安全威胁每周警讯

2013/01/06～2013/01/12

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	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	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
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_LAROUX.CO	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
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	HTML_IFRAME.CBE	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
9	WORM_ECODE.E-CN	蠕虫	★★	↑	该蠕虫在可移动驱动器中植入自身的副本。这些植入副本将所述驱动器或中的文件夹名称用作自己的文件名。它植入 AUTORUN.INF 文件，当用户访问受感染系统的驱动器时，自动执行植入的副本。
10	HTML_IFRAME.LCA	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

本周安全趋势分析

趋势科技热门病毒综述- TROJ_REVETON.IT

感染途径：由其它恶意软件释放，从因特网下载

这个是一个伪装成警方的勒索软件，并且锁定受感染的机器，显示一些所谓的反病毒公司条约，从而迫使用户支付费用。

该恶意软件是在用户访问恶意网站时不经意间下载而抵达系统的。

此恶意软件会与站点收发信息

- 对该病毒的防护可以从以下连接下载最新版本的病毒码：9.609.00

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_REVETON.IT