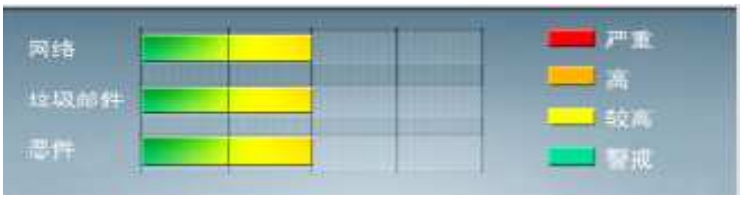
安全威胁每周警讯

2011/06/19～2011/06/27

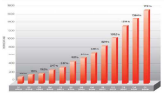
本周威胁指数



***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	TROJ_DOWNAD.INF	木马	★★★	↑	DOWNAD 蠕虫关联木马
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	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
4	TROJ_IFRAME.CP	木马	★★★	→	GIF、jpg 和 SWF 文件中被插入一个恶意的 iframe 标记时，趋势科技会将其判断为 TROJ_IFRAME.CP 病毒。当这些文件被执行时，会重定向到这些 URL，并下载恶意程序
5	Cryp_Xed-12	木马	★★	↑	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	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	HTML_IFRAME.AZ	网页病毒	★★	↑	网页病毒,通常在网页在插入一个恶意 iframe,用户在访问该网页时会下载恶意文件或重定向到恶意网站
8	PAK_Generic.001	木马	★★★	↑	疑似病毒
9	CRCK_KEYGEN	网页病毒	★★	↑	非法破解程序
10	TROJ_SPNR.0BFE11	木马	★★	↑	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



本周安全趋势分析

趋势科技热门病毒综述-- TROJ_FAKEAV.HKZ

病毒描述：

网络罪犯利用苹果公司即将推出的 iCloud 云服务来欺骗用户下载恶意软件。他们利用黑帽子搜索引擎优化，使关键词“iCloud”的搜索结果带有病毒。如此导致用户被引导至恶意链接，通过这些链接可以下载虚假的杀毒软件。

该木马可能会以一个特定名称的虚假反病毒软件为名义将自己安装在受感染的系统上。它会显示一个用户图形界面，并在扫描后显示一个警告。它还会提示用户购买一个完整版本。如果用户决定购买该虚假产品，就会弹出一个窗口询问敏感信息，诸如信用卡号码的信息。

该木马通过用户访问恶意网站并在不经意间下载恶意软件，从而释放出木马来到达用户系统。它在每一个系统开始菜单中加入注册入口来使自身自启动。它用添加特定注册表入口来控制注册表中 shell 这一项。 这样使恶意软件在其它应用程序打开时会被执行。它还会盗取系统和/或用户的特定信息。

该木马会显示警告用户计算机受感染的虚假信息。它还会显示虚假的受感染系统的扫描结果。 当扫描结束时它还会询问客户是否购买。如果用户决定购买欺骗性商品，用户会被定向至一个特定网站，询问敏感信息，比如信用卡号码。它会在执行后将自身删除。

- 对该病毒的防护可以从以下连接下载最新版本的病毒码：8.299.00 或以上版本
  http://support.trendmicro.com.cn/Anti-Virus/Main-Pattern/

- 病毒详细信息请查询：
  http://about-threats.trendmicro.com/Malware.aspx?language=us&name=TROJ_FAKEAV.HKZ