The Russian National Domain Name System

-

structure, evolution and global impact on Internet freedom

13 June 2024

Preface

- The presentation was created using LaTeX
- I'm a DNS nerd
- Over 10 years of studying censorship in the Runet

Preface

- The presentation was created using LaTeX
- I'm a DNS nerd
- Over 10 years of studying censorship in the Runet
- Oh, Great Odin, I was in a hurry

A Brief Background

”The Russian National Domain Name System -*structure, evolution and global impact on Internet freedom*”, 13 June 2024

A Brief Background

- **Stage 1:** Law № 139-FZ of July 28, 2012 ”... Acts of the Russia in the Field of Protection of Children from Information Harmful to Their Health”
  - Changed everything. The good old days of the free internet were over

A Brief Background

- **Stage 1:** Law № 139-FZ of July 28, 2012 ”... Acts of the Russia in the Field of Protection of Children from Information Harmful to Their Health”
  - Changed everything. The good old days of the free internet were over
- **Stage-2:** Low № 90-FZ of May 1, 2019. The so-called ”The Sovereign Runet law”
  - ...and sometimes as the ”The Souvenir Runet law”
  - Changed everything. Fluffy censorship was over
  - Explicit preparation for the war (literally)

The Runet censorship. Stage 1

The Protection of Children from Information Harmful to Their Health...

The Runet censorship. Stage 1

The Protection of Children from Information Harmful to Their Health...

- Unified Register of resources restricted by the Russian Authorities

The Runet censorship. Stage 1

The Protection of Children from Information Harmful to Their Health...

- Unified Register of resources restricted by the Russian Authorities
  - The authorities begin to fill the registry with everything they dislike

The Runet censorship. Stage 1

The Protection of Children from Information Harmful to Their Health...

- Unified Register of resources restricted by the Russian Authorities
  - The authorities begin to fill the registry with everything they dislike
- Every Internet provider must block access to the resources in the Register

The Runet censorship. Stage 1

The Protection of Children from Information Harmful to Their Health...

- Unified Register of resources restricted by the Russian Authorities
  - The authorities begin to fill the registry with everything they dislike
- Every Internet provider must block access to the resources in the Register
- URLs, IP addresses and domains are being blocked

"The Russian National Domain Name System -*structure, evolution and global impact on Internet freedom*", 13 June 2024

The Runet censorship. Stage 1

The Protection of Children from Information Harmful to Their Health...

- Unified Register of resources restricted by the Russian Authorities
  - The authorities begin to fill the registry with everything they dislike
- Every Internet provider must block access to the resources in the Register
- URLs, IP addresses and domains are being blocked
  - Everyone does it as they can
  - Some providers are starting to intercept DNS traffic

"The Russian National Domain Name System -*structure, evolution and global impact on Internet freedom*", 13 June 2024

The Runet censorship. Stage 1

The Protection of Children from Information Harmful to Their Health...

- Unified Register of resources restricted by the Russian Authorities
  - The authorities begin to fill the registry with everything they dislike
- Every Internet provider must block access to the resources in the Register
- URLs, IP addresses and domains are being blocked
  - Everyone does it as they can
  - Some providers are starting to intercept DNS traffic
- Roskomnadzor is the main authority in charge of the registry

The Sovereign (or Souvenir) Runet

”The Russian National Domain Name System -*structure, evolution and global impact on Internet freedom*”, 13 June 2024

The Sovereign (or Souvenir) Runet

- Roskomnadzor is the main authority in charge of the Runet

"The Russian National Domain Name System -*structure, evolution and global impact on Internet freedom*", 13 June 2024

The Sovereign (or Souvenir) Runet

- Roskomnadzor is the main authority in charge of the Runet
- Mandatory Government DPI for Filtering behind borders

"The Russian National Domain Name System -*structure, evolution and global impact on Internet freedom*", 13 June 2024

The Sovereign (or Souvenir) Runet

- Roskomnadzor is the main authority in charge of the Runet
- Mandatory Government DPI for Filtering behind borders
  - Non-public filtering rules without any oversight

"The Russian National Domain Name System -*structure, evolution and global impact on Internet freedom*", 13 June 2024

The Sovereign (or Souvenir) Runet

- Roskomnadzor is the main authority in charge of the Runet
- Mandatory Government DPI for Filtering behind borders
  - Non-public filtering rules without any oversight
  - Control of internal traffic routing rules

"The Russian National Domain Name System -*structure, evolution and global impact on Internet freedom*", 13 June 2024

The Sovereign (or Souvenir) Runet

- Roskomnadzor is the main authority in charge of the Runet
- Mandatory Government DPI for Filtering behind borders
  - Non-public filtering rules without any oversight
  - Control of internal traffic routing rules
- **The Russian National Domain Name System**

"The Russian National Domain Name System -*structure, evolution and global impact on Internet freedom*", 13 June 2024

The Russian National Domain Name System

NSDI(НСДИ) in Russian

The infrastructure of government recursive DNS resolvers

- Very abstract regulation
- No accountability for rules and service levels
- Mandatory for all
  - Internet providers
  - Internet service providers
  - Social networks
  - and other services

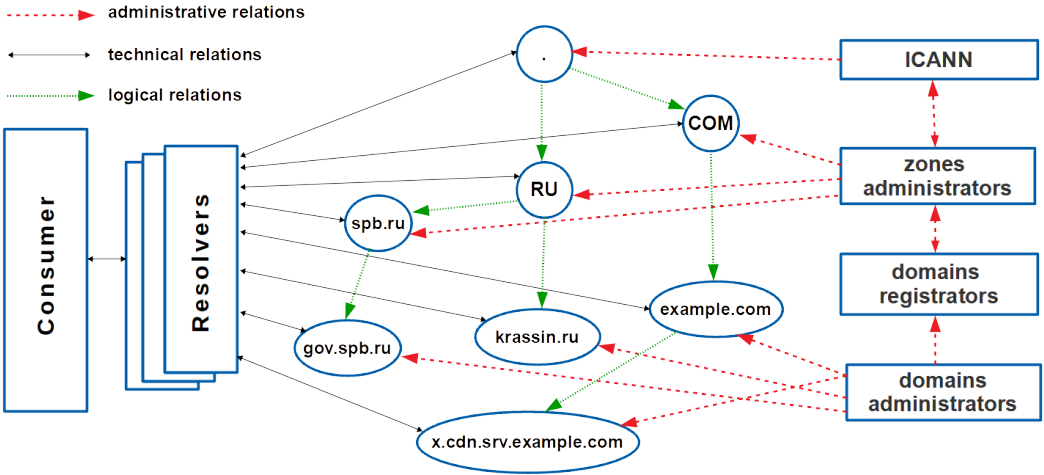
Let’s recall what we know about DNS

”The Russian National Domain Name System -*structure, evolution and global impact on Internet freedom*”, 13 June 2024

Brief Introduction to DNS

- API requests, working with CDN
- Clouds, microservices, auto-discovery and configuration
- Unimaginable amount of everything

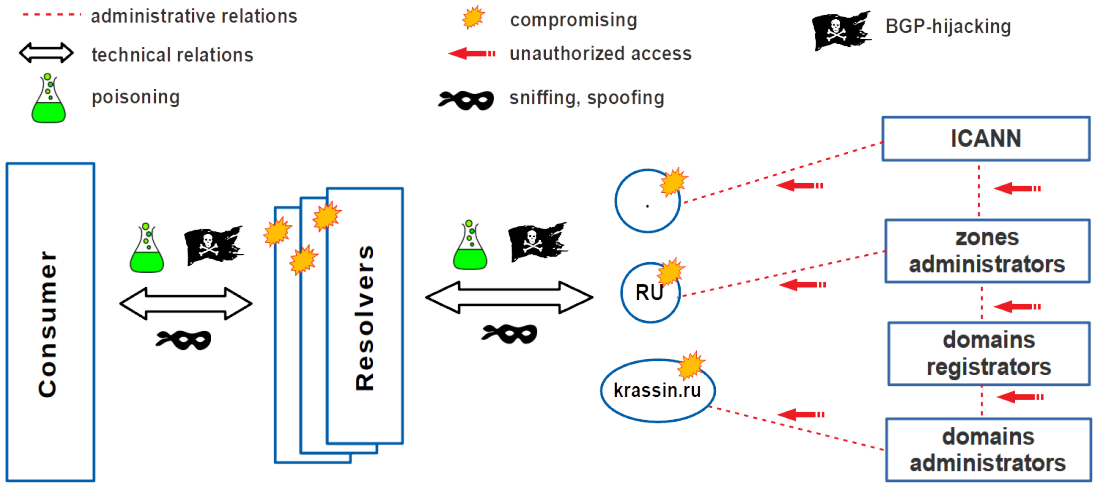
How DNS Works



Features of the classic DNS

- UDP transport. No connection
- No identification of DNS servers
- No data control
- No encryption
- **Not much has changed since then**

Threats to the DNS System



"The Russian National Domain Name System -*structure, evolution and global impact on Internet freedom*", 13 June 2024

Summary of DNS System Threats

- Poisoning, substitution
- Server compromise and record replacement
- Fake servers, BGP hijacking
- Advertising, statistics collection
- Surveillance
  - 73.1% can be identified by DNS fingerprint[1]

[1] "The Russian National Domain Name System -*structure, evolution and global impact on Internet freedom*", 13 June 2024

Authorities surely do not exploit these opportunities

Authorities surely do not exploit these opportunities

Or they do?

"The Russian National Domain Name System -*structure, evolution and global impact on Internet freedom*", 13 June 2024

NSDI. The initial concept

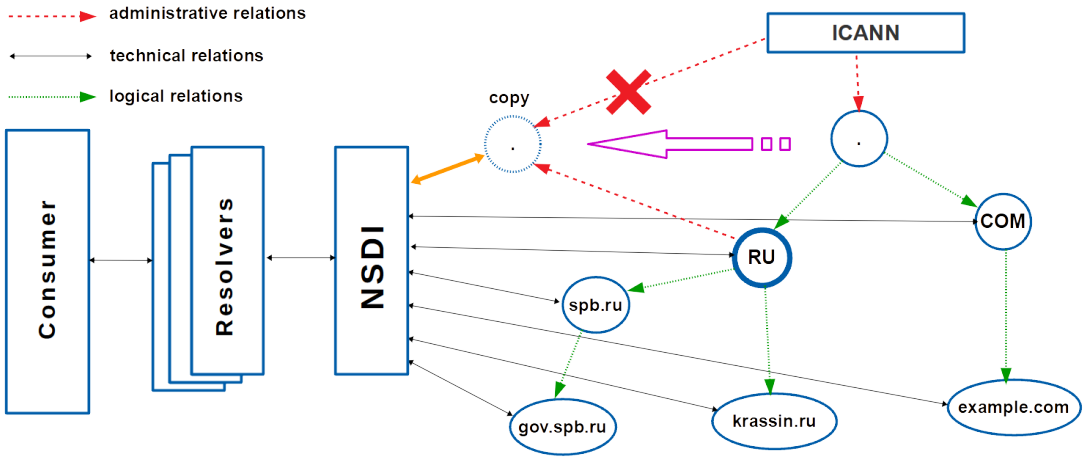
- The infrastructure of recursive DNS resolvers
  - controlled by the Russian government
- Mandatory for all
- Store an acceptable copy of the root zone
- If the root zone becomes unavailable, continue to provide a reliable copy
- win-win situation?

NSDI. The initial concept

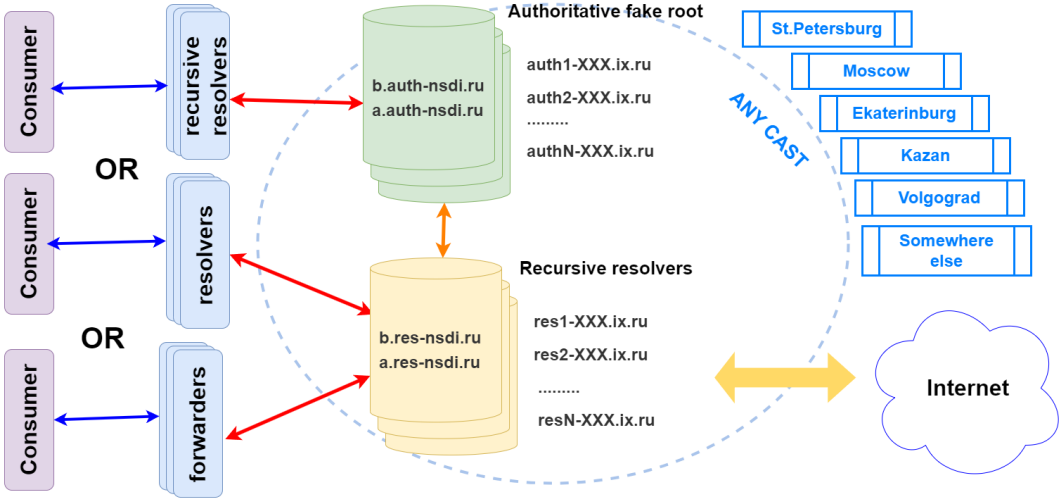
- The infrastructure of recursive DNS resolvers
  - controlled by the Russian government
- Mandatory for all
- Store an acceptable copy of the root zone
- If the root zone becomes unavailable, continue to provide a reliable copy
- win-win situation?
- **DNSSEC. Well, it ruined everything**

"The Russian National Domain Name System -*structure, evolution and global impact on Internet freedom*", 13 June 2024

NSDI. The root copy concept



NSDI. Architecture



NSDI. What about secure DNS?

For what reason? Secure DNS does not help politicians

"The Russian National Domain Name System -*structure, evolution and global impact on Internet freedom*", 13 June 2024

It doesn’t look too scary. Isn’t it?

”The Russian National Domain Name System -*structure, evolution and global impact on Internet freedom*”, 13 June 2024

NSDI. Censorship

- Blocking domains from the Unified Register
  - Sometimes. I don’t know why
  - No ways to know what, when and why
    - No oversight, no problem
  - Technical and political reasons I guess
- Collection and analysis of DNS query statistics
  - I haven’t any avidence but I’m sure

”The Russian National Domain Name System -*structure, evolution and global impact on Internet freedom*”, 13 June 2024

I often say I’m confident

I need to clarify this

- Russian authorities don’t act without legitimization
- But we often see actions not based on the law. How?

”The Russian National Domain Name System -*structure, evolution and global impact on Internet freedom*”, 13 June 2024

I often say I’m confident

I need to clarify this

- Russian authorities don’t act without legitimization
- But we often see actions not based on the law. How?
- Sovereign Runet law is a law about national security
  - The interpretation of threats is very broad
  - Broad powers in the face of threats
  - It is a very convenient concept
  - Does Russian authority use this concept in bad manner?

I often say I’m confident

I need to clarify this

- Russian authorities don’t act without legitimization
- But we often see actions not based on the law. How?
- Sovereign Runet law is a law about national security
  - The interpretation of threats is very broad
  - Broad powers in the face of threats
  - It is a very convenient concept
  - Does Russian authority use this concept in bad manner?
    - They not only use it but also take pride in it

NSDI. Surveillance

- No facts or signs of surveillance
- Except for the general trend and Roskomnadzor’s policies
  - The data obtained from the Roskomnadzor hack two years ago
- I don’t think they are doing this at the moment
  - Roskomnadzor have a lot of other toys now
  - But it can change at any time

NSDI. What else?

The more you have, the more you want

Russian DNS outage 31 Jan 2024

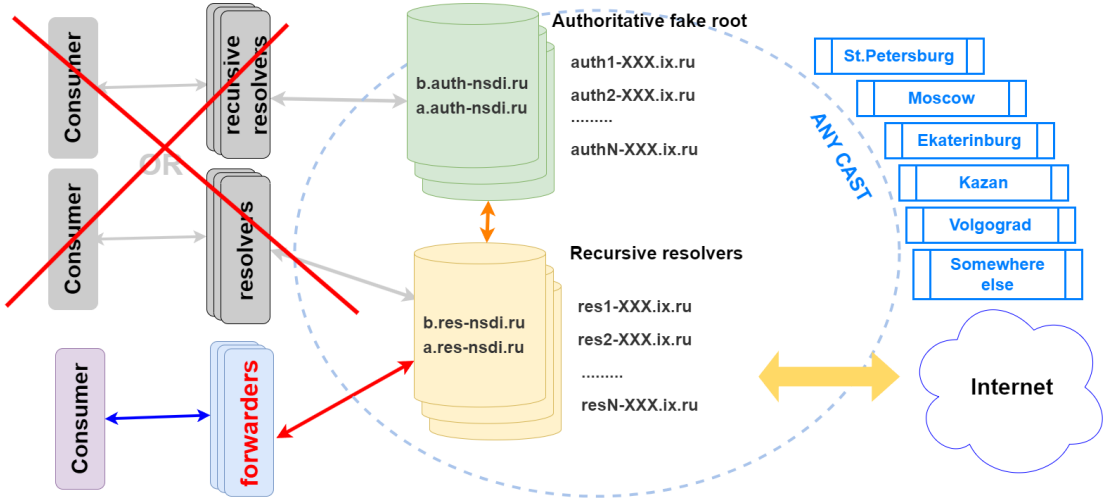
- The RU zone was incorrectly signed for 2 hours
- All Internet resources in the RU zone were unavailable
- NSDI disabled the DNSSEC validation for problem period
  - But the DNSSEC works this way – nothing working without valid signature
- The authorities reported that those who used the NSDI were not affected

"The Russian National Domain Name System -*structure, evolution and global impact on Internet freedom*", 13 June 2024

NSDI. The new features

- As a result of DNSSEC incident, a new regulation was passed
  - Nobody takes care about root zone copy
  - All DNS issues solves by the NSDI in their own way
  - Any consumers MUST NOT use their own validation and decisions
- The old problem with the signature of the root zone copy is solved

NSDI. Architecture Next Generation



NSDI. Conclusion

- Mandatory use by all consumers
  - Possibility of blocking access to other DNS servers
- Mandatory use of insecure DNS
  - All your DNS queries are visible to DPI
- No accountability

Global impact

- A lot of not-bad cheap services inside Runet
  - All services inside Russia MUST use NSDI
  - Globalisation side effects
- Transit traffic
  - Inaccurate filtering rules

"The Russian National Domain Name System -*structure, evolution and global impact on Internet freedom*", 13 June 2024

Adoption of experience

- Fight against the Secure DNS practices
- Using for blocking techniques improvement
- Using for surveillance techniques improvement

Resistance. Fight the good fight

- New Secure DNS protocols and implementations
- New methods of Secure DNS discovery
- DNSSEC and DANE adoption
- Hiding DNS queries within applications

Questions?

References

[1] Herrmann D. Analyzing Characteristic Host Access Patterns for Re-Identification of Web User Sessions. 2012. http://epub.uni-regensburg.de/21103/1/Paper_PUL_nordsec_published.pdf.

[2] Beamer - Overleaf, Online LaTeX Editor. https://www.overleaf.com/learn/latex/Beamer.

[3] Uri Nativ. How to present code. 2016. https://www.slideshare.net/LookAtMySlides/codeware.