Chcesz tego, czego chcesz.

Niewidzialność. Anonimowość. Protokół ducha.

Wziąłeś czerwoną pigułkę i zobaczyłeś prawdę i nie podoba ci się to. Nie winię cię. Ja też tego nie lubiłem. Ale to, co wydawało mi się, że wiem o Torze i innych narzędziach incognito, to tylko kropla w morzu potrzeb, obok tego, co naprawdę tam jest. Rzeczy, których nie znajdziesz na wielu forach technicznych. Oczywiście są szeptane na osobności, ale to wszystko jest dla ciebie niewidoczne. Do teraz. To prowadzi nas do Ciebie i do mnie, a raczej do tego, co mogę dla Ciebie zrobić. To niesamowite, czego facet może się nauczyć za dekadę, kiedy zakasuje rękawy i brudzi sobie ręce. Prywatne fora hakerów. Usenet. Freenet. Przeszukiwałem je wszystkie przez lata i tego, czego się nauczyłem, nie ma nigdzie indziej na Amazon. Równie niesamowite jest to, czego można się nauczyć za kilka dolarów w weekend, który warto przeczytać. To ja i wkrótce będę tobą. Tam, gdzie będziesz do poniedziałku, jestem teraz, tylko bez lat błędów. Błędy, które popełniłem używając Freenet, Tails, PGP. Wymień to, ja to zrobiłem. I chłopcze, zrobiłem DUŻO błędów, których unikniesz, ponieważ po przeczytaniu tego przewodnika poznasz ponad 85% użytkowników Tora i dowiesz się więcej o anonimowości niż większość agentów federalnych. Tak, nawet tak zwani superhakerzy z NSA. Ponieważ po zażyciu czerwonej pigułki nie ma już odwrotu. Nie możesz oduczyć się tego, czego się nauczyłeś, nie zobaczyć tego, co widziałeś, a będziesz chciał więcej. O wiele wiele więcej. Po pierwsze, nie trzymamy się tutaj podstaw. Jeśli wszystko, czego chcesz, to Tor dla Początkujących, poszukaj gdzie indziej. Tam, gdzie jedziemy, jest niebezpieczne terytorium. To terytorium rekina, kiedy już do niego dojdziesz. Ale nie martw się. Mamy środek odstraszający rekiny i wszystko, czego potrzebujesz, aby bezpiecznie surfować. Będziesz czerpać korzyści, o których tylko marzyłeś, a zanim skończymy, zdobędziesz umiejętności anonimowości na poziomie NSA z nastawieniem przeciw inwigilacji, które rywalizuje ze wszystkim, z czym Anonimowi lub ci zbiry z NSA mogą się przeciwstawić. A skoro o tym mowa, nie będą mieli pojęcia, jak cię znaleźć. Po drugie, za kilka dolarów poznasz każdy exploit, jaki ci superhakerzy lubią wykorzystywać przeciwko użytkownikom Tora i nie tylko: jak uniknąć śledzenia przez NSA. Anonimowość Bitcoin (prawdziwa anonimowość), porady Opsec, rynki Darknet i Darkcoins i, szczerze mówiąc, jest to długa lista, ale zanim skończysz, będziesz artystą Darknet, jeśli chodzi o rynki i kupowanie rzeczy incognito. Po trzecie, omówimy wiele technik wykorzystywanych przez CIA i FBI do usidlania użytkowników. Fałszywe wyznania. Clickbait. Honeypoty Tor. To wszystko jest takie samo. Dowiesz się tych samych technik, których używa się do łapania terrorystów, hakerów i grupy Anonymous oraz kurierów Reloaded. Przynęty i przynęty i jak rozpoznać agenta LEA z odległości kilometra. Rozbijam to wszystko na proste kroki, które możesz zrozumieć. Kilka dolarów za te informacje pozwoli Ci zaoszczędzić całe życie w żalu. Nie, nie znajdziesz ich na Reddit, Ars Technica ani Wired. Jeśli się nad tym zastanawiasz, nie rób tego. Potrzebujesz tego teraz, a nie wtedy, gdy jesteś wrobiony w coś, czego nie zrobiłeś. Po czwarte ... przeczytanie niebezpiecznych materiałów zawartych w niniejszym dokumencie wymaga podjęcia DZIAŁAŃ. Federalni podejmują działania. Złodzieje tożsamości podejmują działania. Hakerzy podejmują działania. Podejmiesz? Nie popełnij błędu - to nie jest zwykły przewodnik. To jest sposób myślenia. To profesjonalne rozwiązania, które mają zapewnić Tobie i Twojej rodzinie bezpieczeństwo przez dekadę, wykraczając daleko poza aplikacje i serwery proxy. I wszystko jest twoje, jeśli zrobisz dwie proste rzeczy: czytasz, a potem działasz. Prosty. Ponieważ wiesz, co mówią: wiedza to potęga. Nie, wieerz w to. Wiedza to potencjalna moc. Twoja moc. Ale tylko jeśli działasz. Wszyscy wiemy, że Truecrypt nie jest już bezpieczny, ale to dopiero początek. Poza tym wolność nie jest darmowa. Wreszcie ...

Czy Tor jest bezpieczny?

To wydaje się być pytanie w porządku. A jeśli chodzi o to, to naprawdę zależy od tego, kogo zapytasz, ponieważ zawsze są wilki w owczej skórze, które mogą zyskać na twojej ignorancji. Wielu mówi nie.

Kilku mówi tak. Media, mimo całej ich wiedzy w sprawach politycznych i społecznych, okazują się żałośnie niewystarczające, gdy dyskutuje się o czymś tak złożonym jak Tor.

Przykład: Gizmodo poinformował, że w grudniu 2014 roku grupie hakerów udało się złamać dostęp do wystarczającej liczby przekaźników Tora, aby zdemaskować użytkowników Tora. Jeśli słyszysz to po raz pierwszy, częścią tego, co sprawia, że Tor jest anonimowy, jest to, że przekazuje Twoje dane z jednego węzła do drugiego. Uważano, że jeśli złamią ich wystarczająco dużo, będą mogli śledzić poszczególnych użytkowników w sieci Tor i ujawniać ich rzeczywistą tożsamość. Trochę tak, jak agenci w Matrixie znajdują tych, którzy mieli ają zbyt dużo czasu, po prostu chcieli zhakować nowy cel. Kto wie dlaczego. Możliwe, że wystarczająco długo bawili się z Playstation Network i Xbox, i po prostu chcieli tu i tam ciekawego szczytu. Nie byli to też członkowie NSA na poziomie superhakera. Ale jak to zwykle bywa w przypadku mediów, ten atak przyciągnął uwagę kilku blogerów i dziennikarzy technicznych, którzy nie byli przychylni Torowi i, szczerze mówiąc, nie znali tego, co tak naprawdę stanowi zagrożenie. Twórcy Tora też to skomentowali:

„Wygląda to na zwykłą próbę ataku Sybil: napastnicy zarejestrowali wiele nowych przekaźników w nadziei, że staną się dużą częścią sieci. Ale mimo że obsługują tysiące nowych przekaźników, ich przekaźniki stanowią obecnie mniej niż 1 % sieci Tor według pojemności. Pracujemy teraz nad usunięciem tych przekaźników z sieci, zanim staną się zagrożeniem i nie spodziewamy się żadnych efektów anonimowości ani wydajności w oparciu o to, co widzieliśmy do tej pory. "

Tym blogerom spiskowym nie udało się zgłosić, że każda zdecentralizowana sieć, taka jak Tor, jest głównym celem ataków takich jak powyższe. Ale aby naprawdę mieć szansę na przebicie się przez tę macierz, hakerzy potrzebowaliby Tora, aby bezwarunkowo ufać każdemu nowemu węzłowi, który pojawi się online. To się nie zdarza. Zbieranie ruchu przez nowe przekaźniki wymaga również czasu - niektóre mogą mieć nawet sześćdziesiąt dni lub więcej, a prawdopodobieństwo zgłoszenia jest dość wysokie, ponieważ adresy IP są jawne - co tylko przyspiesza złośliwe raportowanie. Prawdziwym niebezpieczeństwem, które istnieje od samego początku, jest przerażenie użytkowników Tora przed mniej bezpiecznymi metodami komunikacji. Tego właśnie chce NSA. CIA już to robi w innych krajach. Teraz NSA idzie w ich ślady.

PRAWDZIWE ryzyko używania Tora

Wymieniam je tutaj, zanim zanurzymy się w głąb terytorium wroga, abyście wiedzieli, czego unikać przed instalacją, i być może usłyszysz „a-ha!" w kolejnych częściach. Czytając, pamiętaj, że posiadanie włączonego Javascript to tak naprawdę tylko kropla w oceanie obok tego, jak wróg może zabić twoją anonimowość.

<u>Javascript</u>

Powszechnie wiadomo, że pozostawienie włączonego Javascript jest szkodliwe dla użytkownika Tora. Dziewięćdziesiąt pięć procent z nas o tym wie, ale błędy 5% są nieproporcjonalne i rzucane w twarz reszcie z nas. Co gorsza, wiele stron internetowych uruchamia teraz tak wiele skryptów, że wydaje się, że nienawidzą użytkowników Tora. Jedna strona wymagała kilkunastu. Bez tego strona była / jest / będzie w dużym stopniu wzbogacona. Czasami nawet nieczytelna. Możesz sobie wyobrazić, co by się stało, gdybyś używał Tora i zdecydował się odwiedzić tę stronę, jeśli została skonfigurowana tak, aby zwabić użytkowników do pułapki. Pamiętam, jak jeden badacz stwierdził, że „81% użytkowników Tora można zdeanonimizować". Ten wynik 81% powstał, ponieważ docelowi użytkownicy niewiele wiedzieli o dodatku NoScript do przeglądarki i prawdopodobnie mieszali użycie Tora z ich codziennym korzystaniem z otwartej sieci, dostarczając wystarczających danych do ataku korelacyjnego. Ale to była tylko wisienka na torcie. Zostawili dane osobowe *wszędzie* - używając tych samych nazw

użytkowników i haseł, których używali gdzie indziej w otwartej sieci. Chwalenie się ulubionymi filmami Netflix. Mówienieo lokalnych wydarzeniach. Pogoda (huragan w dzielnicy francuskiej!).

Wolontariat jako węzeł wyjściowy

Kolejne zła rzecz, choć nie do końca dziadek wszystkich zagrożeń, ale nadal ryzykowna. Z drugiej strony, jako odważnie wierzący w anonimowość, łaskawie zapewniasz przepustowość i „wyjście" pozostałym użytkownikom Tora (miejmy nadzieję, że żadnego z nich nie znasz), aby mogli przepuszczać zaszyfrowany ruch przez twój węzeł. Hojny? Na pewno. Mądry? Jeśli mieszkasz w Stanach ... to nie.

Nie jest tak, że jest to nielegalne per se. Wręcz przeciwnie, ale to, co przechodzi przez twój węzeł, może wylądować na podsłuchu . Cały ruch wychodzący z twojego węzła (tj. ruch innych osób) jest powiązany z twoim adresem IP i jak odkryli inni, narażasz się na ryzyko przez to, co inni na drugim końcu planety robią z twoim węzłem. Wielu nowych użytkowników Tora uruchamia BitTorrent skonfigurowany dla Tora i zużywa całą przepustowość. Powoduje to bardzo nieszczęśliwe wrażenia korzystania z Tora dla innych użytkowników. Możesz otrzymać zawiadomienie o naruszeniu praw autorskich (lub zostać pozwany) lub być może zostać aresztowany, jeśli pornografia dziecięca wypłynie z twojego węzła. Zastanów się dokładnie i przeprowadź swoje badania, zanim podejmiesz tak ryzykowne obciążenie, aby nie przejąć komputera i nie zrujnować reputacji.

Uruchamianie przekaźnika wyjściowego z domu

Uruchomienie go z domu jest jeszcze gorsze niż korzystanie z pamięci w chmurze i jest nieskończenie niebezpieczne w USA i Wielkiej Brytanii. Jeśli prawo z jakiegokolwiek powodu interesuje się ruchem sieci Tor, Twój komputer może zostać zajęty, tak, ale to dopiero początek. Zatwardziały stary sędzia może dać ci dwa lata za to, że nie rozwidliłeś kluczy szyfrujących (które gdyby tak było, nie zawracaliby sobie głowy najazdem o 6 rano).

Zamiast tego użyj hosta obsługującego Tor. Na przykład Sealandhosting.org. Akceptują Bitcoiny i nie wymagają żadnych danych osobowych, a jedynie e-mail. Oferują gniazda, serwery dedykowane, hosting Tor i VPS, a także domeny.

Później przejdziemy do szczegółów, ale są to Zasady, które wyznaczyłem sobie:

- Powstrzymaj się od kierowania przez nią normalnego ruchu

- Nigdy nie rób niczego nielegalnego (więcej później, ponieważ jest to szara strefa)

- Nigdy nie umieszczaj na nim poufnych plików (informacje finansowe, listy miłosne, dokumenty sądowe)

- Bądź tak przejrzysty, jak to tylko możliwe, jako że prowadzę wyjście

- Jeśli otrzymam skargi od The Olde ISP (lub uniwersytetu), używam tego szablonu [https://2019.www.torproject.org/eff/tor-dmca-response.html.en]

Agencje wywiadowcze

Bez wątpienia wypowiedzieli wojnę Torowi i jego możliwościom ukrywania się. I chociaż będą walczyć zębami i pazurami, aby przekonać cię, że to dla twojego własnego dobra, tak naprawdę to wszystko sprowadza się nie tyle do bezpieczeństwa narodowego, ile do kontroli narodowej: kontrola nad tobą przez to, że nie wiedzą, kim jesteś, co robisz na Tor, ani dlaczego.

Oni tego nie lubią.

To dość galaktycznie pompatyczne z ich strony, że wydają tyle pieniędzy i marnują tyle czasu na gonienie za tobą, tylko dlatego, że cię nie lubią lub twoje działania nie są łatwe do zidentyfikowania. Jak zapewne wiesz, bardziej kosztowne jest dążenie do celu o dużej wartości. Ale nie wiedzą, czy jesteś wartościowym celem, czy tylko nisko wiszącym owocem. Jak widzieliśmy w przypadku znudzonych studentów Harvardu, każdy może wpaść w poważne kłopoty, jeśli wejdzie do Tora jako nietoperz. Nawet Eric Holder publicznie wskazał, że użytkownicy Tora są oznaczani jako „osoby spoza USA", dopóki nie zostaną zidentyfikowani jako obywatele. To więcej niż pompatyczne. To przestępstwo i niezgodność z konstytucją. Wygląda na to, że postrzegają WSZYSTKICH użytkowników Tora jako wartościowe cele. A do czasu, gdy zostaniesz zidentyfikowany jako tacy, uzyskali wystarczającą moc, aby odebrać tobie i milionom innych obywateli ich prawa do prywatności i ochrony na mocy czwartej poprawki do konstytucji. Robią to na dwa sposoby:

https://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity

System Quantum i FoxAcid

Więcej o tym, jak to pokonać później, ale oto istota tego:

- Oba systemy zależą od tajnych ustaleń dokonanych z firmami telekomunikacyjnymi

- Oba polegają na uśpieniu użytkownika w fałszywym poczuciu bezpieczeństwa

- Żaden system nie może wprowadzać zmian na LiveCD (Tails)

- Oba można pokonać, stosując spójne nawyki dotyczące bezpieczeństwa.

Pokonanie tego wymaga staranności. NIE zwlekaj.

Zdecyduj z wyprzedzeniem, aby uniknąć ryzykownych zachowań. Dotrzemy do nich wszystkich. Rozwój dobrego, bezpiecznego sposobu myślenia wymaga czasu, wysiłku i zaangażowania, ale należy go pielęgnować od samego początku, dlatego RYZYKA są umieszczane na samym początku, nawet przed rozdziałem dotyczącym instalacji. Rzeczy ciągną się w środku i często o nich się zapomina. Mówiąc o ryzyku ... jeśli zastanawiasz się, co tak naprawdę nie pozwala mi zasnąć w nocy, to jest to: Co inne narody mówią dyrektorom wysokiego szczebla i agencjom wywiadowczym (na przykład Hongkong)? Jeśli jedyną rzeczą, której mogę zaufać, jest mój zakurzony stary 486 na moim strychu z Ultima 7 nadal zainstalowaną na moim modemie telefonicznym 28,8k, to można bezpiecznie założyć, że każdy podmiot komercyjny jest zagrożony przez NSA. A jeśli to prawda, jeśli NSA musi przeskoczyć przez przeszkody, aby nas szpiegować, jak łatwo jest zinfiltrować systemy za granicą z naszymi danymi w tych systemach? Do tego, jeśli żadna korporacja nie może zachować swoich prywatnych informacji w tajemnicy, to ostatecznie gra końcowa może przekształcić się w siatkę Skynet podobną do bloku Sovietera Wschód / Zachód, w którym dyrektorzy generalni muszą wybrać wschód lub zachód. Ale to tak, jakby próbować zdecydować, czy chcesz zostać zjedzony przez niedźwiedzia grizzly, czy przez lwa. Więc teraz znasz prawdziwe ryzyko. W każdym razie te główne. Każde z tych zagrożeń można zminimalizować lub wręcz pokonać, korzystając z wiedzy zawartej w tych artykułach. Smutne jest to, że większość czytelników zapomina mniej więcej 80% tego, co czytają. Ci, którzy podejmą działania, zachowają te 80%, ponieważ urzeczywistniają to, co przeczytali: robią genialne kontrataki przypominające szachy, gdy NSA grozi twojej królowej. Jeśli nie podejmiesz żadnych działań, a po prostu usiądziesz jak żaba w wolno gotującej się wodzie, nie tylko zginiesz, ale także zginiesz na własne życzenie. W porządku. Dość ryzyka. Weźmy się za to.

Przewodnik krok po kroku Tor

Teraz odpowiedzmy, czym jest Tor, co robi, a czego nie może.

Bez wątpienia słyszałeś, że to jakieś narzędzie hakera i miałbyś rację, ale tylko z punktu widzenia, że potężne narzędzie, takie jak Tor, może być używane do prawie wszystkiego. W rzeczywistości wszystko (może z wyjątkiem zmysłowych blondynek w czerwonych sukienkach) można kupić anonimowo ... pod warunkiem, że jesteś ostrożny. Zanim zapukasz do Tora, pamiętaj, że nie chodzi o kupowanie narkotyków, porno czy egzotycznych białych tygrysów. Chodzi o anonimową komunikację i prywatność - z główną funkcją jest zapewnienie anonimowości poprzez przekierowanie sesji przeglądania z jednego przekaźnika Tora do drugiego - maskowanie adresu IP w taki sposób, że strony internetowe nie mogą znać Twojej prawdziwej lokalizacji. Dzięki temu możesz mieć :

- Dostęp do zablokowanych stron internetowych (Facebook, jeśli jesteś w Chinach)

- Dostęp do witryn .onion, które są nieosiągalne przez otwarty internet

- Zagrozić prezydentowi rzuceniem ciastem w twarz ... i to bez odwiedzin Tajnych Służb!

Robszi to wszystko w procesie zwanym routingiem cebulowym.

Co to jest routing cebulowy?

Potraktujcie to jako macierz proxy z wieloma punktami do punktu. W przeciwieństwie do aplikacji peer-to-peer, takich jak BitTorrent czy eMule, które ujawniają Twój adres IP każdemu, Tor używa szeregu węzłów pośredniczących (a tym samym adresów IP), które szyfrują Twoje dane w całym łańcuchu sieci. W punkcie końcowym dane są odszyfrowywane przez węzeł wyjściowy, aby nikt nie mógł wskazać Twojej lokalizacji ani powiedzieć, który plik pochodzi z którego komputera. Dzięki temu procesowi anonimizacji jesteś anonimowy ze względu na spakowane „warstwy cebuli", które ukrywają Twój prawdziwy adres IP. Możliwe jest nawet zbudowanie witryny, do której dostęp mają tylko użytkownicy Tora. Nazywane również „witrynami cebulowymi", choć technicznie trudne, nie potrzebujesz doktoratu z informatyki, aby je stworzyć. Albo nawet licencjatu. Te strony Onion są niedostępne dla nikogo, kto używa zwykłej sieci i zwykłego, innego niż Tor Firefox. Zagłębimy się w to później, a także zbudujemy fortecę zagłady, której nic nie może przeniknąć.

Instalacja

Instalowanie Tora jest proste. Możesz go pobrać : https://www.torproject.org/download/

Jeśli twój dostawca usług internetowych blokuje ci dostęp do strony Tor, zrób to:

- Wyślij e-maila do Tora. Opowiedz im o sytuacji. Możesz otrzymać automatyczną wiadomość odesłaną do Ciebie wraz z pakietem instalacyjnym Tora.

- Przejdź do Google. Wyszukaj dowolne strony internetowe w pamięci podręcznej, w tym Tor, które mogą mieć pakiet instalacyjny do pobrania. Wiele witryn technologicznych może go mieć po prostu na wypadek totalnej wojny nuklearnej.

- Odwiedź stronę rt.torproject.org i poproś o jej kopię lustrzaną.

- Poproś znajomego, aby wysłał Ci wiadomość e-mail z instalacją Tora. Zapytaj też o Tailsa.

- ZWERYFIKUJ podpis, jeśli otrzymałeś go gdzie indziej niż z głównej strony Tora, ale z miłości do wszystkiego, co święte i święte, Threepwood, sprawdź to, nawet jeśli twój przyjaciel dostarczy to ręcznie. W przeszłości dostawałem wirusy od znajomych udostępniających aplikacje, które uważali za „czyste".

Teraz więc. Wybierz wersję dla systemu Windows, Linux lub Mac i wiedz, że domyślna instalacja Firefoksa nie zostanie nadpisana, chyba że chcesz. Oba używają Firefoksa, ale Tor to zupełnie osobna

umowa. Zauważysz, że ma te same funkcje, co Firefox: Tabs. Zakładki. Pole wyszukiwania. Menu. Wszystko jest tutaj ... oprócz twoich ulubionych dodatków.

W tym momencie możesz ulec pokusie zainstalowania ulubionych. Nie ulegaj tej pokusie. Wiele dodatków, które nie robią nic dla Twojej anonimowości, może pomóc komuś w zlokalizowaniu Cię przez Tora za pomocą tak zwanego „pobierania odcisków palców przeglądarki".

Po instalacji powinieneś zobaczyć zielony ekran powitalny poniżej:

Teraz masz kilka możliwości. Jednym z nich jest dobrowolne zgłoszenie swojej przepustowości, co ułatwia innym użytkownikom Tora, ale wiąże się z ryzykiem. Zostało to szczegółowo wyjaśnione przez programistów Tora tutaj : https://2019.www.torproject.org/getinvolved/relays.html.en

Zalecam przeczytanie go, jeśli nie masz doświadczenia z narzędziami anonimowości. Po zainstalowaniu Tora każda strona, którą odwiedzasz w przeglądarce Tor, będzie anonimowo kierowana przez sieć Tor. Jest jednak ważny szczegół, który musisz wiedzieć o bezpieczeństwie, a mianowicie, że twoje ustawienia Tora są jedynie rozsądnymi punktami startowymi. Nie są optymalne. Wciąż jesteśmy na etapie początkowym i szczerze mówiąc, optymalny, ponieważ Tor wie, że optymalny jest w dużej mierze zależny od sprzętu (sieci, procesora, pamięci RAM, maszyny wirtualnej, VPN), więc konfiguracja każdej osoby będzie inna.

Czego Tor nie może zrobić

Teraz, czego Tor nie może zrobić, a przynajmniej nie może zrobić bardzo dobrze. W przyszłości może się to zmienić, więc jeszcze nie rzucaj się na swój miecz.

1.) Tor nie może cię chronić przed załącznikami.

Nie ogranicza się to do plików wykonywalnych, ale do wszystkiego, co można uruchomić za pomocą kodu. Oznacza to filmy Flash, a także RealPlayer i Quicktime. Te dzieci można skonfigurować tak, aby wysyłały Twój prawdziwy adres IP do przeciwnika. Niedobrze. Dlatego nigdy nie uruchamiaj żadnego

pliku wykonywalnego ani aplikacji, chyba że ufasz źródłu. Jeśli to możliwe, przejdź do open source. Dotyczy to również każdego schematu szyfrowania, którego MUSISZ użyć, jeśli zamierzasz używać Tora. To NIE jest opcja. Niektórzy mówią, że tak, ale to tak, jakby powiedzieć, że nauka tajskiego jest opcjonalna, jeśli zamierzasz mieszkać w Bangkoku. W ten sposób daleko nie zajdziesz.

2.) Tor nie może dobrze obsługiwać torrentów.

Stare wiadomości, prawda? Tysiące nadal to robi. Lepiej bezpiecznie niż żałować, twierdzą Jedyny problem w tym, że ... są bezpieczni i wszystkim innym jest przykro. Tor nie może tworzyć aplikacji P2P, takich jak Emule i Limewire, bez utrudniania wszystkim innym korzystania z Tora. Po prostu wysysa zbyt dużą przepustowość. Oprócz tego, że niektóre węzły wyjściowe domyślnie blokują taki ruch, udowodniono, że adres IP można znaleźć za pomocą torrentów w sieci Tor. eMule też używa UDP, a ponieważ Tor obsługuje protokół TCP, możesz wyciągnąć własne wnioski na temat tego, co wpływa to na twoją anonimowość. To prawda, możesz oszczędzić pozwu o prawa autorskie, ponieważ RIAA prawdopodobnie nie będzie miał kłopotów, próbując zdobyć Twój adres IP, ale proszę, oszczędzaj innym użytkownikom Tora szaleństwa prędkości modemu z 1998 roku. VPN to znacznie lepszy wybór. Jest kilka dobrych.

3.) Tor nie może ukryć twojej tożsamości, jeśli rzucasz prawdziwym e-mailem jak koralikami Mardi Gras. Jeśli podajesz swój prawdziwy adres e-mail na stronach internetowych podczas korzystania z Tora, uważaj, że Twoja anonimowość została naruszona. Twoja wirtualna tożsamość nigdy nie może pasować do Twojej prawdziwej tożsamości. Zawsze. Ci, którzy ignorują tę zasadę, zostają zhackowani, okradzeni, aresztowani lub okaleczeni przez zakapturzone gremliny.

Aplikacje Tor i narzędzia chroniące przed odciskami palców

Kilka aplikacji sprawia, że Tor mniej przyprawia o ból głowy, ale nie są one szczególnie odpowiednie dla użytkowników komputerów stacjonarnych, chyba że wykonujesz jakąś emulację. Ale w dzisiejszych czasach wszyscy używają telefonów komórkowych, niektóre z nich przyniosły mi korzyści w sposób, o którym nigdy nie myślałem, że to możliwe. Pamiętaj i przeczytaj komentarze w Sklepie Play, ponieważ aktualizacje zwykle psują.

Orbot: Proxy z Tor

Tor na Androida, sprawdź to : https://play.google.com/store/apps/details?id=org.torproject.android

Jest to aplikacja proxy, która działa podobnie do aplikacji komputerowej i szyfruje ruch sieciowy oraz chroni przed inwigilacją i zabezpiecza przed analizą ruchu. Możesz używać Orbota z Twitterem, DuckDuckGo lub dowolną aplikacją z funkcją proxy. Używam tego już od dłuższego czasu i przyzwyczaiłem się do tego. Być może czas spróbować czegoś innego.

Invisibox - prosta prywatność

Wystarczy podłączyć InvizBox do istniejącego routera / modemu. Zostanie wyświetlony nowy hotspot Wi-Fi „InvizBox". Połącz się z nowym hotspotem i postępuj zgodnie z jednorazową konfiguracją i gotowe. Wszystkie urządzenia podłączone do InvizBox wifi będą kierować swój ruch przez sieć Tor.

Text Secure

Ta aplikacja szyfruje każdą wiadomość w telefonie komórkowym i jest łatwa do nauczenia. Co więcej, jeśli zostawisz telefon w Marble Slab (Marble Flab to the Mrs.), możesz mieć pewność, że Twoja prywatność jest bezpieczna dzięki szyfrowaniu. Jest również open-source. Zbyt wiele aplikacji nie jest,

więc nikt nie może ich recenzować, w przeciwieństwie do niektórych zastrzeżonych aplikacji, takich jak te oferowane przez SecurStar (tj.Drivecrypt, Phonecrypt).

Red Phone

Ta aplikacja zabezpiecza każde połączenie za pomocą pełnego szyfrowania, zapewniając prywatność i spokój ducha. Korzysta z WiFi i oferuje zgrabne aktualizacje, jeśli obaj rozmówcy mają zainstalowany RedPhone. To nie jest dla każdego. Chociaż nie jest to tak drogie, jak powiedzmy, TrustCall, istnieją problemy z wygodą, takie jak długie czasy połączeń i zerwane połączenia (kiedykolwiek Skype ktoś z Manili?), Więc nie będzie tak szybki i brudny, jak robi to Jason Bourne. Ale plusy przeważają nad minusami. Szczególnie podoba mi się hasło składające się z dwóch słów jako funkcja bezpieczeństwa: jeśli obawiasz się, że agent Boris nie żyje i został zabity przez agentkę Doris (która ma teraz swój telefon), możesz poprosić, aby wypowiedziała drugie hasło. Proste, ale skuteczne.

Google i Tor

Co Google myśli o Tor? Całkiem szczerze podejrzewam, że starają się tego nie robić. Prawdopodobnie nie nienawidzą tego tak jak NSA, ale wiedzą, że gdyby każdy użytkownik Google korzystał z Tora na co dzień, większość ich systemu kierowania reklam zacząłby, powiedzmy, świecić pustkami. Wyobraź sobie, że trzynastoletni chłopiec otrzymał reklamy Cialis, albo osiemdziesięcioletnia kobieta o imieniu Bertha zaczęła widzieć reklamy kuponów trojańskich, albo ... cóż, masz pomysł. Nie mają nic przeciwko przekazywaniu funduszy, ponieważ pozwala to na przyszłe udziały w technologii (w pewnym sensie). W tym celu przekazali darowizny nie tylko Torowi, ale także Freenetowi, a nawet technologii łazików marsjańskich. Wszelkiego rodzaju szalone rzeczy. Nigdy nie wiedzą, która technologia wyskoczy na orbitę za tydzień lub rok od teraz, więc rzucają pieniądze jak Scrooge w świąteczny poranek.

Captchas

Czasami będziesz używać Tora i odkryjesz, że Google wypluwa to wymaganie, aby udowodnić, że jesteś człowiekiem. To, ze względu na ich masowe analizy zapytań wyszukiwania, jest tym, co sprawia, że niektórzy użytkownicy Tora myślą, że Google ma to dla nich. Jednak Google musi znosić wielu spamerów i ogólne kradzieże; boty wbijające serwery tonami zapytań w krótkim czasie, które nadmiernie obciążają serwery, mogą być jedną rzeczą, ale może się również zdarzyć, jeśli Twój pracodawca używa serwerów proxy - wielu pracowników pracujących dla tej samej firmy, która używa jednego z nich, może ustawić z czerwonej flagi. Kiedy twój obwód Tora przełącza się na nowy, zwykle rozwiązuje się sam. Istnieją jednak inne wyszukiwarki, takie jak DuckDuckGo, z których możesz skorzystać. Może się okazać, że strony internetowe robią to samo. Ponownie, dzieje się tak z powodu tak wielu węzłów wyjściowych (z których wszystkie są publicznie widoczne dla każdego administratora witryny), które powodują zatrzaskiwanie witryny ruchem w taki sposób, że zachowanie młotków przypomina bota, takie, jakich lubią używać rosyjskie i chińskie stroje. Twórcy Tora również mają kilka interesujących rzeczy na ten temat :

https://2019.www.torproject.org/docs/faq.html#GoogleCAPTCHA

SpiderOak

Zwykle ostrzegam przed korzystaniem z Cloud Service do wszystkiego, co chcesz mieć prywatne. SpiderOak jest jednym wyjątkiem, z pewnymi zastrzeżeniami. Jest to wystarczająco przyzwoita alternatywa dla DropBox, ponieważ jest zakodowana za pomocą „Zero Knowledge" (tak powiedziałby programista), a po zainstalowaniu zestaw kluczy szyfrujących jest tworzony po stronie klienta. Kiedy przesyłasz dane na serwery SpiderOak, są one szyfrowane na Twoim komputerze, a następnie przesyłane. Znowu, według twórców. Twierdzą, że nawet jeśli wezwanie sądowe wymaga danych

subskrybenta, nie mogą go dostarczyć, ponieważ tylko Ty masz klucze. Nieźle, ale nadal nie przesłałbym niczego niezaszyfrowanego. Na przykład plik kontenera. Inną wadą jest to, że jest scentralizowany. Centralizacja oznacza pojedynczy punkt awarii. Twoje dane mogą zostać przez nich usunięte w dowolnym momencie (tak naprawdę w przypadku każdej usługi online). Pamiętaj, że między tobą a sędzią zawsze będą po stronie sędziego.

Tails

Słyszałeś kiedyś o „systemie na żywo"? Ani ja, dopóki Tails nie pojawił się na scenie. Tails pozwala ci używać Tora i unikać śledzenia i cenzury oraz w praktycznie dowolnym miejscu. Posiada własny system operacyjny i jest przeznaczony dla osób w ruchu. Możesz go uruchomić za pomocą pamięci USB, SD lub nawet DVD. Całkiem przydatne, ponieważ dzięki temu jest odporny na wirusy. Jest to również korzystne, jeśli nie chcesz, aby Twój dysk twardy zostawiał resztki sesji przeglądania. Najlepsze jest to, że jest darmowy i oparty na Linuksie. Annnd zawiera klienta czatu, pocztę e-mail, biuro i przeglądarkę. Wadą używania DVD jest to, że musisz nagrywać go ponownie za każdym razem, gdy aktualizujesz Tails. Niezbyt wygodne. Więc zamiast tego zainstalujmy go na pendrive.

1.) Pobierz instalator tails : https://tails.boum.org/install/ . Najpierw musisz go gdzieś zainstalować, np. na płycie DVD, a NASTĘPNIE sklonować pamięć USB lub kartę SD.

2.) Kliknij Applications -> Tails -> Tails install, aby rozpocząć instalację.

3.) Wybierz Clone & Install, aby zainstalować na karcie SD lub pamięci USB

4.) Podłącz urządzenie, a następnie wyszukaj je w menu rozwijanym Target Device. Otrzymasz ostrzeżenie o tym, że nadpisuje wszystko na urządzeniu, bla-bla. Wybierz tak i potwierdź instalację.

Ograniczenia Tails

Ani Tails, ani Tor nie szyfrują automatycznie twoich dokumentów. W tym celu musisz użyć GnuPG lub LUKS (w zestawie), pamiętając, że niektóre dokumenty, takie jak Word lub Atlantis, mogą zawierać dane rejestracyjne w samym dokumencie (w 2013 r. Auto-wydawcy Amazon odkryli, że nazwy pióra mogą być czasami ujawnione, patrząc na kod powyższych aplikacji i ustalenie prawdziwej tożsamości autorów. Osobiście używam fałszywych informacji podczas „rejestracji" dowolnej aplikacji, której będę używać w połączeniu z Torem lub Tailsem.

Inne warte uwagi rzeczy:

- Metadane dokumentu nie są usuwane za pomocą Tails

- Tails nie ukrywa faktu, że używasz go przed swoim dostawcą Internetu (chyba że używasz mostków Tora). Nie mogą zobaczyć, co robisz w Torze, to prawda, ale wiedzą, że go używasz.

- Tails jest ślepy na błąd człowieka. Staraj się nie używać tej samej sesji Tails do rozpoczynania dwóch różnych projektów. Użyj oddzielnych sesji. Oddzielenie obu tożsamości w ten sposób przyczynia się do silnej anonimowości Twoich sesji.

Chrom

Firefox nie jest jedynym sposobem na zabicie smoka. Jest też Chrome. Tak, to Google i tak, Google odeszło daleko od swojego motta „Nie rób zła", ale jak wszystko inne w życiu, szczęście sprzyja przygotowaniom. Musisz tylko mieć odpowiedni miecz. Właściwa zbroja. Właściwe wytrychy. Preparaty (odczynniki) są następujące:

I. Zainstaluj rozszerzenie ScriptNo. Chromowanie jest tym, czym mysz na PC, przynajmniej jeśli chodzi o precyzyjne celowanie. Zapewnia również doskonałą kontrolę, umożliwiając nawet dostosowanie przeglądarki w sposób, którego NoScript dla Firefox nie może. Jeśli uznasz to za zbyt trudne, ScriptSafe to kolejna opcja. Skorzystałem z obu i wyszedłem bardzo zadowolony, chociaż jak wszystko inne w Internecie, YMMV.

II. FlashControl to fajna alternatywa dla Firefoksa. Jeśli nie widzisz go w sklepie Google Play, po prostu wyszukaj „Flash Block" i powinno się pojawić (Google ma zwyczaj usuwania aplikacji, które nie są aktualizowane w każdy czwartek podczas pełni księżyca).

III. Adblock. Ten jest po prostu niesamowicie dobry w odpieraniu wszelkiego rodzaju złośliwego oprogramowania.

IV. Przełącznik klienta użytkownika dla Chrome. Zainstaluj to. Nigdy nie wychodź z domu (0.0.0.0) bez niego. Fałszuje i naśladuje ciągi znaków agenta użytkownika. Możesz ustawić swój wygląd tak, aby wyglądał jak Internet Explorer. Spowoduje to, że wiele ładunków złośliwego oprogramowania zacznie myśleć, że naprawdę przeglądasz Internet za pomocą IE, a nie Firefoksa lub Chrome, a tym samym strzelasz do ciebie pustkami. To mogło uratować Blake'a Benthalla, 26-letniego operatora Silk Road 2.0, przed nalotem ze strony FBI (wśród tuzina innych firm narkotykowych). Dokonano tego przez wiele miesięcy, ponieważ musieli przejąć kontrolę nad wieloma przekaźnikami, a jeśli masz kontrolę nad przekaźnikami, możesz użyć zaawansowanej analizy ruchu, aby zbadać wzorce w adresach IP i dopasować zachowanie i ustawienia przeglądarki do tych adresów. Przypomnijmy, że każdy prokurator zawsze będzie próbował powiązać adres IP z rzeczywistą osobą, której dotyczy przestępstwo. Powtórzę: adres IP jest uważany za tożsamość na potrzeby ścigania. Wszyscy jesteśmy dla nich liczbą, niezależnie od tego. Ci z Was, którzy mają pożyczki studenckie, wiedzą o tym prawdopodobnie lepiej niż ktokolwiek inny. To się zmieni jako że czas oczywiście płynie - w miarę jak konkurenci Tora, tacy jak Freenet i inne aplikacje, ewoluują, by oferować to, czego Tor nie może. Ivan Pustogarov omawia tutaj znacznie więcej szczegółów, ale wystarczy powiedzieć, że FBI odrobiło swoją pracę domową i kiedy wszystko zostało powiedziane i zrobione, będzie miało więcej zasobów na identyfikację leniwych użytkowników niż typowa sieć VPN. /etap końcowy.

V. CanvasBlocker - Annnnd kolejna świetna wtyczka do przeglądarki Firefox. To dziecko zapobiega używaniu przez strony API JavaScript <canvas> do użytkowników odcisków palców. Możesz zablokować to w każdej witrynie lub być dyskryminującym i zablokować tylko kilka witryn. Zależy od Ciebie. Dla mnie najważniejsze jest to, że nie psuje stron internetowych. Więcej informacji tutaj, ale na wypadek, gdyby Ci nie przeszkadzało, oto sedno:

Różne tryby blokowania to:

</canvas></canvas> </canvas>

- Block readout API: Wszystkie strony internetowe, które nie znajdują się na białej liście lub czarnej liście, mogą używać interfejsu API <canvas> do wyświetlania czegoś na stronie, ale interfejs API odczytu nie może zwracać wartości do witryny.

- fałszywy interfejs API odczytu: domyślne ustawienie Canvas Blocker i moje ulubione! Wszystkie strony internetowe, które nie znajdują się na białej liście lub czarnej liście, mogą używać interfejsu API <canvas> do wyświetlania czegoś na stronie, ale interfejs API odczytu jest zmuszony zwracać nową losową wartość przy każdym wywołaniu.

- poproś o pozwolenie na odczyt API: Wszystkie strony internetowe spoza białej lub czarnej listy mogą używać API <canvas> do wyświetlania czegoś na stronie, ale użytkownik zostanie zapytany, czy za każdym razem witryna powinna mieć możliwość korzystania z interfejsu API odczytu to się nazywa.

- blokuj wszystko: ignoruj wszystkie listy i blokuj API <canvas> na wszystkich stronach internetowych.

- zezwalaj tylko na białą listę: tylko strony internetowe z białej listy mogą korzystać z interfejsu API <canvas>.

- zapytaj o pozwolenie: Jeśli witryna nie jest wymieniona na białej lub czarnej liście, użytkownik zostanie zapytany, czy witryna powinna mieć możliwość korzystania z interfejsu API <canvas> przy każdym wywołaniu.

- blokuj tylko czarną listę: Blokuj API <canvas> tylko dla stron internetowych z czarnej listy.

- zezwalaj na wszystko: ignoruj wszystkie listy i zezwalaj na API <canvas> na wszystkich stronach internetowych.

Jak widać, to potężna rzecz.

Zabójcze opcje Firefoksa

Możesz ulec pokusie, aby włączyć opcję „Sprawdź fałszywe witryny internetowe" w przeglądarce Firefox. Nie rób tego, ponieważ przekaże witryny, które regularnie odwiedzasz, na serwery Google. „Predykcyjne wyszukiwanie tekstu" Google jest również złe, ponieważ przekazuje również naciśnięcia klawiszy do Google. Aby to zmienić, musisz to zrobić ręcznie, przechodząc do about: config w pasku adresu. To powiedziawszy, spójrzmy na inne ustawienia prywatności, o których możesz chcieć wiedzieć. Javascript - Unikaj jak zarazy. Możesz jednak zauważyć, że jest on domyślnie włączony na karcie opcji Firefoksa. Powód jest opisany tutaj przez zespół programistów Tor: Konfigurujemy NoScript, aby domyślnie zezwalał na JavaScript w przeglądarce Tor, ponieważ wiele witryn nie będzie działać z wyłączoną obsługą JavaScript. Większość użytkowników zrezygnowałaby całkowicie z Tora, gdyby strona internetowa, której chcą używać, wymaga JavaScript, ponieważ nie wiedzieliby, jak zezwolić witrynie na używanie JavaScript (lub że włączenie JavaScript może sprawić, że witryna będzie działać). Tutaj jest kompromis. Z jednej strony powinniśmy domyślnie pozostawić JavaScript włączony, aby strony działały tak, jak oczekują użytkownicy. Z drugiej strony powinniśmy domyślnie wyłączyć JavaScript, aby lepiej zabezpieczyć się przed lukami w przeglądarkach (nie tylko teoretycznie!). Ale jest trzeci problem: strony internetowe mogą łatwo określić, czy zezwalasz na JavaScript dla nich, a jeśli domyślnie wyłączysz JavaScript, a następnie pozwolisz kilku witrynom na uruchamianie skryptów (tak, jak większość ludzi używa NoScript), wtedy Twój wybór witryn z białej listy działa jako rodzaj pliku cookie, który sprawia, że jesteś rozpoznawalny (i rozpoznawalny), co szkodzi Twojej anonimowości.

Ghostery i Ghostrank - nie zabójcze, po prostu bezużyteczne na Tor, ponieważ Tor i tak wyłącza śledzenie. Jeśli go użyjesz, prawdopodobnie możesz zmienić „odcisk palca" przeglądarki, ale nie do stopnia złamania anonimowości. Ghostery nadal blokuje wszelkie skrypty śledzące, niezależnie od tego, czy korzystasz z Tora, czy nie. Ale użyj DuckDuckGo, jeśli chcesz wzmocnić swoją anonimowość. Adblock - może to również zmienić Twój odcisk palca. Adblock plus ma domyślnie włączone „akceptowalne reklamy". Istnieją również skandale związane z Adblockiem na przestrzeni lat, z których jeden sugerował, że Google zapłacił dyrektorowi generalnemu Adblock za wyświetlanie Google Ads. Poza tym podstawową ideą paczki Tora z przeglądarką jest użycie jak najmniejszej liczby dodatków. Wydaje im się, że TorButton, NoScript i HTTPS Everywhere wystarczą, aby zachować anonimowość bez dodatkowego ryzyka dodatkowych dodatków. Albo um ... dramat. Witryna Panopticlick również może być przydatna.

Whonix & Tor

Jeśli masz paranoję, że używanie Tora może wpędzić cię w kłopoty (jeśli hostujesz usługę ukrytą), możesz zajrzeć do Whonix, zanim cokolwiek uruchomisz. Wielu zaawansowanych użytkowników, którzy codziennie używają Tora, lubi większe bezpieczeństwo, jakie oferuje. Nie oznacza to, że domyślnie jest lepszy niż Tails. Oba narzędzia oferują mocne i słabe strony przeznaczone do różnych celów i może się okazać, że jedno jest lepsze od drugiego w twojej sytuacji osobistej. Podobnie jak Tails, Whonix jest tworzony z myślą o anonimowości i bezpieczeństwie. Jest również oparty na Debianie / Linuksie, więc jest to dobra synergia, jeśli chodzi o anonimowość. Ta synergia zapewnia anonimowość, przekierowując wszystko przez Tora. Zaletą jest to, że wycieki DNS są prawie niemożliwe, a złośliwe oprogramowanie nie może ujawnić Twojego adresu IP. W rzeczywistości jedyne możliwe połączenia są kierowane przez Tora przez Whonix-Gateway. Pytanie, które możesz się zastanawiać, brzmi: ile bezpieczeństwa jest zbyt dużym bezpieczeństwem? Co przesada, a co nie? Cóż, powinieneś zapytać, jak daleko spadniesz, jeśli zostaniesz złapany, i ile czasu jesteś skłonny zainwestować w czytanie, aby temu zapobiec. Tails jest łatwiejszy do uchwycenia, a jeśli nie spodziewasz się ataków ze stron, które odwiedzasz, zdecydowanie użyj Tails. Jeśli mieszkasz w Korei Północnej lub Chinach, istnieje możliwość ciężkiej pracy przy wbijaniu bezwartościowych kamieni, jeśli zauważą jakąkolwiek aktywność Tora pochodzącą z Twojej lokalizacji, która jest skorelowana z aktywnością nad „rzeczami, których nie lubią" ... lub cokolwiek innego w tym przypadku NK, która daje nadzieję. Winny do czasu udowodnienia niewinności. Jeśli więc powyższe dotyczy Ciebie, korzystaj z Whonix, ponieważ zapewnia większe bezpieczeństwo. Kilka ważnych funkcji Whonix, które zwiększają bezpieczeństwo:

Anonimowe publikacje / anty-cenzura

Anonimowy e-mail w / Thunderbird lub TorBirdy

Dodaj proxy za Torem (użytkownik -> Tor -> proxy)

Czatuj anonimowo.

Ochrona przed wyciekiem protokołu IP / DNS.

Ukryj, że używasz Tora

Ukryj fakt, że używasz Whonix

Mixmaster zamiast Tor

Bezpieczny i rozproszony mechanizm synchronizacji czasu

Bezpieczeństwo dzięki izolacji

Wyślij e-mail anonimowo bez rejestracji

Utrwal dowolną aplikację

Torify Windows

Obrazy maszyn wirtualnych (VM)

Obsługa VPN

Korzystaj z Adobe Flash anonimowo

Używaj Java / Javascript anonimowo

Poniżej znajduje się przykład średnio bezpiecznego systemu:

- Hostuj Whonix na pendrive z wybraną wersją Linuksa

- Używaj zaufanej sieci VPN (ze względu na prywatność, a nie anonimowość)

- Użyj Macchanger, aby sfałszować dowolny adres MAC podczas każdej sesji (Whonix nie ukrywa Twojego adresu Mac przed odwiedzanymi witrynami!). Jeśli Macchanger Ci się nie podoba, wypróbuj Technitium MAC Address Changer.

- Unikaj regularnych połączeń z tabletami innymi niż Tor WiFi, jeśli korzystasz z Cafe WiFi

- Dowiedz się, gdzie znajduje się każdy CCTV w obszarze, na którym planujesz używać Tora.

Adresy MAC

Wspomnieliśmy o adresach Mac. Cóż, zgodnie z technologią, twoja Nowa karta WiFi / Ethernet ma coś, co może pomóc agencjom wywiadowczym w śledzeniu Ciebie. To 48-bitowy identyfikator wypalony przez producenta. Coś jak IMEI do telefonu. Jeśli przez przypadek nie myślałeś jasno i kupiłeś swój komputer z myślą o Torze, używając karty kredytowej, możesz później zostać zaatakowany przez „NIT" FBI, który wyczyści Twój numer MAC. Jeśli tak się stanie, jesteś ugotowany. Więcej informacji na ten temat: Torsploit - https://resources.infosecinstitute.com/fbi-tor-exploit/

Sposobem na pokonanie tego jest posiadanie jednorazowego adresu MAC (numer, a nie produkt Apple). Taki, który kupiłeś za gotówkę bez kamer bezpieczeństwa. W ten sposób możesz się go pozbyć w mgnieniu oka lub wymienić. Można je również miękko konfigurować. Wierz lub nie, ale Tails sam zmienia to losowo podczas każdej sesji. W przypadku maszyny wirtualnej FBI Nit może mieć na celu numer MAC z puli VirtualBox. Naprawdę nie jest to problem, chyba że zdarzy się, że napadną na twój dom i jednocześnie złapią twój system. Tak więc codzienna wymiana tego, jak prawdopodobnie się domyślasz, może być dość uciążliwa. To głównie dla facetów, którzy prowadzą nielegalne rynki. Faceci, którzy zawsze są na celowniku agencji alfabetycznych. Ale ty też możesz. Przekonałem się, że opłaca się myśleć o sobie wyżej niż to, co jest naprawdę warte podczas przemierzania ciemnych sieci. To znaczy. Myślenie o sobie jako o wartościowym celu. Podświadomie zaprogramujesz się, aby dowiedzieć się więcej, dowiedzieć się więcej - od wszystkiego, od złych błędów w zabezpieczeniach, przez złe przyjaźnie, po złe praktyki biznesowe. Do tego nie musisz znajdować się wśród 5% najlepszych facetów, którzy opanowali bezpieczeństwo sieci. Bycie w top 25% puli jest więcej niż wystarczające, aby Mężczyzna był wystarczająco sfrustrowany, by szukać jego krzykliwych nagłówków gdzie indziej ... na przykład nisko wiszącego owocu o imieniu Neb, który mieszka na przykład w piwnicy mamy.

Mosty Whonix

Jeśli mieszkasz w komunistycznym piekle, w którym nawet wspomnienie o Torze może wpędzić cię w kłopoty, używanie Bridge z Whonix może być dosłownie uratowaniem życia.

Czym są mosty

Mosty to narzędzia zaciemniające, które pozwalają ukryć korzystanie z Tora przed wścibskim dostawcą usług internetowych lub rządem, który może widzieć, że używasz Tora, ale nie wie, co z nim robisz. W tym celu mosty Tora są alternatywnymi sposobami wejścia do sieci Tor. Niektóre są prywatne. Wiele z nich jest publicznych. Niektóre są wymienione na stronie domowej Tora. W nieprzyjaznym środowisku możesz dostrzec wartość w korzystaniu z niego na swoją korzyść, ponieważ znacznie utrudnia dostawcy usług internetowych sprawdzenie, że używasz Tora.

Czym mosty nie są

Chociaż nie są szczególnie niewiarygodne, z pewnością są „mniej" niezawodne niż regularne używanie Tora tam, gdzie idzie o wydajność. Ale kompromis może leżeć w twoim najlepszym interesie. Tylko ty możesz zdecydować, czy osiągnięcie wydajności jest uzasadnione. Oto jak to zrobić w Whonix. Mosty należy dodawać ręcznie, ponieważ nie ma metody automatycznej instalacji Whonix, ale nie jest to trudne. Wystarczy wpisać je do odpowiedniego katalogu:

/ etc / tor / torrc.

Jeśli korzystasz z graficznej bramki Whonix, przejdź do:

Menu Start -> Aplikacje -> Ustawienia -> /etc/tor/torrc.examples

Aby edytować plik torrc (niezbędny do dodawania mostka), przejdź do:

Menu Start -> Aplikacje -> Ustawienia -> / etc / tor / torrc

Następnie dodaj dowolny most, który skopiowałeś ze strony mostków Tora (lub plik prywatny, jeśli go masz). Następnie uruchom ponownie Tor'a, aby zadziałał. Jeśli napotkasz kłopoty (i najprawdopodobniej tak się stanie, jeśli to twój pierwszy raz), istnieje kilka forów, które mogą ci pomóc.

Tor Reddit : https://www.reddit.com/r/TOR/

Forum bezpieczeństwa Wildersa :

https://www.wilderssecurity.com/search/44081324/?q=whonix&o=date

Quora : https://www.quora.com/topic/Tor-The-Onion-Router

Tor i VPN

Jeśli chodzi o firmy VPN, wśród początkujących jest wiele nieporozumień. Czytają jedną rzecz, a w mediach widzą coś innego, co zaprzecza tej jednej. Zimna, twarda prawda o firmach VPN polega na tym, że nieliczni chcą twojego patronatu tak bardzo, że prawdopodobnie zakopią drobny druk na swojej stronie internetowej, na której trudno ją przeczytać. Wierz mi, to drobnym drukiem, który może cię wysłać do Wielkiego Domu, jeśli nie będziesz ostrożny. To naprawdę jest pole minowe, jeśli chodzi o te firmy. Z tego powodu musisz zdecydować, czy chcesz zachować prywatność, czy anonimowość. To różne bestie, które wymagają różnych konfiguracji. I nie każdy użytkownik VPN używa Tora i nie każdy użytkownik Tora korzysta z usługi VPN, ale korzystne jest połączenie dwóch potężnych narzędzi; taki, który zapewnia prywatność (VPN) i jedną anonimowość (Tor). Jak powiedziałem, dwie różne bestie. Ale co jest warte, jeśli podoba ci się ta kombinacja, znajdź VPN, która oferuje 128-bitowe szyfrowanie i która nie przechowuje dzienników aktywności. To jest pierwsza zasada biznesu. A oto część, w której pojawia się drobny druk. Wiele firm VPN twierdzi, że niczego nie rejestruje ... ale z chęcią zaoferują dane subskrybenta na srebrnej tacy, jeśli zażąda tego wezwanie do sądu. Pomiędzy wielkimi pieniędzmi a twoją wolnością pieniądze zawsze wygrywają. Nigdy nie pójdą za ciebie do więzienia. Zrób więc swoją należytą staranność i zbadaj. Oczywiście usługa VPN nie jest domyślnie anonimowa. Dostawcy lubią zachwalać, że tak jest, ale spójrzmy prawdzie w oczy, nie ma nic anonimowego w korzystaniu z cudzej linii, jeśli zostawiłeś ślad pieniędzy prowadzący prosto do drzwi wejściowych. Wejdź do Tora, pogromco gremlinów i wiemy, co jest dla ciebie lepsze. Tor zapewnia dodatkową i potężną warstwę bezpieczeństwa, ponieważ złodzieje będą musieli zrobić dodatkowy krok, aby coś ci ukraść. Złodzieje mają różne smaki, od zwykłych złodziei klejnotów po strażników granicznych, którzy chcą, abyś był tak samo nieszczęśliwy jak oni. Dlatego dobrym pomysłem jest zaktualizowanie wszystkich dziur w instalacji Tora. Zaktualizowane aplikacje są odporne na ataki złośliwego oprogramowania, ponieważ

znalezienie luk w kodzie, które można wykorzystać, zajmuje dużo czasu. Ale ... jeśli nie zaktualizujesz, nie ma znaczenia, której sieci VPN używasz z Torem, ponieważ twoja sesja może być zagrożona. Oto co możesz zrobić:

Opcja 1

Płać za VPN anonimowo

Oznacza to brak kart kredytowych. Brak zweryfikowanych połączeń telefonicznych. Brak linków do Ciebie lub kogokolwiek znasz. W rzeczywistości nie zostawiaj żadnego śladu finansowego dla swojego prawdziwego nazwiska, miasta ani źródła utrzymania i nigdy nie łącz się z VPN bez Tora.

Aby uzyskać optymalną anonimowość, połącz się z VPN przez Tor za pomocą Tails. Nawet jeśli VPN rejestruje każdą sesję, jeśli zawsze używasz Tora z Tailsem, złamanie tego łańcucha bezpieczeństwa wymagałoby wyjątkowo dobrze finansowanego przeciwnika. Bez logowania jest jeszcze bezpieczniejszy. Ale zawsze zakładaj, że logują się.

Opcja 2

Zapłać za VPN za pomocą karty kredytowej

Łączenie się z Torem, gdy używasz karty, na której widnieje Twoje nazwisko, nie zapewnia anonimowości. Jest to dobre dla prywatności, ale nie dla anonimowości. Jest to dobre, jeśli chcesz na przykład korzystać z Pandory w Kanadzie, ale nie, jeśli chcesz zatrudnić zabójcę kontraktowego, aby trochę poluzował usta wujka Fricka. Wujek Frick, który ma 115 lat i ma wiedzę na temat tego, gdzie jest zatopiony skarb. Ehem, w każdym razie, usługi VPN są czasami źle oceniane przez entuzjastów anonimowości, ale rejestracja anonimowa w VPN ma zalety. Na przykład wzmacnia anonimowość podczas korzystania z Tora. Nawet jeśli VPN przechowuje dzienniki każdego użytkownika, nawet na podstawie orzeczenia sądowego nie będą oni znać prawdziwej tożsamości danego użytkownika. Jednak jeśli korzystałeś z Paypal, Bitcoin, kart kredytowych lub innych możliwych do zidentyfikowania metod płatności, aby subskrybować VPN w wyraźnym celu korzystania z Tora, anonimowość jest osłabiona, ponieważ pozostawiają ślad na papierze (sam Bitcoin nie jest anonimowy). Ale prawdziwym minusem i brudną rynną są witryny .onion. Są to strony, do których można uzyskać dostęp tylko za pomocą Tora. Problem polega na tym, że ostatnim łączem łączącym te strony musi być Tor, a nie VPN. Zrozumiesz, o co chodzi, gdy połączysz się z takim, które wywołuje nasze następne pytanie.

Jak przyjazny dla Tor jest VPN?

To zależy od Ciebie. Spamerzy używają Tora. Hakerzy używają Tora. Złodzieje tożsamości używają Tora. Kilka sieci VPN ma zastrzeżenia co do umożliwienia użytkownikom uzyskania 100% anonimowości poprzez rejestrację anonimową. Ale jeśli zarejestrowałeś się anonimowo, nie masz się czego obawiać, ponieważ w tym momencie to ich tyłek jest na linii. Jest tylko jeden problem: twardogłowym w FBI nie podoba się taka postawa. W rzeczywistości tak szybko by cię ścigali, jeśli używasz VPN przez Tor. Czy osoba może stać się podwójnie podejrzana, jeśli użyje obu? Może. „Organ dochodzeniowy Departamentu Sprawiedliwości próbuje spiąć kontrolę prawną czwartej poprawki, żądając zmiany w federalnych przepisach postępowania karnego. Te przepisy proceduralne określają, w jaki sposób organy ścigania muszą prowadzić postępowania karne, od śledztwa do wszelkiego odstępstwa od zasad mogą mieć poważne konsekwencje, w tym oddalenie sprawy. Konkretna zasada, na którą kieruje się FBI, określa warunki uzyskania nakazu przeszukania. Nazywa się to Zasada Federalna 41(b), a żądana zmiana pozwoliłaby na wprowadzenie prawa egzekwowanie w celu uzyskania nakazu przeszukiwania danych elektronicznych bez podawania żadnych szczegółowych informacji, o ile lokalizacja komputera docelowego została ukryta za pomocą narzędzia technicznego, takiego jak Tor

lub wirtualna sieć prywatna. Pozwoliłoby to również na niespecyficzne nakazy wyszukiwania w przypadku, gdy komputery były celowo uszkodzone (na przykład przez botnety, ale także przez popularne złośliwe oprogramowanie i wirusy) i znajdują się w co najmniej pięciu oddzielnych federalnych okręgach sądowych. Ponadto przepis umożliwiłby śledczym zajęcie informacji przechowywanych w formie elektronicznej niezależnie od tego, czy informacje te są przechowywane w jurysdykcji sądu, czy poza nim. Zmiana może brzmieć jak modyfikacja techniczna, ale jest to duży krok naprzód obecna procedura. "

NSA robi to bez przeszkód. Wiemy o tym z przecieków Snowdena, że FBI wykorzystuje metadane NSA z zapisów telefonicznych prywatnych obywateli. Dlatego VPN nie jest dla nich naprawdę potężną przeszkodą. Ale to przenosi to na zupełnie inny poziom, ponieważ jeśli samo zarejestrowanie się w VPN stanowi podstawę do legalnego przeszukania, to mogą szpiegować na serwerze dowolnego dostawcy usług internetowych, którego chcą, bez żadnych podstaw prawnych, aby to uzasadnić. Zrobili podobne rzeczy w Brazylii. Ale tutaj, w starych dobrych Stanach Zjednoczonych, zwykle wygląda to tak:

1.) Szpieguj JoBlo, aby zobaczyć, co zamierza.

2.) Uzasadnij przejęcie komputera / rajdu / danych, odtwarzając skrzynkę

3.) Naciskaj na właściwe osoby z bezpośrednim dostępem do informacji o subskrybentach

4.) Wezwanie do odszyfrowania danych subskrybenta. Jeśli zrobili to raz, mogą zrobić to sto razy więcej. Nie ma sprawy.

Rozwiązanie:

Jeśli masz zamiar wybrać trasę VPN, użyj PGP: Pretty Good Privacy. Nigdy, przenigdy nie przesyłaj zwykłych danych przez VPN, nawet taką, która oferuje SSL.

Końcowe przemyślenia:

1.) Rozmowa z policją nigdy ci nie pomoże. Nawet w sytuacji nalotu. Prawdopodobnie obudzą cię na o 6 rano i zagrożą rodzinie, że wezmą wszystkich do więzienia, chyba że ktoś się przyzna. To wszystko kłamstwa, cały czas przez te agencje. Znajomy zauważył kiedyś, że funkcjonariusz w cywilu zapukał kiedyś do jego drzwi, aby zapytać go, czy używa Tora, tylko po to, by upewnić się, że nie robi niczego nielegalnego. Odpowiedział, że tak, ale nic nielegalnego, sir. Później udowodniono, że jest niewinny, ale dopiero wtedy, gdy gliny przrciągnęły reputację tego człowieka przez błoto. Nie przyszły żadne publiczne przeprosiny (czy kiedykolwiek?).

2.) Jeśli nie pobierają opłat za prowadzenie usługi ukrytej, wyjdź. Właściwie, jeśli o nic cię nie oskarżą ... wyjdź. Pomoże im każde słowo z twoich ust, nie ty.

3.) Nie masz powodu, aby usprawiedliwiać im cokolwiek zrobione masz we własnym domu lub gdziekolwiek indziej. Odpowiedzialność za udowodnienie winy spoczywa na nich, a nie na Tobie. Ale jeśli jesteś w sytuacji, w której musisz porozmawiać lub zrezygnować z zaszyfrowanego laptopa, zawsze najpierw rezygnuj z laptopa. Laptopy są tanie i łatwe do wymiany. Pięć lat więzienia nie.

Używanie Bitcoinów do anonimowej rejestracji w usłudze VPN

Bitcoiny nie są przeznaczone do zapewnienia całkowitej anonimowości, ale nie są też VPN. Są zaprojektowane z myślą o prywatności, tak. Dlaczego więc ich używać? Cóż, ponieważ każda dodatkowa warstwa, która wzmacnia twoją anonimowość, jest warstwą, której potrzebujesz. Ale tak jak w przypadku każdego zaawansowanego narzędzia, możesz zmniejszyć anonimowość, jeśli będziesz z nim nieostrożny. Dobre, ciasne narzędzia anonimowości mogą być zgubą lub dobrodziejstwem:

dobrodziejstwem pod warunkiem, że odrobisz pracę domową. Jeśli nie, następuje głupota i zażenowanie, prawdopodobnie sytuacja, w której, w zależności od kraju, w którym się znajdujesz, równie dobrze możesz założyć sobie kajdanki. To smutne, że nadeszły czasy w tej kłopotliwej sytuacji.

Zastanówmy się więc, w jaki sposób płaci się za VPN i uzyskuje ten poziom absolutnej anonimowości ... uznając, że sieć VPN sama w sobie nie zrobi nic, aby osiągnąć ten cel. To tylko jedno narzędzie w skrzynce narzędziowej pełnej narzędzi, a Bitcoin jest tylko jednym z nich. Nie próbowałbyś naprawiać silnika Camaro tylko kluczem, prawda?

A teraz o Bitcoinie ...

Bitcoiny to monety typu open source, cyfrowa waluta, która wykorzystuje kod podobny do P2P i podobnie jak prawdziwe pieniądze można za ich pomocą kupować produkty online. Produkty takie jak karty pamięci w Newegg, a nawet usługa premium Usenet lub VPN. Są dla nas przydatne. Korzystając z tych bitcoinów, użytkownik końcowy całkowicie omija potrzebę unii kredytowej lub banku. Całkiem schludnie. Ale nie są pozbawione wad. Więcej o tym za chwilę. Na razie po prostu wiedz, że są one tworzone na podstawie zbiorczych obliczeń procesora macierzy użytkowników (na przykład takich jak Ty), którzy przekazują darowizny na ich stworzenie. W grę wchodzi wydobywanie bitcoinów i chociaż być może widzieliście obrazy bitcoinów na stronach internetowych ze złotym „B", w rzeczywistości nie są one czymś, co można nosić w kieszeni. A przynajmniej nie w taki sposób, w jaki myślisz. Mają coś wspólnego z PGP - klucze publiczne i prywatne - podobnie jak aplikacja PGP, tylko zamiast weryfikować twoją tożsamość, tak jak robi to PGP, Bitcoiny weryfikują saldo. Tutaj właśnie pojawiają się portfele Bitcoin. Ponownie, nie jest to magiczna kula, ale raczej jedno narzędzie do naszej dyspozycji. W tym momencie portfele bitcoin będą coraz lepsze w wzmacnianiu anonimowości w nadchodzących latach. Osiągną to, przerywając szlak do naszej prawdziwej tożsamości. Aha, a ich rozwój stale się poprawia. Jednak jak wspomnieliśmy wcześniej - zawstydzenie wyniknie, jeśli zaniedbasz odrobinę pracy domowej, za każdy zakup przez określony portfel można prześledzić. Zgadza się. Jeśli kupisz wraz z nią nową kartę graficzną w Newegg, tę samą, która przechowuje dane Twojej karty kredytowej, a następnie zasubskrybujesz usługę Usenet lub VPN, zgadnij, co ... masz już ślad do swojej prawdziwej tożsamości. FBI czy chiński rząd nie będą potrzebować ujadania ogarów, żeby cię wywęszyć. Ale nie, jeśli dokonasz tylko jednego zakupu na portfel. Oznacza to, że nigdy nie używaj go dla żadnego podmiotu internetowego, w którym kupiłeś towary, gdy twoje prawdziwe IP jest podłączone. Oznacza to również rezygnację z Google Plus, Facebooka, Skype'a i wszystkich mediów społecznościowych z tym portfelem. Twitter, Wal-Mart, BestBuy, a nawet małe sklepy typu mom & pop z przyciskami multimediów multisocial rozrzuconymi po wszystkich witrynach internetowych - są to wrogowie anonimowości, niezależnie od tego, czy o tym wiedzą (bardziej prawdopodobne, że nie). Nie są już naszymi przyjaciółmi, tak jak granat jest twoim przyjacielem po wyciągnięciu zawleczki. Pojedyncza osoba może mieć kilka adresów i dokonywać tylko dwóch zakupów rocznie, ale jeśli zanieczyszcza się krzyżowo przez pomieszanie (każda transakcja jest rejestrowana w łańcuchu bloków Bitcoin), anonimowość jest osłabiona i w większości przypadków zniszczona przez jego własne działania. Niedobrze. Sztuczka jest taka: nie twórz wzoru. Ciąg zakupów tworzy wzór; dokładny wzór kodu Google i Amazon w swoich algorytmach do wyszukiwania i lepszego kierowania reklam opartych na zainteresowaniach. Złe dla anonimowości i nie najgorsze, co może się zdarzyć. Rozwiązujemy ten problem za pomocą mikserów Bitcoin. Osłabiają one powiązania między kilkoma różnymi adresami Bitcoin, ponieważ historia tego zakupu jest wymazywana przez wymianę Bitcoinów między innymi użytkownikami Bitcoin. Masz do wyboru kilka opcji. Jednym z nich jest BitFog, ale jest wiele innych.

Portfele Bitcoin

Aby zasubskrybować VPN lub kupić cokolwiek online za pomocą Bitcoinów, wymagany jest portfel Bitcoin. Dostępnych jest więcej niż jeden typ. Omówimy każdy i wymienimy ich zalety i wady.

Portfel na Pulpicie

To jest to, czego używam i nie bez powodu: mam nad tym absolutną kontrolę, nie wspominając już o tym, że mieć dostęp do moich pieniędzy na serwerze internetowym innej osoby, podważa całą ideę anonimowości. Nigdy nie przechowywałbym moich zaszyfrowanych plików „w chmurze" i Ty też nie powinieneś. Przynajmniej nie bez niesamowicie bezpiecznego systemu. Pomyśl o tym. Czy zakopałbyś swój sejf na podwórku sąsiada z tabliczką For Sale z przodu? To ta sama oferta. Serwer mógł się zepsuć. Firma może zbankrutować. Każda osoba po drugiej stronie po stronie gospodarza może zainstalować keylogger bez Twojej wiedzy. Paskudne robale, te rzeczy. Portfele na komputery stacjonarne nie są idealne, pamiętaj, ale są lepsze niż Chmura. Jedynym minusem jest to, że musisz wykonać kopię zapasową portfela Bitcoin, co jest szczególnie konieczne, jeśli zawiera dużo pieniędzy. Robię to dość regularnie co tydzień, tak jak ty. Przepraszam, jeśli to wszystko brzmi jak niedzielne kazanie, ale niektóre z tych rzeczy naprawdę należy traktować jako ewangelię.

Portfel mobilny / podróżny

Jak sama nazwa wskazuje, nosisz je przy sobie, aby dokonywać zakupów w taki sam sposób, jak przy użyciu karty kredytowej. Wygoda x 1000. Jest wiele rodzajów portfeli, takich jak Coinbase i Electrum, ale stwierdziłem, że Multibit jest bardzo łatwy do nauczenia. Jest dostępny zarówno w systemie Linux, jak i Windows i oferuje opcję frazy hasła. Nawet bilans wygląda jak interfejs PGP, ale jest przyjazny dla początkujących i open-source, więc nie ma backdoorów. Dobre dla anonimowości.

Instalacja Multibit w systemie Windows

Teraz dochodzimy do instrukcji czystej instalacji tego cudu.

Pobierz instalator systemu Windows. Uruchom instalator. Możliwe problemy, na które możemy się natknąć: W 64-bitowym systemie Windows, który jest obecnie wybieranym systemem poza Linuksem, może się zdarzyć, że wirtualna maszyna Java (JVM) nie jest poprawnie zlokalizowana lub „Nie udało się utworzyć selektora" pokazane w komunikacie o błędzie. Rozwiązaniem jest zmiana ustawienia zgodności:

-Wybierz okno dialogowe zgodności (kliknij prawym przyciskiem myszy -> ikona - Właściwości ->

Zgodność)

-Wybierz: „Uruchom ten program w trybie zgodności z systemem Windows XP SP3 ".

-Zaznacz pole: „Uruchom ten program jako administrator"

Instalacja Multibit Linux

Jeśli jesteś fanem Linuksa (i powinieneś być, jeśli anonimowość to coś dla ciebie)

Pobierz instalator Linux / Unix. Otwórz okno terminala i utwórz plik wykonywalny instalatora za pomocą:

-chmod + x multibit-0.5.18-linux.jar

-Uruchom instalator: java -jar multibit-0.5.18-linux.jar

-Zainstaluj

Następnie w menu „Aplikacje | Inne” będziesz mieć skrót do uruchomienia MultiBit. Jeśli nie widzisz skrótu MultiBit, możesz uruchomić MultiBit ręcznie, wykonując następujące czynności:

-otwórz okno terminala i 'cd' do katalogu instalacyjnego wpisz java -jar multibit-exe.jar

Teraz czas na zakup Bitcoinów. Istnieje kilka przydatnych przewodników, w których można znaleźć listę możliwych korzyści unikalnych dla danego obszaru geograficznego.

Istnieje kilka opcji, ale to, co chcemy zrobić, to wykonać opcję offline; kupować bitcoiny poza siecią, których nie można prześledzić. Cash n 'carry.

LocalBitcoins wygląda obiecująco, podobnie jak TradeBitcoin. Ale kiedy Trade spogląda w dół, przejdźmy do LocalBitcoins.

- Po wybraniu zestawu Bitcoin, musisz zarejestrować się na stronie (anonimowo), ale pamiętaj o oprocentowaniu, które różni się w zależności od tego, ile chcesz handlować. W przypadku tej transakcji użyj e-maila, w którym zarejestrowałeś się anonimowo. To znaczy:

- Przeglądarka Tor / Tails

- Brak plików cookie Facebooka lub innych mediów społecznościowych / wyszukiwania na komputerze

- Dostęp tylko dla Tor / Bitcoins.

Wybierz opcję „Kup” na stronie sprzedającego i kwotę, którą chcesz kupić. Pamiętaj, że nie kupujemy tutaj domu, tylko VPN do użytku z Torem. Gdy środki zostaną przelane z Escrow, otrzymasz powiadomienie. Zwróć uwagę, że sprzedawca, z którym masz do czynienia, może być w stanie zobaczyć Twoje informacje finansowe, tj. z jakiego banku korzystasz itp., ale zawsze możesz zdecydować się na spotkanie osobiste, jeśli chcesz. Wiąże się to z całym innym zestawem zagrożeń. Sprawdź, czy środki znajdują się w Twoim portfelu Bitcoin.

Płacenie za VPN do użytku z Tor

Nadszedł czas, aby zapłacić za usługę VPN ... anonimowo. Wybierzmy Air VPN za 9 USD / mies., Który akceptuje również płatności w Bitcoinach.

Po pierwsze: zarejestruj się w usłudze, ale nie podawaj żadnych informacji, których używałeś w innych witrynach, takich jak nazwy użytkowników lub hasła. Ponadto, ponieważ nie musimy wprowadzać żadnych danych bankowych, żaden ślad pieniędzy nie zostanie do nas prześledzony. Adres e-mail, którego używamy, to jednorazowy e-mail (używałeś Tora do rejestracji, prawda?) Po drugie: podaj adres portfela dla naszej płatności Bitcoin. Hit wyślij. Gotowe!

Podobnie jak każda usługa Usenet, usługa VPN wyśle potwierdzenie na Twój adres e-mail ze szczegółami potrzebnymi do korzystania z tej usługi. Następnie możesz zobaczyć szczegóły tej płatności w swoim portfelu Bitcoin. Jak widać, doktorat z informatyki nie jest potrzebny do uzyskania tej dodatkowej warstwy anonimowości. Problem z masą ludzi korzystających z Tora polega jednak na tym, że nie można im przeszkadzać, wykonując te proste dodatkowe kroki. To im szkodzi. Dobrze dla ciebie. Ci, którzy noszą dodatkową zbroję, często stoją po długiej bitwie. Pozostał jednak jeden temat do omówienia i jest on najważniejszy (c.d.n.)

Używanie prawdziwego imienia i nazwiska online poza Tor

To jest duża rzecz. Taką, którą jestem winny złamać, ponieważ nawet orzechy anonimowości mogą pękać od czasu do czasu pod presją rówieśników i robić coś głupiego, jak używanie Facebooka zamiast Tora. Pytanie, które wtedy zadawałem, brzmiało:

Jakie niebezpieczeństwo wiąże się z używaniem swojego prawdziwego imienia i nazwiska w Internecie?

Cóż, to zależy.

Organy ścigania i potencjalni pracodawcy, którzy przeszukują Twoją obecność w mediach społecznościowych, są często gorsi niż złodzieje, którzy ślinią się, gdy ogłaszasz na Twitterze, że będziesz poza miastem przez dwa tygodnie. Złodzieje, choć niesmaczni i zboczeni przestępczo, rzadko twierdzą, że są sprawiedliwi. A złodzieje, jak wspomniano wcześniej, mają różne kształty i rozmiary. Jeśli zabiorą Twoje prywatne dane bez uprzedniego zapytania, oznacza to kradzież. Pracodawcy mogą być najgorsi, tak hipokrytyczni jak Harvey Two-Face, żądający przejrzystości w życiu, ale nie w swoim. Zrób rozpalony polityczny post lub napij się wina na wakacjach na Bora Bora z półnagimi Filipinkami wirującymi pałeczkami ognia, a możesz stracić pracę ... lub jej odmówić. Nie żartuję. Wspomnij, że używasz Tora i możesz usłyszeć, jak ankieter pyta:

„Zauważyłem, że jesteś wielkim fanem Tora. Czy mógłbyś wyjaśnić, dlaczego potrzebujesz korzystać z usługi anonimizacji? Lubimy przejrzystość naszych pracowników ”.

Tak, zapytano mnie o to w wywiadzie na stanowisko, które obsługiwało dużo pieniędzy. Pojawił się znikąd, ale najbardziej martwił mnie swobodny sposób, w jaki został poproszony, na przykład każdy kandydat powinien mieć coś do ukrycia, jeśli chce anonimowej komunikacji. Może byłem jakimś wściekłym fanem Jasona Bourne'a i do niczego. W każdym razie nie podobała im się moja odpowiedź.

„Ponieważ cenię wolność”.

Wyszedłem z tego wywiadu zakłopotany, ale bez pracy, traktując prywatność jako coś w rodzaju miecza obosiecznego, ponieważ wielu pracodawców o wyższych dochodach potrzebuje obecności w Internecie. Nie pasowało mi to. Szczerze mówiąc, poczułem się trochę oszukany i kiedy jechałem do domu, niektóre z mamrotań, które później usłyszałem, stały się tak głośne jak ryczące pociągi w uszach: Nie lubisz kogoś na Facebooku? Prawdopodobnie nie spodoba ci się praca z nimi.

Podobnie jak produkty konkurencji? Oto nasz trzyletni zakaz konkurowania , umowa do podpisania. Używasz Tora? Jedynymi ludźmi, którzy tego używają, są terroryści, pedofile i zabójcy. Wkrótce potem, za każdym razem, gdy potencjalny pracodawca zauważył „Tor” w sekcji Hobby mojego CV, zawsze miałoby to negatywną reakcję. Mój oddech stałby się nierówny, gdy moje serce biło szybciej, jakby zamierzali wezwać nieskrępowany „autorytet”, aby ostrzec mnie przed zachowaniem prywatności. Ubierałby się bardzo jak Dilbert, tyle tylko, że byłby szczuplejszy, miałby żółty jak trzmiel długopis i notatnik. Miałby wiele tików na twarzy i dziwaczny zwyczaj unoszenia brwi wulkanu, jakby to było czysto nielogiczne, aby docenić

Prywatność. Nie mam pojęcia, dlaczego miał notatnik, ale zawsze to robił.

Moim rozwiązaniem było słuszne podzielenie mojej tożsamości publicznej i prywatnej w kontekście społecznościowym i usunięcie wszelkich jej śladów z mojego CV. W rzeczywistości w żadnym serwisie społecznościowym nie wskazałem również, że kręci mnie któryś z poniższych:

- PGP

- Szyfrowanie lub szyfrowanie plików lub systemów operacyjnych

- Przekaźniki Tor

- I2P

- Freenet

- Ogólnie anonimowość

- Wszystko, co łączy się z Edwardem Snowdenem

Taka jest natura mas. Po prostu nie można polegać na Facebooku, Twitterze lub Google, jeśli chodzi o poszanowanie wolności korzystania z Tora bez ogłaszania tego całemu światu. Ale dzięki Torowi Google nie może wydobywać Twojej sesji przeglądania w poszukiwaniu reklam. Brak reklam = brak zupy dla nich. Z NBC:

„Gigant wyszukiwarek internetowych zmienia warunki świadczenia usług od 11 listopada. Twoje recenzje restauracji, sklepów i produktów, a także piosenek i innych treści kupionych w sklepie Google Play mogą pojawiać się w reklamach wyświetlanych Twoim znajomym, połączeń i szerszej publiczności, gdy wyszukują w Google. Firma nazywa tę funkcję „rekomendacjami wspólnymi". Dlatego zaporę ogniową zabezpieczam wszystko, co robię. Używam Ghostery do serwisów społecznościowych i udostępniam tylko pseudonimowe dane o sobie. W rzeczywistości staram się unikać jakiejkolwiek korelacji między Torem a jakimkolwiek serwisem społecznościowym, tak jak kanister benzyny i zapalona zapałka.

Anonimowość e-maili

Był czas, kiedy nie musieliśmy się martwić o to, co mówimy w e-mailach. Bezpieczeństwo? To było coś, co zrobili maniacy. Geekowie i supergeekowie, którzy uczestniczyli w konwencjach hakerów i przeszukiwali Usenet w poszukiwaniu exploitów zero-day. Były to czasy Altavista i Infoseek, kiedy Google wciąż był mokry za uszami, a Microsoft wciąż walczył o zaspokojenie kaprysu każdego użytkownika Dos. Pisaliśmy, co chcieliśmy, i wysyłaliśmy bez obaw, że osoby trzecie przechwycą to i użyją naszych własnych słów przeciwko nam. Niestety już nie. Reklamy i wyszukiwarki dostosowują teraz reklamy do osób w oparciu o to, co lubisz i na pewno klikniesz. Pozostają ślady. Wiadomości są skanowane. Gmail nie różni się niczym od Yahoo czy Microsoft. W rzeczywistości sędziowie mają większą władzę piórem niż jakikolwiek dyrektor generalny jakiejkolwiek firmy w Ameryce Północnej. Kiedy wycieknie zwiastun lub ktoś powie coś nieprzyjemnego na temat rządu, możesz założyć się, że adresy IP zostaną wezwane. Czasami wyobrażam sobie, że wielu byłych sowieckich oficerów śmieje się z tego, ile donosicieli produkuje w ciągu roku Internet. Ekstremalna przewrotność. Ale ... czy można wysłać wiadomość, która jest niezawodna w przypadku wezwań? W rzeczywistości istnieje wiele smaków do wyboru, aby wykonać to zadanie. Poniżej znajduje się kilka solidnych usług. W połączeniu z Torem zapewniają wirtualną fortecę. Anonimowość jest podniesiona do kwadratu, jeśli wiadomość jest zaszyfrowana.

Pierwsze to TorGuard. TorGuard umożliwia użytkownikom korzystanie z PGP (Pretty Good Privacy) w e-mailach, więc nie musisz się martwić o szpiegowanie. Otrzymujesz 10 MB plus kilka warstw ochrony z obsługą mobilności. Drugi to W3, The Anonymous Remailer. Możesz łączyć się z Torem, potrzebujesz tylko adresu e-mail, na który chcesz wysłać wiadomość (najlepiej zaszyfrowanego za pomocą PGP - więcej o tym za chwilę). Innym jest Guerrilla Mail. Pozwala użytkownikom tworzyć jednorazowe wiadomości e-mail do użytku w czasie wolnym. Wysłane e-maile są natychmiast usuwane z systemu po naciśnięciu przycisku Wyślij. W każdym razie w ciągu godziny. Wszystkie te usługi twierdzą, że są anonimowe, gdybyśmy nie szyfrowali naszych wiadomości - co prowadzi nas do PGP. PGP to standard szyfrowania wybierany przez wielu starych użytkowników, takich jak ja, i nie bez powodu. Nigdy nie został złamany przez NSA, FBI ani żadną agencję wywiadowczą i prawdopodobnie nie zostanie złamany, dopóki komputery kwantowe nie staną się powszechne. Działa na zasadzie par kluczy, jednego publicznego i jednego prywatnego (tego, którego będziesz używać do odszyfrowywania wiadomości). Nie martw się terminem „klucze". Nie jest to trudne do uchwycenia i będzie tak łatwe, jak kliknięcie przycisku Wyślij, gdy już to zrobisz. Pierwszą rzeczą, którą musisz zrobić, jest udostępnienie klucza

publicznego. Służy to tylko do weryfikacji Twojej tożsamości i nie jest tym samym, co ujawnienie hasła, na przykład kontenera Drivecrypt. Twój odbiorca musi również udostępnić Ci swój klucz, abyś mógł po kolei odpowiedzieć.

Dobre wieści?

Tylko we dwoje będziecie mogli czytać swoje wiadomości. Zastrzeżenie jest takie, jeśli druga osoba jest zagrożona, a Ty o tym nie wiesz. Przeczytają wszystko, co zaszyfrujesz. Oto, co musisz wiedzieć:

1.) Na początek utwórz dwa klucze, jeden publiczny - dla wszystkich poza tobą - i jeden, którego nawet nie udostępnisz swojej matce. Powinieneś wykonać kopię zapasową tego klucza na bezpiecznym nośniku i pamiętaj, że jeśli nie ma kopii zapasowej na trzech różnych typach nośników, nie zostanie utworzona kopia zapasowa. Jeśli jesteś naprawdę paranoikiem, wyślij jedną na zaszyfrowanej karcie microSD do swoich rodziców na wypadek pożaru w domu. Tak, to się zdarza.

2.) Jeśli jednak zdecydujesz się powiedzieć mamie, będzie potrzebowała Twojego klucza publicznego (opublikowałeś go na serwerze kluczy publicznych, prawda?). Następnie możesz go odczytać za pomocą swojego klucza prywatnego. Nie zna tego klucza (dzięki bogom!)

3.) Możesz "podpisać" dowolną wiadomość przez Tora lub gdziekolwiek indziej

(Na przykład Freenet, którego najwyższe ustawienie bezpieczeństwa wymaga absolutnego zaufania do połączenia Darknet twojego przyjaciela), aby sprawdzić, czy to naprawdę Ty je wysyłasz.

... Chyba że Norman Bates zrobi na tobie scenę prysznica i zabierze klucze. Twoja mama może następnie zweryfikować za pomocą Twojego klucza publicznego, że to naprawdę Ty.

4.) Użytkownicy, z którymi komunikowałeś się (lub nie), mogą podpisać Twój klucz publiczny jako sposób weryfikacji Twojej tożsamości. Jak widać, im więcej osób to robi, czyli ręczy za Ciebie, tym lepiej.

Ważny:

Chyba że masz fotograficzną pamięć Dustina Hoffmana z Rainmana, dobrym pomysłem jest przechowywanie kluczy i haseł publicznych / prywatnych, a także certyfikatu unieważnienia na nośniku kopii zapasowej, abyś mógł go odzyskać pięć lat później ... gdybyś tego potrzebował. I uwierz mi, będziesz! Zaszyfruj je w kontenerach. Zawsze drukuj plik klucza lub frazę hasła i przechowuj w bezpiecznym miejscu. Jeśli go zgubisz, wszystkie zaszyfrowane za jego pomocą dokumenty zostaną trwale utracone. Nie ma tylnych drzwi i nie ma możliwości odszyfrowania bez tego. Rozważ także określenie daty wygaśnięcia podczas tworzenia pary kluczy. Jeśli lubisz ładne i łatwe interfejsy, wypróbuj Mymail-Crypt dla Gmaila Google. Jest to wtyczka, która umożliwia użytkownikom korzystanie z wiadomości zaszyfrowanych za pomocą PGP w poręcznym interfejsie, ale upewnij się, że Twoja przeglądarka jest szczelna i ufasz jej kluczem prywatnym.

Jeszcze jedno

Zamiast szyfrować pliki i przesyłać je w niebezpieczne miejsce, spójrz na narzędzie szyfrujące AxCrypt. Jest to przydatne, jeśli jesteś przyzwyczajony do przesyłania plików do Dropbox lub Google Drive. Pamiętaj tylko, że w przypadku, gdy prześlesz zaszyfrowany plik do „The Cloud", nie dowiesz się o tym, jeśli twoje hasło do tego pliku zostało złamane bez ustawiania ścisłych reguł bezpieczeństwa. Mając to na uwadze, skonfigurujmy PGP dla Windows

- Zainstaluj Gpg4Win

- Następnie utwórz swój klucz w Kleopatrze i wybierz Eksportuj-certyfikat-na-serwer, klikając prawym przyciskiem myszy, aby móc opublikować go na serwerze kluczy. Poproś zaufanego przyjaciela o „podpisanie" i zdobycie zaufania.

- Użyj klienta Claws-Mail, który jest z nim dostarczony lub użyj Enigmail, jeśli używasz Thunderbirda.

- Wysyłaj kilka wiadomości w tę iz powrotem do zaufanego przyjaciela przez PGP, aby opanować sytuację.

- Opcjonalnie możesz ustawić filtr Yahoo / Gmail / Hotmail, aby przekazywać wiadomości zawierające komunikat „Rozpocznij wiadomość PGP" na bardziej prywatne konto.

Pakiet Tor Instant Messaging

Nie jest tajemnicą, że NSA ma Skype, Yahoo Chat i inne natychmiastowe usługi wiadomości w swoich rękach, ale dopóki zespół programistów Tora o tym wie, mogą coś z tym zrobić.

Wejdź do pakietu Tor Instant Messaging:

https://trac.torproject.org/projects/tor/wiki/org/meetings/2014WinterDevMeeting/notes/RoadmapTIMB

Celem tej aplikacji jest prawdziwa anonimowość. Jest zbudowany przez tego samego, który opracował pakiet przeglądarki Tor i podobnie jak ta aplikacja, będzie kierować całą komunikację przez przekaźniki Tora ... zaszyfrowaną wstecz i do przodu i ukrytą przed wścibskimi oczami NSA.

Jest też Torchat.

Torchat, podobnie jak komunikator Yahoo, oferuje szyfrowane rozmowy, a nawet udostępnianie plików. Ponieważ jest oparty na Torze, masz zapewnioną całkowitą prywatność tego, co mówisz i komu to mówisz. Dostępne są wersje dla systemu Windows i Mac i nie jest wymagana instalacja. Po prostu rozpakuj w dowolnym miejscu i uruchom (najlepiej z zaszyfrowanego dysku twardego lub napędu USB) symbol niebieskiej ziemi zatytułowany „Torchat". Kilka bardziej przydatnych aplikacji:

ChatSecure - ChatSecure jest używany głównie do szyfrowania wiadomości na urządzeniach mobilnych, ale oferuje również wersje na komputery PC, Linux i Mac.

Projekt Guardian tworzy łatwe w użyciu bezpieczne aplikacje o otwartym kodzie źródłowym, biblioteki oprogramowania i spersonalizowane urządzenia mobilne, które mogą być używane na całym świecie przez każdą osobę, która chce chronić swoją komunikację i dane osobowe przed niesłusznym włamaniem, przechwyceniem i monitorowaniem. Niezależnie od tego, czy jesteś przeciętnym obywatelem, który chce potwierdzić swoje prawa, czy też aktywistą, dziennikarzem lub organizacją humanitarną, która chce chronić Twoją pracę w dobie niebezpiecznej globalnej komunikacji, możemy pomóc Ci stawić czoła zagrożeniom, przed którymi stoisz.

Telegram - ta aplikacja koncentruje się również na przesyłaniu wiadomości, ale z większą szybkością i jest podobna do SMS-ów i umożliwia wysyłanie zdjęć / wideo. Istnieją również „tajne czaty", które oferują zaszyfrowane sesje. Twierdzą, że żadne dane nie są przechowywane na ich serwerach, a nawet możesz ustawić aplikację tak, aby trwale usuwała wszystkie wiadomości.

CryptoCat - Zapowiadany jako alternatywa dla aplikacji do czatu w mediach społecznościowych, takich jak te widoczne na Facebooku, Twitterze i podobnych, CryptoCat zapewnia zaszyfrowaną komunikację przy użyciu standardu szyfrowania AES. Wszystkie zaszyfrowane informacje są usuwane po godzinie bezczynności.

Freenet - to dziadek wszystkich anonimowych systemów na świecie , zarówno do udostępniania plików, jak i wszelkiego rodzaju tajnych rozmów. Wyjaśnienie wszystkiego, co ma do zaoferowania, wykracza daleko poza naszą dyskusję na temat Tora, ponieważ są to dwa różne systemy, ale dołączam to tutaj jako alternatywę, jeśli brakuje Tora. I nie jest tak proste jak Tor, ani nie jest tak szybkie, chyba że zostawisz go działającego 24 godziny na dobę, 7 dni w tygodniu. To nie jest dla wszystkich, ponieważ używają go wszelkiego rodzaju podmioty przestępcze i zauważysz to, jeśli załadujesz jakiekolwiek grupy. Trudno to zignorować iw przeciwieństwie do Usenetu nie ma do kogo reklamować. Nikogo do zgłoszenia. Jest to anarchia zwielokrotniona wielokrotnie w wielu grupach, ale istnieją sposoby na złagodzenie szkód. Ale dla absolutnej anonimowości i wolności słowa nie ma lepszego narzędzia do użycia, jeśli masz cierpliwość, aby zapoznać się z ofertą Darknet. Freenet to darmowe oprogramowanie, które pozwala anonimowo udostępniać pliki, przeglądać i publikować „darmowe strony” (strony internetowe dostępne tylko przez Freenet) oraz rozmawiać na forach bez obawy o cenzurę. Freenet jest zdecentralizowany, aby uczynić go mniej podatnym na ataki, a jeśli jest używany w trybie „darknet”, w którym użytkownicy łączą się tylko ze swoimi znajomymi, jest bardzo trudny do wykrycia. Komunikacja przez węzły Freenet jest szyfrowana i kierowana przez inne węzły, co bardzo utrudnia określenie, kto żąda informacji i jaka jest ich zawartość. Użytkownicy przyczyniają się do pracy w sieci, udostępniając przepustowość i część swojego dysku twardego (nazywaną „magazynem danych”) do przechowywania plików. Pliki są automatycznie zachowywane lub usuwane w zależności od ich popularności, przy czym najmniej popularne są odrzucane, aby zrobić miejsce dla nowszych lub bardziej popularnych treści. Pliki są zaszyfrowane, więc ogólnie użytkownik nie może łatwo odkryć, co znajduje się w jego magazynie danych i miejmy nadzieję, że nie może być za to pociągnięty do odpowiedzialności. Fora czatów, witryny internetowe i funkcje wyszukiwania są oparte na tym rozproszonym magazynie danych. Ważnym niedawnym osiągnięciem, które ma bardzo niewiele innych sieci, jest „darknet”: łącząc się tylko z osobami, którym ufają, użytkownicy mogą znacznie zmniejszyć ich podatność, a mimo to nadal łączyć się z globalną siecią za pośrednictwem znajomych znajomych i tak dalej na. Umożliwia to ludziom korzystanie z Freenet nawet w miejscach, w których Freenet może być nielegalny, utrudnia rządom jego blokowanie i nie polega na tunelowaniu do „wolnego świata”. Nie jest to tak proste, jak korzystanie z czytnika grup dyskusyjnych dostawcy Usenetu. Nie, proszę pana, Freenet wymaga cierpliwości. Używając Frost lub Fuqid (aplikacje Front End dla głównego programu Freenet), może minąć pół godziny, zanim będzie można „subskrybować” grupy lub pobierać je w taki sam sposób, jak Usenet. Niektóre grupy, takie jak grupa Freenet i inne grupy techniczne, będą natychmiast dostępne, ale z kilkoma wiadomościami. Czas to rozwiąże. Więc trzymaj go w szafie i zapomnij o tym na jeden dzień lub dwa, jeśli planujesz zapisać się do wielu grup. Warto czekać

Frost & Fuqid

Dwa wolne zakończenia, które polecam to: Frost i Fuqid.

Frost widział wiele ulepszeń, ale polecam najpierw wypróbować Fuqid, ponieważ jest to pierwsza zewnętrzna aplikacja dla Freenet, która działa jako menedżer wstawiania / pobierania plików. Fuqid oznacza: Freenet Utility for Queued Inserts and Downloads i działa w systemie Windows lub Linux pod wine. Freesite Fuqid znajduje się na samym Freenet pod adresem:

USK @ LESBxzEDERhGWQHl1t1av7CvZY9SZKGbCnsD7txqX0I, nP0CHuKvlbVzcrnz79TEd22E56IbKj-KHB-W8HHi9dM, AQACAAE / Fuqid / -1 /

Będziesz musiał wkleić powyższe do przedniego panelu kontrolnego Freenet, gdzie jest napisane "Klucz". Jeśli system jest nowy, może to potrwać kilka minut. Po zainstalowaniu kliknij prawym przyciskiem myszy lewą stronę z listą tablic i wybierz „Dodaj nową tablicę”. Dla nazwy wpisanej w "fuqid-announce" bez cudzysłowów. Na liście tablic znajdziesz teraz nową tablicę o nazwie „fuqid-

announce". Kliknij prawym przyciskiem myszy tę tablicę i wybierz „Konfiguruj wybraną tablicę". Spowoduje to wyświetlenie nowego okna. W tym oknie kliknij „Zabezpiecz tablicę", aby zmienić tablicę z tablicy publicznej. Teraz w sekcji „Klucz publiczny" wklej klucz poniższy :

SSK @ qoYE5SKRu66pmKH64xa ~ R ~ w3hXmS5ZNtqnpEGoCVww, HTVcdWChaaebfRAublHSxBSRaRFG91qCwsa3mGF3-QE, AQACAAE

Teraz masz tablicę ogłoszeń dla Fuqid dodaną do twoich tablic Frost. Najnowsze wydania Fuqid zostaną opublikowane na tej tablicy wraz z tablicą fuqid na FMS. Pytania? Skieruj ich do płyty Frost lub FMS o nazwie Fuqid.

Hasła

Dobre, mocne hasła są jak para Rottweilerów śpiąca w Twojej jaskini. Większość intruzów odejdzie, gdy zacznie się chaos. Słabe hasła są jak posiadanie Golden Retrievera. Miły, przyjazny i łatwy do zaufania w stosunku do dzieciaków, ale może po prostu wydać z siebie szczekanie o 3 nad ranem, kiedy nadejdzie intruz. Wtedy schowa się pod stolikiem (pies, nie intruz). Od lat słyszałem, że nigdy nie należy używać jako hasła niczego osobistego. Obejmuje to nazwiska rodowe. Ulubione książki. Kino. Więc jakie jest rozwiązanie? Zremiksuj swoje hasła jednym lub dwoma symbolami. Jeśli uważasz, że haker nie będzie w stanie odgadnąć nazwy kombinacji szafki Twojej dziewczyny, to się mylisz. Łatwo jest zgadnąć, nawet jeśli trochę go pomieszasz. Komputery oddane tej praktyce mogą odgadnąć wiele w mniej niż nanosekundę. Ale jak pamiętasz hasło do strony używanej przez Tora, która ma symbole?

- Łatwo. Użyj hasła, które jest łatwe do przywołania tylko dla Ciebie. Najpierw zapisz pierwszą literę każdego słowa, nie uwzględniając wielkości liter i pozycji. Wstaw tam symbole. Na przykład: W zeszłą niedzielę żona kupiła mi zegarek Rolex i był za brzydki.

Co po zmianiet:

LS, twbmarwaiw2u

Powyższe hasło jest trudne do odgadnięcia dla hakera, ale dla Ciebie łatwe, pamiętaj ... zakładając, że jesteś dobry w zastępowaniu.

Zmiana haseł

Pod warunkiem, że postępowałeś zgodnie z powyższym co do joty, nie powinieneś tego robić, wymieniaj hasła co 90 dni. Jestem pewien, że słyszałeś z obu stron alejki ich wypowiedzi na ten temat, ale uważam, że badania dowiodły, że trzymanie silnego hasła (chyba że dowód kompromisu) jest bezpiecznym zakładem. Artykuł badawczy ACM / CCS 2010: „The Security of Modern. Wygaśnięcie hasła: struktura algorytmiczna i analiza empiryczna" ,autorstwa Yinqiana Zhanga, Fabiana Monrose i Michaela Reitera . Doszli do wniosku, że zmiana haseł co kilka miesięcy nie zwiększa, powtarzam, NIE zwiększa bezpieczeństwa: co najmniej 41% haseł można złamać offline poprzednie hasła do tych samych kont w ciągu kilku sekund, a pięć zgadywanych haseł online w oczekiwaniu wystarczy, aby złamać 17% kont.

... nasze dowody sugerują, że może być właściwe całkowite zniesienie wygaśnięcia hasła, być może jako ustępstwo, wymagając od użytkowników podjęcia wysiłku w celu wybrania znacznie silniejszego hasła niż w innym przypadku (np. znacznie dłuższego hasła). .... Uważamy, że w dłuższej perspektywie nasze badanie potwierdza ten wniosek proste uwierzytelnianie za pomocą hasła powinno zostać całkowicie odrzucone."

Przechowywanie haseł w przeglądarce Tor

Być może zauważyłeś, że opcja „Zapamiętaj hasło” w Tor

Przeglądarka nie jest dostępna, a przynajmniej tak się wydaje. Ale jeśli spojrzysz na ustawienie prywatności i zmienisz ustawienia historii na „zapamiętaj historię” i „zapamiętaj hasła do witryn”, nie będzie już wyszarzone.

Diceware

Jeśli musisz przechowywać hasła, dobrą opcją dla unikalnego, losowego jest Diceware (są też inne), gdzie możesz uzyskać datę wygaśnięcia dowolnego hasła miesiące od daty utworzenia. Możesz skopiować dowolne hasło do pliku tekstowego, a następnie zaszyfrować je i wysłać do siebie lub umieścić na wymiennym (zaszyfrowanym) dysku lub pamięci USB. Pamiętaj: Tor nie robi nic, aby poprawić bezpieczeństwo Twojego * systemu * przed codziennymi atakami. Poprawia tylko bezpieczeństwo online, a nawet wtedy, gdy jest używany odpowiedzialnie. Tor nie ma pojęcia, czy twoja wersja systemu Windows nie jest poprawiona

i zainfekowany ładunkiem złośliwego oprogramowania typu zero-day, który zainfekował go keyloggerem. Jednym ze sposobów, w jaki haker może odgadnąć twoje złożone hasło, jest powiązanie korzystania z Tora z korzystaniem z niego bez Tora i złamanie zabezpieczeń haseł z witryny innej niż Tor. Dlatego nigdy nie powinieneś używać tych samych nazw użytkownika / haseł dla Tora, co w przypadku aktywności poza Torem.

Zapobieganie powiązaniu aktywności spoza Tor z aktywnością Tora

Przeglądanie różnych stron internetowych jednocześnie i zachowanie anonimowości jest ryzykowne, ponieważ Tor może wysyłać żądania do każdej witryny w tym samym obwodzie, a węzeł wyjściowy może zobaczyć korelację. Lepiej jest przeglądać jedną witrynę na raz, a następnie wybrać „Nowa tożsamość” z przycisku Tor. Żadne poprzednie obwody nie są używane w nowej sesji. Ponadto, jeśli chcesz odizolować dwie różne aplikacje (zezwolić na odizolowanie akcji wykonywanych przez jedną aplikację od działań innej), możesz pozwolić im na używanie tego samego portu SOCKS, ale zmienić użytkownika / przepustkę. Inną opcją jest ustawienie „flagi izolacji” dla portu SOCKS. Podręcznik Tora zawiera sugestie, ale doprowadzi to do niższej wydajności w porównaniu z Tor. Osobiście lubię korzystać z Whonix. Dwie instancje, dwie maszyny wirtualne. Jeden z nich obsługuje Tor, a drugi Tor Firefox.

Keyloggery

Możesz się zastanawiać, co keylogger ma wspólnego z Torem. A jeśli o to chodzi, czym w ogóle jest keylogger. Nie jesteś sam. W rzeczywistości byłbyś zaskoczony, jak wiele osób nie wie i jest zszokowanych, ilu techników uważa je za nieistotne. W 2010 roku spotkałem starego przyjaciela z dzieciństwa, którego nie widziałem od ponad dziesięciu lat. Był teraz agentem rządowym. Byłem zaskoczony i (fałszywie) założyłem, że jego obszerne szkolenie oznaczało, że wiedział tyle samo co agenci służb specjalnych, jeśli chodzi o bezpieczeństwo komputerów. Błąd. Odpowiedział na post, który opublikowałem na Facebooku, dotyczący grupy hakerskiej „Anonymous”. „Co to jest keylogger?” zapytał. Czekałem, aż ktoś inny odpowie. Nikt tego nie zrobił, powiedziałem mu. Wydawał się zdumiony, oniemiały, jakby to było coś, co dopiero niedawno zerwało się ze smyczy w sieci. Następnie powiedziałem mu, że były w pobliżu od dawna. Ale (westchnij), jest wiele nieporozumień co do tego, co dokładnie robią. Niektórzy nazywają je oprogramowaniem szpiegującym. Inni mówią, że są trojanami. Jeszcze inni, exploitami. Szczerze mówiąc, są po trochu wszystkim. To oprogramowanie monitorujące, które śledzi i rejestruje każde kliknięcie, każdą odwiedzoną witrynę internetową, każde

naciśnięcie klawisza. Czaty, Skype, e-maile. Jeśli możesz to wpisać, może to nagrać i wszystko pod twoim nosem. Może nawet wysłać e-mailem to, co piszesz, do odbiorcy na drugim końcu świata. Numery CC, hasła i dane logowania Paypal to tylko krótka lista celów, które może uzyskać. Jak więc można się zarazić?

- Otwieranie załącznika wiadomości e-mail

- Uruchomienie pliku .exe z sieci P2P od niezaufanego użytkownika

- Dostęp do zainfekowanej witryny internetowej za pomocą nieaktualnej przeglądarki

- NSA, jeśli mogą natłuścić prawe dłonie

Niektórzy pracodawcy używają ich do śledzenia produktywności pracowników. Niektóre żony podłączają jeden przez USB (wersja sprzętowa), aby zobaczyć, z kim ich mężowie rozmawiają wieczorem przed pójściem spać. Rodzice używają ich na komputerze dziecka. Więc to nie jest tak, że są w 100% złośliwe przez cały czas. Ale są diabelsko trudne do wykrycia. Dzierżą niemal wampiryczną postać, ale podobnie jak wampiry istnieją subtelne znaki, które można odczytać bez wyciągania drewnianego kołka.

Znaki wampirów

- Powolna prędkość przeglądania

- Myszka zatrzymuje się / wstrzymanie naciśnięć klawiszy w dokumencie tekstowym

- Litery nie pasują do tego, co wpisujesz

- Błędy na wielu stronach internetowych podczas ładowania ciężkiego tekstu / grafiki

Istnieją dwa rodzaje:

Keyloggery programowe

Ten typ ukrywa się w systemie operacyjnym. Czają się w Windows. W Linux, nie tak bardzo. Keylogger rejestruje naciśnięcia klawiszy i wysyła je do hakera lub innego łotra o określonych porach, pod warunkiem, że komputer jest w trybie online. Zamaskowany, większość użytkowników nigdy nie zobaczy, jak działa jego mroczna sztuka. Wielu popularnych dostawców oprogramowania antywirusowego ma problemy z jego identyfikacją, ponieważ definicje zmieniają się tak często.

Sprzętowe keyloggery

Bond mógł użyć jednego z nich. Będąc sprzętem, jest fizycznym rozszerzeniem, które można podłączyć do dowolnego portu USB w komputerze i można je kupić online przez podejrzanych małżonków lub dzieci, które chcą uzyskać dostęp do magazynu porno ich taty. Naciśnięcia klawiszy są rejestrowane w pamięci RAM. Nie jest wymagana instalacja. Tak więc, jeśli nie jesteś typem, który codziennie sprawdza wnętrze swojego komputera, możesz go nie zauważyć, dopóki nie będzie za późno. Można je również wbudować bezpośrednio w klawiaturę. FBI uwielbia wymieniać cel za pomocą specjalnie zbudowanego urządzenia monitorującego. To prawda, dotyczy to głównie celów o dużej wartości, takich jak mafia, ale są one dostępne dla każdego.

Dla dzieci...

Ci, którzy je sprzedają, zwykle robią to pod pozorem ochrony domeny dzieci. Wiesz, pilnuj ich przez cały czas, tak jak powinna to robić mama. Problem w tym, że to, co jest dobre dla gęsi, nie jest dobre dla gąsiora, a to zwykle wiąże się z podaniem pomocnej dłoni przez Wielkiego Brata. I nie tylko on.

Uwielbiają je złodzieje i hakerzy. Oznacza to, że musisz być jeszcze bardziej czujny. Jeśli zainstalowany jest keylogger, wszelkie szyfrowanie zostaje pokonane. PGP, Tor, Freenet. Wszystko jest zagrożone i musisz całkowicie wyczyścić dysk twardy i zacząć od nowa, zwracając baczną uwagę na to, czy na jakimkolwiek nośniku znajdują się zainfekowane pliki - aby uniknąć ponownej infekcji po nowej instalacji systemu operacyjnego. Jeśli użyłeś tego samego hasła do wejścia w BIOS, jak cokolwiek innego - forum, strony internetowe, Paypal - musisz je natychmiast zmienić.

Zapobieganie keyloggerom

- Sprawdź klawiaturę pod kątem podejrzanych załączników. Jeśli jesteś pracownikiem firmy X i pewnego ranka przy Twoim biurku pojawi się nowa klawiatura, zachowaj ostrożność, chyba że ufasz swojemu szefowi na 200%.

- Użyj wirtualnej klawiatury. Brak naciśnięć klawiszy = brak logowania!

- Użyj chronionego identyfikatora, aby uniemożliwić hakerom przechwytywanie naciśnięć klawiszy. Działa poprzez zaszyfrowanie wszystkiego, co piszesz, czyniąc wszelkie informacje bezużytecznymi dla hakerów.

- Użyj przyzwoitej zapory ogniowej, aby uniemożliwić keyloggerowi dostarczanie danych. Rok temu mój firewall Comodo ostrzegł mnie o podejrzanej aktywności sieciowej, która wydawała się znikąd, kiedy nie robiłem nic online. Okazuje się, że miałem trojana Win64 / Alureon. Musiałem użyć Malwarebytes, aby go wykryć i usunąć. Norton był bezużyteczny! Wyobraź sobie, że.

Inne anty-keyloggery

Jeśli nie masz nic przeciwko wydaniu monety, jest ich kilka więcej:

Zemana AntiLogger (Darmowy)

Ta „bezpłatna" wersja jest prostym wykrywaczem keyloggerów. W rzeczywistości jest całkiem rozebrany, ale jeśli wszystko, czego potrzebujesz, to ostrzeżenie, może to być dla ciebie. Keylog Guard oferuje szyfrowanie wszystkich rzeczy wpisywanych na klawiaturze. Każdy szpieg dostanie od ciebie tylko zniekształcone litery. Wersja płatna jest nieco droga i kosztuje 29,99 USD i zapewnia dodatkową ochronę przed złośliwym oprogramowaniem i tym podobne, ale jest nieco przesadzona. Ponadto będzie Cię denerwować, jeśli spróbujesz uruchomić coś, czego nie lubi, tak jak każdy inny program antywirusowy.

SpyShelter STOP-LOGGER

Darmowa wersja oferuje więcej niż Zemana, ponieważ możesz przechwytywać zrzuty ekranu. Ostrzeże Cię również o każdym kodzie, który próbuje przesunąć od Ciebie naciśnięcia klawiszy, ale wersja bezpłatna nie jest kompatybilna z 64-bitową. To jest 24,99 USD. Należy jednak pamiętać, że usuwanie keyloggera to paskudna sprawa, ponieważ mają zwyczaj ponownej instalacji. Keyloggery często ukrywają się jako usługa w svchost.exe, więc menedżer zadań nie jest zbyt pomocny bez dedykowanej aplikacji. Optymalnym sposobem zapobiegania jest zatrzymanie ich przed włożeniem.

Bądź proaktywny. Przewiduj złamanie hasła. Pamiętaj, czujność!

Darknet Markets

Niektórzy z was mogą się zastanawiać, jak naprawdę bezpieczny jest Darknet w świetle omawianych luk w zabezpieczeniach. Krótka odpowiedź brzmi: tak bezpiecznie, jak to robisz. Jesteś słabym ogniwem. Ostatnie ogniwo w łańcuchu bezpieczeństwa. I chociaż potrzebujesz Tora, aby uzyskać

dostęp do stron Onion, termin ten może odnosić się do dowolnej anonimowej sieci - sieci, takich jak I2P lub Freenet, lub czegokolwiek innego, co maskuje źródło transmisji danych, a co za tym idzie, Twoją tożsamość.

Co prowadzi nas do Darknet Marketplace.

Pełna lista takich rynków w głębokiej sieci jest duża, a ryzyko oszustwa jest dość wysokie. To jeden z powodów, dla których być może o nich nie słyszałeś. Często są szybko niszczeni przez jadowitą reputację lub krach organów ścigania. Czasami wkurzają niewłaściwe osoby, a następnie spamerzy atakują witrynę. Ale jest wiele miejsc, do których można się udać, jeśli jesteś ciekawy, co jest sprzedawane przez kogo. Kiedy mówię o sprzedaży, mam na myśli to, że ... Cokolwiek chcesz, czego nie można uzyskać zwykłymi legalnymi kanałami. I pamiętaj, że to, co jest legalne w jednym kraju, może być nielegalne w innym. W Kanadzie komiksy Lolicon są nielegalne i mogą wpędzić Cię w poważne kłopoty, jeśli przekroczysz granicę. Ale nie w Ameryce. W USA możesz napisać dowolną historię. W Kanadzie? Historie TEXT dotyczące nieletnich są verboten. Inną różnicą jest to, że istnieją siatki bezpieczeństwa przy zakupie prawie wszystkiego w pierwszym kraju świata na otwartym rynku. Myśl najlepiej, kup. Sklepy Mom i Pop. Kwiaciarnie. Co się stanie, jeśli klienci zostaną kontuzjowani? Klienci pozywają za pośrednictwem prawnej sieci bezpieczeństwa i pozwalają zarabiać wielu prawników dużo pieniędzy. Ale Darknet Marketplace śmieje się z takich siatek bezpieczeństwa. W rzeczywistości prawdopodobnie zostaniesz oszukany co najmniej kilka razy, zanim znajdziesz renomowanego sprzedawcę wszelkich towarów, których szukasz. I naprawdę nie ma znaczenia, co to jest - urządzenia teleportacyjne? Zwierzęta? Egzotyczne drzewa? To wszystko dzieje się tak samo. Cokolwiek jest poszukiwane, przyciągnie niesmaczne typy i to nie tylko ze strony kupującego. Dlatego badaj dowolny rynek Darknet za pomocą Tora, uważnie odwiedzając fora i sprawdzaj zaktualizowane informacje, aby zobaczyć, czy jakiekolwiek witryny zostały oznaczone jako podejrzane lub przejęte. Kilka innych porad:

- Zawsze używaj PGP do komunikacji.

- Nigdy nie przechowuj kryptowaluty na żadnym takim rynku.

- Załóż jaskinię złodziei, chyba że * oni * udowodnią inaczej. Odpowiedzialność spoczywa na nich, tak jak w trybie offline, aby udowodnić, że są uczciwym biznesem Jeśli otworzysz własną pamiętaj o tym: klienci nie są ci winni nic. Możesz ich zdradzić tylko raz. A teraz kilka przykładów phisherów i oszustów oraz innych oszustów. Poznacie ich po ich owocach.

1.) Silk Road 2.0 (e5wvymnx6bx5euvy ...) Wiele oszustw z tym związanych.

Podobnie jak w przypadku e-maili na Facebooku i Google, czasami fałszywy adres można rozpoznać po adresie. Wklej kilka pierwszych liter do skrótu obok nazwy. Jeśli nie pasuje, omiń.

2.) Licznik zielonych banknotów (67yjqewxrd2ewbtp ...)

Obiecali swoim klientom fałszywe pieniądze, ale odmówili depozytu. Martwa gratka.

3.) iPhone'y za pół ceny: (iphoneavzhwkqmap ...)

Oto doskonały przykład oszustwa. Każda witryna, która sprzedaje elektroniczne gadżety w głębokiej sieci jest gotowa do oszukiwania klientów. Podczas gdy na Dalekim Wschodzie dostaniesz podrabiane telefony z tanimi chińskimi częściami, które psują się w ciągu miesiąca, w Deep Web po prostu wezmą twoje pieniądze i powiedzą adios. Właściwie nawet nie zawracają sobie głowy mówieniem tego. Jak więc rozpoznać oszustwo?

Ponieważ wielu nowych sprzedawców darknetu powstanie z niczego, z rzadkimi produktami, które sprawią, że klienci zemdleją i wyślą im pieniądze ... bez szukania ich nazwiska lub wcześniejszej sprzedaży. Prawdziwa operacja typu hit and run. Uderz szybko , szybko i nieczysto Uwiedź jak najwięcej, zanim stado złapie wilka w przebraniu. Wielu jest oszołomionych, myśląc „to tylko trochę pieniędzy", ale trochę pieniędzy od wielu użytkowników Tora może znacznie zachęcić innych oszustów do założenia sklepu. Kiedy pytasz ich, dlaczego nie oferują usługi Escrow, odpowiadają: „Uważamy, że to niewiarygodne / podejrzane / niestabilne" wśród innych wymówek BS. Lepiej jest trzymać się swojej drobnej zmiany, niż zostawiać ślad do swojej skrzyni ze skarbami. I nie ma wątpliwości, że niektórzy z tych oszustów są jak ogary, jeśli chodzi o kradzież tożsamości.

- Zrób swoje badania! Sprawdź fora, a zwłaszcza daty recenzji jakie oni mają. Czy zauważasz wzory? Czy dobre recenzje są rozproszone przez długi czas, czy raczej nagle - tak jak robią to niektórzy marketerzy stowarzyszeni z Amazon z płatnymi recenzjami, które świecą? Niewiele recenzji od wspomnianych klientów?

Jeśli widziałeś film „Gorączka" z Alem Pacino i Robertem de Niro, wiesz, kiedy nadszedł czas na Walk Away. W środku nocnego napadu Niro wychodzi na papierosa. Słyszy odległy kaszel. Teraz jest środek nocy w niezamieszkanej części miasta, która pochodzi z drugiej strony ulicy - parking pełen czegoś, co uważał za puste przyczepy. Hmm, myśli. Nie taki pusty (to był policjant). Wraca do banku i przerywa. Drugim aspektem jest czas. Niektóre fałszywe strony ustawiają krótki czas wysyłki i liczą, że nie będziesz się przejmować, aby sprzedaż była sfinalizowana, zanim będziesz mógł wygwizdać Dixie z tyłka. Po sfinalizowaniu masz spieprzone, ponieważ pieniądze są w ich portfelu, zanim będziesz mógł nawet złożyć protest.

Zapobieganie oszustwom

Jednym z nich jest Google, wierz lub nie, pod adresem http://www.google.com/imghp. Serwisy randkowe, takie jak Cherry Blossoms i Cupid, czasami używają wyszukiwania wstecznego obrazu, aby złapać oszustów i nigeryjskich oszustów udających biednych samotnych singli, aby pozbawić ludzi ich monet. Jeśli oni mogą je złapać, ty też możesz. Jeśli obraz należy do innej legalnej witryny, prawdopodobnie jest fałszywy. Foto Forensics również robi to samo i raportuje metadane, dzięki czemu jeszcze trudniej jest uciec od sztuczek Photoshopa.

Kiedy jest w porządku do FE (sfinalizuj wcześniej)

FE oznacza „Sfinalizuj wcześniej". Jego użycie w Internecie zwykle można znaleźć w kolorze czarnym targowiska, takie jak Silk Road i Sheep's Marketplace. Oznacza to po prostu, że pieniądze na rachunku escrow są uwalniane przed otrzymaniem produktu. Każdy klient, z którym kiedykolwiek rozmawiałem, odradza to, chyba że masz duże doświadczenie w tej branży. Buuu ... Wielu dostawców stosuje obecnie standardową praktykę wpłacania środków z góry, zanim będziesz miał cokolwiek w swoich rękach. Na więcej niż jednym forum w Marketplace była gorąca wymiana zdań na temat tego, kiedy jest to właściwe. Możesz usłyszeć: „Czy ten facet jest legalny? A co z tym chińskim strojem tutaj? Wydaje się podejrzany", a inni: „Znajomy powiedział ten facet jest w porządku, ale potem zostałem oszukany! ". Masz pomysł.

Oto moje doświadczenie w tej sprawie.

1.) Jest w porządku, gdy dostajesz to, za co zapłaciłeś.

Może się to wydawać odwrotne do zamierzonych, ale pomyśl, ilu graczy wchodzi do kasyna w Las Vegas i nigdy nie zadają sobie pytania „Ile mogę stracić?". Niestety, nie ma wielu odpowiedzi. Vegas nie

zostało zbudowane na plecach przegranych. Niektórzy kupcy w ogóle nie lubią escrow. Niektórzy. Więc nie wydawaj więcej, niż możesz stracić. Spójrz na to, jak hazardzista patrzy na zarabianie pieniędzy.

2.) Jest w porządku, jeśli masz gwarancję wysyłki.

Istnieją oszuści FE, którzy obdarzają Cię anielskim uśmiechem i kłamią prosto w oczy, gdy cię oszukują. Nie polegaj wyłącznie na recenzjach. Facet na SR może być najlepszym kupcem po tej stronie Tatooine, a jednak pewnego dnia obudzisz się i zostaniesz okradziony. Został podzielony z milionem w BTC, a ty nie masz nawet torby. Większość ci tego nie zrobi. Ale kilku będzie.

Kiedy NIE jest w porządku do FE

- Utrata środków spowoduje eksmisję lub zerwanie związku. Nigdy nie pożyczaj pieniędzy od przyjaciół, a zwłaszcza od rodziny, chyba że chcesz, aby wspomniana rodzina przyszła po ciebie z toporem o podwójnym ostrzu. Jeśli zostaniesz oszukany, stracisz nie tylko pieniądze, ale także szacunek i zaufanie swojej rodziny. Słowo się rozprzestrzenia. Nie spłacasz swoich długów. Co to za powiedzenie w Game of Thrones? Dobrze. Lannister zawsze spłaca swoje długi. Ty też powinieneś.

MultiSigna

Oto, co się dzieje: po zatwierdzeniu zakupu sprzedawca wpłaca pieniądze (w tym przypadku Bitcoiny) na adres z wieloma podpisami. Następnie klient otrzymuje powiadomienie o dokonaniu transakcji ($, €) na konto sprzedawcy. Następnie, gdy sprzedawca poinformuje MultiSigna, że transakcja się powiodła, MultiSigna tworzy transakcję z adresu z wieloma podpisami, która wymaga zarówno od kupującego, jak i sprzedającego, aby mogła zostać wysłana do sieci. Kupujący otrzymuje Bitcoiny i kończy sprzedaż. Zdezorientowany jeszcze? Na początku też byłem. Przyzwyczaisz się.

Krytyczne:

MultiSigna istnieje tylko jako weryfikator / współsygner całej transakcji. W przypadku braku porozumienia między sprzedającym a kupującym wymiana nie następuje. Pamiętasz scenę z Gier Wojennych, kiedy dwóch operatorów silosów jądrowych musi jednocześnie przekręcić klucze, aby wystrzelić? Tak to.

MultiSigna będzie oczywiście faworyzować jedno lub drugie, ale nie oba, jeśli nie mogą się wzajemnie uzgodnić. Plusem jest to, że jeśli rynek lub nabywca lub sprzedawca straci klucz, dwa z trzech nadal są dostępne. Pojedynczy klucz nie może wydawać pieniędzy w 2/3 adresie MultiSig.

Czy to jest bezpieczne? Czy to tajemnica?

Nie polecam ustanowienia wymiany miliona dolarów na jacht, a nawet tysiąca dolarów, ponieważ oba niosą ze sobą ryzyko, ale ostatecznie to zależy od Ciebie. Pamiętaj tylko, że zaufanie jest zawsze problemem w darknetach i generalnie bezpieczniej jest wykonywać kilka przelewów ze sprzedawcą / kupującym, który ma dobrą historię płatności. Innymi słowy, reputacja, jak zawsze, jest wszystkim. Niestety, jest kilka godnych zaufania rynków, które mają dobrą historię robienia rzeczy właściwie, dzięki niebiosom. Blackbank jest jeden. Agora jest inna. Spójrz na stronę Multi-Sig Escrow Onion tutaj z Tor: http://u5z75duioy7kpwun.onion/wiki/index.php/Multi-Sig_Escrow

Bezpieczeństwo

A więc teraz. Możesz się zastanawiać, jaki byłby efekt, gdyby haker uzyskał dostęp do serwera. Jakie psoty mógłby wyrządzić? Jaki chaos mógłby wywołać, gdyby potrafił naśladować wypłatę w taki sam sposób, jak robi to serwer?

Cóż, wygląda to tak: gdyby haker uzyskał dostęp i spróbował wypłacić pieniądze, zostałby zastosowany pojedynczy podpis i przekazany do drugiego sygnatariusza w celu złożenia podpisu. Wtedy protokół bezpieczeństwa włączyłby się tam, gdzie te zasady byłyby egzekwowane:

1.) Limity stawek: spada tempo kradzieży środków

2.) Oddzwanianie do serwera wydawcy: Usługa podpisywania weryfikuje z pierwotnym wydawcą, że zainicjował on i zamierzał dokonać wydatku. Wywołanie zwrotne mogłoby trafić do oddzielnej maszyny, która mogłaby zawierać tylko dostęp do odizolowanych zatwierdzonych informacji o wycofaniu.

3.) Ograniczanie adresów IP: Usługa podpisywania podpisuje tylko transakcje pochodzące z określonej listy adresów IP, zapobiegając przypadkowi, w którym haker lub osoba poufna ukradła klucz prywatny.

4.) Białe listy miejsc docelowych: Niektóre portfele o bardzo wysokim poziomie bezpieczeństwa można ustawić w taki sposób, że usługa podpisywania będzie akceptować tylko wtedy, gdy miejsce docelowe będzie znane wcześniej. Haker musiałby złamać zabezpieczenia zarówno pierwotnego serwera wysyłającego, jak i usługi podpisywania.

Powtórzę, że MultiSigna nigdy nie jest w posiadaniu Twoich bitcoinów. Do podpisania transakcji używają 2 z 3 podpisów (sprzedający, kupujący i MultiSigma). Zwykłe transakcje są podpisywane przez sprzedającego, a następnie przez kupującego.

Kroki kupującego dotyczące usługi MultiSig Escrow

1.) Wpłać swoje Bitcoiny. Możliwość zakupu jest przyznawana po 6 potwierdzeniach

2.) Stwórz klucz prywatny i publiczny (Brainwallet.org jest generatorem adresów Bitcoin po stronie klienta JavaScript)

3.) Kup przedmiot, wprowadź klucz publiczny i adres BTC do zwrotu pieniędzy (łaska na szczęście!)

4.) Odzyskaj zakupiony przedmiot

5.) Wprowadź klucz prywatny i zamknij

Poniżej znajduje się lista giełd obsługujących Multisig:

Bitstamp - usługa Multisig: https://www.bitgo.com

Rock Trading - usługa Multisig: https://greenaddress.it

TeraExchange - usługa Multisig: https://www.bitgo.com

BitQuick - usługa Multisig: https://www.bitgo.com

Jest też ta lista potworów:

http://bitcoinx.io/exchanges

Długie ramię prawa

Czy prawo może kraść fundusze?

- Zakładając, że masz na myśli prawo USA, nie ... ponieważ portfel nie zawiera pieniędzy. Blockchain Bitcoin zapobiega temu. Hakerzy również nie mogą go ukraść, ponieważ wymagane są dwa klucze

prywatne i będą musieli ukraść 2 z 3 posiadaczy kluczy prywatnych ... mało prawdopodobne. A co z bezpieczeństwem korzystania z klucza prywatnego?

- Nigdy nie używaj nieodpowiedzialnie klucza prywatnego z portfela Bitcoin. Zamiast tego utwórz nowy. Daj mu taką samą miłość, jaką dajesz swoim kluczom głównym Truecrypt / DiskDecryptor. Wiele, wiele szczególnej miłości, której nikt inny nie otrzymuje.

Brzmi to bardzo ryzykownie. Czy nie zostanę złapany?

Oto, jak większość ludzi zostaje złapanych i naprawdę nie ma znaczenia, co to jest. Możesz handlować nielegalnymi Furbies (wierz lub nie, w 1999 roku NSA uważała, że te zabawki mogą być w stanie rejestrować wysoce tajne informacje). Większość dealerów zostaje zatrzymanych, popełniając zwykłe błędy:

- Przechwałki w barze

- Przekazywanie zbyt dużej ilości danych osobowych nieznajomym (patrz Ross Ulbricht)

- Sprzedawanie kontrabandy tajnym organom ścigania

- Zniżki

- Popełnianie przestępstw pod nadzorem

- Zarządzanie operacją, która rośnie skokowo (z mnóstwem początkujących popełniających błędy).

Jak daleko posunie się policja, żeby cię złapać? To dobre pytanie. Odpowiedź jest całkiem prosta: o ile pozwalają na to zasoby. Jeśli chcą cię wystarczająco mocno, ale brakuje im funduszy, zwiększą zagrożenie, jakie przedstawiasz mediom, kościołom i synagogom, i wzywają wszystkich błagających o pieniądze, żeby cię złapać, ty przeklęta brudna małpa! Żartuję. Prawdopodobnie nie będzie gorzej niż to, co wycierpiał Charleton Heston, gdy był związany i ciągnięty po mieście małp. Niektóre małpy są gorsze od innych… zwykle małpy wojskowe. Ale tak naprawdę wszystko sprowadza się do tego, że cokolwiek robisz i jeśli jest to nielegalne, w tym Furbies. Naprawdę nie obchodziło ich, co to jest, jeśli tylko umieszcza w wydziale krzykliwe nagłówki. Błyskotliwe nagłówki oznaczają większe fundusze. Więcej funduszy = wyższe pensje. Większe pistolety. Jeśli nie broń, to zbroja. Przykład: w 2010 r. Policja w Los Angeles zorganizowała fałszywy program loterii, aby zwabić osoby z zaległymi nakazami. Nie żartuję, sami nie wpadli na ten pomysł, a raczej wzięli go od The Simpsons. Wysłali blisko tysiąc fałszywych listów pod nazwą grupy marketingowej tylko po to, by nieco ponad pół tuzina pojawiło się w La Mirada Inn po darmową nagrodę: BMW 238. Fajnie, co? Tylko żartowali z nich, gdy ich uśmiechy się rozpłynęły po usłyszeniu tych czterech brudnych słów: „Wszyscy jesteście aresztowani!”. Biedni ludzie przynieśli nawet dowód tożsamości, aby zweryfikować ich tożsamość. Głupi. Równie dobrze mogli sami klepnąć kajdanki. A jeśli chcą przejść przez te wszystkie kłopoty tylko za kilka wykroczeń, wyobraź sobie, co oni, wraz z NSA, zrobią z grupą użytkowników Tora sprzedających Furbies!

A to jest przykład offline. Wyobraź sobie, co może zrobić jeden dział, okłamując samego usługodawcę internetowego lub wyszukiwarkę. Groźby grzywien. Warranty. Zła reputacja. Wezwania użytkowników. Zła reputacja, z której prawdopodobnie nie odzyskają szybko. Szczególnie policjanci w Vegas uwielbiają bawić się w ten sposób, pogłębiając stare prawa, aby zapewnić każdemu członkowi tej operacji Ferbie. W 2013 roku agent Secret Service aresztował kilku online, sprzedając im fałszywe identyfikatory. Kopacz? Wszyscy zostali oskarżeni na mocy ustawy RICO z 1970 roku. Pierwotnie stworzona w celu odstraszania gangsterów, pozwala im łapać całe grupy i oskarżać każdą osobę, jakby popełnił tę samą zbrodnię, którą popełnili wszyscy inni w grupie ... bez względu na rolę. Tłumaczenie: Kurier jest traktowany tak samo, jak przywódca, podobnie jak kupujący. Indywidualnie, niewiele czasu

w więzieniu w wielkim schemacie w 1970 roku, ale zostałeś oskarżony jako GRUPA? Co najmniej dwadzieścia lat. Al Capone nigdy nie widział tak mocnego wyroku. Dla prokuratora po prostu nie ma znaczenia, czy Twój system operacyjny jest zaszyfrowany i nie może uzyskać danych. Wszystko, czego potrzebują, to udowodnić, że byłeś częścią przedsiębiorstwa. Można to zrobić poza nowym błyszczącym dyskiem twardym Western Digital, kierując wezwanie do usługodawcy internetowego i kilka innych usług, które subskrybujesz. Zrobili to (i odnieśli sukces) z biustem porno grupy dyskusyjnej lata temu, w którym każdy członek tej ohydnej grupy pedo miał szyfrowanie Tutaj, według „Grugqa" na Github, była krótka lista reguł w tej grupie.

- Nigdy nie ujawniaj prawdziwej tożsamości innemu członkowi grupy

- Nigdy nie komunikuj się z członkiem grupy poza usenetem

- Członkostwo w grupie pozostaje ściśle związane z Internetem

- Żaden członek nie może jednoznacznie zidentyfikować innego

- Członkowie nie ujawniają danych osobowych

- Podstawowa grupa dyskusyjna ds. Komunikacji jest regularnie migrowana

- Jeśli członek złamie regułę bezpieczeństwa / nie zaszyfruje wiadomości = BAN

- Okresowo zmniejszaj szansę na wykrycie przez organy ścigania każdej migracji grupy dyskusyjnej poprzez:

- Tworzenie nowej pary kluczy PGP, odłączanie od poprzednich wiadomości

- Każdy członek tworzy nowy pseudonim

- Motyw pseudonimu wybrany przez Yardbird (lider grupy)

Oświadczenia brzmią jak lista zasad Hell's Angels. I chociaż nie zgadzam się z jego (właścicielem strony internetowej, a nie Yardbirdem) konkluzją, że „w zasadzie nie ma miłych ludzi, którzy przedstawiliby studia przypadków praktyk OPSEC", uważam, że wiele można się nauczyć studiując nawyki przestrzegających prawa obywateli i przestępców , zwłaszcza biorąc pod uwagę szeroką sieć, w ramach której NSA przerzuca na przestrzegających prawa obywateli. Pamiętajcie, że w nazistowskich Niemczech zniesławienie SS było karane śmiercią. Film „Sophie Scholl" jest doskonałym przykładem podziemnego ruchu oporu nie bez powodu. Zdobył uznanie za realistyczny portret kobiety z college'u, która przeciwstawiła się elicie SS i została za to ścięta. Korea Północna, 2015 ... to samo. Mieliby małe problemy z radzeniem sobie gorzej. Ścięcie może być dla nich prawie zbyt łagodne, ponieważ wolą długie, kręte otoczenie dla swoich poddanych. Chiny? Chiny zrobiły kilka dziwnych rzeczy, na przykład zakazanie rozbierania się na pogrzebach i zakazanie transakcji Bitcoin. Przypominam sobie gwałtowne protesty muzułmanów w 2010 roku i myślę: „Ci komunistyczni głupcy złapią wszystkich tych wrzeszczących głupców i strzelą do nich o świcie, nie oglądając się za siebie! "Moja chińska dziewczyna pochyliła się do mnie, kiedy patrzyliśmy i wymamrotała:„ Nie będą czekać do świtu ".

Lubię myśleć o Darkcoinie jako o mądrzejszym bracie Bitcoina. O wiele mądrzejszy i mroczniejszy. Najlepsze jest oczywiście to, że stale się rozwija. Podobnie jak Bitcoin, są to cyfrowe pieniądze zorientowane na prywatność, oparte na projekcie Bitcoin. To projekt, który pozwala na anonimowość podczas codziennych zakupów, no cóż, prawie wszystkiego, o ile oferuje to sklep cyfrowy. Dzięki Bitcoin każdy może zobaczyć, kto dokonał zakupu, patrząc tylko na publiczny łańcuch bloków. To, co robi Darkcoin, to dalsza anonimizacja transakcji za pomocą węzłów głównych - zdecentralizowanej sieci serwerów, które negują wszelkie wymagania stron trzecich: strony, które mogą oszukać Cię z Twoich

monet. Chociaż korzysta z niej niewiele punktów sprzedaży, jest to jedna z najszybciej rozwijających się walut cyfrowych, której gospodarka przekracza dwadzieścia milionów. Imponujący. I to nie wszystko. Jego funkcja „Darksend" jest dość fascynująca - zwiększa prywatność poprzez złożenie typowej transakcji z dwoma innymi użytkownikami. Nie trzeba dodawać, że jest to niezwykle atrakcyjne dla wielu użytkowników Tora, którzy cenią sobie wysoką anonimowość. Sygnaliści, dziennikarze, podziemne ruchy polityczne. To dobra lista. Jednak zła lista, no cóż, nigdy nie można mieć dobra bez zła: terrorystów. Zabójcy kontraktowi. Uchodźcy podatkowi. Gracze Fallouta z atutem zabijania dzieci.

Słyszę te same argumenty przeciwko jego użyciu, które słyszałem w przypadku Freenet: źli ludzie chcą uniknąć wykrycia. Źli handlują Darkcoinami. Używasz Darkcoins. Dlatego jesteś złym facetem. Latarki, widły i czarne koty katapultowały się nad fosą. Dealerzy heroiny uwielbiają używać gotówki, ale nigdy nie słychać w serwisach informacyjnych krzyczących o użytkownikach posiadających tylko gotówkę, którzy nawiązują do takiego przestępstwa. Poza tym najbardziej skorumpowanymi podmiotami zajmującymi się praniem pieniędzy są banki centralne. To one pozwalają państwom pożyczać od przyszłych obywateli na spłatę dzisiejszych długów. Wystarczy spojrzeć na zadłużenie krajowe, aby to zrealizować. Ale to nie znaczy, że Darkcoiny są bezproblemowe. Pojawiło się kilka doskonałych pytań:

- A co jeśli te „Masternody" w końcu utworzą centralizację?

- Co jeśli Darkcoin zostanie porzucony przez twórców, gdy cena spadnie z dachu?

- Kto jest wystarczająco godny zaufania, aby „audytować" Darkcoin? Widzieliśmy audyt z Truecrypt w 2013 roku, który okazał się nie wykazać żadnych backdoorów ... poza tym, że programiści zamknęli go z tajemniczym komunikatem, że Truecrypt nie był już bezpieczny. Możemy cały dzień spierać się, co to oznacza.

Na te pytania można nigdy nie odpowiedzieć. Ale to nie powinno powstrzymać nas przed wytyczeniem nowej granicy w usługach anonimowości.

Korzystanie z Darkcoin dla biznesu

O wiele trudniej jest uruchomić usługę Hidden Tor niż otworzyć firmę za pomocą Darkcoin. To naprawdę jest tak proste, że zdumiewa umysł, co może być dostępne w przyszłości ... i przy minimalnym ryzyku dla Ciebie. Jeśli to do Ciebie przemawia, zdobądź portfel Darkcoin. Służy do wysyłania / odbierania / przechowywania Darkcoin z korzyścią używania Darksend dla 100% anonimowości. Więcej informacji na ten temat tutaj. Większość twoich klientów będzie chciała, żebyś miał portfel, więc lepiej nauczyć się go na początku biznesu niż później.

Wybierz procesor transakcji

Poniżej znajduje się kilka, które możesz zbadać według własnych upodobań. Nie każdy procesor będzie odpowiadał każdemu, tak jak każdy bank lub SKOK nie każdemu przypadnie do gustu. Musisz to ocenić samodzielnie, ważąc swoje potrzeby z ryzykiem, jakie niesie Twoja firma. Wypróbowałem większość z nich i wyszedłem zadowolony, ale jak wszystko inne z kryptowalutą, to, co działa dla mnie, może nie działać dla ciebie.

AltAccept

Opłaty

Transakcja: 0,25% + 0,0005 DRK; Wypłata: 0,01 DRK

CoinPayments

Transakcja: 0,50%; Wypłata: opłata za transakcję sieciową (TX)

CointoPay

Transakcje: 0% (moneta na monetę) 0,5% (moneta na fiat); Wypłata: opłata za transakcję sieciową (TX)

Transakcja: 0,5%; Wypłata: Wliczone z opłatą transakcyjną Niektóre grafiki promocyjne dla Twojej witryny lub cokolwiek innego, czego używasz do reklamowania się swoim klientom - chcesz, aby wiedzieli, że akceptujesz Darkcoiny, prawda? Darkcoin Graphics (dzięki uprzejmości strony głównej Darkcoin) Następnie należy zarejestrować się w katalogu handlowców.

Następnie (opcjonalnie) przeczytaj tutaj InstantX. InstantX to metoda natychmiastowych transakcji potwierdzająca podwójne wydatki za pośrednictwem sieci masternode. Niezupełnie lekkie czytanie, ale im więcej wiesz ...

Dalsze przemyślenia

Żaden pojedynczy podmiot nie ma kontroli nad całym systemem. Chociaż prawdopodobieństwo wypadku graniczy z mało prawdopodobnym prawdopodobieństwem, musisz pamiętać, że Darkcoin jest wciąż w fazie rozwoju iz tego powodu zdarzają się nieprzewidziane rzeczy. Potrzebna jest więc zdrowa dawka należytej staranności. Proponuję kupować tylko za pieniądze, które nie niszczą banku w przypadku pecha. Częste kopie zapasowe są obowiązkowe dla twojego portfela, bardziej niż Bitcoin, ponieważ proces anonimizacji wykonuje więcej transakcji w tle. Jeśli kiedykolwiek korzystałeś z Freenet, wiesz, jak powolna może być sieć i ile często wymaga anonimowości zasobów systemowych. W ten sposób zrób nową kopię zapasową swojego portfela za każdym razem, gdy trafisz w pułap monet.

Darknet OPSEC

„Trzech może dochować tajemnicy, jeśli dwóch z nich nie żyje…”

- Ben Franklin

Powyższy cytat był moim ulubionym cytatem w szkole podstawowej. Wtedy miało to zastosowanie, tak jak teraz, do posiadania bezpiecznego sposobu myślenia, i chłopcze, jak bardzo lubiłem wygłaszać tę kwestię za każdym razem, gdy przyjaciel błagał mnie o potwierdzenie plotek, które słyszał. Plotka, która, gdyby się potwierdziła, mogła wylądować w gorącej wodzie z moim rudowłosym chemikiem. Na szczęście wiedziałem, kiedy zamknąć buzię. Tak jak powinieneś. Trzymanie gęby na kłódkę na temat rynków Darknet jest ważniejsze niż jakikolwiek schemat szyfrowania, którego używasz, hasło, które znasz, klucz grupy Freenet lub cokolwiek związanego z portfelem Bitcoin. Wiedza to potęga. Nie, uderz w to. Wiedza to potencjalna moc. A władza w śliskich rękach może być katastrofalna. Granie w barowego przechwałka może być zabawne po kilku piwach i zdobyć kilka punktów z innymi facetami, ale powoduje to więcej ludzi uwięzionych z błahych powodów niż cokolwiek innego, co przychodzi mi do głowy. I widziałem więcej niż jednego przyjaciela, który spłonął, ponieważ wspomnieli o rynku darknet komuś, komu myśleli, że mogą zaufać. Ale potem ten przyjaciel powiedział komuś, że ufa, bardziej niż komukolwiek innemu na świecie. Zadzwonimy do mojego przyjaciela Grady. Grady powiedział swojej dziewczynie. Nie szczędził szczegółów dotyczących jego operacji Darknet i tego, jak przemierzali kilka kontynentów. Sprawił, że brzmiał jak Agent Smith z Matrixa. Potrząsnąłem głową, słysząc to ...

Cue Fred Sanford: „Ty głupku!” Ufanie jej, że dotrzyma swojego sekretu, było nie tylko głupie, ale także galaktycznie głupie. To jak oczekiwanie, że Ewa sama zje zakazany owoc. I wiemy, jak ta historia się kończy. Niedola naprawdę kocha towarzystwo. Następnie zwrócił uwagę władz w Hongkongu, a

jednym z nich był jej ojciec. Sekret był wystarczająco bezpieczny, jak przypuszczał, dopóki nie odmówił poślubienia swojej hiper-krytycznej dziewczyny, twierdząc, że wziął „czerwoną pigułkę" i obawiał się, że osiedlenie się z ultra-twardą feministką harpią (jego słowa) zabije jego sny. Cóż, to zabiło coś w porządku. Jego wolność. Lekcja? Nie możesz naprawić głupoty, więc dlaczego miałbyś temu ufać? Chociaż nie musisz całkowicie ciemnieć na temat swojej wiedzy na temat Darknet na całą wieczność, w prawdziwych rozmowach, w mediach społecznościowych, Tinderze, Skype itp., Mam to słowo. Powołaj ciszę radiową tam, gdzie ma to zastosowanie lub lepiej, udawaj ignorancję. Jeśli pokażą ci dowód, po prostu powiedz, że masz dobre kontakty. Następnie kup im piwo i wyjdź. Jeśli nadal się upierają, rozważ ostrzeżenie, że zaraz zerwiesz z nimi wszystkie połączenia. Przyjaciele przychodzą i odchodzą, ale wolność jest bezcenna.

Jak skonfigurować usługę ukrytą w Tor

Zaletą korzystania z Tora jest to, że umożliwia on tworzenie usług ukrytych, które będą maskować Twoją tożsamość przed innymi użytkownikami. W rzeczywistości możesz mieć witrynę internetową, której nie można wykryć osobiście, pod warunkiem, że zastosowałeś wszystkie środki ostrożności, aby system był aktualizowany. Oto przykład strony cebulowej dostępnej tylko za pomocą Tora:

http://duskgytldkxiuqc6.onion/

Oczywiście nie możesz uzyskać do tego dostępu za pomocą przeglądarki Firefox bez Tora. Stąd nazwa „ukryta". Dowiesz się, co jest potrzebne do skonfigurowania własnej usługi ukrytej Tora. Nie ma to być wszystko, co obejmuje wszystko i zlewozmywak, ale tylko po to, aby dać ci wyobrażenie o wiedzy technicznej, którą musisz posiadać.

Krok pierwszy: upewnij się, że Tor działa

Postępuj zgodnie ze wskazówkami dotyczącymi instalowania Tora, zabezpieczając go przede wszystkim przed exploitami i lukami w zabezpieczeniach. Wskazówki dotyczące systemu Windows są tutaj, Linux tutaj, a OS X tutaj. Każdy system operacyjny ma swoje własne luki, a najgorszy jest Windows. Zalecam, abyś wybrał Linuksa po opanowaniu podstaw, ponieważ zapewnia on większą kontrolę nad Torem i jest znacznie bardziej odporny na ataki niż Windows. Teraz może być dobry moment na stwierdzenie tego, co oczywiste, coś, z czego prawdopodobnie już zdałeś sobie sprawę, a to jest to: że żaden dwóch ekspertów kontrwywiadu nigdy nie robi tego samego przez cały czas w ten sam sposób. Nie ma czerwonej pigułki, która sprawia, że wszystko jest jasne. Żadnej ściągawki z Magic Opsec Sauce, którą każdy może opanować, jeśli tylko go połknie. Nie możesz zapamiętać wszystkich kombinacji związków organicznych w chemii organicznej. Wierz mi, próbowałem. Było ich o wiele za dużo. Jednak to, co robisz, to zapamiętywanie ogólnych zasad, na podstawie których możesz znaleźć rozwiązanie każdego problemu, który się pojawia. Czasami taka jest anonimowość. Twoje mocne strony nie będą mocnymi stronami twojego sąsiada. Twoje słabości też będą inne. Dostosowujesz się na bieżąco i mogę zagwarantować, że Twoje umiejętności jako hobbystów znacznie przewyższą te, które pracują na państwowym zasiłku.

Krok drugi: instalacja własnego serwera internetowego

Lokalny serwer WWW to pierwsza rzecz, którą musisz skonfigurować. Jest to nieco bardziej zaangażowane, niż pozwala na to miejsce (bez podnoszenia ceny), ale jeśli nie wiesz, co to jest serwer WWW, tutaj znajdziesz prosty przewodnik.

Chcesz również, aby ten lokalny serwer był oddzielony od wszelkich innych instalacji, których potrzebujesz, aby uniknąć zakażenia krzyżowego. W rzeczywistości nie chcesz ŻADNYCH łączy między twoim ukrytym serwerem a codziennym użytkowaniem komputera poza Tor. Twój serwer musi być

ustawiony tak, aby nie zezwalał na wycieki danych, które mogą ujawnić Twoją tożsamość. Więc musisz podłączyć serwer tylko do localhost. Jeśli wymieniasz się tajemnicami handlowymi i nie chcesz, aby szef o tym wiedział, użyj maszyny wirtualnej, aby zapobiec wyciekom DNS i innych danych, ale tylko wtedy, gdy możesz samodzielnie uzyskać dostęp do hosta fizycznego. Profesjonalne usługi hostingowe (tj. Chmura) to wielka rzecz, ponieważ administratorowi łatwo jest wyrwać klucze szyfrujące z pamięci RAM. Przejdź do http: // localhost: 8080 / przez przeglądarkę, ponieważ jest to numer portu wprowadzony podczas tworzenia. Skopiuj dokument tekstowy do zwykłego folderu html i upewnij się, że został pomyślnie skopiowany, logując się na stronie internetowej.

Czas konfiguracji

Teraz przychodzi część, w której większość ludzi rezygnuje. Nie martw się, to nie jest trudne. Po prostu początkujący widzą te liczby i myślą „O nie ... matematyka!" i wyrzuć książkę przez okno. Ale to nie jest to, co zrobisz ... ponieważ jesteś mądrym ciasteczkiem. Najpierw ustaw usługę ukrytą tak, aby łączyła się z własnym serwerem internetowym. Możesz użyć Notatnika, aby otworzyć plik „torrc" w katalogu Tor i poszukać następującego fragmentu kodu:

########### Ta sekcja dotyczy tylko usług ukrytych lokalizacji ###

Jak widać, funkcja usług ukrytych Tora jest pomniejszona o znak „#", gdzie każdy wiersz odnosi się do usługi ukrytej. HiddenServiceDir to sekcja, która zawiera wszystkie dane dotyczące Twojej własnej usługi ukrytej. Wewnątrz będzie nazwa_hosta.plik. To jest miejsce, w którym będzie Twój adres URL cebuli. "HiddenServicePort" pozwala ci ustawić port wabika dla przekierowań, aby zrzucić wszelkie wysiłki mające na celu wykrycie ciebie. Więc dodaj je do swojego pliku torrc.

HiddenServiceDir / Library / Tor / var / lib / tor / hidden_service /

HiddenServicePort 80 127.0.0.1:8080

Następnie zmień HiddenServiceDir na rzeczywisty katalog, z którego Tor biegnie.

W przypadku systemu Windows użyj:

HiddenServiceDir C: \ Users \ nazwa_użytkownika \ Documents \ tor \ hidden_service

HiddenServicePort 80 127.0.0.1:8080

W systemie Linux:

/ home / username / hidden_service /, zastępując „nazwę użytkownika" jakimkolwiek nazwiskiem tego katalogu.

Zrestartuj Tora po zapisaniu pliku Torrc i powinien on działać. Sprawdź pisownię, jeśli wyrzuca jakieś błędy. A więc teraz. Tworzone są dwa pliki: klucz_prywatny i nazwa hosta; klucze prywatne do usługi ukrytej, które należy trzymać pod kluczem. Jednak nazwa hosta nie jest Twoim kluczem prywatnym. Możesz to dać do jakiegokolwiek chcesz. Deskryptor usługi ukrytej łączy się z innymi serwerami Tora i ich odpowiednimi katalogami, dzięki czemu użytkownicy Tora mogą pobrać go anonimowo, gdy łączą się lub uzyskują dostęp do twojego ukrytego serwera. Inne uwagi:

- Odwiedzający twoją usługę ukrytą mogą być w stanie zidentyfikować, czy twój serwer WWW to Thttpd lub Apache.

- Jeśli jesteś offline przez 50% czasu, twoja usługa ukryta też. Małe fragmenty (lub długie w tym przypadku) danych, takich jak ta, są przydatne dla przeciwnika, który tworzy profil na Ciebie.

- Rozsądniej jest utworzyć usługę ukrytą na klientach Tora w porównaniu z przekaźnikami Tora, ponieważ czas działania przekaźnika jest widoczny publicznie.

- Pamiętaj, że domyślnie nie jesteś węzłem. W tym przypadku zaleca się, aby przekaźnik nie działał na tym samym komputerze co usługa ukryta, ponieważ powoduje to zagrożenie bezpieczeństwa.

Opcja szalotka i cebula

Masz również możliwość użycia szalotki lub cebuli. Shallot umożliwia utworzenie niestandardowego adresu .onion dla usługi ukrytej, takiego jak yyyyynewbietestyyyy.onio

O uruchomieniu ukrytego serwera Tor (i innego magicznego sosu Opsec)

Używając Tora przez wiele lat, miło zaskoczyło mnie, jak niewiele było incydentów, w których NSA zdołała zakłócić działanie Tora. I nie mam tu na myśli spamu, ale raczej coś, co spowodowało gwałtowne zatrzymanie dużych sekcji sieci. Jak się okazuje, szczekają znacznie gorzej niż ugryzienie, zwłaszcza jeśli ktoś jest czujny z własnym bezpiecznym ustawieniem. Rzecz w tym, że większości użytkowników Tora nie przeszkadzało to. Ale większość użytkowników nie jest zainteresowana uruchamianiem ukrytego serwera, tak jak większość użytkowników P2P nie przejmuje się seedowaniem. Większość z nich to downloadery typu hit and run. Wiedzą, że jako obywatele USA mają duże szanse na pozew, jeśli zostawią tam swoje jaja wystarczająco długo. Dlatego niektórzy użytkownicy rezygnują z pogłębiania własnej wiedzy o bezpieczeństwie. Mówią, że niech robią to twórcy Tora. Nie można się tym przejmować. Z wyjątkiem większości porad Tora udzielonych przez twórców Tora, które przeczytałem, okazały się żałośnie niewystarczające. Właściwie uważam, że nie są wystarczająco paranoiczni. Zawsze wierzyłem, że nigdy nie możesz być wystarczająco paranoikiem, jeśli chodzi o ochronę swojej wolności, ponieważ siły, które chcą ją uchwycić i butelkować w sposób, w jaki rak przejmuje kontrolę nad komórką: jedna organelle na raz z niewielką swojego środowiska świadomego wolno gotującego się ataku. Szczerze mówiąc ... Podejrzewam, że polegają na apatii i ignorancji. I wielu użytkowników chętnie się do tego zobowiązuje. Panie Żabie, poznaj wrzący garnek wody ... Więc co możemy zrobić? Na początek możemy uzyskać właściwe podejście do kwestii bezpieczeństwa.

Tor i Twój komputer

Bezpieczny komputer jest najlepszą obroną, ponieważ NSA opiera się głównie na atakach typu man-in-the-middle i exploitach przeglądarek, które dostarczają ładunki do ukrytych serwerów Tor. To powiedziawszy, powinieneś przewidzieć i spodziewać się, że taki exploit może w dowolnym momencie przeniknąć do twojego systemu. Rzeczy takie jak nitki (błędy sieciowe), których musisz być świadomy. W związku z tym należy przestrzegać następujących zasad:

- Używaj Linuksa, kiedy tylko jest to możliwe. Tak, wiem, że czujesz się komfortowo podczas korzystania z systemu Windows i uważasz, że Linux jest zbyt kłopotliwy. Ale nie zrobisz tego, jeśli Twój dostawca usług internetowych zostanie wezwany do sądu za coś, co powiedziałeś na Facebooku. Na przykład coś antyfeministycznego. Więc naucz się go używać.

Pakiet Tora z przeglądarką dla Windows odegrał kluczową rolę w usunięciu Freedom Hosting i Silk Road z powodu niezałatanych luk w zabezpieczeniach. To oraz kilka nieuczciwych węzłów wyjściowych Tora załatało niepodpisane pakiety systemu Windows, aby rozprzestrzeniać złośliwe oprogramowanie. Jeśli jesteś nowy w Linuksie, spójrz na Linux Mint. Jeśli masz doświadczenie, Debian to dobry wybór. Windowsowi nie można ufać przede wszystkim dlatego, że jest on źródłem zamkniętym, ale także dlatego, że złośliwe oprogramowanie jest na nim skuteczniejsze niż Linux. Jeśli Linux nie wchodzi w grę,

rozważ Tails lub Whonix, ponieważ te aplikacje są wstępnie skonfigurowane, aby nie zezwalać na żadne połączenia wychodzące do Clearnet.

Aktualizuj Aktualizuj Aktualizuj!

Twój komputer również musi być zawsze aktualizowany. Brak aktualizacji prowadzi do luk w zabezpieczeniach i exploitów, takich jak te w systemie Windows. Optymalnie, powinieneś upewnić się, że Tails jest zawsze aktualizowany za każdym razem, gdy używasz Tora, i unikaj witryn, które używają Java / Javascript / Flash lub jakiegokolwiek rodzaju skryptów, ponieważ wykonują one kod w sposób, którego nie widzisz. Używaj ich tylko w nagłych wypadkach i nigdy w systemie domowym. Unikaj używania plików cookie, jeśli to możliwe. Rozważ zainstalowanie dodatku Self-Destructing Cookies. Ponownie, nie powinieneś używać niczego poza komputerem przenośnym, ponieważ Twój domowy komputer najprawdopodobniej nie jest wystarczająco przenośny, aby w przypadku kompromisu wyrzucić go do kosza. Unikaj Google jak czarnej plagi. Zamiast tego użyj DuckDuckGo lub Startpage do sesji Tor.

Świadomość sytuacji

Znowu zaczynamy, głosimy tę samą starą pieśń i taniec. Ale trzykrotne czytanie często staje się później wyzwalaczem w mózgu do podjęcia działania, więc oto jest. Jeszcze raz. Jeśli agencja może monitorować połączenie lokalne, a także łącze, które przeglądasz, to (mając wystarczające zasoby) może zastosować analizę ruchu, aby określić Twoją rzeczywistą lokalizację. Dlatego nie zalecam używania Tora w swoim domu. Dla wyjaśnienia, nie używaj Tora w swoim legalnym miejscu pobytu, jeśli wykonujesz jakąkolwiek tajną pracę lub cokolwiek nielegalnego bez ścisłych środków bezpieczeństwa; rodzaj, który przeciętny użytkownik Tora prawdopodobnie przeoczy. Niech ten inny facet nauczy się lekcji To ciężka przerwa, ale lepiej on niż ty. Ma 19 lat i nazywa się Jimmy, który lubi hakować. Jesteś 32-letnim budowniczym z dwójką dzieci i hipoteką. Kto ma więcej do stracenia? Racja, ty. Więc studiuj kontrnadzór i kontr-kryminalistykę, od tego zależy twoje życie ... ponieważ tak jest! W przypadku wrogów operacji na poziomie państwowym radziłbym nie angażować się w nic nawet w pobliżu komputera online w domu. Z pewnością nic takiego myślisz, że potrzebujesz Tora, aby to ukryć. Może to być dobre w przypadku przeglądania prywatnego, ale nie dla kogoś, kto planuje zamach stanu, przeprowadza nielegalną operację (na przykład domowe studium biblijne w Iranie) lub próbuje zniknąć. Uważaj na używanie go również w hotelach, gdzie często jest wiele kamer oglądanych z całodobowym nadzorem. Ta lokalizacja może być powiązana z aktywnością Tora. Nie używaj Tora dłużej niż jeden dzień w określonej lokalizacji. Atak korelacyjny można przeprowadzić w mniej niż godzinę, jeśli w pobliżu zaparkowany jest czarny van - furgonetka, której nie zobaczysz. Mogą nie zakuć cię w kajdanki, kiedy wychodzisz z kawiarni w tym samym tygodniu, ale później mogą. Potraktuj ten obszar jako toksyczne wysypisko po dniu, niezależnie od tego, czy musisz udać się do następnego sklepu lub miasta. Jeśli chcesz naprawdę ukryć się i szeptać, uruchom aplikację (na przykład MMO), gdy jesteś poza domem i wykonujesz swoją aktywność Tor, która sprawia, że wygląda to tak, jakbyś był w tym czasie w domu. - Obserwowaliśmy pana, panie Anderson, i wygląda na to, że żyje pan… dwa… życia. - Agent Smith, Matrix.

Darknet Personas

Bez wątpienia czytałeś o wpadkach Tora, w których tajny agent przechwycił numer telefonu lub system Clearnet od kogoś, kogo był celem, ponieważ wspomniany cel zbytnio ufał, zbyt szybko. Możesz tego uniknąć, przekwalifikowując się, oduczając się tego, czego się nauczyłeś. Musisz uważać swoje sesje Tora za własność swojej drugiej Jaźni. Sklonowany Ty - ten cienisty złodziej wyglądający facet powyżej. Drugie Ty. Taki, który gardzi Incubusem i kocha Tool'a i postrzega Neo jako kolejnego betaorbitującego punka, któremu udało się wylosować, gdy Morfeusz i załoga go odłączyli. Ten klon nie używałby

Twittera, YouTube ani innych śmieci społecznościowych. Nigdy by się z tobą nie spotkał ani nie zadzwonił na kilka piw. W rzeczywistości nienawidzi piwa, woli J&B, gdy hacki z The Thing OST Johna Carpentera grającym jako nastrojową muzykę w tle. To twój drugi Ty. Im mądrzejszy ty. I musi być nowym Ty na Torze. I musisz na zawsze oddzielić go od nie-Tor You. Jego konta na Facebooku, Twitterze i YouTube są fałszywe, ponieważ nigdy nie używał ich na swoim domowym komputerze. Jego nicki są różne, podobnie jak jego hasła, upodobania / antypatie, a nawet czcionki, których używa do przeglądania Deep Web. Mieszanie tej mrocznej osobowości z własną byłoby jak chłopiec z materii całujący dziewczynę z antymaterii ...

BUM.

Ponadto wszelkie rozmowy telefoniczne, które wykonuje ta osoba, są wykonywane za pomocą telefonów prepaid, które nie zostały zakupione żadną z posiadanych przez nią kart kredytowych. Jest facetem z kasą i przewozem tylko wtedy, gdy jest dwadzieścia mil od domu. Wszystkie karty SIM, których używa, są ściśle używane w połączeniu z aktywnością Tora i nigdy nie są używane w telefonach, których używa drugi facet. I ... celowo zostawia fałszywe informacje, gdziekolwiek się pojawi. Coś jak CIA. Ale aby lepiej wyjaśnić ten pomysł, załóżmy, że John Doe nie wie nic lepszego. Ogląda film w serwisie Netflix. Potem idzie do Freenet i przekazuje informacje, nawet nie zdając sobie z tego sprawy, chętny do podzielenia się swoim wspaniałym kinem , doświadczenie z jego pąkami z ciemnej siatki (bez kalamburów). „Hej, chłopaki, właśnie obejrzałem fajny film z Russellem Crowe. Kinda Michael Bay-ish i Liam Neeson był za krótki, ale jest niezły film, jeśli chcesz dowiedzieć się, jak zniknąć. Ale ta policja, słodki Jezu! policjanci z wynajmu są z pewnością głupi jak worek cegieł! ”

Mówi, że policja jest głupia.

Metadane są zbierane przez Netflix tak samo, jak w Google i Yahoo. Każdego użytkownika. Znają każdy film, który oglądałeś, a nawet te, których nienawidziłeś. Opublikował nawet posty na forum wskazujące na podobną pogodę i choć nie wymieniając nazwisk, narzekał, że lokalni politycy są w kajdankach podczas aresztowań bardzo specyficznych dla regionu, a nawet wycofał zarzuty! Jak myślisz, ilu fanów Netflix obejrzało ten film w czasie jego postu na Freenet? Ilu w miastach aresztowano lokalnych polityków za defraudację? Ilu z podobną pogodą przedstawiono w filmie? Najprawdopodobniej mniej niż dziesięć. Może nawet nie to. Jest też element pisma ręcznego. Czy ciągle błędnie pisze te same słowa? Rzucać przecinki jak sztylety? Niewłaściwie używasz średników i zdań run-on? Brak synchronizacji zegara systemowego z jego postami? Wszystko to prowadzi do wspaniałego profilu, który wiąże jego adres IP z jego tożsamością. Często wystarczy dostać nakaz, jeśli choćby szeptał, że zdobył jakąkolwiek kontrabandę. Chyba że, oczywiście, wszystkie te informacje są dostosowane do Twoich potrzeb. Wiemy już, że VPN o nazwie Hide-My-Ass, a także Hushmail i Lavabit dźgnęli swoich użytkowników w plecy, gdy groźby sędziego stały się zbyt gorące (5000 dolarów dziennie w przypadku Lavabit, dopóki nie rozwidli danych użytkowników). A wszystko to tylko po to, żeby wyśledzić Edwarda Snowdena. Konkluzja: ucz się na błędach Snowdena. Traktuj z przymrużeniem oka roszczenia do anonimowości każdej firmy. Dowodem jest liczba aresztowań wniesionych do wspomnianej firmy lub aplikacji. W przypadku Freenet ... żadne. Ale zawsze jest pierwszy raz. Przypomnij sobie, że szczęście im wystarczy tylko raz, co najczęściej zależy od Twojej nieostrożności.

Usługi ukryte Tor - wysokie ryzyko, wysoka nagroda

CNN wraz z FoxNews trąbią o porażce niektórych usług ukrytych już od kilku lat. Usługi takie jak Silk Road i Freedom Hosting, o których jestem pewien, że słyszałeś. Są łatwym celem dla FBI, ponieważ usługi ukryte nie znajdują się jeszcze wysoko na liście priorytetów twórców Tora. To samo dotyczy NSA. Obie agencje znają wszystkie sztuczki i sztuczki związane z prowadzeniem usługi ukrytej. Ty też powinieneś. Nie oznacza to, że potrzebujesz wiedzy specjalistycznej aby dorównać ich zespołowi super

hakerów, ale aby uruchomić taką usługę, potrzebujesz jeszcze większej czujności niż odwiedzanie takiej usługi. Priorytet numer jeden jest prosty: jeśli go prowadzisz, musisz go posiadać. Nie może być uruchamiany pod czyjąś kontrolą, jeśli możesz temu pomóc, ponieważ jeśli ta usługa zostanie naruszona, wszyscy upadną. Oznacza to całkowitą anonimowość, przez 100% czasu ze światowej klasy umiejętnością ukrywania się przed złodziejami klejnotów. Administrator Silk Road nie miał takiej możliwości. W rzeczywistości, przeglądając dokumenty online szczegółowo opisujące aresztowanie, można odnieść wrażenie, że był bardzo luźny w procedurach bezpieczeństwa IT. Wielokrotnie popełniał takie błędy, że szczęście ze strony LE tak naprawdę nigdy do tego nie doszło. Facet był po prostu niechlujny.

Pierwsze

Nigdy, przenigdy nie uruchamiaj usługi ukrytej na maszynie wirtualnej należącej do znajomego lub dostawcy przestrzeni w chmurze. Pamiętaj, że wszystko „Chmura" to dysk lub sieć innej osoby, a nie Twoja. Klucze szyfrowania można zrzucić z RAM. A kto jest właścicielem pamięci RAM? Dobrze. Dostawca chmury. Uderza piorun i nadchodzi twoja własna anonimowość, a także anonimowość odwiedzających, jeśli są leniwi w swoich zwyczajach przeglądania. FBI dostarczyło w ten sposób „nit" (technikę śledztwa sieciowego) do niezałatanych paczek Tora z przeglądarką w 2013 roku. Jeśli jednak jesteś właścicielem maszyny, to inna historia. Ale cofnijmy się o kilka kroków i załóżmy, że nie. Jak możesz go uruchomić w systemie hosta? Po pierwsze, potrzebujesz dwóch oddzielnych hostów fizycznych z różnych stron, obu działających na maszynach wirtualnych z systemem operacyjnym z włączoną zaporą ogniową, który zezwala tylko na aktywność sieci Tor i nic więcej. Drugi host fizyczny to ten, z którego działa usługa ukryta, również wykorzystujący maszynę wirtualną. Bezpieczne połączenia są włączane przez IPSec. Co to jest IPSec, pytasz? „IPSec to zestaw protokołów do zabezpieczania komunikacji protokołu internetowego (IP) poprzez uwierzytelnianie i szyfrowanie każdego pakietu IP sesji komunikacyjnej. IPsec może służyć do ochrony przepływu danych między parą hostów (host-host), między para bram bezpieczeństwa (sieć-sieć) lub między bramą bezpieczeństwa a hostem (sieć-host). " Jeśli agent intruza coś manipuluje, będziesz o tym wiedział i możesz wyłączyć usługę lub przenieść ją w bezpieczniejsze miejsce, a wszystko to będąc duchem w maszynie. Możesz sobie wyobrazić, jak cenne byłoby to w Korei Północnej. Gdybyś był w tym szambie kraju, byłbyś więcej niż trochę paranoikiem, gdyby serwer przestał działać nawet na kilka sekund. Ale zawsze możesz przenieść go do bezpieczniejszej lokalizacji lub nawet zacząć od nowa, a możesz po prostu chcieć, ponieważ nie wiesz, czy wystąpiła awaria RAID lub czy jakiś commie jackboot wysyłał kopię maszyny wirtualnej do wyższych jednostek.

Drugie

Jeśli wybierasz trasę hosta, musisz upewnić się, że konsola zdalna jest zawsze dostępna dla hosta, w dowolnym momencie. W rzeczywistości musisz robić wszystko zdalnie i często zmieniać hasła przez https. Powiedziałbym, że raz dziennie paranoja w takim klimacie jak Korea Północna byłaby dobra dla twojego zdrowia.

Trzecie

Nigdy, ani razu, nie możesz uzyskać dostępu do usługi z domu. Nie z Nexusa 7. Nie z Galaxy Note twojej dziewczyny. Nawet przez Tora z twojego podwórka, używając WiFi twojego sąsiada. Korzystanie z VPN również jest ryzykowne, chyba że wiesz, co robisz. Uzyskaj do niego dostęp tylko przez bezpieczne lokalizacje co najmniej dziesięć mil od Twojego miejsca zamieszkania. Niektórzy mogą powiedzieć, że przesada, ale w gułagu nie ma czegoś takiego jak przesada.

Czwarte

Od czasu do czasu przenieś usługę. Ponownie spójrz na dowolny film na YouTube o tym, jak snajperzy trenują, aby pokonać wroga. Po każdym strzale przesuwają się z miejsca na miejsce, aby ukryć prawdziwą lokalizację przed wrogiem. Jak często zależy od Ciebie. Raz w tygodniu? Raz w miesiącu? Osobiście powiedziałbym, że co dwadzieścia jeden dni. Korzystając z jednego z nich, nigdy nie możesz być zbyt bezpieczny.

Śmierć anonimowości

Premier David Cameron odnotował w styczniu 2015 r., Że chce zakazać stosowania wszystkich aplikacji do przesyłania wiadomości obsługujących szyfrowanie, jeśli rząd nie może mieć kluczy do tylnych drzwi do odszyfrowania szyfrowania. To jest ponad niedorzeczne. To byłoby jak rolnik pozwalający na łatwe wejście do kurnika zarówno kuguarom, jak i lisom. Na szlaku kampanii powiedział: „Czy pozwolimy na środki komunikacji, których po prostu nie da się przeczytać? Moja odpowiedź na to pytanie brzmi: nie, nie wolno". Chociaż odnosił się głównie do programów do czatowania, takich jak WhatsApp, a co nie, można założyć, że ranczo mówił także o aplikacjach takich jak PGP, Freenet i wycofany Truecrypt. Niestety, użył ataku Hebdo (rysownika) jako usprawiedliwienia (czy nie wszyscy używają ich do dalszych planów Wielkiego Brata?). Widzę podobny trend rozwijający się w Kanadzie w zakresie korzystania z VPN. Nowe przepisy wymagają teraz, aby sieci VPN identyfikowały klientów pobierających dzieła chronione prawem autorskim, takie jak filmy i gry, aby powiadomienia o naruszeniu (tj. Listy zastraszające) trafiały do właściwej osoby. Brzmi to raczej powierzchownie, bo kto by nie zaprzeczył zdolności George'a Lucasa do stworzenia większej liczby prequeli Gwiezdnych Wojen? Sztuka, wiesz. Ale w tym tkwi problem. Głównie chodzi o to, że politycy zapominają, jak naprawdę działa internet. Robienie tego, co nakazują, oznacza, że dostawcy VPN muszą przechowywać dzienniki dostępu przez minimum 6 miesięcy. Już samo to gwarantuje, że zdolność VPN do sprzedaży usług anonimowych (a właściwie prywatności) zniknie, co doprowadzi do ogromnych strat, ponieważ klienci nie są głupi. Wiedzą, kiedy ich prywatność jest celem. Niech rozpocznie się exodus! (Rządowe partie plików cookie) Wiedzą również, że sieci VPN przypisują klientom wspólne adresy IP. Jednym z nich możesz być Ty, popijając Rickarda Reda podczas pobierania najnowszego filmu NiN YouTube pozornie zablokowanego, podczas gdy drugim użytkownikiem jest wujek Frick pobierający coś od facetów z grupy Usenet, którzy lubią podskakiwać z warkoczykami-dziewczynami-na-a -kolano. Jedynym rozwiązaniem jest całkowite wyprowadzenie się z Kanady. Ale być może tego właśnie chciał rząd. Najsmutniejsze nie jest to, że nic z tego nie powstrzyma terroryzmu ani praw autorskich lub że zaszkodzi to większości prywatnych firm zajmujących się szyfrowaniem lub że tylko politycy będą mieli szyfrowanie, podczas gdy obywatele go nie mają. Nie, najsmutniejsze jest to, że staniemy się żabą w garnku, która sama włącza piekarnik do maksymalnej temperatury, a następnie wsuwa się z powrotem do garnka, a wszystko dlatego, że ktoś potężniejszy od ciebie lub ja powiedziałem, że to słuszna rzecz. Nasz świat stanie się Światem Bizarro. Tam, gdzie dobro jest złe, a światło jest ciemne i nikt nie ma bezpieczeństwa, z wyjątkiem agentów nowej Matrycy, którą oni będą budować. Gdzie być bardziej bezpiecznym, to być mniej bezpiecznym, gdy my, peoni, idziemy ... bo jeśli rząd tak mówi, to musi to być prawda ewangelii, ponieważ kiedy ostatnio polityk kłamał? Jeśli nie nauczysz się niczego więcej, pamiętaj o dwóch rzeczach: Backdoory to luki w zabezpieczeniach w 100% przypadków. Drugi jest podobny: anonimowość i prywatność oraz wynikająca z tego wolność umrą tylko wtedy, gdy na to pozwolimy.

Myśli końcowe

Jak widać, moce, które są, aktywnie skupiają się na twojej zdolności do dokonywania wyborów dotyczących twojej własnej wolności. Pracują małymi krokami. Myślą, że jesteś głupi. Myślą, że mogą prowadzić twoje życie lepiej niż ty. Tylko oni nie mogą. Czy NSA powstrzymała atak na Charlie Hebdo, francuskiego rysownika? Czy zatrzymali 11 września? Bombardowania w Hiszpanii? Śmierć od tysiąca cięć, po trochu na raz, a zanim się zorientujesz, czujesz zawroty głowy, ale nie wiesz, dlaczego. Uwierz

mi, odkładanie na później swojego bezpieczeństwa i spokoju wystarczy, aby podsycić tsunami raka, które budują jedną komórkę na raz. Jeśli przeczytałeś tę książkę, to znaczy, że zrobiłeś już wszystkie potrzebne kroki dziecka. Zanurzyłeś swój duży palec u nogi w tym wirze i najwyższy czas, abyś wskoczył. Nie zwlekaj. Wiesz, jak ciepła jest woda. Poczekaj zbyt długo, a woda może być zbyt zimna. Jeszcze gorsze jest to, że ktoś może cię po prostu całkowicie zamknąć. Pamiętaj tylko: zawsze pielęgnuj silny sposób myślenia o bezpieczeństwie. Rozwiń umiejętność logicznego konfigurowania rzeczy i przewidywania kłopotów z dużym wyprzedzeniem, widząc słabości w swojej łodzi podwodnej, zanim woda wpłynie z rykiem. W razie wątpliwości obejrzyj film „The Abyss". Widzisz, jak Bud reaguje, gdy woda ryczy do środka? On panikuje! Większość załogi umiera. Nie czekaj do tego pamiętnego dnia. Przygotuj coś na długo przed czasem. Plan B. Plan C. Nawet plan D, jeśli cię na to stać. Każda agencja wywiadowcza ma nieograniczone fundusze na zabijanie wolności poprzez cenzurowanie nas wszystkich - nawet cenzurowanie wolności kupowania tego, co chcesz kupić. Z mediami w tylnej kieszeni mogą wyczarować każdego boogeymana, którego chcą cię przejechać. Okłamywanie cię nie jest nielegalne, ale ty ich okłamujesz. Ta hipokryzja nic ich nie kosztuje, ale kosztuje Cię wszystko, więc podobnie jak oni, musisz na bieżąco śledzić zmiany w dobrym bezpieczeństwie, aktualizując je w razie potrzeby i być w ciągłej gotowości do nowych zagrożeń dnia zerowego. Ale jeśli jest jedna rzecz, której nie mają, jest to zachęta do cięższej pracy niż oni. Odbijają codziennie o 17:00. Będziesz? Moce, które są brudne. Ty też powinieneś.