(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 102819713 A
(43)申请公布日 2012.12.12

(21)申请号 201210226995.4

(22)申请日 2012.06.29

(71)申请人 北京奇虎科技有限公司
地址 100088 北京市西城区新街口外大街28号D座112室(德胜园区)
申请人 奇智软件(北京)有限公司

(72)发明人 付旻

(74)专利代理机构 北京润泽恒知识产权代理有限公司 11319
代理人 苏培华

(51)Int.Cl.
G06F 21/22(2006.01)

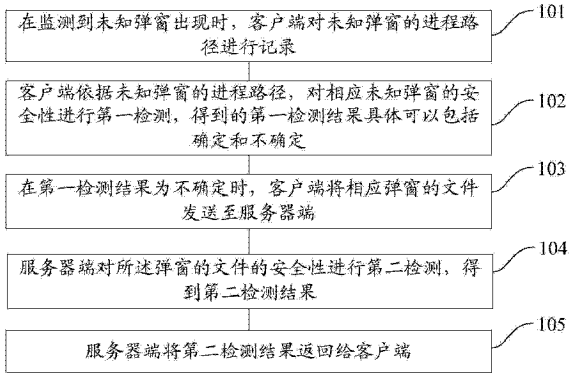
权利要求书 3 页 说明书 12 页 附图 3 页

(54)发明名称

一种检测弹窗安全性的方法和系统

(57)摘要

本申请提供了一种检测弹窗安全性的方法和系统，其中的方法具体包括：在监测到弹窗出现时，客户端对弹窗的进程路径进行记录；客户端依据弹窗的进程路径，对相应弹窗的安全性进行第一检测，在第一检测结果为不确定时，客户端将相应弹窗的文件发送至服务器端；服务器端对所述弹窗的文件的安全性进行第二检测，得到第二检测结果；服务器端将第二检测结果返回给客户端。本申请能够提高检测弹窗的准确性和及时性。



CN 102819713 A

1. 一种检测弹窗安全性的方法，其特征在于，包括：

在监测到弹窗出现时，客户端对弹窗的进程路径进行记录；

客户端依据弹窗的进程路径，对相应弹窗的安全性进行第一检测，在第一检测结果为不确定时，客户端将相应弹窗的文件发送至服务器端；

服务器端对所述弹窗的文件的安全性进行第二检测，得到第二检测结果；

服务器端将第二检测结果返回给客户端。

2. 如权利要求 1 所述的方法，其特征在于，所述客户端依据弹窗的进程路径，对相应弹窗的安全性进行第一检测的步骤，进一步包括：

客户端依据弹窗的进程路径，获取相应弹窗的文件；

判断所述弹窗的文件是否符合预置的信任度条件，若是，则得到确定的第一检测结果，否则，得到不确定的第一检测结果。

3. 如权利要求 2 所述的方法，其特征在于，所述判断所述弹窗的文件是否符合预置的信任度条件的步骤，进一步包括：

判断所述弹窗的进程文件的签名是否在可信签名列表中；和 / 或

判断所述弹窗的进程路径是否在用户白名单中。

4. 如权利要求 3 所述的方法，其特征在于，所述弹窗的进程包括弹窗的父进程和弹窗的进程；则所述弹窗的进程文件包括弹窗的父进程文件和进程本身文件；

所述判断所述弹窗的进程文件的签名是否在可信签名列表中的步骤，进一步包括：

判断所述弹窗的父进程文件的签名是否在第一可信签名列表中；和 / 或

判断所述弹窗的进程本身文件的签名是否在第二可信签名列表中。

5. 如权利要求 4 所述的方法，其特征在于，所述判断所述弹窗的文件是否符合预置的信任度条件的步骤，进一步包括：

判断所述弹窗的父进程文件的签名是否在第一可信签名列表中；

当所述弹窗的父进程文件的签名在第一可信签名列表中时，得到确定的第一检测结果；

当所述弹窗的父进程文件的签名不在第一可信签名列表中时，判断所述弹窗的进程路径是否在用户白名单中；

当所述弹窗的文件在用户白名单中时，得到确定的第一检测结果；

当所述弹窗的文件不在用户白名单中时，判断所述弹窗的进程本身文件的签名是否在第二可信签名列表中，若是，则得到确定的第一检测结果，否则得到不确定的第一检测结果。

6. 如权利要求 1 所述的方法，其特征在于，所述服务器端对所述弹窗的文件的安全性进行第二检测的步骤进一步包括：

对所述弹窗的文件的安全性进行分析，得到相应的第二检测结果。

7. 如权利要求 1 所述的方法，其特征在于，所述服务器端对所述弹窗的文件的安全性进行第二检测的步骤进一步包括：

在服务器端数据库的本地缓存中查询是否存在所述弹窗的文件；

在缓存命中成功时，将查询结果作为第二检测结果；

在缓存命中失败时，对所述弹窗的文件的安全性进行分析，得到相应的第二检测结果。

8. 如权利要求 6 或 7 所述的方法，其特征在于，所述对所述弹窗的文件的安全性进行分析的步骤，进一步包括：

将所述弹窗的文件信息与安全弹窗文件的信息进行匹配，若匹配成功，则判别所述弹窗的文件为安全；和 / 或

将所述弹窗的文件信息与病毒弹窗文件的信息进行匹配，若匹配成功，则判别所述弹窗的文件为不安全；

其中，所述文件信息包括如下信息中的一项或多项：文件内容的 MD5 值，文件的大小，文件最后修改时间，文件名称。

9. 如权利要求 1 至 7 中任一项所述的方法，其特征在于，所述确定的第一检测结果包括安全；

所述方法还包括：在第一检测结果为安全时，删除所记录的相应弹窗的进程路径。

10. 如权利要求 1 至 7 中任一项所述的方法，其特征在于，所述第二检测结果包括安全和不安全；

所述方法还包括：

在第二检测结果为安全时，客户端删除所记录的相应弹窗的进程路径；

在第二检测结果为不安全时，服务器端将相应弹窗的信息样本同步至所有客户端。

11. 一种检测弹窗安全性的系统，其特征在于，包括客户端和服务器端，其中

所述客户端包括：

记录模块，用于在监测到弹窗出现时，对弹窗的进程路径进行记录；

第一检测模块，用于依据弹窗的进程路径，对相应弹窗的安全性进行第一检测，得到的第一检测结果包括确定和不确定；及

上报模块，用于在第一检测结果为不确定时，将相应弹窗的文件发送至服务器端；

所述服务器端包括：

第二检测模块，用于对所述弹窗的文件的安全性进行第二检测，得到第二检测结果；及

返回模块，用于将第二检测结果返回给客户端。

12. 如权利要求 11 所述的系统，其特征在于，所述第一检测模块进一步包括：

文件获取子模块，用于依据弹窗的进程路径，获取相应弹窗的文件；及

信任度判断子模块，用于判断所述弹窗的文件是否符合预置的信任度条件，若是，则得到确定的第一检测结果，否则，得到不确定的第一检测结果。

13. 如权利要求 12 所述的系统，其特征在于，所述信任度判断子模块进一步包括：

签名判断单元，用于判断所述弹窗的进程文件的签名是否在可信签名列表中；和 / 或

用户白名单判断单元，用于判断所述弹窗的进程路径是否在用户白名单中。

14. 如权利要求 13 所述的系统，其特征在于，所述弹窗的进程包括弹窗的父进程和弹窗的进程；则所述弹窗的进程文件包括弹窗的父进程文件和进程本身文件；

所述签名判断单元进一步包括：

第一签名判断子单元，用于判断所述弹窗的父进程文件的签名是否在第一可信签名列表中；和 / 或

第二签名判断子单元，用于判断所述弹窗的进程文件的签名是否在第二可信签名列表中。

15. 如权利要求 14 所述的系统，其特征在于，所述信任度判断子模块进一步包括：

第一判断单元，用于判断所述弹窗的父进程文件的签名是否在第一可信签名列表中；

第一结果获取单元，用于当所述弹窗的父进程文件的签名在第一可信签名列表中时，得到确定的第一检测结果；

第二判断单元，用于当所述弹窗的父进程文件的签名不在第一可信签名列表中时，判断所述弹窗的进程路径是否在用户白名单中；

第二结果获取单元，用于当所述弹窗的文件在用户白名单中时，得到确定的第一检测结果；

第三判断单元，用于当所述弹窗的文件不在用户白名单中时，判断所述弹窗的进程本身文件的签名是否在第二可信签名列表中，若是，则得到确定的第一检测结果，否则得到不确定的第一检测结果。

16. 如权利要求 11 所述的系统，其特征在于，所述第二检测模块进一步包括：

分析子模块，用于对所述弹窗的文件的安全性进行分析，得到相应的第二检测结果。

17. 如权利要求 11 所述的系统，其特征在于，所述第二检测模块进一步包括：

缓存查询子模块，用于在服务器端数据库的本地缓存中查询是否存在所述弹窗的文件；

命中成功子模块，用于在缓存命中成功时，将查询结果作为第二检测结果；

命中失败子模块，用于在缓存命中失败时，对所述弹窗的文件的安全性进行分析，得到相应的第二检测结果。

18. 如权利要求 16 所述的系统，其特征在于，所述分析子模块进一步包括：

第一匹配子模块，用于将所述弹窗的文件信息与安全弹窗文件的信息进行匹配，若匹配成功，则判别所述弹窗的文件为安全；和 / 或

第二匹配子模块，用于将所述弹窗的文件信息与病毒弹窗文件的信息进行匹配，若匹配成功，则判别所述弹窗的文件为不安全；

其中，所述文件信息包括如下信息中的一项或多项：文件内容的 MD5 值，文件的大小，文件最后修改时间，文件名称。

19. 如权利要求 11 至 17 中任一项所述的系统，其特征在于，所述确定的第一检测结果包括安全；

所述客户端还包括：

第一删除模块，用于在第一检测结果为安全时，删除所记录的相应弹窗的进程路径。

20. 如权利要求 11 至 17 中任一项所述的系统，其特征在于，所述第二检测结果包括安全和不安全；

所述客户端还包括：

第二删除模块，用于在第二检测结果为安全时，客户端删除所记录的相应弹窗的进程路径；

所述服务器端还包括：

同步模块，用于在第二检测结果为不安全时，服务器端将相应弹窗的信息样本同步至所有客户端。

一种检测弹窗安全性的方法和系统

技术领域

[0001] 本申请涉及计算机安全技术领域，特别是涉及一种检测弹窗安全性的方法和系统。

背景技术

[0002] 目前，随着互联网技术的迅猛发展，计算机在社会生活各个领域中得到了广泛的应用，计算机网络给用户的生活工作带来了不可估量的帮助；但是，计算机网络上传播的信息姿态不一、错综复杂，既容易引发病毒感染、病毒攻击等计算机安全问题，又容易干扰用户正常的生活工作。

[0003] 近来，一些软件程序（如 QQ、MSN、飞信、迅雷、优酷、千千静听等）通过弹窗传播信息，已成为一种流行趋势。用户在使用上述软件程序的过程中，几乎每隔半小时就有弹窗出现在屏幕的右下角。

[0004] 有些弹窗（如新闻弹窗、商品广告弹窗）带有无害信息，但会干扰用户正常的生活工作，因为用户需要通过单击弹窗上的命令按钮去关闭该弹窗。但是，另外一些弹窗（如游戏弹窗、黄色弹窗）可能隐藏有害信息，如果用户不小心点击了弹窗，则可能引发病毒感染、病毒攻击等计算机安全问题。

[0005] 针对上述干扰问题和计算机安全问题，现有技术具有两种检测弹窗的方案：

[0006] 现有技术 1、

[0007] 用户基于人工操作，判断某个弹窗是否是其需要的，如果不需要，则手动禁止该弹窗对应的进程或者删除该弹窗对应的文件；现有技术 1 需要用户具有一定的电脑知识去获取弹窗对应的进程或文件，且其使用的主观判断不一定保证真正具有威胁的弹窗被处理掉。

[0008] 现有技术 2、

[0009] 使用防病毒软件扫描用户计算机的磁盘文件，并基于磁盘文件与客户端本地病毒特征库中病毒样本进行匹配的方式，判断某个磁盘文件是否对应于弹窗的病毒样本，若是，则处理掉该磁盘文件；通常只有病毒被人工发现并升级病毒库后才可以检测出该病毒，在某种程度上防病毒软件总是落后于病毒的发展，因此，防病毒软件升级的滞后性容易导致恶意弹窗不能被及时检测出。

[0010] 总之，需要本领域技术人员迫切解决的一个技术问题就是：如何能够提高检测弹窗的准确性和及时性。

发明内容

[0011] 本申请所要解决的技术问题是提供一种检测弹窗安全性的方法和系统，能够提高检测弹窗的准确性和及时性。

[0012] 为了解决上述问题，本申请公开了一种检测弹窗安全性的方法，包括：

[0013] 在监测到弹窗出现时，客户端对弹窗的进程路径进行记录；

[0014] 客户端依据弹窗的进程路径，对相应弹窗的安全性进行第一检测，在第一检测结果为不确定时，客户端将相应弹窗的文件发送至服务器端；

[0015] 服务器端对所述弹窗的文件的安全性进行第二检测，得到第二检测结果；

[0016] 服务器端将第二检测结果返回给客户端。

[0017] 优选的，所述客户端依据弹窗的进程路径，对相应弹窗的安全性进行第一检测的步骤，进一步包括：

[0018] 客户端依据弹窗的进程路径，获取相应弹窗的文件；

[0019] 判断所述弹窗的文件是否符合预置的信任度条件，若是，则得到确定的第一检测结果，否则，得到不确定的第一检测结果。

[0020] 优选的，所述判断所述弹窗的文件是否符合预置的信任度条件的步骤，进一步包括：

[0021] 判断所述弹窗的进程文件的签名是否在可信签名列表中；和 / 或

[0022] 判断所述弹窗的进程路径是否在用户白名单中。

[0023] 优选的，所述弹窗的进程包括弹窗的父进程和弹窗的进程；则所述弹窗的进程文件包括弹窗的父进程文件和进程本身文件；

[0024] 所述判断所述弹窗的进程文件的签名是否在可信签名列表中的步骤，进一步包括：

[0025] 判断所述弹窗的父进程文件的签名是否在第一可信签名列表中；和 / 或

[0026] 判断所述弹窗的进程本身文件的签名是否在第二可信签名列表中。

[0027] 优选的，所述判断所述弹窗的文件是否符合预置的信任度条件的步骤，进一步包括：

[0028] 判断所述弹窗的父进程文件的签名是否在第一可信签名列表中；

[0029] 当所述弹窗的父进程文件的签名在第一可信签名列表中时，得到确定的第一检测结果；

[0030] 当所述弹窗的父进程文件的签名不在第一可信签名列表中时，判断所述弹窗的进程路径是否在用户白名单中；

[0031] 当所述弹窗的文件在用户白名单中时，得到确定的第一检测结果；

[0032] 当所述弹窗的文件不在用户白名单中时，判断所述弹窗的进程本身文件的签名是否在第二可信签名列表中，若是，则得到确定的第一检测结果，否则得到不确定的第一检测结果。

[0033] 优选的，所述服务器端对所述弹窗的文件的安全性进行第二检测的步骤进一步包括：

[0034] 对所述弹窗的文件的安全性进行分析，得到相应的第二检测结果。

[0035] 优选的，所述服务器端对所述弹窗的文件的安全性进行第二检测的步骤进一步包括：

[0036] 在服务器端数据库的本地缓存中查询是否存在所述弹窗的文件；

[0037] 在缓存命中成功时，将查询结果作为第二检测结果；

[0038] 在缓存命中失败时，对所述弹窗的文件的安全性进行分析，得到相应的第二检测结果。

[0039] 优选的，所述对所述弹窗的文件的安全性进行分析的步骤，进一步包括：

[0040] 将所述弹窗的文件信息与安全弹窗文件的信息进行匹配，若匹配成功，则判别所述弹窗的文件为安全；和 / 或

[0041] 将所述弹窗的文件信息与病毒弹窗文件的信息进行匹配，若匹配成功，则判别所述弹窗的文件为不安全；

[0042] 其中，所述文件信息包括如下信息中的一项或多项：文件内容的 MD5 值，文件的大小，文件最后修改时间，文件名称。

[0043] 优选的，所述确定的第一检测结果包括安全；

[0044] 所述方法还包括：在第一检测结果为安全时，删除所记录的相应弹窗的进程路径。

[0045] 优选的，所述第二检测结果包括安全和不安全；

[0046] 所述方法还包括：

[0047] 在第二检测结果为安全时，客户端删除所记录的相应弹窗的进程路径；

[0048] 在第二检测结果为不安全时，服务器端将相应弹窗的信息样本同步至所有客户端。

[0049] 另一方面，本申请还公开了一种检测弹窗安全性的系统，其包括客户端和服务器端，其中

[0050] 所述客户端包括：

[0051] 记录模块，用于在监测到弹窗出现时，对弹窗的进程路径进行记录；

[0052] 第一检测模块，用于依据弹窗的进程路径，对相应弹窗的安全性进行第一检测，得到的第一检测结果包括确定和不确定；及

[0053] 上报模块，用于在第一检测结果为不确定时，将相应弹窗的文件发送至服务器端；

[0054] 所述服务器端包括：

[0055] 第二检测模块，用于对所述弹窗的文件的安全性进行第二检测，得到第二检测结果；及

[0056] 返回模块，用于将第二检测结果返回给客户端。

[0057] 优选的，所述第一检测模块进一步包括：

[0058] 文件获取子模块，用于依据弹窗的进程路径，获取相应弹窗的文件；及

[0059] 信任度判断子模块，用于判断所述弹窗的文件是否符合预置的信任度条件，若是，则得到确定的第一检测结果，否则，得到不确定的第一检测结果。

[0060] 优选的，所述信任度判断子模块进一步包括：

[0061] 签名判断单元，用于判断所述弹窗的进程文件的签名是否在可信签名列表中；和 / 或

[0062] 用户白名单判断单元，用于判断所述弹窗的进程路径是否在用户白名单中。

[0063] 优选的，所述弹窗的进程包括弹窗的父进程和弹窗的进程；则所述弹窗的进程文件包括弹窗的父进程文件和进程本身文件；

[0064] 所述签名判断单元进一步包括：

[0065] 第一签名判断子单元，用于判断所述弹窗的父进程文件的签名是否在第一可信签名列表中；和 / 或

[0066] 第二签名判断子单元，用于判断所述弹窗的进程文件的签名是否在第二可信签名列表中。

[0067] 优选的，所述信任度判断子模块进一步包括：

[0068] 第一判断单元，用于判断所述弹窗的父进程文件的签名是否在第一可信签名列表中；

[0069] 第一结果获取单元，用于当所述弹窗的父进程文件的签名在第一可信签名列表中时，得到确定的第一检测结果；

[0070] 第二判断单元，用于当所述弹窗的父进程文件的签名不在第一可信签名列表中时，判断所述弹窗的进程路径是否在用户白名单中；

[0071] 第二结果获取单元，用于当所述弹窗的文件在用户白名单中时，得到确定的第一检测结果；

[0072] 第三判断单元，用于当所述弹窗的文件不在用户白名单中时，判断所述弹窗的进程本身文件的签名是否在第二可信签名列表中，若是，则得到确定的第一检测结果，否则得到不确定的第一检测结果。

[0073] 优选的，所述第二检测模块进一步包括：

[0074] 分析子模块，用于对所述弹窗的文件的安全性进行分析，得到相应的第二检测结果。

[0075] 优选的，所述第二检测模块进一步包括：

[0076] 缓存查询子模块，用于在服务器端数据库的本地缓存中查询是否存在所述弹窗的文件；

[0077] 命中成功子模块，用于在缓存命中成功时，将查询结果作为第二检测结果；

[0078] 命中失败子模块，用于在缓存命中失败时，对所述弹窗的文件的安全性进行分析，得到相应的第二检测结果。

[0079] 优选的，所述分析子模块进一步包括：

[0080] 第一匹配子模块，用于将所述弹窗的文件信息与安全弹窗文件的信息进行匹配，若匹配成功，则判别所述弹窗的文件为安全；和 / 或

[0081] 第二匹配子模块，用于将所述弹窗的文件信息与病毒弹窗文件的信息进行匹配，若匹配成功，则判别所述弹窗的文件为不安全；

[0082] 其中，所述文件信息包括如下信息中的一项或多项：文件内容的 MD5 值，文件的大小，文件最后修改时间，文件名称。

[0083] 优选的，所述确定的第一检测结果包括安全；

[0084] 则所述客户端还包括：

[0085] 第一删除模块，用于在第一检测结果为安全时，删除所记录的相应弹窗的进程路径。

[0086] 优选的，所述第二检测结果包括安全和不安全；

[0087] 则所述客户端还包括：

[0088] 第二删除模块，用于在第二检测结果为安全时，客户端删除所记录的相应弹窗的进程路径；

[0089] 所述服务器端还包括：

[0090] 同步模块，用于在第二检测结果为不安全时，服务器端将相应弹窗的信息样本同步至所有客户端。

[0091] 与现有技术相比，本申请具有以下优点：

[0092] 本申请在客户端对弹窗的进程路径进行自动记录，并依据弹窗的进程路径分别在客户端和服务器端对相应弹窗的安全性进行第一检测和第二检测；这样，在客户端本地病毒特征库中病毒样本的滞后性等原因导致第一检测结果为不确定时，一方面本申请在服务器端的第二检测为利用成千上百的服务器进行的智能检测，另一方面本申请在服务器端的第二检测能够及时聚集大部分客户端上报的病毒样本和信任度条件；更重要的是，由于服务器端的安全性检测是联网进行的，其能够有效克服客户端本地病毒特征库的滞后性，提高安全性检测的及时性和准确性。

附图说明

[0093] 图 1 是本申请一种检测弹窗安全性的方法实施例的流程图；

[0094] 图 2 是本申请一种检测弹窗安全性的示例流程；

[0095] 图 3 是本申请一种检测弹窗安全性的系统实施例的结构图。

具体实施方式

[0096] 为使本申请的上述目的、特征和优点能够更加明显易懂，下面结合附图和具体实施方式对本申请作进一步详细的说明。

[0097] 参照图 1，其示出了本申请一种检测弹窗安全性的方法实施例的流程图，具体可以包括：

[0098] 步骤 101、在监测到弹窗出现时，客户端对弹窗的进程路径进行记录；

[0099] 步骤 102、客户端依据弹窗的进程路径，对相应弹窗的安全性进行第一检测，得到的第一检测结果具体可以包括确定和不确定；

[0100] 步骤 103、在第一检测结果为不确定时，客户端将相应弹窗的文件发送至服务器端；

[0101] 步骤 104、服务器端对所述弹窗的文件的安全性进行第二检测，得到第二检测结果；

[0102] 步骤 105、服务器端将第二检测结果返回给客户端。

[0103] 本申请提供了一种自动检测弹窗安全性的方案，该方案在客户端对弹窗的进程路径进行自动记录，并依据弹窗的进程路径分别在客户端和服务器端对相应弹窗的安全性进行第一检测和第二检测；这样，在客户端本地病毒特征库中病毒样本的滞后性等原因导致第一检测结果为不确定时，一方面本申请在服务器端的第二检测为利用成千上百的服务器进行的智能检测，另一方面本申请在服务器端的第二检测能够及时聚集大部分客户端的病毒样本，故相对于现有技术，能够提高检测弹窗的准确性和及时性。

[0104] 在实际应用中，当用户桌面的右下角出现符合预置窗口大小的弹窗时，可将该弹窗当成弹窗，则步骤 101 会自动记录该弹窗的进程路径；通常，所述弹窗的进程就是弹窗本身的进程；在某些情况下，所述弹窗的进程还可以包括弹窗的父进程。

[0105] 需要说明的是，本申请对弹窗的种类不加以限制，其可以是新闻弹窗、商品广告弹

窗，也可以是游戏弹窗、黄色弹窗等等。

[0106] 在本申请的一种应用示例中，可以针对广告弹窗，设置所述预置窗口大小的取值范围为：小于等于 600*400，此时，可以将小于等于 600*400 的窗口作为广告弹窗来处理。

[0107] 可以理解，600*400 的窗口只是作为广告弹窗的一种预置窗口大小的示例，实际上，本领域技术人员可以根据实际情况设置广告弹窗的其它预置窗口大小，或者，设置其它种类广告弹窗的预置窗口大小。

[0108] 在本申请的一种应用示例中，所述获取该弹窗对应的进程路径的过程具体可以包括：获取该弹窗的句柄；调用 API（应用程序编程接口，Application Programming Interface）取得该弹窗的句柄所在的进程 ID（Identity）；通过进程 ID，获取对应的程序文件；获取该程序文件的路径，作为该弹窗对应的进程路径。

[0109] 其中，一种依据窗口句柄获得所在进程 ID 的 API 示例为

[0110] DWORD GetWindowThreadProcessId(

[0111] HWND hWnd,

[0112] LPDWORD lpdwProcessId)

[0113] 其中，hWnd 为窗口句柄，lpdwProcessId 为一个接受返回进程 ID 的 Long 变量。

[0114] 为了增加操作的便利性，在本申请的一种优选实施例中，可以将弹窗的进程路径记录至一个特定文件中，这样，在检测弹窗安全性的过程中，可以加载该特定文件，并从中逐条读取弹窗的进程路径即可。

[0115] 本申请的步骤 102 可以依据用户操作启动，也可以自行启动。其中，依据用户操作启动的一个例子是，在用户点击防病毒软件上的全盘扫描或者快速扫描按钮时启动步骤 102；自行启动的一个例子是提供用户设置检测周期的一个接口，在检测周期达到时即行启动步骤 102，所述检测周期可以按小时设置或者按天设置等等；自行启动的另一个例子是，在监测到弹窗出现的次数达到预置次数时即行启动步骤 102 等等。总之，本申请对具体的步骤 102 的执行时机不加以限制。

[0116] 本申请可以提供如下对相应弹窗的安全性进行第一检测的方案：

[0117] 方案 A1、

[0118] 方案 A1 可以类似于现有技术 2，具体的流程如下：

[0119] 步骤 A11、依据弹窗的进程路径，获取相应弹窗的文件；

[0120] 步骤 A12、基于文件与客户端本地病毒特征库中病毒样本进行匹配的方式，判断所述弹窗的文件是否对应于弹窗的病毒样本，若是，则认定所述弹窗的文件不安全，将其上报到服务器，并在客户端将其作为病毒进行处理；若否，则认定所述弹窗的文件的第一检测结果为不确定。

[0121] 方案 A2、

[0122] 方案 A1 得到的第一检测结果需要依赖于客户端本地病毒特征库中病毒样本的容量。在容量小的情况下，步骤 A12 很容易匹配不成功以致得到不确定的第一检测结果；在容量大的情况下，则步骤 A12 匹配操作所占用的计算机资源较多，且会花费较多的时间，故容易增加第一检测的时间，影响第一检测的效率。

[0123] 方案 A2 通过判断所述弹窗的文件是否符合预置的信任度条件来进行第一检测，所述预置的信任度条件可由用户设置得到，或者，可由客户端预先分析统计得到，或者，可

由服务器收集众多客户端或用户的预置的信任度条件，并同步到客户端得到；方案 A2 依据大多数客户端或用户预置的信任度条件快速检测所述弹窗的文件的安全性，其能够将符合预置的信任度条件的弹窗的文件的第一检测结果判别为确定，将不符合预置的信任度条件的弹窗的文件的第一检测结果判别为不确定；因此，相对于方案 A1，由于方案 A2 充分考虑了客户端、服务器端或用户预置的信任度条件，既能够增加用户对第一检测结果的信任度，又能够有效提高第一检测的效率。

[0124] 方案 A2 涉及的流程具体可以包括：

[0125] 步骤 A21、依据弹窗的进程路径，获取相应弹窗的文件；

[0126] 步骤 A22、判断所述弹窗的文件是否符合预置的信任度条件，若是，则得到确定的第一检测结果，否则，得到不确定的第一检测结果。

[0127] 在本申请的一种优选实施例中，所述判断所述弹窗的文件是否符合预置的信任度条件的步骤 A22 可以进一步包括：

[0128] 步骤 A221、判断所述弹窗的进程文件的签名是否在可信签名列表中；和 / 或

[0129] 步骤 A222、判断所述弹窗的进程路径是否在用户白名单中。

[0130] 其中，所述可信签名列表中存储有可信文件的签名，其配置在本地客户端；在实际中，可由客户端预先分析统计得到，或者，可由服务器收集众多客户端的可信签名列表，并同步到客户端得到；

[0131] 用户白名单可用于表示用户指定的用户自身确定的无威胁的文件或者目录（目录中的所有文件均认为用户信任），在扫描或者监控的过程中不会报出，无视扫描结果；用户白名单可由客户端用户设置得到，或者，可由服务器收集众多客户端的用户白名单，并同步到客户端得到；所述用户白名单既可以包括文件及目录，又可由包括文件扩展名，例如，用户可由将文本文件的扩展名“.txt”、图片文件的扩展名“.jpg/.bmp”放至白名单中，也可以将一个具体的文本文件及目录放至白名单中。

[0132] 需要说明的是，本领域技术人员可以根据实际需要，使用步骤 A221 和步骤 A222 中的一者或多者，本申请对此不加以限制。

[0133] 在本申请的一种优选实施例中，所述弹窗的进程可以进一步包括弹窗的父进程和弹窗的进程；则所述弹窗的进程文件可以进一步包括弹窗的父进程文件和进程本身文件；

[0134] 则所述步骤 A221 判断所述弹窗的进程文件的签名是否在可信签名列表中的步骤，可以进一步包括：

[0135] 判断所述弹窗的父进程文件的签名是否在第一可信签名列表中；和 / 或

[0136] 判断所述弹窗的进程文件的签名是否在第二可信签名列表中。

[0137] 在具体实现中，本领域技术人员可以根据实际情况配置第一可信签名列表，本申请对具体的配置方式不加以限制。

[0138] 在本申请的另一种优选实施例中，所述判断所述弹窗的文件是否符合预置的信任度条件的步骤，可以进一步包括：

[0139] 步骤 B1、判断所述弹窗的父进程文件的签名是否在第一可信签名列表中；

[0140] 步骤 B2、当所述弹窗的父进程文件的签名在第一可信签名列表中时，得到确定的第一检测结果；

[0141] 步骤 B3、当所述弹窗的父进程文件的签名不在第一可信签名列表中时，判断所述

弹窗的进程路径是否在用户白名单中；

[0142] 步骤 B4、当所述弹窗的文件在用户白名单中时，得到确定的第一检测结果；

[0143] 步骤 B5、当所述弹窗的文件不在用户白名单中时，判断所述弹窗的进程本身文件的签名是否在第二可信签名列表中，若是，则得到确定的第一检测结果，否则得到不确定的第一检测结果。

[0144] 在实际应用中，所述确定的第一检测结果具体可以包括安全的结果；则所述方法还可以包括：在第一检测结果为安全时，删除所记录的相应弹窗的进程路径。如果采用特定文件记录弹窗的进程路径，则在特定文件中删除安全的弹窗对应的进程路径条目即可。

[0145] 当然，所述确定的第一检测结果还可以包括不安全的结果，在处理时，客户端可以强制结束掉对应的活动进程并且删除掉进程对应的文件。

[0146] 本申请可以提供如下对所述弹窗的文件的安全性进行第二检测的方案：

[0147] 方案 C1、

[0148] 所述服务器端对所述弹窗的文件的安全性进行第二检测的步骤可以进一步包括：对所述弹窗的文件的安全性进行分析，得到相应的第二检测结果。

[0149] 服务器端可以利用成千上百的服务器智能检测所述弹窗的文件的安全性，相对于客户端的安全性检测，服务器端的安全性检测能够降低客户端本地病毒特征库升级的频率，降低客户端检测所占用的机器资源，其可以有效减小客户端本地病毒特征库的容量；更重要的是，由于服务器端的安全性检测是联网进行的，其能够有效克服客户端本地病毒特征库的滞后性，提高安全性检测的及时性和准确性。

[0150] 需要说明的是，服务器端的安全性检测可以包括特征匹配的检测方法，也可以利用系统白名单或用户白名单进行检测，还可以使用可信签名列表进行检测，还可以采用行为判断、云查杀等各种检测方式，总之本申请对具体的服务器端的安全性的检测方法不加以限制。

[0151] 在本申请的一种优选实施例中，所述对所述弹窗的文件的安全性进行分析的步骤，可以进一步包括：

[0152] 步骤 C11、将所述弹窗的文件信息与安全弹窗文件的信息进行匹配，若匹配成功，则判别所述弹窗的文件为安全；和 / 或

[0153] 步骤 C12、将所述弹窗的文件信息与病毒弹窗文件的信息进行匹配，若匹配成功，则判别所述弹窗的文件为不安全；

[0154] 其中，所述文件信息具体可以包括如下信息中的一项或多项：文件内容的 MD5（消息摘要算法第五版，Message Digest Algorithm）值，文件的大小，文件最后修改时间，文件名称。

[0155] 本优选实施例中基于文件认证的原理对所述弹窗的文件的安全性进行分析；在实际应用中，病毒弹窗文件为已确认为不安全的弹窗文件，安全弹窗文件为已确认为安全的弹窗文件，病毒弹窗文件和安全弹窗文件均可通过收集得到。

[0156] 方案 C2、

[0157] 所述服务器端对所述弹窗的文件的安全性进行第二检测的步骤可以进一步包括：

[0158] 步骤 C21、在服务器端数据库的本地缓存中查询是否存在所述弹窗的文件；

[0159] 步骤 C22、在缓存命中成功时，将查询结果作为第二检测结果；

[0160] 步骤 C23、在缓存命中失败时，对所述弹窗的文件的安全性进行分析，得到相应的第二检测结果。

[0161] 相对于客户端本地病毒特征库，服务器端数据库的升级频率高一些；故在接收到客户端上报的弹窗的文件时，可以首先去服务器端数据库中查询；这样，服务器端服务器的本地缓存中临时存储有弹窗的文件及相应的查询结果；这样，在缓存命中成功时，直接得到第二检测结果，就能够有效节省服务器端联网检测所占用的服务器端服务器的机器资源。

[0162] 当然，对所述弹窗的文件的安全性进行第二检测的方案还可以包括依据所述弹窗的文件在服务器端数据库中查询的方案，本申请对具体的对所述弹窗的文件的安全性进行第二检测的方案不加以限制。

[0163] 在本申请的一种优选实施例中，所述第二检测结果具体可以包括安全和不安全；

[0164] 则所述方法还可以包括：

[0165] 在第二检测结果为安全时，客户端删除所记录的相应弹窗的进程路径；

[0166] 在第二检测结果为不安全时，服务器端将相应弹窗的信息样本同步至所有客户端。

[0167] 通常，可以将弹窗的文件直接作为相应弹窗的信息样本；或者，对弹窗的文件进行分析得到相应的特征码，作为相应弹窗的信息样本。总之，本申请对相应的依据弹窗的文件得到弹窗的信息样本的方法不加以限制。

[0168] 在处理不安全的第二检测结果时，客户端可以强制结束掉对应的活动进程并且删除掉进程对应的文件。

[0169] 需要说明的是，客户端均可以将确定的第一检测结果，及第二检测结果展示给用户，由用户进行处理。

[0170] 为使本领域技术人员更好地理解本申请，以下通过图 2 说明本申请一种检测弹窗安全性的示例流程，具体可以包括：

[0171] 步骤 201、用户桌面的右下角出现预置窗口大小的弹窗时，客户端自动记录该弹窗的进程路径至 popwnd.dat 文件；

[0172] 步骤 202、用户点击防病毒软件上的“快速扫描”按钮时，客户端加载 popwnd.dat 文件，并从中逐条读取弹窗的进程路径；

[0173] 步骤 203、客户端针对读取的弹窗的进程路径，获取相应弹窗的父进程文件和进程文件；

[0174] 通常，相应弹窗的文件也即弹窗程序的文件，其通常为 PE(Portable Executable) 文件，其为二进制文件格式。

[0175] 步骤 204、客户端判断所述弹窗的父进程文件的签名是否在第一可信签名列表中，若是，则执行步骤 205，否则执行步骤 206；

[0176] 步骤 205、客户端得到确定的第一检测结果；

[0177] 步骤 206、客户端判断所述弹窗的进程路径是否在用户白名单中，若是，则执行步骤 205，否则执行步骤 207；

[0178] 步骤 207、客户端判断所述弹窗的进程本身文件的签名是否在第二可信签名列表中，若是，则执行步骤 205，否则执行步骤 208；

[0179] 步骤 208、客户端得到不确定的第一检测结果，并将相应弹窗的文件发送至服务器端；

[0180] 步骤 209、在服务器端数据库的本地缓存中查询是否存在所述弹窗的文件，若是，则执行步骤 210，否则，执行步骤 211；

[0181] 步骤 210、在缓存命中成功时，将查询结果作为第二检测结果；

[0182] 步骤 211、在缓存命中失败时，对所述弹窗的文件的安全性进行分析，得到相应的第二检测结果；

[0183] 步骤 212、服务器端将第二检测结果返回给客户端。

[0184] 与前述方法实施例相应，本申请还公开了一种检测弹窗安全性的系统实施例，参照图 3 所示的结构图，其具体可以包括客户端 301 和服务器端 302，其中

[0185] 所述客户端 301 具体可以包括：

[0186] 记录模块 311，用于在监测到弹窗出现时，对弹窗的进程路径进行记录；

[0187] 第一检测模块 312，用于依据弹窗的进程路径，对相应弹窗的安全性进行第一检测，得到的第一检测结果包括确定和不确定；及

[0188] 上报模块 313，用于在第一检测结果为不确定时，将相应弹窗的文件发送至服务器端；

[0189] 所述服务器端 302 具体可以包括：

[0190] 第二检测模块 321，用于对所述弹窗的文件的安全性进行第二检测，得到第二检测结果；及

[0191] 返回模块 322，用于将第二检测结果返回给客户端。

[0192] 在本申请的一种优选实施例中，所述第一检测模块 312 可以进一步包括：

[0193] 文件获取子模块，用于依据弹窗的进程路径，获取相应弹窗的文件；及

[0194] 信任度判断子模块，用于判断所述弹窗的文件是否符合预置的信任度条件，若是，则得到确定的第一检测结果，否则，得到不确定的第一检测结果。

[0195] 在本申请的另一种优选实施例中，所述信任度判断子模块可以进一步包括：

[0196] 签名判断单元，用于判断所述弹窗的进程文件的签名是否在可信签名列表中；和 / 或

[0197] 用户白名单判断单元，用于判断所述弹窗的进程路径是否在用户白名单中。

[0198] 在本申请的一种优选实施例中，所述弹窗的进程可以进一步包括弹窗的父进程和弹窗的进程；则所述弹窗的进程文件可以进一步包括弹窗的父进程文件和进程本身文件；

[0199] 则所述签名判断单元可以进一步包括：

[0200] 第一签名判断子单元，用于判断所述弹窗的父进程文件的签名是否在第一可信签名列表中；和 / 或

[0201] 第二签名判断子单元，用于判断所述弹窗的进程本身文件的签名是否在第二可信签名列表中。

[0202] 在本申请的另一种优选实施例中，所述信任度判断子模块可以进一步包括：

[0203] 第一判断单元，用于判断所述弹窗的父进程文件的签名是否在第一可信签名列表中；

[0204] 第一结果获取单元，用于当所述弹窗的父进程文件的签名在第一可信签名列表中

时，得到确定的第一检测结果；

[0205] 第二判断单元，用于当所述弹窗的父进程文件的签名不在第一可信签名列表中时，判断所述弹窗的进程路径是否在用户白名单中；

[0206] 第二结果获取单元，用于当所述弹窗的文件在用户白名单中时，得到确定的第一检测结果；

[0207] 第三判断单元，用于当所述弹窗的文件不在用户白名单中时，判断所述弹窗的进程本身文件的签名是否在第二可信签名列表中，若是，则得到确定的第一检测结果，否则得到不确定的第一检测结果。

[0208] 在本申请的一种优选实施例中，所述第二检测模块 321 可以进一步包括：

[0209] 分析子模块，用于对所述弹窗的文件的安全性进行分析，得到相应的第二检测结果。

[0210] 在本申请的一种优选实施例中，所述分析子模块可以进一步包括：

[0211] 第一匹配子模块，用于将所述弹窗的文件信息与安全弹窗文件的信息进行匹配，若匹配成功，则判别所述弹窗的文件为安全；和 / 或

[0212] 第二匹配子模块，用于将所述弹窗的文件信息与病毒弹窗文件的信息进行匹配，若匹配成功，则判别所述弹窗的文件为不安全；

[0213] 其中，所述文件信息包括如下信息中的一项或多项：文件内容的 MD5 值，文件的大小，文件最后修改时间，文件名称。

[0214] 在本申请的另一种优选实施例中，所述第二检测模块 321 可以进一步包括：

[0215] 缓存查询子模块，用于在服务器端数据库的本地缓存中查询是否存在所述弹窗的文件；

[0216] 命中成功子模块，用于在缓存命中成功时，将查询结果作为第二检测结果；

[0217] 命中失败子模块，用于在缓存命中失败时，对所述弹窗的文件的安全性进行分析，得到相应的第二检测结果。

[0218] 在本申请的再一种优选实施例中，所述确定的第一检测结果包括安全；

[0219] 则所述客户端 301 还可以包括：

[0220] 第一删除模块，用于在第一检测结果为安全时，删除所记录的相应弹窗的进程路径。

[0221] 在本申请的一种优选实施例中，所述第二检测结果具体可以包括安全和不安全；

[0222] 则所述客户端 301 还可以包括：

[0223] 第二删除模块，用于在第二检测结果为安全时，客户端删除所记录的相应弹窗的进程路径；

[0224] 所述服务器端 302 还可以包括：

[0225] 同步模块，用于在第二检测结果为不安全时，服务器端将相应弹窗的信息样本同步至所有客户端。

[0226] 本说明书中的各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。对于系统实施例而言，由于其与方法实施例基本相似，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。

[0227] 本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

[0228] 本申请是参照根据本申请实施例的方法、设备（系统）、和计算机程序产品的流程图和／或方框图来描述的。应理解可由计算机程序指令实现流程图和／或方框图中的每一流程和／或方框、以及流程图和／或方框图中的流程和／或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的装置。

[0229] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能。

[0230] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的步骤。

[0231] 尽管已描述了本申请的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例做出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本申请范围的所有变更和修改。

[0232] 以上对本申请所提供的一种检测弹窗安全性的方法和系统，进行了详细介绍，本文中应用了具体个例对本申请的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本申请的方法及其核心思想；同时，对于本领域的一般技术人员，依据本申请的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本申请的限制。

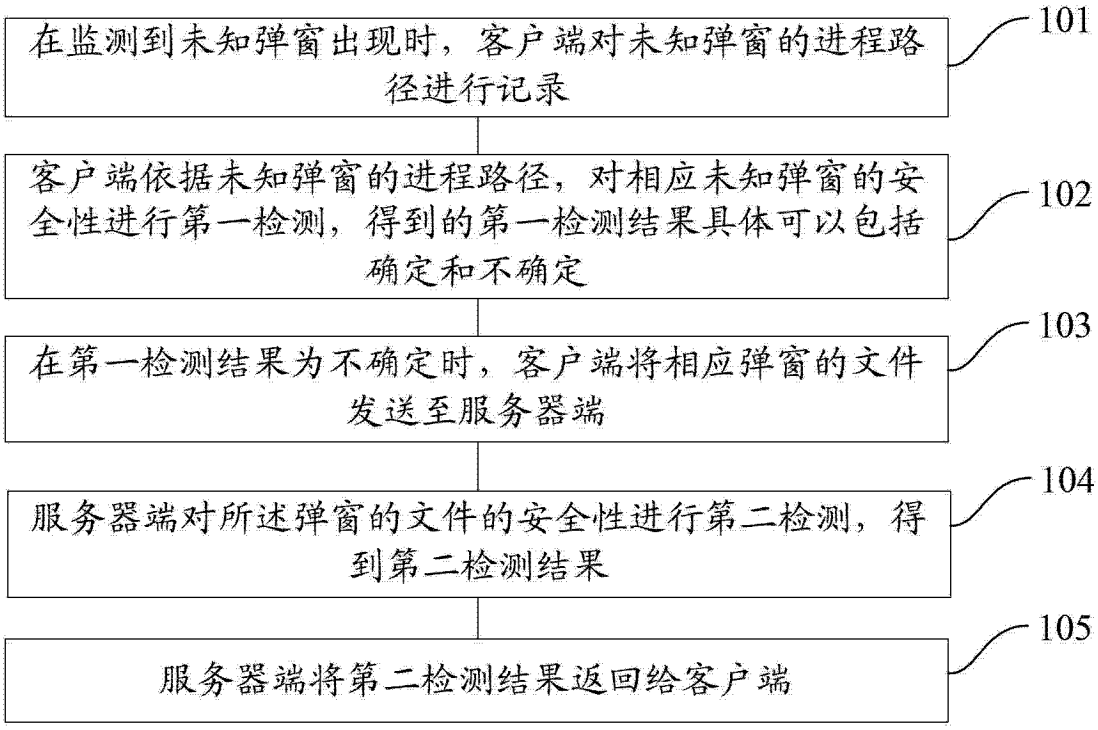

在监测到未知弹窗出现时，客户端对未知弹窗的进程路径进行记录
101
客户端依据未知弹窗的进程路径，对相应未知弹窗的安全性进行第一检测，得到的第一检测结果具体可以包括确定和不确定
102
在第一检测结果为不确定时，客户端将相应弹窗的文件发送至服务器端
103
服务器端对所述弹窗的文件的安全性进行第二检测，得到第二检测结果
104
服务器端将第二检测结果返回给客户端
105

图 1

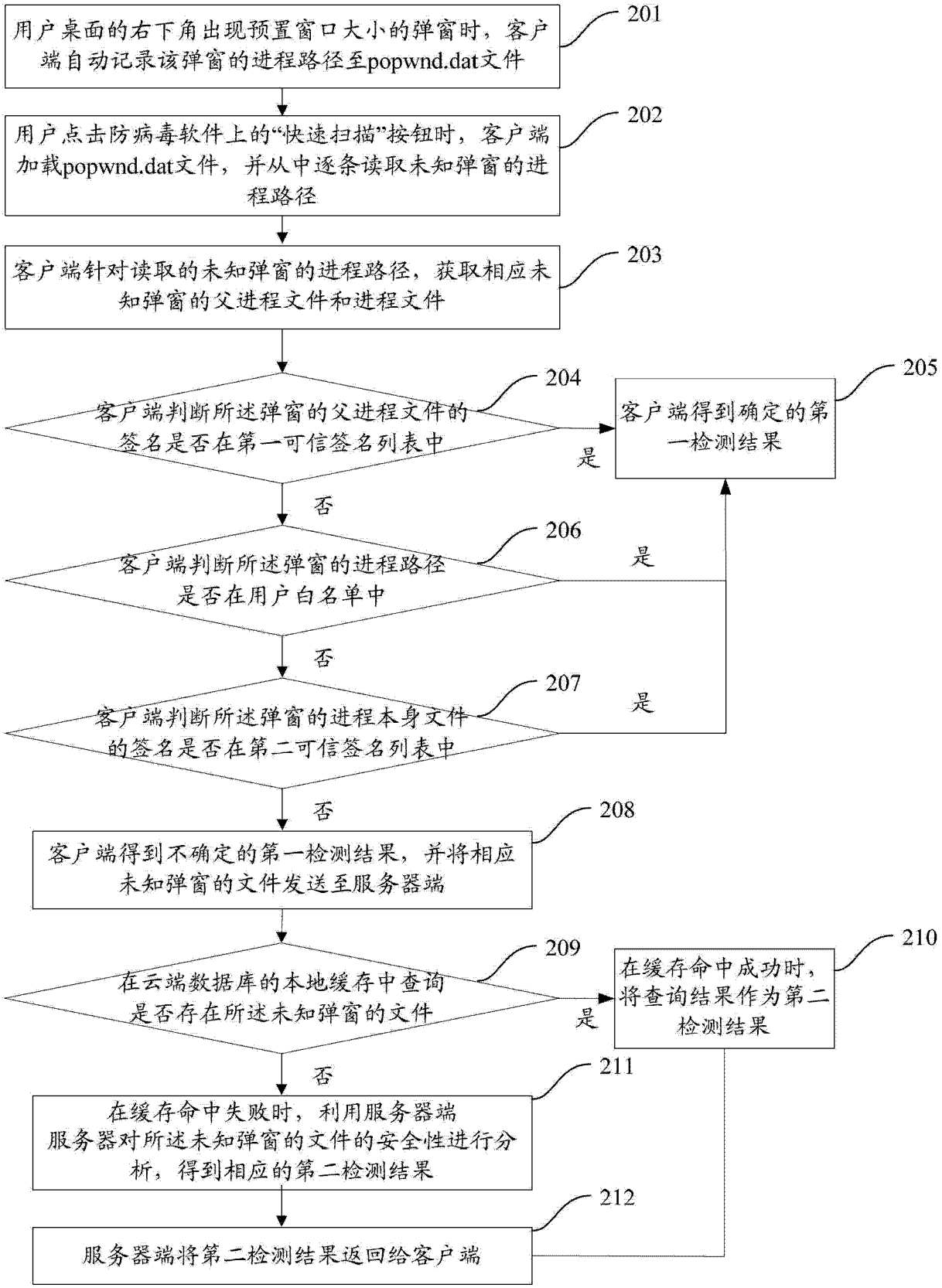

用户桌面的右下角出现预置窗口大小的弹窗时，客户端自动记录该弹窗的进程路径至popwnd.dat文件
201
用户点击防病毒软件上的“快速扫描”按钮时，客户端加载popwnd.dat文件，并从中逐条读取未知弹窗的进程路径
202
客户端针对读取的未知弹窗的进程路径，获取相应未知弹窗的父进程文件和进程文件
203
客户端判断所述弹窗的父进程文件的签名是否在第一可信签名列表中
204
是
客户端得到确定的第一检测结果
205
否
客户端判断所述弹窗的进程路径是否在用户白名单中
206
是
否
客户端判断所述弹窗的进程本身文件的签名是否在第二可信签名列表中
207
是
否
客户端得到不确定的第一检测结果，并将相应未知弹窗的文件发送至服务器端
208
在云端数据库的本地缓存中查询是否存在所述未知弹窗的文件
209
是
在缓存命中成功时，将查询结果作为第二检测结果
210
否
在缓存命中失败时，利用服务器端服务器对所述未知弹窗的文件的安全性进行分析，得到相应的第二检测结果
211
服务器端将第二检测结果返回给客户端
212

图 2

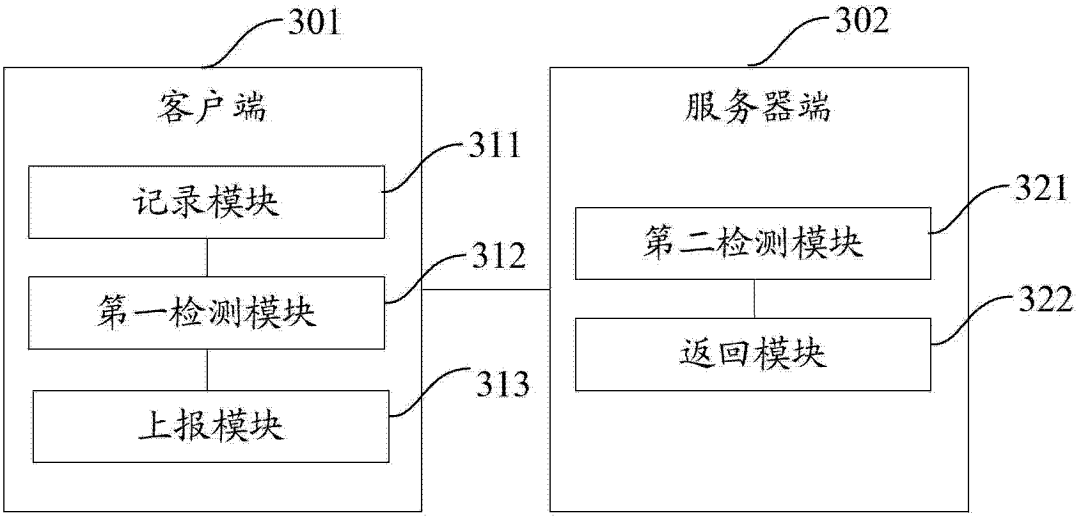

301
客户端
311
记录模块
312
第一检测模块
313
上报模块
302
服务器端
321
第二检测模块
322
返回模块

图 3