安全威胁每周警讯

2012/05/27～2012/06/02

本周威胁指数

***TrendMicro* 中国区网络安全监控中心**

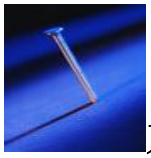
前十大病毒警讯

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。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	疑似病毒	★★★	→	疑似木马病毒，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	X97M_LAROUX.BK	宏病毒	★★	→	宏病毒，主要通过用户浏览恶意网站感染，该病毒主要感染 Office Excel 文件，并且会在 Excel 中创建一个名为 StartUp 的宏脚本
7	CRCK_KEYGEN	黑客程序	★★	↑	非法破解程序
8	PAK_Generic.001	加壳文件	★★	↑	经过加壳技术加密的文件
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	X97M_LAROUX.CO	宏病毒	★★	↑	这个宏病毒通常会在 Microsoft Excel 的启动目录中释放一个名称为 STARTUP.XLS 的文件。这个宏病毒还截获了两个 Microsoft Excel 的功能按钮，即 F8 和 F11。当使用者按这些按钮时将执行恶意的宏脚本。

系统漏洞信息

MS12-020 ：远程桌面中的漏洞可能允许远程执行代码 (2671387)

Windows XP
Windows Vista
Windows 7
Windows Server 2003
Windows Server 2008
描述：http://technet.microsoft.com/zh-cn/security/bulletin/MS12-020



系统安全技巧

社交网络已经成为首选的沟通渠道。虽然一些企业最初抵制在工作时使用社交网络，但是，许多企业现在认为，使用社交网络对于业务工作有益。他们理解企业社交媒体工具能够推动同事之间的协作和改善沟通。公共社交网络网站也许能够帮助机构吸引客户和员工、改善客户服务和管理自己的形象。

然而，社交网络与生俱来的风险对于企业来说是很糟糕的。

主要的风险是：社交网络很容易引起恶意软件攻击。其它威胁包括网络突破、知识产权盗窃、泄露企业敏感的商业信息以及劫持网站和社交媒体账户等。

控制这些威胁需要一个安全战略，制定利用监视和保护企业网络的技术来管理社交媒体使用的政策。通过全面地和持续不断地培训员工以可以接受的方式使用社交网络来加强政策和技术是非常重要的。

制定社交媒体安全战略的第一步是对商务数据分类。这样，员工就可以准确地理解什么是敏感的信息，什么不是敏感的信息。这个过程还应该具体说明谁有权访问企业内容以及这种信息可以如何使用。

政策对于每个员工和每个社交媒体网站都有所不同。例如，一位员工可以在商业媒体网站的公共配置中包含员工的隶属关系和工作职务，但是不能在个人网站披露这些信息。人力资源部门的员工可以提供更多的公司信息，因为这样做对于招聘人员非常重要。

要记住，黑客现在把目标对准了智能手机和平板电脑等移动设备。企业应该具体规定是否允许员工用这些设备访问社交网络网站以及允许哪一种应用程序访问社交网络网站。

一旦制定了政策，把网络监视技术和数据保护技术结合来增强这些政策也许是必要的。在某些情况下，这些技术也许已经作为标准的 IT 安全措施在使用。如果是如此，应该设置这些技术包含社交网络控制。

改变员工行为的挑战

使用社交网络，即使认真规划的政策和技术组合也许也不能完全奏效。那是因为你不能阻止员工在晚上回家之后在社交媒体上发布数据;人们不顾企业的政策想做什么就做什么。你能做什么?实施一个严格的和持续不断的员工教育计划，教育员工以可以接受的方式使用社交网络。

一个企业应该预先培训员工，明确说明如何正确地使用公司信息。一定要具体：告诉员工他们在社交网络上对于本公司能够说什么和不能说什么。员工应该理解发布企业数据是绝对禁止的，除非企业鼓励这样做。

针对员工的安全知识水平采取有针对性的教育计划。应该用非常真实的情况解释恶意软件的风险、数据损失和其它威胁对于企业和个人的影响。向员工介绍如何识别社交媒体攻击中使用的诈骗手段和如果识别钓鱼网站。培训应该展示这些威胁是如何在社交媒体上传播的以及这些威胁是如何下载到用户计算机或移动设备上，然后渗透到企业网络的。要强调这个知识在家里和在工作场所都同样有用。

然而，教育不能排除技术教育。对于许多员工来说，通过社交网络共享已经成为一种条件反射式的事情，他们也许不会意识到无意间在社交网络上发布的消息能够损害一家企业。员工还应该理解，当他们把自己当作一家公司的员工的时候，他们在数字领域正在代表这个公司。

最后，全面解释在使用社交媒体时不遵守公司政策的后果。要非常明确地指出：违反隐私、客户保密和知识产权等公司行为准则的人需要承担风险。

来源：51CTO