TOR: anonimowość, technologia i ciemna strona Internetu

Anonimowość to nie tylko wolność, ale także odpowiedzialność za bezpieczeństwo w cyfrowym świecie.

CYBERSECURITY DAY 2025

ALEKSANDRA PYRKOSZ-DZIUBCZYK

- Absolwentka PCz
- Doktorantka w Szkole Doktorskiej PCz
- Basic Client Security team w ZF Poland IT Center
- Studenckie Koło Naukowe “Cyberhydra”

PAWEŁ GORZAŁKA

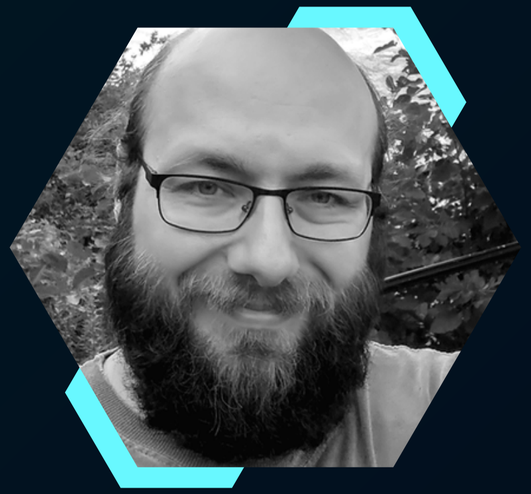
- Student Pcz
- Specjalista ds. IT
- Pentester
- Studenckie Koło Naukowe “Cyberhydra”

CZYM JEST TOR?

TOR (The Onion Router) to zdecentralizowana sieć zaprojektowana w celu zapewnienia anonimowości w internecie. Dzięki wielowarstwowej metodzie szyfrowania, zwanej trasowaniem cebulowym, TOR ukrywa tożsamość użytkownika i jego lokalizację. Powstał z myślą o ochronie prywatności oraz bezpiecznej komunikacji, a dziś znajduje zastosowanie zarówno w legalnych, jak i mniej etycznych celach.

KRÓTKA HISTORIA SIECI TOR

Mniej więcej na początku lat 2000 rozpoczeli projekt TOR, a już w 2002 oficjalnie uruchomiono sieci TOR i podano kod źródłowy. W 2006 roku utworzono fundacje TOR PROJECT, która przejęła opiekę nad siecią TOR.



Nick Mathewson

Współzałożyciel sieci TOR i jeden z głównych programistów, który wniósł ogromny wkład w rozwój i zabezpieczenia protokołu. Mathewson pracował nad kodem źródłowym TOR i był kluczowym członkiem zespołu Tor Project, zajmując się również kwestiami dotyczącymi anonimowości w sieci.

Roger Dingledine

Jeden z głównych twórców sieci TOR, który pełnił rolę dyrektora technicznego w organizacji Tor Project. Dingledine jest również jednym z autorów pierwotnej publikacji na temat systemu trasowania cebulowego, który stał się fundamentem sieci TOR.

Paul Syverson

Profesor i badacz w Naval Research Laboratory, który razem z Dingledinem i Mathewsonem zaprojektował protokół trasowania cebulowego. Syverson jest uważany za jednego z pionierów w dziedzinie anonimowości w internecie, a jego prace miały kluczowe znaczenie dla rozwoju TOR.

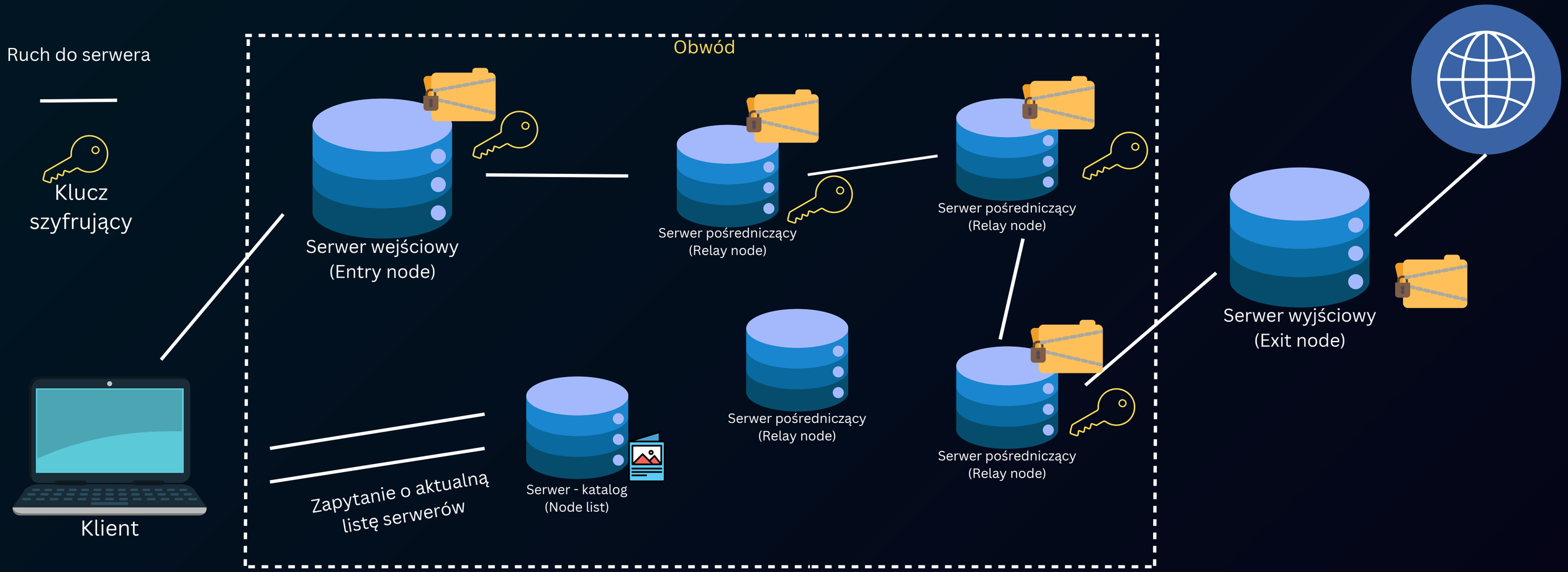
Cyberhydra

CYBERSECURITY DAY 2025

JAK DZIAŁA CEBULOWANIE ?

Najpierw klient wysyła zapytanie do serwera katalogowego o listę dostępnych serwerów wejściowych. Następnie (w przypadku użycia Tor Browser) następuje automatyczne łączenie z dostępnych serwerem wejściowym. Klient wybiera trasę, którą przesłane zostaną dane poprzez węzły wejściowe -> pośredniczące -> wyjściowe.

Węzeł wejściowy, odszyfrowuje pierwszą warstwę, dzięki czemu dowiaduje się gdzie ma przesłać dane dalej, jednak nie zna oryginalnych danych ani celu końcowego. Następnie kolejne warstwy (Relay) odszyfrowują swoje warstwy i przekazują zgodnie z instrukcją do kolejnych, nie znając danych oryginalnych. Na koniec ostatnią warstwę zdejmuję serwer wyjściowy i przesyła dane do serwera docelowego, nie znając jednocześnie danych nadawcy.



PUNKTY KRYTYCZNE TOR

01 Węzeł wyjściowy jest ostatnim punktem w obwodzie TOR, więc ma dostęp do niezaszyfrowanych danych jeśli nie występuje zabezpieczenie HTTPS.

02 Atak typu “end-to-end” to złośliwe działanie, w którym jakiś podmiot kontroluję cały węzeł wejściowy i wyjściowy mogąc analizując ruch sieciowy dostać nasze dane.

03 Niskiej jakości węzły mogą powodować spowolnienie działania i niezawodność sieci co wynika z niskiej przepustowości lub złej konfiguracji.

04 Atak Sybil - jest to wyjątkowo oporny sposób ataku na sieć TOR polegający na stworzeniu jak największej liczby fałszywych węzłów w sieci TOR, tym samym móc kontrolować ruch i analizować go.

05 Największym problemem sieci TOR jest fakt, że ze względu na wysoki potencjał zachowania anonimowości ale niestety też w celach nielegalnych, sieć TOR jest często kontrolowana lub też blokowana w wielu krajach co użytkownicy rozwiązują łącząc się mostkowo.

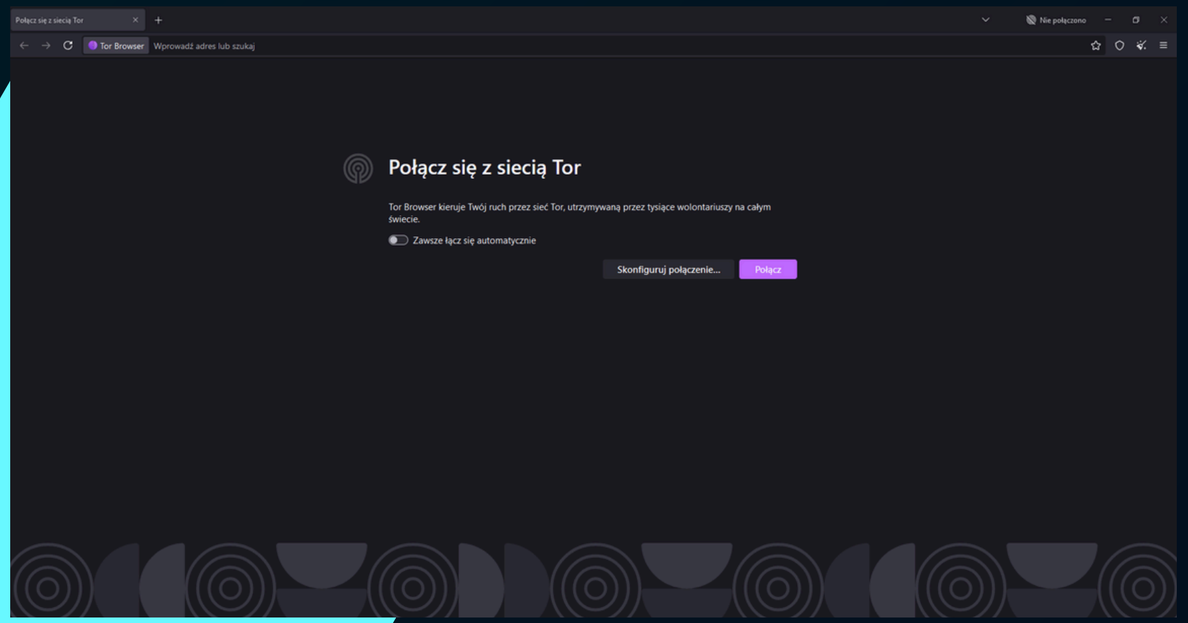
JAK WEJŚĆ DO SIECI TOR?

01

Tor Browser - to specjalnie zmodyfikowana wersja przeglądarki Mozilla Firefox, która automatycznie łączy się z siecią TOR. Typowe i bardzo popularne narzędzie dla osób rozpoczynających swoją anonimową karierę w sieci.

02

System operacyjny Tails OS - ciekawy system oparty na Linuxie, który działa w trybie live i może działać bezpośrednio z pendriv'a i nie zapisuje żadnych danych jeśli użytkownik wcześniej tego jasno nie skonfiguruje, co zwiększa anonimowość i posiada już wbudowane systemy obsługi sieci TOR.

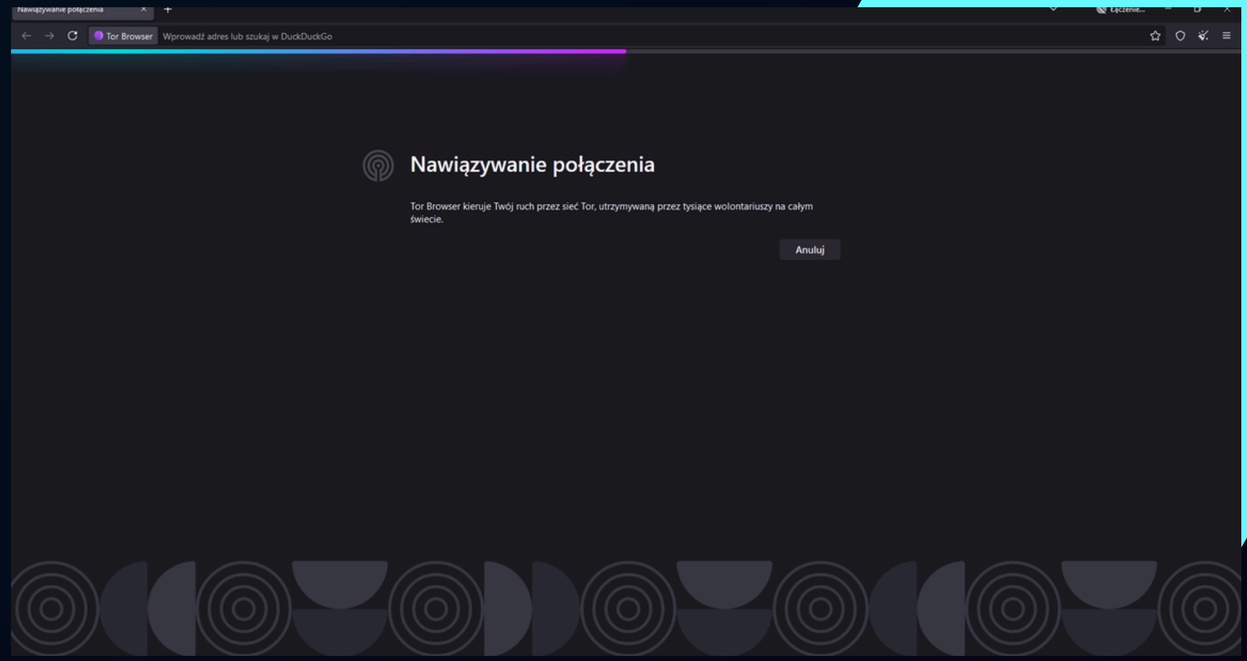


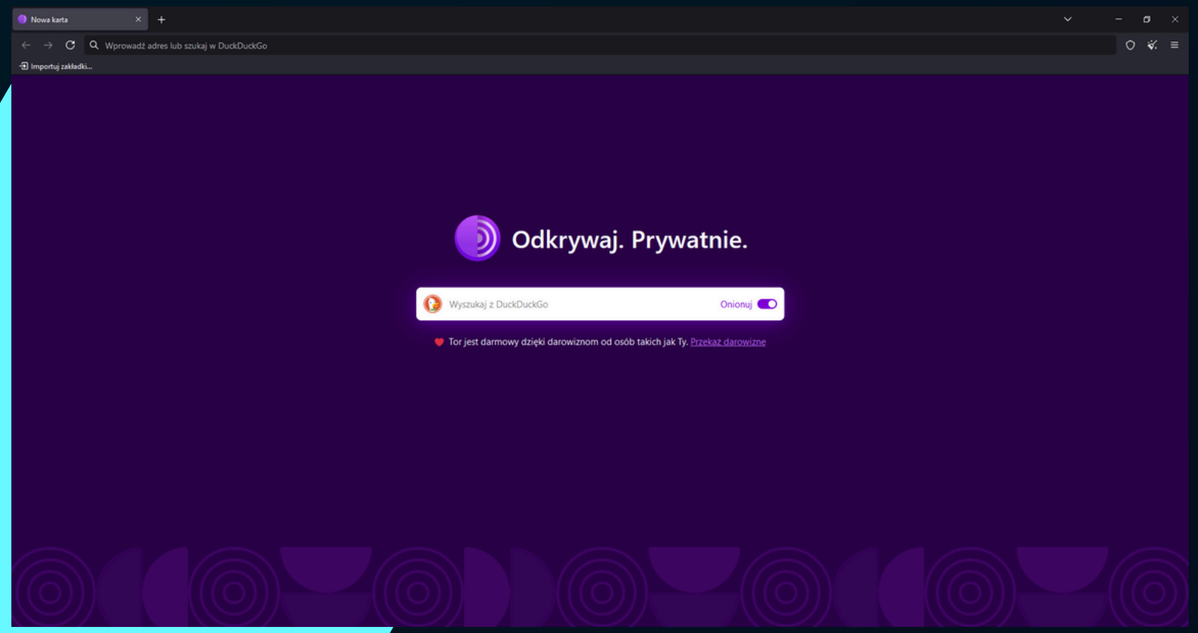
STEP 1

Otwórz Tor Browser po instalacji. Na ekranie powitalnym kliknij przycisk „Połącz”, aby rozpocząć łączenie z siecią TOR lub wybierz opcję skonfigurowania połączenia.

STEP 2

Tor Browser automatycznie nawiązuje bezpieczne połączenie, przekierowując Twój ruch przez sieć węzłów TOR. Czas oczekiwania może chwilę potrwać w zależności od obciążenia sieci.



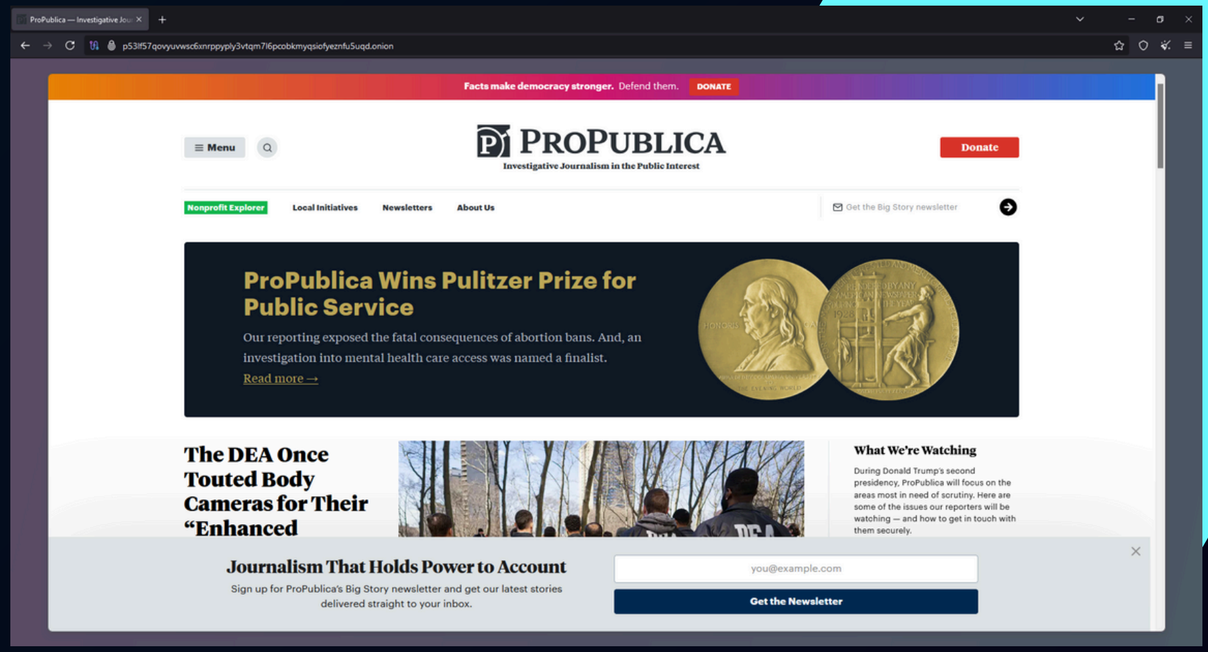


STEP 3

Po udanym połączeniu zobaczysz ekran startowy z wyszukiwarką DuckDuckGo. Możesz teraz bezpiecznie i anonimowo korzystać z internetu

STEP 4

Wpisz bezpieczny adres strony w domenie .onion, np. ProPublica, aby odwiedzić serwis w sieci TOR. Upewnij się, że korzystasz z oficjalnych i sprawdzonych adresów.



Cyberhydra

CYBERSECURITY DAY 2025

JAK BEZPIECZNIE UŻYWAĆ TOR ?

Zasada 1

Zawsze używaj połączeń HTTPS co zapewni szyfrowanie danych od klienta do serwera nawet jeśli przechodzą przez węzeł wyjściowy w sieci TOR.

Zasada 2

Unikaj ujawniania tożsamości - nie zalecam podawania swoich danych osobowych, a tym bardziej logowania się na konta, które wymagają identyfikacji. Utrudnisz w ten sposób analizę ruchu w sieci co utrudni powiązanie twojego ruchu z twoimi danymi osobowymi.

Zasad 3

Nie pobieraj plików z nieznanych źródeł - piliki pobrane z TOR na 99% zawierają w sobie złośliwe oprogramowanie, którego zadaniem będzie wychwycenie twoich danych osobowych. Wyobraź sobie sytuację kiedy przeglądasz przy użyciu TOR strony które poruszają tematy nielegalne w twoim kraju, a następnie taki wirus z pobranego pliku z łatwością kradnie twoje dane i zostajesz przedstawiony przed wyborem, albo zapłata albo ujawnienie twoich danych i stron jakie odwiedzałeś.

ALTERNATYWY SIECI TOR

I2P (Invisible Internet Project)

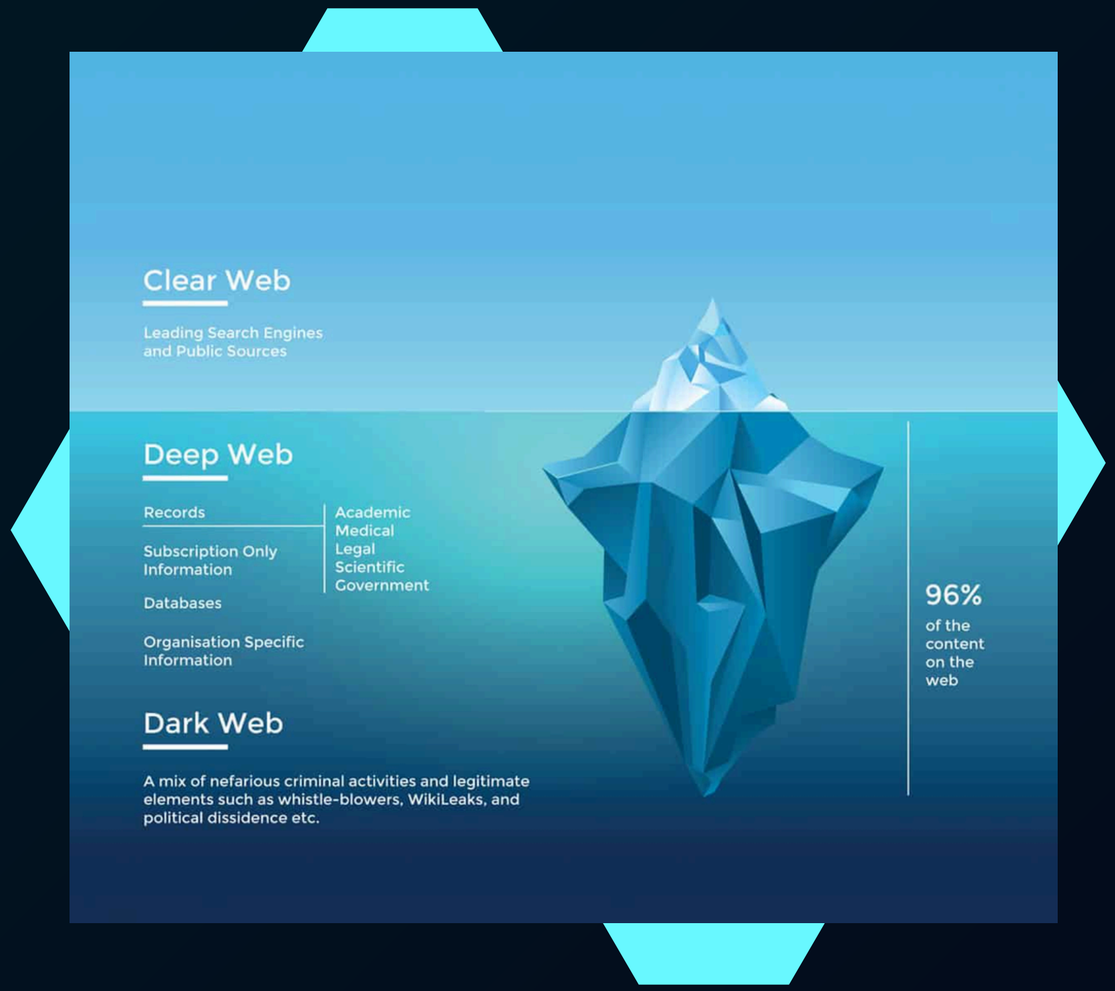
To zdecentralizowana sieć anonimowa, które oferuje podobne funkcje do TOR, ale z innym podejściem do trasowania ruchu. I2P używa własnych mechanizmów routingu i jest zoptymalizowana do komunikacji w ramach samej sieci I2P, co sprawia, że jest mniej narażona na ataki niż TOR w niektórych scenariuszach.

Freenet

Freenet to sieć peer-to-peer, która zapewnia anonimowość w sieci. Użytkownicy mogą udostępniać i pobierać pliki oraz odwiedzać strony internetowe bez ujawniania swojej tożsamości. Freenet wykorzystuje rozproszone przechowywanie danych, co czyni ją bardziej odporną na cenzurę.

VPN (Virtual Private Network)

VPN to technologia, która tworzy zaszyfrowane połączenie między użytkownikiem a serwerem, ukrywając rzeczywisty adres IP i zapewniając prywatność w internecie. Choć VPN nie oferuje takiej samej anonimowości jak TOR (np. nie zapewnia anonimowości w samej sieci)



CLEAR WEB, DEEP WEB, DARK WEB

Clear Web

- To część Internetu dostępna publicznie i indeksowana przez wyszukiwarki
- Przykłady: strony informacyjne, portale społecznościowe, sklepy internetowe

Deep Web

- Zawiera treści niewidoczne dla standardowych wyszukiwarek
- Przykłady: konta bankowe online, dane medyczne, uczelniane bazy danych, treści za paywallem
- Nie jest nielegalny — to po prostu treści wymagające uwierzytelnienia lub dostępu

Dark Web

- Część Deep Webu, do której dostęp uzyskuje się za pomocą specjalnych narzędzi, np. sieci Tor
- Wykorzystywany do anonimowej komunikacji, ale też często kojarzony z nielegalnymi działaniami
- Przykłady: ukryte fora, nielegalne rynki, serwisy oferujące nielegalne usługi

DZIAŁANIA NIELEGALNE

Sieć Tor, choć stworzona z myślą o anonimowości i wolności w internecie, bywa wykorzystywana do nielegalnych celów. Na tzw. darknecie, ukrytym segmencie internetu dostępnym przez Tor, mogą działać nielegalne rynki, fora przestępcze, czy serwisy oferujące handel narkotykami, bronią, fałszywymi dokumentami i danymi osobowymi.

Cyberhydra

CYBERSECURITY DAY 2025

01

Sklepy z używkami
Na darknecie działają nielegalne marketplace'y przypominające Allegro czy Amazon — tyle że zamiast elektroniki oferują substancje psychoaktywne. Transakcje są anonimowe, a płatności realizowane kryptowalutami.

02

Fora hakerskie
Miejsca wymiany wiedzy, narzędzi i usług – użytkownicy dzielą się złośliwym oprogramowaniem, poradami dotyczącymi włamań czy sprzedażą danych z wycieków.

03

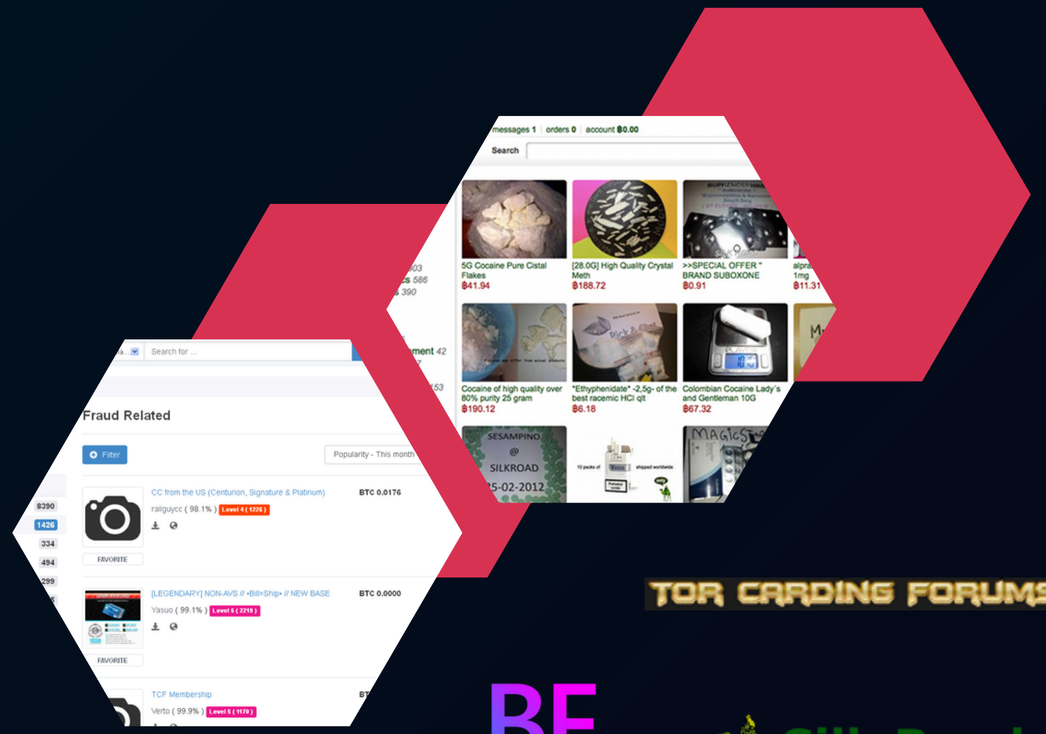
Sklepy z bronią
Platformy te umożliwiają zakup nielegalnych narzędzi przemocy – od prawdziwych replik broni palnej, przez amunicję, po improwizowane urządzenia wybuchowe. Choć wiele z tych ogłoszeń jest fałszywych.

04

Ransomware
W obrębie dark webu funkcjonują usługi związane z ransomware, czyli oprogramowaniem służącym do szyfrowania danych ofiar w celu wymuszenia okupu za ich odblokowanie. Oferty obejmują narzędzia infekcji, wsparcie techniczne oraz wskazówki, jak przeprowadzić atak, czyniąc z tej formy cyberprzestępczości rozbudowaną „usługę as-a-service".

05

Krzywdzące treści (pedofilia)
Najbardziej niebezpieczna część dark webu — mogą się tam pojawiać treści promujące przemoc, wykorzystywanie nieletnich czy inne formy patologii.



TOR CARDING FORUMS

BF

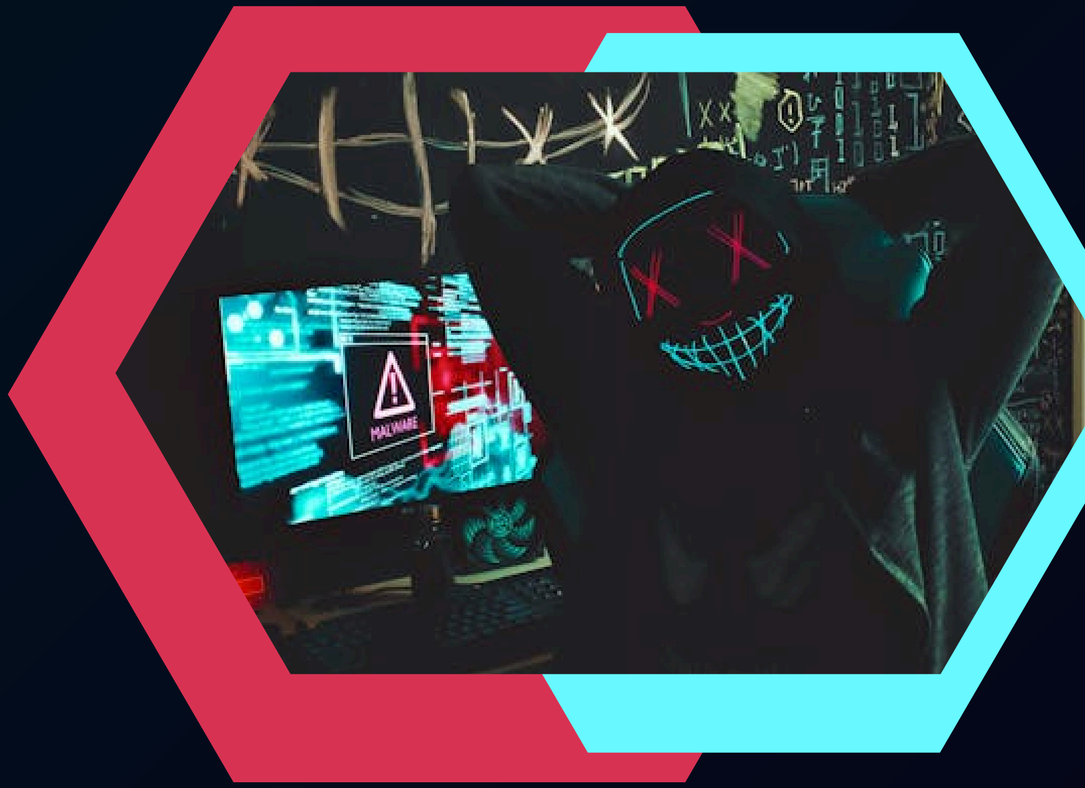
Silk Road
anonymous marketplace

AlphaBay Market

HURT 2 THE CORE

CZY JEST SIĘ CZYM NIEPOKOIĆ?

To zależy.
Z jednej strony, sieć Tor bywa wykorzystywana do nielegalnego handlu, np. narkotykami, bronią czy danymi osobowymi. Dzięki anonimowości, użytkownicy mogą ukrywać swoją tożsamość i unikać służb. To sprawia, że darknet jest atrakcyjny dla przestępców.
Z drugiej strony, podobne ogłoszenia można znaleźć również w zwykłym Internecie, na zamkniętych grupach, komunikatorach czy forach — nie tylko w dark webie. Tor to narzędzie — nie decyduje o tym, do czego zostanie użyte.

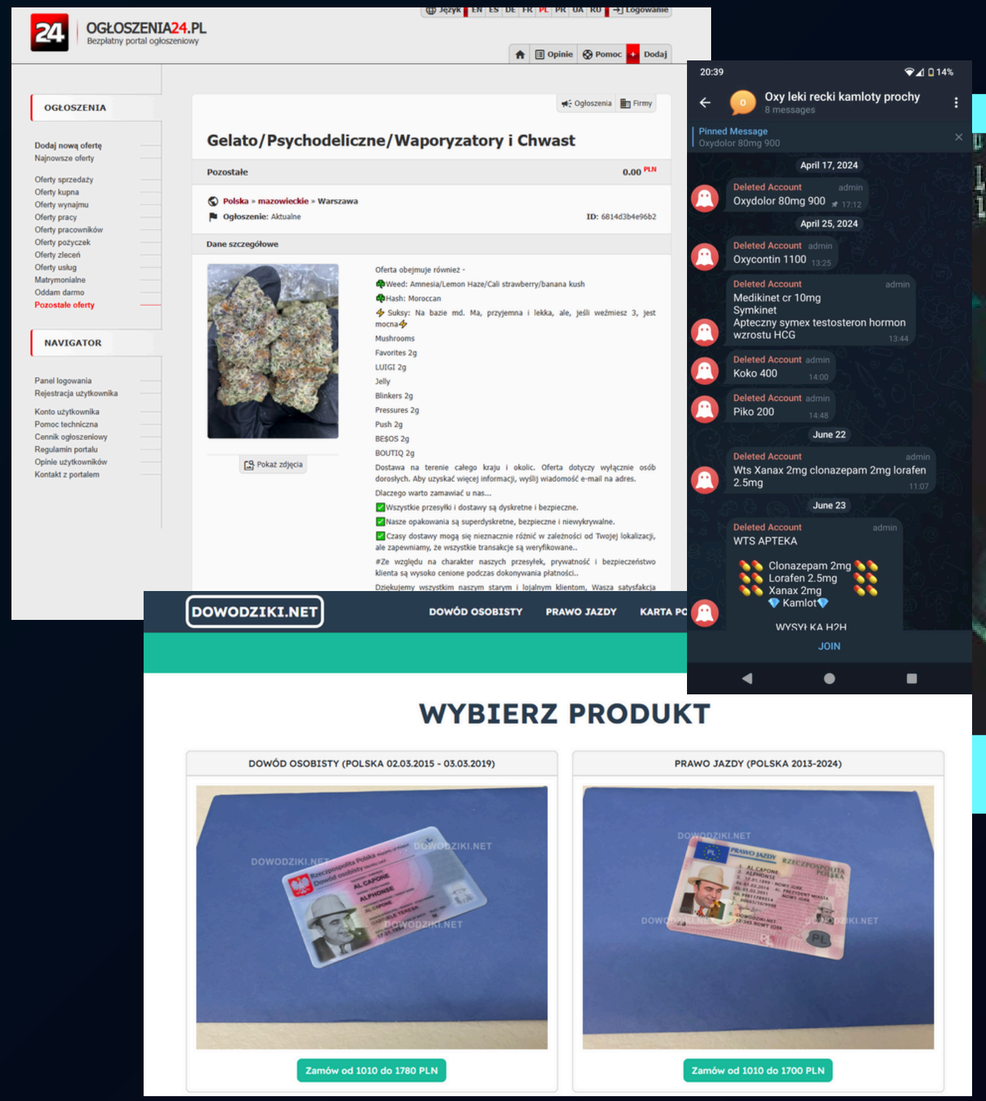


CZY JEST SIĘ CZYM NIEPOKOIĆ?

To zależy.

Z jednej strony, Tor bywa wykorzystywany do nielegalnego handlu, np. narkotykami, bronią czy danymi osobowymi. Dzięki anonimowości, użytkownicy mogą ukrywać swoją tożsamość i unikać służb. To sprawia, że darknet jest atrakcyjny dla przestępców.

Z drugiej strony, podobne ogłoszenia można znaleźć również w zwykłym Internecie, na zamkniętych grupach, komunikatorach czy forach — nie tylko w dark webie. Tor to narzędzie — nie decyduje o tym, do czego zostanie użyte.



Q&A

DZIĘKUJEMY ZA UWAGĘ!

CYBERSECURITY DAY 2025