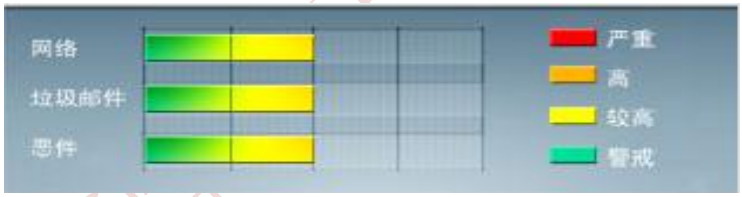
安全威胁每周警讯

2014/01/05～2014/01/11

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	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	X97M_OLEMAL.A	宏病毒	★★	↓	宏病毒，它会将本身的下列副本放置到受影响的系统：%User Profile%\Application Data\Microsoft\Excel\XLSTART\k4.xls
4	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
5	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
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	X97M_LAROUX.CO	宏病毒	★★	↓	Office 宏病毒，由其他恶意软件或访问恶意网站感染
8	ALS_PASSDOC.SM	木马	★★★	→	木马病毒，该病毒由其他恶意程序释放或访问恶意站点感染
9	WORM_VB.DVP	蠕虫	★★	↑	蠕虫病毒，通过访问恶意站点下载感染。感染该病毒后会在每个盘符下生成 autorun.inf 文件已达到用户在访问磁盘时执行该病毒
10	PE_CORELINK.C-1	PE 病毒	★★★★	→	PE 病毒，会感染电脑中其他执行程序，并且该病毒会释放其他恶意代码

本周安全趋势分析

趋势科技热门病毒综述-- BKDR_SHOTODOR.A

病毒描述：此恶意软件使用”无用”的字符串来隐藏恶意代码，该恶意代码是一个经过混淆的 AutoIt 脚本。

感染途径：

- 这个后门可能通过其他恶意软件释放，也可能是用户在不经意间从恶意网站上下载
- 它增加一条用于禁用任务管理器的注册表键值，防止用户使用任务管理器终止恶意进程
- 它可以接受远端黑客指令，从而更有效地攻击
- 它会修改 Internet Explorer 区域设置，并且通过记录用户键盘输入来盗取信息

- 对该病毒的防护可以下载更新趋势最新病毒码：10.329.00 或以上版本
  http://support.trendmicro.com.cn/Anti-Virus/China-Pattern/Pattern/

- 病毒详细信息请查询：
  http://about-threats.trendmicro.com/us/malware/BKDR_SHOTODOR.A