

The current state of DNS Lame delegations

An analysis of the current state of lame delegations within the Swedish .se tld

Student:

Alexander Blaauwgeers
`alexander.blaauwgeers@os3.nl`

University of Amsterdam
Research Project 2
Student Project Presentation

Supervisor:

Arris Huijgen
`ahuijgen@deloitte.nl`

September 16, 2020

 <https://www.scmagazine.com/home/opinions/data-breaches-caused-by-misconfigured-servers/>

December 26, 2018

Data Breaches Caused by Misconfigured Servers



Misconfigured server infrastructure is often considered one of the most significant causes of data breaches within the IT industry. This human error phenomenon is usually unintentional, but it can have catastrophic consequences regarding the exposure of sensitive personal information as well as potentially damaging the reputation of your business.

Introduction: Relevance 2/2

Source: <https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-cloud-adoption-risk-report-iaas.pdf>

REPORT



Cloud-Native: The Infrastructure-as-a-Service (IaaS) Adoption and Risk Report

McAfee Report Demonstrates Cloud-Native Breaches Differ Greatly From Malware Attacks of the Past

*Report uncovers that 99 percent of **misconfiguration** incidents in public cloud environments go undetected, exposing companies to data loss*

Introduction: Problem statement 1/4

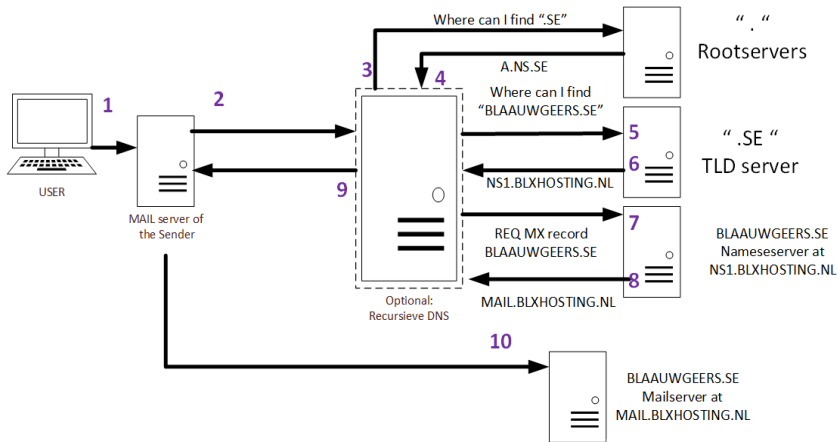


Figure: Normal function of DNS

Introduction: Problem statement 2/4

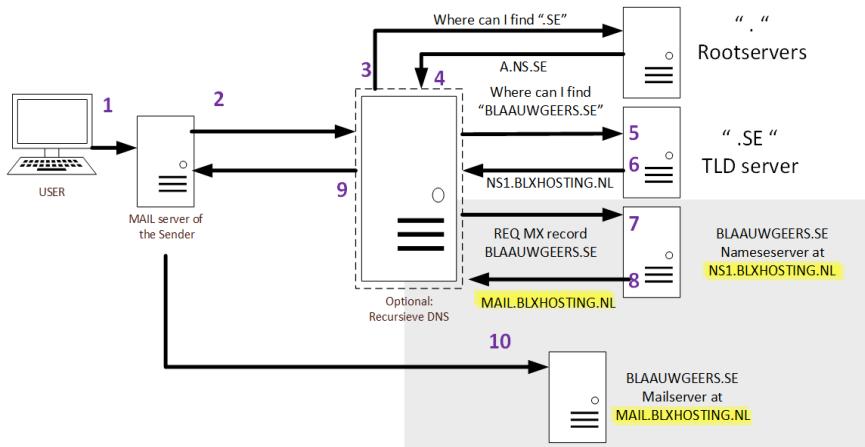


Figure: Normal function of DNS, focus on BLKhosting

Introduction: Problem statement 3/4

```
root@dnsse2:~# dig SOA blxhosting.nl +authority

;<<>> DiG 9.16.1-Ubuntu <<>> SOA blxhosting.nl +authority
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 64901
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:;, udp: 512
;; QUESTION SECTION:
;blxhosting.nl.          IN      SOA

;; AUTHORITY SECTION:
nl.                      0      IN      SOA      ns1.dns.nl. hostmaster.domain-registry.nl. 2020091337 3600 600 2419200 600

;; Query time: 11 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sun Sep 13 20:11:25 CEST 2020
;; MSG SIZE rcvd: 113

root@dnsse2:~# whois blxhosting.nl
blxhosting.nl is free
root@dnsse2:~#
```

Figure: BLKhosting.nl as example

Introduction: Problem statement 4/4

```
$ORIGIN blaauwgeers.se. ; default zone domain
$TTL 5 ; default time to live

@ IN SOA ns1.blaauwgeers.amsterdam. netmaster.blaauwgeers.eu. (
    2020081800 ; serial number
    5 ; Refresh
    5 ; Retry
    5 ; Expire
    5 ; Min TTL
)

NS ns1.blaauwgeers.amsterdam.
NS ns2.blaauwgeers.amsterdam.
A
AAAA
MX 5 mail.newhosting.nl.
MX 10 mx2.blxhosting.nl.
MX 20 mx3.c24ef6fffee9417bd41ceeb1b8a30b3284f5cf94.se
```

Figure: Blaauwgeers.se Zonefile

Project: Research question

The main question for this research is:

Are the domains below the Swedish .se tld vulnerable for lame delegation take-over?

The research question can be divided into multiple sub-questions:

- 1 What are **lame records** and what are possible **security implications** caused by them?
- 2 How many lame records are there within the .se tld?
- 3 Can we identify any **top talkers** among them?


- **In-scope:**

- ▶ This research focus study lame delegations on the **Swedish .se ccTLD**.¹
- ▶ We have chosen the .se tld because the **zone file has been published**.
- ▶ **Delegations which point from** the .se tld to outside are also within scope.
- ▶ The focus of the project will be delegations which are vulnerable to **takeover** by others *to retrieve email*.

- **Out-of-scope:**

- ▶ Third level records below the APEX.
- ▶ Delegations which are below the APEX like CNAME, SRV, and Third level delegations NS.
- ▶ e.g. student.mau.se

- **Goal:** A framework for detection of Lame delegations

¹ICANN assigned the ccTLD ".se" to Sweden based on ISO_3166-1 

Project: Related Work

- David Barr: ² "**Running a nameserver is not a trivial task.** There are many things that can go wrong, and many decisions have to be made about what data to put in the DNS and how to set up servers."
- Amreesh Phokeer ³ has performed a case-study of lame records within the reverse DNS Records in the African Region. In this study it was found that 45% of all reverse domains are lame within the African IP space. However, this research was performed on PTR records pointer records instead of delegations used in functions like the mail system.
- Pappas classified lame delegations in three different categories, depending on the type of error found. ⁴
 - ① Type 1: Non responding server
 - ② Type 2: DNS error indication
 - ③ **Type 3: Non-authoritative answer (!)**

²Common DNS Operational and Configuration Errors rfc1912

³Amreesh Phokeer at all. "DNS Lame delegations: A case-study of public reverse DNS records in the African Region". Springer. 2016,pp. 232–242

⁴Pappas, V., et al.: Impact of configuration errors on DNS robustness. IEEE J. Sel. Areas Commun. 27(3), 275–290 (2009)

Methodology: Approach with stages

- S0 : Zone transfer(AXFR)**
- S1 : The authoritative name server of the .se domain**
- S2 : Checking the authority of the delegation**
- S3 : Checking the registration of the delegation**
- S4 : Manual verification of the results**

Methodology: (0) Zone transfer (AXFR)

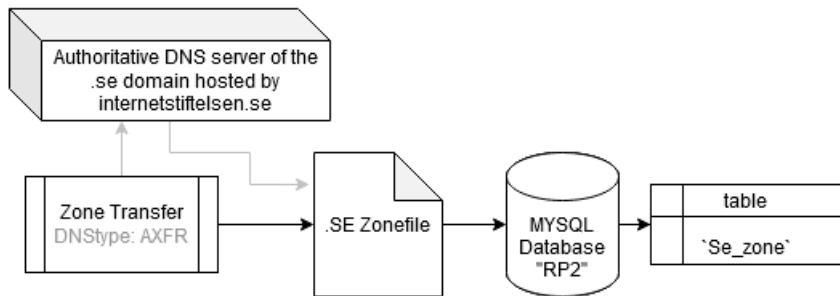


Figure: Stage 0

IN: dig @zonedata.iis.se se AXFR

OUT: INSERT INTO 'se_zone' ('id', 'label', 'ttl', 'class', 'rtype', 'data') VALUES (NULL, 'LABEL.SE', '3600', 'IN', 'NS', 'NS.SERVER.DE')

Methodology: (1) The authoritative name server of the .se domain

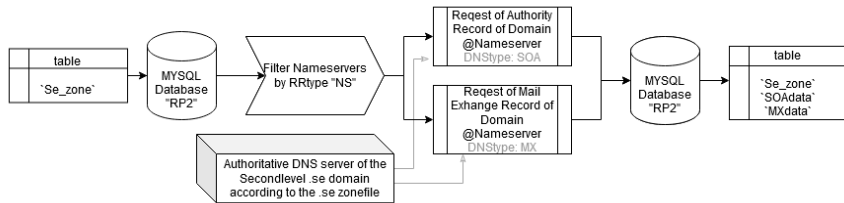


Figure: Stage 1 - Verification of the authoritative name servers of each domain

```
IN: SELECT 'label', 'data' AS 'nameserver' FROM 'se_zone' WHERE  
'rtype' = "NS";
```

```
DO: dig $label @$nameserver SOA
```

```
DO: dig $label @$nameserver MX
```

```
OUT: INSERT INTO ... SOAdata | MXdata
```

Methodology: (2) Checking the authority of the delegation

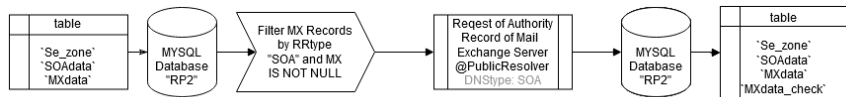


Figure: Stage 1

IN: SELECT 'id','zonelink','rcode','PREFERENCE','EXCHANGE' FROM
'mxdata';

DO: dig \$EXCHANGE @8.8.8.8 SOA

OUT: INSERT INTO ... MXdata_check

Methodology: (3) Checking the registration of the delegation

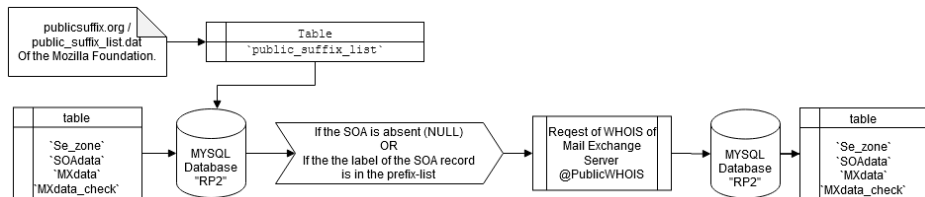


Figure: Stage 2

A "public suffix" is one under which Internet users can (or historically could) directly register names. Some examples of public suffixes are .com, .co.uk and pvt.k12.ma.us. The Public Suffix List is a list of all known public suffixes as an initiative of Mozilla Foundation.

Methodology: (4) Manual verification of the results

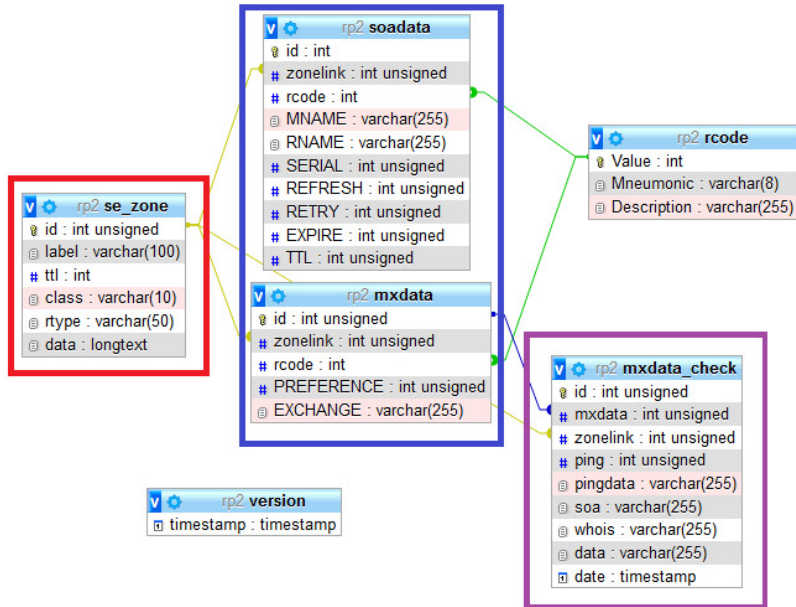
```
mysql> SELECT se_zone.label, soadata.*, rcode.* FROM soadata LEFT JOIN rcode ON rcode.value = soadata
+-----+-----+-----+-----+-----+-----+
| label          | id  | zonelink | rcode | Mnemonic | Description |
+-----+-----+-----+-----+-----+-----+
| 100procentkrokom.se. | 2607 | 5990 | 0 | NOERROR | No error condition. |
| 100procentkrokom.se. | 2608 | 5991 | 1 | FORMERR | The name server was unable to interpret the request due to a format error. |
| 100procentkrokom.se. | 2609 | 5992 | 0 | NOERROR | No error condition. |
| 100procentlevande.se. | 2610 | 5997 | 0 | NOERROR | No error condition. |
+-----+-----+-----+-----+-----+-----+
10 rows in set (0.01 sec)
```



```
mysql> select * FROM se_zone WHERE label = "100procentkrokom.se." AND rtype = '
+-----+-----+-----+-----+-----+-----+
| id  | label          | ttl  | class | rtype | data          |
+-----+-----+-----+-----+-----+-----+
| 5990 | 100procentkrokom.se. | 86400 | IN     | NS    | ns1.mittmedia.se. |
| 5991 | 100procentkrokom.se. | 86400 | IN     | NS    | ns2.mittmedia.se. |
| 5992 | 100procentkrokom.se. | 86400 | IN     | NS    | ns3.mittmedia.se. |
+-----+-----+-----+-----+-----+-----+
3 rows in set (16.51 sec)
```

Figure: M

Proof of Concept



Proof of Concept

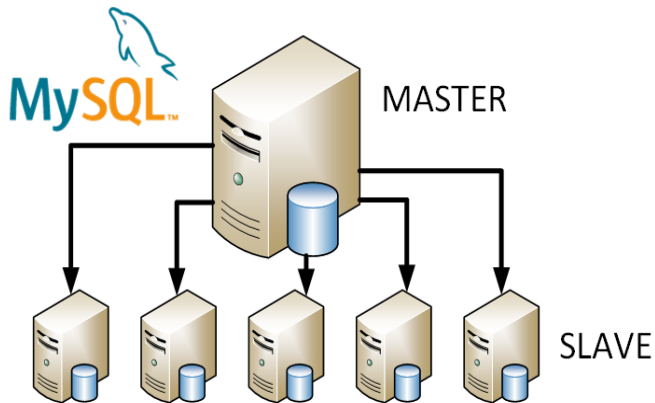



Figure: Database

Result:

- The .se domain had 1530949 active domains on 29th of July 2020. ⁵
- The .se domain had 1471380 active domains with at least one NS record. ⁶
- The Swedish domains are pointing to 360 mail servers on domains which are not registered.
 - 287 domains are pointing to them self and got deleted.
 - 71 mail servers, does not exist, but have other .se domains pointing via MX.
 - ★ 27 of the 71 are within the .se domain
 - ★ 125 se-domains are pointing to 71 non-existing servers.
 - ★ We identified a few top talkers, one with 52 domains pointing.

⁵<https://internetstiftelsen.se/en/domain-statistics/growth-se/>

⁶`(SELECT COUNT(DISTINCT 'se_zone','label') FROM 'se_zone' WHERE 'se_zone'. 'rtype' LIKE "NS")` 

Discussion

- Lot of domains got removed last month including **domains which got removed after step 0**.
- Some special domains are not in the prefix list. Like .google.
- "Main fault are missing "." dots like "ASPMX4GOOGLEMAIL.COM." or "mailclusterloopia.se."

Active domains the last 90 days

Source: <https://internetstiftelsen.se/en/domain-statistics/growth-se/>



Figure: Active domains the last 90 days

The main question for this research is:

Are the domains below the Swedish .se tld vulnerable for lame delegation take-over?

The research question can be divided into multiple sub-questions:

- 1 What are lame records and what are possible security implications caused by them?
- 2 How many lame records are there within the .se tld?
- 3 Can we identify any top talkers among them?

- Perform the framework on different TLD's
- Perform the framework on a regular basis and analyse the difference.
- Improve the framework, e.g. third level and other resource record types like SRV, DNAME and CNAME.
- Improve performance of the the Proof of Concept (database, code, speed)

Closing: Questions? - Thank you for your attention

