Prywatność i anonimowość – pierwsze kroki

5 lipca 2024

Na początek, spróbujmy pobieżnie przyjrzeć się sytuacji związanej z prywatnością i anonimowością oraz niektórym narzędziom. Już teraz chciałbym podkreślić jedną, ważną rzecz: aby uchronić się od popełniania błędów na samym początku, należy najpierw przeczytać wszystko, co dotyczy określonego tematu a dopiero później, podejmować próby wdrożenia wybranego rozwiązania.

Chyba nikogo nie trzeba przekonywać o problemie z cenzurą i inwigilacją, ale co właściwie chcemy osiągnąć? Proponuję takie cele:

1. Zmniejszenie, lub wykluczenie profilowania, na które nie wyraziliśmy zgody.

2. Utrudnienie identyfikacji, lub jej uniemożliwienie.

3. Przeciwdziałanie cenzurze.

4. Uniemożliwienie zerwania kontaktu między szeroko pojętymi „nami”.

5. Poszukiwanie alternatywnych źródeł finansowania treści internetowych.

Ostatni postulat jest najtrudniejszy a rozwiązań bardzo mało. Co gorsze, finansowanie praktycznie wyklucza anonimowość. Co za tym idzie, twórcy będą „wystawieni na strzał”. Dlatego muszą wyjątkowo dbać o treści, które udostępniają.

Punktem, od którego powinniśmy zacząć, jest zmiana systemu operacyjnego. Wiem, że to utopia i na ten krok, zdecyduje się jedynie garstka najbardziej zdeterminowanych, ale trzeba przynajmniej mieć świadomość sytuacji. Telefony komórkowe

wykluczam z tej dyskusji zupełnie, ponieważ to są zawodowi zdrajcy. Oczywiście można podejmować próby ich „deguglizacji" i anonimizacji, ale jaki to ma sens, gdy właściciel jest stale namierzany fizycznie a połączenia, treści rozmów i SMS-ów, są rejestrowane? W najlepszym wypadku, można tylko poprawić prywatność, ale o anonimowości lepiej nawet nie marzyć.

W pecetach, laptopach i czym tam jeszcze, konieczność zmiany systemu operacyjnego, pojawi się prawdopodobnie z początkiem roku 2025, kiedy Microsoft, wprowadzi do Windows 11, sztuczną inteligencję, która na bieżąco będzie śledzić i rejestrować wszystko, co robi użytkownik. Jako że ta SI nie będzie zainstalowana lokalnie, każdy nasz ruch, będzie analizowany przez odpowiednie, zdalne centra. Początkowo, ma to być usługa dobrowolna, ale kto w tym temacie tkwi od dawna, wie jak w praktyce wygląda owa dobrowolność, według Microsoftu.

Od pewnego czasu, dają się też zaobserwować naciski na tworzenie backdoorów w popularnych komunikatorach i zakusy na wolność szyfrowania treści. Nawet Linusa Torwadlsa (twórca jądra Linuksa), usiłowano zmusić do umieszczenia backdoora w jądrze Linuksa. Ponieważ Linus nie jest samodzielnym twórcą jądra, którego kod źródłowy jest otwarty dla tysięcy – jeśli nie milionów programistów – ruch ten był równie głupi jak absurdalny. Istotę tego absurdu, bardzo ładnie oddaje wideo Mateusza Chroboka „Jak pół sekundy uratowało świat przed zagładą?".

Niestety, od 2025 roku, Linux nie będzie już rozwiązaniem doskonałym, ponieważ komunikacja z osobą używającą Windows 11, niemal zagwarantuje także deanonimizację każdego, kto się z nią kontaktuje i szyfrowanie niczego tu nie zmieni. To po prostu tak, jakby ktoś zaglądał Ci przez ramię, kiedy używasz komunikatora, lub piszesz e-mail. Biorąc pod uwagę wspomniane naciski (na tworzenie backdoorów), użytkownicy starszych wersji Windows, byliby naiwni, gdyby wierzyli, że system ich

nie szpieguje od dawna. Jeśli mimo wszystko zamierzasz pozostać przy Windows, zadbaj przynajmniej o to, żeby wszelkie oprogramowanie o zamkniętych źródłach, zastąpić oprogramowaniem open source. To pozwoli Ci kiedyś dokonać łatwiejszej migracji na Linuksa.

Od czego możemy zacząć?

Być może najprostszym i jednocześnie dosyć skutecznym sposobem jest skorzystanie z sieci TOR w przeglądarce i komunikatora „Session" (osobna aplikacja dla najbardziej popularnych systemów operacyjnych, w tym – Android), który także działa w sieci „cebulowej". Niestety, nie są to rozwiązania doskonałe. Samo użycie sieci TOR, może sprawić, że od razu znajdziemy się „na celowniku". W przypadku Tor Browser, możemy temu zapobiec, uruchamiając „mostek". To spowoduje, że nasza aktywność będzie sprawiała wrażenie zwykłego ruchu. Wadą jest powolność. Już sama sieć TOR jest powolna a włączony mostek, spowolni przeglądanie jeszcze bardziej. Niektóre strony blokują ruch pochodzący z takiego źródła. Większość tych blokad można obejść właśnie dzięki mostkom, ale nie wszystkie.

Tor Browser

Pobierz Tor Browser z tej strony i rozpakuj w katalogu, w którym chcesz ją mieć już na stałe. O ile wiem, nie wymaga instalacji nawet w systemie Windows. Wystarczy teraz wejść do jej głównego katalogu, przejść do > Browser i uruchomić plik „firefox". W tej chwili, przeglądarka zacznie się łączyć z siecią TOR. Dobrze by było zdążyć temu zapobiec, aby nawet pierwsze połączenie odbyło się przez mostek, który domyślnie jest wyłączony.

UWAGA! Nie zmieniaj rozmiaru okna przeglądarki. Niech pozostanie domyślnej wielkości. To utrudni identyfikację na podstawie rozdzielczości ekranu. Ważnym elementem zachowania anonimowości jest wtopienie się w tłum użytkowników TOR.

Włączanie mostka

W prawym, górnym rogu, znajdziesz menu (hamburger), kliknij i przejdź > ustawienia > Połączenie (w lewym panelu) > przewiń do pozycji „Mostki” i przełącz na „Użyj mostków”. Wybierz mostek wbudowany (obfs4). Później możesz eksperymentować z innymi mostkami. Kliknij przycisk „Połącz” (jest nieco wyżej), lub uruchom przeglądarkę ponownie i tym razem, pozwól jej na połączenie. Osobiście, odznaczam opcję automatycznego łączenia się, ale to kwestia upodobań. Zamiast menu, do włączenia mostka, możesz użyć przycisku „Skonfiguruj połączenie”, na stronie startowej. Zaprowadzi Cię dokładnie w to samo miejsce.

Pozostaje jeszcze jedna, ważna rzecz. W lewym panelu ustawień, kliknij „Prywatność i bezpieczeństwo”. Przewiń do pozycji „Bezpieczeństwo” i tam, wybierz stopień, w jakim chcesz być chroniony/a. Stopnie bezpieczeństwa są dosyć dobrze opisane, więc tylko powiem, że ostatni, całkowicie wyklucza możliwość logowania się gdziekolwiek, odtwarzania wideo czy nawet obrazków i sprowadza stronę do prostego HTML, pozbawionego wszelkich skryptów. Stopień średni zaś, wymaga udzielenia ręcznego zezwolenia za każdym razem, gdy chcemy odtwarzać w.w treści. To bywa kłopotliwe, ale daje nam pełną kontrolę nad zachowaniem strony. Do ustawień stopnia bezpieczeństwa, znajdziemy szybki dostęp przez kliknięcie ikony tarczy, tuż obok paska adresu, po jego prawej stronie. Kolejna ikona (miotełka), pozwala zmienić „tożsamość”. Co to znaczy? Tor Browser – powiedzmy – „fałszuje” nasze „odciski palców” (fingerprint). Użycie nowej tożsamości, oznacza zmianę tych odcisków i zmianę obwodu, przez który przechodzi nasze połączenie. Klikając ikonę po lewej stronie adresu (wężyk z kropkami, gdy połączenie zostanie nawiązane), możemy zmienić sam obwód, bez restartu przeglądarki.
Instalowanie wtyczek, jest kiepskim pomysłem, ponieważ na ich podstawie, można zawęzić krąg „podejrzanych”. Podobnie jak to ma miejsce w przypadku rozdzielczości ekranu. Nie zmieniaj innych ustawień, chyba, że wiesz co robisz.

Jeśli masz zamiar korzystać ze stron w innych językach niż polski, warto zmienić ustawienia języka. Najlepiej na angielski. Łatwiej się wtedy zgubić w tłumie. Menu > Ustawienia > Ogólne > przewiń do „Język” i zmień na wybrany.

Jeśli o mnie chodzi, to nie sądzę, abym kogokolwiek interesował na tyle, żebym był tropiony w cebulowych zaroślach, więc godzę się na zmniejszenie anonimowości i najczęściej używam podstawowego poziomu bezpieczeństwa, oraz wtyczki „UBlock Origin”. To mi pozwala zachować funkcjonalność stron, ale blokuje reklamy, które mocno spowalniają przeglądanie a same w sobie bywają elementami szpiegującymi.

Komunikator Session

Zdecydowanie najbezpieczniejszy komunikator. Używa swojej własnej sieci cebulowej. Jak Tor Browser, jest open source. Nie wymaga rejestracji ani numeru telefonu. Nie zidentyfikują ani nie zablokują Cię nawet jego twórcy. Wadą jest stosunkowo wolne połączenie (jak to w sieciach cebulowych) i fakt, że tu nie ma mostka. Zatem używając Session’a, z automatu możesz znaleźć się „na celowniku”. Na starych Windowsach, np. Windows 7, Session raczej już nie będzie działał poprawnie. Niektórzy mogą chcieć przejrzeć FAQ, aby osobiście sprawdzić, czy jest godny zaufania.

Komunikator możesz pobrać TUTAJ.

Nie widzę potrzeby, szczegółowego opisywania procesu zakładania konta, bo dostępny jest całkiem przyzwoity przewodnik dla początkujących. Nic nie stoi na przeszkodzie, aby użyć automatycznego tłumacza, jeśli to jest konieczne. Nie obawiaj się, tworzenie konta jest dosyć proste i intuicyjne. Warto mieć świadomość, że jedynym co pozwala Cię odróżnić od innych użytkowników tej sieci, jest identyfikator. Najlepiej wydrukuj go, wraz z frazą odzyskiwania i przechowuj w bezpiecznym miejscu.

Po utworzeniu konta, nowych użytkowników możesz dodawać, klikając znak „+” u góry lewego panelu > Nowa Wiadomość > Wpisz identyfikator znajomego i kliknij przycisk „Dalej”. Nie pamiętam co później się dzieje a teraz nie mam kogo dodać, żeby sprawdzić. Możliwe, że to w tej chwili, zostanie wysłane do tej osoby żądanie wiadomości (akceptacji?). W analogiczny sposób możesz tworzyć czaty grupowe, dodawać do nich znajomych lub dołączyć do czatu społeczności Session.

Do pokonania, pozostaje jeszcze jeden problem: jak przekazywać sobie identyfikatory? Jeśli udostępnisz go publicznie, powiedzmy – tutaj, w komentarzach, to każdy, kto teraz może poznać Twój IP i powiązać go z Tobą, to samo będzie mógł zrobić z identyfikatorem Session’a. Kto ma takie możliwości? Bez wątpienia, nasz dostawca usług internetowych (ISP). Jeśli korzystasz z sieci lokalnej (LAN), to podobne możliwości ma jej administrator. W zależności od sprzętu i rodzaju połączenia, w grę może też wchodzić ktoś zupełnie postronny, jako MITM (Man In The Middle). To może być szczególnie prawdziwe w przypadku korzystania z połączeń wi-fi, zwłaszcza w miejscach publicznych. Dlatego publiczne udostępnianie identyfikatora nie jest dobrym pomysłem. Chyba, że możesz to zrobić naprawdę anonimowo. I tu, zaczynają się schody. Cała sprawa przypomina wyczyn barona Munchausena (nie mylić syndromem Munchausena), który sam wyciągnął się za włosy z bagna i to wraz z koniem. Jak nieanonimowa osoba, może przekazać anonimowo dane na swój temat, ale tak, aby nie zdradziły tożsamości tej osoby?

Nie mam takiej mocy w garści, jak baron Munchausen, więc pozostaje najpierw „zniknąć” aby pojawić się jako anonim, którego tożsamości nie zna nikt i nie może z nikim powiązać. Najprostsze wydaje się użycie Tor Browser i dołączenie do jakiegoś publicznego, darmowego czatu. Właśnie sprawdziłem i po chwili zmagań z captcha, wpuścili mnie TUTAJ.

Mógłbym teraz, całkiem anonimowo wysłać identyfikator Session’a, ale mniej podejrzanie wyglądałby adres e-mail,

utworzony także przez TOR. Na coś takiego, pozwala np. Proton Mail. Nie dość, że sam podsuwa taką możliwość (między wierszami), to można się zarejestrować przy pomocy tymczasowego adresu e-mail (sprawdziłem). Oczywiście, tego tymczasowego adresu, należy użyć także przez TOR. Być może da się też na tymczasowy numer telefonu, ale tego już nie testowałem.

Adresy darmowych usług tymczasowych, które pozwalają na dostęp z TOR:

E-mal: https://internxt.com/temporary-email

Telefon: https://quackr.io/temporary-numbers

Jest ich z pewnością więcej. Takie adresy/numery wygasają zwykle po kilku godzinach, więc proces rejestracji trzeba zacząć i zakończyć w trakcie ich życia. Nie pozwalają wysyłać wiadomości. Można tylko odbierać. Wiem, mętne toto i przekombinowane. Są bardziej zaawansowane narzędzia, ale czy prostsze? Na razie, sugeruję sprawić sobie Session'a i używać go ze znajomymi, którym można przekazać identyfikator np. przez zaufany e-mail (na pewno nie przez Gmail czy Onet itp.) lub nawet na kartce (którą potem powinno się zniszczyć). Ostatecznie, można też obejść się bez tych wszystkich ceregieli i zwyczajnie pokazać światu swój identyfikator Session'a. W końcu nie jesteśmy przestępcami (mam nadzieję). Wypada zdać sobie sprawę i z tego, że cokolwiek zrobimy, jednymi z pierwszych, którzy dołączą do takiej społeczności, będą indywidua o niezbyt czystych intencjach.

Wnioski końcowe

Czy sieci TOR są bezpieczne? W zasadzie tak, ale można mieć wątpliwości odnośnie kilku aspektów.

1. Została zaprojektowana przez Marynarkę Wojenną Stanów Zjednoczonych a później, wspierana przez DARPA. Nie jest to

najlepsza rekomendacja. Celem była bezpieczna sieć anonimowej komunikacji dla urzędników, agentów i różnych mącicieli (dziennikarzy, dysydentów[ich dysydentów], działaczy…). Z pewnością nie obawiali się o naszą wolność słowa, tylko o kontakt ze swoimi wtyczkami.

2. Obecnie, sieć TOR, opiera się na węzłach prowadzonych przez wolontariuszy. To dobrze, ale oznacza również, że część z nich to węzły podstawione przez odpowiednie służby. Na szczęście, dobór węzłów jest randomizowany. To znaczy, że jest bardzo mała szansa, aby trafić na sytuację, w której wszystkie trzy węzły (TOR łączy się minimum przez trzy węzły), były „zdrajcami". W razie podejrzeń, zmiana tożsamości, albo chociaż samego obwodu, zniszczy ten misternie utkany plan. Bez przejęcia wszystkich trzech węzłów, atakujący skazany jest na atak korelacyjny. To z pewnością przysporzy o ból głowy nawet poważne służby.

3. Jeśli zabraknie szyfrowania pomiędzy węzłem wyjściowym a serwerem docelowym (stroną), można będzie odczytać treść, lub aktywność użytkownika i na tej podstawie, próbować go identyfikować. Upewnij się więc, że masz włączone szyfrowanie HTTPS: menu > ustawienia > Prywatność i bezpieczeństwo (w lewym panelu) > przewiń do samego dołu, do pozycji „Tryb używania wyłącznie protokołu HTTPS", zaznacz „Włącz we wszystkich oknach". Pamiętaj, że skrót HTTPS, nie jest magicznym zaklęciem i wiele zależy od tego, kto ma klucz prywatny, sesyjny klucz kryptograficzny lub dostęp do informacji o sesji. W praktyce oznacza to, że – przynajmniej teoretycznie – zdrajcą może być każdy serwer.

Tyle na dzisiaj. Jeśli temat się przyjmie, w przyszłości, chciałbym zapoznać czytelników z takimi pojęciami jak: VPN, IPFS (planetarny system plików) sieć I2P (projekt niewidzialnego internetu), Hyphanet, ZeroNet i zdumiewająca sieć „mesh", która może się stać przyszłością komunikacji a na pewno, może służyć jako sposób na zachowanie łączności w warunkach kryzysowych. Np. gdy padnie internet i telefonia, w

tym – komórkowa. Niektóre z tych narzędzi, można z sobą łączyć. Użycie np. I2P + TOR, zwiększa anonimowość (i uciążliwość) choć to, zakrawa już na lekką paranoję, w przypadku zwykłych użytkowników.

Następnym razem, coś o prywatności w codziennym korzystaniu z internetu.

Autorstwo: Zapluty Karzeł Reakcji
Źródło: WolneMedia.net