安全威胁每周警讯

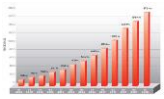
2016/05/15～2016/05/21

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	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
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	TROJ_DOWNAD.INF	木马	★★★	→	Downad 蠕虫关联木马
4	Ripper*	引导区病毒	★★★	→	引导区病毒
5	PE_CORELINK.C-1	PE 病毒	★★★	↑	感染型病毒
6	VBS_RAMNIT.SMC	脚本病毒	★★★	↓	VBS脚本病毒，通过浏览恶意站点感染
7	X97M_OLEMAL.A	宏病毒	★★	↑	宏病毒，通常夹带在 office 文档中
8	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。
9	WORM_ECODE.E-CN	蠕虫	★★★★	↓	易语言编写的蠕虫病毒，会在文件夹下生成同名 exe 文件
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。



本周安全趋势分析

近日，亚信安全截获了最新勒索软件变种 CryptXXX 和 Cerber。亚信安全将 CrptXXX 命名为 RANSOM_WALTRIX.A，与以往不同的是，该勒索软件通过用户访问恶意网站下载到本机，其不仅加密多种类型文件，还窃取系统中特定程序信息。Cerber 病毒加密后的文件扩展名为.cerber，其不但会加密文档文件，还会加密桌面及移动硬盘的数据，亚信安全将其检测为 RANSOM_CERBER.A

CryptXXX 勒索软件执行流程：

- 受害者访问恶意网站
- 下载加密勒索软件
- 勒索软件加密系统中的文件

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：12.536.60

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

病毒详细信息请查询：

http://about-threats.trendmicro.com/Malware.aspx?language=cn&name=RANSOM_CERBER.A