

# Anchoriva 威胁报告 (2010 年第一季度)

作者: Anchoriva 安全实验室

## 目录

|                               |    |
|-------------------------------|----|
| Malware 威胁概况 .....            | 3  |
| Web Malware Top20 .....       | 3  |
| Email Malware Top20 .....     | 5  |
| 恶意网站 Top20.....               | 7  |
| 极光行动 (Operation Aurora) ..... | 8  |
| Web 服务器面临的后门威胁 .....          | 9  |
| 钓鱼网站.....                     | 12 |
| 关于 Anchiva .....              | 14 |
| 关于 Anchiva RapidRX Labs ..... | 14 |

## 图表目录

|  |    |
|--|----|
| “QQ 用户 10 周年庆典” 钓鱼网站 .....                 | 12 |
| “开心辞典” 钓鱼网站 .....                          | 12 |
| Google Doc 被用于钓鱼网站 I .....                 | 13 |
| Google Doc 被用于钓鱼网站 II .....                | 13 |
| 后门功能截图 I.....                              | 10 |
| 后门功能截图 II.....                             | 10 |
| 某客户中 Backdoor/ASP.Ace.1F62 的部分拦截记录 .....   | 11 |
| Exploit/JS.CVE-2010-0249 拦截情况 .....        | 9  |
| 恶意网站 Top20.....                            | 8  |
| Email Malware Top20 .....                  | 6  |
| 某客户中 Trojan/Downloader.F743 的部分拦截记录.....   | 7  |
| Web Malware Top20 .....                    | 4  |
| 某客户中 Trojan/HTML.IFrame.F06E 的部分拦截记录 ..... | 5  |
| 2010 年第一季度 Malware 类别比例图 .....             | 3  |

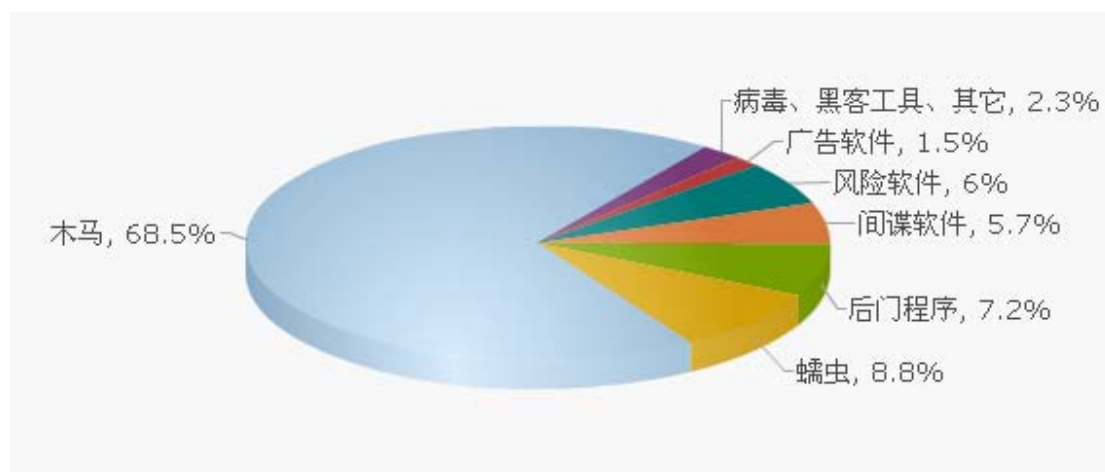
### Q1 2010 Anchiva 季度威胁报告大事记

- Anchiva 截获各类 Malware 将近 150 万，木马依然猖獗
- 木马、后门是 Web 安全的主要威胁
- 假冒杀毒软件依然活跃，组成僵尸网络
- “.cn” 域名在恶意网站中大幅减少
- 漏洞从公布到被恶意利用时差越发缩短
- 钓鱼网站利用人们趋利心理进行欺骗

### Malware 威胁概况

本季度 Anchiva 安全实验室共截获各类 Malware 约 150 万。木马所占的比例与上季度相比大为上升，将近 70%。其余依次为蠕虫、后门程序、间谍软件、风险软件和广告软件，传统病毒和其它类别所占比例与上季度没有变化。

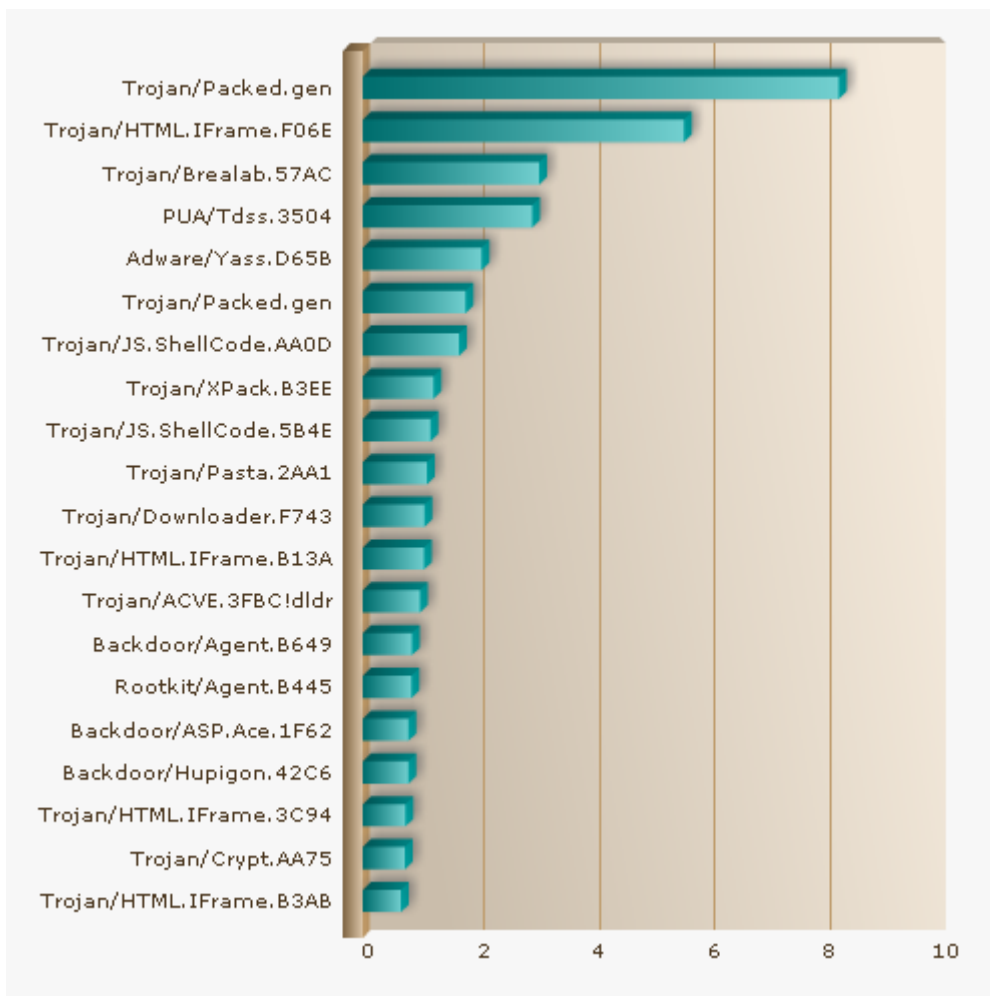
2010 年第一季度 Malware 类别比例图



### Web Malware Top20

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

## Web Malware Top20



本季度 Web Malware 威胁前 20 中木马、后门占绝大多数，通过下载者、利用漏洞等方式传播恶意软件依然是攻击者所热衷的方式。

**Trojan/HTML.IFrame.F06E:** 挂马集团通过该木马传播其它恶意软件。攻击者首先把一段脚本通过感染、SQL 注入等方式挂到成千上万的正常网站。当用户浏览正常网站时，该脚本载入很多隐藏的 Iframe，进而载入另一挂马服务器、恶意站点中存在的恶意软件，达到传播的目的。相较上一季度，该木马上升很快，占据本次 Top20 第二位。

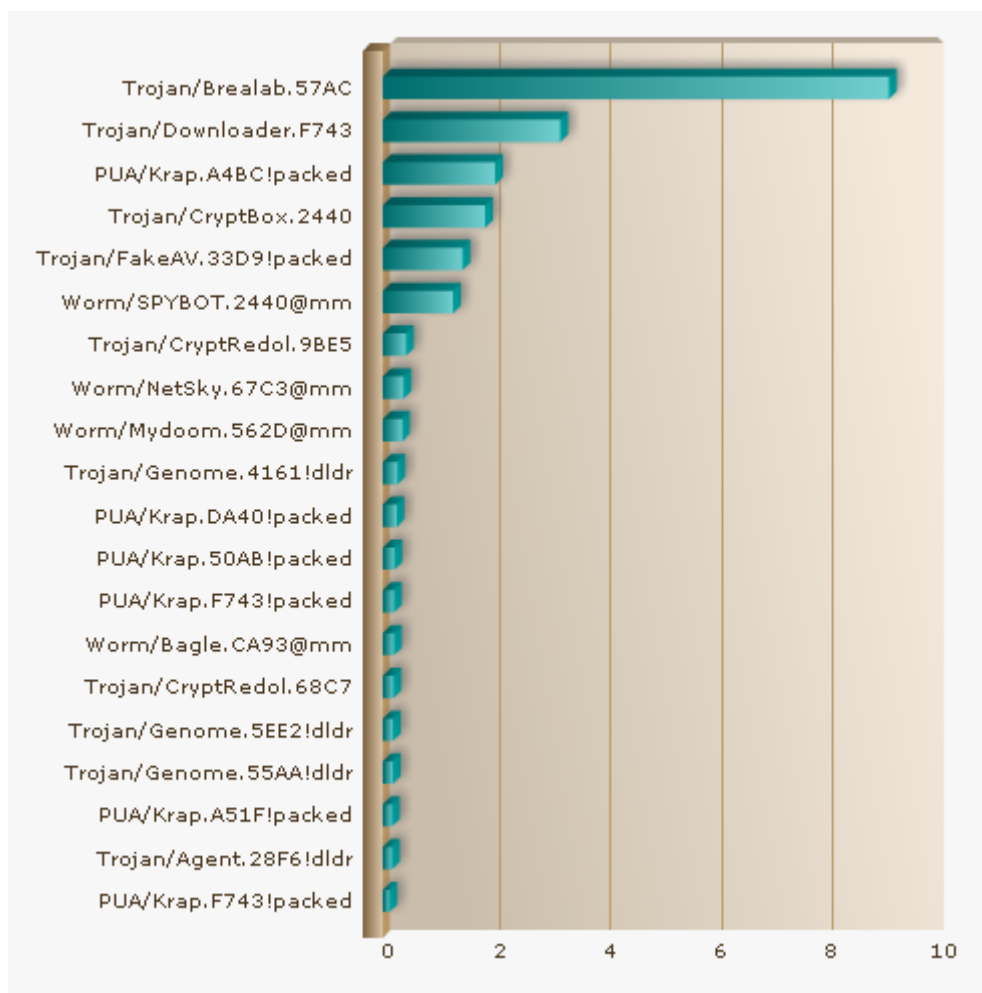
## 某客户中 Trojan/HTML.IFrame.F06E 的部分拦截记录

| date                | name                    | url   |
|---------------------|-------------------------|---|
| 2010-03-22 08:37:53 | Trojan/HTML.IFrame.F06E | www.t :om.cn/js/ads.js?google__             |
| 2010-03-22 08:37:47 | Trojan/HTML.IFrame.F06E | www.t :om.cn/js/ads.js?google__             |
| 2010-03-22 08:37:46 | Trojan/HTML.IFrame.F06E | www.t :om.cn/js/ads.js?google__             |
| 2010-03-16 13:58:31 | Trojan/HTML.IFrame.F06E | google v/js/google.js?ads_it168.c0m_420x760 |
| 2010-03-15 18:09:44 | Trojan/HTML.IFrame.F06E | google v/js/google.js?ad_it168.com_420x760  |
| 2010-03-15 16:36:27 | Trojan/HTML.IFrame.F06E | google v/js/google.js?ad_it168.com_420x760  |
| 2010-03-15 16:07:04 | Trojan/HTML.IFrame.F06E | google v/js/google.js?ad_it168.com_420x760  |
| 2010-03-15 14:14:36 | Trojan/HTML.IFrame.F06E | www.s e.com/images/banner.jpg               |
| 2010-03-15 14:14:33 | Trojan/HTML.IFrame.F06E | www.s e.com/images/banner.jpg               |
| 2010-03-15 14:14:26 | Trojan/HTML.IFrame.F06E | www.s e.com/images/banner.jpg               |
| 2010-03-15 14:14:11 | Trojan/HTML.IFrame.F06E | www.s e.com/images/banner.jpg               |
| 2010-03-15 14:13:57 | Trojan/HTML.IFrame.F06E | www.s e.com/images/banner.jpg               |
| 2010-03-15 14:09:59 | Trojan/HTML.IFrame.F06E | google v/js/google.js?ad_it168.com_420x760  |
| 2010-03-15 13:54:00 | Trojan/HTML.IFrame.F06E | google v/js/google.js?ad_it168.com_420x760  |
| 2010-03-15 08:38:47 | Trojan/HTML.IFrame.F06E | www.c is/ad.js?nokiaads                     |
| 2010-03-14 22:24:37 | Trojan/HTML.IFrame.F06E | www.c is/ad.js?nokiaads                     |
| 2010-03-14 20:01:06 | Trojan/HTML.IFrame.F06E | www.s e.com/images/banner.gif               |
| 2010-03-14 20:00:08 | Trojan/HTML.IFrame.F06E | www.s e.com/images/banner.gif               |
| 2010-03-14 19:58:55 | Trojan/HTML.IFrame.F06E | www.s e.com/images/banner.gif               |
| 2010-03-14 10:51:05 | Trojan/HTML.IFrame.F06E | www.c is/ad.js?nokia                        |
| 2010-03-14 10:50:31 | Trojan/HTML.IFrame.F06E | www.c is/ad.js?nokia                        |

## 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



延续上一季度，假冒杀毒软件传播依然活跃、破坏性很大。Top 20 中 Trojan/Downloader.F743、PUA/Krap 家族、Trojan/FakeAV.33D9!packed 等均与假冒杀毒软件的传播相关。假冒杀毒软件一旦运行，它会阻止正常杀毒软件的查杀、禁止安全补丁自动更新，且一般难以卸载，甚至要求付费。假冒杀毒软件还可能把受害者机器变成僵尸网络的一部分，用于 DDOS 攻击、传播垃圾邮件等。Trojan/Brealab.57AC 在本季度中分别在 Web Malware Top 20 和 Email Malware Top 20 中居前列。它伪装成微软 Word 文档，诱使接收者打开该附件。运行后，它修改受害者的浏览器主页，安装一个 BHO（浏览器插件），并下载其它恶意软件。PUA/Krap 家族伪装、下载假冒杀毒软件，其活动频繁，前 20 中占据六个席位。

Trojan/Downloader.F743: 从特定站点下载假冒杀毒软件，并能通过邮件传播。

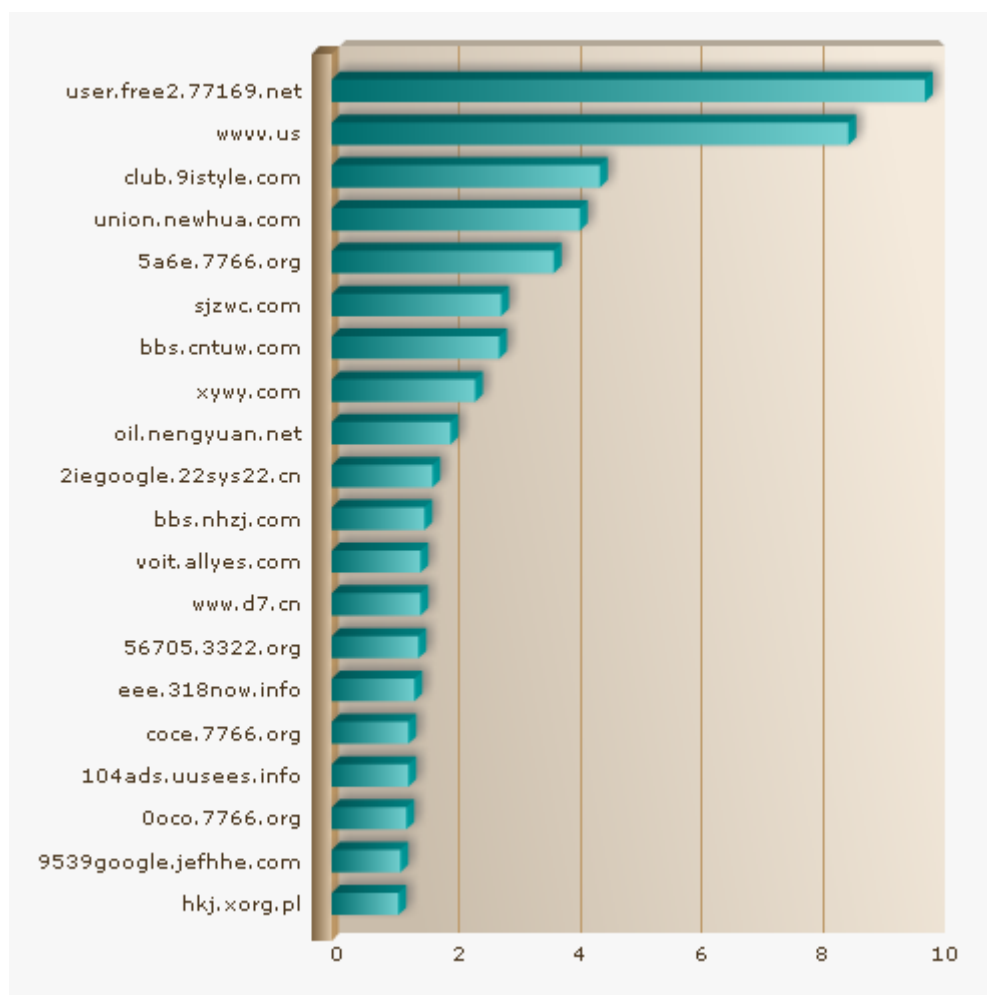
## 某客户中 Trojan/Downloader.F743 的部分拦截记录

| date                | name                   | protocol |
|---------------------|------------------------|----------|
| 2010-02-12 16:09:11 | Trojan/Downloader.F743 | smtp     |
| 2010-02-12 16:09:08 | Trojan/Downloader.F743 | smtp     |
| 2010-02-12 15:34:12 | Trojan/Downloader.F743 | smtp     |
| 2010-02-12 15:33:48 | Trojan/Downloader.F743 | smtp     |
| 2010-02-12 15:33:35 | Trojan/Downloader.F743 | smtp     |
| 2010-02-12 15:31:14 | Trojan/Downloader.F743 | smtp     |
| 2010-02-12 15:31:09 | Trojan/Downloader.F743 | smtp     |
| 2010-02-12 15:31:02 | Trojan/Downloader.F743 | smtp     |
| 2010-02-12 13:56:38 | Trojan/Downloader.F743 | smtp     |
| 2010-02-12 13:55:23 | Trojan/Downloader.F743 | smtp     |
| 2010-02-12 13:54:20 | Trojan/Downloader.F743 | smtp     |
| 2010-02-12 13:51:34 | Trojan/Downloader.F743 | smtp     |
| 2010-02-12 13:50:59 | Trojan/Downloader.F743 | smtp     |
| 2010-02-12 13:50:11 | Trojan/Downloader.F743 | smtp     |
| 2010-02-12 09:54:20 | Trojan/Downloader.F743 | smtp     |
| 2010-02-12 09:53:32 | Trojan/Downloader.F743 | 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



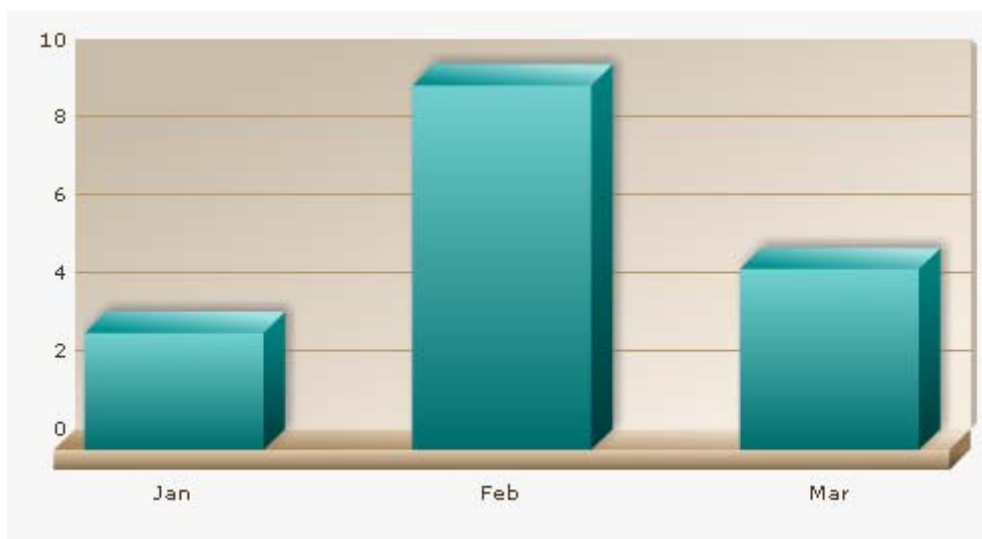
本季度恶意网站 Top 20 相较上一季度，不再是“.cn”域名独占的景象了，表明随着 09 年 12 月后，中国互联网信息中心（cnnic）开始加强域名注册信息审核，有效阻止了部分恶意网站的传播途径。以上列表中，可以注意到相当一部分网站是正常网站，被利用寄存、传播恶意软件，例如 union.newhua.com、bbs.cntuw.com 等。另一部分恶意站点则是 7766.org、3322.org、8800.org 等免费域名转向服务提供的二级域名。

## 极光行动（Operation Aurora）

2010 年 1 月 12 日，Google 在它的官方博客上披露了该公司遭到网络攻击的部分情况。该攻击利用了 Internet Explorer 浏览器中存在的漏洞，执行恶意代码，远程安装了恶意软件。恶意软件中显示了其编译时所在路径的一部分为 aurora，因而

该攻击被命名为极光行动。这是一次典型的有针对性的挂马攻击。其漏洞细节随后不久被公布，并有安全研究人员把它移植到了 Metasploit 的攻击库中（一个开源的攻击工具）。随后不久，网络罪犯、挂马集团便开始更新其挂马工具，利用该漏洞进行其它恶意软件的传播、窃取信息和攫取利益。下图显示了利用方法被公布后，某客户中在本季度 Anchiva 拦截情况的柱状图。

Exploit/JS.CVE-2010-0249 拦截情况



挂马攻击是当今最流行的攻击方式，用户浏览正常网站都有可能受到攻击，令人防不胜防。随着网络的发展，漏洞从公开到被恶意利用的时间越来越短，用户在保持补丁自动更新的同时，还需保持警惕。

## Web 服务器面临的后门威胁

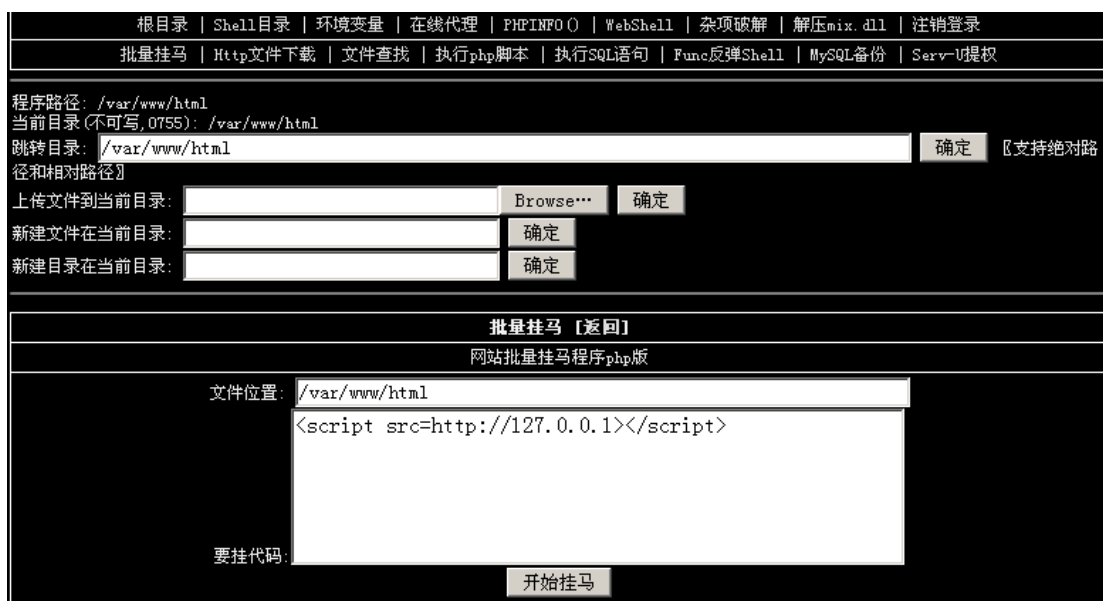
黑客针对 web server 的攻击方式层出不穷，通过扫描器扫描系统漏洞、SQL 注入工具进行网页渗透等等不一而足。Web 服务器被黑客植入后门同样非常普遍，我们在客户实际环境中发现，一个未受保护的服务器甚至存在 10 多个不同的 web 后门：

- <http://jyjs.{masked}.edu.cn/admin/Inc/conn.aspx>
- <http://jyjs.{masked}.edu.cn/admin/Inc/downx.aspx>
- <http://jyjs.{masked}.edu.cn/new.asp>
- <http://jyjs.{masked}.edu.cn/newss.asp>
- <http://cz.{masked}.edu.cn/tt.aspx>
- <http://cjlc.{masked}.edu.cn/111.asp>
- <http://cjlc.{masked}.edu.cn/1111.php>
- <http://cjlc.{masked}.edu.cn/a.asp>
- <http://cjlc.{masked}.edu.cn/ascii.asp>
- <http://cjlc.{masked}.edu.cn/ascii.php>
- <http://cjlc.{masked}.edu.cn/wq.php>
- <http://hq.{masked}.edu.cn/inc/x.aspx>
- <http://tjb.{masked}.edu.cn/查看可写.asp>
- <http://jyjs.{masked}.edu.cn/css.asp>

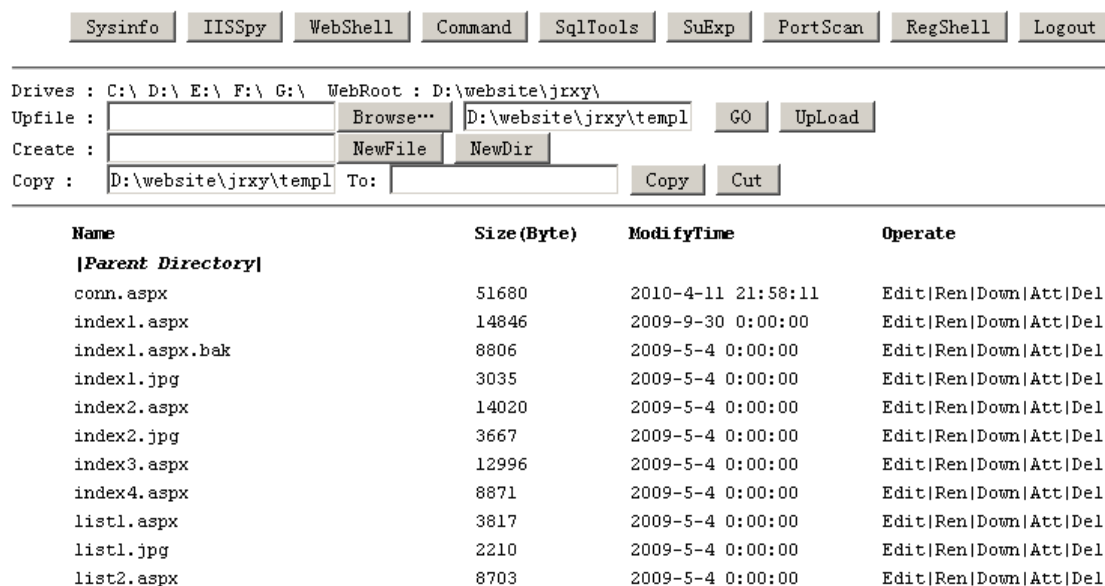
攻击者安装后门后，通常进行提权、上传/下载文件、内容篡改、端口扫描、内网渗透等操作，进一步造成破坏。后门为攻击者提供再一次进入服务器的便利的同时，有的还提供批量挂马功能，正如本季度恶意网站 Top 20 中显示的，把正常网站沦为恶意软件的传播基地。

下图是两个后门的截图，截获于某客户网络中未部署 Anchiva Web 应用防火墙之前。

后门功能截图 I



后门功能截图 II



某客户中 Backdoor/ASP.Ace.1F62 的部分拦截记录

| date                | name                  | url                                     |
|---------------------|-----------------------|---|
| 2010-03-17 13:06:37 | Backdoor/ASP.Ace.1F62 | crpp. du.cn/admin/upfile.asp            |
| 2010-03-17 13:06:08 | Backdoor/ASP.Ace.1F62 | crpp. du.cn/admin/upfile.asp            |
| 2010-03-17 13:05:29 | Backdoor/ASP.Ace.1F62 | crpp. du.cn/admin/upfile.asp            |
| 2010-03-17 13:04:53 | Backdoor/ASP.Ace.1F62 | crpp. du.cn/admin/upfile.asp            |
| 2010-03-17 11:21:04 | Backdoor/ASP.Ace.1F62 | cjlc.z lu.cn/111.asp                    |
| 2010-03-17 11:21:02 | Backdoor/ASP.Ace.1F62 | cjlc.z lu.cn/111.asp                    |
| 2010-03-16 17:52:03 | Backdoor/ASP.Ace.1F62 | cjlc.z lu.cn/111.asp                    |
| 2010-03-16 17:51:51 | Backdoor/ASP.Ace.1F62 | cjlc.z lu.cn/111.asp                    |
| 2010-03-16 17:51:50 | Backdoor/ASP.Ace.1F62 | cjlc.z lu.cn/111.asp                    |
| 2010-03-16 17:51:11 | Backdoor/ASP.Ace.1F62 | cjlc.z lu.cn/wq.asp                     |
| 2010-03-16 17:50:46 | Backdoor/ASP.Ace.1F62 | cjlc.z lu.cn/wq.asp                     |
| 2010-03-15 17:27:54 | Backdoor/ASP.Ace.1F62 | st.zl i.cn/upfile_soft.asp              |
| 2010-03-15 17:25:48 | Backdoor/ASP.Ace.1F62 | cba.: ju.cn/upfile_soft.asp             |
| 2010-03-14 21:53:46 | Backdoor/ASP.Ace.1F62 | jyjs.: ju.cn/admin/img.asp?Action2=Post |
| 2010-03-14 21:53:43 | Backdoor/ASP.Ace.1F62 | jyjs.: ju.cn/admin/img.asp?Action2=Post |
| 2010-03-14 16:11:02 | Backdoor/ASP.Ace.1F62 | dfzs. du.cn/admin/uploadfaceok.asp      |
| 2010-03-12 05:52:26 | Backdoor/ASP.Ace.1F62 | yxy. admin/uploadfaceok.asp             |
| 2010-03-11 13:35:36 | Backdoor/ASP.Ace.1F62 | yxy. admin/uploadfaceok.asp             |
| 2010-03-11 00:21:29 | Backdoor/ASP.Ace.1F62 | cba.: ju.cn/Upfile_Article.asp          |
| 2010-03-11 00:21:14 | Backdoor/ASP.Ace.1F62 | cba.: ju.cn/Upfile_Article.asp          |

上图显示的是 Anchiva 针对某一特定后门的拦截记录，在同一服务器上，显示已经存在的后门，如 111.asp、wq.asp，与绕过上传策略通过 upfile.asp、upfile\_soft.asp 等上传组件来上传后门的恶意行为。

## 钓鱼网站

## “QQ 用户 10 周年庆典” 钓鱼网站



## “开心辞典” 钓鱼网站



钓鱼者往往利用用户存在的趋利心理，通过伪造的中奖信息，引诱受害者输入账号、密码、生日、电话等敏感信息。上图“QQ用户10周年庆典”攻击中，网络罪犯还可利用这些信息，窃取Q币、向其好友行骗等。

Google Doc 被用于钓鱼网站 I

Google Doc 被用于钓鱼网站 I

Browser: Google  
URL: http://spreadsheets.google.com/viewform?formkey=dGZPaEkxdk5vOWpFQjNjdmkt

**Bug Habbo Club**

Coloque corretamente os Campos Abaixo para Multiplicar seus Mobis...  
 AVISO: este bug não multiplica cambios, só mobis.  
 Contas fantasmas não serão toleradas(terá que ter a conta a mais de 1 mês)  
 Aproveite :D

\* Required

**Nome Habbo \***  
 Coloque Corretamente

**Senha Habbo \***  
 Coloque Corretamente

**Data de Aniversário Habbo \***  
 Coloque Corretamente

Google Doc 被用于钓鱼网站 II

Google Doc 被用于钓鱼网站 II

Browser: Google  
URL: http://spreadsheets.google.com/viewform?formkey=dDN2QmFlbFcXy01yNFNHc1JrI

**Habbo Moedas Gratis ;)**

Bem vindos !!!  
 Maneira mais facio de obter moedas no habbo de graça é aqui !!

\* Required

**Nome Habbo : \***  
 Ex : victor123

**Senha Habbo : \***  
 Ex:1234567

**Minha conta é : \***

**Seu Habbo é : \***

钓鱼网站一般注册的域名与被钓鱼网站名称雷同，或稍有差别，比如数字“1”和字母“l”，以迷惑用户。用户稍不小心便可能被欺骗。而上面两图则是存在于 Google 提供的免费文档站点中，用户不可因为相信 Google 而放松警惕。

## 关于 Anchiva

Anchiva Systems 成立于 2006 年 2 月，公司汇集了来自国内外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 Netscreen、Trend Micro、Fortinet、Cisco 等国际企业中担任过重要职务。到目前为止，公司在北京、杭州、台湾、美国加州设立了四个研发中心，拥有超过百位优秀的研发人员。并在北京、上海、广州、香港、台湾、San Jose 设有办事处，产品及服务遍及亚洲以及北美洲。

Anchiva 是 Web 安全网关的领先者，着眼于 Internet 应用安全领域，致力于高性能 Web 安全网关的研发，为企业提供整合反恶意软件、URL 过滤、Internet 应用控制、带宽管理、Web 服务器内容保护等诸多功能的 Anchiva 系列 Web 安全网关 (Anchiva SWG)，帮助企业防御网络威胁，加强信息安全管理，提高生产效率。

Anchiva SWG 采用专门为内容安全而设计的操作系统 AnchivaOS，在自主研发的高性能 ASIC 安全芯片的驱动下，打破了传统应用安全性能瓶颈，为企业提供实时、全方位的安全防护。Anchiva SWG 通过 ICSA 病毒检测认证，能 100%覆盖流行病毒；同时通过 ICSA 性能测试，证明其全球领先的高性能特性。

Anchiva 拥有自己的 RapidRX 安全实验室，由经验丰富的病毒分析家和研究员组成，他们战略性的分布在美国，欧洲以及大中国区。Anchiva 特征库容量、覆盖率在业界遥遥领先，通过 Anchiva SWG 内置的 Malware 特征库可以找到多达 1000 万以上的威胁样本。RapidRX 安全实验室提供 24 小时不间断的升级服务，同时具有启发式扫描技术，确保用户网络随时处在最新技术的保护下，为了在最大限度降低误判的基础上提高查杀率，Anchiva 创新的开辟了多引擎的查杀技术。

Anchiva SWG 产品线分为高、中、低多个型号，覆盖用户由 100 人到 10000 人，为众多行业提供解决方案，客户覆盖金融、电信、教育、医疗、制造、政府、能源、零售等行业。

## 关于 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/>。