安全威胁每周警讯

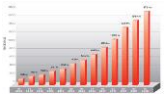
2015/11/01～2015/11/07

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	VBS_OLEAR.SM	脚本病毒	★★	→	VBS 脚本病毒，通过浏览恶意网站感染
2	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
3	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
4	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
5	TROJ_DOWNAD.INF	木马	★★★	↓	DOWNAD 蠕虫关联木马
6	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。它可能是使用者手動安装的。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。
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	VBS_SMALL.IHE	脚本病毒	★★	↓	VBS 脚本病毒，通过浏览恶意网站感染
9	WORM_ECODE.E-CN	蠕虫	★★★★	↑	E 语言病毒,产生与当前文件夹同名 exe 文件
10	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



本周安全趋势分析

亚信安全热门病毒综述-- JS_DLOADE.XXPU

病毒描述：此恶意软件参与了 2015 年 3 月的 Cryptowall 3.0 攻击，它主要存在于邮件附件，并且利用社会工程学诱骗用户点击。

感染途径：

- 由其他恶意程序/可疑程序/间谍软件或恶意使用者，以垃圾邮件的方式夹带于电子邮件附件传播
- 执行该程序后它会执行所下载的程序。如此，所下载程序的便会在受影响的系统上感染

- 对该病毒的防护可以下载更新趋势最新病毒码：11.540.60 或以上版本
  http://support.trendmicro.com.cn/Anti-Virus/China-Pattern/Pattern/

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