# 基于改进 BP 算法的 DNS 图挖掘恶意域名检测方法

马 骁, 蔡满春, 芦天亮
(中国人民公安大学信息网络安全学院, 北京 102600)

**摘 要** 广泛的恶意活动依赖 DNS 来管理其受感染计算机的大型分布式网络,目前,主要的恶意域名检测方法是基于 DNS 相关的局部域特征构建分类器,但这样做存在着一些无法克服的弊端,如攻击者可以在不影响其攻击能力的情况下改变域名模式和时态模式等特性来逃避检测,从而导致这些方法所依赖的特征不稳定。因此,利用攻击者总是循环利用资源,频繁更改域名-IP 解析,并创建新的域名来避免被检测这一特点,从所有域的查询历史回溯的标记域来验证和找出它们之间的关联,图是代表这种关系的最佳候选,有许多基于图开发的算法都具有高性能。我们以域名和主机 ip 为数据源构建 DNS 图,挖掘域和主机 ip 之间的内在关系,并基于置信传播算法(BP 算法)的思想提出了一种计算图中每个节点信誉评分的算法,节点显示出的信誉分数越高,推断出的恶意概率就越高。为了证明方法的有效性,利用恶意域检测技术,并在从 DNS 数据服务器中收集的真实数据集上进行了评估。

**关键词** 恶意域名检测; 置信传播算法; 图挖掘; DNS; 被动数据
**中图分类号** TP393.08 **文献标志码** A

# Detection Method of Malicious Domain by DNS Graph Mining Based on Improved BP Algorithm

MA Xiao, CAI Manchun, LU Tianliang
(School of Information and Cyber Security, People's Public Security University of China, Beijing 102600, China)

**Abstract:** Extensive malicious activity relies on DNS to manage large distributed networks of its infected computers. Currently, the main malicious domain detection method is building classifiers based on DNS-related local domain features. However, this method has some insurmountable drawbacks. For example, attackers can evade detection by changing features like domain patterns and temporal patterns without affecting their attack capabilities, which leads to feature instability. The attackers always recycle resources, frequently change domain-IP parsing and create new domain names to avoid detecting. By using these features, their associations are verified and identified from labeled domains which are backtracked from query history across all domains. Graphs are the best candidate to represent this relationship, and many graph-based algorithms have high performance. In this paper, DNS graphs were constructed by using the domain name and host ip as the data source. The intrinsic relationship between the domain and host ip were also excavated. And an algorithm was established to calculate the credit score of each node in the graph, which was based on the idea of the confidence propagation algorithm (BP algorithm). The higher the credit score displayed by the nodes, the higher the probability of inferred malice. By using malicious

**收稿日期** 2021-10-15
**基金项目** "十三五"国家重点课题(MMJJ20180108);中国人民公安大学 2019 年基本科研业务费重大项目(2019JKF108)。
**作者简介** 马骁(1997—),男,山东人,在读硕士研究生。研究方向为信息网络安全。
**通信作者** 蔡满春(1972—),男,博士,副教授。E-mail: caimanchun@ppsuc.edu.cn

domain detection method, real datasets were collected from the DNS data server to evaluate the effectiveness of this method.

**Key words:** malicious domain detection; belief propagation algorithm; graph mining; DNS; passive data

## 0　引言

恶意域名为近来网络攻击者所使用的主要手段,它也是互联网资源 URL 的重要组成部分[1],互联网设置及其相关管理政策中很少有漏洞允许这些恶意域名在 DNS 服务器上注册。虽然黑名单可以简单、快速识别此类恶意域名,但该技术无法满足域名生成和注册对速度的要求[2]。

前人在研究中已经开始使用 DNS 数据的特征,一般方法从 DNS 记录、查询和响应中提取多个特征,并进一步利用历史模式和本地主机的网络流量特征来增强这些特征,基于这些特征和一些训练数据集,可以建立一个分类器来区分恶意域和良性域[3-4]。但这不仅需要识别更多相关的特征,并且这些所依赖的特征稳定性不强,攻击者可以很轻易地改变这些特征,使分类器无法检测出来,其根本原因是现有的研究中所依赖的许多特性都是关于单个域或主机的本地特性。已经有很多检测恶意域名相关研究。在此,将简要讨论与本研究方法最相关的代表性工作。

Notos[5] 是使用被动 DNS 数据识别恶意域名的先驱。Notos 基于从 DNS 查询中提取的特征动态分配未知域的声誉分数。Expose[6] 遵循类似的方法,并克服了 Notos 的一些限制(例如,Expose 需要更少的训练时间和更少的训练数据)。此外,Expose 的不同之处在于它不知道恶意域提供的服务类型(例如,僵尸网络、钓鱼、快速流动)。本研究通过关注在 ip 上部署恶意域的全局拓扑,而不是其本地特性,是对 Expose 和 Notos 的补充。当 Expose 和 Notos 能够访问单个 DNS 查询时,它们的检测性能最好,这可能是相当敏感的。本研究方法同时适用于公共聚合的被动 DNS 数据,因此不会引起隐私问题。

Rahbarinia[7] 等人提出了一种基于行为的技术来跟踪恶意软件控制的域。其主要思想是从 DNS 查询日志中提取超出二部主机域图的用户行为模式。相反,本研究使用的技术利用的是被动 DNS 数据,而不是用户 DNS 查询行为,Rahbarinia 所使用的特性不适用于本研究的被动 DNS 数据。

Pratyusa K. Manadhata[8] 等人提出通过分析 DNS 查询日志来识别恶意域。其主要技术是建立一个二部主域图(由主机查询哪些域),然后根据已知的恶意域和良性域,应用置信传播来发现恶意域。其原理是: 如果主机查询一个恶意域名,该主机很有可能被恶意域携带的病毒感染,同样被感染主机查询的域名更有可能是恶意的。被动 DNS 数据也可以被建模为二部图,通过在被动 DNS 数据上应用信念传播来识别恶意域似乎很有说服力。然而,研究发现推理直觉虽然在主机域图中工作得很好,但在被动 DNS 数据中推理直觉却不能很好地发挥作用。与主机域图相比,域解析图具有以下几方面优势: 首先,被动 DNS 数据是在全局收集数据,提供了域和 ip 之间映射的更全面的视图,而主机域图通常仅限于单个企业或 ISP 的视角; 其次,主机域图包含关于单个用户敏感的私有信息,分享这些信息可能会引起严重的隐私问题; 再者,域解析图是域 ip 映射的聚合信息,而不涉及个人的信息,是可以公开共享的。

B. Guan[9] 等人设计了一种对域名恶意概率评分的方法。他使用被动 DNS 数据来构建一个域解析图,并在此基础上,构建了未知域到恶意域的任意路径,给出了未知域恶意概率评分的数学公式。该方法对小标记数据非常灵活,它只关心是否存在从域到恶意的路径,并基于该路经计算恶意分数。与该方法相比,本研究通过对 BP 算法进行改进,使检测方式更加灵活。DNS 图中节点之间的关联是通过 DNS 数据建立的,并依赖所有节点之间的关联来计算信誉评分,以此判断图中每个节点是否合法。

已有的研究虽然也涉及到被动 DNS 数据,但本文提出的检测方法与前人所不同的是 DNS 图中节点之间的关联是通过 DNS 数据建立的,并依赖所有节点之间的关联来计算信誉评分,从而判断图中每个节点是否合法。并且该方法也是基于域分辨率图的,考虑到马尔可夫随机场(MRF),我们采用了一个新的置信传播算法来获得域的恶意评分。

通过对 BP 算法的改进,并使用精确率(也称查准率)、召回率(也称查全率)、正确率、F-measure 和

ROC 曲线下面积( AUC) 来衡量该方法的有效性,精确率、召回率和正确率均超过 95%,F-measure 和 AUC 也展示出良好的结果。在实验操作中,以域名和主机 ip 为数据源构建 DNS 图,挖掘域和主机 ip 之间的内在关系,并基于 BP 算法的思想开发了一种基于同质化关系计算图中每个节点信誉评分的算法。

## 1　可用于图挖掘的 BP 算法

在信息产业如此发达的今天,用户产生了大量的数据,这些数据包含有许多信息,为了从数据中提取有价值的信息,数据挖掘应运而生,而图挖掘正是数据挖掘的重要组成部分,图挖掘是指通过图模型的方法来提取数据。

被动 DNS 通过复制用户在其 DNS 基础设施中自愿部署的传感器捕获服务器间的 DNS 消息,并将捕获的 DNS 消息进一步处理,然后存储在一个中央 DNS 记录数据库,就可以对其进行各种查询,它提供了域和 ip 之间映射的全面视图[10]。我们使用网站的 API 从 www. dnsdb. info 下载了被动 DNS 数据库,被动 DNS 数据包含了 DNS 不同方面的丰富信息,本文主要分析 DNS 数据中的 A 记录,仅使用( d, ip) 两列[11]。d 为域名,解析为 ip。尽管 DNS 记录的许多特征都可以被它所属的域名进行改变,但攻击者必须在其控制或访问的 ip 上托管恶意域名。此外,一些恶意域名经常采用逃避检测策略,如频繁创建新域名、更换域名等措施,使其动态特征存在于恶意域名组之间,而不是单个域名[12]之中。实际上恶意域名正在随着时间的推移在互联网空间中大量移动,同时在移动的过程中共享一些不同的特性。因此,很有可能多个恶意域名最终被托管在同一个 ip 上,同样也有可能多个 ip 被用来托管同一个恶意域名,这在它们之间创建了内在的关联。为了消除这种关联,攻击者必须尽量减少托管恶意域的 ip 数量以及每个 ip 所托管的恶意域的数量。而要做到这一点,攻击者则会付出极高的成本代价,并限制自身对可用资源的利用。因此,我们认为域名和 ip 之间的关联为研究攻击者如何组织和部署恶意资源提供了一个可靠稳定的方法,这可以进一步用于图的构建。所构建的图是一个二部图,一边对应域,另一边对应 ip,如图 1 所示,它只有域名与 ip 的连接。如果存在 A 记录中存在( d,ip) 两列,则从域 d 到 ip 形成一条边,在图 1 中由箭头表示。

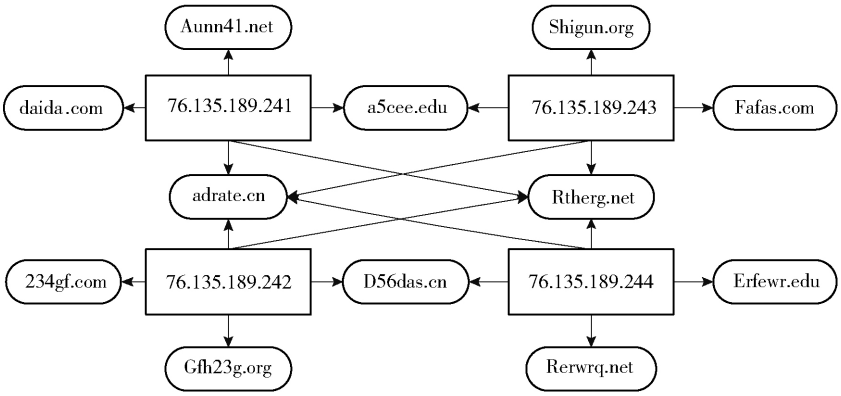


**图 1　域名解析图**

置信传播算法( Belief propagation, BP) 也被称为和积消息传递[13],像贝叶斯网络和马尔可夫随机场都是对图形模型( GM) 执行推理的消息传递算法,以任何观察到的节点为条件来计算每个未观察到的节点的边缘分布。置信传播算法是人工智能和信息理论中常用的方法,并在许多应用中得到应用[14-15]。

作为马尔可夫随机场模型的基础,BP 算法最重要的元素之一是马尔可夫特性。BP 算法依赖于图上节点的交互,当 BP 在图上运行时,消息在任意两个相邻节点之间按照马尔可夫性质进行交互。因此,在解释所提算法的操作之前,首先简单地讨论一下马尔可夫随机场。

马尔可夫随机场( MRF) 是一组具有马尔可夫性质的随机变量,由无向图描述。无向图 $G=(V,E)$,其中 $V=v_1,v_2,\cdots,v_n$ 是顶点集合。每个顶点对应一个随机变量[16],因为它具有马尔可夫性质,因此它只依赖于其相邻节点的性质。给定一个节点 $v_i\in V$,$N_i$ 是节点 $v_i$ 的邻居集,如果 $(v_i,v_j)\in E$,且 $v_j\in N_i$,则节点 $v_i$ 是节点 $N_i$ 的邻集。那么 MRF 符合局部属性:

$$P(v_i \mid v_{j v_j \in V/v_i}) = P(v_i \mid v_{j v_j \in N_i}) \quad (1)$$

将 MRF 模型的上述特性应用到 DNS 图中，DNS 图的每个顶点对应一个随机变量，该随机变量代表主机 ip 或域名的随机变量[17]。然后，为了检测恶意域，定义一个知识集为 $D = (d_l, d_m)$，其中 $v_i = d_l$ 表示该主机 ip 或域是合法的，其余表示该主机 ip 或域是恶意的。

## 2　用于 DNS 图挖掘恶意域名检测的 BP 算法改进

本研究提出的方法承继了 BP 算法的所有特性，并添加了一些条件来优化操作，提高算法的性能以获得最终结果。该算法允许图中的每个节点通过传递消息作为证据与其邻域进行交互，以评估其邻域的标签。算法开始时，给图上的每个节点 $v_i$ 赋初始值为恶意概率，标记为函数 $F_i(v_i)$。节点的 $f_{ji}(v_i, v_j) = P(v_i \mid v_j)$，即节点 $v_j$ 具有标记 $v_j$ 时，$v_i$ 具有 $v_i$ 的概率。因为图是无向的，所以相邻两个节点的势函数是对称的，即 $f_{ji}(v_i, v_j) = f_{ji}(v_j, v_i)$，如表 1 所示:

表 1　两个节点之间的推断表

| $f_{ij}(v_i, v_j)$ | $v_i$ = legitimate | $v_i$ = malicious |
|---|---|---|
| $v_j$ = legitimate | $0.5 + e$ | $0.5 - e$ |
| $v_j$ = malicious | $0.5 - e$ | $0.5 + e$ |

其中 $0 < e < 0.5$，由表 1 可知，合法节点的相邻节点很大概率是合法的。恶意节点的邻近节点被恶意攻击的可能性也更大。在实验中，$e$ 的值通常为 0.1。

该算法的原理是基于消息传递，一个消息从 $v_i$ 发送到 $v_j$，问节点 $v_i$ 如何看待它邻居的标签。消息从 $v_i$ 传递到 $v_j$ 标记为 $m_{ij}(x_i)$，如图 2 所示。对于 $\forall e_{ji} \in E$，将消息 $m_{ij}(v_i)$ 和 $m_{ji}(v_j)$ 按以下公式计算，计算节点 $v_i$ 到节点 $v_j$ 的消息:

$$m_{ij}^t(v_j) = F_i(v_i) f_{ij}(v_i, v_j) \prod_{p \in N_i/j} m_{pi}^{t-1}(v_i) \quad (2)$$

如公式(2)所示，当节点 $v_i$ 希望向节点 $v_j$ 发送消息时，必须先收集其相邻节点的所有消息，然后再向节点 $v_j$ 发送消息。在 BP 方法中，所有节点都实时地将自己的想法发送给它们的邻居，但没有必要这样做，因为并不是图上的所有节点都有知识可以发送给它的邻居。例如在第一次交互中，只有知识节点可以向它的邻居发送消息，告诉他们如何看待自己的恶意概率，因为所有剩余的节点的恶意概率都是 0.5，告诉它的邻居的恶意概率是没有意义的。所以我们设置一条规则，只有节点的恶意概率不等于 0.5 时才发送消息。加入算法的第二条规则是考虑知识节点的恶意概率。在每次交互中，知识节点的概率不应该再次计算，因为它的标签是已知的，无论它的邻居怎么想它都不能改变。

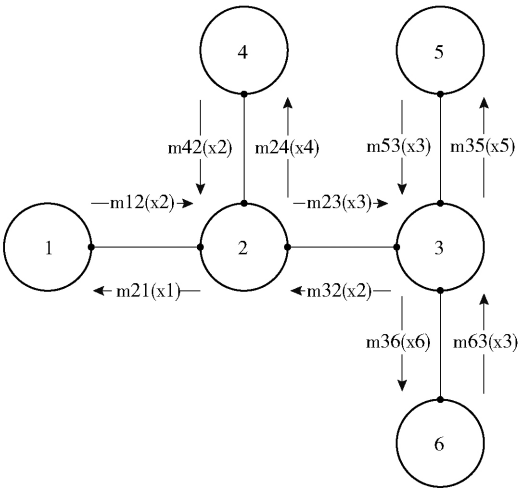


图 2　信息间的传递

根据 BP 算法，每次交互后都会计算每个节点的恶意概率，称之为“置信”，记为 $b_i(v_i)$。其中 $N_i$ 是 $v_i$ 的邻居节点集，$m_{pi}^{t-1}(v_i)$ 是 $v_i$ 在最后一次交互中接收到的所有消息。在每次迭代中，顶点的置信计算基于从邻居处接收到的消息，具体为:

$$b_i(v_i) = \frac{1}{Z_i} F_i(v_i) f_{ij}(v_i, v_j) \prod_{p \in N_i/j} m_{p_i}^{t-1}(v_i) \quad (3)$$

$Z_i$ 是归一化常数，顶点每个标签上的信念之和应为 1。这两个公式都是 BP 算法的原始公式，但在实现过程中会将前面提到的两种规则结合起来，并对公式进行一定的改变。现在，邻居 $N_i^*$ 定义了一个条件，它是节点 $i$ 的邻居，先前的置信不等于 0.5。因此，公式可以写成:

$$m_{ij}^t(v_j) = F_i(v_i) f_{ij}(v_i, v_j) \prod_{p \in N_i^*/j} m_{pi}^{t-1}(v_i) \quad (4)$$

$$b_i(v_i) = \frac{1}{Z_i} F_i(v_i) f_{ij}(v_i, v_j) \prod_{p \in N_i^*/j} m_{p_i}^{t-1}(v_i) \quad (5)$$

消息传递操作将遵循两套规则和由一些顶点的先验知识所组成的最初的置信，然后消息不断迭代，直至顶点的信念收敛(变异小于某一阈值)或算法迭代运行时间达到了极限。

## 3　实验

### 3.1　实验准备

通过在 www.alexa.com、Bambenek Consulting

( https: // osint. bambenekconsulting. com/feeds/) 和 360 网络安全实验室( https: //data. netlab. 360. com/dga/) 上可以收集到实验所需的十万个良性域名和十万个恶意域名。将这些域名分为两组,一组用于训练模型,一组用于实验。

实验所用来构建 DNS 图的数据从 DNS 数据服务器中收集,被动 DNS 数据包括域名系统不同方面的丰富信息,本文主要分析域名系统数据中 A 记录的域名和 ip 数据。由于 Graphlab 上的几乎所有功能都是并行运行的,可以快速高效地得到结果和数据,所有的处理都是在 Graphlab 上远程完成的。Graphlab 在处理对象之间关系数据时表现出良好的性能。虽然实现起来相当复杂,但对于某些网络问题来说,它要优于其他的方法。

首先对无知识的子图进行处理,DNS 图中并不是所有节点都可以连接在一起成为大图,因而 DNS 图中存在大量的子图,而有些子图对恶意域和合法域一无所知,从而不能计算出恶意评分,所以,将他们从构建的图表中删除。其次,实验通过直接与 BP 算法交互来提高算法性能的结果,BP 算法的主要思想是在接收到邻居节点的消息后,改变图上所有节点的概率。但恶意节点或白节点是已知的,其概率不应改变,因此,在实验中,知识节点的概率固定为初始值。通过进行对比实验,将改进 BP 算法与标签传播算法[18] 以及通过被动 DNS 数据图分析发现恶意域名的方法进行比较,说明改进方法的有效性。

从图上所有顶点和边的初始值开始,该算法将挖掘出的图与已知的部分图一起进行处理,从而判断其恶意或合法。这被称为先验知识,恶意节点的初始声誉得分为 0. 99,合法节点为 0. 01。所有其他节点为未知标签,它的声誉评分为 0. 5。在所有边中,一个常数值表示两个相邻节点的关系,如表 1 所示。BP 算法将在具有上述初始值的图上进行挖掘,并运行至满足某个阈值或达到交互次数的限制为止。但在实验过程中阈值固定设置为 0. 005,对于任何子图,所有节点的消息传递将以最大 10 次进行交互。收敛条件设为:

$$\max_{(v_i \in V)} | b_i^t(v_i) - b_i^{t-1}(v_i) | \leqslant 0.005 \qquad (6)$$

### 3. 2　实验结果

通过使用精确率( 也称查准率) 、召回率( 也称查全率) 、正确率、F-measure 和 ROC 曲线下面积( AUC) 来衡量改进 BP 算法的有效性,准确度是通过得到模型正确识别的个体数与识别出来的个体总数之比来反应其正确率; 召回率是正确识别的个体总数与测试集中存在的个体总数之比; F-measure 值是精确度和召回率的调和平均值; ROC 通过预测正例排在负例前面的概率来衡量二分类模型优劣程度。

为了证明本研究提出的改进方法在性能上的优越性,将改进的 BP 算法与标签传播算法[18] ( Label Propagation Algorithm) 以及基于被动 DNS 数据图分析检测恶意域名[19] 进行对照,与处理此数据的步骤相同,也是在 Graphlab 中完成操作。LPA 是基于图的半监督学习方法,它的思路是基于标记的节点信息去预测未标记的节点信息。对照结果如下所示,其中图 3 是 3 种算法的 ROC 曲线,图 4 是 3 种算法的 P-R 曲线,表 2 为 3 种算法的性能对照。

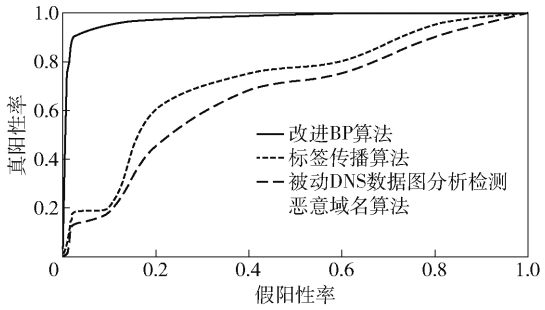


图 3　3 种方法的 ROC 曲线

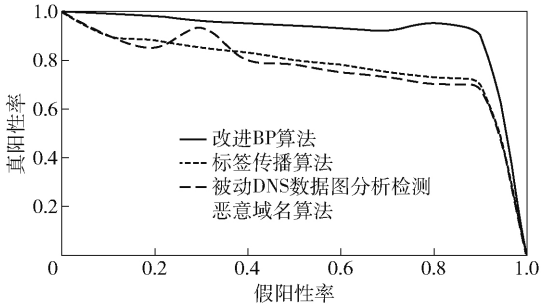


图 4　3 种方法的 P-R 曲线

表 2　3 种方法的性能对照

| 方法 | 精确率/% | 召回率/% | 正确率/% | F-measure | AUC |
|---|---|---|---|---|---|
| 改进的 BP 算法 | 99. 4 | 98. 8 | 98. 5 | 0. 991 | 0. 983 |
| 标签传播算法 | 79. 9 | 77. 6 | 75. 2 | 0. 787 | 0. 801 |
| 被动 DNS 数据图分析 | 68. 1 | 70. 7 | 72. 4 | 0. 694 | 0. 653 |

通过比较 3 种方法的 ROC 曲线以及精确率等性能指标,不难看出本研究的改进 BP 算法与其他两种方法相比优势明显。同时我们也表明这个结果与标签传播中的恶意域并不矛盾,因为他们的方法

是针对不同类型的数据进行推断而设计的。

## 4　结束语

本文提出了一种基于 DNS 图的恶意域名挖掘方法,通过添加算法的条件来改进 BP 算法,并将改进后的 BP 算法应用于基于 DNS 图的恶意域检测中。DNS 图能表示域之间的关系及其 ip 地址,在对图上所有节点设置初始值后,使用置信传播法计算图节点的信誉,这种方法在关系分类问题上取得了显著的效果。该算法应用于真实 DNS 流量,其精确率、正确率和召回率均超过 95%,这表明,该方法在实际应用中对恶意域检测是有效的。此外,此方法并不限定于特定的 DNS 技术,对于 DGA、恶意软件、僵尸网络等都可以发挥作用,具有较强的可扩展性和有效性。因此,实验结果证明了提出的改进 BP 算法可以很好地解决恶意域检测问题。目前,本研究仅使用被动 DNS 数据库中的 A 记录构建 DNS 图,下一步如何将记录类型扩展为 NS、MX、PTR 等,以增强节点间的关系,并评估改进后的检测效果是需要我们进一步研究的内容。

## 参　考　文　献


[1] 王志强,李舒豪,池亚平,等. 基于深度学习的恶意 DGA 域名检测 [J]. 计算机工程与设计,2021(3):601 - 606.

[2] CUCCHIARELLI A,MORBIDONI C,SPALAZZI L,et al. Algorithmically generated malicious domain names detection based on n-grams features [J]. Expert Systems with Applications,2020,170:114551.

[3] 郭烜臻,潘祖烈,沈毅,等. 一种基于被动 DNS 数据分析的 DNS 重绑定攻击检测技术 [J]. 信息网络安全,2021(3):87 - 95.

[4] 李建飞. 基于文本特征及 DNS 查询特征的非常规域名检测 [D]. 南京:南京邮电大学,2019.

[5] ANTONAKAKIS M, PERDISCI R, DAGON D, et al. Building a dynamic reputation system for DNS [C] //19th USENIX Security Symposium,2010.

[6] BILGE L,KIRDA E,KRUEGEL C,et al. Exposure: finding malicious domains using passive DNS analysis [C] // Proceedings of the Network and Distributed System Security Symposium,2011.

[7] RAHBARINIA B,PERDISCI R,ANTONAKAKIS M. Segugio: Efficient behavior-based tracking of new malware-control domains in large ISP networks [C] //In 2015 45rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN),2015.

[8] MANADHATA P K,YADAV S,RAO P,et al. Detecting malicious domains via graph inference [C] // the 2014 Workshop,Springer,2014:1 - 18.

[9] KHALIL I,YU T,GUAN B. Discovering malicious domains through passive DNS data graph analysis [C] // ACM on Asia Conference on Computer & Communications Security,2016.

[10] WEIMER F. Passive DNS replication [C] // Proceedings of First Conference on Computer Security Incident Handling,2005.

[11] 郭烜臻,潘祖烈,沈毅,等. 一种基于被动 DNS 数据分析的 DNS 重绑定攻击检测技术 [J]. 信息网络安全,2021(3):87 - 95.

[12] PEARL J. Reverend bayes on inference engines: a distributed hierarchical approach [C] // Proceedings of the National Conference on Artificial Intelligence,1982.

[13] KIRKLEY A,CANTWELL G T,NEWMAN M E J. Belief propagation for networks with loops [J]. Science Advances,2020,7(17):1 - 9.

[14] 芦磊,王晓峰,牛鹏飞,等. 求解多文字可满足 SAT 问题的置信传播算法 [J]. 计算机应用研究,2021(9):2710 - 2715.

[15] 王晓峰, 许道云. RB 模型实例集上置信传播算法的收敛性 [J]. 软件学报,2016(11):2712 - 2724.

[16] HURTADO P J, RICHARDS C. Building mean field ODE models using the generalized linear chain trick & Markov chain theory [J]. Journal of Biological Dynamics,2021,15(1):1 - 25.

[17] 高鹏翔. 基于变权马尔可夫随机场的遥感图像变化检测 [J]. 计算机应用与软件,2021(5):208 - 212.

[18] 张俊丽,常艳丽,师文. 标签传播算法理论及其应用研究综述 [J]. 计算机应用研究,2013(1):21 - 25.

[19] KHALIL I,YU T,GUAN B. Discovering malicious domains through passive DNS data graph analysis [C] // ACM on Asia Conference on Computer & Communications Security,2016:663 - 674.


(责任编辑　于瑞华)