安全威胁每周警讯

2012/06/03～2012/06/09

本周威胁指数

***TrendMicro* 中国区网络安全监控中心**

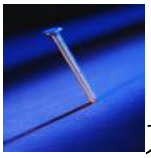
前十大病毒警讯

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	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	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	疑似病毒	★★★	→	疑似木马病毒，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	CRCK_KEYGEN	黑客程序	★★	↑	非法破解程序
7	X97M_LAROUX.BK	宏病毒	★★	↓	宏病毒，主要通过用户浏览恶意网站感染，该病毒主要感染 Office Excel 文件，并且会在 Excel 中创建一个名为 StartUp 的宏脚本
8	X97M_LAROUX.CO	宏病毒	★★	↑	宏病毒，主要通过用户浏览恶意网站感染，该病毒主要感染 Office Excel 文件，并且会在 Excel 中创建一个名为 StartUp 的宏脚本
9	PAK_Generic.001	加壳文件	★★	→	经过加壳技术加密的文件
10	WORM_ECODE.E-CN	蠕虫	★★	↑	它通过将受感染的移动驱动器与系统连接起来而入侵。 它可能是由远程站点的其他恶意软件/灰色软件/间谍软件下载而来。 它可能是用户在访问恶意网站时在无意中下载而来。

系统漏洞信息

MS12-024 ： Windows 中的漏洞可能允许远程执行代码 (2653956)

Windows XP
Windows Vista
Windows 7
Windows Server 2003
Windows Server 2008
Windows Server 2008 R2
描述：http://technet.microsoft.com/zh-cn/security/bulletin/MS12-024



系统安全技巧

“新三年，旧三年，缝缝补补又三年”，这是在那个艰苦的年代中，多少年也没有经济能力添置一件新衣服而留给我们的苦涩记忆，谁也不会因为衣服上打了补丁而被人笑话，因为大家都这样。如今生活水平提高了，有了自己的汽车，有了自己的电脑，下馆子吃饭都得吃腻了，衣服上要是打了个补丁，那得说成是时尚，人们对待生活的观念已经发生了翻天覆地的变化。而今天我们所要探讨的不是经济和生活问题，而是 Window 系统里的“补丁”，但仔细想想，其实也是与我们的生活和经济紧紧相关，因为如果没有了这些“补丁”，系统一旦受到侵害和攻击，就将造成我们的经济损失以至影响到我们的生活。究竟这是为什么?本文我们就来说说 Windows 系统里的“补丁”。

“系统有漏洞，需要打补丁!”这是我们在使用 Windows 系统时经常听到的一句话，那么系统为什么会有漏洞，为什么要打补丁呢?这些补丁的作用又是什么呢?这就好比是我们新建筑的大楼，有各种钢板、水泥、门窗、电器、水暖等等组成，房子虽然建设好了，也住进去了，但是门窗是否安全?供电供暖是否正常?安保设施是否到位?在之后的管理中，我们可能还是得对房屋的各方面进行装修改进，以使得我们未来的生活更加安全舒适。

那就容易理解了，首先操作系统是由一个庞大的代码数据组成的“房屋”，尽管发布时已经是正式版，但是通过众多用户的使用，以及一些“不良分子(黑客)”的破解和攻击，那么我们的系统还是存在一些问题的，有些是严重的，有些是一般性的。这个时候，我们就得针对这些“漏洞”进行打补丁。

再来说说，这些补丁的作用是什么?在系统里，我们都知道系统更新是通过“Windows Update”，也就是说，微软公司就是通过这个 Update 去给我们的操作系统进行“沟通”的。她通常提供了漏洞、驱动、软件的升级。通过她的更新能够扩展系统的功能，让系统支持更多的软、硬件，解决各种兼容性问题，让系统更安全、更稳定。顺便说一句，这些更新是针对全球正版 Windows 用户的，你的系统与世界所有的正版用户是保持一致的!

操作系统中比较大的而且重要的升级补丁就是 Service Pack (SP)，Service Pack 直译是“服务包”，一般说法是补丁，用途是修补系统、大型软件中的安全漏洞。比如 Windows 7 Service Pack 1 (SP1)，就是重要更新，这里面包括以前针对 Windows 7 发行的安全更新、性能更新和稳定性更新。SP1 还包括针对 Windows 7 中功能和服务的新改进，如提高了连接到 HDMI 音频设备时、使用 XPS 查看器打印时以及在重新启动后还原 Windows 资源管理器中以前的文件夹时的可靠性。

要想获得这些更新，必须确保你的 Windows Update 是打开状态，通过控制面板——Windows Update 里的“更改设置”，在重要更新里选择自动安装更新，在这里我们也可以指定一个下载更新的时间，从而不至于影响到我们的工作。如果您打开了“自动更新”功能，Windows Update 就可在第一时间通知高优先级更新到您的计算机。

另外，假如你已经很久没有对系统进行更新升级了，那么你可以通过 Win7 的开始菜单——Windows Update 进行检查，在安装一些重要更新，比如 SP 时，可能会对计算机重启，要确保你的数据备份好，并且关闭正在使用的程序。

我们了解了一些系统补丁和升级的知识，大致知道了打补丁的重要性，所以，在系统的使用中，我们要养成良好的习惯。这里主要是指第一，要选择正版的操作系统，只有正版的操作系统才能在第一时间享受到更多的重要更新和升级;第二，拒绝使用破解的盗版系统，这是因为，盗版的系统修改了系统的文件，并且大部分是默认关闭了系统的自动更新，有可能会在破解补丁里安装了木马程序，对你的财产和个人隐私造成损失;第三，你也可以通过第三方软件进行安装系统的更新。

有了这些保障，你的系统将始终保持最新，并且在安全性上，以及通过升级实现的更为强大的功能组件和良好的兼容性，和在操作上的更好体验，都将进一步提升。所以，你准备了吗?现在就 Update 一下吧，让你的系统始终保持健康的状态!

转自 51CTO