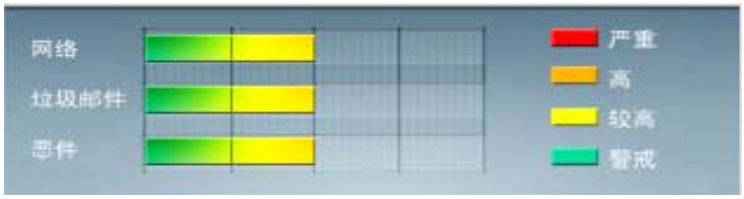
安全威胁每周警讯

2010/12/26～2011/01/01

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	Cryp_Xed-12	木马	★★★	↑	疑似病毒
5	TROJ_IFRAME.CP	木马病毒	★★★	↓	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
6	CRCK_KEYGEN	破解程序	★★	↑	非法破解程序
7	WORM_ECODE.E-CN	蠕虫	★★★★	↓	E 语言病毒,产生与当前文件夹同名 exe 文件
8	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
9	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
10	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

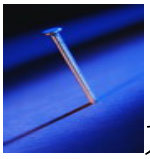
系统漏洞信息

MS10-093:Windows Movie Maker 中的漏洞可能允许远程执行代码 (2424434)

受影响的软件:

Windows Vista

描述: 请见http://www.microsoft.com/china/technet/security/bulletin/MS10-093.mspx



系统安全技巧

摘要: 引起后台打印服务启动不正常的主要原因，就是打印客户端系统遭遇到了病毒或木马的攻击。为了有效应对由网络病毒或木马攻击引起的共享打印失败故障，经过多次实践，总结了以下五项措施，来帮助大家快速、高效地恢复共享打印操作。

为了有效提高网络利用效率，并能降低办公成本，相信不少单位的网管员都会在局域网中，安装使用网 络打印机，以便在局域网中的任何位置处都能快速、方便地打印。可是，在平常的共享打印过程中，我们经常会与一些莫名其妙的打印故障不期而遇;仔细分析这些 共享打印故障，我们发现除了网络连接因素以及打印机自身因素外，还有一个更为常见的因素会造成共享打印操作失败，那就是系统的后台打印服务不能正常启动。 而引起后台打印服务启动不正常的主要原因，就是打印客户端系统遭遇到了病毒或木马的攻击。为了有效应对由网络病毒或木马攻击引起的共享打印失败故障，经过 多次实践，总结了以下五项措施，来帮助大家快速、高效地恢复共享打印操作!

一、查杀网络病毒

既然共享打印失败故障是由病毒、木马攻击引起的，那么首要的应对措施自然就是查杀打印客户端系统 中的病毒和木马了。由于现在的病毒和木马都相当的顽固，当打印客户端系统以正常模式启动运行时，病毒或木马程序往往会自动加载运行，此时再启动运行杀毒软 件，往往会查杀不彻底，甚至根本就无法进行杀毒。为此，我们必须重新启动打印客户端系统，在启动过程中，及时按下 F8 功能键，从弹出的启动菜单中选择“带 网络连接的安全模式”选项，将系统启动到安全模式状态;之后在这种模式状态下，我们可以使用瑞星杀毒软件 2011 版，并按照默认方法将该软件安装到打印客 户端系统中；接着启动运行该杀毒软件，对打印客户端系统执行全面扫描，经过一段时间的杀毒等待之后，相信潜藏在系统中的所有病毒或木马都会被清除干净。

当然，还有一些特殊的网络病毒或木马程序，会跟随硬盘启动而启动运行，对于这类顽固的病毒或木马 文件，我们即使进入安全模式也不能将它们清除干净，此时必须借助光盘版或优盘版的 Windows PE 系统，来启动打印客户端，之后在 Windows PE 系统状态下，对整个硬盘进行全面、彻底地病毒查杀操作，相信这么一来就能把网络病毒或木马程序彻底地消灭掉了。

二、暂停后台服务

在遭受过病毒或木马的攻击之后,系统的后台打印服务可能工作状态会受到影响,为此我们需要暂停该 系统的运行，

以便将该系统服务强行恢复到最原始的状态。在暂停后台打印服务时，我们可以直接用鼠标右键单击打印客户端系统桌面上的“我的电脑”图标，从弹 出的快捷菜单中点选“管理”命令，进入对应系统的计算机管理窗口；其次依次展开该管理窗口左侧列表区域中的“服务和应用程序”、“服务”选项，在对应“服 务”选项的右侧列表区域中，找到目标系统服务 Print Spooler，用鼠标双击该服务选项，打开如图 1 所示的选项设置对话框，单击“常规”标签页面中的“停止”按钮，打印客户端系统的后台打印服务就会被临 时暂停运行了。

三、删除残留信息

暂停后台打印服务之后，网络打印机基本就失效了，此时我们就需要将网络打印机卸载掉，并删除掉残 留在系统中的所有打印机信息，以免造成打印资源的冲突。卸载网络打印机设备很简单，只要依次单击打印客户端系统的“开始”、“设置”、“打印机”命令，在 弹出的打印机列表中，用鼠标右键单击目标网络打印机图标，从右键菜单中点选“删除”命令就可以了。

删除完网络打印机设备后，再依次单击“开始”、“运行”命令，在弹出的系统运行对话框中，输入注 册表编辑命令“regedit”，单击回车键后，进入打印客户端系统的注册表编辑对话框；将鼠标定位在 HKEY_LOCAL_MACHINE\SYSTEM \ControlSet001\Control\Print\Printers 注册表分支上面(如图 2 所示)，删除掉目标分支下面所有打印机的相关键值信 息。

之后，进入打印客户端系统的资源管理器窗口，依次展开“Windows”、“System32”、“Spool”、“Printers”文件夹窗口，将该窗口中所有 SHD 格式和 SPL 格式的文件全部选中，并执行“删除”命令，将它们彻底从系统中清除干净。

四、重启后台服务

在删除干净网络打印机的残留信息后，再重新启动一次打印客户端系统;待系统启动稳定后，依次单击 “开始”、“运行”命令，在弹出的系统运行对话框中，执行 “services.msc”字符串命令，弹出系统服务列表窗口，从中找到目标后台打印服务 Print Spooler，用鼠标双击该服务选项，再在对应选项设置框中的“常规”标签页面中，单击“启动”按钮，打印客户端系统的后台打印服务就会被重新启动运行 了，这时该服务的工作状态就能恢复正常了。

五、重装网络打印

完成上面的各项工作后，我们只要重新安装一遍网络打印机，就能彻底解决由病毒引起的共享打印失败 故障了。在重新安装网络打印机时，依次单击打印客户端系统的“开始”、“设置”、“打印机”命令，之后双击“添加打印机”图标，弹出添加打印机向导对话 框，选中“添加网络打印机”选项，单击“下一步”按钮，当弹出如图 3 所示的向导设置界面时，我们可以根据实际情况选择网络打印机;例如，要是网络打印机有 固定的 IP 地址时，我们必须选中“使用 TCP/IP 地址或主机名称添加打印机”选项，同时输入网络打印机的静态 IP 地址，就能顺利地完成网络打印机的安装 任务了;要是网络打印机是连接在某台主机上时，那么我们必须选中这里的“按名称选择共享打印机”选项，同时直接输入共享打印机的详细路径信息，这样才能保 证网络打印机安装成功。相信经过上面的几项措施处理后，网络打印操作又能正常进行了。

来源： IT 专家网

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。