安全威胁每周警讯

2011/03/27～2011/04/02

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	TROJ_DOWNAD.INF	木马	★★★	→	DOWNAD 蠕虫关联木马
2	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
3	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
4	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
5	Cryp_Xed-12	木马	★★★	↑	疑似病毒
6	TROJ_SPNR.03CG11	木马	★★	↓	该木马程序是一个恶意软件，但危险低，不具备自动传播到其他系统的能力。它通常是从网上下载，并在用户不知情的情况下自动安装。 通常携带有效载荷木马或其他恶意行为，可从轻度恼人的范围到无可挽回的破坏。他们也可以修改系统设置为自动启动。
7	Dialer_Win32Dial	拨号软件	★★★	↑	这是个拨号器文件/组件。它尝试修改的 Internet Explorer（IE）的主页，直接影响用户浏览网站。
8	TROJ_SPNR.03CL11	木马	★★	↑	该木马程序是一个恶意软件，但危险低，不具备自动传播到其他系统的能力。它通常是从网上下载，并在用户不知情的情况下自动安装。
9	WORM_ECODE.E-CN	蠕虫	★★★★	↓	E 语言病毒,产生与当前文件夹同名 exe 文件
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

1.1. MS11-017：远程桌面客户端中的漏洞可能允许远程执行代码

受影响的软件：

Windows XP ,Windows Server 2003

Windows Vista ,Windows Server 2008

Windows 7

描述： http://www.microsoft.com/china/technet/security/bulletin/MS11-017.mspx

系统安全技巧

在规模稍微大一些的局域网工作环境中，网络管理员时常会采用远程控制方式来管理服务器或重要工作主机；虽然这种控制方式可以提高网络管理效率，但是远程控制方式带来的安全威胁往往也容易被管理人员忽视。为了保障服务器远程控制操作的安全性，Windows Server 2008 系统特意在这方面进行了强化，新推出了许多安全防范功能，不过有的功能在默认状态下并没有启用，这需要我们自行动手，对该系统进行合适设置，才能保证远程控制 Windows Server 2008 服务器系统的安全性。

1、只允许指定人员进行远程控制

如果允许任何一位普通用户随意对 Windows Server 2008 服务器系统进行远程控制时，那该服务器系统的安全性肯定很难得到有效保证。有鉴于此，我们可以对 Windows Server 2008 服务器系统进行合适设置，只允许指定人员通过远程桌面连接方式对其进行远程控制，下面就是具体的设置步骤：

首先打开 Windows Server 2008 服务器系统桌面的“开始”菜单，从中依次展开“程序”、“管理工具”、“服务器管理器”选项，在其后出现的对应系统服务器管理器控制台窗口中，点选左侧子窗格中的“服务器管理”节点选项，之后选中目标节点分支下面的“服务器摘要”设置项，再单击“配置远程桌面”项目，进入远程控制 Windows Server 2008 系统的设置对话框；

其次在该设置对话框的“远程桌面”处单击“选择用户”按钮，打开如图 1 所示的设置界面，从中我们会看到可以对 Windows Server 2008 服务器系统进行远程控制的所有用户账号，一旦看到有陌生的用户账号或不信任用户账号存在时，我们可以将它选中并单击“删除”按钮，将它从系统中删除掉；接着单击对应设置界面中的“添加”按钮，打开用户账号设置对话框，从中将指定的管理员用户账号选中并添加进来，再单击“确定”按钮结束用户账号设置操作，如此一来 Windows Server 2008 服务器系统日后只允许指定的系统管理员对其进行远程管理操作，而不允许其

他任何用户对其进行远程控制操作。

2、拒绝 Administrator 进行攻击测试

与传统服务器操作系统一样，Windows Server 2008 服务器系统在默认状态下仍然会使用 Administrator 账号来完成系统登录操作，正因如此 Administrator 账号特别容易被一些非法攻击者利用，他们企图通过破解 Administrator 账号的密码来登录服务器，并尝试对其进行攻击测试。为了拒绝非法攻击者使用 Administrator 账号进行攻击测试，我们可以按照如下步骤设置 Windows Server 2008 服务器系统：

首先在 Windows Server 2008 服务器系统桌面中依次单击“开始”/“运行”命令，在弹出的系统运行文本框中，输入“Secpol.msc”字符串命令，单击回车键后，打开对应系统的本地安全组策略控制台窗口；

其次在本地安全组策略控制台窗口的左侧显示区域，将鼠标定位于其中的“安全设置”节点选项，在目标节点分支下面选中“本地策略”/“安全选项”，在对应“安全选项”分支下面找到目标安全组策略“帐户：重命名系统管理员帐户”，并用鼠标右键单击该组策略选项，从其后出现的快捷菜单中执行“属性”命令，打开“帐户：重命名系统管理员帐户”组策略属性设置对话框；单击该对话框中的“本地安全设置”标签，打开如图 2 所示的标签设置页面，在该页面中我们可以将 Administrator 账号的名称修改为其他人不容易猜中的名称，例如可以将其修改为“guanliyuan”，最后单击“确定”按钮保存好上述设置操作，这样一来非法攻击者企图通过 Administrator 账号对 Windows Server 2008 服务器系统进行攻击测试时，就无法取得成功，那么服务器系统的安全性能就可以得到有效保证了。

3、修改 telnet 端口保护远程连接安全

telnet 命令是 Windows Server 2008 服务器系统中缺省的远程登录程序，因为该程序是直接集成在服务器系统中并且使用起来比较方便，所以网络管理员在管理服务器时经常使用到该程序。不过，在使用 telnet 命令对服务器系统进行远程控制操作时，控制信息往往是以明文方式在网络上传输的，一些恶意攻击者很容易就能将类似账号名称和密码这样的控制信息截获走，同时 telnet 程序的身份验证方式也存在明显的弱点，那就是它特别容易受到其他人的攻击。考虑到 telnet 命令对 Windows Server 2008 服务器系统进行远程控制时，一般会自动使用“23”这个默认的网络端口，并且该端口几乎被所有人都熟悉，为了保护 telnet 远程连接的安全性，我们只要按照下面的方法修改该程序默认的网络端口号码，以阻止其他人随意使用 telnet 命令对服务器系统进行远程控制操作：

首先在 Windows Server 2008 服务器系统桌面中依次单击“开始”/“运行”命令，在弹出的系统运行文本框中，输入“cmd”字符串命令，单击回车键后，打开对应系统的 DOS 命令行工作窗口；

其次在 DOS 窗口的命令行提示符下，输入字符串命令“tlntadmn config port=2991”(其中“2991”是修改后的新端口号码），为了防止新设置的网络端口号码与系统已有端口号码存在冲突，我们必须确保这里输入的新端口号码不能设置成已知系统服务的端口号码；在确认上面的字符串命令输入正确后，单击回车键，telnet 命令使用的端口号码就会自动变成“2991”了，此时网络管理员必须知道新端口号码，才能使用该程序对 Windows Server 2008 服务器

系统进行远程控制操作。

当然，我们不到服务器现场，也能远程修改 Windows Server 2008 服务器系统的 telnet 程序端口号码，我们只要在本地客户端系统打开 DOS 命令行工作窗口，在该窗口的命令行提示符下输入字符串命令“tlntadmn config server port=2991 -u xxx -p yyy ”(Server 表示远程服务器系统的主机名称或 IP 地址，port=2991 要修改为的远程登录端口号码，xxx 为登录服务器系统的用户名，yyy 是对应用户账号的密码，单击回车键后，远程服务器系统的 telnet 端口号码就变成“2991”了。

4、强行使用复杂密码阻止暴力破解

要是 Windows Server 2008 服务器系统的远程登录密码设置得不够复杂时，那么非法远程控制用户就有可能通过暴力方式将该登录密码成功破解掉。而事实上，不少网络管理员为了便于记忆，常常会将服务器系统的远程登录密码设置得比较简单，这无形之中给非法攻击者提供了暴力破解的机会，远程控制操作的安全性也会受到严重威胁。为此，我们可只要对 Windows Server 2008 服务器系统进行如下设置操作，来启用系统自带的密码策略，强制用户必须对远程控制账号设置比较复杂的密码：

首先在 Windows Server 2008 服务器系统桌面中依次单击“开始”/“程序”/“管理工具”命令，在其后出现的系统管理工具列表窗口中，用鼠标双击其中的“本地安全策略”图标，打开对应系统的本地安全设置对话框；

其次在该设置对话框的左侧显示区域，用鼠标选中其中的“账户策略”分支选项，然后再将目标分支选项下面的“密码策略”子项选中，在对应“密码策略”子项的右侧显示区域，我们会看到六个有关密码的设置策略选项，用鼠标双击其中的“密码必须符合复杂性要求”组策略选项，打开如图 3 所示的目标组策略属性设置窗口；

检查其中的“已启用”选项是否处于选中状态，要是发现该选项还没有被选中时，我们应该及时将它重新选中，再单击“确定”按钮保存好上述设置操作，如此一来 Windows Server 2008 服务器系统的远程登录密码设置得不够复杂时，系统就会自动弹出相关提示；

接下来，我们再对“强制密码历史”、“密码长度最小值”、“用可还原的加密来储存密码”、“密码最长使用期限”、“密码最短使用期限”等策略进行按需修改，最后单击“确定”按钮完成所有设置操作，如此一来远程登录密码就能被强行设置得复杂了。

来源： 51CTO