安全威胁每周警讯

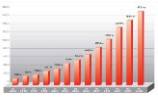
2015/08/16～2015/08/22

本周威胁指数

TrendMicro 中国区网络安全监控中心

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_SMALL.IHE	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	TROJ_DOWNAD.INF	木马	★★	↓	Downad 蠕虫关联木马
5	VBS_RAMNIT.SMC	脚本病毒	★★	↑	VBS 脚本病毒，通过浏览恶意网站感染
6	WORM_ECODE.E-CN	蠕虫	★★★★	↑	E 语言病毒,产生与当前文件夹同名 exe 文件
7	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
8	Ripper*	木马	★★★	↑	引导区病毒
9	TROJ_LPKHJK.A-CN	木马	★★	↓	木马程序，通常夹带在其他软件中
10	SWF_AGENT.CAAS	木马	★★★	↓	木马病毒，该病毒感染.SWF 文件，由其他恶意程序释放或访问恶意站点感染。



本周安全趋势分析

趋势科技热门病毒综述 - JAVA_DLOADR.EFD

这个恶意软件利用了 JAVA 的 0day 漏洞 CVE-2015-2590，它被用于某次 APT 攻击，当它被成功利用漏洞，它会下载另一个恶意软件 TROJ_DROPPR.CXC（用于释放 SEDNIT 的变种）。

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：11.791.00

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/JAVA_DLOADR.EFD