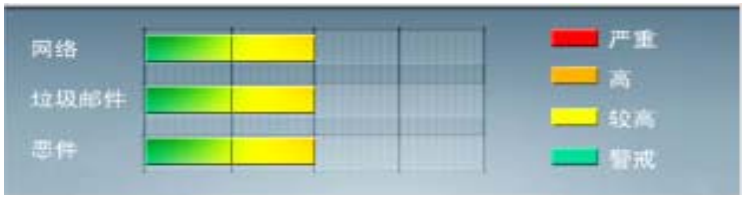
安全威胁每周警讯

2011/02/06～2011/02/12

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	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	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	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
9	ACM_AGENT.AVGL	木马	★★★	↑	AutoCad 脚本病毒
10	JS_ISTBAR.CN	脚本病毒	★★★	↑	Java 脚本病毒

系统漏洞信息

MS10-098:Windows 内核模式驱动程序中的漏洞可能允许特权提升 (2436673)

受影响的软件:

Windows 2003

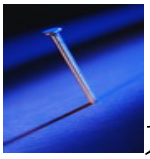
Windows xp

Windows Vista

Windows 2008

Windows 7

描述: 请见http://www.microsoft.com/china/technet/security/bulletin/MS10-098.mspx



系统安全技巧

摘要:下面将着重介绍一下 Windows 系统的 Svchost.exe 和 Explorer.exe 两种进程,作为 Windows 系统中两种重要的进程,下面我们就来看看他们的特点以及在各个操作系统中的应用。

下面将着重介绍一下 Windows 系统的 Svchost.exe 和 Explorer.exe 两种进程,作为 Windows 系统中两种重要的进程,下面我们就来看看他们的特点以及在各个操作系统中的应用。

Explorer.exe

在 Windows 系列的操作系统中,运行时都会启动一个名为 Explorer.exe 的进程。这个进程主要负责显示系统桌面上的图标以及任务栏,它在不同的系统中有不同的妙用。

Explorer 在 Windows 9x 中的应用

在 Windows 9x 中,这个进程是运行系统时所必需的。如果用"结束任务"的方法来结束 Explorer.exe 进程,系统就会刷新桌面,并更新注册表。所以,我们也可以利用此方法来快速更新注册表。方法如下:

按下 Ctrl+Alt+Del 组合键,出现"结束任务"对话框。在该对话框中选择 "Explorer"选项,然后单击"结束任务"按钮,将出现"关闭 Windows"对话框。单击"否"按钮,系统过一会儿将出现另一个对话框,告诉你该程序没有响应,询问是否结束任务。单击"结束任务"按钮,则更新注册 表并返回 Windows 9x 系统环境中。这比起烦琐的重新启动过程要方便多了?

Explorer 在 Windows 2000/XP 中的应用

在 Windows 2000/XP 和其他 Windows NT 内核的系统中,Explorer.exe 进程并不是系统运行时所必需的,所以可以用任务管理器来结束它,并不影响系统的正常工作。打开你需要运行的程 序,如记事本。然后右击任务栏,选择

“任务管理器”，选中“进程”选项卡，在窗口中选择 Explorer.exe 进程，单击“结束进程”按钮，，接下来桌 面上除了壁纸(活动桌面 Active Desktop 的壁纸除外)，所有图标和任务栏都消失了。此时你仍可以像平常一样操作一切软件。

如果你想运行其他软件，但此时桌面上空无一物，怎么办?别着急，下面有两种可以巧妙地打开其他软件：

第一种方法：按下 Ctrl+Alt+Del 组合键，出现“Windows 安全”对话框，单击“任 务管理器”按钮(或是直接按下 Ctrl+Shift+Esc 组合键)，在任务管理器窗口中选中“应用程序”选项卡，单击“新任务”，在弹出的“创建新任务”的对话框中，输入你想要打开的软件的路径和名称即可。

你还可以在正在运行的软件上，选择“文件→打开”，在“打开”对话框中，点击“文件类型”下拉列 表，选择“所有文件”，再浏览到你想打开的软件，右击它，在快捷菜单中选择“打开”命令，就可以启动你需要的软件了。注意，此时不能够通过单击“打开”按 钮来打开软件，此种方法适用于大多数软件，Office 系列除外。

通过结束 Explorer.exe 进程，还可以减少 4520KB 左右的系统已使用内存，无疑会加快系统的运行速度，为资源紧张的用户腾出了宝贵的空间。

Svchost.exe

Svchost.exe 是 NT 核心系统的非常重要的进程，对于 2000、XP 来说，不可或缺。很多病毒、木马也会调用它。所以，深入了解这个程序，是玩电脑的必修课之一。

大家对 Windows 操作系统一定不陌生，但你是否注意到系统中“Svchost.exe”这个 文件呢?细心的朋友会发现 Windows 中存在多个 “Svchost”进程(通过“ctrl+alt+del”键打开任务管理器，这里的“进程”标签中就可看到了)，为什么会这样呢?下面就来揭开它神秘的 面纱。

在基于 NT 内核的 Windows 操作系统家族中，不同版本的 Windows 系统，存在不同数量的 “Svchost”进程，用户使用 “任务管理器”可查看其进程数目。一般来说，Win 2000 有两个 Svchost 进程，Win XP 中则有四个或四个以上的 Svchost 进程(以后看到系统中有多个这种进程，千万别立即判定系统有病毒了哟)，而 Win 2003 server 中则更多。这些 Svchost 进程提供很多系统服务，如：rpcss 服务(remote procedure call)、dmserver 服务(logical disk manager)、dhcp 服务(dhcp clieNT)等。

如果要了解每个 Svchost 进程到底提供了多少系统服务，可以在 Win 2000 的命令提示符窗口中输入“tlist -s”命令来查看，该命令是 Win 2000 support tools 提供的。在 Win XP 则使用“tasklist /svc”命令。

Svchost 中可以包含多个服务

Windows 系统进程分为独立进程和共享进程两种，“Svchost.exe”文件存在于“%systemroot% system32”目录下，它属于共享进程。随着 Windows 系统服务不断增多，为了节省系统资源，微软把很多服务做成共享方式，交由 Svchost.exe 进程来启动。

但 Svchost 进程只作为服务宿主，并不能实现任何服务功能，即它只能提供条件让其他服务在这里被启动，而它自己却不能给用户提供任何服务。那这些服务是如何实现的呢?

原来这些系统服务是以动态链接库(dll)形式实现的，它们把可执行程序指向 Svchost，由 Svchost 调用相应服务的动态链接库来启动服务。那 Svchost 又怎么知道某个系统服务该调用哪个动态链接库呢?这是通过系统服务在注册

表中设置的参数来实现。

服务是靠 Svchost 来启动的

因为 Svchost 进程启动各种服务，所以病毒、木马也想尽办法来利用它，企图利用它的特性来迷惑用户，达到感染、入侵、破坏的目的。但 Windows 系统存在多个 Svchost 进程是很正常的，在受感染的机器中到底哪个是病毒进程呢?这里仅举一例来说明。

假设 Windows XP 系统被病毒感染了。正常的 Svchost 文件存在于“c:\Windows\system32”目录下，如果发现该文件出现在其他目录下就要小心了。 病毒存在于“c:\Windows\system32\Wins”目录中，因此使用进程管理器查看 Svchost 进程的执行文件路径就很容易发现系统是否 感染了病毒。

Windows 系统自带的任务管理器不能够查看进程的路径，可以使用第三方进程管理软件，通过这些工具就可很容易地查看到所有的 Svchost 进程的执行文件路径，一旦发现其执行路径为不平常的位置就应该马上进行检测和处理。

来源： eNet

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。
