(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107786413 B
(45)授权公告日 2022.03.22

(21)申请号 201610712468.2
(22)申请日 2016.08.24
(65)同一申请的已公布的文献号
申请公布号 CN 107786413 A
(43)申请公布日 2018.03.09
(73)专利权人 中兴通讯股份有限公司
地址 518057 广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦
(72)发明人 张金鑫 钟宏
(74)专利代理机构 深圳市力道知识产权代理事务所(普通合伙) 44507
代理人 张传义
(51)Int.Cl.
H04L 51/212(2022.01)
H04L 51/42(2022.01)

(56)对比文件
CN 1961272 A,2007.05.09
CN 1457181 A,2003.11.19
CN 101163274 A,2008.04.16
CN 105227570 A,2016.01.06
CN 1961272 A,2007.05.09

审查员 孟姗

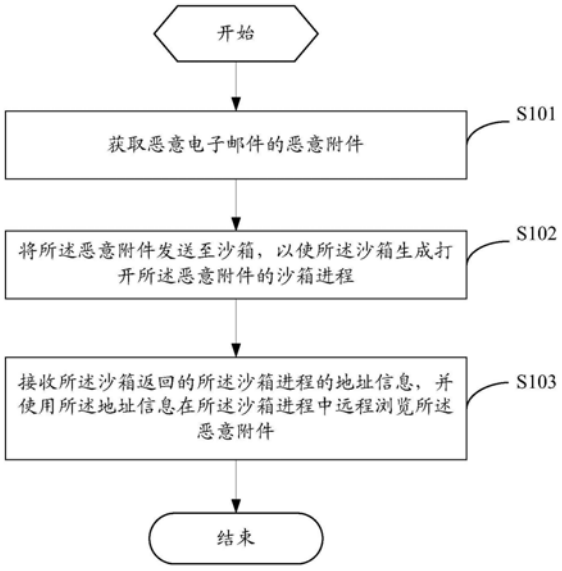
权利要求书2页 说明书8页 附图10页

(54)发明名称

一种浏览电子邮件的方法及用户终端

(57)摘要

通过获取恶意电子邮件的恶意附件;将所述恶意附件发送至沙箱,以使所述沙箱生成打开所述恶意附件的沙箱进程;接收所述沙箱返回的所述沙箱进程的地址信息,并使用所述地址信息在所述沙箱进程中远程浏览所述恶意附件。这样在实际办公环境中,通过远程浏览被送入沙箱中打开的恶意电子邮件的恶意附件,能够实现安全地对恶意电子邮件的恶意附件进行浏览。



CN 107786413 B

1.一种浏览电子邮件的方法,其特征在于,包括:

获取恶意电子邮件的恶意附件;

将所述恶意附件发送至沙箱,以使所述沙箱生成打开所述恶意附件的沙箱进程;

接收所述沙箱返回的所述沙箱进程的地址信息,并使用所述地址信息在所述沙箱进程中远程浏览所述恶意附件;

所述接收所述沙箱返回的所述沙箱进程的地址信息,并使用所述地址信息在所述沙箱进程中远程浏览所述恶意附件,包括:接收所述沙箱返回的所述沙箱进程的协议信息和端口信息,并使用所述协议信息和所述端口信息在所述沙箱进程中远程浏览所述恶意附件,其中,在所述沙箱进程中打开所述恶意文件时,所述沙箱进程所打开的所述恶意文件会被虚拟化重定向。

2.如权利要求1所述的方法,其特征在于,所述获取恶意电子邮件的恶意附件,包括:

获取所述恶意电子邮件的恶意附件和邮件标识;

所述将所述恶意附件发送至沙箱,以使所述沙箱生成打开所述恶意附件的沙箱进程,包括:

所述将所述恶意附件和所述邮件标识发送至沙箱,以使所述沙箱生成打开所述恶意附件的沙箱进程,并将所述邮件标识与所述沙箱进程进行关联;

所述接收所述沙箱返回的所述沙箱进程的地址信息,并使用所述地址信息在所述沙箱进程中远程浏览所述恶意附件之后,还包括:

发送所述邮件标识和结束请求至所述沙箱,以使所述沙箱响应所述结束请求,销毁与所述邮件标识关联的沙箱进程。

3.如权利要求1～2任一项所述的方法,其特征在于,所述获取恶意电子邮件的恶意附件之前,还包括:

接收所述邮件服务器发送的已拦截所述恶意电子邮件的提醒消息,其中,所述提醒消息包括所述恶意电子邮件的邮件标识,且所述恶意电子邮件的邮件标识与所述恶意电子邮件的恶意附件关联并存储于所述邮件服务器中;

所述获取恶意电子邮件的恶意附件,包括:

根据接收到的用户输入的所述邮件标识,从所述邮件服务器中调取与所述邮件标识关联的所述恶意附件。

4.如权利要求1～2任一项所述的方法,其特征在于,所述获取恶意电子邮件的恶意附件之前,还包括:

接收所述邮件服务器发送的被添加恶意标记的恶意电子邮件,其中,所述恶意电子邮件包括邮件标记和恶意附件,且所述邮件标记和所述恶意附件关联并存储于所述邮件服务器中;

根据接收到的用户对所述恶意电子邮件的打开操作,发送所述邮件标记至所述邮件服务器;

所述获取恶意电子邮件的恶意附件,包括:

接收所述邮件服务器返回与所述邮件标记关联的所述恶意附件。

5.一种用户终端,其特征在于,包括:

获取模块,用于获取恶意电子邮件的恶意附件;

发送模块，用于将所述恶意附件发送至沙箱，以使所述沙箱生成打开所述恶意附件的沙箱进程；

远程浏览模块，用于接收所述沙箱返回的所述沙箱进程的地址信息，并使用所述地址信息在所述沙箱进程中远程浏览所述恶意附件；

所述远程浏览模块还用于接收所述沙箱返回的所述沙箱进程的协议信息和端口信息，并使用所述协议信息和所述端口信息在所述沙箱进程中远程浏览所述恶意附件，其中，在所述沙箱进程中打开所述恶意文件时，所述沙箱进程所打开的所述恶意文件会被虚拟化重定向。

6.如权利要求5所述的用户终端，其特征在于，所述获取模块还用于获取所述恶意电子邮件的恶意附件和邮件标识；所述发送模块还用于所述将所述恶意附件和所述邮件标识发送至沙箱，以使所述沙箱生成打开所述恶意附件的沙箱进程，并将所述邮件标识与所述沙箱进程进行关联；所述用户终端还包括进程结束请求模块，用于发送所述邮件标识和结束请求至所述沙箱，以使所述沙箱响应所述结束请求，销毁与所述邮件标识关联的沙箱进程。

7.如权利要求5～6任一项所述的用户终端，其特征在于，所述用户终端还包括：

提醒模块，用于接收所述邮件服务器发送的已拦截所述恶意电子邮件的提醒消息，其中，所述提醒消息包括所述恶意电子邮件的邮件标识，且所述恶意电子邮件的邮件标识与所述恶意电子邮件的恶意附件关联并存储于所述邮件服务器中；

所述获取模块还用于根据接收到的用户输入的所述邮件标识，从所述邮件服务器中调取与所述邮件标识关联的所述恶意附件。

8.如权利要求5～6任一项所述的用户终端，其特征在于，所述用户终端还包括：

恶意电子邮件接收模块，用于接收所述邮件服务器发送的被添加恶意标记的恶意电子邮件，其中，所述恶意电子邮件包括邮件标记和恶意附件，且所述邮件标记和所述恶意附件关联并存储于所述邮件服务器中；

邮件标记发送模块，用于根据接收到的用户对所述恶意电子邮件的打开操作，发送所述邮件标记至所述邮件服务器；

所述获取模块还用于接收所述邮件服务器返回与所述邮件标记关联的所述恶意附件。

一种浏览电子邮件的方法及用户终端

技术领域

[0001] 本发明涉及通信技术领域,特别涉及一种浏览电子邮件的方法及用户终端。

背景技术

[0002] APT(Advanced Persistent Threat,高级持续性威胁)攻击因其具有难检测、持续时间长和攻击目标明确等特征,近年来已作为一种高级攻击手段出现在公众视野中,如极光攻击、震网攻击和夜龙攻击等均为APT攻击。APT攻击是以电子邮件等方式向用户发送使用0Day(0Day的内涵为“即时性”)漏洞的恶意附件,一旦用户打开该恶意附件,0Day漏洞就会被触发,攻击代码注入到用户系统,并进行后续下载其他病毒、木马等操作以利长期潜伏作业,而传统防火墙和企业反病毒软件等对此类无特征签名的恶意附件或代码的检测和防护能力非常有限。

[0003] 目前,对于APT攻击的防御通常先采用静态引擎分析和动态引擎分析结合的方法判定接收的电子邮件是否为恶意电子邮件,当一封电子邮件被判定为恶意电子邮件时,为了避免用户实际办公环境遭到破坏,企业的安全设备一般会直接在邮件服务器处拦截掉此封恶意电子邮件,或者提醒用户此封邮件是恶意的,此时,认为被判定的恶意电子邮件的附件是恶意附件。但是,这种方法在判定接收的电子邮件是否为恶意电子邮件时,存在误报的问题,可能会造成正常的电子邮件由于误报原因被拦截,这样用户就无法接收并查看该邮件,而当用户需要对被判定为恶意电子邮件的恶意附件进行浏览时,存在造成用户的实际办公环境遭受攻击的风险。

[0004] 可见,在实际办公环境中,存在无法安全地对恶意电子邮件的恶意附件进行浏览的问题。

发明内容

[0005] 本发明实施例的目的在于提供一种浏览电子邮件的方法及终端,解决在实际办公环境中,存在无法安全地对恶意电子邮件的恶意附件进行浏览的问题。

[0006] 为了达到上述目的,本发明实施例提供一种浏览电子邮件的方法,包括:

[0007] 获取恶意电子邮件的恶意附件;

[0008] 将所述恶意附件发送至沙箱,以使所述沙箱生成打开所述恶意附件的沙箱进程;

[0009] 接收所述沙箱返回的所述沙箱进程的地址信息,并使用所述地址信息在所述沙箱进程中远程浏览所述恶意附件。

[0010] 本发明还提供一种浏览电子邮件的用户终端,包括:

[0011] 获取模块,用于获取恶意电子邮件的恶意附件;

[0012] 发送模块,用于将所述恶意附件发送至沙箱,以使所述沙箱生成打开所述恶意附件的沙箱进程;

[0013] 远程浏览模块,用于接收所述沙箱返回的所述沙箱进程的地址信息,并使用所述地址信息在所述沙箱进程中远程浏览所述恶意附件。

[0014] 本发明实施例还提供一种计算机存储介质，所述计算机存储介质中存储有计算机可执行的一个或多个程序，所述一个或多个程序被所述计算机执行时使所述计算机执行如上述提供的一种浏览电子邮件的方法。

[0015] 上述技术方案中的一个技术方案具有如下优点或有益效果：

[0016] 通过获取恶意电子邮件的恶意附件；将所述恶意附件发送至沙箱，以使所述沙箱生成打开所述恶意附件的沙箱进程；接收所述沙箱返回的所述沙箱进程的地址信息，并使用所述地址信息在所述沙箱进程中远程浏览所述恶意附件。这样在实际办公环境中，通过远程浏览被送入沙箱中打开的恶意电子邮件的恶意附件，能够实现安全地对恶意电子邮件的恶意附件进行浏览。

附图说明

[0017] 图1为本发明实施例提供的一种浏览电子邮件的方法的流程示意图；

[0018] 图2为本发明实施例提供的另一种浏览电子邮件的方法的流程示意图；

[0019] 图3为本发明实施例提供的另一种浏览电子邮件的方法的流程示意图；

[0020] 图4为本发明实施例提供的另一种浏览电子邮件的方法的流程示意图；

[0021] 图5为本发明实施例中第一应用场景的邮件服务器对恶意电子邮件的提取、存储和通信的流程示意图；

[0022] 图6为本发明实施例中第一应用场景的实现浏览电子邮件的流程示意图；

[0023] 图7为本发明实施例中第二应用场景的邮件服务器对恶意电子邮件的提取、存储和通信的流程示意图；

[0024] 图8为本发明实施例中第二应用场景的实现浏览电子邮件的流程示意图；

[0025] 图9为本发明实施例提供的一种用户终端的结构示意图；

[0026] 图10是本发明实施例提供的另一种用户终端的结构示意图；

[0027] 图11是本发明实施例提供的另一种用户终端的结构示意图；

[0028] 图12是本发明实施例提供的另一种用户终端的结构示意图。

具体实施方式

[0029] 为使本发明要解决的技术问题、技术方案和优点更加清楚，下面将结合附图及具体实施例进行详细描述。

[0030] 如图1所示，本发明实施例提供一种浏览电子邮件的方法的流程示意图，包括以下步骤：

[0031] 步骤S101、获取恶意电子邮件的恶意附件；

[0032] 本发明实施例中，邮件服务器在接收到电子邮件时，其安全设备会判定电子邮件是否为恶意电子邮件，当判定该电子邮件为恶意电子邮件时，会将该恶意电子邮件进行拦截或者在该恶意电子邮件上添加恶意标记，以避免用户在不知道存在风险的情况下打开该恶意电子邮件。

[0033] 上述获取恶意电子邮件的恶意附件，可以理解为：用户终端接收用户输入的被拦截的恶意电子邮件的邮件标记，或者用户对添加恶意标记的恶意电子邮件的打开操作获取的该邮件的邮件标记，并发送该邮件标记至邮件服务器，以请求邮件服务器发送与邮件标

记对应的恶意附件至用户终端。其中，恶意电子邮件的恶意附件和其邮件标记对应关联存储于邮件服务器中。

[0034] 步骤S102、将所述恶意附件发送至沙箱，以使所述沙箱生成打开所述恶意附件的沙箱进程。

[0035] 本发明实施例中，用户终端在接收到恶意附件后，会将该恶意附件发送给沙箱，通过沙箱技术在沙箱中生成新的沙箱进程，并在该沙箱进程中打开恶意文件。其中，在沙箱进程中打开该恶意文件时，沙箱进程所打开的恶意文件会被虚拟化重定向，也就是说对恶意文件的打开操作是虚拟的，真实的恶意文件不会被改动，这样可以确保恶意文件打开后下载的病毒无法改动破坏系统。

[0036] 步骤S103、接收所述沙箱返回的所述沙箱进程的地址信息，并使用所述地址信息在所述沙箱进程中远程浏览所述恶意附件。

[0037] 本发明实施例中，恶意附件在沙箱进程内打开后，沙箱会发送地址信息至用户终端，用户终端在接收沙箱返回的地址信息时，可以使用该地址信息与沙箱建立远程连接，用户通过与沙箱建立远程连接的用户终端，浏览在沙箱进程内打开的恶意附件，从而能够安全地浏览被邮件服务器的安全设备判定的恶意电子邮件。其中，上述地址信息可以为沙箱进程的协议信息或端口信息或者协议信息和端口信息的组合，当然，也可以为其他能用于建立用户终端和沙箱的远程连接的信息，在此不作限定。

[0038] 本发明实施例中，上述用户终端可以为任何具备浏览电子邮件的终端设备，例如：台式电脑、笔记本电脑、掌上电脑、手机、平板电脑(Tablet Personal Computer)、膝上型电脑(Laptop Computer)、个人数字助理(personal digital assistant，简称PDA)、移动上网装置(Mobile Internet Device，MID)或可穿戴式设备(Wearable Device)等。

[0039] 本发明实施例中，通过获取恶意电子邮件的恶意附件；将所述恶意附件发送至沙箱，以使所述沙箱生成打开所述恶意附件的沙箱进程；接收所述沙箱返回的所述沙箱进程的地址信息，并使用所述地址信息在所述沙箱进程中远程浏览所述恶意附件。这样在实际办公环境中，通过远程浏览被送入沙箱中打开的恶意电子邮件的恶意附件，能够实现安全地对恶意电子邮件的恶意附件进行浏览。

[0040] 如图2所示，本发明实施例提供一种浏览电子邮件的方法的流程示意图，包括以下步骤：

[0041] 步骤S201、获取恶意电子邮件的恶意附件；

[0042] 本发明实施例中，用户终端接收用户输入的被拦截的恶意电子邮件的邮件标记，或者用户对添加恶意标记的恶意电子邮件的打开操作获取的该邮件的邮件标记，并发送该邮件标记至邮件服务器，以请求邮件服务器发送与邮件标记对应的恶意附件至用户终端。其中，恶意电子邮件的恶意附件和其邮件标记对应关联存储于邮件服务器中。上述恶意附件可以为包括文本类、网页类以及图片类等中任一形式的附件；上述邮件标记可以为恶意电子邮件的恶意附件存储于邮件服务器中的序列号，也可以为其他识别该邮件的信息。

[0043] 步骤S202、将所述恶意附件发送至沙箱，以使所述沙箱生成打开所述恶意附件的沙箱进程；

[0044] 本发明实施例中，用户终端在接收到恶意附件后，会将该恶意附件发送给沙箱，通过沙箱技术在沙箱中生成新的沙箱进程，并在该沙箱进程中打开恶意文件。其中，上述沙箱

可以是任何沙箱。本发明实施例中，可以采用轻量级沙箱。轻量级沙箱能够在一定程度上节省计算资源。

[0045] 步骤S203、接收所述沙箱返回的所述沙箱进程的协议信息和端口信息，并使用所述协议信息和所述端口信息在所述沙箱进程中远程浏览所述恶意附件。

[0046] 本发明实施例中，恶意附件在沙箱进程内打开后，沙箱会发送其协议信息和端口信息至用户终端，用户终端在接收沙箱返回的协议信息和端口信息时，可以使用该协议信息和端口信息与沙箱建立远程连接，用户通过与沙箱建立远程连接的用户终端，浏览在沙箱进程内打开的恶意附件，从而能够安全地浏览被邮件服务器的安全设备判定的恶意电子邮件。

[0047] 可选的，上述步骤S201，可以包括：获取所述恶意电子邮件的恶意附件和邮件标识；上述步骤202，可以包括：所述将所述恶意附件和所述邮件标识发送至沙箱，以使所述沙箱生成打开所述恶意附件的沙箱进程，并将所述邮件标识与所述沙箱进程进行关联；上述步骤S203之后，还可以包括：发送所述邮件标识和结束请求至所述沙箱，以使所述沙箱响应所述结束请求，销毁与所述邮件标识关联的沙箱进程。

[0048] 本发明实施例中，用户终端可以由用户输入或者用户恶意打开电子邮件时获取恶意电子邮件的邮件标识，并将该邮件标识发送至邮件服务器中，请求邮件服务器将与该邮件标识关联的恶意附件发送至用户终端，用户终端再将获取的邮件标识和恶意附件发送至沙箱内，沙箱会生成打开该恶意附件的沙箱进程，并且将沙箱进程的协议信息与该邮件标识进行关联并记录与关联表中，当用户终端接收到用户完成浏览的操作时，发送与浏览的恶意附件对应的邮件标识和结束请求至沙箱，沙箱响应该结束请求，查询关联表中与邮件标识对应的协议信息，并将拥有该协议信息的沙箱进程销毁，从而避免沙箱的资源浪费。

[0049] 可选的，如图3所示，上述步骤S201之前，还可以包括：

[0050] 步骤S204、接收所述邮件服务器发送的已拦截所述恶意电子邮件的提醒消息，其中，所述提醒消息包括所述恶意电子邮件的邮件标识，且所述恶意电子邮件的邮件标识与所述恶意电子邮件的恶意附件关联并存储于所述邮件服务器中；

[0051] 则上述步骤S201，可以包括：根据接收到的用户输入的所述邮件标识，从所述邮件服务器中调取与所述邮件标识关联的所述恶意附件。

[0052] 本发明实施例中，邮件服务器在其安全设备判定电子邮件件为恶意电子邮件后，对该恶意电子邮件进行拦截，并还原该恶意电子邮件的流量，以提取恶意电子邮件中的恶意附件以及对应的邮件标识。再通过建立关联表将该恶意附件和邮件标识进行关联，将该恶意文件存储与邮件服务器中。邮件服务器在建立邮件标记和恶意附件的关联后，会发送提醒消息至用户终端，且该提醒消息中包括被拦截的恶意电子邮件的邮件标识。

[0053] 用户终端接收到邮件服务器发送的提醒消息后，提醒用户并告知用户被拦截的恶意电子邮件的邮件标识。当用户需要对某一被拦截的恶意电子邮件的恶意附件进行浏览时，可以通过用户终端输入该恶意电子邮件的邮件标识，用户终端根据接收到的用户输入的邮件标识，请求邮件服务器发送与该邮件标识关联的恶意附件，邮件服务器响应用户终端的请求，通过上述关联表查询与该邮件标识关联的恶意电子邮件并发送至用户终端。

[0054] 可选的，如图4所示，上述步骤S201之前，还可以包括：

[0055] 步骤S205、接收所述邮件服务器发送的被添加恶意标记的恶意电子邮件，其中，所

述恶意电子邮件包括邮件标记和恶意附件，且所述邮件标记和所述恶意附件关联并存储于所述邮件服务器中。

[0056] 步骤S206、根据接收到的用户对所述恶意电子邮件的打开操作，发送所述邮件标记至所述邮件服务器。

[0057] 则上述步骤S201，可以包括：接收所述邮件服务器返回与所述邮件标记关联的所述恶意附件。

[0058] 本发明实施例中，邮件服务器在其安全设备判定电子邮件件为恶意电子邮件后，对该恶意电子邮件进行拦截，并还原该恶意电子邮件的流量，以提取恶意电子邮件中的恶意附件以及对应的邮件标识。再通过建立关联表将该恶意附件和邮件标识进行关联，将该恶意文件存储与邮件服务器中。邮件服务器在建立邮件标记和恶意附件的关联后，会将该恶意电子邮件添加恶意标记后发送至用户终端。其中，该恶意标记为告知用户该邮件为恶意电子邮件的标记。

[0059] 用户终端接收到添加有恶意标记的恶意电子邮件后，会实时通知用户已接收到该恶意电子邮件，若用户需要对该恶意电子邮件的恶意附件进行浏览，通过用户终端点击该恶意电子邮件以打开恶意附件，用户终端接收到用户的点击打开带有恶意标记的恶意电子邮件时，会发送恶意电子邮件的邮件标记至邮件服务器，请求邮件服务器返回与该邮件标记关联的恶意附件。

[0060] 本发明实施例中，通过使用沙箱返回的打开恶意文件的沙箱进程的协议信息和端口信息，与沙箱建立远程连接，从而可以在沙箱进程中远程浏览恶意电子邮件的恶意附件，实现用户安全地对恶意附件的浏览。

[0061] 下面举例对本发明实施例的应用场景进行说明：

[0062] 如图5和图6所示，是本发明实施例在第一应用场景的过程，其中，图5为本发明实施例中邮件服务器对恶意电子邮件的提取、存储和通信的流程示意图，该过程可以由邮件服务器的附件提取模块、存储模块以及通信模块执行，包括：附件提取模块对流量还原，提取恶意电子邮件的恶意附件以及对应的邮件标识，并发送恶意附件以及邮件标识至存储模块；存储模块存储接收的恶意附件，建立邮件关联表将恶意文件与邮件标识关联，并发送邮件标识至通信模块；通信模块将邮件标识发送给用户终端。需要说明的是，上述过程仅仅是说明邮件服务器对恶意电子邮件的提取、存储和通信的过程，并不局限于由附件提取模块、存储模块以及通信模块执行。

[0063] 其中，图6为本发明实施例中第一应用场景的实现浏览电子邮件的流程示意图，该过程可以在邮件服务器、载入单元、用户终端以及沙箱中进行，包括：邮件服务器存储提取的恶意电子邮件的恶意附件，建立邮件关联表，并发送提醒消息用户终端；用户终端向载入单元发出浏览启动请求，并传送邮件标识；载入单元在接收到用户终端的浏览启动请求后，发送邮件标识和查询请求至邮件服务器；邮件服务器响应查询请求，根据邮件标识查询邮件关联表并得到关联的恶意附件，并发送恶意附件至载入单元；载入单元将恶意附件和邮件标识发送至沙箱；沙箱生成新的沙箱进程，打开恶意附件，建立沙箱进程的协议信息与邮件标识的进程关联表，并发送沙箱进程的协议信息和端口信息至用户终端；用户终端根据沙箱进程的协议信息和端口信息，与沙箱建立远程连接，浏览恶意文件的内容，当用户完成浏览时，发送结束请求和邮件标识至沙箱；沙箱根据邮件标识在进程关联表中查询到关联

的沙箱进程并进行销毁。需要说明的是，所述载入单元执行的动作可以由邮件服务器或用户终端完成，即邮件服务器或用户包括该载入单元。

[0064] 如图7和图8所示，是本发明实施例在第二应用场景的过程，图7为本发明实施例中邮件服务器对恶意电子邮件的提取、存储和通信的流程示意图，该过程可以由邮件服务器的附件提取模块、存储模块以及邮件标记模块执行，包括：附件提取模块对流量还原，提取恶意电子邮件的恶意附件以及对应的邮件标识，并发送恶意附件以及邮件标识至存储模块；存储模块存储接收的恶意附件，建立邮件关联表将恶意文件与邮件标识关联，并发送邮件标识至邮件标记模块；恶意标记模块将恶意电子邮件打上恶意标记。需要说明的是，上述过程仅仅是说明邮件服务器对恶意电子邮件的提取、存储和通信的过程，并不局限于由附件提取模块、存储模块以及恶意标记模块执行。

[0065] 其中，图8为本发明实施例在第二应用场景中实现浏览电子邮件的流程示意图，该过程可以在邮件服务器、载入单元、用户终端以及沙箱中进行，包括：邮件服务器存储提取的恶意电子邮件的恶意附件，建立邮件关联表，并将恶意电子邮件打上恶意标记；用户终端接收用户点击打开带有恶意标记的恶意电子邮件的操作，并发送浏览启动请求和邮件标记至载入单元；载入单元在接收到用户终端的浏览启动请求后，发送邮件标识和查询请求至邮件服务器；邮件服务器响应查询请求，根据邮件标识查询邮件关联表并得到关联的恶意附件，并发送恶意附件至载入单元；载入单元将恶意附件和邮件标识发送至沙箱；沙箱生成新的沙箱进程，打开恶意附件，建立沙箱进程的协议信息与邮件标识的进程关联表，并发送沙箱进程的协议信息和端口信息至用户终端；用户终端根据沙箱进程的协议信息和端口信息，与沙箱建立远程连接，浏览恶意文件的内容，当用户完成浏览时，发送结束请求和邮件标识至沙箱；沙箱根据邮件标识在进程关联表中查询到关联的沙箱进程并进行销毁。需要说明的是，所述载入单元执行的动作可以由邮件服务器或用户终端完成，即邮件服务器或用户包括该载入单元。

[0066] 如图9所示，本发明实施例提供一种用户终端的结构示意图，所述用户终端90包括：

[0067] 获取模块91，用于获取恶意电子邮件的恶意附件；

[0068] 发送模块92，用于将所述恶意附件发送至沙箱，以使所述沙箱生成打开所述恶意附件的沙箱进程；

[0069] 远程浏览模块93，用于接收所述沙箱返回的所述沙箱进程的地址信息，并使用所述地址信息在所述沙箱进程中远程浏览所述恶意附件。

[0070] 可选的，所述远程浏览模块还可以用于接收所述沙箱返回的所述沙箱进程的协议信息和端口信息，并使用所述协议信息和所述端口信息在所述沙箱进程中远程浏览所述恶意附件。

[0071] 可选的，所述获取模块还可以用于获取所述恶意电子邮件的恶意附件和邮件标识；所述发送模块还可以用于所述将所述恶意附件和所述邮件标识发送至沙箱，以使所述沙箱生成打开所述恶意附件的沙箱进程，并将所述邮件标识与所述沙箱进程进行关联；如图10所示，所述用户终端90还可以包括进程结束请求模块94，用于发送所述邮件标识和结束请求至所述沙箱，以使所述沙箱响应所述结束请求，销毁与所述邮件标识关联的沙箱进程。

[0072] 可选的，如图11所示，所述用户终端90还可以包括：

[0073] 提醒模块95，用于接收所述邮件服务器发送的已拦截所述恶意电子邮件的提醒消息，其中，所述提醒消息包括所述恶意电子邮件的邮件标识，且所述恶意电子邮件的邮件标识与所述恶意电子邮件的恶意附件关联并存储于所述邮件服务器中；

[0074] 所述获取模块91还可以用于根据接收到的用户输入的所述邮件标识，从所述邮件服务器中调取与所述邮件标识关联的所述恶意附件。

[0075] 可选的，如图12所示，所述用户终端90还可以包括：

[0076] 恶意电子邮件接收模块96，用于接收所述邮件服务器发送的被添加恶意标记的恶意电子邮件，其中，所述恶意电子邮件包括邮件标记和恶意附件，且所述邮件标记和所述恶意附件关联并存储于所述邮件服务器中；

[0077] 邮件标记发送模块97，用于根据接收到的用户对所述恶意电子邮件的打开操作，发送所述邮件标记至所述邮件服务器；

[0078] 所述获取模块91还可以用于接收所述邮件服务器返回与所述邮件标记关联的所述恶意附件。

[0079] 所述用户终端90能够实现图1至图8的方法实施例中用户终端实现的各个过程，以及能达到相同的有益效果，为避免重复，这里不再赘述。

[0080] 本领域普通技术人员可以理解实现上述实施例方法的全部或者部分步骤是可以通过程序指令相关的硬件来完成，所述的程序可以存储于一计算机可读取介质中，该程序在执行时，包括以下步骤：

[0081] 获取恶意电子邮件的恶意附件；

[0082] 将所述恶意附件发送至沙箱，以使所述沙箱生成打开所述恶意附件的沙箱进程；

[0083] 接收所述沙箱返回的所述沙箱进程的地址信息，并使用所述地址信息在所述沙箱进程中远程浏览所述恶意附件。

[0084] 可选的，所述接收所述沙箱返回的所述沙箱进程的地址信息，并使用所述地址信息在所述沙箱进程中远程浏览所述恶意附件，包括：

[0085] 接收所述沙箱返回的所述沙箱进程的协议信息和端口信息，并使用所述协议信息和所述端口信息在所述沙箱进程中远程浏览所述恶意附件。

[0086] 可选的，所述获取恶意电子邮件的恶意附件，包括：

[0087] 获取所述恶意电子邮件的恶意附件和邮件标识；

[0088] 所述将所述恶意附件发送至沙箱，以使所述沙箱生成打开所述恶意附件的沙箱进程，包括：

[0089] 所述将所述恶意附件和所述邮件标识发送至沙箱，以使所述沙箱生成打开所述恶意附件的沙箱进程，并将所述邮件标识与所述沙箱进程进行关联；

[0090] 所述接收所述沙箱返回的所述沙箱进程的地址信息，并使用所述地址信息在所述沙箱进程中远程浏览所述恶意附件之后，还包括：

[0091] 发送所述邮件标识和结束请求至所述沙箱，以使所述沙箱响应所述结束请求，销毁与所述邮件标识关联的沙箱进程。

[0092] 可选的，所述获取恶意电子邮件的恶意附件之前，还包括：

[0093] 接收所述邮件服务器发送的已拦截所述恶意电子邮件的提醒消息，其中，所述提

醒消息包括所述恶意电子邮件的邮件标识,且所述恶意电子邮件的邮件标识与所述恶意电子邮件的恶意附件关联并存储于所述邮件服务器中;

[0094] 所述获取恶意电子邮件的恶意附件,包括:

[0095] 根据接收到的用户输入的所述邮件标识,从所述邮件服务器中调取与所述邮件标识关联的所述恶意附件。

[0096] 可选的,所述获取恶意电子邮件的恶意附件之前,还包括:

[0097] 接收所述邮件服务器发送的被添加恶意标记的恶意电子邮件,其中,所述恶意电子邮件包括邮件标记和恶意附件,且所述邮件标记和所述恶意附件关联并存储于所述邮件服务器中;

[0098] 根据接收到的用户对所述恶意电子邮件的打开操作,发送所述邮件标记至所述邮件服务器;

[0099] 所述获取恶意电子邮件的恶意附件,包括:

[0100] 接收所述邮件服务器返回与所述邮件标记关联的所述恶意附件。

[0101] 所述的存储介质,如只读存储器(Read-Only Memory,简称ROM)、随机存取存储器(Random Access Memory,简称RAM)、磁碟或者光盘等。

[0102] 以上所述是本发明的优选实施方式,应当指出,对于本技术领域的普通技术人员来说,在不脱离本发明所述原理的前提下,还可以作出若干改进和润饰,这些改进和润饰也应视为本发明的保护范围。

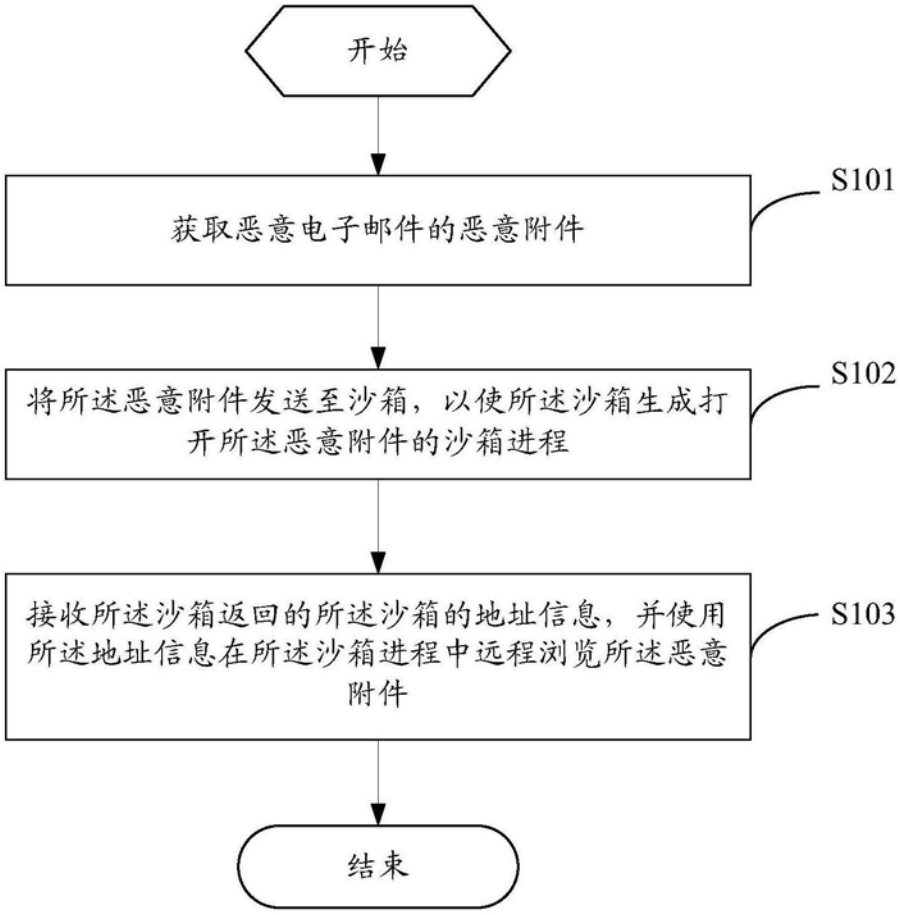

开始
获取恶意电子邮件的恶意附件
S101
将所述恶意附件发送至沙箱，以使所述沙箱生成打开所述恶意附件的沙箱进程
S102
接收所述沙箱返回的所述沙箱的地址信息，并使用所述地址信息在所述沙箱进程中远程浏览所述恶意附件
S103
结束

图1

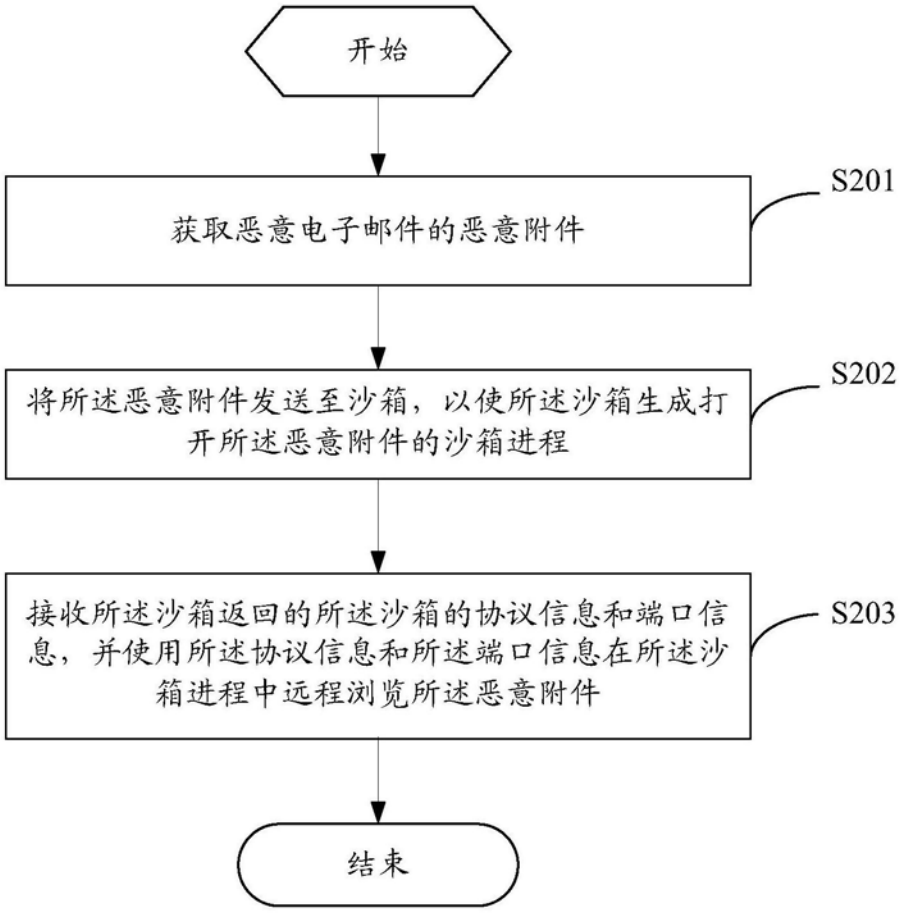

开始
获取恶意电子邮件的恶意附件
S201
将所述恶意附件发送至沙箱，以使所述沙箱生成打开所述恶意附件的沙箱进程
S202
接收所述沙箱返回的所述沙箱的协议信息和端口信息，并使用所述协议信息和所述端口信息在所述沙箱进程中远程浏览所述恶意附件
S203
结束

图2

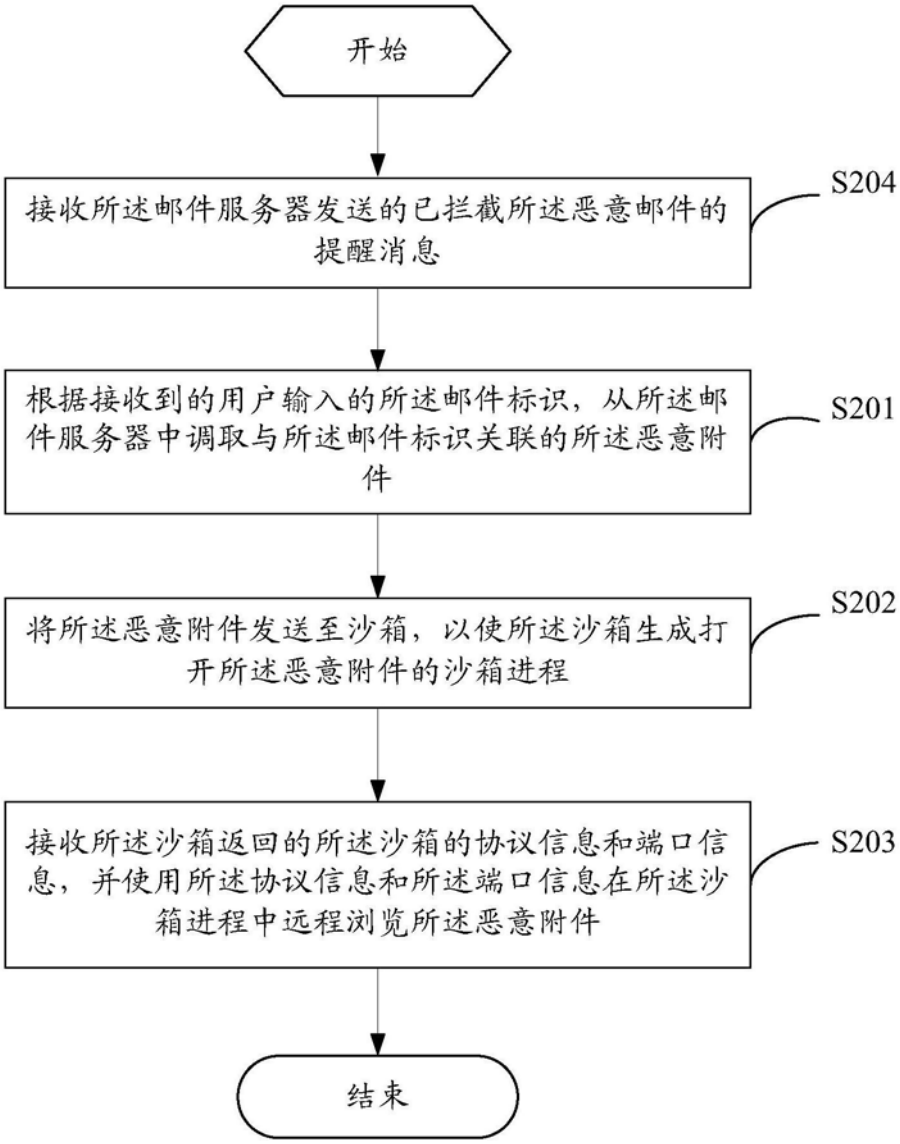

开始
接收所述邮件服务器发送的已拦截所述恶意邮件的提醒消息
S204
根据接收到的用户输入的所述邮件标识，从所述邮件服务器中调取与所述邮件标识关联的所述恶意附件
S201
将所述恶意附件发送至沙箱，以使所述沙箱生成打开所述恶意附件的沙箱进程
S202
接收所述沙箱返回的所述沙箱的协议信息和端口信息，并使用所述协议信息和所述端口信息在所述沙箱进程中远程浏览所述恶意附件
S203
结束

图3

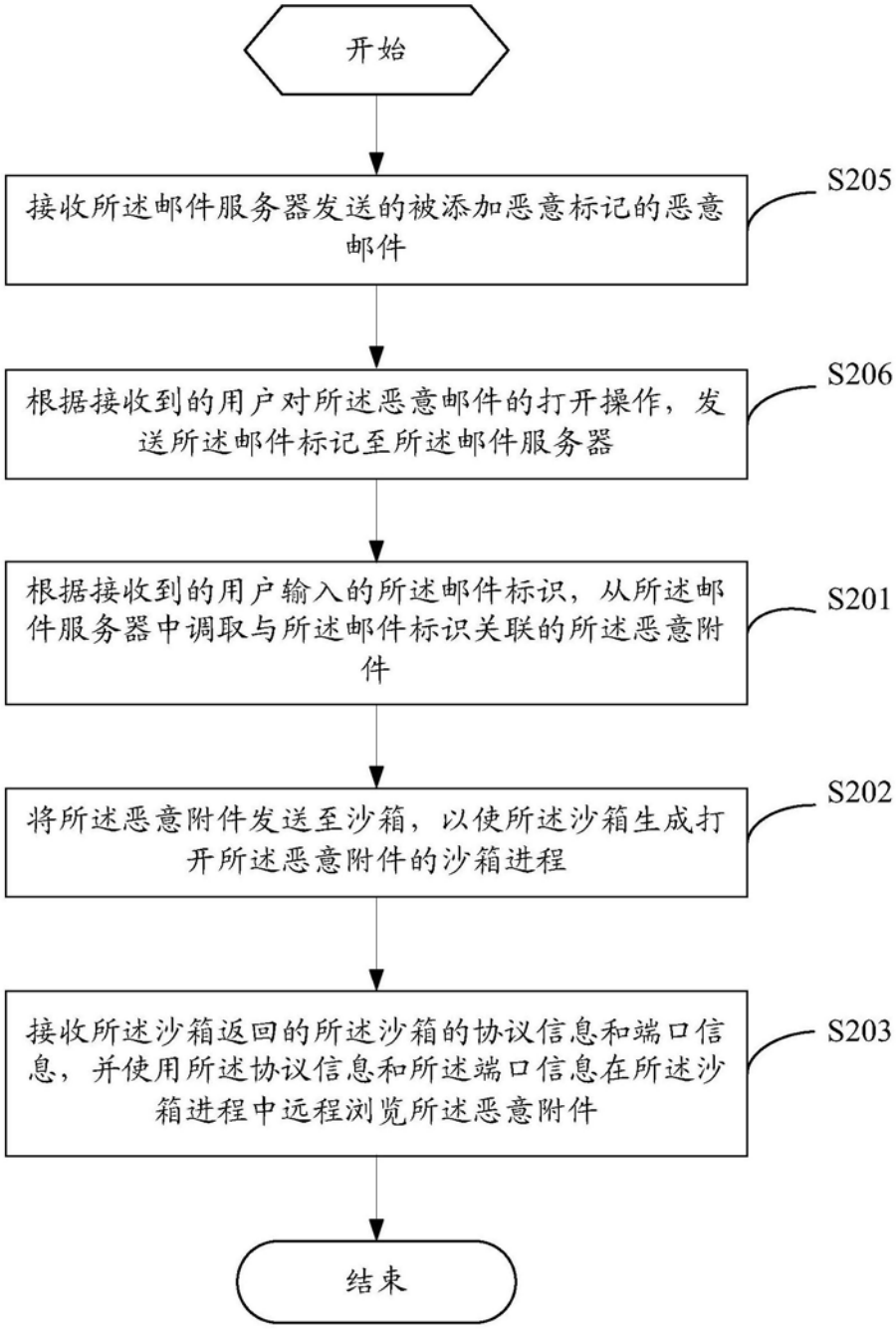

开始
接收所述邮件服务器发送的被添加恶意标记的恶意邮件
S205
根据接收到的用户对所述恶意邮件的打开操作，发送所述邮件标记至所述邮件服务器
S206
根据接收到的用户输入的所述邮件标识，从所述邮件服务器中调取与所述邮件标识关联的所述恶意附件
S201
将所述恶意附件发送至沙箱，以使所述沙箱生成打开所述恶意附件的沙箱进程
S202
接收所述沙箱返回的所述沙箱的协议信息和端口信息，并使用所述协议信息和所述端口信息在所述沙箱进程中远程浏览所述恶意附件
S203
结束

图4

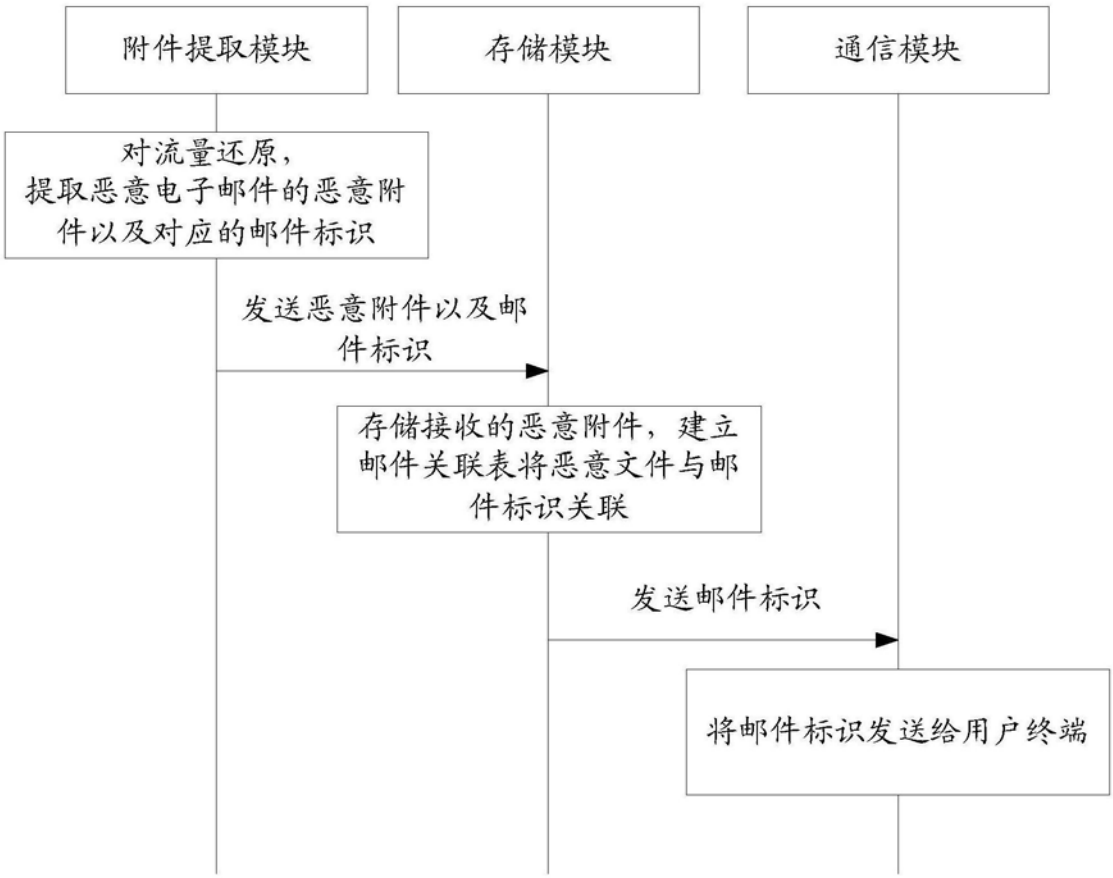

附件提取模块
存储模块
通信模块
对流量还原，
提取恶意电子邮件的恶意附件以及对应的邮件标识
发送恶意附件以及邮件标识
存储接收的恶意附件，建立邮件关联表将恶意文件与邮件标识关联
发送邮件标识
将邮件标识发送给用户终端

图5

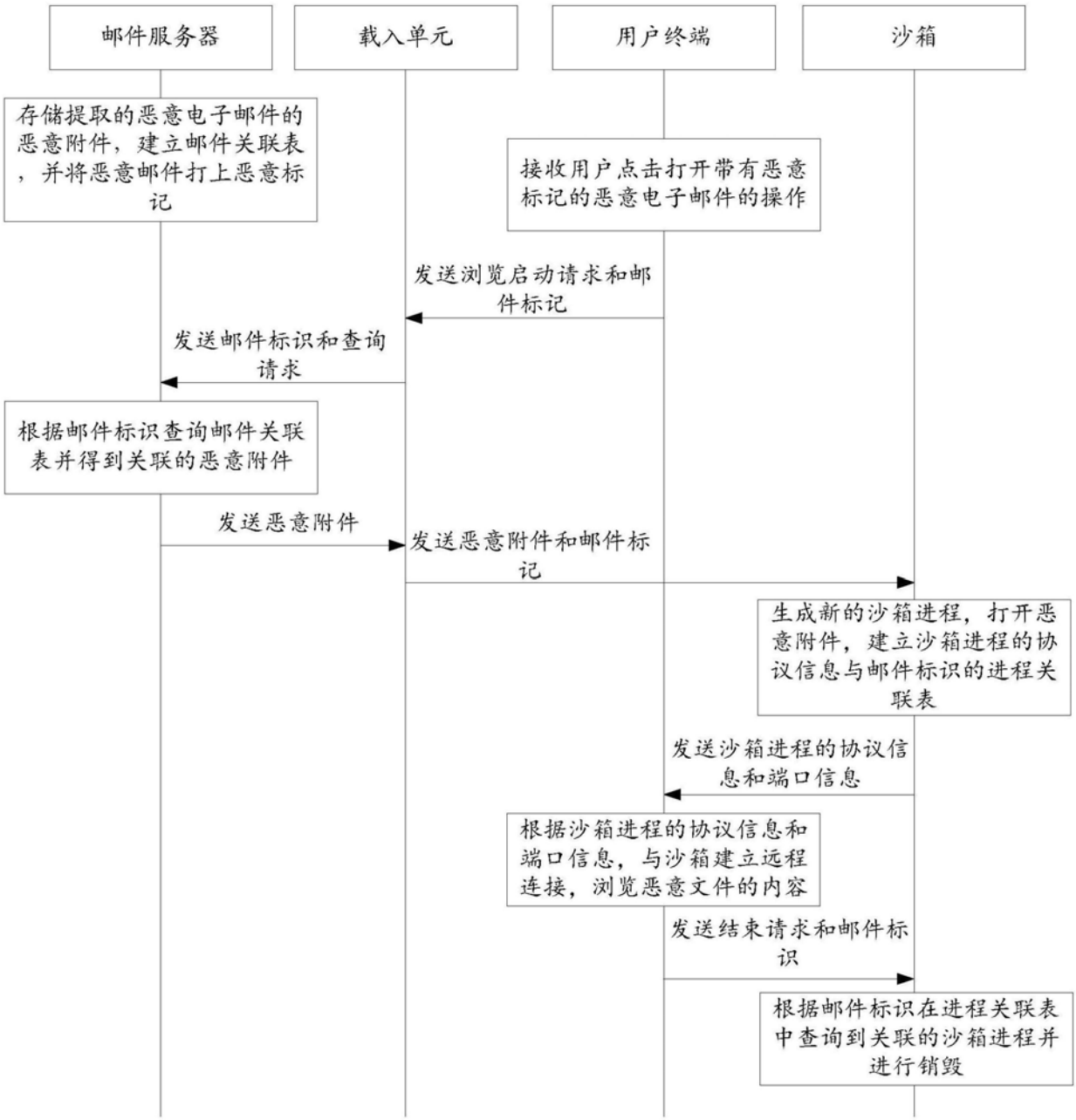

邮件服务器
载入单元
用户终端
沙箱
存储提取的恶意电子邮件的恶意附件，建立邮件关联表，并将恶意邮件打上恶意标记
接收用户点击打开带有恶意标记的恶意电子邮件的操作
发送浏览启动请求和邮件标记
发送邮件标识和查询请求
根据邮件标识查询邮件关联表并得到关联的恶意附件
发送恶意附件
发送恶意附件和邮件标记
生成新的沙箱进程，打开恶意附件，建立沙箱进程的协议信息与邮件标识的进程关联表
发送沙箱进程的协议信息和端口信息
根据沙箱进程的协议信息和端口信息，与沙箱建立远程连接，浏览恶意文件的内容
发送结束请求和邮件标识
根据邮件标识在进程关联表中查询到关联的沙箱进程并进行销毁

图6

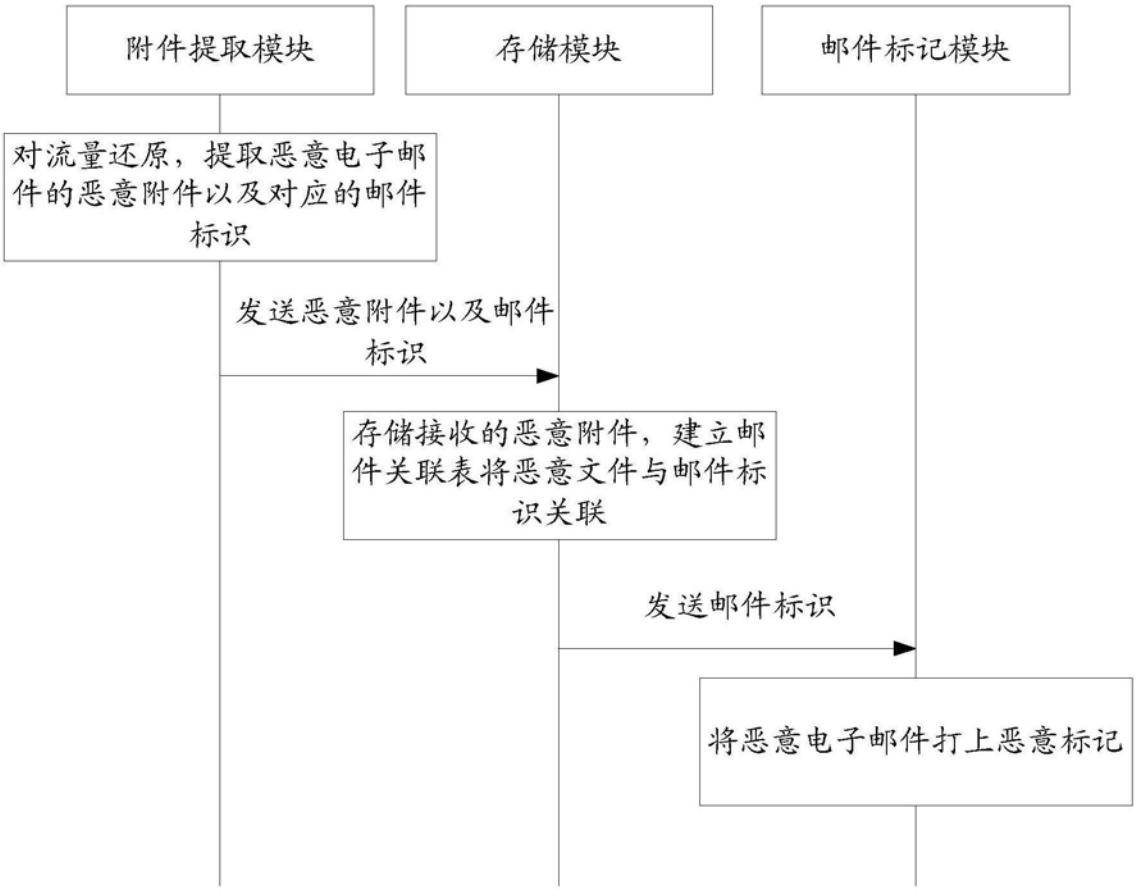

附件提取模块
存储模块
邮件标记模块
对流量还原，提取恶意电子邮件的恶意附件以及对应的邮件标识
发送恶意附件以及邮件标识
存储接收的恶意附件，建立邮件关联表将恶意文件与邮件标识关联
发送邮件标识
将恶意电子邮件打上恶意标记

图7

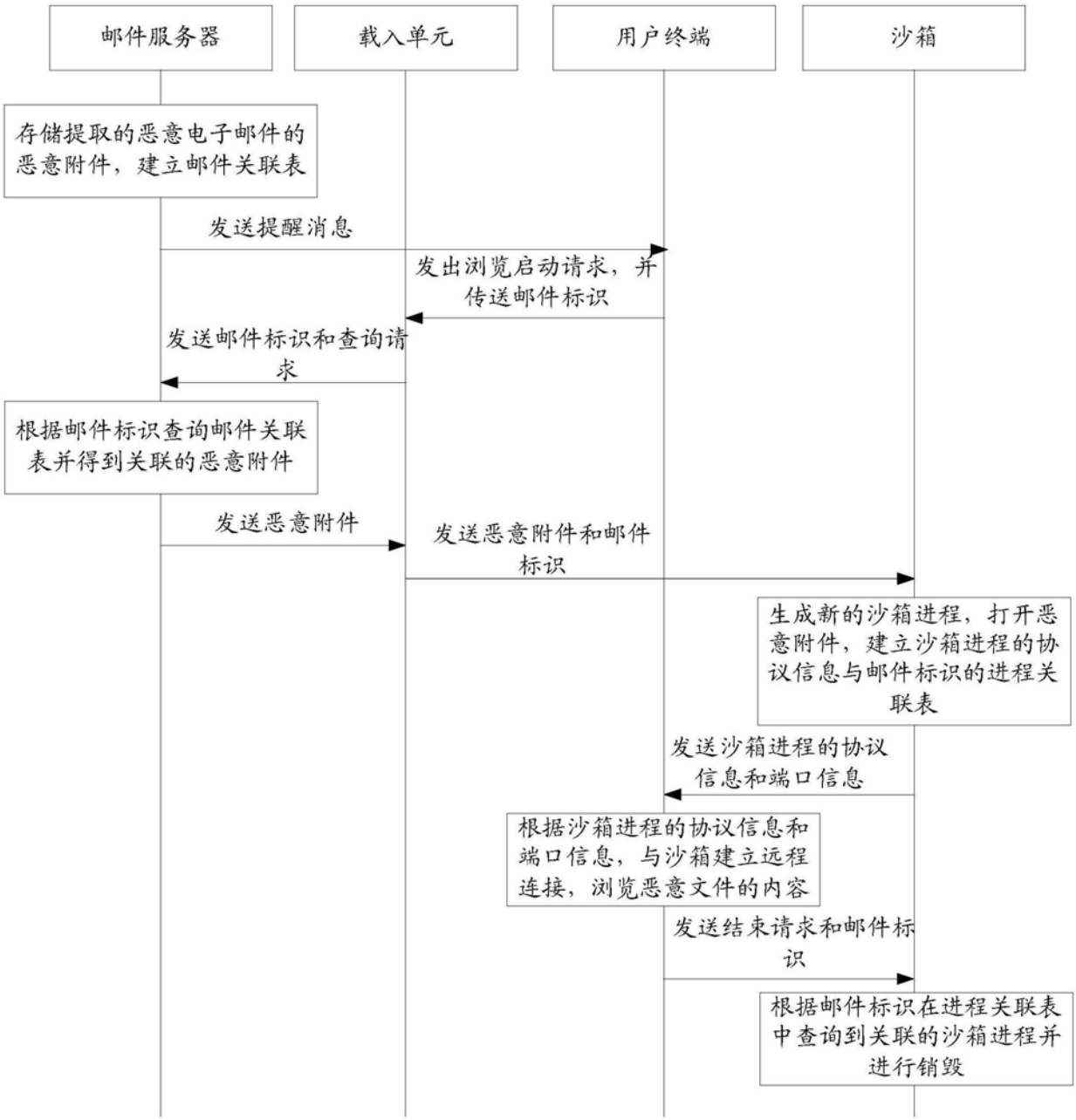

邮件服务器
载入单元
用户终端
沙箱
存储提取的恶意电子邮件的恶意附件，建立邮件关联表
发送提醒消息
发出浏览启动请求，并传送邮件标识
发送邮件标识和查询请求
根据邮件标识查询邮件关联表并得到关联的恶意附件
发送恶意附件
发送恶意附件和邮件标识
生成新的沙箱进程，打开恶意附件，建立沙箱进程的协议信息与邮件标识的进程关联表
发送沙箱进程的协议信息和端口信息
根据沙箱进程的协议信息和端口信息，与沙箱建立远程连接，浏览恶意文件的内容
发送结束请求和邮件标识
根据邮件标识在进程关联表中查询到关联的沙箱进程并进行销毁

图8

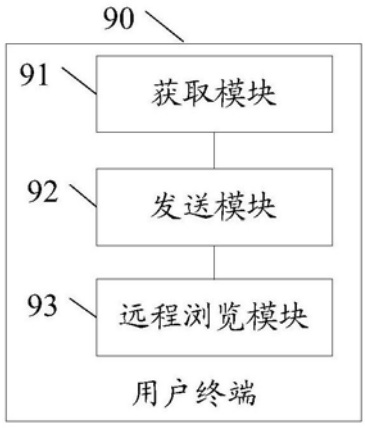

90
91
获取模块
92
发送模块
93
远程浏览模块
用户终端

图9

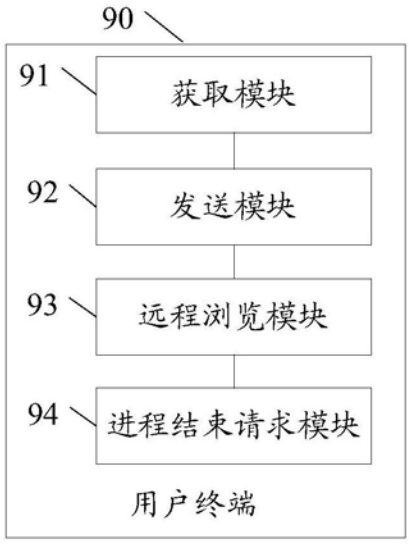

90
91
获取模块
92
发送模块
93
远程浏览模块
94
进程结束请求模块
用户终端

图10

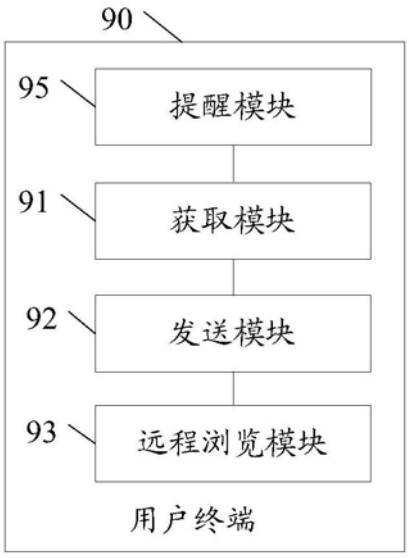

90
95
提醒模块
91
获取模块
92
发送模块
93
远程浏览模块
用户终端

图11


90
96
恶意邮件接收模块
97
邮件标记发送模块
91
获取模块
92
发送模块
93
远程浏览模块
用户终端

图12