安全威胁每周警讯

2015/12/13～2015/12/19

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	TROJ_DOWNAD.INF	木马	★★★	↑	DOWNAD 蠕虫关联木马
3	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。
4	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
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	LNK_IPPEDO.SM	木马	★★★	↑	木马程序，通常夹带在其他软件中
7	TROJ_LPKHJK.A-CN	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	WORM_ECODE.E-CN	蠕虫	★★★★	↓	易语言病毒，会在文件夹下生成同名 exe 文件
9	Ripper*	木马	★★★	↓	引导区病毒
10	VBS_SMALL.IHE	脚本病毒	★★	↑	VBS 脚本病毒，通过浏览恶意网站感染

本周安全趋势分析

亚信安全热门病毒综述 - RANSOM_CRYPTESLA.YYSIX

近日，我们监控到一起英国著名独立报网站被挂马导致传播勒索软件的事件，这可能使数以百万计的读者面临被勒索的风险。与以往的勒索软件病毒行为相同，病毒文件一旦运行，用户计算机上的私人文件就会被加密导致无法打开。此次变种会将所有加密文件后缀名修改为.vvv 格式，该变种属于 Cryptesla 2.2.0 勒索软件家族。

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：12.198.60
http://support.asiainfo-sec.com/Anti-Virus/China-Pattern/Pattern/

病毒详细信息请查询：
http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/ransom_cryptesla.yysix