WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Real-Time Traffic Fingerprinting for Detecting Encrypted Network Threats In Intrusion Detection Systems

M. Hariharan

Department of Forensic Science, Msc in Forensic Science Garden City University, Bangalore, Karnataka, India

A B S T R A C T :

Network security is the key concern in recent years, which has increased the usage of the encrypted form of network communication that improves the data privacy and security which makes it more difficult in identifying the criminals. Due to its lack in the visibility of the packet information in the encrypted data, the traditional intrusion detection systems frequently struggle in identifying the threats. Instead of depending on payload inspection, real-time traffic fingerprinting provides a possible alternative by assessing traffic patterns, metadata, and flow characteristics. This study investigates how enhanced traffic fingerprinting techniques may be used to detect and identify encrypted network threats more efficiently. The methods can differentiate between valid and malicious encrypted communications in real-time using machine learning models and statistical analysis. The suggested approach improves intrusion detection by concentrating on unique traffic characteristics such as packet sizes, time intervals, and flow patterns that stay consistent even after encryption. Experiments show that the system can achieve high detection accuracy and low false positive rates, making it a viable answer to current network security concerns. This research helps to improve the effectiveness of IDS in monitoring and protecting encrypted communications without jeopardizing data privacy.

Keywords: Intrusion Detection System, Encrypted Data, Network threats, Real time Traffic Fingerprinting, Malware.

1. Introduction

The state of network communication security is more serious now than ever given the wider digital abuse landscape. As the cyber threat evolves, many firms are adopting data-in-transit encryption to secure it. While encryption of data in transit provides confidentiality and integrity of data, it also brings new challenges for network security systems, in particular an Intrusion Detection System (IDS). The overall decrease in volume of non-encrypted data packets is limiting access to inspect and analyze packets and traffic at the packet level using traditional signature or pattern matching based techniques. Overall, there is a greater need to discover new methodologies to identify threats that may be hiding under encrypted traffic, but still privacy sensitive. Real-Time Traffic Fingerprinting is one potential approach. Real-Time Traffic Fingerprinting refers to the act of analyzing metadata and behavioural patterns of network traffic with the aim of identifying potential threats. In contrast to deep packet inspection, which checks for the actual content carried within data packets, traffic fingerprinting relies on features such as packet size, timing, direction of flow, and frequency. These features can have the capability to reveal anomalies indicating malicious behaviour even when traffic is encrypted.

By focusing on traffic behaviour rather than content, fingerprinting techniques offer a privacy-preserving and efficient method of threat detection that is well-suited for modern encrypted environments. Real-Time Traffic Fingerprinting also has the advantage of being compatible with machine learning and artificial intelligence. These systems have the potential to greatly improve fingerprinting accuracy and efficiency by learning from past traffic patterns and adjusting to new risks. Supervised learning algorithms, for example, may be trained on labelled datasets to recognise known attack signatures, but unsupervised learning can aid in the discovery of previously unknown abnormalities. Integrating machine learning with traffic fingerprinting not only increases detection rates but also minimizes false positives, which are a significant problem in classical IDS.

With the rising complexity of current cyber threats, companies are increasingly relying on sophisticated, real-time monitoring and analysis capabilities to detect malicious activity, particularly that buried in encrypted network traffic. As previously noted, standard signature-based Intrusion Detection Systems (IDS) have limitations in detecting threats within encrypted data due to the inability to review packet payloads. Next-generation network security designs currently rely on tools like Zeek, Suricata, and the ELK stack, which includes Elasticsearch, Logstash, and Kibana. These solutions not only provide Real-Time Traffic Fingerprinting, but they also allow for a complete and scalable approach to intrusion detection and incident response in encrypted communication settings. As cyber threats continue to grow in complexity and stealth, particularly through the use of encryption, traditional Intrusion Detection Systems (IDS) are struggling to maintain relevance. Encrypted traffic, once a strength in the realm of cybersecurity, has ironically become a vector for hidden threats concealing malicious payloads and command-and-control (C2) communications behind layers of cryptographic protocols like TLS and SSL [1]. In response, the industry is undergoing a change in basic assumptions from payload-based detection to behaviour-centric models such as Real-Time Traffic Fingerprinting [2][3]. This approach, which focuses on analyzing network flow characteristics—packet size, frequency, timing, and direction has proven effective in exposing malicious patterns within encrypted streams without compromising privacy. By moving away from signature-based IDS towards intelligent, adaptive systems powered by AI and statistical modelling, we are beginning to overcome the limitations imposed by encryption [4][5]. Moreover, Real-Time Traffic Fingerprinting has become increasingly potent through its integration with innovative detection tools like Zeek and Suricata. Zeek offers deep visibility into network behaviours, producing rich metadata and logs that serve as input for high-fidelity fingerprinting [7]. Suricata, with its real-time threat detection and multi-threaded architecture, enhances this system by

identifying anomalous flows even in the absence of payload inspection [8].
However, analyzing this vast volume of real-time data would be infeasible without efficient data aggregation and visualization. This is where the ELK stack—Elasticsearch, Logstash, and Kibana becomes indispensable. Logstash collects and normalizes logs, Elasticsearch indexes and searches through terabytes of data in near real time, and Kibana visualizes it through intuitive dashboards [9][10]. These tools enable security analysts to trace, correlate, and respond to encrypted threats effectively, without resorting to decryption. Recent innovations have added further power to these systems. Flow interaction graphs [6], temporal correlation [16], and statistical intelligence [9] have shown remarkable success in modelling encrypted traffic behaviours, achieving high accuracy in anomaly detection. Techniques like adaptive proxying [11], time-series modelling [12], and adversarial learning [13] offer further resilience against sophisticated attacks. Even in constrained environments like IoT, lightweight models are being deployed to deliver proactive security [12].

2. Methodology

Data Collection :

- This phase is been involved with the usage of the three tools i.e., Wireshark Zeek and Suricata. These are some high performance tools which acts as an platform in capturing and monitoring the network security.
- Wireshark was used for the collection of the all the packets and also send it to through Zeek and Suricata for the observation of DNS query, TLS handshake behaviour validates and inspect the suspicious packet flow by capturing the packet data.
- Zeek was deployed for the observation of the network traffic and extract an high level behavioural logs like SSL/TLS handshake, DNS request and response, HTTP headers and the connection metadata. This also captures the metadata from the traffic without even decryption.
- Suricata was used alongside Zeek to have an deeper analysis of the packets and also the generate the alerts when there is an threat patterns recognised. This provided the logs on DNS id, HTTP traffic, TLS sessions and also allowed TCP flags behaviour for further analysis for the encrypted session.

Data Ingestion

- To manage the large volume of data which had been generated and ELK stack (Elasticsearch, Kibana, Logstash) tool was deployed where File beat acted as an log shipper who had collected all the logs from then Zeek and Suricata in real time and forwarded them to the Logstash.
- Logstash is generally used for parsing and filtering and transforming the raw network data logs into an structed format which will be appropriate for indexing in the Elasticsearch.
- Elasticsearch is an analytics engine which stores all the processed data and allowing an efficient querying, aggregation and correlation of multiple traffic attributes.
- For visualisation Kibana dashboard was developed where we can visualise all the network behaviours which was processed an stored in Elasticsearch in the form of pie charts, bar graphs, time series plots and heatmaps.

Data Visualization

- The visualisation had mainly focused on understanding the behaviour of the encrypted network traffic that is:
    1. DNS query and response patterns
    2. TLS/SSL handshake metadata
    3. Flow size distribution the data from client to server in the form of bytes
    4. Transport protocol usage such as TCP and UDP
    5. Source and Destination IP frequency patterns
    6. TCP flag behaviour profiling
    7. Event type occurrence and anomalies over the time.
- These visualisation helped in identifying the fingerprints of the malware even without decrypting the traffic and respecting the privacy while enhancing the security.

Feature Analysis

- These multi layered visualisation had allowed the identification of deviations from the network behaviours by knowing to analyse their clusters of rare JA3 fingerprints, sudden rise in the DNS TTL values and unusual surge in the UDP traffic which were flagged to analyse the potential indicators of encrypted threats like malware communication, covert channel's and unauthorised tunnelling.

3. Result and Discussion

I have examined the metadata generated from Suricata which included features such as DNS answer records, authoritative nameservers, resource owner name, DNS flags, response code, and high level alert categorizations. Even through a series of visualisation and aggregated information I have found out that the behavioural fingerprinting patterns is been linked with the dangerous or suspicious encrypted traffic. The payload inspection has been increasingly limited due to the widespread of the encryption where I have focused in the fingerprinting of the characteristics features such as DNS behaviour, TLS SNI(Server Name Indication) and the traffic anomaly patterns.
The important finding is discussed and presented below:

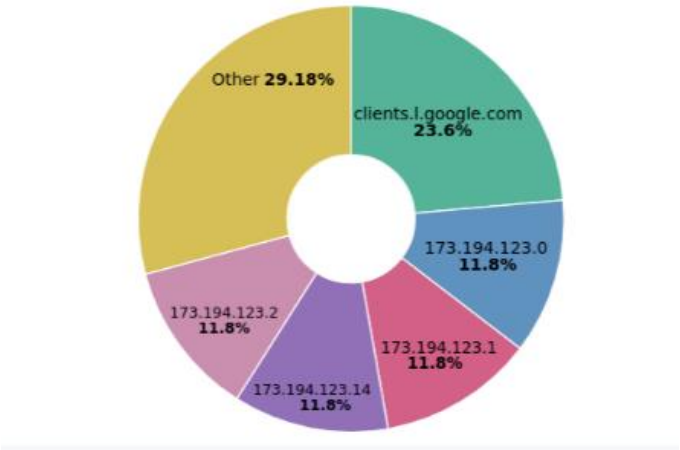

Figure 1: This field of data is DNS answer records (RDATA)

The data represents an initial step of detecting encrypted network threats (e.g. DNS information) and investigators may utilize the DNS information to determine anomalous domain access patterns, unauthorized and/or unverified infrastructure use, or potential beaconing. The data in these columns is essentially limited to notifications and security. This column lists the resolved IP addresses or fully qualified domain names returned from the DNS query. Suricata shows the top 5 DNS replies from that time period with the highest destination frequency. The assigns stress of the image shows three IP addresses that share the same traffic proportion (11.8% each) which may indicate a botnet command and control structure; DNS tunnelling exfiltrating information through the use of DNS queries; and fast flux DNS techniques used by malware to evade detection. Each IP address reflects automated perhaps nefarious traffic and not a human surfing pattern. It is fantastically odd to randomly have an equal proportion of three consecutive IP addresses from lawful traffic and presents as a clear fingerprint of potential nefarious behaviour.

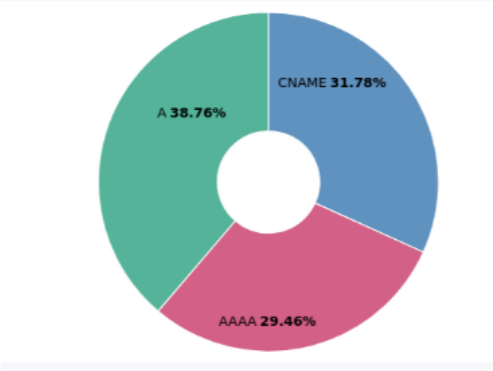

Figure 2: This image depicts the DNS record types (RRType)

The pie chart explains about the critical insights of how the domain names are being resolved and the hidden infrastructure which maybe be potentially dangerous and the IP address usage pattern. From the figure 7 A (IPv4) and AAAA (IPv6) are representing the IP address mapping from the domain names. It helps to identify the preference of the traffic which it is sophisticated to evade the monitoring. Even if the payload is not seen through the encrypted traffic environments, we can use the IPv4 and IPv6. The CNAME depicts the redirection and the hiding behaviour of the malware. In encrypted traffic there is an high chances of malware domains being cloaked behind benign looking CNAME and the dynamic redirection chains which are common in phishing kits and malware droppers. Monitoring the CNAME patterns helps to uncover the hidden malicious infrastructure even if the payloads are fully encrypted.

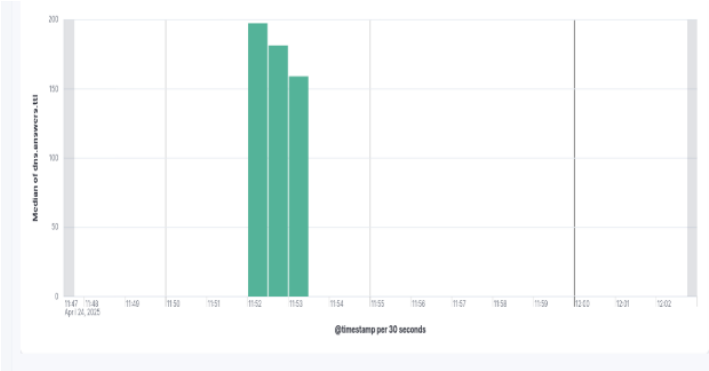

Figure 3: This image depicts the DNS TTL values

The TTL values are clustered between a short interval where after there is no continuous traffic. This shows that even the payloads are encrypted still

the DNS TTLs reveal the server behaviour. Based on seeing the TTLs consistently I can suggest that there was a potential fast flux infrastructure which raises a high suspicion if the TTLs are too low and change the frequently. Malware domain often has two different TTLs : Low TTLs (rotates quickly) and Short Lived records (evade the detection). Based on the figure we may also suggest that there might be a chance of short time burst behaviour where the TTL changes and high traffic volume which are concentrated over a short time which may indicate that there has been a malware exfiltration or tunnelling activity or the DGA bursts. This causes an active threat behaviour rather than passive browsing.

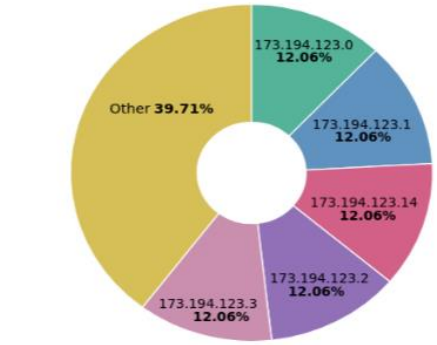

Figure 4: This image depicts the grouped DNS A records

The DNS grouped A visualization provides an IP level granularity which enables us to catch the malware which may be hiding in the legitimate platform or to identify the unusual patterns of the connections even inside the encrypted traffic. Based on the figure the top 5 IPs of 12.06% shown belong to Google IP block. When the normal user accesses the google service, they generate traffic to their addresses but if a repeated lookups to the same IP range could suggest that the malware has been using the legitimate services for C2 (Command and Control). The other 39.71% are of minor IP address which may suggest the beaconing to random or fast changing servers or the DNS tunnelling if there is an unusual or bursty IP hit. The malware often tends to hide into the random looking and fast rotating DNS response.

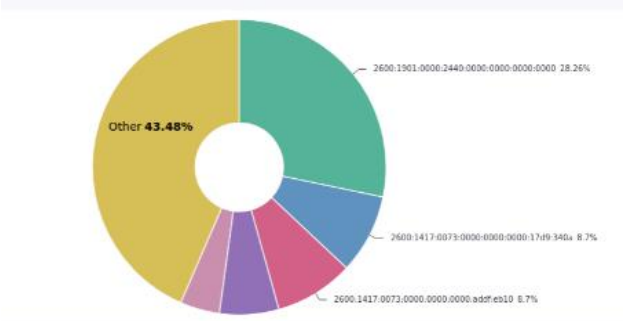

Figure 5: This image depicts the grouped DNS AAAA records

This AAAA record analysis reveals the heavy concentration to a IPv6 address or there may be a potential encrypted botnet or malware behaviour. The 28.26% of DNS resolutions point to the single IPv6 block whose behaviour maybe normal with the heavy use of Content Delivery Network or a cloud provider or it may be suspicious if all the quires are directed to a few fixed address or the IPs are rotating inside the IPv6 block. The attackers use larger address space to randomize the IPv6 which makes the traditional IP based blocklisting almost useless. The other 43.48% have a low frequency hits which has an high variation in the DNS resolved IPs and low TTL values which can signal to the malware DGA behaviour when the random domains of IPv6 address keeps resolving and the botnets using IPv6 tries to evade the defense system which is focused by IPv4.

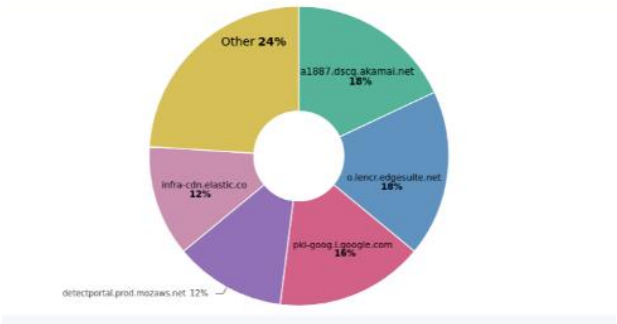

Figure 6: This image depicts the grouped DNS CNAME records

The CNAME is also known as the Canonical Name where the DNS answers the domain maps to the other domain. Based on the figure 11 major of the DNS CNAME traffic lies on the legitimate. It may be seen benign but the threats often abuse to use the trusted infrastructure for Command and Control and make the traffic blend into the normal user so that the malware payload can go undetected. The other 24% of the response in the CNAME points out the various less common aliases where the malware redirectors are often hidden in the long tail of the CNAME. They could be malicious servers rotating behind the CDN front address which makes them dangerous for the malicious infrastructure.

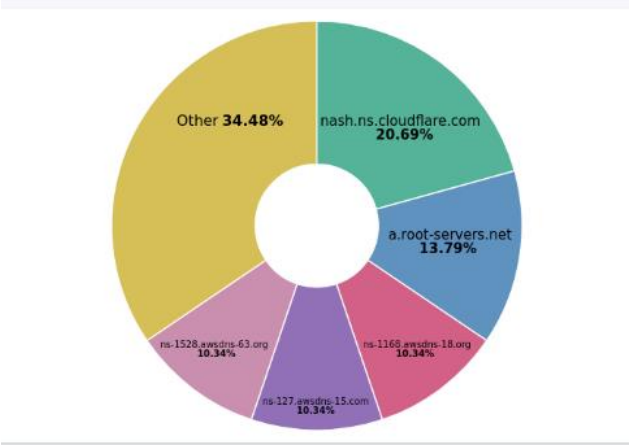

Figure 7: The image is DNS authorities (SOA MNAME field)

The results show that the captured infrastructure layer fingerprinting is an essential component in understanding the threats in encrypted infrastructures and balances documenting the leveraged DNS authorities, the anomalies in the DNS resolution behaviours, and the provided potential abused platforms. The meta data is a vital part of an intelligent intrusion detection, even where there is a lost attention to the payload. The dominant use of Cloudflare and AWS DNS is expected when validating legitimate and malicious uses of cheap cloud infrastructure. The spikes in Cloudflare or AWS are suspect where a misappropriation and or sudden spike may indicate malicious DNS fast flux domains or C2 (Command & Control) beaconing over cloud infrastructure. The queries for rooted servers are definitely suspect even as the fall back queries to rootserver.net at high volumes for non-existence domains and the DGA malware is leveraged with DNS resolution.

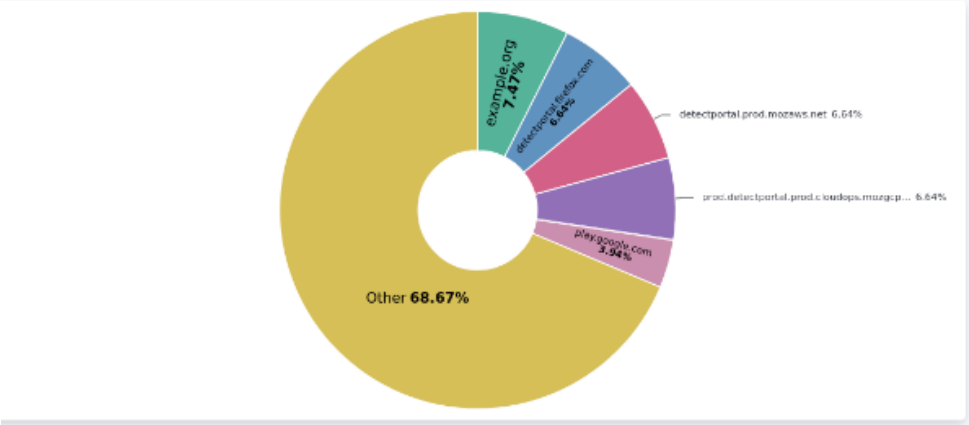

Figure 8: The image depicts the DNS resource record owner (RNAME)

The Resource Record Name (rname) displays a mail-like address for the DNS zone, which usually identifies who the administrator is or the SOA record, or other administrative meta data. The rname is often overlooked, as it adds contextual intel about the DNS patterns, and it also assists in correlating domains to owners or organisations or the TTP. Prediction of encrypted traffic detection is now a part of the behavioural and administrative fingerprinting model. The visualisation complements the DNS layer metadata fingerprinting, as it shows who is administratively responsible for the resolved domains and even when not visible, but the payloads have not been seen the metadata, like the rname, permits pattern detection, group of suspect domains and the threat actor profile and determination of origin via web host and administrators reputation and trust, which is a strong way to detect encrypted network threats, passively, via metadata fingerprinting.

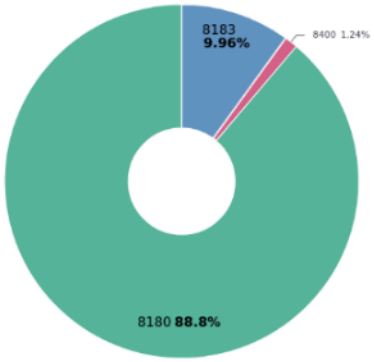

Figure 9: This image depicts the DNS flags

This field contains the hexadecimal representations of DNS packet flags, which describe how the DNS server/client handles or interprets a query. Each flag has a unique deception:

1. **Flag 8180 - Normal Traffic Baseline -** This indicates normal DNS resolution behaviour with recursion enabled and successful resolution. It also describes the typical behaviour fingerprint that will be used to train anomaly detection.

2. **Flag 8183 - NXDOMAIN Response:** Non-existent domains are a critical red flag in detecting encrypted threats. These sorts of responses are commonly found in DGAs (Domain Generation Algorithms), in which malware generates hundreds of domain names that are most likely non-existent, as well as C2 obfuscation, in which the attacker rapidly rotates domains to escape detection. The 9.96% result indicates that malware testing beaconing over DNS may be continuing.
3. **Flag 8400 - Malformed DNS packets** (1.24%) may indicate stealth or encryption masking strategies in DNS. This might suggest a scanning or testing protocol flaw, misconfigured bots, faked packets, or DNS tunnelling efforts with bespoke payloads.

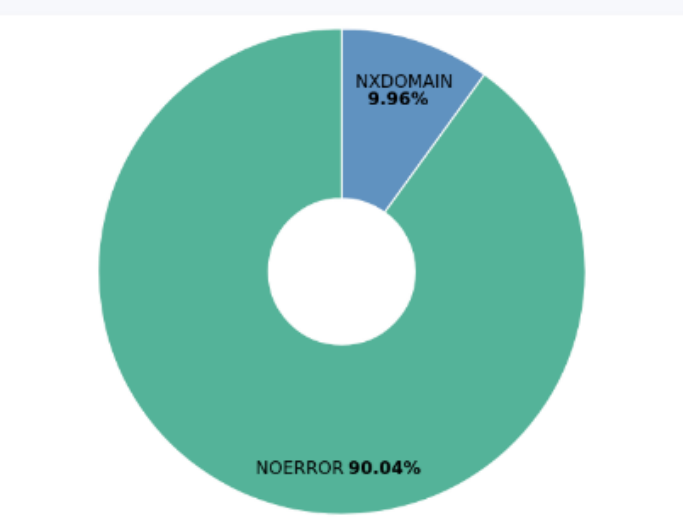

Figure 10: This image depicts the DNS response codes (RCode)

This field represents the DNS response code which has displayed the normal behaviour and potential anomaly. It is also one of the strongest single field indicators.

1. **NOERROR/Normal Behaviour :** These are the expected and benign DNS interactions which helps to define the baseline traffic pattern. 90.04% of the DNS traffic are normal interactions happening between the client and the server.

2. **NXDOMAIN :** The value 9.96% indicates the anomaly or the malware trying to reach the non-existent domains for DNS tunnelling attempts. The misconfigured or randomized domain generation algorithms are common in botnets where the attackers hide the payloads inside a data and tries to send, but their DNS behaviour remains visible.

As a high percentage of NXDOMAIN response suggest that there is an active DGA malware, DNS beaconing or the network scanning behaviour. This forms a metadata fingerprinting for detecting the threats that traditional payload inspection can't reveal.

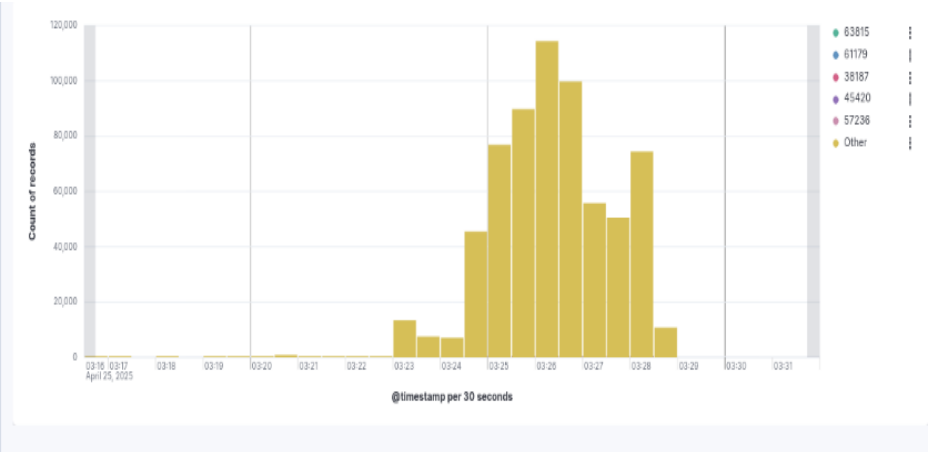

Figure 11: This image depicts the DNS transaction IDs

This bar chart here tells us about the behavioural fingerprinting based on the DNS timing and the transaction IDs. The malware which are using the encrypted DNS tunnelling, DGA or the covert channel communication are often short and intense bursts of DNS traffic which tries to evade the continuous monitoring. The burst which is observed in figure shows that the DNS communication is not uniform across the time, there was a spike

window of covert communication which maybe a data exfiltration or an beacon.
If the IDs are normally randomized it may be benign but the malware is using a custom and nonstandard DNS resolver which manually controls over the DNS tunnelling tools. Checking for the ID reuse, the odd sequences or the non-random patterns tries to strengthen the fingerprinting. The metadata timestamps and the DNS IDs greatly boosts to reveal the anomalies without decryption.

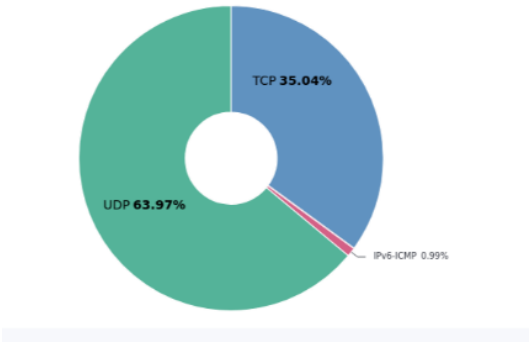

Figure 12: This image depicts the network protocol distribution

The figure shows the UDP heavy environments (63.97%) where it specially focuses on the encrypted DNS, QUIC and the tunnelling activin for threat detection. The encrypted threats frequently use the DNS over the HTTPS or the DNS tunnelling as UDP traffic shares a potential risk of exploitation.
The TCP shows it is still critical (35.04%) for the encrypted web attacks and are persistent to threats. The TCP is an traditional method for the HTTPS encryption in the browsing which also makes it an important for tracking the encryption sessions that hides the exfiltration or command operations.
The minimal ICMP traffic suggest that the captured traffic is mainly focused on the service rather than any attack which makes it an encrypted threat detection cleaner. Thus, the network protocol distribution analysis plays a vital role in the multi-layer fingerprinting.

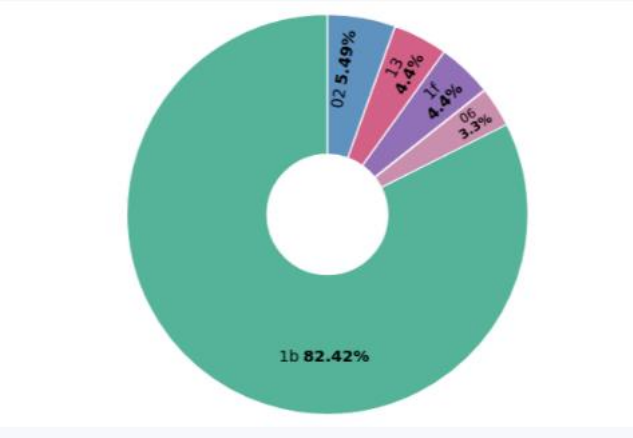

Figure 13: This image depicts the TCP flag distribution

The fingerprinting analysis shows how the TCP flags are more important and how the device communicated with each other at transport layer without any decryption of payload. The specific TCP flag 1b which is maximum (82.42%) shows the pattern are highly repetitive traffic which is an key fingerprint for detection which could indicate a normal session or a repetitive automated communication with the bot. The other flags are the smaller slices which represent the different types such as synchronous, acknowledgement, finish combination. The encrypted attacks often behave differently at their TCP handshake level. This also exhibited that the majority of the network threats are consistent flag patterns with minor deviations, enabling the detection of encrypted network threats without payload inspection.

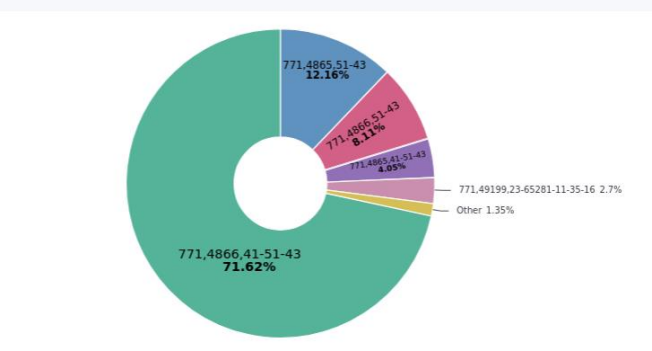

Figure 14: This image depicts the TLS JA3S fingerprints

The JA3/JA3S fingerprinting technique used to fingerprint SSL/TLS traffic without decrypting. It also captures the feature like extensions, cipher suites from the TLS handshake. Based on the figure one of the dominant JA3 fingerprint (71.62%) which indicated the majority of the encrypted traffic are coming from one type of server configuration and other smaller JA3S whose values are 12.16%, 8.1% show the different types of potentially anomalous encrypted communications. This JA3S fingerprinting revealed a dominant server configuration among the encrypted communication which aids the detection of anomalies in the encrypted session without decrypting it.

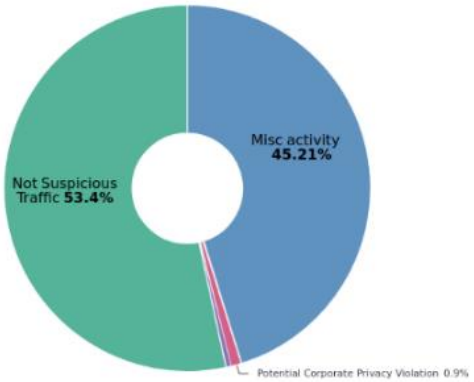

Figure 15: This image depicts the Suricata alert categories

The macro perspective aligns with the cross analysis of the flags, rcode, SNI, TTLs, and domain reputation without decrypting the traffic. The high level alert category had been broken down into different types such as non-suspicious traffic, Misc activity and Potential privacy violation, etc. The Misc activity logs which are 45.21% are under the category of DNS anomalies, unknown TLS values and the misuse in the protocol are caused by the payload which are sent with malicious content in the encrypted format. The remaining 0.9% of Potential Privacy violation may be highly sensitive has it may contain the unencrypted credential leaks or the DNS tunnelling attempts or malware attempting to enumerate the internal systems.

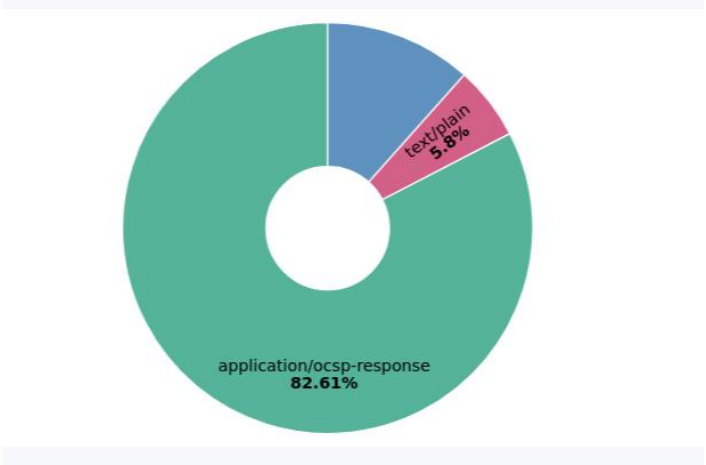

Figure 16: This image depicts the HTTP content types

The figure shows the monitoring the content types and allows the early warning of any encrypted threats which is attempting to hide inside the HTTP based tunnels. The high proportion is on application/ocsp-response layer which is about 82.61% which suggest that the traffic is of legitimate and gives a TLS handshake. The OCSP is used to verify the SSL/TLS certificate. When there is an threat sometimes the OCSP mixes with the malware checking fake tunnels which leads in the malware getting embedded to the C2 channels inside the HTTPS tunnels. The text/plain traffic is very little (5.8%) which is normal has the legitimate web browsing is rarely using the unencrypted in plain text and these may be used for the hidden command transfer. If an unexpected surges are seen in the plaintext, then there could be signal from OCSP for the hidden malicious payloads. The remaining part of the figure indicates that there is a very little diversity and the traffic is highly standardized and not random.

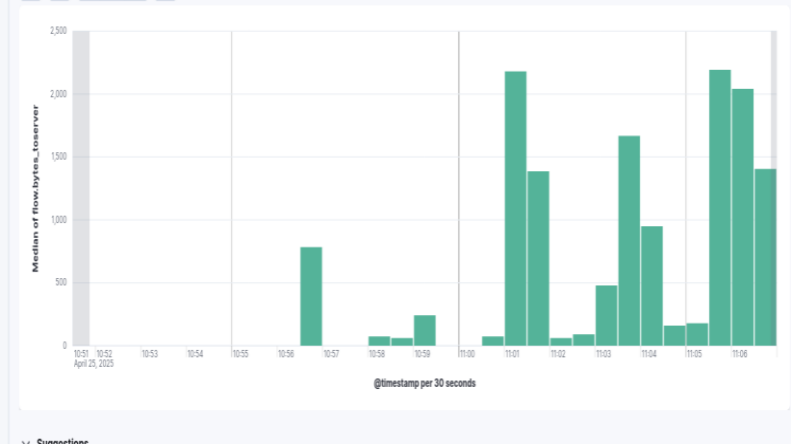

Figure 17: This image depicts the flow bytes sent to the server

The figure tells us about the measures that the number of bytes sent from the client to server. The sudden high flow in the sizes in the graph after a quiet period indicates there is an command exfiltration (sending the stolen data) or the beacon response or the payload delivery. The median flow are around 1500-2500 bytes which indicates there is a minimal handshake or the small data tunnelling in the TLS encrypted session and the DGA botnet quires bundled with an covert signalling. If there is an absence of the larger uploads then it indicates they is an low and slow exfiltration. These small constants flow sizes are of the encrypted malware communication. Based on the timing the byte size we can distinguish between the normal user and the malicious burst even without decrypting the traffic which can create a reliability. Thus, this plays a crucial role in a Morden Intrusion Detection System.

5. Conclusion

This research has conducted an through analysis of an Real Time traffic Fingerprint as an efficient approach to identify the encrypted network attacks in the Intrusion Detection System. Since the encrypted communication are being standardized as an normal means of data transmission through enabling the protocols such as TLS and SSL the current mechanism based on the deep packet inspection or the signature matching are severely affected. The conventual systems lack the capability to examine the concealed payloads of the encrypted packets and leave a blind spots increasingly exploited by the attackers to adopt sophisticated attacks such as command and control communications, DNS tunnelling, Data exfiltration and Malware propagation.

This project aimed to fill the gap by suggestion the fingerprint system based on the flow behaviour and the metadata, instead of payload content. Utilizing tools such as Zeek and Suricata, the system passively gathered massive amounts of metadata, including patterns in DNS searches, JA3 SSL/TLS fingerprints, TCP flagged behaviours, and byte counts of traffic flow available during encrypted connections. The acquired data was analyzed and shown in real time using the ELK stack, resulting in a dynamic dashboard that allows for real-time monitoring and alerting of behavioural abnormalities.

Their fingerprint scheme proved useful in detecting the patterns of an malicious encrypted traffic. IPv6 bursts of traffic, abnormality high volumes of low TTL DNS queries and the occurrence of repeated JA3 fingerprints not seen with the known legitimate clients were all marked as suspicious. Additionally, the system also identified indicator of the domain generation algorithms through the identification of the high rate of NXDOMAIN response along with the fast flux DNS activity, both regarded as an features in malware campaigns. Even without the content decryption the packet stream analysis based on timing size and direction presented an potential indicators of the malicious activities such as the covert channels or beaconing behaviours originating from the compromised hosts.

Another significant outcomes of the project are to priorities the privacy aware analysis techniques to which the utmost importance was given during the design. By only analysis the traffic patterns and metadata the system refrains from explicit content analyses hence staying within the bounds of privacy law and ethics. The design also proved to be scalable and non-intrusive making it deployable within both the enterprises and cloud scale environments without any major alteration of existing infrastructure. Lastly the integration of the statical intelligence and the machine leaning gave the system an added layer of sophistication enabling its ongoing adaptations and its ability to distinguish anomalous from the normal behaviours. This will be critical in fighting in zero day attacks and emerging attack vectors.

This study even marks an effective, privacy friendly, yet scabble means of Intrusion Detection improvements in the areas where encrypted communication is prevalent. It is an step toward the development of the cybersecurity infrastructure for the efficient threat detection without compromising the data confidentiality providing an glimpse into the future of next generation IDS system.

REFERENCES

1. Hongsheng Xui, Libo Sun, et. al., “A Hierarchical Intrusion Detection Model Combining Multiple Deep Learning Models With Attention Mechanism”, IEEE Access, 2017, Volume XX.

2. Sunghyun Yu, Yoojae Won, “A survey of methods for encrypted network traffic fingerprinting”, Mathematical Biosciences and Engineering, Volume 20, Issue 2, 2183–2022.

3. Faeiz Alserhani, “Analysis of Encrypted Network Traffic for Enhancing Cyber-security in Dynamic Environments”, Applied Artificial Intelligence, 2024, Volume 38, No. 1.

4. Sebastien Canard, Chaoyun Li, “Towards practical intrusion detection system over encrypted traffic”, IET Information Security, 2021, Volume 15, Pages 231–246.

5. Tanya Sood, Satyartha Prakash, Sandeep Sharma, "Intrusion Detection System in Wireless Sensor Network Using Conditional Generative Adversarial Network", Springer, 2022.
6. Chuanpu Fu, Qi Li, Ke Xu, "Detecting Unknown Encrypted Malicious Traffic in Real Time via Flow Interaction Graph Analysis", Network and Distributed System Security, 2023.
7. Eva Papadogiannaki, Sotiris Ioannidis, "Acceleration of Intrusion Detection in Encrypted Network Traffic Using Heterogeneous Hardware", Sensors, 2021, 1140.
8. Il Hwan Ji, Ju Hyeon Lee, Seungho Jeon, Jung Taek Seo, "Encrypted Cyberattack Detection System over Encrypted IoT Traffic Based on Statistical Intelligence", Computer Modelling in Engineering & Sciences, 2024, Volume 141, No. 2, Pages 1519-1547.
9. Md Sobuj Ali, Fauzia Yasmin, Saida Sultana, "Machine Learning-Based Intrusion Detection System for Encrypted Attacks," European Journal of Applied Science, Engineering and Technology, Vol. 2(2), pp. 298-309, Mar-Apr 2024.
10. Abdou Romaric Tapsoba, Mohamed Bobo Diallo, Tounwendyam Frederic Ouedraogo, Wend-Benedo Simeon Zongo, "Toward Real Time DGA Domains Detection in Encrypted Traffic", NISS 2024.
11. Aswathy M C, Rajkumar T, "Real Time Anomaly Detection in Network Traffic: A Comparative Analysis of Machine Learning Algorithms", International Research Journal on Advanced Engineering Hub, Vol. 02, 2024 Page No: 1968- 1977, ISSN: 2584-2137.
12. Prabu Jayant, Prathica Shetty M, et. al., "Intrusion Detection in Network Traffic Using LSTM and Deep Learning", International Conference on Computing Communication and Networking Technologies, 2024.
13. Khaled Al-Naami, Swarup Chandra, et. at., "Adaptive Encrypted Traffic Fingerprinting With Bi-Directional Dependence", ACSAC, 2016, ISBN 978-1-4503-4771-6.
14. Ferriyan, A, Thamrin A.H, et. al., "Generating Network Intrusion Detection Dataset Based on Real and Encrypted Synthetic Attack Traffic", Applied Science, 2021, 11, 7868.
15. Pradeep Semwal, Harish Chandra Sharma, "An Efficient Intrusion Detection Technique For Imbalanced Network Traffic Using Deep Learning", Journal for Re Attach Therapy and Developmental Diversities, 2023, 6(10s), 1802-1809, ISSN: 2589-7799.
16. Estabraq Saleem Abduljabbar Alars, Sefer Kurnaz, "Enhancing network intrusion detection systems with combined network and host traffic features using deep learning: deep learning and IoT perspective", Discover Computing, 2024, 27:39.
17. Mahmoud Abdel Hafeez Sayed, Mostafa Taha, "Oblivious network intrusion detection systems", IEEE International Symposium on Hardware Oriented Security and Trust, 2023, 13:22308.
18. Geo Francis E, S. Sheeja, "Intrusion detection system and mitigation of threats in IoT networks using AI techniques: A review", Engineering and Applied Science Research, 2023, 50(6), pp. 633-645.
19. Meng Shen, Yiting Liu, et. al., "Fine-Grained Webpage Fingerprinting Using Only Packet Length Information of Encrypted Traffic" IEEE Transactions on Information Forensics and Security, 2020, PP(99):1-1.
20. Nasreen Fathima. A. H, Syed Ibrahim S. P, Ansam Khraisat, "Enhancing Network Traffic Anomaly Detection: Leveraging Temporal Correlation Index in a Hybrid Framework", IEEE Access, 2016, Volume 4.
21. Jihane Ben Slimane, Eman H. Abd-Elkawy, Albia Maqbool, "Intrusion Detection using Network Traffic Profiling and Machine Learning for IoT", Journal Electrical Systems, 2024, 20-3s, ISSN: 2140-2149.
22. Dr.S. Pavithra, Venkata Vikas K, "Detecting Unbalanced Network Traffic Intrusions with Deep Learning", IEEE Access, 2017, Volume XX.
23. Sandra Siby, Marc Juarez, Claudia Diaz, "Encrypted DNS → Privacy? A Traffic Analysis Perspective", Network and Distributed Systems Security, 2020.
24. Anita Bai, R. Delshi Howsalya Devi, R. Madana Mohana, "High Performance Network Intrusion Detection System", International Journal of Engineering and Advanced Technology, 2019, Volume-9 Issue-2, ISSN: 2249 – 8958.
25. Ibrahim A. Alwhbi, Cliff C. Zou, Reem N. Alharbi, "Encrypted Network Traffic Analysis and Classification Utilizing Machine Learning", Sensors, 2024, 3509.
26. Martin Husak, Milan Cermak, Tomas Jirsik, Pavel Celeda, "HTTPS traffic analysis and client identification using passive SSL/TLS fingerprinting", EURASIP Journal on Information Security, 2016.
27. Ali Hadi, "Using Zeek for Network Investigations", Northeast Collegiate Cyber Defense Competition (NECCDC), 2019.
28. Bhaggiarah S, Shanthini S, Sugantha Mallika S.S, Muthuram R, "Next Generation Intrusion Detection And Prevention Systems for IT and Network Security", ICTACT Journal on Communication Technology, 2023, 14(3):2992-2997.
29. Wai-Tak Wong, "Advanced Elasticsearch 7.0: A practical guide to designing, indexing, and querying advanced distributed search engines", Packt, 2019, ISBN: 978-1789957754.
30. Dim Shayakhmetov, Cholpon Abdisukhanova, "Building a Scalable Logging System on Kubernetes with Elasticsearch", 2025.
31. Radu Gheorghe, Matthew Lee Hinman, Roy Russo, "Elasticsearch in Action". Manning Publication, 2016.