安全威胁每周警讯

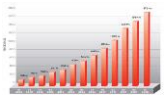
2016/06/27～2016/07/03

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	TROJ_DOWNAD.INF	木马	★★★	↑	Downad 蠕虫关联木马
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	VBS_SMALL.IHE	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	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	Ripper*	引导区病毒	★★★	→	引导区病毒
6	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。
7	WORM_ECODE.E-CN	蠕虫	★★★★	→	易语言病毒，会在文件夹下生成同名 exe 文件
8	X97M_OLEMAL.A	宏病毒	★★★	→	宏语言病毒，通过 office 文件传播
9	LNK_IPPEDO.SM	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。
10	INFECT.MBR-B*	引导区病毒	★★★	↓	引导区病毒



本周安全趋势分析

亚信安全热门病毒综述 - RANSOM_JOKOZY.A

该勒索软件使用 RSA 2048 非对称方式加密，加密后的文件无法通过第三方解密，其加密后的文件扩展名为.31392E30362E32303136_{Key_ID}_LSBJ1

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：12.614.60

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_jokozy.a