(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 104281809 A
(43)申请公布日 2015.01.14

(21)申请号 201410521361.0

(22)申请日 2014.09.30

(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 温铭

(74)专利代理机构 北京鼎佳达知识产权代理事务所(普通合伙) 11348
代理人 王伟锋 刘铁生

(51)Int.Cl.
G06F 21/56(2013.01)
H04L 29/06(2006.01)

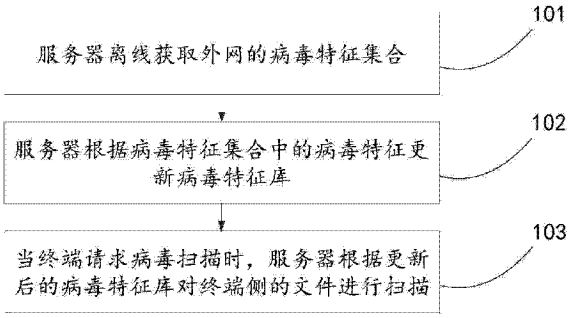
权利要求书2页 说明书15页 附图4页

(54)发明名称

病毒查杀的方法、装置及系统

(57)摘要

本发明公开了一种病毒查杀的方法、装置及系统，涉及互联网技术领域，为解决隔离网环境下病毒查杀率较低的问题而发明。本发明的方法包括：服务器离线获取外网的病毒特征集合，所述病毒特征集合中包含预设时段内热点病毒文件的病毒特征；服务器根据所述病毒特征集合中的病毒特征更新病毒特征库；当终端请求病毒扫描时，服务器根据更新后的病毒特征库对终端侧的文件进行扫描。本发明主要应用于隔离网环境下的私有云查杀过程中。



CN 104281809 A

1. 一种病毒查杀的方法，其特征在于，所述方法包括：

离线获取外网的病毒特征集合，所述病毒特征集合中包含预设时段内热点病毒文件的病毒特征；

根据所述病毒特征集合中的病毒特征更新病毒特征库；

当终端请求病毒扫描时，根据更新后的病毒特征库对终端侧的文件进行扫描。

2. 根据权利要求 1 所述的方法，其特征在于，所述离线获取外网的病毒特征集合，包括：

通过离线工具与所述外网建立通信连接，并通过所述通信连接获取所述外网发送的所述病毒特征集合；

或者，与物理存储介质进行通信，读取物理存储介质存储的所述病毒特征集合；

或者，通过专用的物理链路获取所述外网发送的所述病毒特征集合；

或者，建立隔离沙箱，在所述隔离沙箱环境下通过已有通信连接获取所述外网发送的所述病毒特征集合。

3. 根据权利要求 2 所述的方法，其特征在于，所述离线获取外网的病毒特征集合，包括：

响应所述外网的更新请求，接收所述外网发送的所述病毒特征集合；

或者，按照预设时间间隔定期向所述外网请求所述病毒特征集合；

或者，在接收到终端上报的扫描请求时，向所述外网请求所述病毒特征集合；

或者，选择非忙时段接收所述外网发送的所述病毒特征集合；

或者，根据用户操作向所述外网请求所述病毒特征集合；

或者，根据预设规则向所述外网请求所述病毒特征集合。

4. 根据权利要求 1 所述的方法，其特征在于，所述根据所述病毒特征集合中的病毒特征更新病毒特征库，包括：

清空所述病毒特征库中的病毒特征，并写入所述病毒特征集合中的病毒特征；

或者，根据所述病毒特征集合中的病毒特征对所述病毒特征库进行增量更新。

5. 根据权利要求 1 所述的方法，其特征在于，所述根据更新后的病毒特征库对终端侧的文件进行扫描，包括：

接收所述终端上报的文件特征；

在更新后的病毒特征库中遍历所述文件特征；

若在更新后的病毒特征库中遍历到所述文件特征，则确定所述文件特征对应的文件为病毒文件。

6. 根据权利要求 5 所述的方法，其特征在于，若未在更新后的病毒特征库中遍历到所述文件特征，则所述方法进一步包括：

向所述外网离线发送所述文件特征；

离线接收所述外网对所述文件特征的扫描结果；

根据所述扫描结果对所述病毒特征库进行二次更新。

7. 根据权利要求 1 所述的方法，其特征在于，所述方法进一步包括：

离线获取外网的支持向量机引擎 SVM；

通过所述支持向量机引擎对的病毒样本进行分析，训练得到病毒特征模型；

根据所述病毒特征模型更新所述病毒特征库。

8. 根据权利要求 1 所述的方法，其特征在于，所述方法进一步包括：

离线获取外网的专杀脚本；

向所述终端下发所述专杀脚本，以对所述终端中的病毒文件进行查杀。

9. 一种病毒查杀的装置，其特征在于，所述装置包括：

获取单元，用于离线获取外网的病毒特征集合，所述病毒特征集合中包含预设时段内热点病毒文件的病毒特征；

更新单元，用于根据所述获取单元获取的所述病毒特征集合中的病毒特征更新病毒特征库；

处理单元，用于当终端请求病毒扫描时，根据所述更新单元更新后的病毒特征库对终端侧的文件进行扫描。

10. 一种病毒查杀的系统，其特征在于，所述系统为由服务器和终端组成的隔离网络；其中，所述服务器包括如权利要求 9 所述的装置；

所述服务器，用于离线获取外网的病毒特征集合，所述病毒特征集合中包含预设时段内热点病毒文件的病毒特征；根据所述病毒特征集合中的病毒特征更新病毒特征库；

所述终端，用于向所述服务器发送病毒扫描请求，所述病毒扫描请求中携带有终端中文件的文件特征；

所述服务器，还用于根据更新后的病毒特征库及所述终端发送的文件特征对终端侧的文件进行扫描，并向所述终端下发扫描结果，以便所述终端根据所述扫描结果对文件进行相应处理。

病毒查杀的方法、装置及系统

技术领域

[0001] 本发明涉及互联网技术领域，尤其涉及一种病毒查杀的方法、装置及系统。

背景技术

[0002] 随着计算机技术的不断发展及互联网的广泛应用，木马、病毒、插件等恶意程序也日益猖獗，用户隐私、数据安全及系统运行等方面面临着严重的挑战，计算机安全问题也成为人们关注的首要问题。

[0003] 在局域网内，终端可以通过局域网服务器（后续简称服务器）对本地的病毒文件进行云查杀。这种查杀方式需要服务器侧部署病毒特征库，通过黑白名单的形式对病毒文件进行记录，从而在终端上报文件特征时基于对黑白名单的比对实现病毒文件的识别。

[0004] 目前，出于数据安全的考虑，众多企业或组织开始对自己的运营体系部署隔离网。隔离网属于一种特殊的局域网，通过软件隔离或物理隔离的方式阻断与外网的数据交互，以防止商业秘密、国家机密等数据外泄。实际应用中，隔离网虽然能够对网内数据进行有效保护，但同样因为其数据隔离的特性，服务器无法通过外网对病毒特征库进行更新，所以隔离网内只能部署静态病毒特征库。静态病毒特征库中的病毒样本通常有限，无法应对不断变种的各类病毒，因此隔离网环境下的病毒查杀率往往较低。

发明内容

[0005] 鉴于上述问题，提出了本发明提供了一种病毒查杀的方法、装置及系统，能够解决隔离网环境下病毒查杀率较低的问题。

[0006] 为解决上述技术问题，第一方面，本发明提供了一种病毒查杀的方法，该方法包括：

[0007] 离线获取外网的病毒特征集合，病毒特征集合中包含预设时段内热点病毒文件的病毒特征；

[0008] 根据病毒特征集合中的病毒特征更新病毒特征库；

[0009] 当终端请求病毒扫描时，根据更新后的病毒特征库对终端侧的文件进行扫描。

[0010] 第二方面，本发明还提供了一种病毒查杀的装置，该装置包括：

[0011] 获取单元，用于离线获取外网的病毒特征集合，病毒特征集合中包含预设时段内热点病毒文件的病毒特征；

[0012] 更新单元，用于根据获取单元获取的病毒特征集合中的病毒特征更新病毒特征库；

[0013] 处理单元，用于当终端请求病毒扫描时，根据更新单元更新后的病毒特征库对终端侧的文件进行扫描。

[0014] 第三方面，本发明还提供了一种病毒查杀的系统，该系统为由服务器和终端组成的隔离网络；其中，服务器包括如前述第二方面中任一项的装置；

[0015] 服务器，用于离线获取外网的病毒特征集合，病毒特征集合中包含预设时段内热

点病毒文件的病毒特征；根据病毒特征集合中的病毒特征更新病毒特征库；

[0016] 终端，用于向服务器发送病毒扫描请求，病毒扫描请求中携带有终端中文件的文件特征；

[0017] 服务器，还用于根据更新后的病毒特征库及终端发送的文件特征对终端侧的文件进行扫描，并向终端下发扫描结果，以便终端根据扫描结果对文件进行相应处理。

[0018] 借由上述技术方案，本发明提供的病毒查杀的方法、装置及系统，能够在网络隔离环境下，由服务器离线获取外网的病毒特征集合，并根据病毒特征集合中的病毒特征更新病毒特征库。当终端请求病毒扫描时，服务器根据更新后的病毒特征库对终端侧的文件进行扫描。与现有技术相比，本发明能够在隔离网环境下，通过离线工具突破数据交互的限制，在不影响其他数据隔离状态的条件下，对本地的病毒特征库进行更新，由此提高隔离网环境下的病毒查杀率。

[0019] 上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

[0020] 通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

[0021] 图 1 示出了本发明实施例中一种病毒查杀的方法流程图；

[0022] 图 2 示出了本发明实施例中另一种病毒查杀的方法流程图；

[0023] 图 3 示出了本发明实施例中病毒特征集合与病毒特征库的句柄标识表；

[0024] 图 4 示出了本发明实施例中病毒特征库的示意图；

[0025] 图 5 示出了本发明实施例中一种病毒查杀的装置的结构示意图；

[0026] 图 6 示出了本发明实施例中另一种病毒查杀的装置的结构示意图；

[0027] 图 7 示出了本发明实施例中一种病毒查杀的系统示意图。

具体实施方式

[0028] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0029] 为解决隔离网环境下，因病毒特征库无法更新而导致的病毒查杀率较低的问题，本发明实施例提供了一种病毒查杀的方法，该方法主要应用隔离网环境下，基于服务器侧实现。如图 1 所示，该方法包括：

[0030] 101、服务器离线获取外网的病毒特征集合。

[0031] 在隔离网环境下，服务器通过离线工具获取外网的病毒特征集合，该病毒特征集合中包含预设时段内热点病毒文件的病毒特征。本实施例中所指的病毒特征主要是以特征码形式体现、用于表征病毒文件特性的描述性信息。实际应用中，病毒特征可以为病毒文件

的文件名、版本号、运行日志等，本实施例不对病毒特征的具体形式进行限定。

[0032] 本实施例中所指的病毒特征包括两类：1）病毒属性特征和 2）病毒行为特征。其中，病毒属性特征主要是指能够用于对病毒文件进行标记的描述性信息，包括但不限于是 MD5 值、数字签名、存储路径、文件名称、文件版本号、文件大小、文件摘要信息及文件类型，也可以是上述各信息中至少两种信息的组合（例如文件名称 + 文件版本号）；而病毒行为特征则主要是指能够在文件运行特点上对病毒文件特性予以标注的描述性信息，包括但不仅限于是“修改注册表”、“修改开机选项”、“篡改浏览器设置”等。本实施例仅对病毒属性特征和病毒行为特征进行示例性说明，不对其在实际应用中的具体形式进行限制。

[0033] 上述病毒特征集合的来自于外网，外网也可称作为公网或互联网 (Internet)，其概念是相对局域网而言的，本实施例中与外网相对应的是隔离网。在步骤 101 中，病毒特征集合的生成和下发策略均由外网决定，外网可以决定何种病毒文件为热点病毒文件、将何种时段内的热点病毒文件添加到病毒特征集合中以及病毒特征集合中病毒特征的种类、数量等所有涉及生成病毒特征集合的因素。示例性的，外网可以将本周内外网感染率排名前 100 名的病毒文件的病毒特征加入到病毒特征集合中，并发送给隔离网服务器。

[0034] 实际应用中，筛选热点病毒文件的标准可以是用户感染率，用户感染率的又可以由感染用户数量、感染局域网数量、病毒类型、病毒传播能力、病毒传播范围、感染持续时间、感染破坏力、感染对象等具体参数体现。本实施例不对热点病毒文件的具体定义以及热点病毒文件数量的确定进行限制。

[0035] 在外网生成病毒特征集合后，隔离网中的服务器通过离线工具获取该病毒特征集合。在获取病毒特征集合时，隔离网仍保持隔离状态，网内终端无法与外网进行数据交互。

[0036] 102、服务器根据病毒特征集合中的病毒特征更新病毒特征库。

[0037] 通常，服务器中会保存有记录病毒文件特性的病毒特征库，用以对终端文件进行云查杀。通常，由于数据隔离的特性，隔离网中的病毒特征库无法更新，即隔离网中只能部署静态病毒特征库。而在本实施例中，服务器可以通过步骤 101 从外网中获得用于特征库更新的病毒特征集合，并在本步骤中，根据获取的病毒特征集合对病毒特征库进行更新，由此实现隔离网环境下动态病毒特征库的部署，能够提升网络查杀能力。

[0038] 本实施例中，病毒特征库中记录的病毒特征与病毒特征集合中携带的病毒特征形式相同，服务器可以直接根据病毒特征集合中的病毒特征对病毒特征库进行更新。在进行病毒特征更新时，服务器可以实现的更新方式包括增量更新（增加病毒特征条目）、减量更新（删除病毒特征条目）以及变量更新（修改已有病毒特征条目）。

[0039] 此外，外网也可以预先对病毒特征集合中的病毒特征进行分类（例如按照病毒感染强度、感染对象、传播范围等因素分类），服务器在接收到病毒特征集合后，可以依次或并行对不同类型的病毒特征进行更新。

[0040] 进一步的，在更新时机上，服务器还可以被设定为多种不同的更新模式。例如，服务器可以在接收到病毒特征集合时进行更新，或选择非忙时段（例如午休或夜晚）进行更新，或一次性完成更新，或者分时段更新。

[0041] 本实施例仅对服务器更新病毒特征库的过程进行说明，不对具体的更新时机及更新方式进行限定。

[0042] 103、当终端请求病毒扫描时，服务器根据更新后的病毒特征库对终端侧的文件进

行扫描。

[0043] 在病毒特征库更新完成后，服务器保存更新后的病毒特征库，以便后续进行云查杀之用。当隔离网中某台终端上报查杀请求时，服务器根据更新后的病毒特征库对终端侧的文件进行扫描。

[0044] 本步骤中，服务器可以采用不同的查杀方式对终端中的文件进行扫描。示例性的，服务器可以从终端上报的查杀请求中读取终端文件的文件特征，在更新后的病毒特征库中查找该文件特征，并通过对查杀请求的响应向终端反馈查杀结果；或者，服务器还可以将部分或全部更新后的病毒特征库下发给终端，由终端根据下发的病毒特征库在本地侧进行病毒查杀。本实施例不对病毒查杀的过程进行限制。

[0045] 本实施例提供的病毒查杀的方法，能够在网络隔离环境下，由服务器离线获取外网的病毒特征集合，并根据病毒特征集合中的病毒特征更新病毒特征库。当终端请求病毒扫描时，服务器根据更新后的病毒特征库对终端侧的文件进行扫描。与现有技术相比，本实施例能够在隔离网环境下，通过离线工具突破数据交互的限制，在不影响其他数据隔离状态的条件下，对本地的病毒特征库进行更新，由此提高隔离网环境下的病毒查杀率。

[0046] 进一步的，作为对图 1 步骤 101 的细化，在本发明的另一实施例中，服务器可以采用不同方式离线获取病毒特征集合：

[0047] a、通过离线工具获取病毒特征集合

[0048] 服务器可以通过离线脚本工具与外网建立通信连接，并通过建立的通信连接获取外网发送的病毒特征集合。

[0049] 需要注意的是，在通过离线工具与外网建立通信连接时，需要保证该通信连接为专有连接，即该通信连接仅能下载病毒特征集合，外网中的其他数据无法通过该通信连接传输到隔离网中，并且隔离网内的其他数据信息也无法通过该通信连接传输到外网中。实际应用中，可以在服务器侧的路由器上进行设置，通过数据包解析的方式对涉及病毒特征集合的数据进行识别。

[0050] b、通过物理存储介质获取病毒特征集合

[0051] 在本实施例的另一种实现方式中，病毒特征集合还可以被固化到一个物理存储介质中，在获取病毒特征集合时，服务器与该物理存储介质进行通信，并读取物理存储介质存储的病毒特征集合。

[0052] 实际应用中，包含存储装置及输入输出装置的有源或无源设备均可用作为物理存储介质。在存储毒特征集合时，物理存储介质通过输入输出装置与外网设备（外网服务器或外网终端等）建立通信连接，写入病毒特征集合数据；而在导入病毒特征集合时，物理存储介质通过输入输出装置与隔离网服务器建立通信连接，从而读取其中保存的病毒特征集合。

[0053] 进一步的，为防止其他物理存储介质接入到隔离网中，在服务器与物理存储介质之间建立通信连接后，服务器侧的路由器还可以预先设置授权物理存储介质的 IP 地址，路由器可以通过 IP 地址对授权物理存储介质的身份进行识别，从而排除其他物理存储介质的接入。

[0054] 在本实施例的一个应用场景中，隔离网可以直接采用网络安全供应商提供的病毒特征更新硬件，并定期将该硬件返厂进行数据更新；而在本实施例的另一个应用场景中，隔

离网也可以使用普通的物理存储介质（如移动硬盘等）自行从外网获取病毒特征集合。

[0055] 需要说明的是，对于自行获取病毒特征集合的情况，为保证隔离网内的数据安全，应当在使用物理存储介质前对物理存储介质进行格式化处理，并且在向隔离网导入数据前，对物理存储介质中的文件数据进行较高等级的病毒查杀。

[0056] c、通过专用的物理链路获取病毒特征集合

[0057] 由于隔离网与外网之间已有的通信链路已被“切断”，因此隔离网还可以通过专有用于获取病毒特征集合的物理链路获取病毒特征集合。原则上，该物理链路与隔离网已有的链路同质，但仅能传输与病毒特征集合相关的数据。实际应用中，上述物理链路的形式可以为有线链路或无线链路，外网可以采用 TCP/IP 传输方式传输病毒特征集合。

[0058] 在本实施例的另一个应用场景中，对于无线链路传输方式，外网可以采用广播的形式向隔离网发送病毒特征集合，例如采用用户数据报协议 (User Datagram Protocol，简称 UDP) 的传输方式。该传输方式为广播传输，具有单向传输特性，能够阻止隔离网向外网传输数据，因此可以保证隔离网内的数据安全。

[0059] d、通过隔离沙箱获取病毒特征集合

[0060] 服务器可以在网络隔离状态下建立一个隔离沙箱，并在沙箱环境下解禁隔离网与外网之间的数据隔离。在沙箱环境下，服务器通过网络已有的通信连接获取外网发送的病毒特征集合。

[0061] 需要说明的是，在本实现方式中，服务器侧的路由器需要对沙箱环境下接收的数据包进行解析，防止与病毒特征集合无关的数据进入到隔离网中。此外，服务器还应当对沙箱环境下接收的数据进行查杀，保证隔离网的数据安全。

[0062] 本实施例提供的获取病毒特征集合的实现方式，能够采用不同的通信方式获取病毒特征集合，实际应用中可以针对不同的网络条件选择不同的获取方式，实现起来方便灵活。

[0063] 上述实施例对服务器获取病毒特征集合的方式进行了说明，进一步的，同样作为对图 1 步骤 101 的细化，本发明的另一实施例还提供了获取病毒特征集合的几种不同形式。本实施例所提供的病毒特征集合的获取形式既可以与前述实施例中病毒特征集合的获取方式进行结合实施，也可以单独与图 1 所示方法进行结合实施。具体的，本实施例中病毒特征集合的获取形式包括：

[0064] a、根据外网更新请求接收病毒特征集合

[0065] 本实现方式中，服务器可以在接收到外网发送的更新请求后立刻做出更新响应，对外网发送的病毒特征集合进行接收，即服务器接收病毒特征集合的时机由外网发送病毒特征集合的时刻决定。

[0066] b、周期性接收病毒特征集合

[0067] 本实现方式中，外网可以周期性对隔离网中的病毒特征库进行更新。外网预先与隔离网协商更新的时间间隔，在更新时间点上，外网向隔离网发送病毒特征集合，隔离网服务器接收外网发送的病毒特征集合。

[0068] c、在终端请求查杀时请求病毒特征集合

[0069] 本实现方式中，服务器获取病毒特征集合的时机由隔离网内终端请求进行查杀的时机决定，当有终端发送扫描请求时，服务器首先向外网请求病毒特征集合，然后再根据更

新后的病毒特征数据库对终端文件进行扫描。

[0070] d、选择非忙时段接收外网发送的病毒特征集合

[0071] 本实现方式中，为避免病毒特征库更新对隔离网带宽及处理资源的占用，外网还可以与服务器协商选择非忙时段更新病毒特征库。例如，服务器可以在午休时段接收外网发送的病毒特征集合，或者在夜间接收外网发送的病毒特征集合。

[0072] e、根据用户操作向外网请求病毒特征集合

[0073] 本实现方式中，服务器还可以允许网管人员手动进行病毒特征库的更新。当网管人员通过与服务器相连的人机交互平台输入更新指令时，服务器向外网请求接收病毒特征集合。

[0074] f、根据预设规则向外网请求病毒特征集合

[0075] 本实现方式中，服务器可以根据隔离网的具体情况制定和修改获取病毒特征集合的预设规则。该规则涉及病毒数量、病毒感染范围、病毒类型、病毒传播速度、病毒感染对象等不同因素。服务器通过对预设规则的设定可以实现对特定类型病毒特征对象的定向获取。例如，服务器可以通过对病毒数量的设置，限定病毒特征集合的大小；或者服务器可以通过对病毒类型的设置，限定仅对木马特征库进行更新。

[0076] 示例性的，以按病毒类型分类为例，服务器可以以病毒存在的媒介为分类规则，与外网协商获取网络病毒、文件病毒、引导型病毒、多型病毒中某种或某几种病毒的病毒特征。或者服务器也可以以病毒的传染方式为分类规则，与外网协商获取驻留型病毒或非驻留型病毒的病毒特征。再或者，服务器还可以以病毒的算法为分类规则，与外网协商获取伴随型病毒、寄生型病毒、蠕虫型病毒、诡秘型病毒、变异型病毒中某种或某几种病毒的病毒特征。再或者，服务器还可以简单的以病毒的种类为分类规则，与外网协商获取系统病毒、蠕虫病毒、木马病毒、黑客病毒、脚本病毒、宏病毒、后门病毒、病毒种植程序病毒、破坏程序病毒、玩笑病毒、捆绑机病毒等病毒的病毒特征。本实现方式仅对获取病毒特征集合的预设规则进行示例性说明，不作为对实际应用的限定。

[0077] 本实施例能够针对隔离网的现网条件和 / 或不同需求，制定不同集合获取形式，形式选择类型完善、机动灵活，适用于实际应用。

[0078] 进一步的，作为对上述各实施例的细化，本发明的另一个实施例还提供了一种病毒查杀的方法，用以对病毒特征库的更新以及文件扫描过程进行说明。如图 2 所示，该方法包括步骤 201 至步骤 205，其中步骤 201 和步骤 202 涉及病毒特征库的更新过程，步骤 203 至步骤 205 则涉及病毒的查杀过程：

[0079] 201、服务器离线获取外网的病毒特征集合。

[0080] 本步骤的实现方式与前述各实施例的实现方式相同，此处不再赘述。

[0081] 可选的，在本实施例的一种实现方式中，为保证病毒特征集合的数据安全，外网与服务器之间还可以基于预先协商的加密算法对病毒特征集合进行加密，本实施例不对传输病毒特征集合所采用的加密算法进行限定，示例性的，外网与服务器之间可以采用对称密钥或非对称密钥对病毒特征集合进行加解密处理。

[0082] 进一步可选的，通常外网与服务器之间传输病毒特征集合的数据量较大，为防止传输过大数据量对网络带宽的过度挤占，在本实施例的另一实现方式中，外网和服务器之间还可以对传输的病毒特征集合进行压缩 / 解压缩处理，由此减少网络之间的数据传输

量，节省网络的数据传输资源。

[0083] 202、服务器根据病毒特征集合中的病毒特征更新病毒特征库。

[0084] 如前所述，服务器对病毒特征库的更新方式包括增量更新、减量更新和变量更新。可选的，在本实施例的另一种实现方式中，服务器接收的病毒特征集合包含云查杀所需的所有病毒特征，服务器可以使用接收的病毒特征集合直接对病毒特征库进行整体替换。具体的，服务器在接收到病毒特征集合后，清空本地病毒特征库中的全部病毒特征，然后将病毒特征集合中的病毒特征写入到清空后的病毒特征库中。在写入病毒特征时，服务器可以事先从病毒特征集合中获取病毒特征的索引表或句柄标识表，根据病毒特征的索引或句柄标识将病毒特征集合中的病毒特征依次写入并保存到病毒特征库中，由此完成病毒特征库的更新。

[0085] 进一步的，为对本地病毒特征库进行积累和完善，以不断提高隔离网的云查杀能力，在本实施例的一种可选方式中，服务器还可以仅对病毒特征库进行增量更新，已达到不断扩充病毒特征库的目的。需要注意的是，在进行增量更新时，为避免集合中病毒特征的索引或句柄标识与病毒特征库中已存病毒特征的索引或句柄标识重复或冲突，服务器在将集合中的病毒特征写入到病毒特征库中之前，还可以预先读取病毒特征库的索引表或句柄标识表，并根据读取的索引表或句柄标识表对待写入的病毒特征重新进行索引排序或句柄排序，生成新的索引或句柄标识，最后再根据新的索引或句柄标识将集合中的病毒特征写入到病毒特征库中。

[0086] 本实施例中，外网依据自身标准生成的病毒特征集合可能与服务器侧病毒特征库之间存在部分病毒特征重合，重复的病毒特征不但占用宝贵服务器存储资源，其写入过程也会浪费一定的服务器处理资源，特别是在大量写入病毒特征时，过多重复病毒特征的写入会拖慢服务器的处理速度，影响隔离网中其他在线业务的正常运行。因此在本实施例的一种实现方式中，服务器在向病毒特征库中写入病毒特征之前，可以对病毒特征集合中的病毒特征进行去重处理，由此保证写入到病毒特征库中的病毒特征不会重复。

[0087] 在进行去重处理时，服务器可以分别从病毒特征集合和病毒特征库中逐条读取病毒特征进行比对。但更为快速且节省资源的实现方式为：通过索引表或句柄标识表对两者数据进行快速比对。以句柄标识表为例，如图 3 所示，服务器分别从病毒特征集合和病毒特征库中读取句柄标识表 1（病毒特征集合的句柄标识表）及句柄标识表 2（病毒特征库的句柄标识表）。然后服务器从句柄标识表 1 的第一个句柄标识开始依次与句柄标识表 2 进行比对。当当前句柄标识存在于句柄标识表 2 中时，将该句柄标识对应的病毒特征标记为“已存”状态。在完成句柄标识的遍历后，服务器删除病毒特征集合中被标记为“已存”的病毒特征删除，并将其他病毒特征写入到病毒特征库中。例如在图 3 中，句柄标识表 1 中的句柄标识“A”、“B”、“D”和“E”分别存在于句柄标识表 2 中，因此这些句柄标识对应的病毒特征无需写入到病毒特征库中。

[0088] 203、服务器接收终端上报的文件特征。

[0089] 步骤 201 和步骤 202 涉及病毒特征的更新过程，而从步骤 203 起，将对基于更新病毒特征库的病毒查杀过程进行介绍。

[0090] 如前所述，终端上报的文件特征与服务器记录的病毒特征在形式上相同，服务器可以直接根据文件特征与病毒特征之间的比对实现终端侧文件的云查杀。

[0091] 204、服务器在更新后的病毒特征库中遍历文件特征。

[0092] 若在更新后的病毒特征库中遍历到该文件特征，则服务器确定该文件特征对应的文件为病毒文件；若未在更新后的病毒特征库中遍历到该文件特征，则服务器确定该文件特征对应的文件为正常文件。示例性的，对于如图 4 所示的病毒特征库，当服务器接收的文件特征为“13hf4”时（在病毒特征库中出现），该文件特征对应的文件为病毒文件，而当服务器接收的文件特征为“fdk67”时（未在病毒特征库中出现），该文件特征对应的文件为正常文件。

[0093] 实际应用中，服务器在对病毒特征库更新完成之前，有可能会接收到终端上报的扫描请求。对于此种情况，如若等待病毒特征库更新完成后再响应扫描请求，则会产生较长的业务延时，不利于终端侧的用户业务体验。因此，为解决此问题，在本实施例的另一种实现方式中，服务器还可以在病毒特征库更新完成前，依据原病毒特征库对终端上报的扫描请求进行响应。具体的，服务器在执行步骤 202 之前，可以先对原病毒特征库进行备份，获得备份病毒特征库。当进行病毒特征库更新时，作为对步骤 202 的替换，服务器依据病毒特征集合对备份病毒特征库进行更新，同时通过原病毒特征库响应终端的扫描请求。在文件扫描及病毒特征库更新两者较后完成者完成时，服务器根据更新后的病毒特征库对原病毒特征库进行替换，由此完成病毒特征库的更新。

[0094] 205、服务器向终端下发文件扫描结果。

[0095] 在进行文件特征扫描后，服务器将文件扫描结果下发给终端，以便终端根据文件扫描结果对扫描文件进行相应处理。对于正常文件，终端不对其做任何处理，正常文件可以在终端上继续运行，而对于病毒文件，终端对其进行隔离或删除，并可以向服务器请求该病毒文件的替换文件已对其进行文件修复。同时，终端还可以向用户输出接收的文件扫描结果以及病毒文件的处理结果。

[0096] 上述各实施例涉及的云查杀过程是基于服务器实现的，这种基于隔离网的云查杀过程也被称为私有云查杀。进一步的，当因病毒特征库样本有限或者出现新型变异病毒，以导致服务器未在更新后的病毒特征库中遍历到文件特征时，服务器还可以将终端上报的文件特征发送给外网进行查杀。与私有云查杀相对应的，这种由外网进行病毒查杀过程被称作公有云查杀。服务器在向外网离线发送文件特征之后，离线接收外网对文件特征的扫描结果，该扫描结果用于反应文件特征对应的文件是否为病毒文件。在接收到外网的扫描结果后，服务器将该扫描结果下发给终端，以便终端根据该结果对扫描文件进行相应操作，同时服务器根据接收的扫描结果对本地的病毒特征库进行二次更新，当终端日后再请求相同文件特征的扫描请求时，服务器就可以基于本地的病毒特征库对该文件特征进行扫描了。

[0097] 在向外网上报文件特征时，服务器可以逐条进行上报，也可以在本地将多条文件特征添加到灰名单中，并将灰名单上报给外网。本实施例中所述的灰名单是相对黑名单和白名单而言的。实际应用中，黑名单通常用于记录病毒文件的文件特征（即病毒特征），相当于本实施例中所述的病毒特征库，白名单主要用于记录正常文件的文件特征，而灰名单则介于黑白名单之间，用于记录既未记录于黑名单也未记录于白名单中的“未知”文件特征。本实施例中，服务器可以通过灰名单将本地安全性未知的文件特征上报给外网进行扫描。

[0098] 进一步的，本发明上述各实施例均是以更新病毒特征库进行的说明，即相当于对

黑名单进行的更新。实际应用中与上述实施例实现方式类似的，服务器还可以对本地保存的白名单进行离线更新，并基于更新后的白名单对终端侧文件进行扫描。而在另一种实现方式中，更加适用于实际需求的是，服务器可以对黑白名单均进行更新，并基于更新后的黑白名单进行文件扫描。

[0099] 再进一步的，服务器还可以允许网管人员对更新前后的黑白名单进行设置，这种设置包括增加特征条目、删除特征条目以及修改特征条目。服务器通过连接的人机交互平台接收网管人员输入的操作指令，并向网管人员展示操作结果。

[0100] 以上各实施例对本发明中更新病毒特征库以及基于更新后病毒特征库的文件扫描过程进行了详细介绍。进一步的，为提高隔离网内部病毒特征库的建模能力、减少离线更新病毒特征库的次数，与前述各实施例相结合的，在本发明的另一个实施例中，服务器还可以离线获取外网的支持向量机引擎(Support Vector Machine，简称SVM)，通过支持向量机引擎对的病毒样本进行分析，训练得到病毒特征模型，并根据病毒特征模型更新病毒特征库。支持向量机引擎是一种具有“自学习”、“自进化”能力的安全引擎，能够基于病毒特征样本自动学习训练病毒检测模型。与传统的病毒特征库相比，支持向量机引擎不仅可以对已有的病毒文件进行查杀，还可以通过病毒检测模型预测并查杀未知病毒（例如变异型病毒等），无需频繁更新病毒特征库，且相比病毒特征库而言病毒查杀率更高。将支持向量机引擎部署在隔离网中，可以减少服务器与外网的数据交互频度，降低数据外泄的安全隐患。在本实施例的一种实现方式中，上述支持向量机引擎具体可以但不限于为奇虎支持向量机引擎(Qihoo Support Vector Machine，简称QVM)。

[0101] 再进一步的，在上述各实施例中，云查杀的过程仅仅用于对病毒文件进行识别，而病毒文件的处理则需要隔离网终端自行执行。对于某些顽固型病毒而言（例如木马病毒），终端可能不具备彻底清理病毒文件的能力，因此在本发明的另一实施例中，服务器还可以在识别病毒文件的基础上，进一步离线获取外网的专杀脚本，并将获取的专杀脚本下发给终端，以对终端中的病毒文件进行查杀。终端在接收到服务器下发的专杀脚本后，直接运行该专杀脚本文件，就可以直接对病毒文件进行隔离或清除，使用起来方便快捷，安全性更高。

[0102] 在本实施例的一种实现方式中，服务器可以获取并为终端配置LUA专杀脚本。LUA脚本语言是一种轻量语言，能够嵌入到应用程序中，具有体积小、启动速度快等特点。通过LUA脚本语言配置专杀脚本文件，可以提高专杀脚本的灵活性和扩展性，更加适用于隔离网等小范围局域网场景中。

[0103] 进一步的，作为对上述各方法实施例的实现，本发明另一个实施例还提供了一种病毒查杀的装置，该装置位于隔离网中的服务器内部，或者位于服务器外部但与服务器之间具有数据交互关系。如图5所示，该装置包括：获取单元51、更新单元52、处理单元53，其中，

[0104] 获取单元51，用于离线获取外网的病毒特征集合，病毒特征集合中包含预设时段内热点病毒文件的病毒特征；

[0105] 更新单元52，用于根据获取单元51获取的病毒特征集合中的病毒特征更新病毒特征库；

[0106] 处理单元53，用于当终端请求病毒扫描时，根据更新单元52更新后的病毒特征库

对终端侧的文件进行扫描。

[0107] 进一步的，如图 6 所示，获取单元 51，包括：

[0108] 工具获取模块 511，用于通过离线工具与外网建立通信连接，并通过通信连接获取外网发送的病毒特征集合；

[0109] 介质获取模块 512，用于与物理存储介质进行通信，读取物理存储介质存储的病毒特征集合；

[0110] 物理获取模块 513，用于通过专用的物理链路获取外网发送的病毒特征集合；

[0111] 沙箱获取模块 514，用于建立隔离沙箱，在隔离沙箱环境下通过已有通信连接获取外网发送的病毒特征集合。

[0112] 进一步的，获取单元 51，用于：

[0113] 响应外网的更新请求，接收外网发送的病毒特征集合；

[0114] 按照预设时间间隔定期向外网请求病毒特征集合；

[0115] 在接收到终端上报的扫描请求时，向外网请求病毒特征集合；

[0116] 选择非忙时段接收外网发送的病毒特征集合；

[0117] 根据用户操作向外网请求病毒特征集合；

[0118] 根据预设规则向外网请求病毒特征集合。

[0119] 进一步的，如图 6 所示，更新单元 52，包括：

[0120] 替换更新模块 521，用于清空病毒特征库中的病毒特征，并写入病毒特征集合中的病毒特征；

[0121] 增量更新模块 522，用于根据病毒特征集合中的病毒特征对病毒特征库进行增量更新。

[0122] 进一步的，如图 6 所示，处理单元 53，包括：

[0123] 接收模块 531，用于接收终端上报的文件特征；

[0124] 遍历模块 532，用于在更新后的病毒特征库中遍历接收模块 531 接收的文件特征；

[0125] 确定模块 533，用于当遍历模块 532 在更新后的病毒特征库中遍历到文件特征时，确定接收模块 531 接收的文件特征对应的文件为病毒文件。

[0126] 进一步的，如图 6 所示，该装置还包括：

[0127] 发送单元 54，用于当遍历模块 532 未在更新后的病毒特征库中遍历到文件特征时，向外网离线发送接收模块 531 接收的文件特征；

[0128] 获取单元 51，还用于离线接收外网对发送单元 54 发送的文件特征的扫描结果；

[0129] 更新单元 52，还用于根据获取单元 51 获取的扫描结果对病毒特征库进行二次更新。

[0130] 进一步的，如图 6 所示，该装置还包括：分析单元 55；

[0131] 获取单元 51，用于离线获取外网的支持向量机引擎 SVM；

[0132] 分析单元 55，用于通过获取单元 51 获取的支持向量机引擎对的病毒样本进行分析，训练得到病毒特征模型；

[0133] 更新单元 52，用于根据分析单元 55 分析得出的病毒特征模型更新病毒特征库。

[0134] 进一步的，如图 6 所示，该装置还包括：通信单元 56；

[0135] 获取单元 51，还用于离线获取外网的专杀脚本；

[0136] 通信单元 56，用于向终端下发获取单元 51 获取的专杀脚本，以对终端中的病毒文件进行查杀。

[0137] 进一步的，获取单元 51 获取的专杀脚本为 LUA 专杀脚本。

[0138] 进一步的，获取单元 51 获取的病毒特征包括：病毒属性特征和病毒行为特征。

[0139] 本实施例提供的病毒查杀的装置，能够在网络隔离环境下，由服务器离线获取外网的病毒特征集合，并根据病毒特征集合中的病毒特征更新病毒特征库。当终端请求病毒扫描时，服务器根据更新后的病毒特征库对终端侧的文件进行扫描。与现有技术相比，本实施例提供的装置能够在隔离网环境下，通过离线工具突破数据交互的限制，在不影响其他数据隔离状态的条件下，对本地的病毒特征库进行更新，由此提高隔离网环境下的病毒查杀率。

[0140] 进一步的，作为对上述各方法实施例的实现，本发明另一实施例还提供了一种病毒查杀的系统。如图 7 所示，该系统包括服务器 71 和终端 72，其中，服务器 71 包含或连接如图 5 或图 6 所示的装置。其中，

[0141] 服务器 71，用于离线获取外网的病毒特征集合，病毒特征集合中包含预设时段内热点病毒文件的病毒特征；根据病毒特征集合中的病毒特征更新病毒特征库；

[0142] 终端 72，用于向服务器 71 发送病毒扫描请求，病毒扫描请求中携带有终端 72 中文件的文件特征；

[0143] 服务器 71，还用于根据更新后的病毒特征库及终端 72 发送的文件特征对终端 72 侧的文件进行扫描，并向终端 72 下发扫描结果，以便终端 72 根据扫描结果对文件进行相应处理。

[0144] 本实施例提供的病毒查杀的系统，能够在网络隔离环境下，由服务器离线获取外网的病毒特征集合，并根据病毒特征集合中的病毒特征更新病毒特征库。当终端请求病毒扫描时，服务器根据更新后的病毒特征库对终端侧的文件进行扫描。与现有技术相比，本实施例提供的系统能够在隔离网环境下，通过离线工具突破数据交互的限制，在不影响其他数据隔离状态的条件下，对本地的病毒特征库进行更新，由此提高隔离网环境下的病毒查杀率。

[0145] 本发明的实施例还公开了：

[0146] A1、一种病毒查杀的方法，其特征在于，所述方法包括：

[0147] 离线获取外网的病毒特征集合，所述病毒特征集合中包含预设时段内热点病毒文件的病毒特征；

[0148] 根据所述病毒特征集合中的病毒特征更新病毒特征库；

[0149] 当终端请求病毒扫描时，根据更新后的病毒特征库对终端侧的文件进行扫描。

[0150] A2、根据权利要求 A1 所述的方法，其特征在于，所述离线获取外网的病毒特征集合，包括：

[0151] 通过离线工具与所述外网建立通信连接，并通过所述通信连接获取所述外网发送的所述病毒特征集合；

[0152] 或者，与物理存储介质进行通信，读取物理存储介质存储的所述病毒特征集合；

[0153] 或者，通过专用的物理链路获取所述外网发送的所述病毒特征集合；

[0154] 或者，建立隔离沙箱，在所述隔离沙箱环境下通过已有通信连接获取所述外网发

送的所述病毒特征集合。

[0155] A3、根据权利要求 A2 所述的方法，其特征在于，所述离线获取外网的病毒特征集合，包括：

[0156] 响应所述外网的更新请求，接收所述外网发送的所述病毒特征集合；

[0157] 或者，按照预设时间间隔定期向所述外网请求所述病毒特征集合；

[0158] 或者，在接收到终端上报的扫描请求时，向所述外网请求所述病毒特征集合；

[0159] 或者，选择非忙时段接收所述外网发送的所述病毒特征集合；

[0160] 或者，根据用户操作向所述外网请求所述病毒特征集合；

[0161] 或者，根据预设规则向所述外网请求所述病毒特征集合。

[0162] A4、根据权利要求 A1 所述的方法，其特征在于，所述根据所述病毒特征集合中的病毒特征更新病毒特征库，包括：

[0163] 清空所述病毒特征库中的病毒特征，并写入所述病毒特征集合中的病毒特征；

[0164] 或者，根据所述病毒特征集合中的病毒特征对所述病毒特征库进行增量更新。

[0165] A5、根据权利要求 A1 所述的方法，其特征在于，所述根据更新后的病毒特征库对终端侧的文件进行扫描，包括：

[0166] 接收所述终端上报的文件特征；

[0167] 在更新后的病毒特征库中遍历所述文件特征；

[0168] 若在更新后的病毒特征库中遍历到所述文件特征，则确定所述文件特征对应的文件为病毒文件。

[0169] A6、根据权利要求 A5 所述的方法，其特征在于，若未在更新后的病毒特征库中遍历到所述文件特征，则所述方法进一步包括：

[0170] 向所述外网离线发送所述文件特征；

[0171] 离线接收所述外网对所述文件特征的扫描结果；

[0172] 根据所述扫描结果对所述病毒特征库进行二次更新。

[0173] A7、根据权利要求 A1 所述的方法，其特征在于，所述方法进一步包括：

[0174] 离线获取外网的支持向量机引擎 SVM；

[0175] 通过所述支持向量机引擎对的病毒样本进行分析，训练得到病毒特征模型；

[0176] 根据所述病毒特征模型更新所述病毒特征库。

[0177] A8、根据权利要求 A1 所述的方法，其特征在于，所述方法进一步包括：

[0178] 离线获取外网的专杀脚本；

[0179] 向所述终端下发所述专杀脚本，以对所述终端中的病毒文件进行查杀。

[0180] A9、根据权利要求 A8 所述的方法，其特征在于，所述专杀脚本为 LUA 专杀脚本。

[0181] A10、根据权利要求 A1 至 A9 中任一项所述的方法，其特征在于，所述病毒特征包括：病毒属性特征和病毒行为特征。

[0182] B11、一种病毒查杀的装置，其特征在于，所述装置包括：

[0183] 获取单元，用于离线获取外网的病毒特征集合，所述病毒特征集合中包含预设时段内热点病毒文件的病毒特征；

[0184] 更新单元，用于根据所述获取单元获取的所述病毒特征集合中的病毒特征更新病毒特征库；

[0185] 处理单元，用于当终端请求病毒扫描时，根据所述更新单元更新后的病毒特征库对终端侧的文件进行扫描。

[0186] B12、根据权利要求 B11 所述的装置，其特征在于，所述获取单元，包括：

[0187] 工具获取模块，用于通过离线工具与所述外网建立通信连接，并通过所述通信连接获取所述外网发送的所述病毒特征集合；

[0188] 介质获取模块，用于与物理存储介质进行通信，读取物理存储介质存储的所述病毒特征集合；

[0189] 物理获取模块，用于通过专用的物理链路获取所述外网发送的所述病毒特征集合；

[0190] 沙箱获取模块，用于建立隔离沙箱，在所述隔离沙箱环境下通过已有通信连接获取所述外网发送的所述病毒特征集合。

[0191] B13、根据权利要求 B12 所述的装置，其特征在于，所述获取单元，用于：

[0192] 响应所述外网的更新请求，接收所述外网发送的所述病毒特征集合；

[0193] 按照预设时间间隔定期向所述外网请求所述病毒特征集合；

[0194] 在接收到终端上报的扫描请求时，向所述外网请求所述病毒特征集合；

[0195] 选择非忙时段接收所述外网发送的所述病毒特征集合；

[0196] 根据用户操作向所述外网请求所述病毒特征集合；

[0197] 根据预设规则向所述外网请求所述病毒特征集合。

[0198] B14、根据权利要求 B11 所述的装置，其特征在于，所述更新单元，包括：

[0199] 替换更新模块，用于清空所述病毒特征库中的病毒特征，并写入所述病毒特征集合中的病毒特征；

[0200] 增量更新模块，用于根据所述病毒特征集合中的病毒特征对所述病毒特征库进行增量更新。

[0201] B15、根据权利要求 B11 所述的装置，其特征在于，所述处理单元，包括：

[0202] 接收模块，用于接收所述终端上报的文件特征；

[0203] 遍历模块，用于在更新后的病毒特征库中遍历所述接收模块接收的所述文件特征；

[0204] 确定模块，用于当所述遍历模块在更新后的病毒特征库中遍历到所述文件特征时，确定所述接收模块接收的所述文件特征对应的文件为病毒文件。

[0205] B16、根据权利要求 B15 所述的装置，其特征在于，所述装置还包括：

[0206] 发送单元，用于当所述遍历模块未在更新后的病毒特征库中遍历到所述文件特征时，向所述外网离线发送所述接收模块接收的所述文件特征；

[0207] 所述获取单元，还用于离线接收所述外网对所述发送单元发送的所述文件特征的扫描结果；

[0208] 所述更新单元，还用于根据所述获取单元获取的所述扫描结果对所述病毒特征库进行二次更新。

[0209] B17、根据权利要求 B11 所述的装置，其特征在于，所述装置还包括：分析单元；

[0210] 所述获取单元，用于离线获取外网的支持向量机引擎 SVM；

[0211] 所述分析单元，用于通过所述获取单元获取的所述支持向量机引擎对的病毒样本

进行分析，训练得到病毒特征模型；

[0212] 所述更新单元，用于根据所述分析单元分析得出的所述病毒特征模型更新所述病毒特征库。

[0213] B18、根据权利要求 B11 所述的装置，其特征在于，所述装置还包括：通信单元；

[0214] 所述获取单元，还用于离线获取外网的专杀脚本；

[0215] 所述通信单元，用于向所述终端下发所述获取单元获取的所述专杀脚本，以对所述终端中的病毒文件进行查杀。

[0216] B19、根据权利要求 B18 所述的装置，其特征在于，所述获取单元获取的所述专杀脚本为 LUA 专杀脚本。

[0217] B20、根据权利要求 B11 至 B19 中任一项所述的装置，其特征在于，所述获取单元获取的所述病毒特征包括：病毒属性特征和病毒行为特征。

[0218] C21、一种病毒查杀的系统，其特征在于，所述系统为由服务器和终端组成的隔离网络；其中，所述服务器包括如权利要求 11 至权利要求 20 中任一项所述的装置；

[0219] 所述服务器，用于离线获取外网的病毒特征集合，所述病毒特征集合中包含预设时段内热点病毒文件的病毒特征；根据所述病毒特征集合中的病毒特征更新病毒特征库；

[0220] 所述终端，用于向所述服务器发送病毒扫描请求，所述病毒扫描请求中携带有终端中文件的文件特征；

[0221] 所述服务器，还用于根据更新后的病毒特征库及所述终端发送的文件特征对终端侧的文件进行扫描，并向所述终端下发扫描结果，以便所述终端根据所述扫描结果对文件进行相应处理。

[0222] 在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其他实施例的相关描述。

[0223] 可以理解的是，上述方法及装置中的相关特征可以相互参考。另外，上述实施例中的“第一”、“第二”等是用于区分各实施例，而并不代表各实施例的优劣。

[0224] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统，装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0225] 在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

[0226] 在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

[0227] 类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，

遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

[0228] 本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和／或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0229] 此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0230] 本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据本发明实施例的发明名称（如确定网站内链接等级的装置）中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

[0231] 应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

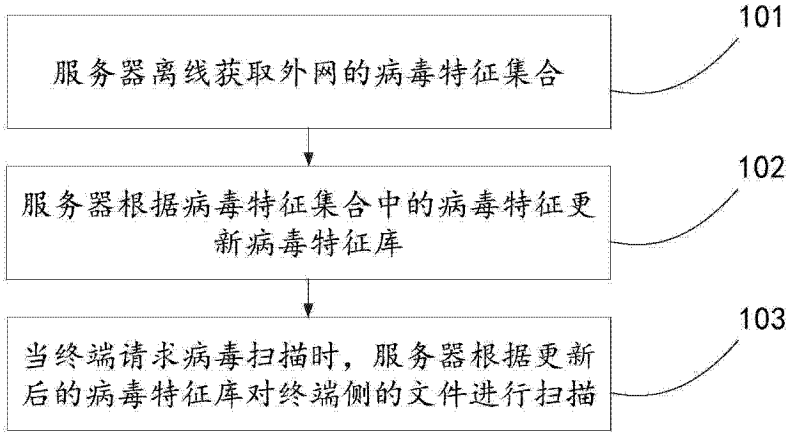

服务器离线获取外网的病毒特征集合
101
服务器根据病毒特征集合中的病毒特征更新病毒特征库
102
当终端请求病毒扫描时，服务器根据更新后的病毒特征库对终端侧的文件进行扫描
103

图 1

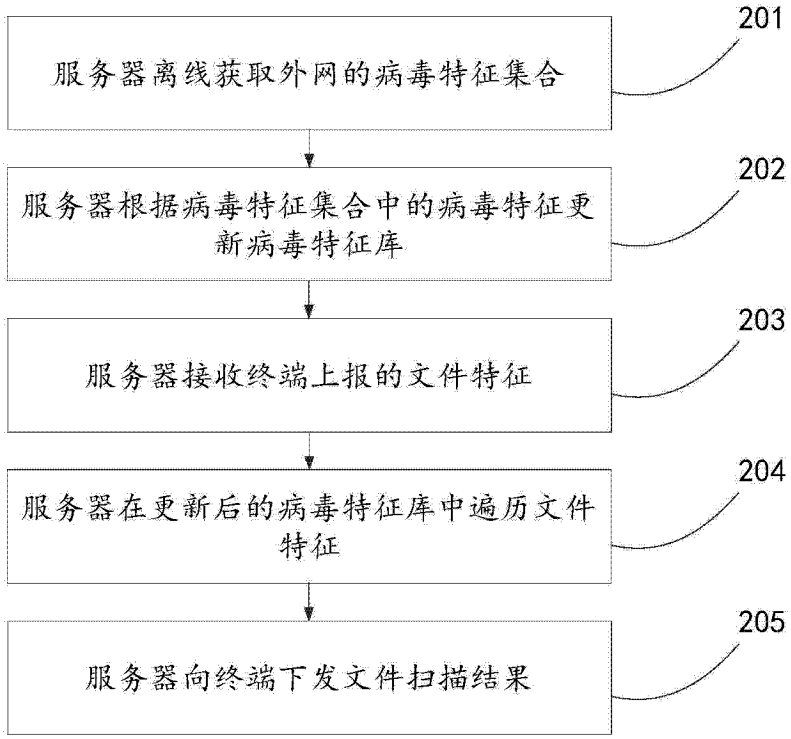

服务器离线获取外网的病毒特征集合
201
服务器根据病毒特征集合中的病毒特征更新病毒特征库
202
服务器接收终端上报的文件特征
203
服务器在更新后的病毒特征库中遍历文件特征
204
服务器向终端下发文件扫描结果
205

图 2

句柄标识	病毒特征
A	df3S5
B	5xDFG
C	D3sfA
D	dh54k
E	30MNz
F	fh793

句柄标识表1

句柄标识	病毒特征
V	XZ340
A	df3S5
B	5xDFG
X	zcx53
D	dh54k
E	30MNz

句柄标识表2

图 3

句柄标识	病毒特征
M	SAFs4
V	XZ340
A	df3S5
i	35724
B	5xDFG
G	cxvjf
X	zcx53
g	13hf4
D	dh54k
E	30MNz

图 4

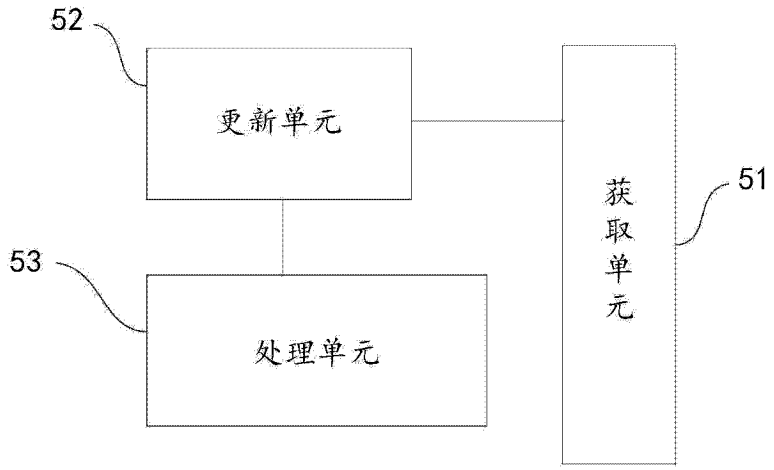

52
更新单元
获取单元
51
53
处理单元

图 5

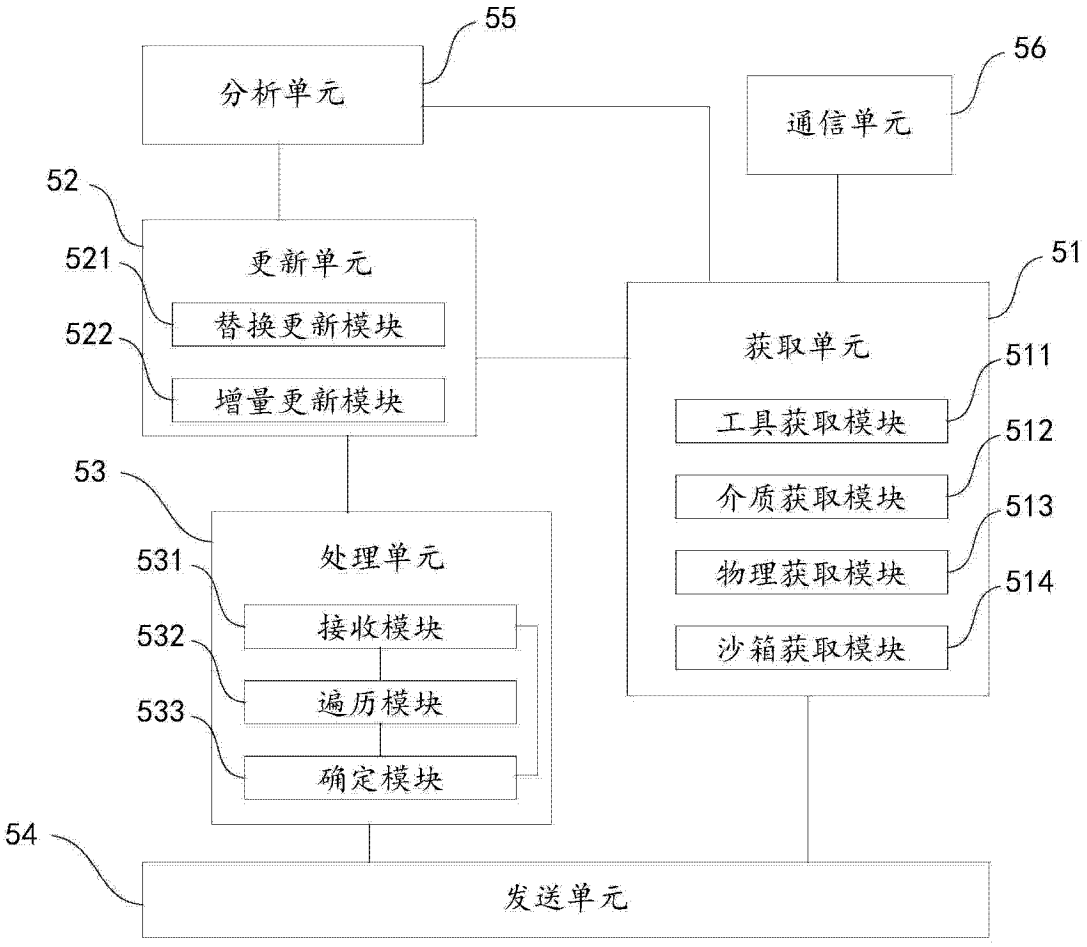

55
分析单元
56
通信单元
52
更新单元
521
替换更新模块
522
增量更新模块
51
获取单元
511
工具获取模块
512
介质获取模块
513
物理获取模块
514
沙箱获取模块
53
处理单元
531
接收模块
532
遍历模块
533
确定模块
54
发送单元

图 6

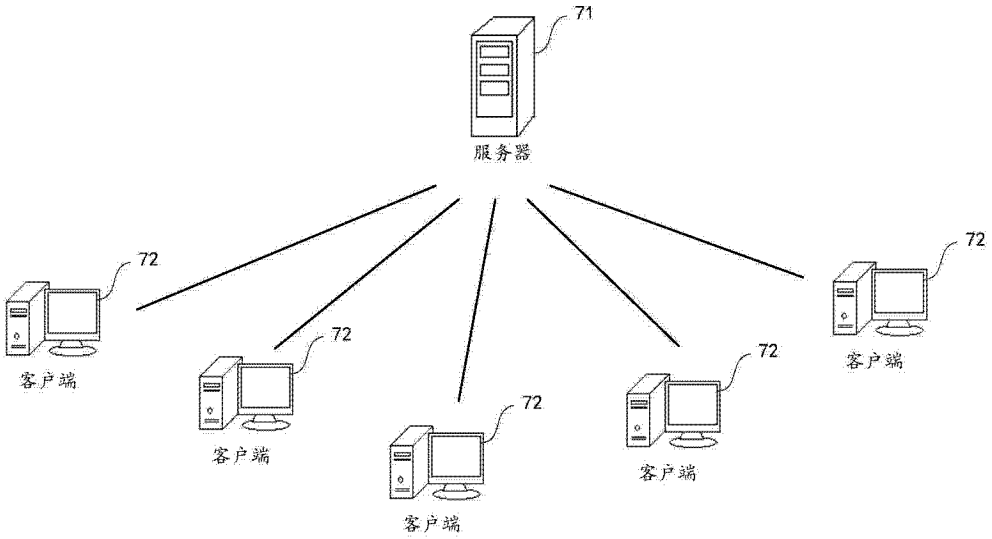


图 7