2011-2012

中国互联网安全研究报告

金山网络
www.ijinshan.com

2011-2012 中国互联网安全研究报告

目录

第一章　2011 年度互联网安全威胁四大特征

1. 钓鱼网站取代病毒木马成为首要安全威胁

金山毒霸云安全中心数据显示：2011 年钓鱼网站增速明显，下半年进入集中爆发期，2011 全年新增钓鱼网站数量达到 45 万个，2011 年 12 月当月新增钓鱼网站是 1 月份的两倍以上。2011 年 11 月，金山毒霸拦截钓鱼网站次数达到 11 亿次，（而 2010 年最高峰也仅有 1000 万次），受影响网民约占总数的 10%，网民平均每浏览 14 个网页就有一次遇到钓鱼网站。

2011 年金山毒霸拦截新增病毒达到 1230 万个，较 2010 年呈现下降趋势，日平均拦截次数约 500 万次。2011 年，钓鱼网站的拦截次数是病毒木马的 5 倍之多，钓鱼网站已经成为中国互联网安全的首要威胁。

钓鱼网站的制造手法也呈现多样性和技术性，从直接复制伪造知名网站的页面，到利用 XSS 的漏洞攻击、制造多次跳转来达成钓鱼的目的。

2. 网购木马呈现增长趋势，网购攻击日益严重

2011 年，网购木马呈现增长趋势，表现十分活跃。网购木马经营者大多使用 QQ、淘宝旺旺等聊天工具实施一对一的诈骗，隐藏性很强，成功率很高，危害性极大。2011 年 3 月，知名互联网交互设计专家“一叶千鸟”网购被骗 5 万余元。

金山毒霸云安全中心数据显示，2011 年，金山毒霸网购保镖日平均保护 2000 万次网购操作，日均覆盖 500 万网民。由于网购涉案金额具有金额小，取证难等问题，一旦受害维权难度极大。为此，金山毒霸推出了敢赔模式，用户在开启敢赔功能的情况下，由于钓鱼或者木马导致网购被骗，金山公司将进行赔付。

除了进行一对一的诈骗以外，部分网购木马还主要针对浏览器进行重点突破，2011 年，金山毒霸经常截获网购木马主动推荐浏览器的情况，用户使用该浏览器进行购物，被害风险极大。金山毒霸提示用户，网购时请谨慎选择浏览器，如果浏览器阻止第三方安全软件在用户网购时进行保护，请及时切换浏览器。

3. 电脑病毒制造者向手机安卓平台转移

高性能智能手机和平板电脑市场份额的快速增长，以及手机购物、手机游戏等应用的风靡，引发了手机安全威胁的爆发，电脑病毒制造者将主要诈骗阵地从 PC 转移到手机。

金山手机卫士云安全中心数据显示，2011 年安卓平台的恶意软件增长速度迅猛，据样本数统计，年末日均新增病毒数量比年初增长十倍。全年安卓平台新增病毒数量 23681 个，受害用户 1037 万人，其中 660 万手机用户是在手机论坛或手机安卓市场下载软件时中毒。

而智能手机的恶意软件类型也呈现多样化，从最开始的暗扣话费、订购服务、浪费流量、消耗电力，发展到窃取隐私和云端控制手机。2011 年底，数以千万计的智能手机被曝植入 CIQ 手机间谍，一时引发全球瞩目。

软件漏洞也是黑客攻击的另一个重要通道，2011 年，数个智能手机管理软件的安全漏洞曝光，安卓平台手机接入无线局域网后，攻击者可以轻易获得手机中存放的个人隐私数据。

4. 社会化媒体成为诈骗传播新宠

2011 年，恶意传播者利用人们社会心理而非技术手段实施欺诈的案例增长十分明显，这种趋势未来会愈演愈烈。防范这种社会工程欺诈和假冒社交熟人欺诈，仅靠安全软件不行，最关键的还在于网民要提高自己的安全意识。

恶意软件传播者往往通过盗取网民登录信息，利用热门的社会化媒体微博、SNS 社区等发送中奖、送礼或广告等钓鱼网站实施进一步的欺诈攻击。由于社交媒体多属于熟人网络，用户极易放松警惕最终受骗。

第二章　安全风险统计数据

1. 病毒感染统计与分布

1)　新增病毒总数再次下滑

2011 年金山毒霸捕获新增病毒 1230 万个，从新增病毒总量来看，这是自 2010 年来的再次下滑。

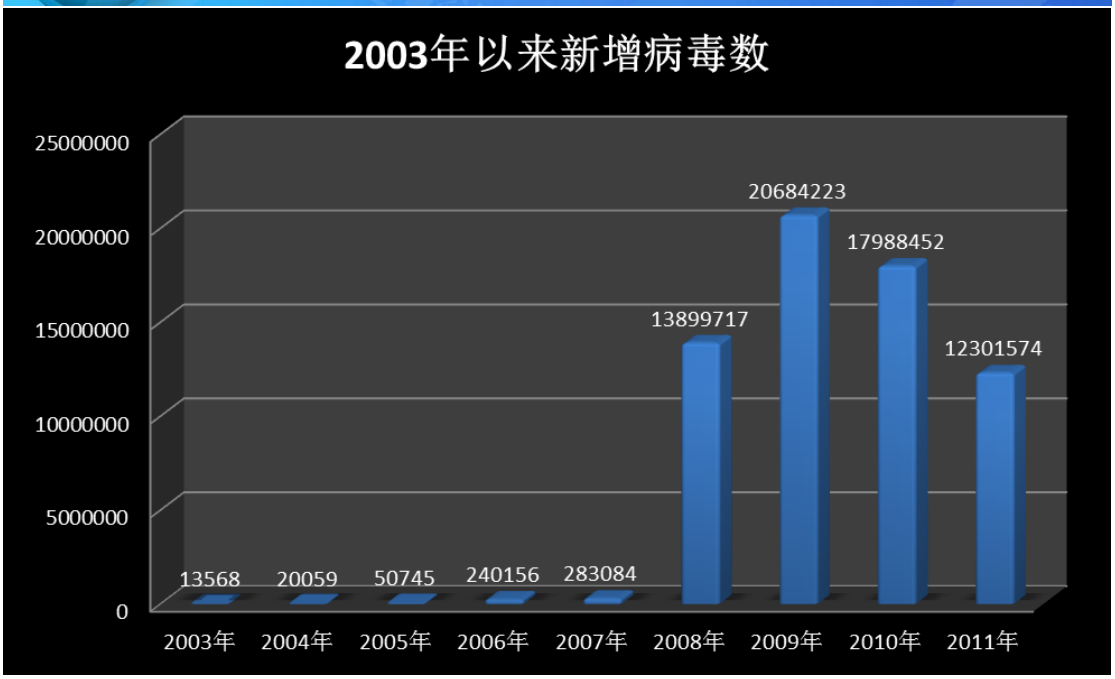

图 1 每年新增病毒数量统计（2003 年以来）

2) 沿海省份是病毒感染或网络攻击高发地区

按病毒感染次数统计，广东、江苏、浙江位列前三，这与相应地区互联网应用普及程度吻合。

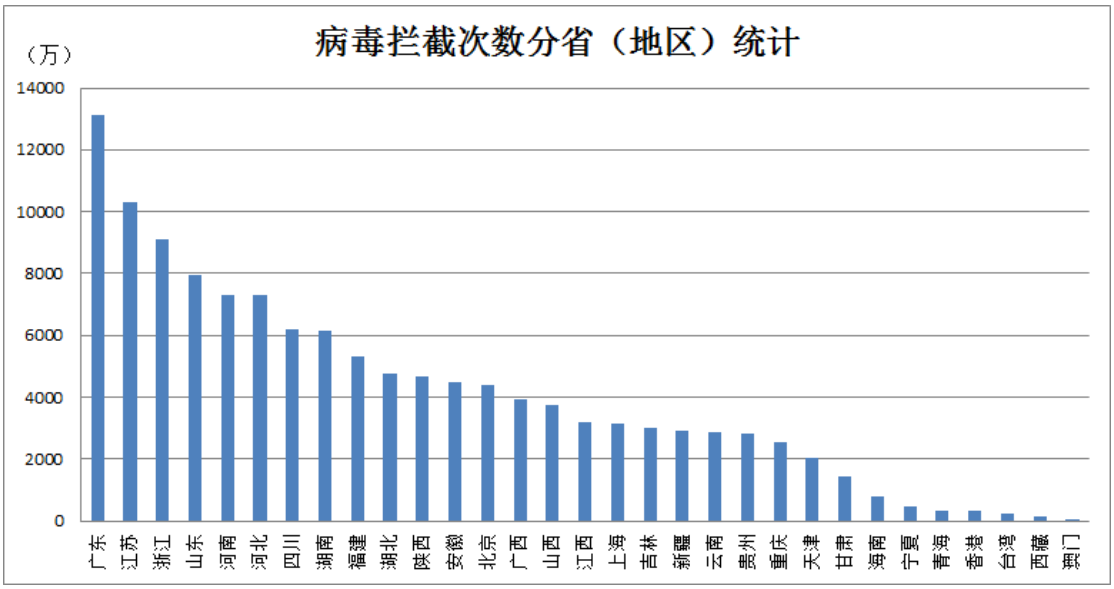

图 2 分省（地区）统计病毒拦截次数

金山毒霸 2012 中集成的防黑墙功能会记录攻击来源和攻击次数。结果发现位于江苏、浙江、上海、香港、广东、北京、山东、黑龙江共 8 个省市的攻击源占到总攻击次数的 75%。

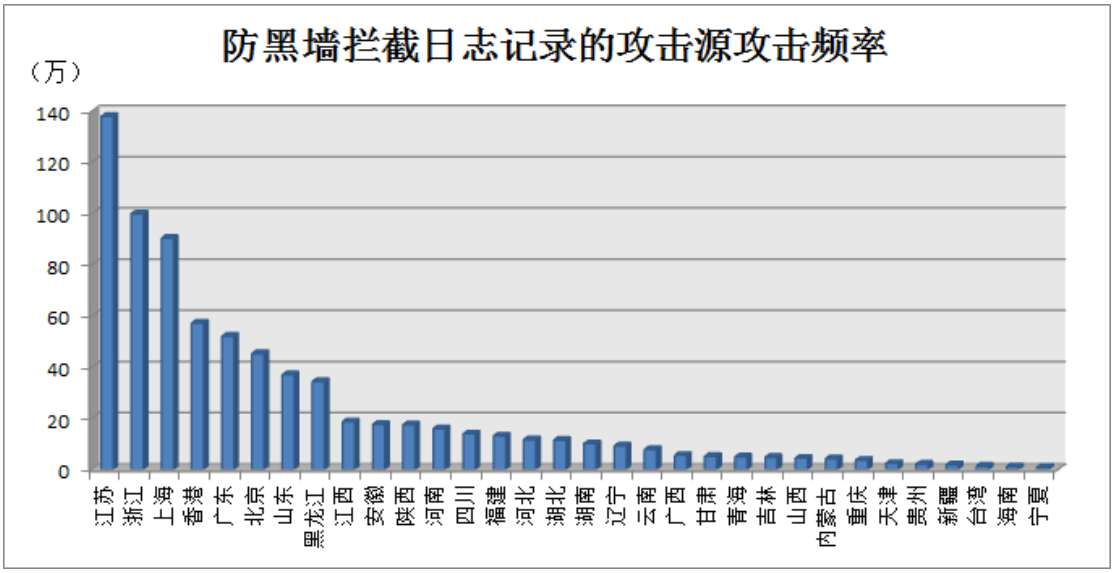

图 3 攻击频率统计（来源：防黑墙日志）

仔细分析攻击源 IP，发现有相当一部分位于 IDC 机房。表明，这些省份的服务器托管资源中有较多已被黑客控制，黑客使用这些系统对其他电脑发起攻击。

3) 金山毒霸保护用户免于病毒攻击的次数约 500 万次/天。

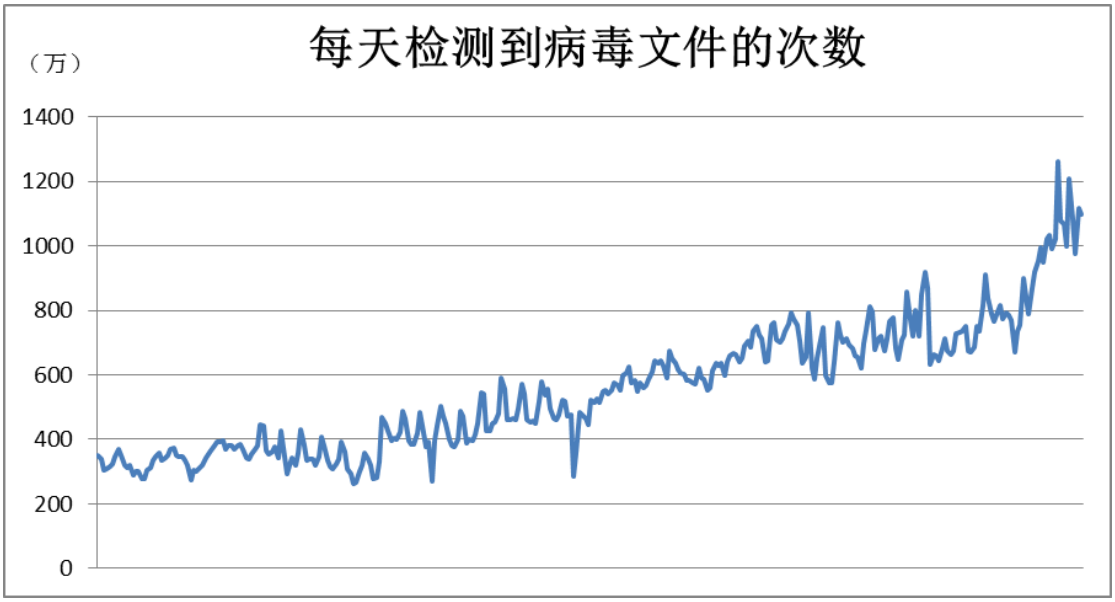

图 4 金山毒霸云安全系统日拦截次数

4) 每天检测到病毒的电脑占总数的 4~8%，每天检测的文件中，有 2~7‰带毒。

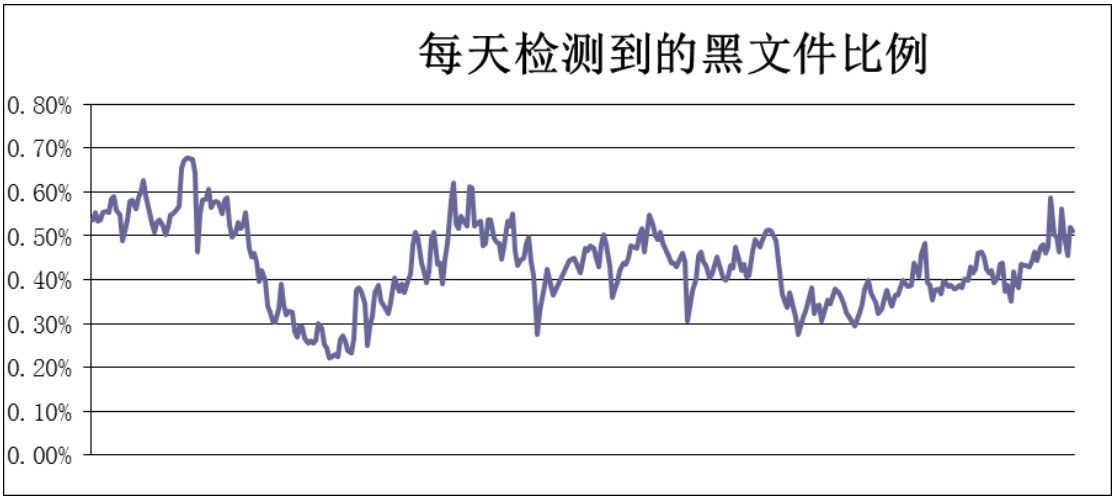

图 5 金山毒霸云安全系统日拦截黑文件的比例

每检测 1000 个文件有 2~7‰的概率发现病毒，若按电脑台数统计，则大大高于这个数字。下图显示，每天有 4%-8%的电脑上会发现病毒。

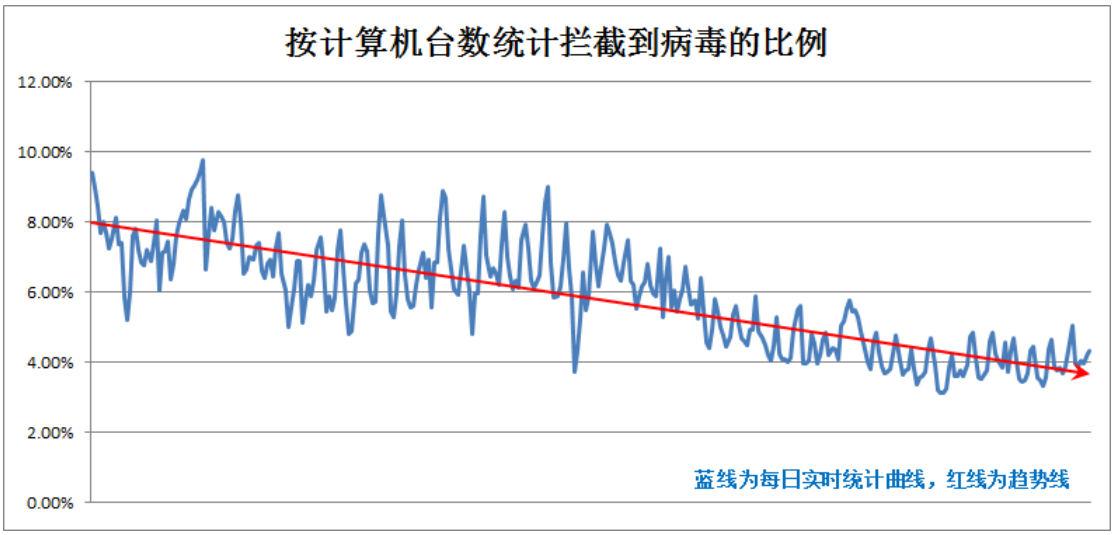

图 6 云安全系统统计数据（按感染病毒的电脑数量计）

2. Android 手机病毒感染数据

金山手机卫士云安全中心监控到 2011 全年安卓平台新增病毒数量 23681 个,受害用户 1037 万人。从每天的样本数统计来看，1 月份日均新增病毒 20 个，到 12 月份时，日均新增病毒数已突破 200 个，年末日均新增病毒数量比年初增长十倍。

对手机病毒种类进行统计，可以看出，恶意广告的比例增速最为迅猛，这与前几年流氓软件在电脑上泛滥的过程极其相似。

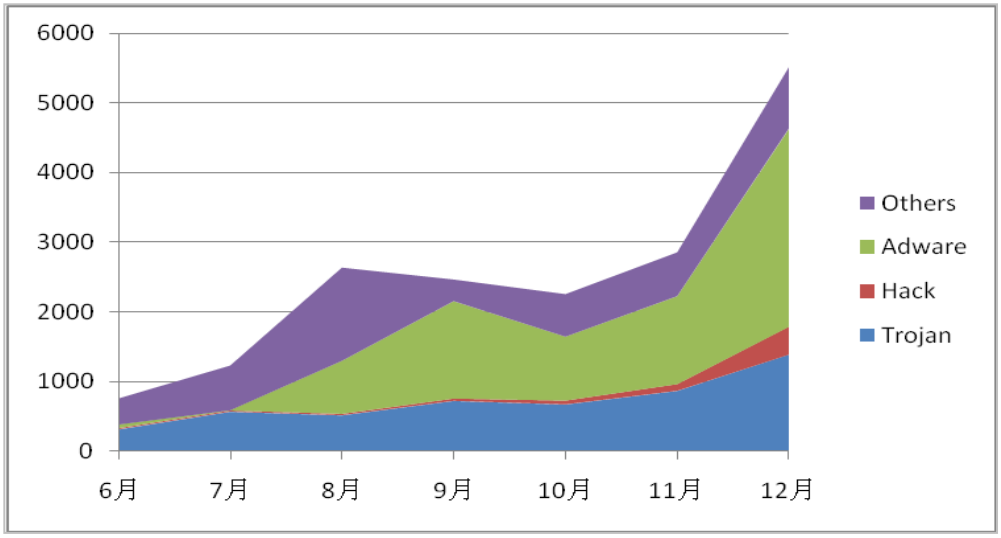

图 7　2011 年新增手机病毒分类统计

Trojan 泛指扣费木马、不包括带后门功能的一般病毒；

Hack 指后门病毒，包含一部分捆绑型黑客工具；

Adware 指恶意泄漏手机信息的广告程序；

Other 指捆绑木马程序及吸费后门的恶意软件。

扣费病毒、恶意监听软件、恶意广告软件占到手机病毒总量的 51%，在各类 Android 市场充斥着大量“打包党”篡改过的恶意应用，（注：打包党，就是将别人开发的 Android 软件拆包后植入恶意程序再继续分发渔利的组织或个人）。

按手机病毒的地区分布看，广东、北京、江苏、上海这四个省市感染量就占了总感染量的 80%。

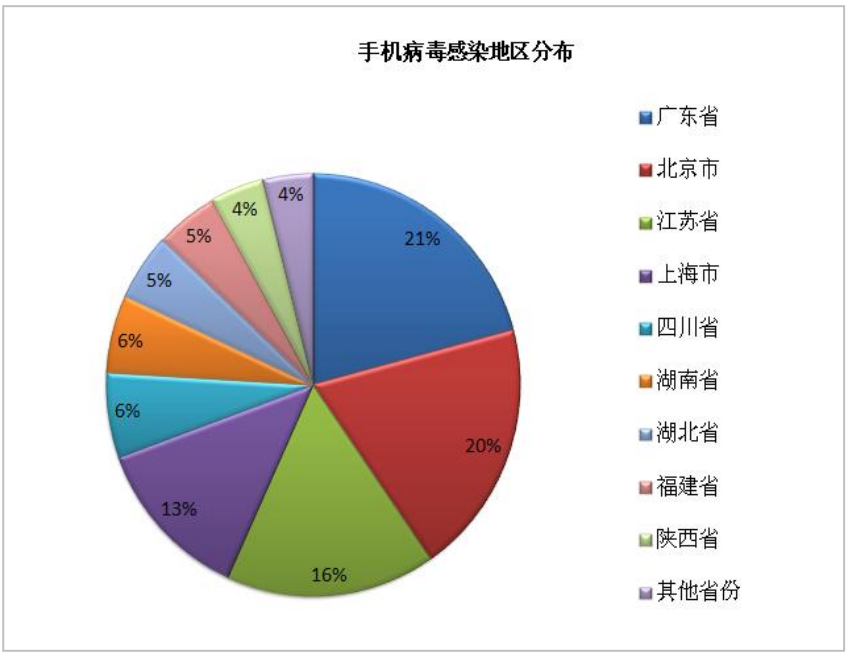

图 8 手机病毒感染情况地区分布

3. 钓鱼网站统计

1) 2011 年新增钓鱼网站在 45 万个左右，年底相比年初约增长了一倍。

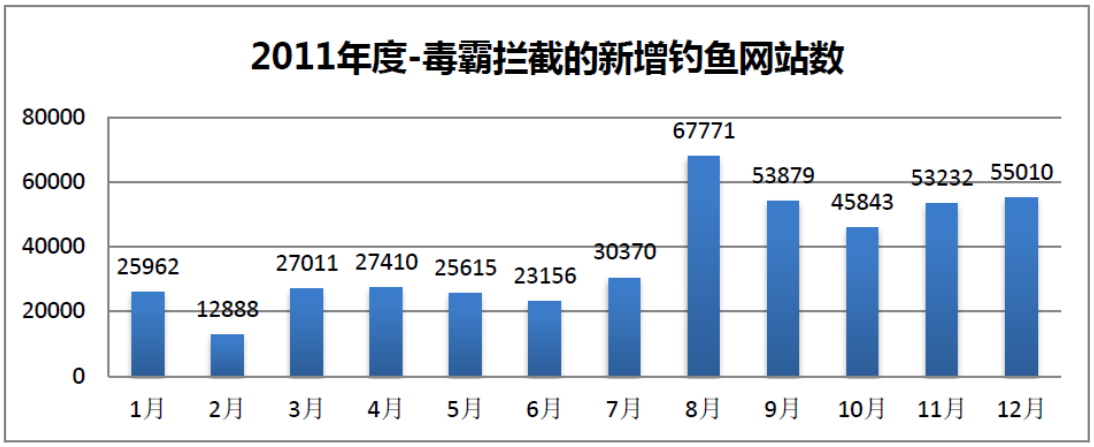

图 9 2011 年新增钓鱼网站数量

2) 每月钓鱼网站的拦截次数在 4 亿~11 亿之间，覆盖网民 4000 万至 7000 万人。这些网民访问到钓鱼网站的概率为 5~7%之间，差不多每浏览 14 个网页就有一次碰到钓鱼网站。

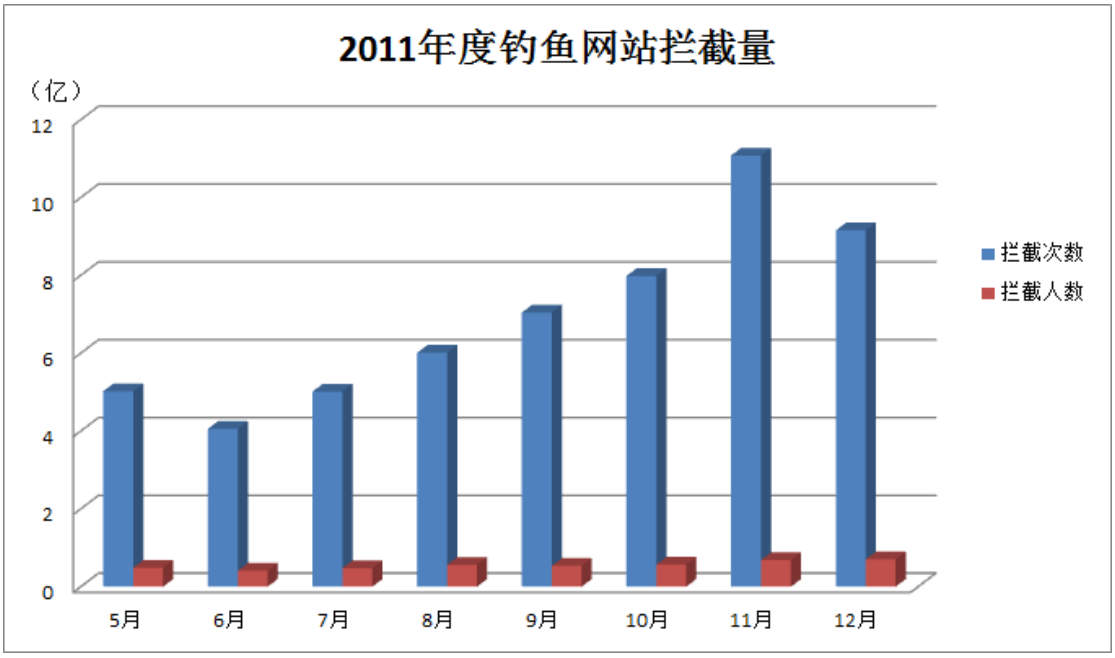

图 10 2011 年 5-12 月拦截到钓鱼网站的次数和人数统计

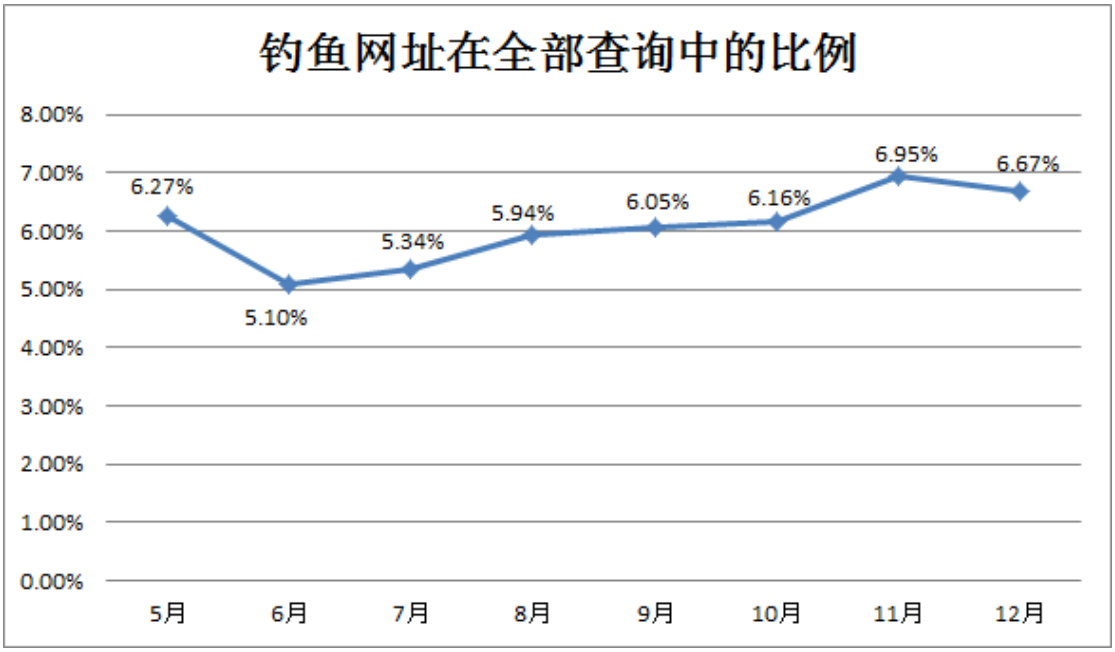

图 9　2011 年 5-12 月拦截的钓鱼网址占正常网址的比例

而在 2010 年，金山毒霸每个月拦截到的钓鱼网站数量，在最高峰的 11 月份，也只有 1000 万次。

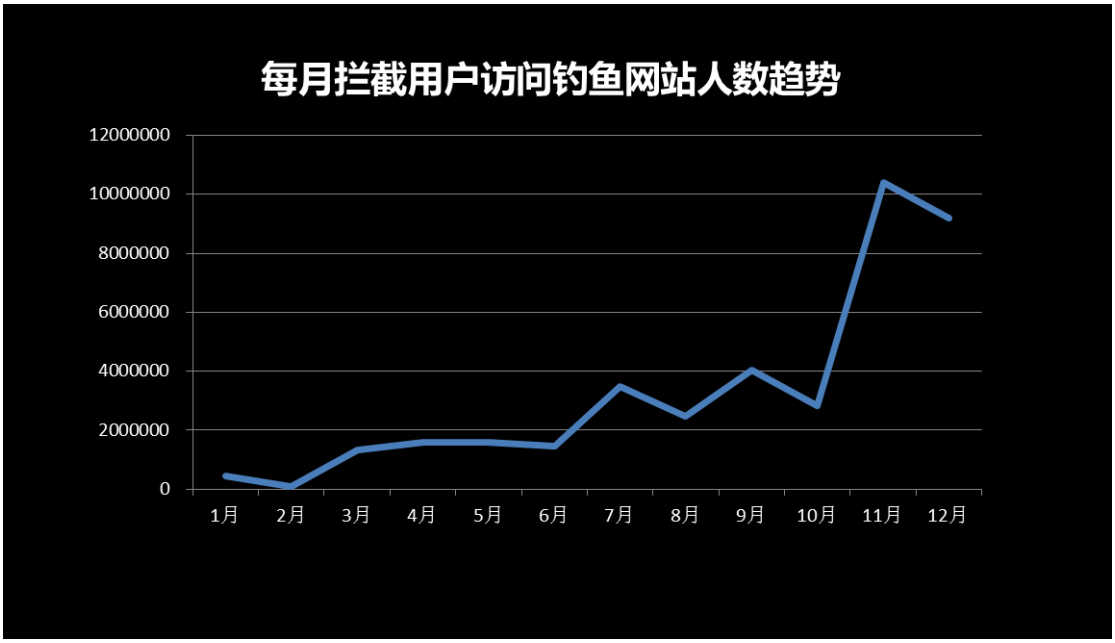

图 10　2010 年金山毒霸拦截钓鱼网站的次数

3)　淘宝网最受钓鱼网站制作者垂青

在 2011 年新增的钓鱼网站中，假淘宝独占鳌头，占总量的 28.21%，其次是各类中奖。

类型	网站数	占比
假淘宝	126417	28.21%
中奖	100140	22.35%
六合彩	36985	8.25%
彩票	26525	5.92%
博彩	20108	4.49%
网游交易	19265	4.30%
足彩	11903	2.66%
假证券	10572	2.36%
腾讯空间及安全中心	9499	2.12%
电视棒	6072	1.35%
监听器	4955	1.11%
兼职	3969	0.89%
办证	3891	0.87%
贷款	3450	0.77%
信用卡	3339	0.75%
QQ 刷钻	2897	0.65%
假药	2094	0.47%
其他	56063	12.51%

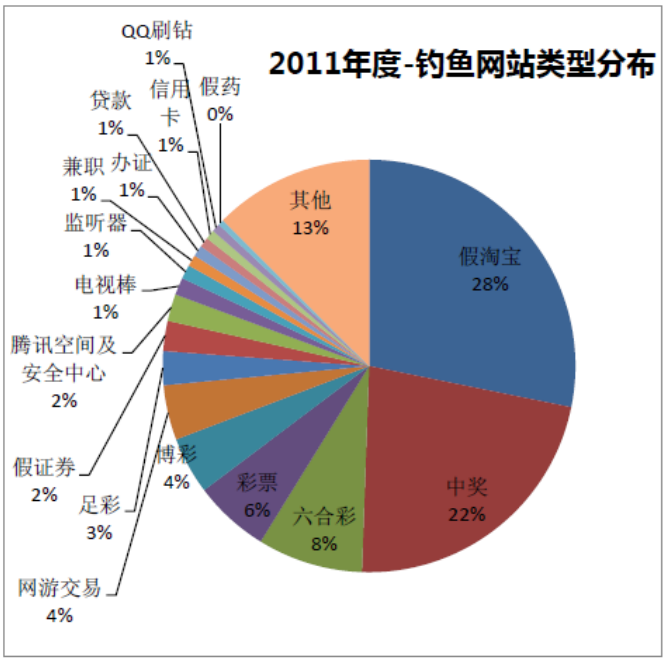

图 13　钓鱼网站类型统计

4)　81.82%的钓鱼网站服务器托管于国外，位于国内的不到 20%。

		总体	中奖	六合彩	网游交易	机票	话费
国外		81.82%	100.00%	97.59%	83.48%	30.23%	57.14%
国内	广东	18.18%		1.20%	4.35%	46.51%	28.57%
	浙江				6.96%	6.98%	
	广西				5.22%		
	天津					4.65%	
	北京					2.33%	3.57%
	江苏						3.57%
	台湾						3.57%
	上海					2.33%	3.57%
	福建			1.20%		2.33%	
	河南					2.33%	
	香港					2.33%	

图 14　钓鱼网站托管服务器分布

4. 网购相关统计

每天启动金山网购保镖的人数约 400 万~600 万，保护次数约 1400 万~2000 万。（见统计表）

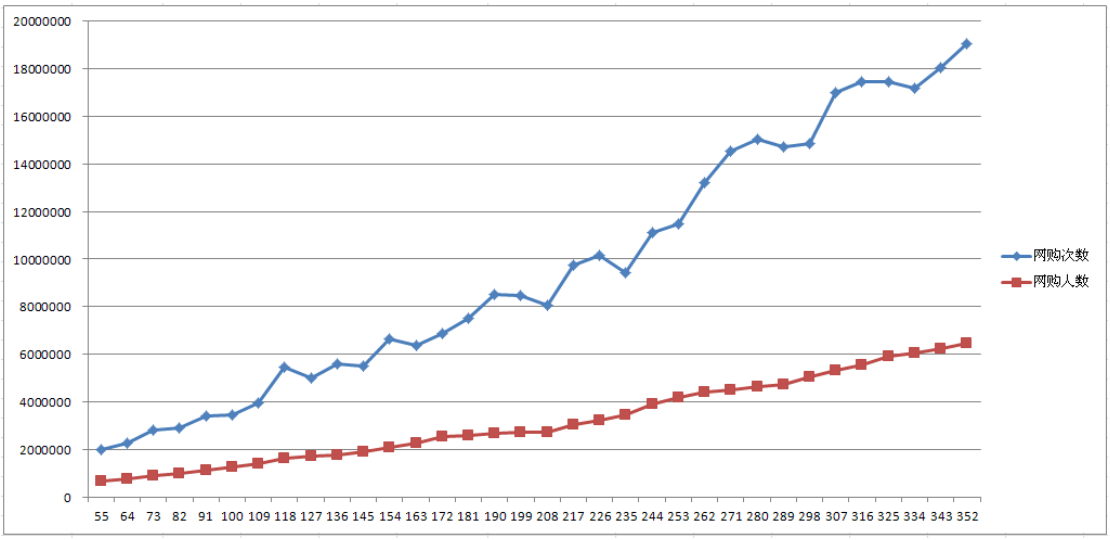

图 15　金山毒霸网购保镖保护次数和人数统计

据金山毒霸安全中心 2011 年中对 1000 余名网购被骗受害者专题调查，全国各地均有网民受害，近 7 成受害者被骗金额在 500 元以下。

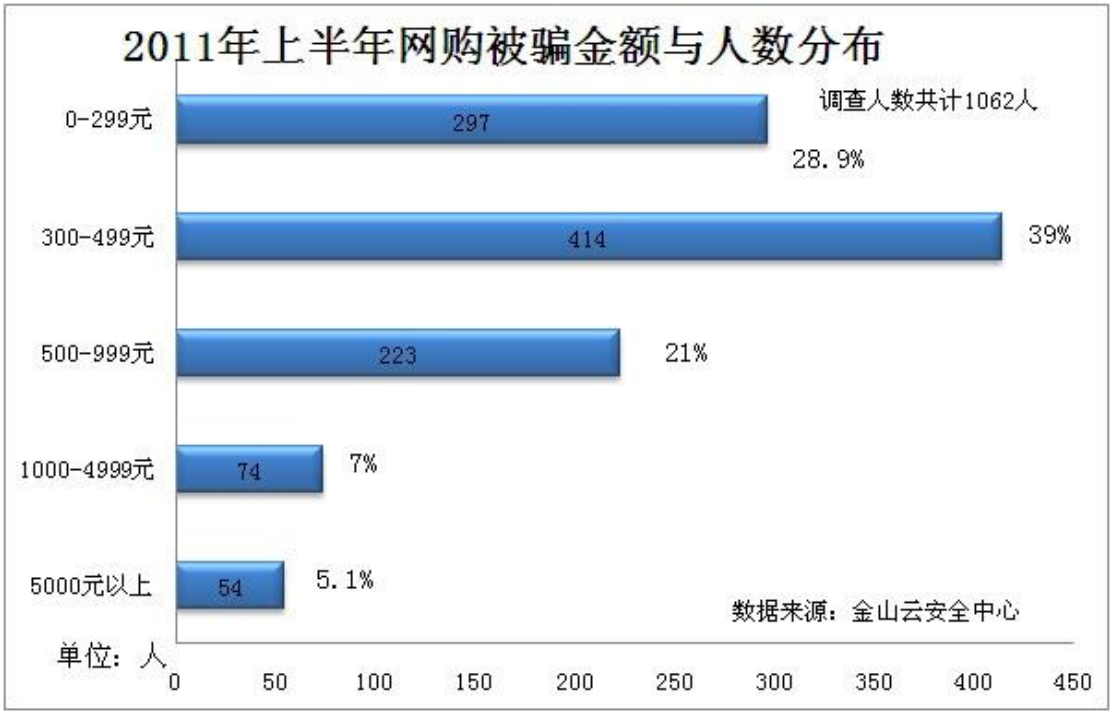

图 116 网购被骗、被盗的金额分布

在 2011 年上半年的网购安全专题调查中，统计受害者的被骗或被盗的入口，有 60%通过聊天工具发生。

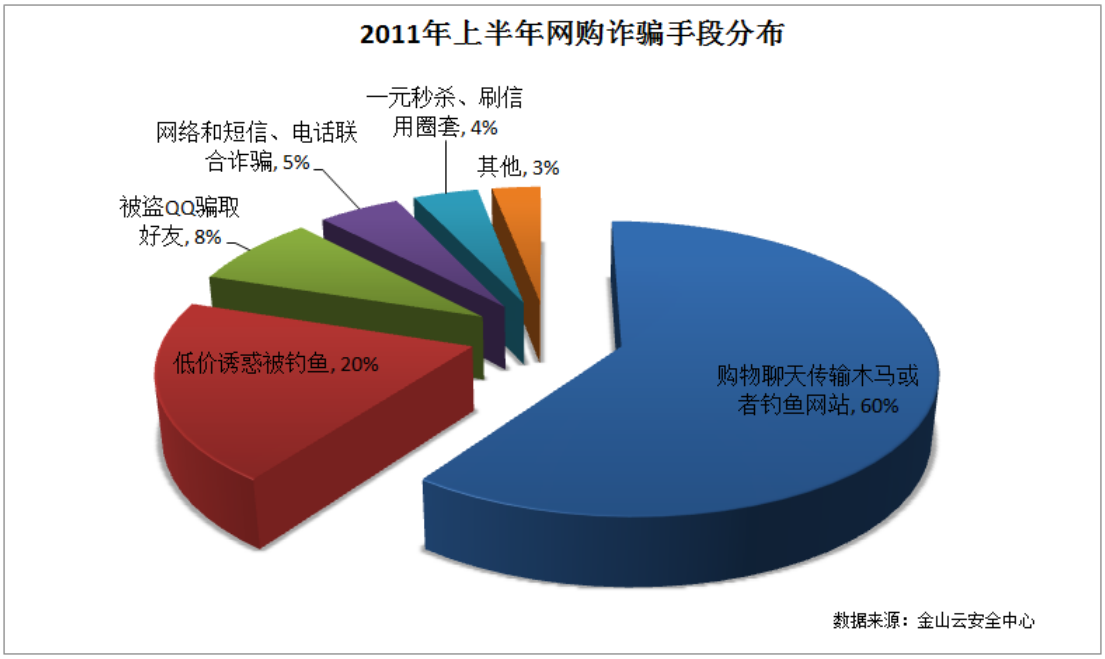

图 17　网购诈骗方式统计

第三章　2011 年度重大安全事件

1. 个人隐私非法泄露

2011 年末，中国公众经历了一次大规模个人信息泄露事件的洗礼，几乎人人自危。CSDN、天涯等众多互联网公司信息被公开下载，截至 12 月 29 日，CNCERT 通过公开渠道获得疑似泄露的数据库有 26 个，涉及帐号、密码 2.78 亿条。这些信息均为黑客攻击商业网站后窃取并泄露到公众面前，而黑客手中掌握的公众信息到底有多少，对公众还是个未知数。

公众熟悉的杀毒软件重点在保护用户端的电脑安全，客户端安全软件对于存储在运营商服务器上数据安全鞭长莫及。此案预示着未来会有更多的攻击针对服务器展开。

2. 网购木马抢劫案

2011 年 3 月，知名互联网交互设计专家“一叶千鸟”网购被骗 5 万余元。互联网行业老兵网上购物尚且被骗，普通网民在线购物面对猖獗的网购木马、钓鱼网站，已成待宰羔羊。

在大量同类案例中，许多受害者向警方报案时，却无法清晰描述受骗经过。大多数案件只骗几百元，甚至几十元。受害者投诉维权的成本太高，最后往往自认倒霉。到目前为

止，众多网购木马制造者仍未落网，网购木马变种仍然层出不穷。

3. 商业银行动态口令升级群发短信诈骗

2011 年 2 月农历春节前后，多家全国性的商业银行和地方城市银行客户遭遇大批量短信诈骗。骗子在短信中声称银行动态口令升级，请储户访问指定网站更新。许多储户信以为真，上网登录了这些网站。将自己的银行卡、手机号等信息提交，并随后还按网站提示的方法，把银行返回的验证码也一并交给骗子。结果导致大量储户资金被盗，损失数千元至数百万元不等。

4. 首个 QQ 群蠕虫被截获

QQ 号称有 5 亿以上的用户群，QQ 号已经成为事实上的网络通行证，QQ 群功能更是深受喜爱。2011 年 9 月，首个自动通过 QQ 群功能传播的蠕虫病毒被截获。该病毒伪装成电视棒破解程序欺骗网民下载，盗取魔兽、邮箱及社交网络账号。

中毒后病毒会自动访问 QQ 群共享空间，将病毒程序提交到群共享空间快速传播，病毒的最终目的是下载更多盗号木马，窃取虚拟财产。

该病毒独特的传播方式令安全研究人员吃惊，金山毒霸安全中心连夜和 QQ 安全中心协作，避免了大规模的蠕虫病毒传播。

5. 新浪微博遭遇 XSS 蠕虫攻击

2011 年 6 月 28 日晚 8 点，新浪微博突然遭遇蠕虫式的“病毒”攻击，众多加 V 认证的名人微博自动发布带攻击链接的私信或微博。后查明，这是攻击者利用新浪微博的 XSS（跨站）漏洞攻击，点击某个微博短址链接后，会自动加好友，自动发微博并同时传播攻击链接。结果在短短半小时左右，数万人受波及。幸运的是，攻击者事实上并无恶意，只是一次恶作剧，但 XSS 蠕虫攻击的威力已被公众领教。

6. “我的照片”QQ 病毒传播广泛

病毒传播者利用 QQ 聊天工具传送伪装成“我的照片”，接收方在打开美女照片的同时，后门程序运行。该木马主要用来盗取 QQ 号，和其他盗号木马不同，这些窃贼只是趁 QQ 号主人不在线时试图向 QQ 好友借钱购买虚拟点卡或代付购物，该病毒集团以骗取钱财为最终目的。

7. Android 手机恶意软件迅猛增长

随着 Android 手机以越来越快的速度被用户接受，寄生于 Android 操作系统的手机后

门程序渐渐高发。2011 年，金山毒霸手机安全中心就先后捕获了伪装成打地鼠游戏、老虎机游戏、美女拼图游戏的手机病毒，这些病毒的主要目的是偷偷定制扣费服务，盗打电话，窃取手机隐私信息，截取手机短信内容，监听手机通话录音和获取位置信息。手机恶意程序对智能手机用户的信息安全构成严重威胁。

8. 两高院通过办理计算机信息安全刑事案件司法解释

《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》于 2011 年 6 月 20 日通过。司法解释进一步明确了非法获取计算机信息系统数据，非法控制计算机信息系统相关的条款做了具体规定。新司法解释的出台，对保护计算机系统安全，限制非法入侵行为，阻止病毒产业链的漫延具有重要意义。

9. 淘宝客欺骗者病毒干扰淘宝店经营

“淘宝客欺骗者”病毒专门劫持淘宝网搜索结果。当用户在淘宝网搜索商品时，会自动跳转到淘宝客搜索推广站点。此后，任意交易卖家就要付出佣金，增加了网店经营成本，淘宝也会因此多支付佣金，而淘宝买家也因浏览器被强行劫持，只搜索到病毒想推广的商品而丧失了自由选择的权利。

10. 社交网站风生水起，安全威胁与之伴行

微博成为 2011 年最火热的网络应用，微博传播消息迅速快捷，成为钓鱼网站传播者的天堂。特别在 2011 年底出现大量网民个人信息被泄露之后，微博成为事件的重灾区，每天有数千乃至上万人的 ID 被盗，盗号者利用偷来的微博帐号发布大量商业广告或钓鱼网站链接。好在公众对中奖之类的钓鱼已经习以为常，微博帐号被盗后，再被骗钱的案例较少。

第四章 年度十大病毒

在追逐经济利益的时代，能给公众留下深刻印象的病毒木马已非常罕见。2011 年，病毒木马变得更隐蔽，病毒行为正在灰色化。恶性病毒在减少，惹人烦的骚扰型病毒却在增加。以下是 2011 年度十大病毒。

1.鬼影病毒

鬼影是 2010 年出现的可以感染硬盘主引导记录的病毒，该病毒甫一出现，就因成功直接在 Windows 下改写硬盘分区表而闻名。2011 年鬼影病毒升级了数个版本，其特点基本为改写硬盘主引导记录（MBR）释放驱动程序替换系统文件，干扰或阻止杀毒软件运行，恶意修改主页，下载多种盗号木马。

在最新出现的版本中，还会释放自己的驱动程序和杀毒软件对抗，阻止杀毒软件修复被改写的硬盘主引导记录（MBR）。2011 年 9 月，鬼影 4 代病毒（其他杀毒厂商称为 BMW 病毒），除了上述特征还可感染电脑特定型号的主板 BIOS 芯片，使病毒的清除更加困难。

2.QQ 群蠕虫病毒

QQ 群蠕虫病毒是 2011 年突然爆发的一种传播性很强的病毒，中毒电脑的 QQ 会自动转发群消息，是第一个可以利用 QQ 群共享来传播的蠕虫病毒。该病毒主要伪装成电视棒破解程序欺骗网民下载，盗取魔兽、邮箱及社交网络账号。

3.变形金刚盗号木马

变形金刚类病毒最初是在一个伪装外挂的网站上发现，病毒利用暴风影音加载 DLL 文件时不校验的漏洞使病毒文件得到运行机会。变形金刚病毒开创了利用正常软件间接加载病毒的先河，此后，这种手法被大量病毒作者复制。中毒电脑会随机不定时弹出网页广告，变形金刚感染了超过 16 万台电脑。

4.输入法盗号木马

2011 年输入法盗号木马病毒释放的 mgtxxx.ocx 文件拦截量曾经居高不下，病毒还推广较多的互联网软件赚取推广费，病毒的主要目的是盗取游戏账号。该病毒最大的特点是注入注入输入法程序，当用户按 ctrl+shift 切换输入法时，会激活病毒程序。

5.QQ 假面病毒

这类病毒是由易语言编写，利用“我的自拍”“美女图片”做诱饵盗取 QQ 账号。该病毒制造了一个透明的按钮贴在 QQ 登录按钮上。强迫中毒电脑 QQ 下线，逼迫用户手动输入 QQ 密码后点击登录。该病毒强大的迷惑性感染了数十万台电脑。

6.空格幽灵病毒

该病毒是一个仿图片的病毒，实质是一个远程控制程序。用户一旦打开查看此“图片”，远控程序就会在计算机后台悄然运行，为黑客打开便利之门。黑客可以像控制自己电脑一样控制中毒电脑，这可能会导致用户隐私信息泄漏和虚拟财产被盗，甚至黑客可以利用其组建僵尸网络，对目标计算机进行攻击。这个病毒的特点是使用空格键为启动快捷键，每按一次空格，就激活病毒程序运行，空格幽灵由此得名。

7.DNF（地下城与勇士）假面病毒

DNF 假面类病毒也是通过伪游戏外挂网站传播的，其最主要目的是盗取网络游戏 DNF（地下城与勇士）账号。病毒巧妙地修改了网络相关的系统组件，当用户开机拨号连网或运行任何有访问网络行为的程序时，比如访问网络邻居时，病毒就被触发。

8.淘宝客劫持木马

淘宝客劫持木马是指劫持浏览器访问淘宝网、淘宝商城到淘宝客页面的一类木马病毒。这类病毒是通过推广淘宝客导致商家成本上升佣金被吸走。淘宝客病毒在2011年严重感染，对淘宝的正常经营构成较严重影响，许多店主表示佣金花冤枉了，不得已只能放弃淘宝客这种推广方式。

9.新型 QQ 大盗

这类病毒通过成人网站的专用播放器传播，感染后，会在后台下载更多木马和流氓软件，窃取用户信息。该病毒窃取 QQ 号的方法比较独特，病毒的主要目标是 Q 币余额不为 0 的帐号。对没有 Q 币的帐号，虽然也可顺手偷走，但病毒作者并未将这些 QQ 号的登录信息发往远程服务器。

10.网购木马

网购木马在 2011 年全年都很活跃，从发现它的第一天到现在，版本一直在更新，手法一直在变换。有多个网购木马成功突破安全软件的防御，甚至有网购木马还会直接推荐安装某安全浏览器，因为只有在网民使用这种浏览器购物时，病毒才会偷窃成功。

网购木马伴随2010年网购爆发增长而激增，2011年前2个月，平均每月增加新变种近3000个。

第五章　流行病毒的破坏现象

在恶意软件的构成中，木马（troj）类（含木马下载器）占据绝对主流，蠕虫病毒、宏病毒、感染型病毒的数量在恶意软件总数中的占比持续减少。

2011 年，病毒感染之后破坏系统的情况进一步减少，病毒导致系统崩溃或者变卡、变慢的情况也在减少，部分原因是计算机硬件性能提升，多核 CPU 正在普及，病毒木马即使耗光一个核心的资源，剩余的系统资源也基本不影响正常功能的运行。

在这种情况下，木马得以有更多机会在中毒电脑隐藏而不被发现。2011 年病毒比较典型的现象有：

1) 浏览器设置被强行篡改：如浏览器主页强行被设定为某个网址导航站，收藏夹中被加入若干网址，手动修改无效。桌面生成商业网站的访问链接，无法轻易删除。浏览器弹出广告，经常访问钓鱼网站。
2) 莫名其妙被安装了较多软件。
3) 在线购物时被骗钱，网银明明显示扣款成功，交易系统却显示未付款。
4) QQ 或 MSN 被盗后出现异常登录，朋友声称自己的 QQ 号或 MSN 自动发出消息，或者被人冒充向好友借钱，或向聊天群组上传带毒附件。
5) 游戏帐号或装备被盗。
6) 其他不易被网民主观察觉且更为严重的影响：电脑被远程控制、个人资料被泄露。

第六章　病毒传播渠道分析

2011 年，病毒木马传播更加依赖互联网通道，利用浏览器及相关组件漏洞挂马攻击的情况虽仍然存在，但由于浏览器自身漏洞的修补越来越及时，网页防护工具越来越有效，挂马攻击的成功率变得很低。

杀毒软件还普遍加强了对 U 盘病毒的防护和查杀，使得 U 盘传播病毒的情况也有所下降，病毒木马更多的使用了网络下载和即时通信工具传播。

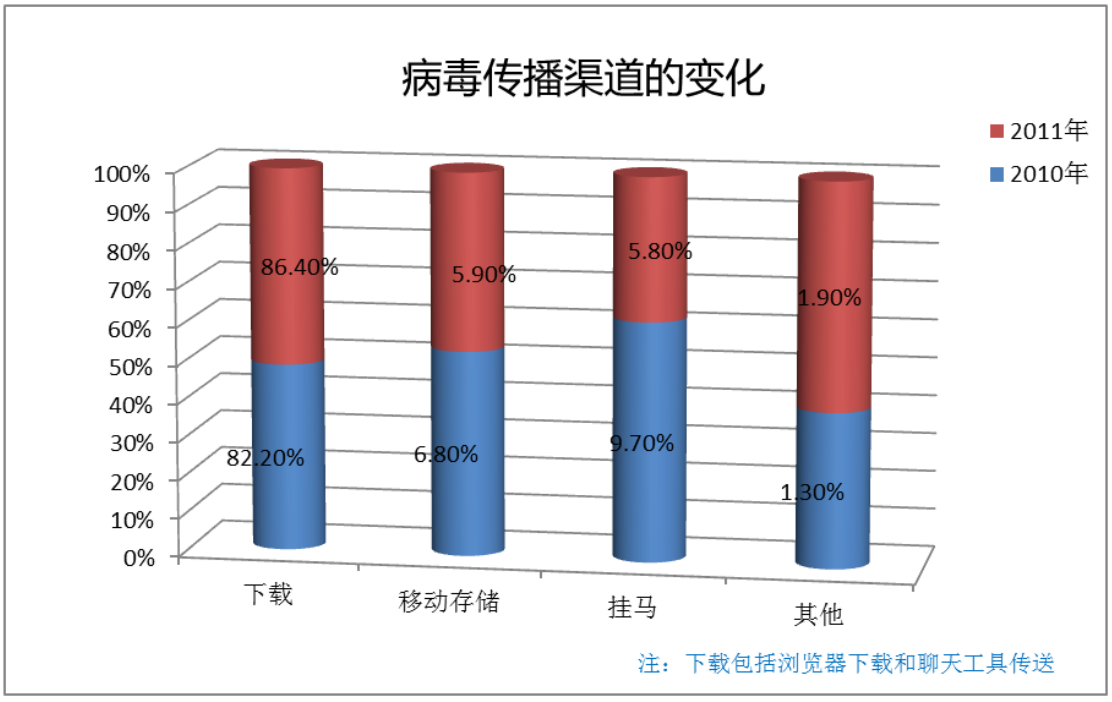

图 12 病毒传播渠道的变化

鉴于下载是病毒传播的主渠道，金山毒霸 2012 中特别强化了边界防御功能。在使用浏览器下载或聊天时接收文件带毒的比例在 6%-10%之间，这是一个相当庞大且危险的数据：意味着，每下载 10 个软件，就可能遇到一个文件带毒。

在杀毒软件不断针对下载渠道改进防御系统的情况下，下载传毒也变得不那么容易了。

观察发现从年初到目前，下载保护拦截到病毒的概率正在缓慢下降。

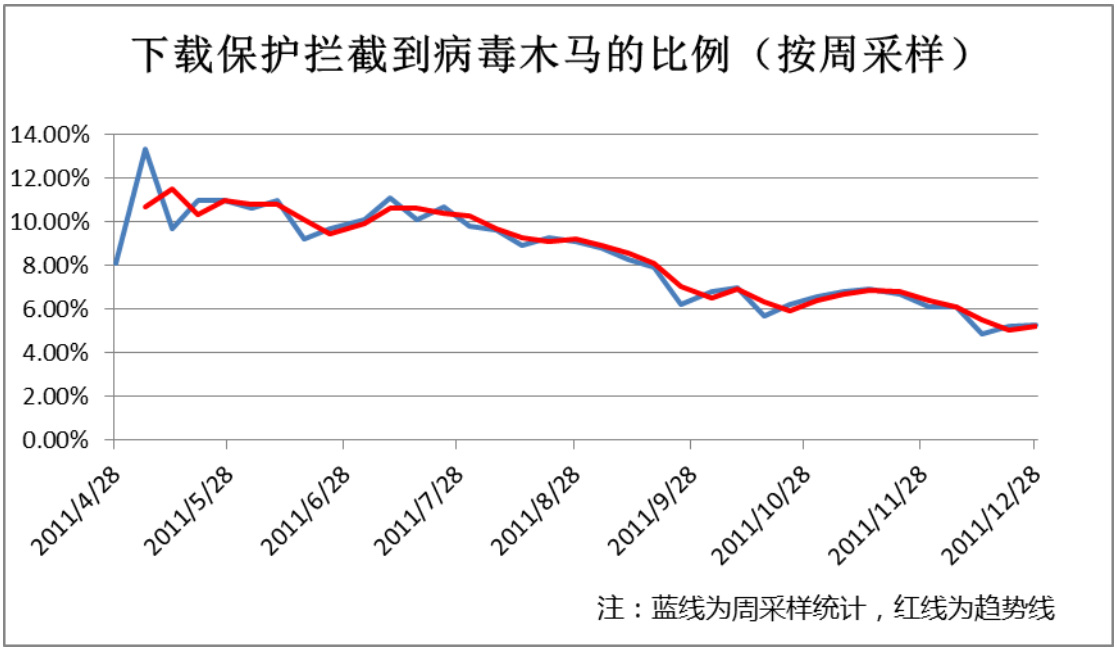

图 19　下载保护拦截到病毒的概率约占下载总量的 8%左右

盗版视频、成人视频网站在病毒传播中起着举足轻重的作用。杀毒软件一般作法是拦截带毒播放器的运行，结果有大约 20%的网民选择关闭杀毒软件后，继续下载带毒播放器。金山毒霸 2012 采用安全看片功能，来隔离病毒运行，该功能推出后大大降低了看片中毒的概率。

统计结果：访问视频网站安装带毒播放器的平均超过 2 万次每天，按提示进入安全看片的超过 1.5 万次，有 4000 余次会选择关闭网页拒绝带毒播放器，坚持下载带毒播放器的下降到数百次。

第七章　新威胁

1. 服务器成为重点攻击目标

2011 年底自 CSDN 被暴库以后各大网站纷纷被“脱裤”，用户的账号密码瞬间暴露出来，相对单个的计算机来说，服务器就是一个宝库。在客户端防御越来越严密时，服务器可能会被列入重点攻击目标。

2011 年底有关隐私泄露的话题引发长达一个月的讨论，之前只在小圈子流传的公众数据一夜之间暴露在公众面前，网民安全感顿失。互联网还值得信任吗？

金山毒霸官方微博对此做了简单调查，调查网民对最常使用的 20 种互联网服务做信任投票，选择心目中最信任的五个互联网服务。这个小调查用来观察网民对常见的互联网服务的信心指数，截止 2 月 9 日，该活动共吸引了 8370 名网民参与。

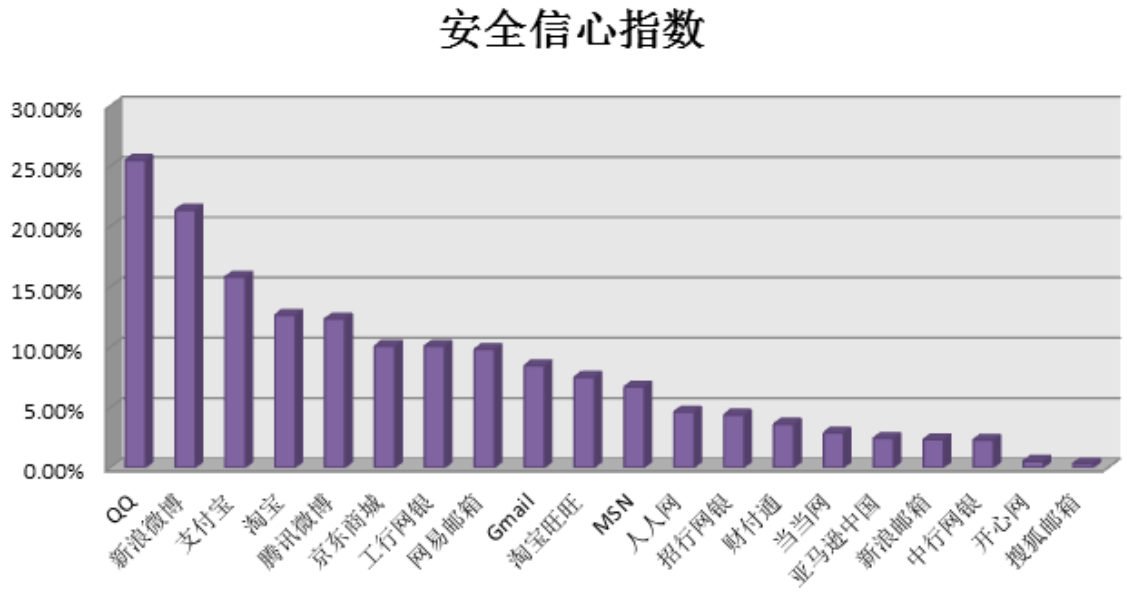

图 13　网民对互联网服务的信心指数

面对黑客从客户端到服务器的全方位威胁，网民需要更加完善的从客户端到服务器的全方位安全服务。希望网络服务除了常规的口令验证之外，还能提供手机验证；发现异常登录时，及时提醒；必要时，可暂时锁定服务；希望所有网络服务都能加密存储、传输用户提交的数据，阻止未经授权的访问，防止数据被监听。从而让更多的互联网服务给网民以安全感。

2. 骗术仍将层出不穷

金山毒霸安全中心在分析病毒传播规律时发现，一些早已可以查杀的病毒总在不断造成较多的感染。在联系过用户之后得知，很多情况下用户明明知道程序有风险（杀毒软件已经报告了），但为了使用这些软件，用户会按那些网站的提示关闭杀毒软件，再运行危险程序。杀毒厂商需要克服这些利用社会工程学欺骗来传播病毒的问题。

3. 病毒灰色化

2012 年，病毒产业追逐经济利益的趋势不会改变，但随着监管部门打击力度的加大，以及杀毒软件云安全体系的防护，我们看到大量病毒正在趋于灰色化：即破坏性越来越不明显，比如锁定主页，添加浏览器书签和推广互联网软件。中毒用户在清除失败时，会觉得破坏并不严重，而对病毒采取姑息态度。有些商业公司为了更快速的推广自己的软件，默许这种恶意推广行为的存在。

病毒和钓鱼网站勾结的情况将会增加，我们已经观察到某些病毒感染后，会篡改 DNS 解析，当用户访问正常网站时，会由于域名解析错误，用户会访问到一个钓鱼网站。

4. 针对移动互联网的攻击会更加剧烈

采用塞班操作系统的手机正在迅速被 Android 系统取代，国内 Android 市场管理又相对宽松混乱。高性能智能手机在移动互联网的使用体验和 PC 没有本质差异。攻击手机系统可以获得非常直接的经济收益，预计原来基于 PC 互联网的攻击者会逐步向手机平台转移，首当其冲的就是迅速普及的 Android 操作系统。