

LEMMINGS: Preventing data leaks

Maarten Wullink & Moritz Müller | CENTR R&D 19

21 October 2021



Agenda

1. The problem
2. The goal
3. LEMMINGS
4. Pilots
5. Evaluation
6. Next steps

The Problem

Data leak caused by deleted domain name



RTL Nieuws
Watch the latest broadcast

News Economy Sport entertainment **Tech** Lifestyle EditionNL Broadcasts

EXCLUSIVE

Major data breach at youth care: files of thousands of vulnerable children leaked

April 10, 2019 4:00 PM
Updated: April 10, 2019 10:30 PM

Image for illustration.

Due to an error at Bureau Jeugdzorg Utrecht, the files of the vulnerable children have been leaked. In the files you will find sensitive information, such as their mental disorders, details of sexual abuse and even suicide attempts.



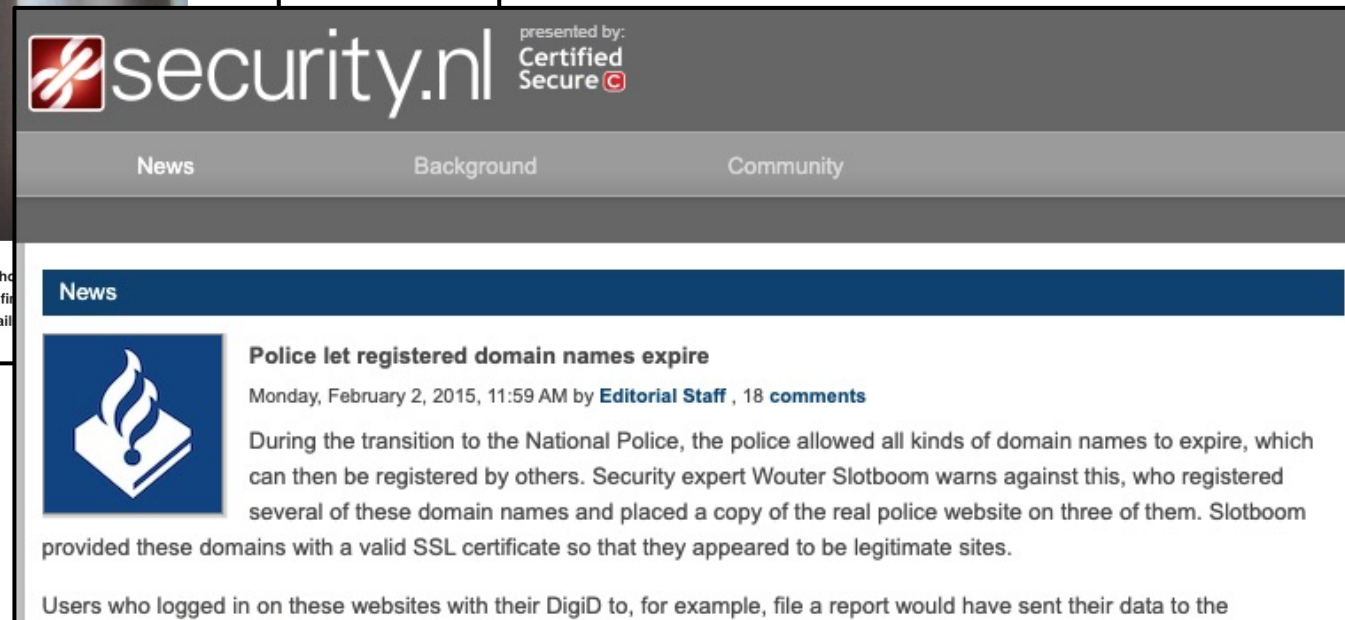
Arnoud Engelfriet
ICTRight

Opinion - October 29, 2020 - 09:10

RTL: BSNs of millions of Dutch people can be seen online due to expired domain name

The health insurance data and social security numbers of millions of Dutch people could be viewed online because a healthcare institution let a domain expire, I [recently](#) read .

...e institution and thus also
...se (a company that provides
...mail addresses. Very painful, and



presented by:
Certified Secure

News Background Community

News

Police let registered domain names expire

Monday, February 2, 2015, 11:59 AM by [Editorial Staff](#) , 18 [comments](#)

During the transition to the National Police, the police allowed all kinds of domain names to expire, which can then be registered by others. Security expert Wouter Slotboom warns against this, who registered several of these domain names and placed a copy of the real police website on three of them. Slotboom provided these domains with a valid SSL certificate so that they appeared to be legitimate sites.

Users who logged in on these websites with their DigiD to, for example, file a report would have sent their data to the



The Goal

- Informing the registrant when a deleted domain name is probably still being used for mail.
 - Do this during the quarantine period
 - Only registrant allowed to restore the domain name

LEMMINGS (deLetEd doMain MaIl warNinG System)

- Rule-based system for:
 - Building filters
 - Analyzing DNS MX query data
 - Sending alerts
- Main challenges:
 - Filter noise caused by unimportant mail (Spam, social media etc.)
 - Make sure registrants understand the problem
 - Not all registrants can be contacted by mail

LEMMINGS (deLetEd doMain Mail warNinG System)

- Data sources:
 - Domainname Registration System
 - DNS Resolver data (ENTRADA)
 - SIDN Web Crawler
 - Abuse Feeds (APWG/Spamhaus)
 - Sinkhole domain names

LEMMINGS Filters

Only count legitimate mail traffic, remove noise using filters:

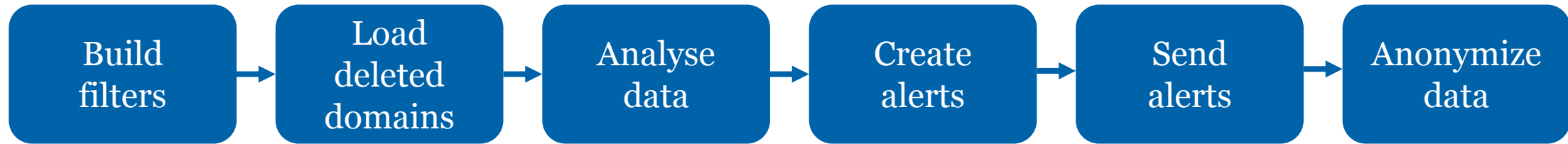
- Spamhaus/APWG
- Custom ASN/IP (known bulkmail senders)
- Open Resolvers
- New IP-addresses
- Senders to high % of no-mail domains
- Senders to high % of NXDOMAIN domains
- Keyword list (high risk professions)
- List of NACE codes (high risk businesses)

Scoring Rules

- On day 30 of quarantine period, evaluate the previous 10 days
- 3 severity levels: low, moderate, high
 - Based on average # of daily MX-queries over the previous 10-day period:
 - <= 5 then low
 - > 5 and <= 10 then moderate
 - > 10 then high
- Use amplifier for special conditions:
 - When keyword OR NACE code match then high
 - When Email address published on website then at least moderate

LEMMINGS Workflow

Every day at 09:00 AM



DNS-data
Abuse feeds

Domain
Registration
System

Filters
DNS-data
Webcrawler

Scoring rules
Analyzer statistics

Alert Design

- Keep message short as possible
 - Created webpage¹ to provide more detailed FAQ
- Assume recipient has zero technical knowledge
- 3 severity levels (low ≤ 5 , moderate ≤ 10 , high > 10)
- Multi-language (MIME) message
- Evaluation of message using survey among SIDN customers

Belangrijke informatie over je opgezegde domeinnaam



Belangrijke informatie over je opgezegde domeinnaam zovintage.nl

Er is mogelijk nog mailverkeer naar de domeinnaam

An English version of this e-mail can be found at www.sidn.nl

Dit is een bericht van SIDN, wij beheren het .nl-domein en ook de domeinnaam zovintage.nl. Je hebt deze domeinnaam opgezegd op 2021-07-28. Met het opheffen van zovintage.nl vervallen ook alle daaraan gekoppelde e-mailadressen. We sturen je dit bericht, omdat er waarschijnlijk nog gemaïld wordt naar een of meerdere e-mailadressen die gekoppeld waren aan de opgezegde domeinnaam. Hier schuilt een risico in. We vertellen je er graag meer over.

Wat is er aan de hand?

Als beheerder van de .nl-domeinnamen kunnen we zien dat er waarschijnlijk nog gemaïld wordt naar mailadressen die gekoppeld waren aan de opgezegde domeinnaam. Het zou dus kunnen zijn dat er nog voor jou of je organisatie bestemde mail naar oude mailadressen wordt gestuurd. Vanaf 2021-09-06 kan de domeinnaam door een ander geregistreerd worden. Het risico bestaat dat deze nieuwe houder toegang krijgt tot de voor jou bestemde mails die dan nog verstuurd worden. Daarmee kan er mogelijk voor jou of je organisatie bestemde persoonlijke en/of gevoelige informatie in handen van derden komen, met alle gevolgen van dien.

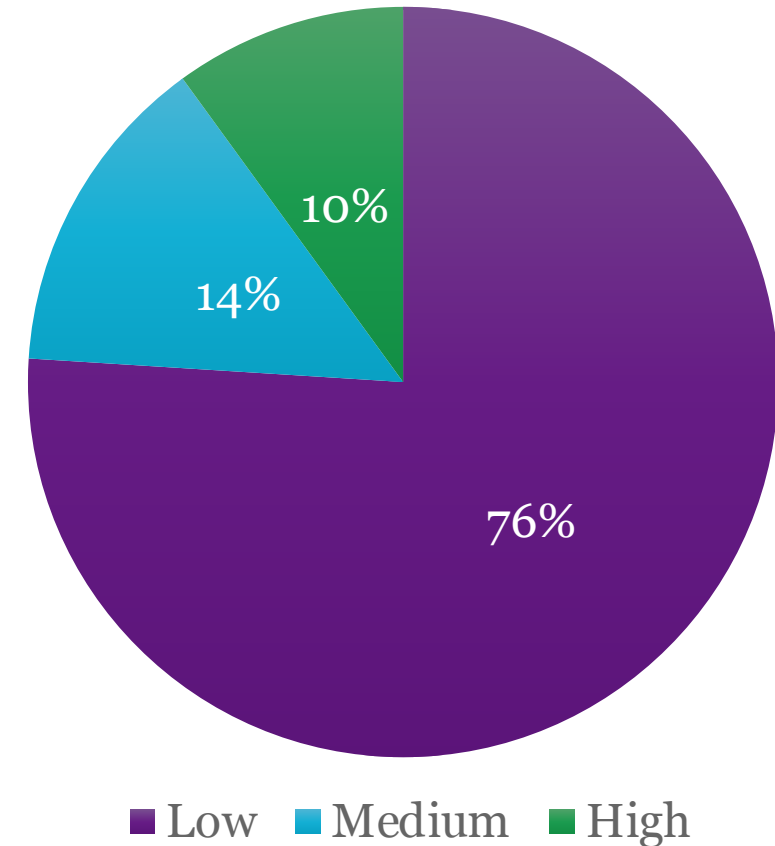
NB. We benadrukken graag dat we niet kunnen zien om welke mailadressen het gaat. Ook kunnen wij de mails zelf en de inhoud daarvan niet zien.

1) <https://www.sidn.nl/en/nl-domain-name/mail-traffic-to-cancelled-domain-names>

LEMMINGS Statistics – in theory

- Monitoring active since: 2021-04-23
- Domain names classified: 430,408
- Potentially warned domain names: 25.184
(5.9% of domain names classified)
- Potentially warned domain names per day:
146 domains on average (max 765 on one day)

Domains per risk category



LEMMINGS Statistics – in practice

2 Pilots:

- Argeweb
 - ~ 150.000 .nl domain names
 - Since 2021-06-05
- Registrar.eu
 - ~ 600.000 .nl domain names
 - Since 2021-09-15



Argeweb Pilot

- Medium scale registrar
- Actively informing registrants before cancelling a domain name
- 622 notified domain names
- 2 domains taken out of quarantine

Argeweb Pilot

- Medium scale registrar
- Actively informing registrants before cancelling a domain name
- 622 notified domain names
- 2 domains taken out of quarantine



Registrar.eu Pilot

- Large scale registrar
- Many resellers
- 259 notified domain names
- 0 domains taken out of quarantine

Registrar.eu Pilot

- Large scale registrar
- Many resellers
- 259 notified domain names
- 0 domains taken out of quarantine



Pilots: The Good Side

- Number of complaints: 0
- Positive feedback from the community



Photo by MARK ADRIANE on Unsplash

Open Questions

- Do people read our email?
- Do people understand our email?
- Do people care?
- Did the domain names still receive relevant email?
- Are there other/better filters?

Next Steps

- Working together with people that care: CERTs
- Scale up pilot
- Contact registrants

Follow us

 SIDN.nl

 @SIDN

 SIDN

Thank you for your attention!