

SIDEKICK

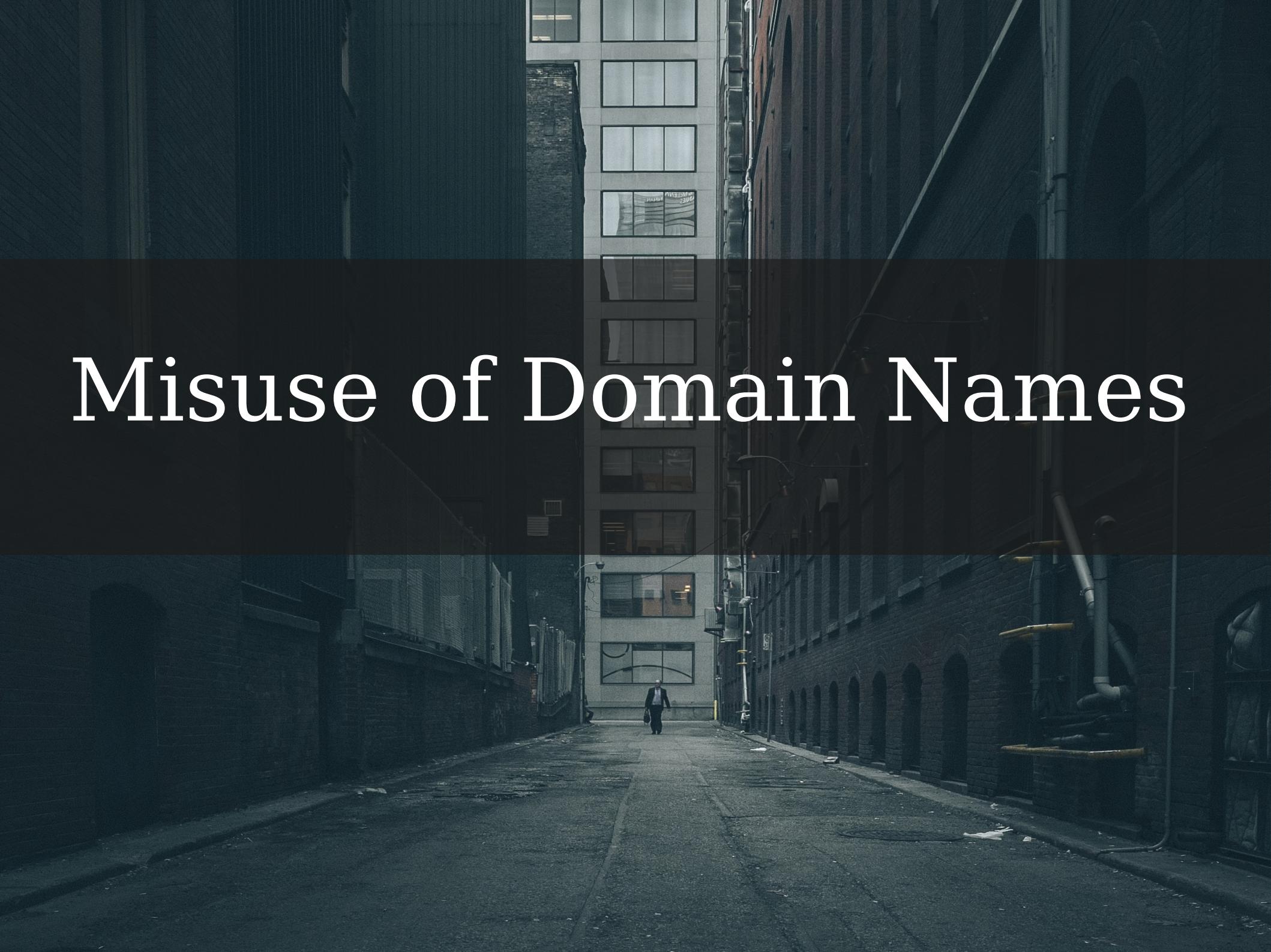
Suspicious Domain Classification

Master Thesis
at SIDN
by Moritz Mueller

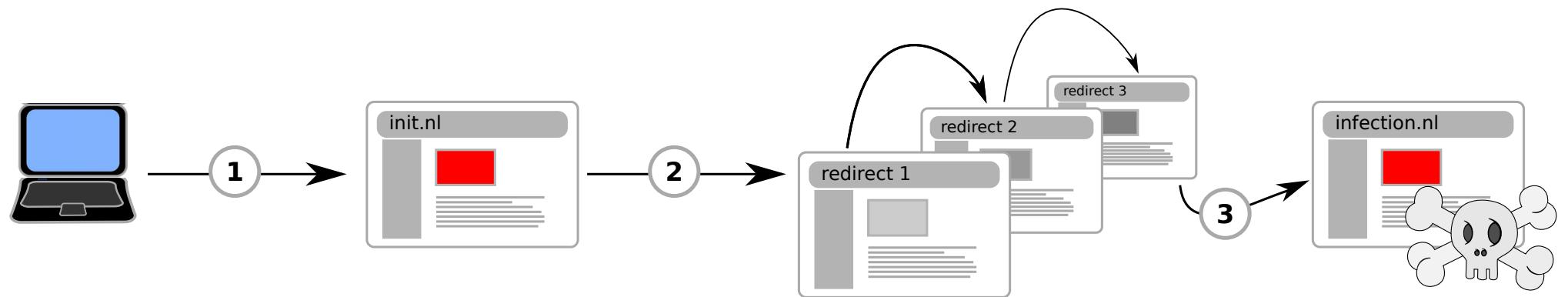
Agenda

- Misuse of Domain Names
- Malicious domains in .nl
- Malicious Domain Characteristics
- What does SIDEKICK do?
- Outlook

Misuse of Domain Names

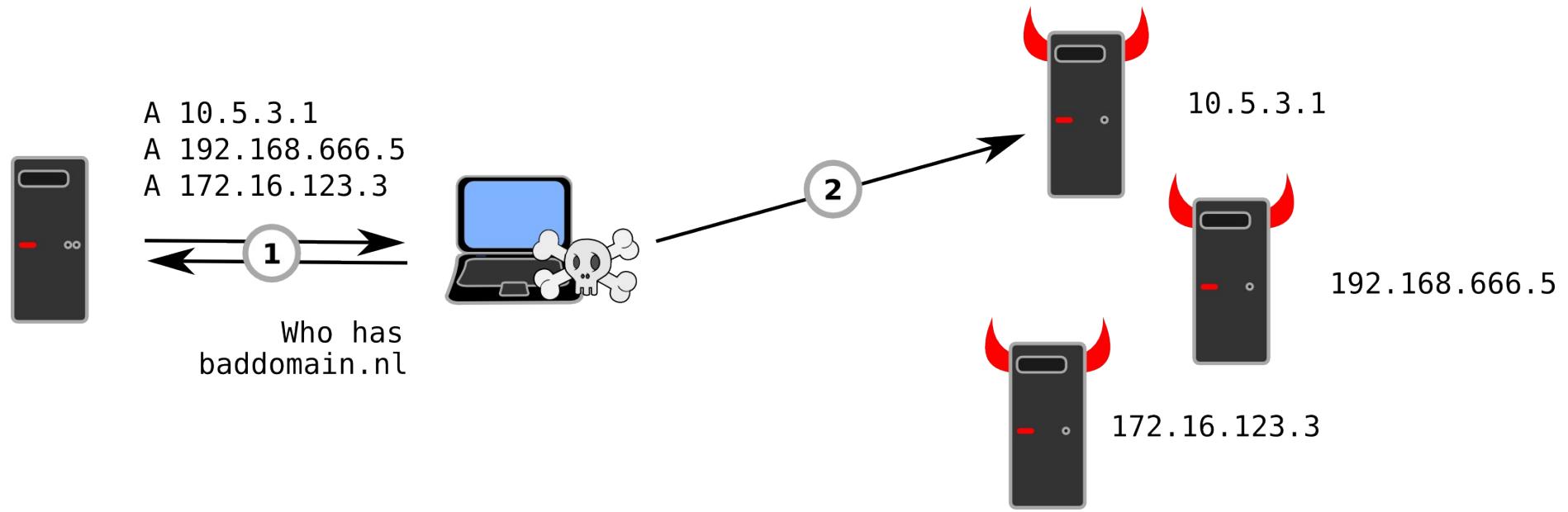
The background of the slide is a dark, moody photograph of an urban environment. In the center, there is a modern building with large windows, some of which have a grid pattern. To the right, a brick wall with arched windows is visible, along with pipes and a drain. A man in a suit walks away from the camera down a paved path between the buildings. The overall tone is somber and mysterious.

Redirection, Exploitation, Infection



Exploit Kit Infection Chain

Command and Control



C&C Address Resolution and Communication

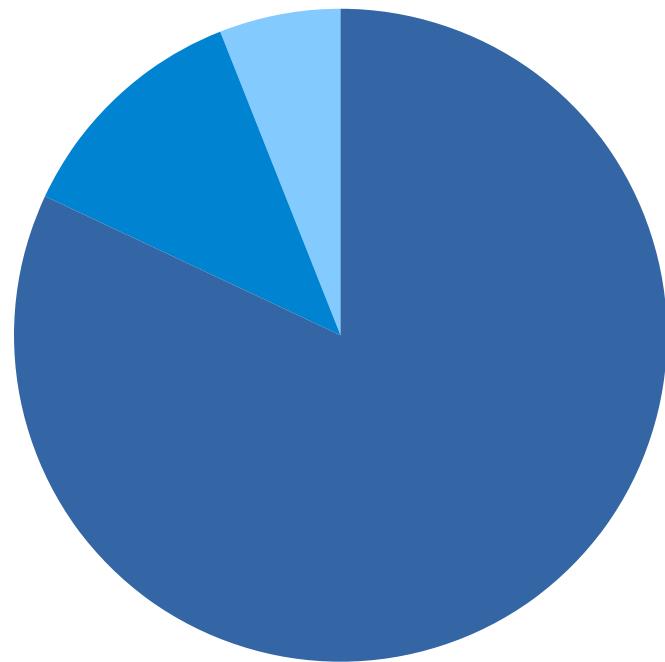
Motivation for SIDN

TRUST

REPUTATION

OVERAL INTERNET SECURITY

Phishing

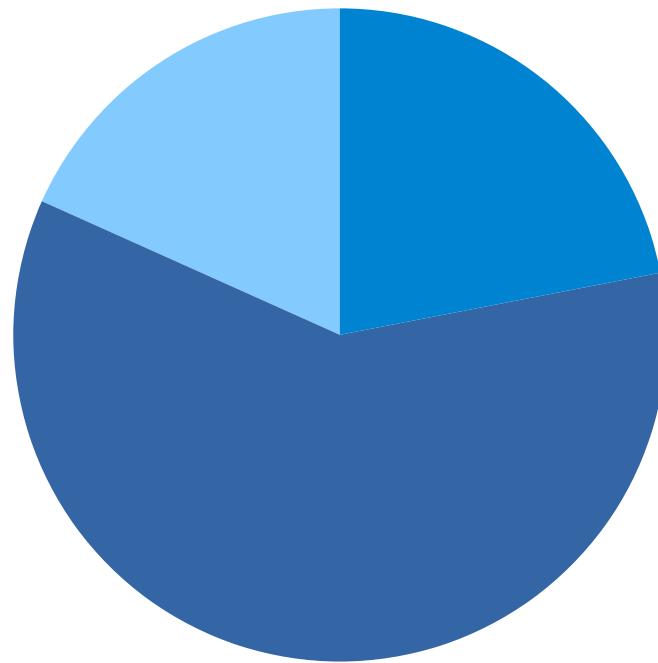


1.923 domains

- one week or younger
- between one week and one year
- one year or older

Age of .nl phishing domains

Botnets



82 domains

■ Sinkhole

■ Other Sources

■ Quarantainenet

Known Botnet Domains

The background image shows a multi-story building with a grey and white tiled facade. Numerous windows are visible, most with dark frames and light-colored curtains. One window, located on the second floor of the rightmost section, has a bright orange frame and matching horizontal bars across its middle, drawing attention to it.

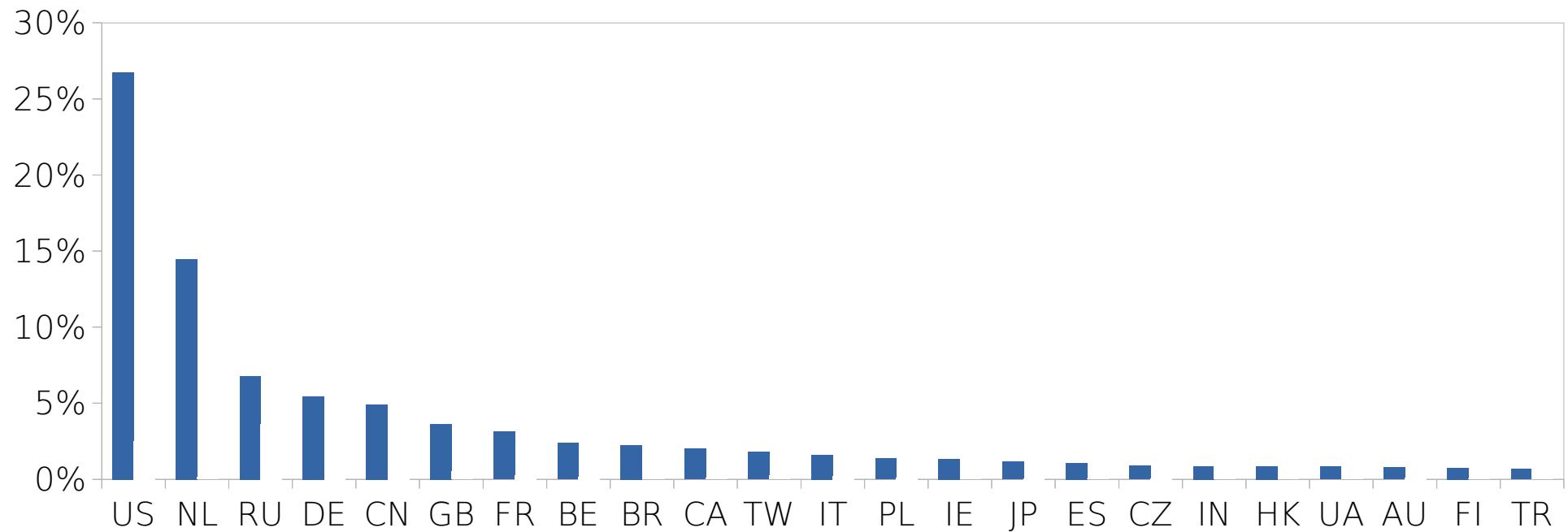
Malicious Domain Characteristics

Geographic Characteristics

95,5 % Dutch registrants

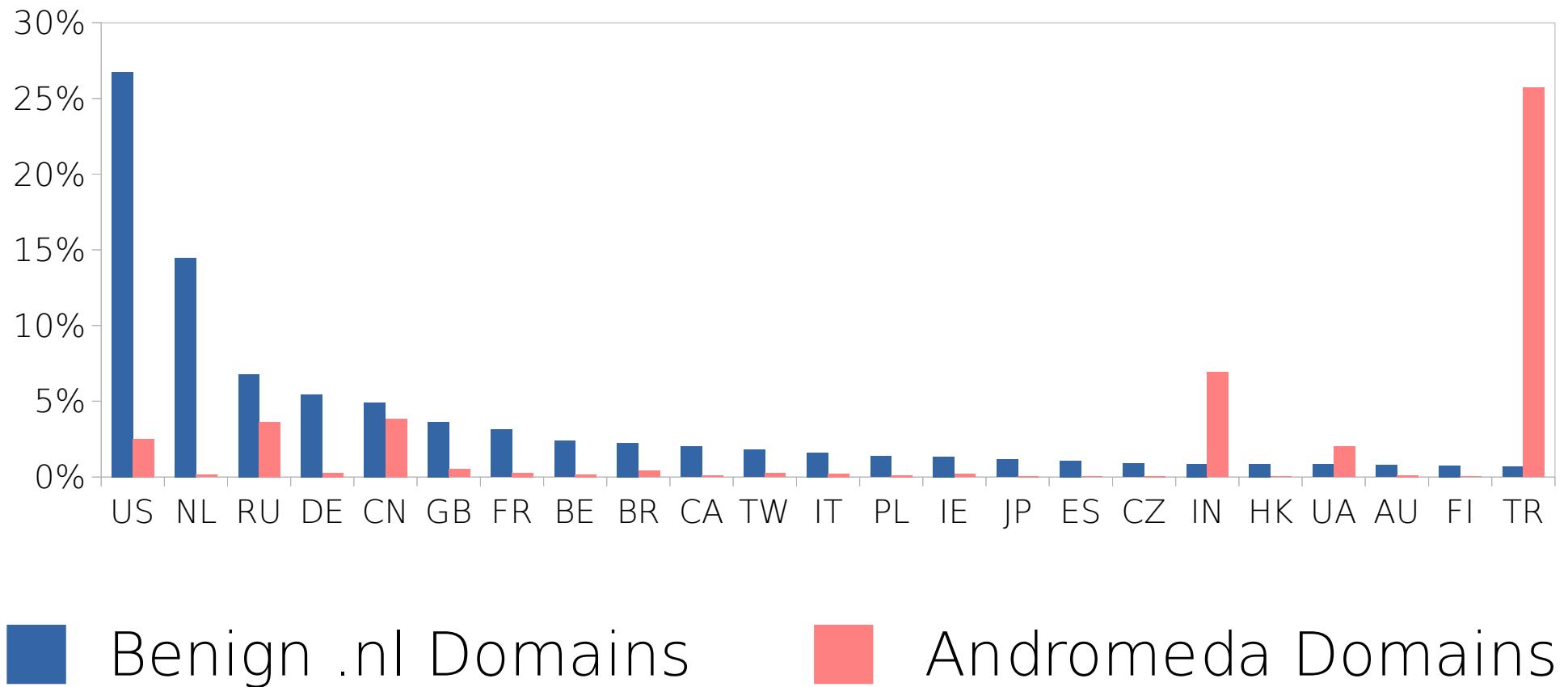
88,5 % Dutch content

Query Origin

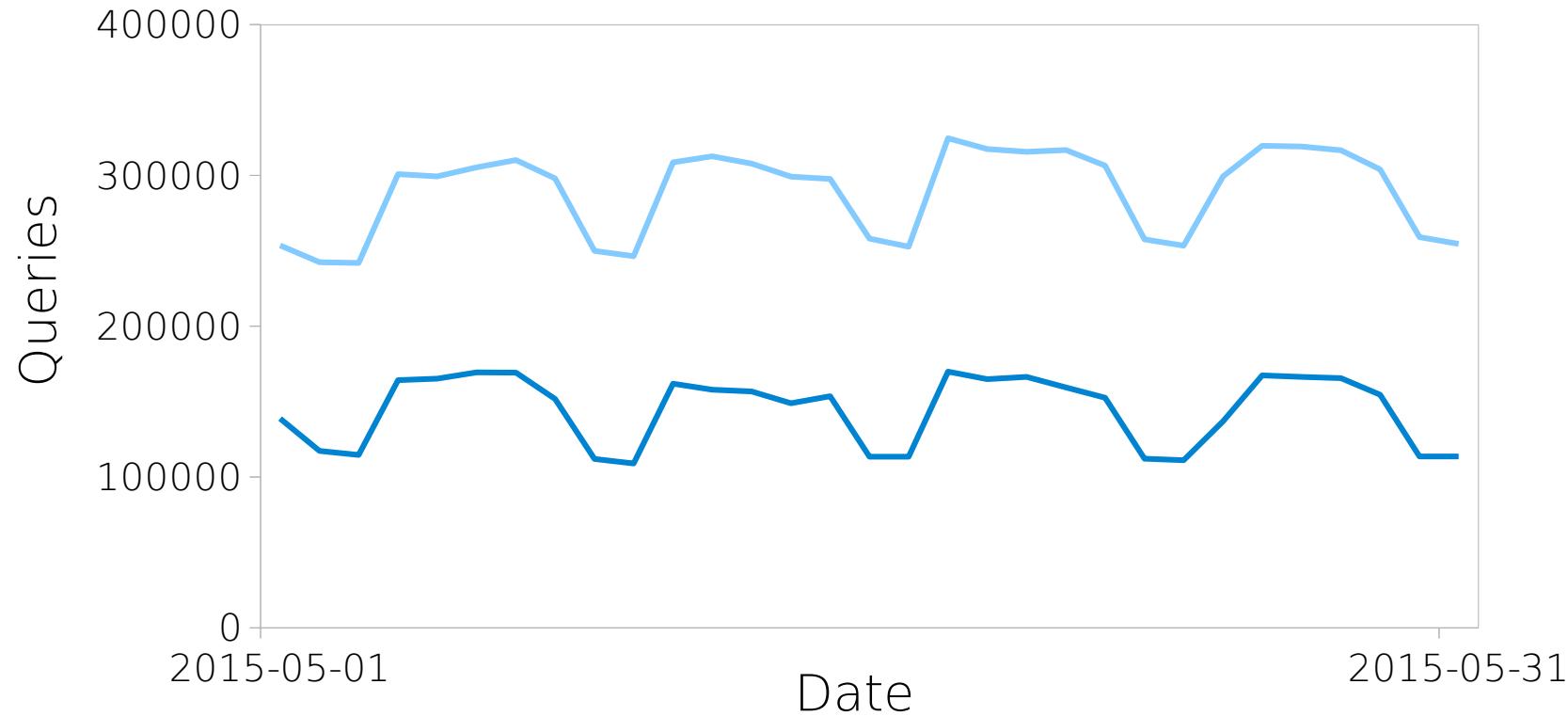


■ Benign .nl Domains

Query Origin

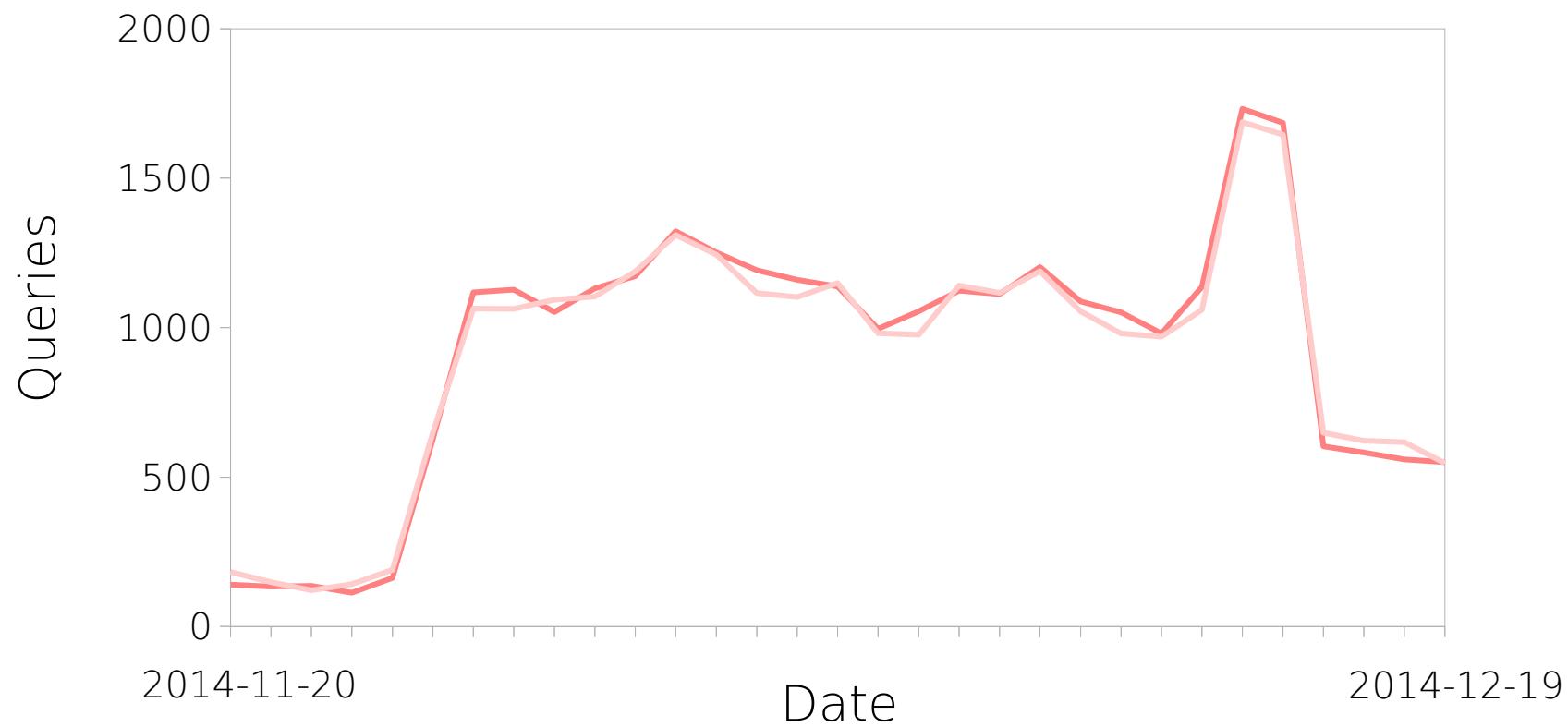


Query Frequency



Popular .nl domains

Query Frequency



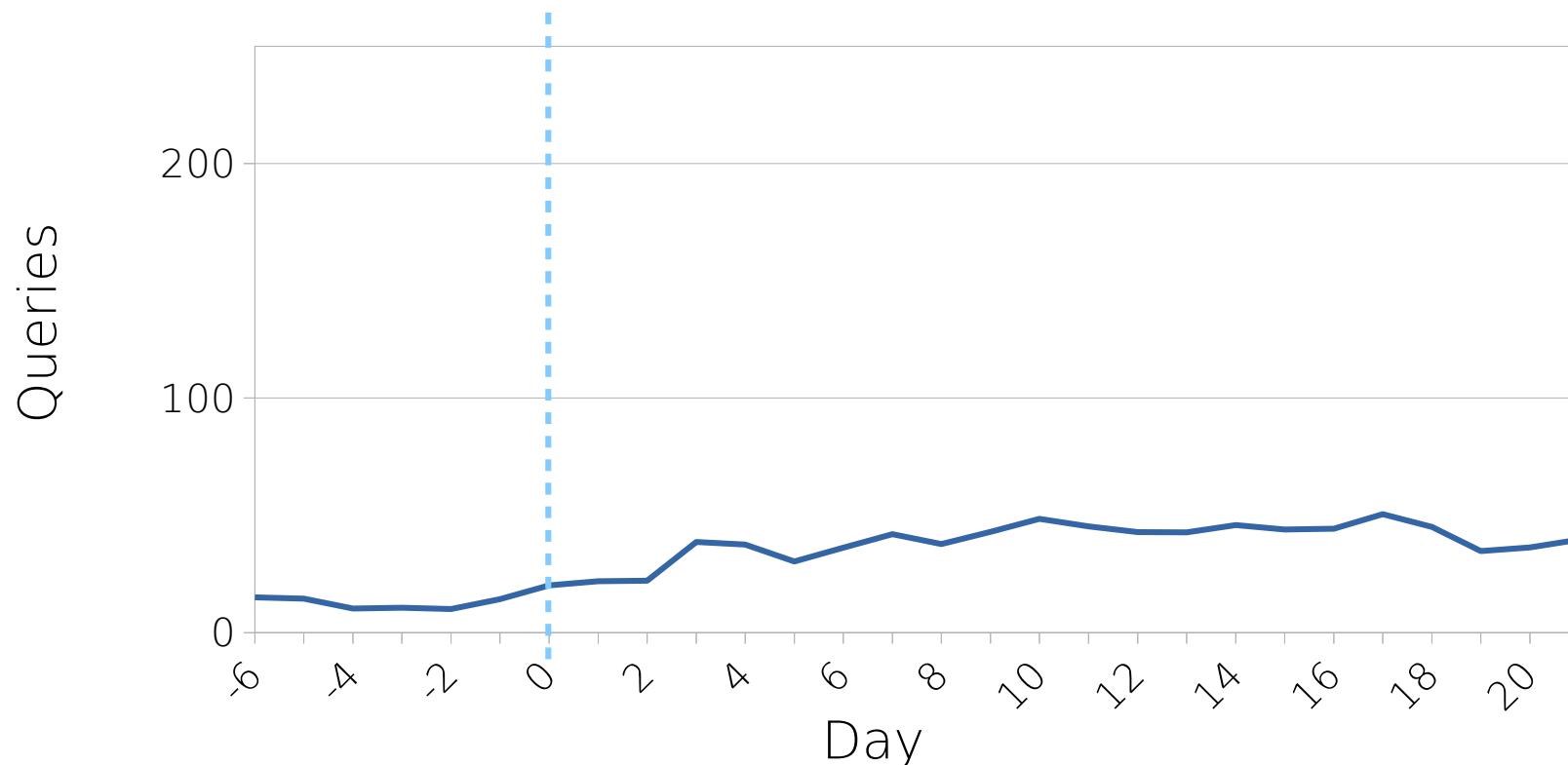
Flashback-Botnet domains

Query Frequency



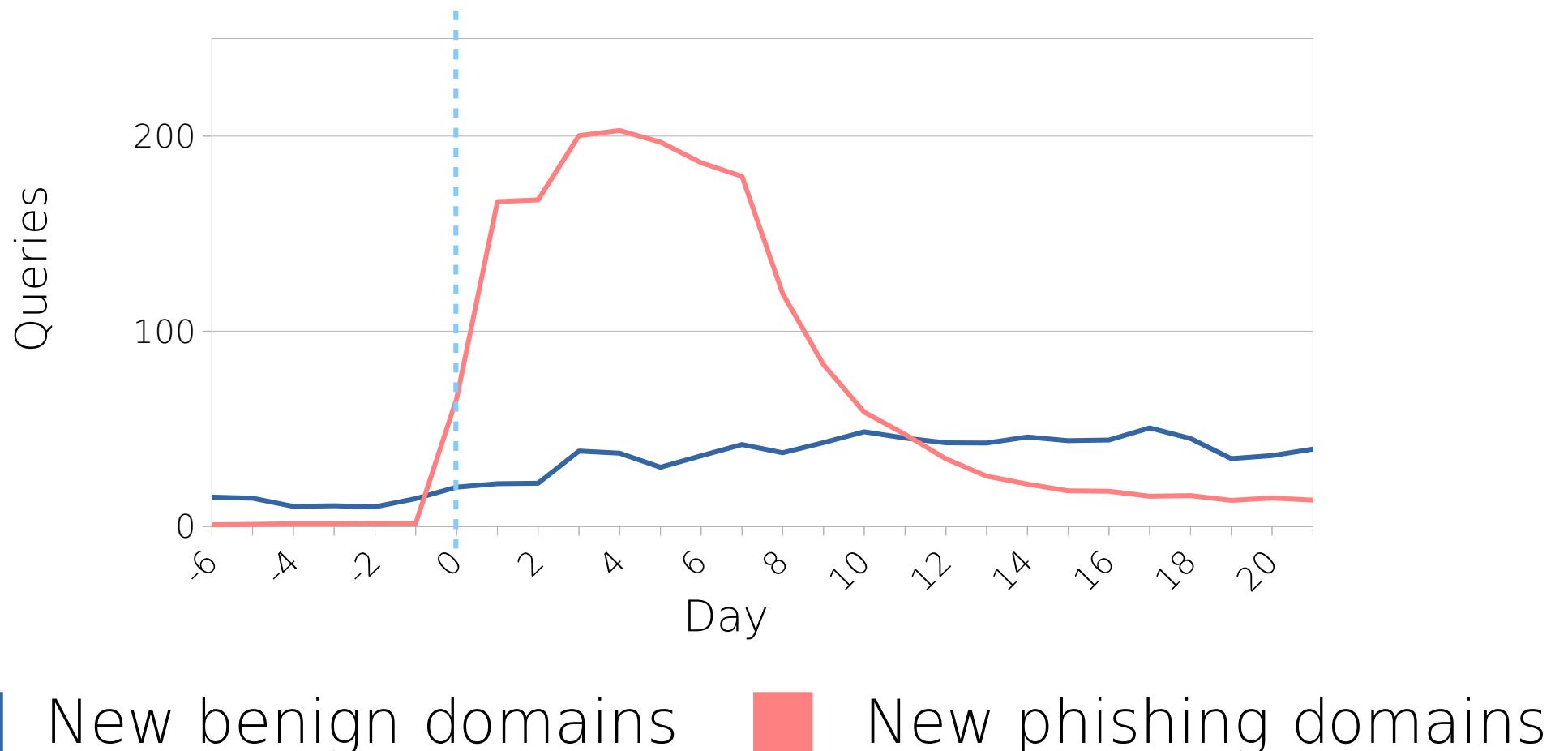
Unpopular .nl domains

Query Frequency



New benign domains

Query Frequency

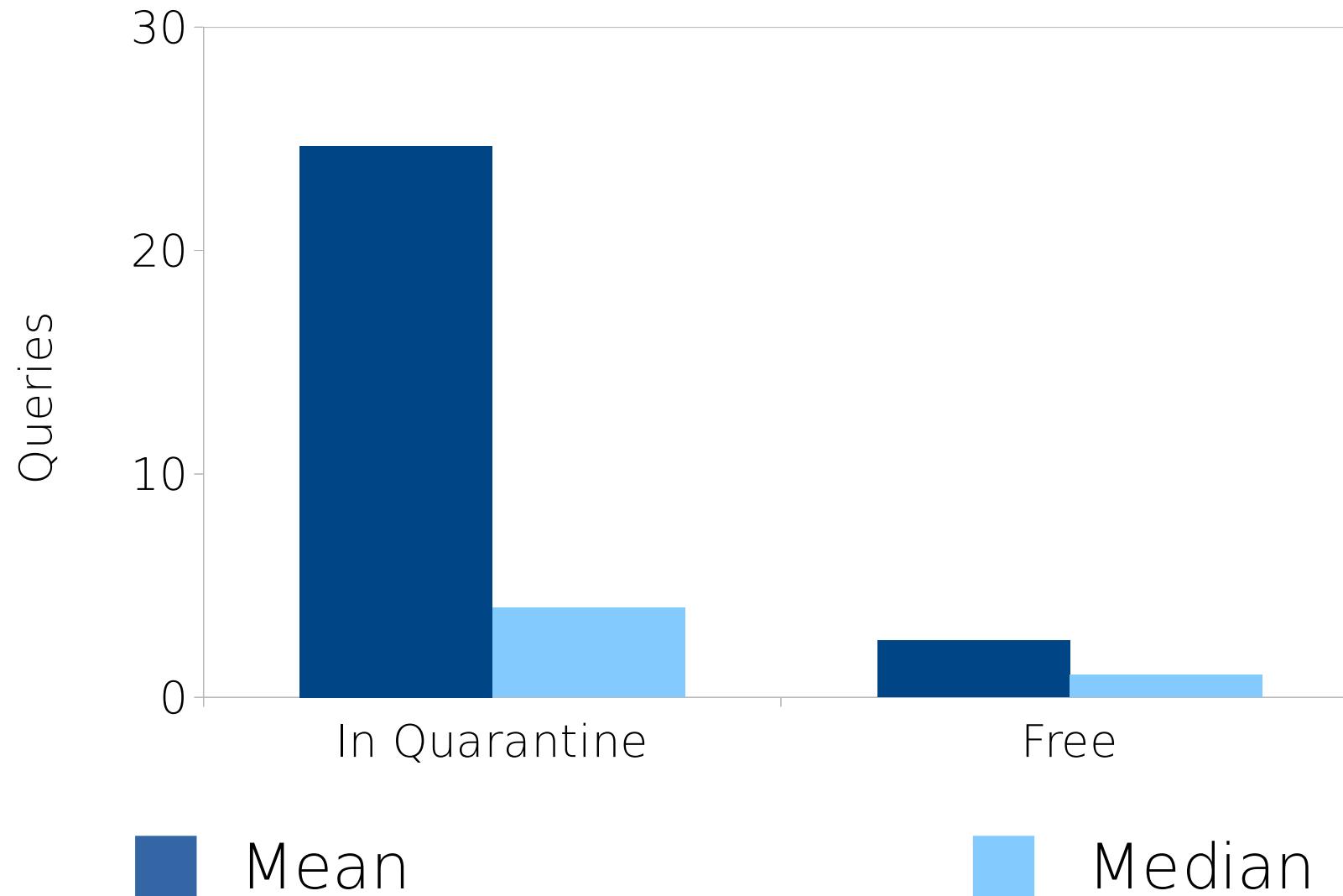


New benign domains



New phishing domains

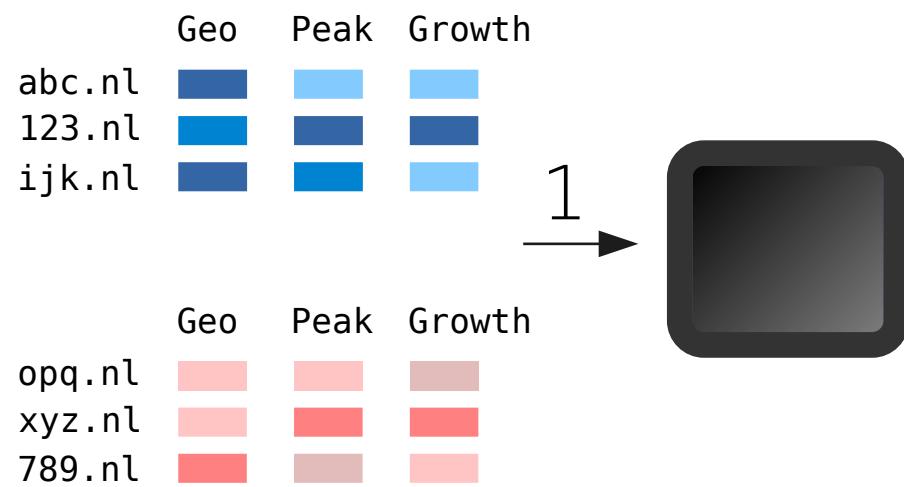
Domains in Quarantine



Catching Bad Domains With SIDEKICK

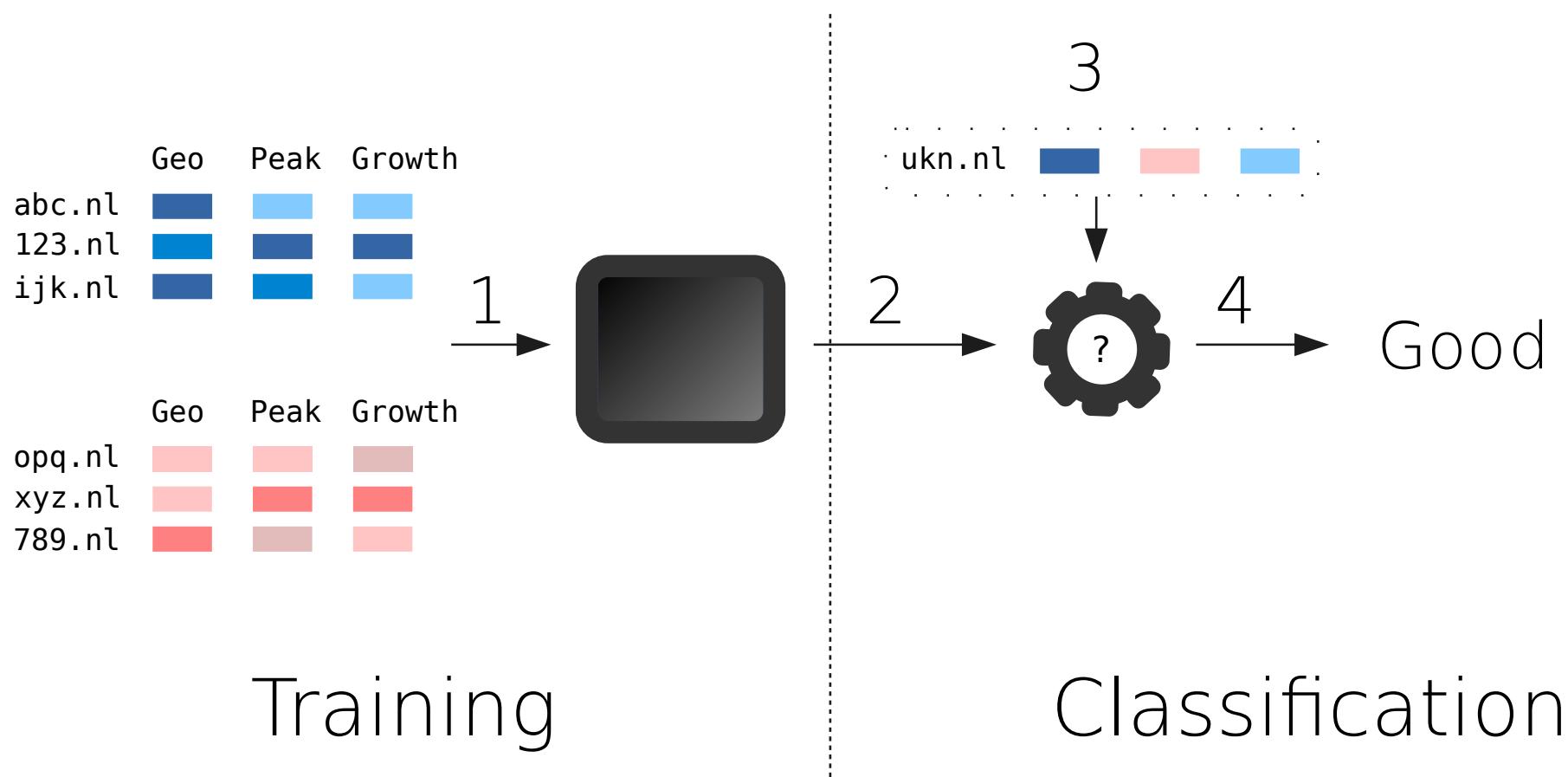


General Approach



Training

General Approach



SIDEKICK Architecture

New Domains

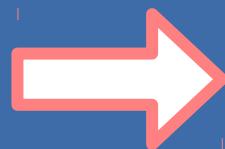
- 61.000 Domains classified
- 33 Malicious domains detected
- False Positive Rate 0,3 %

More domains detected than by
professional Phishing Feed

SIDEKICK Architecture

Old Domains

- 1,7 Million Domains Classified
- 14.000 Malicious domains detected



Can't verify suspicious domains



Next Steps

Improvements

- Early Detection
- Additional Features
 - Non-DNS-related sources (Social Media, Search Engines, CMS and Webserver)
 - EDNS Client Subnet Extension
 - Resolver Reputation

Outlook

- Post Detection
 - Block Content
 - Google Safe Browsing, Netcraft
 - Notify (Registrant, Registrar, Web-Hosting-Firm)
- Post Suspicion
 - Cooperation

SIDEKICK

- Based on geographic location and query patterns
- Effective detection of new domains
- Detection of suspicious compromised domains

Thank You For
Your Attention

