(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111641663 B
(45)授权公告日 2022.08.12

(21)申请号 202010643291.1

(22)申请日 2020.07.06

(65)同一申请的已公布的文献号
申请公布号 CN 111641663 A

(43)申请公布日 2020.09.08

(73)专利权人 奇安信科技集团股份有限公司
地址 100088 北京市西城区新街口外大街28号102号楼3层332号
专利权人 奇安信网神信息技术(北京)股份有限公司

(72)发明人 白敏 万文杰 黄朝文

(74)专利代理机构 中科专利商标代理有限责任公司 11021
专利代理师 周天宇

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 61/4511(2022.01)

(56)对比文件
CN 102724187 A,2012.10.10
CN 102724187 A,2012.10.10
CN 109784049 A,2019.05.21
CN 108092962 A,2018.05.29
CN 104092792 A,2014.10.08
CN 109391602 A,2019.02.26
CN 102682097 A,2012.09.19
CN 106911717 A,2017.06.30
KR 20120087393 A,2012.08.07
US 2010037314 A1,2010.02.11

审查员 魏慧慧

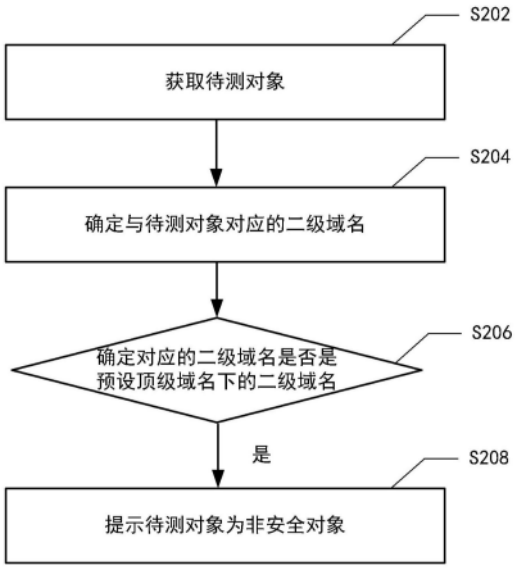
权利要求书2页 说明书10页 附图6页

(54)发明名称

一种安全检测方法和装置

(57)摘要

本公开提供了一种安全检测方法，该方法包括：获取待测对象，其中，待测对象包括以下类型中的一种：域名类、IP类、URL类；确定与待测对象对应的二级域名；确定对应的二级域名是否是预设顶级域名下的二级域名；以及响应于确定对应的二级域名是预设顶级域名下的二级域名，提示待测对象为非安全对象。本公开还提供了一种安全检测装置、一种电子设备以及一种计算机可读存储介质。



CN 111641663 B

1.一种安全检测方法,包括:

获取待测对象,其中,所述待测对象包括以下类型中的一种:域名类、IP类、URL类;

确定与所述待测对象对应的二级域名;

确定所述对应的二级域名是否是预设顶级域名下的二级域名;预设顶级域名下的二级域名为存储在二级域名黑名单中的二级域名,以及

响应于确定所述对应的二级域名是所述预设顶级域名下的二级域名,提示所述待测对象为非安全对象,基于用户请求返回所述非安全对象的基础类关联信息,其中,所述基础类关联信息包括Meta类、Security类、Family类和Campaign类中的一种;

其中,所述Meta类信息仅包含元数据类型信息;Security类包括风险等级、影响平台、恶意家族、威胁类型的信息,Family类信息包括数据详情信息,Campaign类信息包括家族类详情信息。

2.根据权利要求1所述的方法,还包括:

响应于确定所述对应的二级域名不是所述预设顶级域名下的二级域名,确定与所述待测对象对应的原始域名,其中,原始域名的域名类型包括命令和控制类、IP类、DGA类,不同的域名类型对应于不同的检测逻辑;

确定所述对应的原始域名的域名类型;

确定与所述对应的原始域名的域名类型对应的检测逻辑;

对所述待测对象执行所述对应的检测逻辑;以及

基于检测逻辑执行结果,提示所述待测对象是否是安全对象。

3.根据权利要求2所述的方法,其中,所述确定所述对应的原始域名的域名类型,包括:

先确定所述对应的原始域名是否属于命令和控制类;

在确定所述对应的原始域名不属于命令和控制类的情况下,再确定所述对应的原始域名是否属于IP类;

在确定所述对应的原始域名不属于IP类的情况下,再确定所述对应的原始域名的域名类型是否属于DGA类。

4.根据权利要求2或3所述的方法,其中:

如果确定所述对应的原始域名属于DGA类,则确定所述对应的原始域名是否是所述预设顶级域名下的原始域名;

响应于确定所述对应的原始域名是所述预设顶级域名下的原始域名,提示所述待测对象是非安全对象。

5.根据权利要求2或3所述的方法,其中:

与命令和控制类对应的检测逻辑包括以下操作中的至少之一:

顶级域名匹配操作;

IP匹配操作;

URL匹配操作;

端口匹配操作。

6.根据权利要求1所述的方法,还包括:

如果确定所述待测对象为非安全对象,反馈针对所述待测对象的处理策略。

7.一种安全检测装置,包括:

获取模块，用于获取待测对象，其中，所述待测对象包括以下类型中的一种：域名类、IP类、URL类；

第一确定模块，用于确定与所述待测对象对应的二级域名；

第二确定模块，用于确定所述对应的二级域名是否是预设顶级域名下的二级域名，预设顶级域名下的二级域名为存储在二级域名黑名单中的二级域名；以及

提示模块，用于响应于确定所述对应的二级域名是所述预设顶级域名下的二级域名，提示所述待测对象为非安全对象，基于用户请求返回所述非安全对象的基础类关联信息，其中，所述基础类关联信息包括Meta类、Security类、Family类和Campaign类中的一种；

其中，所述Meta类信息仅包含元数据类型信息；Security类包括风险等级、影响平台、恶意家族、威胁类型的信息，Family类信息包括数据详情信息，Campaign类信息包括家族类详情信息。

8.一种电子设备，包括：

一个或多个处理器；

存储器，用于存储一个或多个程序，

其中，当所述一个或多个程序被所述一个或多个处理器执行时，使得所述一个或多个处理器实现权利要求1至6中任一项所述的方法。

9.一种计算机可读存储介质，存储有计算机可执行指令，所述指令在被执行时用于实现权利要求1至6中任一项所述的方法。

一种安全检测方法和装置

技术领域

[0001] 本公开涉及网络安全技术领域,特别是涉及一种安全检测方法和装置。

背景技术

[0002] 传统的防御机制往往是根据以往的“经验”来构建安全防御策略,即使是基于机器学习的检测算法也是如此,都难以应付未知攻击。在网络攻击呈现多样化、复杂化、专业化的趋势下,需要一种能够根据过去和当前网络安全状态动态调整防御策略的手段,威胁情报应运而生。

[0003] 在实现本公开实施例的过程中,发明人发现:传统的威胁情报使用,在误报率及检测率方面没有控制的很好,往往造成使用方的错误使用以及不规范使用,这对威胁情报检测结果的准确性造成了较大影响。

发明内容

[0004] 本公开的一个方面提供了一种安全检测方法,包括:获取待测对象,其中,所述待测对象包括以下类型中的一种:域名类、IP类、URL类;确定与所述待测对象对应的二级域名;确定所述对应的二级域名是否是预设顶级域名下的二级域名;以及响应于确定所述对应的二级域名是所述预设顶级域名下的二级域名,提示所述待测对象为非安全对象。

[0005] 可选地,还包括:响应于确定所述对应的二级域名不是所述预设顶级域名下的二级域名,确定与所述待测对象对应的原始域名,其中,原始域名的域名类型包括命令和控制类、IP类、DGA类,不同的域名类型对应于不同的检测逻辑;确定所述对应的原始域名的域名类型;确定与所述对应的原始域名的域名类型对应的检测逻辑;对所述待测对象执行所述对应的检测逻辑;以及基于检测逻辑执行结果,提示所述待测对象是否是安全对象。

[0006] 可选地,所述确定所述对应的原始域名的域名类型,包括:先确定所述对应的原始域名是否属于命令和控制类;在确定所述对应的原始域名不属于命令和控制类的情况下,再确定所述对应的原始域名是否属于IP类;在确定所述对应的原始域名不属于IP类的情况下,再确定所述对应的原始域名的域名类型是否属于DGA类。

[0007] 可选地,如果确定所述对应的原始域名属于DGA类,则确定所述对应的原始域名是否是所述预设顶级域名下的原始域名;响应于确定所述对应的原始域名是所述预设顶级域名下的原始域名,提示所述待测对象是非安全对象。

[0008] 可选地,与命令和控制类对应的检测逻辑包括以下操作中的至少之一:顶级域名匹配操作;IP匹配操作;URL匹配操作;端口匹配操作。

[0009] 可选地,还包括:如果确定所述待测对象为非安全对象,反馈针对所述待测对象的处理策略。

[0010] 可选地,还包括:如果确定所述待测对象为非安全对象,基于用户需求反馈所述待测对象的关联信息。

[0011] 本公开的另一个方面提供了一种安全检测装置,包括:获取模块,用于获取待测对

象，其中，所述待测对象包括以下类型中的一种：域名类、IP类、URL类；第一确定模块，用于确定与所述待测对象对应的二级域名；第二确定模块，用于确定所述对应的二级域名是否是预设顶级域名下的二级域名；以及提示模块，用于响应于确定所述对应的二级域名是所述预设顶级域名下的二级域名，提示所述待测对象为非安全对象。

[0012] 本公开的另一方面提供了一种电子设备，包括：一个或多个处理器；存储器，用于存储一个或多个程序，其中，当上述一个或多个程序被上述一个或多个处理器执行时，使得上述一个或多个处理器实现本公开实施例的方法。

[0013] 本公开的另一方面提供了一种计算机可读存储介质，存储有计算机可执行指令，上述指令在被执行时用于实现本公开实施例的方法。

[0014] 本公开的另一方面提供了一种计算机程序产品，包括计算机可读指令，其中，上述计算机可读指令被执行时用于实现本公开实施例的方法。

附图说明

[0015] 为了更完整地理解本公开及其优势，现在将参考结合附图的以下描述，其中：

[0016] 图1A示意性示出了根据本公开实施例的适于安全检测方法和装置的系统架构；

[0017] 图1B示意性示出了根据本公开实施例的适于安全检测方法和装置的应用场景；

[0018] 图2示意性示出了根据本公开实施例的安全检测方法的流程图；

[0019] 图3示意性示出了根据本公开实施例的针对恶意对象的处理策略的示意图；

[0020] 图4示意性示出了根据本公开实施例的针对恶意对象反馈关联信息的示意图；

[0021] 图5示意性示出了根据本公开实施例的基于不同类型的原始域名选用不同的检测逻辑的原理图；

[0022] 图6示意性示出了根据本公开实施例的判断原始域名的域名类型的方法逻辑图；

[0023] 图7示意性示出了根据本公开实施例的针对DGA类原始域名的检测逻辑的流程图；

[0024] 图8示意性示出了根据本公开实施例的安全检测装置的框图；以及

[0025] 图9示意性示出了根据本公开实施例的电子设备的框图。

具体实施方式

[0026] 以下，将参照附图来描述本公开的实施例。但是应该理解，这些描述只是示例性的，而并非要限制本公开的范围。在下面的详细描述中，为便于解释，阐述了许多具体的细节以提供对本公开实施例的全面理解。然而，明显地，一个或多个实施例在没有这些具体细节的情况下也可以被实施。此外，在以下说明中，省略了对公知结构和技术的描述，以避免不必要地混淆本公开的概念。

[0027] 在此使用的术语仅仅是为了描述具体实施例，而并非意在限制本公开。在此使用的术语“包括”、“包含”等表明了所述特征、步骤、操作和/或部件的存在，但是并不排除存在或添加一个或多个其他特征、步骤、操作或部件。

[0028] 在此使用的所有术语(包括技术和科学术语)具有本领域技术人员通常所理解的含义，除非另外定义。应注意，这里使用的术语应解释为具有与本说明书的上下文相一致的含义，而不应以理想化或过于刻板的方式来解释。

[0029] 在使用类似于“A、B和C等中至少一个”这样的表述的情况下，一般来说应该按照本

领域技术人员通常理解该表述的含义来予以解释(例如,“具有A、B和C中至少一个的系统”应包括但不限于单独具有A、单独具有B、单独具有C、具有A和B、具有A和C、具有B和C、和/或具有A、B、C的系统等)。

[0030] 附图中示出了一些方框图和/或流程图。应理解,方框图和/或流程图中的一些方框或其组合可以由计算机程序指令来实现。这些计算机程序指令可以提供给通用计算机、专用计算机或其他可编程数据处理装置的处理器,从而这些指令在由该处理器执行时可以创建用于实现这些方框图和/或流程图中所说明的功能/操作的装置。本公开的技术可以硬件和/或软件(包括固件、微代码等)的形式来实现。另外,本公开的技术可以采取存储有指令的计算机可读存储介质上的计算机程序产品的形式,该计算机程序产品可供指令执行系统使用或者结合指令执行系统使用。

[0031] 本公开的实施例提供了一种能够针对不同检测对象自动适用不同检测逻辑的安全检测方法以及能够应用该方法的安全检测装置。该方法包括获取待测对象,其中,该待测对象包括以下类型中的一种:域名类、IP类、URL类;确定与该待测对象对应的二级域名;确定该对应的二级域名是否是预设顶级域名下的二级域名;以及响应于确定该对应的二级域名是该预设顶级域名下的二级域名,提示该待测对象为非安全对象。

[0032] 以下将结合附图和具体实施例详细阐述本公开。

[0033] 图1A示意性示出了根据本公开实施例的适于安全检测方法和装置的系统架构。需要注意的是,图1A所示仅为可以应用本公开实施例的系统架构的示例,以帮助本领域技术人员理解本公开的技术内容,但并不意味着本公开实施例不可以用于其他设备、系统、环境或场景。

[0034] 如图1A所示,该系统架构100包括:内网主机101(或者内网主机集群)和威胁情报检测引擎102。威胁情报检测引擎102主要用于检测内网主机101(或者内网主机集群)是否失陷。威胁情报检测引擎102可以与NGFW、UTM、终端防病毒、虚拟化终端、云安全、NGSOC、态势感知等多种网络设备、主机应用和大数据平台环境结合,进行基于威胁情报的失陷主机检测。使用威胁情报检测引擎102的用户不需要有任何威胁情报、安全对抗知识、只需要通过简单的接口调用,就可以使产品或设备具有高精准、可定性、可拦截的威胁情报检测能力。即只要将出站流量日志作为检测对象给威胁情报检测引擎102进行检测,就可以得到内网主机是否失陷,失陷类型是什么的结论。

[0035] 应该理解,图1A中的内网主机和威胁情报检测引擎的数目仅仅是示意性的。根据实现需要,可以具有任意数目的内网主机和威胁情报检测引擎。

[0036] 图1B示意性示出了根据本公开实施例的适于安全检测方法和装置的应用场景。同样,需要注意的是,图1B所示仅为可以应用本公开实施例的应用场景的示例,以帮助本领域技术人员理解本公开的技术内容,但并不意味着本公开实施例不可以用于其他场景。

[0037] 由于攻击者(如黑客组织)通常使用域名、IP和URL等类型的请求攻击内网主机等网络设备。因此,如图1B所示,在该应用场景中,进行失陷分析时,可以先判断请求类型是否是域名、IP和URL等类型,再基于不同请求类型调用不同的检测逻辑进行检测。

[0038] 图2示意性示出了根据本公开实施例的安全检测方法的流程图。

[0039] 如图2所示,该方法例如可以包括操作S202、S204、S206和S208。

[0040] 在操作S202,获取待测对象。其中,待测对象例如可以包括以下类型中的一种:域

名类、IP类、URL类。

[0041] 具体地，在操作S202，可以通过日志查询，获取目标出站流量日志，进而基于获取的目标出站流量日志，提取请求中的相关信息以作为本公开实施例中的待测对象，并判断与该待测对象对应的请求类型。例如是域名类请求，还是IP类请求，还是URL类请求。

[0042] 示例性的，如果待测对象为abc.com，则表征该待测对象为域名类请求。或者，如果待测对象为10.0.0.0或者172.16.0.0或者192.168.0.0等等，则表征该待测对象为IP类请求。或者，如果待测对象为使用“//＜用户名＞:＜密码＞@＜主机＞:＜端口＞/＜url路径＞”等类似语法定义的请求，则表征该待测对象为URL类请求。

[0043] 接下来，在操作S204，确定与待测对象对应的二级域名。

[0044] 具体地，针对不同请求类型的待测对象，可以使用不同的方法来确定与之对应的二级域名。

[0045] 在一个实施例中，针对域名类待测对象，可以直接从域名中读取对应的二级域名。应该理解，域名由两组或两组以上的ASCLL或各国语言字符构成，各组字符件由点号分隔开，最右边的字符组称为顶级域名或一级域名、倒数第二组称为二级域名、倒数第三组称为三级域名、以此类推。示例性的，如果待测对象为xy.abc.com，则此时二级域名为“abc.com”。

[0046] 或者，在另一个实施例中，针对URL类待测对象，可以直接将URL化分为不同的字段，并将提取host字段，进而基于host字段确定待测对象的二级域名。示例性的，如果待测对象为ftp://@host.com/，则提取的host字段为“host.com”，如果“host.com”表征的是“map.abc.com”，则此时二级域名为“abc.com”。

[0047] 再接下来，在操作S206，确定对应的二级域名是否是预设顶级域名下的二级域名。

[0048] 具体地，可以针对已知安全性和风险等级的顶级域名下的二级域名设置白名单和黑名单，例如将安全的顶级域名下的二级域名(安全情报)存储在二级域名白名单中，例如将具有攻击性的顶级域名下的二级域名(威胁情报)存储在二级域名黑名单中。其中，操作S206中提及的预设顶级域名下的二级域名为存储在二级域名黑名单中的二级域名。

[0049] 因此，在操作S206，可以将通过操作S204确定的二级域名与上述黑名单中的二级域名(顶级私有域名库)进行匹配。

[0050] 其中，在一个实施例中，如果在匹配过程中命中了上述黑名单中的二级域名，则认为上述待测对象是非安全对象(攻击对象、恶意对象)。

[0051] 即，由于顶级私有域名库中的域名为黑名单域名，因此顶级私有域名库中的域名下的所有类型的URL及域名也都可以归一化为一类黑名单域名。基于此，如果与待测对象对应的二级域名匹配到顶级私有域名库中的域名，则待测对象可以认为是恶意对象。

[0052] 示例性的，如果aaa.com是黑名单域名，则aaa.com域名下的map.aaa.com、bb.aaa.com等理论上都可以被认为是黑名单中的域名。

[0053] 或者，在另一个实施例中，如果在匹配过程中没有命中上述黑名单中的二级域名，则尚无法确定上述待测对象是否是安全对象。在这种情况下还可以进一步执行其他检测逻辑，以便做进一步判断。对于其他检测逻辑，本公开将在其他实施例中阐述，在此不再赘述。

[0054] 然后，在操作S208，响应于确定对应的二级域名是预设顶级域名下的二级域名，提示待测对象为非安全对象。

[0055] 如果确定待测对象为非安全对象(攻击对象、恶意对象),那么在本公开的一个实施例中,可以仅发送并展示提示信息,以便提示该待测对象为非安全对象。

[0056] 或者,在本公开的其他实施例中,在提示待测对象为非安全对象的同时,还可以发送并展示其他信息,例如针对该待测对象的Meta类、Security类、Family类和Campaign类等信息。

[0057] 其中,Meta类信息仅包含元数据类型信息。例如,meta类信息可以包括meta id,value1(host),value2(param),value3(port),IOC Category(Indicators of Compromise Category威胁指标类型),以及处理策略的相关建议。

[0058] 其中,Security类信息包括risk(风险等级),platform(影响平台),malicious_family(恶意家族),malicious_type(威胁类型,包括但不限于:攻击利用套件、远控木马、网络蠕虫、僵尸网络、勒索软件等)……等字段信息。

[0059] 其中,Family类信息主要涉及数据等详情信息部分,包括但不限于description(恶意家族详情),reference(家族参考链接),malicious_family(恶意家族),risk,platform,malicious_type等信息。

[0060] 其中,Campaign类信息主要涉及家族类详情信息部分,包括但不限于reference_document(参考文档),first_detection_date(首次检测到攻击事件的日期),reference_link(报告链接)等字段信息,分别适用于请求端对数据的不同字段需求。

[0061] 具体地,作为一种可选的实施例,该方法还可以包括:如果确定待测对象为非安全对象,基于用户请求反馈针对待测对象的处理策略。

[0062] 在本公开的一个实施例中,针对恶意对象的处理策略可以包括但不限于“告警、不告警”与“阻断、不阻断”的相互组合。示例性的,如图3所示,针对恶意对象的处理策略可以包括但不限于:仅告警不阻断、告警且阻断、不告警且不阻断、仅阻断不告警……。

[0063] 通过本公开实施例,可以帮助用户针对不同的恶意对象采取行之有效的处理手段,以便能够积极主动地对恶意攻击进行防御。

[0064] 此外,作为一种可选的实施例,该方法例如还可以包括:如果确定待测对象为非安全对象,基于用户请求反馈待测对象的关联信息。

[0065] 在本公开的一个实施例中,恶意对象的关联信息可以包括但不限于上述的Meta类、Security类、Family类和Campaign类等信息。示例性的,如图4所示,恶意对象的关联信息可以包括但不限于恶意对象所属的恶意家族(攻击团伙)、恶意对象所使用的攻击方法、以及攻击上下文等信息。

[0066] 通过本公开实施例,针对恶意对象除了可以提供提示信息之外,还可以额外提供丰富的关联日志信息,以满足不同用户的个性化需求。

[0067] 需要说明的是,在本公开实施例中,可以在威胁情报检测引擎中设置检测规则和检测逻辑,并执行操作S202、S204、S206和S208。

[0068] 传统的威胁情报使用,在误报率及检测率方面没有控制的很好,往往造成使用方的错误使用以及不规范使用,这对威胁情报检测结果的准确性造成了较大影响。与此不同,通过本公开实施例,使用威胁情报检测引擎的用户不需要有任何威胁情报、安全对抗知识、只需要通过简单的接口调用,就可以使产品或设备具有高精准、可定性、可拦截的威胁情报检测能力。即只要将出站流量日志作为检测对象给威胁情报检测引擎102进行检测,就可以

得到内网主机等网络设备是否失陷,以及失陷类型是什么的结论。

[0069] 此外,通过本公开实施例,还可以实时监测威胁情报检测引擎,对不同的请求类型(如域名类请求,IP类请求,URL类请求等),采用统一化标准的处理方式进行检测并输出检测结果。

[0070] 进一步,在本公开实施例中,在确定待测对象是安全对象后,可以将其动态地更新至对应的域名白名单和/或IP白名单和/或URL白名单中。类似地,在确定待测对象是非安全对象后,可以将其动态地更新至对应的域名黑名单和/或IP黑名单和/或URL黑名单中。由此可以降低后续情报检测的误报率。

[0071] 下面参考图5~图7,并结合具体实施例对图2所示的方法做进一步说明。

[0072] 如前文所述,如果在匹配过程中没有命中上述二级域名黑名单中的二级域名,则尚无法确定上述待测对象是否是安全对象。这种情况下,如果直接忽略该待测对象,即不再做进一步安全检测,则可能存在漏报的情况,由此可能威胁到用户的内网主机等网络设备的安全,甚至造成内网主机失陷。

[0073] 为了克服上述缺陷,在这种情况下还可以进一步执行其他检测逻辑,以便做进一步判断。本公开将在下述实施例中详细阐述其他检测逻辑。

[0074] 具体地,在本公开实施例中,原始域名可以分别命令和控制类(C&C,Comand And Control)域名,IP类域名,DGA类域名。因此,针对不同类型的原始域名,可以预先设置不同的检测逻辑。由此在匹配过程中与待测对象对应的二级域名如果没有命中上述二级域名黑名单中的二级域名,则还可以进一步基于待测对象的原始域名的域名类型调用其他对应的检测逻辑,从而进一步检测待测对象是否是安全对象。

[0075] 作为一种可选的实施例,该方法例如还可以包括如下操作。

[0076] 响应于确定与待测对象对应的二级域名不是预设顶级域名下的二级域名,可以进一步根据获取的目标出站流量日志确定与待测对象对应的原始域名。其中,原始域名的域名类型可以包括命令和控制类(C&C,Comand And Control)、IP类、DGA类(Domain Generate Algorithm),不同的域名类型对应于不同的检测逻辑。

[0077] 确定与待测对象对应的原始域名的域名类型。

[0078] 确定与待测对象对应的原始域名的域名类型对应的检测逻辑。

[0079] 对待测对象执行对应的检测逻辑。

[0080] 基于检测逻辑执行结果,提示待测对象是否是安全对象。

[0081] 示例性的,如图5所示,针对C&C类原始域名,可以执行检测逻辑1,针对IP类原始域名,可以执行检测逻辑2,针对DGA类原始域名,可以执行检测逻辑3。其中,检测逻辑1、检测逻辑2和检测逻辑3彼此不同。

[0082] 进一步,作为一种可选的实施例,与命令和控制类对应的检测逻辑1可以包括以下操作中的至少之一:顶级域名匹配操作、IP匹配操作、top 10w白名单匹配操作、URL匹配操作、端口匹配操作。

[0083] 需要说明的是,本公开实施例中的顶级域名匹配操作与前述实施例中的顶级域名匹配操作类似,都是先提取对应的二级域名,再与上述的二级域名黑名单中的域名匹配。

[0084] 此外,上述IP匹配操作是指判断C&C类原始域名本质上是否是IP地址。

[0085] 此外,URL匹配操作是指判断与待测对象的原始域名对应的URL是否是URL黑名单

或URL白名单中的URL。

[0086] 此外，端口匹配操作是指判断与待测对象的原始域名对应的URL中记载的端口是否是合法的默认常用端口。

[0087] 针对DGA类原始域名，在本公开的一个实施例中，检测逻辑1可以包括顶级域名匹配操作、IP匹配操作、top 10w白名单匹配操作、URL匹配操作、端口匹配操作中的任意一个操作。

[0088] 或者，针对DGA类原始域名，在本公开的其他实施例中，检测逻辑1可以包括顶级域名匹配操作、IP匹配操作、top 10w白名单匹配操作、URL匹配操作、端口匹配操作中的任意多个操作，例如任意两个、三个或四个操作。在这种情况下，检测逻辑1中包含的各操作的执行顺序可以有多种，本公开实施例在此不做限定。

[0089] 优选地，在本公开的一个实施例中，可以在检测逻辑1中设置顶级域名匹配操作、IP匹配操作、top 10w白名单匹配操作、URL匹配操作、端口匹配操作，并控制是否在检测逻辑中对这些操作进行忽略或不忽略。当忽略检测时，会产生更多检测结果及报警，但精度不足可能存在误报问题。

[0090] 检测逻辑2可以包括IP匹配操作，该IP匹配操作表示将该IP类原始域名与IP白名单中的IP进行匹配。

[0091] 检测逻辑3可以包括DGA白名单匹配操作、sinkhole匹配操作和top 10w白名单匹配操作中的一个或多个操作。与检测逻辑1类似，当检测逻辑3包括上述的多个操作时，各操作的执行顺序也可以有多种，本公开实施例在此也不做限定。

[0092] 需要说明的是，在本公开实施例中，sinkhole匹配操作是指与特定安全组织掌握的域名黑名单进行匹配。

[0093] 通过本公开实施例，可以基于不同类型的原始域名执行不同的检测逻辑，以便进一步判断待测对象是否是安全对象。由此，通过对不同类型查询数据进行预处理并根据预处理结果调用并执行不同的检测逻辑，能够让威胁情报IOC检测输出更为准确的检测结果。

[0094] 在本公开的一个实施例中，在判断原始域名的域名类型时，可以将其与C&C类域名库、IP类域名库和DGA类域名库中的域名进行匹配，如果能够命中，则为对应类型数据库中的域名。

[0095] 由于待测对象的原始域名的域名类型可能为C&C类、IP类和DGA类。因此在判断待测对象的原始域名的域名类型会涉及到先对哪种类型进行匹配的问题。在本公开的一个实施例中，考虑到命令和控制类的攻击居多，IP类的次之，DGA类的较少。因此，可以先进行命令和控制类域名匹配，再进行IP类域名匹配，最后进行DGA类域名匹配，以便更快地确定待测对象是否是安全对象。

[0096] 具体地，作为一种可选的实施例，确定对应的原始域名的域名类型可以包括如下操作。

[0097] 先确定对应的原始域名是否属于命令和控制类。

[0098] 在确定对应的原始域名不属于命令和控制类的情况下，再确定对应的原始域名是否属于IP类。

[0099] 在确定对应的原始域名不属于IP类的情况下，再确定对应的原始域名的域名类型是否属于DGA类。

[0100] 示例性的，如图6所示，先判断是否是C&C类，如果是，则调用并执行检测逻辑1；如果不是，则再判断是否是IP类，如果是，则调用并执行检测逻辑2；如果不是，则再判断是否是DGA类，如果是，则调用并执行检测逻辑3；如果不是，可以进一步执行sinkhole匹配操作。

[0101] 通过本公开实施例，在对查询数据进行多层分析过滤之后，结合各类白名单库、TPD(顶级私有域名库)等，返回请求查询的准确结果，提高了威胁情报使用的准确性，同时达到了使用和分发层面的统一。

[0102] 进一步，作为一种可选的实施例，该方法例如还可以包括如下操作。

[0103] 如果确定对应的原始域名属于DGA类，则确定对应的原始域名是否是预设顶级域名下的原始域名。

[0104] 响应于确定对应的原始域名是预设顶级域名下的原始域名，提示待测对象是非安全对象。

[0105] 示例性的，如图7所示，如果待测对象的原始域名属于DGA类，则将其与顶级私有域名库中的域名进行匹配并判断是否命中。如果命中，则确定待测对象为恶意对象。如果没有命中，则还可以执行其他检测操作，如执行sinkhole匹配操作。

[0106] 图8示意性示出了根据本公开实施例的安全检测装置的框图。

[0107] 如图8所示，该安全检测装置800包括获取模块802、第一确定模块804、第二确定模块806和提示模块808。该处理装置可以执行上面参考方法实施例部分描述的方法，在此不再赘述。

[0108] 具体地，获取模块802，用于获取待测对象，其中，该待测对象包括以下类型中的一种：域名类、IP类、URL类。

[0109] 第一确定模块804，用于确定与该待测对象对应的二级域名。

[0110] 第二确定模块806，用于确定该对应的二级域名是否是预设顶级域名下的二级域名。

[0111] 提示模块808，用于响应于确定该对应的二级域名是该预设顶级域名下的二级域名，提示该待测对象为非安全对象。

[0112] 通过本公开实施例，使用威胁情报检测引擎的用户不需要有任何威胁情报、安全对抗知识、只需要通过简单的接口调用，就可以使产品或设备具有高精准、可定性、可拦截的威胁情报检测能力。即只要将出站流量日志作为检测对象给威胁情报检测引擎102进行检测，就可以得到内网主机等网络设备是否失陷，以及失陷类型是什么的结论。

[0113] 此外，通过本公开实施例，还可以实时监测威胁情报检测引擎，对不同的请求类型(如域名类请求，IP类请求，URL类请求等)，采用统一化标准的处理方式进行检测并输出检测结果。

[0114] 作为一种可选的实施例，该方法还可以包括：第三确定模块、第四确定模块、第五确定模块、检测逻辑执行模块和提示模块。具体地，第三确定模块用于响应于确定所述对应的二级域名不是所述预设顶级域名下的二级域名，确定与所述待测对象对应的原始域名，其中，原始域名的域名类型包括命令和控制类、IP类、DGA类，不同的域名类型对应于不同的检测逻辑。第四确定模块用于确定所述对应的原始域名的域名类型。第五确定模块用于确定与所述对应的原始域名的域名类型对应的检测逻辑。检测逻辑执行模块用于对所述待测对象执行所述对应的检测逻辑。提示模块用于基于检测逻辑执行结果，提示所述待测对象

是否是安全对象。

[0115] 作为一种可选的实施例，该第四确定模块可以包括：第一确定单元、第二确定单元和第三确定单元。具体地，第一确定单元用于先确定所述对应的原始域名是否属于命令和控制类。第二确定单元用于在确定所述对应的原始域名不属于命令和控制类的情况下，再确定所述对应的原始域名是否属于IP类。第三确定单元用于在确定所述对应的原始域名不属于IP类的情况下，再确定所述对应的原始域名的域名类型是否属于DGA类。

[0116] 作为一种可选的实施例，该第四确定模块还可以包括：第四确定单元和提示单元。具体地，第四确定单元用于在确定所述对应的原始域名属于DGA类的情况下，确定所述对应的原始域名是否是所述预设顶级域名下的原始域名。提示单元，用于响应于确定所述对应的原始域名是所述预设顶级域名下的原始域名，提示所述待测对象是非安全对象。

[0117] 作为一种可选的实施例，与命令和控制类对应的检测逻辑包括以下操作中的至少之一：顶级域名匹配操作；IP匹配操作；URL匹配操作；端口匹配操作。

[0118] 作为一种可选的实施例，该装置还可以包括：处理策略反馈模块，用于在确定所述待测对象为非安全对象的情况下，反馈针对所述待测对象的处理策略。

[0119] 作为一种可选的实施例，该装置还可以包括：关联信息反馈模块，用于在确定所述待测对象为非安全对象的情况下，基于用户需求反馈所述待测对象的关联信息。

[0120] 需要说明的是，本公开装置部分的实施例与本公开方法部分的实施例对应相同或类似，并且所达到的技术效果也对应相同或类似，本公开实施例在此不再赘述。

[0121] 根据本公开的实施例的模块、单元中的任意多个、或其中任意多个的至少部分功能可以在一个模块中实现。根据本公开实施例的模块、单元中的任意一个或多个可以被拆分成多个模块来实现。根据本公开实施例的模块、单元中的任意一个或多个可以至少被部分地实现为硬件电路，例如现场可编程门阵列(FPGA)、可编程逻辑阵列(PLA)、片上系统、基板上的系统、封装上的系统、专用集成电路(ASIC)，或可以通过对电路进行集成或封装的任何其他的合理方式的硬件或固件来实现，或以软件、硬件以及固件三种实现方式中任意一种或以其中任意几种的适当组合来实现。或者，根据本公开实施例的模块、单元中的一个或多个可以至少被部分地实现为计算机程序模块，当该计算机程序模块被运行时，可以执行相应的功能。

[0122] 例如，获取模块802、第一确定模块804、第二确定模块806和提示模块808中的任意多个可以合并在一个模块中实现，或者其中的任意一个模块可以被拆分成多个模块。或者，这些模块中的一个或多个模块的至少部分功能可以与其他模块的至少部分功能相结合，并在一个模块中实现。根据本公开的实施例，获取模块802、第一确定模块804、第二确定模块806和提示模块808中的至少一个可以至少被部分地实现为硬件电路，例如现场可编程门阵列(FPGA)、可编程逻辑阵列(PLA)、片上系统、基板上的系统、封装上的系统、专用集成电路(ASIC)，或可以通过对电路进行集成或封装的任何其他的合理方式等硬件或固件来实现，或以软件、硬件以及固件三种实现方式中任意一种或以其中任意几种的适当组合来实现。或者，获取模块802、第一确定模块804、第二确定模块806和提示模块808中的至少一个可以至少被部分地实现为计算机程序模块，当该计算机程序模块被运行时，可以执行相应的功能。

[0123] 图9示意性示出了根据本公开实施例的电子设备的框图。图9示出的电子设备仅仅

是一个示例，不应对本公开实施例的功能和使用范围带来任何限制。

[0124] 如图9所示，电子设备900包括处理器910、计算机可读存储介质920。该电子设备900可以执行根据本公开实施例的方法。

[0125] 具体地，处理器910例如可以包括通用微处理器、指令集处理器和/或相关芯片组和/或专用微处理器(例如，专用集成电路(ASIC))，等等。处理器910还可以包括用于缓存用途的板载存储器。处理器910可以是用于执行根据本公开实施例的方法流程的不同动作的单一处理单元或者是多个处理单元。

[0126] 计算机可读存储介质920，例如可以是非易失性的计算机可读存储介质，具体示例包括但不限于：磁存储装置，如磁带或硬盘(HDD)；光存储装置，如光盘(CD-ROM)；存储器，如随机存取存储器(RAM)或闪存；等等。

[0127] 计算机可读存储介质920可以包括计算机程序921，该计算机程序921可以包括代码/计算机可执行指令，其在由处理器910执行时使得处理器910执行根据本公开实施例的方法或其任何变形。

[0128] 计算机程序921可被配置为具有例如包括计算机程序模块的计算机程序代码。例如，在示例实施例中，计算机程序921中的代码可以包括一个或多个程序模块，例如包括921A、模块921B、……。应当注意，模块的划分方式和个数并不是固定的，本领域技术人员可以根据实际情况使用合适的程序模块或程序模块组合，当这些程序模块组合被处理器910执行时，使得处理器910可以执行根据本公开实施例的方法或其任何变形。

[0129] 根据本公开的实施例，获取模块802、第一确定模块804、第二确定模块806和提示模块808中的至少一个可以实现为参考图9描述的计算机程序模块，其在被处理器910执行时，可以实现上面描述的相应操作。

[0130] 本公开还提供了一种计算机可读存储介质，该计算机可读存储介质可以是上述实施例中描述的设备/装置/系统中所包含的；也可以是单独存在，而未装配入该设备/装置/系统中。上述计算机可读存储介质承载有一个或者多个程序，当上述一个或者多个程序被执行时，实现根据本公开实施例的方法。

[0131] 附图中的流程图和框图，图示了按照本公开各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分，上述模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个接连地表示的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图或流程图中的每个方框、以及框图或流程图中的方框的组合，可以用执行规定的功能或操作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0132] 本领域技术人员可以理解，尽管已经参照本公开的特定示例性实施例示出并描述了本公开，但是本领域技术人员应该理解，在不背离所附权利要求及其等同物限定的本公开的精神和范围的情况下，可以对本公开进行形式和细节上的多种改变。因此，本公开的范围不应该限于上述实施例，而是应该不仅由所附权利要求来进行确定，还由所附权利要求的等同物来进行限定。

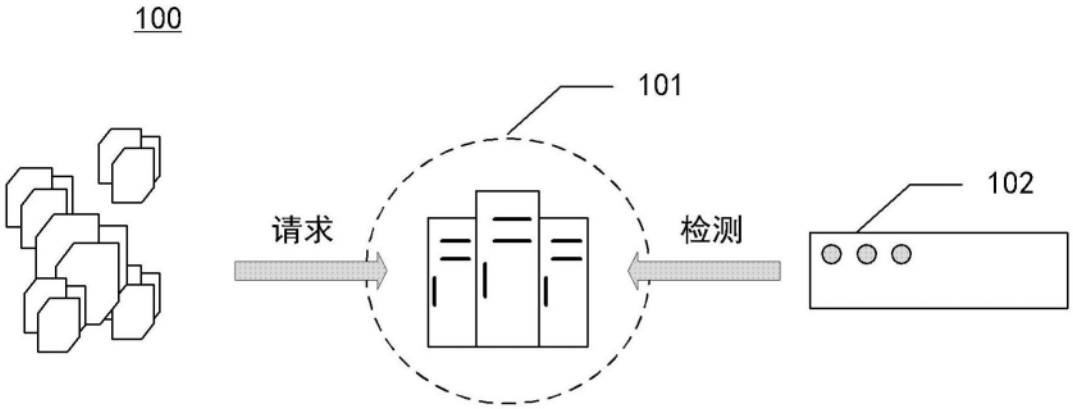


图1A

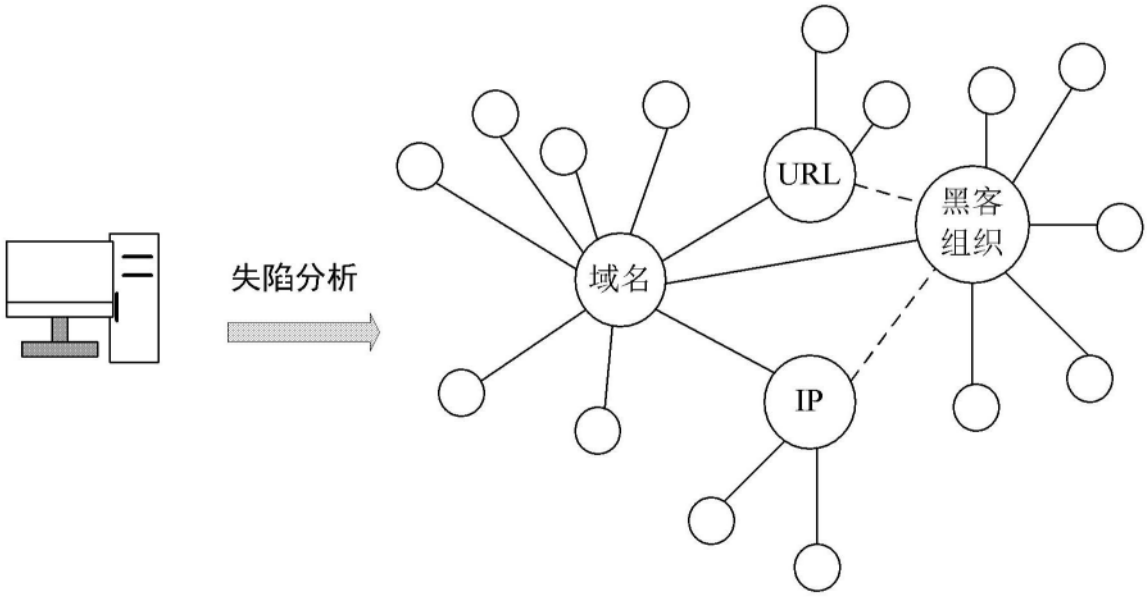


图1B

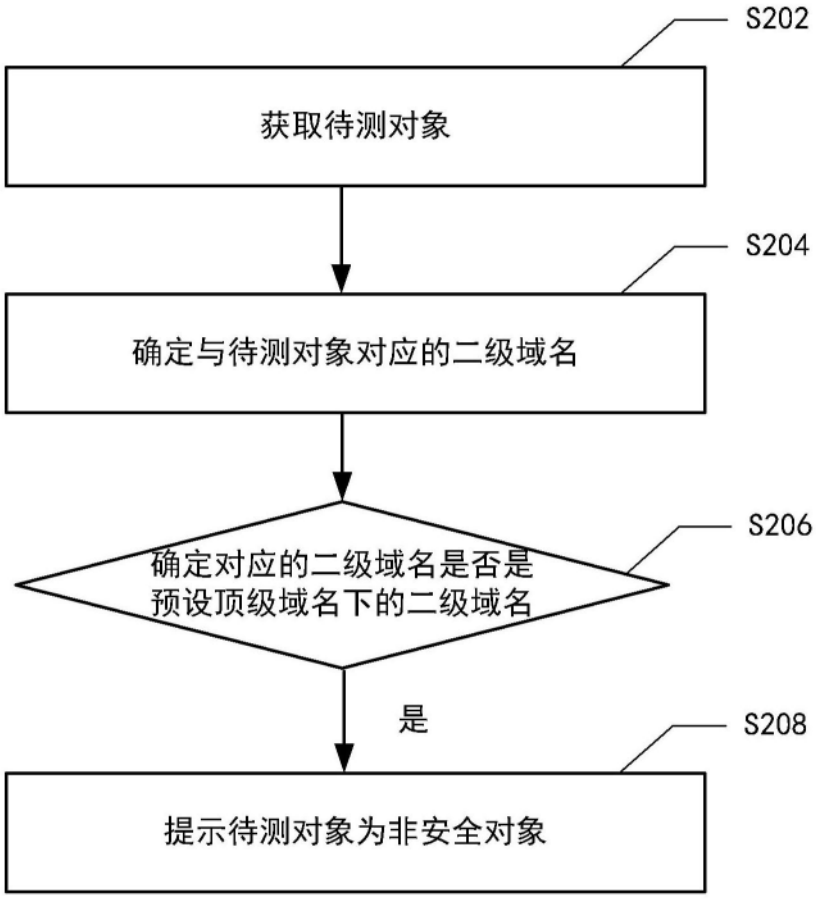

S202
获取待测对象
S204
确定与待测对象对应的二级域名
S206
确定对应的二级域名是否是
预设顶级域名下的二级域名
是
S208
提示待测对象为非安全对象

图2

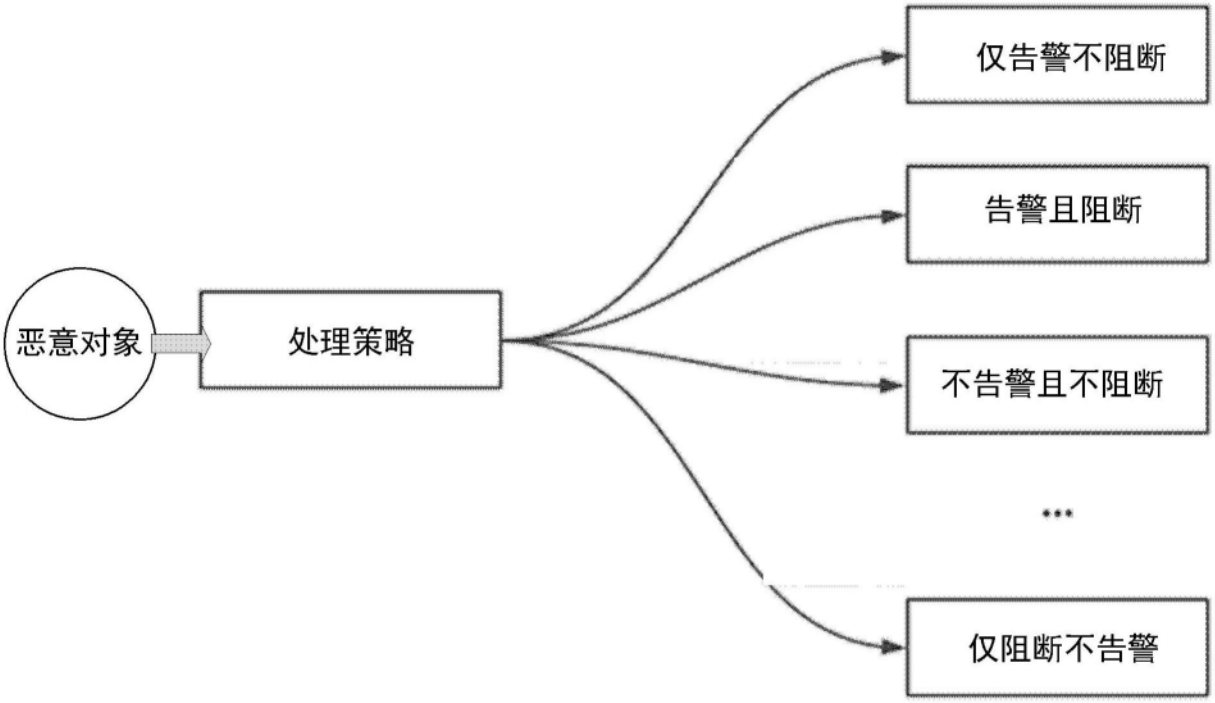

恶意对象
处理策略
仅告警不阻断
告警且阻断
不告警且不阻断
...
仅阻断不告警

图3

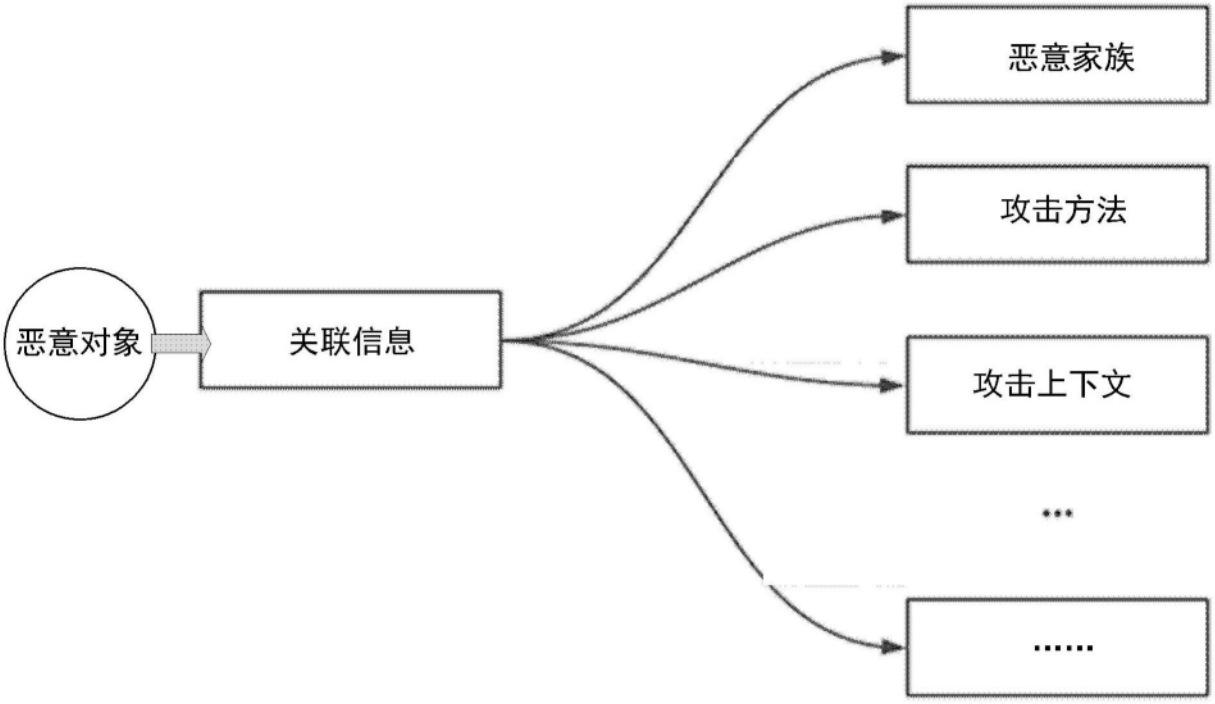

恶意对象
关联信息
恶意家族
攻击方法
攻击上下文
...
.....

图4

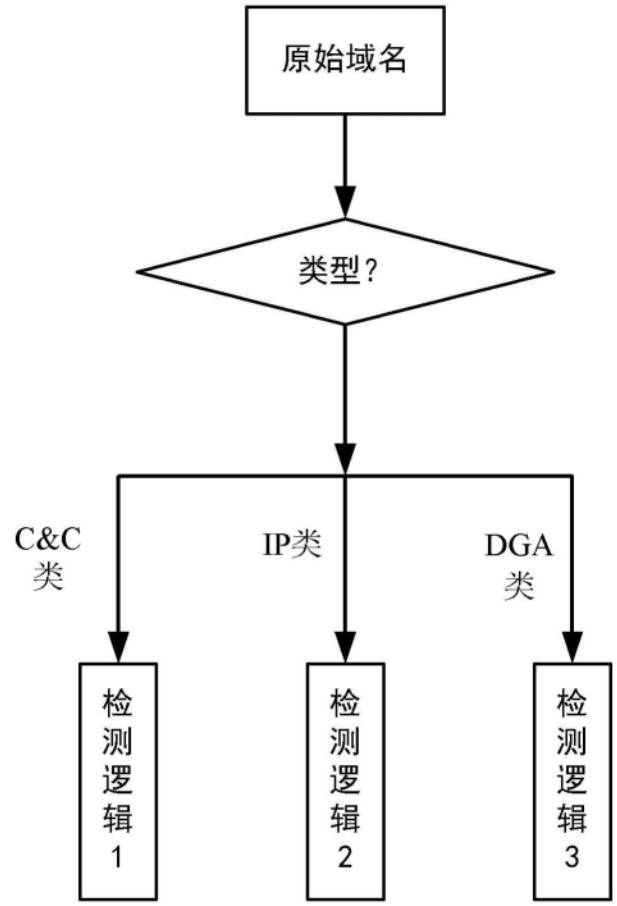

原始域名
类型?
C&C
类
IP类
DGA
类
检测逻辑1
检测逻辑2
检测逻辑3

图5

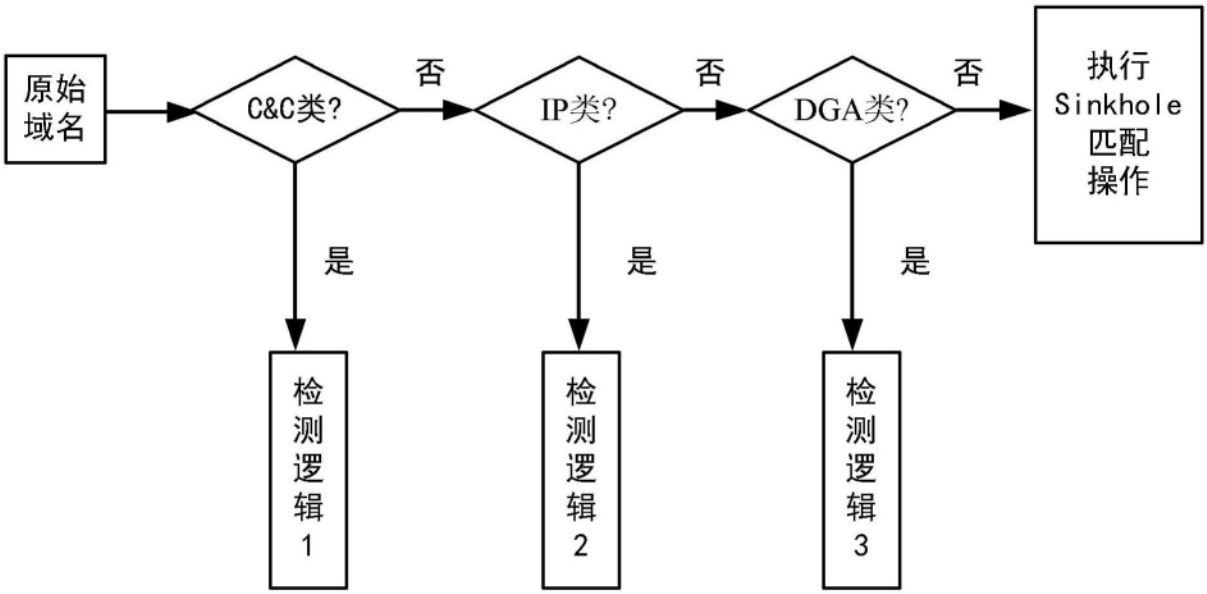

原始域名
C&C类?
否
IP类?
否
DGA类?
否
执行Sinkhole匹配操作
是
是
是
检测逻辑1
检测逻辑2
检测逻辑3

图6

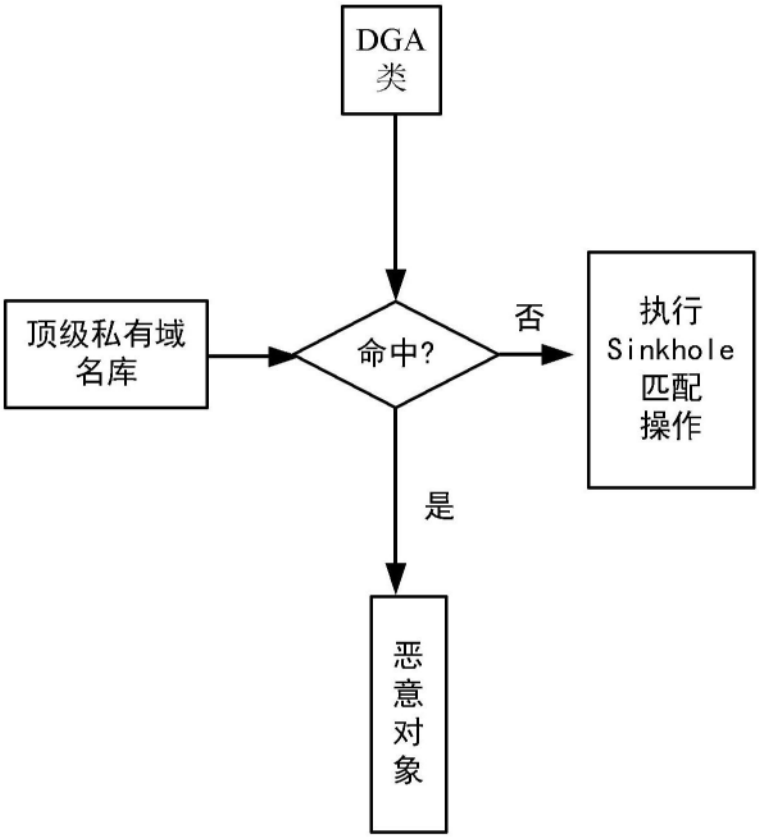


图7

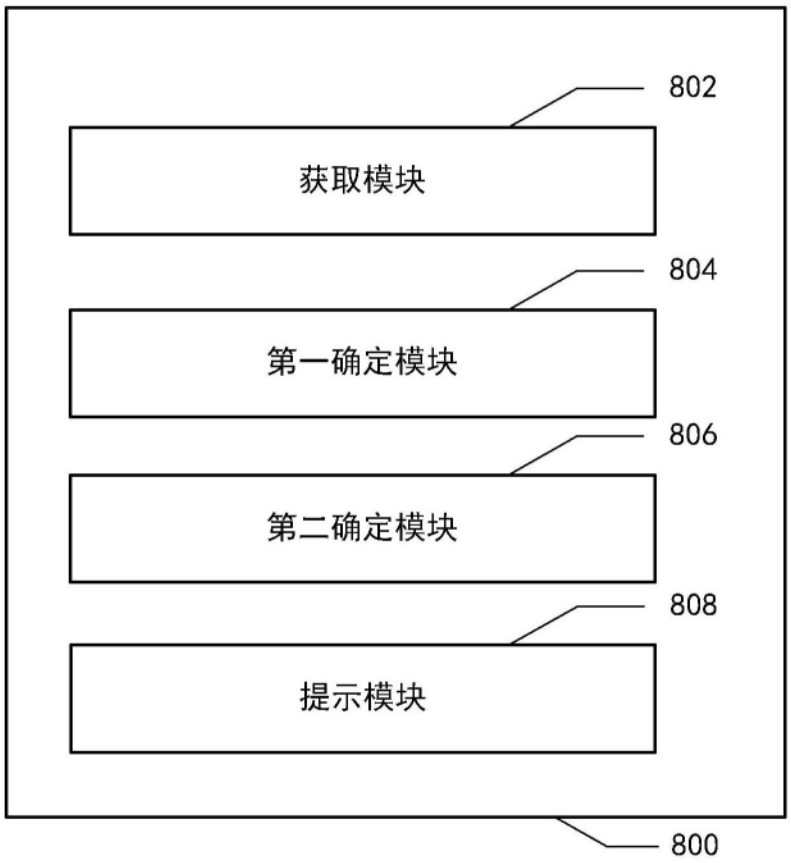

802
获取模块
804
第一确定模块
806
第二确定模块
808
提示模块
800

图8

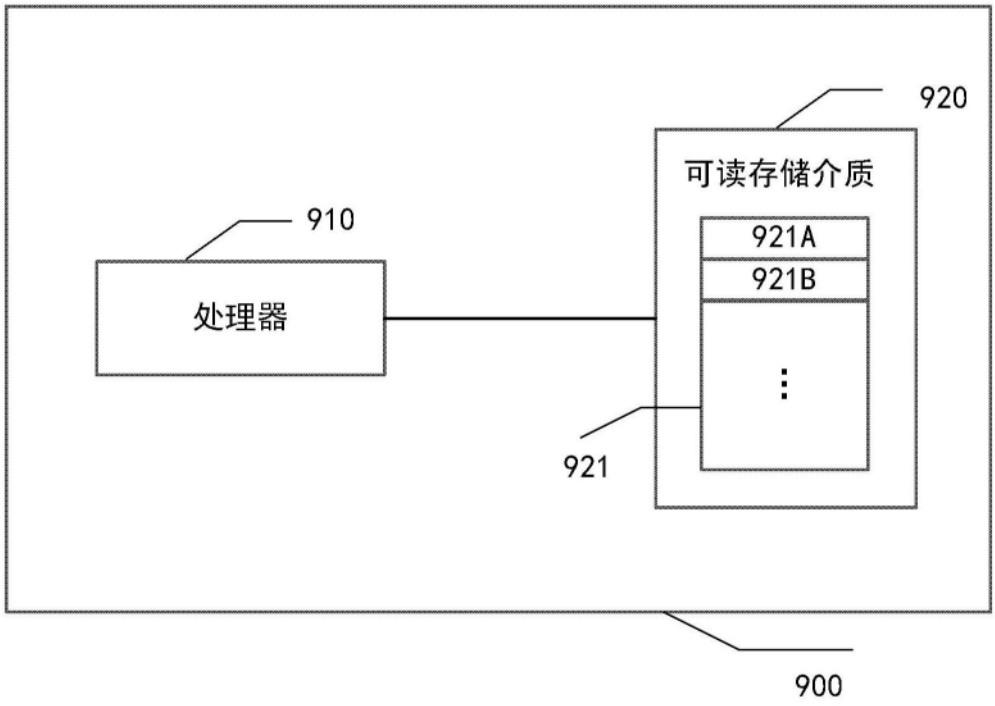

920
可读存储介质
910
处理器
921A
921B
921
900

图9