安全威胁每周警讯

2011/11/05～2011/11/12

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	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	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	JS_AGENT.MJM	Java 病毒	★★	↑	Java 病毒，通过 IE 浏览器安装插件的方式植入电脑中
9	WORM_VB.DVP	蠕虫	★★	↑	蠕虫病毒，通过访问恶意站点下载感染。感染该病毒后会在每个盘符下生成 autorun.inf 文件已达到用户在访问磁盘时执行该病毒
10	TROJ_KILLAV.SMEC	木马	★★★	↑	木马病毒，该病毒具有创建其他恶意病毒/灰色软件的功能，同时它具有按照特定的时间表自己执行的功能

系统漏洞信息

MS11-086：Active Directory 中的漏洞可能允许特权提升 (2630837)

Microsoft Windows XP

Microsoft Windows 2003

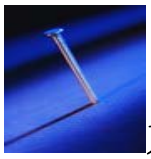
Windows Vista

Windows Server 2008

Windows 7

Windows Server 2008 R2

描述：http://technet.microsoft.com/zh-cn/security/bulletin/MS11-086



系统安全技巧

很多人认为，只要重新安装了操作系统，就可以彻底清除病毒。但却不知道在操作系统进行重新安装后，由于安全设置以及补丁未及时安装等问题，最容易导致病毒的大肆入侵，因此一些必备的补充措施是非常关键的。

病毒防护措施如下所述：

一、 不要急着接入网络

在安装完成 Windows 后，不要立即把服务器接入网络，因为这时的服务器还没有打上各种补丁，存在各种漏洞，非常容易感染病毒。此时要加上补丁后并重新启动再接入网络。

二、给系统打补丁/安装杀毒软件

安装 Windows 补丁。安装完系统后，一定要安装反病毒软件，同时将其更新到最新版本。

三、关闭系统还原

系统还原是 Windows XP、Windows 2003 以及后续版本中具有的功能，它允许我们将系统恢复到某一时间状态，从而可以避免我们重新安装操作系统。不过，有的人在执行系统还原后，发现除 C 盘外，其它的 D 盘、E 盘都恢复到先前的状态了，结果里面保存的文件都没有了，造成了严重的损失!

这是由于系统还原默认是针对硬盘上所有分区而言的，这样一旦进行了系统还原操作，那么所有分区的数据都会恢复。因此，我们必须按下 Win+Break 键，然后单击“系统还原”标签，取消“在所有驱动器上关闭系统还原”选项，然后选中 D 盘，单击“设置”按钮，在打开的窗口中选中“关闭这个驱动器上的系统还原”选项。

依次将其他的盘上的系统还原关闭即可。这样，一旦系统不稳定，可以利用系统还原工具还原 C 盘上的系统，但同时其他盘上的文件都不会有事。

四、给 Administrator 打上密码

可能有的人使用的是网上下载的万能 Ghost 版来安装的系统，也可能是使用的是 Windows XP 无人值守安装光盘安装的系统，利用这些方法安装时极有可能没有让你指定 Administrator 密码，或者 Administrator 的密码是默认的 123456 或干脆为空。这样的密码是相当危险的，因此，在安装完系统后，请右击“我的电脑”，选择“管理”，再选择左侧的“计算机管理(本地)→系统工具→本地用户和组→用户”，选中右侧窗口中的 Administrator，右击，选择“设置密码”。在打开窗口中单击“继续”按钮，即可在打开窗口中为 Administrator 设置密码。

另外，选择“新用户”，设置好用户名和密码，再双击新建用户，单击“隶属于”标签，将其中所有组(如果有)都选中，单击下方的“删除”按钮。再单击“添加”按钮，然后再在打开窗口中单击“高级”按钮，接着单击“立即查找”按钮，找到 PowerUser 或 User 组，单击“确定”两次，将此用户添加 PowerUser 或 User 组。注销当前用户，再以新用户登录可以发现系统快很多。

五、关闭默认共享

Windows 安装后，会创建一些隐藏共享，主要用于管理员远程登录时管理系统时使用，但对于个人用户来说，这个很少用到，也不是很安全。所以，我们有必要要切断这个共享：先在 d：下新建一个 disshare.bat 文件，在其中写上如下语句：

```
@echo off

net share C$/del

net share d$/del

net share ipc$/del

net share admin$ /del
```

接下来将 d：disshare.bat 拷贝到 C：WindowsSystem32GroupPolicyUserScriptsLogon 文件夹下。然后按下 Win+R，输入 gpedit.msc，在打开窗口中依次展开“用户配置→Windows 设置→脚本(登录/注销)”文件夹，在右侧窗格中双击“登录”项，在弹出的窗口中，单击“添加”命令，选中 C：WindowsSystem32GroupPolicyUserScriptsLogon 文件夹下的 disshare.bat 文件。

完成上述设置后，重新启动系统，就能自动切断 Windows XP 的默认共享通道了，如果你有更多硬盘，请在 net share d$/del 下自行添加，如 netshare e$/del、net share f$/del 等。

来源:51CTO