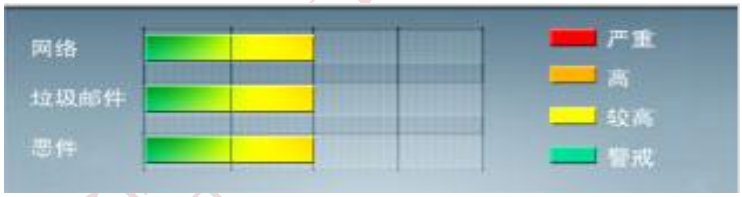
安全威胁每周警讯

2013/10/28～2013/11/03

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	CRCK_KEYGEN	破解程序	★★	↑	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	ANDROIDOS_ KINGROOT.TAA	破解软件	★★	↓	安卓手机 ROOT 软件，属于破解软件，可能会对系统造成损害
5	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
6	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
7	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
8	TROJ_SPNR.0CHR13	木马	★★★	↑	木马程序,通常由其他恶意软件携带
9	Cryp_Xed-12	加壳文件	★★	↓	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
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_LIFTOH.AD

病毒描述：这个恶意软件参与了针对英国用户的垃圾邮件攻击，一旦恶意附件被打开，它必然导致下载一个 ZBOT 恶意软件。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。

- 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：10.349.00

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_LIFTOH.AD