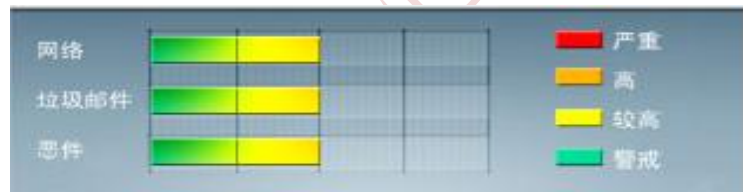


安全威胁每周警讯

2016/11/28~2016/12/04

本周威胁指数



亚信安全 网络安全监控中心



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



ANTIVIRUS



ANTI-PHISHING



WEB FILTERING


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	LNK_IPPEDO.SM	木马	★★★★	↑	木马病毒，会在各个文件夹下释放木马文件
3	TROJ_DOWNAD.INF	木马	★★★★	↑	Downad 蠕虫关联病毒
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	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
6	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。
7	TROJ_FLDSCN.A-CN	木马	★★★★	↑	木马病毒，会在各个文件夹下释放木马文件
8	WORM_ECODE.E-CN	蠕虫	★★★★★	↑	易语言病毒，会在文件夹下生成同名病毒文件
9	PE_CORELINK.C-1	文件感染	★★★★★	↑	文件感染型病毒，会在正常可执行文件代码中插入恶意代码
10	TROJ_LPKHJK.A-CN	木马	★★★★	↑	易语言病毒，会在文件夹下生成同名病毒文件



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



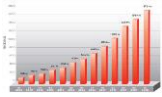
ANTIVIRUS



ANTI-PHISHING



WEB FILTERING



本周安全趋势分析

亚信安全热门病毒综述 - X2KM_LOCKY.ZZZ 和 X2KM_DLOADR.LVN

近日，亚信安全截获了大量含有恶意的 Microsoft Excel 附件的垃圾邮件，这些垃圾邮件以假发票作为诱饵，诱骗用户上当受骗。亚信安全将这些恶意的 Microsoft Excel 文件检测为 X2KM_LOCKY.ZZZ 和 X2KM_DLOADR.LVN。

其中 X2KM_LOCKY.ZZZ 是 locky 勒索软件最新变种，其在 Excel 文档中插入宏病毒，一旦 Excel 文档被运行，其会链接特定 URL 下载勒索软件病毒，加密计算机中的文件。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：12.930.60

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

病毒详细信息请查询：

http://www.trendmicro.com.cn/vinfo/cn/threat-encyclopedia/malware/X2KM_LOCKY.ZZZ

亚信安全 监控中心提供



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



ANTIVIRUS



ANTI-PHISHING



WEB FILTERING