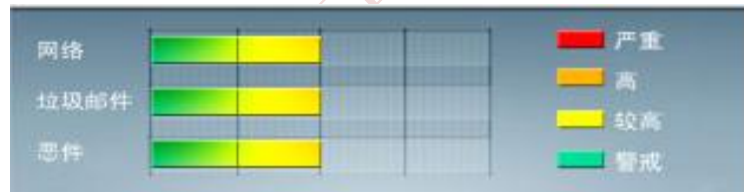




安全威胁每周警讯

2013/03/17 ~ 2013/03/23

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	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
2	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
3	TROJ_DOWNAD.INF	木马	★★★★	↑	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	CRCK_KEYGEN	破解程序	★★★	↑	软件破解程序
6	X97M_OLEMALA	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	Cryp_Xed-12	加壳程序	★★	↑	被加密过的程序
8	HTML_IFRAME.AZ	网页病毒	★★	↑	网页病毒通常隐藏在网站页面中，将浏览者导向钓鱼网站或者暗中下载恶意程序
9	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
10	PAK_Generic.001	加壳文件	★★	↑	经过加壳技术加密的文件



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



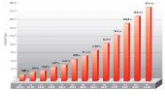
ANTIVIRUS



ANTI-PHISHING



WEB FILTERING



本周安全趋势分析

趋势科技热门病毒综述 - TROJ_MDROP.REF

感染途径：从因特网上下载，由其它恶意文件释放。

该恶意软件利用Adobe Flash Player零日漏洞来释放病毒文件。

该恶意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：9.715.00

<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/TROJ_MDROP.REF

Trend Micro 监控中心提供



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



ANTIVIRUS



ANTI-PHISHING



WEB FILTERING