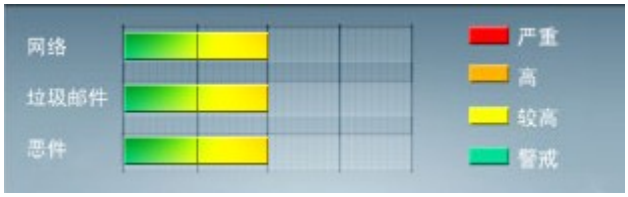
安全威胁每周警讯

2010/04/04～2010/04/10

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	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。
2	TROJ_DOWNAD.INF	木马	★★★	→	DOWNAD 蠕虫关联木马
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	蠕虫病毒	★★★	↓	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	木马病毒	★★★	↓	疑似病毒
6	WORM_ECODE.E-CN	蠕虫病毒	★★★★	→	E 语言病毒,产生与当前文件夹同名 exe 文件
7	GRAY_Gen	灰色软件	★★★	→	智能检测技术检测出的灰色程序,需要收集样本后进一步分析
8	JS_REDIR.SME	脚本病毒	★★	↑	脚本病毒
9	CRCK_KEYGEN	破解程序	★★★	↓	非法破解程序
10	ADW_WEBTHUNDER	广告程序	★	↑	广告程序

系统漏洞信息

Microsoft 安全公告 MS10-016 -
重要 Windows Movie Maker 中的漏洞可能允许远程执行代码 (975561)
受影响的系统:

Windows 7Windows XP Service Pack 2 和 Windows XP Service Pack 3
Windows XP Professional x64 Edition Service Pack 2
Windows Vista、Windows Vista Service Pack 1
Windows Vista Service Pack 2
Windows Vista x64 Edition、Windows Vista x64 Edition Service Pack 1
Windows Vista x64 Edition Service Pack 2
Windows 7（用于 32 位系统）
Windows 7（用于基于 x64 的系统）
Microsoft Producer 2003[3]

描述: 请见http://www.microsoft.com/china/technet/security/bulletin/MS10-016.mspx

Microsoft 安全公告 MS10-017 - 重要
Microsoft Office Excel 中的漏洞可能允许远程执行代码 (980150)
受影响的系统:
Microsoft Office XP Service Pack 3
-- Microsoft Office Excel 2002 Service Pack 3
Microsoft Office 2003 Service Pack 3
-- Microsoft Office Excel 2003 Service Pack 3
2007 Microsoft Office System Service Pack 1
-- Microsoft Office Excel 2007 Service Pack 1[1]
2007 Microsoft Office System Service Pack 2
-- Microsoft Office Excel 2007 Service Pack 2[1]
Microsoft Office 2004 for Mac
Microsoft Office 2008 for Mac
Open XML File Format Converter for Mac
Microsoft Office Excel Viewer Service Pack 1
Microsoft Office Excel Viewer Service Pack 2
用于 Word、Excel PowerPoint 2007 文件格式的 Microsoft Office 兼容包 Service Pack 1
用于 Word、Excel PowerPoint 2007 文件格式 的 Microsoft Office 兼容包 Service Pack 2
Microsoft Office SharePoint Server 2007 Service Pack 1（32 位版本）[2]
Microsoft Office SharePoint Server 2007 Service Pack 2（32 位版本）[2]
Microsoft Office SharePoint Server 2007 Service Pack 1（64 位版本）[2]
Microsoft Office SharePoint Server 2007 Service Pack 2（64 位版本）[2]

描述: 请见http://www.microsoft.com/china/technet/security/bulletin/MS10-017.mspx

系统安全技巧

摘要：大家对病毒都是痛疾若杀，但有时也是无奈，只能靠杀毒软件和防火墙进行简单防护。今天给大家分享的是让病毒一剑穿心的几个方法。
大家对病毒都是痛疾若杀，但有时也是无奈，只能靠杀毒软件和防火墙进行简单防护。今天给大家分享的是让病毒一剑穿心的几个方法。

一、新安装的纯系统

必须是全盘格式化，进行安装的系统，而且是纯净的，不能有点杂草，如果是微软自己种的，那没有办法。

操作“开始→程序→管理工具→计算机管理→本地用户和组→用户”

首先就是把超级管理员密码更改成十位数以上，而且是小写字母，大写字母，数字，特殊符号相混合的。然后再建立一个用户，把它的密码也设置成十位以上并且提升为超级管理员。这样做的目的是为了双保险：如果你忘记了其中一个密码，还有使用另一个超管密码登陆来挽回的余地，免得你被拒绝于系统之外;再者就是网上的黑客无法再通过猜测你系统超管密码的方式远程获得你系统的控制权而进行破坏。接着再添加两个用户，比如用户名分别为：dayua1、dayua2;并且指定他们属于 user 组，好了，准备工作到这里就全部完成了，以后你除了必要的维护计算机外就不要使用超级管理员和 dayua2 登陆了。只使用 dayua1 登陆就可以了。

登陆之后上网的时候找到 IE，并为它建立一个快捷方式到桌面上，右键单击快捷方式，选择“以其他用户方式运行”点确定!要上网的时候就点这个快捷方式，它会跟你要用户名和密码这时候你就输入 dayua2 的用户名和密码!!!好了，现在你可以使用这个打开的窗口去上网了，可以随你便去放心的浏览任何恶毒的、恶意的、网站跟网页，而不必再担心中招了!因为你当前的系统活动的用户时 dayua1。而 dayua2 是不活动的用户，我们使用这个不活动的用户去上网时，无论多聪明的网站，通过 IE 得到的信息都将让它都将以为这个 dayua2 就是你当前活动的用户，如果它要在你浏览时用恶意代码对你的系统搞搞破坏的话根本就时行不通的，即使能行通，那么被修改掉的仅仅时 dayua2 的一个配置文件罢了，而很多恶意代码和病毒试图通过 dayua2 进行的破坏活动却都将失败，因为 dayua2 根本就没运行，怎么能取得系统的操作权呢??既然取不得，也就对你无可奈何了。而他们更不可能跨越用户来操作，因为微软得配置本来就是各各用户之间是独立的，就象别人不可能跑到我家占据我睡觉用的床一样，它们无法占据 dayua1 的位置!所以你只要能保证总是以这个 dayua2 用户做代理来上网(但却不要使用 dayua2 来登陆系统，因为如果那样的话，如果 dayua2 以前中过什么网页病毒，那么在 dayua2 登陆的同时，他们极有可能被激活!)，那么无论你中多少网页病毒，全部都将是无法运行或被你当前的 dayua1 用户加载的，所以你当前的系统将永远无毒!

二、对于已经中标的机器

重新启动计算机，使用超级管理员登陆－－进入系统后什么程序都不要运行

你会惊奇的发现在的系统竟然表现的完全无毒!!，那就再好不过了，现在就立即就打开：

“开始→程序→管理工具→计算机管理→本地用户和组→用户” 吧!

把里面的 dayua1 和 dayua2 两个用户权删掉吧，你只需要这么轻轻的一删就可以了，那么以前随着这两个用户而存在的病毒也就跟随着这两个用户的消失而一起去长眠了。这么做过之后我保证你的 win2k 就象新装的一个样，任何系统文件和系统进程里都完全是没有病毒的!

现在再重复开始的步骤从新建立 dayua1 和 dayua2 两个用户，让他们复活吧。他们复活是复活了，但是曾跟随了他们的病毒却是没这机会了，因为 win2k 重新建立用户的时候会重新分配给他们全新的配置，而这个配置是全新的也是不可能包含病毒的!!!建立完成之后立即注销超级管理员，转如使用 dayua1 登陆，继续你想做的事吧，你会发现你的系统如同全新了!以上方法可以周而复始的用。

来源：赛迪网