安全威胁每周警讯

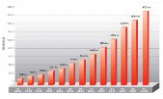
2014/01/16～2014/02/01

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 501 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 501 个恶意网站下载病毒
4	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\k5.xls
5	BKDR_POISON.BXD	木马	★★★	↑	木马病毒，会在受感染电脑上开启后门
6	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
7	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
8	PE_CORELINK.C-1	文件感染	★★★★	↑	该病毒会将恶意代码插入到正常文件中并通过网络共享以及移动存储设备传播
9	WORM_ECODE.E-CN	蠕虫	★★★★	↓	E 语言病毒,产生与当前文件夹同名 exe 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



本周安全趋势分析

趋势科技热门病毒综述 - TSPY_CHISBURG.A

此恶意软件使用 AutoIT 打包，当它被执行后会盗取 Yahoo, Hotmail, Pidgin 等等的用户名和密码。
这个恶意软件可能是用户在不经意间从恶意网站上下载。

对该病毒的防护可以从下述连接中获取最新版本的病毒码：10.481.00

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/TSPY_CHISBURG.A