Identify Malware with Zui

What is Zui?

The Zed User Interface (ZUI) focuses on providing a more user-friendly and visual way to analyze network traffic data, particularly data generated by Zeek and other sources. Zui applies predefined rules to detect malicious activity, including known attack patterns, anomalies, and other threats.

Question: Identify DNS Tunneling malware.

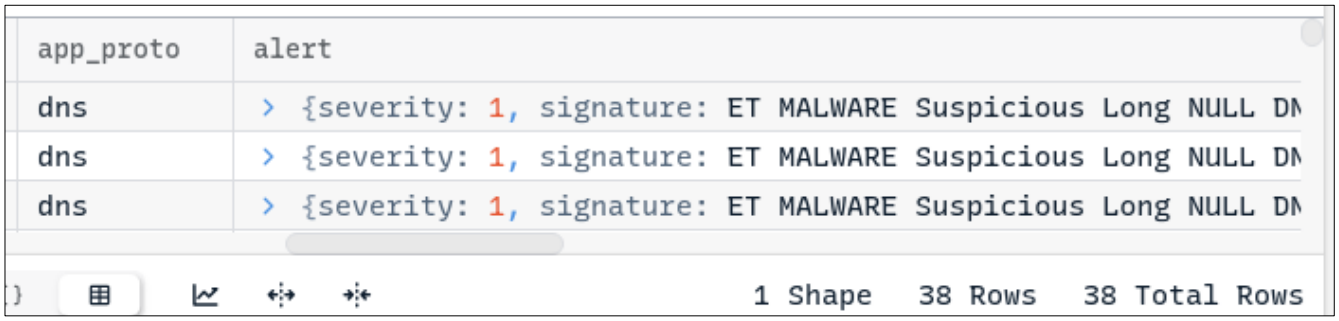
Steps

- Import network data into Zui
- Query the DNS tunneling malware alert type:

```
from dns.pcap

1   event_type=="alert" | fuse
2   | alert.signature=="ET MALWARE Suspicious Long NULL DNS Request - Possible DNS Tunneling"
```

Results



Finding: 38 alerts are possible DNS Tunneling.

Solution

- **User Education:** Train users to recognize phishing attempts and other SE tactics that could lead to malware infection.
- **Endpoint Security:** Ensure robust endpoint protection measures are in place, including antivirus, anti-malware, and regular software updates.
- **Firewall Rules:** Configure firewalls to monitor and restrict DNS traffic, and implement rules to prevent tunneling.