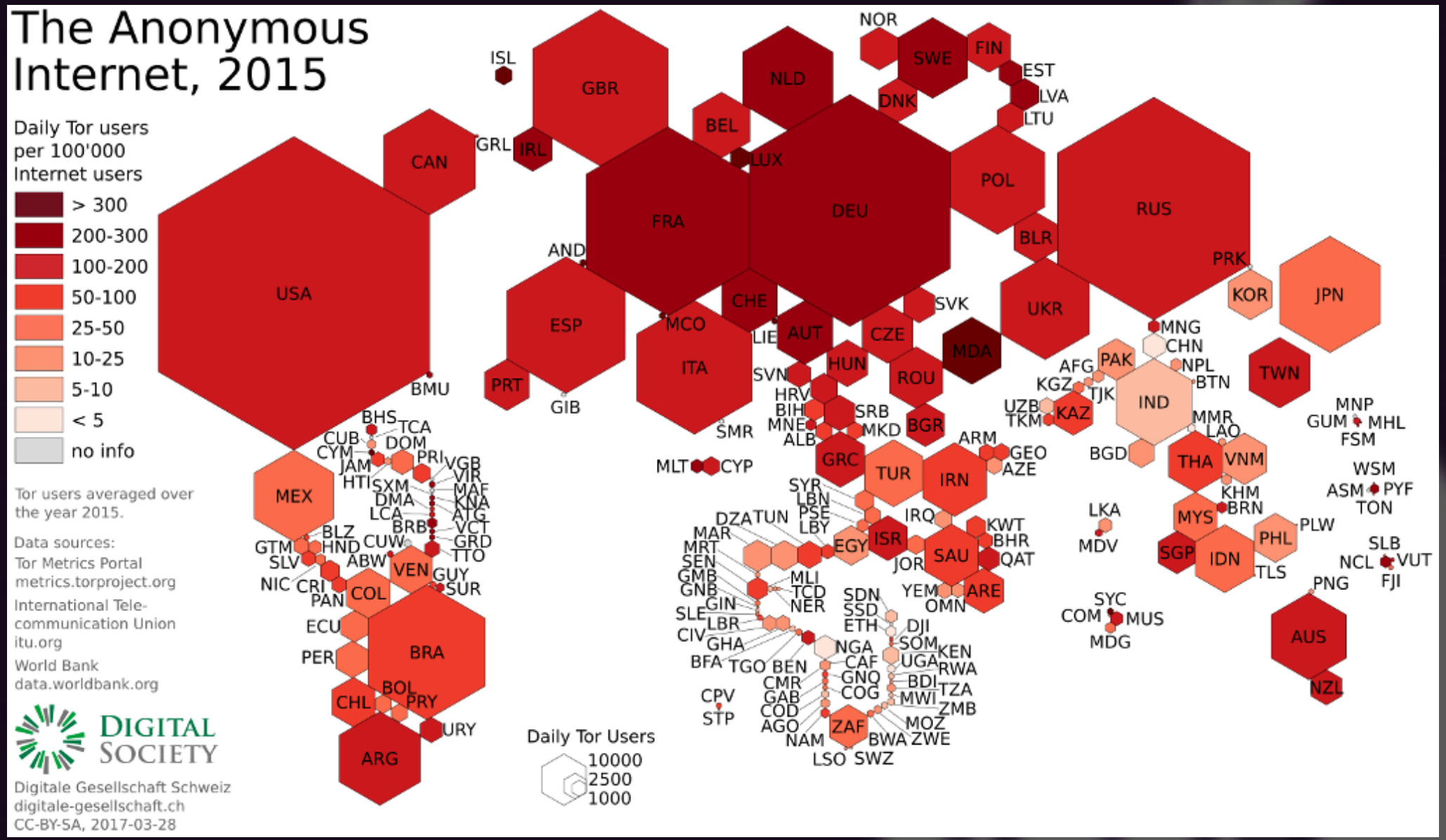
The Utility of the Tor Network

By: Hammas Bin Tanveer
Advisor: Dr. Rishab Nithyanand

The Anonymous Internet



A regular internet connection

Daniyal

Mahnaz

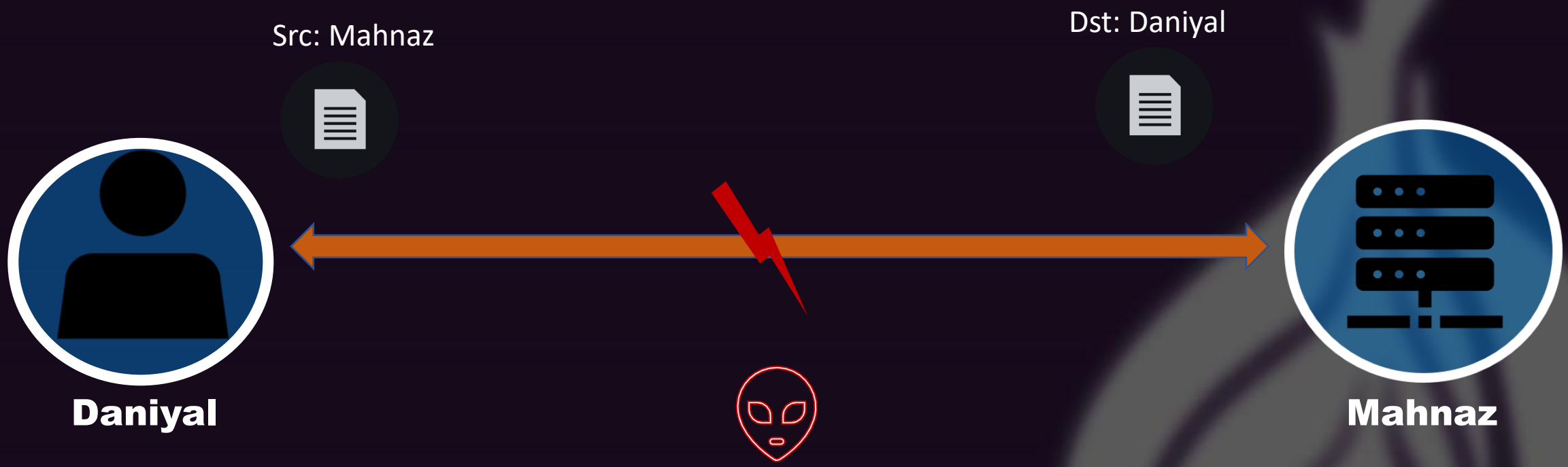
A regular internet connection

A regular internet connection

A regular internet connection

A regular internet connection

A regular internet connection



An internet connection through Tor

Daniyal

Mahnaz

An internet connection through Tor

Tor network

Daniyal

Mahnaz

An internet connection through Tor

Tor network

Daniyal

Mahnaz

An internet connection through Tor

Tor network

Daniyal

Mahnaz

An internet connection through Tor

The setup

Daniyal

An internet connection through Tor

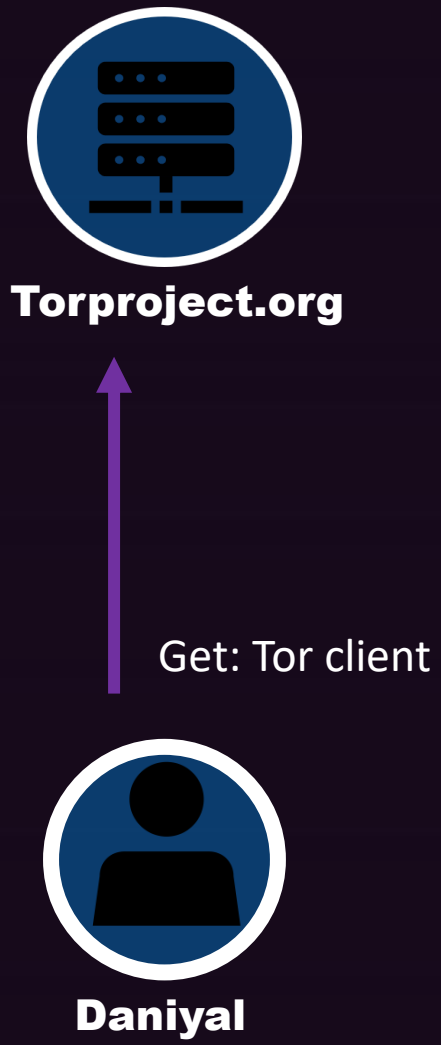
The setup

Torproject.org

Daniyal

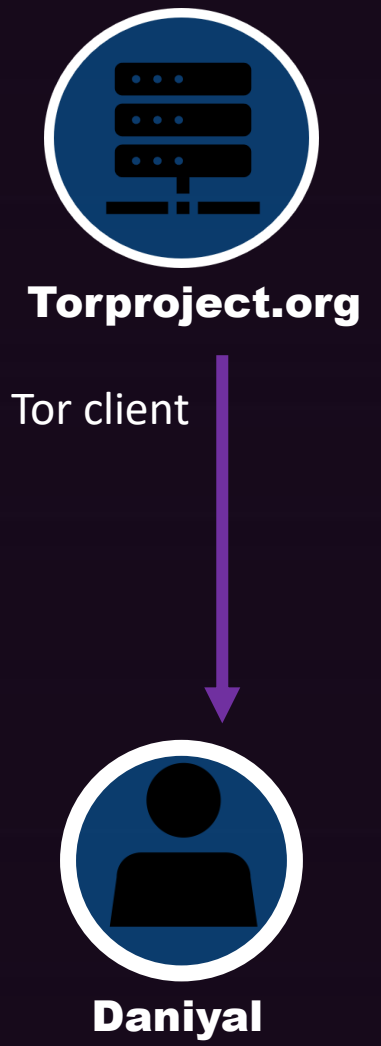
An internet connection through Tor

The setup



An internet connection through Tor

The setup



An internet connection through Tor

The setup

Torproject.org

Daniyal

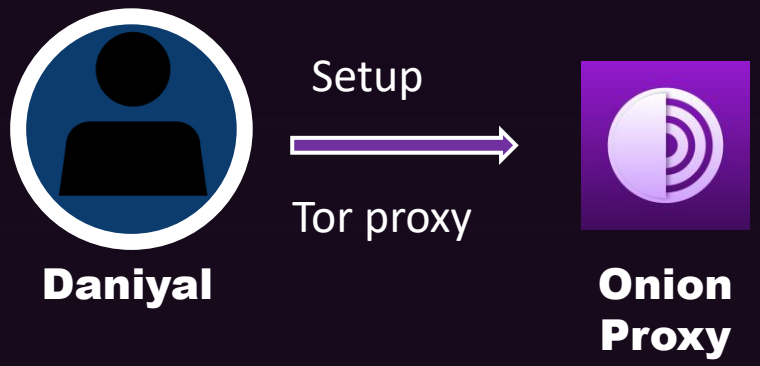
Setup

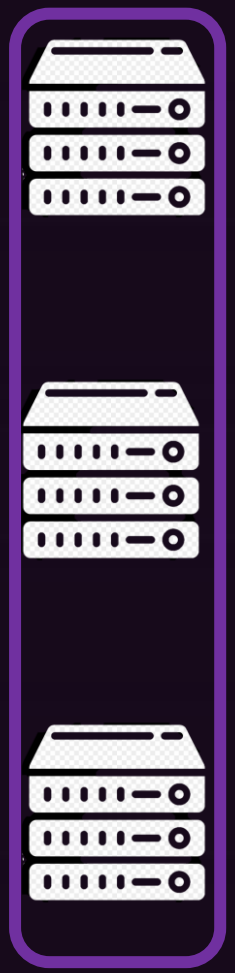
Tor proxy

Onion Proxy

An internet connection through Tor

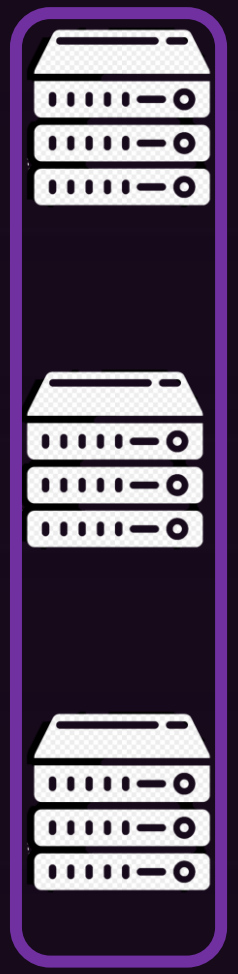
Building a Tor circuit





An internet connection through Tor

Building a Tor circuit



Directory Authorities

Onion Routers

An internet connection through Tor

Service Descriptors

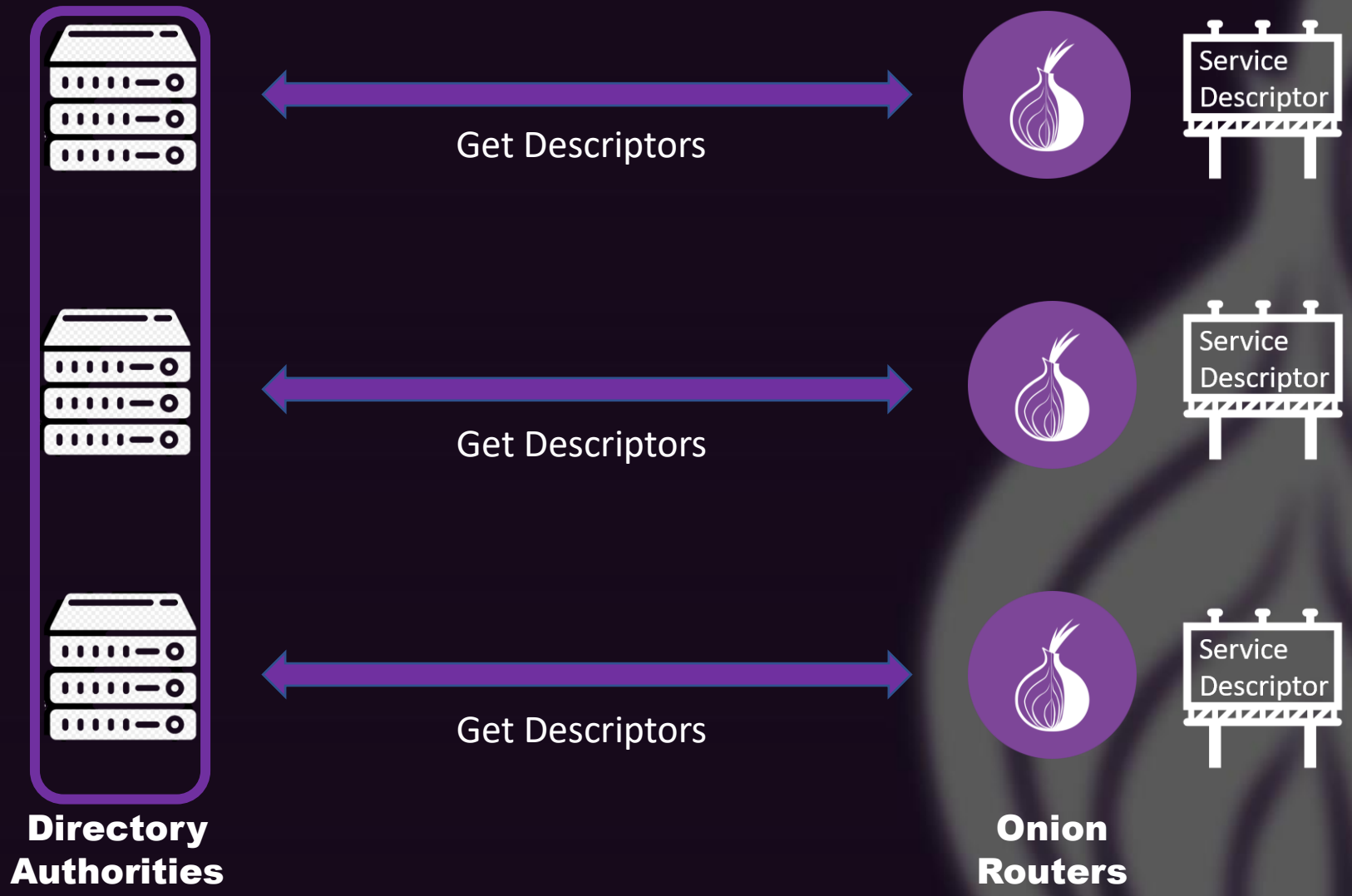
- Contact Information
- Public Keys
- Average Bandwidth
- Exit Policy

A basic Exit policy Example for Web Browsing (*only*) -

```
ExitPolicy accept *:53          # DNS
ExitPolicy accept *:80          # HTTP
ExitPolicy accept *:443         # HTTPS
ExitPolicy reject *:*
```

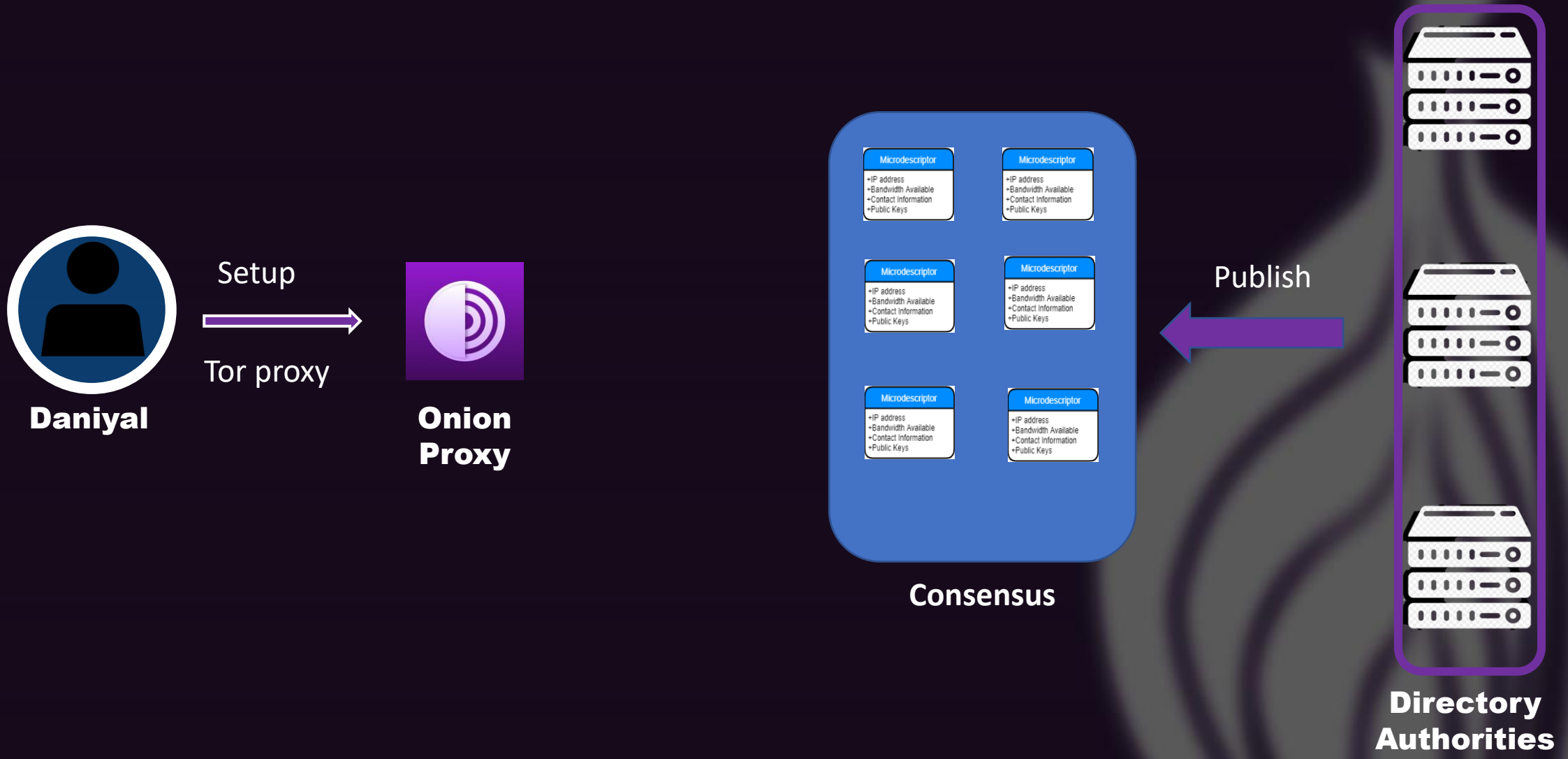
An internet connection through Tor

Building a Tor circuit



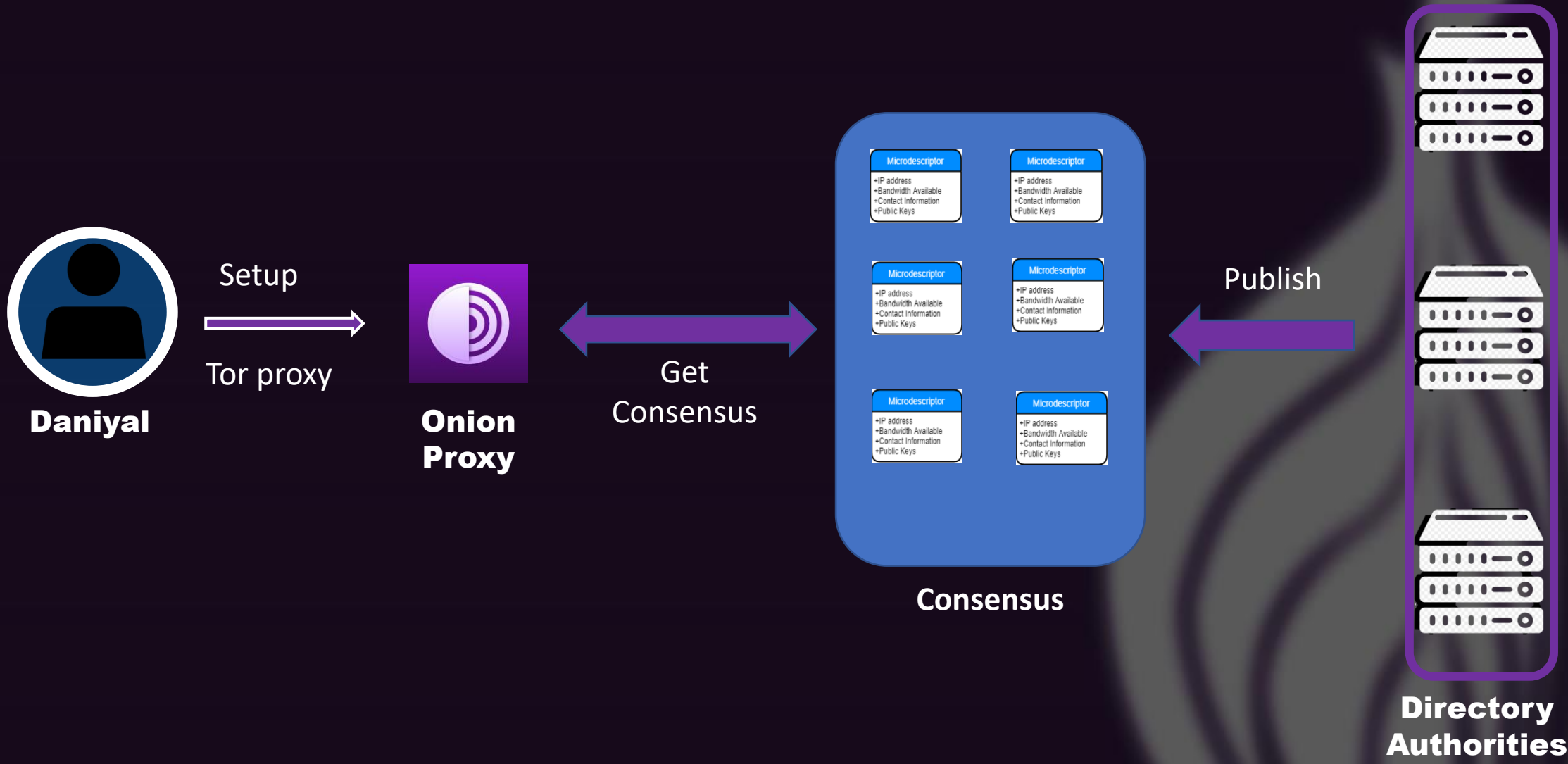
An internet connection through Tor

Building a Tor circuit



An internet connection through Tor

Building a Tor circuit



An internet connection through Tor

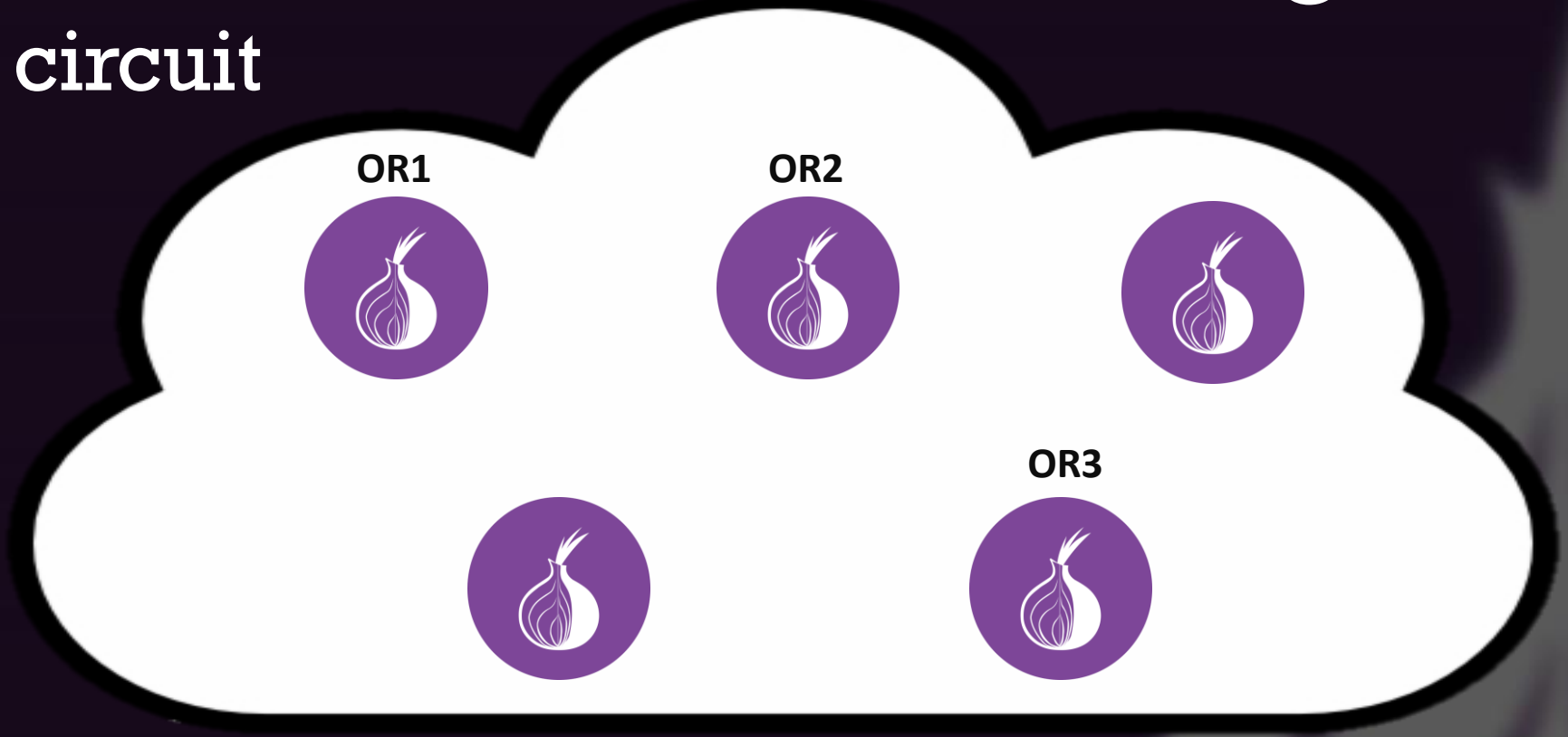
The Tor circuit

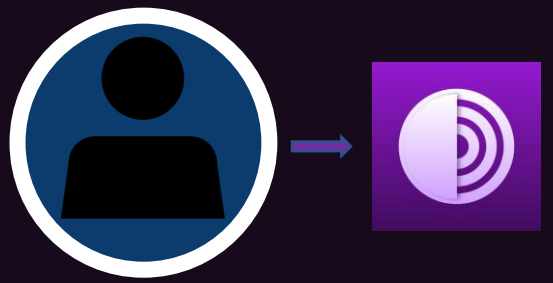
Daniyal

Mahnaz

An internet connection through Tor

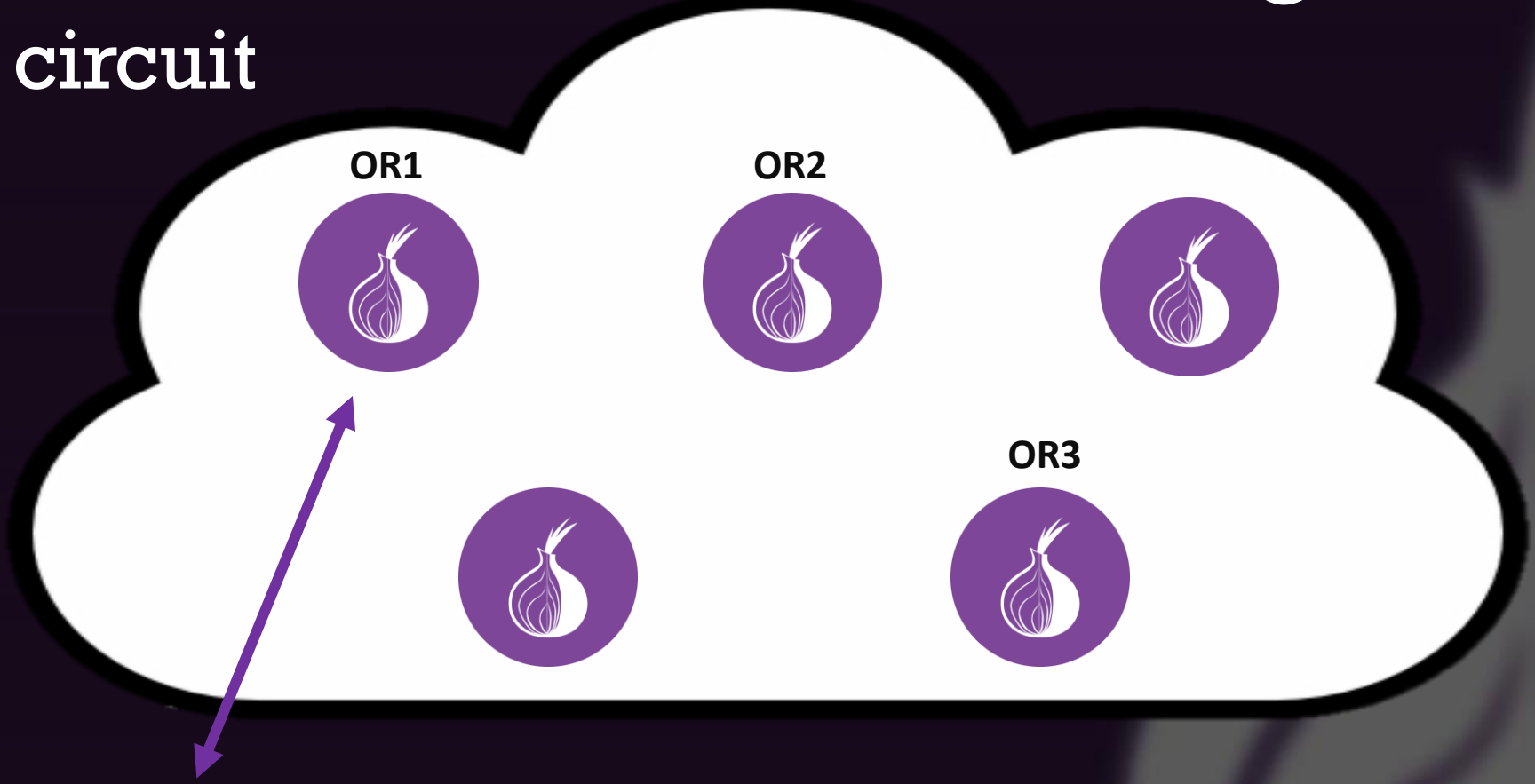
The Tor circuit

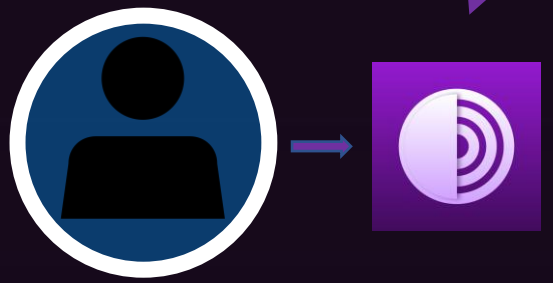




An internet connection through Tor

The Tor circuit



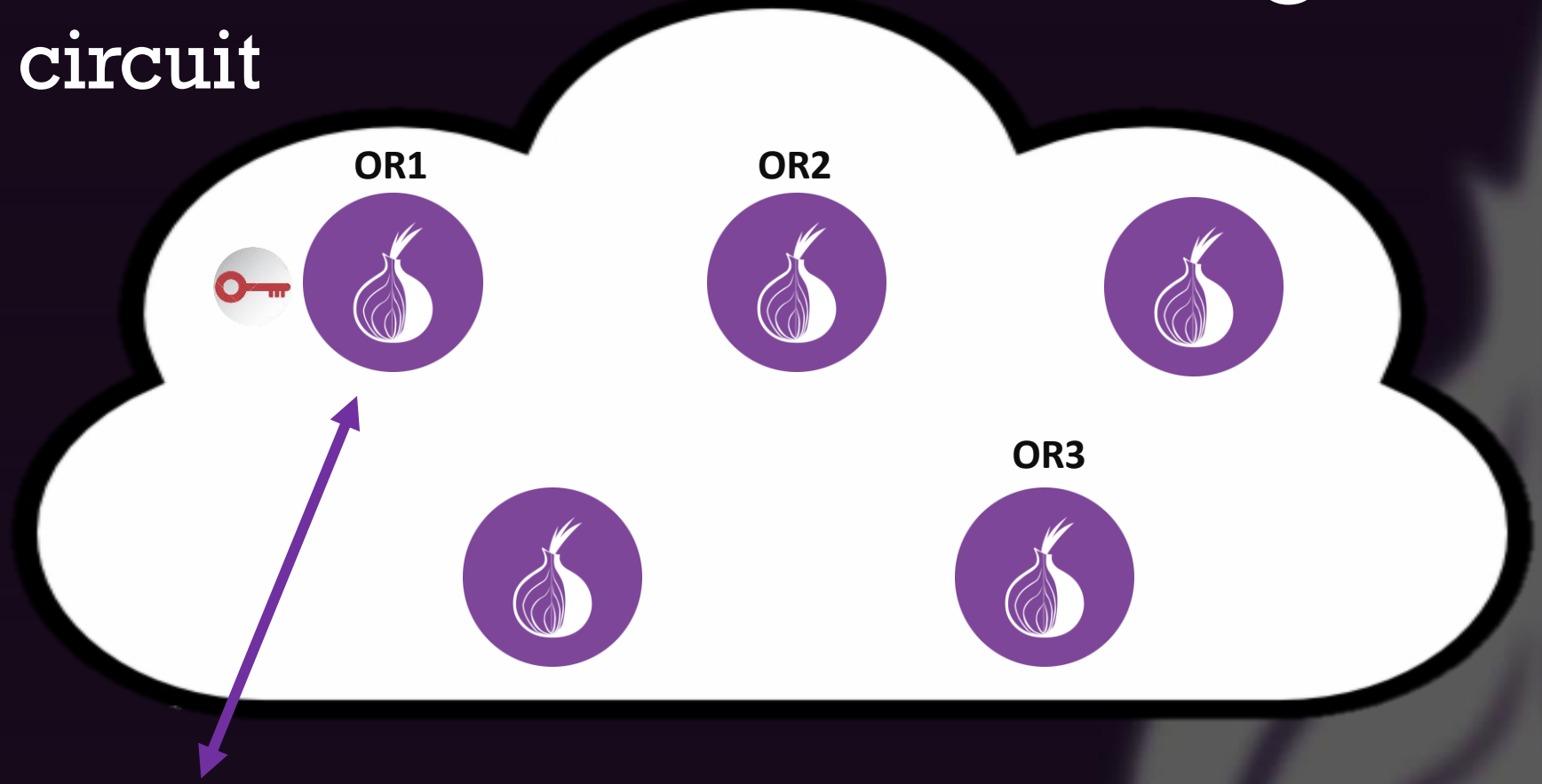


Daniyal

Mahnaz

An internet connection through Tor

The Tor circuit

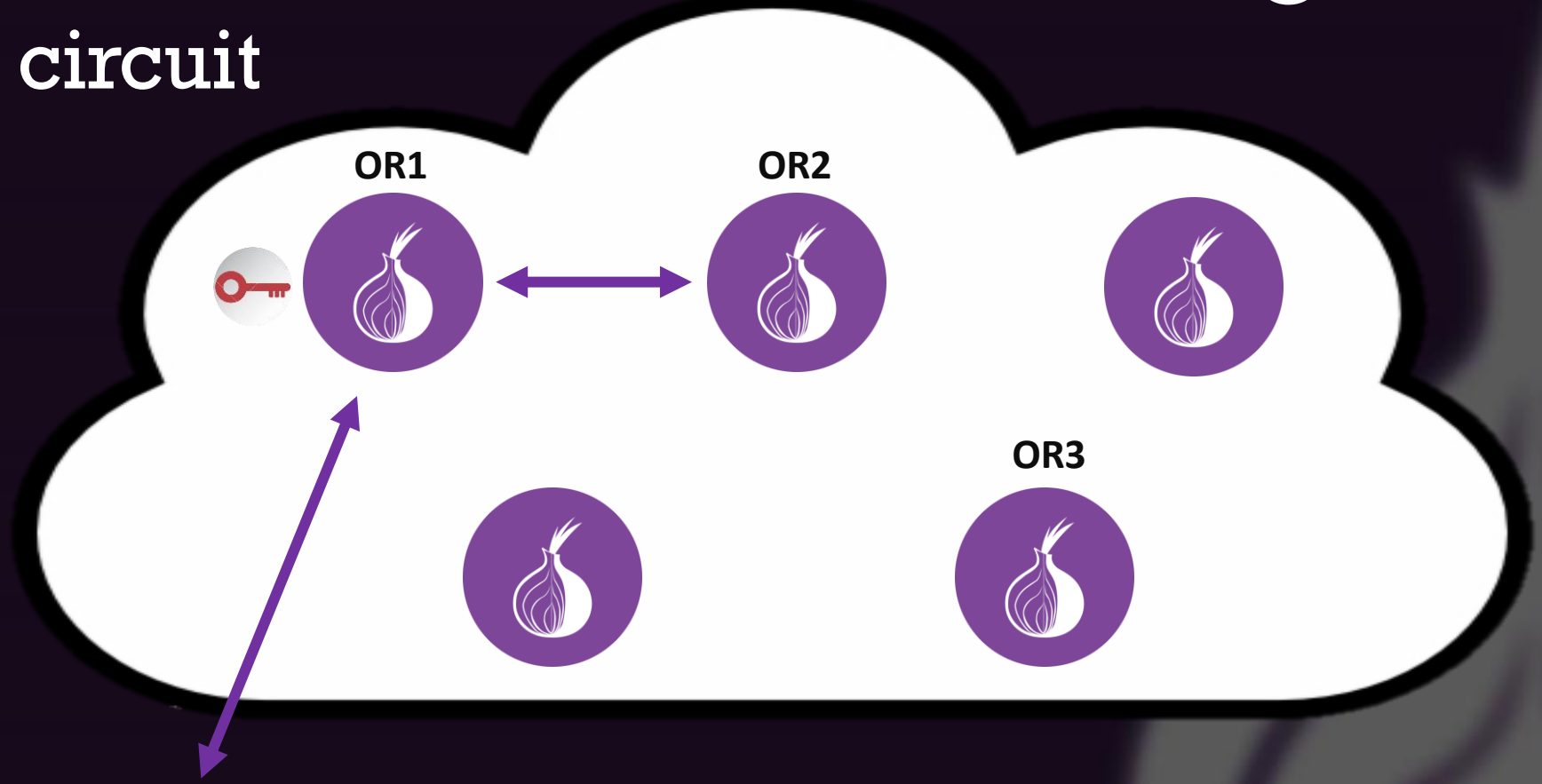


Daniyal

Mahnaz

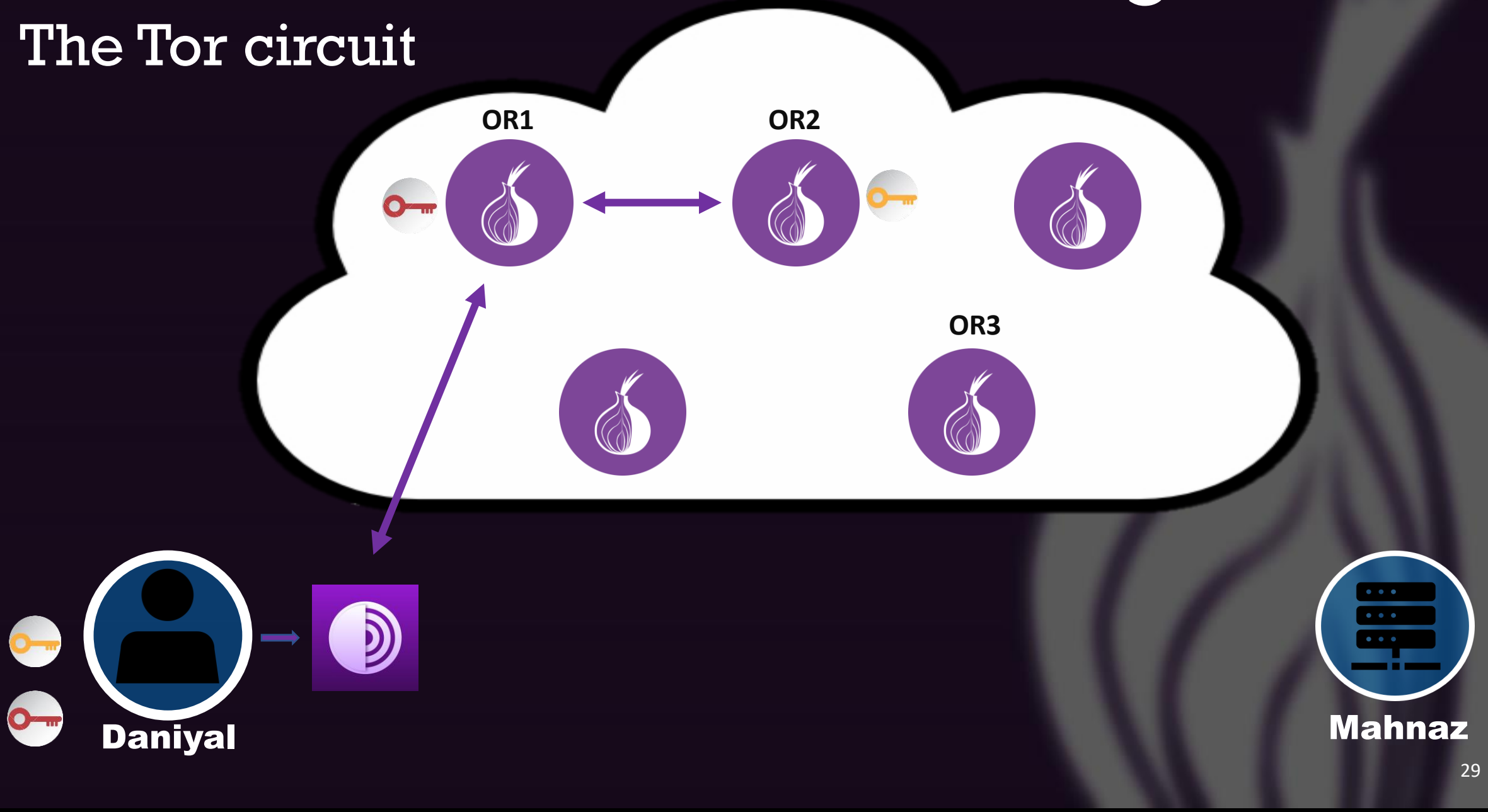
An internet connection through Tor

The Tor circuit



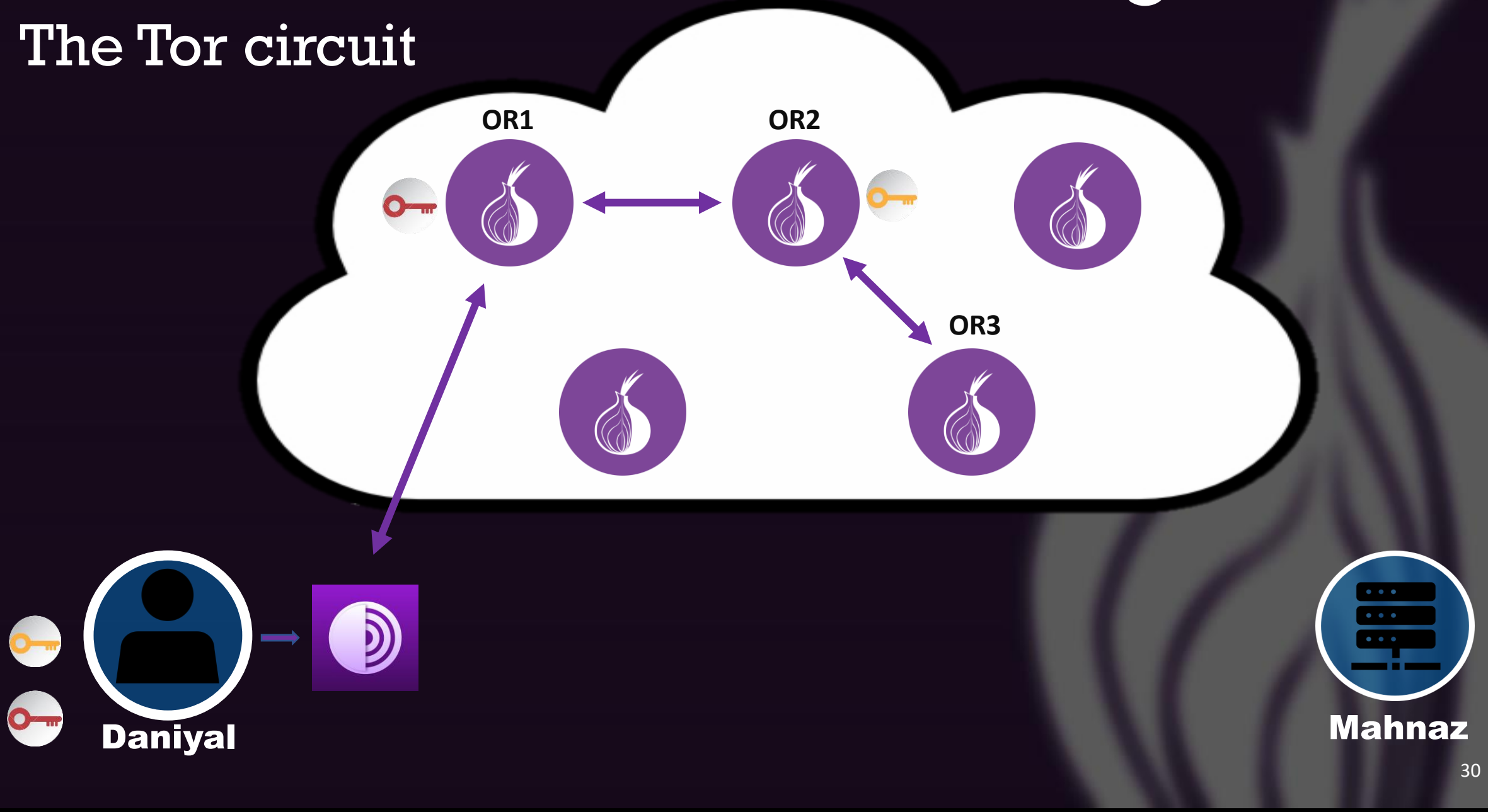
An internet connection through Tor

The Tor circuit



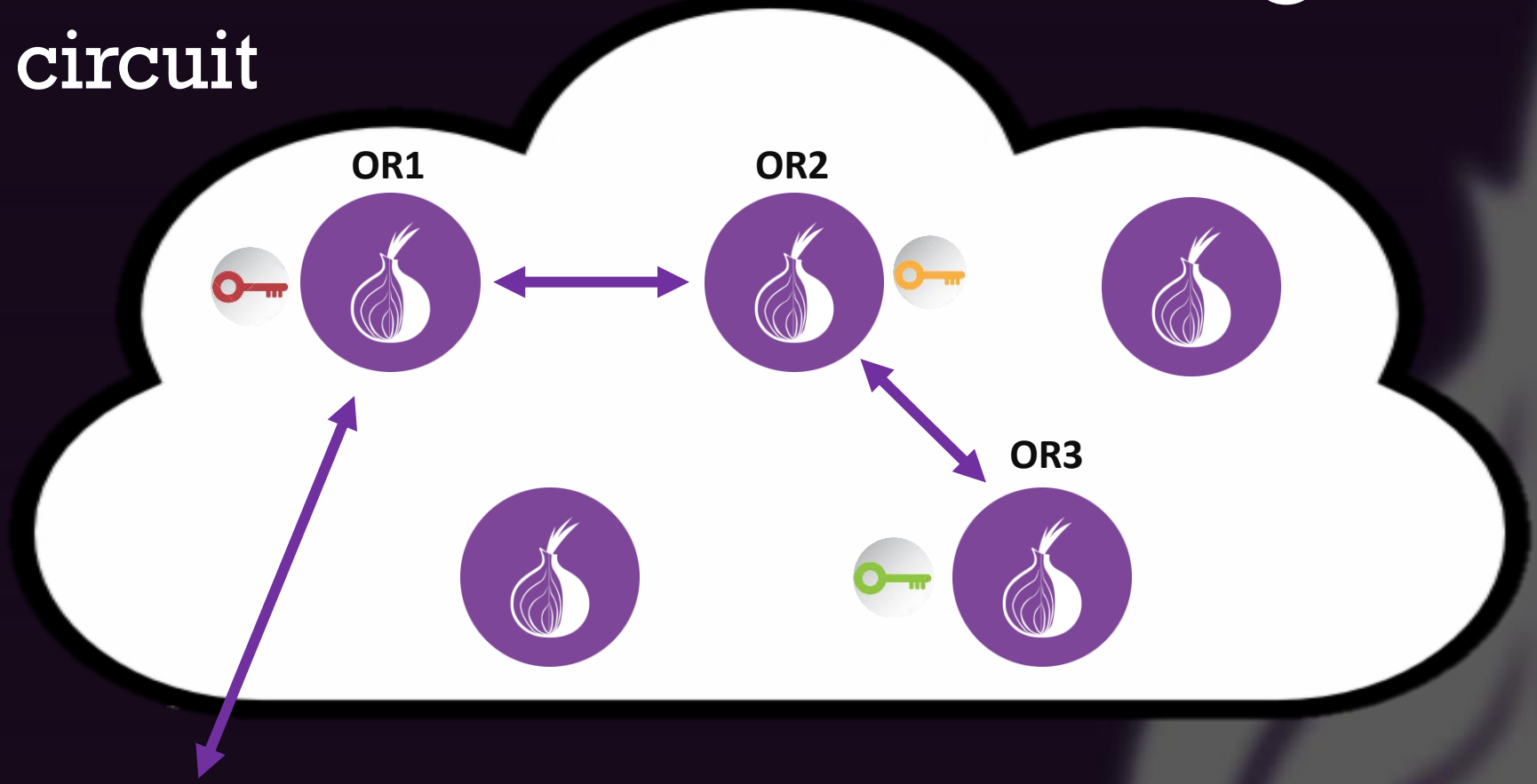
An internet connection through Tor

The Tor circuit



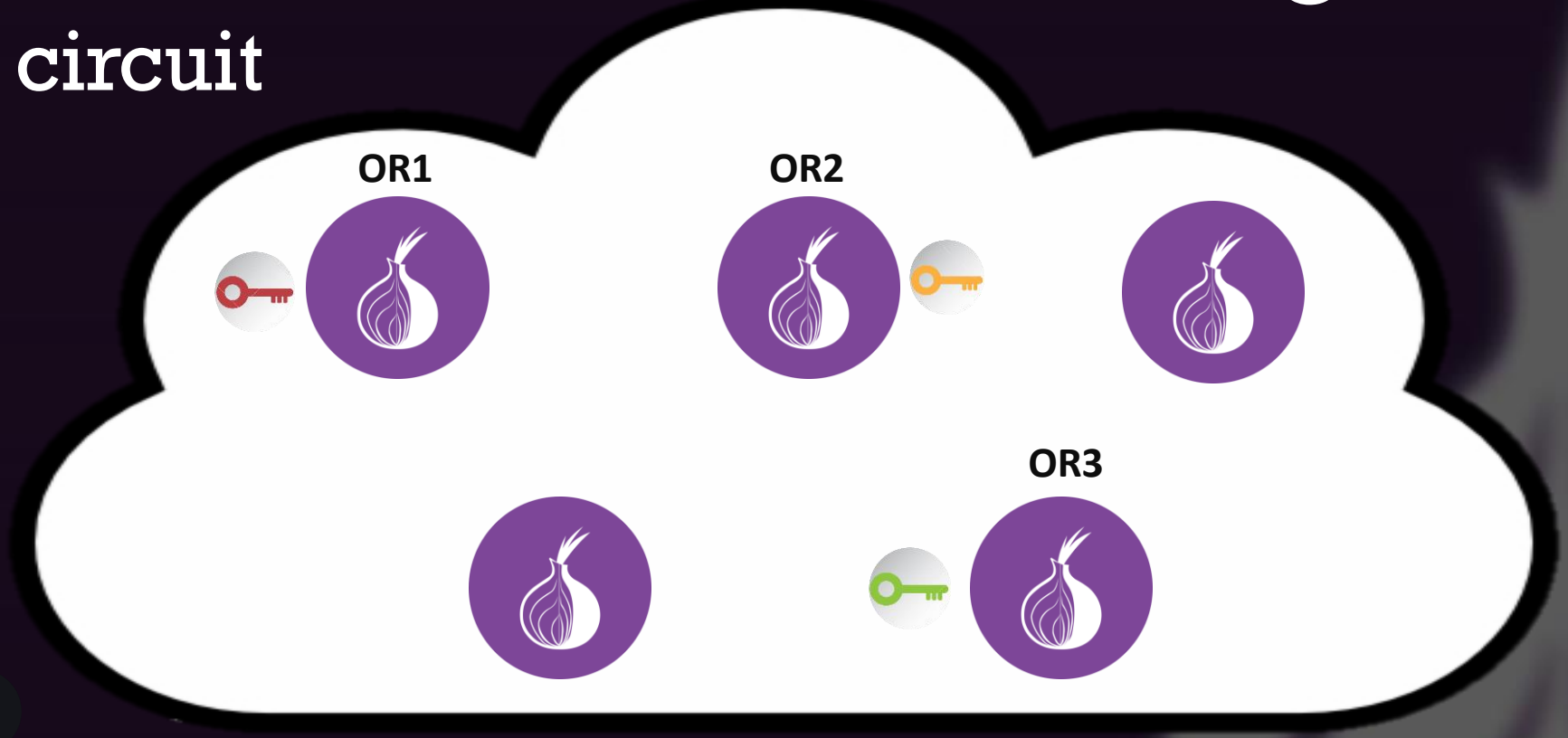
An internet connection through Tor

The Tor circuit



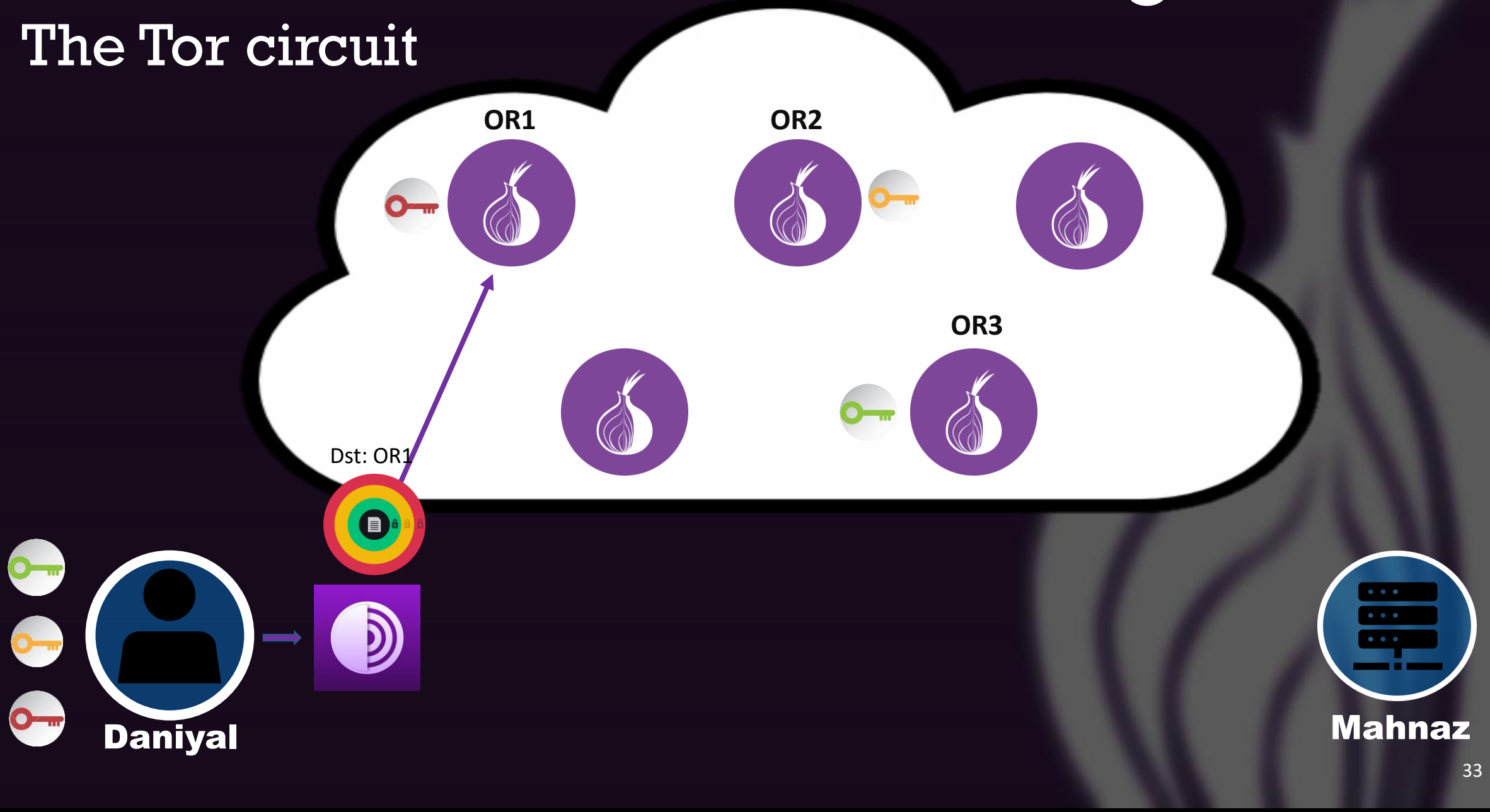
An internet connection through Tor

The Tor circuit



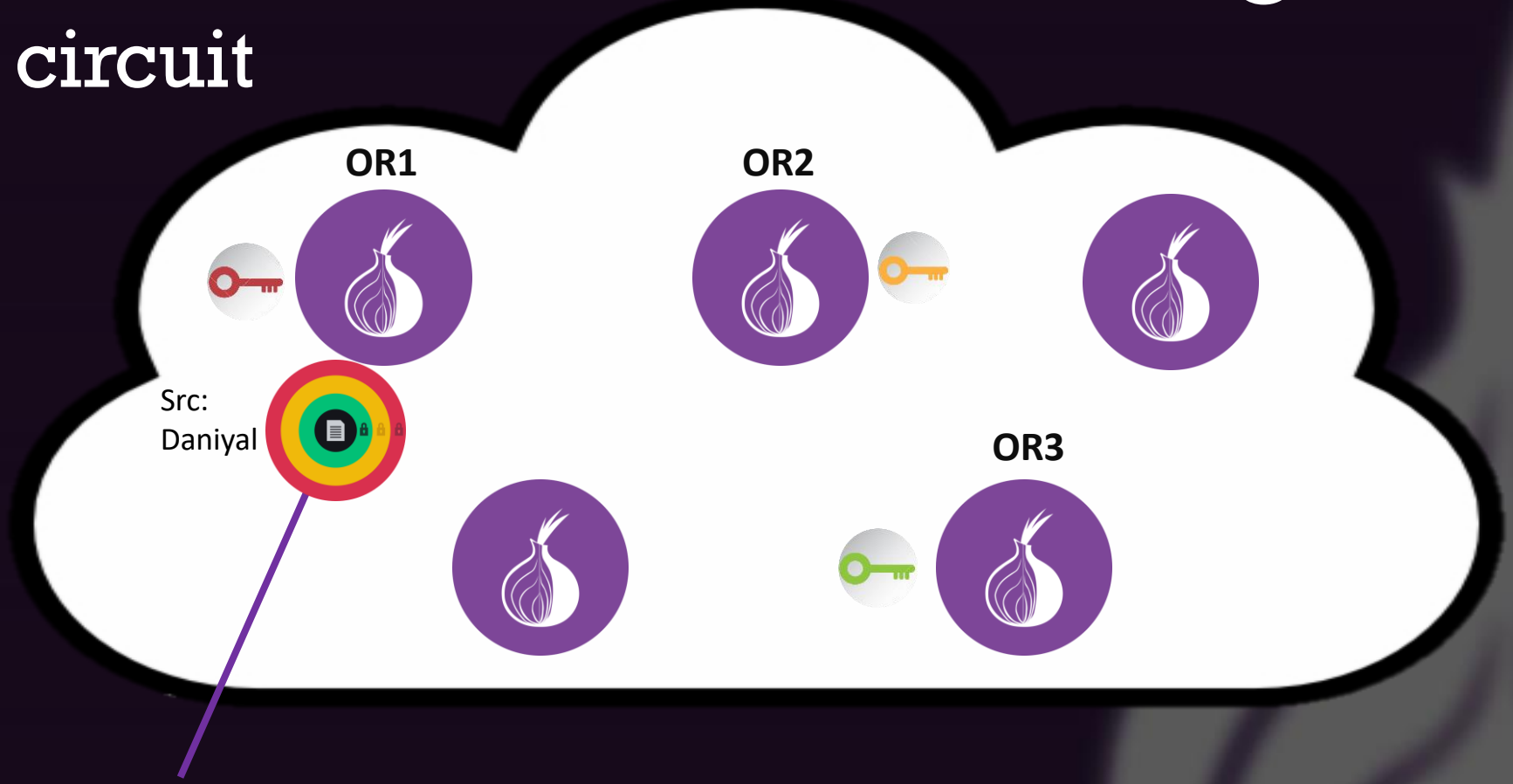
An internet connection through Tor

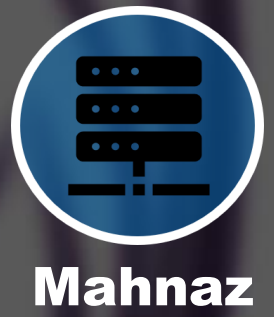
The Tor circuit



An internet connection through Tor

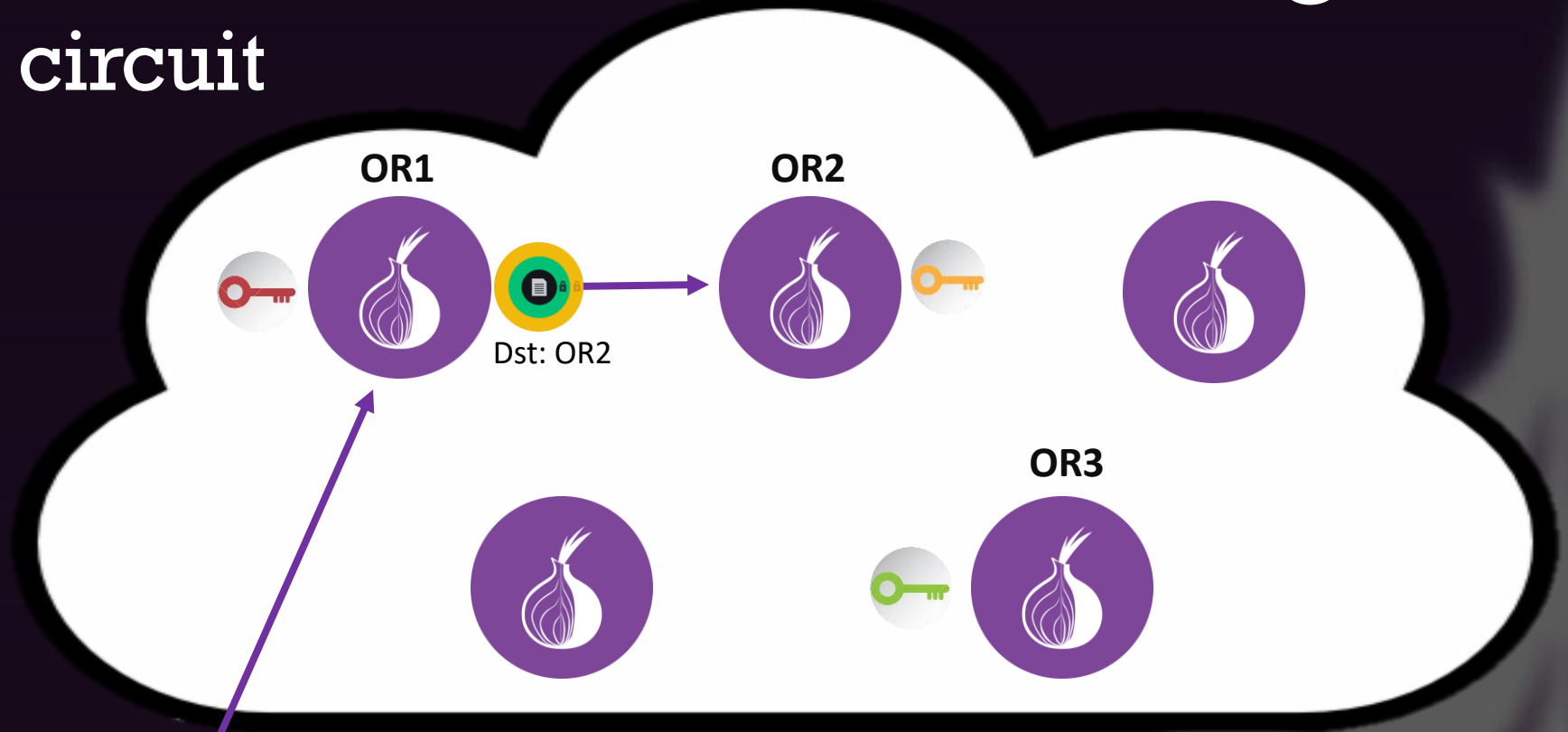
The Tor circuit

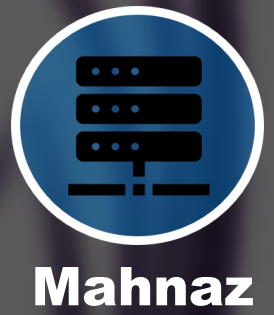




An internet connection through Tor

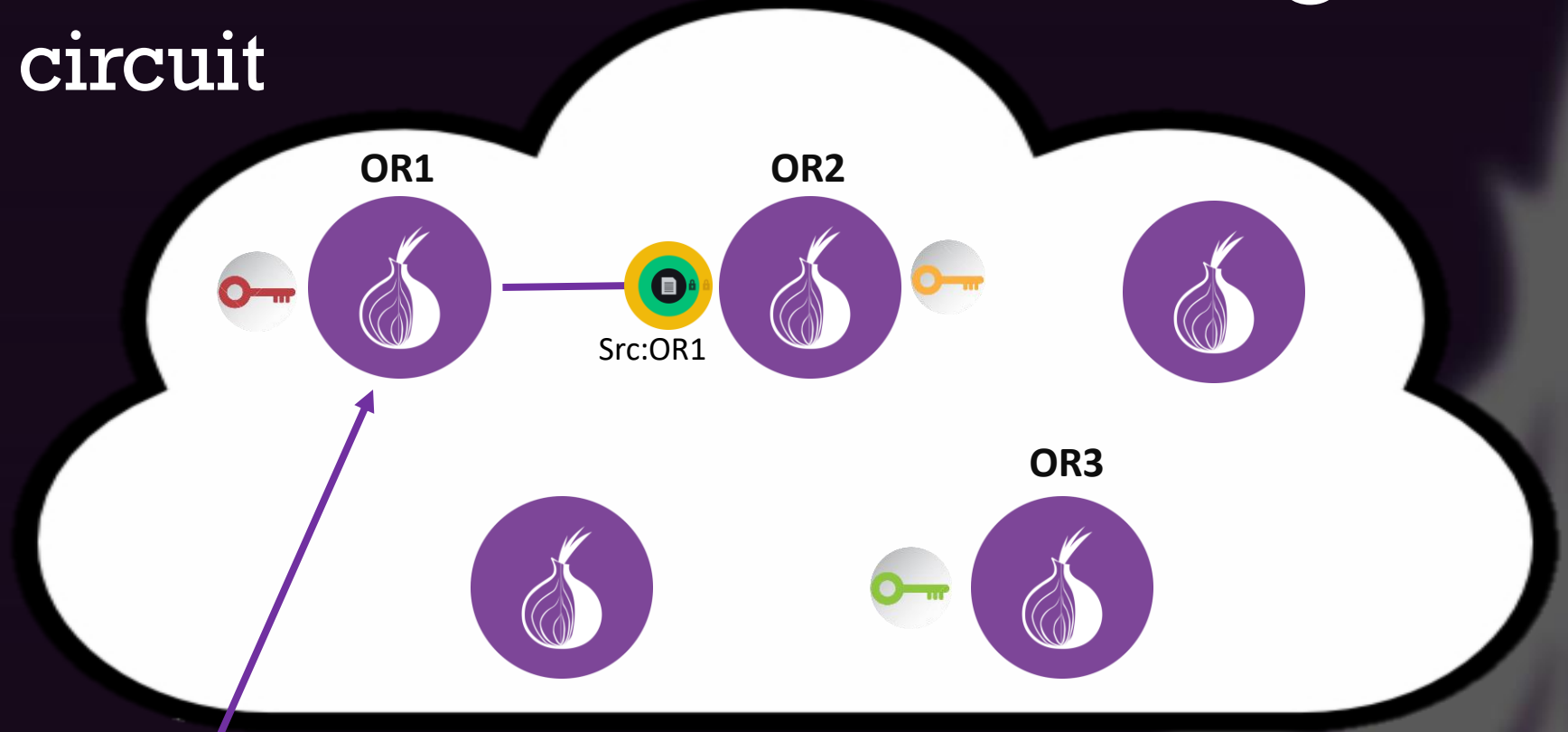
The Tor circuit

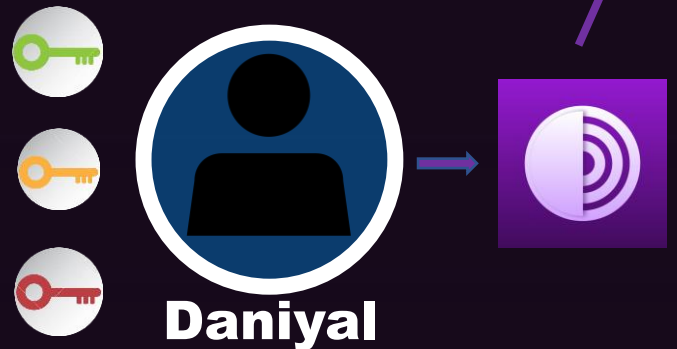




An internet connection through Tor

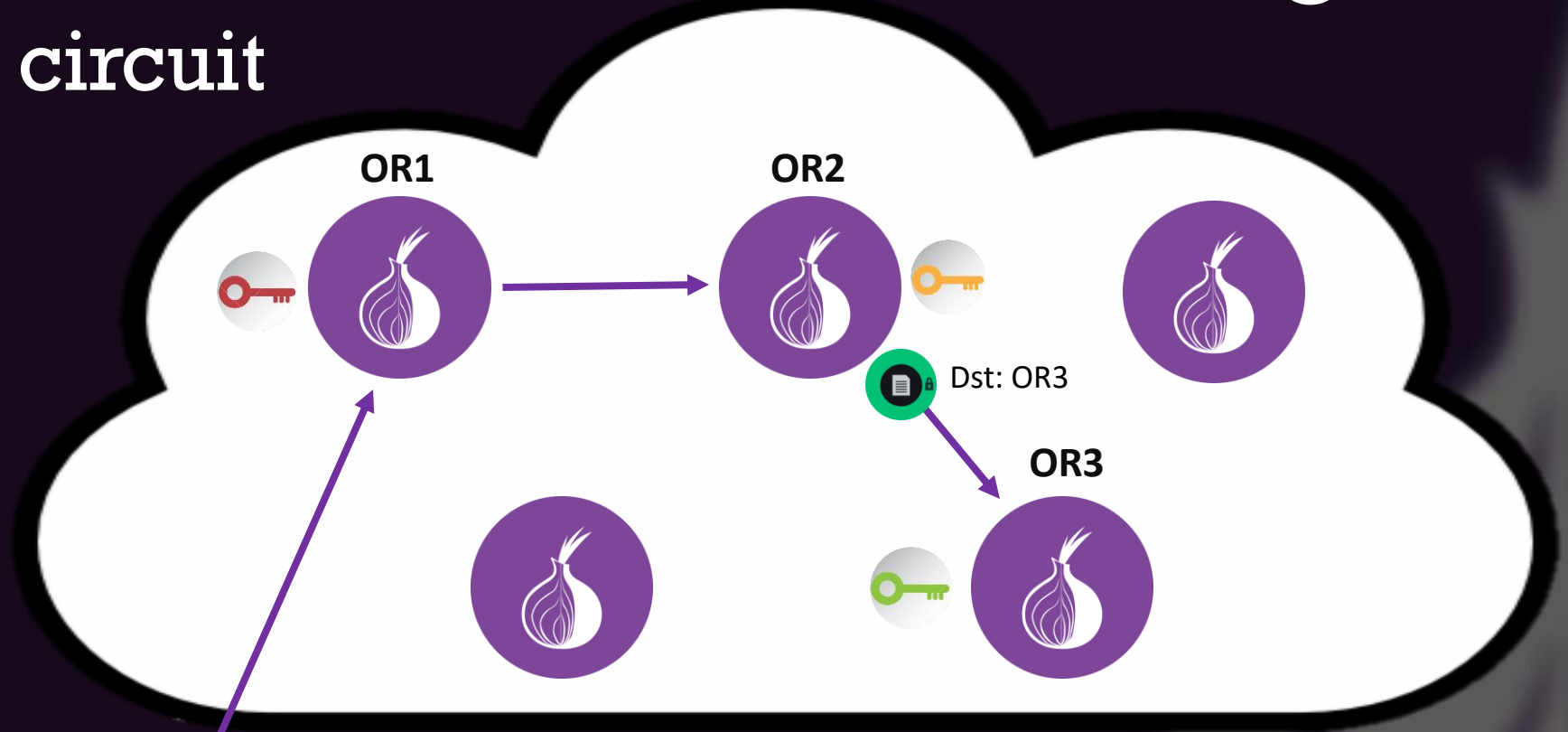
The Tor circuit

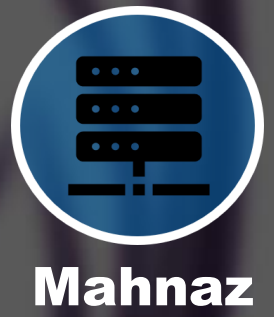




An internet connection through Tor

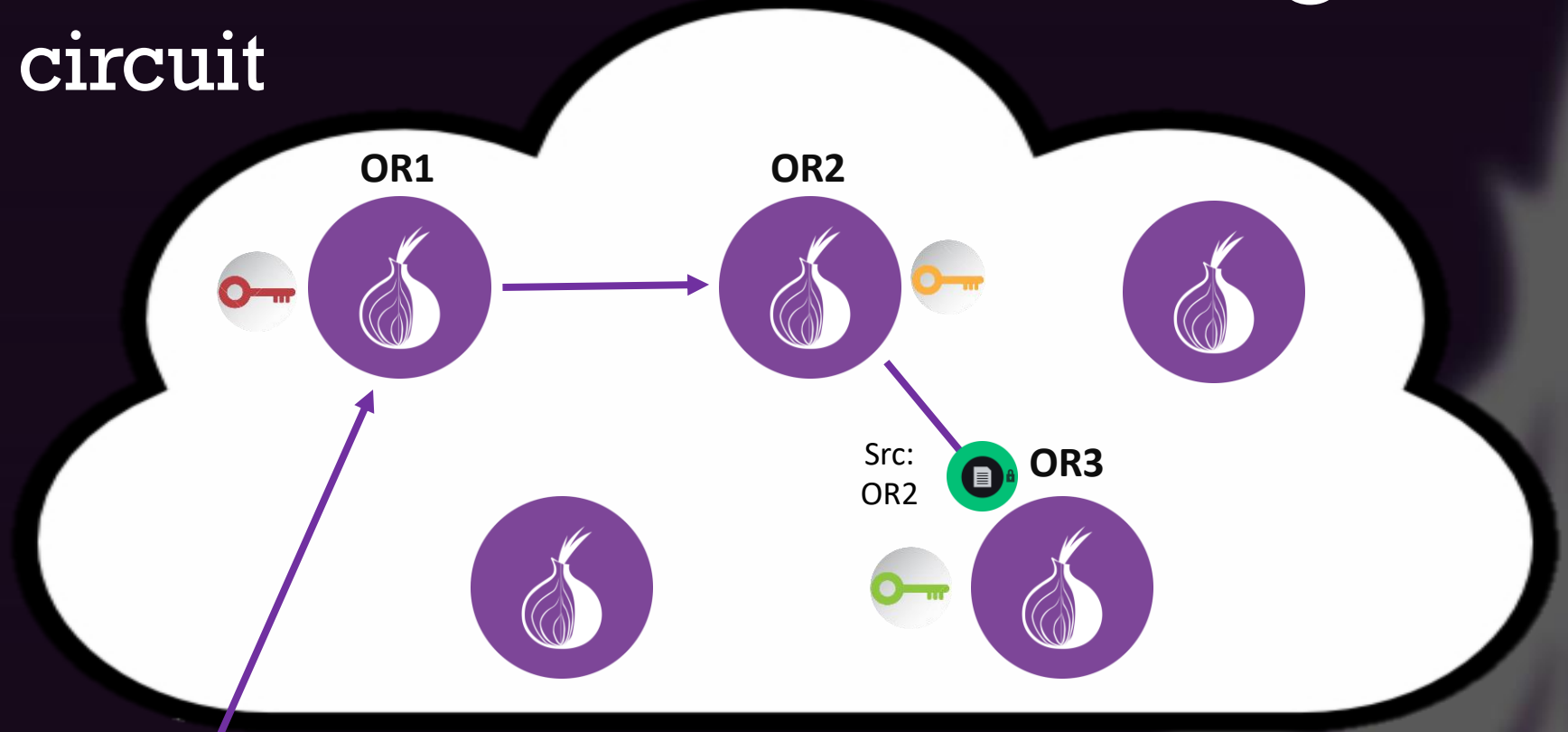
The Tor circuit





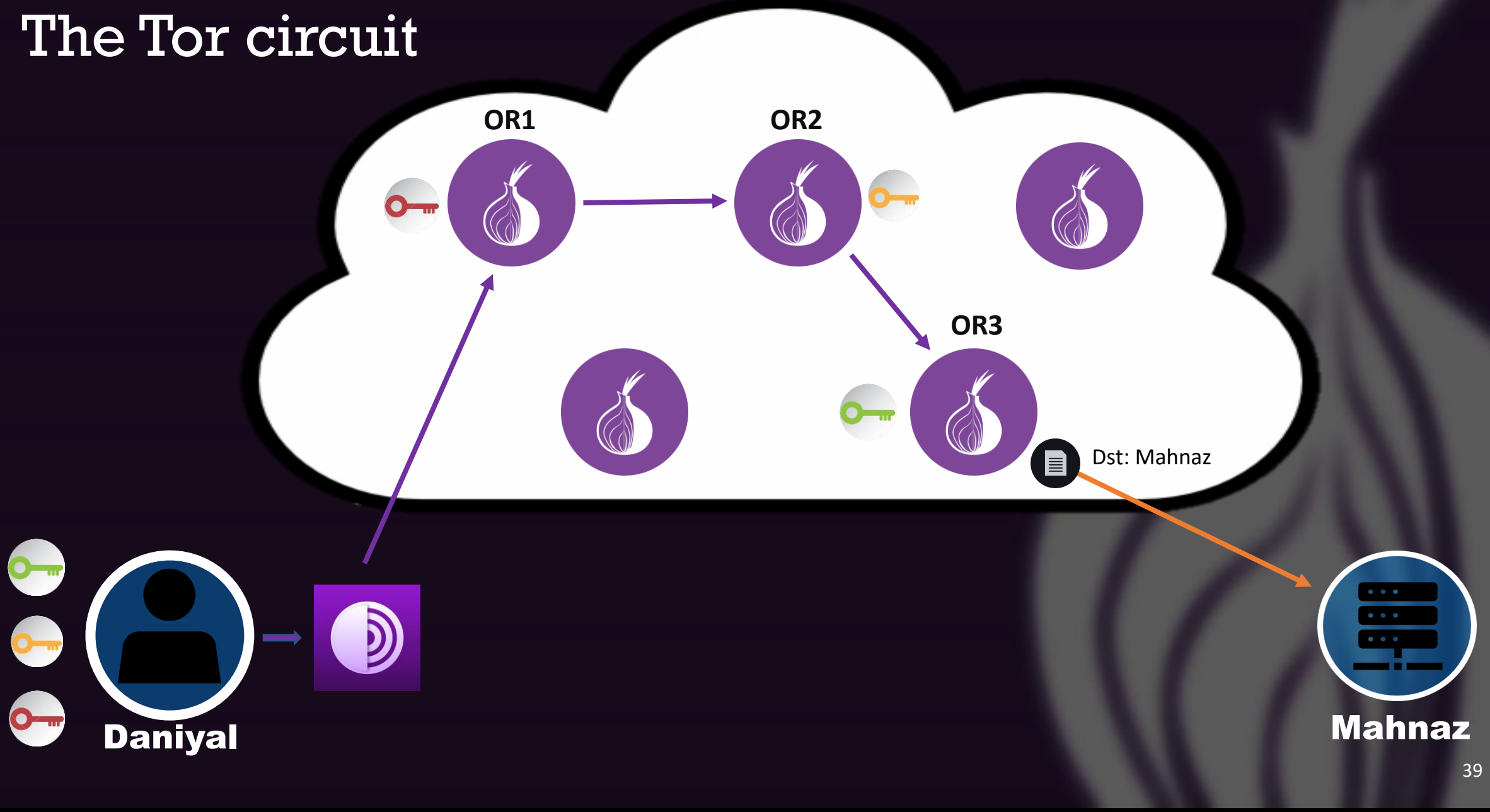
An internet connection through Tor

The Tor circuit



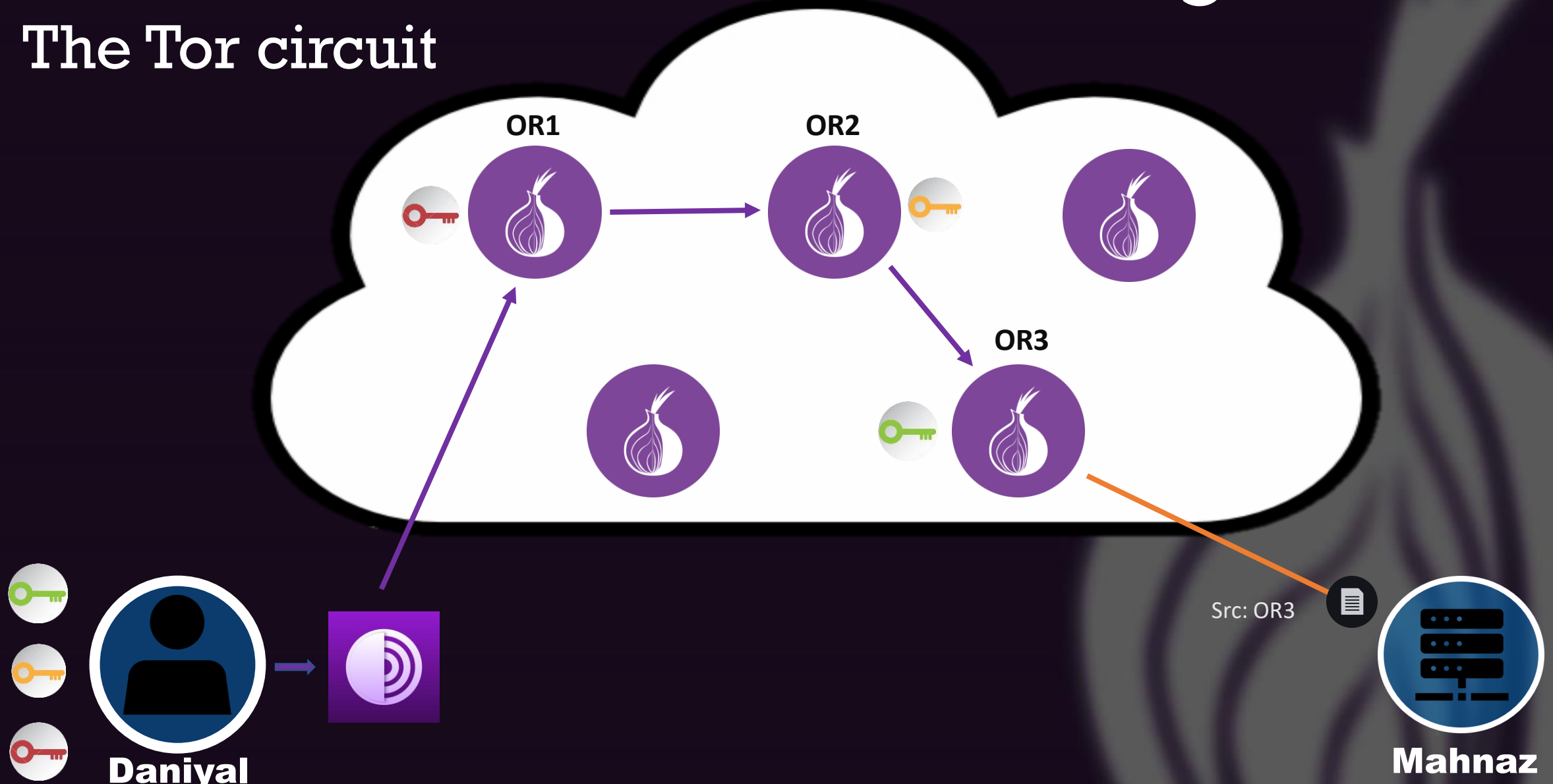
An internet connection through Tor

The Tor circuit



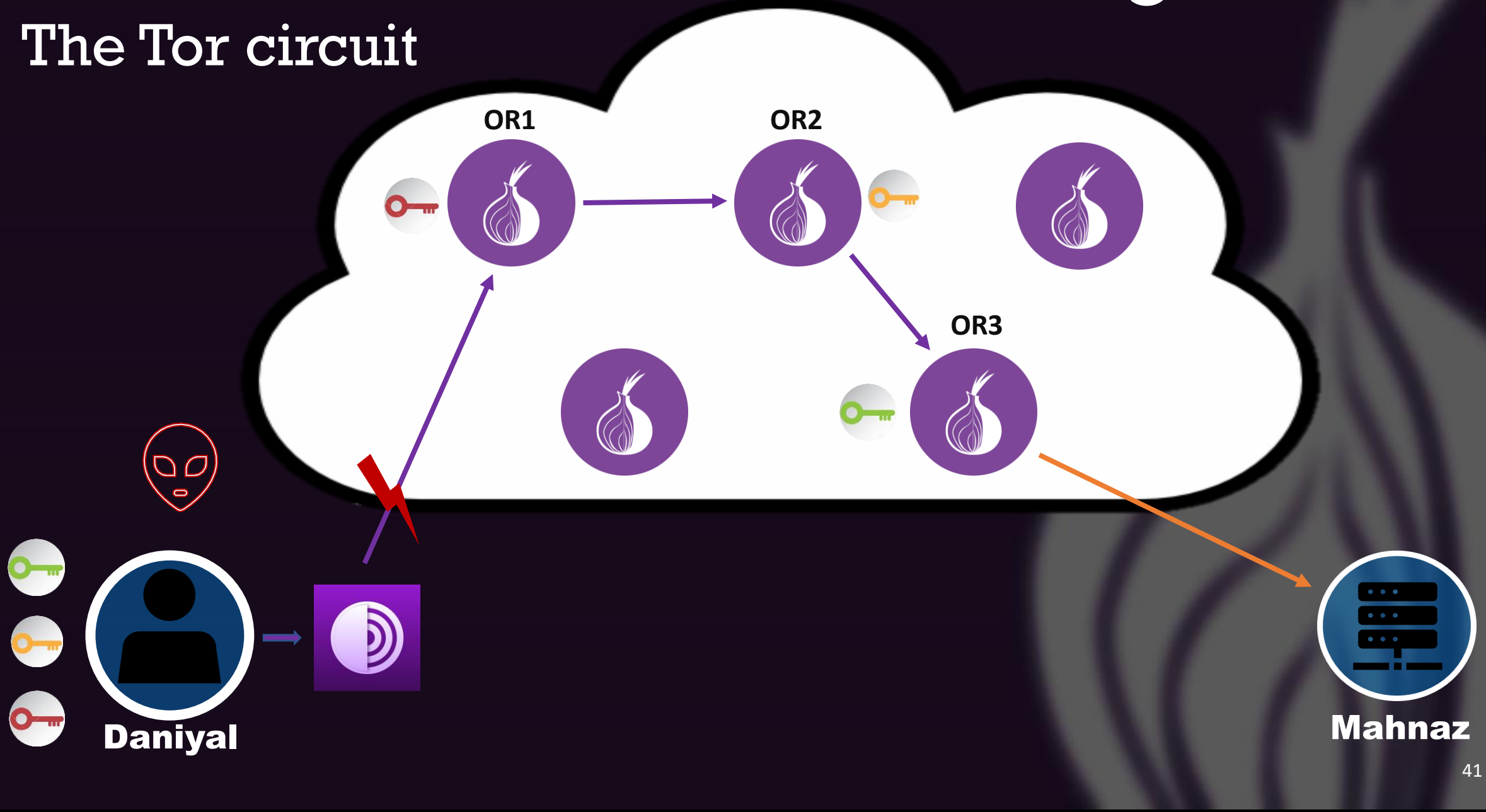
An internet connection through Tor

The Tor circuit



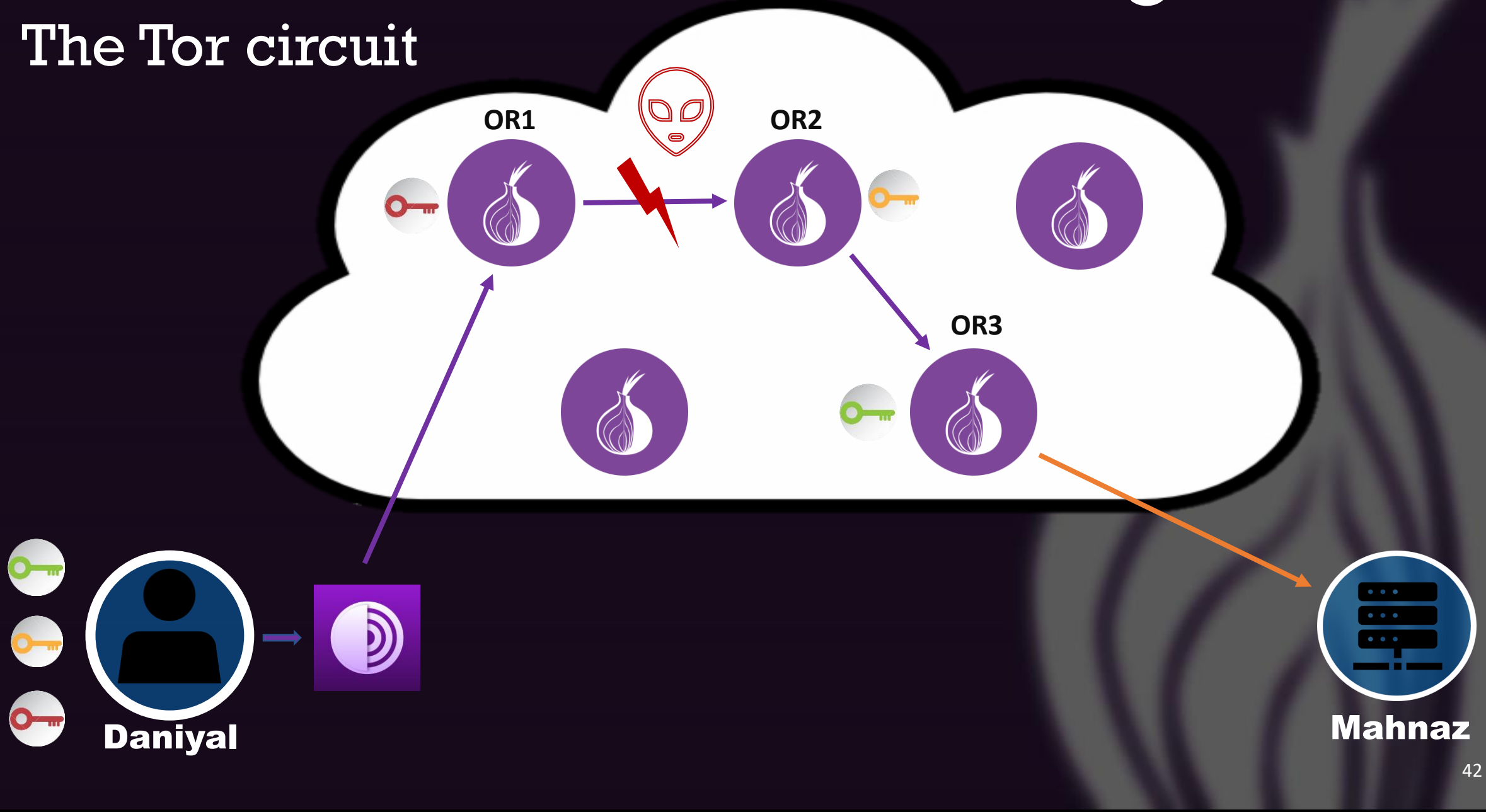
An internet connection through Tor

The Tor circuit



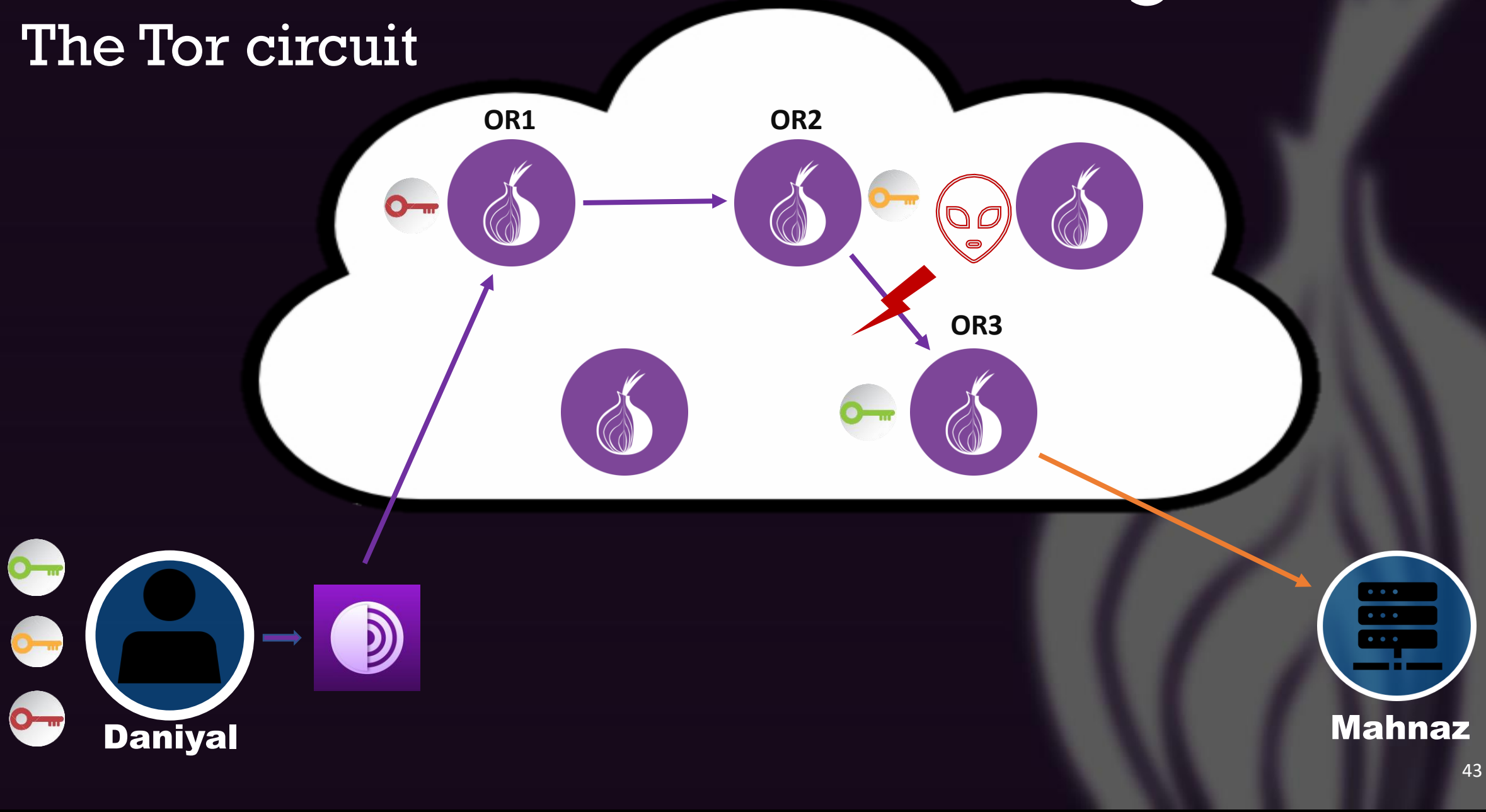
An internet connection through Tor

The Tor circuit



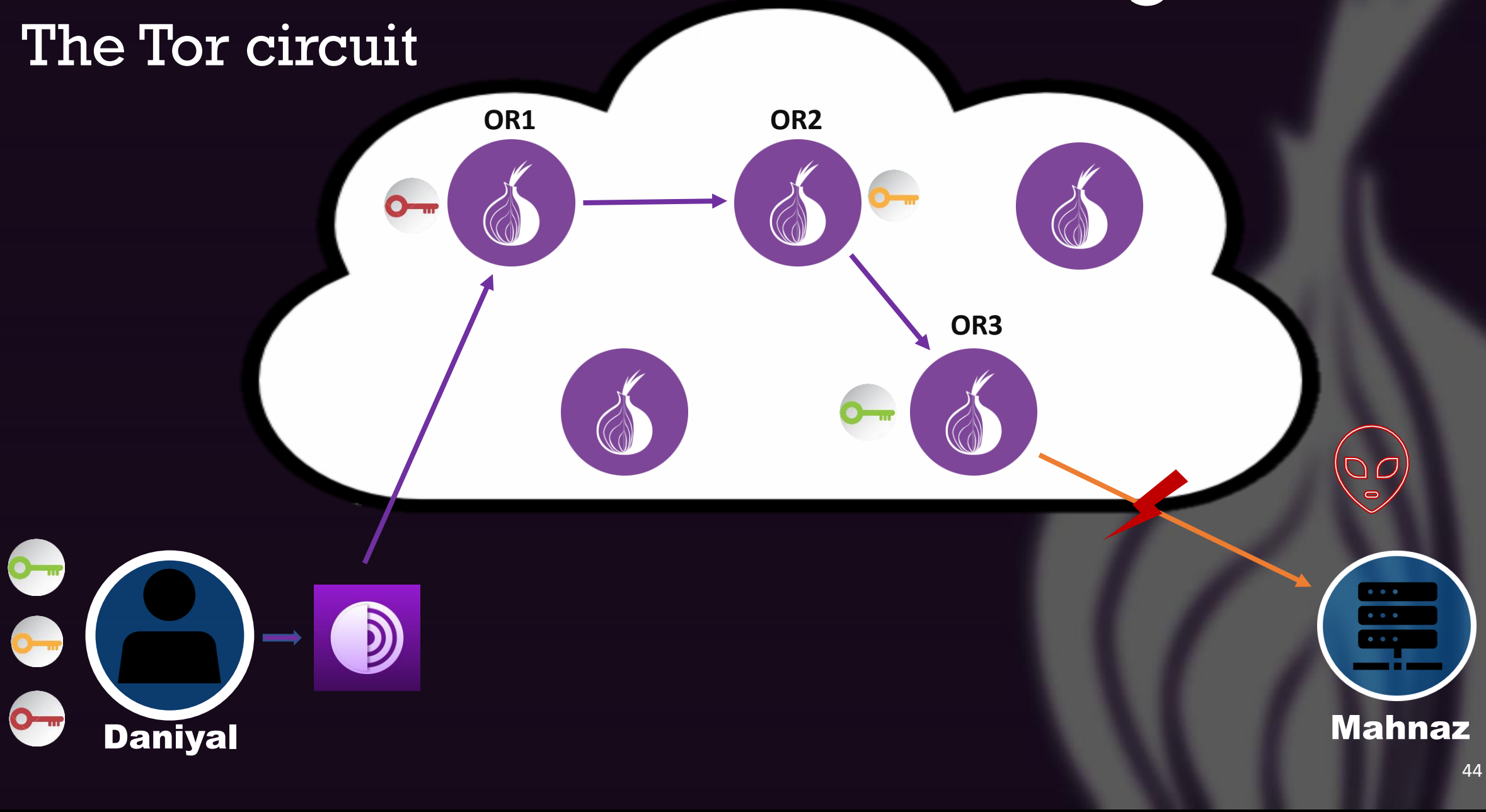
An internet connection through Tor

The Tor circuit



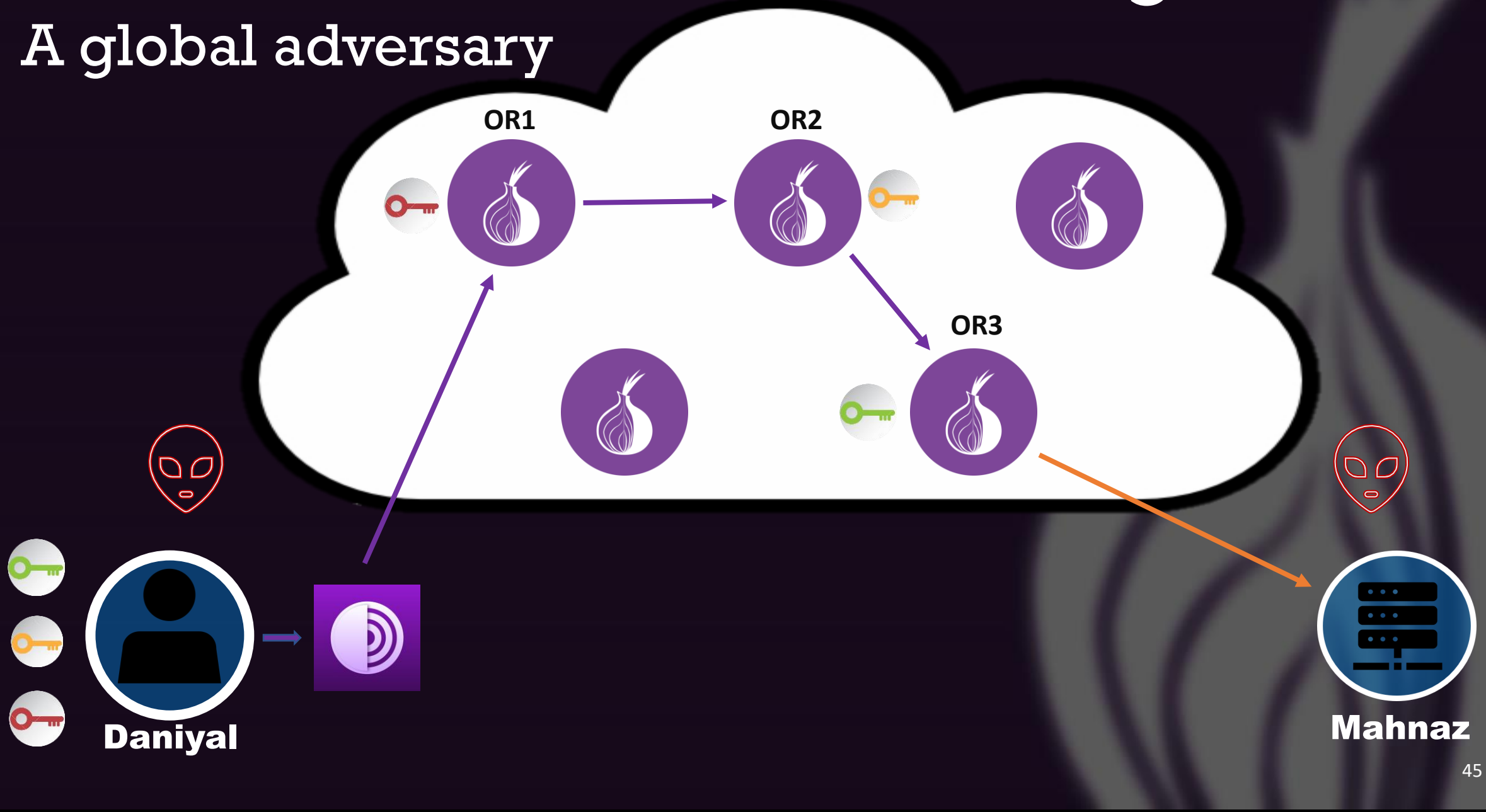
An internet connection through Tor

The Tor circuit



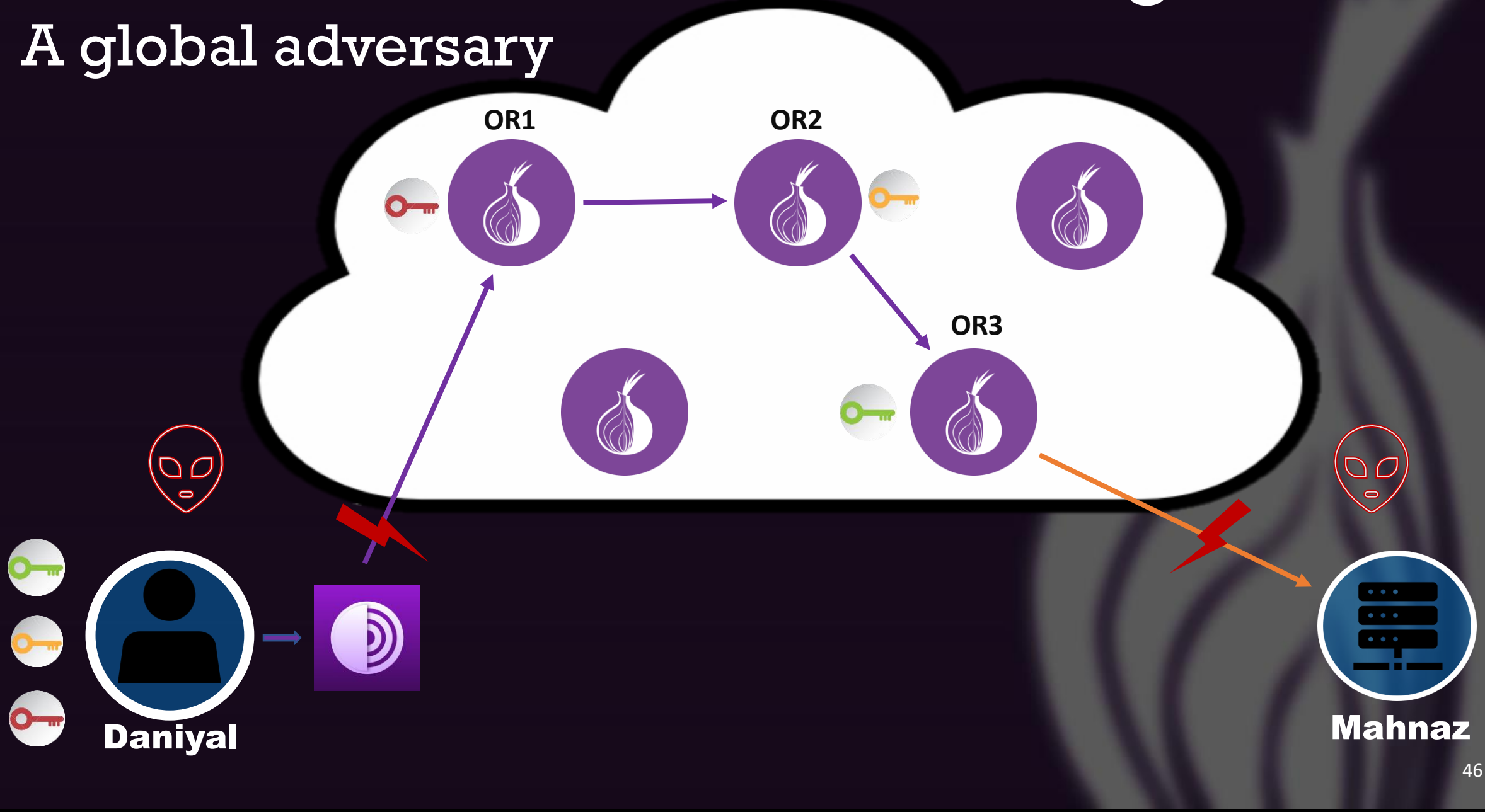
An internet connection through Tor

A global adversary



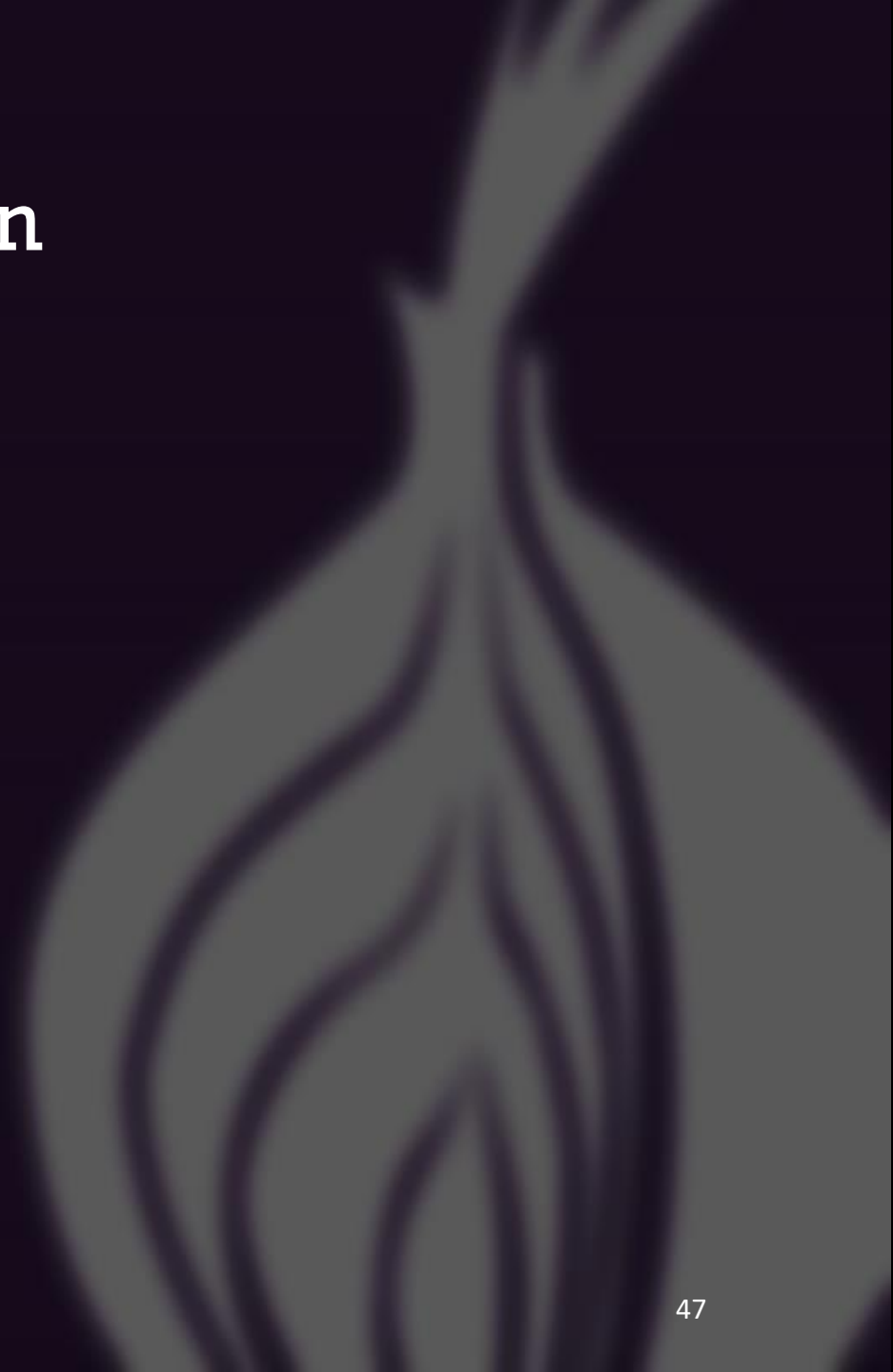
An internet connection through Tor

A global adversary



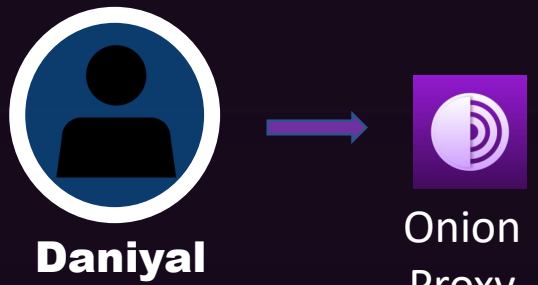
Differences

Tor vs. A regular internet connection



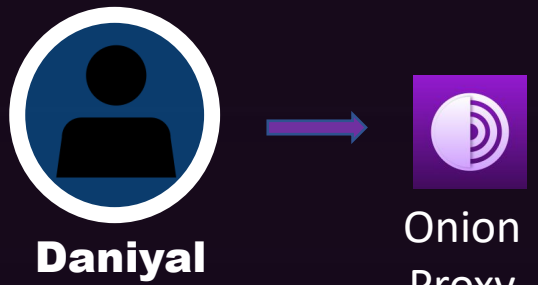
Differences

Tor vs. A regular internet connection



Differences

Tor vs. A regular internet connection

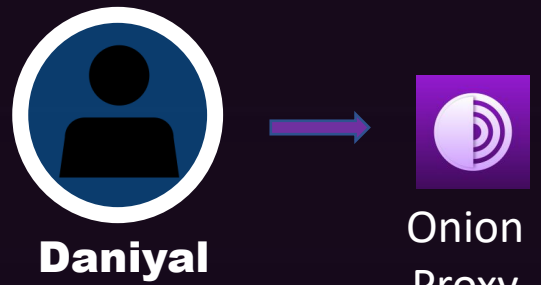


An Onion Proxy needs to be set up to route traffic through Tor:

- Use a regular browser configured to route traffic
- Use the Tor browser which comes preconfigured with the Tor proxy

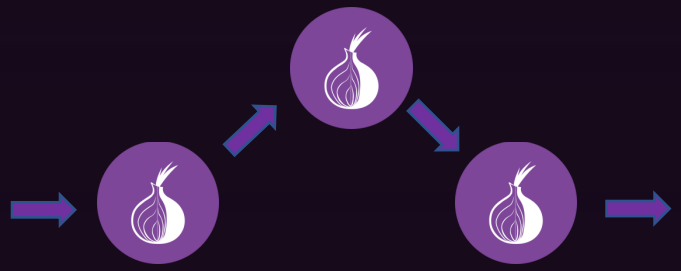
Differences

Tor vs. A regular internet connection



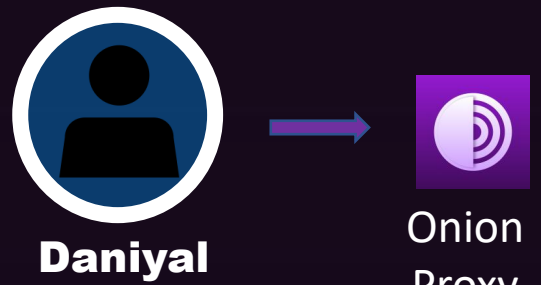
An Onion Proxy needs to be set up to route traffic through Tor:

- Use a regular browser configured to route traffic
- Use the Tor browser which comes preconfigured with the Tor proxy



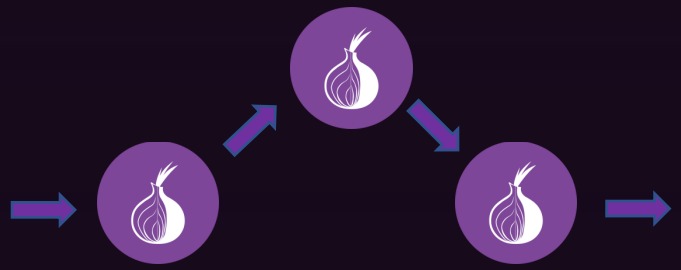
Differences

Tor vs. A regular internet connection



An Onion Proxy needs to be set up to route traffic through Tor:

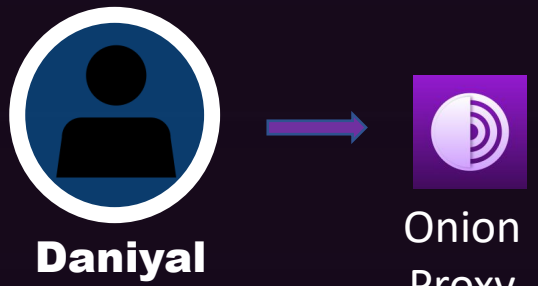
- Use a regular browser configured to route traffic
- Use the Tor browser which comes preconfigured with the Tor proxy



- Setting up a Tor circuit
- Network traffic is routed through a minimum of three Onion routers which are volunteered owned and operated

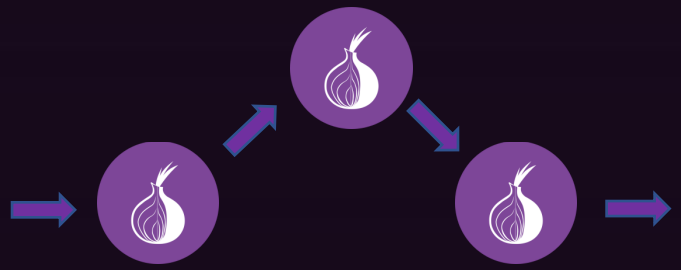
Differences

Tor vs. A regular internet connection

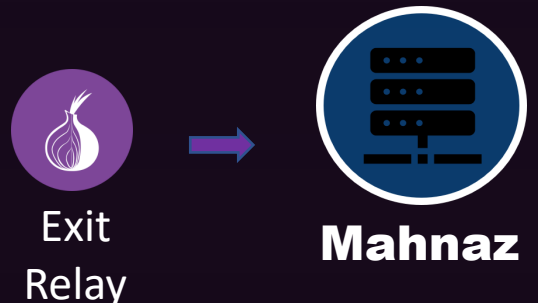


An Onion Proxy needs to be set up to route traffic through Tor:

- Use a regular browser configured to route traffic
- Use the Tor browser which comes preconfigured with the Tor proxy

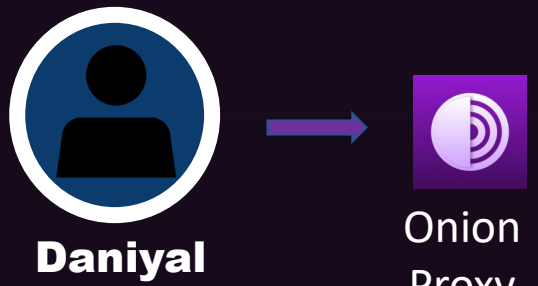


- Setting up a Tor circuit
- Network traffic is routed through a minimum of three Onion routers which are volunteered owned and operated



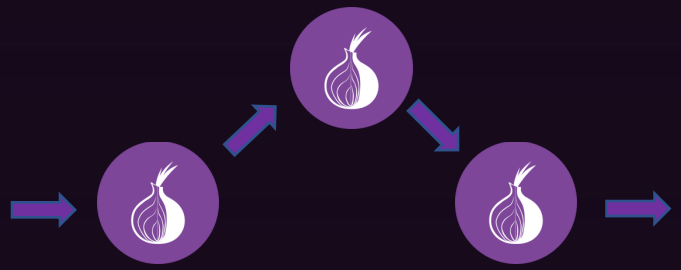
Differences

Tor vs. A regular internet connection

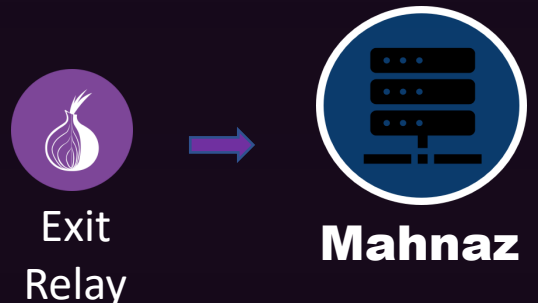


An Onion Proxy needs to be set up to route traffic through Tor:

- Use a regular browser configured to route traffic
- Use the Tor browser which comes preconfigured with the Tor proxy

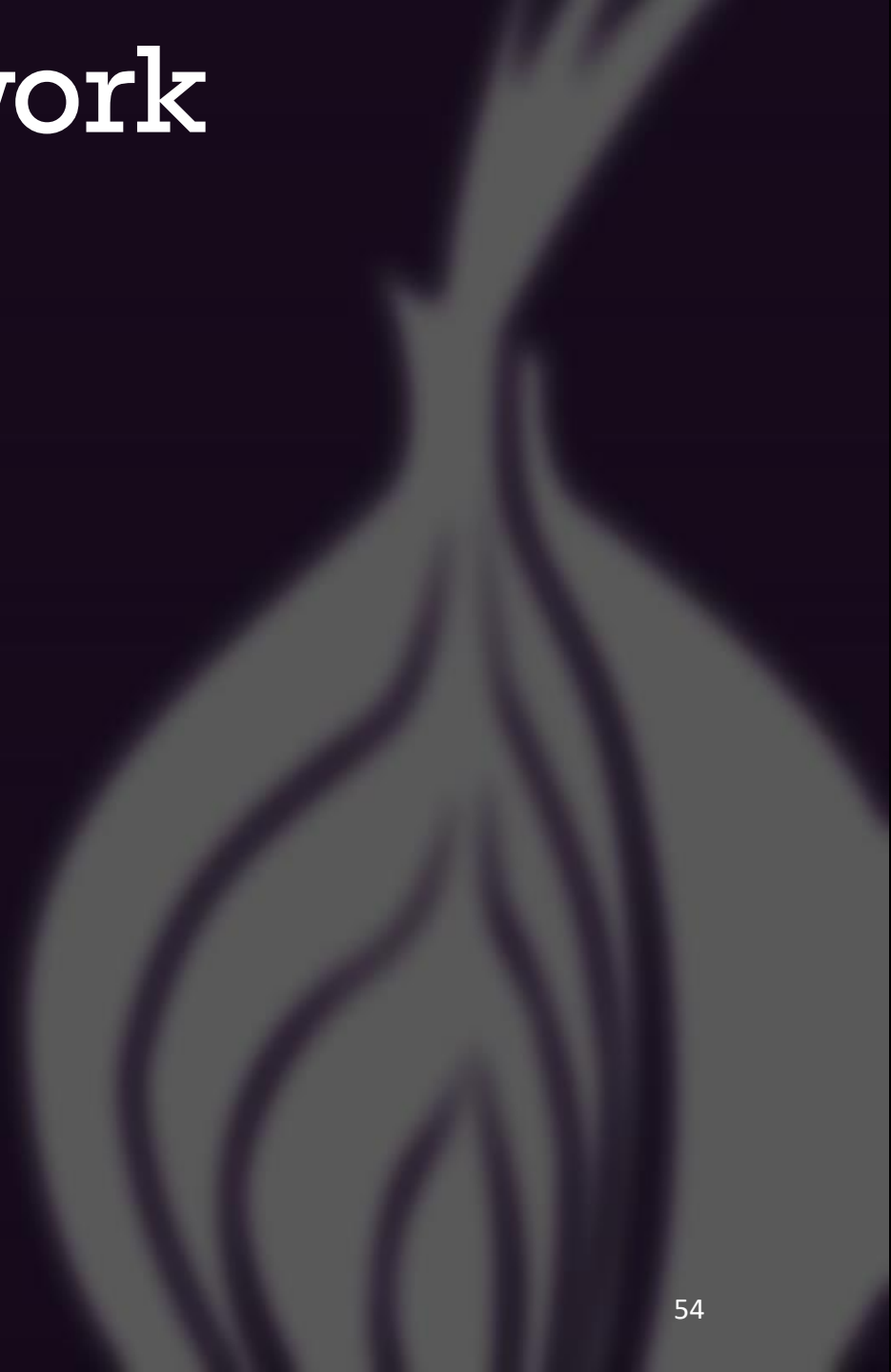


- Setting up a Tor circuit
- Network traffic is routed through a minimum of three Onion routers which are volunteered owned and operated



- The end server (Mahnaz) sees the traffic coming from the Exit Relay instead of the sender (Daniyal)

The Utility of the Tor Network



The Utility of the Tor Network

- The number of people who can successfully access the Tor network as compared to the number of people trying to access the Tor network

The Utility of the Tor Network

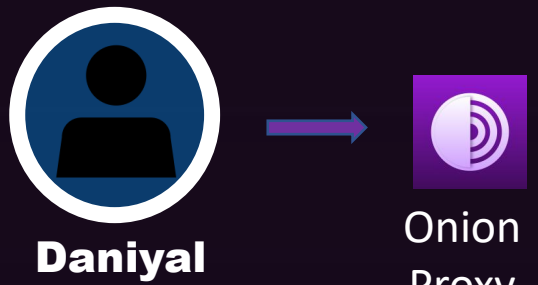
- The number of people who can successfully access the Tor network as compared to the number of people trying to access the Tor network

- The extra latency and bandwidth challenges that Tor users experience as compared to an individual trying to access web resources over the regular internet

The Utility of the Tor Network

- The number of people who can successfully access the Tor network as compared to the number of people trying to access the Tor network
- The extra latency and bandwidth challenges that Tor users experience as compared to an individual trying to access web resources over the regular internet
- The number of web resources on the regular internet that a Tor user can access

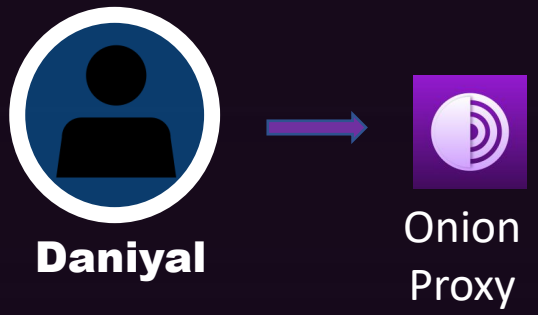
The number of people who can successfully access the Tor network as compared to the number of people trying to access the Tor network



An Onion Proxy needs to be set up to route traffic through Tor:

- Use a regular browser configured to route traffic through Tor
- Use the Tor browser which comes preconfigured with the Tor proxy

The number of people who can successfully access the Tor network as compared to the number of people trying to access the Tor network



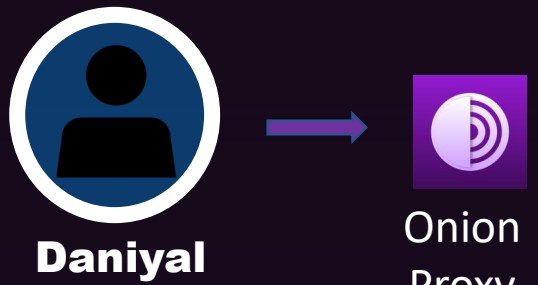
An Onion Proxy needs to be set up to route traffic through Tor:

- Use a regular browser configured to route traffic through Tor
- Use the Tor browser which comes preconfigured with the Tor proxy

Use a regular browser configured to route traffic through Tor

- Directions are not straightforward for a typical internet user
- Installation required knowledge of complicated jargon
- Validating whether Tor proxy is working is not straightforward

The number of people who can successfully access the Tor network as compared to the number of people trying to access the Tor network



An Onion Proxy needs to be set up to route traffic through Tor:

- Use a regular browser configured to route traffic through Tor
- Use the Tor browser which comes preconfigured with the Tor proxy

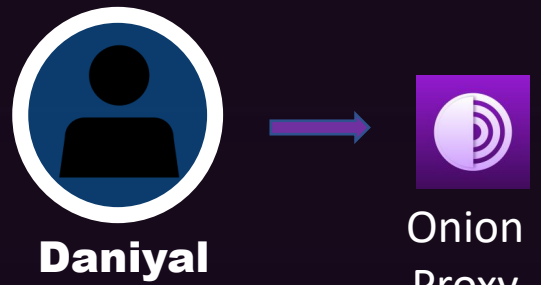
Use a regular browser configured to route traffic through Tor

- Directions are not straightforward for a typical internet user
- Installation required knowledge of complicated jargon
- Validating whether Tor proxy is working is not straightforward

Using the Tor browser

Challenge	Category label
Broken Functionality	Broken websites
	Reduced productivity
	Shopping
Geolocation	Geolocation
Latency	Slower Access
Differential Treatment	CAPTCHAs/Pages inaccessible

The number of people who can successfully access the Tor network as compared to the number of people trying to access the Tor network



An Onion Proxy needs to be set up to route traffic through Tor:

- Use a regular browser configured to route traffic through Tor
- Use the Tor browser which comes preconfigured with the Tor proxy

Use a regular browser configured to route traffic through Tor

- Directions are not straightforward for a typical internet user
- Installation required knowledge of complicated jargon
- Validating whether Tor proxy is working is not straightforward

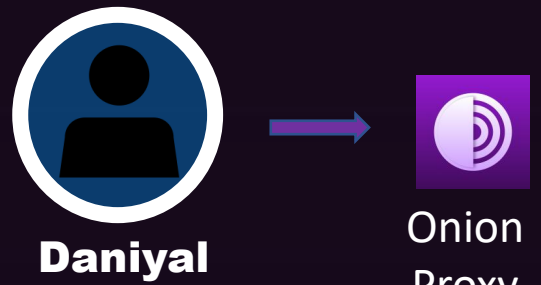
Using the Tor browser

Challenge	Category label
Broken Functionality	Broken websites
	Reduced productivity
	Shopping
Geolocation	Geolocation
Latency	Slower Access
Differential Treatment	CAPTCHAs/Pages inaccessible

Censorship of Tor

- Access blocked to the Tor Project's website
- Access blocked to publicly listed relays in the consensus document
- Analysis of Tor traffic, blocking Tor connections

The number of people who can successfully access the Tor network as compared to the number of people trying to access the Tor network



An Onion Proxy needs to be set up to route traffic through Tor:

- Use a regular browser configured to route traffic through Tor
- Use the Tor browser which comes preconfigured with the Tor proxy

Use a regular browser configured to route traffic through Tor

- Directions are not straight… typical internet user
- Installation required know… complicated jargon
- Validating whether Tor proxy is working is not straightforward

Using the Tor browser

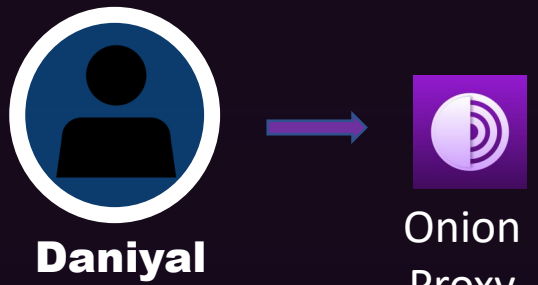
Challenge	Category label
…onality	Broken websites
	Reduced productivity
	Shopping
Geolocation	Geolocation
Latency	Slower Access
Differential Treatment	CAPTCHAs/Pages inaccessible

USABILITY

Censorship of Tor

- Access blocked to the Tor Project's website
- Access blocked to publicly listed relays in the consensus document
- Active analysis of Tor traffic, blocking Tor connections

The number of people who can successfully access the Tor network as compared to the number of people trying to access the Tor network



An Onion Proxy needs to be set up to route traffic through Tor:

- Use a regular browser configured to route traffic through Tor
- Use the Tor browser which comes preconfigured with the Tor proxy

Use a regular browser configured to route traffic through Tor

- Directions are not straight… typical internet user
- Installation required know… complicated jargon
- Validating whether Tor proxy is working is not straightforward

Using the Tor browser

Challenge	Category label
…onality	Broken websites
	Reduced productivity
	Shopping
Geolocation	Geolocation
Latency	Slower Access
Differential Treatment	CAPTCHAs/Pages inaccessible

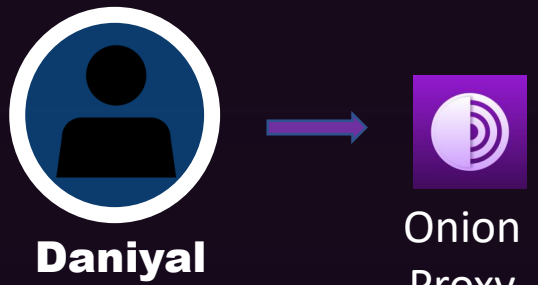
USABILITY

Censorship of Tor

- Access blocked to the Tor Project's w…
- A… …ys in the consensus document
- Active analysis of Tor traffic, blocking Tor connections

CENSORSHIP

The number of people who can successfully access the Tor network as compared to the number of people trying to access the Tor network



An Onion Proxy needs to be set up to route traffic through Tor:

- Use a regular browser configured to route traffic through Tor
- Use the Tor browser which comes preconfigured with the Tor proxy

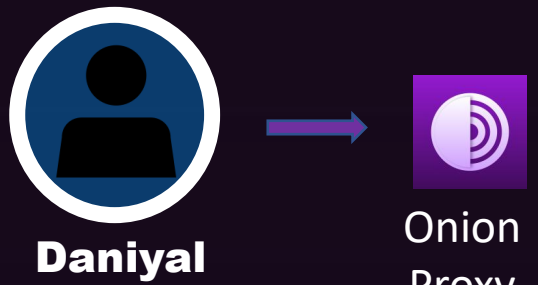
USABILITY

Peeling the Onion's User Experience Layer: Examining Naturalistic Use of the Tor Browser

Kevin Gallagher, New York University, kevin.gallagher@nyu.edu
Sameer Patil, Indiana University Bloomington, patil@indiana.edu
Brendan Dolan-Gavitt, New York University, brendandg@nyu.edu

- 50% of all participants report some type of functional hindrance
- Biggest issues were latency and functionality breaks
- Users also reported lack of trust due to unrefined UX of the browser

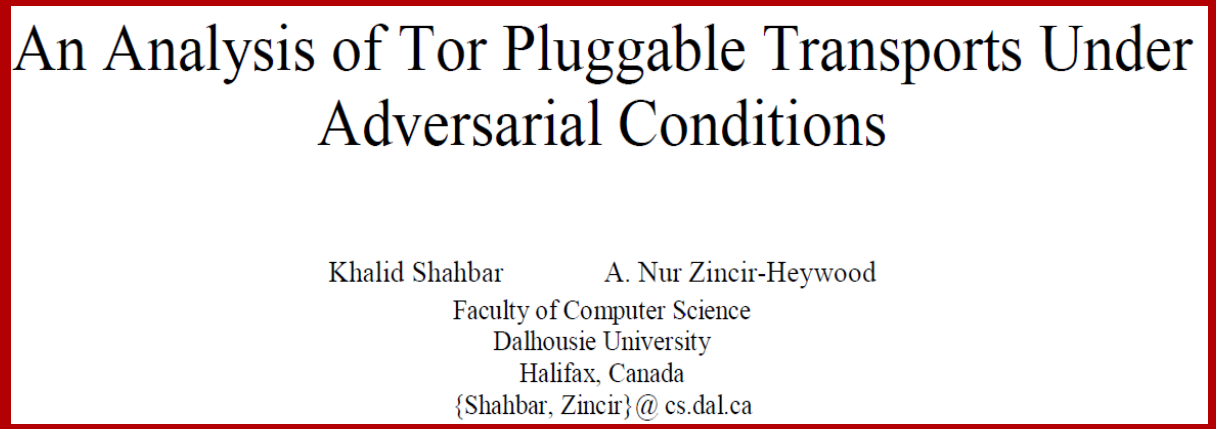
The number of people who can successfully access the Tor network as compared to the number of people trying to access the Tor network



An Onion Proxy needs to be set up to route traffic through Tor:

- Use a regular browser configured to route traffic through Tor
- Use the Tor browser which comes preconfigured with the Tor proxy

CENSORSHIP

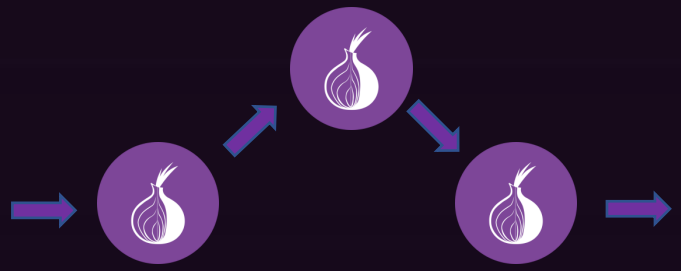


An Analysis of Tor Pluggable Transports Under Adversarial Conditions

Khalid Shahbar A. Nur Zincir-Heywood
Faculty of Computer Science
Dalhousie University
Halifax, Canada
{Shahbar, Zincir}@ cs.dal.ca

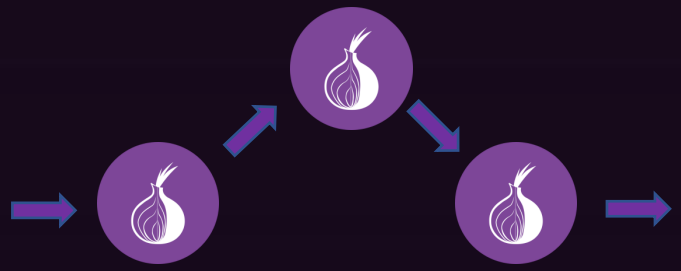
- Tor traffic is identifiable by censors due to certain unique characteristics
- Methods to hide Tor traffic are ineffective
- Tor traffic can be identified with an accuracy of > 90% even if it is made to look like any other protocol's traffic

The extra latency and bandwidth challenges that Tor users experience as compared to an individual trying to access web resources over the regular internet



- Setting up a Tor Circuit
- Network traffic is routed through a minimum of three Onion routers which are volunteered owned and operated

The extra latency and bandwidth challenges that Tor users experience as compared to an individual trying to access web resources over the regular internet

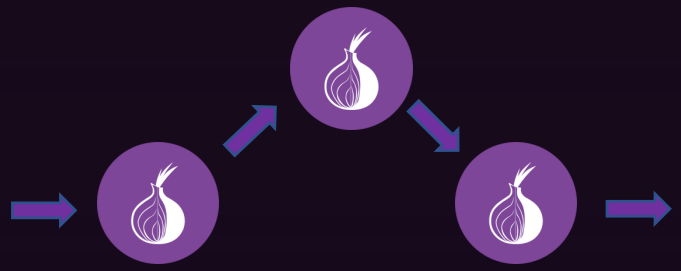


- Setting up a Tor Circuit
- Network traffic is routed through a minimum of three Onion routers which are volunteered owned and operated

Tor Circuit setup

- Requires extra steps and hence extra time before a connection to the internet can be established

The extra latency and bandwidth challenges that Tor users experience as compared to an individual trying to access web resources over the regular internet



- Setting up a Tor Circuit
- Network traffic is routed through a minimum of three Onion routers which are volunteered owned and operated

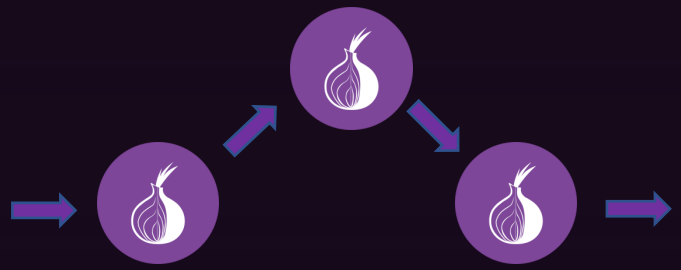
Tor Circuit setup

- Requires extra steps and hence extra time before a connection to the internet can be established

Traffic routing through Tor relays

- User's traffic is routed through at least 3 Tor relays before it reaches the end server adding extra latency
- The Tor relays are volunteer owned and operated network resources and are hence limited in number

The extra latency and bandwidth challenges that Tor users experience as compared to an individual trying to access web resources over the regular internet



- Setting up a Tor Circuit
- Network traffic is routed through a minimum of three Onion routers which are volunteered owned and operated

LATENCY

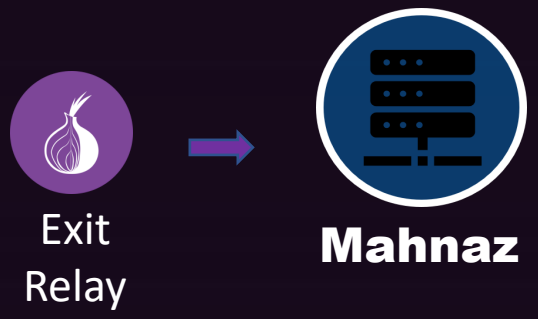
NavigaTor: Finding Faster Paths to Anonymity

Robert Annessi*
Institute of Telecommunications, TU Wien
Gusshausstr. 25/E389, 1040 Vienna, Austria
robert.annessi@nt.tuwien.ac.at
**Corresponding author*

Martin Schmiedecker
SBA Research
Favoritenstraße 16, 1040 Vienna, Austria
mschmiedecker@sba-research.org

- Tor is slower than regular traffic due to the very nature of the network itself
- Evaluating circuit build times and congestion awareness can reduce the latency experienced by a user
- There is a tradeoff between anonymity and latency

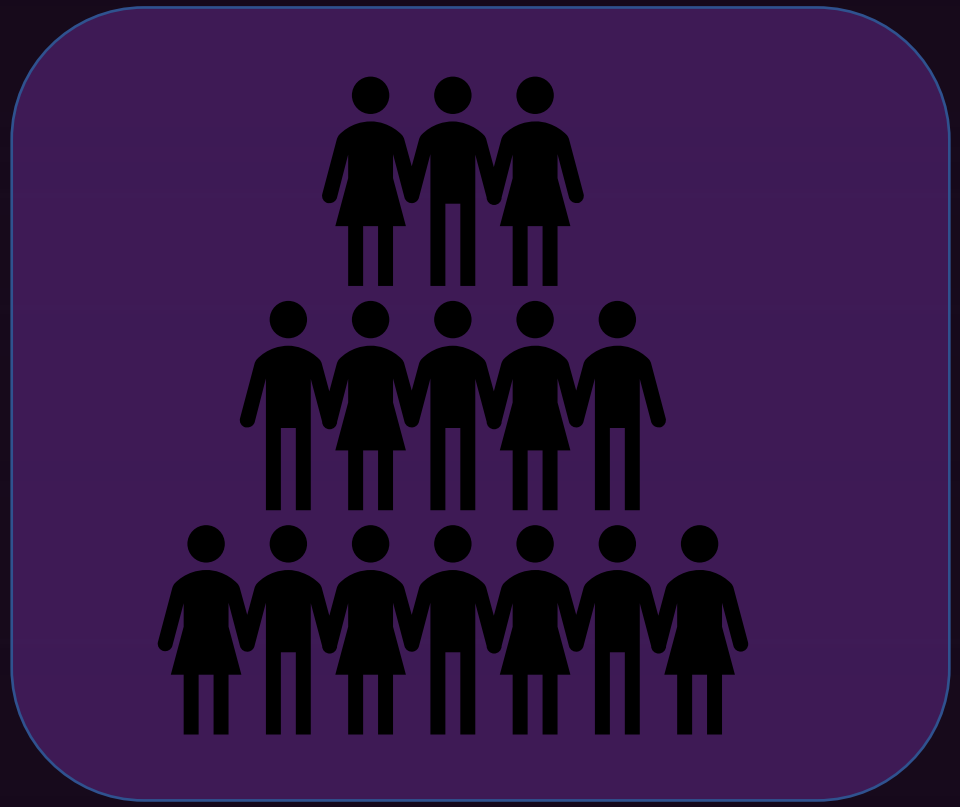
The number of web resources on the regular internet that a Tor user can access



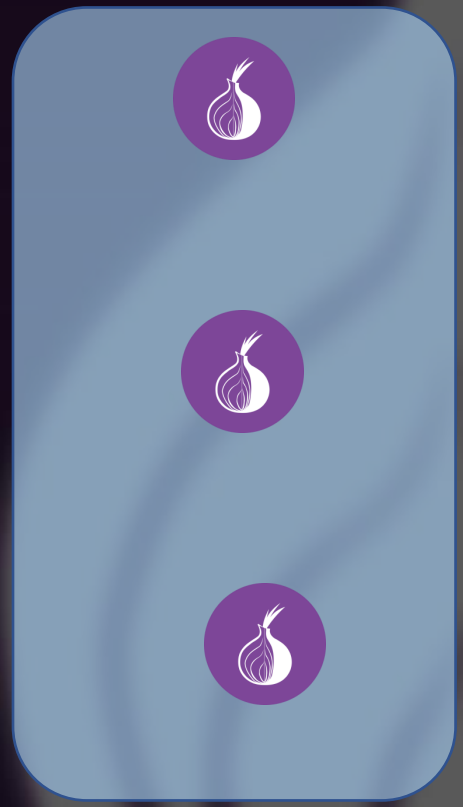
- The end server (Mahnaz) sees the traffic coming from the Exit Relay instead of the sender (Daniyal)

The number of web resources on the regular internet that a Tor user can access

Fate Sharing



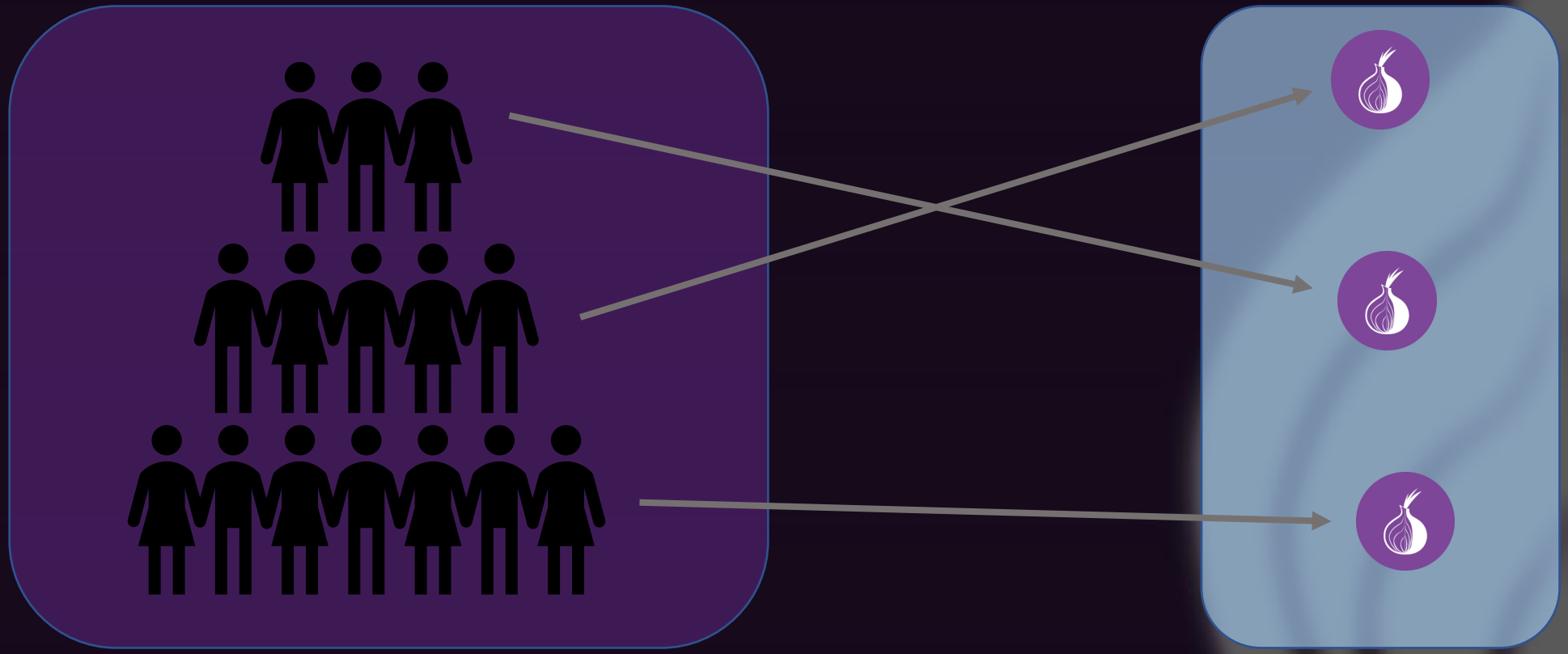
Tor users



Tor relays

The number of web resources on the regular internet that a Tor user can access

Fate Sharing

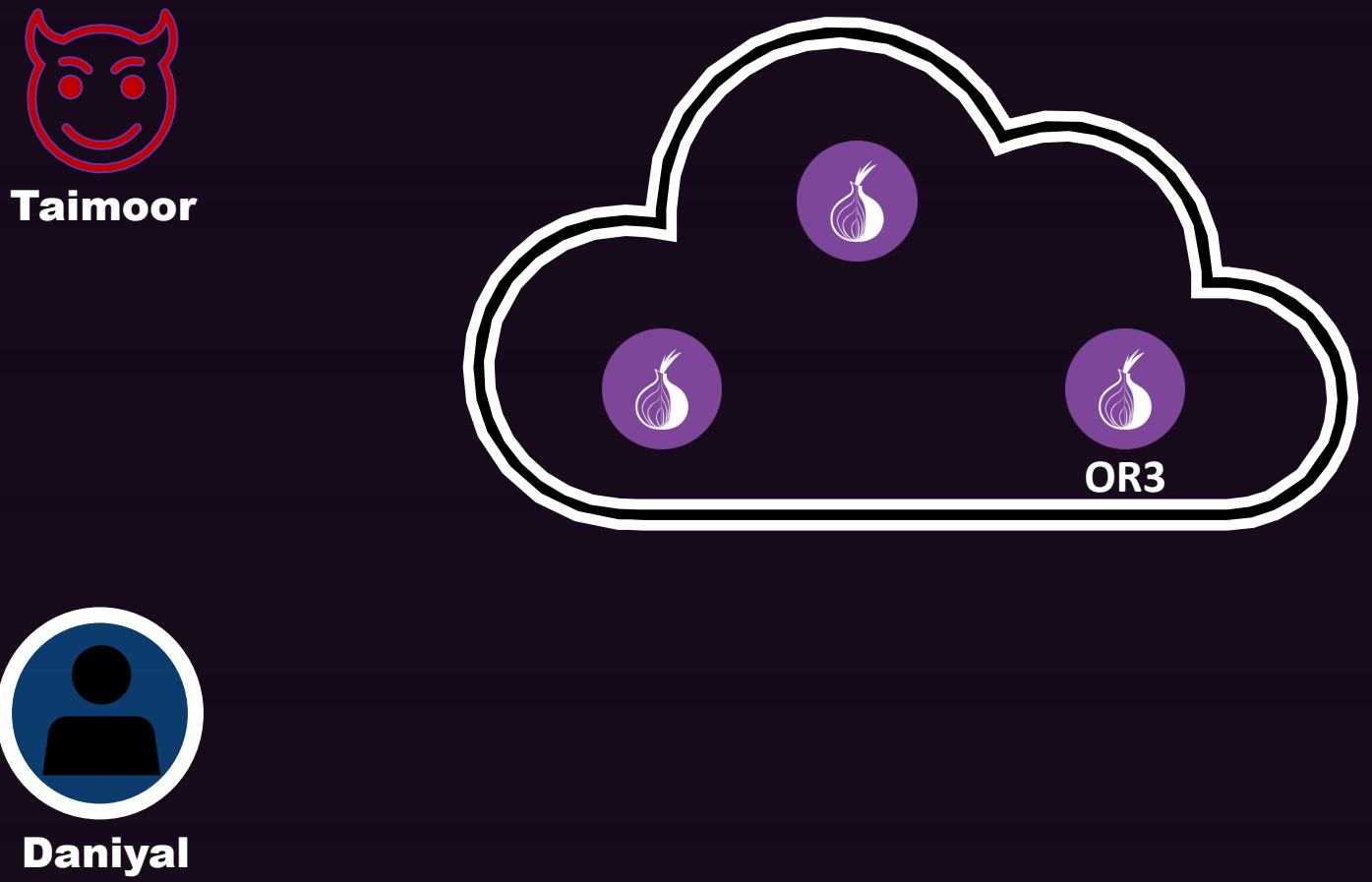


Tor users

Tor relays

The number of web resources on the regular internet that a Tor user can access

Fate Sharing

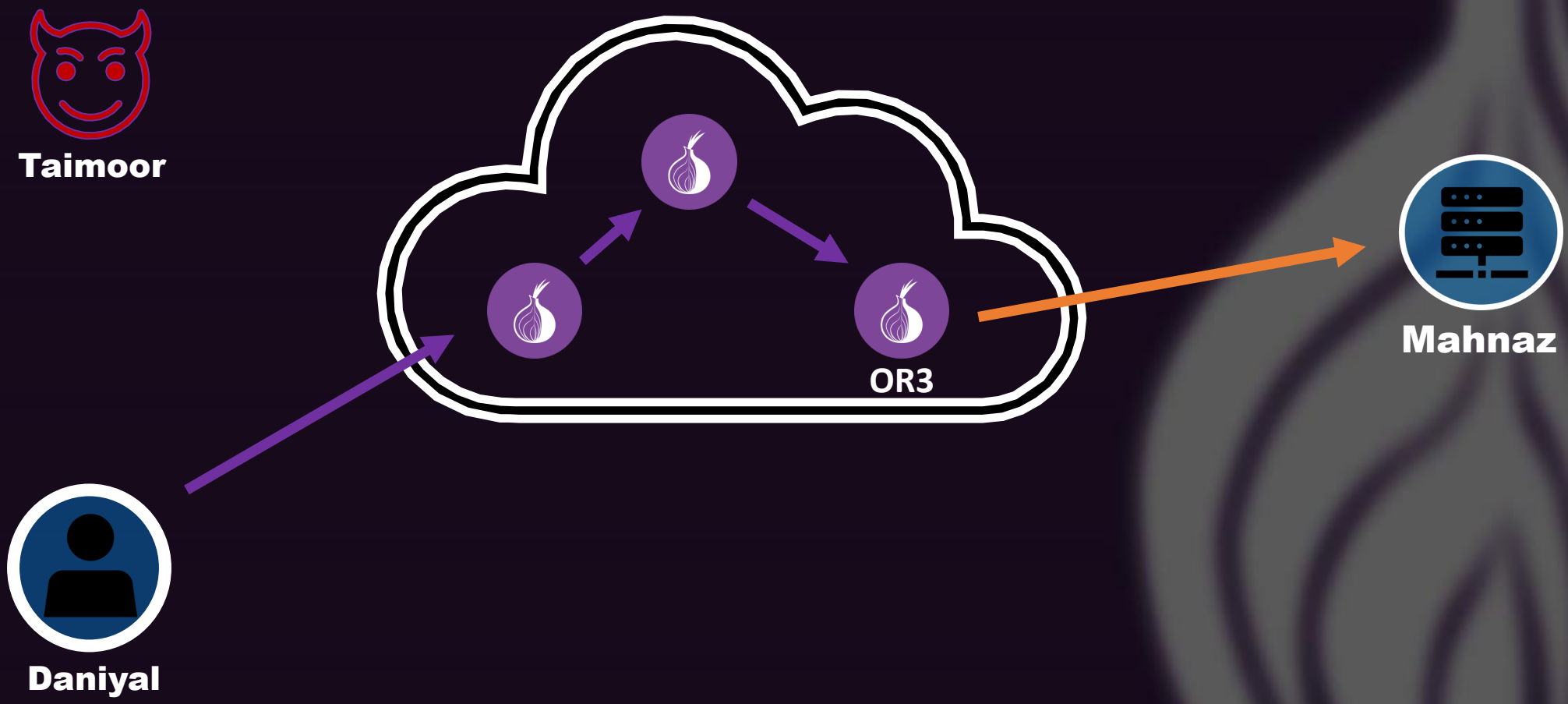


The number of web resources on the regular internet that a Tor user can access

Fate Sharing

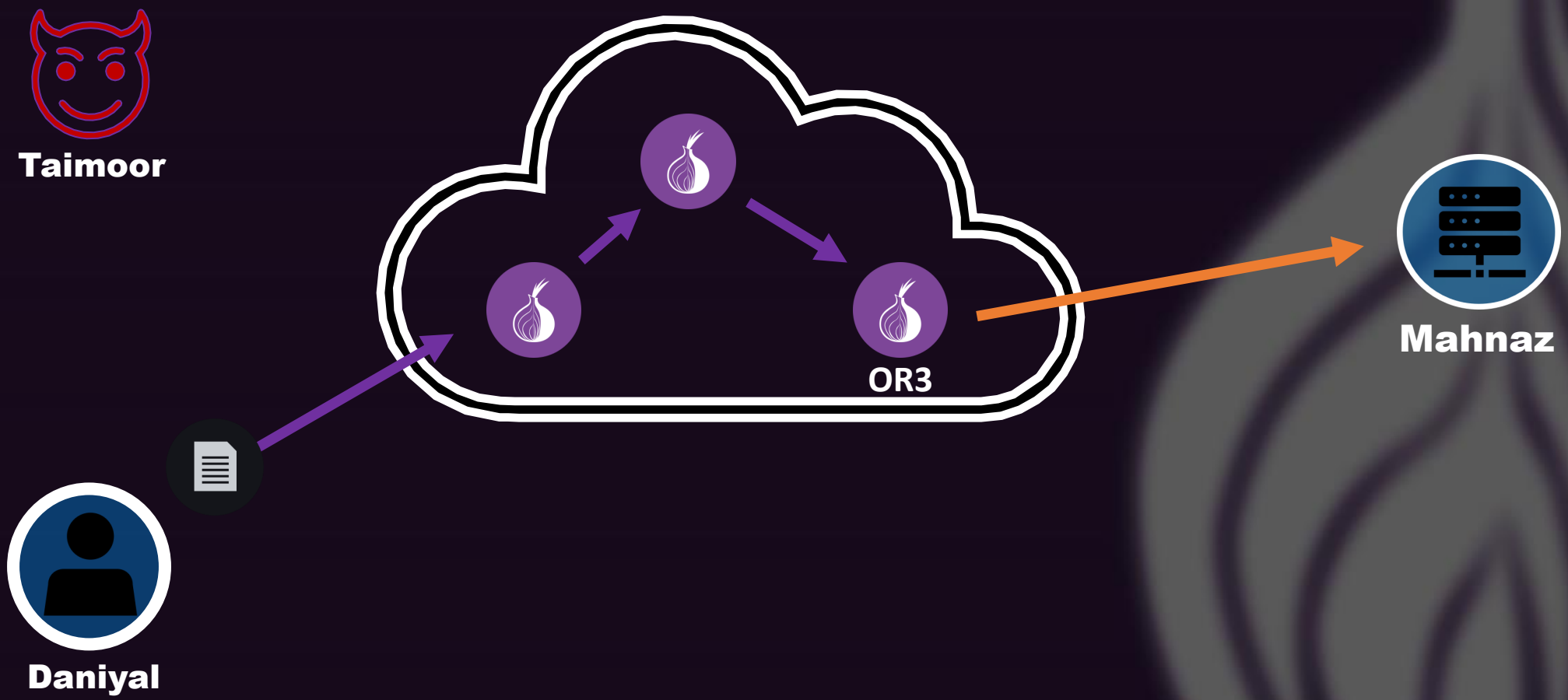
The number of web resources on the regular internet that a Tor user can access

Fate Sharing



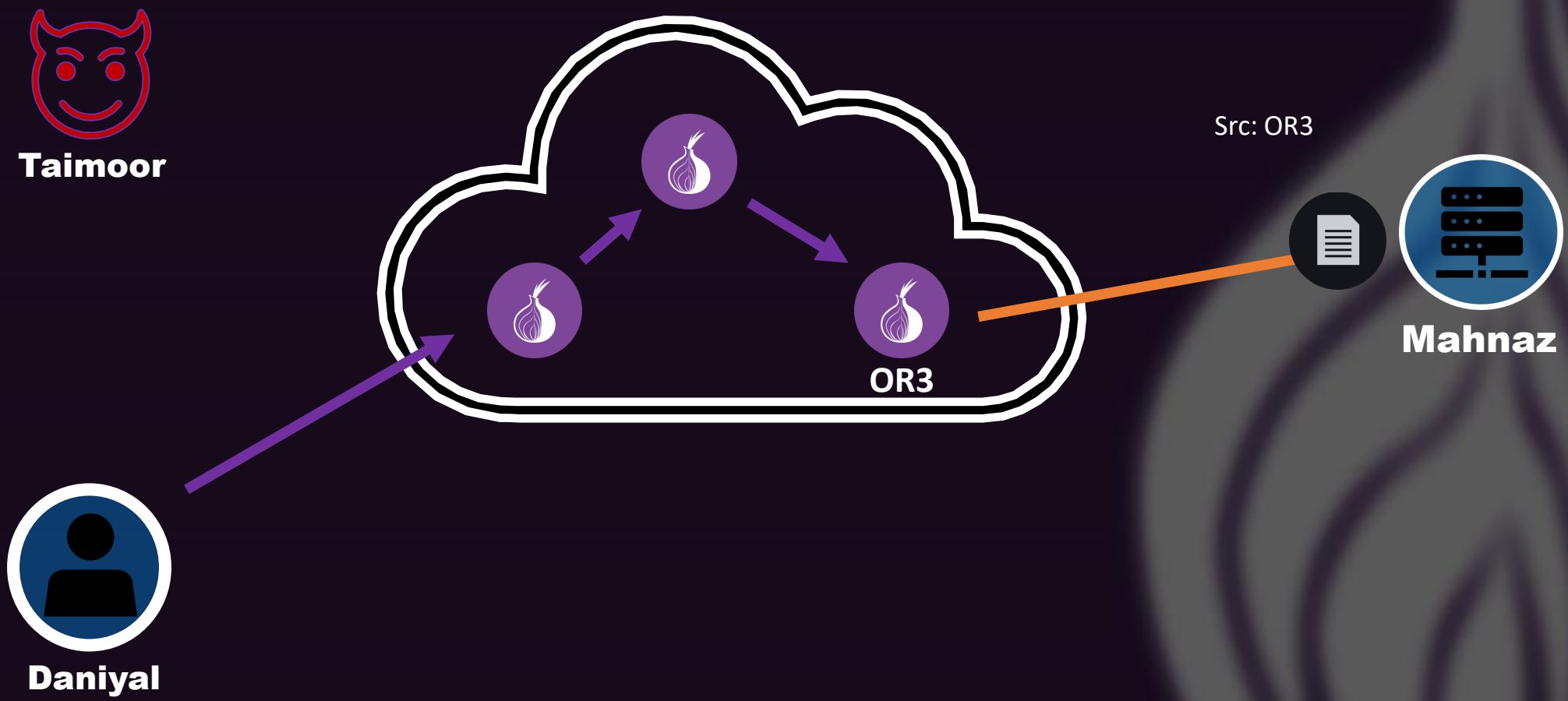
The number of web resources on the regular internet that a Tor user can access

Fate Sharing



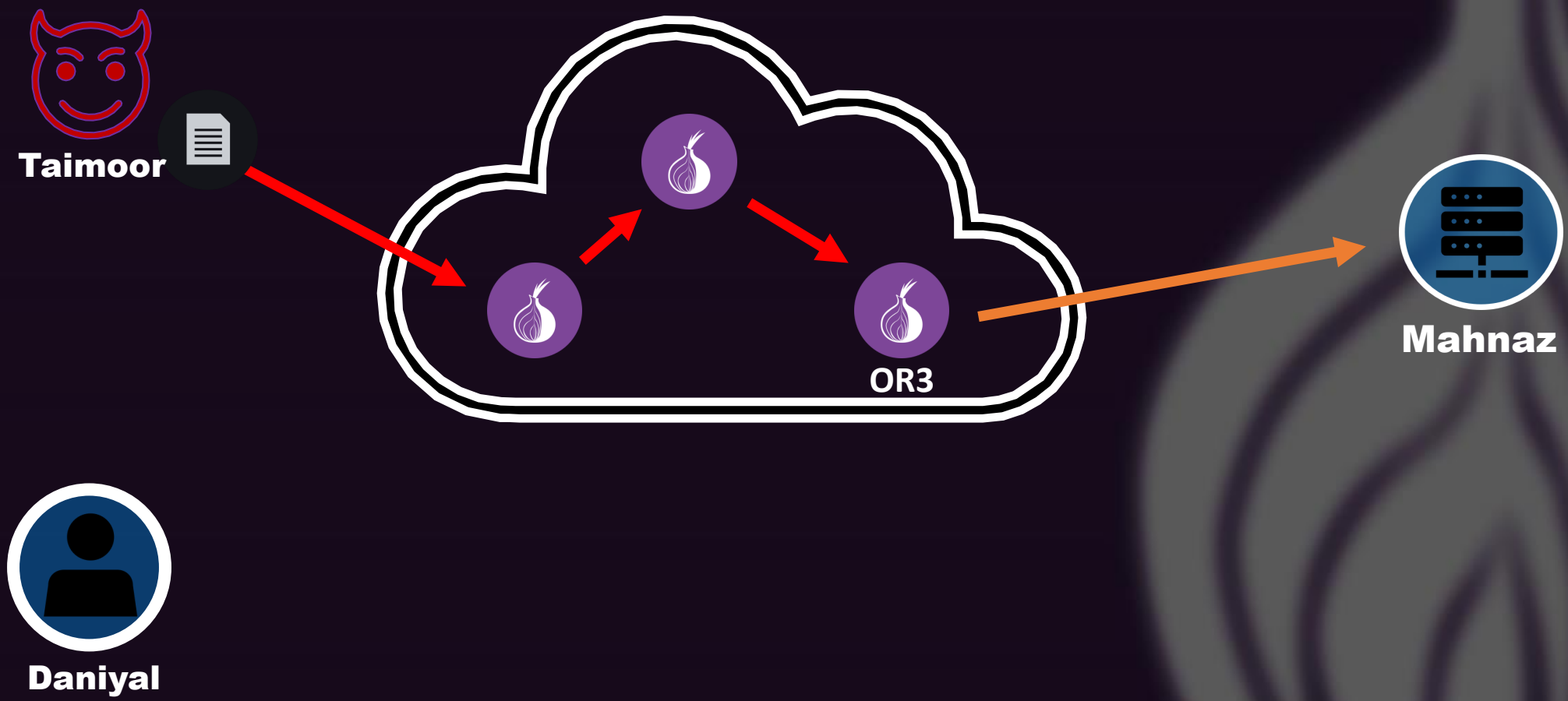
The number of web resources on the regular internet that a Tor user can access

Fate Sharing



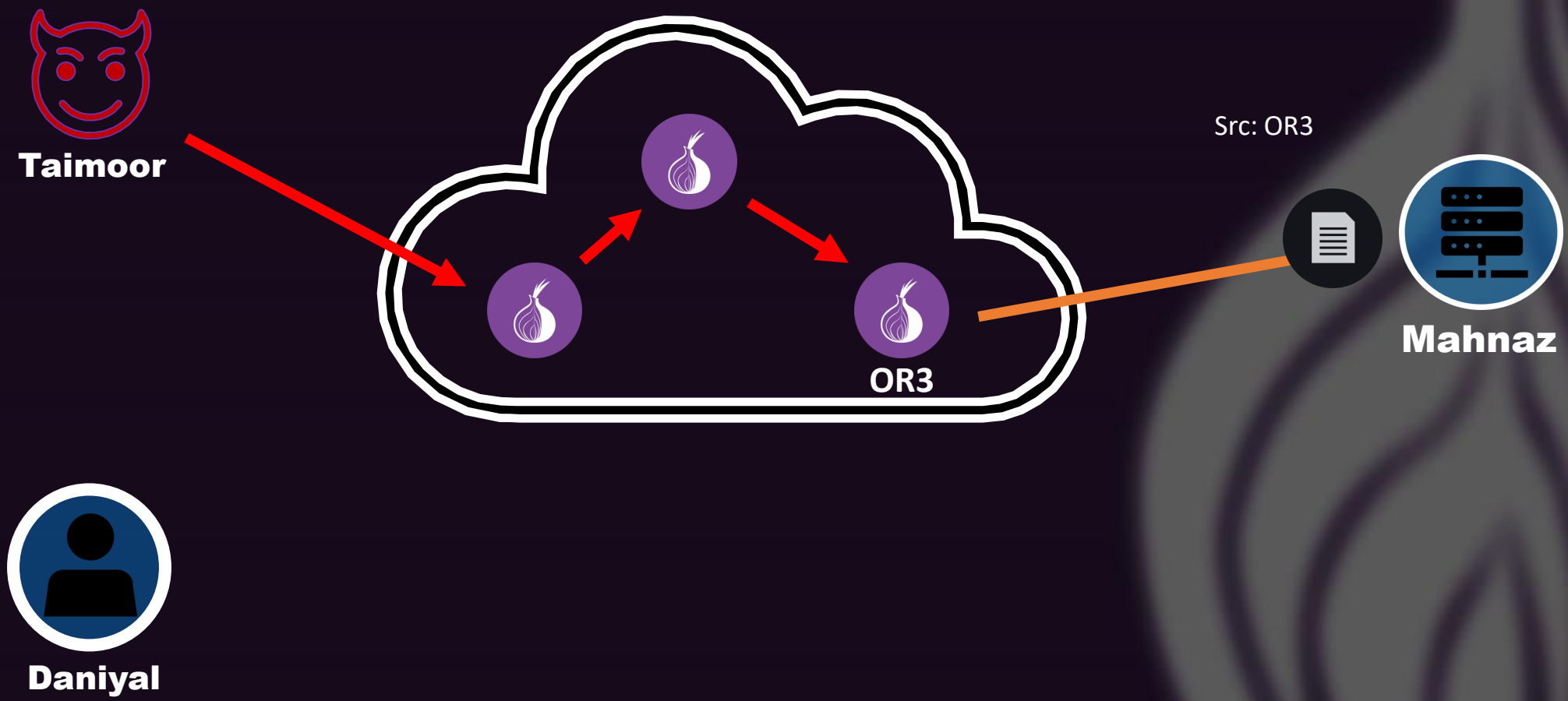
The number of web resources on the regular internet that a Tor user can access

Fate Sharing



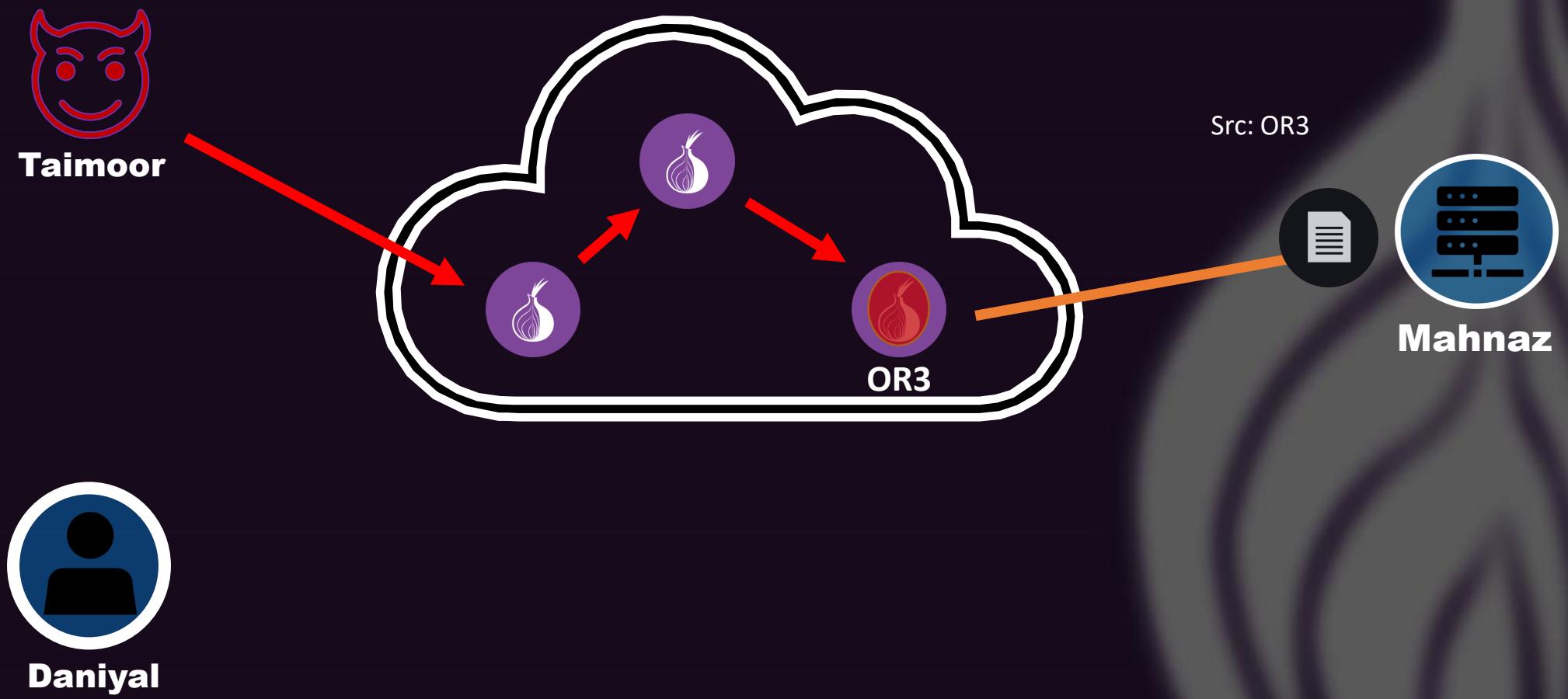
The number of web resources on the regular internet that a Tor user can access

Fate Sharing



The number of web resources on the regular internet that a Tor user can access

Fate Sharing



The number of web resources on the regular internet that a Tor user can access

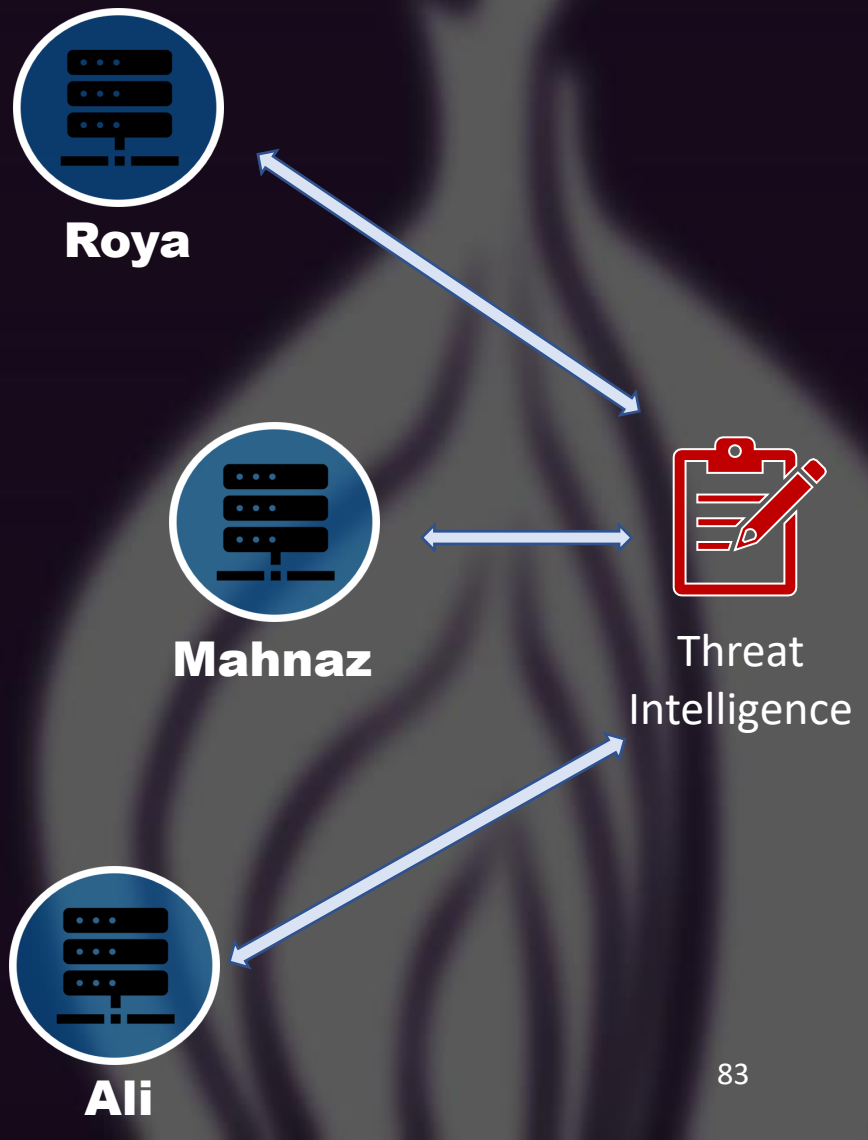
Fate Sharing

The number of web resources on the regular internet that a Tor user can access

Fate Sharing

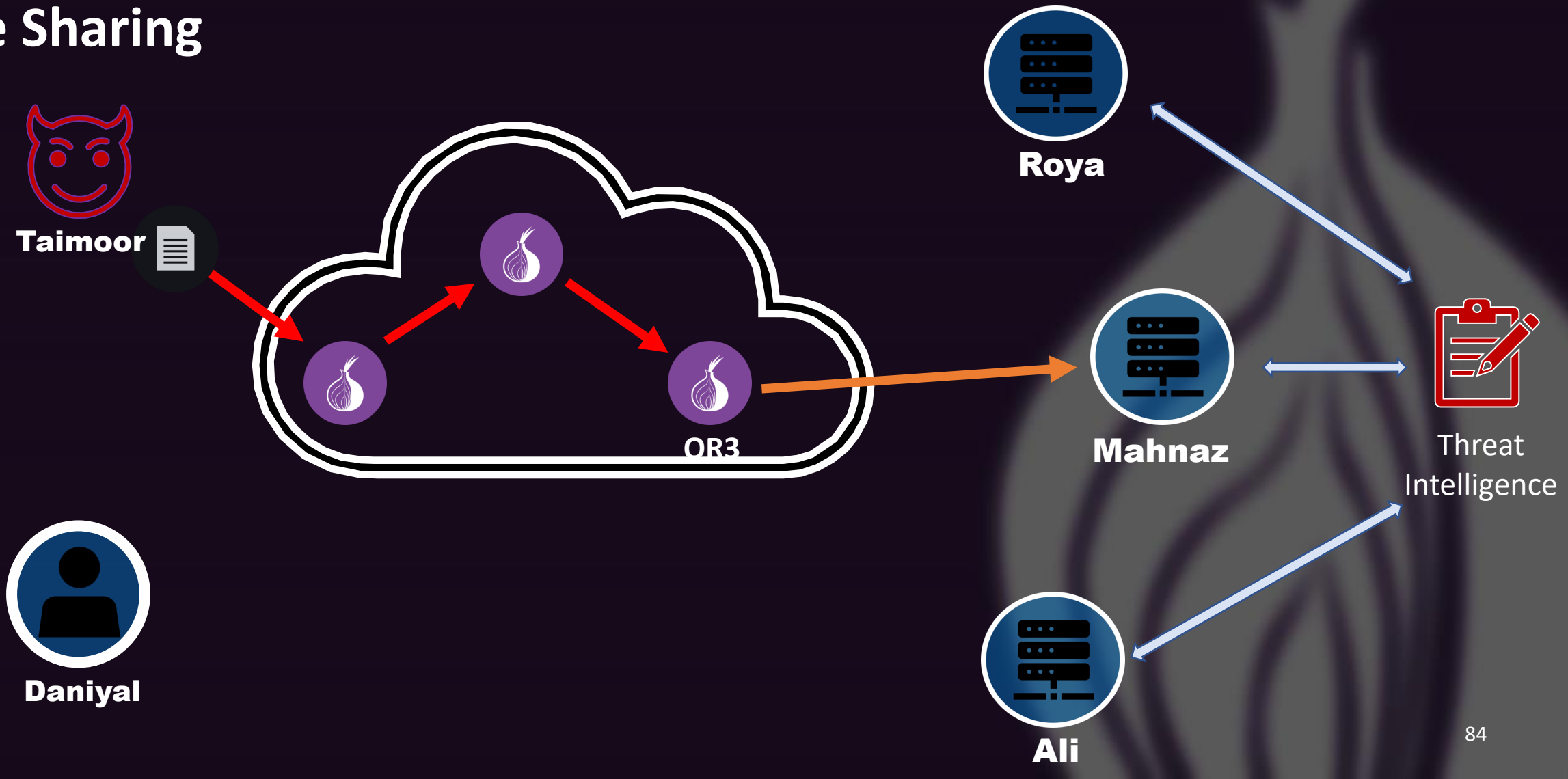
The number of web resources on the regular internet that a Tor user can access

Fate Sharing



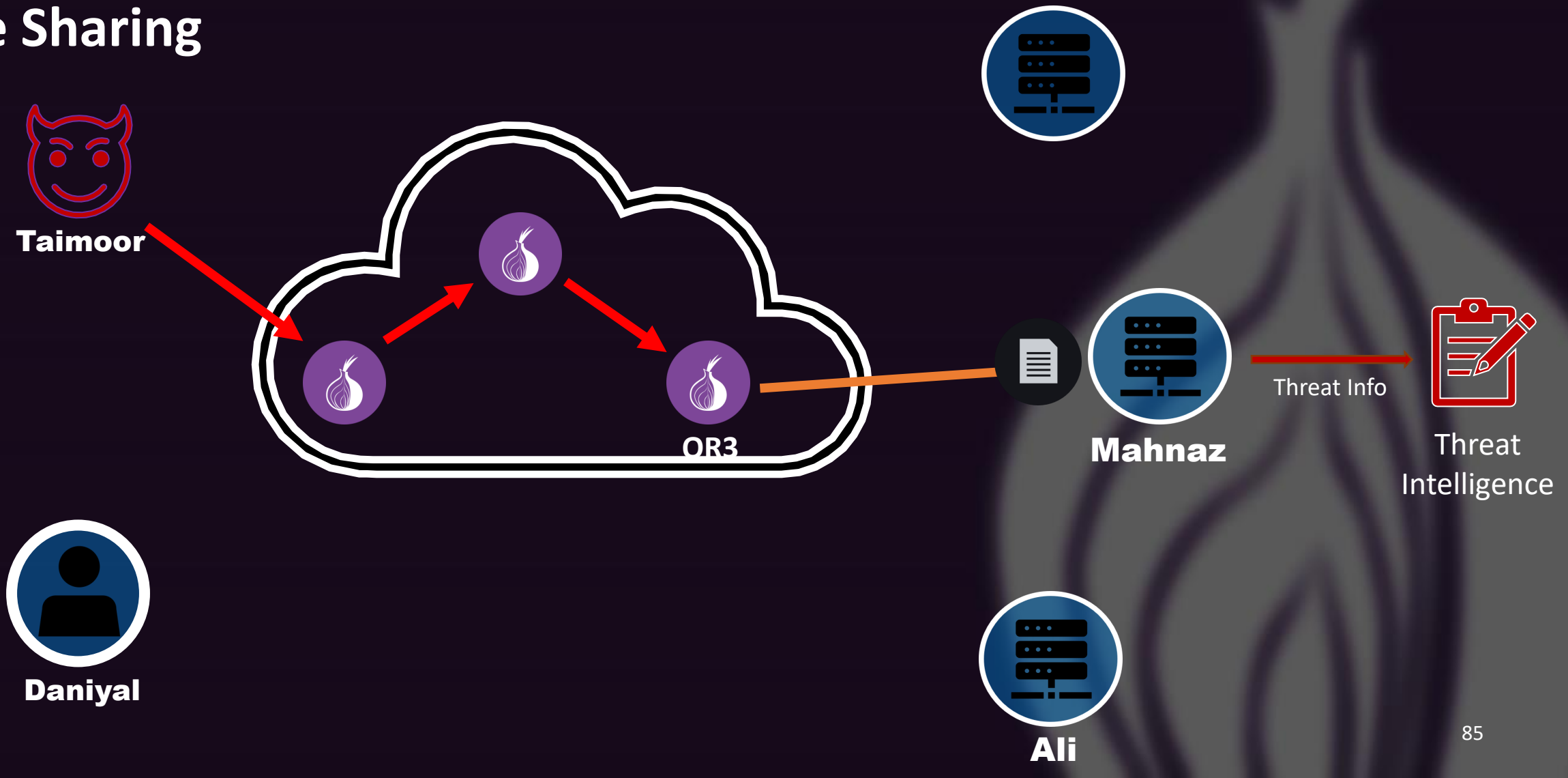
The number of web resources on the regular internet that a Tor user can access

Fate Sharing



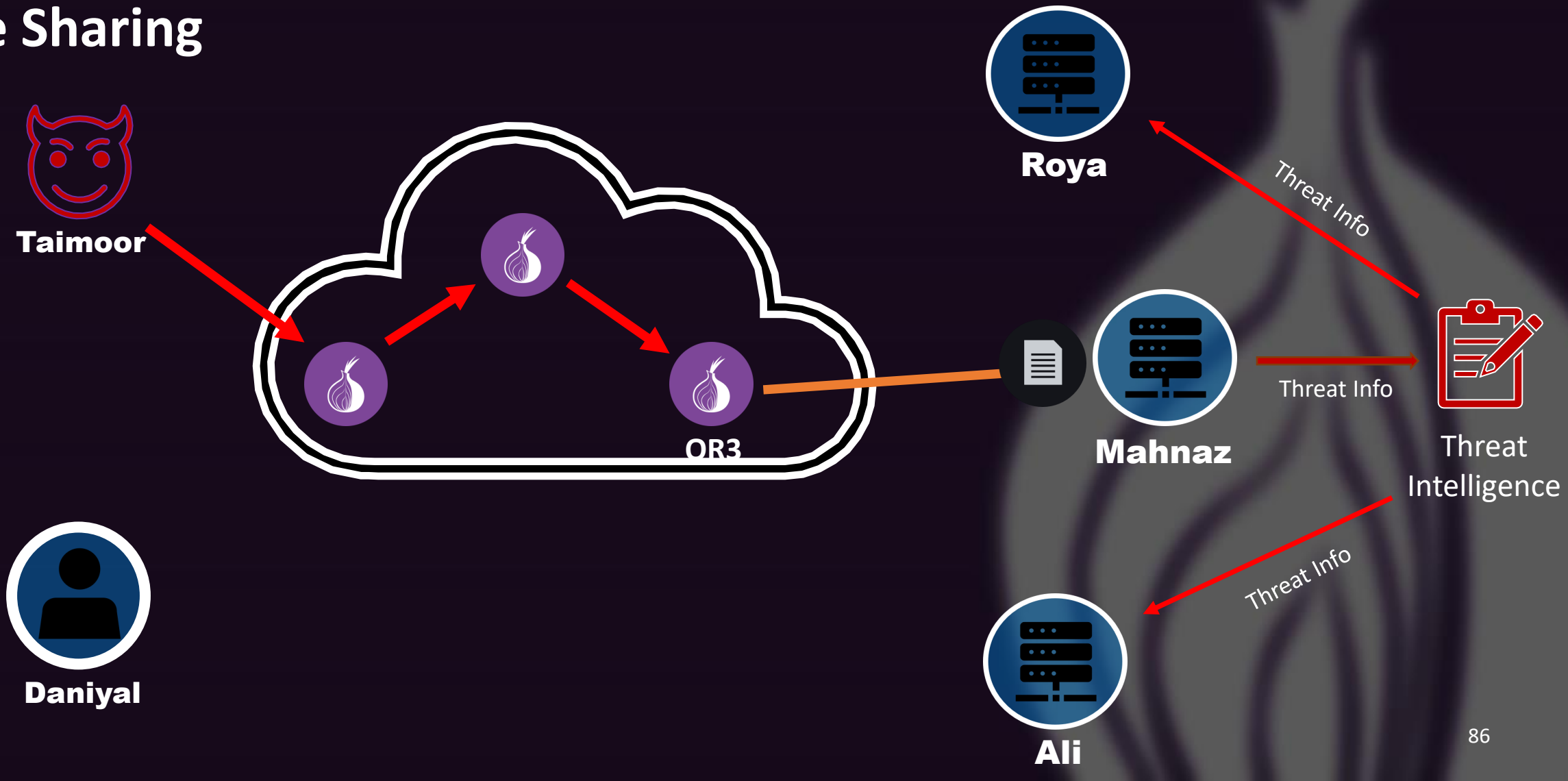
The number of web resources on the regular internet that a Tor user can access

Fate Sharing



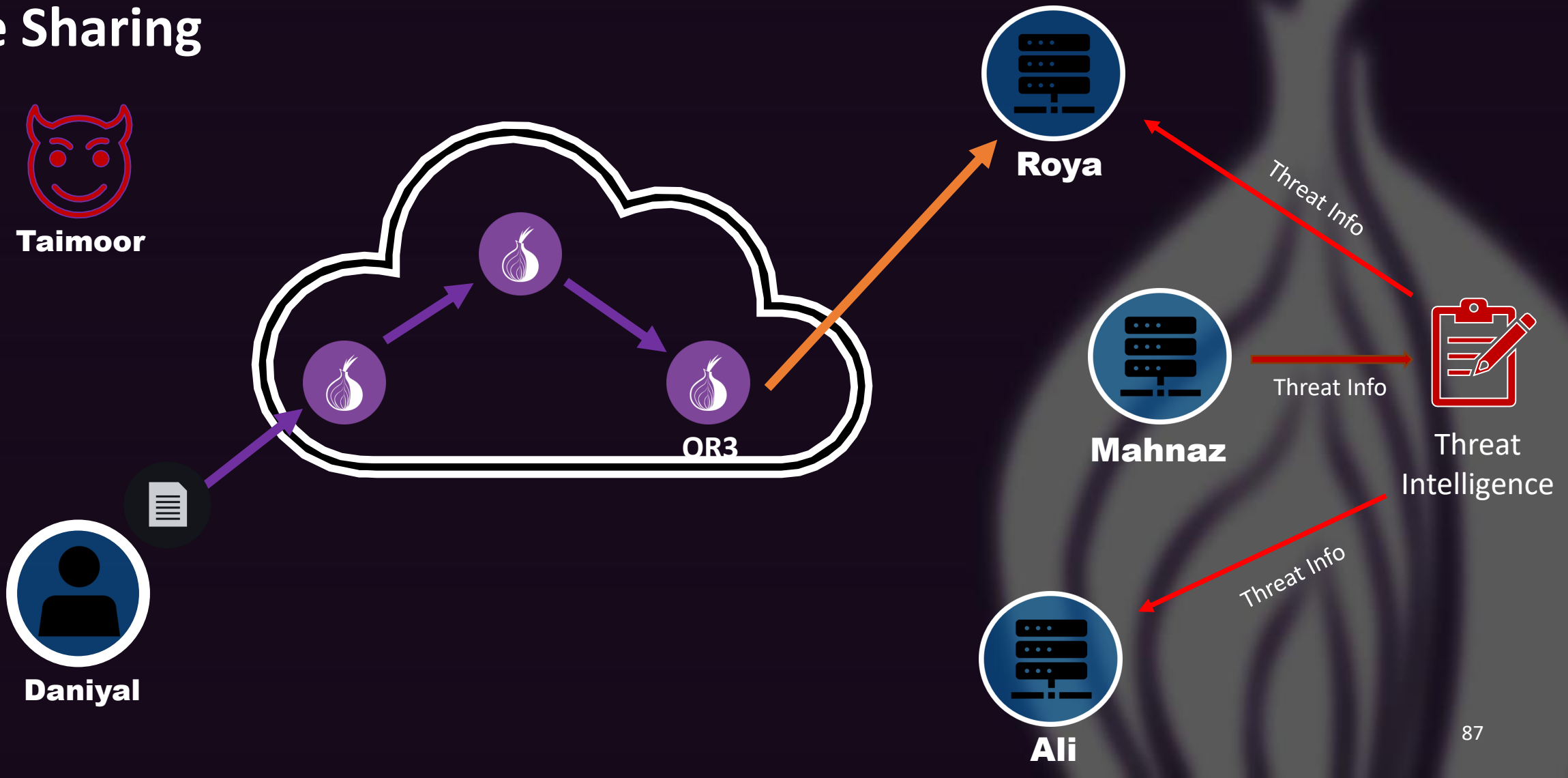
The number of web resources on the regular internet that a Tor user can access

Fate Sharing



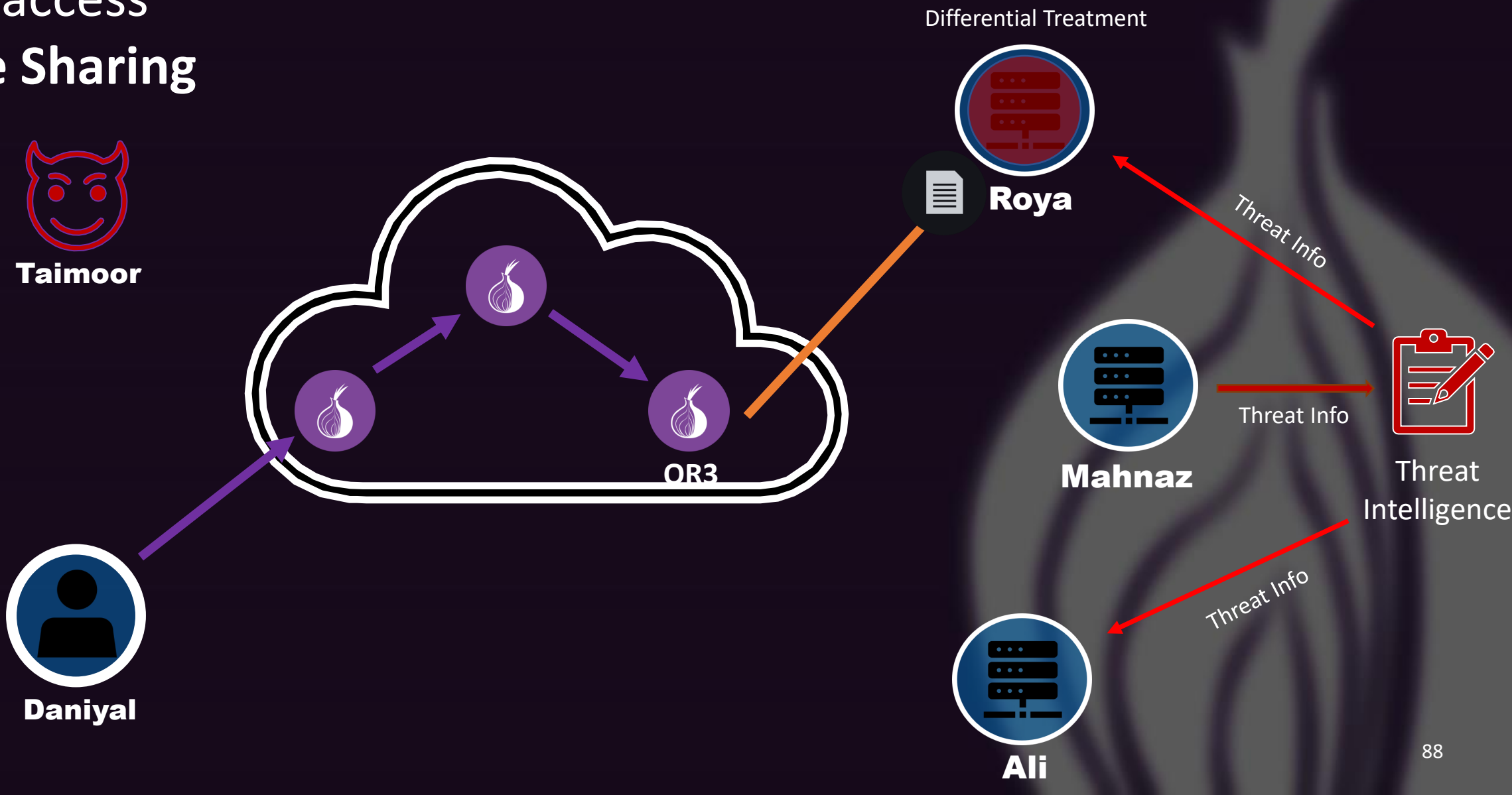
The number of web resources on the regular internet that a Tor user can access

Fate Sharing



The number of web resources on the regular internet that a Tor user can access

Fate Sharing



The number of web resources on the regular internet that a Tor user can access

Characterizing the Nature and Dynamics of Tor Exit Blocking

Rachee Singh[1], Rishab Nithyanand[2], Sadia Afroz[3,4]
Paul Pearce[3], Michael Carl Tschantz[4], Phillipa Gill[1], Vern Paxson[3,4]

The number of web resources on the regular internet that a Tor user can access

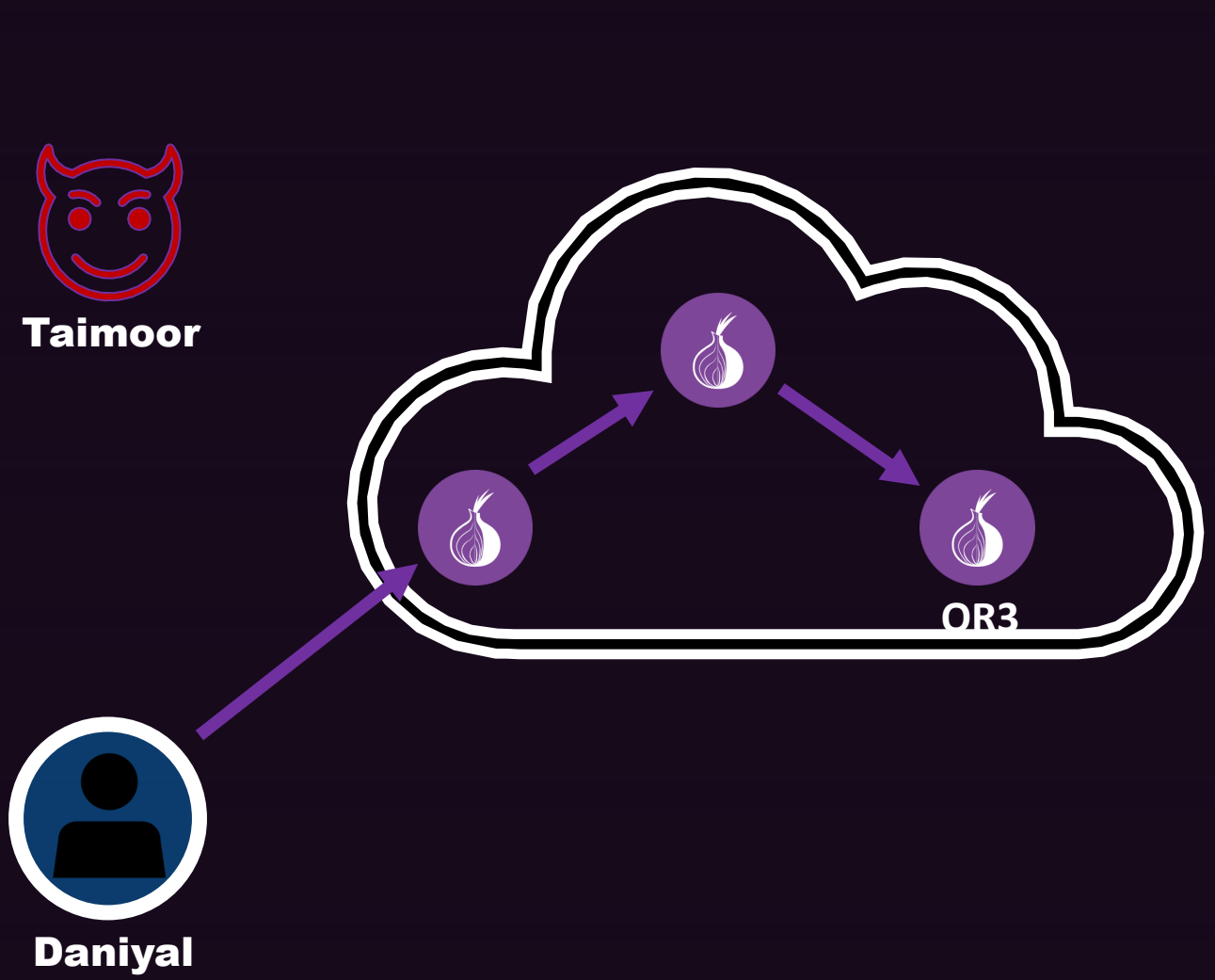
Characterizing the Nature and Dynamics of Tor Exit Blocking

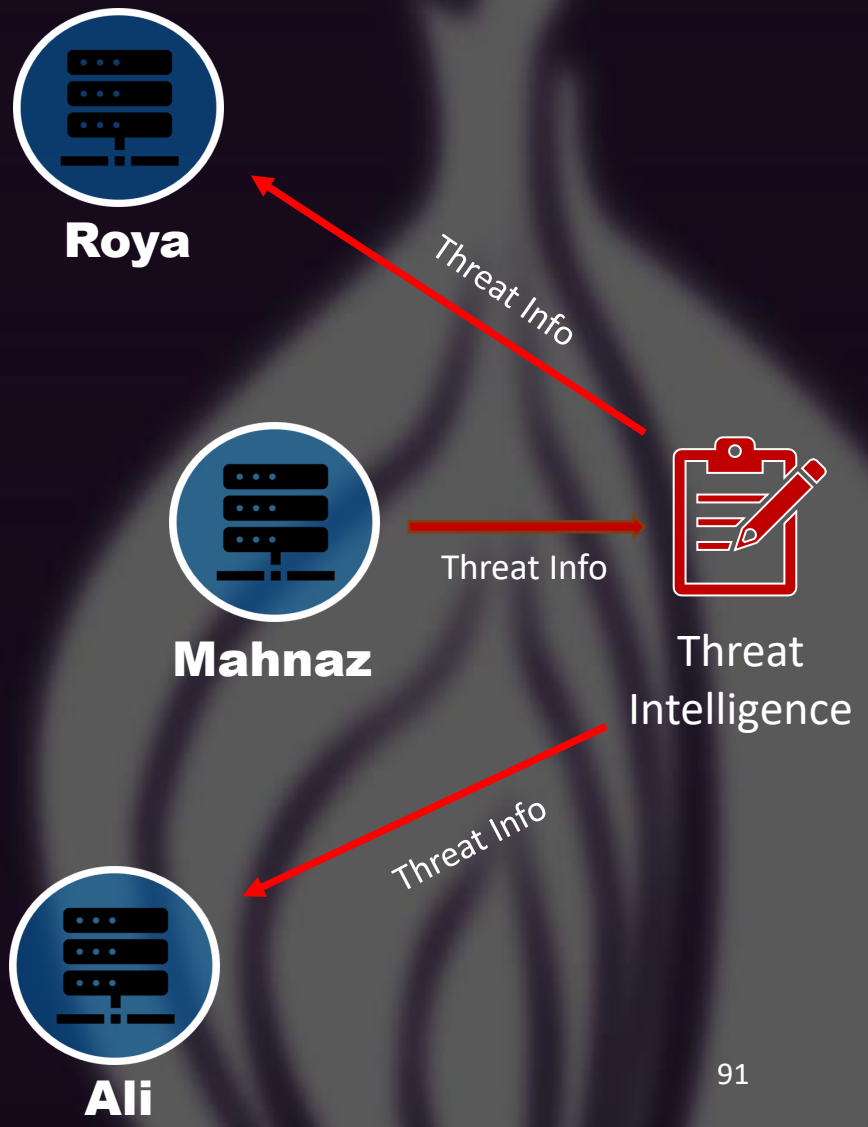
Rachee Singh[1], Rishab Nithyanand[2], Sadia Afroz[3,4]
Paul Pearce[3], Michael Carl Tschantz[4], Phillipa Gill[1], Vern Paxson[3,4]

Key goals

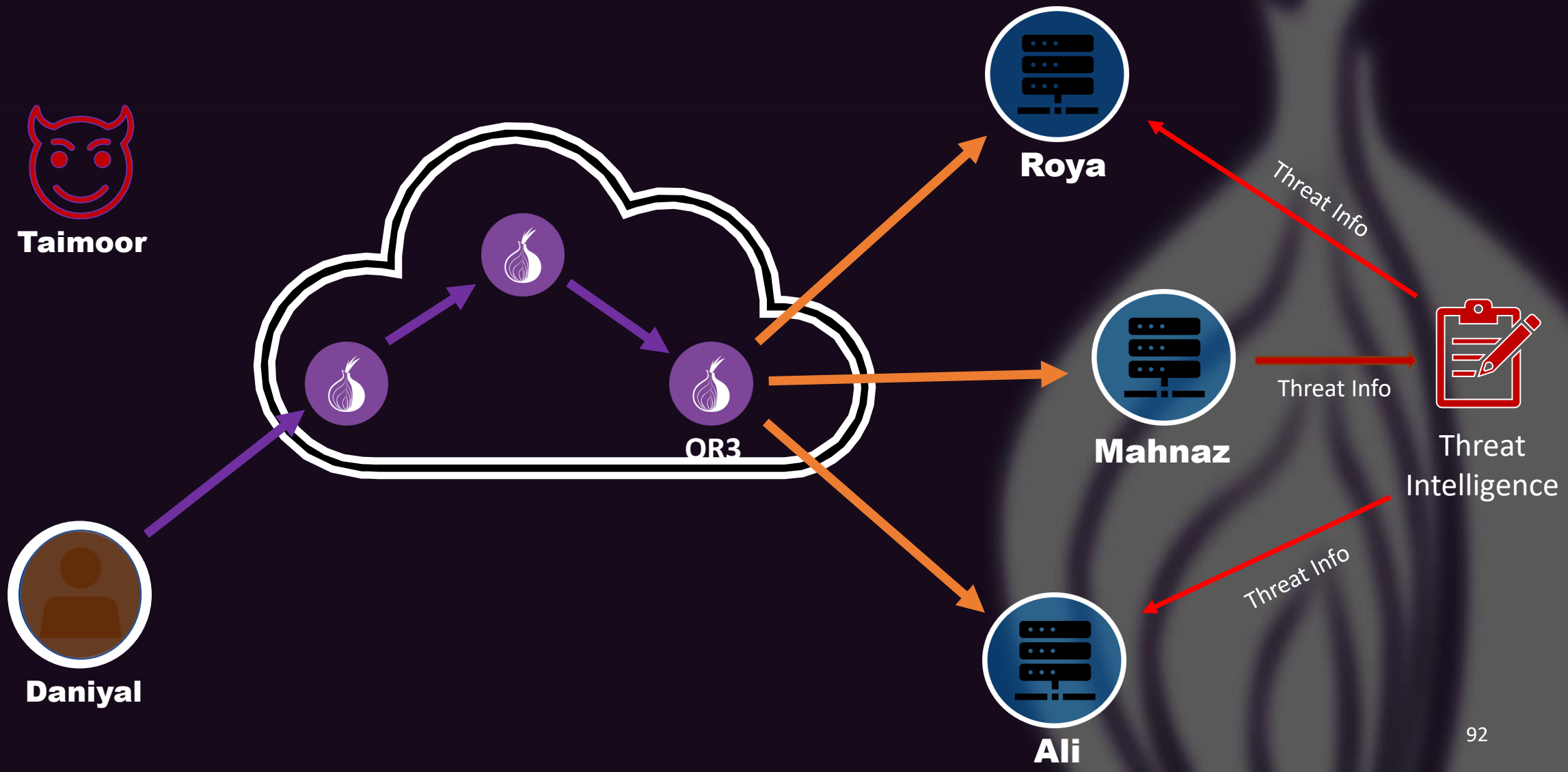
- Analyzing the extent of server-side discrimination faced by Tor users
- Analyzing the undesired traffic sent through Tor relays
- Analyzing whether the Tor network is blocked “reactively” or “proactively”

Analyzing the extent of server-side discrimination faced by Tor users





Analyzing the extent of server-side discrimination faced by Tor users



Analyzing the extent of server-side discrimination faced by Tor users

- Built a web crawler based on selenium
  - Visited the home page of a website
  - Instrumented search functionality
  - Instrumented login functionality

Analyzing the extent of server-side discrimination faced by Tor users

- Built a web crawler based on selenium
  - Visited the home page of a website
  - Instrumented search functionality
  - Instrumented login functionality

- Human like interactions with the website
  - Used a full-fledged browser (Firefox)
  - Bot-detection avoidance technique
    - Rate limited clicking
    - Automating cursor movements
    - Clicking visible elements on a page

Analyzing the extent of server-side discrimination faced by Tor users

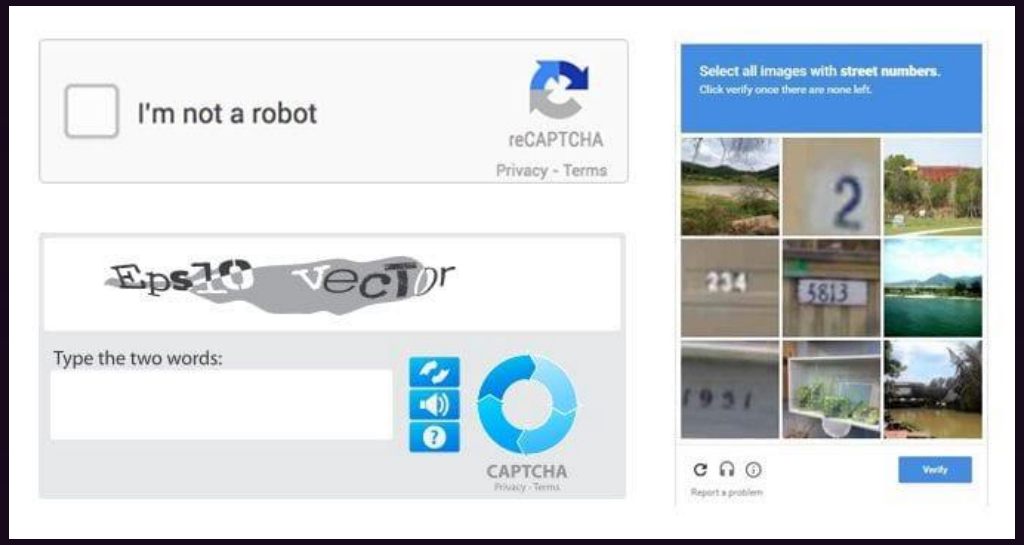
- Built a web crawler based on selenium
  - Visited the home page of a website
  - Instrumented search functionality
  - Instrumented login functionality

- Human like interactions with the website
  - Used a full-fledged browser (Firefox)
  - Bot-detection avoidance technique
    - Rate limited clicking
    - Automating cursor movements
    - Clicking visible elements on a page

- The crawler visited the Alexa top 500 websites
  - Collected HAR files
  - Recorded screenshots of all pages visited

Analyzing the extent of server-side discrimination faced by Tor users

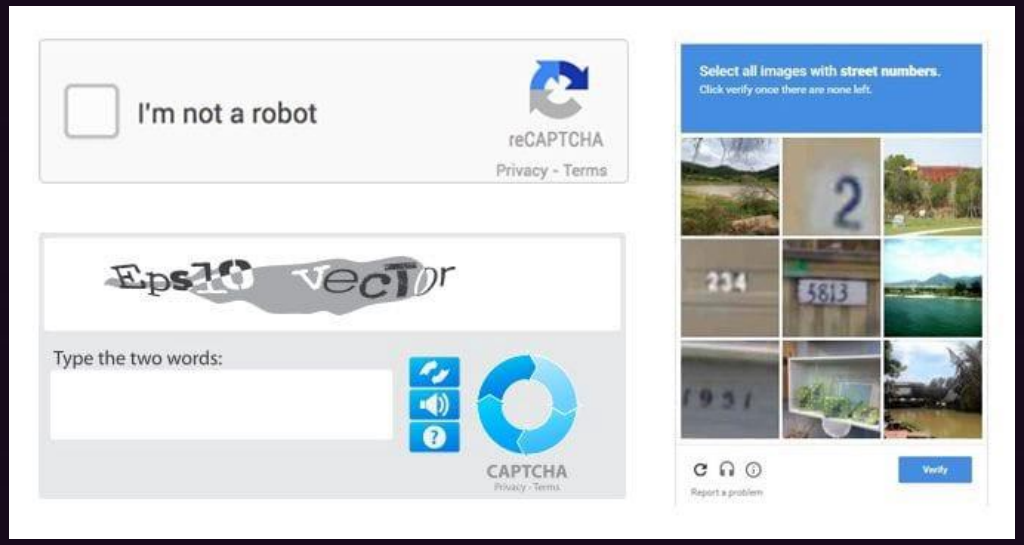
Types of discrimination



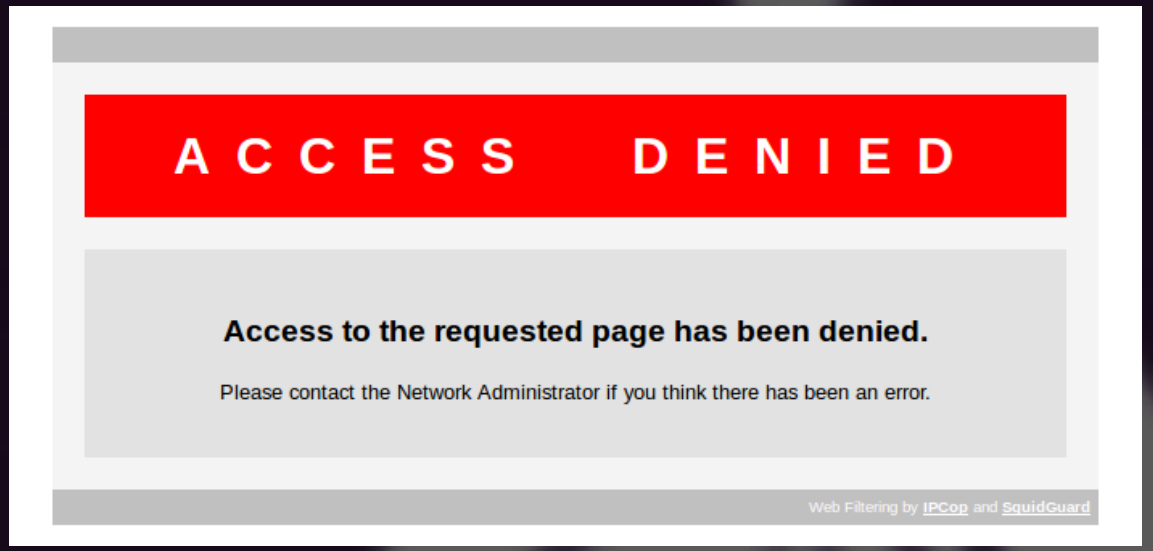
CAPTCHAs

Analyzing the extent of server-side discrimination faced by Tor users

Types of discrimination



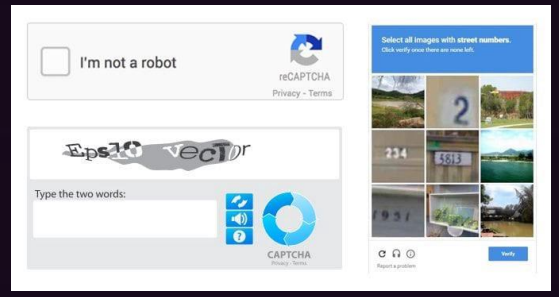
CAPTCHAs



Block pages

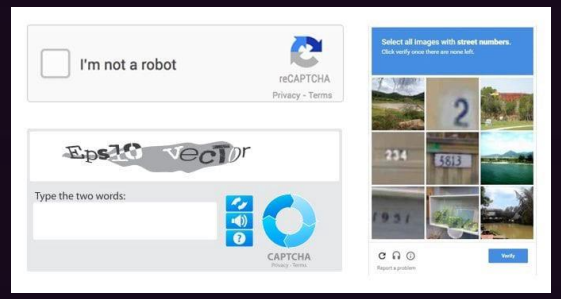
Analyzing the extent of server-side discrimination faced by Tor users

Detecting Discrimination



Analyzing the extent of server-side discrimination faced by Tor users

Detecting Discrimination



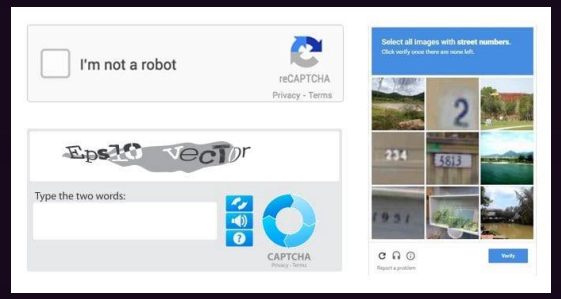
pHash

pHash

pHash

Analyzing the extent of server-side discrimination faced by Tor users

Detecting Discrimination



pHash

pHash distance > 0.75

pHash

pHash distance < 0.40

pHash

Analyzing the extent of server-side discrimination faced by Tor users

Detecting Discrimination

pHash

pHash distance > 0.75

pHash

pHash distance < 0.40

pHash

Analyzing the extent of server-side discrimination faced by Tor users

Extent of Discrimination

Alexa Top 500

Analyzing the extent of server-side discrimination faced by Tor users

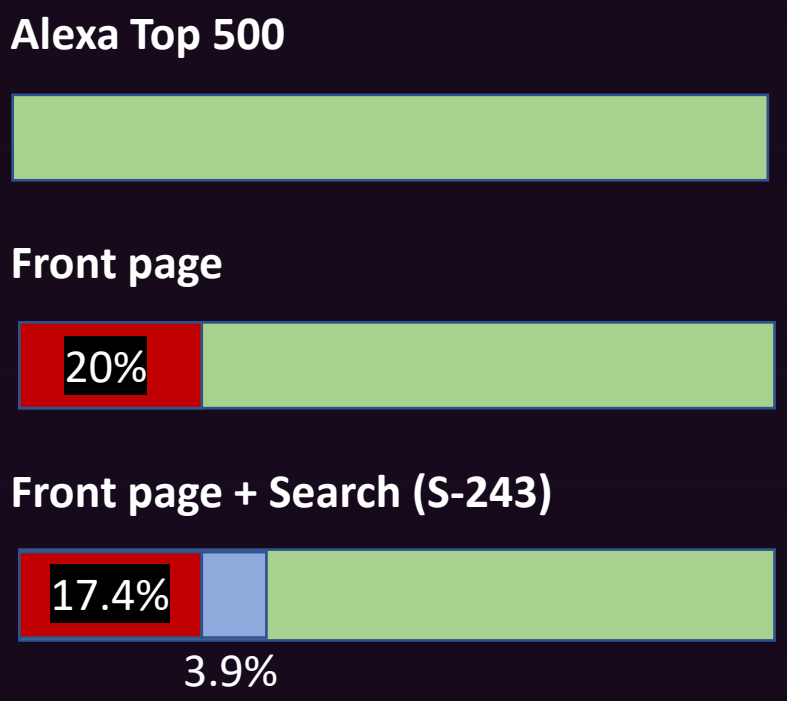
Extent of Discrimination

Alexa Top 500

Front page

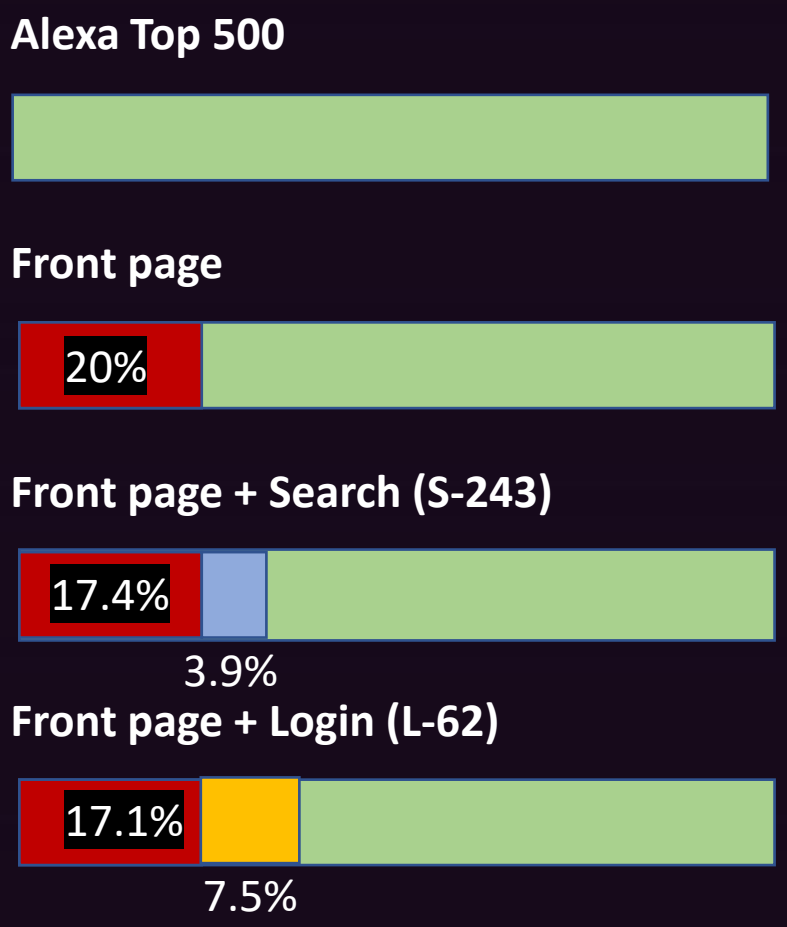
Analyzing the extent of server-side discrimination faced by Tor users

Extent of Discrimination



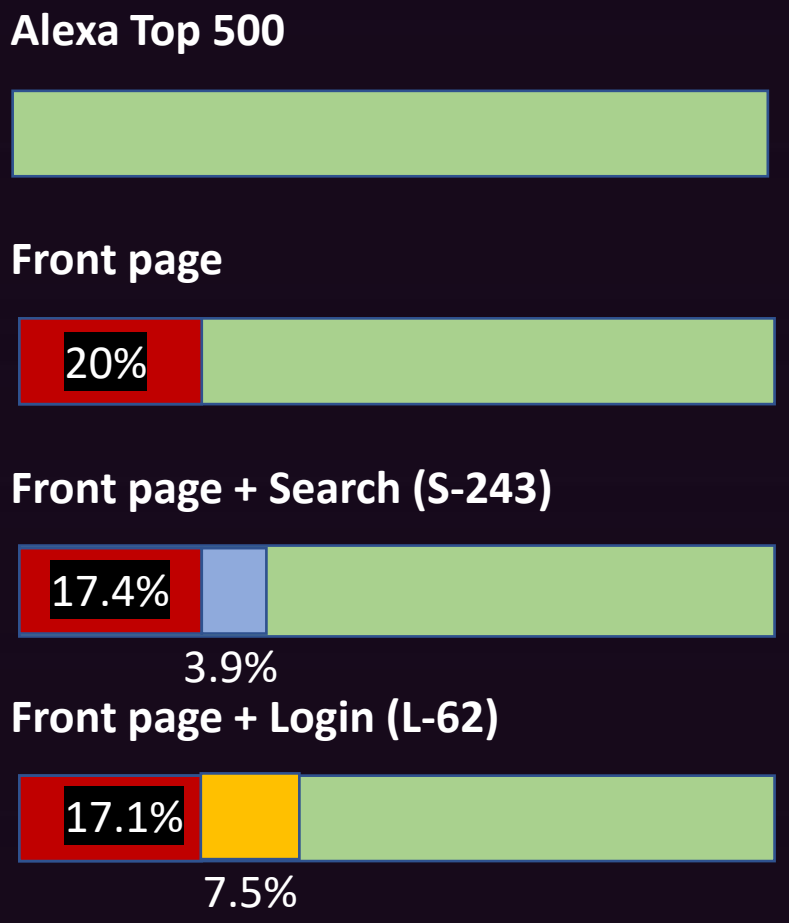
Analyzing the extent of server-side discrimination faced by Tor users

Extent of Discrimination



Analyzing the extent of server-side discrimination faced by Tor users

Extent of Discrimination



31% Of all Tor users face some form of differential treatment on the regular internet

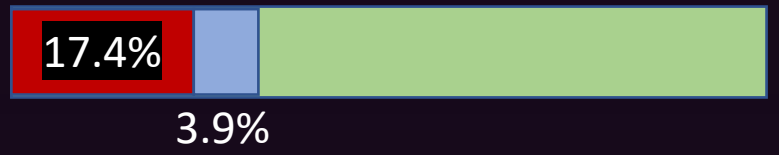
Analyzing the extent of server-side discrimination faced by Tor users

Extent of Discrimination

Alexa Top 500

Front page

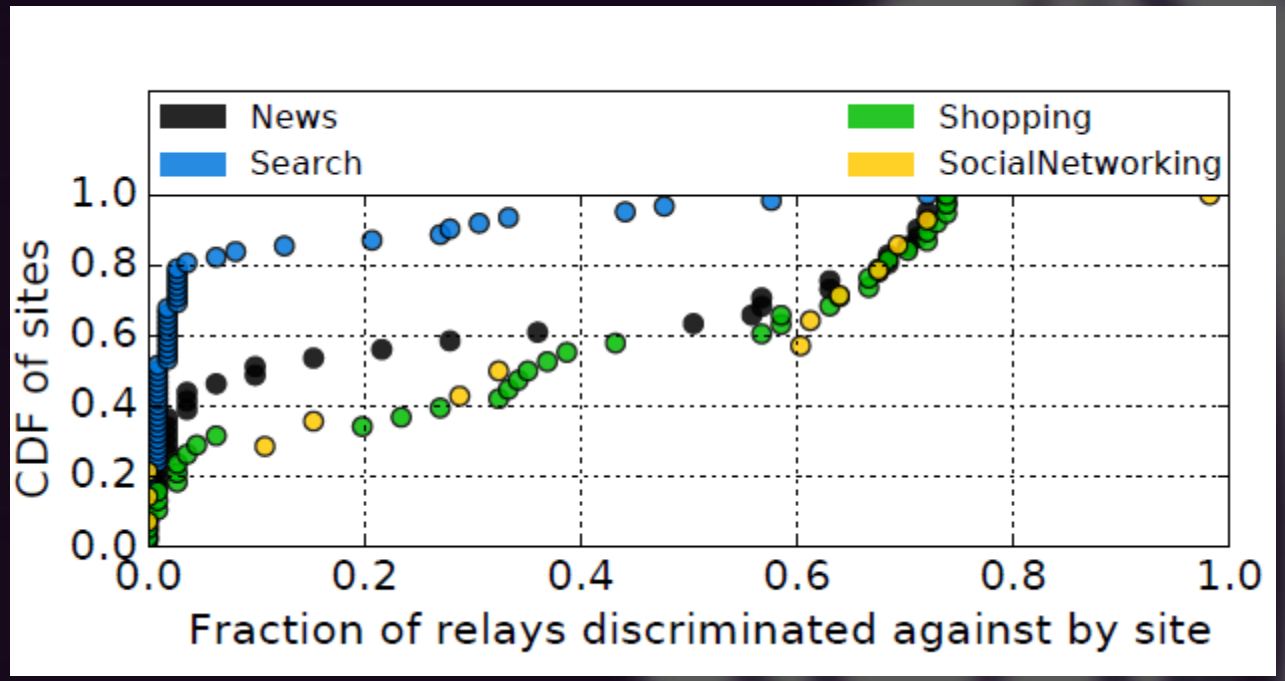
Front page + Search (S-243)



Front page + Login (L-62)

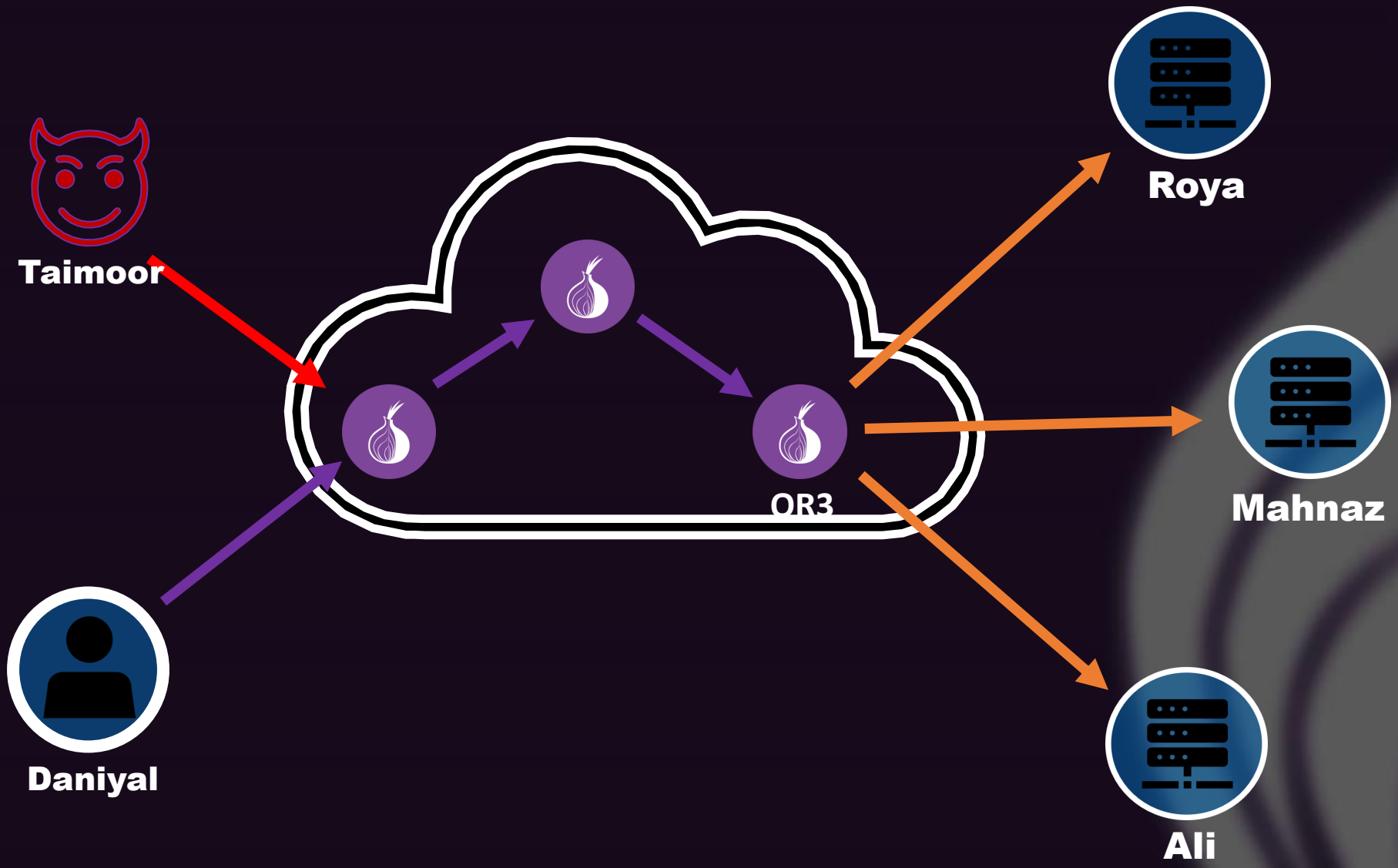
31%

Of all Tor users face some form of differential treatment on the regular internet



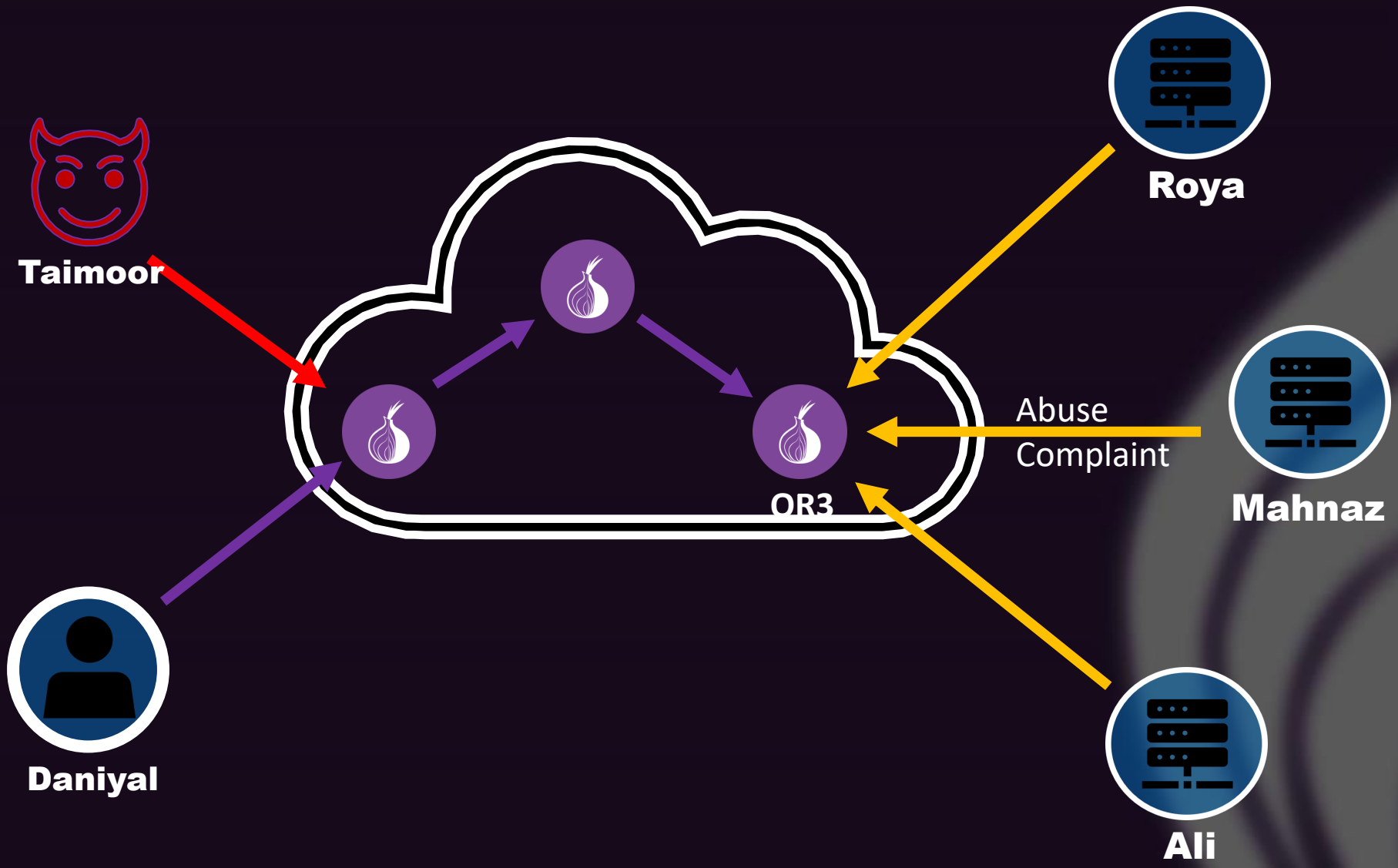
Analyzing the undesired traffic sent through Tor relays

Collection

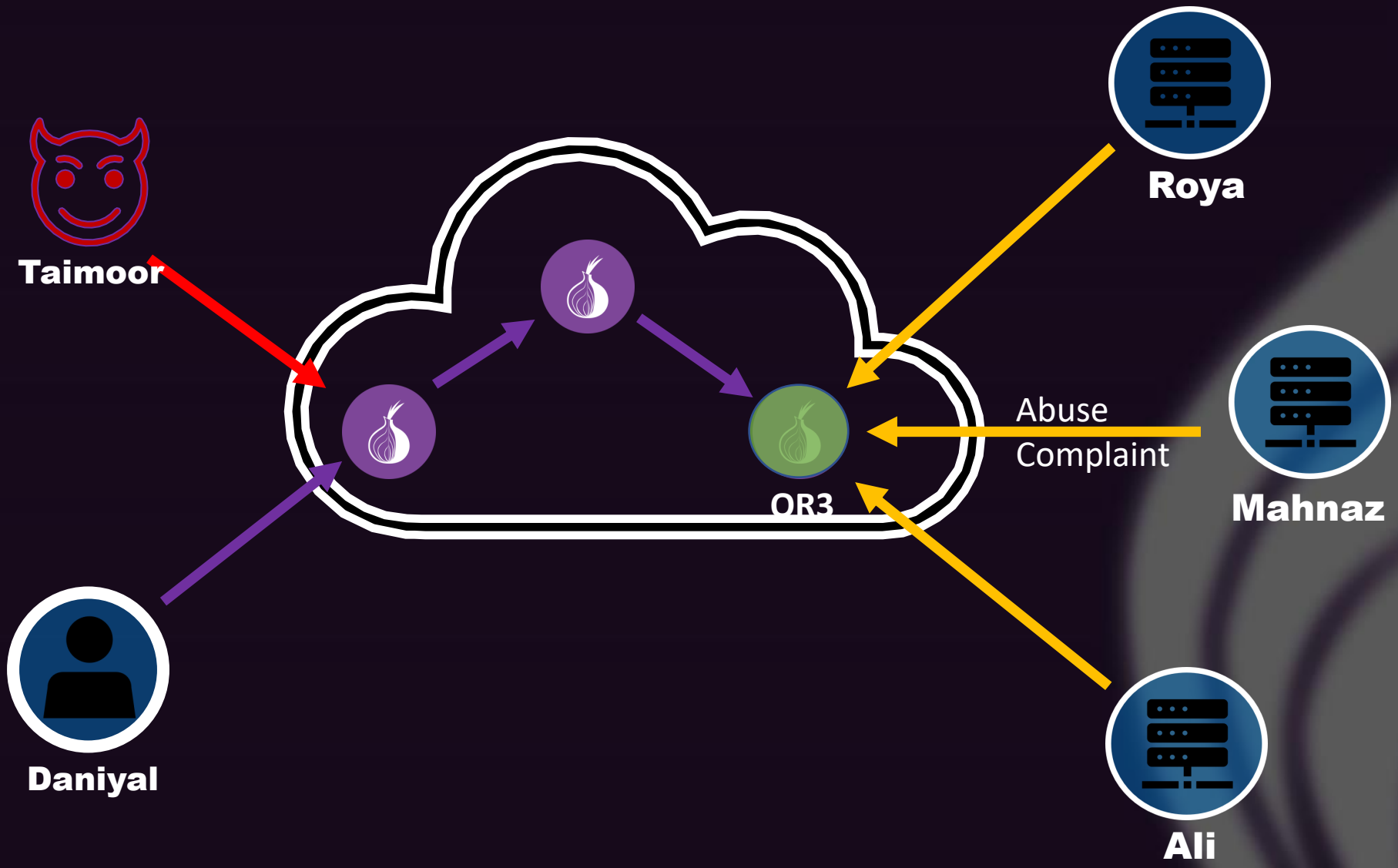


Analyzing the undesired traffic sent through Tor relays

Collection



Analyzing the undesired traffic sent through Tor relays
Collection



Analyzing the undesired traffic sent through Tor relays
Collection

- Abuse E-mails from 25 Tor relays
  - 10 relays run by themselves
  - 15 relays run by other individuals

Analyzing the undesired traffic sent through Tor relays
Collection

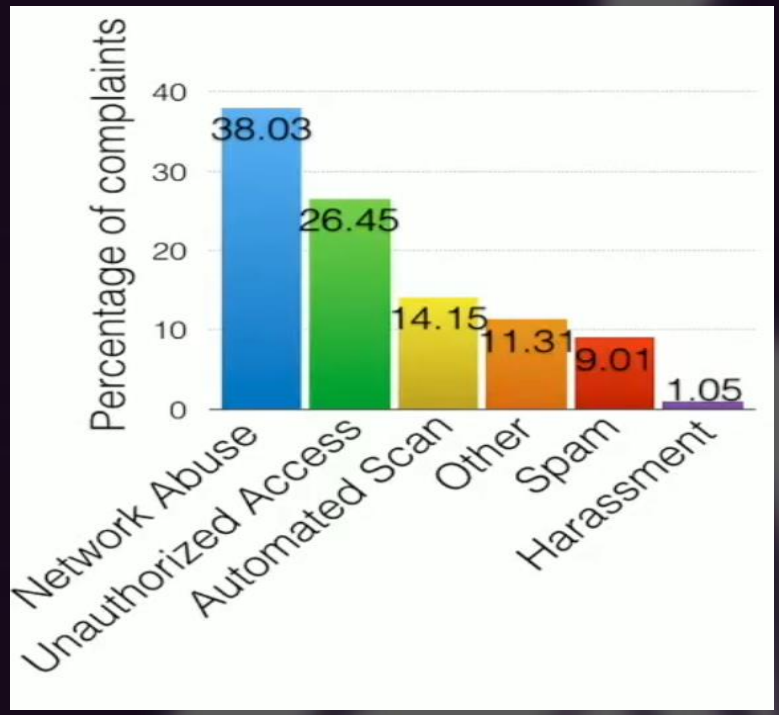
- Abuse E-mails from 25 Tor relays
  - 10 relays run by themselves
  - 15 relays run by other individuals

- 3 million emails
  - Collected over a period of ~6 years
  - Clustering to find similar complaints

Analyzing the undesired traffic sent through Tor relays
Results

- Abuse E-mails from 25 Tor relays
  - 10 relays run by themselves
  - 15 relays run by other individuals

- 3 million emails
  - Collected over a period of ~6 years
  - K-means clustering to find similar complaints



Exit Family	# Exits	% Tor Traffic	Email Dates	# Complaints	Top Complaint
Torservers.net	10–20	7.05%	2010/06–2016/04	2,987,017	DMCA Violation (99.74%)
apx	3	1.94%	2014/11–2016/05	293	Automated Scan (38.49%)
TorLand1	1	0.75%	2011/12–2016/10	307	Malicious Traffic (16.99%)
jahjah	1	0.17%	2016/1–2017/1	75	Unauthorized Login Attempts (34.15%)
Our exits	10	3.14%	2016/9–2017/2	650	Network Attack (48.68%)

Analyzing whether the Tor network is blocked “reactively” or “proactively”

- Threat Intelligence data from Facebook threat exchange
  - Contains 100+ commercially used blacklists
  - Analyze the rate of Tor IP addresses blacklisted

Analyzing whether the Tor network is blocked “reactively” or “proactively”

- Threat Intelligence data from Facebook threat exchange
  - Contains 100+ commercially used blacklists
  - Analyze the rate of Tor IP addresses blacklisted

    - **Proactive Blocking**
      - “Matter of policy”

      - If more than 30% of all Tor relays are blacklisted within 24 hours

Analyzing whether the Tor network is blocked “reactively” or “proactively”

- Threat Intelligence data from Facebook threat exchange
  - Contains 100+ commercially used blacklists
  - Analyze the rate of Tor IP addresses blacklisted

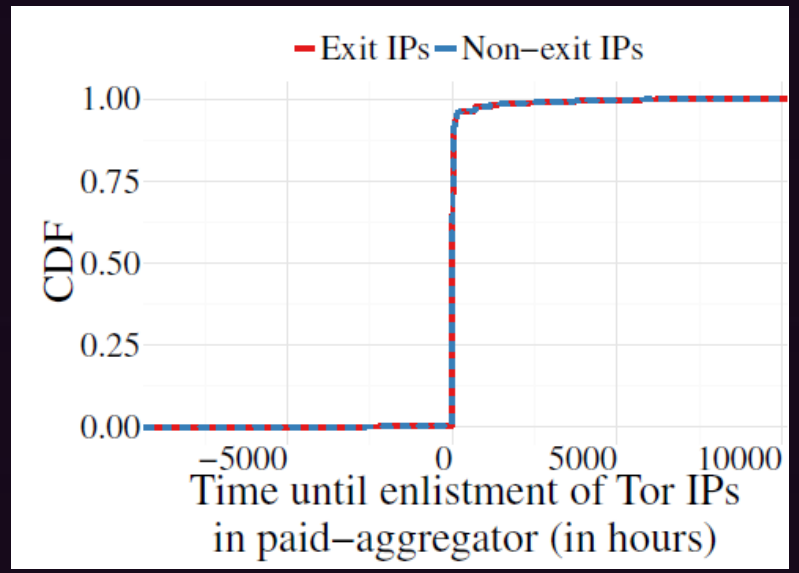
- **Proactive Blocking**
  - “Matter of policy”
  - If more than 30% of all Tor relays are blacklisted within 24 hours

- **Reactive Blocking**
  - “Response to abuse”
  - If less than 30% of all Tor relays were listed within 24 hours

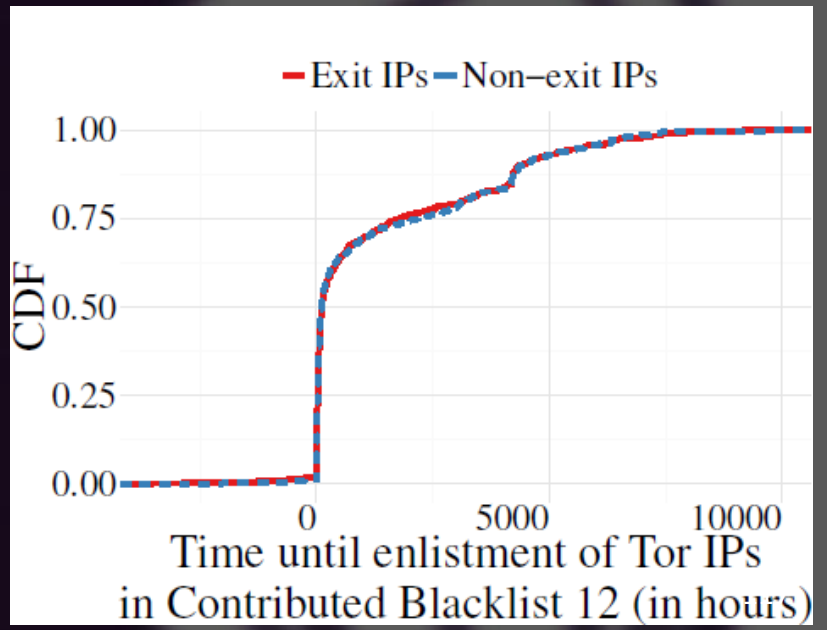
Analyzing whether the Tor network is blocked “reactively” or “proactively”

- Threat Intelligence data from Facebook threat exchange
  - Contains 100+ commercially used blacklists
  - Analyze the rate of Tor IP addresses blacklisted

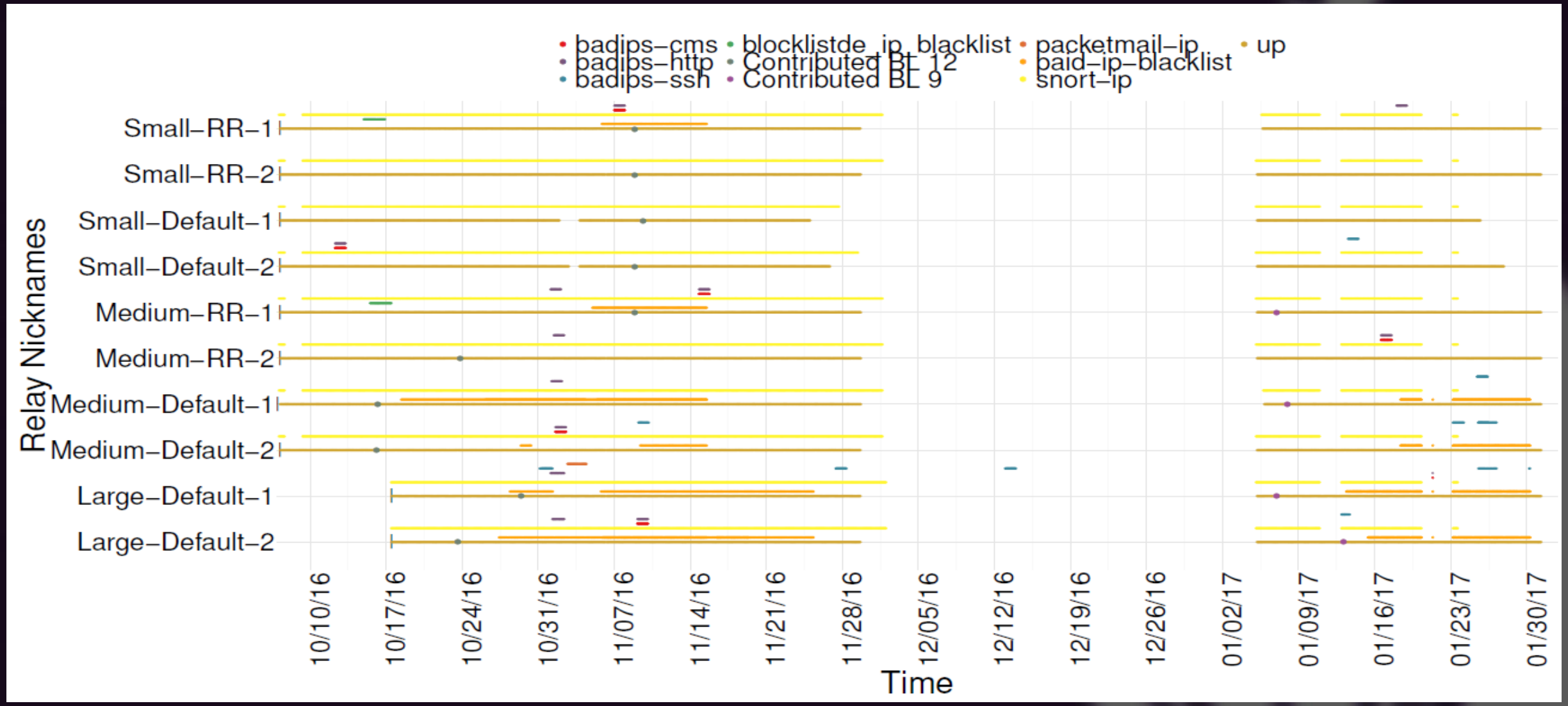
- **Proactive Blocking**
  - “Matter of policy”



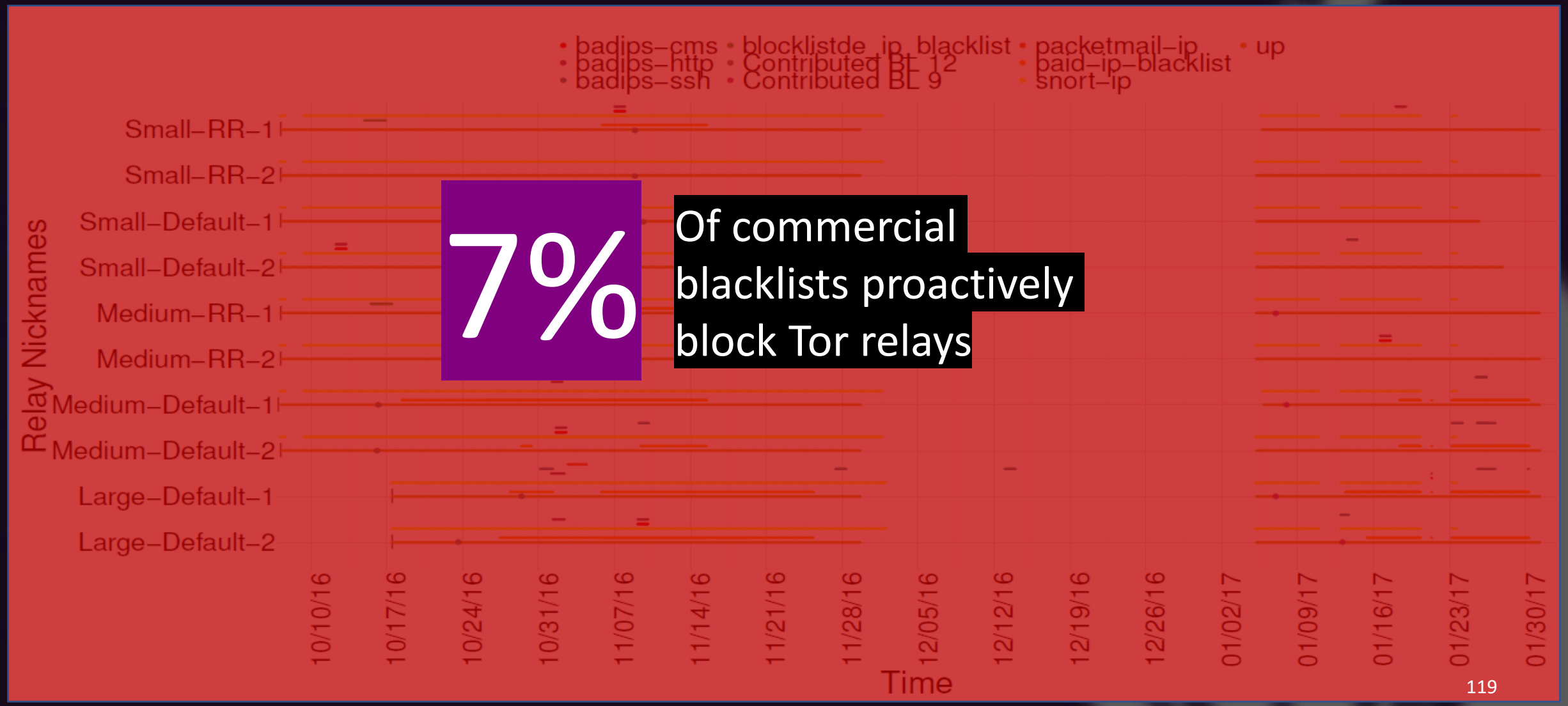
- **Reactive Blocking**
  - “Response to abuse”



Analyzing whether the Tor network is blocked “reactively” or “proactively”



Analyzing whether the Tor network is blocked “reactively” or “proactively”



7%

Of commercial blacklists proactively block Tor relays

Putting it all together

- Individuals wanting to use the Tor network can not access it due to usability and censorship issues

- Users able to access the Tor network face issues of latency due to the very nature of the network itself

- Tor users are discriminated against by end servers

- These problems lead to the degradation of the utility of the Tor network

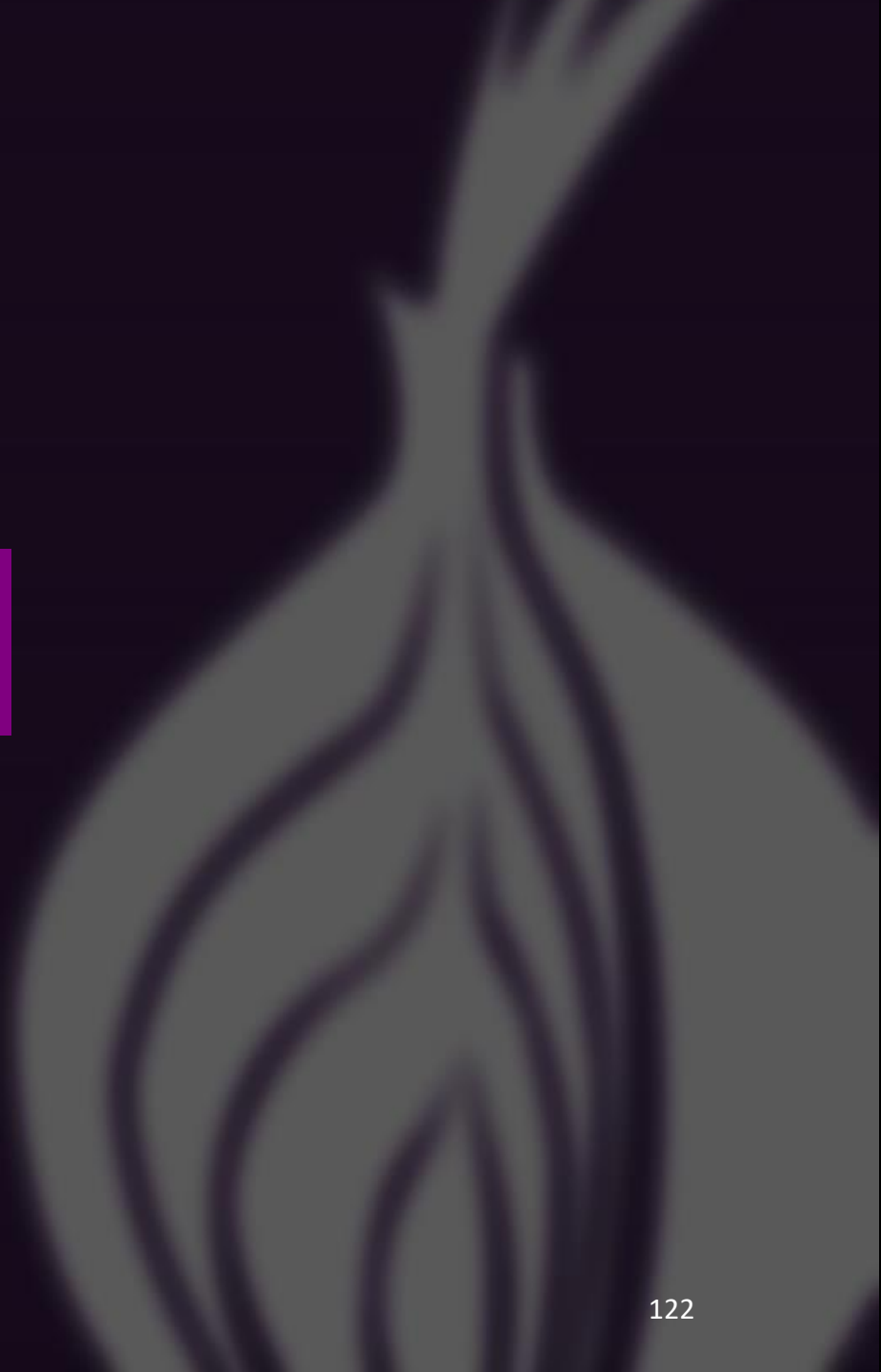
Future work

- Working on identifying users who send in malicious traffic without deanonymizing them

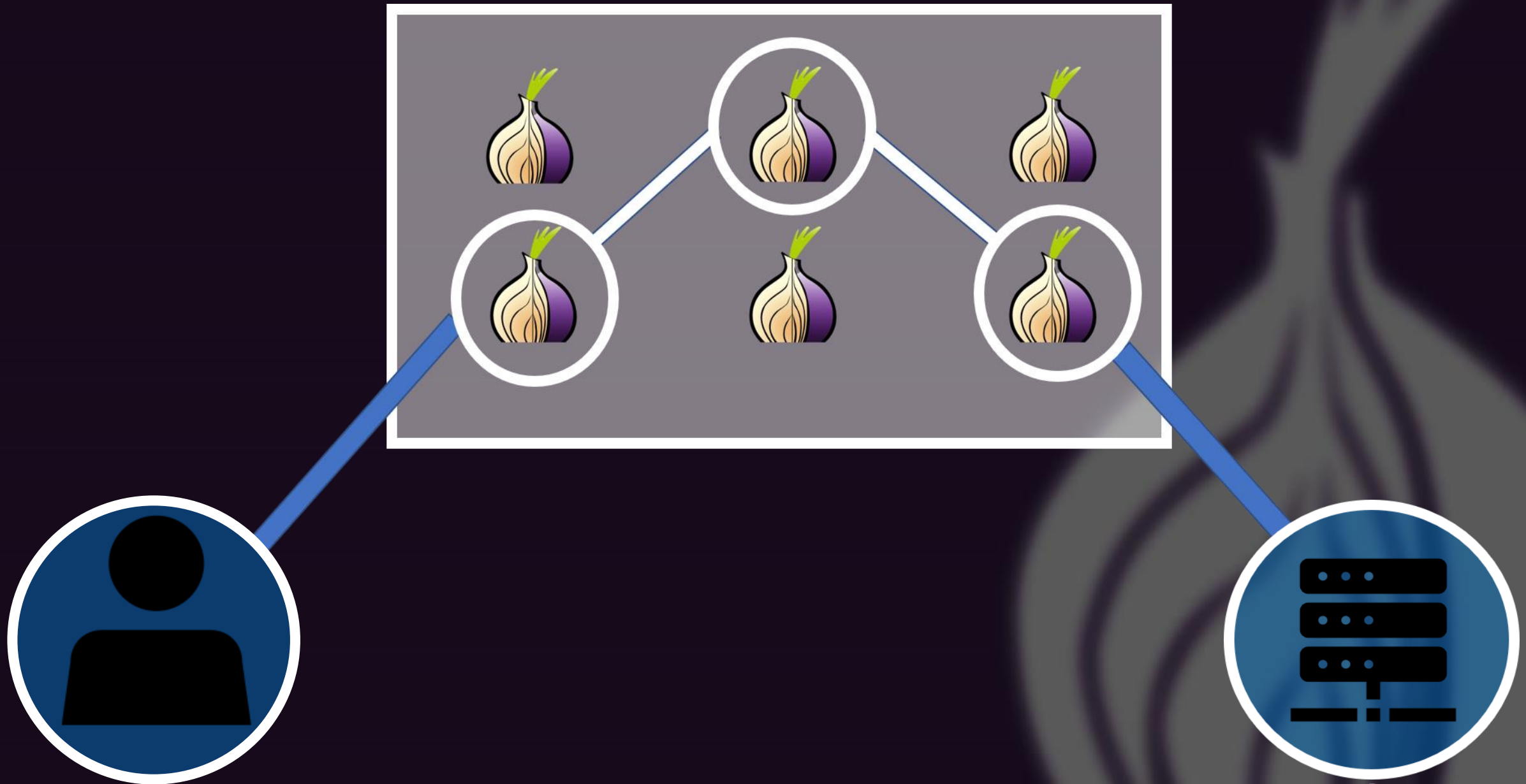
- Incentivizing more volunteers to set up Onion routers

- Spreading awareness about Tor enhancing the reputation of the network

THANK YOU!



THE Tor NETWORK



USER

Research Question:

The number of people who can actually access the Tor network over the number of people trying to access the Tor network

Problems

- Censorship
- Usability of the Tor Browser/Proxy

END SERVER

Research Question:

The number of web resources that an individual using the Tor network can access as compared to an individual using a regular browser

Problems

- Server side blocking