Open INTEL

Creating a "long-term memory" for the global DNS

UNIVERSITY OF TWENTE.

SURF NET

SIDN LABS

NLNET LABS

Introduction

- More than **five years ago**, we started with **an idea**:

  "Can we measure (large parts of) the global DNS on a daily basis?"

Why measure the DNS?

- **DNS translates** from the **human** world **to** the **machine** world (and also helps in machine-to-machine interaction)

- (Almost) **every networked service relies on the DNS**

- Consequently, **measuring what is in the DNS** tells a story about the **evolution of the Internet** and its protocols

How we measure

- **OpenINTEL performs** an **active measurement**, sending a fixed set of queries for all covered domains **once every 24 hours**

- We do this **at scale**, covering **over 226 million domains** per day:
  - **gTLDs:**
    .com, .net, .org, .info, .mobi, .aero, .asia, .name, .biz, .gov
    + almost 1200 "new" gTLDs (.xxx, .xyz, .amsterdam, .berlin, ...)
  - **ccTLDs:**
    .nl, .se, .nu, .ca, .fi, .at, .dk, .ru, .рф, .us, .na, .gt, .ee, .ch, .li
   **<your ccTLD here?>**

Security research

- Snowshoe spam:

  - We implemented a machine-learning based system to detect domains set up for snowshoe spam before they were abused

  - **Challenge: Who do we notify and how?**

- COVID19:

  - ICANN Research Team provided a list of COVID-related keywords linked to abuse

  - We provided information on domains matching these keywords and DNS configurations

  - **Challenge: What to do with the outcome? We are not a player in the ecosystem as academics but we do care about Internet security. What role can we play?**

Example: COVID/corona
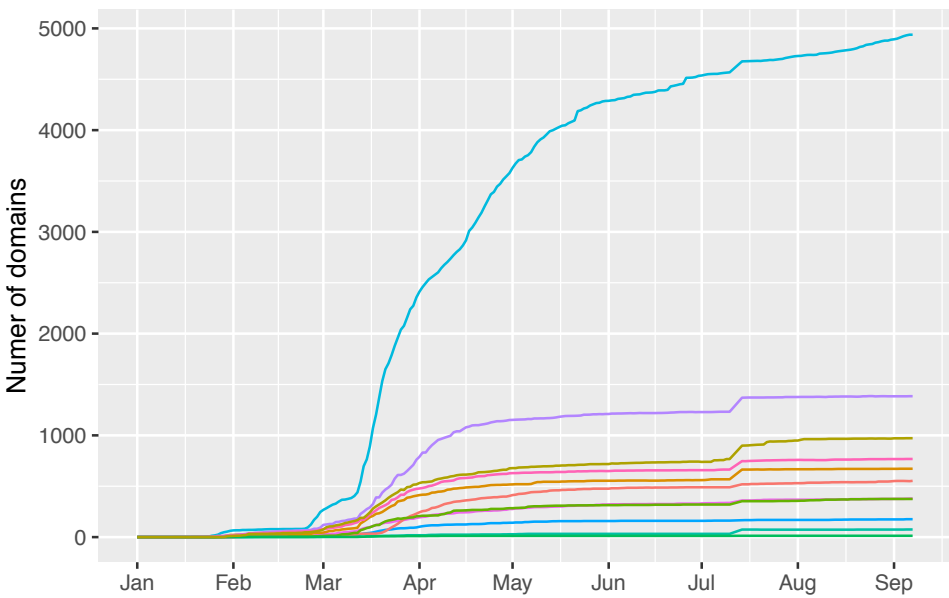
"corona"
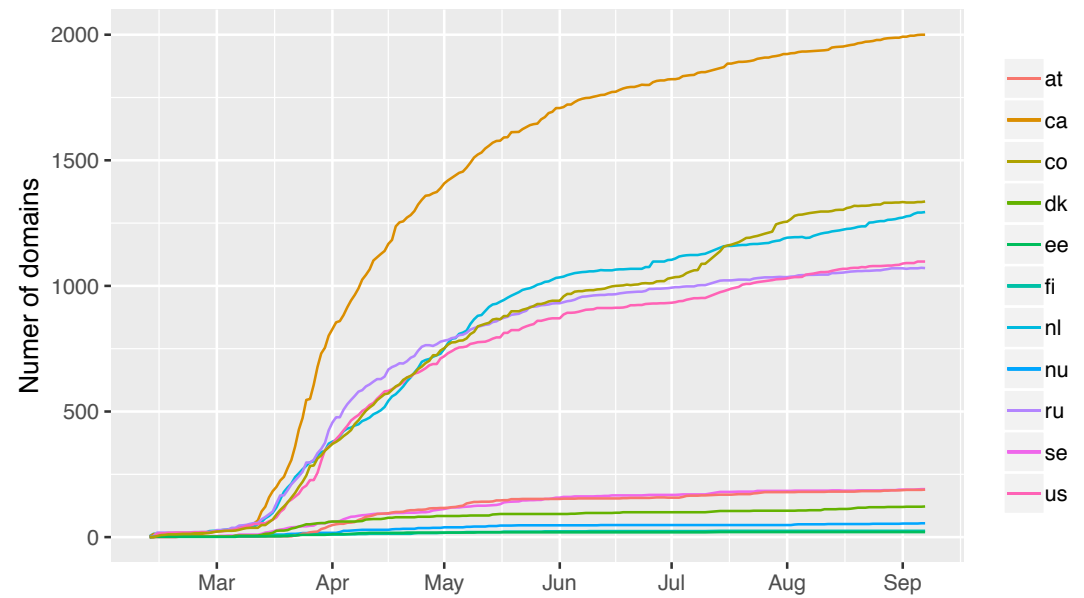
"covid"

Position statements

- We need a coordinated vulnerability disclosure process for academics to registries.

- We are academic researchers and don't want to take the role of law enforcement or incident response, how do we find a balance?

- How do we coordinate research efforts between the security and academic community in immediate emergencies like corona/COVID19?