(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113329035 B
(45)授权公告日 2022.09.30

(21)申请号 202110728721.4
(22)申请日 2021.06.29
(65)同一申请的已公布的文献号
申请公布号 CN 113329035 A
(43)申请公布日 2021.08.31
(73)专利权人 深信服科技股份有限公司
地址 518055 广东省深圳市南山区学苑大道1001号南山智园A1栋
(72)发明人 周凯强 岳巍
(74)专利代理机构 北京派特恩知识产权代理有限公司 11270
专利代理师 李娟 张颖玲
(51)Int.Cl.
*H04L 9/40*(2022.01)
*H04L 61/4511*(2022.01)

审查员 白生斌

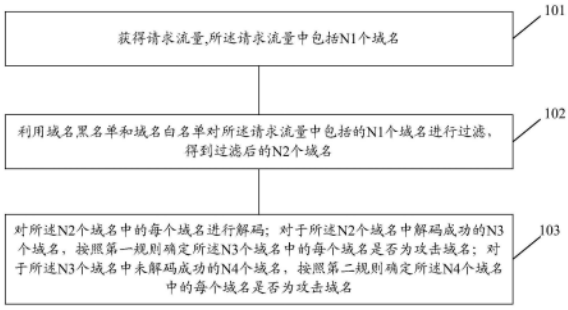
权利要求书3页 说明书14页 附图2页

(54)发明名称

一种攻击域名的检测方法、装置、电子设备及存储介质

(57)摘要

本申请公开了一种攻击域名的检测方法、装置、电子设备及存储介质，其中，所述方法包括：获得请求流量；所述请求流量中包括N1个域名；利用域名黑名单和域名白名单对所述请求流量中包括的N1个域名进行过滤，得到过滤后的N2个域名；对所述N2个域名中的每个域名进行解码；对于所述N2个域名中解码成功的N3个域名，按照第一规则确定所述N3个域名中的每个域名是否为攻击域名；对于所述N3个域名中未解码成功的N4个域名，按照第二规则确定所述N4个域名中的每个域名是否为攻击域名。




CN 113329035 B

1.一种攻击域名的检测方法,其特征在于,所述方法包括:

获得请求流量;所述请求流量中包括N1个域名;

利用域名黑名单和域名白名单对所述请求流量中包括的N1个域名进行过滤,得到过滤后的N2个域名;

对所述N2个域名中的每个域名进行解码;对于所述N2个域名中解码成功的N3个域名,利用第一命令集合执行所述N3个域名中的每个域名;所述第一命令集合中包括至少一个执行命令;将所述N3个域名中利用所述第一命令集合执行成功的域名确定为攻击域名;对于所述N2个域名中未解码成功的N4个域名,按照第二规则确定所述N4个域名中的每个域名是否为攻击域名。

2.根据权利要求1所述的方法,其特征在于,所述按照第二规则确定所述N4个域名中的每个域名是否为攻击域名,包括:

确定所述N4个域名中的N5个可访问域名和N6个不可访问域名;

针对所述N5个可访问域名,按照第三规则确定所述N5个可访问域名中的每个域名是否为攻击域名;

针对所述N6个不可访问域名,按照第四规则确定所述N6个不可访问域名中的每个域名是否为攻击域名。

3.根据权利要求2所述的方法,其特征在于,所述确定所述N4个域名中的N5个可访问域名和N6个不可访问域名之前,所述方法还包括:

确定所述N4个域名中访问频率高于第一频率阈值的N7个域名,将所述N7个域名确定为非攻击域名。

4.根据权利要求2所述的方法,其特征在于,所述按照第三规则确定所述N5个可访问域名中的每个域名是否为攻击域名,包括:

利用第二命令集合执行所述N5个域名中的每个域名,确定执行结果中包括高危明文字符的N8个域名,以及执行结果中不包括高危明文字符的N9个域名;所述第二命令集合中包括至少一个执行命令;

对执行结果中包括高危明文字符的N8个域名的访问请求进行网络流量查询,得到所述N8个域名的访问请求中只存在域名请求流量的N10个域名,以及所述N8个域名的访问请求中除域名请求流量外还存在非域名请求流量的N11个域名;

将所述N10个域名确定为攻击域名,并按照第五规则确定所述N9个域名以及所述N11个域名是否为攻击域名。

5.根据权利要求4所述的方法,其特征在于,所述按照第五规则确定所述N9个域名以及所述N11个域名是否为攻击域名,包括:

利用字符关联性算法模型确定出所述N9个域名以及所述N11个域名中不符合所述字符关联性算法模型的N12个域名,将所述N12个域名确定为攻击域名。

6.根据权利要求5所述的方法,其特征在于,所述利用字符关联性算法模型确定出所述N9个域名以及所述N11个域名中不符合所述字符关联性算法模型的N12个域名之前,所述方法还包括:

确定所述N9个域名以及所述N11个域名中解析到同一IP的至少一个域名集合;所述至少一个域名集合中的每个域名集合中的域名对应同一解析互联网协议IP地址,所述至少一

个域名集合中的各域名集合之间对应的解析IP不同；

确定所述至少一个域名集合中包括的域名数量大于第一数量阈值的M1个域名集合，以及，所述至少一个域名集合中包括的域名数量小于等于第一数量阈值的M2个域名集合；所述M2个域名集合中共包括N13个域名；

将所述M1个域名集合中的每个域名确定为攻击域名；

所述利用字符关联性算法模型确定出所述N9个域名以及所述N11个域名中不符合所述字符关联性算法模型的N12个域名，将所述N12个域名确定为攻击域名，包括：

利用字符关联性算法模型确定出所述N13个域名中不符合所述字符关联性算法模型的N14个域名，将所述N14个域名确定为攻击域名。

7.根据权利要求5所述的方法，其特征在于，所述利用字符关联性算法模型确定出所述N9个域名以及所述N11个域名中不符合所述字符关联性算法模型的N12个域名，将所述N12个域名确定为攻击域名之前，所述方法还包括：

确定出所述N9个域名以及所述N11个域名中对应的请求IP数量大于第二数量阈值的N15个域名，以及所述N9个域名以及所述N11个域名中对应的请求IP数量小于等于第二数量阈值的N16个域名，将所述N15个域名确定为正常域名；

相应的，所述利用字符关联性算法模型确定出所述N9个域名以及所述N11个域名中不符合所述字符关联性算法模型的N12个域名，将所述N12个域名确定为攻击域名，包括：

利用字符关联性算法模型确定出所述N16个域名中不符合所述字符关联性算法模型的N17个域名，将所述N17个域名确定为攻击域名。

8.根据权利要求2所述的方法，其特征在于，所述按照第四规则确定所述N6个不可访问域名中的每个域名是否为攻击域名，包括：

利用字符关联性算法模型确定出所述N6个域名中不符合所述字符关联性算法模型的N18个域名，将所述N18个域名确定为攻击域名。

9.根据权利要求8所述的方法，其特征在于，所述利用字符关联性算法模型确定出所述N6个域名中不符合所述字符关联性算法模型的N18个域名，将所述N18个域名确定为攻击域名之前，所述方法还包括：

确定出所述N6个域名中对应的请求IP的数量大于等于第三数量阈值的N19个域名，以及所述6个域名中对应的请求IP的数量小于等于第三数量阈值的N20个域名，将所述N19个域名确定为正常域名；

相应的，所述利用字符关联性算法模型确定出所述N6个域名中不符合所述字符关联性算法模型的N18个域名，将所述N18个域名确定为攻击域名，包括：

利用字符关联性算法模型确定出所述N20个域名中不符合所述字符关联性算法模型的N21个域名，将所述N21个域名确定为攻击域名。

10.一种攻击域名的检测装置，其特征在于，所述装置包括：

获得单元，用于获得请求流量；所述请求流量中包括N1个域名；

过滤单元，用于利用域名黑名单和域名白名单对所述请求流量中包括的N1个域名进行过滤，得到过滤后的N2个域名；

确定单元，用于对所述N2个域名中的每个域名进行解码；对于所述N2个域名中解码成功的N3个域名，利用第一命令集合执行所述N3个域名中的每个域名；所述第一命令集合中

包括至少一个执行命令;将所述N3个域名中利用所述第一命令集合执行成功的域名确定为攻击域名;对于所述N2个域名中未解码成功的N4个域名,按照第二规则确定所述N4个域名中的每个域名是否为攻击域名。

11.一种电子设备,其特征在于,所述电子设备包括:存储器和处理器,所述存储器上存储有计算机可执行指令,所述处理器运行所述存储器上的计算机可执行指令时可实现权利要求1至9中任一项所述的方法。

12.一种计算机存储介质,其特征在于,所述存储介质上存储有可执行指令,该可执行指令被处理器执行时实现权利要求1至9中任一项所述的方法。

# 一种攻击域名的检测方法、装置、电子设备及存储介质

## 技术领域

[0001] 本申请实施例涉及通信领域，尤其涉及一种攻击域名的检测方法、装置、电子设备及存储介质。

## 背景技术

[0002] 域名系统日志(DNSLOG，Domain Name System Log)技术广泛应用于无法直接进行命令执行回显以及判断服务器是否能够出网等攻击场景，尤其是反序列化漏洞的数量越来越多，利用DNSLOG进行反序列化漏洞探测这样的攻击行为也越来越常见。因此，亟需设计实现一个DNSLOG攻击行为的检测方法来覆盖这些攻击场景。目前已有的技术方案大多都是通过黑名单的方式进行，这种简单的检测方式较容易产生正常访问行为的误报，且对于非黑名单内的攻击行为无法检测，存在较高的漏报。

## 发明内容

[0003] 为解决上述技术问题，本申请实施例提供了一种攻击域名的检测方法、装置、电子设备及存储介质。

[0004] 本申请实施例提供了一种攻击域名的检测方法，所述方法包括：

[0005] 获得请求流量；所述请求流量中包括N1个域名；

[0006] 利用域名黑名单和域名白名单对所述请求流量中包括的N1个域名进行过滤，得到过滤后的N2个域名；

[0007] 对所述N2个域名中的每个域名进行解码；对于所述N2个域名中解码成功的N3个域名，按照第一规则确定所述N3个域名中的每个域名是否为攻击域名；对于所述N2个域名中未解码成功的N4个域名，按照第二规则确定所述N4个域名中的每个域名是否为攻击域名。

[0008] 本申请一可选实施方式中，所述按照第一规则确定所述N3个域名中的每个域名是否为攻击域名，包括：

[0009] 利用第一命令集合执行所述N3个域名中的每个域名；所述第一命令集合中包括至少一个执行命令；

[0010] 将所述N3个域名中利用所述第一命令集合执行成功的域名确定为攻击域名。

[0011] 本申请一可选实施方式中，所述按照第二规则确定所述N4个域名中的每个域名是否为攻击域名，包括：

[0012] 确定所述N4个域名中的N5个可访问域名和N6个不可访问域名；

[0013] 针对所述N5个可访问域名，按照第三规则确定所述N5个可访问域名中的每个域名是否为攻击域名；

[0014] 针对所述N6个不可访问域名，按照第四规则确定所述N6个不可访问域名中的每个域名是否为攻击域名。

[0015] 本申请一可选实施方式中，所述确定所述N4个域名中的N5个可访问域名和N6个不可访问域名之前，所述方法还包括：

[0016] 确定所述N4个域名中访问频率高于第一频率阈值的N7个域名,将所述N7个域名确定为非攻击域名。

[0017] 本申请一可选实施方式中,所述按照第三规则确定所述N5个可访问域名中的每个域名是否为攻击域名,包括:

[0018] 利用第二命令集合执行所述N5个域名中的每个域名,确定执行结果中包括高危明文字符的N8个域名,以及执行结果中不包括高危明文字符的N9个域名;所述第二命令集合中包括至少一个执行命令;

[0019] 对执行结果中包括高危明文字符的N8个域名的访问请求进行网络流量查询,得到所述N8个域名的访问请求中只存在域名请求流量的N10个域名,以及所述N8个域名的访问请求中除域名请求流量外还存在非域名请求流量的N11个域名;

[0020] 将所述N10个域名确定为攻击域名,并按照第五规则确定所述N9个域名以及所述N11个域名是否为攻击域名。

[0021] 本申请一可选实施方式中,所述按照第五规则确定所述N9个域名以及所述N11个域名是否为攻击域名,包括:

[0022] 利用字符关联性算法模型确定出所述N9个域名以及所述N11个域名中不符合所述字符关联性算法模型的N12个域名,将所述N12个域名确定为攻击域名。

[0023] 本申请一可选实施方式中,所述利用字符关联性算法模型确定出所述N9个域名以及所述N11个域名中不符合所述字符关联性算法模型的N12个域名之前,所述方法还包括:

[0024] 确定所述N9个域名以及所述N11个域名中解析到同一IP的至少一个域名集合;所述至少一个域名集合中的每个域名集合中的域名对应同一解析IP,所述至少一个域名集合中的各域名集合之间对应的解析IP不同;

[0025] 确定所述至少一个域名集合中包括的域名数量大于第一数量阈值的M1个域名集合,以及,所述至少一个域名集合中包括的域名数量小于等于第一数量阈值的M2个域名集合;所述M2个域名集合中共包括N13个域名;

[0026] 将所述M1个域名集合中的每个域名确定为攻击域名;

[0027] 所述利用字符关联性算法模型确定出所述N9个域名以及所述N11个域名中不符合所述字符关联性算法模型的N12个域名,将所述N12个域名确定为攻击域名,包括:

[0028] 利用字符关联性算法模型确定出所述N13个域名中不符合所述字符关联性算法模型的N14个域名,将所述N14个域名确定为攻击域名。

[0029] 本申请一可选实施方式中,所述利用字符关联性算法模型确定出所述N9个域名以及所述N11个域名中不符合所述字符关联性算法模型的N12个域名,将所述N12个域名确定为攻击域名之前,所述方法还包括:

[0030] 确定出所述N9个域名以及所述N11个域名中对应的请求IP数量大于第二数量阈值的N15个域名,以及所述N9个域名以及所述N11个域名中对应的请求IP数量小于等于第二数量阈值的N16个域名,将所述N15个域名确定为正常域名;

[0031] 相应的,所述利用字符关联性算法模型确定出所述N9个域名以及所述N11个域名中不符合所述字符关联性算法模型的N12个域名,将所述N12个域名确定为攻击域名,包括:

[0032] 利用字符关联性算法模型确定出所述N16个域名中不符合所述字符关联性算法模型的N17个域名,将所述N17个域名确定为攻击域名。

[0033] 本申请一可选实施方式中，所述按照第四规则确定所述N6个不可访问域名中的每个域名是否为攻击域名，包括：

[0034] 利用字符关联性算法模型确定出所述N6个域名中不符合所述字符关联性算法模型的N18个域名，将所述N18个域名确定为攻击域名。

[0035] 本申请一可选实施方式中，所述利用字符关联性算法模型确定出所述N6个域名中不符合所述字符关联性算法模型的N18个域名，将所述N18个域名确定为攻击域名之前，所述方法还包括：

[0036] 确定出所述N6个域名中对应的请求IP的数量大于等于第三数量阈值的N19个域名，以及所述6个域名中对应的请求IP的数量小于等于第三数量阈值的N20个域名，将所述N19个域名确定为正常域名；

[0037] 相应的，所述利用字符关联性算法模型确定出所述N6个域名中不符合所述字符关联性算法模型的N18个域名，将所述N18个域名确定为攻击域名，包括：

[0038] 利用字符关联性算法模型确定出所述N20个域名中不符合所述字符关联性算法模型的N21个域名，将所述N21个域名确定为攻击域名。

[0039] 本申请实施例还提供了一种攻击域名的检测装置，所述装置包括：

[0040] 获得单元，用于获得请求流量；所述请求流量中包括N1个域名；

[0041] 过滤单元，用于利用域名黑名单和域名白名单对所述请求流量中包括的N1个域名进行过滤，得到过滤后的N2个域名；

[0042] 确定单元，用于对所述N2个域名中的每个域名进行解码；对于所述N2个域名中解码成功的N3个域名，按照第一规则确定所述N3个域名中的每个域名是否为攻击域名；对于所述N2个域名中未解码成功的N4个域名，按照第二规则确定所述N4个域名中的每个域名是否为攻击域名。

[0043] 本申请一可选实施方式中，所述确定单元，具体用于：利用第一命令集合执行所述N3个域名中的每个域名；所述第一命令集合中包括至少一个执行命令；

[0044] 将所述N3个域名中利用所述第一命令集合执行成功的域名确定为攻击域名。

[0045] 本申请一可选实施方式中，所述确定单元，具体用于：确定所述N4个域名中的N5个可访问域名和N6个不可访问域名；针对所述N5个可访问域名，按照第三规则确定所述N5个可访问域名中的每个域名是否为攻击域名；针对所述N6个不可访问域名，按照第四规则确定所述N6个不可访问域名中的每个域名是否为攻击域名。

[0046] 本申请一可选实施方式中，所述确定单元，还用于：确定所述N4个域名中的N5个可访问域名和N6个不可访问域名之前，确定所述N4个域名中访问频率高于第一频率阈值的N7个域名，将所述N7个域名确定为非攻击域名。

[0047] 本申请一可选实施方式中，所述确定单元，还用于：利用第二命令集合执行所述N5个域名中的每个域名，确定执行结果中包括高危明文字符的N8个域名，以及执行结果中不包括高危明文字符的N9个域名；所述第二命令集合中包括至少一个执行命令；对执行结果中包括高危明文字符的N8个域名的访问请求进行网络流量查询，得到所述N8个域名的访问请求中只存在域名请求流量的N10个域名，以及所述N8个域名的访问请求中除域名请求流量外还存在非域名请求流量的N11个域名；将所述N10个域名确定为攻击域名，并按照第五规则确定所述N9个域名以及所述N11个域名是否为攻击域名。

[0048] 本申请一可选实施方式中，所述确定单元，还用于：利用字符关联性算法模型确定出所述N9个域名以及所述N11个域名中不符合所述字符关联性算法模型的N12个域名，将所述N12个域名确定为攻击域名。

[0049] 本申请一可选实施方式中，所述确定单元，还用于：利用字符关联性算法模型确定出所述N9个域名以及所述N11个域名中不符合所述字符关联性算法模型的N12个域名之前，确定所述N9个域名以及所述N11个域名中解析到同一IP的至少一个域名集合；所述至少一个域名集合中的每个域名集合中的域名对应同一解析IP，所述至少一个域名集合中的各域名集合之间对应的解析IP不同；确定所述至少一个域名集合中包括的域名数量大于第一数量阈值的M1个域名集合，以及，所述至少一个域名集合中包括的域名数量小于等于第一数量阈值的M2个域名集合；所述M2个域名集合中共包括N13个域名；将所述M1个域名集合中的每个域名确定为攻击域名；所述确定单元还具体用于：利用字符关联性算法模型确定出所述N13个域名中不符合所述字符关联性算法模型的N14个域名，将所述N14个域名确定为攻击域名。

[0050] 本申请一可选实施方式中，所述确定单元，还用于：利用字符关联性算法模型确定出所述N9个域名以及所述N11个域名中不符合所述字符关联性算法模型的N12个域名，将所述N12个域名确定为攻击域名之前，确定出所述N9个域名以及所述N11个域名中对应的请求IP数量大于第二数量阈值的N15个域名，以及所述N9个域名以及所述N11个域名中对应的请求IP数量小于等于第二数量阈值的N16个域名，将所述N15个域名确定为正常域名；相应的，所述确定单元还具体用于：利用字符关联性算法模型确定出所述N16个域名中不符合所述字符关联性算法模型的N17个域名，将所述N17个域名确定为攻击域名。

[0051] 本申请一可选实施方式中，所述确定单元，还具体用于：利用字符关联性算法模型确定出所述N6个域名中不符合所述字符关联性算法模型的N18个域名，将所述N18个域名确定为攻击域名。

[0052] 本申请一可选实施方式中，所述确定单元，还具体用于：利用字符关联性算法模型确定出所述N6个域名中不符合所述字符关联性算法模型的N18个域名，将所述N18个域名确定为攻击域名之前，确定出所述N6个域名中对应的请求IP的数量大于等于第三数量阈值的N19个域名，以及所述6个域名中对应的请求IP的数量小于等于第三数量阈值的N20个域名，将所述N19个域名确定为正常域名；相应的，所述确定单元还具体用于：利用字符关联性算法模型确定出所述N20个域名中不符合所述字符关联性算法模型的N21个域名，将所述N21个域名确定为攻击域名。

[0053] 本申请实施例还提供了一种电子设备，其特征在于，所述电子设备包括：存储器和处理器，所述存储器上存储有计算机可执行指令，所述处理器运行所述存储器上的计算机可执行指令时可实现上述实施例所述的攻击流量的检测方法。

[0054] 本申请实施例还提供了一种计算机存储介质，其特征在于，所述存储介质上存储有可执行指令，该可执行指令被处理器执行时实现上述实施例所述的攻击流量的检测方法。

[0055] 本申请实施例的技术方案，通过获得请求流量；所述请求流量中包括N1个域名；利用域名黑名单和域名白名单对所述请求流量中包括的N1个域名进行过滤，得到过滤后的N2个域名；对所述N2个域名中的每个域名进行解码；对于所述N2个域名中解码成功的N3个域

名,按照第一规则确定所述N3个域名中的每个域名是否为攻击域名;对于所述N2个域名中未解码成功的N4个域名,按照第二规则确定所述N4个域名中的每个域名是否为攻击域名。如此,能够克服仅利用黑名单方式对请求流量中的域名信息进行检测的局限性,对于非黑名单内的攻击域名也能够进行全面的检测,提高对攻击域名检测的准确率。

## 附图说明

[0056] 图1为本申请实施例提供的一种攻击域名的检测方法的流程示意图;

[0057] 图2为本申请实施例提供的一种攻击域名的检测流程示意图;

[0058] 图3为本申请实施例提供的攻击域名的检测装置的结构组成示意图;

[0059] 图4为本申请实施例提供的一种电子设备的结构组成示意图。

## 具体实施方式

[0060] 为了能够更加详尽地了解本申请实施例的特点与技术内容,下面结合附图对本申请实施例的实现进行详细阐述,所附附图仅供参考说明之用,并非用来限定本申请实施例。

[0061] 下面,对本申请实施例涉及的关键术语进行解释:

[0062] 域名系统(DNS,Domain Name System),将域名和互联网协议(IP,Internet Protocol)地址相互映射的一个分布式数据库,能够使人更方便地访问互联网。DNS使用传输控制协议(TCP,Transmission Control Protocol)和用户数据报协议(UDP,User Datagram Protocol)的53端口作为服务端口,

[0063] DNSLOG,就是存储在DNS服务器上的域名信息,它记录着用户对域名如www.baidu.com等的访问信息,类似日志文件。

[0064] 域生成算法(DGA,Domain Generation Algorithm),是在各种恶意软件家族中频繁使用的算法,用于定期生成大量域名,这些域名可用作恶意软件命令和控制服务器的集合点。比如一个恶意软件A,拥有一个恶意域名AAA.com,通过DGA算法生成BBB.AAA.com、CCC.AAA.com等子域名,不同的子域名代表不同的攻击步骤,如攻击机器通过访问BBB.AAA.com来下载恶意软件,而通过访问CCC.AAA.com来进行数据上传等,通过生成不同的子域名来对攻击步骤甚至不同的控制服务器来进行区分,攻击者只需要修改主域名就可以做到这所有的操作。

[0065] 本申请实施例的技术方案用于解决DNSLOG请求流量中无明显攻击特征,且DNSLOG请求流量特征与DNS隧道较为相似等问题。本申请在现有通过关键字检测DNSLOG流量的场景上,对DNSLOG请求流量特征进行分析,通过结合如netflow及字符关联性算法等方式,将无法直接通过黑名单检测出来的DNSLOG攻击行为做到了基本覆盖,且通过一些频率特征较好降低了误报,做到了对dnslog攻击行为的全覆盖。

[0066] 图1为本申请实施例提供的一种攻击域名的检测方法的流程示意图,如图1所示,本申请实施例提供的攻击域名的检测方法包括如下步骤:

[0067] 步骤101:获得请求流量;所述请求流量中包括N1个域名。

[0068] 本申请实施例中,攻击者或者普通用户利用客户端向DNS服务器发起DNSLOG请求服务,在攻击者或者普通用户利用客户端向DNS服务器发起DNSLOG请求服务的情况下,DNS服务器能够接受到客户端发送的请求流量。

[0069] DNSLOG与DNS隧道请求流量中都是通过在同一个主域名下利用不同的子域名进行拼接来做到信息传递的目的,如主域名A.com,通过将信息拼接在A.com前面,如B.A.com B.B.B.A.com这种形式;子域名都是通过DGA算法、编码算法或者加密算法生成,没用明显的可读性;域名都是解析到同一个IP地址等特征。

[0070] 步骤102:利用域名黑名单和域名白名单对所述请求流量中包括的N1个域名进行过滤,得到过滤后的N2个域名。

[0071] 本申请实施例中,域名黑名单为目前已知的DNSLOG服务域名及本地威胁情报中的DNSLOG域名,白名单为地址路由参数域名(如ip6.arpa)、不规范域名(如localhost)、政府类域名(如gov.cn)等。

[0072] 若请求流量中包括的N1个域名中的部分域名的关键字与域名黑名单中的部分域名相同,则将与域名黑名单中的部分域名相同的这部分域名确定为攻击域名。

[0073] 若请求你流量中包括的N1个域名中的部分域名的关键字与域名白名单中的部分域名相同,则将与域名白名单中的部分域名相同的这部分域名确定为非攻击域名,也可以称之为正常域名。

[0074] 本申请实施通过利用域名黑名单和域名白名单对请求流量中包括的所有N1个域名进行过滤,能够过滤掉请求流量中明显的攻击域名和正常域名,减少后续确定请求流量中的域名是否为攻击域名的判定过程的数据处理量。

[0075] 步骤103:对所述N2个域名中的每个域名进行解码;对于所述N2个域名中解码成功的N3个域名,按照第一规则确定所述N3个域名中的每个域名是否为攻击域名;对于所述N2个域名中未解码成功的N4个域名,按照第二规则确定所述N4个域名中的每个域名是否为攻击域名。

[0076] 对请求流量中包括的域名进行解码操作,主要用于检测通过DNSLOG进行外带数据的攻击场景,对于不在步骤102中域名黑名单和域名白名单中的N2个域名进行域名解码操作,将N2个域名进行常见编码方式的解码尝试,包括hex、base64、base32等。

[0077] 本申请一可选实施方式中,对于所述按照第一规则确定所述N3个域名中的每个域名是否为攻击域名这一步骤具体可通过如下方式实现:

[0078] 利用第一命令集合执行所述N3个域名中的每个域名;所述第一命令集合中包括至少一个执行命令;

[0079] 将所述N3个域名中利用所述第一命令集合执行成功的域名确定为攻击域名。

[0080] 具体的,对于执行域名解码操作后成功解码的域名,对成功解码的内容进行命令执行成功的规则匹配,第一命令集合包括ifconfig、netstat等命令,

[0081] 具体的,如ifconfig命令执行结果为主机网卡及IP信息等,因此可以通过匹配如IP地址或者网卡信息等方式来进行命令执行结果的判断。对于存在命令执行结果的域名,可以认定为该域名是存在通过域名进行外带信息的行为符合DNSLOG的攻击行为特征,因此可以生成DNSLOG攻击事件,即判定该域名为攻击域名。

[0082] 本申请实施例中,对于未执行成功的域名可以可以生成信息类的提醒日志,用于后续人工分析或者作为一个记录的作用。

[0083] 本申请一可选实施方式中,对于所述按照第二规则确定所述N4个域名中的每个域名是否为攻击域名这一步骤具体可通过如下方式实现:

[0084] 确定所述N4个域名中的N5个可访问域名和N6个不可访问域名；

[0085] 针对所述N5个可访问域名，按照第三规则确定所述N5个可访问域名中的每个域名是否为攻击域名；

[0086] 针对所述N6个不可访问域名，按照第四规则确定所述N6个不可访问域名中的每个域名是否为攻击域名。

[0087] 本申请实施例中，请求域名地址及域名对应的IP地址，可访问域名的响应数据包会有该域名的解析IP地址，以便后续访问行为能够顺利进行，不可访问域名就没有这个响应数据包。

[0088] 本申请一可选实施方式中，执行所述确定所述N4个域名中的N5个可访问域名和N6个不可访问域名之前，还可以执行如下步骤：

[0089] 确定所述N4个域名中访问频率高于第一频率阈值的N7个域名，将所述N7个域名确定为非攻击域名。

[0090] 该实施方式用于排除请求域名中的DNS隧道域名及常用域名，通过对一定周期内的访问域名进行频率统计，将其中访问频率较高的域名进行排除，如在一分钟内访问了100次以上，则认为这一类域名不适用于DNSLOG攻击场景，可将其排除，即将访问频率高于一定数值的域名确定为非攻击域名。

[0091] 访问频率高代表这个域名是存在很多主机都有这个访问需求的，这种特征排除极端情况(整个客户内容均被攻陷)不属于DNSLOG攻击特征，因此可以将这些域名排除，减少后面判断逻辑的数据量

[0092] 本申请一可选实施方式中，对于所述按照第三规则确定所述N5个可访问域名中的每个域名是否为攻击域名这一步骤，具体可通过如下方式实现：

[0093] 利用第二命令集合执行所述N5个域名中的每个域名，确定执行结果中包括高危明文字符的N8个域名，以及执行结果中不包括高危明文字符的N9个域名；所述第二命令集合中包括至少一个执行命令；

[0094] 对执行结果中包括高危明文字符的N8个域名的访问请求进行网络流量查询，得到所述N8个域名的访问请求中只存在域名请求流量的N10个域名，以及所述N8个域名的访问请求中除域名请求流量外还存在非域名请求流量的N11个域名；

[0095] 将所述N10个域名确定为攻击域名，并按照第五规则确定所述N9个域名以及所述N11个域名是否为攻击域名。

[0096] 这一步骤用于排除非DNSLOG攻击域名请求。将一些简单的命令(如”whoami”、”hostname”等)执行成功的结果定义为高危明文字符，对DNS请求域名进行匹配。由于DNSLOG攻击场景中，DNSLOG域名大多都没有提供除DNS之外的服务，因此如果是DNSLOG攻击的话，在网络流量(netflow)中只会存在DNS请求流量，而不会有其他如HTTP的请求流量，因此可以对域名存在明文高危字符的访问请求进行netflow查询，当netflow中只有DNS请求流量的话可判定为DNSLOG攻击域名。

[0097] 对于高危明文字符，如whoami的执行结果可能为root，hostname执行结果可能为windowsXXX，高危明文字符主要包括一些简单的命令(whoami、hostname)的执行结果。

[0098] 对DNS请求域名进行匹配时，可以通过对一定时间窗口(如一个请求的前后各几分钟，可以称为一个时间窗口)的数据流进行缓存，然后对这些数据流进行请求域名查询。

[0099] 本申请一可选实施方式中，对于所述按照第五规则确定所述N9个域名以及所述N11个域名是否为攻击域名这一步骤，具体可通过以下方式实现：

[0100] 利用字符关联性算法模型确定出所述N9个域名以及所述N11个域名中不符合所述字符关联性算法模型的N12个域名，将所述N12个域名确定为攻击域名。

[0101] 该实施方式主要通过子域名关联性算法来进行攻击域名的判断，具体的，正常场景中，域名的命名通常是一些英文单词或者中文拼音缩写，这些字词间都会存在一些规律，如在英文单词中，存在如”am”、”as”等单词，因此字母”a”后面接”m”、”s”的概率更大一些，而DNSLOG中使用的域名为了防止出现重复的域名，大多都是使用DGA或者随机字符的方式来生成子域名。因此我们可以通过字符关联性计算的算法，如马尔可夫模型算法、香浓熵算法等，对常用的字符进行建模，然后对不符合字符关联性算法模型的域名就判定为DNSLOG攻击域名。

[0102] 本申请一可选实施方式中，执行所述利用字符关联性算法模型确定出所述N9个域名以及所述N11个域名中不符合所述字符关联性算法模型的N12个域名之一步骤之前，还可以执行如下步骤：

[0103] 确定所述N9个域名以及所述N11个域名中解析到同一IP的至少一个域名集合；所述至少一个域名集合中的每个域名集合中的域名对应同一解析IP，所述至少一个域名集合中的各域名集合之间对应的解析IP不同；

[0104] 确定所述至少一个域名集合中包括的域名数量大于第一数量阈值的M1个域名集合，以及，所述至少一个域名集合中包括的域名数量小于等于第一数量阈值的M2个域名集合；所述M2个域名集合中共包括N13个域名；

[0105] 将所述M1个域名集合中的每个域名确定为攻击域名；

[0106] 所述利用字符关联性算法模型确定出所述N9个域名以及所述N11个域名中不符合所述字符关联性算法模型的N12个域名，将所述N12个域名确定为攻击域名，包括：

[0107] 利用字符关联性算法模型确定出所述N13个域名中不符合所述字符关联性算法模型的N14个域名，将所述N14个域名确定为攻击域名。

[0108] 该实施方式主要通过子域名IP来进行攻击域名的判断，具体的，DNSLOG服务都是只有一个主域名，然后通过访问不同的子域名来进行攻击，但这些子域名都会解析到同一个IP地址，如存在DNSLOG域名”dnslog.cn”，无论是访问”a.dnslog.cn”还是”b.dnslog.cn”都会解析到同一个IP地址，因此可通过如存在10个不同的子域名的解析IP都相同的话则认为该域名为dnslog攻击域名。

[0109] 本申请一可选实施方式中，所述利用字符关联性算法模型确定出所述N9个域名以及所述N11个域名中不符合所述字符关联性算法模型的N12个域名，将所述N12个域名确定为攻击域名这一步骤之前，还可以执行如下步骤：

[0110] 确定出所述N9个域名以及所述N11个域名中对应的请求IP数量大于第二数量阈值的N15个域名，以及所述N9个域名以及所述N11个域名中对应的请求IP数量小于等于第二数量阈值的N16个域名，将所述N15个域名确定为正常域名；

[0111] 相应的，所述利用字符关联性算法模型确定出所述N9个域名以及所述N11个域名中不符合所述字符关联性算法模型的N12个域名，将所述N12个域名确定为攻击域名，包括：

[0112] 利用字符关联性算法模型确定出所述N16个域名中不符合所述字符关联性算法模

型的N17个域名，将所述N17个域名确定为攻击域名。

[0113] 具体的，该步骤主要通过行为分析方法来进行攻击域名的判断，具体的，当存在DNSLOG攻击行为时，一般是通过命令执行这一类的方式进行的，这一类行为的受影响主机数量都不会太多，因此可通过对单个域名的请求IP进行统计，如一个域名存在10个以上不同的IP访问请求，则认为该域名为正常域名。

[0114] 本申请一可选实施方式中，所述按照第四规则确定所述N6个不可访问域名中的每个域名是否为攻击域名这一步骤具体可通过如下方式实现：

[0115] 利用字符关联性算法模型确定出所述N6个域名中不符合所述字符关联性算法模型的N18个域名，将所述N18个域名确定为攻击域名。

[0116] 该实施方式主要通过子域名关联性算法来进行攻击域名的判断，可参照前述通过子域名关联性算法来进行攻击域名判断的举例进行理解。

[0117] 本申请一可选实施方式中，执行所述利用字符关联性算法模型确定出所述N6个域名中不符合所述字符关联性算法模型的N18个域名，将所述N18个域名确定为攻击域名这一步骤之前，还可以执行如下步骤：

[0118] 确定出所述N6个域名中对应的请求IP的数量大于等于第三数量阈值的N19个域名，以及所述6个域名中对应的请求IP的数量小于等于第三数量阈值的N20个域名，将所述N19个域名确定为正常域名；

[0119] 相应的，所述利用字符关联性算法模型确定出所述N6个域名中不符合所述字符关联性算法模型的N18个域名，将所述N18个域名确定为攻击域名，包括：

[0120] 利用字符关联性算法模型确定出所述N20个域名中不符合所述字符关联性算法模型的N21个域名，将所述N21个域名确定为攻击域名。

[0121] 该步骤主要通过行为分析方法来进行攻击域名的判断，可参照前述通过行为分析方法来进行攻击域名的判断的举例进行理解。

[0122] 本申请实施例的技术方案能够用于解决DNSLOG请求流量中无明显攻击特征，且DNSLOG请求流量特征与DNS隧道较为相似等问题，克服了仅利用黑名单方式对请求流量中的域名信息进行检测的局限性，对于非黑名单内的攻击域名也能够进行全面的检测，提高了对攻击域名检测的准确率。

[0123] 图2为本申请实施例提供的一种攻击域名的检测流程示意图，图2中的攻击域名的检测流程包括如下步骤：

[0124] 步骤201：黑名单过滤。

[0125] 针对获取的请求流量，例如确定出该请求流量中包括200个域名，利用域名黑名单对请求流量中包括的200个域名进行过滤，若确定出请求流量的200个域名中存在20个域名的关键字与黑名单中的部分域名相同，则将该20个域名确定为攻击域名，生成DNSLOG事件。此外，还可以利用域名白名单对请求流量包括的剩余180个域名进行过滤，这里，假设该180个域名中不存在关键字与域名白名单中的域名相同的域名，则可最终得到既不属于域名黑名单也不属于域名白名单的180个域名。

[0126] 步骤202：域名解码。

[0127] 针对步骤201得到的180个域名，对这180个域名利用常见的hex、base64、base32的等解码方式进行域名解码操作，得到20个能够解码成功的域名，以及160个未能解码成功的

域名,对其中20个解码成功的域名执行步骤203,并对其中160个未能解码成功的域名执行步骤204。

[0128] 步骤203:命令执行成功规则库。

[0129] 对于解码成功的20个域名,利用ifconfig、netstat等命令执行命令执行成功的规则匹配,对于存在命令执行结果的域名,可以认定为该域名是存在通过域名进行外带信息的行为符合DNSLOG的攻击行为特征,因此可以生成DNSLOG攻击事件,即判定该域名为攻击域名。

[0130] 步骤204:排除高频访问。

[0131] 对于步骤203确定出的160个未能解码成功的域名,统计该160个域名的访问频率,确定出其中一分钟内访问频率大于100的20个域名,将这20个域名确定为非攻击域名,并将剩余的140个域名利用步骤205进一步判断。

[0132] 步骤205:响应数据。

[0133] 利用针对步骤204确定出的140个域名的响应数据,确定出该140个域名中的120个可访问域名和20个不可访问域名。针对确定出的120个可访问域名继续利用步骤206进行判断,针对确定出的20个不可访问域名则利用步骤208进行进一步判断。

[0134] 步骤206:高危明文字符确定及netflow查询。

[0135] 针对步骤205确定出的120个可访问域名,利用一些简单的命令(如"whoami"、"hostname"等)执行该120个可访问域名,其中执行结果包括高危明文字符的域名的个数为100,不包括高危明文字符的域名个数为20,则对执行结果包括高危明文字符的100个域名进行网络流量查询,得到访问请求中只存在域名请求流量的10个域名,以及除域名请求流量外还存在非域名请求流量的90个域名,将访问请求中只存在域名请求流量的10个域名确定为攻击域名,生成DNSLOG攻击事件。并将除域名请求流量外还存在非域名请求流量的90个域名以及执行结果不包括高危明文字符的20个域名共110个域名利用步骤207进行进一步判断。

[0136] 步骤207:子域名IP。

[0137] 针对步骤206得到的共110个域名,确定出该110个域名中每个域名的解析IP,根据各域名的解析IP,确定出对应同一解析IP的数量在10以上的20个域名,将该20个域名确定为攻击域名,生成DNSLOG事件。针对剩余的90个域名利用步骤208进一步判断。

[0138] 步骤208:行为分析。

[0139] 针对步骤207得到的90个域名以及步骤205得到的20个不可访问域名,可以确定出其中每个域名的不同IP访问请求的数量,将域名的不同IP访问请求数量在10以上的域名确定为正常域名,利用该步骤得到100个不同IP访问请求数量在10或10以下的域名,将该100个域名利用步骤209进行进一步判断,对于剩余的10个不同IP访问请求数量在10以上的域名,确定该10个域名为正常域名。

[0140] 步骤209:子域名关联算法。

[0141] 由于攻击域名一般是利用DGA或者随机字符的方式来生成的,因此,不同域名之间的关联性较弱,利用马尔科夫模型等字符关联性算法,确定出步骤208得到的100个域名中不符合字符关联性算法的60个域名,以及符合字符关联性算法的40个域名,可将不符合字符关联性算法的60个域名确定为攻击域名,生成DNSLOG事件。

[0142] 步骤210:DNSLOG事件生成。

[0143] 该步骤主要针对上述步骤201至209确定出的各攻击域名,生成DNSLOG事件,可便于进行后续的攻击域名的分析。

[0144] 图2中按照步骤201至210的顺序依次执行,其中,每一个在前的步骤都能够减少在后的步骤执行时的数据处理的工作量。可以理解的是,步骤201至210中的部分步骤的顺序是可以根据需求进行调换的或增减的,包括但不限于以下几种形式,例如图2中的步骤201、步骤204、步骤207以及步骤208可以部分或全部删除,仅利用剩余的步骤进行请求流量中攻击域名的判断;又或者,图2中的步骤207和步骤208可以调换顺序,也能够实现对请求流量中攻击域名是否为攻击域名的判定。

[0145] 本申请实施例还提供了一种攻击域名的检测装置,图3为本申请实施例提供的攻击域名的检测装置的结构组成示意图,如图3所示,所述装置300包括:

[0146] 获得单元301,用于获得请求流量;所述请求流量中包括N1个域名;

[0147] 过滤单元302,用于利用域名黑名单和域名白名单对所述请求流量中包括的N1个域名进行过滤,得到过滤后的N2个域名;

[0148] 确定单元303,用于对所述N2个域名中的每个域名进行解码;对于所述N2个域名中解码成功的N3个域名,按照第一规则确定所述N3个域名中的每个域名是否为攻击域名;对于所述N2个域名中未解码成功的N4个域名,按照第二规则确定所述N4个域名中的每个域名是否为攻击域名。

[0149] 本申请一可选实施方式中,所述确定单元303,具体用于:利用第一命令集合执行所述N3个域名中的每个域名;所述第一命令集合中包括至少一个执行命令;将所述N3个域名中利用所述第一命令集合执行成功的域名确定为攻击域名。

[0150] 本申请一可选实施方式中,所述确定单元303,具体用于:确定所述N4个域名中的N5个可访问域名和N6个不可访问域名;针对所述N5个可访问域名,按照第三规则确定所述N5个可访问域名中的每个域名是否为攻击域名;针对所述N6个不可访问域名,按照第四规则确定所述N6个不可访问域名中的每个域名是否为攻击域名。

[0151] 本申请一可选实施方式中,所述确定单元303,还用于:确定所述N4个域名中的N5个可访问域名和N6个不可访问域名之前,确定所述N4个域名中访问频率高于第一频率阈值的N7个域名,将所述N7个域名确定为非攻击域名。

[0152] 本申请一可选实施方式中,所述确定单元303,还用于:利用第二命令集合执行所述N5个域名中的每个域名,确定执行结果中包括高危明文字符的N8个域名,以及执行结果中不包括高危明文字符的N9个域名;所述第二命令集合中包括至少一个执行命令;对执行结果中包括高危明文字符的N8个域名的访问请求进行网络流量查询,得到所述N8个域名的访问请求中只存在域名请求流量的N10个域名,以及所述N8个域名的访问请求中除域名请求流量外还存在非域名请求流量的N11个域名;将所述N10个域名确定为攻击域名,并按照第五规则确定所述N9个域名以及所述N11个域名是否为攻击域名。

[0153] 本申请一可选实施方式中,所述确定单元303,还用于:利用字符关联性算法模型确定出所述N9个域名以及所述N11个域名中不符合所述字符关联性算法模型的N12个域名,将所述N12个域名确定为攻击域名。

[0154] 本申请一可选实施方式中,所述确定单元303,还用于:利用字符关联性算法模型

确定出所述N9个域名以及所述N11个域名中不符合所述字符关联性算法模型的N12个域名之前，确定所述N9个域名以及所述N11个域名中解析到同一IP的至少一个域名集合；所述至少一个域名集合中的每个域名集合中的域名对应同一解析IP，所述至少一个域名集合中的各域名集合之间对应的解析IP不同；确定所述至少一个域名集合中包括的域名数量大于第一数量阈值的M1个域名集合，以及，所述至少一个域名集合中包括的域名数量小于等于第一数量阈值的M2个域名集合；所述M2个域名集合中共包括N13个域名；将所述M1个域名集合中的每个域名确定为攻击域名；所述确定单元还具体用于：利用字符关联性算法模型确定出所述N13个域名中不符合所述字符关联性算法模型的N14个域名，将所述N14个域名确定为攻击域名。

[0155] 本申请一可选实施方式中，所述确定单元303，还用于：利用字符关联性算法模型确定出所述N9个域名以及所述N11个域名中不符合所述字符关联性算法模型的N12个域名，将所述N12个域名确定为攻击域名之前，确定出所述N9个域名以及所述N11个域名中对应的请求IP数量大于第二数量阈值的N15个域名，以及所述N9个域名以及所述N11个域名中对应的请求IP数量小于等于第二数量阈值的N16个域名，将所述N15个域名确定为正常域名；相应的，所述确定单元还具体用于：利用字符关联性算法模型确定出所述N16个域名中不符合所述字符关联性算法模型的N17个域名，将所述N17个域名确定为攻击域名。

[0156] 本申请一可选实施方式中，所述确定单元303，还具体用于：利用字符关联性算法模型确定出所述N6个域名中不符合所述字符关联性算法模型的N18个域名，将所述N18个域名确定为攻击域名。

[0157] 本申请一可选实施方式中，所述确定单元303，还具体用于：利用字符关联性算法模型确定出所述N6个域名中不符合所述字符关联性算法模型的N18个域名，将所述N18个域名确定为攻击域名之前，确定出所述N6个域名中对应的请求IP的数量大于等于第三数量阈值的N19个域名，以及所述6个域名中对应的请求IP的数量小于等于第三数量阈值的N20个域名，将所述N19个域名确定为正常域名；相应的，所述确定单元303还具体用于：利用字符关联性算法模型确定出所述N20个域名中不符合所述字符关联性算法模型的N21个域名，将所述N21个域名确定为攻击域名。

[0158] 本领域技术人员应当理解，图3所示的攻击域名的检测装置中的各单元的实现功能可参照前述攻击域名的检测方法的相关描述而理解。图3所示的攻击域名的检测装置中的各单元的功能可通过运行于处理器上的程序而实现，也可通过具体的逻辑电路而实现。

[0159] 本申请实施例还提供了一种电子设备。图4为本申请实施例的电子设备的硬件结构示意图，如图4所示，电子设备包括：用于进行数据传输的通信组件403、至少一个处理器401和用于存储能够在处理器401上运行的计算机程序的存储器402。终端中的各个组件通过总线系统404耦合在一起。可理解，总线系统404用于实现这些组件之间的连接通信。总线系统404除包括数据总线之外，还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见，在图4中将各种总线都标为总线系统404。

[0160] 其中，所述处理器401执行所述计算机程序时至少执行图1或图2所示的方法的步骤。

[0161] 可以理解，存储器402可以是易失性存储器或非易失性存储器，也可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器(ROM，Read Only Memory)、

可编程只读存储器(PROM,Programmable Read-Only Memory)、可擦除可编程只读存储器(EPROM,Erasable Programmable Read-Only Memory)、电可擦除可编程只读存储器(EEPROM,Electrically Erasable Programmable Read-Only Memory)、磁性随机存取存储器(FRAM,ferromagnetic random access memory)、快闪存储器(Flash Memory)、磁表面存储器、光盘、或只读光盘(CD-ROM,Compact Disc Read-Only Memory);磁表面存储器可以是磁盘存储器或磁带存储器。易失性存储器可以是随机存取存储器(RAM,Random Access Memory),其用作外部高速缓存。通过示例性但不是限制性说明,许多形式的RAM可用,例如静态随机存取存储器(SRAM,Static Random Access Memory)、同步静态随机存取存储器(SSRAM,Synchronous Static Random Access Memory)、动态随机存取存储器(DRAM,Dynamic Random Access Memory)、同步动态随机存取存储器(SDRAM,Synchronous Dynamic Random Access Memory)、双倍数据速率同步动态随机存取存储器(DDRSDRAM,Double Data Rate Synchronous Dynamic Random Access Memory)、增强型同步动态随机存取存储器(ESDRAM,Enhanced Synchronous Dynamic Random Access Memory)、同步连接动态随机存取存储器(SLDRAM,SyncLink Dynamic Random Access Memory)、直接内存总线随机存取存储器(DRRAM,Direct Rambus Random Access Memory)。本申请实施例描述的存储器402旨在包括但不限于这些和任意其它适合类型的存储器。

[0162] 上述本申请实施例揭示的方法可以应用于处理器401中,或者由处理器401实现。处理器401可能是一种集成电路芯片,具有信号的处理能力。在实现过程中,上述方法的各步骤可以通过处理器401中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器401可以是通用处理器、DSP,或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。处理器401可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者任何常规的处理器等。结合本申请实施例所公开的方法的步骤,可以直接体现为硬件译码处理器执行完成,或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于存储介质中,该存储介质位于存储器402,处理器401读取存储器402中的信息,结合其硬件完成前述方法的步骤。

[0163] 在示例性实施例中,电子设备可以被一个或多个应用专用集成电路(ASIC,Application Specific Integrated Circuit)、DSP、可编程逻辑器件(PLD,Programmable Logic Device)、复杂可编程逻辑器件(CPLD,Complex Programmable Logic Device)、FPGA、通用处理器、控制器、MCU、微处理器(Microprocessor)、或其他电子元件实现,用于执行前述的通话录音方法。

[0164] 本申请实施例还提供一种计算机可读存储介质,其上存储有计算机程序,其特征在于,该程序被处理器执行时至少用于执行图1或图2所示方法的步骤。所述计算机可读存储介质具体可以为存储器。所述存储器可以为如图4所示的存储器402。

[0165] 本申请实施例所记载的技术方案之间,在不冲突的情况下,可以任意组合。

[0166] 在本申请所提供的几个实施例中,应该理解到,所揭露的方法和智能设备,可以通过其它的方式实现。以上所描述的设备实施例仅仅是示意性的,例如,所述单元的划分,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式,如:多个单元或组件可以结合,或可以集成到另一个系统,或一些特征可以忽略,或不执行。另外,所显示或讨论的各组成部分相互之间的耦合、或直接耦合、或通信连接可以是通过一些接口,设备或单元的间接

耦合或通信连接,可以是电性的、机械的或其它形式的。

[0167] 上述作为分离部件说明的单元可以是、或也可以不是物理上分开的,作为单元显示的部件可以是、或也可以不是物理单元,即可以位于一个地方,也可以分布到多个网络单元上;可以根据实际的需要选择其中的部分或全部单元来实现本实施例方案的目的。

[0168] 另外,在本申请各实施例中的各功能单元可以全部集成在一个第二处理单元中,也可以是各单元分别单独作为一个单元,也可以两个或两个以上单元集成在一个单元中;上述集成的单元既可以采用硬件的形式实现,也可以采用硬件加软件功能单元的形式实现。

[0169] 以上所述,仅为本申请的具体实施方式,但本申请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申请揭露的技术范围内,可轻易想到变化或替换,都应涵盖在本申请的保护范围之内。

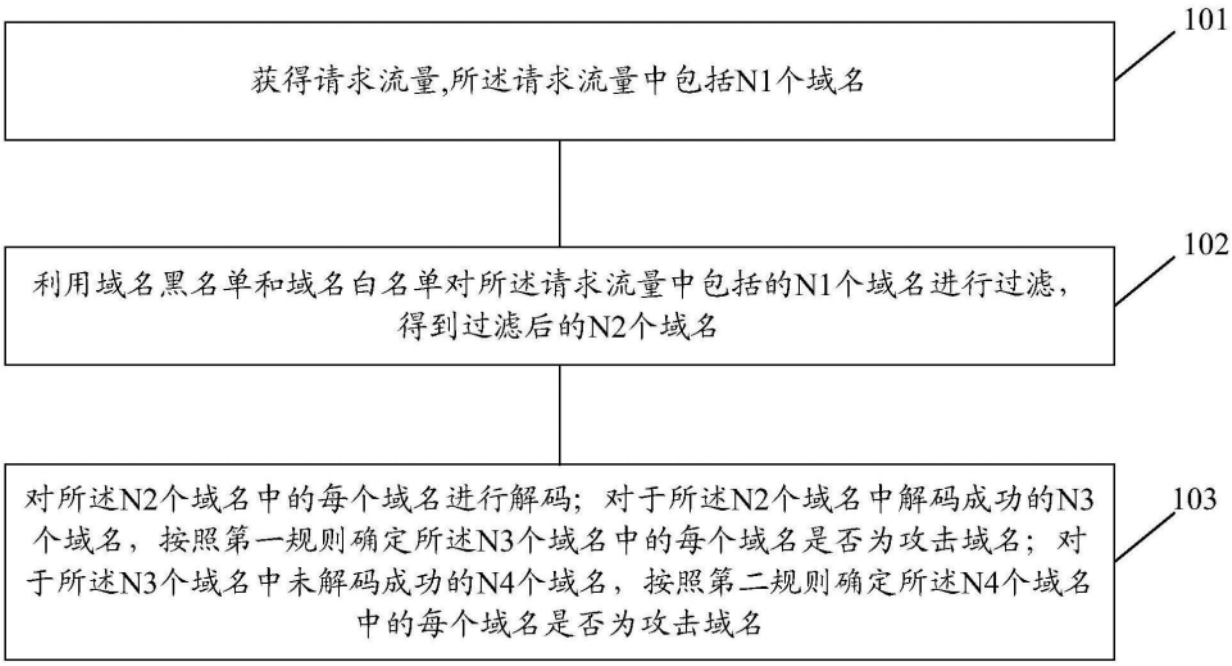

101
获得请求流量,所述请求流量中包括N1个域名
102
利用域名黑名单和域名白名单对所述请求流量中包括的N1个域名进行过滤，得到过滤后的N2个域名
103
对所述N2个域名中的每个域名进行解码；对于所述N2个域名中解码成功的N3个域名，按照第一规则确定所述N3个域名中的每个域名是否为攻击域名；对于所述N3个域名中未解码成功的N4个域名，按照第二规则确定所述N4个域名中的每个域名是否为攻击域名

图1

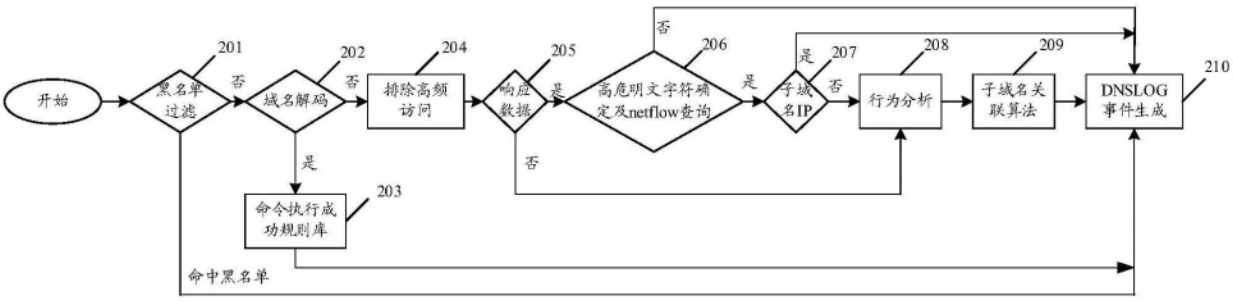

开始
201
黑名单过滤
否
202
域名解码
否
204
排除高频访问
205
响应数据
是
206
高危明文字符确定及netflow查询
是
207
子域名IP
否
208
行为分析
209
子域名关联算法
210
DNSLOG事件生成
否
是
否
是
203
命令执行成功规则库
命中黑名单

图2

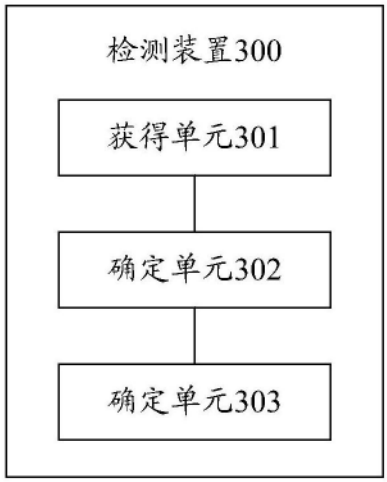

检测装置300
获得单元301
确定单元302
确定单元303

图3

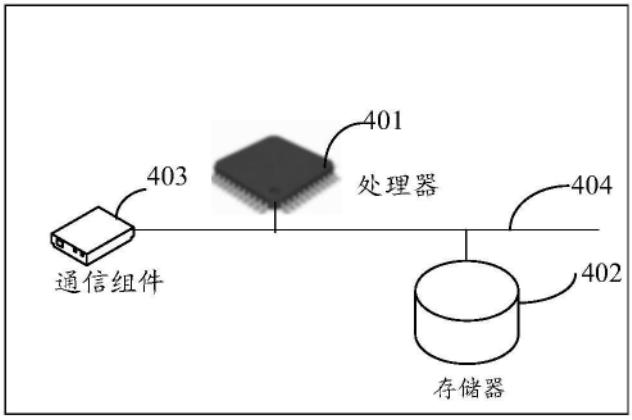

401
处理器
403
通信组件
404
402
存储器

图4