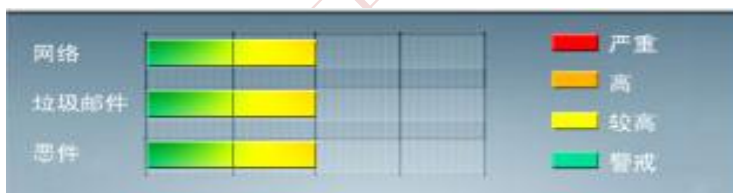




安全威胁每周警讯

2015/04/27 ~ 2015/05/03

本周威胁指数



TrendMicro 中国区网络安全监控中心



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



ANTIVIRUS



ANTI-PHISHING



WEB FILTERING



TOP 10

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	W97M_Generic	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
5	TROJ_LPKHJK.A-CN	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。
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	WORM_ECODE.E-CN	蠕虫	★★★★★	↑	E 语言病毒, 产生与当前文件夹同名 exe 文件
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	Ripper*	木马	★★★★	↑	引导区病毒
10	VBS_RAMNIT.SMC	脚本病毒	★★	→	VBS 脚本病毒, 通过浏览恶意网站感染



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



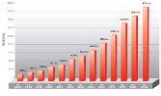
ANTIVIRUS



ANTI-PHISHING



WEB FILTERING



本周安全趋势分析

趋势科技热门病毒综述 - BKDR_SIMDA.SMEP

此恶意软件家族源于 SIMDA 僵尸网络。它于 2015 年 4 月被发现。它会连接远程恶意站点，用于发送与接收数据。它会在执行后删除自身。

- 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：11.504.00

<http://support.trendmicro.com.cn/Anti-Virus/China-Pattern/Pattern/>

- 病毒详细信息请查询：

http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/BKDR_SIMDA.SMEP

Trend Micro 监控中心提供



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



ANTIVIRUS



ANTI-PHISHING



WEB FILTERING