安全威胁每周警讯

2012/09/23～2012/09/29

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

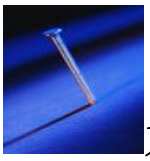
排名	病毒名称	威胁类型	风险等级	趋势
1	WORM_DOWNAD.AD	蠕虫	★★★★	↑
2	WORM_DOWNAD	蠕虫	★★★★	↑
3	TROJ_DOWNAD.INF	木马	★★★	↓
4	X97M_OLEMAL.A	宏病毒	★★	→
5	TROJ_IFRAME.CP	木马	★★★	↓
6	TROJ_SPNR.15IH12	木马	★★★	↑
7	X97M_LAROUX.BK	宏病毒	★★	→
8	X97M_LAROUX.CO	宏病毒	★★	→
9	WORM_ECODE.E-CN	蠕虫	★★★★	↓
10	HTML_IFRAME.AZ	网页病毒	★★★	↑

系统漏洞信息

MS12-055 ： Windows 内核模式驱动程序中的漏洞可能允许特权提升 (2731847)

Windows XP
Windows Vista
Windows 7
Windows Server 2003
Windows Server 2008
Windows Server 2008 R2

描述： http://technet.microsoft.com/zh-cn/security/bulletin/MS12-055



系统安全技巧

1. 安装安全策略

（1） 不要选择从网络上安装虽然微软支持在线安装，但这绝对不安全。在系统未全部安装完之前不要连入网络，特别是 Internet。甚至不要把一切硬件都连接好来再安装。因为 Windows XP 安装时，在输入用户管理员账号“Administrator”的密码后，系统会建立一个“ADMIN”的共享账号，但是并没有用刚输入的密码来保护它，这种情况一直会持续到计算机再次启动。在此期间，任何人都可以通过“ADMIN”进入系统；同时，安装完成，各种服务会马上自动运行，而这时的服务器还到处是漏洞，非常容易从外部侵入。

（2） 要选择 NTFS 格式来分区最好所有的分区都是 NTFS 格式，因为 NTFS 格式的分区在安全性方面更加有保障。就算其他分区采用别的格式(如 FAT32)，但至少系统所在的分区中应是 NTFS 格式。另外，应用程序不要和系统放在同一个分区中，以免攻击者利用应用程序的漏洞(如微软的 IIS 的漏洞)导致系统文件的泄漏，甚至让入侵者远程获取管理员权限。

（3） 系统版本的选择版本的选择：Windows XP 有各种语言的版本，对于我们来说，可以选择英文版或简体中文版，我强烈建议：在语言不成为障碍的情况下，请一定使用英文版。要知道，微软的产品是以 Bug&Patch 而著称的，中文版的 Bug 远远多于英文版，而补丁一般还会迟至少半个月（也就是说一般微软公布了漏洞后你的机子还会有半个月处于无保护状况）。

（4） 组件的定制 Windows XP 在默认情况下会安装一些常用的组件，但是正是这个默认安装是很危险的，你应该确切的知道你需要哪些服务，而且仅仅安装你确实需要的服务，根据安全原则，最少的服务+最小的权限=最大的安全。

（5） 分区和逻辑盘的分配建议建立多于两个分区，一个系统分区，一个以上应用程序分区，把系统分

区和应用程序分区分开，以此来保护应用程序，一般来说，病毒或者黑客利用漏洞攻击，损坏的是系统分区，而不会对应用程序分区造成损坏。

2．账号安全策略

（1）用户安全设置检查用户账号，停止不需要的账号，建议更改默认的账号名。

1)、禁用 Guest 账号在计算机管理的用户里面把 Guest 账号禁用。为了保险起见，最好给 Guest 加一个复杂的密码。

2)、限制不必要的用户 去掉所有的 Duplicate User 用户、测试用户、共享用户等等。用户组策略设置相应权限，并且经常检查系统的用户，删除已经不再使用的用户。

3)、创建两个管理员账号创建一个一般权限用户用来收信以及处理一些日常事物，另一个拥有 Administrator 权限的用户只在需要的时候使用。

4)、把系统 Administrator 账号改名 Windows XP 的 Administrator 用户是不能被停用的，这意味着别人可以一遍又一遍地尝试这个用户的密码。尽量把它伪装成普通用户，比如改成 Guesycludx。

5)、创建一个陷阱用户创建一个名为“Administrator”的本地用户，把它的权限设置成最低，什么事也干不了的那种，并且加上一个超过 10 位的超级复杂密码。

6)、把共享文件的权限从 Everyone 组改成授权用户 不要把共享文件的用户设置成“Everyone”组，包括打印共享，默认的属性就是“Everyone”组的。

7)、不让系统显示上次登录的用户名 打开注册表编辑器并找到注册表项 HKLMSoftwaremicrosoftWindowsTCurrentVersionWinlogonDont-DisplayLastUserName，把键值改成 1。

8)、系统账号/共享列表 Windows XP 的默认安装允许任何用户通过空用户得到系统所有账号/共享列表，这个本来是为了方便局域网用户共享文件的，但是一个远程用户也可以得到你的用户列表并使用暴力法破解用户密码。可以通过更改注册表 Local_MachineSystemCurrentControlSetControlLSA-RestrictAnonymous = 1 来禁止 139 空连接，还可以在 Windows XP 的本地安全策略（如果是域服务器就是在域服务器安全和域安全策略中）就有这样的选项 RestrictAnonymous（匿名连接的额外限制）。

3.应用安全策略

（1）安装杀毒软件杀毒软件不仅能杀掉一些著名的病毒，还能查杀大量木马和后门程序，因此要注意经常运行程序并升级病毒库。

（2）安装防火墙侦听外界对本机所采取的攻击，及早提醒用户采取防范措施。

（3）安装系统补丁到微软网站下载最新的补丁程序：经常访问微软和一些安全站点，下载最新的 Service Pack 和漏洞补丁，是保障服务器长久安全的唯一方法。

（4）停止不必要的服务服务开的太多也不是个好事，将没有必要的服务通通关掉吧！服务组件安装得越多， 用户可以享受的服务功能也就越多。但是用户平时使用到的服务组件毕竟有限， 而那些很少用到的组件除占用了不少系统资源，会引起系统不稳定外，还为黑客的远程入侵提供了多种途径。

为此我们应该尽量把那些暂不需要的服务组件屏蔽掉。具体的操作方法为： 首先在控制面板中找到“管理工具”/“服务”，然后再打开“服务”对话框，在该对话框中选中需要屏蔽的程序，并单击鼠标右键， 从弹出的快捷菜单中依次选择“属性”/“停止”命令，同时将“启动类型”设置为“手动”或“已禁用”，这样就可以对指定的服务组件进行屏蔽了。

4．网络安全策略

（1）关闭不必要的端口

关闭端口意味着减少功能，在安全和功能上面需要你做一点决策。如果服务器安装在防火墙的后面，冒险就会少些。但是，永远不要认为你可以高枕无忧了。用端口扫描器扫描系统已开放的端口，确定系统开放的哪些服务可能引起黑客入侵。在系统目录中的 system32/drivers/etc/services 文件中有知名端口和服务的对照表可供参考。具体方法为：打开“ 网上邻居/属性/本地连接/属性/internet 协议(TCP/IP)/属性/高级/选项/TCP/IP 筛选/属性” 打开“TCP/IP 筛选”，添加需要的 TCP、UDP 协议即可。

（2）设置好安全记录的访问权限

安全记录在默认情况下是没有保护的，把它设置成只有 Administrators 和系统账户才有权访问。

（3）使用 Web 格式的电子邮件系统

不要实用 Outlook、Fox mail 等客户端邮件系统接受邮件，现在的一些邮件危害性很大，一旦植入本机，就有可能造成系统的瘫痪。同时，不要察看陌生人邮件中的附件，这些附件往往带有病毒和木马。

来源：eNet