Client side DNS observability

DNSWatch, Meta's DNS snooping utility

Balint Csergo
Production engineer

Agenda

01 Introduction

02 DNS observability at scale

03 Our solution

04 Demo time

Introduction

Balint Csergo

(deathowl)

PE @ Meta (Since 2019)

Working on all things DNS and Network Time

Golang, Python

02 DNS Observability at scale

The problems we’re facing regarding DNS observability

- Monitoring production DNS service from the client side is troublesome.

The problems we’re facing regarding DNS observability

- Detecting anomalous behaviour from the server side logs is limited and delayed, data is heavily sampled

The problems we’re facing regarding DNS observability

- You found an offending host, but getting in depth and real-time information about every DNS query / process is nontrivial

03 Our Solution

DNSWatch

❤ eBPF

Reusable BPF code

- CO-RE (Compile Once – Run Everywhere)
- Uses Fentry/Fexit for performance reasons
- Kernel space capture of DNS traffic
- Returned struct is easy to parse in the userspace
- Kprobes can still be used in fallback mode.

Go code in the userspace

- Well tested thanks to how amazing Go is
- Easy to build and distribute for all our machines
- Userspace parsing and filtering of DNS packets captured by our eBPF code
- We use the same amazing miekg/dns as in DNSRocks

04 Demo Time

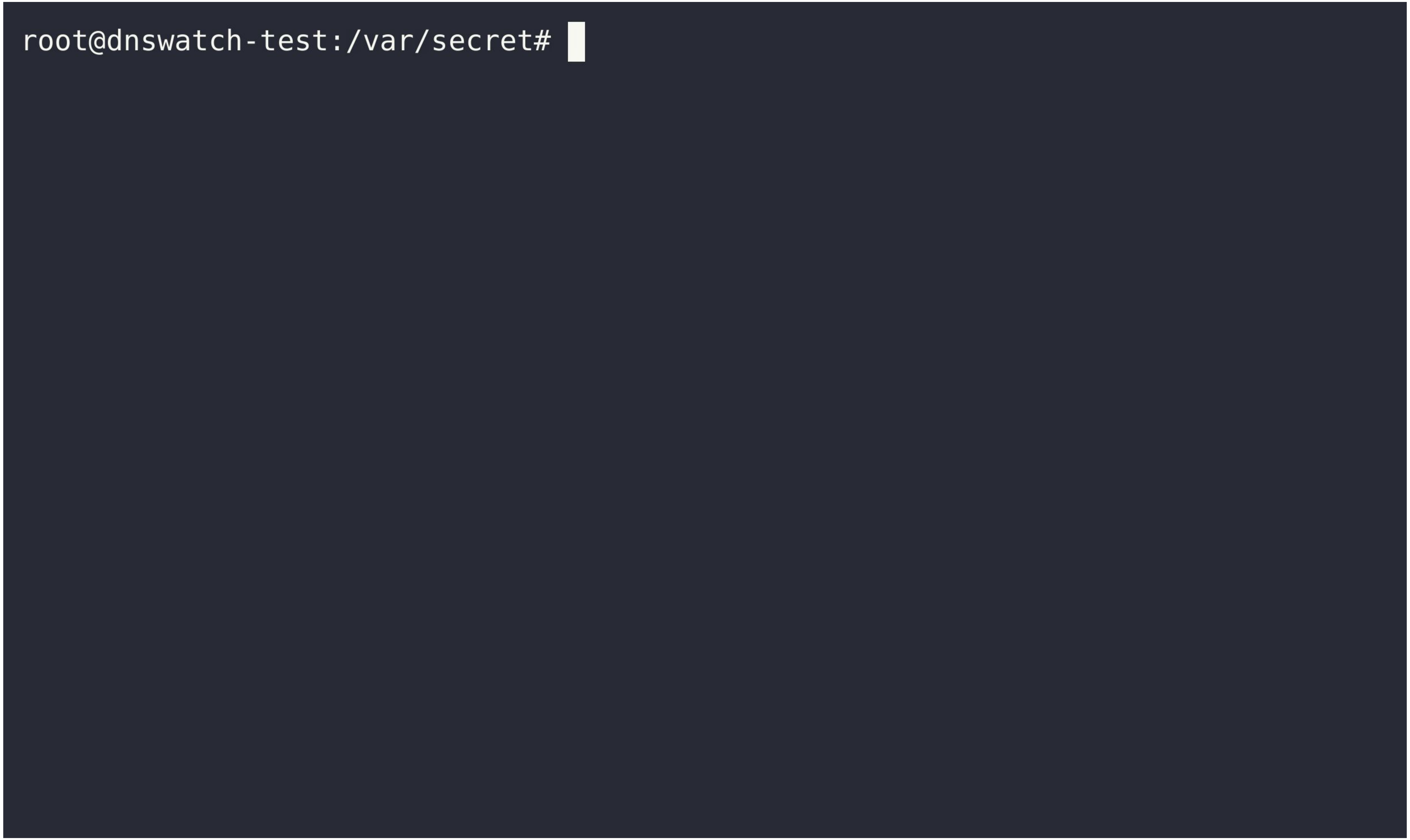
Using DNSWatch to detect DNS Data Exfiltration

Let’s look at this from the attacker’s perspective

04 Demo Time

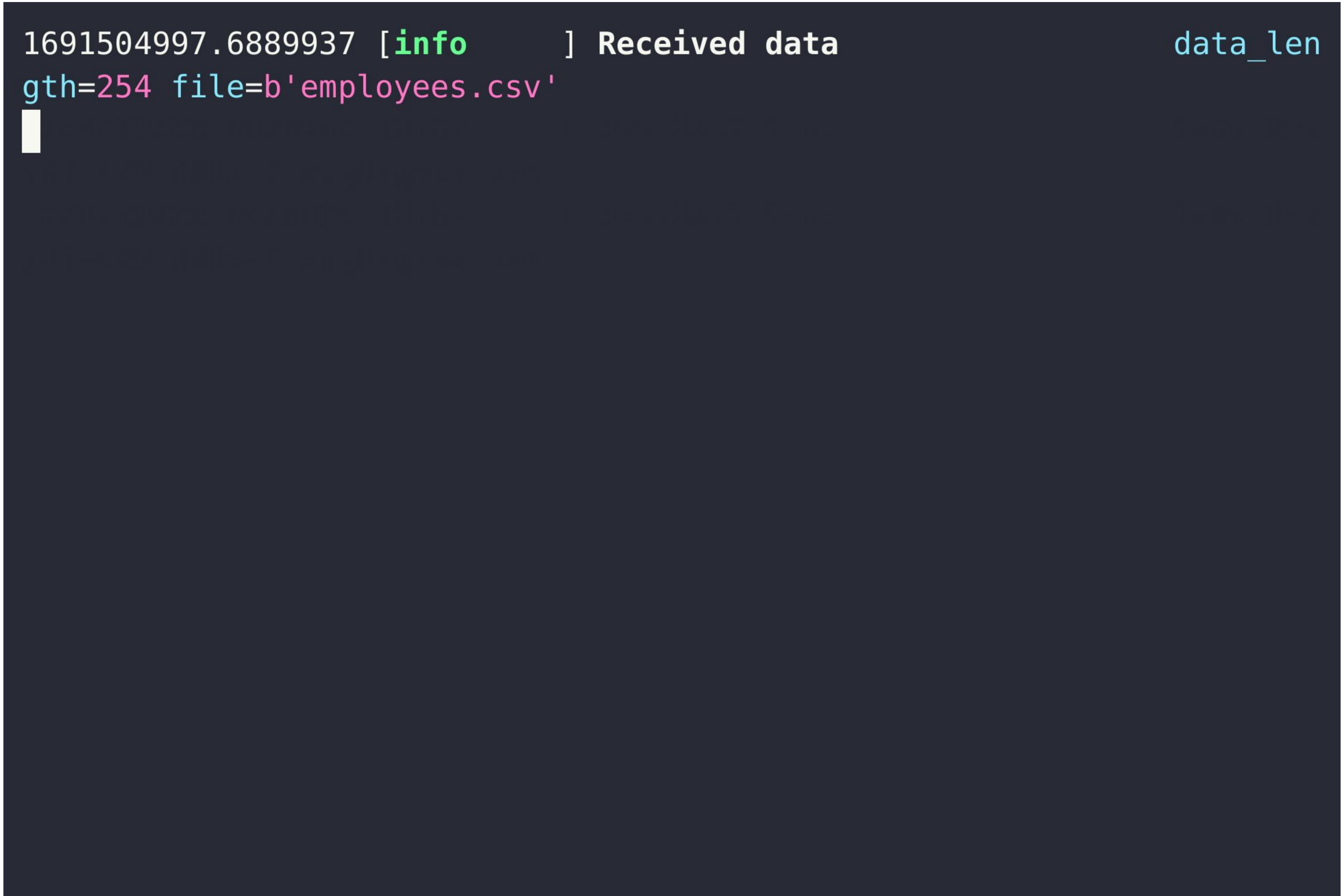
```
root@big-daddy:~/dnsteal# 
```

04 Demo Time



```
root@dnswatch-test:/var/secret# 
```

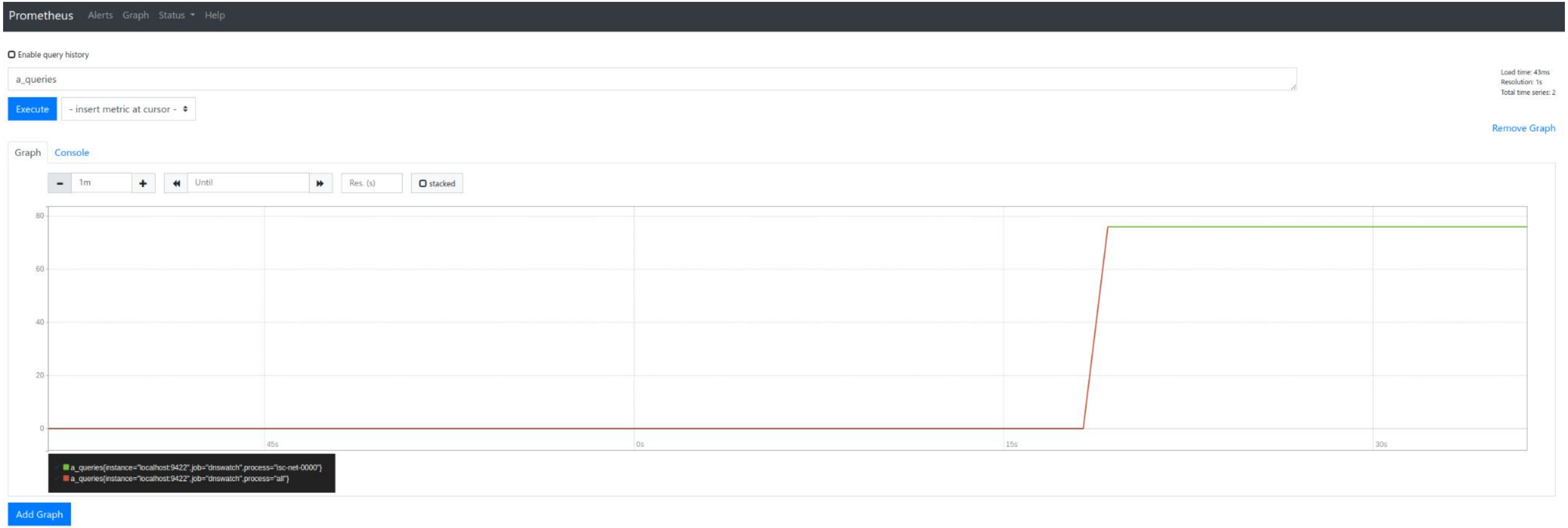
04 Demo Time



```
1691504997.6889937 [info      ] Received data                  data_len
gth=254 file=b'employees.csv'
```

Detecting anomalous behaviour using DNSWatch

04 Demo Time



```
a_queries
```

Load time: 43ms
Resolution: 1s
Total time series: 2

🟩 a_queries{instance="localhost:9422",job="dnswatch",process="isc-net-0000"}
🟥 a_queries{instance="localhost:9422",job="dnswatch",process="all"}

Diving deeper into what actually happens on the host

04 Demo Time

```
root@dnswatch-test:~/dns/dnswatch# 
```

It’s open source

https://github.com/facebook/dns

THX

- Yaroslav Kolomiiets (@yarikk)
- Oleg Obleukhov (@leoleovich)
- Alex Bulimov (@abulimov)
- Pablo Mazzini (@pmazzini)
- Patrick Cullen (@t3lurid3)
- Vadim Fedorenko (@vvfedorenko)
- Vlad Mihailescu

QUESTIONS?
LOVETHISPIC.COM
imgflip.com

Meta