计算机科学
COMPUTER SCIENCE

域名生成算法检测技术综述

汪绪先, 黄缙华, 翟优, 李础南, 王宇, 张宇鹏, 张翼鹏, 杨立群, 李舟军

引用本文

汪绪先, 黄缙华, 翟优, 李础南, 王宇, 张宇鹏, 张翼鹏, 杨立群, 李舟军. 域名生成算法检测技术综述[J]. 计算机科学, 2024, 51(8): 371-378.

WANG Xuxian, HUANG Jinhua, ZHAI You, LI Chu'nan, WANG Yu, ZHANG Yupeng, ZHANG Yipeng, YANG Liqun, LI Zhoujun. Survey of Detection Techniques for Domain Generation Algorithm[J]. Computer Science, 2024, 51(8): 371-378.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230700189

域名生成算法检测技术综述

汪绪先[1,2] 黄缙华[1,2] 翟 优[3] 李础南[4] 王 宇[3] 张宇鹏[4] 张翼鹏[5] 杨立群[4] 李舟军[3]

1 中国南方电网公司重点实验室电网自动化实验室 广州 510080
2 广东电网有限责任公司电力科学研究院 广州 510080
3 北京航空航天大学计算机学院 北京 100191
4 北京航空航天大学网络空间安全学院 北京 100191
5 北方工业大学信息学院 北京 100144
(13538889048@163.com)

摘 要 C&C服务器是网络攻击者用于控制僵尸主机的中间服务器,在僵尸网络中处于核心位置。为增强C&C服务器的隐蔽性,网络攻击者使用域名生成算法来隐藏C&C服务器地址。近年来,域名生成算法检测技术作为检测僵尸网络的重要手段,已经成为一个研究热点。首先,介绍了当前网络安全的发展态势和僵尸网络的拓扑结构。其次,介绍了域名生成算法和相关数据集。接着,介绍了域名生成算法检测技术的分类,并对这些检测技术进行总结综述。最后,探讨了现阶段域名生成算法检测技术存在的问题,并对未来研究方向进行了展望。

关键词:僵尸网络;C&C服务器;域名生成算法;域名生成算法检测;网络安全威胁
中图分类号 TP309

Survey of Detection Techniques for Domain Generation Algorithm

WANG Xuxian[1,2],HUANG Jinhua[1,2],ZHAI You[3],LI Chu'nan[4],WANG Yu[3],ZHANG Yupeng[4],ZHANG Yipeng[5],YANG Liqun[4] and LI Zhoujun[3]

1 Key Laboratory of Power Grid Automation Laboratory,China Southern Power Grid,Guangzhou 510080,China
2 Electric Power Research Institute,Guangdong Power Grid Co.,Ltd.,Guangzhou 510080,China
3 School of Computer Science and Engineering,Beihang University,Beijing 100191,China
4 School of Cyber Science and Technology,Beihang University,Beijing 100191,China
5 School of Information Science and Technology,North China University of Technology,Beijing 100144,China

Abstract The C&C server is an intermediate server used by cyber attackers to control bots,and plays a key role in botnet. In order to enhance the concealment of the C&C server,cyber attackers use domain generation algorithms to hide the IP address of C&C server. In recent years,domain generation algorithm detection technology,as an important means of detecting botnets,has become a research hotspot. This paper first introduces the current development trend of cyber security and the topological structure of botnets. Secondly,the domain generation algorithm and the related dataset are introduced. Then,the classification of domain generation algorithm detection techniques is introduced,and these detection techniques are summarized. Finally,the problems existing in the domain generation algorithm detection technology at the present stage are discussed,and the future research directions are prospected.

Keywords Botnet,Command and Control server,Domain generation algorithm,Domain generation algorithm detection,Cybersecurity threat

到稿日期:2023-07-25 返修日期:2024-05-18
基金项目:国家自然科学基金(U2333205,62302025,62276017);国家电网有限公司总部科技项目(5108-202303439A-3-2-ZN);南方电网公司科技项目(GDDKY2021KF03);2022绿盟科技"鲲鹏"科研基金(CCF-NSFOCUS202210)
This work was supported by the National Natural Science Foundation of China(U2333205,62302025,62276017),A fund project of State Grid Co.,Ltd. Technology R&D Project(5108-202303439A-3-2-ZN),Key Laboratory of Power Grid Automation of China Southern Power Grid Co.,Ltd.(GDDKY2021KF03) and 2022 CCF-NSFOCUS Kun-Peng Scientific Research Fund(CCF-NSFOCUS202210).
通信作者:杨立群(lqyang@buaa.edu.cn)

1 引言

近年来，移动互联网、工业互联网、物联网等技术飞速发展，联网设备急剧增多，对人们的生活和工作产生了深远影响，同时也引发了一系列网络安全问题。网络攻击者利用恶意软件攻击这些联网设备，进而组建僵尸网络(Botnet)，发起一系列网络攻击，如分布式拒绝服务攻击(Distributed Denial of Service，DDoS)[1]、挖矿[2]、垃圾邮件[3]、加密勒索[4]等。网络攻击者需要通过控制与命令(Command and Control，C&C)服务器间接控制这些被恶意软件感染的联网设备(被控主机)。如果C&C服务器被网络安全防御者发现并取缔(Take down或Sinkhole)，那么网络攻击者将失去对被控主机的控制。

僵尸网络通常由3部分组成：僵尸主机(Bot)、C&C服务器和僵尸网络控制者(Botmaster)。图1是一个简单的僵尸网络拓扑结构。C&C服务器在僵尸网络中处于关键位置。僵尸网络控制者通过C&C服务器发布攻击指令和接收数据，僵尸主机则通过C&C服务器获取攻击指令和回传数据。早期网络攻击者将C&C服务器地址等信息硬编码(Hard-code)在恶意程序源码(Source Code)中，这一方式虽然实现难度低，但很容易被检测封禁。为提升C&C服务器的隐蔽性，网络攻击者开始使用Fast-Flux[5]和域名生成算法(Domain Generation Algorithm，DGA)[6]。在僵尸网络控制者利用DGA生成的大量域名中，只有一小部分域名被用于实际C&C通信，僵尸主机按顺序查询这些域名并连接C&C服务器，直到找到可用的域名。使用DGA技术的僵尸网络被称为基于DGA的僵尸网络(DGA-based Botnet)，DGA生成的域名被称为算法生成域名(Algorithmically Generated Domain，AGD)或恶意域名[1)]。DGA技术的应用降低了C&C服务器被发现的风险，给网络防御带来了巨大挑战。

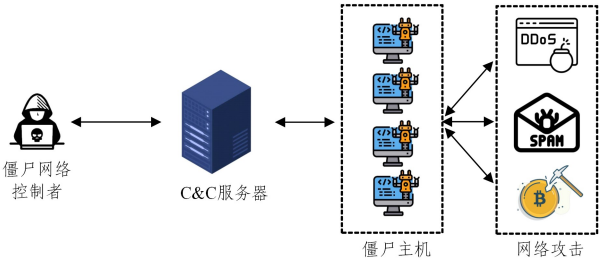

图1 僵尸网络结构示意图

Fig. 1 Diagram of botnet structure

僵尸网络的检测对于维护网络安全至关重要，检测手段主要包括：基于蜜罐的检测、基于签名的检测、基于异常行为的检测和基于DGA的检测等。DGA检测技术是用于发现DGA类型僵尸网络的一种重要手段，对于保障网络安全具有重要意义。

为检测僵尸网络，学术界和工业界对基于DGA的僵尸网络检测技术进行了深入研究，提出了众多DGA检测方法，涵盖统计分析、传统机器学习、深度学习等多种技术。虽然关于DGA检测技术的研究众多，但缺乏系统的整理、归纳、总结。Saeed等[7]对基于传统机器学习和深度学习的DGA检测技术进行了综述，但该综述存在调研不全面、覆盖面小、没有对数据集进行讨论的问题。Wang等[8]对基于域名字符串的DGA检测方法进行了综述，但该工作缺乏对基于域名附属信息的DGA检测方法的总结。总体而言，现有综述工作对DGA检测技术仍然缺乏系统性关注。本文着重关注DGA检测机制，从域名字符串和域名附属信息等角度对DGA检测技术进行系统的总结和分析，并对相关技术的发展方向进行展望。

本文第1章介绍网络安全发展趋势和僵尸网络基本情况，并引出了本文研究框架；第2章介绍域名生成算法；第3章介绍DGA检测常用的一些数据集；第4章对DGA检测技术进行系统的分析、归纳和总结；最后总结全文并展望未来。

2 域名生成算法概述

DGA是一种生成随机域名的算法，生成的域名常被用于网络攻击。网络攻击者使用DGA来增强隐蔽性，避免其恶意活动被检测或阻断。这种算法生成一系列看似随机的域名，恶意程序则通过这些域名与C&C服务器进行通信，获取指令或传输数据。网络攻击者使用DGA的目的是绕过安全防御系统的域名黑名单或基于签名的检测机制。安全防御系统通常会对已知恶意域名进行监测和封锁，因此网络攻击者使用DGA技术动态生成大量随机域名，使其难以被检测和屏蔽。

种子(Seed)是C&C服务器和恶意程序之间的共享秘密(参数集合)，被网络攻击者用来控制某个时间段内生成的域名。网络攻击者可以在预先设定好的时间间隔内使用这些域名与被控主机进行通信。常见的种子有两类：基于时间(Time Dependence)的种子和确定性(Determinism)种子。由于种子数值不断变化，所以DGA生成的域名也会不同。恶意软件通过周期性地利用DGA生成新的域名来保持与C&C服务器的连接。

为防止网络安全研究人员破解出域名的生成规律，DGA通常被设计得足够复杂。然而，研究人员仍然可以通过逆向工程、监测和分析大量的域名生成活动等方式，破解生成算法的模式和规律，进而提前预测可能生成的域名。例如Plohmann等[9]通过逆向工程(reverse engineering)分析了大量DGA及其变体，并将DGA技术分成了4类：基于算术(Arithmetic-based)的域名生成算法、基于哈希(Hash-based)的域名生成算法、基于字典(Wordlist-based)的域名生成算法，以及基于排列(Permutation-based)的域名生成算法。

1)基于算术的域名生成算法即通过算术计算一系列值，这些值要么具有可用于域名的直接ASCII码表示，要么指定一个或多个硬编码数组中的偏移量，构成域名的字母表。基于算术的域名生成算法是最常见的域名生成算法类型。例如，CryptoLocker[10]恶意软件家族使用基于算术的域名生成算法来生成域名，该算法用当前时间作为种子，从英文字母表中选取字符，组成一个长度在12-15之间的字符串，并通过设置频率来控制每天生成的域名总量，生成的域名形式如：

1) 本文中的恶意域名不包括钓鱼网站和非法网站等类型域名，仅指算法生成域名

“qgrkvevybtvckik. org”。

2）基于哈希的域名生成算法使用哈希值的十六进制表示来生成域名，哈希值主要由 MD5 和 SHA256 两种算法生成。例如，Dyre[11] 恶意软件家族使用基于哈希的域名生成算法来生成域名，该算法首先使用一个共享数字进行模 26 运算，根据模运算结果选取二级域名的首字母，接着通过对当前日期和共享数字做 SHA256 哈希运算，选取哈希值的 4-34 位作为二级域名的第 2-32 位，最后添加顶级域即可得到完整的域名，如“q14d2b3366d88cfcbcbf0c2133551e40da. cc”。

3）基于字典的域名生成算法是一种新型域名生成算法，其通过拼接字典中的一个或多个单词组成域名，从而减少域名的随机性，增强伪装性。这些字典有两种获取渠道，一是直接嵌入到恶意软件的二进制文件中，二是可公开访问的数据源。如 Suppobox[12] 恶意软件家族就使用基于字典的域名生成算法来生成域名，使用时间戳作为随机数种子，进行多次异或操作来计算偏移，从而决定对字典中单词的选择。其生成的域名包含两个单词序列，长度在 7-30 之间，顶级域主要有“. net”和“. ru”两种。以 Suppobox 生成的域名“thinkgoodbye. ru”为例，生成这个域名所使用的字典包含了“think”和“goodbye”两个英文单词，顶级域为“. ru”。

4）基于排列的域名生成算法通过对原始域名进行排列操作，进而派生出所有可能的域名，例如 VolatileCedar[13] 恶意软件家族就使用基于排列的域名生成算法。该算法通过对硬编码在恶意程序源码中的域名二级域标签进行排列操作，从而生成新的二级域标签。例如对“dotnetexplorer. net”域名的二级域标签“dotnetexplorer”进行排列来生成新的二级域标签，最终生成的域名如“erdotntexplore. net”。

3 数据集

为了方便网络安全研究人员对 DGA 进行研究，特别是对基于传统机器学习和深度学习的 DGA 检测技术的研究，工业界和学术界构建了一些公开数据集。这些数据集包括 DGA 数据集和良性域名数据集，总体概况如表 1 所列。

表 1 数据集分类

Table 1 Classification of datasets

名称	种类	提供方
AADR	DGA	Andrey Abakumov
OSINT	DGA	Bambenek Consulting
UMUDGA[14]	DGA	穆尔西亚大学
360NetLab	DGA	三六零
DGArchive[9]	DGA	Fraunhofer FKIE
Alexa	良性	亚马逊
Umbrella	良性	思科
Majestic	良性	Majestic
Tranco[15]	良性	Pochat 等

目前被用于研究的 DGA 数据集有：Andrey Abakumov’s DGA Repository[1]（以下缩写为 AADR）、OSINT DGA feed[2]（以下缩写为 OSINT）、UMUDGA dataset[3]（以下缩写为 UMUDGA）、360NetLab dataset[4]（以下缩写为 360NetLab）、DGArchive[5] 等。

1）AADR 数据集由 Andrey Abakumov 于 2016 年创建，包括 DGA 的源代码和这些 DGA 生成的域名。该数据集同时也包含 Alexa 排名前 100 万的域名作为良性数据集，适用于构建神经网络从而检测 DGA 类型僵尸网络，因此在许多研究工作中得到使用。但是由于该数据集域名数量和种类过少，且最近一次更新为七年前，目前已停止维护。

2）OSINT 数据集由 Bambenek Consulting 通过收集和聚合大量 DGA 生成的域名创建，提供 50 多个恶意软件家族 DGA 算法生成的 80 多万个域名。2019 年 7 月 1 日起，将 OSINT 数据集用于商业用途会被收费，学术研究和非营利用途仍将免费。

3）UMUDGA 数据集由穆尔西亚大学的研究团队构建。该数据集通过在受控环境下运行 DGA 源代码生成恶意域名，当没有新域名生成或生成的域名超过 1 000 000 时代码停止运行。UMUDGA 包括 38 个恶意软件家族，提供了超过 30 000 000 个域名，此外还有 50 多个恶意软件变体，所有变体至少包含 10 000 个样本，其中大多数变体包含 1 000 000 个有效且不重复的域名。该数据集提供 ARFF、CSV、文本格式的数据集，适合不同的工具和编程语言，并可以公开访问，从而确保数据集的公开可靠性。

4）360NetLab 数据集是由三六零安全科技股份有限公司的 360NetLab 团队从现实网络环境中收集并创建的 DGA 数据集，其通过检测系统实时筛选被动 DNS 流量和恶意软件样本，实时更新数据库，无需申请即可使用。然而，该数据集缺乏稳定性，且 360NetLab 团队已经发布公告将终止这项服务（2023 年 7 月 15 日访问得到的数据）。

5）DGArchive 数据集由德国 Fraunhofer FKIE 的网络分析和防御部门提供更新和访问服务。该数据集提供了超过一百种 DGA 生成的域名，使用者需要向 ed. refohnuarf. eikf@evihcragd 发送电子邮件申请访问，并通过 web 服务共享数据集。

作为白样本的良性域名数据集，应保证数据集中的域名都是合法域名，不能包含恶意域名。因此，如何构建高质量的良性域名数据集也是工业界和学术界的研究热点之一[15-16]。常用的良性域名数据集有 Alexa[6]，Umbrella[7]，Majestic[8]，Tranco[9] 等。

1）Alexa 数据集是一个常见的域名排名列表，由亚马逊公司通过在客户端浏览器中安装插件获得用户的访问数据，进而基于这些访问数据通过算法计算得出排名，该排名算法不对外公开。这种方法存在以下 3 个问题：(1)该域名排名依赖于浏览器插件的安装率，因此对于插件安装率很低的一些国家和地区，Alexa 排名不能反映这些国家和地区的域名

1) https://github. com/andrewaeva/DGA

2) https://osint. bambenekconsulting. com/feeds/

3) https://data. mendeley. com/datasets/y8ph45msv8/1

4) https://data. netlab. 360. com/dga/

5) https://dgarchive. caad. fkie. fraunhofer. de

6) https://www. alexa. com/topsites(已停止服务)

7) https://s3-us-west-1. amazonaws. com/ umbrella-static/top-1m. csv. zip

8) https://majestic. com/reports/majestic-million

9) https://tranco-list. eu/

排名真实情况;(2)随着移动互联网和物联网技术的普及,PC端浏览器产生的流量占比越来越小,因此基于传统PC端浏览器插件产生的数据进行排名并不能真实反映出现阶段互联网中域名排名的真实情况;(3)Alexa数据集中超过一半的域名每天都在变化。

2)Umbrella数据集是思科公司使用Open DNS的流量作为数据来源计算的域名排名,该排名算法也不公开。这种方法虽然不依赖浏览器插件的安装率,但是也存在一些问题,例如对于不使用Open DNS作为DNS解析服务器的一些国家和地区,Umbrella排名不能反映这些国家和地区的域名排名真实情况。此外,研究[15]指出,Umbrella排名中,仅有49%的域名为真实域名。

3)Majestic数据集主要包含付费级别域名,但也包括一些非常受欢迎的子域名,如plus.google.com,en.wikipedia.org等,自2012年10月起由Majestic公司发布并每日更新。Majestic排名计算基于域名的反向链接(backlinks),数据来源为抓取120天(2018年4月12日之前为90天)约4 500亿个URL。Majestic的排名算法意味着只有从其他网站链接的域名会被考虑,因此该方法偏向于基于浏览器的流量,但不计算实际的页面访问量。与网络搜索引擎类似,爬虫的实现方式影响了Majestic排名数据。此外,研究[15]指出,Majestic数据集中包含2 162个恶意域名。

4)Tranco数据集由Pochat等[15]于2019年发布,其本身并不是由域名排名测量算法生成的,而是通过整合其他域名排名(Alexa,Umbrella,Majestic)来创建新的域名排名。经过算法的过滤筛选,Tranco数据集要比Alexa和Umbrella更加可信。随着Alexa停止服务,未来研究人员可能会转而使用Tranco数据集。

4 DGA检测技术

根据不同维度进行划分,DGA检测技术可分为:基于二分类的DGA检测方法[17]、基于多分类的DGA检测方法[18]、基于域名字符串的DGA检测方法[19]、基于域名附属信息的DGA检测方法[20]、基于传统机器学习的DGA检测方法[21]、基于深度学习的DGA检测方法[22]等。DGA检测技术的分类如表2所列,这些分类方法有些会有交叉,如基于二分类的DGA检测技术既可以使用传统机器学习技术又可以使用深度学习技术。域名附属信息指除域名文本外的一些其他信息,如WHOIS信息(域名是否续订、域名注册电话是否有效等)和DNS信息(域名DNS请求数量、域名第一次和最后一次DNS请求的间隔时间等)。基于域名字符串的DGA检测方法则仅依靠域名文本进行检测。以百度公司的域名("baidu.com")为例,这种检测方法只依赖于"baidu.com"这个字符串文本的一些特征对域名进行判断,如域名长度、元辅音比例、是否以数字开头等特征。

近年来,DGA检测技术的研究以传统机器学习和深度学习为主,因此本文以基于传统机器学习的DGA检测技术、基于深度学习的DGA检测技术和基于其他算法的DGA检测技术为基础,对DGA检测技术进行总结综述。近年来的技术总结如表3所列。

表2 DGA检测技术分类

Table 2 Classification of DGA detection technologies

类别	说明	特点
基于二分类	仅判断域名是良性或恶意	粗粒度;准确率高
基于多分类	判断域名具体由哪种DGA生成	细粒度;准确率低
基于域名字符串	仅依靠域名字符串进行检测	速度快;成本低;误判率高
基于域名附属信息	结合WHOIS等域名附属信息进行检测	速度慢;成本高;涉及个人隐私
基于传统机器学习	使用传统机器学习技术进行检测	需人工提取特征;计算时间长
基于深度学习	使用深度学习技术进行检测	自动提取特征;GPU加速;需要大数据集

表3 DGA检测方法总结

Table 3 Summary of DGA detection technologies

文献	算法	良性域名数据集	DGA数据集	是否使用附属信息
Davuth等[23]	SVM	自建	自建	否
Sivaguru等[24]	RF	Alexa	自建	否
Schuppen等[21]	RF	RWTH Aachen University, Siemens	DGArchive	是
Bilge等[25]	J48	Alexa	malwaredomains.com网站, the Zeus Block List, Malware Domains List等多种来源	是
Antonakakis等[26]	ADT	Alexa	自建	是
Vranken等[20]	LR,SVM,MLP等	Tranco	DGArchive	否
Liu等[27]	SVM	Alexa	DGArchive	是
Sun等[46]	异构信息网	Alexa	DGArchive, malwaredomains.com网站等多种来源	是
Bo等[35]	GCN,BiLSTM,MLP	Alexa;Github	fast-flux-attack-datasets,自建	是
Sivaguru等[36]	LSTM,RF	Alexa;自建	DGArchive	是
Zhou等[19]	CNN	Alexa	DGArchive	否
Xu等[33]	CNN	Alexa	DGArchive	否
Vinayakumar等[38]	CNN,LSTM	Alexa;OpenDNS;自建	DGArchive,OSINT	否
Highnam等[39]	CNN,LSTM	Alexa	DGArchive	否
Liang等[42]	CNN,Attention,RF	Alexa;Majestic	DGArchive,Netlab360	否

（续表）

文献	算法	良性域名数据集	DGA 数据集	是否使用附属信息
Woodbridge 等[17]	LSTM	Alexa	OSINT	否
Tran 等[18]	LSTM	Alexa	OSINT	否
Tuan 等[41]	LSTM，Attention	Alexa	OSINT，UMUDGA，360NetLab	否
Shahzad 等[22]	RNN	Alexa；Umbrella	OSINT，360NetLab	否
Namgung 等[45]	BiLSTM，CNN	Alexa	OSINT	否
Vinayakumar 等[44]	RNN，LSTM，GRU 等	AmritaDGA	AmritaDGA	否
Ren 等[40]	CNN，LSTM	Alexa	OSINT，360NetLab	否

4.1 基于传统机器学习的 DGA 检测技术

随着传统机器学习被广泛应用于自然语言处理、计算机视觉等领域，网络安全人员也开始将传统机器学习用于检测 DGA。基于人为选择的特征，如熵、附属信息、词汇属性等，建立机器学习模型。Davuth 等[23]对域名字符串进行了统计分析，基于良性域名和恶意域名在统计规律上的差别，以 bigram 的形式提取特征，最后使用支持向量机（SVM）检测 DGA。Sivaguru 等[24]提出了一种基于随机森林的 DGA 检测器，它提取了 26 个特征进行训练。Vranken 等[20]使用 *n*-gram 的 TF-IDF 值作为特征，使用逻辑回归（Logistic Regression，LR）算法检测 DGA。Bilge 等[25]通过被动 DNS 流量分析，基于 J48 决策树定义了 15 个特征，主要包括前后响应时间、DNS 返回包字段、域名解析有效期和域名字符串 4 个方面。Antonakakis 等[26]结合聚类和分类算法，通过对解析失败的 DNS 响应（Non-existent Domain，NXDomain）进行分析来检测 DGA，该检测方法的主要原理是 DGA 中指向 C&C 服务器的 DNS 查询数量相对较少，以及来自同一家族的恶意软件包含了类似的 NXDomain 流量。Schuppen 等[21]基于随机森林（RF）算法，提取出 12 个结构特征、7 个语言特征和 2 个统计特征，对 DNS 流量中 NXDomain 类型的域名进行了分类。Liu 等[27]也基于 DNS 流量中的 NXDomain 响应，首先利用白名单过滤掉良性域名的 NXDomain 响应，然后根据 DNS 主机行为对域名进行聚类，最后分析聚类的结果，提取出了 18 个域名附属信息特征。Pochat 等[28]协助执法部门在真实网络环境中对 Avalanche 僵尸网络产生的恶意域名进行查封，他们提取了域名的 36 个特征，其中包含 34 个域名附属信息特征（WHOIS、主动 DNS 和被动 DNS 等），最后基于 4 种传统机器学习算法对恶意域名进行了离线检测。

4.2 基于深度学习的 DGA 检测技术

不同于传统机器学习，基于深度神经网络的深度学习不需要人工特征工程，可以从原始数据中自动学习到高级特征表示。常见的深度学习算法有卷积神经网络（CNN）[29]和循环神经网络（RNN）[30]等。CNN 主要用于处理具有网格结构的数据，如图像数据。RNN 主要用于处理序列数据，如文本和语音等。长短期记忆网络（LSTM）通过引入记忆单元和门控机制，增强了 RNN 处理长期依赖关系的能力。随着深度学习技术成功应用于多个领域[31-32]，网络安全研究人员也开始使用深度学习技术来检测 DGA。

CNN 主要用于处理具有网格结构的数据，在文本领域应用较少，因此单独基于 CNN 的 DGA 检测技术研究并不多。Xu 等[33]设计了一种基于 *n*-gram 和 CNN 的 DGA 检测模型，该模型在 Alexa 和 DGArchive 数据集上进行训练，将域名字符串转换为 *n*-gram 表示形式作为 CNN 模型的输入，不需要人工提取特征和 DNS 等域名附属信息。Zhou 等[19]提出了一种基于时间卷积网络（Temporal Convolutional Network，TCN）的实时 DGA 检测算法，先将域名传递为单词级或字符级组件的序列，然后设计一个基于 TCN 的深度神经网络来提取隐式模式。该算法对基于字符的域名和基于字典的域名均进行了检测，实验结果表明其在二分类任务中表现较好，但在多分类任务中表现较差。

RNN 适合处理序列数据，在文本识别、序列数据预测等领域应用广泛。Woodbridge 等[17]提出了基于 LSTM 的 DGA 检测模型，利用该模型可获取字符串的时序信息的特性，对恶意域名进行检测，后续研究者提出的 LSTM 模型基本都是建立在此 LSTM 模型的基础上。为解决域名数据多分类的问题，基于 Woodbridge 等[17]的工作，Tran 等[18]提出了一种多分类域名检测算法 LSTM. MI，该算法中，原始 LSTM 被调整为成本敏感（Cost-sensitive）来处理多分类的不平衡问题。Shahzad 等[34]提出了一种基于 RNN 架构的 DGA 检测模型，并对比了 GRU、LSTM 和双向 LSTM（BiLSTM）3 种不同的 RNN 架构性能。实验结果表明 RNN 架构之间的性能指标几乎没有差异。

近年来，一些研究开始集成多种模型来对 DGA 进行检测。Bo 等[35]提出了一种基于多模态特征融合的 DGA 域名检测方法，用 GCN 模块、BiLSTM 模块和 MLP 模块分别提取特征，并用神经网络将特征进行融合，明显提升了检测效果。Sivaguru 等[36]拓展了 Tran 等[18]的工作，使用 LSTM. MI 和随机森林的混合模型检测 DGA，其中随机森林由 100 棵树组成，共提取了 35 个特征。Chen 等[37]在 LSTM 模型的基础上加入了注意力机制（Attention），该方法在完成词嵌入（Word Embedding）的过程中能够识别更多特征。Vinayakumar 等[38]提出了基于二分类的 DGA 检测模型，该模型通过在数据集上使用 CNN 和 LSTM 混合模型隐式提取的统计特征来检测恶意域名，实验结果表明了该方法的有效性。为了检测基于字典的 DGA，Highnam 等[39]也提出了一种 CNN 和 LSTM 混合架构，用于检测基于字典的 DGA。该模型在 DGArchive 数据集中的 3 个基于字典的 DGA（Matsnu，Suppobox，Gozi）数据集和 Alexa 数据集上进行训练和评估，然后实时部署。针对基于字典的 DGA 的威胁，Ren 等[40]提出了一种深度学习集成框架。该框架基于 CNN 和 BiLSTM 提取域名序列信息的特征，然后使用注意力层为从域名中提取的深层信息分配相应的权重，最后实现对 DGA 的检测。为检测 DGA 类型的僵尸网络，Tuan 等[41]提出了一种基于 LSTM 和注意力机制（Attention）的混合架构 DGA 检测模型，包括了一个二分类模型和一个多分类模型。Liang 等[42]的研究发现 DGA 检测模型对域名长度较为敏感，他们针对不同长度

的域名(超短域名、中等域名和超长域名),基于 CNN 和随机森林提出了一种异构 DGA 检测模型。为了检测基于字典的 DGA,Curtin 等[43]设计了 smash 分数特征来表示域名与单词的相似性,引入域名注册信息,最终将 RNN 与域名注册信息结合,并取得了较好的检测效果。Vinayakumar 等[44]提出了一种物联网僵尸网络检测的两层框架。框架的第一层使用基于预定义阈值的孪生网络来估计 DNS 查询的相似性度量,进而选择以太网中连接最频繁的 DNS 信息;框架的第二层则使用深度学习算法来检测 DGA。Namgung 等[45]提出了一种基于 BiLSTM 的高效 DGA 检测模型,相比单向 LSTM,BiLSTM 可以捕捉到更全面的语义和上下文信息。之后,他们用 BiLSTM 和 CNN 的集成模型进一步最大化检测性能。结果表明,BiLSTM 模型和集成模型的性能都优于现有的 LSTM 模型和 CNN 模型,而集成模型的性能进一步优于 BiLSTM 模型。

4.3 基于其他算法的 DGA 检测技术

一些 DGA 检测技术并没有使用传统机器学习算法或深度学习算法。Sun 等[46]首次利用异构信息网络来处理 DNS 信息,结合传导分类完成恶意域名的识别。异构信息网络利用了域名、网络段、域名 IP、域名别名等信息构建网络,尽可能利用了客户端、IP、域的信息,最后用直推式节点分类(Transductive Node Classification)方法对 DGA 进行检测。Fang 等[47]探索了域名之间的时间相似性,采用增量词嵌入方法来捕获终端主机和域名之间的交互,表征 IP 地址的 DNS 查询的时间序列模式,从而探索域名之间的时间相似性。通过修改 Word2Vec 算法,使其能够从 190 多万个域名中自动学习到上下文特征表示,并开发了一个简单的分类器来区分恶意域名和良性域名。

5 现实挑战与未来研究方向

工业界和学术界对 DGA 检测技术的不断探索研究提升了基于 DGA 检测技术的僵尸网络发现能力,但该方向的研究仍存在一些挑战,具体问题如下。

5.1 没有统一的数据集

从本文第 4 章可以看到,不同 DGA 检测方法所使用的数据集基本上都不一致。

良性域名数据集主要有 Alexa,Majestic,Umbrella,Tranco 等。此外,域名排名每天都在更新,同一个良性域名数据集会因为选择的时间不同而不一致。从本文第 4 章的研究中可以发现,Alexa 域名排名是被使用最多的良性数据集,但该数据集也存在诸多问题:1)Alexa 排名的结果可以被操纵,导致数据集中存在恶意域名;2)Alexa 数据集里一半的域名每天都在变化更新,导致不同时间的 Alexa 数据集差别较大;3)亚马逊公司已于 2022 年 5 月 1 日停止了 Alexa 域名排名服务,因此之后的研究只能使用历史版本的 Alexa 数据集,这导致 Alexa 数据集的可信度受到很大影响。

对于 DGA 数据集,主要有 DGArchive 和 360NetLab 等。DGA 数据集同样也存在一些问题。以 DGArchive 数据集为例,一方面,DGArchive 数据集也在不断更新,不同时间选取的数据集并不一致。另一方面,即使是同一时间选取的 DGArchive 数据集,但因为进一步选择方法具有不确定性,所以 DGA 数据集也可能不一致。

在没有业内标准数据集的情况下,现阶段研究工作所使用的数据集基本上都有差异。因此,未来的一个研究方向是如何构建一个权威、可用的域名数据集平台,以便对 DGA 检测技术进行进一步的研究。

5.2 实际网络环境中的应用问题

本文调研的 DGA 检测技术在各自的数据集和实验环境中都取得了良好的效果,但很少有工作验证所提出的 DGA 检测技术在实际环境中的应用效果。基于域名字符串的 DGA 检测和基于域名附属信息的 DGA 检测都存在弊端。

基于域名字符串的轻量级 DGA 检测速度快,可以用于线上部署,但该方法存在两个问题:一是因为该检测方法仅依赖于域名字符串,所以很容易造成误判,将合法域名检测为恶意域名,进而造成合法网络服务中断;二是该检测方法对于简单的对抗样本攻击表现得很脆弱,如 CharBot[48],Khaos[49]等算法生成的域名具有很强的抗检测能力。

基于域名附属信息的 DGA 检测技术速度虽然慢但准确率和可信度较高。这种检测方法除了域名本身的字符串特征外,还使用了 DNS 流量和 WHOIS 等域名附属信息。但是,这种方法也存在一些问题:一是在大规模数据背景下的实时部署问题;二是域名附属信息需要成本且很难获取,甚至可能会涉及用户隐私。

针对此问题,在未来的研究中应对 DGA 检测模型在实际环境中的应用效果加以测试,解决实际网络环境中存在的网络安全问题。

5.3 深度学习模型自身的安全问题

从表 3 中可以看出,深度学习已被广泛应用于 DGA 检测领域。基于深度学习的 DGA 检测技术使用的算法也日益复杂,从开始的简单单层网络结构,到现在的复杂网络结构。然而,深度学习等人工智能模型自身也存在诸多安全漏洞,容易被网络攻击者攻击,如对抗样本攻击[50-51]、数据投毒[52]、后门攻击[53-54]等。现阶段,众多基于深度学习的 DGA 检测技术并没有考虑这些安全问题。Yun 等[49]提出了一种基于生成对抗网络的域名生成算法,该算法生成的对抗样本域名在基于 LSTM 的 DGA 检测模型中 AUC 值仅为 0.57,这意味着检测模型无法检测对抗样本域名,检测结果类似于随机猜测。Zhai 等[55]针对基于 LSTM 的 DGA 检测方法,提出了一种后门攻击,并通过实验验证了后门攻击的可行性。

针对此问题,未来研究可以对基于深度学习的 DGA 检测算法自身存在的安全问题多加考虑,比如在选择训练数据集时,要判断训练数据集是否被污染。

结束语 DGA 检测技术是一个备受关注的网络安全领域研究方向,对于检测基于 DGA 的僵尸网络具有重要意义。本文在充分调研和深入分析的基础上,对 DGA 检测技术研究进展进行了全面综述;基于调研结果,对现有 DGA 检测技术存在的问题进行了分析,并展望了未来研究方向和挑战。

参 考 文 献

[1] ANTONAKAKIS M, APRIL T, BAILEY M, et al. Understan-

ding the mirai botnet [C]// Proceedings of the 26th USENIX security symposium(USENIX Security 17). 2017:1093-1110.

[2] SIGLER K. Crypto-jacking:how cyber-criminals are exploiting the crypto-currency boom [J]. Computer Fraud & Security, 2018,2018(9):12-14.

[3] TEAM S R. Emotet exposed:looking inside highly destructive malware [J]. Network Security,2019,2019(6):6-11.

[4] KESSEM L. The Necurs Botnet:A pandora's box of malicious spam [EB/OL]. https://securityintelligence.com/the-necurs-botnet-a-pandoras-box-of-malicious-spam/.

[5] HOLZ T,GORECKI C,RIECK K,et al. Measuring and detecting fast-flux service networks [C]// Proceedings of the Network and Distributed System Security Symposium (NDSS). 2008.

[6] SOOD A K,ZEADALLY S. A taxonomy of domain-generation algorithms [J]. IEEE Security & Privacy,2016,14(4):46-53.

[7] SAEED A M H,WANG D,ALNEDHARI H A M,et al. A Survey of Machine Learning and Deep Learning Based DGA Detection Techniques [C]// Proceedings of the Smart Computing and Communication — 6th International Conference (SmartCom). 2021:133-143.

[8] WANG Y,WANG Z,PAN R. Survey of DGA Domain Name Detection Based on Character Feature [J]. Computer Science, 2023,50(8):251-259.

[9] PLOHMANN D,YAKDAN K,KLATT M,et al. A comprehensive measurement study of domain generating malware [C]// Proceedings of the 25th USENIX Security Symposium(USENIX Security 16). 2016:263-278.

[10] RAHIM A. cryptolocker-dga [EB/OL]. https://github.com/azrilrahim/cryptolocker-dga.

[11] CHIU A,VILLEGAS A. Threat Spotlight:Dyre/Dyreza:An Analysis to Discover the DGA [EB/OL]. https://blogs.cisco.com/security/talos/threat-spotlight-dyre.

[12] GEFFNER J. End-to-end analysis of a domain generating algorithm malware family [C]// Proceedings of the Black Hat USA. 2013.

[13] BAUMGARTNER K,RAIU C. Sinkholing Volatile Cedar DGA Infrastructure [EB/OL]. https://securelist.com/sinkholing-volatile-cedar-dga-infrastructure/69421/.

[14] ZAGO M,PÉREZ M G,PÉREZ G M. UMUDGA:A dataset for profiling DGA-based botnet [J]. Computers & Security,2020, 92:101719.

[15] POCHAT V L,GOETHEM T V,TAJALIZADEHKHOOB S, et al. Tranco:A Research-Oriented Top Sites Ranking Hardened Against Manipulation [C]// Proceedings of the Annual Network and Distributed System Security Symposium San Diego. 2019.

[16] XIE Q,TANG S,ZHENG X,et al. Building an Open,Robust, and Stable Voting-Based Domain Top List [C]// Proceedings of the USENIX Security Symposium. Boston,2022:625-642.

[17] WOODBRIDGE J,ANDERSON H S,AHUJA A,et al. Predicting domain generation algorithms with long short-term memory networks [J]. arXiv:161100791,2016.

[18] 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.

[19] ZHOU S,LIN L,YUAN J,et al. Cnn-based dga detection with high coverage [C]// Proceedings of the 2019 IEEE International Conference on Intelligence and Security Informatics(ISI). 2019: 62-67.

[20] VRANKEN H,ALIZADEH H. Detection of DGA-Generated Domain Names with TF-IDF [J]. Electronics,2022,11(3):414.

[21] SCHÜPPEN S,TEUBERT D,HERRMANN P,et al. {FANCI}:Feature-based Automated {NXDomain} Classification and Intelligence [C]// Proceedings of the 27th USENIX Security Symposium(USENIX Security 18). 2018:1165-1181.

[22] SHAHZAD H,SATTAR A R,SKANDARANIYAM J. DGA Domain Detection using Deep Learning [C]// Proceedings of the 5th IEEE International Conference on Cryptography, Security and Privacy. Zhuhai,2021:139-143.

[23] DAVUTH N,KIM S R. Classification of malicious domain names using support vector machine and bi-gram method [J]. International Journal of Security and Its Applications, 2013, 7(1):51-58.

[24] SIVAGURU R,CHOUDHARY C,YU B,et al. An Evaluation of DGA Classifiers [C]// Proceedings of the IEEE International Conference on Big Data Seattle. 2018:5058-5067.

[25] BILGE L,KIRDA E,KRUEGEL C,et al. Exposure:Finding malicious domains using passive DNS analysis [C]// Proceedings of the Ndss. 2011:1-17.

[26] ANTONAKAKIS M,PERDISCI R,NADJI Y,et al. From {Throw-Away} Traffic to Bots:Detecting the Rise of {DGA-Based} Malware [C]// Proceedings of the 21st USENIX Security Symposium(USENIX Security 12). 2012:491-506.

[27] LIU Z,YUN X,ZHANG Y,et al. CCGA:Clustering and Capturing Group Activities for DGA-Based Botnets Detection [C]// Proceedings of the 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing And Communications/13th IEEE International Conference on Big Data Science and Engineering. Rotorua,2019:136-143.

[28] POCHAT V L,HAMME T V,MAROOFI S,et al. A Practical Approach for Taking Down Avalanche Botnets Under Real-World Constraints [C]// Proceedings of the Annual Network and Distributed System Security Symposium(NDSS). San Diego,2020.

[29] LECUN Y,BOTTOU L,BENGIO Y,et al. Gradient-based learning applied to document recognition [J]. Proceedings of the IEEE,1998,86(11):2278-2324.

[30] ELMAN J L. Finding structure in time [J]. Cognitive Science, 1990,14(2):179-211.

[31] LU Y,MAO Z,QIU Z. Review of Development and Applications of Blockchain Technology in the Field of Energy Internet of Things [J]. Guangdong Electric Power,2021,34(7):1-21.

[32] WU J,LIANG L,JI X,et al. Infrared Image Fault Detection Method for Insulator Based on YOLOv3 Algorithm [J]. Guangdong Electric Power,2019,33(9):77-84.

[33] XU C,SHEN J,DU X. Detection method of domain names generated by DGAs based on semantic representation and deep neural network [J]. Computers & Security,2019,85:77-88.

[34] SHAHZAD H, SATTAR A R, SKANDARANIYAM J. DGA Domain Detection using Deep Learning [C]// Proceedings of the 5th IEEE International Conference on Cryptography, Security and Privacy(CSP). 2021: 139-143.

[35] BO L, CHONG X, SHAOJIE C, et al. Fast-Flux Malicious Domain Name Detection Method Based on Multimodal Feature Fusion [J]. Netinfo Security, 2022, 22(4): 20-29.

[36] SIVAGURU R, PECK J, OLUMOFIN F G, et al. Inline Detection of DGA Domains Using Side Information [J]. IEEE Access, 2020, 8: 141910-141922.

[37] CHEN Y, ZHANG S, LIU J, et al. Towards a deep learning approach for detecting malicious domains [C]// Proceedings of the 2018 IEEE International Conference on Smart Cloud (SmartCloud). 2018: 190-195.

[38] VINAYAKUMAR R, SOMAN K, POORNACHANDRAN P, et al. DBD: Deep learning DGA-based botnet detection [J/OL]. https://link.springer.com/chapter/10.1007/978-3-030-13057-2_6.

[39] HIGHNAM K, PUZIO D, LUO S, et al. Real-Time Detection of Dictionary DGA Network Traffic Using Deep Learning [J]. SN Computer Science, 2021, 2(2): 110.

[40] REN F, JIANG Z, WANG X, et al. A DGA domain names detection modeling method based on integrating an attention mechanism and deep neural network [J]. Cybersecur, 2020, 3(1): 4.

[41] TUAN T A, LONG H V, TANIAR D. On Detecting and Classifying DGA Botnets and their Families [J]. Computers & Security, 2022, 113: 102549.

[42] LIANG J, CHEN S, WEI Z, et al. HAGDetector: Heterogeneous DGA domain name detection model [J]. Computers & Security, 2022, 120: 102803.

[43] CURTIN R R, GARDNER A B, GRZONKOWSKI S, et al. Detecting DGA domains with recurrent neural networks and side information [C]// Proceedings of the 14th International Conference on Availability, Reliability and Security. 2019: 1-10.

[44] VINAYAKUMAR R, ALAZAB M, SRINIVASAN S, et al. A Visualized Botnet Detection System Based Deep Learning for the Internet of Things Networks of Smart Cities [J]. IEEE Transactions on Industry Applications, 2020, 56(4): 4436-4456.

[45] NAMGUNG J, SON S, MOON Y S. Efficient Deep Learning Models for DGA Domain Detection [J]. Secur Commun Networks, 2021, 2021: 8887881-8887815.

[46] SUN X, TONG M, YANG J, et al. {HinDom}: A Robust Malicious Domain Detection System based on Heterogeneous Information Network with Transductive Classification [C]// Proceedings of the 22nd International Symposium on Research in Attacks, Intrusions and Defenses(RAID 2019). 2019: 399-412.

[47] FANG X, SUN X, YANG J, et al. Domain-Embeddings Based DGA Detection with Incremental Training Method [C]// Proceedings of the IEEE Symposium on Computers and Communications(ISCC). Rennes, 2020: 1-6.

[48] PECK J, NIE C, SIVAGURU R, et al. CharBot: A simple and effective method for evading DGA classifiers [J]. IEEE Access, 2019, 7: 91759-91771.

[49] YUN X, HUANG J, WANG Y, et al. Khaos: An adversarial neural network DGA with high anti-detection ability [J]. IEEE Transactions on Information Forensics and Security, 2019, 15: 2225-2240.

[50] CARLINI N, WAGNER D A. Towards Evaluating the Robustness of Neural Networks [C]// Proceedings of the IEEE Symposium on Security and Privacy. San Jose, 2017: 39-57.

[51] PAPERNOT N, MCDANIEL P D, GOODFELLOW I J, et al. Practical Black-Box Attacks against Machine Learning [C]// Proceedings of the the 2017 ACM on Asia Conference on Computer and Communications Security. Abu Dhabi, 2017: 506-519.

[52] HUANG H, MU J, GONG N Z, et al. Data Poisoning Attacks to Deep Learning Based Recommender Systems [C]// Proceedings of the 28th Annual Network and Distributed System Security Symposium. 2021.

[53] ZHAO Z, CHEN X, XUAN Y, et al. DEFEAT: Deep Hidden Feature Backdoor Attacks by Imperceptible Perturbation and Latent Representation Constraints [C]// Proceedings of the the IEEE/CVF Conference on Computer Vision and Pattern Recognition. New Orleans, 2022: 15213-15222.

[54] GU T, DOLAN-GAVITT B, GARG S. Badnets: Identifying vulnerabilities in the machine learning model supply chain [J]. arXiv: 170806733, 2017.

[55] ZHAI Y, YANG L, YANG J, et al. BadDGA: Backdoor Attack on LSTM-Based Domain Generation Algorithm Detector [J]. Electronics, 2023, 12(3): 736.

WANG Xuxian, born in 1994, master. His main research interests include electric power system automation, its network security technology and so on.

YANG Liqun, born in 1990, Ph.D, assistant professor. His main research interests include network security and industrial control system security and so on.

(责任编辑:何杨)