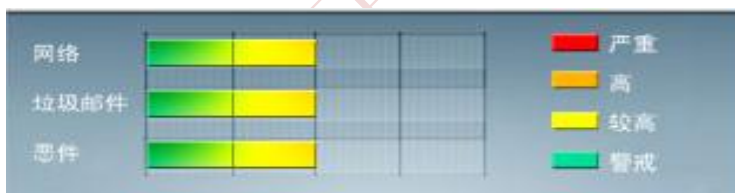




安全威胁每周警讯

2013/06/30~2013/07/07

本周威胁指数



TrendMicro 中国区网络安全监控中心



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



ANTIVIRUS



ANTI-PHISHING



WEB FILTERING



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.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	TROJ_DOWNAD.INF	木马	★★★★	↑	DOWNAD 蠕虫关联木马
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	WORM_ECODE.E-CN	蠕虫	★★★★★	↑	E 语言病毒, 产生与当前文件夹同名 exe 文件
5	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
6	X97M_OLEMALA	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
7	X97M_LAROUX.CO	宏病毒	★★	↑	Office 宏病毒, 由其他恶意软件或访问恶意网站感染
8	WORM_ECODE.B-CN	蠕虫	★★★★★	↑	E 语言病毒, 产生与当前文件夹同名 exe 文件
9	WORM_MICROFAKE.A	蠕虫	★★★★★	↑	蠕虫病毒, 通过访问 Internet 下载, 病毒会复制自身到电脑上的所有驱动器中。感染该病毒后, 远端恶意攻击者可以发送指令给该病毒用来收集和发送可用的信息给攻击者。
10	ACM_AGENT.A VGL	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。



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



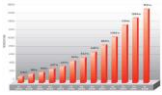
ANTIVIRUS



ANTI-PHISHING



WEB FILTERING



本周安全趋势分析

趋势科技热门病毒综述-- TROJ_DIDKR.A

病毒描述: 这个恶意软件与韩国某个安全事件有关，一些政府网站和新闻站点受到影响。黑客修改了这款软件的安装程序，为了让用户中毒，它还破坏了这个软件的自动更新机制。这是一个被修改的 SimDisk 文件共享软件，它被当作更新包下载到系统。软件被执行后，会下载一些其他组件，其中包括一个 Tor 客户端，一个配置文件，一个连接到 Tor 网络的文件，这个恶意软件利用 Tor 来隐藏自己的行为。

感染途径:

- 通过由其它病毒释放
- 用户浏览恶意网站时不经意间下载而抵达系统。

- ▶ 对该病毒的防护可以下载更新趋势最新病毒码：10.118.60 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://about-threats.trendmicro.com/us/malware/TROJ_DIDKR.A



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



ANTIVIRUS



ANTI-PHISHING



WEB FILTERING