(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 110177114 B
(45)授权公告日 2021.07.13

(21)申请号 201910493265.2
(22)申请日 2019.06.06
(65)同一申请的已公布的文献号
申请公布号 CN 110177114 A
(43)申请公布日 2019.08.27
(73)专利权人 腾讯科技(深圳)有限公司
地址 518057 广东省深圳市南山区高新区科技中一路腾讯大厦35层
(72)发明人 郭豪 洪春华 梁玉
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 孙之刚 刘春元
(51)Int.Cl.
H04L 29/06(2006.01)
G06N 3/04(2006.01)
G06N 3/08(2006.01)

(56)对比文件
CN 107391684 A,2017.11.24
CN 107391598 A,2017.11.24
US 10250621 B1,2019.04.02
徐文韬.面向威胁情报的攻击指示器自动生成.《通信技术》.2017,全文.

审查员 翟倩倩

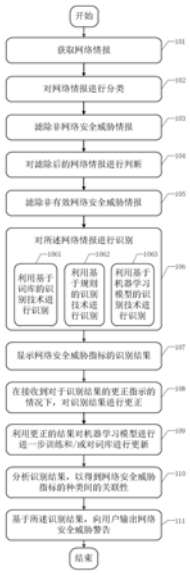
权利要求书3页 说明书12页 附图8页

(54)发明名称

网络安全威胁指标识别方法、设备、装置以及计算机可读存储介质

(57)摘要

公开了一种网络安全威胁指标识别方法,包括:获取网络情报;以及针对至少两种网络安全威胁指标,对所述网络情报进行识别,以得到所述至少两种网络安全威胁指标的识别结果,其中,所述至少两种网络安全威胁指标被预先划分为至少两个组,针对所述至少两个组预先适配各自不同的识别方式,并且其中,所述不同的识别方式包括基于机器学习模型的识别方式。还公开了一种网络安全威胁指标识别设备、装置和计算机可读存储介质。



CN 110177114 B

1．一种网络安全威胁指标识别方法，包括：

获取网络情报；以及

针对至少两种网络安全威胁指标，利用预先适配的识别方式对所述网络情报进行识别，以得到所述至少两种网络安全威胁指标的识别结果，

其中，所述至少两种网络安全威胁指标被预先划分为至少两个组，针对所述至少两个组预先适配各自不同的识别方式，并且

其中，所述不同的识别方式包括基于机器学习模型的识别方式。

2．如权利要求1所述的方法，在对所述网络情报进行识别之前进一步包括：

利用预先配置的机器学习分类模型，将所述网络情报分类成网络安全威胁情报或非网络安全威胁情报；并且

滤除所述网络情报中的非网络安全威胁情报。

3．如权利要求2所述的方法，

其中，所述预先配置的机器学习分类模型包括嵌入层、卷积层、最大池化层和全连接层，并且

其中，所述分类进一步包括：

获取所述网络情报的文本并输入所述嵌入层，以将其编码为分布式表示；

将所述分布式表示输入卷积层，以提取所述网络情报的文本的特征；

将所述特征输入所述最大池化层，以提取每个特征对应的最大值，将提取的每个特征对应的最大值拼接，作为所述最大池化层的输出；

将所述最大池化层的输出输入所述全连接层，基于所述全连接层的输出获得所述分类的结果。

4．如权利要求2所述的方法，在所述分类和所述滤除之后进一步包括：

利用预先配置的机器学习判断模型，判断分类为所述网络安全威胁情报的网络情报是否为有效的网络安全威胁情报；并且

滤除所述网络情报中的非有效的网络安全威胁情报；其中，所述机器学习判断模型包括嵌入层和随机森林层，并且

其中，所述判断包括：

将分类为所述网络安全威胁情报的网络情报的文本输入到所述嵌入层，以将其编码为分布式表示；并且

将所述分布式表示输入到随机森林层，以根据所述随机森林层的输出判断分类为所述网络安全威胁情报的网络情报是否为有效的网络安全威胁情报。

5．如权利要求1-4中任一项所述的方法，其中，所述不同的识别方式还包括：

基于词库的识别方式，其中将所述网络情报中的词与预先建立的词库中的词进行匹配，将能够匹配的词作为识别结果；和

基于规则的识别方式，其中利用预先设置的规则对所述网络情报的文本进行解析，将符合所述规则的内容作为识别结果。

6．如权利要求1-4中任一项所述的方法，进一步包括：

通过web页面显示所述识别结果；以及

在接收到对于所述识别结果的更正指示的情况下，对所述识别结果进行更正。

7．如权利要求1-4中任一项所述的方法，

其中，所述至少两个组中的第一组包括以下种类的网络安全威胁指标：影响地区和平台，并且

其中所述进行识别包括：针对所述第一组中的任一种类的网络安全威胁指标，利用基于词库的识别方式对所述网络情报进行识别，其中基于词库的识别方式是将所述网络情报中的词与预先建立的词库中的词进行匹配，将能够匹配的词作为识别结果。

8．如权利要求1-4中任一项所述的方法，

其中，所述至少两个组中的第二组包括以下种类的网络安全威胁指标：程序的基本数据文件、注册表、服务和启动项，并且

其中所述进行识别包括：针对所述第二组中的任一种类的网络安全威胁指标，利用基于规则的识别方式对所述网络情报进行识别，其中基于规则的识别方式是利用预先设置的规则对所述网络情报进行解析，将符合所述规则的内容作为识别结果。

9．如权利要求1-4中任一项所述的方法，

其中，所述至少两个组中的第三组包括以下种类的网络安全威胁指标：木马家族、威胁组织、威胁对象、威胁手法、漏洞使用、文件哈希、IP地址、域名、文件信息、全球资源定位器、互斥锁和邮箱，并且

其中所述进行识别包括：针对所述第三组中的任一种类的网络安全威胁指标，利用基于机器学习模型的识别方式对所述网络情报进行识别。

10．如权利要求1-4中任一项所述的方法，进一步包括：

统计分析所述识别结果，以得到所述网络安全威胁指标的种类间的关联性；和/或

基于所述识别结果，输出网络安全威胁警告。

11．如权利要求6所述的方法，进一步包括：

在所述识别结果是利用基于机器学习模型的识别方式识别出来的情况下，利用所更正的识别结果对所述机器学习模型进行进一步训练；和/或

在所述识别结果是利用基于词库的识别方式识别出来的情况下，利用所更正的识别结果对词库进行更新，其中基于词库的识别方式是将所述网络情报中的词与预先建立的词库中的词进行匹配，将能够匹配的词作为识别结果。

12.如权利要求1-4中任一项所述的方法，其中，所述机器学习模型包括第一嵌入层、第二嵌入层、第一层双向长短时记忆层、第二层双向长短时记忆层、前馈神经网络层和优化层；并且

其中，利用所述机器学习模型对所述网络情报进行识别包括：

将所述网络情报的词的下一级元素输入所述第一嵌入层，以编码为所述下一级元素的分布式表示；

将所述下一级元素的分布式表示输入所述第一层双向长短时记忆层，得到所述第一层双向长短时记忆层的输出；

将所述网络情报的词输入所述第二嵌入层，以编码为所述词的分布式表示；

将所述第一层双向长短时记忆层的输出与所述词的分布式表示拼接后输入所述第二层双向长短时记忆层，得到第二层双向长短时记忆层的输出；

将所述第二层双向长短时记忆层的输出输入到具有一个隐藏层的前馈神经网络层，得

到词中具有各个网络安全威胁指标的概率;以及

将所述概率输入所述优化层,得到的输出为所述网络情报中的网络安全威胁指标。

13. 一种网络安全威胁指标识别设备,包括:

获取器,其被配置来获取网络情报;以及

识别器,其被配置来针对至少两种网络安全威胁指标,对所述网络情报进行识别,以得到所述至少两种网络安全威胁指标的识别结果,

其中,所述至少两种网络安全威胁指标被预先划分为至少两个组,针对所述至少两个组预先适配各自不同的识别方式,并且

其中,所述不同的识别方式包括基于机器学习模型的识别方式。

14. 一种网络安全威胁指标识别装置,包括:

处理器;以及

存储器,其被配置为在其上存储有计算机可执行指令,所述指令当在所述处理器中执行时,使得所述处理器实现如权利要求1-12中任一项所述的方法。

15.一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中存储有指令,当所述指令在计算机上运行时,使得所述计算机实现如权利要求1-12中任一项所述的方法。

网络安全威胁指标识别方法、设备、装置以及计算机可读存储介质

技术领域

[0001] 本申请涉及网络安全，更具体地，涉及网络安全威胁指标识别方法、设备、装置以及计算机可读存储介质。

背景技术

[0002] 威胁情报，根据Gartner的定义，是某种基于证据的知识，包括上下文、机制、标示、含义和能够执行的建议，这些知识与资产所面临已有的或酝酿中的威胁或危害相关，可用于资产相关主体对威胁或危害的响应或处理决策提供信息支持。业内大多数所说的威胁情报可以认为是狭义的威胁情报，其主要内容为用于识别和检测网络安全威胁指标(Indicators of Compromise，IOC)，如文件哈希、IP地址、域名等，本文中将此类威胁情报称为网络安全威胁情报。网络情报，泛指网络安全威胁情报和非网络安全威胁情报，可能仅具有网络安全威胁情报，或可能仅具有非网络安全威胁情报，或可能二者都有。从可能同时具有网络安全威胁情报和非网络安全威胁情报的网络情报中提取网络安全威胁情报是一件费时费力的工作。此外，网络安全威胁情报中包含威胁信息，可供分析以识别网络安全威胁指标(Indicators of Compromise，IOC)，来例如形成威胁情报库等以供后续使用。网络安全威胁情报根据来源主要分为两大类：内部网络安全威胁情报和外部网络安全威胁情报。内部网络安全威胁情报多是通过分析系统内部数据来收集、处理的，外部网络安全威胁情报主要源自企业和/或社区提供的共享或付费的网络安全威胁情报。鉴于内部网络安全威胁情报的封闭性和特殊性，验证网络安全威胁指标时一般不使用内部网络安全威胁情报。在网络安全领域，外部网络安全威胁情报对全网网络安全感知有很重要的作用，但是外部网络安全威胁情报数据量巨大，很难通过人工的方式逐一识别，费时费力且可能存在漏报、误报。

发明内容

[0003] 本发明的实施例提供了网络安全威胁指标识别方法、设备、装置以及计算机可读存储介质，至少部分地解决上面提及的问题。

[0004] 根据本发明的第一方面，提供一种网络安全威胁指标识别方法，包括：获取网络情报；以及针对至少两种网络安全威胁指标，对所述网络情报进行识别，以得到所述至少两种网络安全威胁指标的识别结果，其中，所述至少两种网络安全威胁指标被预先划分为至少两个组，针对所述至少两个组预先适配各自不同的识别方式，并且其中，所述不同的识别方式包括基于机器学习模型的识别方式。

[0005] 根据一个实施例，在所述识别之前所述方法进一步包括：利用预先配置的机器学习分类模型，将所述网络情报分类成网络安全威胁情报或非网络安全威胁情报；并且滤除所述网络情报中的非网络安全威胁情报。

[0006] 根据一个实施例，其中，所述预先配置的机器学习分类模型包括嵌入层、卷积层、

最大池化层和全连接层，并且其中，所述分类进一步包括：获取所述网络情报的文本并输入所述嵌入层，以将其编码为分布式表示；将所述分布式表示输入卷积层，以提取所述网络情报的文本的特征；将所述特征输入所述最大池化层，以提取每个特征对应的最大值，将提取的每个特征对应的最大值拼接，作为所述最大池化层的输出；将所述最大池化层的输出输入所述全连接层，基于所述全连接层的输出获得所述分类的结果。

[0007] 根据一个实施例，所述方法，在所述分类和所述滤除之后进一步包括：利用预先配置的机器学习判断模型，判断分类为所述网络安全威胁情报的网络情报是否为有效的网络安全威胁情报；并且滤除所述网络情报中的非有效的网络安全威胁情报。

[0008] 根据一个实施例，其中，所述机器学习判断模型包括嵌入层和随机森林层，并且其中，所述判断包括：将分类为所述网络安全威胁情报的网络情报的文本输入到所述嵌入层，以将其编码为分布式表示；并且将所述分布式表示输入到随机森林层，以根据所述随机森林层的输出判断分类为所述网络安全威胁情报的网络情报是否为有效的网络安全威胁情报。

[0009] 根据一个实施例，其中，所述不同的识别方式还包括：基于词库的识别方式，其中将所述网络情报中的词与预先建立的词库中的词进行匹配，将能够匹配的词作为识别结果；和基于规则的识别方式，其中利用预先设置的规则对所述网络情报的文本进行解析，将符合所述规则的内容作为识别结果。

[0010] 根据一个实施例，所述方法进一步包括：显示所述识别结果；以及在接收到对于所述识别结果的更正指示的情况下，对所述识别结果进行更正。

[0011] 根据一个实施例，其中，所述显示所述识别结果包括：通过web页面显示所述识别结果。

[0012] 根据一个实施例，其中，所述至少两个组中的第一组包括以下种类的网络安全威胁指标：影响地区和平台，并且其中所述进行识别包括：针对所述第一组中的任一种类的网络安全威胁指标，利用基于词库的识别方式对所述网络情报进行识别，其中基于词库的识别方式是将所述网络情报中的词与预先建立的词库中的词进行匹配，将能够匹配的词作为识别结果。

[0013] 根据一个实施例，其中，所述至少两个组中的第二组包括以下种类的网络安全威胁指标：程序的基本数据文件、注册表、服务和启动项，并且其中所述进行识别包括：针对所述第二组中的任一种类的网络安全威胁指标，利用基于规则的识别方式对所述网络情报进行识别，其中基于规则的识别方式是利用预先设置的规则对所述网络情报进行解析，将符合所述规则的内容作为识别结果。

[0014] 根据一个实施例，其中，所述至少两个组中的第三组包括以下种类的网络安全威胁指标：木马家族、威胁组织、威胁对象、威胁手法、漏洞使用、文件哈希、IP地址、域名、文件信息、全球资源定位器、互斥锁和邮箱，并且其中所述进行识别包括：针对所述第三组中的任一种类的网络安全威胁指标，利用基于机器学习模型的识别方式对所述网络情报进行识别。

[0015] 根据一个实施例，所述方法进一步包括：统计分析所述识别结果，以得到所述网络安全威胁指标的种类间的关联性；和/或基于所述识别结果，向用户输出网络安全威胁警告。

[0016] 根据一个实施例，其中，所述获取网络情报包括：通过爬虫技术爬取外部情报源以获取网络情报。

[0017] 根据一个实施例，所述方法进一步包括：在所述识别结果是利用基于机器学习模型的识别方式识别出来的情况下，利用所更正的识别结果对所述机器学习模型进行进一步训练；和/或在所述识别结果是利用基于词库的识别方式识别出来的情况下，利用所更正的识别结果对词库进行更新，其中基于词库的识别方式是将所述网络情报中的词与预先建立的词库中的词进行匹配，将能够匹配的词作为识别结果。

[0018] 根据一个实施例，其中，所述机器学习模型包括第一嵌入层、第二嵌入层、第一层双向长短时记忆层、第二层双向长短时记忆层、前馈神经网络层和优化层；并且其中，利用所述机器学习模型对所述网络情报进行识别包括：将所述网络情报的词的下一级元素输入所述第一嵌入层，以编码为所述下一级元素的分布式表示；将所述下一级元素的分布式表示输入所述第一层双向长短时记忆层，得到所述第一层双向长短时记忆层的输出；将所述网络情报的词输入所述第二嵌入层，以编码为所述词的分布式表示；将所述第一层双向长短时记忆层的输出与所述词的分布式表示拼接后输入所述第二层双向长短时记忆层，得到第二层双向长短时记忆层的输出；将所述第二层双向长短时记忆层的输出输入到具有一个隐藏层的前馈神经网络层，得到词中具有各个网络安全威胁指标的概率；以及将所述概率输入所述优化层，得到的输出为所述网络情报中的网络安全威胁指标。

[0019] 根据本发明的第二方面，提供一种网络安全威胁指标识别设备，包括：获取器，其被配置来获取网络情报；以及识别器，其被配置来针对至少两种网络安全威胁指标，对所述网络情报进行识别，以得到所述至少两种网络安全威胁指标的识别结果，其中，所述至少两种网络安全威胁指标被预先划分为至少两个组，针对所述至少两个组预先适配各自不同的识别方式，并且其中，所述不同的识别方式包括基于机器学习模型的识别方式。

[0020] 根据本发明的第三方面，提供了一种网络安全威胁指标识别装置，包括：处理器；以及存储器，其配置为在其上存储有计算机可执行指令，所述指令当在所述处理器中执行时，使得所述处理器实现上述第一方面及其任一实施例的方法。

[0021] 根据本发明的第四方面，提供了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中存储有指令，当所述指令在计算机上运行时，使得所述计算机实现上述第一方面及其任一实施例的方法。

[0022] 根据上述实施例，采用自动化的网络安全威胁标志的识别方式，避免了人工识别的耗时耗力。由于我们对需要识别的至少两个种类的网络安全威胁标志依据识别方式进行分组，通过与不同分组对应的基于机器学习模型的识别方式、基于词库的识别方式和基于规则的识别方式来识别，照此，能够利用不同种类的网络安全威胁指标的特点而有利地进行识别，避免了采用单个识别方式的局限性，例如，基于规则的识别方式对一些种类的网络安全威胁指标(例如攻击组织)是无效的，无法有效识别，而代之以基于机器学习模型的识别方式则可以有效地识别，一定程度上解决了漏报和误报的问题。通过例如和WEB页面的交互，机器学习模型能够不断地收到前端反馈的结果，从而不断训练、优化该机器学习模型，机器学习模型的识别准确性从而不断提高，词库也能得到不断的更新，这也在一定程度上解决了漏报和误报的问题。另外，采用的机器学习模型能识别上下文的特征，从而能区分报告中出现的非恶意网络安全威胁指标，这又在一定程度上解决了漏报和误报的问题。在实

施例中，利用预先配置的机器学习分类模型，将所述网络情报进行分类，以分成网络安全威胁情报和非网络安全威胁情报并去除非网络安全威胁情报，可以进一步解放人力，无需人工筛选，从而可以灵活适用于各种情报来源。在进一步的实施例中，利用预先配置的机器学习判断模型，判断分类为所述网络安全威胁情报的网络情报是否为有效的网络安全威胁情报，并进一步去除所述网络情报中的非有效的网络安全威胁情报，能够进一步帮助提高识别效率。

附图说明

[0023] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例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。

[0024] 图1图示了根据本发明实施例的网络安全威胁指标识别方法的流程图。

[0025] 图2图示了根据本发明实施例的机器学习模型的一个结构示例。

[0026] 图3图示了根据本发明实施例的机器学习分类模型的一个结构和处理示例。

[0027] 图4图示了根据本发明实施例的机器学习判断模型的一个结构和处理示例。

[0028] 图5图示了根据本发明实施例的机器学习模型的一个输出示例。

[0029] 图6a图示了根据本发明实施例的识别结果的一个显示界面。

[0030] 图6b图示了根据本发明实施例的识别结果的另一个显示界面。

[0031] 图7图示了根据本发明实施例的用于网络安全威胁指标识别的设备的框图。

[0032] 图8图示了根据本发明实施例的硬件实施环境示意图。

具体实施方式

[0033] 为使本申请的目的、技术方案和优点更加清楚，下面将结合附图对本申请实施方式作进一步地详细描述。

[0034] 本文中所称的网络安全威胁情报是指包含威胁信息，可供识别以识别出网络安全威胁指标(IOC)的信息。本文所称的网络情报泛指网络安全威胁情报和非网络安全威胁情报，可能仅具有网络安全威胁情报，或可能仅具有非网络安全威胁情报，或可能二者都有。本文中所称的网络安全威胁指标是指标识系统或网络中潜在恶意活动的证据数据。

[0035] 图1图示了根据本发明实施例的网络安全威胁指标识别方法的流程图。需注意，以下描述的先后顺序并不代表步骤本身的执行顺序，这些步骤可以以任何合理的顺序先后或者同时执行，除非后以步骤的执行必须以前一步骤为前提。根据本发明实施例的网络安全威胁指标识别方法开始于步骤101。在其中，获取网络情报，在一个示例中，可以通过爬虫技术爬取外部网络安全威胁情报源以获取网络情报。该外部网络安全威胁情报源通常选自网络威胁情报共享平台，例如是网站www.freebuf.com上共享的网络情报。当然，在另一个示例中，该网络情报也可能掺杂有非网络安全威胁情报。

[0036] 而后在步骤106，针对至少两种网络安全威胁指标，利用预先适配的识别方式对所述网络情报进行识别，以得到所述至少两种网络安全威胁指标的识别结果。其中，所述至少两种网络安全威胁指标被预先划分为至少两个组，针对所述至少两个组预先适配各自不同

的识别方式，在一个示例中，选取了18个种类的网络安全威胁指标，分别是：木马家族、威胁组织、威胁对象、影响地区、威胁手法、漏洞、平台、文件哈希、IP地址、域名、文件信息、全球资源定位器、程序的基本数据文件、互斥锁、注册表、服务、启动项和邮箱。木马家庭例如Trickbot、jasperloader、artradownloader、bulehero等。威胁组织例如有APT10、蔓灵花、muddywater等发起威胁的组织。威胁对象例如有金融部门、政府机构、教育机构等威胁的目标。影响地区是指威胁影响的地理上的范围。威胁手法顾名思义即威胁所采用的手段，例如分布式拒绝服务(DDoS: Distributed Denial of Service)，攻击者借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DDoS攻击，从而成倍地提高拒绝服务攻击的威力。威胁手法还有漏洞利用、诱骗文件、恶意邮件、Windows PowerShell(一种命令行外壳程序和脚本环境)、网络钓鱼(Phishing)等。其中网络钓鱼是指诈骗者通常将自己伪装成网络银行、在线零售商和信用卡公司等可信的品牌，利用欺骗性的电子邮件和伪造的Web站点来进行网络诈骗活动，受骗者往往会泄露自己的私人资料，如信用卡号、银行卡账户、身份证号等内容。漏洞是指所利用的漏洞，例如CVE(Common Vulnerabilities & Exposures，公共漏洞和暴露)编号为CVE-2017-8464、CVE-2019-2725、CVE-2017-12615、CVE-2017-10271、CVE-2017-5638、CNVD-2018-24942等的漏洞。平台指威胁针对的平台，例如windows、linux、Mac OS等。文件哈希(即Hash)又叫文件签名，文件中哪怕一个比特位被改变了，文件哈希就会不同，因此可用于区分不同文件，比较常用的文件哈希算法有MD5和SHA-1，图6b右边下方列出了12个文件哈希。IP地址例如65.182.100.42、81.88.24.211、103.219.22.63等。域名例如：

[0037] breed.wanttobea.com、

[0038] zzi.aircargox.com、

[0039] nono.littlebodiesbigsouls.com、

[0040] tribunaledinapoli.recsinc.com、

[0041] tribunaledinapoli.prepperpillbox.com、

[0042] tribunaledinapoli.lowellunderwood.com、

[0043] tribunaledinapoli.rntman.com等。

[0044] 文件信息例如kernel.dll、winserv.exe、rundll32.exe、rtegre.exe、wprgxyeqd79.exe等。全球资源定位器(URL)例如：

[0045] http://planasolutions.com/wordpress/wp-content/nq3sqe-x875-tt/、

[0046] http://mattheweidem.com/iknOowm-g991-syvw/、

[0047] http://irose.com/lpo7qje-wg556-pnv/等。

[0048] 程序的基本数据文件(PDB,Program Data Base)例如：

[0049] C:\Users\CN_ide\Desktop\TSSL_v3.2.7_BypassSymantec_20180528\TClient\Release\FakeRun.pdb、

[0050] D:\Soft\DevelopedCode_Last\yty2.0\Release\C++\Setup.pdb、

[0051] C:\users\803\documents\visualstudio2010\Projects\helpdll\Release\helpdll.pdb等。互斥锁例如{531511FA-190D-5D85-8A4A-279F2F592CC7}等。注册表例如：

[0052] Software\Microsoft\Office\12.0\Word\Resiliency\DisabledItems、

[0053] Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems、

[0054] Software\Microsoft\Office\11.0\Word\Resiliency\DocumentRecovery、

[0055] Software\Microsoft\Office\11.0\Word\Resiliency\DisabledItems等。启动项例如memory optimizer.lnk、SLVjiAEwaK.url、SMTPLoader.lnk等。服务例如ndisproxy-mn、Wmmvsvc、SCardPrv等。邮箱例如:ijuqodisunovib98@o2.pl、sayanwalsworth96@protonmail.com、abbschevis@protonmail.com、cottleakela@protonmail.com、aperywsqaroci@o2.pl、asuxidoruraep1999@o2.pl、couwetizotofo@o2.pl、dharmaparrack@protonmail.co等。

[0056] 在一个示例中,上述18个种类的网络安全威胁指标被划分成了三个组,每一组预先适配一种识别方式,针对三个组所预先适配的识别方式各不相同。其中第一组包含影响地区和平台,第二组包含基本数据文件、注册表、服务和启动项,第三组包含剩下的,即木马家族、威胁组织、威胁对象、威胁手法、漏洞、文件哈希、IP地址、域名、文件信息、全球资源定位器、互斥锁和邮箱。划分组的依据就是识别方式,对于上述第一组,在步骤1061,利用基于词库的识别方式对所述网络情报进行识别,对于上述第二组,在步骤1062,利用基于规则的识别方式对所述网络情报进行识别,对于上述第三组,在步骤1063,利用基于机器学习模型的识别方式对所述网络情报进行识别。

[0057] 基于词库的识别方式直接对网络情报全文中的所有词与预先建立的词库中的词进行匹配,词库包括平台的词库和影响地区的词库,均可以通过公开的网络安全威胁指标的数据源而获得,当然也可以人工建立或修改。对于这两个种类,由于平台和影响地区比较稳定,可枚举,适合采用词库的方式进行识别。平台的词库例如包括“Linux”、“Windows”等,影响地区的词库例如包括“China”、“US”、“Japan”等,当然词库也可以包括对应的中文或其它国家的语言)。能够匹配上的即识别为相应的网络安全情报指标,例如平台或者影响地区。

[0058] 基于规则的识别方式利用预定规则(例如识别基本数据文件的规则、识别注册表的规则、识别服务的规则和识别启动项的规则)对网络情报的全文中进行解析,将符合所述规则的内容作为识别结果,例如基本数据文件、注册表、服务或启动项,这些种类的规则比较固定,不用经常维护变动。例如识别基本数据文件的规则可以例如用正则表达式表达为:

[0059] r’\b([A-Za-z0-9-_\.]+\.(pdb))\b’

[0060] 其中r’’用’’引出原生字符串,该字符串以.pdb结尾,.pdb前面可以是大小写字母和所列举的符号的任意一个或多于一个,\b表示边界。该正则表达式通用于多种编程环境,或者可能对于某些特定环境需要较小的修改。

[0061] 基于机器学习模型的识别方式中的机器学习模型可以采用多种不同的结构。图2图示了根据本发明实施例的机器学习模型的一个结构示例。所述机器学习模型包括第一嵌入层、第二嵌入层、第一层双向长短时记忆层、第二层双向长短时记忆层、前馈神经网络层和优化层。每一层双向长短时记忆层均由类型为长短时记忆(LSTM)的循环神经网络(RNN,Recurrent Neural Network)元素构成。利用所述机器学习模型对所述网络情报进行识别包括一下操作。将所述网络情报的词的下一级元素输入所述第一嵌入层,以编码为所述下一级元素的分布式表示;将所述下一级元素的分布式表示输入所述第一层双向长短时记忆层,得到所述第一层双向长短时记忆层的输出;将所述网络情报的词输入所述第二嵌入层,以编码为所述词的分布式表示;将所述第一层双向长短时记忆层的输出与所述词的分布式

表示拼接后输入所述第二层双向长短时记忆层，得到第二层双向长短时记忆层的输出；将所述第二层双向长短时记忆层的输出输入到具有一个隐藏层的前馈神经网络层，得到词中具有各个网络安全威胁指标的概率；以及将所述概率输入所述优化层，得到的输出为所述网络情报中的网络安全威胁指标。参见图2，输入X_{ij}是词X_i（其中i=1，……，n， j=1，……，符号X_i中的字符数）中的下一级元素，诸如词素（前缀或后缀）、词根，词X_i来自待识别的网络情报，Vc是词的下一级元素到其分布式表示（词向量）的映射，在此作为第一嵌入层，X_{ij}经过Vc映射后输入第一层双向长短时记忆层。V_T是词X_i（其中i=1，……，n， j=1，……，符号X_i中的字符数）到其分布式表示（即词向量）的映射，在此称为第二嵌入层。第一层双向长短时记忆层的输出与词X_i经过V_T的映射后输出拼接得到e_i（其中i=1，……，n），作为第二层双向长短时记忆层的输入，而后得到第二层双向长短时记忆层的输出d_i（其中i=1，……，n），经过具有一个隐藏层的前馈神经网络，得到概率向量a_i（其中i=1，……，n），a_n的第t个元素是第n个词具有第t个IOC的概率。以a_i为输入，进而得到输出y_i（其中i=1，……，n），即识别出的词中的网络安全威胁指标，例如在a_i中具有最高概率的IOC。在一个示例中，训练数据集来源于人工标注的200篇APT（Advanced Persistent Threats，高级持续性威胁）报告的文本。将训练数据集经过预处理（例如特殊字符替换、分段等）后输入图2所示的机器学习模型中进行训练，训练完成后，即可用于网络安全威胁指标的识别。经测试，该机器学习模型识别的网络安全威胁指标的F1分数（F1分数是是统计学中用来衡量二分类模型精确度的一种指标。它同时兼顾了分类模型的准确率和召回率。F1分数可以看作是模型准确率和召回率的一种加权平均，它的最大值是1，最小值是0）在0.9左右。

[0062] 应注意，各种不同的识别方式可能涉及文本的匹配或输入，并不意味着网络情报必须是文本的形式，其也可以是其他任何的形式，例如图片、音频等形式，它们例如可以转化成文本进行匹配或输入。

[0063] 基于机器学习模型的识别方式更灵活适用于各种目标的识别，对于用基于规则和词库的识别方式都不能很好地识别出来的网络安全威胁指标种类，或者需要大量精力去维护词库或规则的，用基于机器学习模型的识别方式更合适。

[0064] 本发明的发明人认识到不同种类的网络安全威胁指标的不同特点以及与基于词库、规则或机器学习模型的识别方式的适应性，因而采用上述分组适配的方式，相比于无视不同种类的网络安全威胁指标的不同特点的单一识别方式或者盲目多样的识别方式，能够更加高效、准确地进行网络安全威胁指标识别。

[0065] 可选地，在步骤101之后、步骤1061-1063之前，还在步骤102中，考虑到获取的网络情报中存在非网络安全威胁情报，利用预先配置的机器学习分类模型，将步骤101获取的网络情报分类成网络安全威胁情报或非网络安全威胁情报，并且在步骤103中，滤除所述网络情报中的非网络安全威胁情报。这样可以进一步解放人力，无需人工筛选，从而可以灵活适用于各种情报来源。预先配置的机器学习分类模型和处理示例例如如图3所示。在图3中，预先配置的机器学习分类模型300包括嵌入层301、卷积层302、最大池化层303和全连接层304。所述分类包括：首先获取所述网络情报的文本并输入所述嵌入层301，以将其编码为分布式表示，而后将所述分布式表示输入卷积层302，以提取所述网络情报的文本的特征，而后将所述特征输入所述最大池化层303，以提取每个特征对应的最大值，并将提取的每个特征对应的最大值拼接，作为所述最大池化层的输出。最后将所述最大池化层的输出输入所

述全连接层304，就可以基于所述全连接层的输出获得所述分类的结果。所述机器学习分类模型可以采用1万篇网络安全威胁情报和一万篇非网络安全威胁情报的例如标题和关键词进行训练。

[0066] 可选地，在步骤103之后、步骤1061-1063之前，还在步骤104中，利用预先配置的机器学习判断模型，判断分类为所述网络安全威胁情报的网络情报是否为有效的网络安全威胁情报，例如存在这种情况，同样一个词，在不同语境下具有不同的含义，从而有时它是网络安全威胁指标而有时并不是，即，它是非有效的网络安全威胁情报。经过这样的判断，就可以在步骤105中，滤除所述网络情报中的非有效的网络安全威胁情报。预先配置的机器学习判断模型和处理示例例如如图4所示。在图4中，所述机器学习判断模型400包括嵌入层401和随机森林层402。所述判断包括：首先，将分类为所述网络安全威胁情报的网络情报的文本输入到所述嵌入层401，以将其编码为分布式表示，然后将所述分布式表示输入到随机森林层402，以根据所述随机森林层的输出判断分类为所述网络安全威胁情报的网络情报是否为有效的网络安全威胁情报。通过这些步骤，能够进一步帮助提高识别效率。所述机器学习判断模型可以采用人工标注的2000篇网络安全威胁情报进行训练，其中800篇是有效的网络安全威胁情报，1200篇是无效的网络安全威胁情报。

[0067] 应注意，本文中获取的网络情报的文本可以是各种语言，在一个示例中，可以对它们按照语言进行区分，用对应的不同语言训练出来的机器学习分类模型、机器学习判断模型和用于识别IOC的机器学习模型对它们进行处理。

[0068] 根据上述实施例可见，不论是基于词库、规则还是机器学习模型的识别方式，均是自动化的网络安全威胁标志的识别方式，避免了人工识别的耗时耗力。由于我们对需要识别的至少两个种类的网络安全威胁标志依据识别方式进行分组，通过与不同分组对应的基于机器学习模型的识别方式、基于词库的识别方式和基于规则的识别方式来识别，照此，能够利用不同种类的网络安全威胁标志的特点而有利地进行识别，避免了采用单个识别方式的局限性，例如，基于规则的识别方式对一些种类的网络安全威胁标志(例如攻击组织)是无效的，无法有效识别，而代之以基于机器学习模型的识别方式则可以有效地识别，一定程度上解决了漏报和误报的问题。采用的机器学习模型能识别上下文的特征，从而能区分报告中出现的非恶意网络安全威胁指标，这在一定程度上解决了漏报和误报的问题。在实施例中，利用预先配置的机器学习分类模型，将所述网络情报进行分类，以分成网络安全威胁情报和非网络安全威胁情报并去除非网络安全威胁情报，可以进一步解放人力，无需人工筛选，从而可以灵活适用于各种情报来源。在进一步的实施例中，利用预先配置的机器学习判断模型，判断分类为所述网络安全威胁情报的网络情报是否为有效的网络安全威胁情报，并进一步去除所述网络情报中的非有效的网络安全威胁情报，能够进一步帮助提高识别效率。

[0069] 图5图示了根据本发明实施例的机器学习模型的一个输出示例。利用上述训练好的图2所示的模型对例如从www.freebuf.com上获取的网络情报进行识别，得到图5所示的输出，其中第一列为网络情报中的词，例如194.70.136，最后一列是所识别成的网络安全威胁指标，例如B-IP，即指IP地址，B-DOMAIN即指域名，B-FILEHASH即指文件哈希。

[0070] 可选地，在步骤107，显示所述至少两个种类的网络安全威胁指标的识别结果。所述显示可以通过web页面进行显示。图6a图示了根据本发明实施例的识别结果的一个显示

界面，其示出了与所识别的网络情报有关的多个事项。其中第一列GUID是获取的网络情报唯一标识，第二列是其标题，第三列是对该网络情报的标注状态，第四列是操作人，第五列是该网络情报的爬取时间；第六列是人工核查时间。

[0071] 图6b图示了根据本发明实施例的识别结果的另一个显示界面。其示出了能够进行人工核查和修改的操作界面，其中右侧是需标注的网络安全威胁指标，在人工核查前，会将步骤106的识别结果加载到右侧相应的网络安全威胁指标里，通过在相应网络安全威胁指标上点击，可以显示或隐藏所加载的识别结果，可以对识别结果进行手动增加、删除、查找和修改。左侧有一个大的文本框，其中呈现网络情报的原文，其中可以显示可选择的文本。

[0072] 下面讨论可选的步骤108，计算机在接收到的对于所述识别结果的更正指示的情况下，例如通过用户接口从用户收到指示，对所述识别结果进行更正。例如，当需要将某个词人工标注为某一网络安全威胁指标时，需要人工选中该词，然后点击上面的“标注”按钮，然后从随后显示的菜单里选择要标注的网络安全威胁指标的种类。当然，还可以以类似的方式借助于其它菜单或按钮以人工的方式进行修改或删除，此类标注、修改或删除均会在右侧相应字段中体现。人工标注完毕之后，点击“保存修改”按钮。在一个示例中，该保存不仅在本地保存，还会提交到服务器保存。这样就完成了对步骤106的识别结果的更正。图6b所示的界面中还有以下按钮：“重置”按钮，即放弃所有人工标注和修改，重置为步骤106中自动的识别结果；“删除所有标注”按钮，即删除当前网络情报中的所有标注，包括自动的标注和人工的标注。当然还可以有其它按钮来辅助对计算机的识别结果进行手动增加、删除、查找和修改。

[0073] 步骤108得到的更正的结果可以反馈到计算机，以对其识别进行优化，特别是基于机器学习模型的识别和基于词库的识别。因此可选地，在步骤109，在所述识别结果是利用基于机器学习模型的识别方式所识别出来的情况下，利用步骤108中所更正的结果对所述机器学习模型进行进一步训练；和/或在所述识别结果是利用基于词库的识别方式所识别出来的情况下，利用步骤108中所更正的结果对词库进行更新。

[0074] 通过和例如WEB页面的交互，机器学习模型能够不断地收到前端反馈的结果，从而不断训练、优化该机器学习模型，机器学习模型的识别准确性从而不断提高，词库也能得到不断的更新，这也在一定程度上解决了漏报和误报的问题。

[0075] 不论是步骤106得到的由计算机识别出的识别结果，还是步骤108得到的更正的结果，均可作为基础以向用户输出网络安全威胁警告，也可以用作进一步的分析，例如网络安全威胁指标的种类间的关联性的统计分析，例如某个攻击组织，它常用什么攻击手法，攻击什么攻击对象，用到的什么恶意IP地址、域名、作为文件哈希的md5是哪些，域名注册者用的邮箱是什么等等，可以将这些信息关联起来，有助于其它应用，例如基于这些关联的信息更快地实现关联的IOC的识别。因此可选地，在步骤110，分析识别结果，以得到所述网络安全威胁指标的种类间的关联性。以及可选地，在步骤111，基于所述识别结果，向用户输出网络安全威胁警告。

[0076] 该流程可以定期执行，以不断优化。例如，每天爬取新增的网络情报(步骤101)，可选地经过分类、判断和滤除(步骤102-105)的处理之后，进行自动化识别(步骤106)，通过步骤107和108接受人工核查，将更正的结果用于识别方式的优化(步骤109)，如此循环，有利于不断提高自动识别的可靠性，与时俱进。

[0077] 图7图示了根据本发明实施例的网络安全威胁指标识别设备的框图。该设备包括获取器701和识别器702。其中获取器701被配置来获取网络情报，在一个示例中，获取器701通过爬虫技术爬取外部网络安全威胁情报源以获取网络情报。该外部网络安全威胁情报源通常选自网络威胁情报共享平台，例如是网站www.freebuf.com上共享的网络情报。当然，在另一个示例中，该网络情报也可能掺杂有非网络安全威胁情报。识别器702被配置来针对至少两种网络安全威胁指标，对所述网络情报进行识别，以得到所述至少两种网络安全威胁指标的识别结果。其中，所述至少两种网络安全威胁指标被预先划分为至少两个组，针对所述至少两个组预先适配各自不同的识别方式。上述至少两个种类的网络安全威胁指标及其分组的示例，以及对应适配的识别方式的示例——基于词库的识别方式、基于规则的识别方式以及基于机器学习算法的识别方式，可以具体参见上面步骤106中的相应描述，在此不再赘述。图7中分别以词库识别器7021实现基于词库的识别方式，以规则识别器7022实现基于规则的识别方式，以机器学习模型识别器7023实现基于机器学习模型的识别方式。

[0078] 可选地，网络安全威胁指标识别设备还可以包括人机接口703，其中进一步包括输入单元7031和输出单元7032，输出单元7032示出至少两个种类的网络安全威胁指标的识别结果；输入单元7032响应于接收到的对于所述识别结果的更正指示，对所述识别结果进行更正。更正的结果可以反馈到识别器702，以对其识别进行优化，特别是机器学习模型识别器7023和词库识别器7021。优化的方式参考上面步骤109的描述，在此不再赘述。

[0079] 可选地，网络安全威胁指标识别设备还可以包括分类器704和第一滤除器705，分类器704被配置用于在对所述网络情报进行识别之前：利用预先配置的机器学习分类模型，将所述网络情报分类成网络安全威胁情报或非网络安全威胁情报，然后由第一滤除器705滤除所述网络情报中的非网络安全威胁情报。关于分类器的进一步说明可以参见上面步骤102的描述。

[0080] 可选地，网络安全威胁指标识别设备还可以包括判断器706和第二滤除器707，判断器706被配置用于在所述分类和所述滤除之后：利用预先配置的机器学习判断模型，判断分类为所述网络安全威胁情报的网络情报是否为有效的网络安全威胁情报；并且滤除所述网络情报中的非有效的网络安全威胁情报。关于判断器706的进一步说明可以参见上面步骤104的描述。

[0081] 图8图示了根据本发明实施例的硬件实施环境示意图。参见图8，在本发明的实施方式中，网络安全威胁指标识别装置800包括处理器804，其中包括硬件原件810。处理器804例如包括一个或多个数字信号处理器(DSP)、通用微处理器、专用集成电路(ASIC)、现场可编程逻辑阵列(FPGA)或其它等效集成或离散逻辑电路等一个或多个处理器。如本文中所使用的术语“处理器”可指上述结构或适合于实施本文中所描述的技术的任一其它结构中的任一者。另外，在一些方面中，本文描述的功能性可提供于经配置以用于网络安全威胁指标识别的专用硬件和/或软件模块内，或并入在组合式的硬件和/或软件模块中。并且，可将所述技术完全实施于一个或多个电路或逻辑元件中。本公开中的方法可以在各种组件、模块或单元中实现，但不一定需要通过不同硬件单元来实现。而是，如上所述，各种组件、模块或单元可组合或由互操作硬件单元(包含如上所述的一个或多个处理器)的集合结合合适软件和/或固件来提供。

[0082] 在一个或多个示例中，以上结合图1-图7所描述的技术方案可以硬件、软件、固件

或其任一组合来实施。如果以软件实施，那么功能可作为一个或多个指令或代码存储在计算机可读介质上或经由计算机可读介质806传输，且由基于硬件的处理器执行。计算机可读介质806可包含对应于例如数据存储介质等有形介质的计算机可读存储介质，或包含促进计算机程序例如根据通信协议从一处传送到另一处的任何介质的通信介质。以此方式，计算机可读介质806通常可对应于(1)非暂时性的有形计算机可读存储介质，或(2)例如信号或载波等通信介质。数据存储介质可为可由一个或多个计算机或者一个或多个处理器读取以检索用于实施本公开中描述的技术的指令、代码和/或数据结构的任何可用介质。计算机程序产品可包含计算机可读介质806。

[0083] 举例来说且并非限制，此类计算机可读存储介质可包括RAM、ROM、EEPROM、CD_ROM或其它光盘等存储器、磁盘存储器或其它磁性存储器、快闪存储器或可用来以指令或数据结构的形式存储所要程序代码且可由计算机读取的任何其它存储器812。而且，恰当地将任何连接称作计算机可读介质806。举例来说，如果使用同轴电缆、光纤电缆、双绞线、数字订户线(DSL)或例如红外线、无线电及微波等无线技术从网站、服务器或其它远程源传输指令，则同轴电缆、光纤电缆、双绞线、DSL或例如红外线、无线电及微波等无线技术包含于介质的定义中。然而应了解，计算机可读存储介质和数据存储介质不包含连接、载波、信号或其它瞬时介质，而是针对非瞬时有形存储介质。如本文中所使用，磁盘及光盘包含压缩光盘(CD)、激光光盘、光学光盘、数字多功能光盘(DVD)、软磁盘及蓝光光盘，其中磁盘通常以磁性方式再生数据，而光盘使用激光以光学方式再生数据。上文的组合也应包含在计算机可读介质806的范围内。

[0084] 网络安全威胁指标识别装置800还可以包括用于传输数据的I/O接口、以及其他功能814。网络安全威胁指标识别装置800可以包括在不同的装置中，例如移动电话、智能电话、平板、膝上型电脑、台式机、游戏控制台、车载设备、诸如电视、播放器之类的家用电器任何能够联网或以其它方式接收信息的装置，这里图示了计算机816、移动装置818和其它装置820。这些配置中的每个包括可以具有一般不同的构造和能力的设备，并且因此可以根据不同设备类别中的一个或多个配置网络安全威胁指标识别装置800。此外本发明的技术还可以通过使用分布式系统、诸如通过如下所述的平台824在“云”822上全部或部分地实现。

[0085] 云822包括和/或代表用于资源826的平台824。平台824抽象云822的硬件(例如，服务器)和软件资源的底层功能。资源826可以包括在远离计算设备802的服务器上执行计算机处理时可以使用的应用和/或数据。资源826还可以包括通过因特网和/或通过诸如蜂窝或Wi-Fi网络的订户网络提供的服务。

[0086] 平台824可以抽象资源和功能以将计算设备802与其他计算设备连接。平台824还可以用于抽象资源的分级以提供遇到的对于经由平台824实现的资源826的需求的相应水平的分级。因此，在互连设备实施例中，本文描述的功能的实现可以分布在整个系统内。例如，功能可以部分地在计算设备802上以及通过抽象云822的功能的平台824来实现。

[0087] 根据上述实施例，采用自动化的网络安全威胁标志的识别方式，避免了人工识别的耗时耗力。由于我们对需要识别的多个种类的网络安全威胁标志依据识别方式进行分组，通过与不同分组对应的基于机器学习模型的识别方式、基于词库的识别方式和基于规则的识别方式来识别，照此，能够利用不同种类的网络安全威胁指标的特点而有利地进行识别，避免了采用单个识别方式的局限性，例如，基于规则的识别方式对一些种类的网络安

全威胁指标(例如攻击组织)是无效的,无法有效识别,而代之以基于机器学习模型的识别方式则可以有效地识别,一定程度上解决了漏报和误报的问题。通过例如和WEB页面的交互,机器学习模型能够不断地收到前端反馈的结果,从而不断训练、优化该机器学习模型,机器学习模型的识别准确性从而不断提高,词库也能得到不断的更新,这也在一定程度上解决了漏报和误报的问题。另外,采用的机器学习模型能识别上下文的特征,从而能区分报告中出现的非恶意网络安全威胁指标,这又在一定程度上解决了漏报和误报的问题。

[0088] 需要说明,本公开中出现的“第一”、“第二”等表述不代表指示重要性或步骤的先后,仅是用于区分。方法步骤在没有特别说明或者没有前提约束(即一个步骤的执行需以另一个步骤的执行结果为前提)的情况下,方法步骤的描述先后不代表他们的执行先后,所描述的方法步骤可以以可能的、合理的顺序执行。

[0089] 本领域技术人员在考虑说明书及实践这里公开的发明后,将容易想到本申请的其它实施方案。本申请旨在涵盖本申请的任何变型、用途或者适应性变化,这些变型、用途或者适应性变化遵循本申请的一般性原理并包括本申请未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的,本申请的真正范围和精神由权利要求指出。

[0090] 应当理解的是,本申请并不局限于上面已经描述并在附图中示出的精确结构,并且可以在不脱离其范围进行各种修改和改变。本申请的范围仅由所附的权利要求来限制。

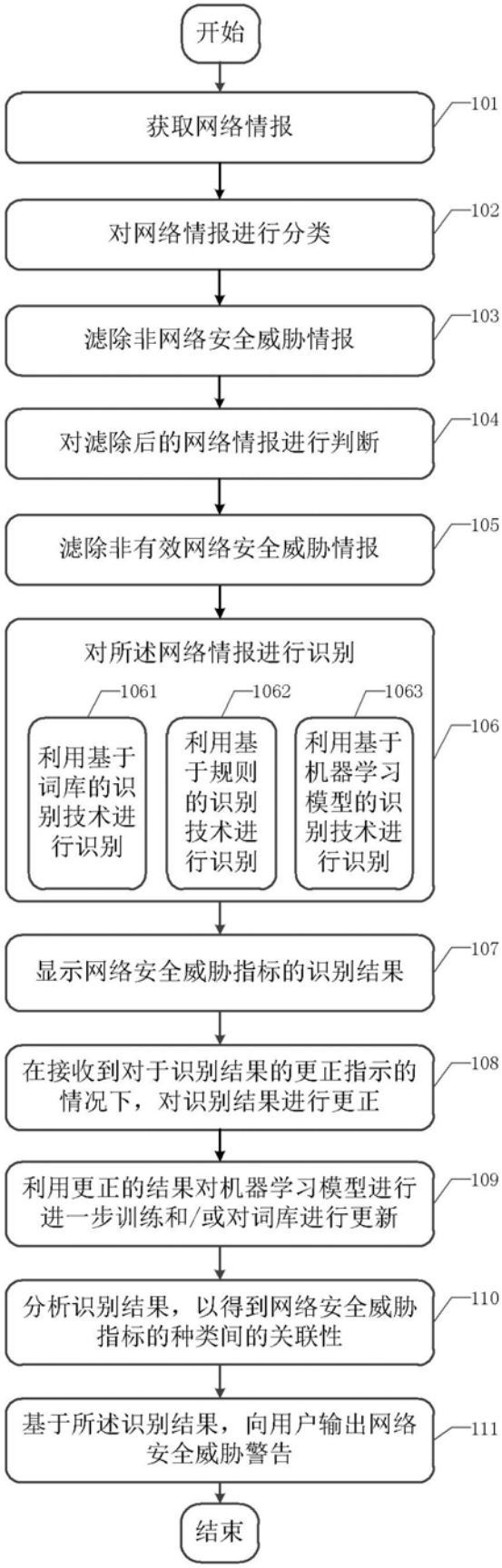

开始
获取网络情报
101
对网络情报进行分类
102
滤除非网络安全威胁情报
103
对滤除后的网络情报进行判断
104
滤除非有效网络安全威胁情报
105
对所述网络情报进行识别
1061
1062
1063
利用基于词库的识别技术进行识别
利用基于规则的识别技术进行识别
利用基于机器学习模型的识别技术进行识别
106
显示网络安全威胁指标的识别结果
107
在接收到对于识别结果的更正指示的情况下，对识别结果进行更正
108
利用更正的结果对机器学习模型进行进一步训练和/或对词库进行更新
109
分析识别结果，以得到网络安全威胁指标的种类间的关联性
110
基于所述识别结果，向用户输出网络安全威胁警告
111
结束

图 1

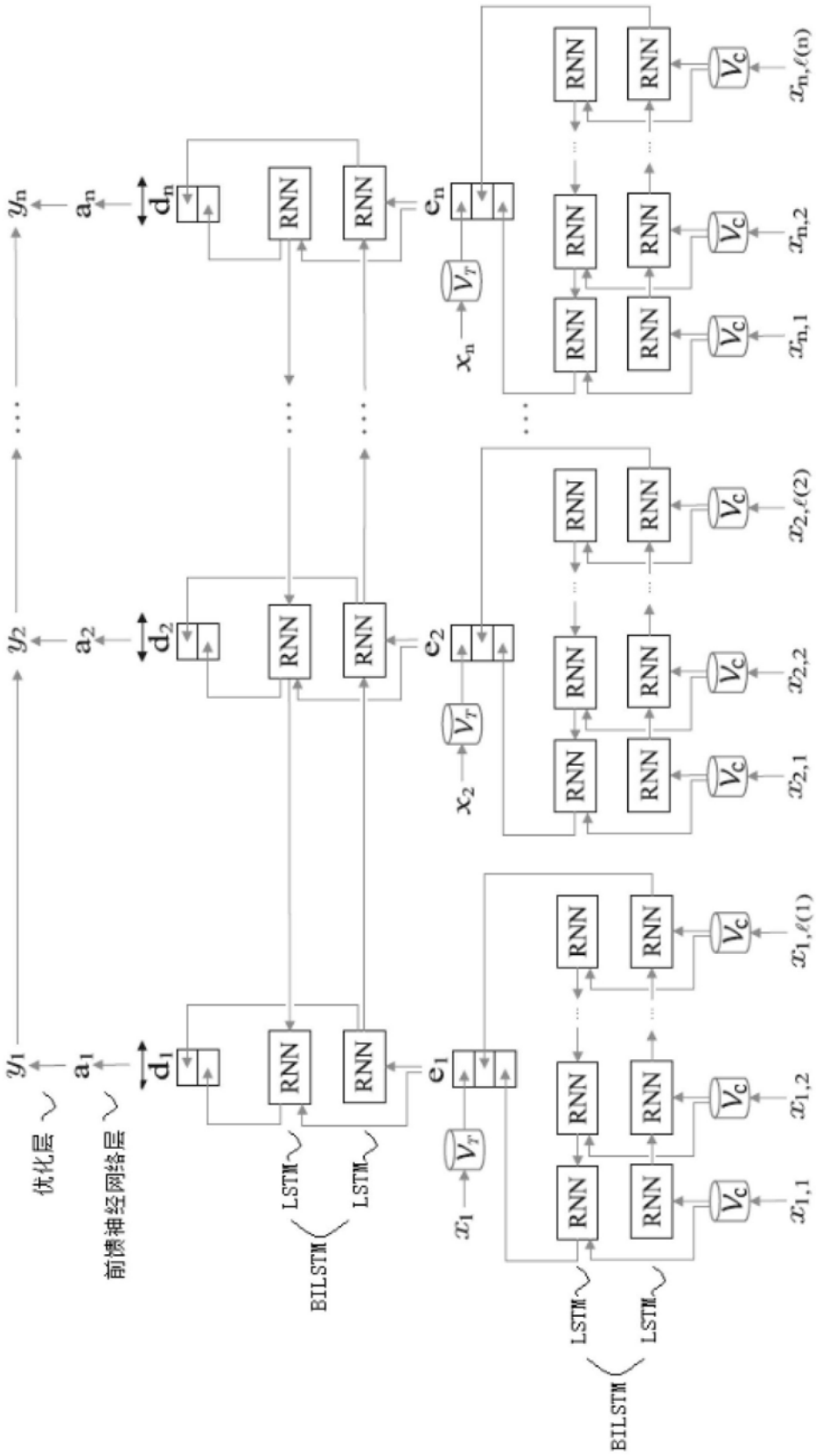


图 2

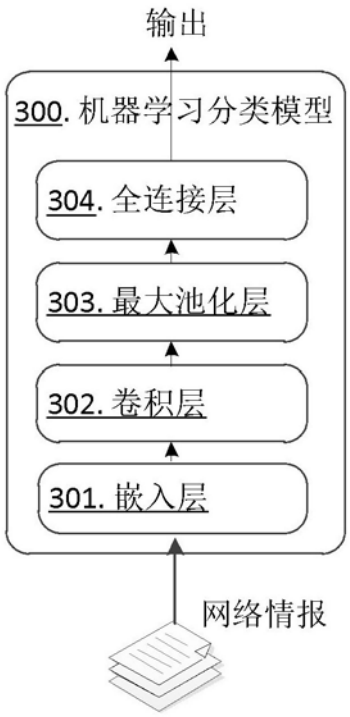

输出
300. 机器学习分类模型
304. 全连接层
303. 最大池化层
302. 卷积层
301. 嵌入层
网络情报

图 3

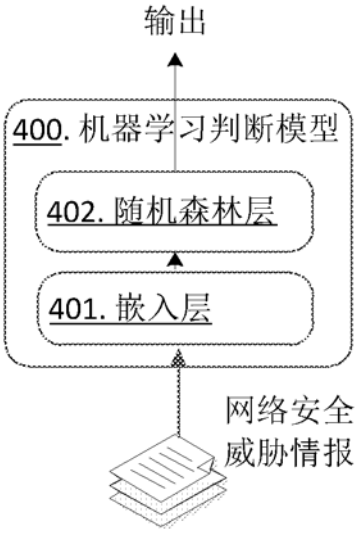

输出
400. 机器学习判断模型
402. 随机森林层
401. 嵌入层
网络安全
威胁情报

图 4

```
194.70.136 valid_text_00054 29 39 NNP NNP O B-IP
Domains valid_text_00054 40 47 NNP NNP O O
000webhostapp.com valid_text_00054 48 65 NNP NNP B-DOMAIN B-DOMAIN
000webhostapp.com valid_text_00054 66 83 NNP NNP B-DOMAIN B-DOMAIN
000webhostapp.com valid_text_00054 84 101 NNP NNP B-DOMAIN B-DOMAIN
nid-help-pchange.atwebpages.com valid_text_00054 102 133 NNP NNP B-DOMAIN B-DOMAIN
inkboom.co.kr valid_text_00054 134 147 NNP NNP B-DOMAIN B-DOMAIN
byethost7.com valid_text_00054 148 161 NNP NNP B-DOMAIN B-DOMAIN
Hashes valid_text_00054 162 168 NNP NNP O O
fef671c13039df24e1606d5fdc65c92fbc1578d9 valid_text_00054 169 209 NNP NNP B-FILEHASH B-FILEHASH
06948ab527ae415f32ed4b0f0d70be4a86b364a5 valid_text_00054 210 250 NNP NNP B-FILEHASH B-FILEHASH
96a2fda8f26018724c86b275fe9396e24b26ec9e valid_text_00054 251 291 NNP NNP B-FILEHASH B-FILEHASH
ad08a60dc511d9b69e584c1310dbd6039aca0d valid_text_00054 292 330 NNP NNP B-FILEHASH B-FILEHASH
c2f01355880cd9dfeef75c189f4a8af421e0d3 valid_text_00054 331 369 NNP NNP B-FILEHASH B-FILEHASH
615447f458463dc77f7ae3b0a4ad20ca2303027a valid_text_00054 370 410 NNP NNP B-FILEHASH B-FILEHASH
bf21667e4b48b8857020ba455531c9c4f2560740 valid_text_00054 411 451 NNP NNP B-FILEHASH B-FILEHASH
bc6cb78e20cb20285149d55563f6fdcf4aaafa58 valid_text_00054 452 492 NNP NNP B-FILEHASH B-FILEHASH
465d48ae849bbd6505263f3323e818ccb501ba88 valid_text_00054 493 533 NNP NNP B-FILEHASH B-FILEHASH
a9eb9a1734bb84bbc60df38d4a1e02a870962857 valid_text_00054 534 574 NNP NNP B-FILEHASH B-FILEHASH
539acd9145befd7e670fe826c2487766f46f0d041 valid_text_00054 575 615 NNP NNP B-FILEHASH B-FILEHASH
d63c7d7305a8b2184f3b0941e596f09287aa66 valid_text_00054 616 654 NNP NNP B-FILEHASH B-FILEHASH
35e5310b6183469f4995b7cd4f795da8459087a4 valid_text_00054 655 695 NNP NNP B-FILEHASH B-FILEHASH
11a38a9d23193d9582d02ab0eae767c39330666ec valid_text_00054 696 736 NNP NNP B-FILEHASH B-FILEHASH
e68f43ecb033300420047b61933583b4144585 valid_text_00054 737 775 NNP NNP B-FILEHASH B-FILEHASH
83706ddaa5ea5ee2cf54b7c809458a391163a7a valid_text_00054 776 814 NNP NNP B-FILEHASH B-FILEHASH
3a0c617d17e7f819775e48f7edefe9af84a1446b valid_text_00054 815 855 NNP NNP B-FILEHASH B-FILEHASH
761b0690cd86fb472738b6dc32661ace5cf18893 valid text 00054 856 896 NNP NNP B-FILEHASH B-FILEHASH
```

图 5

.	GUID	来源	标题	状态	操作人	插入时间	修改时间
□	bb3238ae-20e8-11e9-9e13-6c0b84d74344	Out_Latest articles about Ongoing threats	https://blog.talosintelligence.com/2019/01/threat-roundup-0118-0125.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+feedburner%2FTalos+%28Talos%E2%84%A2+Blog%29	已标注		2019-01-26 05:30:46	2019-04-25 15:49:11
□	e4e00170-8955-11e8-8a10-e04f43ca90f9	Out_Didier Stevens	!exploitable Crash Analyzer – Statically Linked CRT	已标注		2018-07-17 00:00:11	2018-07-19 15:44:38
□	2c3d9da0-4474-11e9-89ae-6c0b84d74344	Out_4hou	#OpJerusalem 2019——一场“开年不顺”的勒索软件攻击行动	已标注		2019-03-12 03:00:43	2019-03-13 09:44:16
□	62a20d12-70c6-11e9-b130-28c13c8f7df7	Out_WX_腾讯御见威胁情报中心	"海莲花"APT 组织 2019 年第一季度针对中国的攻击活动技术揭秘	已标注		2019-05-07 20:48:17	2019-05-08 16:12:18

图 6a

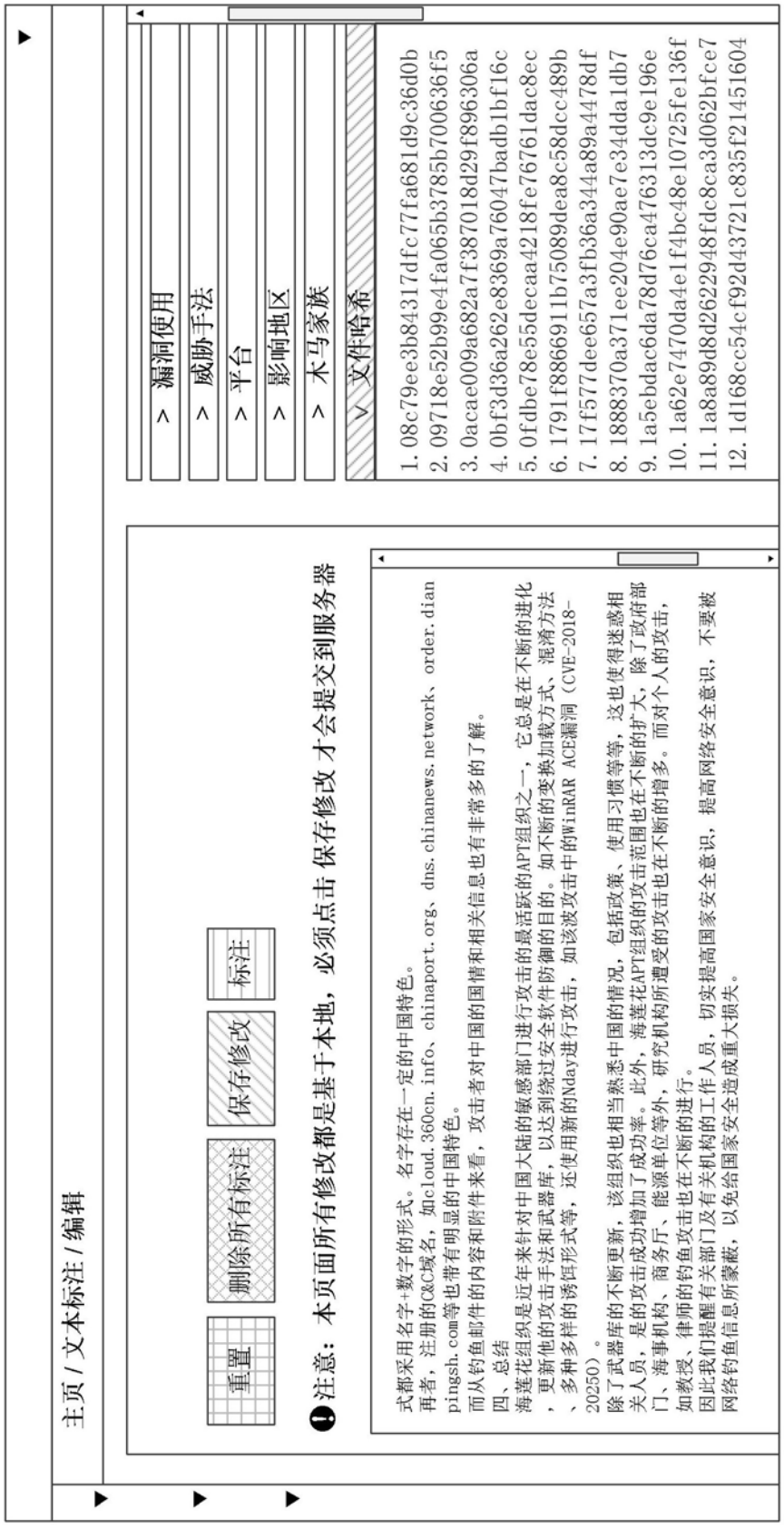

主页 / 文本标注 / 编辑
重置
删除所有标注
保存修改
标注
注意：本页面所有修改都是基于本地，必须点击 保存修改 才会提交到服务器
式都采用名字+数字的形式。名字存在一定的中国特色。
再者，注册的C&C域名，如cloud.360cn.info、chinaport.org、dns.chinanews.network、order.dian
pingsh.com等也带有明显的中国特色。
而从钓鱼邮件的内容和附件来看，攻击者对中国的国情和相关信息也有非常多的了解。
四、总结
海莲花组织是近年来针对中国大陆的敏感部门进行攻击的最活跃的APT组织之一，它总是在不断的进化
，更新他的攻击手法和武器库，以达到绕过安全软件防御的目的。如不断的变换加载方式、混淆方法
、多种多样的诱饵形式等，还使用新的Nday进行攻击，如该波攻击中的WinRAR ACE漏洞（CVE-2018-
20250）。
除了武器库的不断更新，该组织也相当熟悉中国的情况，包括政策、使用习惯等等，这也使得迷惑相
关人员，是的攻击成功增加了成功率。此外，海莲花APT组织的攻击范围也在不断的扩大，除了政府部
门、海事机构、商务厅、能源单位等外，研究机构所遭受的攻击也在不断的增多。而对个人的攻击，
如教授、律师的钓鱼攻击也在不断的进行。
因此我们提醒有关部门及有关机构的工作人员，切实提高国家安全意识，提高网络安全意识，不要被
网络钓鱼信息所蒙蔽，以免给国家安全造成重大损失。
> 漏洞使用
> 威胁手法
> 平台
> 影响地区
> 木马家族
V 文件哈希
1. 08c79ee3b84317dfc77fa681d9c36d0b
2. 09718e52b99e4fa065b3785b700636f5
3. 0acae009a682a7f387018d29f896306a
4. 0bf3d36a262e8369a76047badb1bf16c
5. 0fdbe78e55decaa4218fe76761dac8ec
6. 1791f8866911b75089dea8c58dcc489b
7. 17f577dee657a3fb36a344a89a4478df
8. 1888370a371ee204e90ae7e34dda1db7
9. 1a5ebdac6da78d76ca476313dc9e196e
10. 1a62e7470da4e1f4bc48e10725fe136f
11. 1a8a89d8d2622948fdc8ca3d062bfce7
12. 1d168cc54cf92d43721c835f21451604

图 6b

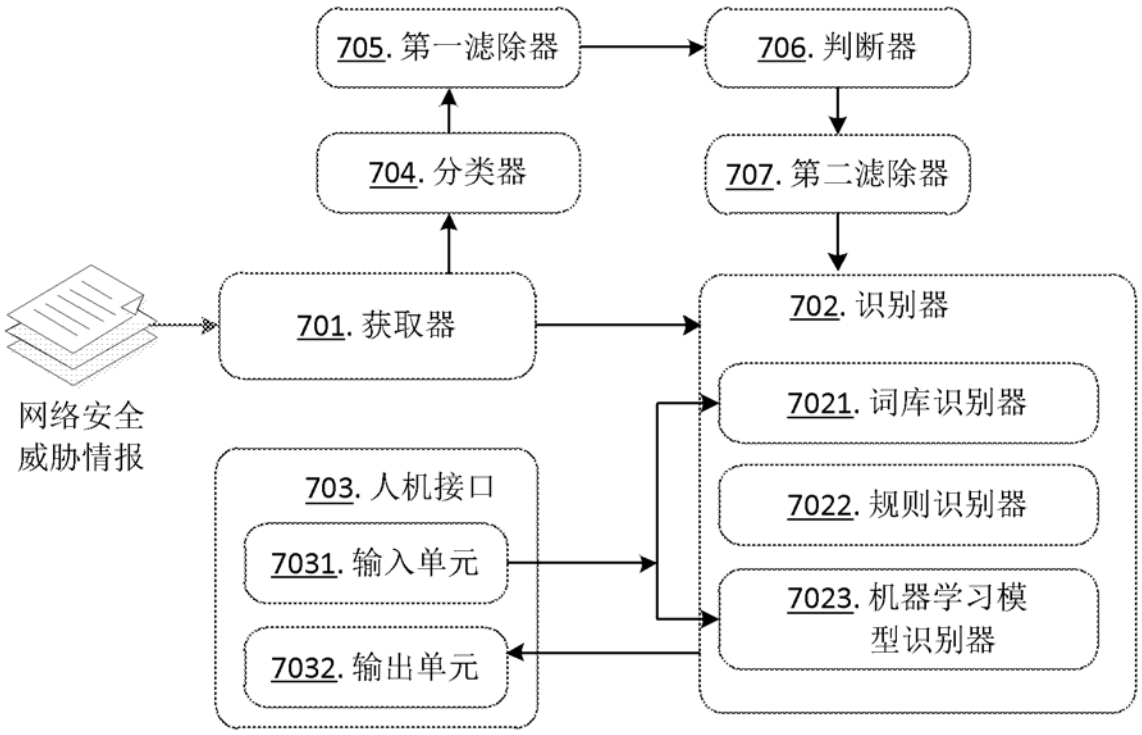

705. 第一滤除器
706. 判断器
704. 分类器
707. 第二滤除器
701. 获取器
702. 识别器
网络安全
威胁情报
7021. 词库识别器
703. 人机接口
7022. 规则识别器
7031. 输入单元
7023. 机器学习模
型识别器
7032. 输出单元

图 7

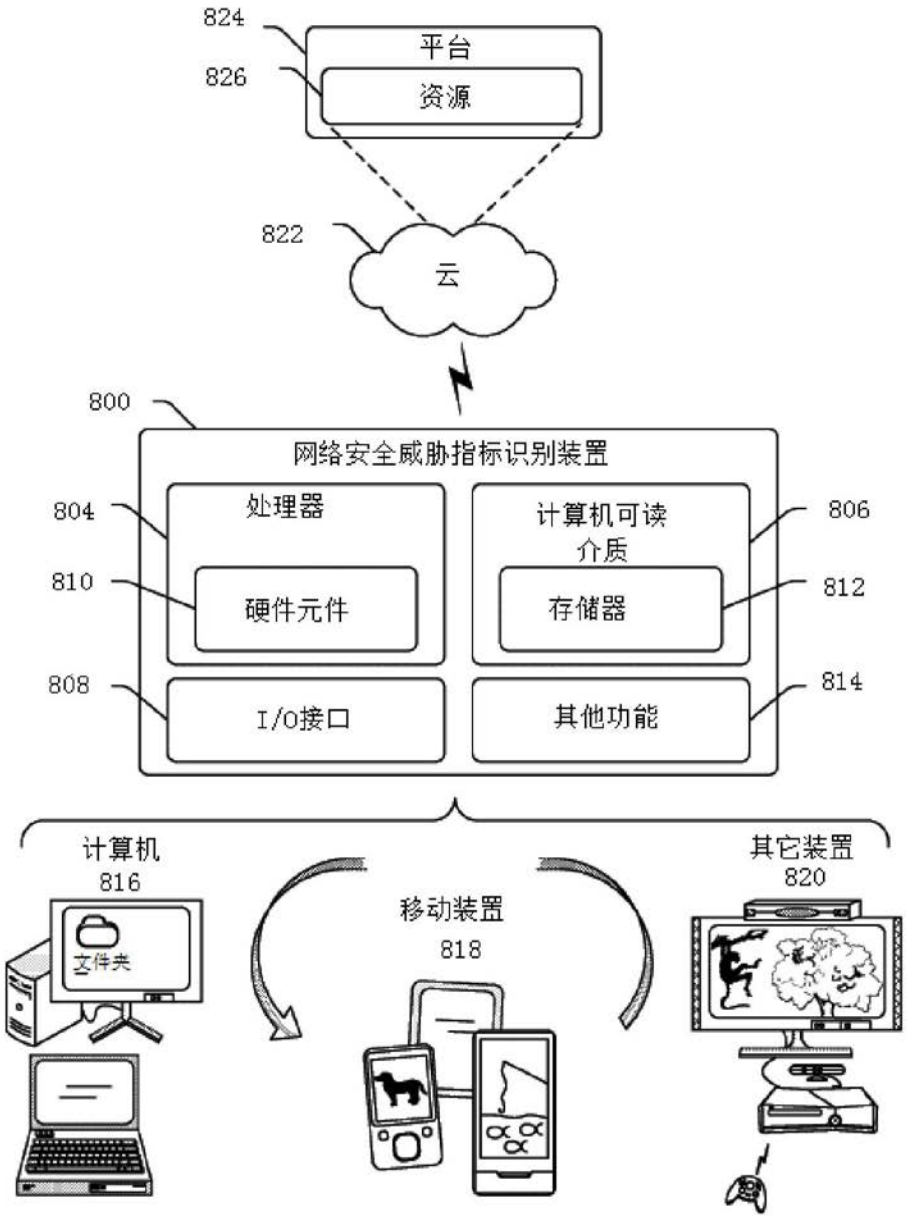

824
平台
826
资源
822
云
800
网络安全威胁指标识别装置
804
处理器
806
计算机可读介质
810
硬件元件
812
存储器
808
I/O接口
814
其他功能
计算机
816
文件夹
移动装置
818
其它装置
820

图 8