(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 108537040 B
(45)授权公告日 2023.03.14

(21)申请号 201810324808.3

(22)申请日 2018.04.12

(65)同一申请的已公布的文献号
申请公布号 CN 108537040 A

(43)申请公布日 2018.09.14

(73)专利权人 腾讯科技(深圳)有限公司
地址 518057 广东省深圳市南山区高新区科技中一路腾讯大厦35层

(72)发明人 全永春 饶帅 程虎 廖崇粮

(74)专利代理机构 北京三高永信知识产权代理有限责任公司 11138
专利代理师 刘映东

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

(56)对比文件
CN 102932329 A,2013.02.13
CN 103279706 A,2013.09.04
CN 102663274 A,2012.09.12
US 2018041540 A1,2018.02.08

审查员 贾勇

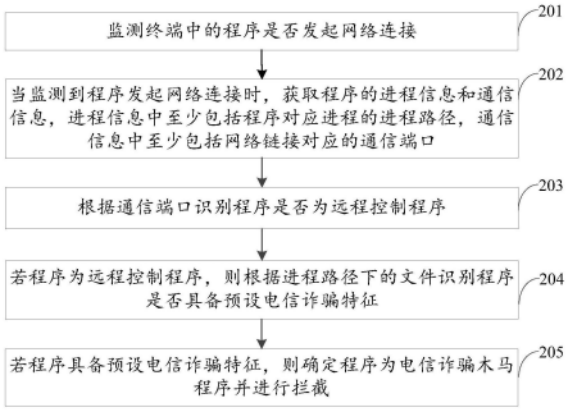
权利要求书3页 说明书14页 附图5页

(54)发明名称

电信诈骗木马程序拦截方法、装置、终端及存储介质

(57)摘要

本申请公开了一种电信诈骗木马程序拦截方法、装置、终端及存储介质，属于网络安全领域。该方法包括：监测终端中的程序是否发起网络连接；当监测到程序发起网络连接时，获取程序的进程信息和通信信息，进程信息中至少包括程序对应进程的进程路径，通信信息中至少包括网络链接对应的通信端口；根据通信端口识别程序是否为远程控制程序；若程序为远程控制程序，则根据进程路径下的文件识别程序是否具备预设电信诈骗特征；若程序具备预设电信诈骗特征，则确定程序为电信诈骗木马程序并进行拦截。本申请实施例基于通信端口和进程文件实现程序拦截，避免因标注不及时造成的拦截率较低的问题，从而提高对新型电信诈骗木马程序的检出和拦截率。



CN 108537040 B

1.一种电信诈骗木马程序拦截方法,其特征在于,所述方法包括:

监测终端中的程序是否发起网络连接;

当监测到程序发起网络连接时,获取所述程序的进程信息和通信信息,所述进程信息中至少包括所述程序对应进程的进程路径,所述通信信息中至少包括所述网络连接对应的通信端口;

根据所述通信端口识别所述程序是否为远程控制程序;

若所述程序为所述远程控制程序,则根据所述进程路径下的文件识别所述程序是否具备预设电信诈骗特征;

若所述程序具备所述预设电信诈骗特征,则确定所述程序为电信诈骗木马程序并进行拦截。

2.根据权利要求1所述的方法,其特征在于,所述根据所述通信端口识别所述程序是否为远程控制程序,包括:

检测所述通信端口是否属于预设通信端口,所述预设通信端口为预设远程控制程序所使用的通信端口;

若所述通信端口属于所述预设通信端口,则确定所述程序为所述远程控制程序。

3.根据权利要求1或2所述的方法,其特征在于,所述根据所述进程路径下的文件识别所述程序是否具备预设电信诈骗特征,包括:

遍历所述进程路径下的文件;

当所述进程路径下包含配置文件时,解析所述配置文件;

若所述配置文件中包含预设电信诈骗关键字,则确定所述程序具备所述预设电信诈骗特征。

4.根据权利要求3所述的方法,其特征在于,所述遍历所述进程路径下的文件之后,还包括:

当所述进程路径下不包含配置文件,且所述进程包含对应的窗口时,提取所述窗口包含的文本内容,所述文本内容为窗口标题和/或窗口文本域内容;

若所述文本内容中包含预设电信诈骗关键字,则确定所述程序具备所述预设电信诈骗特征。

5.根据权利要求1或2所述的方法,其特征在于,所述根据所述进程路径下的文件识别所述程序是否具备预设电信诈骗特征之后,所述方法还包括:

当所述程序为所述电信诈骗木马程序时,获取所述进程路径下的可执行文件,并计算所述可执行文件的消息摘要算法MD5值;

根据所述MD5值识别所述可执行文件是否为合法远程控制文件,其中,当所述可执行文件为所述合法远程控制文件时,表征所述程序由合法远程控制程序修改得到。

6.根据权利要求5所述的方法,其特征在于,所述确定所述程序为电信诈骗木马程序并进行拦截,包括:

若所述程序为所述电信诈骗木马程序,显示提示窗口,所述提示窗口中至少包括拦截控件和取消拦截控件;

当接收到所述拦截控件上的操作信号,且所述可执行文件是所述合法远程控制文件时,拦截所述进程并保留所述进程路径下的文件;

当接收到所述拦截控件上的操作信号，且所述可执行文件不是所述合法远程控制文件时，拦截所述进程并删除所述进程路径下的文件。

7.一种电信诈骗木马程序拦截装置，其特征在于，所述装置包括：

监测模块，用于监测终端中的程序是否发起网络连接；

获取模块，用于当监测到程序发起网络连接时，获取所述程序的进程信息和通信信息，所述进程信息中至少包括所述程序对应进程的进程路径，所述通信信息中至少包括所述网络连接对应的通信端口；

第一识别模块，用于根据所述通信端口识别所述程序是否为远程控制程序；

第二识别模块，用于当所述程序为所述远程控制程序时，根据所述进程路径下的文件识别所述程序是否具备预设电信诈骗特征；

拦截模块，用于当所述程序具备所述预设电信诈骗特征时，确定所述程序为电信诈骗木马程序并进行拦截。

8.根据权利要求7所述的装置，其特征在于，所述第一识别模块，包括：

检测单元，用于检测所述通信端口是否属于预设通信端口，所述预设通信端口为预设远程控制程序所使用的通信端口；

第一确定单元，用于当所述通信端口属于所述预设通信端口时，确定所述程序为所述远程控制程序。

9.根据权利要求7或8所述的装置，其特征在于，所述第二识别模块，包括：

遍历单元，用于遍历所述进程路径下的文件；

解析单元，用于当所述进程路径下包含配置文件时，解析所述配置文件；

第二确定单元，用于当所述配置文件中包含预设电信诈骗关键字时，确定所述程序具备所述预设电信诈骗特征。

10.根据权利要求9所述的装置，其特征在于，所述第二识别模块，还包括：

提取单元，用于当所述进程路径下不包含配置文件，且所述进程包含对应的窗口时，提取所述窗口包含的文本内容，所述文本内容为窗口标题和/或窗口文本域内容；

第三确定单元，用于当所述文本内容中包含预设电信诈骗关键字时，确定所述程序具备所述预设电信诈骗特征。

11.根据权利要求7或8所述的装置，其特征在于，所述装置还包括：

计算模块，用于当所述程序为所述电信诈骗木马程序时，获取所述进程路径下的可执行文件，并计算所述可执行文件的消息摘要算法MD5值；

第三识别模块，用于根据所述MD5值识别所述可执行文件是否为合法远程控制文件，其中，当所述可执行文件为所述合法远程控制文件时，表征所述程序由合法远程控制程序修改得到。

12.根据权利要求11所述的装置，其特征在于，所述拦截模块，包括：

显示单元，用于当所述程序为所述电信诈骗木马程序时，显示提示窗口，所述提示窗口中至少包括拦截控件和取消拦截控件；

第一拦截单元，用于当接收到所述拦截控件上的操作信号，且所述可执行文件是所述合法远程控制文件时，拦截所述进程并保留所述进程路径下的文件；

第二拦截单元，用于当接收到所述拦截控件上的操作信号，且所述可执行文件不是所

述合法远程控制文件时，拦截所述进程并删除所述进程路径下的文件。

13.一种终端，其特征在于，所述终端包括处理器和存储器，所述存储器中存储有至少一条指令、至少一段程序、代码集或指令集，所述至少一条指令、所述至少一段程序、所述代码集或指令集由所述处理器执行以实现如权利要求1至6任一所述的电信诈骗木马程序拦截方法。

14.一种计算机可读存储介质，其特征在于，所述存储介质中存储有至少一条指令、至少一段程序、代码集或指令集，所述至少一条指令、所述至少一段程序、所述代码集或指令集由处理器执行以实现如权利要求1至6任一所述的电信诈骗木马程序拦截方法。

电信诈骗木马程序拦截方法、装置、终端及存储介质

技术领域

[0001] 本申请实施例涉及网络安全技术领域，特别涉及一种电信诈骗木马程序拦截方法、装置、终端及存储介质。

背景技术

[0002] 互联网技术的飞速发展给人们日常生活带来便利的同时，也带来了诸多的安全隐患。比如，不法分子开始利用网络进行电信诈骗。

[0003] 不法分子进行电信诈骗时，首先通过电话、网络或短信等方式编造虚假信息，诱骗受害人进入骗局，然后指示受害人下载并安装电信诈骗木马程序，从而通过电信诈骗木马程序远程控制受害人的终端进行转账操作。为了降低电信诈骗的发生率，越来越多的杀毒应用程序开始具备电信诈骗木马拦截功能。相关技术中，杀毒应用程序基于已经标注的电信诈骗木马程序实现拦截功能，拦截成功率与病毒库中标注的电信诈骗木马程序的数量相关。

[0004] 然而，采用上述方式进行电信诈骗木马程序拦截时，若出现新型的电信诈骗木马程序，杀毒应用程序将无法及时识别并拦截，导致电信诈骗木马的拦截成功率较低。

发明内容

[0005] 本申请实施例提供了一种电信诈骗木马程序拦截方法、装置、终端及存储介质，可以解决基于已标注的电信诈骗木马程序实现拦截功能时，新型的电信诈骗木马程序无法被及时识别并拦截，导致电信诈骗木马拦截成功率较低的问题。所述技术方案如下：

[0006] 第一方面，提供了一种电信诈骗木马程序拦截方法，所述方法包括：

[0007] 监测终端中的程序是否发起网络连接；

[0008] 当监测到程序发起网络连接时，获取所述程序的进程信息和通信信息，所述进程信息中至少包括所述程序对应进程的进程路径，所述通信信息中至少包括所述网络链接对应的通信端口；

[0009] 根据所述通信端口识别所述程序是否为远程控制程序；

[0010] 若所述程序为所述远程控制程序，则根据所述进程路径下的文件识别所述程序是否具备预设电信诈骗特征；

[0011] 若所述程序具备所述预设电信诈骗特征，则确定所述程序为电信诈骗木马程序并进行拦截。

[0012] 第二方面，提供了一种电信诈骗木马程序拦截装置，所述装置包括：

[0013] 监测模块，用于监测终端中的程序是否发起网络连接；

[0014] 获取模块，用于当监测到程序发起网络连接时，获取所述程序的进程信息和通信信息，所述进程信息中至少包括所述程序对应进程的进程路径，所述通信信息中至少包括所述网络链接对应的通信端口；

[0015] 第一识别模块，用于根据所述通信端口识别所述程序是否为远程控制程序；

[0016] 第二识别模块，用于当所述程序为所述远程控制程序时，根据所述进程路径下的文件识别所述程序是否具备预设电信诈骗特征；

[0017] 拦截模块，用于当所述程序具备所述预设电信诈骗特征时，确定所述程序为电信诈骗木马程序并进行拦截。

[0018] 第三方面，提供了一种终端，所述终端包括处理器和存储器，所述存储器中存储有至少一条指令、至少一段程序、代码集或指令集，所述至少一条指令、所述至少一段程序、所述代码集或指令集由所述处理器执行以实现如第一方面所述的电信诈骗木马程序拦截方法。

[0019] 第四方面，提供了一种计算机可读存储介质，所述存储介质中存储有至少一条指令、至少一段程序、代码集或指令集，所述至少一条指令、所述至少一段程序、所述代码集或指令集由所述处理器执行以实现如第一方面所述的电信诈骗木马程序拦截方法。

[0020] 第五方面，提供了一种计算机程序产品，当该计算机程序产品被执行时，其用于执行上述第一方面所述的电信诈骗木马程序拦截方法。

[0021] 本申请实施例提供的技术方案带来的有益效果包括：

[0022] 通过在程序发起网络连接时，获取程序的进程信息和通信信息，并根据通信信息中的通信端口，以及进程信息中进程路径下的文件，识别该程序是否为电信诈骗木马程序，进而对识别出的电信诈骗木马程序的进程进行拦截；基于通信端口和进程文件实现程序拦截，不依赖于已标注的电信诈骗木马程序，能够避免因标注不及时造成的拦截率较低的问题，从而提高对新型电信诈骗木马程序的检出和拦截率。

附图说明

[0023] 为了更清楚地说明本申请实施例中的技术方案，下面将对实施例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申请的一些实施例，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。

[0024] 图1示出了本申请一个实施例提供的电信诈骗木马程序拦截方法所涉及实施环境的示意图；

[0025] 图2示出了本申请一个实施例提供的电信诈骗木马程序拦截方法的流程图；

[0026] 图3示出了本申请一个实施例提供的电信诈骗木马程序拦截方法的流程图；

[0027] 图4是修改配置文件前后远程控制程序的界面示意图；

[0028] 图5是电信诈骗提示界面的界面示意图；

[0029] 图6示出了本申请一个实施例提供的电信诈骗木马程序拦截方法的流程图；

[0030] 图7和图8是图6所示电信诈骗木马程序拦截方法实施过程的界面示意图；

[0031] 图9示出了本申请一个实施例提供的电信诈骗木马程序拦截装置的框图；

[0032] 图10示出了本申请一个示例性实施例提供的终端的结构框图。

具体实施方式

[0033] 为使本申请的目的、技术方案和优点更加清楚，下面将结合附图对本申请实施方式作进一步地详细描述。

[0034] 为了方面理解，下面对本申请实施例中涉及的名词进行解释。

[0035] 远程控制：指通过网络，利用一台终端(比如个人计算机)控制另一台或多台终端执行操作的行为。通常情况下，终端之间通过安装的远程控制程序实现远程控制，常见的远程控制程序包括Teamviewer、LookMyPC和RemoteView等等。

[0036] 消息摘要算法第五版(Message Digest Algorithm 5，MD5)：计算机安全领域使用的一种散列函数，用于将数据(或文件)转化为固定长度的字符串。即使改变原数据中极少的数据，原数据的MD5值和改变后数据的MD5值也将既然不同，因此，MD5常被用于检测数据的一致性。

[0037] 查白：指基于白名单进行检测的过程，本申请实施例中，查白即为检测电信诈骗木马程序的可执行文件是否为白名单中合法远程控制文件的过程。

[0038] 请参考图1，其示出了本申请一个实施例提供的电信诈骗木马程序拦截方法所涉及实施环境的示意图。该实施环境中包括至少终端110和服务器120。

[0039] 终端110是具有木马拦截功能的电子设备，该电子设备可以为智能手机、平板电脑、台式计算机或个人便携式计算机等等，且该木马拦截功能可以通过终端中安装的应用程序来实现，该应用程序可以为病毒查杀应用程序或终端管家类应用程序。

[0040] 终端110与服务器120之间通过有线网络或无线网络相连。

[0041] 服务器120是一台服务器、若干台服务器构成的服务器集群或云计算中心。可选的，本申请实施例中，服务器120是终端110中实现木马拦截功能的应用程序的后台服务器。

[0042] 在一种可能的应用场景下，终端110中的管家类应用程序监测各个程序发起网络链接的行为，并在监测到发起网络链接时，获取程序相关的通信信息以及进程信息，并基于通信信息以及进程信息，在本地识别发起的网络链接是否存在电信诈骗行为。

[0043] 进一步的，当识别出存在电信诈骗行为时，为了进一步确定该程序的风险程度，终端110进一步通过云查的方式与服务器120进行交互，交由服务器120识别该程序的进程文件是否为合法的远程控制文件，并接收服务器120反馈的云查结果。基于云查结果，终端110与用户进行拦截交互，并在接收到确认拦截指令时，对该程序进行拦截。

[0044] 在其他可能的应用场景下，终端110中的管家类应用程序获取到通信信息以及进程信息后，可以直接将上述信息上报至服务器120，由服务器120识别网络链接是否存在电信诈骗行为，并进一步识别该程序的进程文件是否为合法的远程控制文件，进而将识别结果反馈给终端110，以便终端110根据识别结果与用户进行交互并拦截。

[0045] 可选地，上述的无线网络或有线网络使用标准通信技术和/或协议。网络通常为因特网、但也可以是任何网络，包括但不限于局域网(Local Area Network，LAN)、城域网(Metropolitan Area Network，MAN)、广域网(Wide Area Network，WAN)、移动、有线或者无线网络、专用网络或者虚拟专用网络的任何组合)。在一些实施例中，使用包括超文本标记语言(Hyper Text Mark-up Language，HTML)、可扩展标记语言(Extensible Markup Language，XML)等的技术和/或格式来代表通过网络交换的数据。此外还可以使用诸如安全套接字层(Secure Socket Layer，SSL)、传输层安全(Transport Layer Security，TLS)、虚拟专用网络(Virtual Private Network，VPN)、网际协议安全(Internet Protocol Security，IPsec)等常规加密技术来加密所有或者一些链路。在另一些实施例中，还可以使用定制和/或专用数据通信技术取代或者补充上述数据通信技术。

[0046] 为了方便描述，下述各个实施例以电信诈骗木马程序拦截方法应用于终端110为例进行说明。

[0047] 通过对大量电信诈骗木马程序分析发现，大多数电信诈骗木马程序是通过对常用远程控制程序进行伪装后得到。比如，不法分子将常用远程控制程序伪装成政府机关发布的程序，并诱骗用户下载安装此类程序，从而利用此类程序远程控制用户终端进行转账。为了能够识别出此类经过伪装的电信诈骗木马程序，终端基于网络链接的通信端口识别当前程序是否为远程控制程序，并在当前程序是远程控制程序时，进一步基于进程路径下的文件识别远程控制程序是否具备电信诈骗特征。下面采用示意性的实施例进行说明。

[0048] 请参考图2，其示出了本申请一个实施例提供的电信诈骗木马程序拦截方法的流程图。本实施例以该方法应用于终端来举例说明，该方法可以包括以下几个步骤：

[0049] 步骤201，监测终端中的程序是否发起网络连接。

[0050] 在一种可能的实施方式中，终端中的管家类应用程序监测各个程序发起的网络连接。

[0051] 在另一种可能的实施方式中，终端的管家类应用程序中设置有受信任名单和可疑名单，其中，受信任名单中包括经过认证的安全应用程序，而可疑名单中包含存在安全风险且未经过认证的可疑应用程序。终端中的管家类应用程序即监测可疑名单中的可以应用程序是否存在发起网络连接的行为，并在监测到发起网络连接时，执行步骤202；对于受信任名单中的安全应用程序，管家类应用程序则不会对其发起的网络连接进行监测。

[0052] 步骤202，当监测到程序发起网络连接时，获取程序的进程信息和通信信息，进程信息中至少包括程序对应进程的进程路径，通信信息中至少包括网络链接对应的通信端口。

[0053] 可选的，进程信息和通信信息由终端驱动层获取，并上抛至终端应用层进行处理。

[0054] 进程信息是发起网络连接的进程的相关信息，至少包括进程路径，该进程路径下包含程序的各个文件；该进程信息中还可以包括唯一标识当前进程的进程标识(Process IDentity，PID)、进程内存占用量以及进程描述信息等等。

[0055] 通信信息是所发起网络连接的相关信息，至少包括发起网络连接的通信端口，比如，获取到的通信端口为8080。该通信信息中还可以包括通信发起地址、通信目标地址等其他信息。其中，通信发起地址和通信目标地址均采用互联网协议(Internet Protocol，IP)地址。

[0056] 步骤203，根据通信端口识别程序是否为远程控制程序。

[0057] 由于电信诈骗木马程序通常是经过伪装的远程控制程序，而远程控制程序的通信端口较为固定，因此，终端根据通信端口识别该程序是否为远程控制程序。

[0058] 若该程序为远程控制程序，终端则进一步执行下述步骤204；若该程序不是远程控制程序，终端则停止电信诈骗木马程序检测。

[0059] 步骤204，若程序为远程控制程序，则根据进程路径下的文件识别程序是否具备预设电信诈骗特征。

[0060] 由于不法分子对远程控制程序进行伪装时，通常会向远程控制程序中注入电信诈骗元素。比如，一种常见的伪装方式是在远程控制程序中添加公检法(公安局、检察院、法院的简称)机关元素，将其伪装成公检法机关提供的程序。

[0061] 因此，终端进一步基于进程路径下的文件识别该程序是否具备预设电信诈骗特征，其中，该预设电信诈骗特征可以包括预设电信诈骗关键字。

[0062] 若识别出该程序具备预设电信诈骗特征，则将该程序确定为电信诈骗木马程序，并执行步骤205；若该程序不具备预设电信诈骗特征，则确定该程序不是电信诈骗木马程序。

[0063] 步骤205，若程序具备预设电信诈骗特征，则确定程序为电信诈骗木马程序并进行拦截。

[0064] 可选的，对于识别出的电信诈骗木马程序，终端直接对其进行拦截；或者，终端显示相应的提示界面，提示用户该程序存在电信诈骗风险，并基于用户的交互行为对进程进行拦截。

[0065] 可选的，由于不同电信诈骗木马程序的风险等级不同，因此，终端针对电信诈骗木马程序的风险等级，进一步对进程进行风险处理。比如，终端对高风险等级的电信诈骗木马程序进行隔离处理，对低风险等级的电信诈骗木马程序仅进行拦截处理。

[0066] 综上所述，本实施例中，通过在程序发起网络连接时，获取程序的进程信息和通信信息，并根据通信信息中的通信端口，以及进程信息中进程路径下的文件，识别该程序是否为电信诈骗木马程序，进而对识别出的电信诈骗木马程序的进程进行拦截；基于通信端口和进程文件实现程序拦截，不依赖于已标注的电信诈骗木马程序，能够避免因标注不及时造成的拦截率较低的问题，从而提高对新型电信诈骗木马程序的检出和拦截率。

[0067] 请参考图3，其示出了本申请另一个实施例提供的电信诈骗木马程序拦截方法的流程图。本实施例以该方法应用于终端来举例说明，该方法可以包括以下几个步骤：

[0068] 步骤301，监测终端中的程序是否发起网络连接。

[0069] 步骤302，当监测到程序发起网络连接时，获取程序的进程信息和通信信息，进程信息中至少包括程序对应进程的进程路径，通信信息中至少包括网络链接对应的通信端口。

[0070] 上述步骤301至302的实施方式与步骤201至202相似，本实施例在此不再赘述。

[0071] 比如，终端获取到网络链接对应的通信端口为5938，且进程的进程路径为C:\Program Files\A。

[0072] 步骤303，检测通信端口是否属于预设通信端口，预设通信端口为预设远程控制程序所使用的通信端口。

[0073] 由于常用远程控制程序发起网络链接是使用的端口较为固定，因此，在一种可能的实施方式中，终端中存储有包含若干个预设通信端口的通信端口列表，该通信端口列表中的预设通信端口即为远程控制的常用通信端口。

[0074] 可选的，该预设通信端口即为常用远程控制程序所采用的通信端口。比如，该预设通信端口包括Teamviewer、LookMyPC和RemoteView所采用的通信端口。本申请实施例并不对预设通信端口的数量进行限定。

[0075] 可选的，该通信端口列表由服务器下发给各个终端，并每隔预定时间间隔进行更新。

[0076] 在确定当前程序是否为远程控制程序时，终端即检测通信端口是否属于预设通信端口，若属于，则确定当前程序为远程控制程序，并进一步执行下述步骤303，以确定当前程

序是否存在电信诈骗行为;若不属于,则确定当前程序不是远程控制程序,并不再执行电信诈骗行为检测。

[0077] 结合步骤302中的示例,终端中存储的预设通信端口包括3389、5938和1717,由于该进程发起网络链接时的通信端口为5938,因此终端确定当前程序为远程控制程序。

[0078] 步骤304,若通信端口属于预设通信端口,则确定程序为远程控制程序。

[0079] 步骤305,若程序为远程控制程序,则遍历进程路径下的文件。

[0080] 不法分子通常采用修改配置文件的方式对远程控制程序进行伪装,使伪装后的远程控制程序呈现出政府机关或金融行业的特征。

[0081] 示意性的,远程控制程序的原始窗口界面如图4(a)所示,不法分子通过修改远程控制程序的配置文件,向配置文件中增加政府机关相关的文字内容和图片内容,使得修改后远程控制程序的窗口界面(图4(b)所示)中呈现出政府机关的元素,从而诱骗受害人主动告知远程控制ID和密码。

[0082] 因此,为了能够识别出此类通过修改配置文件进行伪装的电信诈骗木马程序,终端根据获取到的进程路径,遍历该进程路径下的各个文件,进而根据进程路径下的文件识别程序是否为电信诈骗木马程序。

[0083] 在一种可能的实施方式中,终端遍历文件时,根据各个文件的文件后缀名确定该进程路径下是否包含配置文件。比如,配置文件的后缀名通常为ini、cfg、xml和config,终端即检测进程路径下是否包含上述后缀名的文件,若包含,则确定包含配置文件,并执行下述步骤306至309;若不包含,则确定不包含配置文件,并执行下述步骤310至313。

[0084] 步骤306,当进程路径下包含配置文件时,解析配置文件。

[0085] 当进程路径下包含配置文件时,终端即根据配置文件的后缀名确定配置文件的文件格式,从而采用相应的方式解析该配置文件。

[0086] 步骤307,检测配置文件中是否包含预设电信诈骗关键字。

[0087] 通过修改配置文件的方式伪装远程控制程序时,修改后的配置文件中通常会包含电信诈骗相关的词汇,因此,在一种可能的实施方式中,终端中内置电信诈骗关键字库,该关键字库中即包含预设电信诈骗关键字,预设电信诈骗关键字可以是与政府机关、金融行业、保险行业、学校相关的词汇。

[0088] 可选的,该关键词库中的预设电信诈骗关键词由服务器预先下发,且为了保证拦截准确率,终端每隔预定时间间隔从服务器处获取更新后的关键字库。

[0089] 进一步的,终端检测配置文件中是否包含预设电信诈骗关键字,若包含,则确定该程序具备预设电信诈骗特征,并执行下述步骤308,若不包含,则确定该程序不具备预设电信诈骗特征,并执行下述步骤309。

[0090] 示意性的,如图4所示,终端检测到进程路径下的配置文件中包含预设诈骗关键字“公安局”,从而确定该程序具备电信诈骗特征。

[0091] 步骤308,若配置文件中包含预设电信诈骗关键字,则确定程序具备预设电信诈骗特征。

[0092] 当发起网络链接的程序为远程控制程序,且该远程控制程序具备电信诈骗特征时,终端即确定该程序为电信诈骗木马程序,并进一步通过步骤314对该程序的进程进行拦截。

[0093] 步骤309,若配置文件中不包含预设电信诈骗关键字,则确定程序不具备电信诈骗特征。

[0094] 当发起网络链接的程序为远程控制程序,但该远程控制程序不具备电信诈骗特征时,终端确定该程序不是电信诈骗木马程序,且不会对该进程进行拦截。

[0095] 可选的,对于识别为非电信诈骗木马程序的远程控制程序,终端显示相应的警示界面,警示用户避免让陌生人远程控制自身终端。

[0096] 步骤310,当进程路径下不包含配置文件,且进程包含对应的窗口时,提取窗口包含的文本内容,文本内容为窗口标题和/或窗口文本域内容。

[0097] 除了修改配置文件这一伪装方式外,不法分子还可能通过直接修改窗口属性的方式对远程控制程序进行伪装。因此,当进程路径下不包含配置文件时,终端进一步检测进程是否包含对应的窗口,并在包含对应的窗口时,提取窗口包含的文本内容,进而基于文本内容确定程序是否具有电信诈骗行为。

[0098] 其中,终端提取到的文本内容为进程对应窗口的窗口标题和/或窗口文本域内容。相应的,终端通过GetWindowText()方法提取窗口的窗口标题,通过getElementById()方法提取窗口文本域内容。本申请实施例并不对获取窗口中文本内容的方式进行限定。

[0099] 示意性的,终端通过GetWindowText()方法从图4(b)所示的窗口中提取到窗口标题“xx市公安局”。

[0100] 步骤311,检测文本内容中是否包含预设电信诈骗关键字。

[0101] 进一步的,终端检测文本内容中是否包含预设电信诈骗关键字,若包含,则确定该程序存在电信诈骗行为,并执行下述步骤310,若不包含,则确定该程序不存在电信诈骗行为,并执行下述步骤311。

[0102] 其中,检测预设电信诈骗关键字的过程与上述步骤305相似,本实施例在此不再赘述。

[0103] 步骤312,若文本内容中包含预设电信诈骗关键字,则确定程序具备预设电信诈骗特征。

[0104] 当发起网络链接的程序为远程控制程序,且该远程控制程序的窗口中包含电信诈骗关键字时,终端即确定该程序为电信诈骗木马程序,并进一步通过步骤314对该程序的进程进行拦截。

[0105] 步骤313,若文本内容中不包含预设电信诈骗关键字,则确定程序不具备预设电信诈骗特征。

[0106] 当发起网络链接的程序为远程控制程序,但该远程控制程序的窗口中不包含电信诈骗关键字时,终端确定该程序不是电信诈骗木马程序,并进一步为进程建立网络链接,而不会对该进程进行拦截。

[0107] 步骤314,若程序具备预设电信诈骗特征,则确定程序为电信诈骗木马程序并进行拦截。

[0108] 当发起网络连接的程序为电信诈骗木马程序时,为了避免不法分子进一步控制终端,终端根据获取到的进程路径,对电信诈骗木马程序的进程进行拦截。拦截后,终端电信诈骗木马程序将无法建立网络连接,不法分子将无法进行远程控制。

[0109] 在一种可能的实施方式中,当程序为电信诈骗木马程序时,终端显示相应的提示

界面，该提示界面中包含拦截控件和取消拦截控件，其中，拦截控件的显示尺寸大于取消拦截控件的显示尺寸。

[0110] 当用户点击拦截控件时，终端即对该程序的进程进行拦截；当用户点击取消拦截控件时，终端则不会对进程进行拦截，即程序能够继续建立网络链接。

[0111] 可选的，该提示界面中还包括获取到的程序名称、目标通信地址、电信诈骗木马程序风险描述以及电信诈骗揭秘等内容。

[0112] 示意性的，如图5所示，提示界面中51中包含程序名称511、风险描述信息512、目标通信地址513、拦截控件514、取消拦截控件515和电信诈骗揭秘控件516。当用户点击拦截控件514时，终端即对程序进程进行拦截；当用户点击取消拦截控件515时，终端则不会拦截进程；当用户点击电信诈骗揭秘控件516时，终端即显示揭秘电信诈骗的预设文字内容。

[0113] 本实施例中，终端根据网络链接对应的通信端口，能够识别当前程序是否为远程控制程序，并能够进一步根据进程路径下的配置文件识别当前程序是否存在电信诈骗行为，从而有效拦截由远程控制程序伪装成的电信诈骗木马程序，进而提高拦截的成功率。

[0114] 另外，当进程路径下不包含配置文件时，终端还能够提取进程窗口中包含的文字内容，并根据文字内容识别当前程序是否存在电信诈骗行为，进一步提高了电信诈骗木马程序的识别率。

[0115] 当电信诈骗木马程序是基于常用远程控制程序修改得到时，此类电信诈骗木马程序通常仅具备远程控制功能，因此其风险等级较低；当电信诈骗木马程序是不法分子自主开发的远程控制程序时，此类电信诈骗木马程序可能还存在其他安全风险，因此其风险等级较高。可选的，当确定程序为电信诈骗木马程序后，终端进一步对进程路径下的可执行文件进行查白，并基于查白结果确定电信诈骗木马程序的风险等级，从而根据风险等级对进程进行相应处理。在图3的基础上，如图6所示，上述步骤308和312之后还包括步骤315和316。

[0116] 步骤315，当程序为电信诈骗木马程序时，获取进程路径下的可执行文件，并计算可执行文件的MD5值。

[0117] 可选的，该可执行文件为进程路径下的exe文件。相应的，终端即通过MD5算法计算进程路径下exe文件的MD5值。

[0118] 在其他可能的实施方式中，终端还可以通过其他算法将可执行文件转化为唯一字符串，本申请实施例仅以计算MD5值为例进行示意性说明，并不对申请构成限定。

[0119] 步骤316，根据MD5值识别可执行文件是否为合法远程控制文件。

[0120] 在一种可能的实施方式中，服务器中构建有合法MD5值数据库，该数据库中包含各种合法远程控制程序对应可执行文件的MD5值。终端计算得到可执行文件的MD5值后，将该MD5值上传至服务器，服务器即检测该MD5值是否属于合法MD5值数据库，并将检测结果反馈给终端。若属于，则确定可执行文件为合法远程控制文件；若不属于，则确定可执行文件为非法远程控制文件。其中，当可执行文件为合法远程控制文件时，表征该程序由合法远程控制程序修改得到。

[0121] 在其他可能的实施方式中，合法MD5值数据库可以存储在终端本地，终端即在本地完成合法远程控制文件识别过程。

[0122] 可选的，当可执行文件为合法远程控制文件时，终端将电信诈骗木马程序的风险

等级设置为低风险级，当可执行文件为非法远程控制文件时，终端将电信诈骗木马程序的风险等级设置为高风险级。

[0123] 进一步的，针对不同风险等级的电信诈骗木马程序，终端采用不同的拦截处理方式。如图6所示，图3中的步骤314可以包括步骤314A至314C。

[0124] 步骤314A，若程序为电信诈骗木马程序，显示提示窗口，提示窗口中至少包括拦截控件和取消拦截控件。

[0125] 当用户点击拦截控件时，终端即对该程序的进程进行拦截；当用户点击取消拦截控件时，终端则不会对进程进行拦截，即程序能够继续建立网络链接。

[0126] 可选的，该提示界面中还包括获取到的程序名称、目标通信地址、电信诈骗木马程序风险描述以及电信诈骗揭秘等内容。

[0127] 步骤314B，当接收到拦截控件上的操作信号，且可执行文件是合法远程控制文件时，拦截进程并保留进程路径下的文件。

[0128] 当接收到拦截控件上的操作信号，且可执行文件是合法远程控制文件时(即电信诈骗木马程序的风险等级为低风险级)，终端仅对进程进行拦截，并保留进程路径下的文件。

[0129] 可选的，终端的信任管理界面中包含被阻止网络链接的进程(即被拦截的进程)，用户在信任管理界面中可以将该进程设置为受信任，从而解除对其的拦截。

[0130] 示意性的，如图7所示，信任管理界面71中显示有被阻止网络链接的进程A，当用户通过操作控件711将进程A设置为受信任后，进程A即可建立网络链接。

[0131] 步骤314C，当接收到拦截控件上的操作信号，且可执行文件不是合法远程控制文件时，拦截进程并删除进程路径下的文件。

[0132] 当接收到拦截控件上的操作信号，且可执行文件不是合法远程控制文件时(即电信诈骗木马程序的风险等级为高风险级)，终端对进程进行拦截的同时，删除该进程路径下的文件，即将电信诈骗木马程序清除。

[0133] 可选的，终端的隔离管理界面中包含被删除的文件，用户在隔离管理界面中可以选择恢复被删除的文件。

[0134] 示意性的，如图8所示，隔离管理界面81中显示有被删除的进程文件“进程A.exe”，当用户通过恢复控件811恢复该进程文件。

[0135] 本实施例中，当确定程序为电信诈骗木马程序后，终端进一步对进程路径下的可执行文件进行查白，并基于查白结果确定电信诈骗木马程序的风险等级，对低风险等级的电信诈骗木马程序仅进行拦截，对高险等级的电信诈骗木马程序进行拦截并删除，从而避免终端内高风险电信诈骗木马程序带来的安全隐患。

[0136] 下述为本发明装置实施例，可以用于执行本发明方法实施例。对于本发明装置实施例中未披露的细节，请参照本发明方法实施例。

[0137] 请参考图9，其示出了本申请一个实施例提供的电信诈骗木马程序拦截装置的框图。该装置可以由硬件实现，也可以由硬件执行相应的软件实现。该装置可以包括：

[0138] 监测模块910，用于监测终端中的程序是否发起网络连接；

[0139] 获取模块920，用于当监测到程序发起网络连接时，获取所述程序的进程信息和通信信息，所述进程信息中至少包括所述程序对应进程的进程路径，所述通信信息中至少包

括所述网络链接对应的通信端口；

[0140] 第一识别模块930，用于根据所述通信端口识别所述程序是否为远程控制程序；

[0141] 第二识别模块940，用于当所述程序为所述远程控制程序时，根据所述进程路径下的文件识别所述程序是否具备预设电信诈骗特征；

[0142] 拦截模块950，用于当所述程序具备所述预设电信诈骗特征时，确定所述程序为电信诈骗木马程序并进行拦截。

[0143] 可选的，所述第一识别模块930，包括：

[0144] 检测单元，用于检测所述通信端口是否属于预设通信端口，所述预设通信端口为预设远程控制程序所使用的通信端口；

[0145] 第一确定单元，用于当所述通信端口属于所述预设通信端口时，确定所述程序为所述远程控制程序。

[0146] 可选的，所述第二识别模块940，包括：

[0147] 遍历单元，用于遍历所述进程路径下的文件；

[0148] 解析单元，用于当所述进程路径下包含配置文件时，解析所述配置文件；

[0149] 第二确定单元，用于当所述配置文件中包含预设电信诈骗关键字时，确定所述程序具备所述预设电信诈骗特征。

[0150] 可选的，所述第二识别模块940，还包括：

[0151] 提取单元，用于当所述进程路径下不包含配置文件，且所述进程包含对应的窗口时，提取所述窗口包含的文本内容，所述文本内容为窗口标题和/或窗口文本域内容；

[0152] 第三确定单元，用于当所述文本内容中包含预设电信诈骗关键字时，确定所述程序具备所述预设电信诈骗特征。

[0153] 可选的，所述装置还包括：

[0154] 计算模块，用于当所述程序为所述电信诈骗木马程序时，获取所述进程路径下的可执行文件，并计算所述可执行文件的消息摘要算法MD5值；

[0155] 第三识别模块，用于根据所述MD5值识别所述可执行文件是否为合法远程控制文件，其中，当所述可执行文件为所述合法远程控制文件时，表征所述程序由合法远程控制程序修改得到。

[0156] 可选的，所述拦截模块950，包括：

[0157] 显示单元，用于当所述程序为所述电信诈骗木马程序时，显示提示窗口，所述提示窗口中至少包括拦截控件和取消拦截控件；

[0158] 第一拦截单元，用于当接收到所述拦截控件上的操作信号，且所述可执行文件是所述合法远程控制文件时，拦截所述进程并保留所述进程路径下的文件；

[0159] 第二拦截单元，用于当接收到所述拦截控件上的操作信号，且所述可执行文件不是所述合法远程控制文件时，拦截所述进程并删除所述进程路径下的文件。

[0160] 综上所述，本实施例中，通过在程序发起网络连接时，获取程序的进程信息和通信信息，并根据通信信息中的通信端口，以及进程信息中进程路径下的文件，识别该程序是否为电信诈骗木马程序，进而对识别出的电信诈骗木马程序的进程进行拦截；基于通信端口和进程文件实现程序拦截，不依赖于已标注的电信诈骗木马程序，能够避免因标注不及时造成的拦截率较低的问题，从而提高对新型电信诈骗木马程序的检出和拦截率。

[0161] 需要说明的是，上述实施例提供的装置在实现其功能时，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将设备的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。另外，上述实施例提供的装置与方法实施例属于同一构思，其具体实现过程详见方法实施例，这里不再赘述。

[0162] 图10示出了本申请一个示例性实施例提供的终端1000的结构框图。该终端1000可以是便携式移动终端，比如：智能手机、平板电脑、MP3播放器(Moving Picture Experts Group Audio Layer III，动态影像专家压缩标准音频层面3)、MP4(Moving Picture Experts Group Audio Layer IV，动态影像专家压缩标准音频层面4)播放器。终端1000还可能被称为用户设备、便携式终端等其他名称。

[0163] 通常，终端1000包括有：处理器1001和存储器1002。

[0164] 处理器1001可以包括一个或多个处理核心，比如4核心处理器、8核心处理器等。处理器1001可以采用DSP(Digital Signal Processing，数字信号处理)、FPGA(Field－Programmable Gate Array，现场可编程门阵列)、PLA(Programmable Logic Array，可编程逻辑阵列)中的至少一种硬件形式来实现。处理器1001也可以包括主处理器和协处理器，主处理器是用于对在唤醒状态下的数据进行处理的处理器，也称CPU(Central Processing Unit，中央处理器)；协处理器是用于对在待机状态下的数据进行处理的低功耗处理器。在一些实施例中，处理器1001可以在集成有GPU(Graphics Processing Unit，图像处理器)，GPU用于负责显示屏所需要显示的内容的渲染和绘制。一些实施例中，处理器1001还可以包括AI(Artificial Intelligence，人工智能)处理器，该AI处理器用于处理有关机器学习的计算操作。

[0165] 存储器1002可以包括一个或多个计算机可读存储介质，该计算机可读存储介质可以是有形的和非暂态的。存储器1002还可包括高速随机存取存储器，以及非易失性存储器，比如一个或多个磁盘存储设备、闪存存储设备。在一些实施例中，存储器1002中的非暂态的计算机可读存储介质用于存储至少一个指令，该至少一个指令用于被处理器1001所执行以实现本申请中提供的视频编码方法。

[0166] 在一些实施例中，终端1000还可选包括有：外围设备接口1003和至少一个外围设备。具体地，外围设备包括：射频电路1004、触摸显示屏1005、摄像头1006、音频电路1007、定位组件1008和电源1009中的至少一种。

[0167] 外围设备接口1003可被用于将I/O(Input/Output，输入/输出)相关的至少一个外围设备连接到处理器1001和存储器1002。在一些实施例中，处理器1001、存储器1002和外围设备接口1003被集成在同一芯片或电路板上；在一些其他实施例中，处理器1001、存储器1002和外围设备接口1003中的任意一个或两个可以在单独的芯片或电路板上实现，本实施例对此不加以限定。

[0168] 射频电路1004用于接收和发射RF(Radio Frequency，射频)信号，也称电磁信号。射频电路1004通过电磁信号与通信网络以及其他通信设备进行通信。射频电路1004将电信号转换为电磁信号进行发送，或者，将接收到的电磁信号转换为电信号。可选地，射频电路1004包括：天线系统、RF收发器、一个或多个放大器、调谐器、振荡器、数字信号处理器、编解码芯片组、用户身份模块卡等等。射频电路1004可以通过至少一种无线通信协议来与其它

终端进行通信。该无线通信协议包括但不限于:万维网、城域网、内联网、各代移动通信网络(2G、3G、4G及5G)、无线局域网和/或WiFi(Wireless Fidelity,无线保真)网络。在一些实施例中,射频电路1004还可以包括NFC(Near Field Communication,近距离无线通信)有关的电路,本申请对此不加以限定。

[0169] 触摸显示屏1005用于显示UI(User Interface,用户界面)。该UI可以包括图形、文本、图标、视频及其它们的任意组合。触摸显示屏1005还具有采集在触摸显示屏1005的表面或表面上方的触摸信号的能力。该触摸信号可以作为控制信号输入至处理器1001进行处理。触摸显示屏1005用于提供虚拟按钮和/或虚拟键盘,也称软按钮和/或软键盘。在一些实施例中,触摸显示屏1005可以为一个,设置终端1000的前面板;在另一些实施例中,触摸显示屏1005可以为至少两个,分别设置在终端1000的不同表面或呈折叠设计;在再一些实施例中,触摸显示屏1005可以是柔性显示屏,设置在终端1000的弯曲表面上或折叠面上。甚至,触摸显示屏1005还可以设置成非矩形的不规则图形,也即异形屏。触摸显示屏1005可以采用LCD(Liquid Crystal Display,液晶显示器)、OLED(Organic Light-Emitting Diode,有机发光二极管)等材质制备。

[0170] 摄像头组件1006用于采集图像或视频。可选地,摄像头组件1006包括前置摄像头和后置摄像头。通常,前置摄像头用于实现视频通话或自拍,后置摄像头用于实现照片或视频的拍摄。在一些实施例中,后置摄像头为至少两个,分别为主摄像头、景深摄像头、广角摄像头中的任意一种,以实现主摄像头和景深摄像头融合实现背景虚化功能,主摄像头和广角摄像头融合实现全景拍摄以及VR(Virtual Reality,虚拟现实)拍摄功能。在一些实施例中,摄像头组件1006还可以包括闪光灯。闪光灯可以是单色温闪光灯,也可以是双色温闪光灯。双色温闪光灯是指暖光闪光灯和冷光闪光灯的组合,可以用于不同色温下的光线补偿。

[0171] 音频电路1007用于提供用户和终端1000之间的音频接口。音频电路1007可以包括麦克风和扬声器。麦克风用于采集用户及环境的声波,并将声波转换为电信号输入至处理器1001进行处理,或者输入至射频电路1004以实现语音通信。出于立体声采集或降噪的目的,麦克风可以为多个,分别设置在终端1000的不同部位。麦克风还可以是阵列麦克风或全向采集型麦克风。扬声器则用于将来自处理器1001或射频电路1004的电信号转换为声波。扬声器可以是传统的薄膜扬声器,也可以是压电陶瓷扬声器。当扬声器是压电陶瓷扬声器时,不仅可以将电信号转换为人类可听见的声波,也可以将电信号转换为人类听不见的声波以进行测距等用途。在一些实施例中,音频电路1007还可以包括耳机插孔。

[0172] 定位组件1008用于定位终端1000的当前地理位置,以实现导航或LBS(Location Based Service,基于位置的服务)。定位组件1008可以是基于美国的GPS(Global Positioning System,全球定位系统)、中国的北斗系统或俄罗斯的伽利略系统的定位组件。

[0173] 电源1009用于为终端1000中的各个组件进行供电。电源1009可以是交流电、直流电、一次性电池或可充电电池。当电源1009包括可充电电池时,该可充电电池可以是有线充电电池或无线充电电池。有线充电电池是通过有线线路充电的电池,无线充电电池是通过无线线圈充电的电池。该可充电电池还可以用于支持快充技术。

[0174] 在一些实施例中,终端1000还包括有一个或多个传感器1010。该一个或多个传感器1010包括但不限于:加速度传感器1011、陀螺仪传感器1012、压力传感器1013、指纹传感

器1014、光学传感器1015以及接近传感器1016。

[0175] 加速度传感器1011可以检测以终端1000建立的坐标系的三个坐标轴上的加速度大小。比如，加速度传感器1011可以用于检测重力加速度在三个坐标轴上的分量。处理器1001可以根据加速度传感器1011采集的重力加速度信号，控制触摸显示屏1005以横向视图或纵向视图进行用户界面的显示。加速度传感器1011还可以用于游戏或者用户的运动数据的采集。

[0176] 陀螺仪传感器1012可以检测终端1000的机体方向及转动角度，陀螺仪传感器1012可以与加速度传感器1011协同采集用户对终端1000的3D动作。处理器1001根据陀螺仪传感器1012采集的数据，可以实现如下功能：动作感应(比如根据用户的倾斜操作来改变UI)、拍摄时的图像稳定、游戏控制以及惯性导航。

[0177] 压力传感器1013可以设置在终端1000的侧边框和/或触摸显示屏1005的下层。当压力传感器1013设置在终端1000的侧边框时，可以检测用户对终端1000的握持信号，根据该握持信号进行左右手识别或快捷操作。当压力传感器1013设置在触摸显示屏1005的下层时，可以根据用户对触摸显示屏1005的压力操作，实现对UI界面上的可操作性控件进行控制。可操作性控件包括按钮控件、滚动条控件、图标控件、菜单控件中的至少一种。

[0178] 指纹传感器1014用于采集用户的指纹，以根据采集到的指纹识别用户的身份。在识别出用户的身份为可信身份时，由处理器1001授权该用户执行相关的敏感操作，该敏感操作包括解锁屏幕、查看加密信息、下载软件、支付及更改设置等。指纹传感器1014可以被设置终端1000的正面、背面或侧面。当终端1000上设置有物理按键或厂商Logo时，指纹传感器1014可以与物理按键或厂商Logo集成在一起。

[0179] 光学传感器1015用于采集环境光强度。在一个实施例中，处理器1001可以根据光学传感器1015采集的环境光强度，控制触摸显示屏1005的显示亮度。具体地，当环境光强度较高时，调高触摸显示屏1005的显示亮度；当环境光强度较低时，调低触摸显示屏1005的显示亮度。在另一个实施例中，处理器1001还可以根据光学传感器1015采集的环境光强度，动态调整摄像头组件1006的拍摄参数。

[0180] 接近传感器1016，也称距离传感器，通常设置在终端1000的正面。接近传感器1016用于采集用户与终端1000的正面之间的距离。在一个实施例中，当接近传感器1016检测到用户与终端1000的正面之间的距离逐渐变小时，由处理器1001控制触摸显示屏1005从亮屏状态切换为息屏状态；当接近传感器1016检测到用户与终端1000的正面之间的距离逐渐变大时，由处理器1001控制触摸显示屏1005从息屏状态切换为亮屏状态。

[0181] 本领域技术人员可以理解，图10中示出的结构并不构成对终端1000的限定，可以包括比图示更多或更少的组件，或者组合某些组件，或者采用不同的组件布置。

[0182] 本申请实施例还提供一种计算机可读存储介质，该存储介质中存储有至少一条指令、至少一段程序、代码集或指令集，所述至少一条指令、所述至少一段程序、所述代码集或指令集由所述处理器加载并执行以实现如上述各个实施例提供的电信诈骗木马程序拦截方法。

[0183] 可选地，该计算机可读存储介质可以包括：只读存储器(ROM,Read Only Memory)、随机存取记忆体(RAM,Random Access Memory)、固态硬盘(SSD,Solid State Drives)或光盘等。其中，随机存取记忆体可以包括电阻式随机存取记忆体(ReRAM,Resistance Random

Access Memory)和动态随机存取存储器(DRAM,Dynamic Random Access Memory)。上述本申请实施例序号仅仅为了描述,不代表实施例的优劣。

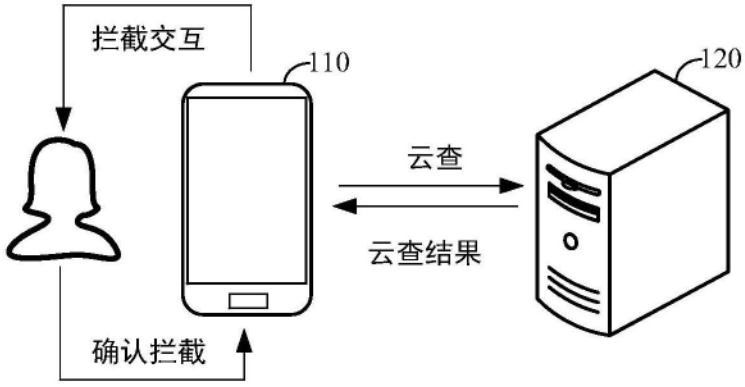

拦截交互
110
120
云查
云查结果
确认拦截

图1

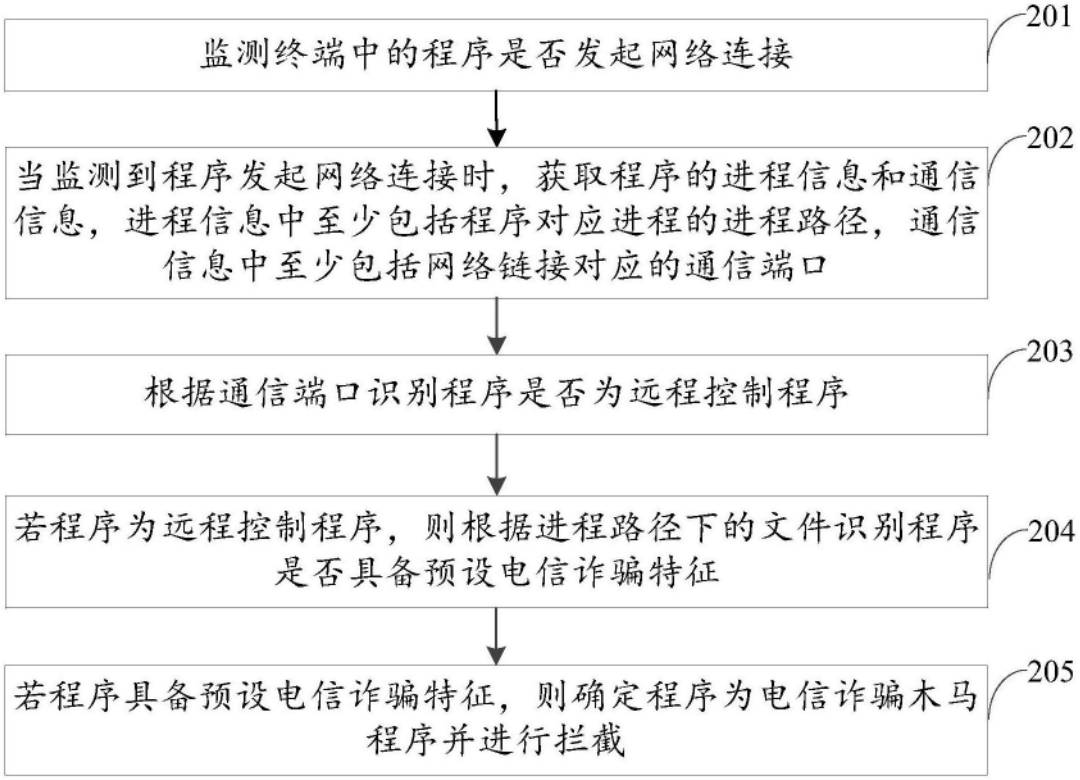

监测终端中的程序是否发起网络连接
201
当监测到程序发起网络连接时，获取程序的进程信息和通信信息，进程信息中至少包括程序对应进程的进程路径，通信信息中至少包括网络链接对应的通信端口
202
根据通信端口识别程序是否为远程控制程序
203
若程序为远程控制程序，则根据进程路径下的文件识别程序是否具备预设电信诈骗特征
204
若程序具备预设电信诈骗特征，则确定程序为电信诈骗木马程序并进行拦截
205

图2

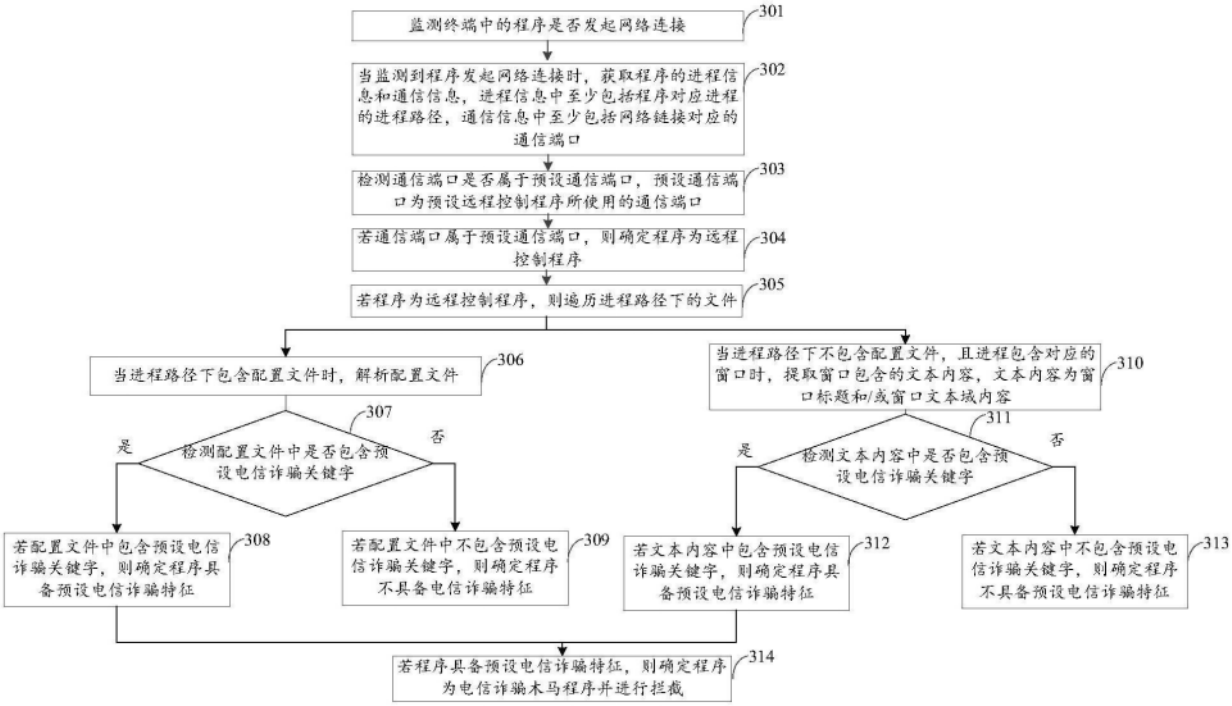

监测终端中的程序是否发起网络连接
301
当监测到程序发起网络连接时，获取程序的进程信息和通信信息，进程信息中至少包括程序对应进程的进程路径，通信信息中至少包括网络链接对应的通信端口
302
检测通信端口是否属于预设通信端口，预设通信端口为预设远程控制程序所使用的通信端口
303
若通信端口属于预设通信端口，则确定程序为远程控制程序
304
若程序为远程控制程序，则遍历进程路径下的文件
305
当进程路径下包含配置文件时，解析配置文件
306
检测配置文件中是否包含预设电信诈骗关键字
307
是
否
若配置文件中包含预设电信诈骗关键字，则确定程序具备预设电信诈骗特征
308
若配置文件中不包含预设电信诈骗关键字，则确定程序不具备电信诈骗特征
309
当进程路径下不包含配置文件，且进程包含对应的窗口时，提取窗口包含的文本内容，文本内容为窗口标题和/或窗口文本域内容
310
检测文本内容中是否包含预设电信诈骗关键字
311
是
否
若文本内容中包含预设电信诈骗关键字，则确定程序具备预设电信诈骗特征
312
若文本内容中不包含预设电信诈骗关键字，则确定程序不具备预设电信诈骗特征
313
若程序具备预设电信诈骗特征，则确定程序为电信诈骗木马程序并进行拦截
314

图3

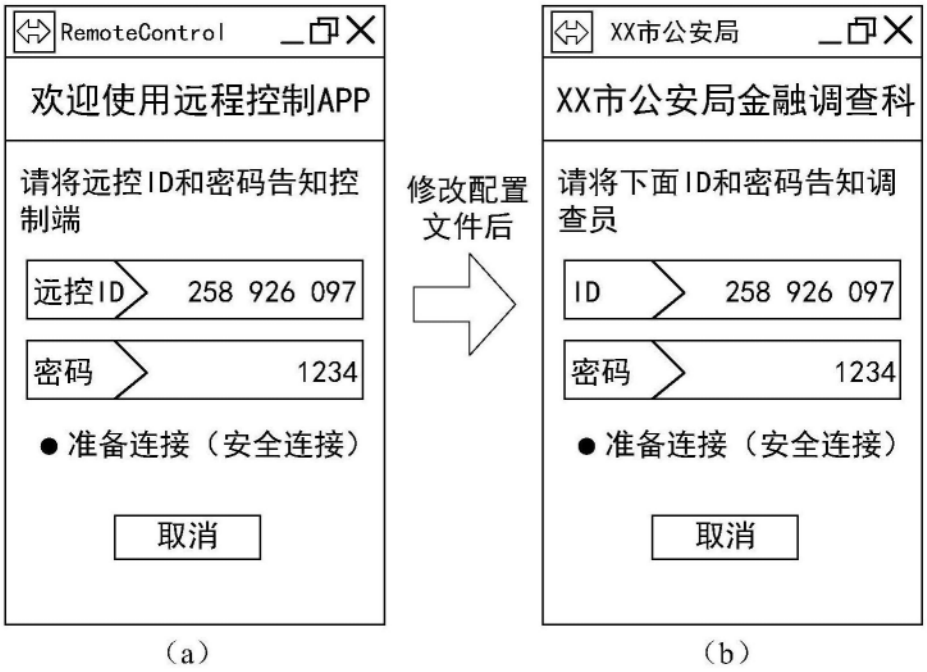

RemoteControl
欢迎使用远程控制APP
请将远控ID和密码告知控制端
远控ID
258 926 097
密码
1234
● 准备连接（安全连接）
取消
（a）
修改配置文件后
XX市公安局
XX市公安局金融调查科
请将下面ID和密码告知调查员
ID
258 926 097
密码
1234
● 准备连接（安全连接）
取消
（b）

图4

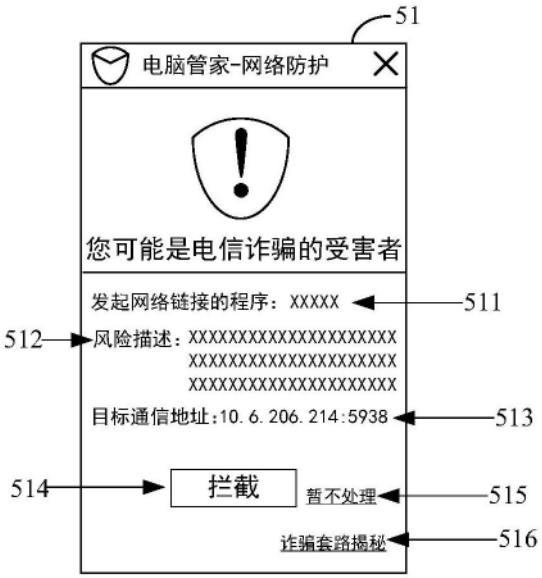

51
电脑管家-网络防护
您可能是电信诈骗的受害者
发起网络链接的程序：XXXXX
511
512
风险描述：XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXX
目标通信地址：10.6.206.214:5938
513
514
拦截
暂不处理
515
诈骗套路揭秘
516

图5

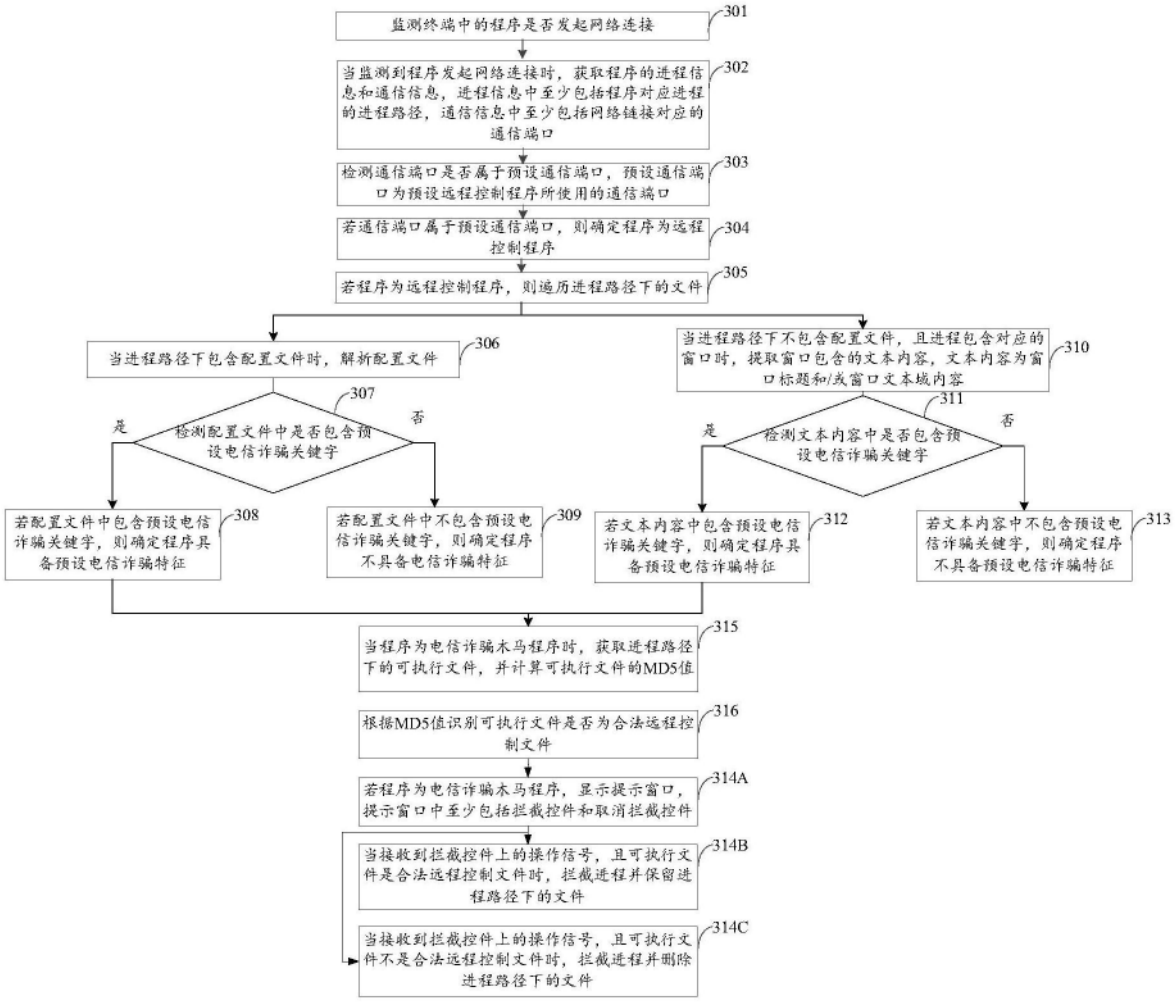

监测终端中的程序是否发起网络连接
301
当监测到程序发起网络连接时，获取程序的进程信息和通信信息，进程信息中至少包括程序对应进程的进程路径，通信信息中至少包括网络链接对应的通信端口
302
检测通信端口是否属于预设通信端口，预设通信端口为预设远程控制程序所使用的通信端口
303
若通信端口属于预设通信端口，则确定程序为远程控制程序
304
若程序为远程控制程序，则遍历进程路径下的文件
305
当进程路径下包含配置文件时，解析配置文件
306
检测配置文件中是否包含预设电信诈骗关键字
307
是
否
若配置文件中包含预设电信诈骗关键字，则确定程序具备预设电信诈骗特征
308
若配置文件中不包含预设电信诈骗关键字，则确定程序不具备电信诈骗特征
309
当进程路径下不包含配置文件，且进程包含对应的窗口时，提取窗口包含的文本内容，文本内容为窗口标题和/或窗口文本域内容
310
检测文本内容中是否包含预设电信诈骗关键字
311
是
否
若文本内容中包含预设电信诈骗关键字，则确定程序具备预设电信诈骗特征
312
若文本内容中不包含预设电信诈骗关键字，则确定程序不具备预设电信诈骗特征
313
当程序为电信诈骗木马程序时，获取进程路径下的可执行文件，并计算可执行文件的MD5值
315
根据MD5值识别可执行文件是否为合法远程控制文件
316
若程序为电信诈骗木马程序，显示提示窗口，提示窗口中至少包括拦截控件和取消拦截控件
314A
当接收到拦截控件上的操作信号，且可执行文件是合法远程控制文件时，拦截进程并保留进程路径下的文件
314B
当接收到拦截控件上的操作信号，且可执行文件不是合法远程控制文件时，拦截进程并删除进程路径下的文件
314C

图6

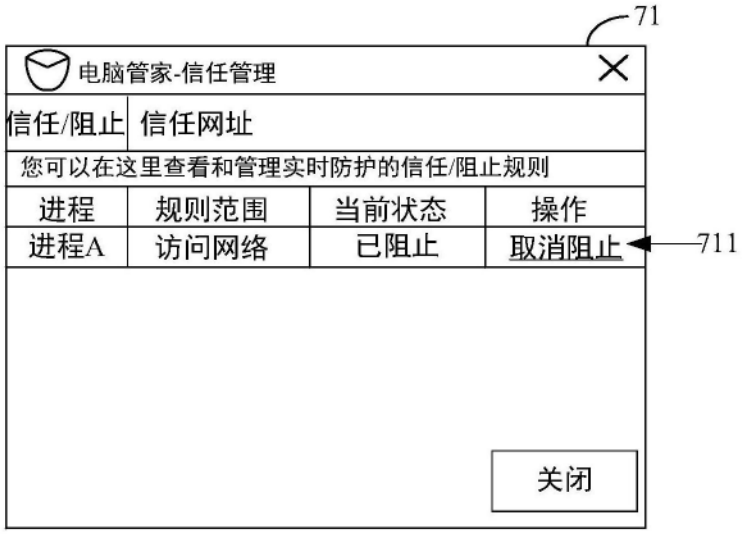

71
电脑管家-信任管理
信任/阻止
信任网址
您可以在这里查看和管理实时防护的信任/阻止规则
进程
规则范围
当前状态
操作
进程A
访问网络
已阻止
取消阻止
711
关闭

图7

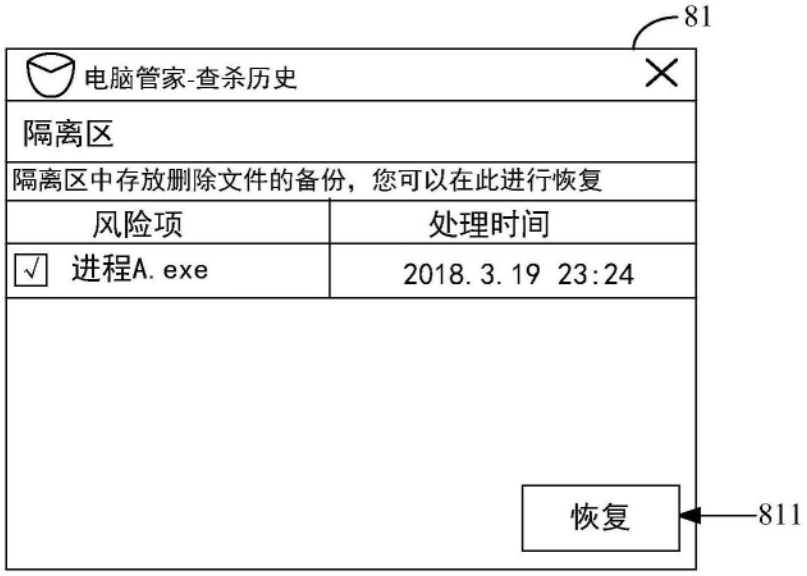

81
电脑管家-查杀历史
隔离区
隔离区中存放删除文件的备份，您可以在此进行恢复
风险项
处理时间
进程A.exe
2018.3.19 23:24
恢复
811

图8

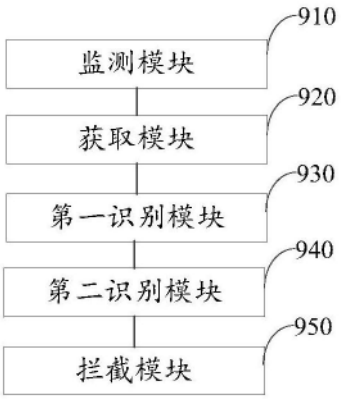

910
监测模块
920
获取模块
930
第一识别模块
940
第二识别模块
950
拦截模块

图9

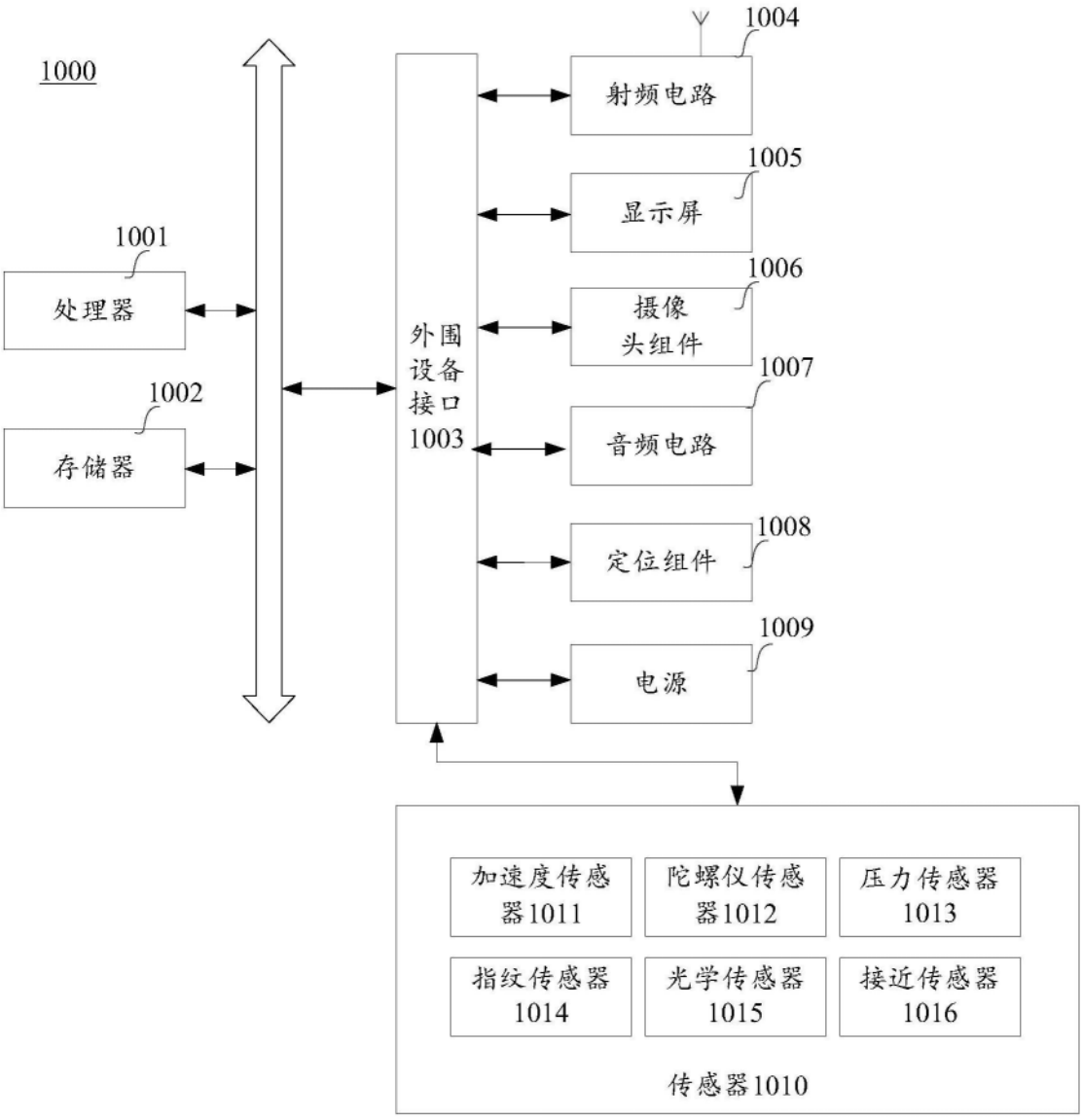

1000
1001
处理器
1002
存储器
外围设备接口1003
1004
射频电路
1005
显示屏
1006
摄像头组件
1007
音频电路
1008
定位组件
1009
电源
加速度传感器1011
陀螺仪传感器1012
压力传感器1013
指纹传感器1014
光学传感器1015
接近传感器1016
传感器1010

图10