安全威胁每周警讯

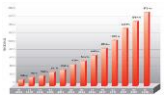
2016/12/12～2016/12/18

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	Ripper*	引导区病毒	★★★	→	引导区病毒
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	X97M_OLEMAL.A	宏病毒	★★★	↑	宏语言病毒，通过 office 文件传播
4	INFECT.MBR-B*	引导区病毒	★★★	↑	引导区病毒，该病毒由其他恶意程序释放或访问恶意站点感染。
5	TROJ_DOWNAD.INF	木马	★★★	↓	Downad 蠕虫关联病毒
6	VBS_RAMNIT.SMC	木马	★★★	↑	当用户访问它托管的某些网站时，它就会开始执行。它可能被托管在网站中，并在用户访问所述网站时运行。 然后，它将执行植入的文件。结果，已植入文件的恶意例程将呈现在受感染的系统中。
7	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
8	ACM_NEYER.NIL	木马	★★★	↓	下载例程 它从下列 URL 中下载文件，并在受感染的系统中进行存储时重命名文件： http://{BLOCKED}b.{BLOCKED}n.com/jbbgxf/?f=xcxg 它使用下列文件名保存下载的文件： {Malware Path}\draw.fas
9	ACM_AGENT.AVGL	木马	★★	↑	木马病毒，会在各个文件夹下释放木马文件
10	TROJ_LPKHJK.A-CN	木马	★★★	→	木马病毒，会在各个文件夹下释放木马文件



本周安全趋势分析

亚信安全热门病毒综述 - RANSOM_ENIGMA.B

该勒索软件由用户访问网站下载或者其它病毒生成感染本机，其会更改 IE 设置，运行后删除自身，加密后的文件命名规则为{原始文件名和扩展名}.1txt

- 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：12.954.60
  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_enigma.b