Security Intelligence for TLD Operators

Moritz Müller | SIDN Relatiedag, 1 december 2016, Utrecht

SIDN LABS

Assets van een TLD Operator

- Domeinnamen
- Registrant informatie
- Registrar informatie
- Registratiesysteem (DRS)
- Domein queries (DNS)

SITO

- Probleem: generieke defense tools (zoals Firewalls) ongeschikt
  - Geen inzicht in registratie transacties
  - Geen verstand van DNS-queries en -responses

- SITO = Security Intelligence for TLD Operators

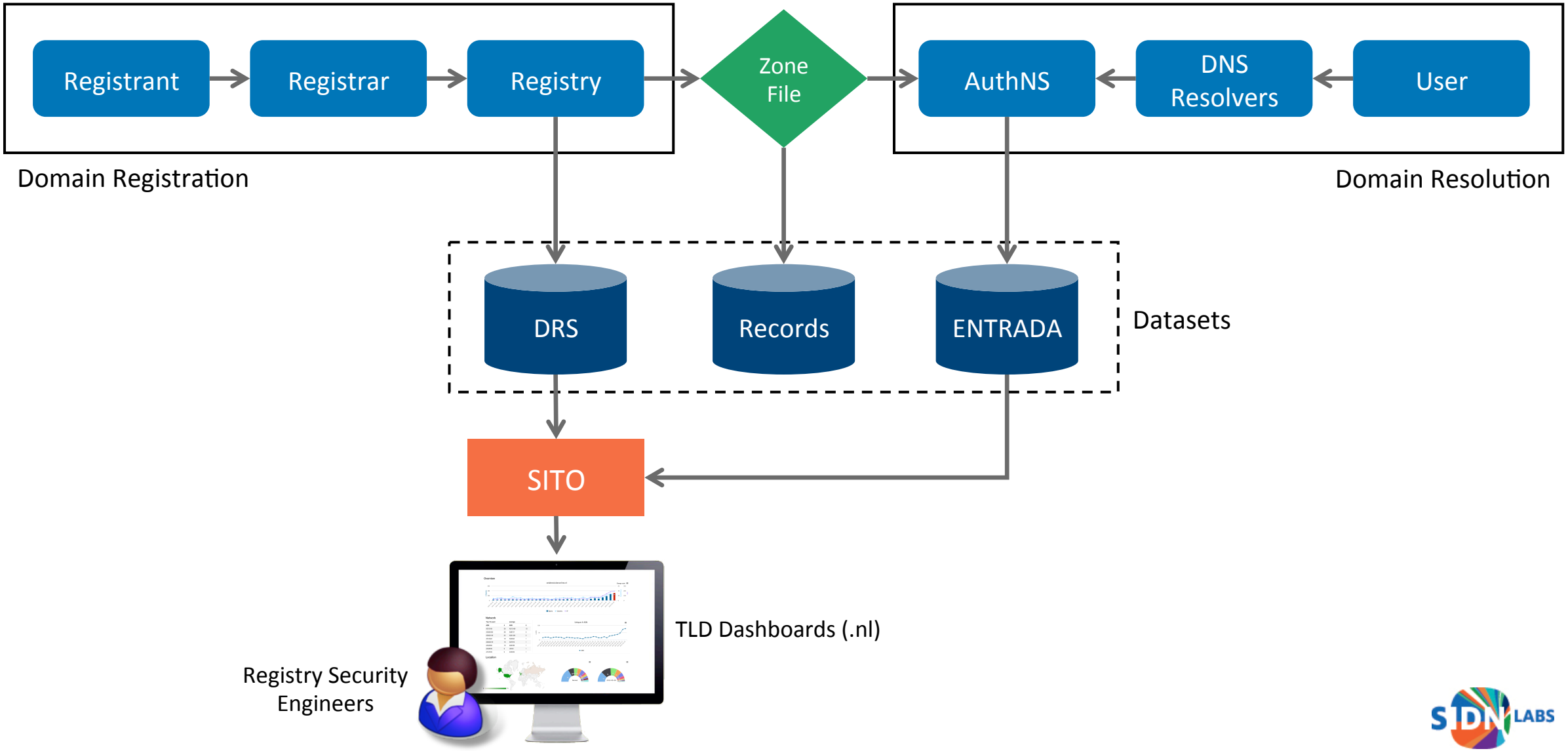
Doel: het automatisch herkennen van

afwijkend gedrag

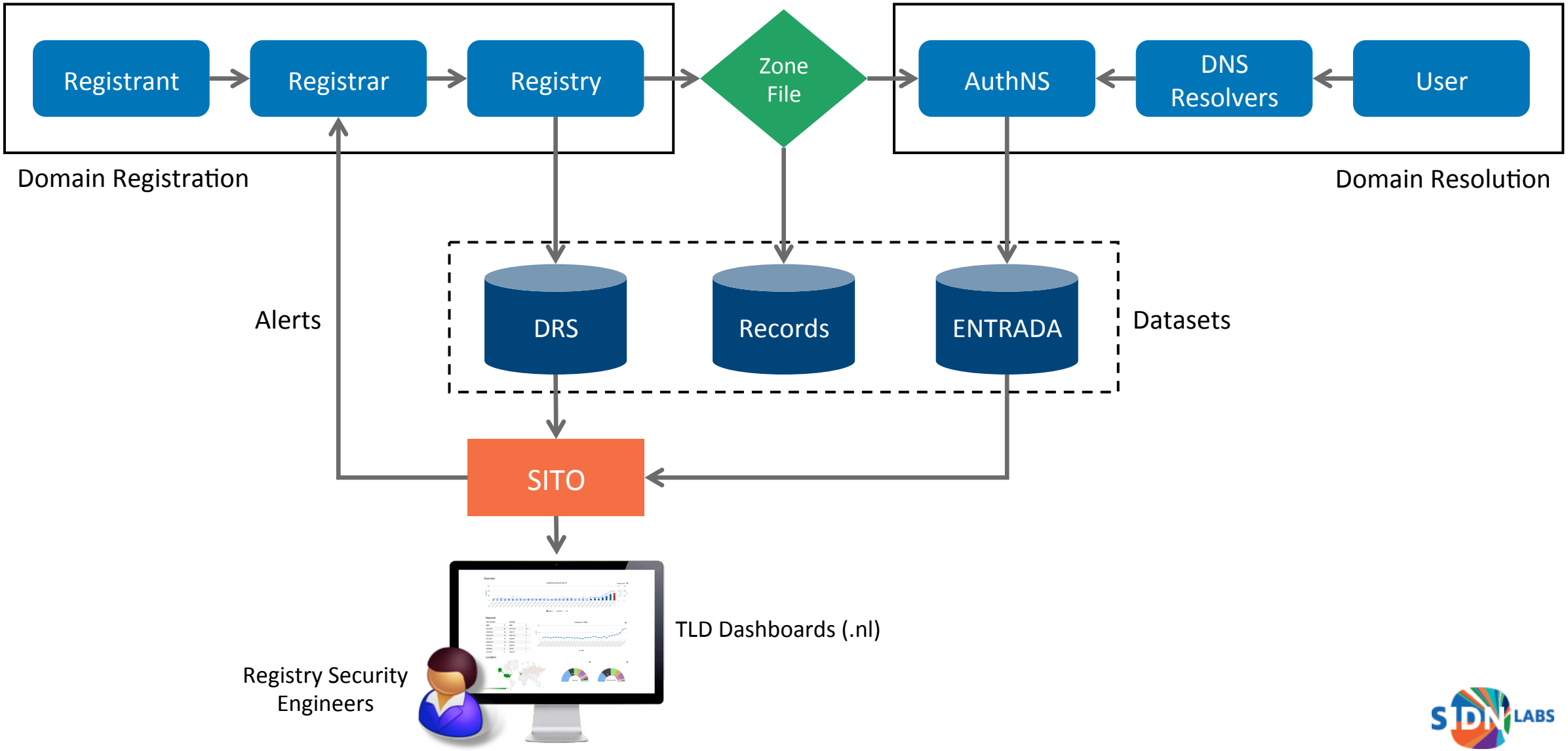
in DRS- en DNS-verkeer om de

integriteit en veiligheid van .nl te beschermen

Overzicht


Registrant
Registrar
Registry
Zone File
AuthNS
DNS Resolvers
User
Domain Registration
Domain Resolution
DRS
Records
ENTRADA
Datasets
SITO
TLD Dashboards (.nl)
Registry Security Engineers

Overzicht


Registrant
Registrar
Registry
Zone File
AuthNS
DNS Resolvers
User
Domain Registration
Domain Resolution
Alerts
DRS
Records
ENTRADA
Datasets
SITO
TLD Dashboards (.nl)
Registry Security Engineers

Voorbeeld transacties

- Domain create: creëren van een nieuwe domeinnaam
- Domain transfer: verhuizen van een domeinnaam naar een andere registrar
- Domain update: veranderen van houdergegevens (b.v. mail of telefoonnummer)
- Name server change: veranderen van name server IP-adres (glue)
- Afwijkingen herkennen (potentieel misbruik) door te berekenen wat “normaal” is

Afwijkende transacties

Verdachte name server updates

- Gebaseerd op IP-adres en land

Ongewone transfers

- B.v. transfer op rare tijdstippen

Mislukte transacties

- B.v. transfer met verkeerde token

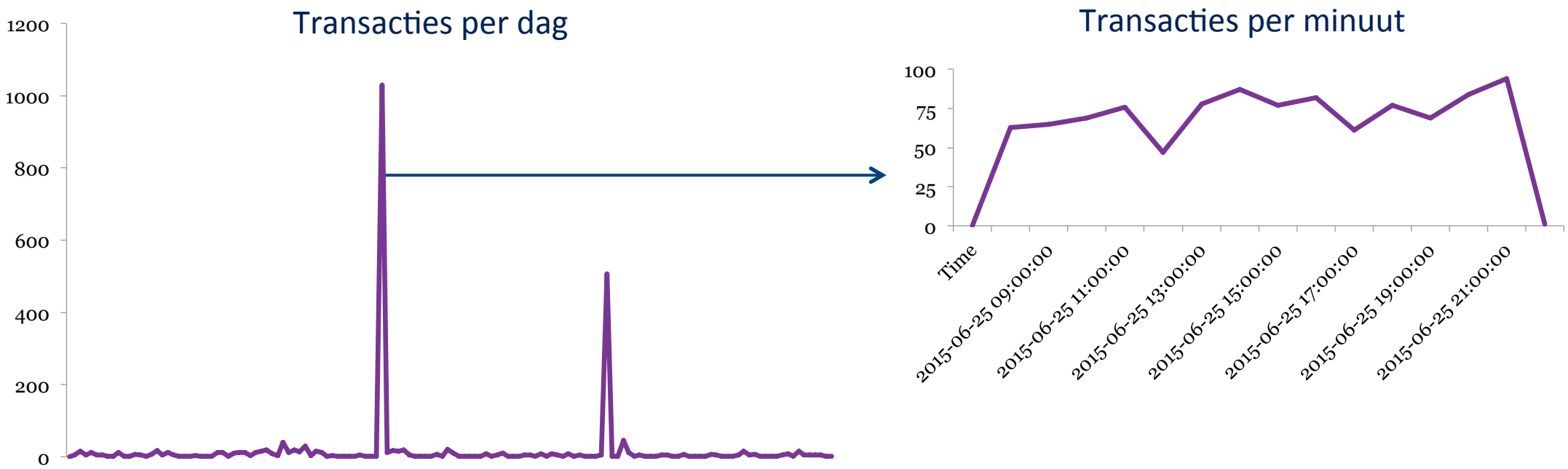
Afwijkende verhuizingen

- Ongewenst verhuizen van domeinnamen
- Registrars hebben vaak een gelijkmatig patroon van verhuizingen
- Eventueel verdacht als op een moment veel domeinnamen worden verhuisd

Mislukte transacties

- Registrar probeert domeinnaam te verhuizen met foute token
- Registrar probeert registrant of name server te wijzigen die niet onder zijn beheer is
- Registrar heeft mislukte logins (EPP of Web)

Voorbeeld



- Mislukte transfers van een registrar
- Meer dan 1.000 verschillende domeinnamen betrokken

Voorlopige resultaten

- Weinig security incidenten in DRS (en dat weten we nu ook)
- Afwijkend gedrag vaak misconfiguratie
- Evaluatie nodig om afwijkend gedrag te prioriteren en beter in te schatten

Voorlopige resultaten

- Weinig security incidenten in DRS (en dat weten we nu ook)
- Afwijkend gedrag vaak misconfiguratie
- Evaluatie nodig om afwijkend gedrag te prioriteren en beter in te schatten

Vragen aan registrars:

Wat zijn andere indicatoren voor security incidenten?

Zijn er andere waardes in de data?

Willen jullie alerts ontvangen? Zo ja, hoe?

Voorbeelden van misbruik van domeinnamen

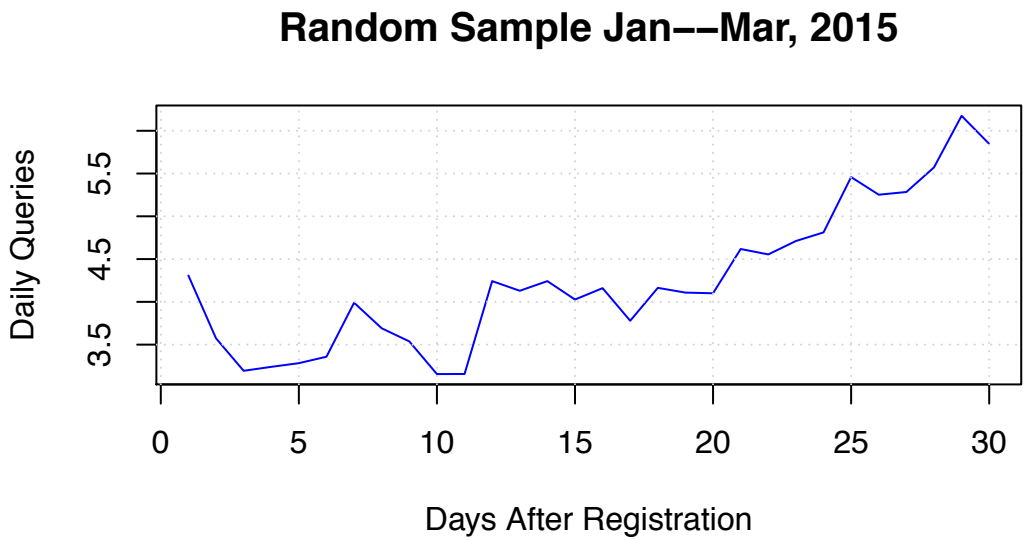
Business	Spam?	Registratie info	DNS Traffic	Records
Phishing (nieuw)	Ja	Zwak	Sterk	Zwak
Phishing (gehacked)	Ja	Geen	Sterk	Zwak
Nepwinkel	Ja	Zwak	Sterk	Zwak
Botnet C&C	Nee	Gemiddeld	Sterk	Gemiddeld
Blackhat SEO	Nee	Gemiddeld	Gemiddeld	Sterk

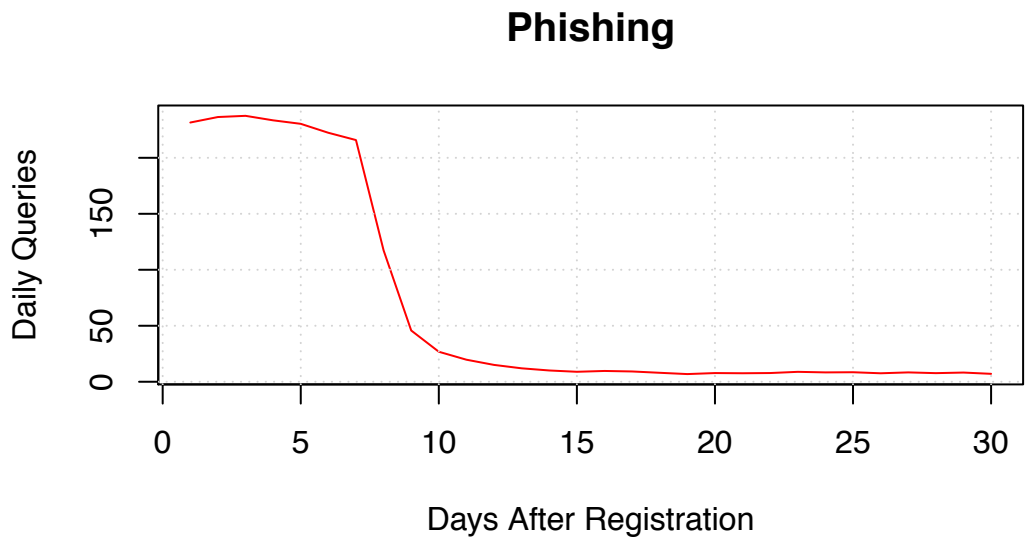
Voorbeelden van misbruik van domeinnamen

Business	Spam?	Registratie info	DNS Traffic	Records
Phishing (nieuw)	Ja	Zwak	Sterk	Zwak
Phishing (gehacked)	Ja	Geen	Sterk	Zwak
Nepwinkel	Ja	Zwak	Sterk	Zwak
Botnet C&C	Nee	Gemiddeld	Sterk	Gemiddeld
Blackhat SEO	Nee	Gemiddeld	Gemiddeld	Sterk

DNS verkeer

- Nieuwe phishing domeinnamen tonen vaak afwijkend DNS verkeer in vergelijking met ongevaarlijke domeinnamen

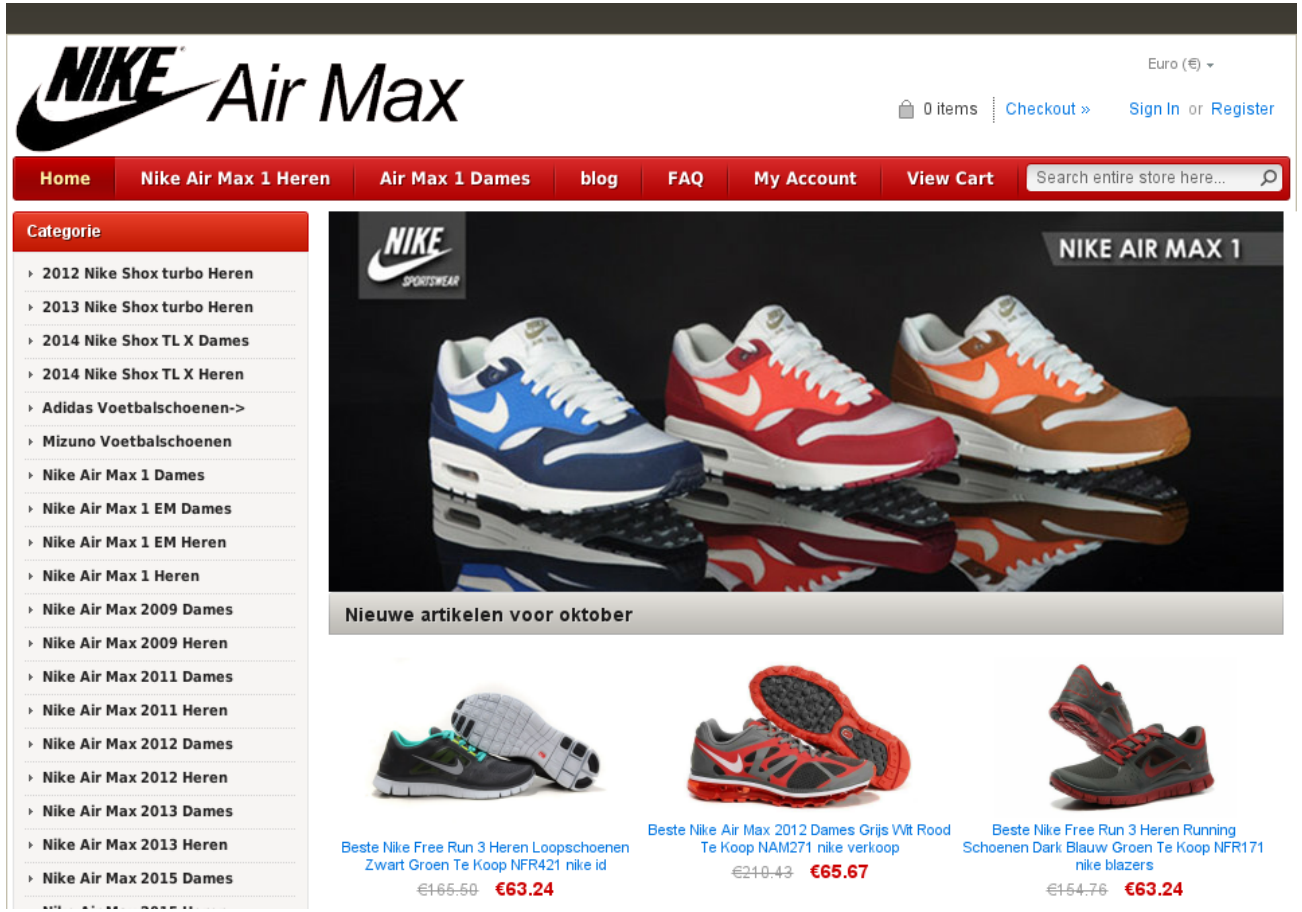




G. Moura, M. Mueller, M. Wullink, and C. Hesselman, *"nDEWS: a New Domains Early Warning System for TLDs"*, IEEE/IFIP International Workshop on Analytics for Network and Service Management (AnNet 2016), Istanbul, Turkey, April 2016

Resultaten nDEWS

- Fake webwinkels, b.v.:
  - Schoenen
  - Medicijnen
- Phishing
- We draaien een pilot



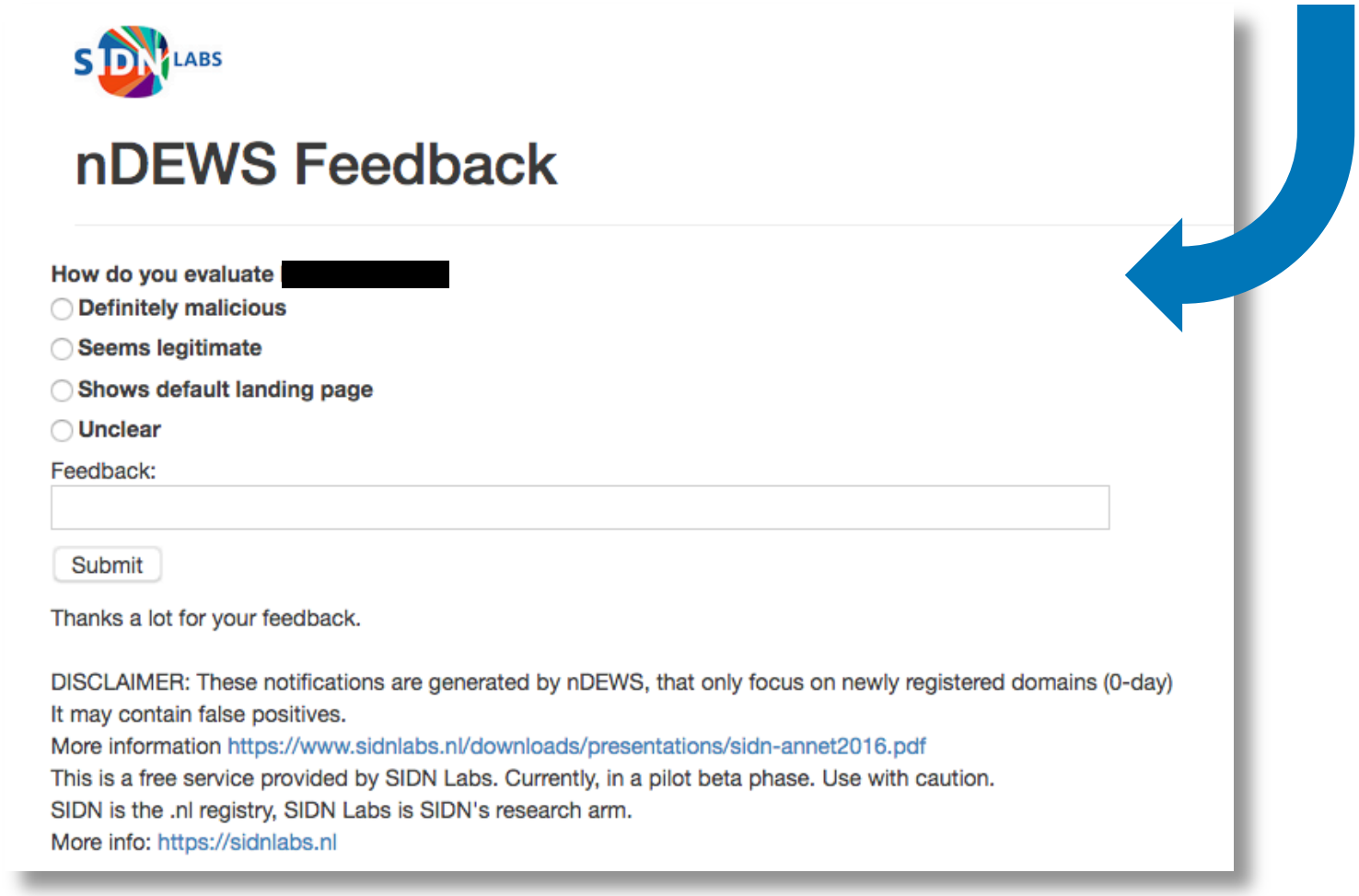
Resultaten nDEWS

- Fake webwinkels, b.v.:
  - Schoenen
  - Medicijnen
- Phishing
- We draaien een pilot

Wij zoeken meer registrars die willen meedoen!

nDEWS email alerts en feedback

```
# domain,Registrar,timestampCreation,TotalRequests,TotalIPs,TotalCountries,TotalASes,FeedbackUrl
example.nl,.,1479376012,8599,3493,124,1386,https://ndews.sidnlabs.nl:5443/ndews/getfeedback/15621685723
```



nDEWS Feedback

How do you evaluate [redacted]

- Definitely malicious
- Seems legitimate
- Shows default landing page
- Unclear

Feedback:

Submit

Thanks a lot for your feedback.

DISCLAIMER: These notifications are generated by nDEWS, that only focus on newly registered domains (0-day)
It may contain false positives.
More information https://www.sidnlabs.nl/downloads/presentations/sidn-annet2016.pdf
This is a free service provided by SIDN Labs. Currently, in a pilot beta phase. Use with caution.
SIDN is the .nl registry, SIDN Labs is SIDN's research arm.
More info: https://sidnlabs.nl

Conclusies en vervolgstappen

- Security intelligence om afwijkend gedrag op te sporen en .nl nog veiliger te maken
- Beschermen van registratie lastig maar belangrijk punt
- Wij zoeken registrars die met onze nDEWS-pilot mee willen meedoen
- We willen de detectie van malafide domeinnamen uitbreiden

Conclusies en vervolgstappen

- Security intelligence om afwijkend gedrag op te sporen en .nl nog veiliger te maken
- Beschermen van registratie lastig maar belangrijk punt
- Wij zoeken registrars die met onze nDEWS-pilot mee willen meedoen
- We willen de detectie van malafide domeinnamen uitbreiden

Vragen?

Moritz Müller

Research Engineer

moritz.muller@sidn.nl

 @dhr_moe

www.sidnlabs.nl