安全威胁每周警讯

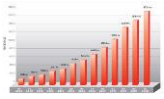
2014/05/18～2014/05/24

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	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	ALS_PASSDOC.SM	木马	★★★	↑	该木马是通过其他恶意下载器在用户访问某些恶意网站时下载到系统中
8	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
9	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
10	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



本周安全趋势分析

趋势科技热门病毒综述-- BKDR_CARETO.A

病毒描述：这是一个与 Careto 攻击有关的恶意软件，它加密数据以及它的网络流量，使得更难以被分析。

感染途径：

- 该后门通过其它恶意软件/灰色软件或恶意用户发送的垃圾邮件附件抵达
- 该恶意软件通过由其它病毒释放或当用户浏览恶意网站时不经意间下载而抵达系统
- 它窃取系统信息，并在执行后删除自身

- 对该病毒的防护可以下载更新趋势最新病毒码：10.601.00 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/BKDR_CARETO.A