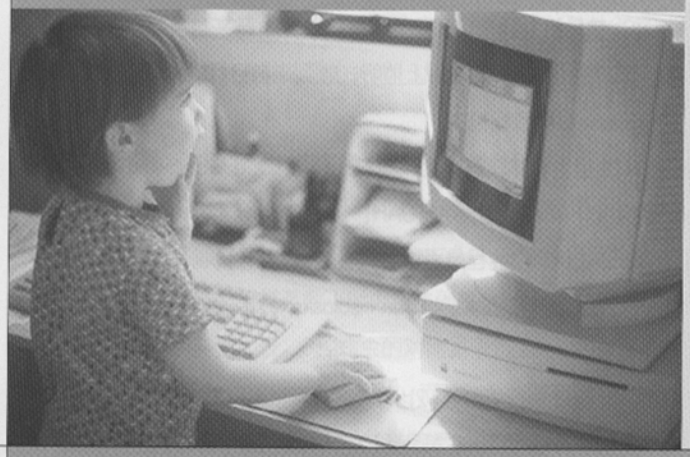
谭毓安 曹元大 (北京理工大学计算机科学与工程系 100081)



"冲击波"蠕虫的分析和防范

The Analysis and Defense of Blaster Worm

摘　要："冲击波"蠕虫利用Windows系统的RPC漏洞下载并执行蠕虫代码，并对发布补丁程序的微软网站进行拒绝服务攻击。蠕虫感染局域网和Internet上的其他Windows系统，使被攻击主机的RPC服务崩溃。本文讨论了其运行机制以及检测和清除方法。对近2年中的3种典型的蠕虫进行了对比，指出了消极防御措施的不足和采取主动式防御措施的必要性。

关键字：蠕虫　系统漏洞　Windows

2003年8月12日，一种新型的蠕虫病毒在Internet上爆发，命名为"冲击波(Worm.Blaster)"。它会不断地扫描网络，然后攻击有RPC(remote procedure call, 远程过程调用)漏洞的计算机，一旦攻击成功，蠕虫将会被传输到该计算机上并运行。计算机被攻击后，可能造成RPC服务终止，系统被自动关闭，蠕虫占用大量的资源，以至不能在Internet Explorer中打开新窗口，复制粘贴操作不能进行等现象。

蠕虫传播的前提之一是系统程序中存在的漏洞。2001年8月的"红色代码"利用的是Windows IIS服务的漏洞，只感染Web服务器。2003年2月的"SQL杀手"利用了SQL Server中的漏洞，感染的范围是运行SQL的系统。而"冲击波"蠕虫利用的RPC漏洞，存在于所有的Windows 2000/XP系统中，因此它的感染范围比前两种更广。因为该漏洞使所有Windows NT以上的系统都面临威胁(包括大型服务器和个人计算机)，而不局限于WWW、SQL等服务器系统，被认为是迄今为止Windows最为严重的安全漏洞。

1 RPC漏洞介绍

2003年7月16日，一个安全研究组织LSD宣布了微软Windows操作系统中存在的一个严重漏洞[1]，它存在于所有的Windows NT/2000/XP和最新的.Net Server 2003中。Windows的分布式组件对象模型(DCOM, distributed component object model)，但LSD并没有宣布该漏洞的技术细节。

7月21日，微软发布针对此漏洞的补丁，号码为823980[2]。用户可以下载补丁修补漏洞，但破坏者也可以利用该公告中对漏洞的有关描述，编写出利用该漏洞进行传播的蠕虫程序。我国的民间安全组织XFOCUS随后对相关Windows代码进行了反汇编分析并进行了实验，于7月25日发布了该漏洞的技术细节[3]。

RPC是Windows操作系统使用的一个应用层协议，它提供了一种进程间通信机制，通过这一机制，本地代码可以调用执行其他计算机上的程序。RPC服务程序RPCSS有一个函数CoGetInstanceFromFile( )，它的第6个参数是指向一个文件名的指针OLECHAR * szName。文件名的形式如"\\主机名\c$\abc.doc"，以Unicode格式存放。

RPCSS为文件名设定的缓冲区大小为544字节。直接调用CoGetInstanceFromFile函数时，该函数会检查文件名的长度，不接受超长的文件名字符串。但是，RPCSS为主机名设定的缓冲区只有32字节。如果构造一个特别的文件名，其中包括的主机名长度超过32字节，RPCSS将它拷贝到缓冲区时，造成缓冲区溢出。

该漏洞存在于所有的Windows NT以上的版本中。对不同版本的操作系统，由于RPCSS的执行代码有所区别，利用该漏洞进行缓冲区溢出攻击的网络攻击包中略有区别。"冲击波"针对Windows XP和Windows 2000设定了两种网络攻击包。

2 运行过程

在蠕虫传播的过程中，计算机有两种角色：蠕虫运行的计算机称为宿主机，它要传染的目标称为目标机。宿主机上，蠕虫已经获得控

制权。

“冲击波”蠕虫的文件名为msblast.exe，存放在Windows system32目录中。从宿主机开始执行msblast.exe时分析其运行过程：

(1)在"HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"注册键中，创建一项："windows auto update"="msblast.exe"。以后，每次启动计算机时，msblast.exe就会被执行。

(2)创建一个名为"BILLY"的互斥锁。如果创建失败，则说明msblast.exe已在内存中运行，本程序退出。因此，在内存中只有一个“冲击波”蠕虫在运行。

(3)调用InternetGetConnectedState()检查宿主机是否可以访问网络，如果可以则转到下一步，否则睡眠20秒后继续检查。

(4)取得系统的日期。如果是在8月16日或以后，创建一个线程以20毫秒的间隔向windowsupdate.com进行SYN淹没攻击。windowsupdate.com是微软提供补丁程序的一个网站，因此“冲击波”蠕虫在广泛传播后，构成对这个网站的分布式拒绝服务攻击DDoS。

(5)产生目标机的IP地址。蠕虫取得一个随机数，分别以40%和60%的几率感染本地局域网和Internet上的计算机。目标机的IP地址的计算方法此处略。

(6)向目标机的TCP端口135发送一个特殊构造的网络攻击包(payload)。分别以20%和80%的几率传送针对Windows 2000和Windows XP的网络包。如果目标机的类型和攻击包不一致，将这种不一致的攻击包称为错误攻击包。如表1所示，收到错误攻击包后，就会导致目标机上的RPC服务中止，svchost.exe报错，系统提示在1分钟之内自动关闭并重新启动；如果类型一致，则目标机上的RPCSS发生缓冲区溢出。

表1 “冲击波”蠕虫对宿主机的攻击

攻击目标 \ 攻击类型	Windows 2000	Windows XP
Windows 2000	成功	自动重启
Windows XP	自动重启	成功
Windows NT/2003	自动重启	自动重启

(7)目标机上发生缓冲区溢出后，包含在网络攻击包中的蠕虫程序获得控制权。程序在端口4444上侦听。将它在该端口收到的所有请求作为命令来执行，构成一个远程命令行环境(remote command shell)。由于缓冲区溢出的上下文环境是在RPC服务中，具有系统权限，因此，宿主机可以通过向端口4444执行任何命令。这段蠕虫程序名为Metasploit。

(8)宿主机建立一个到目标机上TCP端口4444的连接。

(9)宿主机创建一个TFTP线程，接收并执行来自目标机上的tftp请求。TFTP线程在UDP端口69上监听，收到来自目标机的tftp请求后，传送msblast.exe到目标机中。

(10)宿主机从该连接上发送“tftp -i a.b.c.d GET msblast.exe\n”到目标机。“\n”代表字符0AH。

(11)查询TFTP线程是否已将文件传送到目标机。

(12)从该连接上发送“start msblast.exe\n”和“msblast.exe\n”到目标机。

(13)重复执行第5)至12)步，感染其他宿主机。

为加快传播速度，在第5)至12)步同时对20个目标机进行攻击。攻击成功后，在第12)步由宿主机远程控制在目标机上运行msblast.exe，目标机的角色转变为宿主机，又向其他计算机发动攻击。

蠕虫程序除了在网络上产生大量的负载占用网络带宽外，还导致导致Windows自动重启。当收到类型不一致的网络攻击包(见表1)时，RPC服务崩溃。在Windows XP中，出现的信息为“Generic Host Process for Win32 Services 遇到问题需要关闭”。接下来，系统提示：“Remote Procedure Call(RPC)服务意外中止，Windows必须立即重新启动”的信息。在1分钟后，系统自动关闭并重启。重启后，如果再次收到这样的攻击包，会再次关闭/重启。这就是Windows自动重启的真正原因。不论该计算机是否已经被感染，它都可能接收到来自其他计算机的攻击，因此，在蠕虫流行期间，Windows自动重启的现象大量出现。在个人计算机上，一旦拨号上网，在数分钟之内就会收到错误攻击包，导致Windows自动重启。在与网络断开时，则不会出现这种现象。

3 防范措施

由于蠕虫会引起Windows不断自动重启，因此，在提示自动重启时，必须立即在“开始”→“运行”命令提示行上输入“shutdown -a”，以阻止Windows自动重启，再采取其他措施。

执行“services.msc /S”，或者通过控制面板进入“服务”控制界面，双击Remote Procedure Call (RPC)，再选择“恢复”，将“第一次/第二次/后续失败”的设置从“重新启动计算机”改为“不操作”或其他选项。这样，即使在收到错误攻击包时，Windows也不会重启。

在system32目录中，检查是否存在msblast.exe或penis32.exe文件，大小为6176字节。如果存在，将其删除。接着删除这些文件在注册表中的启动项。在任务管理器中查找并结束名为msblast或penis32的进程。一些安全厂商也提供自动清除工具来查找并删除系统中的蠕虫程序。

下载并安装针对该RPC漏洞的Windows补丁程序，可以避免系统

受到攻击。如果系统中安装了防火墙和防病毒软件，更新其特征库以识别“冲击波”蠕虫。在防火墙中关闭135、139和445端口。

4 与“SQL 杀手”和“红色代码”的对比

“冲击波”是继“红色代码”[4]和“SQL杀手”[5]后又一个大规模爆发的蠕虫。它们都是利用网络进行针对Windows软件的缓冲区溢出漏洞进行传播，在数天甚至数小时内覆盖到整个Internet，成为同时期内Internet蠕虫的典型代表。3种蠕虫的对比见表2。

这3个漏洞都不是由微软本身发现的，而且RPC漏洞还存在于微软最新发布的Windows 2003中。为此，微软产品的安全性不断受到质疑。

从表中可以看出，在漏洞被公布后，微软的反应时间较短，在数天内即发布了相应的补丁供用户升级。但从实际情况看，大量的用户并没有及时对系统进行修补，造成蠕虫的大规模传播。因此，系统管理员必须时刻关注系统安全漏洞和补丁程序的发布，及时采取相应的防范措施进行防范。

而蠕虫编写者则时刻在关注Windows系统的漏洞，在漏洞发布后，他们就开始编写利用该漏洞的攻击程序，其周期已逐步缩短。而一些组织将一些漏洞的详细信息和用于演示的攻击程序放到Internet上，蠕虫编写者就会利用这些信息。在“冲击波”蠕虫代码中，有超过50%的执行代码和XFOCUS公布的测试程序代码相同，包括缓冲区溢出后取得控制的方法、网络攻击包的构造等关键部分；在“冲击波”蠕虫代码中包含的文件名“c$\123456111111111111111111111111111.doc”及填充字符“FXNBFXFXNBFXFXFXFX”也与XFOCUS的测试程序完全相同，而这些文件名和填充字符是可以随意改变而不影响蠕虫传播的。这充分证明了“冲击波”是以XFOCUS测试程序为基础加工而形成的。

从感染对象上看，“冲击波”比前两种蠕虫要广，原因是它赖以传播的系统漏洞来自Windows的基础组件，而其他两种蠕虫只能在安装了特定软件的系统中传播。

5 采取主动防御措施的必要性

“冲击波”蠕虫的大规模爆发促使用户去安装补丁或其他措施以弥补RPC漏洞，因此该蠕虫的影响迅速减弱。但操作系统和其他应用程序中必然存在其他的一些未知漏洞，不断地被发现和修补。一般的顺序是“发现漏洞→公布补丁→蠕虫爆发→修补”4个步骤，虽然可以通过加速补丁的发布和部署来抑制甚至杜绝蠕虫的爆发，但是这种防御措施在本质上是消极的。如果漏洞是由蠕虫编写者首先发现的，漏洞并没有公布，那么在蠕虫爆发时就没有补丁可用，蠕虫就不能被有效地遏制。上面的3种蠕虫代码中并没有包括极强破坏性的代码，其目的仅在大规模的传播。如果在蠕虫包括了毁坏或盗窃数据的代码，会造成更大的损失。因此，这种消极的防御措施包括了很多不确定因素，面临极大的风险。

表 2 三种蠕虫程序的对比

蠕虫名称	“冲击波”	SQL 杀手”	“红色代码”
漏洞公布日期	2003/07/16	002/05/15	2001/05/03
补丁发布日期	2003/07/21	2002/07/24	2001/06/18
爆发日期	2003/08/12	2003/01/24	2001/08/06
漏洞位置	RPC(MS03-26)	SQL Server(MS02-39)	IIS(MS01-033)
漏洞发现者	LSD	NGS	eEye
感染对象	所有Windows系统	运行SQL的系统	运行Web服务的系统
存在位置	内存/文件	内存	内存
带宽消耗	一般	高	一般
主要危害	Windows自动重启	大量占用Internet带宽	Web服务器失效

在目前系统中存在未知漏洞的情况下，应该在系统软件中增加缓冲区溢出的处理机制，避免攻击程序通过漏洞获得控制权。在任何程序发生缓冲区溢出时，必须将该程序终止，而不能允许攻击代码在该程序的上下文环境中继续执行。

Stack-Guard等方法通过对编译器的改造，应用程序重新编译后可以部分地防止缓冲区溢出漏洞；而Stack-Guard等方法通过对源程序进行扫描分析来发现其中的编程错误。它们都只能部分地解决缓冲区溢出漏洞问题；SecureStack等方法通过间接地设置堆栈页面为不可执行属性，使得缓冲区溢出代码不会被执行，是一个较为根本的解决方案，但需要对内存页面的使用进行监控，运行开销大，还存在一些兼容性问题。笔者正在Windows环境下研究依据段长限制来禁止在堆栈页中执行代码的方法，以解决其他方法的运行开销和兼容性问题。这种积极防御方案的好处在于：用户不再需要频繁地安装系统补丁，就可以解决缓冲区溢出漏洞问题。

参考文献

1 Last Stage of Delirium, http://lsd-pl.net/special.html

2 The Analysis of LSD's Buffer Overrun in Windows RPC Interface

3 http://www.ngssoftware.com/vna/ms-sql.txt

4 谭毓安，新型网络病毒-红色代码病毒的分析和防范，计算机系统应用，2001年12期。

5 谭毓安，蠕虫病毒-SQL杀手的分析和防范，计算机系统应用，2002年11期。