安全威胁每周警讯

2015/12/27～2016/01/02

本周威胁指数

亚信安全 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	HTML_REDIR.WQUE	网页病毒	★★★	↑	主要存在被挂马网站中。
4	TROJ_DOWNAD.INF	木马	★★★	↓	DOWNAD 蠕虫关联木马
5	WORM_ECODE.E-CN	蠕虫	★★★★	↑	E 语言病毒,产生与当前文件夹同名 exe 文件
6	LNK_IPPEDO.SM	木马	★★★	↑	木马程序，通常夹带在其他软件中
7	VBS_RAMNIT.SMC	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。
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	TROJ_LPKHJK.A-CN	木马	★★	→	木马程序，通常夹带在其他软件中
10	ACM_AGENT.AVGL	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

亚信安全热门病毒综述--X2KM_DRIDEX.YJQ

通过电子邮件发送垃圾邮件或从互联网上下载。它使用下列文件名保存下载的文件：%User Temp%\masqano.exe (注意：%User Temp% 是当前用户的 Temp 文件夹。通常位于 C:\Documents and Settings\{user name}\Local Settings\Temp (Windows 2000、XP 和 Server 2003)。

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：12.240.60
http://support.asiainfo-sec.com/Anti-Virus/China-Pattern/Pattern/

病毒详细信息请查询：
http://about-threats.trendmicro.com/Malware.aspx?language=cn&name=X2KM_DRIDEX.YJQ