

安信华威胁报告（2011 年第二季度）

作者：安信华互联网安全实验室

目录

Malware 威胁概况	3
图 1.1 2011 年第二季度 Malware 类别比例图	3
Web Malware Top20.....	4
图 2.1 Web Malware Top20.....	4
Email Malware Top20.....	5
图 3.1 Email Malware Top20	5
恶意网站 Top20	6
图 4.1 恶意网站 Top20.....	6
图 4.2 恶意站点新域名注册国家分布统计	7
中国地区政府、高校类网站篡改分析	7
图 5.1 中国地区政府、高校类网站篡改（分类）数量统计周报（第二季度）	7
图 5.2 中国地区政府、高校类网站篡改（分类）数量统计周报（第一季度）	8
图 5.3 中国地区政府、高校类网站被篡改数量地区 Top10（第二季度）	8
Web 应用威胁分析.....	8
图 6.1 Web 应用威胁比例图	9
图 6.2 黑客通过网站安全漏洞上传 asp 木马后门.....	9
图 6.3 黑客通过 asp 木马后门程序直接修改网站程序代码	10
图 6.4 被挂黑链的页面出现了很多“第三者”	10
僵尸网络	11
图 7.1 僵尸服务器所处国家比例图.....	11
图 7.2 加密信息的网络通信片段	12
图 7.3 安信华拦截日志	12
关于安信华.....	13
关于安信华互联网安全实验室（Anchiva RapidRX Labs）	14

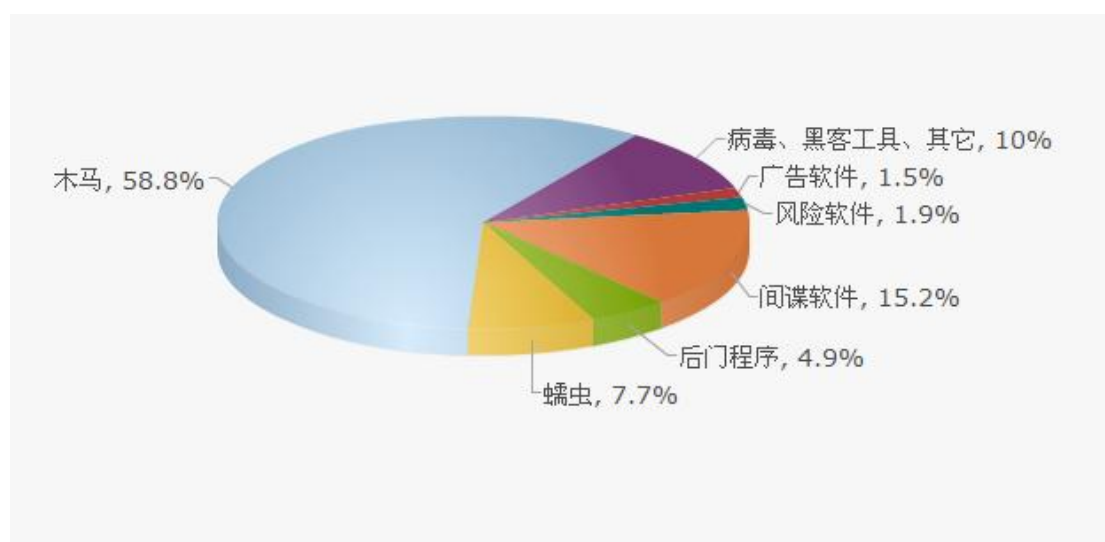
Q2 2011 安信华季度威胁报告大事记

- 安信华截获各类 Malware 超过 210 万，黑客工具成为本季度突出问题。
- 新增恶意域名注册依旧来自中、美、俄三国。
- QQ 钓鱼、微博钓鱼、金融钓鱼呈三足鼎立之势。
- 弹窗广告、导航网站、恶意软件下载成为恶意网站主要表现方式。
- 广告黑链入侵防不胜防。
- 僵尸网络服务器数量美国居首，中国大陆位列第二所占比重呈上升趋势。
- 控制僵尸网络依托的通讯协议呈多样化趋势，社交僵尸网络即将到来。

Malware 威胁概况

本季度安信华互联网安全实验室共截获各类 Malware 超过 210 万。其中木马所占比例仍超过恶意软件一半，约为 58.8%略有下降，相应的黑客工具则上升近 4 个百分点，成为本季度 Malware 威胁的另一突出问题，间谍软件和蠕虫所占比例较上季度的 12.4%、10.5%升降互平，分别为 15.2%和 7.7%，广告软件、传统病毒、后门程序和其它类别所占比例仍变化不大。

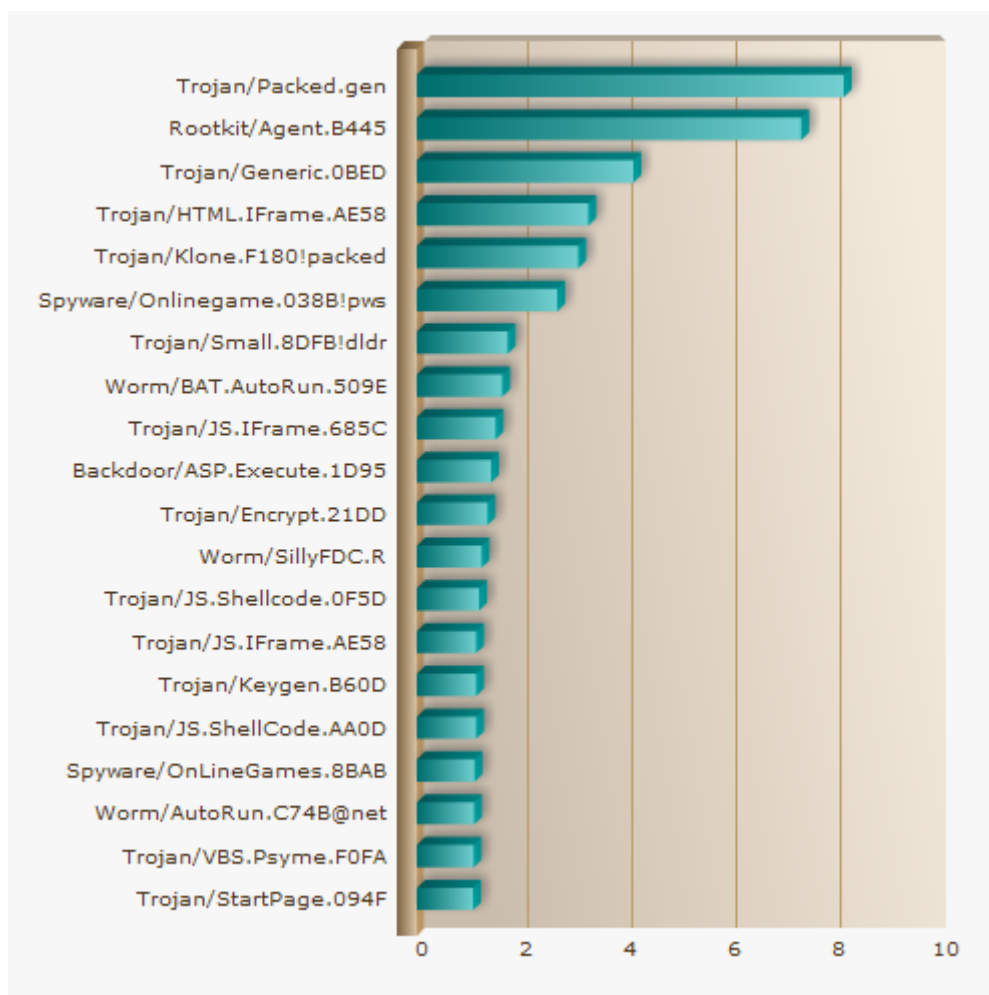
图 1.1 2011 年第二季度 Malware 类别比例图



Web Malware Top20

本季度的 Web 威胁中，其出现频率最高的前 20 个 Malware 如下图 2.1 所示。

图 2.1 Web Malware Top20

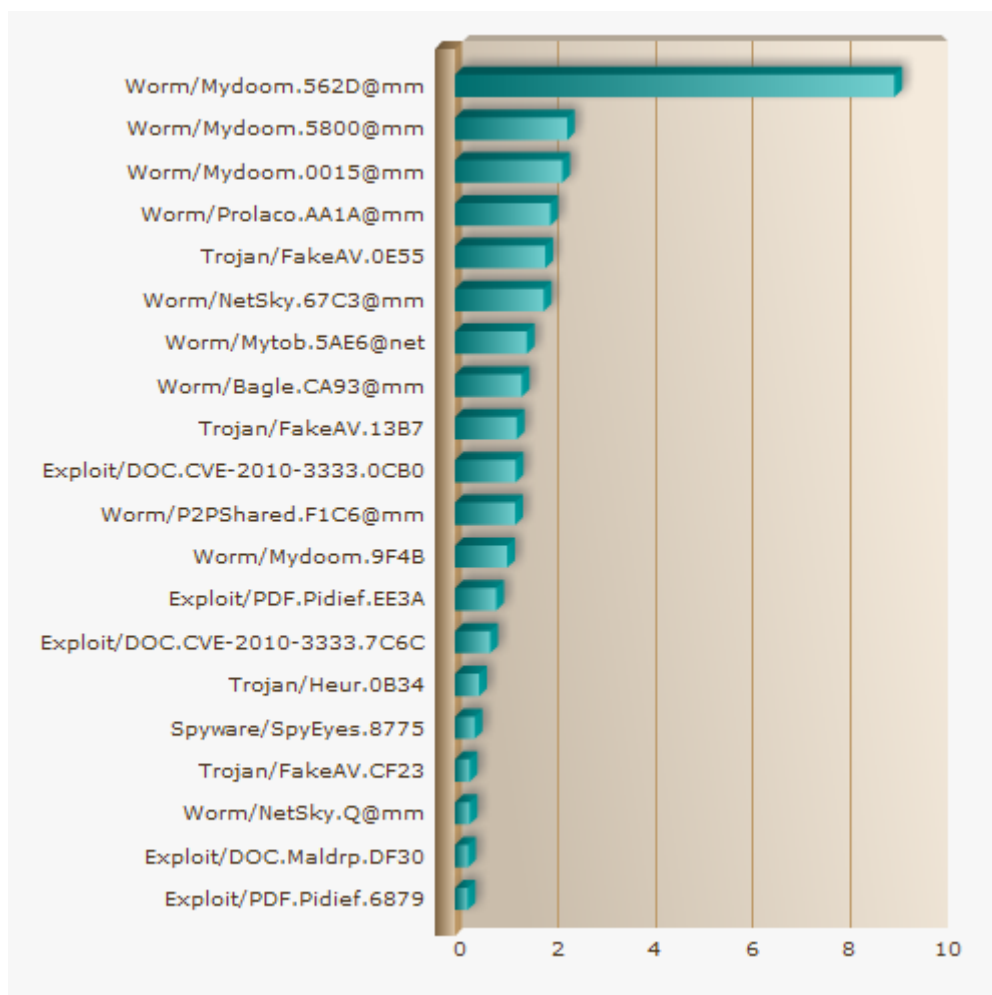


本季度 Web Malware 威胁前 20 中，在桌面平台对抗反病毒软件的 Rootkit 黑客工具已名列第二，它与其它 Malware 相配合将增加其它 Malware 的生存机率，同时也给受感染系统的稳定性埋下隐患；另外，木马（Trojan）在本次 Top20 中占半数以上，依然是安全威胁的重点，值得注意的是网马在其中所占的比重近一半，这将大大增加用户在平常的网页浏览中系统被感染的可能。

Email Malware Top20

根据安信华 Malware 监测网的监测结果，本季度的邮件威胁中，出现频率最高的前 20 种 Malware 如下图 3.1 所示。

图 3.1 Email Malware Top20

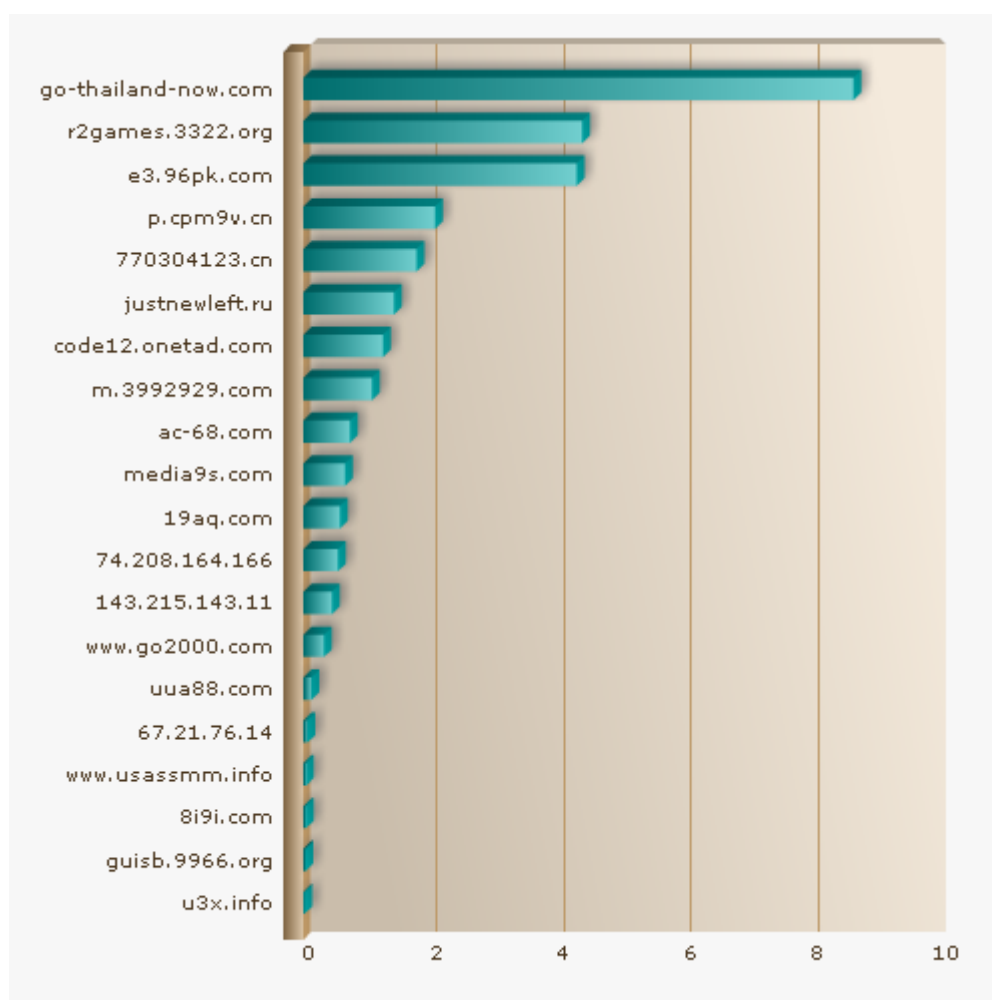


本季度老牌邮件蠕虫依然肆虐，Mydoom、Netsky、Bagle 等家族排名靠前，特别是 Mydoom 占据前三位。另一个突出的问题是：本地漏洞溢出利用工具所占比例大增，其中 Exploit/DOC.CVE-2010-3333.0CB0 排名较上季度上升 7 位，其变种 Exploit/DOC.CVE-2010-3333.7C6C 和 Exploit/PDF.Pidief、Exploit/DOC.Maldrp 家族也名列其中。

恶意网站 Top20

根据安信华 Malware 监测网的监测结果，发布恶意软件数量最多的前 20 个恶意网站如下图 4.1 所示。

图 4.1 恶意网站 Top20



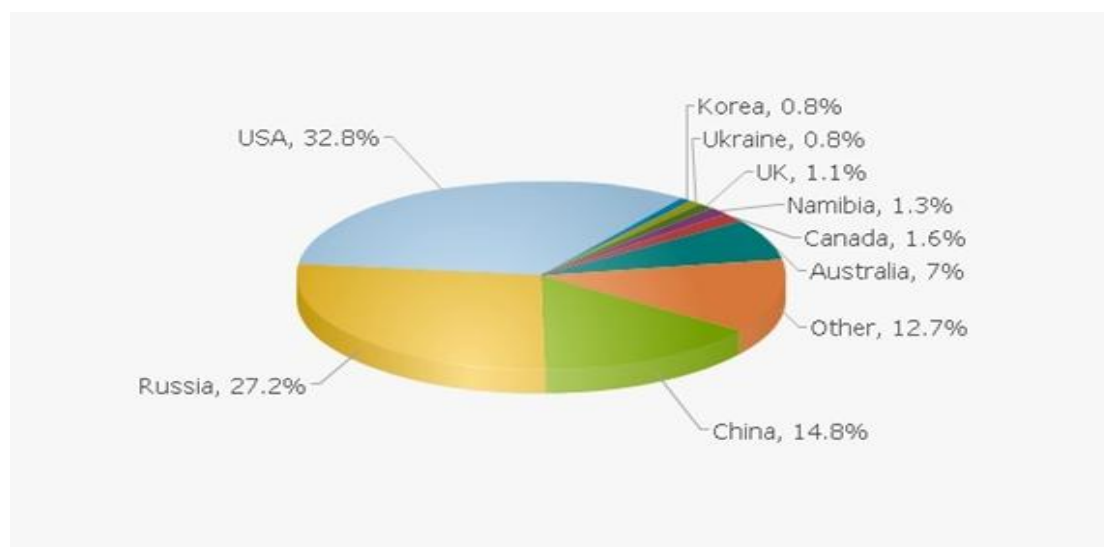
注意，以上所列网站部分仍然存在恶意链接，请勿直接访问！

相较上一季度恶意网站 Top 20，被拦截的网站变化较大，恶意弹窗广告、劫持用户主页的导航网站、恶意软件脚本下载站、内嵌恶意软件或脚本的成人网站依然是恶意网站的几大类型。钓鱼网站内容一般为 qq 中奖，登录伪造 qq 空间，微博中奖，或其他方式的中奖等。其中微博中奖越来越多，这跟微博的普及，用户的增大是相关的。同时也发现一些难以判断欺诈网站，像低价出售苹果手机等，这类网站需要用户用心判断，不要贪图一时的便宜。建议用户在浏览网站时，应做好病毒安全防护、打好电脑补丁，减少或者不浏览不明网站，更不要轻易点击通过邮件、聊

天软件等收到的不明链接，相信不明来历的中奖信息等。

恶意站点除大量使用 3-a.net、7766.org、8866.org、3322.org、9966.org、isgre.at 等免费的二级域名转向服务外，还注册大量新域名做为恶意站点，这些新域名注册国家分布统计如下图 4.2 所示：

图 4.2 恶意站点新域名注册国家分布统计



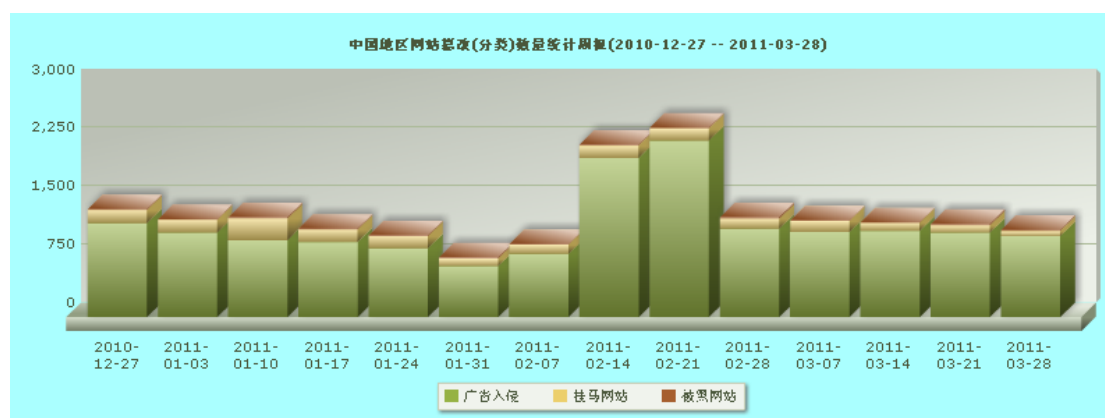
中国地区政府、高校类网站篡改分析

安信华针对中国境内的政府及高校类网站自动化监测，统计第二季度被篡改网站数量结果如下图所示。与上一季度相比较，在网页源代码中植入黑链代码的“广告入侵”类攻击数量有明显增长，广告挂马依然是破坏 web 应用信誉、威胁服务器及浏览者安全的威胁因素。

图 5.1 中国地区政府、高校类网站篡改（分类）数量统计周报（第二季度）



图 5.2 中国地区政府、高校类网站篡改（分类）数量统计周报（第一季度）



第二季度中国地区被篡改网站数量地区前十排名情况如下图 5.3 所示。数量及地域较上一季度没有明显变化。

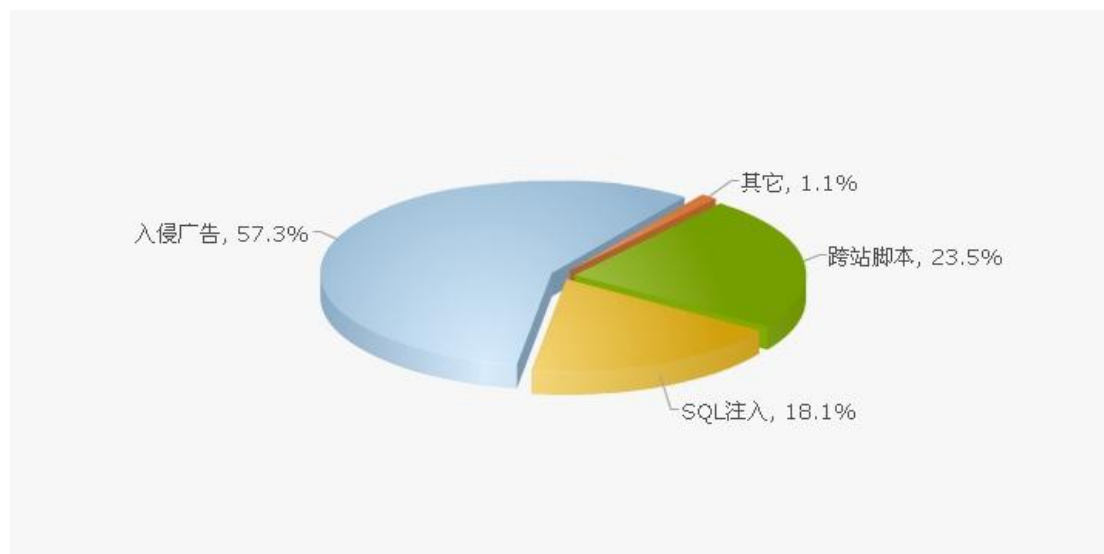
图 5.3 中国地区政府、高校类网站被篡改数量地区 Top10（第二季度）



Web 应用威胁分析

统计我们网站漏洞扫描平台 2011 年第二季度扫描结果，我们发现“入侵广告”类威胁占到 57.3%，传统的“SQL 注入”、“跨站脚本”分别占了 18.1%和 23.5%。如图 6.1 所示。

图 6.1 Web 应用威胁比例图



Web 应用除了面临 SQL 注入、XSS 跨站脚本执行、Cookie 欺骗等威胁外，它还受到网页被挂马、插入广告黑链等危害，使得网站用户信息面临被窃取的危险，网站信誉受损，被安全厂商分类错误而屏蔽等后果。下面介绍下目前非常流行的广告入侵--黑链。

黑链是 SEO 黑帽手法中相当普遍的一种手段，笼统地说，它就是指一些人用非正常的手段获取的其它网站的反向链接，让受益站点在短时间内可以迅速提高在搜索引擎里的排名，从而提高自己的知名度以及网站访问量。

如图 6.2 至 6.4 所示网站是如何被挂马和挂黑链的。

图 6.2 黑客通过网站安全漏洞上传 asp 木马后门

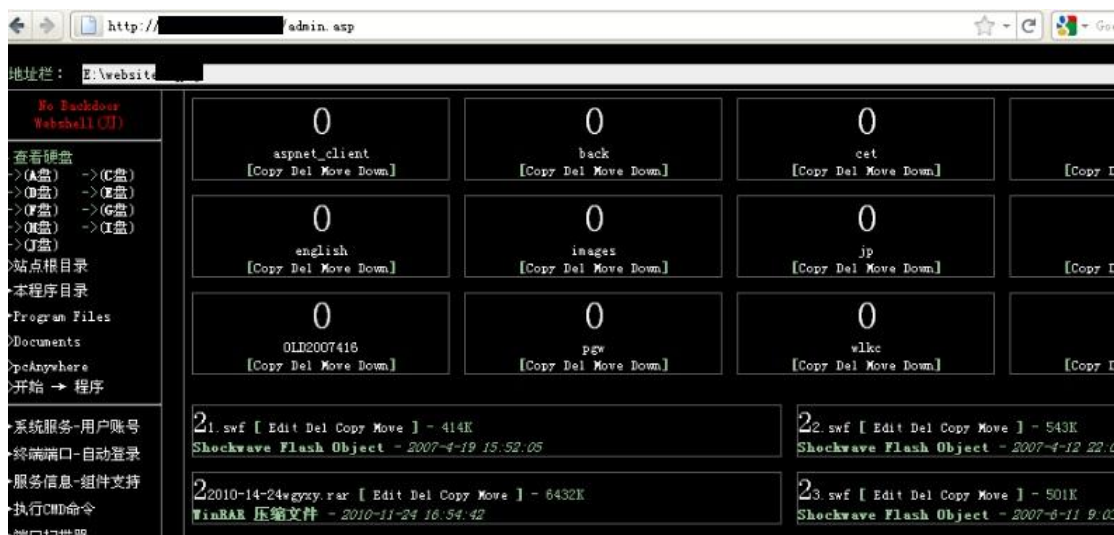


图 6.3 黑客通过 asp 木马后门程序直接修改网站程序代码

```

END FUNCTION
dns = Request.ServerVariables("SERVER_NAME")
path = Request.ServerVariables("PATH_INFO")
qs = Request.ServerVariables("QUERY_STRING")
url= dns&path&"?"&qs
agent = Request.ServerVariables("HTTP_USER_AGENT")
tz = "Windows"
if not Instr(agent,tz)>0 then
if path = "/index.asp" or path="/default.asp" then
'http://www.
com/meiyong/haha.asp?NewsID=23
response.write getBody("http://%
%77%77%
%30%34%
%36%78%69%6E%78
2E%63%6F%6D/meiyong/
else
response.write getBody("http://
%77%77
%30%34%
%78%69%6E%78
2E%63%6F%6D/meiyong/
end if
end if
%>

```

黑链的地址

变形后的地址

图 6.4 被挂黑链的页面出现了很多“第三者”



锦州 信息网 房产网 二手房 锦州二手房 锦州房产网 锦州人才网 锦州在线 锦州天气预
 锦州租房 锦州供求 寂寞博客 网站安全 黑客技术 个人电脑 网站源码出售 免费网站源码 网站源码
 全防护 网站制作 永安信

挂黑链的页面

源: http://www. .com/meiyong/haha.asp?NewsID=21 - Mozilla Firefox

文件(F) 编辑(E) 查看(V) 帮助(H)

```

<body onselectstart="return false" oncontextmenu="return false" >
<marquee align="left" direction="up" width="100%" height="100%" style="color:#fffff;
<table width="100%" align="center" border="0" cellspacing="0" cellpadding="0" style
<tr>
<td height="10" style="color:#ffffff;">友情链接:
<!--&nbsp;
<strong><a title="锦州房产网" href="http://www. .com" style="color:#ffffff;">锦州
<strong><a title="锦州" href="http://www. .com">锦州</a></strong>
<strong><a title="信息网" href="http://www. .com">信息网</a></strong>
<strong><a title="房产网" href="http://www. .com">房产网</a></strong>
<strong><a title="二手房" href="http://www. .com">二手房</a></strong>
<strong><a title="锦州二手房" href="http://www. .com">锦州二手房</a></strong>
<strong><a title="锦州房产网" href="http://www. .com">锦州房产网</a></strong>
<strong><a title="锦州人才网" href="http://www. .com">锦州人才网</a></strong>
<strong><a title="锦州在线" href="http://www. .com">锦州在线</a></strong>
<strong><a title="锦州天气预报" href="http://www. .com">锦州天气预报</a></stro
<strong><a title="锦州百姓网" href="http://www. .com">锦州百姓网</a></strong>
<strong><a title="锦州吧" href="http://www. .com">锦州吧</a></strong>
<strong><a title="锦州房产" href="http://www. .com">锦州房产</a></strong>
<strong><a title="锦州海会" href="http://www. .com">锦州海会</a></strong>
<strong><a title="锦州旅行社" href="http://www. .com">锦州旅行社</a></strong>

```

查看源代码

黑链对受害者网站的影响还是很大的，若一个页面存在太多链接，会直接导致受害者网站的搜索引擎排名，一些被挂黑链的网站往往久了后就出现快照更新慢，排名下降等情况。严重的，一般网站被挂黑链的同时，有时候还伴随着挂马现象，当搜索引擎发现该站点被挂马，会直接屏蔽该网站。

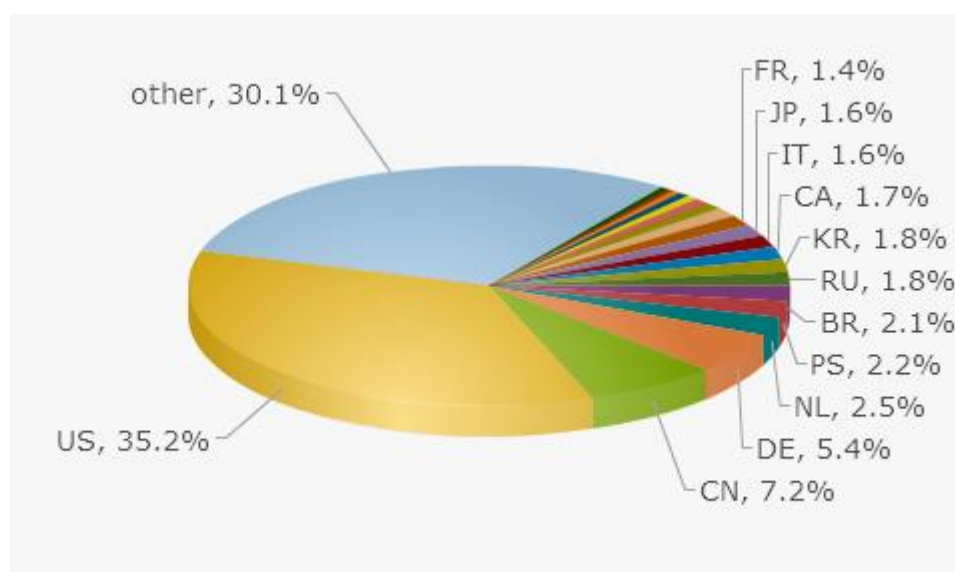
如果要防止自己的网站被挂黑链，最好每天检查自己的站点，时常查看下站点页面的源文件，如果发现异常，及时检查网站的安全情况，清理广告代码，同时做好安全加固工作，防止下次再次被入侵挂马。

僵尸网络

经安信华监控网络发现，第二季度三大僵尸网络 Palevo、Zeus、SpyEye 继续在网络上横行，传统的通过 IRC 协议传播的 Botnet 较上季度略有减少，通过即时通信和 P2P 传播的 Botnet 和上赛季持平，最近流行的是通过网页控制的 Webbot，利用很少禁止的 80，53 端口来进行指令传输，这种 Botnet 被黑客使用的越来越多，大量的 Botnet 样本也更多的来源于此。

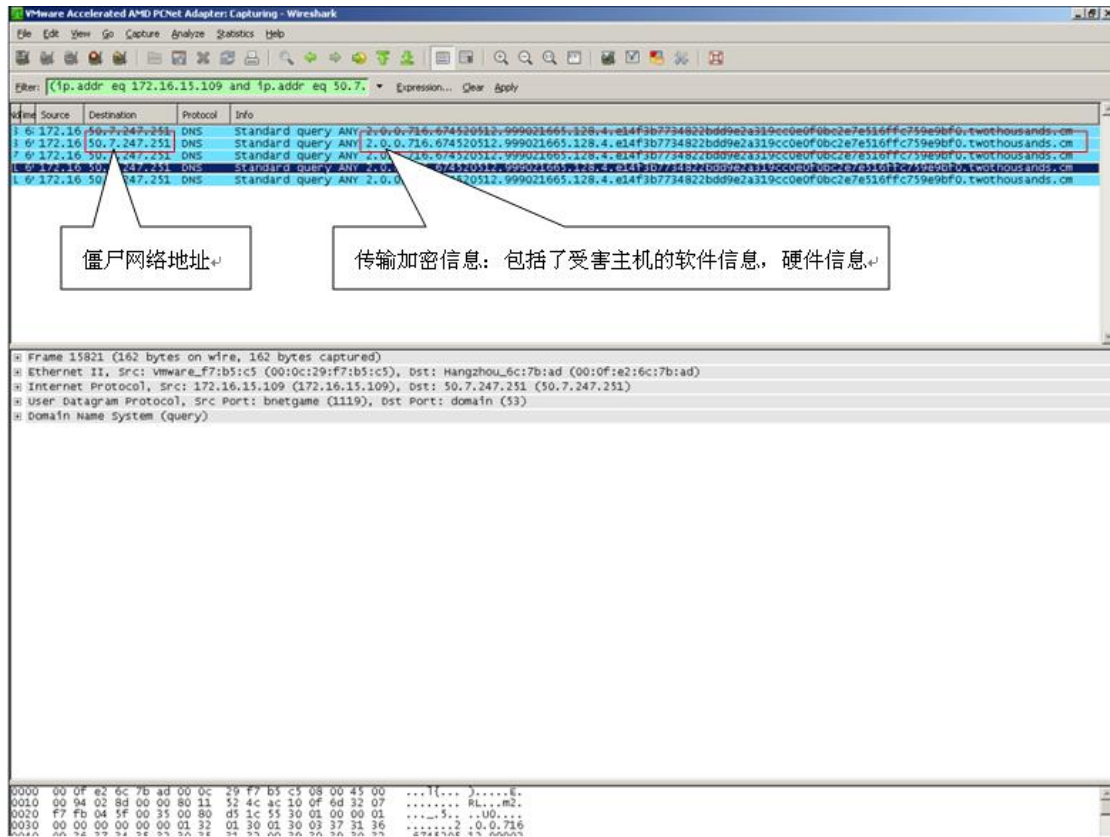
安信华对其捕获的僵尸服务器进行的分析中，如下图所示，美国(US)再次占据 34.6%的高位，中国大陆(CN)依然仅次于美国占据 7.2%排第二位，并有继续上升的趋势，其次是德国(DE) 5.4%，荷兰(NL)2.5%。如下图 7.1:

图 7.1 僵尸服务器所处国家比例图



经安信华互联网安全实验室最新研究，一种利用 DNS 协议传输加密信息的 Botnet 样本已经出现，这给判断是否是僵尸网络带来了迷惑性。经分析，它的加密手法并不神秘，采用的是简单的异或手法。它的迷惑性在于利用 DNS 协议传输数据，因为判断规则很少使用 DNS 作为判断依据，这就为黑客提供了可利用的机会，如下图 7.2 为加密信息的网络通信片段：

图 7.2 加密信息的网络通信片段



安信华产品最新发布的版本已可以对此类 Botnet 进行拦截。如下图 7.3 为 安信华拦截日志：

图 7.3 安信华拦截日志



关于安信华

北京安信华科技有限公司 (Anchiva Systems Ltd.) 成立于 2006 年, 是一家拥有自主创新信息安全产品的中国高新技术企业, 汇集了来自防病毒领域以及网络安全设备领域的优秀人才, 创办人和高管曾经在 Cisco、Netscreen、Fortinet 等国内外著名的安全设备厂商中担任过重要职务。公司总部设在北京, 安全实验室位于杭州, 拥有众多优秀的研发人员; 并在北京、上海、广州、杭州、南京、设有销售办事处, 产品及服务遍及国内外多个区域。

安信华是应用安全网关的领导者, 致力于加强企业边界安全。公司有四款主要产品: 保护企业内部终端上网安全的 A 系列; 保护企业 Web 服务器安全的 S 系列; 内网安全预警系统以及 Web 安全专业服务。A 系列产品集安全与管理功能于一身, 强大的综合威胁防御功能, 有效的过滤随上网而来的蠕虫, 木马, 僵尸网络感染以及其他各种恶意软件; 同时通过 Web 站点过滤、Internet 应用控制与带宽管理、上网行为与内容审计、外发信息过滤来规范员工上网行为, 提高办公效率, 防止商业机密外泄, 是一款功能全面的上网安全网关。S 系列产品部署在 Web 服务器群前端, 有效地抵御 SQL 注入以及 XSS 攻击等, 防范应用层攻击于未然; 同时具备网站挂马监测、Webshell 回传阻拦、信息防泄露、访问日志审计等多种功能, 是一款使用简单, 功能强大的 Web 应用防火墙。内网安全预警系统应用于大型用户内网环境, 集成了 A 系列产品的全部特性以及统一管理平台, 从网络应用流量、网络应用威胁、内网信息泄漏等几方面, 让内网的安全可视、透明。安信华在内容安全领域的多年研究, 积累的丰富经验, 诸多的业内专业人士, 推出的针对 Web 应用系统的运营监控、木马监测与漏洞风险评估服务, 配合 S 系列 web 应用防火墙为用户的 web 应用系统提供全面的运营安全解决方案。

安信华全系列产品均采用支持多核均衡分发机制并且优化重写 TCP 协议栈的操作系统 AnchivaOS, 并且在自主研发的高性能 ASIC 芯片驱动下, 打破了传统信息安全网关性能瓶颈, 为企业提供实时、全方位的安全防护。其中 A 系列产品能 100%覆盖病毒研究权威组织 Wildlist 监控的流行病毒, 连续 5 年通过 ICSA 的防病毒认证, 并参加了 ICSA 以及中国信息安全测评中心的性能测试, 证明其全球领先的 HTTP 处理高性能特性。

安信华拥有自己的互联网安全实验室, 由经验丰富的病毒分析师和威胁研究员组成, 他们战略性的分布在中国、北美和欧洲, 负责监测、采集与研究互联网中传播的恶意代码, 构建覆盖全球的云安全服务。通过安信华产品内置的 Malware 特征库可以找到多达 2000 万以上的恶意软件, 而且这个数量还在以每日上万条的速度在增长, 网关特征库容量、覆盖率在业界遥遥领先。实验室提供 7X24 小时不间断的升级服务, 包括 Malware 特征库、恶意站点库、URL 分类库、Web 威胁特征库、僵尸网络数据库、应用协议特征库; 并且具有启发式扫描技术与“零日保护”计划, 安信华确保用户网络随时处在最新技术的保护下。目前, 安信华安全实验室凭借自身的专业性已经成为国家互联网应急中心的安全信息通报工作组成员单位以及国家计算机病毒应急处理中心的合作单位。

安信华的 A 系列产品线分为五个型号, S 系列分为四个型号, 覆盖用户由 100 人到 10000 人, 单台设备支持的带宽从 10M 到 1.3G, 单台最高端设备在所有功能同时开启时支持的吞吐量超过 1G。安信华的客户涉及金融、政府、运营商、能源、医疗、制造、科技、零售和教育等多个行业, 在国内拥有数百位的重要客户。A 系列产品审计功能通过保密局涉密产品检测, 获得相关资质, 也在服务于涉密用户。

通过持续不断的技术创新，安信华致力于为各类型客户提供更清洁的 Internet 内容。

关于安信华互联网安全实验室（Anchiva RapidRX Labs）

安信华互联网安全实验室创建于 2006 年，聚集了来自计算机安全、网络安全和 Web 安全等领域的安全专家，致力于病毒木马、间谍软件、僵尸网络、恶意网站、网络钓鱼、网站入侵等互联网威胁的研究，为安信华产品提供威胁特征库的升级服务，向安信华客户提供安全技术支持。作为国家互联网应急中心的网络安全信息通报单位，安信华互联网安全实验室是其向公众发布的《网络安全信息与动态周报》的主要贡献者。另外，安信华互联网安全实验室也是国家计算机病毒应急处理中心的合作单位，在病毒和木马的收集与监测等方面进行着技术合作。