

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



Innovation with
new technologies



Consultancy
& expertise



Internal & external
knowledge transfer



Support for
going live



Decathlon victime d'une fuite de données

Il a ainsi injecté des informations comme des identifiants et mots de passe, qu'il a trouvés 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

Une affaire de pédocriminalité horrifique un village

interpellé par la police néerlandaise après que des vidéos de la fillette ont été retrouvées sur le **Darknet**

La Libre
BELGIQUE

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

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**."

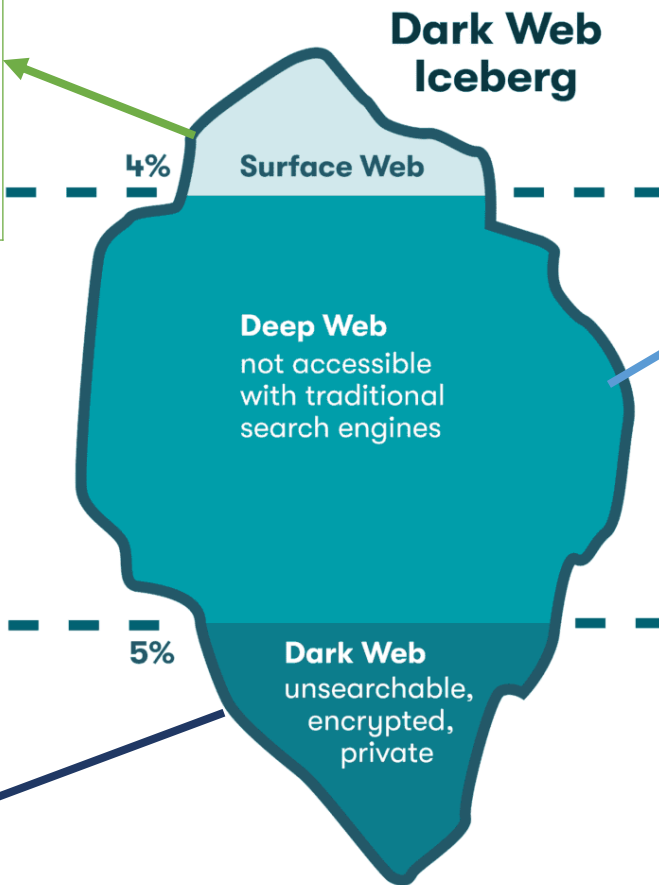
Het Nieuwsblad

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.rtbef.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...




Why
was Tor created

How
does Tor work

Technical part 

What's
in there

Who's
active

Business part 



Why

was Tor created

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

How

does Tor work

What's

in there

Who's

active



Why

was Tor created

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

How

does Tor work

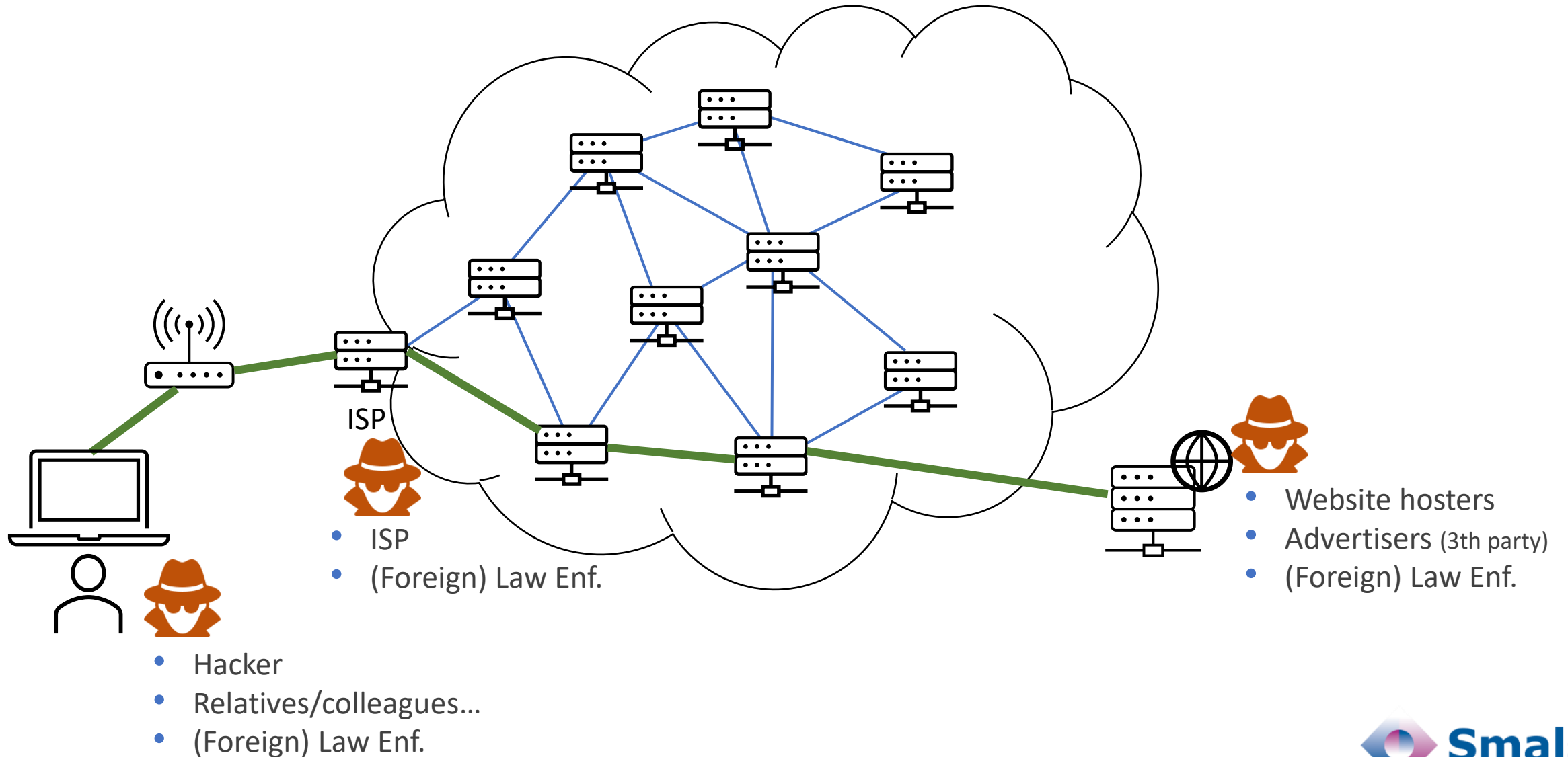
What's

in there

Who's

active

Who can observe you?



Anonymity vs privacy



Anonymity: preserve **who** you are

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

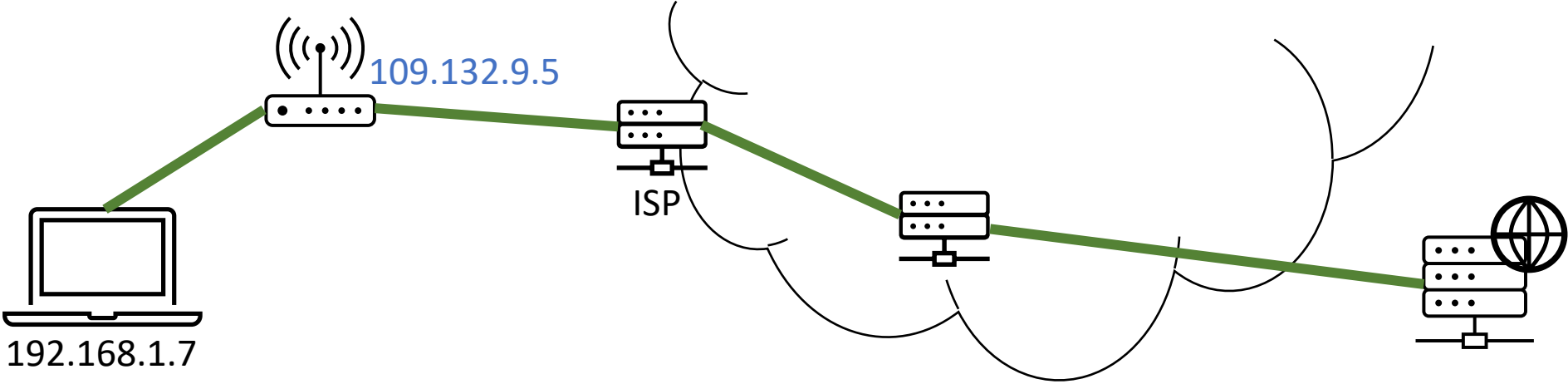


Privacy: protect **what** you do

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



Client IP address



IP address is:

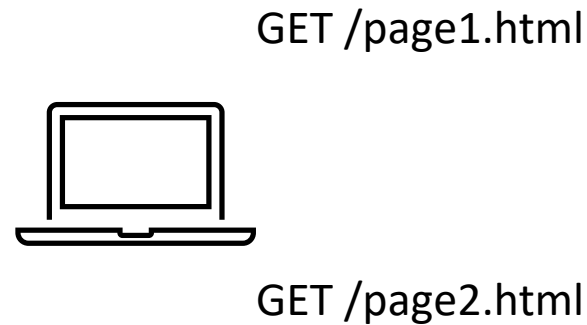
- Shared
- Dynamic
- Not itinerant resistant

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

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



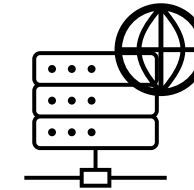
Cookies



```
<html>...  
</html>
```



```
<html>...  
</html>
```



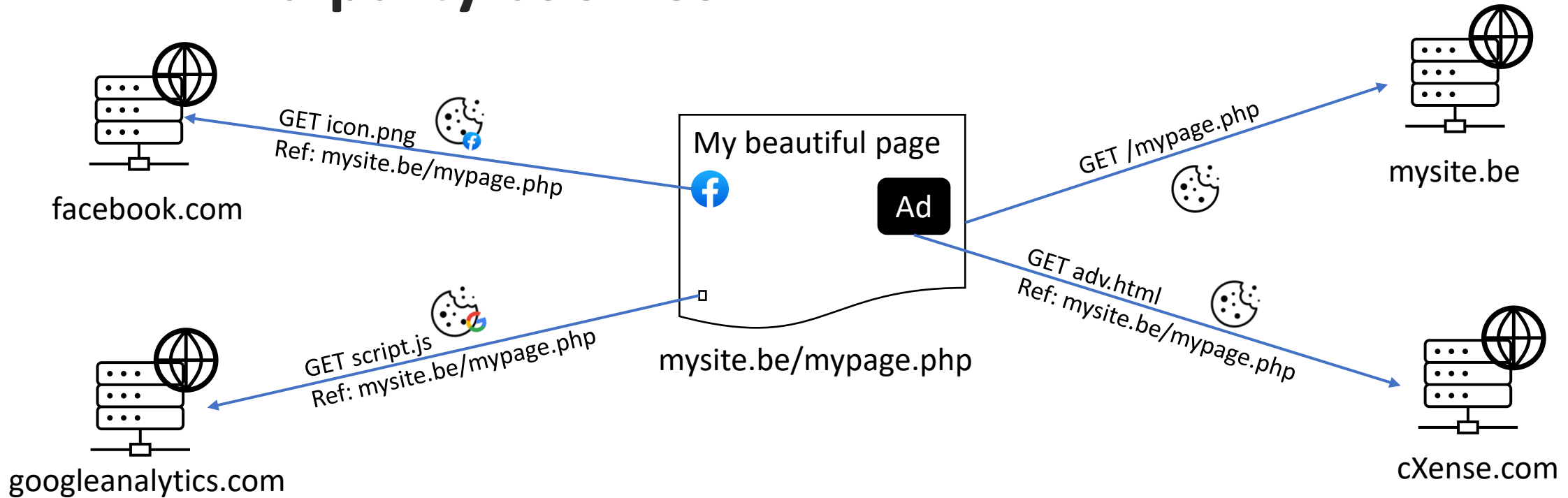
www.smals.be

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



Third party cookies



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...)



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

<https://amiunique.org/fingerprint>

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



Local traces

- Many traces about activity on a computer
 - Browsing history
 - Cookies' content
 - Cache
 - Downloads
 - Logs
 - **DNS cache**
 - ...
- Can be sensitive if computer is seized, lost, hacked

```
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
```

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
3 th 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



Why

was Tor created

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

How

does Tor work

What's

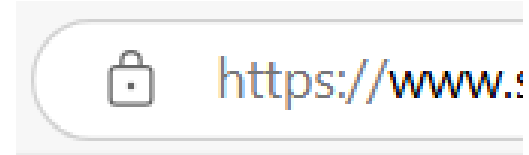
in there



Who's

active

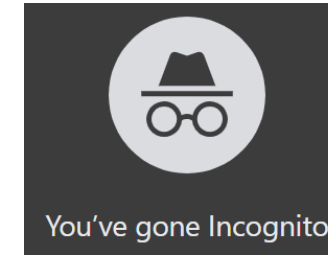
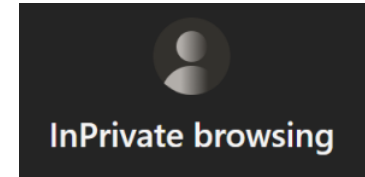
HTTPS

- Almost unavoidable on modern browsers
- End-to-end encryption browser \leftarrow \rightarrow web server
- Encrypt:
 - Content
 - HTTP headers
 - Cookies
 - URL (Domain name + path) \rightarrow But DNS request was needed!
- Do not encrypt IP address (source/target)

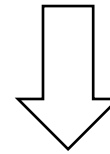


	ISP/Access point	Website	Trackers	Other users
 Anonymity	/	/	/	/
 Privacy	No access to content Limited domain knowledge	/	/	/

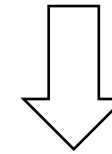
Private browsing



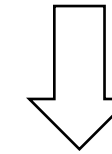
End of session:
delete all cookies





Block 3th party cookies



Delete cache, form
data, browsing history



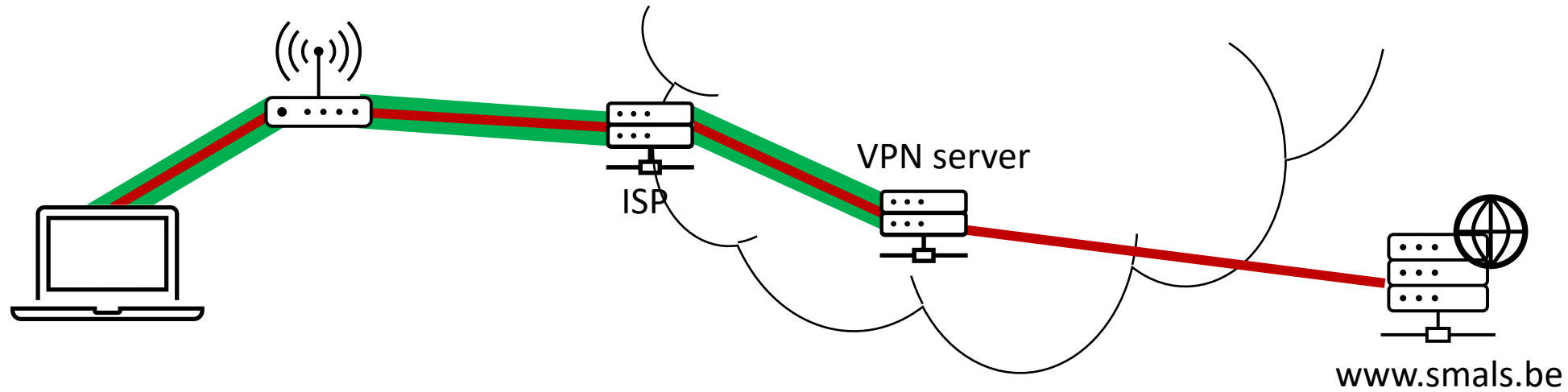
	ISP
 Anonymity	/
 Privacy	/

Do not:

- Mask IP address
- Impact ISP
- Impact some local traces (DNS cache...)
- Delete downloads



Virtual Private Network (VPN)



- ISP: ~~destination IP~~

Encrypt:



- Content
- HTTP headers
- Cookies
- URL

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

Same as HTTPS!

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	/	/	/



Why

was Tor created

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

How

does Tor work

What's

in there

Who's

active

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!



Why
was Tor created

How
does Tor work

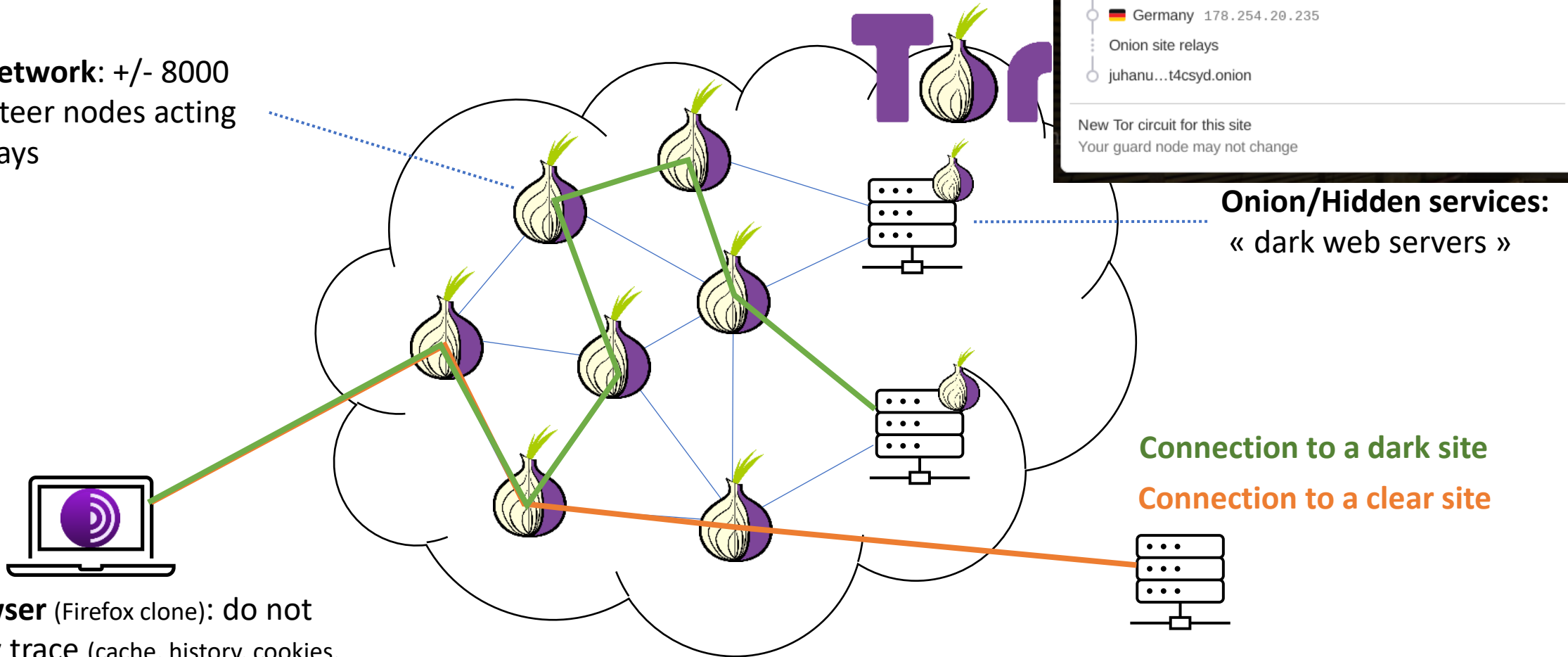
- Components
- Onion peeling
- Hidden services
- Tails

What's
in there

Who's
active

Tor: 3 components

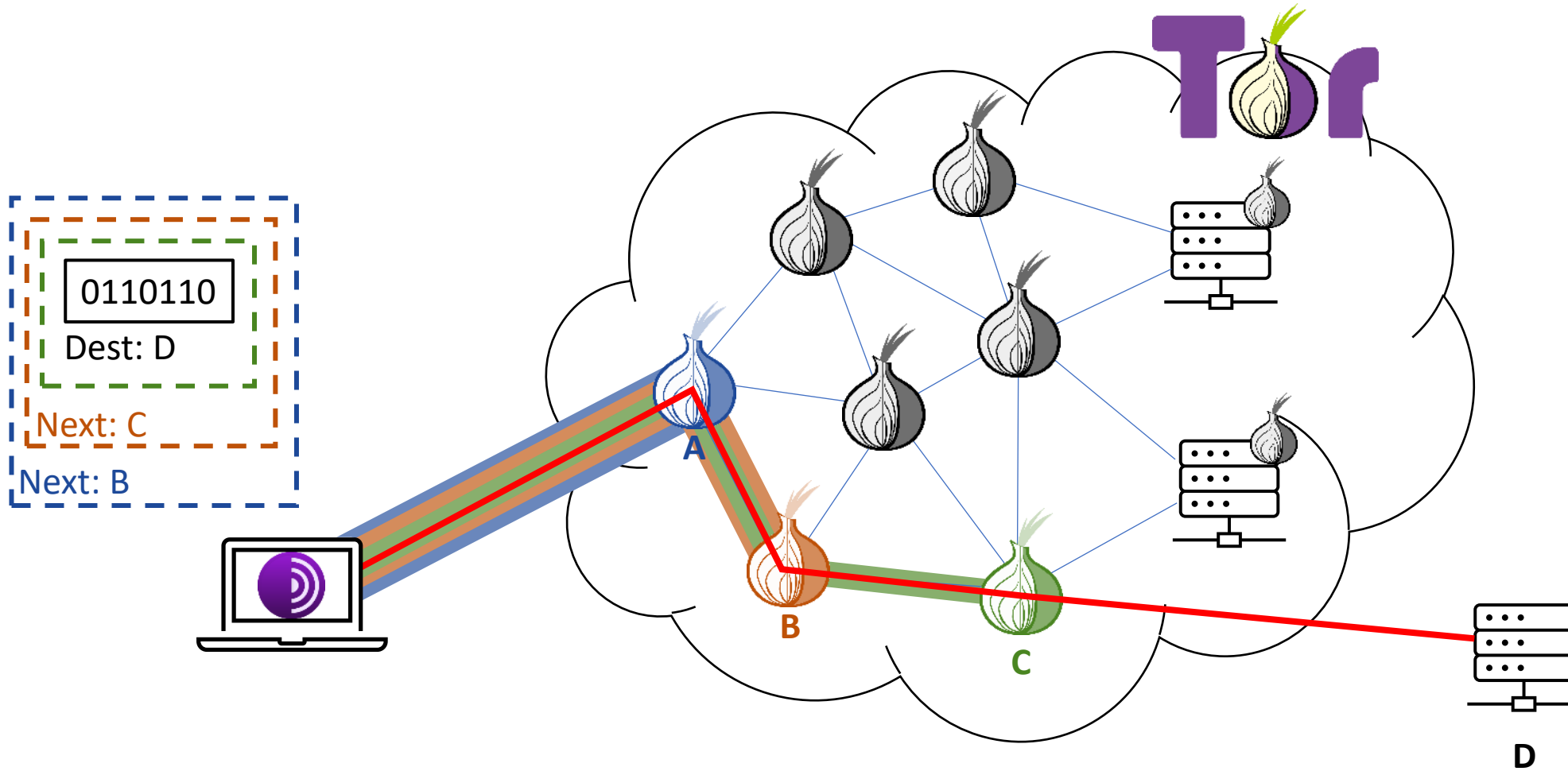
Tor Network: +/- 8000 volunteer nodes acting as relays



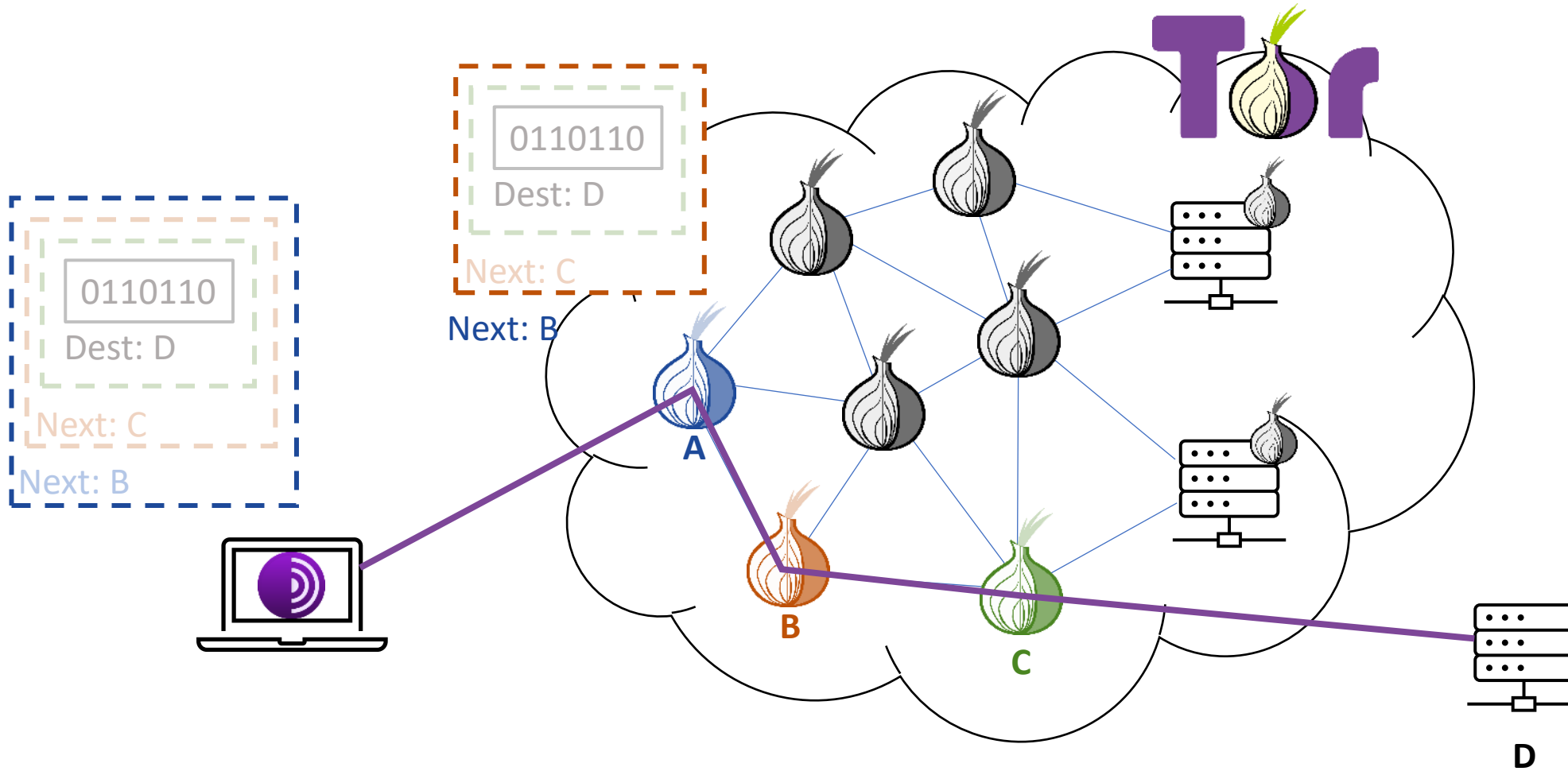
Tor browser (Firefox clone): do not keep any trace (cache, history, cookies, downloads, DNS...), limit JavaScript

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

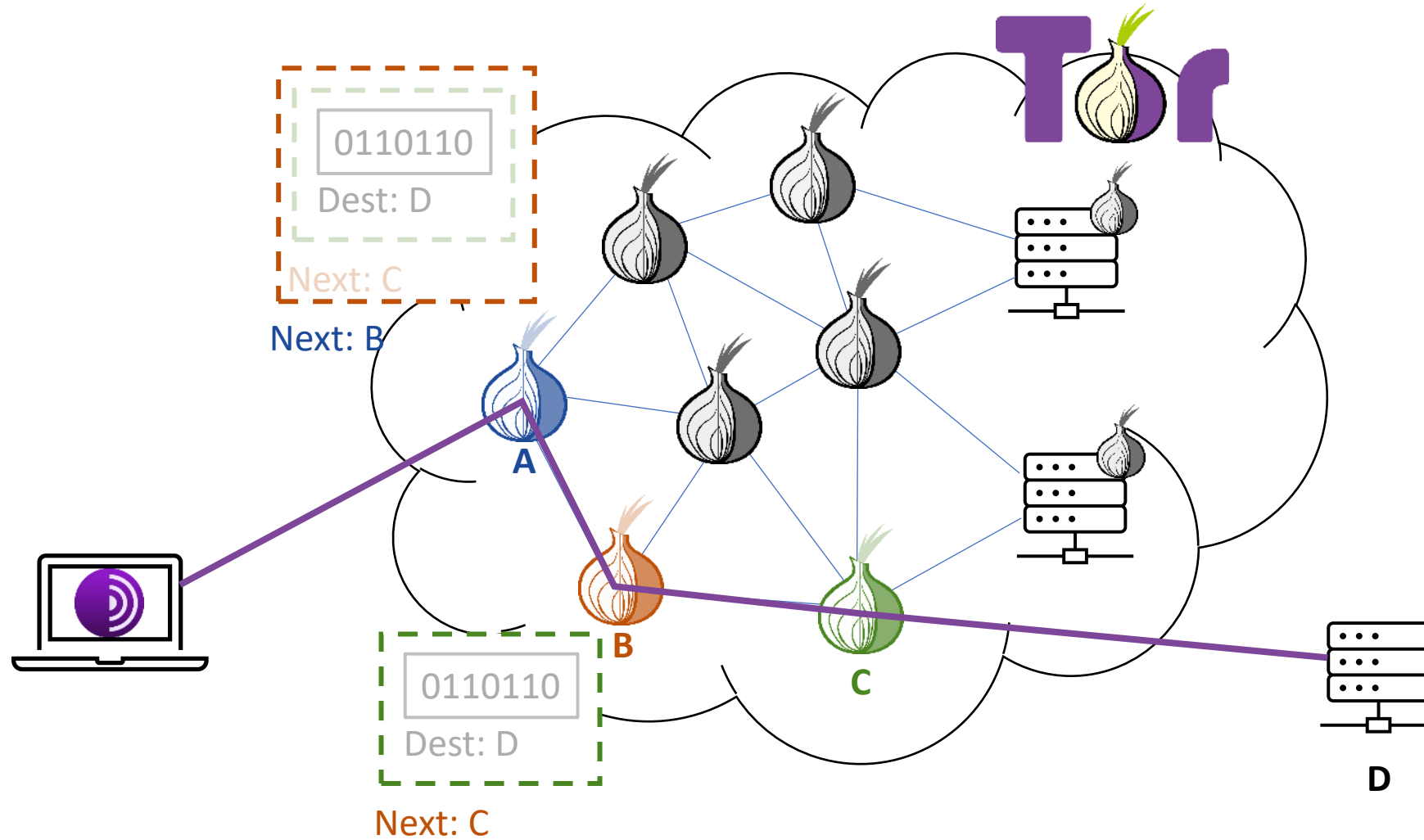
Tor: onion peeling



Tor: onion peeling

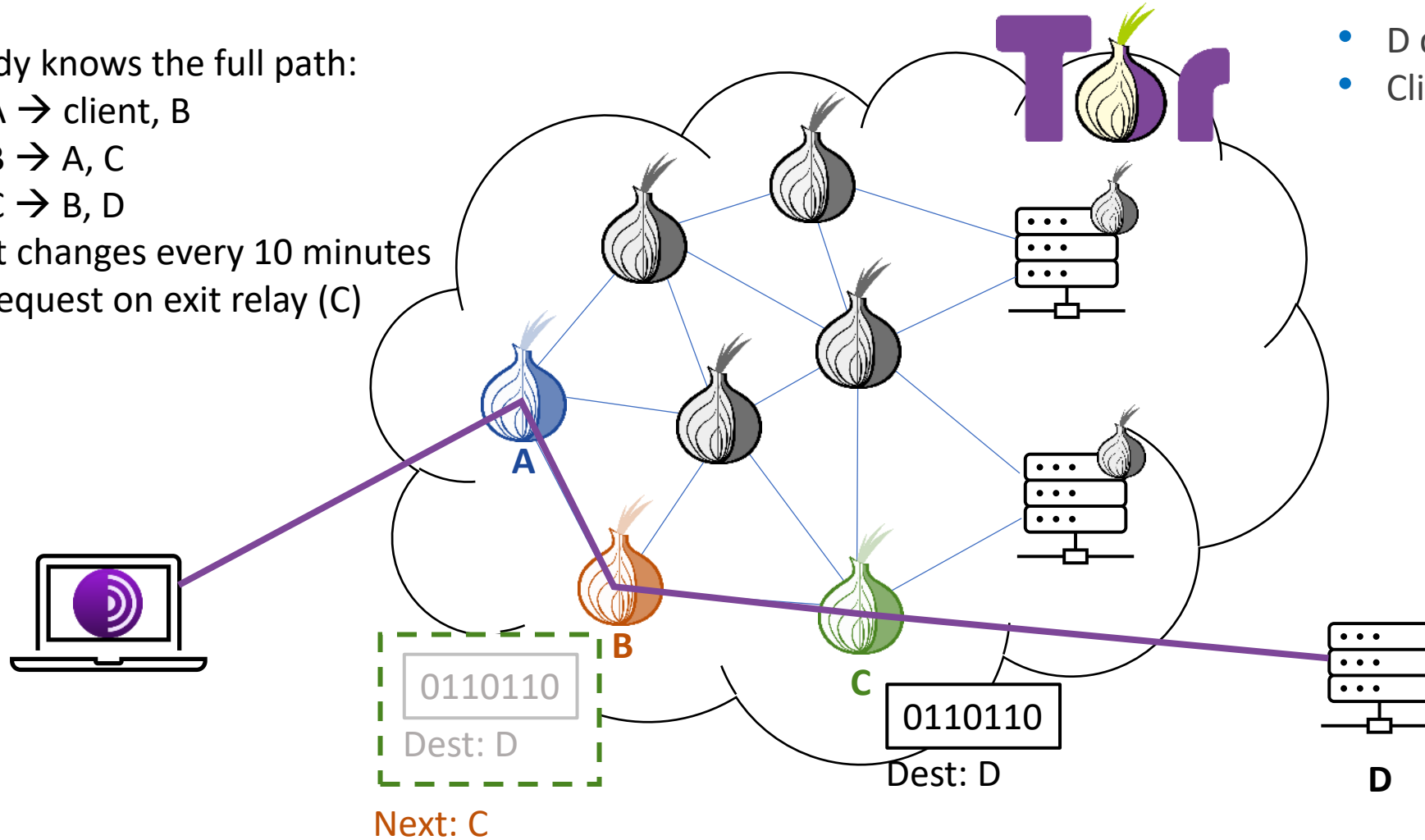


Tor: onion peeling



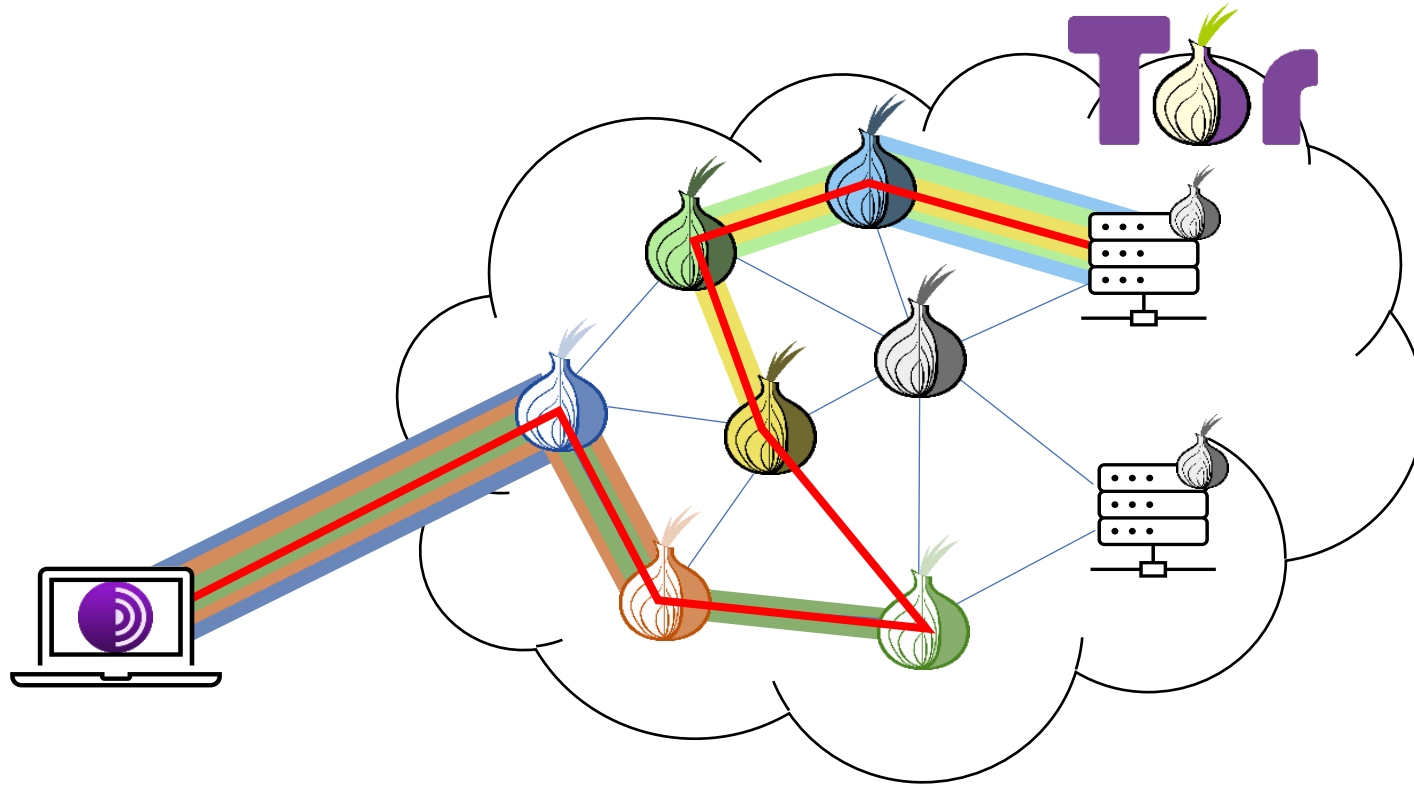
Tor: onion peeling

- 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

Tor: Hidden service



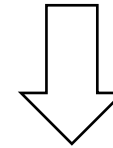
- Hidden service/Onion service: allow (web) server to hide as much as client
- Both client and server choose 3 relays and meet at a « rendezvous » point



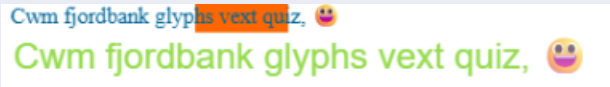

Onion service URL: <http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion>

54 random characters = public key

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		



➔ Goal: making all Tor users look alike

Letterboxing size: 1000 x 800

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
3 th 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

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



Why
was Tor created

How
does it work

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

Who's
active

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!



<https://icons8.com>

Tor: uncomfortable user experience

ANTI PHISHING

CHECK THE URL IN THE ADDRESS BAR FOR THE 5 MISSING CHARACTERS, IF NO ONION URL LISTED MATCHES THE ONE DISPLAYED IN THE ADDRESS BAR, DO NOT CONTINUE AND LEAVE THE SITE IMMEDIATELY!

nexusabcdkq4pd1ubs6wk
6ad7pobuupzoomoxi6p71
32ci4vj**71qd.on**

Enter the 5 missing * characters

To continue, click on the image displayed the least amount of times

ROTATE THE IMAGES

If you over rotate the image, click on "reset" before continuing to rotate the image.

Rotate

Reset

Next

I am not a bot

Login

Select each text box and enter the letter or number you see within the circle below.

R Q N A S I

4 1 : 6 2

SUBMIT

ShadowX

You have been placed in a queue, awaiting forwarding to the platform.

Your estimated wait time is **<3 minutes**

Please do not refresh the page, you will be automatically redirected.

Entry Portal — Shadow X

Please first solve this captcha.

Submit by clicking the circle with a cut

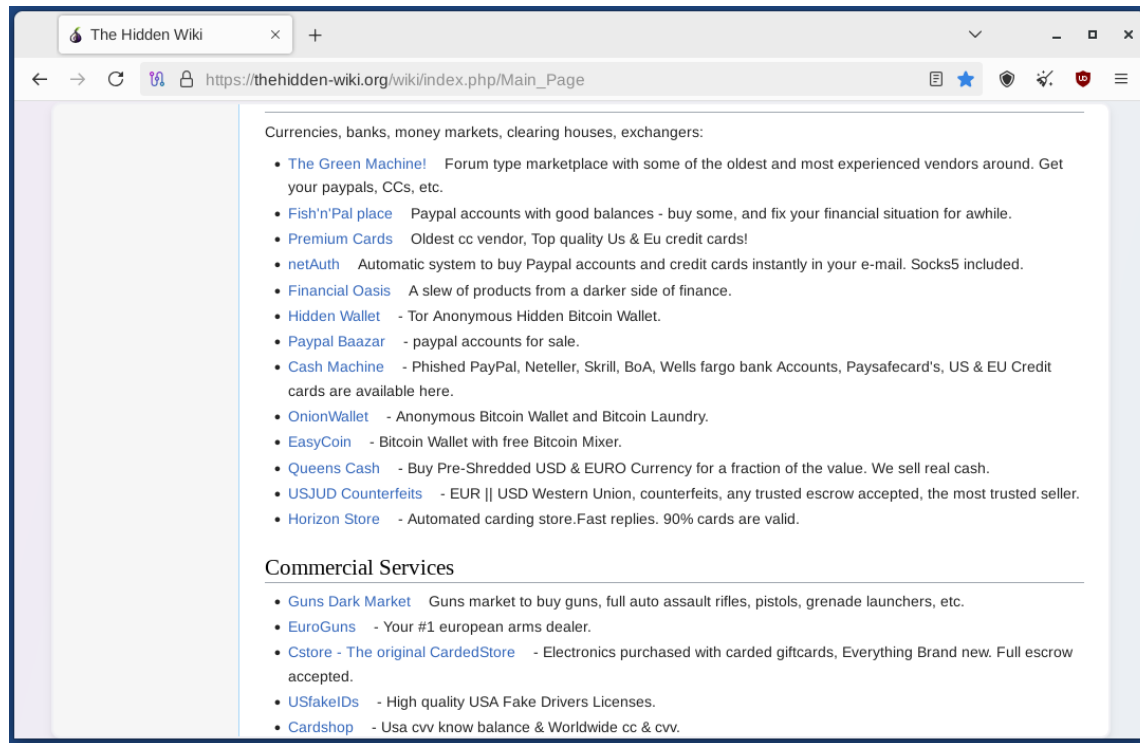
Compare address below with your browser.

shadowxn3o... ...x5dvfhad.onion

Entry points

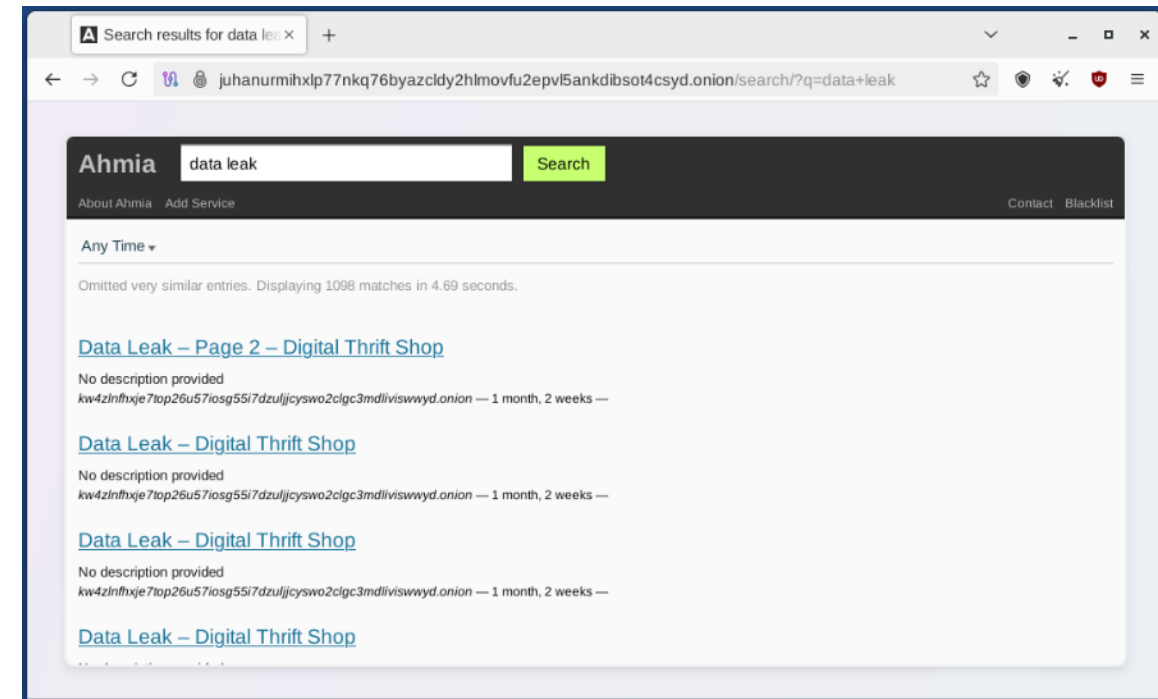
Hidden wiki

List of links (“clear” or “dark web”)



Search engines

Torch, Ahmia, Haystack...



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

Markets

SHADOWX Forum Market Search English Sign in Create an Account

NEXUS NEXT GENERATION MARKET HOME MY ORDERS BECOME A VENDOR WALLET Monero accepted here

SEARCH RESULTS

Relevance

Search

Related Categories


- Vicodin
- Potency Enhancers
- Simvastatin
- Lisinopril
- Levothyroxine
- Azithromycin
- Metformin Lipitor
- Pregabalin
- Amlodipine
- Other Prescription Drugs

Product	Quantity	Price	Source	Ships to
PREGABALIN 300MG UK NDD	15 Pill	€ 19.6	@martell (20,328 98%)	United Kingdom
	30 Pill	€ 28.82		
	60 Pill	€ 40.35		
Viagra Sildenafil AmaroX 25mg BOXED	1 Piece	€ 11.53	@NextGeneration (252,843 99%)	United Kingdom
	2 Piece	€ 20.75		
Cialis Tadalafil 1x Pill 100mg	1 Pill	€ 7	@NarcoTikker (5 100%)	Worldwide
	5 Pill	€ 30		
	10 Pill	€ 50		
	30 Pill	€ 120		
SUPER VIGA DELAY CREAM 1piece = 100mg Lidocain	7 Tab	€ 35	@NarcoTikker (5 100%)	Worldwide
	14 Tab	€ 60		
	21 Tab	€ 80		

Listing Feedback: ★★★★★ Views: 1708 | Sales: 389 Listing Feedback: ★★★★★ Views: 1708 | Sales: 389


Source: rakoostore (547|0) truegenerics (54|3861)

Markets



PRODUCTS FAQS REGISTER LOGIN

Stimulants




Uncut cocaine and speed
We are shipping from
We have the best stea

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

Psychedelics

First class psychedel




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 see
making the Rick Simpson Oil.

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

Products Login Register FAQs

NLGrowers

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

Markets

The screenshot displays a dark web marketplace interface. At the top, there is a navigation bar with categories: FIREARMS, AMMO, GUN ACCESSORIES, CLONED CARDS, and DOCUMENTS. Below this, a secondary navigation bar lists: ASSASSIN, KIDNAPPING, ARSON SERVICE, and ASSAULT SERVICES. A message prompt says "Message our NULL account :- @tornetwork".

The main content area is titled "HOME / ID CARDS" and shows "Showing 1-12 of 14 results" with a "Default sorting" dropdown. The marketplace logo is "NEXUS NEXT GENERATION MARKET". Navigation links include HOME, MY ORDERS, BECOME A VENDOR, and a WALLET icon.

Below the navigation, there are filters for "CATEGORIES" and "PHYSICAL MODE" (set to "Change"). A search bar contains the text "What do you need?".

The section "PRODUCTS FROM THE CATEGORY" is active, with a breadcrumb trail: Digital >> Fraud >> CVV & Cards.

Five product listings are visible:

- Carding Groupchat (200 Members) (Starter Pack) 10 CC Shop Links...**
Price: 39.99 USD / item
Seller: TaxEvader (271|1432)
- USA SNIFFED VISA DB BUSINESS \$5k in - 1 Card ordered = 1 free**
Price: 15.00 USD / item
Seller: Tuts4Ever (1226|4707)
- Anonymous Prepaid Debit Cards - \$150 for \$3500 loaded credit**
Price: 150.00 USD / item
Seller: Trio (546|333)
- [VISA SNIFFED] BOA DEB BUSINESS OVER \$5K BALANCE**
Price: 15.00 USD / item
Seller: Tuts4Ever (1226|4707)
- Dumps 201 TR1&TR2 \$5000+ PIN**
Price: 20.00 USD / item
Seller: slipperypete (1241|5837)

Forums

[Accueil](#) » [L'Arène](#) » [Je vends du contenu pédophile](#)

Pages : 1 [Répondre](#)

15-04-2025 22:36:18 #1

mrt J'ai plusieurs photos et vidéos d'une fille de 13 ans qui m'a envoyé beaucoup de nudes si intéressée contacter moi @proton.me

 [frontpage](#) [all](#) [dread](#)



[/d/coke](#)

[Wiki/Guides Index](#) [!!!RULES!!!](#) [Review/Image Posting Guide](#) [Vendor Flair Application](#)

▲ 1 Cocaine prices are crashing in almost all of Europe!
▼ by /u/DrugMahal · 4 weeks ago in /d/coke

Despite the multiple big European busts in cocaine trafficking world, with latest two famous seizures in Portugal [a submarine with 1.6 tonnes] and France [Dunkirk port 10 Tonnes].

In cities like Rotterdam and Antwerp a kilogram of cocaine is selling less than 18000 Euro and registered a price of 15000 Euro in some cases.

Data leaks (credentials)

terena	.com:Adip	@
simonc	L.fr:Mago	
majorc	ail.com:C	
salam.	otmail.co	1@*
alial:	ok.com:Al	
ghenav	l@outlook	ova
housse	l.com:Hal	
florer	L.com:Rob	
mark1:	com:xs.Ma	
jahma	Devilrays	
star.c	L.co.uk:W	
iem_l.	allstadt.	ein
birigi:	@mv-hall	sikve
sshoc	no-barbin	8
darsi:	nempata.c	g123
sandra	@mv-hall	sikve
huaice	veiwoduzu	

HelloOfHackers - Hacking Forum

Discuss Guides **Leaks** Breaches Marketplace Cracking/Accounts Hell Updates

9	@CHECKMATELOGS NEW DAILY ULP 06-05	Stealer Logs	May 6, 2025
10	22.000.000+ [URL-LOGIN-PASS] MILLION LINES	Stealer Logs	May 7, 2025
11	100K NEW VIP ULP By @CHECKMATELOGS	Stealer Logs	May 4, 2025
12	03-05-25 PREMIUM ULP BY @CHECKMATELOGS	Stealer Logs	May 3, 2025
13	26.000.000+ [URL-LOGIN-PASS] MILLION LINES	Stealer Logs	May 5, 2025
14	45k PREMIUM ULP USA	Stealer Logs	May 1, 2025
15	41K Full valid ULP Mix By @CHECKMATELOGS 30.04	Stealer Logs	Apr 30, 2025
16	29-4-2025 ULP UP-TG @CHECKMATELOGS	Stealer Logs	Apr 29, 2025
17	@CHECKMATELOGS - FRESH 64993 LINES 28.04.2025	Stealer Logs	Apr 28, 2025

NEXUS NEXT GENERATION MARKET

HOME MY ORDERS BECOME A VENDOR WALLET User

CATEGORIES PHYSICAL MODE Change Q What do you need? Search

PRODUCTS FROM THE CATEGORY Digital > Accounts

<p>PAYPAL \$50000 + [FULL GUIDE] - Verified Account CC included + CVV and S...</p> <p>CardMart (1058 5011)</p> <p>19.00 USD / item</p>	<p>2016 Facebook [Verified By Email] [Market Place Feature] [Ready To Use]</p> <p>SeriousSells (31 0)</p> <p>36.00 USD / item</p>	<p>EUROPE - 145k ireland combolist</p> <p>CyberGhost (672 749)</p> <p>15.00 USD / item</p>	<p>FB Fresh Account (Manually Created) Verified by email. Sex can ...</p> <p>SeriousSells (31 0)</p> <p>39.00 USD / item</p>	<p>ACCOUNT Secumd.org bank login + BALANCE</p> <p>GermanBorn (164 0)</p> <p>118.00 USD / item</p>	<p>Badlinkvr.com VR Porn Account Warranty</p> <p>enjoymyaccounts (403 11582)</p> <p>8.00 USD / item</p>
--	---	--	--	---	---

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



Data leaks (health example)

Index of /full/

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	

Download

Dear manag

Data leaks (health example)

2	NO	1	F	G	I	K	N	O	R	S	U	AG	BN	EB
		NAAM	VOORNAAM	GEBDA	TI	ADRES	GEMEENTE	POS	TELPRIVE	GSM	EMAIL	SALD	OPMERK	
24028		289242			M								0 bisoprolol-insuline-mirtazapine-burinex-creon 150-rivotril	
24029		289243			M								0 Eliquis-bisoprolol-simvastatine-Fosamax-pantaprazol	
24030		289244			M								0 Methadone 70 mg	
24031		289245			M								0 Asaflow	
24032		289246			M								-982 Pacemaker 12/2021	
24033		289247			M								0 dentialia	
24034		289248			M								0 Parkinson	
24035		289249			M								0 Dialyse 3 X / semaine	
24036		289250			M								0 Pantaprazol 20 mg 1co matin-Diazepam 10mg 1co soir	
24037		289251			M								0 Amlopidine-bisoprolol-D cure-Lormetazepam-Losartan-Losfer	
24038		289252			M								0 Pontage cardiaque il y a 35 ans-Xarelto-ramipril-lipitor	
24039		289253			M								0 ass	
24040		289254			M								0 Valve cardiaque 2012	
24041		289255			M								0 Mari décédé	
24042		289256			M								0 Médecin	
24043		289257			M								0 dentialia	
24044		289258			M								0 Bisoprolol-Simvastatine -asaflow-nolvadex	
24045		289259			M								0 ASSURANCE	
24046		289260			M								0 Coversyl+Asaflow	
24047		289261			M								0 DENTALIA	
24048		289262			M								0 dentialia	
24049		289263			M								0	
24050		289264			M								0 CPAS	
24051		289265			M								0 La radio panoramique de mr se trouve dans l'historique10/23	
24052		289266			M								0 voir dans le planning les extractions prévue	
24053		289267			M								0 attention yanelle tu n'as pas facturé la pano qui date 10/22	
24054		289268			M								0 opg à fact la px 07/07	
24055		289269			M								0 bisoprolol-insuline-mirtazapine-burinex-creon 150-rivotril	
24056		289270			M								0 Asaflow	
24057		289271			M								0 dentialia	
24058		289272			M								0 CPAS	
24059		289273			M								-75 Coruno-Lixiana-Bisoprolol-Simvastatine Metformax	
24060		289274			M								0 DENTALIA	
24061		289275			M								0 le 09/06/22 prochaine fois compter la plaque de nance 250e	
24062		289276			M								0 DENTALIA	
24063		289277			M								0 voir les notes dans x care	
24064		289278			M								0 2-3 pontage et valve biologique-Asaflow-glucophage-novano	
24065		289279			M								0 Asaflow	
24066		289280			M								0 Vanlafaxine-gabapentine Myélopathie	
		289281			M								0 cpas berchem	
		289282			M								0 DENTALIA	
		381880			Mad								0	

Authorities/Whistleblowing

Central Intelligence Agency

Today's CIA Careers Legacy Newsroom Library

Report Information

INSTRUCTIONS **ONLINE FORM**

People from all over the world share information with the Central Intelligence Agency (CIA) daily. If you have information you think might help us and our foreign intelligence collection mission, there are many ways to reach us.

Your Tor Browser's **Security Level** is too low. Use the button in your browser's toolbar to change it.

The Guardian

First submission

First time submitting to our SecureDrop? Start here.

English

GET STARTED

Return visit

Already have a codename? Check for replies or submit something new.

LOG IN

Powered by SecureDrop 2.12.0

FAQ Verification PGP-public key Canary Seized domains

Active on Dark Markets? You have our attention!

The National Police of the Netherlands and judicial authorities collaborate with their foreign counterparts to combat IRL crime and cyber-enabled crime. Those who offer illicit goods or services have our attention. Are you one of them? How's your OpSec?

ARRESTED **ARRESTED** **ARRESTED**

- Dionysus
- Ikdev
- MickeyMouseNL
- Tomandjerry
- PostNL
- Syntopy
- Syntopy2021
- blue30s
- SVR667
- DutchMasters
- BHShop
- BarryBusiness
- DShop
- DrugsTradeCentre
- DutchCartel
- DutchLucky
- Fatamorgana
- Foggyperson
- Xtcmen
- Yourfinest
- gemstoned.net
- largomonkey
- Mirageexpress
- Mr.Ted
- NEVERPRESSED
- Nardhipples
- NoLove2323

GreenLeaks

GreenLeaks vous permet de nous transmettre en toute sécurité, des documents d'intérêt public concernant notamment, mais non exclusivement, les sujets écologiques et environnementaux.

Le régime de protection des lanceurs et lanceuses d'alertes a été créée en 2016. Il est fortement conseillé de lire les règles applicables dans le [Guide à usage du lanceur d'alerte et de ses soutiens](#) de la [Maison des Lanceurs d'Alerte](#) qui propose également un soutien juridique ou psychologique aux lanceurs et lanceuses d'alerte.

Greenleaks est une plateforme hébergée par Greenpeace France destinée à recueillir des informations ou des documents de façon sécurisée et anonyme (si souhaité par l'envoyeur)

Par courrier postal à cette adresse :
Service Investigation - Greenpeace France, 13 rue d'Enghien, 75010 Paris

envoyer un document

suivre un envoi passé

GREENPEACE

Media

BBC Home News Sport Earth Reel Worklife Travel

NEWS

Home | Israel-Gaza war | War in Ukraine | Climate | Video | World | UK | Business | Tech | Science

World | Africa | Asia | Australia | Europe | Latin America | Middle East | US & Canada

LIVE • 29,273 viewing

Trump denies he wrote lewd birthday note for Epstein as he asks for release of court papers

Summary

- US President Donald Trump asks for the release of court papers

PROPUBLICA
Investigative Journalism in the Public Interest

Menu

Nonprofit Explorer Local Initiatives Newsletters About Us

Get the Big Story

What We're Watching

During Donald Trump's second term, we will focus on the areas most in need of scrutiny — and how to get in touch.

bellingcat Investigations Guides Ukraine Justice & Accountability Workshops

POLICE UNITED STATES

Masked, Armed and Forceful: Finding Patterns in Los Angeles Immigration Raids

HINDUTVA INDIA

Violence in the Name of 'Animal Welfare': Up Truck Drivers

Activism



Why
was Tor created

How
does it work

What's
in there

Who's
active

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

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!

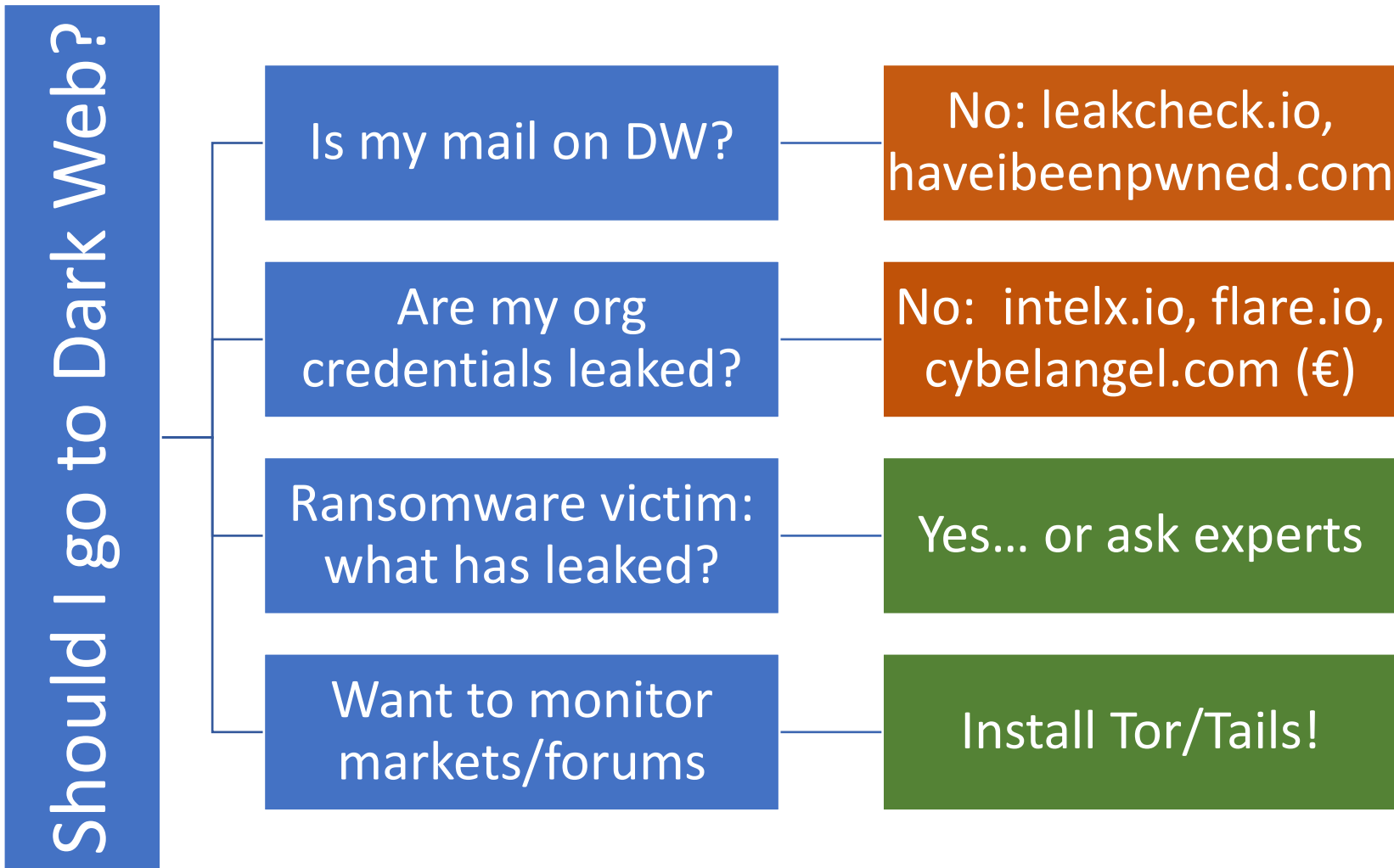
Police/FCCU



Police

- 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?



vandy.berten@ [redacted] [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.

[IntelligenceX](#) ☰

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

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?

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

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...

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!

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** against **ensorship**/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)

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)

Thank you for your attention!

Feedback / questions / discussion welcome!



vandy.berten@smals.be



www.smalsresearch.be
www.smals.be

Please share your
feedback with us!

