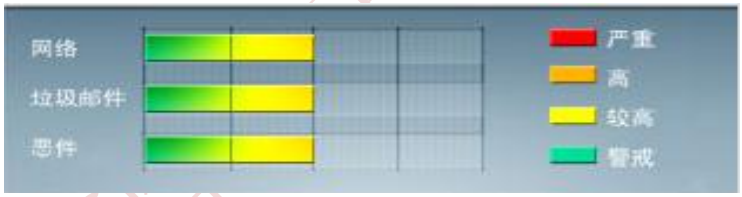
安全威胁每周警讯

2013/12/01～2013/12/07

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	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
4	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\k5.xls
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	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
9	TROJ_FLDSCN.A-CN	木马	★★	↑	木马病毒，通过浏览恶意网站或下载带有恶意软件的程序感染
10	WORM_ECODE.B-CN	蠕虫	★★★★	↑	E 语言病毒,产生与当前文件夹同名 exe 文件

本周安全趋势分析

趋势科技热门病毒综述 - BKDR_EVILOGE.SM

病毒描述：这个恶意软件被用于 EvilGrab 运动，主要针对中国和日本。
这个恶意软件通过由其它病毒释放或当用户浏览恶意网站时不经意间下载而抵达系统。
它会检索系统中的特定信息，接受黑客远程控制。并在执行后删除自身。

- 对该病毒的防护可以从下述连接中获取最新版本的病毒码：10.193.00
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_EVILOGE.SM