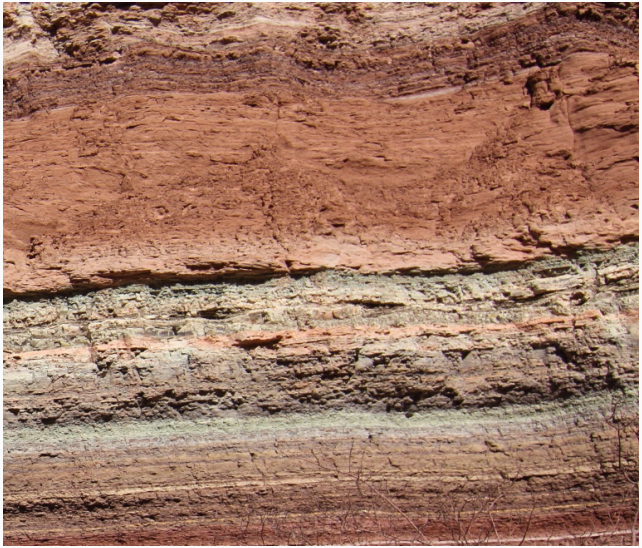
OpenIntel: a user' perspective

Giovane C. M. Moura

Platform Internetstandaarden

2020-09-10

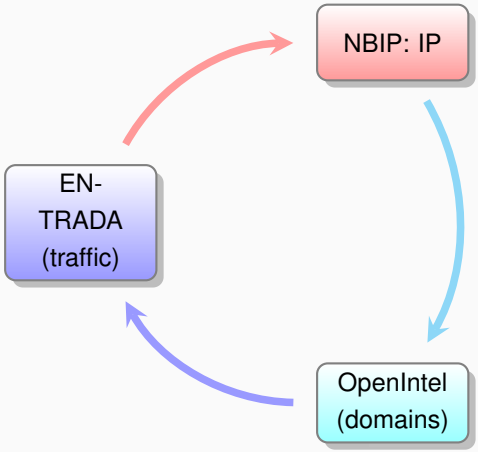
What's OpenIntel for me: *stratum*



SDN LABS

The Power of Combining Datasets

- Study between SIDN Labs and NBIP (NaWas)
- DDoS metadata → target IP addresses
- OpenIntel: what does were on these IPs?
- ENTRADA (DNS traffic): what was the DNS traffic like?
- Paper: https://tinyurl.com/y5yothlf



Shared hosting: 1 IP $\rightarrow$ 6 domains

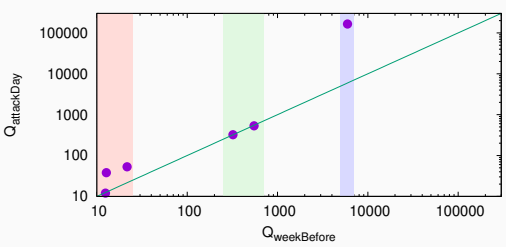


Figure 1: Shared hosting: 6 `.nl` domains, 1 targeted domain

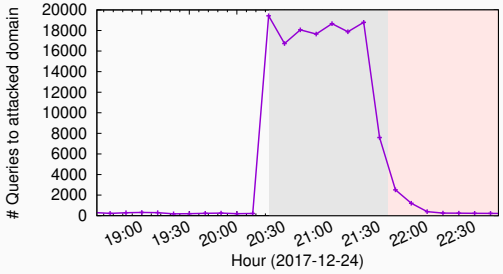


Figure 2: Timeseries of queries to targed domain from Fig. 1.

5 domains likely suffered alongside this targeted domain

Shared hosting: 1 IP $\rightarrow$ 6 domains

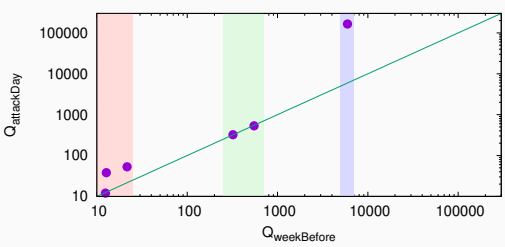


Figure 1: Shared hosting: 6 `.nl` domains, 1 targeted domain

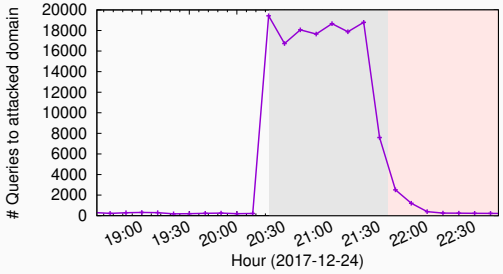


Figure 2: Timeseries of queries to targed domain from Fig. 1.

5 domains likely suffered alongside this targeted domain

OpenIntel keeps the memory of DNS

- By keeping historical data, it allow us to combine a series of datasets
- Like pieces in a puzzle to have a clear picture