安全威胁每周警讯

2011/07/30～2011/08/06

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

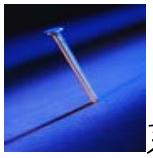
排名	病毒名称	威胁类型	风险等级	趋势	病毒行为描述
1	TROJ_DOWNAD.INF	木马	★★★	→	DOWNAD 蠕虫关联木马
2	WORM_DOWNAD.AD	蠕虫	★★★★	→	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
3	TROJ_IFRAME.CP	木马	★★★	↑	GIF、jpg 和 SWF 文件中被插入一个恶意的 iframe 标记时，趋势科技会将其判断为 TROJ_IFRAME.CP 病毒。当这些文件被执行时，会重定向到这些 URL，并下载恶意程序
4	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	WORM_ECODE.E-CN	蠕虫	★★★★	↑	E 语言病毒,产生与当前文件夹同名 exe 文件
6	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
7	JS_EXPLOIT.SMAD	脚本病毒	★★	↑	该脚本病毒通过浏览网页被下载，当用户访问该站点时还有可能会感染名为 SWF_EXPLOIT.JE 的病毒
8	ACM_AGENT.AVGL	脚本病毒	★★	↑	AutoCad 脚本病毒
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	TROJ_LAMEWAR.VTG	木马	★★	↑	该木马病毒嵌套在一些广告/灰色/共享软件中，用户在安装这些软件的时候会被执行

系统漏洞信息

1.1. MS11-054：Windows 内核模式驱动程序中的漏洞可能允许特权提升

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

描述：http://www.microsoft.com/china/technet/security/bulletin/MS11-054.mspx



系统安全技巧

你的服务器上是否存有一些不能随意公开的重要数据呢?当然有吧?而最近，偏偏服务器遭受的风险又特别大，越来越多的病毒、心怀不轨的黑客，以及那些商业间谍都将服务器当作目标。很显然，服务器的安全问题一刻都忽视不得。

不可能在一篇文章中谈遍电脑安全问题，毕竟，市面上的已有许多这方面的书籍，不过，我倒是可以告诉你七个维护服务器安全的技巧。

技巧一：从基本做起

从基本做起是最保险的方式。你必须将服务器上含有机密数据的区域通通转换成 NTFS 格式;同理，防毒程序也必须按时更新。建议同时在服务器和桌面电脑上安装防毒软件。这些软件还应该设定成每天自动下载最新的病毒定义文件。另外，Exchange Server(邮件服务器)也应该安装防毒软件，这类软件可扫描所有寄进来的电子邮件，寻找被病毒感染的附件，若发现病毒，邮件马上会被隔离，减低使用者被感染的机会。

另一个保护网络的好方法是依员工上班时间来限定使用者登录网络的权限。例如，上白天班的员工不该有权限在三更半夜登录网络。

最后，存取网络上的任何数据皆须通过密码登录。强迫大家在设定密码时，必须混用大小写字母、数字和特殊字符。在 Windows NT Server Resource Kit 里就有这样的工具软件。你还应该设定定期更新密码，且密码长度不得少于八个字符。若你已经做了这些措施，但还是担心密码不安全，你可以试试从网络下载一些黑客工具，然后测试一下这些密码到底有多安全。

技巧二：保护备份

大多数人都没有意识到，备份本身就是一个巨大的安全漏洞，怎么说呢?试想，大多数的备份工作多在晚上 10 点或 11 点开始，依数据多寡，备份完成后大概也是夜半时分了。现在，想像一下，现在是凌晨四点，

备份工作已经结束。有心人士正好可趁此时偷走备份磁盘，并在自己家中或是你竞争对手办公室里的服务器上恢复。不过，你可以阻止这种事情发生。首先，你可利用密码保护你的磁盘，若你的备份程序支持加密功能，你还可以将数据进行加密。其次，你可以将备份完成的时间定在你早上进办公室的时间，这样的话，即使有人半夜想溜进来偷走磁盘的话也无法了，因为磁盘正在使用中;如果窃贼强行把磁盘拿走，他一样无法读取那些损毁的数据。

技巧三：使用 RAS 的回拨功能

Windows NT 最酷的功能之一就是支持服务器远端存取(RAS)，不幸的是，RAS 服务器对黑客来说实在太方便了，他们只需要一个电话号码、一点耐心，然后就能通过 RAS 进入主机。不过你可以采取一些方法来保护 RAS 服务器的安全。

你所采用的技术主要端赖于远端存取者的工作方式。如果远端用户经常是从家里或是固定的地方上网，建议你使用回拨功能，它允许远端用户登录后即挂断，然后 RAS 服务器会拨出预设的电话号码接通用户，因为此一电话号码已经预先在程序中了，黑客也就没有机会指定服务器回拨的号码了。

另一个办法是限定远端用户只能存取单一服务器。你可以将用户经常使用到的数据复制到 RAS 服务器的一个特殊共用点上，再将远端用户的登录限制在一台服务器上，而非整个网络。如此一来，即使黑客入侵主机，他们也只能在单一机器上作怪，间接达到减少破坏的程度。

最后还有一个技巧就是在 RAS 服务器上使用“另类”网络协议。很都以 TCP/IP 协议当作 RAS 协议。利用 TCP/IP 协议本身的性质与接受程度，如此选择相当合理，但是 RAS 还支持 IPX/SPX 和 NetBEUI 协议，如果你使用 NetBEUI 当作 RAS 协议，黑客若一时不察铁定会被搞得晕头转向。

技巧四：考虑工作站的安全问题

在服务器安全的文章里提及工作站安全感觉似乎不太搭边，但是，工作站正是进入服务器的大门，加强工作站的安全能够提高整体网络的安全性。对于初学者，建议在所有工作站上使用 Windows 2000。Windows 2000 是一个非常安全的操作系统，如果你没有 Windows 2000，那至少使用 Windows NT。如此你便能将工作站锁定，若没有权限，一般人将很难取得网络配置信息。

另一个技巧是限制使用者只能从特定工作站登录。还有一招是将工作站当作简易型的终端机(dumb terminal)或者说，智慧型的简易终端机。换言之，工作站上不会存有任何数据或软件，当你将电脑当作 dumb terminal 使用时，服务器必须执行 Windows NT 终端服务程序，而且所有应用程序都只在服务器上运作，工作站只能被动接收并显示数据而已。这意味着工作站上只有安装最少的 Windows 版本，和一份微软 Terminal Server Client。这种方法应该是最安全的网络设计方案。

技巧五：执行最新修补程序

微软内部有一组人力专门检查并修补安全漏洞，这些修补程序(补丁)有时会被收集成 service pack(服务包)发布。服务包通常有两种不同版本：一个任何人都可以使用的 40 位的版本，另一个是只能在美国和加拿大发行的 128 位版本。128 位的版本使用 128 位的加密算法，比 40 位的版本要安全得多。

一个服务包有时得等上好几个月才发行一次，但要是有严重点的漏洞被发现，你当然希望立即进行修补，不想苦等姗姗来迟的服务包。好在你并不需要等待，微软会定期将重要的修补程序发布在它的 FTP 站上，这些最新修补程序都尚未收录到最新一版的服务包里，我建议你经常去看看最新修补程序，记住，修补程序

一定要按时间顺序来使用，若使用错乱的话，可能导致一些文件的版本错误，也可能造成 Windows 当机。

技巧六：颁布严格的安全政策

另一个提高安全性的方式就是制定一强有力的安全策略，确保每一个人都了解，并强制执行。若你使用 Windows 2000 Server，你可以将部分权限授权给特定代理人，而无须将全部的网管权利交出。即使你核定代理人某些权限，你依然可县制其权限大小，例如无法开设新的使用者帐号，或改变权限等。

技巧七：防火墙，检查，再检查

最后一个技巧是仔细检查防火墙的设置。防火墙是网络规划中很重要的一部份，因为它能使公司电脑不受外界恶意破坏。

首先，不要公布非必要的 IP 地址。你至少要有一个对外的 IP 地址，所有的网络通讯都必须经由此地址。如果你还有 DNS 注册的 Web 服务器或是电子邮件服务器，这些 IP 地址也要穿过防火墙对外公布。但是，工作站和其他服务器的 IP 地址则必须隐藏。

你还可以查看所有的通讯端口，确定不常用的已经全数关闭。例如，TCP/IP port 80 是用于 HTTP 流量，因此不能堵掉这个端口，也许 port 81 应该永远都用不着吧，所以就应该关掉。你可以在网络上查到每个端口的详细用途。

服务器安全问题是个大议题，你总不希望重要数据遭病毒/黑客损毁，或被人偷走做为不利你的用途，本文介绍了 7 个重要的安全检查关卡，你不妨试试看。

来源：51CTO