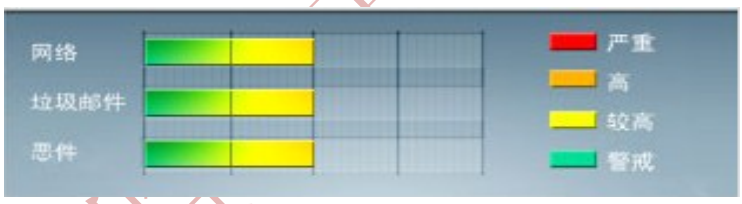
安全威胁每周警讯

2014/02/09～2014/02/15

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 501 个恶意网站下载病毒
2	TORJ_DOWNAD.INF	木马	★★★	↓	DOWNAD 蠕虫关联木马
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 501 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	WORM_ECODE.E-CN	蠕虫	★★★★	↑	E 语言病毒,产生与当前文件夹同名 exe 文件
6	TROJ_SPNR.38B814	木马	★★★	↑	通过云端病毒码发现的可疑文件
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	TORJ_IFRAME.CP	木马	★★★	↑	IFRAME 病毒，通常是网页中插入可疑 IFRAME 框架，这会引导用户访问恶意站点
10	TROJ_SPNR.03J313	木马	★★★	↑	通过云端病毒码发现的可疑文件

本周安全趋势分析

趋势科技热门病毒综述 - TROJ_BANLOAD.GB

这个 BANLOAD 变种会检查 G-buster 插件是否运行，G-buster 插件是一个保护在线网银的插件。

它这样做的目的主要是侦测用户正在使用网银。

如果发现正在使用，该恶意软件可以无视这个插件执行它的例程。

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：10.529.00
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/TROJ_BANLOAD.GB