文章编号:1004-1478(2011)04-0082-03

基于注册表配置的计算机病毒防治

张宇

(河南省理工学校 专业二部, 河南 郑州 450008)

摘要:研究了合理配置和管理注册表以防治Windows平台下计算机病毒的方法:通过监控与系统启动和文件关联启动相关的子键防范病毒,通过修改注册表相关子键防范和清除病毒,从而达到提高计算机系统安全性的目的.

关键词:注册表配置;计算机病毒;病毒防范
中图分类号:TP311 **文献标志码**:A

Computer virus prevention based on the registration table configuration

ZHANG Yu

(*The Second Dept. of School Teaching., He'nan Poly. School of Sci. and Eng., Zhengzhou* 450008, *China*)

Abstract: The method of reasonably configuring and managing registration table for preventing computer viruses under the Windows operating system was studied. The way is introduced to prevent and eliminate computer viruses by mornitoring and modifying sub-keys relevant to system and file association startup on registration table in order to improve the security of a computer system.

Key words: registration table configuration; computer virus; virus protection

0 引言

Windows操作系统下的注册表是一个用于保存硬件配置、软件配置、用户环境和操作系统界面的中央分层数据库.作为Woindows操作系统的核心文件,注册表可以直接控制系统启动、硬件驱动程序的装载以及系统应用程序的运行[1].合理地配置和管理注册表,将会对系统本身和其中的软件进行优化.目前注册表的修改主要用于提高系统性能,增强系统安全性,解决系统常见故障、个性化操作系统和远程管理等方面的问题,而系统安全和系统故障往往与计算机病毒是分不开的.随着计算机技术的广泛普及,计算机病毒也在不断地变幻花样,使人防不胜防.一般的计算机用户往往依靠成熟的杀毒软件来查杀病毒,但是,单单依靠杀毒软件并不能完全清除顽固的计算机病毒,很多病毒在计算机重新启动后又会滋生演变.在这种情况下,用户需要借助特有杀毒工具手动清除病毒.由于计算机病毒是人为编制的一段可执行的计算机程序[2],这些程序感染计算机的一个共同特点是在注册表中写入信息,来达到自动运行、破坏和传播等目的.因此了解和掌握如何利用注册表来手动查杀病毒就显得尤为重要.目前在公共技术领域中,注册表及利用其查杀病毒的技术已经有了一定的发展,本文将从注册表监控和修改2方面对如何利用其进行计算机病毒的防范和清除进行探讨,以期达到提高计算机系统安全性的目的.

收稿日期:2011-07-01

作者简介:张宇(1980—),男,河南省郑州市人,河南省理工学校助教,主要研究方向为软件开发.

1　利用注册表防范病毒

1.1　通过对注册表的监控防范病毒

相当一部分病毒是通过修改注册表侵入并寄生在计算机内部的,因此对注册表进行严密的监控,及时发现注册表中的异常,可以有效地防范和发现病毒.由于注册表中内容众多,监控的重点可以放在病毒经常会利用的与系统启动和文件关联启动相关的子键上.

1)与系统启动相关的子键.注册表中有些项可以指定系统启动后自动运行下级子键所包含的程序,病毒程序常常利用这些项在系统启动后自动运行.

比如系统启动时自动执行的程序

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run、RunOnce

以及系统启动时自动执行的系统服务程序

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ RunServices、RunServicesOnce

2)与文件关联启动相关的子键.注册表中有些文件项的键值与某个应用程序关联起来,使得用户在打开该文件时,系统会自动调用相关联的应用程序.有些时候病毒会将该键值修改,当用户打开该文件时系统会先调用病毒程序然后再执行相关联的应用程序,使得用户很难发现系统已经执行了病毒程序.比如

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\HKEY_CLASSES_ROOT\txtfile\shell\open\command

中系统默认的值为%SystemRoot%\system32\NOTEPAD.EXE%1,当用户打开以.txt为后缀的文本文件时,系统会自动调用应用程序NOTEPAD.EXE.如果病毒将该键值修改为%SystemRoot%\system32\SYSEXPLR.EXE%1,用户在打开文本文件的时候,系统会先执行病毒程序SYSEXPLR.EXE,然后再运行NOTEPAD.EXE程序[3].

用户需要通过监控查看这类键值中有没有陌生的奇怪的自动启动文件,比如键值分支中可能出现类似.html或.htm的内容,其实这类键值是在计算机系统启动后自动访问包含网络病毒的特定网站从而导致该网络病毒发作的.一旦发现类似病毒程序,需要先将相关键值删除,然后在系统中查找出相关的文件并将其删除.

1.2　通过对注册表的修改防范病毒

计算机病毒一般需要在特定的触发条件下利用计算机系统的漏洞进行攻击,因此,通过对注册表的修改,可以阻止病毒的触发条件,填补系统漏洞,从而防范病毒的入侵.以下通过几个常见的实例来加以说明.

1)阻止移动磁盘传播病毒.通过移动磁盘(U盘、移动硬盘等)传播病毒已经成为目前病毒传播的主要途径之一.病毒通过移动磁盘传播的原理是:当Windows系统发现移动磁盘的分区盘符时,会查找并运行该盘符根目录下的Autorun.inf文件,然后根据其内部所指向的病毒路径查找并运行病毒程序从而达到自动启动的目的[4].对此,可以通过修改注册表禁止磁盘的AutoRun功能来防止计算机感染病毒.具体的操作方法是在注册表中找到以下表项:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2

对其权限进行修改,取消当前用户对该注册表项的所有访问权限.修改完毕后,即使用户双击该移动磁盘的分区盘符,系统也不会执行Autorun.inf所指向的病毒程序,而只是打开该分区目录,这样就避免了病毒感染.

2)限制病毒自行启动.正如之前提到的,很多病毒都是通过注册表中的RUN值进行加载而随操作系统的启动而启动的,用户需要找到注册表中的

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

将everyone对该分支的"读取"权限设置为"允许",取消对"完全控制"权限的选择.这样病毒就无法通过该键值启动自身了.

3)拒绝ActiveX恶意控件骚扰.当计算机收到ActiveX控件后,该控件会被下载到用户的计算机中,并在注册表适当的位置创建注册表项,通过调用Windows scripting host组件来执行程序.不少病毒都是通过在网页中隐藏恶意ActiveX控件的方法来私自运行系统中的程序,从而对本地系统造成破坏.用户可以在"system32"目录下删除wshom.ocx文件来限制ActiveX控件对Windows scripting host组件的调用,然后再找到注册表项

HKEY_LOCAL_MACHINE/SOFTWARE/Classes/CLSID

{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}

并将其删除,ActiveX 控件就再也无法私自调用脚本程序了[5].

4)禁止远程修改注册表.其他用户有可能通过远程连接对本机的注册表进行修改,禁止该项功能将有助于增强上网的安全性.通过修改注册表来实现禁止远程修改注册表的具体步骤如下:找到 HKEY_LOCAL_ MACHINE\SYSTEM\CurrentControlSet\SecurePipeServers\Winreg 子键,在键值窗口中新建名为"RemoteRegAccess"的键值,将数值数据设置为"0"并选择16进制作为基数,关闭注册表编辑器并注销或重新启动计算机即可生效[1].

2 修改注册表清除病毒

大部分常见的病毒都可以使用杀毒软件进行清除,但有些顽固的病毒杀毒重启后会利用在注册表启动项中遗留的修复选项恢复到杀毒前的状态.在这种情况下,用户需要先手动结束病毒进程,删除病毒文件,然后将注册表中病毒遗留选项删除掉,才能彻底清除该病毒.比如很多用户在使用 Internet Explore 的时候会碰到 IE 默认连接首页被篡改的情况,这是因为注册表项

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\Start Page

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Start Page

中的"Start Page"键值被病毒更改为恶意网站的网址.要解决这个问题,用户需要打开表项

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main

在右半部分窗口中找到串值"Start Page"双击,将 Start Page 的键值改为"about:blank",然后退出注册表编辑器,重新启动计算机,这样 Internet Explore 的首页就被设置为空了[6].如果重新启动计算机后,问题依然存在,很有可能是病毒通过注册表中的 RUN 值进行加载而实现随操作系统的启动而启动.用户可以打开注册表项

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Run

将其下的 registry.exe 子键删除,然后将位于 c:\Program Files\registry.exe 的自动运行程序也删除掉,从 IE 选项中重新设置首页,重新启动计算机后问题应该就得以解决.

3 结语

在当前计算机快速普及的形势下,计算机病毒的攻击和防范技术也在不断拓展.通过对注册表的监控和修改可以对病毒起到积极防范的作用.本文结合了一些病毒实例对注册表的分析、修改进行了阐述.另外需要强调的是,切忌在备份好注册表前进行盲目的修改,否则可能导致系统无法正常工作甚至崩溃.

参考文献:

[1] 华联科技.BIOS 与注册表[M].北京:机械工业出版社,2007.

[2] 李冬梅,郭红转.计算机病毒及防治方法探讨[J].科技广场,2009(1):99.

[3] 林洁.浅议注册表在反计算机病毒中的作用[J].中国高新技术企业,2008(4):115.

[4] 刘功申.计算机病毒及其防范技术[M].北京:清华大学出版社,2008.

[5] 许薇.基于注册表计算机病毒的防治[J].中国高新技术企业,2010(25):80.

[6] 梁波,水淼.2009 注册表全攻略[M].北京:电脑报电子音像出版社,2009.