Antoni Krauz

Mroczna strona internetu – TOR niebezpieczna forma cybertechnologii

Dydaktyka Informatyki 12, 63-74

2017

Dydaktyka Informatyki 12(2017)
ISSN 2083-3156
DOI: 10.15584/di.2017.12.8
http://www.di.univ.rzeszow.pl

Wydział
Matematyczno-Przyrodniczy UR
Laboratorium Zagadnień
Społeczeństwa Informacyjnego

Antoni KRAUZ

Dr inż., Uniwersytet Rzeszowski, Wydział Pedagogiczny, Katedra Pedagogiki Pracy i Andragogiki, ul. Ks. Jałowego 24, 35-010 Rzeszów; e-mail: antonikrs@ur.edu.pl

MROCZNA STRONA INTERNETU – TOR NIEBEZPIECZNA FORMA CYBERTECHNOLOGII

THE DARK SIDE OF THE INTERNET THE ONION ROUTER IS A DANGEROUS FORM OF CYBERTECHNOLOGII

Słowa kluczowe: Internet, cybertechnologia, zagrożenia, sieć internetowa, TOR.
Keywords: Internet, Internet network, threats, cybertechnology, The Onion Router.

Streszczenie

W artykule przedstawiono zasady działania jednej z anonimowych sieci TOR, której skrót pochodzi od angielskiej nazwy *The Onion Router*, oraz omówiono, jakie niesie ze sobą zagrożenia, dlaczego jest taka niebezpieczna i czy można temu zaradzić. TOR jest to sieć komputerowa implementująca trasowanie cebulowe trzeciej generacji. Sieć uniemożliwia analizowanie ruchu sieciowego przez co zapewnia użytkownikowi prawie całkowicie anonimowy dostęp do zasobów Internetu. TOR może być użyty w celu pominięcia mechanizmów filtrowania treści oraz innych ograniczeń komunikacyjnych, może być wykorzystywana przez terrorystów, przestępców, hakerów, handlarzy bronią, narkotykami itp.

Summary

This article presents the principles of operation of one of the anonymous network TOR whose abbreviation is derived from the English name of The Onion Router and posed a threat, why is this dangerous and whether this can be remedied. The Onion Router This is a network that implements the third-generation onion routing. The network makes it impossible to analyze network traffic by providing the user almost completely anonymous access to Internet resources. The Onion Router can be used to bypass the content filtering mechanisms and other constraints, may be used by terrorists, criminals, hackers, arms dealers, drug, etc.

Wprowadzenie

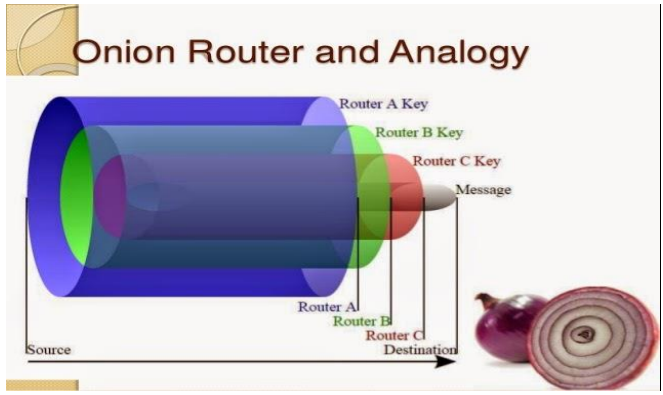
TOR to system, którego celem jest zapewnienie anonimowego dostępu do Internetu. Dzięki niemu można skutecznie chronić się przed próbami inwigilacji ze strony nieuczciwych użytkowników sieci bądź służb państwowych, znanej

jako analiza ruchu sieciowego. Program umożliwia bezpieczne przeprowadzanie interesów, osobistej komunikacji, ale także może służyć osobom w celach nielegalnych, w których potrzebna jest anonimowość. System początkowo był sponsorowany przez laboratoria badawcze Marynarki Wojennej Stanów Zjednoczonych, pod koniec 2004 r. stał się projektem firmowanym przez Electronic Frontier Foundation (EFF), która wspierała go finansowo aż do listopada 2005 r. Obecnie rozwojem oprogramowania Tor zajmuje się TOR Project – organizacja non profit (niedochodowa) o charakterze badawczo-edukacyjnym, z siedzibą w Stanach Zjednoczonych, otrzymująca wsparcie finansowe z różnych źródeł. Zasada działania sytemu TOR polega na komunikacji przez rozproszoną sieć przekaźników sieciowych, które są udostępniane przez zainteresowanych. Dzięki temu bardzo utrudnione jest odkrywanie odwiedzanych przez petentów stron poprzez podsłuchiwanie połączenia sieciowego. Program nie pozwala także na śledzenie adresatów przez systemy statystyczne zainstalowane na odwiedzanych stronach internetowych. Niemożliwe zatem staje się wskazanie np. naszego miejsca zamieszkania, dodatkowo program pozwala na przeglądanie stron blokowanych przez państwo, np. Iran, Chiny lub dostawców sieci[1].

Zasada działania TOR (The Onion Router)

Routing używany przez TOR-a działa na zasadzie wielokrotnego szyfrowania pakietów i przesyłaniu ich przez kilka węzłów sieciowych, zwanych *routerami cebulowymi*. Każdy *router cebulowy* odczytuje informacje dotyczące dalszego routowania i następnie przesyła wiadomość dalej do kolejnego routera, który ponawia operację (rys.1, 2, 3, 4). Chroni to przed poznaniem przez węzły treści wiadomości jak i adresów (źródłowego i docelowego). Sieć TOR to grupa bezpłatnych serwerów, które pozwalają poprawić prywatność i bezpieczeństwo w Internecie. Użytkownicy TOR-a wykorzystują tę sieć poprzez podłączenie przez serię wirtualnych tuneli, zamiast dokonywać bezpośredniego połączenia, dzięki czemu organizacje i osoby mogą dokonać wymiany informacji w sieciach publicznych bez naruszania ich prywatności. Wzdłuż tej samej linii, TOR jest skutecznym narzędziem uniknięcia cenzury, co pozwala użytkownikom na dotarcie do zablokowanych treści. TOR może być również używany przez programistów do tworzenia nowych narzędzi komunikacyjnych z wbudowanymi funkcjami ochrony prywatności. TOR ukrywa użytkownika pośród innych użytkowników sieci, więc im liczniejsza i bardziej różnorodna jest grupa użytkowników TOR-a, tym bardziej chroniona będzie anonimowość[2].

[1] http://www.torproject.org/docs/tor-hidden-service (dostęp: 04.01.2017 r.).
[2] http://web.archive.org/web/20080403151246 (dostęp: 07.01.2017 r.).



Rys. 1. Adresy przesyłanych informacji (forma graficzna) – źródłowy i docelowy
Źródło: http://www.torproject.org/docs/tor-hidden-service (dostęp: 08.01.2017 r.)

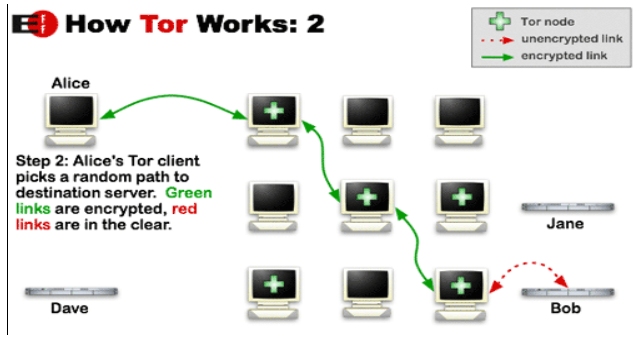
Program minimalizuje ryzyko przeprowadzania skutecznej analizy sieciowej, rozpraszając transakcje w różnych miejscach Internetu, w taki sposób, aby żaden pakiet nie trafiał do celu z oryginalną lokalizacją.

Rys. 2. Petent pobiera szyfrowanym połączeniem listę węzłów TOR-a z serwera katalogowego
Źródło: https://www.TORproject.org/ (dostęp: 04.01.2017 r.)

Można to porównać do tworzenia zawiłych, trudnych do śledzenia różnych tras, które co pewien czas zmieniamy obawiając się, że jesteśmy śledzeni. Zatem pakiety przechodzą przez przypadkowe węzły, które zacierają ślady w taki sposób, że analiza ich nie jest w stanie wykryć skąd i dokąd zmierzają (rys. 2).

W celu stworzenia prywatnej ścieżki, oprogramowanie użytkownika i klienci budują etapami obwód bezpiecznych, szyfrowanych połączeń między przekaźnikami sieci. Za każdym razem obwód powiększa się o jeden węzeł. Dzięki temu każdy z przekaźników po drodze zna jedynie dane przekaźnika, z którego otrzymał dane i do którego wysyła dane. Żaden z przekaźników nie potrafi od-

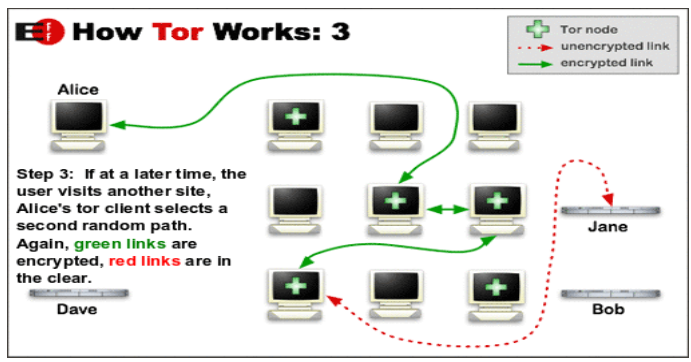
tworzyć pełnej ścieżki pakietu, tj. źródłowego i docelowego. Do każdego ogniwa w obwodzie używana jest inna para kluczy, w celu zapewnienia, że żaden z węzłów nie będzie w stanie odtworzyć pełnej trasy pakietu (rys. 3).



Rys. 3. Petent wybiera dowolną ścieżkę do serwera docelowego. Linie ciągłe połączenia są szyfrowane, przerywane nie

Źródło: https://pl.wikipedia.org/wiki/Tor_(sie%C4%87_anonimowa)#cite_ref-autonazwa1_9-0. (dostęp: 08.01.2017 r.).

Po utworzeniu obwodu przesyłanie danych między różnymi aplikacjami staje się możliwe. Ze względu na to, że żaden z przekaźników nie zna więcej niż jednego ogniwa w obwodzie, podsłuch nawet przez jeden niewiarygodny przekaźnik w obwodzie staje się niemożliwy. Aby zapewnić większą szybkość działania aplikacji, ten sam obwód używany jest do około 10 minut. Kolejne zapytania przesyłane są już nowo utworzonym obwodem. Dzięki temu wcześniejsze akcje połączeń (petent, ogniwo, obwód) nie są w żaden sposób wiązane z nowymi (rys. 4).



Rys. 4. Jeżeli osoba chce połączyć się z innym serwerem, petent TOR-a wybiera inną dowolną ścieżkę. Linie ciągłe połączenia są szyfrowane, przerywane nie

Źródło: https://wiki.torproject.org/noreply/TheOnionRouter/TorFAQ?action=recall&rev=554# EntryGuards (dostęp: 06.01.2017 r.).

Anonimowa sieć TOR w globalnej cyberprzestrzeni

TOR ochrania działania oraz tożsamość użytkowników sieci przed analizą ruchu sieciowego. Operatorzy utrzymują wirtualną sieć złożoną z routerów cebulowych, zapewniającą anonimowość zarówno w sensie ukrycia lokalizacji użytkownika, jak również możliwości udostępniania anonimowych ukrytych usług. TOR wykorzystuje kryptografię, szyfrując wielowarstwowo przesyłane pakiety, zapewniając doskonałą poufność przesyłania między routerami. Użytkownik musi mieć uruchomionego na swoim komputerze klienta, który łączy się z serwerem pośredniczącym sieci TOR. Serwery te zwane węzłami może uruchomić u siebie każda osoba chcąca wesprzeć rozwijanie sieci TOR. Oprogramowanie tworzące połączenie z Internetem może korzystać z TOR-a dzięki interfejsowi SOCKS[3].

Użytkownicy uruchamiają na swoich komputerach oprogramowanie klienckie sieci TOR, które okresowo tworzy wirtualne obwody w sieci. TOR wielowarstwowo szyfruje przesyłane komunikaty zapewniając doskonałą poufność przesyłania pomiędzy routerami. 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[4].

Wewnątrz sieci TOR ruch jest przekazywany pomiędzy routerami, 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. Sieć TOR może być wykorzystywana do celów uznawanych za nielegalne w niektórych jurysdykcjach, jak na przykład krytykowanie przywódców państwowych, wymiana materiałów chronionych prawem autorskim bądź dystrybucja pornografii dziecięcej. Do utrzymania stron internetowych organizacji, śledzenia lub łączenia się z serwisami informacyjnymi, komunikatorami i tym podobne, gdy są one blokowane przez lokalnych dostawców usług internetowych. Ukryte usługi TOR-a pozwalają na publikację serwisów internetowych oraz innych usług sieciowych bez potrzeby ujawniania fizycznej lokalizacji serwera. Także można używać TOR-a do społecznie wrażliwej komunikacji: czatów i forów internetowych wśród bardzo różnych osób. Program ten jest (może być) wykorzystywany między innymi przez:

– społeczność internetową, do ochrony swojej prywatności, zabezpieczeniu haseł, które mogą zostać podsłuchane w sieci, do ochrony swoich dzieci, aby

[3] https://www.torproject.org/docs/tor-doc-windows.html.en (dostęp: 03.01.2017 r.).

[4] https://pl.wikipedia.org/wiki/Tor_(sie%C4%87_anonimowa)#cite_ref-autonazwa1_9-0 (dostęp: 08.01.2017 r.).

podczas korzystania z Internetu nie udostępniały danych identyfikujących miejsce zamieszania w sieci, lub do przeglądania stron, które w danym państwie są cenzurowane jak np. Facebook czy YouTube;

– stróżów prawa, głównie zajmujących się oszustwami internetowymi, bez obawy, że zostaną wykryci przez administratorów stron. Wymiar sprawiedliwości używa TOR-a do odwiedzania i obserwacji witryn bez pozostawiania adresów IP w logach rządowych serwerów internetowych, dla bezpieczeństwa operacyjnego;

– dziennikarzy i blogerów, aby mogli pisać bez obawy o swoją prywatność i bezpieczeństwo, unikać cenzury państwa, a także, aby przesyłać artykuły z innych państw bez obawy o firewalle danego państwa. Dziennikarze również używają TORa, by bardziej bezpiecznie komunikować się z informatorami i dysydentami;

– biznesmenów, aby nie naruszać bezpieczeństwa informacji, żeby strategie firmy nie wyciekły oraz sprawdzić, czy przypadkiem konkurencja nie ma przygotowanej innej strony dla nich i dla społeczeństwa;

– aktywistów, walczących o prawa człowieka, aby w anonimowy sposób zgłaszać naruszenia prawa, walczących o wolność wypowiedzi, np. w Chinach. Aktywiści jak Electronic Frontier Foundation (EFF) zalecają TORa jako mechanizm utrzymania swobód obywatelskich w Internecie;

– polityków, celem ochrony różnych informacji;

– profesjonalnych informatyków, do weryfikowania zasad firewalla, gdy mają problemy z DNSami, gdy mają np. taką politykę w firmie, w której pracują itp.;

– wojsko, gdyż nie jest trudne dla służb zbadanie ruchu sieciowego odnalezienia hotelu czy serwerów wojskowych, gdyby łączyli się nieszyfrowanymi połączeniami, do wydawania rozkazów, aby nie zostały przechwycone i zniszczone. Pewien oddział US Navy używał TOR-a jako biały wywiad, a jeden z zespołów używał go niedawno podczas operacji na Bliskim Wschodzie;

– grupy, takie jak Indymedia[5] polecają TOR-a jako zabezpieczenie prywatności i bezpieczeństwa swoim członkom;

– skorumpowane grupy osób prowadzących działalność przestępczą. Daje też pewne możliwości w zakresie prania brudnych pieniędzy;

– organizacje pozarządowe (NGO) używają TOR-a, by umożliwić swoim pracownikom połączenie się z ich serwerami podczas pobytu w innym kraju, minimalizując możliwość ujawnienia, że pracuje ktoś z ich organizacji;

– przestępców, handlarzy narkotyków, kryminalistów, hakerów, celem wymiany nielegalnych informacji, do handlu narkotykami, bronią, płatnymi morderstwami, dziecięcą pornografią i szeroko rozumianymi globalnymi przestępstwami o niespotykanej skali;

[5] Indymedia (Ośrodki Niezależnych Mediów, ang. *Independent Media Center*) jest siecią grup medialnych i dziennikarzy, zostały zainicjowane pod koniec 1999 roku. Do 2002 roku powstało 89 lokalnych autonomicznych ośrodków w 31 krajach na 6 kontynentach.

– korporacje, jako bezpieczny sposób prowadzenia analizy działania konkurencji oraz zabezpieczają swoje operacje przed podsłuchem. Używają go również w celu zastąpienia tradycyjnego VPN, który ujawnia dokładną wielkość i czas komunikacji. Gdzie pracownicy pracują i ile czasu? Gdzie informatycy poszukują logi pracy stron internetowych? Jakie działy badawcze komunikują się z prawnikami zajmującymi się patentami?[6].

Podsumowując można stwierdzić, iż anonimowa sieć chroni nasze własne wartości, ale także wszystkie jakie tylko można sobie wyobrazić – wszelkie antywartości[7].

Globalna mroczna strona zagrożeń sieci TOR w Internecie

Są w Internecie miejsca, dokąd nie docierają globalne macki Google'a, dokąd nie wejdzie się używając zwykłej przeglądarki, a gdzie jeszcze można być anonimowym. Tym miejscem jest *cebulka*, czyli sieć TOR (*The Onion Router,* inaczej *Deep Web, Darknet*) czyli **ukrytym Internetem.** Jest to bowiem sieć mniej dostępna i dużo bardziej mroczna od zwykłego Internetu, niemal całkowicie anonimowa[8]. Lubią ją: przestępcy, hakerzy, oszuści, paranoicy, anarchiści, pedofile, również funkcjonariusze rządowych służb. Oraz wszyscy dbający o prywatność. To osobny podziemny świat, z własnymi bezprawnymi zasadami, kulturą, a nawet specjalną walutą. Surfując po *cebulowych* stronach ukrytej sieci, spotykamy Internet z jego początków: prymitywne strony bez zbędnej grafiki, reklam, a fora i kanały dyskusyjne zapełnione są przez wąską grupę *wtajemniczonych*, gardzących niezorientowanymi *noobami* (nowicjuszami). *Znajdziemy tu pełną gamę tematów: od tego, jak przeprowadzić oszustwo, poprzez ofertę narkotyków, aż po porady, jak pozbyć się zwłok.* To, co odróżnia ją od pierwszych stron sieci WWW, to adresy: najczęściej seria losowych cyfr i liter zakończona końcówką *.onion*. Inna jest także niekiedy szokująca zawartość. Znajdziemy tu dosłownie wszystko, co zakazane i nielegalne: od instrukcji, jak przeprowadzić wszelkiego rodzaju oszustwa po witryny np. płatnych zabójców. Nie wspominając o czyhającej zewsząd dziecięcej pornografii[9].

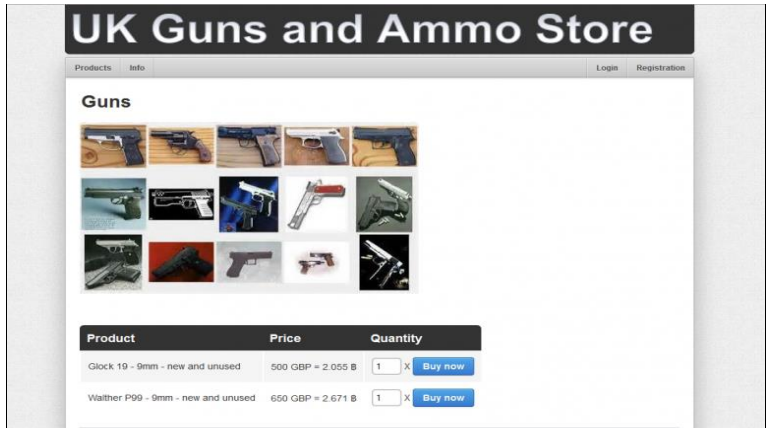
[6] Szerzej: https://www.torproject.org/sponsors (dostęp: 05.01.2017 r.).

[7] A. Piecuch, *Cybernetyczna wolność wartości* [w:] *Z badań nad wartościami w pedagogice,* red. W. Furmanek, Rzeszów 2006, s. 253–260.

[8] Zob. szerzej A. Krauz, *Internet narzędziem groźnej broni cyfrowej dla infrastruktury krytycznej globalny świecie wiedzy*, „Edukacja – Technika – Informatyka" 2013-1, Rocznik Naukowy nr 4, cz. 1, *Wybrane problemy edukacji technicznej i zawodowej*, red. W. Walat, W. Lib, Rzeszów 2013, s. 388–399.

[9] http://arstechnica.com/news.ars/post/20060911-7709.html (dostęp: 07.01.2017 r.).

Największym zagrożeniem są oczywiście przestępcy, którzy pod ochroną anonimowości wykonują bardzo wiele nielegalnych rzeczy[10]. W sieci TOR na bardzo dużą skalę odbywa się nielegalny handel, gdzie prym wiodą narkotyki, pośród których dominują: marihuana, leki na receptę, MDMA (ecstasy), LSD, kokaina czy metamfetamina (rys. 6). Ale to dopiero początek, bo można kupić tutaj każdą broń (rys. 5), karty kredytowe, sprzęt elektroniczny po okazyjnych cenach, fałszywe pieniądze, podrobione paszporty, dowody osobiste i wiele innych nielegalnych rzeczy, a głównym środkiem zapłaty jest elektroniczna gotówka – pieniądz[11], kryptocyfrowa wirtualna waluta bitcoin[12].



Rys. 5. Możliwy nielegalny zakup broni

Źródło: http://www.rp.pl/artykul/948289-ciemna-strona-sieci.html#ap-6 (dostęp: 06.01.2017 r.).

Poza handlem rozpowszechniane są też treści pornograficzne. Nawet takie jak nekrofilia czy pornografia dziecięca. Przedstawione są wskazówki czy opisy, jak zgwałcić dziecko, są do tego różne fora dyskusyjne, a nawet jest założona organizacja Sidprotect, która ma na celu pomagać pedofilom, a celami jej jest legalizacja pornografii dziecięcej, jak i seksu z nieletnimi. **W linku są wulgarne, karygodne, wypaczone, zboczone, ze względu na treści nie do zacytowa-**

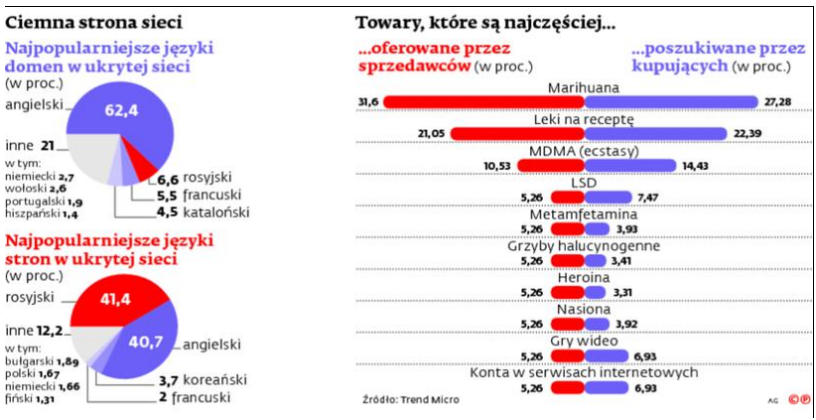
[10] Szerzej: A. Olak, J. Mika, *Społeczne postrzeganie zagrożeń. Bezpieczeństwo w warunkach globalizacji, wybrane zagadnienia*, Wyższa Szkoła Biznesu i Przedsiębiorczości w Ostrowcu Św., Ostrowiec Świętokrzyski 2014, s. 22–34.

[11] bitcoin.org/bitcoin.pdf (dostęp: 008.01.2017 r.).

[12] Szerzej: R. Kościelny, *Dziwności w cyberprzestrzeni,* „Warszawska Gazeta", 5–12 stycznia 2017 r., s. 23. Kryptowaluta wprowadzona w 2009 roku przez osobę (bądź grupę osób) o pseudonimie Satoshi Nakamoto. W grudniu 2015 roku amerykańskie portale Wired i Gizmondo, po przeprowadzeniu śledztwa dziennikarskiego, zasugerowały, iż twórcą bitcoina może być australijski przedsiębiorca z branży IT – Craig Steven Wright. Australijski biznesmen w celu zakończenia spekulacji na swój temat oficjalnie przyznał się i przedstawił dowody, iż to on pod pseudonimem Satoshi Nakamoto stworzył najpopularniejszą wirtualną walutę.

nia dyskusje występujące właśnie na takim forum internetowym, gdzie pedofile dosłownie w szczegółach opisują praktyczne rady i problemy, w tym związane z dziećmi, bezczeszczeniem ciał zmarłych (zgroza)[13].

Na forach ohackingu w sieci TOR możemy się dowiedzieć, zazwyczaj za opłatą, o łamaniu haseł, podsłuchach, trojanach, keylogerach, dzięki którym przestępca dowie się, co wpisuje się na klawiaturze, czyli pozna hasła, może np. wyczyścić tej osobie konto w banku. Albo dzięki tym informacjom weźmie pożyczkę na osobę, którą okradł z haseł i danych osobowych. Na forach tak naprawdę możemy się dowiedzieć praktycznie wszystkiego. Hakerzy włamują się również do baz danych z prywatnymi danymi (wykorzystując w laptopach kamerki), a następnie publikują je w Internecie, albo żądają za nie pieniędzy. Jak udowodnimy, że mamy wystarczająco dużo pieniędzy, to można zlecić gwałt, okaleczenie czy nawet zabójstwo osoby[14].



Rys. 6. Wykaz najczęściej poszukiwanych towarów

Źródło: http://www.rp.pl/artykul/948289-ciemna-strona-sieci.html#ap-6 (dostęp: 06.01.2017 r.).

Podejmowane przeciwdziałania w tym zakresie

Na szczęście sieć TOR ma też słabości, które mogą pomóc w zlokalizowaniu sprawców przestępstw, czy administratorów giełd handlujących nielegalnym towarem. Do takich słabości zaliczają się wycieki zapytań DNS, analiza ruchu, podsłuchiwanie węzłów wyjściowych czy po prostu błędy ludzkie. Dlatego przez takie słabości, cały czas monitorowanie ruchu sieciowego na węzłach

[13] Szerzej: https://groups.google.com/forum/#!topic/pl.sci.psychologia/mnwlNMpzq2M (dostęp: 08.01.2017 r.).

[14] https://zaufanatrzeciastrona.pl/post/wyciekla-lista-policyjnych-antyterrorystow/https://zaufanatrzeciastrona.pl/post/wlamywacz-spelnil-grozbe-i-publikuje-dane-klientow-plus-banku/ (dostęp: 07.01.2017 r.).

i wkład dużych pieniędzy przyczyniły się do sukcesu FBI, jak i polskiej Policji w walce z tego rodzaju przestępczością. Już we wrześniu 2006 r. władze niemieckie, w trakcie operacji wymierzonej przeciwko pornografii dziecięcej, skonfiskowały sprzęt jednego z centrów danych, na którym uruchomione było oprogramowanie TOR.

Następnie, w dniu 3 października 2013 r. została zamknięta jedna z największych nielegalnych internetowych giełd z handlem między innymi narkotykami i dopalaczami o nazwie Silk Road. Jednak już miesiąc później została nadal wznowiona działalność pod nazwą Silk Road 2.0, która została zamknięta 5 listopada 2014 r. Autor tej strony otrzymał za to karę dożywotniego więzienia bez możliwości wcześniejszego zwolnienia. W 2014 roku FBI opublikowało przykłady przejętych serwisów z ponad 400 stron. Na liście znalazły się następujące sklepy:

– sklepy narkotykowe, *Blue Sky* (blueskyplzv4fsti.onion), *Hydra* (hydrampvvnunildl.onion), *Pandora* (pandora3uym4z42b.onion), *Cloud Nine* (xvqrvtnn4pbcnxwt.onion);
– sklep z bronią, *Executive Outcomes* (http://iczyaan7hzkyjown.onion);
– sklep z kartami kredytowymi, *Fake Real Plastic* (http://igvmwp3544wpnd6u.onion);
– sklep z fałszywymi dowodami osobistymi, *Fake ID* (http://23swqgocas65z7xz.onion);
– sklepy z fałszywymi banknotami, *Fast Cash* (http://5oulvdsnka55 buw6.onion), *Super Notes Counter*, (http://67yjqewxrd2ewbtp.onion)[15].

Przejęte serwery znajdowały się w takich krajach jak: Bułgaria (tam znajdowało się 129 ze zlikwidowanych serwisów, prawdopodobnie mógł to być jeden z hostingów w sieci Tor), Czechy, Finlandia, Francja, Niemcy, Węgry, Irlandia, Łotwa, Litwa, Luksemburg, Holandia, Rumunia, Hiszpania, Szwecja, Szwajcaria i Wielka Brytania. Od listy krajów, gdzie znajdowały się serwery, ciekawsza jest lista krajów, których tam nie ma, jak chociażby Rosja czy Ukraina. Czyżby tam działały serwisy, które przetrwały rzeź? Natomiast w Polsce końcem 2015 r. został zatrzymany jeden ze sprawców ataku na Plus Bank; wyciekła pełna baza danych i użytkowników forum ToRepublic, zatrzymano wówczas również administratorów tego forum[16].

Zakończenie

Jak każdy rozwój techniki w dzisiejszych czasach, tak i anonimowość sieci ma swoje dobre strony, ale niestety, także te bardzo groźne i to właśnie z nich jest najbardziej znana. Jedną z najbardziej znanych jest TOR, który zwiększa

[15] http://www.torproject.org/faq-abuse.html.en (dostęp: 07.01.2017 r.).
[16] Szerzej: https://zaufanatrzeciastrona.pl/post/tag/torepublic/ (dostęp: 09.01.2017 r.).

cały czas liczbę użytkowników z niej korzystających. A że jest to sieć anonimowa, to nie wiadomo, czy w celach zapewniających sobie bezpieczeństwo w przekazywaniu normalnych danych czy w celach przestępczych, korupcyjnych[17]. Na forach polskich czy zagranicznych związanych z siecią TOR mamy wiele przewodników, poradników jak krok po kroku wykonać daną nielegalną rzecz, zawsze będzie to bardzo groźne narzędzie, gdy wykorzystywać go będą nieodpowiedni ludzie.

Bibliografia

Janczyk J., *W głębi Internetu – inne zastosowania informatyki*, „Dydaktyka Informatyki" 2014, nr 9, red. A. Piecuch, W. Furmanek, Wyd. Uniwersytet Rzeszowski.

Kościelny R., *Dziwności w cyberprzestrzeni*, „Warszawska Gazeta", 5–12 stycznia 2017 r.

Krauz A., *Internet narzędziem groźnej broni cyfrowej dla infrastruktury krytycznej globalny świecie wiedzy*, „Edukacja – Technika – Informatyka", Rocznik Naukowy nr 4 /2013-1, cz. 1, *Wybrane problemy edukacji technicznej i zawodowej*, red. W. Walat, W. Lib, Rzeszów 2013.

Krauz A., *Nowe wydanie terroryzmu z wykorzystaniem broni CBRN we współczesnej cywilizacji śmierci*, „Edukacja – Technika – Informatyka", Rocznik Naukowy nr 5/2014-1, cz. 1, *Wybrane problemy edukacji technicznej i zawodowej*, red. W. Walat, W. Lib, Rzeszów 2014.

Mesároš M., Kelemen M., Nečas P., *Badania nad technologią zabezpieczeń oraz rozwoju ochrony osób i mienia: kwestie ochrony na świecie*, „Bezpieczeństwo i ochrona" R. 2, nr 3–4 (7–8), Kosice 2009.

Nečas P., Ivančík R., *Globalizácia, obrana a bezpečnosť vysokoškolská učebnica,* 1 Vyd.: Akadémia ozbrojených síl generála M.R. Štefánika, Liptovský, grafy, obr. tab., Mikuláš 2011.

Olak A., *Globalizacja jako wyzwanie współczesnych systemów edukacyjnych* [w:] *Edukacja dla bezpieczeństwa*. Stowarzyszenie Nauka Edukacja Rozwój, Ostrowiec Świętokrzyski 2011.

Olak A., Mika J., *Społeczne postrzeganie zagrożeń. Bezpieczeństwo w warunkach globalizacji, wybrane zagadnienia*, Wyższa Szkoła Biznesu i Przedsiębiorczości w Ostrowcu Św., Ostrowiec Świętokrzyski 2014.

Piecuch A., *Cybernetyczna wolność wartości* [w:] *Z badań nad wartościami w pedagogice*, red. W. Furmanek, Rzeszów 2006.

Sokół R., *Jak pozostać anonimowym w sieci*, Wyd. Helion, Gliwice 2014.

Netografia

https://www.torproject.org/about/overview.html.en

https://en.wikipedia.org/wiki/Tor_(anonymity_network)

https://en.wikipedia.org/wiki/Onion_routing

https://metrics.torproject.org/

https://www.fbi.gov/news/pressrel/press-releases/more-than-400-.onion-addresses-including-dozens-of-dark-market-sites-targeted-as-part-of-global-enforcement-action-on-tor-network

[17] Szerzej: P. Nečas, R. Ivančík, *Globalizácia, obrana a bezpečnosť vysokoškolská učebnica,* 1 Vyd.: Akadémia ozbrojených síl generála M.R. Štefánika, Liptovský, grafy, obr., tab., Mikuláš 2011, s. 190.

http://www.ibtimes.com/pulse/tour-deep-web-illegal-marketplaces-book-clubs-everything-between-1729404
http://www.buzzfeed.com/josephbernstein/if-you-dont-want-to-read-about-the-apple-watch-read-this-gui#.divPBRqKj
https://zaufanatrzeciastrona.pl/post/wiemy-jakim-cudem-fbi-moglo-namierzyc-i-zamknac-400-serwisow-w-sieci-tor/
https://en.wikipedia.org/wiki/Darknet
http://www.prosperitum.pl/praca_inzynierska.html
http://silkroaddrugs.org/category/silk-road-drugs-2/