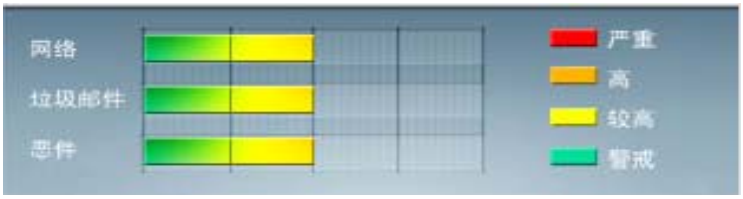
# 安全威胁每周警讯

2011/02/27～2011/03/05

本周威胁指数




***TrendMicro 中国区网络安全监控中心***

# 前十大病毒警讯

| 排名 | 病毒名称 | 威胁类型 | 风险等级 | 趋势 | 病毒行为描述 |
|---|---|---|---|---|---|
| **1** | TROJ_DOWNAD.INF | 木马 | ★★★ | ↑ | DOWNAD 蠕虫关联木马 |
| **2** | WORM_DOWNAD.AD | 蠕虫 | ★★★★ | ↓ | 该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒 |
| **3** | TROJ_IFRAME.CP | 木马 | ★★★ | → | GIF、jpg 和 SWF 文件中被插入一个恶意的 iframe 标记时，趋势科技会将其判断为 TROJ_IFRAME.CP 病毒。当这些文件被执行时，会重定向到这些 URL，并下载恶意程序 |
| **4** | WORM_DOWNAD | 蠕虫 | ★★★★ | → | 该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒 |
| **5** | Cryp_Xed-12 | 木马 | ★★★ | → | 疑似病毒 |
| **6** | WORM_ECODE.E-CN | 蠕虫 | ★★★★ | ↑ | E 语言病毒,产生与当前文件夹同名 exe 文件 |
| **7** | CRCK_KEYGEN | 破解程序 | ★★ | ↓ | 非法破解程序 |
| **8** | HTML_IFRAME.AZ | 网页病毒 | ★★ | → | 网页病毒,通常在网页在插入一个恶意 iframe,用户在访问该网页时会下载恶意文件或重定向到恶意网站 |
| **9** | Gray_Gen | 灰色软件 | ★★★ | → | 灰色软件的通用检测名。在用户不知情的情况下，在其电脑上安装后门、收集用户信息的软件 |
| **10** | PAK_Generic.001 | 加壳程序 | ★★ | → | 对加壳文件的通用检测。病毒通常会使用加壳手法来达到不被杀毒软件检测的目的 |

# 系统漏洞信息

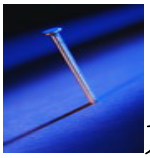
**MS10-101:Windows Netlogon 服务中的漏洞可能允许拒绝服务 (2207559)**

**受影响的软件:**

Windows 2003

Windows 2008

**描述:** 请见http://www.microsoft.com/china/technet/security/bulletin/MS10-101.mspx



# 系统安全技巧

摘要: 如今服务器便宜了，很多企业都购买了自己的网页服务器。在和别人分享自己的快乐的同时，却不得不考虑流量与安全问题，因为毕竟我们是在用低端服务器，哪能跟那些大把烧银子的服务器相比呢？下面我们就以常见的 IIS 发布的网站为便来看看如何解决这些问题。

如今服务器便宜了，很多企业都购买了自己的网页服务器。在和别人分享自己的快乐的同时，却不得不考虑流量与安全问题，因为毕竟我们是在用低端服务器，哪能跟那些大把烧银子的服务器相比呢？下面我们就以常见的 IIS 发布的网站为便来看看如何解决这些问题。

一、如何限制同时访问你网站的人数

依次单击“开始”→"程序" →“管理工具” →“Internet 服务管理器”，打开管理器窗口，单击机器名前面的加号，展开列表，右击“默认 Web 站点”项或者是你的站点名，选择“属性”命令，打开“属性”设置对话框。

然后选择“Web 站点”标签页，选择“连接”框中的“限制到”选项，然后在后面的输入框中输入你允许的最多同时在线的人数，如“50”。设置完成后，单击“确定”按钮保存设置。重启 IIS 服务后你的网站就只允许 50 个人同时在线浏览了！

二、如何限制网站的访问流量

如果网页内容只是普通的页面，那么人数多一点也没关系。但如果是下载服务器，那么对带宽和服务器 的压力将更大，这不仅要限制网站访问人数，也要限制网站的访问流量。打开“属性”对话框中，单击“性能”标签，单击选中“启用带宽限制”选项，然后在此选 项框中的“最大网络使用”后的文本框后输入你能承受的最大数据访问流量，比如我们把它改成“500KB/S”，最后单击“确定”按钮。重新启动 IIS 服务 后设置就可以生效了。

三、如何限制访问你网站的 IP 地址

对于一些重要的服务器，我们并不想让所有人都能访问，或者将一些总是攻击网站的用户屏蔽掉。这就需要添加限制访问风站的 IP 地址了。

将网站的属性窗口切换到“目录安全性”标签，这时我们可以看到“IP 地址及域名限制”选项框中， 通过选项框中的功能描述，可以确定我们要找的就是它了。单击框中的“编辑...”按钮，弹出的对话框，我们可以看到有两个选项：“授权访问”和“拒绝访问”。 如果你想网站只给少部分人浏览，可以选择“拒绝访问”，如相反则选“授权访问”项。

我们先来看“授权访问”，选择此项后，我们单击“添加”按钮，打开对话框，在这里我们可以将少部 分不允许访问我们的网站的 IP 黑名单输入进去。这里的黑名单可以是一台单独的机器，或是一个网段的机器，甚至可以是一个域内的所有机器。设置好后单击“确 定”按钮，这下那些黑名单份子就不得进来了！我们也可以看到添加的 IP 地址的访问设为了“被拒”，也就是“授权访问”中的例外不允许访问的范围，这样可以 正确理解为什么在 “授权访问”下添加的 IP 地址是拒绝访问的列表。

下面再来看“拒绝访问”，方法同“授权访问”一样，不过这里添加的可是“黄金账号”啊，只有你添加的 IP 才能访问你的网站！全部添加完毕后，一路“确定”保存设置，然后重启 IIS 服务就可以生效了。

好了，这里介绍的三个方法操作起来一点也不难，即使你不是网络管理人员，也能够轻松实现。想毕各位也要自己操练一下了吧，可以说合理设置好这三项，从此就不必再为经常当机而发愁了！

来源： IT168