DNSAttackStream

Investigating the Impact of DDoS Attacks on the DNS

Mattijs Jonker

UNIVERSITY OF TWENTE.

caida

DACS Design and Analysis of Communication Systems

NWO Netherlands Organisation for Scientific Research

U.S. DEPARTMENT OF HOMELAND SECURITY

Investigating the Impact of DDoS Attacks on the DNS

- Two data sources:
  1. DNS measurement data
  2. Indicators of DDoS attack activity

DNS measurement data

- **OpenINTEL** performs an **active** DNS measurement, sending a fixed set of queries for all covered names, **once every 24 hours**
- We do this **at scale**, covering over **236 million** domains per day:
  - **gTLDs**, **ccTLDs**, various **other** sources (e.g., Alexa)
- Notably provides:
  - Mapping between IP addresses to auth. nameserver infrastructure (A records)
  - Mappings between SLDs and auth. nameserver (NS records)

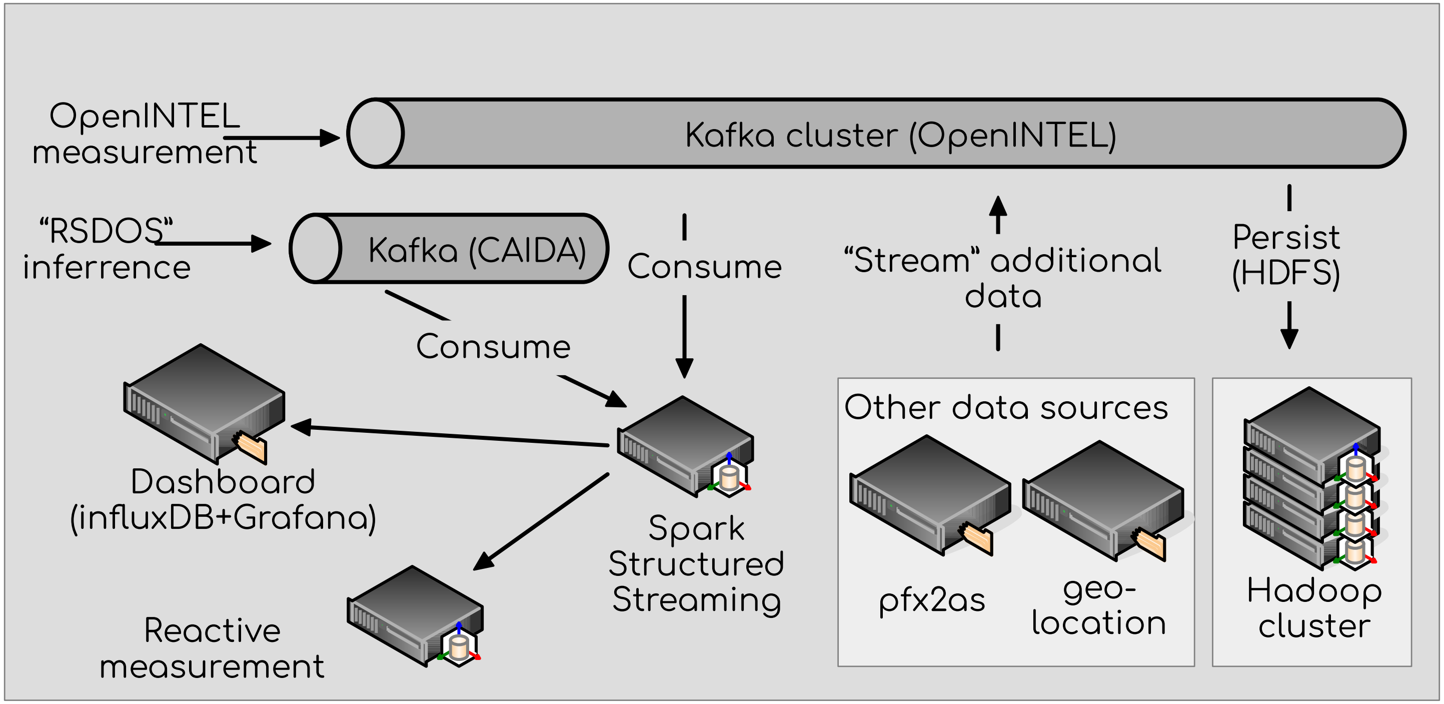
UCSD-NT

- CAIDA UCSD Network Telescope
  - Sizable IPv4 darknet
  - Receives unsolicited backscatter (from certain types of DoS attacks)
- We receive a data feed of attacks (target IP, #pkt, #byt, …)

  … and can analyze a breakdown of attack-associated “flows“ (specific ports, protocols, …)

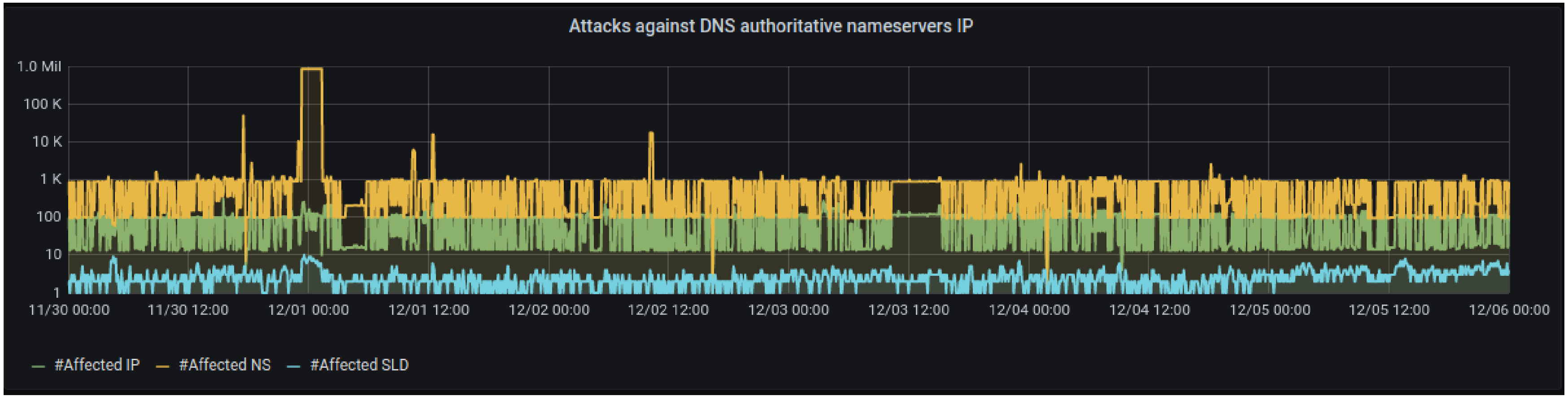
DNSAttackStream

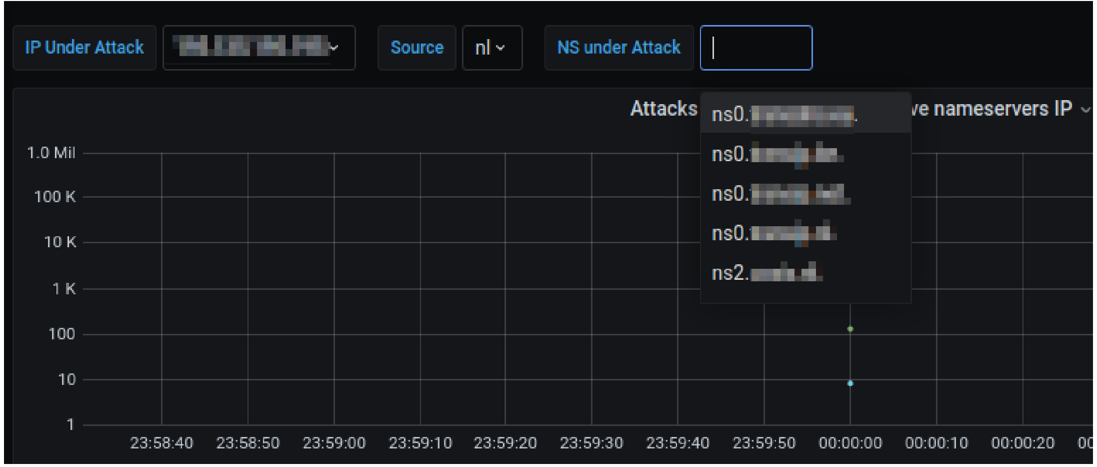
- We fuse UCSD-NT data with DNS data in near real-time
  - Yields authoritative nameservers under attack
  - Provides domain names that delegate authority to NS
  - Creates reactive measurement opportunity!



Dashboard

- Show #NS$_{IP}$, #NS$_{FQDN}$, and #SLDs (that delegate to NS) affected by attacks
- Dec ‘20 peak reveals attack on large registrar in the Netherlands (multiple of its nameservers attacked)





IP Under Attack [redacted]

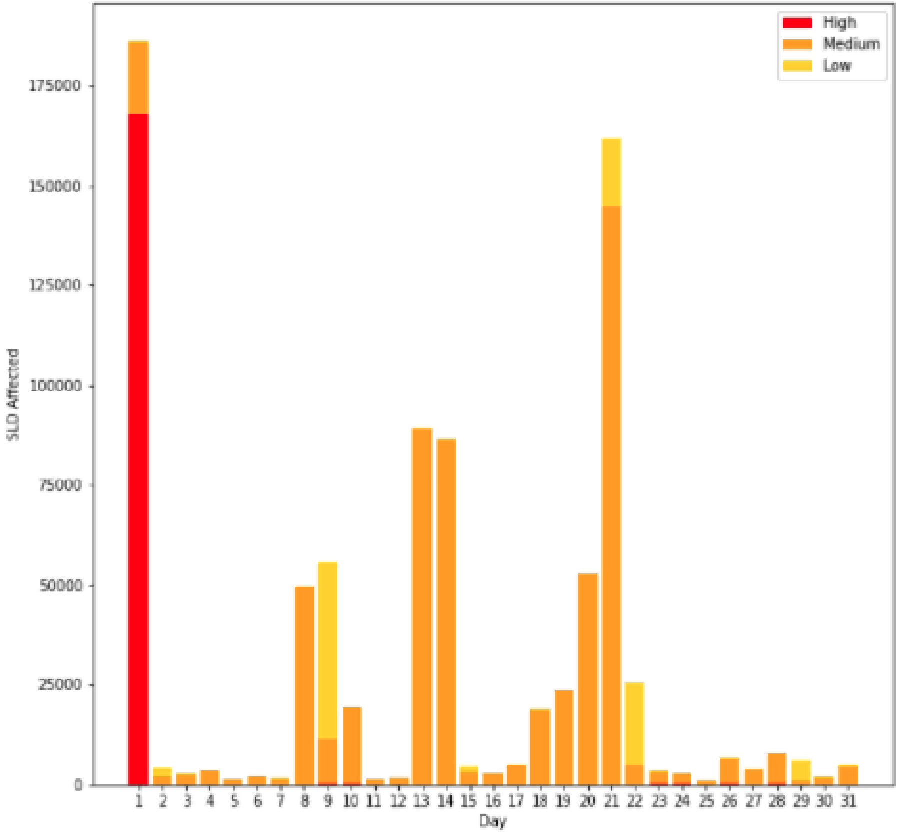
Source nl

NS under Attack

ns0.[redacted]
ns0.[redacted]
ns0.[redacted]
ns0.[redacted]
ns2.[redacted]

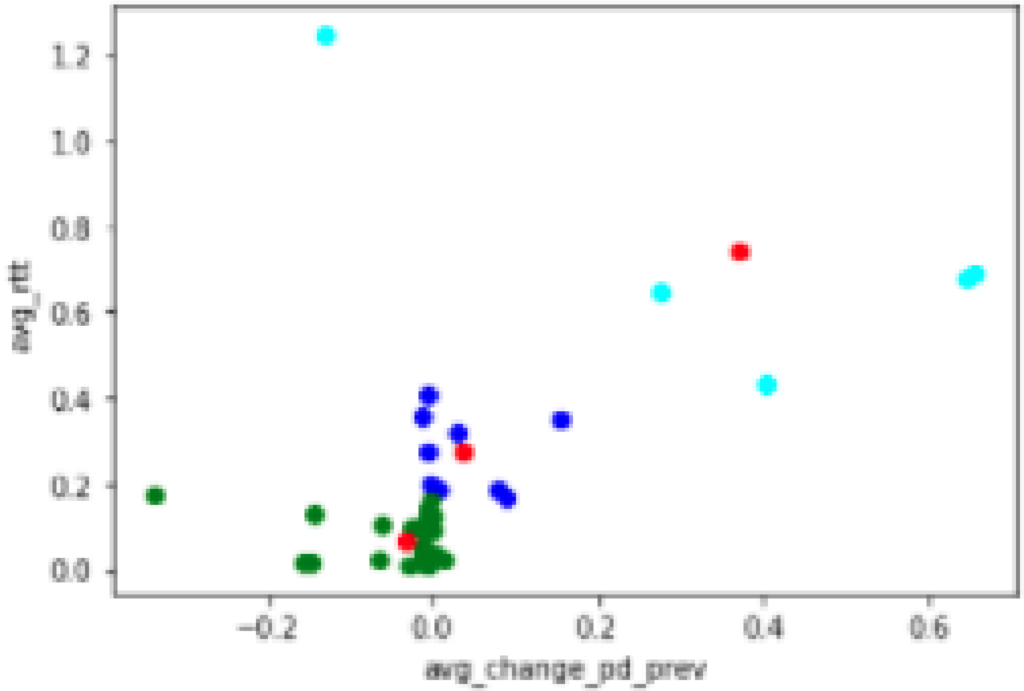
Affected domain names (potentially)

- Take SLDs that delegate authority to NS under attack
- Use RSDOS metrics (pps rate + IP count) to assign attack intensity *{low,medium,high}*
- Dec 1 attack of the high category



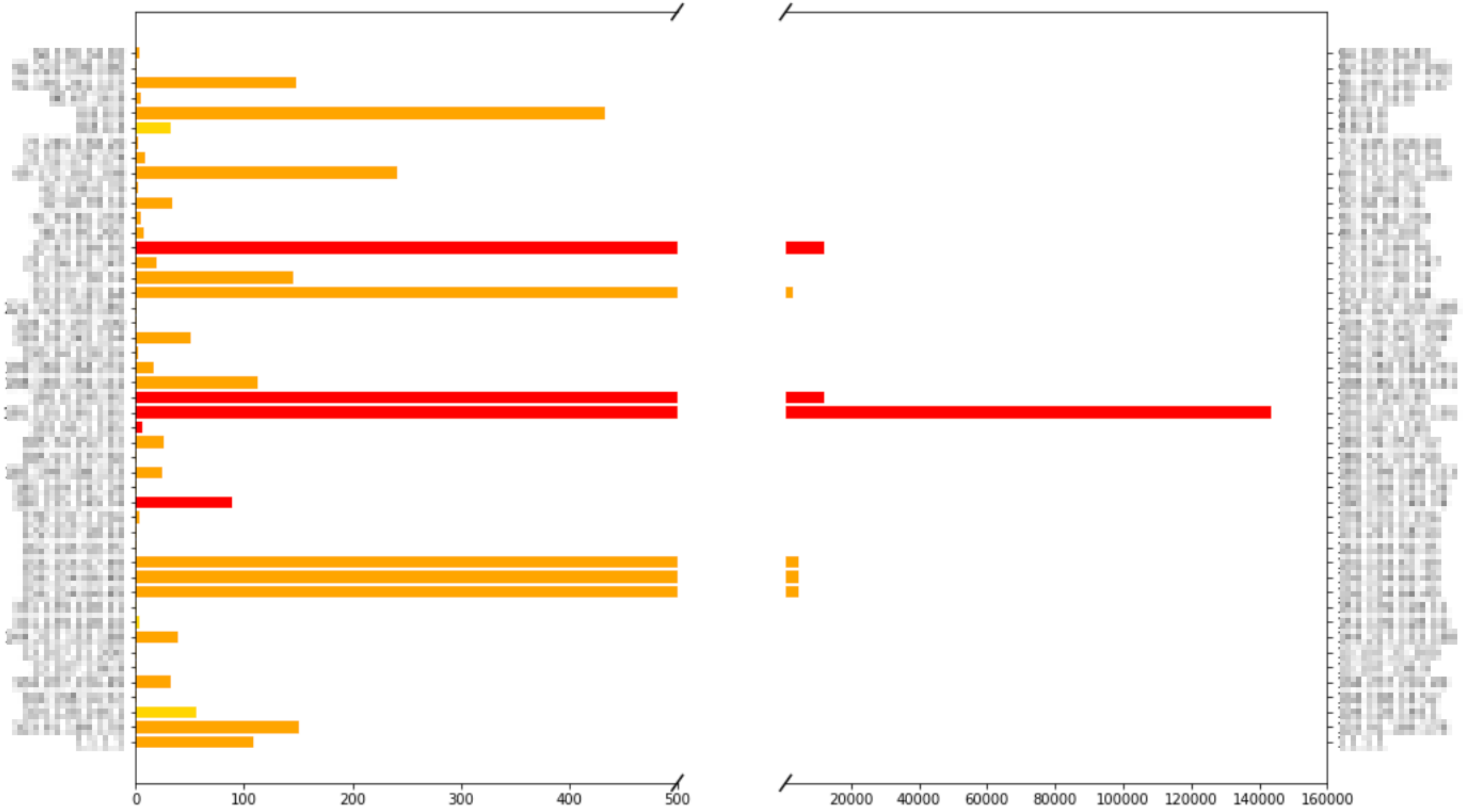
Impact assessment 1/2

- High-intensity attack, but did it have an effect on the DNS?
- We store the RTT of DNS RR resolutions
- Create metrics on day of (and adjacent to) attack (e.g., avg_rtt)
- Use PCA to identify features that explain max variance
- Use k-Means (k=3) to cluster into {low,medium,high} impact on DNS operation



Impact assessment 2/2

- #SLDs per attacked NS, with impact intensity
- DNS resolution for SLDs that delegate to various NS of the registrar under attack was adversely affected



Work in progress

- Cross-reference attack breakdown (flows) with Rapid7 data to see if ports were open/in use on/near date of attack
- **Reactive measurements** to improve attack impact assessment (closer to moment of attack)
- Fuse with **other indicators** of attack activity (e.g., reflection & amplification attacks from honeypot data)

Questions
?