(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114499928 B
(45)授权公告日 2024.06.28

(21)申请号 202111520073.X

(22)申请日 2021.12.13

(65)同一申请的已公布的文献号
申请公布号 CN 114499928 A

(43)申请公布日 2022.05.13

(73)专利权人 奇安信科技集团股份有限公司
地址 100088 北京市西城区新街口外大街28号102号楼3层332号
专利权人 奇安信网神信息技术(北京)股份有限公司

(72)发明人 林岳川 孙诚

(74)专利代理机构 北京路浩知识产权代理有限公司 11002
专利代理师 王宇杨

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 67/133(2022.01)
H04L 67/51(2022.01)
G06F 9/448(2018.01)

(56)对比文件
CN 105354498 A,2016.02.24
CN 112351017 A,2021.02.09

审查员 肖敬伟

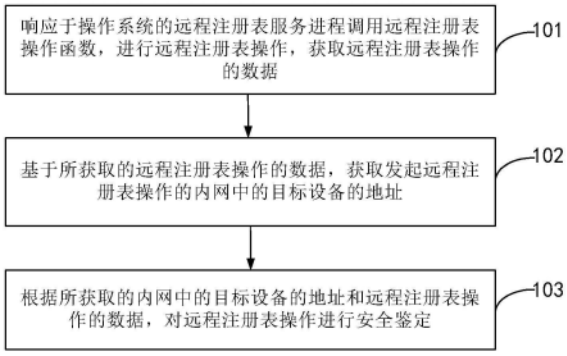
权利要求书2页 说明书10页 附图4页

(54)发明名称

远程注册表监测方法及装置

(57)摘要

本发明实施例提供一种远程注册表监测方法及装置。其中监测方法应用于内网中的设备，包括:响应于操作系统的远程注册表服务进程调用远程注册表操作函数,进行远程注册表操作,获取所述远程注册表操作的数据;基于所获取的所述远程注册表操作的数据,获取发起所述远程注册表操作的所述内网中的目标设备的地址;根据所获取的所述内网中的目标设备的地址和所述远程注册表操作的数据,对所述远程注册表操作进行安全鉴定。本发明实施例可以解决对网络攻击的监测缺乏有效精确的识别内网远程注册表操作的行为,提高设备对安全威胁的检测能力。



1.一种远程注册表监测方法,其特征在于,应用于内网中的设备,包括:

响应于操作系统的远程注册表服务进程调用远程注册表操作函数,进行远程注册表操作,获取所述远程注册表操作的数据;

基于所获取的所述远程注册表操作的数据,获取发起所述远程注册表操作的所述内网中的目标设备的地址;

根据所获取的所述内网中的目标设备的地址和所述远程注册表操作的数据,对所述远程注册表操作进行安全鉴定;

所述监测方法由在所述内网中的设备的所述远程注册表操作函数中设置HOOK函数执行;

在所述远程注册表操作函数中设置所述HOOK函数,包括:

查找所述操作系统的所述远程注册表服务进程,在所述远程注册表服务进程中安装监控模块;

通过所述监控模块在所述远程注册表服务进程的所述远程注册表操作函数中设置所述HOOK函数;

在所述远程注册表服务进程的所述远程注册表操作函数中设置所述HOOK函数,包括:

确定所述远程注册表服务进程调用的远程注册表核心功能文件;

基于远程注册表接口的标识符,在所述远程注册表核心功能文件中确定所述远程注册表接口;

在所确定的远程注册表接口的所述远程注册表操作函数中设置所述HOOK函数。

2.根据权利要求1所述的远程注册表监测方法,其特征在于,所述远程注册表服务进程进行所述远程注册表操作,调用的所述远程注册表操作函数包括修改注册表键值函数、删除注册表键函数、删除注册表键值函数、查询注册表键值函数和还原注册表数据函数中的至少一种。

3.根据权利要求2所述的远程注册表监测方法,其特征在于,所述确定所述远程注册表服务进程调用的远程注册表核心功能文件,包括:

确定所述远程注册表服务进程调用的regsvc.dll文件的内存地址;

所述基于远程注册表接口的标识符,在所述远程注册表核心功能文件中确定所述远程注册表接口,包括:

基于IRemoteRegistry接口的标识符,在所述regsvc.dll文件中确定IRemoteRegistry接口的地址;

所述在所确定的远程注册表接口的所述远程注册表操作函数中设置所述HOOK函数,包括:

基于所述IRemoteRegistry接口的内存地址,在所述IRemoteRegistry接口的BaseRegSetValue函数、BaseRegDeleteKe函数、BaseRegDeleteValue函数、BaseRegQueryValue函数和BaseRegRestoreKey函数中设置所述HOOK函数。

4.根据权利要求1至3任一项所述的远程注册表监测方法,其特征在于,获取所述远程注册表操作的数据,包括:

调用应用程序接口函数获取所述远程注册表操作的返回数据;

所述基于所获取的所述远程注册表操作的数据,获取发起所述远程注册表操作的所述

内网中的目标设备的地址,包括:

从所获取的所述远程注册表操作的返回数据中,获取发起所述远程注册表操作的所述内网中的目标设备的地址。

5.根据权利要求4所述的远程注册表监测方法,其特征在于,所述根据所获取的所述内网中的目标设备的地址和所述远程注册表操作的数据,对所述远程注册表操作进行安全鉴定之后,还包括:

判断所述安全鉴定结果是否为所述远程注册表操作为攻击行为;

若所述安全鉴定结果为所述远程注册表操作为攻击行为,对所述远程注册表操作进行防护拦截;

若所述安全鉴定结果为所述远程注册表操作为非攻击行为,返回所述远程注册表操作函数继续执行。

6.一种远程注册表监测装置,其特征在于,应用于内网中的设备,包括:

数据获取模块,用于响应于操作系统的远程注册表服务进程调用远程注册表操作函数,进行远程注册表操作,获取所述远程注册表操作的数据;

地址获取模块,用于基于所获取的所述远程注册表操作的数据,获取发起所述远程注册表操作的所述内网中的目标设备的地址;

信息发送模块,用于根据所获取的所述内网中的目标设备的地址和所述远程注册表操作的数据,对所述远程注册表操作进行安全鉴定;

所述监测装置由在所述内网中的设备的所述远程注册表操作函数中设置HOOK函数执行;

所述装置还包括:

监控安装模块,用于查找操作系统的远程注册表服务进程,在远程注册表服务进程中安装监控模块;

HOOK函数设置模块,用于通过监控模块在远程注册表服务进程的远程注册表操作函数中设置HOOK函数;

所述HOOK函数设置模块,包括:

核心文件确定单元,用于确定远程注册表服务进程调用的远程注册表核心功能文件;

服务接口确定单元,用于基于远程注册表接口的标识符,在远程注册表核心功能文件中确定远程注册表接口;

HOOK函数设置单元,用于在所确定的远程注册表接口的远程注册表操作函数中设置HOOK函数。

7.一种电子设备,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,其特征在于,所述处理器执行所述程序时实现如权利要求1至5任一项所述远程注册表监测方法的步骤。

8.一种非暂态计算机可读存储介质,其上存储有计算机程序,其特征在于,该计算机程序被处理器执行时实现如权利要求1至5任一项所述远程注册表监测方法的步骤。

远程注册表监测方法及装置

技术领域

[0001] 本发明涉及网络安全技术领域,尤其涉及一种远程注册表监测方法及装置。

背景技术

[0002] 在网络渗透完整攻击链中,内网远程横向渗透阶段是攻击者在一台已经被攻陷的设备上,以这台设备作为跳板,尝试去攻击同一网络内的其他设备,获取更多有价值的凭据,更高级的权限,以此扩大攻击面,进而达到控制整个内网网络。

[0003] 注册表在windows系统中具有重要的作用,其中存放着各种参数,直接控制着windows操作系统的启动、硬件驱动程序的装载以及一些windows应用程序的运行,远程注册表(Remote Registry)服务是windows系统为远程修改和查看本地设备的注册表信息提供的一项功能。通过远程注册表进行远程攻击是攻击者进行内网横向渗透的一个常用攻击手段,它是一种利用操作系统自身机制的能力。

[0004] 现有的注册表监测方法,只能识别本地发起的注册表操作,对于攻击者利用内网已经被攻陷的设备作为跳板,对内网的其他设备发起远程注册表操作的行为,缺乏有效精确识别的防护机制,使得作为防御方的设备处于监测失效状态,现有的网络攻击检测手段也无法有效精确的覆盖此类攻击手段。

发明内容

[0005] 针对现有技术中的问题,本发明实施例提供一种远程注册表监测方法及装置。

[0006] 具体地,本发明实施例提供了以下技术方案:

[0007] 第一方面,本发明实施例提供了一种远程注册表监测方法,应用于内网中的设备,包括:

[0008] 响应于操作系统的远程注册表服务进程调用远程注册表操作函数,进行远程注册表操作,获取所述远程注册表操作的数据;

[0009] 基于所获取的所述远程注册表操作的数据,获取发起所述远程注册表操作的所述内网中的目标设备的地址;

[0010] 根据所获取的所述内网中的目标设备的地址和所述远程注册表操作的数据,对所述远程注册表操作进行安全鉴定。

[0011] 进一步地,所述监测方法由在所述内网中的设备的所述远程注册表操作函数中设置HOOK函数执行;

[0012] 在所述远程注册表操作函数中设置所述HOOK函数,包括:

[0013] 查找所述操作系统的所述远程注册表服务进程,在所述远程注册表服务进程中安装监控模块;

[0014] 通过所述监控模块在所述远程注册表服务进程的所述远程注册表操作函数中设置所述HOOK函数。

[0015] 进一步地,在所述远程注册表服务进程的所述远程注册表操作函数中设置所述

HOOK函数,包括:

[0016] 确定所述远程注册表服务进程调用的远程注册表核心功能文件;

[0017] 基于远程注册表接口的标识符,在所述远程注册表核心功能文件中确定所述远程注册表接口;

[0018] 在所确定的远程注册表接口的所述远程注册表操作函数中设置所述HOOK函数。

[0019] 进一步地,所述远程注册表服务进程进行所述远程注册表操作,调用的所述远程注册表操作函数包括修改注册表键值函数、删除注册表键函数、删除注册表键值函数、查询注册表键值函数和还原注册表数据函数中的至少一种。

[0020] 进一步地,所述确定所述远程注册表服务进程调用的远程注册表核心功能文件,包括:

[0021] 确定所述远程注册表服务进程调用的regsvc.dll文件的内存地址;

[0022] 所述基于远程注册表接口的标识符,在所述远程注册表核心功能文件中确定所述远程注册表接口,包括:

[0023] 基于IRemoteRegistry接口的标识符,在所述regsvc.dll文件中确定IRemoteRegistry接口的地址;

[0024] 所述在所确定的远程注册表接口的所述远程注册表操作函数中设置所述HOOK函数,包括:

[0025] 基于所述IRemoteRegistry接口的内存地址,在所述IRemoteRegistry接口的BaseRegSetValue函数、BaseRegDeleteKe函数、BaseRegDeleteValue函数、BaseRegQueryValue函数和BaseRegRestoreKey函数中设置所述HOOK函数。

[0026] 进一步地,获取所述远程注册表操作的数据,包括:

[0027] 调用应用程序接口函数获取所述远程注册表操作的返回数据;

[0028] 所述基于所获取的所述远程注册表操作的数据,获取发起所述远程注册表操作的所述内网中的目标设备的地址,包括:

[0029] 从所获取的所述远程注册表操作的返回数据中,获取发起所述远程注册表操作的所述内网中的目标设备的地址。

[0030] 进一步地,所述根据所获取的所述内网中的目标设备的地址和所述远程注册表操作的数据,对所述远程注册表操作进行安全鉴定之后,还包括:

[0031] 判断所述安全鉴定结果是否为所述远程注册表操作为攻击行为;

[0032] 若所述安全鉴定结果为所述远程注册表操作为攻击行为,对所述远程注册表操作进行防护拦截;

[0033] 若所述安全鉴定结果为所述远程注册表操作为非攻击行为,返回所述远程注册表操作函数继续执行。

[0034] 第二方面,本发明实施例还提供了一种远程注册表监测装置,应用于内网中的设备,包括:

[0035] 数据获取模块,用于响应于操作系统的远程注册表服务进程调用远程注册表操作函数,进行远程注册表操作,获取所述远程注册表操作的数据;

[0036] 地址获取模块,用于基于所获取的所述远程注册表操作的数据,获取发起所述远程注册表操作的所述内网中的目标设备的地址;

[0037] 信息发送模块,用于根据所获取的所述内网中的目标设备的地址和所述远程注册表操作的数据,对所述远程注册表操作进行安全鉴定。

[0038] 第三方面,本发明实施例还提供了一种电子设备,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,所述处理器执行所述程序时实现如第一方面所述远程注册表监测方法的步骤。

[0039] 第四方面,本发明实施例还提供了一种非暂态计算机可读存储介质,其上存储有计算机程序,该计算机程序被处理器执行时实现如第一方面所述远程注册表监测方法的步骤。

[0040] 第五方面,本发明实施例还提供了一种计算机程序产品,其上存储有可执行指令,该指令被处理器执行时使处理器实现如第一方面所述远程注册表监测方法的步骤。

[0041] 本发明实施例提供的远程注册表监测方法及装置,通过在操作系统的远程注册表服务进程调用远程注册表操作函数,进行远程注册表操作时,获取远程注册表操作的数据,对远程注册表操作进行监测,可以精确识别来自内网的远程注册表操作的行为,并获取发起远程注册表操作的内网设备的地址,可以根据所获取的数据和地址进一步对远程注册表操作的行为进行安全鉴定,在内网远程横向渗透攻击时可以实时掌握攻击者的信息,并且通过获取攻击者的地址可以进一步追踪溯源,从而有效提高设备的安全防御能力,解决对网络攻击的监测缺乏有效精确的识别内网远程注册表操作的行为,可以提高设备对安全威胁的检测能力。

附图说明

[0042] 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一简单地介绍,显而易见地,下面描述中的附图是本发明的一些实施例,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,还可以根据这些附图获得其他的附图。

[0043] 图1是本发明提供的远程注册表监测方法的流程示意图;

[0044] 图2是本发明提供的在远程注册表操作函数中设置HOOK函数的流程示意图;

[0045] 图3是本发明提供的通过监控模块设置HOOK函数的流程示意图;

[0046] 图4是本发明提供的另一监控模块设置HOOK函数的流程示意图;

[0047] 图5是本发明提供的获取远程注册表操作的数据的流程示意图;

[0048] 图6是本发明提供的远程注册表监测方法的一种应用场景的流程示意图;

[0049] 图7是本发明提供的远程注册表监测装置的组成结构示意图;

[0050] 图8是本发明提供的电子设备的实体结构示意图。

具体实施方式

[0051] 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作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。

[0052] 下面结合图1-图6描述本发明的远程注册表监测方法。

[0053] 请参阅图1,图1是本发明提供的远程注册表监测方法的流程示意图,图1所示的远程注册表监测方法应用于内网中的设备,如图1所示,该远程注册表监测方法至少包括:

[0054] 101,响应于操作系统的远程注册表服务进程调用远程注册表操作函数,进行远程注册表操作,获取远程注册表操作的数据。

[0055] 在本发明实施例中,内网可以为企业局域网、校园局域网、商场局域网等,本发明实施例对内网的应用场景不作限定,内网可以包括有线网和/或无线网。内网中的设备可以为个人计算机、服务器、工作站等,本发明实施例对内网中的设备的类型不作限定。在内网中的设备中运行的管理计算机硬件与软件资源的操作系统为Windows系统,例如Windows10,本发明实施例对内网中的设备中运行Windows系统的版本不作限定。远程注册表服务可以由在操作系统启动时启动并在后台运行的远程注册表服务进程执行。远程注册表操作函数是用于进行远程注册表操作的函数,远程注册表服务进程可以通过远程注册表操作函数对注册表进行远程操作,例如通过远程过程调用(Remote Procedure Call,简称RPC)对注册表进行远程查询键值、远程修改键值、远程还原数据等操作,本发明实施例对远程注册表操作函数的类型不作限定。

[0056] 在本发明实施例中,当操作系统的远程注册表服务进程调用远程注册表操作函数,进行远程注册表操作时,可以通过捕获该远程注册表操作函数进行远程注册表操作时的数据,即远程注册表操作的数据,通过所获取的远程注册表操作的数据可以反映远程注册表操作的行为特征,例如所获取的远程注册表操作的数据可以包括远程注册表操作的返回数据,本发明实施例对所捕获的远程注册表操作的数据的类型不作限定。

[0057] 102,基于所获取的远程注册表操作的数据,获取发起远程注册表操作的内网中的目标设备的地址。

[0058] 在本发明实施例中,在获取远程注册表操作的数据之后,可以根据所获取的远程注册表操作的数据,获取发起远程注册表操作的内网中的目标设备的地址。可选地,可以根据所获取的远程注册表操作的数据的类型,确定获取发起远程注册表操作的内网中的目标设备的地址的方法,从而根据所获取的远程注册表操作的数据获取发起远程注册表操作的内网中的目标设备的地址,本发明实施例对此不作限定。例如,所获取的远程注册表操作的数据包括远程注册表操作的返回数据,可以直接从远程注册表操作的返回数据中获取发起远程注册表操作的内网中的目标设备的IP地址。

[0059] 103,根据所获取的内网中的目标设备的地址和远程注册表操作的数据,对远程注册表操作进行安全鉴定。

[0060] 在本发明实施例中,在获得远程注册表操作的数据和内网中的目标设备的地址之后,可以根据所获得的远程注册表操作的数据和内网中的目标设备的地址,对远程注册表操作进行安全鉴定。可选地,还可以根据安全鉴定结果,确定是否对远程注册表操作进行防护拦截,例如可以通过判断安全鉴定结果是否为远程注册表操作为攻击行为,若安全鉴定结果为远程注册表操作为攻击行为,则可以对远程注册表操作进行防护拦截,以阻止攻击者进一步扩大攻击面,提升设备的安全防护能力,若安全鉴定结果为远程注册表操作为非攻击行为,则可以返回远程注册表操作函数继续执行。例如可以将所获得的远程注册表操作的数据和内网中的目标设备的地址发送到威胁行为识别引擎,进行安全鉴定,并接收威胁行为识别引擎反馈的安全鉴定结果。威胁行为识别引擎是一个基于云端的行为识别系

统,它通过安全运营专家的积累经验形成的一套对行为数据进行匹配的规则,可以检测出操作行为是否为攻击行为。

[0061] 本发明实施例提供的远程注册表监测方法,通过在操作系统的远程注册表服务进程调用远程注册表操作函数,进行远程注册表操作时,获取远程注册表操作的数据,对远程注册表操作进行监测,可以精确识别来自内网的远程注册表操作的行为,并获取发起远程注册表操作的内网设备的地址,可以根据所获取的数据和地址进一步对远程注册表操作的行为进行安全鉴定,在内网远程横向渗透攻击时可以实时掌握攻击者的信息,并且通过获取攻击者的地址可以进一步追踪溯源,从而有效提高设备的安全防御能力,解决对网络攻击的监测缺乏有效精确的识别内网远程注册表操作的行为,可以提高设备对安全威胁的检测能力。

[0062] Hook函数也称为钩子函数,用于在系统调用一个函数时优先捕获该函数调用,获得该函数的控制权,对该函数进行额外的处理。可以通过在远程注册表操作函数中预先设置HOOK函数,通过HOOK函数对远程注册表操作进行监测。请参阅图2,图2是本发明提供的在远程注册表操作函数中设置HOOK函数的流程示意图,如图2所示,在远程注册表操作函数中设置HOOK函数至少包括:

[0063] 201,查找操作系统的远程注册表服务进程,在远程注册表服务进程中安装监控模块。

[0064] 在本发明实施例中,可以通过调用操作系统提供的应用程序接口函数(Application Programming Interface,简称API),查找操作系统的远程注册表服务进程,获得远程注册表服务进程的进程标识符((Process Identification,简称PID),例如应用程序接口函数为QueryServiceStatusEx,然后可以根据所获得的远程注册表服务进程的进程标识符,在远程注册表服务进程中注入监控模块,其中,在远程注册表服务进程中注入监控模块的方法可以采用现有的进程注入的方法,本发明实施对此不作限定。

[0065] 202,通过监控模块在远程注册表服务进程的远程注册表操作函数中设置HOOK函数。

[0066] 在本发明实施例中,在操作系统的远程注册表服务进程中安装监控模块之后,可以通过监控模块根据远程注册表服务进程确定远程注册表操作函数,并在远程注册表操作函数中设置HOOK函数。本发明实施例对监控模块根据远程注册表服务进程确定远程注册表操作函数的方法不作限定,例如可以根据远程注册表服务进程确定远程注册表服务进程调用的远程注册表核心功能文件,在远程注册表核心功能文件中确定远程注册表操作函数。本发明实施例对监控模块在远程注册表操作函数中设置HOOK函数的方法不作限定,例如可以通过修改远程注册表操作函数的代码在远程注册表操作函数中设置HOOK函数。

[0067] 请参阅图3,图3是本发明提供的通过监控模块设置HOOK函数的流程示意图,如图3所示,监控模块设置HOOK函数至少包括:

[0068] 301,确定远程注册表服务进程调用的远程注册表核心功能文件。

[0069] 在本发明实施例中,监控模块可以根据远程注册表服务进程,获得远程注册表服务进程所调用的文件,并根据远程注册表服务进程所调用的文件确定远程注册表核心功能文件,远程注册表核心功能文件是用于提供远程注册表功能的文件,例如远程注册表核心功能文件可以为动态链接文件(Dynamic Link Library,简称DLL)。其中,获得远程注册表

服务进程所调用的文件的方法可以采用现有技术的方法来实现,本发明实施例对此不作限定。在获得远程注册表服务进程所调用的文件之后,可以根据远程注册表核心功能文件的名称,确定远程注册表服务进程调用的远程注册表核心功能文件在内存中的地址。

[0070] 302,基于远程注册表接口的标识符,在远程注册表核心功能文件中确定远程注册表接口。

[0071] 在本发明实施例中,在确定远程注册表服务进程调用的远程注册表核心功能文件之后,监控模块可以根据在远程注册表接口的数据结构中具有唯一性的标识符(Globally Unique Identifier,简称GUID),在远程注册表核心功能文件中进行搜索,在远程注册表核心功能文件中定位对应的远程注册表接口。其中,根据GUID在远程注册表核心功能文件中进行搜索定位远程注册表接口的方法可以采用现有技术的方法来实现,本发明实施例对此不作限定。根据GUID在远程注册表核心功能文件中进行搜索,可以在远程注册表核心功能文件中定位对应的远程注册表接口在内存中的地址。

[0072] 303,在所确定的远程注册表接口的远程注册表操作函数中设置HOOK函数。

[0073] 在本发明实施例中,在远程注册表核心功能文件中确定远程注册表接口之后,监控模块可以根据所确定的远程注册表接口,在远程注册表接口的远程注册表操作函数中设置HOOK函数。其中,可以根据所确定的远程注册表接口在内存中的地址,在远程注册表接口的远程注册表操作函数中设置HOOK函数,例如,可以根据远程注册表接口在内存中的地址,在内存中修改远程注册表操作函数的代码,将HOOK函数设置于远程注册表操作函数中,使得当远程注册表操作函数被调用时,可以进入到HOOK函数中,在HOOK函数执行完成之后,可以再次回到远程注册表操作函数中继续执行。

[0074] 在一些可选的例子中,远程注册表服务进程进行远程注册表操作,调用的远程注册表操作函数可以包括修改注册表键值函数、删除注册表键函数、删除注册表键值函数、查询注册表键值函数和还原注册表数据函数中的至少一种。例如,监控模块在远程注册表接口的修改注册表键值函数、删除注册表键函数、删除注册表键值函数、查询注册表键值函数和还原注册表数据函数中均设置HOOK函数;当操作系统的远程注册表服务进程调用修改注册表键值函数进行远程注册表键值的修改时,设置于修改注册表键值函数中的HOOK函数,响应于远程注册表服务进程对修改注册表键值函数的调用,会获取远程修改注册表键值的数据;当操作系统的远程注册表服务进程调用查询注册表键值函数和删除注册表键值函数,进行远程注册表键值的查询并对查询到的注册表键值进行远程删除时,设置于调用查询注册表键值函数中的HOOK函数,响应于远程注册表服务进程对查询注册表键值函数的调用,会获取远程查询注册表键值的数据,设置于删除注册表键值函数中的HOOK函数,响应于远程注册表服务进程对删除注册表键值函数的调用,会获取远程删除注册表键值的数据。

[0075] 请参阅图4,图4是本发明提供的另一监控模块设置HOOK函数的流程示意图,如图4所示,监控模块设置HOOK函数至少包括:

[0076] 401,确定远程注册表服务进程调用的regsvc.dll文件的内存地址。

[0077] 402,基于IRemoteRegistry接口的标识符,在regsvc.dll文件中确定IRemoteRegistry接口的地址。

[0078] 403,基于IRemoteRegistry接口的内存地址,在IRemoteRegistry接口的BaseRegSetValue函数、BaseRegDeleteKe函数、BaseRegDeleteValue函数、

BaseRegQueryValue函数和BaseRegRestoreKey函数中设置HOOK函数。

[0079] 在本发明实施例中,监控模块首先确定Windows系统远程注册表服务进程调用的远程注册表核心功能文件regsvc.dll的内存地址,然后根据远程注册表接口IRemoteRegistry的数据结构中的GUID,在regsvc.dll的内存地址中进行搜索,并在regsvc.dll的内存地址中定位IRemoteRegistry接口的内存地址,之后在IRemoteRegistry接口的修改注册表键值函数BaseRegSetValue、删除注册表键函数BaseRegDeleteKe、删除注册表键值函数BaseRegDeleteValue、查询注册表键值函数BaseRegQueryValue和还原注册表数据函数BaseRegRestoreKey中,分别通过修改函数的代码设置HOOK函数。

[0080] 请参阅图5,图5是本发明提供的获取远程注册表操作的数据的流程示意图,如图5所示,获取远程注册表操作的数据至少包括:

[0081] 501,调用应用程序接口函数获取远程注册表操作的返回数据。

[0082] 在本发明实施例中,HOOK函数可以通过调用应用程序接口函数RpcServerInqCallAttributes,获取远程注册表操作的返回数据,远程注册表操作的返回数据中记载了远程注册表操作名称、远程注册表操作执行数据、发起远程注册表操作的设备的IP地址等信息。

[0083] 502,从所获取的远程注册表操作的返回数据中,获取发起远程注册表操作的内网中的目标设备的地址。

[0084] 在本发明实施例中,在获取远程注册表操作的返回数据之后,HOOK函数可以直接从所获取的远程注册表操作的返回数据中,获取发起远程注册表操作的内网中的目标设备的IP地址。例如远程注册表操作为远程注册表操作名称:删除注册表键值,远程注册表操作执行数据:KeyPath:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run,KeyValueName:AntiVirus,IP:192.168.44.138,可以直接获取发起远程删除注册表键的内网中的目标设备的IP地址为192.168.44.138。

[0085] 请参阅图6,图6是本发明提供的远程注册表监测方法的一种应用场景的流程示意图,如图6所示,在本发明实施例中,首先查找操作系统的远程注册表(RemoteRegistry)服务进程,在远程注册表服务进程中安装监控模块;然后通过监控模块调用GetModuleHandle函数获取远程注册表服务进程的regsvc.dll文件的内存地址,并根据IRemoteRegistry接口的GUID在regsvc.dll文件中进行搜索定位IRemoteRegistry接口的内存地址,在IRemoteRegistry接口的RPC远程注册表操作函数中设置HOOK函数;IRemoteRegistry接口的RPC服务函数包括BaseRegSetValue(修改注册表键值)函数、BaseRegDeleteKey(删除注册表键)函数、BaseRegDeleteValue((删除注册表键值)函数、BaseRegQueryValue(查询注册表键值)函数、BaseRegRestoreKey(还原注册表数据)函数;之后通过HOOK函数对远程注册表操作进行监测,在远程注册表服务进程调用远程注册表操作函数进行远程注册表操作时,HOOK函数可以获取远程注册表操作的数据,并从远程注册表操作的数据获取发起该远程注册表操作行为的内网中的设备的IP地址;最后将获取的远程注册表操作的数据和IP地址发送至威胁行为识别引擎进行安全鉴定,可以根据最终鉴定的结果对远程注册表操作的行为进行拦截。

[0086] 下面对本发明提供的远程注册表监测装置进行描述,下文描述的远程注册表监测装置与上文描述的远程注册表监测方法可相互对应参照。

[0087] 请参阅图7,图7是本发明提供的远程注册表监测装置的组成结构示意图,图7所示的远程注册表监测装置应用于内网中的设备,如图7所示,该远程注册表监测装置至少包括:

[0088] 数据获取模块710,用于响应于操作系统的远程注册表服务进程调用远程注册表操作函数,进行远程注册表操作,获取远程注册表操作的数据。

[0089] 地址获取模块720,用于基于所获取的远程注册表操作的数据,获取发起远程注册表操作的内网中的目标设备的地址。

[0090] 信息发送模块730,用于根据所获取的内网中的目标设备的地址和远程注册表操作的数据,对远程注册表操作进行安全鉴定。

[0091] 可选地,该远程注册表监测装置设置于在内网中的设备的远程注册表操作函数中设置的HOOK函数,该远程注册表监测装置,还包括:

[0092] 监控安装模块,用于查找操作系统的远程注册表服务进程,在远程注册表服务进程中安装监控模块。

[0093] HOOK函数设置模块,用于通过监控模块在远程注册表服务进程的远程注册表操作函数中设置HOOK函数。

[0094] 可选地,HOOK函数设置模块,包括:

[0095] 核心文件确定单元,用于确定远程注册表服务进程调用的远程注册表核心功能文件。

[0096] 服务接口确定单元,用于基于远程注册表接口的标识符,在远程注册表核心功能文件中确定远程注册表接口。

[0097] HOOK函数设置单元,用于在所确定的远程注册表接口的远程注册表操作函数中设置HOOK函数。

[0098] 可选地,远程注册表服务进程进行远程注册表操作,调用的远程注册表操作函数包括修改注册表键值函数、删除注册表键函数、删除注册表键值函数、查询注册表键值函数和还原注册表数据函数中的至少一种。

[0099] 可选地,核心文件确定单元,用于确定远程注册表服务进程调用的regsvc.dll文件的内存地址。

[0100] 服务接口确定单元,用于基于IRemoteRegistry接口的标识符,在regsvc.dll文件中确定IRemoteRegistry接口的地址。

[0101] HOOK函数设置单元,用于基于IRemoteRegistry接口的内存地址,在IRemoteRegistry接口的BaseRegSetValue函数、BaseRegDeleteKe函数、BaseRegDeleteValue函数、BaseRegQueryValue函数和BaseRegRestoreKey函数中设置HOOK函数。

[0102] 可选地,数据获取模块710,用于调用应用程序接口函数获取远程注册表操作的返回数据。

[0103] 地址获取模块720,用于从所获取的远程注册表操作的返回数据中,获取发起远程注册表操作的内网中的目标设备的地址。

[0104] 可选地,该远程注册表监测装置,还包括:

[0105] 结果判断模块,用于判断安全鉴定结果是否为远程注册表操作为攻击行为。

[0106] 防护拦截模块,用于根据结果判断模块的判断结果,若安全鉴定结果为远程注册表操作为攻击行为,对远程注册表操作进行防护拦截。

[0107] 结束返回模块,用于根据结果判断模块的判断结果,若安全鉴定结果为远程注册表操作为非攻击行为,返回远程注册表操作函数继续执行。

[0108] 图8示例了一种电子设备的实体结构示意图,如图8所示,该电子设备可以包括:处理器(processor)810、通信接口(Communications Interface)820、存储器(memory)830和通信总线840,其中,处理器810,通信接口820,存储器830通过通信总线840完成相互间的通信。处理器810可以调用存储器830中的逻辑指令,以执行如下方法:响应于操作系统的远程注册表服务进程调用远程注册表操作函数,进行远程注册表操作,获取所述远程注册表操作的数据;基于所获取的所述远程注册表操作的数据,获取发起所述远程注册表操作的所述内网中的目标设备的地址;根据所获取的所述内网中的目标设备的地址和所述远程注册表操作的数据,对所述远程注册表操作进行安全鉴定。

[0109] 此外,上述的存储器830中的逻辑指令可以通过软件功能单元的形式实现并作为独立的产品销售或使用时,可以存储在一个计算机可读取存储介质中。基于这样的理解,本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质中,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备等)执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括:U盘、移动硬盘、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0110] 另一方面,本发明实施例还提供一种非暂态计算机可读存储介质,其上存储有计算机程序,该计算机程序被处理器执行时实现以执行上述各实施例提供的方法,例如包括:响应于操作系统的远程注册表服务进程调用远程注册表操作函数,进行远程注册表操作,获取所述远程注册表操作的数据;基于所获取的所述远程注册表操作的数据,获取发起所述远程注册表操作的所述内网中的目标设备的地址;根据所获取的所述内网中的目标设备的地址和所述远程注册表操作的数据,对所述远程注册表操作进行安全鉴定。

[0111] 以上所描述的装置实施例仅仅是示意性的,其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性的劳动的情况下,即可以理解并实施。

[0112] 通过以上的实施方式的描述,本领域的技术人员可以清楚地了解到各实施方式可借助软件加必需的通用硬件平台的方式来实现,当然也可以通过硬件。基于这样的理解,上述技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来,该计算机软件产品可以存储在计算机可读存储介质中,如ROM/RAM、磁碟、光盘等,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备等)执行各个实施例或者实施例的某些部分所述的方法。

[0113] 最后应说明的是:以上实施例仅用以说明本发明的技术方案,而非对其限制;尽管参照前述实施例对本发明进行了详细的说明,本领域的普通技术人员应当理解:其依然可

以对前述各实施例所记载的技术方案进行修改,或者对其中部分技术特征进行等同替换;而这些修改或者替换,并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

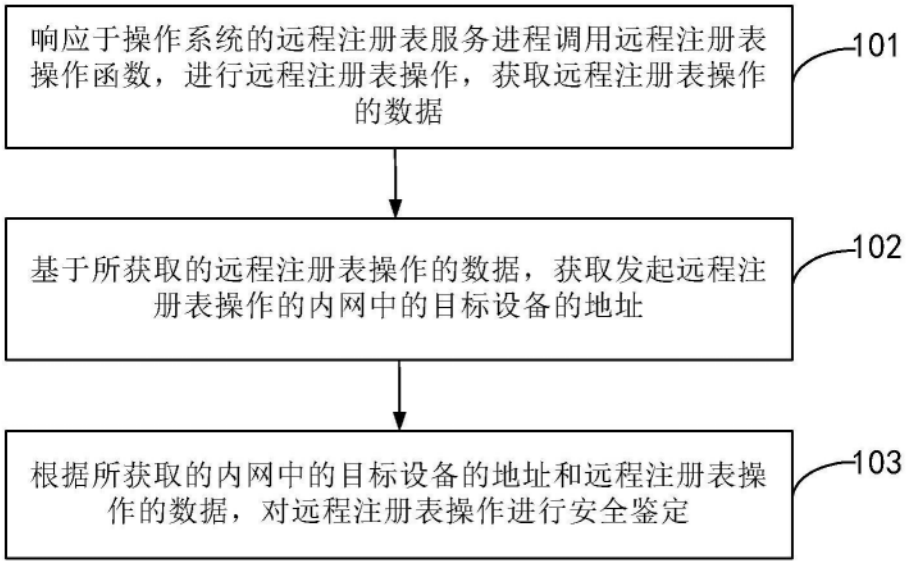

响应于操作系统的远程注册表服务进程调用远程注册表操作函数，进行远程注册表操作，获取远程注册表操作的数据
101
基于所获取的远程注册表操作的数据，获取发起远程注册表操作的内网中的目标设备的地址
102
根据所获取的内网中的目标设备的地址和远程注册表操作的数据，对远程注册表操作进行安全鉴定
103

图1

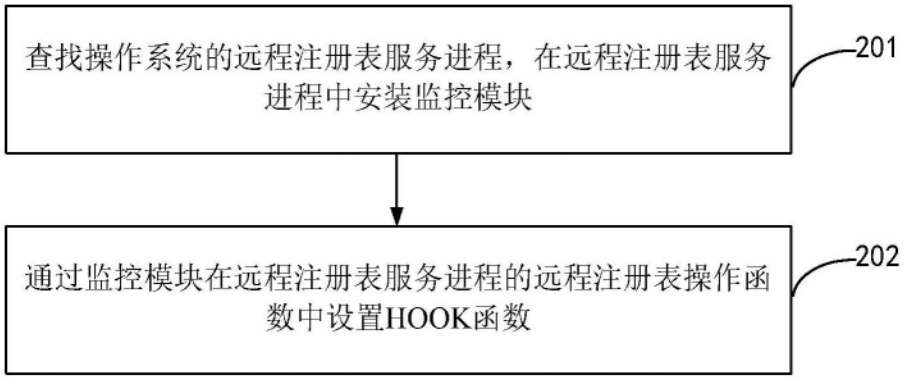

查找操作系统的远程注册表服务进程，在远程注册表服务进程中安装监控模块
201
通过监控模块在远程注册表服务进程的远程注册表操作函数中设置HOOK函数
202

图2

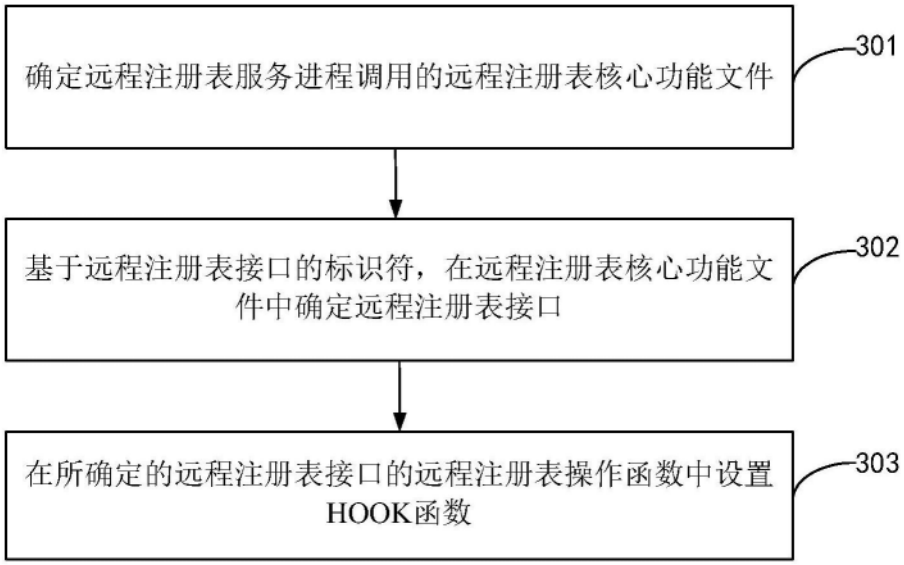

确定远程注册表服务进程调用的远程注册表核心功能文件
301
基于远程注册表接口的标识符，在远程注册表核心功能文件中确定远程注册表接口
302
在所确定的远程注册表接口的远程注册表操作函数中设置HOOK函数
303

图3

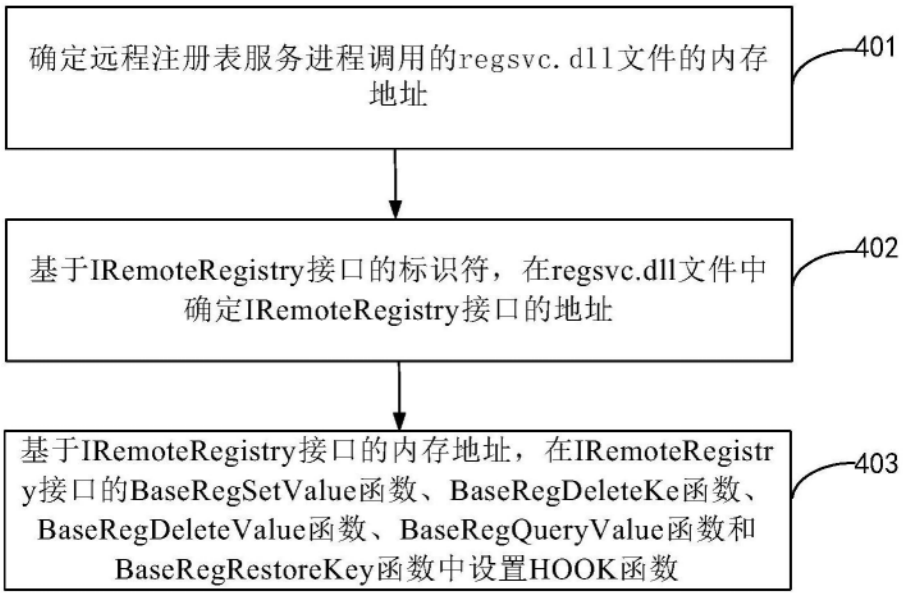

确定远程注册表服务进程调用的regsvc.dll文件的内存地址
401
基于IRemoteRegistry接口的标识符，在regsvc.dll文件中确定IRemoteRegistry接口的地址
402
基于IRemoteRegistry接口的内存地址，在IRemoteRegistry接口的BaseRegSetValue函数、BaseRegDeleteKe函数、BaseRegDeleteValue函数、BaseRegQueryValue函数和BaseRegRestoreKey函数中设置HOOK函数
403

图4

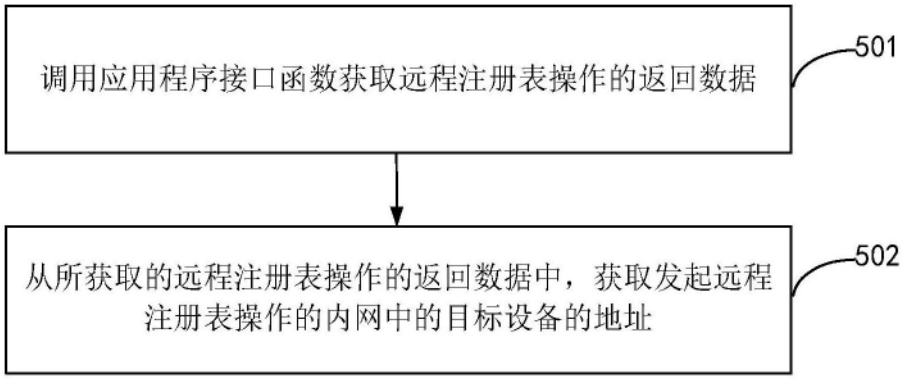

调用应用程序接口函数获取远程注册表操作的返回数据
501
从所获取的远程注册表操作的返回数据中，获取发起远程注册表操作的内网中的目标设备的地址
502

图5

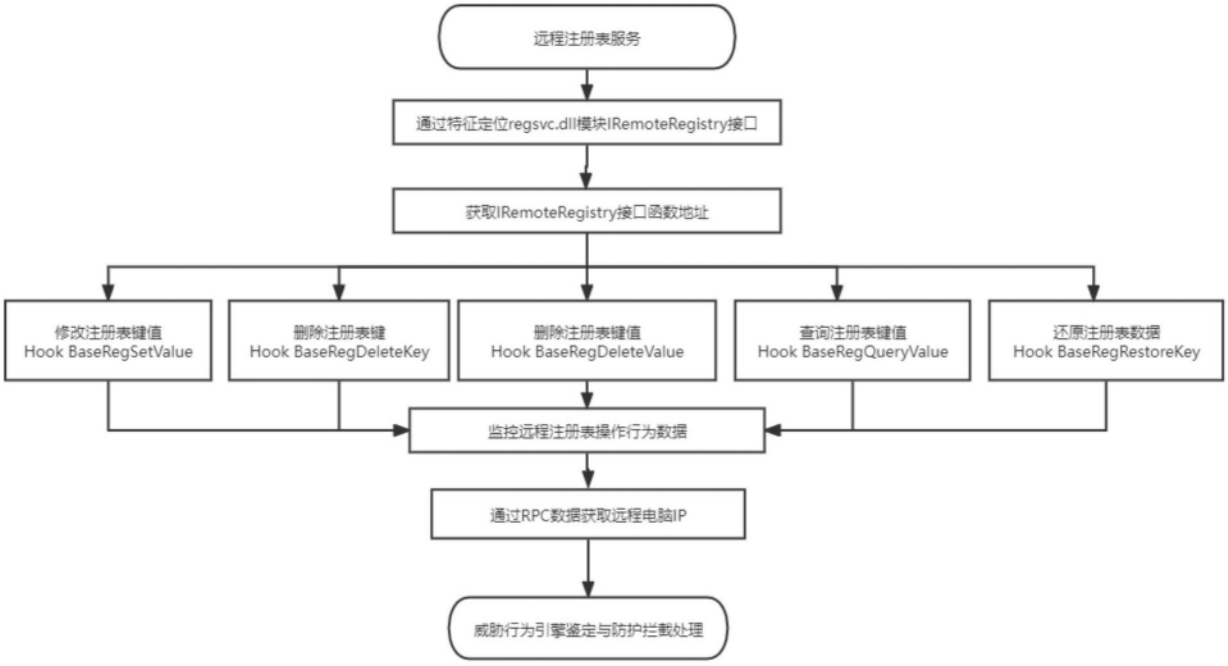

远程注册表服务
通过特征定位regsvc.dll模块IRemoteRegistry接口
获取IRemoteRegistry接口函数地址
修改注册表键值
Hook BaseRegSetValue
删除注册表键
Hook BaseRegDeleteKey
删除注册表键值
Hook BaseRegDeleteValue
查询注册表键值
Hook BaseRegQueryValue
还原注册表数据
Hook BaseRegRestoreKey
监控远程注册表操作行为数据
通过RPC数据获取远程电脑IP
威胁行为引擎鉴定与防护拦截处理

图6

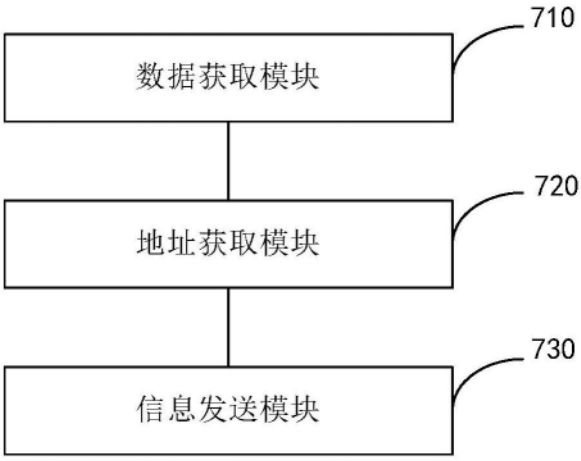

710
数据获取模块
720
地址获取模块
730
信息发送模块

图7

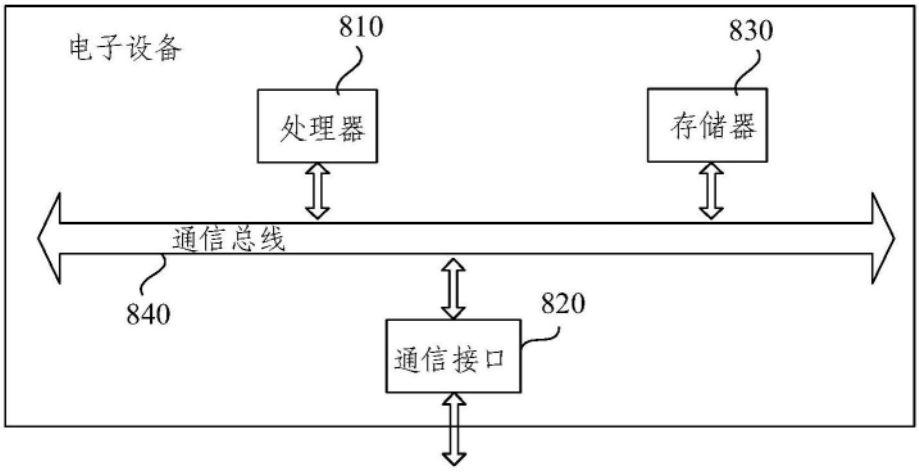

电子设备
810
处理器
830
存储器
通信总线
840
820
通信接口

图8