(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 109104441 A
(43)申请公布日 2018.12.28

(21)申请号 201811244932.5

(22)申请日 2018.10.24

(71)申请人 上海交通大学
地址 200240 上海市闵行区东川路800号

(72)发明人 邹福泰 许文亮 马志远 高逸飞 李林森

(74)专利代理机构 上海旭诚知识产权代理有限公司 31220
代理人 郑立

(51)Int.Cl.
*H04L 29/06*(2006.01)

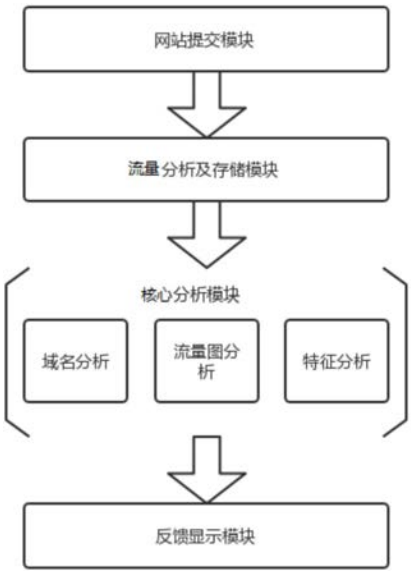
权利要求书2页 说明书4页 附图2页

(54)发明名称

一种基于深度学习的加密恶意流量的检测系统和方法

(57)摘要

本发明公开了一种基于深度学习的加密恶意流量的检测系统和方法,涉及计算机网络安全领域,包括网站提交模块,流量分析及存储模块,核心分析模块,反馈显示模块。流量分析软件对PCAP包进行分析得到日志文件,然后对这些日志文件根据IP地址进行聚合;对于聚合出的一条流进行特征提取、流量图制作,以及域名的提取;使用xgboost、word2vec+LSTM、CNN产生识别模型,进行组合后实现最终判断。本发明在不需要知道解密后流量内容的情况下,就能对流量的恶意与否进行判断,从而对加密恶意流量进行分析。




CN 109104441 A

1.一种基于深度学习的加密恶意流量的检测系统,其特征在于,包括

网站提交模块:用以在自建服务器上接受用户所上传的流量PCAP包;

流量分析及存储模块:使用流量分析软件对所述网站提交模块的所述流量PCAP包进行分析,将分析结果存为日志文件;

核心分析模块:对所述流量分析及存储模块的日志文件进行数据预处理,然后使用识别模型进行识别,最终组合模型结果,产生最终识别结果;

反馈显示模块:收到所述核心分析模块产生的最终识别结果,判断是否检测到恶意流量,如果检测为非恶意流量,告知用户该流量包不存在恶意流量;如果检测为恶意流量,提取出恶意流量的域名信息,并根据白名单再次过滤,得到最终流量的信息,并显示给用户。

2.如权利要求1所述的基于深度学习的加密恶意流量的检测系统,其特征在于,所述流量分析软件为BRO。

3.如权利要求1或2所述的基于深度学习的加密恶意流量的检测系统,其特征在于,所述流量分析及存储模块包括事件引擎,所述事件引擎将传入的数据包流减少为一系列更高级别的事件,并保存为日志文件。

4.如权利要求3所述的基于深度学习的加密恶意流量的检测系统,其特征在于,所述流量分析及存储模块还包括脚本解释器,脚本解释器执行事件处理程序处理从事件引擎得到的事件。

5.如权利要求1所述的基于深度学习的加密恶意流量的检测系统,其特征在于,所述预处理包括特征分析、流量图分析,以及域名分析;所述识别模型包括xgboost模型、word2vec+LSTM模型、CNN模型。

6.如权利要求1所述的基于深度学习的加密恶意流量的检测系统,其特征在于,所述最终流量的信息包括IP地址以及域名。

7.一种基于深度学习的加密恶意流量的检测方法,其特征在于,所述方法包括以下步骤:

101、基于已有的加密流量数据,通过流量分析软件进行分析,获得日志文件,通过一些字段进行连接,获得一系列的聚合数据;

102、从所述聚合数据中提取一系列的特征数据;

103、利用xgboost算法,对所述特征数据进行训练,获得第一模型;

104、对于每条流量聚合,对于所有的域名,利用word2vec训练出一个词向量转换模型,然后转换成词向量矩阵;

105、将域名转换成词向量矩阵后,用LSTM进行训练,获得第二模型;

106、利用数据包的payload中的特征,构建流量图,获得第三模型;

107、将所述第一模型、所述第二模型、所述第三模型,以不同比例进行加权,获得最终的恶意流量概率;

108、当有用户上传PCAP包时,利用BRO软件对其进行分析,提取其中的特征,根据第一模型、第二模型、第三模型的组合模型对加密流量包进行判断,将结果返回用户。

8.如权利要求7所述的基于深度学习的加密恶意流量的检测方法,其特征在于,所述流量分析软件为BRO。

9.如权利要求7所述的基于深度学习的加密恶意流量的检测方法,其特征在于,所述特

征数据包括连接的持续时间,平均每个传入、传出包的字节数,普通连接和SSL连接的相对比例,证书的有效均值。

10.如权利要求7所述的基于深度学习的加密恶意流量的检测方法,其特征在于,所述步骤106中的特征包括源IP发送字节数,目的IP发送的字节数,源IP发送的数据包个数,目的IP发送的数据包个数,源IP发送IP层字节数,目的IP发送IP层字节数。

# 一种基于深度学习的加密恶意流量的检测系统和方法

## 技术领域

[0001] 本发明涉及计算机网络安全领域，尤其涉及一种基于深度学习的加密恶意流量的检测系统和方法。

## 背景技术

[0002] SSL安全套接层协议提供应用层和传输层之间的数据安全性机制，在客户端和服务器之间建立安全通道，对数据进行加密和隐藏，确保数据在传输过程中不被改变[1]。SSL协议在应用层协议通信之前就已经完成加密算法和密钥的协商，在此之后所传送的数据都会被加密，从而保证通信的私密性。

[0003] HTTPS加密恶意流量就是在流量传输时使用了SSL加密协议，躲避普通的流量分析技术，为加密流量检测带来新的挑战。而现有的恶意流量检测技术大都要对流量有效载荷内容进行分析，那么对于加密的流量需要先解密再进行分析，但很多时候都没有足够的条件可以对加密恶意流量进行解密，这种方法的实际应用价值不高。所以近年来逐渐出现了基于机器学习的分析方法。

[0004] 因此，本领域的技术人员致力于开发一种基于深度学习的加密恶意流量的检测系统和方法。

## 发明内容

[0005] 有鉴于现有技术的上述缺陷，本发明所要解决的技术问题是在不需要知道解密后流量内容的情况下，对流量的恶意与否进行判断。

[0006] 为实现上述目的，本发明提供了一种基于深度学习的加密恶意流量的检测系统和方法。在不需要知道解密后流量内容的情况下，就能对流量的恶意与否进行判断，使用流量分析软件对PCAP(Process Characterization Analysis Package，过程特性分析软件包)包进行分析得到日志文件，然后对这些日志文件根据IP地址进行聚合。对于聚合出的一条流，进行特征提取、流量图制作，以及域名的提取，使用xgboost、word2vec+LSTM、CNN产生共三种识别模型，进行组合后实现最终判断，得出最后的结果。本发明不仅判断PCAP包是否还有恶意流量，还会从中判断出恶意的IP地址及其域名(如果存在)。

[0007] xgboost实现的是一种通用的Tree Boosting算法，此算法的一个代表为梯度提升决策树。这是一种增强算法，构建T棵回归树，当构建第t棵树时，对前t-1棵树训练样本分类回归产生的残差进行拟合。每次拟合产生新树时，遍历可能的树，选择使目标函数最小的树。

[0008] LSTM(Long Short-Term Memory，长短时记忆网络)最早由Sepp Hochreiter和Jürgen Schmidhuber于1997年提出，是RNN(Recurrent neural Network，循环神经网络)的一种特殊类型，可以学习长期依赖信息。LSTM通过增加输入门限，遗忘门限和输出门限，使得自循环的权重是变化的，这样一来在模型参数固定的情况下，不同时刻的积分尺度可以动态改变，从而避免了梯度消失或者梯度膨胀的问题。

[0009] 卷积神经网络(Convolutional Neural Network,CNN)是一种前馈神经网络,它的人工神经元可以响应一部分覆盖范围内的周围单元。CNN的基本结构一般由输入层、卷积层(convolutional layer)、池化层(pooling layer,也称为下采样层)、全连接层及输出层构成。

[0010] 在本发明的较佳实施方式中,提供了一种基于深度学习的加密恶意流量的检测系统包括以下模块:

[0011] 1)网站提交模块:用以在自建服务器上接受用户所上传的流量PCAP包;

[0012] 2)流量分析及存储模块:使用流量分析软件对用户提交的PCAP包进行分析,将分析结果存为日志文件;

[0013] 3)核心分析模块:对流量分析及存储模块的日志文件进行数据预处理,然后使用识别模型进行识别,最终组合模型结果,产生最终识别结果;

[0014] 4)反馈显示模块:收到核心分析模块产生的最终识别结果,判断是否检测到恶意流量,如果检测为非恶意流量,则告知用户该流量包不存在恶意流量;否则提取出恶意流量的域名信息,并根据白名单再次过滤,得到最终流量的信息,并显示给用户。

[0015] 进一步地,流量分析及存储模块使用的流量分析软件为BRO,BRO是一个开源功能强大的流量分析工具;

[0016] 进一步地,流量分析及存储模块包括事件引擎(或核心),事件引擎将传入的数据包流减少为一系列更高级别的事件,并保存为日志文件。

[0017] 进一步地,流量分析及存储模块还包括脚本解释器,脚本解释器执行事件处理程序处理从事件引擎得到的事件。

[0018] 进一步地,流量分析及存储模块还包括脚本解释器,事件处理程序使用BRO的自定义脚本语言编写。

[0019] 进一步地,核心分析模块的数据预处理,包括特征分析、流量图分析,以及域名分析。

[0020] 进一步地,核心分析模块使用的识别模型包括xgboost模型、word2vec+LSTM模型、CNN模型。

[0021] 进一步地,反馈显示模块展示的最终流量的信息包括IP地址以及域名(server name)。

[0022] 在本发明的另一较佳实施方式中,提供了一种基于深度学习的加密恶意流量的检测方法,包括以下步骤:

[0023] 101、基于已有的加密流量数据,通过流量分析软件进行分析,获得三个日志文件,通过一些字段进行连接,获得一系列的聚合数据;

[0024] 102、从上述的聚合数据中提取一系列的特征数据;

[0025] 103、利用xgboost(eXtreme Gradient Boosting)算法,对102中的特征数据进行训练,获得第一模型;

[0026] 104、对于每条流量聚合,对于所有的server name,利用word2vec训练出一个词向量转换模型,然后转换成词向量矩阵;

[0027] 105、将server name转换成词向量矩阵后,用LSTM进行训练,获得第二模型;

[0028] 106、利用数据包的payload中的特征,构建流量图,获得第三模型;

[0029] 107、将获得的第一模型、第二模型、第三模型，以不同比例进行加权，获得最终的恶意流量概率；

[0030] 108、当有用户上传PCAP包时，利用BRO软件对其进行分析，提取其中的特征，根据第一模型、第二模型、第三模型的组合模型对加密流量包进行判断，将结果返回用户。

[0031] 进一步地，步骤101中的流量分析软件为BRO。

[0032] 进一步地，步骤101中的日志文件为conn.log，ssl.log，x509.log。

[0033] 进一步地，步骤102中的特征数据包括连接的持续时间，平均每个传入、传出包的字节数，普通连接和SSL连接的相对比例，证书的有效均值。

[0034] 进一步地，步骤106中的特征包括源IP发送字节数，目的IP发送的字节数，源IP发送的数据包个数，目的IP发送的数据包个数，源IP发送IP层字节数，目的IP发送IP层字节数。

[0035] 本发明提供了一种基于深度学习的加密恶意流量的检测系统和方法，在不需要知道解密后流量内容的情况下，就能对流量的恶意与否进行判断，从而对加密恶意流量进行分析。

[0036] 以下将结合附图对本发明的构思、具体结构及产生的技术效果作进一步说明，以充分地了解本发明的目的、特征和效果。

## 附图说明

[0037] 图1是本发明的一个较佳实施例的组成和流程示意图；

[0038] 图2是本发明的一个较佳实施例的流量分析和存储模块工作过程示意图；

[0039] 图3是本发明的一个较佳实施例的核心分析模块流程图；

[0040] 图4是本发明的一个较佳实施例的反馈显示模块流程图。

## 具体实施方式

[0041] 以下参考说明书附图介绍本发明的多个优选实施例，使其技术内容更加清楚和便于理解。本发明可以通过许多不同形式的实施例来得以体现，本发明的保护范围并非仅限于文中提到的实施例。

[0042] 在附图中，结构相同的部件以相同数字标号表示，各处结构或功能相似的组件以相似数字标号表示。附图所示的每一组件的尺寸和厚度是任意示出的，本发明并没有限定每个组件的尺寸和厚度。为了使图示更清晰，附图中有些地方适当夸大了部件的厚度。

[0043] 如图1所示，本实施例包括以下模块：

[0044] 1)网站提交模块：用以在自建服务器上接受用户所上传的流量PCAP包；

[0045] 2)流量分析及存储模块：使用BRO软件对用户提交的PCAP包进行分析，将分析结果存为日志文件；

[0046] 3)核心分析模块：对流量分析及存储模块的日志文件进行数据预处理，然后使用识别模型进行识别，最终组合模型结果，产生最终识别结果；

[0047] 4)反馈显示模块：收到核心分析模块产生的最终识别结果，判断是否检测到恶意流量，如果为非恶意流量，则告知用户该流量包不存在恶意流量；否则提取出恶意流量的域名信息，并根据白名单再次过滤，得到最终流量的信息，并显示给用户。

[0048] 如图2所示，流量分析及存储模块包括事件引擎(或核心)和脚本解释器，事件引擎将传入的数据包流减少为一系列更高级别的事件，并保存为日志文件；脚本解释器，脚本解释器执行一组用BRO的自定义脚本语言编写的事件处理程序，也就是用于处理从事件引擎得到的事件。

[0049] 如图3所示，核心分析模块对流量分析及存储模块的日志文件进行数据预处理，包括特征分析、流量图分析，以及域名分析。

[0050] 如图4所示，反馈显示模块收到核心分析模块产生的最终识别结果，判断是否检测到恶意流量，如果为检测到恶意流量，则告知用户该流量包不存在恶意流量；否则提取出恶意流量的域名信息，并根据白名单再次过滤，得到最终流量的信息，包括IP地址以及域名(server name)，并展示给用户

[0051] 在本发明的另一较佳实施方式中，提供了一种基于深度学习的加密恶意流量的检测方法，包括以下步骤：

[0052] 101、基于已有的加密流量数据，通过BRO软件进行分析，获得三个日志文件为conn.log，ssl.log，x509.log，通过一些字段进行连接，获得一系列的聚合数据；

[0053] 102、从上述的聚合数据中提取一系列的特征数据，包括连接的持续时间，平均每个传入、传出包的字节数，普通连接和SSL连接的相对比例，证书的有效均值；

[0054] 103、利用xgboost算法，对102中的特征数据进行训练，获得第一模型；

[0055] 104、对于每条流量聚合，对于所有的server name，利用word2vec训练出一个词向量转换模型，然后转换成词向量矩阵；

[0056] 105、将server name转换成词向量矩阵后，用LSTM进行训练，获得第二模型；

[0057] 106、利用数据包的payload中的特征，包括源IP发送字节数，目的IP发送的字节数，源IP发送的数据包个数，目的IP发送的数据包个数，源IP发送IP层字节数，目的IP发送IP层字节数，构建流量图，获得第三模型；

[0058] 107、将获得的第一模型、第二模型、第三模型，以不同比例进行加权，获得最终的恶意流量概率；

[0059] 108、当有用户上传PCAP包时，利用BRO软件对其进行分析，提取其中的特征，根据第一模型、第二模型、第三模型的组合模型对加密流量包进行判断，将结果返回用户。

[0060] 以上详细描述了本发明的较佳具体实施例。应当理解，本领域的普通技术无需创造性劳动就可以根据本发明的构思作出诸多修改和变化。因此，凡本技术领域中技术人员依本发明的构思在现有技术的基础上通过逻辑分析、推理或者有限的实验可以得到的技术方案，皆应在由权利要求书所确定的保护范围内。

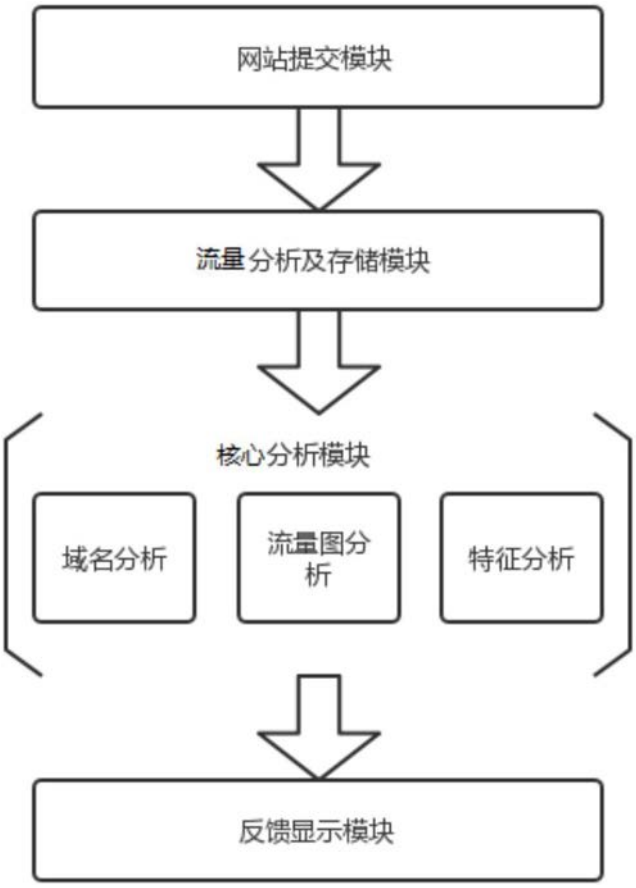

网站提交模块
流量分析及存储模块
核心分析模块
域名分析
流量图分析
特征分析
反馈显示模块

图1

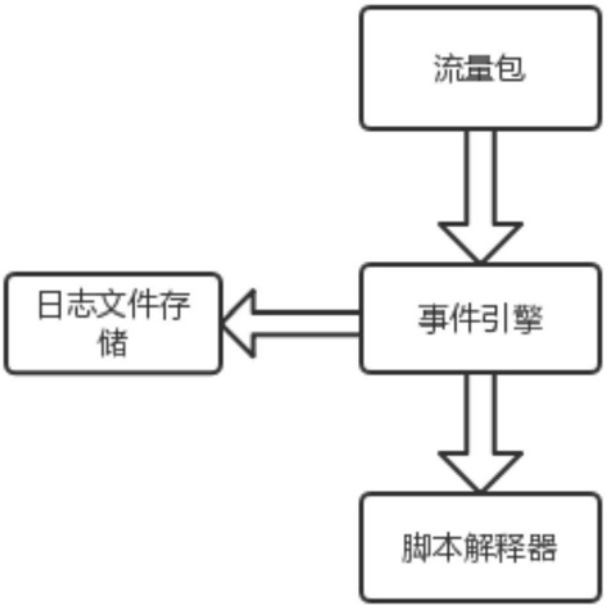

流量包
日志文件存储
事件引擎
脚本解释器

图2

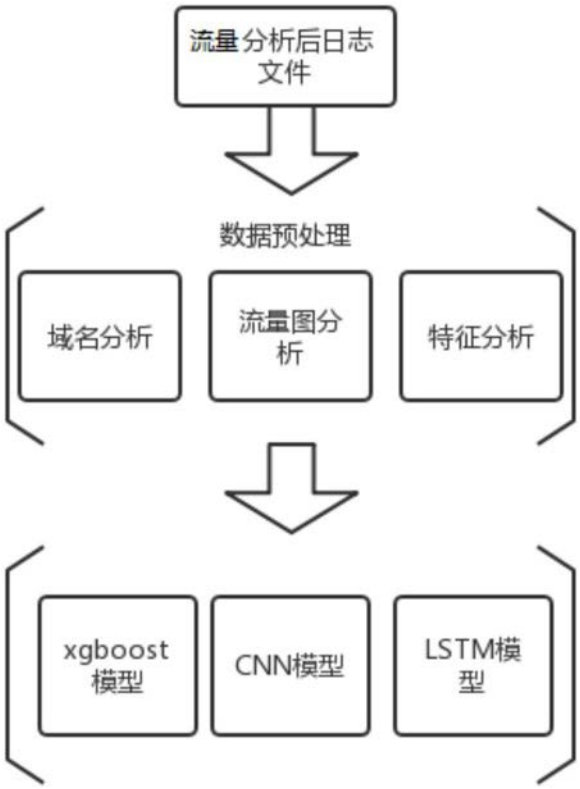

流量分析后日志文件
数据预处理
域名分析
流量图分析
特征分析
xgboost模型
CNN模型
LSTM模型

图3

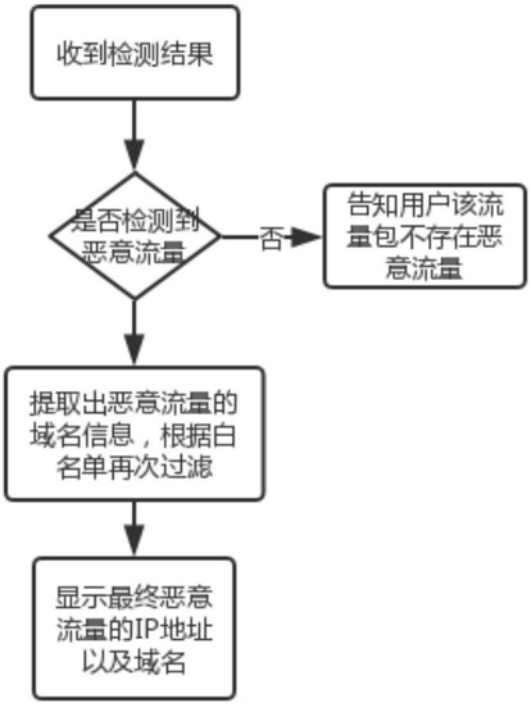

收到检测结果
是否检测到恶意流量
否
告知用户该流量包不存在恶意流量
提取出恶意流量的域名信息，根据白名单再次过滤
显示最终恶意流量的IP地址以及域名

图4