安全威胁每周警讯

2012/01/29～2012/02/04

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	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	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	JS_AGENT.BBCK	脚本病毒	★★	↓	该程序为 Java 脚本病毒，通常是用户访问恶意网站是所感染的。
7	CRCK_KEYGEN	破解程序	★★	↑	非法破解程序
8	Adware_Adplus	灰色软件	★★	↑	广告软件，常见行为如在 Internet Explorer 和 Mozilla 的 Web 浏览器上显示广告横幅。虽然没有将此归类为恶意软件，但是此类广告软件通常会对系统造成不良影响，如弹出式广告、影响网络连接速度或降低系统性能等。
9	Downloader_Agent	灰色软件	★★	↑	这灰色软件下载器会自动下载并安装额外的其他的灰色软件，如广告软件和间谍软件。
10	WORM_ECODE.E-CN	蠕虫	★★★★	↓	E 语言病毒,产生与当前文件夹同名 exe 文件

系统漏洞信息

MS12-003 ： Windows 客户端/服务器运行时子系统中的漏洞可能允许特权提升 (2646524)

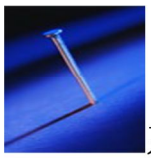
Windows XP

Windows Server 2003

Windows Vista

Windows Server 2008

描述： http://technet.microsoft.com/zh-cn/security/bulletin/MS12-003



系统安全技巧

一：预防

1.在员工进入公司时进行相关信息安全的教育，使其认识到信息安全的重要性，以及可能带来的危害；

2.对公司的老员工进行在教育，进一步明确安全方面的知识，并且定期将其他公司由于员工不遵守安全规则而导致的危害进行通报；

3.坚持每天查看服务器上的安全日志以及杀毒软件的管理端，遇到问题即时处理上报；

4.屏蔽掉相关的与工作无关的网站；

5.适当的屏蔽掉 USB 端口，控制 USB 在公司的使用；

6.对确实要用到 USB 的部门配发专门的存储设备。

二：处理

1.在发现病毒时及时进行上报；

2.确认病毒的性质：传播与不传播以及病毒的危害性；

3.追查源并进行相关的处理。

三：总结

定期对公司的信息教育以及病毒发生情况进行总结，进行想关方面适当的调整，积极反思相关病毒的防止对策以及处理过程的总结并进行改进。

这是我们公司在防毒方面的一些经验，希望您给予指正，我们将会积极的采纳您的建议并进行更正。

在视频中追根溯源还是防病毒软件的使用在同事的工作中没有引起其足够的重视，一下是我的一点防止发法：

1.安装服务器版的杀软，在终端电脑上安装客户端，这样就可以实时进行监控与更新并进行杀毒；

2.让公司的网络处于内网运行，对有特殊需求的部门开放相关的端口；

3.禁掉 USB，防止木马与病毒通过 USB 进入公司；

4.对于在公司存取资料的 USB 必须经过 IT 部门进行查杀并进行资料的存取；

5.对发现的病毒给相关部门负责人进行通报进行及时的沟通。

来源：51CTO