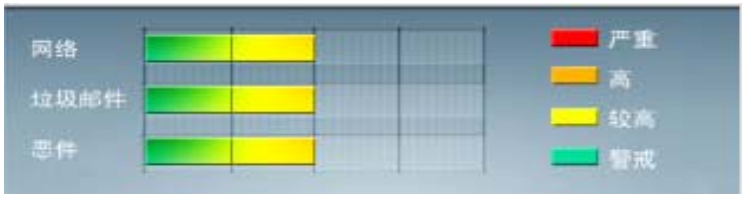
安全威胁每周警讯

2011/04/24～2011/04/30

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	WORM_ECODE.E-CN	蠕虫	★★★★	↑	E 语言病毒,产生与当前文件夹同名 exe 文件
6	TROJ_SPNR.03CG11	木马	★★	→	该木马程序是一个恶意软件，但危险低，不具备自动传播到其他系统的能力。它通常是从网上下载，并在用户不知情的情况下自动安装。 通常携带有效载荷木马或其他恶意行为，可从轻度恼人的范围到无可挽回的破坏。他们也可以修改系统设置为自动启动。
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	Dialer_Win32Dial	拨号软件	★★★	↓	这是个拨号器文件/组件。它尝试修改的 Internet Explorer（IE）的主页，直接影响用户浏览网站。
9	TROJ_SPNR.03CL11	木马	★★	↓	该木马程序是一个恶意软件，但危险低，不具备自动传播到其他系统的能力。它通常是从网上下载，并在用户不知情的情况下自动安装。
10	Gray_Gen	木马	★★	↑	灰色软件

系统漏洞信息

MS11-031：JScript 和 VBScript 脚本引擎中的漏洞可能允许远程执行代码

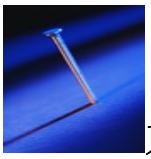
受影响的软件：

Windows XP ,Windows Server 2003

Windows Vista ,Windows Server 2008

Windows 7

描述：http://www.microsoft.com/china/technet/security/bulletin/MS11-031.mspx



系统安全技巧

技巧一：系统安全基础设置

黑客开始对你的网络发起攻击的时候，他们首先会检查是否存在一般的安全漏洞。因此，当你服务器上的数据都存在一个 FAT 的磁盘分区的时候，即使安装上世界上所有的安全软件也不会对你有多大帮助的。

因此，你需要从基本做起。将服务器上所有包含了敏感数据的磁盘分区都转换成 NTFS 格式的。同时，可以为 Exchange Server 安装反病毒软件，将被感染的邮件在到达用户以前隔离起来。

技巧二：保护你的备份

备份实际上是一个巨大的安全漏洞。应该考虑通过密码保护你的磁带，并且如果你的备份程序支持加密功能，你还可以加密这些数据，如果窃贼还是把磁带弹出来带走的话，磁带上的数据也就毫无价值了。

技巧三：使用 RAS 回叫功能

Windows NT 最酷的功能之一就是对服务器进行远程访问(RAS)的支持。不幸的是，一个 RAS 服务器对一个企图进入你的系统的黑客来说是一扇敞开的大门。黑客们所需要的一切只是一个电话号码。

你所要使用的技术将在很大程度上取决于你的远程用户如何使用 RAS。如果远程用户经常是从家里或是类似的不太变动的地方呼叫主机，建议你使用回叫功能，它允 许远程用户登录以后切断连接。然后 RAS 服务器拨通一个预先定义的电话号码再次接通用户。黑客也就没有机会设定服务器回叫的号码了。

另一个可选的办法是限定所有的远程用户都访问单一的服务器。这样，即使黑客通过破坏手段来进入主机，那么他们也会被隔离在单一的一台机器上。

最后还有一个技巧就是在你的 RAS 服务器上使用出人意料的协议，迷惑一些不加提防的黑客。

技巧四：考虑工作站的安全问题

工作站是通向服务器的一个端口，在所有的工作站上使用 Windows 2000。Windows 2000 是一个非常安全的操作系统。你也可以使用 Windows NT。锁定工作站，使得一些没有安全访问权的人想要获得网络配置信息变得困难或是不可能。

另，一个技术是将工作站的功能限定一个“聪明的”哑终端，让程序和数据驻留在服务器上但却在工作站上运行。所有安装在工作站上的是一份 Windows 拷贝以及 一些指向驻留在服务器上的应用程序的图标。当你点击一个图标运行程序时，这个程序将使用本地的资源来运行，而不是消耗服务器的资源。这比你运行一个完全的 哑终端程序对服务器造成的压力要小得多。

技巧五：使用流行的补丁程序

微软雇佣了一个程序员团队来检查安全漏洞并修 补它们。这些补丁被捆绑进一个大的软件包并做为服务包(service pack)发布。通常有两种不同的补丁程序版本:一个 40 位的版本和一个 128 位的版本。128 位的版本使用 128 位的加密算法，比 40 位的版本要安全得 多。微软定期将重要的补丁程序发布在它的 FTP 站点上。这些热点补丁程序是自上一次服务包发布以后被公布的安全修补程序。要经常查看热点补丁。但要记住一 定要按逻辑顺序使用这些补丁。避免导致一些文件的版本错误。

技巧六：使用强有力的安全政策

要提高安全性，另一个可以做的工作就是制定一个好的，强有力的安全策略。确保每一个人都知道它并知道它是强制执行的。如果你使用 Windows 2000 Server，你就有可能指定用户特殊的使用权限来使用你的服务器而不需要交出管理员的控制权，可以授予这种删除和禁用账号权限并限制创建用户或是更改许 可等这些活动的权限了。

技巧七：反复检查防火墙

防火墙是网络的一个重要部分，因为它将你公司的计算机同互联网上那些可能对它们造成损坏的蛊惑仔们隔离开来。

你首先要做的事情是确保防火墙不会向外界开放超过必要的任何 IP 地址。你总是至少要让一个 IP 地址对外界可见。这个 IP 地址被使用来进行所有的互联网通讯。如果你还有 DNS 注册的 Web 服务器或是电子邮件服务器，它们的 IP 地址也许也要通过防火墙对外界可见。但是，工作站和其他服务器的 IP 地址必须被隐藏起来。

你还可以查看端口列表验证你已经关闭了所有并不常用的端口地址。例如，TCP/IP 端口 80 用于 HTTP 通讯，因此你可能并不想堵掉这个端口。但是，你也许永远都不会用端口 81，因此它应该被关掉。你可以在 Internet 上找

到每个端口使用用途的列表。

来源： PConline

免责声明

该邮件列表仅用于提供信息，此邮件列表内容不负任何担保责任，没有明示或默示的保证，包括但不限于对适销性、特定用途适用性以及不受侵害的暗示保证。用户对此邮件列表的准确性和使用承担全部风险，因依赖该资料所致的任何损失，趋势科技均不负责。
