4　网站安全监测情况

4.1网页篡改情况

自 2003 年 CNCERT 便开始每日对中国大陆地区网站被篡改情况进行跟踪监测，在发现被篡改网站后及时通知网站所在省份的分中心协助解决，争取被篡改网站快速恢复。

■ 中国网站被篡改总体情况

2011 年，中国大陆地区被篡改网站各月累计为 36612 个，与 2010 年的 34858 个相比略增 5.1%。2011 年，CNCERT 监测到中国境内（大陆地区）被篡改网站月度统计情况如图 4-1 所示，总体呈现下降趋势。2011 年，中国大陆地区被篡改网站按域名去重后为 15443 个。

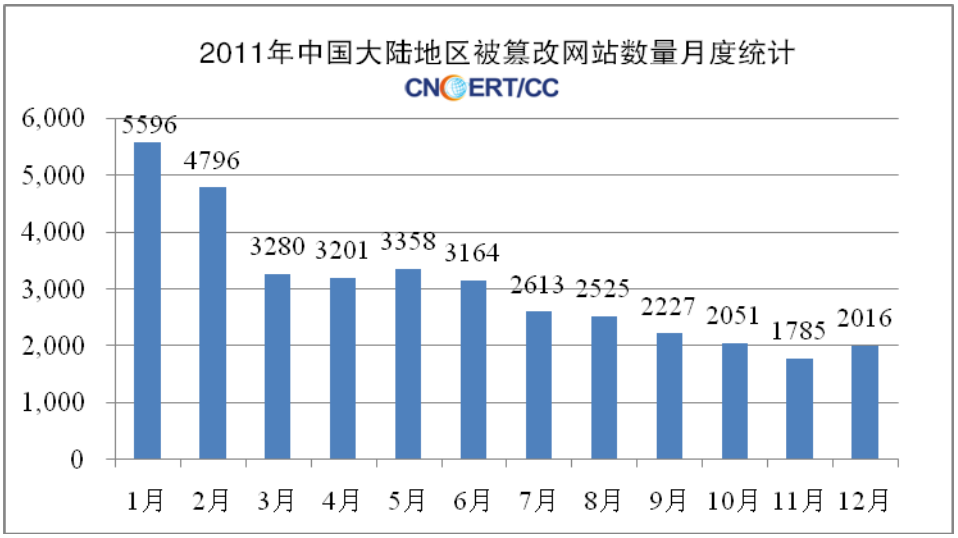

图 4-1　2011 年中国大陆地区被篡改网站数量月度统计

根据域名类型进行统计，如图 4-2 所示，2011 年中国大陆地区被篡改网站中，被篡改最多的是.com 和.com.cn 等域名网站，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 9.6%，.org.cn 所占比例达到 1.9%，.edu.cn 域名网站所占比例达到 1.0%。在 CNCERT 监测的网站数量中，上述三类域名网站的占比分别为 2.94%、0.54%、0.18%，量化后的被篡改概率指数分别为：3.27、3.44、9.9[11]，这说明政府部门、公益组织、教育机构网站的安全防护较为脆弱，

[11] CNCERT 定义的网站被篡改概率指数=CNCERT 监测发现的该类网站被篡改数量比例/CNCERT 对该类网站监测的数量比例。概率指数越大，则该类网站相对被篡改的概率就越大。概率指数主要用于反映网站的脆弱性和黑客攻击时的目标选择喜好。

容易成为黑客篡改的目标。

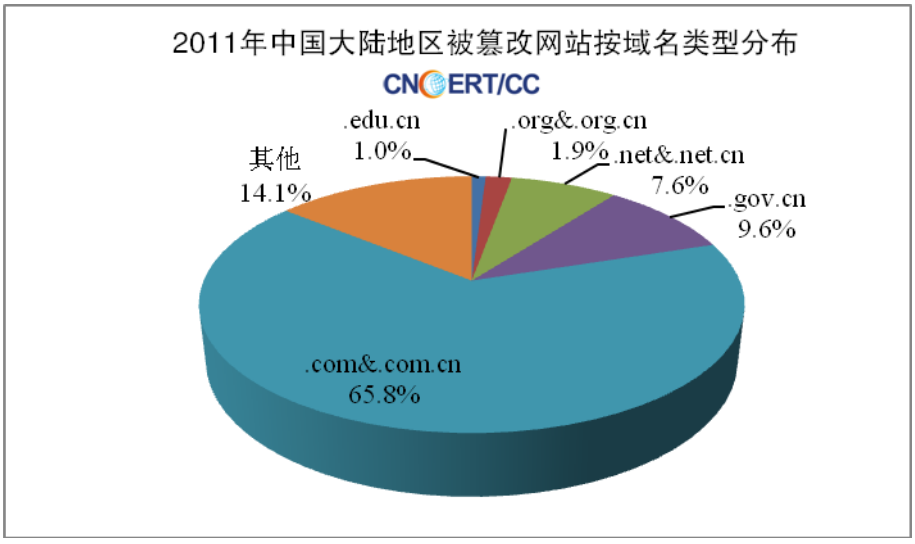

图 4-2　2011 年中国大陆地区被篡改网站按域名类型分布

如图 4-3 所示，2011 年中国大陆地区被篡改网站按地域进行统计，排行前十位的省份分别是：北京市、江苏省、广东省、福建省、上海市、河南省、浙江省、四川省、安徽省、湖北省。与 2010 年监测情况比，前十位省份均在列，上述省份为我国互联网发展状况较好的地区。

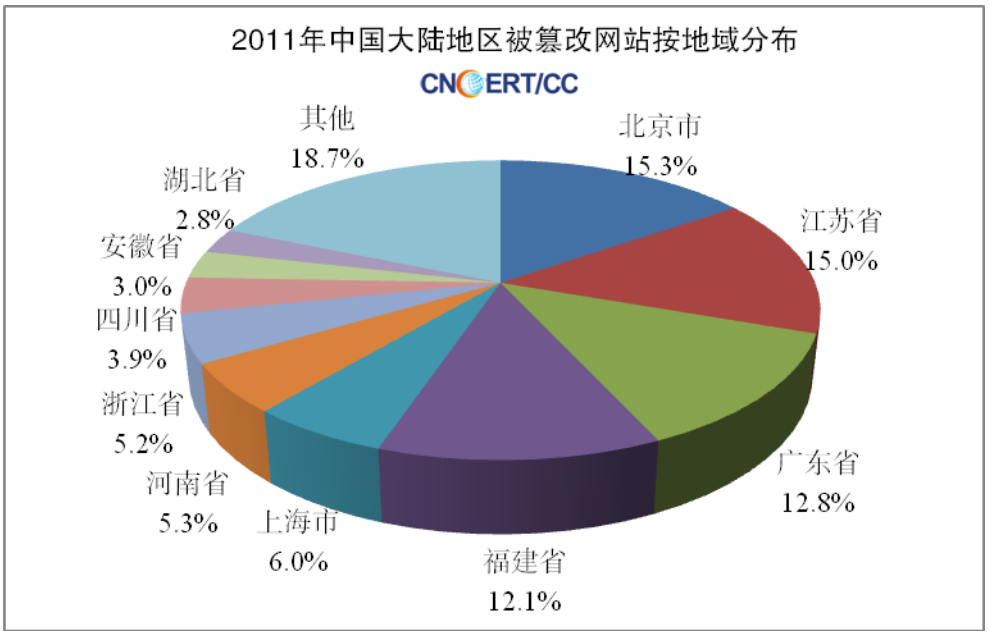

图 4-3　2011 年中国大陆地区被篡改网站按地域分布

■ 中国大陆地区政府网站被篡改情况

2011 年，中国大陆地区政府网站被篡改数量各月累计为 2807 个，与 2010 年的 4635 个相比下降 39.4%，按域名去重后为 1484 个，在 CNCERT 监测的政府网

站列表中所占比例达到 3.4%。

2011 年中国大陆地区被篡改的网站中政府网站的数量和占被篡改网站总数的比例月度统计如图 4-4 所示。

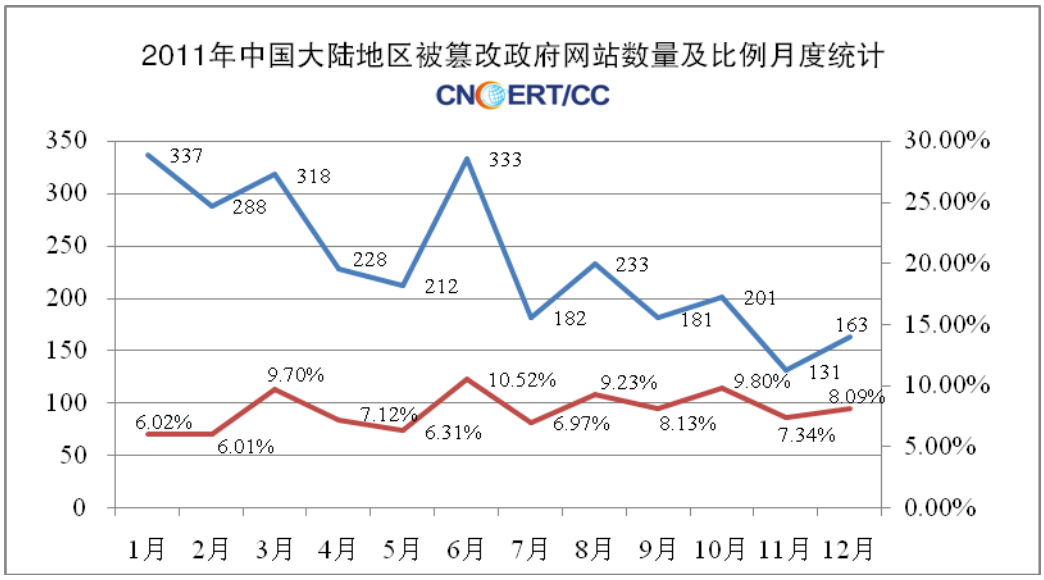

图 4-4　2011 年中国大陆被篡改的网站中政府网站的数量和比例月度统计

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 2011 年被篡改的部分省部级政府网站列表。

表 4-1 2011 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	被篡改后的 URL	监测时间
黑龙江省水利厅	http://www.hljsl.gov.cn/hack1990.txt	2011/1/4
中国气象局大气成分观测与服务中心	http://www.cawas.cma.gov.cn/cawasweb/zxl.txt	2011/1/4
福建省地震局	http://www.fjea.gov.cn/admin/Upload_File//%20simon.txt	2011/1/12
宁夏回族自治区金融管理办公室	http://www.nxjr.gov.cn/ina.htm	2011/1/16
江西省制造业信息化网	http://www.jxmie.gov.cn/ina.htm	2011/1/19
贵州省旅游局	http://www.gz12301.gov.cn/dflzjslyb/index.asp	2011/1/20
湖北省防汛抗旱指挥部办公室	http://www.hbfxb.gov.cn/index.htm	2011/1/31
安徽省交通厅	http://zhuanjia.ahjt.gov.cn/default.asp	2011/2/4
安徽省交通厅	http://ahjt.gov.cn/default.asp	2011/2/4
安徽省交通厅	http://shangbao.ahjt.gov.cn/default.asp	2011/2/5
安徽省交通科学研究所	http://jtkx.ahjt.gov.cn/default.asp	2011/2/5
安徽省交通厅	http://chaxun.ahjt.gov.cn/default.asp	2011/2/6
青海省招商局	http://qhwit.gov.cn	2011/2/13
四川省标准化研究院	http://tiaoma.scbzhy.gov.cn/index.php	2011/2/13
国务院南水北调工程建设委员会	http://www.nsbd.gov.cn/others/gzlx/gzlx.htm#1	2011/2/18

甘肃省直机关工委	http://www.szgw.gansu.gov.cn/index.htm	2011/3/4
青海省公安交通管理局	http://jjzd.qhga.gov.cn/indonesia.htm	2011/3/13
江西省劳动就业服务管理局	http://jxjy.gov.cn/index.htm	2011/4/3
宁夏回族自治区统计局	http://www.nxtj.gov.cn/jgzn/	2011/4/19
教育部语言文字应用研究所	http://www.china-language.gov.cn/xiaozan.html	2011/5/11
天津市人民政府人民防空（民防）办公室	http://www.tjrf.gov.cn/w.txt	2011/5/16
山东省经济和信息化委员会	http://miisd.gov.cn	2011/5/23
黑龙江省档案局	http://www.hljdaj.gov.cn/cert/wlpage/wl716wb502.html	2011/6/13
陕西人民教育出版社	http://www.sxxwcb.gov.cn/bk/post/285.html	2011/6/17
广西自治区老领委	http://www.gxllw.gov.cn/wsly/index_main.asp?page3	2011/6/26
福建省信息化局	http://fjtwit.gov.cn/index.htm	2011/8/14
山东省监察厅	http://www.mirror.gov.cn/index.htm	2011/8/20
四川省测绘地理信息局	http://scbsm.gov.cn/index.htm	2011/8/21
江西省委政法委员会	http://www.jxzfw.gov.cn/tzzwd/index.asp	2011/8/29
内蒙古自治区测绘事业局	http://www.nmgch.gov.cn/htm/xczl/default.htm	2011/8/29
安徽省省直住房公积金网	http://www.ahgjj.gov.cn/prince.html	2011/8/30
安徽省省直住房公积金网	http://ahgjj.gov.cn/index.htm	2011/9/7
宁夏回族自治区商务厅	http://www.nxdofcom.gov.cn/INDEX.HTML	2011/9/18
新疆维吾尔自治区关工委	http://www.xjggw.gov.cn/admin\Databackup\semeng.txt	2011/9/21
湖北省安全生产监督管理局	http://hubeisafety.gov.cn/index.htm	2011/9/29
黑龙江省制造业信息化服务平台	http://www.hljzzy.gov.cn/index.htm	2011/9/30
陕西省中小企业促进局	http://www.smte.gov.cn/tr-x.txt	2011/10/26
湖北省企业上市领导小组办公室	http://www.hbssb.gov.cn/index.htm	2011/11/7
江苏省民防局	http://www.jsrf.gov.cn/RSS/	2011/11/27
海南省安全生产监督管理局	http://www.hnsajj.gov.cn/news/	2011/12/17
陕西省测绘局	http://www.shasm.gov.cn/xuehui/View.asp	2011/12/22
湖南省林业厅	http://rsjy.hnforestry.gov.cn	2011/12/24
安徽省省直住房公积金网	http://ahgjj.gov.cn/index.htm	2011/12/24
新疆自治区出入境检验检疫局	http://www.xjciq.gov.cn//Index.asp	2011/12/30

■ 网站篡改攻击行为分析

CNCERT 对当前较为活跃的篡改网站的攻击者进行了跟踪，2011 年对中国大陆地区网站进行网页篡改攻击数量最多的前 20 位攻击者如表 4-2 所示。其中，境外攻击者有 5 名。

表 4-2　2011 年 CNCERT 监测到的篡改中国大陆地区网站按数量排行 TOP20 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	soojoy	900	中国
2	s4r4d0	468	葡萄牙
3	Link	261	中国
4	冰寒	231	中国
5	QQ:124320170	197	中国
6	ZoRRoKiN	160	土耳其
7	Ashiyane Digital Security Team	158	土耳其
8	iskorpitx	113	土耳其
9	Cracker-Mr.X	113	中国
10	qq1281232825	111	中国
11	Bð12812	100	中国
12	twy	83	中国
13	HLck	75	中国
14	haaie	69	中国
15	hack1990	68	中国
16	linux	65	中国
17	By_aGReSiF	59	土耳其
18	Dirk	54	中国
19	hu1s4	52	中国
20	卖菜的大婶	50	中国

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程序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，达到快速传播恶意程序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的事件，以及网页挂马相关的恶意域名是 CNCERT 事件处置的重点。

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，与 CNCERT 建立了良好的协作关系。安全企业主要通过两种途径获取挂马网站及恶意域名信息：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。

■ 挂马网站监测情况

根据知道创宇公司[12]、奇虎 360 公司、安天公司、网御星云公司[13]和金山网络公司的监测数据，2011 年中国大陆地区网页挂马较 2010 年相比活跃度呈下降趋势。随着国家主管部门对传播恶意程序行为的不断治理和打击，网页挂马在黑色地下产业链中的运作成本日益增强，黑色地下产业从业者逐步转向其他趋利性更强的活动。如图 4-5、4-6、4-7 所示，分别为知道创宇公司、奇虎 360 公司、安天公司监测的挂马网站数量趋势图。此外，根据知道创宇公司对全国网站的监测结果，如图 4-8 所示，中国大陆地区挂马网站数量按地域统计前 10 位分别是北京市、江苏省、广东省、上海市、福建省、浙江省、四川省、山东省、湖北省、安徽省。

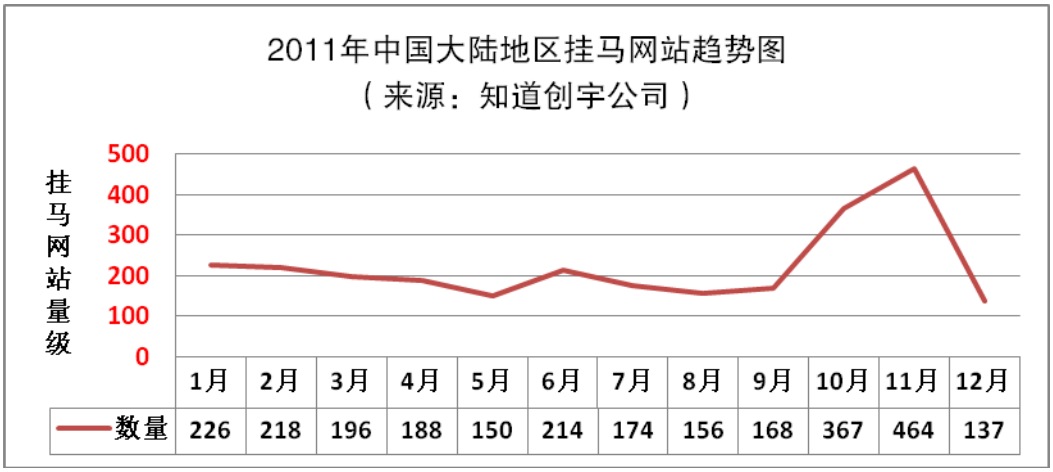

图 4-5　2011 年中国大陆地区挂马网站趋势图（来源：知道创宇公司）

[12]知道创宇公司即北京知道创宇信息技术有限公司，是通信行业互联网网络安全信息通报工作单位，同时也是 CNCERT 省级应急服务支撑单位。
[13]网御星云公司即北京网御星云信息技术有限公司，是通信行业互联网网络安全信息通报工作单位。

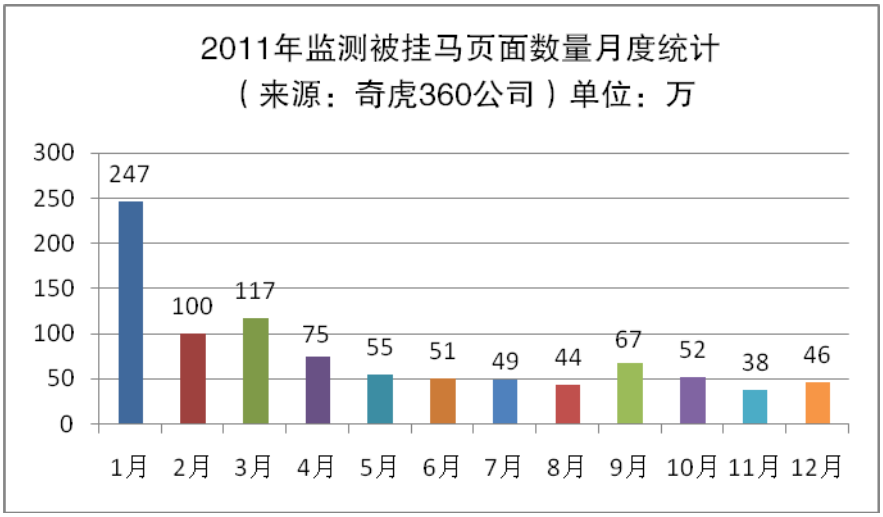

图 4-6　2011 年监测被挂马页面数量月度统计（来源：奇虎 360 公司）

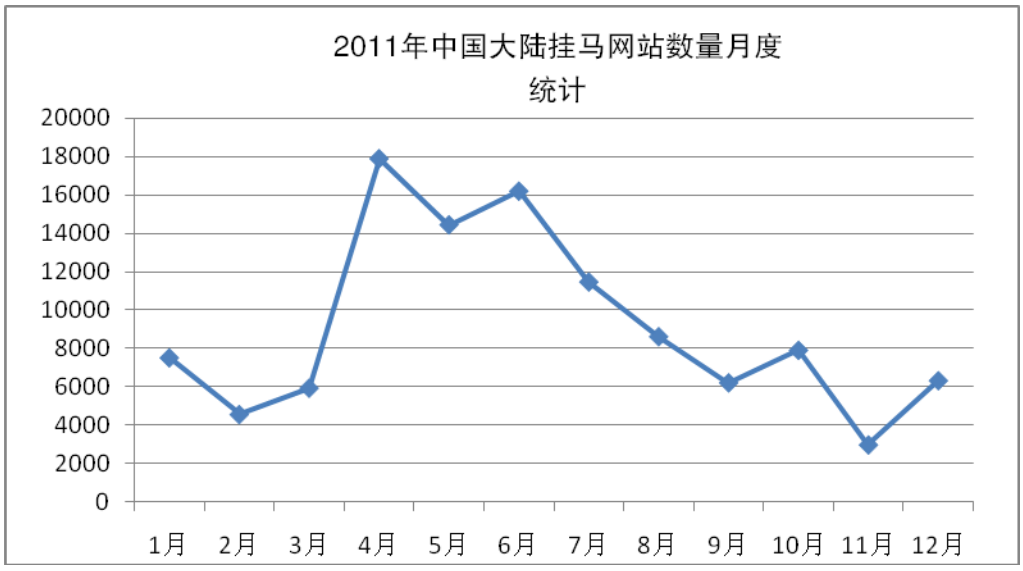

图 4-7　2011 年中国大陆挂马网站数量月度统计（来源：安天公司）

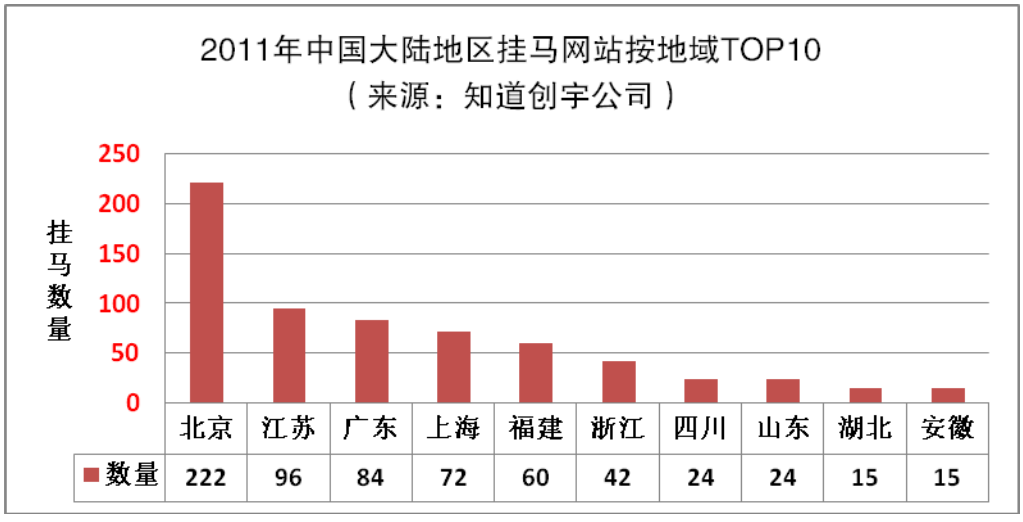

图 4-8　2011 年中国大陆地区挂马网站按地域 TOP10（来源：知道创宇公司）

■ 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反映了攻击者进行挂马攻击的能力。如表 4-3、表 4-4 所示，奇虎 360 公司和安天公司的监测结果都显示，黑客目前惯用的挂马手法是在 3322.org、8866.org 等动态域名中注册大量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：奇虎 360 公司）

挂马网站域名	相关挂马子域名数	部分挂马子域名举例
3322.org	3261	qqaazz48.3322.org ty02dngf1f.3322.org 123qwer2.3322.org
8866.org	855	360se.aq33ff.8866.org tgb1.8866.org aaahsgz11.8866.org
3-a.net	696	bdj.3-a.net anj.3-a.net ane.3-a.net
isgre.at	631	bur.isgre.at ccv.isgre.at die.isgre.at
2288.org	627	emb.2288.org dgr.2288.org epq.2288.org
0303.in	610	qqqq51.0303.in qqqq388.0303.in qqqq55.0303.in
6600.org	531	444setrj7jh5eh67k7tj.6600.org hengsan001.6600.org guangxi003.6600.org
7766.org	259	xrgth.7766.org dewe.7766.org 360sd.chunan001.7766.org
8800.org	227	bug4.8800.org aiwo225.8800.org vava12.8800.org
ns02.us	218	evb.ns02.us dyq.ns02.us eil.ns02.us

表 4-4　挂马网站（恶意域名）按子域名数排行 TOP 10 （来源：安天公司）

挂马网站域名	相关挂马子域名数	部分挂马子域名举例
3322.org	3732	y568.3322.org y65f.3322.org y6tg.3322.org
8866.org	1064	xiao1.8866.org xiao2.8866.org xiao3.8866.org
6600.org	800	zhongsanji001.6600.org zhongsanji002.6600.org zhongsanji004.6600.org
8800.org	404	ads1.8800.org ads2.8800.org ads3.8800.org
2288.org	398	eod.2288.org eog.2288.org eow.2288.org
cncshj.com	351	1a.cncshj.com 1b.cncshj.com 1c.cncshj.com
cgwx.info	300	lt.cgwx.info nk.cgwx.info nt.cgwx.info
09466.net	282	1c.09466.net 1d.09466.net 1e.09466.net
nshl.in	266	sd4.nshl.in tr4.nshl.in u6n.nshl.in
thesswws.com	155	kxkx.thesswws.com qvod.thesswws.com

■ 网页挂马攻击特点

当用户访问相关挂马页面时，系统会自动下载和执行黑客嵌入的恶意程序或恶意脚本。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程序。黑客借此可以控制用户主机，进而窃取用户私密信息。黑客挂马常用技术步骤如表 4-5 所示。

表 4-5　一个典型的挂马事件案例（来源：安天公司）

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 [wide] http://outdoor.cnad.com/　（被挂马网站）

	[script]http://ad.cnad.com/Js/outdoor/ad_outdoor_top.js （恶意跳转链接）
第二步	通过恶意跳转链接，再次跳转至多个集成网马页面 [script] http://ad.cnad.com/Js/outdoor/ad_outdoor_top.js（恶意跳转链接） [script]http://t.crabdance.com:10086/images/1.gif （集成网马页面）
第三步	通过集成网马页面，跳转至漏洞触发页面 [script]http://t.crabdance.com:10086/images/1.gif （集成网马页面） [iframe]http://bugs.chickenkiller.com:10/images/1.htm （CVE-2010-0806 漏洞） [iframe]http://bugs.chickenkiller.com:10/images/2.htm （CVE-2010-0611 漏洞）
第四步	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程序 http://bbs.jk136.com:123/js/js/js.js
第五步	在用户主机上执行下载的恶意程序

随着安全防护软件对挂马行为的跟踪查杀，网页挂马技术对抗也在不断升级，产生很多技术变形或策略触发，以规避安全防护软件。表 4-6、4-7 所示为通过技术变形或控制触发策略的典型挂马页面实例。

表 4-6　黑客网页挂马使用的技术变形示例（来源：奇虎 360 公司）

步骤	说明
第一步	网站被 ARP，嵌入网马跳转链接 [wide] http://www.eauto365.com/a/langyi/20110604/24608.html（被挂马网站） [iframe] http://axswx.3322.org:9898/index.html?id=101 （网马跳转地址）
第二步	通过网马跳转地址，跳转至漏洞触发页面 [iframe] http://axswx.3322.org:9898/index.html?id=101 （网马跳转地址） [iframe] http://gax.ns02.us/11/6.htm （极光漏洞并且进行了变异加密。） 变形的代码片段： 'K'+'58'+'58'+'K5858'+'K10EB'+'K4B5BK'+'C933KB966'+'K03B8K3480KBD'+'0BKFAE2K05EBKEBE8KFFFFK54FFKBEA3KBDBDKD9E2K8D1CKBDBDK36BDKB1FDKCD36'+'K10A1KD536K36B5KD74AKE4ACK03
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程序 http://gax.ns02.us/o/ue.exe
第四步	在用户主机上执行下载的恶意程序

表 4-7　黑客网页挂马使用的策略控制示例（来源：奇虎 360 公司）

步骤	说明
第一步	网站被 ARP，嵌入网马控制 JS 地址 [wide] http://700.cc/question.asp?cityid=334 （被挂马网站） [iframe]http://dsp.UglyAs.com/b.js?google=12x203 （网马控制 JS）
第二步	通过网马跳转地址，进行判断是否出发木马 [iframe] http://dsp.UglyAs.com/b.js?google=12x203 （网马跳转地址）

	[iframe] http://gay.ns02.us/11/lyay.htm （集成木马地址）
	策略控制:如果是当天第一次访问将触发网马,否则不触发木马。
	代码片段如下：
	“function baiduuu(){
	var Then = new Date()
	Then.setTime(Then.getTime() + 12*60*60*1000)
	var cookieString = new String(document.cookie)
	var cookieHeader = "Cookvie1="
	var beginPosition = cookieString.indexOf(cookieHeader)
	if (beginPosition != -1){
	} else……”

第三步	通过集成网马页面，跳转至漏洞触发页面 [iframe] http://gay.ns02.us/11/lyay.htm （集成网马页面） [iframe] http://gay.ns02.us/11/6.htm（极光漏洞） [iframe] http://gay.ns02.us/11/7.htm（iepeers 漏洞）

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。

2011 年 3 月-12 月，CNCERT 共监测到仿冒境内银行网站的域名 3841 个，这些域名分别解析到境内外 667 个 IP 地址，平均每个 IP 地址承载 5.8 个仿冒网站域名。在这 667 个 IP 中, 有 95.8%位于境外, 美国（72.1%）、中国香港（17.8%）和韩国（2.7%）居前三位，分别仿冒了 2943 个、766 个和 85 个境内银行网站，如图 4-9 和图 4-10 所示。

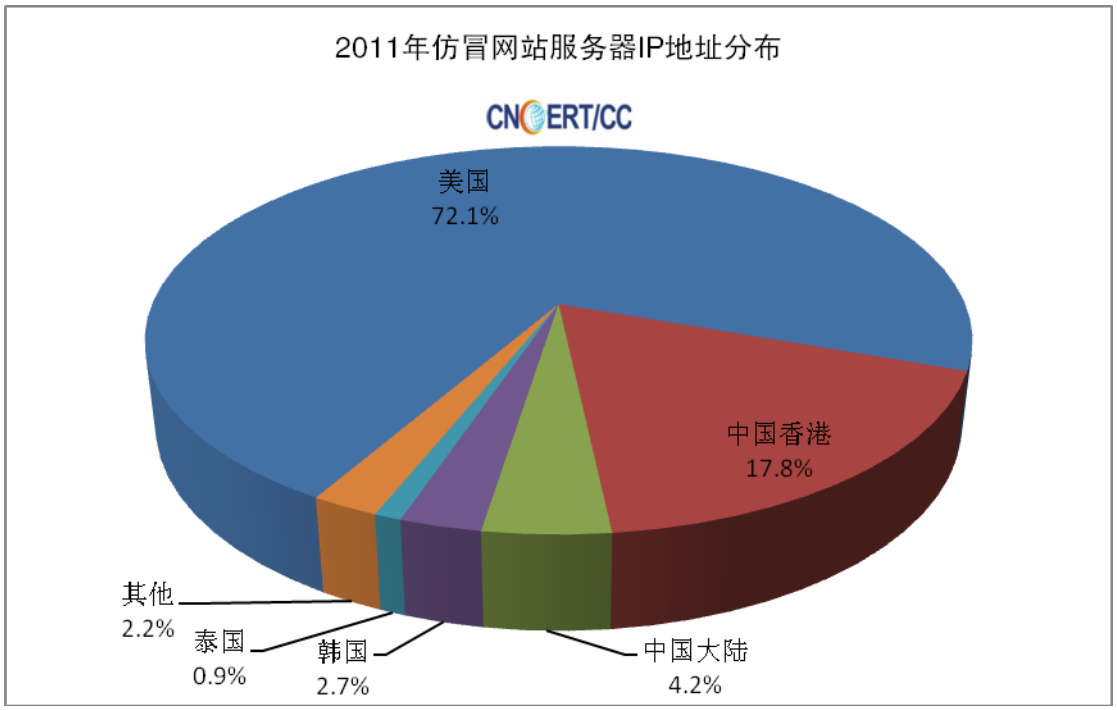

图 4-9　2011 年仿冒网站服务器 IP 地址分布

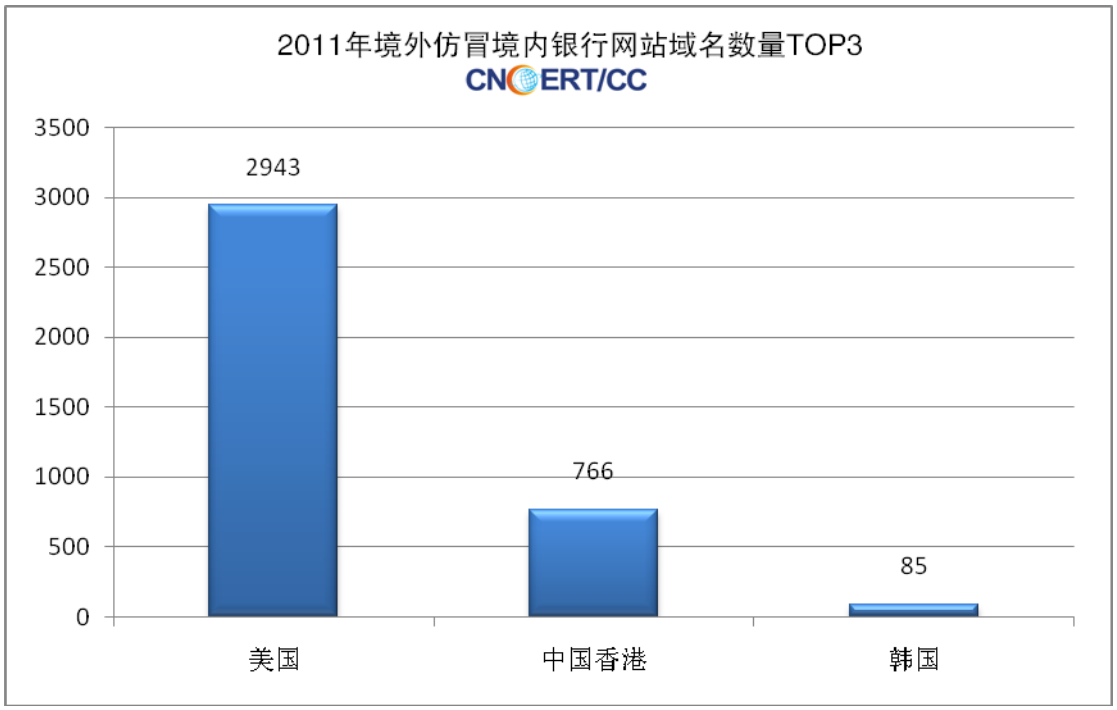

图 4-10　2011 年境外仿冒境内银行网站域名数量 TOP3

4.4网站后门情况

网站后门是黑客成功入侵网站服务器后留下的后门程序。通过网站后门，黑客可以上传、查看、修改、删除网站服务器上的文件，可以读取并修改网站数据

库的数据，甚至可以直接在网站服务器上运行系统命令。

2011 年 4 月-12 月 CNCERT 共监测到境内 12513 个网站被植入网站后门，其中政府网站有 1167 个。位于境外的攻击 IP 有 11851 个，主要位于美国（28.1%）、韩国（8.0%）和尼日利亚（5.8%）等国家或地区。其中，位于美国的 IP 地址共向我国境内 3437 个网站植入了后门程序，侵入网站数量居首位，其次是位于韩国和位于中国香港的 IP 地址，分别向我国境内 2255 个和 1408 个网站植入了后门程序，如图 4-11 和图 4-12 所示。

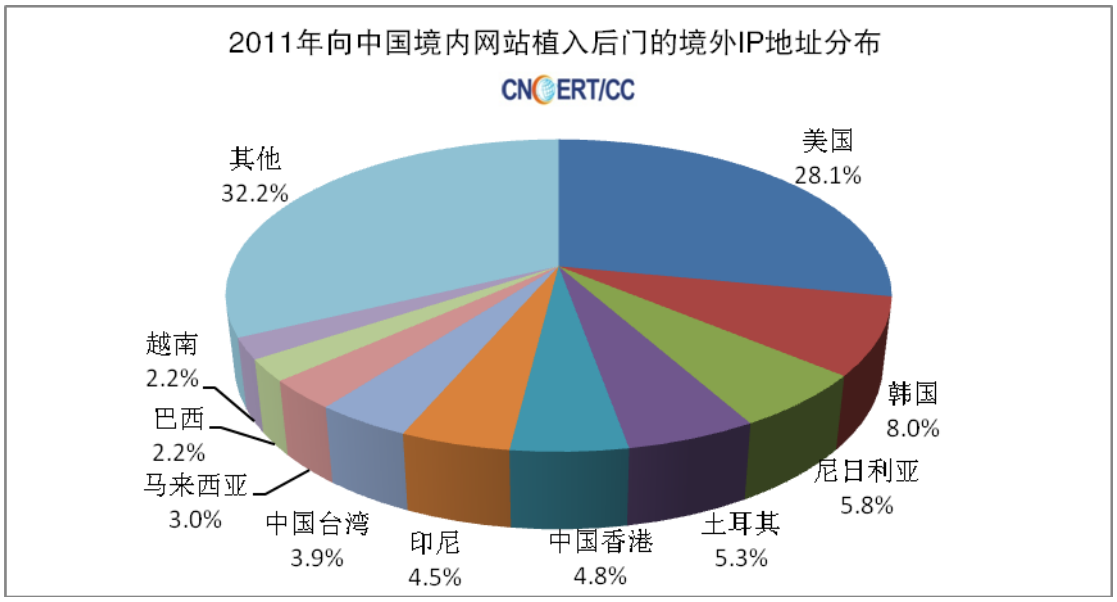

图 4-11　2011 年向中国境内网站植入后门的境外 IP 地址分布

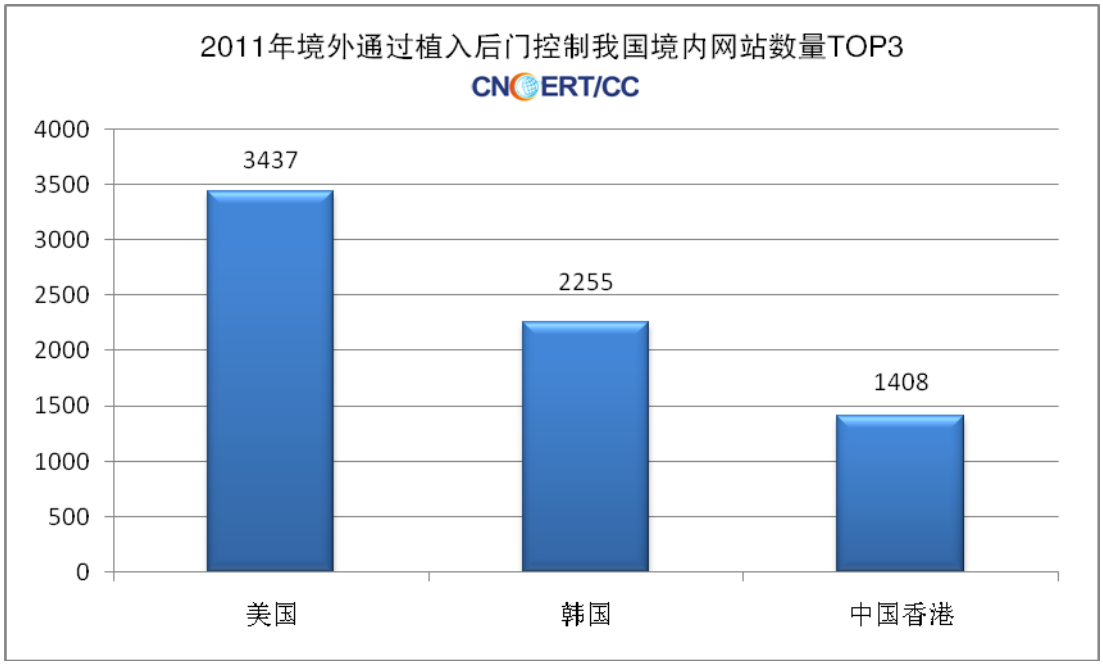

图 4-12　2011 年境外通过植入后门控制我国境内网站数量 TOP3