(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113779570 B
(45)授权公告日 2024.02.23

(21)申请号 202111100935.3
(22)申请日 2021.09.18
(65)同一申请的已公布的文献号
申请公布号 CN 113779570 A
(43)申请公布日 2021.12.10
(73)专利权人 深信服科技股份有限公司
地址 518055 广东省深圳市南山区学苑大道1001号南山智园A1栋一层
(72)发明人 王启超
(74)专利代理机构 深圳市深佳知识产权代理事务所(普通合伙) 44285
专利代理师 陈彦如
(51)Int.Cl.
G06F 21/55(2013.01)

(56)对比文件
CN 103019653 A,2013.04.03
KR 101358815 B1,2014.02.11
WO 2018001048 A1,2018.01.04
CN 112346946 A,2021.02.09
CN 106293969 A,2017.01.04
CN 106980575 A,2017.07.25
CN 111177623 A,2020.05.19
US 2015278515 A1,2015.10.01
US 2020193017 A1,2020.06.18
WO 2015174512 A1,2015.11.19
兰超;王静.网络攻击中的监听技术分析.兵工自动化.2007,(第07期),全文.
王晨等.基于系统内核与共享内存的守护进程实现研究.《工业控制计算机》.2020,第33卷(第3期),第115-117,121页.

审查员 张娇

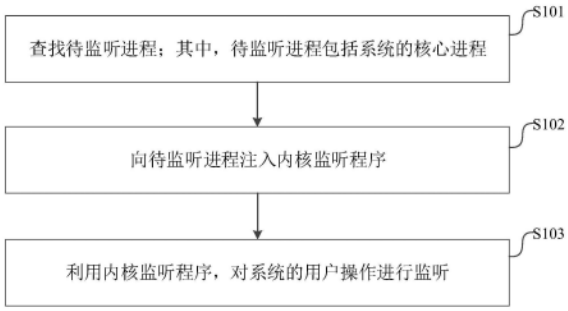
权利要求书2页 说明书10页 附图3页

(54)发明名称

一种基于核心进程的安全防护方法、装置及电子设备

(57)摘要

本发明公开了一种基于核心进程的安全防护方法、装置、电子设备及可读存储介质,该方法包括:查找待监听进程;其中,待监听进程包括系统的核心进程;向待监听进程注入内核监听程序;利用内核监听程序,对系统的用户操作进行监听;本发明通过向待监听进程注入内核监听程序,对系统的核心进程进行内核级注入,以利用核心进程中注入的内核监听程序的运行,对系统的用户操作进行监听,从而能够减少安全管理软件的监管功能被误杀、禁用、卸载和粉碎等情况发生,提升了终端的信息安全能力。



CN 113779570 B

1.一种基于核心进程的安全防护方法,其特征在于,包括:

根据系统中进程的状态信息,查找待监听进程;其中,所述待监听进程包括所述系统的核心进程,所述状态信息为内核执行体状态,所述状态信息包括保护状态信息和使用状态信息,所述待监听进程的状态信息中的保护状态信息为受保护状态且使用状态信息不为退出状态;

向所述待监听进程注入内核监听程序;

利用所述内核监听程序,对所述系统的用户操作进行监听。

2.根据权利要求1所述的基于核心进程的安全防护方法,其特征在于,所述根据系统中进程的状态信息,查找待监听进程,包括:

查找所述系统中的全部目标监听进程;其中,所述目标监听进程包括所述系统的全部进程中目标类的核心进程;

根据所述目标监听进程的命令行和/或令牌信息,对所述目标监听进程进行过滤,得到筛选进程;

根据所述筛选进程的状态信息,确定所述筛选进程中的待监听进程。

3.根据权利要求2所述的基于核心进程的安全防护方法,其特征在于,所述根据所述目标监听进程的命令行和/或令牌信息,对所述目标监听进程进行过滤,得到筛选进程,包括:

根据所述目标监听进程的命令行,过滤得到所述筛选进程中的高权限进程;其中,所述高权限进程的命令行中包括预设的高权限命令行;

根据所述高权限进程的令牌信息,过滤得到所述高权限进程中的筛选进程。

4.根据权利要求2所述的基于核心进程的安全防护方法,其特征在于,所述待监听进程为所述系统的任一核心进程时,所述根据所述筛选进程的状态信息,确定所述筛选进程中的待监听进程,包括:

根据当前筛选进程的ID,获取当前筛选进程的内核执行体;其中,当前筛选进程为任一所述筛选进程;

根据所述内核执行体,确定当前状态信息;其中,当前状态信息为当前筛选进程对应的状态信息;

若当前状态信息中的保护状态信息为受保护状态且使用状态信息不为退出状态,则将当前筛选进程确定为所述待监听进程,并执行所述向所述待监听进程注入内核监听程序以及后续的步骤;

若当前状态信息中的保护状态信息不为受保护状态或使用状态信息为退出状态,则将下一筛选进程作为当前筛选进程,并执行所述根据当前筛选进程的ID,获取当前筛选进程的内核执行体以及后续的步骤。

5.根据权利要求1所述的基于核心进程的安全防护方法,其特征在于,所述利用所述内核监听程序,对所述系统的用户操作进行监听之后,还包括:

判断当前销毁进程是否为所述待监听进程;

若是,则执行所述查找待监听进程以及后续的步骤。

6.根据权利要求1所述的基于核心进程的安全防护方法,其特征在于,所述待监听进程为所述系统的任一核心进程时,所述根据系统中进程的状态信息,查找待监听进程之后,还包括:

若未查找到所述待监听进程,则判断当前创建进程是否为所述待监听进程;

若是,则执行所述向所述待监听进程注入内核监听程序以及后续的步骤。

7.根据权利要求1至6任一项所述的基于核心进程的安全防护方法,其特征在于,所述向所述待监听进程注入内核监听程序,包括:

向所述待监听进程创建新的线程;

利用所述线程向所述待监听进程对应的应用层目标存储空间注入所述内核监听程序。

8.一种基于核心进程的安全防护装置,其特征在于,包括:

进程查找模块,用于根据系统中进程的状态信息,查找待监听进程;其中,所述待监听进程包括所述系统的核心进程,所述状态信息为内核执行体状态,所述状态信息包括保护状态信息和使用状态信息,所述待监听进程的状态信息中的保护状态信息为受保护状态且使用状态信息不为退出状态;

程序注入模块,用于向所述待监听进程注入内核监听程序;

监听模块,用于利用所述内核监听程序,对所述系统的用户操作进行监听。

9.一种电子设备,其特征在于,包括:

存储器,用于存储计算机程序;

处理器,用于执行所述计算机程序时实现如权利要求1至7任一项所述的基于核心进程的安全防护方法的步骤。

10.一种可读存储介质,其特征在于,所述可读存储介质上存储有计算机程序,所述计算机程序被处理器执行时实现如权利要求1至7任一项所述的基于核心进程的安全防护方法的步骤。

一种基于核心进程的安全防护方法、装置及电子设备

技术领域

[0001] 本发明涉及软件服务技术领域,特别涉及一种基于核心进程的安全防护方法、装置、电子设备及可读存储介质。

背景技术

[0002] 目前,通常在需要管理的终端上安装安全管理软件来对其面临的安全风险进行监控和防御,然而在终端上安装安全管理软件会面临被终端上安装的杀毒软件禁用、杀死、卸载或粉碎等问题,导致安全管理软件不能用。

[0003] 因此,如何能够减少安全管理软件被禁用、杀死、卸载或粉碎等问题的出现,提升终端的信息安全能力,是现今急需解决的问题。

发明内容

[0004] 本发明的目的是提供一种基于核心进程的安全防护方法、装置、电子设备及可读存储介质,以减少安全管理软件被禁用、杀死、卸载或粉碎等问题的出现,提升终端的信息安全能力。

[0005] 为解决上述技术问题,本发明提供一种基于核心进程的安全防护方法,包括:

[0006] 查找待监听进程;其中,所述待监听进程包括系统的核心进程;

[0007] 向所述待监听进程注入内核监听程序;

[0008] 利用所述内核监听程序,对所述系统的用户操作进行监听。

[0009] 可选的,所述查找待监听进程,包括:

[0010] 查找所述系统中的全部目标监听进程;其中,所述目标监听进程包括所述系统的全部进程中目标类的核心进程;

[0011] 根据所述目标监听进程的命令行和/或令牌信息,对所述目标监听进程进行过滤,得到筛选进程;

[0012] 根据所述筛选进程的状态信息,确定所述筛选进程中的待监听进程;其中,所述状态信息包括保护状态信息和/或使用状态信息。

[0013] 可选的,所述根据所述目标监听进程的命令行和/或令牌信息,对所述目标监听进程进行过滤,得到筛选进程,包括:

[0014] 根据所述目标监听进程的命令行,过滤得到所述筛选进程中的高权限进程;其中,所述高权限进程的命令行中包括预设的高权限命令行;

[0015] 根据所述高权限进程的令牌信息,过滤得到所述高权限进程中的筛选进程。

[0016] 可选的,所述待监听进程为所述系统的任一核心进程时,所述根据所述筛选进程的状态信息,确定所述筛选进程中的待监听进程,包括:

[0017] 根据当前筛选进程的ID,获取当前筛选进程的内核执行体;其中,当前筛选进程为任一所述筛选进程;

[0018] 根据所述内核执行体,确定当前状态信息;其中,当前状态信息为当前筛选进程对

应的状态信息；

[0019] 若当前状态信息中的保护状态信息为受保护状态且使用状态信息不为退出状态，则将当前筛选进程确定为所述待监听进程，并执行所述向所述待监听进程注入内核监听程序以及后续的步骤；

[0020] 若当前状态信息中的保护状态信息不为受保护状态或使用状态信息为退出状态，则将下一筛选进程作为当前筛选进程，并执行所述根据当前筛选进程的ID，获取当前筛选进程的内核执行体以及后续的步骤。

[0021] 可选的，所述利用所述内核监听程序，对所述系统的用户操作进行监听之后，还包括：

[0022] 判断当前销毁进程是否为所述待监听进程；

[0023] 若是，则执行所述查找待监听进程以及后续的步骤。

[0024] 可选的，所述待监听进程为所述系统的任一核心进程时，所述查找待监听进程之后，还包括：

[0025] 若未查找到所述待监听进程，则判断当前创建进程是否为所述待监听进程；

[0026] 若是，则执行所述向所述待监听进程注入内核监听程序以及后续的步骤。

[0027] 可选的，所述向所述待监听进程注入内核监听程序，包括：

[0028] 向所述待监听进程创建新的线程；

[0029] 利用所述线程向所述待监听进程对应的应用层目标存储空间注入所述内核监听程序。

[0030] 本发明还提供了一种基于核心进程的安全防护装置，包括：

[0031] 进程查找模块，用于查找待监听进程；其中，所述待监听进程包括系统的核心进程；

[0032] 程序注入模块，用于向所述待监听进程注入内核监听程序；

[0033] 监听模块，用于利用所述内核监听程序，对所述系统的用户操作进行监听。

[0034] 本发明还提供了一种电子设备，包括：

[0035] 存储器，用于存储计算机程序；

[0036] 处理器，用于执行所述计算机程序时实现如上述所述的基于核心进程的安全防护方法的步骤。

[0037] 此外，本发明还提供了一种可读存储介质，所述可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现如上述所述的基于核心进程的安全防护方法的步骤。

[0038] 本发明所提供的一种基于核心进程的安全防护方法，包括：查找待监听进程；其中，待监听进程包括系统的核心进程；向待监听进程注入内核监听程序；利用内核监听程序，对系统的用户操作进行监听；

[0039] 可见，本发明通过向待监听进程注入内核监听程序，对系统的核心进程进行内核级注入，以利用核心进程中注入的内核监听程序的运行，对系统的用户操作进行监听，从而能够减少安全管理软件被禁用、杀死、卸载或粉碎等问题的出现，提升终端的信息安全能力。此外，本发明还提供了一种基于核心进程的安全防护装置、电子设备及可读存储介质，同样具有上述有益效果。

附图说明

[0040] 为了更清楚地说明本发明实施例或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本发明的实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据提供的附图获得其他的附图。

[0041] 图1为本发明实施例所提供的一种基于核心进程的安全防护方法的流程图;

[0042] 图2为本发明实施例所提供的另一种基于核心进程的安全防护方法中查找待监听进程的流程图;

[0043] 图3为本发明实施例所提供的一种基于核心进程的安全防护装置的结构框图;

[0044] 图4为本发明实施例所提供的一种电子设备的结构示意图;

[0045] 图5为本发明实施例所提供的一种电子设备的具体结构示意图。

具体实施方式

[0046] 为使本发明实施例的目的、技术方案和优点更加清楚,下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本发明保护的范围。

[0047] 请参考图1,图1为本发明实施例所提供的一种基于核心进程的安全防护方法的流程图。该方法可以包括:

[0048] 步骤101:查找待监听进程;其中,待监听进程包括系统的核心进程。

[0049] 可以理解的是,本步骤中的待监听进程可以为电子设备的系统(即操作系统)中需要注入内核监听程序的进程,即需要运行注入的内核监听程序监听系统中的用户操作的进程。也就是说,本步骤中电子设备可以通过查找待监听进程,确定系统中需要注入内核监听程序的进程。

[0050] 具体的,对于本步骤中待监听进程的具体数量和类型的设置,可以由设计人员根据使用场景和用户需求自行设置,如待监听进程可以包括系统的核心进程,以利用系统的核心进程监听系统的用户操作;例如待监听进程可以为系统中一个的核心进程,待监听进程也可以为系统中一类或多类的核心进程中的全部进程;待监听进程还可以包括系统的非核心进程,以利用系统的核心进程的非核心进程监听系统的用户操作,本实施例对此不做任何限制。

[0051] 需要说明的是,对于本步骤中电子设备查找待监听进程的具体方式,可以由设计人员根据实用场景和用户需求自行设置,如电子设备可以根据进程的命令行和/或令牌信息,查找出系统中的待监听进程;例如待监听进程需要较高权限且具备网络通信能力时,电子设备可以根据进程的命令行和令牌信息,从系统的全部核心进程中过滤得到命令行中包括预设的高权限命令行且令牌信息中包括网络令牌的进程(即筛选进程),从而从筛选进程中确定待监听进程,如将第一个过滤得到筛选进程确定为待监听进程,或将全部筛选进程确定为待监听进程,或从全部筛选进程的各类核心进程中分别确定出一个待监听进程。为了减少查找待监听进程的运算量,本步骤中电子设备可以从系统目标类的核心进程中查找待监听进程,即预先设置待监听进程的进程类型(即目标类),如svchost.exe。电子设备还

可以根据进程的状态信息(如内核执行体状态),查找系统中的待监听进程;例如为了保证查找的待监听进程能够平稳注入且长时间运行内核监听程序,电子设备可以根据进程的状态信息中的保护状态信息和使用状态信息,从筛选进程中过滤查找出保护状态信息为受保护状态且使用状态信息不为退出状态的待监听进程,如将过滤查找出的第一个筛选进程确定为待监听进程。只要电子设备能够从系统的全部进程中查找出待监听进程,本实施例对此不做任何限制。

[0052] 需要说明的是,本步骤之前电子设备还可以检测系统是否已经完成监听,即之前已经完成了全部待监听进程的注入,从而在系统未完成监听时,进入步骤101,完成系统的监听;在系统监听时,结束本流程,避免待监听进程的重复注入。如待监听进程为目标类的核心进程时,电子设备获取系统中的目标监听进程的内核监听程序注入情况;根据内核监听程序注入情况,判断系统是否完成监听;若否,则执行步骤101以及后续的步骤102和步骤103;若是,则结束本流程;其中,目标监听进程为系统的全部进程中目标类的核心进程。

[0053] 例如,系统为Windows系统的WinVista及以上系统时,电子设备可以利用ZwQuerySystemInformation函数(Windows系统中的一种函数)获取系统中所有进程的列表,利用该列表遍历查找得到系统中的全部目标监听进程;获取所有目标监听进程的PEB(进程环境描述块),通过PEB获取各目标监听进程的模块链表;利用模块链表,获取目标监听进程的内核监听程序注入情况;根据内核监听程序注入情况,判断系统是否完成监听,如待监听进程为一个核心进程时,可以判断内核监听程序注入情况中是否存在注入内核监听程序,从而在检测到内核监听程序注入情况中存在注入内核监听程序的进程时,确定系统完成监听。

[0054] 步骤102:向待监听进程注入内核监听程序。

[0055] 其中,本步骤中的内核监听程序可以为能够在被注入该内核监听程序的进程运行,监听系统的用户操作的内核级文件,如dll文件。也就是说,本步骤中通过向待监听进程注入内核监听程序,实现对系统的核心进程进行内核级注入,使得后续待监听进程能够运行内核监听程序,监听系统的用户操作。

[0056] 具体的,对于本步骤中电子设备向待监听进程注入内核监听程序的具体方式,可以由设计人员根据实用场景和用户需求自行设置,如可以根据电子设备的系统(即操作系统)的版本和类型对应进行设置,如系统为Windows系统的WinVista及以上系统时,电子设备可以利用NtCreateThreadEx函数(Windows系统中的一种函数)、目标机器码、LdrLoadDll函数(Windows系统中的一种函数)、线程的PreviousMode参数(Windows系统中的一种属性参数)和待监听进程对应的应用层目标存储空间,将内核监听程序注入到应用层目标存储空间;其中,目标机器码为待监听进程的位数(如32位或64位)对应的预设机器码。对应的,电子设备可以通过上述方式完成内核级的待监听进程的注入,电子设备也可以使用应用层进行待监听进程的,如利用SYSTEM权限的注入器完成待监听进程的注入。只要电子设备可以将内核监听程序注入到待监听进程,本实施例对此不做任何限制。

[0057] 可以理解的是,本实施例中电子设备可以通过运行预先安装的内核级驱动程序(如Windows内核级驱动程序),执行本实施例所提供的基于核心进程的安全防护方法,完成待监听进程的查找和注入。

[0058] 步骤103:利用内核监听程序,对系统的用户操作进行监听。

[0059] 可以理解的是,本步骤中的电子设备可以利用待监听进程中注入的内核监听程序的运行,对系统的用户操作进行监听,从而实现安全管理软件的监管功能,通过待监听进程对内核监听程序的运行,可以减少内核监听程序被误杀、禁用、卸载和粉碎等情况的发生。

[0060] 具体的,本步骤中的用户操作可以为操作系统中需要进行监听用户的操作行为。对本步骤中电子设备利用内核监听程序,所需要监听的用户操作的具体设置,可以由设计人员根据实用场景和用户需求自行设置,如根据企业端客户的监管需求对应进行设置,例如监听的系统的用户操作可以包括办公软件和非办公软件的启动和关闭等操作。

[0061] 对应的,本实施例中电子设备还可以利用待监听程序运行过程中的用户操作,并将用户操作发送到管理设备(如服务器)。

[0062] 本实施例中,本发明实施例通过向待监听进程注入内核监听程序,对系统的核心进程进行内核级注入,以利用核心进程中注入的内核监听程序的运行,对系统的用户操作进行监听,从而能够减少安全管理软件被禁用、杀死、卸载或粉碎等问题的出现,提升终端的信息安全能力。

[0063] 基于上述实施例,本实施例将对上述实施例中的若干步骤进行具体阐述。请参考图2,图2为本发明实施例所提供的另一种基于核心进程的安全防护方法中查找待监听进程的流程图。

[0064] 从系统中查找待监听进程的方式包括但不限于下述方式:

[0065] 步骤201:查找系统中的全部目标监听进程;其中,目标监听进程包括系统的全部进程中目标类的核心进程。

[0066] 可以理解的是,本步骤中电子设备可以从系统的全部进程中查找出目标进程类型(即目标类)的核心进程(即目标监听进程),从而能够从目标监听进程中查找出待监听进程,减少待监听进程的查找运算量。

[0067] 对应的,本步骤中的目标类可以为预先设置的能够作为待监听进程的核心进程的进程类型。对于目标监听进程的具体进程类型设置,即目标类的具体数量和进程类型,可以由设计人员根据实用场景和用户需求自行设置,如目标监听进程可以为一种核心进程,即目标类可以为一种核心进程的进程类型,例如目标监听进程可以为svchost.exe(Windows系统中的一种核心进程)进程,即目标类可以包括svchost.exe进程的进程类型;目标监听进程可以包括多种核心进程,即目标类可以包括多种核心进程的进程类型,例如目标监听进程包括csrss.exe进程(Windows系统中的一种核心进程)和svchost.exe进程。本实施例对此不做任何限制。

[0068] 具体的,本实施例并不限定电子设备查找系统中的全部目标监听进程的具体方式,如电子设备可以先获取系统中所有进程的列表,再遍历查找得到系统中的全部目标监听进程;例如系统为Windows系统的WinVista及以上系统时,电子设备可以利用ZwQuerySystemInformation函数(Windows系统中的一种函数)获取系统中所有进程的列表,利用该列表遍历查找得到系统中的全部目标监听进程,如全部svchost.exe进程。

[0069] 步骤202:根据目标监听进程的命令行和/或令牌信息,对目标监听进程进行过滤,得到筛选进程。

[0070] 其中,本步骤中电子设备可以根据各目标监听进程的命令行和/或令牌信息,过滤出符合要求的进程(即筛选进程)。如待监听进程需要较高权限且具备网络通信能力时,电

子设备可以根据目标监听进程的命令行和令牌信息,从目标监听进程中过滤得到包括预设的高权限命令行(如netsvcs命令行)且令牌信息中包括网络令牌的进程(即筛选进程);例如电子设备可以根据目标监听进程的命令行,过滤得到筛选进程中的高权限进程;根据高权限进程的令牌信息,过滤得到高权限进程中的筛选进程;其中,高权限进程的命令行中包括预设的高权限命令行;筛选进程的令牌信息中可以包括网络令牌。

[0071] 步骤203:根据筛选进程的状态信息,确定筛选进程中的待监听进程;其中,状态信息包括保护状态信息和/或使用状态信息。

[0072] 可以理解的是,本步骤中电子设备可以根据步骤202过滤得到筛选进程的状态信息,从筛选进程确定出状态符合要求的进程(即待监听进程)。如为了保证查找的待监听进程能够平稳注入内核监听程序且长时间运行内核监听程序,本步骤中的状态信息包括保护状态信息和使用状态信息,以根据筛选进程的状态信息,确定筛选进程中保护状态信息为受保护状态且使用状态信息不为退出状态的进程(即待监听进程)。

[0073] 具体的,对于本步骤中电子设备根据筛选进程的状态信息,确定筛选进程中的待监听进程的具体方式,可以由设计人员自行设置,如待监听进程的数量为1时,处理器可以根据当前筛选进程的ID,获取当前筛选进程的内核执行体;根据内核执行体,确定当前状态信息;若当前状态信息中的保护状态信息为受保护状态且使用状态信息不为退出状态,则将当前筛选进程确定为待监听进程,并继续执行步骤102和后续的步骤103;若当前状态信息中的保护状态信息不为受保护状态或使用状态信息为退出状态,则将下一筛选进程作为当前筛选进程,并可以返回执行根据当前筛选进程的ID,获取当前筛选进程的内核执行体的步骤以及后续根据内核执行体,确定当前状态信息的步骤,直至确定得到待监听进程,从而继续执行步骤102和步骤103,实现对系统的用户操作的监听;其中,当前筛选进程为任一筛选进程,当前状态信息为当前筛选进程对应的状态信息。也就是说,电子设备可以通过筛选进程的ID,获得筛选进程的内核执行体;利用该内核执行体,判断该筛选进程是否为受保护进程和该筛选进程是否正在退出,从而将不为受保护进程且不处于退出状态的筛选进程确定为待监听进程;否则,继续通过下一筛选进程的ID,获得筛选进程的内核执行体并进行判断。

[0074] 需要说明的是,本实施例并不限定步骤202与步骤203的逻辑先后顺序,如可以在步骤202完成后再进入步骤203,例如本实施例中可以在步骤202中过滤完成得到全部筛选进程后,再进入步骤203,确定待监听进程;也可以在步骤202执行过程中进入步骤203,例如待监听进程的数量为1时,电子设备可以在步骤202中过滤得到一个筛选进程后,便通过步骤203,判断该筛选进程是否为待监听进程。

[0075] 基于上述实施例,本实施例将对上述实施例中的若干步骤进行具体阐述。上述实施例中向待监听进程注入内核监听程序的过程可以包括:

[0076] 向待监听进程创建新的线程;利用该线程向待监听进程对应的应用层目标存储空间注入内核监听程序。

[0077] 其中,应用层目标存储空间注入内核监听程序可以为向待监听进程申请的用于存放注入的内核监听程序的应用层内存的基址。

[0078] 具体的,电子设备可以利用线程配置参数和内核创建文件函数,向待监听进程创建新的线程;利用该线程通过目标机器码调用模块加载函数,向应用层目标存储空间注入

内核监听程序;其中,目标机器码可以为待监听进程的位数对应的预设机器码。例如,电子设备的系统为Windows系统(如WinVista及以上系统)时,电子设备可以将线程的PreviousMode参数(即线程配置参数)设置为0,利用NtCreateThreadEx函数(即内核创建文件函数)创建新的线程;利用新创建的线程通过目标机器码(如shellcode)调用LdrLoadDll函数(即模块加载函数)向应用层目标存储空间注入内核监听程序。

[0079] 相应的,本实施例所提供的基于核心进程的安全防护方法还可以包括内核创建文件函数、目标机器码、模块加载函数、线程的线程配置参数和待监听进程对应的应用层目标存储空间的获取过程。

[0080] 其中,线程的线程配置参数为Windows系统中的PreviousMode参数时,线程的线程配置参数的获取过程可以包括:获取系统的操作系统版本;判断该操作系统版本是否为预设操作系统版本(如WinVista及以上系统的版本号);若为预设操作系统版本,则利用该操作系统版本,获取该操作系统版本对应的预设的PreviousMode参数的偏移位置;根据该偏移位置,获取PreviousMode参数;若不为预设操作系统版本,则可以直接结束本流程。也就是说,本实施例中可以预先设置各操作系统版本对应的PreviousMode参数的偏移位置,如使用调试工具WinDbg提前获得TEB(Thread Environment Block,线程环境块)成员PreviousMode的偏移位置。

[0081] 对应的,内核创建文件函数为Windows系统中的NtCreateThreadEx函数时,内核创建文件函数的获取过程可以包括:获取系统的系统服务描述符表;查找NtCreateThreadEx函数在系统服务描述符表(SSDT,System Services Descriptor Table)中的索引;利用索引,获取NtCreateThreadEx函数。

[0082] 例如电子设备可以先通过__readmsr(0xC0000082)指令,获取KiSystemCall64函数的基地址;利用相应的特征码(attribute code)从KiSystemCall64Shadow的基地址向上查找SSDT的地址(即KSERVICE_TABLE_DESCRIPTOR地址);在上述方式未查找到SSDT的地址时,再获取NtOpenFile函数(一种内核级函数);利用NtOpenFile函数枚举所有内核模块,获得模块信息(如模块基址和大小等);遍历所有模块信息,获得ntoskrnl.exe模块的基址;利用相应的特征码,从ntoskrnl.exe模块中查找SSDT的地址。电子设备可以查找NtCreateThreadEx函数在SSDT中的索引的过程可以为先在内核层创建\SystemRoot\System32\ntdll.dll模块的内存映象(Section);再使用PE(Portable Executable,可移植的执行体)文件结构查找NtCreateThreadEx函数的实现;之后通过相应的特征码匹配,查找该NtCreateThreadEx函数在内核层SSDT上的索引。

[0083] 具体的,电子设备的系统为Windows系统时,目标机器码的获取过程可以包括:确定的待监听进程的位数(如32位或64位);将待监听进程的位数对应的预设机器码确定为目标机器码。例如电子设备的系统为32位系统时,可以确定待监听进程的位数为32;电子设备的系统为64位系统时,可以使用PsGetProcessWow64Process函数,获取进程的Wow64PEB,从而确定待监听进程是否为32位进程运行在64位系统下;若是,则确定待监听进程的位数为32;若否,则确定待监听进程的位数为64。相应的,本实施例中可以预先设置32位进程和64位进程各自的对应的机器码(即预设机器码)。

[0084] 其中,模块加载函数为Windows系统中的LdrLoadDll函数时,模块加载函数的获取过程可以包括:利用待监听进程的(进程环境描述块),获取待监听进程的模块链表;利用模

块链表,查找ntdll.dll核心模块映象;利用ntdll.dll获取应用层LdrLoadDll函数的地址。

[0085] 相应的,待监听进程对应的应用层目标存储空间的获取过程可以包括:向待监听进程申请应用层内存(即应用层目标存储空间),用于存放注入的内核监听程序的基址。

[0086] 基于上述实施例,本实施例所提供的基于核心进程的安全防护方法还可以包括:进程销毁回调过程,以在待监听进程销毁后,查找新的待监听进程,并注入内核监听程序,以提高安全管理软件的监管功能的健壮性。

[0087] 具体的,本实施例中电子设备可以在检测到被销毁的进程(即销毁进程)时,判断当前检测到的销毁进程(即当前销毁进程)是否为待监听进程;若否,则可以结束本流程,或继续检测销毁进程;若是,则可以执行步骤101以及后续的步骤102和步骤103,以查找新的待监听进程并注入内核监听程序,从而替换被销毁的待监听进程;例如当前销毁进程为待监听进程时,可以直接进入步骤203,继续从筛选进程中的待监听进程,从而在筛选确定待监听进程后,继续执行步骤102和步骤103,实现对系统的用户操作的监听。

[0088] 对应的,本实施例所提供的基于核心进程的安全防护方法还可以包括:进程创建回调过程,以在当前不能从系统的进程中查找到待监听进程时,可以检测新创建的进程(即创建进程),并判断当前检测到的新创建的进程(即当前创建进程)是否为待监听进程;若否,则可以结束本流程,或继续检测创建进程;若是,则可以继续执行步骤102以及后续的步骤103。例如在进程销毁回调过程中若当前销毁进程为待监听进程且查找不到新的待监听进程时,可以记录空进程标志,以使进程创建回调过程中电子设备直接可以根据空进程标志,确定未查找到待监听进程,从而判断当前创建进程是否为待监听进程。

[0089] 相应于上面的方法实施例,本发明实施例还提供了一种基于核心进程的安全防护装置,下文描述的一种基于核心进程的安全防护装置与上文描述的一种基于核心进程的安全防护方法可相互对应参照。

[0090] 请参考图3,图3为本发明实施例所提供的一种基于核心进程的安全防护装置的结构框图。该装置可以包括:

[0091] 进程查找模块10,用于查找待监听进程;其中,待监听进程包括系统的核心进程;

[0092] 程序注入模块20,用于向待监听进程注入内核监听程序;

[0093] 监听模块30,用于利用内核监听程序,对系统的用户操作进行监听。

[0094] 可选的,进程查找模块10可以包括:

[0095] 目标查找子模块,用于查找系统中的全部目标监听进程;其中,目标监听进程包括系统的全部进程中目标类的核心进程;

[0096] 过滤子模块,用于根据目标监听进程的命令行和/或令牌信息,对目标监听进程进行过滤,得到筛选进程;

[0097] 确定子模块,用于根据筛选进程的状态信息,确定筛选进程中的待监听进程;其中,状态信息包括保护状态信息和/或使用状态信息。

[0098] 可选的,过滤子模块可以包括:

[0099] 第一过滤单元,用于根据目标监听进程的命令行,过滤得到筛选进程中的高权限进程;其中,高权限进程的命令行中包括预设的高权限命令行;

[0100] 第二过滤单元,用于根据高权限进程的令牌信息,过滤得到高权限进程中的筛选进程。

[0101] 可选的,待监听进程为系统的任一核心进程时,确定子模块可以包括:

[0102] 执行体获取单元,用于根据当前筛选进程的ID,获取当前筛选进程的内核执行体;其中,当前筛选进程为任一筛选进程;

[0103] 状态确定单元,用于根据内核执行体,确定当前状态信息;其中,当前状态信息为当前筛选进程对应的状态信息;

[0104] 第一确定单元,用于若当前状态信息中的保护状态信息为受保护状态且使用状态信息不为退出状态,则将当前筛选进程确定为待监听进程,并向程序注入模块20发送启动信号;

[0105] 第二确定单元,用于若当前状态信息中的保护状态信息不为受保护状态或使用状态信息为退出状态,则将下一筛选进程作为当前筛选进程,并向执行体获取单元发送启动信号。

[0106] 可选的,该装置还可以包括:

[0107] 销毁回调模块,用于判断当前销毁进程是否为待监听进程;若是,则向进程查找模块10发送启动信号。

[0108] 可选的,待监听进程为系统的任一核心进程时,该装置还可以包括:

[0109] 创建回调模块,用于若未查找到待监听进程,则判断当前创建进程是否为待监听进程;若是,则向程序注入模块20发送启动信号。

[0110] 可选的,程序注入模块20可以包括:

[0111] 线程创建子模块,用于向待监听进程创建新的线程;

[0112] 程序注入子模块,用于利用线程向待监听进程对应的应用层目标存储空间注入内核监听程序。

[0113] 本实施例中,本发明实施例通过程序注入模块20向待监听进程注入内核监听程序,对系统的核心进程进行内核级注入,以利用核心进程中注入的内核监听程序的运行,对系统的用户操作进行监听,从而能够减少安全管理软件被禁用、杀死、卸载或粉碎等问题的出现,提升终端的信息安全能力。

[0114] 相应于上面的方法实施例,本发明实施例还提供了一种电子设备,下文描述的一种电子设备与上文描述的一种基于核心进程的安全防护方法可相互对应参照。

[0115] 请参考图4,图4为本发明实施例所提供的一种电子设备的结构示意图。该电子设备可以包括:

[0116] 存储器D1,用于存储计算机程序;

[0117] 处理器D2,用于执行计算机程序时实现上述方法实施例所提供的基于核心进程的安全防护方法的步骤。

[0118] 具体的,请参考图5,图5为本发明实施例所提供的一种电子设备的具体结构示意图,该电子设备310可因配置或性能不同而产生比较大的差异,可以包括一个或一个以上处理器(central processing units,CPU)322(例如,一个或一个以上处理器)和存储器332,一个或一个以上存储应用程序342或数据344的存储介质330(例如一个或一个以上海量存储设备)。其中,存储器332和存储介质330可以是短暂存储或持久存储。存储在存储介质330的程序可以包括一个或一个以上模块(图示没标出),每个模块可以包括对数据处理设备中的一系列指令操作。更进一步地,中央处理器322可以设置为与存储介质330通信,在电子设

备310上执行存储介质330中的一系列指令操作。

[0119] 电子设备310还可以包括一个或一个以上电源326,一个或一个以上有线或无线网络接口350,一个或一个以上输入输出接口358,和/或,一个或一个以上操作系统341。例如,Windows系统。

[0120] 上文所描述的基于核心进程的安全防护方法中的步骤可以由电子设备的结构实现。

[0121] 相应于上面的方法实施例,本发明实施例还提供了一种可读存储介质,下文描述的一种可读存储介质与上文描述的一种基于核心进程的安全防护方法可相互对应参照。

[0122] 一种可读存储介质,可读存储介质上存储有计算机程序,计算机程序被处理器执行时实现上述方法实施例所提供的基于核心进程的安全防护方法的步骤。

[0123] 该可读存储介质具体可以为U盘、移动硬盘、只读存储器(Read-Only Memory,ROM)、随机存取存储器(Random Access Memory,RAM)、磁碟或者光盘等各种可存储程序代码的可读存储介质。

[0124] 说明书中各个实施例采用递进的方式描述,每个实施例重点说明的都是与其他实施例的不同之处,各个实施例之间相同相似部分互相参见即可。对于实施例公开的装置、电子设备及可读存储介质而言,由于其与实施例公开的方法相对应,所以描述的比较简单,相关之处参见方法部分说明即可。

[0125] 以上对本发明所提供的一种基于核心进程的安全防护方法、装置、电子设备及可读存储介质进行了详细介绍。本文中应用了具体个例对本发明的原理及实施方式进行了阐述,以上实施例的说明只是用于帮助理解本发明的方法及其核心思想。应当指出,对于本技术领域的普通技术人员来说,在不脱离本发明原理的前提下,还可以对本发明进行若干改进和修饰,这些改进和修饰也落入本发明权利要求的保护范围内。

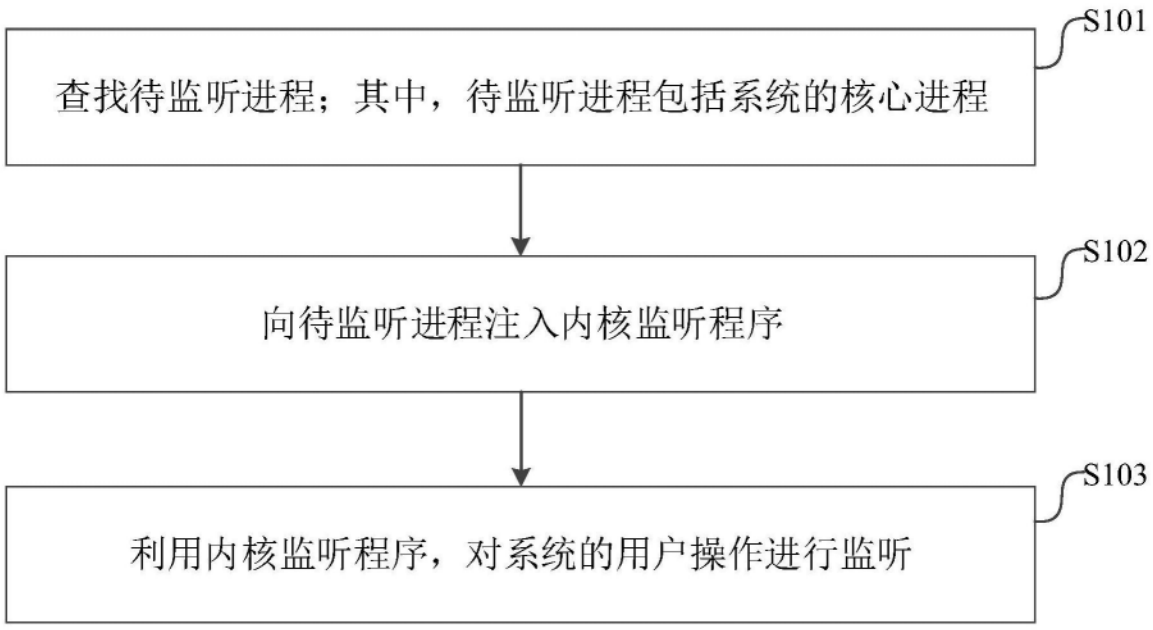

S101
查找待监听进程；其中，待监听进程包括系统的核心进程
S102
向待监听进程注入内核监听程序
S103
利用内核监听程序，对系统的用户操作进行监听

图1

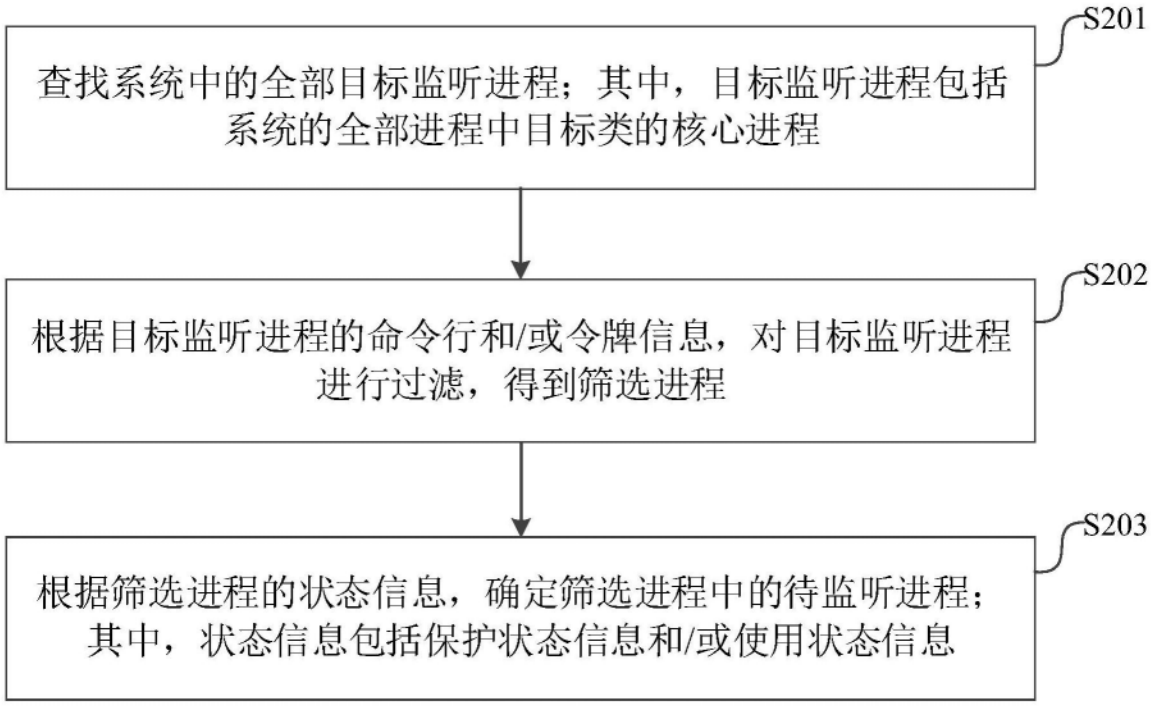

S201
查找系统中的全部目标监听进程；其中，目标监听进程包括系统的全部进程中目标类的核心进程
S202
根据目标监听进程的命令行和/或令牌信息，对目标监听进程进行过滤，得到筛选进程
S203
根据筛选进程的状态信息，确定筛选进程中的待监听进程；其中，状态信息包括保护状态信息和/或使用状态信息

图2

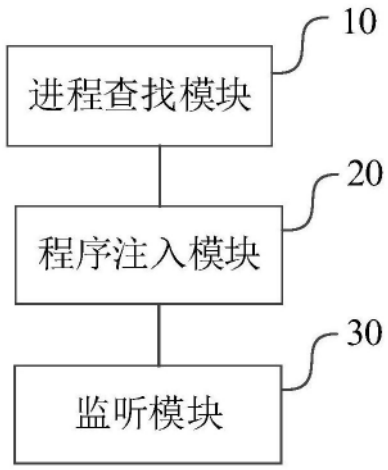


图3

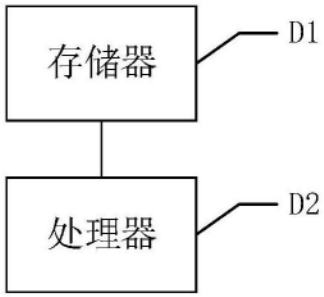


图4

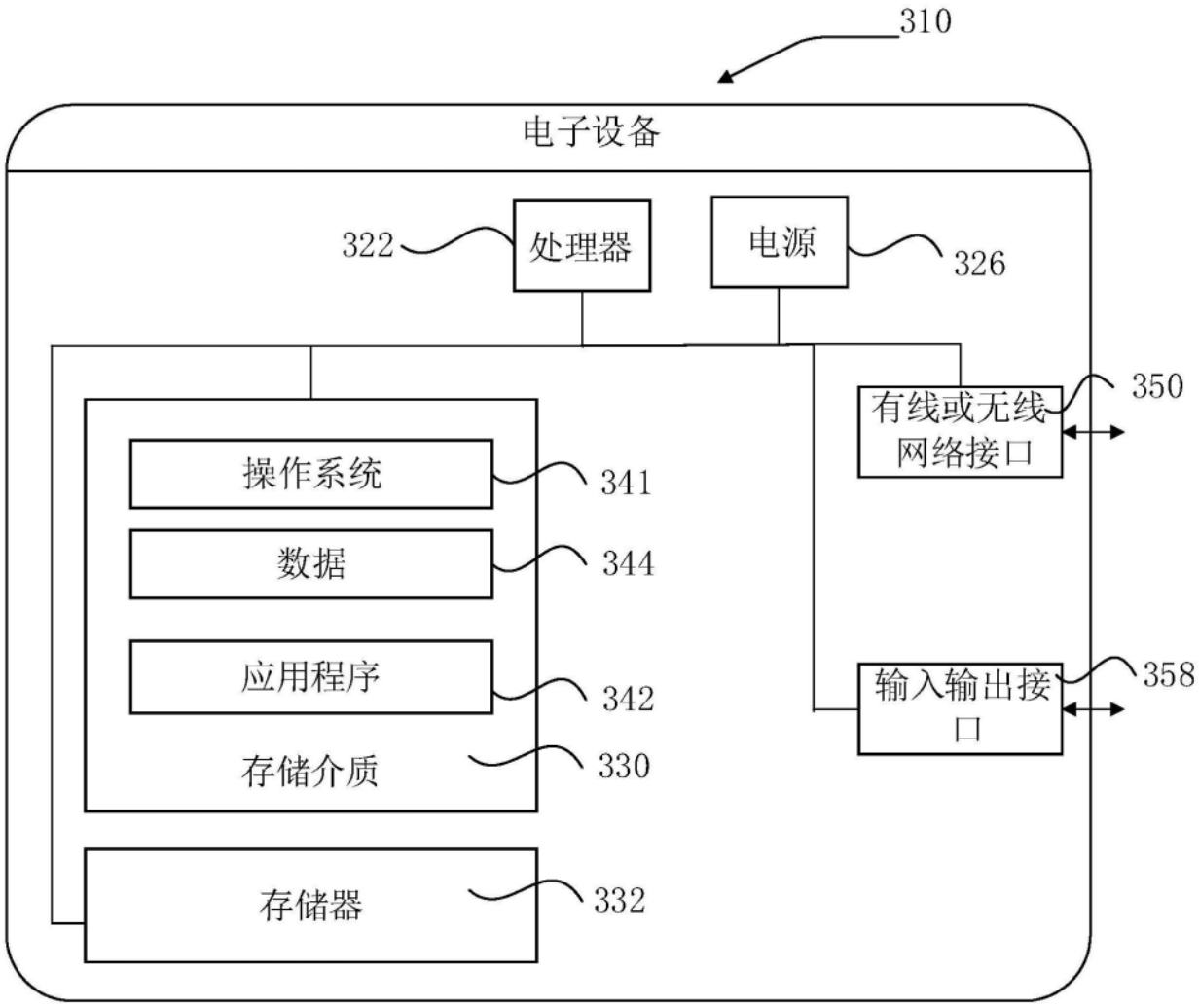

310
电子设备
322
处理器
电源
326
350
有线或无线网络接口
操作系统
341
数据
344
应用程序
342
存储介质
330
358
输入输出接口
存储器
332

图5