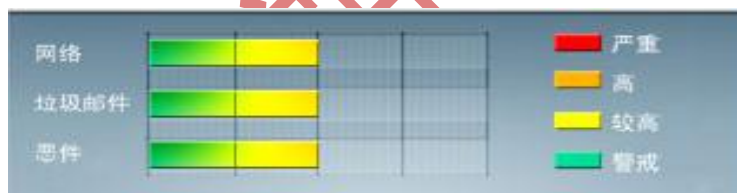




安全威胁每周警讯

2013/06/17 ~ 2013/06/23

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	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
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	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
5	CRCK_KEYGEN	破解程序	★★	↓	疑似木马病毒, 通过访问恶意站点下载感染或由其他恶意程序下载感染
6	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
7	Adware_Adplus 16	灰色软件	★★	↑	广告程序, 它可能是用户在访问恶意网站时在无意中下载而来。
8	X97M_LAROUX.BK	宏病毒	★★	→	宏病毒, 主要通过用户浏览恶意网站感染, 该病毒主要感染 Office Excel 文件, 并且会在 Excel 中创建一个名为 StartUp 的宏脚本
9	Cryp_Xed-12	加壳文件	★★	↓	疑似木马病毒, 通过访问恶意站点下载感染或由其他恶意程序下载感染
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



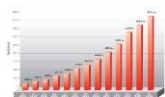
ANTIVIRUS



ANTI-PHISHING



WEB FILTERING



本周安全趋势分析

趋势科技热门病毒综述 -- TSPY_PASSTEAL.A

病毒描述:

这个恶意软件包含一个密码恢复工具，用来盗取用户存储在浏览器中的密码。

该恶意软件是由用户访问恶意网站时不经意间下载的文件释放出的。

- 对该病毒的防护可以下载更新趋势最新病毒码：9.495.00 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://about-threats.trendmicro.com/us/malware/TSPY_PASSTEAL.A

Trend Micro 监控中心提供



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



ANTIVIRUS



ANTI-PHISHING



WEB FILTERING