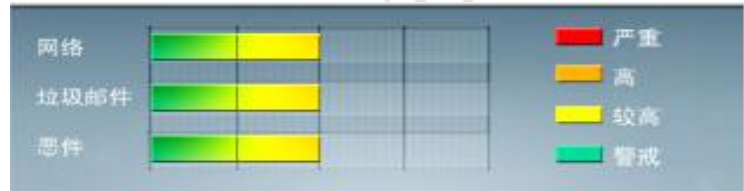


安全威胁每周警讯

2016/01/10~2016/01/16

本周威胁指数



亚信安全 网络安全监控中心

TOP 10 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	TROJ_DOWNAD.INF	木马	★★★★	↓	Downad 蠕虫关联木马
4	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。
5	Cryp_Xed-12	加壳文件	★★★	↑	疑似木马病毒, 通过访问恶意站点下载感染或由其他恶意程序下载感染
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	Ripper*	木马	★★★★	↑	引导区病毒
9	HTML_REDIR.WQUE	网页病毒	★★★★	↑	主要存在被挂马网站中。
10	CRCK_KEYGEN	破解程序	★★★	↑	它可能是用户在访问恶意网站时在无意中下载而来。它可能是使用者手动安装的。它生成序列号, 破解需要输入有效序列号的程序, 开启所有功能。



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



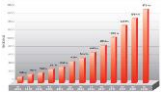
ANTIVIRUS



ANTI-PHISHING



WEB FILTERING



本周安全趋势分析

亚信安全热门病毒综述 - ransom_cryptesla.yysix

该恶意软件关联到英国新闻媒体网站页面，"独立"。用户一旦访问了被攻击页面，用户会被重定向到钓鱼站点或下载漏洞利用工具包。会有感染勒索病毒的可能性

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：12.199.00

<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

亚信安全 监控中心提供



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



ANTIVIRUS



ANTI-PHISHING



WEB FILTERING