安全威胁每周警讯

2013/03/24～2013/03/30

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	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	TROJ_DOWNAD.INF	木马	★★★	→	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	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
7	HTML_IFRAME.AZ	网页病毒	★★	↑	网页病毒通常隐藏在网站页面中，将浏览者导向钓鱼网站或者暗中下载恶意程序
8	WORM_ECODE.E-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	WORM_VB.DVP	蠕虫	★★	↑	蠕虫病毒，通过访问恶意站点下载感染。感染该病毒后会在每个盘符下生成 autorun.inf 文件已达到用户在访问磁盘时执行该病毒
10	TROJ_FLDSCN.A-CN	木马	★★	↑	木马病毒，通过浏览恶意网站或下载带有恶意软件的程序感染

本周安全趋势分析

趋势科技热门病毒综述 - JAVA_EXPLOIT.XE

感染途径：从因特网上下载，由其它恶意文件释放。

该恶意软件利用了Java零日漏洞，一旦成功利用此漏洞，它会下载并执行McRAT后门。

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。

- 对该病毒的防护可以从以下连接下载最新版本的病毒码：9.775.00

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/JAVA_EXPLOIT.XE