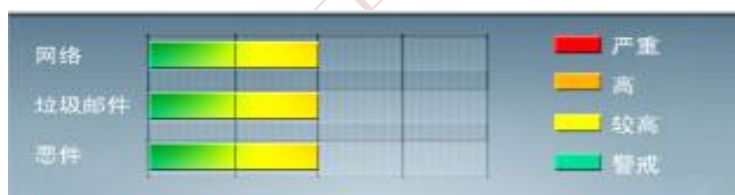




安全威胁每周警讯

2015/03/01 ~ 2015/03/08

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	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
3	TROJ_DOWNAD.INF	木马	★★★	➔	DOWNAD 蠕虫关联木马
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\k4.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_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。
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	WORM_ECODE.B-CN	蠕虫	★★★★	↑	E 语言病毒, 产生与当前文件夹同名 exe 文件
9	WORM_DOWNAD.FUF	蠕虫	★★★★	↑	蠕虫病毒, 该病毒通过其他恶意程序、移动磁盘和网络传播, 感染该病毒后病毒会将自己复制到本地逻辑磁盘中, 然后通过网络扩散。 病毒会修改注册表文件来禁用某些系统服务, 同时会释放 autorun.inf 文件到自动启动项中, 使得用户访问磁盘时激活病毒。
10	TROJ_DOWNAD.E	木马	★★★	↑	木马病毒, 该病毒由其他恶意软件释放或访问恶意网站感染。



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



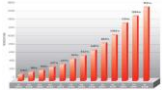
ANTIVIRUS



ANTI-PHISHING



WEB FILTERING



## 本周安全趋势分析

趋势科技热门病毒综述-- BKDR\_ALINA.SM

**病毒描述:** 这是 point-of-sale (PoS)家族的新变种 Alina。它在 2015 年 1 月被发现。

**感染途径:**

- 通过其他恶意软件下载
- 访问恶意网站感染

- ▶ 对该病毒的防护可以下载更新趋势最新病毒码: 11.500.60 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://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/BKDR\\_ALINA.SM](http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/BKDR_ALINA.SM)

Trend Micro 监控中心提供



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



ANTIVIRUS



ANTI-PHISHING



WEB FILTERING