2011-2012 年度

中国互联网安全报告

360 安全中心

360 互联网安全学院

2012 年 2 月 20 日

免责声明

本报告为 360 安全中心发布的研究数据和分析资料。主要数据来源于 360 云安全系统、360 客服中心，以及网络公开资料。报告针对 2011 年中国互联网安全状况进行统计总结，并发布安全趋势研究结论。

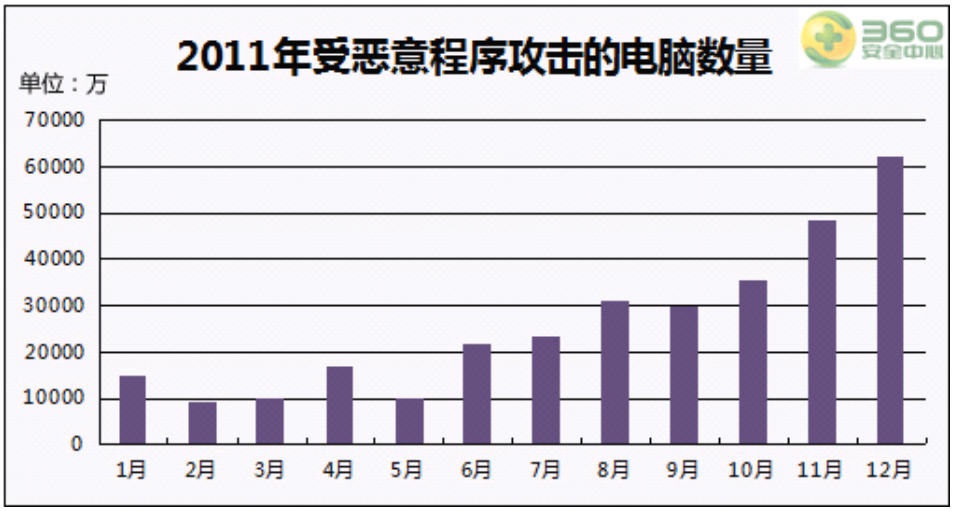
本报告可供任何个人、政府相关部门及行业机构、企事业单位参考，但对于本报告所阐述之内容、数据及分析结果，360 安全中心不承担与此相关的一切法律责任。

目录

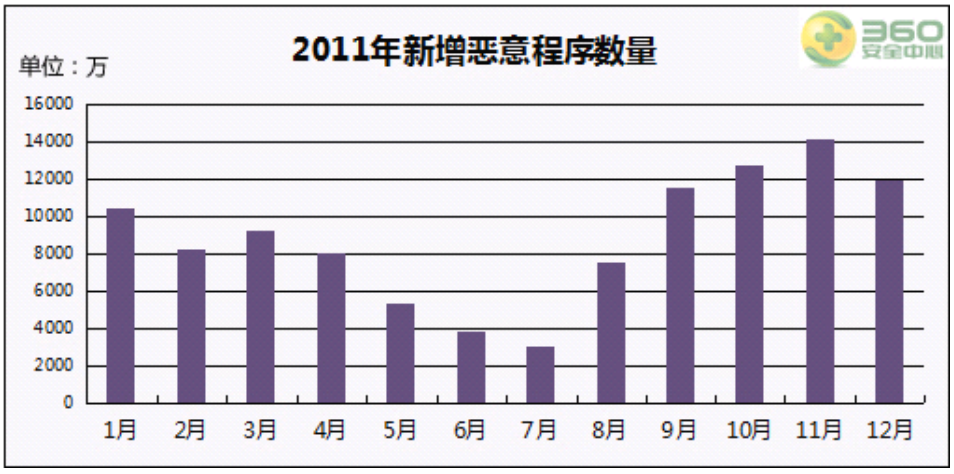
第一章 2011 年安全状况总结

（一）木马病毒疫情

2011 年，国内日均约 853.1 万台电脑遭到木马病毒等恶意程序攻击，占每天开机联网的电脑比例约为 5.7%，相比 2010 年增长 48.0%。其中，1%-3%的电脑终端实际感染木马病毒，主要原因为部分木马利用游戏外挂、盗版软件、视频等诱惑性网络资源伪装，欺骗用户关闭安全软件防护。

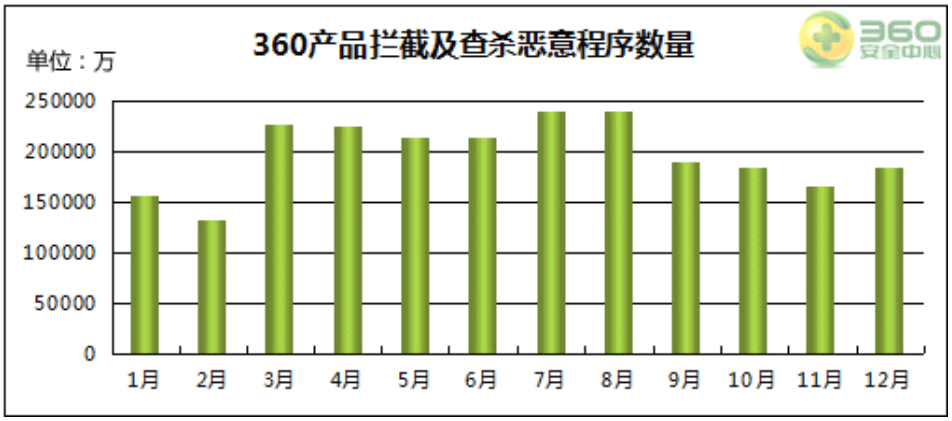


2011 年全年，360 安全产品共截获新增恶意程序 10.56 亿个（以新增恶意程序的文件指纹数量计算），相比 2010 年增加 87.7%。2011 年 11 月新增恶意程序数量创造历史峰值，当月截获 14087 万个新增木马病毒，相当于平均每秒出现 54 个新的恶意程序。

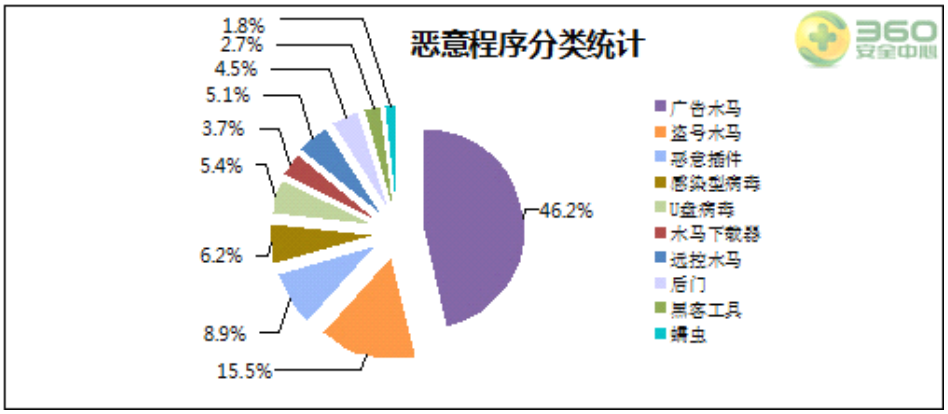


以清除的恶意程序文件数量计算，360 安全卫士、360 杀毒系列产品 2011 年共为用户拦截并查杀了 236.1 亿次木马病毒。在 360 云安全体系下，绝大多数木马病毒刚刚出现就立刻失效，黑客只能使用自动化工具加快木马病毒的更新速度，间接导致新增恶意程序数量持续

增多。

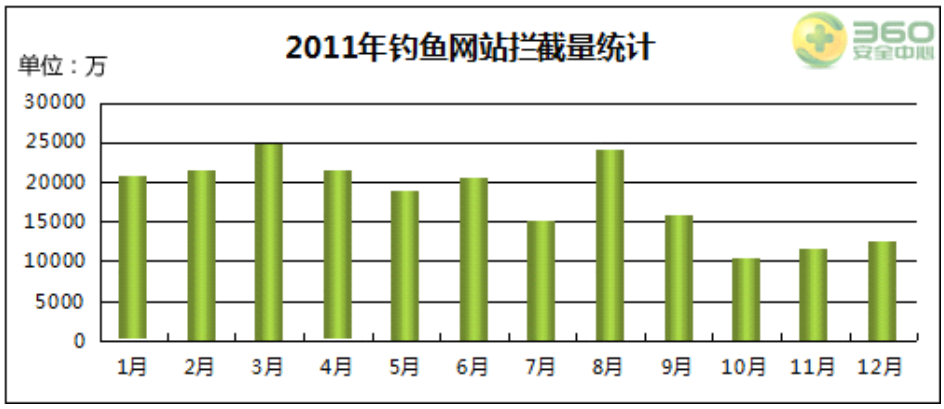


360 安全中心抽样统计发现，2011 年国内流行度最高的恶意程序仍然以木马为主，带有篡改浏览器首页、劫持浏览器访问特定网址、创建桌面广告图标、欺骗安装推广软件等行为特征的广告木马占据绝大多数。

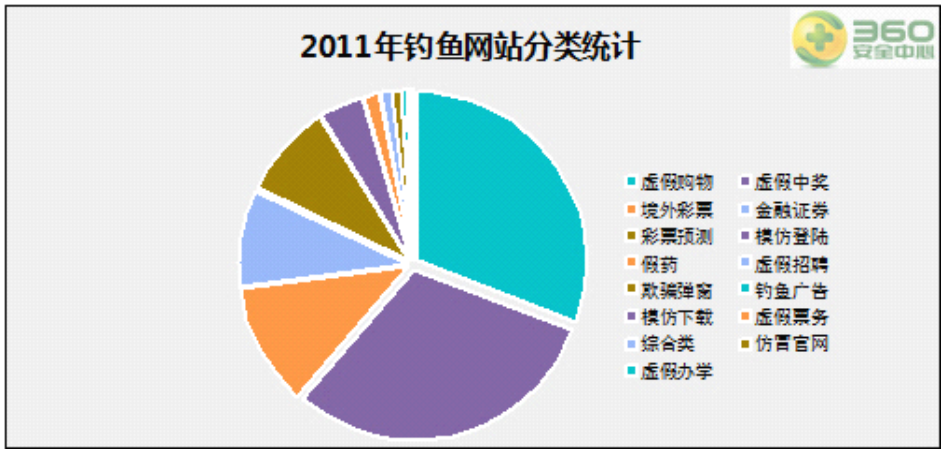


（二）钓鱼网站疫情

钓鱼网站是目前仅次于木马的第二大网络安全威胁，2011 年全年，360 安全卫士共截获各类钓鱼网站 501078 家，拦截钓鱼网站访问量 21.5 亿次，日均拦截量为 590.1 万次。2011 年 3 月是钓鱼网站最为活跃的时期，当月日均拦截量达到 792.6 万次。



2011 年出现的钓鱼网站中，虚假购物类网站数量最多，占比达到 30.73%，包括假冒淘宝、手机充值欺诈网站、网游交易欺诈网站，以及模仿知名品牌的山寨购物网站等。随着电子商务应用普及，网购人群成为钓鱼网站主要欺诈目标。



在虚假购物网站之后，虚假中奖钓鱼网站的数量排名第二，尤其是在微博应用兴起后，以微博活动、微博抽奖等名义欺骗用户的钓鱼网站数量也水涨船高。

此外，金融证券欺诈、假药网站、虚假招聘、假机票假火车票等票务钓鱼网站等也在 2011 年数量大幅增多，涉及人们理财、医疗、工作和出行等生活中的各个环节，对不熟悉互联网的电脑用户极具威胁。

目前，360 安全中心已经建立起一套能够自动抓取和识别钓鱼网站的智能反钓鱼系统，再加上 3 亿多用户的实时举报和网址反馈，能够最快、最全地拦截钓鱼网站。360 安全中心同时呼吁，域名服务提供商、搜索引擎，以及网络广告运营者等相关厂商也应该严格审核机制，共同为用户清除网络上的钓鱼欺诈信息。

（三）网站泄密事件

2011 年 12 月 21 日，程序员网站 CSDN 的 600 余万个帐号密码在网上公开，犹如多米诺骨牌般，众多知名网站也随之爆出被黑客“拖库”的传闻，尽管其中部分消息被证实为谣言，中国网站不安全现状仍由此暴露在公众面前。

1、网站泄密的原因

网站泄密的主要原因有两点，第一是网站安全防护缺陷，例如缺乏专业安全维护人员、没有及时为系统和网站程序打补丁、网站管理员安全意识淡薄等，这样的网站相对更容易被黑客窃取数据库；第二，有的网站没有对用户数据进行加密保护（用户密码什么样，网站数据库就存成了什么样），一旦数据泄露，大量用户的注册邮箱和密码就直接被黑客获取。

2、网站泄密的影响

电子邮箱是注册互联网服务的一种泛 ID 身份，对普通网民而言，一个电子邮箱往往关联着数十种网络服务的帐号；同时，部分网民习惯为不同网络帐号设置相同的密码，因此如有一家网站被黑客拖库，该网站用户的大批网络帐号都可能蒙受盗号损失。

具体到黑客拖库获利，大致可以归纳为以下六种：

1) 筛选有价值的注册邮箱，比如知名企业的工作邮箱，“洗号”分子有可能窃取邮箱中的重要商业资料，甚至进一步通过社会工程手段进行诈骗（一些贸易企业电子邮箱失窃后，引发巨额的交易诈骗）；

2) 利用密码库在网上支付平台自动批量发起交易，如果恰好用户泄露的注册邮箱和密码与网上支付账户的交易密码相同，支付账户中的余额就可能被洗号者转移走；

3) 利用密码库尝试登录 QQ、MSN 等聊天软件帐号（如 QQ 邮箱、hotmail、live 邮箱注册的帐号密码泄露），向好友发送借钱诈骗消息；

4) 利用密码库在微博等社交网站上尝试登录，由此产生出付费加粉丝、发布广告信息或钓鱼诈骗链接等多种获利途径；

5) 利用注册邮箱数据发布垃圾邮件。这些邮箱一方面成了垃圾邮件的发送对象，另一方面也可能被黑客利用作为垃圾邮件发件人（最极端的例子，有网民反馈邮箱收到了自己发给自己的垃圾邮件）；

6) 一些游戏厂商的用户数据库被黑客窃取后，洗号者会将受影响用户的游戏装备和游戏币窃取，在第三方交易网站上出售赚钱。

3、网民如何防范网站泄密

360 安全中心关于密码管理的安全建议：

第一，分级管理密码，重要帐号（如常用邮箱、网上支付、聊天帐号等）单独设置高强度密码（大小写字母结合数字、特殊符号）；

第二，定期修改密码，可有效避免网站泄密后影响到自身帐号；

第三，工作邮箱不用于注册网络帐号，以免密码泄露后危及企业信息安全。

第二章 木马变化趋势

（一）技术变化：木马结合钓鱼攻击渐成主流

随着免费安全软件普及和云安全技术发展，特别是在 360 云安全主动防御的行为拦截体系下，传统的木马病毒逐渐丧失了生存空间，只能伪装成热门网络资源诱骗用户关闭安全软件。

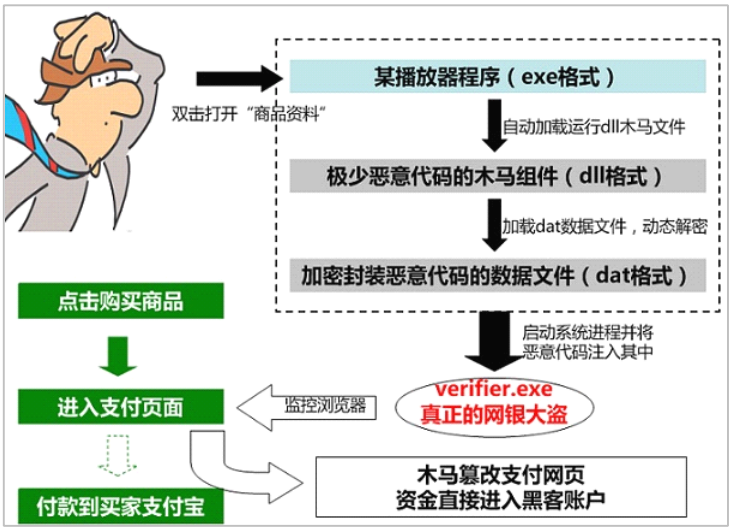
不过与此同时，一些木马制作者也开始变化思路，转而生产“钓鱼式木马”，包括如下三类：

第一、黏虫木马

以“QQ 黏虫”为例，这类木马盗号分为三步：第一，盗号分子以发照片或电子相册的名义把木马发给 QQ 好友；第二，“QQ 黏虫”运行后强制终止 QQ 程序，迫使用户重新登录；最后，木马创建透明窗覆盖在 QQ 登录窗口上，收集受害用户输入的密码信息，自动发送到盗号分子指定的远程服务器上。除盗号 QQ 外，黏虫技术也已被木马制作者广泛应用在多款热门游戏盗号上。

第二、网购木马

以“网银大盗”为例，该木马以商品图片、商品优惠码等名义传播，运行后可篡改正常网页的页面显示，暗中则修改订单数据、网页显示数据、订单结算数据等，将网页支付订单的收款人改为木马作者，并把付款金额改为木马作者定制的数目，从而达到窃取受害者网购支付资金的目的。目前，这类篡改网页技术还被木马制作者利用在 Q 币充值、手机充值等网上支付环境中。



第三、劫持浏览器木马

此类木马的典型案例是“假文凭木马”，该木马行为更加简单，只是篡改受害电脑的 Host 设置，把“中国高等教育学生信息网”的网址指向一个页面仿真的钓鱼网站，欺骗受害网民

在钓鱼网站上查询学历，查询到的结果当然也是假的。由于大量正当软件也会修改 Host 设置，安全软件因此很难根据木马的这一项行为判断其是否有害。

与普通木马相比，“钓鱼式木马”行为极其简单，只做与钓鱼欺诈相关的动作。就像一个平时很老实的人，忽然干坏事反而更难防范，因此也增加了安全软件检测识别的难度。

为防范上述木马结合钓鱼的攻击手段，360 木马防火墙针对黏虫木马推出“除虫防盗号功能”，360 网购保镖则采用最严格的防护机制，在用户上网购物和使用网银支付、充值时拦截未知可疑程序，并独创“支付页面防篡改”，全面保护用户网上支付安全。

（二）渠道变化：网站黑链偷渡式下载

2011 年 4 月，一个名为“黑桃 J”的木马被 360 安全中心截获，该木马采用“色情关键词+跳转代码+网站黑链”的全新推广模式，实现偷渡式下载推广目的：黑客首先入侵篡改大批高校网站，在这些网站页面中埋藏色情关键词，并设置了网址跳转代码。其结果是，一些网民在搜索色情词汇时，搜索结果中列出的是高校网站的网址，点击后却会自动跳转到一个带毒视频站上。

黑客高明之处在于，被篡改的高校网站页面只有通过搜索引擎打开时才会自动跳转。而网站管理者大多是直接输入网址或从收藏夹访问自己的网站，这种情况下页面既不会自动跳转到带毒视频站，也不会显示出色情关键词，因此很难察觉自己的网站已经被黑客偷偷篡改。

由于 gov. cn、. edu. cn 等政府和教育网站域名在搜索引擎中的权重较高，黑客篡改此类网站页面，加入黑链和关键词后，就能由搜索引擎带来巨大的流量。除推广木马外，网站黑链还被不法分子广泛利用于推广假药钓鱼网站、吸引广告点击等，如下两图所示，网站黑链不仅内容多样，还有其地下交易的完整价格体系。

```
<script language="javascript" type="text/javascript">
document.write("<div style=\"position: absolute; top: -978px;left: -978px;\">")
</script>
<a href="http://www.baidianfeng1.net">白癜风</a>
<a href="http://www.gaomax.com.cn">生长激素</a>
<a href="http://www.gaomax.com.cn">美国快高</a>
<a href="http://www.gao-max.com">长高药</a>
<a href="http://www.gao-max.com">美国快高</a>
<a href="http://www.shangwuqiche.cn">大连租车</a>
<a href="http://www.guke630.com/">重庆骨科医院</a>
<a href="http://www.125job.com">义乌人才网</a>
<a href="http://www.toomei.com">美女</a>
<a href="http://www.guccongucci.com">Gucci</a>
<a href="http://www.guccongucci.com">Gucci包</a>
<a href="http://www.guccongucci.com">Gucci官网</a>
<a href="http://www.517cai.cn">有机蔬菜</a>
<a href="http://www.klzqb.com/">宝利棋牌</a>
<a href="http://yy.dzwww.com/pfxb/">生殖器疱疹</a>
<a href="http://health.jinghua.cn/xb/">疱疹</a>
<a href="http://guanxinbing.5j5k.com/">冠心病</a>
<a href="http://health.fjsen.com/sjxl/dianxian/">癫痫</a>
<a href="http://health.fjsen.com/pifu/jrsy/">尖锐湿疣的症状</a>
<a href="http://www.fh21.com.cn/pifu/npx/">牛皮癣</a>
<a href="http://www.cheaprunescapegold.com">cheap runescape gold</a>
<a href="http://www.cheaprunescapegold.com">buy runescape gold</a>
<a href="http://www.cheaprunescapegold.com">cheap rs gold</a>
<a href="http://www.0992.org">三唑仑</a>
<a href="http://www.0992.org">三唑仑片</a>
<a href="http://www.9000f.com">1.76蓝魔精品</a>
<a href="http://www.6gdy.com">有什么好看的电影</a>
<a href="http://www.6gdy.com">网吧电影</a>
```

近期推出:

包月套餐(疯狂折扣)活动火爆进行中 —— 每天增加外链持续30日

购买包月套餐免费提供SEO优化大礼包，快速提升网站的权重！

活动期间购买包月套餐3套以上，赠送A包月一个月，购买5套以上，赠送B套餐包月一个月。

多买多送，机会不容错过！

包月	PR1	PR2	PR3	PR4	PR5	PR6	套餐说明	折扣价
A	3	3	4	3	-	-	持续增加链接30日共390个站点	300元
B	-	-	8	5	-	-	持续增加链接30日共390个站点	525元
C	-	-	6	5	2	-	持续增加链接30日共390个站点	675元
D	-	-	5	4	2	2	持续增加链接30日共390个站点	780元
E	-	-	-	8	5	-	持续增加链接30日共390个站点	840元
F	7	7	-	-	-	-	持续增加链接30日共420个站点	225元
G	每天随机增加PR2-PR6链接35条						持续增加链接30日共1050个站点	630元
H	客户自己制定各PR网站数量						另议	

（三）2011 年十大木马盘点

根据木马流行度、危害，以及公众影响力等综合因素考虑，360 安全中心发布 2011 年国内十大木马榜单如下：

一、BMW（Bios Rootkit）

全球首例可刷写 BIOS 的 BMW 木马(国际厂商命名为 Mebromi)，感染电脑主板的 BIOS 芯片和硬盘 MBR（主引导区），再控制 Windows 系统文件加载恶意代码，使受害用户无论重装系统、格式化硬盘，甚至换掉硬盘都无法将其彻底清除。

二、QQ 黏虫

新一代盗号毒王，主要利用伪装图片传播，运行后以透明窗体覆盖 QQ 登录窗，“黏”走受害用户的 QQ 密码。

三、Duqu

全球闻名的“超级工厂 2 代”，利用 Windows 内核 0day 漏洞传播，使嵌入恶意字体文件的 Word 文档成为木马载体，再针对攻击目标窃取机密技术资料。在国内，一家拥有蓝牙软硬件技术的高科技企业也曾遭到 Duqu 攻击。

四、新“网银大盗”

2011 年技术最成熟的网购木马，它利用合法程序加载组装恶意代码，运行后篡改支付页面，劫持受害者的网购资金。

五、鬼影 3

感染电脑硬盘的主引导记录（MBR），无论重装系统或是格式化硬盘都无法杀掉。此外，该木马还释放一个恶意驱动作为“保镖”，用来禁止任何修复 MBR 的操作，因此成为比较难以清除的顽固木马。

六、桌面雪花

利用 QQ 邮箱附件传播的木马下载器，同时带有蠕虫特征。它采用分进合击的攻击手段，将木马分为两部分：一部分是不带有恶意代码的“桌面雪花”屏保，另一部分是加密的 ini 配置文件，也不可能单独作为木马。然而当屏保程序运行时，木马会自动合体，下载其他木马病毒进入受害者电脑。

七、图纸大盗

通过电子邮件传播的商业间谍木马，邮件附件名为“趣味机械制图.rar”。如有网民下载运行了附件，同时电脑中又装有 AutoCAD 软件，“图纸大盗”就会被激活。当中招电脑再打开任意 CAD 图纸时，木马都会把这张图纸发送到黑客指定的邮箱。

八、魔影（TDSS.TDL-4）

号称拥有世界尖端黑客技术、长期肆虐欧美地区，曾迫使微软制作了一款专门用于防御“魔影”（TDL-4）的反病毒补丁（KB2506014），然而这个补丁在发布后第二天便被“魔影”作者攻破。不过在国内，该木马传播范围较小，感染量低于与其相似的鬼影系列木马。

九、黑桃 J

伪装为成人播放器、专用播放器等视频软件，运行后篡改浏览器首页为不良网址导航。该木马的防御和查杀难度并不高，但其传播渠道在当时颇为新颖，是“网站黑链偷渡式下载”的开先河者。

十、替身

2011 年游戏盗号木马的代表，它会替换 QQ、YY 语音等 16 款网民常用软件的正常文件，在这些软件运行的同时激活木马，从而对《QQ 幻想世界》、《刀剑英雄》等热门游戏实施盗号。

第三章 钓鱼网站变化趋势

（一）社交网络风险

2011 年 5 月，一位名叫罗萨里.瓦洛塔（Rosario Valotta）的意大利网络安全研究者在 Facebook 上玩了个小把戏——在他的个人页面上，好友可以对一张美女照片拖拽衣服。短短 3 天内，瓦洛塔的 150 名好友中有 80 多个好友参加了这个游戏。但他们没有想到的是，自己仅仅动了动鼠标，浏览器的 Cookie 文件就自动发送到瓦洛塔的服务器上，而 Cookie 保存着浏览器登录网络帐号的身份验证信息，这意味着，瓦洛塔随时可以利用这些 Cookie 登录自己好友的 Facebook 帐号。

瓦洛塔的测试验证了 IE 浏览器 cookiejacking 漏洞，但这也只是社交网络的安全风险的冰山一角：

一、基于社交网络的钓鱼欺诈风险急剧增加

360 反钓鱼系统抽样调查显示：2011 年，利用社交网络传播的钓鱼网站比例达到 15.7%，是仅次于搜索引擎、聊天软件之后的第三大钓鱼欺诈信息传播渠道。

钓鱼网站利用社交网络传播的方式目前主要包括三种：

第一，对网站拖库撞号后，盗用他人微博或其他社交网站帐号发布钓鱼链接。也就是说，如果一个网民在微博和 CSDN 使用相同的注册邮箱和密码，由于 CSDN 曾被黑客拖库，该网民的微博帐号密码可能因此泄露，被盗号分子用来刷粉丝、发布钓鱼链接和其它广告信息（关于网站拖库，下一章将有更详细的阐述）；

第二，不法分子注册大批微博帐号，以评论和转发的形式诱骗正常微博用户点击钓鱼链接，此类钓鱼链接以假冒微博官方抽奖送礼活动为主，2011 年此类钓鱼网站数量高达 10 余万家（以 Host 计算），是全年增速最快的钓鱼网站类型；

第三，利用社交网站的网页 XSS 跨站漏洞制作蠕虫，通过好友关系以几何级数自动扩散钓鱼链接。由于此类钓鱼传播方式社会影响大、被追究法律责任的风险高，目前并不多见。

二、社交网络正在成为下一个黑客“金矿”

过去十年，游戏产业一直是国内黑客网络犯罪获利的主攻方向；其次是电子商务，以网购钓鱼和木马为代表的新型安全威胁不断渗透到电商产业中。如今随着社交网络蓬勃兴起，极大地改变了人们上网交流和信息传播的方式，社交安全威胁开始与日俱增，正在成为继游戏、电商之后下一个黑客“金矿”。

360 安全中心认为，社交安全威胁产生的根源来自以下三个方面：

第一、海量用户基础

来自 CNNIC 的第 29 次《中国互联网络发展状况统计报告》显示，2011 年我国微博用户数量达到 2.5 亿，较上一年底增长了 296.0%；此外，专业 SNS 网站用户数量也积累了 2.44 亿。即便上述两个数据间存在巨大重合，国内社交网络用户至少也有 3 亿。

第二、社交商务发展

海量用户之上，是社交商务的快速发展。大批企业员工活跃在微博、SNS 网站上，企业信息在社交网络中快速流通，涉及各种公司的市场活动、客户服务、人员招聘、产品战略等各个层面，其信息价值已不亚于游戏盗号所能获取的虚拟货币和装备。

第三、好友信任关系

利用社交好友关系间的天然信任，不法分子进行信息获取、诱骗点击、借钱等欺诈活动的效率远远高于传统的搜索引擎优化和网络广告。同时，不少网民出于方便，习惯为多个网络帐号设置相同的密码和注册邮箱，为黑客批量盗号提供了便利。正因如此，社交用户的帐号安全威胁将会成为比游戏盗号更为严峻的网络安全问题。

（二）网购支付风险

2011 年，360 安全中心与易宝支付联合调查统计显示：当年 1 月至 11 月间，易宝支付共接到用户对钓鱼网站的投诉 4923 笔，在投诉案例中占比为 89%，涉及金额 278 万余元，购物钓鱼网站对受害者造成的平均经济损失为 565 元。

购物类钓鱼网站特点

伪装知名购物网站是目前最流行的一种钓鱼网站形式。当骗子使用钓鱼模板生成一个表面上真的购物网站几乎一模一样的网页后，接下来会以“调低商品价格”等名义为由，通过聊天工具把钓鱼链接发给买家。通常，这个链接会利用一些网站的跨域漏洞，在阿里旺旺、QQ 等聊天消息中显示为安全链接，从而使买家放松警惕，在钓鱼页面的引导下进行付款操作。

由此，假购物网站钓鱼可以实现两种目的，其一是套取买家的网银、网上支付等密码信息，窃取账户余额，甚至修改绑定的手机肆意消费；其二是欺骗买家为骗子提前设计好的订单进行支付，相当于为骗子购买手机充值卡、游戏点卡等虚拟财产，使骗子得以从中套现获利。在部分受害买家严重缺乏安全意识的情况下，还可能被骗子以“卡单”等借口诱导反复多次付款，造成大额经济损失。

除上述两种获取经济利益的途径外，许多购物钓鱼网站并没有提供网银在线支付，而是在网站上公布个人银行账户，用稀缺商品资源和极低的价格诱惑买家使用 ATM、网银转账付款。

典型案例

钓鱼网站不会平白无故出现在电脑上，消费者究竟在哪些情况下最容易遭遇钓鱼呢？以下是几种常见的网络钓鱼案例。

案例一　偷梁换柱，把消费者从真网站带到假网站

今年 9 月，刘小姐在某知名网站搜到一家店铺打算购买商品，与店家联系后对方声称店内有活动，于是按店家要求加了 QQ 号继续砍价，之后店家以修改价格为由给刘小姐发了一个链接。刘小姐没有想到的是，点开链接后，她已经脱离真网站打开了冒牌的钓鱼网站，之后当她付款了 200 元，才发现自己的账户里根本没有购买记录，钱却已经通过第三方支付平

台付给了陌生账户，没有办法追回。

案例二　借刀杀人，利用搜索引擎吸引点击

车主邵先生为图方便，上网搜索“中石化充值网站”，在搜索结果前列中打开了一个网址是 www.95115888.com 的网站，付款 5000 元给自己的加油卡充值。事后经过查询，他发现钱迟迟没有充到自己油卡里，于是询问网站在线“客服”，只得到“现在系统正忙，请您稍后再充一次”的答复。隐约觉察到自己被骗的邵先生急忙拨打官方客服热线，才知道之前搜到的充值网站是钓鱼网站。

案例三　趁火打劫，连哄带吓制造恐慌

在危害特别重大的网银钓鱼诈骗中，不法分子通常以银行名义群发诈骗短信或邮件，通过“网银口令升级”、“冻结银行账户”等诈骗信息，恐吓人们在钓鱼网站上输入网银账户密码“解冻”，在口令有效期内快速转走账户资金。利用一些网银安全机制的缺陷，不法分子在获取网银账户和密码后还会迅速修改账户绑定的手机，使其能从容地完全掌握账户中的资金。

网购安全解决方案

针对网购安全威胁，360 安全卫士于 2011 年初国内首推出专业的网购安全工具——网购保镖，能够为消费者有效排除网上支付交易过程中的钓鱼和木马威胁。

与传统安全功能不同，360 网购保镖采用更严格的“非白即黑”机制，在用户进行网络购物、网银充值等重要操作时会自动清理、拦截电脑中所有危险、可疑的程序，自动拦截虚假购物、充值网站，最大限度保证用户财产安全。

作为用户网购主要的交易平台，浏览器产品的安全特性具备更贴身的防护作用。为此，360 安全浏览器推出“官网认证”，在浏览器地址栏显示交易类、银行支付类、团购类、政

府类网站等官方网站的认证铭牌，帮助用户方便辨识真正的官方网站，从而避免因为访问假冒的钓鱼网站受骗。此外，当用户访问的网站是木马网站或钓鱼欺诈网站时，地址栏铭牌会显示为红色“危险”，对用户起到安全警示作用。

访问银行类网站示例，360 安全浏览器地址栏显示为绿色“可信网站”：

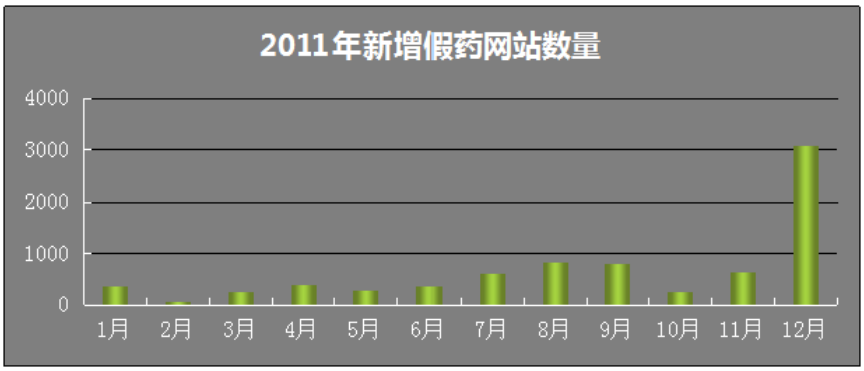
访问钓鱼网站时，360 安全浏览器发出警报提示：

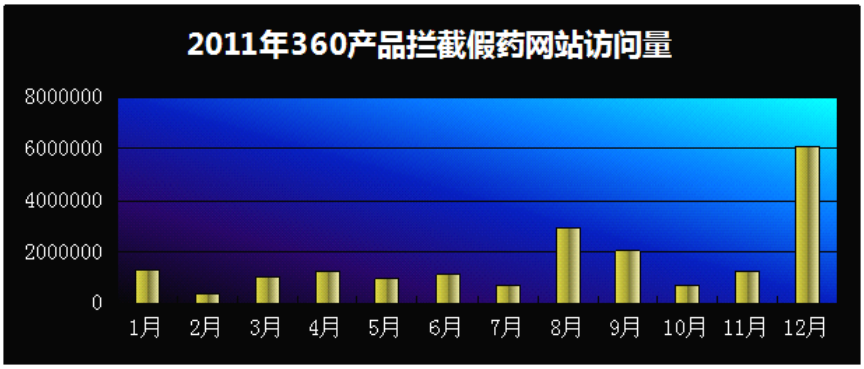
（三）多元化欺诈手段

除社交网络和网购中的钓鱼网站威胁以外，金融证券、彩票、医药医疗、网上招聘、春运买票等不同领域均存在一定程度的网络钓鱼欺诈现象。

以假药网站为例，2011 年 1 月至 12 月间，360 反钓鱼系统共监测到 7906 家假药网站，

共计拦截 19837991 次假药网站访问量：





按药品特征分类，假药网站主要包括以下四大类别：

第一、伟哥等男性壮阳药。此类假药网站数量最多，同时也是色情网站获得广告利益的主要收入来源；

第二、以德国拜耳、英国阿斯利康、美国辉瑞等跨国医药公司名义，销售冒牌的抗癌、抗肿瘤等名贵进口药。此类药物对症患者大多身患重病，假药即便造成不良状况，病人家属也很难判断是否与药品有关；

第三、以各种疑难杂症“特效药”作为诱饵，如治疗牛皮癣、去红血丝、糖尿病、高血压、肾病、风湿、痛风等，包装成功案例和专家证言欺骗患者购买；

第四、假冒北京同仁堂、红花药业等企业的中药处方药，典型的如金鸡胶囊、红花片、千金片等。

假药网站传播途径示例如下：

随着网络普及，包括智能手机等移动终端上网设备使用率持续攀升，网络钓鱼欺诈将进一步渗透到人们生活中，对人们健康、财产、工作、交友、娱乐等方方面面的问题制造麻烦，破坏人们对互联网的信任，极大阻碍互联网经济的健康可持续发展。

因此，可信网站体系的建设是从根源上瓦解网络钓鱼欺诈生存空间的基础：

一、以政府工信部备案数据、网站被许可的经营范围为可信网站识别标准；

二、推广可信网站身份认证标识，引导用户意识到在非可信网站上购物消费存在安全风险。

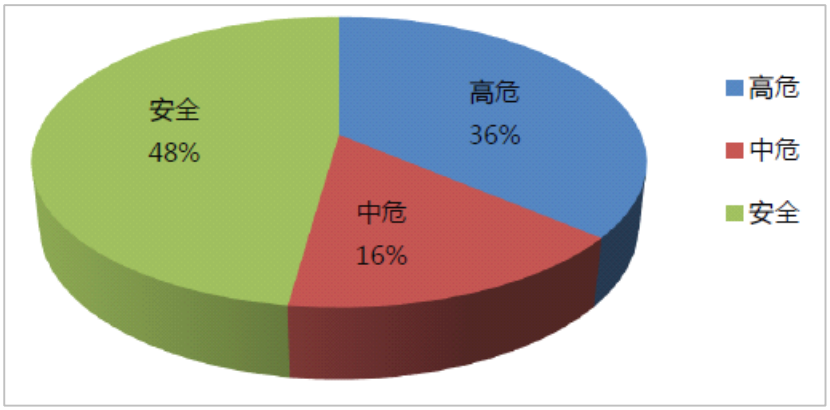
第四章 网站安全问题

（一）多数网站防护能力薄弱

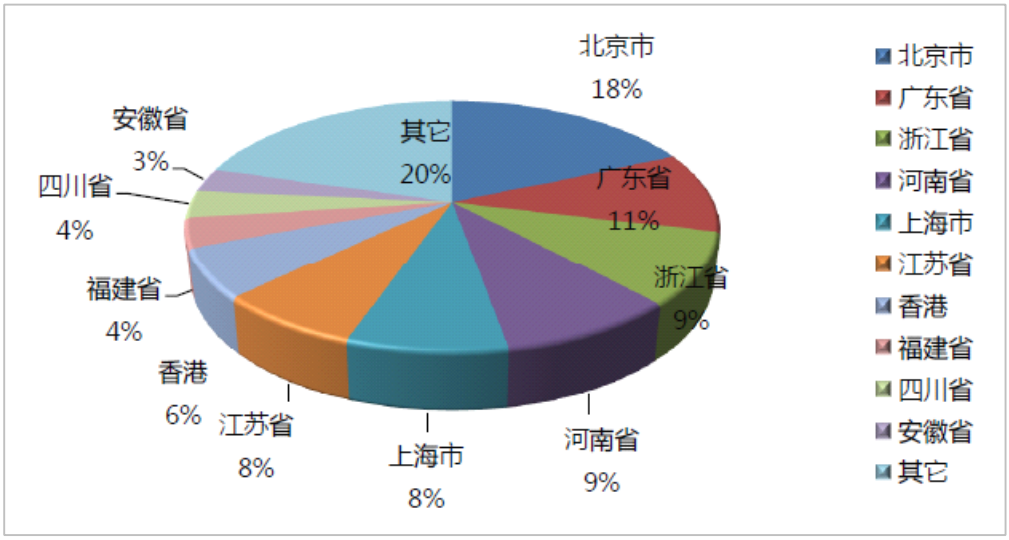
2011 年底曝出多网站泄密事件，事故发生主要原因在于网站存在漏洞，从而遭到黑客入侵拖库。通过 360 网站安全检测的统计，目前国内存在高危漏洞的网站约占 36%，中危漏洞的网站约占 16%，而相对比较安全的网站只有 48%。

一、网站漏洞总体情况

通过 360 安全检测平台全年对互联网部分网站的监控和检测，从中随机抽取了 93233 个网站，其中存在高危漏洞的网站 33753 个（占 36%），中危漏洞的网站 14917 个（占 16%），安全的网站 44567 个（占 48%），各等级分布如下图所示。

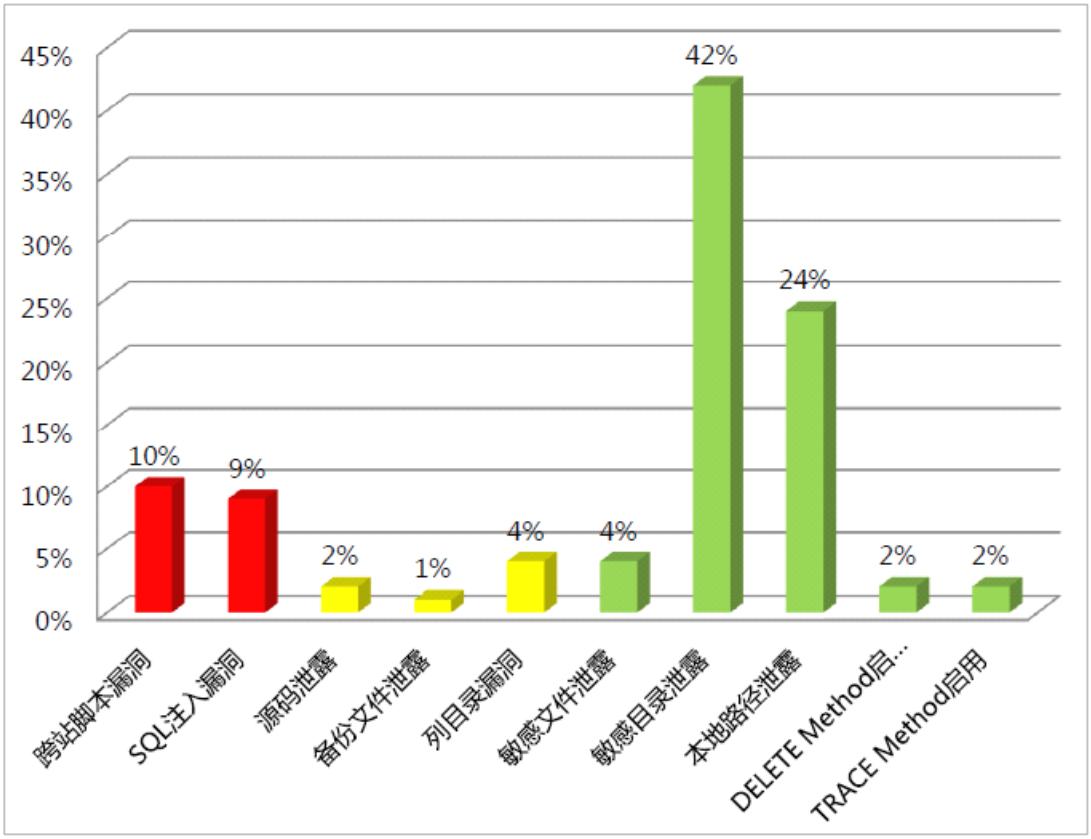


2011 年全国存在漏洞网站按地域进行统计，排行前十位的地区分别是：北京市、广东省、浙江省、 河南省、上海市、江苏省、香港、福建省、四川省和安徽省：



目前国内网站存在最多的高危级别的漏洞是跨站漏洞和注入漏洞；中危级别的漏洞是源码泄露、备份文件泄露和列目录漏洞；低危级别的漏洞是敏感文件泄露、敏感目录泄露、本

地路径信息暴露、Delete Method 启用和 Trace Method 启用：



由于网站漏洞的触发需要特定的场景，在黑客针对网站的实际攻击行为中，通常会组合利用多种不同类型的漏洞，包括运用社会工程学手段、弱口令破解等方式，达到其入侵和渗透目的。

比如高危级别的“SQL 注入漏洞”和警告级别的“本地路径暴露”，如果有网站的某个目录同时存在这两个漏洞，黑客就可以在网站服务器上运行脚本后门程序，随意篡改网站内容；如果服务器操作系统又存在本地提权漏洞，黑客又可以利用漏洞使脚本后门获得系统最高权限，这意味着网站服务器的硬盘也可能被黑客格式化。

（二）拖库危害远超盗号木马

2011 年 11 月下旬，大量 MSN 用户在网上反馈遭遇盗号情况，其中有些是自己的帐号无法登录，系统提示“密码错误”，还有些用户收到 MSN 好友突然发来借钱消息，很明显是对方帐号被盗号分子恶意利用，事故发生的主要原因就在于多网站被黑客拖库。

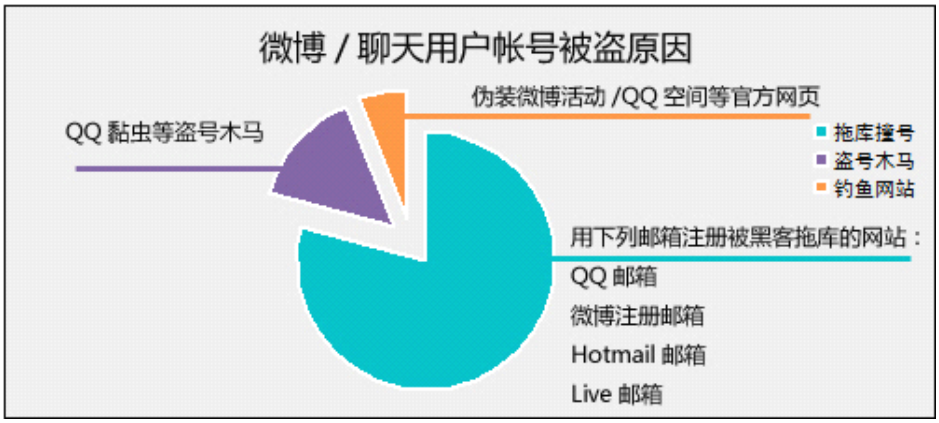
早在 360 安全中心发布的《2011 上半年安全报告》中就指出：黑客拖库（又称“刷库”）危害已远超盗号木马。也就是说，黑客入侵网站服务器、窃取用户数据库后，通常会利用其获取的大量帐号密码在网上支付等平台上试探盗号，也就是俗称的“先拖库、后撞号”。

过去数年间，国内多家大型网站均曝出被黑客拖库的消息，间接导致一些知名支付平台和微博网站相继遭到大规模撞号攻击。而在 MSN 盗号事件中，遭遇盗号的 MSN 用户大多关联的是 Hotmail 邮箱及 Live 邮箱，这两类邮箱都带有鲜明的 MSN 用户特征，因此成为黑

客重点撞号的对象。

举例来说：假设一个安全性薄弱的论坛有 10 万注册用户，这些用户的注册邮箱和密码全部被黑客从论坛服务器窃取，其中 1 万个注册邮箱是 Hotmail 邮箱和 Live 邮箱，黑客就会用这 1 万个邮箱和密码试探登录 MSN。如果其中又有 50%用户为论坛和 MSN 设置了相同的密码，就意味着黑客攻陷一个论坛可批量窃取 5000 个 MSN 帐号！

360 用户求助中心调查发现，在 QQ、MSN 等盗号重灾区，黑客拖库造成的盗号现象比例高达 80%左右，远远超过盗号木马和钓鱼网站。



（三）网站安全建议

网站安全是一个综合性多元化问题，包括系统安全、数据安全、交易平台安全等，全方位解决安全问题需要完善的管理机制和专业技术保障。360 网站安全检测平台建议，网站应该从以下三个方面提升网站的安全性：

一、强化网站安全意识

1) 由专业技术人员进行安全维护

有些网站的 WEB 程序是外包开发的，而且网站程序的开发人员没有安全编程经验，极易造成各种漏洞。

2) 及时为服务器操作系统和网站程序打好补丁

有些网站使用版本陈旧的程序，服务器操作系统也不注意更新补丁，存在大量广为人知的漏洞，当然会轻易被黑客利用入侵，成为傀儡主机。

3) 严谨的测试流程

在任何网站应用上线前，都应从安全角度进行测试，去除不必要的风险因素。在用户交互环节，更应注意控制权限，过滤可能出现的威胁。

二、定期进行网站安全检测

一些网站管理者认为，“在网络中不断部署防火墙、入侵检测系统、入侵防御系统等设备，就可以提高网络的安全性”。其实这样的认识存在误区，根本原因在于，传统的网络安全设备难以抵御应用层的攻击，最有效的网站安全解决方案是修复漏洞。

在网站安全检测方面，360 网站安全检测平台提供了集“漏洞检测”、“挂马检测”和“篡改检测”于一体的一站式免费服务平台，拥有国内最全的网站漏洞检测库及强大的蜜罐集群检测系统，并可在第一时间为高危 0day 漏洞提供修复建议。

三、实时监控网站安全状况

网站被挂马或篡改，不仅会降低用户对其的信任度，更严重危害网络安全或造成不良影响。此外，360 网站安全检测平台提供了实时的挂马监控和篡改监控功能，一旦发现网站被挂马或被篡改，能够自动以邮件等方式通知站长，将网站蒙受损失的风险降到最低。