DNS Security

Securing the Internet's Directory & AI Potential

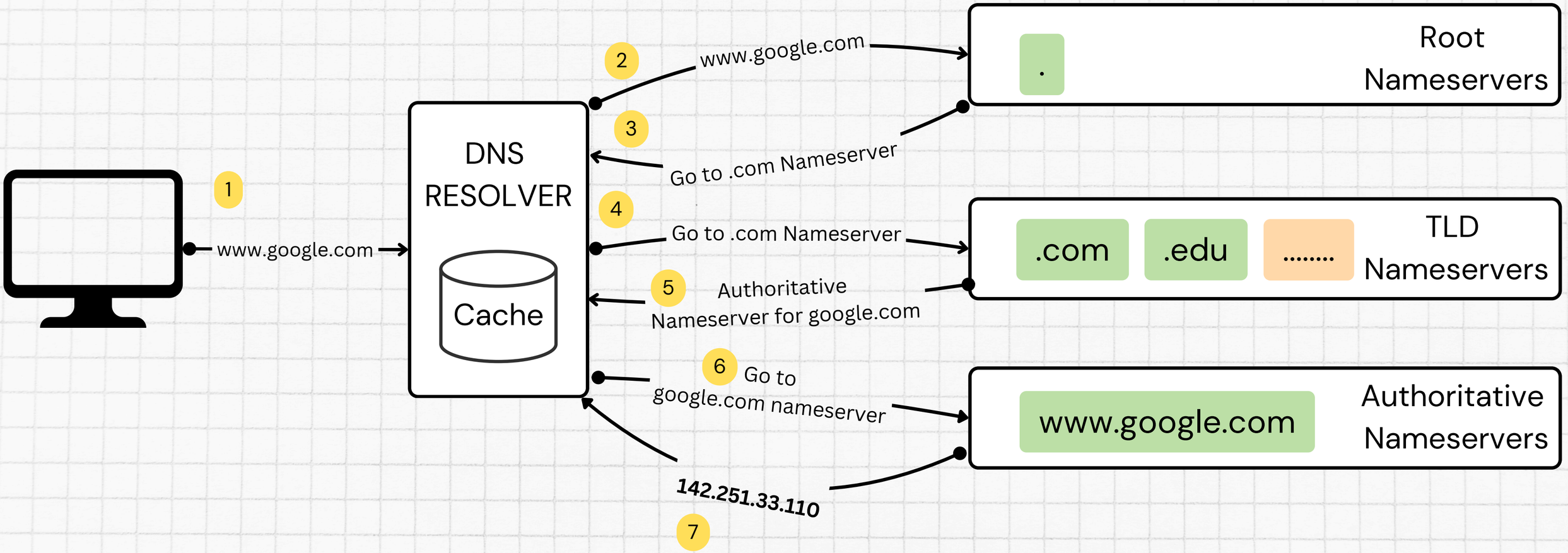
By Aviral Kaintura

About me

I'm a student pursuing a unique dual degree combination - Data Science at IIT Madras and Cybersecurity at National Forensic Sciences University, Delhi.
I'm passionate about where AI meets security, and love exploring how modern tech can make our digital world safer.

DNS (Domain Name System) Basics

- Translates human-readable names into IP addresses
- Example: www.google.com ➜ 142.251.33.110



Vulnerabilities in DNS

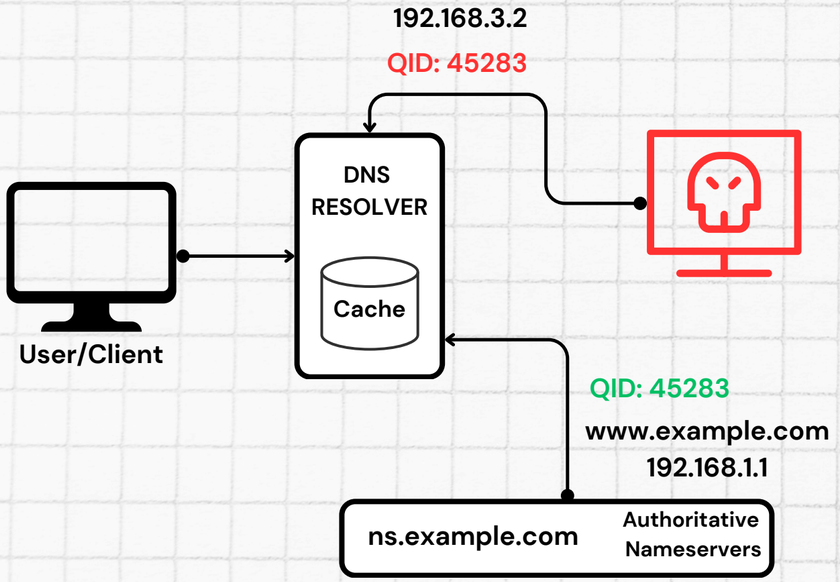
- Data corruption during transfers between servers and resolvers
- No built-in validation mechanisms
    1. Exploitable resolver implementations
    2. Cache pollution risks
    3. Long-term corruption persistence
- Compromised transactions between primary and secondary servers

DNS Attacks

DNS Spoofing

Method: DNS Cache Poisoning

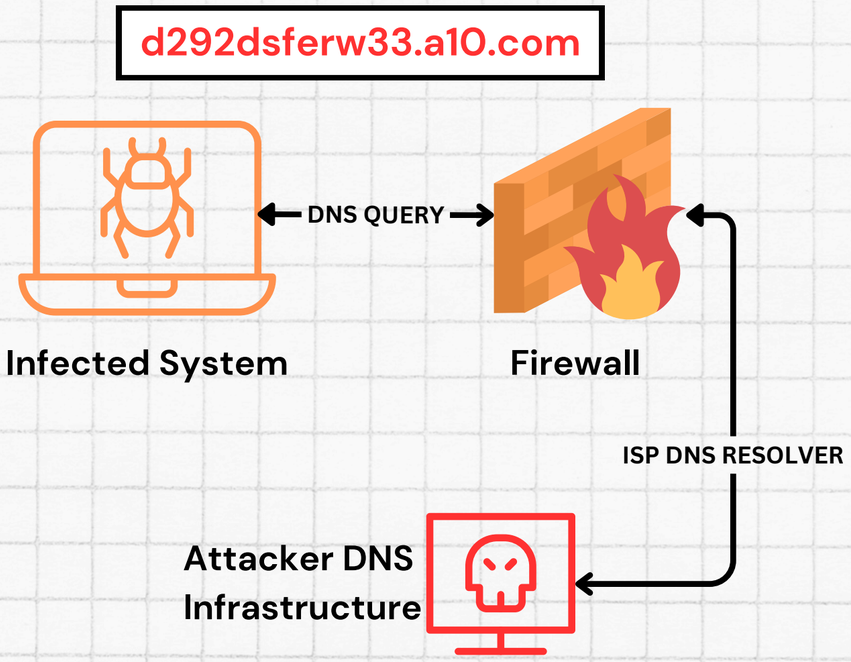
Redirects users to fake sites by corrupting DNS resolver cache with malicious IP addresses.



DNS Based Malware

Method: DNS Tunneling

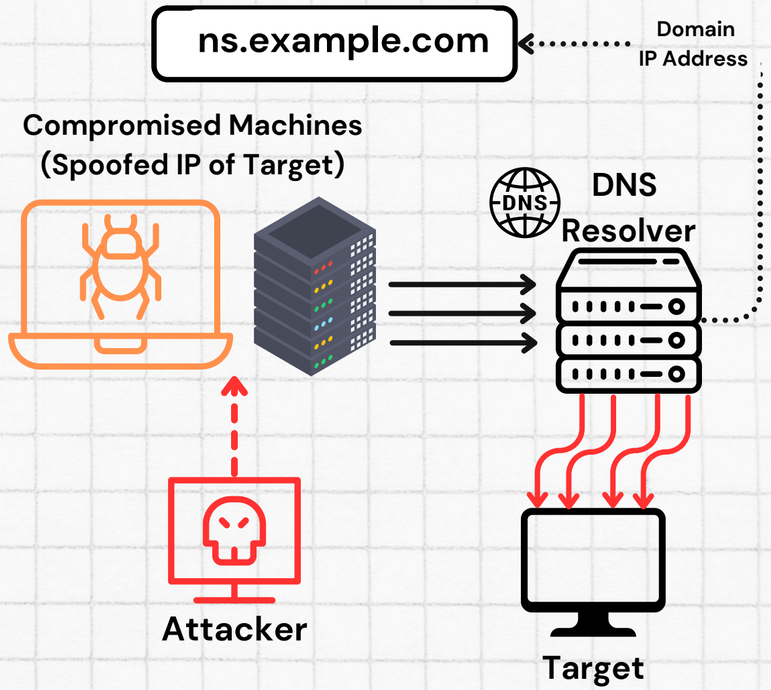
Exploits DNS queries to create covert communication channels for data theft and malware control.



DDOS using DNS

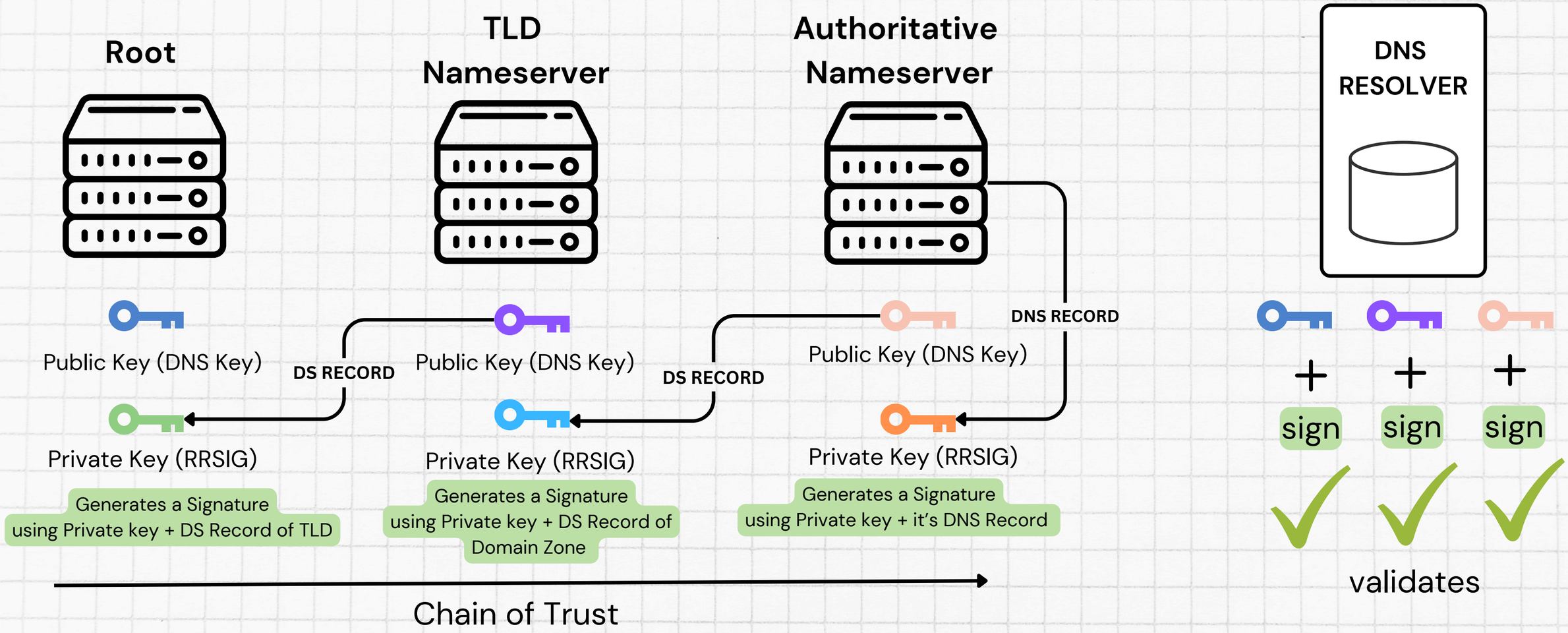
Method: DNS Amplification

Overwhelms targets by using DNS servers to multiply attack traffic (**small query → large response**)



DNSSEC (DNS Security Extensions) Basics

- DNSSEC makes sure that the responses to the DNS queries are from the correct source
- Adds cryptographic signatures to DNS records
- *"Like adding a digital seal of authenticity to DNS data"*



Mitigation Strageties

Prevention

- DNSSEC

Detection

- Traffic Monitoring
- Pattern Analysis
- Packet Analysis:
  - Deep Packet Inspection
  - Protocol Analysis
  - Header Examination

Response

- Filtering
- Rate Limiting

DNS Spoofing

- Implement DNSSEC
- Use random transaction IDs
- Query port randomization

DNS Based Malwares

- Monitor DNS query patterns
- Implement DNS filtering
- AI-based anomaly detection

DDOS Using DNS

- Response Rate Limiting (RRL)
- Anycast DNS infrastructure
- Traffic filtering

Using LLM for Real-Time Network Analysis

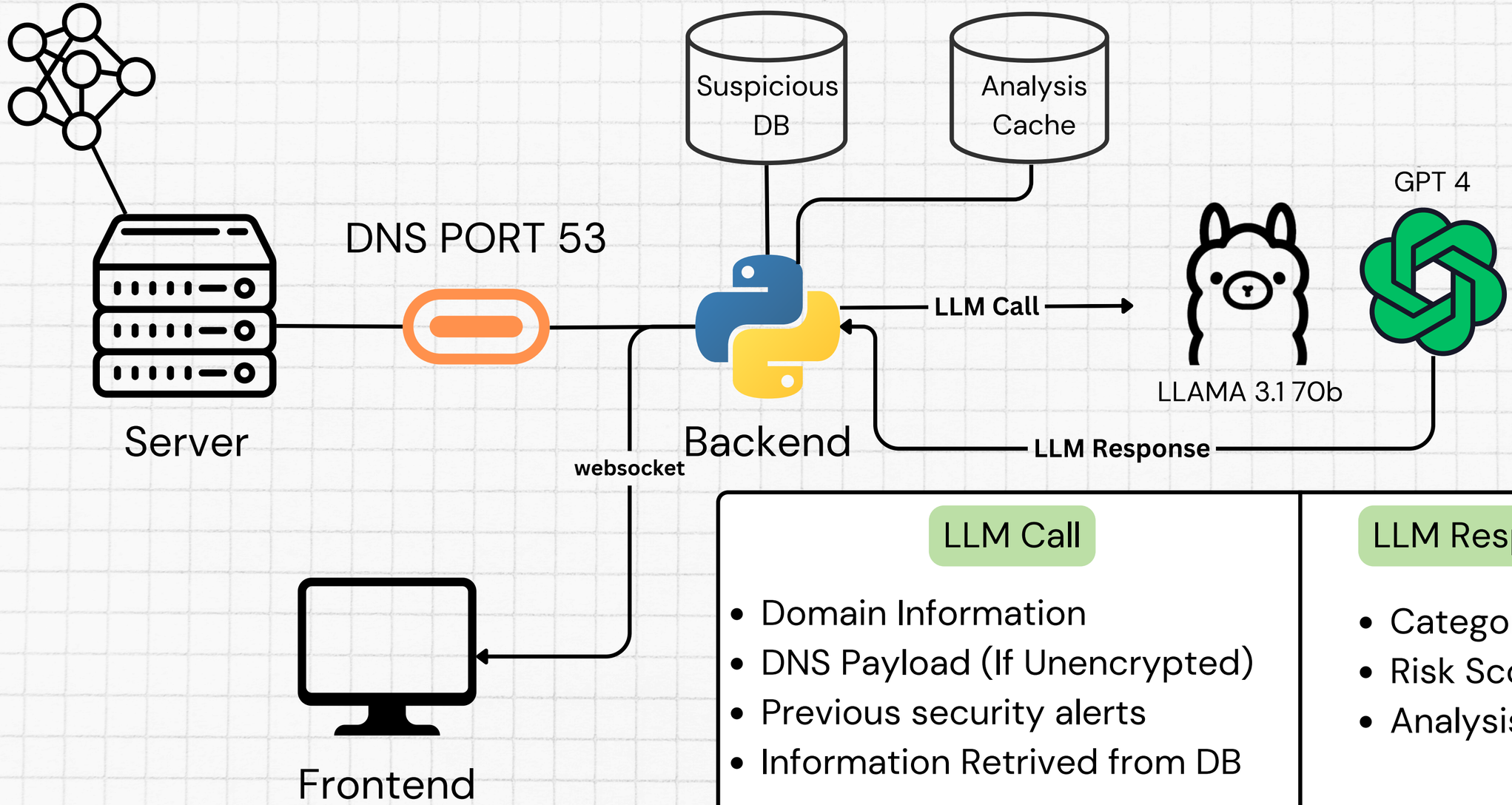
Benefits of LLM Integration:

- Real-time pattern recognition in DNS queries and responses
- Ability to learn and adapt to new attack patterns
- Natural language processing for threat intelligence
- Automated correlation of multiple data sources
- Predictive analysis of potential threats

Advanced Filtering & Response:

- Intelligent classification of DNS queries
- Context-aware blocking decisions
- Dynamic rule generation based on emerging threats
- Behavioral analysis of DNS traffic patterns
- Automated response to identified threats

Using LLM for Real-Time Network Analysis



LLM Call

- Domain Information
- DNS Payload (If Unencrypted)
- Previous security alerts
- Information Retrived from DB

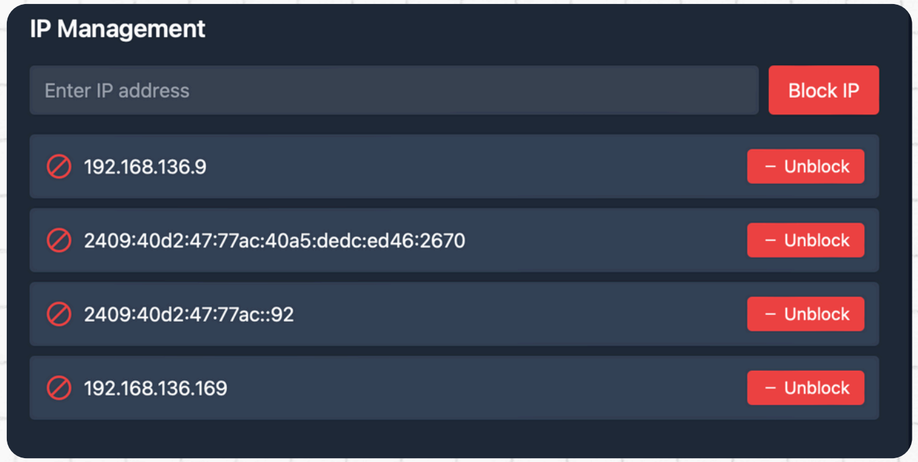
LLM Response

- Category
- Risk Score
- Analysis

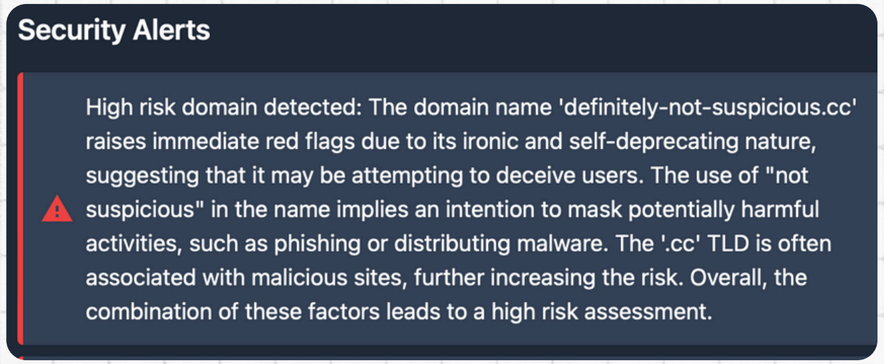
Recent Queries

Time	Domain	Category	Risk Score	Analysis
03:38:56	definitely-not-suspicious.cc	Malicious	0.90	The domain name 'definitely-not-suspicious.cc' raises immediate red flags due to its ironic and self-deprecating nature, suggesting that it may be attempting to deceive users. The use of "not suspicious" in the name implies an intention to mask potentially harmful activities, such as phishing or distributing malware. The '.cc' TLD is often associated with malicious sites, further increasing the risk. Overall, the combination of these factors leads to a high risk assessment.
03:38:56	5165899.xyz	malicious	0.80	The domain '5165899.xyz' appears to be associated with potentially malicious activities, as the '.xyz' TLD is often used for temporary or disposable websites. The numeric structure of the domain suggests it may be part of a larger scheme, possibly for phishing or spamming purposes. Additionally, the lack of recognizable branding or content further raises concerns about its legitimacy, leading to a higher risk score.
03:38:56	malicious-looking-domain.top	Malicious	0.90	The domain name 'malicious-looking-domain.top' suggests a clear intent to deceive or mislead users, as it explicitly includes the term "malicious-looking." The use of the top-level domain '.top' is often associated with less reputable sites, further indicating potential risk. Given these factors, the risk score is high, reflecting the likelihood that this domain could be used for phishing, scams, or other malicious activities.
03:38:56	5165899.xyz	malicious	0.80	The domain '5165899.xyz' exhibits characteristics often associated with malicious activity, such as the use of a less common top-level domain (TLD) which is frequently utilized for spam, phishing, or other harmful purposes. The numeric nature of the domain name also suggests it may be a randomly generated name, a common tactic used by malicious actors to evade detection. Given these factors, the risk score is elevated.
03:39:01	www.googleapis.com	API	0.10	The domain 'www.googleapis.com' is associated with Google APIs, which provide developers with tools and services to build applications. It is a legitimate domain used for accessing various Google services, making it low risk. The domain is well-known and widely used in the tech industry, indicating a trusted source.

LLM labels '**definitely-not-suspicious.cc**' as malicious with a **0.90** risk score, while legitimate domains like '**googleapis.com**' receive low risk scores (**0.10**) and are properly categorized as API endpoints.



Auto Blocking Malicious IPs



Showing Security Alerts

Source: xkcd

Any Questions ?