(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 110866253 A
(43)申请公布日 2020.03.06

(21)申请号 201811632299.7

(22)申请日 2018.12.28

(71)申请人 北京安天网络安全技术有限公司
地址 100195 北京市海淀区玉泉山闵庄路3号清华科技园玉泉慧谷1号楼

(72)发明人 胡洲 郑言语 夏姗姗

(74)专利代理机构 北京市广友专利事务所有限责任公司 11237
代理人 祁献民

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

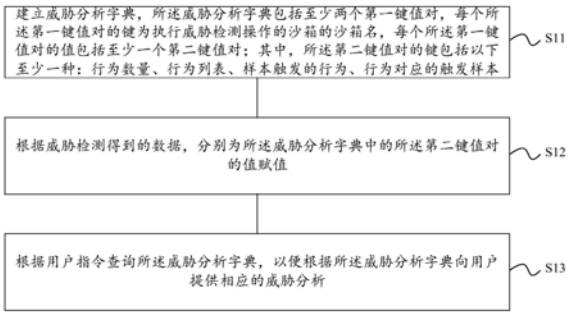
权利要求书2页 说明书8页 附图3页

(54)发明名称

一种威胁分析方法、装置、电子设备及存储介质

(57)摘要

本发明实施例公开一种威胁分析方法、装置、电子设备及存储介质，涉及信息安全技术领域，能够提高对威胁的分析效率并改善分析效果。所述方法包括：建立威胁分析字典，所述威胁分析字典包括至少两个第一键值对，每个所述第一键值对的键为执行威胁检测操作的沙箱的沙箱名，每个所述第一键值对的值包括至少一个第二键值对；其中，所述第二键值对的键包括以下至少一种：行为数量、行为列表、样本触发的行为、行为对应的触发样本；根据威胁检测得到的数据，分别为所述威胁分析字典中的所述第二键值对的值赋值；根据用户指令查询所述威胁分析字典，以便根据所述威胁分析字典向用户提供相应的威胁分析。本发明可用于威胁的综合分析。



CN 110866253 A

1.一种威胁分析方法,其特征在于,包括:

建立威胁分析字典,所述威胁分析字典包括至少两个第一键值对,每个所述第一键值对的键为执行威胁检测操作的沙箱的沙箱名,每个所述第一键值对的值包括至少一个第二键值对;其中,所述第二键值对的键包括以下至少一种:行为数量、行为列表、样本触发的行为、行为对应的触发样本;

根据威胁检测得到的数据,分别为所述威胁分析字典中的所述第二键值对的值赋值;

根据用户指令查询所述威胁分析字典,以便根据所述威胁分析字典向用户提供相应的威胁分析。

2.根据权利要求1所述的方法,其特征在于,所述第二键值对中行为数量键对应的值包括至少一个第三键值对;每个所述第三键值对的键为行为名称,值为所述行为名称对应的行为的被触发次数。

3.根据权利要求2所述的方法,其特征在于,所述根据威胁检测得到的数据,分别为所述威胁分析字典中的所述第二键值对的值赋值包括:

从威胁检测得到的预设文件中提取威胁样本引发的威胁行为的行为名称;

将所述威胁行为的行为名称赋值给所述第三键值对的键,并将所述第三键值对的值初始化为0;

遍历威胁检测得到的检测报告,利用所述检测报告中的信息更新所述行为名称对应的行为的被触发次数。

4.根据权利要求3所述的方法,其特征在于,所述预设文件包括翻译文件。

5.根据权利要求1所述的方法,其特征在于,所述根据威胁检测得到的数据,分别为所述威胁分析字典中的所述第二键值对赋值包括:

遍历威胁检测得到的检测报告,利用所述检测报告中的信息为所述威胁分析字典中的所述第二键值对的值赋值。

6.根据权利要求1所述的方法,其特征在于,所述根据用户指令查询所述威胁分析字典,以便根据所述威胁分析字典向用户提供相应的威胁分析包括:

根据用户的第一指令查询所述威胁分析字典,根据所述威胁分析字典向用户提供一个或多个沙箱中威胁样本与威胁行为之间的对应关系;和/或

根据用户的第二指令查询所述威胁分析字典,根据所述威胁分析字典向用户提供一个或多个沙箱中,一个或多个版本的检测系统对威胁行为的检出对比。

7.一种威胁分析装置,其特征在于,包括:

建立单元,用于建立威胁分析字典,所述威胁分析字典包括至少两个第一键值对,每个所述第一键值对的键为执行威胁检测操作的沙箱的沙箱名,每个所述第一键值对的值包括至少一个第二键值对;其中,所述第二键值对的键包括以下至少一种:行为数量、行为列表、样本触发的行为、行为对应的触发样本;

赋值单元,用于根据威胁检测得到的数据,分别为所述威胁分析字典中的所述第二键值对的值赋值;

查询单元,用于根据用户指令查询所述威胁分析字典,以便根据所述威胁分析字典向用户提供相应的威胁分析。

8.根据权利要求7所述的装置,其特征在于,所述第二键值对中行为数量键对应的值包

括至少一个第三键值对;每个所述第三键值对的键为行为名称,值为所述行为名称对应的行为的被触发次数。

9.根据权利要求8所述的装置,其特征在于,所述赋值单元包括:

提取模块,用于从威胁检测得到的预设文件中提取威胁样本引发的威胁行为的行为名称;

赋值模块,用于将所述威胁行为的行为名称赋值给所述第三键值对的键,并将所述第三键值对的值初始化为0;

更新模块,用于遍历威胁检测得到的检测报告,利用所述检测报告中的信息更新所述行为名称对应的行为的被触发次数。

10.根据权利要求9所述的装置,其特征在于,所述预设文件包括翻译文件。

11.根据权利要求7所述的装置,其特征在于,所述赋值单元,具体用于:

遍历威胁检测得到的检测报告,利用所述检测报告中的信息为所述威胁分析字典中的所述第二键值对的值赋值。

12.根据权利要求7所述的装置,其特征在于,所述查询单元包括:

第一查询模块,用于根据用户的第一指令查询所述威胁分析字典,根据所述威胁分析字典向用户提供一个或多个沙箱中威胁样本与威胁行为之间的对应关系;和/或

第二查询模块,用于根据用户的第二指令查询所述威胁分析字典,根据所述威胁分析字典向用户提供一个或多个沙箱中,一个或多个版本的检测系统对威胁行为的检出对比。

13.一种电子设备,其特征在于,所述电子设备包括:壳体、处理器、存储器、电路板和电源电路,其中,电路板安置在壳体围成的空间内部,处理器和存储器设置在电路板上;电源电路,用于为上述电子设备的各个电路或器件供电;存储器用于存储可执行程序代码;处理器通过读取存储器中存储的可执行程序代码来运行与可执行程序代码对应的程序,用于执行前述权利要求1至6任一项所述的威胁分析方法。

14.一种计算机可读存储介质,其特征在于,所述计算机可读存储介质存储有一个或者多个程序,所述一个或者多个程序可被一个或者多个处理器执行,以实现前述权利要求1至6中任一项所述的威胁分析方法。

一种威胁分析方法、装置、电子设备及存储介质

技术领域

[0001] 本发明涉及计算机技术领域，尤其涉及一种威胁分析方法、装置、电子设备及存储介质。

背景技术

[0002] 目前，一些专用的威胁监测软件能够监测出多种威胁的动态，为了掌握威胁的特征以便对威胁进行有效防护，常常需要对动态分析检测出来威胁的各种行为及其数量进行统计和分析。然而由于威胁种类繁多数据量巨大，目前尚没有分析效率高、效果好的方法。

发明内容

[0003] 有鉴于此，本发明实施例提供一种威胁分析方法、装置、电子设备及存储介质，能够提高对威胁的分析效率并改善分析效果。

[0004] 第一方面，本发明实施例提供一种威胁分析方法，包括：建立威胁分析字典，所述威胁分析字典包括至少两个第一键值对，每个所述第一键值对的键为执行威胁检测操作的沙箱的沙箱名，每个所述第一键值对的值包括至少一个第二键值对；其中，所述第二键值对的键包括以下至少一种：行为数量、行为列表、样本触发的行为、行为对应的触发样本；根据威胁检测得到的数据，分别为所述威胁分析字典中的所述第二键值对的值赋值；根据用户指令查询所述威胁分析字典，以便根据所述威胁分析字典向用户提供相应的威胁分析。

[0005] 可选的，所述第二键值对中行为数量键对应的值包括至少一个第三键值对；每个所述第三键值对的键为行为名称，值为所述行为名称对应的行为的被触发次数。

[0006] 可选的，所述根据威胁检测得到的数据，分别为所述威胁分析字典中的所述第二键值对的值赋值包括：从威胁检测得到的预设文件中提取威胁样本引发的威胁行为的行为名称；将所述威胁行为的行为名称赋值给所述第三键值对的键，并将所述第三键值对的值初始化为0；遍历威胁检测得到的检测报告，利用所述检测报告中的信息更新所述行为名称对应的行为的被触发次数。

[0007] 可选的，所述预设文件包括翻译文件。

[0008] 可选的，所述根据威胁检测得到的数据，分别为所述威胁分析字典中的所述第二键值对赋值包括：遍历威胁检测得到的检测报告，利用所述检测报告中的信息为所述威胁分析字典中的所述第二键值对的值赋值。

[0009] 可选的，所述根据用户指令查询所述威胁分析字典，以便根据所述威胁分析字典向用户提供相应的威胁分析包括：根据用户的第一指令查询所述威胁分析字典，根据所述威胁分析字典向用户提供一个或多个沙箱中威胁样本与威胁行为之间的对应关系；和/或根据用户的第二指令查询所述威胁分析字典，根据所述威胁分析字典向用户提供一个或多个沙箱中，一个或多个版本的检测系统对威胁行为的检出对比。

[0010] 第二方面，本发明的实施例还提供一种威胁分析装置，包括：建立单元，用于建立威胁分析字典，所述威胁分析字典包括至少两个第一键值对，每个所述第一键值对的键为

执行威胁检测操作的沙箱的沙箱名，每个所述第一键值对的值包括至少一个第二键值对；其中，所述第二键值对的键包括以下至少一种：行为数量、行为列表、样本触发的行为、行为对应的触发样本；赋值单元，用于根据威胁检测得到的数据，分别为所述威胁分析字典中的所述第二键值对的值赋值；查询单元，用于根据用户指令查询所述威胁分析字典，以便根据所述威胁分析字典向用户提供相应的威胁分析。

[0011] 可选的，所述第二键值对中行为数量键对应的值包括至少一个第三键值对；每个所述第三键值对的键为行为名称，值为所述行为名称对应的行为的被触发次数。

[0012] 可选的，所述赋值单元包括：提取模块，用于从威胁检测得到的预设文件中提取威胁样本引发的威胁行为的行为名称；赋值模块，用于将所述威胁行为的行为名称赋值给所述第三键值对的键，并将所述第三键值对的值初始化为0；更新模块，用于遍历威胁检测得到的检测报告，利用所述检测报告中的信息更新所述行为名称对应的行为的被触发次数。

[0013] 可选的，所述预设文件包括翻译文件。

[0014] 可选的，所述赋值单元，具体用于：遍历威胁检测得到的检测报告，利用所述检测报告中的信息为所述威胁分析字典中的所述第二键值对的值赋值。

[0015] 可选的，所述查询单元包括：第一查询模块，用于根据用户的第一指令查询所述威胁分析字典，根据所述威胁分析字典向用户提供一个或多个沙箱中威胁样本与威胁行为之间的对应关系；和/或第二查询模块，用于根据用户的第二指令查询所述威胁分析字典，根据所述威胁分析字典向用户提供一个或多个沙箱中，一个或多个版本的检测系统对威胁行为的检出对比。

[0016] 第三方面，本发明的实施例还提供一种电子设备，所述电子设备包括：壳体、处理器、存储器、电路板和电源电路，其中，电路板安置在壳体围成的空间内部，处理器和存储器设置在电路板上；电源电路，用于为上述电子设备的各个电路或器件供电；存储器用于存储可执行程序代码；处理器通过读取存储器中存储的可执行程序代码来运行与可执行程序代码对应的程序，用于执行本发明实施例提供的任一种威胁分析方法。

[0017] 第四方面，本发明的实施例还提供一种计算机可读存储介质，所述计算机可读存储介质存储有一个或者多个程序，所述一个或者多个程序可被一个或者多个处理器执行，以实现本发明实施例提供的任一种威胁分析方法。

[0018] 本发明的实施例提供的威胁分析方法、装置、电子设备及存储介质，能够建立了威胁分析字典，在威胁分析字典中对不同沙箱检测到的威胁进行行为数量、行为列表、样本触发的行为、行为对应的触发样本等多方面的统计，并利用威胁检测数据为这些统计项目赋值，这样，当用户需要了解威胁的上述相关特征时，可以根据用户指令从指令中快速调取相应的信息提供给用户，从而有效提高了对威胁的分析效率并改善分析效果。

附图说明

[0019] 为了更清楚地说明本发明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发明的一些实施例，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它的附图。

[0020] 图1为本发明的实施例提供的威胁分析方法的一种流程图；

[0021] 图2为本发明的实施例提供的威胁分析方法的应用场景示意图；

[0022] 图3为本发明的实施例提供的威胁分析方法的一种详细流程图；

[0023] 图4为本发明的实施例提供的威胁分析装置的一种结构示意图；

[0024] 图5为本发明的实施例提供的电子设备的一种结构示意图。

具体实施方式

[0025] 下面结合附图对本发明实施例进行详细描述。

[0026] 应当明确，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其它实施例，都属于本发明保护的范围。

[0027] 第一方面，本发明实施例提供一种威胁分析方法，能够提高对威胁的分析效率并改善分析效果。

[0028] 如图1所示，本发明的实施例提供的威胁分析方法可以包括：

[0029] S11，建立威胁分析字典，所述威胁分析字典包括至少两个第一键值对，每个所述第一键值对的键为执行威胁检测操作的沙箱的沙箱名，每个所述第一键值对的值包括至少一个第二键值对；其中，所述第二键值对的键包括以下至少一种：行为数量、行为列表、样本触发的行为、行为对应的触发样本；

[0030] 具体的，威胁分析字典可以是以预设数据结构组织的与威胁相关的数据库。为了便于管理和查询，本发明的实施例中，威胁分析字典采用键值对的形式组织。其中，键值对之间可以进行嵌套，即一个键值对的键、或值可以为另一个键值对，整个威胁分析字典可以由多层键值对嵌套构成。

[0031] 本实施例中，威胁分析字典最外层的键值对为第一键值对，第一键值对将不同沙箱相区分，每个沙箱中威胁的特征用第二键值对表示。第二键值对的键可以包括行为数量、行为列表、样本触发的行为、行为对应的触发样本中的一种或多种。

[0032] S12，根据威胁检测得到的数据，分别为所述威胁分析字典中的所述第二键值对的值赋值；

[0033] 建立了威胁分析字典，相当于有了信息索引，但每项信息的具体内容需要在本步骤中填充。填充具体信息内容的过程，也就是给第二键值对的值赋值的过程。可选的，由于第二键值对的键可以为行为数量、行为列表、样本触发的行为、行为对应的触发样本等，给第二键值对的值赋值也就看行为数量具体是多少、行为列表中具体包括哪些行为、每个样本分别触发了哪些行为、每个行为对应哪些触发样本等。

[0034] S13，根据用户指令查询所述威胁分析字典，以便根据所述威胁分析字典向用户提供相应的威胁分析。

[0035] 本步骤中，可以根据用户需要从威胁分析字典中提取相应的威胁分析信息展示给用户，从而使用户可以快捷准确地获知与威胁相关的多种信息。

[0036] 本发明的实施例提供的威胁分析方法，建立了威胁分析字典，在威胁分析字典中对不同沙箱检测到的威胁进行行为数量、行为列表、样本触发的行为、行为对应的触发样本等多方面的统计，并利用威胁检测数据为这些统计项目赋值，这样，当用户需要了解威胁的上述相关特征时，可以根据用户指令从指令中快速调取相应的信息提供给用户，从而有效

提高了对威胁的分析效率并改善分析效果。

[0037] 可选的，第二键值对中行为数量键用于统计每种行为的发生次数，例如进行了多少次复制、访问了多少次预设网站、进行了多少次重启等。这样，不同的行为都具有自己的发生次数。因此，本发明的实施例中，行为数量键对应的值也可以以键值对的形式存在。例如，行为数量键对应的值可以包括一个或多个第三键值对；其中，每个第三键值对的键为行为名称，值为该行为名称对应的行为的被触发次数。例如，在本发明的一个实施例中，第三键值对包括：劫持行为--3次、自我复制行为--10次、文件隐藏行为-20次、连接网络行为--4次等。

[0038] 可选的，在步骤S12中，对第二键值对的值赋值也就是要对第三键值对赋值，具体来说就是第三键值对都包括哪些键，每个键对应的值是什么。具体而言，在本发明的一个实施例中，根据威胁检测得到的数据，分别为所述威胁分析字典中的所述第二键值对的值赋值可以包括：

[0039] 从威胁检测得到的预设文件中提取威胁样本引发的威胁行为的行为名称；

[0040] 将所述威胁行为的行为名称赋值给所述第三键值对的键，并将所述第三键值对的值初始化为0；

[0041] 遍历威胁检测得到的检测报告，利用所述检测报告中的信息更新所述行为名称对应的行为的被触发次数。

[0042] 也就是说，在对威胁进行检测时会生成一些检测文件，某些预设文件中可以记录各种威胁行为的名称，在本发明的实施例中，可以直接利用这些文件中的威胁行为的行为名称，将这些名称引用到第三键值对的键中。由于此时还有没统计每种威胁行为的发生次数，可以先对第三键值对的值初始化为0，即每种行为开始时都发生了0次。可选的，预设文件可以包括翻译文件。

[0043] 第三键值对的值初始化后，可以进一步统计每种威胁行为实际发生的次数。可选的，可以遍历威胁检测得到的检测报告，利用所述检测报告中的信息更新所述行为名称对应的行为的被触发次数。例如，某份检测报告中记录着自我复制行为被执行了80次，则第三键值对中，自我复制键对应的值由初始化时的0更新为80。

[0044] 以上详细说明了第二键值对中的行为数量键的赋值和更新情况，对于第二键值对中的行为列表、样本触发的行为、行为对应的触发样本等，其对应的键值的赋值方法也类似，也可以遍历威胁检测得到的检测报告，利用所述检测报告中的信息为所述威胁分析字典中的所述第二键值对的值赋值。

[0045] 例如，遍历检测报告获知检测到了劫持行为、自我复制行为、文件隐藏行为、连接网络行为等，则将这些检测到的行为加入第二键值对的行为列表键对应的键值中。可选的，每读取一份检测报告，就可以查看该检测报告中的行为是否已经被第二键值对收录，如果没有，则将该行为收入行为列表。

[0046] 样本触发的行为是指某个威胁触发了哪些行为。例如，文件A中的语句A1触发了文件隐藏行为，语句A2触发了网络连接行为等。行为对应的触发样本是指一种行为可以被哪种威胁触发。例如，自我复制的行为可以被文件B触发，也可以被文件C触发，则B和C都是自我复制行为对应的触发样本。样本与行为的对应关系也可以通过相应的键值对表示。

[0047] 在步骤S12中完成对威胁分析字典的赋值之后，就可以利用该威胁分析字典获知

威胁相关的各种分析信息。具体而言，在步骤S13中根据用户指令查询所述威胁分析字典，以便根据所述威胁分析字典向用户提供相应的威胁分析可以包括：

[0048] 根据用户的第一指令查询所述威胁分析字典，根据所述威胁分析字典向用户提供一个或多个沙箱中威胁样本与威胁行为之间的对应关系；和/或

[0049] 根据用户的第二指令查询所述威胁分析字典，根据所述威胁分析字典向用户提供一个或多个沙箱中，一个或多个版本的检测系统对威胁行为的检出对比。

[0050] 举例说明，在本发明的一个实施例中，如果需要收集触发了行为P的威胁样本，则可以根据用户的第一指令，在威胁字典中查询，选择输出json格式的统计文件，即可用notepad(文本编辑器)或者Sublime Text 3(文本编辑器)查询到该行为，并能直观的看到其后由哪些样本触发，给出触发样本的MD5值。

[0051] 当需要对多种沙箱的检测结果进行对比测试时，可以执行脚本文件查看威胁分析字典，就能给出一份直观、有序的csv格式的对比分析报告。当需要对同一批样本、不同版本的测试系统进行多种沙箱对比测试时，可以将其他csv里的内容复制到一个csv再微调一下，就能看到一个直观的多个测试系统版本、多种沙箱动态行为检出对比分析报告。

[0052] 本发明的实施例提供的威胁分析方法的应用场景可以如图2所示。

[0053] 下面通过具体实施例对本发明实施例提供的威胁分析方法进行详细说明。

[0054] 如图3所示，本发明的实施例提供的威胁分析方法可以包括：

[0055] S201、建立威胁分析字典；

[0056] 该威胁分析字典包括3个第一键值对，每个第一键值对的键，为执行威胁检测操作的沙箱的沙箱名："kk_executer"、"kk_executer_win7"、"kk_executer_win7_x64"。每个第一键值对的值，包括4个第二键值对：行为列表"behavior_list":[]、行为数量"behavior_num":{}、样本触发的行为"md5_behavior":{}、行为对应的触发样本"behavior_md5":{}。其中大括号“{}”表示括号中的内容仍然为键值对，中括号[]表示括号中的内容是单独的数值。

[0057] 威胁分析字典以键值对的形式可以表示为：

[0058] {"kk_executer":{"behavior_list":[],"behavior_num":{},"md5_behavior":{},"behavior_md5":{}},

[0059] "kk_executer_win7":{"behavior_list":[],"behavior_num":{},"md5_behavior":{},"behavior_md5":{}},

[0060] "kk_executer_win7_x64":{"behavior_list":[],"behavior_num":{},"md5_behavior":{},"behavior_md5":{}}}

[0061] S202、从威胁检测得到的翻译文件中提取威胁样本引发的威胁行为的行为名称；

[0062] S203、将所述威胁行为的行为名称赋值给行为数量"behavior-num":{}的键，并将该键对的值初始化为0；

[0063] S204、遍历威胁检测得到的检测报告，利用所述检测报告中的信息为威胁分析字典中的所述第二键值对的值赋值。

[0064] 具体而言，可以轮询预设数据库(例如mongoDB数据库)，读取每一个威胁样本的检测报告。每取到一份检测报告，就取出该威胁样本的MD5和其中各个沙箱检出的行为，每有一个行为会使相应的沙箱名称中behavior_num下相应的行为次数加一，behavior-list增

加一个未添加过的行为。如果某行为未在behavior_md5出现，则会将该行为做为键，一个列表为值并将触发该行为的威胁样本的MD5放入。md5_behavior中MD5为键其值是列表，将触发的行为记录到该列表，轮询分析报告时如发现某行为不存在于behavior_num的键中将会把该行为报出并将MD5报出。

[0065] S205、根据用户指令查询所述威胁分析字典，以便根据所述威胁分析字典向用户提供相应的威胁分析。

[0066] 可选的，威胁分析可以包括统计分析和对比分析。其中，统计分析是指为了方便操作人员根据行为查找样本或进行反向查找即根据样本定位行为的分析。对比分析是指对一批样本需要不同版本的测试系统进行对比测试，或者对同一批样本进行多次测试，查看多次测试的对比结果。

[0067] S206、根据用户的选项用相应的数据输出相应的分析文件。

[0068] 可选的，如果用户选择输出统计分析文件，则可以将各个沙箱下的md5_behavior和behavior_md5做为元数据，经过格式化处理然后输出为相应的json文件。如果用户选择输出对比分析文件，则可以用behavior_num下的数据，格式化处理输出相应的对比分析文件。

[0069] 本步骤中，如果多种沙箱都未检测到一些行为、则可以将该行为给从分析文件中删除。

[0070] 第二方面，本发明的实施例还提供一种威胁分析装置，能够提高对威胁的分析效率并改善分析效果。

[0071] 如图4所示，本发明实施例提供的威胁分析装置可以包括：

[0072] 建立单元31，用于建立威胁分析字典，所述威胁分析字典包括至少两个第一键值对，每个所述第一键值对的键为执行威胁检测操作的沙箱的沙箱名，每个所述第一键值对的值包括至少一个第二键值对；其中，所述第二键值对的键包括以下至少一种：行为数量、行为列表、样本触发的行为、行为对应的触发样本；

[0073] 赋值单元32，用于根据威胁检测得到的数据，分别为所述威胁分析字典中的所述第二键值对的值赋值；

[0074] 查询单元33，用于根据用户指令查询所述威胁分析字典，以便根据所述威胁分析字典向用户提供相应的威胁分析。

[0075] 本发明的实施例提供的威胁分析装置，建立了威胁分析字典，在威胁分析字典中对不同沙箱检测到的威胁进行行为数量、行为列表、样本触发的行为、行为对应的触发样本等多方面的统计，并利用威胁检测数据为这些统计项目赋值，这样，当用户需要了解威胁的上述相关特征时，可以根据用户指令从指令中快速调取相应的信息提供给用户，从而有效提高了对威胁的分析效率并改善分析效果。

[0076] 可选的，所述第二键值对中行为数量键对应的值包括至少一个第三键值对；每个所述第三键值对的键为行为名称，值为所述行为名称对应的行为的被触发次数。

[0077] 可选的，赋值单元32包括：

[0078] 提取模块，用于从威胁检测得到的预设文件中提取威胁样本引发的威胁行为的行为名称；

[0079] 赋值模块，用于将所述威胁行为的行为名称赋值给所述第三键值对的键，并将所

述第三键值对的值初始化为0；

[0080] 更新模块，用于遍历威胁检测得到的检测报告，利用所述检测报告中的信息更新所述行为名称对应的行为的被触发次数。

[0081] 可选的，所述预设文件包括翻译文件。

[0082] 可选的，赋值单元32，具体用于：

[0083] 遍历威胁检测得到的检测报告，利用所述检测报告中的信息为所述威胁分析字典中的所述第二键值对的值赋值。

[0084] 可选的，查询单元33可以包括：

[0085] 第一查询模块，用于根据用户的第一指令查询所述威胁分析字典，根据所述威胁分析字典向用户提供一个或多个沙箱中威胁样本与威胁行为之间的对应关系；和/或

[0086] 第二查询模块，用于根据用户的第二指令查询所述威胁分析字典，根据所述威胁分析字典向用户提供一个或多个沙箱中，一个或多个版本的检测系统对威胁行为的检出对比。

[0087] 第三方面，本发明实施例提供一种电子设备，能够提高对威胁的分析效率并改善分析效果。

[0088] 如图4所示，本发明的实施例提供的一种电子设备，可以包括：壳体41、处理器42、存储器43、电路板44和电源电路45，其中，电路板44安置在壳体41围成的空间内部，处理器42和存储器43设置在电路板44上；电源电路45，用于为上述电子设备的各个电路或器件供电；存储器43用于存储可执行程序代码；处理器42通过读取存储器43中存储的可执行程序代码来运行与可执行程序代码对应的程序，用于执行前述任一实施例所述的威胁分析方法。

[0089] 处理器42对上述步骤的具体执行过程以及处理器42通过运行可执行程序代码来进一步执行的步骤，可以参见前述实施例的描述，在此不再赘述。

[0090] 该电子设备以多种形式存在，包括但不限于：

[0091] (1)移动通信设备：这类设备的特点是具备移动通信功能，并且以提供话音、数据通信为主要目标。这类终端包括：智能手机(例如iPhone)、多媒体手机、功能性手机，以及低端手机等。

[0092] (2)超移动个人计算机设备：这类设备属于个人计算机的范畴，有计算和处理功能，一般也具备移动上网特性。这类终端包括：PDA、MID和UMPC设备等，例如iPad。

[0093] (3)便携式娱乐设备：这类设备可以显示和播放多媒体内容。该类设备包括：音频、视频播放器(例如iPod)，掌上游戏机，电子书，以及智能玩具和便携式车载导航设备。

[0094] (4)服务器：提供计算服务的设备，服务器的构成包括处理器、硬盘、内存、系统总线等，服务器和通用的计算机架构类似，但是由于需要提供高可靠的服务，因此在处理能力、稳定性、可靠性、安全性、可扩展性、可管理性等方面要求较高。

[0095] (5)其他具有数据交互功能的电子设备。

[0096] 第四方面，本发明的实施例还提供一种计算机可读存储介质，所述计算机可读存储介质存储有一个或者多个程序，所述一个或者多个程序可被一个或者多个处理器执行，以实现前述实施例提供的任一种威胁分析方法，因此也能实现相应的技术效果，前文已经进行了详细说明，此处不再赘述。

[0097] 需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个.....”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0098] 本说明书中的各个实施例均采用相关的方式描述，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。

[0099] 尤其，对于装置实施例而言，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。

[0100] 为了描述的方便，描述以上装置是以功能分为各种单元/模块分别描述。当然，在实施本发明时可以把各单元/模块的功能在同一个或多个软件和/或硬件中实现。

[0101] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体(Read-Only Memory，ROM)或随机存储记忆体(Random Access Memory，RAM)等。

[0102] 以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到的变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应以权利要求的保护范围为准。

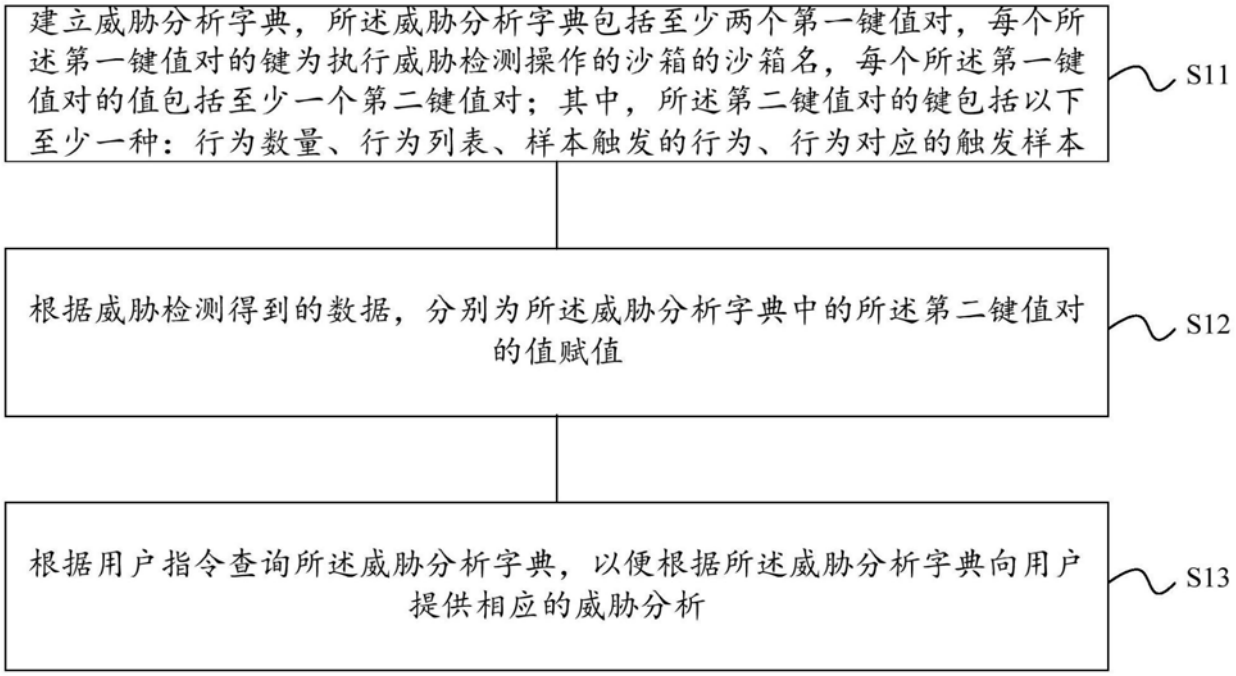

建立威胁分析字典，所述威胁分析字典包括至少两个第一键值对，每个所述第一键值对的键为执行威胁检测操作的沙箱的沙箱名，每个所述第一键值对的值包括至少一个第二键值对；其中，所述第二键值对的键包括以下至少一种：行为数量、行为列表、样本触发的行为、行为对应的触发样本
S11
根据威胁检测得到的数据，分别为所述威胁分析字典中的所述第二键值对的值赋值
S12
根据用户指令查询所述威胁分析字典，以便根据所述威胁分析字典向用户提供相应的威胁分析
S13

图1

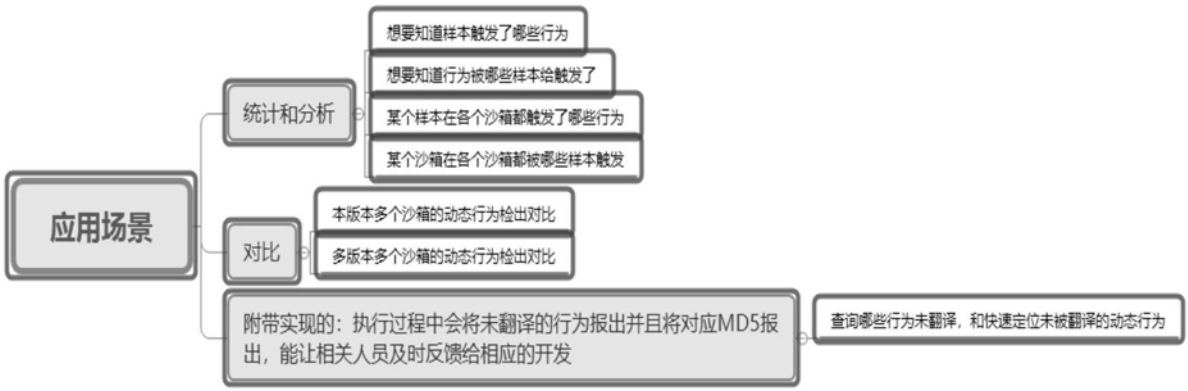

应用场景
统计和分析
想要知道样本触发了哪些行为
想要知道行为被哪些样本给触发了
某个样本在各个沙箱都触发了哪些行为
某个沙箱在各个沙箱都被哪些样本触发
对比
本版本多个沙箱的动态行为检出对比
多版本多个沙箱的动态行为检出对比
附带实现的：执行过程中会将未翻译的行为报出并且将对应MD5报出，能让相关人员及时反馈给相应的开发
查询哪些行为未翻译，和快速定位未被翻译的动态行为

图2


建立威胁分析字典
S201
从威胁检测得到的翻译文件中提取威胁样本引发的威胁行为的行为名称
S202
将所述威胁行为的行为名称赋值给行为数量"behavior_num":{}的键，并将该键对的值初始化为0
S203
遍历威胁检测得到的检测报告，利用所述检测报告中的信息为威胁分析字典中的所述第二键值对的值赋值
S204
根据用户指令查询所述威胁分析字典，以便根据所述威胁分析字典向用户提供相应的威胁分析
S205
根据用户的选项用相应的数据输出相应的分析文件
S206

图3

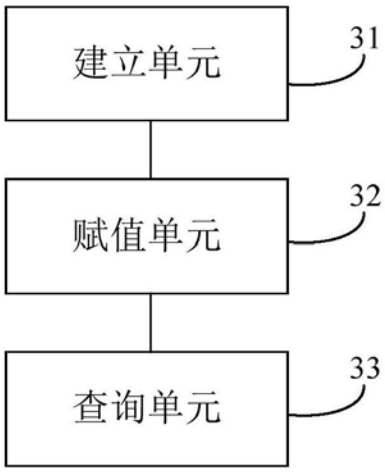

建立单元
31
赋值单元
32
查询单元
33

图4

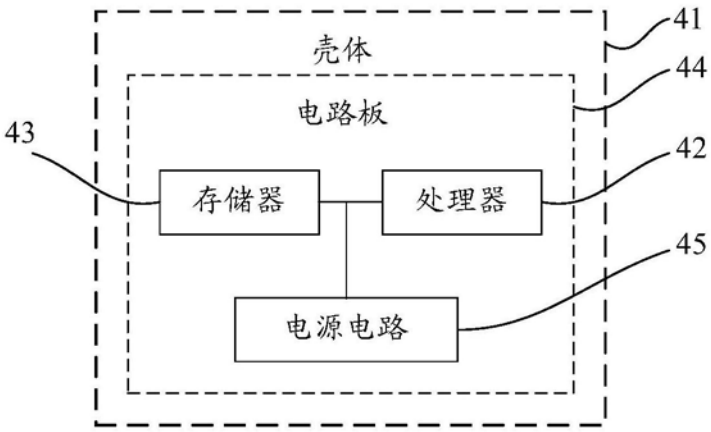


图5