Le Dark web: menace ou opportunité pour le secteur public ?
Dark web: threat or opportunity for the public sector?

Vandy Berten

Smals Research

30/09/2025

Smals Research

Decathlon victime d'une fuite de données
Il a ainsi injecté des informations comme des identifiants et mots de passe, qu'il a trouvées sur le dark web, dans différents systèmes de connexion dont celui de Decathlon.
LE SOIR

Des milliers de boîtes mail professionnelles belges sans défense
Les données de login de nombre de boîtes mail professionnelles (...) sont en vente (...) le 'dark web' (...) 33.568 adresses e-mail de départements financiers: 83 pour cent d'entre elles avec des mots de passe.
DataNews

Démembrement de la plus vaste plate-forme au monde dans le web clandestin
Les autorités allemandes ont mis fin au plus grand marché installé dans ce qu'on appelle le 'dark web'
DataNews

Jemeppe-sur-Sambre : 1,3 billion de données volées à la Commune
Si la rançon de 700 000 € n'est pas payée, les cybercriminels publieront une partie des données volées ce jeudi, à 2h du matin, sur le dark web
l'avenir

WhatsAppgegevens van 3,2 miljoen Belgen te koop op dark web
Op een forum op het dark web zijn telefoonnummers en gebruikersnamen te koop
HLN

La FWA victime de cyber-criminels qui pensaient s'en prendre au SPW
Sur le dark web, 8Base revendique pour sa part huit nouvelles victimes, dont le Service public de Wallonie
RTL info.

Hackers publiceren gegevens na cyberaanval in Geraardsbergen
Die software versleutelt informatie en vraagt de eigenaar om losgeld te betalen. Dat is niet gebeurd, zegt het lokaal bestuur, en de gegevens zijn vandaag gepubliceerd op het dark web.
De Standaard

Une affaire de pédocriminalité horrifie un village
interpellé par la police néerlandaise après que des vidéos de la fillette ont été retrouvées sur le Darknet
La Libre BELGIQUE

Politie waarschuwt voor valse bankmedewerkers: "Cijfers gaan elk jaar de hoogte in"
"Mensen hebben vertrouwen omdat bankmedewerkers alles weten", vertelt de hoofdinspecteur. "Die gegevens verkrijgen ze echter via het dark web."
Het Nieuwsblad

Smals ICT for society

The dark web iceberg

Disclaimer: questionable distribution!

Clear web / Surface web

Part of the web accessible with a browser, indexed by traditional search engines
Examples: www.smals.be, www.rtbf.be, www.belgium.be, www.wikipedia.org...

Deep web

Non-indexed part of web. Accessible with a traditional browser + address or credentials
Examples: Mails, Sharepoints...

Dark web

Part of web requiring specific tools (browser + network)
Examples: **Tor** (The Onion Router), I2P, Hyphanet...

Dark Web Iceberg

4% Surface Web

Deep Web
not accessible with traditional search engines

5% **Dark Web**
unsearchable, encrypted, private

https://www.dashlane.com

Smals
ICT for society

Why was Tor created

How does Tor work

Technical part

What's in there

Who's active

Business part

Smals
ICT for society

Why
was Tor created

- What to protect?
- How to protect?
- Is that enough?

How
does Tor work

What's
in there

Who's
active

Smals
ICT for society

Why
was Tor created

- **What to protect?**
- How to protect?
- Is that enough?

How
does Tor work

What's
in there

Who's
active

Smals
ICT for society

Who can observe you?

- ISP
- (Foreign) Law Enf.

- Website hosters
- Advertisers (3th party)
- (Foreign) Law Enf.

- Hacker
- Relatives/colleagues…
- (Foreign) Law Enf.

https://icons8.com

Smals
ICT for society
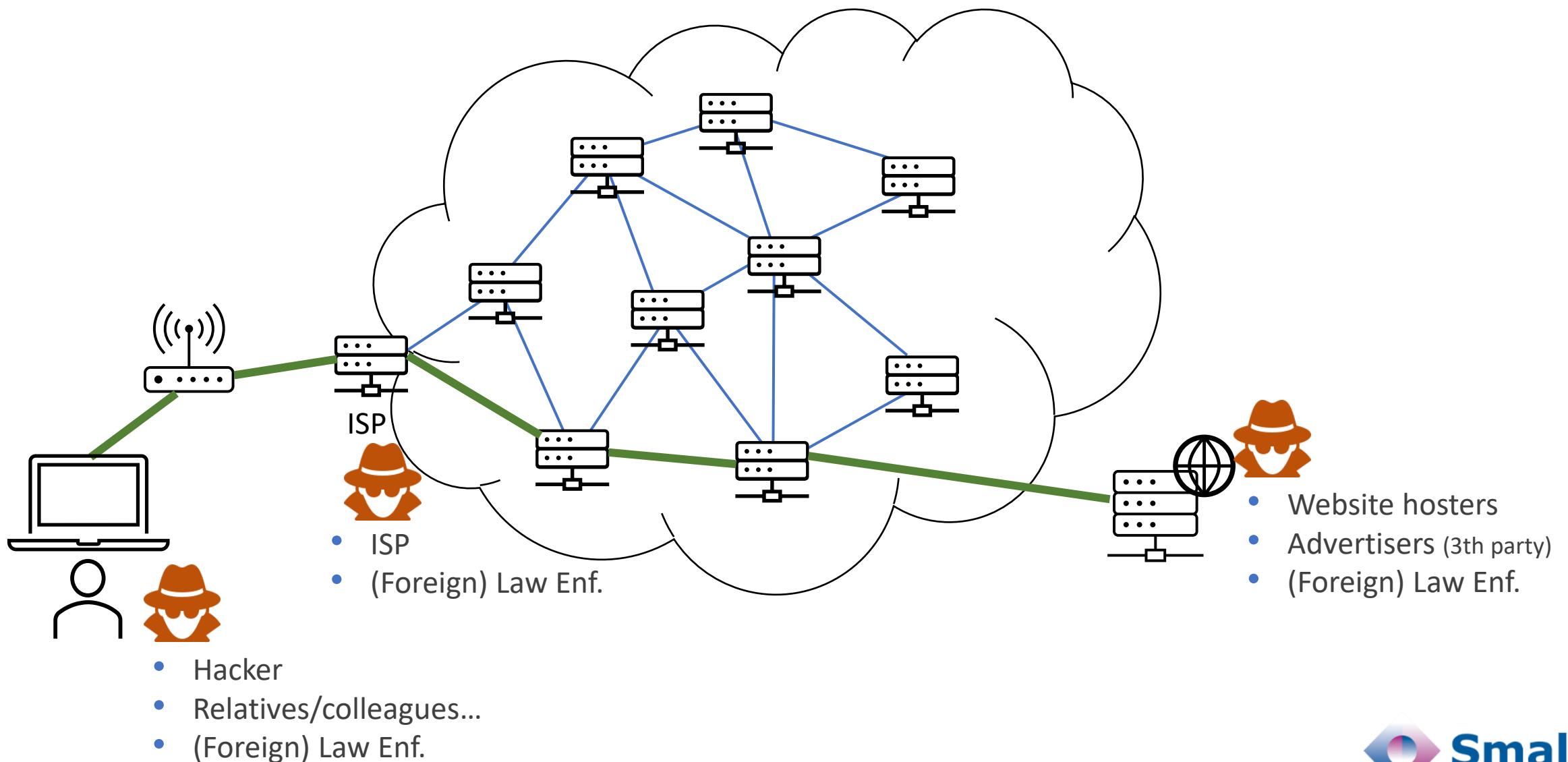
Anonymity vs privacy

Anonymity: preserve who you are

- Identity (post or mail address, phone n°, id…)
- IP address
- Localisation
- ISP
- Try to hide?

Privacy: protect what you do

- Message content
- Visited servers (IP or domain name)
- Browsing history:
  - Current session or past
  - This website or other

https://icons8.com

Smals
ICT for society

Client IP address

109.132.9.5

ISP

192.168.1.7
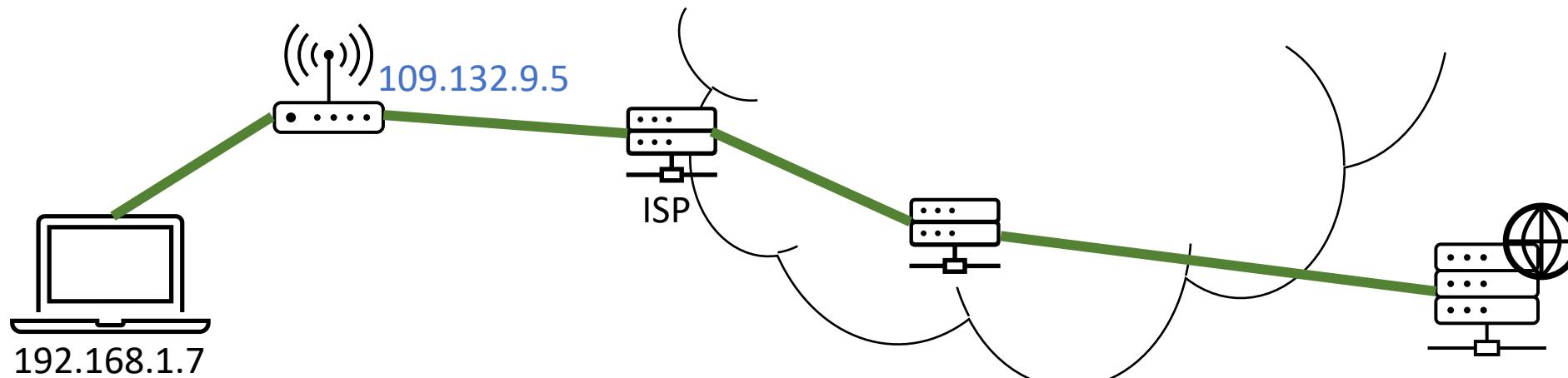
IP address is:
- Shared
- Dynamic
- Not itinerant resistant

Information for website: (very) approximative location
➔ Very limited

But: with IP + timestamp, ISP/Law Enf. can find "you"!

Cookies

GET /page1.html
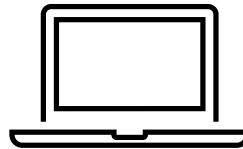
GET /page2.html

<html>…
</html>

<html>…
</html>
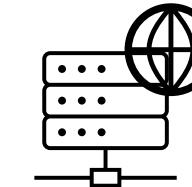
www.smals.be

Cookies:
- Inoffensive/passive (text) file
- Do not (usually) contain history, but Ids and preferences
- Unreadable by other websites
- Unreadable by intermediates (modem, ISP…) if HTTPS
- Allow to keep the session alive between clicks
- But allow to link successive sessions
- …and help websites to 'profile' visitors

Smals
ICT for society

Third party cookies

GET icon.png
Ref: mysite.be/mypage.php

facebook.com

GET /mypage.php

mysite.be

My beautiful page

Ad

GET adv.html
Ref: mysite.be/mypage.php

GET script.js
Ref: mysite.be/mypage.php

mysite.be/mypage.php

googleanalytics.com

cXense.com
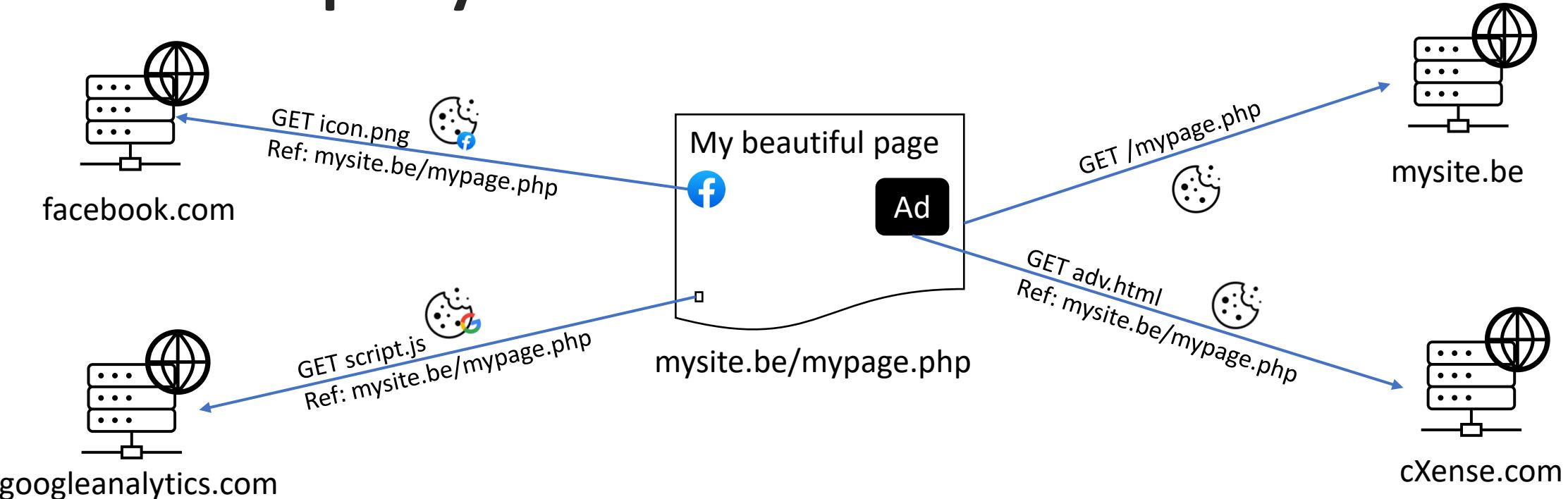
Third party cookies:
- Not readable by main site (and vice-versa)
- Facebook cookie: same as on facebook.com (even if logged off!)
- Allow to track visitors on other sites with the same snippet
- (Almost) no added value for visitors

Good news:
- Easy to disable (with almost no effect)
- Blocked by Firefox or Edge… but not (yet) by Chrome
- Good plugins available (Ghostery…)

Smals
ICT for society

Fingerprinting

Goal: Bypass cookies decline - **Method**: Collect (with JavaScript) as many details to build a "fingerprint"

HTTP header

JavaScript

Attribute	Similarity ratio	Value
1 - User agent	0.18 %	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36
4 - Content language	0.00 %	en,en-US;q=0.9,fr-FR;q=0.8,fr;q=0.7,nl;q=0.6
4 - Timezone	13.12 %	UTC+02:00
6 - Canvas	0.11 %	Cwm fjordbank glyphs vext quiz, 😛 Cwm fjordbank glyphs vext quiz, 😛
7 - List of fonts (JS)	1.02 %	Agency FB Algerian Arial Arial Black Arial Narrow And 158 others
19 - List of plugins	36.19 %	Plugin 0: PDF Viewer; Portable Document Format; internal-pdf-viewer. Plugin 1: Chrome PDF Viewer; Portable Document Format; internal-pdf-viewer. Plugin 2: Chromium PDF Viewer; Portable Document Format; internal-pdf-viewer. Plugin 3: Microsoft Edge PDF Viewer; Portable Document Format; internal-pdf-viewer. Plugin 4: WebKit built-in PDF; Portable Document Format; internal-pdf-viewer.
20 - Screen width	4.59 %	1536
21 - Screen height	4.18 %	864

Yes! You are unique among the 4108223 fingerprints in our entire dataset.

Smals
ICT for society

Local traces

- Many traces about activity on a computer
  - Browsing history
  - Cookies' content
  - Cache
  - Downloads
  - Logs
  - **DNS cache**
  - …

```
PS C:\Users\vab> ipconfig /displaydns

Windows IP Configuration
...
    www.smalsresearch.be
    ----------------------------------------
    Record Name . . . . . . : www.smalsresearch.be
    Record Type . . . . . . : 1
    Time To Live  . . . . . : 35421
    Data Length . . . . . . : 4
    Section . . . . . . . . : Answer
    A (Host) Record . . . : 185.22.109.12
```

- Can be sensitive if computer is seized, lost, hacked

Smals
ICT for society

Who can see what?

	ISP/Access point *	Website	Trackers	Other users
IP Client	User identity (if registered)	Approx geo	Approx geo	/
IP Destination	Website: sometimes Page: never	(na)	(na)	
Main cookies	/	Visitor tracking (on current website)	/	Activity history
3th party cookies	/	/	Visitor tracking (on all sites using the same tracker)	/
Fingerprinting	(na)	Visitor tracking (on current website)	Visitor tracking (on all sites using the same tracker)	/
Local traces	(na)	(na)	(na)	Activity history

* Assuming HTTPS

Smals
ICT for society

Why
was Tor created

- What to protect?
- **How to protect?**
- Is that enough?

How
does Tor work

What's
in there

Who's
active

Smals
ICT for society

HTTPS

- Almost unavoidable on modern browsers

- End-to-end encryption browser ← → web server

- Encrypt:

  - Content

  - HTTP headers

  - Cookies

  - URL (Domain name + path) → But DNS request was needed!

- Do not encrypt IP address (source/target)
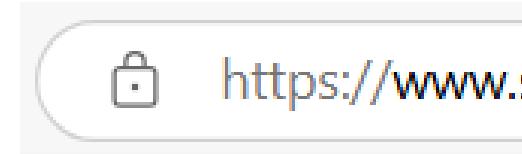
	ISP/Access point	Website	Trackers	Other users
Anonymity	/	/	/	/
Privacy	No access to content Limited domain knowledge	/	/	/

Smals
ICT for society

Private browsing

InPrivate browsing

You've gone Incognito

Firefox
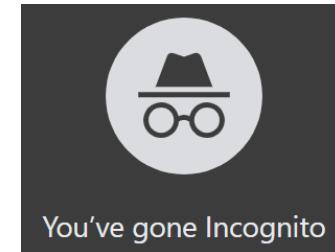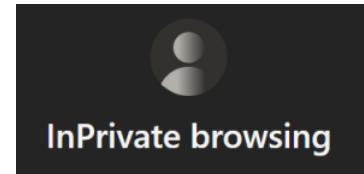
End of session: delete all cookies

⬇
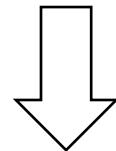
Block 3th party cookies

⬇
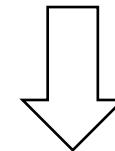
Delete cache, form data, browsing history
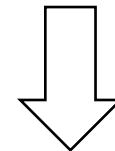
⬇

	ISP
Anonymity	/
Privacy	/

Do not:
- Mask IP address
- Impact ISP
- Impact some local traces (DNS cache…)
- Delete downloads

Smals
ICT for society

Virtual Private Network (VPN)

VPN server

ISP

www.smals.be

Encrypt:
- Content
- HTTP headers
- Cookies
- URL
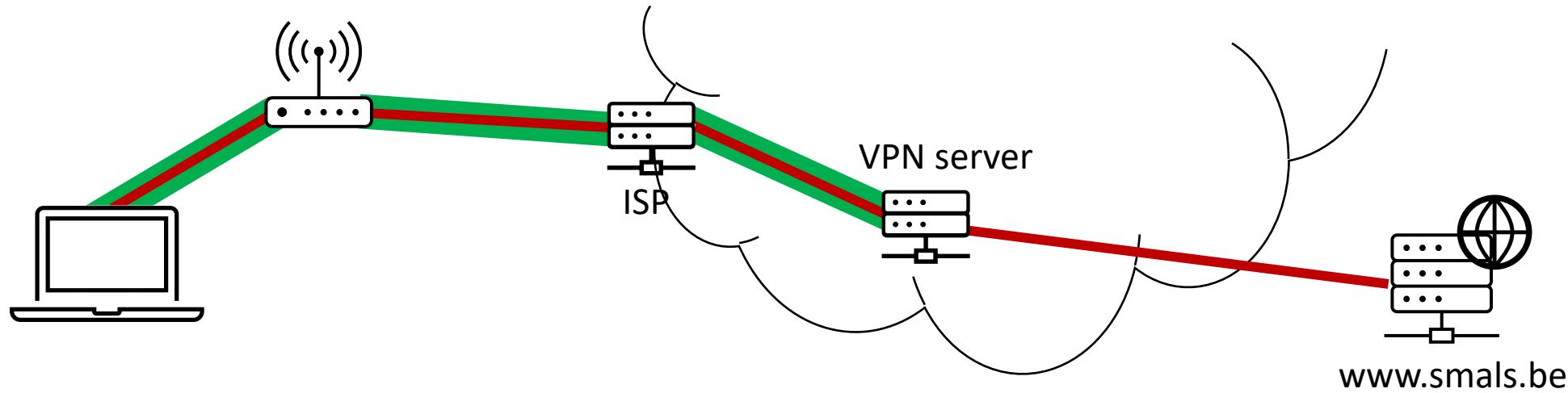
- ISP: ~~destination IP~~

- Target server: ~~source IP (geo)~~

Same as HTTPS!

Smals
ICT for society

Virtual Private Network (VPN)

- VPN usage: mainly a trust shift from ISP to VPN

- Useful if:
  - Untrustworthy ISP (abroad, public access point)
  - Need to bypass service or geo-blocking
  - In a corporate context

- Does not prevent HTTPS

- Does not block cookies

		ISP/Access point	Website	Trackers	Other users
	Anonymity	Can detect VPN usage	No access to IP or geo	No access to IP or geo	/
	Privacy	No more access to visited websites/services	/	/	/

Smals
ICT for society

Why
was Tor created

- What to protect?
- How to protect?
- **Is that enough?**

How
does Tor work

What's
in there

Who's
active

Smals
ICT for society

Is that enough?

- Have to trust someone (ISP/access point or VPN)

- With help of ISP or VPN, Law Enforcement can find a server or a user based on IP address & timestamp

- A lot of people need stronger protection:

Journalists

Dissidents
Activists
Whistleblowers

Travellers

Criminals!

Smals
ICT for society

Why
was Tor created

How
does Tor work

- Components
- Onion pealing
- Hidden services
- Tails

What's
in there

Who's
active

Smals
ICT for society

Tor: 3 components

Tor Network: +/- 8000 volunteer nodes acting as relays

Onion/Hidden services: « dark web servers »
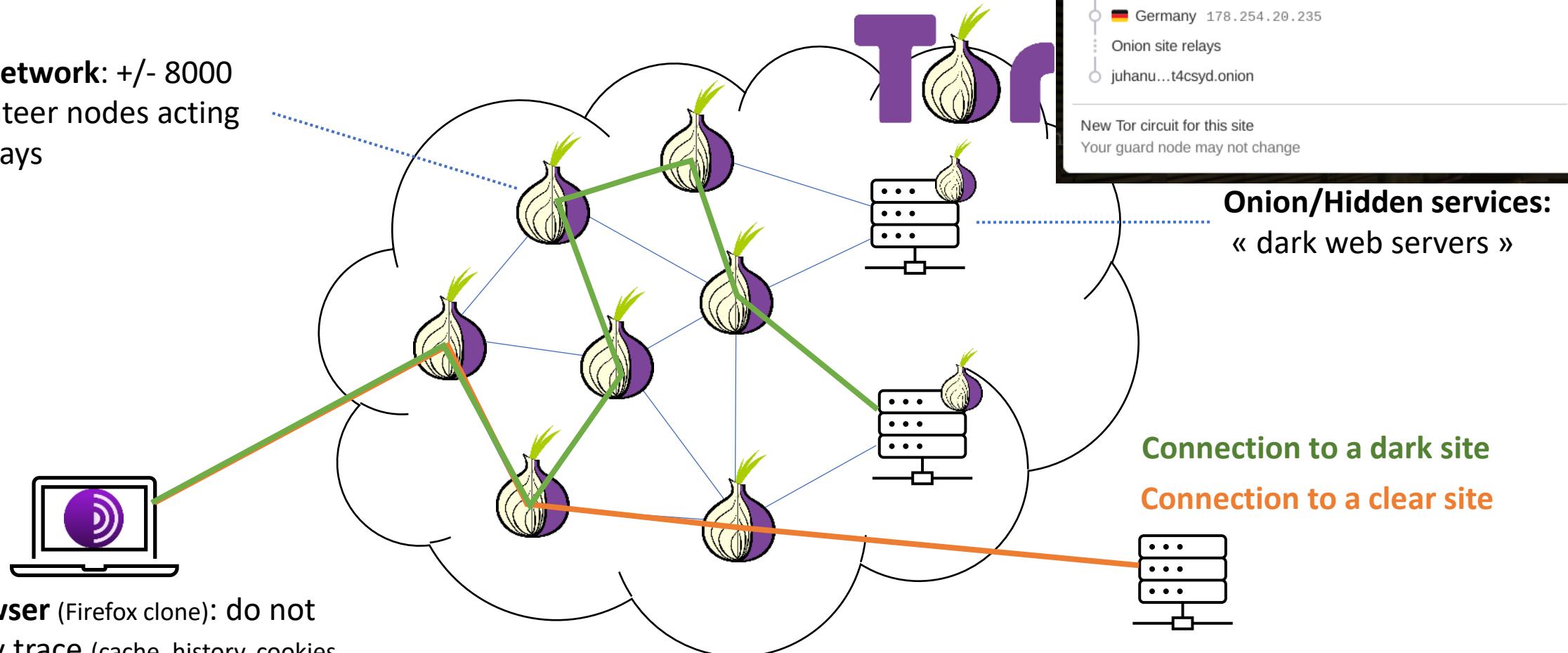
Tor browser (Firefox clone): do not keep any trace (cache, history, cookies, downloads, DNS…), limit JavaScript

Connection to a dark site

Connection to a clear site

juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.

Circuit for juhanu…t4csyd.onion

Tor Circuit

○ This browser
○ 🇳🇱 Netherlands (guard) 185.157.120.51
○ 🇫🇷 France 45.13.119.200, 2a10:4640:0:ff03::1
○ 🇩🇪 Germany 178.254.20.235
⋮ Onion site relays
○ juhanu…t4csyd.onion

New Tor circuit for this site
Your guard node may not change

- Dark net: network, protocols…
- Dark web: web content

Smals ICT for society

Tor: onion pealing

0110110
Dest: D

Next: C

Next: B

A

B

C

D

Smals
ICT for society
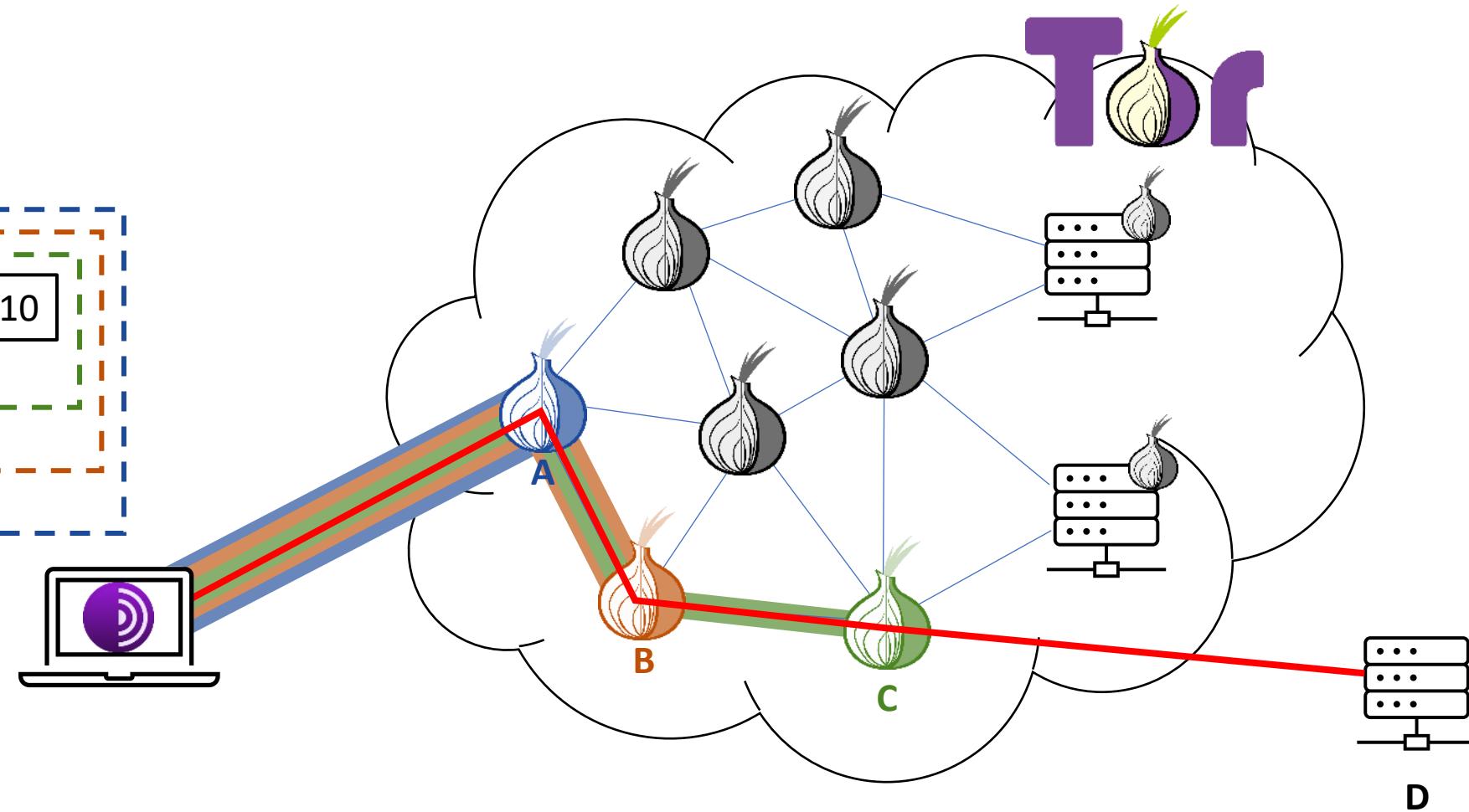
Tor: onion pealing

Tor: onion pealing

0110110
Dest: D
Next: C

Next: B

A

B

0110110
Dest: D

Next: C

C

D

Smals
ICT for society
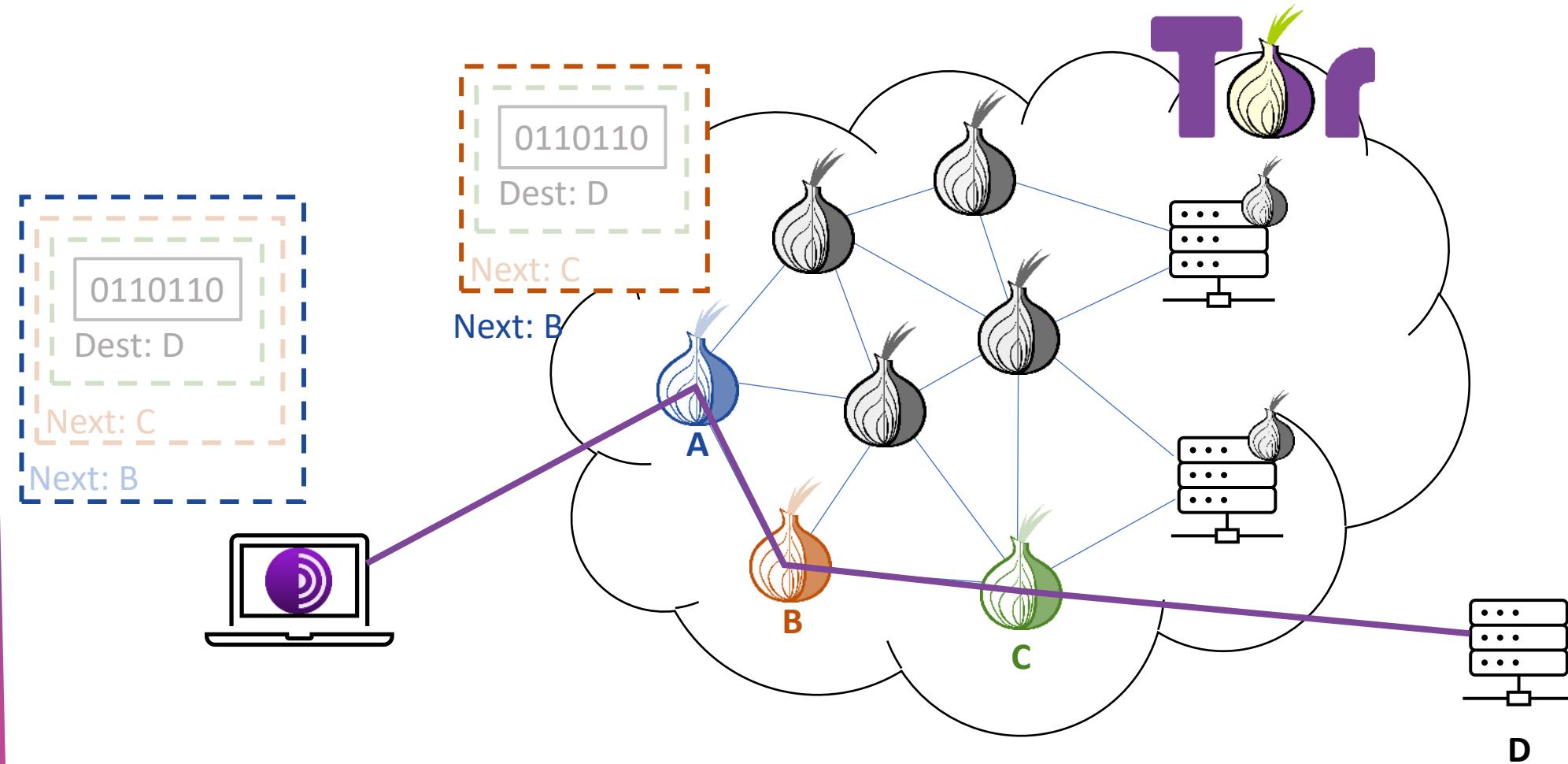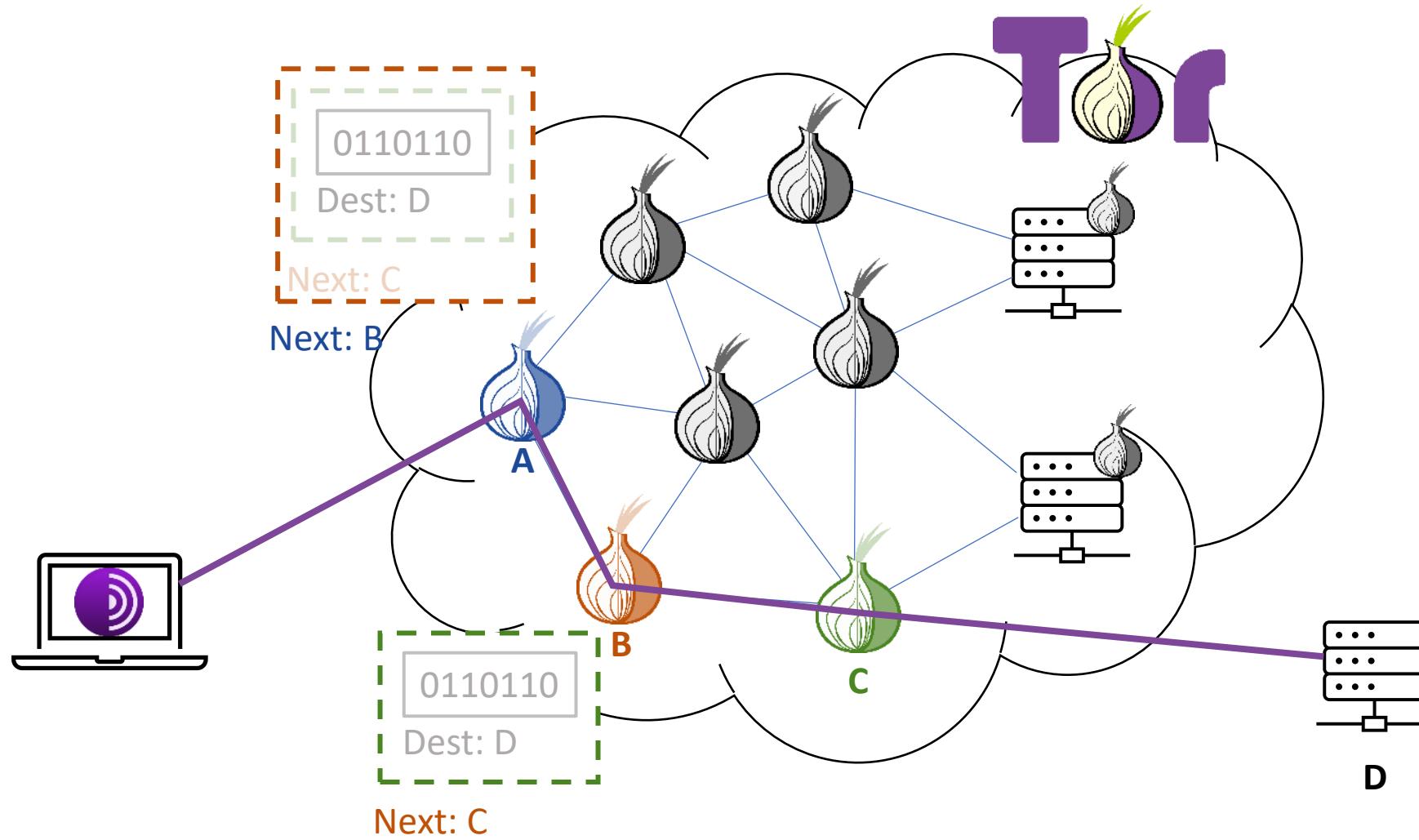
Tor: onion pealing

- Nobody knows the full path:
  - A → client, B
  - B → A, C
  - C → B, D
- Circuit changes every 10 minutes
- DNS request on exit relay (C)

- D does not know client IP
- Client still needs D IP

0110110
Dest: D

Next: C

0110110
Dest: D

A

B

C

D
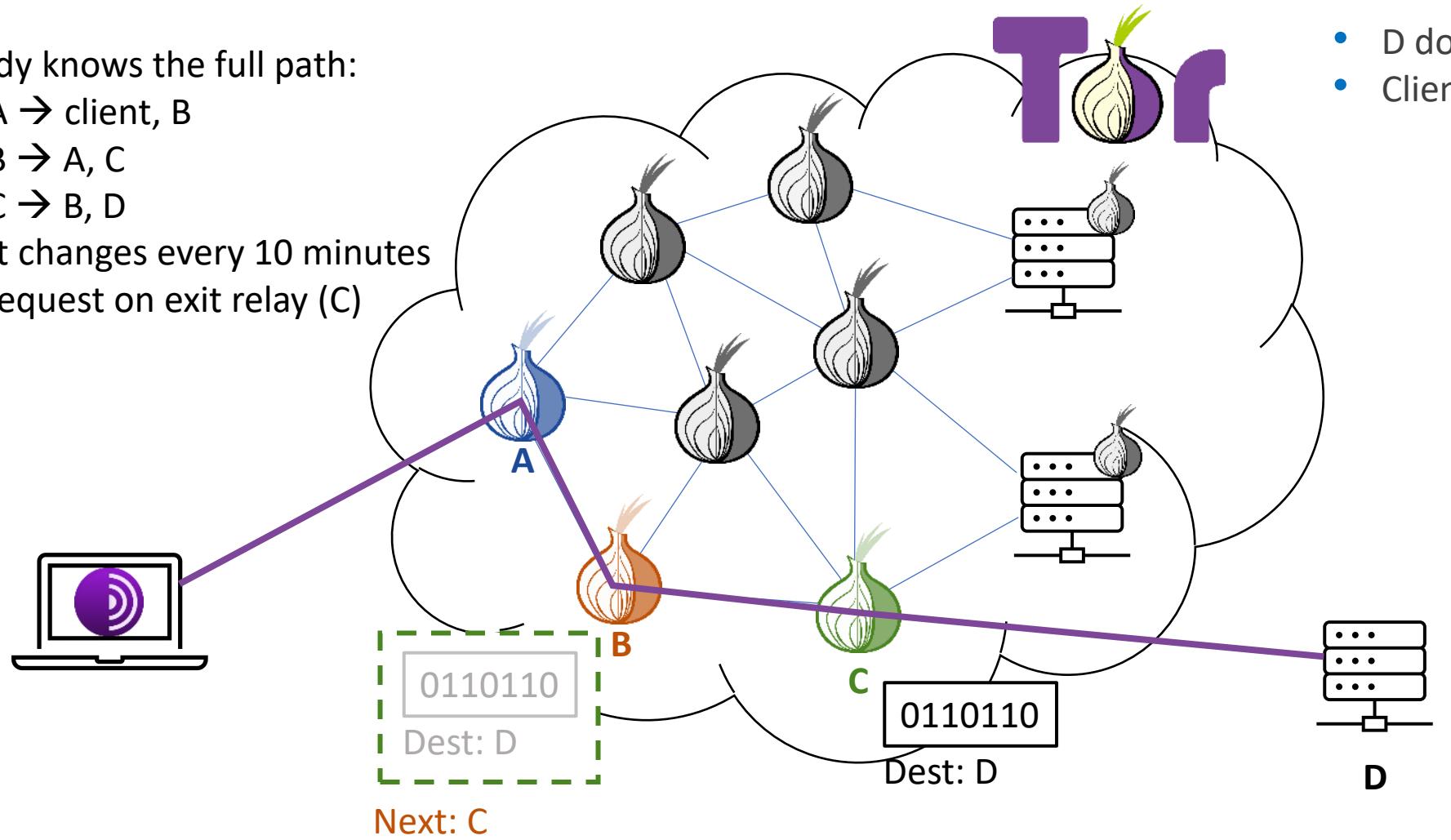
Tor: Hidden service

- Hidden service/Onion service: allow (web) server to hide as much as client
- Both client and server choose 3 relays and meet at a « rendezvous » point

Onion service URL: http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion
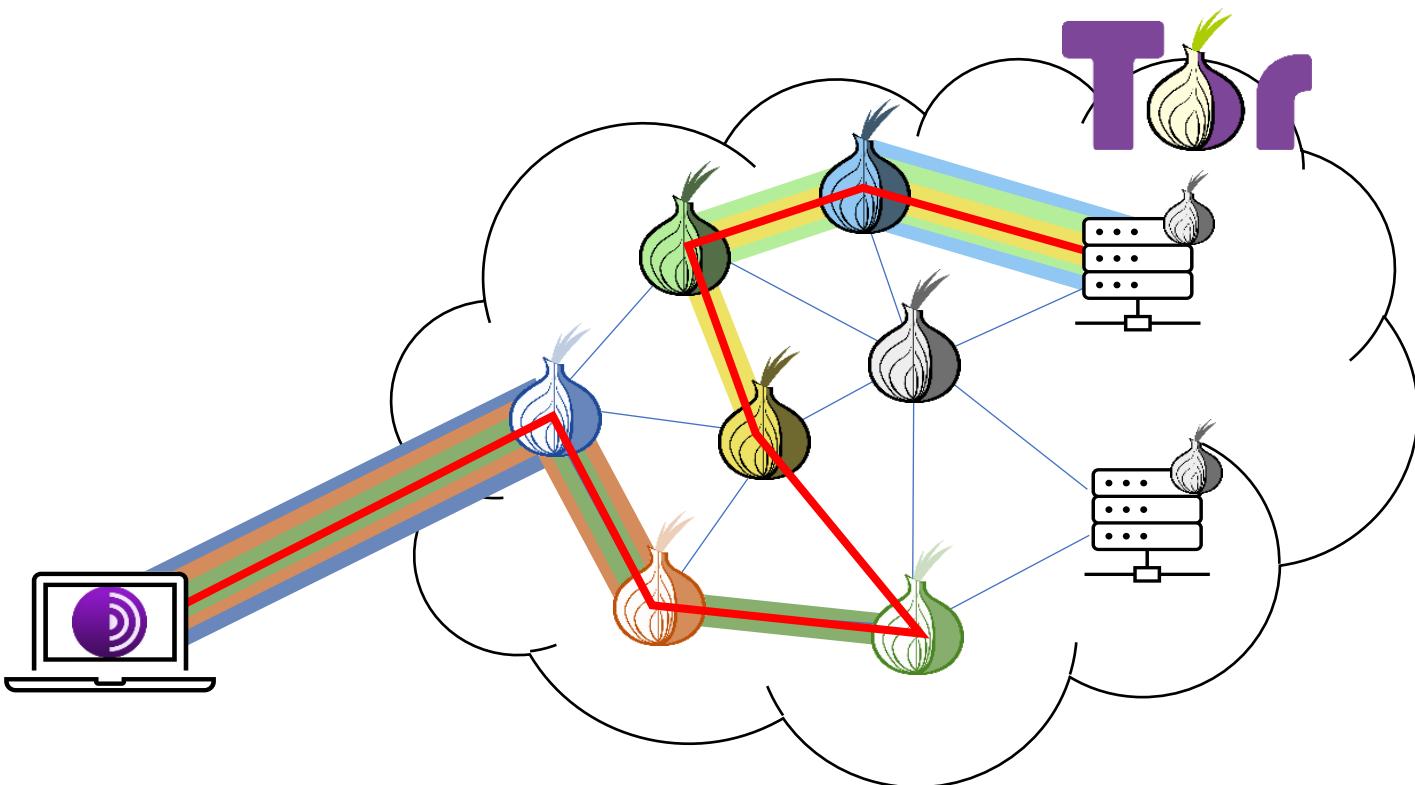
54 random characters = public key

Smals
ICT for society

Preventing fingerprinting

Attribute spoofing
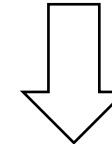
	Chrome	Tor
User agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36	Mozilla/5.0 (Windows; Win64; x64) Gecko/20100101 Firefox/128.0
Timezone	UTC+02:00	UTC-00:00
Content language	en,en-US;q=0.9,fr-FR;q=0.8,fr;q=0.7,nl;q=0.6	en-US,en;q=0.5
Screen resolution	1536 x 864	1400 x 800 (letterboxing 200 x 100)
List of fonts	Agency FB, Algerian, Arial, Arial Black, Arial Narrow, **And 158 others**	Arial, Arimo, Courier, Courier New, Helvetica, **And 27 others**
Canvas	Cwm fjordbank glyphs vext quiz, 😃 Cwm fjordbank glyphs vext quiz, 😃	
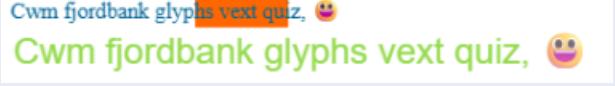
➜ Goal: making all Tor users look alike

Letterboxing size: 1000 × 800

Smals
ICT for society

Tails

- Tor weakness: OS it runs on!

- Cannot control OS traces ➔ indices that/when Tor ran might be easy to find

- Tails (https://tails.net) = Live OS, on a USB stick:

  - Can boot on (almost) any computer
  - No trace on that computer (main OS is not started, HD is not used)
  - No trace on the USB stick
  - Optional « persistent storage »

	ISP/Access point	Website	Trackers	Other users
Anonymity	Can detect Tor usage (unless bridge)	Can detect Tor No access to IP or geo	No access to IP or geo	Not any trace on computer
Privacy	No access to visited website/services	No access to history between sessions	No access to history	No access to history

Who can see what with Tails?

	ISP/Access point *	Website	Trackers	Other users
IP Client	~~User identity (if registered)~~	~~Approx geo~~	~~Approx geo~~	/
IP Destination	~~Website: sometimes Page: never~~	(na)	(na)	
Main cookies	/	~~Visitor tracking (on current website)~~	/	~~Activity history~~
3th party cookies	/	/	~~Visitor tracking (on all sites using the same tracker)~~	/
Fingerprinting	(na)	~~Visitor tracking (on current website)~~	~~Visitor tracking (on all sites using the same tracker)~~	/
Local traces	(na)	(na)	(na)	~~Activity history~~

* Assuming HTTPS

Smals
ICT for society

Required precaution

To stay anonymous, Tor users have to compartmentalise their online live!

- No email/bank account/phone number/… linkable to a real identity

- No payment with a identifiable card ➔ use Bitcoin, Monero…

- Delete metadata before sharing files

- Never go to same service without using Tor

Bomb alert at Harvard, 2013

- Author used a mail service (Guerilla Mail) from Tor (Tor output relay IP in the mail header)

- He was the only one connected to Tor (input relay) from the campus Wi-Fi!

Silk road founder (Ross W. Ulbricht, 2011-2013)

- Mentioned once « rossulbricht@gmail.com » on a crypto-money forum with « Altoid » pseudo

- Same pseudo was used on another DW forum, linked by FBI as a Silk Road

Smals
ICT for society

Why
was Tor created

How
does it work

What's
in there
- Entry points
- Markets
- Forums
- Leaks
- Activism

Who's
active

Smals
ICT for society

Tor: uncomfortable user experience

☹ Onion name very user-unfriendly

✂ Very high turn-over, dead links are everywhere

⇄ Erratic/hazardous browsing

🛡 Suspicion is the norm!
- Captcha very difficult to solve
- Queue to protect from DDoS

🐌 Very slow (relays, encryption…)

🥷 Most content is criminal (>< Initial goal: help to fight censorship)

⚙🧠 BUT: no technical skills needed!

THIS HIDDEN SITE HAS BEEN SEIZED

This hidden site and the criminal content have been seized by the Bavarian State Criminal Police Office on behalf of the Office of the Public Prosecutor General in Bamberg

Select all images containing...
(check following image)

Zoom: 1 x1.5 x2 x2.5

VERIFY

https://icons8.com

Smals
ICT for society
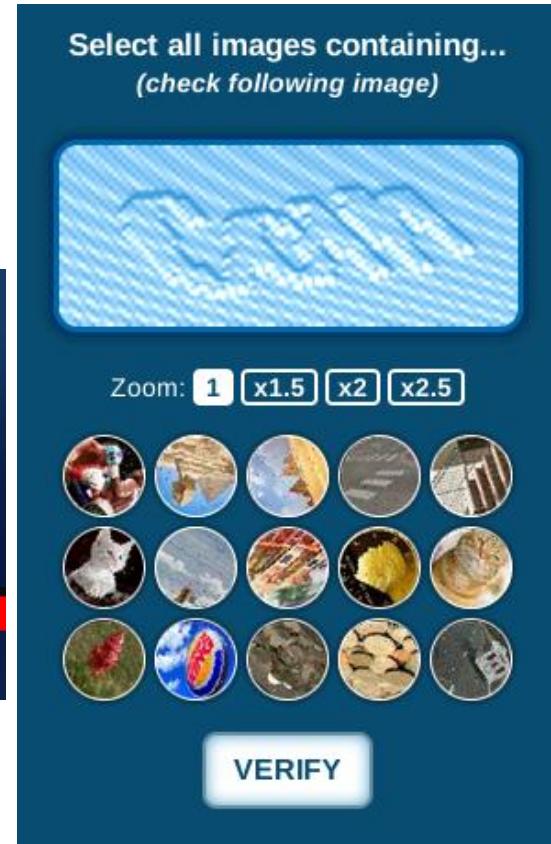
Tor: uncomfortable user experience
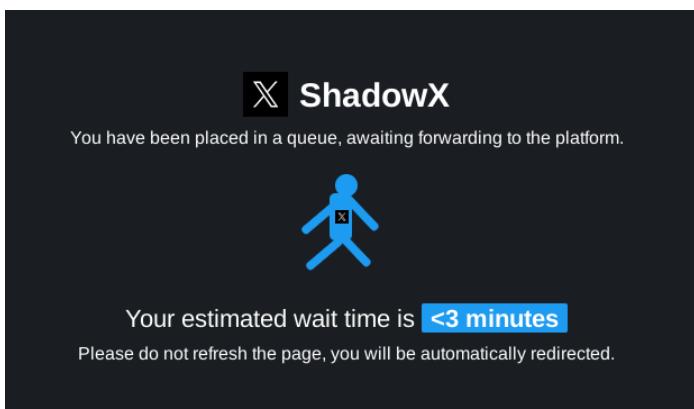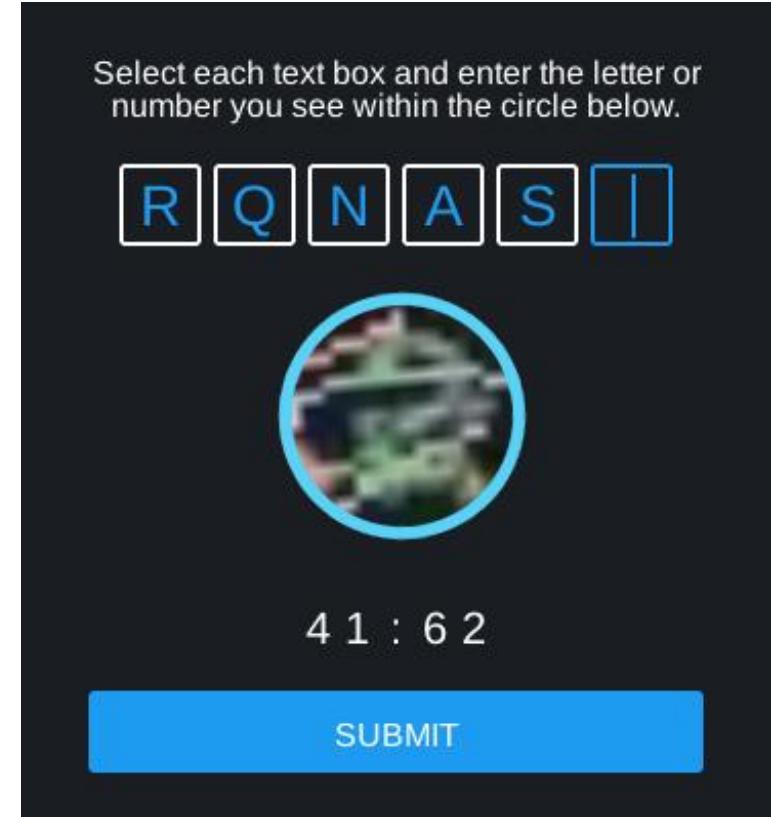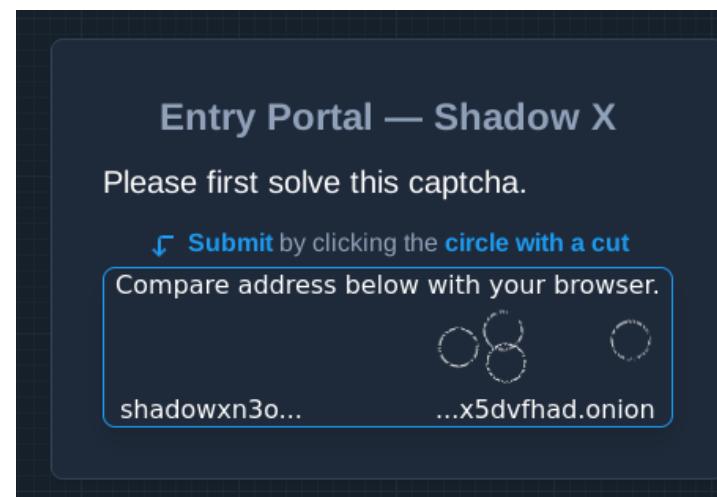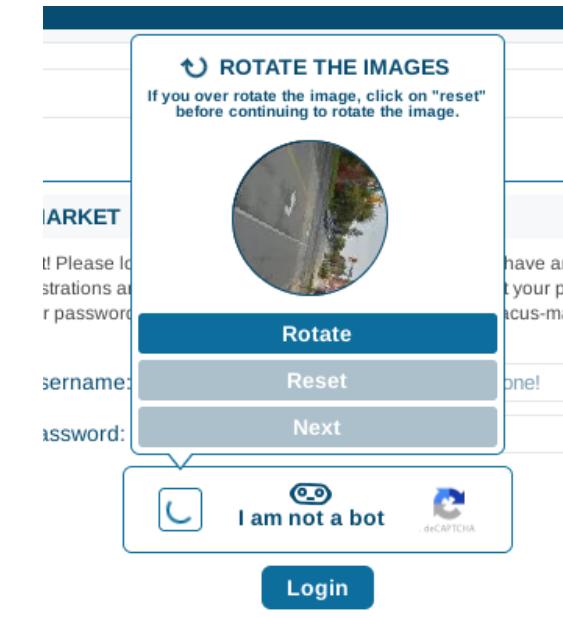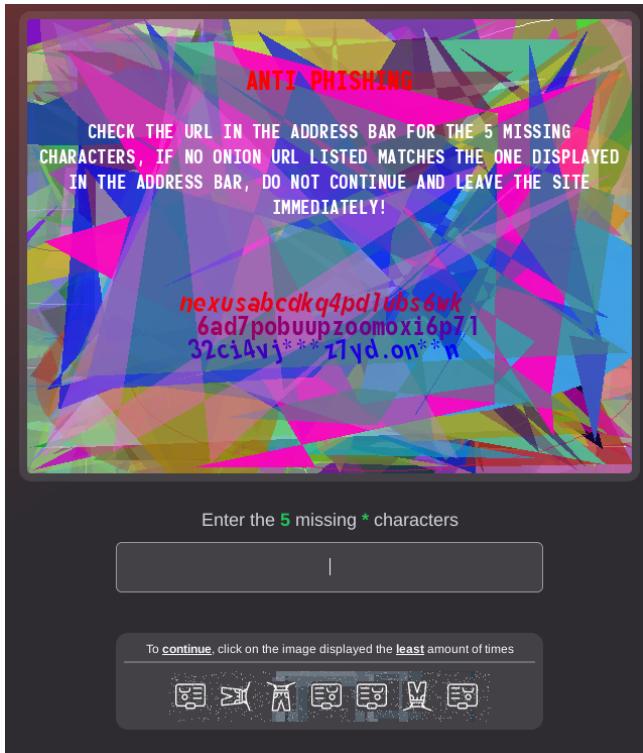
Entry points

Hidden wiki
List of links ("clear" or "dark web")

Search engines
Torch, Ahmia, Haystack…

thehidden2.wiki, thehidden-wiki.org, thehiddenwiki.org…

Smals
ICT for society

Markets

Markets

BitPharma

PRODUCTS   FAQS   REGISTER   LOGIN

Stimulants

Uncut cocaine and spe...
We are shipping from g...
We have the best stea...

Product	Price	Q...
1g pure Cocaine	75 EUR = 0.00081 ฿	
2g pure Cocaine	130 EUR = 0.00141 ฿	
5g pure Cocaine	250 EUR = 0.00271 ฿	
25g pure Cocaine	950 EUR = 0.01029 ฿	
10g pure Speed	90 EUR = 0.00097 ฿	
50g pure Speed	390 EUR = 0.00422 ฿	
100g pure Speed	650 EUR = 0.00704 ฿	
5g pure Crystal Meth	120 EUR = 0.00130 ฿	
10g pure Crystal Meth	200 EUR = 0.00217 ฿	
50g pure Crystal Meth	800 EUR = 0.00866 ฿	
50g MDMA Crystals	140 EUR = 0.00152 ฿	
100g MDMA Crystals	220 EUR = 0.00238 ฿	

Psychedelics

First class psychedelic...

EuCanna

Products   Info   Login   Register

Buds | Oil | Ointment | Supposit...

Soaps | CannaCaps | Edibles | S...

Medical Grade Cannabis Buds

We stock high quality hydroponic...
We are experienced professional...
quantity we produce.
This is why you will frequently se...
making the Rick Simpson Oil.

Product	Price	Quantity
3.5g Organic White Russian	42 EUR = 0.00045 ฿	1
7g Organic White Russian	70 EUR = 0.00076 ฿	1
14g Organic White Russian	120 EUR = 0.00130 ฿	1
50g Organic White Russian	295 EUR = 0.00319 ฿	1
3.5g Organic Chronic	42 EUR = 0.00045 ฿	1
7g Organic Chronic	70 EUR = 0.00076 ฿	1
14g Organic Chronic	120 EUR = 0.00130 ฿	1
50g Organic Chronic	295 EUR = 0.00319 ฿	1

Copyright© 20...

NLGrowers

Products   Login   Register   FAQs

Coffee Shop grade Cannabis

Finest organic cannabis grown by professional growers in the netherlands.
We double seal all packages for odorless delivery.
Shipping within 24 hours!

Product	Price	Quantity		
1g Original Haze	15 EUR = 0.00016 ฿	1	X	Buy now
5g Original Haze	65 EUR = 0.00070 ฿	1	X	Buy now
10g Original Haze	110 EUR = 0.00119 ฿	1	X	Buy now
50g Original Haze	550 EUR = 0.00596 ฿	1	X	Buy now
1g Bubblegum	10 EUR = 0.00011 ฿	1	X	Buy now
5g Bubblegum	45 EUR = 0.00049 ฿	1	X	Buy now
10g Bubblegum	85 EUR = 0.00092 ฿	1	X	Buy now
50g Bubblegum	450 EUR = 0.00487 ฿	1	X	Buy now
1g Jack Herer	14 EUR = 0.00015 ฿	1	X	Buy now
5g Jack Herer	60 EUR = 0.00065 ฿	1	X	Buy now
10g Jack Herer	110 EUR = 0.00119 ฿	1	X	Buy now
50g Jack Herer	480 EUR = 0.00520 ฿	1	X	Buy now
1g Chronic	9 EUR = 0.00010 ฿	1	X	Buy now
5g Chronic	40 EUR = 0.00043 ฿	1	X	Buy now
50g Chronic	350 EUR = 0.00379 ฿	1	X	Buy now
1g Banana Kush	11 EUR = 0.00012 ฿	1	X	Buy now
5g Banana Kush	45 EUR = 0.00049 ฿	1	X	Buy now

Markets

Forums

Data leaks (credentials)

ICT for society

Data leaks (full dumps)

- Ransomware: if ransom not paid → data published on Dark Web for free!

- Thousands of « full dumps » available on ransomware groups hidden websites

- Examples: listings (names, birthdates, phones, emails, payments…), factory plans, confidential contracts, DB content, HR docs, Ids…

> 50 public agencies (abroad)

Iraq, China, Thailand, Tonga, Vietnam, Indonesia, Ukraine, S. Korea, USA, Israel, France…

~ Some public Belgian agencies

SPW, Geraardsbergen, Jemeppe-sur-Sambre, FRS-FNRS, limburg.net, Maldegem

→ Offline

~ 110 private Belgian companies

Schools, IT, Pharma, Health, Bank, Insurance, Logistics…

→ Some still online
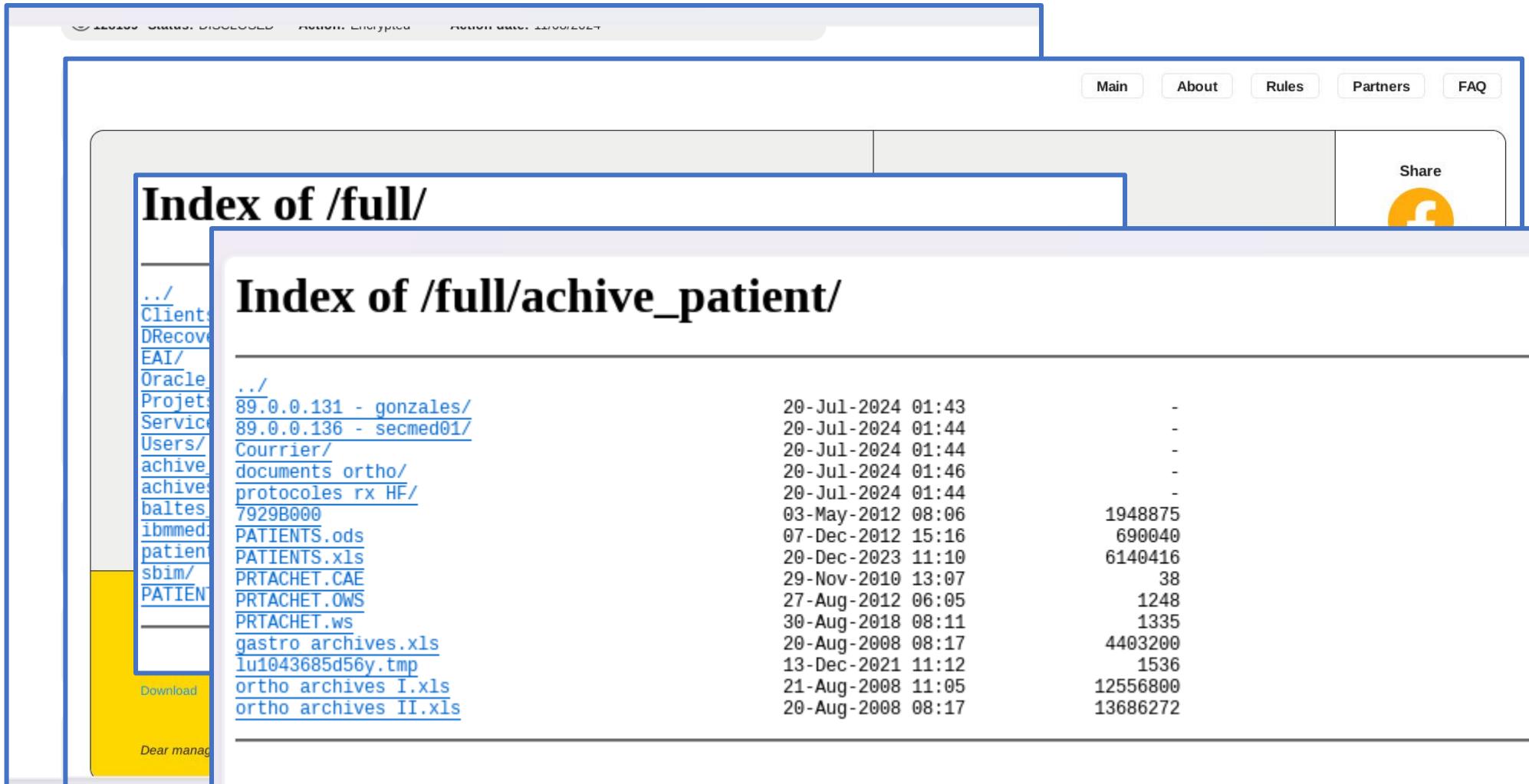
According www.ransomware.live

Smals
ICT for society

Data leaks (health example)

Index of /full/

../
Client[s]
DRecov[e]
EAI/
Oracle[_]
Projet[s]
Service[s]
Users/
achive[_]
achive[s]
baltes[_]
ibmmed[i]
patien[t]
sbim/
PATIEN[T]

Download

Dear manag[e]

Index of /full/achive_patient/

../		
89.0.0.131 - gonzales/	20-Jul-2024 01:43	-
89.0.0.136 - secmed01/	20-Jul-2024 01:44	-
Courrier/	20-Jul-2024 01:44	-
documents ortho/	20-Jul-2024 01:46	-
protocoles rx HF/	20-Jul-2024 01:44	-
7929B000	03-May-2012 08:06	1948875
PATIENTS.ods	07-Dec-2012 15:16	690040
PATIENTS.xls	20-Dec-2023 11:10	6140416
PRTACHET.CAE	29-Nov-2010 13:07	38
PRTACHET.OWS	27-Aug-2012 06:05	1248
PRTACHET.ws	30-Aug-2018 08:11	1335
gastro archives.xls	20-Aug-2008 08:17	4403200
lu1043685d56y.tmp	13-Dec-2021 11:12	1536
ortho archives I.xls	21-Aug-2008 11:05	12556800
ortho archives II.xls	20-Aug-2008 08:17	13686272

Main   About   Rules   Partners   FAQ

Share

Data leaks (health example)

Authorities/Whistleblowing

Media

Activism

Why
was Tor created

How
does it work

What's
in there

Who's
active

Smals
ICT for society

Who's active in Belgium

Sciensano (2020)
[N]ous analysons les risques engendrés par les nouvelles drogues (…) disponibles via Internet et le dark web. L'idée consiste (…) à acheter et analyser des échantillons.

SPF Finance (2019)
Des spécialistes en cybercriminalité (…) recherche des auteurs de crimes informatiques, tant sur le Web que sur le Dark Web

Myria (Federal Migration Center, 2023)
Pour détecter les cas de traite des êtres humains (…) les États membres ont mis en place (…) la surveillance d'internet (à la fois le web visible et le dark web)

AFMPS (2025)
Les réseaux sociaux et les marchés en ligne, tant sur l'internet que sur le dark web, continuent de jouer un rôle central dans le trafic de médicaments contrefaits.

SPF Finance (2017)
CDC « Cyber Intelligence Feeds »: l'analyse automatisées d'informations de sources ouvertes (dark web (…) compris)

Bpost (2020)
Le lancement d'un suivi proactif (…) de l'Internet (réseau public, deep web et dark web) afin de recevoir (…) des signaux sur les (…) attaques qui se préparent.

SPF Justice (2016)
Le dark web permet aussi à ses utilisateurs de (…) diffuser à grande échelle du matériel pédopornographique (…) et du matériel lié à l'exploitation sexuelle des enfants (…)
La vente de drogues via internet a augmenté. Des 491 sites (…) sur le 'darknet', 98% vendaient des drogues illicites.

SPF Santé publique (2024)
La valeur des données médicales serait (…) 10 à 20 fois plus élevée sur le dark web que les données financières. Plusieurs hôpitaux belges ont été victimes de cyberattaques ces derniers mois.

Police/FCCU (2017)
Nous sommes à l'affût des dernières tendances et des menaces (…). Le dark web en est un bon exemple, tout comme le hacking et les logiciels de type ransomware.

Mention ⇏ Action

Action ⇏ In/by Belgium

Smals
ICT for society

CCB/CERT

- At CCB, CERT (Cyber Emergency Response Team) actively monitors dark web (including creds/data leaks)

- To do ASAP: → Register (and update!) your org on https://atwork.safeonweb.be

- When a threat is detected: → CCB contacts victim, and provides support (tech/admin)

- If you detect any (cyber) incident: → Report on https://notif.safeonweb.be

- CCB won't:
  - Start any legal proceeding
  - Investigate/identify criminals → Contact police!

Police/FCCU

- Federal Computer Crime Unit

- Federal Police
  - Federal Judicial Police
    - DJSOC (Direction centrale de la lutte contre la criminalité grave et organisée / Centrale directie van de bestrijding van de zware en georganiseerde criminaliteit)
      - FCCU

- Missions:
  - Investigation about critical infrastructures attacks
  - IT Support for other DJSO units
  - Contact point for Europol

Should I go to Dark Web?

Should I go to Dark Web?

Is my mail on DW? — No: leakcheck.io, haveibeenpwned.com

Are my org credentials leaked? — No: intelx.io, flare.io, cybelangel.com (€)

Ransomware victim: what has leaked? — Yes... or ask experts

Want to monitor markets/forums — Install Tor/Tails!
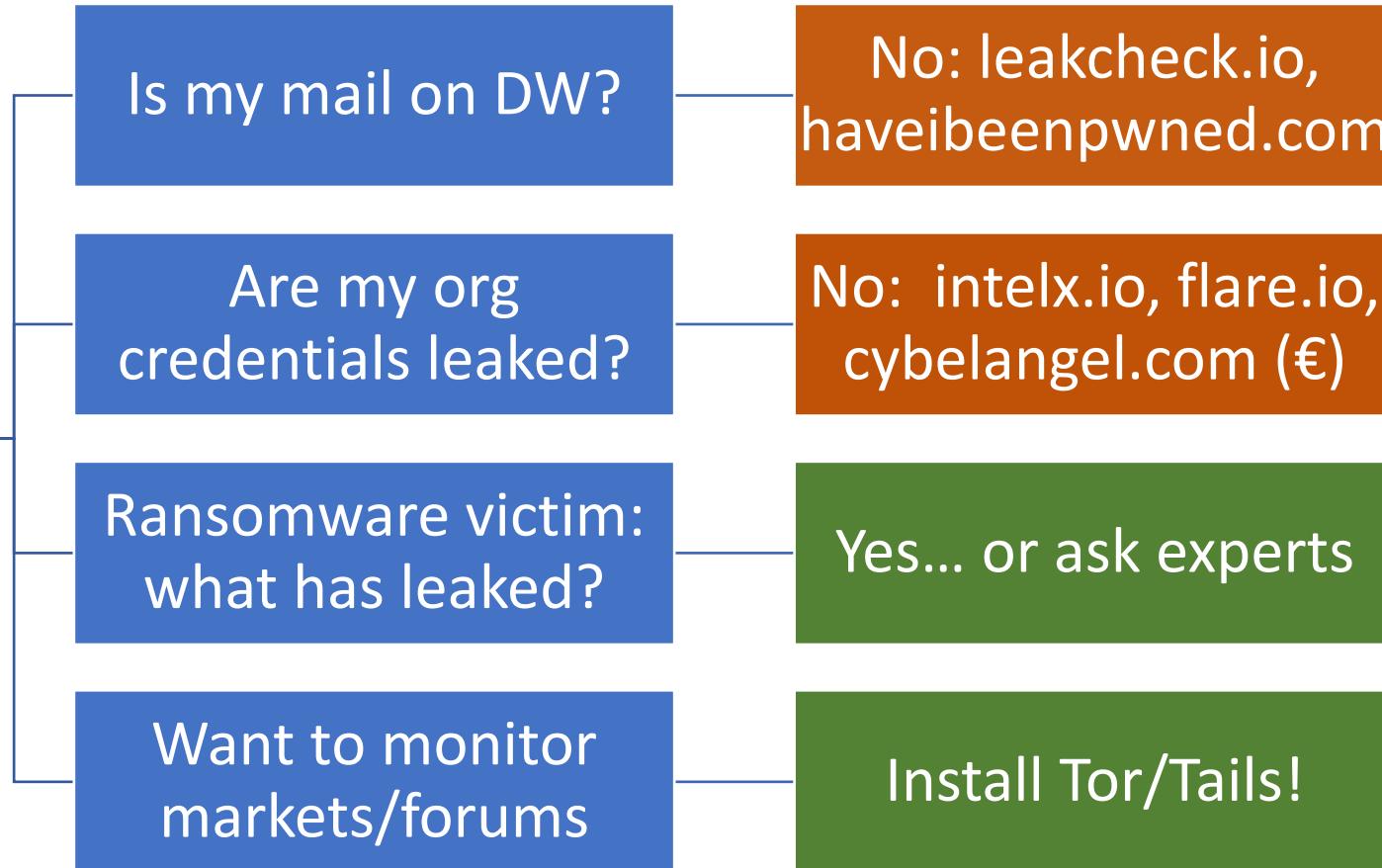
vandy.berten@_____   Check

Using Have I Been Pwned is subject to the terms of use

Email Breach History

Timeline of data breaches affecting your email address

2
Data Breaches

Oh no — pwned! This email address has been found in multiple data breaches. Review the details below to see where your data was exposed.

_Intelligence**X**

smals.be

Search

Advanced

📊 ▲ Found 527 Text Files, 153 Website HTMLs, 31 CSV Files, 8 Database Files, 7 Pastes, 5 Email Files, 2 Domains, 2 PDF Files, 1 Excel File

Smals
ICT for society

Legal comments

- Going to Dark Web/using Tor → Legal! (in Belgium)

- Buying illegal products/data → Illegal!

- No intention = No crime! Cannot commit an offence « by accident »

- Civil servants obliged to report offences

- Legal framework:
  - Investigation mandate?
  - Permission to create fake profile?
  - Permission to buy illegal products?

Smals
ICT for society

Threat or Opportunity?

Threat

- Credential leaks

- Full dump leaks

- Hacking tools

Opportunity

- Monitoring Market:
  - Drugs
  - Medicines
  - Counterfeit items, documents, money
- Fighting pedopornography/human trafficking
- Whistleblowing secure drop
- Securing exchanges with threatened partners

Smals
ICT for society

Conclusion (as a threat)

- Risk is high to be leaked

- Prepare your org!

- Don't stay alone! Contact CCB/FCCU

- Once it's there, it's forever…

Smals
ICT for society

Conclusion (as an opportunity)

- Tor is not only an hacker tool, Dark web is not only a crime zone!

- Several public services monitor it, but further exploration is possible

- Not difficult to go to Dark web, but poor UX

- Part of Dark web is even more hidden and can only be accessed « by trust »

- First exploration at very low cost: decommissioned machine, internet access (outside org network!!) … no software cost, only a few hours of manpower!

Smals
ICT for society

Management summary (1/2)

- Dark Web: part of the web requiring special software

- Tor: Browser + Network, by far the main « dark web/dark net »

- Onion service/Hidden service: « Dark website », only reachable using Tor browser

- No way to shutdown Tor network ; Almost impossible to find client or server IP/Owner

- Tor browser can be used to navigate on normal website, with a high level of anonymity

- Originally, Tor was build to protect citizens again censorship/repression in authoritarian regimes

- Today, most of its content seems to be illegal

- Most problematic content:
  - Drugs, Medicines
  - Hacking (credentials, tools)
  - Counterfeit items, documents, money
  - Pedopornography
  - Data leaks (phishing/ransomware result)

Smals
ICT for society

Management summary (2/2)

- Some public services already use/monitor Dark Web, but there is room for evolution

- What should public service do:
  - Consider if they should monitor some specific markets
  - Search for credential leaks from their members
  - If they are a ransomware victim, search for their data leaks

- Contact CCB/FCCU for support in case of incident/data leaks

- What Smals can further offer:
  - Ad hoc webinar, Tor tutorial/workshop: yes
  - First introduction to content for a specific field: depends
  - Help to buy monitoring solution: to be discussed
  - Monitoring, recovery in case of hacking, data deletion: no (→ CCB)

Smals
ICT for society

Thank you for your attention!

Feedback / questions / discussion welcome!

Please share your feedback with us!

✉ vandy.berten@smals.be

🌐 www.smalsresearch.be
www.smals.be

◆ Smals
ICT for society