安全威胁每周警讯

2011/06/26～2011/07/02

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

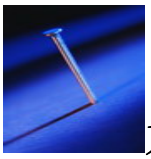
排名	病毒名称	威胁类型	风险等级	趋势	病毒行为描述
1	WORM_DOWNAD.AD	蠕虫	★★★★	↑	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
2	TROJ_DOWNAD.INF	木马	★★★	↓	DOWNAD 蠕虫关联木马
3	TROJ_IFRAME.CP	木马	★★★	↑	GIF、jpg 和 SWF 文件中被插入一个恶意的 iframe 标记时，趋势科技会将其判断为 TROJ_IFRAME.CP 病毒。当这些文件被执行时，会重定向到这些 URL，并下载恶意程序
4	WORM_DOWNAD	蠕虫	★★★★	↓	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	★★	→	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	HTML_IFRAME.AZ	网页病毒	★★	→	网页病毒,通常在网页在插入一个恶意 iframe,用户在访问该网页时会下载恶意文件或重定向到恶意网站
8	PAK_Generic.001	木马	★★★	→	疑似病毒
9	CRCK_KEYGEN	网页病毒	★★	→	非法破解程序
10	Expl_ShellCodeSM	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

系统漏洞信息

MS11-048：SMB 服务器中的漏洞可能允许拒绝服务

受影响的软件：
Windows Vista
Windows Server 2008
Windows 7

描述：http://www.microsoft.com/china/technet/security/bulletin/MS11-048.mspx



系统安全技巧

无线安全你该掌握的六个拿手绝活是本文所要讲述的内容，Linksys、TP-LINK、D-Link、NETGEAR、SMC 等厂商，均有多款 802.11a/b/g 标准的无线产品，甚至出现了同时兼容三种标准的双频三模无线产品，这预示着双频三模成为无线网络产品发展的一个新方向。

以无线路由器、AP 及无线网卡为代表的无线网络产品，已经逐渐打破家庭和中小企业市场中 Hub 以及普通路由器“一统天下”的局面，成为构建 SOHO 和中小型网络的首选。市场需求巨大、价格的敏感、同类产品竞争的激烈，都要求无线产品生产厂商必须想尽一切办法压低成本，而一些中小企业为了降低成本更是“饥不择食”。同时，随着无线产品显示的巨大商机，一些假冒伪劣产品也不断在市场中出现。(一些质量低下的无线产品，其外表虽然光鲜，但打开机箱就会发现其中的猫腻，例如使用的是二手主板、元器件是杂牌、内部结构设计凌乱复杂、布线杂乱等。)

六大问题困扰消费者

从目前无线产品使用者反馈的情况看，无线产品的死机、无线信号有效距离短、无线连接频频断线、兼容性差、抗干扰性差。

1. 死机

恐怕现在无线产品消费者反映最强烈的问题就是无线产品突然停止工作、死机。特别是在新手第一次使用无线路由器的时候，这个问题更常见，一般的原因就是配置出现问题，在反复选择恰当的选项后一般都能解决。但有的

用户反映，无线产品总是隔三差五出现死机，而无线产品的售后服务人员也没有什么好办法来解决，无非是再三告诉用户将软件版本升级到最新，或者干脆说硬件设计存在问题。

2. 有效距离短

这个问题已经见怪不怪了，一般无线产品的实际有效距离能够达到其宣称的最大距离的 1/3～1/2 就算不错了。这个问题的出现有诸多方面的因素，例如无线天线的有效性、无线产品的位置、无线产品间的障碍物、无线产品的散热效果等，这些都会成为无线产品厂家推脱其产品质量的借口。在这种情况下，要达到增加传输距离的目的，可以采取重新选择合理的位置布放无线天线、为无线产品增加增益天线等方式。如果感兴趣，还可以自己动手做一个简单的增益天线，说不定增益效果能让你十分满意。

3. 频频断线

很多朋友在使用无线产品的时候，经常会发现无线信号忽强忽弱、忽断忽续，除了环境影响和电磁波的干扰因素外，主要是由无线产品本身的稳定性和质量原因造成的。比如在使用无线路由器时，虽然网络连接仍然“健在”，但是已经无法访问到互联网，而重新启动路由器后，就可以恢复正常，这种情况就是典型的无线产品的不稳定造成的。

拨打厂家的售后服务电话进行询问，很可能得到两种答案，一种是说与之配合的无线网卡兼容性有问题，一种是说升级一下软件版本，实在解释不通时，就说这是个特殊情况，总之承认自身产品有问题的厂商几乎没有。

4. 兼容性差

我们常常会遇到这样的情况，无线产品的说明书中清楚地告诉消费者，其产品兼容某某技术的产品，但是在实际使用中却并非如此。无线安全兼容性差主要表现在一个厂商生产的无线路由器或无线 AP 与另外的厂商生产的无线网卡连接工作时不兼容。

产生不兼容的原因是，不同厂家使用的芯片等硬件和使用的技术有区别，或者是早期的产品跟应用新技术的新产品之间的兼容性不好，例如一些无线产品是在迅驰技术出现之前就设计完成的，在设计时根本就没有考虑到迅驰会如此普遍使用，从而导致对迅驰的兼容性不好。兼容性问题将直接导致无线产品之间无法连接，或者连接速度较差。

5. 抗干扰性差

随着日常使用的电子产品的逐渐增多，与无线产品使用相同频段的产品也越来越多，这极大地影响了无线路由器与无线网卡之间数据传输的速率，这就对无线产品的抗干扰性提出了更高的要求。

干扰主要来自两个方面，首先是来自附近同频段无线设备的干扰，随着无线市场的发展与无线产品的使用密度

不断增大，该问题在公司、写字楼、商业区、住宅区都极易发生。另外，其他一些干扰源也会对无线路由器的天线收发效果有较大影响，例如无绳电话(2.4 或 5.xGHz)、蓝牙设备(2.4GHz)、脉冲雷达 (5.4GHz)、微波炉(在 2.4GHz 频宽中 50%的忙闲度将产生脉冲干扰)、低能量 RF 光源(2.4GHz)等。一些无线产品为了降低制造成本，抗干扰性设计和屏蔽金属材料都比较差，导致无线产品抗干扰性差或者根本没有抗干扰性。

6. 散热性差

无论是无线路由器还是无线网卡，其芯片和各种器件都是工作在一定工作环境下的，例如温度有一定的范围，如果温度太高将直接导致工作效率的下降，甚至导致无线产品的损坏。无线产品工作时必然会产生一定的热量，所以能否及时散热是无线产品质量检验的重要指标，这与无线产品的设计结构、工作功率、散热特点、散热材料等密切相关。

有的无线产品因为片面追求美观和低成本，而大量采用散热效果不好的材料和结构，这都会导致无线产品长时间工作过热，从而影响连接速度，甚至损坏硬件。(无线网卡的工作并不是只要能在 PC 上正常安装即可，要充分考虑与无线路由器或 AP 的兼容性和配合性，否则会影响无线传输距离和工作效率，所以在购买时不要仅仅试验在笔记本电脑中能否正常安装使用，而关键要看能否与无线设备配合好。

以上的相关内容就是对无线安全 你应该掌握的六个拿手绝活的介绍，望你能有所收获。

来源： 比特网