安全威胁每周警讯

2013/04/14～2013/04/20

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.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
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	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	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
7	X97M_LAROUX.CO	宏病毒	★★	↑	宏病毒，由其他恶意软件或访问恶意网站感染
8	Adware_Adplus	广告程序	★★	↑	广告程序

9	Downloader_Agent	木马	★★★	↑	该恶意软件通常被用于下载其他恶意程序
10	TROJ_FLDSCN.A-CN	木马	★★★	↑	木马程序, 通常在浏览恶意站点时被下载或夹带在其他程序中

本周安全趋势分析

趋势科技热门病毒综述 - TSPY_MINOCDO.A

感染途径：由其它恶意软件释放，从因特网下载。

该恶意软件拦截访问 Facebook 的访问流量，并且重定向到一个欺诈页面，诱导用户输入他们的信用卡信息。受此恶意软件的影响，用户可能会发现他们的财务账户收到影响。

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。

它修改系统 HOST 文件，阻止用户访问某些站点；

它在受影响系统中检索特定信息；

它连接到某些站点，用于发送接收信息。

- 对该病毒的防护可以从以下连接下载最新版本的病毒码：9.827.00

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_MINOCDO.A