(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 104573515 A
(43)申请公布日 2015.04.29

(21)申请号 201410802502.6

(22)申请日 2014.12.19

(71)申请人 百度在线网络技术(北京)有限公司
地址 100085 北京市海淀区上地十街10号百度大厦

(72)发明人 邹荣新 梅银明 项柱 胡汉中

(74)专利代理机构 北京鸿德海业知识产权代理事务所(普通合伙) 11412
代理人 袁媛

(51)Int.Cl.
*G06F 21/56*(2013.01)
*G06F 11/34*(2006.01)
*H04L 29/08*(2006.01)

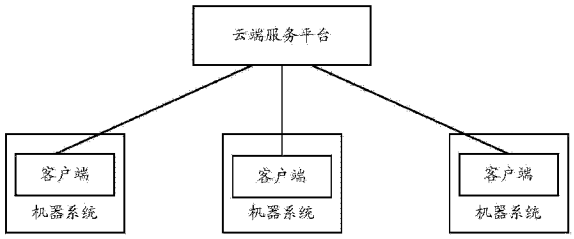
权利要求书3页 说明书9页 附图4页

(54)发明名称

一种病毒处理方法、装置和系统

(57)摘要

本发明提供了一种病毒处理方法、装置和系统，客户端将扫描日志上报给云端服务平台，和/或在根据扫描日志鉴定出病毒家族信息后将病毒家族信息上报给云端服务平台。云端服务平台对扫描日志进行鉴定后得到的病毒家族信息，和/或接收到来自客户端的病毒家族信息后，将病毒家族信息对应的病毒清除指令下发给客户端，供客户端执行病毒清除指令。本发明这种由云端针对病毒家族信息进行病毒清除指令下发的方式，相比较单纯由客户端进行行为分析和删除文件的方式，对病毒的处理更加个性化和精准，提高了机器系统的安全性。




CN 104573515 A

1. 一种病毒处理方法，其特征在于，该方法包括：

确定客户端扫描的病毒体行为所对应的病毒家族信息；

根据病毒家族信息与病毒清除指令之间的对应关系，将确定的病毒家族信息所对应的病毒清除指令下发给所述客户端，以供所述客户端执行所述病毒清除指令进行病毒体的清除。

2. 根据权利要求 1 所述的方法，其特征在于，所述确定客户端扫描的病毒体行为所对应的病毒家族信息包括：

接收所述客户端上报的扫描日志，所述扫描日志包含所述客户端扫描的病毒体行为信息；

将所述病毒体行为信息与云端的行为链脚本库进行匹配，确定恶意病毒体行为对应的病毒家族信息，其中所述行为链脚本库包含病毒家族的恶意病毒体行为信息。

3. 根据权利要求 1 所述的方法，其特征在于，所述确定客户端扫描的病毒体行为所对应的病毒家族信息包括：

接收所述客户端上报的鉴定结果；

从所述鉴定结果中获取病毒家族信息，所述病毒家族信息是所述客户端将扫描的病毒体行为信息与客户端本地的行为链脚本库进行匹配后确定的，其中所述行为链脚本库包含病毒家族的恶意病毒体行为信息。

4. 根据权利要求 2 所述方法，其特征在于，该方法还包括：

对客户端上报的扫描日志进行分析得到更新病毒体行为信息；

利用更新病毒体行为信息更新云端的行为链脚本库。

5. 根据权利要求 2 所述的方法，其特征在于，所述确定客户端扫描的病毒体行为所对应的病毒家族信息还包括：

接收所述客户端上报的鉴定结果；

从所述鉴定结果中获取病毒家族信息，所述病毒家族信息是所述客户端将扫描的病毒体行为信息与客户端本地的行为链脚本库进行匹配后确定的，其中所述行为链脚本库包含病毒家族的恶意病毒体行为信息。

6. 根据权利要求 5 所述的方法，其特征在于，该方法还包括：

如果将扫描日志包含的病毒体行为信息与云端的行为链脚本库进行匹配确定出的病毒家族信息与从所述鉴定结果中获取的病毒家族信息不一致，则采用将扫描日志包含的病毒体行为信息与云端的行为链脚本库进行匹配确定出的病毒家族信息来确定下发的病毒清除指令，或者采用人为鉴定出的病毒家族信息来确定下发的病毒清除指令。

7. 根据权利要求 1 至 6 任一权项所述的方法，其特征在于，所述病毒体行为信息为对以下内容中的至少一种进行扫描后得到的行为信息：

进程、加载模块、驱动、服务、Rootkit、启动项、IE 相关的项目、引导病毒、系统目录、桌面目录、开始菜单、常用软件、脚本、系统组件、登录部分、系统启动项等。

8. 根据权利要求 1 至 6 任一权项所述的方法，其特征在于，所述病毒清除指令包括以下操作的指令：

锁定默认主页、修改默认浏览器搜索主页、下载指定工具软件或清除恶意病毒体行为的关联内容。

9. 一种病毒处理方法，其特征在于，该方法包括：

扫描病毒体行为；

将扫描日志上报云端服务平台；和 / 或，利用本地的行为链脚本库，对所述病毒体行为进行鉴定，如果鉴定出恶意病毒体行为，则将恶意病毒体行为对应的病毒家族信息上报给云端服务平台，其中所述行为链脚本库包含病毒家族的恶意病毒体行为信息；

接收并执行所述云端服务平台下发的病毒清除指令。

10. 根据权利要求 9 所述的方法，其特征在于，该方法还包括：如果鉴定出恶意病毒体行为，则清除恶意病毒体行为的关联内容。

11. 根据权利要求 9 所述的方法，其特征在于，该方法还包括：

加载云端的行为链脚本库，利用云端的行为链脚本库更新所述本地的行为链脚本库。

12. 根据权利要求 9 至 11 任一权项所述的方法，其特征在于，所述病毒清除指令包括以下操作的指令：

锁定默认主页、修改默认浏览器搜索主页、下载指定工具软件或清除恶意病毒体行为的关联内容。

13. 一种病毒处理装置，其特征在于，该装置包括：

病毒确定单元，用于确定客户端扫描的病毒体行为所对应的病毒家族信息；

指令下发单元，用于根据病毒家族信息与病毒清除指令之间的对应关系，将所述病毒确定单元确定的病毒家族信息所对应的病毒清除指令下发给所述客户端，以供所述客户端执行所述病毒清除指令进行病毒体的清除。

14. 根据权利要求 13 所述的装置，其特征在于，所述病毒确定单元包括：

第一接收子单元，用于接收所述客户端上报的扫描日志，所述扫描日志包含所述客户端扫描的病毒体行为信息；

匹配子单元，用于将所述病毒体行为信息与云端的行为链脚本库进行匹配，确定恶意病毒体行为对应的病毒家族信息，其中所述行为链脚本库包含病毒家族的恶意病毒体行为信息。

15. 根据权利要求 13 所述的装置，其特征在于，所述病毒确定单元包括：

第二接收子单元，用于接收所述客户端上报的鉴定结果；

获取子单元，用于从所述鉴定结果中获取病毒家族信息，所述病毒家族信息是所述客户端将扫描的病毒体行为信息与客户端本地的行为链脚本库进行匹配后确定的，其中所述行为链脚本库包含病毒家族的恶意病毒体行为信息。

16. 根据权利要求 14 所述的装置，其特征在于，该装置还包括：

联合分析单元，用于对客户端上报的扫描日志进行分析得到更新病毒体行为信息；

库更新单元，用于利用更新病毒体行为信息更新云端的行为链脚本库。

17. 根据权利要求 14 所述的装置，其特征在于，所述病毒确定单元还包括：

第二接收子单元，用于接收所述客户端上报的鉴定结果；

获取子单元，用于从所述鉴定结果中获取病毒家族信息，所述病毒家族信息是所述客户端将扫描的病毒体行为信息与客户端本地的行为链脚本库进行匹配后确定的，其中所述行为链脚本库包含病毒家族的恶意病毒体行为信息。

18. 根据权利要求 17 所述的装置，其特征在于，如果所述匹配子单元确定出的病毒家

族信息与所述获取子单元获取的病毒家族信息不一致，则所述指令下发单元采用所述匹配子单元确定出的病毒家族信息来确定下发的病毒清楚指令，或者采用人为鉴定出的病毒家族信息来确定下发的病毒清除指令。

19. 根据权利要求 13 至 18 任一权项所述的装置，其特征在于，所述病毒体行为信息为对以下内容中的至少一种进行扫描后得到的行为信息：

进程、加载模块、驱动、服务、Rootkit、启动项、IE 相关的项目、引导病毒、系统目录、桌面目录、开始菜单、常用软件、脚本、系统组件、登录部分、系统启动项等。

20. 根据权利要求 13 至 18 任一权项所述的装置，其特征在于，所述病毒清除指令包括以下操作的指令：

锁定默认主页、修改默认浏览器搜索主页、下载指定工具软件或清除恶意病毒体行为的关联内容。

21. 一种病毒处理装置，其特征在于，该装置包括：日志上报单元和病毒鉴定单元中的至少一个、行为扫描单元以及指令处理单元；

所述行为扫描单元，用于扫描病毒体行为；

所述日志上报单元，用于将扫描日志上报云端服务平台；

所述病毒鉴定单元，用于利用本地的行为链脚本库，对所述病毒体行为进行鉴定，如果鉴定出恶意病毒体行为，则将恶意病毒体行为对应的病毒家族信息上报给云端服务平台，其中所述行为链脚本库包含病毒家族的恶意病毒体行为信息；

所述指令处理单元，用于接收并执行所述云端服务平台下发的病毒清除指令。

22. 根据权利要求 21 所述的装置，其特征在于，该装置还包括：

病毒清除单元，用于如果所述病毒鉴定单元鉴定出恶意病毒体行为，则清除恶意病毒体行为的关联内容。

23. 根据权利要求 21 所述的装置，其特征在于，该装置还包括：

库更新单元，用于加载云端的行为链脚本库，利用云端的行为链脚本库更新所述本地的行为链脚本库。

24. 根据权利要求 21 至 23 任一权项所述的装置，其特征在于，所述病毒清除指令包括以下操作的指令：

锁定默认主页、修改默认浏览器搜索主页、下载指定工具软件或清除恶意病毒体行为的关联内容。

25. 一种病毒处理的系统，该系统包括：客户端和云端处理平台；

所述云端处理平台包括如权利要求 13 至 18 任一权项所述的装置；

所述客户端包括如权利要求 21 至 23 任一权项所述的装置。

# 一种病毒处理方法、装置和系统

## 【技术领域】

[0001] 本发明涉及计算机应用技术领域，特别涉及一种病毒处理方法、装置和系统。

## 【背景技术】

[0002] 随着互联网的快速发展，基于病毒模式聚集网站流量，并通过流量广告变现的灰色产业利益链已经形成。每日新增的流氓软件已经数以百计，使用各种猥琐的技术，通过进程、注册表、文件等方式相互捆绑或守护，不断更新病毒体的行为特征，防止杀毒软件进行查杀。

[0003] 目前互联网式病毒文件流行的方式是：通过云端控制指令在机器系统修改用户默认的浏览器主页以及搜索引擎，修改关键词搜索排名，劫持浏览器弹出广告，恶意篡改桌面快捷方式关联，安装用户不需要的浏览器插件恶意软件，窃取用户的隐私内容等。而传统的杀毒软件主要查杀文件的恶意行为，发现恶意行为时删除相应的文件。当遇到这类互联网式病毒文件时，单纯在机器系统的客户端进行行为分析和删除文件往往无法完全清除病毒体，机器系统安全性较差。

## 【发明内容】

[0004] 有鉴于此，本发明提供了一种病毒处理方法、装置和系统，以便于提高机器系统的安全性。

[0005] 具体技术方案如下：

[0006] 本发明提供了一种病毒处理方法，该方法包括：

[0007] 确定客户端扫描的病毒体行为所对应的病毒家族信息；

[0008] 根据病毒家族信息与病毒清除指令之间的对应关系，将确定的病毒家族信息所对应的病毒清除指令下发给所述客户端，以供所述客户端执行所述病毒清除指令进行病毒体的清除。

[0009] 根据本发明一优选实施方式，所述确定客户端扫描的病毒体行为所对应的病毒家族信息包括：

[0010] 接收所述客户端上报的扫描日志，所述扫描日志包含所述客户端扫描的病毒体行为信息；

[0011] 将所述病毒体行为信息与云端的行为链脚本库进行匹配，确定恶意病毒体行为对应的病毒家族信息，其中所述行为链脚本库包含病毒家族的恶意病毒体行为信息。

[0012] 根据本发明一优选实施方式，所述确定客户端扫描的病毒体行为所对应的病毒家族信息包括：

[0013] 接收所述客户端上报的鉴定结果；

[0014] 从所述鉴定结果中获取病毒家族信息，所述病毒家族信息是所述客户端将扫描的病毒体行为信息与客户端本地的行为链脚本库进行匹配后确定的，其中所述行为链脚本库包含病毒家族的恶意病毒体行为信息。

[0015] 根据本发明一优选实施方式，该方法还包括：

[0016] 对客户端上报的扫描日志进行分析得到更新病毒体行为信息；

[0017] 利用更新病毒体行为信息更新云端的行为链脚本库。

[0018] 根据本发明一优选实施方式，如果将扫描日志包含的病毒体行为信息与云端的行为链脚本库进行匹配确定出的病毒家族信息与从所述鉴定结果中获取的病毒家族信息不一致，则采用将扫描日志包含的病毒体行为信息与云端的行为链脚本库进行匹配确定出的病毒家族信息来确定下发的病毒清除指令，或者采用人为鉴定出的病毒家族信息来确定下发的病毒清除指令

[0019] 根据本发明一优选实施方式，所述病毒体行为信息为对以下内容中的至少一种进行扫描后得到的行为信息：

[0020] 进程、加载模块、驱动、服务、Rootkit、启动项、IE 相关的项目、引导病毒、系统目录、桌面目录、开始菜单、常用软件、脚本、系统组件、登录部分、系统启动项等。

[0021] 根据本发明一优选实施方式，所述病毒清除指令包括以下操作的指令：

[0022] 锁定默认主页、修改默认浏览器搜索主页、下载指定工具软件或清除恶意病毒体行为的关联内容。

[0023] 本发明还提供了一种病毒处理方法，该方法包括：

[0024] 扫描病毒体行为；

[0025] 将扫描日志上报云端服务平台；和 / 或，利用本地的行为链脚本库，对所述病毒体行为进行鉴定，如果鉴定出恶意病毒体行为，则将恶意病毒体行为对应的病毒家族信息上报给云端服务平台，其中所述行为链脚本库包含病毒家族的恶意病毒体行为信息；

[0026] 接收并执行所述云端服务平台下发的病毒清除指令。

[0027] 根据本发明一优选实施方式，该方法还包括：如果鉴定出恶意病毒体行为，则清除恶意病毒体行为的关联内容。

[0028] 根据本发明一优选实施方式，该方法还包括：

[0029] 加载云端的行为链脚本库，利用云端的行为链脚本库更新所述本地的行为链脚本库。

[0030] 根据本发明一优选实施方式，所述病毒清除指令包括以下操作的指令：

[0031] 锁定默认主页、修改默认浏览器搜索主页、下载指定工具软件或清除恶意病毒体行为的关联内容。

[0032] 本发明还提供了一种病毒处理装置，该装置包括：

[0033] 病毒确定单元，用于确定客户端扫描的病毒体行为所对应的病毒家族信息；

[0034] 指令下发单元，用于根据病毒家族信息与病毒清除指令之间的对应关系，将所述病毒确定单元确定的病毒家族信息所对应的病毒清除指令下发给所述客户端，以供所述客户端执行所述病毒清除指令进行病毒体的清除。

[0035] 根据本发明一优选实施方式，所述病毒确定单元包括：

[0036] 第一接收子单元，用于接收所述客户端上报的扫描日志，所述扫描日志包含所述客户端扫描的病毒体行为信息；

[0037] 匹配子单元，用于将所述病毒体行为信息与云端的行为链脚本库进行匹配，确定恶意病毒体行为对应的病毒家族信息，其中所述行为链脚本库包含病毒家族的恶意病毒体

行为信息。

[0038] 根据本发明一优选实施方式，所述病毒确定单元包括：

[0039] 第二接收子单元，用于接收所述客户端上报的鉴定结果；

[0040] 获取子单元，用于从所述鉴定结果中获取病毒家族信息，所述病毒家族信息是所述客户端将扫描的病毒体行为信息与客户端本地的行为链脚本库进行匹配后确定的，其中所述行为链脚本库包含病毒家族的恶意病毒体行为信息。

[0041] 根据本发明一优选实施方式，该装置还包括：

[0042] 联合分析单元，用于对客户端上报的扫描日志进行分析得到更新病毒体行为信息；

[0043] 库更新单元，用于利用更新病毒体行为信息更新云端的行为链脚本库。

[0044] 根据本发明一优选实施方式，如果所述匹配子单元确定出的病毒家族信息与所述获取子单元获取的病毒家族信息不一致，则所述指令下发单元采用所述匹配子单元确定出的病毒家族信息来确定下发的病毒清楚指令，或者采用人为鉴定出的病毒家族信息来确定下发的病毒清除指令。

[0045] 根据本发明一优选实施方式，所述病毒体行为信息为对以下内容中的至少一种进行扫描后得到的行为信息：

[0046] 进程、加载模块、驱动、服务、Rootkit、启动项、IE 相关的项目、引导病毒、系统目录、桌面目录、开始菜单、常用软件、脚本、系统组件、登录部分、系统启动项等。

[0047] 根据本发明一优选实施方式，所述病毒清除指令包括以下操作的指令：

[0048] 锁定默认主页、修改默认浏览器搜索主页、下载指定工具软件或清除恶意病毒体行为的关联内容。

[0049] 本发明还提供了一种病毒处理装置，该装置包括：日志上报单元和病毒鉴定单元中的至少一个、行为扫描单元以及指令处理单元；

[0050] 所述行为扫描单元，用于扫描病毒体行为；

[0051] 所述日志上报单元，用于将扫描日志上报云端服务平台；

[0052] 所述病毒鉴定单元，用于利用本地的行为链脚本库，对所述病毒体行为进行鉴定，如果鉴定出恶意病毒体行为，则将恶意病毒体行为对应的病毒家族信息上报给云端服务平台，其中所述行为链脚本库包含病毒家族的恶意病毒体行为信息；

[0053] 所述指令处理单元，用于接收并执行所述云端服务平台下发的病毒清除指令。

[0054] 根据本发明一优选实施方式，该装置还包括：

[0055] 病毒清除单元，用于如果所述病毒鉴定单元鉴定出恶意病毒体行为，则清除恶意病毒体行为的关联内容。

[0056] 根据本发明一优选实施方式，该装置还包括：

[0057] 库更新单元，用于加载云端的行为链脚本库，利用云端的行为链脚本库更新所述本地的行为链脚本库。

[0058] 根据本发明一优选实施方式，所述病毒清除指令包括以下操作的指令：

[0059] 锁定默认主页、修改默认浏览器搜索主页、下载指定工具软件或清除恶意病毒体行为的关联内容。

[0060] 本发明还提供了一种病毒处理的系统，该系统包括：客户端和云端处理平台；

[0061] 所述云端处理平台包括上述第一种装置；

[0062] 所述客户端包括上述第二种装置。

[0063] 由以上技术方案可以看出，在本发明中客户端将扫描日志上报给云端服务平台，和/或在根据扫描日志鉴定出病毒家族信息后将病毒家族信息上报给云端服务平台。云端服务平台对扫描日志进行鉴定后得到的病毒家族信息，和/或接收到来自客户端的病毒家族信息后，将病毒家族信息对应的病毒清除指令下发给客户端，供客户端执行病毒清除指令。本发明这种由云端针对病毒家族信息进行病毒清除指令下发的方式，相比较单纯由客户端进行行为分析和删除文件的方式，对病毒的处理更加个性化和精准，提高了机器系统的安全性。

## 【附图说明】

[0064] 图 1 为本发明实施例提供的系统结构图；

[0065] 图 2 为本发明实施例提供的客户端执行的病毒处理方法流程图；

[0066] 图 3 为本发明实施例提供的云端服务平台执行的病毒处理方法流程图；

[0067] 图 4 为本发明实施例提供的一种装置结构图；

[0068] 图 5 为本发明实施例提供的另一种装置结构图。

## 【具体实施方式】

[0069] 为了使本发明的目的、技术方案和优点更加清楚，下面结合附图和具体实施例对本发明进行详细描述。

[0070] 本发明实施例主要基于如图 1 中所示的系统，该系统中包括客户端和云端服务平台，其中客户端可以设置于诸如 PC、手机、平板电脑等机器系统中，负责该机器系统的安全。

[0071] 其中在本发明实施例中，客户端可以具备以下功能：

[0072] 1) 扫描病毒体行为，这是客户端最基本的功能。在此说明本发明实施例中涉及的几个概念：“病毒体”指的是病毒母体，即病毒传播的初始文件，母体执行后会产生各种子文件及其相关行为，病毒母体本身的文件并不一定都是恶意的。“恶意病毒体”指的是恶意病毒母体，即本身能释放出恶意子文件或恶意的网络行为。“病毒体行为”包括病毒母体可能的所有行为，例如病毒体行为可以是对以下内容进行扫描后得到的行为信息：进程、加载模块、驱动、服务、Rootkit(Rootkit 是指其主要功能为隐藏其他程式进程的软件，可能是一个或一个以上的软件组合)、启动项、IE 相关的项目、引导病毒、系统目录、桌面目录、开始菜单、常用软件、脚本、系统组件、登录部分、系统启动项等。“恶意病毒体行为”为恶意病毒母体的行为。

[0073] 2) 将扫描日志上报云端服务平台，该扫描日志包含该客户端扫描的病毒体行为信息，上报给云端服务平台供其进行分析。

[0074] 3) 利用本地的行为链脚本库，对病毒体行为进行鉴定。其中行为链脚本库包含病毒家族的恶意病毒体行为信息，将客户端扫描的病毒体行为信息与行为链脚本库进行匹配，以确定扫描的病毒体行为是否为恶意病毒体行为，并可以进一步确定出病毒家族信息。其中，“病毒家族”指的是一组行为相似的恶意病毒体的统称，属于同一病毒家族的恶意病毒体通常属于同一制作者或者来源于同一病毒源文件（例如由同一病毒源文件修改得

到)。例如,在行为链脚本库中,将属于同一病毒家族的恶意病毒体行为信息进行了整合,通过恶意病毒体行为能够确定出其对应的病毒家族信息。

[0075] 另外,客户端本地的行为链脚本库可以是加载云端服务平台的行为链脚本库后存储于本地得到的。举例来说,客户端可以周期性地从云端服务平台加载行为链脚本库并对本地的行为链脚本库进行更新,即下述的功能 6)。

[0076] 4) 如果鉴定出恶意病毒体行为,则将恶意病毒体行为对应的病毒家族信息上报给云端服务平台。这里的病毒家族信息可以是诸如病毒家族 ID(标识)等信息。也就是说,如果客户端本地已经鉴定得到病毒家族 ID,则将病毒家族 ID 直接上报给云端服务平台。

[0077] 5) 如果鉴定出恶意病毒体行为,则清除该客户端所在机器系统中的恶意病毒体行为的关联内容。除了上报病毒家族信息之外,在客户端本地可以存在病毒清除的机制,清除客户端所在机器系统中恶意病毒体行为的关联内容,诸如:停止恶意病毒体的服务,删除恶意病毒体的文件,删除恶意病毒体的注册表项或相关活动项,修复浏览器默认主页。在进行上述清除处理之后,还可以进一步对可能影响机器系统运行的文件进行初始化修复处理,即将其恢复至初始状态,从而确保机器系统能够正常工作。

[0078] 6) 加载云端的行为链脚本库,利用云端的行为链脚本库更新本地的行为链脚本库。

[0079] 云端服务平台可以具备以下功能:

[0080] 1) 确定客户端扫描的病毒体行为所对应的病毒家族信息。在此,本功能的实现可以采用以下两种方式:

[0081] 第一种方式、接收客户端上报的扫描日志,该扫描日志包含了客户端扫描的病毒体行为信息,将该病毒体行为信息与云端的行为链脚本库进行匹配,确定恶意病毒体行为信息对应的病毒家族信息。同样,该行为链脚本库中也包含病毒家族的恶意病毒体行为信息。该行为链脚本库是由各机器系统中客户端上报的扫描日志进行分析后得到的,也可以结合人工分析和设置的因素。

[0082] 第二种方式、直接接收客户端上报的鉴定结果,该鉴定结果中包含客户端将扫描的病毒体行为信息与客户端本地的行为链脚本库进行匹配后确定的病毒家族信息。

[0083] 2) 根据病毒家族信息与病毒清除指令之间的对应关系,将病毒家族信息所对应的病毒清除指令下发给客户端。在云端服务平台中维护着病毒家族信息与病毒清除指令之间的对应关系,这些病毒清除指令用于指导客户端进行操作以对相应病毒家族的行为进行清除。这一对应关系可以采用人工设置的方式。

[0084] 上述的病毒清除指令可以包括但不限于:锁定默认主页的指令、修改默认浏览器搜索主页的指令或者下载指定工具软件等。上述指定工具软件可以是诸如安全卫士软件、系统修复小工具、恶意插件清除工具、浏览器保护工具等。

[0085] 上述病毒家族信息对应的病毒清除指令是云端可配置的,可以根据实时捕获的流行病毒行为分析,增加或调整对应病毒清除指令。

[0086] 也就是说,云端服务平台能够有针对性地给予客户端以清除一类病毒的指导意见,避免了客户端只有单纯地删除文件所带来的无法完全清除病毒体的问题。

[0087] 3) 对各机器系统的客户端上报的扫描日志进行联合分析得到更新病毒体行为,利用更新病毒体行为更新云端的行为链脚本库。

[0088] 下面结合具体实施例对客户端和云端服务平台所执行的方法流程进行描述。图 2 为本发明实施例提供的客户端执行的病毒处理方法流程图，如图 2 中所示，该流程主要包括以下步骤：

[0089] 在 201 中，客户端扫描机器系统中的病毒体行为，例如扫描进程、加载模块、驱动、服务、Rootkit、启动项、IE 相关的项目、引导病毒、系统目录、桌面目录、开始菜单、常用软件、脚本、系统组件、登录部分、系统启动项等。

[0090] 在 202 中，客户端将扫描日志上报给云端服务平台。

[0091] 在 203 中客户端利用本地的行为链脚本库对扫描的病毒体行为进行鉴定，如果鉴定出恶意病毒体行为，则执行 204，图 2 中仅示出该种情况，如果未鉴定出恶意病毒体行为，则监听客户端与云端服务平台进行通信的接口。需要说明的是，监听客户端与云端服务平台进行通信的接口并不一定是未鉴定出恶意病毒体行为后才执行的操作，也可以保持持续监听。

[0092] 需要说明的是，上述步骤 202 和 203 可以以任意的顺序先后执行，也可以同时执行。图 2 仅是其中一种执行顺序。

[0093] 由于行为链脚本库中包含的是病毒家族的恶意病毒体行为信息，因此可以将客户端扫描的病毒体行为与行为链脚本库进行匹配，这里的匹配可以是行为特征的匹配，也可以是脚本的匹配等，如果存在一致的行为特征或脚本，则确定鉴定出恶意病毒体行为，确定该恶意病毒体行为对应的病毒家族信息。

[0094] 在 204 中，将恶意病毒体行为对应的病毒家族信息上报给云端服务平台。客户端在上报病毒家族信息时，可以同时上报所在机器系统的信息，例如 GUID(Globally Unique Identifier，全局唯一标识符)，以便云端服务平台能够区分上报信息的机器系统。

[0095] 在 205 中，由于鉴定出了恶意病毒体行为，因此在客户端可以对恶意病毒体行为的关联内容进行清除。上述 204 和 205 可以按照任意的顺序先后执行，也可以同时执行，图 2 仅为其中一种执行顺序。在 204 之后，客户端开始监听客户端与云端服务平台进行通信的接口，一旦监听到云端服务平台下发的病毒清除指令，则执行 206，即接收并执行云端服务平台下发的病毒清除指令。

[0096] 图 3 为本发明实施例提供的云端服务平台执行的病毒处理方法流程图，如图 3 中所示，该流程可以包括以下步骤：

[0097] 在 301 中，云端服务平台接收客户端上报的扫描日志，该扫描日志包含客户端扫描的病毒体行为信息。

[0098] 在 302 中，将扫描日志中的病毒体行为信息与云端的行为链脚本库进行匹配，确定恶意病毒体行为信息对应的病毒家族信息。由于云端的行为链脚本库是综合各机器系统的客户端上报的扫描日志进行分析后得到的，因此在针对一个客户端进行病毒体行为的鉴别时，实际上也是关联分析了其他机器系统的扫描日志。

[0099] 上述步骤 301 和 302 是其中一个执行分支，即接收到扫描日志后的情况，在 302 之后执行步骤 304。还有一个分支，即如果接收到客户端上报的病毒家族信息，即步骤 303，则直接执行步骤 304。

[0100] 在步骤 304 中，根据病毒家族信息与病毒清除指令之间的对应关系，将病毒家族信息对应的病毒清除指令下发给客户端。上述病毒家族信息与病毒清除指令之间的对应关

系是在云端服务平台预先加载的，针对各病毒家族分别设置对应的病毒清除指令以指导客户端进行病毒体的清除。

[0101] 另外，还可能存在这样的情况，假设对于同一客户端，云端服务平台根据客户端上报的扫描日志确定出的病毒家族信息与该客户端上报的病毒家族信息不一致，也就是说，云端服务平台与客户端的鉴定结果不一致时，可以采用云端服务平台的鉴定结果为准，即将云端服务平台确定出的病毒家族信息对应的病毒清除指令下发给客户端。当然，也可以采用其他策略，例如当云端服务平台与客户端的鉴定结果不一致时，可以人为参与鉴定，将人为鉴定出的病毒家族信息对应的病毒清除指令下发给客户端。

[0102] 下面对本发明提供的装置进行详细描述，图 4 为本发明实施例提供的第一种装置结构图，该装置设置于云端服务平台中，如图 4 所示，该装置可以包括 :病毒确定单元 41 和指令下发单元 42，还可以进一步包括联合分析单元 43 和库更新单元 44。

[0103] 其中病毒确定单元 41 负责确定客户端扫描的病毒体行为所对应的病毒家族信息。具体地，该病毒确定单元 41 可以采用以下两种方式中的至少一种确定病毒家族信息，图 4 中以同时采用以下两种方式时的结构为例。

[0104] 第一种方式 :病毒确定单元 41 根据客户端上报的扫描日志在云端服务平台进行病毒鉴定，此时病毒确定单元 41 可以具体包括 :第一接收子单元 401 和匹配子单元 402。

[0105] 其中第一接收子单元 401 负责接收客户端上报的扫描日志，扫描日志包含客户端扫描的病毒体行为信息。匹配子单元 402 将病毒体行为信息与云端的行为链脚本库进行匹配，确定恶意病毒体行为信息对应的病毒家族信息，其中行为链脚本库包含病毒家族的恶意病毒体行为信息。

[0106] 第二种方式 :病毒确定单元 41 直接接收客户端上报的病毒家族信息，即在客户端进行病毒鉴定，此时病毒确定单元 41 具体包括 :第二接收子单元 411 和获取子单元 412。

[0107] 第二接收子单元 411 接收客户端上报的鉴定结果。获取子单元 412 从鉴定结果中获取病毒家族信息，病毒家族信息是客户端将扫描的病毒体行为与客户端本地的行为链脚本库进行匹配后确定的，其中行为链脚本库包含病毒家族的恶意病毒体行为信息。

[0108] 指令下发单元 42，用于根据病毒家族信息与病毒清除指令之间的对应关系，将病毒确定单元 41 确定的病毒家族信息所对应的病毒清除指令下发给客户端，以供客户端执行病毒清除指令进行病毒体的清除。在云端服务平台中维护着病毒家族信息与病毒清除指令之间的对应关系，这些病毒清除指令用于指导客户端进行操作以对相应病毒家族的行为进行清除。这一对应关系可以采用人工设置的方式。

[0109] 上述的病毒清除指令可以包括但不限于 :锁定默认主页的指令、修改默认浏览器搜索主页的指令或者下载指定工具软件等。上述指定工具软件可以是诸如安全卫士软件、系统修复小工具、恶意插件清除工具、浏览器保护工具等。

[0110] 上述病毒家族信息对应的病毒清除指令是云端可配置的，可以根据实时捕获的流行病毒行为分析，增加或调整对应病毒清除指令。

[0111] 另外，有可能存在这样的情况，假设上述确定病毒家族信息的两种方式确定出的病毒家族信息不同，则可以将云端服务平台确定出的病毒家族信息对应的病毒清除指令下发给客户端。当然，也可以采用其他策略，例如当云端服务平台与客户端的鉴定结果不一致时，可以人为参与鉴定，将人为鉴定出的病毒家族信息对应的病毒清除指令下发给客户端。

[0112] 上述的行为链脚本库是由各机器系统中客户端上报的扫描日志进行分析后得到的，也可以结合人工分析和设置的因素。随着病毒的不断更新，会持续出现新的病毒体行为，因此，云端服务平台需要及时对行为链脚本库进行更新。有鉴于此，联合分析单元 43 对客户端上报的扫描日志进行分析得到更新病毒体行为，然后库更新单元 44 利用更新病毒体行为更新云端的行为链脚本库。

[0113] 图 5 为本发明实施例提供的另一种病毒处理装置的结构图，该装置设置于机器系统中的客户端，如图 5 中所示，该装置可以具体包括：日志上报单元 52 和病毒鉴定单元 53 中的至少一个（图 5 中以同时包含这两个单元的情况为例）、行为扫描单元 51 以及指令处理单元 54，还可以进一步包括病毒清除单元 55 和库更新单元 56。

[0114] 其中，行为扫描单元 51 负责扫描病毒体行为信息，即扫描机器系统中恶意病毒体可能的所有行为内容，病毒体行为信息可以是对以下内容中的至少一种进行扫描后得到的行为信息：网络修复、进程、加载模块、驱动、服务、Rootkit、启动项、IE 相关的项目、引导病毒、系统目录、桌面目录、开始菜单、常用软件、脚本、系统组件、登录部分、系统启动项等。

[0115] 日志上报单元 52 负责将扫描日志上报云端服务平台，扫描日志中包含了行为扫描单元 51 扫描的病毒体行为信息，上报给云端服务平台供其进行分析鉴定。

[0116] 病毒鉴定单元 53 利用本地的行为链脚本库，对病毒体行为进行鉴定，如果鉴定出恶意病毒体行为，则将恶意病毒体行为信息对应的病毒家族信息上报给云端服务平台，其中行为链脚本库包含病毒家族的恶意病毒体行为信息。

[0117] 指令处理单元 54 接收并执行云端服务平台下发的病毒清除指令。具体地，病毒清除指令可以包括但不限于以下操作的指令：锁定默认主页、修改默认浏览器搜索主页、下载指定工具软件或清除恶意病毒体行为的关联内容。

[0118] 更进一步地，如果病毒鉴定单元 53 鉴定出恶意病毒体行为，则病毒清除单元 55 清除恶意病毒体行为的关联内容。其中，清除恶意病毒体行为的关联内容可以包括但不限于：停止恶意病毒体的服务，删除恶意病毒体的文件、注册表项或相关活动项，修复浏览器默认主页。

[0119] 客户端本地的行为链脚本库是加载云端服务平台的行为链脚本库后存储于本地得到的，客户端可以周期性地从云端服务平台加载行为链脚本库并对本地的行为链脚本库进行更新。此时，库更新单元 56 加载云端的行为链脚本库，利用云端的行为链脚本库更新本地的行为链脚本库。

[0120] 由以上描述可以看出，本发明提供的方法、装置和系统具备以下优点：

[0121] 1）本发明这种由云端针对病毒家族信息进行病毒清除指令下发的方式，相比较单纯由客户端进行行为分析和删除文件的方式，对病毒的处理更加个性化和精准，提高了机器系统的安全性。

[0122] 2）本发明中云端服务平台针对病毒家族信息下发的病毒清除指令并不局限于清除恶意病毒体行为的关联内容，还可以是诸如锁定默认主页、修改默认浏览器搜索主页、下载指定工具软件等，对病毒的处理更加多样化，有助于彻底清除病毒，加强机器系统的安全性。

[0123] 3）云端服务平台能够联合各机器系统的客户端上报的扫描日志进行行为链脚本库的更新，从而及时地满足互联网式病毒更新快的特征。

[0124] 4) 在云端服务平台中针对病毒家族信息的病毒清除指令能够灵活配置，并可以及时增加或调整，从而满足互联网时代的快速响应要求。

[0125] 在本发明所提供的几个实施例中，应该理解到，所揭露的系统，装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式。

[0126] 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单元来实现本实施例方案的目的。

[0127] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能单元的形式实现。

[0128] 上述以软件功能单元的形式实现的集成的单元，可以存储在一个计算机可读取存储介质中。上述软件功能单元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）或处理器（processor）执行本发明各个实施例所述方法的部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（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以存储程序代码的介质。

[0129] 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。

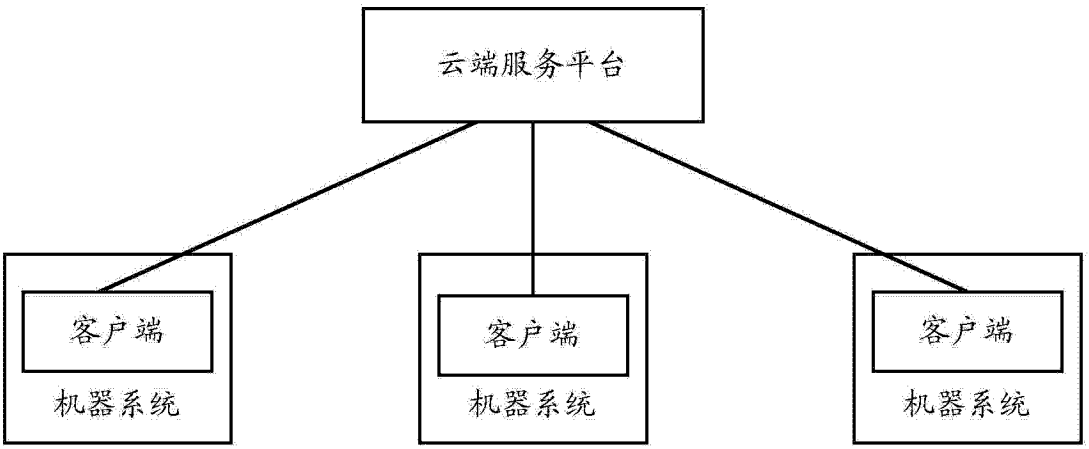



图 1

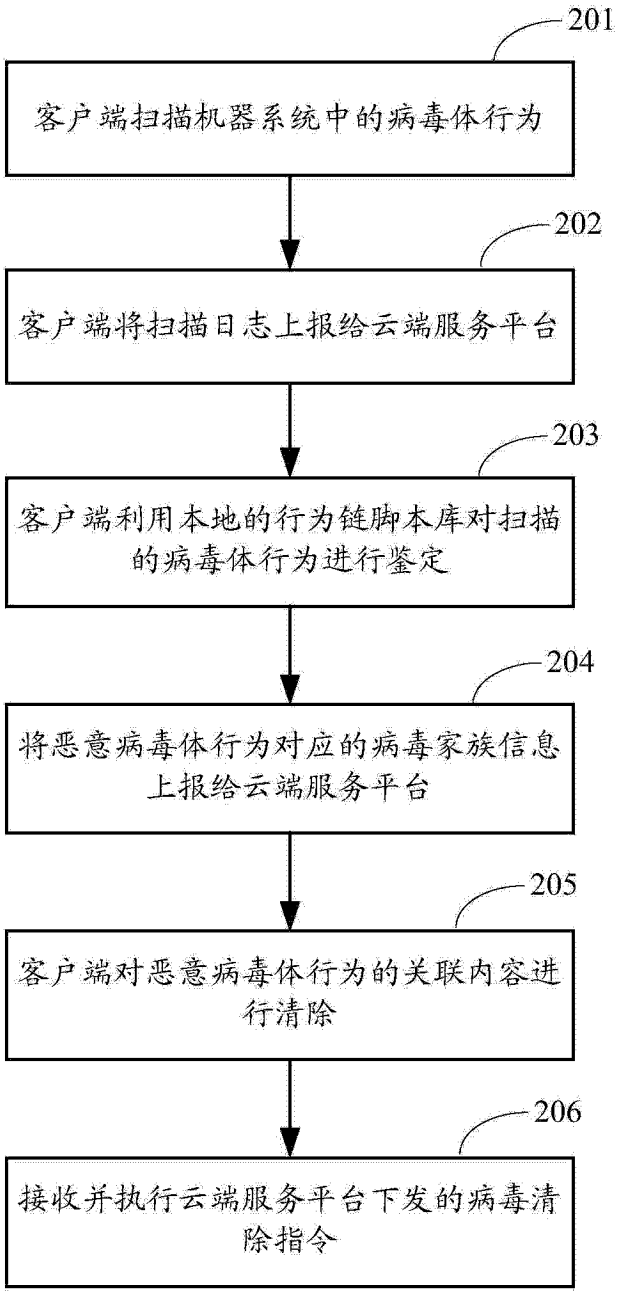

201
客户端扫描机器系统中的病毒体行为
202
客户端将扫描日志上报给云端服务平台
203
客户端利用本地的行为链脚本库对扫描的病毒体行为进行鉴定
204
将恶意病毒体行为对应的病毒家族信息上报给云端服务平台
205
客户端对恶意病毒体行为的关联内容进行清除
206
接收并执行云端服务平台下发的病毒清除指令

图 2

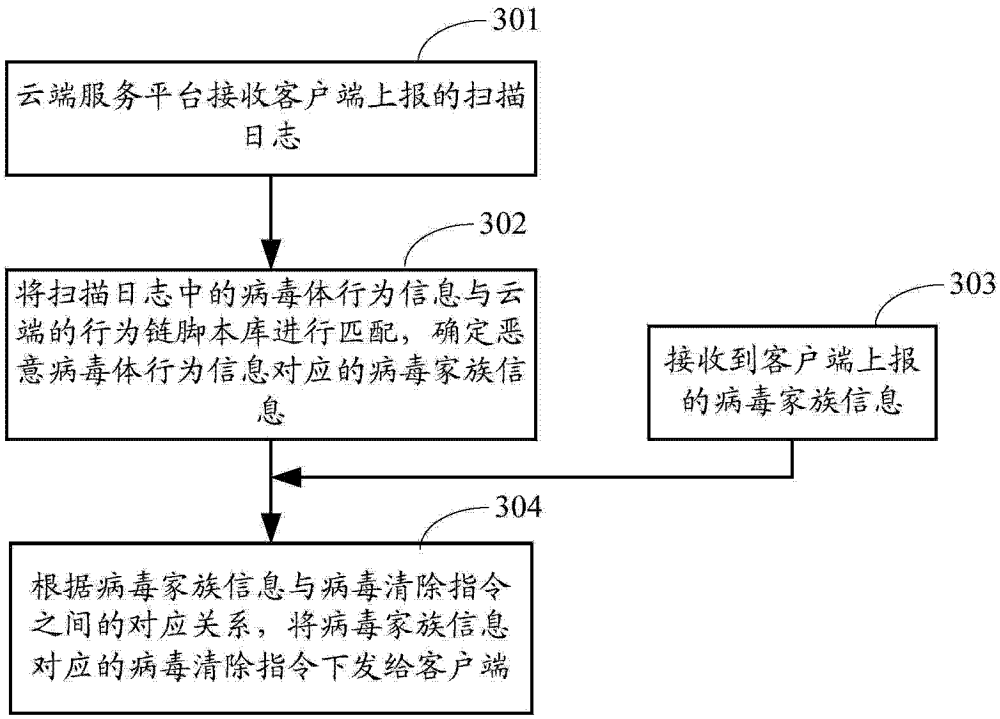

301
云端服务平台接收客户端上报的扫描日志
302
将扫描日志中的病毒体行为信息与云端的行为链脚本库进行匹配，确定恶意病毒体行为信息对应的病毒家族信息
303
接收到客户端上报的病毒家族信息
304
根据病毒家族信息与病毒清除指令之间的对应关系，将病毒家族信息对应的病毒清除指令下发给客户端

图 3

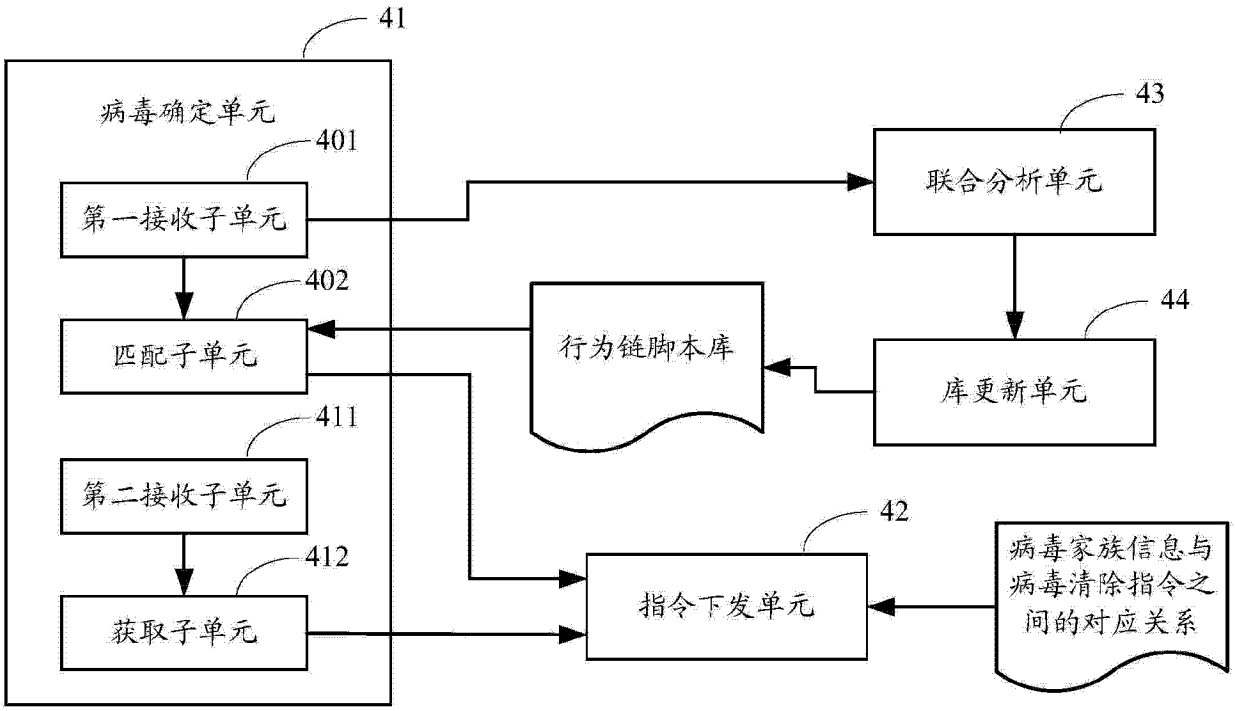

41
病毒确定单元
401
第一接收子单元
402
匹配子单元
411
第二接收子单元
412
获取子单元
43
联合分析单元
44
行为链脚本库
库更新单元
42
指令下发单元
病毒家族信息与病毒清除指令之间的对应关系

图 4

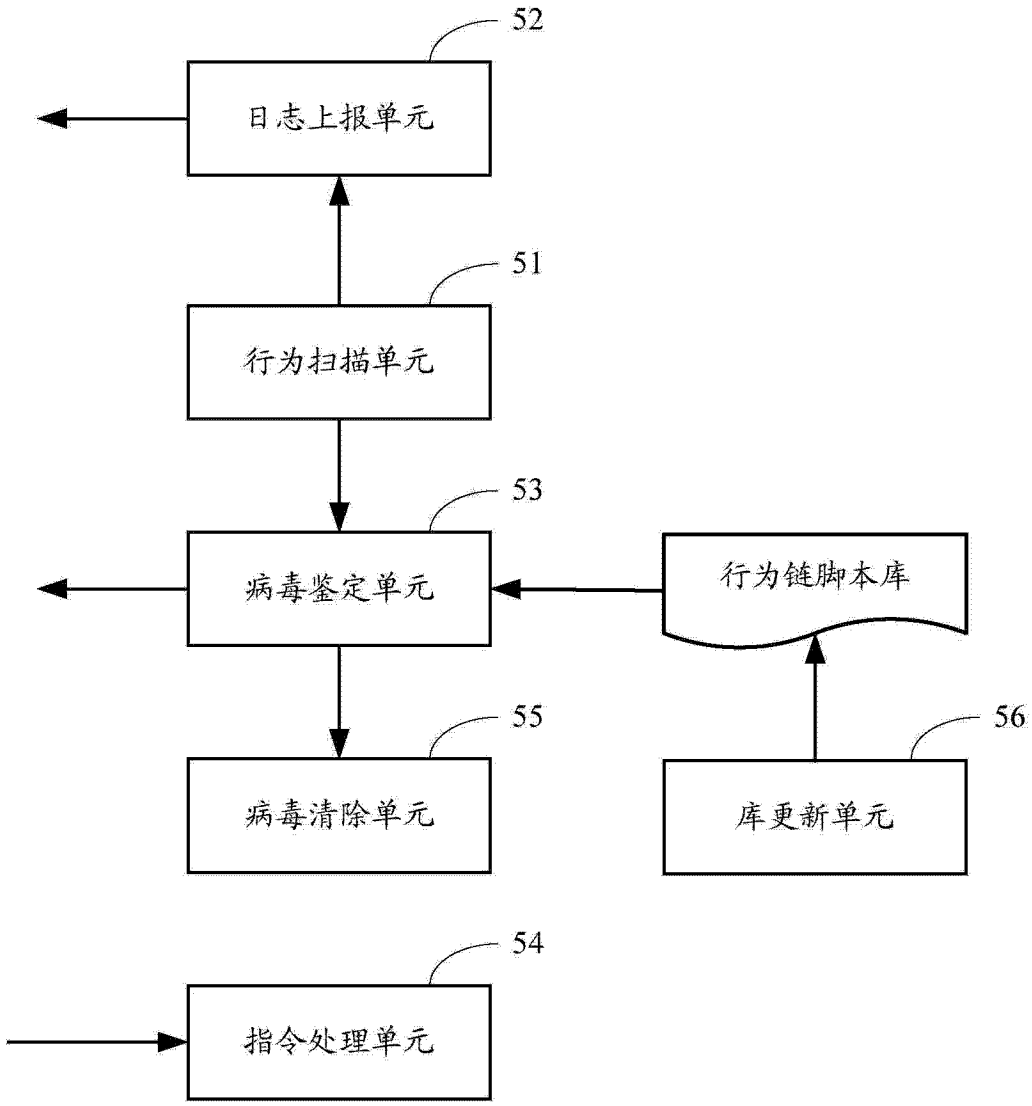

52
日志上报单元
51
行为扫描单元
53
病毒鉴定单元
行为链脚本库
55
病毒清除单元
56
库更新单元
54
指令处理单元

图 5