

进行安装包病毒查杀的方法及装置

技术领域

本发明涉及病毒查杀技术，尤其涉及进行安装包病毒查杀的方法及装置。

5 发明背景

随着智能手机等移动终端的普及，各种移动终端应用软件层出不穷，与此同时网络上出现了许多不合法或者非正规的安装包，其中一些也就是通常所说的移动终端病毒，具体如手机病毒。

10 目前，常在移动终端增加病毒查杀功能，例如在移动终端安装安全软件，用于对移动终端上的所有安装包进行病毒查杀。现有进行病毒查杀的方案包括：接收病毒查杀指令后，找出移动终端上存储的所有安装包，读取安装包的描述信息，根据读取的描述信息进行安装包分析，确定安装包是否有病毒。所述描述信息包括安装包名称、厂商证书、统一标识（UID，Union Identification）、安装包版本号及文件大小等。

15 找到安装包、读取安装包的描述信息，是对安装包进行拆包的过程，该过程非常耗时；在接收病毒查杀指令后，对所有安装包进行拆包、分析，将耗费较长的时间，大大影响了病毒查杀速度。

发明内容

20 本发明提供了一种进行安装包病毒查杀的方法，该方法能够提高安装包病毒查杀的速度。

本发明还提供了一种进行安装包病毒查杀的装置，该装置能够提高安装包病毒查杀的速度。

一种进行安装包病毒查杀的方法，该方法包括：

对安装包进行拆包，缓存拆包得到的描述信息；

接收病毒查杀启动指令，读取缓存的描述信息；

根据读取的描述信息进行安装包分析，确定安装包是否有病毒。

- 5 一种进行安装包病毒查杀的装置，该装置包括拆包单元、指令处理单元和分析单元；

所述拆包单元，用于对安装包进行拆包，缓存拆包得到的描述信息；

所述指令处理单元，用于接收病毒查杀启动指令，从所述拆包单元读取缓存的描述信息，传送给所述分析单元；

- 10 所述分析单元，用于根据读取的描述信息进行安装包分析，确定安装包是否有病毒。

从上述方案可以看出，本发明先对安装包进行拆包，缓存描述信息，当需要对安装包进行病毒查杀时，直接读取缓存的描述信息，进行安装包分析，确定安装包是否有病毒。这样，将病毒查杀分解为拆包和分析
15 两个操作异步进行，将比较耗时的拆包操作率先完成，大大加快了病毒查杀的速度。

附图简要说明

图 1 为本发明实施例中进行安装包病毒查杀的方法示意性流程图。

图 2 为本发明实施例中进行安装包病毒查杀的方法流程图实例。

- 20 图 3 为本发明实施例中进行安装包病毒查杀的装置结构示意图。

实施本发明的方式

为使本发明的目的、技术方案和优点更加清楚明白，下面结合实施例和附图，对本发明进一步详细说明。

本发明实施例中将病毒查杀分解为拆包和分析两个操作异步进行，将比较耗时的拆包操作率先完成；参见图 1，为本发明实施例中进行安装包病毒查杀的方法示意性流程图，其包括以下步骤：

步骤 101，对安装包进行拆包，缓存拆包得到的描述信息。

5 本步骤可采用创建活动对象(Active Object)的方式进行安装包拆包，具体包括：创建关于拆包的活动对象，调度活动对象，进行安装包路径扫描，读取扫描到的安装包的描述信息。

活动对象为一种对象类型，创建活动对象后，可在需要时对活动对象进行调度以执行相应的操作，本发明实施例中创建的活动对象为关于拆包的活动对象。调度活动对象之前，该方法还可以包括：判断当前资源是否处于空闲状态，如果是，则执行所述调度活动对象的步骤。所述
10 判断当前资源是否处于空闲状态可包括：判断当前资源占用率是否小于或等于设定数值，如果是，则确定当前资源处于空闲状态。所述当前资源占用率例如为 CPU 占用率或内存占用率等。

15 所述描述信息包括安装包名称、厂商证书、UID、安装包版本号及文件大小等。

步骤 102，接收病毒查杀启动指令，读取缓存的描述信息。

步骤 103，根据读取的描述信息进行安装包分析，确定安装包是否有病毒。

20 参见图 2，为本发明实施例中进行安装包病毒查杀的流程图实例，其包括以下步骤：

步骤 201，创建关于拆包的活动对象。

步骤 202，判断当前资源占用率是否小于或等于设定数值。

判断当前资源占用率是否小于或等于设定数值，如果是，则确定当前资源处于空闲状态，执行步骤 203；否则，继续判断。
25

所述设定数值可根据需要设置。

步骤 203, 调度所述活动对象, 进行安装包路径扫描, 读取扫描到的安装包的描述信息。

步骤 204, 缓存所述描述信息。

5 步骤 205, 接收病毒查杀启动指令。

用户需要进行病毒查杀时, 启动移动终端上的安全功能。

步骤 206, 判断是否有缓存的描述信息, 如果有, 则执行步骤 207, 否则执行步骤 208。

步骤 207, 读取缓存的描述信息, 根据读取的描述信息进行安装包
10 分析, 确定安装包是否有病毒。

步骤 208, 进行安装包拆包, 根据拆包得到的描述信息进行安装包分析, 确定安装包是否有病毒。

进行安装包拆包可具体包括: 进行安装包路径扫描, 读取扫描到的安装包的描述信息。

15 参见图 3, 为本发明实施例中进行安装包病毒查杀的装置结构示意图, 该装置包括拆包单元、指令处理单元和分析单元。

所述拆包单元, 用于对安装包进行拆包, 缓存拆包得到的描述信息。

所述指令处理单元, 用于接收病毒查杀启动指令, 从所述拆包单元读取缓存的描述信息, 传送给所述分析单元。

20 所述分析单元, 用于根据所述指令处理单元传送的描述信息进行安装包分析, 确定安装包是否有病毒。

可选地, 所述拆包单元包括活动对象创建子单元和调度器。

所述活动对象创建子单元, 用于创建关于拆包的活动对象。

所述调度器, 用于调度所述活动对象创建子单元创建的活动对象,
25 进行安装包路径扫描, 读取扫描到的安装包的描述信息。

可选地，所述调度器包括判断模块和调度模块。

所述判断模块，用于在判断出当前资源处于空闲状态时，向所述调度模块发送调度指令。

所述调度模块，用于接收所述调度指令，调度所述活动对象创建子
5 单元创建的活动对象，进行安装包路径扫描，并对安装包进行拆包。

可选地，所述描述信息包括安装包名称、厂商证书、UID、安装包版本号及文件大小等，所述当前资源占用率包括 CPU 占用率或内存占用率。

本发明实施例中的技术方案适用于移动终端的安装包病毒查杀，所
10 述移动终端例如为手机、个人数字助理（PDA, Personal Digital Assistant）等。

本发明实施例中先对安装包进行拆包，并缓存拆包得到的描述信息，当需要对安装包进行病毒查杀时，直接读取缓存的描述信息，进行安装包分析，确定安装包是否有病毒。这样，将病毒查杀分解为拆包和分析
15 两个操作异步进行，将比较耗时的拆包操作率先完成，大大加快了病毒查杀的速度。

并且，在系统资源处于空闲状态时主动执行拆包操作、并缓存描述信息，这样，既不影响其它任务的执行，也充分利用了系统的空闲资源。

以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡
20 在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明保护的范围之内。

权利要求书

- 1、一种进行安装包病毒查杀的方法，其特征在于，该方法包括：
对安装包进行拆包，并缓存拆包得到的描述信息；
在接收到病毒查杀启动指令后，读取缓存的描述信息；
5 根据读取的描述信息进行安装包分析，确定安装包是否有病毒。
- 2、如权利要求 1 所述的方法，其特征在于，所述对安装包进行拆包包括：
创建关于拆包的活动对象；
调度所述活动对象，进行安装包路径扫描，读取扫描到的安装包的
10 描述信息。
- 3、如权利要求 2 所述的方法，其特征在于，所述调度所述活动对象之前，该方法还包括：
判断当前资源是否处于空闲状态，如果是，则执行所述调度所述活动对象的步骤。
- 15 4、如权利要求 3 所述的方法，其特征在于，所述判断当前资源是否处于空闲状态包括：判断当前资源占用率是否小于或等于设定数值，如果是，则确定当前资源处于空闲状态。
- 5、如权利要求 4 所述的方法，其特征在于，所述当前资源占用率包括 CPU 占用率或内存占用率。
- 20 6、如权利要求 1 至 5 中任一项所述的方法，其特征在于，所述描述信息包括安装包名称、厂商证书、统一标识、安装包版本号及文件大小。
- 7、一种进行安装包病毒查杀的装置，其特征在于，该装置包括拆包单元、指令处理单元和分析单元；
所述拆包单元，用于对安装包进行拆包，缓存拆包得到的描述信息；

所述指令处理单元，用于在接收到病毒查杀启动指令后，从所述拆包单元中读取缓存的描述信息，传送给所述分析单元；

所述分析单元，用于根据所述指令处理单元传送的描述信息进行安装包分析，确定安装包是否有病毒。

- 5 8、如权利要求 7 所述的装置，其特征在于，所述拆包单元包括活动对象创建子单元和调度器；

所述活动对象创建子单元，用于创建关于拆包的活动对象；

所述调度器，用于调度所述活动对象创建子单元创建的活动对象，进行安装包路径扫描，读取扫描到的安装包的描述信息。

- 10 9、如权利要求 8 所述的装置，其特征在于，所述调度器包括判断模块和调度模块；

所述判断模块，用于在判断出当前资源处于空闲状态时，向所述调度模块发送调度指令；

- 15 所述调度模块，用于接收所述调度指令，调度所述活动对象创建子单元创建的活动对象，进行安装包路径扫描，并对安装包进行拆包。

10、如权利要求 9 所述的装置，其特征在于，所述当前资源占用率包括 CPU 占用率或内存占用率。