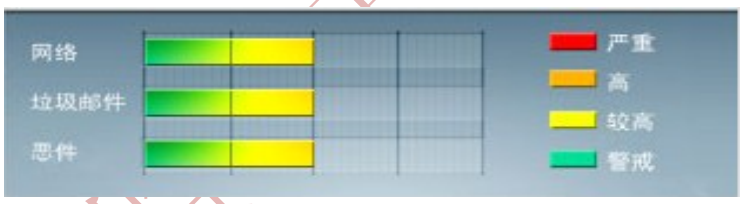
安全威胁每周警讯

2013/12/22～2013/12/29

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	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.AD	蠕虫	★★★★	↑	它可能是用户在访问恶意网站时在无意中下载而来。它可能是使用者手動安装的。它生成序列号，破解需要输入有效序列号的程序，开启所有功能。
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	PE_CORELINK.C-1	文件感染病毒	★★★★	↑	文件感染型病毒，病毒会将恶意代码植入到受感染电脑上的可执行文件中
8	PAK_Generic.001	加壳程序	★★	→	经过加壳技术加密的文件
9	X97M_LAROUX.CO	宏病毒	★★	↑	宏病毒，由其他恶意软件或访问恶意网站感染
10	TROJ_SPNR.0BL612	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。

本周安全趋势分析

趋势科技热门病毒综述 - BKDR_BLYPT.A

这个后门属于 BLYPY 家族，它使用 BLOB 将信息存放在系统注册表中。同时它还是用加密技术。用户可能会发现他们的系统已经被感染。

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。

黑客可以远程执行恶意指令。

- 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：10.291.00
  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_BLYPT.A