POLITECHNIKA
OPOLSKA

PRZEGLĄD NAUK STOSOWANYCH

pod redakcją
Mariusza Rząsy

nr 19

Wydział Ekonomii i Zarządzania
Opole, 2018

Przegląd Nauk Stosowanych

Nr 19

ISSN 2353-8899

Przegląd Nauk Stosowanych Nr 19 (2)

Redakcja: Mariusz R. Rząsa

Wszystkie artykuły zostały ocenione przez dwóch niezależnych recenzentów

All contributions have been reviewed by two independent reviewers

Projekt okładki: Krzysztof Kasza

Opracowanie graficzne: Oficyna Wydawnicza Politechniki Opolskiej

Wydanie I, 2018 r.

ISSN 2353-8899

Spis treści

SŁOWO WSTĘPNE

Ten numer Przeglądu Nauk Stosowanych poświęcony jest w całości ogólnopolskiej konferencji naukowej zatytułowanej „Praktyczne aspekty i możliwości wykorzystania potencjału naukowo- badawczego oraz transfer wiedzy pomiędzy sektorem nauki, a jednostkami Krajowej Administracji Skarbowej", która odbyła się w Opolu w dniach 13-14 marca 2018 r. z inicjatywy Izby Administracji Skarbowej w Opolu i Politechniki Opolskiej. W niniejszym numerze Przeglądu Nauk Stosowanych zamieszczono informacje o konferencji oraz opublikowano wybrane artykuły autorów wystąpień konferencyjnych. Wśród autorów artykułów są zarówno pracownicy naukowi uczelni, jak również pracownicy i funkcjonariusze jednostek Krajowej Administracji Skarbowej. Wiele artykułów posiada dwóch autorów reprezentujących obydwa środowiska, co dowodzi współpracy pomędzy tymi sektorami.

Głównym celem tego naukowego wydarzenia była dyskusja i wymiana doświadczeń pomiędzy środowiskiem naukowym uczelni a przedstawicielami izb administracji skarbowej z całego kraju dotycząca możliwych form i obszarów zacieśnienia współpracy obu środowisk. W trakcie dwóch dni konferencji teoretycy i praktycy mogli spotkać się i podyskutować o możliwościach oraz korzyściach, jakie daje partnerstwo nauki z administracją skarbową. Ku satysfakcji Organizatorów konferencja charakteryzowała się wysokim poziomem merytorycznym dyskusji, a jej tematyka spotkała się z dużym zainteresowaniem przedstawicieli obu środowisk. Mamy nadzieję, że publikacja będzie nie tylko źródłem wiedzy, dobrych praktyk,ale także inspiracją dla innych jednostek administracji publicznej.

Paweł Cybulski
Podsekretarz Stanu
Zastępca Szefa Krajowej Administracji Skarbowej
Ministerstwo Finansów
ul. Świętokrzyska 12
00-916 Warszawa
pawel.cybulski@mf.gov.pl

Rafał KOKOT
Tomasz TURBA

ZARYS HISTORYCZNY SIECI DARKNET ORAZ ASPEKTY LEGALNEGO I NIELEGALNEGO WYKORZYSTANIA TECHNOLOGII TOR

Streszczenie: Artykuł opisuje zarys historyczny sieci darknet oraz legalne i nielegalne zastosowania anonimowej technologii opartej o sieć TOR. W kolejnych rozdziałach została opisana historia powstania, zalety i wady rozwiązania oraz potencjalne kierunki rozwoju i wykorzystania technologii w przyszłości w kontekście działań służb zwalczających przestępczość w Internecie, a także po stronie zwykłego użytkownika pragnącego zachować anonimowość w sieci.

Słowa kluczowe: sieć tor, darknet, deepweb, anonimowość.

HISTORICAL OUTLINE OF DARKNET AND THE LEGAL AND ILLEGAL ASPECTS OF USE THE TOR TECHNOLOGY

Summary: Article describes the legal and illegal uses of anonymous technology based on the Tor network. The following chapters describe the history of uprising, the advantages and disadvantages of the solution, and the potential trends for the development and use of technologies in the futures in context of the customs service to fight cybercrime, as well as for the ordinary user wishing to remain anonymous online.

Keywords: tor, darknet, deepweb, anonymity.

1. HISTORIA POWSTANIA SIECI DARKNET

Od początku powstania sieci Internet zaczęto zastanawiać się nad problemem wolności i anonimowości w Internecie. Stale pojawiają się kontrowersje i spory pomiędzy zwolennikami pełnej swobody i anonimowości w sieci, a stronnikami prawnego ograniczania korzystania z zasobów Internetu. W latach siedemdziesiątych, w zasadzie równocześnie, z sieci ARPANET [Biddle 2002: 3] ewoluowały dwie technologie – Internet znany dzisiaj każdemu oraz „Darknet" -określany ogólnie -zbiorem technologii wyizolowanych sieci zapewniających anonimowość, stworzonych do celów bezpieczeństwa. Określenie „Darknet" pojawiło się w 2002 w publikacji pracowników firmy Microsoft [Biddle 2002: 10] i od tej pory oficjalnie zaczęto używać tego pojęcia do ukrytej części internetu. Ludzie od zawsze kopiowali zawartość sieci, jednak w przeszłości większość tych obiektów musiała reprezentować policzalną, walutową wartość. Nielegalne działania w tym zakresie zostały zatrzymane dzięki wprowadzeniu przepisów prawa patentowego i ekonomicznego. Dzisiaj trudność polega na

tym, że przestępstwo kradzieży intelektualnej może być nienamacalne. Z reguły przestępstwa komputerowe są zapisem bitów i bajtów przetłumaczonych w sposób zrozumiały dla odbiorcy. Wraz z przyspieszeniem technologicznym w zakresie rozszerzenia dostępności sieci Internet na cały świat, wiele aspektów prawnych do dzisiaj nie jest uregulowanych, nie wspominając o trudności w nadążaniu nad opanowaniem nowych technologii przez człowieka. Jednakże istnieje prosta i tania możliwość pozyskania dobrej jakości pożądanej treści. Największym wyzwaniem jest sformułowanie, czy kontent może być dystrybuowany legalnie, jeżeli tak- to w jakim zakresie. Prawo autorskie strzeże legalności kopiowania i dystrybuowania cennych danych, ale ochrona tego prawa w ogólnodostępnej i szybkiej sieci jest trudna i stanowi ogromne wyzwanie dla regulatorów. Typowym przykładem ideologii stojącej za określeniem „darknet" jest kreatywność twórców oprogramowania, którzy mają na celu udostępnianie plików audio. Po raz pierwszy zostało to spopularyzowane przez aplikację Napster jeszcze przed czasem, gdy nagrywarki CD stały się ogólnodostępne [Goos 2016: 172]. Można powiedzieć, że udostępnianie plików na dużą skalę miało miejsce od początku pojawienia się komputerów klasy PC. Idea darknetu opiera się na trzech założeniach podstawowych:

- każdy szeroko rozproszony plik będzie dostępny dla części użytkowników w formie umożliwiającej kopiowanie i dystrybuowanie,
- użytkownicy będą kopiować i udostępniać pliki ,jeżeli jest to możliwe i interesujące,
- użytkownicy są połączeni bezpośrednimi węzłami o wysokiej przepustowości.

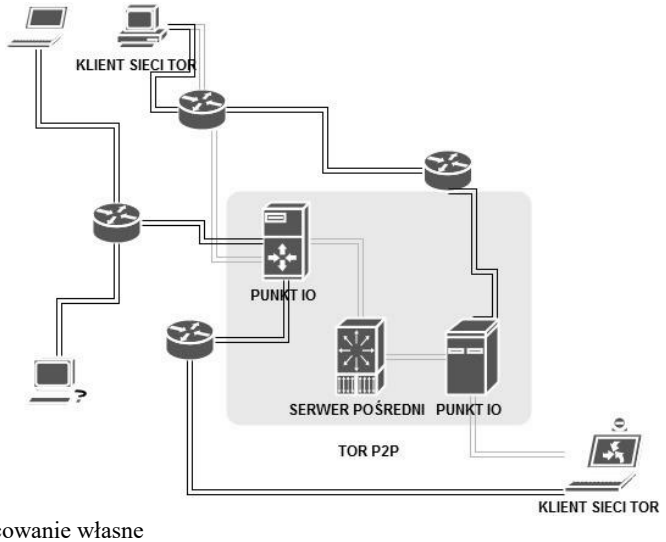
Darknet jest więc siecią dystrybucyjną, która rośnie wraz z ze zwiększoną liczbą udostępnianych plików bądź treści. Jedną z podstawowych implikacji jest założenie, że każdy system ochrony treści zostanie złamany i dojdzie do wycieku do w/w sieci, ponieważ część użytkowników – ekspertów bezpieczeństwa – pokona większość mechanizmów zabezpieczania przed kopiowaniem. Ważne jest też zrozumienie pojęcia „szeroko rozproszonego pliku" – ma to na celu uchwycenie pojęcia dystrybucji na rynku masowym dla milionów, praktycznie anonimowych użytkowników. Jest to założenie sprzeczne w zakresie ochrony tajemnic wojskowych, przemysłowych lub osobistych, które zazwyczaj nie są szeroko rozpowszechniane. Warto w tym momencie zwrócić uwagę na mechanizmy inżynierii społecznych stosowanych na portalach społecznościowych. Użytkownicy sami publikują i udostępniają tam swoje treści, pozostawiając wieczny ślad [Goos 2016: 176]. W kontekście służb mundurowych – wszelkie ślady mogące potwierdzić działalność podejrzanego użytkownika mogą być wykorzystane do jego zatrzymania. Pomimo, że nadal to tylko bity danych, to jednak ich cena na czarnym rynku niebotycznie wzrasta każdego dnia [Gorle 2015: 9]. Na cenę danych także ogromny wpływ miało niedawno wprowadzone rozporządzenie Parlamentu Europejskiego i Rady (UE) GDPR 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych, w Polsce noszące skrótową nazwę „RODO".

Pomimo, że rozporządzenie niesie za sobą wartość dodaną w postaci podnoszenia świadomości użytkowników i przedsiębiorców o przetwarzaniu danych i potrzebie zachowania ich bezpieczeństwa, to jednak na nielegalnych forach sieci darknet dało się zauważyć wzmożone podnoszenie cen związanych z wyciekami danych.

2. MODEL I EWOLUCJA SIECI NIELEGALNEJ DYSTRYBUCJI

Sieć darknet jest siecią dystrybucyjną która związuje ze sobą wstrzykiwanie plików i danych do sieci poprzez udostępnienie ich określonym użytkownikom. Opiera się na założeniu, że użytkownicy zainteresują się danymi i zaczną je kopiować dla siebie, a także udostępniać dla innych. Tak jak inne sieci tego typu (np. Napster, Gnutella), sieć darknet może zostać zamodelowana jako graf bezpośredni z krawędziami oznaczonymi. Graf ma po jednym wierzchołku dla każdego użytkownika (hosta), a dla każdej pary wierzchołków do których skierowana jest krawędź - jeśli obiekty mogą być kopiowane pomiędzy nimi. Etykiety brzegowe mogą służyć do modelowania istotnych informacji na temat topologii fizycznej sieci i mogą zawierać informację do których zalicza się: przepustowość, dostępność, priorytet i opóźnienie. Wierzchołki charakteryzowane są biblioteką obiektu (np. zbiór filmów), ilością żądań dostępu do obiektu od innych wierzchołków, a także spełnionych żądań do obiektów (kopiowanie zakończone sukcesem).

Rysunek 1. Schemat sieci TOR



Źródło: Opracowanie własne

By sieć darknet mogła prawidłowo funkcjonować niezbędne jest spełnienie kilku wymagań związanych z procesem przepływu danych, do których zalicza się:

1. Wymaganie związane z kompromisem udostępnienia danych w sposób technologicznie umożliwiający przesłanie obiektów do sieci poprzez ich konwersję. Jako przykład podaje się konwersję oryginalnego formatu wideo AVC na MP4 lub z XVID.
2. Istnienie mechanizmów magazynowania i replikacji danych w celu zezwolenia tworzenia i kopiowania danych przez użytkowników w sieci typu peer-to-peer (P2P). Jako przykład dzisiaj podaje się dysk twardy komputera, lub pamięć przenośną.
3. Istnienie urządzeń lub oprogramowania renderującego dane pozyskane z sieci. Dawniej były to przenośne odtwarzacze muzyki, odtwarzacze płyt DVD. Dzisiaj mówi się o oprogramowaniu i kodekach potrafiących obsługiwać konkretny standard kompresji i konwersji (np. K-Lite Codec-Pack, VLC Media Player).

Sieć darknet w rdzennej koncepcji musi spełniać następujące wymagania technologiczne:

1. Dowolna sieć darknet wymaga istnienia węzłów, które operują jako źródła przechwytywania danych. Użytkownicy wskazują co udostępniają w sieci i czekają na innych użytkowników chcących pozyskać dane.
2. Jeżeli istnieje nadawca, to musi w sieci istnieć także odbiorca operujący na tych samych zasadach. W dzisiejszych sieciach zwykle użytkownik jest jednocześnie nadawcą (seeder) i odbiorcą (leecher).
3. Łącza transmisyjne są niezbędne do transferowania obiektów (ich kopii) pomiędzy węzłami. W dzisiejszych czasach wykorzystuje się połączenie internetowe do nawiązania szyfrowanego połączenia z siecią darknet (np. za pomocą przeglądarki TOR Onion Browser).
4. Wyszukiwarki lub inne mechanizmy rozpoznawania nowych i istniejących użytkowników w celu odnalezienia pożądanej treści/danej.
5. Sieć może szyfrować wiele mikro-sieci wewnątrz struktury uniemożliwiając namierzenie użytkownika, zapewniając dzięki temu anonimowość

Można sklasyfikować różne manifestacje istnienia sieci darknet, które pojawiły się w ostatnich kilku latach ze względu na spełnienie pięciu podstawowych założeń opisanych wyżej. Także ze względu na analizę słabości i punktów ataków. Jako system, sieć darknet jest obiektem wielu ataków. Identyfikacja i powstrzymanie naruszeń prawa w sieci Internet w drodze postępowania sądowego jest wyzwaniem dla służb, zwłaszcza w kontekście problemu anonimowości. Dodatkowym problemem jest masowe też „wstrzykiwanie" i testowanie złośliwego oprogramowania bez kontroli. Wirusy, malware oraz spam stają się coraz bardziej szkodliwe.

Na początku lat 90-tych dystrybuowanie danych komputerowych było organizowane w obrębie grup znajomych. Do głównego nurtu danych należały wówczas muzyka i proste programy komputerowe (dyskietkowe). Urządzenia obsługujące były powszechnie dostępne, a sposób ich użytkowania nie decydo-

wał o legalności zastosowania. Przekazywanie danych w żaden sposób nie było regulowane i nie istniały formalne zabezpieczenia systemowe przed kopiowaniem. Nawet jeżeli istniały, to sposób zabezpieczenia był na tyle trywialny, że nie wymagał specjalnego instruktażu wykonawczego. Głównym źródłem transmisji danych były osoby same w sobie, które wymieniały dane „z ręki do ręki" lub za pośrednictwem poczty „pantoflowej" – głównego sposobu dystrybucji danych na owe czasy. Główną wadą takiej sieci było opóźnienie w dostępie do danych. Pozyskiwanie danych z sieci darknet (nazwanej wówczas po prostu „czarnym rynkiem") za pomocą linii modemowej o przepustowości 56.6 Kbps, kopiowanie oraz dystrybuowanie - mogło trwać tygodniami. Dodatkowym problemem był brak istnienia wyspecjalizowanej wyszukiwarki.

W roku 1998 powstała nowa forma darknetu ze względu na znaczące postępy technologiczne w kilku obszarach. Internet wszedł do głównego nurtu kultury i powoli stawał się głównym medium do transmisji danych prywatnych i służbowych. Kontynuacja spadków cenowych sprzętu komputerowego zapewniała zwiększenie dostępności do sieci Internet. Wraz ze wzrostem mocy obliczeniowej pojawiły się nowe algorytmy kompresji danych, gdzie nawet przy stosunkowo niskich przepustowościach (1 Mbps) pobranie pliku w formacie MP3 nie zajmowało już dużo czasu. Rok 1998 został określony także jako rok, w którym skok technologiczny spowodował, że komputery klasy PC przekroczyły granicę, w której ich moc obliczeniowa mogła służyć do odtwarzania multimediów. Wraz ze wzrostem w/w. czynników, pojawiały się pierwsze nielegalne sieci nazwane potocznie „Warez" z serwerami w Internecie w scentralizowanej strukturze. Sieć oparta o pocztę „pantoflową" została wyparta siecią Internet, gdzie dostęp jest znacznie szybszy i istnieją wyszukiwarki oraz sposoby komunikacji z innymi użytkownikami. Jednakże wraz z pozyskiwaniem plików z serwerów FTP oraz HTTP – użytkownik zawsze pozostawiał po sobie ślad w postaci adresu IP, znaczników czasu i celu pobierania. Spowodowało to początkową lawinę procesów o naruszenie praw autorskich, więc scentralizowany darknet stosunkowo szybko zniknął z głównego nurtu Internetu.

Zrozumienie problemu „anonimowości" stało się ważnym aspektem do rozwiązania i zaczęto powracać do koncepcji połączenia peer-to-peer. Jedną z pierwszych sieci opartych o protokół P2P był Napster [Goos 2016: 180] uruchomiony w 1999 r. oraz Gnutella o otwartym kodzie źródłowym [Goos 2016: 180]. Jednakże pierwsza sieć była scentralizowaną, zarządzaną siecią przez jedną firmę, a Gnutella nie zachowywała żadnych reguł anonimowości, gdyż opierała się o protokół adresowania IPv4 nadawcy i odbiorcy. Dzisiaj w pełni rozproszone systemy P2P nie posiadają pojedynczych punktów awarii, jak było w przypadku Napstera, co doprowadziło do jego upadku po skutecznych atakach DDoS. W systemach opartych o Gnutellę można było zaobserwować dwie słabości: pobieranie bez skrupułów, brak anonimowości. Systemy P2P często są określane jako zdecentralizowane sieci zawierające kopie danych rozproszone pomiędzy hostami. Liczne badania wskazują, że w typowych sieciach istniały tzw. „super peery" czyli osoby, które udostępniały znacznie więcej danych niż

pobierały. Natomiast całą resztę sieci tworzyli użytkownicy „żerujący" na nich, czyli pobierający dane, a nie udostępniający, co w znacznym stopniu inhibitowało dynamikę rozwoju takiej sieci. Należało więc wprowadzić system tzw. hierarchii bądź nagradzania osób bardziej zaangażowanych w rozwój sieci. Na kanwie Gnutelli powstały takie projekty jak KazaA, czy eDonkey który przekształcił się w eMule. Następnie w roku 2008 zapanowała era protokołu BitTorrent, trwająca do dzisiaj. Jednak z boku tych sieci, niezależnie od idei pobierania rozwija się sieć TOR – sieć nie bezpośrednio związana z przechowywaniem danych, a z zachowaniem anonimowości. Pojęcie DarkNet zostało całkowicie wchłonięte jako podsieć oparta o technologię TOR.

3. SPECYFIKACJA SIECI TOR I SPOSÓB GROMADZENIA DANYCH

TOR jest nabierającym popularności systemem wzmagającym prywatność użytkownika w celu strzeżenia jego prawa do prywatności w Internecie od analizy ruchu sieciowego uruchomionego przez nieglobalnych adwersarzy. Ponieważ TOR zapewnia usługę anonimowości z wykorzystaniem TCP przy stosunkowo małym opóźnieniu i wysokiej przepustowości – jest idealnym systemem do interakcji z użytkownikiem, do których zaliczyć można: przeglądanie sieci web, udostępnianie plików i komunikatory internetowe. Technologia TOR nakłada warstwę anonimowości na warstwę TCP tworząc ścieżkę trzy-punktową przez którą routery TOR używają warstwowego szyfrowania podobnego do onion routingu [Kobayashi 2016: 17]. Informacja o trasach jest przesyłana przez grupę autorytatywnych serwerów. W uproszczeniu, wszelka komunikacja TCP użytkownika jest tunelowana w jednym węźle, który rotuje w czasie. Trzy punkty sieci TOR są określane jako: wejściowy router TOR, pośredni router TOR oraz wyjściowy router TOR. Tylko wejściowy router TOR jest w stanie obserwować ruch od oryginatora w celu nabycia wiedzy o hoście docelowym. Dodatkowo w celu zapewnienia niskich opóźnień, sieć TOR nie wymusza retransmisji zgubionych pakietów. W celu lepszego zrozumienia funkcjonowania sieci w realnym świecie, został skonfigurowany router o przepustowości 1 Gbps dołączony do sieci globalnej [Goos 2016: 184] zgodnie z topologią rys. 1. W celu zbierania statystyk należało zdefiniować polityki określające co i z którego miejsca należy zbierać, by reprezentowało to wartość statystyczną. Zdecydowano się na przechwytywanie logów z węzłów nawiązujących połączenie z routerem oraz kierowanymi dalej przez badany router. Dodatkowo należało zebrać wystarczającą ilość do przechwytywania nagłówków protokołów warstwy aplikacji modelu ISO/OSI z ruchu wychodzącego od routera. W Tabeli 1 zostały opisane protokoły warstwy siódmej, które zostały przechwycone wraz ze wskazaniem ilości. Jednakże nie da się jednoznacznie stwierdzić, czy ruch był ruchem interaktywnym, jak w przypadku typowego ruchu protokołu HTTP/HTTPS w Internecie, czy też pobieraniem plików za pośrednictwem tego protokołu (co jest często spotykane w sieci TOR i BitTorrent).

Tabela 1. Zebrane protokoły warstwy aplikacji

PROTOKÓŁ	LICZBA POŁĄCZEŃ	LICZBA DANYCH
HTTP + SSL	13 145 103	422 GB
BitTorrent	438 395	285 GB
SMTP	7611	291 MB
FTP	1337	792 MB

Źródło: http://www.bearcave.com/misl/misl_tech/msdrm/darknet.htm

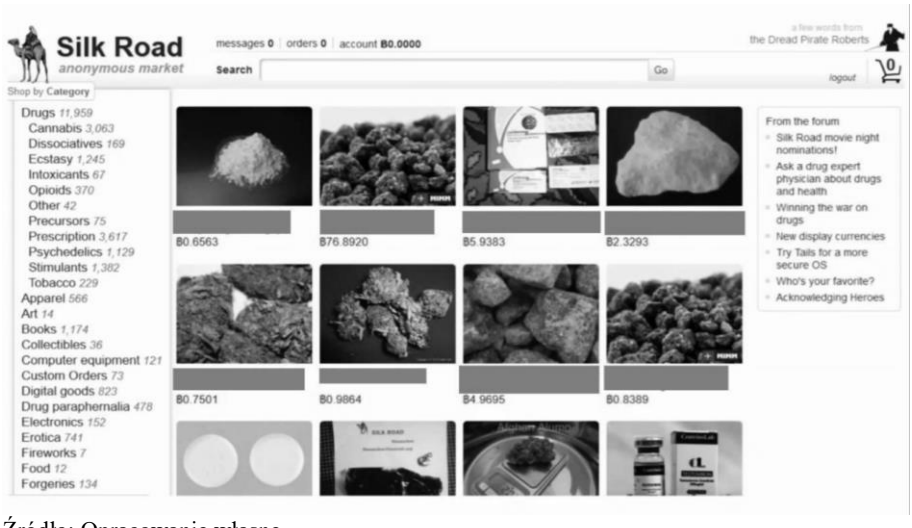
Ponieważ ruch sieciowy protokołu HTTP zdecydowanie dominuje w statystykach połączeń do routera należało przyjąć kryterium wskazujące, które połączenie mogło być interaktywne, a które nie. Dla danych statystycznych przyjęto, że ruch powyżej 1 MB danych stanowił połączenia nieinteraktywne przy założeniu, że strony internetowe w sieci TOR nie mają skomplikowanej konstrukcji. Zaledwie 3.5 % danych zostało w ten sposób określone [http://www.bearcave.com/misl/misl_tech/msdrm/darknet.htm]. Jednakże najbardziej znaczącym protokołem w stosunku liczby połączeń TCP jest protokół BitTorrent, który wykorzystywał nieproporcjonalnie dużą wartość pobieranych danych. Można było się spodziewać, że względu na fakt, że protokół jest częścią klienta P2P (np. uTorrent) służącego do pobierania plików. Jednakże pełna liczba połączeń TCP po protokole HTTP może wskazywać, że jest to ruch przechodzący przez anonimowych klientów usługi proxy. Niezwykłą obserwacją jest także fakt, że na liście znajdują się trzy protokoły uznawane za niebezpieczne. Protokoły POP, SMTP oraz FTP bez szyfrowania SSL są stosunkowo proste do przechwycenia i rozszyfrowania komunikacji w postaci otwartego tekstu. Sieć TOR multipleksuje połączenia TCP tego samego węzła, co oznacza, że przechwycenie ruchu jest stosunkowo prostsze niż w tradycyjnym Internecie (składanie pakietów i numerów kontrolnych). Biorąc pod uwagę stosunkowo dużą ilość niebezpiecznego ruchu, który można obserwować, to istnieje wielka zachęta dla potencjalnych napastników tworzących złośliwe oprogramowanie na stronach internetowych do infekowania komputera użytkownika.

4. NIELEGALNE SPOSOBY ZASTOSOWANIA SIECI TOR

Nie podlega dyskusji, że technologia TOR oraz wczesna sieć DarkNet dzisiaj stanowią jedną całość. Ideologiczna sieć DarkNet służy do dystrybucji, współdzielenia nielegalnych treści, a technologia TOR zapewnia anonimowość, a tym samym pewien sposób bezkarności. Jednoznacznie nazwany dzisiaj współczesny DarkNet, jest magistralą łączącą ideę nielegalnego współdzielenia i pozyskiwania danych z wykorzystaniem technologii TOR. Sieć DarkNet oparta o TOR jest dzisiaj jednym z głównych kanałów komunikacji przestępców oraz

serwisów oferujących nielegalne usługi i towary. Jednym z najbardziej znanych sklepów jest Silk Road (rys.2) oferujący międzynarodową sprzedaż narkotyków.

Rysunek 2. Zrzut ekranu ze sklepu Silk Road w sieci DarkNet



Źródło: Opracowanie własne

Niestety sieci DarkNet nikt nie kontroluje i nie jest ona w żadnym stopniu ustandaryzowana.

Co więcej, ideologicznie, samoczynnie zachęca do bycia przestępcą operując socjotechnicznie na wartościach takich jak ciekawość czy pobudzenie. Zgodnie z badaniami przedstawionymi wyżej, ruch w sieci nie jest w większości przypadków szyfrowany. Powodowałoby to dodatkowy impakt i trudności w działaniu, co negatywnie wpłynęłoby na popularność serwisów. Jednakże użytkownicy korzystający z sieci DarkNet muszą być świadomi, że poza infekcją swojego komputera w pewien sposób narażają się służbom monitorującym. Użytkownik ciekawy sieci DarkNet z reguły łączy się ze swojego domowego komputera, od jednego dostawcy Internetu. W przypadku wykrycia przez dostawcę anomalnego ruchu ze znacznikami wskazującymi na ruch DarkNet – służby mogą poprosić o logi od operatora, by jednoznacznie namierzyć użytkownika. Oczywiste jest, że z racji braku kontroli, nie ma formalnie mechanizmu pomocy w przypadku zostania ofiarą oszustwa. Najczęściej dochodzi do utraty pieniędzy, nieuprawnionego lub nieświadomego przekazania danych osobowych. Handel fałszywymi dokumentami (rys.3) jest bardzo powszechny w sieci DarkNet i stanowi główne źródło zarobkowania przestępców, którzy swoją płatność otrzymują w krypto-walucie (także anonimowej) – głównie BitCoin (BTC) i Monero (XMR).

Rysunek 3. Zrzut ekranu ze sklepu oferującego fałszywe paszporty do UK

Źródło: Opracowanie własne

Rysunek 4. Zrzut ekranu ze oferującego usługi płatnego zabójstwa

Źródło: Opracowanie własne

Znacznie rzadziej spotyka się strony z „poważniejszymi" usługami, jak płatne zabójstwo (rys.4) czy strony terrorystyczne. Przestępcy administrujący tymi stronami mają świadomość, że upublicznienie nawet w anonimowej sieci powoduje potencjalne zostawianie śladów i namierzenie przez służby. Dlatego tak jak

w życiu realnym, tak samo w sieci DarkNet istnieje łańcuch powiązań i zaufanych osób (w tym wypadku – zaufanych węzłów), które udostępniają „klientom" hiperłącze TOR do usługi, gdy zostaną oni zweryfikowani.

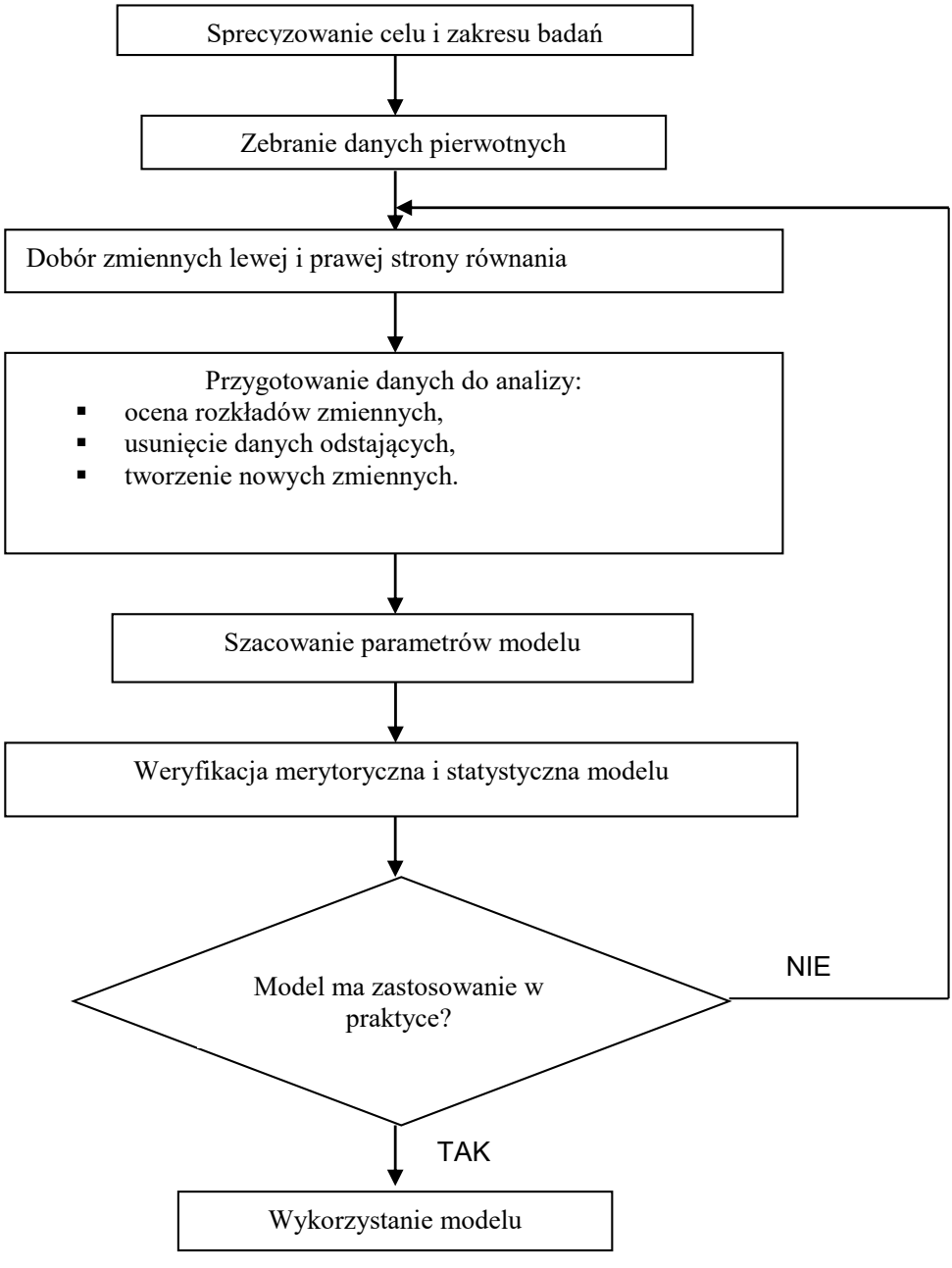
5. LEGALNE SPOSOBY ZASTOSOWANIA SIECI TOR

Nie podlega też dyskusji, że sieć TOR sama w sobie nie jest zagrożeniem technologicznym, a jedynie umożliwia pewną dystrybucję treści, których legalność jest ustanawiana warstwy wyżej – na podłożu regulacji prawnych. Jednoznacznie ideowo sieć TOR jest bardzo dobrym rozwiązaniem technologicznym, zwłaszcza w kontekście wprowadzonej dyrektywy RODO. Technologia ta zapewnia użytkownikowi anonimowość do której ma on prawo. Dodatkowo istnieje sporo serwisów w DarkNecie oferujących profesjonalne szyfrowanie VPN za niewielkie pieniądze, co daje użytkownikowi możliwość przesyłania newralgicznych plików w sposób zabezpieczony. Rozważyć należy także sytuację, w której użytkownik często do wykonania jakiejś czynności w aplikacji internetowej, zobowiązany jest podać swój adres e-mail. Nie chce jednak tego robić i w tym momencie musi z usługi zrezygnować lub skazać się na „wieczny" spam na swojej skrzynce. Usługi DarkNetu oferują jednorazowe konta e-mail potrzebne do rejestracji, a później „zapomnienie o nich", tym samym użytkownik może zachować czystość swojej skrzynki e-mail. Jednym z największych profitów ostatnich lat jest niewątpliwie pojawienie się serwisu WikiLeaks. Serwis służy do informowania społeczeństwa o wyciekach poufnych dokumentów rządowych. Przeglądając tradycyjny Internet, użytkownik bardzo często nie wie że jego zachowania i dane osobowe są właśnie przetwarzane. Przykładem jest usługa AdContent, AdWords od firmy Google lub Cortana z systemu Windows firmy Microsoft. Wszystkie te usługi łączy jeden cel – profilowanie reklamy dostarczanej do użytkownika w celu trafienia w jego gusta, co spowoduje jego zainteresowanie i zakup. Prawidłowo wyświetlane nam reklamy zawdzięczamy głównie wyszukiwarce Google, która kataloguje wszelkie możliwe dane. W/w. wyszukiwarka ogranicza także pewne wyniki wyszukiwań, co nie każdemu może się podobać. W sieci DarkNet, a także w Internecie powstała konkurencja – wyszukiwarka DuckDuckGo, która nie indeksuje wszystkiego co robi użytkownik, nie dostarcza reklam, a także nie blokuje dostępu do dowolnych treści. Jest to niewątpliwie ważny aspekt w dobie ochrony danych osobowych.

6. PODSUMOWANIE

W artykule opisano historyczny zarys sieci określanej jako „Darknet" (tzw. czarny rynek), który wyewoluował do postaci technologicznej z pomocą sieci TOR, która zapewnia anonimowość. Pomimo, że przesłanki do stworzenia sieci TOR są znane, to jednak należy poddać wątpliwość, czy nie jest to kolejna z usług po nawigacji satelitarnej GPS, Google'u oraz Facebook'u, która została udostępniona ludzkości za darmo, a tak naprawdę jest kolejnym narzędziem służb specjalnych do kontroli wszystkiego, co się dzieje na świecie. Sieć TOR

może służyć zarówno rozwiązaniom legalnym, jednak z uwagi na zebrane staty-



POLITECHNIKA OPOLSKA

ISSN 2353-8899