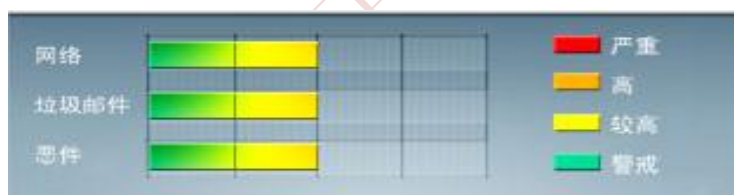




安全威胁每周警讯

2013/01/13 ~ 2013/01/20

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	★★★★	↑	DOWNAD 蠕虫关联木马
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_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
6	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
7	HTML_IFRAME.CBE	网页病毒	★★	↑	网页病毒, 通常在网页在插入一个恶意 iframe, 用户在访问该网页时会下载恶意文件或重定向到恶意网站
8	HTML_IFRAME.AZ	网页病毒	★★	↓	网页病毒, 通常在网页在插入一个恶意 iframe, 用户在访问该网页时会下载恶意文件或重定向到恶意网站
9	WORM_ECODE.E-CN	蠕虫	★★★★★	➡	E 语言病毒, 产生与当前文件夹同名 exe 文件
10	PE_CORELINK.C-1	PE 病毒	★★★★★	↑	PE 病毒, 主要通过其他恶意程序释放或浏览恶意网站感染。该病毒会感染电脑上的可执行文件。



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



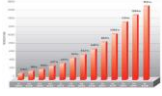
ANTIVIRUS



ANTI-PHISHING



WEB FILTERING



本周安全趋势分析

趋势科技热门病毒综述-- TROJ_GUPBOOT.A

病毒描述: 该木马会覆写 MBR 并写入新代码。它还包含病毒 TSPY_UREL.A.S.A, 这个间谍软件会对用户系统上的一款韩国游戏进行截屏, 威胁玩家的账户安全。该木马病毒是在用户访问恶意网站时不经意间下载而感染用户系统的。

感染途径: 由其它恶意软件释放, 从因特网下载。

- ▶ 对该病毒的防护可以下载更新趋势最新病毒码: 9.644.60 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/TROJ_GUPBOOT.A



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



ANTIVIRUS



ANTI-PHISHING



WEB FILTERING