**Temat: Sieć TOR**

**Sieć TOR** (The Onion Router) powstała w 2004 roku. Często można znaleźć o niej informacje pod takimi hasłami jak „**drugi Internet**” czy „**czarny Internet**”. Jej nazwa pochodzi od techniki trasowania cebulowego polegającego na wysyłaniu wiadomości warstwami szyfrowania. **Sieć TOR** została opatentowana w latach 90. XX wieku przez osoby związane z amerykańską marynarką wojenną po to, żeby zamaskować działalność agentów wywiadu w sieci. Jak działają **sieci cebulowe**? Każdy serwer w tym łańcuchu odszyfrowuje dane, podmienia adres IP, szyfruje go po raz kolejny i przesyła dalej. Wyjątkiem jest końcowy punkt połączenia zwany ExitNode, czyli nic innego, jak ostatni serwer, do którego trafiają dane, zanim połączysz się z witryną, którą chcesz odwiedzić. Ten serwer odszyfrowuje dane, jednak nie szyfruje ich ponownie, przez co stanowi słaby punkt łańcucha.

Kolejność serwerów, do których dane są rozsyłane, zmienia się co około 10 minut, dzięki czemu nawet jeśli ktoś śledzi poszczególne punkty proxy (czyli właśnie serwery), pozyska jedynie bezwartościowe, szyfrowane dane, które szybko się dezaktualizują.

ANONIMIZACJA: Tor jest siecią tysięcy serwerów (proxy), które podczas otwierania stron internetowych włączają się między internautę i stronę w różnej kolejności. Pierwszy serwer proxy podmienia przy tym adres IP peceta na własny. Na każdym następnym przystanku oznaczenie zmienia się kolejny raz. W ten sposób operator strony nie poznaje prawdziwego pochodzenia zapytania.

SZYFROWANIE: Tor wysyła zaszyfrowane zapytania i adresy IP użytkownika do operatora strony. Każdy serwer proxy w łańcuchu rozszyfrowuje teraz dane poprzedniego proxy i szyfruje je ponownie dla następnego. Jeśli jeden z serwerów proxy jest inwigilowany, to otrzymane informacje będą bezwartościowe. Tylko ostatni

serwer w łańcuchu tłumaczy zapytanie z powrotem na otwarty tekst - to jedyny słaby punkt.

ZASADA PRZYPADKU: Co dziesięć minut wybierana jest nowa, przypadkowa droga przez sieć serwerów proxy. To sprawia, że efektywna inwigilacja jest niemożliwa nawet w przypadku kontroli kilku proxy.

OTWARTOŚĆ: Kod programu jest publiczny (Open Source). Pozwala to na szybkie wykrywanie słabych punktów i wyklucza ukrywanie w nim funkcji szpiegowskich.

Trasa pakietu

Użytkownicy uruchamiają na swoich komputerach oprogramowanie klienckie sieci Tor, które okresowo tworzy wirtualne obwody w sieci.

Tor wielowarstwowo szyfruje przesyłane komunikaty (stąd nazwa „trasowanie cebulowe”), zapewniając doskonałą poufność przesyłania pomiędzy ruterami. Jednocześnie oprogramowanie udostępnia interfejs SOCKS klientom. Aplikacje potrafiące obsługiwać protokół SOCKS mogą być skonfigurowane tak, by łączyły się z internetem za pośrednictwem oprogramowania klienckiego Tor, pełniącego w tym wypadku funkcję proxy, które następnie multipleksuje ruch sieciowy przez wirtualny obwód sieci Tor.

Wewnątrz sieci Tor ruch jest przekazywany pomiędzy ruterami, osiągając w końcu węzeł wyjściowy, z którego niezaszyfrowany pakiet jest przekazywany do miejsca przeznaczenia. Z punktu widzenia docelowego komputera, ruch wydaje się pochodzić z wyjściowego węzła sieci Tor.

Schemat połączenia:

Użytkownik → węzeł1 → węzeł2 → węzeł3 → Serwer docelowy.

Pakiet jest zaszyfrowany szyfrem, do którego klucz posiada wyłącznie węzeł 3. Dołączony do niego jest zaszyfrowany adres węzła 2 – klucz do niego posiada węzeł 1 – a także zaszyfrowany adres węzła 3 – klucz do niego posiada węzeł 2.

Węzeł 3 komunikuje się z serwerem docelowym, a następnie odpowiedź przekazuje analogicznie w drugą stronę.

Sieć Tor działa na poziomie protokołu TCP i – inaczej niż większość pozostałych sieci anonimowych – nie narzuca ograniczeń co do możliwych zastosowań.

**Darknet** jest częścią większej „głębokiej sieci”, sieci tajnych witryn internetowych, które istnieją w zaszyfrowanej sieci. Nie wszystkie działania związane z darknetem są nielegalne. Większości tych stron nie można przeszukiwać tradycyjnymi kanałami, ponieważ są chronione hasłem i wymagają określonych narzędzi lub autoryzacji. Darknet to nic innego jak ukryte fora, sklepy internetowe czy portale.   
W darknecie znajduje się praktycznie wszystko. W tajnej sieci można wygłaszać poglądy polityczne czy ideologiczne na forach zrzeszających użytkowników.

TOR Browser - przeglądarka w sieci TOR

1. [The Hidden Wiki](https://pl.wizcase.com/blog/bezpiecznie-znajdz-najlepsze-ciemne-strony-internetowe/#thehiddenwiki) — katalog Dark Web
2. [TorLinks](https://pl.wizcase.com/blog/bezpiecznie-znajdz-najlepsze-ciemne-strony-internetowe/#torlinks) — katalog stron .onion
3. [DuckDuckGo](https://pl.wizcase.com/blog/bezpiecznie-znajdz-najlepsze-ciemne-strony-internetowe/#duck) — wyszukiwarka, która indeksuje strony .onion i nie śledzi wyszukiwań, nie korzysta z trackerów.
4. [ProtonMail](https://pl.wizcase.com/blog/bezpiecznie-znajdz-najlepsze-ciemne-strony-internetowe/#proton) — bezpieczna usługa e-mail, która zapewnia anonimowość.