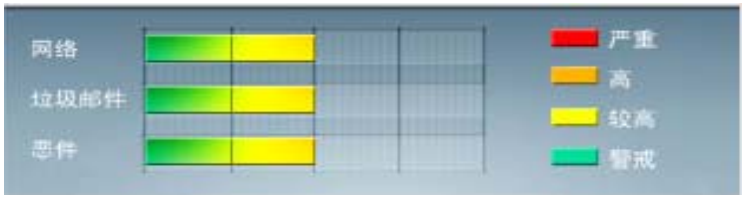
安全威胁每周警讯

2010/11/20～2010/11/27

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
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	WORM_AUTORUN.IJB	蠕虫	★★★★	↑	该病毒会将自己复制到移动存储中，并且创建一个 autorun.inf 文件，使得移动设备在每次启动时运行该病毒
7	CRCK_KEYGEN	破解程序	★★	↑	非法破解程序
8	WORM_ECODE.E-CN	蠕虫	★★★★	↓	E 语言病毒,产生与当前文件夹同名 exe 文件
9	HTML_IFRAME.AZ	网页病毒	★★	↑	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
10	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

系统漏洞信息

MS10-087:Microsoft Office 中的漏洞可能允许远程执行代码 (2423930)

受影响的软件：

Microsoft Office 2003

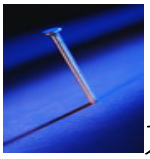
Microsoft Office 2007

Microsoft Office 2010

Microsoft Office 2004 for mac

Microsoft Office 2008 for mac

描述：请见 http://www.microsoft.com/china/technet/security/bulletin/MS10-087.mspx



系统安全技巧

摘要：恶意软件已经成为网络安全的重要问题之一了。那么对于恶意软件监测方法你知道多少呢？如果你曾经遇到过系统被恶意软件感染的情况，下面给出的几种方法可以让你在系统刚被恶意软件感染的情况就能迅速察觉，从而可以立即处理以降低带来的危害。

恶意软件已经成为网络安全的重要问题之一了。那么对于恶意软件监测方法你知道多少呢？如果你曾经 遇到过系统被恶意软件感染的情况，就一定它知道造成的麻烦有多大，尽快对计算机进行清理，可以防止恶意软件造成更大的危害或感染其它机器。下面给出的几种 方法可以让你在系统刚被恶意软件感染的情况就能迅速察觉，从而可以立即处理以降低带来的危害。

1. 经常使用工具软件对系统进行检测

显然，这是最明确的做法。现在市面上有许多优秀的防恶意软件工具可供选择，你可以从中找到自己喜 欢的。此外，你可能会遇到选择的防恶意软件工具没有配备实时扫描工具的情况。因此，你需要保证最终用户经常进行手动扫描，以发觉感染的蛛丝马迹。如果客户 端不及时进行扫描的话，不仅会导致恶意软件带来更多问题，而且有可能导致感染更多的恶意软件。

2. 系统性能出现下降的趋势

恶意软件臭名昭著的原因就是它会导致系统性能下降，无论是网络连接还是应用运行的速度都不例外。 当然，仅仅出现系统性能下降的情况并不意味着受到恶意软件的感染。由于很多其它问题都可能导致系统性能下降，因此，我建议首先采取措施来处理系统性能下降 的问题（通常的措施有进行磁盘碎片整理、增加内存等等）。如果在采取了必要措施后，系统性能依然没有提高，这就有可能是恶意软件带来的了。

3. 关注弹出窗口的情况

被恶意软件感染的一个潜在迹象是出现令人尴尬的弹出窗口。有时候用户的电脑会弹出色情窗口，它让 用户既尴尬又愤怒。意料之外的弹出窗口（尤其是那些没有启动网络浏览器就出现的）是系统已经被恶意软件感染的一种迹象。关键的问题是，这时候，恶意软件往 往已经不能在标准模式下删除了；而是你必须重新启动系统，转换到安全模式。为了对恶意软件的所有部分进行清理，你需要一个功能强大的防恶意软件工具来将其 删除。

4. 主页连接被更改

如果你没有进行调整却发现浏览器默认首页发生变化的话，非常大的可能是系统被恶意软件感染了。同样，在你利用百度搜索时，点击百度提供的连接，却被引导到一个随机连接上。这类的情况，都表明系统被病毒或恶意软件所感染。

5. 浏览器无法上网

在网络连接正常（利用 ping 命令可以很方便地确认这一点）的时间，却出现不能访问互联网的情 况，造成这一问题的很大可能就是系统被恶意软件感染。这时间，我们要做的就是对设置进行仔细检查，进入浏览器的网络连接项目，确保没有设置代理服务器。如 果是这样，并且你知道自己没有使用代理服务器的话，就说明系统被恶意软件感染了。

来源 51CTO