安全威胁每周警讯

2011/05/29～2011/06/04

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	TROJ_DOWNAD.INF	木马	★★★	↑	DOWNAD 蠕虫关联木马
3	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
4	Cryp_Xed-12	木马	★★★	↓	疑似病毒
5	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
6	TROJ_DLOADER.UVD	木马	★★★	↑	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
7	TROJ_VBKRYPT.CK	木马	★★★	↑	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
8	Expl_ShellCodeSM	木马	★★★	↑	疑似病毒
9	HEUR_OLEXP.A	木马	★★★	↑	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
10	WORM_ECODE.E-CN	蠕虫	★★★★	↓	E 语言病毒,产生与当前文件夹同名 exe 文件

系统漏洞信息

MS11-030：DNS 解析中的漏洞可能允许远程执行代码

受影响的软件及补丁链接：

Windows XP Service Pack 3

Windows XP Professional x64 Edition Service Pack 2

Windows Server 2003 Service Pack 2

Windows Server 2003 x64 Edition Service Pack 2

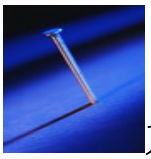
Windows Vista Service Pack 1 和 Windows Vista Service Pack 2

Windows Server 2008（用于 32 位系统）和 Windows Server 2008（用于 32 位系统）Service Pack 2

Windows 7（用于 32 位系统）和 Windows 7（用于 32 位系统）Service Pack 1

Windows Server 2008 R2（用于基于 x64 的系统）和 Windows Server 2008 R2（用于基于 x64 的系统）Service Pack 1

描述： http://www.microsoft.com/china/technet/security/bulletin/MS11-030.mspx



系统安全技巧

增强网络整体安全

很多网管往往在维护网络安全方面存在这样的误区，认为只要将服务器单机打好补丁，安装好防护墙、操作系统定期升级就可以安枕无忧了。可实际上，很多黑客和病毒并非直接攻击服务器，而是通过入侵其他计算机作为跳板来攻击整个网络的。目前很多网络都是通过域的方式来管理，一旦黑客或病毒成功入侵与服务器有信任关系的一台计算机，那么从这台计算机攻击服务器将会变得非常简单。所以要办证整个网络的安全要从根本来考虑。

首先是安全管理，要从管理角度出发，利用规章制度等文字性的材料规范，约束各种针对计算机网络的行为，例如禁止员工随便下载非法程序，禁止网络管理员以外的人员进入中心机房，完善网络管理员的值班制度等等。

其次是安全技术，要从技术角度出发，利用各种软件和硬件，各种技巧和方法来管理整个计算机网络，杀毒软件与防火墙双管齐下力保网络的安全。

这两方面缺一不可，试想如果只有安全技术的支持而在规章制度上没有进行任何约束，即使刚开始安全做的很到位，但员工随意下载非法软件，随便关闭杀毒软件的保护的话，整个网络安全形同虚设。而只有严格的规章没有技术作为支持的话病毒和黑客也会通过网络漏洞轻松入侵。因此安全管理与安全技术两方面相辅相成，网络管理员对于这两方面都要抓，力度都要硬。

加强服务器本地文件格式安全级别

目前服务器都采用的是windows 2000以上版本，所以在加强安全级别上需要利用windows 2000 server提供的

用户权限功能，根据每个用户的特点单独地为其制定访问服务器的特殊使用权限，从而避免因使用统一的访问服务器权限而带来的安全隐患。

为了确保服务器的安全首先要在本地文件格式上做文章,即将FAT格式转换为安全系数更高的NTFS文件格式。毕竟对于黑客来说存储在FAT格式的磁盘分区里的数据要比存储在NTFS格式的磁盘分区的数据更容易访问,也更容易破坏，另外目前所有安全软件及加密软件也都是针对NTFS格式来说的，对FAT格式的保护非常薄弱。

另外最好使用专门的网络检测软件对整个网络的运行情况进行7*24小时的不间断监视，尤其要关注“非法入侵”和“对服务器的操作”两方面的报告，笔者做在的公司就使用IISLOCK来监视网页服务器的正常运行和MRTG来检测整个网络的流量。

定期备份数据

数据的保护是一个非常重要的问题，也许服务器的系统没有崩溃但里面存储的数据发生了丢失，这种情况所造成的损失会更大，特别对于数据库服务器来说也许存储的是几年的珍贵数据。怎么才能有效的保护数据?备份是唯一的选择。以往对于数据的备份都是采取在服务器上另外一个区建立备份文件夹甚至是建立一个备份区。不过这样备份方法有一个非常大的弊端，那就是一旦服务器的硬盘出现问题所有分区的数据都将丢失，从而备份没有了保证。按照“不要把所有鸡蛋放到同一个篮子”的理论我们应该使用单独的专门设备保存这些珍贵数据。

使用B服务器保存A服务器的数据，同时用A服务器保存B服务器的文件，这种交叉备份的方法在一段时间非常流行。另外还有一个有效的方法就是使用磁带来保存珍贵数据，不过这样的投资会比较大。

就拿采用的备份方式来说，采用的备份方式是通过网络存储设备NAS来保存的，将单独的NAS设备连接到网络中，定期通过工具将珍贵数据写入到NAS的硬盘中，由于NAS设备自身使用了RAID方式进行数据的冗余，所以数据得到了最好的保证。

但是数据备份也存在巨大的安全漏洞，因为备份好的数据也有可能被盗窃，所以在备份时应该对备份介质进行有效的密码保护，必要时还需要使用加密软件对这些数据进行加密，这样即使数据被盗也不会出现数据泄露的问题。

来源：51CTO