恶意域名检测方法研究进展

王 青[1,2], 韩冬旭[1,2], 卢志刚[1,2], 姜 波[1,2], 董 聪[1,2], 刘俊荣[1,2], 石文昌[3], 刘玉岭[1,2]

[1] 中国科学院信息工程研究所 北京 中国 100093
[2] 中国科学院大学网络空间安全学院 北京 中国 100049
[3] 中国人民大学信息学院 北京 中国 100872

摘要 近年来, 网络攻击事件愈发严重, 域名系统因其简单性和敏捷性而受到攻击者的广泛使用。域名系统可以实现域名与 IP 地址之间的快速映射, 从而可以被攻击者用来隐藏其攻击地址, 域名也因此成为网络攻击的主要载体之一。随着恶意域名不断变化的形式以及数量的剧增, 迫切需要对恶意域名进行检测和防御, 而传统的基于黑白名单的域名检测方法已变得不再有效。基于 DNS 数据的恶意域名检测方法可以实现对恶意域名的高效检测, 因此被广泛提出。本文主要针对基于 DNS 数据的恶意域名检测方法进行梳理分析, 首先简要回顾域名系统的层次结构和解析过程及原理, 以及攻击者基于域名系统所产生的一些滥用技术, 例如域通量技术和快速通量技术; 其次对 DNS 数据按照收集方式的不同将其分为主动 DNS 数据和被动 DNS 数据, 并对这两类数据进行优缺点的对比; 然后按照检测技术的不同将恶意域名检测方法分为三大类, 包括基于规则发现的检测方法、基于动态特征的检测方法和基于关联推理的检测方法, 并依次对每一类检测方法按照类型的不同再次进行细分, 并对各方法的优缺点、适用场景等进行分析说明; 文中对现有检测方法的评估准则进行了划分, 将其分为基于分类性能的评估准则和基于真实环境的评估准则; 最后讨论了现有研究中存在的问题和未来工作方向。

关键词 域名系统; 恶意活动; 恶意域名检测
中图法分类号 TP391.1 DOI 号 10.19363/J.cnki.cn10-1380/tn.2022.12.12

Malicious Domain Names Detection Methods Analysis: A Survey

WANG Qing[1,2], HAN Dongxu[1,2], LU Zhigang[1,2], JIANG Bo[1,2], DONG Cong[1,2], LIU Junrong[1,2], SHI Wenchang[3], LIU Yuling[1,2]

[1] Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
[3] School of Information, Renmin University of China, Beijing 100872, China

Abstract In recent years, cyber attacks have become more and more serious, and the domain name system is widely used by attackers because of its simplicity and agility. The domain name system enables fast mapping between domain names and IP addresses, which can be used by attackers to hide their attack addresses, and domain names have thus become one of the main vectors of cyber attacks. With the ever-changing form and dramatic increase in the number of malicious domain names, there is an urgent need to detect and defend against malicious domain names, and the traditional black and white list-based domain name detection methods have become less effective. DNS data-based malicious domain name detection methods can achieve efficient detection of malicious domain names, and are therefore widely proposed. This paper mainly focuses on DNS data-based malicious domain name detection methods to sort out and analyze, firstly, briefly reviewing the hierarchical structure and resolution process and principles of the domain name system, and some abusive techniques generated by attackers based on the domain name system, such as domain flux technology and fast flux technology; secondly, classifying DNS data into active DNS data and passive DNS data according to the different collection methods, and comparing the advantages and disadvantages of these. Then, the malicious domain name detection methods are divided into three categories according to the different detection techniques, including rule-based discovery detection methods, dynamic feature-based detection methods and association-based inference detection methods, and each category of detection method is subdivided again according to the specific type of detection, and the advantages and disadvantages

通讯作者: 刘玉岭, 博士, 高级工程师, Email: liuyuling@iie.ac.cn。

本论文得到国家重点研发计划(No. 2019QY1303, No. 2019QY1302, No. 2018YFB0803602)、中国科学院战略性先导 C 类(No. XDC02040100)、国家自然科学青年基金(No. 61702508, No. 61802404)的资助。这项工作也得到了中国科学院网络评估技术重点实验室和北京市网络安全与保护技术重点实验室的部分支持。
收稿日期: 2020-09-15; 修改日期: 2020-12-29; 定稿日期: 2022-12-07

of each method and its application scenarios are analyzed and explained; the evaluation criteria of existing detection methods are divided into those based on classification performance and those based on real environment; finally, the problems in existing research and future work directions are discussed.

Key words domain name system; malicious activities; malicious domain names detection

1 引言

域名系统(Domain Name System, DNS)[1]作为互联网的基础设施, 实现域名到 IP 地址的映射。随着互联网的发展, 越多越多的服务提供商使用 DNS 实现其网络运营的敏捷化和可扩展化。然而, DNS 自身简单性和健壮性的体系结构易遭到大量滥用, 使得域名(Domain Name)成为各种网络犯罪中使用的主要攻击媒介之一[2]。攻击者可以使用 DNS 进行远程服务器(Command and Control Server, C&C 服务器)的定位与通信[3-5]、传播恶意软件[6]、发送垃圾邮件[7-8]等恶意活动。因此, 针对恶意域名(本文将涉及到恶意活动的域名统称为恶意域名)的检测至关重要[9]。

传统基于黑白名单等的静态检测方法[10-12]在面对攻击者多样性的技术(例如 Fast-Flux[13], Domain-Flux[14])时略显不足。因此, 研究人员使用统计学习、机器学习等动态方法进行恶意域名的检测。DNS 数据指域名在解析时产生的数据, 例如域名映射的 IP 地址信息、域名的 CNAME 记录等。通过分析发现: 恶意行为会在 DNS 数据中留下痕迹[9,15-18], 例如恶意域名的解析记录具有与良性域名明显不同的分布; 与 DNS 数据相关的资源数据能反映更丰富的恶意域名信息, 例如恶意域名所映射的 IP 地址通常分布在不同的国家和地区。与此同时, DNS 数据仅占整体网络流量的一小部分, 因此有大量工作试图开发基于 DNS 数据的恶意域名检测方法[19-28]。

本文的组织结构如下: 第 2 节简要介绍 DNS 及 DNS 滥用的背景知识; 第 3 节描述域名检测中使用的 DNS 数据的类型及收集方式; 第 4 节介绍三类不同的恶意域名检测方法, 第 5 节对评估方法性能的准则进行总结; 第 6 节讨论现有检测方法存在的问题及未来工作方向; 第 7 节对本文内容进行总结。

2 背景知识

2.1 域名系统

DNS 是互联网基础结构的重要组成部分, 可以将一个 IP 地址关联到一组有意义的字符(如网站域名)上, 当用户访问网站时, 输入字符便可访问该 IP 地址, 实现对 IP 地址的便捷式管理。

DNS 的名字空间是层次结构的, 使用点符号来划分层次结构, 点之间的部分称为标签, 最右边的标签称为顶级域名(Top-Level Domains, TLD), TLD 左侧的域名为二级域名(Second-Level Domains, 2LD), 例如在 “www.a.com” 中, “com”为顶级域名, “a.com”为二级域名, “www.a.com”为完全限定域名(Fully Qualified Domain Name, FQDN), 即同时带有主机名和域名的名称。

域名解析过程如图 1 所示: (1)当用户请求域名解析时, 客户端主机会将域名提交给本地名称服务器, 本地名称服务器首先检查自身缓存, 如果解析记录存在则直接返回结果; (2)如果记录不存在, 本地名称服务器则会将域名发送给根域名服务器; (3)根域名服务器进行本地查找, 如果没有相关域名信息, 则会将下一层顶级域名服务器的 IP 地址返回给本地名称服务器; (4)本地名称服务器通过获得的 IP 地址将域名信息发送给顶级域名服务器; (5)得到权威名称服务器的 IP 地址; (6)本地名称服务器通过获得的 IP 地址将域名信息发送给权威名称服务器; (7)通过权威名称服务器得到域名解析记录并存入本地名称服务器缓存到一定时间, 即生存时间(Time to Live, TTL); (8)本地名称服务器将解析记录返回给客户端。

在上述解析过程中, 包括两种查询方式: 递归查询和迭代查询。其中客户端向本地名称服务器进行查询采用的是递归查询的方式, 如图 1 中第 1 个步骤及第 8 个步骤均采用的是递归查询。递归查询中, 客户端只需发出一次请求, 要求对方给出最终请求的结果; 本地名称服务器向各域名服务器发送请求采用的均是迭代查询的方式, 如图 1 中第 2～7 个步骤。迭代查询中, 客户端发出一次请求, 如果对方没有授权回答, 则会返回一个能解答该请求的名称服务器地址, 客户端继续发出请求, 直至得到结果。

请求域名解析过程中, 客户端会向本地名称服务器发出 DNS 请求报文, 报文里携带需要查询的域名以及希望获得的资源记录类型。本地名称服务器查询后会向客户端返回 DNS 响应报文, 里面包含着域名对应的 IP 地址以及别名等信息。DNS 响应报文中包含大量资源记录(Resource Records, RRs)信息, 例如 A/AAAA 记录表示 IPv4/ IPv6 的主机地址、NS 记录表示权威服务器的记录信息等[29]。上述记录可以为恶意域名检测提供丰富的数据。

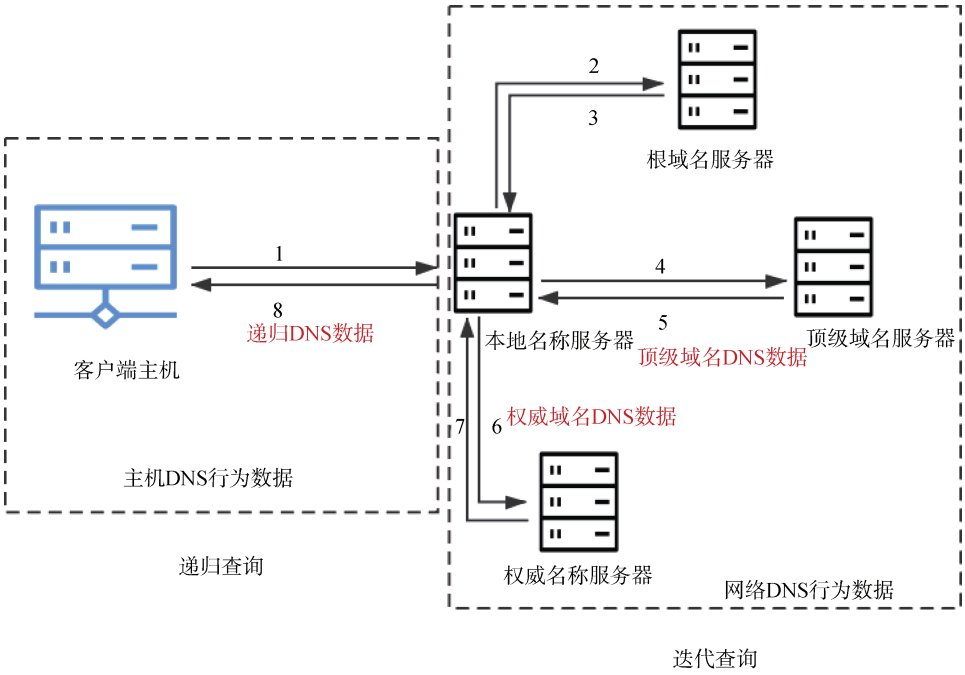

图 1 域名解析过程

Figure 1 Domain name resolution process

2.2 DNS 滥用技术

作为互联网的重要基础设施, 大量的网络服务依托于域名系统。攻击者利用 DNS 的可用性服务实现域名和 IP 地址的不断变换, 以此来快速切换其恶意系统。为了实现其高可用性和对抗检测系统的抵御能力, 攻击者采用基于动态 DNS 的网络策略, 实现高度动态的域名和 IP 地址的映射, 即敏捷 DNS 技术。著名的敏捷 DNS 技术包括域通量(Domain-Flux)技术和快速通量(Fast-Flux)技术。

Domain-Flux 技术采用的是一个 IP 地址与多个域名进行关联, 其域名根据不同的域名生成算法(Domain Generation Algorithm, DGA)[30]动态生成。DGA 是最重要的技术之一, 其生成的域名被称为由算法生成的域名(Algorithmically-Generated Domain, AGD), AGD 的生命周期都较为短暂。DGA 算法由两部分组成: 生成算法和种子, 使用 DGA 算法生成的 AGD 由于生成算法和种子的不同而导致差异很大。例如 Conficker-A[31]每三个小时生成 250 个域名, 使用 UTC 的当前时间作为种子来使僵尸主机每天都生成相同的域名; Conficker-C[32]将每个僵尸主机随机生成的域名的数量增加至 50K。AGD 最直接的检测方式是逆向恶意程序解析[33], 通过对相应的样本进行手动反向工程, 提取种子和算法, 计算其生成的域名集, 但是这种方法严重依赖于分析人员能力和知识。因此, 目前对 AGD 的检测主要基于 DNS 数据分析[14,34-40]。

Fast-Flux(又称为 IP-Flux)技术是 Domain-Flux 的逆过程。攻击者通过将 TTL 设置为很小的值, 使得短时间内查询使用 Fast-Flux 技术部署的域名时, 获得的 IP 地址都不相同, 滥用该技术来更改与 FQDN 相关的 IP 地址信息。对 Faat-Flux 的检测主要集中在域名映射 IP 地址的个数、TTL 值等 DNS 应答信息[13,15]。

Domain-Flux 和 Fast-Flux 技术被广泛用于动态托管恶意站点或在 C&C 基础架构中提供可靠的通信。僵尸网络通常使用 DGA 来自动生成大量域名, 攻击者在进行恶意活动时, 需要在 C&C 服务器上托管各种服务, 指挥大量受感染的主机进行攻击, 这些主机形成的平台称为僵尸网络。恶意软件通常会对 C&C 服务器的域名或 IP 地址进行硬编码, 僵尸主机通过这些信息来访问 C&C 服务器, 但是这种方式很容易被阻断, 攻击者需要可以不断变换的 IP 地址来快速切换恶意系统。DGA 为攻击者管理僵尸网络提供了便捷, DGA 用于生成大量域名, 其中只有部分域名被用来进行 C&C 通信, 僵尸主机可以通过访问不断变换的域名来获取 C&C 服务器的 IP 地址, 即使一个域名被阻断, 则可以迅速更换域名, 从而保护远程服务器不被暴露。

在僵尸网络中部署 Fast-Flux 技术可以动态的频繁更改 IP 地址信息, 从而有效隐藏 C&C 服务器的地址。一个完整的 Fast-Flux 僵尸网络中包含大量的 C&C 主机, 其中只有少量 C&C 主机具备控制与命令

的功能, 其他 C&C 主机仅充当命令转发与跳板的作用。Fast-Flux 中, 一个域名对应无数条不断变化的 IP 地址, 攻击者通过控制底层域名服务器, 不断修改域名服务器中 C&C 服务器的 IP 地址, 使得被控主机每次访问的 IP 地址都不相同, 从而避免 C&C 服务器的地址暴露。

尽管这些滥用技术与 DNS 协议的规范保持一致, 但是攻击者滥用它们以提高其服务器的移动性[9]。利用这些技术生成的域名所产生的 DNS 数据与正常域名有所不同, 例如 TTL 值的分布、域名解析的 IP 地址的个数以及地区位置信息等。因此研究人员通过分析 DNS 数据来对恶意域名进行检测。

3 DNS 数据

DNS 数据是恶意域名检测方法的重要基础。根据收集方式以及收集位置的不同, DNS 数据存在诸多差异。本节对 DNS 数据及其收集方法进行了梳理分析, 如表 1 所示。

表 1 主被动 DNS 数据对比分析

Table 1 Comparative analysis of active and passive DNS data

数据源	收集方式	参考文献	数据来源	数据集示例	优点	缺点
DNS 数据	主动	[13,19-23]	白名单、流行域名列表、黑名单、动态构造、信誉系统、情报网站	LANL Thale	方式灵活、不涉及隐私、高时效	信息有限、易被攻击者发现
	被动	[15-18,24-28,61-63]	主机 DNS 服务器的 DNS 日志	Google public DNS、360NetLab	信息丰富、视角宏观	涉及隐私、无法共享、数据范围受限

3.1 主动 DNS 数据

主动 DNS(Active Domain Name System, ADNS)数据[13,19-23]是指主动访问公共域名列表, 查询响应过程中产生的数据。

域名列表包含良性域名和恶意域名。良性域名从公共白名单、流行域名列表 Alexa Top Sites[41]、顶级域名区域文件等来源收集, 通常选取排名较高的热门域名作为良性域名, 例如选取流行域名列表 Aleax top sites、Cisco Umbrella 中排名前 k 个的域名[16-17,42]。这一做法基于以下假设: 恶意域名通常被访问的频率相对较低。

恶意域名从各种公共黑名单中收集, 例如 SURBL[43]、Malware Domain List[44]、malwaredomains.com、abuse.ch、domaincrawler.com、Malc0de[45]、CleanMX[46]、UrlVoid[47]等, 上述域名列表包含涉及到各种恶意活动的域名。还有一些涉及到特定恶意活动的域名列表, 例如网络钓鱼(PhishTank[48]、APWG[49])、垃圾邮件(Spamhaus DBL[50])、与恶意软件相关的域名(ZeuS Tracker[51]、Ransomware Tracker[52]、Conficker[53]、StopBadware[54])等。获取恶意域名的另一个来源是动态构造恶意域名, 例如在实验环境中运行受感染的客户端来获得 C&C 域名以及将捕获到的恶意域名归纳入恶意域名列表。

此外, 在某些信誉系统和开源情报网站, 例如 Google Safe Browsing[55]、Web of Trust[56]、McAfee SiteAdvisor[57]、Secure Domain Foundation[58]中也提供良性域名和恶意域名, 例如 McAfee SiteAdvisor 在其红色/绿色/黄色报告中提供了“威胁等级”, 可以作为判定域名恶意性的标准。

主动 DNS 数据集均是按照需求自定义构成, 例如现有的公开主动数据集 LANL[59]和 Thales[19]系统。LANL 数据集包含来自 LANL 领域专家模拟的 20 个独立感染活动的攻击, 其中包含大量与这些攻击有关的恶意域名和受感染主机。Thales 系统主动查询并收集来自种子的域名记录, 为安全社区提供免费公开的主动 DNS 数据集。

主动 DNS 数据的收集方式较为灵活, 数据收集器可以轻松查询收集列表中的域名, 而无需任何涉及用户行为的信息, 因此不存在隐私问题。使用主动 DNS 数据还可以发现新注册但尚未使用的潜在恶意域名[60]。然而, 主动 DNS 数据只能提供有限的域名行为信息, 且主动 DNS 数据存在访问恶意域名时被攻击者发现的风险。

3.2 被动 DNS 数据

被动 DNS 数据是指在真实网络环境中部署数据收集器或者访问 DNS 服务器日志, 收集的真实网络环境中域名查询响应相关的数据[15-18,24-28,61-63]。

在真实网络环境中, 根据 DNS 的层次分布, 可以从主机解析器、递归 DNS(Recursive DNS, RDNS)服务器、顶级或权威名称 DNS 服务器上部署数据收

集器以收集被动 DNS 数据。本文根据数据收集位置的不同将收集到的数据分为主机 DNS 行为数据、网络 DNS 行为数据。

主机 DNS 行为数据[24,64-67]是指在本地主机解析器部署数据收集器获得的主机访问域名时产生的 DNS 流量数据, 包含主机查询的域名信息及其查询时间规律等。主机 DNS 行为数据可以反映用户查询域名的行为模式, 例如文献[66]通过分析主机查询的 DNS 流量发现受感染的主机倾向于生成不存在的域名(Non-Existent Domain, NXDomain)查询数据; 文献[26-27,68]利用主机查询域名的映射关系构造图, 从而发现未知的恶意域名。

不同于主机行为数据仅反映单个用户行为, 在 DNS 服务器上部署数据收集器可以获得更全面视角的 DNS 数据, 这些数据称为网络 DNS 行为数据。RDNS 数据[17,24,42,69-70]通过在 RDNS 服务器部署数据收集器进行收集, 需要收集不同位置的大量 RDNS 服务器数据才能获得给定区域内相关的 DNS 流量[18]。从 DNS 层次结构较高的位置, 即顶级或权威名称服务器部署收集器, 可以获得更全面范围的 DNS 流量数据, 例如在某个二级域名的权威名称服务器处收集数据可以获得所有查询这个二级域名的 RDNS 服务器的 DNS 信息。例如 Kopis[18]使用权威名称服务器和顶级域名服务器上的 DNS 查询及响应流数据来检测恶意软件域名; nDEWS[71]使用往返于各顶级域名的权威名称服务器的 DNS 流量, 来为新注册的恶意域名建立预警检测器。

被动 DNS 数据涉及用户的实际查询行为信息, 因此存在一定的隐私性。现有的公开被动数据集包括 Google Public DNS[72]、Farsight Security[73]、360 NetLab 等, 均对主机信息进行了隐私处理, 通常仅提供域名查询的汇总视图, 例如域名出现的第一次及最后一次的时间戳, 以及这段时间内域名和 IP 映射的关联信息等, 不包含任何客户端主机信息。

被动 DNS 数据包含更广泛的恶意行为信息, 从而可以更全面的进行全局视角分析。由于数据收集器的位置问题, 收集到的被动 DNS 数据存在局限性。在本地主机部署收集器只能获取单个主机的 DNS 查询信息, 无法获取全局的恶意活动信息; 恶意活动通常跨多个网络活动, 有限的 RDNS 收集器可能无法完全捕获恶意域名的行为信息。此外, 对网络行为数据的获取较为困难, 数据存在一定的隐私性, 互联网服务提供商(Internet Service Provider, ISP)不易公开。要想获得更高层级的 DNS 数据, 例如权威、顶级域名 DNS 服务器数据, 通常需要注册服务商的协作。尽管从 DNS 服务器上获取的流量数据可以进行隐私处理, 但是数据获取仍然存在一定的限制。

4 恶意域名检测方法

最初的恶意域名检测方式采用静态域名黑名单的方式[10-12], 即通过使用商业和免费的域名黑名单, 建立不断更新的黑名单, 以此来识别和防止恶意域名的访问[10,74]。例如垃圾邮件过滤系统和 DNS 黑名单(仅针对于垃圾邮件来源的域名列表)相结合, 通过将 DNS 黑名单客户端内置在邮件转移代理中, 在本地主机接收邮件前可以通过黑名单先对发送邮件的域名进行检测, 以此过滤垃圾邮件[75]。

但是由于黑名单列表依赖于人工添加, 只能被动的进行检测, 且不能发现未被记录的恶意域名。同时, 黑名单具有较高的误报率, 文献[76]通过比较四个著名的黑名单, 发现其均具有较高的误报率及漏报率。随着域名注册数量的剧增以及攻击形式的增加, 恶意域名每天呈指数倍增长, 使用黑名单进行恶意域名检测已不再有效。

恶意域名检测必须是一个能够持续自动化检测的过程, 许多动态检测系统被逐渐提出。最初, 研究人员分析所观察到的恶意活动场景或 DNS 请求模式, 总结提炼出相应的检测规则实现恶意域名的检测, 本文称这种方法为基于规则发现的检测方法。后来, 随着攻击者技术的增长和域名数据量的剧增, 依赖人工提炼的检测规则无法满足复杂动态场景下域名的检测需求, 基于动态特征的检测方法应运而生。该类方法分析 DNS 数据, 选取能够有效区分域名恶意行为的统计特征, 使用机器学习、深度学习等算法训练检测模型, 实现了高维数据下恶意域名的实时检测。然而, 随着攻击者规避检测技术的发展, 特征逐渐变得不再有效, 研究人员提出使用域名、主机、IP 地址等之间的信息来刻画恶意域名行为之间的关联, 即基于关联推理的检测方法。通过观察域名及其映射的 IP 地址、查询域名主机之间的关联, 制定强有力的关联规则以形成图, 依靠部分图中已知恶意域名来发现更多与之关联的潜在恶意域名。

由于现有的检测方法均采用自定义收集的数据集, 且检测的目标对象也不相同, 因此无法制定统一的判定基准来对其进行比较。本节对已有的文献进行研究总结, 通过制定统一的判定基准, 将检测方法从检测技术上划分为三类: 基于规则发现的检测方法、基于动态特征的检测方法和基于关联推理的检测方法, 如图 2 所示。本节对这三类检测方法进

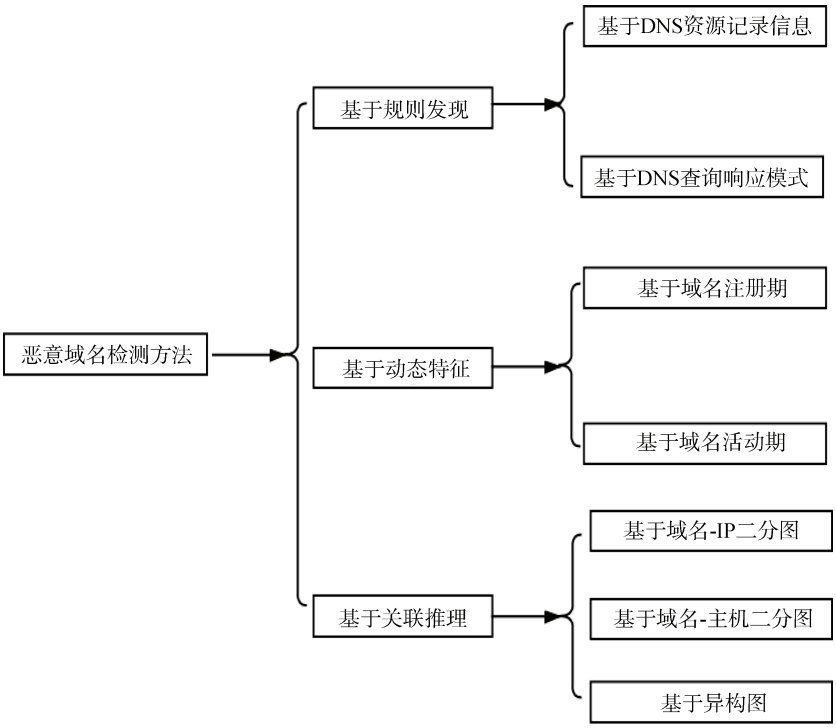

图 2　恶意域名检测方法

Figure 2　Malicious domain names detection methods

行梳理分析, 并制定统一的评估准则框架, 以此来对检测方法性能进行判定。

4.1　基于规则发现的检测方法

在恶意域名检测早期阶段, 研究人员通过观察恶意域名在网络中的活动场景或其 DNS 请求模式, 发现恶意域名存在与良性域名明显不同的异常行为, 例如 DNS 资源记录信息、异常的 DNS 查询响应模式等, 通过分析这些异常行为, 制定规则来对其进行检测。以下针对这两类对基于规则发现的检测方法进行详细介绍, 如表 2 所示。

4.1.1　基于 DNS 资源记录信息的检测方法

文献[13,15,23,64]通过分析特定场景下的 DNS 资源记录信息, 发现恶意域名的 DNS 资源记录与良性域名在分布上具有明显不同。文献[13]基于 Fast-Flux 域名映射更多的 IP 地址, 使用主动方式对良性域名和 Fast-Flux 域名进行查询, 选取 DNS 响应报文中返回的不同 A 记录、一次查询中域名服务器的查询(Name Server, NS)记录、A 记录映射的不同自治系统(Autonomous System, AS)的数量等特征, 定义能够区分 Fast-Flux 域名的线性决策函数, 以此来计算域名的通量分数。决策函数中的参数值和阈值需要人工进行定期调整, 以防攻击者逃避检测。

文献[23]采用与文献[13]相同的查询方式, 对从垃圾邮件中收集到的欺诈域名进行主动 DNS 查询。不同于文献[13]仅对域名的 DNS 记录进行分析, 文献[23]分析欺诈域名及其相应的恶意活动中更改 DNS 映射记录的速率, 发现欺诈域名具有比合法域名更频繁的更改速率, 且欺诈域名在 IP 空间上具有比良性域名更广泛的分布。结果表明, 监视 DNS 映射中存在的异常信息有助于对恶意域名的检测。

不同于文献[13,23]使用主动查询域名的方式, 文献[15]通过观察本地解析器收集的被动 DNS 响应数据, 发现依靠 DNS 异常的资源解析记录可以检测不仅限于 Fast-Flux 域名, 还包括与僵尸网络、垃圾邮件、域名抢注等有关的域名。例如部署外部代理程序来检测 Fast-Flux 域名, 通过观察不同时间间隔内关联的资源记录的数量, 制定相关阈值, 如果域名关联的资源记录的数量达到某个阈值, 则可以将其判定为恶意域名。垃圾邮件管理员使用 Fast-Flux 域名快速切换 IP 地址, 通过检查 IP 地址及其相关联的 NS 记录等历史行为信息, 以此计算新域名的“信誉”。但是这种方法过于依赖历史行为信息, 因此只能检测与已知恶意域名相关的新域名, 检测范围存在局限性。

文献[64]依赖更丰富的资源数据, 以此获得更高的准确率。通过从域名的资源记录中获取邮件交换(Mail Exchanger, MX)记录, 从 WHOIS 查询及黑名单中获取权威 DNS 服务器记录等, 将这些特征值加权

表 2 基于规则发现的检测方法

Table 2 Metrics-based detection methods

类型	文献	领域知识	检测方法	优点	缺点
基于DNS的资源记录	[13]	A、NS、AS 记录数量与良性域名不同	使用决策函数计算域名的通量分数	提供对 Fast-Flux 现象的首次实证研究	函数需要手动调整参数
	[23]	DNS 映射记录随时间变化的速率及 IP 空间分布与良性域名不同	反复解析域名以获取其 IP 增长率及累计率	数据信息具有局限性	受域名更新 DNS 记录的速率限制
	[15]	不同时间间隔内关联的资源记录数量与良性域名不同	对资源记录进行排序, 设置阈值检测	自动检测异常及恶意攻击	依赖历史行为信息
	[64]	DNS 记录及使用期限、权威域名服务器、网络状态与良性域名不同	将所选特征值加权求和计算域名的可疑比率	高准确率	数据缺失导致高误报率
基于DNS查询响应模式	[74]	僵尸网络查询 DNS 黑名单列表的方式与良性域名不同	构造 DNSBL 查询图, 基于查询流量的空间及时间特征设计启发式方法	有效检测早期的僵尸程序	误报率较高、易被规避
	[81]	僵尸网络域名的 DNS 查询速率与良性域名不同	使用 Chebyshev 不等式和简化的马氏距离公式判定域名的查询速率	有效检测僵尸网络域名	误报率较高
	[83]	基于异常重复的 NXDOMAIN 响应速率	使用 Chebyshev 不等式和简化的马氏距离判定域名的 NXDOMAIN 响应速率	有效检测到可疑域名	计算量较大
	[11]	同一恶意软件家族的恶意域名具有相同的查询规律	使用 Jaccard 索引计算两个域名的 DNS 查询数据之间共现关系的程度	有效检测未知的恶意域名	检测恶意域名的范围有限

求和计算域名的可疑比率, 以此发现未知的恶意域名。尽管这一检测规则具有较强的区分能力, 同时也伴随着较高的误报率。

DNS 数据库提供与域名解析相关联的资源记录, 其中包括 MX、NS、反向解析查询记录(Pointer Record, PTR)等。Maxmind 数据库及 Team Cymru 服务[77]、iPlane[78]的映射数据集提供域名及其 IP 托管 AS 的信息。Maxmind 数据库[79]还提供域名及 IP 地址的地理位置信息, 例如其所处的国家和地区信息。

4.1.2 基于 DNS 查询响应模式的检测方法

文献[11,65,74,80-83]通过观察分析 DNS 查询流量, 发现恶意域名具有与良性域名明显不同的 DNS 行为模式。文献[74]基于僵尸网络程序查询 DNS 黑名单列表(DNS Blackhole List, DNSBL)的方式与合法服务器有所不同这一发现, 构造 DNSBL 查询图, 使用基于查询模式的空间及时间关系设计启发式方法, 以此来发现僵尸程序。但是这种方法容易导致较高的误报率, 且易被攻击者规避。

不同于文献[74]利用僵尸网络程序查询黑名单列表的方式, 文献[81]基于与僵尸网络有关的域名的动态DNS查询率远高于合法域名这一发现, 提出“规范动态DNS请求速率”这一检测规则。通过将SLD的查询速率与SLD的子级 3LD的查询速率的比率进行汇总, 使用Chebyshev不等式及简化的马氏距离公式判定域名的查询速率是否存在异常高或短暂的时间集中等现象, 以此来检测僵尸网络的C＆C服务器。不同于文献[81]使用动态DNS请求速率进行检测, 文献[82]基于异常重复的NXDOMAIN响应速率的检测规则来检测异常的响应速率。文献[83]使用Chebyshev不等式及简化的马氏距离公式对文献[81]及文献[82]中提出的方法进行评估, 结果表明, 由于某些合法域名具有较短的TTL值, 从而导致文献[81]中的方法具有较高的误报率; 实验证明文献[82]中的方法可以更有效的检测恶意域名, 但是这两种方法均具有较大的计算量。

为了解决提出的规则易被规避、误报率较高等问题, 文献[11]使用 DNS 查询数据和已知的恶意域名黑名单, 基于同一恶意软件家族的恶意域名具有相同的查询规律这一发现, 使用 Jaccard 索引计算两个域名的 DNS 查询数据之间共现关系的程度, 以此来发现与已知黑名单中的恶意域名有较强关联的未知的恶意域名及受感染主机, 实验证明验证列表中91%的域名可被该方法检测到。

4.1.3 总结与讨论

基于规则发现的检测方法中, 研究人员通过观察恶意活动场景或 DNS 请求模式, 总结相应的检测

规则来对恶意域名进行检测。这些规则在恶意域名检测早期起到了一定效果, 但是随着攻击者技术的增长及恶意域名在互联网中的泛滥, 基于规则发现的检测方法不具备处理大型数据集的能力。人工提炼的检测规则无法满足复杂动态场景下域名的检测需求, 且由于检测规则较为单一化, 导致该类方法准确率较低, 并伴随着较高的误报率; 检测规则易被攻击者所规避, 基于规则发现的检测方法逐渐变得不可行。

4.2 基于动态特征的检测方法

随着攻击者技术的发展和域名生产机制的变化, 传统的基于规则发现的检测方法无法应对网络中产生的大量 DNS 数据, 因此提出了基于动态特征的检测方法。基于动态特征的检测方法首先从多种 DNS 相关数据中选取能够有效区分域名恶意行为的统计特征, 然后使用机器学习、深度学习等算法训练能够在高维数据下进行自动化检测恶意域名的检测模型。

基于域名的生命周期, 本文将基于动态特征的检测方法划分为两个阶段: 在域名注册期对域名进行检测, 即仅通过域名注册数据、历史记录对刚注册的域名进行检测; 在域名活动期对其进行检测, 即基于域名在网络活动中的行为特征判定域名的恶意性。以下针对这两个阶段对基于动态特征的检测方法进行详细介绍, 如表 3 所示。

4.2.1 基于域名注册期的检测方法

攻击者在进行恶意活动时, 通常会注册大量的备选域名, 因此即使恶意域名被列入黑名单, 攻击者仍然可以注册新的域名来进行恶意活动。文献[84]通过对 14 个月的.eu 域名注册数据分析发现恶意域名在首次注册后仅在非常短的时间内运行, 60%的域名仅存在一天的活动时间。攻击者使用“即按即用”的策略, 即一旦域名实现其目的, 攻击者就可以放弃他们并使用新注册的域名进行下一次恶意活动。

一系列检测方法旨在从域名的注册阶段对其进行检测[60,84-86], 通常基于以下原则: 攻击者需要注册大量域名, 又要考虑注册成本问题, 从而产生大批量的域名相似、注册时间相同、拥有同一注册商等异常注册行为。随着对恶意域名的大量需求, 域名注册过程已实现半自动化批量注册。

部分研究工作仅依靠域名的注册记录来识别恶意域名[60,84-85,87]。域名注册记录可以从“WHOIS”域名注册数据库[88-90]和顶级域名区域文件中获得, 通常包含域名的注册时间以及域名注册商、注册人信息、域名的权威域名服务器等基础注册信息。注册历史记录可以从诸如 DomainTools[91], Who.is[92]之类的第三方服务获得, 也可以在注册服务商处[93-94]获得。

在文献[85]中, 作者使用有限的“WHOIS”域名注册数据、DNS 区域文件数据以及少量的恶意域名种子, 基于不良活动会成组的注册域名这一假设, 从中选取名称服务器特征以及域名注册特征对未知域名进行集群聚类, 以此发现潜在的恶意域名。然而由于该假设并不总是成立, 仅对部分域名有效, 从而该类方法存在局限性。

不同于文献[85]仅关注域名的名称服务器和注册特征, 文献[95]通过观察 5 个月内来自.com 区域内 TLD 的区域更改信息, 发现垃圾邮件发送者采用批量注册域名的方式, 并且经常重用他人注册过的域名。作者分析垃圾邮件域名注册过程中在域名命名模式、权威名称服务器、域名生命周期、批量注册等特征上与良性域名的区别, 研究表明, 使用这些注册特征可以有效检测垃圾邮件域名。

除了使用域名的注册数据外, 托管域名的 DNS 基础结构以及域名早期的 DNS 查找模式也能表现出域名的恶意性。文献[86]通过分析域名的 DNS 基础结构, 发现良性域名和恶意域名在域名映射的 IP 所属的地址空间、关联的资源记录、AS 分布、所属国家及地区等分布上有明显不同, 因此提取域名的 DNS 基础结构特征以及查找模式特征可以有效区分良性域名和恶意域名。

在文献[86,95]的基础上, 文献[60]设计了第一个可以在域名注册时主动检测其恶意性的信誉系统 PREDATOR。该系统从域名注册信息中选取注册配置文件信息、注册历史记录、批处理关联等特征, 结合凸多面体机算法对标记好的域名进行模型训练, 以此来检测未标记域名。PREDATOR 实现在注册阶段准确、自动的识别恶意域名, 从而在域名注册时期消除域名滥用。但是该检测系统仅对单个区域下(例如.com、.net)注册的域名进行检测, 无法实现跨区域域名之间的检测。

文献[71]则引入更广泛的检测视角。文献[71]提出一种用于 TLD 注册管理机构运营商的预测系统 nDEWS, 这是第一项为整个 DNS 区域提供新注册域名检测的系统。nDEWS 首先通过分析域名注册数据和 TLD 权威服务器提供的全局 DNS 查找数据, 利用 DNS 请求数量、IP 地址总数、所属国家、自治系统等基于域名注册特征及顶级域名的全局查找模式特征, 然后使用基于 K 均值(K-means)的聚类算法来监测和分类整个 DNS 区域新注册的域名。但是由于数

据涉及整个 DNS 区域及隐私问题, 文献[71]中的数据较难获取, 因此无法进行大范围的应用。

不同于上述研究工作仅专注于单个的恶意域名, 文献[84]是第一个将检测重点转移到恶意活动上的研究。通过使用注册信息来识别恶意活动, 从恶意域名注册数据中选取基于域名、注册人信息、名称服务器等特征, 首先使用欧几里得距离计算域名之间的距离, 然后使用分层聚类算法将域名按照不同类型的恶意活动进行划分。

在域名注册阶段对恶意域名进行检测的优点是现有的检测系统均是观察分析恶意域名的使用情况, 即分析 DNS 行为数据, 从而对域名恶意性进行检测。使用在域名注册期对恶意域名进行检测的方法可以更早发现潜在的恶意域名, 该类检测方法通常早于现有的黑名单检测, 因此可以提前防御恶意攻击。

基于域名注册期的特征进行恶意域名检测的方法仍然存在一些限制。首先, 可被使用的域名注册数据较难获得, 例如委托的注册商及域名的历史记录信息等。NS 数据需要从区域文件中获取; 某些顶级域名的区域文件无法获取, 且数据可用性较差, 缺少部分域名的额外资源信息容易产生漏报。例如文献[64]仅识别出数据集中 70%的僵尸网络域名, 其余30%的域名由于缺失 WHOIS 数据信息而被检测为良性域名。为了规避检测, 攻击者通常使用不同的注册模式和注册数据, 且一些注册服务商会向客户提供匿名服务以此来模糊其注册信息, 这类混淆服务会对检测造成影响。大多数基于新注册域名的检测方法准确率较低, 因为其完全依赖历史信息, 无法检测与已知恶意域名没有任何关联的域名。

4.2.2 基于域名活动期的检测方法

由于恶意 DNS 行为产生其独特的、与合法 DNS 服务不同的流量, 因此可以在域名活动期对恶意域名进行检测[17]。该类方法通常收集一段时间内的域名活动产生的 DNS 流量数据, 然后对 DNS 数据及其丰富的相关资源信息进行统计分析, 从中选取能够准确有效区分恶意域名的特征, 并训练分类模型以学习恶意域名不同于良性域名的行为方式, 以此来对未知的域名进行检测[3,16,35,96-100]。

文献[62]分析从 ISP 收集的被动 RDND 流量数据, 首先根据域名解析 IP 地址集合之间是否相交计算域名之间的相似性, 使用单链接分层聚类算法对各个候选 Fast-Flux 域名进行分类, 其中可能包含合法的内容分发网络(Content Delivery Network, CDN)群集。从收集到的被动 DNS 数据及外部资源信息中提取能够有效区分 Fast-Flux 域名群集及 CDN 群集的统计特征, 例如域名解析的 IP 地址数量、IP 映射的 AS、BGP 前缀、国家及地区多样性等特征, 使用 C4.5 决策树算法对群集进行分类以检测 Fast-Flux 域名。结果表明, 该方法无法有效区分模仿 CDN 的僵尸网络流量和合法 CDN 流量。

文献[101]使用被动 DNS 流量, 并结合主机查询域名的信息, 提出 Fast-Flux 网络检测系统 FluXOR。FluXOR 通过分析监视与 Fast-Flux 网络有关的主机查询信息, 选取基于域名、DNS 应答、网络主机异构体等特征训练朴素贝叶斯分类器, 从而准确区分与 Fast-Flux 网络有关的恶意域名及主机。

文献[17]提供第一个为域名建立的动态 DNS 信誉系统 Notos, 该信誉系统通过分析从多个 RDNS 服务器收集到的 DNS 历史流量数据, 从中提取域名映射 IP 地址的 BGP 前缀、地理位置、不同 AS 数量等基于网络的特征; 域名映射的 IP 地址所属 AS 中 IP 地址的相关历史域名的域名、字符分布等基于区域的特征; 已知恶意域名及恶意 IP 地址等基于已有证据的特征, 使用聚类和 J48 决策树算法对合法域名、恶意域名的网络及区域行为训练模型。该模型可以动态的为未知域名分配信誉分数, 如果域名涉及恶意活动, 则为其分配低信誉分数。Notos 具有较高的准确率以及较低的误报率, 其明显缺陷在于过于依赖历史 DNS 数据, 而对于历史信息较少的域名无法(较难)为其分配信誉分数。

不同于文献[17,19,62,102]等从 RDNS 服务器收集数据, 文献[18]使用从 DNS 结构中更高层次的顶级域名、权威名称服务器中收集到具有全局可见性的 DNS 查询响应流, 从中提取查询域名的递归服务器的分布特征(BGP 前缀、AS、国家及地区)、域名请求者配置文件特征、域名映射 IP 地址的历史信誉特征等, 并使用随机森林等算法对良性域名及恶意软件域名进行模型训练, 从而检测恶意软件域名, 但是该系统无法有效处理活动时间较短的域名。

文献[16]提出 EXPOSURE, 该检测系统不局限于检测 Fast-Flux 域名、恶意软件域名等涉及特定恶意活动的域名, EXPOSURE 可以检测任何与恶意活动相关的域名。EXPOSURE 从收集的被动 DNS 数据中提取基于时间、DNS 应答、TTL 值、域名等四类特征, 使用 J48 分类算法对模型进行训练, 以此来实时检测恶意域名。由于 EXPOSURE 中提取的 TTL 值等特征易被攻击者规避, 从而逃避检测, 导致该方法鲁棒性较差。

除了从 DNS 数据中提取特征外, 部分研究工作选择从查询模式、时间行为等宏观角度提取特征。例如文献[19]通过观察从多个分布式 RDNS 服务器收集的 DNS 查询-响应数据发现 DNS 查询之间具有相互关联这一规则, 选取 DNS 查询中的时间相关性特征, 即如果一个域名经常与来自同一 RDNS 服务器的恶意域名一起查询, 则认为这两个域名之间具有相关性。这种方法不需要使用带标记的数据集进行训练, 仅使用少量已知的恶意域名作为锚。通过基于 TF-IDF 概念的两个度量标准粗略计算未知域名与已知恶意锚域名之间的紧密程度, 使用聚类算法对域名进行更精细的识别, 从而检测与已知恶意域名相关联的恶意域名。

上述检测方法均依赖于 DNS 历史流量数据, 此外, 研究人员还结合与主机相关的特征来同时检测恶意域名与受感染主机[3,66,101,103]。例如文献[3]基于具有相同 DGA 的僵尸主机生成相似的 NXDomain 应答流量这一直觉, 从少量 NXDomain 流量中提取 *n*-gram、字符分布的熵、域名结构等域名字符级特征, 使用 *X* 均值(*X*-means)聚类算法对这些域名进行划分, 将其划分为若干群集, 同时结合主机查询产生的 NXDomain 之间的相似性度量, 使用基于谱聚类的图划分策略对其进行聚类。将两类聚类结果相关联, 得到多个分别由同一 DGA 生成的域名群集, 并结合交替决策树算法对新发现的 DGA 生成的域名进行模型训练, 以此来识别受感染的主机。

表 3 基于动态特征的检测方法

Table 3 Dynamic Features-based detection methods

类型	文献	分类特征	检测算法	优点	缺点
基于域名注册期的检测	[85]	名称服务器、域名注册特征	聚类	仅使用部分已知恶意域名及有限注册信息	方法仅对部分域名有效
	[95]	域名命名、权威名称服务器、域名生命周期、批量注册特征	Jaccard 相似性度量、Poisson 分布	证明恶意域名在注册阶段就显示其恶意性	无法进行自动化检测
	[60]	域名配置文件信息、注册历史记录、批处理关联特征	凸多面体机	域名注册时自动检测其恶意性	仅能检测单个区域下的注册域名
	[71]	域名注册特征、顶级域名的全局查找模式特征	*K*-means 聚类	对整个 DNS 区域新注册域名进行检测	数据较难获取
	[84]	域名、注册人、注册商、名称服务器特征	层次聚类	将恶意域名按照恶意活动分类	注册服务商提供匿名服务以进行混淆
基于域名活动期的检测	[17]	网络、区域、已有证据特征	J48 决策树、聚类	高准确率及低误报率	无法检测历史数据很少的域名
	[18]	查询域名的服务器分布、域名请求者配置文件、IP 地址历史信誉特征	随机森林等算法	全局查询视角检测域名	无法有效处理短时间内活动的域名
	[16]	时间、DNS 应答、TTL 值、域名特征	J48 决策树	检测任意类型恶意域名	特征易被攻击者规避
	[20]	DNS 查询中的时间相关性特征	基于 TF-IDF 的度量标准及聚类算法	仅需少量恶意域名种子	检测范围有限
	[3]	*n*-gram、字符分布的熵等域名字符级特征	*X*-means 聚类、谱聚类、交替决策树	能够发现新的 DGA 生成的域名	无法区分使用相同 DGA 的不同僵尸网络
	[108]	域名字符级特征	I-DGA-DC-Net、机器学习算法	具有较高检测精度	无法检测非 DGA 域名
	[67]	WHOIS、IP 分布、DNS 活动等特征	随机森林、逻辑回归、*k* 最近邻等	误报率较低、可以有效检测隐身攻击	无法检测缺乏 DNS 活动的恶意进程

在对由 DGA 生成的域名, 即 AGD 的检测方法中, 研究人员通常仅基于域名字符级特征对其进行检测。最初, 研究人员通过人工提取统计特征, 例如域名的长度、字符分布、*n*-gram 模型等, 使用机器学习算法对 AGD 进行检测[39,103]。

由于只使用域名字符级特征对 AGD 进行检

测具有较低的准确率, 且攻击者可以通过修改生成算法轻易绕过检测, 因此研究人员倾向于结合域名字符级特征及DNS应答特征等对AGD进行检测[3,14,34-35,66,98,111-113]。

文献[3,66,98,112]基于僵尸网络倾向于生成NXDomain应答这一事实, 使用NXDomain流量对AGD进行检测。与文献[3]所提出的方法相似, 文献[112]提供具有分类精度和泛化能力更好的检测方法, 通过监视DNS流量中NXDomain的响应信息, 从中提取域名字符级特征, 例如重复字符的比例、连续辅音的比例等特征, 使用随机森林、支持向量机等算法来检测AGD。结果表明, 该方法可以识别出未知的AGD。

不同于仅基于相似的NXDomain流量这一特征进行检测, 文献[103]提出名为DFBotKiller的域名信誉系统, 通过对可疑的恶意活动及DNS流量中可疑的历史记录来自动的为参与这些可疑域名活动的主机分配分数, 使用例如Levenshtein距离等三种度量方式对AGD进行检测。文献[103]中提出的检测方法在一定程度上依赖于DNS的历史记录信息,更进一步, 文献[99]仅基于普通DNS流量和僵尸网络产生的DNS流量具有明显不同这一发现, 使用Stratosphere Project中基于网络的行为模型对DNS流量进行建模, 从而将DGA流量和普通DNS流量进行有效区分以此来发现僵尸网络域名。

随着攻击者的躲避策略逐渐增加, 通过人工提取的特征需要频繁进行更改, 基于机器学习的检测方法逐渐变得不可行。随后, 研究人员利用深度学习自动提取特征这一有效特性对AGD进行检测[37-38,40,105-110]。例如文献[107]使用深度递归神经网络架构, 即长短期记忆(Long Short-Term Memory, LSTM)模型和双向LSTM模型自动提取AGD域名字符级中的有效特征, 从而进行检测模型的训练。基于深度学习的检测方法省去了人工提取特征的工作, 且方法精度较高于机器学习。文献[108]在深度学习的基础上, 使用基于深度学习的框架I-DGA-DC-Net结合经典的机器学习算法对AGD进行检测。该框架首先使用暹罗神经网络以及白名单对域名相似性进行检测, 然后将处理后的域名字符传入LSTM层中自动提取域名字符级特征, 最终使用机器学习算法对其分类。结果表明, 深度学习结合机器学习的方法比现有的基于深度学习的检测方法具有更高的精度。

此外, 还有一些工作结合DNS流量及其他层次的数据来对恶意域名进行检测。例如文献[5]使用DNS流量和网络流量检测APT恶意软件感染, 基于这些数据提取恶意DNS特征和网络流量特征来对可疑的APT恶意软件域名及其可疑IP流量进行检测。文献[67]提出PDNS(Process-DNS)系统, DNS传感器捕获主机的DNS活动以及相关程序及进程数据, 通过分析DNS及其关联的程序信息, 选取WHOIS、IP地址分布、权威域名服务器等基于网络的特征以及进程与DNS活动之间关系的特征, 以检测恶意域名及受感染主机内的恶意进程。PDNS具有较高的准确率, 且可以有效检测发生在合法域名上的隐式攻击。

攻击者通过劫持合法顶级域名以创建大量的子域名, 这些域名被称为阴影域名。阴影域名由于继承其合法域名的信任, 其注册信息和顶级域名的注册信息相同, 因此基于域名注册数据的检测方法无法对其进行检测。研究发现许多阴影域名仅被访问过一次, 因此无法使用DNS流量的统计特征对阴影域名进行检测。文献[114]通过分析发现可以从以下两个维度对阴影域名进行检测: 同一顶级域名下的子域名之间的偏差、不同顶级域名下各阴影域名之间的关联来识别阴影域名。从这两个维度中选取17个特征训练分类模型, 以此来检测潜在的阴影域名。

4.2.3 总结与讨论

基于动态特征的检测方法在目前研究中所占比例较大, 且起到了不错的效果, 但是仍然存在一些局限性: 检测方法依赖于特征, 而特征易被规避。基于动态特征的检测方法中通常对DNS数据进行分析, 选取其统计结果作为特征, 导致特征鲁棒性普遍较差, 这使得检测方法易于被复杂的攻击者规避。

4.3 基于关联推理的检测方法

随着攻击者规避检测技术的发展, 仅依靠分析从DNS数据提取的统计特征来识别恶意域名逐渐变得不再有效。研究人员提出使用域名、客户端主机、IP地址等刻画恶意域名行为之间的关联来对恶意域名进行检测, 这种方法被称为基于关联推理的检测方法。基于关联推理的检测方法使用域名及其映射的IP地址、查询主机等之间的联系制定关联规则, 并构建图, 对图中部分节点进行标记, 使用例如信念传播(Belief Propagation, BP)算法、基于路径的推理算法等推断图中未知节点的恶意性。

基于关联推理的检测方法通常基于以下原则: 与恶意域名有强关联的域名通常也是恶意的, 攻击者可以伪造域名的特征, 但是无法伪造域名之间的关联, 如果某个域名与一组已知的恶意域名具有强关联, 则该域名很可能也是恶意的; 攻击者倾向于

资源的重用, 在不同的攻击活动中通过重用资源从而建立了恶意域名之间的关联, 例如文献[87]中将具有相同的名称服务器、注册人信息、IP 地址等关联视为恶意域名资源重用的表现。

本节将基于关联推理的检测方法按照关联规则的不同划分为三类: 基于域名及其映射的 IP 地址之间的关联、基于域名及其查询主机之间的关联、基于多种类型(CNAME、IP、主机)之间的关联。本节对这三类检测方法进行详细介绍, 如表 4 所示。

4.3.1 基于域名-IP 二分图的检测方法

文献[21,90,115-119]仅使用域名及其映射的 IP 地址之间的关系构造关联规则, 形成域名-IP 二分图, 其中域名和 IP 为节点, 边表示节点之间存在映射关系。文献[90]提出一种半手动标记方法, 将域名及其映射的 IP 地址构造成二分图的形式, 提取基于图、域名、IP 地址、域名黑白名单、IP 地址黑名单等 6 类特征, 结合 *K*-means 聚类算法将图形组件聚类为两类, 使用恶意群集中被列入黑名单中的域名权重高于良性群集这一分类策略为集群分配临时标签, 最后手动验证标签的正确性。该方法减轻了对域名进行手动标记的工作量, 但是分类策略过于依赖域名黑名单, 导致该方法具有较高的误报率。

表 4 基于关联推理的检测方法

Table 4 Associative reasoning-based detection methods

类型	文献	关联规则	检测算法	优点	缺点
域名-IP 二分图	[90]	域名及其映射的 IP 地址	*K*-means 聚类	无需手动标记大量数据集	过于依赖域名黑名单
	[115]	域名在一段时间内由相同的 IP 地址托管	基于路径的推理算法	少量已知恶意域名便可检测恶意域名	恶意域名建立与良性域名的虚假关联导致误报
	[116]	域名及其映射的 IP 地址	流算法	提前预测恶意域名	误报率较高
	[21]	两个域名共享至少一个专用 IP, 或共享来自不同 AS 的多个公共 IP	基于路径的推理	具有良好的覆盖范围的强关联规则, 实现高准确率	计算量较大
	[117]	域名及其映射的 IP 地址	马尔可夫链、支持向量机等算法	无需外部资源信息	计算量较大
	[118]	域名及其映射的 IP 地址	图嵌入、随机森林等算法	计算量较小	关联规则较弱
域名-主机二分图	[120]	共享主机的数量及主机查询域名的顺序行为	统计分析、顺序分析	有效检测 C&C 域名之外的间接关联域名	计算的时间复杂度较大
	[26]	主机及其查询域名的关联	循环信念传播算法	仅依靠少量的标记数据集	方法不具备可扩展性
	[68]	客户端查询的域名之间的顺序相关性	聚类算法	有效检测躲避时间、空间检测技术的 DNS 活动相关恶意域名	无法检测不涉及恶意活动的单个恶意域名
	[27]	企业网络内部主机与外部域名的可疑通信	信念传播算法	可以检测到被防病毒技术忽略的恶意域名	方法易被规避
	[24]	客户端主机查询域名的行为关联	随机森林算法	发现新的恶意软件家族域名	难以检测未被已知的受感染主机查询的恶意域名
异构图	[119]	主机查询域名、域名及其映射的 A、CNAME 记录	马尔可夫随机场、信念传播算法	有效检测恶意软件域名及受感染主机	误报率较高
	[2]	受感染主机查询的域名倾向于是恶意的	转导分类算法	训练样本较少时仍具有较高的性能	系统消耗大量资源、效率较低, 检测范围有限
	[121]	主机查询域名、域名及其映射的 A、CNAME 记录	GCN、基于元路径的注意力机制	具备更好的检测能力	计算量较大、消耗资源

文献[115]基于与文献[90]相同的假设构造关联规则: 如果两个域名在一段时间内由相同的 IP 地址托管, 则这两个域名之间存在某种关联关系。不同于文献[90]使用聚类算法对域名-IP 二分图进行分类,

文献[115]首先按照域名映射 IP 地址之间的关联关系构建二分图, 其中节点表示域名, 边表示域名之间的关联。然后基于域名之间解析的 IP 地址越通用, 则关联越强, 权重越大这一假设计算边的权重, 并使用基于路径的推理算法来检测图中未知的恶意域名。该方法仅依赖少量已知的恶意域名种子便可检测与其相关联的潜在恶意域名。由于关联规则较为薄弱, 该方法存在恶意域名“故意”建立与良性域名虚假连接的现象, 即恶意域名映射与良性域名相关联的 IP 地址, 从而导致误报率的增加。

文献[116]不仅仅使用域名解析的 A 记录, 同时结合一些外部资源数据作为辅助信息来计算域名和 IP 之间的连接强度。文献[116]使用 A 记录构建域名-IP 二分图, 同时利用例如 IP 所属的 BGP 前缀、AS 编号、注册商、国家、日期等特征计算四种类型边(域名-IP、IP-域名、IP-IP、域名-域名)的权重, 并将其表示为矩阵。对一组已标记的域名进行迭代计算, 得到最终每个域名的信誉向量。使用矩阵及向量作为流算法的输入, 以计算图中域名的信誉分数, 从而识别更多的可疑域名。

仅依靠域名及其 IP 地址之间的映射关系容易产生弱关联规则, 使得方法准确率较低, 且具有较高的误报率。文献[21]为避免弱关联, 使用主动 DNS 数据构造域名之间的强关联规则, 通过基于共享专用 IP 地址的域名很可能来自同一实体这一直觉将 IP 分为公共和专用 IP, 然后基于两个域名(i)共享至少一个专用 IP, 或(ii)共享来自不同 AS 的多个公共 IP, 则两个域名相关联的直觉构造域名-IP 二分图, 以形成图, 在图上使用基于路径的推理算法来预测其他未知节点的恶意性。

以上关联规则仅包含域之间的映射关系, 文献[117]提出一种新的检测系统 MalPortrait, MalPortrait 具有更丰富的关联信息。该系统使用基于图的方法, 通过域名映射的 IP 地址信息, 即将解析为相同 IP 地址的域名连接起来以构建图, 并结合域名的单个特征(字符级特征、网络级特征等)及域名之间的关联信息组合生成新的特征。使用新生成的特征训练分类器, 以此对未知域名进行检测。该检测方法不依赖于其他外部资源信息, 但是在计算域名的新特征时需要消耗大量计算资源。

为缓解使用图分析消耗的大量计算资源, 文献[118]开发一种轻量级的方法 MalShoot, 基于域名映射 IP 地址的关联关系构建图, 并使用图嵌入技术将域名的 DNS 解析数据嵌入到低维向量机中, 共享相似上下文信息的域名会被嵌入到相似的向量机中, 然后使用机器学习分类器对其进行训练分类。由于图中边之间的权重仅依赖于 IP 地址映射的次数, 从而导致该方法关联规则较弱。

4.3.2 基于域名-主机二分图的检测方法

不仅限于域名及其映射的 IP 地址作为节点构造图, 研究人员结合域名及查询域名的客户端主机之间的关联构造域名-主机二分图[26-27,68,120]。例如文献[120]根据域名与恶意域名共享客户端主机的数量及客户端主机查询域名的顺序关系这两个关联规则构造图, 对域名进行聚类以检测未知的恶意域名。

文献[120]的检测方法具有较高的时间复杂度, 在文献[120]的基础上, 文献[26]通过分析企业的事件日志数据, 利用恶意软件固有的通信结构, 为企业中的每个主机及主机访问的域名建立边的联系, 构造域名-主机二分图, 通过仅对图中少量域名进行标记, 使用信念传播算法来推断图中其他未知域名的恶意性。相对于文献[26]对每个主机请求域名的连接都建立边之间的关系, 文献[68]制定了更具关联性的规则, 文献[68]提出一种恶意软件活动检测机制 GMAD, GMAD 基于图的形式来表示 DNS 客户端主机的域名查询序列, 即客户端查询的域名之间的顺序相关性, 以此来检测受感染的恶意域名和客户端以及恶意的 DNS 活动。该方法可以有效检测出躲避使用时间、空间行为特征检测方法的恶意域名, 但是该检测方法不能很好的检测不涉及恶意活动的单个恶意域名。

以上检测方法均需要初始恶意域名种子, 文献[27]提出一种不使用任何恶意域名便可进行检测的方法。文献[27]仅通过观察企业网络内部主机与外部域名的可疑通信, 以此来构造域名主机二分图。根据给定的恶意种子或者是不使用任何恶意种子, 使用信念传播算法来发现更多潜在的恶意域名和受感染主机。

文献[24]相较于以上检测方法具有更高分类精度的原因在于其不仅利用主机查询域名的关联关系, 并选取节点之间的特征作为辅助信息。文献[24]提出基于客户端主机及其查询的域名之间的关联构造域名主机二分图 Segugio, 对图中部分节点进行标记, 结合例如基于主机行为、域名活动行为、IP 恶意性等的特征训练分类器, 以此来对图中未知的域名进行检测。Segugio 通过监视已知的受恶意软件感染的主机以及未感染主机的 DNS 查询行为, 有效地跟踪了 ISP 网络中由恶意软件控制的域名, 并学习发现新的恶意软件家族域名。

4.3.3 基于异构图的检测方法

上述检测方法大多仅使用了两种类型的节点和

一种类型的关系, 这种结构被称为同构网络, 由于仅存在一种关系的边, 同构网络分析方法具有局限性, 无法表达更多 DNS 数据的信息[2]。

基于这一局限性, 文献[119]使用查询域名的客户端主机 IP、域名及其映射的 IP 地址之间的关系构造两类二分图: DNS 查询响应图(DNS Query Response Graph, DQRG)和被动 DNS 图(Passive DNS Graph, PDG), 其中 DQRG 图由主机查询域名以及域名映射的 IP 地址之间的关联组成; PDG 图由域名映射的 CNAME 记录及 A 记录组成。应用马尔可夫随机场模型和信念传播算法计算图中节点的信誉分数, 结果表明, 该方法可以有效识别恶意软件域名及受感染的机。但是由于图中部分节点无法与具有先验知识的节点进行连接, 从而导致未得到有效评估的良性节点被误判为恶意节点, 该方法具有较高的误报率。

文献[2]使用更多能够表示多种类型节点和边的关系的异构信息网络(Heterogeneous Information Network, HIN)模型, 将客户端主机、域名、IP 地址及其不同的关系建模为异构信息网络模型, 并使用基于元路径的转导分类方法来检测与已知恶意域名有关联的潜在恶意域名。该方法不仅具有较高的分类精度, 还可以在较少标记域名的数据集中具有较高的稳健型。

文献[121]在文献[2]的基础上, 提出一种基于异构图卷积网络的系统 HGDom, 系统结合图卷机神经网络(Graph Convolutional Network, GCN)和基于元路径的注意力机制构建 MAGCN(GCN Meta-path-based Attention mechanism)模型, MAGCN 使用注意力机制来自适应的学习根据不同的元路径提取的各子图的重要性。结果表明, HGDOM 优于现有的基于图的恶意域检测方法, 其具有更高的准确性和检测能力。

4.3.4 总结与讨论

基于关联推理的检测方法具有更宏观的视角, 不仅使用了相对容易获得访问权限的聚合 DNS 数据, 还结合了域名、主机、IP 地址等之间的关联关系。基于关联推理的检测方法也存在一些缺点和问题, 构造图需要设置巧妙的图规则, 如果域名之间的关联较为虚弱或者存在不相关的关联, 则会导致较高的误报率; 设置较为限制的关联规则将会忽略许多潜在的恶意域名[21]。基于关联推理的检测方法涉及到的恶意域名的范围有限, 只能检测到与图中恶意域名节点有关联的恶意域名, 无法检测到从未被已知恶意域名或主机查询的恶意域名或者是新注册还未参与恶意活动的域名[2]。

5 检测方法的评估准则

不同的检测方法在进行实验和方法评价时采用了不同的评估准则, 缺乏统一的评估维度和评估准则的系统梳理。因此, 本节对现有研究中使用的评估准则进行了整理总结。

现有研究工作通常使用准确率、精确率、召回率、*F1* 值等基于分类性能的评估准则对方法性能进行评估。除此之外, 还包括对检测方法的鲁棒性、方法是否容易被攻击者规避、在真实网络环境中的部署情况、与公开信誉系统的对比等基于真实环境的评估准则。因此, 本节将按照基于分类性能和基于真实环境这两类对评估准则进行总结。

5.1 基于分类性能的评估准则

基于分类性能的评估准则中, 方法性能的好坏取决于准确率、精确率、召回率、*F1* 值、误报率、漏报率等评估准则。准确率(*Accuracy*)指的是被正确标记的样本数占总样本数的比率; 精确率(*Precision*)指的是被正确标记的良性样本数占被标记为良性样本数的比率; 召回率(*Recall*)指的是被正确标记的良性样本数占良性样本数的比率; *F1* 值(*F1-Score*)用来衡量精确率和召回率之间的关系, 被定义为 *2*(Precision*Recall)/(Precision+Recall)*; 误报率(*False Positive Rate, FPR*)指的是恶意样本被错误标记的个数占整体恶意样本的比率; 漏报率(*False Negative Rate, FNR*)指的是良性样本被错误标记占整体良性样本的比率。研究人员通常使用这些评估准则进行方法性能的评估, 希望其检测方法在具有高准确率的同时具有较低的误报率及漏报率。这些参数之间呈正负相关, 例如增强方法准确率的同时可能会导致误报率和漏报率的增加, 因此如何权衡方法的评估准则取决于研究人员的目标需求。

研究人员在构造检测方法时选取的特征、规则等对检测方法的性能至关重要。例如选取能够有效区分恶意域名的特征能使依赖特征的检测方法具有较高的性能, 使用不相关的特征可能会降低方法的准确性且消耗计算资源。因此研究人员会对所选取的特征进行评估[24,60,68,122-123], 通过构造单个特征的分类模型, 根据模型的准确率等性能对特征进行选择[2,16,18,27]。部分检测方法使用基于机器学习算法, 例如随机森林算法中能够对特征重要性进行排序的方法, 从而获得各特征对训练生成的分类模型的影响。选取能够使恶意域名之间形成强关联的关联规

则, 从而使构造的图更为紧密, 因此研究人员会对其所选择的关联规则进行评估[2,21,26-27,68,90,116,119]。例如文献[116]通过构造三种域名之间的关联规则, 对其形成的图进行基准测试, 从而发现具有较高准确精度的规则。

研究人员需要衡量特征、规则等的度量标准的有效性及计算资源之间的关系, 选取不同特征集的组合及关联规则对方法性能进行评估, 以此来进行精简计算, 实现以相对较低的准确率换取系统更高的效率。现有研究工作中均未提供可用于特征、规则评估的通用方法, 该方法必须同时考虑准确率、鲁棒性、是否易被攻击者规避等准则, 以此来对特征及规则进行全面性能的评估。

5.2 基于真实环境的评估准则

一个具有较高准确率以及较低误报率的检测方法, 在实际使用时还需要考虑检测方法的鲁棒性等评估准则, 即是否可以在不同的环境下仍然具有稳定的高性能[14,24,114]。例如某些检测方法仅适用于特定的时间及空间数据集, 则该方法鲁棒性较差。文献[24]为了评估其系统 Segugio 的准确性和通用性, 对在给定网络上训练的 Segugio 进行跨时间和跨网络测试, 结果证明 Segugio 在 0.1%的误报下始终能够达到 92%的准确率。HinDom[2]为了测试标签噪声的鲁棒性, 通过保留 70%的标签信息, 随机更改 kd% 特定比例的样本标签信息, 测试训练方法的准确率; 实验表明此方法在处理标签噪声时仍然可以保持相对稳定的性能, 证明该检测方法在面对标记数量较少的数据集时仍然具有较高的鲁棒性。

研究人员通常还会对其检测方法是否易被攻击者所规避进行评估。例如在基于动态特征的检测方法中, 特征的鲁棒性对检测方法是否易被规避至关重要。选取易被攻击者规避的特征容易导致较高的漏报率, 文献[67]通过观察新的恶意软件与良性进程之间新的特征差异, 从而调整其检测特征及方法, 以提高检测方法的鲁棒性。

真实场景的基准测试也常用于检测方法的有效性。通常做法是将检测系统部署在真实网络中, 以证明其在真实网络环境中的可用性以及检测新的恶意域名的能力[2-3,16,24,112]。研究人员通常会将其在真实网络环境中检测的结果与公开的黑名单、信誉系统进行对比, 以此来证明系统可以比黑名单更早的发现恶意域名[19-20,24,60]。例如文献[16]将系统 Exposure 与其他 11 个公开黑名单的检测时间进行了比较, 对比发现, 通过 Exposure 检测到的域名总数约为 5 万, 其中超过 50%的内容仅通过 Exposure 检测到。

5.3 总结与讨论

使用诸如误报率、漏报率等的评估准则时, 仍然会存在一定的局限性。研究人员采用自定义的形式对数据集进行标记, 设置定义不规范的黑白名单容易产生噪声, 即如果对某些域名进行错误标记, 则将会导致较高的误报率。由于庞大的实验数据量, 手动对误报率进行审核存在较大的困难。

在真实网络环境下进行系统检测时, 由于数据量较大, 很多检测系统会在检测时对数据集进行过滤。过滤规则会减少大量的数据量, 但是也遗漏了某些恶意域名, 过滤掉这些域名可能会增加检测方法的漏报率。因此误报率和漏报率等评估准则也只能在一定程度上提供对方法性能的参考。

6 讨论

目前, 恶意域名检测研究领域已经提出许多检测方法, 且这些检测方法均取得了较好的效果, 但是在数据集标记、检测方法中仍然存在一些问题。本文从以下方面对恶意域名检测的研究进行讨论。

(1) 数据集的标记

在恶意域名检测中, 大多数检测方法均需要使用标记的数据集从而对检测模型进行训练。然而, 由于训练期间观察到的域名数据量较大、全域名标记较为困难、手工标记成本较高、缺乏统一的参考标准等问题, 导致如何对数据集进行有效标记仍然是恶意域名检测方法中的一大困难。

研究人员通过建立参考标准(Ground Truth,GT)来对域名进行恶意性判定。如 3.1 节所述, 恶意域和良性域通常从公共黑白名单、动态构建恶意域、流行域中前 k 个域、信誉系统和公共情报网站中获得, 使用这些信息对数据集进行标记。但是由于标签来源及准确性尚未形成统一标准, 参考标准的建立仍然存在较大挑战。

文献[17,67,112,114]等采用监督学习算法, 该算法要求标记完整的训练集对分类器进行训练。如果选取的训练集具有一定的局限性, 则容易产生过拟合, 从而导致分类器性能较差。为了减少人工标记的成本, 研究人员使用半监督学习[2,21,26,68,116,119], 即仅使用少量标记数据集便可对域名进行检测, 这些检测方法在准确率等的性能上均有所下降。例如 HinDom 利用基于元路径的转导分类方法更好地利用了未标记样本的结构信息, 在标签数量较少的情况下, HinDom 的准确率等检测性能均有所下降。

部分文献使用聚类算法和半监督学习算法相结合的方法[21,27,90], 例如文献[90]提出了一种半手动标

记方法, 使用聚类算法和特征集将构建的图聚类为两个集群: 恶意域和良性域组件, 以此来添加标签, 通过查看所提取特征的值再对标签进行手动验证。这些方法试图使用较少的标记数据集来对模型进行训练。无监督学习不依赖于标记的数据集, 直接对无标签数据进行学习分类[85,98,123]。但是聚类算法较难设计, 在已有文献中并不普遍, 且性能一般。

如何设计能够在较少标记域名的情况下仍然可以有效的检测恶意域这一问题仍然需要进一步努力。研究人员使用半监督学习[2,21,26,68,116,119]、聚类[85,98,123]、图 [27,115-118]等方法, 可以在仅有部分已知恶意域名种子时仍然能对大量未知恶意域名进行检测。因此可着重考虑使用半监督学习结合聚类等的方法对含有少量标记域名的数据集进行训练检测。

(2) 不平衡数据的检测

现有检测方法在一定程度上取得了优异的效果, 但较少考虑数据不平衡的问题。在实际的网络环境中, 恶意域名的数量远小于良性域名, 现有检测方法通常使用数量相匹配的恶意域名及良性域名进行模型训练, 从而导致训练出的检测方法应用在真实网络环境中性能较差[2,100,111]。例如文献[2]在对恶意域进行多分类问题时, 发现大多数错误分类的原因是因为不同类别的域之间的数据量相差较大导致。

通常有两种方法可以解决数据不平衡问题: 第一种来自算法层, 通过修改算法在数据集上的偏差从而使决策平面趋向于少数类样本; 第二种方法来自数据层, 通过对不平衡的数据进行重采样来达到数据平衡。

在算法层对不平衡数据进行处理, 例如文献[106]在对 AGD 的检测中, 非 DGA 生成的域远超过由 DGA 生成的域, 不平衡比例高达 1∶1000, 通过使用 LSTM.MI 算法解决对 AGD 进行检测时存在的类不平衡问题。在数据层的方法中, 使用重采样来对不平衡数据进行处理。重采样包括欠采样和过采样, 欠采样的思想是从原始数据集中删除多数类样本, 而过采样的思想是在原始数据集中增加少数类样本。例如文献[100]使用改进的 EasyEnsemble 方法将集成学习与欠采样相结合, 以学习不平衡的被动 DNS 流量数据并生成可检测恶意域的分类模型。

研究表明, 不平衡数据的解决方法同样适用于恶意域的数据不平衡问题。因此, 针对域名检测中数据不平衡这一问题, 可以综合考虑对数据层及算法层进行结合、改进, 从而提高检测模型的性能。

(3) 检测延迟问题

现有检测方法中, 通常需要一定时间的观察期来对检测模型进行训练[16,25], 例如基于规则发现的检测方法中, 规则的生成需要时间积累; 基于动态特征的检测方法中, 通过学习恶意域名的行为特征对模型进行训练后才能进行检测; 基于关联推理的检测方法同样不能做到实时监测, 需要经过一段时间的训练才能进行检测。

许多恶意域名仅工作较短的时间, 当被检测为恶意时, 该域名已经达到其目的, 因此以上方法在检测这类域的过程中均具有较大的延迟性。对从注册到完成任务不足一天的域名进行检测, 一系列检测方法旨在从域名的注册阶段对其进行检测[60,84-86], 但是仅依靠注册信息进行检测的方法准确率通常较低, 且伴随着较高的误报率, 因此如何有效的检测短时间恶意域名仍存在较大的问题。

研究人员通过设置过滤规则[2,16,85], 使用域名公共黑白名单、自定义恶意域名、威胁情报数据库等对数据执行预处理, 以此过滤真实网络世界中产生的大量良性域流量。通过减少数据流量, 提高计算速率, 从而实现更高的检测效率。

考虑到攻击者的适应性, 检测模型必须定期进行训练、调整, 以此来防御攻击者的躲避策略。通过对检测模型设置训练周期、调整训练时间窗口[2,121]等方式不断更新, 从而减少检测延迟时间, 使其达到较高性能。

针对这一问题, 可以考虑在数据预处理阶段设置规则、修剪图中的冗余信息, 从而减少数据量, 过滤无效数据; 通过使用图嵌入, 将高维图数据映射为低维向量的方式减轻数据计算量, 从而提高模型训练的速率, 从而减轻模型的检测延迟问题。

7 结束语

目前, 对于恶意域名的检测技术的研究随着恶意行为的逐渐泛滥变得越来越重要。由于域名系统被攻击者广泛使用, 使用 DNS 数据对恶意域名进行检测的方法被广泛提出。本文主要针对恶意域名检测技术展进行深入讨论, 对 DNS 数据按照收集方式和位置的不同进行划分: 按照恶意域名检测技术的不同将现有的检测技术进行划分, 对各类方法进行详细介绍; 然后对现有检测方法的评估准则进行整理总结; 最后提出现有检测方法中仍然存在的问题和挑战。从这些角度出发, 可以对恶意域名检测现状进行更详细的了解。本文提供了对该领域的深入概述, 并对现存的问题进行了讨论总结, 希望本次调查将有助于未来的研究工作, 更有效的对抗利用恶意域名的攻击。

致 谢 感谢中国科学院网络测评技术重点实验室的各位老师和同学提出的有益建议。感谢审稿专家和编辑部老师对本文提出的有益建议及指导。

参考文献

[1] Mockapetris P V. DNS Encoding of Network Names and other Types[J]. *RFC*, 1989, 1101: 1-14.

[2] Sun X Q, Tong M K, Yang J H. HinDom: A Robust Malicious Domain Detection System Based on Heterogeneous Information Network with Transductive Classification[EB/OL]. 2019: arXiv: 1909.01590. https://arxiv.org/abs/1909.01590

[3] Antonakakis M, Perdisci R, Nadji Y, et al. From Throw-Away Traffic to Bots: Detecting the Rise of DGA-Based Malware[C]. *The 21st USENIX conference on Security symposium*, 2012: 24.

[4] Arends R, Austein R, Larson M, et al. DNS Security Introduction and Requirements[J]. *RFC*, 2005, 4033: 1-21.

[5] Zhao G, Xu K, Xu L, et al. Detecting APT Malware Infections Based on Malicious DNS and Traffic Analysis[J]. *IEEE Access*, 3: 1132-1142.

[6] Kara A M, Binsalleeh H, Mannan M, et al. Detection of malicious payload distribution channels in DNS[C]. *2014 IEEE International Conference on Communications*, 2014: 853-858.

[7] Hao S, Syed N A, Feamster N, et al. Detecting Spammers with SNARE: Spatio-Temporal Network-Level Automatic Reputation Engine[C]. *The 18th conference on USENIX security symposium*, 2009: 101-118.

[8] Qian Z , Mao Z M , Xie Y , et al. On Network-level Clusters for Spam Detection[C]. *Network & Distributed System Security Symposium*. DBLP, 2010.

[9] Zhauniarovich Y, Khalil I, Yu T, et al. A Survey on Malicious Domains Detection through DNS Data Analysis[J]. *ACM Computing Surveys*, 2019, 51(4): 67.

[10] Ramachandran A, Dagon D, Feamster N. Can DNS-based blacklists keep up with bots?[C]. *CEAS 2006 - The Third Conference on Email and Anti-Spam*, July 27-28, 2006, Mountain View, California, USA. DBLP, 2006.

[11] Sato K, Ishibashi K, Toyono T, et al. Extending Black Domain Name List by Using Co-Occurrence Relation between DNS Queries[J]. *IEICE Transactions on Communications*, 2012, E95-B(3): 794-802.

[12] Dietrich C J, Rossow C. Empirical Research of IP Blacklists[M]. ISSE 2008 Securing Electronic Business Processes. Wiesbaden: Vieweg+Teubner, 2009: 163-171.

[13] Holz T, Gorecki C, Rieck K, et al. Measuring and Detecting Fast-Flux Service Networks[J]. *Ndss*, 2008, 1(5):487 - 492.

[14] Yadav S, Reddy A K K, Reddy A L N, et al. Detecting Algorithmically Generated Malicious Domain Names[C]. *The 10th ACM SIGCOMM conference on Internet measurement*, 2010: 48-61.

[15] Zdrnja B, Brownlee N, Wessels D. Passive Monitoring of DNS Anomalies[M]. Detection of Intrusions and Malware, and Vulnerability Assessment. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007: 129-139.

[16] Bilge L, Sen S, Balzarotti D, et al. Exposure: A Passive DNS Analysis Service to Detect and Report Malicious Domains[J]. *ACM Transactions on Information and System Security*, 2014, 16(4): 14.

[17] Antonakakis M, Perdisci R, Dagon D, et al. Building a Dynamic Reputation System for DNS[C]. *The 19th USENIX conference on Security*, 2010: 18.

[18] Antonakakis M, Perdisci R, Lee W K, et al. Detecting Malware Domains at the Upper DNS Hierarchy[C]. *The 20th USENIX conference on Security*, 2011: 27.

[19] Kountouras A, Kintis P, Lever C, et al. Enabling Network Security through Active DNS Datasets[M]. Research in Attacks, Intrusions, and Defenses. Cham: Springer International Publishing, 2016: 188-208.

[20] Gao H Y, Yegneswaran V, Jiang J, et al. Reexamining DNS from a Global Recursive Resolver Perspective[J]. *IEEE/ACM Transactions on Networking*, 2016, 24(1): 43-57.

[21] Khalil I M, Guan B, Nabeel M, et al. A Domain is only as Good as Its Buddies: Detecting Stealthy Malicious Domains via Graph Inference[C]. *The Eighth ACM Conference on Data and Application Security and Privacy*, 2018: 330-341.

[22] Chia P H, Knapskog S J. re-Evaluating the Wisdom of Crowds in Assessing Web Security[M]. Financial Cryptography and Data Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012: 299-314.

[23] Konte M, Feamster N, Jung J. Dynamics of Online Scam Hosting Infrastructure[M]. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009: 219-228.

[24] Rahbarinia B, Perdisci R, Antonakakis M, et al. Segugio: efficient behavior-based tracking of malware-control domains in large ISP networks[C]. *2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 2015: 403-414.

[25] 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, NDSS* 2011, 2011: 1-17.

[26] Manadhata P K, Yadav S, Rao P, et al. Detecting Malicious Domains via Graph Inference[C]. *Computer Security - ESORICS 2014*, : 1-18.

[27] Oprea A, Li Z, Yen T F, et al. Detection of early-stage enterprise infection by mining large-scale log data[C]. *2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 2015: 45-56.

[28] Rahbarinia B, Perdisci R, Antonakakis M. Efficient and Accurate Behavior-Based Tracking of Malware-Control Domains in Large ISP Networks[J]. *ACM Transactions on Privacy and Security*, 2016, 19(2): 4.

[29] Mockapetris P. Domain Names - Implementation and Specification[J]. *RFC*, 1987, 1035: 1-55.

[30] Sood A K, Zeadally S. A Taxonomy of Domain-Generation Algorithms[J]. *IEEE Security & Privacy*, 2016, 14(4): 46-53.

[31] P. Porras, H. Saidi, and V. Yegneswaran. An Analysis of Conficker's Logic and Rendezvous Points. Technical report,mar 2009.

[32] Porras P , Saidi H , Yegneswaran V . Conficker C analysis[J]. *Sri International*, 2009, 1: 1-1.

[33] Stone-Gross B, Cova M, Cavallaro L, et al. Your Botnet is my Botnet: Analysis of a Botnet Takeover[C]. *The 16th ACM conference on Computer and communications security*, 2009: 635-647.

[34] Yadav S, Reddy A K K, Reddy A L N, et al. Detecting Algorithmically Generated Domain-Flux Attacks with DNS Traffic Analysis[J]. *IEEE/ACM Transactions on Networking*, 2012, 20(5): 1663-1677.

[35] Schiavoni S, Maggi F, Cavallaro L, et al. Phoenix: DGA-Based Botnet Tracking and Intelligence[M]. Detection of Intrusions and Malware, and Vulnerability Assessment. Cham: Springer International Publishing, 2014: 192-211.

[36] Mowbray M, Hagen J, Processing C A. Finding domain-generation algorithms by looking at length distribution[C]. *2014 IEEE International Symposium on Software Reliability Engineering Workshops*, 2014: 395-400.

[37] Lison P, Mavroeidis V. Automatic Detection of Malware-Generated Domains with Recurrent Neural Models[EB/OL]. 2017: arXiv: 1709.07102. https://arxiv.org/abs/1709.07102.

[38] Anderson H S, Woodbridge J, Filar B. DeepDGA: Adversarially-Tuned Domain Generation and Detection[C]. *The 2016 ACM Workshop on Artificial Intelligence and Security*, 2016: 13-21.

[39] Bottazzi G, Italiano G F, Communication N A B T, et al. Fast mining of large-scale logs for botnet detection: A field study[C]. *2015 IEEE International Conference on Computer and Information Technology*; *Ubiquitous Computing and Communications*; *Dependable*, *Autonomic and Secure Computing*; *Pervasive Intelligence and Computing*, 2015: 1989-1996.

[40] Zhao K J, Ge L S, Qin F L, et al. Deep Model for DGA Botnet Detection Based on Word-Hashing[J]. *Journal of Southeast University* (*Natural Science Edition*), 2017, 47(S1): 30-33.
(赵科军, 葛连升, 秦丰林, 等. 基于 word-hashing 的 DGA 僵尸网络深度检测模型[J]. *东南大学学报(自然科学版)*, 2017, 47(S1): 30-33.)

[41] Amazon Web Services, Inc. AWS | Alexa Top Sites - Up- to-date lists of the top sites on the web. https://www.alexa.com/topsites.

[42] Perdisci R, Corona I, Giacinto G. Early Detection of Malicious Flux Networks via Large-Scale Passive DNS Traffic Analysis[J]. *IEEE Transactions on Dependable and Secure Computing*, 2012, 9(5): 714-726.

[43] SURBL. (2016) SURBL - URI Reputation Data. [Online]. Available: http://www.surbl.org.

[44] Malware Domain List. Retrieved from https://www. malwaredomainlist.com/.

[45] Malc0de, https://www.malc0de.org/.

[46] CleanMX. Spam-Filter Anti-Spam Virenschutz. https://www. accessify.com/c/clean-mx.dehttp://clean-mx.de.

[47] URLVoid: Website reputation checker tool. Retrieved from http://www.urlvoid.com/.

[48] PhishTank, https://www.phishtank.com/.

[49] APWG. 2017. APWG: Cross-industry Global Group Supporting Tackling the Phishing Menace. https://apwg.org.

[50] The Spamhaus Project Ltd. (2016) The Domain Block List. [Online]. Available: https://www.spamhaus.org/dbl/.

[51] ZeuS Tracker, https://feedreader.com/observe/zeustracker.abuse.chhttps://zeustracker.abuse.ch.

[52] Ransomware Tracker, https://www.accessify.com/a/ ransomwaretracker.abuse.chhttps://ransomwaretracker.abuse.ch/.

[53] Cert.at Conficker, http://www.cert.at/static/conficker/all domains.txt.

[54] StopBadware. StopBadware: A Nonprofit Anti-malware Organization.https://www.stopbadware.org.

[55] Google Safe Browsing. Retrieved from https://developers.google.com/safe-browsing.

[56] Web of Trust (WOT)—Crowdsourced web safety. Retrieved from https://www.mywot.com/.

[57] McAfee SiteAdvisor.Retrieved from http://www.siteadvisor.com/.

[58] The Secure Domain Foundation.https://securedomain.org/.

[59] Ferrell, Paul S. APT INFECTION DISCOVERY USING DNS DATA[J]. *World Manufacturing Engineering & Market*, 2013.

[60] Hao S, Kantchelian A, Miller B, et al. PREDATOR: Proactive Recognition and Elimination of Domain Abuse at Time-of- Registration[C]. *The 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016: 1568-1579.

[61] Zhou C L, Chen K, Gong X X, et al. Detection of Fast-Flux Domains Based on Passive DNS Analysis[J]. *Acta Scientiarum Naturalium Universitatis Pekinensis*, 2016, 52(3): 396-402.
(周昌令, 陈恺, 公绪晓, 等. 基于 Passive DNS 的速变域名检测[J]. *北京大学学报(自然科学版)*, 2016, 52(3): 396-402.)

[62] Perdisci R, Corona I, Dagon D, et al. Detecting malicious flux service networks through passive analysis of recursive DNS traces[C]. *2009 Annual Computer Security Applications Conference*, 2010: 311-320.

[63] Mahjoub D, Communication N A B T, Processing C A. Monitoring a fast flux botnet using recursive and passive DNS: A case study[C]. *2013 APWG eCrime Researchers Summit*, 2014: 1-9.

[64] Prieto I, Magaña E, Morató D, et al. Botnet detection based on DNS records and active probing[C]. *The International Conference on Security and Cryptography*, 2014: 307-316.

[65] Choi H, Lee H, Lee H, et al. Botnet detection by monitoring group activities in DNS traffic[C]. *7th IEEE International Conference on Computer and Information Technology*, 2007: 715-720.

[66] Krishnan S, Taylor T, Monrose F, et al. Crossing the threshold: Detecting network malfeasance via sequential hypothesis testing[C]. *2013 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks* (*DSN*), 2013: 1-12.

[67] Sivakorn S, Jee K, Sun Y X, et al. Countering Malicious Processes with Process-DNS Association[C], *NDSS,* 2019.

[68] Lee J, Lee H. GMAD: Graph-Based Malware Activity Detection by DNS Traffic Analysis[J]. *Computer Communications*, 2014, 49: 33-47.

[69] Nagaraja S, Mittal P, Hong C Y, et al. BotGrep: Finding P2P Bots with Structured Graph Analysis[C]. *The 19th USENIX conference on Security*, 2010: 7.

[70] Yarochkin F, Kropotov V, Huang Y, et al. Investigating DNS traffic anomalies for malicious activities[C]. *2013 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop*, 2013: 1-7.

[71] Moura G C M, Müller M, Wullink M, et al. nDEWS: A new do-

mains early warning system for TLDs[C]. *NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium*, 2016: 1061-1066.

[72] Google Public DNS. Retrieved from https://developers.google. com/speed/public- dns/.

[73] Farsight Security, Inc. DNS Database. https://www.farsightsecurity. com.

[74] Ramachandran A, Feamster N, Dagon D. Detecting Botnet Membership with DNSBL Counterintelligence[M]. Botnet Detection. Boston, MA: Springer US, 2007: 131-142.

[75] Jung J, Sit E. An Empirical Study of Spam Traffic and the Use of DNS Black Lists[C]. *The 4th ACM SIGCOMM conference on Internet measurement*, 2004: 370-375.

[76] Sinha S, Bailey M, Jahanian F, et al. Shades of grey: On the effectiveness of reputation-based "blacklists"[C]. *2008 3rd International Conference on Malicious and Unwanted Software*, 2008: 57-64.

[77] Team Cymru. Retrieved from http://www.team-cymru.org/.

[78] iPlane.http://iplane.cs.washington.edu/data/data.html, 2015.

[79] MaxMind. GeoLite2 Databases. Retrieved from http://www. maxmind.com.

[80] Ishibashi K, Toyono T, Toyama K, et al. Detecting Mass-Mailing Worm Infected Hosts by Mining DNS Traffic Data[C]. *The 2005 ACM SIGCOMM workshop on Mining network data*, 2005: 159-164.

[81] Dagon, David. Botnet Detection and Response The Network is the Infection[J]. *Oarc Workshop*, 2005.

[82] Antoine Schonewille, Dirk Jan van Helmond. The domain name service as an IDS[R]. Amsterdam: Master System and Network Engineering at the University, 2006.

[83] Villamarin-Salomon R, Brustoloni J C, Communication N A B T, et al. Identifying botnets using anomaly detection techniques applied to DNS traffic[C]. *2008 5th IEEE Consumer Communications and Networking Conference*, 2008: 476-481.

[84] Vissers T, Spooren J, Agten P, et al. Exploring the Ecosystem of Malicious Domain Registrations in the.eu TLD[M]. Research in Attacks, Intrusions, and Defenses. Cham: Springer International Publishing, 2017: 472-493.

[85] Felegyhazi M, Kreibich C, Paxson V. On the Potential of Proactive Domain Blacklisting[C]. *The 3rd USENIX conference on Large-scale exploits and emergent threats*: *botnets*, *spyware*, *worms*, *and more*, 2010: 6.

[86] Hao S, Feamster N, Pandrangi R. Monitoring the Initial DNS Behavior of Malicious Domains[C]. *The 2011 ACM SIGCOMM conference on Internet measurement conference*, 2011: 269-278.

[87] XU, W., SANDERS, K., AND ZHANG, Y. We Know It Before You Do: Predicting Malicious Domains[C]. In *Proceedings of the 24th Virus Bulletin Conference*, 2014: 73-77.

[88] WHOISDataCenter. https://w3techs.com/sites/info/whoisdatacenter. comhttps://whoisdatacenter.com.

[89] Whois History, https://research.domaintools.com.

[90] Stevanovic M, Pedersen J M, D'Alconzo A, et al. On the Ground Truth Problem of Malicious DNS Traffic Analysis[J]. *Computers & Security*, 2015, 55: 142-158.

[91] DomainTools.https://www.domaintools.com.

[92] Who.is. https://who.is.

[93] NameJet Domain Name Aftermarket. http://www.namejet.com.

[94] Verisign Domain Countdown. http://domaincountdown. verisignlabs. com.

[95] Hao S, Thomas M, Paxson V, et al. Understanding the Domain Registration Behavior of Spammers[C]. *The 2013 conference on Internet measurement conference*, 2013: 63-76.

[96] Grill M, Nikolaev I, Valeros V, et al. Detecting DGA malware using NetFlow[C]. *2015 IFIP/IEEE International Symposium on Integrated Network Management*, 2015: 1304-1309.

[97] S. Yadav and A. N. Reddy, Winning with DNS failures: Strategies for faster botnet detection[C]. in *Proc. SecureComm*, 2011, 446-459.

[98] Choi H, Lee H. Identifying Botnets by Capturing Group Activities in DNS Traffic[J]. *Computer Networks*, 2012, 56(1): 20-33.

[99] Erquiaga M J, Catania C, García S, et al. Detecting DGA malware traffic through behavioral models[C]. *2016 IEEE Biennial Congress of Argentina*, 2016: 1-6.

[100] Liu Z Y, Zeng Y F, Zhang P F, et al. An Imbalanced Malicious Domains Detection Method Based on Passive DNS Traffic Analysis[J]. *Security and Communication Networks*, 2018, 2018: 1-7.

[101] Passerini E, Paleari R, Martignoni L, et al. FluXOR: Detecting and Monitoring Fast-Flux Service Networks[M]. Detection of Intrusions and Malware, and Vulnerability Assessment. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008: 186-206.

[102] Stalmans E, Irwin B. A Framework for DNS Based Detection and Mitigation of Malware Infections on a Network[C]. *2011 Information Security for South Africa*, 2011: 1-8.

[103] Sharifnya R, Abadi M. DFBotKiller: Domain-Flux Botnet Detection Based on the History of Group Activities and Failures in DNS Traffic[J]. *Digital Investigation*, 2015, 12: 15-26.

[104] Tong V, Nguyen G. A Method for Detecting DGA Botnet Based on Semantic and Cluster Analysis[C]. *The 7th Symposium on Information and Communication Technology*, 2016: 272-277.

[105] Chiba D , Hasegawa A A , Koide T , et al. DomainScouter: Understanding the Risks of Deceptive IDNs[C]. *22nd International Symposium on Research in Attacks, Intrusions and Defenses* 2019, 2019: 413-426.

[106] Chen L H, Cheng H, Fang Y Q. Detecting Domain Generation Algorithm Based on Attention Mechanism[J]. *Journal of East China University of Science and Technology*, 2019, 45(3): 478-485.
(陈立皇, 程华, 房一泉. 基于注意力机制的DGA域名检测算法[J]. *华东理工大学学报(自然科学版)*, 2019, 45(3): 478-485.)

[107] Bharathi B, Bhuvana J. Domain Name Detection and Classification Using Deep Neural Networks[M]. Communications in Computer and Information Science. Singapore: Springer Singapore, 2019: 678-686.

[108] Vinayakumar R, Soman K P, Poornachandran P, et al. Improved DGA Domain Names Detection and Categorization Using Deep Learning Architectures with Classical Machine Learning Algorithms[M]. Advanced Sciences and Technologies for Security Applications. Cham: Springer International Publishing, 2019: 161-192.

[109] Zeng F . Classification for DGA-Based Malicious Domain Names with Deep Learning Architectures[C]. *2017 第二届应用数学与信息技术国际会议*. 2017: 5.

[110] Vinayakumar R, Soman K P, Poornachandran P, et al. Detecting Malicious Domain Names Using Deep Learning Approaches at Scale[J]. *Journal of Intelligent & Fuzzy Systems*: *Applications in Engineering and Technology*, 2018, 34(3): 1355-1367.

[111] Tran D, Mac H, Tong V, et al. A LSTM Based Framework for Handling Multiclass Imbalance in DGA Botnet Detection[J]. *Neurocomputing*, 2018, 275: 2401-2413.

[112] Schüppen S, Teubert D, Herrmann P, et al. FANCI: Feature-Based Automated NXDomain Classification and Intelligence[C]. *The 27th USENIX Conference on Security Symposium*, 2018: 1165-1181.

[113] Wang Y Y, Wu C J, Liu Q H, et al. Overview of Malicious Domain Name Detection and Application[J]. *Computer Applications and Software*, 2019, 36(9): 310-316.
(王媛媛, 吴春江, 刘启和, 等. 恶意域名检测研究与应用综述[J]. *计算机应用与软件*, 2019, 36(9): 310-316.)

[114] Liu D P, Li Z, Du K, et al. Don't Let one Rotten Apple Spoil the Whole Barrel: Towards Automated Detection of Shadowed Domains[C]. *The 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017: 537-552.

[115] Khalil I, Yu T, Guan B. Discovering Malicious Domains through Passive DNS Data Graph Analysis[C]. *The 11th ACM on Asia Conference on Computer and Communications Security*, 2016: 663-674.

[116] Mishsky I, Gal-Oz N, Gudes E. A Topology Based Flow Model for Computing Domain Reputation[M]. Data and Applications Security and Privacy XXIX. Cham: Springer International Publishing, 2015: 277-292.

[117] Liang Z Z, Zang T N, Zeng Y W. MalPortrait: Sketch Malicious Domain Portraits Based on Passive DNS Data[C]. *2020 IEEE Wireless Communications and Networking Conference*, 2020: 1-8.

[118] Peng C W, Yun X C, Zhang Y Z, et al. MalShoot: Shooting Malicious Domains through Graph Embedding on Passive DNS Data[M]. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Cham: Springer International Publishing, 2019: 488-503.

[119] Zou F T, Zhang S Y, Rao W X, et al. Detecting Malware Based on DNS Graph Mining[J]. *International Journal of Distributed Sensor Networks*, 2015, 2015: 1.

[120] Lee J, Kwon J, Shin H J, et al. Tracking Multiple C&C Botnets by Analyzing DNS Traffic[C]. *2010 6th IEEE Workshop on Secure Network Protocols*, 2010: 67-72.

[121] Sun X Q, Yang J H, Wang Z L, et al. HGDom: Heterogeneous Graph Convolutional Networks for Malicious Domain Detection[C]. *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium*, 2020: 1-9.

[122] Ma X B, Zhang J J, Tao J, et al. DNSRadar: Outsourcing Malicious Domain Detection Based on Distributed Cache-Footprints[J]. *IEEE Transactions on Information Forensics and Security*, 2014, 9(11): 1906-1921.

[123] Kwon J, Lee J, Lee H, et al. PsyBoG: A Scalable Botnet Detection Method for Large-Scale DNS Traffic[J]. *Computer Networks*, 2016, 97: 48-73.

王青 于 2018 年在河南大学软件工程方向获得学士学位。现在中国科学院信息工程研究所第六研究室攻读博士学位。研究领域为网络安全态势感知, 恶意域名检测等。Email: wangqing@iie.ac.cn

韩冬旭 于 2013 年在华北电力大学获得硕士学位。现任中国科学院信息工程研究所工程师, 并攻读网络安全方向博士学位。研究领域为网络攻击检测、网络安全态势感知等。Email: handongxu@iie.ac.cn

卢志刚 于 2010 年在中国科学院研究生院获得博士学位。现任中国科学院信息工程研究所高级工程师, 中国科学院网络空间安全学院副教授。研究领域为网络安全态势感知、网络攻击检测、移动终端安全等。Email: luzhigang@iie.ac.cn

姜波 于 2016 年在中国科学院大学计算机系统结构专业获得博士学位。现任中国科学院信息工程研究所副研究员。研究领域为网络安全态势感知、知识图谱、数据挖掘、行为分析等。Email: jiangbo@iie.ac.cn

董聪 于 2017 年在天津大学信息管理与信息系统(保密方向)专业获得学士学位。现在中国科学院信息工程研究所第六研究室攻读硕士学位。研究领域为网络安全态势感知、知识图谱等。Email: dongcong@iie.ac.cn

刘俊荣 于 2010 年在北京邮电大学获得硕士学位, 现任中国科学院信息工程研究所高级工程师。研究领域为网络安全态势感知, 网络安全可视化等。Email: liujunrong@iie.ac.cn

石文昌 于 2002 年在中科院软件所计算机软件与理论专业获得工学博士学位。现任中国人民大学信息学院教授。研究领域为网络空间系统安全, 研究兴趣包括系统安全、可信计算、数字取证、安全心理学。Email: wenchang@ruc.edu.cn

刘玉岭 于 2013 年在中国科学院软件研究所获得博士学位。现任中国科学院信息工程研究所高级工程师。研究领域为网络安全态势感知、网安大数据分析、安全测评认证等。Email:liuyuling@iie.ac.cn