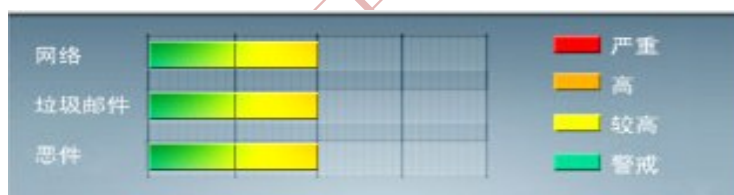




安全威胁每周警讯

2014/03/23 ~ 2014/03/29

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	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
5	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.x
6	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
7	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
8	TROJ_SPNR_03J313	木马	★★★★	↑	疑似木马
9	WORM_ECODE.E-CN	蠕虫	★★★★★	↓	易语言编写的蠕虫，会在文件夹下产生同名 exe 文件
10	PE_CORELINK.C-1	文件感染	★★★★★	↑	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



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



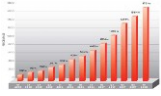
ANTIVIRUS



ANTI-PHISHING



WEB FILTERING



本周安全趋势分析

趋势科技热门病毒综述 - SWF_EXPLOIT.PB

这恶意软件利用一个关于 Internet Explorer 多个版本的 0day 漏洞，如果利用成功，它将会释放一个后门。

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：10.607.00

<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/SWF_EXPLOIT.PB

Trend Micro 监控中心提供



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



ANTIVIRUS



ANTI-PHISHING



WEB FILTERING