安全威胁每周警讯

2012/12/30～2013/01/06

本周威胁指数

***TrendMicro* 中国区网络安全监控中心**

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	★★	↓	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	CRCK_KEYGEN	破解程序	★★	↑	软件破解程序
7	Cryp_Xed-12	加壳程序	★★	↓	被加密过的程序
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	PAK_Generic.001	加壳文件	★★	↑	经过加壳技术加密的文件
10	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

本周安全趋势分析

趋势科技热门病毒综述 --TROJ_RANSOM.SMAC

病毒描述：

感染途径：由其它恶意软件释放，从因特网下载

该恶意程序伪装成来自联邦调查局（FBI）或警方的罚款通知发送到收件人邮箱。也可能来源于被其他恶意软件感染后的主机。

- 对该病毒的防护可以下载更新趋势最新病毒码：9.637.00 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/Malware.aspx?language=cn&name=TROJ_RANSOM.SMAC