
# 安全威胁每周警讯

2011/12/04～2011/12/11

本周威胁指数


***TrendMicro* 中国区网络安全监控中心**

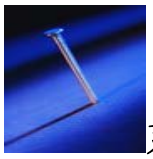

# 前十大病毒警讯

| 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 | 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 |
| 4 | 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 |
| 5 | CRCK_KEYGEN | 破解程序 | ★★ | ↑ | 非法破解程序 |
| 6 | TROJ_SPNR. | 木马 | ★★★ | ↑ | 木马病毒，由趋势科技主动式云端拦截技术检测，这类病毒通常是由于用户从恶意的 WEB 页面下载感染 |
| 7 | 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 |
| 8 | WORM_ECODE.E-CN | 蠕虫 | ★★★★ | ↓ | E 语言病毒,产生与当前文件夹同名 exe 文件 |
| 9 | Downloader_Agent | 下载器 | ★★ | ↑ | 下载器程序，由恶意程序释放所得，下载器会从外部恶意站点上下载其他的恶意程序到电脑上 |
| 10 | PAK_Generic.001 | 加壳文件 | ★★ | ↑ | 经过加壳技术加密的文件 |


# 系统漏洞信息

**MS11-083：**TCP/IP 中的漏洞可能允许远程执行代码 (2588516)
Windows Vista
Windows Server 2008
Windows 7
Windows Server 2008 R2

**描述：**http://technet.microsoft.com/zh-cn/security/bulletin/MS11-083



# 系统安全技巧

随着无线网络的普及，电脑用户实现了随时在家庭进行互联网冲浪的梦想。与此同时，由于无线网络的暴露性，极易给黑客留下可乘之机。建议电脑安全软件程序设计人员在开发软件时，将各种安全设置设计得更为简捷适用，使电脑用户很快能够熟悉使用。

尽管当前大多数无线网络在使用的同时都配备有安全软件作为保护屏障,以防止黑客对电子邮件或者其他文档的浏览，但许多电脑用户面对功能复杂、难以操作的 电脑安全软件不知所措，使他们的电脑失去安全软件的保护;另外一些电脑用户没有更改原来由制造商提供的默认密码，但对于电脑知识无所不晓的网络黑客而言， 他们略施小计，就可以轻松突破密码保护，进入用户电脑系统。一个不安全的无线网络可能造成服务丢失或是被利用来对其他网络发起攻击。为了避免类似的一些无线网络安全漏洞，这里我们介绍几种便捷的无线网络安全技巧。

**改变无线路由口令**

为无线路由的互联网访问设置一个口令至关重要，一个强口令有助于无线网络的安全，但不要使用原始无线路由器的默认口令，建议更改较为复杂的口令避免简单被攻破。

**添加加密协议**

无线加密协议(WEP)是无线网络上信息加密的一种标准方法。现在出产的无线路由器几乎都向用户提供加密数据的选择，妥善使用此功能就可以避免自己的银行账户的细节信息(包括口令等)被居心叵测的人截获。不过，需要注意，Wi-Fi 保护访问技术(WPA 和 WPA2)要比 WEP 协议更加强健，因此在保障无线通信安全方面作用更大。

**MAC 地址过滤**

这种功能是通过比较试图连接到路由器的设备 MAC 地址和路由器所保存设备的 MAC 地址而实现的。因此，通过启用这种特性，并且只告诉路由器本单位或家庭中无线设备的 MAC 地址，我们就可以防止他人盗用自己的互联网连接，从而提升安全性。

**非使用时关闭无线网络**

如果用户的无线网络并不需要每周的 24 小时都提供服务，可以通过关闭它而减少被黑客们利用的机会但对一个系统安全性的最重大改进措施之一就是直接关闭它，可能对于企业来说，关闭是不可能的，但是对于家用来说还是十分有必要的，因为没有任何人可以访问一种并不存在或打开服务。

**养成监视网络的习惯**

用户应当养成收集有关扫描和访问企图的日志，并利用现有的大量统计数字生成工具，以便于将这些日志变为更有用的信息。及时有效的查看是否有不明入侵者侵入，马上采取手段制止，使用最有效的加密手段，更改网络密码，避免造成更大损失。

**禁止 SSID 广播**

SSID 是无线接入的身份标识符，用户用它来建立与接入点之间的连接。你需要给你的每个无线接入点设置一个唯一并且难以推测的 SSID，或者干脆禁止广播 SSID，这样非连接用户，无法找到你的网络信息。

**仅在某些时段允许互联网访问**

如果你有规律的上网习惯，可以设定对互联网的访问限制在一天的某些时段。例如你是上班族，你一天 8 小时在公司，周末放假，你可以限制上网在早 8 点到晚 5 点，周末不限制，这样可以有效的防止盗取手段。

来源：中国计算机安全