第十六次全国计算机和移动终端病毒疫情调查分析报告

国家计算机病毒应急处理中心

2017年6月

目 录

前　言

为全面了解并掌握 2016 我国信息网络安全状况，宣传、普及信息网络安全知识，提高广大用户网络安全的防范意识，国家计算机病毒应急处理中心（以下简称“病毒中心”）于 2017 年 3 月 17 日至 2017 年 4 月 17 日在全国范围内组织开展了“第十六次全国计算机和移动终端病毒疫情调查活动”。此次活动由公安部网络安全保卫局指导，国家计算机病毒应急处理中心主办，亚信安全协办，多家信息安全企业共同参与并提供支持。新华社、腾讯网、新浪网、搜狐网、网易网、北方网、赛迪网、《信息网络安全》、《中国信息安全》、51CTO 等多家单位作为支持媒体参与此次调查活动。

术语释义

网络安全事件

指针对计算机或网络发起的、能对网络中的数据或系统的完整性、保密性和可用性造成损害的攻击事件，如网络攻击和传播计算机病毒等。

恶意代码（也称恶意软件）

是指能够影响计算机操作系统、应用程序和数据的完整 性，可用性、可控性和保密性的计算机程序或代码。主要包括计算机病毒、蠕虫、木马程序等。

计算机病毒（简称病毒）

指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

木马

特洛伊木马（简称木马），指通过伪装欺骗手段诱使用户激活自身，但不具有复制、传播能力的恶意代码。

蠕虫

指可以通过网络等途径将自身的全部代码或部分代码通过网络复制、传播给其它的网络节点的程序。它不同于计算机病毒，不需要文件宿主。蠕虫由于通过网络大量复制传播，可造成网络阻塞，甚至瘫痪。

脚本类病毒

脚本类病毒通常是用 JavaScript 代码编写的恶意代码,它们利用 Windows 系统的开放性特点，通过调用 Windows 对象、组件，可以直接对文件系统、注册表等进行控制。很多脚本类病毒带有广告性质，会修改 IE 首页、修改注册表等信息。

网页挂马

指在网页中嵌入恶意代码，通过用户访问网页时，利用用户系统存在的安全漏洞进行传播、破坏的行为。

APT

高级持续性威胁（Advanced Persistent Threat，APT），是指组织（特别是政府）或者小团体，使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，威胁着企业的数据安全。这种行为往往经过长期的经营与策划，并具备高度的隐蔽性。

移动终端

移动终端或者叫移动通信终端是指可以在移动中使用的计算机设备，广义的讲包括手机、笔记本、平板电脑、POS 机甚至包括车载电脑。但是大部分情况下是指手机或者具有多种应用功能的智能手机以及平板电脑。

勒索软件

勒索软件是黑客用来劫持用户资产或资源并以此为条件向用户勒索钱财的一种恶意软件。通常会将用户系统内的文档、邮件、数据库、源代码、图片、压缩文件等多种文件进行某种形式的加密操作，使其不可用，或者通过修改系统配置文件、干扰用户正常使用系统的

方法使系统的可用性降低，然后通过弹出窗口、对话框或生成文本文件等方式向用户发出勒索通知，要求用户向指定帐户支付赎金来获得解密文件的密码或者获得恢复系统正常运行的方法。

调查方法说明

“第十六次计算机和移动终端病毒疫情调查活动”采用了线上线下同步发布的方式，不仅在权威媒体、门户网站、各支持单位网站上开展网络调研，而且通过摸排、走访的方式对关键基础设施和重要信息系统的安全状况进行调查。

线上部分，一是国家计算机病毒应急处理中心在官网设立调查专区；二是协办单位亚信公司通过官方网站、官方微博等线上活动推广调查；三是52家支持单位通过官方网站及微信/微博公众号转发疫情调查活动的相关信息及调查问卷，对调查活动进行推广。

线下部分，一是与支持单位举办的市场活动进行联动，在山东、浙江、广东、上海、云南、陕西、湖南、湖北、四川等九省市开展安全巡展，配合宣传调查活动，针对活动参会对象进行调研。同时，通过首都网络安全周、第二届四川省信息安全技术展览会暨四川省信息安全技术高峰论坛等大型活动对调查进行推广；二是调查活动走进校园，先后在北京大学、天津大学、哈尔滨工业大学、成都信息工程大学等九所院校开展活动，普及网络安全和病毒防护知识，分发调查问卷；三是对重点地区、重点行业、重点领域的安全问题进行实地走访。中心派员赴北京、天津、上海、江苏、安徽、福建、河南、广东、陕西省（市）等九个省市的公安厅（局）网安总队，与属地等保部门交流，了解当地重点单位2016年度整体安全状况、基础设施和重要信息系统的安全状况、发生的网络安全事件及其防范措施等情况。赴重

要信息系统进行调研走访，深入了解重要信息系统的安全状况和急待解决的问题。

主要调查内容为：2016 年 1 月至 2016 年 12 月间，我国联网单位及个人用户发生网络安全事件的次数、种类、造成的损失等情况，以及我国计算机用户感染病毒的次数、种类、感染途径等内容。并且针对我国 2016 年度内主要的信息安全事件，如网络欺诈、网络钓鱼以及勒索软件等情况展开调查和危害分析。

一、 疫情调查结果概述

根据 CNNIC 数据显示，我国已是全球互联网用户规模最大的国家。截止 2016 年底，我国网民数量达 7.31 亿，其中移动终端用户达到 95.1%，互联网普及率达到 53.2%。与此同时，由于我国互联网业务规模巨大、业务种类繁多、业务环境复杂，使得我国网络安全面临的威胁不仅体量巨大，而且形态复杂多样。

调查数据显示，2016 年我国网络安全状况较为平稳，计算机病毒感染率和移动终端病毒感染率均有小幅下降；用户的网络安全意识普遍提升。但当前网络安全形势依旧严峻，移动互联网恶意程序数量呈高速增长态势，病毒感染、网络攻击、信息泄露、勒索软件等安全事件时有发生，政府部门、关键信息基础设施的网络安全防护能力有待进一步加强。

2016 年全球勒索软件大范围爆发，为全球企业、组织机构和个人用户都带来了严重影响；网络诈骗也是用户面临的主要安全威胁之一；全球范围内信息泄露事件屡见不鲜；僵尸网络肆虐，物联网（IoT）安全任重道远。

2016 年可谓是我国的网络安全年，国家层面高度重视打击网络犯罪，维护网络安全，习总书记发表“ 419 讲话 ”，明确指出了我国互联网建设和发展中遇到的问题，厘清了我国互联网发展的总体目

标。《中华人民共和国网络安全法》的出台，使网络安全有法可依。国家各级主管部门携手推进的“社会共治”模式起到了明显作用。

二、计算机和移动终端病毒疫情调查情况分析

2.1 计算机病毒疫情调查分析

2.1.1 我国计算机用户病毒感染情况

我国计算机用户病毒感染率有小幅下降。2016 年我国计算机病毒感染率为 57.88%，与 2015 年的 63.89%相比，下降 6 个百分点。下降原因得益于广大计算机用户安全意识的提升、安全产品的普及和多级防护体系的建立，如图 2-1 所示。

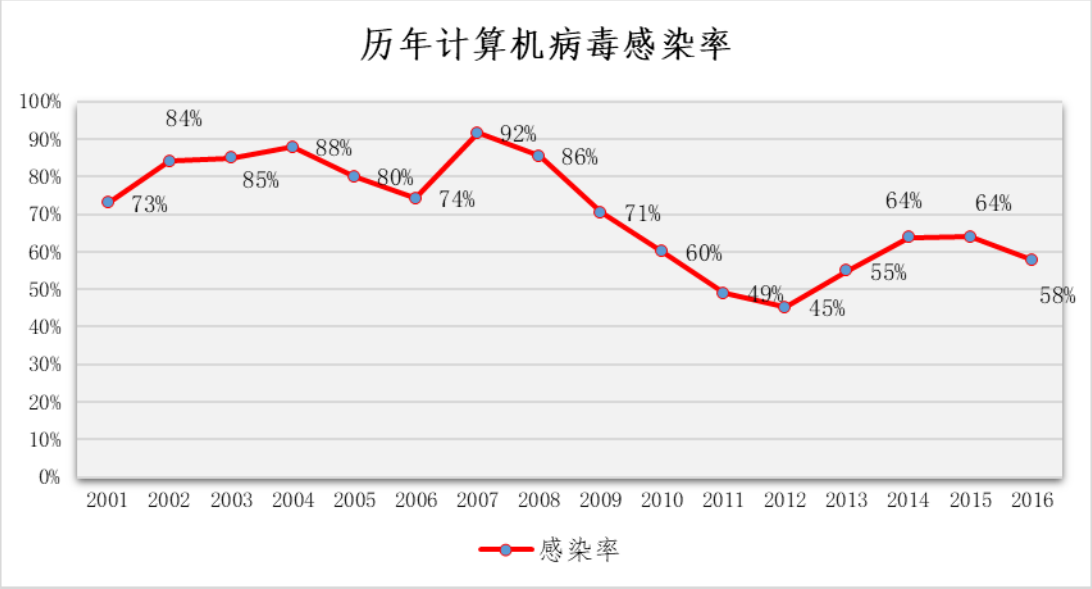

图 2-1 历年病毒感染比例曲线图

2.1.2 我国计算机病毒传播的主要途径

调查显示，2016 年我国计算机病毒传播主要途径为通过网络下载或浏览，比例为 69.02%，较 2015 年下降了 3.86%。局域网传播紧随其后，占 35.39%，排第三的为移动存储介质，占 30.87%。此外，电子邮件、网络游戏、系统和应用软件漏洞等也是病毒传播的主要途径，如图 2-2 所示。

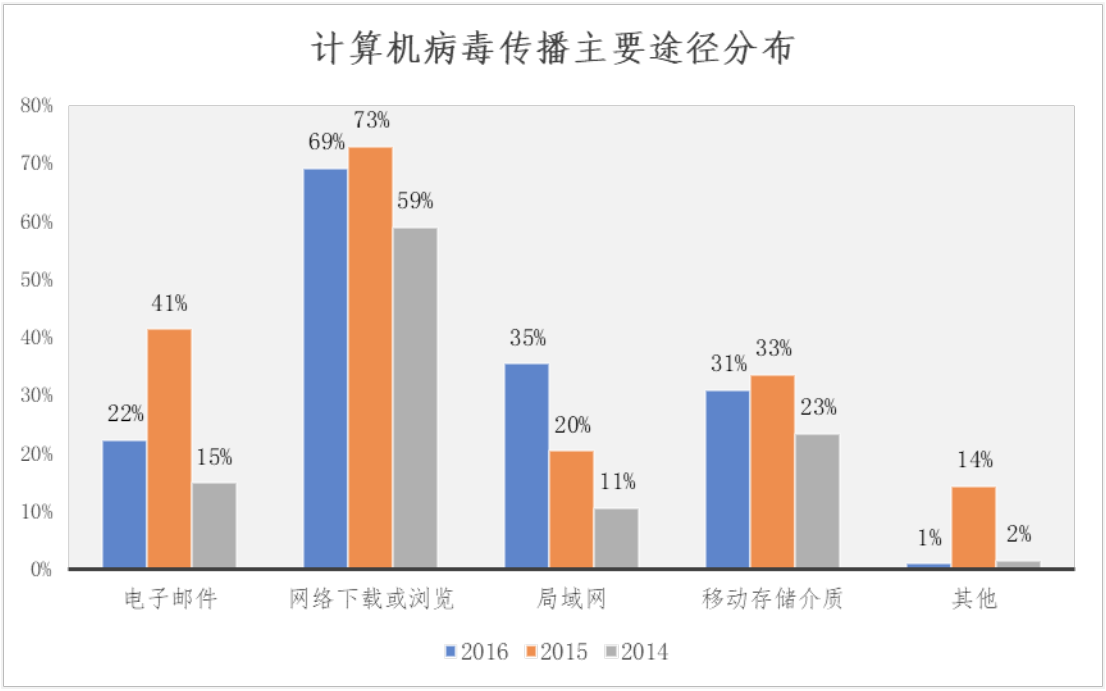

图 2-2 计算机病毒传播的主要途径

网络下载或浏览中，通常病毒、木马喜欢伪装成游戏外挂、色情播放器、软件破解补丁、刷会员软件、刷 Q 币软件等。用户在使用浏览器浏览网页时，病毒、木马会主动弹出并诱导用户下载，也有部分存储在网络云盘中，提供下载链接诱导用户下载。

局域网传播中，由于局域网共享资源的便利性，一旦局域网中的某台设备被感染，病毒或木马就会扫描并利用局域网中的开放端口，快速感染局域网服务器及局域网中的其他终端设备。局域网是病毒和木马传播重要的途径之一。

电子邮件是黑客利用社会工程学攻击的最主要途径之一。黑客通常会发送一封看似正常的邮件，例如将发件人伪造成 IT 管理部门、收件人的领导或下属，获取收件人信任，然后通过收件人下载或点击附件中的病毒、木马（通常会伪装成正常的 Word、PDF、Excel 文件），达到攻击目的。目前，社会工程学邮件攻击是网络钓鱼、勒索软件、APT 攻击最主要的攻击途径。

2.1.3 计算机病毒造成的主要危害情况

2016 年计算机病毒主要造成的危害包括浏览器配置被修改、系统（网络）无法使用、密码与账号被盗、受到远程控制和数据受损或丢失。其中，浏览器配置被修改以 53.13%的占比排名第一，成为计算机病毒造成的最主要危害，较 2015 年上升 9.76%；53.13%的用户遭受系统（网络）无法使用，比 2015 年上升 9.73%；下降幅度最大的是密码与账号被盗，下降了 18.62%，占比 35.06%。总的来看，计算机病毒给用户带来的困扰和危害更大了，尤其是对浏览器、系统与网络带来的威胁显著提升，如图 2-3 所示。

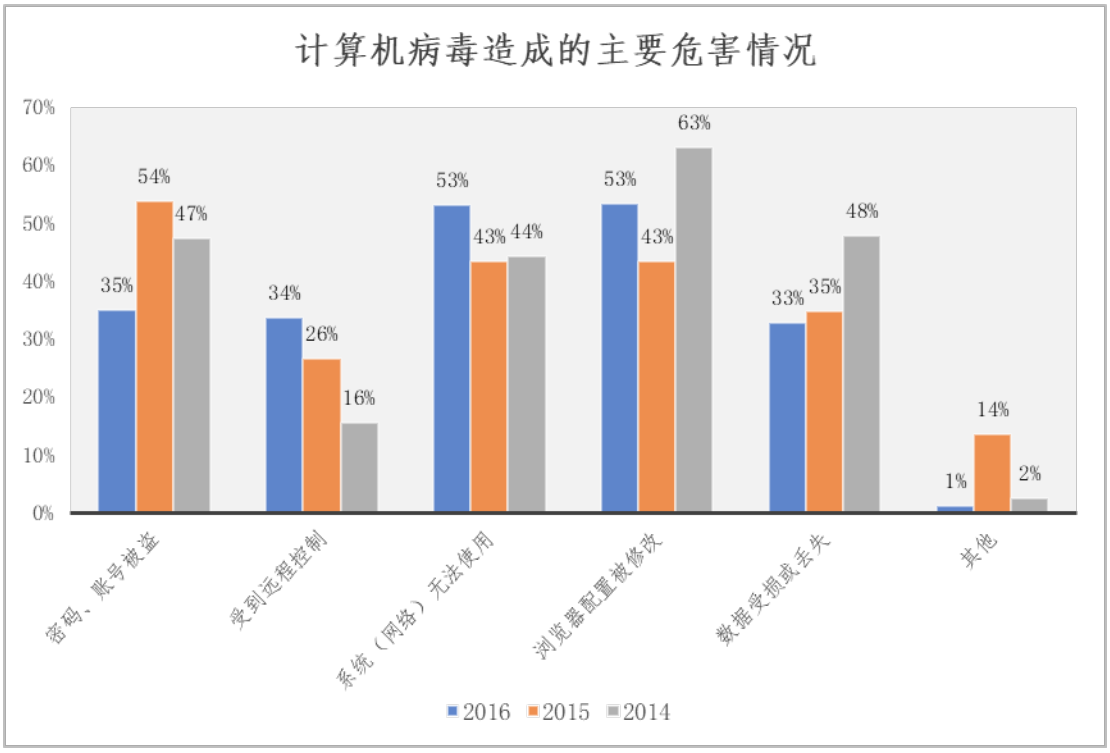

图 2-3 计算机病毒造成的主要危害

浏览器是最常用互联网应用之一，是黑色产业链重点攻击的对象。浏览器配置被修改通常表现为主页被修改，由于互联网商业模式建立在“流量”基础上，因此黑客利用恶意软件修改用户浏览器主页内容，达到为网站导流，进而获得非法收入的目的。

黑客利用恶意软件非法盗取用户账号密码，既可以直接盗取用户账号中的资金或虚拟资产，向黑产直接贩卖用户个人信息牟利，也可以利用“撞库”攻击方式，尝试以相同的用户名和密码，盗取用户在其他的更有价值的网站中注册的账号进行牟利。特别是在当前个人信息泄露频发的背景下，用户账号、密码是黑客主要攻击目标。

2.1.4 2016 年计算机病毒感染量 TOP20

调查显示，在 2016 年传播的病毒中，木马仍是传播最广泛的恶意代码。

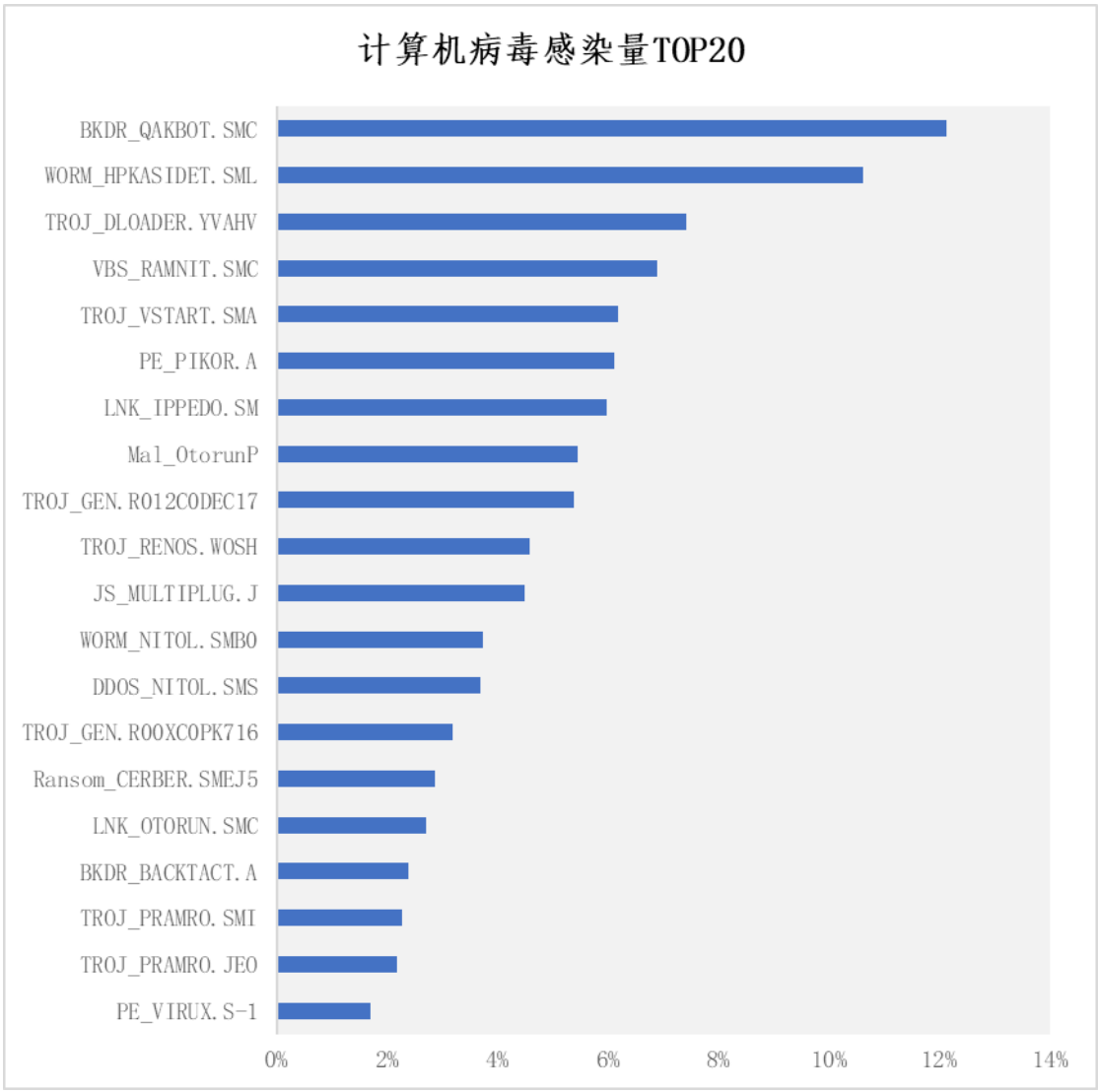

图 2-4 2016 年计算机病毒感染量 TOP20

2.2 移动终端安全问题和病毒疫情调查分析

2.2.1 我国移动终端操作系统使用情况

调查显示，2016 年各种移动终端操作系统使用较 2015 年均有所增加。其中，安卓以 68.64%居首位，IOS 占 41.54%，居第二位，Windows Phone 操作系统以 13.76%排在第三位。安卓、IOS 的用户比例较前两年有明显上升。安卓和 IOS 系统因操作简便，可扩展性好、系统稳定、安全性高等特性受到人们的青睐，用户数量大幅增加，如图 2-5 所示。

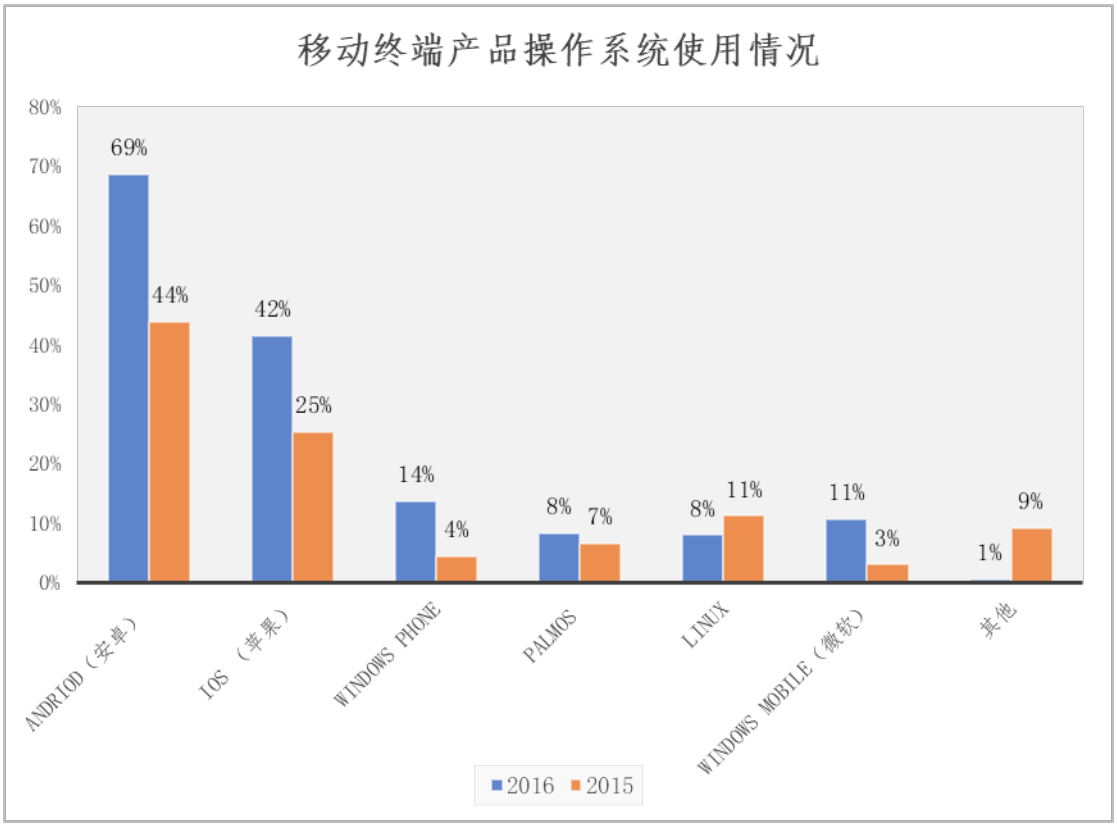

图 2-5 移动终端产品操作系统使用情况

2.2.2 移动终端互联网应用情况

调查显示，2016 年，使用频度较高的移动终端互联网应用主要包括社交软件、金融服务、网页浏览、收发邮件、网络游戏、音视频等。社交软件以 86.39%占据首位，较 2015 年略有上升，依然是最主要的互联网应用；金融服务以 73.43% 位居第二，较 2015 年上升 19.55%；排在第三位的是网页浏览，占 57.39%，较 2015 年下降 17.16%；收发邮件占 44.88%，较 2015 年略有增加；视频和网络游戏分别占 37.76% 和 28.37%，均较 2015 年有所下降。可以看出，随着互联网医疗、共享单车等新业务不断涌现，网络支付、互联网金融等业务持续发展，非娱乐型应用呈现持续上涨趋势，如图 2-6 所示。

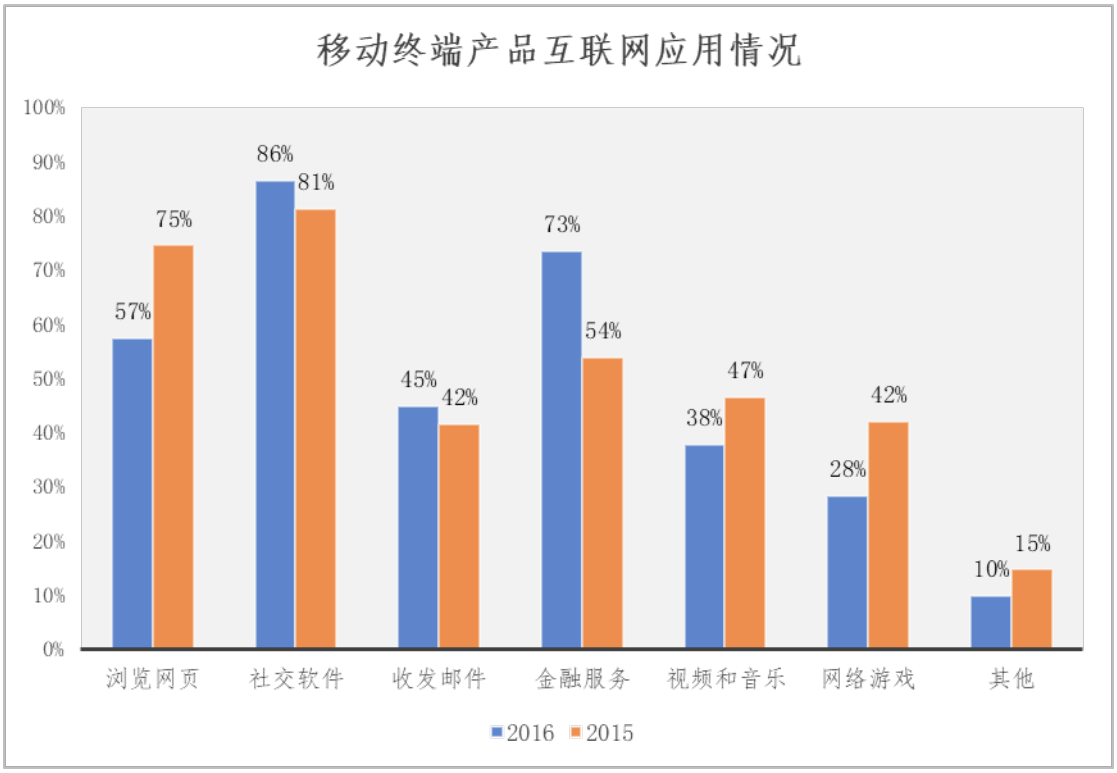

图 2—6 移动终端产品互联网应用情况

2.2.3 移动终端安全问题的主要途径

调查显示，在造成移动终端安全问题的主要途径中，垃圾短信排名首位，占调查总数的 54.39%，比 2015 年降低 15.94%，降幅较大。主要原因是由于近年来，公安部加大对垃圾短信和伪基站的打击力度；手机安全厂商通过技术改进，对垃圾短信的识别率和拦截率不断提高；电信运营商积极履行社会责任，切断垃圾短信传播渠道。如图 2-7 所示。

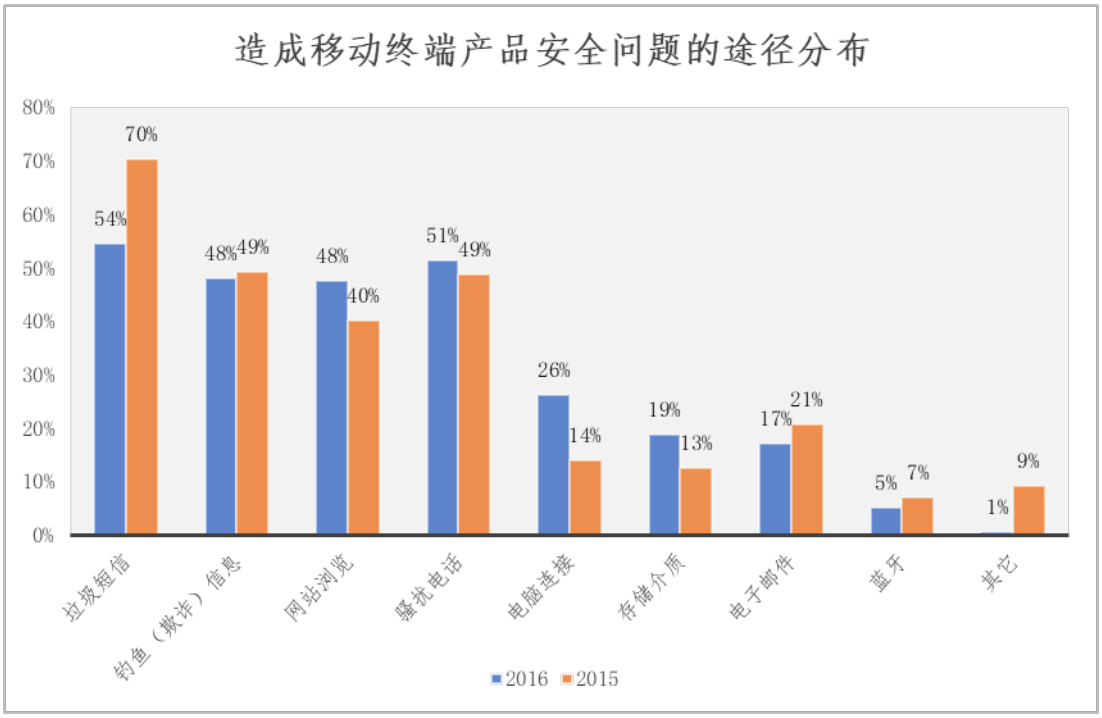

图 2-7 造成移动终端产品安全问题的途径

排名第二位的是骚扰电话，占 51.49%，比 2015 年略有增加。由于个人隐私数据泄露严重及垃圾短信治理成效显著，使诈骗短信传播受阻，恶意用户不得不转而利用电话这一传统渠道进行欺诈。

排名第三位的是钓鱼（欺骗）信息，占 48.04%，与 2015 年基本持平。网络钓鱼正在向移动终端发展。不法分子为提高钓鱼成功率，采用伪造网站、伪造移动应用、伪造应用界面等技术，实施钓鱼和欺诈，对广大用户财产安全带来极大的危害。

排名第四位的是网络浏览，占 48.04%，比 2015 年增加 7.50%。大量移动终端安全威胁通过网页挂马、诱导下载等方式传播。

2.2.4 移动终端病毒感染情况

调查显示，2016 年有 43.33%的移动终端使用者感染过病毒，比 2015 年下降了 7.13%。下降的主要原因一是由于移动终端安全产品的普遍应用，部分安卓系统在出厂时也预装了安全产品，有效遏制了病毒的传播；二是国家对网络安全高度重视，2016 年《中华人民共和国网络安全法》出台，公安机关不断加大对网络犯罪的打击力度，用户的安全意识得到普遍提升。如图 2-8 所示。

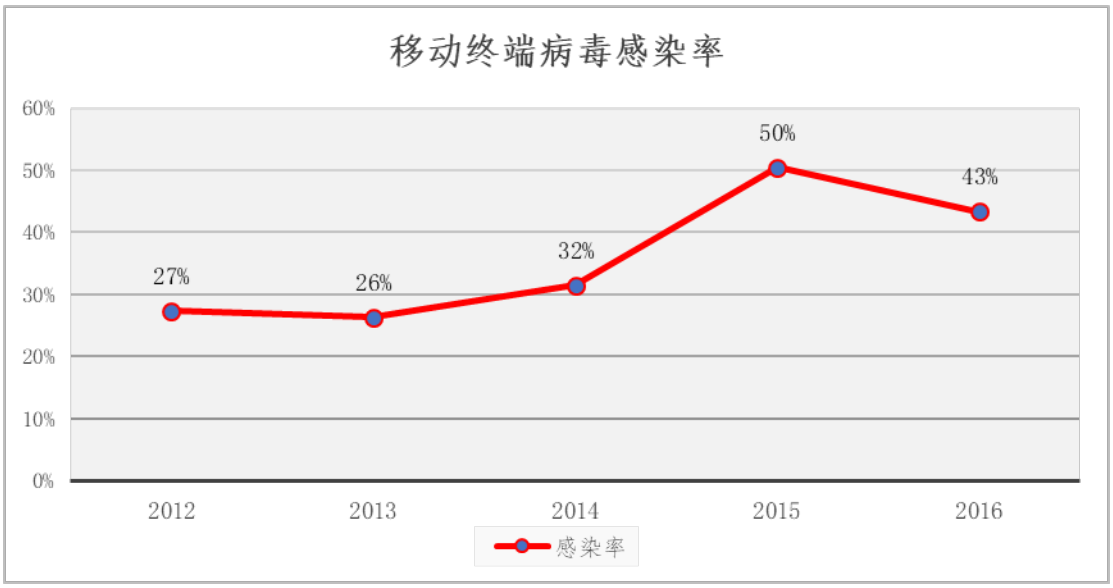

图 2-8 移动终端病毒感染率

虽然调查结果显示移动终端病毒感染率有所下降，但移动终端恶意样本数量仍在大规模增长，新的恶意样本层出不穷。例如出现多起攻击者利用社工欺诈手段绕过安卓系统安全权限事件；Root 型恶意代码无论从数量和功能上都呈现出较为迅猛的增长和进化趋势；IOS 操作系统的安全性也受到挑战，如 2016 年 IOS 系统曝出“三叉戟”漏洞。

2.2.5 移动终端病毒传播主要途径

调查显示，移动终端病毒感染的途径中，网站浏览以 50.00%高居榜首，比 2015 年下降 4.8%。短信/彩信排名第二位，占 44.82%，比 2015 年下降 16.67%。电子邮件、社交软件、电脑连接分别占 35.20%、34.04%和 27.71%。随着社交软件功能日益完善，支付方式被广泛使用，使用人群快速增长，部分新增用户由于安全意识薄弱，使得通过社交软件的病毒感染量增加 4.43%。短信/彩信由于受到移动 OTT（“Over The Top”的缩写，是指通过互联网向用户提供各种应用服务。）应用影响，加之安全厂商协同电信运营商在 DNS（域名系统）层面开展电信反欺诈，病毒通过短信/彩信中短链接传播有所下降。如图 2-9 所示

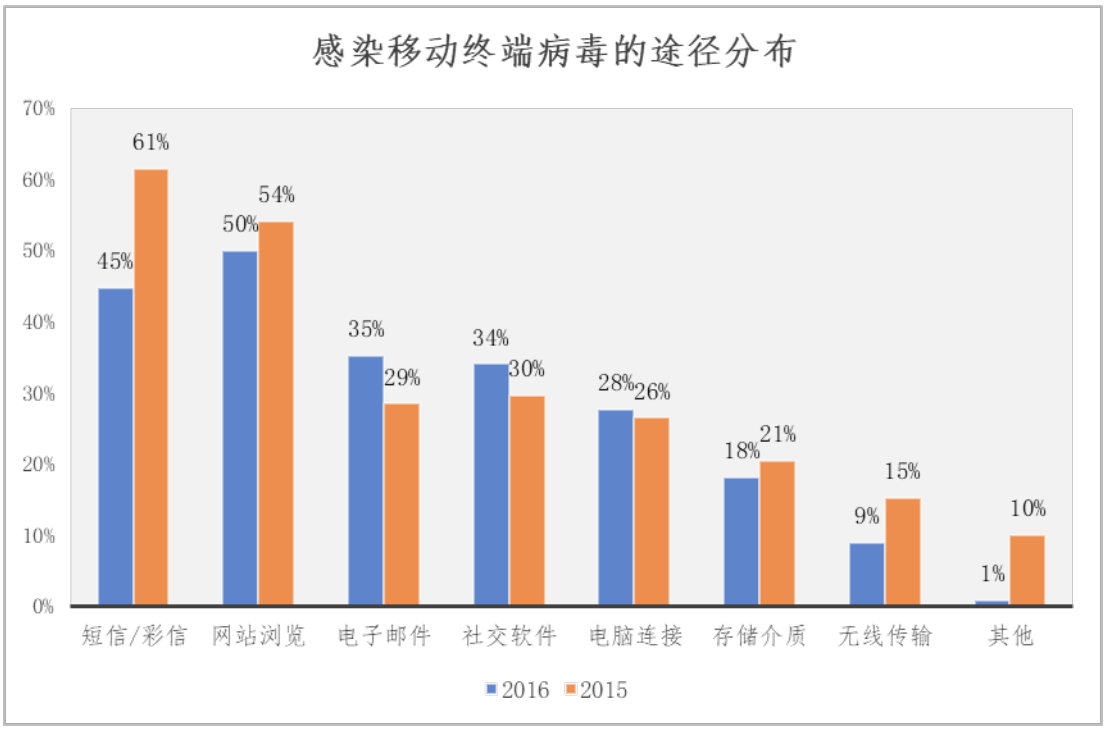

图 2-9 感染移动终端病毒的途径

2.2.6 移动终端病毒造成的主要危害

调查显示，用户移动终端感染病毒后造成的主要危害有影响手机正常运行、恶意扣费、远程受控、信息泄露、网络欺诈等。影响手机正常运行以 60.08%居首位，与 2015 年基本持平；恶意扣费位居第二位，占比 43.48%，比 2015 年下降 6.27%；远程控制和信息泄露分列三、四名，分别占 38.39%和 33.7%。远程受控比 2015 年增加了 20.62%。如图 2-10 所示。

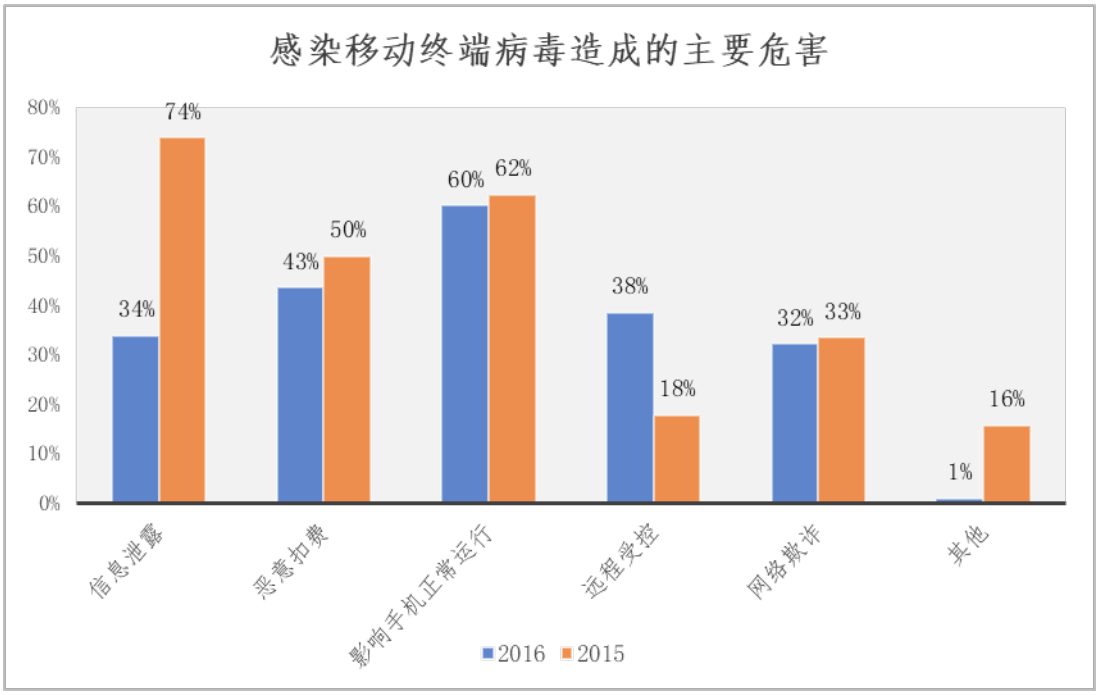

图 2-10 感染移动终端病毒造成的主要危害

2.2.7 移动终端安全产品使用情况

随着移动终端厂商预装安全软件及用户个人安全意识的上升，调查显示，52.25%用户使用移动终端防病毒产品，44.36%用户使用防火墙，43.08%用户安装了数据恢复软件，另有 32.23%用户安装使用了移动终端安全管理软件。与 2015 年相比,用户移动终端安全产品使用率整体呈现上升趋势。如图 2-11 所示。

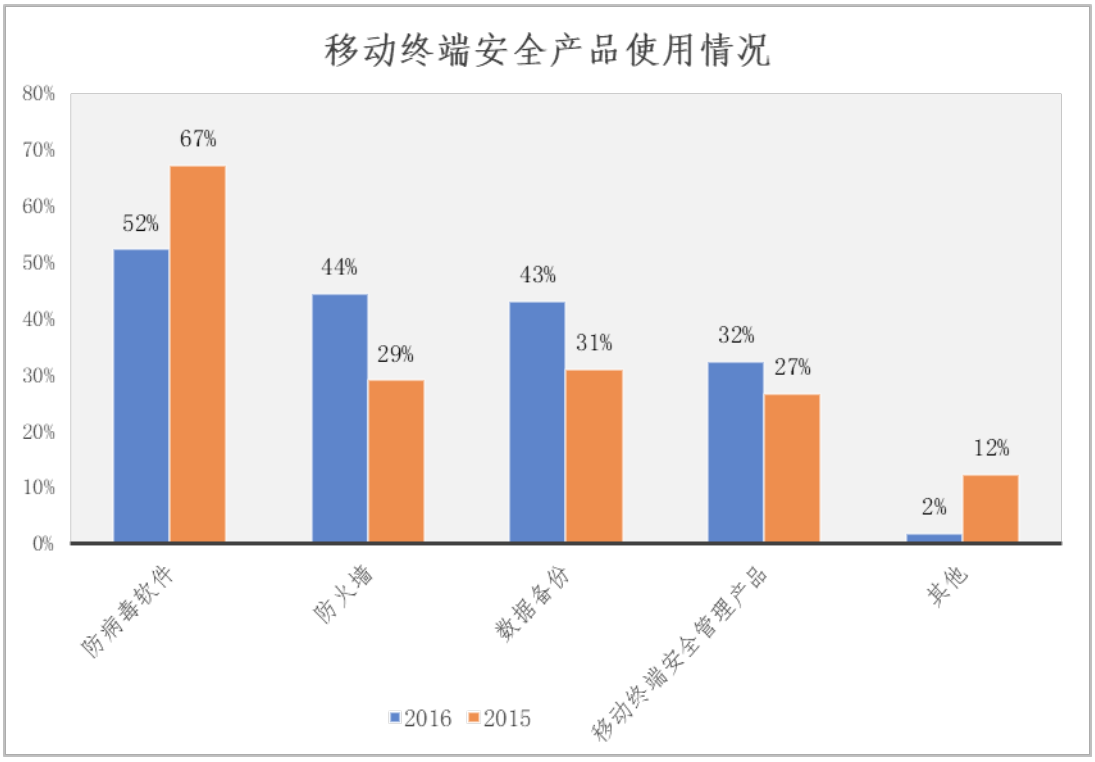

图 2-11 移动终端安全产品使用情况

2.2.8 2016 年移动终端病毒感染量 TOP20

调查显示，移动终端病毒感染量排名 TOP20 全部为安卓平台病毒。

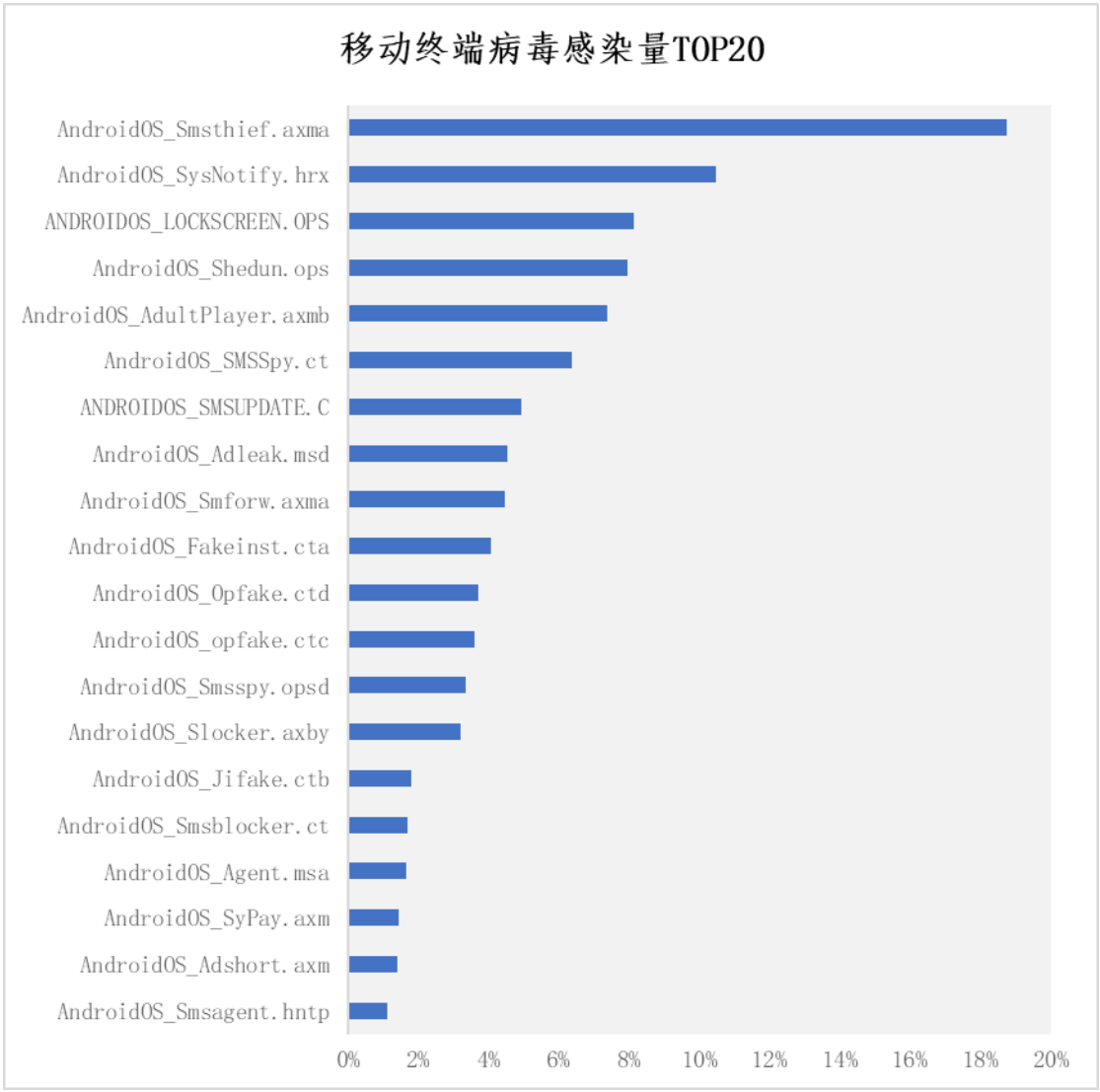

图 2-12 移动终端病毒感染量 TOP20

2.3 2016 年勒索软件状况调查分析

2.3.1 2016 年勒索软件状况

2016 年是勒索软件大爆发的一年，勒索软件是一种敲诈型病毒，通过限制用户访问系统，或者通过加密系统中的文件，导致用户无法进入系统，无法使用应用、设备、文件，强迫用户支付赎金。

勒索软件大多通过邮件渠道传播，利用人性弱点，如：好奇心、轻信、贪婪等发动社会工程攻击。该种传播方式成本相对低，但却效果显著。低成本高回报是勒索病毒一大特点。

早期勒索软件主要是将用户设备锁住，迫使用户支付赎金以解开设备。2014 年起，勒索软件开始将用户计算机内最为宝贵的数据加密，强迫用户支付赎金，赎回数据。

加密勒索软件之所以得以快速发展并形成较大影响，一方面是因为部分勒索软件作者会在网络上公开售卖，使得一些没有能力制造勒索软件的黑客也加入其中；另一方面，勒索软件的开源促进其发展，黑客通过修改代码，开发出不同种类的勒索软件，导致其不仅数量增加，种类也大幅增长。

2.3.2 2016 年勒索软件疫情及危害情况

调查显示，59.36%用户认为勒索软件普遍存在，主要影响 PC、手机两种设备，其中手机占 65%、PC 占 28%；27%用户遭受过勒索软件，但用户被勒索软件每笔的金额大多在 5000 元以下，如图 2-13 所示。

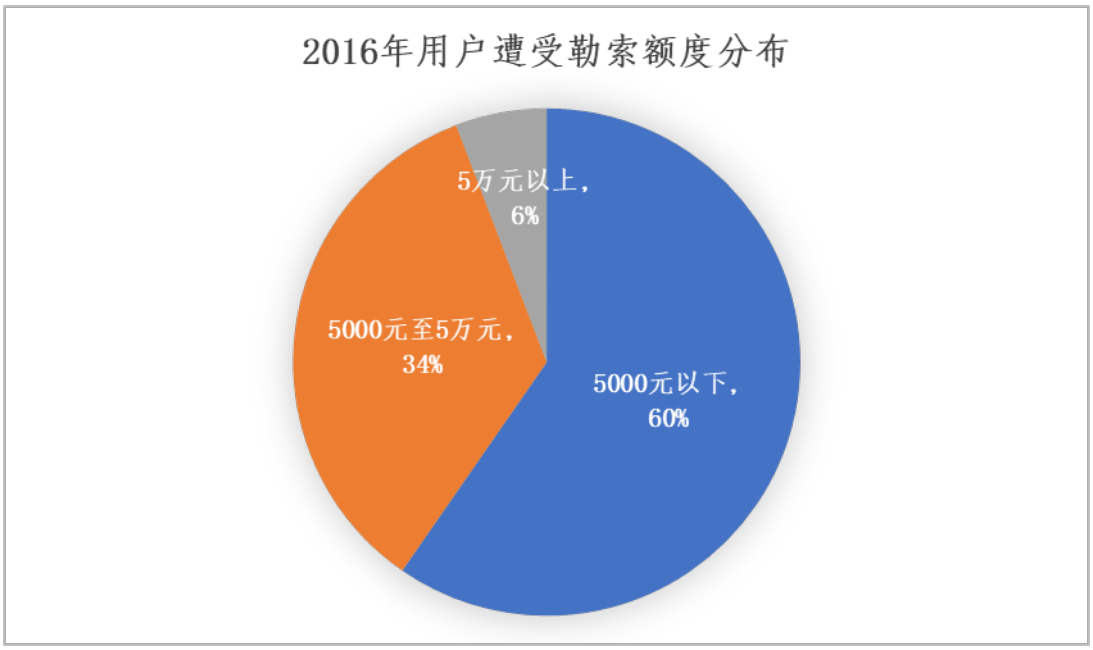

图 2-13 单用户被勒索的额度

调查显示，勒索软件的敛财方式并非针对单用户进行大额勒索，而是通过多用户小额勒索的方式实现。勒索软件造成的主要危害是数据被加密、设备被锁定两种方式，占 99%。其他还包括文件丢失、QQ 号被盗，支付宝转账诈骗等。如图 2-14 所示。

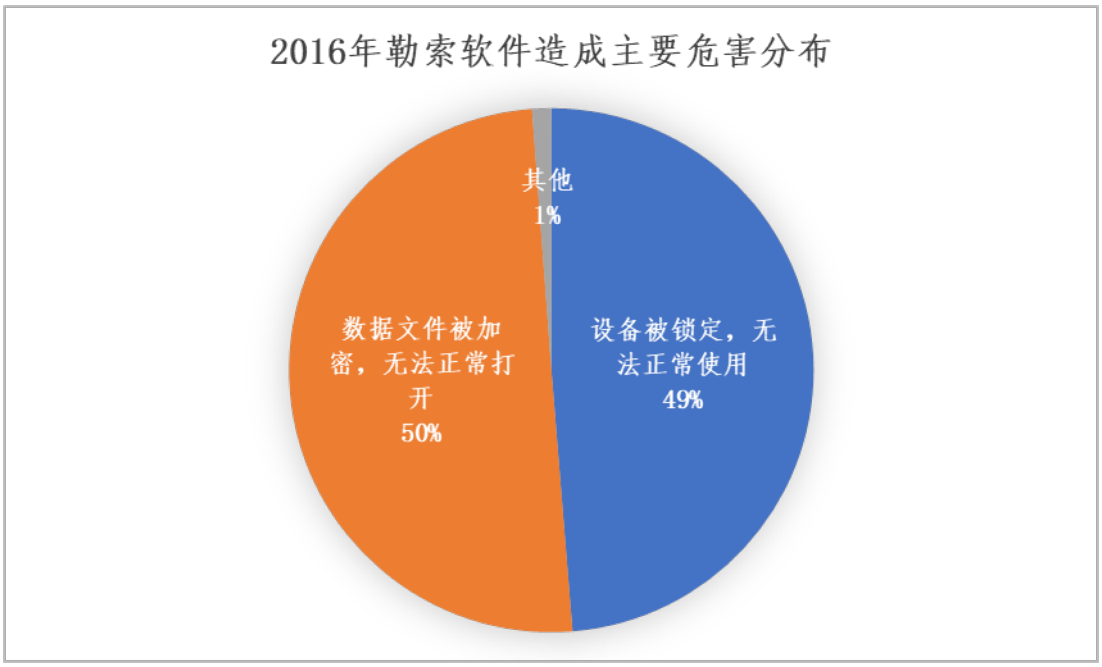

图 2-14 勒索软件造成的危害

调查显示，用户遭遇勒索事件后选择的处理方式主要是报警、找技术人员解决、自行解决三种，采用这三种解决方案的用户共占 71%，其中报警的比例占 19%，说明用户被勒索后报警意识淡薄。用户愿意支付勒索赎金的仅占 10%。如图 2-15 所示。

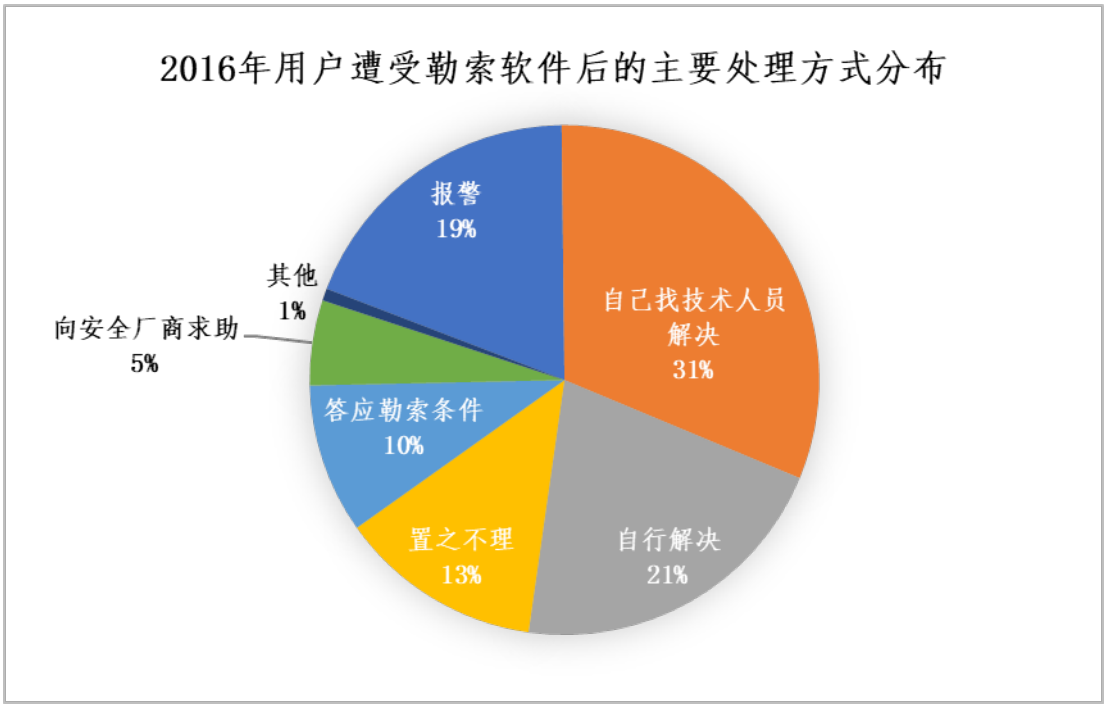

图 2-15 被勒索后的处理方式

用户被勒索后，建议不要轻易答应黑客勒索条件，原因是即使答应，也不一定能够恢复数据。正确应对勒索软件的方式应该是提前防御，包括定期备份数据、安装防护软件、及时更新病毒库、及时打补丁、养成良好的上网习惯等。

2.4 2016 年网络欺诈状况调查分析

2.4.1 2016 年网络欺诈状况

网络欺诈给广大用户生命财产造成严重伤害和巨大损失, 已成为社会关注热点问题之一。近几年，网络欺诈案件与日俱增，作案手法不断变化。

通过对大量网络诈骗案件的分析发现, 钓鱼网站是网络欺诈最主要手段之一。钓鱼网站通常用于获取受害人网站账号、密码信息，骗取受害人信任、传播木马。除钓鱼网站外，诈骗短信同样是黑客常用手段。诈骗短信是移动恶意代码进入用户手机中的重要入口。伪基站是诈骗短信的主要传播途径。

2016 年，北京、天津、山西、辽宁、吉林、广西等 17 个省、自治区、直辖市成立省级反电信网络诈骗中心,公安机关和银行、电信运营商派员入驻。根据新华社报道，2016 年破获网络欺诈案件 9.3 万起, 收缴赃款赃物价值人民币 23.8 亿元, 挽回经济损失 48.7 亿元。反网络欺诈工作成果喜人，有效打击了网络欺诈犯罪份子的嚣张气焰。

2.4.2 2016 年网络欺诈疫情及危害情况

调查显示，网络钓鱼/网络欺诈事件呈逐年上升态势，在五大类主要安全事件中位列第三，其中 2014 年为 30.40%，2015 年为 37.24%，2016 年则达到了 46.23%。如图 2-16、图 2-17 所示。

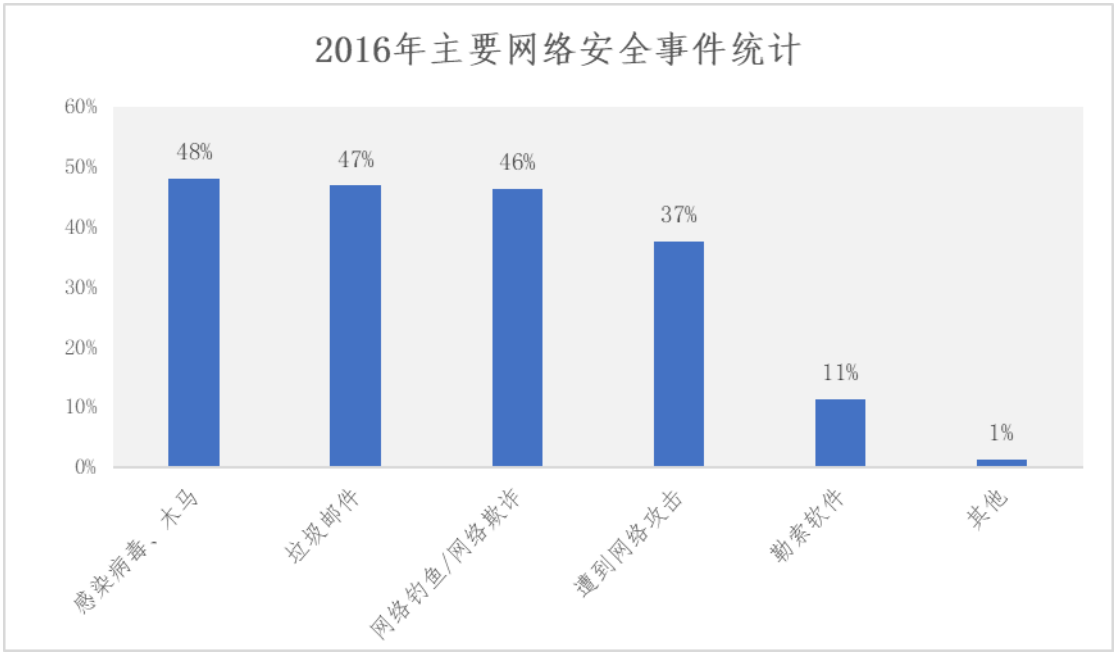

图 2-16 2016 年主要安全事件统计

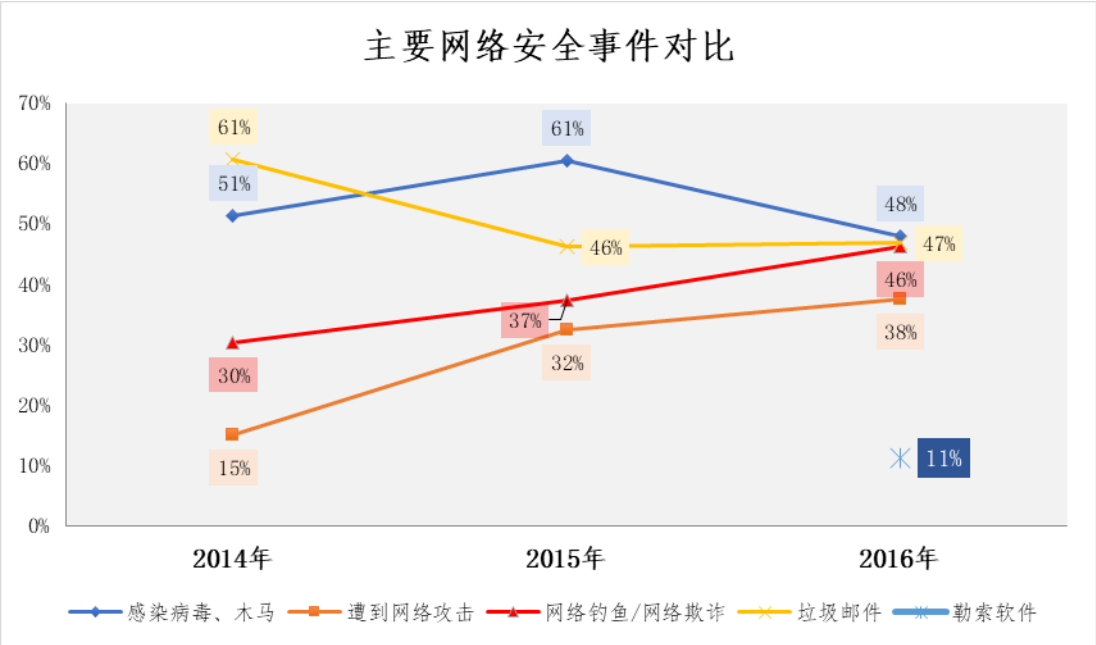

图 2-17 网络安全事件发生情况统计

用户浏览网页时发生主要安全事件中，网络钓鱼/网络欺诈占40.50%，处于较高水平。如图 2-18、图 2-19 所示。

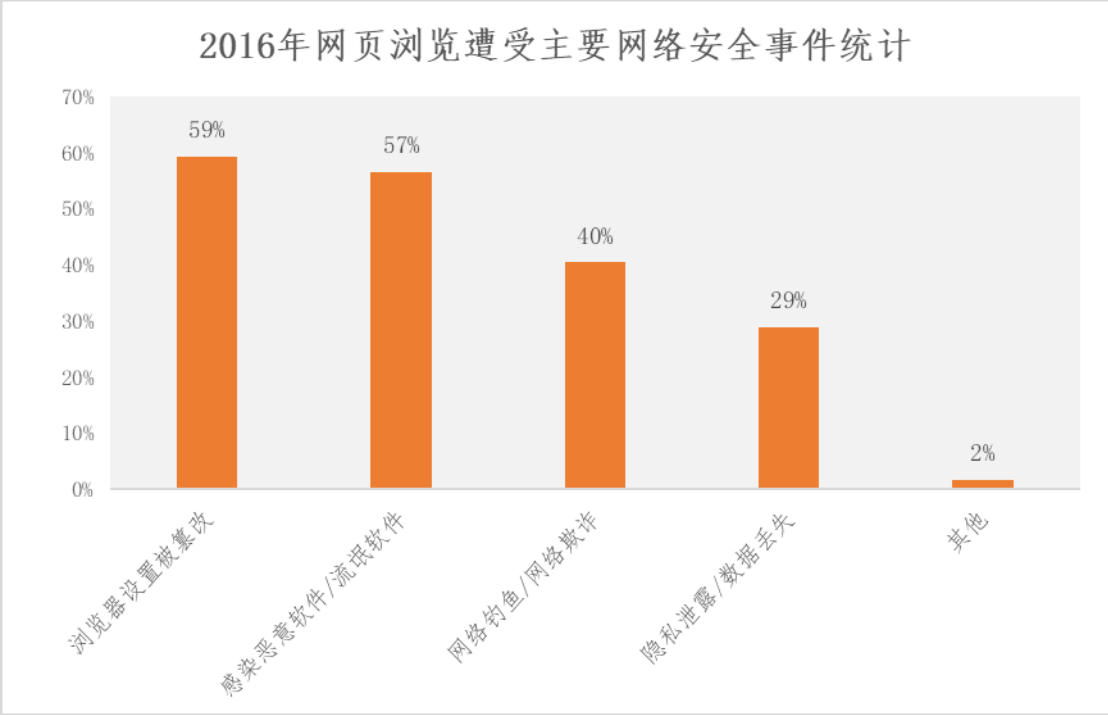

图 2-18 浏览网页时发生的主要安全事件统计

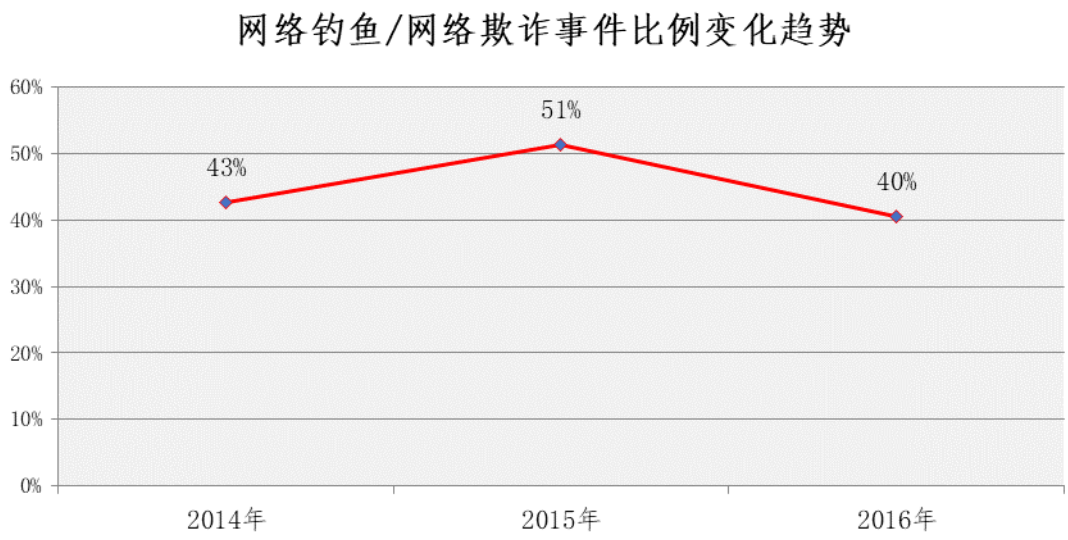

图 2-19 网络钓鱼/网络欺诈事件占比变化趋势

用户在移动终端中遭遇网络欺诈的比例为 48.04%，处于较高水平，同时，网络欺诈也是移动终端病毒带来的主要危害之一。如图 2-20、图 2-21 所示。

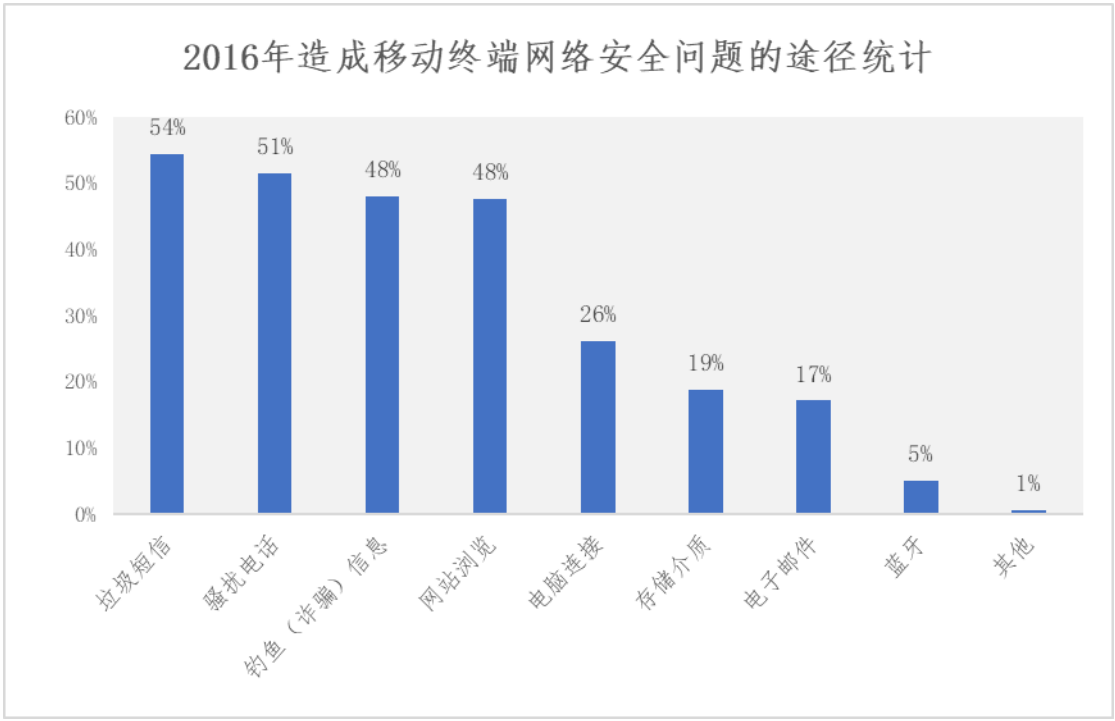

图 2-20 2016 年移动终端安全事件统计

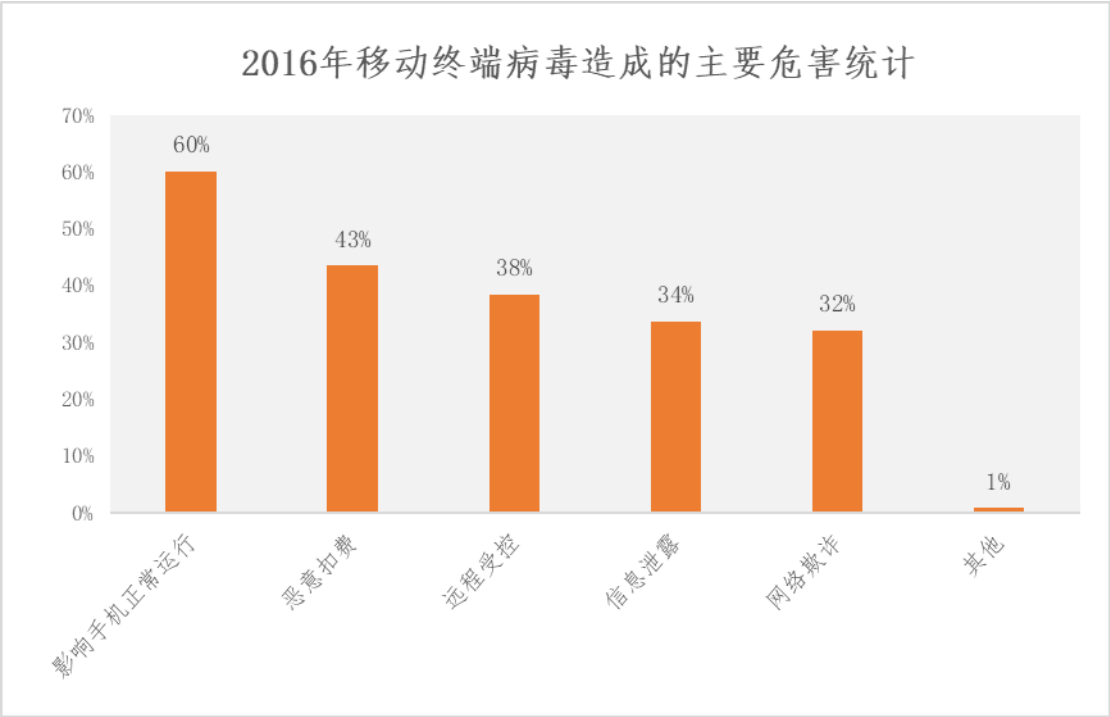

图 2-21 2016 年移动终端病毒的主要危害统计

调查显示，2016 年度遭遇网络欺诈的人数占比达 46.3%，诈骗方式主要为电话、短信和钓鱼网站等，如图 2-22 所示。

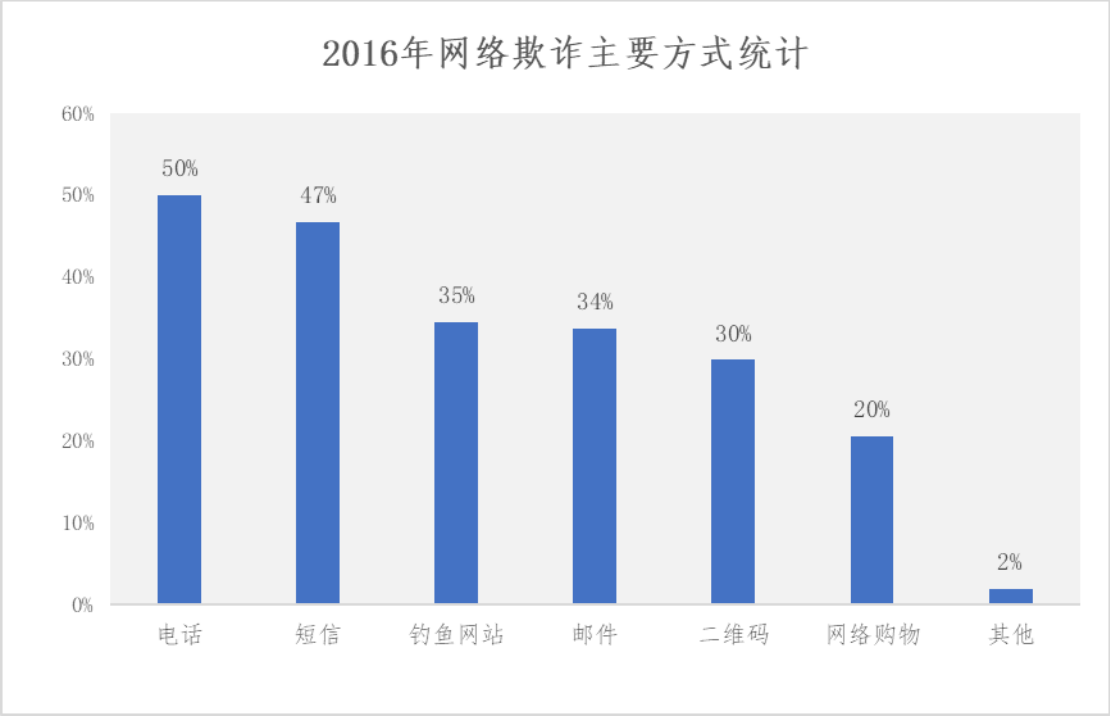

图 2-22 2016 年网络欺诈主要方式统计

调查显示，用户遭遇网络欺诈后发生经济损失的占比 53.08%，超过半数。其中单用户经济损失金额在 100 元-1000 元区间的占比最高，如图 2-23 所示。

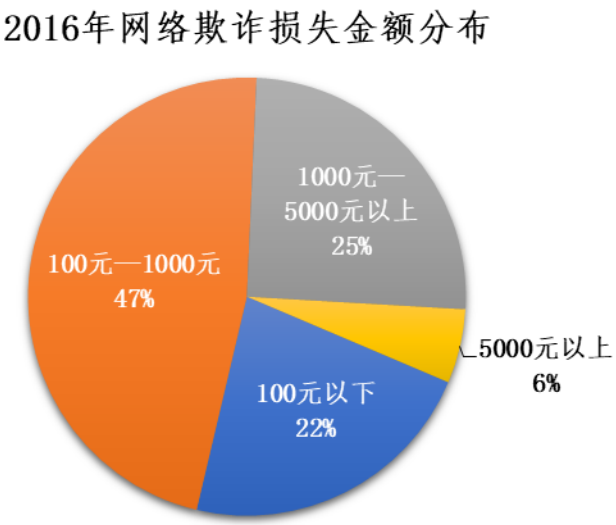

图 2-23 2016 年网络欺诈损失金额分布

用户遭遇网络欺诈后选择报案的比例占 40%，说明多数用户遭遇网络欺诈后选择不报案，用户维权意识相对不高。

报案后公安部门受理案件占比 86%，全部追回经济损失占 61%，说明公安部门高度重视网络欺诈案件侦破。如图 2-24 所示。

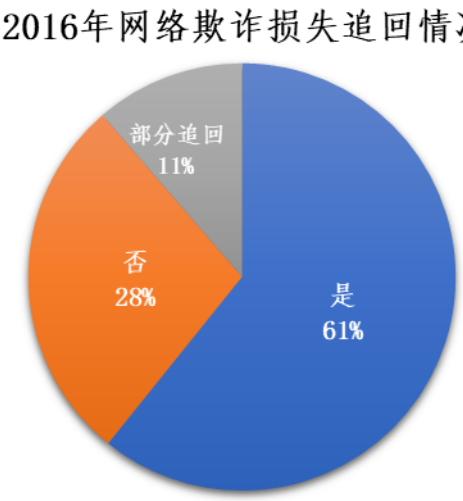

图 2-24 网络欺诈损失追回情况

从网络欺诈场景看，既有传统的中奖欺诈、假冒银行、网购退款，又新增虚假兼职、金融互助、APK 木马、虚假红包等新的欺诈形式。值得注意的是，一些传统的诈骗手法结合了新的通讯信息工具和社会热门趋势，爆发出更大的危害，也使得骗局更难以识别，如图 2-25 所示。

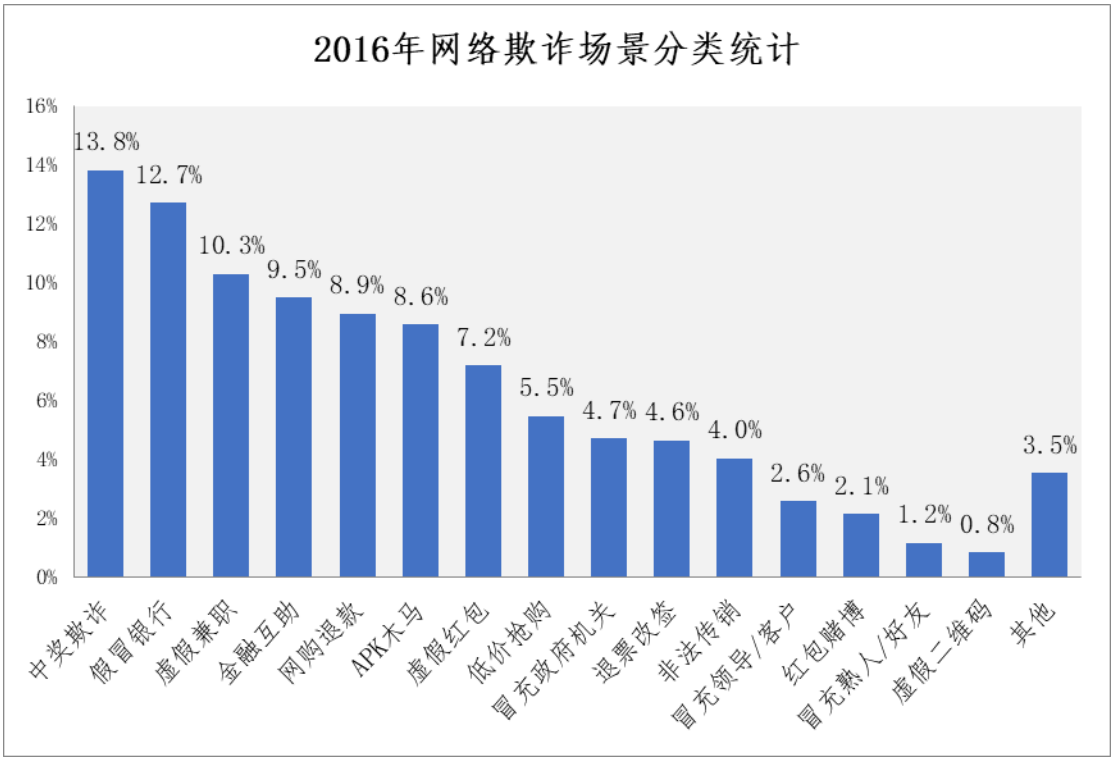

图 2-25 网络欺诈场景分类统计

2016 年，国家相关部门为打击网络诈骗犯罪做出了积极的努力，各企事业单位也通过自身努力积极参与，形成齐抓共管的治理局面。但打击网络诈骗将是一个长期的过程，建议广大用户应提升网络安全意识，避免上当受骗。

2.5 网络安全厂商品牌信赖度调查分析

2016 年我国网络安全市场最受用户信赖的厂商品牌调查结果显示，奇虎 360、安天电子、安信华、华为、亚信安全、安博士、安讯奔、腾讯、小米、瑞星成为排名前十位的网络安全厂商品牌，其中国产品牌占半数以上，近年来，国产品牌在网络安全防护产品的自主研发上取得了丰硕的成果，市场份额也逐年增长，赢得了用户的信赖。

企业名称	企业品牌
360	360
安天	安天 ANTIY
安信华	ANCHIVA
华为	HUAWEI
亚信安全	AsiaInfo 亚信安全
安博士	AhnLab
安讯奔	安讯奔 安全认证 超越云端

腾讯	Tencent 腾讯
小米	小米 www.mi.com
瑞星	RISING 瑞星

网络安全细分市场众多，产业链环节丰富，涉及行业广泛，在参与评选的 52 家网络安全厂商中，包括专业安全厂商、互联网厂商和创新型网络安全厂商。各类厂商基于各自核心资源和竞争优势，为个人用户、政企客户提供安全保障和安全服务。

三、2016 年网络安全状况

3.1 2016 年网络安全状况分析

3.1.1 勒索软件爆发式增长

2016 年全球范围内勒索软件爆发式增长。根据国内外防病毒厂商提供的数据显示，新的勒索病毒家族数量从 2015 年的 29 个暴增至 247 个，较 2015 年，勒索病毒家族数量增长了 752%。勒索病毒在全球导致企事业单位的损失高达 10 亿美金。2016 年，一款名为“ Locky ”的勒索软件变种在中国肆虐，爆发后短短几天内，国内数十家大型机构陆续受到侵害。该勒索软件导致某央企一周内连续三次中招，导致企业部分终端瘫痪，造成极大损失。

3.1.2 关键信息基础设施成为黑客攻击的新目标

当前，黑客攻击目标已从个人电脑、企事业单位转向关键信息基础设施领域。政府、金融、能源等行业成为黑客攻击新目标。关键信息基础设施一旦遭到破坏，会对国家安全、经济稳定和公众安全产生严重影响。

近年来，各国因关键信息基础设施被攻击而遭受重大损失的事件层出不穷，如 2011 年伊朗数千台离心机因感染“震网病毒”而损毁；爱沙尼亚和格鲁吉亚的政府、金融系统都因大规模网络攻击而被迫关闭；乌克兰电站因网络攻击而瘫痪等。

2016 年相继曝出多个关键信息基础设施被攻击的事件，如德国核电站计算机系统在安全检测中发现恶意程序，关闭发电厂，造成业务中断。美国旧金山地铁电脑票价系统遭到黑客攻击，被黑客勒索 100 比特币赎金，导致所有地铁购票系统无法正常工作，旧金山地铁公司被迫开放地铁免费乘坐。

3.1.3 金融网络安全事件频发，损失惨重

金融系统由于其高价值特性，是黑客攻击重点领域。黑客攻击金融行业已不仅满足盗取个人数据、金融重要信息，而是开始大规模转向系统类网络攻击。系统类网络攻击主要是破坏入侵金融流程、支付交易后台系统、攻击企业服务器导致网站系统崩溃，客户无法使用。

2016 年，针对银行 SWIFT 银行结算系统攻击逐渐增多，全球多个国家金融系统遭到网络攻击，导致巨大损失。如孟加拉央行遭受黑客攻击，损失 8100 万美金；厄瓜多尔银行 1200 万美金被盗；俄罗斯中央银行由于黑客攻击损失 3100 万美金。

3.1.4 个人信息泄露事件依旧高发

近几年来，个人信息泄露事件频发，根据中国互联网协会发布的数据显示，2016 年 54%网民认为个人信息泄露情况严重，84%网民亲身感受到因个人信息泄露带来的不良影响。

2016 年国内外均被曝出重大个人信息泄露事件，如被誉为史上最大规模互联网信息泄露事件的雅虎 5 亿条用户信息被黑客盗取，包括用户姓名、电子邮箱、电话号码、出生日期和部分登录密码；希拉里邮件门事件，影响美国大选结果；支付宝实名认证存在漏洞，用户实名认证信息多出 5 个未知账户，引起舆论广泛关注。

3.1.5 移动终端成为 APT 攻击新战场

移动终端已成为 APT 的新战场。2013 年，安全公司披露了首个移动终端上的针对性攻击事件，其结合传统网络攻击下的邮件钓鱼攻击模式和移动终端的木马程序完成对特定目标人物智能设备的攻击和控制。这个事件的公开披露意味着移动威胁的攻击动机已不局限于

利用黑色产业链牟取直接的经济利益，在攻击目标群体的选择上也不局限于泛化的移动终端用户。

截止到 2016 年末，已公开揭露的针对移动终端的 APT 攻击事件已有数十例，其不仅针对 Android 平台，也覆盖了 IOS、黑莓等其它智能平台。

3.2 国内外重大网络安全事件概览

3.2.1 国内两大漏洞平台突然关闭引发行业热议

2016 年 7 月 19 日晚间，国内最大的“白帽黑客”社区乌云网突然关闭。与此同时，企业级互联网测试平台漏洞盒子也宣布，暂停接受互联网漏洞与威胁情报。

乌云网和漏洞盒子的关闭，引发业界关于“白帽子”黑客行为边界的大讨论。

3.2.2 孟加拉国中央银行黑客攻击事件

2016 年 2 月，孟加拉国中央银行在美国纽约联邦储备银行开设的账户遭黑客攻击，失窃 8100 万美元。据相关执法部门调查，赃款几经分批中转，最终流入菲律宾两家赌场和一名赌团中介商的账户，随后很可能变成一堆筹码，就此消失无踪。而孟加拉央行并非个案，2015 年 1 月，黑客攻击了厄瓜多尔南方银行，利用 SWIFT 系统转移了 1200 万美元。

3.2.3 德国电信黑客攻击事件

2016 年 11 月 27 日 17 时左右，德国电信遭遇网络攻击，超 90 万路由器无法联网，持续数小时。30 日 8 时，再次出现断网。除了联网服务外，德国电信用户还用这些路由器来连接电话和电视服务。事件影响全国范围内的众多用户。

研究人员分析，攻击中的恶意 payload 源自于一台已知的 Mirai C&C 服务器，恶意程序是基于 Mirai 代码构建的互联网蠕虫。

3.2.4 希拉里邮件门事件

2015 年年初，邮件门事件首次被曝光，希拉里在 2009 年至 2013 年担任美国国务卿期间，违规使用私人电子邮箱和位于家中的私人服务器收发大量涉密的邮件．涉嫌违反美国《联邦档案法》，面临调查时又匆匆删除。2016 年夏季，美国民主党全国委员会、筹款委员会、竞选团队被黑客组织入侵，近 2 万封邮件被维基解密披露。邮件显示，希拉里涉嫌抹黑竞争对手，以及可能涉嫌洗钱等财务问题。10 月 28 日，黑客 Kim Dotcom 翻出被希拉里删除的邮件，导致 FBI 重新开始调查希拉里邮件门事件。主流媒体大多认为黑客行为直接影响了此次美国大选，并最终导致希拉里落选。

3.2.5 Mirai 僵尸网络攻击导致网络瘫痪

10 月 21 日，恶意软件 Mirai 控制的僵尸网络对美国域名服务器管理服务供应商 Dyn 发起 DDoS 攻击，导致美国多个城市出现互联网瘫痪情况，包括 Twitter、Shopify、Reddit 等在内的大量互联网知名网站数小时无法正常访问。Mirai 僵尸网络中包含了大量可联网设备，例如监控摄像头、路由器以及智能电视等等。由于此次攻击中有大约 60 万台的物联网设备参与到 Mirai 僵尸网络大军中，成为大规模物联网设备首次参与企业级攻击的一个关键案例。

3.2.6 雅虎大规模用户信息泄露事件

2016 年 9 月，雅虎突然宣称其至少 5 亿条用户信息被黑客盗取，其中包括用户姓名、电子邮箱、电话号码、出生日期和部分登录密码。并建议所有雅虎用户及时更改密码。此次雅虎信息泄漏事件被称为史上最大规模互联网信息泄露事件，也让正在出售核心业务的雅虎再受重创。此次事件导致雅虎股价下跌 2.4%，至 39.91 美元。

3.2.7 美国 NSA 再现泄密风波

继斯诺登泄密风波之后，美国国家安全局（NSA）再次敲响内部威胁警钟。NSA 承包商哈罗德仕马丁于 8 月 27 日因窃取国安局数据被捕，马丁与曾揭露美国政府大规模监听行动的斯诺登受雇于同一家公司，马丁还被怀疑掌握了 NSA 的“源代码”，这些源代码通常被用

来入侵俄罗斯、中国、伊朗等国的网络系统。调查人员在马丁家中和车内搜出美国政府高度机密文件的复印文本和数字文档，其中数字文档至少有几 TB，还包括 6 份“敏感情报”。

3.2.8 NSA 下属方程式黑客组织（Equation Group）被黑事件

2016 年 8 月，美国国安全局（NSA）疑似遭遇黑客攻击。黑客团伙声称入侵了“Equation Group”（方程式组织），并获取了该黑客组织的黑客工具。该黑客团伙自称为“The Shadow Brokers”（影子经纪人），该团伙表示，其手中掌握着大量机密数据，计划在网上举行一次拍卖会，并将这些机密信息出售给竞价最高的竞标者。从后续发展来看，该事件属实。

3.2.9 俄罗斯央行黑客袭击事件

2016 年 12 月，俄罗斯央行官员称账户遭黑客袭击，被盗取了 20 亿俄罗斯卢布(约合 3100 万美元)资金。而 2016 年 11 月，已有俄罗斯五家主流大型银行遭遇长达两天的 DDoS 攻击，攻击来源是由 30 个国家 2.4 万台计算机构成的僵尸网。

3.2.10 德国核电站检测出恶意程序被迫关闭

2016 年 4 月，德国 Gundremmingen 核电站的计算机系统，在常规安全检测中发现了恶意程序。虽然未发生较大事故，但仍旧被迫关

闭发电厂。此恶意程序是在核电站负责燃料装卸系统的 Block B IT 网络中被发现。

3.3 病毒技术发展趋势分析

3.3.1 人工智能引领下一代防病毒技术发展

随着人工智能技术（Artificial Intelligence，简称 AI）的发展，防病毒技术已从第一代病毒库特征码比对阶段，第二代云扫描引擎或沙盒分析技术（行为比对阶段），发展为机器学习模型为主的人工智能防病毒技术。

机器学习（Machine Learning，简称 ML），利用数据模型对于大量数据、样本进行分析对比，并总结成为可不断积累不断成长的分析模型，对于未知威胁可以快速预测和判定，从而达到病毒检测、病毒分析的目标。

人工智能技术的出现，弥补了网络安全界中对于未知威胁侦测的不足。传统的病毒库特征码比对、云扫描等检测技术，针对已知病毒具有非常高效的侦测能力，但对于新出现的未知病毒，在没有病毒特征码的情况下，往往无法快速有效的识别和阻拦病毒的扩散，而基于机器学习模型的人工智能技术，则可以根据未知病毒的行为和特征做出迅速识别并抵御风险。目前，国内已有安全企业率先将机器学习模

型成功的应用到下一代防病毒系统中, 未来人工智能技术在网络安全方面的大范围应用，也势必带来新的技术变革发展趋势。

3.3.2 VMI 技术引领移动终端安全技术发展

随着智能终端的快速普及, 移动终端逐渐成为一块主流“ 屏幕 ”。移动化浪潮改变了人们的生活、工作方式, 线下手机支付已成为习惯, 三成网民使用线上办公，各级政府及机构加快“ 两微一端 ”（微博、微信及新闻客户端）线上布局，推动互联网政务信息公开向移动、即时、透明的方向发展，提高用户生活幸福感和满意度。智能终端在实现便利生活、提升办公效率的同时，也模糊了网络安全边界，移动终端安全也成为网络安全综合管理的重要一环。

移动终端安全技术，目前以终端安全管理为核心，通过移动终端部署相应的安全防护产品, 并加强网络边界接入控制和身份认证等传统技术防护措施为主，但无法有效解决移动办公时诸如“ 手机丢失、数据泄露 ”等风险。

针对这类问题, 虚拟手机解决方案可以有效避免生产数据在移动终端本地留存、数据泄露等问题。

虚拟手机技术, 采用了虚拟移动基础架构在 x86 服务器上创建若干个安卓虚拟手机系统, 用户使用移动终端通过网络连接来获取账号权限所对应的独立虚拟手机系统，所有的应用、办公系统的使用、查询、处理等操作均在服务器上完成，用户的移动终端只是作为屏幕来显示和操控，并且服务器与终端设备之间加密传输的是屏幕信号，这

样就实现了生产数据不在本机留存，也无需担心网络劫持，有效的解决了“数据不落地”的风险，甚至手机丢失，也无需担心数据泄露。

虚拟手机技术彻底颠覆了移动终端安全管理的架构，改变了传统的安全防护重心，将原本庞大而复杂的网络边界变得清晰明确，把重点防护由移动终端安全转变成中心服务器安全；并且有效解决传统模式下数据在本地留存引起的数据泄露等问题，实现真正意义上的“数据不落地”。随着未来移动办公应用的普及，虚拟手机技术将引领移动终端安全的技术革新，形成产业技术整体突破，在全国乃至全球形成技术影响力。

3.3.3 联动防护技术成为 APT 治理发展趋势

目前，在 APT 治理层面，主要是以网络分析、沙箱等技术为主，部分国内安全企业还推出了针对社工邮件、加密勒索邮件的网关设备。上述技术大都能实现对于 APT 威胁的发现或侦测，但发现问题后，因其工作原理限制，无法高效的处理 APT 威胁，不能形成从侦测到处置的完整闭环，而联动防护机制的出现，恰好弥补了这一问题。

联动处置，是指将已侦测出来的 APT 威胁， 通过标准化的 API 接口，加入到防火墙、入侵检测 IPS、加密勒索邮件网关或企业版防病毒管理中心等安全防护类设备中，通过实时获取这些威胁的特征码（包含威胁的源头、目标、种类等信息），并加入到安全防护技术产品的黑名单中，实现对于 APT 威胁的阻断或拦截，从而实现从侦测发现到联动处理的处置闭环。

当然，联动处置体系的实现需要借助其可扩展性及与多种技术产品的集成能力，以满足不同的网络安全环境需求。联动防护技术，会将整个安全基础架构编排到可适应防御体系中，并可根据特定环境和攻击者来调整此防御策略，覆盖了 APT 治理的事前发现探测、事中控制处理以及事后排查追溯的所有环节，其重要性不言而喻，已逐渐成为 APT 治理技术的发展趋势。

四、病毒疫情与安全事件的对策和建议

4.1 积极落实《中华人民共和国网络安全法》相关要求

2016 年 11 月 7 日，第十二届全国人大常委会第二十四次会议通过了《网络安全法》，并将于 2017 年 6 月 1 日正式实施。《网络安全法》的公布施行，对于贯彻落实总体国家安全观，依法加强国家网络安全管理，维护国家网络空间主权、安全和发展权益，健全国家网络安全保障体系，全面提高网络安全保障水平，具有十分重要的意义。

对于政府主管部门要努力做到：

一是政府部门自身要自觉主动地按照法律要求，进一步健全完善内部各项网络安全规定，落实法律规定的义务和责任。

二是相关主管部门要加强打击网络犯罪行为。现阶段，网络犯罪逐渐呈现出产业化、低龄化、专业化等特征，已经成为危害公共安全、

国家安全的重要方面。落实《网络安全法》，强化网络犯罪的打击能力。

三是相关主管部门要加强行业监管力度。按照《网络安全法》及《网络产品和服务安全审查办法》的相关规定，金融、电信、能源等重点行业主管部门，应加强行业监管力度，组织开展本行业、本领域的网络产品和服务安全审查工作。

四是扎实开展《网络安全法》的宣贯工作，在本单位及广大民众中普及宣传网络安全法的相关知识，增强网络安全意识。

五是加强网络安全人才培养工作。当前网络空间的竞争，归根结底是人才的竞争，我国网络安全人才缺口巨大，高级网络安全攻防取证专家严重匮乏。相关主管部门应通过学科建设、实践对抗等方式，加强网络安全人才培养。

对于企事业单位要努力做到：

一是要积极学习和贯彻《网络安全法》各项内容和规定，完善企事业单位的信息安全管理规定。

二是切实落实网络安全等级保护工作。按照国家网络安全等级保护相关要求，按标准建设安全保护措施，建立安全保护制度，落实安全责任，有效保护本企事业单位的信息系统安全。

三是加强对本单位员工计算机病毒防治工作的教育及引导，提升员工网络安全防护意识。

4.2 积极建设网络安全防御技术体系

一是建议政府、企事业单位部署综合计算机病毒防护产品，在用户计算机、移动终端、服务器、网关（含邮件网关）等位置采购专业、有效的防病毒产品，提升本单位网络安全防御技术水平。

二是购买专业化应急响应服务，建立专业的安全运维体系，定期更新病毒库、及时为系统打补丁，定期进行重要系统信息安全检查工作。

4.3 加强公众信息安全教育工作

加强教育与引导，向广大计算机用户普及网络安全防护知识，提升网络安全防护意识，形成良好的上网习惯，包括不打开可疑邮件和可疑网站、不随意接收或打开收到的网站链接、使用移动介质时养成先扫描的习惯、及时更新操作系统补丁等，以降低病毒、木马感染的可能性。

致谢

报告撰写过程中，得到亚信科技（成都）有限公司的鼎力协助，腾讯科技(深圳)有限公司、哈尔滨安天科技股份有限公司、奇虎 360 公司、北京瑞星信息技术有限公司、金山软件股份有限公司等为病毒中心提供了相关数据支持，在此表示感谢！

新华社、腾讯网、新浪网、搜狐网、网易网、北方网、赛迪网、《信息网络安全》、《中国信息安全》、51CTO 多家单位作为支持媒体参与此次活动，在此表示感谢！

同时,感谢以下单位对“ 第十六次计算机和移动终端病毒疫情调查活动 ”的支持。

协办单位：

AsiaInfo | 亚信安全

支持单位：