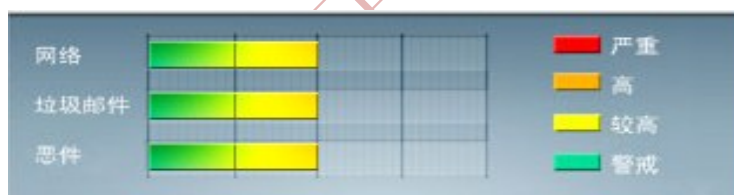




安全威胁每周警讯

2014/04/27 ~ 2014/05/03

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	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	★★★★★	↑	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	★★★★	↑	木马病毒，通常是在网页中嵌入一个隐藏的 iframe 框架，浏览者可能会被诱导至恶意网站
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	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	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
8	X97M_LAROUX.CO	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
9	HTML_IFRAME.AZ	木马	★★★★	↑	网页木马，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	TORJ_LPKHJK.A-CN	木马	★★★★	↑	木马程序



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



ANTIVIRUS



ANTI-PHISHING

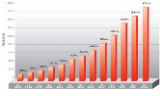


WEB FILTERING



TREND
MICRO
趋势科技

全程护航
迈向云端



本周安全趋势分析

趋势科技热门病毒综述 - TROJ_EXPLOYT.AGH

这个题为暴力恐怖袭击的 DOC 文档利用了 2014 年 3 月初的昆明事件，作为社会工程学的诱饵。它利用了微软的 Office 漏洞 CVE-2012-0158 释放后门 (BKDR_GHOST.LRK)。

此病毒主要通过邮件进行传播。

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：10.642.07

<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_EXPLOYT.AGH

Trend Micro 监控中心提供



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



ANTIVIRUS



ANTI-PHISHING



WEB FILTERING