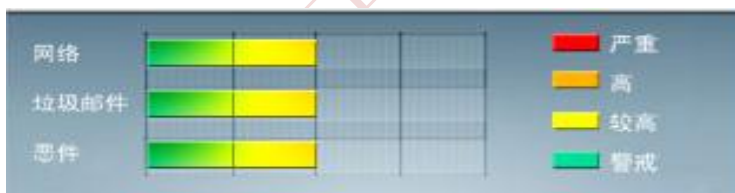




安全威胁每周警讯

2013/04/21 ~ 2013/04/28

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.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
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	TROJ_DOWNAD.INF	木马	★★★★	➔	DOWNAD 蠕虫关联木马
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.xls
6	TROJ_UPACK.A-CN	木马病毒	★★★★	↑	木马病毒, 通过浏览恶意网站感染
7	WORM_ECODE.E-CN	蠕虫	★★★★★	↓	蠕虫病毒, 通过移动存储传播, 该病毒会产生与当前文件夹同名 exe 文件。感染该病毒的电脑会在外接的移动存储上复制一个 AUTORUN.INF 文件和自身拷贝, 使得其他电脑使用该移动存储时运行该病毒文件
8	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
9	WORM_VB.DVP	蠕虫	★★★	↑	蠕虫病毒, 通过访问恶意站点下载感染。感染该病毒后会在每个盘符下生成 autorun.inf 文件已达到用户在访问磁盘时执行该病毒
10	TROJ_IFRAME.AKD	木马	★★★	↑	木马病毒, 通过浏览恶意网站或下载带有恶意软件的程序感染



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



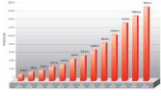
ANTIVIRUS



ANTI-PHISHING



WEB FILTERING



本周安全趋势分析

趋势科技热门病毒综述-- OSX_PINTSIZED.ENV

病毒描述: 由其它恶意软件释放, 从因特网下载。该恶意软件参与了 2013 年 1 月的 JAVA 零日漏洞攻击, 后门程序允许攻击者远程执行指令, 这可能会危及系统安全。

感染途径:

- 由其它恶意软件释放
- 从因特网下载感染

- 对该病毒的防护可以下载更新趋势最新病毒码: 9.749.60 或以上版本

<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/OSX_PINTSIZED.ENV



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



ANTIVIRUS



ANTI-PHISHING



WEB FILTERING