# A Comparative Analysis of Machine Learning Techniques for DGA based botnet detection

**Ranjana B Nadagoudar, Research Scholar, PDA College of Engineering, Gulbarga & India,**

**ranjanapriya8@gmail.com**

**Sujatha P Terdal, Professor, PDA College of Engineering, Gulbarga & India,**

**sujatha.terdal@gmail.com**

**Abstract - In the recent years, the cyber security incidents were reported worldwide through DDoS attacks. Many of these attacks were conducted through botnet, which usually consists of a group of infected computers, Smartphone's or internet connected devices. Botnet can be used to perform various malicious activities such as launching of DDoS attack's, sending spam emails and compromising sensitive information, click fraud, information and identity theft. However, intrusion detection system-based solutions will make use of signatures which seems to be very much ineffective because of the advancement in the botnets. Further various methods have been proposed to detect botnets which are based on DNS traffic or DNS queries; however, the problem still persists and is very much challenging due to several factors. Firstly for not considering important features and the rules that contribute to the detection of botnet based on DNS. Botnet detection has become a major research challenge in the recent years. Researchers have developed numerous approaches for botnet detection to combat botnet threat against cyber-security. A comprehensive literature overview of current botnet detection based on DNS techniques with a focus on revealing the strengths and weaknesses of the existing techniques in the research area. In line with this, some selected techniques were retrieved and analyzed and a conclusion is drawn which exposed the need for more robust detection techniques to detect and prevent the emerging sophisticated botnet versions in the domain.**

**Keywords:** ***Botnet, Botnet detection, Cyber Security, Domain Name System, Machine learning.***

## I. INTRODUCTION

Today Internet has becomes an important element in everyone's life, the user online presence, advancement of content learning such as e-learning, e-banking and social media access [1, 2]. But unfortunately, today Internet is targeted by cyber security attackers; one of such preferred attacker's tools using now a days is a botnet. Recently it is observed that botnets are constantly evolving on the global scale. The word botnet is derived from the words robot and network. These botnets are basically built to carry out larger attacks or crimes. Each member in the botnet is called as a bot. Botnets are commonly used to carry out various cyber security attacks such as sending spam emails, DDoS, Phishing, malware dissemination and click frauds. A bot is created by a *botmaster* which allows them to control infected devices remotely. If the location of the Command & Control server is identified, it is easier for the detection methods to detect the botnet.

The Domain Name System (DNS) is a naming system that translates domain names (www.google.com) into machine readable IP addresses (192.0.2.4) [1]. This translation is carried out by looking up the DNS records of the requested domain. In addition, the domain name system is used to locate servers and mailing hosts which can directly impact the data exchange across the Internet [2]. The domain name system botnet detection methods are classified into 5 categories in [11]: anomaly-based, flow-based, flux-based, bot infection-based and DGA-based. These DNS based detection techniques have been widely used because of the following reasons Firstly it requires less resources and cost of the detection tools are relatively low and Second advantage is botnet detection technique does not affect the network performance. The earlier detection methods relies on IP The most significant solution for detecting DNS-based botnet attacks is adopting machine learning (ML) and Deep learning methods.

The main purpose of this work is to provide a literature survey on most recent domain name system based botnet detection methods and the contributions of this paper will list the comprehensive presentation of DNS based botnet detection methods, review of the most recent botnet detection methods along with their strengths and weaknesses and finally emphasis on the need for more

 DOI : 10.35291/2454-9150.2022.0099 

robust botnet techniques that will be able to detect the emerging sophisticated variants of botnets.

## II. Background and Preliminaries

### A. Botnet

The term botnet is derived from the word Robot and network. The bots are mainly designed to carry out some predefined tasks in automated way. Other way of defining bots is it's a software program that performs automated and repetitive tasks.

A botnet is a number of connected devices which are used to carry out various cyber security attacks and these devices are controlled by a bot master remotely through the C&C server. A bot master uses these bots to host various malicious activities.

The communication of C&C takes place between bot and bot master, Initially A bot master connects the bots by supplying a command based on the command received by the bot, a botnet performs malicious activities; and finally botnet forwards the results to the bot master.

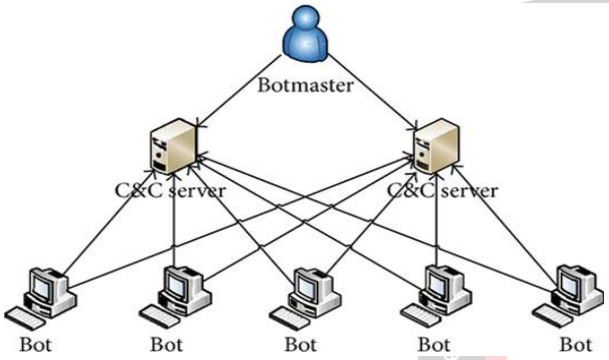


**Fig 1: Botnet structure**

The Fig: 1 represents the structure of botnet. The bot can communicate either with other bot or communicate with the Command &Control server [4]. Botmaster controls the communication between the C&C server and bots. Botnet developer's uses either static IP addresses to establish the connection, or the domain names, these domain names are generated via domain name generation algorithms [5] instead of having names and numbers.

### B. Botnet Life Cycle

The botnet life cycle includes various stages begin with propagation, rally, interaction, and malicious activities. Botnet often follows five stages to accomplish or execute instruction ordered by the bot master through the Command & Control channel. Botnet follows the five stages to execute instruction ordered by the botmaster through the C&C channel.

In the interaction stage botnets are interconnected computers performing the series of tasks repeatedly to keep the website going and they are mostly used in connection with IRC (Internet Relay Chat), the bot master investigates the target subnet for vulnerabilities and uses different exploitation methods to infect the target's device. As soon as the bot master is in control of your device, he will usually use your machine to carry out malicious activities.

In the second stage botnets are normally spread to infect other devices via malicious content injection on a visitation of unprotected websites. Botnets are capable of propagating themselves to recruit more devices into their army of bots. In the execution stage, the malicious activities are executed as instructed by the botmaster and this is for the botmaster to accomplish his set goals. The last stage upgrade and maintenance, the botnets report to the botmaster upon completion or execution of the instruction given and wait for further instructions.

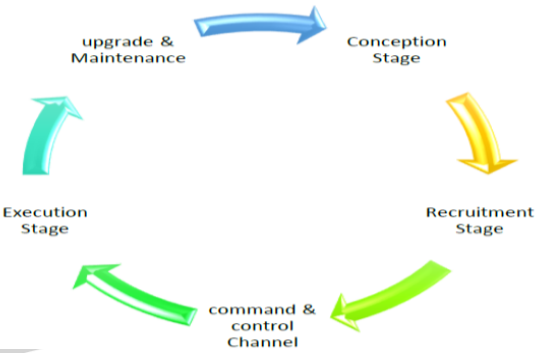


**Fig 2: Botnet Life Cycle**

### C. Domain Generation Algorithm

Domain generation algorithm (DGA) is an approach used by the cyber criminals to generate large list of domain names and Internet protocol addresses for C & C servers. DGAs provide malware with random new domains in order to evade security countermeasures. Cyber criminals use domain generation algorithms to deliver malware that can generate hundreds of new, random domains they can switch between during attacks, making it harder for the victim that is being targeted to block and remove these domains. Frequently changing the domain names might helps the attackers by preventing their servers from being block listed. The main idea is that to use domain generation algorithm which generates random domain names that the malwares can use and quickly switch between. DGAs are considered as one of the top most known methods that make it harder for malware victims to protect against attacks. If a particular domain is identified as malicious then it should be taken down and further the domain and C&C server are quickly switched. DGAs generate random domains over times that are used as rendezvous points where the infected hosts and the C&C server connect. At predetermined intervals, the DGA generates new names for its C&C server using one of several techniques. Usually, hundreds or thousands of domain names emerge from each run. Attackers only need to register a single one of those domains (it's usually done automatically) to have a fresh C&C DNS entry.

For example, if a website owner wants to use the domain name mysite.com and a search on a domain name registrar's site reveals that the desired domain name is not available, a

 DOI : 10.35291/2454-9150.2022.0099 

DGA running in the site's background might return suggestions for 50 similar site names that actually are available.

## III. RELATED WORKS

Machine learning technique is widely used in cyber security field such as detecting cyber security attacks, malwares and botnets. Because of rapid evolving nature of botnets at the massive scale the detection of botnets is a trending research topic. Lots of work has been carried out detect the botnet using IDS and other methods. Numerous works in the literature related to domain name system based botnet detection have motivated to carry out this work.

The traditional method called signature-based techniques can detect only known bots. The author Ramachandran et al. [2] presented a DNSBL (Blacklist) method that monitors domain name system traffic and also looks for stored signatures for detecting the bots before the attack. DNSBL-based method basically identifies the signatures of the bots which are already known in the monitored domain traffic. This method attempts to recognize the bot masters address and identify their location. Limitation of DNSBL method required to constantly maintain the updated malicious addresses in the database.

The author Antonakakis et al. [11] developed a system called 'Notos'. The proposed system can distinguish a malign DNS query from the benign DNS query [51]. Therefore Notos method can provide better accuracy and less FP rate. This method doesn't perform well for hybrid botnet architecture because this method is inefficient to handle frequently changing domains [52].

Mentor method proposed by Kheir et al. [23] it is a scalable reputation system for DNS which removes authenticated domains from the blacklist. The Mentor system collects statistical features of suspicious domain names. Further it applies supervised ML to categorize benign and suspicious domain names. The proposed method is tested against larger set of public botnet blacklists. The results shows that mentor system can efficiently detects the malicious bots and also removes benign domain names with low false positive rate.

Yadav et al. [12] presented a method for detecting algorithmically generated domains those are used for domain fluxing. The author used various statistical measures like Kullback-Leibler divergence and Jaccard index for classifying the domains as either malicious or not. Out of all the classifiers the Jaccard measure performs better. Further, the limitation of domain fluxing method is it cannot identify unknown botnets.

Shin, Xu et al. proposed [36] EFFORT framework. The proposed method combines various approaches to monitors the DNS traffic at various levels of network. Irrespective of communication protocol the EFFORT method uses controlled ML algorithms to report about the presence of malicious domains.

Monitoring of domain name system requests can able to detect the existence of botnets. Villamarin Salomon et al. [9] introduced anomaly detection techniques for monitoring the DNS queries. The method proposed in this paper tries to detect the domain names with high query rates therefore the said method is not efficient for detecting malicious attacks.

The author Bilge et al. [18] developed EXPOSURE system which employs DNS analysis technique for detecting suspicious domains. The experimental results proved that the proposed method works well for automatically identifying large scale of malicious domains such as phishing sites. Compared to earlier approaches the proposed approach is very much generic and it focuses on specific class of attack or threat.

BotGAD (Botnet Group Activity Detector) was introduced by Choi, et al. [10]. It functions in group behaviors monitoring. These behaviors are shown in the monitored network's DNS traffic. BotGAD basically focuses on botnets behavior and also defines group activity to detect various unknown botnets

A domain name system rule-based schema proposed by K. Alieyan [35] this approach improves the accuracy of DNS traffic-based botnet detection that are based on domain name system rule query and response behaviors. The technique aimed at detecting inconsistencies present in domain name system query and response behaviors. The result of the technique in this study showed an accuracy of 99.35% in terms of botnet detection and a low FP Rate of 0.25. This approach is effective only on DNS-based traffic flows.

Mathew [42] developed a classification of domain generation algorithm based on DNS traffic and other detection techniques for DGA botnet were presented. The proposed technique in the genetic algorithm for DGA detection. Computational complexity and high implementation cost are some of the weaknesses of this method.

## IV. METHODOLOGY

This study aims to provide a survey on the most recent DNS based botnet detection techniques were proposed by various researchers and to achieve this, we formulated research questions which are: 1) What are the strengths and limitations of the current techniques for detecting DNS based botnets 2) Which of the DNS based botnet detection techniques is proposed most frequently in current studies. Based on these research questions we formulated three research objectives. The first objective is to review the most recent DNS based botnet detection techniques. The second objective is to identify the strengths and weakness

 DOI : 10.35291/2454-9150.2022.0099 

of recent method for DNS based botnet detection and third objective is to discover the most effective and commonly used techniques in DNS based botnet detection. Various recent publications on DNS based botnet detection techniques that include journal articles and conferences papers were considered in the literature search. Current methods for DNS based botnets detections are investigated from the reviewed literature and their strengths and weaknesses were identified. The second and third objectives were achieved in Table 1 for identifying the strengths and weaknesses as well as the most effective and commonly used technique respectively. Here, we discuss the methods that are used in detecting DNS based botnet. Researchers have articulated numerous botnet detection techniques with different approaches. Broadly, botnet detection techniques are classified in two [14] [35].

### 1. *DNS BASED BOTNET DETECTION TECHNIQUES*

Researchers have articulated numerous botnet detection techniques with different approaches. Broadly, botnet detection techniques are classified in two [14] [35].

### *A. Host-based Techniques for Botnet Detection*

Host-based botnet detection is also known as client-based botnet detection or stand-alone detection system. Host-based botnet detection techniques encompass all processes involved in detecting, identifying, and preventing bots and other malicious flows on the host device [36][14], these methods are ancient ways of determining whether the host device is compromised by way of incessantly checking the network connection, process files and registries underneath controlled situation the host-based detection works, but work by [18] considers host-based botnet detection less realistic for detecting compromised devices due to some reasons they discovered. However, bot malicious software running on the compromised devices easily detect these kinds of detection methods, in an attempt to evade the bot's malicious activity on the host devices, the botmaster employed different anti-detection techniques such as rootkits-enable, code obfuscation, and the likes, thereby making botnet detection hard to security professionals [14].

### *B. Network-based Detection Techniques*

Network-based bot detection is a more preferred technique compare to host-based bot detection. Network-based techniques involve the analysis of DNS traffic flow, network behaviour as a result of bots running on the network. The resistance techniques employed by the attackers' such as encryption, fast-flux, and domain flux to make the bots more resilient and resistant to detection methods produce further traits that be so conspicuous via the DNS traffic flow analysis. Network-based detection techniques can be further divided into two: 1) Signature-based detection techniques and 2) Anomaly-based botnet detection techniques [37] [38].

### 2. *SIGNATURE-BASED DETECTION TECHNIQUES*

The signature-based botnet detection technique can detect botnets with known signatures. These techniques are effective on predefined botnet features or characteristics, and one of the major drawbacks of signature-based detection techniques is its failure to detect a zero-day attack (i.e. attack with no corresponding signature in the repository) [38].

### 3. *ANOMALY-BASED DETECTION TECHNIQUES*

The third detection technique relies on distinct domain name system inconsistency to identify the botnets. Anomaly-based botnet detection approach does not require signatures to detect bot or malware. In addition, an anomaly-based detection technique can even identify unknown attacks depending on the similar behavior of other bot activities.

### 4. *MACHINE LEARNING TECHNIQUES*

Machine learning (ML) techniques have also pave way for themselves into botnet detection approaches because of their usefulness and robustness in the area among others. Machine learning, been a subset of Artificial Intelligence (AI), where machines will make to mimic human beings in virtually all aspects of human endeavor through machine learning. It is used to train a system to learn how to detect and classify whether or not a network traffic flow belongs to a malware bot or benign. Supervised and unsupervised ML are the most used types of machine learning in botnet detection techniques.

## V. RESULTS AND DISCUSSION

The summary of reviewed domain name system based botnet detection techniques is presented in this section from the reviewed literatures. Table 1 presents a tabular form of the summary and the detailed summary comprises of publication year, detection technique/method, design details, strength and limitation respectively.

As mentioned in table 1, it is evident that, due to the size and sophisticated nature of the emerging botnets, host-based detection techniques work well only on the host devices and do not detect unknown botnet and also, have little or no ability to detect botnet over the network. While Network-based detection techniques work effectively only on known botnet signatures stored in the memory over the network.

Machine learning techniques are mostly employed in detecting botnet attacks for machine learning approaches have proven effectiveness in terms of accuracy and true positive rates only that machine learning techniques are computationally expensive and complex in implementation. Several techniques used in detecting domain name system

 DOI : 10.35291/2454-9150.2022.0099 

based botnet attacks as surveyed in this study have one drawback or the other. However, Machine learning techniques demonstrated efficiency and effectiveness in detecting DNS botnet over the network traffic

**Table 1: Summary of Domain Name System based botnet detection techniques**

| Detection Approach | Year | Category | Design Details | Detection Method | Drawbacks |
|---|---|---|---|---|---|
| Ramachandran et al.[2] | 2006 | Signature Based | Detects spam traffic | It Monitors DNS traffic against an IP blacklist database | Only detect reconnaissance Botmaster and need to update DNSBL database |
| Guofei Gu et al. [6] | 2007 | Signature Based | Intrusion Detection System - Driven Dialog Correlation Strategy | Intrusion Detection System | Unable to detect new malware's |
| Guofei Gu et al. BotSniffer [7] | 2008 | Network-Anomaly based | Similarity Analysis of Command & Control activities | Detect centralized C & C activities | It's not robust for encrypted communication |
| Villamarin et al. [9] | 2008 | Anomaly based botnet | It exhibits high DDNS query rates replies | Chebyshev's inequality | Misclassify legitimate domains if TTL value is low |
| Hyunsang Choi et al. BotGAD[10] | 2009 | DNS based | It Focuses on group activities of botnets | Kulczynski, Cosine and Jaccard similarities | It requires high Processing time |
| Yadav et al. [ 12] | 2010 | DNS based | Able to detect DGA | Kullback-Leibler divergence and Jaccard index. | In-effective for known botnets |
| Leyla Bilge et al. Exposure[13] | 2011 | DNS based | Carried out passive DNS analysis | Decision Tree | It has access to massive RDNS sensors in different locations |
| Manos Antonakakis et al. Kopis[14] | 2011 | DNS based | It Analyzes the Domain Name System Traffic at TLD | Utilizes the Statistical features | It's very much ineffective for DNS resolutions with short epochs |
| Bilge et al. [18] | 2011 | DNS based | Monitoring of DNS traffic to detect malicious behaviours | Through machine learning classifier it identifies new botnet | The detection model is inefficient. |
| Antonakakis et al. [16] | 2012 | DNS based | Analyzes unsuccessful DNS resolution | Hidden Markov Model | Unable to differentiate botnets with similar DGA |
| Schiavoni et al. Phoenix[21] | 2014 | DNS based | Classifies DGA domains | Unsupervised machine learning | Less accuracy for pronounceable domains |
| Kheir et al. [23] | 2014 | DNS based | Removes authenticated/legitimate domains from the blacklist. | Supervised machine learning technique | Only identify legitimate domains; weak against hybrid botnet |
| Reza Sharifnya et al. DFBotkiller[24] | 2015 | DNS based | Gives high-negative reputation score | Spearman Rank Coefficient for Correlation | It requires massive history of suspicious domain activities |
| Jonghoon Kwon et al. PsyBog[26] | 2016 | DNS based | This utilized simultaneous and periodic behavior of botnet queries | Power spectral density analysis | Randomized query patterns reduces efficiency |
| Han Zhang et al. BotDigger[27] | 2016 | DNS based | It detects bot from DNS traffic which is collected across a single network. | Single Linkage hierarchical clustering algorithm | It fails to detect, if bot hits Command &Control in few attempts. |
| Xi Luo et al. DGASensor[30] | 2017 | DNS based | It Utilizes domain information to detect DGA domains. | Random forest algorithm | Syntactic structures reduces efficiency |
| Alenazi et al. [31] | 2017 | DNS based | Able to detect insignificant DNS. | DNS Traffic Analysis | Requires High computing resources and training time |
| Gadelrab et al. [34] | 2018 | DNS based | It identifies and detects the bots without collecting large volumes of data | Feature-statistical features of botnet traffic | Low detection rate |
| Alieyan *et al*. [35] | 2019 | DNS based | Detects abnormal DNS query and response behaviours. | DNS-rule Based Schema | Effective only on DNS-based traffic flow was considered |
| Shi & Sun et al. [36] | 2020 | DNS based | Used a hybrid approach to classify botnet based on DNS | Deep learning method | To discover new categories of botnet, it is required to train whole model |

 DOI : 10.35291/2454-9150.2022.0099 

| | | | | | |
|---|---|---|---|---|---|
| Saif Al-mashhadi et al. [40] | 2020 | DNS based | Detect the botnet from DNS traffic using rule based approach. | ML classifier gives high detection accuracy. | Unable to deal with DNS traffic that is encrypted. |

## CONCLUSION

In this paper we have surveyed various techniques used for botnet detection based on domain name system traffic features. The security scientists are facing various challenges for detecting botnets in real-time scenario. As observed in the literature, there are several effective researches available in the area of domain name system based botnet detection and despite the milestone achieved so far in this research domain, none of the techniques has achieved better accuracy in terms of detection. Therefore, researcher's needs to develop more robust domain name system based botnet detection techniques that can detect and prevent the emerging sophisticated botnet attack.

## REFERENCES

[1] Abu Rajab M, Zarfoss J, Monrose F, Terzis A. 2006. A multifaceted approach to understanding the botnet phenomenon. In: Proceedings of the 6th ACM SIGCOMM on Internet measurement.

[2] Ramachandran A, Feamster N, Dagon D (2006) Revealing botnet membership using DNSBL counter-intelligence. In: Proceedings of the 2nd USENIX steps to reducing unwanted traffic on the Internet, pp 49–54.

[3] Al-Ani AK, Anbar M, Manickam S, Al-Ani A (2018) DAD-match: technique to prevent DoS attack on duplicate address detection process in IPv6 link-local network. J Communication 13(6):317–324.

[4] Canavan J (2005) The evolution of malicious IRC bots. In: Virus bulletin conference, pp 104–114.

[6] Guofei Gu, Phillip A Porras, Vinod Yegneswaran, Martin W Fong, and Wenke Lee. Bothunter: Detecting malware infection through ids-driven dialog correlation. In USENIX Security Symposium, volume 7, pages 1–16, 2007.

[7] Guofei Gu, Junjie Zhang, and Wenke Lee. Botsniffer: Detecting botnet command and control channels in network traffic. In NDSS, volume 8, pages 1–18, 2008.

[8] Guofei Gu, Roberto Perdisci, Junjie Zhang, Wenke Lee, et al. Bot- miner: Clustering analysis of network traffic for protocol-and structure- independent botnet detection. In USENIX security symposium, volume 5, pages 139–154, 2008.

[9] Ricardo Villamarin-Salomon and Jose Brustoloni. Identifying botnets using anomaly detection techniques applied to dns traffic.nConsumer Communications and Networking Conference, 2008. CCNC 2008 5th IEEE, pages 476–481.

[10] Hyunsa ng Choi, Heejo Lee, and Hyogon. Botgad: detecting botnets by capturing group activities in network traffic. In Proceedingsnof the 4th International ICST Conference on Communication System software ACM, 2009.

[11] Manos Antonakakis, Roberto Perdisci, David Dagon, Wenke Lee, and Nick Feamster. Building a dynamic reputation system for dns. In USENIX security symposium, pages 273–290, 2010.

[12] Sandeep Yadav, Ashwath Reddy, AL Reddy. Detecting algorithmically generated malicious domain names. In Proceedings of the 10th ACM SIGCOMM conference on Internet measurement, pages 48–61. ACM, 2010.

[13] Leyla Bilge, Engin Kirda, Christopher Kruegel, and Marco Balduzzi. Exposure: Finding malicious domains using passive dns analysis. In Ndss, 2011.

[14] Manos Antonakakis, Roberto Perdisci, Wenke Lee, Nikolaos Vasiloglou, and David Dagon. Detecting malware domains at the upper dns hierarchy. In USENIX security symposium, volume 11, pages 1–16, 2011.

[15] Manasrah AM, Hasan A, Abouabdalla OA, Ramadass S (2009) Detecting botnet activities based on abnormal DNS traffic. arXiv preprint arXiv:09110487.

[16] Manos Antonakakis, Roberto Perdisci, Yacin Nadji, Nikolaos Vasiloglou, and David Dagon. From throw-away traffic to bots: Detecting the rise of dga-based malware. In USENIX security symposium, volume 12, 2012.

[17] Zhong Z, Krasser S, Tang Y (2010) Mining DNS for malicious domain registrations. In: 2010 6th International conference on collaborative computing: networking, applications and worksharing (CollaborateCom). IEEE, pp 1–6

[18] Bilge L, Kirda E, Kruegel C, Balduzzi M, Antipolis S. 2011. EXPOSURE : finding malicious domains using passive DNS analysis. ACM Transactions on Information and System Security 16(4):1–17 DOI 10.1145/2584679.

[19] Nizar Kheir, Fre´de´ric Tran, and Nicolas Deschamps. Mentor: positive dns reputation to skim-off benign domains in botnet c&c blacklists. In IFIP International Information Security Conference, pages 1–14. Springer, 2014.

 DOI : 10.35291/2454-9150.2022.0099 

[20] Khattak S, Ramay NR, Khan KR, Syed AA, Khayam SA (2014) IEEE Commun Surv Tutorials 16(2):898. https://doi.org/10.1109/SURV.2013.091213.00134

[21] Stefano Schiavoni, Federico Maggi, Lorenzo Cavallaro, and Stefano Zanero. Phoenix: Dga-based botnet tracking and intelligence. In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, pages 192–211. Springer, 2014.

[22] Shan G, Wang Y, Xie M, Lv H, Chi X (2014) Visual detection of anomalies in DNS query log data. In: 2014 IEEE Pacific visualization symposium (PacificVis). IEEE, pp 258–261

[23] Kheir N, Tran F, Caron P, Deschamps N. 2014. Mentor: positive DNS reputation to skim-off benign domains in botnet C&C blacklists. In. ICT Systems Security and Privacy Protection. Berlin: Springer, 1–14.

[24] Reza Sharifnya and Mahdi Abadi. Dfbotkiller: Domain-flux botnet detection based on the history of group activities and failures in dns traffic. Digital Investigation, 12:15–26, 2015.

[25] Jonghoon Kwon, Jehyun Lee, Heejo Lee, and Adrian Perrig. Psybog: a scalable botnet detection method for large-scale dns traffic. Computer Networks, 97:48–73, 2016.

[26] Jonghoon Kwon, Jehyun Lee, Heejo Lee, and Adrian Perrig. Psybog: a scalable botnet detection method for large-scale dns traffic. Computer Networks, 97:48–73, 2016.

[27] Han Zhang, Manaf Gharaibeh, Spiros Thanasoulas, and Christos Pa- padopoulos. Botdigger: Detecting dga bots in a single network. In Proceedings of the IEEE International Workshop on Traffic Monitoring and Analaysis, 2016.

[28] [2] K. Alieyan, A. Almomani, A. Manasrah, and M. M. Kadhum, “A survey of botnet detection based on DNS,” Neural Computing and Applications, vol. 28, no. 7, pp. 1541–1558, 2017.

[29] X. Li, J. Wang, and X. Zhang, “Botnet detection technology based on DNS,” Future Internet, vol. 9, no. 4, p. 55, 2017.

[30] Xi Luo, Liming Wang, Mo Sun, and Jing Wang. Dgasensor: Fast detection for dga-based malwares. In 5th International Conference on Communications and Broadband Networking, pages 47–53. ACM, 2017.

[31] A. Alenazi, I. Traore, and K. Ganame, “Holistic Model for HTTP Botnet Detection Based on DNS Traf fi c Analysis,” vol. 3, pp. 1–18, 2017, doi: 10.1007/978-3-319-69155-8.

[32] X. D. Hoang and Q. C. Nguyen, “Botnet detection based on machine learning techniques using DNS query data,” Future Internet, vol. 10, no. 5, p. 43, 2018.

[33] S. Ryu and B. Yang, “A comparative study of machine learning algorithms and their ensembles for botnet detection,” Journal of Computer and Communications, vol. 6, no. 5, pp. 119–129, 2018.

[34] Gadelrab MS, Elsheikh M, Rashwan M. 2018. BotCap: machine learning approach for botnet detection based on statistical features. International Journal of Communication Networks and Information Security (IJCNIS) 10:563–579.

[35] K. Alieyan, A. Almomani, M. Anbar, R. Abdullah, and B. B. Gupta, “DNS rule-based schema to botnet detection,” Enterp. Inf. Syst., vol. 00, no. 00, pp. 1–20, 2019, doi: 10.1080/17517575.2019.1644673.

[36] Shi WC, Sun HM. 2020. DeepBot: a time-based botnet detection with deep learning. Soft Computing 24(21):16605–16616 DOI 10.1007/s00500-020-04963.

[37] . K. Alieyan, A. Almomani, M. Anbar, R. Abdullah, and B. B. Gupta, “DNS rule-based schema to botnet detection,” Enterp. Inf. Syst., vol. 00, no. 00, pp. 1–20, 2019, doi: 10.1080/17517575.2019.1644673.

[39] Tzy-Shiah Wang, Hui-Tang Lin, Wei-Tsung Cheng, and Chang-Yu Chen. Dbod: Clustering and detecting dga-based botnets using dns traffic analysis. Computers & Security, 64:1–15, 2017.

[40] Al-Mashhadi S, Anbar M, Karuppayah S, Al-Ani AK. 2019. A review of botnet detection approaches based on DNS traffic analysis. In Intelligent and Interactive Computing Singapore, 305–321.

[41] Alieyan K, Almomani A, Anbar M, Alauthman M, Abdullah R, Gupta BB. 2021. DNS rule-based schema to botnet detection. Enterprise Information Systems 15(4):545–564 DOI 10.1080/17517575.2019.1644673.

[42] S. E. Mathew and A. Pauline, “Classification of dga botnet detection techniques based on dns traffic and parallel detection technique for dga botnet,” in Advances in Intelligent Systems and Computing, 2021, vol. 1167, pp. 297–304.

 DOI : 10.35291/2454-9150.2022.0099 