

Windows 服务隐藏技术研究与实践

曹 磊, 蔡皖东

(西北工业大学 计算机学院, 陕西 西安 710072)

摘 要: 恶意程序利用 Windows 服务可以实现自启动及部分隐藏功能, 研究服务隐藏技术能够提高对此类恶意程序的检测能力. 研究了 Windows 服务的启动过程及服务对象的内部数据结构, 提出一种结合内存隐藏和注册表隐藏的多点联合隐藏方法, 设计并实现了一个基于该方法的服务隐藏程序, 在实验条件下测试了此方法的隐藏效果, 分析了应对该类型服务隐藏技术的检测策略. 实验证明该方法能够在不影响服务功能的前提下, 有效隐藏服务, 躲避各类检测工具.

关键词: Windows 服务; 服务隐藏; 内存信息隐藏; 注册表项隐藏

中图分类号: TP316

文献标识码: A

文章编号: 1000-7180(2011)12-0010-04

Research and Implementation of Windows Service Concealing Technology

CAO Lei, CAI Wan-Dong

(College of Computer, Northwestern Polytechnical University, Xi'an 710072, China)

Abstract: Malware may use Windows services to achieve auto-starting and partial concealing. In order to improve the detecting ability to such kind of malware, it is necessary to research the services concealing technology. The boot process of Windows services and the inner data structure of service object are researched, and then a multi-point concealing method combining memory hidden and registry hidden is proposed. Design and realize a service concealing program based on the method, test the hidden effect of the method in experimental conditions, analyze the detecting strategy dealing with this kinds of service concealing technology. The experiment proves that this method can hide service effectively with no influence on the service function, and evade kinds of detecting tools.

Key words: Windows service; service concealing; memory hidden; registry hidden

1 引言

随着计算机网络的普及, 恶意程序已经成为网络安全的主要威胁, 恶意程序通常利用主机操作系统服务来实现程序运行和隐藏^[1-2]. 在 Windows 操作系统中, 服务是一种特殊的应用程序, 通常独立于用户登录而运行, 由服务控制管理器(SCM)负责启动所有服务. Windows 服务分为进程共享型和进程独占型. 在进程共享型服务中, 多个服务共享一个进程, 服务程序以动态链接库的形式存在, 由服务宿主进程(Svchost \ Windows\System32\Svchost.exe)负责加载, 很多恶意程序正是利用这一特性来实现

自启动和隐藏的, 以逃避防护软件的检测与查杀. 因此, 研究服务隐藏技术, 对于改进恶意程序防护软件的性能, 提高其检测能力具有重要意义.

传统 Windows 服务隐藏技术分为两种: 系统 API 挂钩技术和直接服务操控技术. 系统 API 挂钩技术属于伪隐藏, Windows 提供了一系列 API 函数, 为应用程序提供访问系统服务信息的接口, 通过挂钩这些 API 函数可以实现服务隐藏, 该方法实现简单; 直接服务操控技术借鉴直接内核对象操作技术(DKOM)^[3], 通过直接修改系统维护的服务对象链表, 从链表中摘除需要隐藏的服务对象, 该方法依赖于操作系统未公开的内部数据结构, 实现难度大,

但隐蔽性好。

本文针对 Windows 操作系统,提出一种多点联合服务隐藏技术,通过内存信息隐藏和注册表项隐藏来实现服务隐藏,为检测该类恶意程序提供了技术原型。

2 服务隐藏方法

2.1 服务启动过程

Windows 使用注册表记录系统中安装的所有服务,在系统启动时,SCM 根据注册表中记录的服务信息建立服务数据库,为每一个服务创建一个服务对象,并使用双链表管理所有服务对象,然后启动相应服务^[4],如图 1 所示。服务信息分别存放在注册表和 SCM 进程中,可以利用这一特性来设计服务隐藏模型,结合内存信息隐藏和注册表项隐藏,实现服务信息的隐藏。

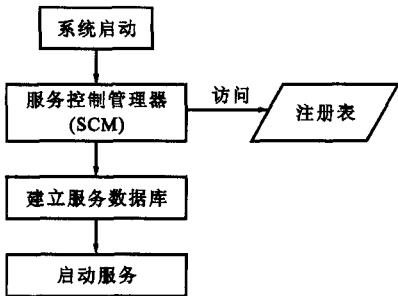


图 1 服务启动流程

2.2 内存信息隐藏方法

在 Windows 系统中,由 SCM 来管理系统中安装的所有服务。SCM 使用 ScCreateServiceDB 创建服务数据库,该服务数据库存储在进程 services.exe 的内存空间中。为了实现更好的隐蔽性,本文采用了直接服务操控技术来实施服务隐藏。使用直接服务操控技术的前提条件是必须了解服务对象在 services.exe 进程中地址及数据结构。由于它们属于不公开的操作系统内部数据结构,因此本文对 services.exe 进程进行了反复调试,发现了 Windows 下服务对象部分数据结构,如表 1 所示。

由于 Windows 所有的服务信息都存储在该双向链表中,因此可以采用“摘链法”将需要隐藏的服务条目从链表中摘除,如图 2 所示。其中,有 3 个服务对象 A、B、C,实线连接表示摘链前三个对象之间的链接关系,A 的 FLINK 指向 B,B 的 FLINK 指向 C,C 的 BLINK 指向 B,B 的 BLINK 指向 A,虚线连接表示了隐藏对象 B 后的链接关系,A 的 FLINK 指向 C,C 的 BLINK 指向 A。

表 1 服务对象部分数据结构

名称	大小/Byte	解释
FLINK	4	上一个对象指针
服务名称指针	4	服务名 UNICODE 字符串指针
服务描述指针	4	服务描述 UNICODE 字符串指针
条目编号	4	从 1 开始的连续编号
未知信息	...	...
Offset:0x60 BLINK	4	下一个对象指针
其他信息	...	...

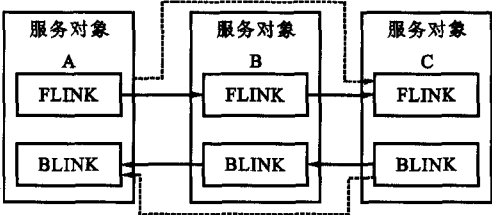


图 2 使用摘链法隐藏服务

2.3 注册表项隐藏方法

在 Windows 操作系统中,使用注册表来记录所有已经安装的服务,注册表 HKLM\System\CurrentControlSet\Services 项的每一个子键都对应一个服务。操作系统使用特殊的文件(储巢文件)来存储注册表的内容。

目前的注册表隐藏大都采用挂钩技术,根据它们不同的运行环境和模式,可以把注册表隐藏技术称为用户态下注册表隐藏技术和核心态下注册表隐藏技术。它们通常是利用 IAT Hook, Inline Hook、远程线程注入、SSDT Hook 等方式来实现,比较常见的核心态隐藏技术是 SSDT 挂钩 NtEnumerateKey 和 Inline 挂钩 CmEnumerateKey。然而这些方法已经很容易被防护软件发现。

本文提出一种新方法,通过挂钩回调函数,修改储巢内存结构中的特殊指针来实现注册表项的隐藏。在磁盘上,注册表并不是简单的一个大文件,而是一组称为储巢的单独文件。每个储巢文件包含了一棵注册表树。有一个键作为该树的根。子键和他们的值存储在根的下面,而每个储巢文件是由许多巢箱组成,一个巢箱是由很多巢室组成。为了处理内存中存放储巢数据的地址不连续的问题,配置管理器采取了一种类似 Windows 内存管理器将虚存地址映射到内存时所使用的策略。配置管理器用了一个两级系统^[5],如图 3 所示。

图 3 中,系统以一个巢室索引作为输入而后返

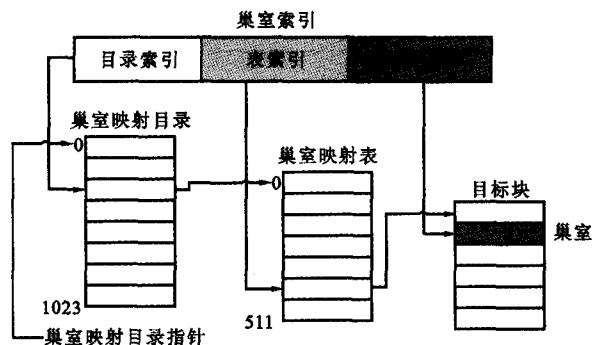


图3 Windows 储巢两级映射系统

回巢室索引所在块的内存地址以及巢室所在的块的内存地址作为输出。为了方便依据巢室的索引来计算出巢室的内存位置,在 Windows 内核提供了一个计算函数 `GetCellRoutine`。这个函数的原型为: `PVOID HvpGetCellMapped (IN PVOID Hive, OUT PVOID Cell)`,该函数的函数指针存放在一个称为 HHIVE 的结构中。

当一个应用程序打开或者创建一个注册表键时,对象管理器会给应用程序一个句柄,让它通过这个句柄来引用该键,该句柄所代表的键对象(KO)是配置管理器在对象管理器的协助下分配的。有了对象管理器的支持,配置管理器就可以利用对象管理器所提供的引用计数功能了。对于每个打开的注册表键,配置管理器还会为它分配一个键控制块(KCB),一个 KCB 中存储了该键的完整路径名、该 KCB 所对应的键节点的索引以及一个标识用以指示在该键的最后一个句柄被关闭后配置管理器是否要删除此 KCB 所对应的的键索引。Windows 将所有的 KCB 放进一个哈希表中,以便用名字对存在的 KCB 进行快速查找。一个 KO 指向一个与它相关的 KCB。

因此通过 KO 可以获取 KCB,而 KCB 中存放有该键的 keyhive,也就是前面提到的存放 `GetCellRoutine` 的 HHIVE 结构。将需要隐藏键的 `GetCellRoutine` 函数替换为钩子函数,在钩子函数中调用原来的回调函数,得到指向一个表示键的结构体的指针,如果这个指针指向需要隐藏的键,则返回该键的下一个结点,如果这个结点已经是最后一个,则返回 NULL,这样就可实现注册表隐藏了。

3 服务隐藏实现技术

3.1 内存信息隐藏实现

`services.exe` 是 SCM 对应的服务管理进程,为了隐藏服务,需要修改 `services.exe` 虚拟地址空间

中维护的双向链表。访问进程虚拟地址空间有两种方法,一种是内核模式下修改 CR3 寄存器的值,访问进程的虚拟地址空间,这种方法不够稳定,如果操作不当,就会引起系统崩溃。第二种方法是用户模式下使用远程线程注入方式,向目标进程中注入一个 DLL,在 DLL 的 `dllMain` 函数中实现目标进程的内存修改,该方式容易被防护软件发现。

如果使用远程线程注入方式修改服务链表,则必须保证注入过程是在防护软件启动之前进行,否则就会被防护软件拦截。在 Windows XP 下,使用 Windows API `CreateRemoteThread` 可以实现远程线程注入,这种方法可以注入任意进程。但在 Windows 7 下,系统增强了保护机制,不允许向系统进程进行注入,而 `services.exe` 就是系统进程。通过调试 `CreateRemoteThread` 函数,发现该函数会根据 `CsrClientCallServer` 的返回码来决定是否允许创建线程,当返回码为 0 时,允许注入。因此使用运行时补丁技术修改 `CsrClientCallServer` 的返回码,就可以成功注入系统进程。

当注入 `services.exe` 后,在其虚拟地址空间中搜索目标服务名为 UNICODE 字符串指针,找到后,判断下一个 DWORD 指针指向的 UNICODE 字符串是否是目标服务的服务描述字符串,如果是,则将该服务从双向链表上摘除。

3.2 注册表项隐藏实现

Windows 在系统启动时使用配置管理器加载储巢文件,因此储巢文件会被加载到内核空间,为了操作内核空间中的储巢文件,需要编写驱动程序进行注册表隐藏。

假设有一个字符串表示要隐藏的注册表键的完整路径,使用 `ZwOpenKey` 函数获得一个指向此注册表路径的 HANDLE,其对应的 ObjectType 是 `_CM_KEY_BODY`,其第二个成员是偏移量为 4 字节的 `KeyControlBlock`,它是一个指向结构体 `_CM_KEY_CONTROL_BLOCK` 的指针, `_CM_KEY_CONTROL_BLOCK` 结构体中偏移量为 20 字节的成员 `_HHIVE` 指向一个 `_HHIVE` 结构体,而在 `_HHIVE` 结构体中偏移量为 4 字节是 `GetCellRoutine` 函数指针,通过该函数可以根据巢室索引计算出巢室的内存地址,挂钩 `GetCellRoutine`,如果返回的巢室内存地址等于上面计算出的隐藏的巢室地址,则让其返回子键列表中下一个巢室地址;如果该键是最后一个节点,则返回 NULL。

4 隐藏测试与检测方法

4.1 服务隐藏效果测试

为了测试服务隐藏的效果,本文使用4种检测工具进行了测试,它们分别是XueTr^[6]、Windows服务配置管理器、360系统服务状态工具和IceSword^[7]冰刃v1.22,测试隐藏BITS服务,该服务是Windows提供的默认服务,负责在网络空闲时在后台传送文件,Windows自动更新依赖于该服务。运行隐藏程序隐藏BITS服务后,这4种检测工具均检测不到此服务,但Windows更新能够正常运行,达到了很好的服务隐藏效果。

4.2 服务隐藏检测方法

隐藏检测方法可以分为两类:一是Rutkowski^[8]提出的基于交叉视图的差异检测方法,该方法的依据是:总可通过多种途径来获取系统关键信息,每种途径获得的结果成为一个视图,对这些视图进行比较,判断信息是否相同,若相同则认为正常,否则就认为系统信息遭到了篡改。注册表中存储着系统中的所有服务,虽然GetCellRoutine函数已经被钩挂,但磁盘上的注册表文件并未修改,通过解析储巢文件可以获得到所有的服务信息,这是注册表视图,然后通过系统提供的API函数枚举系统中的服务,这构成API视图,对比这两个视图,即可发现隐藏的服务。二是暴力检测方法,主要利用穷举法来获取需要的系统信息,在搜索范围不大时,不失为一种有效的检测方法。前面提到的Windows服务数据库是由SCM建立并存储在services.exe进程的地址空间。因此,使用暴力检测方法来搜索services.exe进程空间,就可以枚举出系统中的所有服务。

5 结束语

本文在分析Windows服务运行原理的基础上,提出了新的服务隐藏方法,并通过编程实现了内核

级服务隐藏,该方法具有如下优点:隐蔽性好,能够绕过多种检测工具而不被发现;对系统影响小,由于服务只是被隐藏起来,并没有从系统中删除,不会影响服务正常功能。

通过对Windows服务隐藏技术的研究,有助于加深对该技术的认识,提高对恶意程序攻击的防范意识,从而进一步掌握恶意程序隐藏技术的发展方向,开发针对该类型程序的检测工具。

参考文献:

- [1] 王玲. 广告软件和间谍软件的危害与防治[J]. 微电子学与计算机, 2004, 21(9): 107-110.
- [2] 杨珂, 房鼎益, 陈晓江. 间谍软件和反间谍软件的分析与研究[J]. 微电子学与计算机, 2006, 23(8): 46-48.
- [3] Butler J. DKOM (Direct Kernel Object Manipulation) [EB/OL]. [2011-05-15]. <http://www.blackhat.com/presentations/win-usa-04/bh-win-04-butler.pdf>.
- [4] Mark E Russinovich, David A Solomon. Windows internals 5th[M]. America: Microsoft Press, 2009: 300-307.
- [5] Mark E Russinovich, David A. Solomon. Windows Internals 5th[M]. America: Microsoft Press, 2009: 269-276.
- [6] Linxer. XueTr [EB/OL]. [2011-05-10]. <http://www.xuetr.com>
- [7] Pjif. IceSword1.22 中文版 [EB/OL]. [2011-05-13]. <http://pjf.blogcn.com/diary/9956289.shtml>.
- [8] Rutkowski J K. Thoughts about cross-view based root-kit detection [EB/OL]. [2011-05-14]. <http://www.invisiblethings.org/papers/crossview-detection-thoughts.pdf>

作者简介:

曹磊 男, (1985-), 硕士研究生. 研究方向为网络信息安全.

蔡晓东 男, (1955-), 教授, 博士生导师. 研究方向为网络信息安全.