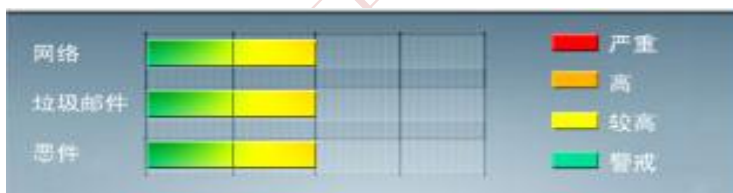




安全威胁每周警讯

2013/10/13 ~ 2013/10/19

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	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_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
4	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
5	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
6	ANDROIDOS_KINGROOT.TAA	破解软件	★★	↑	安卓手机 ROOT 软件, 属于破解软件, 可能会对系统造成损害
7	WORM_ECODE.E-CN	蠕虫	★★★★★	➡	蠕虫病毒, 通过移动存储传播, 该病毒会产生与当前文件夹同名 exe 文件。感染该病毒的电脑会在外接的移动存储上复制一个 AUTORUN.INF 文件和自身拷贝, 使得其他电脑使用该移动存储时运行该病毒文件
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	WORM_ECODE.B-CN	蠕虫	★★★★★	↑	蠕虫病毒, 通过移动存储传播, 该病毒会产生与当前文件夹同名 exe 文件。感染该病毒的电脑会在外接的移动存储上复制一个 AUTORUN.INF 文件和自身拷贝, 使得其他电脑使用该移动存储时运行该病毒文件
10	ALS_PASSDOC.SM	木马	★★★★	↓	木马病毒, 该病毒由其他恶意程序释放或访问恶意站点感染。



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



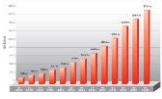
ANTIVIRUS



ANTI-PHISHING



WEB FILTERING



本周安全趋势分析

趋势科技热门病毒综述-- ANDROIDOS_OPFAKE.CTD

病毒描述: 这个恶意软件会伪造成 WhatsApp 的通知。一旦用户点击电子邮件中的“Play”按钮，它将导致一个多平台的恶意软件被执行，Windows、IOS、Android 的设备将受影响。

感染途径:

➤ 下载自互联网，或由其他恶意软件释放

▶ 对该病毒的防护可以下载更新趋势最新病毒码：1.567.00 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/ANDROIDOS_OPFAKE.CTD



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



ANTIVIRUS



ANTI-PHISHING



WEB FILTERING