安全威胁每周警讯

2012/09/09～2012/09/15

本周威胁指数

***TrendMicro* 中国区网络安全监控中心**

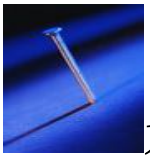
前十大病毒警讯

排名	病毒名称	威胁类型	风险等级	趋势	病毒行为描述
1	TROJ_DOWNAD.INF	木马	★★★	→	DOWNAD 蠕虫关联木马
2	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
3	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
4	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
5	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
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	WORM_ECODE.E-CN	蠕虫	★★★★	↑	E 语言病毒,产生与当前文件夹同名 exe 文件
8	X97M_LAROUX.CO	脚本病毒	★★	↑	Office 宏病毒，由其他恶意软件或访问恶意网站感染
9	WORM_VB.DVP	蠕虫	★★	↑	蠕虫病毒，通过访问恶意站点下载感染。感染该病毒后会在每个盘符下生成 autorun.inf 文件已达到用户在访问磁盘时执行该病毒
10	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

系统漏洞信息

MS12-054 ： Windows 网络组件中的漏洞可能允许远程执行代码 (2733594)

Windows XP Service Pack 3
Windows Server 2003
Windows Vista
Windows Server 2008
Windows 7
Windows Server 2008 R2
描述：http://technet.microsoft.com/zh-cn/security/bulletin/MS12-054



系统安全技巧

需要注意的是，没有什么安全做法是绝对有效的。没有对邮件进行有效的安全保护将导致一个很危险的趋势。所以让我们来看一下，从这次事件中得到的启示，以及怎样才能保证邮件的安全。

1、密码

关于密码的话题我们已经谈过很多次了，密码使用的简单就像黑客容易打破一样，成正比，最重要的是人们应该由衷地引起注意。电子邮件的安全第一步必须从密码开始。设定一些觉得没人会猜对的简单的密码，却会导致一个企业都陷入麻烦。邮件账户必须有牢不可破的密码，这也意味着信息不会被盗取。

2、加密

确保邮件安全，加密是个不错的做法。加密与认证是分不开的，这就增加了人们读取数据所需要的时间，多数人认为加密是一个不会带来多少好处的做法。但是实际上，加密为用户提供了安全的多一层保护。如果电邮安全是重要的，那么加密就应该被采用。

3、不要泄露证书

用户在面对邮件安全的时候一个重要的问题就是他们对待证书的态度。与他人分享证书是没有任何好处的。一个想保证数据安全和隐私安全的人为什么要向他们泄露证书呢?分享证书却是导致信息泄露的罪魁祸首。

4、不要相信钓鱼邮件

有着不良企图的黑客意识到了向用户发送垃圾邮件有利可图，于是他们就疯狂地加大垃圾邮件的发送量。有一些邮件是来自银行的、信用卡公司或其他需要用户敏感信息的非法公司。用户始终都要认真对待钓

鱼邮件并牢记住一点，没有人有权获取这些私人信息，除非是绝对必要的情况。

5、认证的有效期

企业应该告诉员工，认证都是有有效期的。换言之，在 6 个月到一年的时间里使用同一个密码时间未免太长了。用户更换密码的频率越高，信息遭到泄露的风险就越小。

6、不要忽视任何一环的安全保护

在一个企业中，只要一个人没有保护好安全策略，整个企业的电子邮件、敏感客户信息和其他数据就可以轻易泄露出去。最重要的是，损失的不只是那个人自己。在安全这根盔甲中出现的一个小的漏洞，企业安全风险增加的几率就增加好几倍。

7、信任不能保证邮件安全

在电子邮件问题上，信任是没什么用的。你收到一封来自家人的邮件，然后立刻认为他发送的这封邮件也是安全的，这样做是不明智的。每一份打开的邮件和回复的邮件都应该做好真实性的审核。这不是一件容易的事情，但是，如果你盲目信息邮件的内容会很快招致麻烦却是一定的。

8、反恶意软件工具的作用

对于邮件用户来说，使用反恶意软件工具是很重要的。用户计算机出现了安全问题，很多不好的事情都可能接踵而至。有了反恶意软件工具的存在，你的邮件账户以及一些敏感信息就不会被不法分子“召回”到他们的服务器中。同样，反恶意软件不见得是万无一失的解决方案，但是却会起到一定的作用。

9、企业应部署邮件策略

对于企业来说，能有一个安全策略是很重要的事情。员工应该知道，什么是策略，他们应该把好最后一关。如果他们没有做好，就要被追究责任。如果企业没有执行好这一点，那么无论是邮件还是计算机的信息就都不保了。

10、做好最坏的准备

对于恶意企图的黑客来说，邮件是获取敏感信息的“要道”。有了灾难恢复计划的存在，企业和个人就会知道如何对这些事件做出应对。对邮件安全有了正确的理解以及有了渴望保护信息安全的意识，气候学家所面临的很多问题就迎刃而解了。我们需要的只是一个计划和一些时间。

来源：51CTO