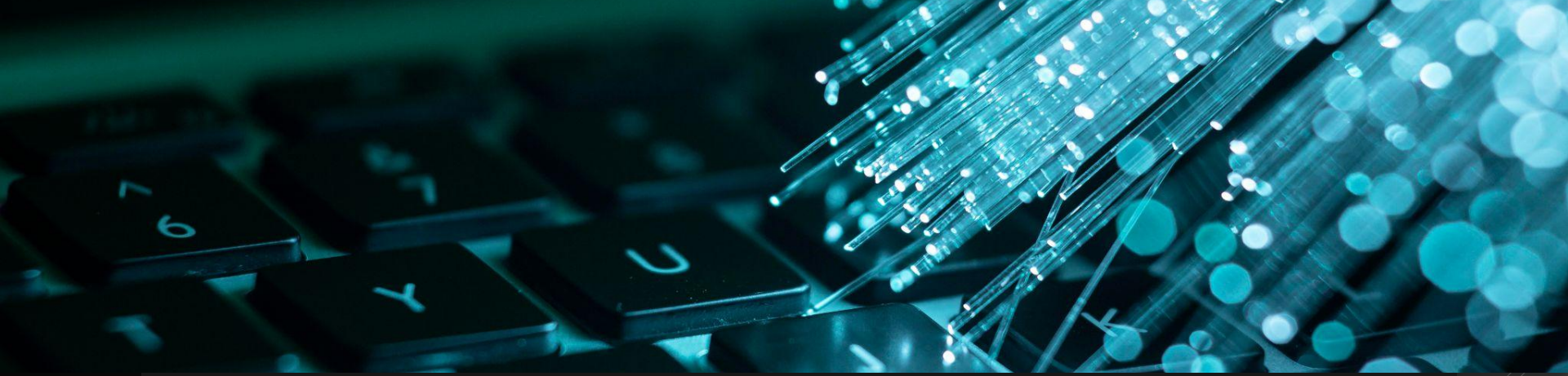


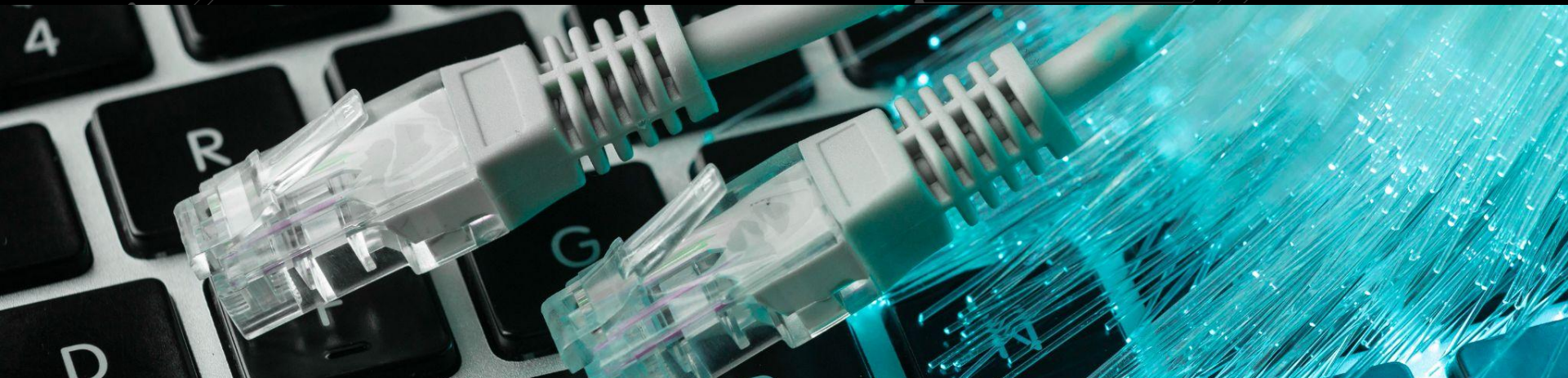
Técnicas e Perceção de Redes

DNS Tunneling

João Viegas - 98372
Tiago Marques - 98459

Table of contents

01 Security Problem



Why attackers use DNS for tunneling?

1. DNS is a common and essential part of internet communication
2. Typically uses UDP port 53, which is often allowed through firewalls for legitimate DNS queries
3. Is a fundamental service used by virtually every device connected to the internet

Importance of Security/Issue

DNS tunneling uses a client program on compromised machines and a server program on the attacker's DNS server.

Some attacks by dns tunneling are:

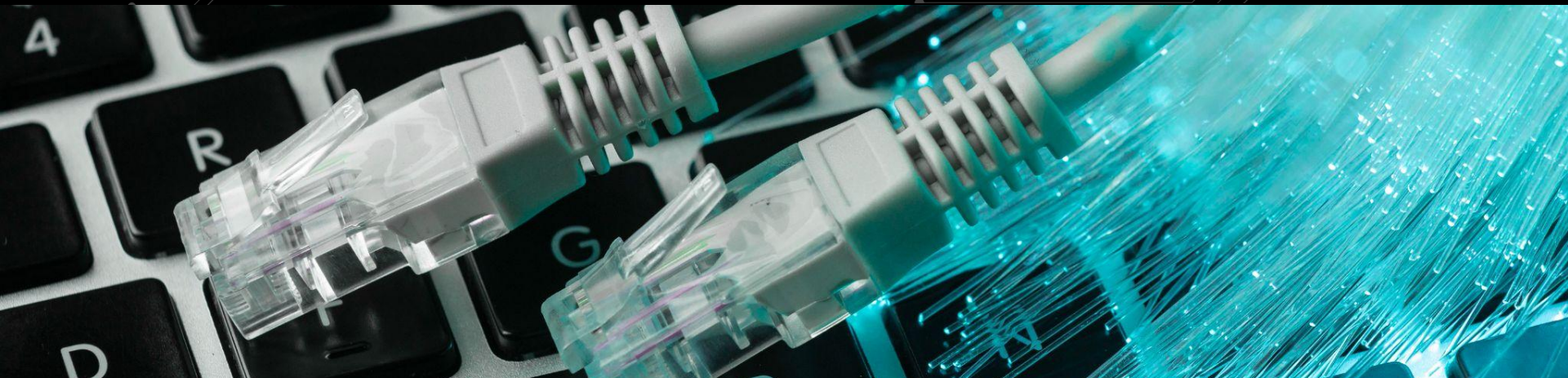
- C&C server communication

- Data exfiltration

- Malware propagation

It gives attackers a hidden way to control and communicate while stealing data, often going unnoticed because DNS traffic is noisy

02 Data Sources



Used Datasets

Not malicious Source

The non-malicious datasets will be obtained from an IEEE dataset w/10 days of DNS traffic.

Malicious Source

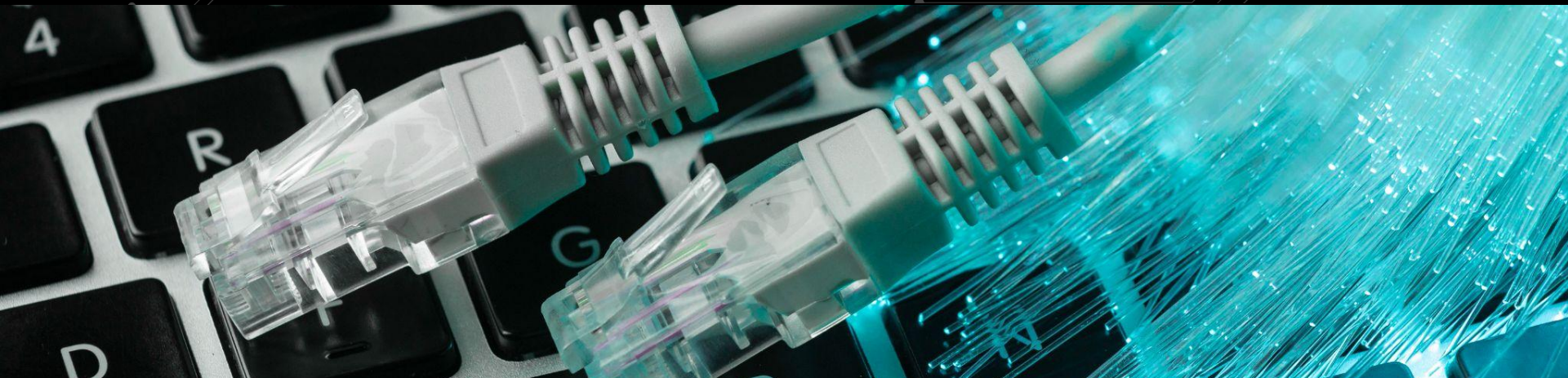
Our malicious dataset will be generated in-house through the use of virtualization (VMs), DNScat2 (DNS Tunneling Software) and bind9(DNS software).

Real World Scenario

- Encapsule malicious commands, data, or communication channels
- It's possible to encrypt DNS queries making it impossible to verify the contents of the query

- Make use of the DNS nature to:
  - Try to evade detection
  - Try to establish a stealthy communication channel

03 Test Scenario



Our Scenario

Assumptions:

- Outgoing DNS requests are not filtered
- Attacker got access to a normal machine
- It installed DNS Tunneling software
  - DNScat2, Iodine, Heyoka

Anomaly Detection:

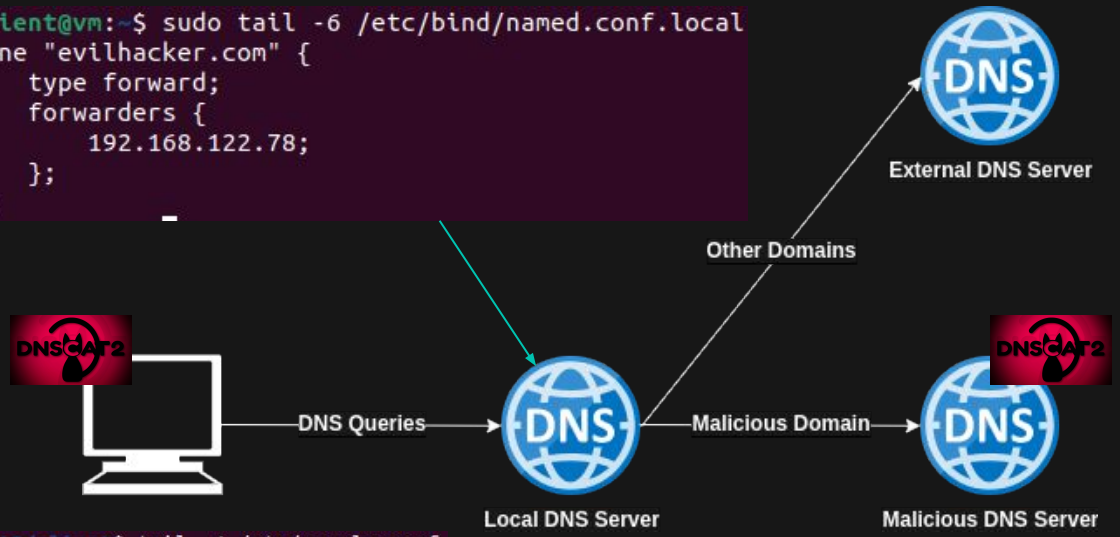
- Normal user behaviour is used to construct a profile
- Deviations from this profile will be identified as anomalies

Scenarios:

- Reverse shell usage to search for important information
- Copy files (scp command) which incites abnormal behaviour

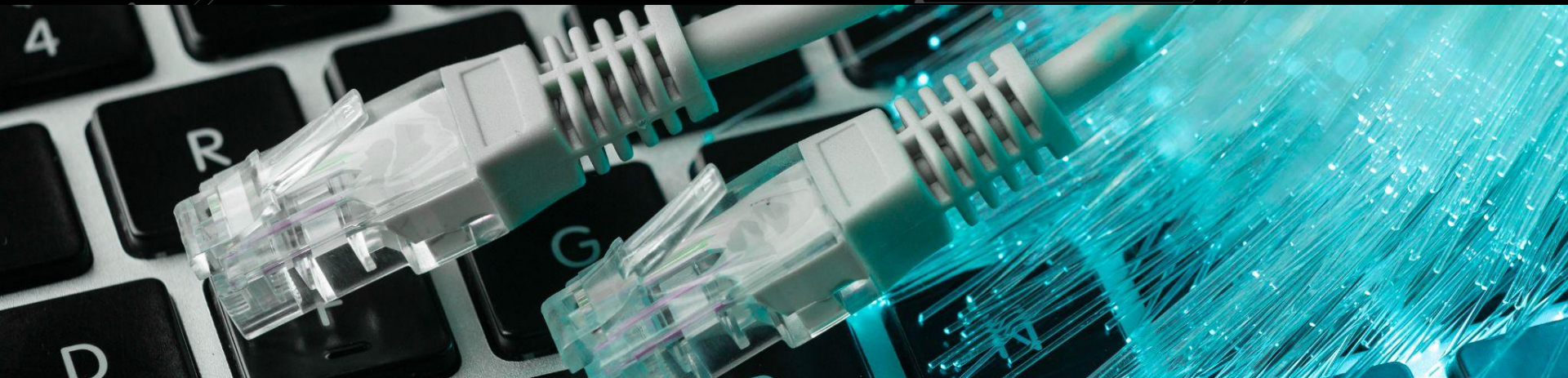
Test Scenario

```
client@vm:~$ sudo tail -6 /etc/bind/named.conf.local
zone "evilhacker.com" {
    type forward;
    forwarders {
        192.168.122.78;
    };
};
```




```
client@vm:~/dnscat2/client$ tail -4 /etc/resolv.conf
nameserver 192.168.122.58
nameserver 127.0.0.53
options edns0 trust-ad
search .
```

04 Data Sampling



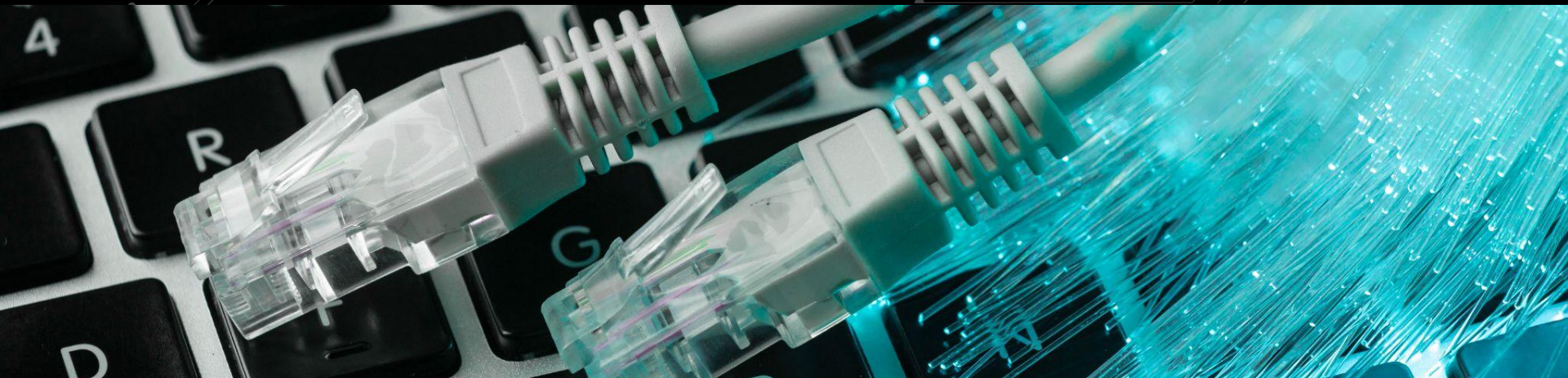
Metrics to extract

- **Number of Packets TCP/UDP**
  - Source IP address
    - Check weird IPs
    - Identify users and respective upload/download packets
  - Source ports
    - Check for unusual ports usage
  - Packet timestamp
    - Check for frequency between group of packets
  - Query Response Time
    - After sending a DNS query the time it takes to get a response

Observation Window

- **Sliding window**
  - To detect abnormalities as quickly and e ciently as possible
  - Size of 5-10 minutes
  - Sliding 1 minute
  - Considering a sampling period of 1-5 seconds to gather data

05 Features



Features

- **Number of Packets TCP/UDP**
  - Mean, Median, Variance
  - Number of packets in a given time frame
  - Autocorrelation of number of packets (periodicity)
  - Percentiles
  - Periods of activity
  - Mean, Median, Variance of activity periods
- **Number Upload/Download Packets**
  - Mean, Median, Variance
  - Quantiles/Percentiles

Bibliography

- **Cyber Attacks using DNS Tunneling**
  - https://www.bleepingcomputer.com/news/security/new-linux-botnet-exploits-log4j-uses-dns-tunneling-for-comms/
  - https://www.bleepingcomputer.com/news/security/chinese-hackers-use-dns-over-https-for-linux-malware-communication/
- **Dataset Source**
  - https://ieee-dataport.org/documents/ti-2016-dns-dataset