Prywatność na co dzień

12 lipca 2024
Rzut oka na sytuację, wyjaśnienie podstawowych pojęć i kilka recept na poprawę prywatności.

Przeglądarki. Komu ufać?

Najprościej byłoby powiedzieć „nikomu” i wyciągnąć wtyczkę od Internetu. Nic prostszego, nad wygłaszanie podobnych komunałów. Istnieje jednak duże prawdopodobieństwo, że takie rozwiązanie nikogo nie interesuje, więc przyjrzyjmy się jedynemu kryterium, mogącemu zapewnić minimum zaufania – otwartości kodu źródłowego.

Większość współczesnych przeglądarek, zbudowana jest w oparciu o silnik „Blink” lub „Gecko”. Obydwa udostępniają swój kod źródłowy do publicznego wglądu. Silnik silnikiem, ale to jeszcze nie przeglądarka. Dla silnika „Blink” podstawową przeglądarką, która dała początek wszystkim pozostałym, jest „Chromium” (nie mylić z „Google Chrome”). Natomiast dla silnika „Gecko” jest to „Firefox”. O ile w pełni otwarte źródła dla przeglądarek opartych na „Chromium” są rzadkością, o tyle pochodne „Firefoksa” (rozgałęzienia/forki), rzadko

zamykają jakąś część kodu. Szczerze mówiąc: nie znam takiej ani jednej.

Niektóre przeglądarki oparte na „Chromium”: „Chromium”, „Ungoogled Chromium”, „Google Chrome”, „Opera”, „Brave”, „Vivaldi”, „Microsoft Edge”, „Yandex Browser”, „Thorium”. Spośród nich, tylko „Chromium”, „Ungoogled Chromium” i „Thorium”, mają w pełni otwarty kod źródłowy. Pozostałe, ukrywają części dodane przez siebie. Jeśli można mówić o jakimś zaufaniu, to brać pod uwagę można jedynie te trzy. Zapewne w tym miejscu zaprotestują puryści i będą mieli trochę racji: Nawet „Ungoogled Chromium”, której ambicją jest całkowita deguglizacja „Chromium”, może zawierać komponenty, które nie mają swojego odpowiednika open source, więc muszą korzystać z kodu Google. Takie podejście wydaje się jednak nieco przesadzone.

Wybrane przeglądarki oparte na „Firefoksie”, czyli „Gecko”: „Firefox”, „Tor Browser”, „Waterfox”, „LibreWolf”, „Pale Moon”, „Mullvad Browser”, „SeaMonkey”. Wszystkie mają w pełni otwarte źródła. W przeciwieństwie do „Firefoksa” pozostałe raczej nie budzą wątpliwości co do intencji ich producentów i są naprawdę interesującymi alternatywami dla „Ognistego Lisa”. Jedne koncentrują się na prywatności i anonimowości, inne – na wydajności, oszczędności zasobów użytkownika.

Poza ww. warto jeszcze wspomnieć o takich jak…

1. „Konqueror” – oparty na silniku KHTML, Kod źródłowy jest całkowicie otwarty. Pełni także rolę managera plików, ale dostępny tylko dla Linuksa.

2. „Falkon” – oparty na silniku „Qt WebEngine”, w pełni otwarty kod. Młoda, wyjątkowo lekka przeglądarka. Z pewnością godna uwagi dla osób, których sprzęt nie radzi sobie z innymi. Pod tym względem, warto również rozważyć „Pale Moon”, ale nie są to jedyne, które liczą się z zasobami użytkownika.

3. „Safari” – oparta na silniku „WebKit”. Choć jej „WebKitb

jest w pełni otwarty, to sama przeglądarka już taką nie jest.

Z uwagi na niezadowalającą stabilność lub – czasem – przestarzały silnik, albo znacząco ograniczoną funkcjonalność, pominąłem wiele innych, mało popularnych przeglądarek. Warto jednak mieć świadomość, że to, co tutaj wymieniłem, nie jest końcem możliwości. Poza tym wciąż powstają nowe silniki i nowe przeglądarki.

Ciasteczka (cookies)

Ciasteczka to zwykłe pliki tekstowe, które mogą przechowywać dowolne informacje. No, może nie takie zwykłe, ponieważ mogą również posłużyć do wstrzykiwania złośliwego kodu, czego nie da się powiedzieć np. o notatkach. Tworzone są przez przeglądarkę na polecenie serwera. Dostęp do nich i możliwość edycji, mają skrypty po stronie serwera i po stronie klienta (typowym klientem jest przeglądarka). Dostęp ten podlega pewnym rygorom, które zależą od zabezpieczeń strony i ustawień użytkownika. Aby wyrobić sobie opinię w sprawie wpływu, jaki mają ciasteczka na prywatność, rozważmy kilka przykładów.

Dla zobrazowania podawanych rozmiarów porównajmy je z rozmiarem niniejszego artykułu, zapisanego w formacie .txt. Ciasteczka, zwykle zapisywane są w pliku bazy danych (.sqlite), ale skonwertowałem je do .txt, aby nie było niedomówień. Zatem cały ten artykuł ma rozmiar 29,7 KB. Moje ciasteczka jako niezalogowanego użytkownika portalu „Wolne Media” mają rozmiar… 0 B. Więc nie jest to nawet ułamek kilobajta tylko czyste, okrągłe zero. Magazyn przeglądarki raportuje jednak 4 MB danych, które najprawdopodobniej są pamięcią podręczną, pozwalającą na szybsze ładowanie stron WordPressa. Aby porównanie było kompletne, sprawdziłem także serwis „Ruble”, na którym odwiedziłem najpierw kanał dobrze znanego nam Marmirowa i przeszedłem na stronę główną, którą przewinąłem kilka razy, aby wczytać trochę miniatur. Efekt? Zero ciasteczek, zero innych danych. A ile informacji

zgromadził mój „Proton Mail” z kontem wypchanym listami? Znalazłem 14 plików cookies o łącznym rozmiarze 18,8 KB. Dużo? Z pewnością niemało, ale same ustawienia usług oferowanych przez Protona muszą trochę zajmować. Nie zachował żadnych danych w pamięci podręcznej, co spowalnia wczytywanie, ale też wzmacnia prywatność.

No to teraz zajrzyjmy na „YouTube” i „Gmaila” z Google. Jako zalogowany użytkownik „YouTube’a”, rozmiar zachowanych danych wynosi u mnie 11,6 MB, natomiast same ciasteczka to 173 pliki o łącznym rozmiarze 325,4 KB, ale jako niezalogowanemu użytkownikowi „YouTube’a” zaserwowało mi 37,2 MB danych, z których 6 plików było ciasteczkami, ale już darowałem sobie dokładne badanie, jakiego rodzaju są to dane. Warto zaznaczyć, że przeglądarka nie wczytała żadnych miniatur, bo przy moich ustawieniach „YouTube” wyświetla tylko lewy panel i pustą stronę, zachęcając do użycia wyszukiwarki, zanim wyświetli coś więcej. Natomiast jako zalogowany użytkownik „Gmaila”, gdzie mam tylko puste konto a z wyszukiwarki nie korzystam, trzyma w mojej przeglądarce 15,3 MB danych. Więcej niż „YouTube”.

Podsumujmy:

– „YouTube”: 11,6 MB danych (zalogowany) i 37,2 MB danych (niezalogowany);

– „Rumble”: brak jakichkolwiek danych (niezalogowany);

– „Gmail”: 15,3 MB danych (zalogowany);

– „Proton Mail”: 18,8 KB i tylko ciasteczka.

– „Wolne Media”: 4 Mb danych (niezalogowany) i 0 B ciasteczek (niezalogowany);

– „YouTube”: 325,4 KB samych ciasteczek (zalogowany);

– niniejszy artykuł: 29,7 KB.

Google zastrzega sobie możliwość przetwarzania tych danych i

ostatecznie musimy im wierzyć na słowo, że nie zostaną odsprzedane lub udostępnione w inny sposób. Zgadzając się na warunki korzystania z usług Google, zgadzamy się wprost na udostępnianie naszych danych, podmiotom zależnym Google. Wszystko oczywiście okraszone zapewnieniami, zasadami, które mają świadczyć o trosce Google o naszą prywatność. Nawet jeśli weźmiemy to za dobrą monetę, nie mamy zielonego pojęcia, kto jest podmiotem zależnym, czy innym „kooperantem" tego giganta. Jednakże warunki, na które wyrażamy zgodę, stale ulegają zmianie. Znakomity moment na przemycenie kolejnych „ułatwień" dla Google, w inwigilacji użytkowników i udostępniania danych. Mało tego, szacuje się, że 50 do 60% wszystkich stron internetowych, implementuje narzędzie „Google Analytics", co przekłada się na 800 mln stron (dane za rok 2023). Wśród stron o najwyższej liczbie odwiedzin, odsetek ten sięga nawet 70 do 80%. Zatem jakby mało było zbierania danych z takich usług jak serwis „YouTube", wyszukiwarka „Google", poczta „Gmail" i wiele innych, jesteśmy przez nich śledzeni na większości odwiedzanych stron.

Pamięć podręczna przeglądarki (cache)

Może przechowywać znacznie więcej informacji niż ciasteczka i może obejmować takie dane jak: obrazy, skrypty, arkusze stylów, treści offline, preferencje użytkownika. Dostęp do tych danych nie jest już tak ściśle regulowany jak w przypadku ciasteczek i może tam zajrzeć praktycznie każdy. W przeglądarce, której używam wyłącznie do „YouTube'a" i „Gmaila", rozmiar przechowywanych danych wynosi 1 GB. Wspaniała kopalnia wiedzy o użytkowniku na każdy temat. Identyczna sytuacja ma miejsce w przypadku historii, ale nie należy ich utożsamiać. Czyszczenie danych przeglądania może, ale nie musi obejmować obu. Do historii przeglądania, JavaScript ma praktycznie nieograniczony dostęp. Z pamięcią podręczną jest niewiele lepiej, ponieważ nowoczesne

przeglądarki zapewniają w tym celu API (Application Programming Interface), z pewnymi ograniczeniami, ale nie są one tak restrykcyjne, jak w przypadku ciasteczek.

Skrypty

Można je podzielić na dwa gatunki: skrypty po stronie serwera i skrypty po stronie klienta (przeglądarki). Po stronie serwera są to głównie: PHP, Java, Python i kilka innych, mniej popularnych. Po stronie klienta, działa wyłącznie JavaScript i tak pozostanie jeszcze bardzo długo. O ile na skrypty po stronie serwera nie mamy żadnego wpływu, to JavaScript możemy zablokować całkowicie. To oczywiście spowoduje, że niektóre strony mogą przestać działać zupełnie. Inne utracą część funkcjonalności, lub pogorszy się ich czytelność. Tylko proste strony, używające wyłącznie HTML, prostych CSS i skryptów po stronie serwera, pozostaną niezmienione.

JavaScript może brać udział w przetwarzaniu wszystkich, wcześniej wymienionych danych. Mało tego, często mogą same gromadzić dane o nas i naszym sprzęcie i przekazywać w sobie tylko znane miejsce. Mogą też edytować ciasteczka, podobnie jak serwer. Jakby tego wszystkiego było mało, dzięki JavaScriptowi możliwa jest cała gama ataków XSS (cross-site scripting), jeśli zabezpieczenia strony nie są wystarczające. Z pomocą ataku XSS, można uzyskać dostęp nawet do danych, które wydawały się być dobrze zabezpieczone.

Obrazki i pliki audio/wideo

Mogą zdradzić więcej, niż się wydaje. Poza oczywistym rozpoznaniem twarzy na fotografii skrypty mogą użyć systemów śledzenia wzroku. Metadane EXIF także mogą ujawnić wiele informacji, którymi niekoniecznie chcieliśmy się podzielić. Wraz z HTML 5 i wprowadzenia elementu <canvas>, niewinnie wyglądające animacje mogą stać się przyczyną wycieku danych na kilka sposobów.

1. Mogą śledzić aktywność użytkownika na stronie.

2. Przemycać dane, których nie sposób przekazać innymi kanałami (np. przez cookies).

3. Mogą być podatne na ataki XSS.

Na szczęście element <canvas>, w razie zablokowania JavaScript, staje się bezużyteczny, jako szpieg, ale animacji także nie będzie. Prawie tak samo wygląda problem plików audio/wideo. Ani <canvas>, ani ww. pliki same z siebie danych gromadzić nie potrafią, ale mogą je przenosić, jeśli zostaną w nich zapisane. W przypadku plików AV możliwości są jednak znacznie szersze niż <canvas>. Co gorsze, zbieranie danych może się odbywać poza przeglądarką, ponieważ takie pliki, można odtwarzać w całej masie aplikacji i to one mogą nam „wyciąć numer”.

Odciski palców

Dotyczą unikalnej kombinacji takich informacji, jak…

1. Typ i wersja przeglądarki.

2. Zainstalowane rozszerzenia i wtyczki.

3. Ustawienia systemowe.

4. Czcionki.

5. Rozdzielczość ekranu.

6. Język systemowy.

7. Zainstalowane skrypty.

Ustawienia systemowe, wymagają kilku słów wyjaśnienia, ponieważ nie dotyczą samej przeglądarki a całego systemu operacyjnego. Należą do nich: język systemowy, strefa czasowa, rozdzielczość ekranu, czcionki systemowe, ustawienia proxy.

Odcisk palca stanowi także zawartość pamięci podręcznej przeglądarki, z powodu jej unikalnej treści. Także historia przeglądania i pobierania plików. Elementy <canvas> w połączeniu z JavaScript, na podstawie unikalnych cech twojej przeglądarki, mogą wygenerować na stronie grafikę, której nie zobaczysz gołym okiem i ta grafika może stać się rodzajem identyfikatora.

Do tej samej kategorii należą również wzorce dostępu. Skrypt na stronie, może nie tylko uzyskać dostęp do pamięci podręcznej przeglądarki, ale także wykryć unikalny sposób, w jaki twoja przeglądarka zapisuje w niej dane. Np. pobieranie tych samych obrazków z określonej strony.

Powiadomienia „push”

To te wszystkie aktualizacje czegoś tam i alerty, które otrzymujesz na telefon, ale i na pulpit peceta. Mogą zbierać informacje o twojej aktywności online, nawykach korzystania z urządzenia, lokalizacji, czasie spędzonym na określonych stronach, kliknięcia i rozpowszechniać phishingowe linki. Po prostu ich unikaj. Wyłącz, a najlepiej nie używaj wcale. Nie zgadzaj się na żadne powiadomienia i już.

Trwa „wyścig zbrojeń”. Po jednej stronie występują użytkownicy dbający o swoją prywatność, przeglądarki, które chcą chronić swoich użytkowników a po drugiej stronie – mnóstwo podmiotów. Od rządów, ich służb specjalnych począwszy, przez dostawców usług internetowych i korporacje, na pryszczatych hakerach z zatęchłych piwnic skończywszy. Przy czym ci ostatni, są najmniej szkodliwi. Zarówno zabezpieczenia, jak i metody ataku, ciągle się zmieniają a żadne z nich, nie są doskonałe. To ciągła gra na przechytrzenie. Skuteczne dziś metody obrony lub ataku nie będą takie jutro. W grę wchodzi nie tylko skuteczność stuprocentowa. Metody usiłujące np. określić rozmiar naszego monitora, zwykle dają tylko obraz przybliżony. Z drugiej strony, mechanizmy obronne, nie są w stanie

całkowicie zapobiec wykryciu tego parametru. W odniesieniu do innych danych sytuacja jest analogiczna i – jak widać – obszar, na którym może dojść do naruszenia prywatności, jest ogromny. W związku z tym, twierdzenie jakoby skrypty nie stanowiły problemu, jest – delikatnie mówiąc – mało rozsądne. Osoba, która koncentruje się na „wtopieniu w tłum", nawet jeśli używa „Tor Browsera", ale zaniedba którykolwiek z ww. tematów, jest podobna do uciekiniera chowającego się w tłumie, ale na całe gardło wrzeszczącego: „Tu jestem! Jestem Jozin z Bazin i właśnie ubrałem zielone majtki!". Cóż z tego, że takich wielu, skoro każdy jest łatwy do zidentyfikowania i namierzenia? Wystarczy tylko wybrać sobie cel i można bez problemu wyłuskać naiwniaka. Wtapianie się w tłum, jest tylko elementem prywatności czy anonimowości oraz bezpieczeństwa. Lepiej jednak wtapiać się w tłum faktycznie anonimowych, niż jeleni.

Jak się bronić?

Najprostsze jest korzystanie z trybu incognito tak często, jak tylko się da, ale to nie jest zbyt wygodne. Należy też mieć świadomość, że z trybu incognito w przeglądarce „Google Chrome", drwią nawet deweloperzy Google. Jeśli musisz jej używać, ogranicz się tylko do niezbędnych stron. Wszystkie inne odwiedzaj z innej przeglądarki. Do tego tematu wrócimy za chwilę.

Większość przeglądarek umożliwia usuwanie tych wszystkich danych w chwili zamykania przeglądarki (sesji). Można też wybrać okres, który obejmie usunięcie danych. Polecam jednak usuwać je „od początku", aby nikt nie grzebał nam w cache przeglądarki. Ponieważ większość z nas, zechce zachować takie dane jak hasła i/lub ustawienia stron, można pozostawić je odznaczone, pamiętając, że jest to dodatkowy element, potencjalnie ułatwiający identyfikację lub nawet kradzież hasła. Warto pochylić się nad dokładnym wyborem danych objętych usuwaniem i dopasować go do własnych potrzeb.

Zazwyczaj, domyślnym ustawieniem ciasteczek, jest zezwalanie na zapisywanie wszystkich. Jeśli tak to zostawimy, złośliwa strona będzie miała możliwość ustawienia ciasteczka, które umożliwi dostęp do zebranych informacji, komu tylko zechce, a zwłaszcza – wszystkim. Trudno sobie wyobrazić gorszą sytuację. Każdy skrypt, zarówno po stronie serwera, jak i po stronie przeglądarki, będzie mógł zrobić z danymi, co tylko zapragnie. Można zablokować obsługę wszystkich ciasteczek, ale to może ograniczyć funkcjonalność niekrócących stron. Optymalnym rozwiązaniem jest zablokowanie ciasteczek spoza serwera, lub inaczej zwanych „ciasteczkami stron trzecich", czy też „ciasteczkami innych firm". W takiej sytuacji przeglądarka zezwoli stronom tylko na dostęp do własnych ciasteczek. Dzięki temu złośliwe ciasteczko będzie mogło być odczytane tylko przez swoją, złośliwą stronę. Mimo wszelkich zabezpieczeń wciąż istnieje ryzyko wycieku informacji na kilka, różnych sposobów. Pominę ich opis, bo to nie kurs dla hakerów.

Jeśli usuniemy wszystkie ciasteczka, natrafimy na pewien problem. Będziemy zmuszeni do każdorazowego potwierdzania naszej zgody na ustawienie ciasteczka, a to, może być uciążliwe. Rozszerzenie „I don't care about cookies" automatycznie zamyka te uciążliwe powiadomienia. Niestety, zostało przejęte przez Avasta, co wzbudziło dość szeroki sprzeciw. Niemal natychmiast powstał fork, który, który nazywa się „I still don't care aobut cookies" i to rozszerzenie polecam tym, którzy chcą usuwać dane po każdej sesji (lub częściej).

Rozszerzenia przeglądarek internetowych

Także i one mogą stanowić zagrożenie. Głównym „materiałem"używanym przy ich tworzeniu jest… tak zgadliście – JavaScript. Udział biorą także: HTML, CSS, skrypty/języki po stronie serwera, oraz API przeglądarki. Trzeba więc uważać, co

się instaluje jako rozszerzenie i kontrolować prawa, jakie im się przyznaje w tym procesie. Jednakże istnieje całkiem sporo, bardzo przydatnych i godnych zaufania rozszerzeń:

1. „uBlock Origin” – blokuje reklamy i wiele elementów śledzących. W odróżnieniu od „AdBlocka” jest bardzo wydajny i nie obciąża procesora nadmiernie. Dlatego polecam „uBlock Origin”, zamiast „AdBlocka”. Pozwala tworzyć reguły dla różnych elementów. Zauważ, że reklamy to nie tylko dokuczliwe byty. Same w sobie bywają „trackerami”.

2. „Privacy Badger” – ceniony bloker elementów śledzących.

3. „I still don’t care about cookies” – automatycznie zamyka powiadomienia o ciasteczkach.

4. „NoScript” – pozwala blokować skrypty i – podobnie jak „uBlock” – wyznaczać dla nich własne reguły.

Dobrych i przydatnych rozszerzeń jest znacznie więcej, ale zajęłoby to zbyt wiele miejsca, a nie wszystkie są konieczne. Nawet ww. nierzadko są już wbudowane w przeglądarkę. Tak jest np. w przypadku „Tor Browsera” i „NoScriptu”. Również „uBlock” nie będzie konieczny w przypadku „Brave”. „Privacy Badger”, choć znakomity, jest już powszechnie zastępowany przez natywne rozwiązania przeglądarek. Z powyższej listy, nieodzowny wydaje się jedynie „I still don’t care about cookies”. Mimo to warto pamiętać o tych rozszerzeniach, bo wiele zależy od samej przeglądarki. Co więcej, można poszukać dalszych. Np. przydatne mogą być rozszerzenia, usuwające dane natychmiast po zamknięciu karty. To może być coś, co zdecyduje o utracie prywatności lub anonimowości, bo zanim zamkniemy przeglądarkę, nasza historia przeglądania, pamięć podręczna i magazyn ciasteczek może puchnąć w szwach, gdy cały świat ma uciechę, czytając o kolorze naszych majtek.

WebRTC (Web Real-Time Communication)

To technologia umożliwiająca świadczenie takich usług jak: komunikacja P2P w przeglądarce, udostępnianie ekranu, czaty, wideorozmowy, strumieniowanie, gry wieloosobowe i wiele innych. Tym razem, nie wchodzą w grę żadne, nowe zagrożenia. Jak ze wszystkim, tak i tutaj może dojść do wycieku adresu IP, lokalizacji, metadanych wszelkiego rodzaju, złośliwe oprogramowanie itd. Jeśli nie potrzebujesz takich usług, najlepiej wyłącz technologię WebRTC w przeglądarce, jeśli jest obecna. Zauważ, że wyłączenie JavaScriptu uniemożliwi ci korzystanie z WebRTC, ale też może nie zapewnić pełnego bezpieczeństwa.

W poprzednim artykule zastanawialiśmy się, jak przekazywać sobie identyfikatory komunikatora „Session”. Pisząc ten artykuł, przypomniałem sobie o prostej i skutecznej metodzie, której chętnie kiedyś używałem (kiedy miałem z kim). Otóż przeglądarka „Brave”, oferuje czat „Brave Talk”. To właśnie przykład technologii WebRTC. Znajdziesz ją na pulpicie „Brave”, w kartach, zwykle po prawej stronie. Uaktywnij tę kartę i kliknij „Rozpocznij połączenie”. Być może poprosi cię o udzielenie odpowiednich zezwoleń (domyślnie: na czas sesji), na które trzeba się zgodzić. Jeśli coś nie działa, jak trzeba, to musisz sprawdzić, czy masz włączoną obsługę WebRTC i czy nie blokujesz JavaScript. Jeśli wszystko pójdzie dobrze, to za chwilę pojawi się okno, gdzie – w lewym panelu – podasz swój pseudonim (Enter your name). Kliknij „Join meetingb i już możesz rozpocząć czat, rozmowę głosową, wideokonferencję, a nawet udostępnić ekran. Wszystko jest szyfrowane.

Aby skontaktować się z kimś, kliknij menu z trzema kropkami. Znajdziesz je u dołu ekranu, na wysuwanym pasku, po jego prawej stronie. Z menu wybierz „Invite people”. Ukaże się okienko z Twoim identyfikatorem. Wystarczy na nim kliknąć (na identyfikatorze), aby go skopiować. Możesz go teraz przesłać

dowolnym, nawet publicznym kanałem. W zasadzie to samo możesz osiągnąć, klikając ikonę „Participants”. Kiedyś można było prowadzić konferencje ograniczone do czterech osób, ale teraz nie widzę żadnej informacji. Możliwe, że zrezygnowali z takiego ograniczenia.

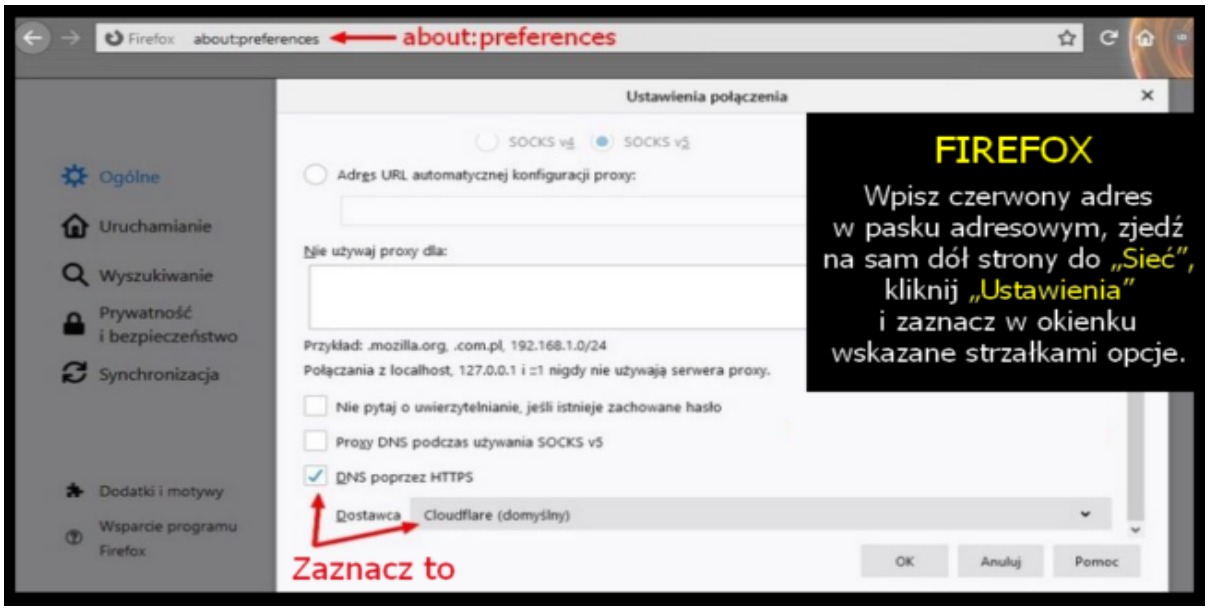
Połączenie jest bezpośrednie (P2P), czyli bez żadnych pośredników. Identyfikator będzie istniał tak długo, jak długo nie zakończysz rozmowy, lub rozmów. Zamknięcie Brave talk, bezpowrotnie niszczy identyfikator i wszystkie rozmowy, które miały miejsce w trakcie sesji. Nie ma niczego, na czym można by je zapisać. Żadnych logów ani archiwów. Jedyną wadą jest to, co teraz stanowi zaletę: nie ma możliwości zachowania identyfikatora. Każda rozmowa musi się zacząć od przekazania go komuś. Znakomicie nadaje się do przekazywania informacji, po których ślad ma zniknąć na zawsze.

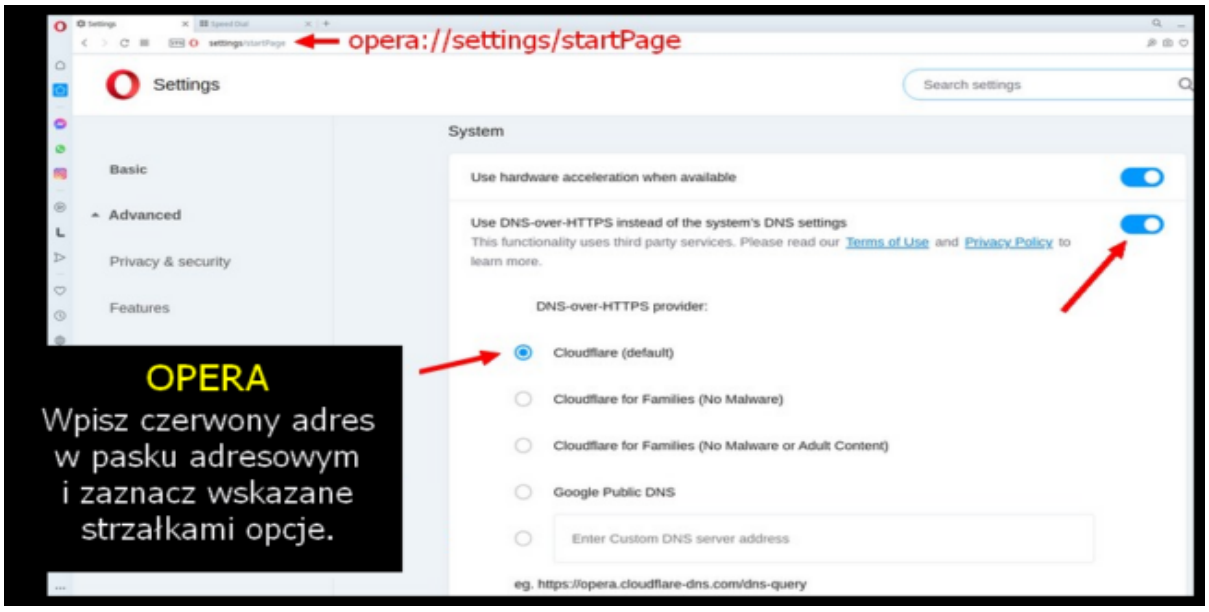
Szyfrowanie DNS

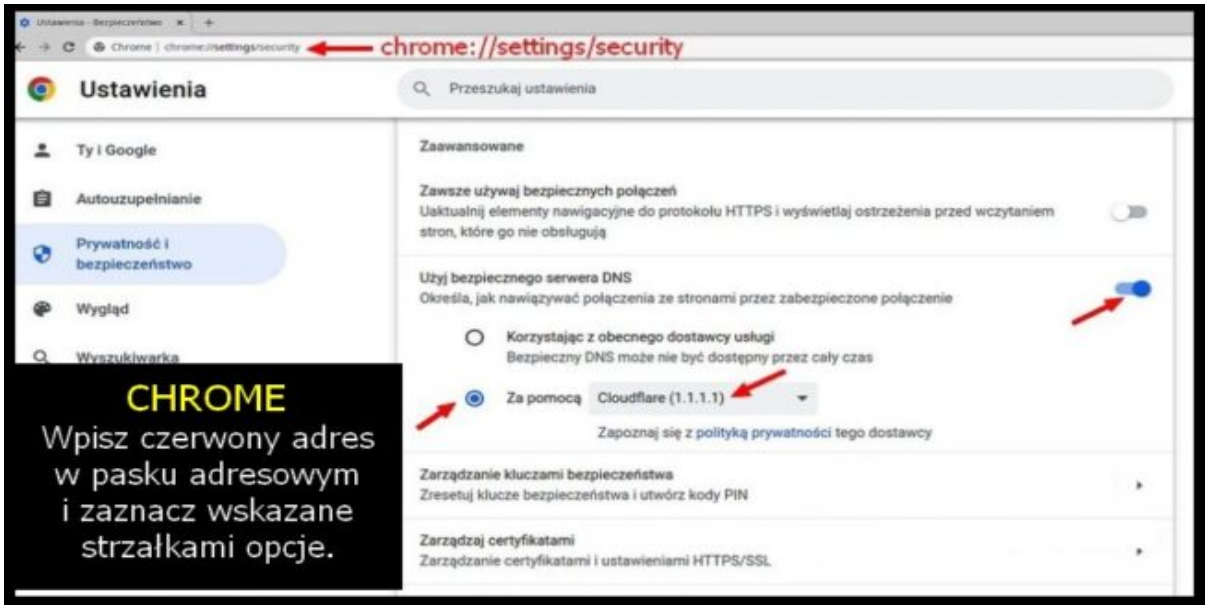
Kiedy chcemy się połączyć z jakąś stroną, wysyłamy żądanie do serwera nazw – DNS (Domain Name System). Tłumaczy on nazwę domeny, np. wolnemedia.net na adres IP i dopiero serwer obsługujący tę domenę, zaserwuje nam konkretną stronę. Problem w tym, że o ile komunikacja z serwerem WWW jest zazwyczaj szyfrowana protokołem https (SSL), o tyle rzadko szyfrowana jest komunikacja z serwerem DNS. Zatem nasze żądanie może zostać przechwycone przez osoby postronne. Wyciek wprawdzie dotyczy tylko metadanych, ale to żadna pociecha. Jeśli chcę utrzymać w tajemnicy moją obecność na „Wolnych Mediach” to guzik mi z tego, że komentarz, który tu chcę przesłać, będzie zaszyfrowany, skoro wiadomo, że o danej porze byłem w danym miejscu i przebywałem w nim określoną ilość czasu. Dlatego wartym zachodu może się okazać zaszyfrowanie naszej komunikacji z serwerem DNS. Całkiem niedawno wszystkie, albo prawie wszystkie wiodące przeglądarki udostępniają taką możliwość. Niestety, domyślnie jest zazwyczaj wyłączona. W „Firefoksie” można to włączyć przez: menu > Prywatność i

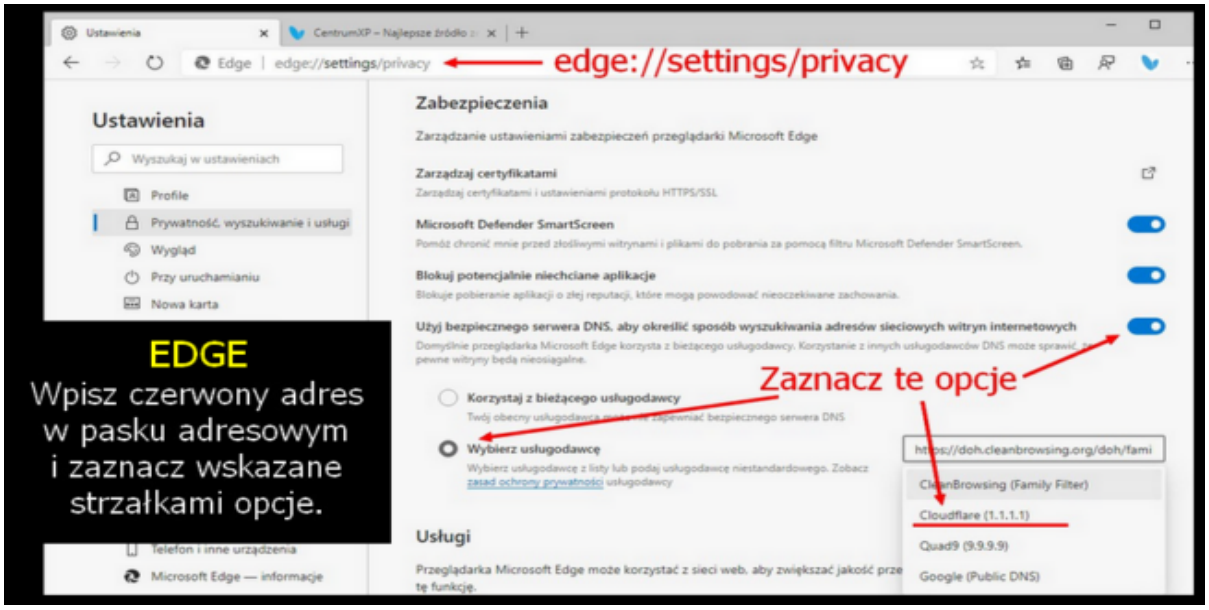
bezpieczeństwo (w lewym panelu) > przewiń do samego dołu i w sekcji „DNS poprzez HTTPS”, podpunkt „Włącz zabezpieczony serwer DNS”, ustaw „Zwiększona ochrona” lub „Maksymalna ochrona”. Na samym dole jednej z tych opcji, zobaczysz „Wybierz dostawcę”. W tej chwili widzę, że „Cloudflare” jest domyślnym DNS-em i to jest chyba najlepszy wybór. Jeśli masz inny jako domyślny, sugeruję ustawić „Cloudflare (1.1.1.1)”. Czasem jest to miejsce na te liczby „1.1.1.1” (dla „Cloudflare”) a czasem sama nazwa.

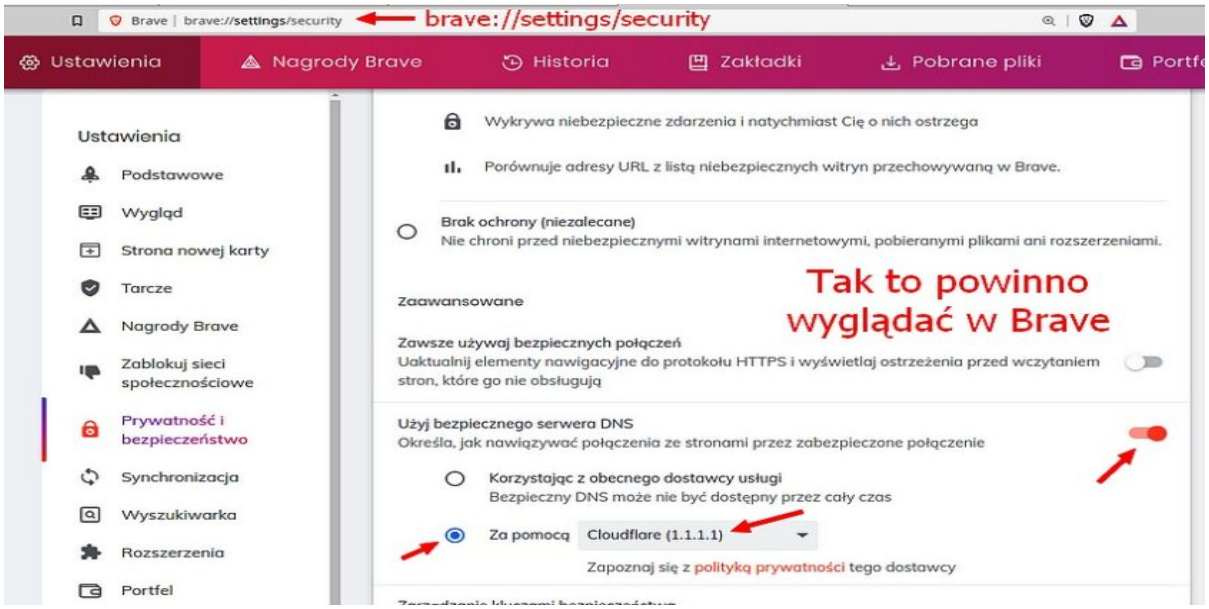
Kliknij na obrazki, aby je powiększyć.











To szyfrowanie nazywa się „DNS over HTTPS” (DoH). Można je

ustawić dla całego systemu, a nie tylko dla przeglądarek i to jest całkiem dobry pomysł. Niestety, może być skomplikowany lub wymagać odpowiedniej aplikacji, która zrobi to za ciebie. Nie chodzi tu o samą zmianę DNS, ale o wybór takiego serwera, który obsługuje DoH. Nie potrafi tego np. domyślny w Polsce DNS Orange, czy jak mu tam. Bonusem wynikającym z tej zmiany będzie ominięcie blokad DNS, czyli takich, jaka spotkała swego czasu „Wolne Media”.

Niektórzy argumentują tutaj, jakoby szyfrowanie DNS było bezsensowne, ponieważ zmieniamy tylko punkt, w którym dane mogą wyciekać. Poza tym dostawca (np. Oragne) i tak może zobaczyć, co robimy, więc zamiast jednego, wątpliwego podmiotu, w naszej komunikacji biorą udział już dwa. Pozwolę się z tym nie zgodzić. Po pierwsze: firma Cludflare jest bez porównania bardziej godnym zaufania podmiotem niż Orange, a po drugie, Orange – owszem – może zobaczyć, co robimy, ale zobaczy tylko, że wysyłam żądanie do „Cloudflare”, ale to, że proszę o adres portalu „Wolne Media”, jest już zaszyfrowane i zaszyfrowana będzie także odpowiedź serwera DNS. Problem pojawi się dopiero wtedy, gdy serwer, którego szukam, nie będzie miał szyfrowania. Dlatego warto zwracać uwagę na adresy stron, które powinny zawsze zaczynać się od „https”, a nie od „http”. Warto też ustawiać w przeglądarkach opcję, która nakazuje realizować tylko żądania „https”. O ile taka opcja istnieje w twojej przeglądarce. W przypadku „Firefoksa” jest ona nieco wyżej, niż opcje przed chwilą rozważane. Znajdziesz ją w sekcji „Tryb używania wyłącznie protokołu HTTPS” > „Włącz we wszystkich oknach”.

Znów o przeglądarkach

Z powodu wspomnianego „wyścigu zbrojeń”, nigdy nie wiadomo, co ani kiedy zawiedzie. Właściwie to żadne zabezpieczenia nie są doskonałe, ani żadna ich ilość. Zawsze trzeba liczyć się z tym, że prywatność zostanie naruszona. Aby zminimalizować możliwość szpiegowania, warto rozważyć używanie kilku

przeglądarek. Np. Dla konta „Gmaila” i „YouTube’a”, użyć przeglądarki „Opera”. To nic, że już ona sama próbuje nas wykiwać. Ustawienia domyślne można zmienić, a nawet jeśli tego nie zrobimy, i tak nie tracimy zbyt wiele, bo do niczego więcej nie będziemy jej używać. Google, jeśli chce, niech nas śledzi. Znajdzie tam tyle, ile i tak o nas wie, z aktywności na koncie. „Opera” oferuje także przeglądarkowy VPN. W cudzysłowie, bo to raczej tylko serwer proxy, ale efekt jest podobny. Trzeba też z nim uważać, bo domyślnie, włączona jest opcja, która pozwala pominąć ten VPN w połączeniach ze stronami firmy Google i pewnie kilkoma innymi stronami, które blokują „podejrzane połączenia”. Jeśli nie masz nad sobą litości, możesz tutaj użyć nawet „Google Chrome”.

Drugiej przeglądarki, sugeruję użyć do załatwiania spraw „biznesowych”. Mam tu na myśli takie rzeczy, jak bankowość internetowa, zakupy i czy nawet sprawy stricte zawodowe. Nic nie stoi na przeszkodzie, żeby dla każdej kategorii użyć osobnej przeglądarki. Tu polecałbym „Firefoksa”.

Za osobną kategorię uważam kontakty prywatne. Zapewne trzeba tu wliczyć te wszystkie „Facebooki”, „Instagramy” i co tam jeszcze, bo to znów jest ta sama rodzina szpiegów i dobrze, żeby kisiła się we własnych danych. Dla tej kategorii odpowiednie wydają się „Waterfox”, „LibreWolf” czy „Mullvad Browser”.

Ostatnia, ale może najważniejsza to przeglądarka do codziennego użytku. Być może tutaj można się o nas dowiedzieć najwięcej. Przeglądanie niegrzecznych stron, jak np. „Wolne Media”, powinno się znaleźć w tej kategorii. Dla tej kategorii, za najlepszą uważam „Brave” z uwagi na jej domyślne ustawienia bezpieczeństwa, łatwość szybkiej zmiany tych ustawień, ogrom możliwości konfiguracyjnych i wiele ciekawych funkcjonalności, które mogą się przydać przy takim użytkowaniu.

Podział ten sprawi, że zadbamy zarówno o prywatność,

bezpieczeństwo i anonimowość, ale też będzie to wygodne. Będziemy mogli sobie pozwolić na pozostawanie zalogowanym tu czy tam, a jednocześnie nie obawiać się, że wycieknie coś naprawdę ważnego. W ten sposób, za każdym razem, gdy uruchomimy przeglądarkę „ogólną”, będziemy kimś nowym dla elementów szpiegujących. Jedyne co będzie świadczyło o naszej tożsamości to adres IP, bo np. „Brave” potrafi zacierać także odciski palców. Nie tylko „Brave”. W tej chwili już wiele przeglądarek wprowadza podobne zabezpieczenia. Zatem IP jest tym, co może nas zdradzić i tu, wkracza sieć VPN.

VPN (Virtual Private Network)

Przypuszczam, że nie trzeba nikomu wyjaśniać, o co chodzi, więc tylko powiem, że Proton Mail, udostępnia prawdziwy VPN za darmo, ale z ograniczonym transferem. Jeśli chcesz płacić za VPN, to znajdziesz całkiem sporo, dobrych usług tego rodzaju. Jeśli chcesz wszystko za darmo, co uważam za rozsądną cenę, użyj wspomnianego VPN „Opery”. Czego by o niej nie mówić, pozwala ukryć adres IP. Tylko pamiętaj, aby wyłączyć opcję rezygnowania z VPN, gdy korzystasz z usług Google. Wtedy, zamiast myśleć, że się chronisz, po prostu nie nawiążesz połączenia i otrzymasz możliwość zadecydowania co z tym zrobić.

Alternatywą dla VPN może być zwykły serwer proxy. Trzeba tylko znaleźć jakiś przyzwoity, co może okazać się problematyczne. Najczęściej, oferowany poziom anonimizacji jest niski, serwery bywają powolne, bardzo często znikają i co chwilę trzeba szukać nowego. Przed użyciem, dobrze jest sprawdzić, czy faktycznie ukrywają nasz adres IP. W tym celu sprawdź swój adres IP np. na tej stronie, po czym wróć na nią, przez proxy a będziesz wiedzieć, co trzeba.

Jeśli VPN potraktujesz jako sposób na prywatność, a nie na anonimowość, będzie to bardzo dobre rozwiązanie, które zamyka naszą pulę przepisów. Zamyka, bo VPN traci sens, jeśli nie

zadbasz o prywatność w sposób, opisany we wcześniejszych punktach tego artykułu. Na niewiele się zda, ukrywanie IP, jeśli pozwalasz się panoszyć reklamom, nie masz kontroli nad ciasteczkami, historią i pamięcią podręczną a skrypty, robią z ciebie serfującą tablicę informacyjną. Niemniej, nie pozwól się przytłoczyć. Nie każde z tych rozwiązań jest konieczne w każdej przeglądarce. Wiele zależy od Twoich preferencji, sposobu, w jaki korzystasz z internetu i używanego oprogramowania.

To tyle na dzisiaj. Udało mi się jedynie prześlizgnąć po powierzchni, a kilka tematów pominąłem, a kto wie, o czym zapomniałem. Może kiedyś znów do tego wrócimy a ty, będziesz już bardziej doświadczonym użytkownikiem. A może dokończysz za mnie? To byłby najlepszy scenariusz.

Autorstwo: Zapluty Karzeł Reakcji
Źródło: WolneMedia.net