DNS Tunnel Problem In Cybersecurity

Güneş Gürsoy
Dept. of Computer Engineering
College of Eng. and Natural Sciences
Maltepe University
İstanbul, Turkey
gunesgursoy@hotmail.com
ORCID: 0000-0003-3716-0334

Asaf Varol
Dept. of Eng. Management and Technology
College of Eng. and Computer Science
The Uni. of Tennessee at Chattanooga
Chattanooga, TN, US
asaf-varol@utc.edu
asafvarol@maltepe.edu.tr
ORCID: 0000-0003-1606-4079

Ahad Nasab
Dept. of Eng. Management and Technology
College of Eng. and Computer Science
The Uni. of Tennessee at Chattanooga
Chattanooga, TN, US
ahad-Nasab@utc.ede
ORCID: 0000-0001-6069-0822

2024 12th International Symposium on Digital Forensics and Security (ISDFS) | 979-8-3503-3036-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/ISDFS60797.2024.10527301

***Abstract*— The Domain Name System (DNS) is the most important building block of the Internet. Websites, file transfer applications, and e-mail services use the DNS service. Therefore, these services can rarely be blocked by firewalls to prevent their access from being affected. Since applications such as firewalls and Intrusion Detection Systems (IDS) do not check the allowed protocols, attackers can open a secret path called DNS Tunnel through the DNS protocol to access sensitive data and cause many attacks. In this study, DNS Tunnel, DNS Tunnel detection methods and detection methods, and DNS attack types are included.**

Keywords — cybersecurity, machine learning, deep learning, DNS Tunneling

I. INTRODUCTION

All devices connected to the Internet have an IP (Internet Protocol) address, through which they reach the desired destination. These can be websites, e-mail servers, applications, and IoT (Internet of Things) devices (cameras, phones, refrigerators, vehicles, etc.). DNS resolves domain names to IP addresses, allowing that address to access an internet-based service (web, email, file server, etc.). DNS is usually not blocked by major firewalls and intrusion detection (IDS) software because many applications and services use DNS and blocking the DNS protocol will cause problems accessing services such as web, e-mail, file servers, etc. Attackers take advantage of this and use the DNS protocol to access networks. Therefore, the convenience provided by the unblocked DNS protocol plays a central role in ensuring that many services are not affected by cyber-attacks [1].

With the number of devices connected to the internet, the volume of sensitive data stored on computers is increasing, creating security risks. In 2020, 130 high-profile twitter accounts were breached, including Elon Musk, and Bill Gates [1]. In 2020, in a report prepared by the National Cyber Security Centre (NCSC) and Canada's Communications Security Establishment (CSE), a group called "APT29" stated that they developed malware known as WellMess and WellMail to steal information about the development and testing of COVID-19 vaccines and that the protocols and services supported in the use of this software are HTTP, TLS, and DNS [2]. When the responses of companies participating in a study on the importance of DNS are compared between 2022 and 2023, the rate for remote working increased from 54% in 2022 to 77% in 2023, for IoT devices from 51% in 2022 to 54% in 2023, for Cloud from 56% in 2022 to 84% in 2023, and for Datacenters from 48% in 2022 to 70% in 2023 [3]. In the same report, the average cost of each attack is stated as 1.1 million USD [3]. Microsoft's "Microsoft Digital Defense Report 2023" states that the cost of cybercrime is estimated to be 10.5 trillion USD annually by 2025 [4].

Another study on cyberattacks in general shows that cyberattacks in 2023 were 5.5 billion malware attacks with a 2% increase compared to the previous year, 6.3 trillion intrusions with a 19% increase, 139. 3 million cryptojacking attacks with a 43% increase and 112.3 million malware attacks were detected with an 87% increase on IoT devices, which are expected to be 26 billion units worldwide by 2030 [5], while encrypted threads decreased by 28% with 7.3 million attacks and ransomware attacks decreased by 21% with 493.3 million attacks [6].

With the developing technology, measures can be taken with artificial intelligence against increasing risks. Machine learning, deep learning, and other techniques are used to detect and prevent these attacks. Research organization Gartner estimates that artificial intelligence will detect 90% of cyber-attacks and that the intervention of artificial intelligence in these attacks will be 60% [7].

II. DNS

The first version of the DNS protocol was published in 1984 by Paul Mockapetris. It has a decentralized hierarchical structure developed to resolve IP addresses into names, allowing the naming of resources. DNS performs name resolution over port 53 in the UDP protocol. Since security requirements were not considered at the time of its development, many different attacks (DNS Tunneling, DNS Poisoning, DoS and DDoS Attack, DNS Hijacking, DNS Amplification, etc.) are carried out by attackers through DNS [8].

The limits used in DNS are important for monitoring anomalies in DNS Tunnel detection. In the RFC 1035 publication, the limits of DNS are given as follows.

Labels: 63 octets or less
Names: 255 octets or less
TTL: Positive values of a signed 32-bit number.
UDP messages: 512 octets or less

Changes in these limits are used in various research to monitor and identify unnatural DNS traffic [9]. Due to the critical role of DNS and the presence of security vulnerabilities, attackers use techniques such as DNS Tunneling to exfiltrate data from target computers.

III. DNS TUNNEL

DNS Tunneling is one of the methods of DNS attacks. DNS Tunneling is based on attackers using DNS packets to

perform data exfiltration by creating a command and control (C&C) system between the target computer and their own computers. Attackers need C&C to control malware on target computers, and they need constantly changing domains to perform data exfiltration through queries. To change domains, they use binary or script-based Domain Generation Algorithms (DGAs) that generate fake domain names. By changing DGAs at the time of attack, they manage malware-spreading websites or C&C on target computers [10]. The encapsulated data is transported through queries and responses to the changing domains.

In DNS Tunneling, data from other protocols such as SSH or FTP is encapsulated [11]. DNS data is in plain text format, and data leakage occurs by hiding the data to be hidden in the subdomain of the domain (such as subdomain.domain.com). Since all data is encoded in the subdomain, the attacker also takes control of all name servers belonging to the domain, and when all subdomain resolution requests reach the name servers, the data encapsulated there is obtained by decoding it with a tool used by the attacker [12].

HTTP Tunneling, HTTPS Tunneling, FTP Tunneling and POP3 Tunneling are the types of DNS Tunneling, with HTTP and HTTPS occurring in web browsers, FTP in file transfers and POP3 in e-mail transactions [13]. Attackers do not limit their attacks by using only communication channels, they also use channels such as ICMP tunnels, IPV6 tunnels, SSH tunnels and HTTP/s tunnels. DNS Tunnel is one of these tunnels [14].

DNS Tunneling is a secret way for attackers to access the systems they have identified [15]. With DNS Tunnels, attackers can control many computers infected with malware (Botnet) and damage the networks or servers they have identified. Many data such as customer data, financial data, personal information, health information can be obtained by attackers. Therefore, detecting DNS Tunnels is one of the most important issues for network security.

A. *Working Principle of DNS Tunneling*

The working principle of the DNS Tunnel is described below in order [16].

1) The data from the target computer is converted into Base32, Base64 or Base128 format and added to the DNS query packet to start the query. The DNS query is made from the malware infected computer controlled by the attacker to the DNS server controlled by the attacker. The domain used in the DNS query (for example domain.com) has "." root server, "com" top-level name server and domain.

2) The root server (.) is then queried.

3) The top-level name server (top-level name server like 'com' in Fig.1) is then queried.

4) Next, the obfuscated name server (attacker.com in Figure 1) is queried.

5) The disguised name server decodes the DNS packet to receive the incoming message and replies with an encoded DNS response.

6) This process is repeated.

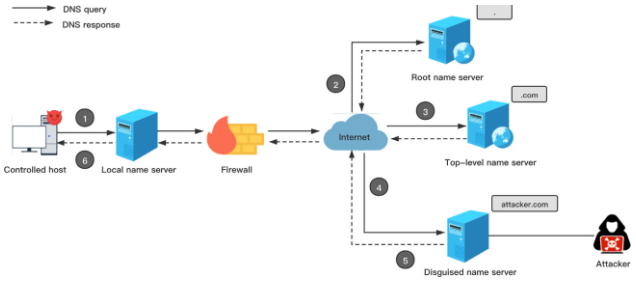

Fig. 1. DNS tunnel communication between Attacker and Controlled Host [16].

B. *Other Types of DNS Attacks*

The DNS Tunnel is not only used for communication and data exfiltration. Malware uses the DNS Tunnel for different purposes such as BotNet distribution and control, attacks on sales terminals (POS Devices) and network attacks [17]. Apart from DNS Tunnel attacks, different attacks are also carried out through DNS. In general, attacks on the DNS system are divided into two as DNS protocol related and DNS misuse. DNS attacks that exploit the shortcomings and weaknesses of the DNS protocol are attacks such as DNS cache poisoning, DNS spoofing and phishing, and the other is DNS abuse attacks such as DOS, DDOS, cache poisoning, which consume the resources of the DNS system and try to prevent its functioning [18].

Some DNS attacks outside the DNS Tunnel are briefly described below.

a) *DNS Poisoning* : DNS Cache Poisoning is when an attacker makes DNS data unusable or modifies it for malicious routing [19].

b) Random Subdomain Attack : DNS Random Subdomain Attack is a type of DNS attack that causes denial of service by querying non-existent subdomains in DNS servers [20] .

c) DDoS Attack : DDoS attacks are a type of DNS attack that uses clients and servers, uses the resources of other computers as an attack tool, and makes a website or service temporarily or permanently inoperable [21].

d) DNS Hijacking : In this type of attack, attackers cause false responses to DNS queries to redirect users to servers (websites) requested by the attacker [22]. This allows attackers to capture user and password information, credit card details, etc. of users who are redirected to malicious websites.

e) DNS Amplification : A type of DDoS attack that uses DNS resolvers to mirror and amplify network traffic, using zombie computers on the attacker's side to disrupt or slow down the target system by consuming its resources [23].

f) *Botnet-Based Attacks* : Botnets are among the most serious dangers on the Internet, a network of compromised and vulnerable computers used by an attacker for malicious purposes [24].

g) *TCP SYN Floods* : TCP/IP is the most commonly used data communication protocol. TCP/IP data transmission takes place in three phases. This is called a handshake. First, a SYN (Syncronize) message is sent from the client to the server. Then the server returns by adding an ACK (acknowledge) message to the client's message (SYN+ACK) and finally the client returns to the server with an ACK message of acknowledgment and communication is established. Here the attacker sends the SYN packet to the

server, but since the source IP address will not be available, the ACK message from the server will not be responded to, so the server will renew the SYN+ACK message to the client and the timeout will double with each renewal (3, 6, 12, 24, 48, 96 seconds etc.). Eventually the timeout becomes so long that no requests, including real requests, can be responded to and the system goes down [25].

IV. DNS Tunnel Detection and Prevention

DNS queries have a minimum character range of 64 characters and an upper limit of 256 characters. Data leaks using the DNS Tunnel can change these character counts, so it is important to keep these character counts in mind [9].

DNS servers use the DNS cache, which holds previous queries, to process incoming data more quickly in queries. The DNS cache generates a cache hit for data leaks using the DNS Tunnel. A cache hit is when the data or query is found in memory. In other words, the presence of this data in the DNS cache indicates a data leak [26]. Therefore, malware directly connects to the DNS cache during the data leakage process [26].

There are different methods for detecting and blocking DNS Tunnels. In general, these methods are divided into rule-based and model-based methods. Rule-based methods, which are easy to implement and deploy on different platforms but are easily overcome by attackers, are methods that manually analyze the content and signature matches of DNS traffic, while model-based methods are methods based on deep learning using algorithms such as Convolutional Neural Networks (CNN), Long Short Term Memory (LSTM) with machine learning and automatic feature extraction using supervised learning algorithms using labeled data sets or unsupervised learning algorithms using unlabeled data sets [27].

The various methods are presented below.

a) Machine Learning: In DNS Tunnel detection methods, statistical methods that take into account the size of DNS request/response packets, source record types, packet lengths, and domain name length, using methods such as mean, variance, skewness, and kurtosis, and deep learning algorithms based on neural networks such as LSTM, Recurrent Neural Networks (RNN), CNN, classification and clustering algorithms of machine learning are also used [28].

b) *Payload Analysis and Traffic Analysis*: Other detection methods include load analysis and traffic analysis techniques. Load analysis refers to the evaluation of the response received when a DNS query occurs, while traffic analysis refers to the evaluation of DNS traffic during the monitoring period [26]. However, since these methods do not always provide accurate results and are easily circumvented by attackers, deep learning and machine learning algorithms that provide more reliable results are also used in DNS Tunnel detection [29]. Hybrid models created by using machine learning and deep learning algorithms together increase the success rate. When the automatic feature extraction of deep learning and the classification capabilities of machine learning algorithms are combined, satisfactory results are obtained.

c) *DNS-over-HTTS (DoH)* : By default, DNS queries are sent in plain text over UDP, which means that any user can read DNS traffic [30]. To prevent this, DNS over HTTPS (DoH) was developed, which runs on web browsers and uses TCP port 443. DoH encrypts DNS queries to protect the connection between the end user and the recursors and authenticates the user with SSL [31]. However, since DoH traffic is not identifiable in other HTTPS traffic, attackers can exfiltrate encrypted data through DoH tunnels [30].

d) DNS-over-TLS (DoT) : Clients and servers negotiate a handshake over the encryption protocol Transport Layer Security (TLS), and DNS messages transmitted over TCP are encrypted, preventing the data from being accessed secretly [32]. Standardized in 2016, DoT has been supported by Google Android since 2018 and Apple desktop and mobile operating systems since 2020 [33]. However, since DoT does not provide 100% complete protection, attackers can use it to fingerprint websites that contain metadata with unique attributes such as timestamps, cookies, user settings, etc. [33]. DoT uses port 853 by default.

e) Passive DNS: Another method for detecting DNS Tunneling attacks is to use the Passive DNS method, which was developed by Florian Weimer in 2004 to take precautions against data leaks and malicious domain hijacking [34]. In a normal DNS query, the DNS query is resolved simultaneously by DNS Servers, whereas in Passive DNS, the query is first registered in a DNS database, which is then analyzed to detect malware or unusual conditions [35].

Tunnels detected with different methods can be blocked with different techniques. In addition to DNS TXT records, analysis of domain name lengths, statistical analysis of DNS packets, classification methods using time series (algorithms such as RNN, LSTM), and blacklisting of domain names and IP addresses are also methods that help in the detection and blocking of DNS Tunnels [36].

V. Related Works

J.Liang et al. studied a model called Feature Extraction CNN and Clustering (FECC), which is a combination of CNN and k-means clustering algorithms for the detection and evaluation of DNS Tunnel traffic, and observed that this model gave satisfactory results in both classification and detection of unknown samples [28].

Borges et al. used unsupervised learning from machine learning techniques for anomaly detection over an AWS cloud-based system. They used Poisson, Gaussian, and log-normal probability distributions and concluded that the DNS Tunnel was successfully detected by the anomaly detection method [11].

In their study, J. Zhang et al. applied an approach based on deep learning models using 1D-CNN, RNN, and DNN for DNS Tunnel detection. They found that the accuracy rate of the model they developed with the methods they applied in a real network environment was 99.90% [37].

G. Sakarkar et al. worked on a natural language processing-based approach for DNS Tunnel detection using timestamp, source and destination address, protocol, length of network packets, and packet information. They observed that the LSTM model they developed has a 98.42% accuracy rate, which is higher than GRU, 1D-CNN, and RNN models, and is effective in detecting malicious and non-malicious network packets [38].

According to M. Zhan, they analyzed TLS fingerprints of DoH clients for DoH and DNS Tunneling detection and observed that this method can detect DoH Tunneling [12].

In their work, C. Qi et al. designed a solution that can distinguish in real-time whether a DNS packet is present in the DNS Tunnel by scoring domain names based on Bigram character frequency. They achieved high accuracy using correct (normal) domains published by Alexa and domains generated by DNSCAT [39].

In their study S. Chen used LSTM, a deep learning algorithm for DNS Tunnel detection in a real network environment. They applied the end-to-end LSTM detection approach by taking the Full Qualified Domain Name (FQDN) addresses of DNS Packets as input, then created a model with the packets they created from the internet and by running different DNS Tunnel tools and obtained a 99.38% accuracy rate over the test data set with the methods they created [40].

J. Liu et al. used a binary classification approach. They used time interval feature, request packet size, record type features, and subdomain entropy features as features in their proposed methods and evaluated the performance of their models with machine learning algorithms Support Vector Machines (SVM), Decision Tree, and Logistic Regression and obtained an accuracy rate of 99.96% [41].

According to Y. Chen et al. designed a model that automatically extracts features using LSTM and Gated Recurrent Unit (GRU) for DNS Tunnel detection. The Char-CNN technique in their study gave higher classification accuracy than LSTM, GRU, and Kernel-SVM algorithms [42].

A. Chowdhar et al. used the entropy of hostname for DNS Tunnel query detection. They chose the length of the query and entropy as two main features and evaluated the overall performance with Gaussian Naive Bayes, Multinomial Naive Bayes (NB), Bernoulli Naive Bayes, Random Forest (RF), Decision Tree (DT), Multilayer Perceptron (MLP), Linear Support Vector Machine (LSVM), Quadratic Support Vector Machine (QSVM) and K-Nearest Neighbors (KNN) algorithms. Among these algorithms, the KNN algorithm gave the highest accuracy rate with 93.95% [43].

Xiao Dong Li et al. categorized the available domain name features into three groups as payload-based features, traffic-based features, and resolution-based features to detect DNS Tunneling and then built a classification model with Logistic Regression and Random Forest from supervised learning algorithms of machine learning. They observed that the model they developed gave good performance [44].

According to A. Almusawi, used Multilabel Support Vector Machine, a machine learning algorithm for DNS Tunnel detection and classification using Java programming language. To evaluate the performance of their model, they compared it with the Multilabeled Bayes classifier and observed that SVM is a more effective method [13].

Chen et al. developed an automatic feature extraction model for DNS Tunnel detection using an LSTM language model with an attention mechanism and a gated recurrent unit (GRU) language model with an attention mechanism. They observed that they achieved high accuracy with LSTM and GRU based on a character-level convolutional neural network, which they proposed as a classifier [45].

Z. Yang et al. used machine learning algorithms KNN, SVM, DT, and RF classifiers to detect DNS Tunnels using DNS session behaviors and observed that the RF classifier gave the highest accuracy rate [46].

Anushka Lal et al. developed a hybrid model for the DNS Tunnel using CNN feature extraction from deep learning algorithms and SVM from machine learning classifiers. In addition to SVM, they also used KNN, DT, and RF algorithms in their experiments, and the RF classifier gave the highest accuracy rate in their tests [47].

H. Jha et al. developed models for DNS over HTTPS (DoH) tunnel detection based on the size of DNS packets and request times using machine learning classifiers KNN, SVM, RF, and DeepFM, a hybrid model and observed that the highest accuracy rate for DNS tunnel identification was 99.5% with DeepFM, followed by 99.3% with SVM and 99.3% with RF [48].

According to A. Nguyen et al. developed a model for detecting malicious DoH tunnels using semi-supervised learning and statistical features of machine learning with a dataset consisting of labeled and unlabeled data. They achieved a 98% success rate in DoH tunnel detection with the semi-supervised method [30].

O. Abualghanam et al. used a Pigeon-inspired Optimization (PIO) feature extraction algorithm and DNS packet lengths for DNS tunnel detection and developed a hybrid model with a 98.3% accuracy rate, which is better than other studies using the same dataset [49] .

According to D.Tatang in their DNS Tunneling detection study, they proposed that NULL and TXT records from DNS requests are related to DNS Tunneling and that almost all NULL records can be completely blocked because they are DNS Tunneling [17] .

C. Liu et al. propose a model (Byte-level CNN Method) that translates DNS data into byte-level computable CNN models. They compare machine learning methods such as SVM, LR, and Neural Networks (NN) with their method and observe that their method can learn sequential and structured information in DNS packets, avoids manual feature extraction and their model achieves better results than traditional machine learning methods. [50].

VI. Conclusion

DNS is a name resolver system whose structure has not changed much since its development. It has security vulnerabilities since it was developed only as a name resolver. There are many types of DNS attacks and various methods developed to detect attacks and data leaks. Machine learning and deep learning algorithms, a sub-branch of artificial intelligence, which will detect and block anomalies in DNS traffic in blocking remote DNS Tunneling, as well as users being aware of malware and taking precautions, which is the most definitive solution, come to the fore in many studies. Especially deep learning algorithms with less human intervention will give better results in detecting and preventing DNS Tunneling and other DNS attacks by monitoring the normal behavior of the network and detecting and detecting abnormal behavior.

REFERENCES

[1] T. S. Chad Anderson, John 'Turbo' Conwell, "Investigating cyber attacks using domain and DNS data", doi: https://doi.org/10.1016/S1353-4858(21)00028-3.

[2] N. C. S. Centre, "Advisory: APT29 targets COVID-19 vaccine development," *2020*, no. July 2020, [Online]. Available: https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development

[3] P. Detection and E. Threat, "Augmenting Cyber Threat Intelligence," no. August 2023.

[4] M. T. Intelligence, "Microsoft Digital Defense Report," *Network Security*, vol. 2020, no. 10, pp. 4–4, 2020, doi: 10.1016/s1353-4858(20)30114-8.

[5] Statista, "Cybersecurity: market data & analysis," Market Insights report. [Online]. Available: https://www.statista.com/study/124902/cybersecurity-report/

[6] SonicWall, "SONICWALL CYBER THREAT REPORT sonicwall.com I @sonicwall," p. 69, 2023, [Online]. Available: https://www.sonicwall.com/medialibrary/en/white-paper/2020-sonicwall-cyber-threat-report.pdf

[7] Gartner, "Gartner Opening Keynote: Cybersecurity 2032: Accelerating the Evolution of Cybersecurity." [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2022-06-07-gartner-security-and-risk-management-summit-national-harbor-day-1-highlights

[8] Sanjay, B. Rajendran, and P. Shetty, "DNS Amplification DNS Tunneling Attacks Simulation, Detection and Mitigation Approaches," *Proceedings of the 5th International Conference on Inventive Computation Technologies, ICICT 2020*, pp. 230–236, 2020, doi: 10.1109/ICICT48043.2020.9112413.

[9] S. Sugasawa, Y. Shibahashi, H. Kunimune, H. Goromaru, and S. Tanimoto, "DNS-tunneling-detection Method by Monitoring DNS Subdomain Length for General Usage," *2022 IEEE 11th Global Conference on Consumer Electronics (GCCE)*, pp. 121–122, 2023, doi: 10.1109/gcce56475.2022.10014255.

[10] A. K. Sood and S. Zeadally, "A Taxonomy of Domain-Generation Algorithms," *IEEE Secur Priv*, vol. 14, no. 4, pp. 46–53, 2016, doi: 10.1109/MSP.2016.76.

[11] L. De Souza Bezerra Borges, R. De Oliveira Albuquerque, and R. T. De Sousa Junior, "A security model for DNS tunnel detection on cloud platform," *2022 Workshop on Communication Networks and Power Systems, WCNPS 2022*, no. Wcnps, pp. 5–10, 2022, doi: 10.1109/WCNPS56355.2022.9969715.

[12] M. Zhan, Y. Li, G. Yu, B. Li, and W. Wang, "Detecting DNS over HTTPS based data exfiltration," *Computer Networks*, vol. 209, no. February 2022, doi: 10.1016/j.comnet.2022.108919.

[13] A. Almusawi and H. Amintoosi, "DNS tunneling detection method based on multilabel support vector machine," *Security and Communication Networks*, vol. 2018, 2018, doi: 10.1155/2018/6137098.

[14] J. Hou *et al.*, "A Survey of DNS Tunnel Detection," *2022 7th International Conference on Signal and Image Processing, ICSIP 2022*, pp. 338–342, 2022, doi: 10.1109/ICSIP55141.2022.9886602.

[15] J. Liang, S. Wang, S. Zhao, and S. Chen, "FECC: DNS tunnel detection model based on CNN and clustering," *Comput Secur*, vol. 128, 2023, doi: 10.1016/j.cose.2023.103132.

[16] Y. Tu, S. Liu, and Q. Sun, "DNS tunneling detection by fusing encoding feature and behavioral feature," *Comput Secur*, vol. 132, 2023, doi: 10.1016/j.cose.2023.103357.

[17] D. Tatang, F. Quinkert, N. Dolecki, and T. Holz, "A Study of Newly Observed Hostnames and DNS Tunneling in the Wild," 2019, [Online]. Available: http://arxiv.org/abs/1902.08454

[18] X. Guo, Z. Pan, and Y. Chen, "Application of Passive DNS in Cyber Security," *Proceedings of 2020 IEEE International Conference on Power, Intelligent Computing and Systems, ICPICS 2020*, pp. 257–259, 2020, doi: 10.1109/ICPICS50287.2020.9202344.

[19] H. S. H. Z. L. H. K. A. Y. Zhang, "Adaptive Caching Approach to Prevent DNS Cache Poisoning Attack," OUP - Oxford University Press, 2015, pp. 973–985. doi: 10.1093/comjnl/bxu023.

[20] H. Griffioen and C. Doerr, "Taxonomy and adversarial strategies of random subdomain attacks," *2019 10th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2019 - Proceedings and Workshop*, pp. 1–5, 2019, doi: 10.1109/NTMS.2019.8763820.

[21] M. A. Msaad, R. A. Saed, and A. M. Sllame, "A Simulation-based analysis study for DDoS attacks on Computer Networks," *2021 IEEE 1st International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering, MI-STA 2021 - Proceedings*, no. May, pp. 756–761, 2021, doi: 10.1109/MI-STA52233.2021.9464444.

[22] R. Houser, S. Hao, Z. Li, D. Liu, C. Cotton, and H. Wang, "A Comprehensive Measurement-based Investigation of DNS Hijacking," *Proceedings of the IEEE Symposium on Reliable Distributed Systems*, vol. 2021-Septe, pp. 210–221, 2021, doi: 10.1109/SRDS53918.2021.00029.

[23] N. Tripathi, M. Swarnkar, and N. Hubballi, "DNS spoofing in local networks made easy," *11th IEEE International Conference on Advanced Networks and Telecommunications Systems, ANTS 2017*, no. October 2017, pp. 1–6, 2018, doi: 10.1109/ANTS.2017.8384122.

[24] H. Dhayal and J. Kumar, "Botnet and P2P Botnet Detection Strategies: A Review," *Proceedings of the 2018 IEEE International Conference on Communication and Signal Processing, ICCSP 2018*, pp. 1077–1082, 2018, doi: 10.1109/ICCSP.2018.8524529.

[25] L. Kavisankar and C. Chellappan, "A mitigation model for TCP SYN flooding with IP spoofing," *International Conference on Recent Trends in Information Technology, ICRTIT 2011*, pp. 251–256, 2011, doi: 10.1109/ICRTIT.2011.5972435.

[26] N. Ishikura, D. Kondo, I. Iordanov, V. Vassiliades, and H. Tode, "Cache-Property-Aware Features for DNS Tunneling Detection," *2020 23rd Conference on Innovation in Clouds, Internet and Networks and Workshops, ICIN 2020*, no. ICIN, pp. 216–220, 2020, doi: 10.1109/ICIN48450.2020.9059472.

[27] X. Liu *et al.*, "DNS Tunnel Detection for Low Throughput Data Exfiltration via Time-Frequency Domain Analysis," *IEEE International Conference on Communications*, vol. 2023-May, no. Icc, pp. 2331–2337, 2023, doi: 10.1109/ICC45041.2023.10279472.

[28] J. Liang, S. Wang, S. Zhao, and S. Chen, "FECC: DNS tunnel detection model based on CNN and clustering," *Comput Secur*, vol. 128, 2023, doi: 10.1016/j.cose.2023.103132.

[29] G. D'Angelo, A. Castiglione, and F. Palmieri, "DNS tunnels detection via DNS-images," *Inf Process Manag*, vol. 59, no. 3, p. 102930, 2022, doi: 10.1016/j.ipm.2022.102930.

[30] A. T. Nguyen and M. Park, "Detection of DoH Tunneling using Semi-supervised Learning method," *International Conference on Information Networking*, vol. 2022-Janua, pp. 450–453, 2022, doi: 10.1109/ICOIN53446.2022.9687157.

[31] Q. Huang, D. Chang, and Z. Li, "A comprehensive study of DNS-over-HTTPS downgrade attack," *FOCI 2020 - 10th USENIX Workshop on Free and Open Communications on the Internet, co-located with USENIX Security 2020*, 2020.

[32] C. Lu *et al.*, "An End-to-End, Large-Scale Measurement of DNS-over-Encryption: How Far Have We Come?".

[33] A. M. Koshy *et al.*, "An Insight into Encrypted DNS protocol: DNS over TLS," *2021 4th International Conference on Recent Developments in Control, Automation and Power Engineering, RDCAPE 2021*, vol. 3, pp. 379–383, 2021, doi: 10.1109/RDCAPE52977.2021.9633480.

[34] C. Liu, "Actively boosting network security with passive DNS," 2016, pp. 18–20. doi: https://doi.org/10.1016/S1353-4858(16)30050-2.

[35] Y. Wang, A. Zhou, S. Liao, R. Zheng, R. Hu, and L. Zhang, "A comprehensive survey on DNS tunnel detection," *Computer Networks*, vol. 197, no. January, p. 108322, 2021, doi: 10.1016/j.comnet.2021.108322.

[36] M. Montazerishatoori, L. Davidson, G. Kaur, and A. Habibi Lashkari, "Detection of DoH Tunnels using Time-series Classification of Encrypted Traffic," *Proceedings - IEEE 18th International Conference on Dependable, Autonomic and Secure Computing, IEEE 18th International Conference on Pervasive Intelligence and Computing, IEEE 6th International Conference on Cloud and Big Data Computing and IEEE 5th Cybe*, pp. 63–70, 2020, doi: 10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00026.

[37] M. J. Jiacheng, Zhang, Yang Li, Yu Shui, "A DNS Tunneling Detection Method Based on Deep Learning Models to Prevent Data Exfiltration," 2019. doi: 10.1007/978-3-030-36938-5_32.

[38] G. Sakarkar *et al.*, "Advance Approach for Detection of DNS Tunneling Attack from Network Packets Using Deep Learning Algorithms Advance Approach for Detection of DNS Tunneling Attack from Network Packets Using Deep Learning Algorithms Advance Approach for Detection of DNS Tun," *ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal Regular Issue*, vol. 10, no. 3, pp. 241–266, 2021.

[39] C. Qi, X. Chen, C. Xu, J. Shi, and P. Liu, "A bigram based real time DNS tunnel detection approach," *Procedia Comput Sci*, vol. 17, pp. 852–860, 2013, doi: 10.1016/j.procs.2013.05.109.

[40] S. Chen, B. Lang, H. Liu, D. Li, and C. Gao, "DNS covert channel detection method using the LSTM model," *Comput Secur*, vol. 104, p. 102095, 2021, doi: 10.1016/j.cose.2020.102095.

[41] J. Liu, S. Li, Y. Zhang, J. Xiao, P. Chang, and C. Peng, "Detecting DNS tunnel through binary-classification based on behavior features," *Proceedings - 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 11th IEEE*

International Conference on Big Data Science and Engineering and 14th IEEE International Conference on Embedded Software and Systems. pp. 339–346, 2017. doi: 10.1109/Trustcom/BigDataSE/ICESS.2017.256.

[42] Y. Chen and X. Y. Li, "A High Accuracy DNS Tunnel Detection Method without Feature Engineering," *Proceedings - 2020 16th International Conference on Computational Intelligence and Security, CIS 2020*, pp. 374–377, 2020, doi: 10.1109/CIS52066.2020.00086.

[43] A. Chowdhary, M. Bhowmik, and B. Rudra, "DNS tunneling detection using machine learning and cache miss properties," *Proceedings - 5th International Conference on Intelligent Computing and Control Systems, ICICCS 2021*, no. Icicc, pp. 1225–1229, 2021, doi: 10.1109/ICICCS51141.2021.9432279.

[44] X. D. Li, Y. F. Song, and Y. Q. Li, "DNS Tunnel Detection Scheme Based on Machine Learning in Campus Network," *Proceedings - 2022 4th International Conference on Machine Learning, Big Data and Business Intelligence, MLBDBI 2022*, pp. 253–257, 2022, doi: 10.1109/MLBDBI58171.2022.00056.

[45] Y. Chen and X. Y. Li, "A High Accuracy DNS Tunnel Detection Method without Feature Engineering," *Proceedings - 2020 16th International Conference on Computational Intelligence and Security, CIS 2020*, pp. 374–377, 2020, doi: 10.1109/CIS52066.2020.00086.

[46] Z. Yang, Y. Hongzhi, L. Lingzi, H. Cheng, and Z. Tao, "Detecting DNS tunnels using session behavior and random forest method," *Proceedings - 2020 IEEE 5th International Conference on Data Science in Cyberspace, DSC 2020*, pp. 45–52, 2020, doi: 10.1109/DSC50466.2020.00015.

[47] A. Lal, A. Prasad, A. Kumar, and S. Kumar, "DNS-Tunnet: A Hybrid Approach for DNS Tunneling Detection," *CTISC 2022 - 2022 4th International Conference on Advances in Computer Technology, Information Science and Communications*, pp. 1–6, 2022, doi: 10.1109/CTISC54888.2022.9849774.

[48] H. Jha, I. Patel, G. Li, A. K. Cherukuri, and S. Thaseen, "Detection of Tunneling in DNS over HTTPS," *2021 7th International Conference on Signal Processing and Communication, ICSC 2021*, pp. 42–47, 2021, doi: 10.1109/ICSC53193.2021.9673380.

[49] O. Abualghanam, H. Alazzam, B. Elshqeirat, M. Qatawneh, and M. A. Almaiah, "Real-Time Detection System for Data Exfiltration over DNS Tunneling Using Machine Learning," *Electronics (Switzerland)*, vol. 12, no. 6, pp. 1–21, 2023, doi: 10.3390/electronics12061467.

[50] C. Liu, L. Dai, W. Cui, and T. Lin, "A Byte-level CNN Method to Detect DNS Tunnels," *2019 IEEE 38th International Performance Computing and Communications Conference, IPCCC 2019*, pp. 1–8, 2019, doi: 10.1109/IPCCC47392.2019.8958714.