安全威胁每周警讯

2014/11/02～2014/11/08

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	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
2	TROJ_DOWNAD.INF	木马	★★★	→	DOWNAD 蠕虫关联木马
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_ECODE.E-CN	蠕虫	★★★★	↑	E 语言病毒,产生与当前文件夹同名 exe 文件
5	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
6	TROJ_LPKHJK.A-CN	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。
7	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
8	PE_CORELINK.C-1	PE 病毒	★★★★	↓	PE 病毒，会感染电脑中其他执行程序，并且该病毒会释放其他恶意代码
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	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

本周安全趋势分析

趋势科技热门病毒综述-- TSPY_DYRE.EKW

病毒描述：这个名为 DYREZA 的恶意软件利用了 CVE-2013-2729 漏洞(Adobe Reader 和 Acrobat 9.5.5 之前的 9.x 版本，10.1.7 之前的 10.x 版本，11.0.03 之前的 11.x 版本中存在整数溢出漏洞。攻击者可利用该漏洞执行任意代码)，此恶意软件会盗取用户的银行及比特币信息。该病毒会连接到某个网站接收和发送信息，并且病毒执行后会自动删除。

感染途径：

- 该间谍软件也会由以下恶意程序从远程网络上下载
  - TROJ_PIDIEF.LK
  - TROJ_PIDIEF.UXL
  - TROJ_PIDIEF.YYGA
- 通过访问恶意网站下载或邮件传播

- 对该病毒的防护可以下载更新趋势最新病毒码：11.220.60 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://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/tspy_dyre.ekw