新型网络病毒——红色代码病毒的分析和防范

谭毓安　(北京理工大学计算机科学与工程系　100081)

摘要	“红色代码”病毒利用IIS的idq.dll缓冲区溢出漏洞传染Web服务器，具有拒绝服务攻击的功能，通过设置特洛伊木马可完全控制被感染的Web服务器。本文讨论了其运行机制以及检测和清除方法。
关键词	病毒　蠕虫　系统漏洞　特洛伊木马

1　引言

“红色代码”病毒是一种新型网络病毒，其传染过程充分体现了网络时代网络攻击技术与病毒机制的巧妙结合，它将网络蠕虫、计算机病毒、木马程序、分布式拒绝服务攻击等功能合为一体，可称之为新一代的病毒。对其中的代码进行改造后，其破坏能力更强，通过网络攻击得到目标主机的管理权限后，可以为所欲为，毁坏或盗走机密数据，严重威胁网络安全。

2001年7月中旬该病毒在美国等地大规模蔓延，国外通讯社大量地报道该病毒的破坏情况；8月初出现了该病毒的变种（红色代码II），针对中文系统加强了攻击能力，导致在国内的大规模蔓延，受灾情况相当严重，公安部发布紧急通告，要求对该病毒严加防范。

2　“红色代码”病毒的新特点

不同于以往的文件型病毒、引导型病毒或通过邮件传染的蠕虫病毒，“红色代码”并不将病毒信息写入被传染对象(Web服务器)的硬盘。它只存在于内存，不通过文件这一常规载体传染和存储，而是借助这个服务器的网络连接来传染其他的服务器，在计算机的内存之间不断进行复制。从传染途径上看，该病毒在Web服务器之间通过80端口发送HTTP请求进行传播。

在“红色代码II”病毒中，还包含了特洛伊木马功能。被感染的主机随时会受到更进一步的攻击。由于攻击者的破坏命令是通过Web请求发送到目标主机，在目标主机本地执行破坏操作，因此，网络系统中的防火墙不能识别并阻止这些破坏操作。更加危险的是攻击者还能够以这个服务器为跳板，进一步攻击系统内的其他主机，危及到Web服务器所处的整个网络系统。

3　传染过程

“红色代码”利用了微软公司IIS系统的一个漏洞（发布于2001年6月18日，公告编号: MS01-033）[1]。该漏洞存在于Windows NT 4.0和Windows 2000系统中。IIS中包括一些ISAPI扩展DLL，其中的idq.dll属于索引服务(Index Server)，支持在Web中使用管理脚本(.ida文件)和Internet数据查询（.idq文件）。

idq.dll在处理输入请求的URL时存在一个缓冲区溢出漏洞，攻击者可以构造一个超长的URL，其中包含攻击代码。该攻击代码在系统中运行时没有任何权限限制，因此能够完成任意操作。

“红色代码”病毒的传染对象是运行Windows NT或Windows 2000并使用微软IIS系统的Web服务器。在传染Web服务器时，它向服务器的端口80发送一包含病毒自身的“数据包”；使idq.dll处理请求时产生堆栈覆盖，函数的返回地址被病毒设定的数据覆盖，执行返回指令时就会执行处于idq.dll堆栈中的病毒代码[2]。病毒驻留后再次通过此漏洞感染其他服务器。

4　“红色代码”病毒的运行过程

在侵入一台服务器后，其运行步骤为：

(1) 设置其运行环境。首先修改堆栈指针，设置堆栈大小为218h字节。接着使用RVA（相对虚拟地址）查找GetProcAddress的函数地址，再

调用此函数获得其他函数的地址，如socket、connect、send、recv、closesocket等。

(2) 如果c:\notworm文件存在，则不进一步传染其他主机。

(3) 传染其他主机。创建100个线程，其中99个线程用于感染其他的Web服务器。通过一个算法来计算出一系列的IP地址作为传染目标。按照IP地址的生成算法，能够产生重复传染的情况，从而在这些服务器之间传输大量的数据而消耗其网络带宽，达到拒绝服务攻击的效果。

(4) 篡改主页。如果系统的默认语言不为美国英语（代码页不等于0x409），第100个线程和前99个线程一样去感染其他系统。否则会篡改系统的网页，被感染的Web服务器的网页将被篡改成这样一条消息："Welcome to http://www.worm.com !, Hacked By Chinese! "。这个消息持续10个小时后会消失。与其他通过网络攻击篡改网页的方法不同，该病毒并不修改磁盘上的主页文件，而是修改w3svc.dll的TcpSockSend入口指向病毒代码，当浏览器访问这个被感染的Web服务器时，TcpSockSend返回前述的篡改消息。

(5) 产生对www.whitehouse.gov的拒绝服务攻击。每一蠕虫线程都会检查c:\notworm文件。如果文件存在，则转为休眠，否则检查当前时间，如果时间在20:00 UTC和23:59 UTC之间，将对www.whitehouse.gov进行攻击。创建一个socket并与198.137.240.91（www.whitehouse.gov的IP地址）80端口建立连接，并发送18000h（98K字节）的数据。在休眠大约4个半小时后，再次重复发送数据。由于在全世界范围内有大量Web服务器被感染，其结果就可能会产生对www.whitehouse.gov的拒绝服务攻击。

5 "红色代码II"病毒

"红色代码"病毒主要攻击使用0x409代码页的美国网站，而"红色代码II"病毒则对中国网站更具破坏性。其目标则是摧毁系统而不是感染系统和扩散自身，并增加了特洛伊木马功能。与第一代"红色代码"病毒的主要区别为：

(1) 计算IP地址的算法进行了修改。减小了在本地网络重复传染的机会，使病毒传染的速度更快。

(2) 检查是否存在"CodeRedII"原子（atom），若已存在则进入睡眠状态，确保此主机不会被重复感染。若不存在，则创建"CodeRedII"原子。

(3) 创建300个线程进行传染，若系统的默认语言为简体中文或繁体中文（代码页为0x804或0x404），则创建600个线程。

(4) 检查年份是否超过2002或者月份是否超过10。如果超过2002年或者月份超过10，就重新启动本地系统。可以认为，设计者的意图是使传播在2001年10月1日完成，之后，蠕虫会爆发而使系统不断重新启动。

(5) 在系统中设置一个特洛伊木马。首先，将系统目录的cmd.exe拷贝到IIS scripts目录和MSADC目录中并更名为root.exe。病毒体内包含的特洛伊木马的压缩版本，将其解压还原后写到c盘和d盘的explorer.exe。这就意味着，每次系统启动后将运行这个explorer.exe将作为Windows外壳（用户界面）运行。

特洛伊木马在每次系统启动时都会被激活，它先执行系统目录下的explorer.exe，进入Windows外壳。接着进入一个死循环中，在循环体中修改注册表项，禁止系统的文件保护功能，创建虚拟web路径（/c和/d），映射到c:\和d:\。

攻击者可能运行的攻击形式为：http://IP地址/c/inetpub/scripts/root.exe?/c+dir或者http://IP地址/c/winnt/system32/cmd.exe?/c+dir。

在实际进行攻击时，dir可能会攻击者被替换为任意命令，如删除系统中的文件，向外发送机密数据等等。

6 "红色代码"病毒的检测和防范

"红色代码"病毒的传染对象是安装IIS的Windows系统。根据其运行特点，有以下几种手段来检查系统中是否有"红色代码"病毒：

(1) 是否出现负载显著增加(CPU/网络）的现象。

(2) 可用"netstat -an"命令检查是否存在对许多外部IP地址的80端口的连接。

(3) 在web日志中检查是否有被病毒攻击的记录，如"/default.ida?XXX... %u0078%u0000%u00=a HTTP/1.0 "。

(4) 查找系统中是否存在文件c:\explorer.exe或d:\explorer.exe，以及IIS脚本目录和msadc目录中是否有文件root.exe存在。

(5) 检查注册表中是否增加了c和d虚拟目录，以及是否文件保护功能被禁止。

(6) 在任务管理器中检查是否存在两个"exploer.exe"进程。

为防止系统被"红色代码"病毒感染，可下载针对.ida漏洞的微软补丁，或者从系统中删除对.ida文件的支持。通过将"红色代码"攻击时发送的数据包加入到IDS特征数据库中，IDS将拒绝病毒传染URL请求。在网

（下转第71页）

(上接第 68 页)

络出口处设置防火墙或入侵检测软件，通过日志或流量异常来定位网络病毒的存在，再使用反病毒软件进行清除。此外，还可以自动探测系统中是否存在微软IIS安全漏洞，变“被动查杀”为“主动防杀”，防范于未然。

在发现系统被病毒感染后，可以使用新版杀毒工具来清除。其清除过程为：

① 删除 C:＼exploer.exe 和 D:＼exploer.exe。

② 删除 IIS 的 scripts 和 MSADC 目录下的 root.exe。

③ 恢复注册表项，将＼W3SVC＼Parameters＼Virtual Roots 的 "/C" 和 "/D" 的项删除。将 "/scripts" 和 "/MSADC" 项中的 ",,217" 改成 ",,201"，WinLogon＼SFCDisable 的值恢复为 0。

④ 安装微软提供的补丁。

⑤ 重新启动系统以清除在内存中存在的病毒。

7 结束语

“红色代码”病毒的出现，是病毒技术的一大突破。病毒本身不依赖与特定的可执行文件，而通过网络在系统中传播，使得病毒防范的重点必须转向阻止病毒的侵入。该病毒通过80端口传染Web服务器，但其传染机制同样适用于其他网络服务。而随着其他系统漏洞的不断发现和公布，也可能会产生利用这些漏洞进行传播的新病毒。因此，提高对新病毒的反应速度，及时对系统进行修补，是一个必然要求。而目前的反病毒技术主要是基于对已发现病毒的分析和防范，对未知病毒缺乏抵御能力，针对网络病毒和攻击急需实现基于广谱技术的解决方案。从另一方面，网络攻击和病毒能够得逞的根源在于系统中存在的各种漏洞，加强我国具有自主知识产权的网络操作系统和网络基础设施的开发与建设，必将对提高国家的安全水平具有重要的意义。■

参考文献

1 *http://www.microsoft.com/technet/security/bulletin/MS01-033.asp。*

2 *张小斌、严望佳，黑客分析与防范技术 [M]，北京清华大学出版社，1999．97-104。*