THE ONION ROUTER (TOR) – ZAGROŻENIEM DLA BEZPIECZEŃSTWA GLOBALNEGO

Leszek LISIECKI

Wojskowa Akademia Techniczna

Kamil KUCHARSKI[1]

Wojskowa Akademia Techniczna

Streszczenie. Rewolucja informacyjna i informatyczna, a także wydarzenia i kampanie medialne związane z problemem ochrony prywatności w Internecie, determinują rzeczywistość społeczno-gospodarczą współczesnego świata. Odpowiedzią na potrzebę zachowania anonimowości jednostki jest sieć TOR. Zasady funkcjonowania oraz możliwości sieci TOR, które udostępnia swoim użytkownikom, doprowadziły jednak do rozwoju zjawiska cyberprzestępczości w nowym wymiarze. Przedmiotem artykułu są zasady działania TOR oraz zjawiska patologiczne w tej sieci. Jej silna integracja z anonimową walutą Bitcoin może w przyszłości przyczynić się do powstania nowych zagrożeń o charakterze globalnym.
Słowa kluczowe: TOR, Bitcoin, anonimowość, cyberbezpieczeństwo, przestępczość zorganizowana.

WSTĘP

Przestrzeń teleinformatyczna, wraz z rozwojem informatyki i informatyzacji stała się nowym obszarem funkcjonowania współczesnego człowieka. Zdaniem organizacji międzynarodowej Internet Society zajmującej się m.in. popularyzacją World Wide Web –„Internet daje możliwość, jednocześnie na całym świecie nadawania i rozpowszechniania informacji. Jest medium współpracy i interakcji między ludźmi a komputerami, bez względu na położenie geograficzne”[2]. Naturalnie więc wykorzystanie World Wide Web to jeden z obszarów zainteresowań krajów zaangażowanych w prowadzenie działań wojennych (element konfliktu hybrydowego)[3] oraz przestępców, którzy do realizacji swojej działalności starają się wykorzystywać coraz to nowe rozwiązania techniczne.

---

[1] Doktorant WCY WAT

[2] D. Marczuk, K. Kucała, *Wolność słowa w świecie wirtualnym - wartość nadużywana,* w: J. Bednarek, A. Andrzejewska (red.), *Zagrożenia cyberprzestrzeni i świata wirtualnego*, Difin, Warszawa 2014, s. 148.

[3] Grzegorz Kostrzewa-Zorbas zauważa, że na szczycie Sojuszu Północnoatlantyckiego w Walii w 2014 r. NATO uznało, że cyberobrona jest częścią zbiorowej obrony jako centralnego zadania sojuszu i że atak cybernetyczny wpisuje się w znamiona agresji opisywanej w art. 5 Traktatu Północnoatlantyckiego. Więcej na ten temat: G. Kostrzewa-Zorbas, *NATO w nowym środowisku strategicznym: cyberataki podlegają już artykułowi 5 traktatu północnoatlantyckiego*, w: *Studia Bezpieczeństwa Narodowego WAT nr 6 Kryptologia i Cyberbezpieczeństwo*, WAT, Warszawa 2016, s. 339-410.

Rewolucja informacyjna, która również determinuje intensywność procesu globalizacji, wpłynęła znacząco na zmianę modelu komunikacji społecznej, ułatwiając nawiązywanie kontaktu między ludźmi przy jednoczesnym ograniczaniu bezpośredniej interakcji. Rozwój narzędzi anonimizujących w Internecie stworzył jednocześnie dobre warunki i środowisko do nasilenia się zjawiska przestępczości w sieci. Najbardziej popularnym narzędziem wykorzystywanym przez przestępców do szeroko zakrojonych działań bezprawnych jest sieć TOR (*The Onion Router*).

Zasady działania sieci TOR

Sieć TOR należy do części tzw. głębokiego Internetu (ang. *deep web*) i stanowi niezwykle ważną jego część. Według „The Guardian" znane silniki wyszukiwarek internetowych takie jak Google czy Yahoo mają dostęp jedynie do 0,03% zasobów Internetu[4]. Pozostała część to ukryta sieć, do której dostęp mają użytkownicy korzystający z odpowiedniego oprogramowania i posiadający fachową wiedzę. TOR samą nazwą obrazuje zasady funkcjonowania tej sieci. Odwołuje się ona do warstwowości cebuli (*onion*), która przez swoją budowę uniemożliwia bezproblemowe sprawdzenie tego co znajduje się w środku.

Proces tworzenia sieci TOR trwał kilka lat, a za początek jej działalności przyjmuje się rok 2003, kiedy to zaczęła funkcjonować przy wsparciu Marynarki Wojennej USA. W 2004 roku sieć została przejęta przez prywatny podmiot – firmę Electronic Frontier Foundation. Obecnie rozwijają ją sami użytkownicy (współtworzący organizację non-profit o nazwie TOR Project), którzy podłączając się do TORa tworzą kolejne warstwy tej najpopularniejszej sieci anonimowej komunikacji na świecie. Siedziba TOR Project znajduje się w Stanach Zjednoczonych[5].

Zabezpieczenie ruchu sieciowego w sieci TOR przebiega w kilku etapach. Pierwszym krokiem jest uruchomienie aplikacji TOR, która jest przeglądarką przypominającą wizualnie zmodyfikowany program Mozilla Firefox. Po jej uruchomieniu użytkownik pobiera listę węzłów z oficjalnego serwera. Próbując połączyć się z innym serwerem (np. udostępniającym usługę witryny internetowej) łączy się z losowym węzłem. „Na początku każdy pakiet danych ma ustalaną drogę wybieraną z listy węzłów. Istotnym jest, że żaden węzeł nie zapamiętuje tego co otrzymał, odkodował i przesłał dalej. Generalnie ujmując strukturę TOR należy wyróżnić trzy rodzaje węzłów:

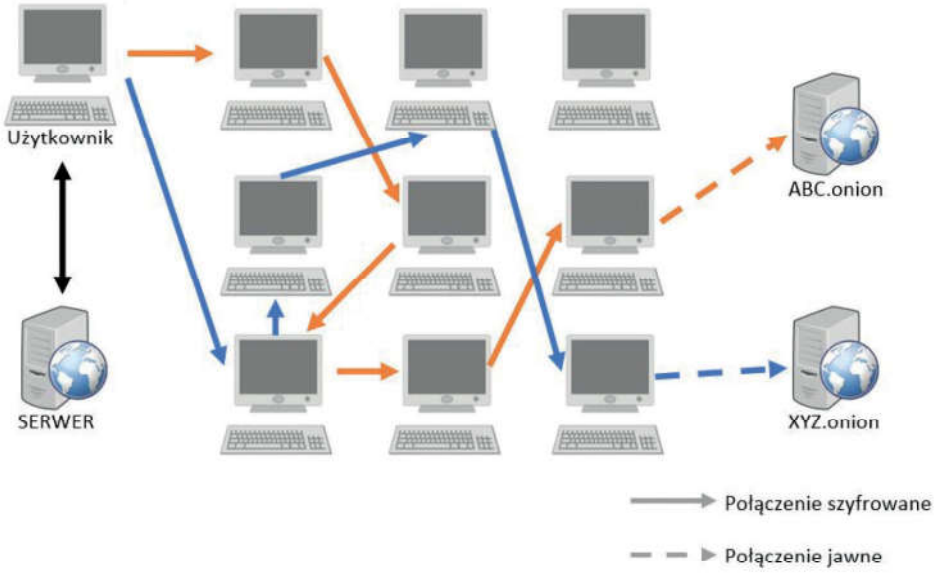
1. Wejściowy – EntryNode.
2. Przekaźnikowy – RelayNode.
3. Wyjściowy – ExitNode"[6].

[4] http://www.sickchirpse.com/deep-web-guide/

[5] http://www.onion-router.net/History.html

[6] M. Górka, *Cyberbezpieczeństwo jako podstawa bezpieczeństwa państwa i społeczeństwa w XXI wieku*, Difin, Warszawa 2014, s. 37.

Kolejno pakiet danych łączy się do innych losowych węzłów przekaźnikowych aby ostatecznie tzw. węzeł brzegowy/wyjściowy połączył się z serwerem. Warto zaznaczyć, że połączenie pomiędzy ostatnim węzłem a serwerem jest jawne (ostatni węzeł rozszyfrowuje dane), natomiast wszystkie połączenia między węzłami przekaźnikowymi są szyfrowane. Cała sieć TOR jest zdecentralizowana. Charakterystyczną cechą witryn w sieci jest alias domeny. W Internecie przyjęło się wiele oznaczeń, które zwykle utożsamiają domenę z krajem lub prowadzoną działalnością. Przykładem jest *.pl dla Polski, *.de dla Niemiec czy *.co.uk dla Wielkiej Brytanii. Inne aliasy to np. *.org dla organizacji lub *.gov dla witryn rządowych. Sieć TOR posiada alias *.onion, który znajduje się za dodatkowym firewallem oraz jest ukryty przed Network Adress Translation (NAT) tj. usługą, która zmienia adres strony na bardziej czytelny. W konsekwencji adresy w sieci TOR to ciągi losowych znaków. Jest to właściwość, która dodatkowo utrudnia znalezienie odpowiedniej witryny. Mówiąc inaczej – dostęp do właściwych treści mają osoby, które wiedzą jak ich szukać. W odpowiedzi na to powstały serwisy funkcjonujące zarówno w sieci TOR, jak i w ogólnodostępnym Internecie, które zawierają listy serwerów TORa. W przeciwnym razie dostęp do niektórych usług byłby praktyczne niemożliwy[7]. Sposób działania sieci TOR został przedstawiony na schemacie 1 na następnej stronie.



Rys. 1. Przepływ pakietu danych w sieci TOR
Źródło: Opracowanie własne na podstawie M. Górka, *Cyberbezpieczeństwo jako podstawa bezpieczeństwa państwa i społeczeństwa w XXI wieku*, op. cit., s. 35-38

[7] Ibidem, s. 37-38.

Użytkownik po pobraniu listy dostępnych węzłów (strzałka czarna) wpisuje w przeglądarkę adres, z którym chce się połączyć (np. ABC.onion – połączenie pomarańczowe). W kolejnym kroku pakiet danych wysyłany jest do losowego węzła, który przekazuje go do kolejnego losowego węzła, aż do trafienia na węzeł brzegowy. Węzeł brzegowy po rozszyfrowaniu danych zwraca się do serwera o udostępnienie usługi np. witryny albo przesłania plików. Wówczas na ekranie użytkownika pojawia się obraz domeny (w pierwszym przypadku ABC.onion).

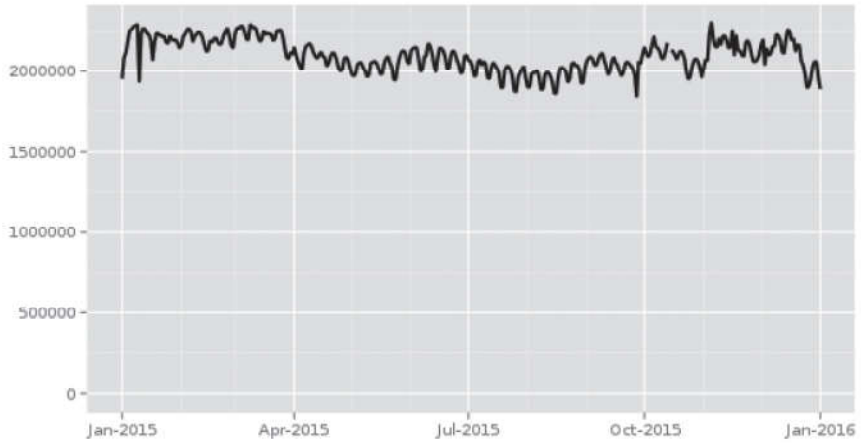
Kiedy użytkownik chce otworzyć inną witrynę (np. XYZ.onion – strzałki niebieskie) wszystkie czynności wykonywane są analogicznie, ale zmienia się trasa przesyłanego pakietu danych. Co więcej – nawet powtórne połączenie się do przykładowej witryny ABC.onion nie odbywa się dwa razy przez taką samą trasę węzłów. Takie zasady funkcjonowania TORa sprawiają, że niemożliwym jest zidentyfikowanie osoby, która wysyła zapytanie do sieci.

TOR tworzą użytkownicy, którzy łączą się z siecią. Każdy dodatkowy komputer korzystający z TORa może być węzłem przekaźnikowym lub brzegowym. W związku z tym sieć się rozrasta, tworząc pajęczynę powiązań, które uniemożliwiają zidentyfikowanie jej poszczególnych użytkowników. Skalę przedsięwzięcia obrazuje wykres 1 (na następnej stronie) przedstawiający liczbę użytkowników TOR na całym świecie w okresie od 01.01.2015r. do 01.01.2016 r.

Jak widać, popularność usługi oscyluje w granicach 2 mln użytkowników każdego dnia. TOR działa w każdym kraju na świecie gdzie dostępny jest Internet i komputer. Oznacza to, że możliwość zidentyfikowania osoby znajdującej się po drugiej stronie monitora jest prawie niemożliwa. Trzeba jednak pamiętać istnieje kilka zasad, których należy przestrzegać podczas korzystania z TORa, aby pozostać w pełni anonimowym[8].

Medialne afery wywołane takimi wydarzeniami jak wystąpienie Edwarda Snowdena czy ACTA oraz ogólnoświatowy protest grupy hakerów Anonymous sprawiają, że społeczność internetowa na całym świecie stara się znaleźć rozwiązanie dla zachowania prywatności. Wynika to zarówno z przesłanek społecznych, jak i ekonomicznych. Prawo do prywatności stało się jednym z determinantów poczucia bezpieczeństwa. W związku z tym sieć TOR oraz wykorzystywany w niej Bitcoin (który podobnie zapewnia anonimowość, co zostało opisane w artykule *Anonimowość Bitcoin zagrożeniem bezpieczeństwa*) znajdują coraz więcej zwolenników na całym świecie.

[8] Szerzej na ten temat: K. Kucharski, *Narzędzia anonimizujące działania w Internecie jako instrumentarium do prowadzenia operacji informacyjnych w ramach wojny hybrydowej*, Przegląd Bezpieczeństwa Wewnętrznego ABW – Wydanie specjalne – Wojna hybrydowa, ABW, Warszawa 2015, s. 92-93.



Wykres 1. Liczba użytkowników TOR na świecie. Okres od 1 stycznia 2015 r. do 1 stycznia 2016 r.
Źródło: *metrics.torproject.org*

Sieć TOR jako czarny rynek

Sieć TOR to środowisko zapewniające anonimowość i gwarantujące prawo do prywatności. Współczesne społeczeństwo decyduje się na korzystanie z tego narzędzia głównie za sprawą medialno-politycznych kampanii pokazujących jak głęboko podmioty państwowe i rządowe są w stanie wkraczać w sferę prywatną jednostki. Warto zaznaczyć, że do prowadzenia tzw. białego wywiadu tj. opierającego się jedynie o źródła otwarte, nie potrzeba zaawansowanej wiedzy. W Internecie powstaje szereg witryn zajmujących się przekazywaniem doświadczenia i narzędzi do prowadzenia wywiadu z jawnego źródła[9].

Mogłoby się wydawać, że anonimowy Internet będzie miejscem bezpiecznym. Korzysta z niego ograniczona liczba osób (tylko jednostki zainteresowane). Ponadto każdy użytkownik jest anonimowy, więc treści, które przegląda w żaden sposób nie narażają go na stratę (w szerokim ujęciu). Mimo tego należy zaznaczyć, że serwisy funkcjonujące w sieci TOR to często społeczność, która zainteresowana jest prowadzeniem nielegalnej działalności. Tak więc bezpieczeństwo TOR pozostaje jedynie w zakresie prywatności jego użytkowników.

Prowadzenie nielegalnej działalności w sieci TOR jest możliwe dzięki założonym tam forom internetowym działającym na zasadach e-sklepów. Serwery TOR, na których funkcjonują takie usługi, również są anonimowe, dlatego służby, które starają się przeciwdziałać temu zjawisku mają utrudnione zadanie. Najbardziej znanym serwisem

[9] http://osintinsight.com/

oferującym nie tylko narkotyki, ale również pornografię dziecięcą, materiały wybuchowe oraz rozwiązania dotyczące oszustw podatkowych, był Silk Road, którego założycielem był Ross Ulbricht[10]. Forum funkcjonowało od 2011 roku. Na początku października 2013 roku każdy użytkownik korzystający z sieci TOR, który próbował połączyć się z forum Silk Road został poinformowany, że forum przejęło i zamknęło FBI. Komunikat pojawiający się przy połączeniu z Silk Road przedstawia rysunek 2.

Rys. 2. Informacja FBI o zamknięciu forum Silk Road
Źródło: *niebezpiecznik.pl*

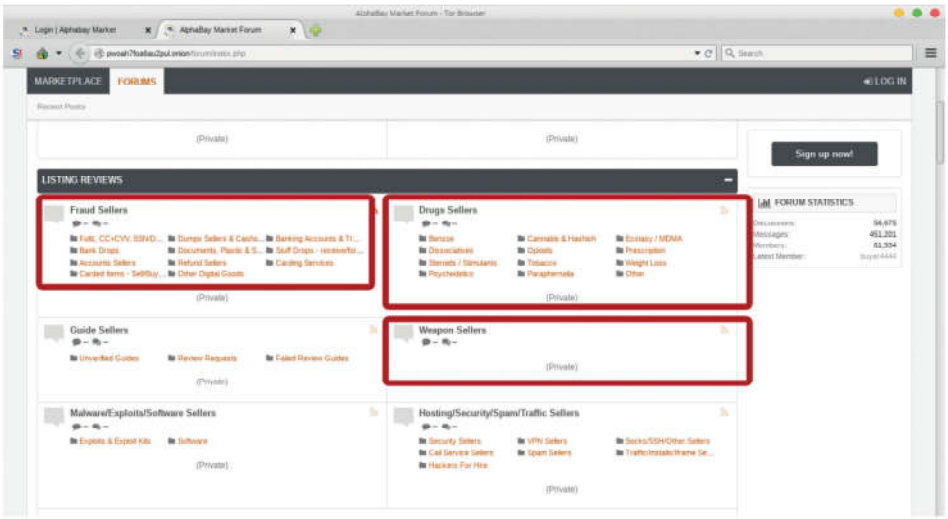
Wówczas w Internecie rozpoczęła się dyskusja dotycząca tego czy TOR jest faktycznie dobrym narzędziem do zachowania anonimowości w sieci? Okazało się, że tak, bo opublikowane materiały dotyczące zatrzymania twórcy Silk Road pokazały, że do przejęcia forum nie doszło w wyniku błędów sieci TOR, ale przez nieuwagę samego założyciela. Analiza dokumentacji wskazała, że podstawowym błędem administratora Silk Road było łączenie działalności w sieci TOR z działalnością w jawnym Internecie. Korzystał on bowiem z takich samych pseudonimów reklamując stworzone przez siebie forum. Punktem zwrotnym w śledztwie prowadzonym przez FBI było zatrzymanie przesyłki adresowanej do Rossa Ulbrichta, która zawierała 9 fałszywych dowodów tożsamości. Wówczas to administrator miał się tłumaczyć, że zamówił je na forum Silk Road[11].

[10] http://freeross.org/

[11] http://niebezpiecznik.pl/post/silk-road-najwiekszy-sklep-z-narkotykami-w-internecie-zamkniety-fbi-namierzylo-i-aresztowalo-jego-tworce/

Zamknięcie najpopularniejszego serwisu oferującego nielegalny obrót narkotykami i innymi towarami zabronionymi nie zahamowało rozwój tego typu działalności w sieci TOR. Silk Road stał się prekursorem nielegalnych sklepów w anonimowym Internecie. Liczba podobnych serwisów rośnie z roku na rok. Co gorsze – zwiększa się również liczba użytkowników, którzy bezkarnie obracają nielegalnymi towarami w sieci. Obecnie najpopularniejszym sklepem w skali międzynarodowej, który działa na wzór Silk Road, jest AlphaBay Market[12].

Na dzień 1marca 2016 roku serwis AlphaBay Market posiadał 61 931 zarejestrowanych użytkowników, którzy napisali 451 207 postów w 56 675 tematach. Forum zawiera panele dyskusyjne, w których znajdują się oferty użytkowników dotyczące pornografii, narkotyków, Bitcoinów, sposobów na wyłudzenia oraz innych kwestii związanych z działalnością przestępczą. Spektrum ofert na forum jest bardzo szerokie – użytkownicy oferują wszelkie rodzaje narkotyków, od tzw. miękkich takich jak konopie indyjskie, aż po heroinę, kokainę i inne substancje psychodeliczne. Na AlphaBay Market można nabyć pornografię dziecięcą i inną – np. nielegalne prywatne zdjęcia. Rysunek 2(na następnej stronie) przedstawia wycinek przykładowych paneli dyskusyjnych założonych przez użytkowników AlphaBay Market.



Rys. 3. Przykładowe panele dyskusyjne założone przez użytkowników AlphaBay Market
Źródło: Opracowanie własne, według stanu na 1 marca 2016 r.

Na podstawie przedstawionego poniżej zdjęcia można stwierdzić, że użytkownicy TOR realizują swoją nielegalną działalność bez poczucia strachu i zagrożenia

[12] pwoah7foa6au2pul.onion

poniesieniem konsekwencji. Oferty na AlphaBay Market można liczyć w tysiącach, a ich ilość wciąż wzrasta. Serwis funkcjonuje na zasadach swoistego internetowego bazaru produktów. Każdy z zarejestrowanych użytkowników ma prawo założyć swój własny temat ogłaszając towar, który oferuje. Co więcej każdy – bez jakiejkolwiek weryfikacji (np. wieku) – jest w stanie odpowiadać na zamieszczone ogłoszenia, kontaktować się z ich autorem i ostatecznie nabywać nielegalny towar. System rejestracji wymaga jedynie podania nazwy użytkownika oraz hasła. W serwisie AlphaBay Market, w odróżnieniu do innych serwisów tego typu, nie występuje ograniczony dostęp do forum, tj. konieczność posiadania tzw. *referral link* – zaproszenia od jednego z już zarejestrowanych użytkowników. Najniebezpieczniejszym aspektem funkcjonowania tego typu serwisów jest opisywana wcześniej anonimowość, która eliminuje możliwość ustalenia tożsamości oraz miejsca zamieszkania konkretnego użytkownika. Weryfikacja jakości i rzetelność oferowanych usług została rozwiązana w sposób prosty i skuteczny. W serwisach tego typu często funkcjonują oceny (zarówno sprzedawcy i dostarczanego przez niego towaru, jak i kupującego). Na podstawie systemu recenzji – nowi członkowie społeczności TOR weryfikują i wybierają m.in. dostawcę narkotyków, czy broni.

Warto zaznaczyć, że oprócz użytkowników oraz ich aktywności, która rośnie z dania na dzień, wzrasta również ilość serwisów działających na zasadach prekursorskiego Silk Road, czy też najbardziej popularnego obecnie AlphaBay Market. Zestawienie wybranych popularnych serwisów wzorujących się na Silk Road oraz Agora Forum przestawia tabela 1 na następnej stronie.

Tabela 1. Serwisy oferujące sprzedaż nielegalnych towarów w sieci TOR

L.p.	Nazwa	Adres
1.	AlphaBay	http://pwoah7foa6au2pul.onion
2.	Dream Market	http://lchudifyeqm4ldjj.onion
3.	Valhalla (Silkkitie)	http://valhallaxmn3fydu.onion
4.	Outlaw Market	http://outfor6jwcztwbpd.onion
5.	Python Market	http://25cs4ammearqrw4e.onion
6.	Tochka	http://tochka3evlj3sxdv.onion
7.	Acropolis Market	http://acropol4ti6ytzeh.onion
8.	TheRealDeal	http://trdealmgn4uvm42g.onion
9.	The Majestic Garden	http://bm26rwk32m7u7rec.onion
10.	Nucleus Market	http://nucleuspf3izq7o6.onion
11.	Ramp (Russian Forum)	http://ramp2bombkadwvgz.onion
12.	Oasis Market	http://oasisnvwltxvmqqz.onion
13.	Bloomsfield	http://spr3udtjiegxevzt.onion
14.	Crypto Market	http://cryptomktgxdn2zd.onion
15.	Havana Marketplace	http://havana3cofejesta.onion

Źródło: opracowanie własne, stan na 1 marca 2016 r.

Powyższe zestawienie pokazuje skalę problemu, który dotknął współczesny świat. Użytkownicy sieci bez trudu, po krótkiej kwerendzie Internetu, są w stanie odnaleźć adres każdego z powyższych sklepów TOR. Warto zwrócić uwagę, że oferta tych serwisów jest bogata. Różnią się one tylko samym sposobem działania.

Nowatorskie podejście w tym zakresie wdrożył serwis Tochka, gdzie cały system kupna i sprzedaży został opracowany przez jego twórców. Transakcje przeprowadza się bez konieczności kontaktu ze sprzedającym lub kupującym (tak jak np. w popularnych na całym świecie serwisach aukcyjnych). Kupno i sprzedaż przebiegają błyskawicznie, a co istotne – niezadowolony klient jest w stanie ubiegać się o zwrot pieniędzy. Wśród wymienionych serwisów wyróżnia się również The Real Deal gdzie oprócz tradycyjnych narkotyków, kupujący jest w stanie nabyć exploity[13] (program wykorzystujący błędy w zabezpieczeniach, za pośrednictwem którego haker włamuje się do systemu), kody źródłowe oraz sprzęt i oprogramowanie komputerowe (np. szpiegujące).

Co więcej, sklepy internetowe oferujące produkty nielegalne znajdują się również w polskiej części sieci TOR. Jednym z przykładów był funkcjonujący od kilku lat Polish Black Market – założony przez użytkownika o pseudonimie Zdzisław Dyrma. Na dzień 1 maja 2015 roku serwis składał się z 2 681 zarejestrowanych użytkowników, którzy napisali 40 360 postów w 4 204 tematach. Historia polskiej wersji Silk Road jest krótka, bo forum miało duże problemy w funkcjonowaniu. Obecnie dostępna witryna zawiera całe archiwum z działalności do 2013 roku. Założyciel forum deklaruje, że dla zarejestrowanych użytkowników dostępne są 24 tematy główne, a w tym:

- anonimowość fizyczna (przebrania, przesyłki, ucieczka, dokumenty);
- anonimowość w Internecie (TOR, VPN, Proxy);
- hacking, carding, phreaking (przejmowanie kont, wycieki baz, wyłudzenia Allegro, simlocki);
- motoryzacja (przemyt, dokumenty);
- alchemia (narkotyki, przepisy, dystrybucja, dawkowanie);
- finanse (unikanie podatków, konto „na słupa");
- kradzieże (w domu, w sklepie, kieszonkowcy, napady);
- oszustwa (wyłudzenia, oszustwa urzędowe, podróbki);
- porachunki (zemsta, walka wręcz, szantaż, stalking);
- prawo (unikanie odsiadki, nowe przepisy);
- pornografia (od 15 lat, porady, gwałt, prostytucja);
- sklep[14].

Kontynuatorem Polish Black Market stało się forum Victoria[15] stworzone przez tego samego użytkownika – Zdzisława Dyrmę. Na tym forum (na dzień 1 maja 2015

[13] https://www.exploit-db.com/

[14] Opracowanie własne na podstawie danych zawartych w witrynie ig6ndt6anbg2dimk.onion.

[15] Forum Victoria obecnie nie funkcjonuje.

roku) zarejestrowanych było 1 562 użytkowników, którzy napisali 13 731 postów w 1 638 tematach. Victoria to swoisty klon Polish Black Marketu – zawiera wszystkie tematy, które były przedmiotem jego zainteresowania. Ponadto część użytkowników ze starego serwisu przeniosła się do nowej odsłony. Forum miało rozwinięty dział poświęcony narkotykom, oszustwom podatkowym i wyłudzeniom. Ponadto użytkownicy aktywnie tworzą tzw. profile, czyli tematy poświęcone konkretnym osobom (przede wszystkim kobietom)i zamieszczają ich dokładne dane osobowe (łącznie z wzrostem, wagą, CV, skanami dowodu osobistego lub paszportu i innych dokumentów) oraz kompromitujące zdjęcia wykradnięte z prywatnych komputerów. Profile tworzone są głównie w celu szantażowania tych osób.

Warto zaznaczyć, że Polish Black Market i Victoria to nie jedyne polskie inicjatywy funkcjonujące w sieci TOR na wzór Silk Road oraz Agora Forum. Przykładowe inne serwisy tego typu to Polish Underground, Poligamia, Cebulka, PolishOnion Forum, Anonimowa Polska, ToRepublic oraz PolishOnionPalace[16]. Obecnie żaden z wyżej wymienionych serwisów, z nieznanych przyczyn, nie jest dostępny.

Funkcjonowanie „czarnych sklepów" w anonimowym Internecie jest przesłanką do stwierdzenia, że postęp niesie ze sobą nie tylko pozytywne zjawiska, ale również szereg zagrożeń. Działalność przestępcza staje się łatwiejsza, bo kontakt bezpośredni został ograniczony do niezbędnego minimum. Warto zastanowić się co dalej? Niewykluczone, że zorganizowane grupy przestępcze i terroryści stworzą swoje własne serwisy – dostępne tylko dla ścisłego grona członków, gdzie będą mogli w prosty sposób wymieniać informacje i doświadczenia, a także debatować na temat przyszłych planów. Nie można zaprzeczyć, że takie rozwiązania już funkcjonują, albo są już w zaawansowanej fazie koncepcyjnej.

Bitcoin i sieci TOR

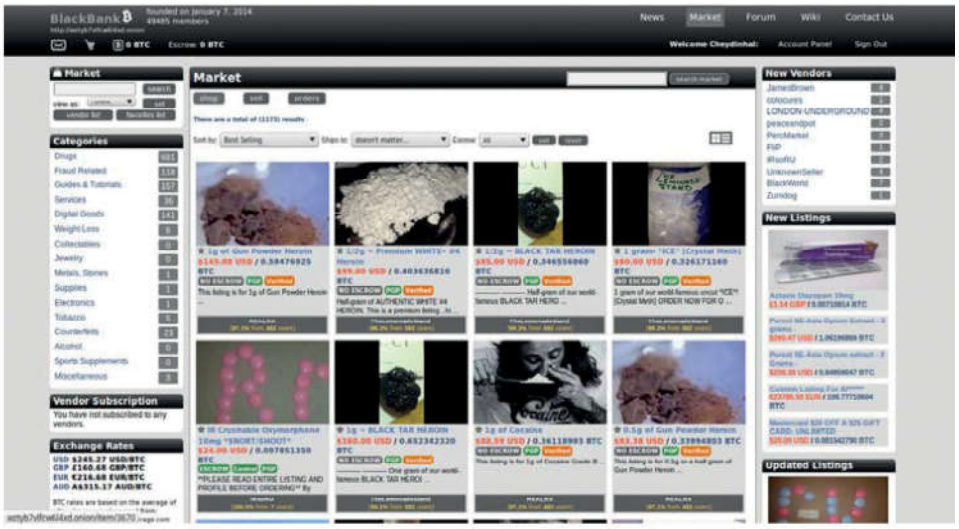
Bitcoin (BTC), mimo tego, że jest odpowiednikiem pieniądza, nie jest tak znany jak złotówka, dolar czy funt. Szczególnie osobom, które nie wychowały się w erze Internetu, trudno jest zrozumieć całą ideę i sposób funkcjonowania tej waluty. System, mimo że jest dość intuicyjny – jeszcze nie jest tak popularny jak dotychczasowe formy pieniądza. Należy jednak stwierdzić, że grono jego zwolenników oraz ilość sklepów i usług akceptujących płatność w tej walucie wzrasta. Bardzo istotnym aspektem wpływającym na jego popularność jest kurs elektronicznej waluty, który nie jest stabilny.

Kwestia popularności Bitcoina jest zupełnie inna, kiedy przeanalizujemy zasoby ukrytego Internetu. BTC w sieci TOR jest nieodłącznym elementem anonimowego

[16] http://zaufanatrzeciastrona.pl/post/siedmiu-nastepcow-pbm-ktory-z-nich-przetrwa-pozostalych/

systemu. Można stwierdzić, że TOR byłby tworem niekompletnym, gdyby nie funkcjonowanie anonimowej e-waluty.

Osoby badające problematykę Bitcoina podkreślają, że swoistą zmianę oblicza zanotował on od momentu powstania opisywanego wcześniej forum Silk Road. Wówczas po raz pierwszy BTC został wykorzystywany oficjalnie do nielegalnego handlu podrabianymi lekami, bronią, pornografią czy środkami narkotycznymi. Twórcy elektronicznej waluty podkreślają, że jej stworzenie nie miało na celu wsparcia działalności przestępczej w sieci. Mają również nadzieję, że udział BTC w obsłudze nielegalnych transakcji będzie marginalny[17].



Rys. 4. Sklep BlackBank funkcjonujący w sieci TOR
Źródło: http://www.deepdotweb.com/2015/04/02/tutorial-how-to-buy-drugs-on-blackbank-market/

Doskonałym przykładem obecności wirtualnej waluty w anonimowej sieci TOR był niefunkcjonujący obecnie sklep BlackBank. Tak jak na AlphaBay Market czy kiedyś Silk Road – BlackBank oferuje pełne spektrum narkotyków, produktów nielegalnych, pornografii i innych nielegalnych towarów. W odróżnieniu od najbardziej popularnych serwisów w TOR – BlackBank do złudzenia przypominał zwykły sklep internetowy. Posiadał on katalogowy podział na kategorie, wyszukiwarkę, koszyk do którego użytkownik dodaje wybrane przez siebie produkty oraz dział promocji. Twórcy sklepu na bieżąco aktualizują kurs BTC. Praktycznie nie wychodząc poza witrynę BlackBanku – kupujący był w stanie nabyć dowolny towar (łącznie z wyborem

[17] M. Szymankiewicz, *Bitcoin – wirtualna waluta Internetu*, op. cit., s. 94.

dowozu lokalnego lub rodzaju przesyłki międzynarodowej). Rysunek 3 na następnej stronie pokazuje interfejs BlackBank.

Warto zauważyć, że przy każdym produkcie oferowanym w sklepie, podana była cena w dolarach oraz jej odpowiednik w walucie BTC. Jest to ważne, bowiem twórca BlackBanku założył, że główną walutą, którą będą posługiwać się jego użytkownicy będzie właśnie BTC. Elementem zachęcającym do powyższego rozwiązania był stworzony przez założyciela tzw. depozyt Bitcoin. Powyższy system transakcji zatrzymywał przesłane przez kupującego Bitcoiny. BlackBank przechowywał je do czasu sprawdzenia zakupionego produktu. Wówczas, jeżeli kupujący był zadowolony z produktu, akceptował przeprowadzoną transakcje i BTC były automatycznie przesyłane na konto sprzedającego. W przypadku kiedy nie otrzymano produktów albo ich jakość/ilość lub cokolwiek innego było niezgodne z opisem – można było wejść na drogę sporu i odzyskać przesłane elektroniczne środki płatnicze. BlackMarket funkcjonował od 7 stycznia 2014 roku. W odróżnieniu od AlphaBay Market, gdzie wszystkie transakcje przebiegają na zasadzie dwustronnych lub wielostronnych rozmów pomiędzy kontrahentami, BlackBank stworzył system kupna i sprzedaży przy wykorzystaniu BTC.

Wprowadzenie powyższego systemu to rezultat incydentu, który miał miejsce w innym, podobnym sklepie w sieci TOR – Evolution Marketplace. Wówczas doszło do masowego oszustwa, w którym udział brali współadministratorzy i moderatorzy serwisu. Jednym z obowiązków administratorów oraz moderatorów było zatwierdzanie realizowanych transakcji. To oni pełnili rolę tzw. depozytów. Mimo początkowego sukcesu powyższego systemu – doszło do nieoczekiwanego zatrzymania wpłat i wypłat na konto osób sprzedających i kupujących. Okazało się, że pewna grupa osób kierujących Evolution Marketplace wyprowadziła z serwisu znaczną ilość BTC. Nie jest wiadomo dokładnie ile zyskali oszuści, ale szacuje się, że kwota ta sięgała po przeliczeniu 12 milionów dolarów[18]. Należy zatem stwierdzić, że brak centralnej regulacji waluty (przez rząd, organizację lub inny podmiot) jest z jednej strony zaletą, ale z drugiej – wadą, która pojawia się w takich sytuacjach.

Warto zaznaczyć, że na Polish Black Market oraz Victoria, waluta Bitcoin była wykorzystywana równie często. Analizując transakcje w tych sklepach należy stwierdzić, iż większość użytkowników preferowała bardziej płatności w BTC od tradycyjnych przelewów. Polacy zwracali również uwagę na problemy związane z przysłaniem nielegalnych towarów do Polski. Bardzo często zwracano uwagę, że dobrym rozwiązaniem jest korzystanie z oferty paczkomatów firmy In-Post[19].

[18] http://www.deepdotweb.com/2015/03/18/evolution-marketplace-exit-scam-biggest-exist-scam-ever/

[19] Warto jednak nadmienić, że In-Post nie obsługuje przesyłek z zagranicy do Polski i odwrotnie.

Poza wykorzystywaniem elektronicznej waluty w celu dokonywania prostych transakcji sprzedaży i kupna, Bitcoin funkcjonuje w sieci TOR zupełnie autonomicznie. Deep Web posiada szereg stron poświęconych wyłącznie najpopularniejszej e-walucie. Przykładem jest usługa EasyCoin. Jest to projekt umożliwiający założenie konta (portfela) BTC w sieci TOR. Dzięki temu rozwiązaniu możliwe jest całkowite pominięcie korzystania z zasobów jawnego Internetu, a co za tym idzie – wyeliminowanie kolejnego newralgicznego punktu mogącego zdemaskować użytkownika sieci. Innym przypadkiem podobnej usługi jest OnionWallet. Działa on podobnie do serwisu EasyCoin. Autorzy powyższych domen podkreślają, że ich rozwiązanie daje faktyczną pewność zachowania anonimowości przy wykorzystaniu BTC. Zarówno EasyCoin, jak i OnionWallet eliminują możliwość zdemaskowania użytkownika e-waluty, nawet w przypadku korzystania z serwisów wymagających podania tożsamości (np. kiedy posiadacz BTC chce go sprzedać na giełdzie Bitcoinów). Ponadto główna strona obu serwisów informuje wprost, że *tylko wykorzystanie Bitcoinów poprzez usługi dostępne w sieci TOR oraz samo funkcjonowanie w sieci TOR jest w stanie zapewnić stuprocentowy poziom anonimowości i prywatności*[20].

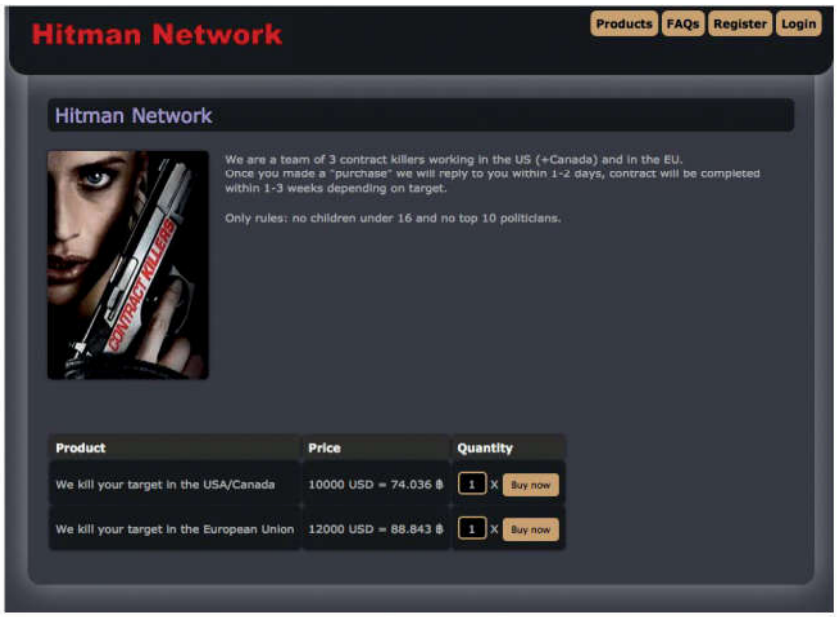
Kolejnym obszarem, w którym użytkownicy TOR wykorzystują walutę Bitcoin jest tzw. sieć płatnych morderców. Sieć TOR zapewniając jej użytkownikom pełną anonimowość, oprócz rozwijania działalności polegającej na wymianie handlowej towarów nielegalnych, oferuje inne inicjatywy przestępcze. Doskonałym przykładem jest Hitman Network[21]. Strona ta, jak sama nazwa wskazuje, oferuje wynajęcie płatnego mordercy albo zakup broni. Usługa proponowana przez użytkowników jest honorowana praktycznie na całym świecie zarówno w USA, jak i w Europie oraz Azji. Zakres oferty jest uzależniony od aktywnych tam osób. Przykładowe ogłoszenie na Hitman Network przedstawia rysunek 4 na następnej stronie.

Z powyższego przykładu wynika, że oferta obejmuje zarówno morderstwo na terenie Stanów Zjednoczonych/Kanady, jak i Unii Europejskiej. Jedyne ograniczenie jakie określił morderca to wiek ofiary (nie zabija dzieci poniżej 16 roku życia) oraz polityków znajdujących się w czołowej 10 popularności w danym kraju. W przytoczonym przypadku widać, że koszt takiej usługi w USA to 10 000 dolarów lub 74,036 BTC. W UE zabójstwo kosztuje 12 000 dolarów lub 88,843 BTC. Warto zwrócić uwagę na to jak powszechnie w tym serwisie jest wykorzystywana e-waluta. Zgodnie z informacjami portalu The DailyBeast, płatności w Bitcoinach zostały zaakceptowane przez twórców Hitman Network na początku 2013 roku[22].

[20] http://ow24et3tetp6tvmk.onion/

[21] http://ybp4oezfhk24hxmb.onion/

[22] http://www.thedailybeast.com/articles/2013/10/17/hitman-network-says-it-accepts-bitcoins-to-murder-for-hire.html



Rys. 4. Ogłoszenie na Hitman Network
Źródło: https://www.dailydot.com/crime/deep-web-murder-assassination-contract-killer/

Ciekawym przypadkiem, w którym wykorzystuje się walutę Bitcoin, jest High Quality Euro Replicas (HQER). Jest to francuski serwis oferujący fałszywe banknoty Euro. Jak twierdzą twórcy – ich produkt przeszedł odpowiednie testy (nawet UV), zawiera odpowiednie zabezpieczenia i jest na tyle dobrze przygotowany, że użytkownik nie napotka problemów wydając fałszywe pieniądze na terenie całej Europy. Warto zaznaczyć, że fałszywe Euro można kupić płacąc jedynie Bitcoinem. Stawka za 25 banknotów o wartości 50 Euro wynosi 2,274 BTC, 60 banknotów o wartości 50 Euro – 4,547 BTC oraz 120 banknotów o wartości 50 Euro – 8,640 BTC[23].

Można stwierdzić, że wykorzystanie waluty BTC w ramach działania TOR to „dodatkowa warstwa cebuli", która ogranicza dostęp do centrum tej technologii. Stopień integralności tych dwóch efektów postępu technologicznego i teleinformatycznego jest znaczny. Co więcej – wciąż się rozwija i staje się coraz bardziej popularny. Internauci funkcjonujący w ramach DeepWebu oraz wykorzystujący do operacji finansowych elektroniczną walutę z miesiąca na miesiąc mają większy wybór usług i witryn, które zapewnią im anonimowość.

Anonimowa działalność w sieci TOR przy wykorzystaniu waluty BTC jest problemem, z którym trudno walczyć. Mimo że niektóre służby zajmują się monitorowaniem tego zjawiska, zachowanie odpowiednich zasad wyklucza ryzyko

[23] http://www.y3fpieiezy2sin4a.onion/

identyfikacji użytkowników. Współczesny świat zaczyna zauważać problem, który wiąże się z siecią TOR i BTC. Przykładowo Federacja Rosyjska wyznaczyła nagrodę (340 tys. zł) dla osoby lub organizacji, która będzie w stanie złamać zabezpieczenia TOR[24]. Podmioty państwowe są coraz bardziej świadome skali zagrożenia. TOR może służyć nie tylko do wymiany handlowej towarów prawnie zabronionych. Przykładem innego wykorzystania TORa było działanie siedemnastolatka z Kalisza, który przez anonimową sieć wysyłał fałszywe informacje o bombach w 87 instytucjach państwowych. Pomimo komunikatów prasowych Policji, które sugerowały, że sieć nie jest w pełni anonimowa, specjaliści portalu *niebezpiecznik.pl* twierdzą, że nastolatek został zidentyfikowany przez własny błąd (na wzór twórcy portalu Silk Road)[25]. Można sobie wyobrazić skutki zorganizowanych działań o podobnym charakterze, które będzie ukierunkowane np. na destabilizację działań szpitali w Polsce albo szczytu politycznego państw. Jest to istotne, ponieważ użytkownik może oddziaływać na różne procesy i wydarzenia z dowolnego miejsca na ziemi pozostając niezidentyfikowanym. Anonimowość i wiążąca się z nią bezkarność w sieci TOR może więc stać się w przyszłości powszechna. W związku z tym należy przeciwdziałać negatywnym skutkom działalności w sieci TOR przy wykorzystaniu waluty BTC, co będzie sprzyjać poprawie bezpieczeństwa w skali globalnej.

BIBLIOGRAFIA

[1] Bednarek J., Andrzejewska A. (red.), *Zagrożenia cyberprzestrzeni i świata wirtualnego*, Difin, Warszawa 2014.

[2] Górka M., *Cyberbezpieczeństwo jako podstawa bezpieczeństwa państwa i społeczeństwa w XXI wieku*, Difin, Warszawa 2014.

[3] Kostrzewa-Zorbas G., *NATO w nowym środowisku strategicznym: cyberataki podlegają już art. 5 Traktatu Północnoatlantyckiego*, w: *Studia Bezpieczeństwa Narodowego WAT nr 6 Kryptologia i Cyberbezpieczeństwo*, WAT, Warszawa 2016.

[4] Kucharski K., *Narzędzia anonimizujące działania w Internecie jako instrumentarium do prowadzenia operacji informacyjnych w ramach wojny hybrydowej*, w: Przegląd Bezpieczeństwa Wewnętrznego ABW – Wydanie specjalne – Wojna hybrydowa, ABW, Warszawa 2015.

[5] Szymankiewicz M., *Bitcoin – wirtualna waluta Internetu*, Helion, Gliwice 2014.

Witryny internetowe:

[1] http://freeross.org/

[2] http://niebezpiecznik.pl/post/cbs-ujelo-cyberterroryste-pomimo-korzystania-przez-niego-z-tor-a/

[24] http://www.chip.pl/news/internet-i-sieci/dostep-do-internetu/2014/07/rosja-chce-zlamac-zabezpieczenia-sieci-tor

[25] http://niebezpiecznik.pl/post/cbs-ujelo-cyberterroryste-pomimo-korzystania-przez-niego-z-tor-a/

[3] http://niebezpiecznik.pl/post/silk-road-najwiekszy-sklep-z-narkotykami-w-internecie-zamkniety-fbi-namierzylo-i-aresztowalo-jego-tworce/
[4] http://niebezpiecznik.pl/post/silk-road-najwiekszy-sklep-z-narkotykami-w-internecie-zamkniety-fbi-namierzylo-i-aresztowalo-jego-tworce/
[5] http://osintinsight.com/
[6] http://ow24et3tetp6tvmk.onion/
[7] http://www.chip.pl/news/internet-i-sieci/dostep-do-internetu/2014/07/rosja-chce-zlamac-zabezpieczenia-sieci-tor
[8] http://www.deepdotweb.com/2015/03/18/evolution-marketplace-exit-scam-biggest-exist-scam-ever/
[9] http://www.deepdotweb.com/2015/04/02/tutorial-how-to-buy-drugs-on-blackbank-market/
[10] http://www.onion-router.net/History.html
[11] http://www.sickchirpse.com/deep-web-guide/
[12] http://www.thedailybeast.com/articles/2013/10/17/hitman-network-says-it-accepts-bitcoins-to-murder-for-hire.html
[13] http://www.y3fpieiezy2sin4a.onion/
[14] http://ybp4oezfhk24hxmb.onion/
[15] http://zaufanatrzeciastrona.pl/post/siedmiu-nastepcow-pbm-ktory-z-nich-przetrwa-pozostalych/
[16] https://www.dailydot.com/crime/deep-web-murder-assassination-contract-killer/
[17] https://www.exploit-db.com/
[18] ig6ndt6anbg2dimk.onion
[19] metrics.torproject.org

THE ONION ROUTING (TOR) – ANONYMOUS NETWORK OF CRIMINALS

Abstract. The ongoing revolution of informatics and information processes influences the economic and social realities of the modern world, as well as the extensive media campaigns, and other events relating to the problem of privacy safeguarding within the Internet. influences the economic and social realities of the modern world. The TOR network became one of the fastest responding to the individual needs for privacy protection. Unfortunately, the TOR network principles of operation, and the possibilities it provides to its users, led to the development of new dimension of cybercrime possibilities. In the article, authors describe the principles of TOR, and the development of pathological phenomena within this network. In their analysis, they advise that the TOR network's strong integration with the anonymous currency Bitcoin can contribute to the emergence of new global threats.
Keywords: TOR, Bitcoin, anonymity, cybersecurity, organized crime.