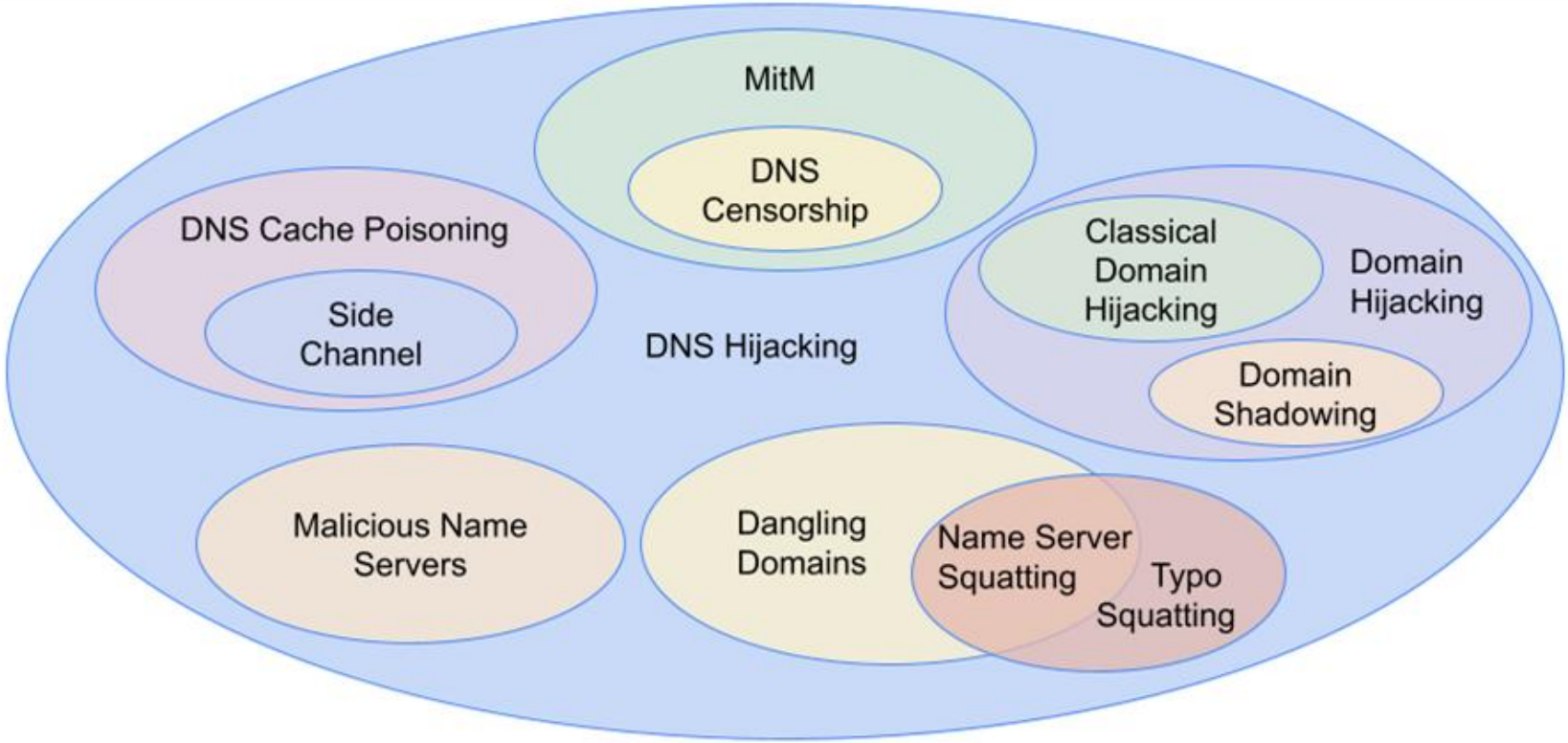
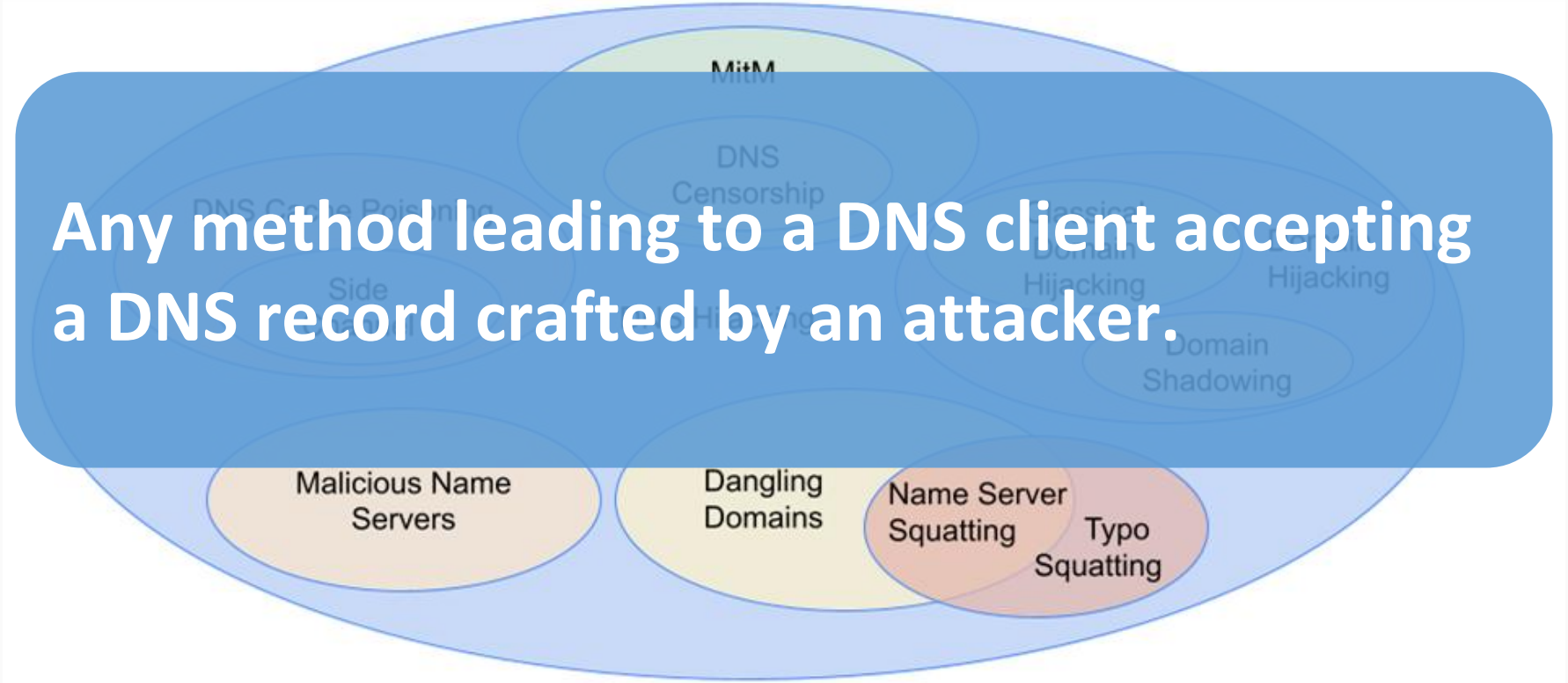
Practical Real-time Detection of IPv4 Record Classical Domain Hijacking at Scale

Janos Szurdi, Mohammad Ghasemisharif, Reethika Ramesh, Zhanhao Chen, Ruian Duan, William Melicher, Daiping Liu

DNS Hijacking

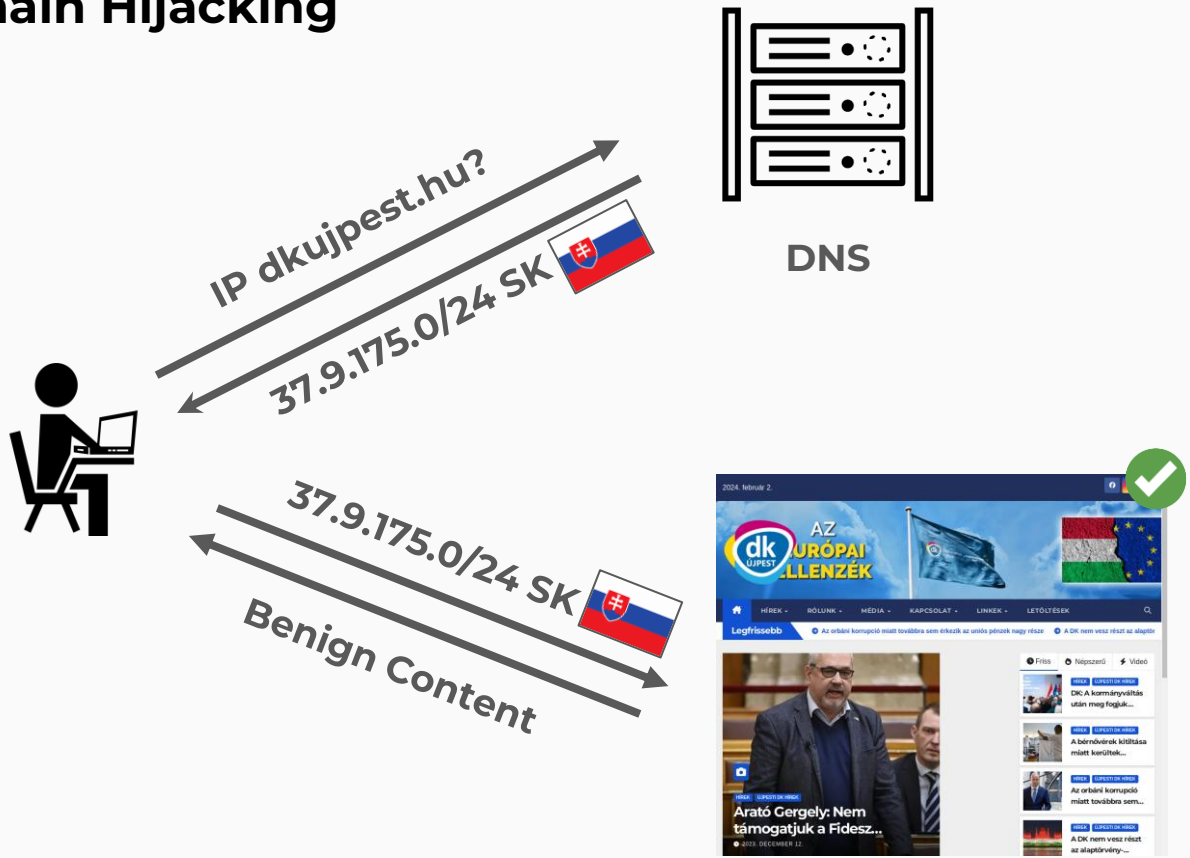


DNS Hijacking

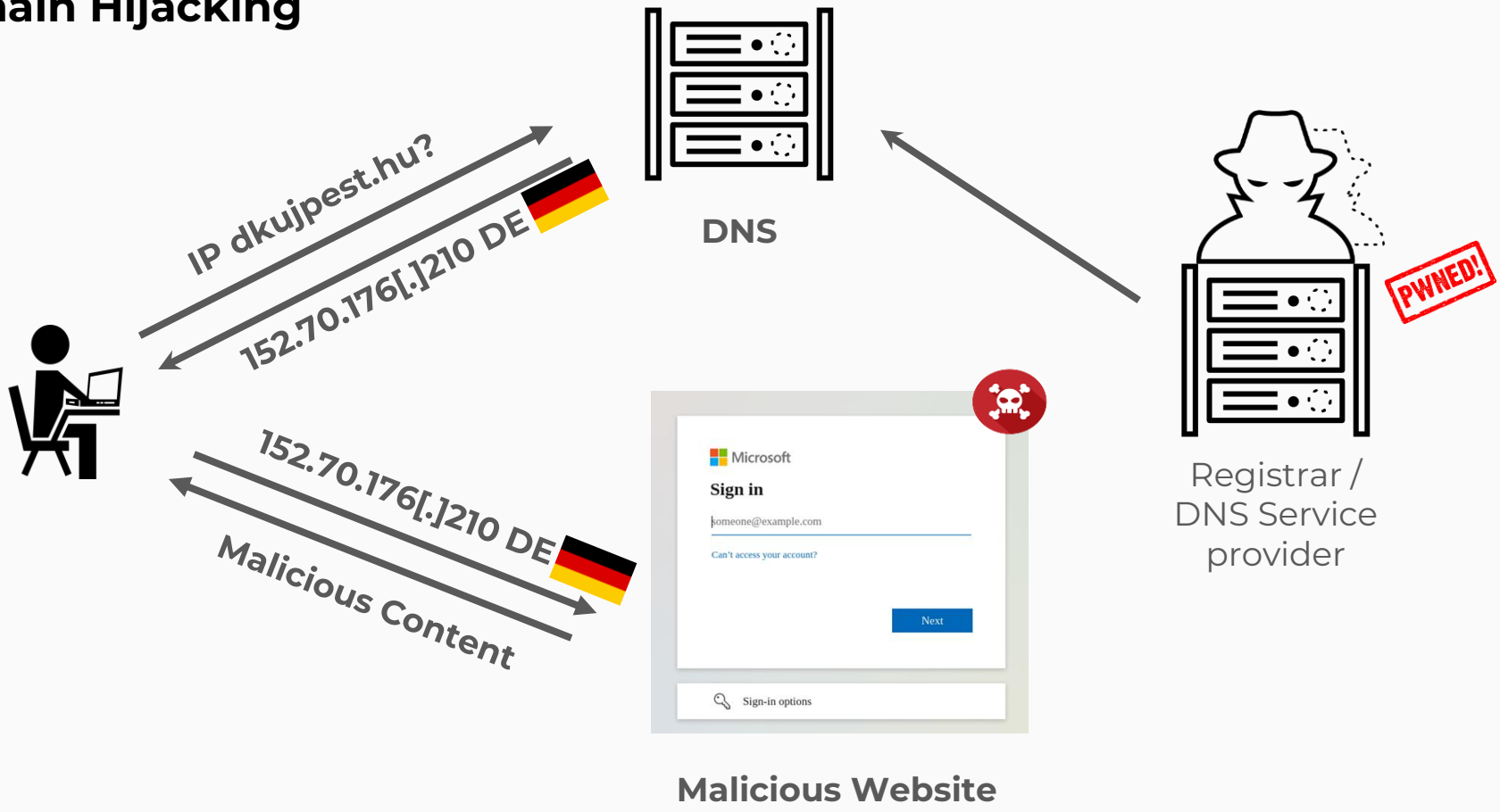


Any method leading to a DNS client accepting a DNS record crafted by an attacker.

Domain Hijacking



Domain Hijacking



Domain Hijacking of a Large Brazilian Bank

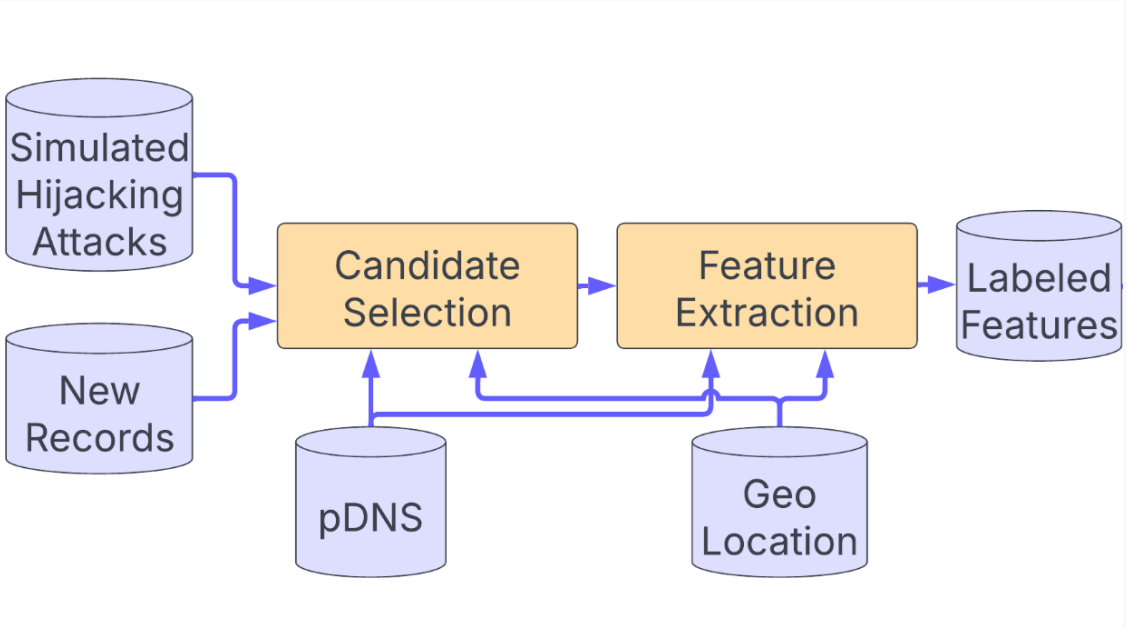
- On Oct. 22, 2016 cybercriminals gained control of all **36 domains of the bank**
  - Compromised DNS service provider
  - Used Let's Encrypt to establish certificates
- **Pointed** all of the bank's employees and customers to **malicious servers**
  - Over 5 million customers exposed
  - Phishing sites and malware
- Malware
  - Disabled antimalware software
  - Harvested Credentials
  - Targeted other banks

Challenges

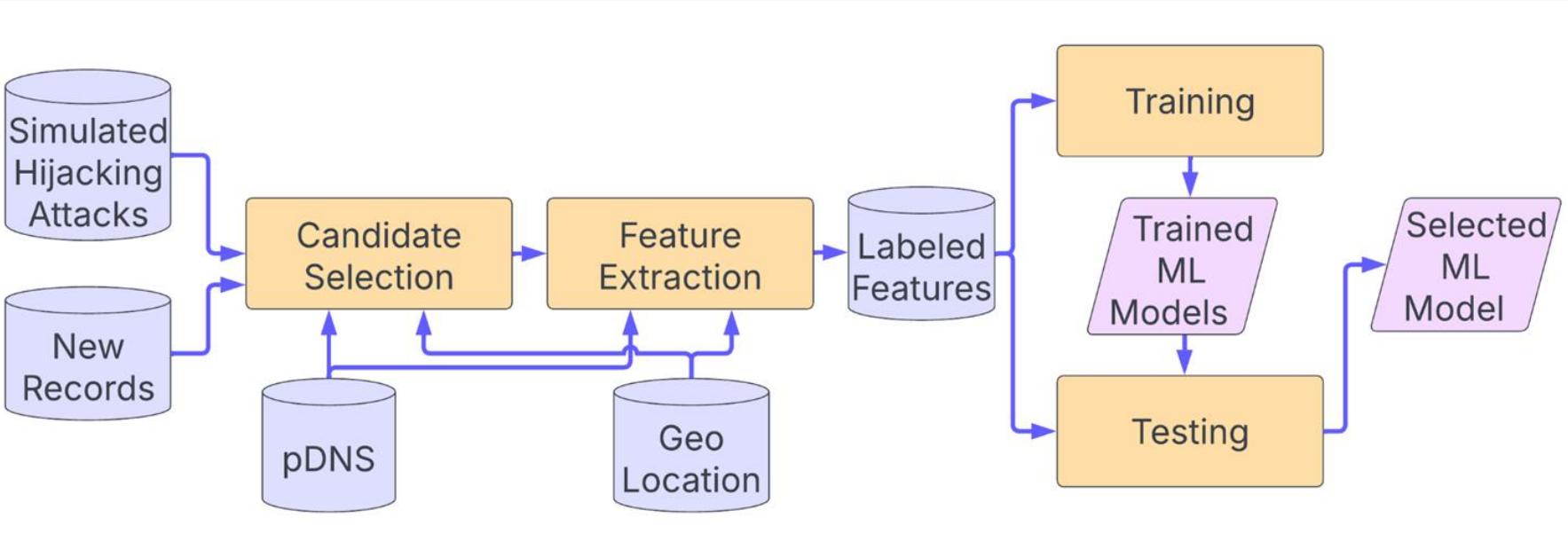
- Hundreds of millions of new DNS records every day
- Only a few domain hijacking records expected
- Hundreds of terabytes of historical data to process
- Very few cases of known hijacking DNS records for training an ML model

Training a Machine Learning Model

Training a Machine Learning Model



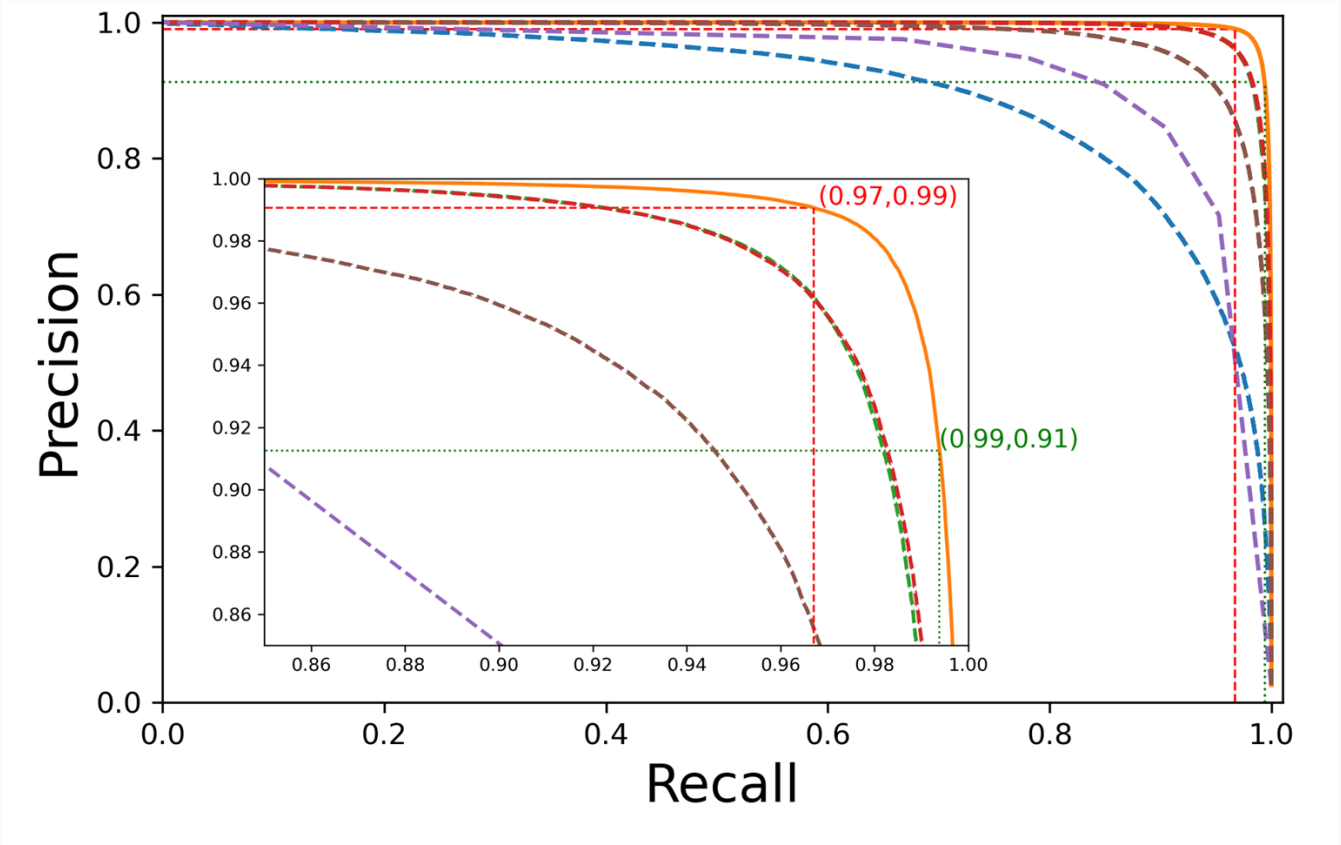
Training a Machine Learning Model



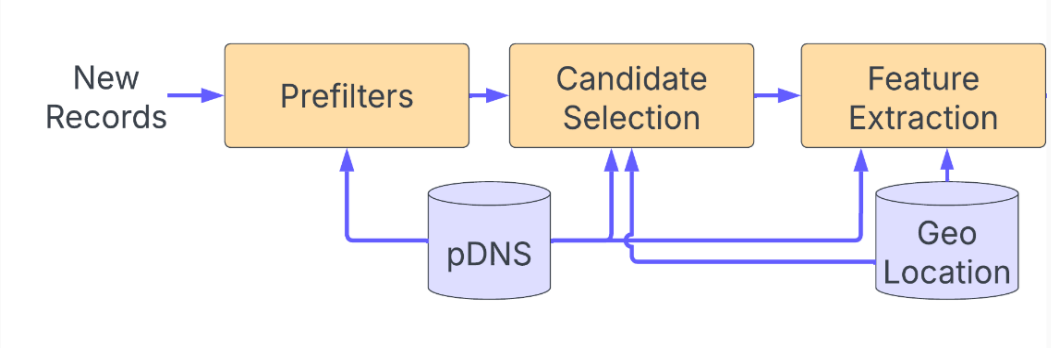
Features used

- Comparison of **DNS History** of new IP and old IP addresses
  - Average DNS record age
- **DNS History** of new IP
  - # domains where IP address is new
- Comparison of **geolocation** of new IP and old IP addresses
  - Is country, ISP, ASN new?
- **DNS History** of the compromised domain
  - # IP addresses, # of IP countries
  - # of new record types

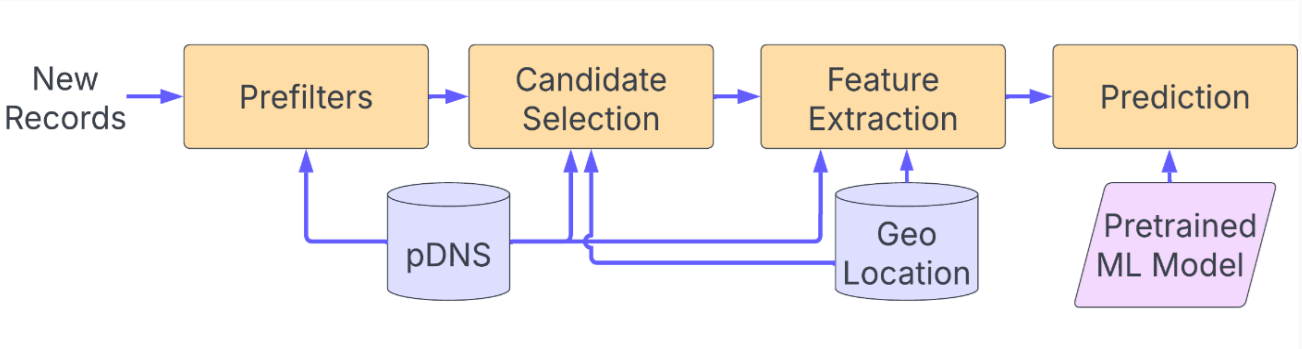
Precision Recall Tradeoff



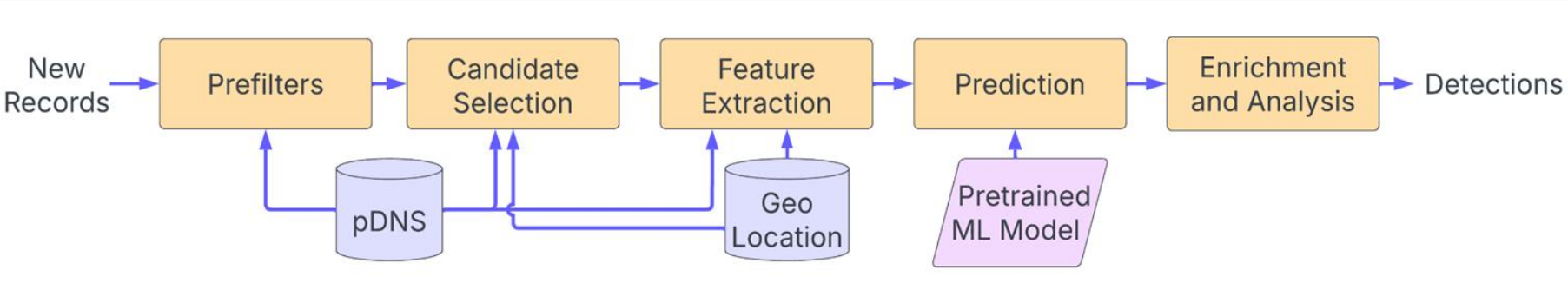
Offline ML Pipeline in Production



Offline ML Pipeline in Production



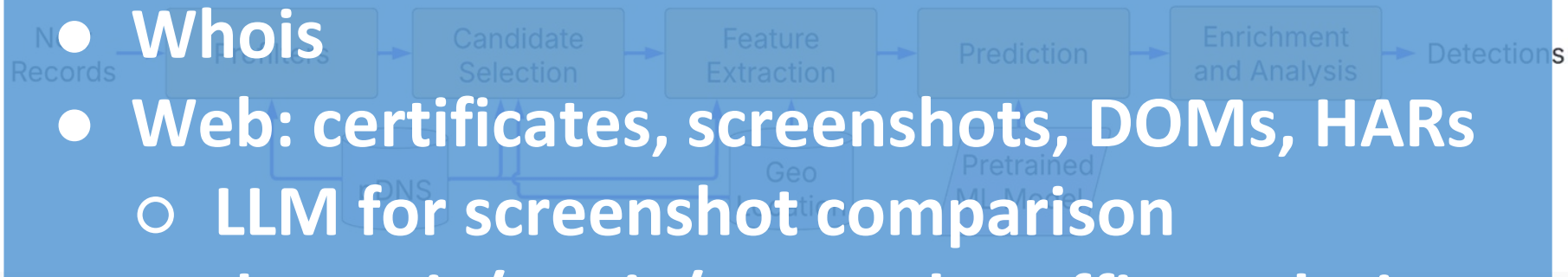
Offline ML Pipeline in Production



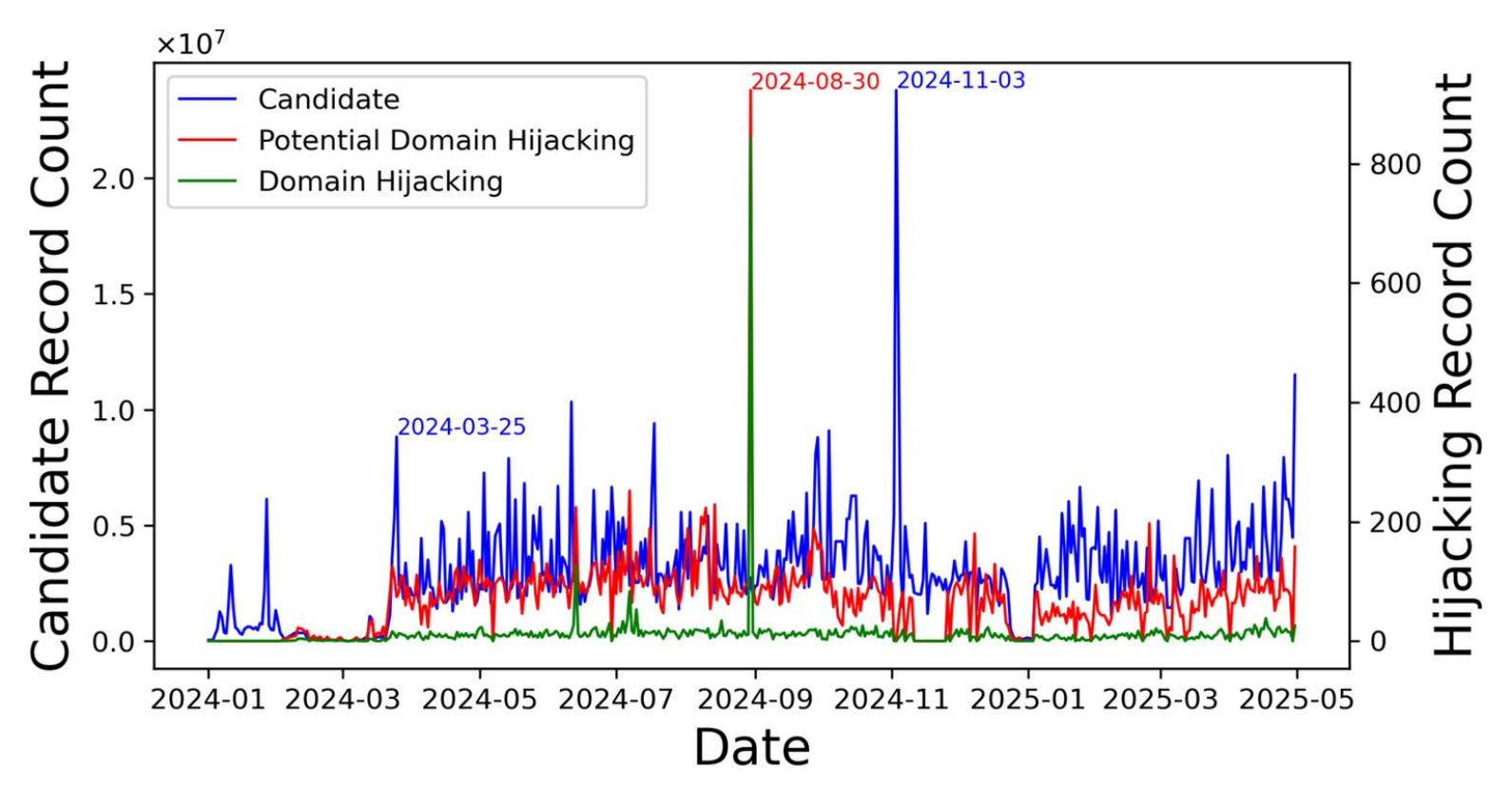
Offline ML Pipeline in Production

Enrichment and Analysis:

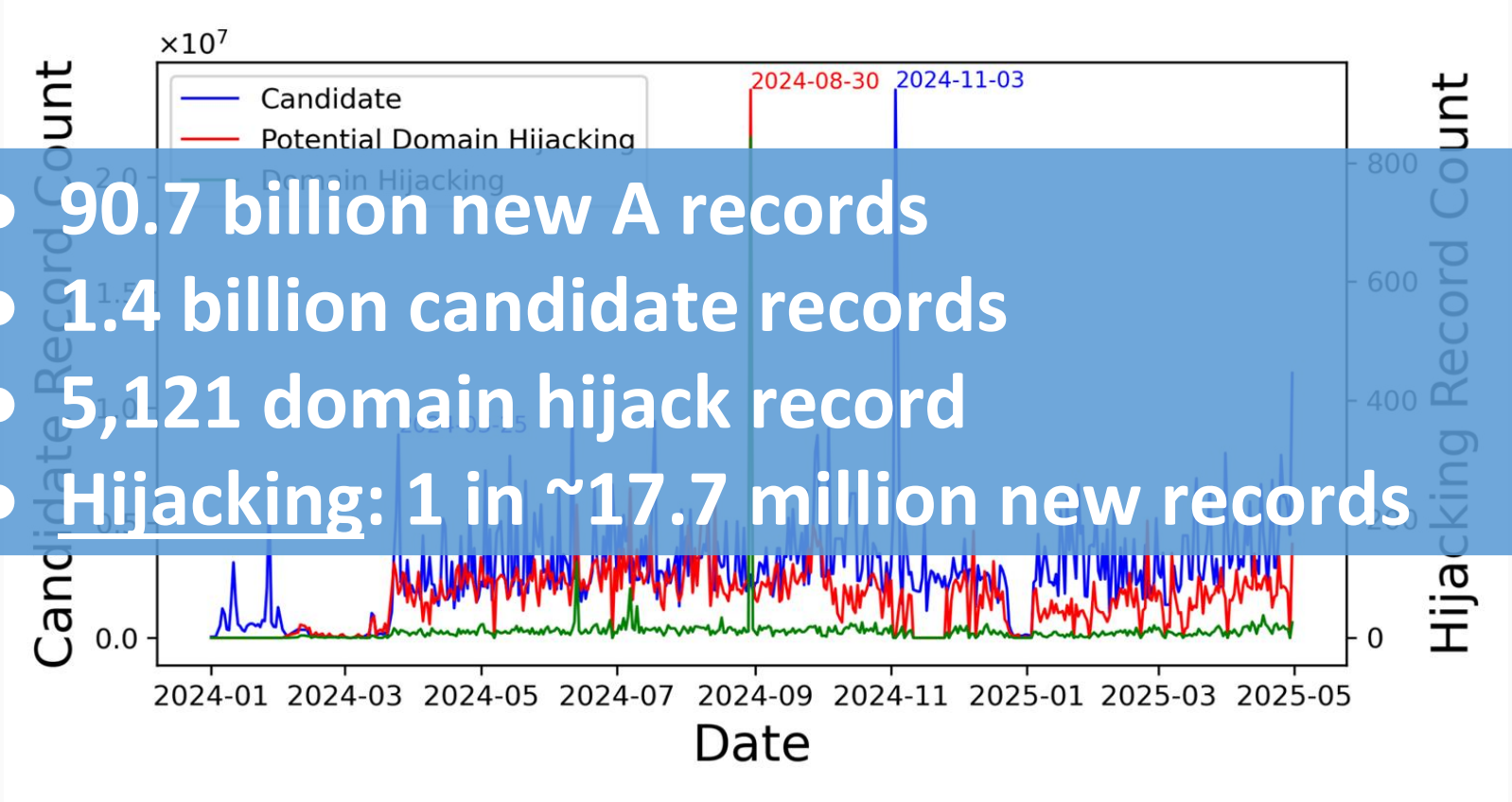
- Whois
- Web: certificates, screenshots, DOMs, HARs
  - LLM for screenshot comparison
  - dynamic/static/network traffic analysis



Numbers in Production

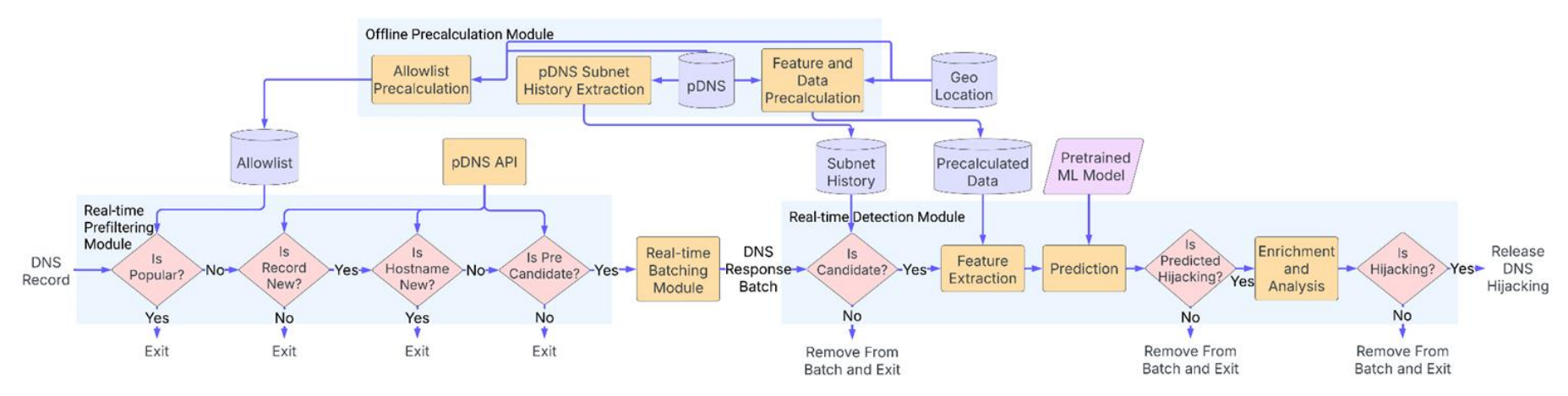


Numbers in Production

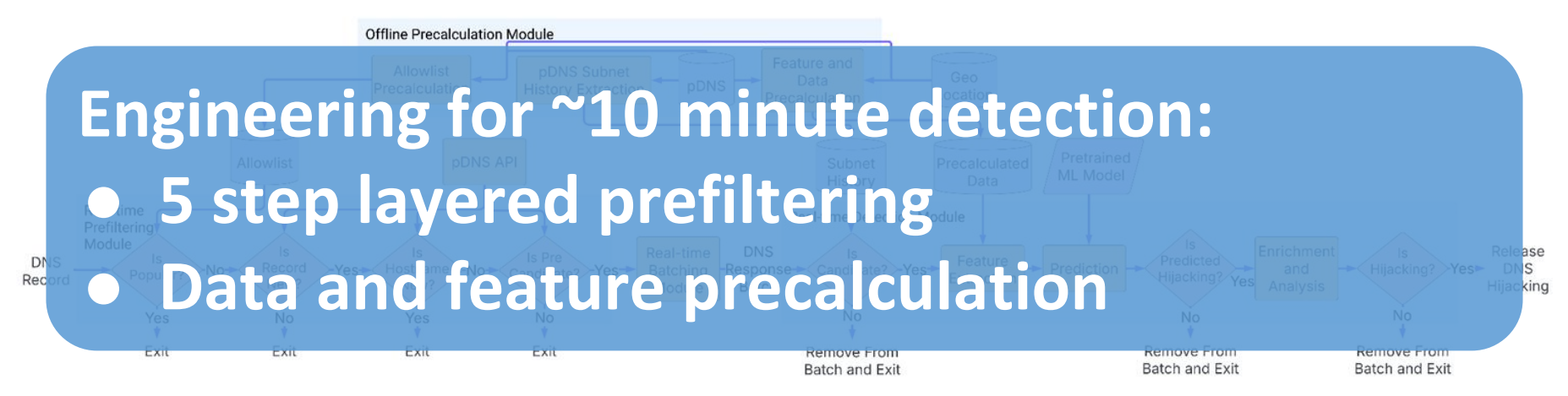


- 90.7 billion new A records
- 1.4 billion candidate records
- 5,121 domain hijack record
- Hijacking: 1 in ~17.7 million new records

Real-time ML Pipeline in Production



Real-time ML Pipeline in Production



Engineering for ~10 minute detection:

- 5 step layered prefiltering
- Data and feature precalculation

Large U.S. utility management company - defaced webpage

Large U.S. utility management company - hijacked DNS record

Hijacked A record

IP	Geolocation/ASN	Last Seen	First Seen
[redacted]	[redacted] US) **ISP name:** [redacted] **Subnet:** [redacted] **ASN:** [redacted]	07/02/2024 18:45 PDT	02/03/2014 20:28 PST
176.9.24.28	Falkenstein, Sachsen, Germany (DE) **ISP name**: Hetzner Online GmbH **Subnet**: 176.9.21.128 - 176.9.49.55 **ASN**: ASNumber: 24940 ASName: "HETZNER-AS, DE")	05/07/2024 08:45 PDT	05/07/2024 08:45 PDT

Large internet service provider - hijacked DNS record

Name Server	Last Seen	First Seen
[redacted]	07/03/2024 16:56 PDT	12/19/2013 22:44 PST
[redacted]	07/03/2024 16:56 PDT	12/19/2013 22:44 PST
ns1.csit-host.com	05/25/2024 20:47 PDT	05/24/2024 11:29 PDT
ns2.csit-host.com	05/25/2024 20:47 PDT	05/24/2024 11:29 PDT

Name server hijacked

Summary

- **Detecting Domain Hijacking from pDNS is possible**
  - In production
  - At scale
  - Real-time
- **Domain hijacking is rare but a regular occurrence**
  - More frequent than previous known hijacking
  - Potentially him impact but most often not as sophisticated: Defacement, phishing, malware, ...

Q&A

Janos Szurdi - szurdi.janos@gmail.com
linkedin.com/in/**szurdi**

Mohammad Ghasemisharif - mghasemishar@paloaltonetworks.com
linkedin.com/in/moebit/