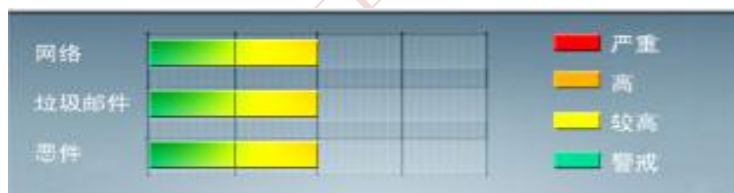




安全威胁每周警讯

2014/08/17 ~ 2014/08/23

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 | 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 |
| 3 | 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 |
| 4 | 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 |
| 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 | WORM_ECODE.E-CN | 蠕虫 | ★★★★★ | ↓ | E 语言病毒,产生与当前文件夹同名 exe 文件 |
| 7 | 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。 |
| 8 | 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 |
| 9 | 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。 |
| 10 | W97M_RELAX.J | 宏病毒 | ★★ | ↑ | 宏病毒，通过移动附件，软盘，U 盘，网络下载，文件传输，以及合作应用传播。 |



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



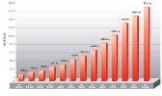
ANTIVIRUS



ANTI-PHISHING



WEB FILTERING



本周安全趋势分析

趋势科技热门病毒综述-- TSPY_POSLOGR.B

病毒描述: 此病毒参与了 2014 年 8 月的 Backoff POS 的事件，它可以从被感染主机中盗取金融信息。受影响的用户可能会发现账户资金突然被耗尽！

▶ 对该病毒的防护可以下载更新趋势最新病毒码：10.957.00

<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/TSPY_POSLOGR.B

Trend Micro 监控中心提供



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



ANTIVIRUS



ANTI-PHISHING



WEB FILTERING