

# Phishing detection using various parts of the DNS ecosystem

Piotr Białczak

Michał Hałoń

TLP:CLEAR

## Who we are

# NASK

National Research  
Institute

Runs .pl DNS registry

Hosts CERT POLSKA

# CERT.PL >

**NASK**

Polish National CSIRT  
Securing Polish internet

# Most common threats

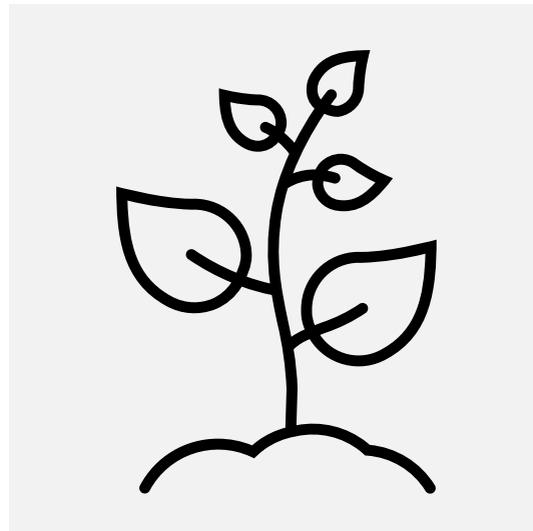
**phishing + fraud**

**98 000 incidents in 2024**

**= 95% total**



# Using DNS to protect our constituency



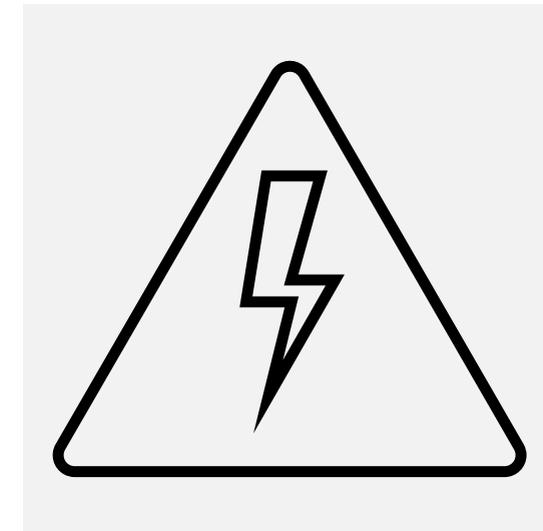
**Block domains at the  
.pl registry**

**Proof required**



**Block domains at  
resolvers**

**Proof required**



**Block domains at  
resolvers**

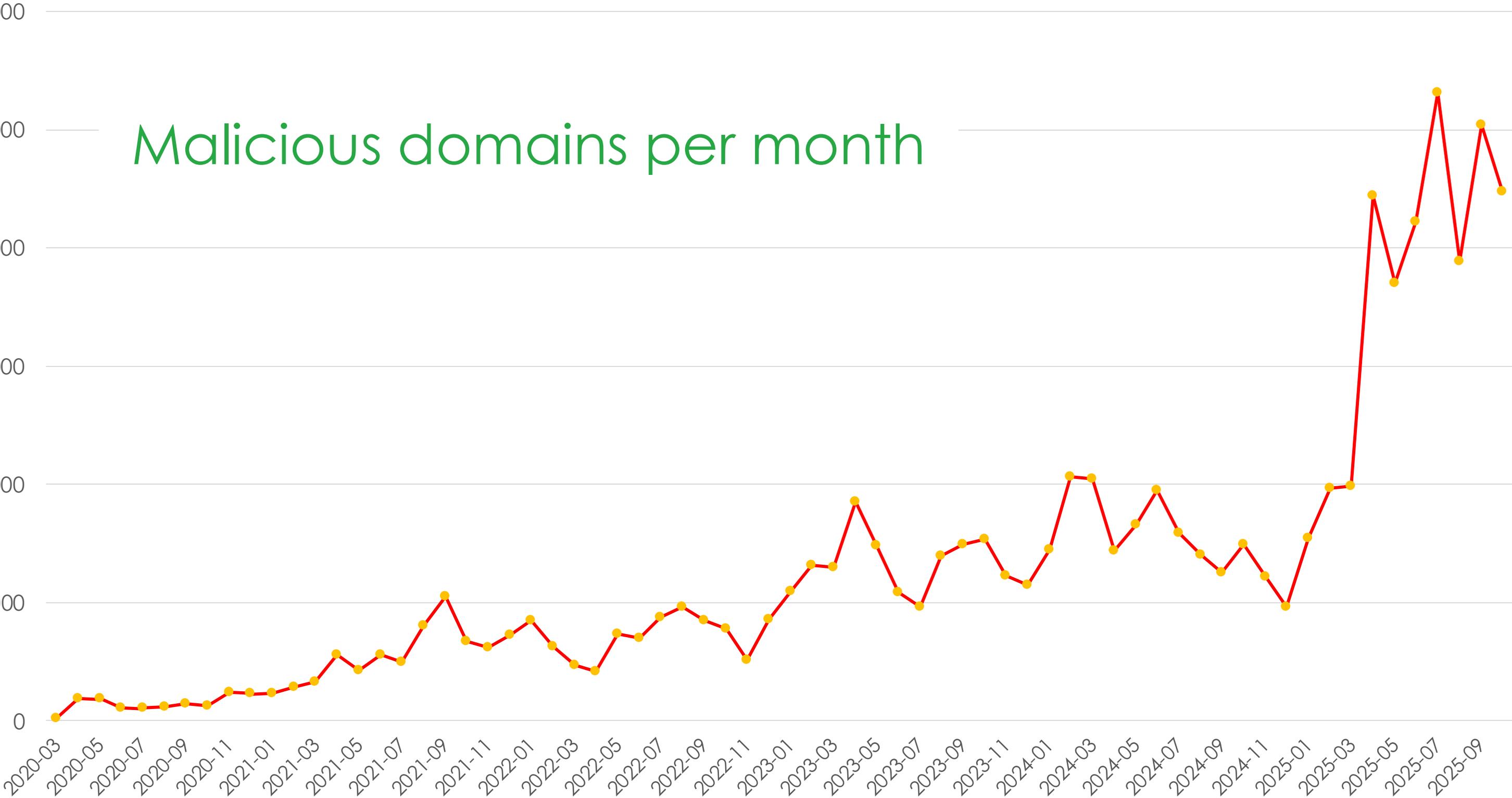
**If likely malicious**

# Country-level DNS firewall

- Launch: March 2020
- We provide a feed of malicious domains: "Warning List"
- Manually verified
- Updated 24/7
- Data is public
- Blocking is voluntary
- Used by all big Polish telcos



# Malicious domains per month



# How to identify malicious domains?

1. URLs reported by users (multiple channels)
2. Hunting (CT, pDNS, registry data, etc)
3. ML-powered hunting = main topic of this talk!

# DNS4EU project

Project number: 101095329 21-EU-DIG-EU-DNS  
Project name: DNS4EU and European DNS Shield.  
This project is co-funded by the European Union.



Co-funded by  
the European Union

# Goals of the European Commission

1. Offer a high-end **alternative to existing dominant non-EU public resolvers**, leading to a more resilient, more secure and diversified DNS resolution offering for EU internet users.
2. **Autonomy** of DNS resolving, diminishing the dependency on major public resolvers established outside the EU, and reducing vulnerability to outages of these resolvers.
3. Complete safeguards for EU internet users that their data and **privacy** are protected and handled according to EU rules.
4. Increased **protection** against malicious activities **based on both global and local (EU) threat feeds** and intelligence.
5. Testing and deploying innovative technologies to enhance internet access **security and privacy**.



LEARNING

June 11, 2025

# DNS4EU Goes live: A European Alternative to Google and Cloudflare DNS, Powered by Whalebone

# Looking into .pl registry

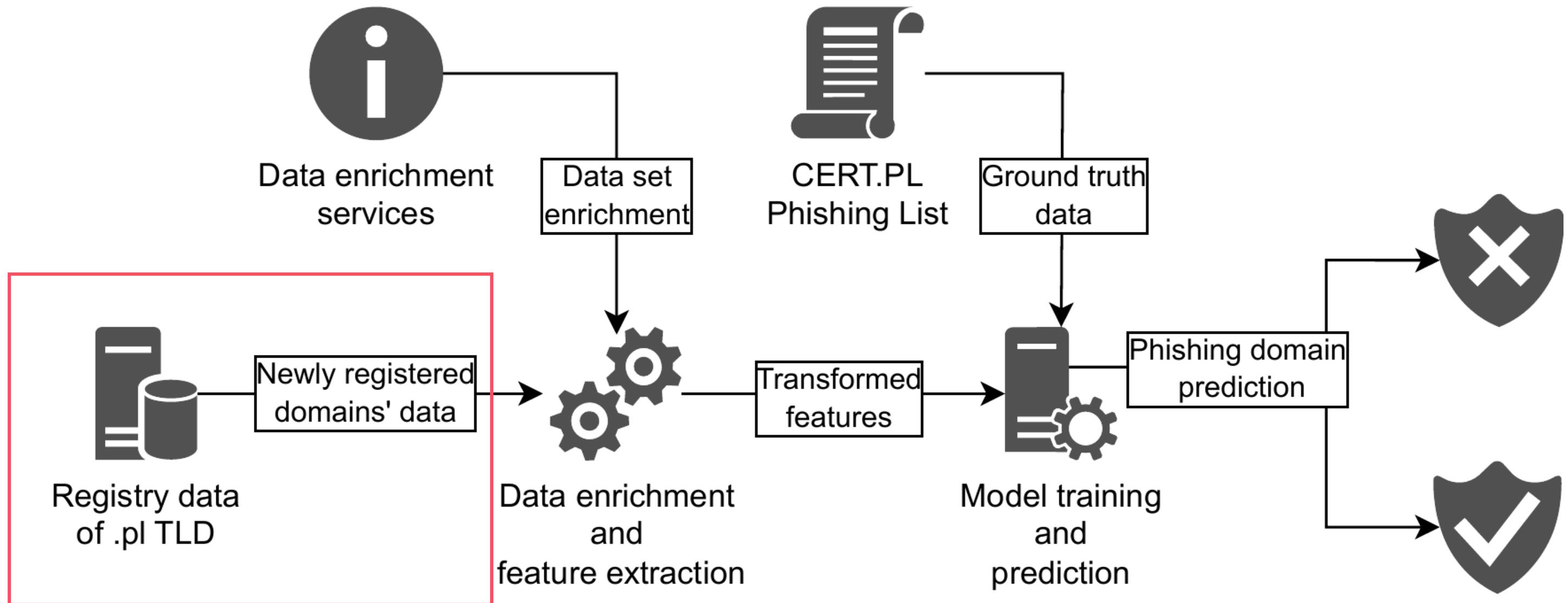
---

# Approach

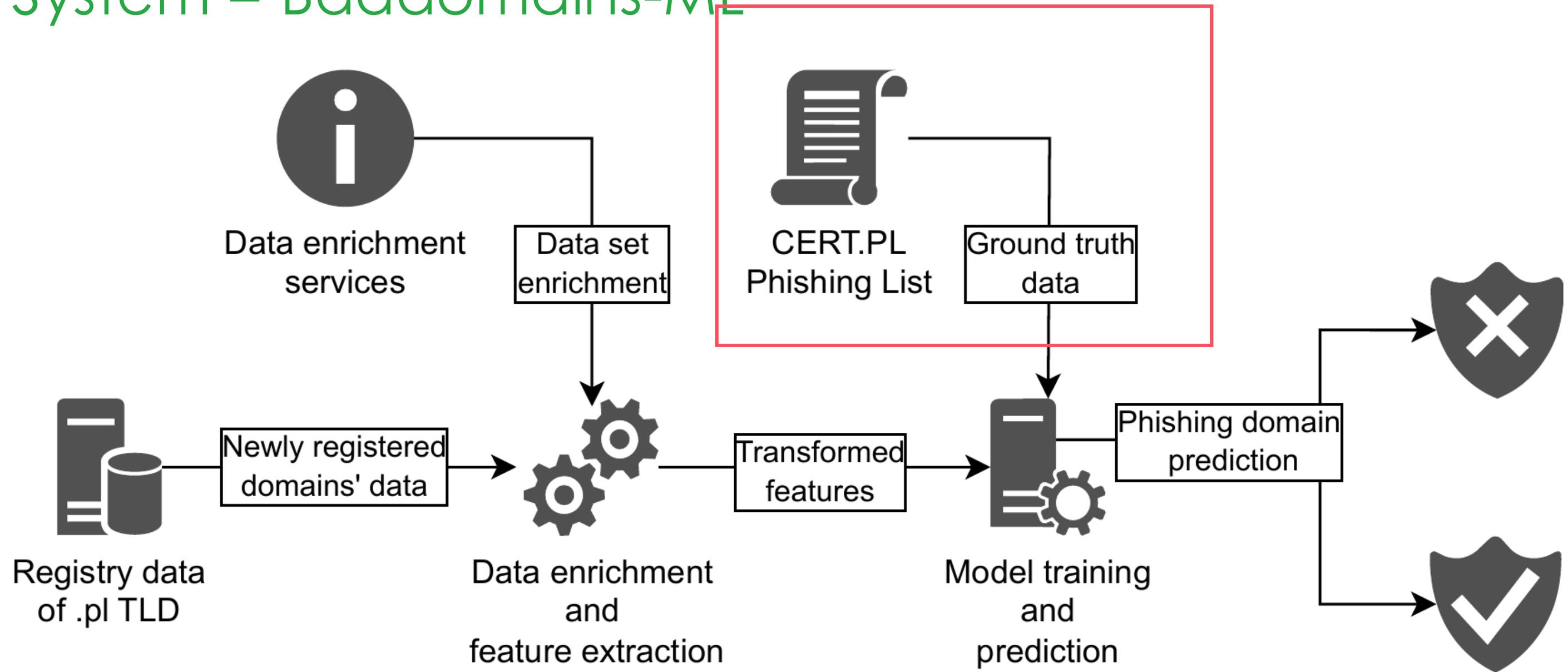
- Phishing domain detection shortly after registration
- Registry data used as model's feature basis: domain name, registrar, registrant's contact information, nameserver, ...
- Focus on campaigns targeting Polish internet users

Domain Name	pl-oferta923475.pl
State	Active in DNS [REGISTERED]
Created	2025-06-01 12:41:46
Last modified	2025-06-16 16:44:47
End of the billing period	2026-06-01 12:41:46
Nameservers	pns1.regery.net pns2.regery.net pns3.regery.net

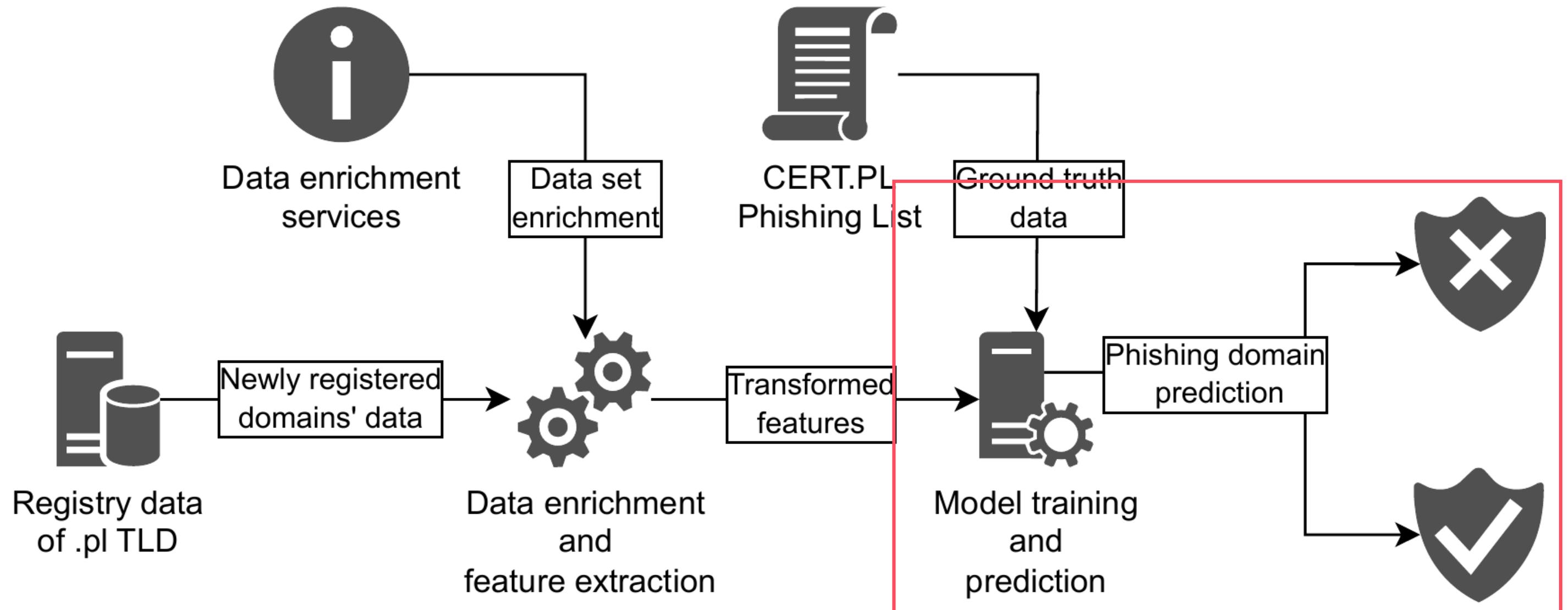
# System = Baddomains-ML



# System = Baddomains-ML



# System = Baddomains-ML



# Detection levels

Rolling value of F1 for the last 7 days



Significant drop in the detection levels

Drop in numbers: from couple of domains per day to couple per week

# Problems with detection

- Predicting domain is not enough
- Phishing payload on subdomains
- Main domains commonly without  
DNS A record

Cannot GET /

id3283[.]pl

# Addressing the problems – subdomains

- Subdomains guessing
- Pivoting using known phishing payload URLs
- Hunting in DNS queries

The screenshot shows a checkout page for AleBilet. On the left, a table lists the items: 3 x 150 zł for 450 zł, a 67.5 zł service fee, and a total of 517.50 zł. Below this is a delivery method section for 'Natychmiastowe pobranie' and a note that PDF tickets will be emailed. A payment method section shows 'BLIK' as the selected option. At the bottom, there are two checked checkboxes for terms and conditions, and a pink 'ZAMÓW I ZAPŁAĆ' button. On the right, a ticket preview shows details for 'Bilety na Finał Pucharu Polski 2025 Legia - Pogoń' at PGE Narodowy, Warsaw, on May 2nd at 16:00. The ticket location is Trybuna, Sektor: G22, Rząd: 7, with a nominal price of 150 zł. A security guarantee icon and text are also present.

Cena	
3 x 150 zł	450 zł
Oplata serwisowa	67.5 zł
<b>Razem</b>	<b>517.50 zł</b>

**Dostawa**  
Natychmiastowe pobranie

📧 Bilety w formie plików PDF zostaną wysłane na e-mail od razu po zakupie.

**Wybierz formę płatności**

BLIK

Oświadczam, że znam i akceptuję [regulamin](#) AleBilet.  
Przyjmuję do wiadomości, że po opłaceniu zamówienia stracę prawo do odstąpienia od umowy z AleBilet sp. z o.o., ponieważ usługa pośrednictwa w sprzedaży biletów zostanie wykonana niezwłocznie po jej zamówieniu. \*

Chcę otrzymywać wiadomości e-mail z powiadomieniami o imprezach i ofertach dostępnych w AleBilet. Możesz z tego zrezygnować klikając na link znajdujący się każdej wiadomości.

**ZAMÓW I ZAPŁAĆ**

Administratorem danych osobowych jest AleBilet sp. z o.o. z siedzibą w Warszawie (02-611) przy ul. Huculskiej 6. [rozwij](#)

**Impreza**  
★ Bilety na Finał Pucharu Polski 2025 Legia - Pogoń

**Miejsce**  
📍 PGE Narodowy, Warszawa

**Termin**  
📅 2 maja 2025, piątek, 16:00

**Trybuna**  
Sektor: G22  
Rząd: 7  
Cena nominalna za 1 bilet: 150 zł

**Bezpieczeństwo zakupu**  
W AleBilet masz gwarancję, że otrzymasz autentyczne bilety na czas przed imprezą.

alebilet.id3283[.]pl

# Addressing the problems – low number of detections

- Model tweaking
- Result: the number of detected domains is **doubled**
- Only 30% of .pl domains on the Warning List are detected with this method - is it enough given the effort invested?
- Value – **unique detections**
  - Not seen by other non-ML methods (20% of detected domains)
  - Earlier detection than waiting for an incident report (80% of time it was faster)
  - Uncovering FPs of the Warning List

# DNS query stream

---

# Monitoring resolvers: why and how

- **Goal:** monitor activity on resolvers to detect phishing

# Monitoring resolvers: why and how

- **Goal:** monitor activity on resolvers to detect phishing
- **Change of scope:** all campaigns, not just targeting Poland

# Monitoring resolvers: why and how

- **Goal:** monitor activity on resolvers to detect phishing
- **Change of scope:** all campaigns, not just targeting Poland
- **Dataset:** anonymized DNS queries from DNS4EU resolvers

# Monitoring resolvers: why and how

- **Goal:** monitor activity on resolvers to detect phishing
- **Change of scope:** all campaigns, not just targeting Poland
- **Dataset:** anonymized DNS queries from DNS4EU resolvers
- Research **in progress**

# example.com

## Domain names

**example.com**

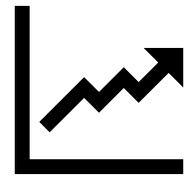
Domain names



Time related

**example.com**

Domain names



Time related

**ASN etc.**

Other features

**example.com**

Domain names

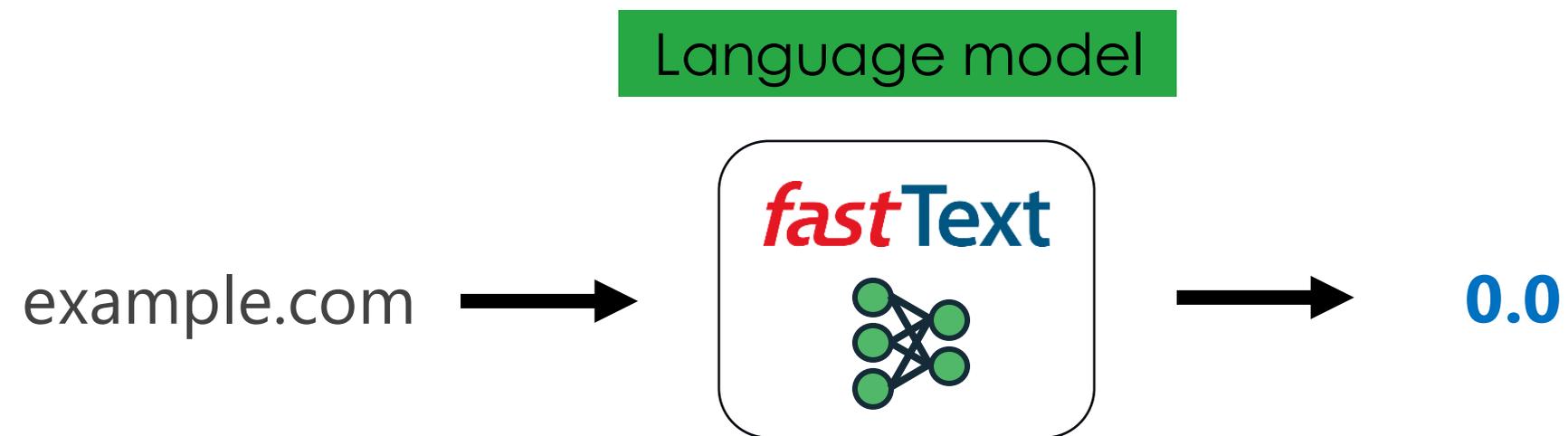


Time related

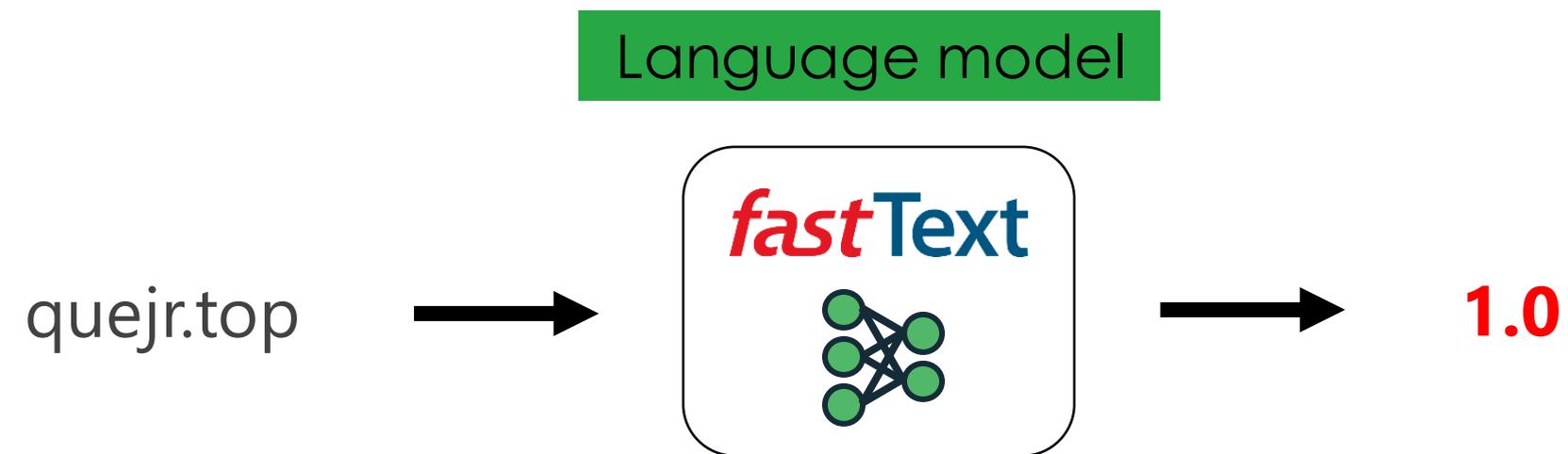
ASN etc.

Other features

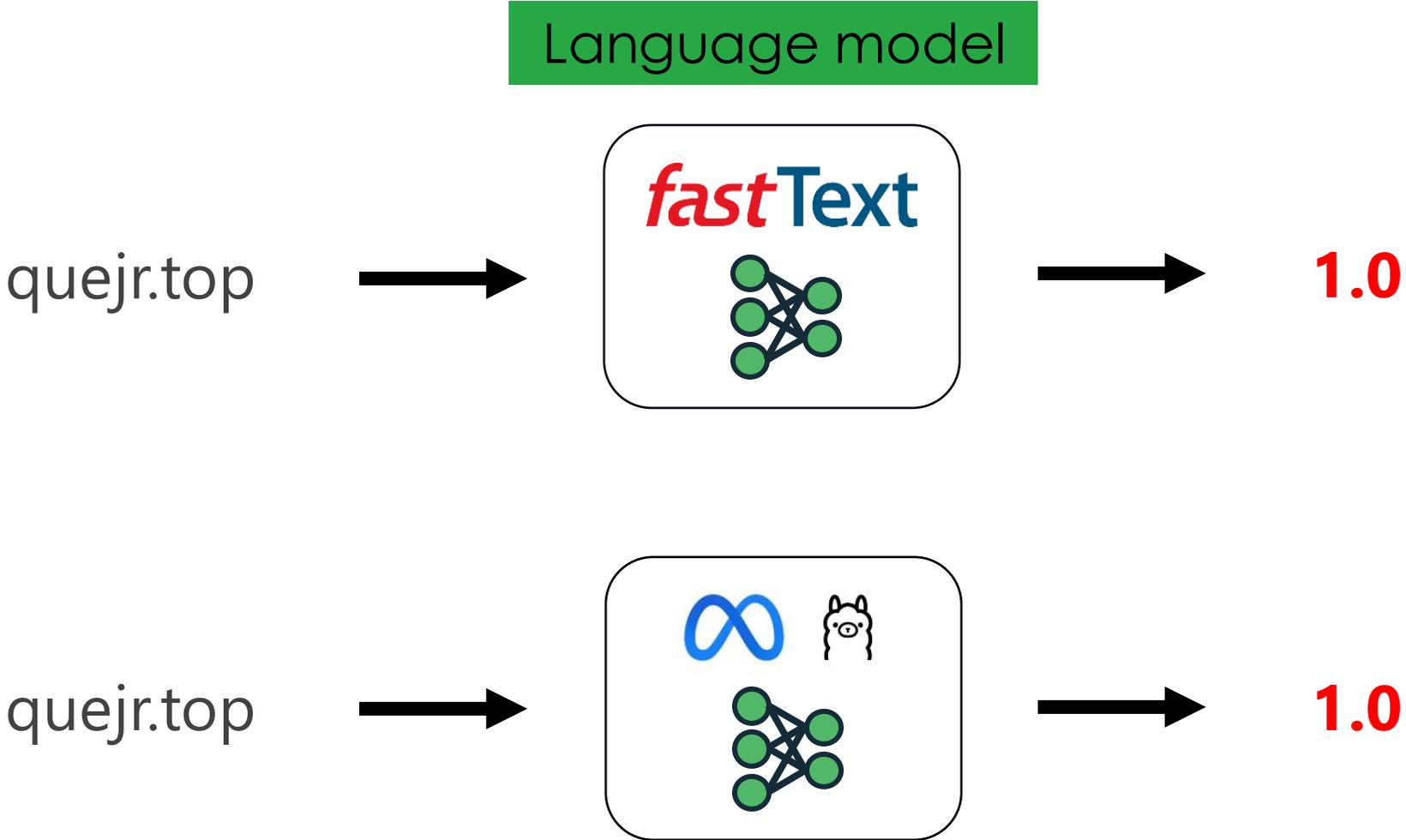
# Domain names



# Domain names



# Domain names



# Current processing pipeline

glimzo.com

trexify.net

zuntra.org

google.com

kieab.top

quejr.top

# Current processing pipeline

glimzo.com

trexify.net

zuntra.org

google.com

kieab.top

quejr.top

# Current processing pipeline

glimzo.com

trexify.net

zuntra.org

~~google.com~~

kieab.top

quejr.top



filter out domains from Tranco

Research-Oriented Top Sites Ranking

Hardened Against Manipulation

# Current processing pipeline

glimzo.com

trexify.net

zuntra.org

~~google.com~~

kieab.top

quejr.top



filter out domains from Tranco

Research-Oriented Top Sites Ranking

Hardened Against Manipulation

+

our own whitelist

# Our whitelist

amazonaws.com

cloudfront.net

microsoft.com

google.com

googleapis.com

apple.com

akadns.net

akamai.net

## reported malicious domains

93	amazonaws.com
1758	cloudfront.net
0	microsoft.com
0	google.com
1	googleapis.com
0	apple.com
3	akadns.net
0	akamai.net

## Our whitelist

## reported malicious domains

93

1758

0

0

1

0

3

0

## Our whitelist

amazonaws.com

cloudfront.net

microsoft.com

google.com

googleapis.com

apple.com

akadns.net

akamai.net

# Current processing pipeline

glimzo.com

trexify.net

zuntra.org

~~google.com~~

kieab.top

quejr.top



filter out domains from Tranco  
Research-Oriented Top Sites Ranking  
Hardened Against Manipulation

+

our own whitelist

+

other whitelists

# Current processing pipeline

glimzo.com  
trexify.net  
zuntra.org  
~~google.com~~  
kieab.top  
quejr.top



filter out domains from Tranco  
Research-Oriented Top Sites Ranking  
Hardened Against Manipulation

+ our own whitelist  
+ other whitelists



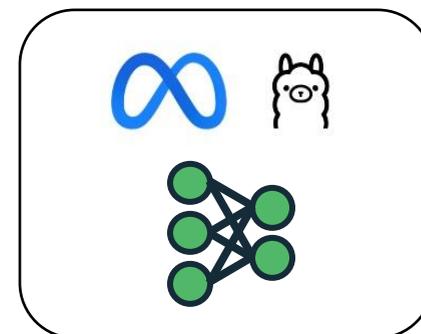
# Current processing pipeline

glimzo.com  
trexify.net  
zuntra.org  
~~google.com~~  
kieab.top  
quejr.top

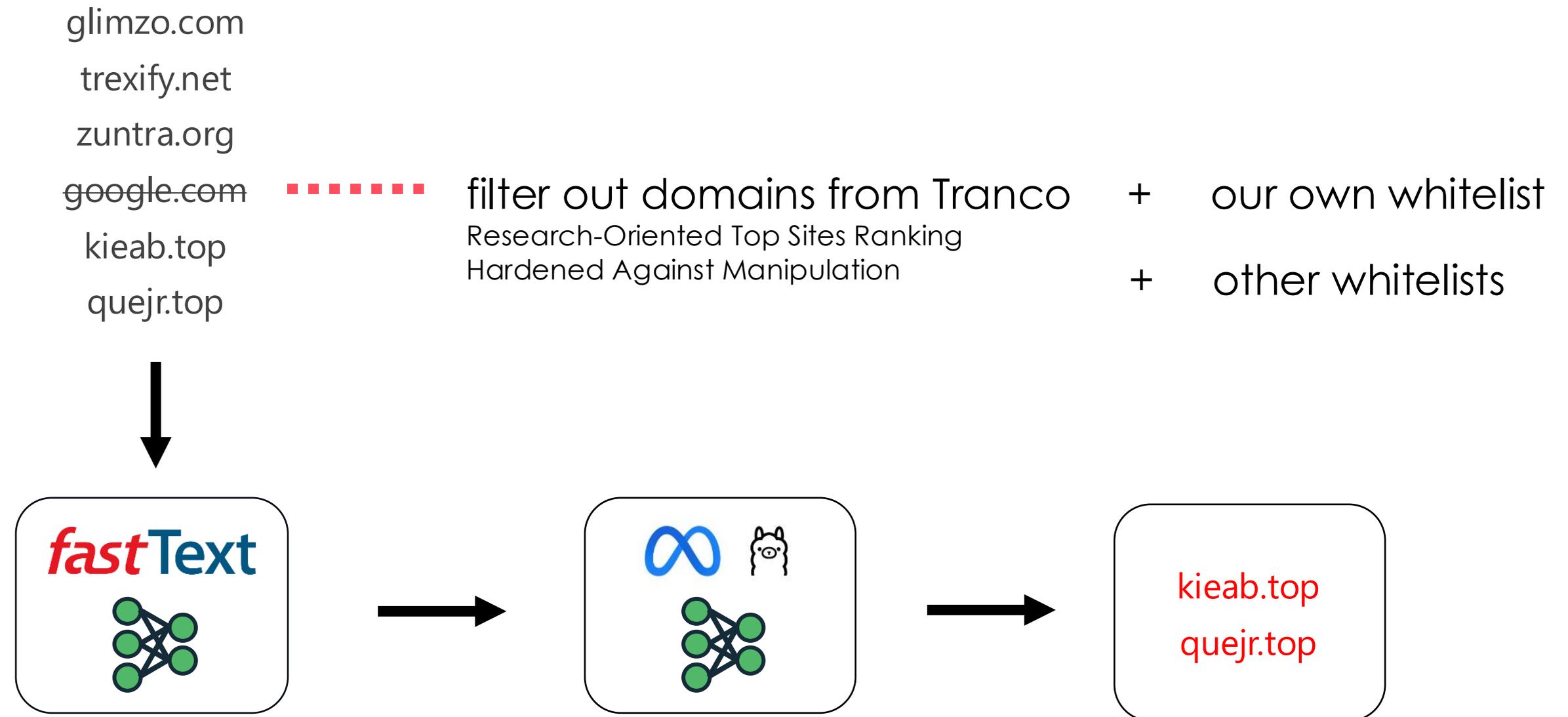


filter out domains from Tranco  
Research-Oriented Top Sites Ranking  
Hardened Against Manipulation

+ our own whitelist  
+ other whitelists



# Current processing pipeline



example.com

Domain names

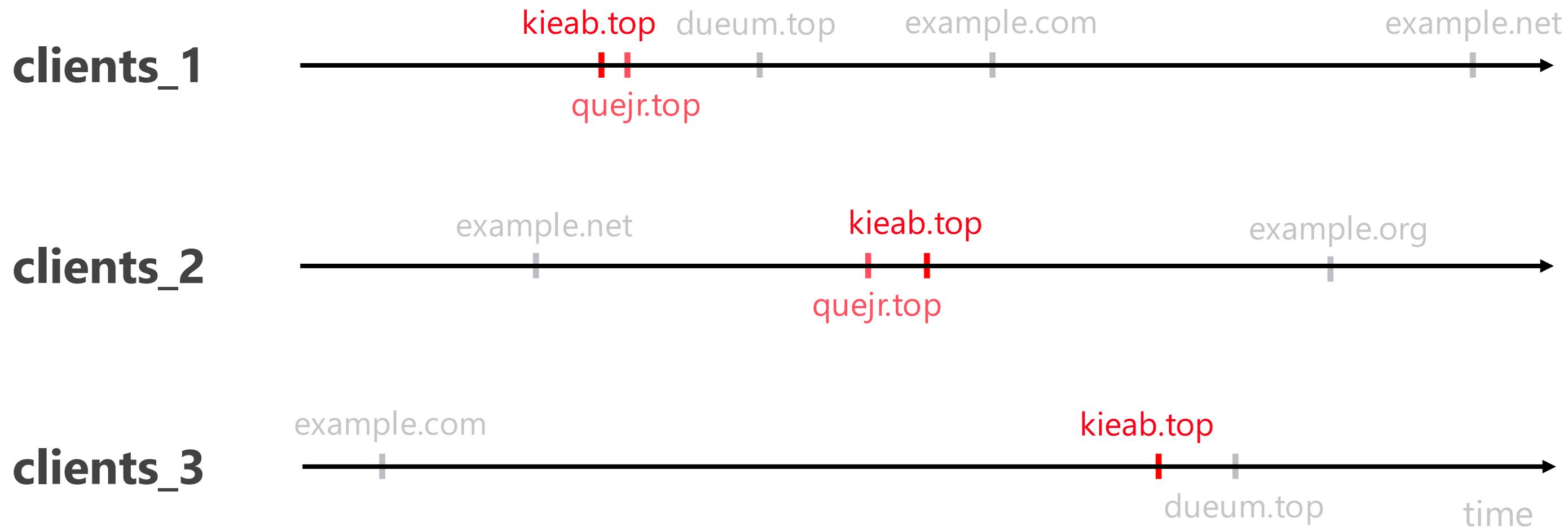


Time related

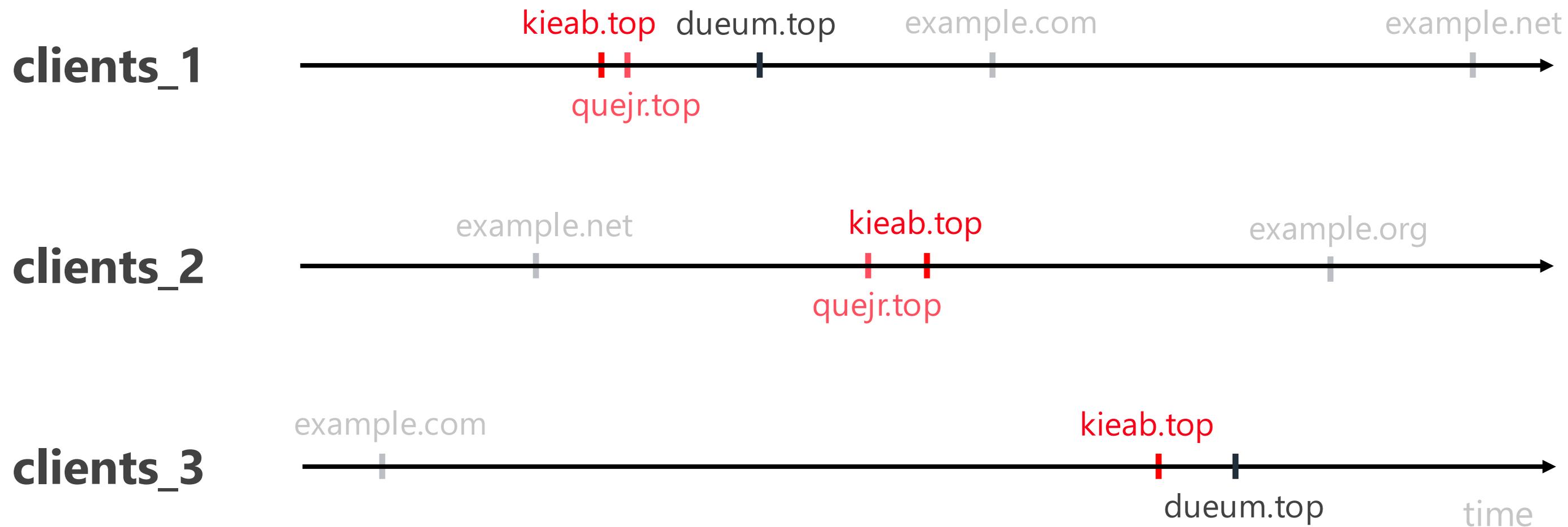
ASN

Other features

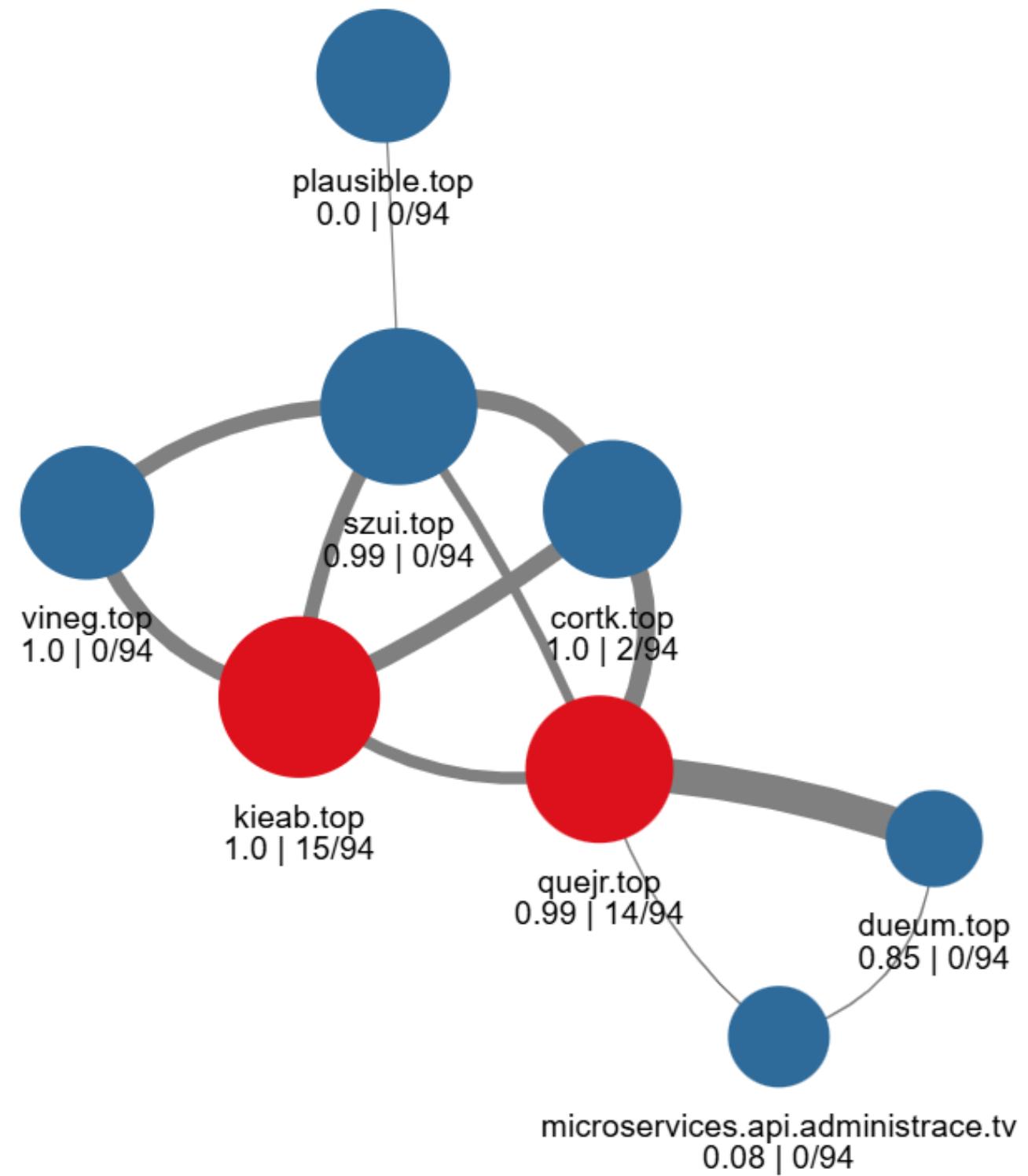
# CO-OCCURRENCE



# CO-OCCURRENCE



# CO-OCCURRENCE



example.com

Domain names



Time related

**ASN**

Other features

# ASN

## Autonomous System Number

# ASN

## Autonomous System Number

### ASN **reputation score**

# ASN

## Autonomous System Number

### ASN **reputation score**

work in progres...

# Results

**3h** long analysis (**17.10**, Friday)

# Results

**3h** long analysis (**17.10**, Friday)

**31M** queries in total



# Results

**3h** long analysis (**17.10**, Friday)

**31M** queries in total



**14.9M** on FastText based model



**16.1M** (52%) filtered out on whitelists



# Results

**3h** long analysis (**17.10**, Friday)

**31M** queries in total 

**14.9M** on FastText based model 

**16.1M** (52%) filtered out on whitelists

**1.2M** on Llama based model 

**13.7M** filtered out on FastText

# Results

**3h** long analysis (**17.10**, Friday)

**31M** queries in total 

**14.9M** on FastText based model 

**16.1M** (52%) filtered out on whitelists

**1.2M** on Llama based model 

**13.7M** filtered out on FastText

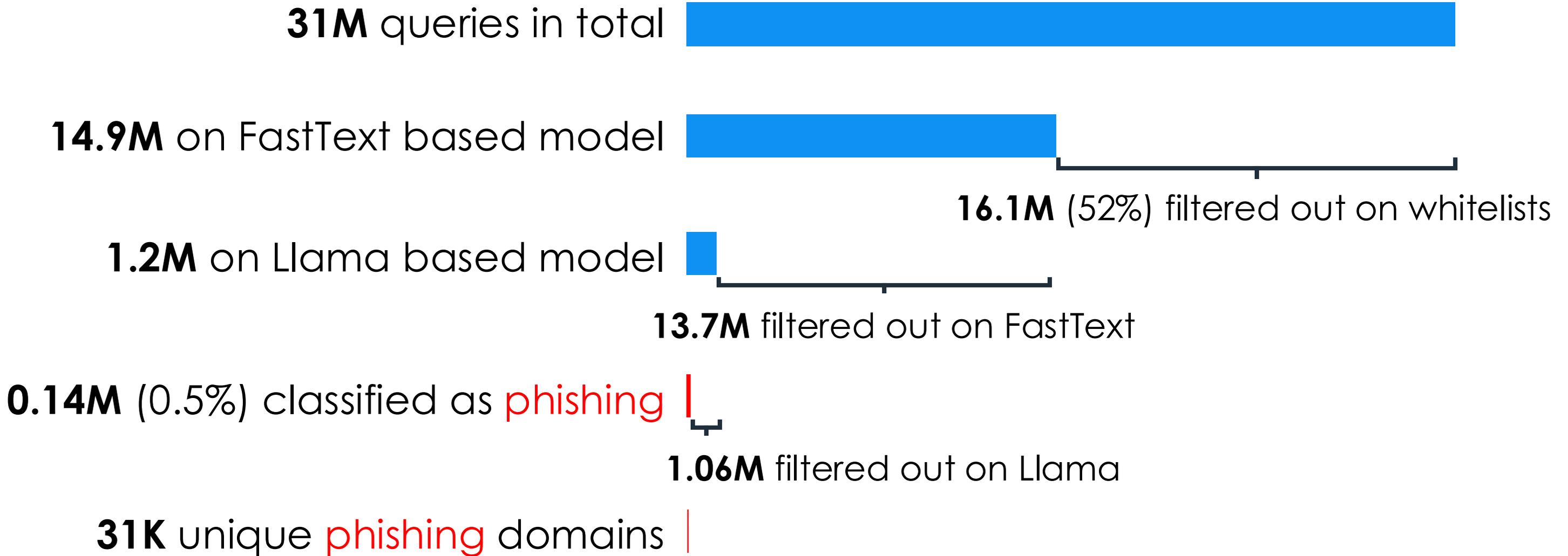
**0.14M** (0.5%) classified as **phishing** 

**1.06M** filtered out on Llama

# Results

## 3h long analysis (17.10, Friday)

31M queries in total



Category	Count
Total queries	31M
FastText based model	14.9M
Filtered out on whitelists	16.1M (52%)
Llama based model	1.2M
Filtered out on FastText	13.7M
Classified as phishing	0.14M (0.5%)
Filtered out on Llama	1.06M
Unique phishing domains	31K

14.9M on FastText based model

16.1M (52%) filtered out on whitelists

1.2M on Llama based model

13.7M filtered out on FastText

0.14M (0.5%) classified as phishing

1.06M filtered out on Llama

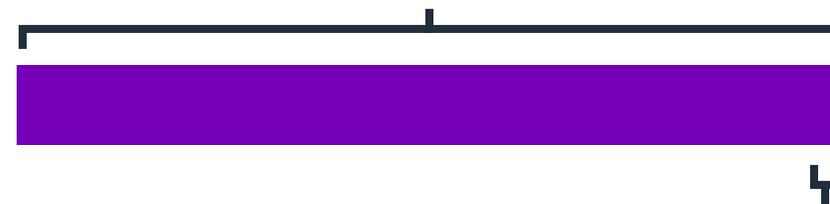
31K unique phishing domains

# Results

## Random **800 elements** sample analysis



**455** (57%) >0 score on Virus Total



including **9** in a high confidence  
additional phishing domains data source

# Challenges

Domain names approach: **TLD balancing**

Non-phishing

domain1.tld

domain2.tld

phishing

phish1.tld

phish2.tld

phish3.tld

phish4.tld

phish5.tld

phish6.tld

...

# Challenges

Domain names approach: **TLD balancing**

Non-phishing

domain1.tld

domain2.tld

phishing

phish1.tld

phish2.tld

phish3.tld

phish4.tld

phish5.tld

phish6.tld

...

# Challenges

Domain names approach: **TLD balancing**

## Non-phishing

domain**1**.tld

domain**2**.tld

domain**1**.tld

domain**2**.tld

domain**1**.tld

domain**2**.tld

...

## phishing

phish1.tld

phish2.tld

phish3.tld

phish4.tld

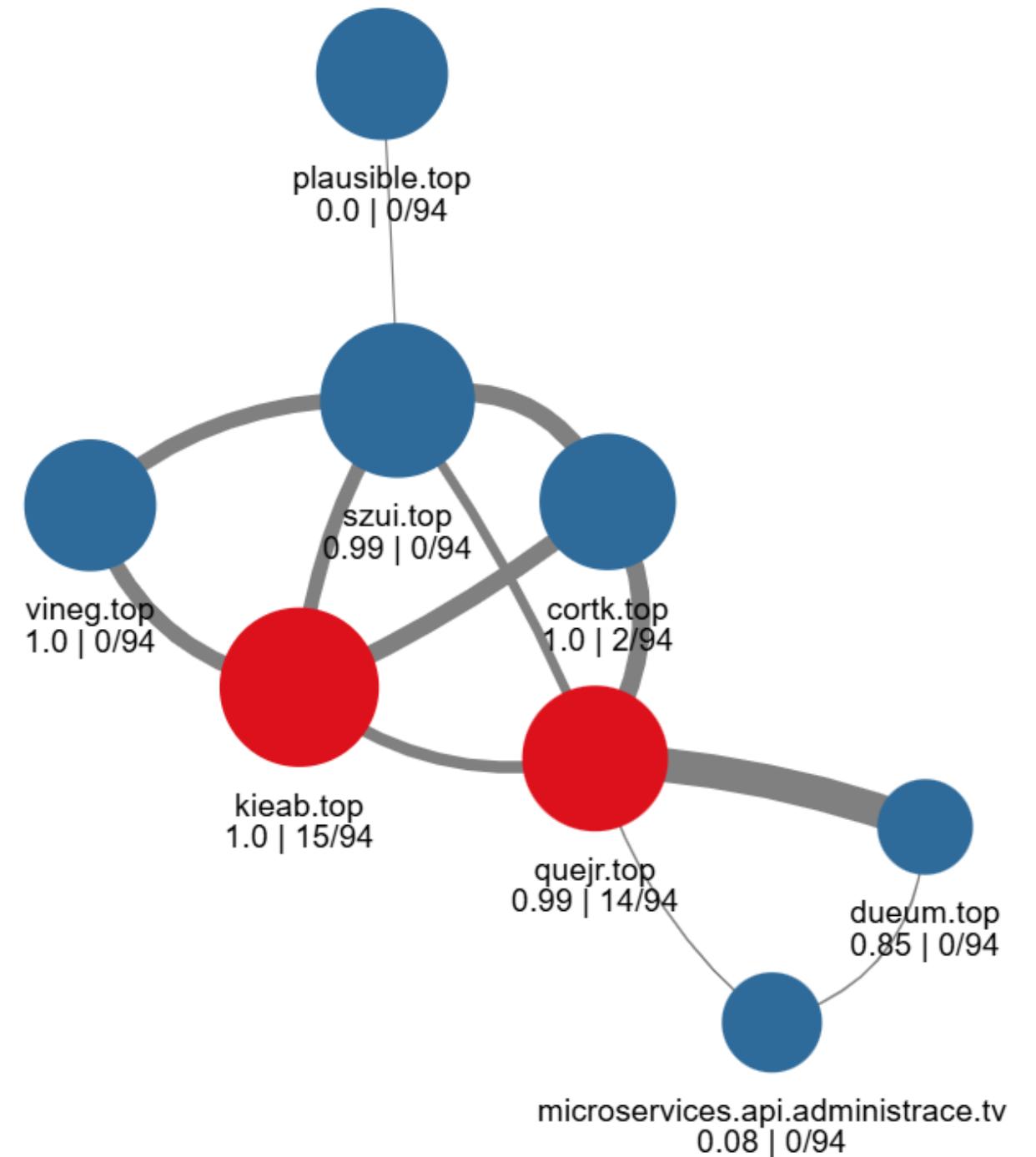
phish5.tld

phish6.tld

...

# Challenges

Co-occurrence: **difficult to automate**



# Challenges

- Dealing with **a lot of** streaming **data**

# Challenges

- Dealing with **a lot of** streaming **data**
- Hard to **check** (and proof) whether detected domains are **truly phishing**

# Challenges

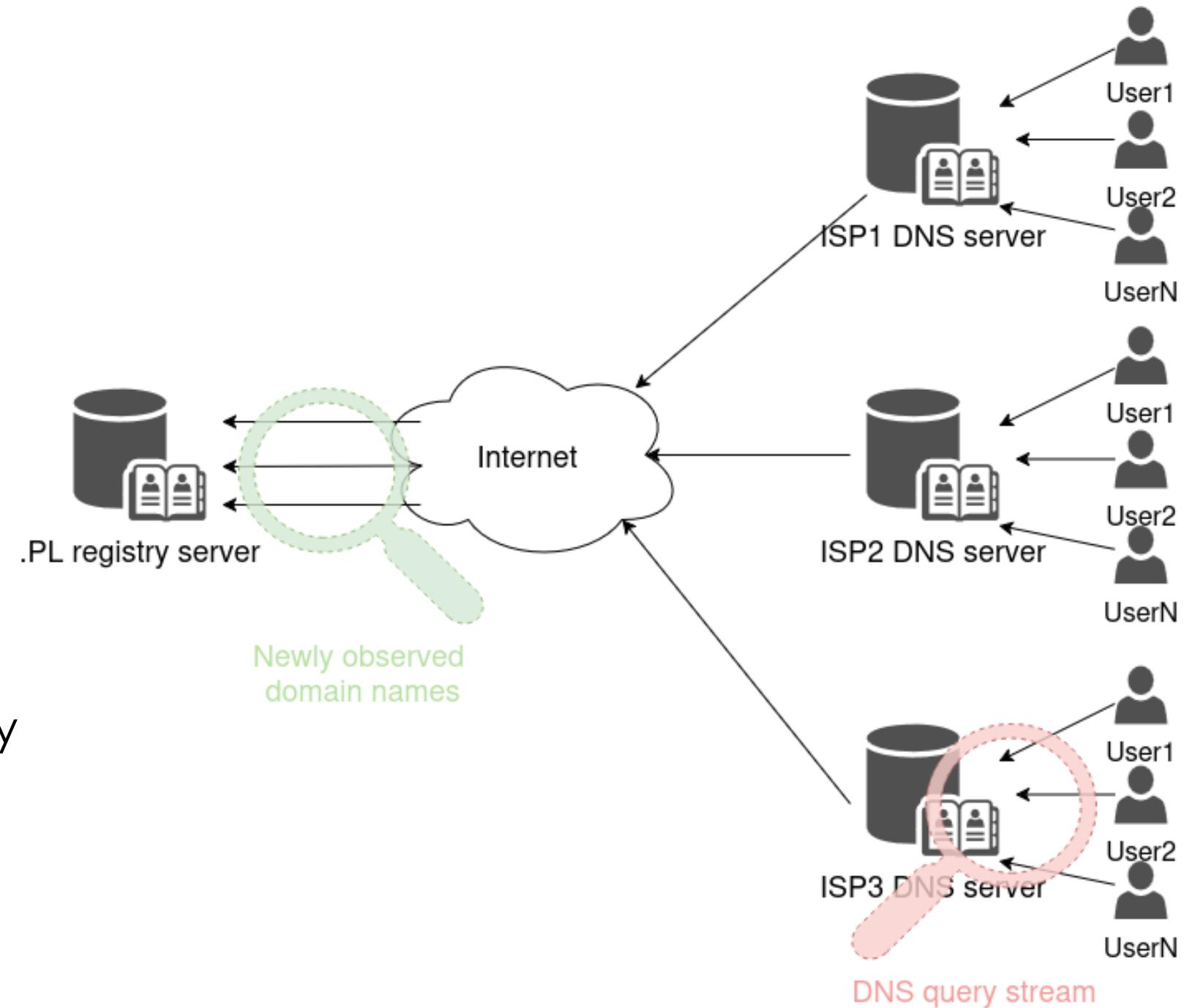
- Dealing with **a lot of** streaming **data**
- Hard to **check** (and proof) whether detected domains are **truly phishing**
- Status: moving to **production environment**

# .pl DNS servers

Monitoring DNS requests for newly observed domain names

# Approach

- Monitoring DNS requests at .PL registry server level
- Collecting data only about domain names not seen previously
- Advantage: observing subdomains not seen in other sources, e.g., CT log, registry data



# Newly observed domain names

- Collecting tuples for all DNS records
- Domain names with various number of sublevels
- Hunting for:
  - keywords, suffixes, regexes
  - subdomains of specific domains
- Cooperation with other CERT.PL systems, incl. Baddomains-ML

FQDN	Record type	First Seen	Last Seen
sub1.example.pl	A	1750765434	1750851789

# Newly observed domain names vs CT logs

- No subdomains visibility for wildcard certificates in CT logs
- Newly observed domain names can uncover other subdomains from a hunting set

9527ukfs486yvre.hb20[.]pl

The only subdomain of hb20[.]pl  
on the Warning List

7fbn34olxcm6avw.hb20[.]pl  
h190uao6wcrkl2i.hb20[.]pl

Subdomains from the NOD monitor  
Candidates for blocking  
Strong indicator for *hb20[.]pl* blocking

# Lessons learned

---

# ML classifier on registry data

- Early detection possible: at registration
- **If significant number of malicious domains: good results**



# ML classifier on registry data

- Early detection possible: at registration
- If significant number of malicious domains: good results
- **If low number of malicious domains: problems with getting detections**



# ML classifier on query stream

- Just looking at domain names gives quite good results
- Challenge: using other features for detection: work ongoing
- Sufficient scale/coverage needed to see dynamic behaviors

# Challenges

- Evaluation: difficult when we go beyond threats targeting Poland
- ML models identify **suspicious** domains
- ... but we need proof when using as high confidence source = full URL and defeat

cloaking (outside scope of this talk)

# Data from TLD servers

- Underutilized data source for domain hunting
- Not everything has to be a ML model
- Moving to a prototype stage

# Current status

Early phishing detection system – Baddomains-ML  
Status: Deployed

Phishing detection in DNS query stream  
Status: Deployment in 2025Q4

Newly observed domains monitor  
Status: Deployment in 2025Q4



The Warning List

Questions,  
feedback &  
ideas welcome!

piotr.bialczak@cert.pl

michal.halon@nask.pl

[joindns4.eu](https://joindns4.eu)