# The DNS Abuse Institute

Survey of ML Approaches to
Preventing Abuse

DNS
ABUSE
INSTITUTE

# The DNS Abuse Institute

- Project of Public Interest Registry
- Mission: Reduce DNS Abuse
- Education, Collaboration, Innovation
- NetBeacon™
- DNSAI: Compass™
- ZOMFG FREE

“

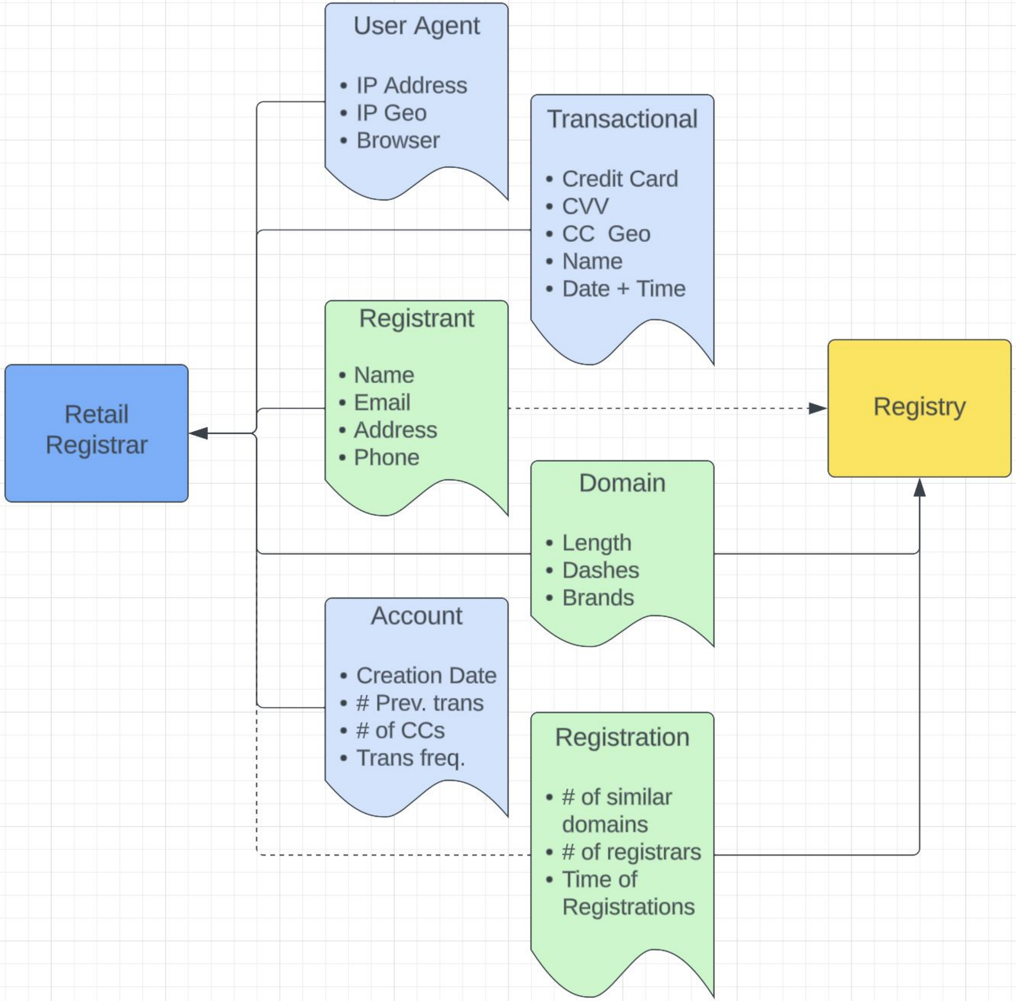
# Can we predict potentially abusive domain names *before* the abuse has happened?

(as  in, before an abusive website resolves or email is sent)

# And now for an important note about outcomes…

- *Detecting* potentially abusive names doesn’t presuppose an action
- Detection could lead to everything from nothing, to deletion of domain
- Plenty of room for reasonable, responsible processes

# Using what data?



# Timeline

| Date | Name | What |
|---|---|---|
| April 2016 | nDEWS: A new domains early warning system for TLDs \| .nl | DNS Lookups and Reg data |
| 24 October 2016 | PREDATOR | Primarily aimed at bulk registrations |
| January 15, 2019 | PaDAWaNS: Proactive Domain Abuse Warning and Notification System \| .nl | Fraudulent web shops |
| 2019 | Domain Watch \| .uk | Domain based |
| 09 December 2019 | PREMADOMA \| .eu | Primarily aimed at bulk registrations |
| 27 March 2021 | Proactive Recognition of Domain Abuse | Thesis / SIDN Labs |
| 27 January 2023 | RegCheck \| .nl | SIDN Labs |

# Who has ML detection in production?

- SIDN / .nl - RegCheck
- EURid / .eu - PREMADOMA
- Nominet / .uk - NameWatch
- Others?

# Three Approaches

- Registration Based - Is the domain likely to have been part of an abusive bulk registration?
- Domain Based - Does the domain have attributes commonly found in abusive names (brands, special terms)
- Registant Based - Is the registrant information ‘correct’

# Class Imbalance Problems

- Abuse is still a tiny fraction of new registrations
- Requires real work to train and balance ML models

# Precision & Recall

**Precision:** Of the predicted abusive names, how many were actually abusive?

**Recall:** How many of the total abusive names were correctly predicted?

- Domain Watch: 60% precision
- RegCheck (live): 22.08% precision, 47.80% recall
- Premadoma (testing): 84.57% precision, 66.23 recall

Is that good? Good is really about what you do with it.

# Potential Issues

- Do registration attribute based models become less relevant as targeting abuse becomes cheaper and easier?
- Will we see abuse move to more sub-domains?
- Are threat feeds reliable/complete enough for training?

# …so, why only (ccTLD) registries?

- ccTLDs have different economics, incentives, and regulatory requirements
- ccTLDs are also more willing to share their work
- Kudos to SIDN Labs for their significant transparency and contributions

# Registrar Approaches

- Far more useful data, especially at the transaction layer
- Overlaps with anti-fraud tools typically from payment processor
- Develop and employ own ML model vs. Pay $0.07 more a transaction?

pir DNS ABUSE INSTITUTE

# Sources

- nDEWS
- PREDATOR
- PREMADOMA
- PaDaWans
- Domain Watch
- Regcheck from SIDN, built on this thesis.