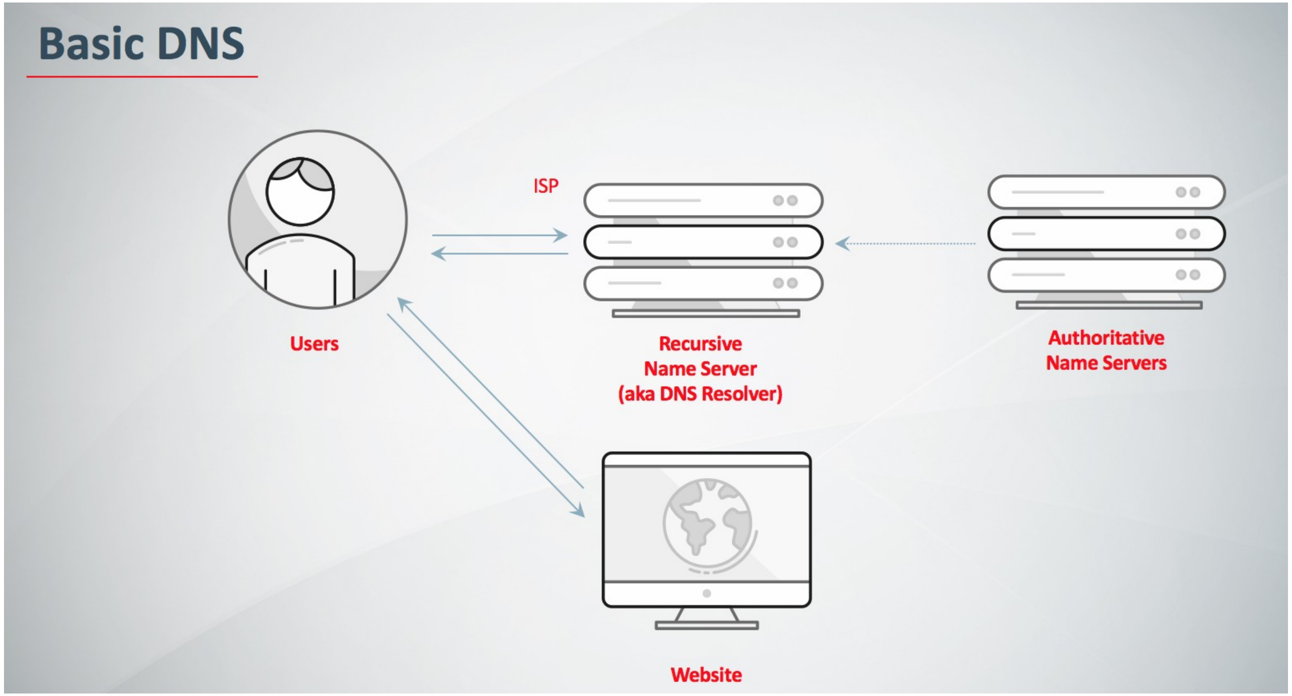
DNS
FTW!

PARENTAL

ADVISORY

EXPLICIT CONTENT

DNS basics

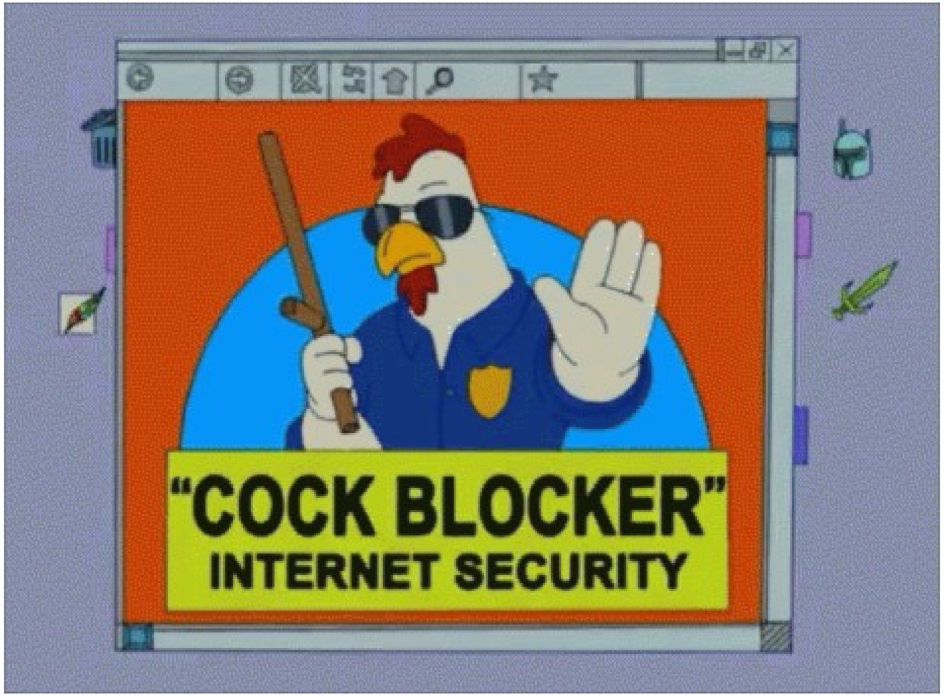

Basic DNS
ISP
Users
Recursive
Name Server
(aka DNS Resolver)
Authoritative
Name Servers
Website

Where do I get the data?

- Client
- Server
- On the wire

DNS-over-HTTPS = Game Over?

Block it!



Enrichment ideas

- Lookup types
- GeoIP the responses
- Split up the queries into TLD, domain and so on
- Count, count, count

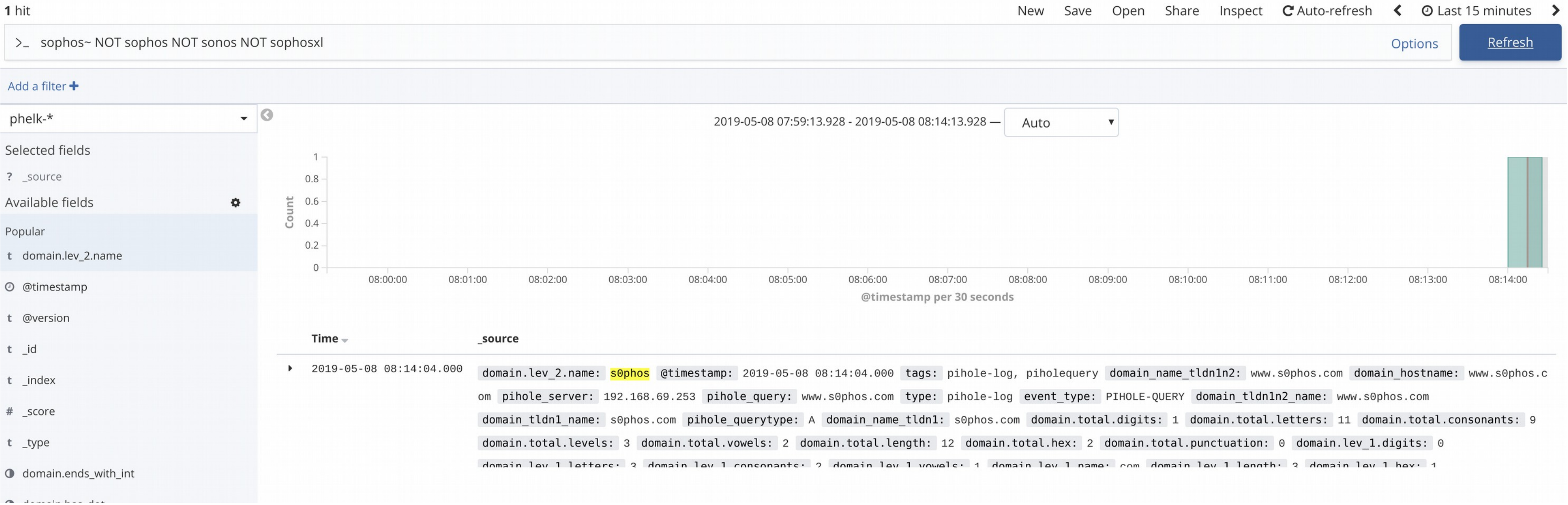
What can I use my enriched DNS data for?

- DNS exfiltration detection (also C2)
- Typo squatting / Phishing detection
- IDN / Homograph attack detection
- Incident Response
- Passive DNS

DNS exfiltration

- Many and shorter
- Fewer and longer

Typo squatting / phishing

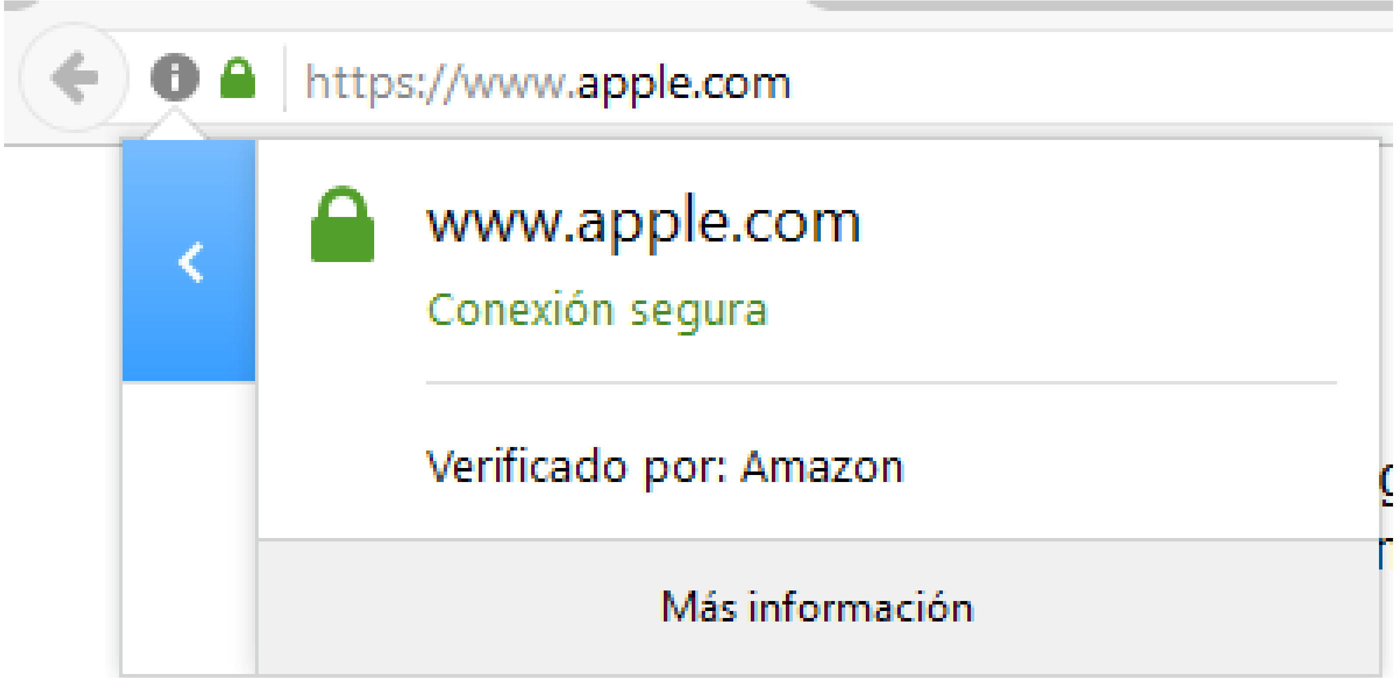


```
>_ sophos~ NOT sophos NOT sonos NOT sophosxl
```

2019-05-08 07:59:13.928 - 2019-05-08 08:14:13.928 —

```
2019-05-08 08:14:04.000   domain.lev_2.name: s0phos @timestamp: 2019-05-08 08:14:04.000 tags: pihole-log, piholequery domain_name_tldn1n2: www.s0phos.com domain_hostname: www.s0phos.c
om pihole_server: 192.168.69.253 pihole_query: www.s0phos.com type: pihole-log event_type: PIHOLE-QUERY domain_tldn1n2_name: www.s0phos.com
domain_tldn1_name: s0phos.com pihole_querytype: A domain_name_tldn1: s0phos.com domain.total.digits: 1 domain.total.letters: 11 domain.total.consonants: 9
domain.total.levels: 3 domain.total.vowels: 2 domain.total.length: 12 domain.total.hex: 2 domain.total.punctuation: 0 domain.lev_1.digits: 0
domain.lev_1.letters: 3 domain.lev_1.consonants: 2 domain.lev_1.vowels: 1 domain.lev_1.name: com domain.lev_1.length: 3 domain.lev_1.hex: 1
```

IDN / Homograph



https://www.apple.com

www.apple.com

Conexión segura

Verificado por: Amazon

https://www.xn--80ak6aa92e.com/

Failures can be your friend!*

* Not this particular failure though

Your DNS log data needs TLC

- Log
- Enrich
- Search / Alert
- Investigate
- Refine
- Repeat

Quick demo of some data

Pi-hole - Phelk

Contact and links

twitter.com/swedishmike

github.com/swedishmike/DNS-data-presentation

github.com/swedishmike/phelk

Sophos needs some good people

sophos.com/careers

So do we…

mwrinfosecurity.com/careers

Questions?