安全威胁每周警讯

2013/11/10～2013/11/16

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	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.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	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	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
6	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
7	WORM_ECODE.E-CN	蠕虫	★★★★	↑	E 语言病毒,产生与当前文件夹同名 exe 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	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。
10	ACM_AGENT.AVGL	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。

本周安全趋势分析

趋势科技热门病毒综述-- TROJ_CRILOCK.NS

病毒描述：这个 CryptoLocker 勒索软件会下载一个 ZeuS/ZBOT 的变种，检测名称为 TSPY_ZBOT.VNA 。当它执行后，它会加密文件，并且让用户购买解密工具。

感染途径：

- 通过由其它病毒释放
- 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下载更新趋势最新病毒码：10.314.60 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_CRILOCK.NS