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

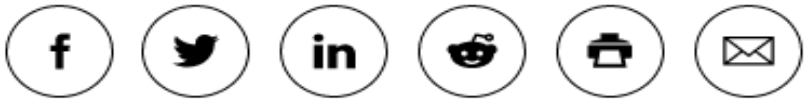
September 16, 2020

Introduction: Relevance 1/2

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

December 26, 2018

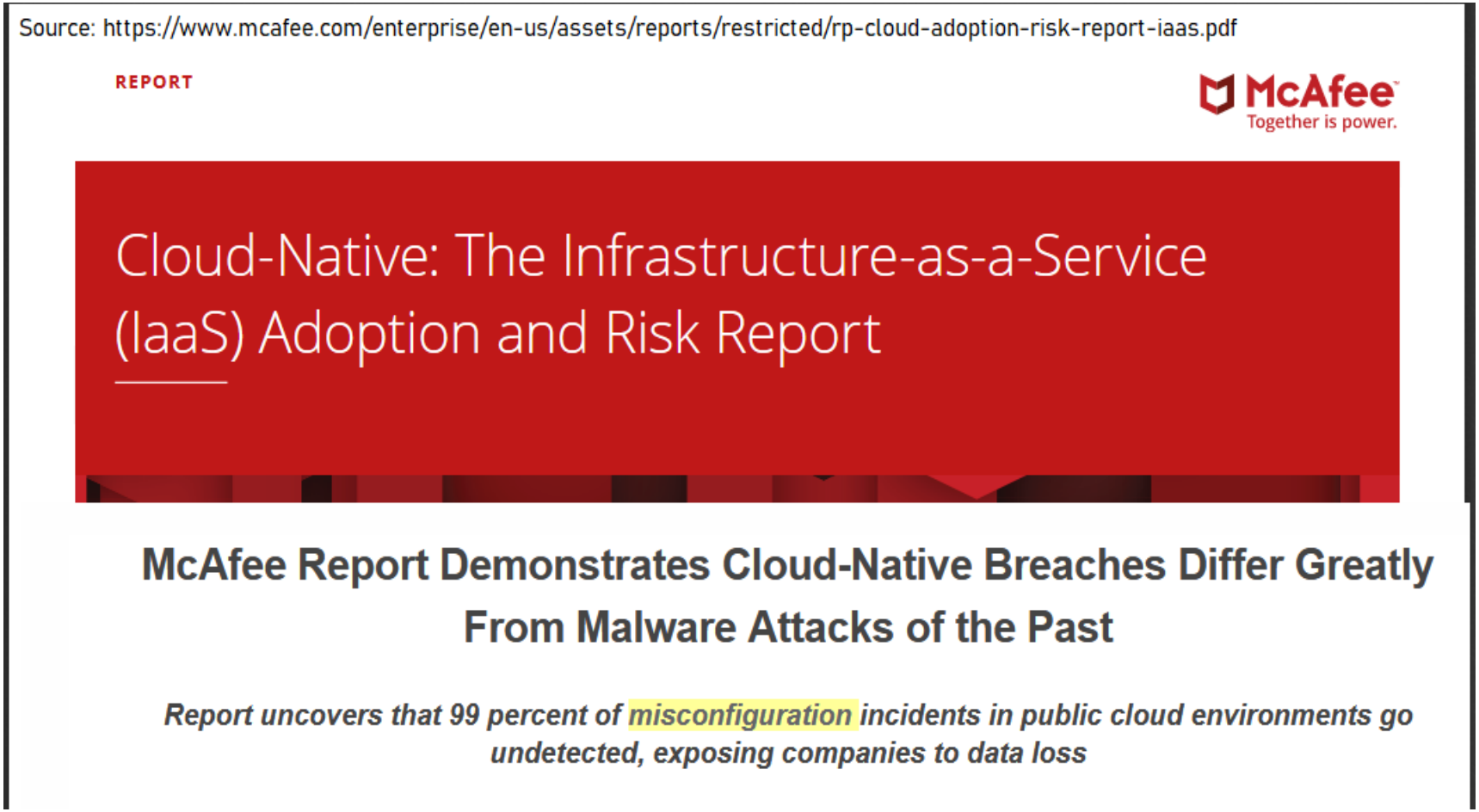
Data Breaches Caused by Misconfigured Servers



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



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

Figure: BLKhosting.nl as example

Introduction: Problem statement 4/4

Figure: Blaauwgeers.se Zone le

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:

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

Project: Scope

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

[1] ICANN assigned the ccTLD ".se" to Sweden based on ISO3166-1

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 abo 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 classi ed lame delegations in three di erent categories, depending the type of error found.[4]

Type 1: Non responding server
Type 2: DNS error indication
Type 3: Non-authoritative answer (!)

---

[2] Common DNS Operational and Con guration Errors rfc1912

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

[4] Pappas, V., et al.: Impact of con guration 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 veri cation of the results

Methodology: (0) Zone transfer(AXFR)

Figure: Stage 0

IN: dig @zonedata.iis.se se AXFR
OUT: INSERT INTO `sezone` (`id`, `label`, `ttl`, `class`, `rtype`, `data`) VALUES (NULL, 'LABEL.SE', '3600', 'IN', 'NS', 'NS.SERVER.DE')

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

Figure: Stage 1 - Veri cation 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 delegati

Figure: Stage 1

IN: SELECT `id`,`zonelink`,`rcode`,`PREFERENCE`,`EXCHANGE` FROM `mxdata`;
DO: dig $EXCHANGE @8.8.8.8 SOA
OUT: INSERT INTO ... MXdatacheck

Methodology: (3) Checking the registration of the delegation

Figure: Stage 2

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

Methodology: (4) Manual veri cation of the results

Figure: M

Proof of Concept

Proof of Concept

Figure: Database

Results

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 Swedisch domains are pointing to 360 mail servers on domains which 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 identi ed 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 `sezone` WHERE `sezone`.`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 pre x list. Like .google.
"Main fault are missing "." dots like "ASPMX4GOOGLEMAIL.COM." or "mailclusterloopia.se.

Figure: Active domains the last 90 days

Conclusion

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:

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

Future work

Preform the framework on di erent TLD's

Preform the framework on a regular basis and analyse the di erence.

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)