Detection, Analysis and Measurement of DNS Tunneling Techniques

Master's Thesis Research

Speaker: Damianos Christos Nikou

SIDN Supervisor: Moritz Müller

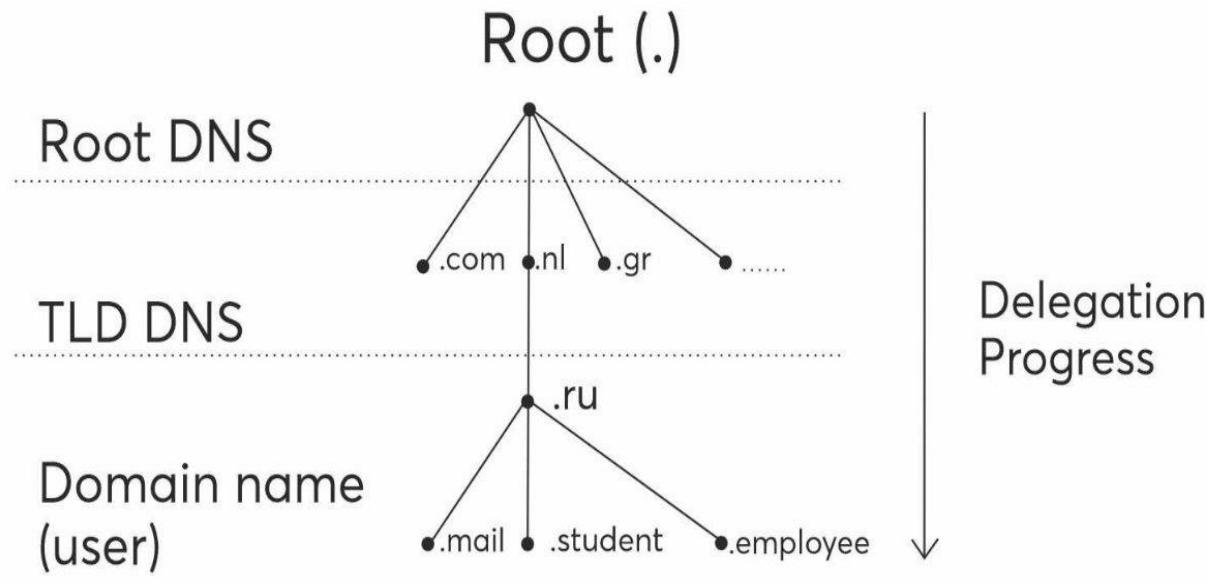
Research Purpose

Target:

- .nl ccTLD
- Detection of DNS tunneling techniques
- Analysis of DNS tunneling queries
- Validation of DNS tunneling queries
- Measurement of DNS tunneling queries

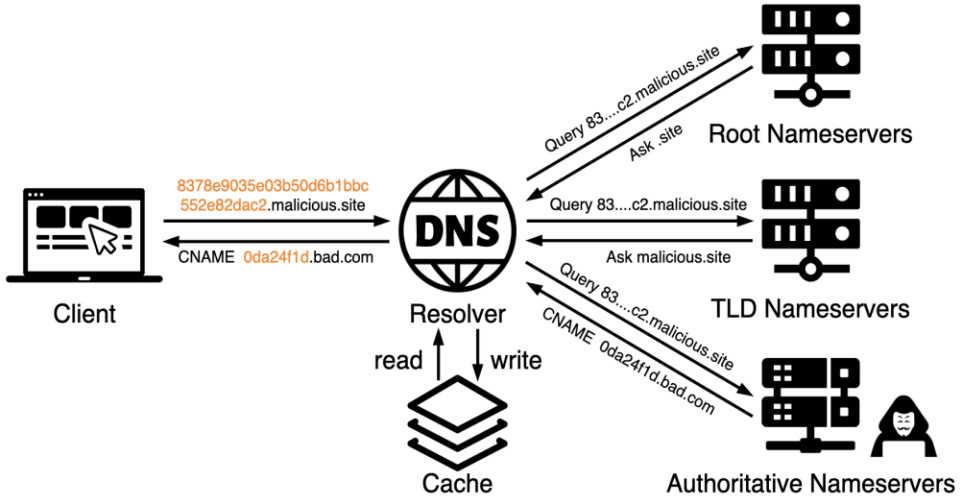
Implementation:

- SIDN's authoritative name servers
- ENTRADA Tool



DNS Tunneling

- Embedded data into DNS queries and responses
- Covert communication between server and client
- Bypass network protection
- Hidden into legitimate DNS traffic
- Modified authoritative name servers to process exfiltrated data
- Transmit data in restricted environments



DNS Tunneling Tools

Client Side

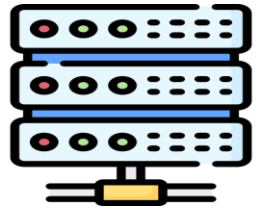
- Installed on user machine
- Acts as stub resolver
- Search the server on DNS hierarchy

Server Side

- Resides on C2 server
- Masquerades as authoritative name server

DNS Tunnels Types:

- Over UDP
- Over TCP



Detection of DNS Tunneling

Payload Analysis

- Size of Request
- Entropy of Subdomains
- Uncommon Records Types

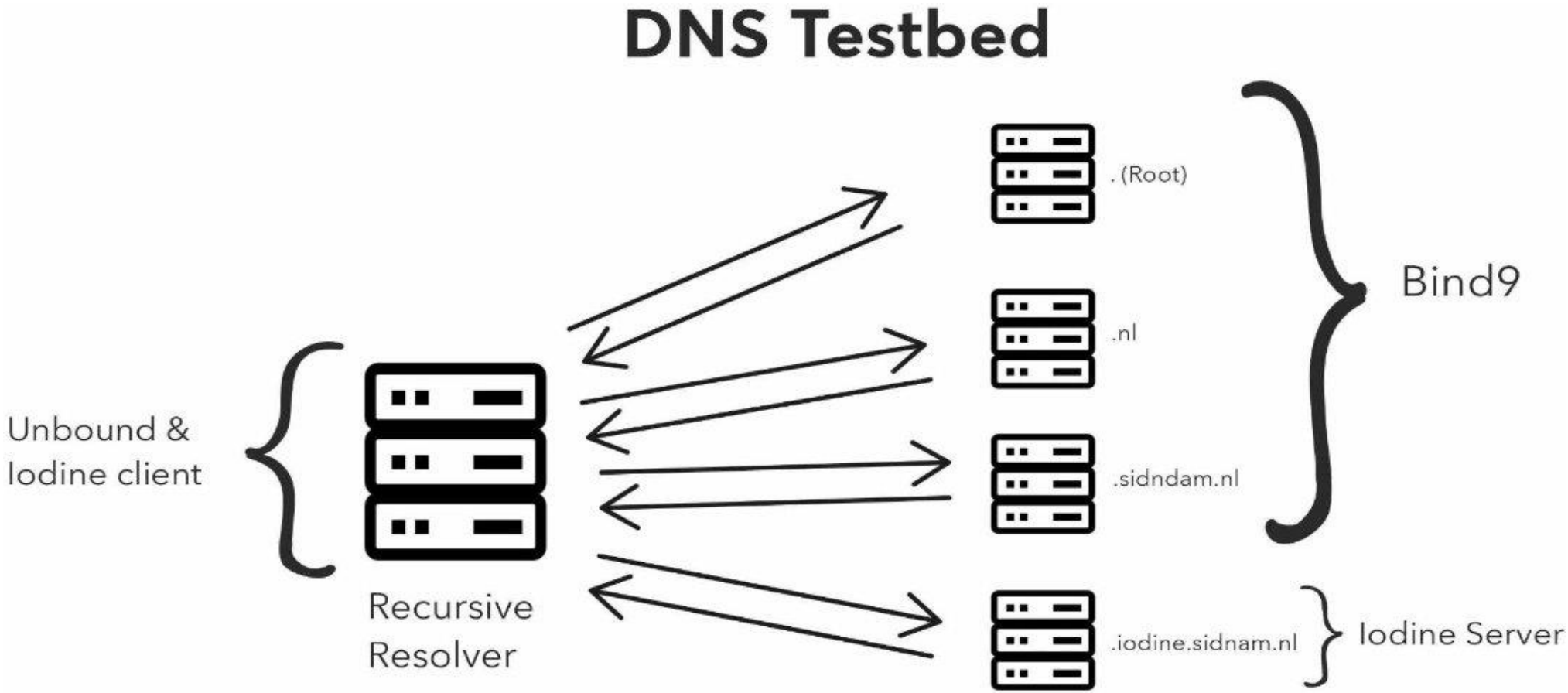
Traffic Analysis

- Volume of DNS Traffic per IP Address
- Number of Hostnames per Domain
- Volume of NXDOMAIN Responses

Implementation Environments

- DNS Testbed
- ENTRADA Tool

DNS Testbed Environment



ENTRADA Tool Environment

Capabilities

- Open-Source Tool
- Daily DNS traffic of .nl
- Data more than a year
- DNS queries in human-readable format
- DNS queries captured as PCAP files
- Select specific datasets of .nl traffic

Data Processing

- Custom rules on SQL Queries on DNS queries
- Drop queries that are unlikely caused by DNS tunneling
- Select potential DNS tunneling queries
- Application of detection rules on DNS queries
- Scripts for analysis of DNS packets

ENTRADA: https://entrada.sidnlabs.nl/

Custom Detection Rules

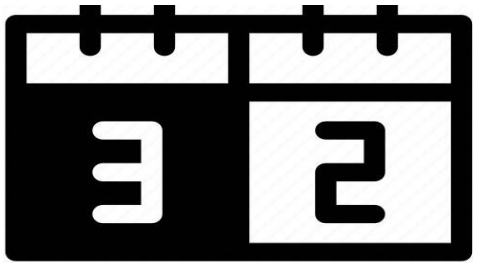
- **Rule 1**: Entropy > 3.8 of query names per label
- **Rule 2**: "Base32", "Base64", "Hex", and "NetBIOS" encoding per label
- **Rule 3**: Uncommon RR such as "TXT", "NULL", and "PRIVATE"
- **Rule 4**: Continuous sequences of characters and numbers
- **Rule 5**: Characters "z" or "y" in first letter and leftmost label of query
- **Rule 6**: Error types such as NXDOMAIN responses

qname	QUERY TYPE
y6tbwbiffzn52xyefrhcgv6ns.xi7cxcqtkfwpd6pm4cxq.*.*.nl.	TXT
aqyrybnsuih67lxpjqjcmgpxndypwira.ipg5namibkuyv7fbmscq.*.*.nl.	TXT

These Rules based on observations of DNS testbed and literature analysis.

Validation of DNS Tunneling

- Develop a scoring system based on detection rules.
- Weights of score based on literature and DNS testbed.
- Score on DNS queries assign the likelihood of DNS tunneling.



Real User Validation

- Genuine user utilizes Iodine DNS tunneling tool.
- Custom detection rules for DNS tunneling queries.
- Detection of DNS tunneling query.
- User verification of IP and validation of findings.

Validation of DNS Tunneling

qname	ERROR	ERRORTYPE	Total Score	Query Type
yrbbb0.*.*.nl.	True	NXDOMAIN	5	NULL

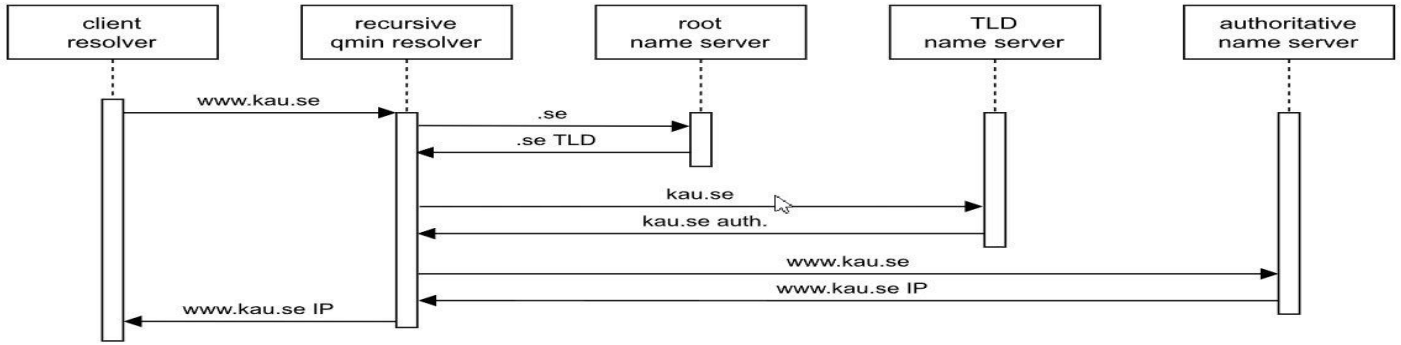
Score Distribution:

- NULL RR: 1 point
- Leftmost label "y": 1 point
- Continuous patterns: 2 points
- NXDOMAIN error: 1 point

Limitations

QNAME Minimization

- Enabled on DNS resolvers for privacy and security
- Minimizes amount of information leaked



https://www.sidnlabs.nl/en/news-and-blogs/taking-another-look-at-query-name-minimization-in-the-dns

Only DNS queries

- Investigation based only DNS quries
- Unique DNS data to operation of .nl ccTLD
- Hard to validate our results

Measurements on .nl traffic

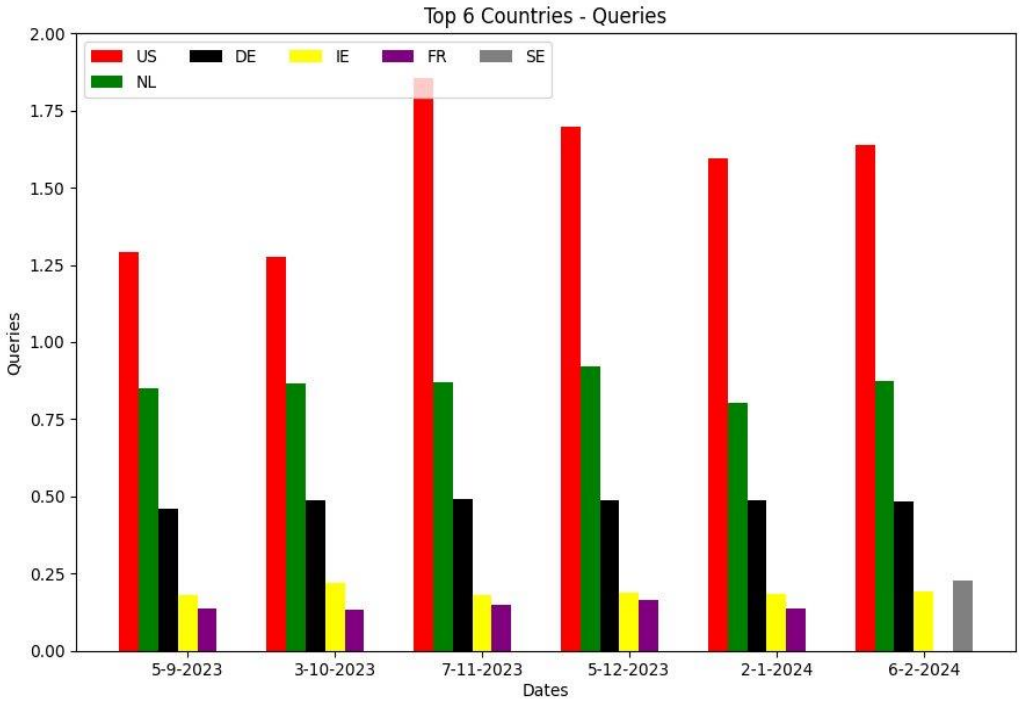
DNS Tunneling Measurements

- Over several months
- Over a specific date
- Over a single domain name

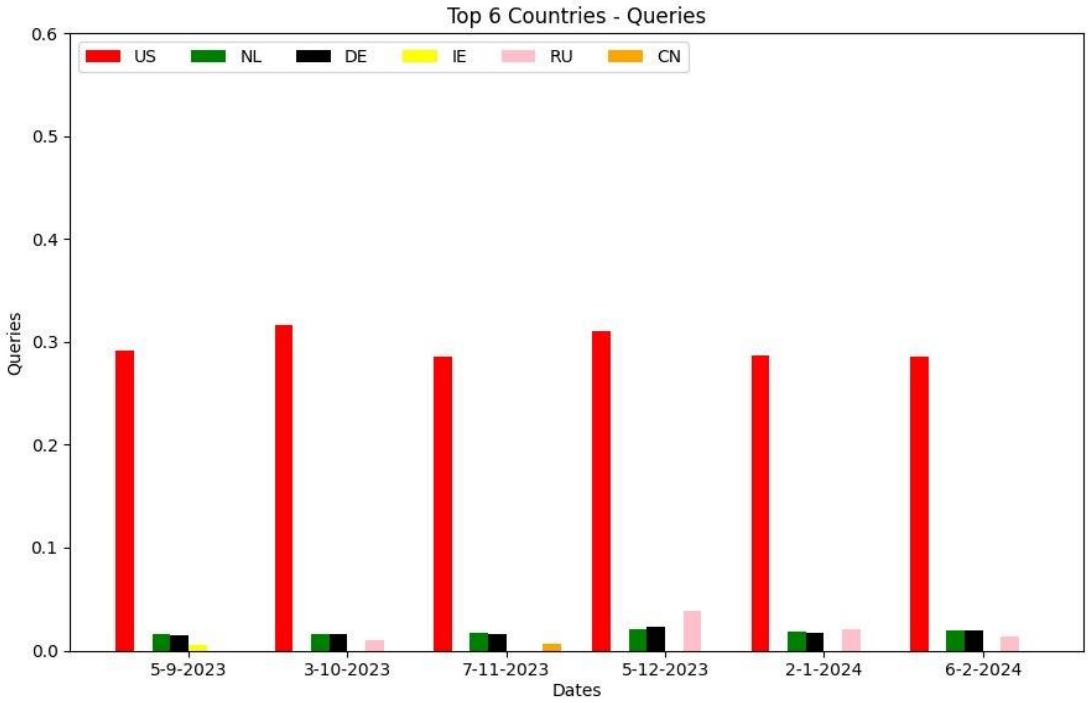
Attributes

- Frequency by origin country
- RR of DNS queries
- Unique IP addresses
- Number of DNS queries

Measurements on several months



TOTAL DATA



FILTERED DATA

Conclusion

- DNS Tunneling is being used in the wild and can be detected in ccTLD traffic
- DNS query features like high entropy, encoded types, Uncommon RR, and NXDOMAIN.
- Highest ratio observed from U.S in .nl traffic.
- Russia included on the top 6 ratio in potential DNS tunneling queries in .nl traffic.
- Detection almost 3000 unique domains remain in a specific day.
- Universal detection techniques apply in all DNS hierarchy.
- Common usage of DNS tunneling in daily traffic.

Future Work

- DNS Tunneling with QNAME Minimization
- More in-depth analysis of identified queries
- Custom Rules on ccTLDs
- Custom Rules on Root DNS Servers
- Machine Learning Detection of DNS tunneling

Damianos Christos Nikou
Graduate Student at Radboud University

LinkedIn: https://www.linkedin.com/in/damianos-christos-nikou/

Thesis: https://www.sidnlabs.nl/en/news-and-blogs/detection-analysis-and-measurement-of-dns-tunnelling-techniques

Thank You For Your Attention!

QUESTIONS?