Internet jest niewątpliwie jednym z najbardziej niesamowitych osiągnięć w historii ludzkości. Światowa sieć komputerów na zawsze zmieniła nasze postrzeganie komunikacji. Zaczęło się jako innowacyjne rozwiązanie w laboratorium do wymiany wiadomości tekstowych. Możesz sobie to wyobrazić? We wczesnych stadiach Internet miał tylko kod i zwykły tekst; żadnych obrazów, żadnych multimediów, nic poza tekstem. Prawie 30 lat później sieć całkowicie się zmieniła w szybkim tempie. W dzisiejszych czasach Internet zawiera istotne informacje o każdym użytkowniku. Zawiera nasze dane osobowe, zdjęcia, filmy i wiele więcej. Dane, o których możesz nigdy nie zdawać sobie sprawy, że tworzyłeś, unoszą się w cyberprzestrzeni, gdy czytasz te strony, takie jak preferencje wyszukiwania, pliki cookie, najnowsze zapytania wyszukiwarek i tak dalej. Tak więc Internet jest niebezpieczny nie tylko ze względu na złośliwych użytkowników, którzy próbują przechwycić Twoje dane osobowe w swoich przewrotnych celach (takich jak kody PIN do kart kredytowych; ryzyko, którego nigdy nie powinieneś lekceważyć), ale także z powodu ciągłego „wycieku" danych osobowych ", Które występuje podczas regularnego korzystania z usług online. Czy zgadzasz się z manipulowaniem Twoimi danymi osobowymi? Najprawdopodobniej nie. Jednak trudno jest całkowicie uciec od tej ekspozycji. W końcu za każdym razem, gdy używasz określonego narzędzia programowego lub aplikacji internetowej; musisz zgodzić się z warunkami użytkowania. W przeciwnym razie nie będziesz korzystać z tych usług. Dlatego otwierając przeglądarkę, aby surfować po Internecie, zgadzasz się na wykorzystanie Twoich danych osobowych po stronie programistów. Na przykład Google zbiera dane od nas wszystkich, od lokalizacji po osobiste wyszukiwania. Czy to nie brzmi dobrze? Na szczęście są tam bezpieczniejsze opcje; głównym kandydatem w sektorze wyszukiwarek jest DuckDuckGo: silnik wyszukiwania, który nie przechowuje danych osobowych użytkowników. Jednak, jak być może już wiesz, większość ludzi będzie nadal korzystać z Google. Czemu? Istnieją dwa ważne powody. Z jednej strony ryzyko nie jest tak duże i najprawdopodobniej ludzi to nie obchodzi. Większość z nas może od dłuższego czasu korzystać z globalnej sieci. Czy kiedykolwiek zostałeś zhakowany? A jeśli tak, to czy to była twoja wina, czy po prostu natknąłeś się na boskiego hakera, który złamał wszystkie protokoły bezpieczeństwa, aż do pojawienia się zielonkawego komunikatu „Przyznano dostęp" na czarnym ekranie? Jeśli myślisz, że to drugie; być może oglądałeś zbyt wiele filmów o nieistniejących ekspertach od cyber-hakowania. Spójrzmy na chwilę z rzeczywistością, zanim wznowimy bieg wpisów. Tylko nieliczni, naprawdę niewielka mniejszość z nas, kiedykolwiek będzie narażona na zagrożenia internetowe. I nie, nie mówię o tej wiadomości, która pojawia się na twojej przeglądarce, twierdzi, że wirus zniszczy komputer, miasto i wszystkich mieszkańców, chyba że - przypadkowo - zapłacisz trochę pieniędzy. To tylko żart - obrzydliwy przy pierwszym spotkaniu. Omówimy, jak unikać tego typu sytuacji i jak sobie z nimi radzić, gdy się pojawią. W końcu pojawią się, dopóki będziesz kontynuować nawigację online. Tylko nieliczni z nas stracą pieniądze z powodu hakerów internetowych. A wśród tych niefortunnych większość z nich popełni poważny błąd - na przykład zapomni wylogować się z konta na Facebooku na publicznym komputerze. Czy to ci się przydarzyło? Mój przyjaciel poniósł konsekwencje takiego niewinnego błędu. Nie miało to poważnych konsekwencji, ale mogło. Tak jak w prawdziwym życiu, nigdy nie należy ujawniać danych osobowych w Internecie. Nigdy przenigdy. Więc jeśli zostałeś zhakowany, czy były to umiejętności hakera, czy Twoja „własna" wina? Nie próbuję nikogo winić; takie sytuacje się zdarzają. Celem naszym jest zilustrowanie technik stawania się ninja online: kimś, kto nawiguje i nie jest widziany. A przede wszystkim nauczysz się wielu strategii, które zebrałem przez lata, aby zachować bezpieczeństwo w Internecie. Ostatecznym narzędziem, które omówimy, jest The Onion Routine Project (TOR). Pierwotnie opracowany przez wojsko, The Onion Routine Project narodził się w Naval Research Laboratory. Na szczęście w dzisiejszych czasach to niesamowite narzędzie programowe jest regularnie używane; i jest dostępny dla każdego w Internecie. Pozwala stać się niewidzialnym podczas codziennej nawigacji. W związku z tym TOR będzie pomocny w zmniejszaniu ryzyka wycieku danych do zera, o ile będziesz przestrzegać zalecanego użycia. Rozpocznijmy naszą podróż, aby stać się

doświadczonymi nawigatorami i opracować zestaw praktyk zapewniających bezpieczeństwo Twoich danych osobowych.

Dlaczego TOR jest opłacalnym rozwiązaniem?

Jak już zauważyliśmy, TOR to krótka nazwa routera cebulowego. Jego pierwotny rozwój przez wojsko miał na celu ustanowienie bezpiecznej sieci komunikacyjnej do celów rządowych. W dzisiejszych czasach serwery TOR pozwalają każdemu użytkownikowi stać się anonimowym online. Podobnie jak skórki cebuli (symbol TOR), ta usługa ma kilka warstw (routerów) do przenoszenia ruchu w celu ukrycia Twojej prawdziwej tożsamości. Tak więc każdy, kto chce poznać twoją tożsamość podczas korzystania z TOR, napotka kilka losowych serwerów TOR; co oczywiście nic nie znaczy. Głównym celem tego odchylenia ruchu jest to, że węzły w sieci TOR służą do kamuflażu prawdziwego źródła aktywności (Ciebie). Dzięki temu będziesz mógł pozostać ukryty przed usługami stron trzecich, które śledzą dane osobowe.

Jakie są zastosowania TOR?

Aby dodać kontekst do tego wszechstronnego narzędzia programowego, oto kilka przypadków, w których TOR może się przydać:

* Chcesz wyszukać jakieś informacje, ale NIE MASZ tego robić. Dlatego musisz zachować anonimowość.

* Chcesz uczynić nas publicznym komputerem, aby uniknąć wycieku danych osobowych.

* Nie chcesz udostępniać osobistej aktywności online reklamodawcom, dostawcom usług internetowych, witrynom internetowym i podobnym źródłom gromadzenia danych.

* Musisz unikać policji lub cenzury państwowej (najprawdopodobniej w krajach, w których obowiązują takie zasady) lub chcesz podzielić się wiedzą z organizacją taką jak WikiLeaks.

Poprawne działanie TOR

Poniższe wskazówki opisują DO, które sprawią, że Twoje doświadczenie z TOR będzie najbardziej satysfakcjonujące:

* Zainstaluj przeglądarkę TOR. Pobieranie przeglądarki TOR w systemie Windows jest dość proste. Wystarczy otworzyć oficjalną stronę pobierania przeglądarki TOR, znaleźć najnowszą wersję i postępować zgodnie z instrukcjami, aby zakończyć instalację. W innym systemie operacyjnym musisz postępować zgodnie z określonymi instrukcjami w zależności od systemu. W tym samym załączniku zamieszczę odniesienia do najczęstszych przypadków.

* Nie używaj torrentów z TOR. Sieć TOR nie jest przeznaczona do korzystania z połączeń peer-to-peer do udostępniania plików. W związku z tym będziesz źle korzystać z usługi i spowalniając przy tym połączenie wszystkich innych osób w sieci. Ponadto BitTorrent ujawnia Twój adres IP; w związku z tym ujawnisz swój identyfikator używając P2P, czyniąc TOR bezwartościowym.

* Nie zezwalaj na wtyczki przeglądarki. Czy osobiście tworzyłeś wtyczki? Najprawdopodobniej nie. Dlatego NIE wiesz, czy narzędzie programowe zbiera informacje o Twoim identyfikatorze podczas normalnego użytkowania. Dlatego zezwolenie na swobodne działanie dowolnego z takich programów stanowi ryzyko dla Twojej anonimowości.

* Użyj protokołu HTTPS. Węzeł opuszczający sieć TOR to najbardziej narażone punkty na Twoją anonimowość. TOR szyfruje informacje w swojej sieci i kamufluje źródło Twojej aktywności. Jednak aktywność poza siecią jest ujawniona. Co możesz z tym zrobić? Konsekwentnie używaj kompleksowego

szyfrowania, takiego jak SSL lub TLS. Możliwość korzystania z HTTPS przez cały czas zapewnia po prostu przełączenie dodatku HTTPS Everywhere lub podobnego w obsługiwanej witrynie. Witryny, które nie pozwalają na nawigację HTTPS, mogą ujawniać Twoją aktywność.

* Nigdy nie otwieraj pobranego dokumentu przez TOR podczas surfowania po Internecie. Wyobraź sobie więc, że właśnie pobrałeś dokument podczas korzystania z TOR. Teraz - niewinnie - kliknij nazwę dokumentu, aby rzucić okiem. Co się dzieje? Najprawdopodobniej przeglądarka otworzy obsługiwany dokument w formacie osobnej zakładki. Większość z tych dokumentów jest udostępniana przez Google Dysk lub podobne usługi przechowywania… które WYMAGAJĄ logowania do konta użytkownika. Będziesz więc surfować anonimowo i jednocześnie mówić „Hej, jestem John Sanders". Widzisz, niespójność? Rozwiązanie: NIE klikaj rzeczy, które otwierają więcej rzeczy podczas korzystania z TOR.

* Używaj mostów. Co robisz w prawdziwym życiu, gdy jest rzeka i bardzo chcesz ją przekroczyć bez dotykania wody? Płyniesz łodzią! Ok, nie jest to odpowiedź, której szukałem… przez większość czasu można dojść do mostu i skorzystać z niego, aby dostać się na drugą stronę. Pomysł jest prawie taki sam, gdy korzystasz z TOR; robisz z nas mosty (przekaźniki = bezpieczne przejścia), aby pozbyć się krytyki. Organizacja projektu Tor zapewnia również wiele pomostów dla użytkowników. Są to bezpieczne przejścia do nawigacji online bez narażania Twojego dowodu tożsamości. Dlatego konsekwentnie z nich korzystaj.

* Rekrutuj więcej użytkowników. Aby zostać wartościowym członkiem społeczności TOR, nie surfuj sam. Zadzwoń do znajomych; powiedz im o TOR. Pamiętaj, że im więcej jesteśmy online w TOR, tym silniejsza będzie sieć powoli, ale systematycznie.

Kiedy nie używać TOR?

Zachowanie anonimowości to nie to samo, co bezpieczeństwo w Internecie. W końcu sieć TOR jest daleka od idealnego rozwiązania w bardzo konkretnym scenariuszu; jest to projekt wciąż rozwijany. Aby skorzystać z TOR, potrzebujesz przeglądarki obsługującej ten protokół. Protokół nie został jeszcze zepsuty, ale przeglądarka jest tutaj najsłabszym ogniwem. Przeglądarka to program, który współdziała z użytkownikiem i siecią online. Niestety jest poddawany exploitom, na których ktoś inny może zyskać. Niedawno ogłoszono, że NSA jest w stanie odsłonić użytkownika sieci TOR. Oczywiście nie możesz obstawiać swoich szans na ucieczkę przed władzami za pomocą tej sieci. W związku z tym nielegalne zastosowania nie są „bezpieczniejsze" ani poza zasięgiem radaru, gdy aktywujesz TOR. Po prostu utrudniasz władzom kontakt z tobą; a i tak ostatecznie odniosą sukces. TOR nie jest narzędziem do zostania przestępcą; nie może być używane do celów niezgodnych z prawem. Nieprawidłowa manipulacja siecią zagraża społeczności TOR na całym świecie. Ta lista podsumowuje niektóre niezalecane zastosowania TOR:

* Anonimowe pobieranie dużych plików. Powód: najprawdopodobniej użyjesz P2P, takiego jak Torrent. W związku z tym spowolnisz połączenie wszystkich, aby nie uzyskać żadnych korzyści, tj. władze będą w stanie śledzić Twój rekord pobierania.

* Próba uniknięcia inwigilacji ze strony NSA. Powód: nie próbuj tego. To nie jest skuteczne w ten sposób. Po prostu nie.

* „Zabezpieczanie" Twojej aktywności online w sieciach społecznościowych. Powód: logiczną niespójnością jest korzystanie z usług wymagających Twojego dowodu tożsamości i jednoczesne staranie się zachować anonimowość, nie sądzisz? Poza tym nie będziesz w tym bezpieczniejszy; będziesz w równym stopniu narażony na eksploatację usługi.

* Nie powinieneś próbować wchodzić na oficjalne strony (rządowe lub podobne). Powód: każda osoba, która żąda takich usług, potrzebuje identyfikacji.

* Nielegalne wykorzystanie (pornografia dziecięca, nieautoryzowane zakupy, handel narkotykami itp.). Oczywiste powody: moralna niepoprawność i ściganie. Chociaż te zastosowania są powszechne z oczywistych powodów, są one nielegalne i mogą prowadzić do ścigania i więzienia bez ostrzeżenia. Środowisko TOR bardzo ułatwia korzystanie z przeglądarki do tych celów, ale nie były to zamierzone zastosowania TOR.

Jak widać, istnieje kilka scenariuszy, w których TOR jest rozwiązaniem Twoich problemów. Jednak w niektórych przypadkach nie zaleca się korzystania z tej usługi, aby nie przyciągać niepotrzebnej uwagi władz; pod warunkiem, że NSA i FBI obserwują jakiekolwiek podejrzane zachowanie w tej sieci. Odpowiedzialne korzystanie z TOR jest zawsze zalecane i jest to Twoja własna odpowiedzialność. Przyjrzyjmy się bardziej szczegółowo, jak działa ta cała sieć serwerów.

Jak działa TOR?

Cebula ma wiele warstw, które chronią - i formują - warzywo. Podobnie TOR jest siecią złożoną z kilku routerów, które służą jako „warstwy". Podobnie jak w prawdziwym odpowiedniku etui, warstwy zewnętrzne chronią wnętrze, w Twoim przypadku Twoją tożsamość. Wyobraź sobie, że musisz wysłać paczkę z wartościową zawartością. Jak możesz zabezpieczyć ten przedmiot przed dostawą? Możesz chwycić folię bąbelkową, aby przykryć przedmiot. Następnie możesz dodać dodatkowe warstwy, aby to zapewnić integralność. TOR działa w podobny sposób. Cennym przedmiotem są Twoje dane osobowe oraz zapytania, które przesyłasz do Internetu. Aby uniknąć łatwego śledzenia, TOR kieruje przepływem informacji przez różne punkty swojej sieci. Jest to odpowiednik posiadania kilku warstw chroniących Twój identyfikator online. Węzły sieci składają się z routerów i serwerów na całym świecie. Czy to brzmi prosto? Na szczęście nie potrzebujesz specyfikacji technicznych, aby skorzystać z usługi. Teraz przeanalizujmy poziom bezpieczeństwa TOR…

Jak bezpieczny jest TOR?

W życiu nie ma nic w 100% bezpiecznego. Nawet mieszkanie pod ogromnym kamieniem nie uchroni cię całkowicie przed zagrożeniami ze świata zewnętrznego. Dlatego nie ma powodu, aby wierzyć, że TOR jest bezpieczniejszy niż inne alternatywy w każdym przypadku. Chociaż rzeczywiście wyróżnia się w regularnych zastosowaniach, na przestrzeni lat ujawniono kilka słabych punktów. Ta lista podsumowuje niektóre exploity związane z TOR:

* Podsłuch w systemie autonomicznym (AS). Każdy może szpiegować ruch przychodzący i wychodzący z sieci TOR. Dzięki zaawansowanemu śledzeniu mogą wskazać Twój identyfikator lub lokalizację. Oczywiście nie jest to możliwe, chyba że naprawdę jesteś profesjonalistą w strategiach hakerskich.

* Podsłuchiwanie węzłów wyjściowych. Węzeł wyjściowy to punkt, w którym TOR nie ma już kontroli nad informacjami przesyłanymi do serwera, czyli łączy się z dowolnym komputerem na świecie. W związku z tym ekspert może odzyskać hasła, konta e-mail itp. Z tych punktów. Oczywiście, jeśli nie użyjesz żadnego z tych wewnątrz TOR, jesteś bezpieczny i zdrowy.

* Atak analizy ruchu. Chociaż tego rodzaju atak nie ujawnia ID, mogliby zebrać informacje o użytkowniku w sieci TOR. Nie jest to jednak duży problem.

* Blok węzła wyjściowego TOR. Niektóre strony internetowe blokują użytkownikom TOR, aby uniemożliwić dostęp do ich usług bez identyfikacji siebie. Dlatego nie będziesz mógł edytować Wikipedii podczas korzystania z TOR, korzystać z odtwarzacza online BBC i tak dalej.

* Zły atak jabłka. Ta luka polega na wykorzystywaniu słabych usług, takich jak klienci P2P BitTorrent wewnątrz TOR. Dlatego nie używaj takich połączeń do „pobierania" anonimowo; zamiast tego narazisz swoją anonimowość.

* Protokoły, które ujawniają adresy IP. Oprócz BitTorrent jest więcej protokołów, które ujawniają adres IP (a tym samym Twój prawdziwy identyfikator), takie jak komunikacja z trackerem P2P, rozproszone tablice skrótów itp. Ataki te koncentrują się na lukach w zabezpieczeniach man in the middle.

* Ataki snajperskie. Co jest gorszego niż atak typu „odmowa usługi" (DDoS)? Rozproszony odpowiednik; DDoS, czyli grupowy atak na węzły wyjściowe, aby atakujący mógł stwierdzić, z których korzystasz. Działa to w „prosty" sposób: blokujesz wystarczająco dużą liczbę węzłów, tak że użytkownik TOR będzie musiał polegać na jednym z nielicznych, które nadal działają. Co dostajesz? Wyższe prawdopodobieństwo wskazania węzłów, których „używasz"; stąd większa szansa, aby dowiedzieć się, kim jesteś. Oczywiście nie jest to do końca technika laika.

* Błąd krwawienia z serca. Ten błąd ujawnił i złamał hasła w kwietniu 2014 w sieci TOR. Te protokoły zostały wkrótce dezaktywowane. Istnieje jednak szansa, że w przyszłości pojawią się podobne luki, chociaż nie są one wysokie. Główną przesłanką uniknięcia takich problemów jest poleganie na usługach ukrytych;

* Odciski palców myszy. Ten jest trochę za pokręcony, ale działa. Porównanie kliknięć, które robisz w witrynie, z JavaScriptem do śledzenia ruchy myszy, ekspert udowodnił, że określenie tożsamości osoby jest „wykonalne". Na szczęście, jeśli nie korzystasz z publicznych komputerów, to ryzyko nie jest zagrożeniem.

* Atak polegający na pobieraniu odcisków palców. Były częściowo ujawnione wiadomości luki w zabezpieczeniach związanych z odciskami palców w sieci TOR. Dlatego lepiej nie używać bio trackerów.

* Informacje o objętości. Anonimowość oferowana przez TOR nie pozwala ukryć ilości danych, które poruszasz. Dlatego jeśli jesteś pod jakimkolwiek inwigilacją, mogą śledzić Twoje kroki nawet przy użyciu TOR.

* Inny. Z biegiem czasu coraz więcej exploitów będzie się pojawiać.

Niektóre z nich zostaną natychmiast rozwiązane; inne będą trwać dłużej, ale zostaną w jakiś sposób pominięte. Oczywiście, nie ma nic lepszego niż wszechstronny, nigdy nie używany system ochrony Twojego identyfikatora online; tak jak w prawdziwym życiu. Lista może wydawać się zniechęcająca do regularnego korzystania z TZW, ale tak nie jest. Jednak pokazanie możliwych zagrożeń jest częścią moich obowiązków w tym wprowadzeniu do usługi. Morał z tej historii jest następujący: TOR nie zapewnia 100% bezpieczeństwa Twojej aktywności online; tworzy anonimowość.

Ten krok jest raczej prosty. Do korzystania z TOR potrzebna jest przeglądarka zgodna z usługą. Możesz przejść do witryny internetowej projektu TOR, aby pobrać najnowszą wersję tego narzędzia programowego. W szczególności możesz być zainteresowany korzystaniem z przeglądarki TOR; co jest prawdopodobnie wszechstronną alternatywą, aby zacząć anonimowość online. Istnieją również dodatki do innych popularnych przeglądarek, takich jak Mozilla Firefox. Jeśli jesteś już użytkownikiem Mozilli, ta opcja może Cię zainteresować. Oczywiście funkcjonalności są nieco ograniczone w porównaniu z posiadaniem przeglądarki TOR; ale prostota instalacji dodatku jest niesparowana. Jeśli chcesz poznać zalety i wady obu opcji, oto kilka wskazówek.

Zalety i wady przeglądarki TOR

Oto najbardziej niezwykłe zalety i wady związane z używaniem TOR do nawigacji.

Zalety TOR

* Najbardziej niezawodne funkcje anonimowości. To świetna sieć, w której Twój identyfikator jest ukrywany w większości zastosowań i normalnych czynnościach w sieci; na przykład po prostu przeglądając wiadomości bez pozostawiania śladów.

* Dostęp do Deep Web (lub Dark Web). Soczysta, ale niebezpieczna strefa internetu. To „miejsce" nie jest objęte wyszukiwarkami - stąd jest po omacku. Ponadto w tej internetowej „czarnej dziurze" mają miejsce nielegalne działania. Powinieneś bardzo uważać na to, co robisz i gdzie surfujesz w tym miejscu - w przeciwnym razie możesz mieć problemy z władzami.

* Większość początkujących „hakerów" Cię nie zauważy. TOR natychmiast zapewnia niezawodną ochronę przed tymi, którzy widzieli zbyt wiele seriali lub filmów o hakowaniu. Nie dotkną cię, ALE prawdziwy haker może to zrobić. Więc nie myśl, że jesteś w 100% bezpieczny.

*Więcej. TOR ustanawia standard przeglądania prywatnego, jest przenośny, dostęp jest ukryty za pośrednictwem witryn .onion.

Wady TOR

* Wydajność nie jest dla wybrednych. Chociaż wydajność poprawiła się w ciągu ostatnich kilku lat; nie przypomina to normalnego przeglądania. Jednak musi być cena za takie dodatkowa warstwa anonimowości, nie sądzisz?

* Nie jesteś w 100% bezpieczny ani niewidoczny. Władze cię obserwują. Nie zapomnij tego. NSA i FBI bardzo poważnie traktują tę anonimową działalność. Jeśli zbyt często lub przypadkowo trafisz na nielegalne witryny internetowe w Dark Web; znajdą cię. Unikaj ich za wszelką cenę. Nie bój się jednak, jeśli popełnisz błąd (np. Przypadkowo wejdziesz na nielegalną stronę internetową) i działasz poprawnie (A. Natychmiastowe wyjście lub B. Zgłoś stronę), po Twojej stronie nie będzie już więcej problemu. Nie ma też nic do ukrycia. Oczywiście mogą zadać ci kilka pytań. Parafrazując starego wuja Bena „wielka moc wymaga wielkiej odpowiedzialności". Tak więc, jako obywatel zawsze wybierasz, czy postępujesz właściwie.

*Reputacja. Wszystkie poprzednie problemy z władzami związane z nadużyciem TOR prowadzą nas do tego punktu. Niestety społeczność TOR ma na odwrocie żniwo. Jednak jest to miecz obosieczny; stał się bardzo popularny wśród dziennikarzy i aktywistów na całym świecie. Zawsze jest miejsce na cenny wkład z wykorzystania TZW.

*Małe opóźnienia. To naprawdę częsty problem w sieci TOR. Więc, lepiej bądź cierpliwy. Ten, kto jest cierpliwy, znajdzie to, czego szuka.

Plusy i minusy Mozilli

Oto najbardziej niezwykłe cechy korzystania z dodatkowej wersji usługi TOR do Mozilli. Przyjrzyjmy się im, abyś sam zdecydował, czy to się opłaca.

Zalety dodatku Mozilla

* Bezpłatna społeczność open source. Wszystkie produkty Mozilli mają licencję publiczną. Dlatego każdy programista może przyczynić się do ulepszenia usługi. Co więcej, każdy może upewnić się, że usługa NAPRAWDĘ zapewnia to, co twierdzi. Przejrzystość jest kluczowym czynnikiem w społecznościach open source.

* Dostosowywanie. Tak jak to zwykle bywa w Mozilli, możesz dostosować dodatek do swoich preferencji. Dzięki temu będziesz mieć zupełnie wyjątkowe wrażenia z przeglądania.

*Społeczność. Większość użytkowników preferuje tę wersję usługi TOR; zwłaszcza zwolenników Mozilli. Mozilla Firefox to wszechstronna, solidna przeglądarka, która jest wysoce kompatybilna z większością urządzeń i systemów operacyjnych. Jeśli więc zmienisz urządzenie w przyszłości, nie wpłynie to zbyt poważnie na Twoje wrażenia. Ponadto wsparcie społeczności jest zawsze plusem.

* Więcej. Istnieje duża lista funkcji, na które warto zwrócić uwagę, takich jak silny ciągły rozwój, solidna obsługa HTML5, synchronizacja urządzeń, tagowanie zakładek, tryb czytnika bez rozpraszania w celu ulepszenia skanowania, automatyczne aktualizacje, szybkie zarządzanie zakładkami, najniższe obciążenie pamięci i procesora, integracja z Pocket, aby zapisywać strony w podróży.

Wady dodatku Mozilla

* Instalacja rozszerzeń wymaga ponownego uruchomienia. Jest to nieznośna sytuacja, pod warunkiem, że nie każde rozszerzenie obsługuje uruchamianie bez ponownego uruchamiania. W związku z tym,

lepiej bądź cierpliwy.

* Niska wydajność w niektórych systemach operacyjnych. Najwyraźniej użytkownicy zwracają uwagę, że wydajność w OS X jest znacznie wolniejsza niż w Windows czy Linux. Dlatego zachowaj ostrożność, jeśli jesteś użytkownikiem komputera Mac.

* Stawką jest trwałość przedłużek. Przedłużenie życia to ujawniona tajemnica w Firefoksie. Dzieje się tak, że Firefox ma swoje własne tempo, a rozszerzenia mają swoje. Dlatego może się zdarzyć, że dane rozszerzenie zostanie pozostawione i stanie się bezużyteczne, ponieważ jest przestarzałe. Jeśli więc polegasz na rozszerzeniu, aby poprawić swoje wrażenia, weź również pod uwagę aktywność programistów w aktualizacjach.

* Więcej. Istnieją inne wady korzystania z nawigacji Firefox dla TOR, ale są one głównie sytuacyjne (tj. Wpływają tylko na mniejszość użytkowników w niektórych przypadkach). Na przykład istnieje wsparcie dla przedsiębiorstw. Możesz to zignorować, jeśli jesteś osobą indywidualną korzystającą z Internetu w domu. Ponadto nie ma obsługi HDiDPI; na ekranach o wysokiej rozdzielczości ikony są niewyraźne. Nie zauważysz tego, chyba że przeglądasz na ekranie 4K.

Jak zacząć

Więc teraz masz do dyspozycji przeglądarkę TOR lub odpowiednik dodatku - a może obie! Czas wypróbować kilka podstawowych zadań online, aby zobaczyć różnicę w porównaniu z przeglądaniem bez funkcji anonimowych. W następnej sekcji omówimy najbardziej odpowiedniego kandydata do usług TOR. Przeczytaj szczegółowo tę sekcję, aby zrozumieć, czego możesz oczekiwać od tej usługi, a czego nie. Zawsze odpowiedzialnie używaj tego niesamowitego narzędzia.

Czy jesteś odpowiednim użytkownikiem dla TOR?

Powiedzieliśmy już, że TOR nie jest dla wszystkich. Uważam, że najlepszym sposobem zrozumienia, dla kogo jest przeznaczona TOR, jest przejrzenie najbardziej zalecanych praktyk, które są zgodne z tą usługą. Przyjrzyjmy się najlepszym DO, aby odnieść sukces jako użytkownik TOR. W tym rozdziale omówiono niektóre z najbardziej odpowiednich zorientowanych na bezpieczeństwo i przyjaznych anonimowości praktyk dla użytkowników online.

Zmień swój system operacyjny (OS) i inne…

Exploity „Winbug" są nieco legendarne. Najczęściej używany system operacyjny na świecie został zaprojektowany tak, aby był przyjazny dla użytkownika. Dlatego nie udało się uniknąć luk w zabezpieczeniach. Zmiana na inny system operacyjny może wydawać się radykalna, ale w dłuższej perspektywie może się okazać, że korzyści są znaczne. Systemy Linux są w pełni kompatybilne z TOR. W rzeczywistości istnieją dystrybucje skonfigurowane jako TOR, takie jak Tails i Whonix. Mac jest również kompatybilny z TOR, wystarczy zainstalować przeglądarkę i gotowe; jest również bezpieczniejszy niż Windows.

Być na bieżąco

W każdym razie, niezależnie od używanego systemu operacyjnego, aktualizuj system. Nie należy tego pomijać, pod warunkiem, że stare wersje zawierają exploity powszechnie znane złośliwym hakerom. Dlatego należy aktualizować wszystko tak, jak to tylko możliwe; Twój system operacyjny i przeglądarka TOR.

HTTPS Everywhere

Możesz się zastanawiać, jak używać https w witrynie, która oferuje tylko wersję http. Na szczęście istnieje rozwiązanie o nazwie HTTPS Everywhere. Obsługiwane strony internetowe automatycznie przełączają się na przeglądanie w trybie HTTPS przy użyciu tego dodatku.

Zaszyfruj swoje dane

Po co więc zawracać sobie głowę anonimowością w Internecie, jeśli nie korzystasz z dodatkowych warstw bezpieczeństwa, takich jak cebula - dzwonek? LUKS i TrueCrypt to dwa narzędzia programowe, które umożliwiają szyfrowanie w systemach Linux. Im więcej szyfrowania, tym większe bezpieczeństwo.

Uważaj na pakiet TOR

Wbrew powszechnemu przekonaniu użycie tego pakietu może przynieść efekt przeciwny do zamierzonego. Tak, dodajesz dodatkową warstwę, ale są luki, które zostały ujawnione przez FBI. Uważaj na nadużywanie tych narzędzi.

Wyłącz Java Script, Flash i Javę

Te obrzydliwe skrypty mogą udostępniać Twoje dane osobowe, nie dając Ci szansy na uniknięcie tego. Po prostu je wyłącz, aby cieszyć się surfowaniem z większą anonimowością.

Brak P2P

To chyba trzeci raz, kiedy o tym wspominam, ale jest to kwestia kluczowa. Jeśli korzystasz z połączeń peer-to-peer, ujawniasz się.

Brak plików cookie i danych lokalnych

Dodatki, takie jak samoniszczące się pliki cookie, automatycznie usuwają niepożądane fragmenty informacji. Mogą przechowywać dane osobowe; więc bez żadnego z nich będziesz bardziej anonimowy.

Brak prawdziwego e-maila

Nigdy, przenigdy nie twórz nam własnych rachunków rzeczywistych w TOR. W przeciwnym razie będziesz mówić ludziom „Hej, witaj świecie. Jestem anonimowy. Podpis: John Smith ". Widzisz problem?

Brak Google

Najpopularniejsza wyszukiwarka na świecie aktywnie gromadzi dane osobowe. Będziesz więc bezpieczniejszy, korzystając z innej wyszukiwarki, takiej jak DuckDuckGo lub StartPage

Rób legalne rzeczy

Wreszcie, przestrzegaj przepisów i przepisów podczas surfowania po Internecie. NSA i FBI obserwują codziennie 24 godziny na dobę, 7 dni w tygodniu, aby dowiedzieć się, kto niewłaściwie korzysta z usług tego rodzaju. Lepiej nie zwracać na to zbędnej uwagi, przestrzegając w 100% przepisów. Oczywiście, jeśli omijasz zakazy ze strony swojego rządu, staraj się zachować jak największą anonimowość. Możesz polegać tylko na usługach ukrytych w celu ustanowienia bezpiecznych kanałów komunikacji, anonimowego wysyłania plików i tym podobnych. Prawdopodobnie jednym z najbezpieczniejszych sposobów korzystania z TOR jest sprawdzanie wiadomości bez interakcji z jakąkolwiek witryną, usługą itp. Jeśli wybierzesz tę opcję, pamiętaj, że im mniej interakcji masz ze stronami internetowymi, tym bardziej dyskretny staniesz się . Przechodząc do następnej sekcji, teraz dowiemy się, jakie informacje będziesz przeglądać podczas surfowania w TOR. Przyjrzyj się z bliska szerokiemu zakresowi możliwości, jakie ta sieć daje do Twojej dyspozycji; zaczynając od Hidden Wiki.

Pierwsze kroki z TOR

Do tego czasu wybrałeś już jedną opcję, albo przeglądarkę TOR, albo odpowiednik dodatku Mozilla, aby nawigować anonimowo. Znasz również ryzyko i korzyści, jakie niesie ze sobą ta internetowa aktywność przypominająca ninja. Dlatego nadszedł czas, aby dowiedzieć się, co dokładnie możesz zrobić ze swoim nowym statusem anonimowości. Kiedy uruchamiasz przeglądarkę TOR, masz wrażenie, że wystrzeliwuje się bombę dymną, którą ninja robią w filmach.

Zostań ninja

Możesz się zastanawiać, co zrobić w TOR teraz, gdy wylogowałeś się z każdej innej aplikacji (aby uniemożliwić im udostępnianie danych). Oto najbardziej zalecane pierwsze kroki w Deep Web. Ukryta Wiki

Ta witryna ma podobny układ niż Wikipedia; jest to odpowiednik TOR. Możesz tam przeglądać interesujące Cię kategorie, aby znaleźć preferencje. The Hidden Wiki to miejsce, w którym wymienione są wszystkie witryny .onion w Deep Web, na różne tematy. Znalezienie ukrytej Wiki jest proste, po prostu wpisz je w wyszukiwarce DuckDuckGo za pomocą TOR, a dostęp do tego centrum Wiki dzieli Cię tylko jedno kliknięcie. Możesz znaleźć tutaj dość dużą listę stron internetowych, takich jak:

• Punkty wprowadzenia. Są to najpopularniejsze strony internetowe, do których użytkownicy mają dostęp w pierwszej kolejności po uruchomieniu przeglądarki TOR. W większości przypadków odwiedzasz te strony za pomocą StarPage, wbudowanej wyszukiwarki TOR.

• Aktualności. To jeden z głównych powodów, dla których warto korzystać z TOR. Możesz ominąć rządowe zakazy, cenzurę i zakazy sprawdzania międzynarodowych wiadomości bez ograniczeń. W TOR znajdują się portale umożliwiające śledzenie najnowszych wiadomości; sprawdź te, które są często aktualizowane.

• Historia. Wbrew powszechnemu przekonaniu historia nie jest nauczana w ten sam sposób w każdym kraju. Co więcej, istnieją narody, które zmieniają rzeczywiste wydarzenia historyczne zgodnie z osobistymi przekonaniami, interesami politycznymi i tak dalej. Stąd, podobnie jak w przypadku wiadomości, TOR oferuje bezstronną wersję faktów.

• Usługi komercyjne. Chcesz kupić przedmiot bez ujawniania swojego identyfikatora? Oczywiście mogą istnieć prostsze sposoby. Jednak wzrost liczby bitcoinów umożliwia jak najbardziej anonimowy zakup przedmiotów w społeczności internetowej. Oczywiście możesz zostać odkryty, jeśli ktoś śledzi twoje kroki, ale ogólnie będzie to trudniejsze w TOR.

• Fora. Chcesz omówić sprawę anonimowo? Istnieją aplikacje, które oferują tę usługę, takie jak społeczność pytań i odpowiedzi, którą Quora ma obecnie w języku angielskim i hiszpańskim. Możesz tam zadać pytanie i anonimowo odpowiedzieć społeczności; programiści oczywiście wiedzą, kim jesteś. Jeśli jednak chcesz pójść o krok dalej, obejmując swoje dane osobowe, możesz rozważyć skorzystanie z forów wewnątrz TOR i usług ukrytych.

• Inne „niebezpieczne" tematy, takie jak Hack, Phreak, Anarchy, Warez, Virus i Crack itp. Podczas przeglądania TOR staraj się unikać wszelkich potencjalnie nielegalnych witryn internetowych. W niektórych przypadkach strony internetowe mogą pojawiać się bez możliwości zapobiegania temu. Jednak zwracanie uwagi na informacje dookoła jest jedynym niezawodnym sposobem na uniknięcie źródeł nielegalnej działalności w jak największym stopniu. Możesz nie być w stanie uniknąć wyskakujących okienek, ale możesz je natychmiast zamknąć bez interakcji, prawda? Ta sama zasada dotyczy regularnego korzystania z Internetu.

Głównym katalogiem stron internetowych wewnątrz TOR jest Hidden Wiki. Chociaż listy witryn internetowych w Ukrytej Wiki nie zawsze są aktualizowane; biorąc pod uwagę, że niektóre z nich mogą być offline jakiś czas temu, nadal jest to realne źródło adresów cebulowych. Należy pamiętać, że trwałość witryn wewnątrz TOR jest bardziej zmienna niż w bardziej dostępnej części Internetu. Po znalezieniu interesujących Cię stron internetowych radzę uważnie je dodać do zakładek. W przeciwieństwie do zwykłego przeglądania, adresy URL TOR są prawie niemożliwe do zapamiętania. Co więcej, katalogi mogą nagle się drastycznie zmienić, zmuszając cię do dokładnego przeszukiwania przez chwilę. Inteligentne wykorzystanie zakładek zawsze będzie niezawodnym źródłem adresów po Twojej stronie.

Onion Chat

Istnieją również pokoje rozmów, które obsługują anonimową komunikację, znane jako OnionChat. Są wspierane przez usługę TOR, dzięki czemu dostępność usługi jest bardziej trwała. Jeśli zdarzy się, że masz znajomych korzystających z TOR, możesz użyć tych czatów jako środka komunikacji. W końcu po co zawracać sobie głowę anonimowością, jeśli nie zamierzasz w 100% przyznać się do tego statusu, prawda? Używanie pseudonimów jest powszechną praktyką podczas rozmów w TOR. Nigdy nie używaj prawdziwych nazwisk.

New Yorker Strongbox

To jest witryna do bezpiecznych transmisji, których autorzy używają do wysyłania wiadomości lub plików do redakcji New Yorker. To jest anonimowe. Po uzyskaniu dostępu otrzymasz kryptonim, aby nigdy nie ujawniać swoich danych osobowych. Większość blogerów, którzy utrzymują strony internetowe w sieci TOR, rzadko publikuje posty; więc możesz nie otrzymywać nowych kanałów od osób, które lubisz czytać w tej strefie światowej sieci.

Inne istotne wzmianki

Niestety TOR nie jest narzędziem, które wszyscy teraz opanowali. Gdy znajdziesz się w Deep Web, jesteś całkowicie wolny. Dlatego uczucie samotności jest silniejsze niż podczas normalnej nawigacji. Co więcej, dość krótki średni czas życia stron internetowych nie pomaga w zmniejszeniu tego wrażenia. Tak więc, gdy szukasz informacji za pomocą TOR, zasadą numer jeden ma być cierpliwy. Pozornie

wszechobecność małego opóźnienia w służbie wymaga również większej wytrwałości niż zwykle. Punktem wyjścia jest Hidden Wiki; rodzaj nieoficjalnego katalogu, w którym zawsze można znaleźć świeże pomysły na zaplanowanie nawigacji. Następnie uzyskujesz dostęp do jednej witryny; sprawdź zawartość, kliknij linki i tak dalej. Oczywiście przez cały czas należy trzymać się z dala od podejrzanych źródeł.

Porady i wskazówki

W tej sekcji podsumowuję przydatne codzienne praktyki, które uzupełnią regularne korzystanie z TOR do celów nawigacyjnych i komunikacyjnych.

Bezpieczne przeglądanie

Pamiętaj, że TOR jest tak skuteczny, jak twoje nawyki surfowania w zakresie anonimowości osobistego identyfikatora. Domyślnie TOR NIE łączy się z Google. Najbardziej znana wyszukiwarka na świecie służy do gromadzenia danych osobowych; gromadzi obszerne dzienniki wszystkiego, czego szukasz w usłudze. Zamiast tego TOR łączy się ze „Stroną początkową", pośrednikiem między Tobą a oogle; tak, że sesja jest całkowicie niezidentyfikowana. Używając strony początkowej jako przekaźnika, zapewniasz, że Twoje wyszukiwania nie są przypisane - ani możliwe do prześledzenia - ze źródłem Twojej aktywności; czyli ty. Przynajmniej nie w żaden prosty sposób; Pomijam poziom inspekcji NSA dla tej obserwacji. TOR nie jest w stanie kontrolować zachowania rozszerzeń, skryptów i stron internetowych. Dlatego najlepszym sposobem uniknięcia tego potencjalnego ryzyka jest zapobieżenie ich wystąpieniu. Domyślnie przeglądarka TOR nie pozwala na taką aktywność. Nie zaleca się zmiany tego ustawienia w żadnym momencie nawigacji, aby uniknąć niepotrzebnego narażenia. Czy wiesz, że możesz oglądać transmisje strumieniowe anonimowo? Chociaż może nie działać za każdym razem; YouTube ma teraz uruchomioną usługę HTML5 beta. Domyślne filmy flash tej słynnej witryny nie są dostępne podczas korzystania z TOR ze względu na luki w zabezpieczeniach protokołów Flash. Dlatego możesz nie cieszyć się tym doświadczeniem tak bardzo, jak w normalnym trybie surfowania. Wreszcie, TOR ostrzeże Cię o dokumentach i plikach, które mogą potencjalnie ujawnić informacje o Twoim identyfikatorze - przypadkowo lub celowo. Zaleca się uważne przyjrzenie się takim ostrzeżeniom; przekonasz się, że nie warto ryzykować.

Anonimowe wiadomości

W normalnym trybie nawigacji nie ma to jak anonimowe wiadomości. Każdy klient do obsługi wiadomości, o którym myślisz, ma dzienniki monitorowania Twoich „prywatnych" czatów - takich jak czaty Google, Facebook, Skype i tym podobne. Jak więc możemy uciec na chwilę przed „Wielkim Bratem", aby wysłać nieujawnione wiadomości? Na szczęście TorChat właśnie to umożliwia. Możesz używać tej anonimowej aplikacji do czatu nawet w formie rozszerzenia. Aby skorzystać z tej usługi, przejdź do oficjalnej witryny usługi i pobierz folder zip. Znajdziesz tam plik wykonywalny do uruchomienia aplikacji. Ten klient czatu działa tak samo, jak każdy inny komunikator; układ będzie bardzo intuicyjny. Niezwykła różnica w porównaniu ze zwykłymi klientami do przesyłania wiadomości polega na tym, że zamiast prawdziwego imienia i nazwiska w usłudze będziesz reprezentowany przez losowy zestaw znaków. Na szczęście możesz zmienić nazwy kontaktów, aby ułatwić nawiązywanie rozmów - zalecane są kryptonimy. Ponadto, ponieważ usługa działa w tle TOR; nikt w sieci nie będzie w stanie określić, z kim komunikujesz się w danym momencie.

Crypto Messaging

Jeśli chcesz pójść o krok dalej, możesz wypróbować wiadomości kryptograficzne za pośrednictwem TOR. Jednak te usługi nie działają w tle jak poprzednie. Mocną stroną jest to, że wiadomości - chociaż

przechwycone - są trudniejsze do odszyfrowania jako takie. Jednym z powszechnych wyborów jest „Cryptocat", który jest dostępny na jego oficjalnej stronie internetowej.

Anonimowy e-mail

A co z e-mailami? Wysyłanie niezidentyfikowanych wiadomości jest dopuszczalne, ale czasami może być konieczne wysłanie zamiast tego wiadomości e-mail. Wśród „usług ukrytych" dostępnych w TOR jest oczywiście e-mail. Należy jednak pamiętać, że każda usługa ukryta JEST dostępna TYLKO wewnątrz TOR; może nie istnieć w sieci bez naruszenia informacji identyfikacyjnych. Aby skorzystać z poczty TOR, wystarczy otworzyć stronę internetową tej usługi z sieci TOR. Postępuj zgodnie z instrukcjami, aby się zarejestrować i rozpocząć. Główną zaletą takiej usługi jest brak możliwości wyszukania dostępu do niej spoza sieci TOR. Układ nie różni się zbytnio od układu poczty Gmail i Yahoo, więc będzie bardzo intuicyjny.

Głęboka sieć

W tej sekcji omówimy więcej usług ukrytych. Ponadto odbędzie się kolejny przegląd ograniczeń i obaw dotyczących bezpieczeństwa.

Usługi ukryte

Mówiliśmy już o najczęstszych usługach ukrytych, które użytkownicy lubią rozważać w TOR. W miarę czytania tych wierszy coraz więcej tych usług jest opracowywanych, a inne stają się przestarzałe; Deep Web podlega ciągłym zmianom.

Dlaczego warto korzystać z usług ukrytych?

Korzystanie z usługi ukrytej w TOR jest idealnym rozwiązaniem problemów prywatności, ponieważ nigdy nie jest ona narażona na zewnętrzne szpiegostwo (ze zwykłego Internetu). Dlatego takie usługi nie są wyłączane ani blokowane. Można łatwo odmówić dostępu do regularnych usług internetowych. Przeanalizujmy to na prostym przykładzie. Mogłem bardzo dobrze wysyłać ogromne pakiety danych do routera mojego sąsiada, aby odmówić mu dostępu do Internetu z powodu nasycenia. Innymi słowy, mogę zakłócać komunikację między routerem a komputerem, którego używa mój sąsiad. Ale ja nie, jestem dobry

sąsiad! Gdyby jednak mój sąsiad chciał zachować usługę dla siebie, łącząc dwa komputery na swoim miejscu, wystarczyłby kabel, aby zapobiec jakiejkolwiek interwencji spoza domu. Po prostu wyłącz Wi-Fi. Widzisz, dokąd jadę? Podobnie, zwykłej usłudze internetowej można odmówić „łatwo" - możesz potrzebować tysięcy komputerów, aby odrzucić oficjalną witrynę, ale zasada jest taka sama: spam. Połączenia wewnętrzne są jak sieć TOR, po prostu dlatego, że nie można odmówić anonimowym serwerom cebulowym. Dlatego możesz codziennie przeczytać e-mail TOR lub skorzystać z prywatnego czatu. Ponadto ludzie lubią korzystać z anonimowych usług do przesyłania swoich kryptowalut, takich jak niesławne Bitcoiny.

Korzystanie z zakładek

Konsekwentne używanie zakładek to umiejętność, której potrzebujesz podczas surfowania w Deep Web. Należy pamiętać, że typowy link w sieci TOR wygląda następująco: http: // [tu kilka losowych znaków] .onion

Innymi słowy, zapamiętanie adresów stron internetowych lub usług w TOR jest prawie niemożliwe ze względu na losowe znaki w adresach URL. Dlatego zakładki to Twoi najlepsi przyjaciele, po których

możesz nawigować tak, jak lubisz. W Deep Web nie ma Google ani stron indeksowanych przez zwykłe wyszukiwarki. Jak więc możesz tam znaleźć informacje?

TorSearch

Ta usługa jest odpowiednikiem Google inside TOR; ale bez ciągłego pobierania danych osobowych z Twojej strony przy każdym wyszukiwaniu. Ta usługa działa na tej samej zasadzie, co wyszukiwarka Google. Wraz z włączeniem TorSearch natężenie ruchu w sieci gwałtownie wzrosło. Obecnie znacznie się poprawił od pierwszych etapów. Znalezienie danej usługi ukrytej, witryny internetowej i w zasadzie wszystkiego, co chciałbyś znaleźć w Deep Web, jest znacznie prostsze niż kiedykolwiek. Oczywiście ukryta Wiki pozostaje punktem odniesienia dla każdego, kto chce przeglądać kategorie w celu znalezienia własnych zainteresowań. Ta strona jest moderowana, aby pokazywać tylko publiczne i „akceptowalne" treści dla wszystkich odbiorców. Ograniczenia, zagrożenia i inne kwestie do rozważenia Chociaż TOR oferuje doskonałe rozwiązanie w zakresie anonimowości online, nie jest zwolnione z luk w zabezpieczeniach. Pod warunkiem, że przeglądarka TOR jest zmodyfikowaną wersją odpowiednika Mozilla Firefox, te same exploity mogą mieć zastosowanie. Ponadto jesteś narażony na trojany, nawet jeśli korzystasz z regularnego przeglądania. W końcu nigdy nie wiadomo, kiedy i gdzie natkniesz się na wirusa, prawda? Inną wadą korzystania z przeglądarki TOR jest to, że zwrócisz uwagę NSA i być może innej podobnej agencji rządowej. Są w stanie śledzić Twoją aktywność, aby zrekonstruować Twoje kroki online. Dlatego naprawdę musisz uważać na kliknięcia podczas surfowania. Nawet pojawienie się na nielegalnych witrynach może powodować problemy z władzami. Uważaj, zostałeś ostrzeżony.

Witryny internetowe, na które należy uważać

Oprócz Hidden Wiki masz również wyszukiwarki produktów wewnątrz TOR. Należy jednak uważać na wszelkiego rodzaju oszustwa. Możesz trzymać się z daleka od niektórych z tych wyszukiwarek, aby uniknąć problemów z władzami, takimi jak Grams, słynna witryna internetowa, która nabrała rozpędu w TOR. Ta wyszukiwarka jest jak replika Google, która jest połączona z kryptowalutami narkotyków. Dlatego uważaj, jeśli spróbujesz znaleźć przedmiot za pomocą tego narzędzia. Jeśli chodzi o rynki internetowe, masz między innymi Śródziemie, Agorę i Evolution. Chociaż Śródziemie oferuje więcej funkcji na swojej platformie, odpowiedniki przytłaczają rynek. Powodem tego sukcesu po stronie Agory i Evolution jest większa niezawodność ich usług; co jest ogromnym atutem w Deep Web. Przed zakupem w TOR upewnij się, że rozumiesz proces i rozumiesz usługę / przedmiot, który otrzymujesz; i możliwe konsekwencje - jeśli takie istnieją. Ponadto uważaj na metodę płatności; nigdy nie będziesz chciał ujawniać swoich danych osobowych. Jeśli jesteś w stanie zdobyć trochę Bitcoinów, jest to najbezpieczniejszy sposób zakupu w TOR.

Wreszcie, przed podjęciem ostatecznej decyzji przeczytaj referencje usługi. W niektórych witrynach użytkownicy mają bardzo aktywne społeczności. Oczywiście, jeśli nie możesz znaleźć wystarczających informacji o usłudze lub stronie internetowej; unikać korzystania z ich ofert.

Więcej obaw dotyczących bezpieczeństwa treści

Surfowanie po TOR może być potencjalnie bardziej niebezpieczne niż w zwykłej sieci. W tej sekcji przeprowadzamy analizę bezpieczeństwa rodzajów treści, które można znaleźć w sieci TOR.

• Dynamiczna treść. Tego rodzaju witryny wymagają zapytań lub formularzy podczas nawigacji. Aby przeglądać te witryny, będziesz potrzebować doświadczenia z domenami.

• Treści niepowiązane. Te witryny nie są indeksowane przez wyszukiwarki. Ponadto w tych witrynach nie ma linków zwrotnych ani wewnętrznych.

• Prywatne sieci. Witryny wymagające logowania, aby były dostępne. Uważaj na potencjalne luki w zabezpieczeniach prywatnych danych lub fałszywe dane logowania, które mogą spowodować, że będziesz ujawniać informacje osobiste o sobie.

• Sieci kontekstowe. Kontekst dostępu do tych witryn może się różnić. Na przykład mogą polegać na poprzednich klientach.

• Ograniczony dostęp do treści. Witryny te wdrażają standardy wykluczania robotów, CAPTCHA i tym podobne. W związku z tym unikają systematycznego indeksowania przez wyszukiwarki.

• Treść oparta na skryptach. Ten rodzaj witryn wymaga linków utworzonych za pomocą JavaScript lub innego klienta oprogramowania, takiego jak Flash, Ajax i pokrewne.

• Oprogramowanie. Aby uzyskać dostęp do tego rodzaju witryn internetowych, wymagane są aplikacje lub programy.

• Archiwa internetowe. Niektóre archiwa umożliwiają sprawdzenie starej wersji innych witryn internetowych. Przechowują te starsze wersje do przyszłych kontroli.

Jak widać, treść pojawia się w różnych formatach online albo podczas zwykłego przeglądania, tak jak to się dzieje w TOR. Dlatego umiejętność dostrzeżenia różnicy jest ważna, aby zrozumieć, jak bezpieczne mogą być strony internetowe lub usługi. Ogólnie rzecz biorąc, unikaj instalowania programów lub uruchamiania plików wykonywalnych, które znajdziesz losowo w Internecie, aby zminimalizować ryzyko.

Przyszłość Deep Web

Niestety musiała to być ostatnia niestabilność polityczna na Bliskim Wschodzie, jeden z głównych powodów zwiększenia wykorzystania TZW. W ciągu ostatnich kilku lat możliwości wykorzystania tego oprogramowania i sieci były konsekwentnie pokazywane. Ludzie unikają cenzury ze strony swoich rządów z wielu powodów - w niektórych przypadkach po to, aby zobaczyć filmy z kotami online na Facebooku. Jednak w Deep Web jest znacznie więcej. W rzeczywistości nikt nie może powiedzieć, ile informacji jest przechowywanych w Deep Web; sekcja Internetu, która nie jest indeksowana przez wyszukiwarki. Kilka lat temu oszacowano, że TOR zawiera kilka petabajtów informacji. Jednak kwota ta może gwałtownie wzrosnąć w ciągu ostatnich kilku lat. Może być dziesięciokrotnie, stokrotnie; lub nawet więcej niż te wstępne szacunki. Możesz przekonać się - w ostatniej części dodatku do tej książki - jak łatwo jest stworzyć własny serwer w TOR. To już nie jest fizyka jądrowa; tylko procedura laika w tej chwili. Istnieje mnóstwo samouczków, z którymi możesz skorzystać, aby wymyślić jedną własną ukrytą usługę. Tak jak ty jesteś w stanie to zrobić, tak samo jest z ludźmi z całego świata. Dlatego zawartość w TOR rośnie wykładniczo. Użytkownicy doceniają korzyści płynące z anonimowych interakcji online, aby poczuć - czasem nieuzasadnione - poczucie bezpieczeństwa. Nigdy nie zapominaj, że TOR tak naprawdę nie chroni Cię bardziej niż przeglądarka Firefox. Te same exploity mogą potencjalnie mieć zastosowanie do obu usług w w danym momencie. Co więcej, ponieważ popularność korzystania z TOR pozostaje nadal wysoka, więcej hakerów może próbować przechwytywać dane osobowe w sieci w celu wykorzystania w złośliwy sposób. Dlatego jest to miejsce, na które należy uważać. Deep Web nie jest tak delikatny, merytoryczny i oszukańczy, jak zwykły odpowiednik. To jak w prawdziwym świecie, ale bez żadnych zasad ani nadzoru. To jest problem, pod warunkiem, że wiesz już, jak „łatwo" jest natknąć się na oszustów w Internecie. Istnieje mnóstwo witryn internetowych, które próbują nakłonić Cię do podjęcia błędnych decyzji za pomocą pieniędzy; w większości przypadków kończy się to marnowaniem dolarów na próżno. To zagraża wiarygodności uczciwych dostawców. Jednak taki właśnie jest Internet; to się nie zmieni w dającej się przewidzieć przyszłości.

Czy to oznacza, że nie możesz korzystać z WWW? Oczywiście, że tak nie jest. Istnieje również ryzyko wypadku, gdy wychodzisz z domu - a nawet z domu. Stosując tę samą tendencyjną logikę, powinieneś po prostu leżeć w łóżku, aby być „bezpieczniejszym". Codziennie pracuję online. Robię to od ponad dziesięciu lat; Będę to robić za dziesięć lat. Wiesz co? Nie mogę się doczekać, aby zobaczyć, jak jeden z najbardziej zdumiewających wydarzeń w historii ludzkości będzie ewoluował w ciągu następnych kilku lat; Internet zmienił nasze życie. Wyobraź sobie, jak komunikacja była pół wieku temu, pamiętaj, jaka jest teraz. Pamiętaj, jak wyglądało kupowanie przed internetem, trzeba było być osobiście w każdym sklepie, dopóki nie znalazłeś cennego przedmiotu, którego szukałeś. Wyobraź sobie, jak dawno temu była jazda, bez GPS; tylko ty i droga; i być może mapa.

Obawy dotyczące prywatności

Teraz błyskawicznie czytamy wiadomości z całego świata, utrzymujemy komunikację na żywo, uczestniczymy w wideokonferencjach itp. W takim krajobrazie można sobie wyobrazić, że potrzebujemy prywatności, prawda? Stąd powstał TOR. Niezaprzeczalna liczba osób wykorzystała TOR, aby stać się aktywistami i częścią sił anonimowej partii przeciwnej. Należy pamiętać, że w niektórych krajach nieprzestrzeganie niektórych przepisów dotyczących cenzury może oznaczać ściganie, a nawet karę więzienia. Dlatego używanie TOR stało się koniecznością dla tych, którzy nie chcą być uciskani. Ponadto TOR umożliwia prywatną komunikację przy prawie zerowych kosztach; wystarczy zainstalować oprogramowanie. Oczywiste jest, że wykorzystanie Deep Web do różnych celów będzie nadal rosło w dającej się przewidzieć przyszłości. Po wejściu do internetu wraca. To niekończące się źródło informacji, które - we właściwych rękach - może posłużyć do poszerzenia wiedzy. Chociaż istnieje duża liczba osób wykorzystujących TOR do nielegalnych działań, społeczność będzie stale się rozwijać. W zwykłym odpowiedniku Internetu ludzie dokonywali również oszukańczych zastosowań; nigdy nie był to powód do zakazania jego używania. Władze muszą ustanowić przepisy w celu egzekwowania odpowiedzialnego korzystania z tych usług ukrytych i całej sieci TOR. Przepisy muszą ewoluować, aby objąć możliwe nadużycia Deep Web. W większości krajów ledwo skupili się na tym problemie. Jednak internet porusza się w gorączkowym tempie; rządy muszą być na bieżąco w tej sprawie. Miejmy nadzieję, że za kilka lat władze będą bardziej zaniepokojone aktualizacjami do najnowszych przepisów dotyczących nowych technologii. Idealnie byłoby, gdyby za każdym razem, gdy nowy projekt został zatwierdzony do dystrybucji, prawo powinno być w stanie regulować każdy możliwy użytek, jaki ludzie mogą zrobić. Widzisz, dlaczego jest to ogromne wyzwanie. W końcu kto kilka lat temu mógł sobie wyobrazić obecne zastosowania Deep Web, prawda? Czasami nie ma innej alternatywy, jak dostosowywanie się w biegu do najnowszych innowacji.

Instalacja przeglądarki TOR w systemie Windows 10

1. Przejdź do witryny projektu TOR lub po prostu wyszukaj najnowszą wersję tej przeglądarki, obecnie wersja 6.5 dla Windows 10, 8, 7, Vista i XP. W oficjalnym projekcie TOR kliknij kartę Pobierz w prawym górnym rogu strony. W wynikach wyszukiwania kliknij link do oficjalnej strony; dotrzesz do strony pobierania.

2. Następnie wybierz swój system operacyjny. Jak możesz docenić, przeglądarka j TOR jest dostępna dla systemu Windows 10, Apple OS X, Linux, smartfonów oraz w kodzie źródłowym. Tak, dobrze przeczytałeś; możesz także skorzystać z tego niesamowitego narzędzia anonimowego na swoim ulubionym urządzeniu.

3. Następnie wybierz język, aby pobrać właściwą wersję instalatora. Na tej samej stronie możesz pobrać pakiet TOR, który jest najlepszym zestawem narzędzi zwiększających prywatność podczas przeglądania Internetu.

4. Teraz musisz wybrać ścieżkę do zapisania instalatora na swoim komputerze. Należy pamiętać, że nie wpłynie to na kolejne kroki procesu.

5. Po zakończeniu pobierania pliku wykonywalnego kliknij go, aby uzyskać bezpośredni dostęp. W przeciwnym razie będziesz musiał uruchomić instalator ze ścieżki, którą wcześniej wybrałeś.

6. Wybierz język programu i kliknij OK.

7. Wybierz odpowiednią ścieżkę do zapisania plików programu; możesz także wybrać dodatkowy dysk twardy lub inną pamięć, np. kartę SD. Upewnij się, że jest wystarczająco dużo miejsca na instalację (plik wykonywalny pokazuje dostępną i potrzebną pamięć).

8. Zachowaj cierpliwość do zakończenia instalacji.

9. Tworzenie menu Start i skrótu na pulpicie jest powszechnym wyborem. Będziesz mógł uruchomić przeglądarkę natychmiast po zakończeniu instalacji.

Jak korzystać z TOR z serwerem proxy Firefox: prywatność BlackBelt

W tej sekcji wyjaśniono, jak wykorzystać aktualną instalację Firefoksa do nawigacji wewnątrz TOR za pomocą BlackBelt.

1. Przejdź do tej witryny, aby pobrać najnowszą wersję tego narzędzia programowego. To dość małe pobieranie, które zajmie najwyżej kilka minut.

2. Po otwarciu pliku wykonywalnego zostaniesz poproszony o wybranie rodzaju wykorzystania tej instalacji. Dostępne są następujące opcje:

1. Operator przekaźnika mostkowego. Aby używać TOR i pomóc ludziom zachować anonimowość podczas przekazywania do komputera.

2. Operator tylko klienta TOR. Chcesz po prostu skorzystać z TOR, nie stając się przekaźnikiem.

3. Użytkownik ocenzurowany. Jeśli w Twoim kraju internet podlega cenzurze, wybierz tę opcję.

3. Po wybraniu odpowiedniej opcji dla swojego profilu jako użytkownika TOR, Ty

wystarczy kontynuować instalację.

4. Po zakończeniu instalacji BlackBelt możesz przeglądać

Internet. Wszystko powinno być teraz gotowe, abyś mógł nawigować anonimowo.

Konfiguracja ręczna

W przypadku, gdy poprzednia konfiguracja nie działa poprawnie, możesz łatwo skonfigurować proxy TOR dla Mozilli w ciągu kilku minut. Oto kroki, które należy podjąć:

1. Przede wszystkim musisz mieć zainstalowaną przeglądarkę TOR na swoim komputerze. Jednak do nawigacji zamierzamy używać przeglądarki Firefox Mozilla. Powód takiego wyboru jest prosty: Mozilla to przeglądarka z wyższym współczynnikiem aktualizacji niż odpowiednik TOR. Programiści Mozilli są bardziej aktywni; w związku z tym częściej ustawiają aktualizacje. Poprawia to bezpieczeństwo tej przeglądarki.

2. Następnie otwierasz Mozilla Firefox; przejdź do ustawień, ustawień proxy.

3. W systemie Windows podążaj tą ścieżką: Menu> Opcje> Zaawansowane> Sieć

> Ustawienia.

4. Teraz wystarczy ręcznie skonfigurować serwery proxy:

*SOCKS Host: 127.0.0.1

*Port box: 9150

*Select SOCKs v5 if available

*Make sure you have “Remote DNS” check marked

*After No Proxy for introduce: 127.0.0.1

5. Sprawdź, czy TOR działa. Otrzymasz wiadomość z gratulacjami, informującą, że surfujesz anonimowo. W przeciwnym razie zostaniesz powiadomiony, że Twój adres IP jest widoczny. Jeśli serwer proxy nie działa, dezaktywuj go do czasu rozwiązania problemu.

Konfigurowanie usług ukrytych

Czy wiesz, co może być lepszego niż korzystanie z jakiejkolwiek usługi ukrytej w TOR? Konfiguruję Twoje! Stworzenie własnej usługi ukrytej jest możliwe i niezbyt trudne. Na przykład sprawdź tę witrynę internetową, aby zobaczyć, jak powstaje prawdziwa usługa ukryta. Oczywiście najpierw musisz mieć zainstalowaną przeglądarkę TOR. Konfigurowanie serwera lokalnego

1. TOR zaleca Savant (dla Windows) i „thttpd Web server” w Mac OS X, Linux i innych systemach operacyjnych Unix, jako serwer sieciowy do tworzenia usług ukrytych w sieci. Możesz użyć innego na własne ryzyko domniemanych luk w zabezpieczeniach.

2. Po otwarciu konfiguracji przejdź do HTTP, a następnie Server DNS, wpisz „localhost”. Wpisz „80” w polu „Port # To Serve From” poniżej.

3. Typowa ścieżka na stronie głównej Windows for Savant jest następująca:

Katalog C: \ Savant \ Root

Upewnij się, że dokument „index.html” zastępuje ten, którego Savant używał domyślnie w tym katalogu w ścieżce.

4. Aby sprawdzić, czy wszystko działa poprawnie, wystarczy wpisać localhost w pasku adresu przeglądarki. Jeśli chcesz użyć innego portu, innego niż # 80, wpisz localhost: [# portu], na przykład localhost: 100 dla portu # 100.

5. Jak dotąd lokalny serwer mamy online.

Konfigurowanie usługi ukrytej

Teraz wystarczy, że TOR dowie się o nowym skonfigurowanym serwerze WWW. Wykonaj następujące kroki, aby osiągnąć cel:

1. Zamknij przeglądarkę TOR, jeśli jest uruchomiona.

2. Musisz wyszukać plik „torrc”; możesz użyć narzędzia wyszukiwania na swoim komputerze. Możesz go również znaleźć na tej ścieżce:

Katalog Browser \ Data \ Tor

3. Po zlokalizowaniu tego pliku otwórz go w zwykłym edytorze tekstu, takim jak Notatnik lub podobny. Będziesz musiał dodać kilka wierszy do tego dokumentu, takich jak te:

Usługa ukryta

HiddenServiceDir C: \ Users \ Name \ tor_service

HiddenServicePort 80 127.0.0.1:80

4. Musisz zmienić ciąg C: \ Users \ Name \ tor_service, aby uzyskać rzeczywistą ścieżkę w komputerze. W takim przypadku nie wybieraj swojej witryny jako katalogu. Ostatnia liczba powyższego ciągu musi być numerem portu wybranego dla serwera WWW; w tym przypadku 80.

5. Utwórz folder tor_service na wypadek, gdyby jeszcze nie istniał. Zapisz i uruchom ponownie przeglądarkę TOR.

6. Zajrzyj do dziennika komunikatów, aby sprawdzić, czy w konfiguracji nie było błędów.

7. Wewnątrz tego folderu zobaczysz teraz 2 dokumenty: nazwę hosta i klucz_prywatny. Służą do zapewnienia prawidłowego funkcjonowania Twojej usługi;

chroń klucz bez względu na wszystko. Ktoś inny może usunąć twoją usługę ukrytą za pomocą tego klucza.

8. Wewnątrz nazwy hosta będziesz mieć adres cebulowy swojej usługi ukrytej. Otwórz ten dokument, aby przeczytać adres i udostępnić go innym osobom.

9. Teraz wystarczy, że umieścisz cokolwiek na tej nowej stronie TOR.

Nie zapominaj, że odwiedzający będą musieli użyć TOR, aby uzyskać do niego dostęp.

Jak widać, skonfigurowanie usług wewnątrz TOR nie jest takie trudne. Dzięki temu będziesz mógł publikować wiadomości, informacje i udostępniać je każdemu użytkownikowi w sieci. Rozpoczęcie pracy z witryną zarządzającą w tej sieci jest tak proste. Oczywiście, aby tworzyć eleganckie projekty, możesz potrzebować opanowania podstaw HTML i CSS. Na szczęście istnieje mnóstwo samouczków na temat tworzenia witryn internetowych. Ponadto w całym Internecie są dostępne próbki. Możesz zacząć od prostego szablonu, który możesz dowolnie dostosowywać.