第十四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

2015 年 6 月

目　录

报告摘要

为了解掌握2014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于2015年2月2日至2015年2月28日组织开展了“第十四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，国家计算机病毒应急处理中心计算机病毒防治技术国家工程实验室承办，腾讯电脑管家协办，国内外主要计算机病毒防治和网络安全厂商提供技术支持。

调查结果显示，2014 年，88.7%的被调查者发生过网络安全事件，与2013年相比增长了37.5%；感染计算机病毒的比例为63.7%，比2013年增长了8.8%；移动终端的病毒感染比例为31.5%，比2013年增长了5.2%。无论是传统PC还是移动终端，安全事件和病毒感染率都呈现出了上升的态势。

回顾2014年，对互联网影响重大的安全问题层出不穷，“心脏出血”（Heartbleed）漏洞影响了数以万计的服务器，敲诈者病毒、伪银行木马让上百万用户陷入困境，社交网络钓鱼真假难辨，网络安全状况日益严重，其中各种新型及变种的病毒、木马、恶意软件等发展趋势依然严峻。垃圾邮件的数量近两年也持续攀升，2009年就已被认定为是最大的垃

圾邮件僵尸网络的“UPATRE 家族病毒”，至今仍在传播。电子邮件成为主要针对性攻击的入口，这些攻击的目的仍是窃取用户的商业和私密信息并用以进行网络攻击及非法的网络行为，最终获取更高的经济利益。

2014 年钓鱼网站数量急速增加，攻击者通过制造恶意钓鱼地址诱骗用户点击，进而窃取访问者的个人敏感数据，网站仿冒成为网络安全的突出问题。调查显示，仿冒对象涉及媒体传播类、金融证券类和网上支付交易类等信息，同时紧贴重大事件和热点话题。重大新闻事件、会议活动等都会被钓鱼网站制作者借题发挥。网购和热点新闻话题给生活带来便利、传递了新鲜的资讯信息的同时也伴随着不安全因素的产生，消费者应当自觉提升自身的网络安全意识，同时大型购物平台、门户网站也应在安全方面加大投入，为用户构建更加安全的网络平台，保障用户的数据和财产安全。

2014 年网络犯罪黑色产业链开始在各国之间泛滥，俄罗斯、中国、巴西的网络犯罪分子通过地下论坛等多种途径购买定制的黑客工具，竞争日益激烈的地下黑市导致黑客工具的价格十分诱人；类似的网络犯罪集团还在美国和加拿大制造多起大型数据外泄事件。预计 2015 年越南、英国和印度等国也将被黑客列为重点攻击目标，更多针对性来源和目标国家的名字，将会出现在 2015 年的盘点列表之上。国与国之间的通力合作，加大了共同打击网络犯罪的力度，如：美

国联邦调查局(FBI)宣布在多国协力合作下阻断了 Gameover Zeus 病毒。

较之往年，2014 年漏洞数量大幅增加，随着微软在 2014 年终止了对 Windows XP 系统的服务，相继爆出了针对此系统的“零日”（0-day）漏洞及其它诸多漏洞，同时利用漏洞的攻击也层出不穷，最典型的当属“心脏出血”（Heartbleed）漏洞和“破壳”（Shellshock）漏洞，它们的发现警示人们没有一个应用程序和操作系统是永不可摧的。网络犯罪集团通过成功利用这些漏洞进行攻击，导致大量信息外泄事件的频发，如 12306 网站用户数据泄露事件以及 2014 年底曝出的 130 万考研考生信息泄露等。这些外泄信息涉及个人的身份信息、健康信息甚至金融交易等私密信息，一旦泄露对受害者的影响将及其深远，也因此，公众对漏洞危险性的关注提升到一个新的高度。

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，各部委联合组织了“净网 2014”、“剑网 2014”等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；2014 年，我国举办了首届“中国—东盟网络空间安全论坛”和首届“世界互联网大会”，充分展示了中国互联网发展理念和成果，彰显了我国在互联网世界的话语权；此外，还举办了首届国家网络安全宣传周活动，提升了全民的网络

安全意识；同时，十八届三中全会上也提出了“依法治网”的概念，标志着我国已全面深入地进行网络安全法制建设。

截至 2014 年 12 月，我国网民数量达 6.49 亿，互联网普及率为 47.9%。其中手机网民数量为 5.27 亿。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。智能终端保存更多个人隐私信息，但由于尚处于推广期，智能终端的操作系统存在安全漏洞、防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。而大数据的发展降低削弱了个人信息的可控性，导致姓名、住址、电话、身份证号、消费记录等重要生活信息网络泄露问题频发。经济活动从线下发展到线上电子商务，互联网金融市场火爆。互联网经济的活跃不仅带来了行业的繁荣，同时也导致了钓鱼攻击的猛增，并呈现跨平台发展趋势。除了传统钓鱼网站之外，不法分子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，实施跨平台的钓鱼欺诈攻击。

手机支付类病毒越来越体现出一种融合化的发展动向。由于支付类病毒智能化程度提升，“仿冒”的银行 APP、电商、支付类 APP 散布在各大中小型的电子市场，一旦点击下载，就会触发进入黑客操控的支付流程。手机支付类病毒由

二次打包、仿冒程序、验证码转发、监控诱导一步步深入窃取用户支付隐私，并逐步突破银行、运营商、第三方支付软件构建的“手机验证码+密码”的双重认证防御，盗取用户资金。手机支付类病毒正走向高危化、智能化，融合社会工程学等多种特征的发展趋势。

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

调查采取网上调查的方式，我们在国家计算机病毒应急处理中心网站开设了调查专栏，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。

本次调查活动时间为 2015 年 2 月 2 日至 2015 年 2 月 28 日，调查内容主要为我国计算机、移动终端用户 2014 年以来发生网络安全事件状况、计算机病毒感染情况、移动终端的安全状况。

第二章 信息网络安全状况调查分析

一、2014 年网络安全事件

调查结果显示，2014 年网络安全事件中，垃圾邮件占 60.7%，感染病毒、木马紧随其后，占 51.4%，排在第三位的是诈骗短信/电话，占 47.9%。除此之外，其他的网络安全事件还有个人信息泄露、虚拟身份被盗（QQ、微信）、网络钓鱼/网络欺诈、盗版手机 APP（应用软件）、遭到网络攻击、虚拟 WIFI 盗号、财产被盗等。

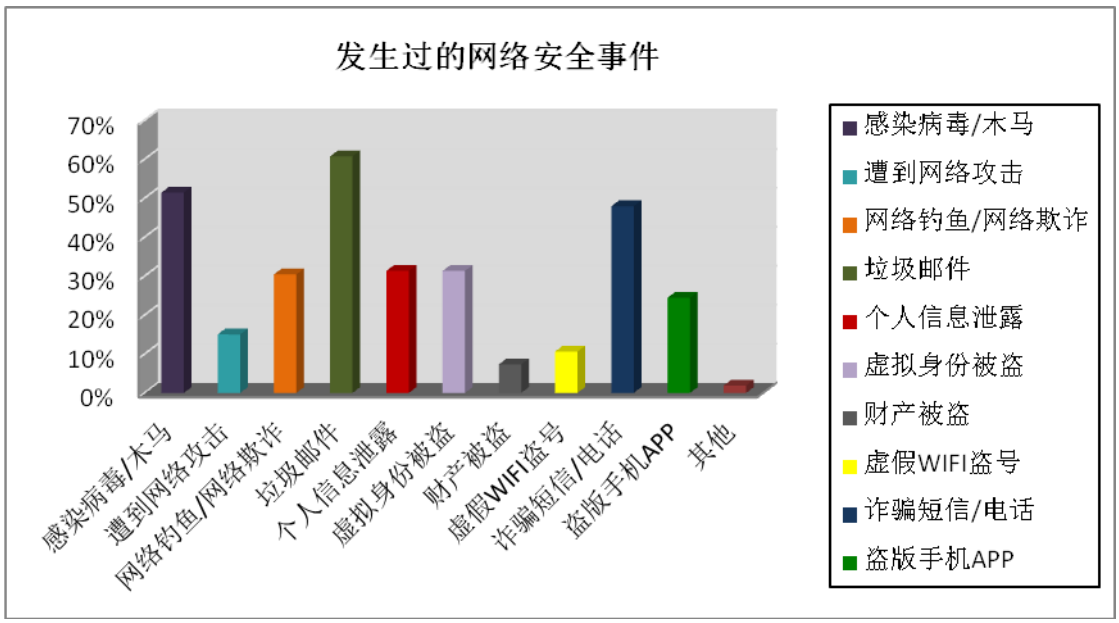

图 1　发生过的网络安全事件

垃圾邮件的主要目的是传播恶意程序/恶意网站、商业广告以及涉嫌违法垃圾邮件。通过垃圾邮件传播的恶意程序/恶意网站种类繁多，且是恶意程序的重要传播方式，它们不仅能够窃取受害计算机的数据，还能使其成为僵尸网络中

的一员，或者下载其他恶意软件运行，而恶意网站是直接威胁用户金融财产的重要组成部分，比如不法分子通过网络银行类钓鱼网站诱使用户输入网络银行账号和密码；涉嫌违法的垃圾邮件包括赌博类、欺诈类、色情类、违法类、办证类、谣言类等,作为垃圾邮件的重要组成部分,给用户带来了严重的困扰。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，严格的过滤规则会面临着误报的可能性，在反垃圾邮件产品不断进步的同时，垃圾邮件同样调整信息以躲避反垃圾邮件产品的拦截。

感染病毒、木马仍旧是用户面临的主要威胁，病毒、木马可以窃取用户计算机中的数据、威胁用户隐私、影响计算机性能等；病毒、木马对企业的威胁主要是窃取商业机密信息，严重的甚至会影响生产、销售等环节。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，使用云查杀等处理方式更是提高了病毒和木马被查杀的机率。病毒和木马的传播方式越来越注重利用社会工程学的方法，通过结合用户的使用习惯、身份信息等构造出仿真度极高的网站、电子邮件、即时通讯消息等诱骗用户中毒。网络中被泄漏的大量的个人数据信息常常被不法分子用来从事非法活动。

在调查中，47.9%的用户遭遇过诈骗短信/电话。诈骗短信、电话主要威胁用户的金融财产安全。诈骗短信、电话通常采用法院通知违约、淘宝订单冻结退款、异性开房被查、窃听工具、抽奖活动、金融理财等关键字诱骗用户。例如:“我是某电信局（公安局、检察院）的，您的电话已欠费，而且您的银行账户涉嫌洗钱、诈骗等犯罪，请配合...”。诈骗短信的主要目的是诱使用户拨打指定电话或登录指定网站，不法分子通过用户拨打电话，使用诱导、恐吓性语言骗取用户钱财。不法分子使用多种手段使用户相信其所设的骗局，并诱导用户向指定的银行账号“汇款”。伪基站也是诈骗短信的重要源头，伪基站除了发送诈骗短信外，还会发送大量的广告推销和违法信息。2014 年国家多部门在全国范围内部署开展打击伪基站整治专项行动，取得了重大成果，破获了多起重大典型案件。

2014 年被曝光的信息泄漏事件涉及的个人信息有数亿条之多，其中仅 ebay 就泄漏了约 1.45 亿，国内多家快递被泄漏的个人信息近 1400 万。而影响最为严重的还是“12306 撞库攻击事件”，该事件使用已泄漏的个人数据信息通过撞库形成少量数据集合，并进一步制造舆论，声称后台数据泄露，造成了一定的社会恐慌。除了保存在网站和服务器中的用户数据信息被批量窃取外，个人电脑中的数据也会直接受到病毒和木马的窥探。用户在注册多个网站、社交平台的账

号时，如果使用相同的用户名和密码，一旦某网站或社交平台的用户数据信息被泄露，就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。

调查显示，有31.3%的用户虚拟身份曾被盗（QQ、微信），虚拟身份被盗不仅会威胁用户及好友的财产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。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，诱骗其联系人向指定账号汇款。如：虚构被盗号的用户遭遇车祸急需用钱、违法入狱需要保释金、用户钱卡丢失汇款等。

30.4%的用户遭遇过网络钓鱼/网络欺诈，这也是传统PC和移动终端共同面临的安全问题。不法分子通过网络钓鱼/网络欺诈的手段窃取用户的银行或网站的账号和密码。例如，假冒网络银行页面诱骗用户输入银行账号和密码；假冒淘宝、京东网站，遥控用户执行指定操作，进而骗取用户金钱；假冒网购打折邮件，发送钓鱼网址。随着智能手机等移动终端的普及，网络钓鱼/网络欺诈已经逐步向移动终端转移，网络欺诈形成了“网络+社交+电话”的复合模式。

盗版手机APP是移动终端用户面临的主要安全问题之一，2014年有24.4%的用户遭遇过此类问题。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Adroid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是否为正版。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。

调查显示,有15%的用户确认遭到过网络攻击。包括APT、DDOS、网络监听、密码破解、端口扫描及渗透、漏洞扫描、协议攻击等。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。2014年被曝光的APT事件攻击范围涉及了近百个国家，其中遭受攻击最多的是美国、俄罗斯、中国、日本等。攻击的目标主要为能源、金融、医疗保健、媒体和电信、公共管理、安全与防务、运输和交通等行业。近期，卡巴斯基曝光的APT事件“Equation Group”（方程式组织）更是具备了攻击硬盘固件的能力，使用固件程序的硬件还包括网卡、鼠标、键盘、路由器等，这意味着APT的攻击范围从传统的终端向周边设备延伸，APT攻击将呈现全方位、立体式的多点攻击模式。

虚假 WiFi 盗号是近些年来较为突出的安全问题，调查中有 10.6%的用户受到此类安全问题的困扰。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、支付宝等操作时，不法分子即可记录并窃取用户的这些信息。

调查显示，2014 年有 7.3%的用户财产被盗。不法分子窃取用户财产主要有两种手段，一是利用用户安全意识薄弱，诱骗用户向诈骗者“汇款”；二是利用 PC 端或移动终端窃取用户的网络银行账号和密码。移动终端的恶意程序在窃取用户财产时，还会截取银行的验证短信。

2014 年有 11.3%的用户没有遇到过网络安全问题。这部分数据有两种可能性，一是确实没有遇到过网络安全问题，另一种可能是遇到了网络安全问题而没有发现。例如，恶意软件运行时没有界面，用户“看不到”，而恶意软件的危险行为也未被用户发现，如窃取用户数据。

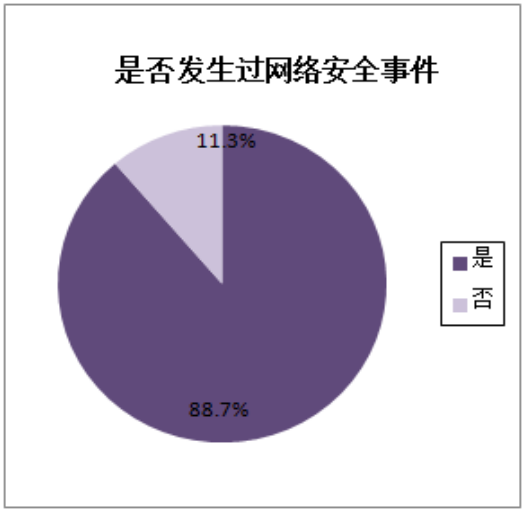

图 2　是否发生过网络安全事件

二、发生网络安全事件的设备

2014 年的调查结果显示,在常用的各类设备中,有 84.5%的个人电脑发生过网络安全事件，手机和平板电脑位居其后，分别占 63.1%和 12.4%，与往年相比，路由器在 2014 年网络安全事件设备中占据的比重有所增加，这主要是由于 2014 年被曝光的路由器漏洞较多而导致的。

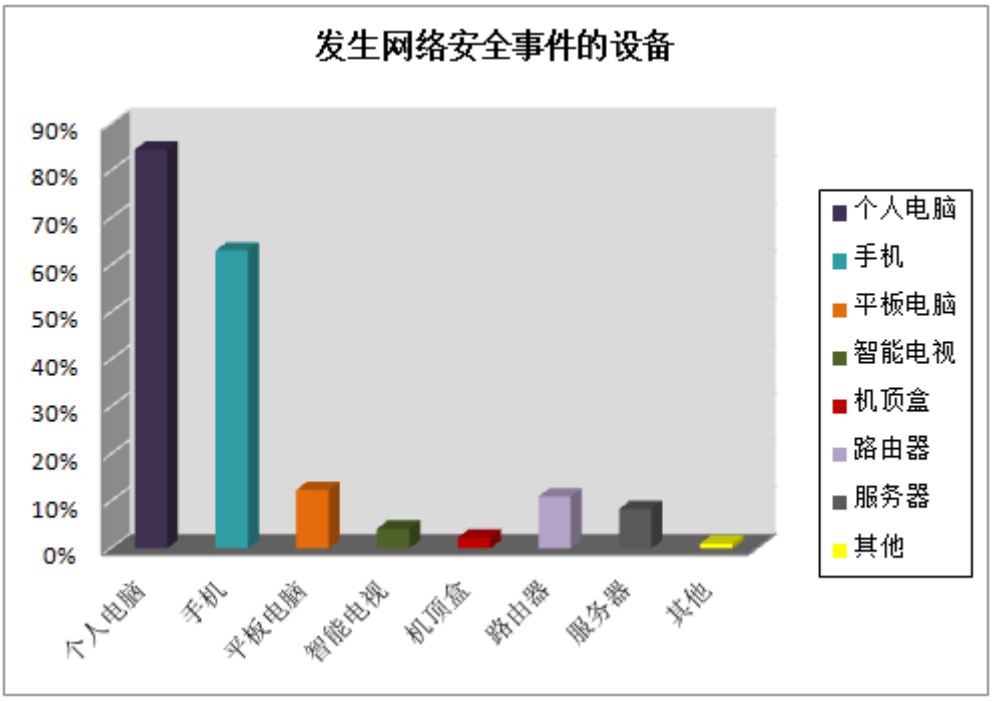

图 3　发生网络安全事件的设备

路由器主要有三个方面的安全隐患，一是路由器自身的安全漏洞；二是路由器的 WiFi 网络缺乏有效的管理；三是用户对路由器设置不当。2014 年多款路由器产品被曝出存在漏洞，导致不法分子可以非法获得路由器的家庭地址及宽带账号和密码。至今仍有大量用户使用早期的不安全的 WEP 加密方式,而不修改默认密码则有可能会受到 DNS 篡改等攻击,同时还有部分用户没有设置 WiFi 密码，这些设置都会导致

路由器存在严重的安全隐患，如用户隐私被窃取、跳转到恶意网站等。

服务器安全一直是网络安全中需要重点保护的区域，可是仍有较多的服务器因忽略安全配置的原因导致系统被入侵。针对服务器的安全事件中，密码暴力破解一直都是排在首位的，WEB 注入、漏洞扫描、敏感路径探测是入侵者常用的手段，端口扫描和系统漏洞扫描也是入侵服务器的手段之一，而上述攻击方法都可以利用安全的配置来阻止和防范。随着云技术的普及，针对云服务器的攻击事件也越来越频繁。2014 年针对服务器的 DDoS 事件有所增加，攻击者调用的大量肉鸡发起针对域名的随机查询攻击，导致服务器性能大幅降低。

2014 年也发生了针对智能家居的攻击事件，2014 年 12 月的一起 DDoS 攻击事件中发现了感染智能摄像头的蠕虫，攻击者利用智能硬件漏洞获取权限后执行蠕虫，并利用被感染的智能摄像头发起 DDoS 攻击。这类病毒驻留在智能设备的固件系统中，而在固件系统中清除病毒极其困难。这也预示了今后将有更多的恶意代码针对智能设备，同时也将有更多的平台及行业受到恶意代码的直接或间接威胁。

三、网络安全事件造成的经济损失

调查结果显示，在 2014 年网络安全事件造成的经济损失中，有接近一半的用户没有造成经济损失，有 3 成的用户损失 500 元以下，造成 500 元-4999 元损失的用户占 14.2%，造成 5000 元以上损失的用户占 4.5%。

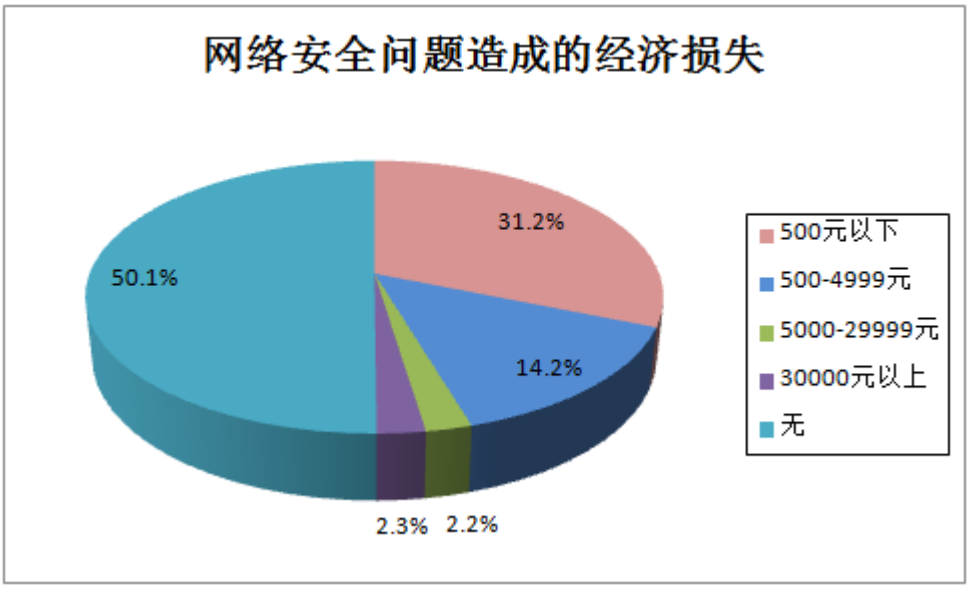

图 4　网络安全问题造成的经济损失

在被发现的案例中，不法分子使用诈骗手段给用户造成的损失往往较大；银行卡被窃取也会造成较大的损失;在被窃取 500 元以下的损失案例中,以虚拟财产和网购财物居多。2014 年广州警方破获了银行卡盗窃的特大案件,不法分子通过网络入侵多个网站的数据库,利用盗取的用户信息在其他网站尝试登录，“碰撞”出数百万条用户个人信息和银行卡资料，并通过出售信息、网络盗窃等犯罪方式，非法获利 1400 余万元。

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

2014 年我国计算机病毒感染率为 63.7%，比 2013 年上升了 8.8%，在 2012 年跌至最低点后,连续两年上涨。在新增的恶意软件中，木马占 54.7%，紧随其后的是后门和间谍软件。与蠕虫、感染型病毒不同，这些类型的恶意软件并不以大范围破坏文件、造成拥堵网络为目的，而是瞄准受害者的资金账户和私密信息，它们通常以窃取攻击目标的账户密码为目的，并通过多种途径获取经济利益。受经济利益的驱动，网上银行、网络支付等仍然是病毒的主要攻击目标，在盗取钱财的同时，不法分子还会窃取用户的私密信息。账号信息可以让信息盗取者直接获利，因此也成为了不法分子的主要目标。数据表明，在有针对性感染的目标机构中，九成以上将金融行业列为主要目标，在高额经济回报的驱动下，犯罪分子利用先进的木马技术，攻击金融机构，在全球范围内从事大规模金融诈骗和盗窃活动。大多数金融机构的网上银行业务通过浏览器来实现，因此浏览器也成为了当前网银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。勒索软件多通过使用新的加密和回避方法，打着“不给赎金就永久加

密被绑文档”的旗号敲诈用户钱财。

在攻击与反攻击的博弈过程中，网络犯罪分子不断采取新的技术手段，试图突破和绕过金融机构所部署的各种安全防线。为了躲避安全产品的检测或干扰安全产品的正常运行，恶意攻击者采用多种手段对自身进行更新。攻击者还将某些特殊对象作为逐利目标，如比特币、密码管理器等。其中，针对 Bitstamp 的攻击最为引人注目，约 19000 枚比特币从运营商的钱包中被盗取。

个人隐私信息成为黑色产业重点关注的对象。随着大数据时代的发展，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。网络攻击是盗取信息的重要手段。攻击者的目标已不只是个人用户，政府、银行、大型企业也成为攻击的主要目标。这些重要机构应加大力度提升自身的安全措施，避免大规模数据泄露的发生。

调查中我们发现，普通用户的个人隐私信息泄露问题会越来越突出。随着大数据挖掘的不断商业化演进，相关的用户行为信息会越来越多的被收集，甚至可直接进行现金交易。与此同时，用户隐私信息的保护，也将成为 2015 年安全厂商关注的重点。

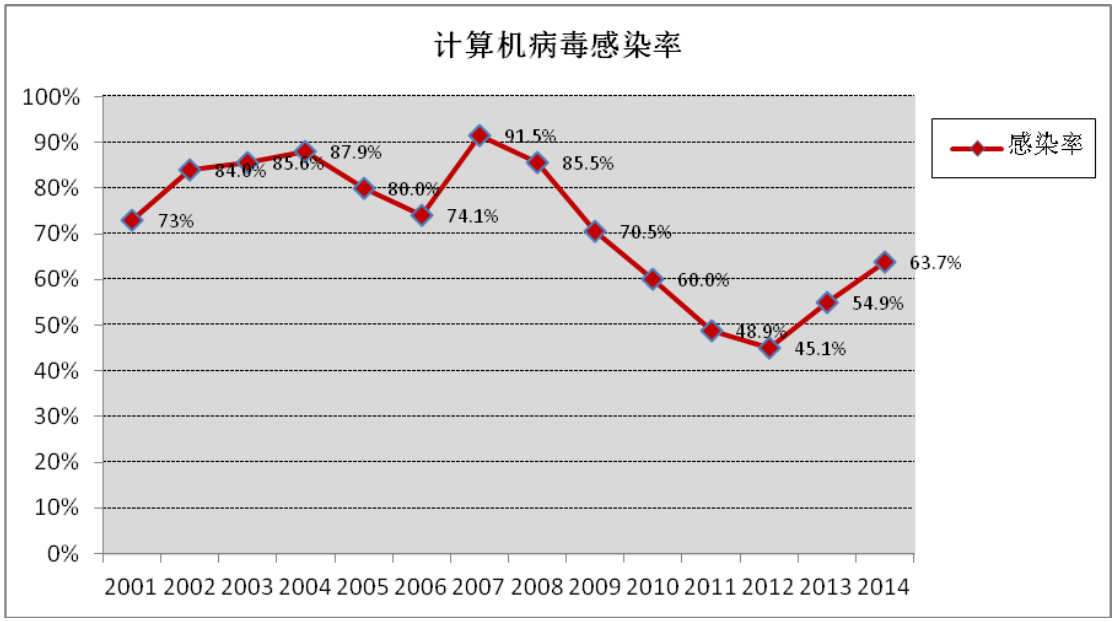

图 5　历年病毒感染比例曲线图

二、我国计算机病毒传播的主要途径

调查显示，2014 年通过网络下载或浏览传播病毒的比例占 59%，比 2013 年下降了 26.2%，应用软件下载紧随其后，占 57.6%，排在第三位的是漏洞攻击，占 37.4%。除此之外，移动存储介质、社交软件、电子邮件也是病毒传播的主要途径。

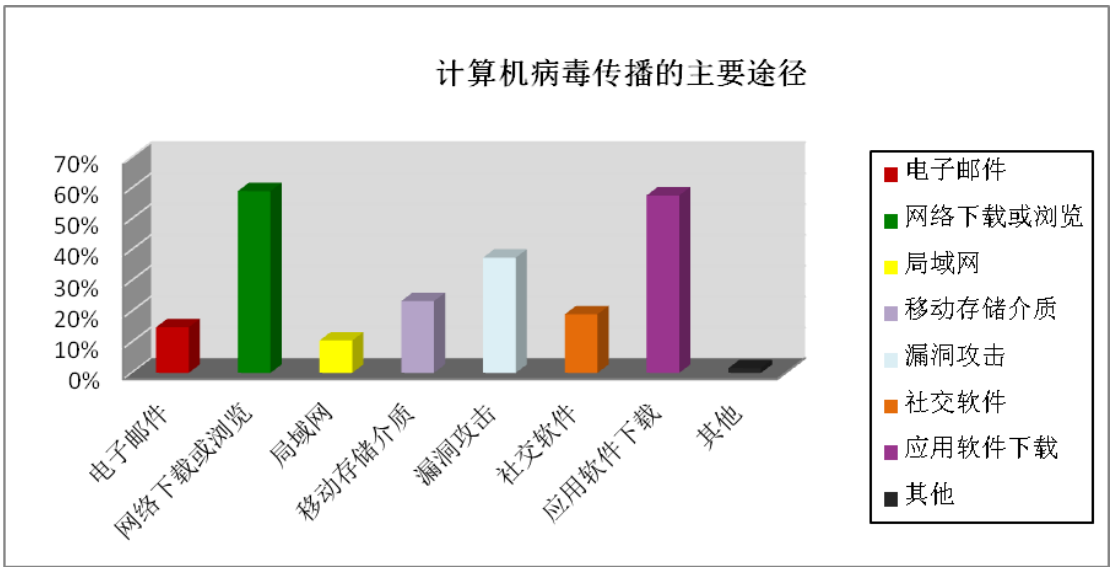

图 6　计算机病毒传播的主要途径

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。

但操作系统、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。美国国家漏洞库（NVD）公布的统计数据显示，2014 年 NVD 新加入漏洞 7038 个，被标注为“严重”的漏洞共计 1704 个。在所有漏洞中有 83%的漏洞属于第三方应用程序上的漏洞，其次是操作系统漏洞占 13%，硬件漏洞占 4%。其中浏览器中发现的漏洞数量最多，这其中 IE 更是拔得头筹。“心脏出血”（Heartbleed）漏洞和“破壳”（Shellshock）漏洞是 2014 年出现的两个波及范围广影响大的漏洞，它们的出现再次给安全界敲起了警钟：没有一个应用程序或是操作系统是坚不可摧的。

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。例如在 2014 年美国黑帽大会上，展示的 BadUSB 攻击方法让 USB 安全和几乎所有和 USB 相关的设备(包括具有 USB 端口的电脑)都陷入相当危险的境地。这些威胁主要有键盘模拟、网上欺骗、USB 引导区病毒等。

2014 年，钓鱼网站数量持续增长，在新增的钓鱼网站中，超过半数的钓鱼网站服务器分布在中国境内，中国已经成为

钓鱼网站的主要生产国。在新增的钓鱼网站中，虚假购物、银行证券、假博彩、假医假药网站占据新增钓鱼网站的绝大多数。钓鱼网站的仿冒对象通常还会紧跟媒体热点话题的变化而转移。此外，诸如节假日、重大会议活动、新闻事件、电子产品新品发布等热点都会被钓鱼网站制作者借题发挥，诱骗用户点击进而窃取访问者的个人敏感数据。对于用户而言，危害最为严重的当属侵财类的钓鱼网站，如假冒淘宝网、中奖、假理财网、假充值中心和假银行钓鱼网站。2014 年情人节期间，就又有不法分子在网上散布能够“低价”购买情人节礼品的钓鱼网站，并通过这些网站盗取用户邮箱、银行卡账户等隐私个人信息。

调查显示，应用软件下载仍然是病毒、木马传播的主要途径，特别是一些中小型网站，由于管理上的欠缺，成为病毒、木马散布的温床，游戏、视频等娱乐相关软件更是其中的重灾区。一些视频播放网站要求用户下载特定的播放器，但实际上用户下载的却是木马文件；还有一些网站采用流氓推广等手段，给用户静默安装各种软件或病毒、木马。很多色情网站和山寨在线电影网站还打着“新快播”的名义浑水摸鱼，侵害用户的电脑安全。部分用户在安全软件做出风险提示后仍然选择了信任放行，从而导致电脑沦陷。通过这种途径传播的恶意代码绝大多数为盗号木马和网购木马。

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。

2014 年日本一家计算机设备司的网站遭到供应链攻击，将植入木马的版本替换了原来的驱动程序更新，几个小时后该公司发现并清理了网站，但在这几个小时内下载更新驱动程序的用户均已被感染了木马。

三、计算机病毒造成的主要危害情况

2014 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。63%的用户浏览器配置被修改，比上一年上升了 3.8 %，连续多年成为最主要危害。系统（网络）无法使用上升了 7.9%，占 54.2%；数据受损或丢失以及密码、账号被盗分别占 47.9%和 47.3%，比上一年都有较大幅度的增长。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。

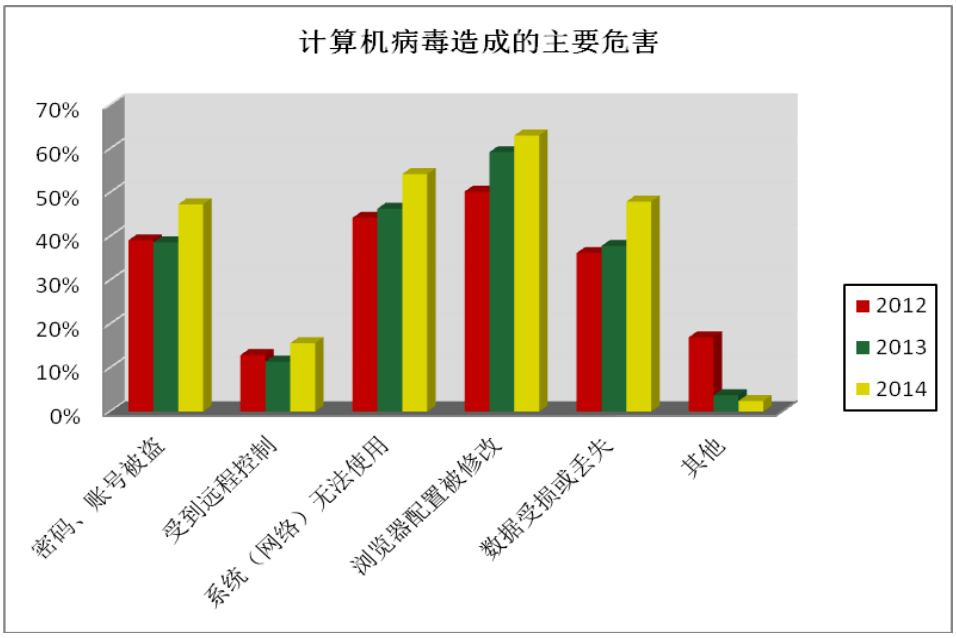

图 7　计算机病毒造成的主要危害

浏览器配置被修改是病毒、木马长期以来给用户带来的困扰，虽然安全厂商通过各种技术手段对浏览器进行保护和防篡改，但该问题仍难以得到彻底解决。通过聊天工具传播的木马，绝大多数都具备盗号功能。由于 QQ、旺旺等账号经常会与社交、娱乐、游戏、购物等多种网络服务相关联，因此，一旦聊天账号被窃取或泄漏，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。目前，越来越多的安全事件结合了社会工程学，在事件的整个过程中，最终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，也正是因为如此，社会工程学在安全事件中大行其道。虽然近两年，个人电脑的使用数量没有大幅度的上涨，但绝大多数政府、企业办公仍依赖于个人电脑，因而个人电脑的安全问题不容小视，尤其是其存储的数据保护也应成为关注的重点。

第四章 移动终端安全问题和病毒疫情调查分析

2014年，移动互联网已经成为最大的信息消费市场、最活跃的创新领域，智能手机、可穿戴设备、智能家居、互联网金融等迎来了快速的发展。2014年，我国手机网民数量达5.27亿，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。

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。2014年数据泄露、网络钓鱼事件不断暴发并呈现出针对大型机构、针对特定群体的趋势。恶意应用数量随着安卓(Android)系统用户量的增长也急剧增加，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，实施跨平台的钓鱼欺诈攻击。APP大肆窃取个人隐私，钓鱼和欺诈事件频发，移动支付类病毒成为移动用户的主要威胁。

一、 我国移动终端产品使用情况

2014年，移动终端用户中使用智能手机的用户占总数的88.3%，比 2013 年略有下降；非智能手机的用户数量则连续四年下降，占 5.3%；31.3%的用户使用平板电脑。随着智能

手机的发展，手机终端性能不断提高、网速不断提升，更多的传统互联网应用模式转移到移动互联网，越来越多的用户选择使用手机和平板电脑等移动终端上网，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，在很大程度上改变着我们的生活。在终端系统所属平台方面，90%以上为安卓（Android）系统，因其操作系统的开源性及大量的市场占有率，越来越多的系统漏洞被挖掘利用，手机恶意程序呈现井喷式地爆发，新出现的手机恶意代码中九成以上都是基于安卓系统的，用户由此造成的损失不断增加、投诉不断增长，移动终端的安全形势不容乐观。

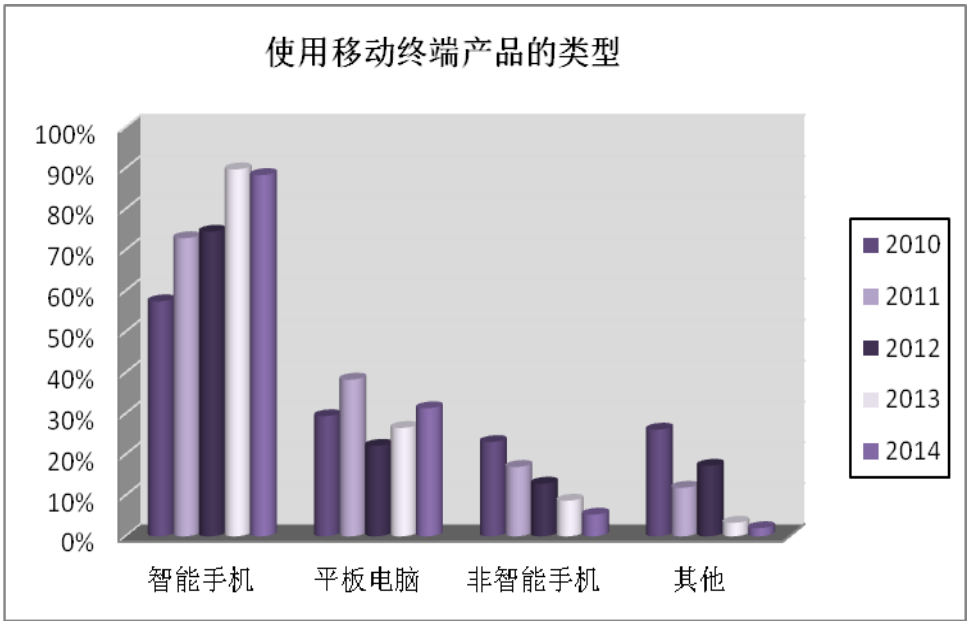

图 8　移动终端产品使用类型

二、 移动终端互联网应用情况

2014 年，用户最常使用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 85.1%稳居首位，比 2013 年上涨了 1.9%，依然是最主要的互联网应用；网页浏览以 74.5%位居第二；排在第三位的是网络游戏，占 56.3%；音视频和金融服务分别占 48.3%和 39.4%。

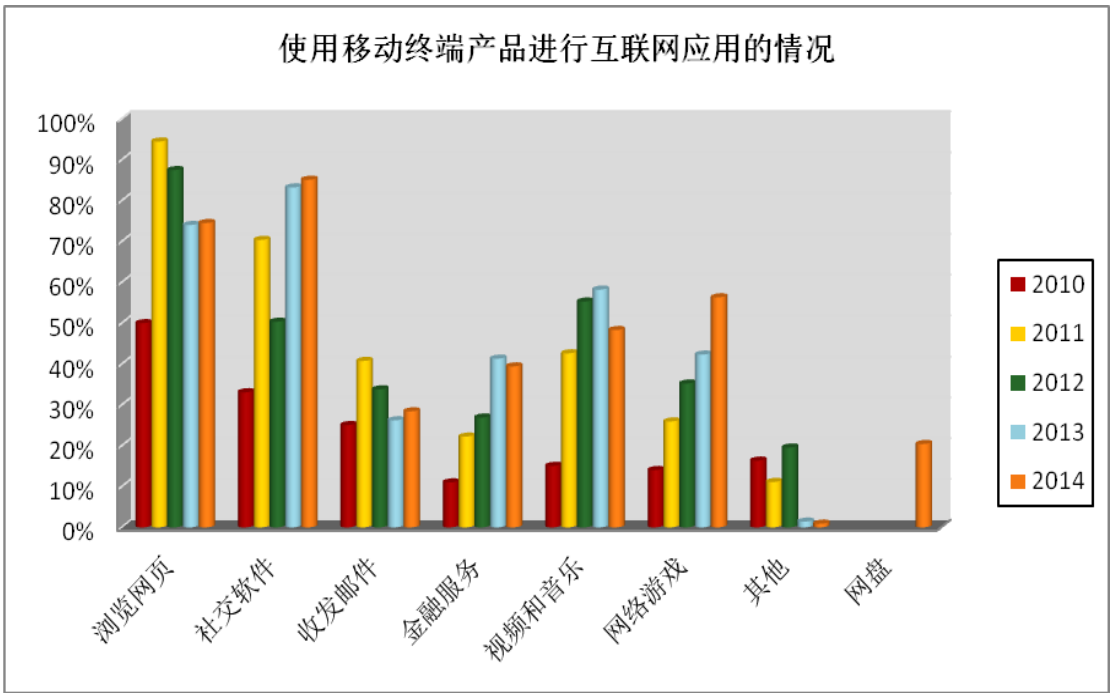

图 9　移动终端产品互联网应用情况

微信等即时通讯工具功能的不断完善，使其保持了稳定的市场份额，短信、电话等传统的通讯模式被逐步取代；网页浏览虽然与去年相比较有所下降，但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也有较大增长；手机打车软件、带有红包功能等应用的涌现，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，使移动支付安全问题凸显。2014 年，

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。但第三方应用商店对于 APP 的审核和管理仍存在相当多的问题和漏洞，给恶意软件的滋生提供了便捷的途径。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、 使用移动终端过程中遇到的主要问题

调查显示，用户在使用移动终端过程中遇到的问题可谓是形形色色，排在前三位的是垃圾邮件、诈骗短信/电话和恶意扣费（流量、话费），分别占 56.3%、56.1%和 37.8%。接下来是个人信息泄露和感染病毒、木马，分别占 32.9%和 31.3%，超过四分之一的用户遭遇过虚拟身份被盗、网络钓鱼/网络欺诈的情况。

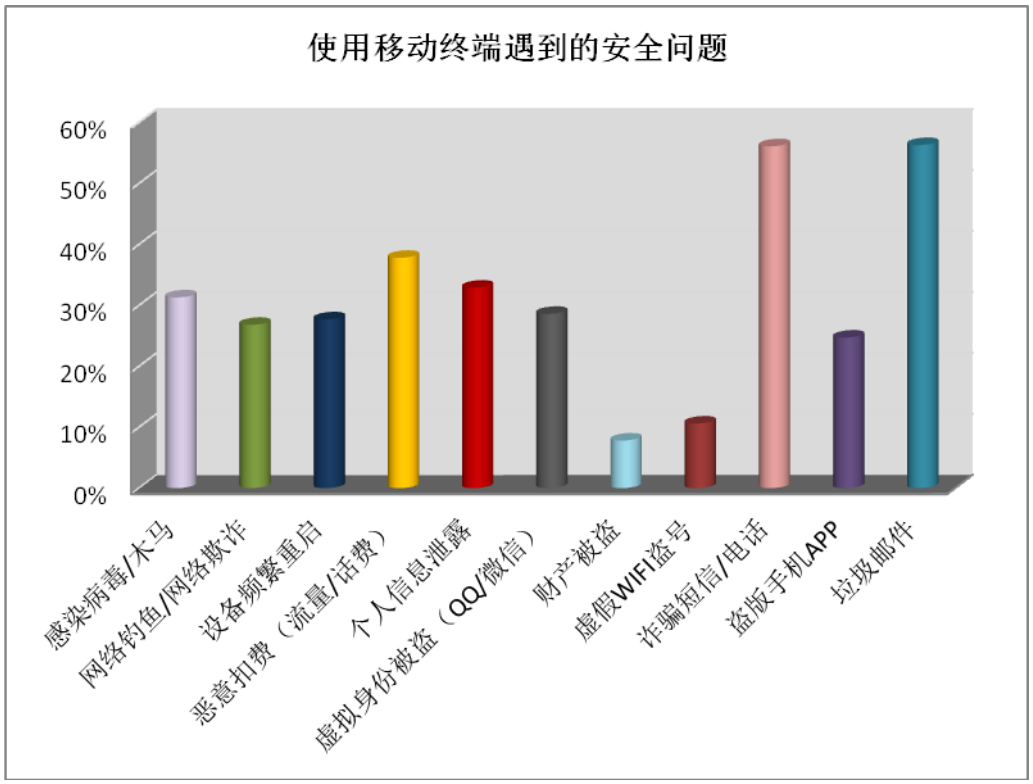

图 10　使用移动终端遇到的安全问题

2014 年，垃圾短信成为病毒、木马传播的重要途径之一，2014 年 4 月出现的“北极短信炸弹”就具有类蠕虫功能，联网从服务器获取短信内容后，读取通讯录并向通讯录联系人发送传播短信，其具有窃取用户隐私、远程控制用户手机、消耗资费等多种危害。基于手机联系人之间的强信任关系，恶意程序通过通讯录联系人群发传播短信是进行快速传播的一种有效手段，因此，也必将会被更广泛的应用。

2014 年手机用户越来越多地选择移动支付，因移动应用的监管不够全面及网民的安全意识不够，使得移动支付安全问题异常突出。从 2014 年爆发的恶意程序来看，通过诱骗页面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。

针对网银、支付、购物应用和社交应用的“山寨”情况持续泛滥，光是各种网银应用的“山寨”版本就有几百款。由于这类应用往往都需要用户输入账号密码等隐私信息，一旦用户使用“山寨”应用，这些隐私就会轻易被窃取。“山寨”应用开发门槛极低，欺骗性很强，已成为对用户隐私的最大威胁之一。近期发现“微信支付大盗”属于一个典型的“山寨”软件，其界面足以以假乱真，普通用户根本无法分辨。

37.8%的用户遭遇了恶意扣费（流量、话费），另外有大量的智能手机用户面临恶意软件的“吸费”威胁而不知。安卓智能手机的普及和山寨机的萎缩，促使恶意扣费产业链发生变化，新角色的加入使恶意扣费行为更加灵活、隐蔽，导致不知情投诉数量逐年上升。

导致不知情订购投诉增加的主要原因之一是SP/CP擅自将计费代码和地址（SDK）提供给产业链中的推广渠道。推广渠道采用恶意扣费程序在客户不知情条件下由系统后台发送订购请求，同时代替用户实现订购确认交互，最终导致用户在不知情的情况下话费被扣除。

医院检查、办信用卡、上购物网站……生活中有太多场合需要填报个人信息，手机号码、住宅电话、通讯地址、邮箱等个人信息一应俱全。而当这些个人信息被无意或者恶意泄漏之后，就如同打开了“潘多拉的盒子”，推销产品、电

话骗局、骚扰短信接踵而至。据统计，2014 年 32.9%的用户遭遇个人信息泄露。从根本上解决信息泄露问题，需要建立完善的法律、法规，通过法律的手段来保护用户个人信息。同时网络服务提供商需加大网络安全方面的投入，从源头上阻断诈骗短信等恶意信息和病毒木马的流通。个人用户还要养成良好的上网习惯，提高安全意识，尽量避免公开自己的个人信息，以免给自己带来不必要的损失。

公共 WiFi 安全状况令人堪忧，2014 年全国频现虚假 WiFi 钓鱼，不法分子通过此手段还能窃取到用户的银行账户、网络支付账户密码，从而实施资金的盗刷。如果有消费者连接了钓鱼 WiFi 并登录自己的银行系统，服务器将直接把 IP 跳到黑客设置的银行钓鱼网站。山寨网站与原网站的相似度很高，一旦用户在网页上进行登录，黑客将掌握用户的全部银行卡信息。除了虚假 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、窃取网购支付账号密码等。据统计，10.6%的人曾遭遇虚假 WiFi 威胁。针对这种情况，WiFi 提供商要进一步加强安全措施，如进行双向认证等。普通用户应谨慎使用公共场合的 WiFi 热点，尤其繁华地区一些可以直接连接且不需要验证或密码的公共 WiFi，很有可能就是黑客设计的钓鱼陷阱，尽量不使用。其次，使用公共场合的 WiFi 热点时，尽量不进行网购和网银

的操作。家用路由器一定要经常变更密码，防止被窃取和盗用。

盗版手机 APP 通常是将正版 APP 进行篡改后重新打包生成的应用。与盗版影视作品或书籍的简单复制不同，盗版 APP 的作者常常会在盗版应用中植入恶意广告插件。据统计，2014 年 24.7%的人遭遇盗版手机 APP，这些恶意广告插件不仅会在手机上乱弹广告，骚扰用户，还常常会偷偷在后台自动下载其它应用，消耗用户手机流量与存储空间。更有甚者，一些恶意广告插件还会盗取用户的通信录、短信、通话记录等信息，甚至是帐号和密码信息。盗版、山寨 APP 之所以难以遏制，除了高额利润对开发者的吸引之外，监管不到位也是一大原因。对管理部门来说，国内在手机应用立法方面存在空白，很多时候无法可依，海量的移动应用也不可能一一排查；而对于大多数移动应用商店来说，出于利益目的，往往把关不严，放低 APP 准入门槛。由于各方面缺乏监督和约束，开发者违法成本极低，使得不良 APP 数量一直有增无减。解决盗版、山寨 APP 问题必须从下载的源头抓起，在应用市场上做好管理和引导；同时，加大对移动应用上传者（包括个人和企业用户）的审核认证力度，营造一个安全可靠的移动互联网环境。

26.8%的人曾遭遇网络钓鱼/欺诈，在安全软件和安全浏览器的双重防御之下，网页挂马日渐式微。而钓鱼网站很难

被传统的安全技术所识别，因此利用钓鱼网站进行网络钓鱼成为近两年的趋势。搜索引擎传播成为钓鱼网站传播的主要手段，同时通过社交网站结合网络热点的传播方式也成为2014年网络钓鱼的新特点。

四、 移动终端病毒疫情及危害情况

调查结果显示，2014年有31.5%的移动终端使用者感染过病毒，移动终端病毒感染率居高不下，移动安全问题仍为网络安全的焦点。

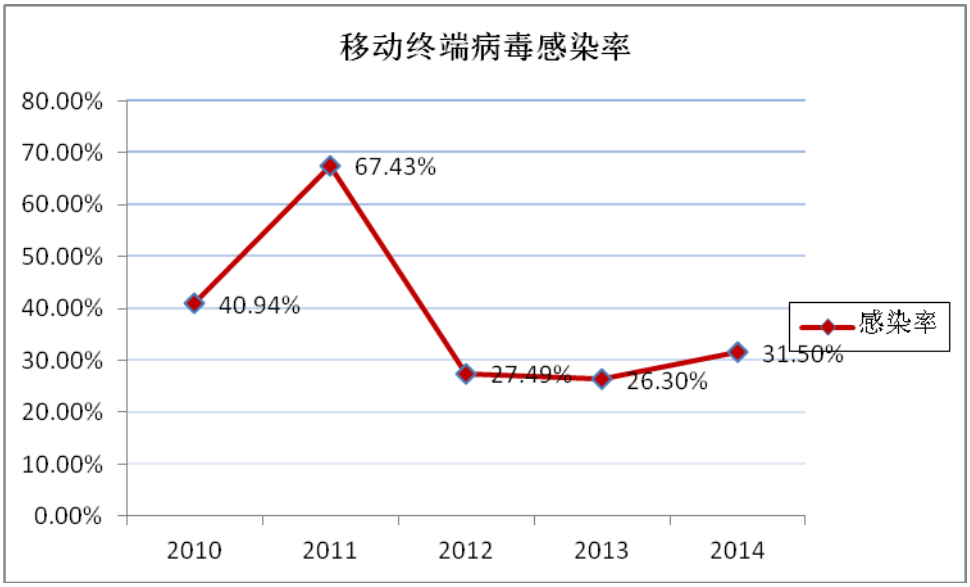

图11 移动终端病毒感染率

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，网站浏览以69.7%高居榜首，连续五年排名第一，APP下载紧随其后，占44.5%，通过社交软件进行感染的比例高达40.5%，相比上一年有大幅提高。微信等社交工具的快速流行，导致了伪造微信等社交工具的应用泛滥。病毒传播者伪造微信最新测试版、内测版，欺骗网民

安装，再伪造微信支付要求提交银行卡信息，进而骗取网民详细个人信息（身份证号、手机号）和银行卡号、有效期、卡背面的 CVV 码。一旦中招，银行卡资金即被盗取。通过电脑连接进行感染的比例为 38.9%，相比去年增长了 11%，由于 PC 端的病毒产业依然猖獗，电脑连接被感染的途径也是一直困扰着广大网民。通过短信、彩信进行感染的比例为 32.6%，相比去年有所提升，主要因为短信木马以一种蠕虫式的方式进行传播，通过在短信息或彩信中附带恶意链接的方式给用户造成威胁，其中最典型的案例为“XX 神器”病毒，该病毒在 2014 年七夕期间于全国范围内爆发，被称之为超级手机病毒，通过好友发出含有病毒下载链接的短信在短时间达到 754 万， 2 小时蔓延全国各大省市，该病毒也因此成为 2014 年度手机安全重大影响力病毒。安卓（Android）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消费者带来了不少安全隐患。安卓（Android）移动应用非常容易被篡改，木马制作者可随意在正常 APP 中捆绑恶意代码并发布。

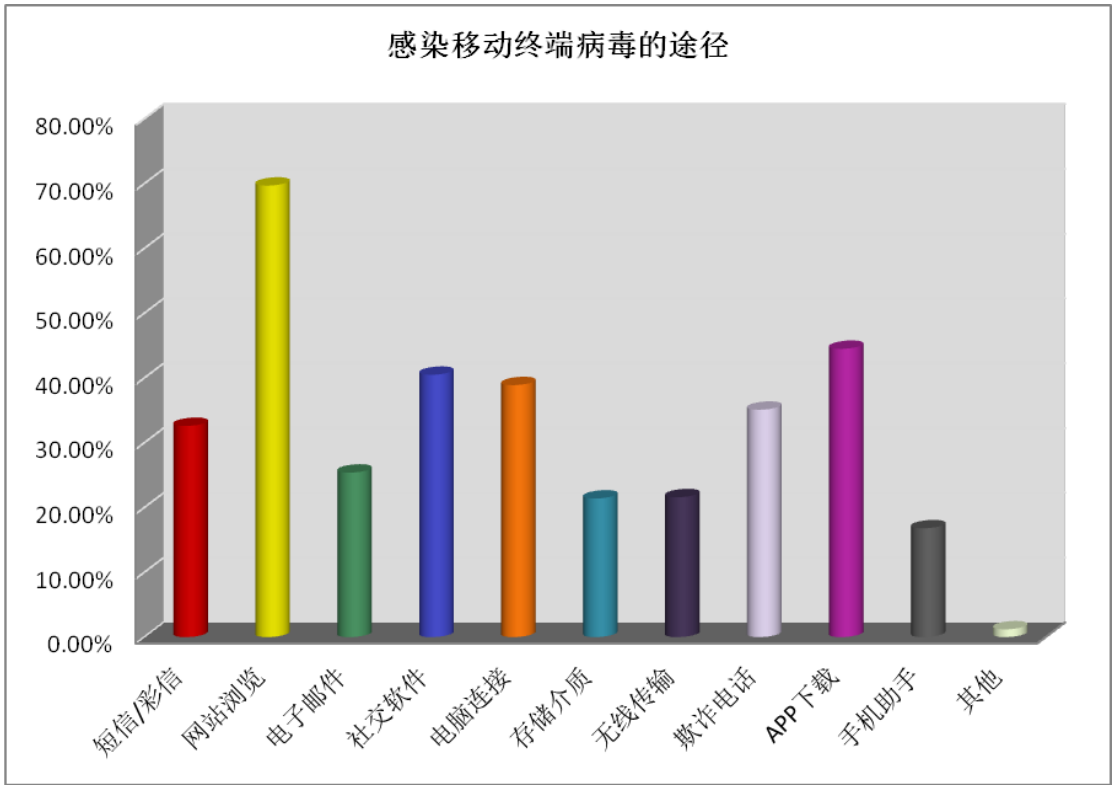

图 12　感染移动终端病毒的途径

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。影响手机正常运行连续三年排在第一位，2014 年感染此类病毒的用户达到了 74.4%，这类病毒会导致手机耗电过快，频繁重启，出现发热、卡慢等现象。2014 年信息泄露用户高达 61.5%，相比去年大幅度攀升，随着大数据时代的来临， 对海量数据的分析越来越重要，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，数据变得越来越有价值，也正因为这样攻击者也在不断发起针对数据的攻击。2014 年感染恶意扣费程序的用户达到了 57%，其主要恶意行为是通过自动联网，上传和下载数据，安装其他应用，消耗用户手机流量和资费。远程受控用户占 21.3%，病毒通过短信接收

特殊控制指令，实现远程控制、开启后门、在指定日期开启或结束病毒的功能。病毒实现的远程控制功能通常包括：短信监控及上传、电话监控、窃取通讯录、安装和卸载手机程序、GPS 定位、开启摄像头。

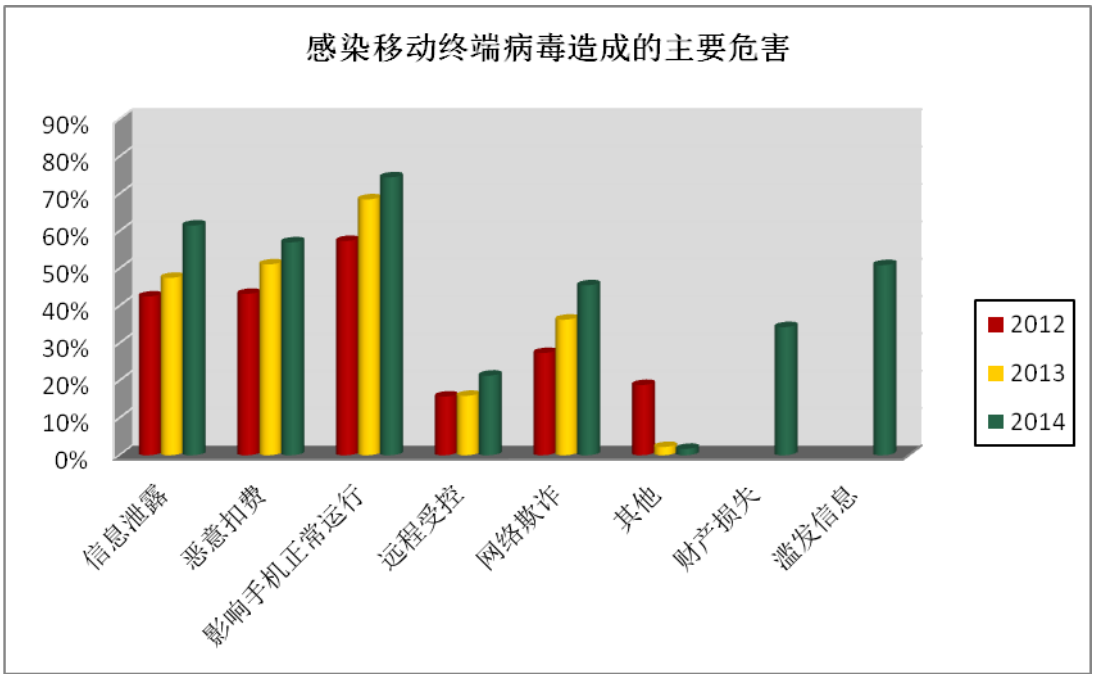

图 13　感染移动终端病毒造成的主要危害

目前，我国拥有手机网民 5.27 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，据统计，有 16.3%的用户不使用移动终端安全产品，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，在人们的工作生活中扮演着越来越重要的角色：通讯、工作社交、娱乐等都离不开手机，因此培养安装使用手机安全软件的习惯非常重要。

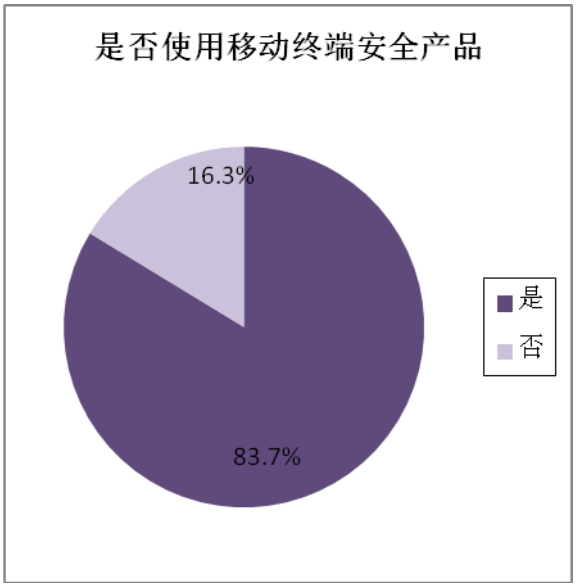

图 14　是否使用移动终端安全产品

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、趋势科技（中国）有限公司、猎豹移动、北京奇虎科技有限公司、北京瑞星信息技术有限公司、恒安嘉新（北京）科技有限公司等为国家计算机病毒应急处理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“第十四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。