2012 年

中国互联网安全报告

360 互联网安全中心

2013 年 2 月 25 日

摘　　要

- 360 安全中心 2012 年截获新增木马病毒等恶意程序样本 13.7 亿个（以 MD5 计算），拦截恶意程序攻击 415.8 亿次，恶意程序增速较以往明显放缓；
- URL 欺诈，网盘、聊天群等文件分享在木马传播渠道中的比例持续提高，以 Game456、飞五游戏等为代表的在线棋牌游戏则成为木马产业链的主攻对象；
- 0day 漏洞仍然层出不穷，但主要被黑客利用在 APT（高级持续性威胁）攻击中，以高价值情报作为目标，对普通网民并未造成大范围影响。与此同时，Adobe、Java 等第三方漏洞受攻击情况超过微软漏洞；
- 360 安全中心“恶意网址库”发现新增钓鱼网站 87.3 万个（以 Host 计算），较 2011 年增长 73.9%；360 安全浏览器和网盾对钓鱼网站拦截量达到 81.0 亿次，较 2011 年增长了 273.3%，是同期挂马网页拦截量的近 200 倍；
- 企业安全市场掀起免费潮，永久免费的 360 企业版终端用户数突破 1000 万；
- 根据 360 网站安全检测评估，75.6%的国内网站存在高危漏洞，政府网站、高校网站以及网络论坛的安全性成为短板，网站拖库、篡改以及植入黑链 SEO 的危害进一步凸显，网站安全问题相比个人电脑安全形势更加严峻。

目　　录

第一章　木马病毒威胁明显降低

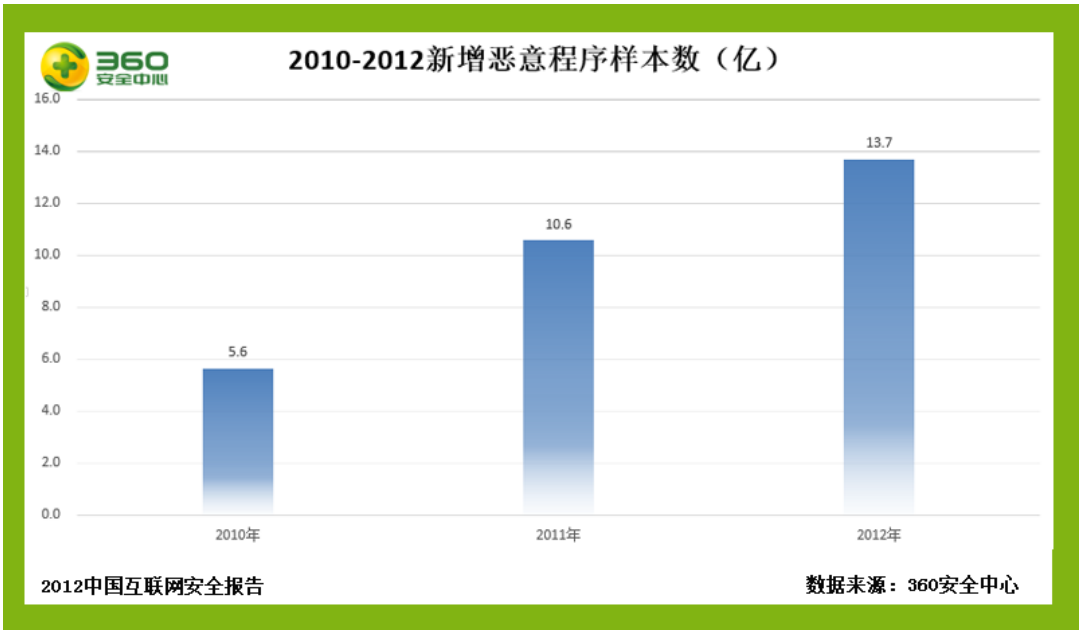
随着网络交易的日渐繁荣，恶意程序逐渐呈现出面向高价值目标的精准化攻击趋势，木马病毒的自动批量变形和更新越来越普遍。不过，这些被批量制作的恶意程序大多属于原有病毒家族的简单变种，新种类病毒的出现并不常见。

同时由于安全软件的快速普及，木马疫情已经得到了有效的控制。截至 2012 年底，中国网民个人电脑安全软件普及率已达 99.1%，中国进入全民网络安全化时代。其中，超过 97%的国内用户选择使用免费的国产安全软件，安全软件的免费化和国产化已成定局。

在与安全软件的攻防斗争中，木马病毒也逐渐出现一些新的技术特点和传播方式，最典型的是利用合法程序组装加载木马（安全行业说法称之为“白加灰”），此外，网盘等文件分享服务也被木马病毒利用作为新兴的传播渠道。

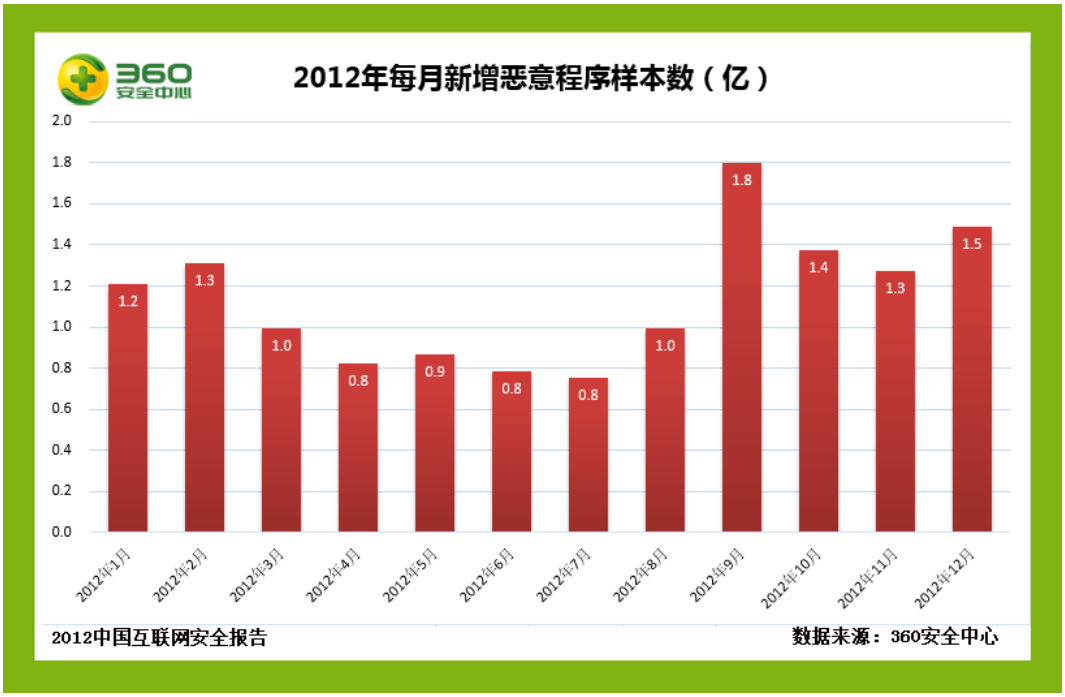
一、　恶意程序增速明显放缓

2012 年，360 安全中心共截获新增恶意程序样本 13.7 亿个（以 MD5 计算），较 2011 年增加 29.7%；360 安全软件拦截恶意程序攻击 415.8 亿次，较 2011 年增加了 76.1%。下图给了出了 360 安全中心最近 3 年截获的新增恶意程序样本数的年度统计情况。



从图中可以看出，2011 年的新增恶意程序样本数较 2010 年增加了约 5 亿个，增幅高达 89.3%，而 2012 年的新增恶意程序样本数较 2011 年仅增加了 3.1 亿个，增幅缩小到 29.2%。无论从增长的绝对值还是涨幅来看，恶意程序样本数的增速都在明显放缓。

下图是 360 安全中心 2012 年截获的新增恶意程序样本数的月度统计。2012 年新增恶意程序样本数在上半年呈现下降态势，但随着暑假期间网民游戏、娱乐活动的增多，木马活跃度也随之反弹，并在 9 月达到年度最高值。另据 360 安全软件对恶意程序的拦截量和查杀量对比统计，木马病毒攻击感染率已经下降至千分之三以内。



二、 木马攻击更加精准和隐蔽

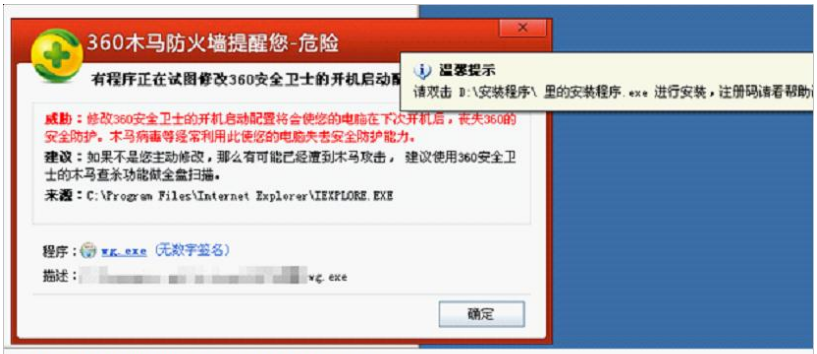
从 2012 年的监测分析来看，恶意程序的制作者更倾向于选择互联网上的“高危人群”或更具商业价值的目标群体进行有针对性的攻击。同时，恶意程序与安全软件之间的攻防对抗也在不断加强，顽固化和隐蔽化木马病毒不断出现。

1） 精准化攻击瞄准高危人群

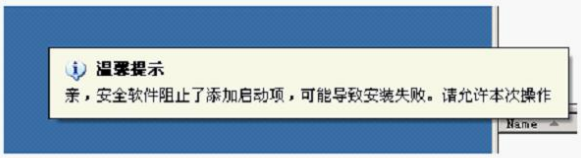
所谓互联网上的高危人群，是指那些为了特别的兴趣爱好，经常不顾安全软件的风险提示，宁愿感染病毒也要冒险运行恶意程序的特定人群。此类人群主要集中在游戏外挂玩家、色情视频浏览者、破解软件下载者和一些过度追求低价商品的网购用户中。2012 年发现的多个典型的木马都是针对上述高危人群。

例如，伪装 Game456 游戏客户端的盗号木马在 2012 年活跃度相对较高。2012 年，犯罪份子陶某利用豪华酒店局域网传播捆绑有远控木马的 Game456 游戏客户端，专门针对的就是入驻豪华酒店的高收入人群，从而能够轻易在游戏赌局中赚得利益，通过赢得游戏币非法获利 1500 多万元，最终因触犯非法控制计算机信息系统罪，被云和县人民法院判处有期徒刑 6 年。

在网购交易威胁中，360 安全中心于 2012 年 12 月截获了一款名为“支付大盗”的木马程序。“支付大盗”通过搜索引擎竞价排名传播，运行后会潜伏在系统后台，实时监视浏览器地址栏。一旦受害者在淘宝等购物网站为商品付款，木马就会篡改交易数据，将付款对象转换为黑客的“洗钱账户”，使受害者花了钱却收不到商品。从受害用户的反馈来看，此类木马病毒的技术水平通常并不是高明到无法被安全软件检出，而是通过诱导性提示，先要求用户关闭安全软件，之后再感染用户电脑，或者选择网吧、酒店等安全防护薄弱的电脑“下手”。事实上，经常冒险进行高危操作的用户正是木马病毒热衷攻击的对象。



360木马防火墙拦截“卖萌”木马的攻击行为



木马遭安全软件拦截后弹窗欺骗用户选择允许

2） APT 攻击瞄准高价值情报信息

APT（Advanced Persistent Threat）攻击是指针对特定组织或目标进行的高级持续性渗透攻击，是多方位的系统攻击。极光行动、夜龙攻击、震网病毒（超级工厂病毒）、暗鼠行动等都是 APT 攻击的著名案例。

与前述的精准化攻击有所不同，APT 攻击的目标不是高危人群，而是具有较高攻击价值的个人或组织，如明星、企业、政府、军队等。APT 攻击往往是通过多个步骤，多个间接目标和多种辅助手段最终实现对特定目标的攻击，而且经常结合各种社会工程学手段。APT 攻击是一种比较专业的互联网间谍行为，某些 APT 攻击往往会持续数年才被发现曝光。

从技术角度看，APT 攻击一般会利用 0day 漏洞隐蔽植入木马程序以实现网络攻击。所谓 0day 漏洞，是指已经被外界（黑客）发现，但软件厂家尚未发布补丁的安全漏洞。发现 0day 漏洞有一定的难度，但利用 0day 漏洞进行攻击，往往使攻击对象防不胜防。随着软件发布更新的日益频繁和免费安全软件的防护普及，通过已知漏洞传播木马程序很容易被拦截，于是，APT 攻击就经常选择 0day 漏洞为载体。几乎每次 APT 攻击案例出现时，都会伴随着一个或多个 0day 漏洞的暴露。

2012 年最为著名的 APT 攻击当属火焰病毒。该病毒可能是有史以来最复杂的病毒之一，病毒文件达到 20MB 之巨。该病毒利用微软的数字签名漏洞骗过验证系统，使其看起来像是由微软发布的软件，因此突破了众多杀毒软件的拦截。“火焰”病毒的攻击对象主要是伊朗等中东地区的电脑，国内没有出现大规模感染迹象。

3） 通过感染 MBR 等手段顽固驻留系统

一旦感染就难以清除，也成为 2012 年木马病毒技术的一个重要特点。360 安全专家在查杀分析过程中发现，某些木马病毒一旦入侵用户电脑，就会通过阻止安全软件对特定区域的扫描和校验，阻止安全软件运行或开启防护功能，甚至是直接将安全软件卸载等方式，使用户无法将其有效和彻底的清除。

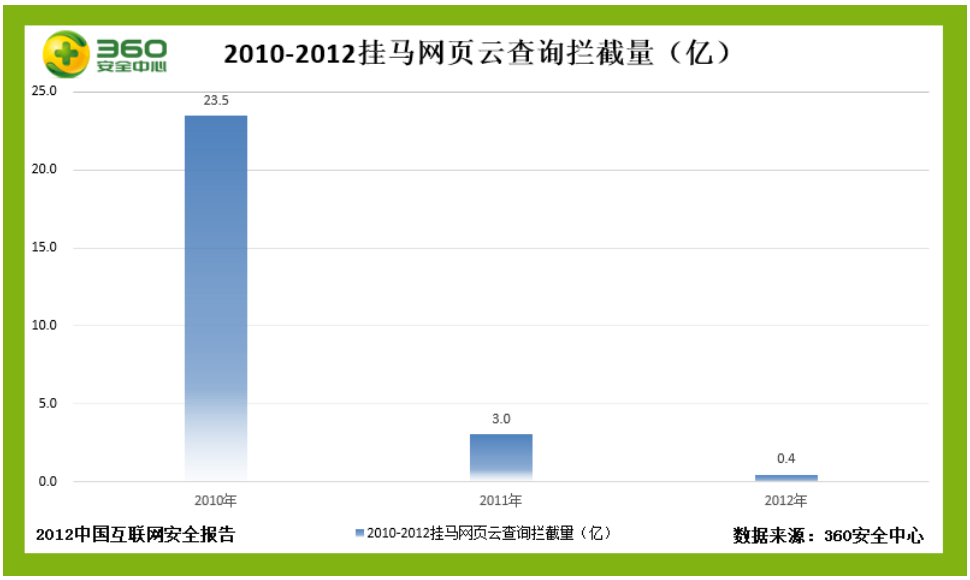
2012 年，最为顽固和难以清除的木马类型仍然是 MBR 病毒，包括鬼影系列、TDL4 系列和 BMW 病毒等。与一般的木马不同，这类木马会入侵电脑的主引导扇区（MBR）或 BIOS 之中，从而实现开机启动并获得高级系统权限的目的。2012 年新截获的 MBR 病毒变种还增

加了很多伪装、隐蔽和自我保护技术。

一般而言，具备“主动防御”功能的安全软件可以通过拦截应用层对 MBR 区域的写操作，阻止恶意驱动的加载，从而实现对 MBR 病毒的有效防御。不过，如果用户手动解除了安全软件的防御并强制运行了 MBR 病毒程序，那么清除起来就非常复杂，需要配合类似“360 系统急救箱”等工具才能彻底查杀。

三、 网络存储和共享成为木马新兴渠道

自 2010 年以后，安全浏览器的普及程度大幅提高，配合安全软件的共同使用，挂马网页的攻击成功率急剧下降。从图中可以看出，360 安全中心在 2011 年对挂马网页的拦截量为 2010 年的 12.9%，而 2012 年又仅为 2011 年的 14.0%。从这组统计数字来看，网页挂马对大众网民的危害已经日益减弱。



相应的，以云存储为代表的网络存储和共享服务开始被黑客利用藏毒传毒。2012 年，网盘服务流行度不断提升，娱乐、办公等用户间通过网盘分享文件愈发便利，一些黑客攻击者也开始将木马病毒伪装为热门网络资源，以分享网盘文件链接的方式进行传播。尤其是在微博等社交平台上，此类木马传播方式已相当普遍，值得用户高度警惕。

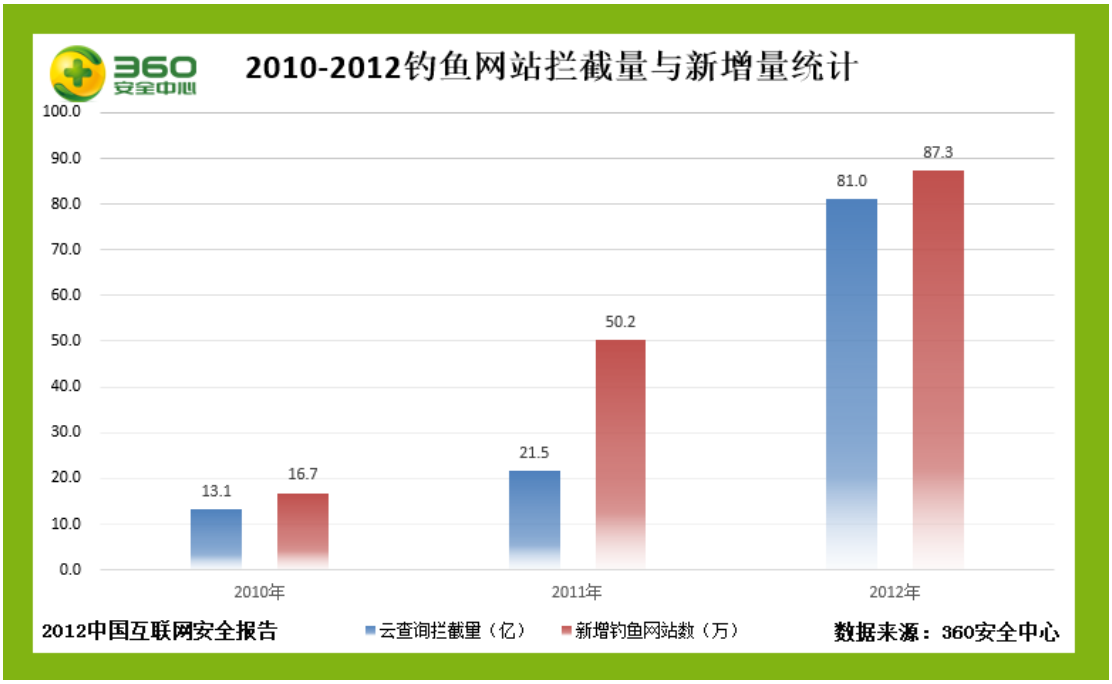
第二章 钓鱼网站成网民上网首要危害

挂马网页和钓鱼网站是恶意网址的两个主要形式。不过，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。而单纯的钓鱼网站本身不包含恶意代码，因此很难被传统的安全技术方法所识别；加之绝大多数的钓鱼网站设在境外，因此也很难通过法律手段进行有效的打击。钓鱼网站的这些特点，使其在最近两年中呈现出快速增长的势头，并且已经超过网页挂马和木马病毒，成为危害网民上网安全的首要威胁。

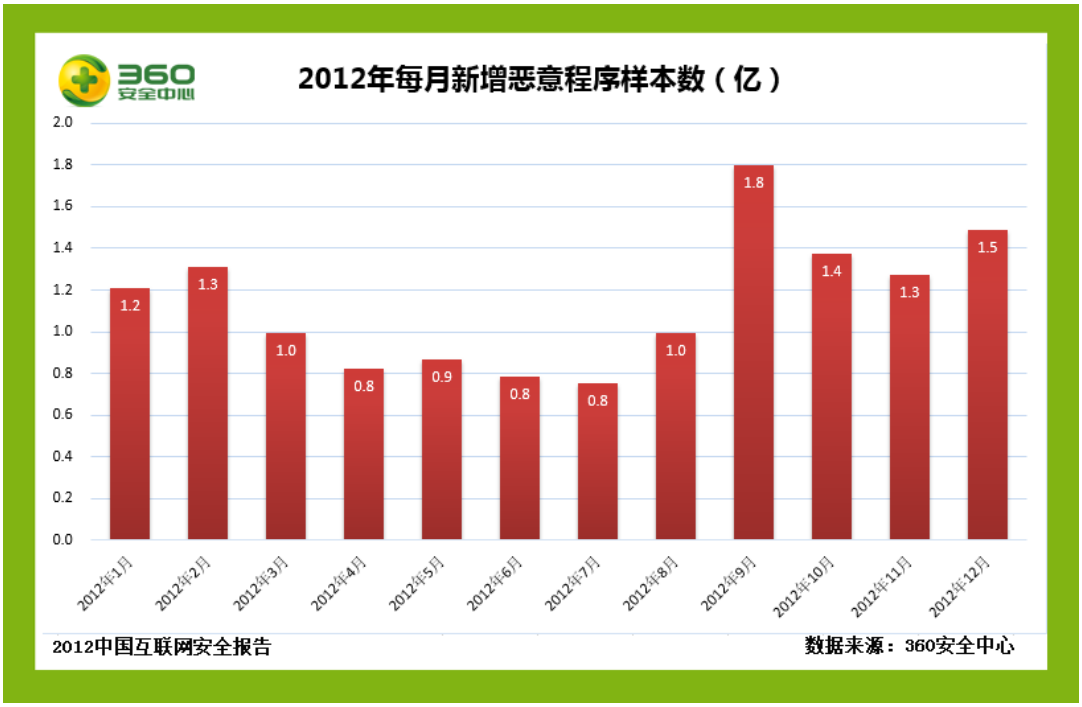
网址云安全仍然是现阶段识别和拦截钓鱼网站最有效的方法，同时，网站身份认证也为用户识别钓鱼网站提供了更彻底的解决方案。

一、 钓鱼网站呈现快速增长势头

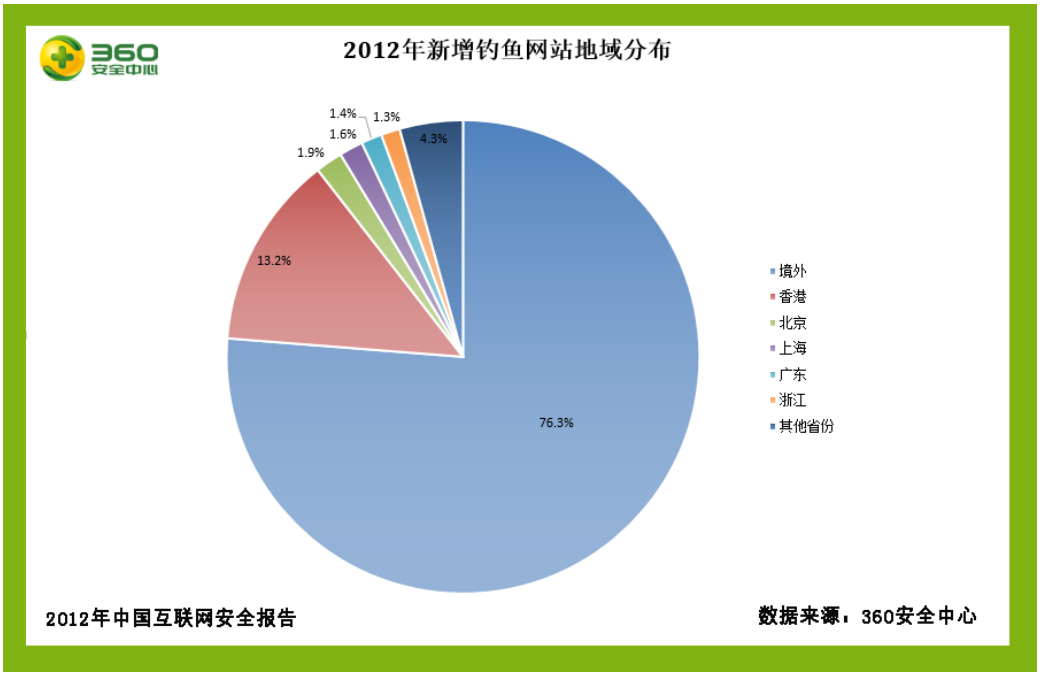
2012 年，360 安全中心截获新增钓鱼网站 87.3 万个（以 Host 计算），较 2011 年增长 73.9%；钓鱼网站的云查询拦截量为 81.0 亿次，较 2011 年增长了 273.3%，是同期挂马网页拦截量的近 200 倍。下图给出了 360 安全中心 2010-2012 年捕获的新增钓鱼网站数（万）和云查询拦截的钓鱼网站访问量（亿）。从图中可以看出，钓鱼网站无论从数量上还是活跃程度上都呈现快速增长的势头。



下面两图分别给出了 2012 年钓鱼网站云查询拦截量和新增钓鱼网站数量的月度统计。特别值得注意的是，钓鱼网站在 12 月的活跃程度是空前的，云查询拦截量占到了全年总量的 47.3%。而新增钓鱼网站的高峰则出现在双十一网购节所在的 11 月。

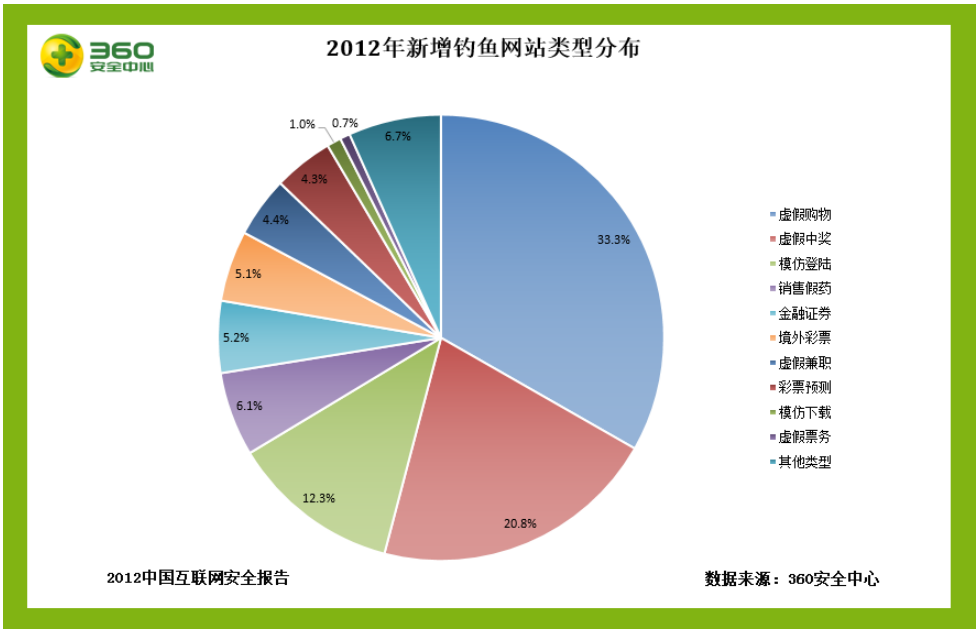


从地域分布的角度看，钓鱼网站主要分布在境外地区（76.3%）和香港地区（13.2%），二者之和达到 89.5%。这也就为有关部门通过法律手段监管和打击钓鱼欺诈行为制造了很大的困难。现阶段，安全厂商通过技术手段来识别和拦截钓鱼网站，仍然是打击钓鱼网站最为切实可行的方式。



二、 虚假购物占钓鱼网站总量的 33.3%

从钓鱼网站的类型分布上看，虚假购物仍然以 33.3%的比例蝉联钓鱼网站排名的榜首，紧随其后的是虚假中奖和模仿登录类钓鱼网站。排名前三的钓鱼网站占到钓鱼网站总量的 66.4%。值得一提的是，去年排名靠前的各种博彩类钓鱼网站的排名明显下降，而模仿登录的比例却大幅上升，排名也大幅提前。



在虚假购物类网站中，最为常见的是“假冒淘宝”。此类网站利用伪造商品页面诱骗买家支付，实际付款对象是不法分子的账户。有时此类钓鱼网站也会套取受骗者的帐号密码。

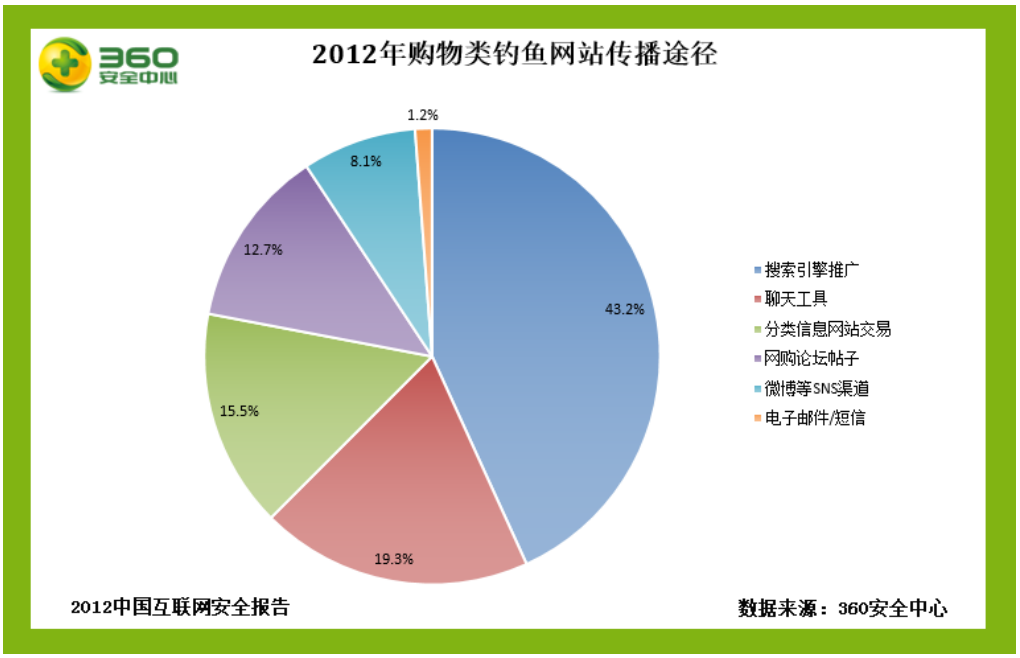
此外，网游交易欺诈、手机充值欺诈、仿冒品牌官网等也都是典型的虚假购物网站。从更广义的角度看，仿冒网银、销售假药、虚假票务网站也都属于虚假购物一类，不过由于这几类网站相对特殊，危害性也尤其突出，因此通常有必要进行专门统计。下面两图分别给出了仿冒网银和销售假药的网站案例。

虚假中奖类网站的数量虽然也超过了 20%，不过其中绝大多数并不很难识别，网民只要提高警惕，增强自我保护意识，就不容易上当受骗。但是，排名第三的模仿登录类网站则往

往会通过精良的页面制作，使其网站看上去十分逼真，普通网民仅凭肉眼一般难以分辨。下图给出了一个模仿 QQ 安全中心登录界面的高仿网站截图。

三、 搜索引擎是钓鱼网站传播的主要途径

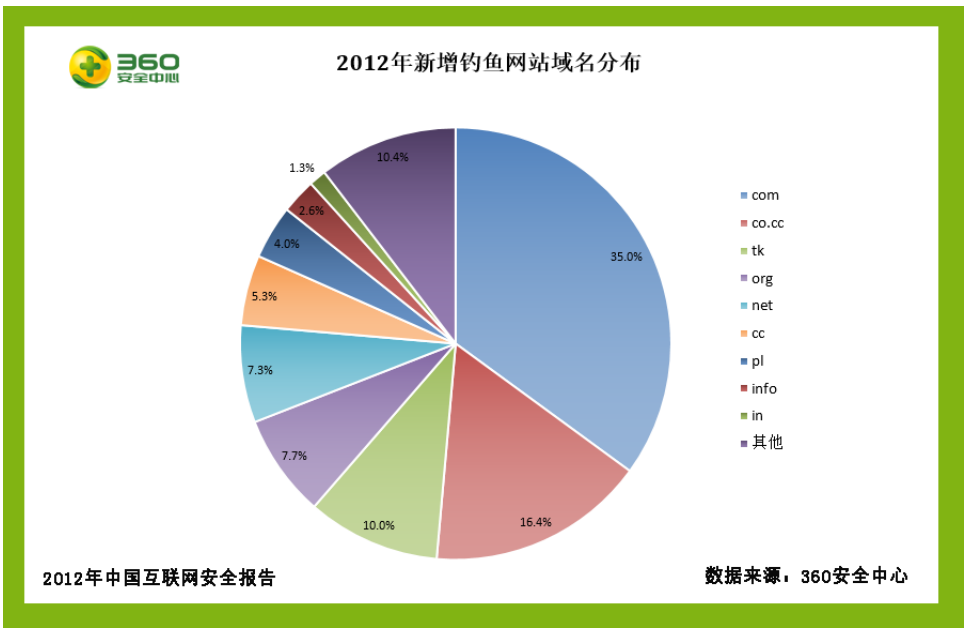
360 安全中心综合用户举报与“网购先赔”案例发现，钓鱼网站通过搜索引擎传播的比例达到 43.2%；此外，不法分子通过聊天工具一对一或聊天群发送钓鱼网址，通过分类信息网站、论坛、微博发布低价商品信息，诱骗用户访问钓鱼网站也是其重要传播渠道。



钓鱼网站通过搜索引擎进行传播的方式主要有两种，一种是黑链植入 SEO（搜索引擎优化），一种是直接利用竞价排名系统。所谓黑链植入 SEO，简单的说就是黑客首先入侵政府、高校等搜索引擎权重较高的网站，在网站页面植入自己的网站链接和关键词，并且巧妙隐藏使人不易发现。但搜索引擎在抓取页面信息时，却会抓取到这些隐蔽的链接，从而使钓鱼网

站在热词搜索结果中排名靠前。利用竞价排名系统进行推广则更为恶劣。由于某些搜索引擎审查不严，使得钓鱼网站的制作者可以直接在竞价排名系统中购买关键词，让自己的网站排在搜索结果的顶端，从而让网民误入钓鱼网站。

下图给出了钓鱼网站的域名分布。从中可以看出，常见的 com、org 和 net 都名列前茅。因此，我们不能简单的根据网站域名来识别钓鱼网站。



四、 网站身份认证成为反钓鱼解决方案

客观地说，对于不法分子最新制作出来的钓鱼网站，任何安全技术都不能保证 100%的第一时间识别和拦截，只能通过云安全不断缩短拦截周期。而钓鱼网站又主要依靠仿冒身份行骗，因此，对正规网站展现身份认证才是反钓鱼最根本、彻底的解决方案。

按照相关法规，国内经营的网站均需在工信部进行 ICP/IP 备案，目前的备案类别主要分为：军队、政府机关、事业单位、企业、社会团体和个人这么几种。ICP/IP 备案信息实际上就是政府颁发给网站的一张身份证，这些信息均可以在工信部网站进行查询。

下图是 360 安全浏览器在地址栏上，通过“网站名片”显示的网站备案信息。除了工信部的 ICP/IP 备案信息外，360“网站名片”还联合了多家权威认证机构，提供经过审核的其他身份信息，例如医院、政府、银行、品牌官网等资质信息。

网站的身份认证信息可以有效帮助用户识别安全软件暂时没有加入“恶意网址库”的钓鱼网站。比如，某家网站自称是工商银行网上银行，但身份认证信息去显示其为个人备案的网站或根本没有备案，则可以断定这是身份造假的钓鱼网站。

需要说明的是，某些企业网站虽然进行了 ICP/IP 备案，但仍然可能在自己的网站上发布虚假信息；另外，也不能排除某些身份可靠的网站遭遇黑客攻击或页面被篡改的可能性。虽然上述情况概率极低，用户也需要加以防范。

第三章 企业安全成为信息安全短板

与普通的个人电脑安全不同，企业用户的电脑安全，属于一种集体安全范畴，涉及内网管理、风险控制、流量监测和商业机密保护等多个方面。不过，由于绝大多数国内企业，特别是中小企业在信息安全方面的投入有限，使用免费的个人版安全软件代替企业版安全软件的现象非常普遍，这也给企业用户带来了相当程度的安全隐患。中小企业期待企业级安全服务也能像个人版安全软件那样，实现全面永久的免费化！

一、 企业面临多种安全风险

目前，U 盘是黑客对企业用户发动攻击的常用媒介。由于很多企业都会对内网系统进行隔离保护：有的是在网络层隔离，有的则干脆进行物理隔离。对于这种与世隔绝的网络，U 盘就成为了一个很好的木马载体。除了 U 盘病毒外，针对办公软件发动攻击的宏病毒和利用局域网系统传播的 ARP 病毒，也是对企业用户威胁较大的病毒。

某些企业简单的通过内外网的隔离来进行安全防护，却可能导致其内网用户的电脑系统无法在第一时间安装漏洞补丁，安全软件也不能实现及时有效的安全更新，客观上反而使内网系统处于一种更加不安全的状态，一旦遭遇木马病毒的入侵，就可能造成严重的系统破坏。

与个人电脑安全不同，企业安全属于一种集体安全问题。一般来说，联入内网系统的电脑中，只要有一台电脑被黑客攻破，那么就有可能造成内网安全体系的崩溃和商业机密的泄漏。也就是说，安全性最差的一台电脑实际上就决定了整个企业内网系统的安全级别，这就是企业安全问题中的“木桶效应”。

二、 9 成中小企业存在集体安全隐患

根据 360 安全中心 2012 年的抽样调查统计，国内企业普遍存在用免费的个人版安全软件代替企业版安全软件的情况。在接受调查企业中，国有大中型企业使用企业版安全软件的比例较高，达到 78%；而中小企业的情况则让人担忧。配备企业版安全软件的比例不足 5%，约 94%的中小企业仅为员工电脑安装个人版安全软件，还有 1%左右的企业根本不使用任何安全软件。

对于拥有大量商业机密并且对信息安全保护要求较高的企业来说，仅仅使用个人版安全软件确实存在一定程度的安全隐患，这主要表现在以下几个方面：

1） 缺乏统一管理容易形成木桶效应

如前所述，安全性最差的一台电脑实际上就决定了内网系统的整体安全级别。而对于使用个人版安全软件的企业来说，很难掌握员工的电脑安全水平，也很难对企业内网安全状况进行全面的了解和监控。安全维护只能依赖于员工个人的职业技能和安全素养。另外，一旦有员工电脑被感染或是企业内网被入侵，网络管理员也很难及时的发现和解决问题。

而使用管理功能较强的企业版软件，终端的安全状况都会汇总到一个控制中心，网络的管理员可以通过管理平台掌控全网的安全状况，为企业内部终端进行统一的查杀病毒、修复漏洞和产品更新等操作，还可以为每个终端配置正确的安全策略，并能在出现问题时及时收到报警通知，从而有效的避免木桶效应的影响。

下图为 360 企业版网管端显示的内网用户电脑的体检结果。通过这种全网体检和全网安全管理的方式，就能有效的控制内网系统的整体安全风险。

2） 内部软件或网址易遭安全软件误报

很多企业都会使用一些内部专用的软件。由于这些软件并未公开发行，也没有接受过安全公司的检测，并且某些敏感的操作可能和病毒木马比较接近，因此很有可能被安全软件误判为恶意软件。也有一些企业需要用一些远程控制软件管理网络或者终端，某些远程控制软件甚至与木马功能类似，因此也很有可能被个人版安全软件当做木马病毒或可疑程序予以禁止或删除。

另外，某些企业，包括某些大型国企，为了使用方便，经常会用自己内网专有的 DNS，将本来不是自己企业注册的域名重定向到企业内部的办公系统。而相同的域名在公共互联网上可能也会同时存在，只是普通用户与企业内网用户的 DNS 解析结果不同而已。如果公网上相同域名的网站恰好是钓鱼网站或挂马网站，那么当企业内网用户请求访问该域名时，就有可能被个人版安全软件拦截，从而形成误报。

而使用企业版安全软件，可以通过企业私有文件和网址白名单的设置，杜绝内网用户电脑上的安全软件对私有文件和内部网址的误报。下图为 360 企业版网管端的文件白名单和网址白名单设置界面：

3） 每台电脑独立升级占用企业上网带宽

个人版安全软件一般都是各自独立进行升级、打补丁等操作。而对于企业用户来说，如果每个员工电脑都要独立的联网升级，就会占用大量的网络带宽，影响正常的上网速度。这对于那些租用固定网络带宽，同时员工数量又比较多的企业来说，影响尤为明显。

而使用企业版安全软件，则可以通过控制中心端的缓存数据，进行二次分发，给内网用户统一升级，统一打补丁，从而在最大程度上减少升级、打补丁等联网操作对企业网络带宽的占用。

三、 企业级安全服务期待免费化

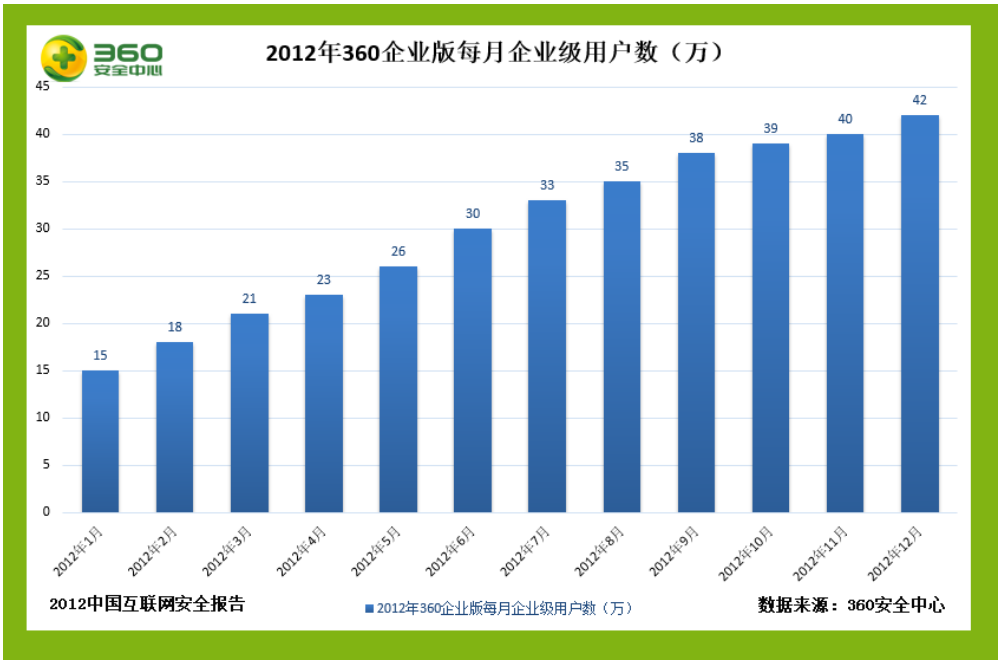
360 安全中心的用户调查分析显示，之所以会有 9 成以上的中小企业选择用免费的个人版安全软件代替企业版安全软件，主要是由于以下两方面的原因：

1） 绝大多数企业版安全软件都是收费的，而个人版安全软件则有很多免费品牌可以选择。由于中小企业在信息安全方面的投入能力有限，因此，用免费的个人版安全软件代替收费的企业版安全软件也就是很自然的事了。

2） 某些企业版安全软件（包括部分国外产品）的设计和功能老旧简单，不仅杀防能力不及某些免费的个人版安全软件，而且管理功能也极其简单，有的企业版安全软件甚至只有统一升级病毒库的管理功能。从使用角度看，购买这样的企业版安全软件就相当于批发购买了一定数量的个人版安全软件使用权。与其如此，还不如使用免费的个人版安全软件。

实际上，早在 2011 年 6 月，360 就率先推出了首款免费的企业版安全软件，但绝大多数多数中小企业对此并不了解。另外，一些大中型企业更倾向于企业安全产品的付费习惯。从长远来看，企业级安全市场将出现免费与收费并存的格局。

目前，免费的 360 企业版安全软件已经能够为用户统一提供包括修复漏洞、清除插件、修复系统危险项、开机加速、软件管理、软件分发、流量监控、内网体检、资产管理等全线的企业级安全服务。免费加上强大的管理功能，也使免费的企业版安全软件在 2012 年实现了全年的稳定快速增长。仅以 360 企业版为例，截至 2012 年 12 月 31 日，已经有 42 万家企事业单位选择使用 360 企业版，终端用户数也已经突破 1000 万，成为企业版安全软件市场的主流产品。企业级安全软件的免费化可能成为未来安全市场新的发展方向。


2012年360企业版每月企业级用户数（万）
45
40
35
30
25
20
15
10
5
0
15
18
21
23
26
30
33
35
38
39
40
42
2012年1月
2012年2月
2012年3月
2012年4月
2012年5月
2012年6月
2012年7月
2012年8月
2012年9月
2012年10月
2012年11月
2012年12月
2012中国互联网安全报告
2012年360企业版每月企业级用户数（万）
数据来源：360安全中心

第四章 高危安全漏洞严重威胁网站安全

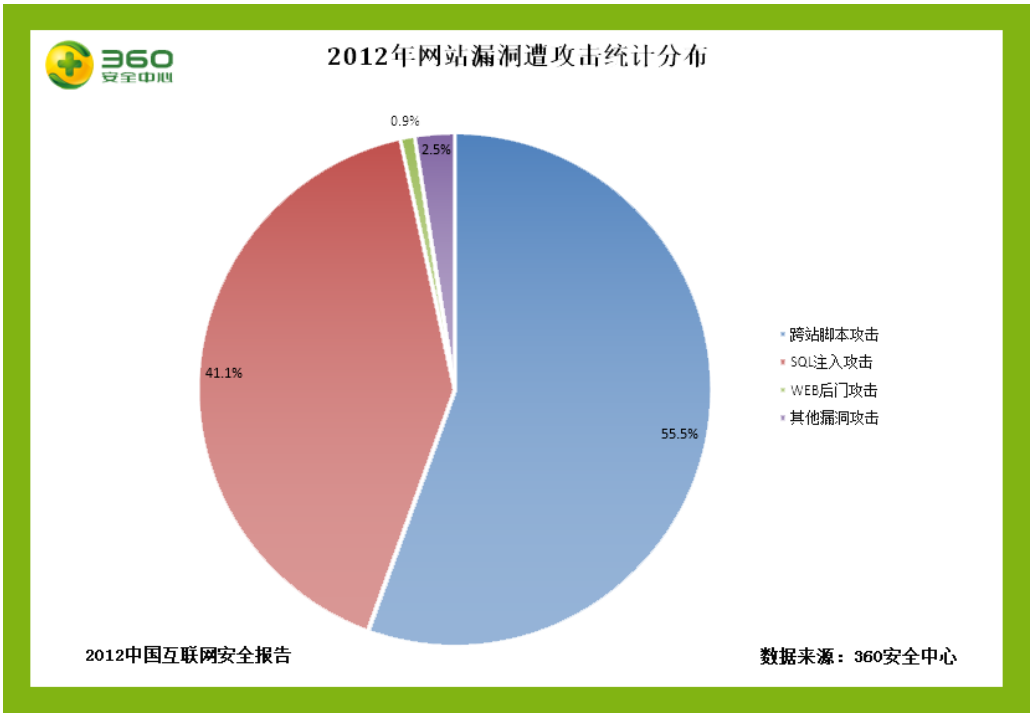
在木马病毒对个人电脑的攻击变得越来越困难的同时，一些黑客开始转向攻击安全性较差的网站。2012 年，网站安全问题进一步突显，网站被拖库、网页被篡改、用户信息被泄漏的事件频频曝光。网站频遭黑客入侵的一个主要原因就网站自身存在高危安全漏洞。

此外，雇佣黑客对竞争对手的网站进行流量攻击，也成为 2012 年网站安全的突出问题。大量中小网站面对此类攻击束手无策，甚至因此陷入生存困境。为网站提供专业的安全服务将成为互联网安全行业发展的重要领域，WEB 安全的行业关注度将因此提升到前所未有的高度。

一、 网站安全性问题迫在眉睫

根据 360 网站安全检测平台的抽样统计显示，75.6%的国内网站存在高危安全漏洞，而 39.6%的网站存在大量高危安全漏洞。黑客可以利用这些漏洞入侵网站系统，夺取最高权限，篡改网页内容，窃取数据库信息。

目前已知的各类高危网站漏洞大约有 1000 多种。不过，从 360 网站卫士拦截漏洞攻击的数量统计来看，遭黑客攻击量排名前两位的安全漏洞分别是：跨站脚本漏洞和 SQL 注入漏洞。针对这两个漏洞的攻击量之和，占到了网站卫士拦截的漏洞攻击总量的 96.6%。另据 360 网站安全检测平台的统计结果显示，在所有被检测出存在高危安全漏洞的网页中，存在上述两种漏洞的网页占到了总量的 93%以上。



另据 360 网站安全检测平台的安全性评分系统显示，在首次接受安全检测的十个主要类别的网站中，政府网站的成绩排名垫底，平均得分仅为 35 分（百分制）。紧随其后的是高校网站，平均得分为 37 分。这样的成绩意味着，政府和高校网站非常容易被黑客入侵、篡

改数据和窃取资料。

令人担忧的是，政府网站和高校网站上往往存有大量的敏感数据和个人信息，因此也一直是黑客窃取资料和篡改数据的重要目标。另外，这两类网站在搜索引擎中的权重也比较高，因此也是钓鱼网站通过植入黑链进行 SEO 的重点攻击目标。所以说，政府和高校网站在安全性方面的严重欠缺，直接威胁着公共安全的多个方面。

在首次接受检测的网站中，购物类网站 65 分的平均成绩虽然勉强及格，但由于此类网站直接关系到用户的个人财产，因此其安全性实际上还不足以保障安全网购。而团购类网站 43 分的平均成绩则更是让消费者担忧。另外，游戏网站上也往往存有用户的大量虚拟财富，67 分的平均成绩也亟待提高。

二、 拖库风险与篡改现象日益加剧

如前所述，由于大量网站存在高危安全漏洞，就为黑客入侵网站提供了可乘之机。2012 年，网站遭遇黑客攻击的事件频频发生，拖库与篡改的案例时有发生。所谓拖库，是指黑客入侵网站后将网站数据库中的数据导出。而黑客拖库的主要目标就是窃取用户的帐号、Email 和密码。

1）大量知名网站遭遇拖库

国内方面，2012 年 6 月，某知名网址导航被曝因 SQL 注入漏洞致使大量用户详细资料泄露；12 月，国内某著名电商网站曝出验证码设计缺陷，用户认证缺陷，可被暴力破解，导致大量账号信息泄露。

国际方面，1 月，亚马逊旗下的电子商务网站 Zappos 被黑客入侵，2400 万用户的账户信息被窃取，被窃信息包括用户姓名、电子邮件、电话号码、住址、信用卡号的最后四位等。6 月， 1500 万 eHarmony（相亲网站）密码和 3 万 LinkedIn（社交网站）密码被破解，遭破解的帐号和密码被公布在网络论坛上。7 月，雅虎旗下网站 Yahoo Voice 遭黑客攻击，45.3 万用户信息被曝光在网上，被张贴在网上的信息包括用户名和明文密码。

一个网站遭遇拖库，其他网站的用户帐号也会受到威胁。因为拖库还有一个叫做撞号

的“孪生兄弟”。所谓撞号，就是黑客利用已经窃取的帐号和密码，到其他网站上进行批量的尝试登录（通常都是编写程序自动执行的）。如果登录成功，则撞号成功。

由于很多国内用户习惯于在多个网站上使用相同帐号和密码，因此，黑客的撞号成功率实际上很高，一般可以达到 10%以上。事实上，当一个用户在多个网站上使用相同的帐号和密码时，安全性最差的一个网站就决定了这套帐号和密码的安全级别。

2）政府网站成为网页篡改的重灾区

据《广州日报》2012 年 7 月 26 日报道，公安部破获一系列通过攻击政府网站制作贩卖假证书的重大网络犯罪案件。截至 7 月 12 日，该案共抓获犯罪嫌疑人 165 名，收缴各类假证书 7100 多本、假印章 10000 多枚；已经发现被黑的政府网站多达 185 家，涉及 30 个省市自治区，共有 300 多万条个人隐私资料数据被盗卖，涉案金额超过 3 亿元。

与一般的制作假证方式不同，在这起系列案件中，假证制造者雇佣电脑黑客入侵相关政府网站，不仅窃取大量真实证书的用户信息用以制作假证，并且还将虚假证书的信息直接植入网站系统，使得假证购买者可以在政府网站上真的查询到自己的证书，这就使假证书看起来更像是真证书。

此次系列案件的破获再次暴露了国内大量政府网站存在的严重安全隐患。如前所述，政府网站的安全性在各类网站中实际上是最差的。较高的攻击价值和极低的攻击门槛必然使政府网站成为黑客攻击的“宠儿”。根据 360 网站安全检测平台的统计显示，在 2012 年检测出的 9 万余个遭到篡改的网页中，仅政府网站就占到了 15%。

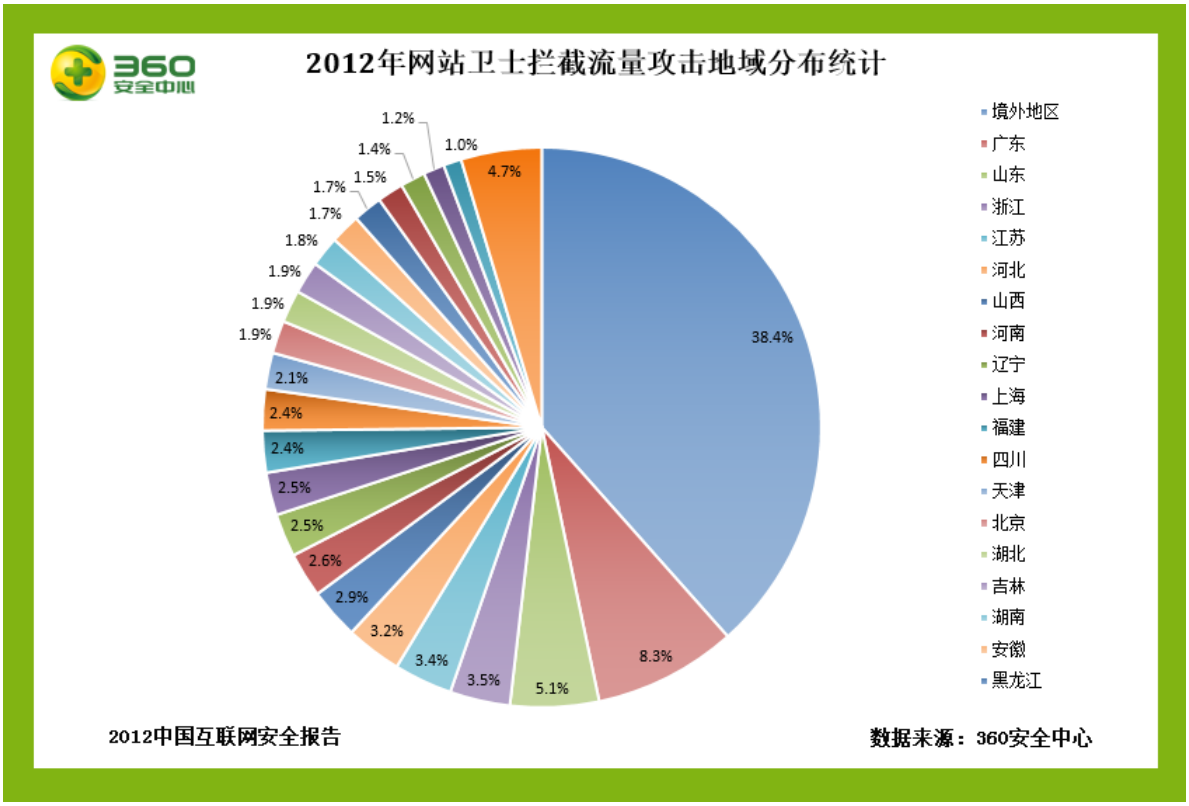
三、 流量攻击威胁中小网站生存

除了网页篡改和拖库风险之外，中小网站往往还必须面对一种实际威胁更大的黑客攻击——流量攻击。谓流量攻击，简单的说就是攻击者在同一时间对某个网站发起大量的访问请求，当访问量大大超过网站服务器的承受能力时，就会造成网站系统瘫痪、服务器无响应、无法访问、无法登录等异常现象。

2012 年，360 网站卫士共接到遭遇流量攻击的网站求助 1297 起，平均每天拦截各种流量攻击 659 波次，平均每天约有 14%的网站卫士用户遭到流量攻击。在网站卫士拦截的各种流量攻击中， CC（Challenge Collapsar）攻击最为常见，约占流量攻击拦截总量的 90%以上。

根据 360 网站卫士的用户反馈：绝大多数的流量攻击都是竞争对手雇佣黑客进行的恶意攻击，也有一部分网站是因为拒绝了网上讹诈之后，遭到了黑客的报复打击。中小网站在面对流量攻击时往往束手无策，只能通过重新启动服务器的方式来恢复系统。但恢复后的系统仍然无法防御新的流量攻击。

由于流量攻击并非针对网站的任何技术漏洞，而是一种纯粹的挑战系统极限的暴力攻击，因此，理论上说只能通过增加网络带宽，提高服务器响应能力的方法来解决。但提高系统容量又势必大幅增加运营成本，这对于中小网站来说，通常是难以承受的。



四、 网站安全将成为安全服务新焦点

对于拖库风险和数据篡改，最有效的防范措施就是尽快修补系统漏洞，提高网站自身的安全性。特别是对于普遍存在的，黑客攻击也比较集中的跨站脚本漏洞、SQL 注入漏洞和 WEB 后门漏洞，网站开发者应当及时检测并予以修补。

不过，对于绝大多数中小网站来说，要招聘专业的安全团队来维护网站安全实际上是非常困难的，这不仅会带来巨大的成本压力，而且相关人才本身也非常稀缺，业务水平也难以衡量。因此，很多中小网站非常期望能够获得安全公司的专业服务。

随着网站安全问题的日渐突显，网站安全服务已经和个人电脑安全服务一样，成为了一种普遍的公共安全需求。为网站提供页面安全检测、漏洞攻击拦截和流量攻击拦截等服务已经成为非常现实，且增长迅速市场需求。同时，如果网站能够像个人用户一样，得到安全公司专业且免费的安全服务，将有利于整个互联网安全行业的健康发展和网民利益全面的、有效的保护。

在网站安全方面，360 公司目前主要推出了两项免费的安全服务，一个是 360 网站安全检测平台（http://webscan.360.cn)，一个是 360 网站卫士（http://wangzhan.360.cn/）。

360 网站安全检测平台可以为网站检测各种已知的网页漏洞。截至 2012 年 12 月底，接受该平台检测的网页数量累计已达 12.5 亿，共发现各种网页漏洞 4400 多万个。

而 360 网站卫士不仅可以防范针对各种已知高危安全漏洞的攻击，同时也可以通过流量攻击识别技术和超过 200GB 带宽的服务器系统有效的拦截各种流量攻击。截至 2012 年 12 月底，360 网站卫士已经累计为各类网站拦截恶意攻击 3.7 亿次，加速页面 193.9 亿多个。