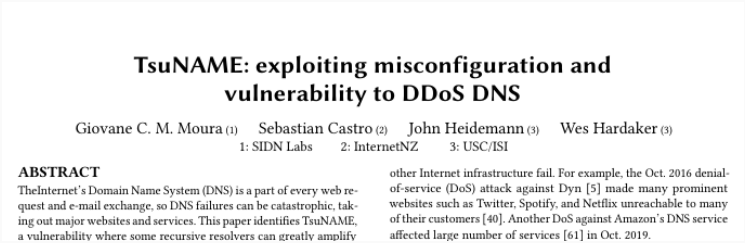
Responsible Disclosure: the TsuNAME case

Giovane C. M. Moura
SIDN Labs/TU Delft

RIPE83
Virtual Meeting
2021-11-22

Case study: TsuNAME

1. We found a DNS vulnerability (ACM IMC2021)



TsuNAME: exploiting misconfiguration and vulnerability to DDoS DNS

Giovane C. M. Moura (1) Sebastian Castro (2) John Heidemann (3) Wes Hardaker (3)
1: SIDN Labs 2: InternetNZ 3: USC/ISI

ABSTRACT

TheInternet's Domain Name System (DNS) is a part of every web request and e-mail exchange, so DNS failures can be catastrophic, taking out major websites and services. This paper identifies TsuNAME, a vulnerability where some recursive resolvers can greatly amplify other Internet infrastructure fail. For example, the Oct. 2016 denial-of-service (DoS) attack against Dyn [5] made many prominent websites such as Twitter, Spotify, and Netflix unreachable to many of their customers [40]. Another DoS against Amazon's DNS service affected large number of services [61] in Oct. 2019.

   - Paper: https://www.isi.edu/~johnh/PAPERS/Moura21b.pdf
   - Video (MAPRG @ IETF112): https://youtu.be/U04MXLvQKjw?t=461
2. We carried out responsible disclosure
   - This talk: we share our experience

SIDN LABS TU Delft

Finding a vulnerability

- So you've found a **vulnerability**
  - protocol, software, hardware ...
- For most of us, this is a ***rare*** event
- What to do in these cases?
  - Default: responsible disclosure ?
- How does that work **in practice**?

SIDN LABS TU Delft

Finding a vulnerability

- So you've found a **vulnerability**
  - protocol, software, hardware ...
- For most of us, this is a ***rare*** event
- What to do in these cases?
  - Default: responsible disclosure ?
- How does that work **in practice**?

SIDN LABS TU Delft

This talk

- **Goal:** share our experience
- It may help others in the future
- Show our **mistakes**
- Show what went well

SDM LABS TU Delft

Disclaimer

- Our sample size is ...

Disclosing a vulnerability: 4 options

1. Private disclosure (vendor only)
2. Public disclosure (everyone at the same time)
3. Responsible disclosure (both of the above)
4. Go rogue:
   - https://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html
   - Public interest not priority

Vendor	Public
Private Disclosure	Public Disclosure
Responsible Disclosure	

SIDN LABS TU Delft

Private Disclosure

Vendor	Public
Private Disclosure	Public Disclosure
Responsible Disclosure	

- You tell only the vendor
- They decide if they want to fix or not
- Pretty much `defunct`
- Vendors would simply ignore researchers
- More: https://www.schneier.com/essays/archives/2007/01/schneier_full_disclo.html

SIDN LABS TU Delft

Public Disclosure

Vendor	Public
Private Disclosure	Public Disclosure
Responsible Disclosure	

- “Dammed good idea" (Schneier)
- Brings public scrutiny to vulnerabilities
- The "only reason" vendors patch their systems
- **Problem**: patches are not typically available at disclosure time
  - See https://mailman.nanog.org/pipermail/nanog/2021-October/216309.html

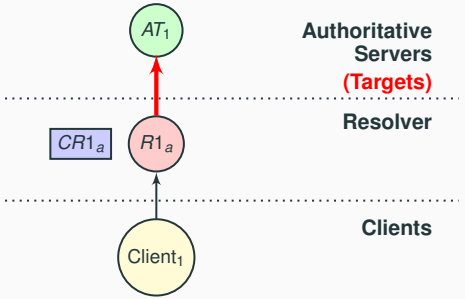
“Responsible” Disclosure

Vendor	Public
Private Disclosure	Public Disclosure
Responsible Disclosure	

- It combines both private + public disclosure
- Gives the vendor a heads up so they can patch their systems
- Normal procedure nowadays
- Only exists because public disclosure became the norm earlier
- Our choice for TsuNAME

TsuNAME in a nutshell

- A configuration error cause resolvers/clients to send non-stop queries to authoritative servers



TsuNAME assymetry

- The bug is on **resolvers**
- But the **authoritative servers** pay the price

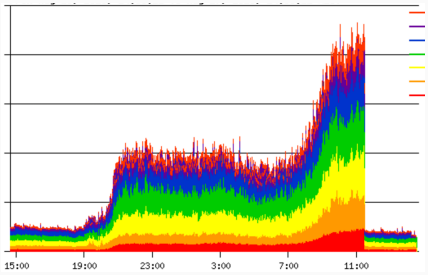


Figure 1: TsuNAME event at an EU-based ccTLD operator. **10x traffic growth**

TsuNAME disclosure timeline

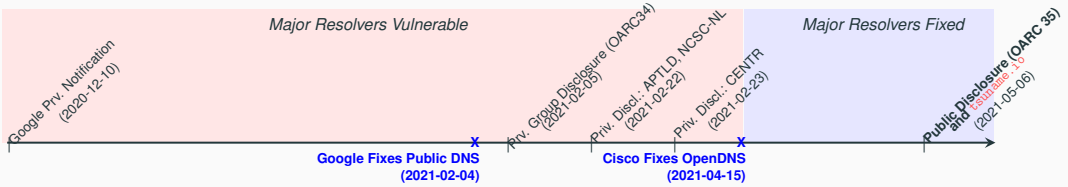


Figure 2: Disclosure Timeline

- Private, **group**, and public disclosure
  - **Thanks a lot DNS-OARC**
- Google fixed its Public DNS in less than 90 days
- Cisco fixed OpenDNS in 40 days

SIDN LABS TU Delft

TsuNAME disclosure timeline

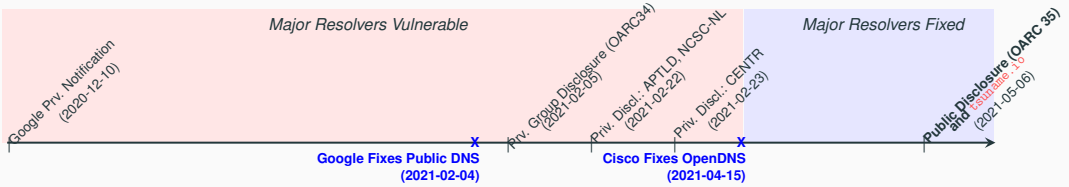


Figure 2: Disclosure Timeline

- Private, **group**, and public disclosure
  - **Thanks a lot DNS-OARC**
- Google fixed its Public DNS in less than 90 days
- Cisco fixed OpenDNS in 40 days

Lessons learned

1. Responsible Disclosure worked

- Google and Cisco fixed their public DNS services
- By first *privately disclosing* it to them, it gave them enough time to react
- Also obtained self-reports from other vendors:
  - BIND
  - NSD
  - PowerDNS
- (but this is case-by-case)

2. Set the public disclose date from the start

- People work with deadlines
- We maybe waited for too long for Google in the beginning
- Weight out the severity/risks with deadlines
- 90 days are enough for vendors

3. When it doubt, disclose

- We had *no* evidence of large DDoS based on TsuNAME
- The vulnerability likely existed for years
- We asked: should we disclose it them?
  - YES

Reasons to disclose:

1. You don't have a complete view
2. Let others take responsibly
3. Not disclosing would be security by obscurity
4. Better safe than sorry

3. When it doubt, disclose

- We had *no* evidence of large DDoS based on TsuNAME
- The vulnerability likely existed for years
- We asked: should we disclose it them?
  - **YES**

Reasons to disclose:

1. You don't have a complete view
2. Let others take responsibly
3. Not disclosing would be security by obscurity
4. Better safe than sorry

3. When it doubt, disclose

- We had *no* evidence of large DDoS based on TsuNAME
- The vulnerability likely existed for years
- We asked: should we disclose it them?
  - **YES**

Reasons to disclose:

1. You don't have a complete view
2. Let others take responsibly
3. Not disclosing would be security by obscurity
4. Better safe than sorry

3. When it doubt, disclose

- We had *no* evidence of large DDoS based on TsuNAME
- The vulnerability likely existed for years
- We asked: should we disclose it them?
  - **YES**

Reasons to disclose:

1. You don't have a complete view
2. Let others take responsibly
3. Not disclosing would be security by obscurity
4. Better safe than sorry

3. When it doubt, disclose

- We had *no* evidence of large DDoS based on TsuNAME
- The vulnerability likely existed for years
- We asked: should we disclose it them?
  - **YES**

Reasons to disclose:

1. You don't have a complete view
2. Let others take responsibly
3. Not disclosing would be security by obscurity
4. Better safe than sorry

3. When it doubt, disclose

- We had *no* evidence of large DDoS based on TsuNAME
- The vulnerability likely existed for years
- We asked: should we disclose it them?
  - **YES**

Reasons to disclose:

1. You don't have a complete view
2. Let others take responsibly
3. Not disclosing would be security by obscurity
4. Better safe than sorry

3. When it doubt, disclose

- We released `CycleHunter`, a tool that search for bugs in zone files
  - https://github.com/SIDN/CycleHunter
- Upon disclosure at DNS-OARC 34, several folks contributed to
- The community got involved

- Thanks to all of them

4. Disclosure takes time, energy and patience

- TsuNAME involved two groups:
  - resolver dev/ops
  - authoritative servers OPs
- We had to notify **both**
- Several private disclosures:
  - DNS-OARC
  - APTLD
  - CENTR
  - LACTLD
  - NCSC-NL

SIDN LABS TU Delft

5. Trust is essencial

1. Trust is key
    - We asked first for PGP key to exchange e-mails
    - Then we were very open and transparent
2. You may want to check it with your legal folks

5. Trust is essencial

1. Trust is key
    - We asked first for PGP key to exchange e-mails
    - Then we were very open and transparent
2. You may want to check it with your legal folks

6. You can’t make everybody happy

Reactions varied:

- **Positive**: vendors, OPs that suffered TsuNAME events before
- **Negative**: “fear mongering”
  - “there are easier ways to DDoS”
- **Indifferent**: “meh”, “not my problem”

And that is OK.

- Google and Cisco fixed their software
  - That protects *everybody*

SIDN LABS TU Delft

6. You can’t make everybody happy

Reactions varied:

- **Positive**: vendors, OPs that suffered TsuNAME events before
- **Negative**: “fear mongering”
  - “there are easier ways to DDoS”
- **Indifferent**: “meh”, “not my problem”

And that is OK.

- Google and Cisco fixed their software
  - That protects *everybody*

SIDN LABS TU Delft

6. You can't make everybody happy

Reactions varied:

- **Positive**: vendors, OPs that suffered TsuNAME events before
- **Negative**: "fear mongering"
  - "there are easier ways to DDoS"
- **Indifferent**: "meh", "not my problem"

And that is OK.

- Google and Cisco fixed their software
  - That protects *everybody*

SIDN LABS TU Delft

6. You can’t make everybody happy

Reactions varied:

- **Positive**: vendors, OPs that suffered TsuNAME events before
- **Negative**: “fear mongering”
  - “there are easier ways to DDoS”
- **Indifferent**: “meh”, “not my problem”

And that is OK.

- Google and Cisco fixed their software
  - That protects *everybody*

SIDN LABS TU Delft

6. You can’t make everybody happy

Reactions varied:

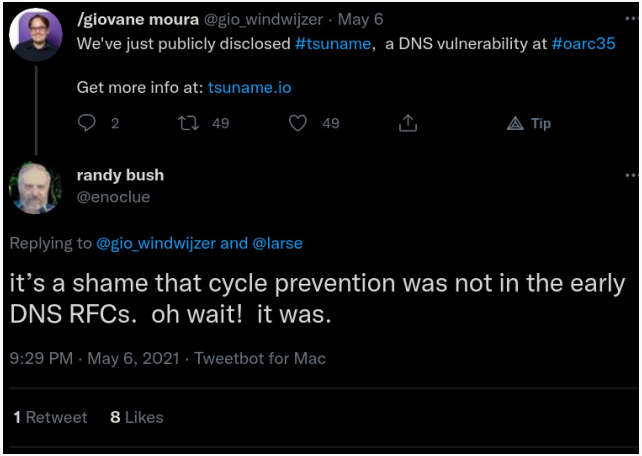
- **Positive**: vendors, OPs that suffered TsuNAME events before
- **Negative**: “fear mongering”
  - “there are easier ways to DDoS”
- **Indifferent**: “meh”, “not my problem”

And that is OK.

- Google and Cisco fixed their software
  - That protects *everybody*

SIDN LABS TU Delft

7. Make most of constructive feedback



7. Make the most of constructive feedback

- Randy was *partially* right:
  - we had missed 4 RFCs that mentioned loops
- **None** of them fully address the issue
- That motivated us to write a **new IETF draft**
  - draft-moura-dnsop-negative-cache-loop

(extra): Did I talk about taxes?

- Google awarded us a bug bounty
- The US IRS would not let you get the money easily
  - 30% tax
  - 8 pages long form, 30 sections:
    - https://www.irs.gov/pub/irs-pdf/fw8bene.pdf
- We wanted to donate the money anyway
  - We simply asked if they could donate it for us
  - *there was an app for it*
  - no taxes, much easier, 1 click.

(extra): Did I talk about taxes?

- Google awarded us a bug bounty
- The US IRS would not let you get the money easily
  - 30% tax
  - 8 pages long form, 30 sections:
    - https://www.irs.gov/pub/irs-pdf/fw8bene.pdf
- We wanted to donate the money anyway
  - We simply asked if they could donate it for us
  - *there was an app for it*
  - no taxes, much easier, 1 click.

SIDN LABS TU Delft

(extra): Did I talk about taxes?

- Google awarded us a bug bounty
- The US IRS would not let you get the money easily
  - 30% tax
  - 8 pages long form, 30 sections:
    - https://www.irs.gov/pub/irs-pdf/fw8bene.pdf
- We wanted to donate the money anyway
  - We simply asked if they could donate it for us
  - *there was an app for it*
  - no taxes, much easier, 1 click.

(extra): Did I talk about taxes?

- Google awarded us a bug bounty
- The US IRS would not let you get the money easily
  - 30% tax
  - 8 pages long form, 30 sections:
    - https://www.irs.gov/pub/irs-pdf/fw8bene.pdf
- We wanted to donate the money anyway
  - We simply asked if they could donate it for us
  - *there was an app for it*
  - no taxes, much easier, 1 click.

Summary

- Responsible disclosure *worked*
- Took more effort and energy
- Overall, positive responses
- Suggestion to researchers:
  - try responsible disclosure
- Positive outcome:
  - two major public resolvers fixed
  - an IETF draft under review
  - a *slightly* safer DNS

https://tsuname.io

SIDN LABS TU Delft