文章编号: 1007-2985(2010) 03-0043-04

基于文件系统过滤驱动的内核 Rootkit 隐藏技术*

侯春明, 刘 林
(吉首大学物理科学与信息工程学院, 湖南 吉首 416000)

摘 要: Rootkit 是能够持久或可靠地、无法检测的存在于计算机上的一组程序和代码. 研究了基于文件系统过滤驱动技术的内核 Rootkit, 阐述了文件系统过滤驱动的工作原理、过滤驱动的实现、基于文件系统过滤驱动的内核 Rootkit 对文件隐藏的实现, 并讨论了针对 Rootkit 隐藏的检测技术.

关键词: 文件系统; Rootkit; 过滤驱动; 隐藏
中图分类号: TP316 文献标志码: A

随着信息技术的飞速发展, 以窃取计算机控制权和敏感信息为目标的程序迅速增加. Rootkit 是能够持久或可靠地、无法检测的存在于计算机上的一组程序和代码[1]. Rootkit 能在目标计算机中长期潜伏, 窃取信息而不被察觉, 因此在计算机战争、间谍、反计算机犯罪、证据收集等领域得到广泛应用, 同时也被计算机病毒、木马、恶意软件等恶意代码使用者用来实现计算机的恶意控制. 控制者一旦获得操作系统的控制权限, 种植了 Rootkit, 它就能维护一个后门, 允许控制者一直以管理员权限控制系统, 并且通过隐藏文件、进程、注册表项、端口等来隐藏攻击行为, 从而逃避用户和安全软件的检测[2].

隐蔽性是 Rootkit 的最大特性, 而文件系统是 Rootkit 应用的重要领域. 许多 Rootkit 需要在文件系统中存储文件, 并且要求这些文件实现隐藏. Rootkit 的文件隐藏技术有 2 种: 利用钩子技术实现文件隐藏, 这种方法效率低; 利用文件系统过滤驱动技术, 效率高, 可靠性强. 利用文件系统过滤驱动技术来实现 Rootkit 的文件隐藏, 成为当前 Windows 操作系统内核信息安全领域的热点.

1 文件系统过滤驱动工作原理

1.1 Windows 文件系统驱动

文件系统驱动程序是存储管理子系统的一个组件, 为用户提供在持久性介质上存储和读取信息的功能, 可以创建、修改和删除文件, 同时可以安全可控地在用户之间共享和传输信息, 并以适当的方式向应用程序提供结构化的文件内容[3]. 用户应用程序对磁盘上的文件进行的各种操作, 如创建、打开、关闭、读数据、写操作等, 最终都要借助文件系统驱动才能完成. 各种操作调用 Kernel32.dll, 通过 Win32 子系统调用 Native API 向内核层传送请求, 然后通过系统服务函数将上层的请求传递给 I/O 管理器, 在 I/O 管理器中, 将对磁盘文件的各种操作请求都统一为输入输出请求包 IRP, 然后向下层传送 IRP 给文件系统驱动, 最终由文件系统驱动调用磁盘及其他存储设备驱动, 进而完成对物理存储设备的各种操作. 操作完成后, 再将处理结果沿着相反路径返回, 整体执行过程如图 1 所示.

* 收稿日期: 2010-04-25
基金项目: 吉首大学校级科研课题(09JD015)
作者简介: 侯春明(1979-), 男, 湖南桑植人, 吉首大学物理科学与信息工程学院讲师, 硕士, 主要从事计算机应用与信息安全研究.

© 1994-2011 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

1.2 Windows 文件系统过滤驱动

Windows NT 操作系统的内核驱动模型 WDM (Windows Driver Model)采用了分层结构的驱动程序结构[4]. I/O 管理器实现 1 个分层的数据结构, 在 DEVICE_OBJECT 对象中保存某种关系, 自动将请求 IRP 发给设备栈中的最高的 1 个设备, 由其决定如何处理, 或是自身处理, 或是向下传递, 从而实现分层. 在 WDM 模型中, 过滤驱动程序可以在应用程序读写数据的过程中, 先于操作系统本身的文件系统驱动截获数据处理相关的 IRP, 进而进行各种相应的操作, 比如隐藏文件、修改数据等. 从图 1 可以看出, 文件系统过滤驱动位于 I/O 管理器和文件系统驱动程序之间.

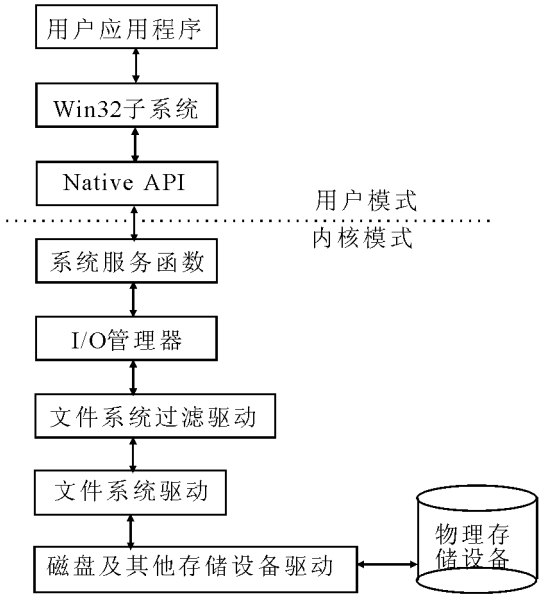

图 1 文件系统过滤驱动原理

2 基于文件系统过滤驱动的 Rootkit 隐藏技术

2.1 文件系统过滤驱动的实现

基于文件系统过滤驱动的 Rootkit 本质上就是驱动程序, 在将自身载入内核的同时, 完成特定的功能.

在 Windows 操作系统中, 对于应用最广泛的 FAT32 和 NTFS 文件系统, 主要生成 2 类设备, 一类是文件系统驱动本身生成的控制设备 CDO, 另外一类是该文件系统的卷设备. 驱动程序和应用层程序类似, 有 1 个主函数 DriverEntry, 是 Windows 驱动程序的入口函数. DriverEntry 函数由内核中 I/O 管理器负责调用. DriverEntry 的第 1 个参数是 1 个指针, 指向 1 个刚被初始化的驱动程序对象, 该对象就代表对应的驱动程序, WDM 驱动程序的 DriverEntry 例程应完成对这个对象的初始化并返回, 其主要工作是把各种函数指针填入驱动程序对象. 这些指针为操作系统指明了驱动程序容器中各种子例程的位置[5]. 针对文件系统过滤驱动的实现, 在 DriverEntry 函数中生成 1 个控制设备, 设置分发函数和快速 I/O 分发函数和回调函数, 再对文件系统的卷设备进行绑定.

在 DriverEntry 中调用内核函数 IoCreateDevice 生成文件系统控制设备 CDO, 这是文件系统过滤驱动和应用层程序的通信的主要接口. 基于文件系统过滤驱动的 Rootkit 主要利用这个 CDO 修改驱动程序的内部配置以及实现挂载和通信. CDO 生成后, 需要在 DriverEntry 中针对来自上层驱动的 IRP 设置分发函数和快速 I/O 分发函数, 然后对 Rootkit 所要监控的文件系统的卷设备进行绑定操作. 首先利用内核函数 SfAttachDeviceToDeviceStack 函数绑定文件系统控制设备, 绑定后, Rootkit 可以获得发送给文件系统控制设备的文件控制请求, 之后针对文件系统卷设备进行绑定. 在文件系统的底层, 采用物理设备对象 VPB 来表示卷控制块 VCB 和物理磁盘 Device Object 的联系(VPB 是一个重要数据结构, 用来将实际存储媒介设备对象和文件系统上的卷设备对象联系起来). 文件系统过滤驱动程序从 IRP 中获取 VPB 的指针, 进而获取文件系统的卷设备, 然后调用 SfAttachToMountedDevice 完成卷设备的绑定.

文件系统过滤驱动的绑定完成后, 基于文件系统过滤驱动的 Rootkit 被载入到内核的驱动程序设备链中, 可以针对各种操作进行过滤.

2.2 Rootkit 隐藏技术的实现

Windows 操作系统中, 磁盘等存储设备的每一个分区都被抽象成驱动程序中的设备对象(即卷设备). 卷设备是由卷管理器生成, 而不是文件系统生成, 当 1 个卷使用某种文件系统时, 该文件系统会对应的为该设备生成 1 个设备对象, 称为文件系统的卷设备. Windows 操作系统中对文件的各种操作就是通过向这些设备发送 IRP 来完成. 基于文件系统过滤驱动的 Rootkit, 首先创建驱动程序, 在驱动上生成设备对象, 然后去绑定这些卷设备, 从而实现文件系统过滤驱动程序, 发送给卷设备的 IRP, 在到达文件系统之

© 1994-2011 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

前, 被过滤驱动进行过滤, 在过滤驱动对应的例程中实现文件的隐藏.

(1) Rootkit 首先创建文件系统过滤驱动程序, 在完成对卷设备的绑定后, 使用内核函数 IoSetCompletionRoutine 为 IRP 设置完成例程, 以便在下层的文件系统驱动完成 IRP 的时候, 对返回的结果进行修改, 进而把想要的文件隐藏起来.

(2) 通过内核函数 IoCallDriver 沿着驱动程序链向下传递 IRP, 针对文件操作的每个请求最终由通过文件系统驱动完成处理. 在 IRP 到达文件系统驱动之后, 对应的操作处理完毕, IRP 返回. 在过滤驱动中对应的完成例程的处理中隐藏文件.

(3) 在 IRP 返回时执行的完成例程中可以实现对特定文件实现隐藏. 当用户在操作系统应用层查看文件时, 每个文件返回 1 个 FILE_BOTH_DIR_INFORMATION 的结构, 该结构用来描述指定目录的详细信息[6]. 用户打开的目录中所有文件返回信息形成 1 个 FILE_BOTH_DIR_INFORMATION 的结构的链表, 只要遍历这样的链表, 就可以获取当前目录下的所有文件信息, 进而显示到用户层供用户查看. 只要从链表中删除指定文件对应的节点, 指定的文件就会被隐藏. 使用链表操作中对指定节点进行删除的算法, 删除指定文件对应的节点, 则可以实现文件的隐藏.

2.3 用户层与内核层的通信

如果需要指定特定路径下特定文件名的文件被隐藏, 可以使用 DeviceControl 实现用户层程序与内核层 Rootkit 驱动程序之间的通信. 利用工作在用户层的程序, 输入需要隐藏的文件和对应的目录路径, 用在 DeviceControl 中定义的 IOCTL 控制码进行传递, 到达文件系统过滤驱动程序, 驱动中自行创建的 IRP 处理例程检测到对应的路径中的文件名后, 相关文件名信息可以传递给 IRP 的派遣函数, 用来在派遣函数中实现指定文件的隐藏.

3 Rootkit 的检测与防范

Rootkit 技术是一种中立技术, 在恶意软件和安全软件中都大量使用, 从而导致内核级 Rootkit 的检测变得非常重要. 因此, Rootkit 的检测技术也是 Window 操作系统内核信息安全领域的研究热点, Rootkit 的检测技术较多, 针对 Rootkit 隐藏相关的检测技术如下:

(1) 隐藏进程检测. 文件和进程的隐藏是内核 Rootkit 的常见功能, 大多数内核 Rootkit 都通过各种手段达到进程隐藏的目的. 检测进程隐藏的方法中最常见的是挂钩 SwapContext 方法: ntoskrnl.exe 中存在一个 SwapContext 函数, 用于将当前运行线程的上下文与重新执行线程的上下文进行交换, 在每次线程切换的时候执行. 因此, 挂钩这个函数可以得到每次线程切换时换出、换入线程的信息, 通过收集所有的线程信息, 可以进一步得到所有进程的列表.

(2) 隐藏文件的检测. 针对基于文件系统过滤驱动的 Rootkit 的文件隐藏, 可以利用直接读取磁盘扇区来分析文件系统进行隐藏文件的检测, 或者向建立在卷设备驱动上的文件系统驱动程序发送 IRP. 首先, 利用 ObReferenceObjectByName 获取文件系统驱动程序的 driver object, 然后根据用户层指定的检测路径用 DeviceControl 代码传递给 Rootkit 隐藏文件检测驱动程序, 用 CreateFile 函数打开对应的文件夹路径, 获取对应文件夹路径的句柄, 利用内核函数 ObReferenceObjectByName 可以根据对应的文件夹路径的句柄获取文件对象. 获取文件对象后, 创建 IRP, 向对应的文件系统驱动程序发送 IRP, 在返回的信息中检测所有的文件信息, 进而获取被隐藏文件.

4 结论

文件系统过滤驱动技术是近年来操作系统内核信息安全领域研究热点, 过滤驱动附着在文件系统上, 通过截获文件系统发出的 I/O 请求包来对文件系统进行各种控制操作. 内核 Rootkit 是一种基于 Windows 内核层的中立技术, 它既可以为善意的安全软件、监控软件、取证软件等服务, 也可能被病毒、木马等恶意攻击所利用. 笔者介绍了 Windows 操作系统的文件系统过滤驱动工作原理、基于文件系统过滤驱动的 Rootkit 实现文件隐藏的关键技术以及 Rootkit 的检测方法. 利用文件系统过滤驱动技术和 Rootkit 隐藏技术, 可以提高安全软件的技术性能, 并有效地防止其被恶意利用, 对 Windows 操作系统内核信息安全

© 1994-2011 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

技术应用有广泛的参考意义.

参考文献:

[1] GREG HOGLUND, JAMES BUTLER. Rootkit: Windows 内核的安全防护[M]. 北京: 清华大学出版社, 2007.
[2] 杨 平, 罗 红, 乔向东. Windows Rootkit 隐藏技术研究[J]. 计算机与信息技术, 2009(3): 73-74.
[3] NAGAR R. Windows NT File System Internals [EB/OL]. [2007-04-01]. http://download.csdn.net/source/168266.
[4] 张 帆, 史彩成. Windows 驱动开发技术详解[M]. 北京: 电子工业出版社, 2008.
[5] WALTER ONEY. Programming the Microsoft Windows Driver Mode [EB/OL]. [2008-02-15]. http://download.csdn.net/source/353955.

Research on Occultation Techniques of Kernel Rootkit Based on File System Filter Driver

HOU Chun-ming, LIU Lin
(College of Physics Science and Information Engineering, Jishou University, Jishou 416000, Hunan China)

Abstract: A Rootkit is a set of programs and code that allows a permanent or consistent, undetectable presence on a computer. Windows kernel Rootkit based on file system filter driver has been researched. The work principle of file system filter driver and the realization of filter driver and occultation techniques of kernel Rootkit based on file system filter driver have been introduced. The techniques of Rootkit detection have been discussed.

Key words: file system; Rootkit; filter driver; occultation

(责任编辑 陈炳权)

(上接第 28 页)

Maximum-Norm Superapproximation of the Triquadratic Block Finite Element Solution to the Three Dimension Problem with Variable Coefficients

DENG Yi-jun
(Department of Mathematics, Hunan International Economics College, Changsha 410205, China)

Abstract: For an variable coefficients elliptic equation in 3D, weak estimates for the block finite element over rectangular parallelepiped partitions of the domain are obtained by using three- dimensional interpolation operator of projection type and interpolating approximation properties. Furthermore, in combination with three-dimensional discrete Green functions, the author derives the maximum-norm superapproximation results with high accuracy of the displacement and gradient for block finite elements.

Key words: variable coefficients elliptic equation; block finite element; interpolation operator of projection type; discrete Green funtions; superapproximation

(责任编辑 向阳洁)

© 1994-2011 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net