(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 110866248 A
(43)申请公布日 2020.03.06

(21)申请号 201811438897.0

(22)申请日 2018.11.28

(71)申请人 北京安天网络安全技术有限公司
地址 100195 北京市海淀区玉泉山闵庄路3号清华科技园玉泉慧谷1号楼

(72)发明人 孙洪伟 徐翰隆 王小丰 肖新光

(74)专利代理机构 北京市广友专利事务所有限责任公司 11237
代理人 祁献民

(51)Int.Cl.
G06F 21/56(2013.01)

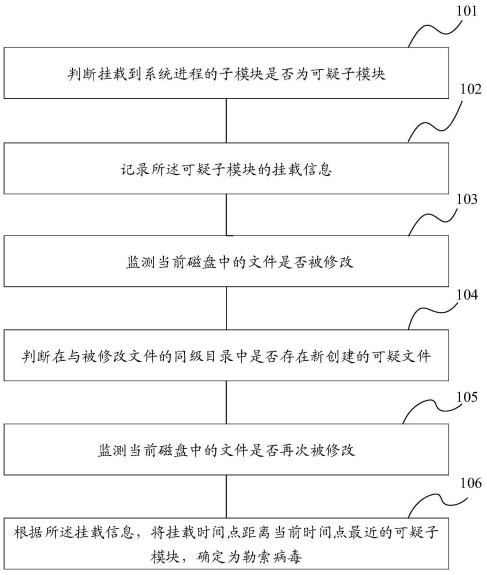
权利要求书2页 说明书7页 附图3页

(54)发明名称

一种勒索病毒识别方法、装置、电子设备及存储介质

(57)摘要

本发明的实施例公开一种勒索病毒挂载系统进程的识别方法，涉及计算机安全技术领域，能够快速准确地识别出勒索病毒。所述方法包括：判断挂载到系统进程的子模块是否为可疑子模块；记录所述可疑子模块的挂载信息；监测当前磁盘中的文件是否被修改；若监测到当前磁盘中的文件被修改，则判断在与被修改文件的同级目录中是否存在新创建的可疑文件；若在与被修改文件的同级目录中存在新创建的可疑文件，则监测当前磁盘中的文件是否再次被修改；若监测到当前磁盘中的文件再次被修改，则根据所述挂载信息，将挂载时间点距离当前时间点最近的可疑子模块，确定为勒索病毒。本发明适用于勒索病毒的识别。



CN 110866248 A

1.一种勒索病毒识别方法,其特征在于,包括:

判断挂载到系统进程的子模块是否为可疑子模块;

若挂载到系统进程的子模块为可疑子模块,则记录所述可疑子模块的挂载信息;其中,所述挂载信息包括可疑子模块挂载到系统进程的时间点;

监测当前磁盘中的文件是否被修改;

若监测到当前磁盘中的文件被修改,则判断在与被修改文件的同级目录中是否存在新创建的可疑文件;

若在与被修改文件的同级目录中存在新创建的可疑文件,则监测当前磁盘中的文件是否再次被修改;

若监测到当前磁盘中的文件再次被修改,则根据所述挂载信息,将挂载时间点距离当前时间点最近的可疑子模块,确定为勒索病毒。

2.根据权利要求1所述的勒索病毒识别方法,其特征在于,所述判断挂载到系统进程的子模块是否为可疑子模块,包括:

根据预设的检查规则,判断已挂载到系统进程的子模块是否为可疑子模块。

3.根据权利要求1所述的勒索病毒识别方法,其特征在于,所述判断挂载到系统进程的子模块是否为可疑子模块,包括:

监测是否有新的子模块挂载到系统进程;

若监测到有新的子模块挂载到系统进程,则根据预设的检查规则,判断新挂载到系统进程的子模块是否为可疑子模块。

4.根据权利要求1所述的勒索病毒识别方法,其特征在于,在确定挂载到系统进程的子模块为可疑子模块之后,所述方法还包括:

将可疑子模块加入到危险模块监控列表中。

5.根据权利要求1所述的勒索病毒识别方法,其特征在于,所述若在与被修改文件的同级目录中存在新创建的可疑文件,则监测当前磁盘中的文件是否再次被修改,包括:

若在与被修改文件的同级目录中存在新创建的可疑文件,则加载深度分析模块,通过所述深度分析模块,监测当前磁盘中的文件是否再次被修改。

6.一种勒索病毒识别装置,其特征在于,包括:

第一判断模块,用于判断挂载到系统进程的子模块是否为可疑子模块;

记录模块,用于若挂载到系统进程的子模块为可疑子模块,则记录所述可疑子模块的挂载信息;其中,所述挂载信息包括可疑子模块挂载到系统进程的时间点;

第一监测模块,用于监测当前磁盘中的文件是否被修改;

第二判断模块,用于若监测到当前磁盘中的文件被修改,则判断在与被修改文件的同级目录中是否存在新创建的可疑文件;

第二监测模块,用于若在与被修改文件的同级目录中存在新创建的可疑文件,则监测当前磁盘中的文件是否再次被修改;

第三判断模块,用于若监测到当前磁盘中的文件再次被修改,则根据所述挂载信息,将挂载时间点距离当前时间点最近的可疑子模块,确定为勒索病毒。

7.根据权利要求6所述的勒索病毒识别装置,其特征在于,所述第一判断模块,具体用于根据预设的检查规则,判断已挂载到系统进程的子模块是否为可疑子模块。

8.根据权利要求6所述的勒索病毒识别装置，其特征在于，所述第一判断模块，包括：

挂载监测子模块，用于监测是否有新的子模块挂载到系统进程；

可疑判断子模块，用于若监测到有新的子模块挂载到系统进程，则根据预设的检查规则，判断新挂载到系统进程的子模块是否为可疑子模块。

9.根据权利要求6所述的勒索病毒识别装置，其特征在于，还包括：危险模块监控列表模块。用于将可疑子模块加入到危险模块监控列表中。

10.根据权利要求6所述的勒索病毒识别装置，其特征在于，所述第二监测模块，具体用于：若在与被修改文件的同级目录中存在新创建的可疑文件，则加载深度分析模块，以通过所述深度分析模块，监测当前磁盘中的文件是否再次被修改。

11.一种电子设备，其特征在于，所述电子设备包括：壳体、处理器、存储器、电路板和电源电路，其中，电路板安置在壳体围成的空间内部，处理器和存储器设置在电路板上；电源电路，用于为上述电子设备的各个电路或器件供电；存储器用于存储可执行程序代码；处理器通过读取存储器中存储的可执行程序代码来运行与可执行程序代码对应的程序，用于执行前述任一权利要求所述的方法。

12.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质存储有一个或者多个程序，所述一个或者多个程序可被一个或者多个处理器执行，以实现前述任一权利要求所述的方法。

一种勒索病毒识别方法、装置、电子设备及存储介质

技术领域

[0001] 本发明涉及计算机安全技术领域，尤其涉及一种勒索病毒识别方法、装置、电子设备及存储介质。

背景技术

[0002] 勒索病毒，是一种新型电脑病毒，该病毒性质恶劣、危害极大，一旦感染将给用户带来无法估量的损失。勒索病毒渗透进企业内网后，通过勒索病毒宿主机检索内网主机，并通过系统漏洞对目标主机发起攻击，攻击成功后将具备勒索功能的恶意代码释放到目标主机磁盘中并挂载系统进程中，执行后续的加密破坏。这种病毒利用各种加密算法对文件进行加密，被感染者一般无法解密，必须拿到解密的私钥才有可能破解。

[0003] 勒索病毒具有隐蔽的特性：载荷文件通过某些途径落地用户主机中，并通过某些途径挂载在操作系统进程下，并立即对当前磁盘进行加密，此时传统杀毒软件会识别为系统文件，对此行为进行放行处置。

发明内容

[0004] 有鉴于此，本发明实施例提供一种勒索病毒识别方法、装置、电子设备及存储介质，能够快速准确地识别出勒索病毒。

[0005] 第一方面，本发明实施例提供一种勒索病毒识别方法，包括：判断挂载到系统进程的子模块是否为可疑子模块；若挂载到系统进程的子模块为可疑子模块，则记录所述可疑子模块的挂载信息；其中，所述挂载信息包括可疑子模块挂载到系统进程的时间点；监测当前磁盘中的文件是否被修改；若监测到当前磁盘中的文件被修改，则判断在与被修改文件的同级目录中是否存在新创建的可疑文件；若在与被修改文件的同级目录中存在新创建的可疑文件，则监测当前磁盘中的文件是否再次被修改；若监测到当前磁盘中的文件再次被修改，则根据所述挂载信息，将挂载时间点距离当前时间点最近的可疑子模块，确定为勒索病毒。

[0006] 根据本发明实施例中的一具体实现方式，所述判断挂载到系统进程的子模块是否为可疑子模块，包括：根据预设的检查规则，判断已挂载到系统进程的子模块是否为可疑子模块。

[0007] 根据本发明实施例中的一具体实现方式，所述判断挂载到系统进程的子模块是否为可疑子模块，包括：监测是否有新的子模块挂载到系统进程；若监测到有新的子模块挂载到系统进程，则根据预设的检查规则，判断新挂载到系统进程的子模块是否为可疑子模块。

[0008] 根据本发明实施例中的一具体实现方式，在确定挂载到系统进程的子模块为可疑子模块之后，所述方法还包括：将可疑子模块加入到危险模块监控列表中。

[0009] 根据本发明实施例中的一具体实现方式，所述若在与被修改文件的同级目录中存在新创建的可疑文件，则监测当前磁盘中的文件是否再次被修改，包括：

[0010] 若在与被修改文件的同级目录中存在新创建的可疑文件，则加载深度分析模块，

通过所述深度分析模块，监测当前磁盘中的文件是否再次被修改。

[0011] 第二方面，本发明实施例提供一种勒索病毒识别装置，包括：

[0012] 第一判断模块，用于判断挂载到系统进程的子模块是否为可疑子模块；

[0013] 记录模块，用于若挂载到系统进程的子模块为可疑子模块，则记录所述可疑子模块的挂载信息；其中，所述挂载信息包括可疑子模块挂载到系统进程的时间点；

[0014] 第一监测模块，用于监测当前磁盘中的文件是否被修改；

[0015] 第二判断模块，用于若监测到当前磁盘中的文件被修改，则判断在与被修改文件的同级目录中是否存在新创建的可疑文件；

[0016] 第二监测模块，用于若在与被修改文件的同级目录中存在新创建的可疑文件，则监测当前磁盘中的文件是否再次被修改；

[0017] 第三判断模块，用于若监测到当前磁盘中的文件再次被修改，则根据所述挂载信息，将挂载时间点距离当前时间点最近的可疑子模块，确定为勒索病毒。

[0018] 根据本发明实施例中的一具体实现方式，所述第一判断模块，具体用于根据预设的检查规则，判断已挂载到系统进程的子模块是否为可疑子模块。

[0019] 根据本发明实施例中的一具体实现方式，所述第一判断模块，包括：挂载监测子模块，用于监测是否有新的子模块挂载到系统进程；可疑判断子模块，用于若监测到有新的子模块挂载到系统进程，则根据预设的检查规则，判断新挂载到系统进程的子模块是否为可疑子模块。

[0020] 根据本发明实施例中的一具体实现方式，所述的勒索病毒识别装置，还包括：危险模块监控列表模块。用于将可疑子模块加入到危险模块监控列表中。

[0021] 根据本发明实施例中的一具体实现方式，所述第二监测模块，具体用于：若在与被修改文件的同级目录中存在新创建的可疑文件，则加载深度分析模块，以通过所述深度分析模块，监测当前磁盘中的文件是否再次被修改。

[0022] 第三方面，本发明实施例提供一种电子设备，所述电子设备包括：壳体、处理器、存储器、电路板和电源电路，其中，电路板安置在壳体围成的空间内部，处理器和存储器设置在电路板上；电源电路，用于为上述电子设备的各个电路或器件供电；存储器用于存储可执行程序代码；处理器通过读取存储器中存储的可执行程序代码来运行与可执行程序代码对应的程序，用于执行前述任一权利要求所述的方法。

[0023] 第四方面，本发明实施例提供一种计算机可读存储介质，所述计算机可读存储介质存储有一个或者多个程序，所述一个或者多个程序可被一个或者多个处理器执行，以实现前述任一权利要求所述的方法。

[0024] 本发明实施例提供的一种勒索病毒识别方法、装置、电子设备及存储介质，通过判断挂载到系统进程的子模块是否为可疑子模块；并记录可疑子模块的挂载信息；其中，所述挂载信息包括可疑子模块挂载到系统进程的时间点；监测当前磁盘中的文件是否被修改；若当前磁盘中的文件被修改，则判断在与被修改文件的同级目录中是否存在新创建的可疑文件；若在与被修改文件的同级目录中存在新创建的可疑文件，则监测当前磁盘中的文件是否再次被修改；若监测到当前磁盘中的文件再次被修改，则根据所述挂载信息，将挂载时间点距离当前时间点最近的可疑子模块，确定为勒索病毒。本实施例可弥补恶意代码进入内网主机环境进行横向扩散后进入目标主机，强制挂载并隐藏在系统进程下，造成杀毒软

件无法防御的困境,能够快速准确地识别出勒索病毒。

附图说明

[0025] 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它的附图。

[0026] 图1为本发明的勒索病毒挂载系统进程的识别方法的示意图;

[0027] 图2为本发明的判断挂载到系统进程的子模块是否为可疑子模块的一个实施例的示意图;

[0028] 图3为本发明的勒索病毒识别装置的结构示意图;

[0029] 图4为本发明的勒索病毒识别装置的一个实施例的结构示意图;

[0030] 图5为本发明电子设备一个实施例的结构示意图。

具体实施方式

[0031] 下面结合附图对本发明实施例进行详细描述。

[0032] 应当明确,所描述的实施例仅仅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它实施例,都属于本发明保护的范围。

[0033] 第一方面,本发明实施例提供一种勒索病毒识别方法,本实施例的应用场景是应用于计算机系统中安全类应用程序,以对计算机系统中的勒索病毒进行识别。

[0034] 图1为本发明一实施例勒索病毒识别方法的示意图,如图1所示,本实施例的方法可以包括:

[0035] 步骤101、判断挂载到系统进程的子模块是否为可疑子模块。

[0036] 本实施例中,基于勒索病毒是通过挂载在操作系统进程下,从而实现对当前磁盘进行加密的特点,本实施例对挂载到当前系统已经启动或准备启动的操作系统进程(可根据配置对全系统进程或常被注入的敏感系统进程)的子模块进行安全检查,即判断其是否为可疑子模块。本步骤中对操作系统进程进行安全检查,判断操作系统进程中是否存在可疑子模块,可弥补恶意代码进入内网主机环境进行横向扩散后进入目标主机,强制挂载并隐藏在操作系统进程下,造成杀毒软件无法防御的困境。

[0037] 经过判断,若挂载到系统进程的子模块为可疑子模块,则执行步骤102,否则,监控是否有新的子模块挂载到系统进程。

[0038] 步骤102、记录所述可疑子模块的挂载信息。

[0039] 本实施例中,所述挂载信息包括可疑子模块挂载到系统进程的时间点。由于勒索病毒挂载到操作系统进程后,会立即对当前磁盘进行加密,基于勒索病毒此特点,记录可疑子模块的挂载到系统进程的时间点,有助于找出与勒索病毒行为对应的子模块。

[0040] 步骤103、监测当前磁盘中的文件是否被修改。

[0041] 本实施例中,由于勒索病毒在入侵当前磁盘后,会对当前磁盘的文件进行新建、加密和/或删除等操作,本步骤中对当前磁盘中的文件进行检测,可以对可疑子模块的行为进

行检测，从而有助于确定该进程中是否存在符合勒索病毒行为特征的可疑子模块。

[0042] 本实施例中，若监测到当前磁盘中的文件被修改，则执行步骤104，否则，继续监测当前磁盘中的文件是否被修改。

[0043] 步骤104、判断在与被修改文件的同级目录中是否存在新创建的可疑文件。

[0044] 本实施例中，由于勒索病毒对当前磁盘的文件进行加密后会生成加密文件，基于勒索病毒的此特点，本步骤中对被修改的文件的同级目录中的新建文件进行监控和判断，若被修改的文件的同级目录中存在新创建的可疑文件，则该新创建的可疑文件极有可能为勒索病毒创建的加密文件。本步骤中对被修改文件的同级目录的新建文件进行监控和判断，有助于进一步确定该进程中是否存在符合勒索病毒行为特征的可疑子模块。

[0045] 经过判断，若在与被修改文件的同级目录中存在新创建的可疑文件，则执行步骤105，否则，继续监测当前磁盘中的文件是否被修改。

[0046] 步骤105、监测当前磁盘中的文件是否再次被修改。

[0047] 本实施例中，由于磁盘中的文件通常有多个，当磁盘中的其中一个文件被修改后，又出现其他的文件被修改，则此种行为与勒索病毒的行为极为相似。本步骤结合上述步骤，即可确定此进程中存在与勒索病毒的行为一致的可疑子模块。

[0048] 本实施例中，若监测到当前磁盘中的文件再次被修改，则执行步骤106，否则继续监测当前磁盘中的文件是否被修改。

[0049] 步骤106、根据所述挂载信息，将挂载时间点距离当前时间点最近的可疑子模块，确定为勒索病毒。

[0050] 本实施例中，由于勒索病毒挂载到操作系统进程后，会立即对当前磁盘进行加密，基于勒索病毒此特点，则可以将挂载时间点距离当前时间点最近的可疑子模块，确定为勒索病毒。

[0051] 在本发明一实施例中，所述判断挂载到系统进程的子模块是否为可疑子模块(步骤101)，可包括：

[0052] 根据预设的检查规则，判断已挂载到系统进程的子模块是否为可疑子模块。

[0053] 本实施例中，对已经挂载到系统进程的子模块进行遍历安全检查。

[0054] 可选的，所述检查规则包括：文件版本合法、数字签名有效、为系统文件、建立时间距当前时间小于预设时间(所述预设时间可以设置为为1小时、30分钟等，所述预设时间可以根据需要设定)，当所述子模块不符合任一项检查规则时，判定所述子模块为可疑子模块。

[0055] 在本发明一实施例中，所述判断挂载到系统进程的子模块是否为可疑子模块(步骤101)，可包括：

[0056] 步骤1011、监测是否有新的子模块挂载到系统进程；

[0057] 本实施例中，若监测到有新的子模块挂载到系统进程，则执行步骤1012，否则，继续监控是否有新的子模块挂载到系统进程。

[0058] 步骤1012、根据预设的检查规则，判断新挂载到系统进程的子模块是否为可疑子模块。

[0059] 本实施例中，实时的检测是否有新的子模块挂载到系统进程中，当系统进程增加了新的子模块后，将对新的子模块做安全检查，使对挂载到系统进程的子模块的检查更加

全面。

[0060] 在本发明一实施例中，在确定挂载到系统进程的子模块为可疑子模块(步骤101)之后，所述方法还可包括：

[0061] 将可疑子模块加入到危险模块监控列表中。

[0062] 本实施例中，对不符合安全检查的可疑子模块均加入高危模块监控列表，对高危模块监控列表中的可疑子模块进行针对性的采集分析，结合文件版本、数字签名、系统文件归属等条件信息定位高危级别；高危模块监控列表结合勒索病毒操作特性动作，分析采集信息，精准判别勒索行为。

[0063] 在本发明一实施例中，所述监测当前磁盘中的文件是否再次被修改(步骤105)，可包括：

[0064] 加载深度分析模块，通过所述深度分析模块，监测当前磁盘中的文件是否再次被修改。

[0065] 本实施例中，在检测到在被修改的文件同级目录中建立一个可疑文件时(例如，未知扩展名的文件)，触发将具备子模块深度分析功能的深度分析模块挂载到该进程中，并进行深度监控。一旦该进程对磁盘文件再次尝试修改、删除时，可以判定该进程中的哪个子模块做了加密操作，从而精准判定勒索行为。深度分析模块在防御软件启动时，可先不加载，在需要时在加载，可使防御软件快速启动，并可节省系统资源消耗等。

[0066] 第二方面，本发明实施例提供一种勒索病毒识别装置，本实施例的应用场景是应用于计算机系统中安全类应用程序，以对计算机系统中的勒索病毒进行识别。

[0067] 图2为本发明一实施例勒索病毒识别装置的结构示意图，参看图2所示，本实施例勒索病毒识别装置，可包括：第一判断模块11、记录模块12、第一监测模块13、第二判断模块14、第二监测模块15、以及第三判断模块16；其中，第一判断模块11，用于判断挂载到系统进程的子模块是否为可疑子模块；记录模块12，用于若挂载到系统进程的子模块为可疑子模块，则记录所述可疑子模块的挂载信息；其中，所述挂载信息包括可疑子模块挂载到系统进程的时间点；第一监测模块13，用于监测当前磁盘中的文件是否被修改；第二判断模块14，用于若监测到当前磁盘中的文件被修改，则判断在与被修改文件的同级目录中是否存在新创建的可疑文件；第二监测模块15，用于若在与被修改文件的同级目录中存在新创建的可疑文件，则监测当前磁盘中的文件是否再次被修改；第三判断模块16，用于若监测到当前磁盘中的文件再次被修改，则根据所述挂载信息，将挂载时间点距离当前时间点最近的可疑子模块，确定为勒索病毒。

[0068] 本实施例的装置，可以用于执行图1所示方法实施例的技术方案，其实现原理和技术效果类似，此处不再赘述。

[0069] 在本发明一实施例中，所述第一判断模块，具体用于根据预设的检查规则，判断已挂载到系统进程的子模块是否为可疑子模块。

[0070] 在本发明一实施例中，所述第一判断模块，包括：挂载监测子模块111，用于监测是否有新的子模块挂载到系统进程；可疑判断子模块112，用于若监测到有新的子模块挂载到系统进程，则根据预设的检查规则，判断新挂载到系统进程的子模块是否为可疑子模块。

[0071] 在本发明一实施例中，所述的勒索病毒识别装置，还可包括：危险模块监控列表模块。用于将可疑子模块加入到危险模块监控列表中。

[0072] 在本发明一实施例中，所述第二监测模块，具体用于：若在与被修改文件的同级目录中存在新创建的可疑文件，则加载深度分析模块，以通过所述深度分析模块，监测当前磁盘中的文件是否再次被修改。

[0073] 本实施例中，通过判断挂载到系统进程的子模块是否为可疑子模块；并记录可疑子模块的挂载信息；其中，所述挂载信息包括可疑子模块挂载到系统进程的时间点；监测当前磁盘中的文件是否被修改；若当前磁盘中的文件被修改，则判断在与被修改文件的同级目录中是否存在新创建的可疑文件；若在与被修改文件的同级目录中存在新创建的可疑文件，则监测当前磁盘中的文件是否再次被修改；若监测到当前磁盘中的文件再次被修改，则根据所述挂载信息，将挂载时间点距离当前时间点最近的可疑子模块，确定为勒索病毒。本实施例可弥补恶意代码进入内网主机环境进行横向扩散后进入目标主机，强制挂载并隐藏在系统进程下，造成杀毒软件无法防御的困境，可快速精准的识别勒索病毒。

[0074] 第三方面，本发明实施例提供一种电子设备，如图3所示，所述电子设备可以包括：壳体41、处理器42、存储器43、电路板44和电源电路45，其中，电路板44安置在壳体41围成的空间内部，处理器42和存储器43设置在电路板44上；电源电路45，用于为上述电子设备的各个电路或器件供电；存储器43用于存储可执行程序代码；处理器42通过读取存储器43中存储的可执行程序代码来运行与可执行程序代码对应的程序，用于执行前述任一实施例所述的方法。

[0075] 处理器42对上述步骤的具体执行过程以及处理器42通过运行可执行程序代码来进一步执行的步骤，可以参见本发明图1-3所示实施例的描述，在此不再赘述。

[0076] 该电子设备以多种形式存在，包括但不限于：

[0077] (1)移动通信设备：这类设备的特点是具备移动通信功能，并且以提供话音、数据通信为主要目标。这类终端包括：智能手机(例如iPhone)、多媒体手机、功能性手机，以及低端手机等。

[0078] (2)超移动个人计算机设备：这类设备属于个人计算机的范畴，有计算和处理功能，一般也具备移动上网特性。这类终端包括：PDA、MID和UMPC设备等，例如iPad。

[0079] (3)便携式娱乐设备：这类设备可以显示和播放多媒体内容。该类设备包括：音频、视频播放器(例如iPod)，掌上游戏机，电子书，以及智能玩具和便携式车载导航设备。

[0080] (4)服务器：提供计算服务的设备，服务器的构成包括处理器、硬盘、内存、系统总线等，服务器和通用的计算机架构类似，但是由于需要提供高可靠的服务，因此在处理能力、稳定性、可靠性、安全性、可扩展性、可管理性等方面要求较高。

[0081] (5)其他具有数据交互功能的电子设备。

[0082] 第四方面，本发明实施例提供一种计算机可读存储介质，所述计算机可读存储介质存储有一个或者多个程序，所述一个或者多个程序可被一个或者多个处理器执行，以实现前述任一权利要求所述的方法。

[0083] 需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备

所固有的要素。在没有更多限制的情况下，由语句“包括一个.....”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0084] 本说明书中的各个实施例均采用相关的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。

[0085] 尤其，对于装置实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0086] 为了描述的方便，描述以上装置是以功能分为各种单元/模块分别描述。当然，在实施本发明时可以把各单元/模块的功能在同一个或多个软件和/或硬件中实现。

[0087] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体(Read-Only Memory，ROM)或随机存储记忆体(Random Access Memory，RAM)等。

[0088] 以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到的变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应以权利要求的保护范围为准。

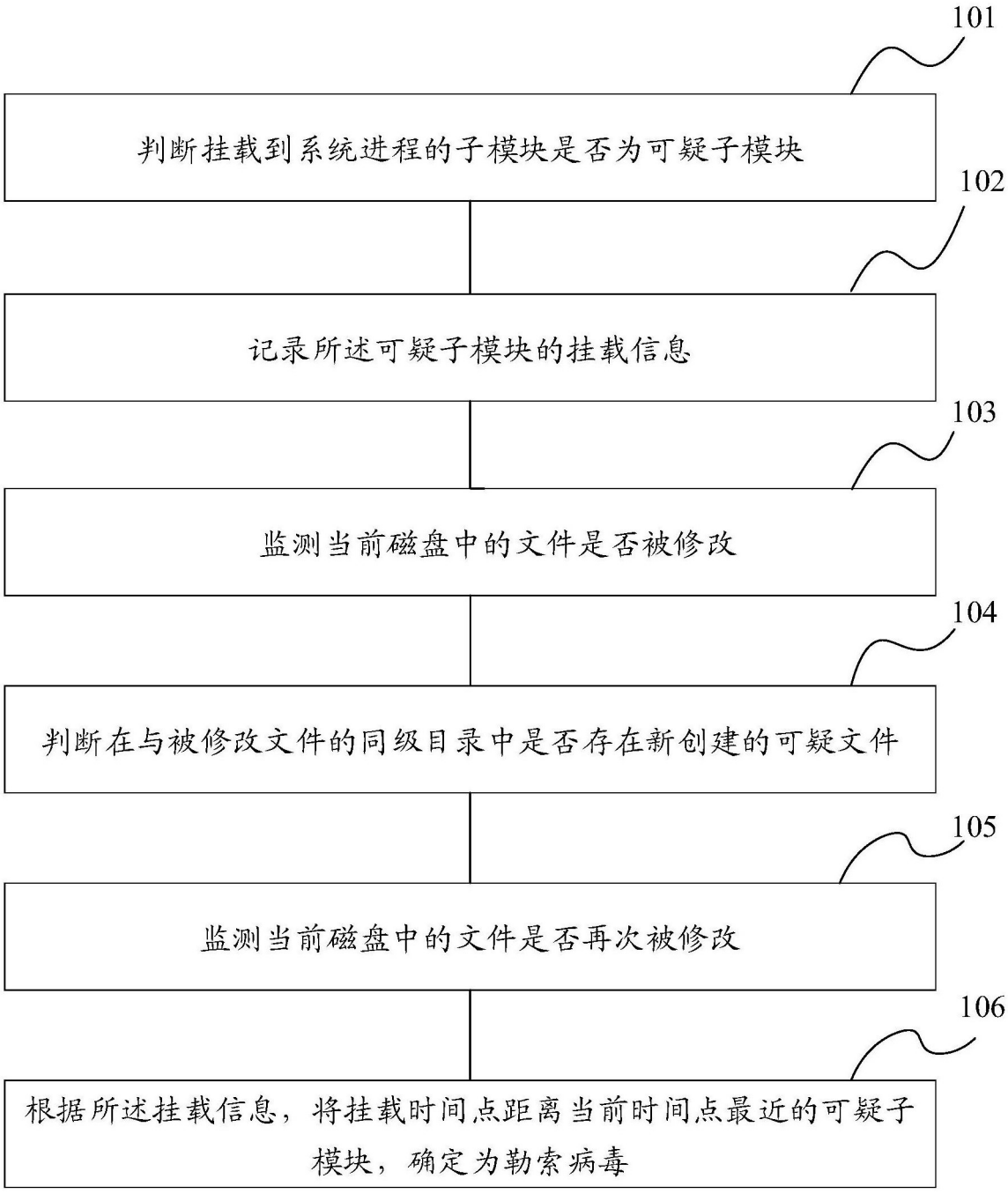

101
判断挂载到系统进程的子模块是否为可疑子模块
102
记录所述可疑子模块的挂载信息
103
监测当前磁盘中的文件是否被修改
104
判断在与被修改文件的同级目录中是否存在新创建的可疑文件
105
监测当前磁盘中的文件是否再次被修改
106
根据所述挂载信息，将挂载时间点距离当前时间点最近的可疑子模块，确定为勒索病毒

图1

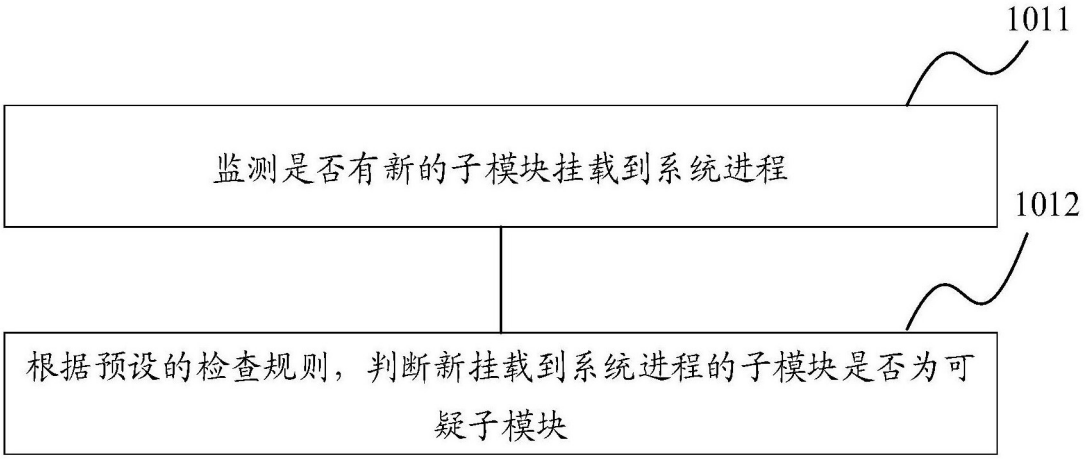

1011
监测是否有新的子模块挂载到系统进程
1012
根据预设的检查规则，判断新挂载到系统进程的子模块是否为可疑子模块

图2

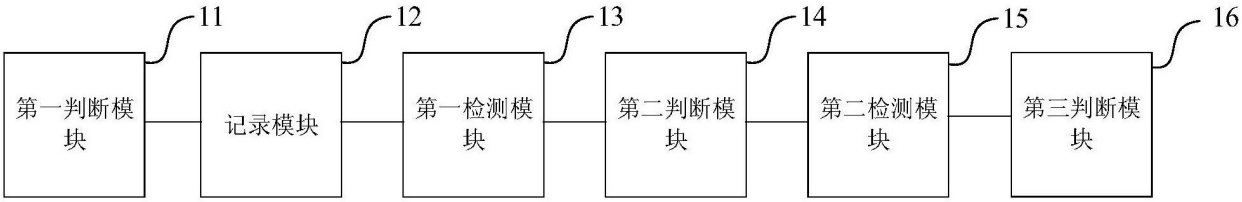

11
12
13
14
15
16
第一判断模块
记录模块
第一检测模块
第二判断模块
第二检测模块
第三判断模块

图3

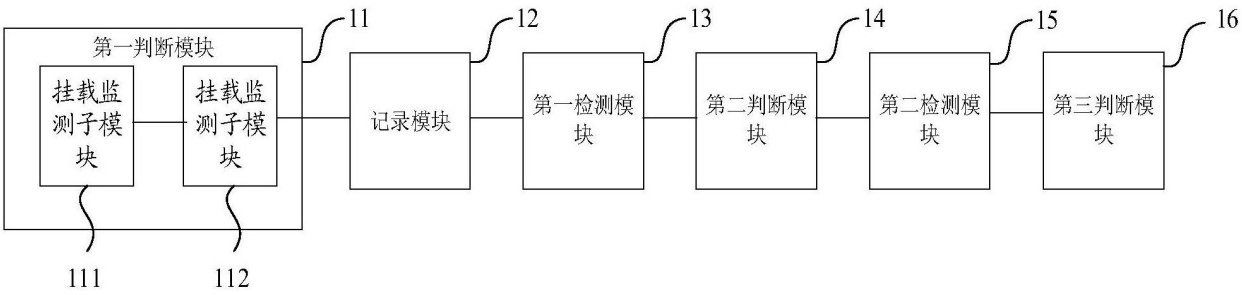

第一判断模块
挂载监测子模块
挂载监测子模块
111
112
11
12
13
14
15
16
记录模块
第一检测模块
第二判断模块
第二检测模块
第三判断模块

图4

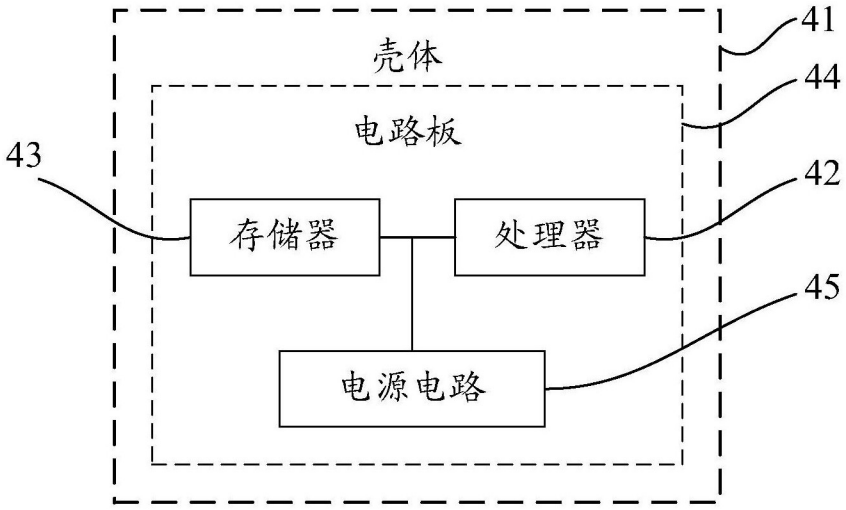


图5