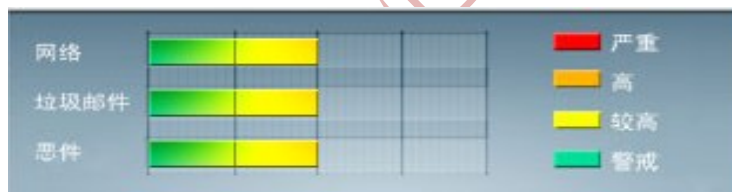


安全威胁每周警讯

2015/11/29~2015/12/05

本周威胁指数



亚信安全 网络安全监控中心



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



ANTIVIRUS



ANTI-PHISHING



WEB FILTERING


**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	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	VBS_RAMNIT.SMC	脚本病毒	★★	↑	VBS 脚本病毒, 通过浏览恶意网站感染
6	Ripper*	木马	★★★★	↑	引导区病毒
7	VBS_SMALL.IHE	脚本病毒	★★	↑	VBS 脚本病毒, 通过浏览恶意网站感染
8	WORM_ECODE.E-CN	蠕虫	★★★★★	↓	易语言病毒, 会在文件夹下生成同名 exe 文件
9	JS_IFRAME.XXSU	脚本病毒	★★	↑	Javascript 病毒, 会诱导用户访问恶意站点
10	LNK_IPPEDO.SM	木马	★★★★	↑	木马程序, 通常夹带在其他软件中



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



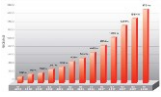
ANTIVIRUS



ANTI-PHISHING



WEB FILTERING



## 本周安全趋势分析

### 亚信安全热门病毒综述 - BKDR\_KASIDET.XXRO

这个恶意软件与 adobe flash 零日漏洞 CVE-2015-7645 有关。

该后门程序通常由其他恶意软件传播，或在用户不知情的情况下由恶意网站下载  
它会受感染的计算机上执行黑客的远程指令

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：12.192.60

<http://support.asiainfo-sec.com/Anti-Virus/China-Pattern/Pattern/>

病毒详细信息请查询：

[http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/bkdr\\_kasidet.xxro](http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/bkdr_kasidet.xxro)

亚信安全 监控中心提供



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



ANTIVIRUS



ANTI-PHISHING



WEB FILTERING