

# Nástroje a možnosti internetu

Hlubší vrstvy Internetu II.

24. 11. 2023

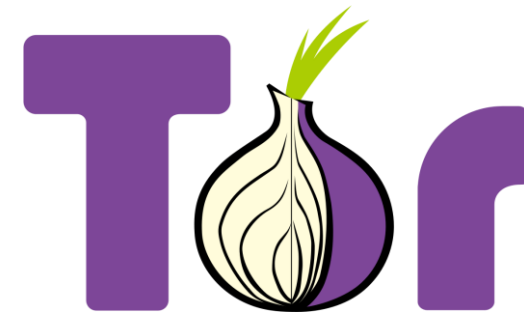
# Onion routing



- původ v armádním [výzkumu](#)
- vytvořit spojení, které neprozradí kdo s kým mluví
- nosnou myšlenkou byl onion routing
- MIT (2000) – výzkumy *Tor* (The Onion Routing)
- fungování založeno na decentralizované síti

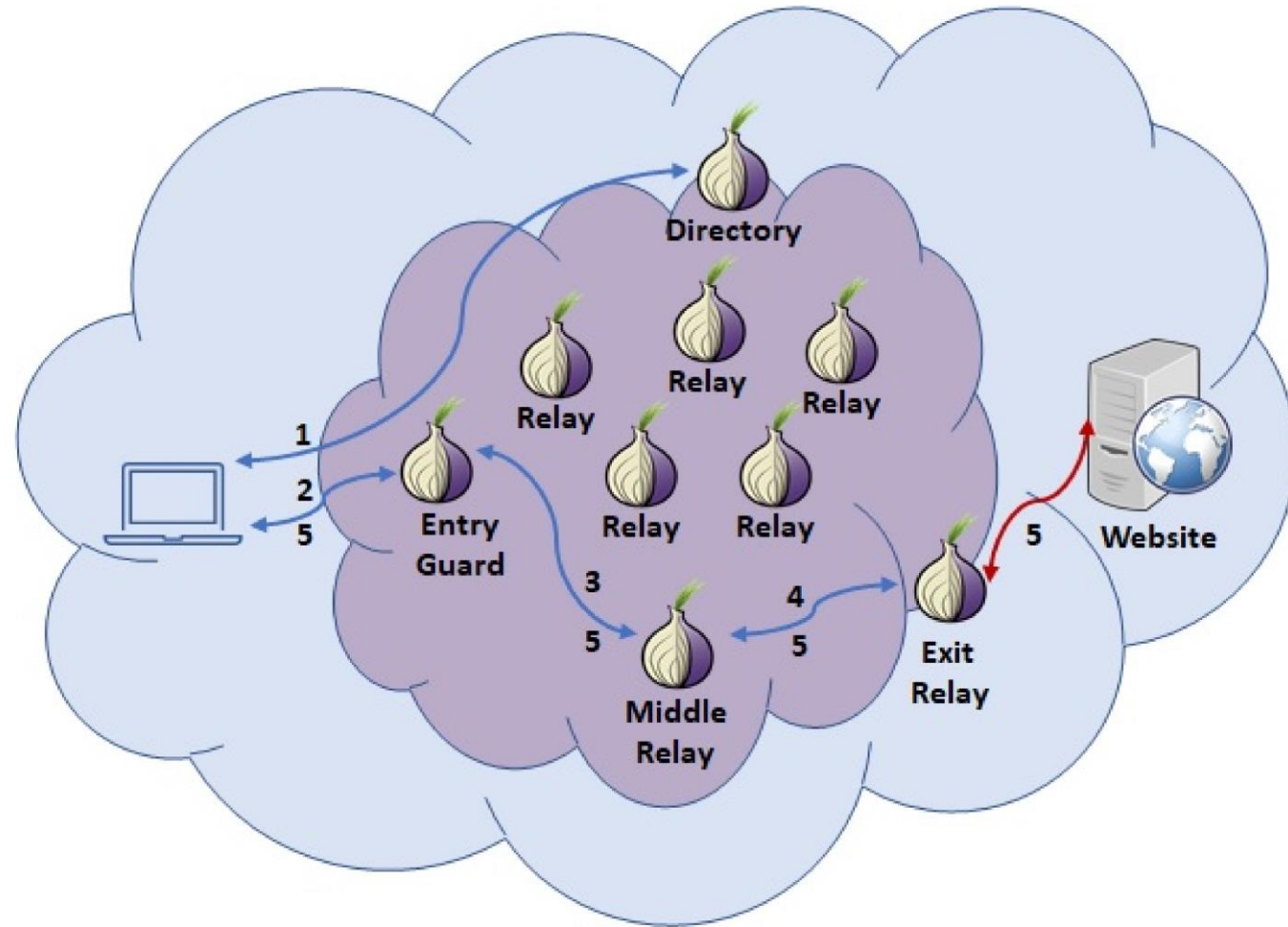
MINULE

# Tor



- potřeba uzlů: otevřeno (2002)
- 2004 – podpora EFF
- ALE: technologická náročnost
- zjednodušení: Tor Browser (2008)
- 2010 – Arabské jaro (*ochrana identity, přístup*)
- 2013 – kauza Snowden

MINULE






2022

## State of the Onion



Wednesday November 9 @ 17:00 UTC  
Wednesday November 16 @ 17:00 UTC

 @torproject  @torproject  @TorProjectInc

2023

## State of the Onion



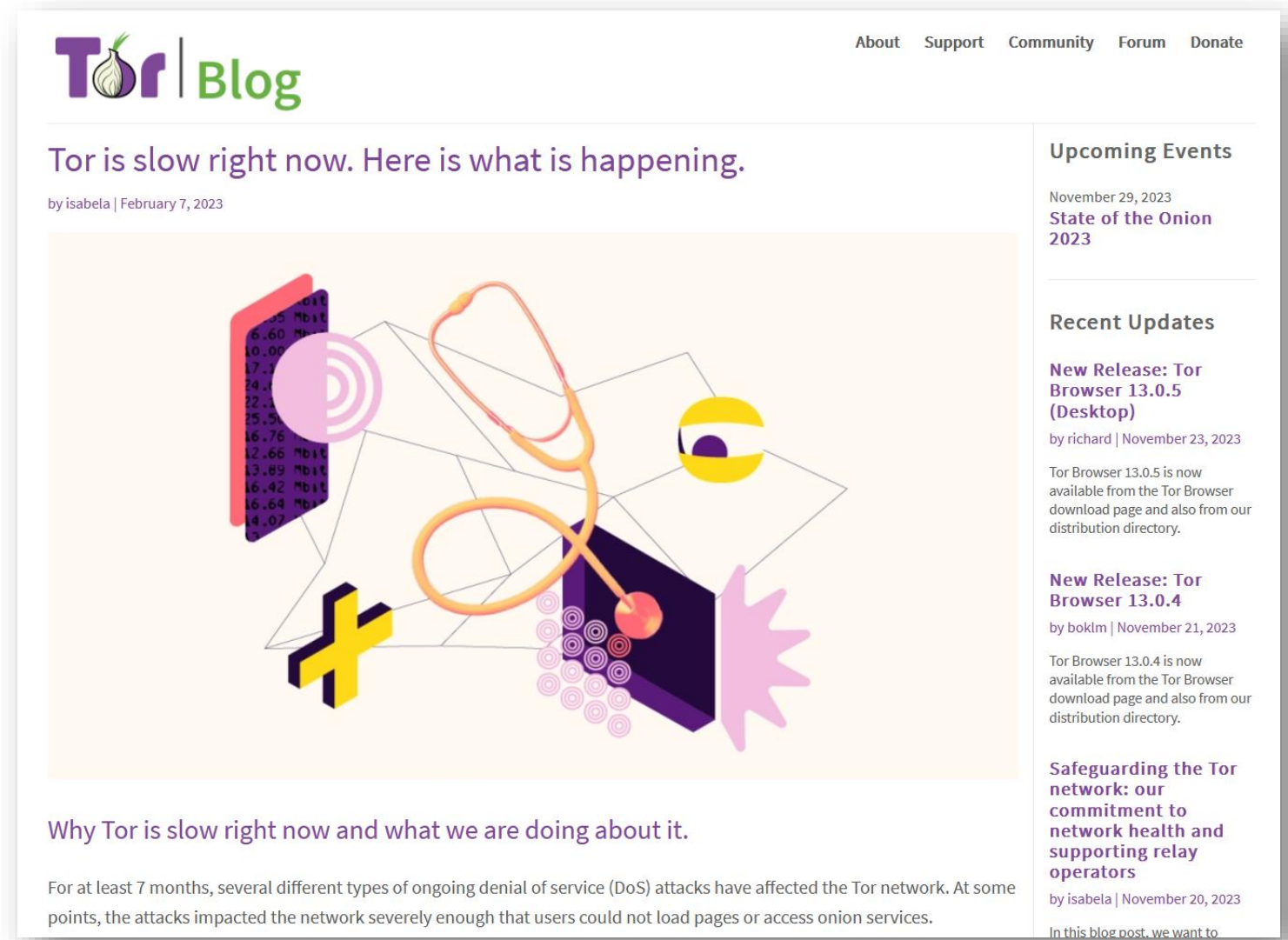
**The Tor Project** November 29 @ 17:00 UTC

**Community Day** December 6 @ 17:00 UTC

 @torproject  @torproject  @TorProjectInc



# Náchylnost k DoS útokům



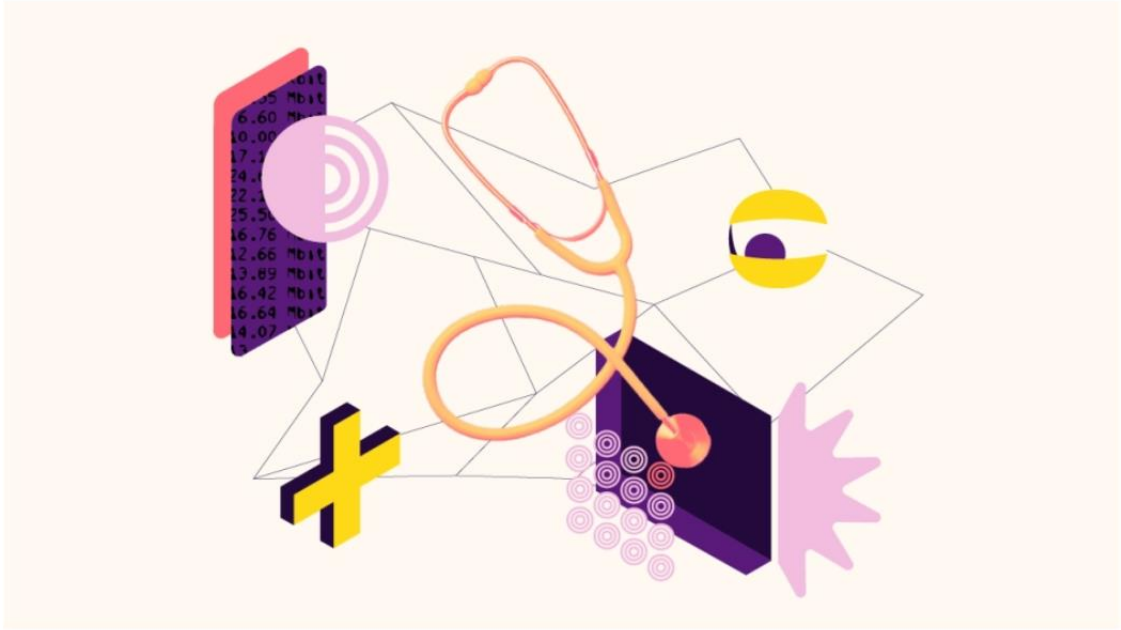
The image is a screenshot of the Tor Blog website. At the top left is the Tor logo (an onion) and the word "Blog". At the top right are navigation links: "About", "Support", "Community", "Forum", and "Donate". The main content area features a post titled "Tor is slow right now. Here is what is happening." by isabela, dated February 7, 2023. The post includes a large, colorful illustration with various symbols: a smartphone with data, a stethoscope, a yellow eye, a purple cube, a yellow plus sign, and a pink starburst. To the right of the main content is a sidebar with sections for "Upcoming Events" (listing "State of the Onion 2023" on November 29, 2023) and "Recent Updates" (listing "New Release: Tor Browser 13.0.5 (Desktop)" and "New Release: Tor Browser 13.0.4"). Below the main content, there is a sub-section titled "Why Tor is slow right now and what we are doing about it." with a paragraph explaining that for at least 7 months, several different types of ongoing denial of service (DoS) attacks have affected the Tor network.

**Tor** | Blog

About Support Community Forum Donate

## Tor is slow right now. Here is what is happening.

by isabela | February 7, 2023



### Why Tor is slow right now and what we are doing about it.

For at least 7 months, several different types of ongoing denial of service (DoS) attacks have affected the Tor network. At some points, the attacks impacted the network severely enough that users could not load pages or access onion services.

### Upcoming Events

November 29, 2023  
**State of the Onion 2023**

### Recent Updates

**New Release: Tor Browser 13.0.5 (Desktop)**  
by richard | November 23, 2023  
Tor Browser 13.0.5 is now available from the Tor Browser download page and also from our distribution directory.

**New Release: Tor Browser 13.0.4**  
by boklm | November 21, 2023  
Tor Browser 13.0.4 is now available from the Tor Browser download page and also from our distribution directory.

### Safeguarding the Tor network: our commitment to network health and supporting relay operators

by isabela | November 20, 2023  
In this blog post, we want to

# Proof-of-Work Defense

*Client Puzzle Protocol*

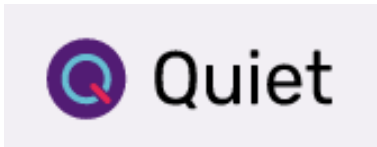
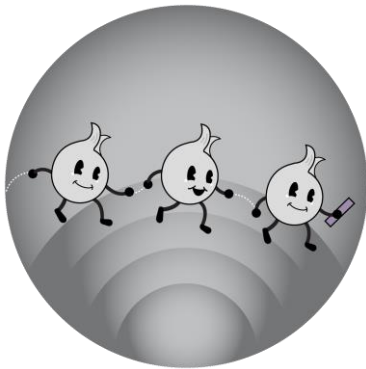
---

 I am human





OONI



Guardian Project

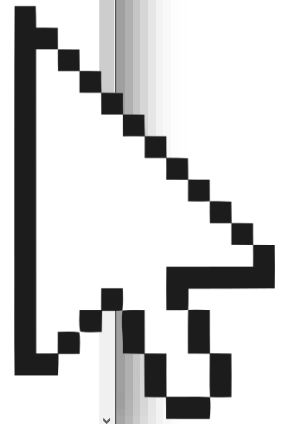
While smartphones have been heralded as the coming of the new communication and collaboration, they are a step backwards with respect to personal security, anonymity and privacy.

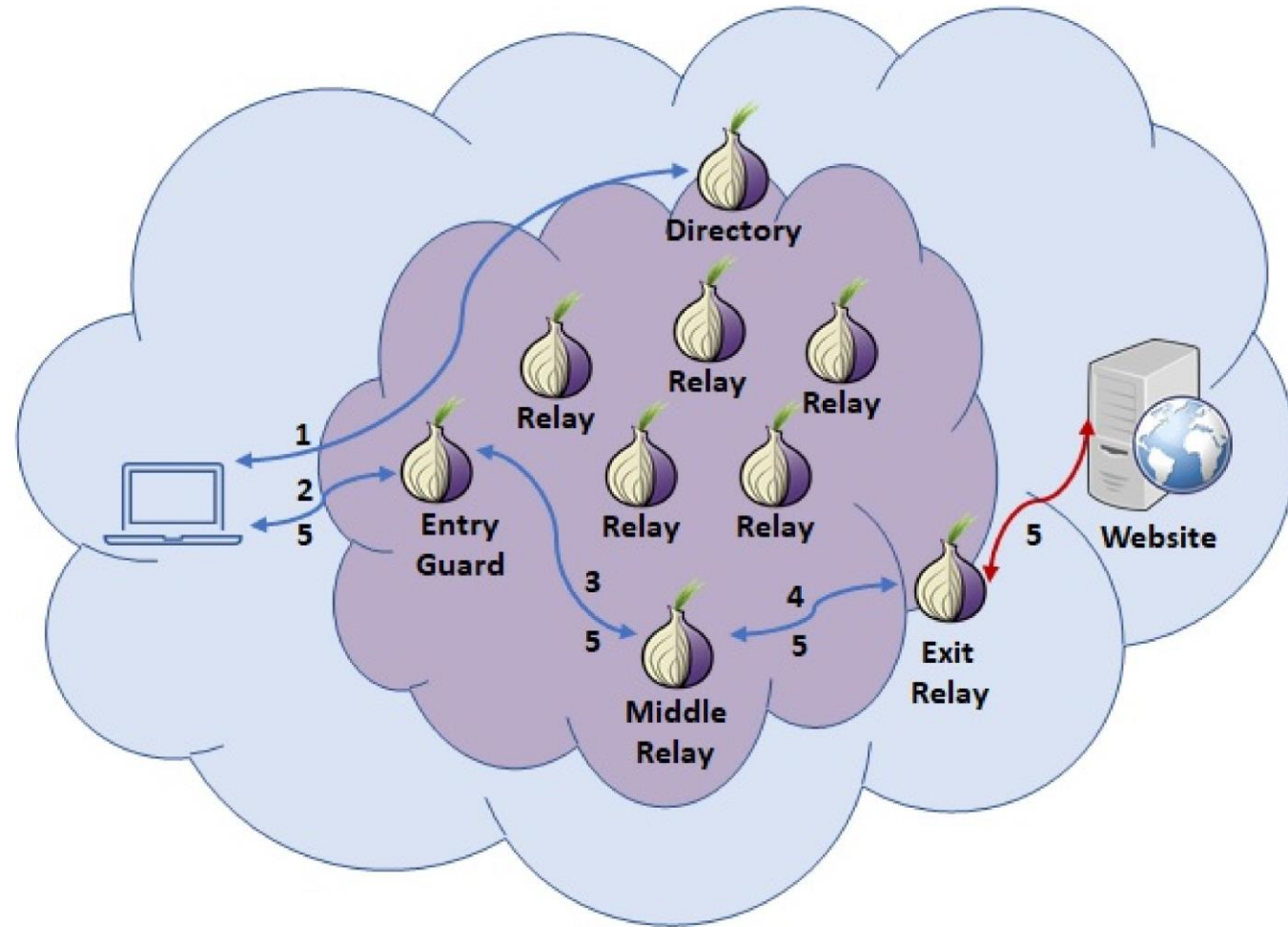
Guardian Project creates easy to use secure apps, open-source and customized solutions that can be used around the world by journalists and human rights activists to protect their communications and personal data from unjust interception and monitoring.

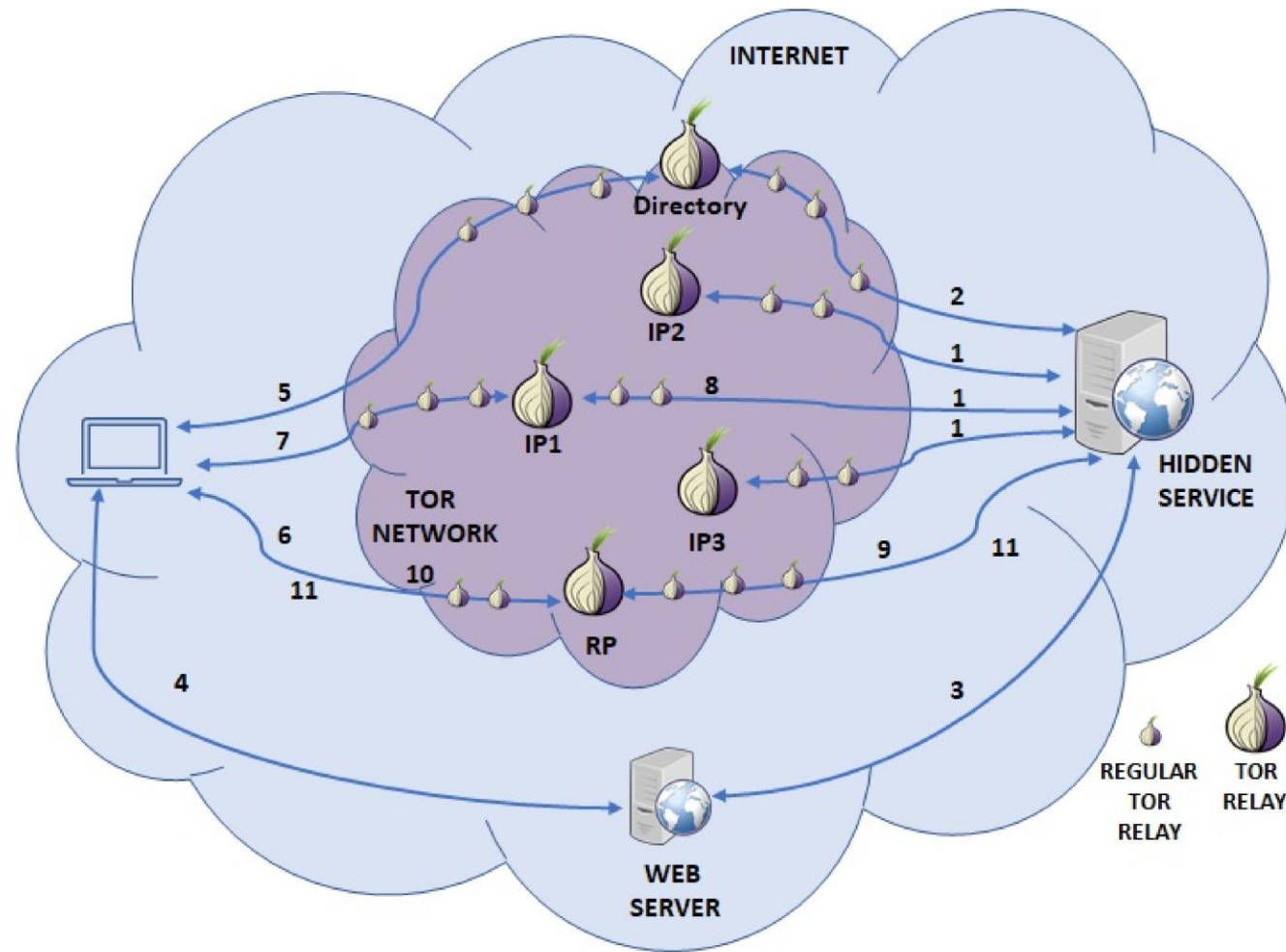
Whether you are an average person looking to affirm your rights as a journalist or humanitarian organization looking to safeguard your communications in a perilous global communication, we can help address the threats.

GUARDIAN

https://guardianproject.info/apps/org.havenapp.main/



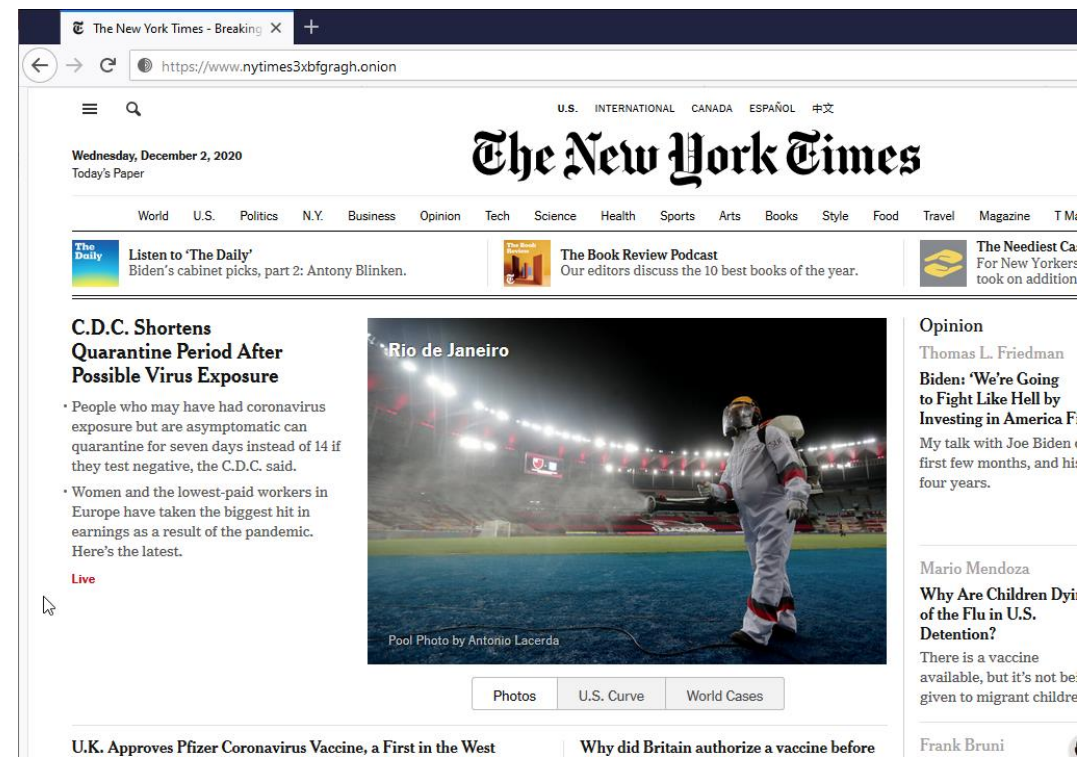




skryté služby

# Onion Hidden Services

- .onion pseudo-doména
- speciální doména pro onion služby
- dostupné pouze skrze Tor
- existují *www2onion* brány, ale to ztrácí smysl



The screenshot shows a web browser window displaying a hidden service page for The New York Times. The browser's address bar shows the URL `https://www.nytimes3xbfgragh.onion`. The page header includes the New York Times logo and navigation links for various sections like World, U.S., Politics, N.Y., Business, Opinion, Tech, Science, Health, Sports, Arts, Books, Style, Food, Travel, Magazine, and T.M. The main content area features a headline: "C.D.C. Shortens Quarantine Period After Possible Virus Exposure". Below the headline, there are two bullet points: "People who may have had coronavirus exposure but are asymptomatic can quarantine for seven days instead of 14 if they test negative, the C.D.C. said." and "Women and the lowest-paid workers in Europe have taken the biggest hit in earnings as a result of the pandemic. Here's the latest." To the right of the text is a photograph of a person in a white protective suit and mask, standing in a large stadium at night. The photo is captioned "Rio de Janeiro" and "Pool Photo by Antonio Lacerda". Below the photo are navigation buttons for "Photos", "U.S. Curve", and "World Cases". At the bottom of the page, there are more headlines: "U.K. Approves Pfizer Coronavirus Vaccine, a First in the West" and "Why did Britain authorize a vaccine before". On the right side, there is an "Opinion" section with articles by Thomas L. Friedman and Mario Mendoza.

[www.nytimes3xbfgragh.onion](http://www.nytimes3xbfgragh.onion)

Kolik procent adres  
na *.onion* doménách  
obsahuje nelegální  
obsah?

[muni.cz/go/nami23](https://muni.cz/go/nami23)



# .onion doména

- [Darksum](#) (2016): 30.000 adres – 13.000 *fčních* zkoumáno
- něco málo přes 50 % obsahovalo nelegální obsah
- 28 % domén k prodeji uniklých dat a hesel
- ilegální pornografie, prodej nelegálního zboží
- ultraprivátní socializační prostory (*furry atp.*)
  
- Moore, Rid (2016) – *etika výzkumu?*
- <https://doi.org/10.1080/00396338.2016.1142085>



Category	Details
Arms	Trading of firearms and weapons
Drugs	Trade or manufacture of illegal drugs, including illegally obtained prescription medicine
Extremism	Content espousing extremist ideologies, including ideological texts, expressions of support for terrorist violence, militant how-to guides and extremist community forums
Finance	Money laundering, counterfeit bills, trade in stolen credit cards or accounts
Hacking	Hackers for hire, trade or distribution of malware or DDoS <sup>45</sup> capabilities
Illegitimate pornography	Pornographic material involving children, violence, animals or materials obtained without participants' consent
Nexus	Websites primarily focused on linking to other illicit websites and resources within the darknet
Other illicit	Materials that did not easily fit into the other categories but remain problematic, such as trade of other illegal goods and fake passports or IDs
Social	Online communities for sharing illicit material in the form of forums, social networks and other message boards
Violence	Hitmen for hire, and instructional material on conducting violent attacks
Other	Non-illicit content, such as ideological or political content, secure drop sites, information repositories, legitimate services
None	Websites which were either completely inaccessible or otherwise had no visible content, including websites which hosted only placeholder text, indicating that their operator had yet to generate indicative content

Category	Details
Arms	Trading of firearms and weapons
Drugs	Trade or manufacture of illegal drugs, including illegally obtained prescription medicine
Extremism	Content espousing extremist ideologies, including ideological texts, expressions of support for terrorist violence, militant how-to guides and extremist community forums
Finance	Money laundering, counterfeit bills, trade in stolen credit cards or accounts
Hacking	Hackers for hire, trade or distribution of malware or DDoS <sup>45</sup> capabilities
Illegitimate pornography	Pornographic material involving children, violence, animals or materials obtained without participants' consent
Nexus	Websites primarily focused on linking to other illicit websites and resources within the darknet
Other illicit	Materials that did not easily fit into the other categories but remain problematic, such as trade of other illegal goods and fake passports or IDs
Social	Online communities for sharing illicit material in the form of forums, social networks and other message boards
Violence	Hitmen for hire, and instructional material on conducting violent attacks
Other	Non-illicit content, such as ideological or political content, secure drop sites, information repositories, legitimate services
None	Websites which were either completely inaccessible or otherwise had no visible content, including websites which hosted only placeholder text, indicating that their operator had yet to generate indicative content

Category	Websites
None	2,482
Other	1,021
Drugs	423
Finance	327
Other illicit	198
Unknown	155
Extremism	140
Illegitimate pornography	122
Nexus	118
Hacking	96
Social	64
Arms	42
Violence	17
Total	5,205
Total active	2,723
Total illicit	1,547

2017; 195748 domén

## The Onions Have Eyes: A Comprehensive Structure and Privacy Analysis of Tor Hidden Services

Iskander Sanchez-Rola  
DeustoTech,  
University of Deusto  
iskander.sanchez@deusto.es

Davide Balzarotti  
Eurecom  
davide.balzarotti@eurecom.fr

Igor Santos  
DeustoTech,  
University of Deusto  
isantos@deusto.es

### ABSTRACT

Tor is a well known and widely used darknet, known for its anonymity. However, while its protocol and relay security have already been extensively studied, to date there is no comprehensive analysis of the structure and privacy of its *Web Hidden Services*.

To fill this gap, we developed a dedicated analysis platform and used it to crawl and analyze over 1.5M URLs hosted in 7257 onion domains. For each page we analyzed its links, resources, and redirections graphs, as well as the language and category distribution. According to our experiments, Tor hidden services are organized in a sparse but highly connected graph, in which around 10% of the onions sites are completely isolated.

Our study also measures for the first time the tight connection that exists between Tor hidden services and the Surface Web. In fact, more than 20% of the onion domains we visited imported resources from the Surface Web, and links to the Surface Web are even more prevalent than to other onion domains.

Finally, we measured for the first time the prevalence and the nature of web tracking in Tor hidden services, showing that, albeit not as widespread as in the Surface Web, tracking is notably present also in the Dark Web: more than 40% of the scripts are used for this purpose, with the 70% of them being completely new tracking scripts unknown by existing anti-tracking solutions.

### Keywords

privacy; dark web; browser security & privacy

### 1. INTRODUCTION

Informally, the *Dark Web* refers to the small portion of the *Deep Web* (the part of the Web which is normally considered to be beyond reach from current search engines) based on *darknets*. Common darknets include, among other smaller P2P networks, *FreeNet* [6], the *Invisible Internet Project*

(I2P) [5], and *Tor* [2]. In the case of Tor, Tor hidden services are used to provide access to different applications such as chat, email, or websites, through the Tor network. In this paper, we focus in particular on the analysis of *websites* hosted on Tor hidden services — due to Tor's much larger popularity between users, which comprised around 7,000 relays or proxies by the time of this writing [4]. The Tor network is based on the onion routing technique [33] for network traffic anonymization.

Due to its hidden nature, Tor hidden services are used for a large range of (cyber)-criminals activities [13, 14, 38, 35]. Thereby, several studies [9, 27, 16, 26] focused on how to discover, access, crawl, and categorize the content of the Dark Web.

Recently, the *OnionScan* [22, 25, 24, 23] and the *DeepLight* reports [17] have analyzed some features related to the content, the size, and the connectivity of the Dark Web. While these studies have helped to better understand its nature, we still lack a complete analysis of Tor hidden services to compare their structure with the corresponding studies of the *Surface Web* [11, 29].

Similarly, while the research community has put a considerable effort to analyze the privacy and security of Tor relays [28, 12, 41, 36] and of its routing protocol [30, 18, 39, 19], a comprehensive analysis of the privacy implications at the application level and of the prevalence of fingerprinting and web tracking is still missing (although these subjects have been extensively studied for the Surface Web [32, 8, 7, 20, 21]).

To fill these gaps, in this paper we present the most comprehensive structure and privacy analysis of the Tor hidden services. Our work is divided in three parts. In the first, we present the most complete exploration of the websites hosted on the Tor hidden services performed to date. Previous measurement studies were limited just to the home pages of each site. While it is true that 80% of the websites have less than 18 URLs, according to our experiments their home pages contain only 11% of the outgoing links, 30% of the resources, 21% of the scripts, and 16% of the tracking attempts. To overcome this limitation, in our analysis we exhaustively downloaded all the reachable content for over 80% of the websites (for a total of 1.5M pages), and we completely crawled 99.46% of the sites to extract links to other domains.

## Recognition of Service Domains on TOR Dark Net using Perceptual Hashing and Image Classification Techniques

Rubel Biswas<sup>1,2,3</sup>, Eduardo Fidalgo<sup>1,2</sup>, and Enrique Alegre<sup>1,2</sup>

<sup>1</sup>Department of Electrical, Systems and Automation, Universidad de León, Spain

<sup>2</sup>Researcher at INCIBE (Spanish National Cyber security Institute), León, Spain

<sup>3</sup>Department of Computer Science and Engineering, BRAC University, Dhaka, Bangladesh  
{rbis,eduardo.fidalgo,ealeg}@unileon.es

Table 1: Most Popular Languages in Onion Domains.

Language	% Domains
English	73.28%
Russian	10.96%
German	2.33%
French	2.15%
Spanish	2.14%

Table 2: Categories in Onion Domains.

Category	% Domains
Directory/Wiki	63.49%
Default Hosting Message	10.35%
Market/Shopping	9.80%
Bitcoins/Trading	8.62%
Forum	4.72%
Online Betting	1.72%
Search Engine	1.30%

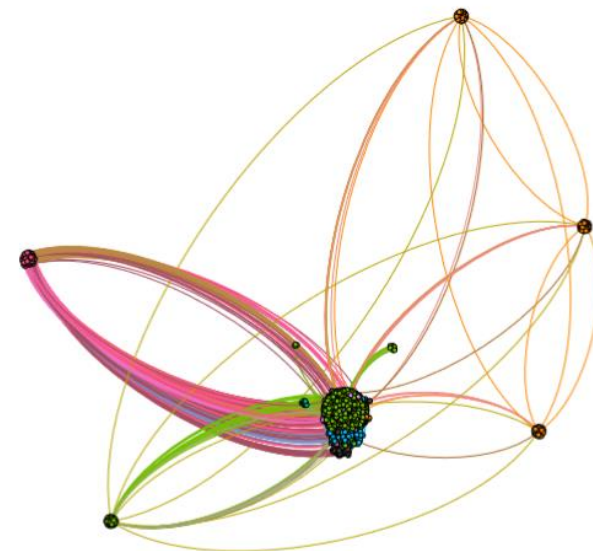


Figure 3: Links Graph of Onion Domains computed with the OpenOrd force-directed layout algorithm and colored communities through modularity. Isolated domains were removed from the figure for clearness of the representation.

## On the state of V3 onion services

Tobias Hoeller  
Johannes Kepler University Linz  
Linz, Austria  
tobias.hoeller@ins.jku.at

Michael Roland  
Johannes Kepler University Linz  
Linz, Austria  
michael.roland@ins.jku.at

René Mayrhofer  
Johannes Kepler University Linz  
Linz, Austria  
rene.mayrhofer@ins.jku.at

### ABSTRACT

Tor onion services are a challenging research topic because they were designed to reveal as little metadata as possible which makes it difficult to collect information about them. In order to improve and extend privacy protecting technologies, it is important to understand how they are used in real world scenarios. We discuss the difficulties associated with obtaining statistics about V3 onion services and present a way to monitor V3 onion services in the current Tor network that enables us to derive statistically significant information about them without compromising the privacy of individual Tor users. This allows us to estimate the number of currently deployed V3 onion services along with interesting conclusions on how and why onion services are used.

### CCS CONCEPTS

• **Networks** → **Network measurement**; Network monitoring; • **Security and privacy** → *Pseudonymity, anonymity and untraceability; Privacy-preserving protocols*

### 1 INTRODUCTION

Tor onion services enable individuals to operate publicly reachable servers without disclosing their network location. Historically, they have been a sideline of the work done by the Tor project. Some have even claimed that onion services were originally conceived as a demonstration of interesting applications that could be built on top of a free and open network like Tor [2]. This sentiment is also supported by their own statistics which show that in 2021 onion services accounted for only 6 Gbit/s of traffic within the Tor network [9]. This pales in comparison to the almost 300 Gbit/s of bandwidth that the Tor network currently consumes in total.

In stark contrast to these numbers, the public opinion often considers onion services a significant building block of the “Darknet” which is believed to be several times larger in size than the easily accessible parts of the Internet. While it is commonly accepted that this perception is incorrect, it does show that reliable figures on the state of the Tor network and onion services in particular are of interest to a lot of parties.

Unfortunately, the desire to collect this information directly conflicts with the fact that onion services are designed to avoid data collection as much as possible so there is actually a very limited amount of information about onion services that is gathered and

published by the Tor project. Currently, the only collected metrics are the number of V2 onion services which were around 200,000 in the first months of 2021 and the amount of traffic generated by V2 and V3 onion services [9].

In the past there have been several other research efforts to learn more about how onion services are being used [6, 7], but they all focused on V2 onion services. This is mainly caused by the fact that certain weaknesses in V2 onion services made it easier to collect and analyze data about them. Since there are no similar issues known about V3 onion services, we know much less about the current version of onion services than we knew about the previous version.

A simple and obvious example would be the total number of active onion services in the Tor network. Right now, we have a solid estimate on the number of V2 onion services but have no information about V3. This is especially relevant, because V2 onion service will be discontinued in 2021 [3] leaving the research community with no information on how many onion services are currently running.

This work tackles the challenge of collecting basic information about V3 onion service usage like the number of currently running V3 onion services and the amount of users they have.

We first discuss the improvements introduced by V3 onion services that make gathering and interpreting data about onion services harder. In section 3 we describe our measurement setup in detail. Afterwards, we present a detailed analysis of our collected data which answers several open questions about V3 onion services.

### 2 TOR AND ONION SERVICES

Tor is an onion routing technology that anonymizes network traffic by tunneling it via several nodes. A connection established via the Tor network is referred to as *circuit* and usually consists of three nodes. The currently available members of the Tor network are defined by the *consensus*, a document that is created by a selected small group of trusted relay operators called *directory authorities*. This consensus is published every hour and lists all currently known relays along with all the information needed to create circuits through them. Additionally, the consensus assigns *flags* on relays based on their behavior and capabilities. The most important flags in the context of this paper are *Fast*, *Stable*, and *HSDir*. A relay is considered fast if it has a bandwidth of more than 105 KB/s, stable if it has a weighted mean time between failure of more than 7 days, and HSDir if it is stable, fast, and has an uptime of more than 96 hours. Of special importance when talking about onion services is the fact that the consensus also includes a shared random value which changes every 24 hours to ensure that certain parts of the

## How Do Tor Users Interact With Onion Services?

Philipp Winter  
Princeton University

Anne Edmundson  
Princeton University

Laura M. Roberts  
Princeton University

Agnieszka Dutkowska-Żuk  
Independent

Marshini Chetty  
Princeton University

Nick Feamster  
Princeton University

### Abstract

messaging [4] and file sharing [15]. The Tor Project currently does not have data on the number of onion

Even if the onion domain is more readable, the user still needs to have a way of discovering the onion service in the first place. In contrast to conventional network services, onion services are designed to be difficult to discover. The operator of an onion service must manually advertise the domain, for example by manually adding it to onion site search engines such as Ahmia [22]. The lack of a go-to service such as a “Google for onion services” prompted the community to devise various ways to disseminate onion services through a variety of search engines and curated lists.

ices differ from conventional web services. First, they can only be accessed over the Tor network, and onion domains are hashes over their IP addresses which make them difficult to remember. Third, the path between client and the onion service is obfuscated, increasing latency and thus reducing the performance of the service. Finally, onion services are not advertised, meaning that users must discover these services manually, rather than with a search engine.

In this paper, we study how users cope with these data collection challenges by exploring the following questions:

• How do users’ mental models of onion services differ from conventional web services?  
• How do users use and manage onion services?  
• What are the challenges of using onion services?

Onion services depend on the Tor Browser and the Tor network to exchange traffic, some of which we explored users’ mental models of Tor itself, but this is not the focus of our paper.

To answer these questions, we employed a mixed-method approach. First, we conducted exploratory interviews with Tor and onion service users to guide the design of an online survey. We then conducted a large-scale online survey that included questions on Tor Browser, onion service usage and operation, onion site phishing, and users’ general expectations of privacy. Next, we conducted follow-up interviews to further explore the topics and themes that we discovered in the exploratory interviews and survey. We complemented this qualitative data

to anonymity for clients (e.g., obfuscating a client IP address using a virtual private network), Tor onion services provide anonymity for servers, allowing a web server to obfuscate its network location (specifically, its IP address). An operator of a web service may need to anonymize the location of a web service to escape harassment, speak out against power, or voice dissenting opinions.

Onion services were originally developed in 2004 and



Darknet market search

Grams Search

I'm Feeling Lucky

The screenshot shows the main interface of the Grams website. At the top, there is a navigation bar with a logo on the left, a search bar, and links for 'search', 'vendors', and 'markets'. On the right side of the navigation bar, there is a currency selector set to '\$ USD' and a 'Login' link. Below the navigation bar is a large blue banner with the word 'search' in white. Underneath the banner, there is a white search bar with a magnifying glass icon and a gear icon for settings. Below the search bar, there are three statistics displayed in large bold text: '23.7k Vendors', '61k Listings', and '1.3m Reviews'. At the bottom of the page, there are three white boxes with blue icons and text: 'Vendors' (with a person icon) 'Search vendors by username or PGP Key.', 'Markets' (with a storefront icon) 'Compare active markets and their statistics.', and 'Network' (with a network diagram icon) 'Explore the largest Dark Net Forum Platform.'

Imperial Library Home About News Upload Forum Help Search Login/SignUp

There are 596566 books on the library.

**Last books added:** [\(more\)](#)

- Ein wahres Verbrechen
- L'Eredità sotto chiave
- PR 3094 – Herz des Lichts
- Dare Me: A Novel
- The Case against Education: Why the Education System Is a Waste of Time and Money
- Air

romance fantasy mystery contemporary science fiction roman fiction young adult thriller history classics general suspense adult adventure [heft]  
 horror roman-science fiction childrens roman-fantasy roman-krimi biography [erotik] humour sachbuch philosophy politics vampires historical  
 roman-thriller science religion war anthologies short stories psychology [kinder] poetry self help reference business writing literature & fiction  
 paranormal travel mystery & detective roman-historisch erotica spirituality john sinclair

Chief Librarian: Las Zenow <zenow@riseup.net>  
 Fork the source code from [gitlab](#).

## Copyright

Copyright laws are obsolete. With the technology to copy books without cost we can finally have universal access to the culture. We can provide the tools to allow everybody read any book without dependence on their monetary resources.

Of course we have to feed the authors, but with the capitalist way of commercialize culture now we are doing a really bad job at that. We are feeding big corporations, not the authors.

The Imperial Library of Trantor won't listen to any content remove request from corporations, editorials, right management organizations or any other blood-suckers.

We are a team of 3 contract killers working in the US (+Canada) and in the EU. Once you made a “purchase” we will reply to you within 1-2 days, contract will be completed within 1-3 weeks depending on target. Only rules: no children under 16 and no top 10 politicians.

Our notes are made with the highest quality cotton fibre, all security features are included: watermarks, security thread, microprint, magnetic ink, color shifting ink, etc.

When you use CleanCoin to mix your Bitcoins, you will receive Bitcoins that originate from lots and lots of different transactions and wallet addresses, making it almost impossible for someone to track your wallet activity.

Kamagra is the preferred alternative to Viagra for customers wishing to use the generic version of this popular treatment for impotence and erectile dysfunction.



## Commerce [\[ edit \]](#)

See also: [Darknet market](#)





- [Agora](#) (defunct)
- [Atlantis](#) (defunct)
- [AlphaBay](#) (defunct)
- [Black Market Reloaded](#) (defunct)
- [Dream Market](#) (defunct)
- [Evolution](#) (defunct)
- [The Farmer's Market](#) (defunct)
- [Hansa](#) (defunct)
- [Sheep Marketplace](#) (defunct)
- [Silk Road](#) (defunct)
- [TheRealDeal](#) (defunct)
- [Utopia](#) (defunct)





procesní vospělost  
*kvalita služeb*

### Ordering form

	US Fullz	<b>69\$</b>	0.0173 BTC 1.21 LTC 0.523 ETH	Quantity: <input type="text"/>
	US Dumps (101)	<b>49\$</b>	0.0123 BTC 0.86 LTC 0.371 ETH	Quantity: <input type="text"/>
	EU Fullz	<b>59\$</b>	0.0148 BTC 1.04 LTC 0.447 ETH	Quantity: <input type="text"/>
	EU Dumps (102)	<b>55\$</b>	0.0138 BTC 0.96 LTC 0.417 ETH	Quantity: <input type="text"/>

### Payment type

 **bitcoin**

 **litecoin**

 **ETHEREUM**

1 btc = 3985 usd. 1 ltc = 57 usd. 1 eth = 132 usd.

**LOCKBIT 3.0** **LEAKED DATA**

TWITTER > HOW TO BUY BITCOIN > CONTACT US >  
 PRESS ABOUT US > AFFILIATE RULES > MIRRORS >

Instant search  Company name:

File Name	File Size
2ee	-
7ge	-
a-r-	-
abc	-
abi	-
abv	-
aca	-
acc	-
ad.l	-
adj	-
adv	-
age	-
age	-

**RAN**  
**SOM**  
 With Love!  
**WARE**  
*Vice Society*

**FOR JOURNALISTS** **FOR VICTIMS** **OUR BLOG**

**OUR PARTNERS**

SSV Architects  
<http://www.ssv-architekten.de/>  
 Germany

Our office realizes a wide range of different construction tasks. We design buildings that are natural, individual and clearly designed. These include both new buildings and the majority of conversions of mostly listed buildings.

**SSV ARCHITEKTEN**

šifrování, mazání, zveřejňování

There are many journalists asking questions about us and our attacks.  
If you are a journalist and want to ask some questions you should write:

1. Who are you?
2. Where are you from?
3. Where will you publish our answers?

We are trying to answer everyone in 24 hours.

#Frequently Asked Questions:

Why did you choose GTA as branding?

-Some old articles about us used GTA logo, so we decided to use it too.

How long have you been in operation?

-From January 2021.

Are you recruiting partners or are you closed?

-We have been closed from the beginning and we don't have affiliates.

How did you decide to team up and start a dedicated ransomware group? How was ViceSociety born?

-Group of friends that were interested in pentest. We decided to try.

What do you do if the law says that someone can't pay you? Does that matter? What happens if the customer doesn't respond?

-We don't care about laws. If someone doesn't pay or doesn't contact us, we will publish their documents.

Has Vice Society published all the data it took from "company name" or does Vice Society have additional data that still has not been published?

-We always publish everything.

Can you explain your decision to publish "company name" data?

--They didn't pay.

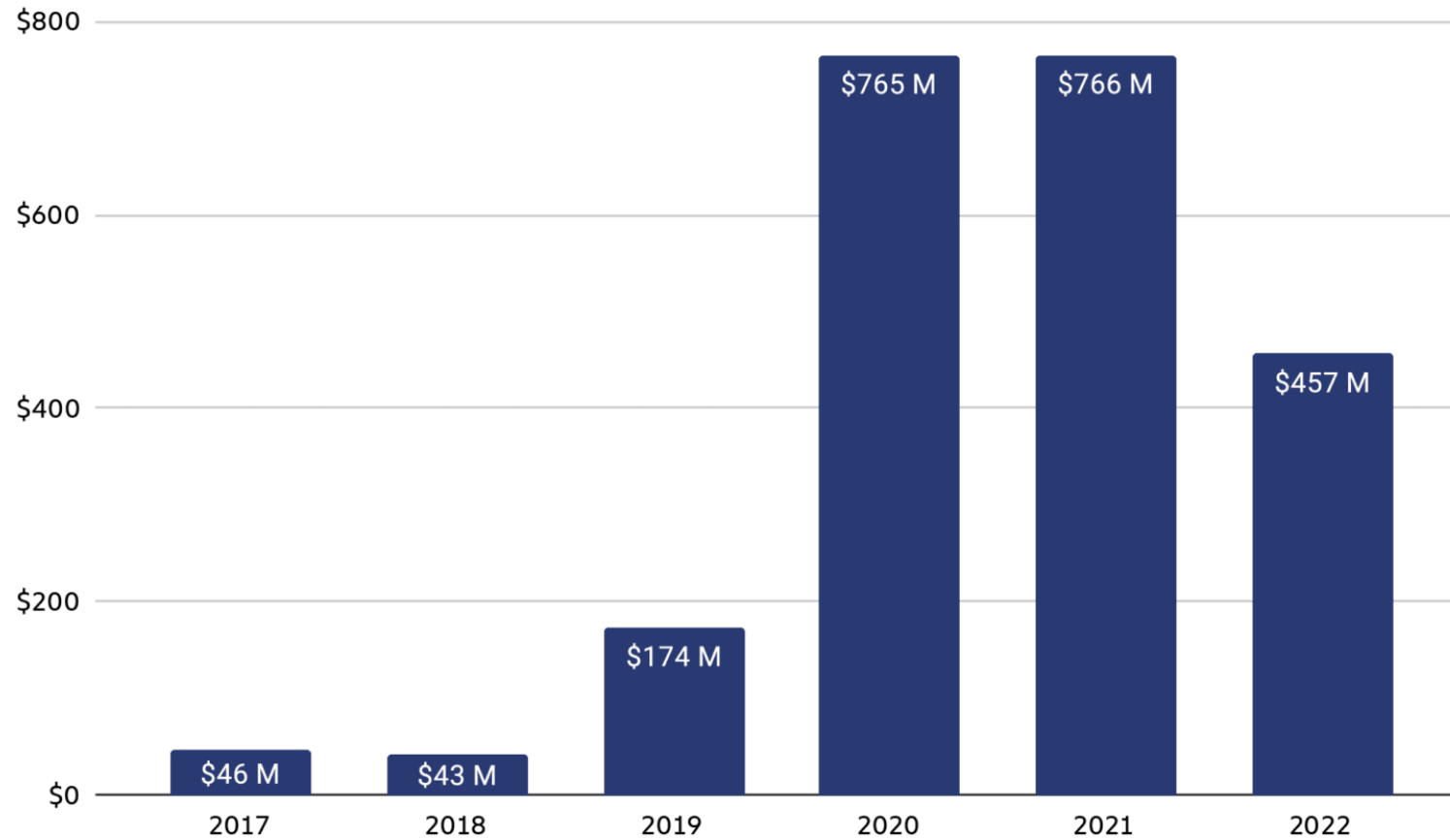
We DON'T answer questions like:

What country or region of the world are you from?

How old are you?

What vulns/cve do you use?

## Total value received by ransomware attackers, 2017 - 2022



In an action carried out between 16 and 20 October, searches were conducted in Czechia, Spain and Latvia. The “key target” of this malicious ransomware strain was arrested in Paris, France, on 16 October, and his home in Czechia was searched. Five suspects were interviewed in Spain and Latvia in the following days. At the end of the action week, the main perpetrator, suspected of being a developer of the Ragnar group, has been brought in front of the examining magistrates of the Paris Judicial Court.

LANDES-KRIMINALAMT | POLIZEI Sachsen | STAATSANWALTSCHAFT LEIPZIG | Freistaat SACHSEN | PARQUET DE PARIS JUNALCO | Federal Criminal Police Office

DEPARTMENT OF JUSTICE IRELAND | Gendarmerie nationale | POLITIE | POLIZIA POSTALE

**This service has been seized as part of a coordinated international law enforcement action against the RagnarLocker group**

EUROPOL EC3 European Cybercrime Centre | EUROJUST | POLICIJA | GUARDIA CIVILE CIBERCRIMEN

<https://metrics.torproject.org/>

Jak odhalovat, řešit  
a postihovat nelegální  
obsah na takovéto síti?



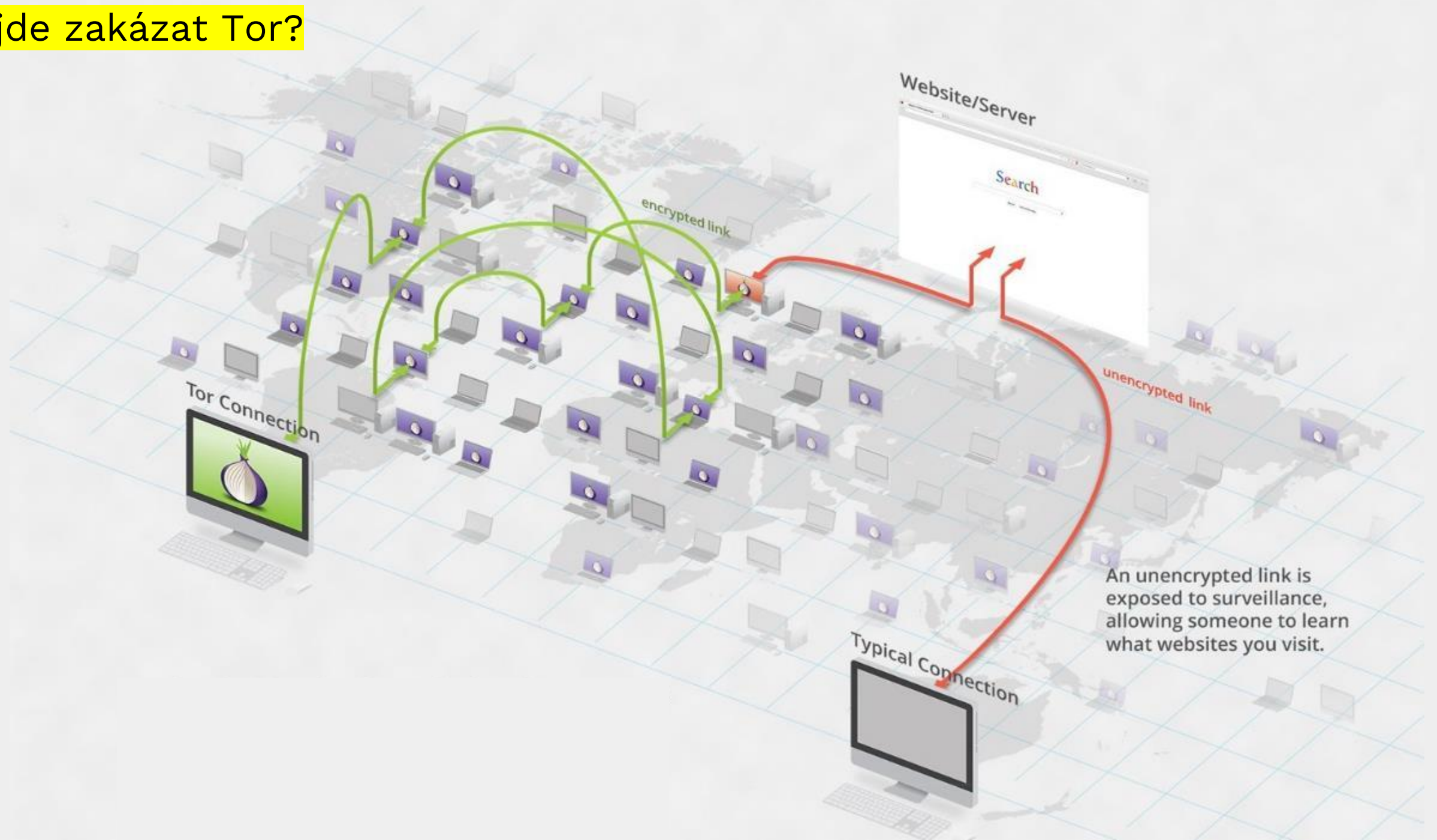


Věra  
Pohlová,  
72 let,  
důchodkyně:

- Tyhle aféry  
každého jenom  
otravují. Já bych  
všechny ty inter-  
nety a počítače zakázala.



# jde zakázat Tor?



# Jde to zakázat?

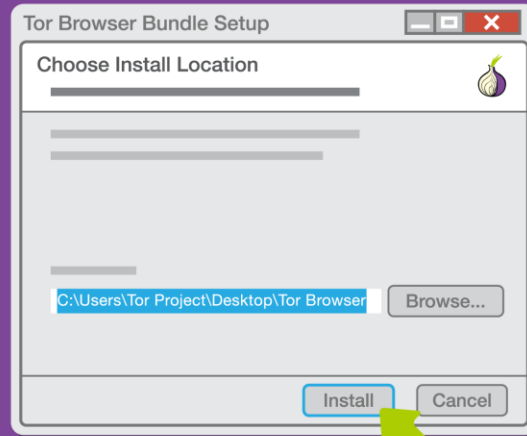
- [databáze exit relays](#)
- [Tor Bridges](#)
- *obfuscation*
- DPI (Deep Packet Inspection) *packet sniffing*
- *i to lze obejít*
- [Pluggable Transports](#)

# What to do when Tor is blocked?

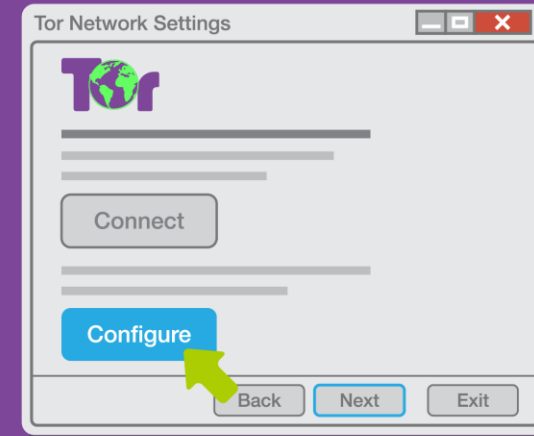
## Step 1: Download Tor Browser



## Step 2: Install



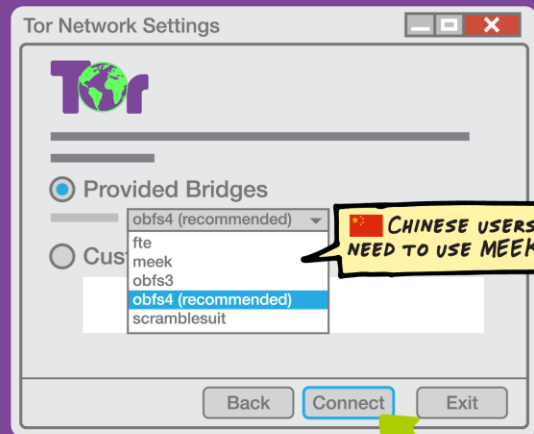
## Step 3: Configure



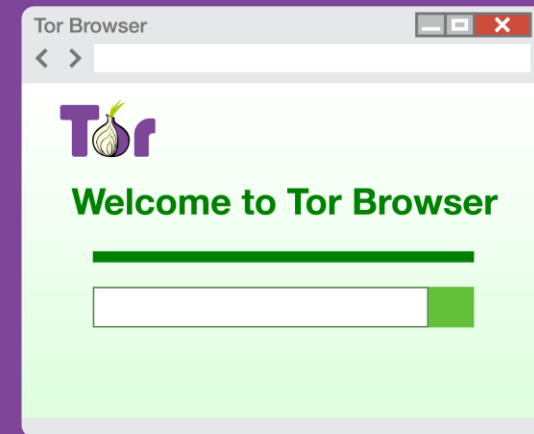
## Step 4: Does your ISP block Tor?



## Step 5: Pick a Bridge



## Step 6: Enjoy!



# Krájení cibule

- Operation Onymous (2014)
- 17 zapojených zemí, 400 onion služeb zaříznuto
- 17 zatčených, milion \$ v Bitcoinu zabaveno, €180,000 v hotovosti, drogy a zlato
- *Blake Benthall*, zakladatel Silk Road 2.0
- [\*jak se to povedlo?\*](#)
- Europol: „This is something we want to keep for ourselves. The way we do this, we can't share with the whole world, because we want to do it again and again and again.“ ZDROJ

Měl by EUROPOL  
zveřejnit, jak přesně  
k odhalení došlo?



operational security



*Silk Road -> Silk Road 2.0 -> Silk Road 3.0*

## Categories

Drugs	18836
Fraud Related	2026
Guides & Tutorials	3702
Services	1431
Jewellery	54
Digital Goods	12425
Erotica	1396
Counterfeits	683
Electronics	33
Security & Hosting	90
Miscellaneous	312

# Welcome to HANSA Market

The Darknet Market with the main focus on a trustless payment system, which makes it impossible for the vendors OR the site staff to run away with Bitcoins of the buyers.

### Multisig escrow

Optional 2-of-3 multisig for buyers and 2-of-2 multisig as a fallback for buyers that do not want to bother with multi-signature. Money can never be accessed by the market staff. Theft is impossible.

### No Bitcoin deposits

Every order has its unique Bitcoin address similar to BitPay's or Coinbase's payment system. Buyers have 15 minutes to pay the order and do not have to wait for deposits to arrive.

### No Finalize Early

We do not support FE or partial escrow releases and we don't have to! The multisignature escrow makes it impossible for the site staff or vendors to steal any Bitcoins.

Current Lottery Jackpot: ₿ 8.4545 USD 21,635.72

[Buy tickets](#)

## Featured Listings

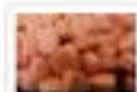


USD 11.35  
₿ 0.0044

0.2G Sample - 80% Pure Bolivian Cocaine (Levamisole Free) (Free shipping) 10 €

AmsterdamSupply [+8|0]

Level 2 (9)



USD 199.00  
₿ 0.0778

100 XTC Pill 230mg (MDMA) 84% ★ PINK DONALD TRUMP FACE ★ ONLY USA ★ SPECIAL DISCOUNT

DreamShop [+588|0]

★ Level 9 (800+)



USD 150.99  
₿ 0.059

100 - Xanax Pfizer X2 Replicas 3mg Alprazolam - US2US - Tracked

StarkoftheNorth [+1|0]

★ Level 1 (1)



Bylo podle vás  
v pořádku, že policie  
zvolila tento způsob  
zátahu?



# Police arrest 150 suspects after closure of dark web's largest illegal marketplace

15

*The international operation seized millions of dollars in cash, crypto, and drugs*

By [James Vincent](#) | Oct 27, 2021, 6:53am EDT

[f](#) [t](#) [SHARE](#)

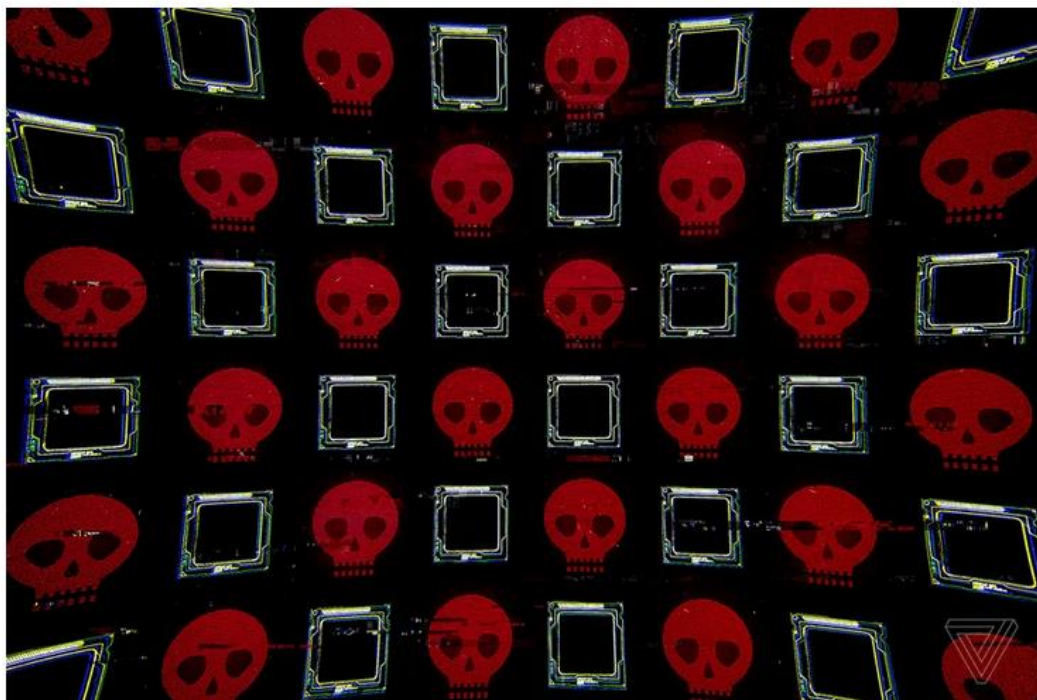


Illustration by Alex Castro / The Verge

  
**verge  
deals**

Subscribe to get the best Verge-approved tech deals of the week.

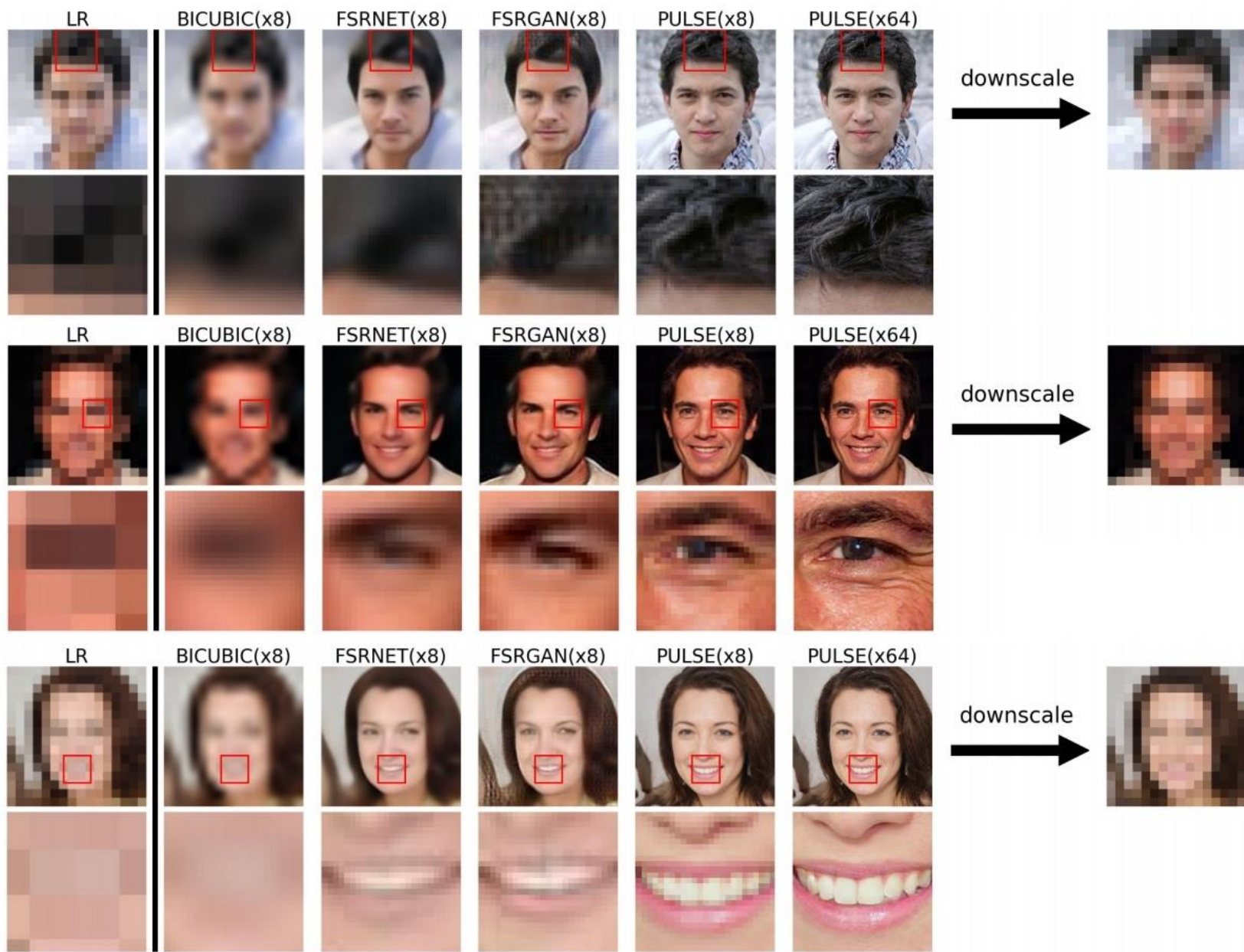
Email (required)

By signing up, you agree to our [Privacy Notice](#) and European users agree to the data transfer policy.

SUBSCRIBE

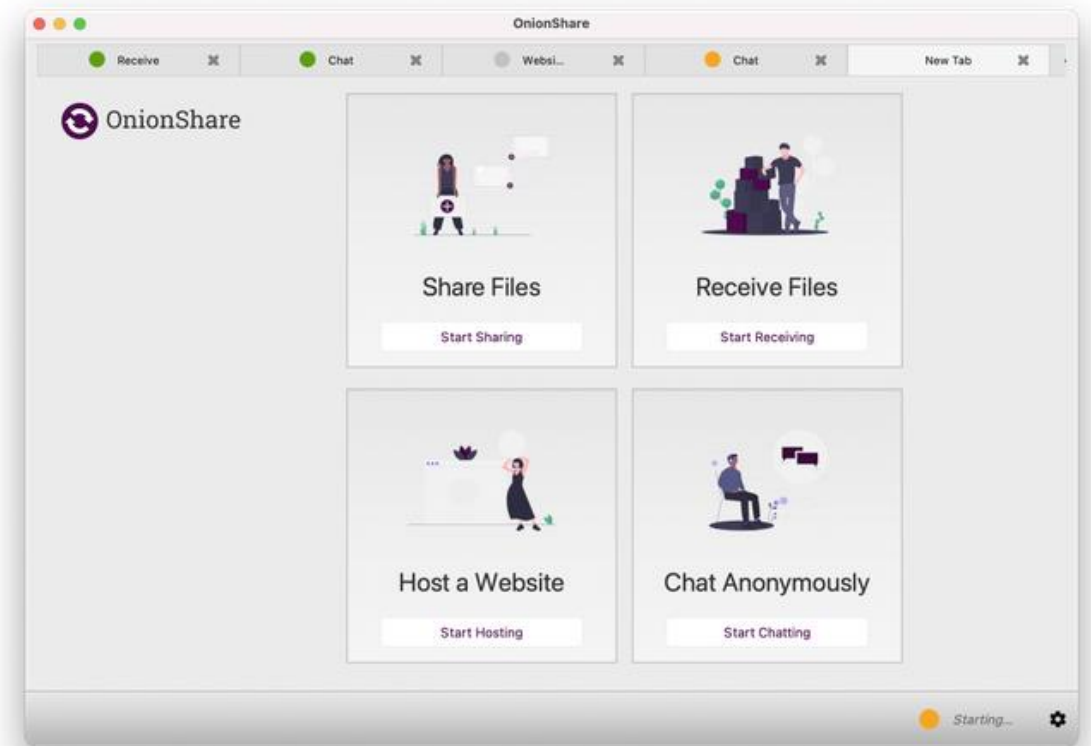
operational security





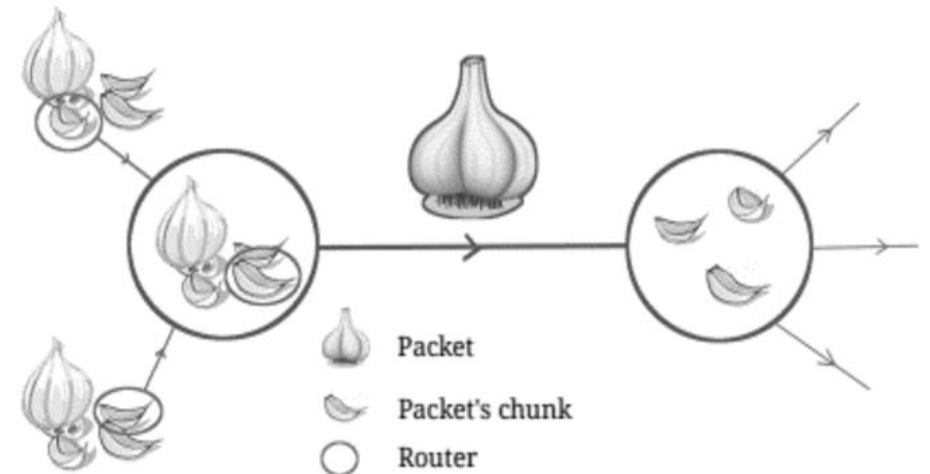
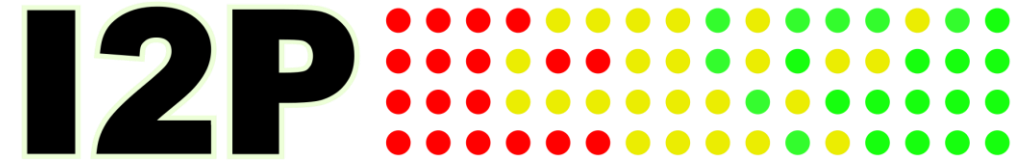
# Další Tor služby

- Tor Messenger – *skončil 2018*
- [OnionShare](#)
- [Whonix](#)



# I2P

- Invisible Internet Project
- *garlic routing*
- <https://geti2p.net/>
- vlastní aplikace (I2PMessenger,...)
- eepsites *.i2p*
- hidden service, ~~exit traffic~~





Version: 0.9.31-0  
Uptime: 3 min

**BANDWIDTH IN/OUT**

3 Sec: 0.13 / 1.64 KBps  
Total: 0.27 / 1.57 KBps  
Used: 79.96 KB / 335.46 KB

Network: Firewallled



**LOCAL TUNNELS**

- shared clients
- shared clients (DSA)

# I2P ROUTER CONSOLE

8/12/17 CONGRATULATIONS ON GETTING I2P INSTALLED!

Welcome to I2P! Please have patience as I2P boots up and finds peers.

While you are waiting, please **adjust your bandwidth settings** on the [configuration page](#).

Also you can setup your browser to use the I2P proxy to reach eepsites. Just enter 127.0.0.1 (or localhost) port 4444 as a http proxy into your browser settings. Do not use SOCKS for this. More information can be found on the [I2P browser proxy setup page](#).

Once you have a "shared clients" destination listed on the left, please **check out our FAQ**.

Point your IRC client to **localhost:6668** and say hi to us on **#i2p**.

## WELCOME TO I2P



### APPLICATIONS AND CONFIGURATION

 Addressbook	 Configure Bandwidth	 Configure UI	 Customize Home Page	 Email	 Help	 Manage Plugins	 Router Console	 Torrents
 Web Server								

### HIDDEN SERVICES OF INTEREST

 anoncoin.i2p	 Dev Forum	 diftracker	 echelon.i2p	 exchanged.i2p	 git.repo.i2p	 I2P Bug Reports	 I2P FAQ	 I2P Plugins
 I2P Technical Docs	 I2P Wiki	 Open4You	 Pastebin	 Planet I2P	 Postman's Tracker	 Project Website	 stats.i2p	 The Tin Hat
 Trac Wiki								



## případ Z-Library

10,870,978 Books 84,837,646 Articles ZLibrary Home

Sign In - Donate

# zlibrary

Part of Z-Library project. The world's largest ebook library

General Search Fulltext Search

Search for title, author, ISBN, publisher, md5.. Search

[Search options](#)

### Most Popular

The image displays a row of five book covers from the Z-Library website. From left to right, the books are: 'The Psychology of Money' by Morgan Housel, 'The Midnight Library' by Matt Haig, 'Smart Thinking' by Matthew Allen, 'It Ends With Us' by Colleen Hoover, and 'People We Meet on Vacation' by Emily Henry. Each cover features the book's title, author's name, and a small illustration or graphic related to the book's theme.

On November 16, 2022, U.S. Attorneys for the Eastern District of New York of the Department of Justice unsealed the indictment for two Russian nationals: Anton Napolsky and Valeriia Ermakova, who had been arrested in [Argentina](#) on November 3, 2022.<sup>[33]</sup> They were charged with [criminal copyright infringement](#), [wire fraud](#) and [money laundering](#) for operating the Z-Library website.<sup>[34][35][36]</sup> The indictment pertains to alleged criminal activity taking place from 2018 to 2022, though the pair are suspected to have operated Z-Library for "over a decade".<sup>[37]</sup> Based on details laid out in the criminal complaint, the arrests were accomplished by the FBI with data from Google and Amazon (among other sites), accessed with [search warrants](#), that helped identify the founders of the website.<sup>[38]</sup> The U.S. lawyers retained as official representatives<sup>[39]</sup> requested a dismissal of the criminal indictment in June 2023.<sup>[40]</sup>

When the domains z-lib.org, b-ok.org, and 3lib.net were seized, the DNS servers utilised switched to NS1.SEIZEDSERVERS.COM and NS2.SEIZEDSERVERS.COM, used commonly in US law enforcement seizures. However, these DNS servers have switched to [Njalla](#), an anonymous [hosting provider](#).<sup>[14]</sup> The website continued to be active and accessible through the [Tor network](#) and the [I2P network](#),<sup>[25][30][16]</sup> before returning to the regular Internet through private personal domains issued to each user on February 11, 2023.<sup>[31][32]</sup>

operational security

14. Google records reflect that a Russian-based telephone number ending in - 2458 (“Napolsky Phone-1”) was used to register the email Napolsky7@gmail.com as well as the emails donation.zlib@gmail.com, zlibdoms@gmail.com and feedback.bookos@gmail.com.

15. Google records also reflect that the account associated with the email address feedback.bookos@gmail.com was created with the name “Z-Library Team” and feedback.bookos@gmail.com is the recovery e-mail for the account zlibsupp@gmail.com, which was created with the name “ZLibrary Support.” Similarly, zlibsupp@gmail.com is the recovery e-mail account associated with the email address zlibdonat@gmail.com, that was created with the name “Zlibrary Mailer.”

ss internet connection) was used to log in to all three accounts.

nts logged in from the IP address 5.8.39.0 as indicated below:

	Time Stamp
	10/27/2021 8:48:31 AM
	10/27/2021 8:55:31 AM
Ermakova Personal Email-1	10/27/2021 8:55:31 AM
zlibsupp@gmail.com	10/27/2021 8:55:31 AM
feedback.bookos@gmail.com	10/30/2021 9:49:14 PM
zlibsupp@gmail.com	10/30/2021 9:49:39 PM
Ermakova Personal Email-1	10/30/2021 9:49:39 PM
Ermakova Personal Email-1	10/31/2021 8:58:57 AM
zlibsupp@gmail.com	10/31/2021 8:58:58 AM
Ermakova Personal Email-1	11/3/2021 3:33:39 PM
zlibsupp@gmail.com	11/3/2021 3:33:36 PM
Ermakova Personal Email-1	11/6/2021 11:13:14 AM
zlibsupp@gmail.com	11/6/2021 11:13:15 AM
Ermakova Personal Email-1	11/7/2021 8:23:02 PM
zlibsupp@gmail.com	11/7/2021 8:23:03 PM

# Anonymní OS

- nejvyšší level anonymity
- běží z CD nebo USB
- nezanechává stopu v PC
- <https://tails.net/>
- <https://www.qubes-os.org/>



Nabídli byste službu  
Tor uživatelům  
své knihovny  
na lokálních PC?



# Tor | Knihovny

- Aktuální debata
- <https://doi.org/10.1080/01616846.2019.1696078>
- [Toronto Public Library](#)
- [Library Freedom Project](#)
- knihovny jako prostředník k osvětě
- knihovny jako [hostitelé](#) *exit relays* ([na chvíli](#))

Co s tím vším?





# Slovníček pro další roky

- decentralizace
- splinternet
- small internet
- web3

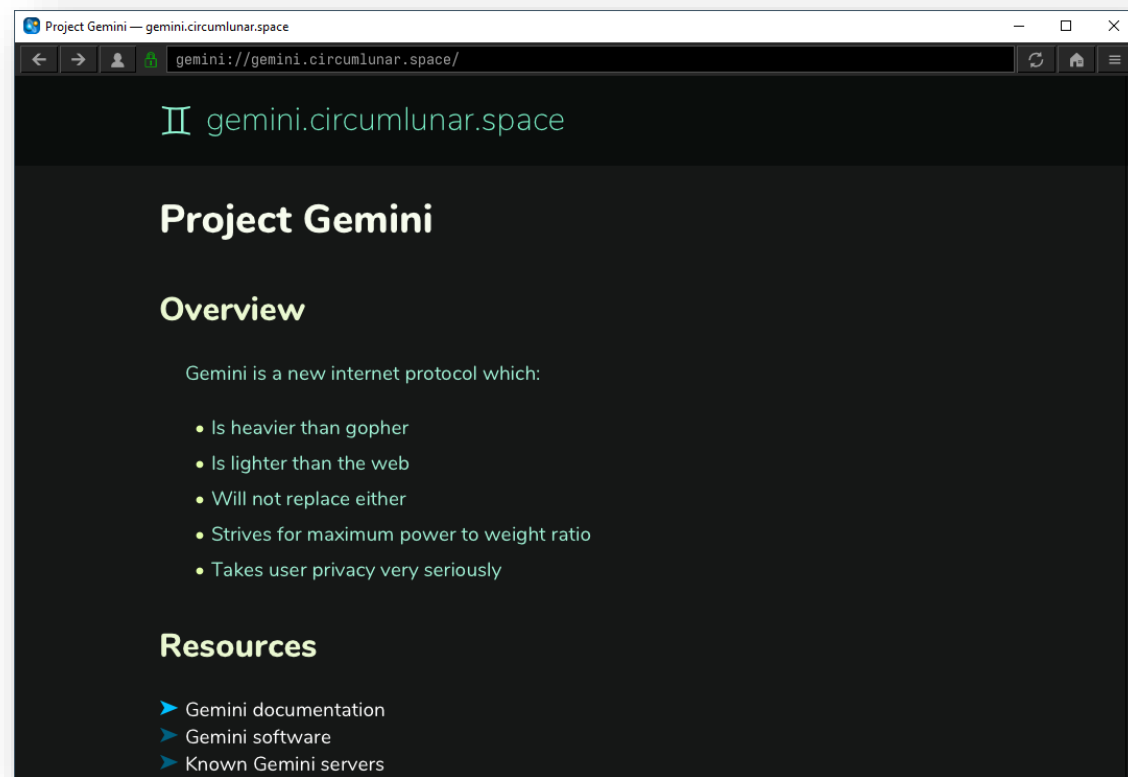
# Splinternet

- také jako „balkanizace“
- národní firewally
- štěpení do platforem
- walled gardens
- různé protokoly
- překryvné služby

Splinternet je označení pro trend štěpení Internetu do mnoha protokolů a sítí. Důvodem je množství potíží tradičního Internetu, založeného na protokolech HTTP/TCP/IP: od cenzury přes monopolizaci Internetového provozu i fyzickou centralizaci, až po problémy se soukromím a sledováním v prostředí webu. V jádru *splinteringu* je nejčastěji otázka svobody slova, mnohdy ale také DIY a technologické hračičkovství.

# Small Internet

- např. návrat ke GOPHERu
- <gopher://i-logout.cz/>
- nové lehké protokoly
- např. Gemini
- <https://gemini.circumlunar.space/>



# Web3

## FF:ISKM73 Commons, P2P a digitální ident - Informace o ...

### ISKM73 Commons, P2P a digitální identita ✳

Filozofická fakulta

podzim 2020

#### ▣ Rozsah

1/1/0. 4 kr. Ukončení: k.

Vyučováno online.

#### ▣ Vyučující

Bc. et Bc. Jakub Lanc (přednášející)

Mgr. Roman Novotný (přednášející)

PhDr. Ladislava Zbiejczuk Suchá, Ph.D. (cvičící)

#### ▣ Garance

PhDr. Petr Škyřík, Ph.D.

Katedra informačních studií a knihovnictví - Filozofická fakulta

Kontaktní osoba: Mgr. Alice Lukavská

Dodavatelské pracoviště: Katedra informačních studií a knihovnictví - Filozofická fakulta

#### ▣ Rozvrh

každé liché úterý 9:00–11:40 B2.22 🗄

#### ▣ Předpoklady

TYP\_STUDIA ( N )

Studium	Prerekvizity	Splněno
CST C-CV	typ_studia(N)	Nesplněné předpoklady: <b>Studentovo studium není typu 'N'.</b>

#### ▣ Omezení zápisu do předmětu

Předmět je nabízen i studentům mimo mateřské obory.

Předmět si smí zapsat nejvýše 20 stud.

Momentální stav registrace a zápisu: zapsáno: 8/20, pouze zareg.: 0/20, pouze zareg. s předností (mateřské obory): 0/20

#### ▣ Mateřské obory/plány

předmět má 7 mateřských oborů, [zobrazit](#)

#### ▣ Cíle předmětu

- Přiblížit aktuální socioekonomické trendy související s nástupem platformové ekonomiky.
- Zmapovat klíčové souvislosti s problematikou "osobních dat" a digitální identity.
- Přiblížit možnou roli "commons-based" přístupů ve snahách směřovat ke zdravějším řešením.
- Ukázat jejich relevanci pro designové uvažování.
- Podnítit schopnost uvažovat v těchto kategoriích a zájem aktivně experimentovat s jejich aplikací.

pomalu končíme...



eseje?



sdílení!

P2P setkání!

praskání bublin!

# NaMI barcamp

spolupráce!

decentralizovaná přednáška!

Jaké služby vám pomáhají v každodenní práci?  
Na jaké (legální) weby chodíte a chcete je ukázat  
i ostatním? Jak vám Internet změnil život?  
Co nejvtipnějšího jste s Internetem zažili?  
Co nejhoršího se Vám na Internetu stalo? Jaké  
tipy a triky používáte na webu a chcete je  
naučit i ostatní? Pojd'te to sdílet!

## 12. NaMI P2P ukončení

### Materiály k setkání



Vyplnění docházky

Vyplňte do 21. 12. 2023.

### Registrujte svůj příspěvek!

Jaké služby vám pomáhají v každodenní práci?

Na jaké (legální) weby chodíte a chcete je ukázat i ostatním?

Jak vám Internet změnil život?

Co nejvtipnějšího jste s Internetem zažili?

Co nejhoršího se Vám na Internetu stalo?

Jaké tipy a triky používáte na webu a chcete je naučit i ostatní? **Pojďte to sdílet!**



**Setkání nebude nahráváno!**

Závěrečné setkání předmětu NaMI nebude zaznamenáno.



Registrujte svůj příspěvek!

← Předchozí

Následující →

### Nástroje a možnosti internetu

- ➔ 1. Úvodně-organizační setkání
- ➔ 2. Síťová neutralita
- ➔ 3. Publikování na webu
- ➔ 4. Wellbeing, rekompozice a demetrikace
- ➔ 5. Organizační metafory webu
- ➔ 6. Internet jako nástroj sledování
- ➔ 7. Internet jako nástroj... II.
- ➔ 8. Hlubší vrstvy internetu
- 🔒 9. Bude upřesněno
- 🔒 10. Bude upřesněno
- 🔒 11. Bude upřesněno

➔ **12. NaMI P2P ukončení**

### NYNÍ STUDOVAT

🔒 Závěrečné eseje

### Operace

- Editovat
- Prohlédnout vše
- Pohled studenta
- Přečtenost