

# 安启华威胁报告（2009 年第三季度）

作者：安启华 RapidRX 安全实验室

## 目录

Malware 威胁概况.....	3
Web Malware Top20 .....	3
Email Malware Top20.....	6
恶意网站 Top20 .....	9
Web 服务器的安全.....	10
零日漏洞频现的 7 月.....	11
一个零日漏洞诱发的 SQL 注入攻击狂潮.....	12
钓鱼网站 .....	12
关于安启华(Anchiva) .....	15
关于安启华安全实验室 (Anchiva RapidRX Labs) .....	16

## 图表目录

2009 年第三季度 Malware 类别比例图 .....	3
Web Malware Top20 .....	4
Spyware/Onlinegame.BEA0 的拦截记录.....	5
Trojan/GIF.IFrame.gen 的拦截记录.....	5
Adware/PopupURL.6D69 的拦截记录 .....	6
Trojan/JS.Shellcode.5B4E 的拦截记录 .....	6
Email Malware Top20 .....	7
传播 Worm/Zafi.40D1@mm 的邮件.....	7
传播 Trojan/Pif.0441!dldr 的邮件 .....	8
传播 Spyware/Zbot.C877 的邮件.....	8
传播 Worm/FakeAlert.4840@mm 的邮件 .....	9
恶意网站 Top20.....	10
安启华 Web 防火墙关于某高校网站的攻击拦截统计 .....	11
利用零日漏洞的 Trojan/JS.Shellcode.0F5D 的拦截记录.....	11
Web SQL 注入攻击统计 .....	12
Web Malware 监测统计 .....	12
Ebay 钓鱼网站.....	13
淘宝钓鱼网站 .....	14
MSN 钓鱼网站.....	14
QQ 钓鱼网站 .....	15

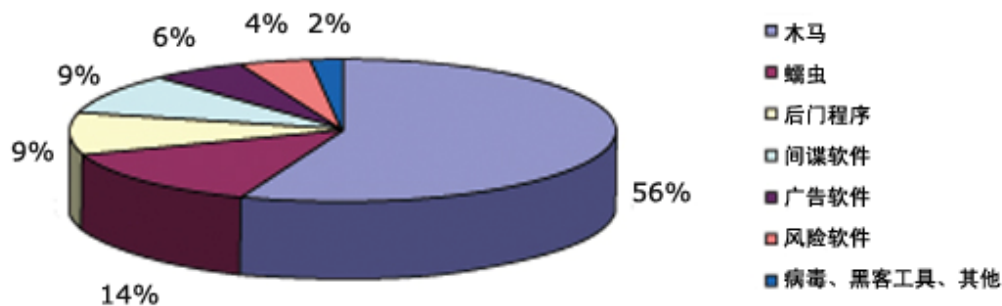
### Q3 2009 安启华季度威胁报告大事记

- 本季度安启华共截获约 150 万个 Malware，木马依旧位列第一，其余依次为蠕虫、后门程序、间谍软件、广告软件和风险软件，传统病毒和其它类别所占比例仅占 2% 左右。
- 本季度 Web 威胁中 Spyware/Onlinegame.BEA0 异常活跃。20 种最活跃 Malware 类别中网页脚本类占半数以上。
- 邮件威胁前 20 名中，10 个新 Malware 上榜，其中的 Spyware/Zbot.C877 来势汹汹，以窃取网银等重要帐号密码为目标。
- 安启华公布发布恶意软件数量最多的前 20 个恶意网站。
- 某高校网站日受攻击 2000 次，SQL 注入和跨站脚本攻击是主流。
- 7 月份零日漏洞接二连三，互联网安全形势异常严峻。
- SQL 注入携手零日漏洞发起攻击狂潮，安启华 WAF 联合防毒网关筑起铜墙铁壁。
- 网络钓鱼攻击本土化，淘宝和 QQ 成钓鱼新宠。

## Malware 威胁概况

本季度安启华安全实验室共截获各类 Malware 约 150 万，比上季度略有上升。木马所占的比例与上季度相同，仍占一半以上。其余依次为蠕虫、后门程序、间谍软件、广告软件和风险软件，传统病毒和其它类别所占比例仅占 2% 左右。

2009 年第三季度 Malware 类别比例图



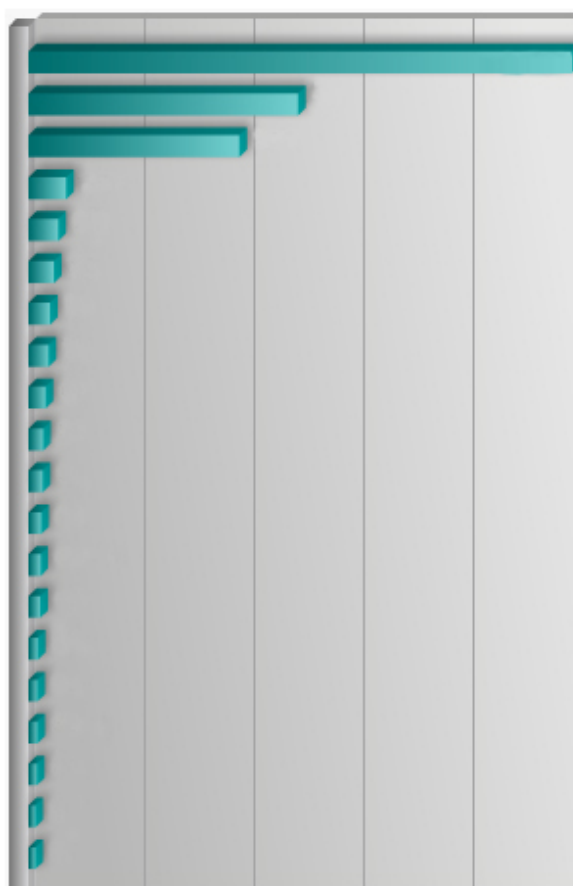
## Web Malware Top20

根据安启华 Malware 监测网的监测结果，本季度的 Web 威胁中，出现频率最高的前 20 个 Malware 如下图所示。引人注目的是 Spyware/Onlinegame.BEA0 这个 Malware 异常活跃，另外在这 20 个 Malware 中，网页脚本类（红色名称的）占了

14 个。对于一个 Web 防病毒网关来说，拦截了这些恶意脚本，也就阻挡了随之而来的大量恶意软件，可以起到事半功倍的效果。

### Web Malware Top20

Spyware/Onlinegame.BEA0  
Trojan/GIF.IFrame.gen  
Adware/PopupURL.6D89  
Trojan/JS.ShellCode.5B4E  
Trojan/Packed.gen  
Trojan/HTML.IFrame.EDA6  
Trojan/HTML.IFrame.9F8D  
PUA/Cnsmin.5B5E  
Trojan/JS.Iframe.5F2A  
Trojan/JS.Shellcode.7C6F  
Exploit/JS.Agent.FA66  
Exploit/JS.OWCSheet.1B05  
Exploit/JS.Agent.BF0C  
PUA/CnsMin.6278  
Spyware/QQPass.8F4D  
Trojan/JS.Shellcode.0F5D  
Trojan/HTML.Iframe.9C89  
Exploit/JS.MS09002.5ECC  
Exploit/JS.Agent.58ED  
Spyware/Onlinegame.B2A0!pws



**Spyware/Onlinegame.BEA0:** 该间谍软件用来窃取多种网络游戏的帐号密码，窃取的信息将自动回传到特定的网站上。该间谍软件在本季度通过 Web 下载的方式大量传播，并产生了大量的变体，好消息是这些变体并不能逃脱安启华 Web 安全网关的检测。

## Spyware/Onlinegame.BEA0 的拦截记录

Time	Malware	URL
2009-07-01 06:18:39	Spyware/Onlinegame.BEA0	http://www.sdfsdfzxcvdfse.cn/25.exe
2009-07-01 06:19:17	Spyware/Onlinegame.BEA0	http://www.sdfsdfzxcvdfse.cn/22.exe
2009-07-01 06:19:25	Spyware/Onlinegame.BEA0	http://www.sdfsdfzxcvdfse.cn/23.exe
2009-07-01 06:23:34	Spyware/Onlinegame.BEA0	http://www.sdfsdfzxcvdfse.cn/1.exe
2009-07-01 06:25:05	Spyware/Onlinegame.BEA0	http://www.sdfsdfzxcvdfse.cn/24.exe
2009-07-01 06:38:04	Spyware/Onlinegame.BEA0	http://60.173.10.4/download/mhxu9m1.exe
2009-07-01 06:38:18	Spyware/Onlinegame.BEA0	http://60.173.10.4/download/wd9m.exe
2009-07-01 06:39:20	Spyware/Onlinegame.BEA0	http://60.173.10.4/download/dnf9m.exe
2009-07-01 06:39:26	Spyware/Onlinegame.BEA0	http://60.173.10.4/download/mhxu9m.exe
2009-07-01 06:40:16	Spyware/Onlinegame.BEA0	http://www.sdfsdfzxcvdfse.cn/1.exe

**Trojan/GIF.IFrame.gen:** 这是一些感染了木马链接的图片。一些网站曾经被黑客入侵过，黑客可以通过一个挂马工具将网站中的所有文件插入木马链接，一些图片因此也被感染，网站的管理员在恢复网站时可能忽略了这些图片，因此很多网站仍然包含这些有问题的图片。

## Trojan/GIF.IFrame.gen 的拦截记录

Time	Malware	URL
2009-07-01 07:29:25	Trojan/GIF.IFrame.gen	http://www2. .edu.cn/jw/Images/Gaobei_skin/C
2009-07-01 07:30:21	Trojan/GIF.IFrame.gen	http://www2. .edu.cn/jw/count/images/0.gif
2009-07-01 07:30:21	Trojan/GIF.IFrame.gen	http://www2. .edu.cn/jw/count/images/4.gif
2009-07-01 07:31:30	Trojan/GIF.IFrame.gen	http://www2. .edu.cn/jw/Images/Gaobei_skin/C
2009-07-01 07:32:54	Trojan/GIF.IFrame.gen	http://www2. .edu.cn/jw/count/images/4.gif
2009-07-01 07:33:50	Trojan/GIF.IFrame.gen	http://www2. .edu.cn/jw/count/images/8.gif
2009-07-01 07:35:53	Trojan/GIF.IFrame.gen	http://www2. .edu.cn/jw/count/images/0.gif
2009-07-01 07:38:40	Trojan/GIF.IFrame.gen	http://www. .com.cn/images/logo_gif.gif
2009-07-01 07:38:41	Trojan/GIF.IFrame.gen	http://www. .com.cn/images/submit.gif
2009-07-01 07:38:54	Trojan/GIF.IFrame.gen	http://www2. .edu.cn/jw/count/images/8.gif

**Adware/PopupURL.6D89:** 这是一个用于弹出广告网页的 JavaScript 程序，许多网站使用该程序来弹出广告，因此它在拦截记录中出现的频率也较高。

## Adware/PopupURL.6D89 的拦截记录

Time	Malware	URL
2009-07-01 08:13:22	Adware/PopupURL.6D89	http://popunder.paypopup.com/popup.php?id=lal
2009-07-01 08:13:23	Adware/PopupURL.6D89	http://popunder.adsrevenue.net/popup.php?124€
2009-07-01 08:20:45	Adware/PopupURL.6D89	http://popunder.adsrevenue.net/popup.php?124€
2009-07-01 08:42:30	Adware/PopupURL.6D89	http://popunder.adsrevenue.net/popup.php?124€
2009-07-01 08:52:24	Adware/PopupURL.6D89	http://popunder.paypopup.com/popup.php?id=lal
2009-07-01 08:59:03	Adware/PopupURL.6D89	http://popunder.paypopup.com/popup.php?id=lal
2009-07-01 08:59:33	Adware/PopupURL.6D89	http://popunder.paypopup.com/popup.php?id=lal
2009-07-01 09:26:47	Adware/PopupURL.6D89	http://popunder.adsrevenue.net/popup.php?124€
2009-07-01 09:45:07	Adware/PopupURL.6D89	http://popunder.adsrevenue.net/popup.php?124€
2009-07-01 09:46:14	Adware/PopupURL.6D89	http://popunder.adsrevenue.net/popup.php?124€

Trojan/JS.Shellcode.5B4E: 这是一个经过复杂编码的 JavaScript 程序, 它利用各种浏览器相关的漏洞自动下载安装一些 Malware 到用户的系统上。用户如果浏览了包含这些恶意脚本的网站, 就可能在不知不觉中感染了 Malware。

## Trojan/JS.Shellcode.5B4E 的拦截记录

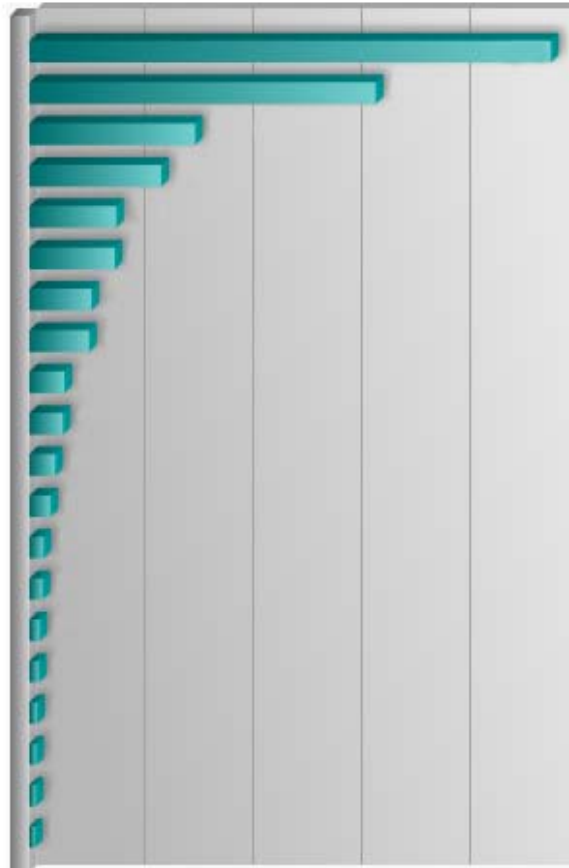
Time	Malware	URL
2009-08-15 03:33:58	Trojan/JS.ShellCode.5B4E	http://i1i1.cn/x18/b.jpg
2009-08-15 09:32:35	Trojan/JS.ShellCode.5B4E	http://dunhill.9966.org/root/3/go.jpg
2009-08-15 13:43:42	Trojan/JS.ShellCode.5B4E	http://dkny.9966.org/root/3/go.jpg
2009-08-15 13:43:42	Trojan/JS.ShellCode.5B4E	http://dkny.9966.org/root/3/hh.js
2009-08-15 13:43:46	Trojan/JS.ShellCode.5B4E	http://dkny.9966.org/root/3/of.js
2009-08-15 15:07:57	Trojan/JS.ShellCode.5B4E	http://ky.iciba.com/zujian/dongtai/a1/16/va
2009-08-15 16:30:30	Trojan/JS.ShellCode.5B4E	http://123.123dfas.cn/0808123456/xx.jpg
2009-08-15 20:09:40	Trojan/JS.ShellCode.5B4E	http://g1a1e.cn/x8/b.jpg
2009-08-15 21:35:32	Trojan/JS.ShellCode.5B4E	http://hjfgu.6600.org/aa/a.js
2009-08-15 21:35:34	Trojan/JS.ShellCode.5B4E	http://htyiu.6600.org/aa/a.js

## Email Malware Top20

根据安启华 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 如下图所示。其中红色标识的 10 个 Malware 是本季度新产生的, 其余 10 个是一些长期流行的较老蠕虫。

## Email Malware Top20

Worm/Zafi.40D1@mm  
Trojan/Pif.0441!dlldr  
Spyware/Zbot.C877  
Worm/FakeAlert.4840@mm  
Worm/NetSky.67C3@mm  
Trojan/FakeAlert.ED62  
Trojan/Murlo.136B!dlldr  
Trojan/FraudLoad.ED62!dlldr  
Worm/LovGate.64B7@mm  
Trojan/Krap.C512  
Worm/Mydoom.562D@mm  
Worm/Mydoom.5800@mm  
Worm/NetSky.F6C7@mm  
Trojan/Agent.9130!dlldr  
Trojan/Enpack.A3AB  
Backdoor/UltimateDefender.BFB2  
Worm/NetSky.Q@mm  
Worm/NetSky.A186@mm  
Worm/Mytob.5C39@net  
Trojan/Zbot.C749



Worm/Zafi.40D1@mm: 这是一个古老的邮件蠕虫，本季度又再次爆发。它会产生大量的垃圾邮件，并可对特定的网站产生 DDoS 攻击。

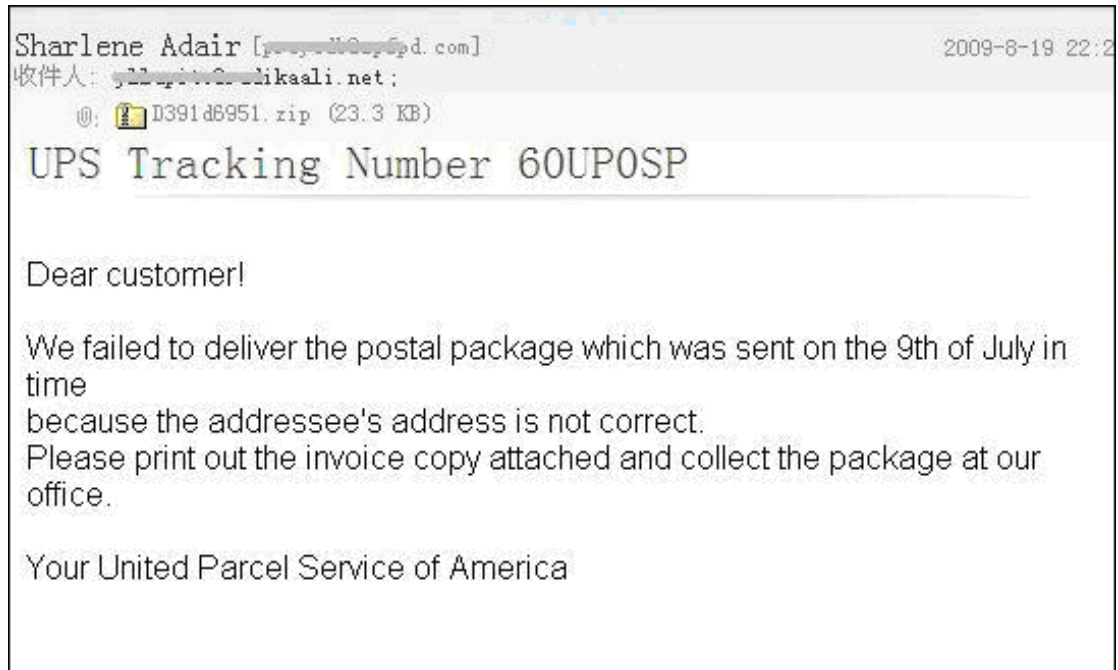
## 传播 Worm/Zafi.40D1@mm 的邮件



Trojan/Pif.0441!dlldr: 这是一个 PIF 文件，它被作为邮件附件发送。当接收者打开该附件时，它会通过 FTP 下载另一个 Malware 并运行它。Trojan/Pif.0441!dlldr 在台



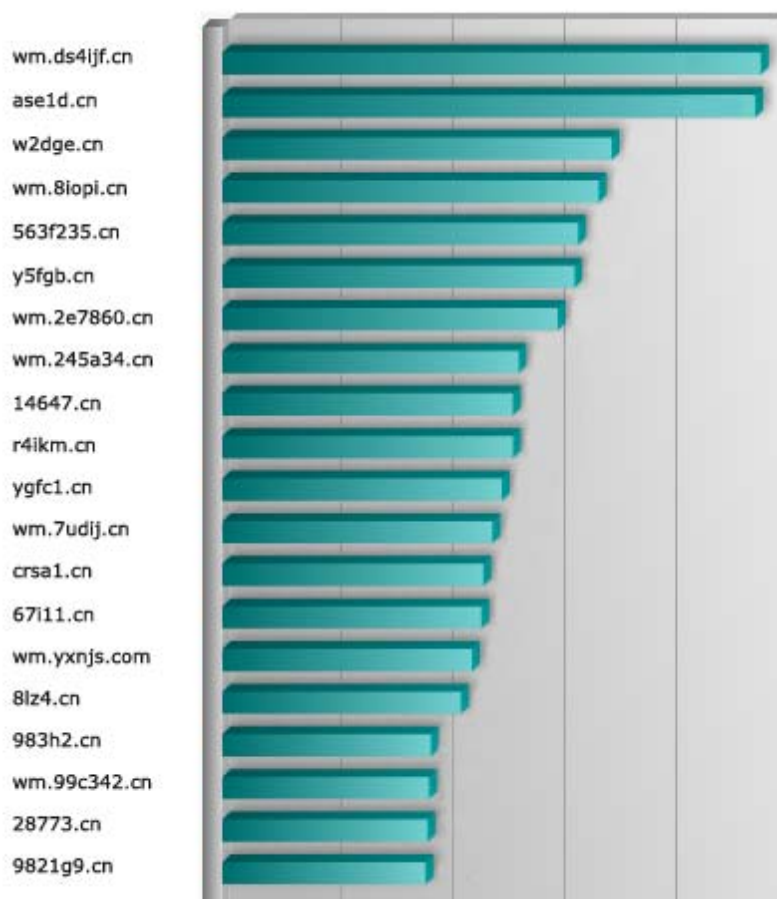
## 传播 Worm/FakeAlert.4840@mm 的邮件



## 恶意网站 Top20

根据安启华 Malware 监测网的监测结果，发布恶意软件数量最多的前 20 个恶意网站如下图所示。这些网站作为专用的恶意软件发布服务器，为大量的挂马网站提供了最终的恶意软件下载地址，同时这些网站也被作为众多恶意软件的升级服务器。安启华 Web 安全网关通过屏蔽这些恶意网站，有效的阻止了来自这些网站的 Malware 威胁。

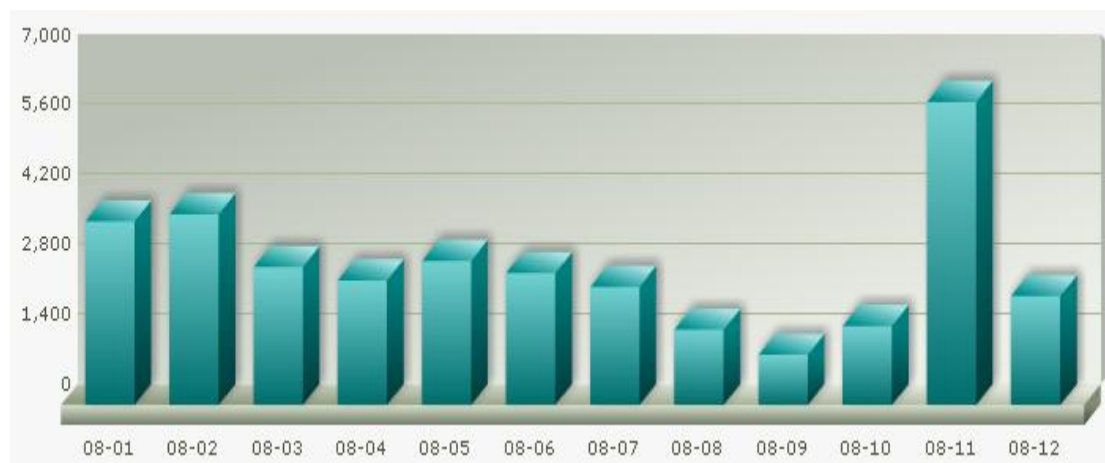
## 恶意网站 Top20



## Web 服务器的安全

现有的网站普遍采用动态网页加数据库模式，由于一些网站开发人员缺乏安全意识，使得 SQL 注入漏洞和跨站脚本漏洞普遍存在，而 SQL 注入攻击和跨站脚本攻击就成了当前最主要的 Web 攻击形式。下图显示某高校的网站平均每天受攻击次数达到了 2000 次以上。

安启华 Web 防火墙关于某高校网站的攻击拦截统计



## 零日漏洞频现的 7 月

让我们来回顾一下 7 月份出现的高危漏洞：

- 2009-07-06：微软公布视频零日漏洞（CVE-2008-0015）
- 2009-07-13：微软公布 Office 网页组件零日漏洞（CVE-2009-1136）
- 2009-07-22：Adobe 公布 Flash Player 零日漏洞（CVE-2009-1862）

不到一个月的时间，出现了三个高危的零日漏洞，而且这三个漏洞在公布时都已经被 Malware 所利用，这对广大计算机用户的上网安全造成了极大威胁。

下面是安启华实验室对一个利用微软视频零日漏洞的 Malware（Trojan/JS.Shellcode.0F5D）的监测结果，该 Malware 也位列本季度 Web Malware Top20。注意下表的检测时间(东 8 区)，我们在微软公布该漏洞前，就已经监测到了利用该漏洞传播的 Malware，成功的阻挡了利用该漏洞的 Malware 对用户发起的零日攻击，实现了对用户的零日保护。

利用零日漏洞的 Trojan/JS.Shellcode.0F5D 的拦截记录

Time	Malware	URL
2009-07-06 05:55:33	Trojan/JS.Shellcode.0F5D	http://6gerere3e.cn/04/go.jpg
2009-07-06 06:53:19	Trojan/JS.Shellcode.0F5D	http://6gerere3e.cn/04/go.jpg
2009-07-06 07:15:01	Trojan/JS.Shellcode.0F5D	http://6gerere3e.cn/04/go.jpg
2009-07-06 07:20:20	Trojan/JS.Shellcode.0F5D	http://6gerere3e.cn/04/go.jpg
2009-07-06 07:21:23	Trojan/JS.Shellcode.0F5D	http://6gerere3e.cn/04/go.jpg
2009-07-06 07:22:22	Trojan/JS.Shellcode.0F5D	http://ccfsdee32.cn/01/go.jpg
2009-07-06 07:24:23	Trojan/JS.Shellcode.0F5D	http://ccfsdee32.cn/01/go.jpg
2009-07-06 07:34:35	Trojan/JS.Shellcode.0F5D	http://6gerere3e.cn/04/go.jpg
2009-07-06 07:35:50	Trojan/JS.Shellcode.0F5D	http://6gerere3e.cn/04/go.jpg
2009-07-06 07:38:09	Trojan/JS.Shellcode.0F5D	http://ccfsdee32.cn/01/go.jpg

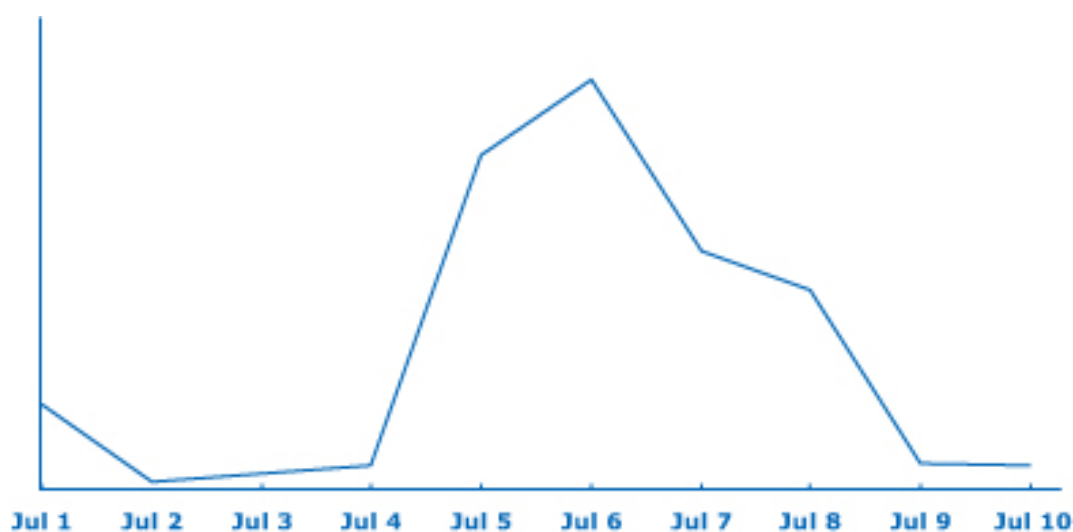
## 一个零日漏洞诱发的 SQL 注入攻击狂潮

7月5日，安启华的 Web 攻击监测系统显示，SQL 注入攻击的频率突然大幅度提高，攻击次数比平时高出了一个数量级。经分析，发现大量的 SQL 注入攻击代码都包含着一些木马链接，这些木马链接最终指向的恶意脚本都涉及到一个未知的漏洞。随后我们的 Malware 监测系统也显示了大量的网站被挂上了和该漏洞相关的网页木马（Trojan/JS.Shellcode.0F5D）。后经分析证实，这些 SQL 注入攻击所使用的网页木马（Trojan/JS.Shellcode.0F5D）利用的漏洞正是后来微软公布的零日视频漏洞（CVE-2008-0015）。

整个过程如下：黑客发现新漏洞=>编写利用漏洞的网页木马=>发起 SQL 注入攻击进行挂马=>一些网站被成功挂马=>访问该网站的用户被感染木马。

从下面的 Web 攻击监测图和 Web Malware 监测图可以看出，大范围的 SQL 注入攻击持续了四天，同期拦截的 Web Malware 数量也比平时高出一倍。

### Web SQL 注入攻击统计



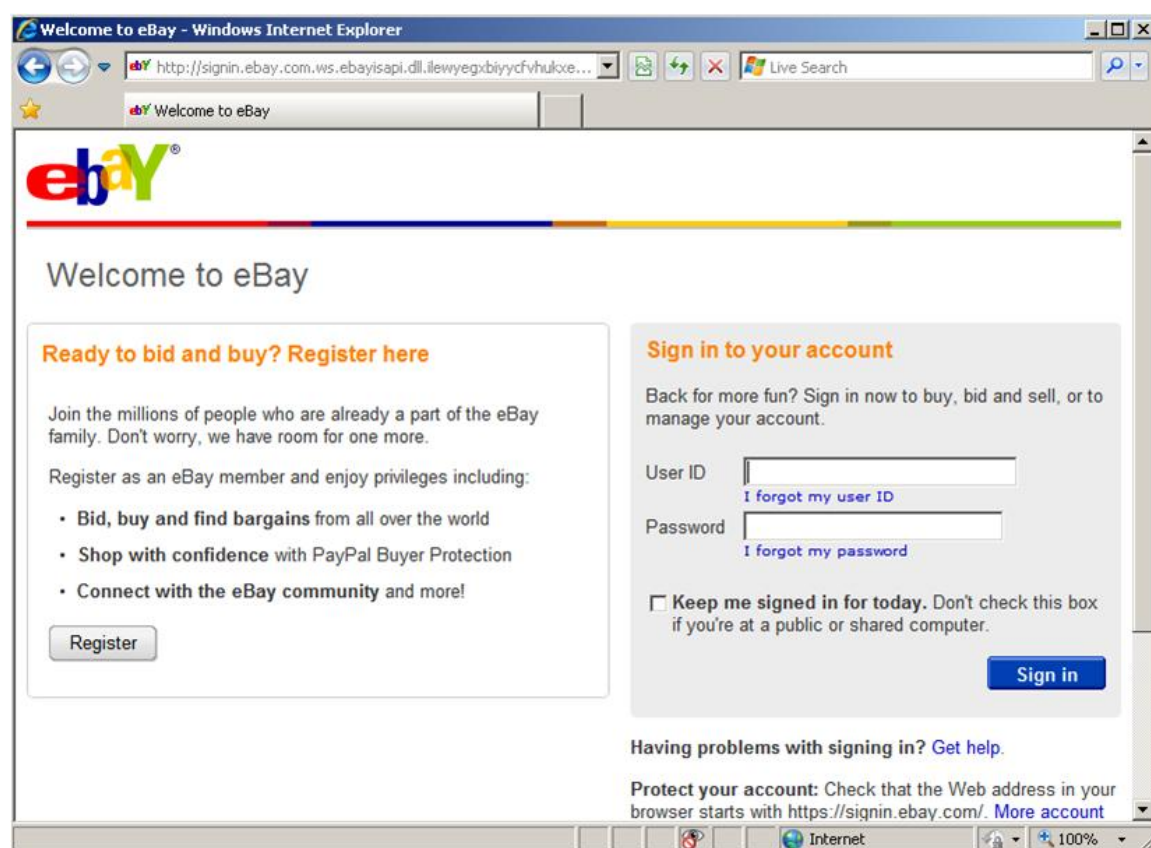
### Web Malware 监测统计



## 钓鱼网站

网上银行及网上支付系统仍然是钓鱼网站的主要针对目标，即时通讯工具和邮箱的帐号密码也成了钓鱼者的新目标，可以预见的是各种有价值的帐号信息（如网络游戏，社区论坛等）都可能成为新的钓鱼对象。针对淘宝网，QQ 的钓鱼攻击的兴起，也让中国地区的用户感受到了真实的威胁。

### Ebay 钓鱼网站



淘宝钓鱼网站



MSN 钓鱼网站



## QQ 钓鱼网站



## 关于安启华(Anchiva)

北京安启华科技有限公司（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，安启华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。更多资讯请访问<http://www.anchiva.com/virus/>。