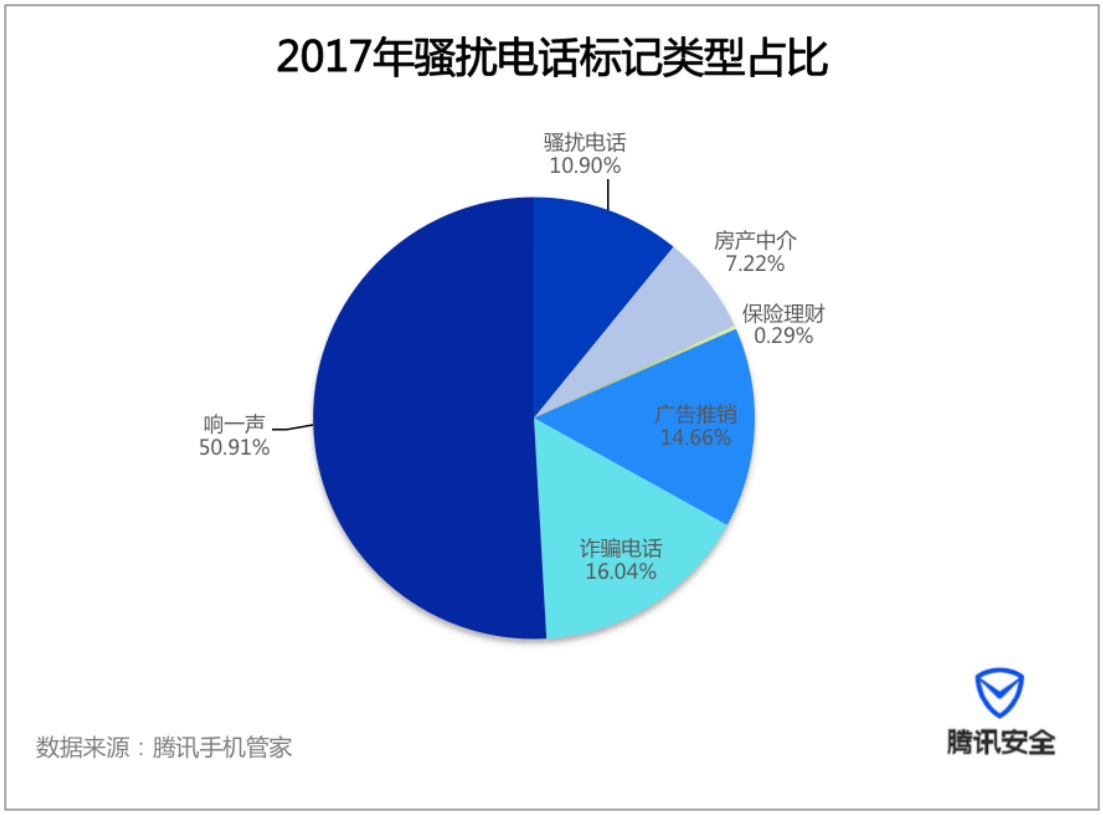
3.2.1 2017 年用户共标记骚扰电话 3.97 亿次，同比下降 33.4%

在经历了 2015 年的爆发式增长后，2016 年开始，骚扰电话标记数呈现逐年下降趋势，2017 年全年骚扰电话标记总数为 3.97 亿次，相较 2016 年同比下降 33.4%。



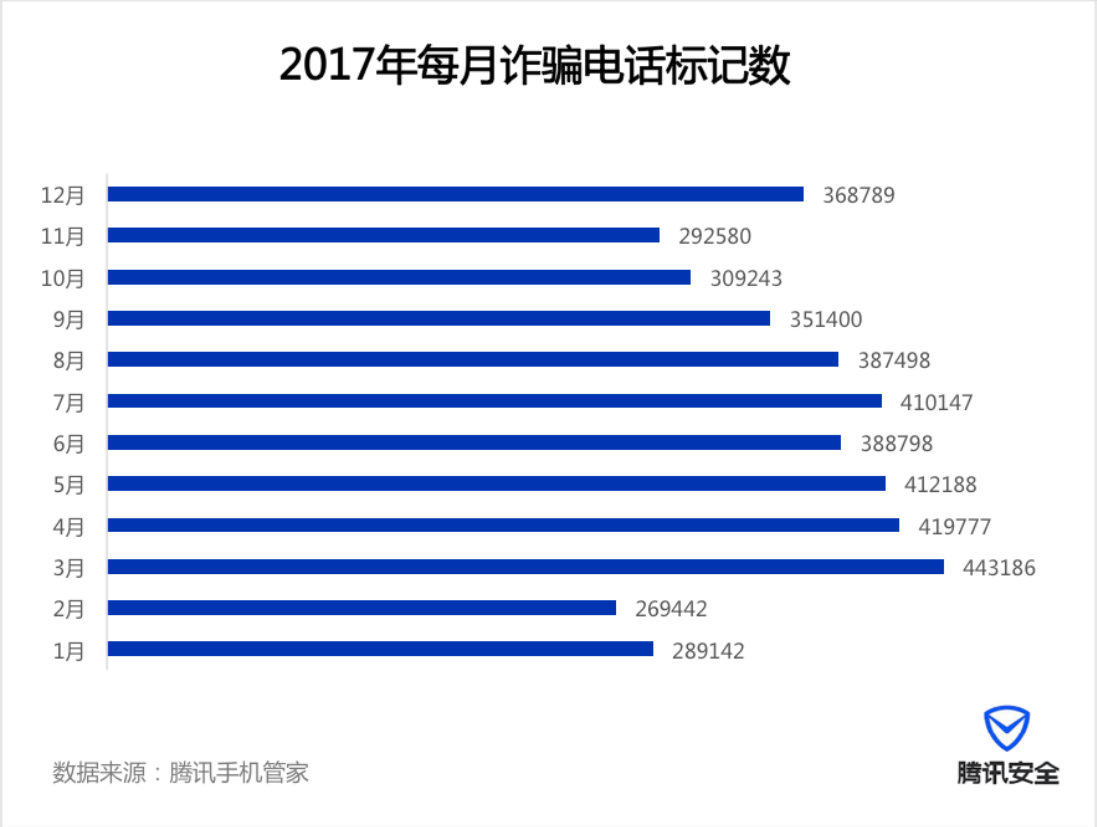
3.2.2 2017 年骚扰电话超过 50%为响一声

用户标记的骚扰电话类型主要分为 5 大类。其中 ,响一声排名第一 ,占比超过 50%。诈骗电话占比 16.04%，排名第二，此外广告推销、房产中介和保险理财等也占据了一定比例。

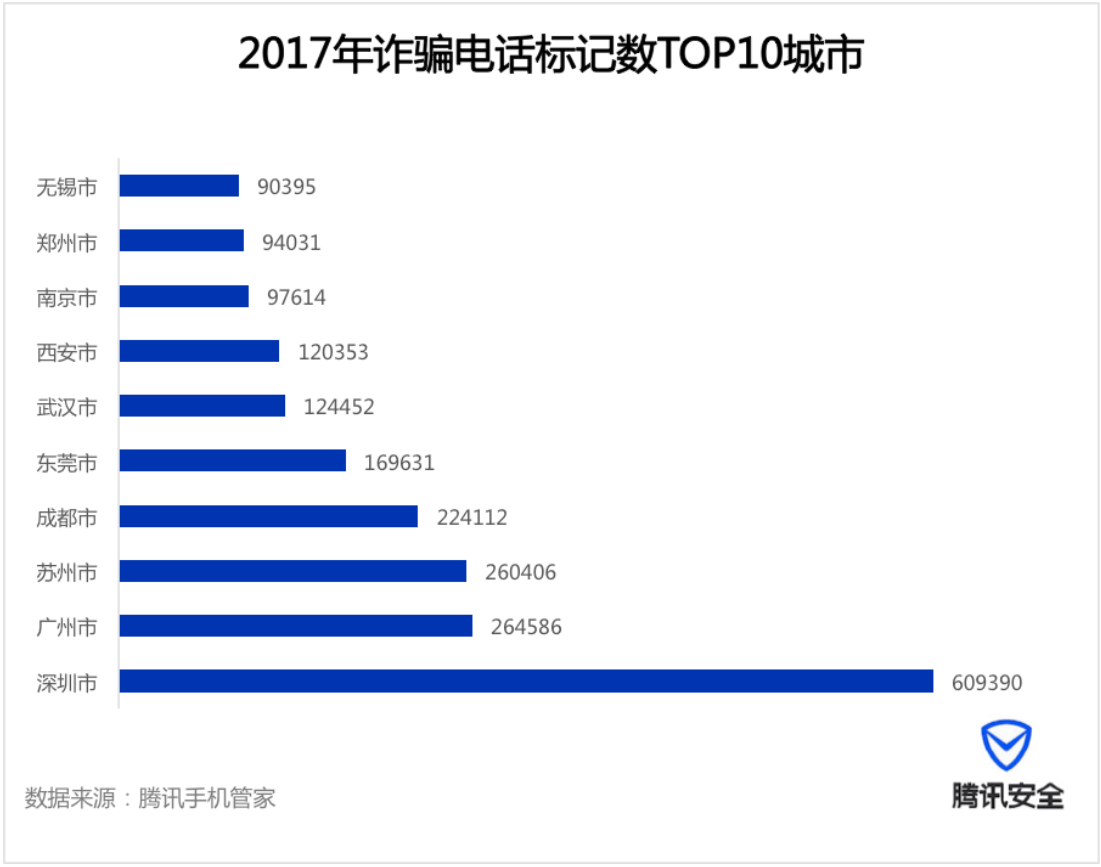


3.2.3 2017 年诈骗电话标记总数为 6716 万，深圳市最多

在用户已标记的 3.97 亿次骚扰电话中，诈骗类电话占比虽远不及响一声多，但其造成的实质性危害却最大。基于腾讯手机管家用户诈骗电话标记相关数据显示，2017 年诈骗电话标记总数为 6716 万，同比下降 46.2%。



这些诈骗电话针对的目标地域较为明确，以东部沿海经济发达地区与内陆中心省份为主。城市方面，深圳是诈骗电话标记数最多的城市，总数达 60.9 万。广州和苏州分别以 26.4 万和 26.1 万的标记数紧随其后。



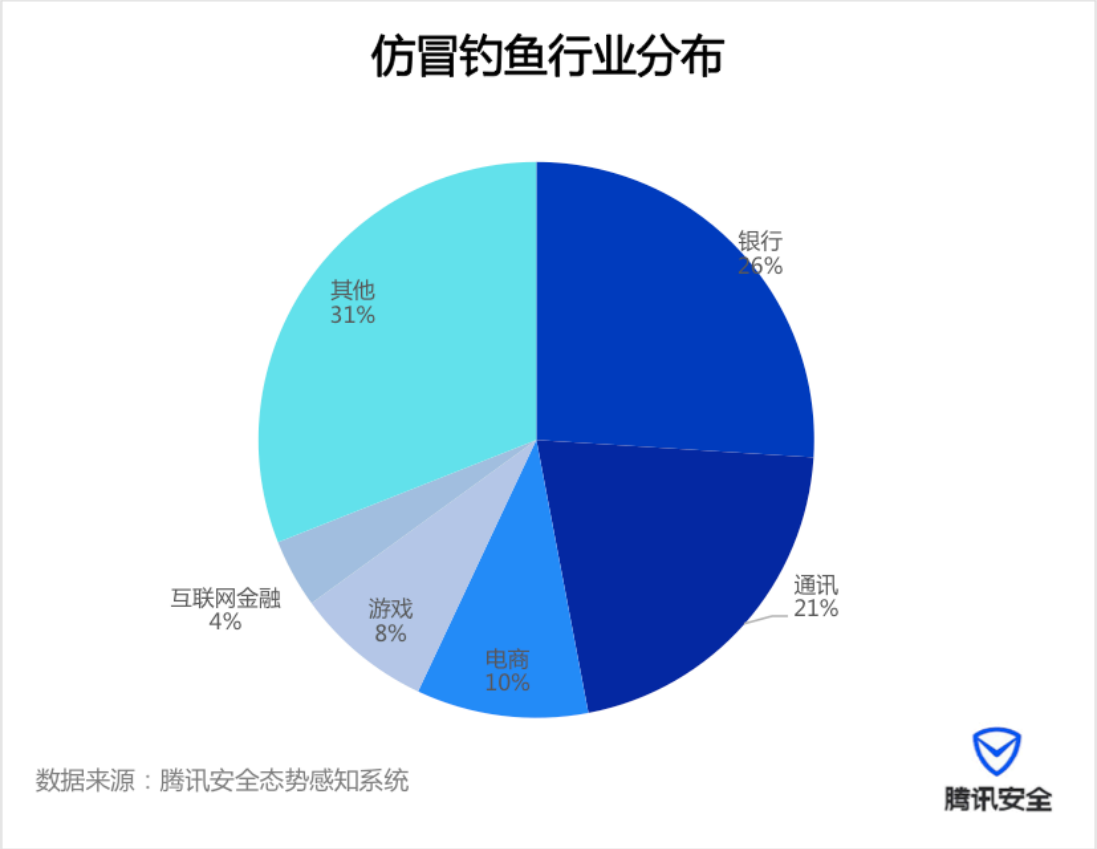
3.2.4 iOS 骚扰电话标记总数为 2573 万，整体呈下降趋势

从整体趋势上看，除了 12 月，iOS 骚扰电话标记数呈现波动下降趋势。1 月标记数最高，为 304.7 万次，11 月则只有 147 万次，为全年最低点。

值得注意的是，年底诈骗分子活动明显更为活跃，骚扰电话标记数 12 月一度激增到 218 万，也提醒民众需加强反骚扰诈骗意识。

3.3 累计拦截恶意网址访问 6729 亿次，色情及赌博类占比近 7 成

根据腾讯安全态势感知系统监测数据，2017 年全年新增识别恶意网址 7800 万，其中新增识别仿冒类诈骗网站 75 万，被仿冒网址数量前 5 名的行业是：银行、通信、电商、游戏、互联网金融。

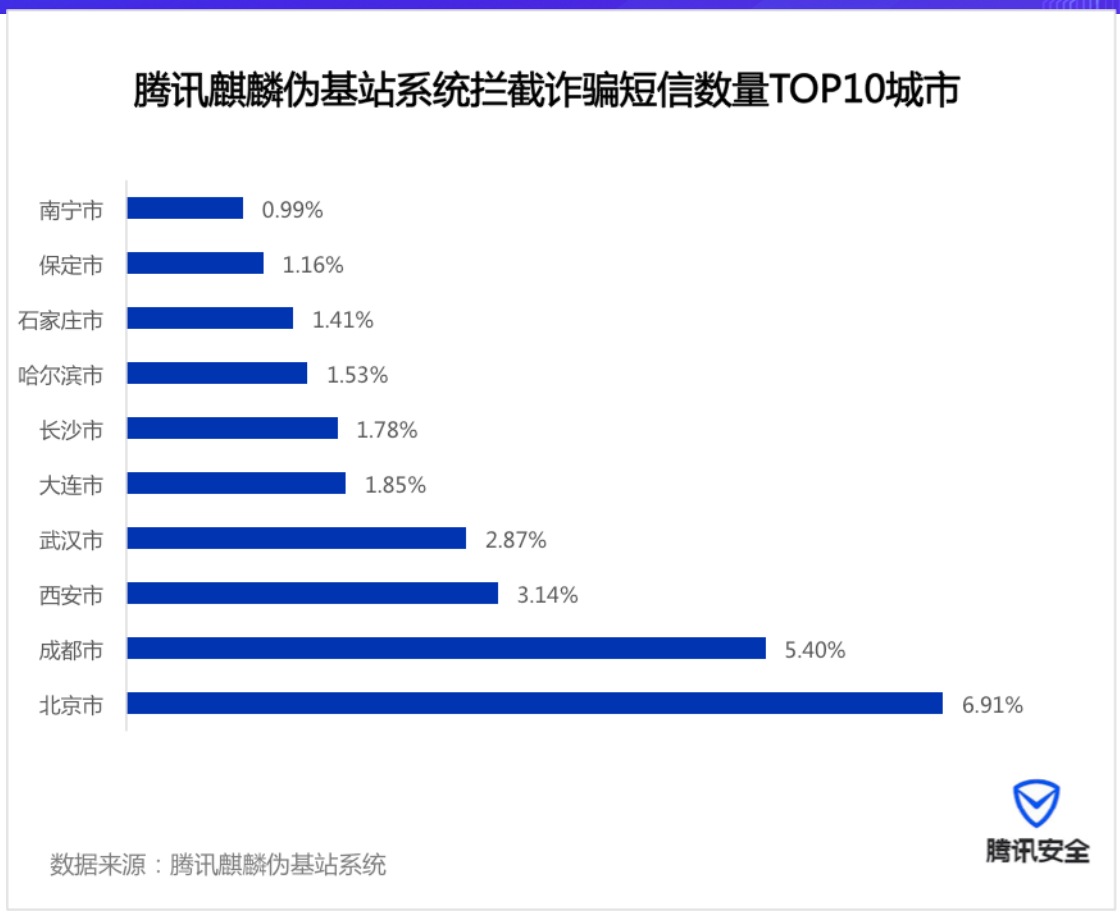


针对恶意网址威胁形势，腾讯神荼网址反诈骗系统在腾讯系产品以及外部 100 多家合作伙伴渠道里累计拦截恶意网址访问 6729 亿次 其中拦截虚假色情网站访问 3100 多亿次、网络赌博类网站访问 1600 多亿次。为了扩大网址拦截的覆盖面，神荼和各地公安展开合作，能有效降低当地网络诈骗案件数 40%-70%。

3.4 伪基站瞄准经济发达地区，银行及电信运营商成最大仿冒对象

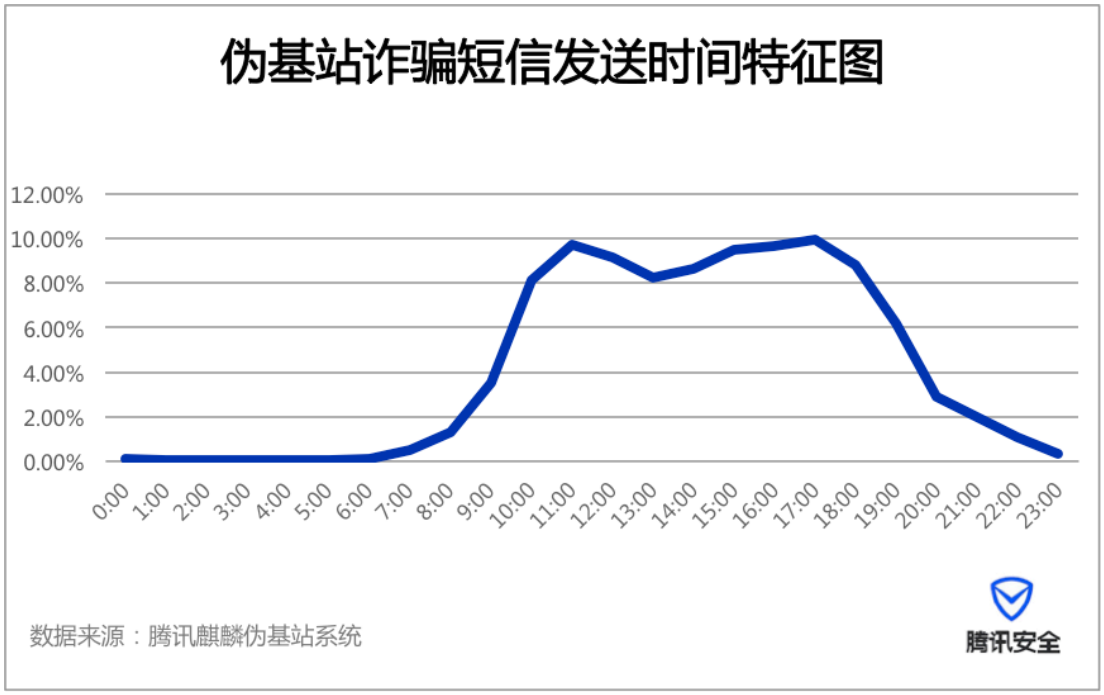
3.4.1 伪基站地域特征：北京、成都占比最多

从城市来看，拦截诈骗短信数量 Top 10 的城市如北京、成都、西安等几乎均为省会城市或经济较发达城市，由于人口密集、城市居民收入较高，被伪基站诈骗团伙列入重点攻击对象。



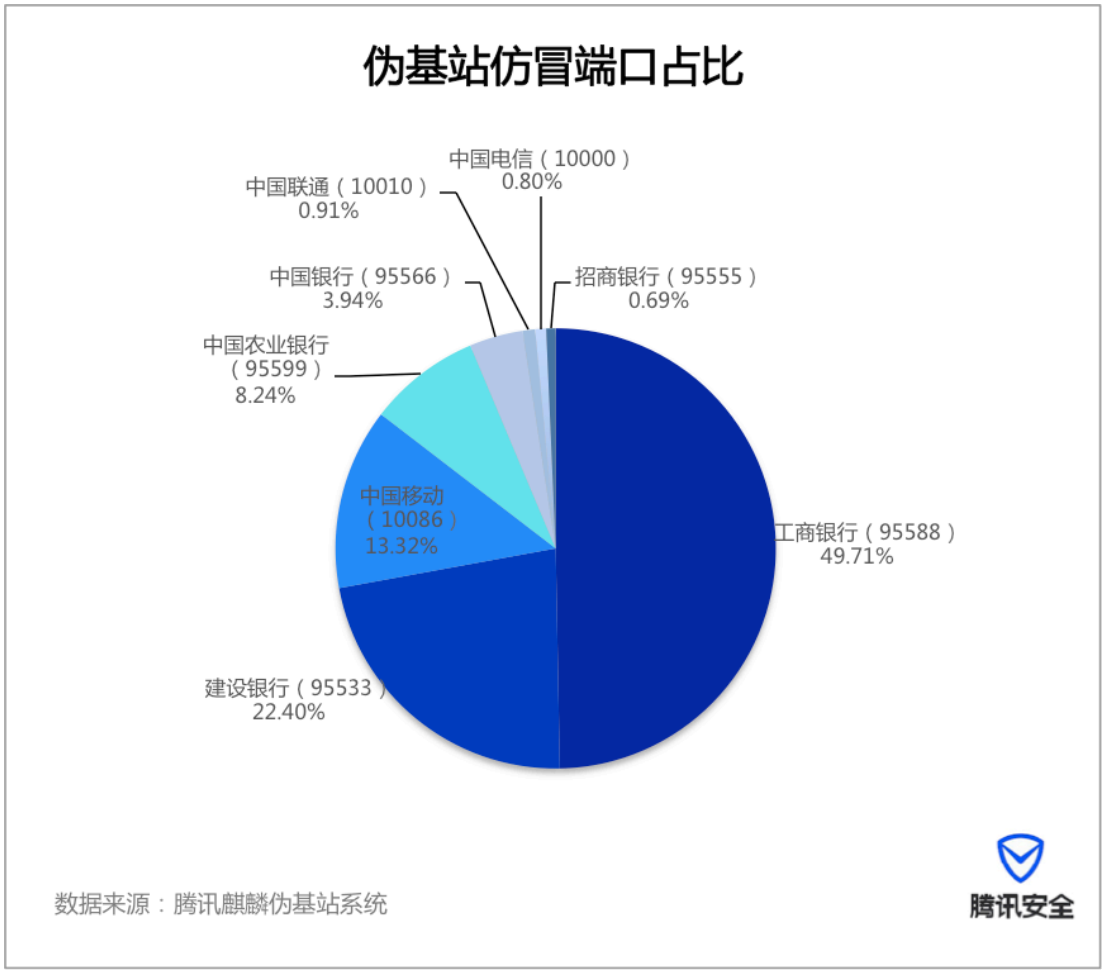
3.4.2 伪基站作案时间特征：工作时间最频繁

从作案时间来看，伪基站诈骗短信发送之间集中在上午 9 时至下午 19 时，其中又以上午 10 时至 12 时、下午 15 时至 18 时为两个高峰。不难看出，诈骗短信高峰期与每日工作时段相合。



3.4.3 内容特征：工商银行、中国移动最“躺枪”

腾讯麒麟拦截的伪基站仿冒端口中，仿冒工商银行的诈骗短信最多（高达 49%），Top 5 仿冒端口除中农工建四大银行，还有运营商中国移动。不难看出，这些“躺枪”的企业是因为用户群体巨大，业务模式中短信息又尤为重要，因此成为伪基站诈骗团伙主要模拟的发送对象。



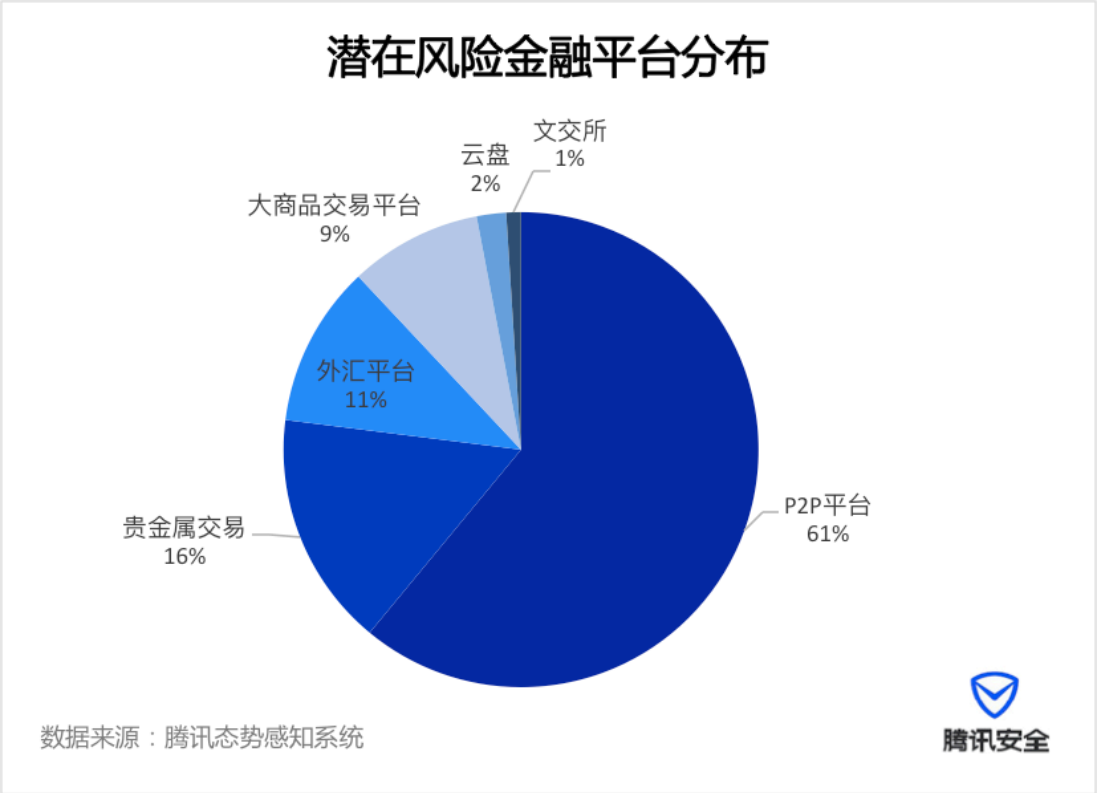
3.5 网络金融诈骗引入传销手法 P2P 平台潜在风险最高

在互联网+金融快速发展的同时，各种金融领域的诈骗手法、擦边球模式也逐渐进入公众视野，从传统的以信用卡代办、小额贷款办理为由骗取小额手续费，到各种如非法集资、非法外汇交易、非法贵金属等期货交易等。特别是金融诈骗引入传销手法，更是危害严重，比如虚拟币传销、非法集资传销、商城返利传销等。

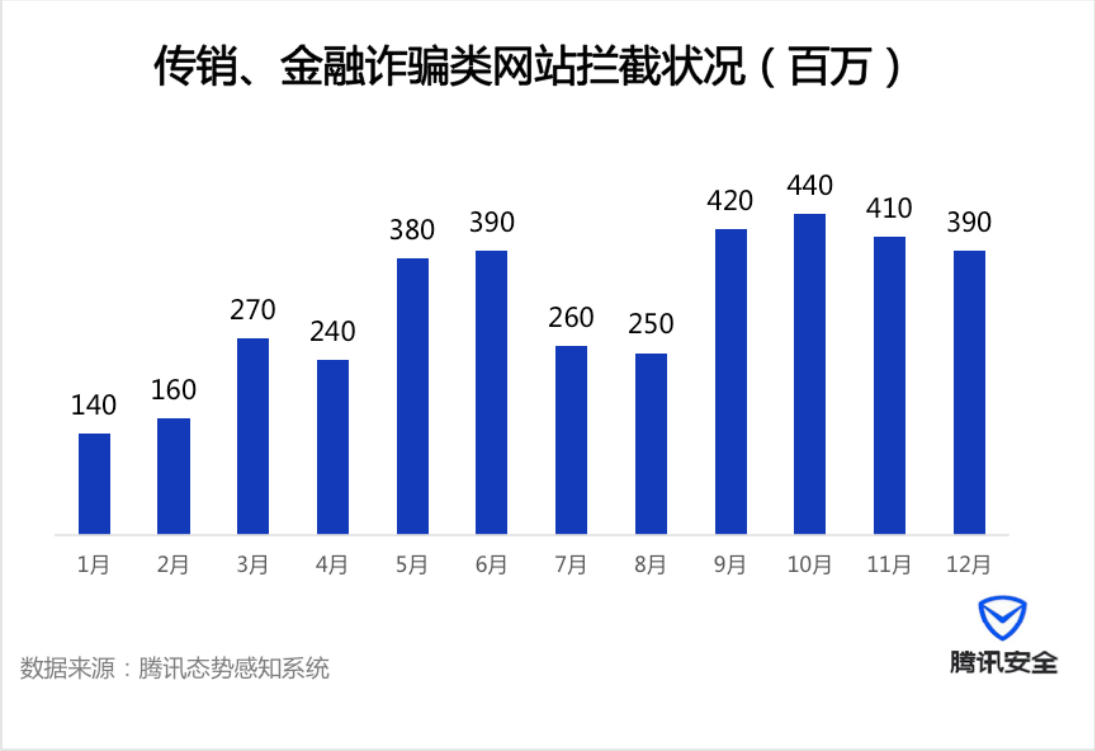
2017 年，出现多起以“慈善”、“互助”、“复利”等为噱头的新型金融传销案件，为社会构成严重影响。2017 年 7 月，大型传销组织“善心汇”被查处。该组织打

着“扶贫救济,均富共生”的幌子，以发展人员的数量作为获取提成的依据，骗取大量财物。此外，2017 年 12 月曝光的钱宝网，以高额收益为诱饵，要求投资者缴纳保证金，之后可通过签到、做任务、分享链接等方式来获取高收益，涉案金额或达百亿。

2017 年，腾讯态势感知系统累计发现有潜在风险的金融平台数万家。



针对监管部门已经定性的传销、金融诈骗类网站，目前腾讯神荼会在所有覆盖渠道拦截，日均拦截访问达千万次。


传销、金融诈骗类网站拦截状况（百万）
140
160
270
240
380
390
260
250
420
440
410
390
1月
2月
3月
4月
5月
6月
7月
8月
9月
10月
11月
12月
数据来源：腾讯态势感知系统
腾讯安全

四、数字加密货币引发网络安全新问题

4.1 比特币等数字加密货币掀起 2017“炒币”风暴

数字加密货币（Digital Cryptocurrency）又称为加密货币，其特点在于利用密码学原理来确保交易安全及控制交易单位的创造，是数字货币（或称虚拟货币）中的一种，比如大家较为熟悉的比特币、莱特币和门罗币等等。自 2009 年世界上第一个比特币区块链诞生以来，各种数字加密货币层出不穷，目前已多达 1500 多种。2017 年“炒币”风暴来袭，也将比特币、以太坊、比特币现金的价格推至历史最高点。

#	名称	市值	价格	交易量（24小时）	流通供给量	变化量	价格图（7天）
1	Bitcoin	¥1,493,934,769,285	¥88,949.57	¥117,108,673,150	16,795,300 BTC	-5.04%	
2	Ethereum	¥763,167,660,666	¥7,875.32	¥57,278,080,050	96,906,234 ETH	-11.68%	
3	Ripple	¥424,269,376,890	¥10.95	¥27,560,233,450	38,739,142,811 XRP *	-9.95%	
4	Bitcoin Cash	¥275,593,543,116	¥16,302.20	¥16,322,594,365	16,905,300 BCH	0.37%	
5	Cardano	¥115,274,950,748	¥4.45	¥1,594,105,329	25,927,070,538 ADA *	-5.73%	
6	Litecoin	¥82,544,723,791	¥1,508.92	¥7,194,216,000	54,704,683 LTC	-5.38%	
7	NEM	¥77,913,359,272	¥8.66	¥653,109,696	8,999,999,999 XEM *	-5.67%	
8	IOTA	¥60,462,911,405	¥21.75	¥1,728,768,801	2,779,530,283 MIOTA *	-2.53%	
9	Stellar	¥56,097,975,182	¥3.14	¥1,586,937,179	17,889,943,656 XLM *	-7.43%	
10	Dash	¥51,525,368,675	¥6,596.46	¥1,305,065,972	7,811,067 DASH	-8.15%	
11	NEO	¥48,279,640,695	¥742.76	¥2,154,367,933	65,000,000 NEO *	-4.62%	

（数字加密货币市值排行-数据来源：coinmarketcap.com）

近年来升值最疯狂的莫过于比特币。比特币诞生之初，按当时的价格 1 美元可以买到大约 1300 个比特币，而今天比特币价格已经接近 1.5 万美元，最高时甚至接近 2 万

美元。目前比特币已被开采 1670 万个，约占总量的 79.90%。不断攀升的价格和日益减少的加密货币数量吸引越来越多人通过各种方式获取加密货币。

（2017 比特币交易价格走势图-数据来源：coinbase）

4.2 “勒索”、“盗窃”及“木马”成数字加密货币三大网络安全威胁

“挖矿”是最基本的获取数字加密货币的方式，然而想要通过“挖矿”获取更多的币，唯一的途径是提升算力。但前期的资金投入是非常巨大的，以一个中型矿场（1 万台矿机）为例，一台普通的矿机约 2.5 万人民币，仅前期机器采购费用就高达 2.5 亿人民币，而后期持续的电费、维护费也是数额巨大。

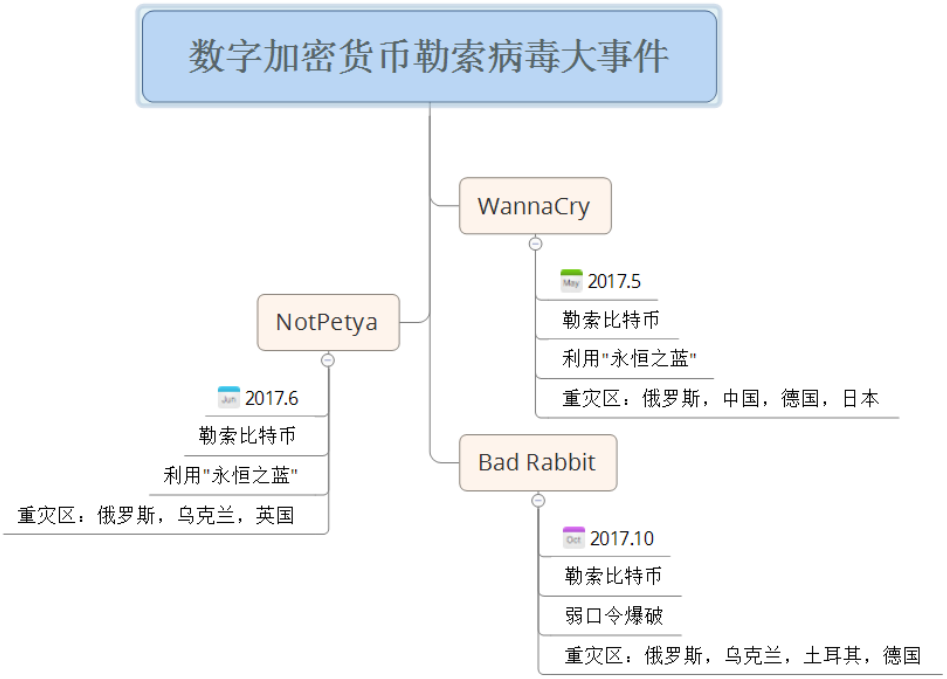
进入 2017 年，由数字加密货币引发的互联网安全问题频频爆发，不法分子看中数字加密货币的匿名性，使用勒索、盗窃、非法挖矿等手段获取了大量不义之财。

4.2.1 勒索

2017 年 5 月，WannaCry 勒索病毒借助“永恒之蓝”漏洞肆虐全球，是数字加密货币广泛进入群众视野的关键性事件。这次安全事件中，中毒用户被要求在 72 小时内

支付价值 300 美元的比特币。据相关报道，WannaCry 勒索病毒给全球造成的损失超 80 亿美元。

随着“永恒之蓝”漏洞逐渐修复，勒索病毒也开始寻找其它新的的传播手段，2017 年 10 月爆发的 Bad Rabbit（坏兔子）勒索病毒就使用了挂马的方式：攻击者首先入侵新闻媒体类网站，随后利用这些新闻类网站发起水坑攻击，当用户浏览这些网站时便会被诱导下载病毒。Bad Rabbit 同样要求受害者在 40 小时内支付 0.05 比特币（当时约合 300 美元）。



（2017 数字加密货币勒索病毒大事件时间轴）

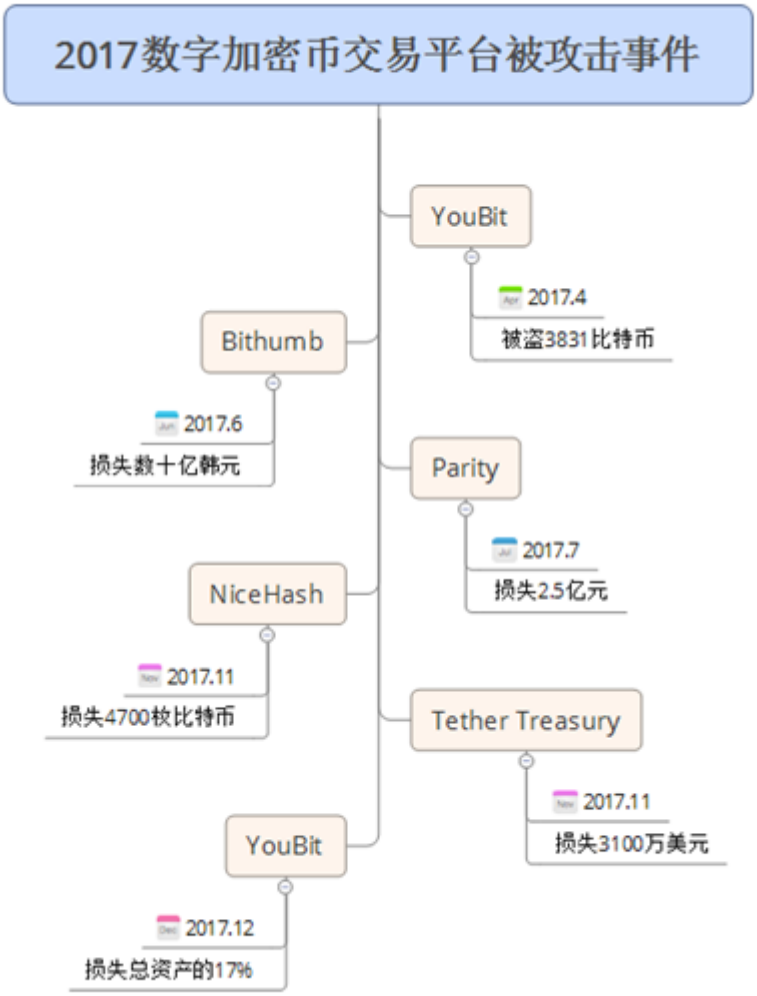
4.2.2 盗窃

除了勒索病毒造成的损失，盗窃行为也同样可对数字加密货币持有者造成大量损失，

从数字加密货币诞生初期，数字加密货币被盗的新闻就层出不穷。

1）交易平台被黑

2017 年，数字加密货币交易平台遭入侵的新闻屡见不鲜。比如韩国 YouBit 数字加密货币交易平台今年就曾遭到两次入侵：2017 年 4 月的第一次入侵造成 YouBit 近 4000 比特币的损失，按当时的价格，总损失价值约为 360 万美元；第二次入侵发生 2017 年 12 月，此次事件也导致 YouBit 交易平台破产倒闭。



（2017 数字加密币交易平台被攻击时间轴）

2）个人钱包被黑

2017 年伴随着数字加密货币的价格飙涨，不法分子更是无孔不入，试图利用各种黑客技术盗取个人及交易平台钱包密码，转走加密货币。

4.2.3 挖矿木马

整个 2017 年行业内频频爆出各种挖矿木马，且木马隐藏手段也越来越高明，实现了从“裸奔”到“隐身”的升级。

“裸奔期”：僵尸网络挖矿

上半年“裸奔期”，挖矿木马没有隐藏在普通软件中，而是成为僵尸网络的一个新拓展“业务”，做到了挖矿、DDoS 两不误。

2017 年 5 月发现的“Adylkuzz”僵尸网络，甚至比“WannaCry”出现的时间要早，影响了全球几十万台机器，有意思的是，“Adylkuzz”入侵成功后会利用“永恒之蓝”漏洞阻止其他病毒也利用此类漏洞，这在一定程度上限制了“WannaCry”的传播。木马入侵成功后，就会链接 C&C 服务器，接受挖矿指令，已知该木马目前专门挖取门罗币。

（Adylkuzz 挖矿协议）

“遮掩期”：植入普通软件挖矿

下半年“遮掩期”，挖矿木马开始隐藏到浏览器、插件、外挂辅助等普通软件进行传播。

1） 浏览器插件挖矿

2017 年年底，一个名为 Archive Poster 的浏览器插件被爆植入挖矿木马，影响数十万台用户机器。Archive Poster 的功能是协助用户在社交平台“汤不热”上进行多账号协作，其开发商表示说，经过调查发现起因是一名团队前成员的邮箱被入侵，导致产品被植入挖矿木马。

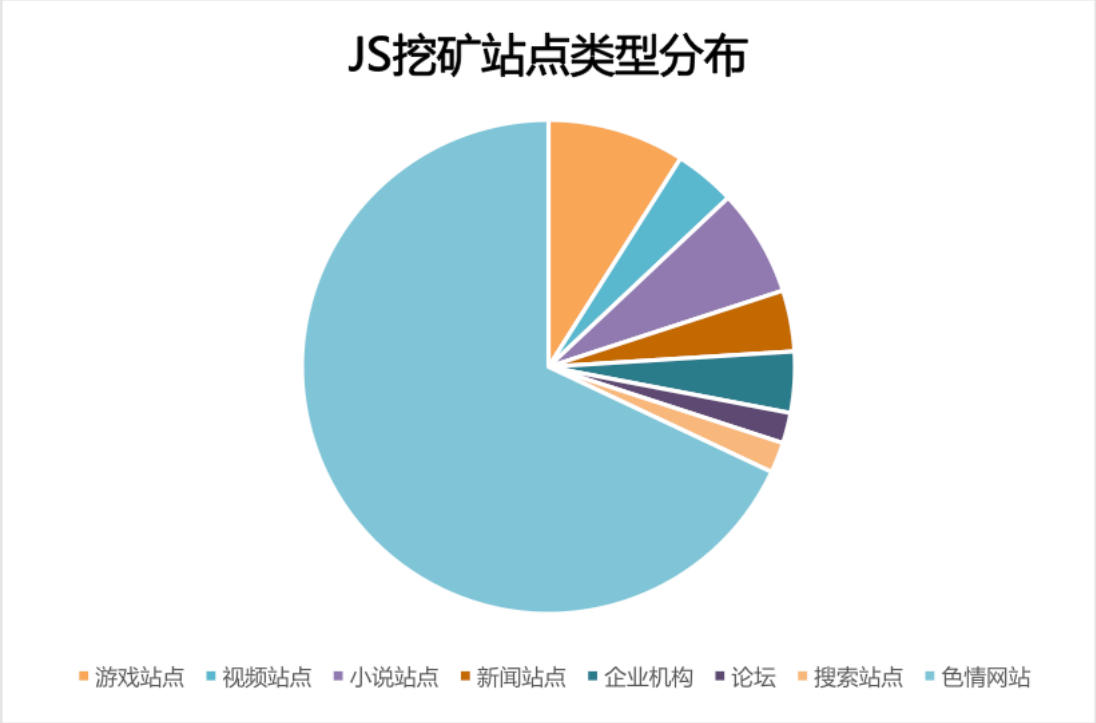
2）外挂辅助挖矿

在 2017 年年底腾讯电脑管家发现一款名为“tlMiner”的挖矿木马，隐藏在《绝地求生》辅助程序中进行传播。由于《绝地求生》游戏对电脑性能要求较高，不法分子瞄准《绝地求生》玩家电脑，相当于找到了“绝佳”的挖矿机器。该木马由一游戏辅助团队投放，单日影响用户高达 20 万。

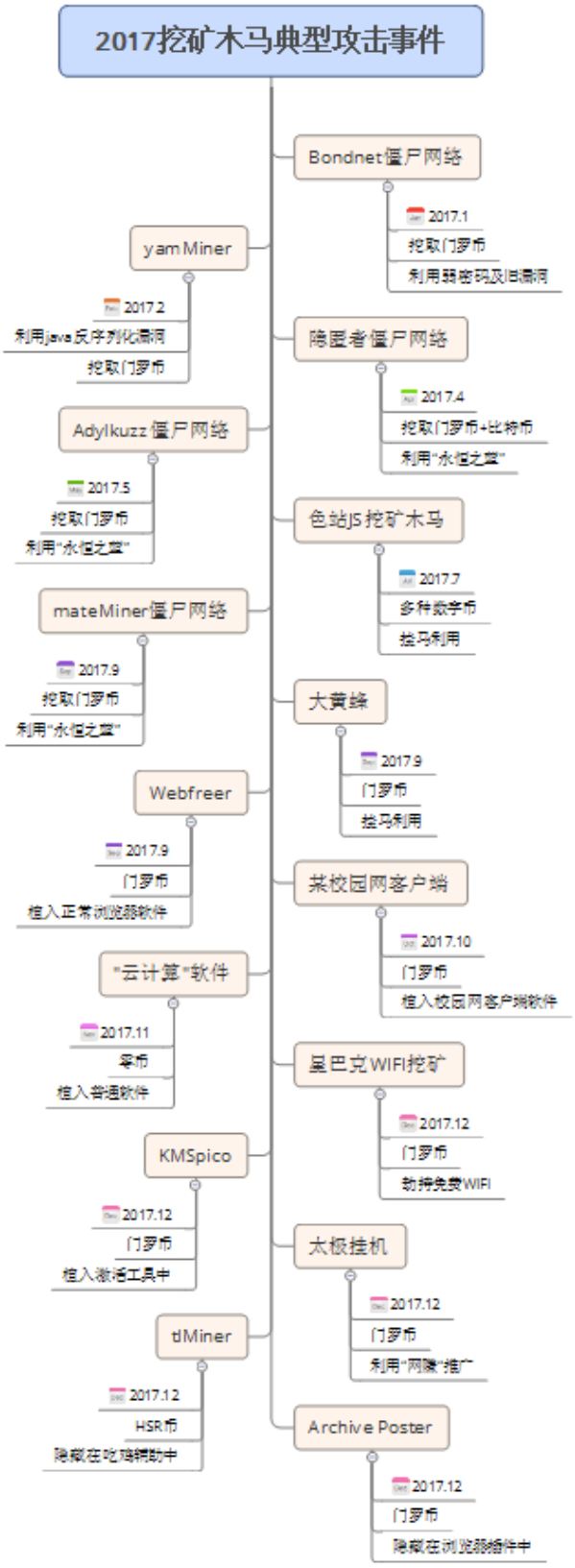
“隐身期”：网页挖矿

下半年“隐身期”，挖矿木马不再有可执行文件落地，而是直接嵌入在网页中，在用户上网看小说、看视频的同时“隐身”后台偷偷干活。

2017 年 9 月 ,数百个色情、小说、游戏网站在其网页内嵌了挖矿 JavaScript 脚本，用户一旦进入此类网站 ,JS 脚本就会自动执行 ,占用大量的机器资源挖取数字加密货币，导致电脑异常卡顿。



（JS 挖矿站点类型分布图）



（2017 挖矿木马典型攻击时间轴）

通过观察 2017 挖矿木马攻击事件也可以发现，不法分子最喜爱挖的数字加密货币不是比特币，而是门罗币，目前单枚门罗币的交易价格在 2500 人民币以上。

（门罗币走势-数据来源：coinmarketcap.com）

4.3 数字加密货币未来安全态势

随着数字加密货币价格持续上涨、挖取难度不断增大、数字加密货币数量越来越少，可以预见 2018 年由数字加密货币而起的犯罪活动或将呈现高发态势。

1、传播手段

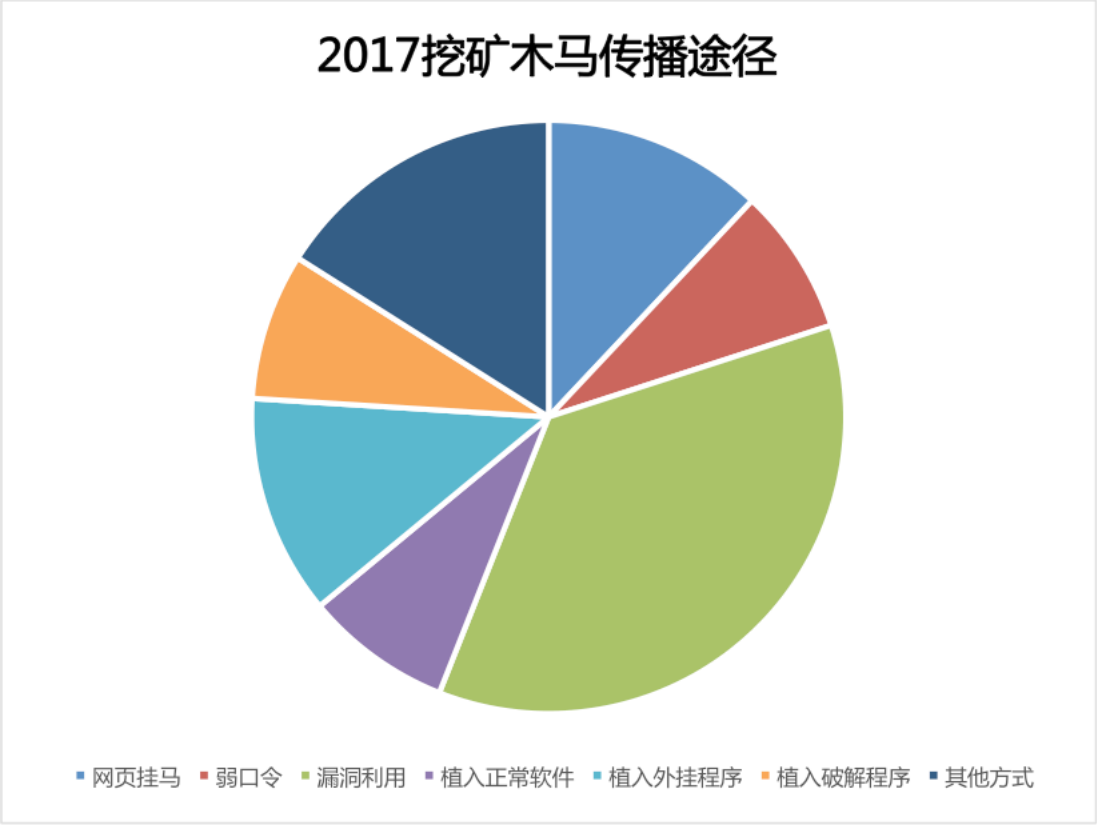
漏洞利用因其传播速度快、影响面广，在 2018 年仍然会是不法分子获取数字加密货币的重要手段。

2、获利手段

数字加密货币持有量少的用户，将可能不再是黑客主要攻击对象。2018 年或将出现大量针对团体以及持大量数字加密货币用户的 APT 攻击。针对普通网民，黑客更倾向在其电脑植入挖矿木马。

3、隐藏手段

隐藏在网页中的挖矿脚本，由于没有可执行文件落地，隐秘性极高，2018 年或将会有越来越多的挖矿脚本隐藏在各类网站进行挖矿。此外，部分玩家对游戏辅助的“青睐”，也将促使不法分子将更多恶意程序植入到游戏辅助等常规软件中。



（2017 年挖矿木马主要传播途径）

五、网络攻击加剧企业安全危机，治理机制亟需改善

5.1 针对企业的病毒攻击方式呈多样化发展

5.1.1 勒索病毒席卷全球 150 个国家，严重威胁办公安全

5 月 12 日，“WannaCry”勒索病毒在全球范围内进行大规模攻击，这是史上影响最广，危害最大的勒索程序，也成为本年度对企业办公安全危害最广的恶意程序。

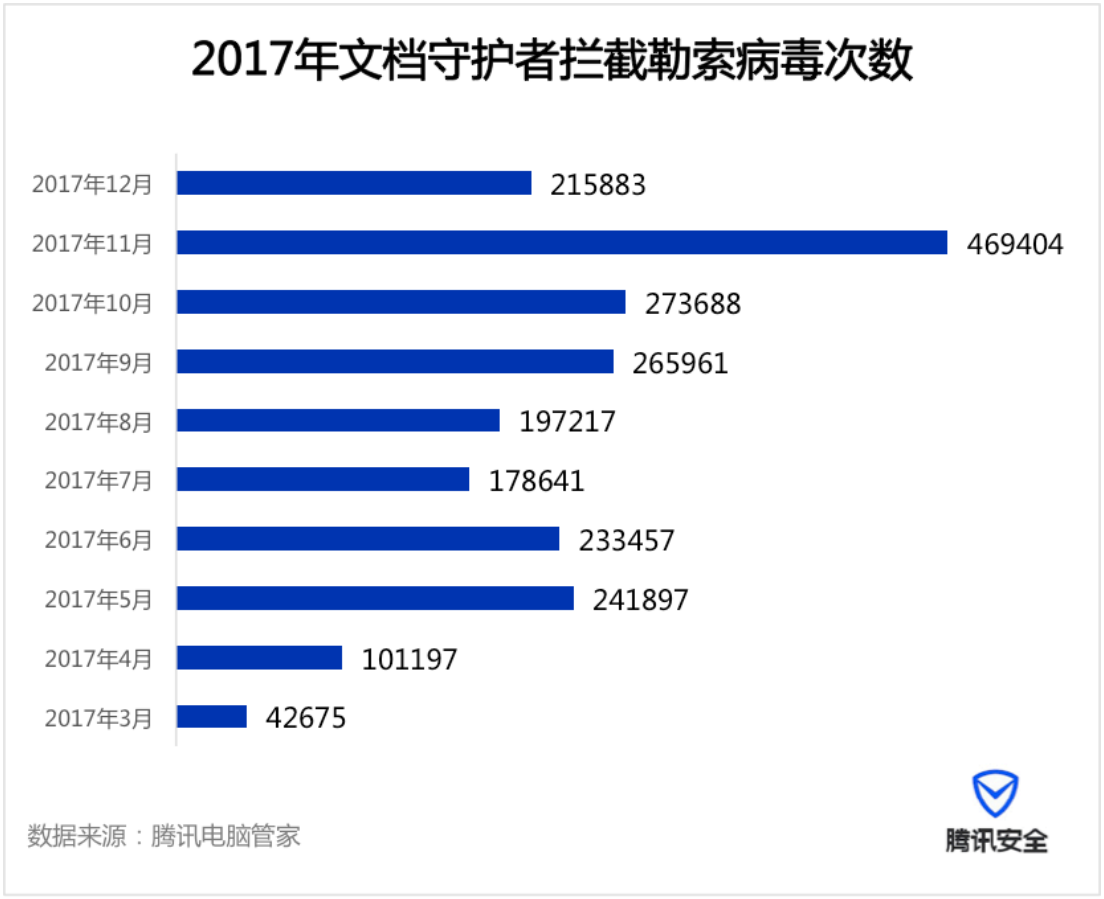
“WannaCry”勒索病毒通过加密形式，锁定个人电脑里的 txt、doc、ppt、xls 等后缀名类型的文档，要求支付 300 美金等价的比特币才能解锁文件，大量企业重要数据及个人用户工作文档被加密，严重阻碍企业正常运营；此外，勒索病毒还与挖矿机（运算生成虚拟货币）、远控木马组团传播，形成一个集合挖矿、远控、勒索多种恶意行为的木马病毒“大礼包”，针对高性能服务器挖矿牟利，中招电脑 CPU 被大量损耗，系统变卡变慢。

5.1.1.1 2017 年腾讯电脑管家文档守护者每周保护文档量达 74 亿

2017 年勒索病毒爆发期间，腾讯安全团队迅速推出勒索病毒免疫工具和文档守护者工具，为用户提供了事前防御、事中拦截、事后恢复的全套解决方案。据数据统计，腾讯电脑管家文档守护者平均每周保护文档量达 74 亿，全年开启文档守护者进行备份和防护的用户量超过 1.3 亿。

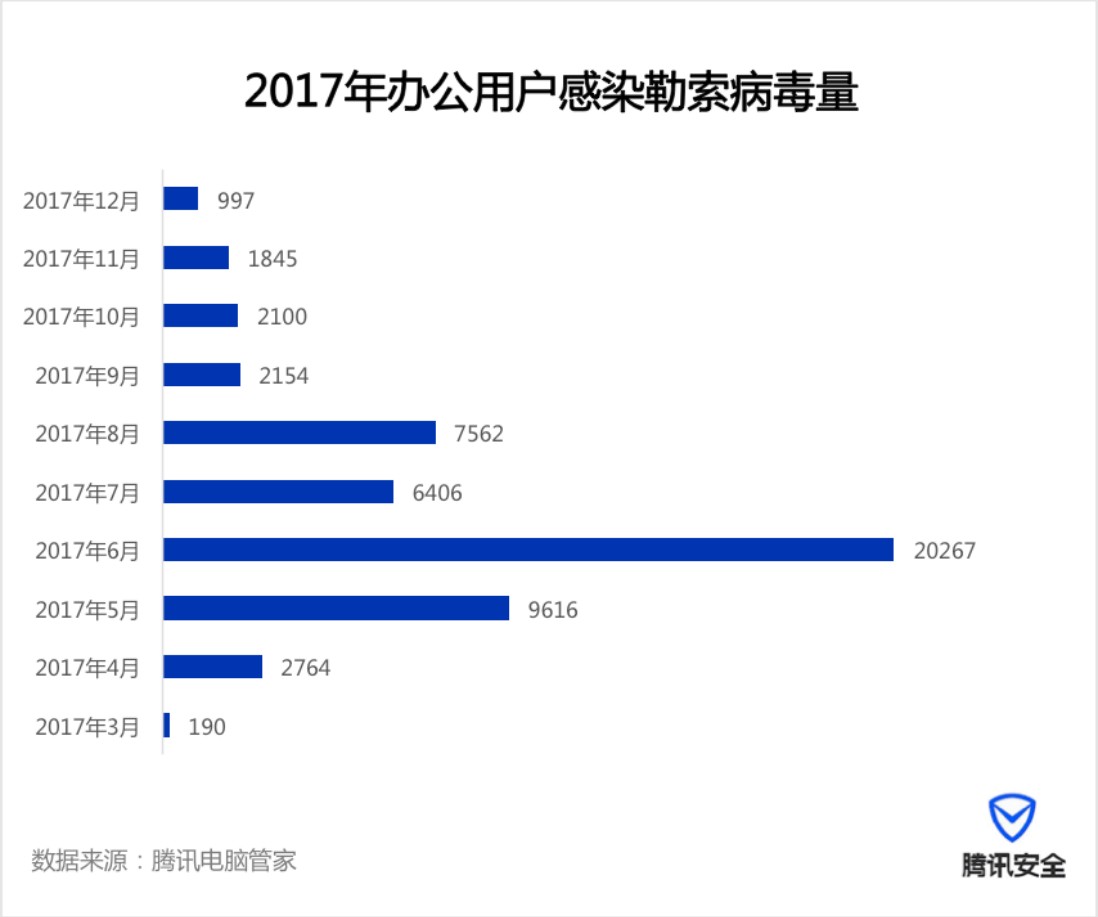
根据腾讯电脑管家 2017 年拦截勒索病毒的数据统计，3 月以来，文档守护者共拦

截勒索病毒次数达 222 万。11 月拦截勒索病毒量达到 46.9 万次，为全年最高峰。



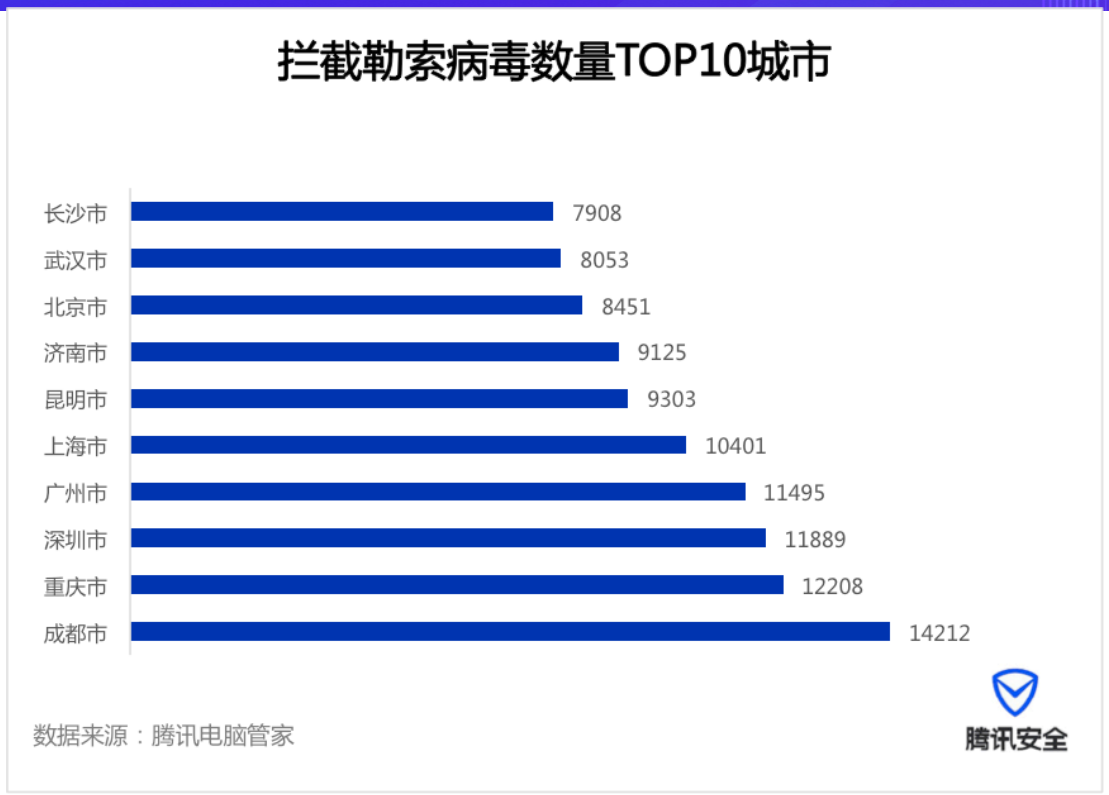
5.1.1.2 5 月勒索病毒爆发，6 月用户感染情况最严重

从数据可以看出 ,自 5 月勒索病毒爆发后 ,5 月-6 月是用户感染的最高峰期。此后，勒索病毒的迅猛之势减缓，用户感染量逐渐下降，截止 12 月用户感染数仅为 997 人，也反映出安全厂商在应对勒索病毒侵袭时的抵御措施是及时且卓有成效的。



5.1.1.3 发达城市遭勒索病毒侵袭更严重，成都受影响最甚

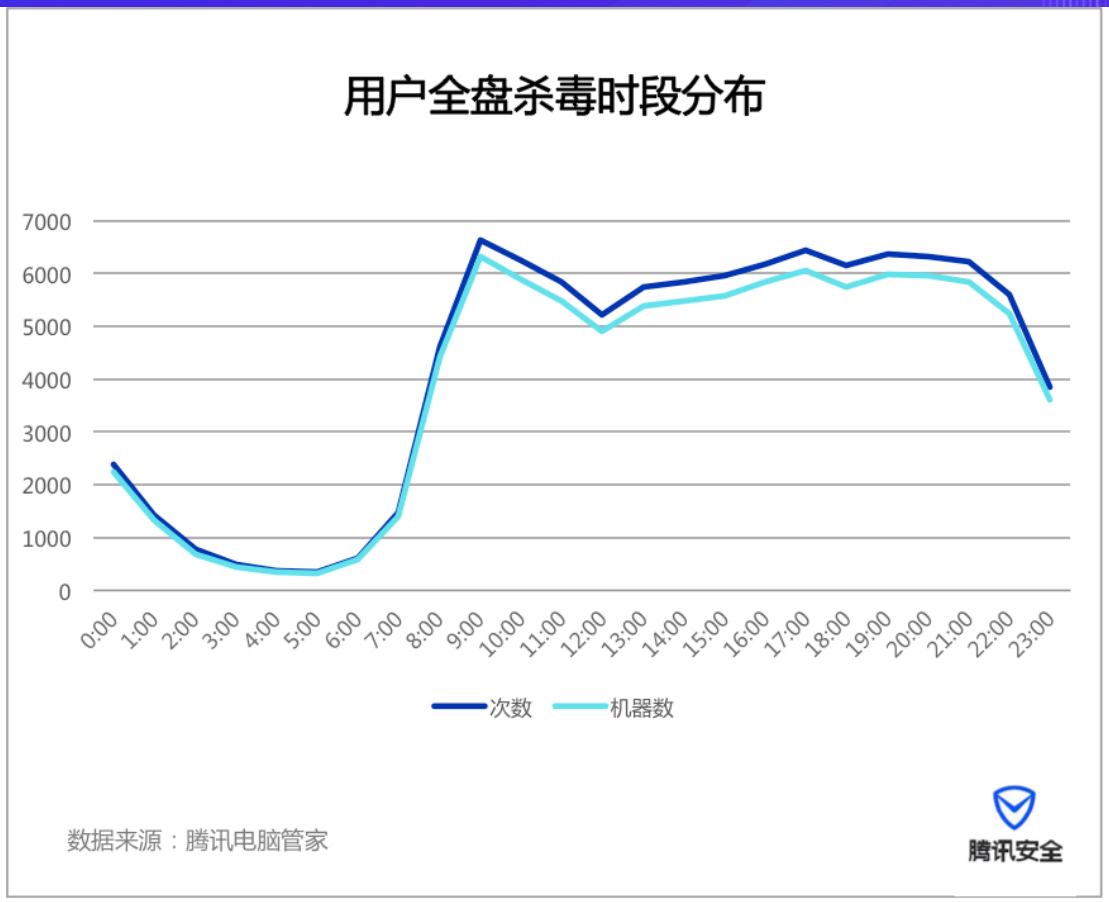
在城市分布方面，拦截勒索病毒数量 TOP10 城市如成都、深圳、北京、上海等几乎均为省会城市或经济发达的一二线城市。这类城市外来工作人口较多，且互联网发展程度高，成为勒索病毒广泛传播的地域。

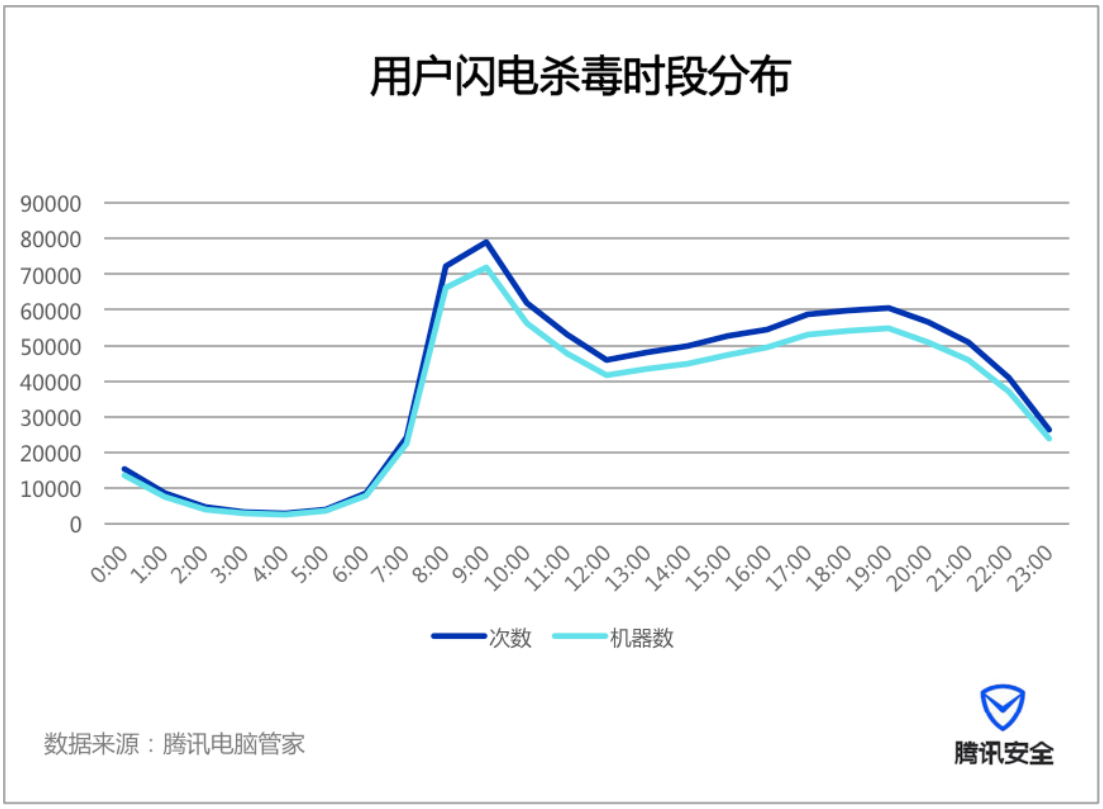


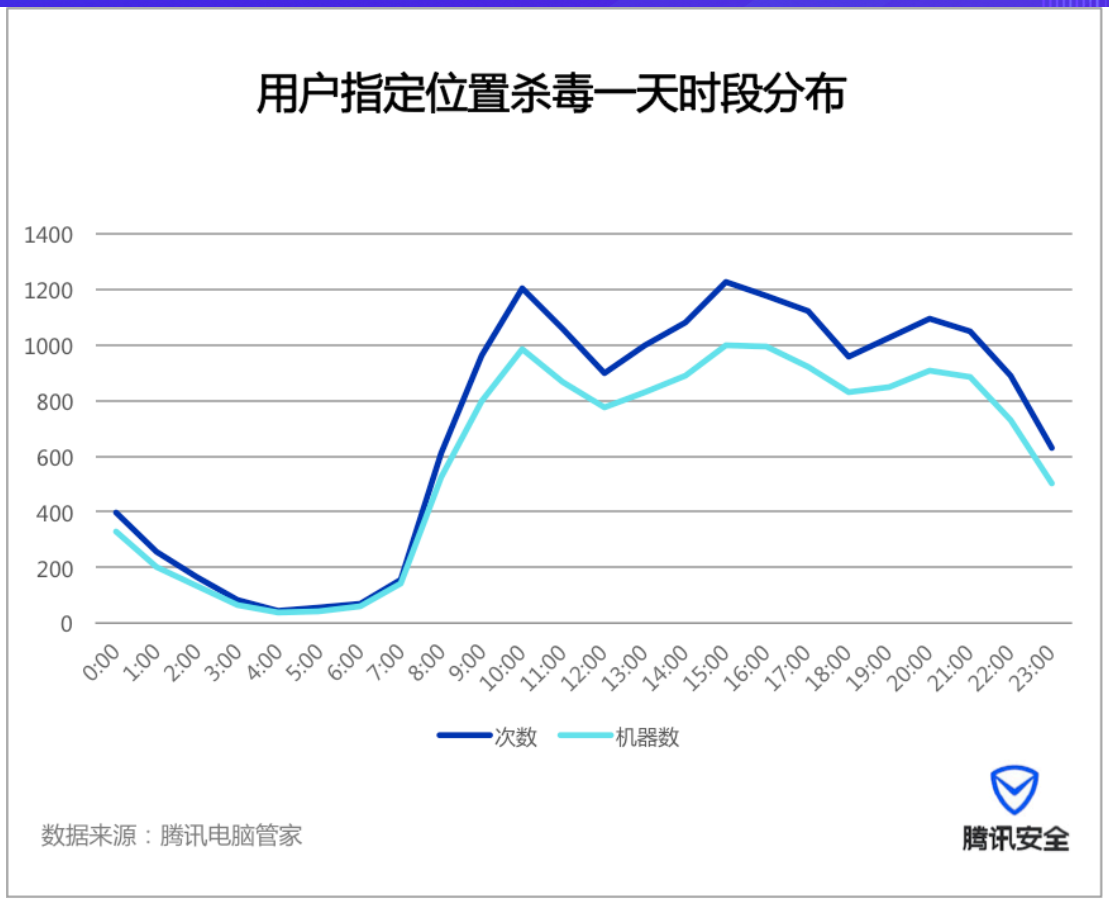
5.1.1.4 用户上午 7 时到 9 时之间最易感染勒索病毒

从病毒传播时间来看，勒索病毒感染用户的高峰集中在上午 7 时到 9 时之间，下午 12 时到 18 时之间也持续出现用户机器感染。这符合白领用户早上开启电脑处理工作，中午午休，下午连续开机的办公规律。这段时间勒索病毒传播持续活跃，也可见办公安全防护形势的严峻性。

据腾讯电脑管家统计数据显示，用户杀毒时间普遍集中于 7 时-10 时之间，说明用户普遍习惯早上一开机就为电脑杀毒。其中，全盘查杀基本覆盖了用户一天当中所有办公时间；闪电杀毒集中在 8 时-9 时、17 时-20 时两个时段；指定位置杀毒在一天当中的早（9 时-10 时）、中（14 时-15 时）、晚（20 时-21 时）分别迎来三个高峰。

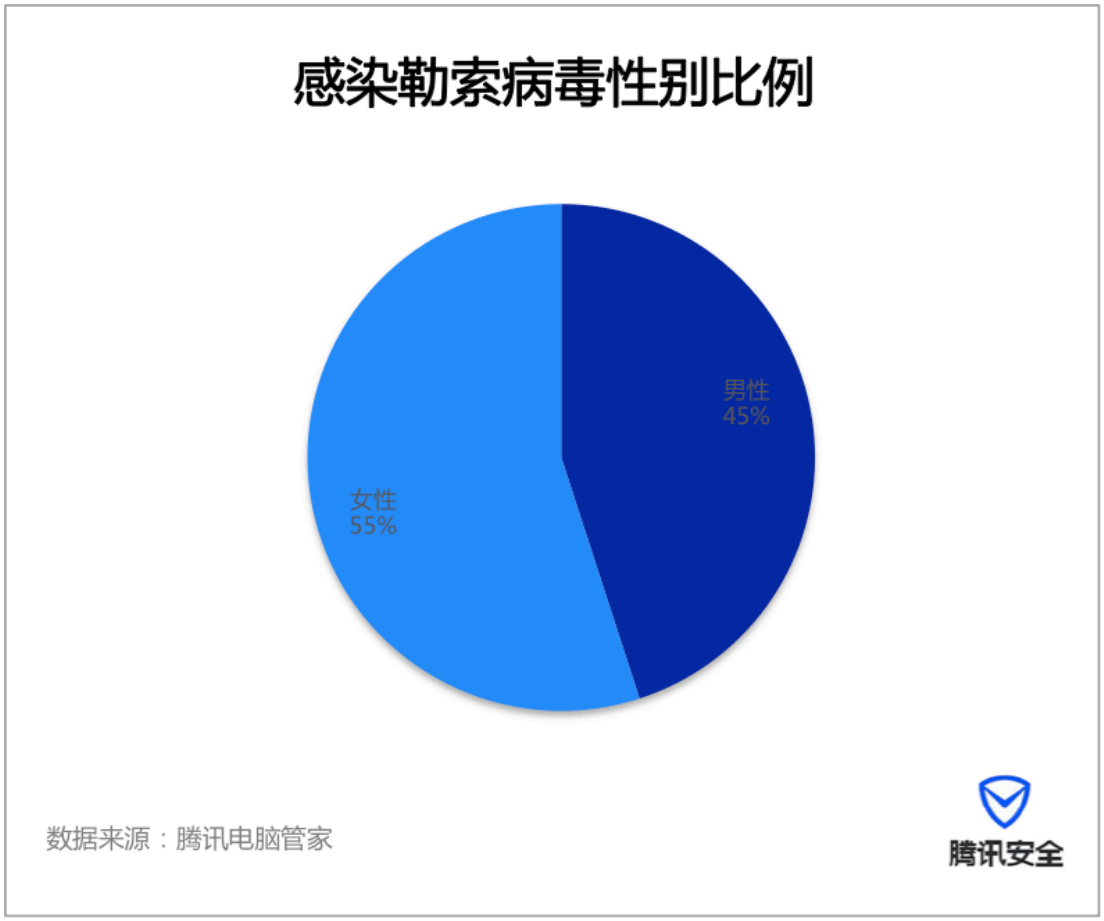

用户全盘杀毒时段分布
7000
6000
5000
4000
3000
2000
1000
0
0:00 1:00 2:00 3:00 4:00 5:00 6:00 7:00 8:00 9:00 10:00 11:00 12:00 13:00 14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00
次数
机器数
数据来源：腾讯电脑管家
腾讯安全


用户闪电杀毒时段分布
90000
80000
70000
60000
50000
40000
30000
20000
10000
0
0:00 1:00 2:00 3:00 4:00 5:00 6:00 7:00 8:00 9:00 10:00 11:00 12:00 13:00 14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00
次数
机器数
数据来源：腾讯电脑管家
腾讯安全



5.1.1.5 男女比例 9:11，女性用户更易染毒

在感染勒索病毒用户的用户中，男女比例为 9:11。可见男性防御意识高于女性，女性用户更容易染毒。



5.1.2 钓鱼邮件 APT 攻击

APT（Advanced Persistent Threat）是一种高级持续性威胁攻击，利用先进的攻击手段对特定目标进行长期持续性网络攻击的攻击形式。

APT 目标攻击通常采用鱼叉式网络钓鱼攻击手法，针对企业内部的个人或团体，伪造包含目标对象相关信息的电子邮件。打开附件，会显示伪装的正常文件给员工阅读，而该文件在后台会释放恶意代码，外联恶意网站并取得联系。外部的 APT 攻击组织接收到信息后，则会遥控下载更多的恶意组件，并对企业内部网络进行攻击、信息收集。

5.1.3 DNS 劫持

DNS（Domain Name System）劫持又称域名劫持，是指对正常的域名解析请求加以拦截，转而反馈给用户一个假的 IP 地址或令请求失去响应，导致打开的任意网址指向定制的钓鱼网站或是恶意网站，进而获取用户个人信息的网络攻击行为。

DNS 劫持往往会对网站造成严重影响，导致其用户无法正常浏览页面，尤其是访问热度较高的域名被劫持，将直接导致应用业务流程终断，严重损害网站运营效果，造成经济损失。DNS 劫持威胁用户上网安全，可能导致用户隐私数据泄露。

5.1.4 软件供应链攻击

软件供应链攻击是指在合法软件正常传播和升级过程中，利用软件供应商的各种疏忽和漏洞，对合法软件进行劫持或篡改，从而绕过传统安全产品检查，达到非法目的的攻击类型。

软件供应链攻击不是一种全新的攻击类型，过去几年间时有发生，只是 2017 年呈现出爆发态势，如今不少网络犯罪分子已经转向针对企业供应链的攻击。

5.2 企业应对网络攻击需建立全套威胁应对机制

基于企业目前面临的多样化网络攻击方式，腾讯安全专门推出“御”系列产品解决方案，整合腾讯安全安全技术能力及大数据资源，针对事前、事中、事后提供包括感知、检测、拦截、溯源在内的全套威胁应对机制，帮助企业有效抵御网络攻击。

其中，腾讯御点是国际领先的企业级安全服务提供者，整合腾讯百亿量级云查杀病毒库、引擎库以及腾讯 TAV 杀毒引擎和系统修复引擎，并应用于企业内部，可实现企业内网终端病毒木马攻击的有效防御。企业管理员可通过后台管理页面对全网或指定分组下发不同的杀毒/修复漏洞等策略，满足企业内不同分组差异化的安全管理需求。同时，日志报表内容可为企业管理员全面展现企业内网安全状况。

腾讯御界防 APT 邮件网关系统，是专门为邮箱打造的安全产品，依托哈勃分析系统的核心技术，结合大数据与深度学习，通过对邮件多维度信息的综合分析，迅速识别 APT 攻击邮件、钓鱼邮件、病毒木马附件等，有效抵御最新的邮件威胁，保护企业免受数据和财产损失。而腾讯御界高级威胁检测系统，是基于腾讯安全联合实验室反病毒实验室的安全能力，依托腾讯在云和端的大数据，形成了强大且独特的威胁情报和恶意检测模型，凭借基于行为的防护和智能模型两大核心能力，高效检测未知威胁。

此外，腾讯还推出御见智能态势感知平台，依托腾讯 19 年的安全经验积累，以及腾讯哈勃系统提供强大的 APT 威胁检测能力，通过对企业全面的基础信息（用户+行为+流量+日志+资产）进行集中采集、存储和持续深层分析，并融合防御、检测、响应溯源和预测全生命周期的威胁应对机制，为客户构建自适应安全体系，弹性应对来自外部和内部的各种威胁，实现企业全网安全态势可知、可见、可控的闭环。

六、互联网安全生态搭建

6.1 技术创新推动安全产业链开放、合作、共享

6.1.1 政府借力厂商技术能力，协作打击治理

在所有合作形式中，国家政府职能部门借助安全厂商人才技术优势，开展共享共治模式最先释放势能。2017 年，腾讯在推动普惠金融发展、打击网络传销、维护食药安全三大领域，相继与国家食药总局、国家工商总局、北京市金融局、深圳市金融办展开合作 :与国家食品总局合作建立互联网食药大数据监管指数平台 ;同北京市金融工作局、深圳市金融办合作建立大数据金融安全监管科技平台 ;与国家工商总局共同建立“网络传销监测治理基地” ;并借助腾讯安全反诈骗实验室的“可疑网络传销态势感知平台 “，形成从主动发现传销平台-传销平台预警播报-传销平台线索追踪-推动警方案件侦查的业务链条，推动线下监管和精准打击。

6.1.2 安全安全厂商合作，合力构筑安全堤坝

在网络安全产业分工更加精细化的趋势下，安全厂商之间联动可在彼此防护能力的基础上由点成线，合力构筑一条安全堤坝。腾讯安全在第三届中国互联网安全领袖峰会上，启动了 P13 体系，联合天融信、卫士通、启明星辰、立思辰、美亚柏科、拓尔思、蓝盾股份、任子行、北信源、绿盟科技、飞天诚信、北京数字认证、中孚信息等 13 家中大型骨干安全厂商，共同应对信息安全新威胁，链接利益，共谋发展。

6.1.3 助力第三方厂商，赋能“互联网+”

在互联网+不断深入生活方方面面时代背景下，安全厂商的赋能作用凸显。

在互联网安全方面，腾讯安全联合实验室七大实验室 2016 年为苹果、微软、Adobe、谷歌等全球四大厂商贡献了 269 个漏洞报告；在移动互联方面，腾讯安全除了发现并提交 IOS 漏洞之外，还与苹果达成深度合作。iPhone 系列手机时首次接入腾讯手机管家的骚扰拦截功能，让亿万中国 iPhone 用户免受信息骚扰之苦；在车联网方面，腾讯安全科恩实验室与特斯拉汽车的默契配合，仅在十天就完成了漏洞的修复，避免了“僵尸汽车”的危机发生。

6.2 安全人才建设奠定网络安全新生态基础

6.2.1 腾讯安全联合实验室护航六大互联网关键领域

2016 年 7 月，腾讯安全整合旗下实验室资源，成立国内首个互联网实验室矩阵——腾讯安全联合实验室，旗下涵盖包括科恩实验室、玄武实验室、湛泸实验室、云鼎实验室、反病毒实验室、反诈骗实验室、移动安全实验室在内的七大实验室。实验室专注安全技术研究及安全攻防体系搭建，安全防范和保障范围覆盖了连接、系统、应用、信息、设备及云，触达六大互联网关键领域。

2016 年，凭借“全球首次远程无物理接触方式入侵特斯拉汽车”研究成果，腾讯安全联合实验室科恩实验室入选“特斯拉安全研究员名人堂”，并获特斯拉 CEO 马斯克的亲笔致谢。

在举国关注的反诈骗领域，腾讯安全联合实验室中的反诈骗实验室基于多年来在反诈骗领域的深耕研究，已经形成一整套基于 AI 创新+能力开放的反欺诈评价新标准，形成有效的止损模式。在 AI 创新和能力开放的双轮驱动下，反诈骗实验室继推出鹰眼反电话诈骗系统、神荼网址反诈骗系统、麒麟伪基站定位系统、神羊情报分析平台后，2017 年又连续推出阻断诈骗资金流转的神侦资金流查控系统，以及利用大数据服务于虚假食药、金融诈骗监管的网络安全态势感知系统和灵鲲金融安全产品。并将这些产品通过腾讯云的 SaaS 服务开放给有需要的政府单位、企业等，帮助相关职能部门及企业升级监管模式。

(图：大数据金融安全监管科技平台，基于反诈骗实验室灵鲲金融安全系统)

6.2.2 安全人才培养“腾讯模式”驱动更加健全的安防体系

在数字经济时代到来之际，信息安全威胁不断升级，网络犯罪也呈现出“全球化”、“突发性”、“危害重”三大显著特点。这要求我们需建立更为健全的网络安全防御体系。而安全人才梯队建设是推动网络安全建设的重要力量，也是建立健全网络安全防护体系的核心驱动力。

腾讯副总裁马斌认为，人才队伍建设需要持续系统化、规模化、体系化；并推动政府、企业、院校等全方位合作，建立全面的培养体系。在数字经济时代，腾讯一直注重培养网络安全人才，持续探索行之有效的网络安全人才培养方式。通过发起 TCTF、GeekPwn 等信息安全赛事，推动安全人才突破技术瓶颈，提升技术水平。除此之外，腾讯安全联合实验室在 2017 年 2 月发起的 TCTF 大赛上还宣布启动“百人计划”，即通过 TCTF 大赛选拔出最具潜力的百名安全人才，并通过后续持续培养，打造互联网安全领域未来领军人才，“形成一个由高校理论教育到企业技能培养到国际赛事锻炼的完整人才培养闭环。”

为了进一步提升中国网络安全人才的视野和格局，腾讯安全还积极拓展国际交流。旗下的安全专家在 DEF CON 黑客大会、BlackHat 黑帽大会、VB 大会、Cansecwest 安全峰会等全球顶尖会议频频发表研究观点，备受行业瞩目。

七、2018 年网络安全威胁八大趋势分析

一、物联网设备将成为新的 DDoS 攻击目标

在 2017 年，我们看到利用家庭和工作场所中成千上万的存在安全漏洞的物联网设备生成流量而发起的大型 DDoS 攻击。在 2018 年，网络罪犯仍会寻求利用采取欠佳的安全设置和管理措施的家庭物联网设备来发动攻击。此外，攻击者还会劫持设备的输入/传感器，然后通过音频、视觉或其他伪造输入，让这些设备按照他们的期望而非用户的期望操作。

二、机器学习加剧攻防两方的对抗

当下，有关人工智能和机器学习的讨论都专注于如何将这些技术用于保护和侦测机制。2018 年，这种情况将发生变化，网络罪犯将会利用人工智能和机器学习发动攻击，并且用于探索受害者的网络，而这通常是他们成功入侵受害者系统后最耗费精力的环节。

三、数字勒索或成为未来主流网络犯罪手法

2017 年爆发出不少全球性的信息安全危机，从 WannaCry、Petya 到 BadRabbit，勒索病毒风暴席卷全球企业端及消费者，黑客攻击手法日益多样化。与过去几年相比，网络犯罪手法已由间接诱骗使用者的帐号密码，转向直接勒索钱财的“数字勒索”为主。专家预估，通过勒索病毒、诈骗来获利的模式，仍将会是 2018 年网络犯罪的主流手法。

四、家庭设备或将成为勒索软件的劫持目标

在丰厚利益的诱惑下，越来越多的网络罪犯分发勒索软件，并且导致勒索软件即服务(Ransomware-As-A-Service)及其他服务在黑市日益盛行。不仅如此，专业的网络罪犯还希望通过利用不断增长的昂贵的互联家庭设备，攻击更多的目标。用户一般意识不到智能电视、智能玩具和其他智能设备所面临的威胁，使之成为网络罪犯的主要攻击目标。

五、网络黑产技术手段持续升级，威胁源更加多变

未来网络黑产将呈现四种新趋势：1、黑产人员的作案模式从偷偷摸摸的潜伏偷窃数据或诈骗，升级到更简单粗暴的公然犯案，制作勒索病毒公然勒索的施害手法将在未来更加流行；2、犯罪团伙开始披上合法外衣，通过成熟的运作流程与渠道弄到企业资格，涉及资金流转的环节以诈骗手法获取第三方接口，犯罪手法更为隐蔽；3、黑产目标从 C 端延伸到 B 端，越来越多的黑产分子通过提供假的实名认证信息来觅得市场，同时“刷票党”、“羊毛党”、“刷粉党”等各种挑战的对抗压力持续增大；4、黑产逐渐觊觎信用建设相关领域，各类买卖公民个人信息和篡改学历的案件或将高发；传统的病毒木马和电话诈骗等模式，向更为先进的撞库拖库、精准诈骗等模式发展。

六、电信诈骗与移动木马结合，传统电信诈骗再升级为移动木马诈骗

2018 年利用植入移动木马实施诈骗的手段将进一步盛行。移动木马与电信诈骗结

合后，较之过去的 PC 远程诈骗，不仅提高了隐私窃取能力、远控能力等，同时还降低了用户感知度，在用户完全不知情的情况下完成远程转账。移动木马诈骗可以实现通话控制（拦截用户通话，不允许用户拨打 110 等电话求证）、短信控制（拦截网银等支付验证码信息，自动同步给诈骗者）、获取手机联系人信息、地理位置等。

七、移动支付成主流，手机支付安全引关注

随着我国移动支付业务愈发普及，犯罪分子可以通过各种手段完全控制用户手机(特别是在手机 root 情况下)，进而控制更多的用户隐私信息(如短信内容、通话记录、地理位置等隐私信息)来精确了解用户群体，实施更加精准的攻击。支付类病毒作为危害程度最大的木马病毒之一，通常会窃取用户短信验证码，并结合其他非法渠道获得的个人隐私信息完成转账，造成用户财产损失。

八、国家层面加快信息安全、网络安全等方面立法进程

12 月 24 日，全国人大常委会建议通过加快个人信息保护法立法进程、加大打击力度等方式，进一步提升用户个人信息保护力度，促进完善网络安全法配套法规规章，加快《关键信息基础设施安全保护条例》《网络安全等级保护条例》的立法进程。这也意味着国家已充分意识到网络安全及个人信息安全保护的重要性，未来信息安全监管力度将持续加大。


腾讯安全
腾讯安全联合实验室