4 “您访问的网站安全吗？”—网站安全监测情况

4.1网页篡改情况

自 2003 年起，CNCERT 持续监测、跟踪和分析境内网站被篡改情况，在发现重要网站被篡改后及时通知网站所在省份的分中心协助处理，争取快速恢复被篡改网站。

■ 境内网站被篡改总体情况

2010 年，CNCERT 监测到境内被篡改网站月度统计情况如图 4-1 所示。其中，每月被篡改网站数量平均为 2904 个。11 月、12 月，CNCERT 增强了对互联网上从事网页篡改活动较为活跃的黑客群体的监测，并将一类新型网页篡改攻击事件，即以非授权的方式挂载非法网站链接（俗称“黑链”）纳入监测范围，使得 11 月、12 月监测到的被篡改网站数量出现较大幅度的增加。关于挂载“黑链”类网页篡改攻击的具体特点，参见本章“网站篡改攻击行为分析”一节。

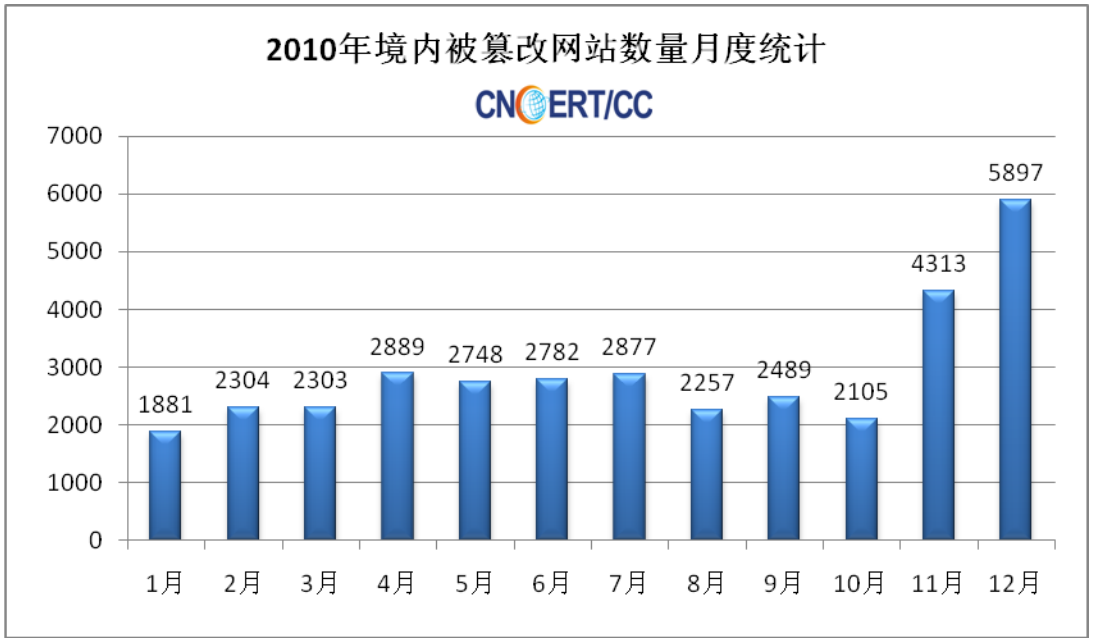


图 4-1　2010 年境内被篡改网站数量月度统计

如图 4-2 所示，2010 年境内被篡改网站按域名类型进行统计，被篡改数量最多的是.com 和.com.cn 类域名网站，其多为企业、公司网站。不过值得注意的是，.gov.cn 域名网站所占比例达到 13.30%，.org.cn 所占比例达到 1.76%，.edu.cn 域名网站所占比例达到 1.15%。

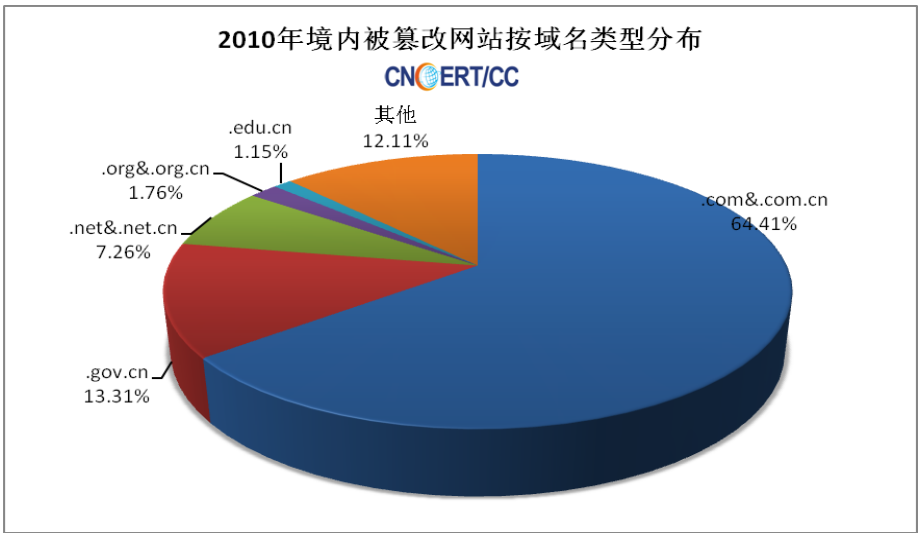


图 4-2　2010 年境内被篡改网站按域名类型分布

如图 4-3 所示，2010 年境内被篡改网站按地域进行统计，排行前十位的地区分别是：北京市、江苏省、广东省、福建省、上海市、浙江省、河南省、四川省、安徽省和湖北省。其中前六位与 CNNIC2011 年 1 月发布的境内分省网站数量的前六位一致[1]。

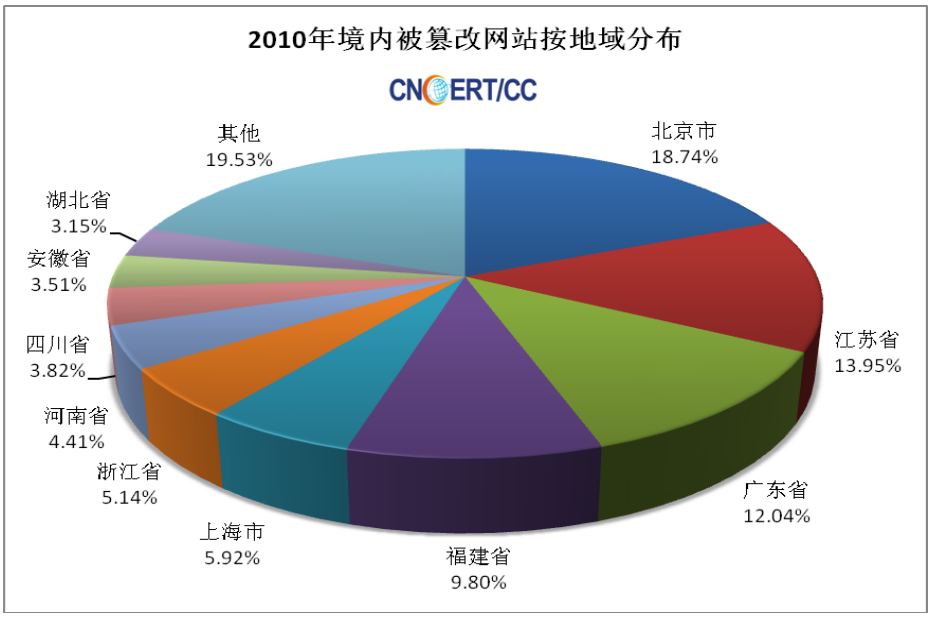


图 4-3　2010 年境内被篡改网站按地域分布

■ 境内政府网站被篡改情况

2010 年，境内政府网站被篡改数量为 4635 个，与 2009 年的 2765 个相比增加 67.6%。在 CNCERT 监测的政府网站列表中，2010 年被篡改的政府网站

[1] 根据中国互联网络信息中心（CNNIC）2011 年 1 月发布的《第 27 次中国互联网络发展状况统计报告》，分省网站数量排名前六位分别是广东、北京、上海、浙江、江苏、福建。

比例达到 10.3%，即全国有十分之一的政府部门网站遭遇黑客篡改。2010 年境内被篡改政府网站数量及其占境内被篡改网站总数的比例月度统计如图 4-4 所示。

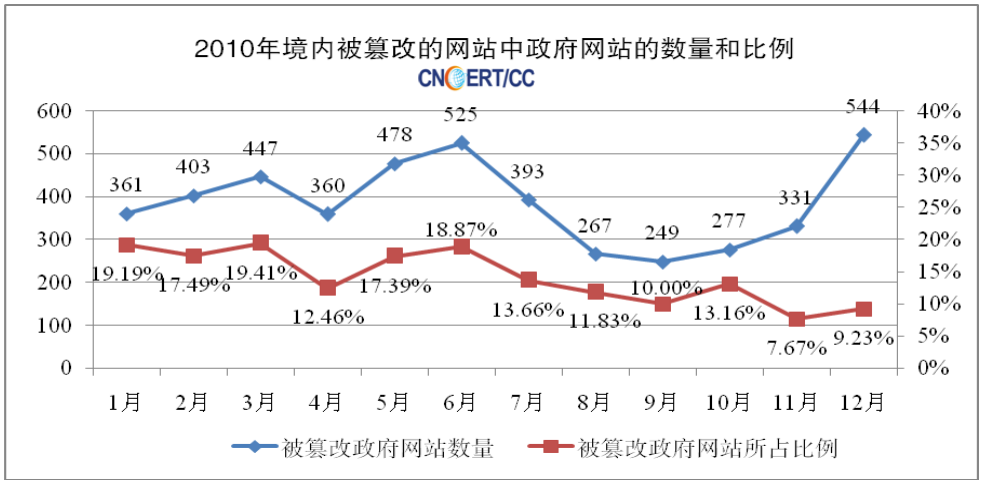


图 4-4 2010 年境内被篡改的网站中政府网站的数量和比例

政府网站易被篡改的主要原因是网站整体安全性差，缺乏必要的经常性维护，某些政府网站被篡改后长期无人过问，还有些网站虽然在接到报告后能够恢复，但并没有根除安全隐患，从而遭到多次篡改。表 4-1 所示为 CNCERT 监测发现的 2010 年被篡改的部分重要政府网站列表。

表 4-1 2010 年 CNCERT 监测发现被篡改的部分省部级政府网站列表

网站所属部门	被篡改页面 URL	监测时间
国家广播电影电视总局电影数字节目管理中心	http://www.dmcc.gov.cn	2010-2-7
福建省财政厅	http://rc.fjkj.gov.cn/ndh.htm	2010-2-15
四川省民政厅	http://scmz.gov.cn/index.htm	2010-2-24
中国气象局	http://training.cma.gov.cn	2010-2-25
最高人民检察院	http://fdzqq.spp.gov.cn	2010-5-8
中国人民共和国商务部对外贸易司	http://ibdaily.mofcom.gov.cn	2010-5-8
国家发改委宏观经济发展研究院	http://www.amr.gov.cn	2010-5-26
安徽省交通厅	http://shangbao.ahjt.gov.cn/index.htm	2010-6-1
福建省安全生产监督管理局	http://www.fjsafety.gov.cn/ImageUpload/agresif.htm	2010-6-10
河北省气象局	http://www.heblp.gov.cn/index.htm	2010-7-13
中华人民共和国水利部	http://www.mwr.gov.cn/wasdemo/test.jsp	2010-7-22
中华人民共和国国土资源部	http://wcm.mlr.gov.cn/mail/test.jsp	2010-7-22
中华人民共和国国防部	http://search.mod.gov.cn/wasdemo/test.jsp	2010-7-22
贵州省林业厅	http://www.gzforestry.gov.cn/index.htm	2010-8-13
中国人寿保险公司	http://dgmsa.gov.cn/index.php	2010-8-23
新疆维吾尔自治区粮食局	http://www.xjgrain.gov.cn/index.htm	2010-9-1
宁夏回族自治区商务厅	http://www.nxdofcom.gov.cn/indonesia.htm	2010-9-30

吉林省住房和城乡建设厅	http://www.jljsw.gov.cn/indonesia.htm	2010-9-30
贵州省公安厅	http://tp.gzga.gov.cn/index.htm	2010-11-15
广西自治区出入境检验检疫局	http://caexpo.gxciq.gov.cn/indonesia.htm	2010-11-20
新疆维吾尔自治区扶贫办	http://xjfp.gov.cn/help.asp	2010-11-24
北京市粮食局	http://www.bjlsj.gov.cn/ina.htm	2010-12-28

■ 网站篡改攻击行为分析

2010 年对境内网站进行网页篡改攻击数量最多的前 20 位的攻击者如表 4-2 所示。其中，疑为来自境外的攻击者有 8 名。

表 4-2 2010 年 CNCERT 监测到的篡改境内网站按数量排行 TOP 20 的攻击者

排名	攻击者名称	篡改网站数量(个)	攻击者所属国家
1	ZoRRoKiN	711	土耳其
2	aGReSiF	646	土耳其
3	Cracker-Mr.X	462	中国
4	Timeless	459	未知
5	王可欣	456	中国
6	iskorpitx	410	土耳其
7	冰鱼	383	中国
8	s4r4d0	346	葡萄牙
9	Hmei7	324	印度尼西亚
10	小云	296	中国
11	流浪汉	292	中国
12	Joker	244	土耳其
13	幽浮ぐ潜入	228	中国
14	夜猫子	223	中国
15	HEXB00T3R	172	土耳其
16	木鱼工作室	166	中国
17	qq1281232825	163	中国
18	3n_byt3	143	印度尼西亚
19	Trotou	129	中国
20	QQ120244818 接单收徒	125	中国

上述攻击者发起网页篡改的攻击动机可以分为三类：第一类是出于政治、宗教目的，如：ZoRRoKiN 和 aGReSiF 经常将境内政府部门网站作为重点攻击目标，攻击成功后通常会在网站留下宣扬其政治、宗教理念的文字或图片，相关示例如图 4-5 所示；第二类是出于技术炫耀目的，如图 4-6 所示，攻击者篡改网站成功后留下大名，并留有调侃风格的文字或图片；第三类则是在网站上留存后门页面，如图 4-7 所示，一是方便其以后再次进入，二则不排除其将该后门用于地下交易牟取非法利益的可能。

图 4-5　黑客篡改网站后留下的页面图例一(攻击者：aGReSiF)

图 4-6　黑客篡改网站后留下的页面图例二（攻击者：卖火机的男孩）

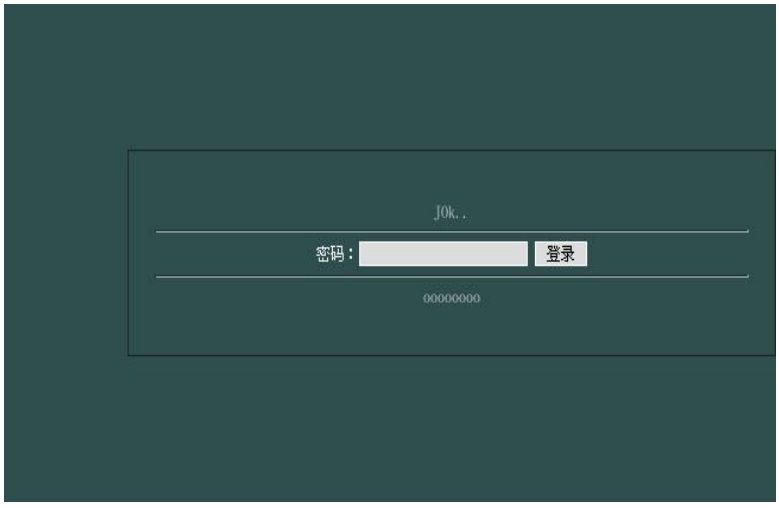


图 4-7　黑客篡改网站后留下的页面图例三（攻击者：J0K）

CNCERT 还对互联网中大量存在的所谓“广告联盟”组织进行跟踪分析，发现

一些“广告联盟”幕后组织者利用网站的安全漏洞，在网站上（通常为首页面）嵌入和挂载大量网站链接，以达到通过增加网站点击流量非法牟利的目的。如图 4-8 所示，攻击者不仅以非授权的方式挂载非法网站链接（俗称“黑链”），并且留下文字变相地威胁网站所属部门。

2010 年 11 月、12 月，CNCERT 对“广告联盟”挂载的网游私服网站、网游外挂网站、网络博彩网站等三类链接特征进行了监测，对应监测到的被挂载黑链的受害网站约占被篡改网站总数的 37%。此外，CNCERT 对黑链产业进行了初步的摸底调研，一些“广告联盟”的组织者对在各类域名上挂载“黑链”的活动进行明码标价。其中，在.gov.cn、.edu.cn、.org、.org.cn 等站点挂“黑链”的收费较高，这有两方面原因：一是上述各类域名在搜索引擎检索时权重值较高，二是政府、高校、事业单位和公益组织的网站在安全管理方面更可能存在疏漏，黑链存活的时间较长。综合上述情况看，由这些“广告联盟”一手导致的网页篡改（或称网页挂载黑链）事件已经成为诸多政府部门、高校和公司企业网站安全的重要威胁。

```
<div style="position: absolute; top: -999px;left: -999px;">
友情提示：<!--请站长不要删我的链接，只是挂个链，对你的站没有影响，也不会破坏你的站，我还在帮你维护你的站！
<a title="香港六合彩" target="_blank" href="http://288ok.com">香港六合彩</a>
<a title="六合彩开奖" target="_blank" href="http://www.6666ok.info">六合彩开奖</a>
<a title="香港六合彩" target="_blank" href="http://www.99958.info">香港六合彩</a>
<a title="六合彩资料" target="_blank" href="http://www.jt558.info">六合彩资料</a>
<a title="香港六合彩" target="_blank" href="http://93368.com">香港六合彩</a>
<a title="六合彩开奖" target="_blank" href="http://www.dtt888.com">六合彩开奖</a>
<a title="六合彩资料" target="_blank" href="http://www.loneve.com">六合彩资料</a>
<a title="六合彩资料" target="_blank" href="http://www.666789.info">六合彩资料</a>
<a title="六合彩开奖" target="_blank" href="http://www.888889.info">六合彩开奖</a>
<a title="香港六合彩" target="_blank" href="http://www.533788.info">香港六合彩</a>
</div>

<title>广州市番禺区财政局</title>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<style type="text/css">
<!--
.txt12 {  font-size: 12px}
.txt14 {  font-size: 14px; line-height: 20px}
-->
</style>
</head>
<link rel="stylesheet" href="/css.css" type="text/css">
<body leftmargin="0" topmargin="0" marginwidth="0" marginheight="0" background="../bg2.jpg">
<div align="center">
  <table border="0" cellspacing="0" cellpadding="0" height="477">
    <tr>
      <td><object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000" codebase="http://download.macromed
          <param name=movie value="../zhu/topn.swf">
          <param name=quality value=high>
          <embed src="../zhu/topn.swf" quality=high pluginspage="http://www.macromedia.com/shockwave/down
```

图 4-8 “广告联盟”在受害网站放置的“黑链”

4.2 网页挂马情况

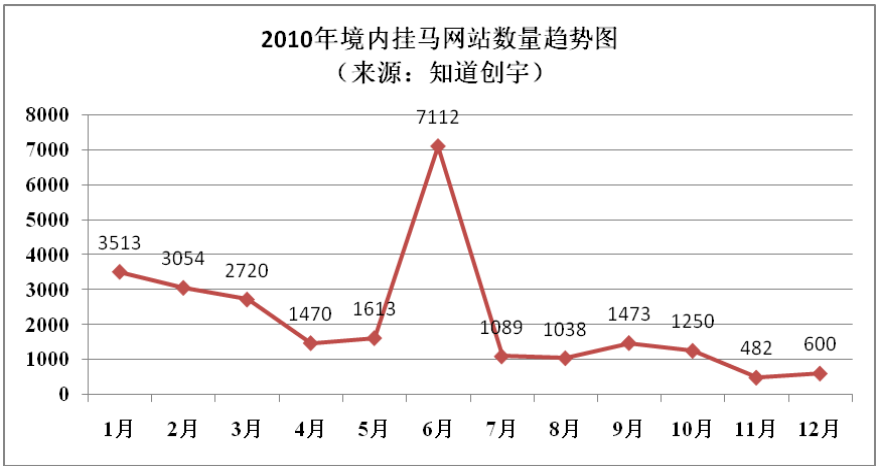
网页挂马是目前互联网黑色地下产业中进行最为猖獗的、对互联网安全危害较为严重的非法活动。一些针对新披露的信息安全漏洞制造的新型恶意代码往往会借网页挂马的方式进行大规模传播；网络中一些搜索热词或社会热点事件的出

现引发了网民大量搜索和点击，相关页面也容易被黑客利用来挂马，达到快速传播恶意代码并控制大量用户主机的目的。网页挂马是揭开互联网黑色地下产业链黑幕的重要一环，是 CNCERT 监测的重点目标。政府和重要信息系统部门、访问量较大的网站被挂马事件，以及网页挂马相关的恶意域名同时也是 CNCERT 事件处置的重点[2]。

在通信行业互联网网络安全信息通报工作中，有多家安全企业定期向 CNCERT 报告网页挂马情况[3]，与 CNCERT 建立了良好的协作关系。对挂马网站及恶意域名信息的获取，安全企业主要通过两种途径：一是通过主动巡检的方式，对设定的目标网站进行遍历、抓取相关页面后研判分析得到；二是通过企业安全防护软件产品客户端进行拦截捕获；两种方式都能有效地掌握当前网站安全及用户访问网站安全的相关情况。本报告主要关注境内网站被挂马及恶意域名威胁情况。

■ 挂马网站监测情况

根据知道创宇公司、奇虎 360 公司、网御星云公司的监测数据，2010 年境内网页挂马情况呈现先扬后抑的趋势，各公司监测到的挂马网站（页面）数量在 5 月或 6 月份间出现全年最高点，而在下半年数量逐渐下降。如图 4-9、4-10、4-11 所示。此外，根据知道创宇公司对全国 200 余万个网站的监测结果，如图 4-12 所示，境内挂马网站数量按地域统计前十位分别是北京市、江苏省、广东省、浙江省、上海市、福建省、安徽省、山东省、湖北省和四川省。



[2] 2010 年在 CNCERT 组织的木马和僵尸网络多次专项治理行动中，恶意域名作为一项重要治理内容，由 CNCERT 协调 CNNIC、中国万网、新网互联、新网数码、东南融通、希网网络等域名注册管理和服务机构进行清除。

[3] 每月或每周定期向 CNCERT 报送网页挂马信息的安全企业有：微软公司、北京神州绿盟科技有限公司、北京网御星云信息技术有限公司、奇虎 360 软件（北京）有限公司、华为技术有限公司、北京知道创宇信息技术有限公司、哈尔滨安天信息技术有限公司、北京天融信科技有限公司、金山网络科技有限公司、北京启明星辰信息技术有限公司、沈阳东软软件股份有限公司、浪潮集团有限公司、北京安信华科技有限公司。

图 4-9　2010 年境内挂马网站数量趋势（来源：知道创宇）

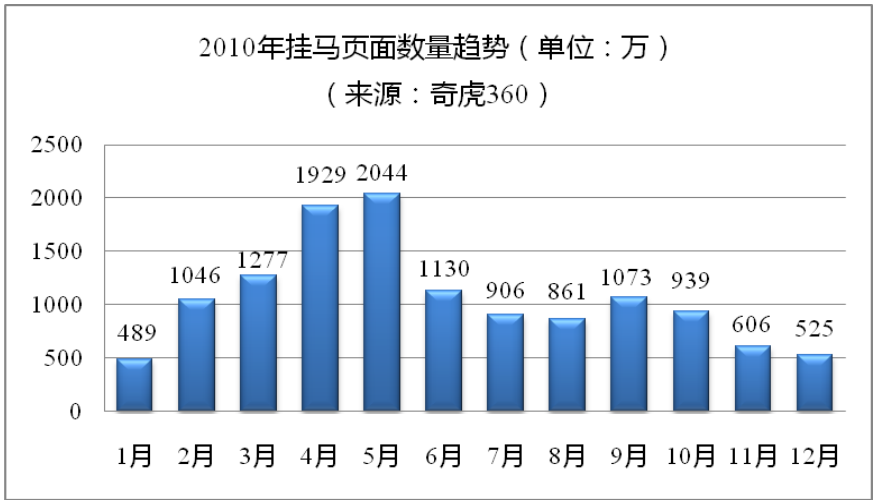


图 4-10　2010 年挂马页面数量趋势（来源：奇虎 360）

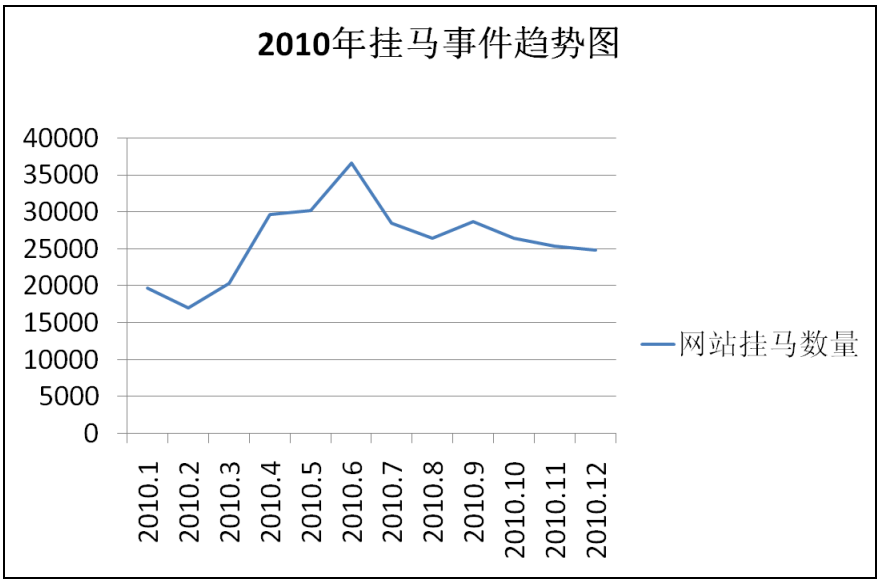


图 4-11　2010 年挂马事件数量趋势（来源：网御星云）

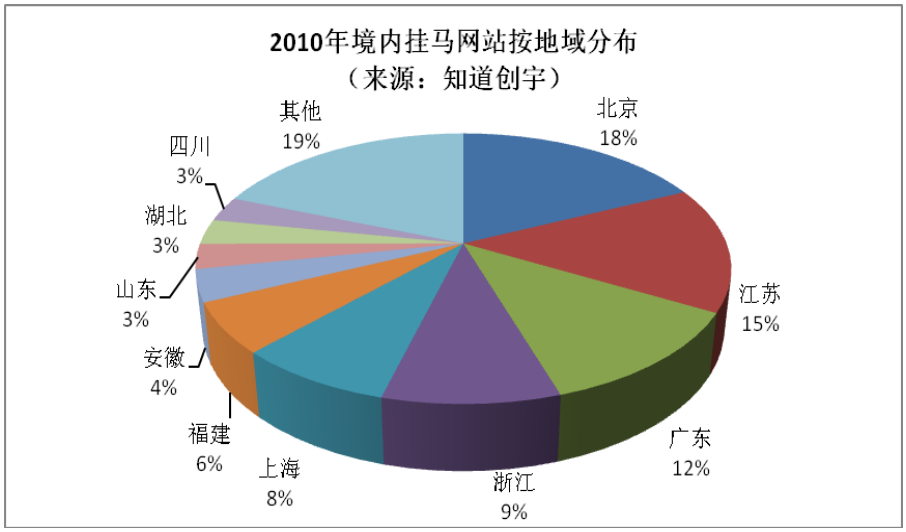


图 4-12　2010 年境内挂马网站按地域分布（来源：知道创宇）

■ 恶意域名监测情况

恶意域名是黑客进行网页挂马的重要资源。挂马网站数量反映的是黑客对网站的侵害情况以及对用户的威胁情况,而恶意域名的活跃情况则进一步反映了攻击者进行挂马攻击的能力。如表 4-3 所示,黑客注册了类似 7766.org、8866.org 等动态域名用于传播网页木马。

表 4-3　用于网页挂马的恶意域名 TOP10（来源：安天公司）

排名	恶意域名
1	www.w22rt.com
2	annil.8866.org
3	a.ppmmoo.cn
4	lsrc.cn
5	vod123.8866.org
6	ferrari10.7766.org
7	jjeffyfc19.info
8	web.9bic.net
9	ghtoto.3322.org
10	ada.bij.pl

2010 年 CNCERT 对境内外活跃的恶意域名进行了分类跟踪，发现侵害我国境内网站和用户的恶意域名主要有以下几组,如表 4-4 所示。从下表也可以看出，目前，侵害我国网站的恶意域名其注册商主要为境外机构。

表 4-4　用于网页挂马的恶意域名组（来源：CNCERT）

2010 年侵害境内网站的恶意域名组	
组别	**恶意域名组特征和数量描述**
第一组	注册在 inc.0rg.fr、conna.dtdns.net、officea.ze.tc 等域上的恶意域名，主要用于构建恶意跳转链接,每周监测发现的三级域名数量以数十、数百计。注册商为境外机构。
第二组	注册在 2288.org、3322.org、8800.org、8866.org、9966.org 上的恶意域名，被发现用于网页挂马的各个环节，如：恶意跳转链接、网页木马集成页面、漏洞触发页面以及恶意代码下载服务器，每周监测发现的三级域名数量以数百计。注册商主要为境内机构。
第三组	注册在 xorg.pl 域上的恶意域名,主要用于构建恶意跳转链接,每周监测发现的三级域名数量以数十计，6 月份之后活跃程度有所下降。注册商为境外机构。
第四组	注册在 wwvv.us 域上的恶意域名 ,三级域名前缀经常采用境内外知名站点,特征明显,每周监测发现的三级域名数量约为 10 余个,活跃周期较长,侵

	害的网站数量均较大。注册商为境外机构。
第五组	注册在 isgre.at、rr.nu 域上的恶意域名，三级域名命名呈现有规律的按字母顺序变换，用于构建恶意跳转链接，每周监测发现的三级域名数量以数十计。注册商为境外机构。
第六组	注册在.info 域上的恶意域名，三级域名命名为“单字母+含 2012 字符串+.info”形式，用于构建恶意跳转链接，每周监测发现的三级域名数量以数十计甚至上百。注册商为境外机构。
第七组	注册在 25u.com 域外的恶意域名，三级域名命名呈现有规律的按字母顺序变换，用于构建恶意跳转链接，每周监测发现的三级域名数量以数十计。注册商为境外机构。

■ 网页挂马攻击特点

对于网页挂马攻击的行为特点，首先通过一个挂马事件案例进行说明。2010 年 9 月 6 日，CNCERT 监测发现某电视台网站存在挂马页面，当用户访问相关页面时，系统会自动执行黑客嵌入的恶意链接或恶意脚本。在用户主机存在相关操作系统或应用软件漏洞，又没有做好安全防护的情况下，会感染黑客放置的恶意代码。黑客借此可以控制用户主机，进而窃取用户私密信息。黑客挂马的技术步骤如表 4-5 所示。

表 4-5　一个挂马事件案例（来源：CNCERT）

步骤	说明
第一步	利用网站漏洞取得相关权限，嵌入恶意跳转链接 [root]http://www.qhstv.com/Style/dm/dm.html （被挂马页面） [script]http://www.cdzgh.com/uploadfiles/admin.js （跳转页面）
第二步	通过恶意跳转链接，跳转至漏洞触发页面 [iframe]http://www.cdcc.gov.cn/css/test1test.html （MS10-018 漏洞）
第三步	漏洞触发条件执行成功，取得用户主机权限，自动下载带有远程控制或窃取信息等功能的恶意代码 [script]http://www.cdcc.gov.cn/css/pack.js（跳转页面） [script]http://www.cdcc.gov.cn/css/pack.css （跳转页面） [exe]http://www.cdcc.gov.cn/css/dmlq123.exe（恶意代码下载链接）
第四步	在用户主机上执行下载的恶意代码

通过利用操作系统和应用软件漏洞，特别是利用最新披露的零日漏洞进行挂马是黑客常用的攻击手段，图 4-13 所示为 2010 年监测到的网页挂马利用的漏洞情况。2010 年出现的高危漏洞如“极光”漏洞（CVE-2010-0249）、“极风”漏洞（CVE-2010-0806）、CVE-2010-3962 漏洞，在漏洞披露的短时间内，CNCERT

以及各安全企业就监测到大量利用相关漏洞进行挂马攻击的事件。此外，由于一些用户疏于防范，对于一些较早就披露的漏洞并未进行及时的修复。黑客仍然利用这些漏洞进行挂马，并且造成的危害也不小。例如，2006 年微软操作系统发布的安全公告 MS06-014 中修复的漏洞仍被大量挂马攻击所利用。

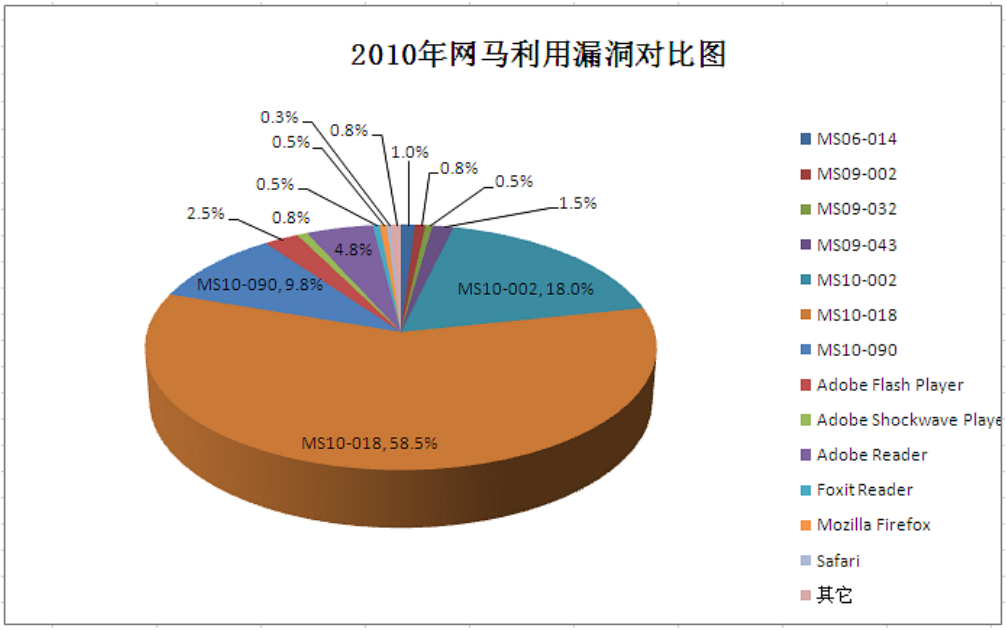


图 4-13　2010 年网页挂马利用的漏洞列表（来源：安天公司）

4.3网页仿冒情况

网页仿冒俗称网络钓鱼，这类事件是社会工程学欺骗原理结合网络技术的典型应用。2010 年 CNCERT 共接到网页仿冒事件报告 1566 件，经归类合并后 CNCERT 成功处理了 631 件。在 CNCERT 接收到的这些网页仿冒事件中，被仿冒的大都是电子商务网站、金融机构网站、第三方在线支付站点、社区交友网站。表 4-6 列出了 CNCERT 接收到的按事件次数排名前十位的被仿冒网站。

表 4-6　2010 年 CNCERT 接收到被仿冒网站 TOP10

2010 年 CNCERT 接收到的被仿冒网站按事件次数 TOP10	
被仿冒网站	次数
bbva.com（毕尔巴鄂比斯开银行）	170
ebay.com（美国电子商务网站）	134
bradesco.com.br（巴西布拉德斯科银行）	127
Hsbc.com.cn（中国香港汇丰银行）	115
I irs.gov（美国国家税务局）	73
wachovia.com（美国瓦霍维亚银行）	71
alliance-leicester.co.uk（英国联合莱斯特银行）	57
Icbc.com.cn（中国工商银行）	51
cctv.com（中国中央电视台）	51
ceca.es（西班牙储蓄银行联盟）	37