Outbreak Mechanism and solution of on"CodeRed II"Computer Virus

"红色代码II (Code RedII)"蠕虫病毒发作机制和解决方案

刘睿 (长春吉林大学电子科学与工程学院 130023)

摘要: "红色代码(Code Red)"蠕虫病毒，是目前互联网上出现的一种新型计算机蠕虫病毒。本文介绍了其发作机制和攻击原理，并给出了相应的解决方案。

关键词: 红色代码　网络安全　蠕虫　病毒　系统漏洞

1 前言

随着"红色代码(Code Red)"蠕虫病毒正在互连网上的肆虐传播，已对整个互连网的正常运转造成了严重影响，目前已入侵了全球约36万台网络服务器，在7月份的爆发中，管理着上千个网站的美国国防部不得不临时关闭了公共访问路径，估计该蠕虫病毒已让整个互联网业损失了12亿美元，其最新变种"红色代码II (CodeRed II)"已经开始大范围入侵国内网站，截止到8月9日，国家计算机病毒应急处理中心统计国内遭受红色代码II攻击的用户共180余家，被感染的服务器超过200台。绝大多数为企业用户，波及北京、天津、上海、重庆、河南、吉林、辽宁、浙江、福建、江苏、广东、湖北、云南等十几个省及直辖市，涉及计算机信息行业、网站、企事业单位、教育科研行业、政府机构、金融证券行业等多种行业，造成大量Web服务器因遭受其攻击而瘫痪。因为此蠕虫病毒已经不再采用传统的基于文件的感染和传播方式，并且攻击手段趋向智能化，使传统的反病毒软件难以有效预防和清除，这次全球化的大规模爆发再次给互联网时代网络安全敲响了警钟。

2 分析

代号为"红色代码(Code Red)"是一种新的计算机蠕虫病毒。与其蠕虫程序不同的是，"CodeRed"不将任何病毒代码写入被入侵的系统硬盘里，它在入侵系统后直接从内存中运行和传播。除此之外，它还利用Microsoft Index Server 2.0和Indexing Service中存在的安全漏洞从而执行自己提供的代码。(注：索引服务器Index Server和Indexing Service是分别安装在IIS4.0 (NT4.0)及IIS5.0 (Windows2000)上的系统服务)故该蠕虫病毒只攻击使用Windows NT或Windows 2000包含IIS 4.0、IIS 5.0 (微软网络服务器)的电脑系统(大多数是些企业用户)，普通的Internet用户则不必担心。

与第一代相比，"红色代码II (Code RedII)"(又名：CodeRed.C, CodeRedIII,IIS-Worm,CodeRed v3,W32.Bady.C)传播速度要快，威害性更大，新的蠕虫变种修改了Windows注册表并放置特洛伊木马程序(cmd.exe改名为boot..exe)，最终导致受感染系统后门大开,丧失安全策略。任何攻击者能取得对受影响系统的特权访问，而且新的蠕虫会从受感染机优先扫描同一网段内的机器。

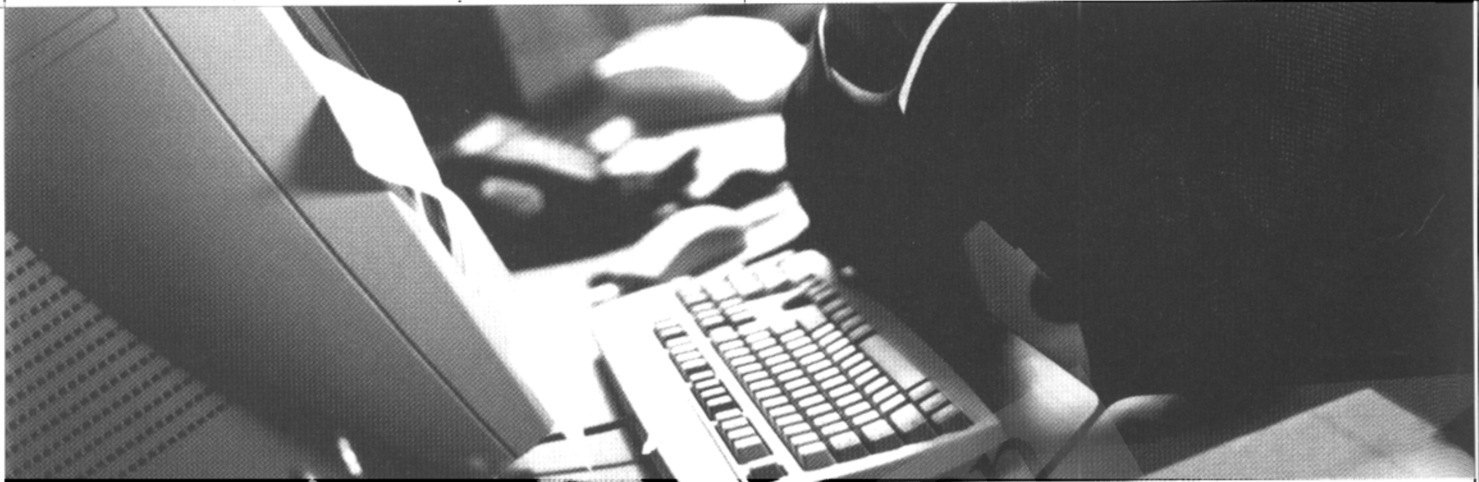
在具体分析该病毒的工作流程前，先简单介绍一下存在于Microsoft Index Server的安全漏洞。

微软IIS在缺省安装情况下带了一个索引服务器(Index Server,在Windows 2000下名为Index Service)。缺省安装时，IIS支持两种脚本映射：管理脚本(.ida文件)、Inernet数据查询脚(.idq文件)。这两种脚本都由一个ISAPI扩展——idq.dll来处理和解释。但是，idq.dll在一段处理URL输入代码中存在一个未经检查的缓冲区，如果攻击者提供一个特殊格式的URL，就可能引发一个缓冲区溢出。通过非法构造发送数据，攻击者可以改变程序执行流程，执行任意代码。而更为严重的是idq.dll是以SYSTEM身份运行的，可利用此漏洞取得系统管理员权限。例如，当提交下列URL请求：

```
GET /NULL.ida?[buffer] =X HTTP/1.1
Host: werd
```

如果[buffer]的长度超过240个字节，就可能触发溢出。

(注：以上实例仅供安全研究与教学之用。使用者风险自负！)



3 判定系统感染方法

(1) 在 WINNT＼SYSTEM32＼LOGFILES＼W3SVC1 目录下的日志文件中如有以下内容：

GET, /default.ida,
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXX%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0

那么该系统已经遭受“红色代码II”的攻击。

(2) 使用命令 netstat-a

如果在 1025 以上端口出现很多 SYN-SENT 连接请求，或者 1025 号以上的大量端口处于 Listening 状态，那么该系统已经遭受“红色代码II”病毒的感染。

(3) 如果在以下目录中存在 Root.exe 文件，说明系统已被感染。

C:＼inetpub＼Scripts＼Root.exe

D:＼inetpub＼Scripts＼Root.exe

C:＼Program Files＼Common Files＼system＼MSADC＼Root.exe

D:＼Program Files＼Common Files＼system＼MSADC＼Root.exe

同时，“红色代码II”还会释放出以下两个文件 C:＼Explorer.exe or D:＼Explorer.exe。这两个文件都是木马程序。

(4) 由于遭受“红色代码II”病毒的攻击，NT 服务器中的 Web 服务和 Ftp 服务会异常中止。网络性能急剧下降，路由器、交换机等网络设备负载加重，甚至崩溃。

不受影响的系统：

已经安装了微软安全公告 MS01-033 中补丁的 Windows NT/2000 系统

4 该蠕虫攻击工作流程如下

(1) “红色代码II (Code RedII)”蠕虫病毒利用上述微软 Index Server (.ida/idq) ISAPI 扩展远程溢出漏洞，通过 80 端口发送一个构造过后的 HTTP GET 请求到该服务器。当本地 IIS 服务程序收到某个来自 CodeRedII 发的请求数据包时，由于存在漏洞，导致处理函数的堆栈溢出(Overflow)。当函数返回时，原返回地址已被病毒数据包覆盖，系统强迫运行病毒代码，此时病毒被激活，并运行在 IIS 服务程序的堆栈中。

(2) 该蠕虫病毒首先调用初始化程序确定内核程序 KERNEL32.DLL 中的 IIS 服务器的基地址，然后寻找函数 GetProcAddress 获取进程地址的开始地址，并通过该函数获得别的一系列的 API 的函数地址。

该网络蠕虫的主线程检查 2 个不同的标记：

第一个标记是 29A，该标记控制该网络蠕虫程序的安装；

第二个是检查系统内存中是否已注册了一个名为 CodeRedII 的 Atom (系统用于对象识别)，如果已存在此对象，表示此机器已被感染，病毒进入永久休眠状态，由此确保此系统不会被重复感染。若没有发现“CodeRedII”Atom，则增加一个“CodeRedII”Atom，用来表示此主机已经被感染。

(3) 此后该蠕虫进入繁殖传播过程。蠕虫开始检查当前的系统的语言，如果默认的语言是简体或繁体的汉字系统，它会建立 600 个新的线程；如果不是，该蠕虫程序建立 300 个线程。每一个线程产生一组随机的 IP 地址，并寻找其中可以感染的目标机器，每 100 毫秒就会向一目标地址的 80 端口发送一长度为 3818 字节的病毒传染数据包。这里，该蠕虫用到一个随机数发生器，此发生器产生用于病毒感染的目标地址 IP 地址。其工作流程如下：

首先在 1 到 254 的范围内随机生成 4 个字节 (防止 IP 地址为一个 0 或

255)，然后，随机从这些字节中取出一个字节，后与7做与操作（'AND'），产生一个0到7之间的随机数。然后根据这个随机数从一个地址掩码表中取出相应的掩码（实际掩码在内存中的位置是反向存储的）：

dd 0FFFFFFFFh ; 0

dd 0FFFFFF00h ; 1

dd 0FFFFFF00h ; 2

dd 0FFFFFF00h ; 3

dd 0FFFFFF00h ; 4

dd 0FFFF0000h ; 5

dd 0FFFF0000h ; 6

dd 0FFFF0000h ; 7

如果发现产生的IP是127.x.x.x或224.x.x.x或与当前IP相同，它就会重新产生一个新的攻击地址。因为与被感染的主机在同一或相近网段内的主机也大多使用相同的系统，所以该蠕虫病毒可大大增加感染的成功率。

(4) 然后，该蠕虫将原来的Windows NT/2000系统System目录下的CMD.EXE文件改名为root.exe并拷贝到以下路径中：

C:\inetpub\Scripts\Root.exe

D:\inetpub\Scripts\Root.exe

C:\Program Files\Common Files\system\MSADC\Root.exe

D:\Program Files\Common Files\system\MSADC\Root.exe

这样，为以后通过HTTP GET请求运行root.exe来获得对受感染系统的完全访问控制权提供条件。

(5) 不仅如此，该蠕虫还将在C盘和D盘根目录下生成一个大小为8,192字节的explorer.exe特洛伊木马程序。以此来修改系统注册表文件，留下系统后门，对系统进一步控制。蠕虫之所以将"explorer.exe"木马放在"C:\"和"D:\"下是因为Windows操作系统还存在另一安全漏洞。当Windows操作系统在执行可执行程序时，会先搜索系统盘根目录下面有没有同名的程序。如有，则先执行该程序。因此，攻击者将"exploer.exe"木马放在系统盘的根目录下面，目的是要先于真正的"exploer.exe"来提前执行。当属于管理员组的用户地登录进入系统时，木马将被执行。

(6) 当该蠕虫病毒从体内释放完explorer.exe木马程序后进入休眠状态。如果是中文系统（即默认的语言是简体或繁体的汉字系统），蠕虫休眠2天；如果是非中文系统，蠕虫休眠1天。此外，当系统时间超过2002年或月份超过10月份，蠕虫也会重启系统。

(7) 重启系统完毕后，exploer.exe木马得以优先执行。并对系统注册表进行以下修改：

将HKEY-LOCAL-MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SFCDisable由缺省值0改为0xFFFFFF9D，使得系统启动时不检查系统文件的完整性，丧失对系统文件的保护能力。并且还在注册表中创建，修改了以下键值：HKEY-LOCAL-MACHINE\SYSTEM\CurrentControlsSet\Services\W3SVC\Parameters\Virtual Roots/Scripts=%rootdir%\inetpub\scripts,,204；

HKEY-LOCAL-MACHINE\SYSTEM\CurrentControlsSet\Services\W3SVC\Parameters\Virtual Roots/MSADC=%rootdir%\program files\common files\system\msadc,,205

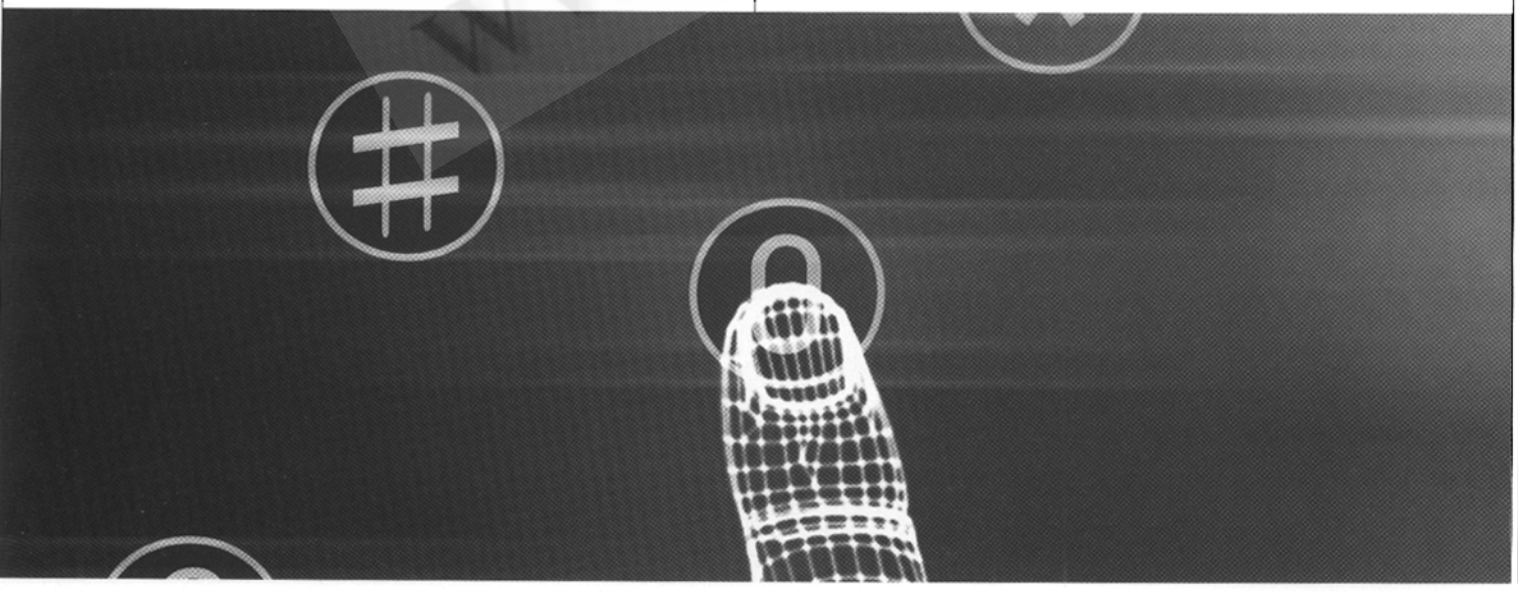
HKEY-LOCAL-MACHINE\SYSTEM\CurrentControlsSet\Services\W3SVC\Parameters\Virtual Roots/C

改为C:\,,217

HKEY-LOCAL-MACHINE\SYSTEM\CurrentControlsSet\Services\W3SVC\Parameters\Virtual Roots / D

改为D:\,,217

在此之后，木马程序完成了它的感染周期，并会每隔10分钟重复进行



以上提到的注册表项修改。

通过上面的修改，木马创建两个虚拟 IIS 目录 C 和 D，分别映射到系统的C:盘和D:盘。这些虚拟目录被赋予读写及可执行权限,这样木马程序通过 IIS 向所有黑客提供了对被感染服务器C:盘和D:盘的完全控制能力。并且，即使用户删除了root.exe,但只要explorer.exe木马仍在运行，黑客仍然可以利用这两个虚拟目录来远程访问您的系统

5 综述

"红色代码II(Code RedII)"蠕虫病毒是一种全新的计算机病毒。与以往的病毒相比,它不再将病毒执行代码写入可执行文件或磁盘的主引导区，并且传播途径也不再是软盘，光盘。它只存于内存中，并且在释放完木马后重新启动系统，使得自身消失。传染是通过互联网由一台电脑内存直接感染到另一台电脑内存中，传染速度极快。这使传统的查毒手段很难捕捉到。此外,该蠕虫病毒首次利用到系统存在的安全漏洞来进行自身传播,并且该蠕虫病毒可加载特洛伊木马程序，为黑客开启系统后门取得超级用户完全访问特权。这对整个互联网的安全性能提出了新的问题，对全球的网络管理员们提出了新的考验。

6 解决方案(根据不同感染情况可能略有不同)

(1) 立刻停止 IIS 服务，以防止蠕虫的进一步攻击。

(2) 用任务管理器，杀掉只有一个线程的 exploer.exe 木马程序。去除 C:\exploer.exe 和 D:\exploer.exe 的隐藏和只读属性，并删除。

(3) 删除 C 盘和 D 盘\inetpub\scripts\和\program files\common files\system\MSADC\下的 root.exe 文件。

(4) 使用 RegEdit 修复蠕虫创建的注册表项。把 HKEY-LOCAL-MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots 对于 c:和 d:的完全控制键值删除。重新启动计算机，将键值 HKEY-LOCAL-MACHINE\SoftWare\Microsoft\WindowsNT\CurrentVersion\winLogon\SFCDisable 设为 0，使系统文件保护有效。

(5) 运行"开始"-->"程序"-->"管理工具"-->"internet服务器"，在"默认 WEB"站点中，把对 c:\和 d:\的引用删除。

(6) 安装补丁程序，完全消除系统安全漏洞的威胁，避免系统再次感染。

可根据微软为此发布的安全公告 (MS01-033) 来下载相应补丁程序：

7 安全公告

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

补丁程序：

Windows NT 4.0：

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30833

Windows 2000 Professional, Server and Advanced Server：

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30800

8 注意

Windows NT 4.0 补丁需要安装在 Windows NT 4.0 Service Pack 6a 系统中

Windows 2000 补丁需要安装在 Windows 2000 Service Pack1 或 Service Pack2 系统中

只有在正确安装并重新启动后补丁才能生效。

参考文献

1 http://www.cert.org [EB/OL]

2 http://www.securityfocus.com [EB/OL]