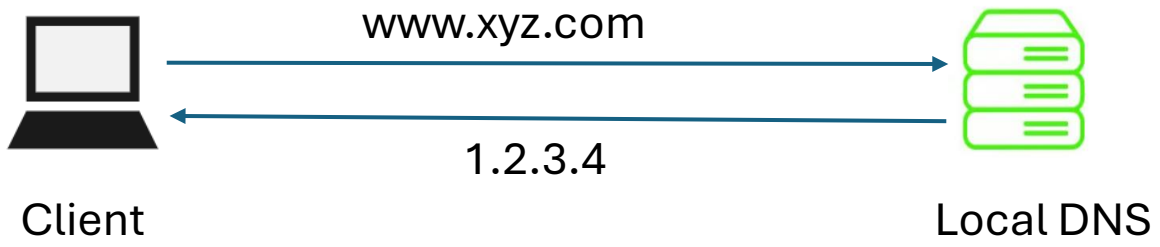
DNS Tunnel Attack
Detection and Measures

A S M Nazimuddoullah

Fahim Uddin

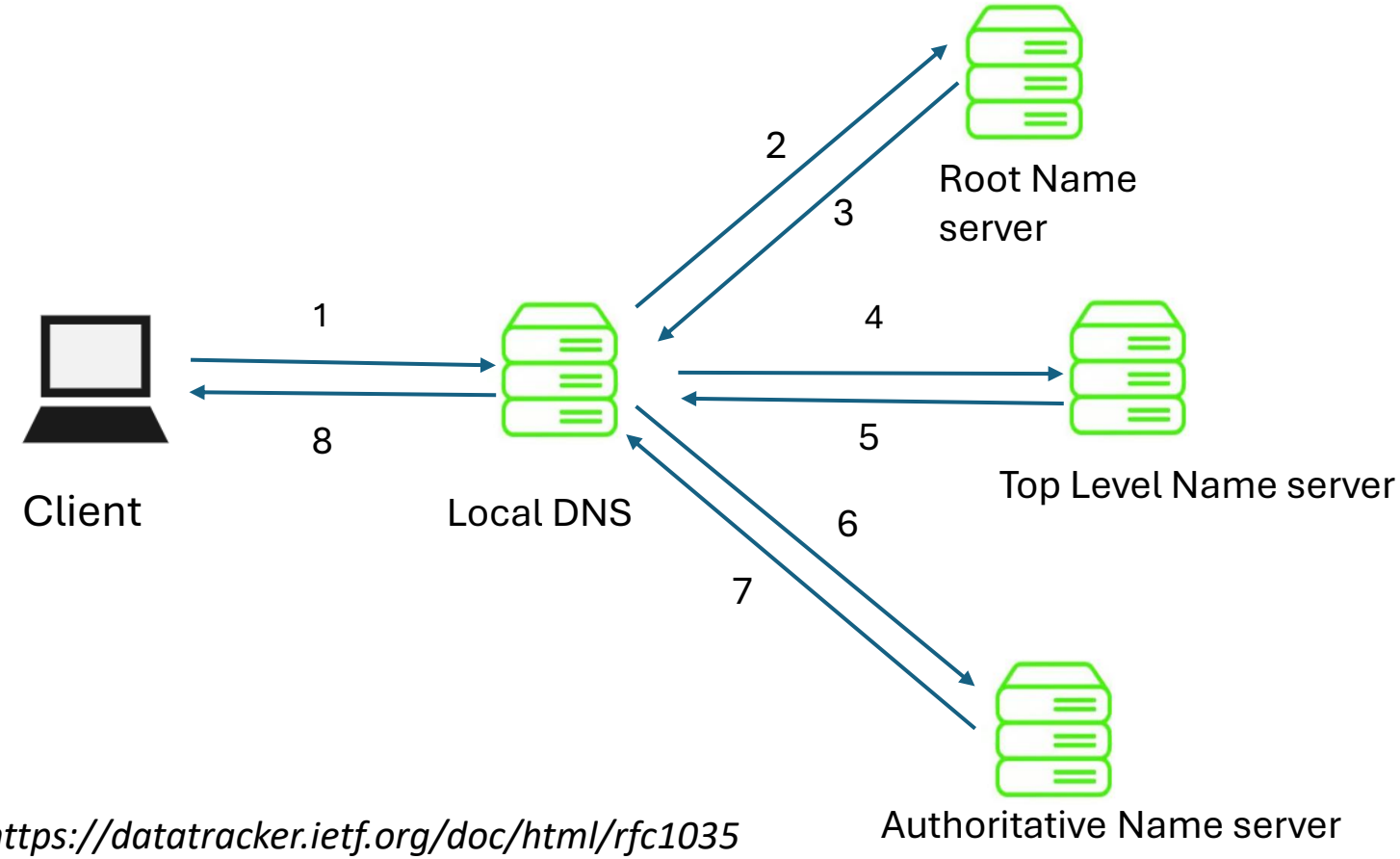
DNS

- Domain Name System (DNS) translates human readable hostname with IP address
- Described in RFC1034 and RFC1035



DNS

- Local DNS server will do iterative query(step 2-7) if answer not available



https://datatracker.ietf.org/doc/html/rfc1035

Popular DNS Record Types

Record Type	Type ID	Function
A	1	Translates 32-bit IPv4 address
AAAA	28	Translates 128-bit IPv6 address
CNAME	5	Alias of one name to another
NS	2	Name record server
MX	15	List of mail exchange servers
NAPRT	35	Naming authority pointer
PTR	12	Pointer to a CNAME
SOA	6	Start of zone authority record
TXT	16	Human readable text in DNS record

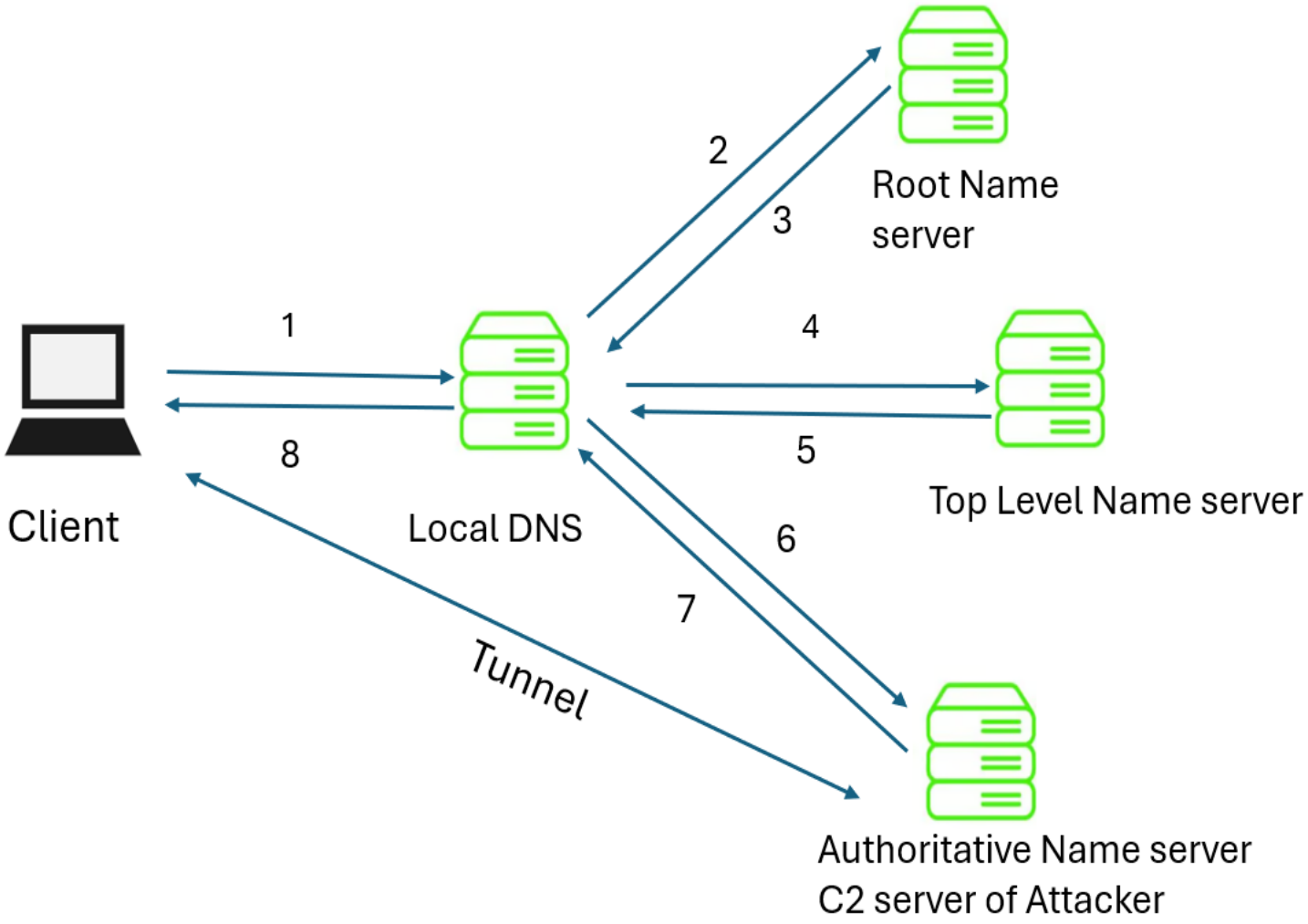
https://en.wikipedia.org/wiki/List_of_DNS_record_types

DNS Tunneling

- Creating a tunnel in client-server model using DNS protocol
- Mostly used for malpractice
- Encapsulates the data in the DNS query and DNS response packet
- Create a tunnel between sender and receiver through DNS protocol
- Use DNS requests to implement a command and control (C2) channel for malware

https://www.sciencedirect.com/science/article/pii/S1389128621003248

How DNS Tunnel works



https://www.sciencedirect.com/science/article/pii/S1389128621003248

How DNS Tunnel works (Cont.)

- Attacker registers a domain (example: maldomain.com)
- Domain's name server points to the attacker's server installed with a tunneling malware program
- Attacker infects targeted computer with malware
- Infected computer can send a query to the local DNS server just like regular DNS query
- Local DNS relays requests for IP addresses to root and top-level domain servers (recall iterative DNS)
- The C2 server reply several command control instructions as response back to the local name server inside DNS answer

https://www.paloaltonetworks.com/cyberpedia/what-is-dns-tunneling

How DNS Tunnel works (Cont.)

- Local DNS send the computer(victim) with the attacker's C2 (command-and-control) message, where the tunneling program is installed
- A connection (tunnel) is now established between the victim and the attacker
- Inbound DNS traffic can carry commands to the malware, while outbound traffic can exfiltrate sensitive data
- The subdomain name in DNS packets can be used to encapsulate upstream data

https://www.paloaltonetworks.com/cyberpedia/what-is-dns-tunneling

Purpose of DNS Tunnel

- DNS protocol is widely used and trusted
- Usually, organizations allow DNS traffic to pass through the firewall
- Legitimate purposes to bypass the firewall in restricted environment.
- Availability of DNS tunneling toolkits for malicious actor
- Mostly used by attackers to exfiltrate data or establish hidden communication channels

https://www.akamai.com/glossary/what-is-dns-tunneling

Motivations for DNS tunneling attack

DNS tunneling is a secret method used by attackers to hide malicious activity within apparently normal DNS traffic like the following:

Command and control (C2) communication: Malware can bypass firewalls and other security measures to establish C2 communication with remote servers.

Data Exfiltration: Sensitive information can be leaked using DNS queries.

Botnet control: Attackers can create networks of affected devices (botnets) using DNS tunneling to open attacks or perform other malicious activities.

Avoiding censorship: DNS tunneling can be used to bypass internet restrictions and access harmful blocked content.

https://blogs.blackberry.com/en/2023/03/dns-tunneling-guide-to-detection-and-prevention

Actors for DNS tunneling attack

Cybercriminals: For executing attacks like ransomware, data theft, fraud, etc.

State-sponsored attackers: DNS tunneling for intelligence or warfare.

Hacktivists: Motivated by political or ideological causes.

DNS tunneling creates a considerable threat due to its secret nature.

https://www.scworld.com/brief/threat-actors-expanding-malicious-use-of-dns-tunneling

DNS Tunnel Tools

- IP over a DNS tunnel: encapsulates IP packets in the DNS tunnel
- Example: NSTX, Dnscat2, Iodine, and TUNs

- TCP over a DNS tunnel: encapsulates TCP packets in the DNS tunnel
- Example: Dns2tcp, OzymanDns, Heyoka

https://www.sciencedirect.com/science/article/pii/S1389128621003248

Features of DNS Tunnel

Payload analysis to analyze the content of DNS packet (Real-time)

- Size of packet (uplink usually bigger in exfiltration)
- Upload-download ratio (upload is extensive)
- Length of domain name and number of subdomains
  (Checking if each label in a domain is larger than 63 bytes which will also increase subdomain numbers)
- Special characters or meaningful words in the domain name
- Unusual subdomain names
- Uncommon record type
- Searching for specific DNS tunnel tool's signature and policy violation in directly connected DNS tunnel

https://www.sciencedirect.com/science/article/pii/S1389128621003248

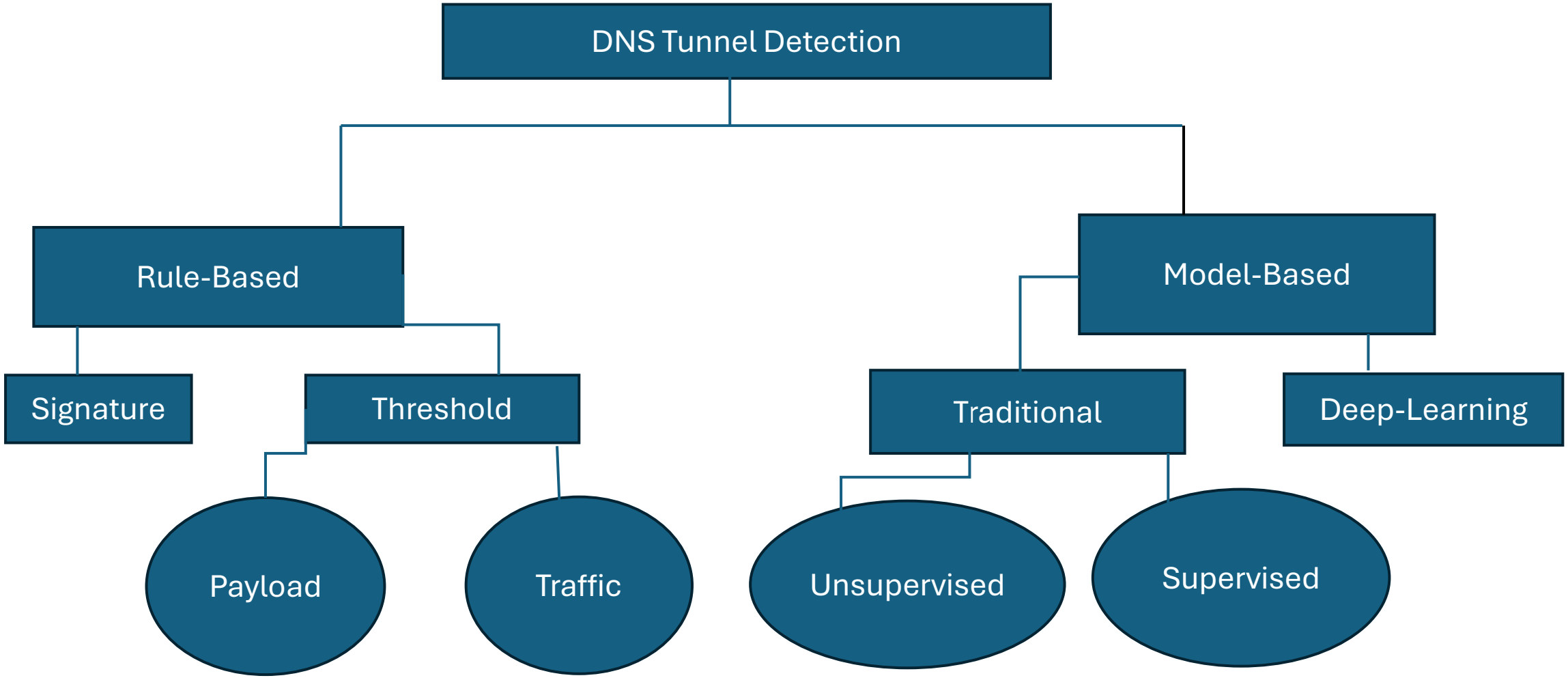
Features of DNS Tunnel (Cont.)

Flow analysis to analyze the overall DNS traffic (Not real-time)

- Volume of DNS traffic (Average traffic be unusual and larger than 512 bytes for some IP addresses each also unusual DNS traffic to a particular domain)
- Volume of hostnames to the domain name
- Longer time interval due to disguised server
- Geographic location of DNS server
- Isolated DNS queries (No other consequent traffic)
- Volume of response type (other than successful)
- DNS traffic visualization

https://www.sciencedirect.com/science/article/pii/S1389128621003248

Detection Mechanism of DNS Tunnel [1]



https://www.sciencedirect.com/science/article/pii/S1389128621003248

Detection Mechanism of DNS Tunnel

Rule-Based detection (Setting manual preset rules to target specific features). Can be achieved by:

- IDS or IPS solution
- Big data search components (Splunk)
- Firewalls (PaloAlto)

https://www.sciencedirect.com/science/article/pii/S1389128621003248

Detection Mechanism of DNS Tunnel (Cont.)

A. Signature-Based methods (Rule-Based)
   - By deep packet inspection of DNS header and payload to find specific signature
   - Not fruitful for new pattern/signature and high resource consumption

B. Threshold-Based methods (Rule-Based)
   - Payload-based threshold quantitively analysis of several packets to find for domain related features like length, character frequency etc. Although difficult to implement but performance is good.

   - Traffic-based threshold analysis focus on entire traffic-related features thus it can detect both known and unknown based on abnormal behaviors of DNS tunneling tools.

https://www.sciencedirect.com/science/article/pii/S1389128621003248

Detection Mechanism of DNS Tunnel (Cont.)

Model-Based detection (Built on the training of machine learning model)

- Use different machine learning algorithms for both traditional and deep learning.

A. Traditional Machine Learning-Based methods (Model-Based)

a) Unsupervised Learning [1]: In DNS tunnel detection, the most popular K-means algorithm has a low true-positive rate; however, for data leak activity, the logistic regression algorithm with statistical feature subdomains is used, which has higher high-level accuracy.

The k-means model performed poorly when random starting points were used, suggesting that it might not be helpful for identifying odd samples. The small and somewhat unbalanced dataset generated by just four clients may be the reason for this, as it may lack sufficient details to accurately identify malicious DNS traffic.

https://www.sciencedirect.com/science/article/pii/S1389128621003248

Detection Mechanism of DNS Tunnel (Cont.)

b) Supervised Learning[1]: The most popular algorithm is the support vector machine (SVM) for DNS tunnel detection. The SVM algorithm is better than Bayes, logistic regression, decision trees, and other algorithms in performance.

   Additionally, the linear SVM is not as effective as the SVM based on kernel functions. While k-means is commonly utilized in unsupervised learning, it is less effective than unsupervised SVM in a mobile network setting.

https://www.sciencedirect.com/science/article/pii/S1389128621003248

Detection Mechanism of DNS Tunnel (Cont.)

Model-Based detection by Deep Learning-Based Detection methods (Less used though)

- Mostly supervised learning
- The convolutional neural network (CNN) is the most popular deep learning algorithm for DNS tunnel detection.
- It can use sequential and structural information to extract features automatically to analyze the whole data to find any anomaly in DNS.
- It is not commonly used as it needs costly hardware and large data sets to train the model.

https://www.sciencedirect.com/science/article/pii/S1389128621003248

Additive measure for DNS Tunnel Detection

More steps can be taken to consider the following two aspects in addition to DNS tunnel detection

A. Importance of detecting heartbeat traffic in DNS tunnels
   - Properly detecting the heartbeat traffic in DNS tunnels can save the system before any malicious activities take place.
   - It also improves the performance of DNS tunnel detection by early determining the inactive DNS tunnel.

B. All protocols that use encapsulation in DNS tunnels
   - If protocols such as FTP, HTTP, SMTP, SSH, etc., are encapsulated in the DNS tunnel, it will make detection more difficult.
   - Further research is needed to address the challenges of detecting DNS tunnels that use encapsulation.

https://www.sciencedirect.com/science/article/pii/S1389128621003248

Challenges of DNS Tunnel Detection

DNS over TLS (DoT) and DNS over HTTPS (DoH) are making DNS tunnel detection more difficult:

- These new protocols use TLS or HTTPS encryption to protect DNS traffic during transmission.
- This creates double encryption, which results in double tunneling and creates challenges for DNS tunnel detection.
- Further research ongoing to address the challenges related with such scenario.

https://www.sciencedirect.com/science/article/pii/S1389128621003248

Future Proof of DNS Tunnel

- Regularly Monitor DNS Traffic: Search for unusual patterns, such as high volumes of queries, large text strings, or queries to unusual domains.

- Robust Firewall Rules and Traffic Analysis: Implement strong firewall rules and conduct thorough traffic analysis. HAR file analysis can also be a great approach

https://www.sciencedirect.com/science/article/pii/S1389128621003248

Future Proof of DNS Tunnel

- Limit Unnecessary DNS Queries: Specially record types TXT, NULL, SRV, etc.
- Blocking domain names, IP addresses, or geolocation based on their known reputation or vulnerability.
- Properly configuring DNS security extensions (DNSSEC) during the authentication of DNS data.

https://www.sciencedirect.com/science/article/pii/S1389128621003248

References

1. A comprehensive survey on DNS tunnel detection https://www.sciencedirect.com/science/article/pii/S1389128621003248
2. Malicious DNS Tunneling Detection in Real-Traffic DNS Data https://ieeexplore.ieee.org/abstract/document/9378418/authors#authors
3. https://www.paloaltonetworks.com/cyberpedia/what-is-dns-tunneling
4. https://datatracker.ietf.org/doc/html/rfc1034
5. https://datatracker.ietf.org/doc/html/rfc1035
6. https://www.checkpoint.com/cyber-hub/network-security/what-is-dns-tunneling/
7. https://www.akamai.com/glossary/what-is-dns-tunneling
8. https://en.wikipedia.org/wiki/List_of_DNS_record_types
9. https://unit42.paloaltonetworks.com/dns-tunneling-how-dns-can-be-abused-by-malicious-actors/
10. https://blogs.blackberry.com/en/2023/03/dns-tunneling-guide-to-detection-and-prevention
11. https://www.scworld.com/brief/threat-actors-expanding-malicious-use-of-dns-tunneling