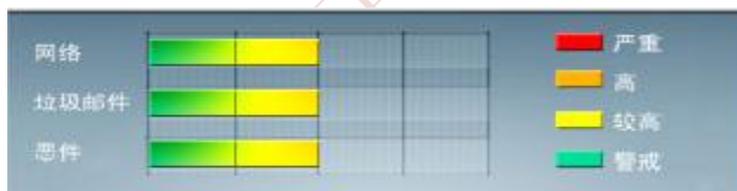




安全威胁每周警讯

2013/09/16~2013/09/21

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	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	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	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	★★★	↑	Office 宏病毒, 由其他恶意软件或访问恶意网站感染
6	TROJ_SPNR.0CHR13	木马	★★★★	↓	木马程序, 通常由其他恶意软件携带
7	WORM_ECODE.E-CN	蠕虫	★★★★★	↑	E 语言病毒, 产生与当前文件夹同名 exe 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	ALS_PASSDOC.SM	木马	★★★★	↑	该木马是通过其他恶意下载器在用户访问某些恶意网站时下载到系统中的。
10	ACM_AGENT.AVGL	木马	★★★★	↑	该木马是通过其他恶意下载器在用户访问某些恶意网站时下载到系统中的。



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



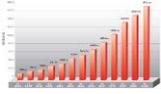
ANTIVIRUS



ANTI-PHISHING



WEB FILTERING



本周安全趋势分析

趋势科技热门病毒综述 - BKDR_FIDOBOT.A

感染途径：从因特网下载,由其他恶意软件释放

这个后门经常被犯罪分子用于暴力破解 WordPress 的后台管理密码。它被执行后，它会连接到一个控制服务器，下载目标站点的列表以及用于破解的密码。

该间谍软件通过由其它病毒释放或当用户浏览恶意网站时不经意间下载而抵达系统。

对该病毒的防护可以从以下连接下载最新版本的病毒码：10.255.00

<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/BKDR_FIDOBOT.A



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



ANTIVIRUS



ANTI-PHISHING



WEB FILTERING