安全威胁每周警讯

2011/10/23～2011/10/29

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	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
3	TROJ_DOWNAD.INF	木马	★★★	→	DOWNAD 蠕虫关联木马
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	Cryp_Xed-12	木马	★★	→	木马病毒，通过访问恶意站点下载感染或由其他恶意程序下载感染
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	PAK_Generic.001	木马	★★★	↑	疑似病毒
8	CRCK_KEYGEN	木马	★★	→	非法破解程序
9	ACM_AGENT.AVGL	脚本病毒	★★	↑	AutoCad 脚本病毒
10	TROJ_SPNR.03CG11	木马	★	→	通过可执行文件传播的木马病毒

系统漏洞信息

MS11-078：.NET Framework 和 Microsoft Silverlight 中的漏洞可能允许远程执行代码(2604930)**:**

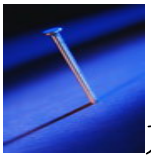
Microsoft Windows XP

Microsoft Server 2003

Microsoft Server 2008

Microsoft Server 2008 R2

描述：http://technet.microsoft.com/zh-cn/security/bulletin/MS11-078



系统安全技巧

究竟何为网页病毒？

网页病毒是利用网页来进行破坏的病毒，它使用一些 SCRIPT 语言编写的一些恶意代码利用 IE 的漏洞来实现病毒植入。当用户登录某些含有网页病毒的网站时，网页病毒便被悄悄激活，这些病毒一旦激活，可以利用系统的一些资源进行破坏。轻则修改用户的注册表，使用户的首页、浏览器标题改变，重则可以关闭系统的很多功能，装上木马，染上病毒，使用户无法正常使用计算机系统，严重者则可以将用户的系统进行格式化。而这种网页病毒容易编写和修改，使用户防不胜防。现在上网的人几乎都有自己的 QQ 号，并且现在网页病毒很多都通过 QQ 来进行传播，所以当你的 QQ 好友给你发过来的是一段网址的时候，你一打开。在不知情的情况下，你的电脑就中毒了，你的电脑若是没有网络安全服务防护就会遭受不同程度的损害。那么我们就从以下几方面加强自己电脑的网络安全防护，这样我们就能让网页病毒对我们的电脑无从下手了。

管理好 Cookie

在 IE6.0 中，打开“工具”→“Internet 选项”→“隐私”对话框，这里设定了“阻止所有 Cookie”、“高”、“中高”、“中”、“低”、“接受所有 Cookie”六个级别(默认为“中”)，你只要拖动滑块就可以方便地进行设定，而点击下方的“编辑”按钮，在“网站地址”中输入特定的网址，就可以将其设定为允许或拒绝它们使用 Cookie。

禁用或限制使用 Java 程序及 ActiveX 控件

在网页中经常使用 Java、Java Applet、ActiveX 编写的脚本，它们可能会获取你的用户标识、IP 地址，乃至口令，甚至会在你的机器上安装某些程序或进行其他操作，因此应对 Java、Java 小程序脚本、ActiveX 控件和插件的使用进行限制。打开“Internet 选项”→“安全”→“自定义级别”，就可以设置“ActiveX 控件和插件”、“Java”、“脚本”、“下载”、“用户验证”以及其它安全选项。对于一些不太安全的控件或插件以及下载操作，应该予以禁止、限制，至少要进行提示。

防止泄露自己的信息

缺省条件下，用户在第一次使用 Web 地址、表单、表单的用户名和密码后，同意保存密码，在下一次再进入同样的 Web 页及输入密码时，只需输入开头部分，后面的就会自动完成，给用户带来了方便，但同时也留下了安全隐患，不过我们可以通过调整“自动完成”功能的设置来解决。设置方法如下:依次点击“Internet 选项”→“内容”→“自动完成”，打开“自动完成设置”对话框，选中要使用的“自动完成”复选项。

提醒:为发安全起见，防止泄露自己的一些信息，应该定期清除历史记录，方法是在“自动完成设置”对话框中点击“清除表单”和“清除密码”按钮。

清除已浏览过的网址

在“Internet 选项”对话框中的“常规”标签下单击历史记录区域的“清除历史记录”按钮即可。若只想清除部分记录，单击 IE 工具栏上的“历史”按钮，在左栏的地址历史记录中，找到希望清除的地址或其下网页，单击鼠标右键，从弹出的快捷菜单中选取“删除”。

清除已访问过的网页

为了加快浏览速度，IE 会自动把你浏览过的网页保存在缓存文件夹“C:\Windows\Temporary Internet Files”下。当你确认不再需要浏览过的网页时，在此选中所有网页，删除即可。或者在“Internet 选项”的“常规”标签下单击“Internet 临时文件”项目中的“删除文件”按钮，在打开的“删除文件”对话框中选中“删除所有脱机内容”，单击“确定”，这种方法会遗留少许 Cookie 在文件夹内，为此 IE6.0 在“删除文件”按钮旁边增加了一个“删除 Cookie”的按钮，通过它可以很方便地删除遗留的

永远不怕 IE 主页地址被修改

众所周知，修改 IE 默认主页地址是恶意网页常用的一招。IE 被修改后，会自动连接到恶意网页的地址。大家常用的方法是修改注册表，其实，只要简单给 IE 加个参数，就再也不怕 IE 主页地址被修改了。下面是具体的方法和步骤。

首先，打开“我的电脑”，找到 IE 的安装目录，这里假设你的 IE 安装在 C:\Program Files\Internet Explorer 下。进入该文件夹，找到 Iexplore.exe 文件，对着它点击鼠标右键，在弹出的快捷菜单中选择“发送到→桌面快捷方式”，这样就在桌面上建立了一个 Iexplore.exe 文件的快捷方式。如果你够仔细的话，你会发现你建立的这个快捷方式名字为“Iexplore.exe”，而桌面上原来的 IE 快捷方式名字为“Internet Explorer”，两者不仅名字不相同，而且“内涵”也不尽相同。

继续我们的工作，用鼠标右键单击该快捷方式，选择“属性”，会弹出“Iexplore.exe 属性”对话框，选择其中的“快捷方式”标签，然后在“目标”框里填入:"C:\Program Files\Internet Explorer\IEXPLORE.EXE" -nohome，给 Iexplore.exe 加上参数“-nohome”，输入时请大家注意在参数“-nohome”前面有一个空格，不要忘了，输入完毕。点击“确定”退出即可。

这样即使主页被修改也没有关系，打开 IE 就是一片空白，就连 about:blank 也不显示。而且这样能够加快启动速度，一点 IE 窗口马上就出蹦来了。

对于 IE 在安装时自己建立的快捷方式，我们无法为它加上上述参数。如果不信可以试试，用鼠标右键点击桌面上原来 IE 自建的快捷方式，选“属性”，会发现“目标”栏、“起始位置”栏、“快捷键”栏和“运行方式”栏都是灰色不可选取状态。这就是它们之间最大的不同!也是本文的关键所在。

网页病毒随着互联网的发展也在逐步扩大，网民的数量在不断的增多，所以，也许在你不经意间，病毒的黑手就已经伸向了你，请读者提高自己的防范意识。

来源:51CTO