安全威胁每周警讯

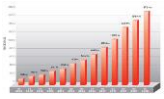
2013/05/12～2013/05/18

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	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。
5	CRCK_KEYGEN	破解程序	★★	↑	软件破解程序
6	Cryp_Xed-12	加壳程序	★★	↑	被加密过的程序
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	TROJ_UPACK.A-CN	木马病毒	★★★	↓	木马病毒，通过浏览恶意网站感染。
9	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。
10	HTML_IFRAME.AZ	网页病毒	★★	↑	网页病毒通常隐藏在网站页面中,将浏览者导向钓鱼网站或者暗中下载恶意程序



本周安全趋势分析

趋势科技热门病毒综述 - BKDR_POISON.MEA

感染途径：通过垃圾邮件 或由其他恶意软件释放。

恶意脚本会从美国劳工部下载这个后门文件。

该恶意软件通过由其它病毒释放或当用户浏览恶意网站时不经意间下载而抵达系统。

它连接到某些站点，用于发送接收信息。

- 对该病毒的防护可以从以下连接下载最新版本的病毒码：9.891.00

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/BKDR_POISON.MEA

安全风险漏洞

MS13-027：内核模式驱动程序中的漏洞可能允许特权提升 (2807986)

受影响的系统：

Windows XP Service Pack 3
Windows XP Professional x64 Edition Service Pack 2
Windows Server 2003 Service Pack 2
Windows Server 2003 x64 Edition Service Pack 2
Windows Server 2003 SP2（用于基于 Itanium 的系统）
Windows Vista Service Pack 2
Windows Vista x64 Edition Service Pack 2
Windows Server 2008（用于 32 位系统）Service Pack 2
Windows Server 2008（用于基于 x64 的系统）Service Pack 2
Windows Server 2008（用于基于 Itanium 的系统）Service Pack 2
Windows 7（用于 32 位系统）
Windows 7（用于 32 位系统）Service Pack 1
Windows 7（用于基于 x64 的系统）
Windows 7（用于基于 x64 的系统）Service Pack 1
Windows Server 2008 R2（用于基于 x64 的系统）
Windows Server 2008 R2（用于基于 x64 的系统）Service Pack 1
Windows Server 2008 R2（用于基于 Itanium 的系统）
Windows Server 2008 R2（用于基于 Itanium 的系统）Service Pack 1
Windows 8（用于 32 位系统）
Windows 8（用于 64 位系统）
Windows Server 2012
Windows Server 2008 R2（用于基于 x64 的系统）（服务器核心安装）
Windows Server 2008 R2（用于基于 x64 的系统）Service Pack 1（服务器核心安装）
Windows Server 2012（服务器核心安装）

描述：http://technet.microsoft.com/zh-cn/security/bulletin/MS13-027