2014-2015 中国互联网安全研究报告

目录

2014 年度互联网安全威胁的主要特征

1. 新增电脑病毒数及病毒感染量双双下滑

猎豹移动安全实验室的监控数据表明，2014 年全年截获的新病毒比去年下降 15.6%，病毒感染量比去年下降 19%。病毒数量和感染量双双下降，但仍是个庞大的数字，每天有近 10 万个新电脑病毒被捕获，网民及安全厂商不可掉以轻心。

2. 捆绑安装流氓软件成电脑病毒主要赢利点

病毒木马黑色产业链出现新变化：大量推广流氓软件安装、强行篡改浏览器成为主要威胁。电脑游戏玩家、常看网络视频的用户、经常下载安装盗版破解软件的网民是高风险人群。

3. 钓鱼网站数量继续高速增长

与电脑病毒影响下滑相反，钓鱼网站危害明显上升。相对于病毒攻击来讲，钓鱼网站的攻击门槛更低，攻击成本也更低，而攻击成功后的收益却很高。2014 年猎豹移动安全实验室拦截新增钓鱼网站数比 2013 年增长 165%，平均每天有 1.44 万个新出现的钓鱼网站。

危害最严重的钓鱼网站是假冒淘宝网、假中奖网站、假理财网、假充值中心、假银行网站和假 QQ 安全中心的危害最为严重，其最终目的都是骗钱。

4. 中国网民网银安全遭遇严重挑战

2014 年全球中安卓病毒的手机共 2.8 亿部，平均每天 80 万部安卓手机中毒。中国以近 1.2 亿部手机中毒高居全球榜首，中国成为全球受安卓病毒之害最严重的国家。

安卓手机病毒超 6 成会窃取手机位置信息和上传手机号，超 3 成会收发短信、上传联系人信息。与手机支付业务有关的安卓病毒占总量的 60%，其主要恶意行为是：伪装诱骗用户输入银行卡号、身份证号、预留手机号等敏感信息，利用拦截短信、盗刷、诈骗等手段给用户造成重大财产损失。

尤其值得高度关注的是，2014 年病毒从业者几乎完美结合了钓鱼网站和手机病毒两种攻击手法，他们利用假冒 10086 积分兑奖钓鱼网站骗取网民身份信息和银行卡信息，再利用手机病毒拦截验证码短信，在全国范围内利用伪基站设备广泛撒网，制造了空前的网银被盗灾难。

5. 垃圾短信困扰全球用户

由于手机短信业务全球范围内受微信、Whatsapp、Line 等智能手机应用软件影响较大，正常网民短信使用量下降，使得垃圾短信比重显得更加突出。

2014 年猎豹移动旗下多款安全产品拦截了超过 637 亿条垃圾短信，中国用户收到的相当一部分垃圾短信来自伪基站设备。在全球范围内，苹果手机用户都受到 iMessage 垃圾消息的骚扰，由于 iOS 设备的特殊性，安全软件对此类垃圾消息缺乏拦截有效手段，苹果手机用户只能选择举报或关闭 iMessage 来减轻骚扰。

安全风险数据分享

1. 电脑病毒的感染情况

2014 年，猎豹移动安全实验室共截获电脑病毒样本 3587 万个，截获的新病毒数比 2013 年的 4250 万个下降近 15.6%。2014 年平均每天拦截 9.8 万个新病毒，病毒数量虽有所减少，总量仍然十分庞大。

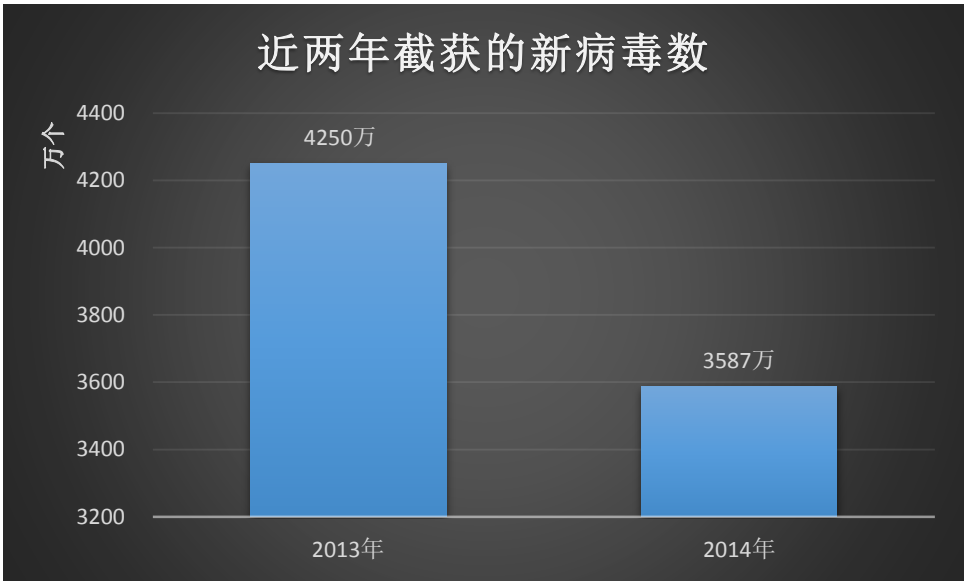

图 1 近两年截获的新病毒数

2014 年监测到感染恶意程序的电脑共 1.7 亿台，比 2013 年的 2.1 亿台下降了 19%。

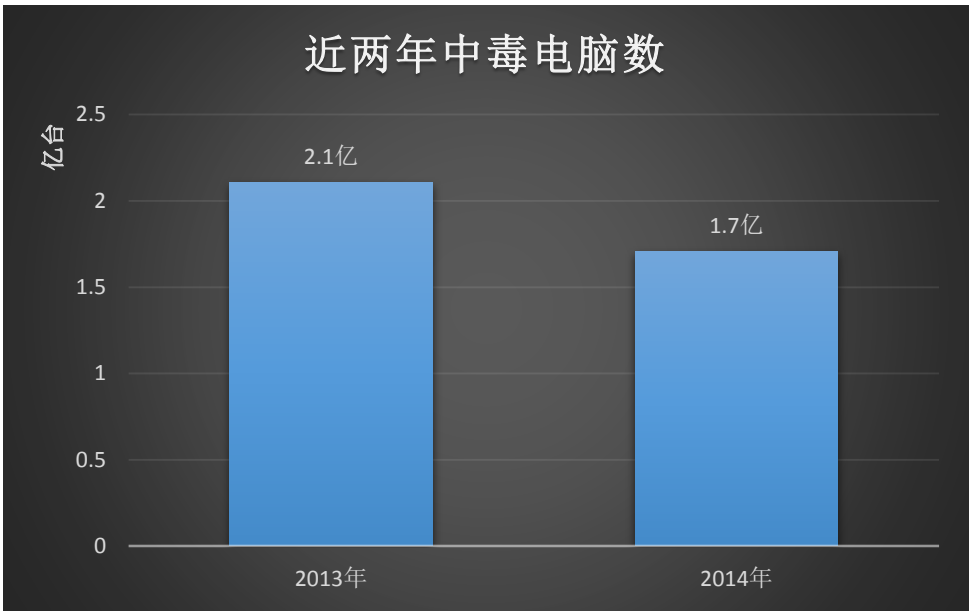

图 2 近两年中毒电脑数

从 2014 年各月捕获的病毒数和感染量变化趋势来看，呈下滑态势，其中病毒感染的机器数量下滑更为明显。

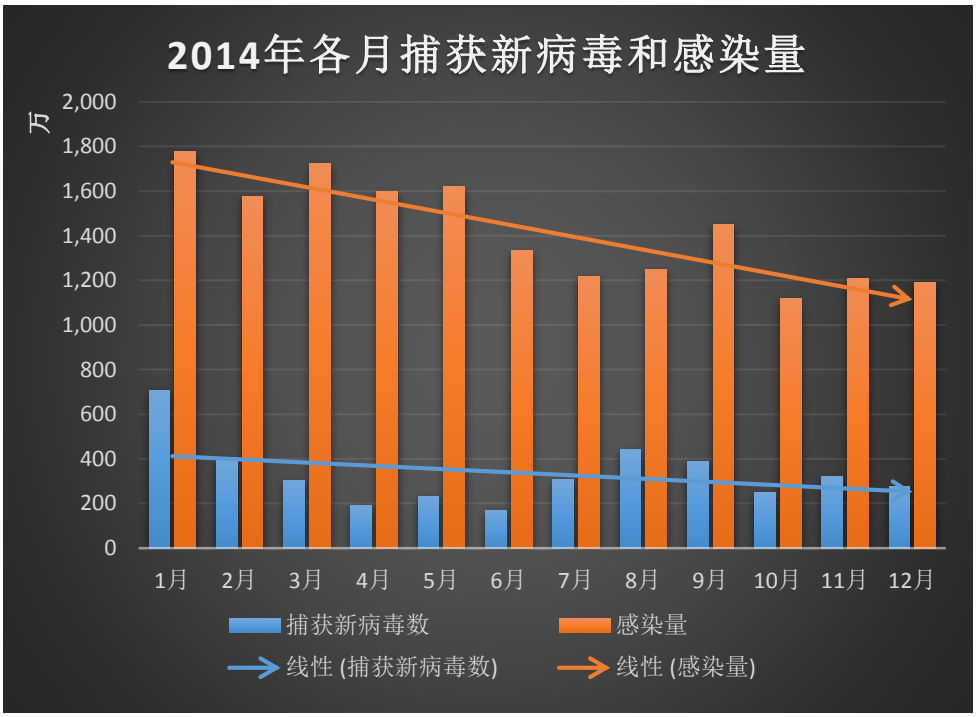

图 3 2014 年各月捕获的新病毒数及病毒感染量

电脑病毒感染排名前五的省份依次为广东、江苏、山东、浙江、河南，其中广东省电脑感染量为其他四个省份的 2-3 倍。

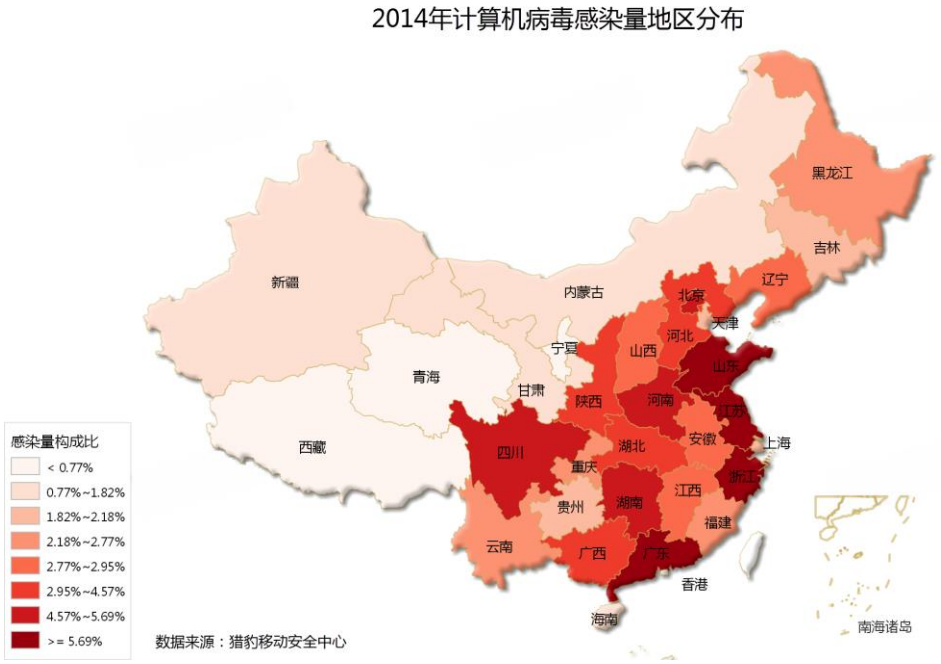

图 4　2014 年电脑病毒感染地区分布

2. 电脑病毒的新变化

分析 2014 年电脑病毒的传播手法，发现和以往并无太大差异。最活跃的电脑病毒主要通过假冒游戏外挂、辅助插件、高清视频播放器、软件破解汉化注册机等众多网民喜爱的工具传播。

病毒程序也主要分布在盗版视频下载站、盗版软件下载站、网络聊天室、色情网站、小说下载站、游戏外挂插件下载站、QQ 群空间和网盘中。

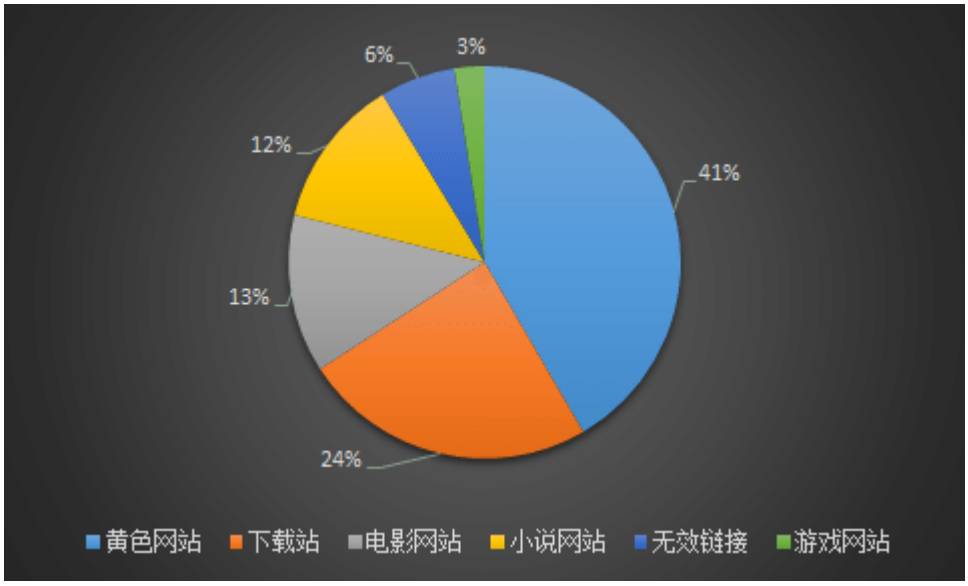

图 5 电脑病毒的主要下载渠道

2014 年电脑病毒的主要危害包括远程控制、捆绑安装大量软件、篡改浏览器主页、劫持家用路由器 DNS、在电脑端强行弹出广告和钓鱼网站。

针对这种情况，2014 年金山毒霸特别强化了针对钓鱼网站的防御及阻止病毒安装流氓软件的功能。平均每天阻止病毒安装流氓软件的次数超过 140 万次（峰值超过 200 万次/天），病毒恶意捆绑安装流氓软件的趋势明显上升，被病毒捆绑安装流氓软件的电脑台数平均超过 60 万台。

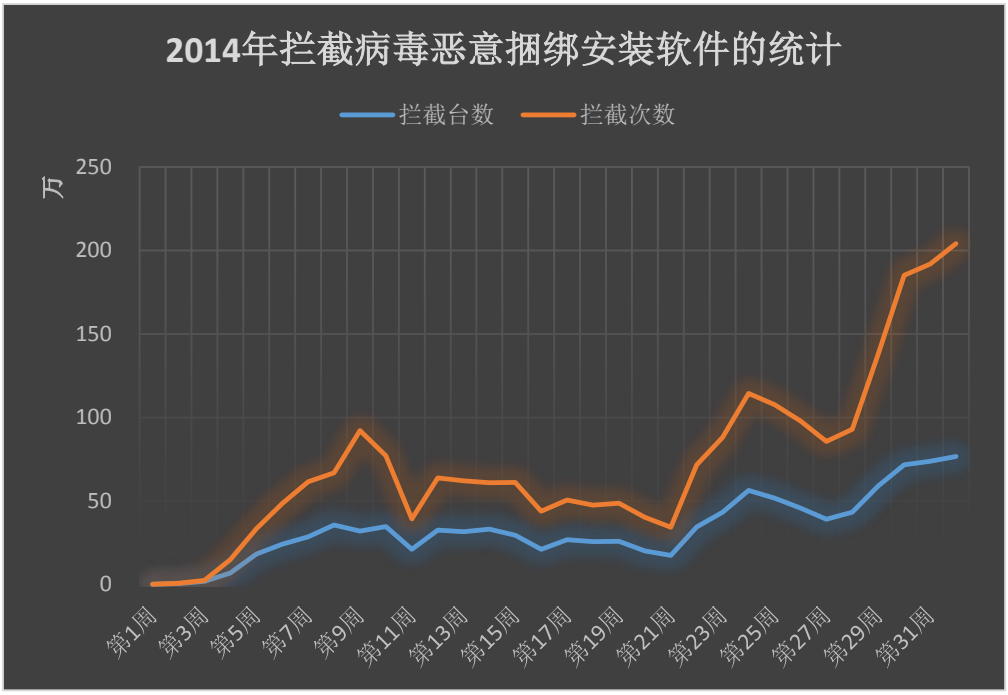

图 6　2014 年金山毒霸拦截病毒捆绑安装流氓软件的情况

3. 安卓手机恶意软件感染数据

2014 年 Android 用户量达到 20 亿，Android 系统在智能手机系统的市场占有达到 84%，Android 手机病毒也不断增加，2014 年猎豹移动安全实验室共捕获 280 万个安卓病毒样本，较 2013 年的 85 万个增长 2.29 倍，其中与移动支付业务相关的手机病毒占 60%以上。

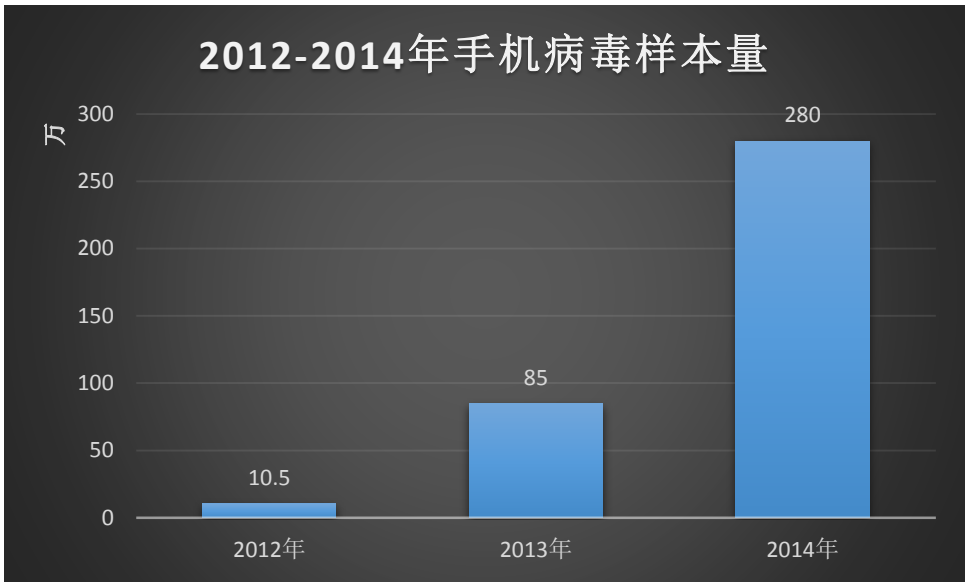

图 7 近三年手机病毒样本增长情况

全球感染病毒的安卓手机也不断增加，2014 年，全球曾经中毒的安卓手机数量超过 2.8 亿部，较 2013 年的 1.5 亿部增长，平均每天 80 万部安卓手机中毒。

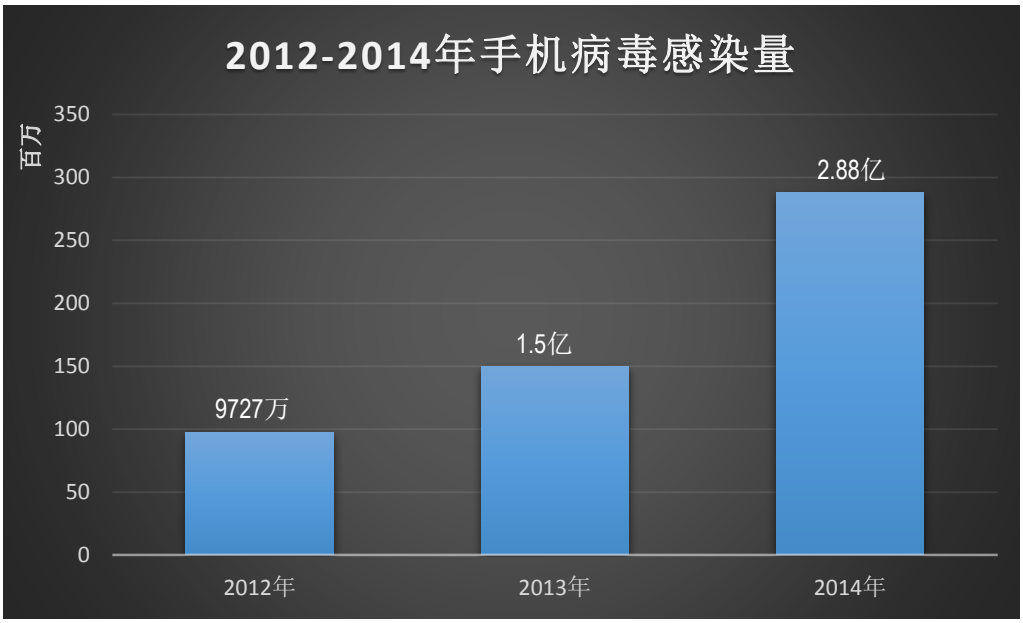

图 8 近三年手机病毒感染量

安卓病毒感染量最高的十个国家，中国以 1.2 亿部手机中毒高居榜首，印度、印尼分列第二，第三。

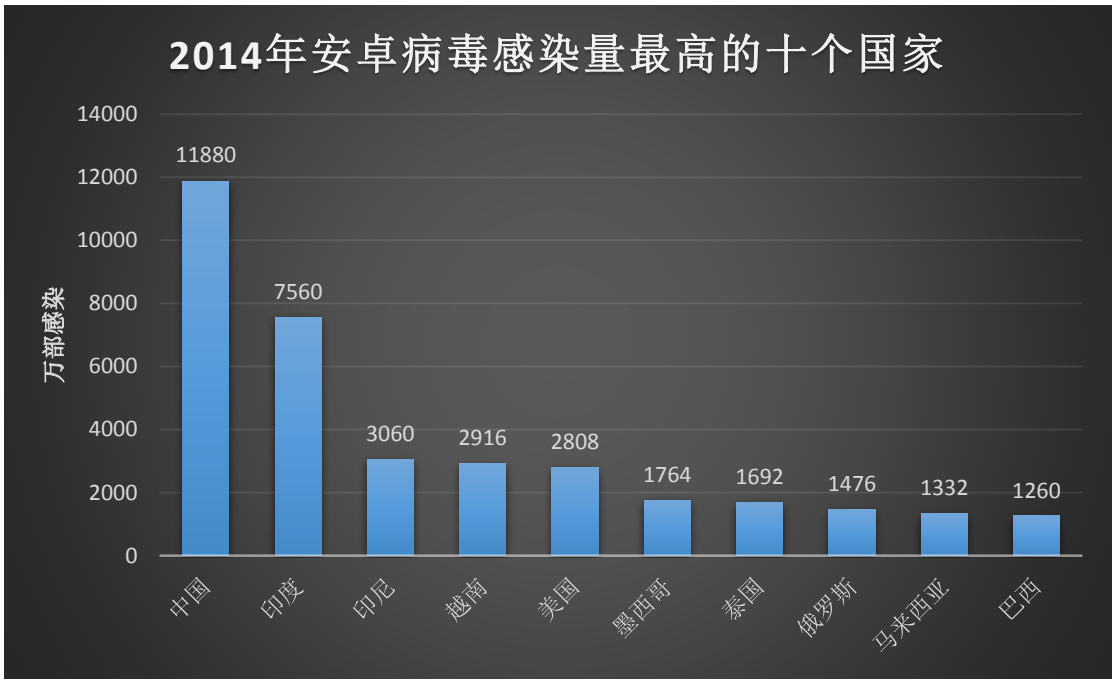

图 9　2014 年全球安卓病毒感染最严重的十个国家

安卓病毒的危害分类：

猎豹移动实验室根据病毒的危害结果对安卓病毒分五大类：移动支付、资费消耗、隐私窃取、远程控制、黑客工具。

移动支付类病毒的感染量高居榜首，占总病毒样本总量的 60%，其主要恶意行为是：伪装诱骗用户输入银行卡号、身份证号、预留手机号等敏感信息，利用拦截短信、盗刷、诈骗等手段给用户造成重大财产损失。

资费消耗占 14%，其主要恶意行为主要表现为：偷偷发送 SP 短信订购扣费业务，静默下载垃圾应用或后台联网消耗用户流量，以及在游戏、色情应用中诱骗用户支付等。

隐私窃取占 20%，其主要恶意行为是：窃取短信、通讯录、精确位置信息，甚至照片，电话录音等。

远程控制类占 2%，其主要恶意行为是通过远程指令操纵手机完成特定动作。

黑客工具类占 4%，其主要行为是对其他电脑或手机执行网络攻击动作。

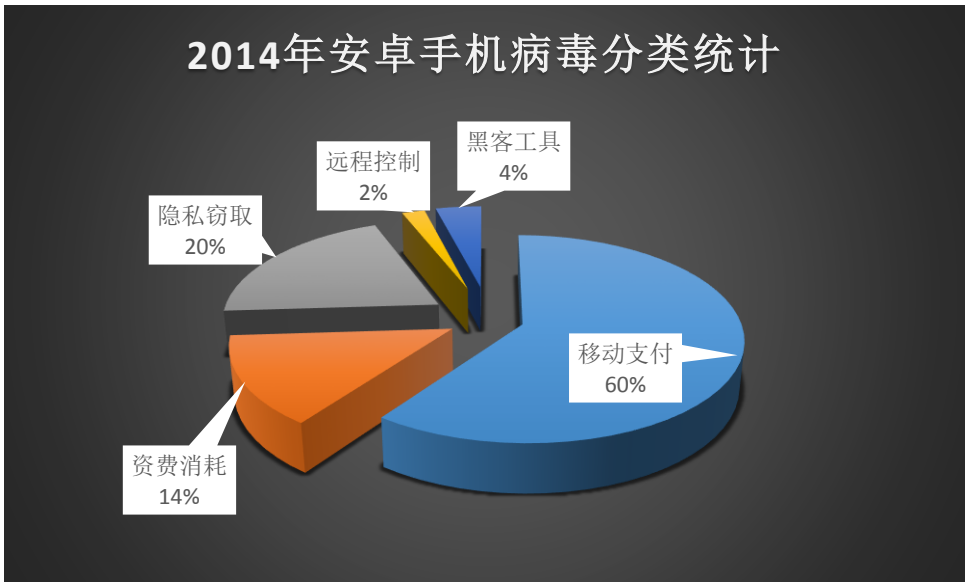

图 10 安卓手机病毒分类统计

安卓病毒的主要恶意行为统计：

安卓病毒最常用的恶意行为前三位是上传定位信息、上传手机号和发短信。

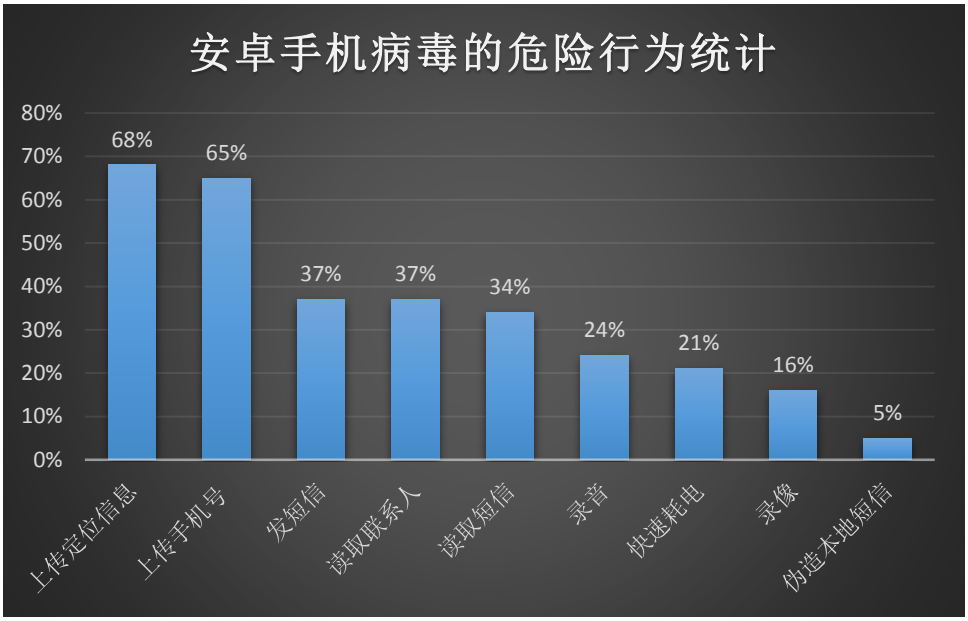

图 11 安卓手机病毒的主要恶意行为

2014 年，中国网民深受假银行 APP、假微信 APP 及假中国移动营业厅 APP 的毒害，这三个典型的手机病毒均以窃取用户网银资金为目的。通过病毒程序内嵌的网页或通过浏览器访问钓鱼网站先收集网银信息，再拦截受害者手机短信，给大量受害者造成严重损失。

用户名	开户行	银行卡号	卡密码	身份证号	手机号码	类型	有效期	CVV	提交时间
威	中国农业银行	622848 :11	92	42102319 19	1397 92	储蓄卡			2014-12-4 20:58:16
珍	工商银行	62220 3	1 7	420104 3	135 46	储蓄卡			2014-12-4 20:57:57
成	邮政银行	62179 0011	1 9	42900419 5	186	储蓄卡			2014-12-4 20:56:00
禁 洋	农业银行	622 8	5 6	420621 8	159 48	储蓄卡			2014-12-4 20:55:24
马 成	邮政银行	62179 11		429004 35	186 3	储蓄卡			2014-12-4 20:51:07

图 12 假 10086 网银大盗窃取的网银及身份信息

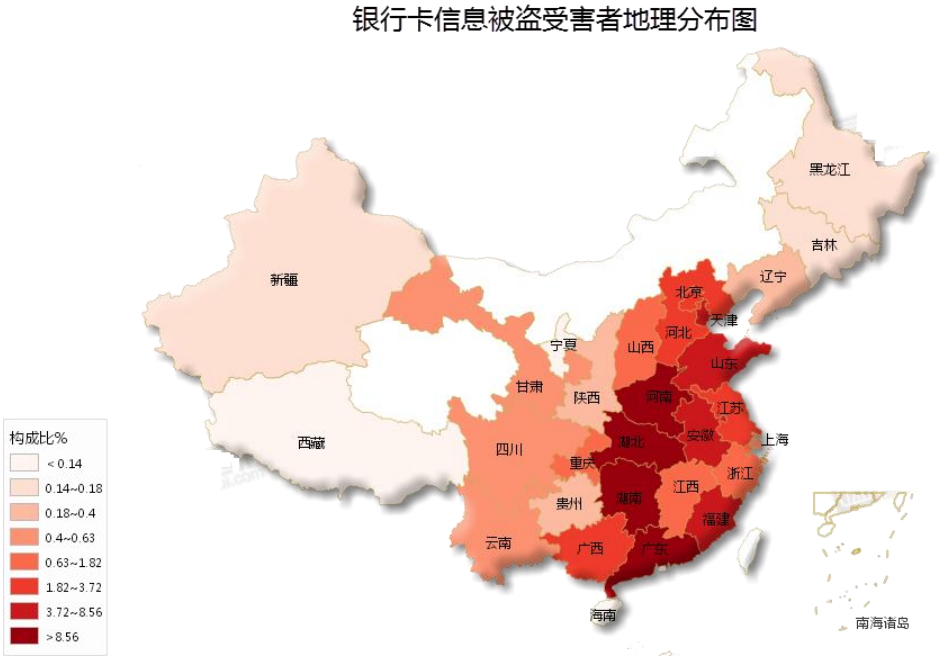

图 13 假 10086 移动营业厅手机病毒的受害者分布

4. 垃圾短信拦截数据

2014 年日常短信使用量下降，垃圾短信显得更加突出。猎豹移动旗下多款安全产品仍然拦截了总量超过 637 亿条垃圾短信。

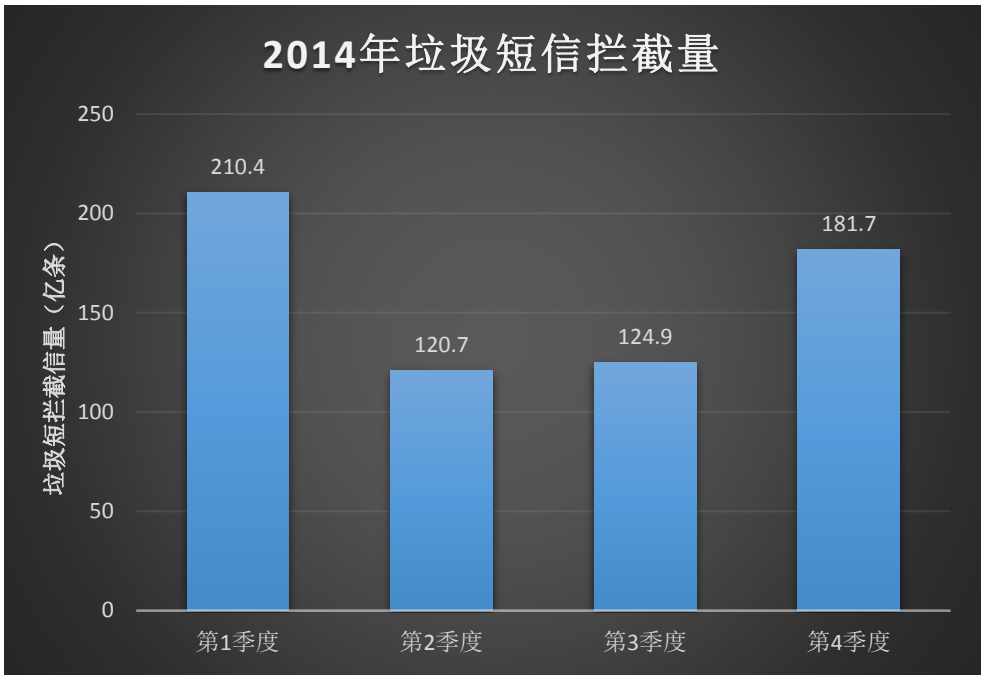

图 14　2014 年垃圾短信拦截量

垃圾短信中，除了商业机构群发的广告骚扰短信，对网民影响最大的当属诈骗短信。猎豹移动安全实验室将诈骗短信分以下 6 类：

中奖类（19.2%）：爸爸去哪儿等热门综艺节目抽奖

假房东（13.12%）：假冒房东收房租

赌博诈骗（11.78%）：各种博彩广告诈骗短信

假冒熟人诈骗（8.21%）：诱使手机用户拨打电话， 然后以交谈、沟通等技巧诱使当事人一步步掉入陷阱。

网购诈骗（8.15%）：特别多见的是网购退款类诈骗短信

其他类型（39.54%）：假冒电信营业厅积分送礼，假冒银行短信升级动态口令等

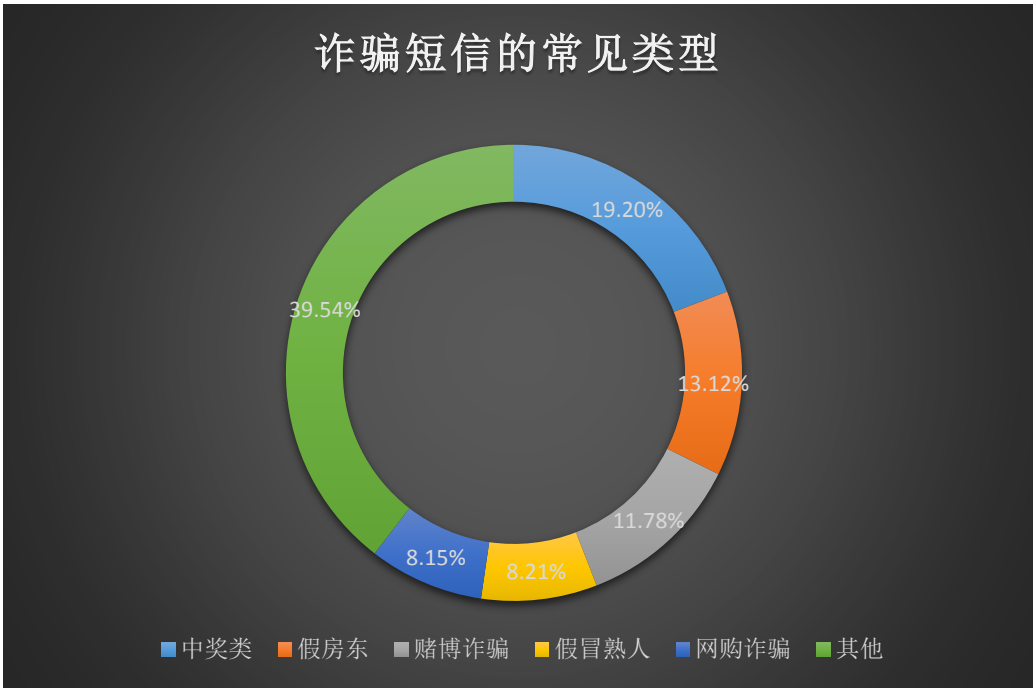

图 15 诈骗短信分类统计

由于运营商强化了在服务器端的垃圾短信过滤，大量垃圾短信经营者使用伪基站设备和改号软件（使用 VoIP 服务，伪造发件人大量群发）

特别需要指出的是，苹果 iMessage 服务遭遇严重垃圾消息侵扰。由于未越狱苹果手机无法使用第三方的垃圾消息过滤工具，苹果手机用户只能通过举报垃圾消息或关闭 iMessage 服务来屏蔽垃圾消息骚扰。

5. 钓鱼网站拦截统计

2014 年，金山毒霸安全中心累计拦截新增钓鱼网站 524 万个，比 2013 年 243 万个增长 165%。

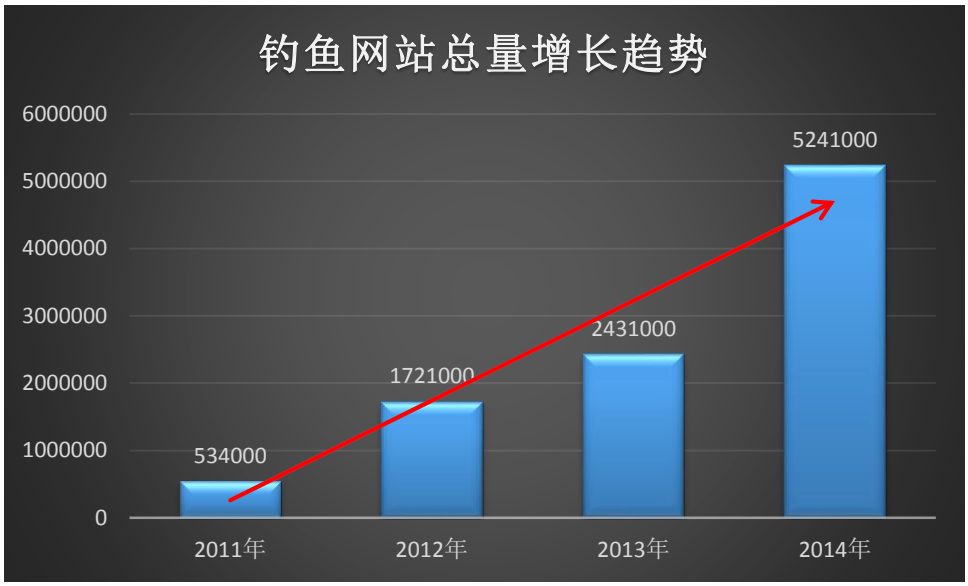

图 16 新增钓鱼网站增长趋势

2014 年平均每天拦截新出现的钓鱼网站约 1.44 万个。

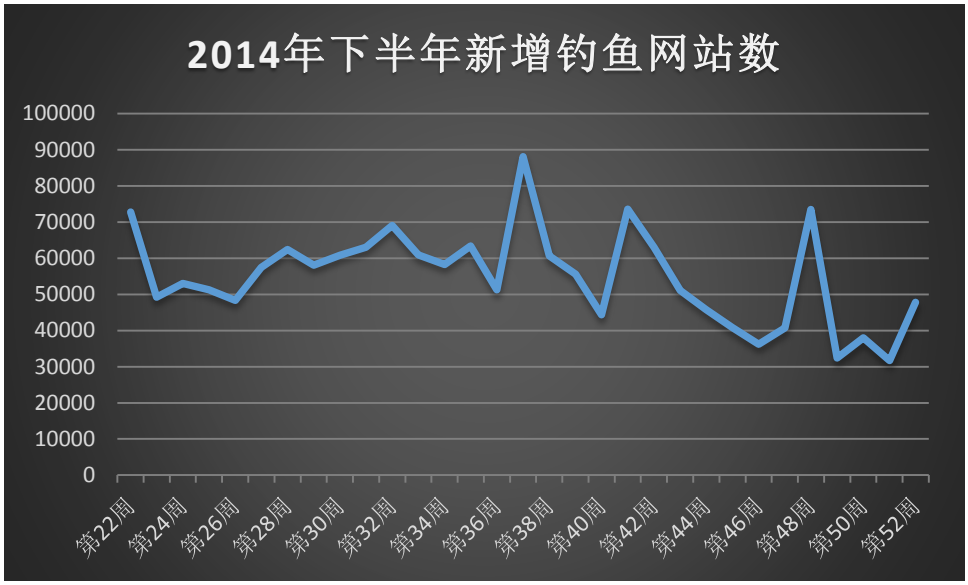

图 17 2014 年下半年钓鱼网站增长情况

在网民日常接触到的钓鱼网站中，假博彩网站一枝独秀，2014 年累计新增超过 250 万个，这类钓鱼网站借世界杯、非法六合彩大量传播。假色情网站 95 万个，这类钓鱼网站主要借色情网站的噱头欺骗网民安装专用播放器来传播病毒。

对网民来说，危害最严重的当属那些假冒淘宝网、中奖、假理财网、假充值中心和假银行钓鱼网站，这些钓鱼网站从数量上来讲，比假博彩站、假色情网站少得多，但危害更加严重。

假 QQ 空间的主要危害是盗 QQ 号和密保信息，得手之后，再假冒受害者身份向 QQ 好友借钱消费，或继续发送同样的钓鱼网站盗窃更多 QQ 号。

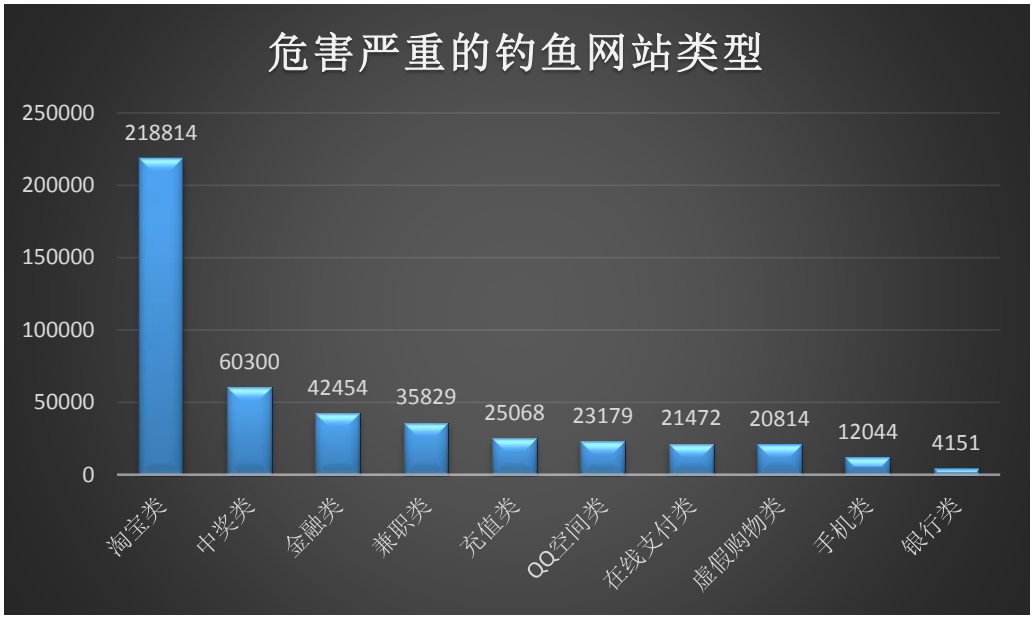

图 18 危害最严重的钓鱼网站分类统计

2014 年是猎豹移动为金山毒霸客户提供网购敢赔服务的第二个年头，这一年，共有超过 5000 名用户因各种原因上网时被骗、被盗向金山毒霸安全中心提出网购敢赔申请，5000 余名网友共计上报的损失额超过 700 万人民币。

假 10086 网银大盗将手机病毒和钓鱼网站结合在一起，通过伪基站设备群发短信攻击，在全国范围内制造了大量受害者。假 10086 移动营业厅钓鱼网站数从 2014 年 7 月的 500 余个增长到 12 月的 3000 余个，半年时间，仅这一种钓鱼网站就增长了 6 倍。

图 19 伪 10086 积分兑奖钓鱼网站增长情况

2014 年重大安全事件

1. OpenSSL Heartbleed（心脏出血漏洞）

这是一个可以影响上百万个不同网站的严重安全漏洞，黑客通过漏洞可轻易盗取用户的账户信息与密码。据相关人士估计，目前全球有三分之二的互联网服务使用 OpenSSL 来保护用户的信息安全，心脏出血漏洞会导致这些服务器的用户数据暴露在危险之中。

2. 安卓任意拨打电话漏洞

该漏洞可不经用户许可，允许恶意应用发起或结束通话，也可以使其向预定号码发送 USSD/SS/MMI 代码（使用拨号盘拨出特定号码，可完成特定任务，比如重置手机）。此种行为在手机自带通话服务启动之前，就可完全绕过正常应用应被授予的通话权限展开通话。

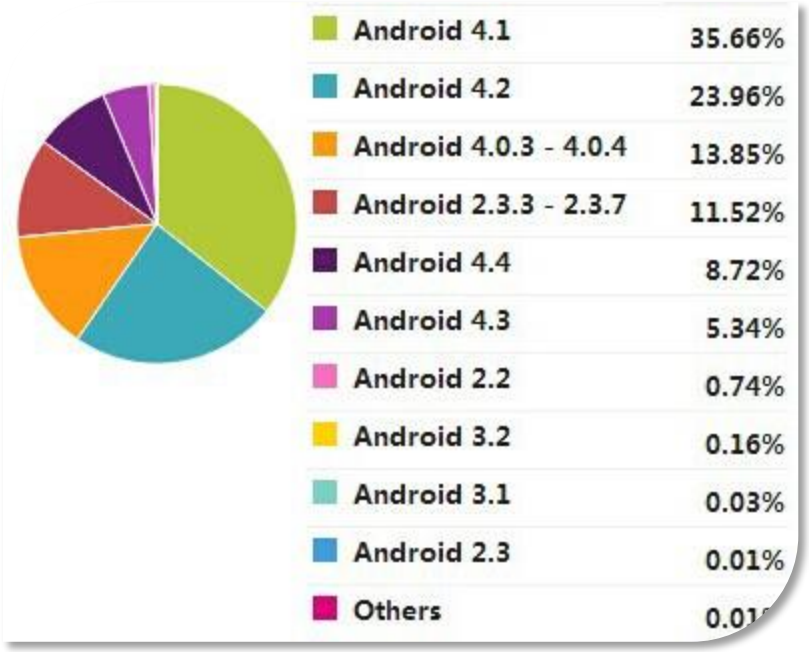

图 20 任意拨打电话的漏洞安卓系统分布

3. Bash ShellShock（破壳漏洞）

影响到几乎每一个基于 Unix 的操作系统，包括 Linux 和苹果的 Mac OS X，甚至比 2014 年最具噱头的心脏出血漏洞危害更大。

利用这个漏洞，攻击者可能会接管计算机操作系统，可以访问机密信息，并对系统进行更改，网站的用户信息会被偷走：用户数据，如账号密码、信用卡号码、个人照片，甚至逛街的历史完全暴露在黑客面前。更糟糕的是，黑客还可以利用该漏洞偷偷将病毒移植到网站上，当其他用户访问这些网站时，会被安装恶意程序。

4. 安卓漏洞层出不穷

由于安卓的碎片化，使得漏洞修复代价的较高，漏洞可能一直持续存在，直到用户更换新的智能设备。

漏洞名称	版本	时间
Fake ID 漏洞	4.4 及以下版本	2014 年 7 月
任意拨打电话漏洞	4.1.1-4.4.2	2014 年 7 月

broadanywhere 漏洞	5.0 以下版本	2014 年 11 月
WebView 漏洞	几乎所有版本	近年来多次出现
安卓提权漏洞	三星猎户座 Exynos 4210 或 4412 CPU Towelroot 漏洞，Linux 内核小于等于 3.14.5 版本的手机存在该漏洞	

5. **eBay 数据泄露事件**

   2014 年 5 月，eBay 要求 1.28 亿活跃用户重置密码，黑客可能从 eBay 获得用户密码、电话号码、地址和其他个人信息。这次泄密事件给 eBay 造成 1800 万美元的损失。

6. **iCloud 数据泄露**

   2014 年 9 月，100 多名好莱坞明星艳照被泄露在社交网站，引发用户对 iCloud 数据安全的信任危机。苹果随后在全球推行帐号密码两步验证。

7. **黑客声称获得 Dropbox 700 万用户密码**

   2014 年 10 月，黑客声称窃取了 700 万条 Dropbox 用户信息，并放出 400 个电子邮箱供验证。Dropbox 拒绝承认遭遇攻击，并认为已泄露的帐号来自第三方服务。

8. **Gmail 500 万数据泄露**

   2014 年 9 月，俄罗斯黑客公布了近 500 万个 Gmail 邮箱帐号密码，这些密码可能是用户访问钓鱼网站泄露的，安全人员建议 Gmail 用户启用两步验证加强安全性。

9. **索尼遭遇黑客攻击**

   由于极具争议的电影《采访》上映，索尼影业遭遇黑客攻击。大量员工明星的个人信息因此泄露，这场网络安全危及还引发外交争端，多方相互指责。

10. **12306 13 万用户数据泄露**

    2014 年 12 月，有黑客通过地下产业链出售 12306 用户数据，由于正值春运，该消息立刻轰动中国社交媒体。虽泄露的数据量并不大，但媒体和网民的关注度极高。经安全专家鉴定，这 13 万用户数据泄露为黑客通过以往泄露的大量网民数据撞库攻击筛选所得，泄露数据的两名黑客也很快被抓获。

2014 年度十大病毒

1. **Win32.ADWARE.Agent.ac 及其变种**

   广告弹窗插件,2014 年第一季度此类样本变种非常活跃，感染用户近千万，中招电脑频繁弹出色情、钓鱼等诱导性广告弹窗，普通用户无法正常卸载清理。

2. **QQ 蠕虫木马(Win32.Troj.AgentQQ.ao)及其变种**

   该蠕虫病毒家族利用 Windows 系统漏洞、网络共享文件夹、垃圾邮件附件和可移动存储设备等进行传播，可造成系统文件删除、计算机用户访问文件夹受限、系统程序无法启动等。

3. **“食猫鼠”(Win32.Troj.Agent.a)及其变种**

该木马属于典型的流量推广类病毒，使用多种技术手段对抗杀毒查杀防御，主要恶意行为包括静默安装推广第三方软件、劫持用户的主页设置以及垃圾广告推送等，严重干扰用户正常使用电脑。

4. **“高清影视”流氓木马(Win32.ADWARE.Agent.ac)及其变种**

“高清影视”流氓木马，具体症状表现为篡改 IE 主页 hao123.com，在桌面生成“美女直播室”的网页快捷方式，双击运行浏览器时会打开 hao123.com；还会往电脑里安装第三方软件以赚取推广费。该流氓软件主要通过宅男影音等流氓播放器捆绑安装，而这些播放器又是通过其他软件推广安装、下载站和色情网站诱导下载安装进行传播的。用户或在安装其他软件时被推广安装，或因无法抵制诱惑主动下载安装，进而遭受损失。

5. **远控木马(Win32.Troj.Dropper.uw)及其变种**

主要通过“吉吉影音”等流氓软件捆绑传播，“吉吉影音”通过色情网站进行诱导安装，用户一旦下载安装了该播放器，其捆绑的木马便会连接 xzhan.120dxyy.com 并上传用户信息，用户电脑便成了木马团伙的肉鸡。

6. **假 10086 网银大盗**

病毒传播者利用伪基站设备，伪造 10086、110、银行客服电话等号码，群发诈骗短信，该类病毒样本的变种数量高达 3000 个。中毒用户首先会通过手机浏览器访问一个收集银行卡、身份证、手机号的钓鱼网站，接下来下载病毒程序安装到手机上，然后犯罪分子可以在几分钟内将受害人银行卡的资金转移到其他帐号，全国各地出现大量受害者。

7. **XX 神器、聚餐相册**

病毒传播主要利用“聚会照片“”好有信息“等噱头在朋友间传播。病毒主要危害是，窃取用户隐私，拦截短信上传短信内容，然后利用隐私交易的黑色产业链通过贩卖用户隐私获利。从 8 月爆发到现在，相关病毒样本及变种数量达到 49 个其中本月初爆发最新变种”聚餐相册“病毒 9 个，主要感染中国大陆地区。XX 神器受害者几十万人，聚餐相册受害者超万人。

8. **爱魔鬼**

爱魔鬼”(Imogui)病毒伪装成手机系统服务(System Service)，藏身于数量庞大的山寨手机和水货手机的 ROM 中。该病毒运行后，就会像“魔鬼”一样通过远程服务器的指令控制用户手机：获取手机硬件敏感信息，静默下载其他应用，静默安装其他应用，强制启动指定应用，强制卸载指定应用，推送通知栏广告。平均每天 25000 人，三月份至今感染用户超过 800 万。

9. **山寨网银客户端**

在中国多个第三方安卓应用市场传播，几乎中国内地所有商业银行的客户端均被山寨伪造。受害者在手机安装这类 APP 之后，会被诱骗提交银行卡详细信息，部分病毒同时具备拦截短信的功能，会造成受害者网银资金迅速被盗。

10. **山寨微信客户端**

微信是中国内地非常受欢迎的手机软件，病毒传播者伪造微信最新测试版、内测版，欺骗偏爱软件新版本的网民安装，再伪造微信支付要求提交银行卡信息为借口骗取网民详

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。

典型电脑病毒产业链分析

随着移动互联网的快速发展，网民越来越多的时间在使用手机和平板设备，使用电脑的时间在减少，今天的计算机病毒几乎个个以牟取非法利益为目的。2014 年，金山毒霸安全中心深入挖掘了多个典型电脑病毒的利益链。

1. Game670 棋牌游戏盗号木马

这个棋牌游戏盗号团伙伪造了大量的官方网站，通过优化“game670”,"670 棋牌" 等关键词搜索排名，诱导玩家下载捆绑了盗号木马和远控木马的安装包，通过窃取账号密码或者通过远程监控与玩家对玩，再将获取的游戏币通过中间“银商”进行套现。运作模式和以前的 game456 案件类似。

病毒团伙	传播网站	安装包MD5	技术手段
团伙A	http://wwwgarne670.com:67/670/ http://wwwgama670.com:67/670/ http://wwgama670.com:670/670/ http://wwgema670.com:680/670/ http://www.game670.cm/	899A43105FA215BBFD49BB8C9B150D8C	捆绑远控木马+盗号木马
团伙B	http://wwwgarne670.com:67/670/ http://wwwgama670.com:67/670/ http://wwgama670.com:670/670/ http://wwgema670.com:680/670/ http://www.game671.cm/	7231E8002826EDFB13DB29A5D0D66777	捆绑远控木马+盗号木马
团伙C	http://www.gnme670.com:670/ http://www.gane670.com:670/ http://www.grme670.com:670/ http://www.gmae670.com:670/ http://game670.gmae09.com:670/ http://game670.nmtex.com:670/	5dd5e578b489c4bdc39cd248acd2721d	捆绑远控木马+盗号木马
团伙D	http://www.xjniran.com/ http://www.rrbiefa.com/ http://www.oyjyh.com/	4471B3BB822499B8FB8D8E6EE7B6CDFF	捆绑远控木马 (白加黑)
团伙E	http://www.game670.com.cn	C9EC1F58DD744B1E2CAA68E329DA7EA5	捆绑远控木马
团伙F	http://game670.zjxys.com/	8B028AB1C812FE5EE0A4B06E85FEF27B	捆绑远控木马+盗号木马
团伙G	http://www.gamo670.com/ http://www.dnfxiaoyouxi.com/	29B3B454C98335C22776696A9744508B	捆绑远控木马 (白+黑)
团伙H	http://game670com.net/ http://www.game670.cc/ http://www.gmae670.com:670/	55D032ABA047AE8AD634848D83F3CAD6	捆绑远控木马 (gh0st变种)
团伙I	http://www.gems670.com:67/ http://www.gaos670.com:670/ http://www.geso670.com:670/	F2E4819A91C07EE357DF8E65DB228B10	捆绑盗号木马
团伙J	http://www.vilian8.com/670/ http://www.tjdydj.com/670/	959C3B6C3D8D97214A27F0EDDA8040F1	捆绑盗号木马
团伙K	http://wvvw.garme670.com:71/ http://wvvw.gerna670.com:67/	8768E599F3E1522BCD4CE1F343A5D198	捆绑盗号木马
团伙L	http://gaeme670.com:89/	5F1D904F19D3E66120757AFE071B7C7A	捆绑远控木马 (gh0st变种)

图 21 Game670 病毒样本的跟踪情况

2. 豆豆（又名“天涯”）QQ 群蠕虫病毒产业链

2014 年上半年出现大量 QQ 蠕虫木马（盗取用户 QQ 帐号 ClientKey），电脑中毒

后，会自动向 QQ 空间、腾讯说说、微博中发布大量垃圾广告、色情信息，还会自动向好友或群空间上传木马，造成此类病毒更大范围的传播，散播的垃圾信息也对用户造成恶劣影响。

对 QQ 蠕虫的传播源进行分析，发现主要幕后传播团伙为“豆豆工作室”，豆豆工作室开发运营“病毒营销系统”，同时多级代理大批量传播 QQ 蠕虫木马获取非法收益，顶峰时期“豆豆工作室”下面拥有超过 1000 名的代理商。

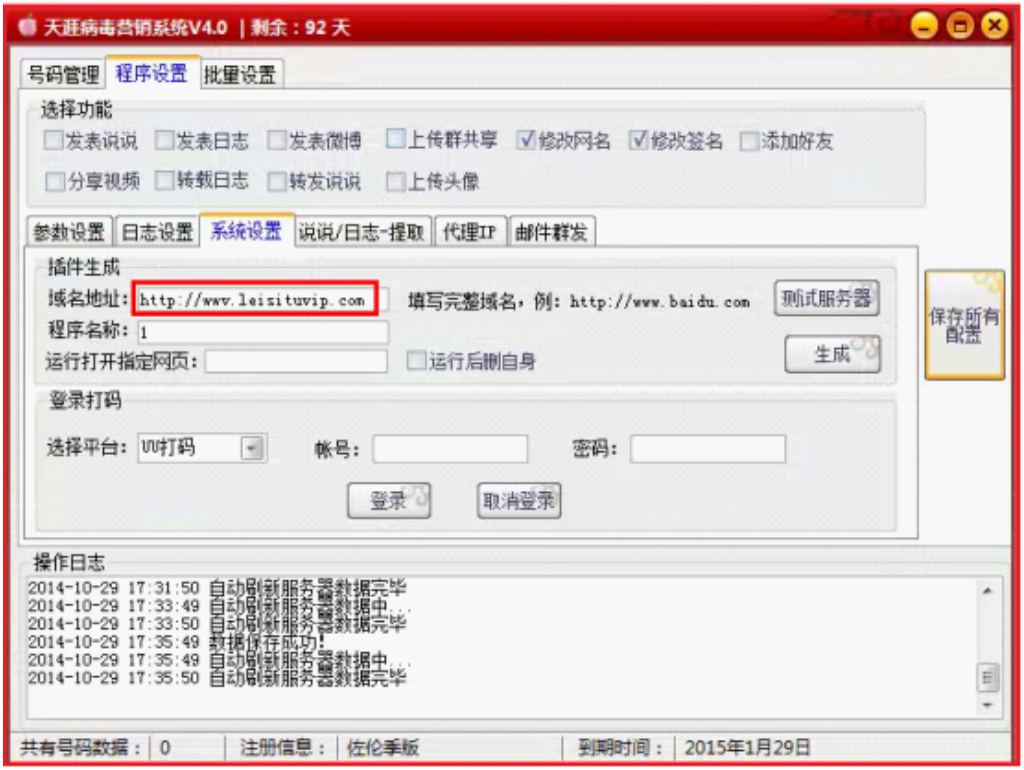

图 22 豆豆工作室的病毒营销系统界面

3. “食猫鼠”流氓软件传播案

“食猫鼠”病毒属于非常典型的恶意推广类病毒，病毒捆绑在一款名为“好爱 FM 收音机”的流氓软件中，主要通过一些色情站点和下载站点的诱导虚假下载链接进行传播。

病毒作者使用了系列复杂的手法逃避和对抗杀毒软件，病毒的最终目的是向中毒电脑远程无提示自动大量流氓软件，篡改浏览器快捷方式和主页。从“食猫鼠”病毒服务器得到的安装统计数据中可以看出，该病毒一天最高感染 9 万台电脑，在一个半月的时间里，累计感染电脑超过 95 万。

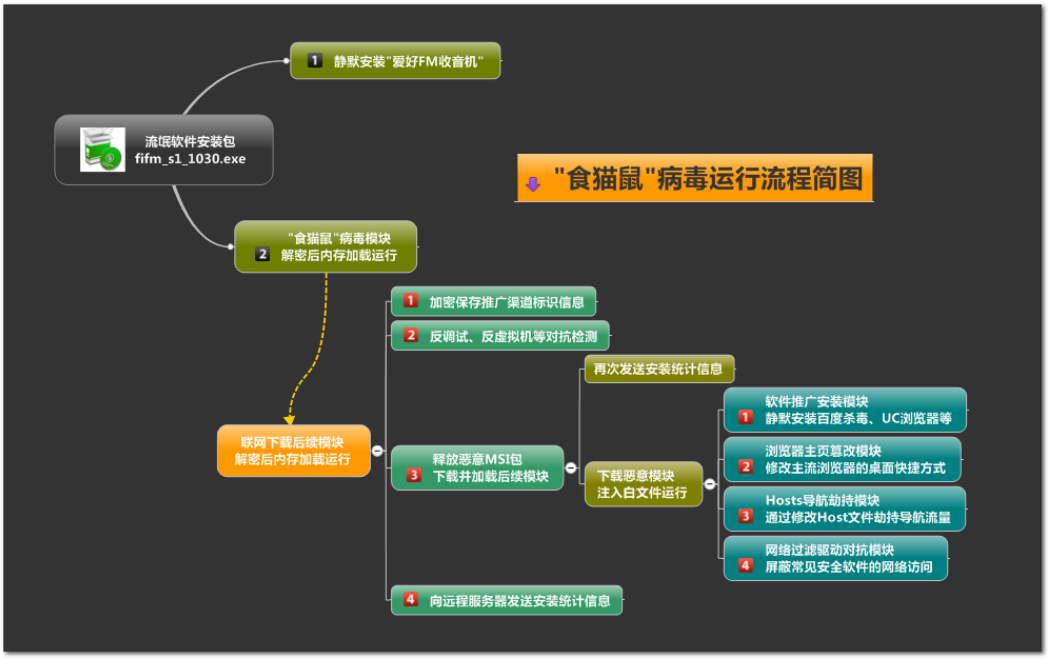

图 23 食猫鼠病毒产业链的关系图