

# Anchiva 威胁报告 (2010 年第二季度)

作者: Anchiva 安全实验室

## 目录

<b>Malware 威胁概况</b> .....	<b>3</b>
2010 年第一季度 Malware 类别比例图 .....	3
<b>Web Malware Top20</b> .....	<b>3</b>
Web Malware Top20 .....	4
某客户中 Spyware/OnLineGames. 2B17 的部分拦截记录 .....	5
<b>Email Malware Top20</b> .....	<b>5</b>
Email Malware Top20 .....	6
某客户中 Trojan/Koobface. D611 的部分拦截记录 .....	7
<b>恶意网站 Top20</b> .....	<b>7</b>
恶意网站 Top20 .....	8
<b>疯狂的广告马</b> .....	<b>8</b>
某测试环境中拦截到的后门上传 .....	9
Google 搜索显示某黑链工具感染超过 5 百万页面 .....	10
某测试环境中拦截到的黑链请求 .....	10
<b>钓鱼网站</b> .....	<b>11</b>
“QQ 安全中心”钓鱼网站 .....	11
“谷歌中奖信息”钓鱼邮件 .....	12
“谷歌中奖信息”钓鱼网站 .....	12
“工商银行”钓鱼网站 .....	13
“网易中奖信息”钓鱼网站 .....	13
<b>关于 Anchiva</b> .....	<b>14</b>
<b>关于 Anchiva 安全实验室 (Anchiva RapidRX Labs)</b> .....	<b>15</b>

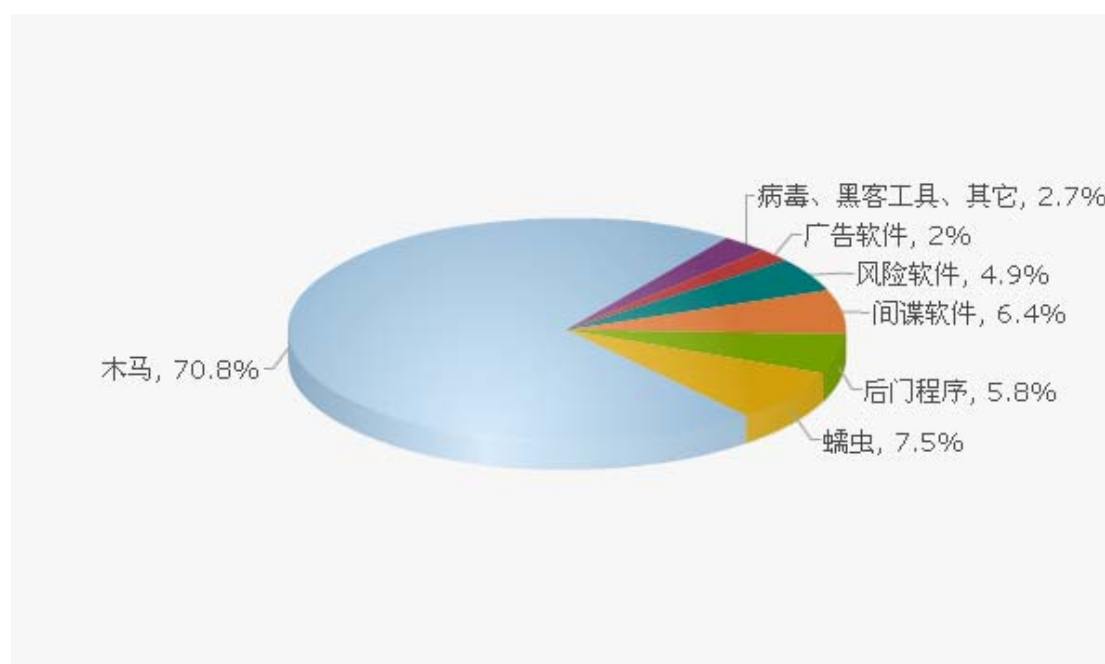
### Q2 2010 Anchiva 季度威胁报告大事记

- Anchiva 截获各类 Malware 将近 150 万，木马是主要威胁
- 正规网站被寄存、传播恶意软件，服务器面临巨大威胁
- 网络黑色地下产业链疯狂挂广告、黑链
- QQ、网上银行等依然是钓鱼网站主要对象

## Malware 威胁概况

本季度 Anchiva 安全实验室共截获各类 Malware 约 150 万。蠕虫、后门程序、间谍软件、风险软件和广告软件占到将近 25%，木马所占的比例与上季度相比小幅上升，占到 70.8%，传统病毒和其它类别所占比例与上季度类似。

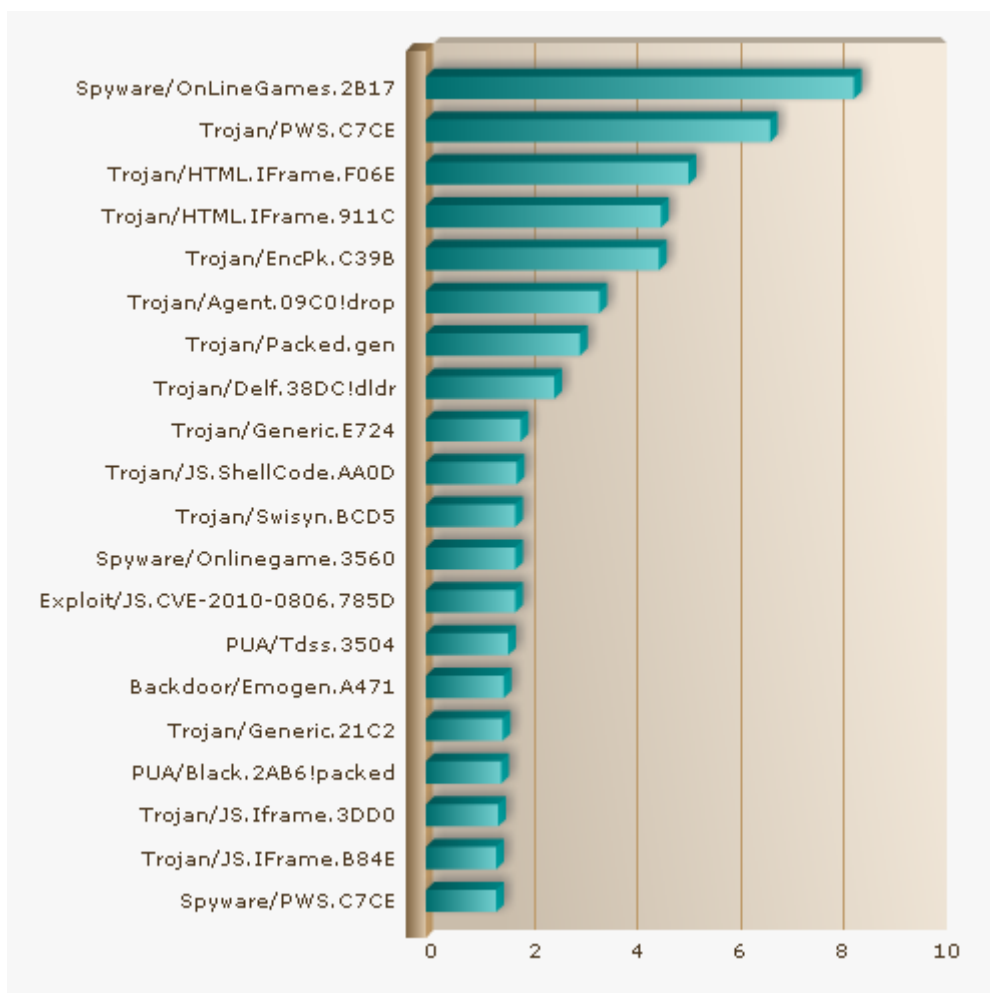
2010 年第二季度 Malware 类别比例图



## Web Malware Top20

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

## Web Malware Top20



本季度 Web Malware 威胁前 20 中，利用浏览器或第三方组件中存在的漏洞等方式传播的恶意软件占据较大比重，总计有 6 个。其余恶意软件多为下载者、木马，为下载其它恶意软件、窃取敏感信息提供便利。

**Spyware/OnLineGames.2B17**：它是间谍软件，窃取受害者的网络游戏账号、密码等敏感信息。一般通过网页挂马的形式，利用浏览器或第三方组件中的漏洞，在用户浏览网页的同时，执行恶意代码，进而下载远程恶意网站中的间谍软件。不法分子通过这一系列的操作，最终达到窃取个人敏感信息的目的。

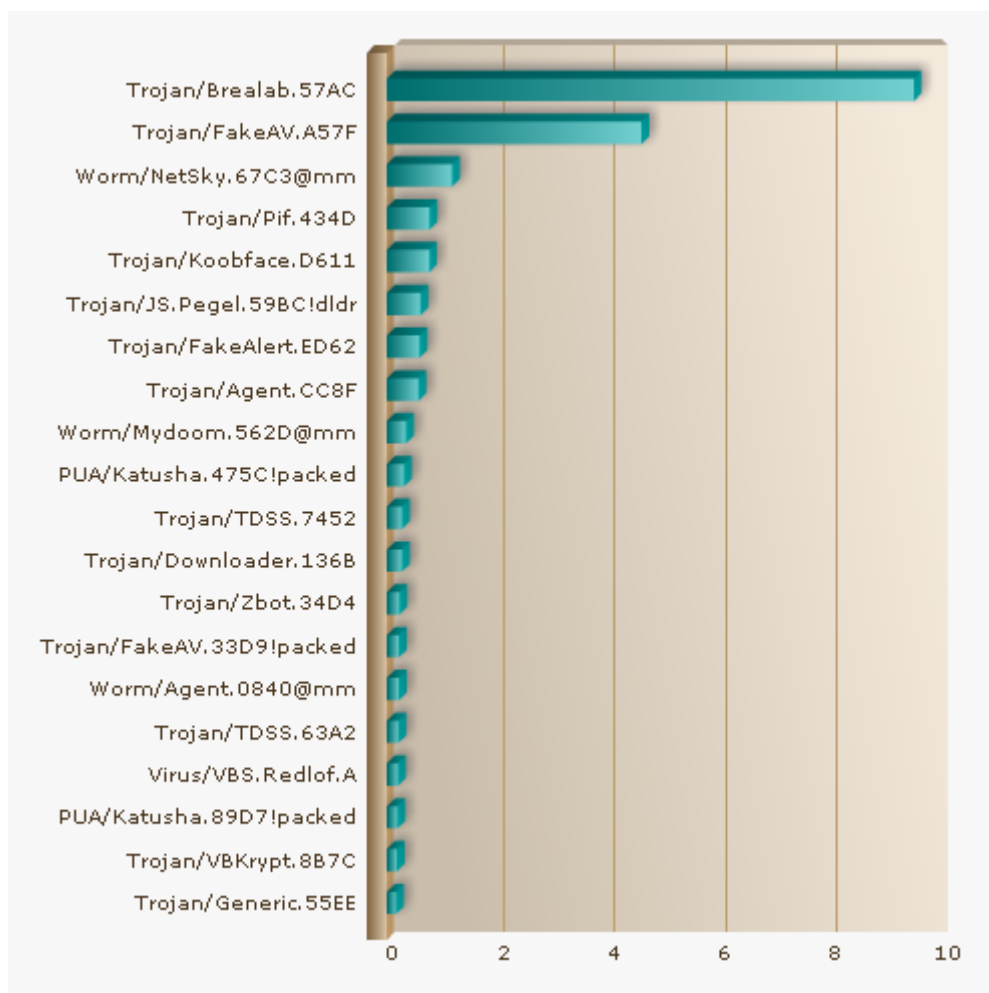
## 某客户中 Spyware/OnLineGames.2B17 的部分拦截记录

date	name	url
2010-04-22 09:06:49	Spyware/OnLineGames.2B17	txt.x8wdns.com:18364/x14.js
2010-04-22 09:06:48	Spyware/OnLineGames.2B17	txt.x8wdns.com:18364/x14.js
2010-04-22 09:06:47	Spyware/OnLineGames.2B17	txt.x8wdns.com:18364/x14.js
2010-04-22 09:06:23	Spyware/OnLineGames.2B17	txt.x8wdns.com:18364/x9.js
2010-04-22 09:06:22	Spyware/OnLineGames.2B17	txt.x8wdns.com:18364/x9.js
2010-04-22 09:06:21	Spyware/OnLineGames.2B17	txt.x8wdns.com:18364/x9.js
2010-04-22 09:06:14	Spyware/OnLineGames.2B17	txt.x8wdns.com:18364/x7.js
2010-04-22 09:06:13	Spyware/OnLineGames.2B17	txt.x8wdns.com:18364/x7.js
2010-04-22 09:06:12	Spyware/OnLineGames.2B17	txt.x8wdns.com:18364/x7.js
2010-04-20 17:21:39	Spyware/OnLineGames.2B17	208.98.41.191/x17.js
2010-04-20 17:21:37	Spyware/OnLineGames.2B17	208.98.41.191/x17.js
2010-04-20 17:21:36	Spyware/OnLineGames.2B17	208.98.41.191/x17.js
2010-04-20 17:21:33	Spyware/OnLineGames.2B17	208.98.41.191/x17.js
2010-04-20 17:21:31	Spyware/OnLineGames.2B17	208.98.41.191/x17.js
2010-04-20 17:21:30	Spyware/OnLineGames.2B17	208.98.41.191/x17.js
2010-04-20 17:21:21	Spyware/OnLineGames.2B17	208.98.41.191/x14.js
2010-04-20 17:21:20	Spyware/OnLineGames.2B17	208.98.41.191/x14.js
2010-04-20 17:21:19	Spyware/OnLineGames.2B17	208.98.41.191/x14.js

## Email Malware Top20

根据 Anchiva 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 如下图所示。

## Email Malware Top20



本季度中，假冒杀毒软件家族的传播依然活跃。Trojan/Brealab.57AC 在本季度和上一季度 Email Malware Top 20 中均排名首位，它是假冒杀毒软件家族的传播载体，有的变种也存在下载其它恶意软件的行为。假冒杀毒软件通过阻止正常杀毒、安全等软件的正常查杀、禁止自动更新安全补丁等手段，达到占领受害者机器的目的，进而形成僵尸网络，用于 DDOS 攻击、传播垃圾邮件等恶意行为。另一方面，社会化交友网络被用于恶意软件传播呈逐渐扩大的趋势。这类恶意软件，例如 Trojan/Koobface.D611，利用社交网络的联系人圈子，及其相互易信任的因素，大量发送附带恶意软件的邮件，或引导受害者浏览存在恶意软件的站点，最终侵入受害者机器，进行窃取敏感信息、传播其它恶意软件等行为。

**Trojan/Koobface.D611:** 该木马主要通过邮件传播，它伪装成 Facebook、Myspace、Twitter 等社交网站发出的交友信息，诱使受害者从特定站点下载其它恶意软件。

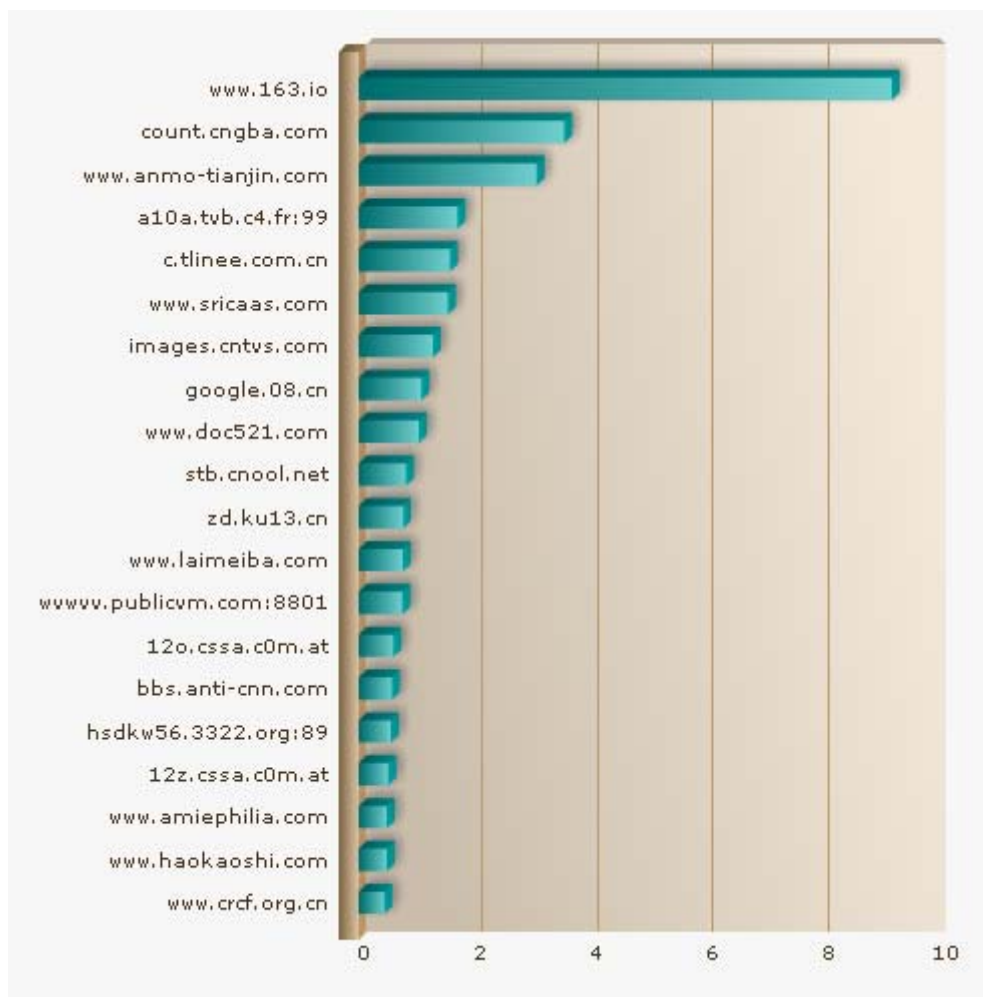
某客户中 Trojan/Koobface.D611 的部分拦截记录

date	name	protocol
2010-06-23 01:46:30	Trojan/Koobface.D611	smtp
2010-06-23 01:46:24	Trojan/Koobface.D611	smtp
2010-06-23 01:29:36	Trojan/Koobface.D611	smtp
2010-06-23 01:29:29	Trojan/Koobface.D611	smtp
2010-06-23 01:09:54	Trojan/Koobface.D611	smtp
2010-06-23 01:08:35	Trojan/Koobface.D611	smtp
2010-06-23 01:01:46	Trojan/Koobface.D611	smtp
2010-06-23 00:44:24	Trojan/Koobface.D611	smtp
2010-06-23 00:37:09	Trojan/Koobface.D611	smtp
2010-06-23 00:31:40	Trojan/Koobface.D611	smtp
2010-06-23 00:14:40	Trojan/Koobface.D611	smtp
2010-06-23 00:07:00	Trojan/Koobface.D611	smtp
2010-06-22 23:57:56	Trojan/Koobface.D611	smtp
2010-06-22 23:55:42	Trojan/Koobface.D611	smtp
2010-06-22 23:52:09	Trojan/Koobface.D611	smtp
2010-06-22 23:44:39	Trojan/Koobface.D611	smtp

## 恶意网站 Top20

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

恶意网站 Top20



本季度恶意网站 Top 20 相较上一季度，正规网站被利用、寄存、传播恶意软件的比例大幅上升，占据半数以上，例如 [www.163.io](http://www.163.io)、[images.cntvs.com](http://images.cntvs.com)、[www.haokaoshi.com](http://www.haokaoshi.com)、[www.crcf.org.cn](http://www.crcf.org.cn) 等。这类网站一般存在一个小 js 脚本，当用户浏览包含该恶意脚本的网站时，它会载入另一恶意站点中存在的脚本，并利用某些漏洞，执行恶意代码，最终下载存在于同一服务器或另一恶意站点中的恶意软件。这表明攻击者已经倾向于利用正规网站来散播恶意软件，而大多数的网站本身存在的安全问题、漏洞亟待解决。

## 疯狂的广告马

Anchiva RapidRX 网络安全实验室研究发现，互连网黑色地下产业链新的盈利模式开始崛起，黑客团伙在进行网站挂马的同时，对目标网站植入大量的非法内容，通常为网络游戏、私服、办证、婚纱摄影等广告。下图显示的是某网站被潜入大量

有关网络游戏、婚纱摄影、饮料代理批发等连接信息。

```

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
<a href=" http://www.18qn.net" title="千年私服,最新千年私服">千年私服</a>
<a href=" http://www.qn8787.com" title="千年私服,新开千年私服">千年私服</a>
<a href=" http://www.3000f.net" title="千年私服">千年私服</a>
<a href=" http://www.1000qn.net" title="千年私服,最新开千年私服">千年私服</a>
<a href=" http://www.917b.com" title="完美国际私服,完美私服,完美世界国际版私服">完美国际私服</a>
<a href=" http://www.917net.net" title="网络游戏">网络游戏</a>
<a href=" http://www.917net.com" title="网络游戏,网络游戏大全">网络游戏</a>
<a href=" http://www.543f.com" title="蜀门私服,蜀门SF">蜀门私服</a>
<a href=" http://www.515f.net" title="完美国际私服">完美国际私服</a>
<a href=" http://www.33gn.net" title="传奇私服">传奇私服</a>
<a href=" http://www.917gm.com" title="天龙八部2私服">天龙八部2私服</a>
<a href=" http://www.543f.net" title="天龙八部私服">天龙八部私服</a>
<a href=" http://www.xwssf.com" title="蜀门私服,蜀门SF,蜀门私服发布网站">蜀门私服</a>
<a href=" http://www.98866.com" title="DNF私服,DNF私服发布网">DNF私服</a>
<a href=" http://www.3ky.org.cn" title="dnf外挂,dnf免费外挂">dnf外挂</a>
<a href=" http://www.xinqn888.com" title="蜀门私服发布网站">蜀门私服发布网站</a>
<a href=" http://www.1104f.cn" title="诛仙私服">诛仙私服</a>
<a href=" http://www.e6top.net" title="蜀门私服">蜀门私服</a>
<a href=" http://e6top.net" title="诛仙私服,诛仙私服发布网">诛仙私服发布网</a>
<a href=" http://www.10004y.cn" title="蜀门私服">蜀门私服</a>
<a href=" http://www.gmzhaosf.cn" title="奇迹私服">奇迹私服</a>
<a href=" http://www.1234mu.com" title="奇迹私服">奇迹私服</a>
<a href=" http://trbok.com" title="唐人减肥瘦身">唐人减肥瘦身</a>
<a href=" http://xporg.com" title="魅力丰胸网">魅力丰胸网</a>
<a href=" http://Learnchineseuall.com" title="唐人创业网">唐人创业网</a>
<a href=" http://Chinesetutorial.net" title="唐人娱乐新闻">唐人娱乐新闻</a>
<a href=" http://pu5a.com" title="热血江湖私服">热血江湖私服</a>
<a href=" http://new66.com" title="魔兽世界私服">魔兽世界私服</a>
<a href=" http://510g.com" title="蜀门私服">蜀门私服</a>
<a href=" http://zx2f.com" title="诛仙私服,诛仙2私服">诛仙私服</a>
<a href=" http://pro4f.com" title="破天一剑私服">破天一剑私服</a>
<a href=" http://www.00315.cc" title="唐山信息港">唐山信息港</a>
<a href=" http://www.fangzhan.org" title="房展会">房展会</a>
<a href=" http://www.qq8e.com" title="完美国际私服">完美国际私服</a>
<a href=" http://www.d14f.com" title="蜀门私服">蜀门私服</a>
<a href=" http://www.toppic.cc" title="婚纱摄影,丽江婚纱摄影,三亚婚纱摄影">丽江婚纱摄影</a>
<a href=" http://www.zssjsp.cn" title="饮料,饮料厂,饮料代理,饮料批发">饮料</a>
<a href=" http://www.010uou.com" title="大牌插件">大牌插件</a>
</div>
<div style="position: absolute; top: -999px;left: -999px;"><strong>
<a href=" http://www.1818qn.net" title="千年私服,变态千年私服">千年私服</a>
<a href=" http://www.978f.com" title="斗地主,棋牌游戏,斗地主小游戏">斗地主</a>

```

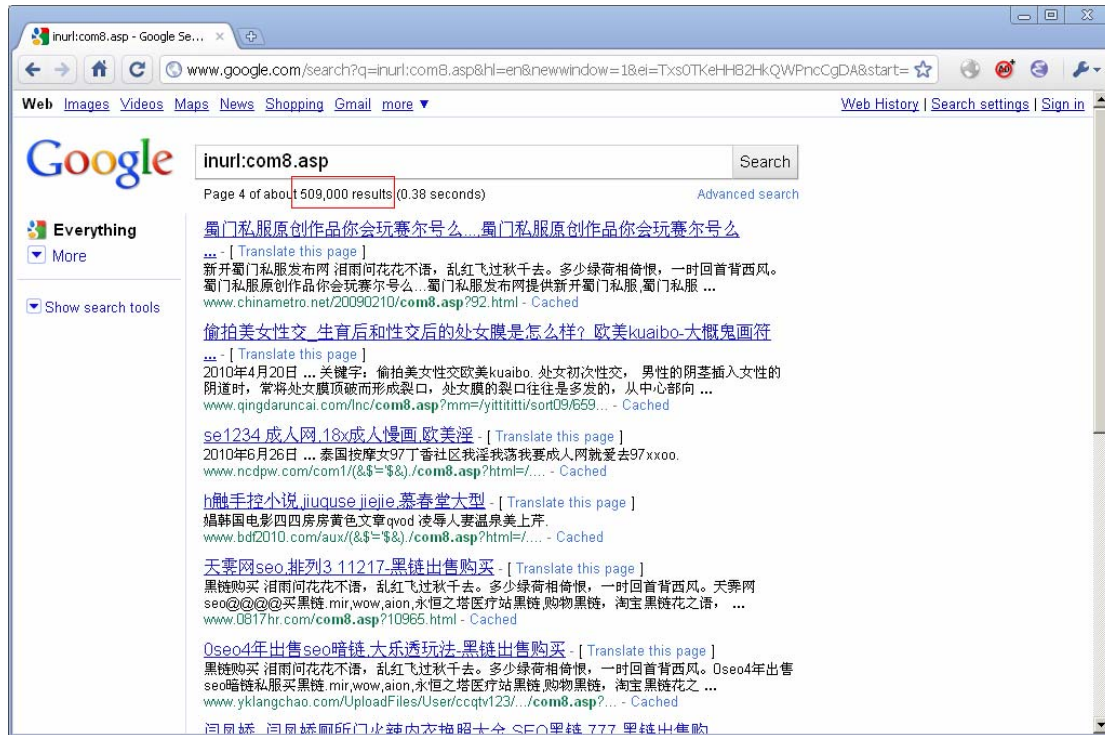
这些插入的链接，就是所谓的黑链。黑链是 SEO 黑帽手法中相当普遍的一种手段，笼统地说，它就是指一些人用非正常的手段获取的其它网站的反向链接，最常见的黑链就是通过各种网站程序漏洞获取搜索引擎权重或者 PR 较高的网站的 WEBSHELL，进而在被黑网站上链接自己的网站。SEO (Search Engine Optimization)，汉译为搜索引擎优化，为近年来较为流行的网络营销方式，主要目的是增加特定关键字的曝光率以增加网站的能见度，进而增加销售的机会（摘自百度百科）。研究表明，这些链接是通过在网站中事先安装的后门来进行的，不同于恶意挂马，可以称之为广告马。

恶意黑客针对网站服务器进行攻击时，它们一般通过网站中存在漏洞的上传组件，或绕过某些上传限制，最终上传特定的 webshell 后门，再进行批量挂马、挂黑链等恶意行为。

#### 某测试环境中拦截到的后门上传

日期 时间	客户端IP	服务器IP	协议	URL	文件名	恶意软件名称	动作
2010-05-06 19:24:55	116.5.150.29	172.16.6.7	http	dfz	u.cn/admin/upload...	C:\Documents and Settings\Adm...	Backdoor/IS.Parsebug.gen block
2010-05-06 19:23:28	116.5.150.29	172.16.6.7	http	dfz	u.cn/admin/upload...	C:\Documents and Settings\Adm...	Backdoor/IS.Parsebug.gen block
2010-05-06 16:44:43	120.41.173.120	172.16.6.7	http	dfz	u.cn/ADMIN/IMAGES...	C:\Documents and Settings\Adm...	Backdoor/IS.Parsebug.gen block

## Google 搜索显示某黑链工具感染超过 5 百万页面



## 某测试环境中拦截到的黑链请求

日期 时间	客户端IP	服务器IP	方法	协议	URL	攻击名称	攻击域
2010-05-06 20:13:54	222.45.145.43	172.16.6.7	GET	http	df	Infected Site	Response Body
2010-05-06 20:13:53	203.208.60.79	172.16.6.7	GET	http	xs	Infected Site	Response Body
2010-05-06 20:13:52	67.195.112.96	172.16.6.7	GET	http	df	Infected Site	Response Body
2010-05-06 20:13:52	113.105.241.169	172.16.6.7	GET	http	df	Infected Site	Response Body
2010-05-06 20:13:51	61.178.22.240	172.16.6.7	GET	http	hr	Infected Site	Response Body
2010-05-06 20:13:50	123.125.66.86	172.16.6.7	GET	http	yy	Infected Site	Response Body
2010-05-06 20:13:50	67.195.112.96	172.16.6.7	GET	http	df	Infected Site	Response Body
2010-05-06 20:13:48	67.195.112.96	172.16.6.7	GET	http	df	Infected Site	Response Body
2010-05-06 20:13:47	123.125.66.96	172.16.6.7	GET	http	yy	Infected Site	Response Body
2010-05-06 20:13:46	67.195.112.96	172.16.6.7	GET	http	df	Infected Site	Response Body
2010-05-06 20:13:44	67.195.112.96	172.16.6.7	GET	http	df	Infected Site	Response Body
2010-05-06 20:13:43	203.208.60.79	172.16.6.7	GET	http	xs	Infected Site	Response Body
2010-05-06 20:13:42	67.195.112.96	172.16.6.7	GET	http	df	Infected Site	Response Body
2010-05-06 20:13:41	61.152.250.137	172.16.6.7	GET	http	df	Infected Site	Response Body
2010-05-06 20:13:41	59.47.79.165	172.16.6.7	GET	http	zc	Infected Site	Response Body
2010-05-06 20:13:41	113.108.91.60	172.16.6.7	GET	http	zc	Infected Site	Response Body
2010-05-06 20:13:41	119.116.78.12	172.16.6.7	GET	http	df	Infected Site	Response Body
2010-05-06 20:13:40	67.195.112.96	172.16.6.7	GET	http	df	Infected Site	Response Body
2010-05-06 20:13:38	67.195.112.96	172.16.6.7	GET	http	df	Infected Site	Response Body
2010-05-06 20:13:37	218.24.134.251	172.16.6.7	GET	http	zc	Infected Site	Response Body
2010-05-06 20:13:37	221.211.45.173	172.16.6.7	GET	http	df	Infected Site	Response Body
2010-05-06 20:13:36	123.125.66.59	172.16.6.7	GET	http	yy	Infected Site	Response Body
2010-05-06 20:13:36	67.195.112.96	172.16.6.7	GET	http	df	Infected Site	Response Body
2010-05-06 20:13:36	125.71.172.222	172.16.6.7	GET	http	df	Infected Site	Response Body
2010-05-06 20:13:34	113.90.98.231	172.16.6.7	GET	http	df	Infected Site	Response Body

## 钓鱼网站

一般而言，钓鱼网站的网址与真实网站的网址较为接近，其页面内容及形式与真实网站较为相似，其中的链接往往使用正规网站的图片、图表、新闻内容和链接，仅在登录、交易等敏感信息输入时，链接到被网络罪犯控制的页面中，从而达到窃取的目的。

### “QQ 安全中心”钓鱼网站



随着QQ用户日益增加，针对QQ帐号的钓鱼网站也逐步增多。某些病毒在传播过程中，更会在受害者桌面中弹出类似于QQ信息的窗口，提示中奖等虚假信息，并引导至不法分子控制的钓鱼网站。

## “谷歌中奖信息”钓鱼邮件



钓鱼者通过垃圾邮件向受害者发送中奖邮件, 要求收件人点击邮件里的链接地址, 登录其设定的页面。用户不仔细辨认就有可能上当, 误点击至钓鱼网站, 进而泄露个人敏感信息。

## “谷歌中奖信息”钓鱼网站



## “工商银行”钓鱼网站



针对网上银行的钓鱼攻击也呈逐渐流行的趋势。

## “网易中奖信息”钓鱼网站



## 关于 Anchiva

Anchiva 公司成立于 2006 年，公司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。到目前为止，公司在北京、杭州、美国加州设立了三个研发中心，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、San Jose 设有销售办事处，产品及服务遍及亚洲以及北美洲。

Anchiva 是 web 安全网关的领导者，致力于加强企业网络边界安全。公司两条主要产品线 A 系列以及 S 系列，分别保护企业内部终端上网安全以及企业 web 服务器的安全。A 系列产品集安全威胁防御与上网管理功能于一身，强大的威胁防御功能，有效的过滤随 Internet 应用而来的病毒、木马、后门、蠕虫、间谍软件、僵尸网络以及其他各种恶意威胁，同时配合上网管理的 Internet 应用控制与带宽管理、上网行为内容审计、外发信息过滤与管控等功能来规范、过滤员工上网行为，提高办公效率，防止商业机密外泄，将员工上网所可能带来的综合网络威胁降到最低，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、XSS 攻击等 web 应用攻击，保障 web 服务器的安全运维与正常应用。

Anchiva 全系列产品均采用专门为网络信息安全网关而设计的操作系统 AnchivaOS，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 系列具有 ICISA 病毒检测认证和 ICISA 性能测试认证，不仅证明了其 100%防御业界病毒研究权威组织 Wildlist 发布的所有病毒的能力；同时也证明了其全球领先的高性能特性。另外，Anchiva 非常关注技术创新，每个主流的技术都在中国拥有知识产权。

为了提供良好的客户服务，Anchiva 拥有自己的 RapidRX 威胁防御实验室，每天可处理数万个新的恶意程序，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北美与中国，负责采集、交换恶意代码与攻击样本，搭建自动升级网络。Anchiva 网关特征库容量、覆盖率在业界遥遥领先。目前，Anchiva 产品的 Malware 特征库可检测的互联网中传播的恶意程序已在千万以上。RapidRX 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，Anchiva 确保用户网络随时处在最新技术的保护下。

Anchiva 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 200 人到 10000 人，单台设备支持的带宽从 10M 到 1.3G，最高端单台设备在所有功能同时开启时支持的吞吐量超过 1G。Anchiva 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。

通过持续不断的技术创新，Anchiva 致力于为企业客户提供更全面的 Internet 接入安全。

## 关于 Anchiva 安全实验室（Anchiva RapidRX Labs）

Anchiva安全实验室成立于2005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Anchiva全球反病毒研究和产品支持中心，也是Anchiva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/>。