(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 102346827 A
(43)申请公布日 2012.02.08

(21)申请号 201110277746.3

(22)申请日 2011.09.19

(71)申请人 奇智软件(北京)有限公司
地址 100025 北京市朝阳区酒仙桥路 14 号兆维大厦 4 层东侧单元

(72)发明人 付旻 邹贵强

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 陈蕾 逯长明

(51)Int.Cl.
G06F 21/00(2006.01)
G06F 17/30(2006.01)

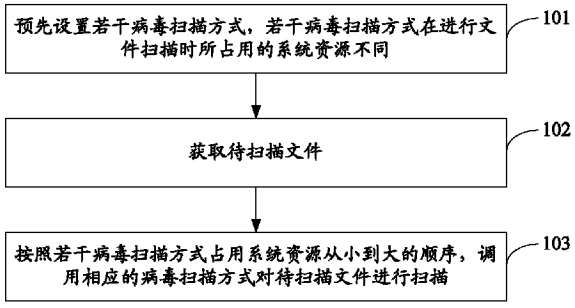
权利要求书 3 页 说明书 9 页 附图 3 页

(54)发明名称

处理计算机病毒的方法及装置

(57)摘要

本申请实施例公开了一种处理计算机病毒的方法及装置，预先设置若干病毒扫描方式，所述若干病毒扫描方式在进行文件扫描时所占用的系统资源不同，所述方法包括：获取待扫描文件；按照所述若干病毒扫描方式占用系统资源从小到大的顺序，调用相应的病毒扫描方式对所述待扫描文件进行扫描。应用本申请实施例对文件进行病毒扫描，由于按照占用系统资源从小到大的顺序调用相应的病毒扫描方式，因此可以先通过占用系统资源较少的病毒扫描方式，例如内存扫描方式对文件进行扫描，从而减少占用系统资源较大的病毒扫描方式所需扫描的文件数量，由此提高系统的病毒扫描速度，节约系统资源。



CN 102346827 A

1. 一种处理计算机病毒的方法，其特征在于，预先设置若干病毒扫描方式，所述若干病毒扫描方式在进行文件扫描时所占用的系统资源不同，所述方法包括：

获取待扫描文件；

按照所述若干病毒扫描方式占用系统资源从小到大的顺序，调用相应的病毒扫描方式对所述待扫描文件进行扫描。

2. 根据权利要求 1 所述的方法，其特征在于，所述若干病毒扫描方式至少包括第一病毒扫描方式和第二病毒扫描方式，所述第一病毒扫描方式占用的系统资源小于所述第二病毒扫描方式；

所述调用相应的病毒扫描方式对所述待扫描文件进行扫描包括：

调用所述第一病毒扫描方式对所述待扫描文件进行扫描，获得所述待扫描文件中的确定文件；

调用所述第二病毒扫描方式仅对所述待扫描文件中除所述确定文件以外的其它文件进行扫描。

3. 根据权利要求 1 所述的方法，其特征在于，所述若干病毒扫描方式按照占用系统资源从小到大顺序排列，包括下述至少两种方式：

根据缓存中保存的已扫描文件的扫描结果进行病毒扫描的内存扫描方式，所述扫描结果包括确定为恶意文件或非恶意文件的文件属性信息，所述文件属性信息包括文件大小、文件修改时间和文件路径；

通过预先保存的黑名单和白名单中的至少一种名单进行病毒扫描的名单扫描方式；

通过杀毒引擎进行病毒扫描的引擎扫描方式。

4. 根据权利要求 3 所述的方法，其特征在于，所述按照若干病毒扫描方式占用系统资源从小到大的顺序，调用相应的病毒扫描方式对待扫描的文件进行扫描包括：

调用所述内存扫描方式对所述待扫描文件进行扫描，获得包含第一确定文件的第一扫描结果；

调用所述名单扫描方式仅对所述待扫描文件中除所述第一确定文件的其它文件进行扫描，获得包含第二确定文件的第二扫描结果；

调用所述引擎扫描方式仅对所述其它文件中除所述第二确定文件以外的剩余文件进行扫描，获得包含第三确定文件的第三扫描结果。

5. 根据权利要求 4 所述的方法，其特征在于，采用内存扫描方式对所述待扫描文件进行扫描包括：

获取待扫描文件的文件属性信息；

将所述文件属性信息与缓存中保存的文件属性信息进行匹配；

当待扫描文件的文件属性与缓存中保存的文件属性匹配时，将所述待扫描文件确定为恶意文件或非恶意文件，当待扫描文件的文件属性与缓存中保存的文件属性不匹配时，将所述待扫描文件确定为通过名单扫描方式进行扫描的其它文件。

6. 根据权利要求 4 所述的方法，其特征在于，

通过预先保存的黑名单对经过内存扫描方式扫描后的除所述第一确定文件的其它文件进行扫描包括：

将所述其它文件中的每一个文件的文件名与所述黑名单中预先保存的文件名进行比

较，当某个文件的文件名与所述预先保存的文件名匹配时，确定所述某个文件为属于所述第二确定文件的恶意文件；

通过预先保存的白名单对经过内存扫描方式扫描后的除所述第一确定文件的其它文件进行扫描包括：

将所述其它文件中的每一个文件的文件名与所述白名单中预先保存的文件名进行比较，当某个文件的文件名与所述预先保存的文件名匹配时，确定所述某个文件为属于所述第二确定文件的非恶意文件。

7. 根据权利要求 4 所述的方法，其特征在于，还包括：

根据待扫描文件的扫描结果，将所述第二确定文件和第三确定文件的文件属性存入缓存中。

8. 一种处理计算机病毒的装置，其特征在于，所述装置包括：

设置单元，用于预先设置若干病毒扫描方式，所述若干病毒扫描方式在进行文件扫描时所占用的系统资源不同；

获取单元，用于获取待扫描文件；

扫描单元，用于按照所述若干病毒扫描方式占用系统资源从小到达的顺序，调用相应的病毒扫描方式对所述待扫描文件进行扫描。

9. 根据权利要求 8 所述的装置，其特征在于，所述设置单元中设置的若干病毒扫描方式至少包括第一病毒扫描方式和第二病毒扫描方式，所述第一病毒扫描方式占用的系统资源小于所述第二病毒扫描方式；

所述扫描单元包括：

第一调用扫描单元，用于调用所述第一病毒扫描方式对所述待扫描文件进行扫描，获得所述待扫描文件中的确定文件；

第二调用扫描单元，用于调用所述第二病毒扫描方式仅对所述待扫描文件中除所述确定文件以外的其它文件进行扫描，获得第二扫描结果。

10. 根据权利要求 8 所述的装置，其特征在于，所述设置单元设置的若干病毒扫描方式按照占用系统资源从小到达顺序排列，包括下述至少两种方式：

根据缓存中保存的已扫描文件的扫描结果进行病毒扫描的内存扫描方式，所述扫描结果包括确定为恶意文件或非恶意文件的文件属性，所述文件属性包括文件大小、文件修改时间和文件路径；

通过预先保存的黑名单和白名单中的至少一种名单进行病毒扫描的名单扫描方式；

通过少度引擎进行病毒扫描的引擎扫描方式。

11. 根据权利要求 10 所述的装置，其特征在于，所述扫描单元包括：

第一扫描单元，用于调用所述内存扫描方式对所述待扫描文件进行扫描，获得包含第一确定文件的第一扫描结果；

第二扫描单元，用于调用所述名单扫描方式仅对所述待扫描文件中除所述第一确定文件的其它文件进行扫描，获得包含第二确定文件的第二扫描结果；

第三扫描单元，用于调用所述引擎扫描方式仅对所述其它文件中除所述第二确定文件的剩余文件进行扫描，获得包含第三确定文件的第三扫描结果。

12. 根据权利要求 11 所述的装置，其特征在于，第一扫描单元包括：

信息获取单元，用于获取待扫描文件的文件属性信息；

信息匹配单元，用于将所述文件属性信息与缓存中保存的文件属性信息进行匹配；

结果确定单元，用于当待扫描文件的文件属性与缓存中保存的文件属性匹配时，将所述待扫描文件确定为恶意文件或非恶意文件，当待扫描文件的文件属性与缓存中保存的文件属性不匹配时，将所述待扫描文件确定为通过名单扫描方式进行扫描的其它文件。

13. 根据权利要求 11 所述的装置，其特征在于，所述第二扫描单元包括至少一个下述单元：

黑名单扫描单元，用于将所述其它文件中的每一个文件的文件名与所述黑名单中预先保存的文件名进行比较，当某个文件的文件名与所述预先保存的文件名匹配时，确定所述某个文件为属于所述第二确定文件的恶意文件；

白名单扫描单元，用于将所述其它文件中的每一个文件的文件名与所述白名单中预先保存的文件名进行比较，当某个文件的文件名与所述预先保存的文件名匹配时，确定所述某个文件为属于所述第二确定文件的非恶意文件。

14. 根据权利要求 11 所述的装置，其特征在于，还包括：

存储单元，用于根据所述第二扫描单元和第三扫描单元的扫描结果，将所述第二确定文件和第三确定文件的文件属性存入缓存中。

处理计算机病毒的方法及装置

技术领域

[0001] 本申请涉及计算机技术领域，特别是涉及一种处理计算机病毒的方法及装置。

背景技术

[0002] 计算机病毒是编制或者在计算机程序中插入的破坏计算机功能的数据，其会影响计算机的正常使用并且能够自我复制，通常以一组计算机指令或者程序代码的形式呈现。而杀毒引擎就是一套判断特定程序行为是否为病毒程序（包括可疑程序）的技术机制。杀毒引擎是杀毒软件的主要部分，是检测和发现病毒的程序，而病毒库是已经发现的病毒的特征集合。在杀毒过程中，用病毒库中的特征去对照机器中的所有程序或文件，对于符合这些特征的程序或文件，判定为病毒。

[0003] 发明人在对现有技术的研究过程中发现，每一次采用杀毒引擎进行杀毒的过程均相互独立，即无论前一次采用杀毒引擎对文件进行扫描后输出何种结果，下一次仍然采用杀毒引擎对所有文件进行扫描，前后两次扫描过程中发现的病毒文件类型可能相同。由此可知，虽然杀毒引擎具有杀毒功能强大的特点，但是每次采用杀毒引擎对所有文件进行扫描时，都将占用大量的系统资源。

发明内容

[0004] 本申请实施例提供了一种处理计算机病毒的方法及装置，以解决现有杀毒引擎每一次杀毒都对所有文件进行扫描，占用大量系统资源的问题。

[0005] 为了解决上述技术问题，本申请实施例公开了如下技术方案：

[0006] 一种处理计算机病毒的方法，预先设置若干病毒扫描方式，所述若干病毒扫描方式在进行文件扫描时所占用的系统资源不同，所述方法包括：

[0007] 获取待扫描文件；

[0008] 按照所述若干病毒扫描方式占用系统资源从小到大的顺序，调用相应的病毒扫描方式对所述待扫描文件进行扫描。

[0009] 所述若干病毒扫描方式至少包括第一病毒扫描方式和第二病毒扫描方式，所述第一病毒扫描方式占用的系统资源小于所述第二病毒扫描方式；

[0010] 所述调用相应的病毒扫描方式对所述待扫描文件进行扫描包括：

[0011] 调用所述第一病毒扫描方式对所述待扫描文件进行扫描，获得所述待扫描文件中的确定文件；

[0012] 调用所述第二病毒扫描方式仅对所述待扫描文件中除所述确定文件以外的其它文件进行扫描。

[0013] 所述若干病毒扫描方式按照占用系统资源从小到大顺序排列，包括下述至少两种方式：

[0014] 根据缓存中保存的已扫描文件的扫描结果进行病毒扫描的内存扫描方式，所述扫描结果包括确定为恶意文件或非恶意文件的文件属性信息，所述文件属性信息包括文件大

小、文件修改时间和文件路径；

[0015] 通过预先保存的黑名单和白名单中的至少一种名单进行病毒扫描的名单扫描方式；

[0016] 通过杀毒引擎进行病毒扫描的引擎扫描方式。

[0017] 所述按照若干病毒扫描方式占用系统资源从小到大的顺序，调用相应的病毒扫描方式对待扫描的文件进行扫描包括：

[0018] 调用所述内存扫描方式对所述待扫描文件进行扫描，获得包含第一确定文件的第一扫描结果；

[0019] 调用所述名单扫描方式仅对所述待扫描文件中除所述第一确定文件的其它文件进行扫描，获得包含第二确定文件的第二扫描结果；

[0020] 调用所述引擎扫描方式仅对所述其它文件中除所述第二确定文件的剩余文件进行扫描，获得包含第三确定文件的第三扫描结果。

[0021] 采用内存扫描方式对所述待扫描文件进行扫描包括：

[0022] 获取待扫描文件的文件属性信息；

[0023] 将所述文件属性信息与缓存中保存的文件属性信息进行匹配；

[0024] 当待扫描文件的文件属性与缓存中保存的文件属性匹配时，将所述待扫描文件确定为恶意文件或非恶意文件，当待扫描文件的文件属性与缓存中保存的文件属性不匹配时，将所述待扫描文件确定为通过名单扫描方式进行扫描的其它文件。

[0025] 通过预先保存的黑名单对经过内存扫描方式扫描后的除所述第一确定文件的其它文件进行扫描包括：

[0026] 将所述其它文件中的每一个文件的文件名与所述黑名单中预先保存的文件名进行比较，当某个文件的文件名与所述预先保存的文件名匹配时，确定所述某个文件为属于所述第二确定文件的恶意文件；

[0027] 通过预先保存的白名单对经过内存扫描方式扫描后的除所述第一确定文件的其它文件进行扫描包括：

[0028] 将所述其它文件中的每一个文件的文件名与所述白名单中预先保存的文件名进行比较，当某个文件的文件名与所述预先保存的文件名匹配时，确定所述某个文件为属于所述第二确定文件的非恶意文件。

[0029] 还包括：

[0030] 根据待扫描文件的扫描结果，将所述第二确定文件和第三确定文件的文件属性存入缓存中。

[0031] 一种处理计算机病毒的装置，所述装置包括：

[0032] 设置单元，用于预先设置若干病毒扫描方式，所述若干病毒扫描方式在进行文件扫描时所占用的系统资源不同；

[0033] 获取单元，用于获取待扫描文件；

[0034] 扫描单元，用于按照所述若干病毒扫描方式占用系统资源从小到达的顺序，调用相应的病毒扫描方式对所述待扫描文件进行扫描。

[0035] 所述设置单元中设置的若干病毒扫描方式至少包括第一病毒扫描方式和第二病毒扫描方式，所述第一病毒扫描方式占用的系统资源小于所述第二病毒扫描方式；

[0036] 所述扫描单元包括：

[0037] 第一调用扫描单元，用于调用所述第一病毒扫描方式对所述待扫描文件进行扫描，获得所述待扫描文件中的确定文件；

[0038] 第二调用扫描单元，用于调用所述第二病毒扫描方式仅对所述待扫描文件中除所述确定文件以外的其它文件进行扫描，获得第二扫描结果。

[0039] 所述设置单元设置的若干病毒扫描方式按照占用系统资源从小到达顺序排列，包括下述至少两种方式：

[0040] 根据缓存中保存的已扫描文件的扫描结果进行病毒扫描的内存扫描方式，所述扫描结果包括确定为恶意文件或非恶意文件的文件属性，所述文件属性包括文件大小、文件修改时间和文件路径；

[0041] 通过预先保存的黑名单和白名单中的至少一种名单进行病毒扫描的名单扫描方式；

[0042] 通过少度引擎进行病毒扫描的引擎扫描方式。

[0043] 所述扫描单元包括：

[0044] 第一扫描单元，用于调用所述内存扫描方式对所述待扫描文件进行扫描，获得包含第一确定文件的第一扫描结果；

[0045] 第二扫描单元，用于调用所述名单扫描方式仅对所述待扫描文件中除所述第一确定文件的其它文件进行扫描，获得包含第二确定文件的第二扫描结果；

[0046] 第三扫描单元，用于调用所述引擎扫描方式仅对所述其它文件中除所述第二确定文件的剩余文件进行扫描，获得包含第三确定文件的第三扫描结果。

[0047] 第一扫描单元包括：

[0048] 信息获取单元，用于获取待扫描文件的文件属性信息；

[0049] 信息匹配单元，用于将所述文件属性信息与缓存中保存的文件属性信息进行匹配；

[0050] 结果确定单元，用于当待扫描文件的文件属性与缓存中保存的文件属性匹配时，将所述待扫描文件确定为恶意文件或非恶意文件，当待扫描文件的文件属性与缓存中保存的文件属性不匹配时，将所述待扫描文件确定为通过名单扫描方式进行扫描的其它文件。

[0051] 所述第二扫描单元包括至少一个下述单元：

[0052] 黑名单扫描单元，用于将所述其它文件中的每一个文件的文件名与所述黑名单中预先保存的文件名进行比较，当某个文件的文件名与所述预先保存的文件名匹配时，确定所述某个文件为属于所述第二确定文件的恶意文件；

[0053] 白名单扫描单元，用于将所述其它文件中的每一个文件的文件名与所述白名单中预先保存的文件名进行比较，当某个文件的文件名与所述预先保存的文件名匹配时，确定所述某个文件为属于所述第二确定文件的非恶意文件。

[0054] 还包括：

[0055] 存储单元，用于根据所述第二扫描单元和第三扫描单元的扫描结果，将所述第二确定文件和第三确定文件的文件属性存入缓存中。

[0056] 由上述实施例可以看出，本申请实施例中预先设置若干病毒扫描方式，这些病毒扫描方式在进行文件扫描时所占用的系统资源不同，获取待扫描文件，按照若干病毒扫描

方式占用系统资源从小到大的顺序，调用相应的病毒扫描方式对待扫描文件进行扫描。应用本申请实施例对文件进行病毒扫描，由于按照占用系统资源从小到大的顺序调用相应的病毒扫描方式，因此可以先通过占用系统资源较少的病毒扫描方式，例如内存扫描方式对文件进行扫描，从而减少占用系统资源较大的病毒扫描方式所需扫描的文件数量，由此提高系统的病毒扫描速度，节约系统资源；进一步，由于占用系统资源较小的内存扫描方式可以保存前一次扫描的扫描结果，因此再次扫描时，可以通过内存扫描方式确定大部分文件的扫描结果，从而进一步提升扫描速度。

附图说明

[0057] 为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，对于本领域普通技术人员而言，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0058] 图 1 为本申请处理计算机病毒的方法的第一实施例流程图；

[0059] 图 2 为本申请处理计算机病毒的方法的第二实施例流程图；

[0060] 图 3 为本申请处理计算机病毒的方法的第三实施例流程图；

[0061] 图 4 为本申请处理计算机病毒的装置的第一实施例框图；

[0062] 图 5 为本申请处理计算机病毒的装置的第二实施例框图。

具体实施方式

[0063] 本发明如下实施例提供了处理计算机病毒的方法及装置。本申请实施例中由于按照占用系统资源从小到大的顺序调用相应的病毒扫描方式，因此可以先通过占用系统资源较少的病毒扫描方式，从而减少占用系统资源较大的病毒扫描方式所需扫描的文件数量，由此提高系统的病毒扫描速度，节约系统资源。

[0064] 为了使本技术领域的人员更好地理解本发明实施例中的技术方案，并使本发明实施例的上述目的、特征和优点能够更加明显易懂，下面结合附图对本发明实施例中技术方案作进一步详细的说明。

[0065] 参见图 1，为本申请处理计算机病毒的方法的第一实施例流程图：

[0066] 步骤 101：预先设置若干病毒扫描方式，若干病毒扫描方式在进行文件扫描时所占用的系统资源不同。

[0067] 其中，若干病毒扫描方式按照占用系统资源从小到大顺序排列，包括下述至少两种方式：根据缓存中保存的已扫描文件的扫描结果进行病毒扫描的内存扫描方式，其中扫描结果包括确定为恶意文件或非恶意文件的文件属性信息，文件属性信息包括文件大小、文件修改时间和文件路径；通过预先保存的黑名单和白名单中的至少一种名单进行病毒扫描的名单扫描方式；通过杀毒引擎进行病毒扫描的引擎扫描方式。

[0068] 步骤 102：获取待扫描文件。

[0069] 步骤 103：按照若干病毒扫描方式占用系统资源从小到大的顺序，调用相应的病毒扫描方式对待扫描文件进行扫描。

[0070] 其中，当若干病毒扫描方式至少包括第一病毒扫描方式和第二病毒扫描方式，且第一病毒扫描方式占用的系统资源小于第二病毒扫描方式时，先调用第一病毒扫描方式对

待扫描文件进行扫描，获得待扫描文件中的确定文件，然后调用第二病毒扫描方式仅对待扫描文件中除确定文件以外的其它文件进行扫描。其中，确定文件指确定为恶意文件或非恶意文件的文件。

[0071] 具体的，当同时采用内存扫描方式、名单扫描方式和引擎扫描方式对待扫描文件进行扫描时，首先调用内存扫描方式对待扫描文件进行扫描，获得包含第一确定文件的第一扫描结果，然后调用名单扫描方式仅对待扫描文件中除第一确定文件的其它文件进行扫描，获得包含第二确定文件的第二扫描结果，最后调用引擎扫描方式仅对其它文件中除第二确定文件的剩余文件进行扫描，获得包含第三确定文件的第三扫描结果。

[0072] 参见图 2，为本申请处理计算机病毒的方法的第二实施例流程图，该实施例详细描述了采用三种扫描方式对待扫描文件进行扫描的过程：

[0073] 步骤 201：预先设置按照占用系统资源从小到大顺序排列的内存扫描方式、名单扫描方式和引擎扫描方式。

[0074] 其中，内存扫描方式指根据缓存中保存的已扫描文件的扫描结果进行病毒扫描，扫描结果包括确定为恶意文件或非恶意文件的文件属性信息，文件属性信息包括文件大小、文件修改时间和文件路径等；名单扫描方式指通过预先保存的黑名单和白名单中的至少一种名单进行病毒扫描；引擎扫描方式指通过杀毒引擎进行病毒扫描的引擎扫描方式。

[0075] 步骤 202：获取待扫描文件。

[0076] 步骤 203：调用内存扫描方式对待扫描文件进行扫描，获得包含第一确定文件的第一扫描结果。

[0077] 获取待扫描文件的文件属性信息，例如文件大小、文件修改时间和文件路径等。系统中文件属性记录了该文件最后一次被修改后的文件大小、修改时间和文件路径等属性信息，属性信息根据文件的修改进行实时更新。

[0078] 将文件属性信息与缓存中保存的文件属性信息进行匹配，当待扫描文件的文件属性与缓存中保存的文件属性匹配时，将待扫描文件确定为恶意文件或非恶意文件，当待扫描文件的文件属性与缓存中保存的文件属性不匹配时，将待扫描文件确定为通过名单扫描方式进行扫描的其它文件。由于文件属性信息包括多种信息，因此在进行匹配时可以按照预设顺序对每一种属性信息进行逐一匹配，例如，先匹配文件大小，其次匹配文件修改时间，最后匹配文件路径等。其中，当某一文件的所有属性信息都与缓存中保存的文件属性信息一致时，才确定该文件的文件属性与缓存中保存的文件属性匹配，当某一文件的任意一种属性信息与缓存中保存的文件属性信息不一致时，则确定该文件的文件属性与缓存中保存的文件属性不匹配。

[0079] 由于内存扫描方式是根据缓存中保存的已扫描文件的扫描结果进行病毒扫描，因此通过匹配获得的第一扫描结果中的确定文件是根据前次扫描已经确定为恶意文件和非恶意文件的文件集合。由于内存信息读取速度快，且前后两次扫描过程中病毒文件发生的变化不大，因此通过内存扫描方式可以对系统中的大部分文件进行查杀，因此提升了查杀速度，节约了系统资源。

[0080] 步骤 204：调用名单扫描方式仅对待扫描文件中除第一确定文件的其它文件进行扫描，获得包含第二确定文件的第二扫描结果。

[0081] 通过预先保存的黑名单进行扫描时，将其它文件中的每一个文件的文件名与黑名

单中预先保存的文件名进行比较，当某个文件的文件名与预先保存的文件名匹配时，确定某个文件为属于第二确定文件的恶意文件；通过预先保存的白名单进行扫描时，将其它文件中的每一个文件的文件名与白名单中预先保存的文件名进行比较，当某个文件的文件名与预先保存的文件名匹配时，确定某个文件为属于第二确定文件的非恶意文件。

[0082] 其中，白名单通常由用户在客户端进行维护，用户将确定为非恶意的文件加入到白名单中进行保存，白名单中可以记录文件的文件名和文件路径等信息；黑名单通常由杀毒软件提供方进行维护，根据监控将确定的恶意文件加入到黑名单中进行保存。

[0083] 步骤 205：调用引擎扫描方式仅对其它文件中除第二确定文件的剩余文件进行扫描，获得包含第三确定文件的第三扫描结果。

[0084] 采用引擎扫描方式对剩余文件进行扫描时，可以采用的杀毒引擎可以包括：云查杀引擎，QVM(Qihoo Virtual Machine，人工智能引擎)引擎，小红伞杀毒引擎等任意现有已存在的杀毒引擎。

[0085] 步骤 206：根据待扫描文件的扫描结果，将第二确定文件和第三确定文件的文件属性存入缓存中。

[0086] 由于本次扫描过程中，通过名单扫描方式和引擎扫描方式得到的扫描结果中的确定文件与在缓存中保存的确定文件不同，因此为了进一步提高下一次病毒扫描速度，将第二确定文件和第三确定文件的文件属性，包括文件大小、文件修改时间及文件路径等记录到缓存中，则下一次对这些文件可以直接通过占用系统资源最少的内存扫描方式进行扫描。

[0087] 参见图 3，为本申请处理计算机病毒的方法的第三实施例流程图，该实施例详细示出了通过内存扫描方式对待扫描文件进行扫描的过程：

[0088] 步骤 301：缓存中预先保存已扫描文件的扫描结果，该扫描结果包括确定为恶意文件或非恶意文件的文件属性信息，文件属性信息包括文件大小、文件修改时间和文件路径。

[0089] 步骤 302：顺序获取待扫描文件中的一个文件。

[0090] 步骤 303：获取该文件的文件大小、文件修改时间和文件路径。

[0091] 系统中文件的文件属性记录了该文件最后一次被修改后的文件大小、修改时间和文件路径等属性信息，属性信息根据文件的修改进行实时更新。

[0092] 步骤 304：判断该文件的文件大小是否与预先保存的文件大小匹配，若是，则执行步骤 305，否则，执行步骤 309。

[0093] 步骤 305：判断该文件的文件修改时间是否与预先保存的文件修改时间匹配，若是，则执行步骤 306；否则，执行步骤 309。

[0094] 步骤 306：判断该文件的文件路径是否与预先保存的文件路径匹配，若是，则执行步骤 307；否则，执行步骤 309。

[0095] 步骤 307：根据匹配结果将该文件确定为恶意文件或非恶意文件。

[0096] 当某一文件的所有属性信息都与缓存中保存的文件属性信息一致时，才确定该文件的文件属性与缓存中保存的文件属性匹配，此时如果内存中相匹配的文件属性信息对应的文件为恶意文件，则该文件的扫描结果即为恶意文件，如果内存中匹配的文件属性信息对应的文件为非恶意文件，则该文件的扫描结果即为非恶意文件。

[0097] 由于内存扫描方式是根据缓存中保存的已扫描文件的扫描结果进行病毒扫描，因此通过匹配获得的第一扫描结果中的确定文件是根据前次扫描已经确定为恶意文件和非恶意文件的文件集合。由于内存信息读取速度快，且前后两次扫描过程中病毒文件发生的变化不大，因此通过内存扫描方式可以对系统中的大部分文件进行查杀，因此提升了查杀速度，节约了系统资源。

[0098] 步骤 308 ：将该文件确定为需要通过其它扫描方式进行扫描的文件。

[0099] 当某一文件的任意一种属性信息与缓存中保存的文件属性信息不一致时，则确定该文件的文件属性与缓存中保存的文件属性不匹配。此时，说明该文件为需要通过除内存扫描方式的其它扫描方式进行扫描，例如，通过前述实施例中示出的名单扫描方式，和 / 或引擎扫描方式。

[0100] 步骤 309 ：是否匹配完所有待扫描文件，若是，则结束流程，否则，返回步骤 302。

[0101] 由上述本申请实施例可见，在对文件进行病毒扫描时，由于按照占用系统资源从小到大的顺序调用相应的病毒扫描方式，因此可以先通过占用系统资源较少的病毒扫描方式，例如内存扫描方式对文件进行扫描，从而减少占用系统资源较大的病毒扫描方式所需扫描的文件数量，由此提高系统的病毒扫描速度，节约系统资源 ；进一步，由于占用系统资源较小的内存扫描方式可以保存前一次扫描的扫描结果，因此再次扫描时，可以通过内存扫描方式确定大部分文件的扫描结果，从而进一步提升扫描速度。

[0102] 与本申请处理计算机病毒的方法的实施例相对应，本申请还提供了处理计算机病毒的装置的实施例。

[0103] 参见图 4，为本申请处理计算机病毒的装置的第一实施例框图 ：

[0104] 该装置包括 ：设置单元 410、获取单元 420 和扫描单元 430。

[0105] 其中，设置单元 410，用于预先设置若干病毒扫描方式，所述若干病毒扫描方式在进行文件扫描时所占用的系统资源不同 ；

[0106] 获取单元 420，用于获取待扫描文件 ；

[0107] 扫描单元 430，用于按照所述若干病毒扫描方式占用系统资源从小到达的顺序，调用相应的病毒扫描方式对所述待扫描文件进行扫描。

[0108] 其中，所述设置单元 410 中设置的若干病毒扫描方式至少包括第一病毒扫描方式和第二病毒扫描方式，所述第一病毒扫描方式占用的系统资源小于所述第二病毒扫描方式 ；

[0109] 所述扫描单元 430 可以具体包括（图 4 中未示出）：

[0110] 第一调用扫描单元，用于调用所述第一病毒扫描方式对所述待扫描文件进行扫描，获得所述待扫描文件中的确定文件 ；

[0111] 第二调用扫描单元，用于调用所述第二病毒扫描方式仅对所述待扫描文件中除所述确定文件以外的其它文件进行扫描，获得第二扫描结果。

[0112] 参见图 5，为本申请处理计算机病毒的装置的第二实施例框图 ：

[0113] 该装置包括 ：设置单元 510、获取单元 520、扫描单元 530 和存储单元 540。

[0114] 其中，设置单元 510，用于预先设置若干病毒扫描方式，所述若干病毒扫描方式在进行文件扫描时所占用的系统资源不同 ；其中，所述设置单元设置的若干病毒扫描方式按照占用系统资源从小到达顺序排列，包括下述至少两种方式 ：根据缓存中保存的已扫描文

件的扫描结果进行病毒扫描的内存扫描方式，所述扫描结果包括确定为恶意文件或非恶意文件的文件属性，所述文件属性包括文件大小、文件修改时间和文件路径；通过预先保存的黑名单和白名单中的至少一种名单进行病毒扫描的名单扫描方式；通过少度引擎进行病毒扫描的引擎扫描方式；

[0115] 获取单元 520，用于获取待扫描文件；

[0116] 扫描单元 530，用于按照所述若干病毒扫描方式占用系统资源从小到达的顺序，调用相应的病毒扫描方式对所述待扫描文件进行扫描；该扫描单元 530 可以包括：第一扫描单元 531，用于调用所述内存扫描方式对所述待扫描文件进行扫描，获得包含第一确定文件的第一扫描结果；第二扫描单元 532，用于调用所述名单扫描方式仅对所述待扫描文件中除所述第一确定文件的其它文件进行扫描，获得包含第二确定文件的第二扫描结果；第三扫描单元 533，用于调用所述引擎扫描方式仅对所述其它文件中除所述第二确定文件的剩余文件进行扫描，获得包含第三确定文件的第三扫描结果；

[0117] 存储单元 540，用于根据所述第二扫描单元和第三扫描单元的扫描结果，将所述第二确定文件和第三确定文件的文件属性存入缓存中。

[0118] 具体的，第一扫描单元 531 可以包括（图 5 中未示出）：

[0119] 信息获取单元，用于获取待扫描文件的文件属性信息；

[0120] 信息匹配单元，用于将所述文件属性信息与缓存中保存的文件属性信息进行匹配；

[0121] 结果确定单元，用于当待扫描文件的文件属性与缓存中保存的文件属性匹配时，将所述待扫描文件确定为恶意文件或非恶意文件，当待扫描文件的文件属性与缓存中保存的文件属性不匹配时，将所述待扫描文件确定为通过名单扫描方式进行扫描的其它文件。

[0122] 具体的，第二扫描单元 532 可以包括（图 5 中未示出）：

[0123] 黑名单扫描单元，用于将所述其它文件中的每一个文件的文件名与所述黑名单中预先保存的文件名进行比较，当某个文件的文件名与所述预先保存的文件名匹配时，确定所述某个文件为属于所述第二确定文件的恶意文件；

[0124] 白名单扫描单元，用于将所述其它文件中的每一个文件的文件名与所述白名单中预先保存的文件名进行比较，当某个文件的文件名与所述预先保存的文件名匹配时，确定所述某个文件为属于所述第二确定文件的非恶意文件。

[0125] 通过对以上实施方式的描述可知，本申请实施例中预先设置若干病毒扫描方式，这些病毒扫描方式在进行文件扫描时所占用的系统资源不同，获取待扫描文件，按照若干病毒扫描方式占用系统资源从小到大的顺序，调用相应的病毒扫描方式对待扫描文件进行扫描。应用本申请实施例对文件进行病毒扫描，由于按照占用系统资源从小到大的顺序调用相应的病毒扫描方式，因此可以先通过占用系统资源较少的病毒扫描方式，例如内存扫描方式对文件进行扫描，从而减少占用系统资源较大的病毒扫描方式所需扫描的文件数量，由此提高系统的病毒扫描速度，节约系统资源；进一步，由于占用系统资源较小的内存扫描方式可以保存前一次扫描的扫描结果，因此再次扫描时，可以通过内存扫描方式确定大部分文件的扫描结果，从而进一步提升扫描速度。

[0126] 本领域的技术人员可以清楚地了解到本发明实施例中的技术可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解，本发明实施例中的技术方案本质上或者

说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在存储介质中，如 ROM/RAM、磁碟、光盘等，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）执行本发明各个实施例或者实施例的某些部分所述的方法。

[0127] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例而言，由于其基本相似于方法实施例，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。

[0128] 以上所述的本发明实施方式，并不构成对本发明保护范围的限定。任何在本发明的精神和原则之内所作的修改、等同替换和改进等，均应包含在本发明的保护范围之内。

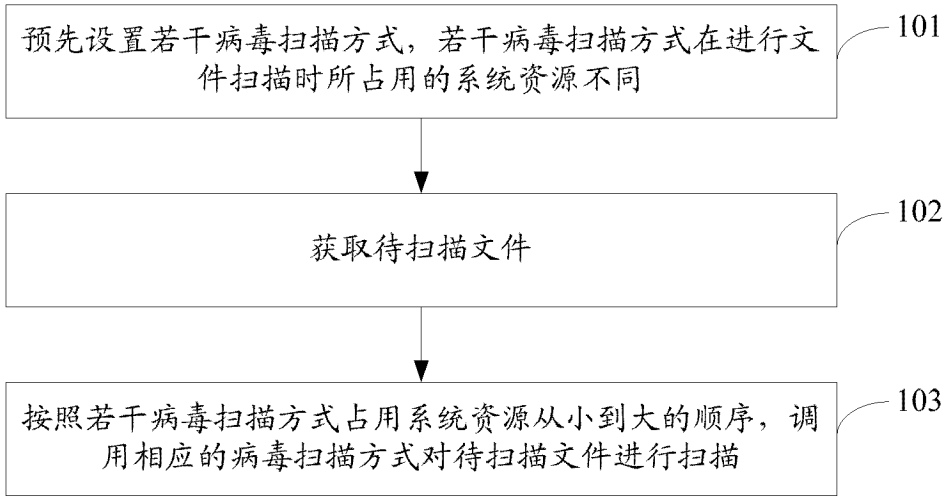

预先设置若干病毒扫描方式，若干病毒扫描方式在进行文件扫描时所占用的系统资源不同
101
获取待扫描文件
102
按照若干病毒扫描方式占用系统资源从小到大的顺序，调用相应的病毒扫描方式对待扫描文件进行扫描
103

图 1

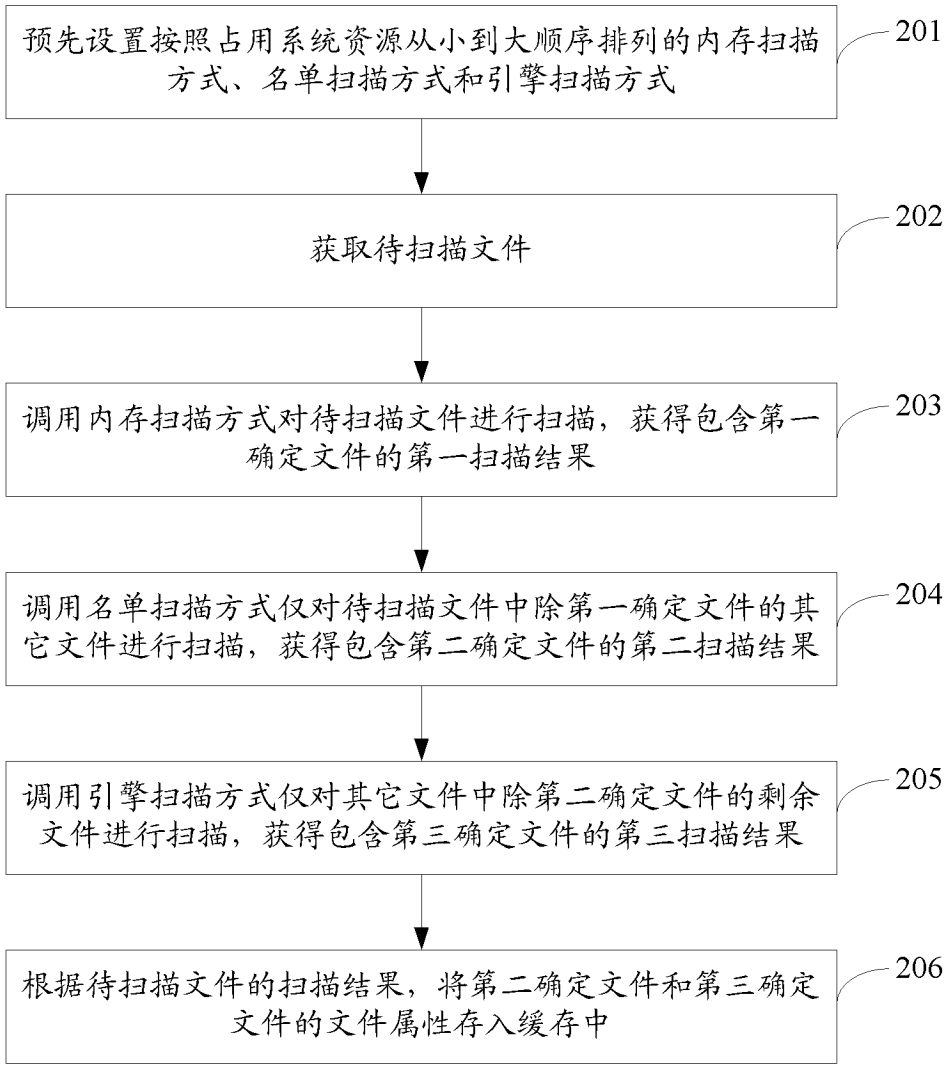

预先设置按照占用系统资源从小到大顺序排列的内存扫描方式、名单扫描方式和引擎扫描方式
201
获取待扫描文件
202
调用内存扫描方式对待扫描文件进行扫描，获得包含第一确定文件的第一扫描结果
203
调用名单扫描方式仅对待扫描文件中除第一确定文件的其它文件进行扫描，获得包含第二确定文件的第二扫描结果
204
调用引擎扫描方式仅对其它文件中除第二确定文件的剩余文件进行扫描，获得包含第三确定文件的第三扫描结果
205
根据待扫描文件的扫描结果，将第二确定文件和第三确定文件的文件属性存入缓存中
206

图 2

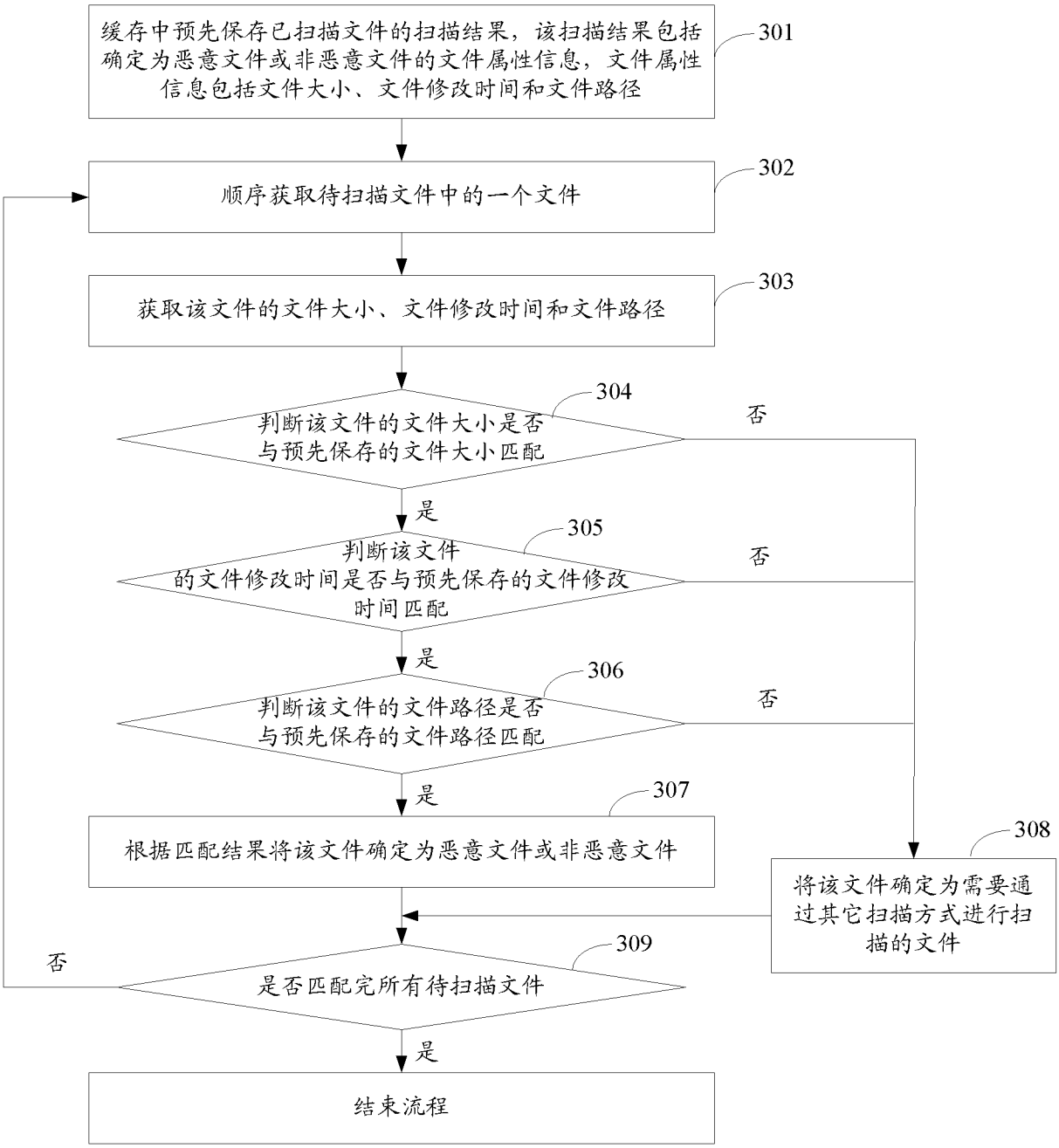

缓存中预先保存已扫描文件的扫描结果，该扫描结果包括确定为恶意文件或非恶意文件的文件属性信息，文件属性信息包括文件大小、文件修改时间和文件路径
301
顺序获取待扫描文件中的一个文件
302
获取该文件的文件大小、文件修改时间和文件路径
303
判断该文件的文件大小是否与预先保存的文件大小匹配
304
否
是
判断该文件的文件修改时间是否与预先保存的文件修改时间匹配
305
否
是
判断该文件的文件路径是否与预先保存的文件路径匹配
306
否
是
根据匹配结果将该文件确定为恶意文件或非恶意文件
307
将该文件确定为需要通过其它扫描方式进行扫描的文件
308
是否匹配完所有待扫描文件
309
否
是
结束流程

图 3

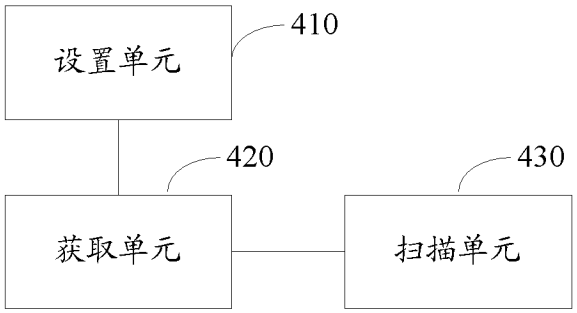


图 4

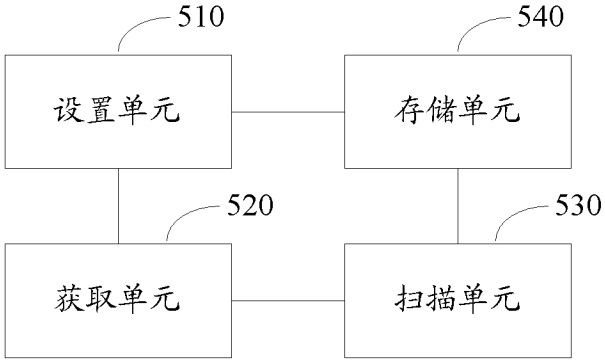


图 5