(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 106709352 B
(45)授权公告日 2019.09.24

(21)申请号 201510771668.0

(22)申请日 2015.11.12

(65)同一申请的已公布的文献号
申请公布号 CN 106709352 A

(43)申请公布日 2017.05.24

(73)专利权人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼资本大厦一座四层847号邮箱

(72)发明人 季玉超

(74)专利代理机构 北京三友知识产权代理有限公司 11127
代理人 李辉

(51)Int.Cl.
G06F 21/57(2013.01)
G06F 21/56(2013.01)

(56)对比文件
CN 103761481 A,2014.04.30,
CN 104182688 A,2014.12.03,
CN 103839005 A,2014.06.04,
CN 104751057 A,2015.07.01,
CN 103902909 A,2014.07.02,
CN 102737188 A,2012.10.17,
CN 104598824 A,2015.05.06,
CN 103049696 A,2013.04.17,
US 8656338 B2,2014.02.18,

审查员 刘婷

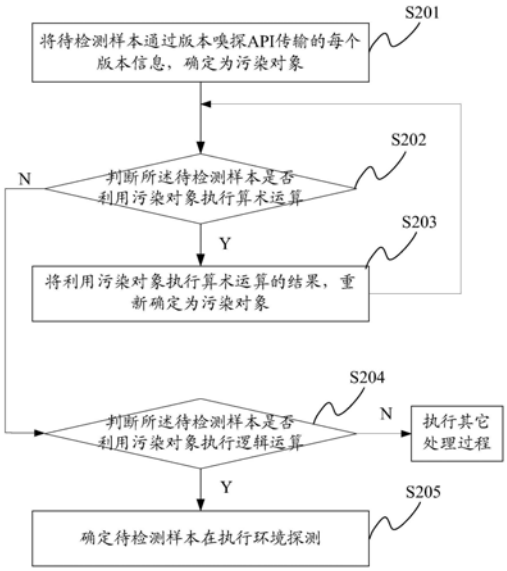
权利要求书2页 说明书9页 附图3页

(54)发明名称

样本处理方法、装置及系统

(57)摘要

本申请提供了一种样本处理方法、装置及系统，其中方法包括：将待检测样本通过版本嗅探API传输的每个版本信息，确定为污染对象；其中，所述版本嗅探API为待检测样本与控制端对接的应用程序接口；在所述待检测样本利用任一污染对象执行逻辑运算的情况下，确定所述待检测样本在执行环境探测。本申请将通过版本嗅探API传输的版本信息作为污染对象，所以本申请无论待检测样本是否变形，均可以准确检测到待检测样本是否有执行环境探测，从而可以在确定待检测样本执行环境探测后，用其它方法来进一步确定待检测样本是否为恶意样本。



CN 106709352 B

1.一种样本处理方法,其特征在于,包括:

将待检测样本通过版本嗅探API传输的每个版本信息,确定为污染对象;其中,所述版本嗅探API为待检测样本与控制端对接的应用程序接口;

在所述待检测样本利用任一污染对象执行逻辑运算的情况下,确定所述待检测样本在执行环境探测;

还包括:

在所述待检测样本利用任一污染对象执行算术运算的情况下,将利用该污染对象执行算术运算的结果,重新确定为污染对象。

2.如权利要求1所述的方法,其特征在于,在所述将待检测样本通过版本嗅探API传输的每个版本信息,确定为污染对象之前,还包括:

获取终端上传的待检测样本;或,

在终端上抓取待检测样本。

3.一种样本处理装置,其特征在于,包括:

确定污染对象单元,用于将待检测样本通过版本嗅探API传输的每个版本信息,确定为污染对象;其中,所述版本嗅探API为待检测样本与控制端对接的应用程序接口;

确定探测单元,用于在所述待检测样本利用任一污染对象执行逻辑运算的情况下,确定所述待检测样本在执行环境探测;

还包括:

重新确定污染对象单元,用于在所述待检测样本利用任一污染对象执行算术运算的情况下,将利用该污染对象执行算术运算的结果,重新确定为污染对象。

4.如权利要求3所述的装置,其特征在于,还包括:

获取单元,用于获取终端上传的待检测样本;或,在终端上抓取待检测样本。

5.一种样本处理系统,其特征在于,包括:

多个终端,与所述多个终端相连的服务器;

所述服务器,用于获取待检测样本,并且针对每个待检测样本执行以下步骤:将待检测样本通过版本嗅探API传输的每个版本信息,确定为污染对象;其中,所述版本嗅探API为待检测样本与控制端对接的应用程序接口;在所述待检测样本利用任一污染对象执行逻辑运算的情况下,确定所述待检测样本在执行环境探测;

所述服务器,还用于在所述待检测样本利用任一污染对象执行算术运算的情况下,将利用该污染对象执行算术运算的结果,重新确定为污染对象。

6.如权利要求5所述的系统,其特征在于,

所述服务器,还用于获取终端上传的待检测样本;或,在终端上抓取待检测样本。

7.一种样本处理系统,其特征在于,包括:

终端,用于获取待检测样本,并且针对每个待检测样本执行下述步骤:将待检测样本通过版本嗅探API传输的每个版本信息,确定为污染对象;其中,所述版本嗅探API为待检测样本与控制端对接的应用程序接口;在所述待检测样本利用任一污染对象执行逻辑运算的情况下,确定所述待检测样本在执行环境探测;

所述终端,还用于在所述待检测样本利用任一污染对象执行算术运算的情况下,将利用该污染对象执行算术运算的结果,重新确定为污染对象。

8.如权利要求7所述的系统,其特征在于,

所述终端,还用于在与之相连的其它终端或服务器上获取待检测样本。

样本处理方法、装置及系统

技术领域

[0001] 本申请涉及网络安全技术领域，尤其涉及一种样本处理方法、装置及系统。

背景技术

[0002] 随着智能设备的不断增加，适用于智能设备的应用也不断增加。由于应用可以方便用户生活，所以许多用户会将应用安装至智能设备中。正因为如此，应用也被攻击者所热衷。攻击者可以利用应用的脚本语言所存在的漏洞，利用异常样本通过应用漏洞来获取终端的控制权，以达到任意执行异常样本的目的。由于异常样本中存在很多异常代码，所以在智能终端中任意执行异常样本，会对智能设备的应用系统和信息安全造成严重威胁。

[0003] 以应用为flash播放器为例，目前绝大部分的智能设备上均安装有flash播放器。flash播放器可以用于播放flash样本，flash样本为通常所见的视频文件。攻击者可以利用flash播放器的脚本语言所存在的漏洞，使用异常flash样本来获取终端的控制权，以达到任意执行异常flash样本的目的。

[0004] 目前，环境探测技术是利用异常样本攻击智能设备时，所经常使用的技术手段。环境探测大体执行过程为：异常样本检测智能设备的版本信息，只有在智能设备的版本信息满足特定条件下，异常样本才会释放真正的异常代码，以便提高漏洞利用成功率。

发明内容

[0005] 本申请发明人经研究发现：异常样本执行环境探测的过程为：异常样本判断其在智能设备获取的版本信息集合是否满足特定条件。由于具有判断过程，所以异常样本在环境探测过程中必然会将版本信息集合进行对比匹配过程。由于对比匹配过程均属于逻辑运算(等于、不等于、大于、小于和是否等运算均属于逻辑运算)，所以，环境探测过程在软件程序体现上为逻辑运算。

[0006] 目前异常样本为了躲避智能设备的检测，异常样本采用变形的手段来执行环境探测。具体而言：由于智能设备判定一个待检测样本是否执行环境探测的依据为：待检测样本依据版本信息集合进行逻辑运算。因此，异常样本为了躲避智能设备的检测，会将版本信息集合先进行算术运算，以将版本信息集合变形为其它信息。然后，再将其它信息进行逻辑运算，以躲避智能设备对版本信息集合进行逻辑运算的检测，从而躲避智能设备的检测。

[0007] 在异常样本将版本信息集合进行变形之后，智能设备中现有的检测手段只能检测到异常样本在执行逻辑运算，而无法识别出异常样本在执行环境探测(因为异常样本未对版本信息集合进行逻辑运算)。因此，目前的检测手段可能无法准确识别出异常样本在执行环境探测，继而可能会将异常样本误判为正常样本。

[0008] 鉴于此，本申请提供了一种样本处理方法、装置及系统，来准确判定待检测样本是否有执行环境探测，以便可以使用其它判断方法来进一步确定待检测样本是否为异常样本。

[0009] 为了实现上述目的，本申请提供了以下技术手段：

[0010] 一种样本处理方法，包括：

[0011] 将待检测样本通过版本嗅探API传输的每个版本信息，确定为污染对象；其中，所述版本嗅探API为待检测样本与控制端对接的应用程序接口；

[0012] 在所述待检测样本利用任一污染对象执行逻辑运算的情况下，确定所述待检测样本在执行环境探测。

[0013] 优选的，还包括：

[0014] 在所述待检测样本利用任一污染对象执行算术运算的情况下，将利用该污染对象执行算术运算的结果，重新确定为污染对象。

[0015] 优选的，在所述将待检测样本通过版本嗅探API传输的每个版本信息，确定为污染对象之前，还包括：

[0016] 获取终端上传的待检测样本；或，

[0017] 在终端上抓取待检测样本。

[0018] 一种样本处理装置，包括：

[0019] 确定污染对象单元，用于将待检测样本通过版本嗅探API传输的每个版本信息，确定为污染对象；其中，所述版本嗅探API为待检测样本与控制端对接的应用程序接口；

[0020] 确定探测单元，用于在所述待检测样本利用任一污染对象执行逻辑运算的情况下，确定所述待检测样本在执行环境探测。

[0021] 优选的，还包括：

[0022] 重新确定污染对象单元，用于在所述待检测样本利用任一污染对象执行算术运算的情况下，将利用该污染对象执行算术运算的结果，重新确定为污染对象。

[0023] 优选的，还包括：

[0024] 获取单元，用于获取终端上传的待检测样本；或，在终端上抓取待检测样本。

[0025] 一种样本处理系统，包括：

[0026] 多个终端，与所述多个终端相连的服务器；

[0027] 所述服务器，用于获取待检测样本，并且针对每个待检测样本执行以下步骤：将待检测样本通过版本嗅探API传输的每个版本信息，确定为污染对象；其中，所述版本嗅探API为待检测样本与控制端对接的应用程序接口；在所述待检测样本利用任一污染对象执行逻辑运算的情况下，确定所述待检测样本在执行环境探测。

[0028] 优选的，所述服务器，还用于在所述待检测样本利用任一污染对象执行算术运算的情况下，将利用该污染对象执行算术运算的结果，重新确定为污染对象。

[0029] 优选的，所述服务器，还用于获取终端上传的待检测样本；或，在终端上抓取待检测样本。

[0030] 一种样本处理系统，包括：

[0031] 多个终端，与所述多个终端相连的服务器；

[0032] 所述终端，用于获取待检测样本，并且针对每个待检测样本执行下述步骤：将待检测样本通过版本嗅探API传输的每个版本信息，确定为污染对象；其中，所述版本嗅探API为待检测样本与控制端对接的应用程序接口；在所述待检测样本利用任一污染对象执行逻辑运算的情况下，确定所述待检测样本在执行环境探测。

[0033] 优选的，所述终端，还用于在所述待检测样本利用任一污染对象执行算术运算的

情况下,将利用该污染对象执行算术运算的结果,重新确定为污染对象。

[0034] 优选的,所述终端,还用于在与之相连的其它终端或所述服务器上获取待检测样本。

[0035] 一种样本处理方法,包括:

[0036] 将待检测样本通过版本嗅探API传输的每个版本信息,确定为污染对象;其中,所述版本嗅探API为待检测样本与控制端对接的应用程序接口;

[0037] 在所述待检测样本利用任一污染对象执行逻辑运算的情况下,确定所述待检测样本在执行环境探测;

[0038] 利用异常检测规则处理所述待检测样本,并获得检测结果。

[0039] 从以上技术手段可以看出,本申请具有以下有益效果:

[0040] 本申请将通过版本嗅探API传输的版本信息作为污染对象,采用污染源跟踪的方式,可以时时刻刻跟踪版本信息,不论版本信息被待检测样本如何变形,污染对象即相当于版本信息。由于环境探测为利用版本信息进行逻辑运算,所以本申请判断待检测样本是否利用污染对象在执行逻辑运算。若待检测样本利用污染对象在执行逻辑运算,便可以确定待检测样本在进行环境探测。

[0041] 本申请中无论待检测样本是否对版本信息进行变形,均可以准确检测到待检测样本是否有执行环境探测,以便可以在确定待检测样本执行环境探测后,利用其它方法来进一步确定待检测样本是否为异常样本。

附图说明

[0042] 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,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。

[0043] 图1为本申请实施例公开的样本处理系统的结构示意图;

[0044] 图2为本申请实施例公开的样本处理方法的流程图;

[0045] 图3为本申请实施例公开的样本处理装置的结构示意图;

[0046] 图4为本申请实施例公开的又一样本处理装置的结构示意图。

具体实施方式

[0047] 下面将结合本申请实施例中的附图,对本申请实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本申请一部分实施例,而不是全部的实施例。基于本申请中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本申请保护的范围。

[0048] 在介绍本申请实施例之前首先介绍一种样本处理系统,以方便本领域技术人员更容易理解本申请实施例的应用场景。

[0049] 如图1所示,样本处理系统包括:多个终端100,与所述多个终端相连的服务器200。多个终端100分别采用:终端1、终端2……终端N表示,N为非零自然数。

[0050] 基于上述样本处理系统,服务器200可以接收终端100上传的待检测样本,或者,在

终端100上抓取待检测样本，或者，利用其自身已有的待检测样本。由于服务器不确定待检测样本是否为异常样本，为了保证终端100的安全性，服务器200可以对待检测样本进行检测，以便确定待检测样本是否为异常样本。

[0051] 在服务器200确定待检测样本为异常样本的情况下，则可以对异常样本进行处理，防止异常样本对终端100造成安全威胁。在服务器200确定待检测样本为正常样本的情况下，则可以将正常样本下发至终端100，以便满足终端100的使用样本的需求。

[0052] 所以，本申请所提供的样本处理方法，可以应用于图1所示的服务器中。在图1所示的系统中，服务器200可以统一处理待检测样本，可以提高待检测样本的处理效率和准确性。

[0053] 此外，本申请所提供的样本处理方法，还可以应用于终端100上。终端100可以在与之相连的其它终端(图示未示出)上获取待检测样本，或者获取用户上传的待检测样本，或者在服务器200上获取待检测样本，或者获取其自身已有的待检测样本。

[0054] 在终端100确定待检测样本为正常样本之后，再将正常样本上传至服务器200。服务器200便可以将正常样本发送至其它终端100，以满足其它终端100使用样本的需求。当然，在终端100确定待检测样本为正常样本之后，可以使用正常样本，以满足自身使用样本的需求。

[0055] 本申请所提供的样本处理方法，无论应用于服务器还是终端上，均可以实现本申请的目的。在应用于终端的情况下，需要每个终端均安装执行本申请的软件程序；如果本申请应用于服务器的情况下，则需要在服务器上安装本申请的软件程序。相对于在每个终端上安装执行本申请的软件程序而言，仅在服务器上安装执行本申请的软件程序，相对而言较为简单方便。

[0056] 由于终端与服务器对待检测样本的处理过程是一致的，为了清楚介绍本申请的执行过程，所以本申请将服务器和终端统称为控制端，以控制端来表示服务器200或终端100。并且，控制端针对每个待检测样本的执行过程均是一致的，所以本申请仅针对控制端对一个待检测样本的具体执行过程进行详细说明。可以理解的是，其它待检测样本的处理过程与此类似，在此不再赘述。

[0057] 在介绍本申请所提供的样本处理方法的具体执行过程之前，先介绍本申请的大体思路：

[0058] 待检测样本可能为正常样本，可能为异常样本。异常样本可以获取控制端的版本信息集合，以便进行环境探测。少量的正常样本也可以获取控制端的版本信息集合，以便利用版本信息集合确定适应控制端的使用需求。因此，待检测样本一般会获取版本信息集合，版本信息集合可以包括控制端的系统版本信息以及播放器的版本信息等信息。

[0059] 为了获取控制端的版本信息集合，待检测样本可以调用版本嗅探版本嗅探API，利用该版本嗅探API可以与控制端进行连接，从而方便待检测样本获取控制端的版本信息集合。其中，版本嗅探API(Application Programming Interface，应用程序编程接口)是一些预先定义的函数，目的是提供应用程序与开发人员基于某软件或硬件得以访问一组例程的能力，而又无需访问源码，或理解内部工作机制的细节。

[0060] 为了实现在待检测样本对版本信息集合变形之后，仍可以识别出待检测样本是否有执行环境探测过程的目的，本申请采用污染源跟踪方法。污染源跟踪方法的原理为：假定

某个数据是不可信、被污染的，则为该数据打上污染标记，由该数据计算后得到的所有数据均是不可信、被污染的。

[0061] 在本申请中利用污染源跟踪方法的具体执行过程为：将获取版本信息集合的版本嗅探API作为污染源，那么通过版本嗅探API传输的所有版本信息均为被污染的污染对象。并且，经过版本嗅探API传输的版本信息在经过一系列变形之后得到的信息，仍然为污染对象。即，污染对象为版本信息或者版本信息的变形，所以污染对象即相当于版本信息。由于污染对象即相当于版本信息，因此在后续判断过程中，可以判断待检测样本有无对污染对象执行逻辑计算；如果待检测样本对污染对象执行逻辑计算，则可以直接确定待检测样本在对版本信息执行逻辑运算，即待检测样本在执行环境探测。

[0062] 在上述技术思路的前提下，参见图2，本申请提供了一种样本处理方法，包括步骤S201～S204：

[0063] 步骤S201：将待检测样本通过版本嗅探API传输的每个版本信息，确定为污染对象。

[0064] 由于版本信息均有一定的表现形式，通过一定的表现形式，控制端则可以得知一个信息是否为版本信息。但是，若待检测样本对版本信息变形之后，则可能导致版本信息具有其它的表现形式，从而使得控制端则无法识别出版本信息。

[0065] 由于版本信息均是从版本嗅探API传输的，所以从版本嗅探API传输的信息均为版本信息。因此，不论一个信息改变为何种表现形式，只要其根源为由版本嗅探API传输而来，则可以确定其为版本信息。因此，本申请将传输版本信息的版本嗅探API作为污染源。由于版本嗅探API为污染源，因此从版本嗅探API输出的每个版本信息，均为污染对象；即本申请将版本信息作为污染对象。

[0066] 在具体实现时，控制端可以将从版本嗅探API输出的每个信息添加标记，以表示其为污染对象，此外，还可以表示其为版本信息。添加标记的方式可以为添加特殊内容，或者，增加指定的前缀或指定的后缀等方式，在此不再一一列举。

[0067] 针对在步骤S201中确定的每个污染对象，均执行下述步骤S202～步骤S205。

[0068] 步骤S202：判断所述待检测样本是否利用污染对象执行算术运算，若是则进入步骤S203，否则进入步骤S204。

[0069] 异常样本为了伪装其利用版本信息进行环境探测，可能对版本信息进行一次或多次算术运算，从而使得版本信息改变为其它信息，然后再利用其它信息执行环境探测，从而躲避控制端检测环境探测的技术手段。

[0070] 例如，异常样本对版本信息A进行一次算术计算后变成信息B，再次进行一次算术运算后，变成信息C。信息C与版本信息A已经完全不一致，所以异常样本在利用信息C执行环境探测时，控制端仅可以识别出信息C在进行逻辑运算，而无法识别出异常样本在利用版本信息进行环境探测。

[0071] 为此，本申请判断待检测样本是否利用污染对象执行算术运算，若是，则进入步骤S203，以便跟踪版本信息，也即跟踪污染对象。

[0072] 步骤S203：将利用污染对象执行算术运算的结果，重新确定为污染对象。即，在所述待检测样本利用任一污染对象执行算术运算的情况下，将利用该污染对象执行算术运算的结果，重新确定为污染对象。然后，再次进入步骤S202。

[0073] 为了在版本信息改变表现形式之后仍可以识别出版本信息，本申请可以跟踪版本信息即跟踪污染对象。针对任一污染对象，跟踪污染对象的具体实现过程为：当污染对象(版本信息)进行一次算术运算后，会改变其原来表现形式时，将污染对象(版本信息)进行算术运算的运算结果重新作为污染对象。

[0074] 由于待检测样本可能会对版本信息进行多次算术运算，所以再次进入步骤S202，重复执行步骤S202和步骤S203，直到污染对象不再执行算术运算。在待检测样本不再对污染对象执行算术运算之后，则表明待检测样本对污染对象变形已结束，此时可以进入步骤S204。

[0075] 即，如果一个信息为污染对象，由此计算得到的其它信息同为污染对象。这样即便在异常样本多次利用算术运算更改版本信息的情况下，控制端仍然可以通过污染对象，来识别一个信息为版本信息。

[0076] 例如，将版本信息A确定为污染对象，对版本信息A添加标记“污染”。在版本信息A进行算术计算后变成信息B后，仍然为信息B添加标记“污染”；在信息B再次进行算术运算后变成信息C后，仍然为信息C添加标记“污染”。

[0077] 控制端通过信息C的标记“污染”，仍然可以确定信息C为由版本信息演变而来，所以仍然可以确定信息C为版本信息。

[0078] 步骤S204：判断所述待检测样本是否利用污染对象执行逻辑运算；若是，进入步骤S205，否则，执行其它处理过程。即，在所述待检测样本利用任一污染对象执行逻辑运算的情况下，确定所述待检测样本在执行环境探测。

[0079] 本申请采用污染源跟踪的方式，可以时时刻刻跟踪版本信息，不论版本信息被待检测样本如何对版本信息进行变形，污染对象即相当于版本信息。由于环境探测为利用版本信息进行逻辑运算，所以本申请判断待检测样本是否利用污染对象在执行逻辑运算。若待检测样本利用污染对象在执行逻辑运算，便可以确定待检测样本在进行环境探测。

[0080] 若待检测样本未利用污染对象在执行逻辑运算，则说明待检测样本未执行环境探测，可以执行其它处理过程。

[0081] 步骤S205：确定待检测样本在执行环境探测。即，在所述待检测样本利用任一污染对象执行逻辑运算的情况下，确定所述待检测样本在执行环境探测。

[0082] 从以上内容可以看出，本申请具有以下有益效果：

[0083] 本申请将通过版本嗅探API传输的版本信息作为污染对象，采用污染源跟踪的方式，可以时时刻刻跟踪版本信息，不论版本信息被待检测样本如何变形，污染对象即相当于版本信息。由于环境探测为利用版本信息进行逻辑运算，所以本申请判断待检测样本是否利用污染对象在执行逻辑运算。若待检测样本利用污染对象在执行逻辑运算，便可以确定待检测样本在进行环境探测。

[0084] 在利用图2所示的过程，确定待检测样本执行环境探测之后，便可以确定待检测样本为可疑样本。为了进一步确定可疑样本是否为异常样本，可以利用异常检测规则来处理待检测样本，以对待检测样本进行进一步检测，并确定待检测样本是否异常样本。异常检测规则可以为检测堆喷射、类型混淆、shellcode(shellcode通常是一段利用软件漏洞的代码，用来作为进行攻击的负载)等技术手段。

[0085] 如果进一步检测确定可疑样本为异常样本，则对异常样本进行处理；如果进一步

检测确定可疑样本不为异常样本，则确定可疑样本为正常样本，可以按照正常样本的处理方式继续处理。

[0086] 以待检测样本为待检测flash样本为例，介绍本申请的一种场景实施例：

[0087] 控制端将待检测flash样本获取版本信息的API称为版本嗅探API，并将版本嗅探API作为污染源。然后，将待检测flash样本通过版本嗅探API传输的每个版本信息，确定为污染对象。

[0088] 控制端检测到待检测flash样本对一个污染对象进行算术运算后，将对污染对象进行算术运算的结果，重新确定为污染对象。即，控制端利用污染源跟踪的方式跟踪每个污染对象，也即为跟踪每个版本信息。即使待检测样本对版本信息进行变形之后，控制端仍可以通过判定一个信息为污染对象，来判定该信息为版本信息。

[0089] 控制端在检测到待检测flash样本利用任一污染对象执行逻辑运算的情况下，则可以确定所述待检测flash样本在执行环境探测。然后，将待检测flash样本确定为可疑flash样本，并利用进一步的技术手段来检测可疑flash样本是否为异常flash样本。

[0090] 如果进一步检测确定可疑flash样本为异常flash样本，则对异常flash样本进行处理；如果进一步检测确定可疑flash样本不为异常flash样本，则确定可疑flash样本为正常flash样本，可以按照正常flash样本的处理方式继续处理。

[0091] 与图2所示的一种样本处理方法相对应，本申请提供了一种样本处理装置。如图3所示，具体包括：

[0092] 确定污染对象单元31，用于将待检测样本通过版本嗅探API传输的每个版本信息，确定为污染对象；其中，所述版本嗅探API为待检测样本与控制端对接的应用程序接口；

[0093] 确定探测单元32，用于在所述待检测样本利用任一污染对象执行逻辑运算的情况下，确定所述待检测样本在执行环境探测。

[0094] 重新确定污染对象单元33，用于在所述待检测样本利用任一污染对象执行算术运算的情况下，将利用该污染对象执行算术运算的结果，重新确定为污染对象。

[0095] 如图4所示，本申请还提供了一种样本处理装置，还包括：

[0096] 获取单元34，用于获取终端上传的待检测样本；或，在终端上抓取待检测样本。

[0097] 通过以上技术内容，可以看出本装置具有以下有益效果：

[0098] 本申请将通过版本嗅探API传输的版本信息作为污染对象，采用污染源跟踪的方式，可以时时刻刻跟踪版本信息，不论版本信息被待检测样本如何变形，污染对象即相当于版本信息。由于环境探测为利用版本信息进行逻辑运算，所以本申请判断待检测样本是否利用污染对象在执行逻辑运算。若待检测样本利用污染对象在执行逻辑运算，便可以确定待检测样本在进行环境探测。

[0099] 本申请无论待检测样本是否变形，均可以准确检测到待检测样本是否有执行环境探测，从而可以在确定待检测样本执行环境探测后，用其它方法来进一步确定待检测样本是否为异常样本。

[0100] 参见图1，本申请提供了一种样本处理系统，包括：

[0101] 多个终端100，与所述多个终端相连的服务器200。多个终端100分别采用：终端1、终端2……终端N表示，N为非零自然数。

[0102] 其中，服务器200，用于获取待检测样本，针对每个待检测样本执行以下步骤：将待

检测样本通过版本嗅探API传输的每个版本信息，确定为污染对象；其中，所述版本嗅探API为待检测样本与控制端对接的应用程序接口；在所述待检测样本利用任一污染对象执行逻辑运算的情况下，确定所述待检测样本在执行环境探测。

[0103] 所述服务器200，还用于获取终端100上传的待检测样本；或，在终端100上抓取待检测样本。并且，所述服务器200，还用于在所述待检测样本利用任一污染对象执行算术运算的情况下，将利用该污染对象执行算术运算的结果，重新确定为污染对象。

[0104] 服务器200，可以在所述多个终端100上获取待检测样本，并针对每个待检测样本判断其是否在执行环境探测。如果待检测样本在执行环境探测，则采用进一步的技术手段，来判断其是否为异常样本。

[0105] 通过以上技术内容，可以看出本系统具有以下有益效果：

[0106] 本申请将通过版本嗅探API传输的版本信息作为污染对象，采用污染源跟踪的方式，可以时时刻刻跟踪版本信息，不论版本信息被待检测样本如何变形，污染对象即相当于版本信息。由于环境探测为利用版本信息进行逻辑运算，所以本申请判断待检测样本是否利用污染对象在执行逻辑运算。若待检测样本利用污染对象在执行逻辑运算，便可以确定待检测样本在进行环境探测。

[0107] 本申请无论待检测样本是否变形，均可以准确检测到待检测样本是否有执行环境探测，从而可以在确定待检测样本执行环境探测后，用其它方法来进一步确定待检测样本是否为异常样本。

[0108] 参见图1，本申请提供了一种样本处理系统，包括：

[0109] 多个终端100，与所述多个终端相连的服务器200。多个终端100分别采用：终端1、终端2……终端N表示，N为非零自然数。

[0110] 其中，所述终端100，用于获取待检测样本，并且针对每个待检测样本执行下述步骤：将待检测样本通过版本嗅探API传输的每个版本信息，确定为污染对象；其中，所述版本嗅探API为待检测样本与控制端对接的应用程序接口；在所述待检测样本利用任一污染对象执行逻辑运算的情况下，确定所述待检测样本在执行环境探测。

[0111] 所述终端100，还用于在所述待检测样本利用任一污染对象执行算术运算的情况下，将利用该污染对象执行算术运算的结果，重新确定为污染对象。

[0112] 终端100，可以在与之相连的其它终端或服务器200上获取待检测样本，并针对每个待检测样本判断其是否在执行环境探测。如果待检测样本在执行环境探测，则采用进一步的技术手段，来判断其是否为异常样本。

[0113] 通过以上技术手段，可以看出本申请提供的系统具有以下有益效果：

[0114] 本申请将通过版本嗅探API传输的版本信息作为污染对象，采用污染源跟踪的方式，可以时时刻刻跟踪版本信息，不论版本信息被待检测样本如何变形，污染对象即相当于版本信息。由于环境探测为利用版本信息进行逻辑运算，所以本申请判断待检测样本是否利用污染对象在执行逻辑运算。若待检测样本利用污染对象在执行逻辑运算，便可以确定待检测样本在进行环境探测。

[0115] 本申请无论待检测样本是否变形，均可以准确检测到待检测样本是否有执行环境探测，从而可以在确定待检测样本执行环境探测后，用其它方法来进一步确定待检测样本是否为异常样本。

[0116] 本实施例方法所述的功能如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算设备可读取存储介质中。基于这样的理解，本申请实施例对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该软件产品存储在一个存储介质中，包括若干指令用以使得一台计算设备(可以是个人计算机，服务器，移动计算设备或者网络设备等)执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0117] 本说明书中各个实施例采用递进的方式描述，每个实施例重点说明的都是与其它实施例的不同之处，各个实施例之间相同或相似部分互相参见即可。

[0118] 对所公开的实施例的上述说明，使本领域专业技术人员能够实现或使用本申请。对这些实施例的多种修改对本领域的专业技术人员来说将是显而易见的，本文中所定义的一般原理可以在不脱离本申请的精神或范围的情况下，在其它实施例中实现。因此，本申请将不会被限制于本文所示的这些实施例，而是要符合与本文所公开的原理和新颖特点相一致的最宽的范围。

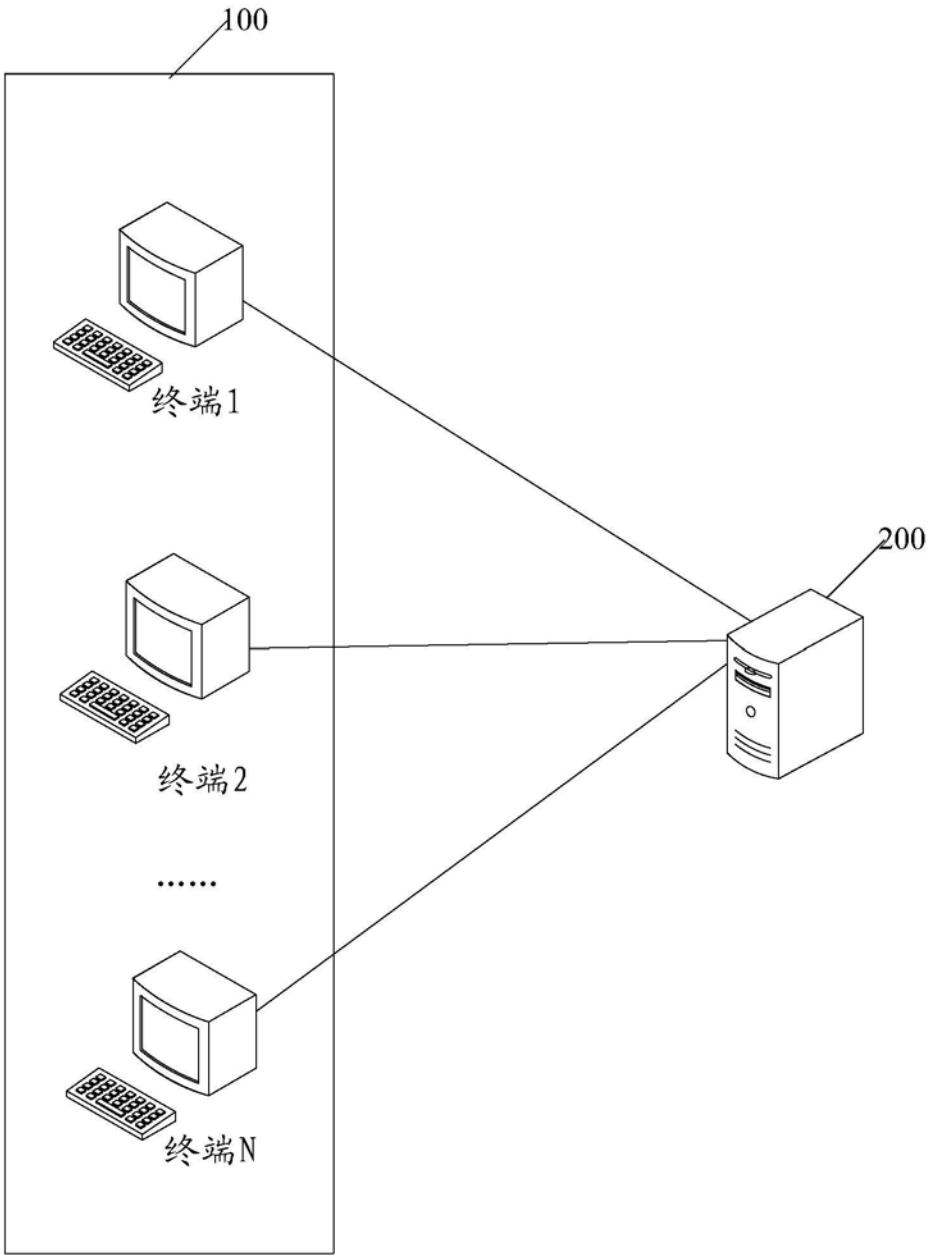


图1

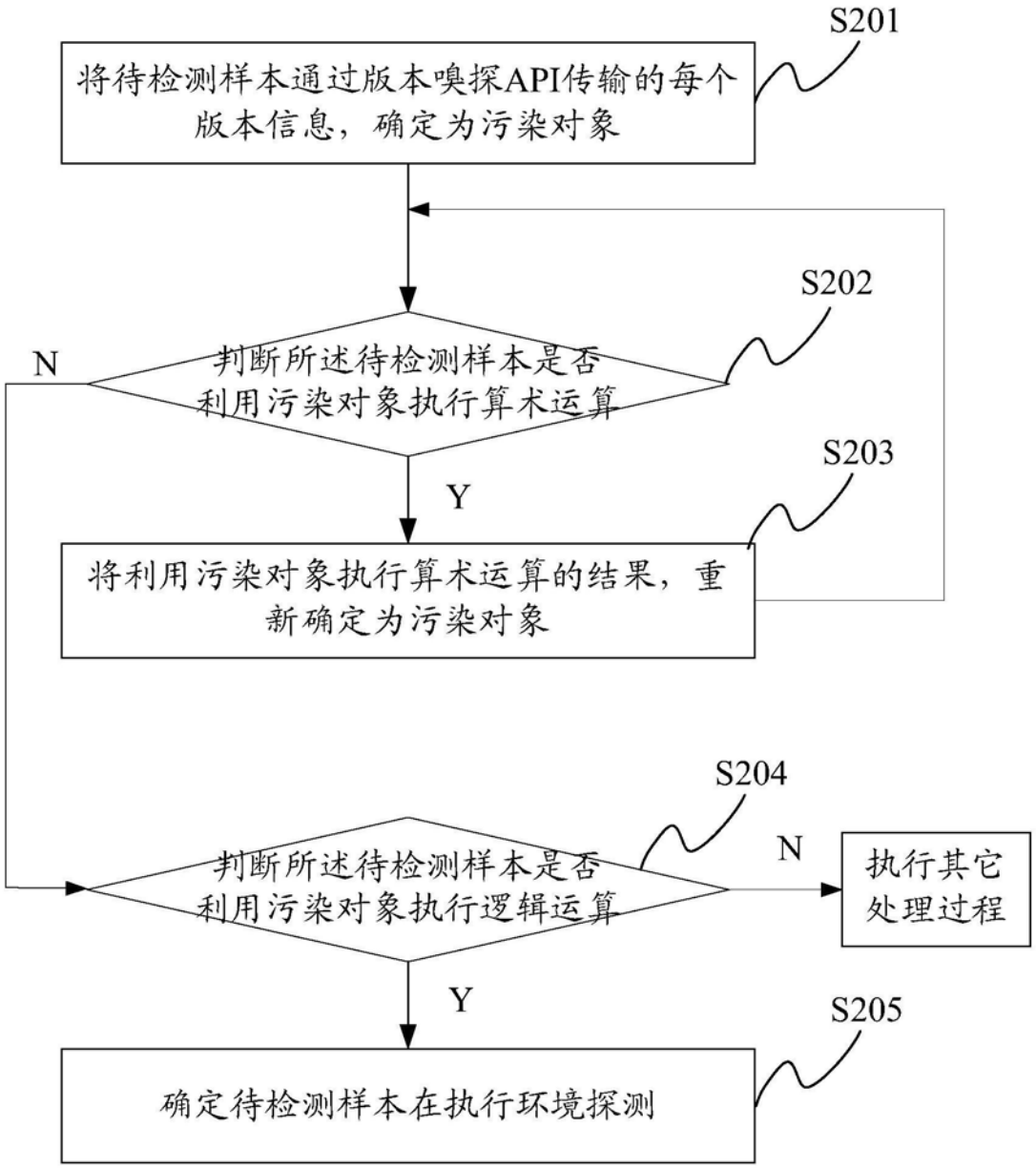

S201
将待检测样本通过版本嗅探API传输的每个版本信息，确定为污染对象
S202
判断所述待检测样本是否利用污染对象执行算术运算
N
Y
S203
将利用污染对象执行算术运算的结果，重新确定为污染对象
S204
判断所述待检测样本是否利用污染对象执行逻辑运算
N
执行其它处理过程
Y
S205
确定待检测样本在执行环境探测

图2

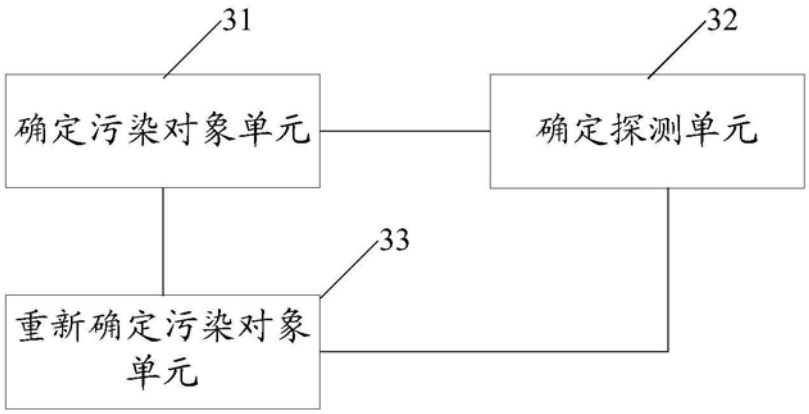

31
32
确定污染对象单元
确定探测单元
33
重新确定污染对象单元

图3

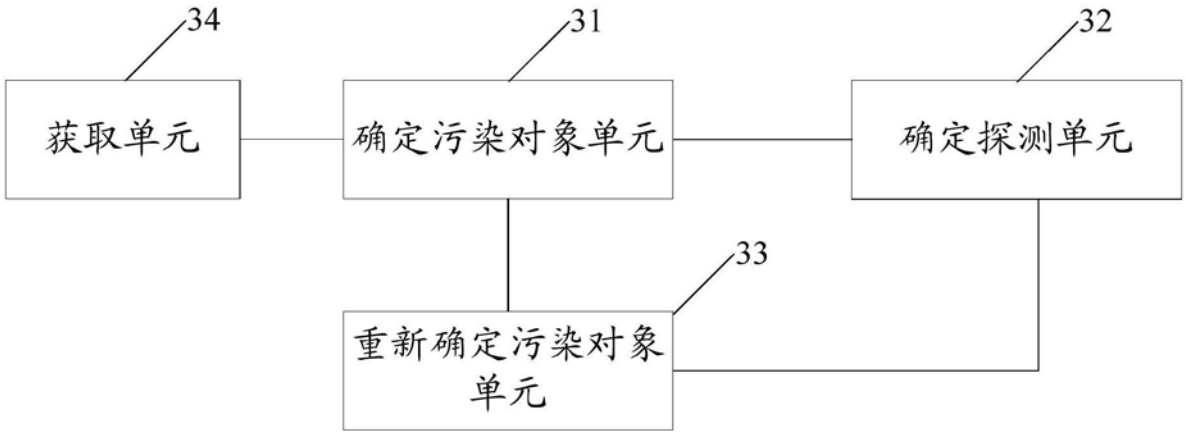

34
31
32
获取单元
确定污染对象单元
确定探测单元
33
重新确定污染对象单元

图4