Complex DNS misconfigurations

ambiguous responsibility and ICANN

Agenda

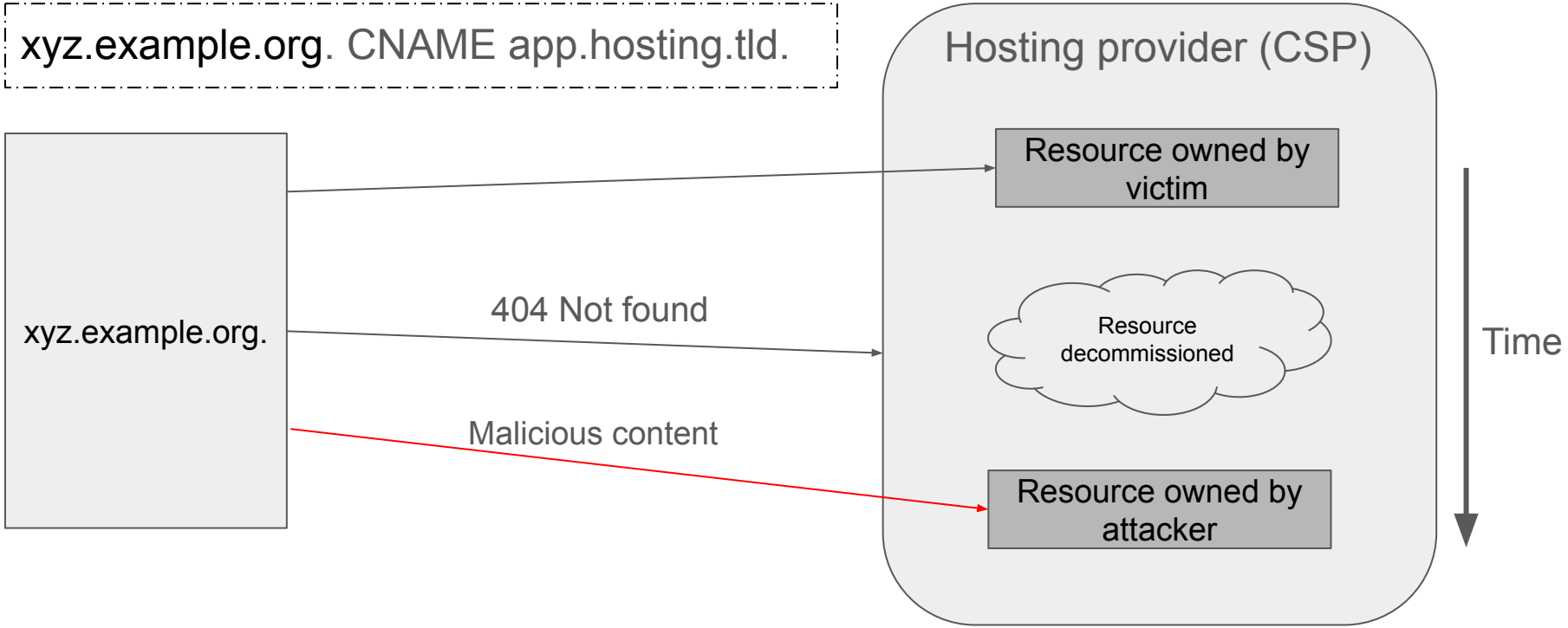
- Introduction
- Subdomain takeover
- ICANNs role in safety norm building
- My recommendation

Introduction

Hi! I’m Movitz Sunar, a Swedish student of Political Science

- Please talk to me about…
  - DNS, the internet, web standards, browsers, CTFs
  - National and/or Cyber Security
  - Anything else!

What is subdomain takeover?

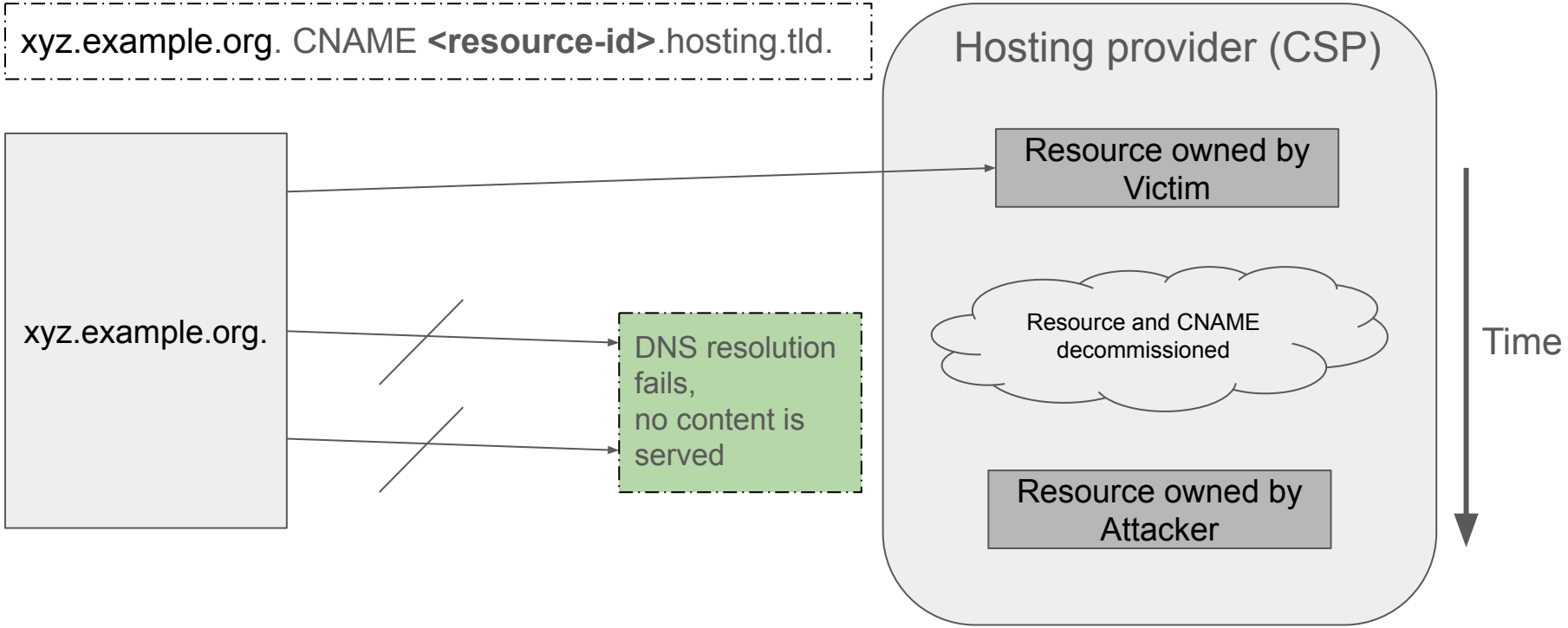


Subdomain takeover is very common!

- It requires
  - The CSP to provide generic CNAME targets
  - The customer to leave dangling DNS records after resource is decommissioned
- It can lead to
  - Targeted phishing on trusted domains
  - SEO spam on high reputation domains
  - Same-site attacks

- All of the major cloud providers have been affected
- Too many orgs are vulnerable

How to mitigate subdomain takeover as a hosting provider



Whose responsibility is it?

- ICANN/IETF can't prevent insecure use of DNS
- CSPs can’t be held responsible for customers invalid DNS records
- CSPs seldom warn customers of the vulnerability
- Customers only follow CSP instructions, exposure is hard to detect

However, only the CSP can fully mitigate the risks!

ICANNs role in safety norm building

MANRS - routing safety norms

KINDNS - only includes DNS operators, not CSP/SaaS

DSFI-TSG: recognized the risk in 2021, no relevant recommendation

The subdomain takeover risk producers are not well represented in ICANN:

How can they be included in norm building?

Recommendation: normalize CSP responsibility through public accountability

1. Declare subdomain takeover protection as norm
2. Actively seek out risk producers, enquire/investigate vulnerability
3. Publically track status of mitigation implementation

Questions? Objections?

movitz.sunar(at)gmail.com

Movitz Sunar on LinkedIn