



安全威胁每周警讯

2014/12/28 ~ 2015/01/03

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	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	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。
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	TROJ_CORELINK.D	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	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	WORM_ECODE.B-CN	蠕虫	★★★★	↑	E 语言病毒, 产生与当前文件夹同名 exe 文件
10	TROJ_VSTART.SMA	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。



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



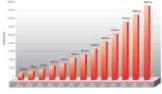
ANTIVIRUS



ANTI-PHISHING



WEB FILTERING



## 本周安全趋势分析

### 趋势科技热门病毒综述-- TSPY\_POSLUSY.A

**病毒描述:** 这是一种被称之为 LusyPOS 的新 POS 恶意软件家族, 它与 Dexter 和 Chewbacca 有类似之处。该间谍软件会将已收集到的信息资源发送到已知的恶意站点, 同时它会删除自身的副本文件。

#### 感染途径:

➤ 该间谍软件由其他恶意程序释放或从恶意的网站下载

➤ 对该病毒的防护可以下载更新趋势最新病毒码: 11.318.60 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/TSPY\\_POSLUSY.A](http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/TSPY_POSLUSY.A)



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



ANTIVIRUS



ANTI-PHISHING



WEB FILTERING