Sprostowanie w sprawie szyfrowania DNS

13 lipca 2024

Z przykrością stwierdzam, że z powodu mojej naiwności i – co za tym idzie – niedbalstwa, oraz niedouczenia, wprowadziłem czytelnika w błąd. Szyfrowanie łączności z DNS, za pomocą HTTPS (DoH), nie daje takiej anonimowości, o jakiej pisałem w poprzednim artykule.

Moja opinia brzmiała tak: „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”.

Wypowiedź ta była prawdziwa tylko częściowo. Nie dołożyłem należytych starań, aby przyjrzeć się problemowi dokładnie i samodzielnie. W efekcie zaufałem ekspertom i chociaż miałem pewne podejrzenia, wszystkie, najmądrzejsze czaty, systematycznie wybijały mi z głowy możliwość wycieku pewnych danych. Nie byłby to ani pierwszy raz, kiedy próbowały mnie oszukać lub coś przede mną ukryć. Tym razem się udało.

W rzeczywistości sytuacja wygląda tak, że już po faktycznie tajnym otrzymaniu adresu domeny, dochodzi do negocjacji TLS, pomiędzy moją przeglądarką a serwerem strony. W tym momencie ISP (np. Orange) rzeczywiście może zobaczyć adres domeny i

będzie go widział z każdym następnym żądaniem, nawet do tej samej domeny. Tym, czego nie zobaczy, będzie treść przesłana przez stronę. Przy obecnym poziomie cenzury i inwigilacji marna to dla nas pociecha. Oczywiście możesz wierzyć w zapewnienia, że ISP szanuje twoją prywatność i nigdy nie będzie zbierał danych na twój temat. Jak już kilkakrotnie wspominałem, jestem naiwniakiem, ale nie aż takim.

Nie oznacza to jednak, że DoH jest całkiem bezużyteczne. Obciąża jednak procesor i spowalnia cały proces. Nie są to wielkie straty, ale dla niektórych użytkowników mogą mieć znaczenie. Ostatecznie skórka może nie być warta wyprawki. Musisz samodzielnie zdecydować, czy szyfrować DNS, czy przywrócić domyślny, rezygnując z bezpiecznego.

Fakt, że się myliłem, nie oznacza również, że osoby, które mi na to zwróciły uwagę, są nieomylne. Skoro jednak prostuję swój błąd, wyprostuję też inne zarzuty.

Open-source

Rzekomo open-source nie jest żadnym kryterium w temacie zaufania, z powodu ogromu kodu, który trzeba by analizować, co jest ponad ludzkie możliwości. Taka opinia świadczy tym razem o niedouczeniu jej wyraziciela. Cały ten kod, nie został napisany wczoraj. Był pisany etapami, przez całe lata i nieustannie analizowany, poprawiany. Z gotowego produktu, wylicza się sumę kontrolną, podpisuje cyfrowo i obydwa parametry przekazuje użytkownikom, aby mieli pewność, że nic nie zostało w nim podstępnie zmienione. Jak to działa na innym poziomie, pokazuje wideo, które dołączyłem w artykule o anonimowości.

Najwyraźniej niektórzy go nie obejrzeli, albo nie byli w stanie pojąć. Należy też zrozumieć, że nie ma potrzeby analizowania np. całego jądra Linuksa. Wystarczy wybrać interesujący fragment i tylko jemu się przyjrzeć. Trzeba się „tylko” na tym znać. Te same osoby, przejawiają zadziwiającą

zdolność do nagłej zmiany poglądów. W jednym miejscu open-source nie jest godne zaufania a w drugim, godną zaufania jest tylko przeglądarka „Firefox”. Dlaczego? Mogę tylko zgadywać, że z powodu pełnej otwartości kodu źródłowego. Zapewne ważnym powodem jest też fakt, że z tego samego kodu, korzysta „Tor Browser”. Ale ta przeglądarka wprowadza swoje zmiany i poprawki. Nie jest „Firefoksem”, choć nazwy plików wyglądają podobnie.

Firefox

Zostałem też zasypany m.in. żądaniami uzasadnienia i – zapewne – udowodnienia każdej opinii, która podważa bezgraniczną wiarę w zespół Mozilli (Firefoksa), co do ich intencji, zasad, tudzież moralności. Zatem podaję kilka interesujących faktów:

1. Wieloletnie stręczenie „Google” i „Yahoo”, jako domyślnej wyszukiwarki. Mimo że były dostępne inne, mniej kontrowersyjne. W oczywisty sposób chodziło o pieniądze, ale czy to mało? Czy możemy być pewni, że tylko na tym się skończyło?

2. W roku 2020 Mozilla wyrzuciła dyrektora ds. marketingu, Jessiego Jamesa Arona, ponieważ na „Twitterze” pozwolił sobie na taki post: „BLM jest ruchem białych supremacji przebranym za ruch o sprawiedliwość rasową”. Nie miało to żadnego związku z Mozillą i nawet początkowo był przez nią broniony. Ostatecznie jednak kierownictwo uległo naciskom i został zwolniony z pracy.

3. W roku 2014 współzałożyciel „Firefoksa” i ówczesny dyrektor generalny, został zwolniony za to, że złożył całkowicie prywatną darowiznę na rzecz jakiegoś ruchu pro life. Wartości, jakie wówczas promowała Mozilla, obejmowały silne zaangażowanie na rzecz „równości płci i praw osób LGBTQ+”. Darowizna została uznana jako sprzeczna z tymi wartościami. Wtedy, na całe lata porzuciłem „Firefoksa”, bo „wartości” LGBTQ+ z przyległościami, nie są czymś, pod czym bym się

podpisał. Wyrzucałem soft za mniejsze przegięcia. Np. Drupala, gdy zaczął świecić ukraińską flagą. Robił to raczej z głupoty i w dobrej wierze, niż z fałszu, więc gdy flaga zniknęła, wrócił i Drupal.

4. Zbieranie danych telemetrycznych przez „Firefoksa”, jest często krytykowane przez użytkowników, nastawionych na prywatność. Stąd wiele forków „Firefoksa”, które właśnie na ten aspekt kładą szczególny nacisk.

Niech każdy sam oceni, czy chce wspierać tego rodzaju organizację. Jeśli o mnie chodzi, to akceptuję obecny stan rzeczy, ale stosuję zasadę ograniczonego zaufania. Zresztą, tę zasadę stosuję wobec każdej przeglądarki. Bardzo mało jest takich, przeciw którym nie jestem w stanie wysunąć jakiegoś zarzutu, ale to znów może wynikać z mojego lenistwa.

Cloudflare

Rzekomo Cloudflare jest jednym z najgorszych wrogów… czegoś tam. To z powodu blokowania dostępu do niektórych stron z sieci Tor. To nic, że Cloudflare udowodniło swoją wyjątkową troskę o użytkowników. Nieważne też, że oferuje całą gamę usług, związanych z bezpieczeństwem i to klient, czyli strona, decyduje o sile tych zabezpieczeń. Nie jestem paranoikiem, więc niezbyt często korzystam z „Tora”. Może dlatego dotąd spotkałem tylko jedną stronę, do której nie mogłem się dostać z „Tora” nawet z mostkiem. Nie mam problemu ani z „Google”, ani „YouTube” czy „Infowarsem”, które ma prawdziwe powody bronić się przed atakami. Nie mogę się dostać na polską stronę, porównywalną z „Wolnymi Mediami”, choć tam nie ma niczego, co uzasadniałoby tak potężne zabezpieczenia. Co gorsze, ostatecznie nie ma tam też niczego takiego, co by uzasadniało odwiedzanie tej strony w ogóle. Ale zabezpieczenia są silniejsze niż gdziekolwiek. Oczywiście każdy ma prawo się bać ataków i bronić przed nimi. Nawet jeśli obawy są przesadzone, ale to jego sprawa, a nie „walka Cludflare z

Torem”.

Jak Cloudflare udowodniło swoje żelazne zasady?

1. W roku 2017 firma odmówiła ujawnienia danych użytkowników, powiązanych z jakimś ruchem „alt-right” na ich platformie. Nie wiem co to za ruch, ale pomimo nacisku rządu USA, nie ugięła się, twierdząc, że bez nakazu sądowego, nie ma obowiązku cenzurowania treści ani ujawniania danych użytkowników. Oczywiście rząd USA, mógłby ich nękać procesami i doprowadzić do upadku. A jednak to on się poddał, a nie Cloudflare. Tego nie można powiedzieć o żadnym dostawcy VPN.

2. W roku 2019 Cloudflare chroniło „WikiLeaks” przed atakami DDoS. Nie wiem, kto naciskał, ale wiadomo, jaka śmierdząca jest to sprawa. Cloudflare znów pozostała nieugięta i oznajmiła, że ma prawo do ochrony dostępu do informacji wszystkich użytkowników, niezależnie od ich poglądów.

3. W roku 2020 Cloudflare stanęło tym razem po stronie BLM, co uważam za znakomity dowód ich bezstronności. Pomimo nacisków organów ścigania, nie zostały ujawnione żadne dane, które mogłyby narazić protestujących.

I to jest ten „zbrodniarz”, czyhający na naszą wolność słowa, prywatność i podobne wartości? Cóż, gdybym mógł w ogóle zrezygnować z usług Orange i korzystać wyłącznie z Cloudflare, to niewątpliwie bym to zrobił. Byłbym skłonny nawet uwierzyć na słowo, że oni mnie nie zdradzą, choćbym przeskrobał coś poważnego. Zapewne padnie tradycyjne pytanie o źródła. Odpowiem więc: w dobie sztucznej inteligencji, potężnych wyszukiwarek i tematów, które nie są szczególnie cenzurowane, takie żądanie zakrawa poważne zaburzenia zdolności poznawczych, albo zwykłą szykanę. Ostatecznie żadne źródło nie okaże się „wiarygodne”, a ja znów utknę na całe godziny, by udowodnić, że nie jestem wielbłądem. Co oczywiście mi się nie uda. Jakżeby inaczej? Zatem: kto chce to zweryfikować, niech się sam pofatyguje. Reszty nie będę komentował.

Podsumowując: nadal polecam szyfrowanie DNS i sam je zachowuję, pamiętając, że nie gwarantuje anonimowości a jedynie poprawę prywatności, o czym zresztą był cały artykuł. Polecam też „Cludflare” z całym przekonaniem i sugeruję zdrową nieufność także wobec „Firefoksa”.

Autorstwo: Zapluty Karzeł Reakcji
Źródło: WolneMedia.net