第十五次全国信息网络安全状况暨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发布

2016 年 6 月

目　录

报告摘要

为了解掌握2015年我国信息网络安全情况，宣传、普及信息网络安全知识，提高广大用户网络安全防范意识，国家计算机病毒应急处理中心（以下简称“病毒中心”）于2015年12月20日至2016年1月20日在全国范围内组织开展了“第十五次全国信息网络安全状况暨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主办，病毒中心和计算机病毒防治技术国家工程实验室承办，中国反恶意软件联盟及十一家反病毒产品生产厂商参与活动并提供支持。中央电视台、新华社、人民网、新浪网、搜狐网、网易网、北方网、腾讯网、《中国计算机报》、《信息网络安全》、《中国信息安全》11家单位作为支持媒体参与此次调查活动。

网络空间已成为继海、陆、空、天之后，人类“同呼吸、共命运”的新空间，成为各国力量博弈的新战场。互联网的出现使得信息流动不再受地理空间所限，资源获取更加便捷。互联网的发展改变着我们的生活，同时也对我国的政治、经济、文化等方面，产生了重大的影响。伴随着互联网发展的不断推进，网络安全在整个国家安全中的地位不断提升，可以说没有网络安全，就没有国家安全。在过去的一年时间

内，中国政府、组织机构和安全企业以不同的方式在各自的领域里，对网络安全的发展倾注自己的力量。在政策引领、法律规范、技术提升、安全教育、打击犯罪、行业自律、网络行为规范等不同方面，为实现网络空间的安全可信共同努力。

基于上述背景，在公安部网络安全保卫局的指导下，病毒中心继续开展了病毒疫情调查活动。调查结果显示，2015年，64.22%的被调查者发生过网络安全事件，与 2014 年相比下降了 24.48%; 感染计算机病毒的比例为 63.89%, 比 2014 年增长了 0.19%; 移动终端的病毒感染比例为 50.46%，比 2014 年增长了 18.96%。安全事件呈现出下降的态势，但移动终端的病毒感染率涨幅较大。

2015 年，感染病毒、木马等恶意代码再次回潮，成为最主要的网络安全威胁。值得注意的是，更多的恶意代码并不像传统意义上的病毒，而是向灰色地带过渡。作为传统 PC 和移动终端共同面临的安全问题, 网络钓鱼/网络欺诈日趋严重。网络诈骗告别了以往单纯依靠病毒的局面，更多的与数据泄露的信息相结合，将大数据统计分析得出的结果应用于网络诈骗，使诈骗定位更精准，得手几率大大提高。APT 攻击愈演愈烈，2015 年出现了多起高水准的 APT 事件，“方程式（EQUATION）”、DUQU2.0 和 APT-TOCS 等事件都极具代表性。5 月出现的“毒液漏洞”（VENOM）可造成虚拟机

逃逸，使数以百万计的虚拟机处于网络攻击风险之中，攻击者可以使监控程序崩溃，并获得目标机及其运行的虚拟机的控制权。该漏洞威胁到全球各大云服务提供商的数据安全，并有可能影响到成千上万的机构和数以百万计的终端用户。

2015 年，各类敲诈勒索软件在我国大量涌现、肆虐传播，成为近两年增长最快的网络威胁之一。数据泄露事件频繁发生，由网络攻击引发的数据泄露事件依旧猖獗，造成了巨大经济损失和舆论压力。网络攻击目标从政府机构扩大到民众社会生活各个方面，涉及电信、金融、能源等多个领域。

针对这些网络犯罪活动频发与升级的现象，我国加速了信息安全法律法规的制定，同时也加大了对网络犯罪的打击力度，2015 年 6 月，第十二届全国人大常委会第十五次会议初次审议了《中华人民共和国网络安全法(草案)》。各部委联合组织了“剑网 2015”、“猎狐”专项行动全面治理网络乱象，打击网络非法行为，净化网络环境。这标志着我国已全面深入地进行网络安全法制建设。

伴随互联网的快速发展，网络与信息安全问题也逐渐凸显，并日益受到人们的关注。移动互联网的扁平网络、多元业务和智能终端，既是其区别于传统互联网的优势，同时也导致安全威胁叠加。智能终端的操作系统存在安全漏洞、防病毒软件功能还不够完善，加之用户防范意识不足，受攻击的概率大大高于传统 PC 机。2015 年移动终端网络钓鱼事件

大幅度上涨、勒索软件大量涌现。基于安卓系统的恶意应用和恶意软件数量急剧增加，IOS 也走下神坛，不再是坚不可摧。移动设备已经取代传统个人电脑成为主流上网工具，移动安全领域的问题日趋复杂，不法分子利用钓鱼网站瞄准手机支付用户群体，利用仿冒移动应用、移动互联网恶意程序、伪基站等多种手段，实施跨平台的欺诈和攻击。

除了针对传统 PC 平台，针对移动平台的 APT 攻击也越来越多。智能手机等移动终端，用户粘性大，实时在线率高，联系人之间的信任强度更大。加之移动终端与传统 PC 存储的信息具有差异性，如电话簿、短信息、地理位置信息等都是从传统 PC 端无法获取的。因此，各类安全威胁纷纷向移动终端转移。移动安全已经成为安全领域的焦点话题。

第一章 调查介绍

一、报告术语界定

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。

二、调查方法说明

为了进一步增强调查数据的代表性、全面性和准确性，此次调查活动在延续以往线上调查的基础上，增加了线下调查的方式。线上部分调查采取网上调查的方式，在病毒中心网站（www.cverc.org.cn）开设了调查专栏，调查范围面向全国信息网络联网单位和计算机及移动终端用户，同时通过腾讯安全管家推送调查问卷。线下部分病毒中心联合参与此次活动的反病毒产品生产厂商在北京、上海、天津、广州、哈尔滨、成都、武汉、南京、福州、珠海、银川等11个城市，开展以“2015年全国信息网络安全状况暨计算机病毒疫情调查活动”为主题的入校园、入企业等系列宣传、教育活动。

主要调查内容为：2015年1月至2015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、感染途径等情况。

第二章 信息网络安全状况调查分析

一、2015 年网络安全事件

调查结果显示，2015 年 64.22%的用户发生过网络安全事件，比 2014 年下降了 24.48%。在发生的网络安全事件中，排在前三位的分别是感染病毒/木马程序、垃圾邮件、网络钓鱼/网络欺诈。其中感染病毒/木马占 60.5%，跃居到第一位，比 2014 年上涨了 9.1%；垃圾邮件比去年降低了 14.5%，以 46.2%位居第二；有 37.24%的用户遭遇了网络钓鱼/网络欺诈，比去年提升了 6.84%。除此之外，超过三成的用户（32.37%）遭到过网络攻击，相比去年有较大幅度增长，其它的网络安全事件还有个人信息泄露、虚拟身份被盗（QQ、微信）、盗版手机 APP、虚拟 WIFI 盗号、财产被盗等。

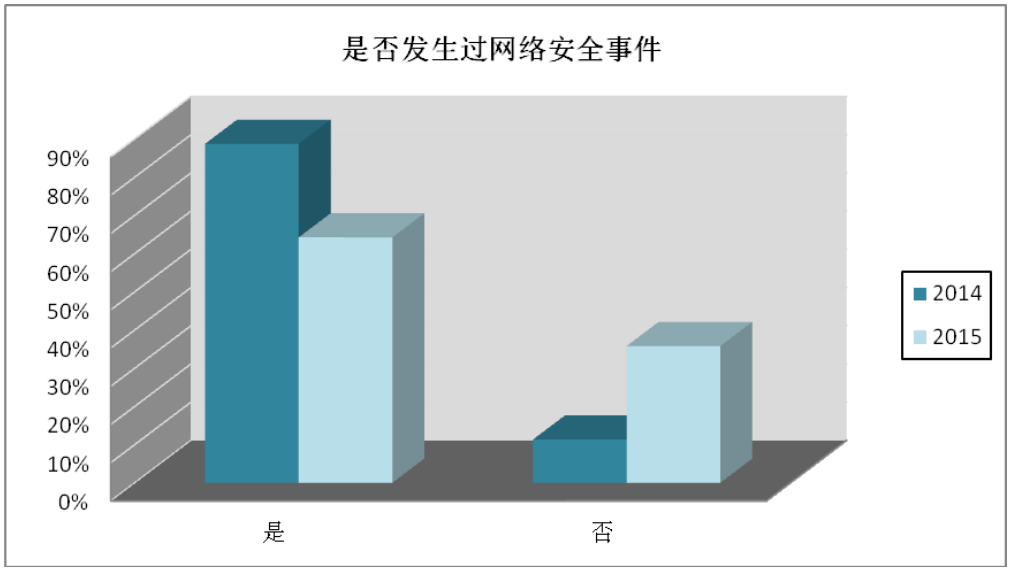

图 1　是否发生过网络安全事件

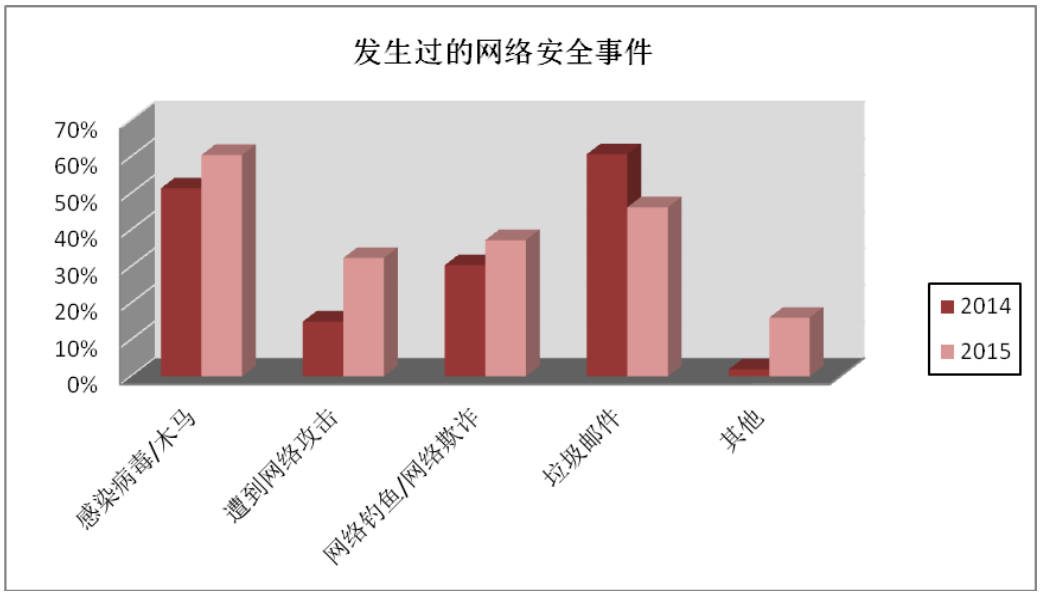

图 2　发生过的网络安全事件

2015 年，感染病毒、木马等恶意代码再次回潮，成为最主要的网络安全威胁。值得注意的是，更多的恶意代码并不像传统意义上的病毒，而是向灰色地带过渡。很多恶意代码并不会给用户系统带来直接的损害，而通常在是在不影响系统运行的前提下，与垃圾邮件、广告、购物网站、博彩网站等相结合，强制捆绑、强制安装，进而实施获取流量、盗取个人信息等恶意行为。其捆绑的软件，也从中获得了巨大的收益。事实证明，此种方式具备较强的隐蔽性，通常会形成更广泛的传播，并给用户造成更持久的危害。虽然随着安全软件的广泛普及，病毒和木马被发现的时间越来越早，同时多层面全方位的病毒防控措施也提高了病毒和木马被查杀的机率，但病毒、木马不断推陈出新，仍然是用户和安全厂家面临的最主要的安全问题。

垃圾邮件仍然是安全事件关注的重点。长久以来，垃圾邮件不仅是商业推广的利器，也是恶意用户的帮凶。通过垃圾邮件传播恶意程序、虚假链接、诈骗信息等，是恶意用户优先选择的传播途径。它们或感染系统、窃取受害计算机的数据，威胁用户的数据和财产安全，还有可能使其成为僵尸网络中的一员，甚至成为 APT 攻击的切入点。垃圾邮件在出现多年后，还得以生存的原因主要是成本低廉，一方面可以很容易申请到邮箱地址，另一方面可以通过感染用户系统进而利用用户的邮箱继续发送垃圾邮件；而反垃圾邮件产品很难提出一套完整的解决方案，严格的过滤规则会导致误报率的提高，在反垃圾邮件产品不断改进的同时，垃圾邮件也不断变换内容和形式，以躲避反垃圾邮件产品的拦截。

作为传统 PC 和移动终端共同面临的安全问题，网络钓鱼/网络欺诈日趋严重。不法分子实施欺诈的手法不断推陈出新，他们广泛利用数据泄露的私密信息，充分结合社会工程学，使得遭受欺诈的用户有增无减。“网络+社交+电话”的复合模式成效显著。网络诈骗告别了以往单纯依靠病毒的局面，更多的与数据泄露的信息相结合，将大数据统计分析得出的数据应用于网络诈骗，使诈骗定位更精准，得手几率大大提高。钓鱼、欺诈的最终落脚点几乎都直指经济利益，绝大多数上当受骗的用户都蒙受了不同程度的经济损失。

2015 年,遭到过网络攻击的用户大幅度增长,APT、DDOS、网络监听、密码破解、端口扫描及渗透、漏洞扫描等都是常见的攻击模式。除传统的攻击模式外,针对国家、重点行业、关键社会基础设施的 APT 攻击则愈演愈烈,出现了多起高水准的 APT 事件,“方程式(Equation)”、Duqu2.0 和 APT-TOCS 等事件都极具代表性。

APT 紧密围绕政治、经济、科技、军工等热点领域及事件,事关经济、国家安全和公共安全等方方面面。在 APT 攻击威胁的阴霾笼罩下,能源化工、基础交通、电力生产、配送安全都面临重重风险。但 APT 的目标还不仅仅局限于此,由商业竞争引发的 APT 攻击也不断增加,任何有价值的机构甚至个人都有可能成为 APT 的目标。统计显示,鱼叉攻击和水坑攻击依然是 APT 组织最青睐的入侵方式,相对于高成本的物理接触,攻击者更多的会选择利用社会工程学方式,并充分结合漏洞,精心伪装,引诱目标中招。由于已公开的后门会被安全软件频繁查杀,攻击者更倾向于自主开发和使用委托定制的后门程序。

商用木马、标准化的渗透平台等已经被广泛用于各种定向持续攻击中,这使得攻击者不再需要高昂的恶意代码开发成本,这种成本较低的攻击模式大大降低了对攻击者能力和资源储备的要求。但同时,这种高度“模式化”攻击也会让攻击缺少鲜明的基因特点,给攻击的追根溯源带来了更大的难度。

与电脑相比，路由器系统软件更新补丁程序的速度较慢，设备厂商对于安全性的重视程度也与电脑系统厂商有一定的差距，因此，路由器安全漏洞也频频被恶意软件和黑客加以利用。低端家用路由器与电脑、手机已经成为了黑客重点攻击的三大目标。2015 年仍有多款路由器产品被曝出存在漏洞，黑客可以利用漏洞任意下载配置文件，绕过设备认证，随意修改系统配置，造成用户敏感信息泄露，危害极大。另外，一些路由器厂家为了便于产品售出后的调试和检测，会在产品上保留超级管理权限。一般情况下，这个超级管理权限是不容易被外人发现的，但一旦被黑客发现并破解，就意味着黑客可以直接对路由器进行远程控制，进一步发起 DNS 劫持、窃取信息、网络钓鱼等攻击，直接威胁用户网上交易和数据存储安全。

虚假 WiFi 盗号是近些年来较为突出的安全问题。公共场所 WiFi 几乎已经成为了公共场所服务范围内的标准配置，目前我国 WiFi 热点覆盖至少超过千万个。不法分子经常在提供免费上网的场所搭建不需要密码即可接入的虚假 WiFi，当用户进行浏览网页、聊天、登录网银、网上交易等操作时，不法分子即可记录并窃取用户的这些信息。

二、浏览器安全状况

浏览器作为用户与网络连接的主要窗口，已经成为发生

网络安全事件的重要途径，调查显示，浏览器市场呈现出百家争鸣的态势，占有率较高的有 360 浏览器、IE 浏览器、QQ 浏览器，搜狗、百度、谷歌浏览器的使用者也都超过了 10%。

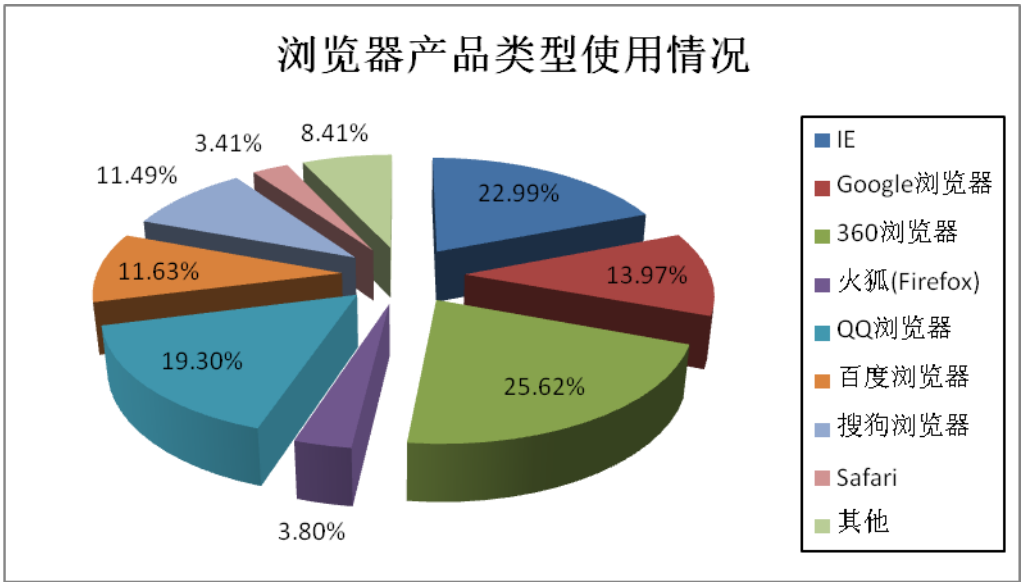

图 3　浏览器产品类型使用情况

用户在使用浏览器过程中遇到的最主要安全问题是“恶意软件/流氓软件”，占 54.8%，随后的是“网络钓鱼/网络欺诈”和“浏览器设置被篡改”，分别占 51.35%和 48.33%，25.27%的用户遭遇了隐私泄露或数据丢失。与往年相比，“浏览器设置被篡改”的比例有了显著下降。为了提升自身的安全性，更多的浏览器选择与安全厂家合作，融入了防篡改、防病毒等功能。但“网络钓鱼/网络欺诈”的比例有所提升，此类问题的防范通常仍采用黑白名单方式，因此，对于新出现的链接、事件等难于防范，用户稍有疏忽便会中招。

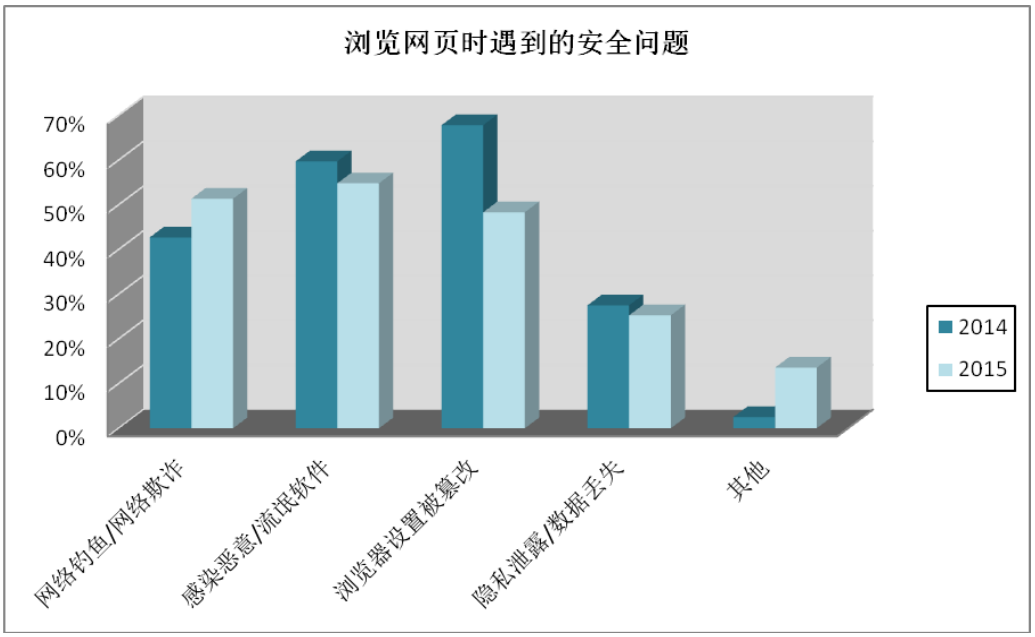

图 4　浏览器使用过程中发生的网络安全事件类型

三、网络安全管理情况

调查显示，在用户采用的安全管理技术和措施方面，76.94%的用户安装了主机或网络防病毒产品，42.2%的用户使用了防火墙。伴随着个人版防病毒软件和防火墙的免费化，基础安全软件的使用比例维持在较高水平。在企业用户中，尤其是在政府机关、大型企事业单位、金融系统和重要基础设施等关键部位，防病毒网关、邮件防病毒产品、IDS、IPS、APT 防护等产品也有一定数量的部署。

调查选项中的安全产品主要分为几大类，其中边界安全防护产品主要包括：防病毒网关、邮件防病毒网关、防火墙、IPS、UTM；系统安全防护产品主要包括：主机防病毒产品、网络防病毒产品；安全监测类产品主要包括：VDS、IDS；数据泄露防护（DLP）系统以及高级可持续威胁（APT）安全监

测产品。从总体情况来看，目前用户采用最多的产品为主机防病毒产品、网络防病毒产品和邮件防病毒产品，上述三类产品也是最基本的用户安全防护产品。从类别上来看用户目前较为关注的是边界安全和系统安全，而在安全状态监控和防治数据泄露上的重视程度还有待提高。而随着近几年高级可持续威胁的不断增多，用户对 APT 安全监测产品的部署正在增加。

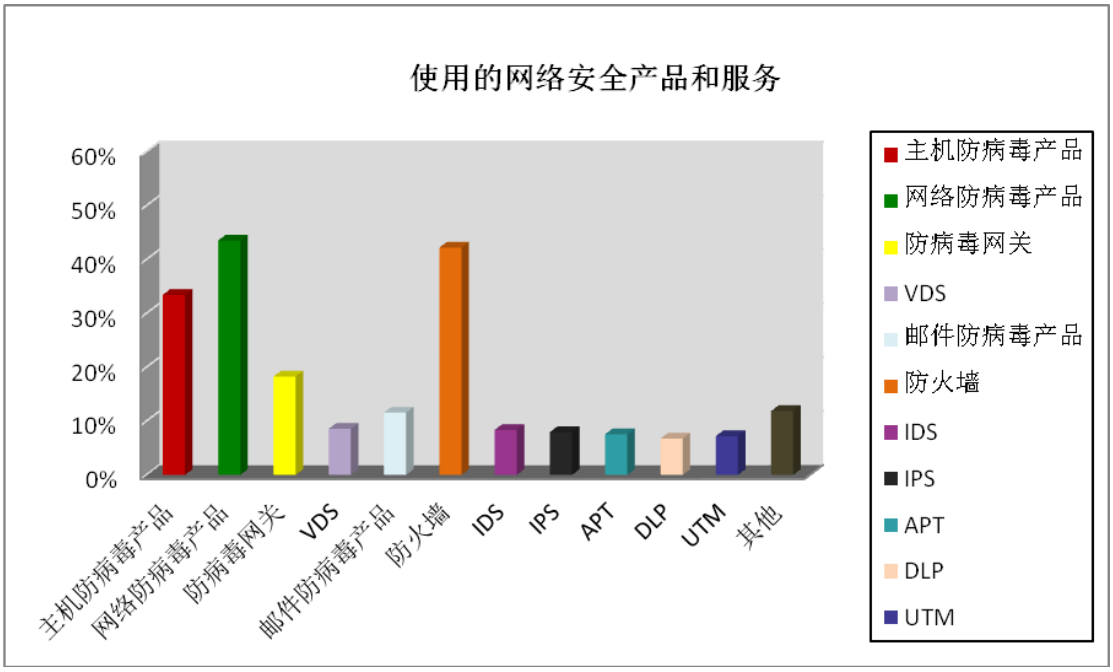

图 5　使用的网络安全产品和服务

调查显示，77.64%的用户使用过免费的云安全产品和服务。通过在云端存储数据，可以为企业节省大量成本，也给用户带来了方便快捷的用户体验，但大量的云端数据也成为恶意用户瞄准的攻击目标，其安全性已经引起了较为普遍的重视，基于云的网站安全检测和安全防护服务已被广泛应用。为了保护数据安全，互联网行业的巨头纷纷加大在该领域的技术和资金投入，越来越多的安全厂商通过云端技术进

行安全服务。

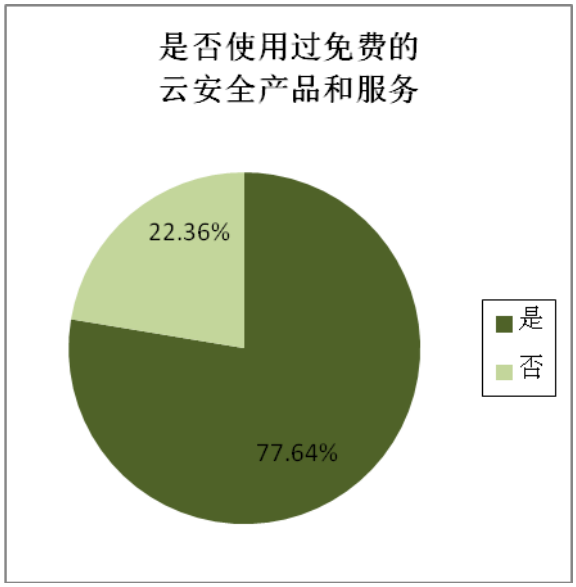

图 6　云安全产品使用情况

第三章 计算机病毒疫情调查分析

一、我国计算机用户病毒感染情况

2015 年我国计算机病毒感染率为 63.89%，与 2014 年基本持平。资金账户和私密信息，仍然是病毒、木马的主要攻击目标。通过 Web 注入的方式实现操控浏览器并辅以社会工程学，仍然是非常有效的攻击方法。除传统的安全事件外，钓鱼、诈骗和敲诈勒索事件也频繁发生。通过在前端部署安全产品，形成多级防护，可以拦截部分恶意软件和恶意网站，防止用户访问受感染的网站，在一定程度上降低了通过网络浏览传播木马、病毒的几率。

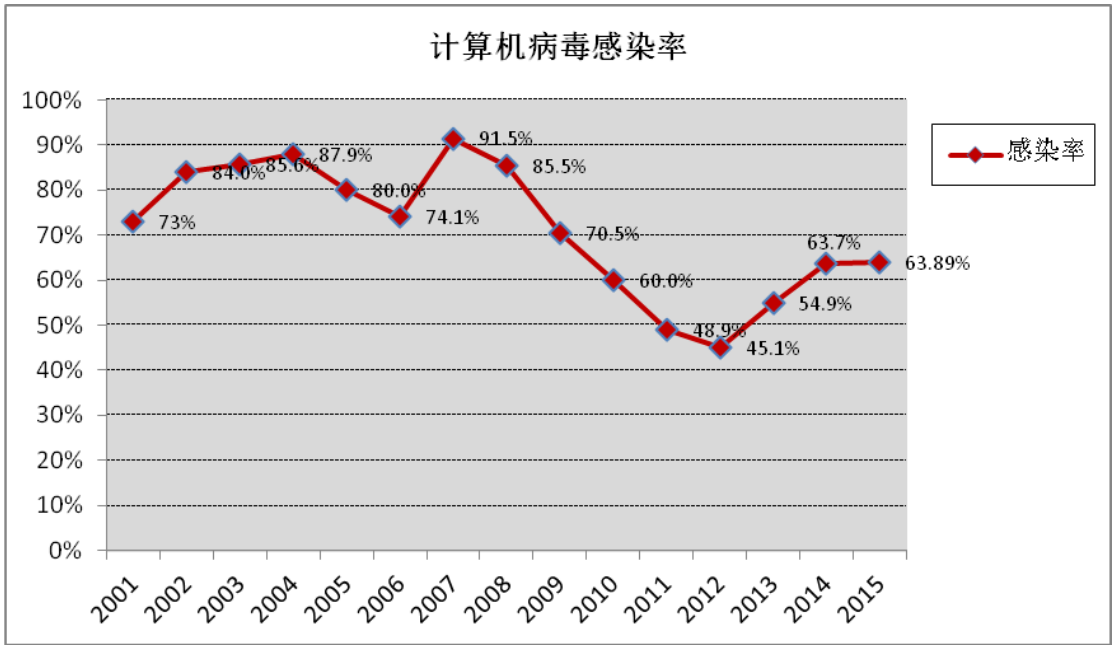

图 7　历年病毒感染比例曲线图

2015 年，勒索软件大量涌现。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。最早的移动终端勒索软件出现在 2013 年，伪装成安全软件蒙骗用户安装并用于勒索。如 CTB-Locker，2013 年首次出现，目前已经发展到第四代，勒索软件带有可通过验证的数字签名，可有效躲避多款杀毒软件的查杀。国外的勒索软件，往往是对重要文件进行加密进而实施勒索，为逃避事后追踪，勒索金往往是收取比特币。而国内勒索软件，多数用较低的技术勒索钱财，并没有将精力放在高强度加密的技术对抗上，勒索金收取的金额相对较少，但由于国内用户基数大，收入也颇为可观。

数据泄露事故不断发生，由网络攻击引发的数据泄露事件依旧猖獗，造成了巨大经济损失和舆论压力。网络攻击目标从政府机构扩大到民众社会生活各个方面，电信、金融、能源等多个领域均遭受攻击。2015 年 7 月，有新时代的 IT 军火供应商之称、专门从事 hacking 活动的 Hacking Team 被入侵，Hacking Team 是一家专门为攻击者提供工具和手段的公司，该公司 400GB 的内部资料遭到泄漏，各种平台的木马程序、大量未公开漏洞曝光，包括一些重磅级的 0DAY 漏洞。这些漏洞已经进入了黑色产业链，被用来进行病毒、蠕虫传播或者挂马盗号。此次泄露的各平台的木马后门程序，已经工程化的漏洞和后门代码大批量的公开，使得漏洞的利

用难度大大降低，整个灰色产业链的平均技术水平得到了普遍提升。针对政府部门机构、基础行业设施和社会民众生活的大量网络攻击行为呈现出肆无忌惮、泛滥成灾的特点。2015 年，我国也出现了多次大规模的信息泄露事件，如国内知名电子邮箱过亿数据泄漏，涉及邮箱账号、密码、用户密保等；国内多家品牌酒店存在安全漏洞，海量开房信息存泄露风险等。

在步入大数据时代的进程中，数据的价值和安全逐步得到用户认可和重视，对于海量数据分析所带来的价值日益凸显，对数据的分析极大的促进社交媒体、物联网和电子商务的发展，正因为如此，攻击者也更多的将目光集中在这里，不断发起针对数据的攻击。大量被泄露的数据已经成为黑色产业链中的重要信息资源。业务数据和用户数据的价值快速攀升，这些信息被分门别类，有针对性地匹配和精确定位，被用于团伙诈骗、钓鱼，或被用于精准营销，形成了一条完整的利益链条。与此同时，通讯、互联网厂商、应用和服务提供商都纷纷加大在数据安全方面的投入，开始布局数据安全。

二、我国计算机病毒传播的主要途径

调查显示，2015 年通过网络下载或浏览传播病毒的比例占 72.88%，比 2014 年上升了 12.88%，电子邮件紧随其后，

占 41.37%，排在第三位的是移动存储介质，占 33.46%。除此之外，局域网、社交软件、系统和应用软件漏洞等也是病毒传播的主要途径。

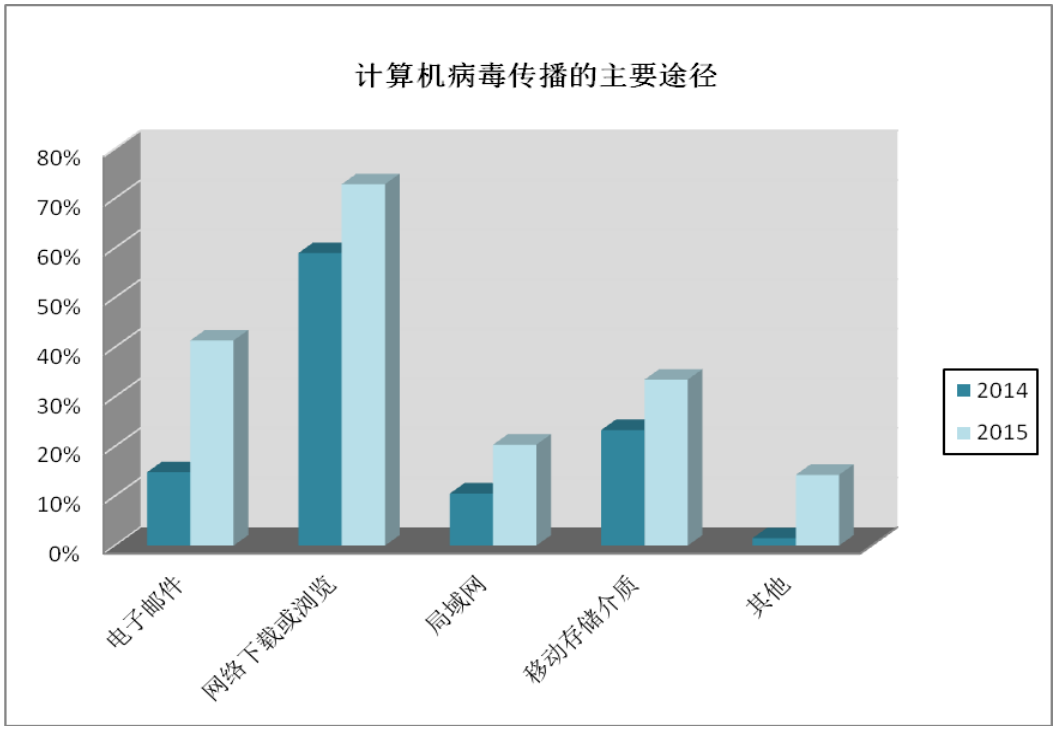

图 8　计算机病毒传播的主要途径

操作系统、浏览器和应用软件中存在的大量未修补的漏洞，仍然是联网用户的重大安全隐患，“零日”漏洞也成为恶意用户发动攻击的左膀右臂。国家信息安全漏洞库（CNNVD）统计显示，2015 年，新增信息系统安全漏洞 7754 个，比 2014 年略有下降，但漏洞数量总体增长趋势依旧持续。信息技术产品安全漏洞频频曝出，各种高危漏洞层出不穷，波及政府部门、互联网金融、移动终端等多个领域。各种后门、漏洞不断推陈出新，传统软硬件厂商漏洞数量居高不下，移动系统漏洞数量持续增长，知名杀毒软件、安全防护软件连续爆出严重漏洞。

除往年受关注的 Windows 平台威胁依然存在外，主机外设、Linux 及其它类 UNIX 系统、智能设备、智能家庭、智能穿戴、智能交通、工控系统及社会基础设施均受到不同程度的威胁。这些威胁主要有键盘模拟、网上欺骗、USB 引导区病毒等。

三、计算机病毒造成的主要危害情况

2015 年计算机病毒主要造成的危害包括浏览器配置被修改、数据受损或丢失、受到远程控制、系统（网络）无法使用、密码与账号被盗等。密码、帐号被盗以 53.68%排名第一，成为病毒感染后用户遭受的主要危害，比 2014 年上涨了 6.38%; 43.46%的用户浏览器配置被修改，比 2014 年下降了 19.54 %; 系统（网络）无法使用下降了 0.8%; 数据受损或丢失以及密码、帐号被盗分别占 43.4%和 34.83%,均比 2014 年有所下降。整体上看，病毒、木马给用户造成的危害和困扰增加了，尤其是对用户各类数据带来的威胁有了显著的提升。

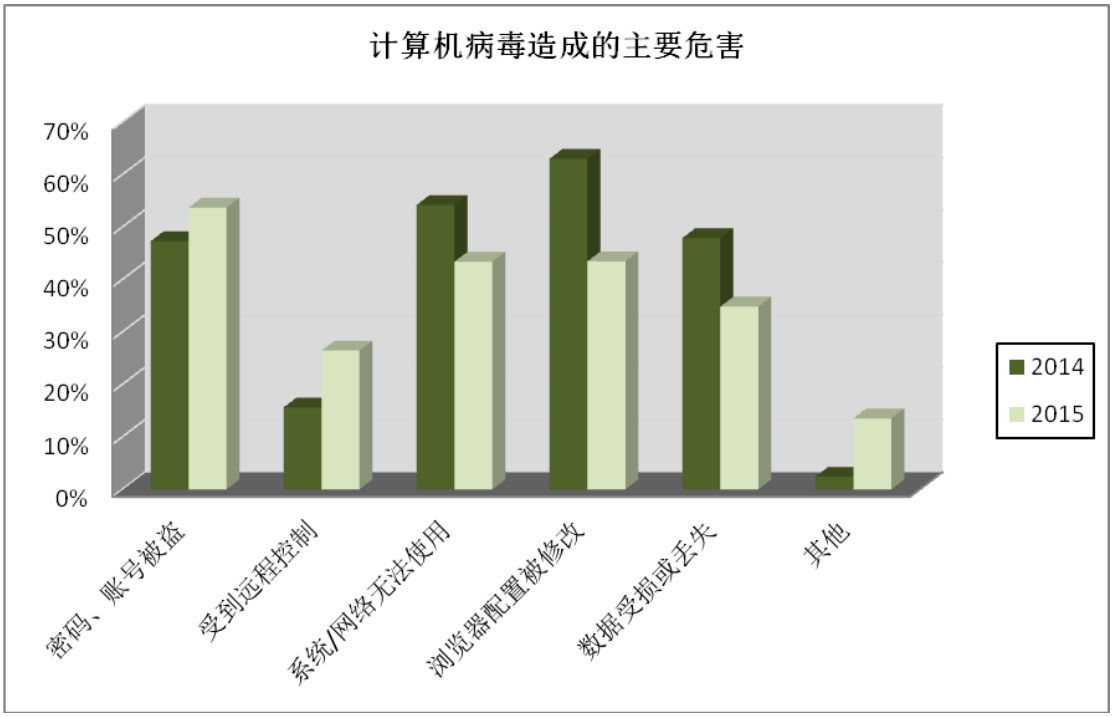

图 9　计算机病毒造成的主要危害

在信息泄露事件频发的同时，个人电脑中的数据直接受到病毒、木马的窥探。在经济利益的驱动下，资金账户和私密信息仍然是病毒、木马等恶意代码的主攻目标，此类病毒在技术上要求不高，变种数量庞大。为了便于记忆，很多用户在注册多个网站、社交平台的账号时，使用相同的用户名和密码，一旦某一平台的用户数据信息被泄露，也会导致用户的其他网站、社交平台的用户名和密码存在被“撞库”的风险。越来越多的安全事件辅以社会工程学，在事件的整个过程中，用户往往是其中最薄弱的环节，即便再强大的技术也难以阻止事件的发生。

浏览器配置被修改在多年占据首要危害之后，首次呈现下降态势。传统 PC 上的浏览器安全已经有了较为全面的解决方案，尽管如此，浏览器作为使用频率最高的应用之一，

仍然是恶意软件传播最为便捷和有效的途径。单纯依靠安全软件检测来实现浏览器的安全浏览仍然存在诸多难题，在这种形势下，很多浏览器选择了通过与安全厂商合作的方式，提升浏览器的安全性，并且取得了一定的成效。

虚拟身份被盗（如微博、微信等）也是病毒感染后造成的主要危害之一。由于虚拟身份经常会与社交、支付、娱乐等多种网络服务相关联，因此，一旦账号被窃取或泄漏，就很有可能引发一系列个人信息的泄漏和相关财产（包括虚拟财产）的损失。除了给个人造成损失，虚拟身份被盗还常常会波及好友的数据和财产安全，甚至还会影响用户的声誉。不法分子可以利用用户的虚拟身份向其亲戚、好友发送虚假消息，用以骗取好友金钱，还可以在其空间、朋友圈、好友群中发表具有商业或色情类的消息。如用户 QQ 账号和密码被窃取，可以导致与其关联的微信同时遭受风险，不法分子可以利用窃取的虚拟身份与其联系人进行消息通讯，实施新一轮的病毒感染、网络欺诈或发动攻击。

四、2015 年计算机病毒感染量 TOP20

调查显示，在 2015 年病毒传播 Top20 中，木马占据了半数以上，仍然是传播最为广泛的恶意代码。

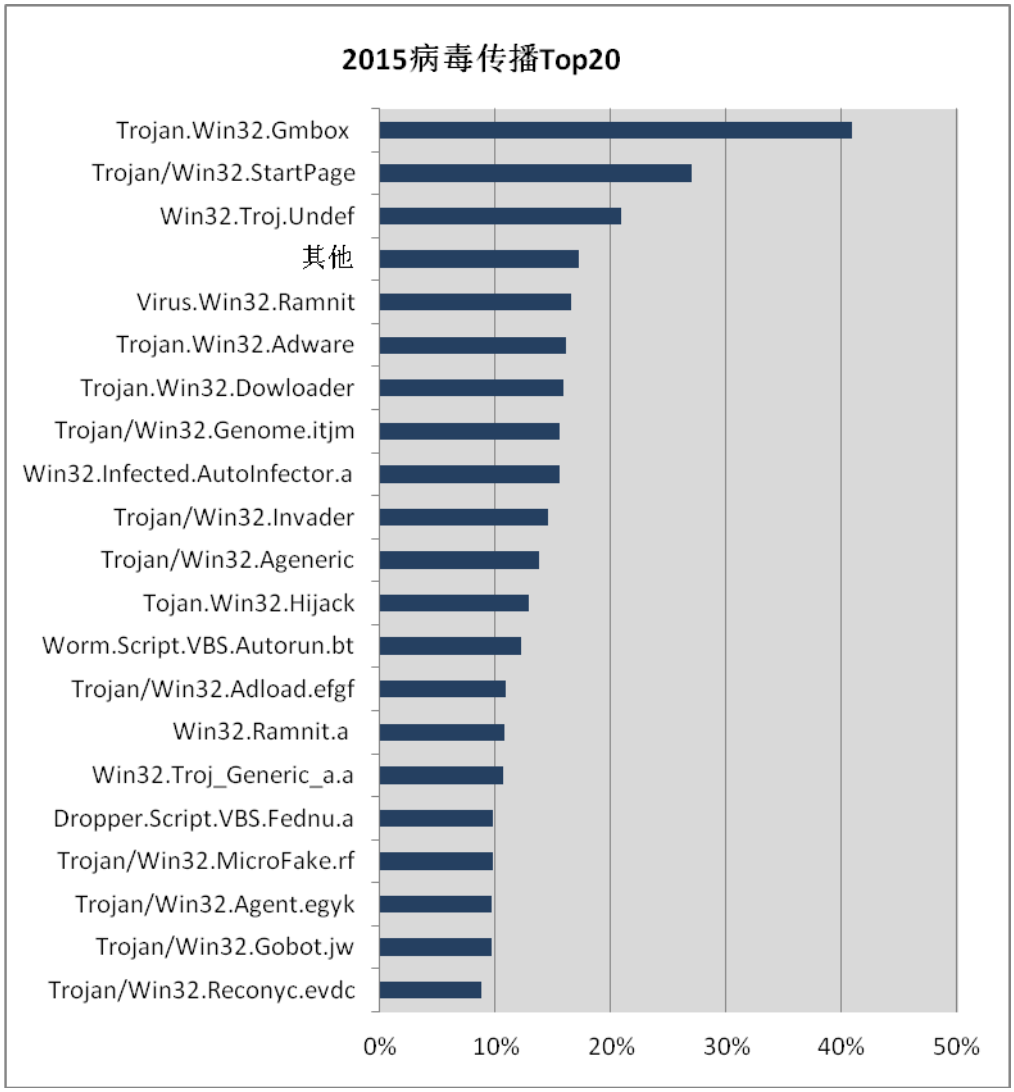

图 10　2015 年病毒传播 Top20

第四章 移动终端安全问题和病毒疫情调查分析

2015 年，我国手机网民数量达 6.2 亿，移动互联网已经成为最重要的网络接入途径和信息共享渠道、最大的信息消费市场、最活跃的创新领域。

移动互联网的扁平网络、多元业务和智能终端，既是其区别于传统互联网的优势，同时也导致安全风险叠加。2015 年数据泄露频发、网络钓鱼事件大幅度上涨、勒索软件大量涌现。基于安卓系统的恶意应用和恶意软件数量持续增长；iOS 也走下神坛，不再是坚不可摧。移动设备已经取代传统个人电脑成为主流上网工具，移动安全领域的问题日趋复杂，不法分子利用钓鱼网站瞄准手机支付用户群体，通过仿冒移动应用、移动互联网恶意程序、伪基站等多种手段，实施跨平台的欺诈和攻击。移动安全已经成为安全领域的焦点话题。

一、 我国移动终端产品使用情况

调查显示，2015 年移动终端用户中使用智能手机的用户占总数的 93.48%，比 2014 年上涨了 5.18%；非智能手机的用户数量占 12.79%；43.2%的用户使用平板电脑。87.16%的用户使用移动终端产品进行了互联网应用。越来越多的应用

转移到移动互联网，移动互联网的强社交属性增加了用户平台的粘性，它打破了传统的信息产业运作模式，影响和改变着我们的生活。从操作系统看，安卓以 43.88%居首位，IOS（苹果）占 25.33%，居第二位，Linux 操作系统以 11.25%排在第三位。IOS 的用户比例较前两年有所上升。

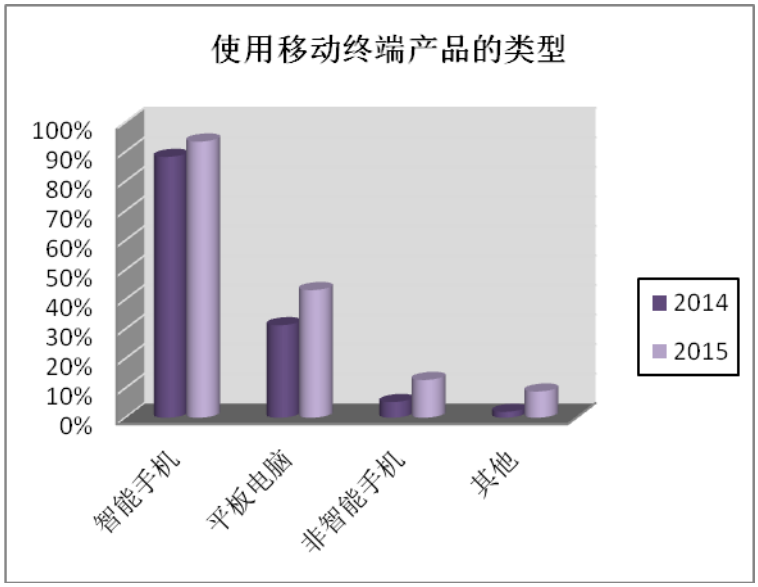

图 11　移动终端产品使用类型

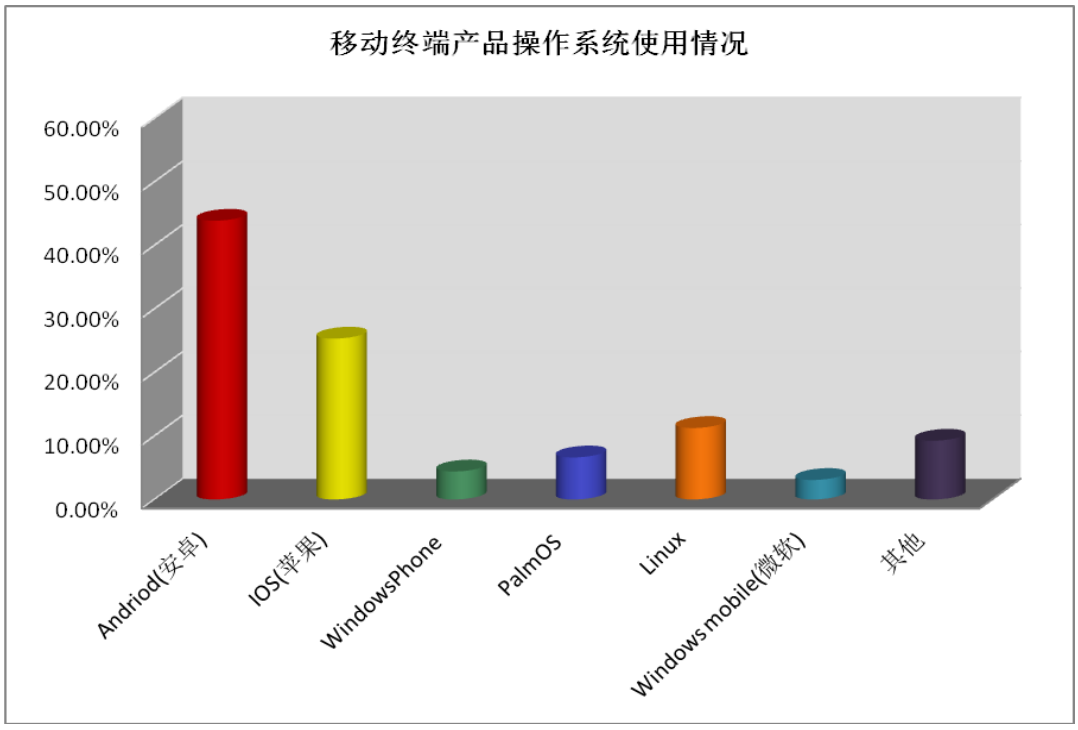

图 12　移动终端产品操作系统使用情况

二、 移动终端互联网应用情况

2015 年，使用频度较高的移动终端互联网应用主要包括网页浏览、社交软件（QQ、微信、微博等）、金融服务（手机支付、手机银行、股票证券、余额宝等金融产品）、网络游戏、音视频等。社交软件以 81.21%稳居首位，比 2014 年略有下降，依然是最主要的互联网应用；网页浏览以 74.55%位居第二，与 2014 年基本持平；排在第三位的是金融服务，占 53.88%，比 2014 年上涨了 14.48%；收发邮件比 2014 年增长了 13.12%，占 41.52%；音视频和金融服务分别占 46.57%和 41.98%，都比 2014 年有所下降。可以看出，随着在线教育市场、互联网医疗、网络租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；邮件收发等非娱乐型应用呈现出较大幅度的上涨趋势。

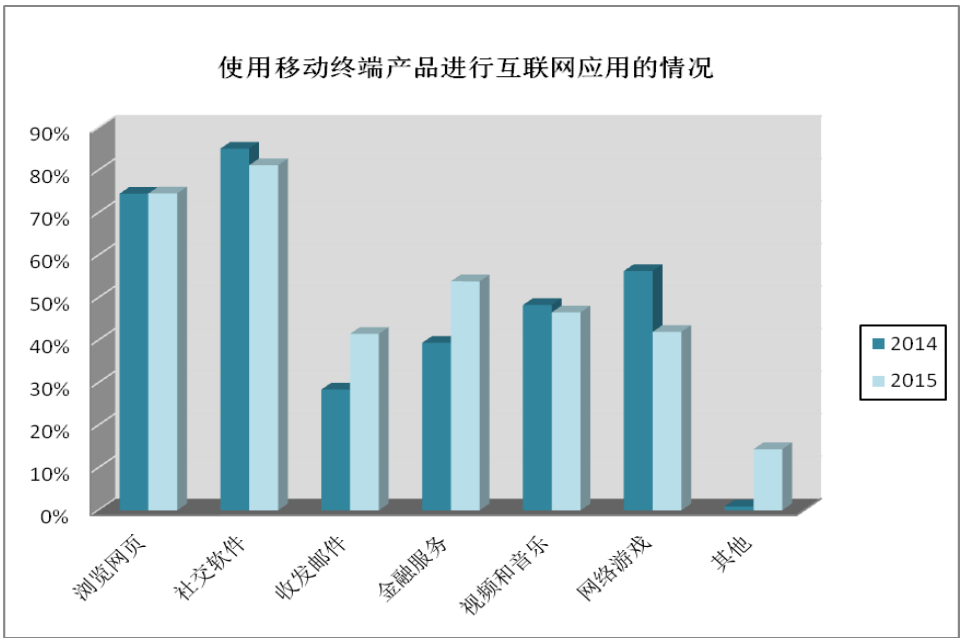

图 13　移动终端产品互联网应用情况

微信等即时通讯工具功能的日渐强大，使其保持了大份额的市场占有率，短信、电话等传统的通讯模式被逐步削弱；网页浏览与去年基本持平，仍然是网民获取信息的主要窗口；音视频、网络游戏等娱乐方面的应用略有下降；手机打车软件、外卖、红包、缴费功能等应用的涌现，使得更多用户实现了手机与银行卡等支付媒介的捆绑，越来越多的用户选择使用移动支付，但移动应用的监管尚不全面以及网民的安全意识的欠缺，移动支付尚存在很多的安全威胁。社交和音视频应用程序在移动领域蓬勃发展，此类 APP 下载量大、使用频繁，已成为病毒、木马传播的主要载体。手机论坛、伪基站短信、网盘、QQ 群等提供的诱惑欺骗性 APP 也吸引了众多的用户，严重危害移动终端的使用安全。盗版手机 APP 可以非法窃取用户数据，占用大量无线网络资源，植入扣费广告。不法分子通过盗版、篡改数据、破解官方版本等方式损害用户及正版开发者的利益。更严重的还有捆绑恶意软件，在用户不知情的情况下，自动发短信、内嵌广告、连接网络、产生扣费等现象，窃取并上传用户的个人信息。盗版 APP 主要集中在安卓平台，因其管理松散导致盗版 APP 泛滥，管理的不规范，使用户很难鉴定应用软件的真伪。另外，盗版 APP 的开发成本偏低、容易仿冒也是其泛滥的主要原因。大量捆绑和感染了恶意程序的 APP 充斥于网络之中，严重威胁着手机用户的数据、隐私和财产安全。

三、 移动终端安全状况

调查显示，垃圾短信和钓鱼（欺诈）信息是造成移动终端安全问题的主要途径，分别占调查总数的 70.33％和 49.32%。对于短信内容，目前还缺乏有效的应对措施，因此很多恶意链接、钓鱼网站都是通过短信传播，成为恶意用户的有利武器。垃圾短信的确给用户带来了诸多困扰。大量信息的泄露，加之社会工程学的有效结合，使恶意用户能够更为有效的实施钓鱼（欺诈）。骚扰电话和网站浏览分列第三第四位，分别占 48.78%和 40.06%。2015 年，网络钓鱼和网络欺诈已经成为网民面对的最主要安全威胁，通过诱骗页面、短信等获取用户银行账户信息、通过监听短信，获取短信验证码，对用户的财产安全带来极大的危害。虽然开展了多次针对伪基站的专项打击行动，但由于装备简单、技术含量低、打击难度大，以伪基站为代表的金融诈骗仍然十分猖獗、屡禁不止。犯罪分子使用与电信运营商相同频率的移动基站设备，冒充运营商连接用户的移动设备，并可通过任何号码向用户发送诈骗短信，迷惑性极强，这些短信通常会携带短链接，诱惑用户点击下载恶意程序，或骗取个人信息。此类犯罪涉及地域广，严重危害国家通信安全。

另外，电子邮件、APP 下载、电脑连接、移动存储介质等也是造成移动终端产品安全的主要途径。“山寨”应用开发门槛极低，欺骗性强。针对网银、支付、购物应用和社交

应用的“山寨”情况持续泛滥，其界面往往可以假乱真，普通用户根本无法分辨，成为对用户隐私的最大威胁之一。

智能城市的推广使公共 WiFi 得到大范围普及，其安全状况令人堪忧。除了常见的虚假 WiFi 钓鱼外，“DNS 劫持”、“ARP 欺骗攻击”等黑客攻击手段也会被用来在免费 WiFi 网络下对在网用户进行恶意攻击，导致网络瘫痪、窃取账号密码和私密信息等。

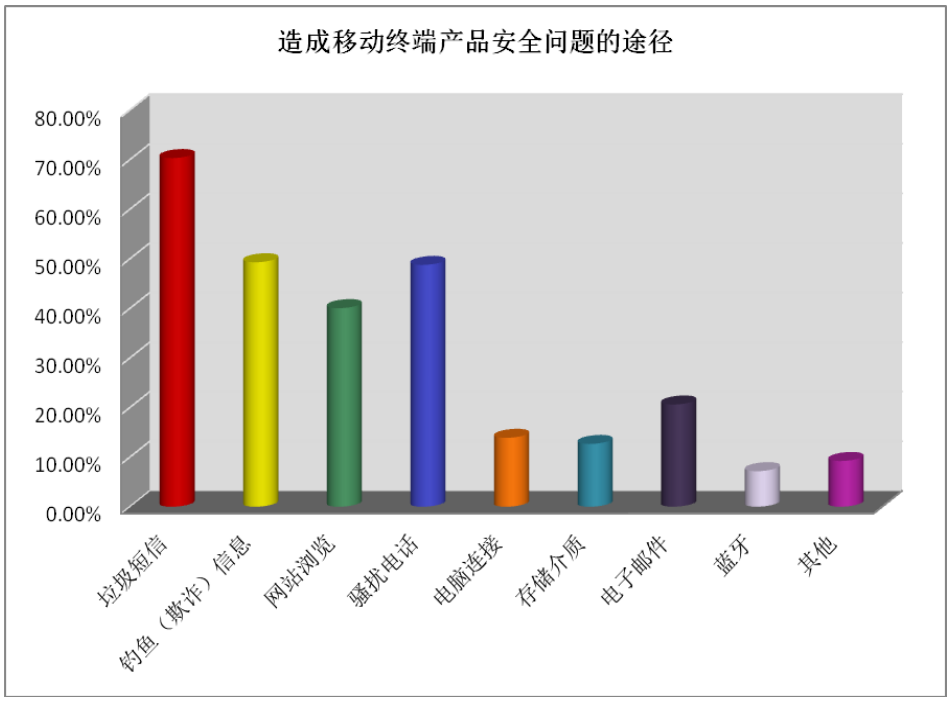

图 14　造成移动终端产品安全问题的途径

四、　移动终端病毒疫情及危害情况

调查结果显示，2015 年有 50.46%的移动终端使用者感染过病毒，比 2014 年上涨了 18.96%，涨幅较大。移动终端病毒感染率居高不下，移动安全成为网络安全的焦点。

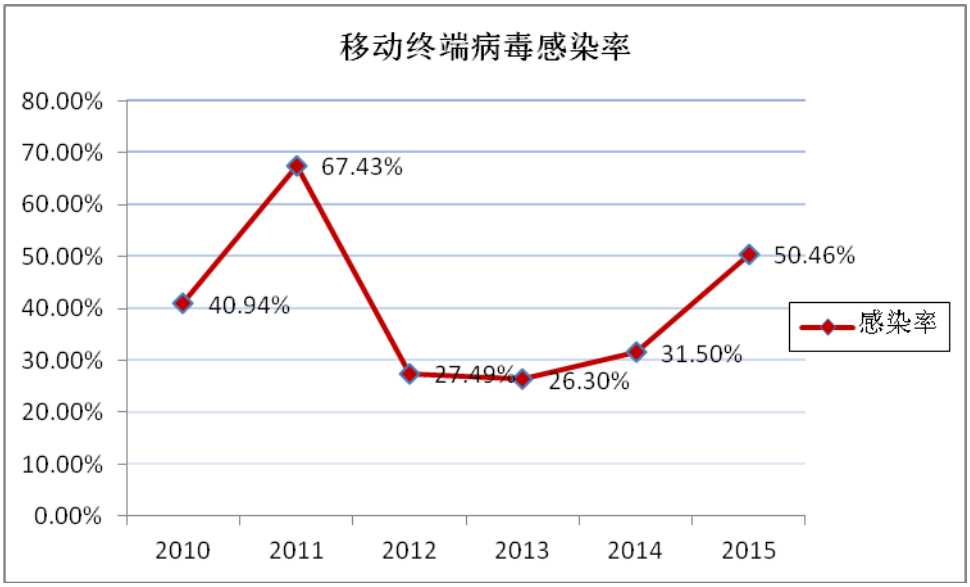

图 15　移动终端病毒感染率

尽管传统 PC 安全事件仍然占据较大份额，但安全风险向移动终端转移已成大势所趋。由于移动终端更多的与银行账户、支付账户等金融业务绑定，获利更为直接，针对移动支付的黑色产业链近两年迅速成长。同时，第三方可视化编程工具降低了编程的门槛，使得移动终端恶意软件的制作成本越来越低。通过高强度的加密混淆等方法，给恶意代码的发现和分析带来了更大的难度 。

苹果操作系统的安全性也受到挑战。苹果操作系统一直以高安全性著称，然而，苹果电脑“百毒不侵”的历史已被终结。2015 年 9 月的 XcodeGhost 事件，通过篡改 IOS 系统下的程序员开发工具 Xcode，导致使用这些工具编译出的应用被嵌入恶意代码，包括微信、滴滴出行、12306、高德地图等多款知名 App 受到影响，形成了波及数千万用户的互联网安全大事件。另外，该事件采用污染非官方供应链的方式。（供应链攻击是指攻击者将恶意代码植入正规产品的源代

码或程序中，随着正规产品的发布、更新而感染用户。）这种方法可以针对指定的目标群体进行攻击，通过感染目标群体经常使用的产品达到上述目的，集中攻击的效果显著。也反映出了我国互联网厂商研发环境的缺陷和安全意识薄弱的现状。IOS AirDrop 作为 IOS9 的首个漏洞，可以在用户未主动同意的情况下，向设备推送并安装恶意应用。可以想见，随着苹果操作系统用户数量的逐日增加，尤其是是移动终端用户保有量的持续增长，必将会有更多黑客将目光投向苹果，其操作系统的安全性将进一步受到挑战。

移动终端病毒通过各种途径侵入到用户的手机，移动终端病毒感染的途径中，短信/彩信以 69%高居榜首，比 2014 年上涨了 36.4%，比例大幅攀升。网站浏览在连续五年排名第一后，跌至第二位，占 54.18%，比 2014 年下降了 15.52%。社交软件、电子邮件、电脑连接分别占 29.61%、28.5%和 26.49%。携带短链接的短信和彩信，成为移动终端病毒传播的重要手段。为了提升安全性，社交软件、网上支付等应用纷纷加强了对异地登陆的安全审核，使得通过社交软件的病毒感染状况有所好转，比去年下降了 10.89%。

安卓和 IOS 系统都拥有广大的客户群体，因此也成为恶意用户关注的重点，其漏洞数量持续增长。2015 年 8 月曝光的 Stagefright 漏洞，可通过发送彩信或构造特殊的应用程序触发 Stagefright 攻击，涉及到 90%以上的安卓智能设备。

而庞大的移动终端用户群体在信息安全防范意识及措施上存在严重不足，同时以上种种都为不法者的利用提供了便利。信息安全环境依然复杂,安全形势依然严峻，安全挑战层出不穷。

安卓平台的开源、开放、免费等特性虽然带来了大量的市场占有率，但是这把双刃剑也给用户带来了不少安全隐患。安卓移动应用的篡改相对简单，木马制作者可随意在正常 APP 中捆绑恶意代码并发布。另外，由于 PC 端的病毒产业依然猖獗，通过电脑连接被感染也一直困扰着广大网民。

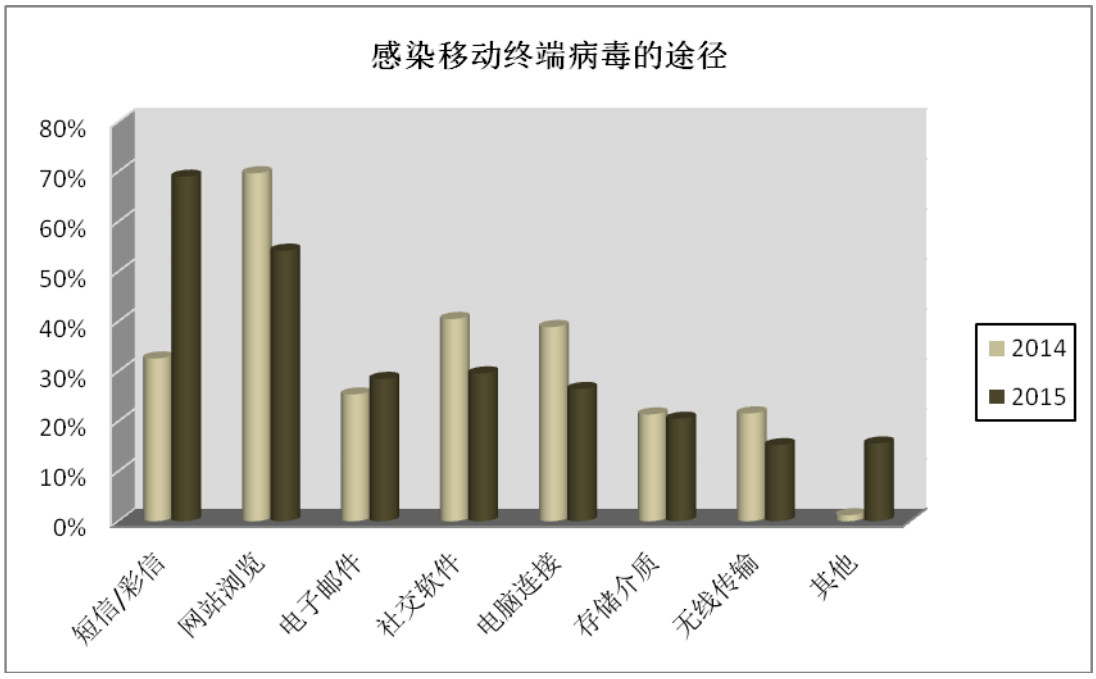

图 16　感染移动终端病毒的途径

用户感染移动终端病毒后造成的后果主要有影响手机正常运行、信息泄露、恶意扣费、网络欺诈、远程受控等。信息泄露连续两年上涨，以 73.68%居首位，比 2014 年上涨了 12.36%；影响手机正常运行以 62.38%位居第二，比 2014

年下降了 12.02%，恶意扣费和网络欺诈分列三、四名，分别占 19.75%和 33.36%。随着智能终端支付类应用的普及，用于窃取个人金融信息的钓鱼网站空前活跃，利用短信诱骗用户访问钓鱼网站的事件大幅增长。

除了这些常年困扰用户的危害之外，2015 年，各类移动终端敲诈勒索软件在我国大量涌现、肆虐传播，成为近两年数量增加最快的网络威胁之一。它们通常会锁定屏幕或加密文档，随后要求受害的用户支付赎金或比特币获取密码或密钥，用以解密文档、恢复正常使用。其中以锁屏勒索类恶意软件数量居多。

在 APT 攻击中，除了针对传统 PC 平台，针对移动平台的攻击也越来越多。智能手机等移动终端，用户粘性大，实时在线率高，联系人之间的信任强度更大。另外，移动终端与传统 PC 存储的信息具有差异性，如电话簿、短信息、地理位置信息等都是从传统 PC 端无法获取的。因此，各类安全威胁纷纷向移动终端转移。

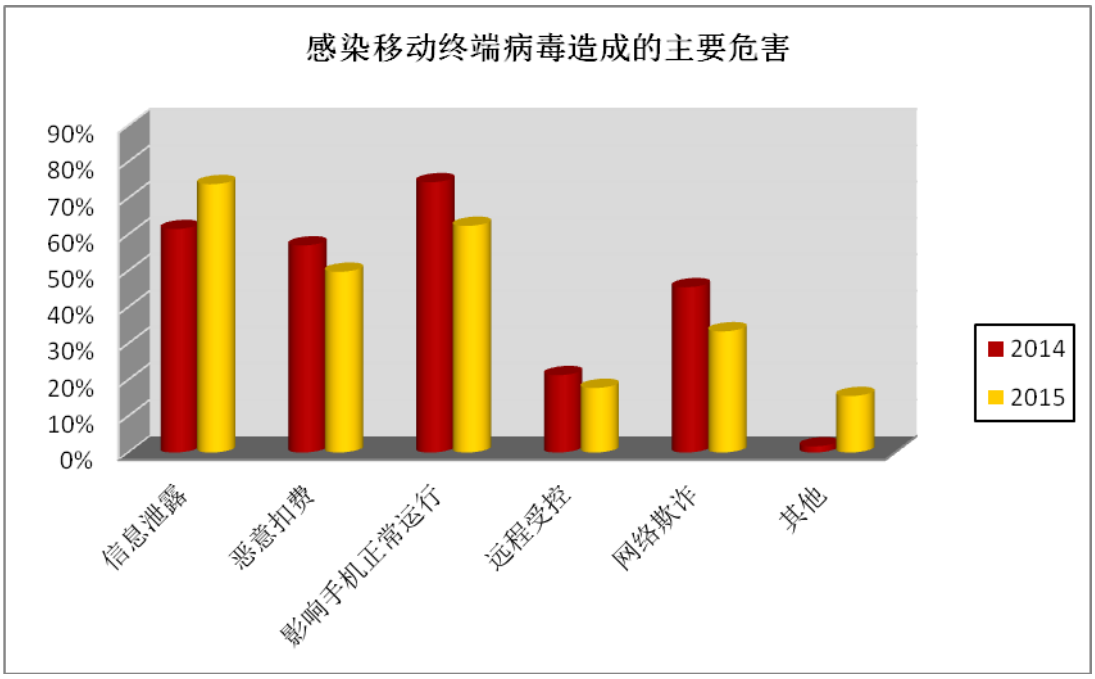

图 17　感染移动终端病毒造成的主要危害

五、移动终端安全产品使用情况

目前，我国拥有手机网民 6.2 亿，用户在性别、年龄、学历等方面的结构复杂导致我国用户在移动互联网的安全意识和安全行为呈现参差不齐的现象，而近些年随着移动互联网的快速发展和智能移动终端设备的普及，移动终端安全产品呈现了快速增长的态势。据统计，有 67.25%的用户使用移动终端防病毒产品，29.01%的用户使用防火墙，26.59%的用户安装使用了移动终端安全管理软件，还有 30.86%的用户安装了数据恢复软件。安全管理软件通常汇集了软件管理、病毒防护、数据备份、数据恢复、通信拦截、流量管理、手机清理等多种功能于一身，为用户的使用带来一定的便捷。移动终端安全产品、管理软件的功能不断完善。移动终端安

全产品使用维持在一个较高的比例，但仍有部分移动终端缺乏必要的安全防护，有的甚至处于“裸奔”状态。同时大量用户使用习惯存在潜在的安全隐患。手机作为一种移动通讯工具，已成为人们的工作生活不可或缺的一部分，移动终端特别是手机的安全引起了普遍关注。随着智能设备功能的不断强大，BYOD 成为了一种趋势。企业移动安全的需求也不断增加，企业移动终端安全管理产品成为了企业新的配置。

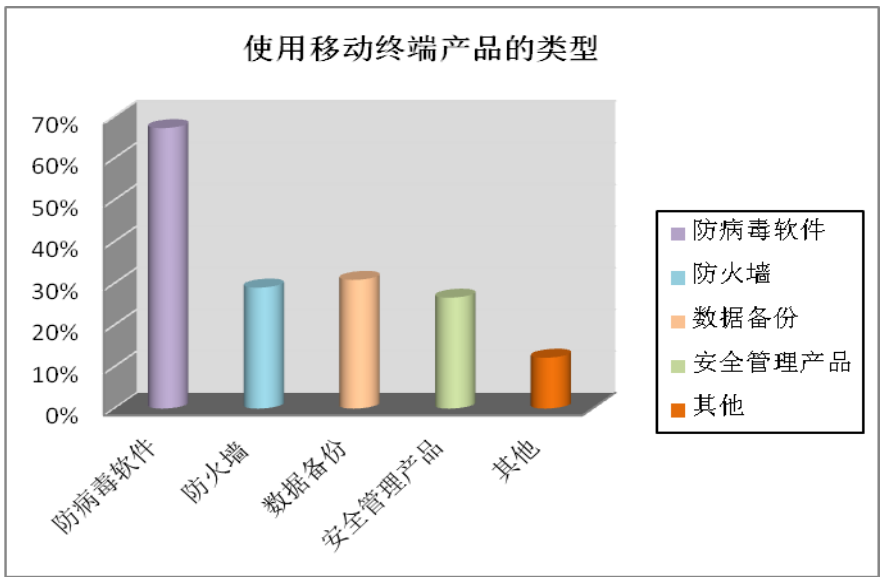

图 18　使用移动安全产品的类型

调查结果显示，75.9%的用户使用过免费的云安全产品和服务。云服务存储的海量数据，使其成为网络攻击的新目标。2015 年云宕机事故显著增加，受害企业众多，数据泄露事件频发。云安全已经引起了普遍关注，各大商家纷纷成立云安全事业部甚至子公司，加大了云安全方面在技术和资金上的投入。

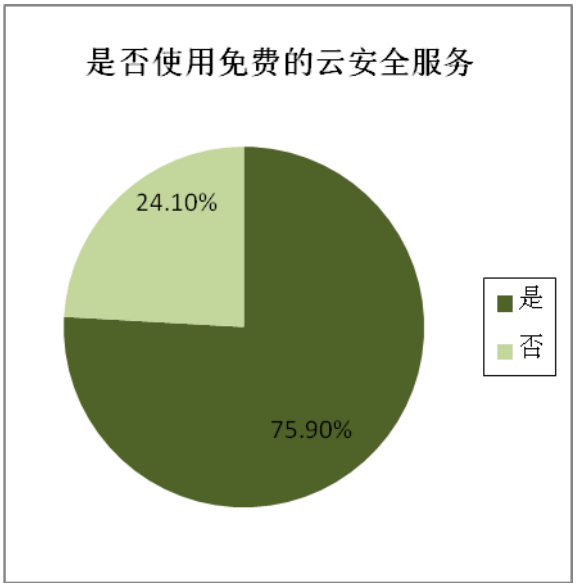

图 19　是否使用免费的云安全和服务

六、2015 年移动终端病毒感染量 TOP20

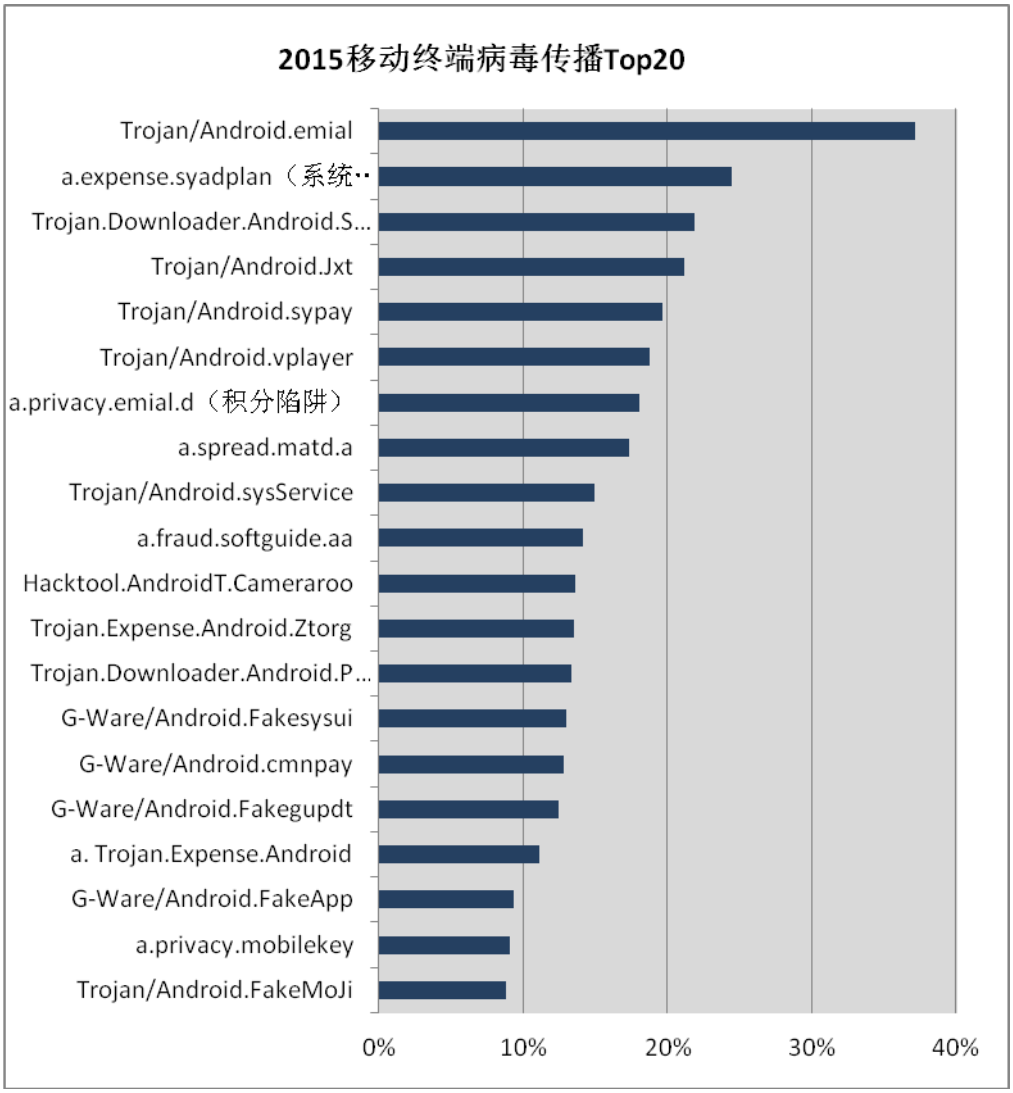

图 20　2015 年移动终端病毒传播 Top20

第五章 网络支付安全状况调查分析

一、网络支付基本情况

随着信息技术的飞速发展，电子商务已经逐渐成为人们进行商务活动的重要形式之一，越来越多的互联网应用与支付关联，网络支付已成为最重要的互联网应用之一。因此，如何建构一个完整、便捷、可靠的网上支付环境成为当前的热门话题。据统计，截至 2015 年 12 月底，已有 268 家支付机构获得支付业务许可证。

2015 年，79.39%的用户使用过网络支付，其中 36.99%的用户在使用网络支付服务时出现了安全问题，使用网络支付服务时遭受到经济损失的用户比例为 50.58%。74.61%的用户选择通过移动终端发起支付，40.39%用户从个人电脑发起支付。

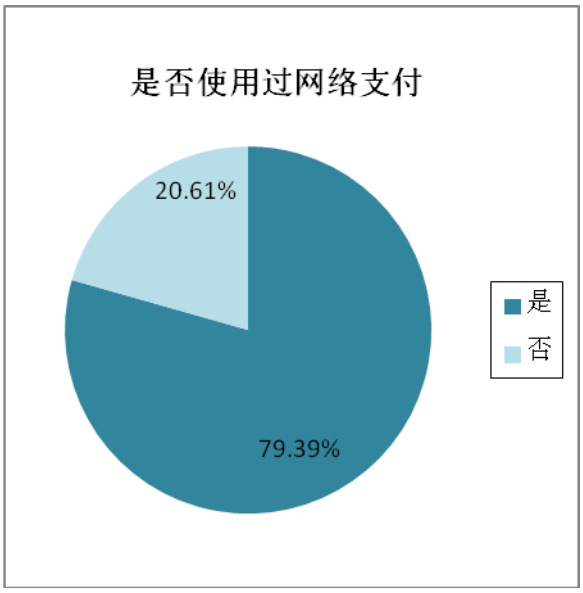

图 21　网络支付服务使用情况

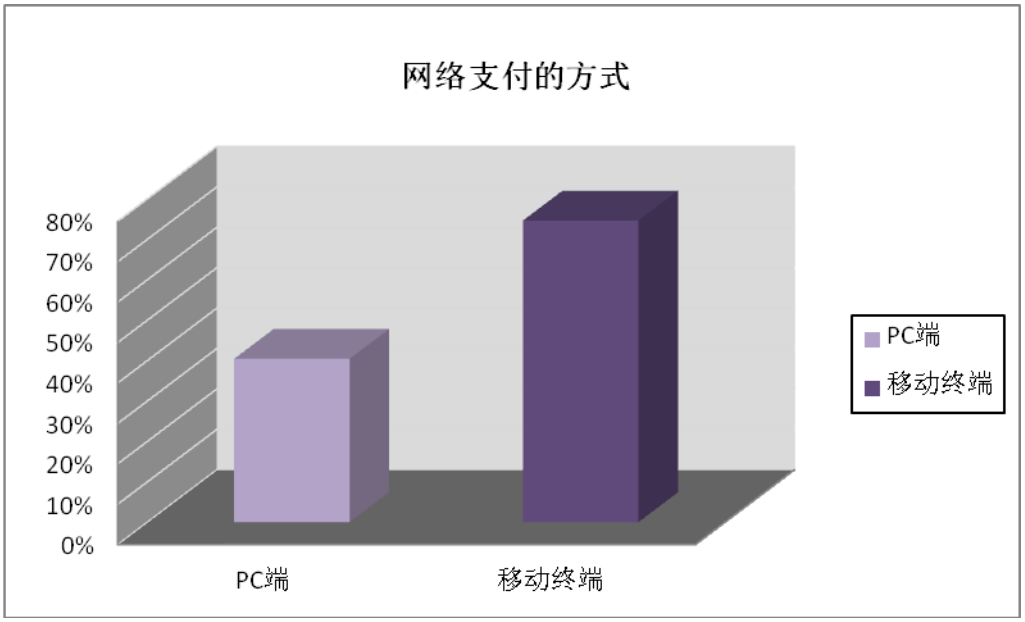

图 22　网络支付方式

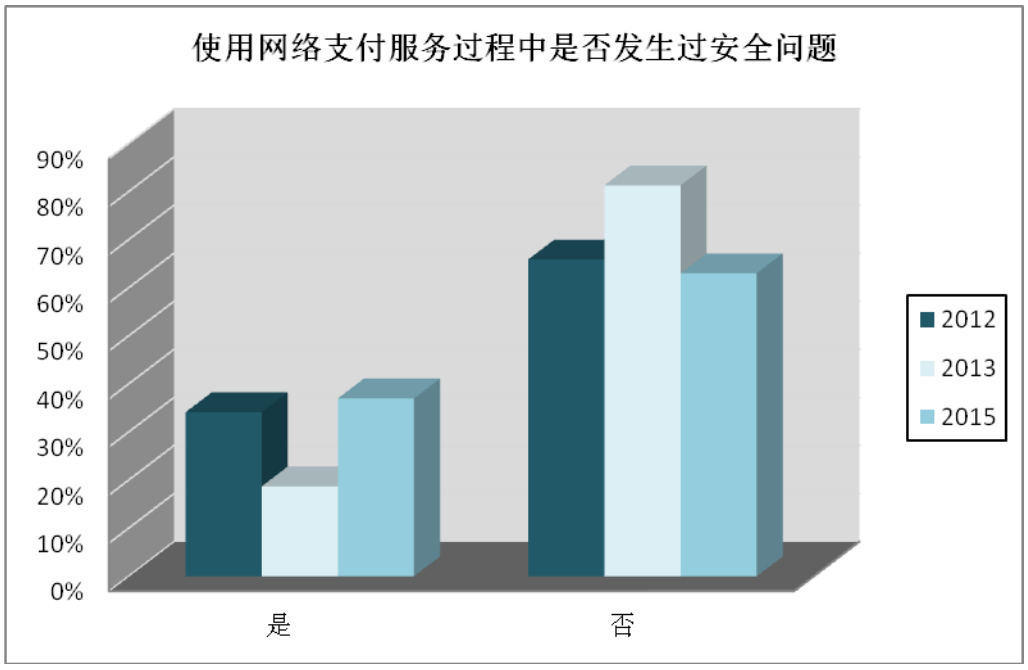

图 23　网络支付时是否发生过安全问题

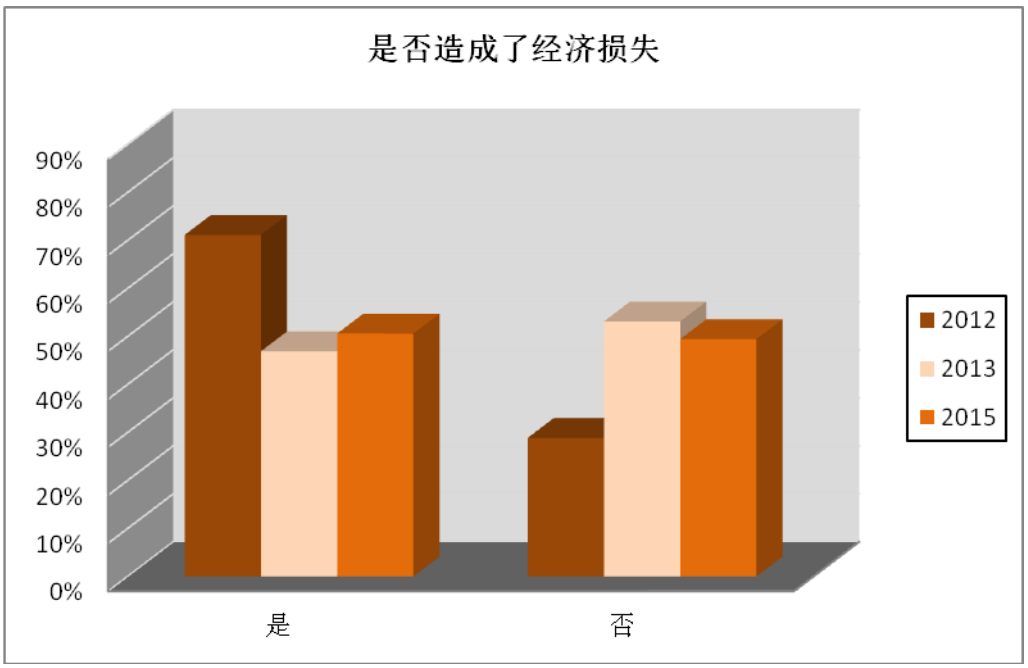

图 24　网络支付时是否造成经济损失

二、网络支付安全状况

调查显示，在网络支付出现安全问题后，所占比重最大的用户是损失在 100 元以下的用户，占 73.83%；17.11%的用户遭受的经济损失在 100 元到 1000 元之间；另外 8.09%用户的损失在 1000 元至 5000 元之间；0.97%的用户损失超过了 5000 元。大额度损失比例与往年相比有所下降，而 100 元以下的小额损失比率涨幅较大。相对而言，小额损失往往难于形成案件，有些用户则抱着自认倒霉的心理，不去报案，因此追回的可能性也较小。

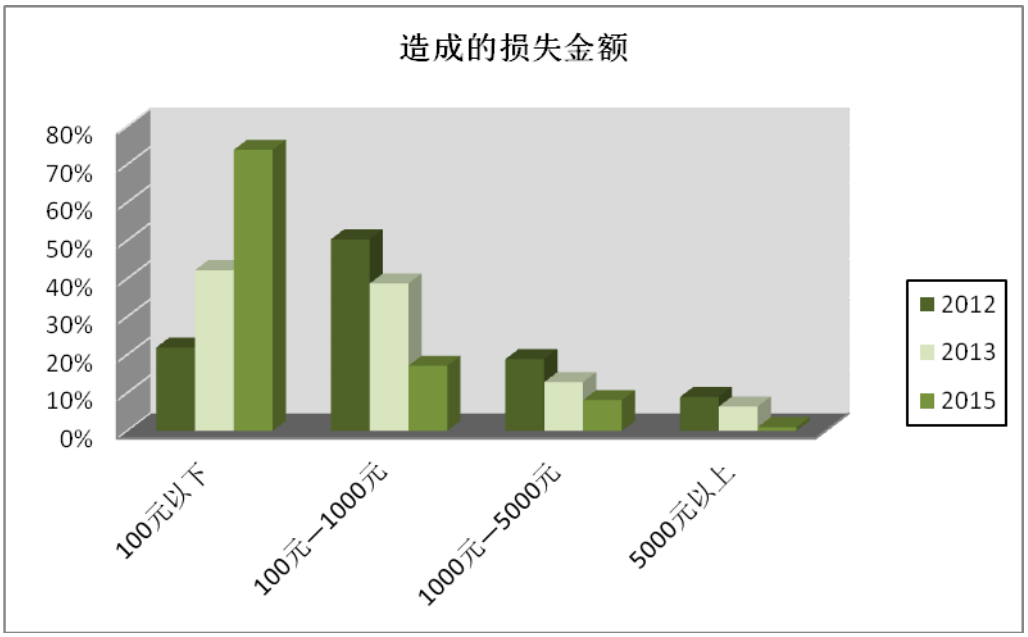

图 25　网络支付造成的损失金额

在造成经济损失后，43.18%的用户选择了向公安机关报案，其中 38.09%的案件被受理，37.36%的用户追回了经济损失，52.45%的用户未能挽回经济损失，10.19%的用户挽回了部分经济损失。公安机关加大了对网络犯罪的打击力度，以用户利益为基础，不以经济损失大小为破案原则，加大了对网络支付安全的监管，使得用户更加信任公安机关。在受到经济损失后向公安机关报案率有所增长，并能够积极配合公安机关的取证工作，使得公安机关能更有效、更快速的打击相关犯罪活动。网络支付在给用户带来便利的同时，也给用户带来了新的安全威胁，加强对网络上虚拟交易的监管，实施网络实名制，这样会使犯罪分子不敢明目张胆地进行非法活动，也有利于监管部门掌握具体的资金流向，使其得到有效地控制。另一方面，应加强对网上银行和第三方支付机构等相关组织的监管。加强电子商务行业的监管，规范市场主

体行为。

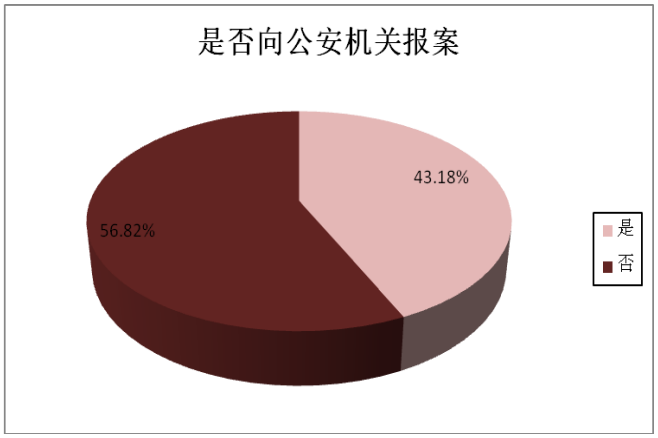

图 26　是否向公安机关报案

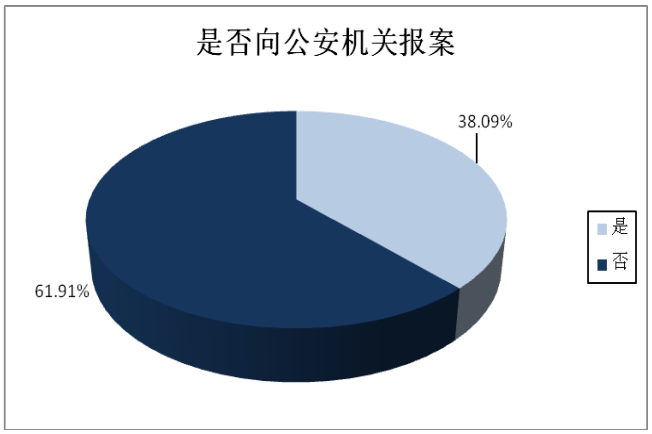

图 27 公安机关受理情况

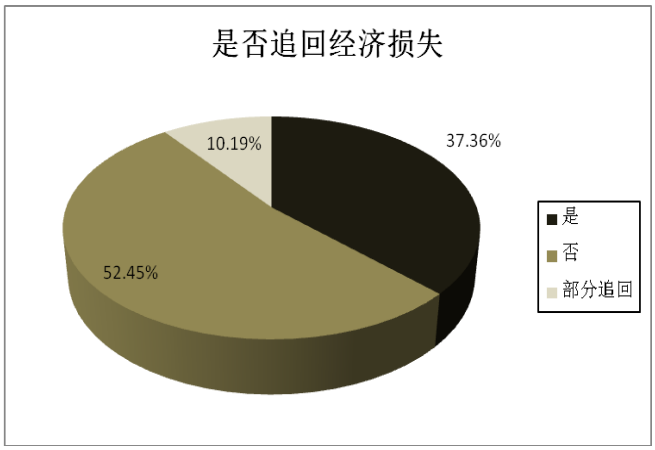

图 28 是否追回经济损失

致谢

报告撰写过程中，腾讯科技（深圳）有限公司、哈尔滨安天科技股份有限公司、猎豹移动、奇虎 360 公司、北京瑞星信息技术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。

同时，感谢以下单位对“第十五次全国信息网络安全状况暨计算机和移动终端病毒疫情调查活动”的支持。

协办单位:

支持单位（排名不分先后）: