MADDVIPR

Open INTEL

DNSAttackStream: Impact of DDoS attacks against DNS Infrastructure

caida

UNIVERSITY OF TWENTE.

Mattijs Jonker, Raffaele Sommese

University of Twente

DUST 2021

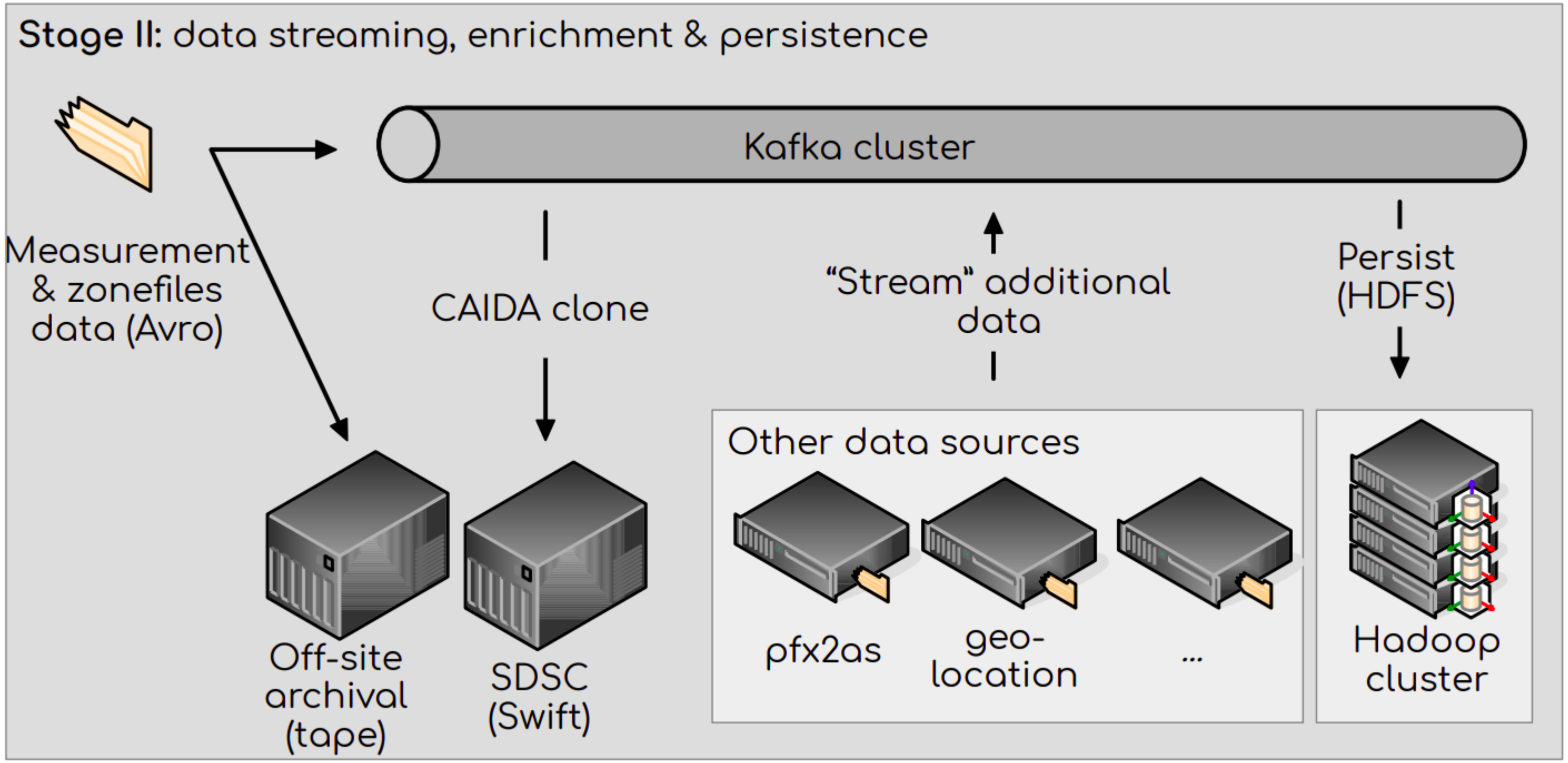
NWO
Netherlands Organisation
for Scientific Research

U.S. DEPARTMENT OF HOMELAND SECURITY

Introduction

- STARDUST via RSDoS Metadata dataset provides live insights of randomly spoofed Denial-of-Service attacks.
- In the frame of MADDVIPR project, we join this data with OpenINTEL DNS live measurements.
- We shed light on impact of DDoS attack against DNS infrastructure.
- In this talk, we will discuss:
  1. The evolution of OpenINTEL towards a streaming platform.
  2. DNSAttackStream
  3. The path for new reactive measurements.

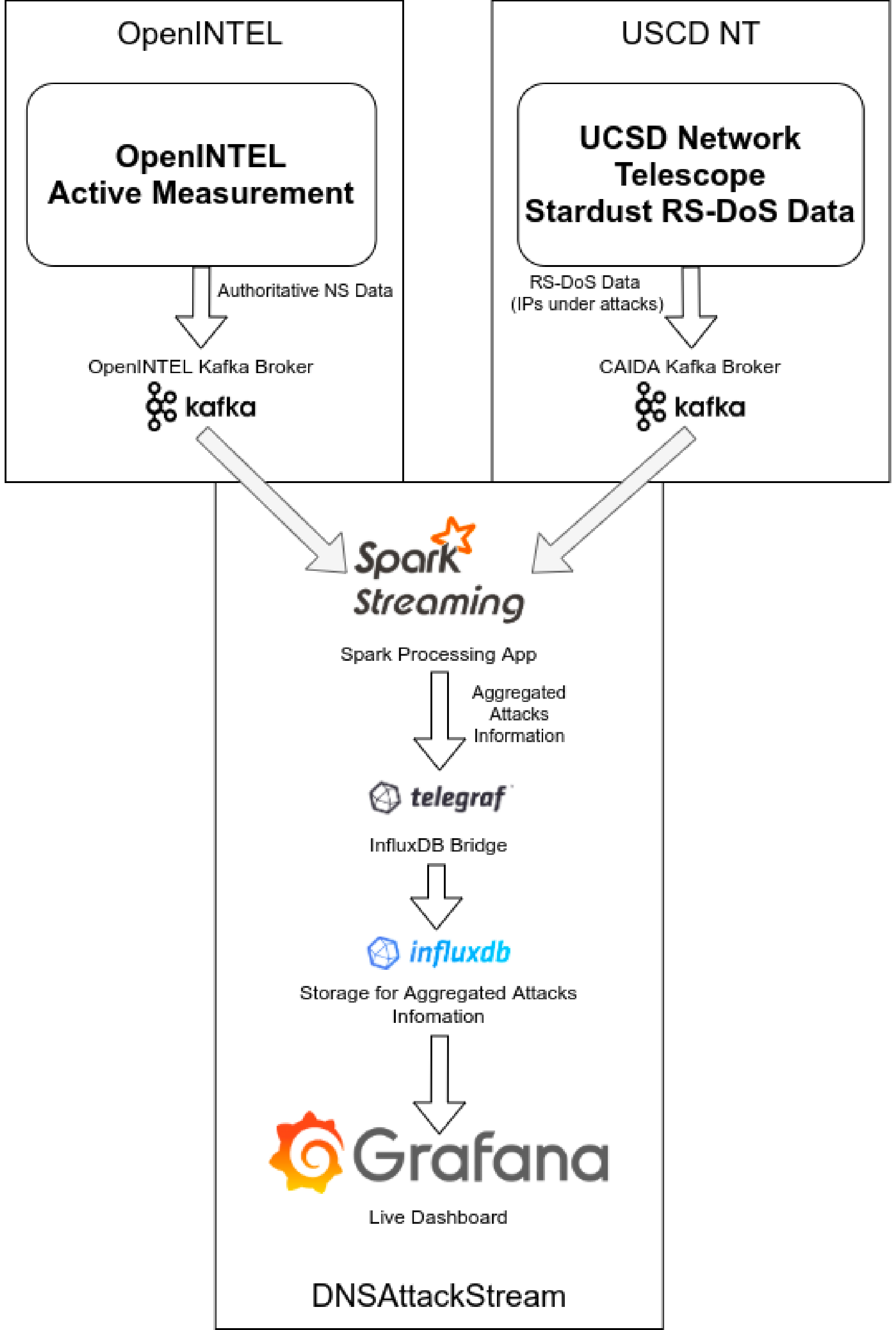
The streaming architecture



DNSAttackStream

- Joining the live Kafka feed of **RS-DoS** attack information with **OpenINTEL** live measurements every 5 minutes.
- DNSAttackStream identifies IP addresses of authoritative nameservers measured by OpenINTEL under attack.
- We provide insights of the number of authoritative nameservers and related Second Level Domains (SLDs) affected by attacks.

The Architecture



OpenINTEL

OpenINTEL Active Measurement

Authoritative NS Data

OpenINTEL Kafka Broker

kafka

USCD NT

UCSD Network Telescope Stardust RS-DoS Data

RS-DoS Data (IPs under attacks)

CAIDA Kafka Broker

kafka

Spark Streaming

Spark Processing App

Aggregated Attacks Information

telegraf

InfluxDB Bridge

influxdb

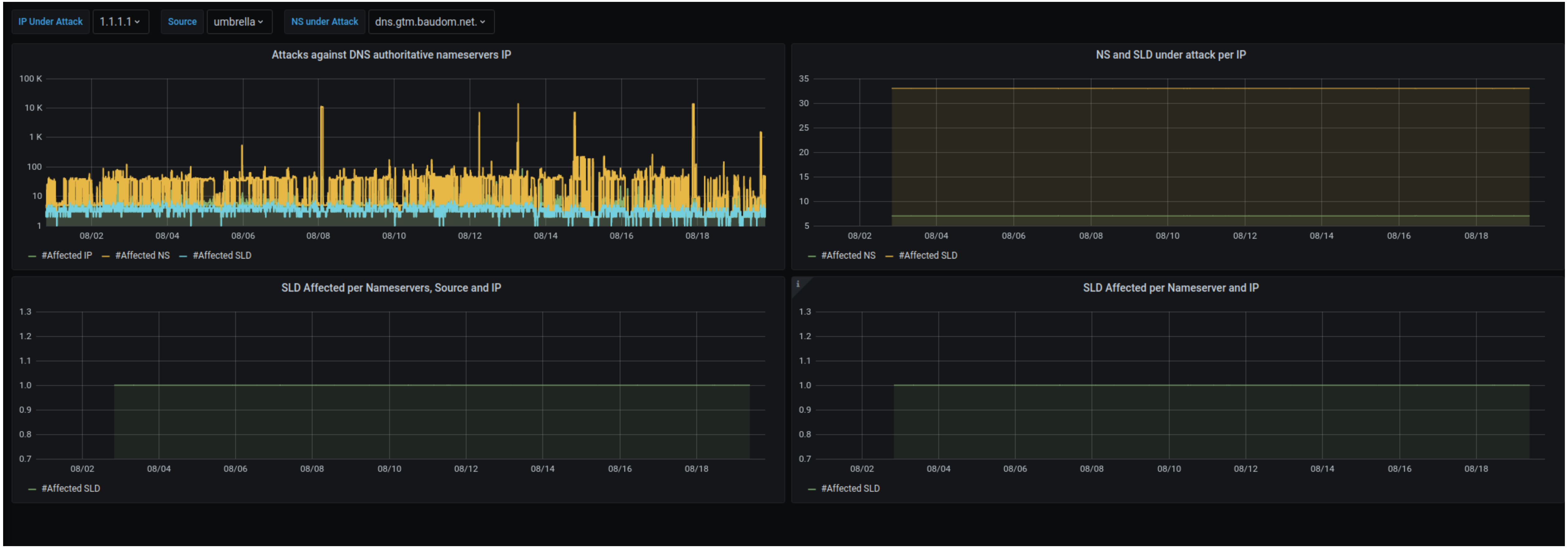
Storage for Aggregated Attacks Infomation

Grafana

Live Dashboard

DNSAttackStream

Live Attacks Dashboard

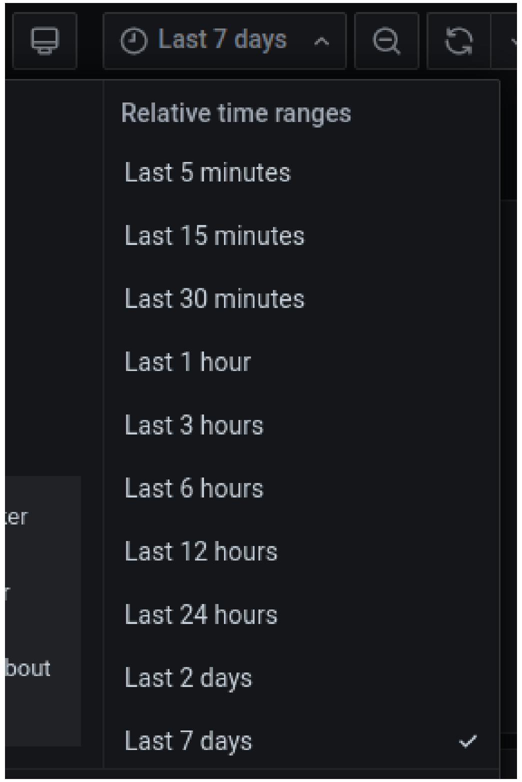


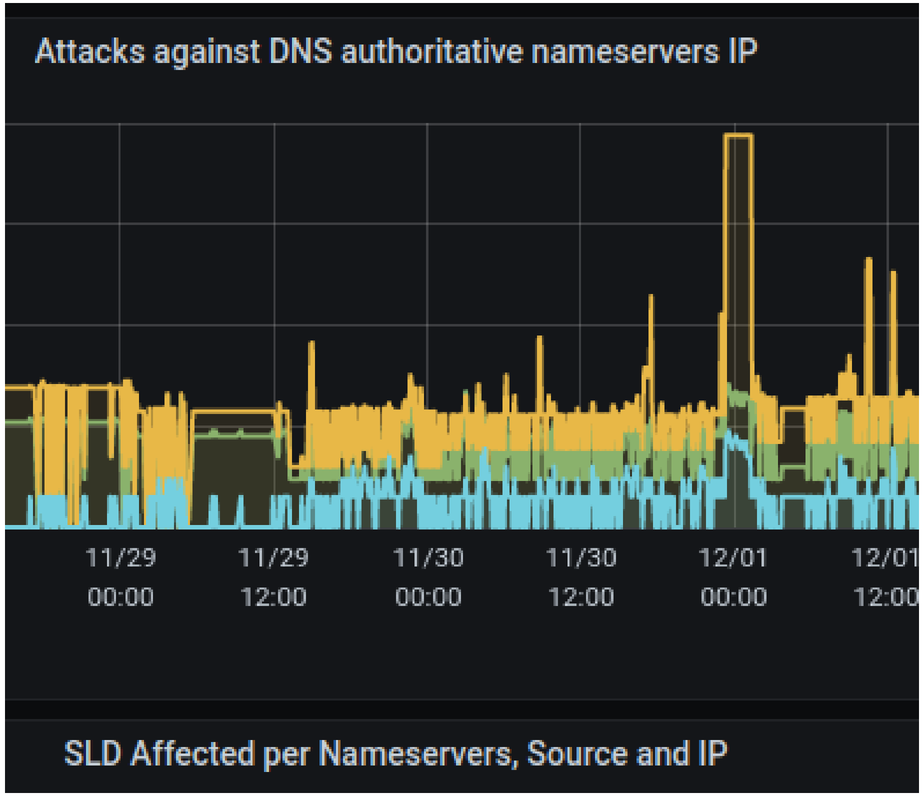
IP Under Attack: 1.1.1.1

Source: umbrella

NS under Attack: dns.gtm.baudom.net.

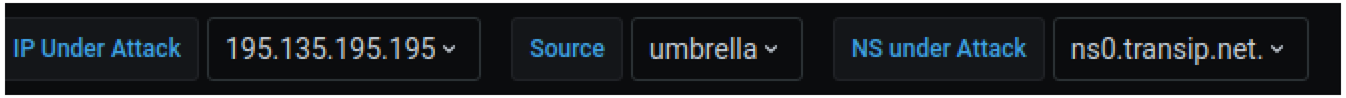
Live Attacks Dashboard




Attacks against DNS authoritative nameservers IP

SLD Affected per Nameservers, Source and IP

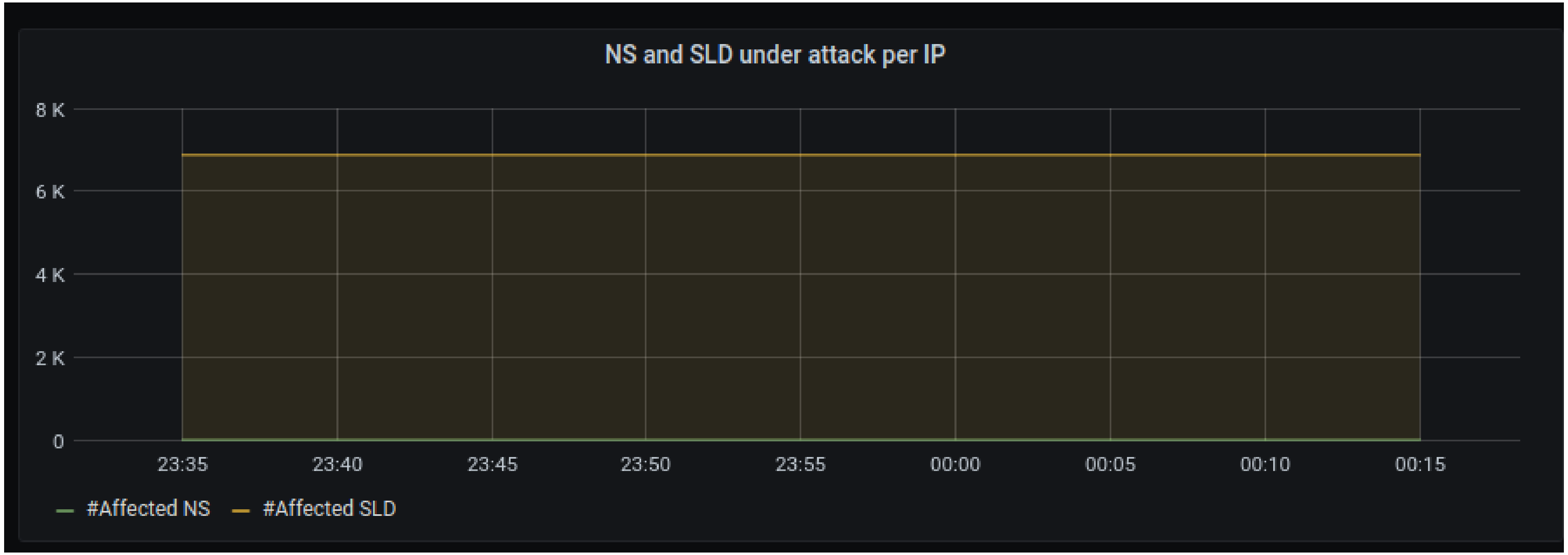
ProActive Attack Detection: The TransIP Case



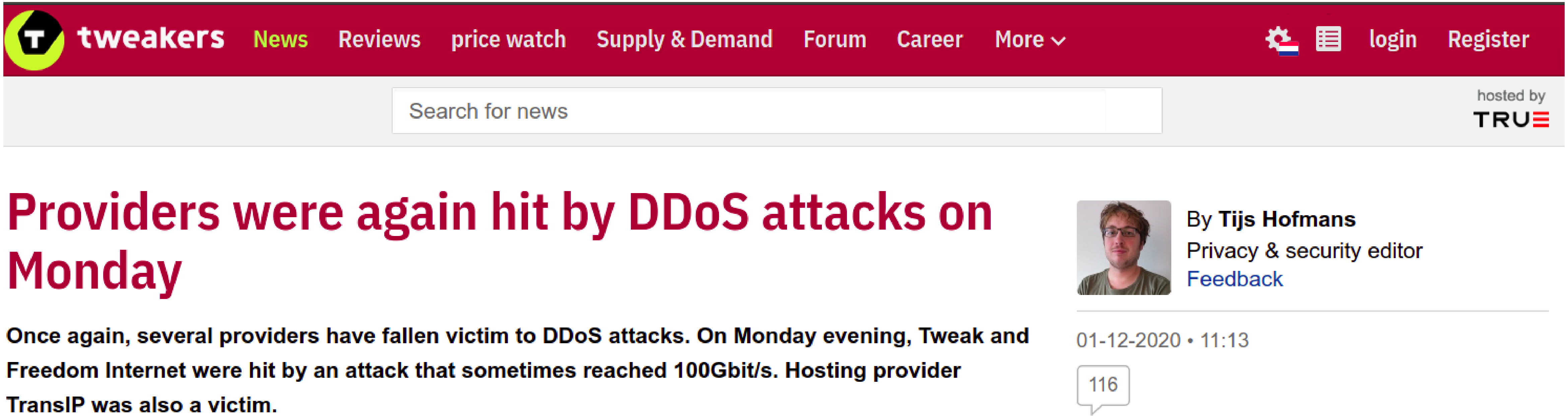
IP Under Attack 195.135.195.195

Source umbrella

NS under Attack ns0.transip.net.



Reported by the news



Providers were again hit by DDoS attacks on Monday

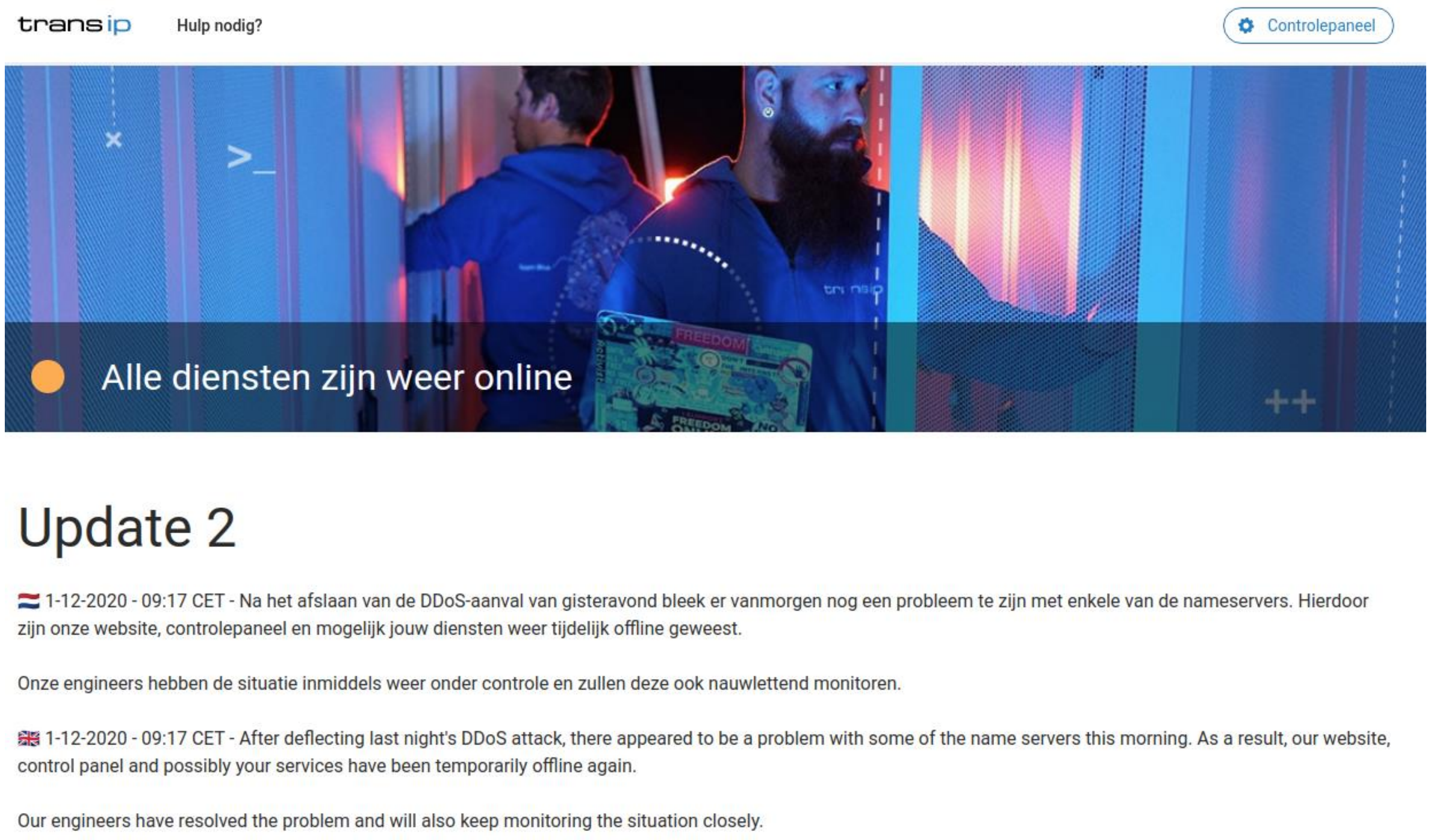
By **Tijs Hofmans**
Privacy & security editor
Feedback

01-12-2020 • 11:13

116

Once again, several providers have fallen victim to DDoS attacks. On Monday evening, Tweak and Freedom Internet were hit by an attack that sometimes reached 100Gbit/s. Hosting provider TransIP was also a victim.

Reported by the NOC



● Alle diensten zijn weer online

Update 2

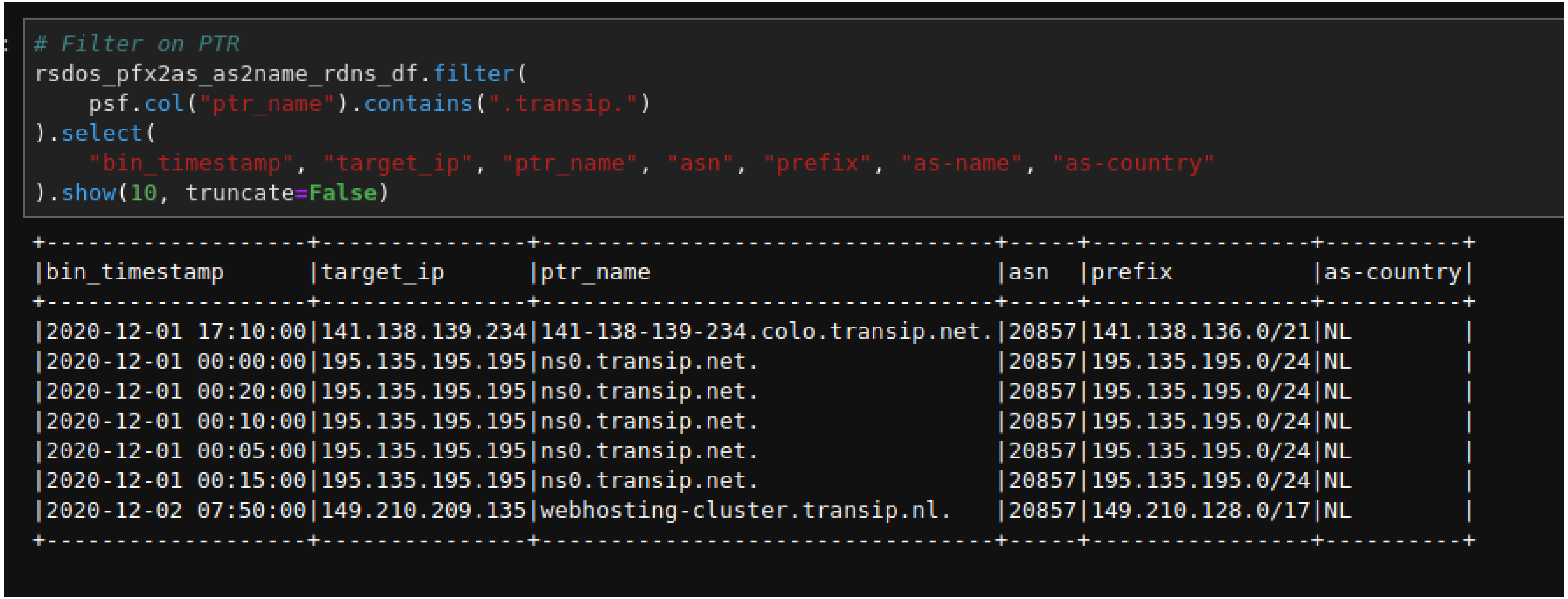
🇳🇱 1-12-2020 - 09:17 CET - Na het afslaan van de DDoS-aanval van gisteravond bleek er vanmorgen nog een probleem te zijn met enkele van de nameservers. Hierdoor zijn onze website, controlepaneel en mogelijk jouw diensten weer tijdelijk offline geweest.

Onze engineers hebben de situatie inmiddels weer onder controle en zullen deze ook nauwlettend monitoren.

🇬🇧 1-12-2020 - 09:17 CET - After deflecting last night's DDoS attack, there appeared to be a problem with some of the name servers this morning. As a result, our website, control panel and possibly your services have been temporarily offline again.

Our engineers have resolved the problem and will also keep monitoring the situation closely.

Impacts more than authoritative

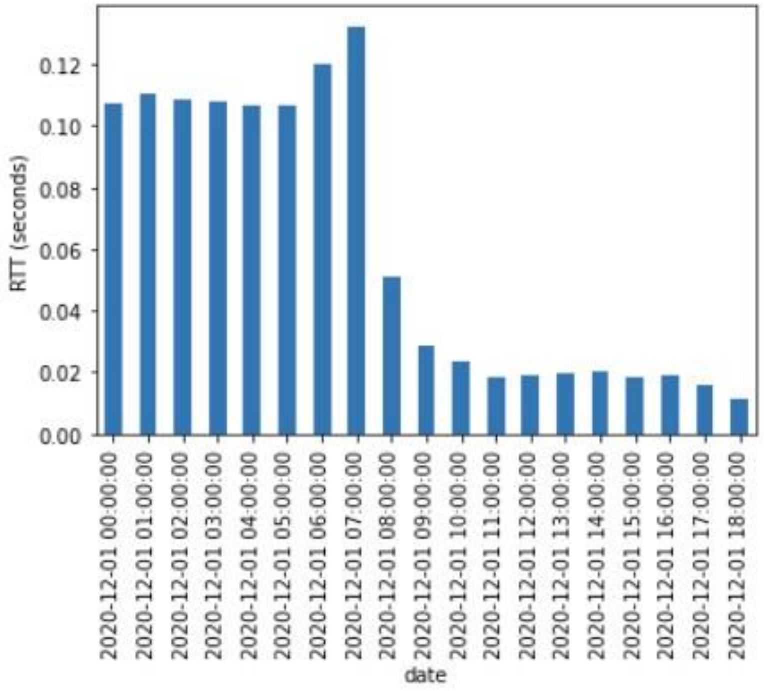


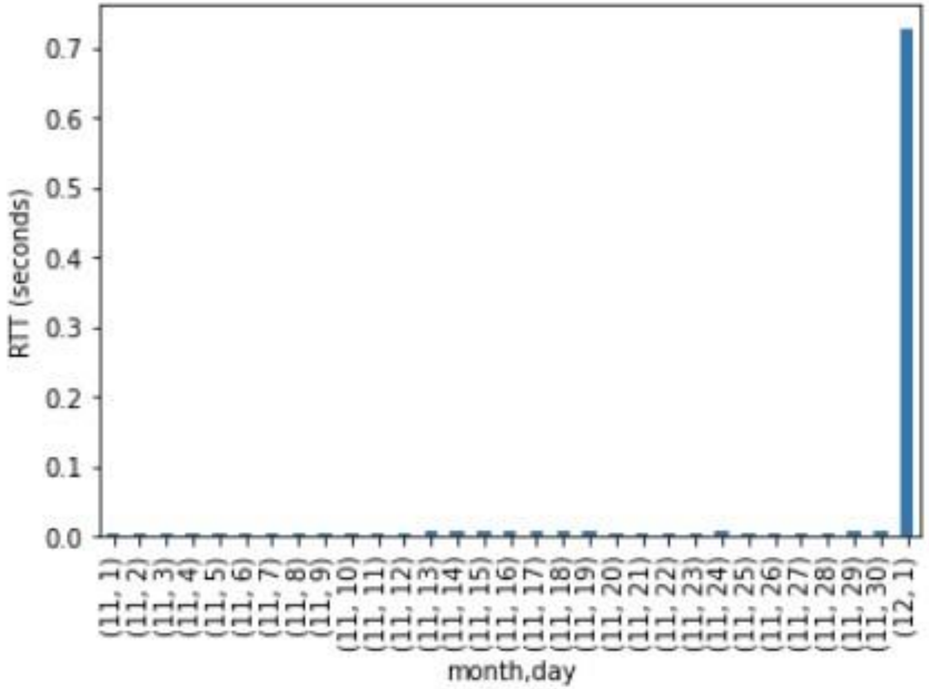
```
# Filter on PTR
rsdos_pfx2as_as2name_rdns_df.filter(
    psf.col("ptr_name").contains(".transip.")
).select(
    "bin_timestamp", "target_ip", "ptr_name", "asn", "prefix", "as-name", "as-country"
).show(10, truncate=False)
```

```
+-------------------+---------------+---------------------------------+-----+----------------+----------+
|bin_timestamp      |target_ip      |ptr_name                         |asn  |prefix          |as-country|
+-------------------+---------------+---------------------------------+-----+----------------+----------+
|2020-12-01 17:10:00|141.138.139.234|141-138-139-234.colo.transip.net.|20857|141.138.136.0/21|NL        |
|2020-12-01 00:00:00|195.135.195.195|ns0.transip.net.                 |20857|195.135.195.0/24|NL        |
|2020-12-01 00:20:00|195.135.195.195|ns0.transip.net.                 |20857|195.135.195.0/24|NL        |
|2020-12-01 00:10:00|195.135.195.195|ns0.transip.net.                 |20857|195.135.195.0/24|NL        |
|2020-12-01 00:05:00|195.135.195.195|ns0.transip.net.                 |20857|195.135.195.0/24|NL        |
|2020-12-01 00:15:00|195.135.195.195|ns0.transip.net.                 |20857|195.135.195.0/24|NL        |
|2020-12-02 07:50:00|149.210.209.135|webhosting-cluster.transip.nl.   |20857|149.210.128.0/17|NL        |
+-------------------+---------------+---------------------------------+-----+----------------+----------+
```

Postmortem Report of TransIP attack

- Average RTT for .nl TransIP SLDs measured by OpenINTEL during the attack and on the previous month.





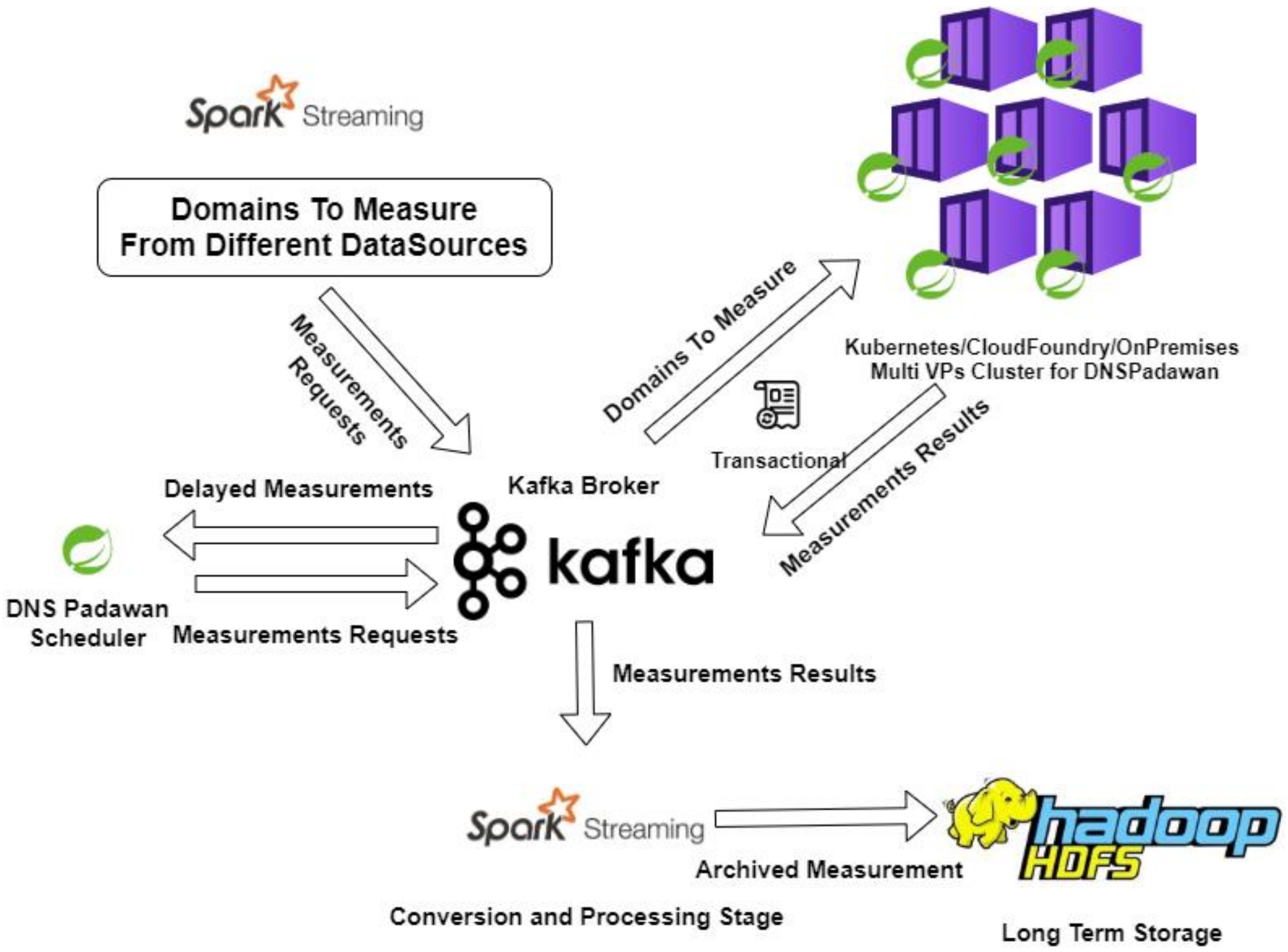
Matter of Luck?

- The TransIP case was a "lucky" case for us.
- The attacks started around midnight, that is the exact time where OpenINTEL measurements starts.
- Moreover, TransIP is a very popular Dutch registrar and our (paced) .nl measurements completes at 18:00 in the evening.
- What if attacks happens during OpenINTEL "stand-by" time or if the measurments for domains related to a nameserver under attack are already performed?

Measure -> Stream -> Analyze -> Measure

- The previous example shown not only the necessity of being able to live analyze incoming measurements to provide insights on attacks.
- Additional measurements should be scheduled an performed live in reaction to certain events (e.g., attacks, hijacks).
- For this reason, based on OpenINTEL lessons learned, we designed a reactive DNS measurement software.

Reactive Measurements



React to attacks

- Reactive measurements become fundamental when it comes to nameservers under attacks.
- Being able to measure the resolution time and the failure rate of domains with infrastructure under attack will help us to better understand the impacts.
- (Public?) live dashboard with insight on attacks for operators.
- Software to perform it is ready (in testing phase): we are currently finishing the deployment of the infrastructure.

Conclusion

- Streaming data has proven to be an effective way to detect and visualize ongoing attacks and perform research.
- With UCSD NT data and UTwente OpenINTEL data, we were able to build a system for better understanding the impact of attacks on the DNS ecosystem.
- Future research will focus on correlation between attacks characteristics provided by STARDUST and impact data collected by OpenINTEL.