

Kradzież danych w sieci Tor

<http://ipsec.pl/kradziez-danych-w-sieci-tor.html>

Dan Egerstad z Deranged Security ujawnił szczegóły eksperymentu, w wyniku którego niedawno upubliczniono loginy i hasła kilkudziesięciu ambasad i innych instytucji rządowych z całego świata. Informacje te zebrano podsłuchując ruch sieciowy, wychodzący z serwerów Tor.

Sieć [ja href="http://tor.eff.org/"](http://tor.eff.org/) zapewnia anonimowość nieporównywalną z żadnymi wcześniejszymi anonimizatorami - każdy pakiet w Torze przechodzi przez trzy węzły wybrane przypadkowo z bazy około dwóch tysięcy działających stale na całym świecie.

Z punktu widzenia klienta - np. przeglądarki WWW - Tor jest lokalnym serwerem proxy dostępnym przez protokół SOCKS. Ruch jest szyfrowany na trasie od klienta do pierwszego węzła, a także między wszystkimi kolejnymi węzłami. Ale odwołanie do strony HTTP oczywiście wyjdzie z ostatniego węzła Tor w postaci niezaszyfrowanej, bo niezaszyfrowany jest sam protokół HTTP, a ostatni węzeł zadziała tutaj w roli ostatecznego klienta HTTP.

Rola ostatniego węzła Tor jest więc kluczowa - jako jedyny na całej trasie ma on wgląd w niezaszyfrowaną treść sesji klienta. Fakt ten wykorzystał Dan Egerstad, właściciel Deranged Security - na kilku kontrolowanych przez siebie węzłach Tor zainstalował sniffer monitorujący niezaszyfrowane sesje POP3 i IMAP, wyłapujący w pobieranych mailach szczególnie interesujące słowa kluczowe ("gov, government, embassy, military, war, terrorism, passport, visa" itd). Sesje te były logowane i to właśnie przypisane do nich loginy i hasła Egerstad [ja href="http://www.derangedsecurity.com/deranged-gives-you-100-passwords-to-governments-embassies/"](http://www.derangedsecurity.com/deranged-gives-you-100-passwords-to-governments-embassies/) opublikował wcześniej na swojej stronie [ja href="http://www.derangedsecurity.com/deranged-gives-you-100-passwords-to-governments-embassies/"](#). Wyglądało to tak:

```
blockquote

```
Indian Embassy in Sweden 81.228.8.31 u81004859 Brdv8H5j Russian Embassy
in Sweden 81.228.11.36 u86119749 y9z8ApZp Kazakhstan Embassy in Russia 81.176.67.157 ak-
maral@kazembassy.ru 86rb43 i/pre i/blockquote;
```


```

W całej historii najbardziej zaskakujące jest to, że to administratorzy tych instytucji zasugerowali użytkownikom korzystanie z Tora. Zapewne po to, by uniknąć lokalnej inwigilacji w kraju, z którego łączą się do serwera. Niewybaczalnym błędem jest jednak niestosowanie szyfrowania SSL, które jest przecież dzisiaj standardowo obsługiwane przez większość klientów i serwerów POP3 i IMAP. Być może administratorom wydawało się, że Tor zapewnia szyfrowanie punkt-punkt, od klienta do serwera - tak jednak nie jest.

Egerstad na swoim blogu wyjaśnił, że podsłuchanych zostało w większości znacznie więcej haseł i loginów niż te 100 opublikowane na jego stronie. W rzeczywistości miały ich być "tysiące", co jest w pełni możliwe.

Podkreślmy więc jeszcze jeden raz - Tor gwarantuje anonimowość, ale Tor nie gwarantuje prywatności. Większość serwerów Tor prawdopodobnie nie podsłuchuje ruchu, ale takiej gwarancji nie mamy. Standardowy użytkownik nie ma wpływu na ścieżkę, jaką wędrują jego dane - trzy kolejne węzły są wybierane losowo. Każdy węzeł może być węzłem pośrednim (wtedy widzi tylko zaszyfrowane dane), albo węzłem końcowym (wtedy widzi oryginalną treść sesji użytkownika).

Co istotniejsze, każdy może uruchomić nowy węzeł Tor i podłączyć go do publicznej sieci. Także z intencją celowej inwigilacji lub kradzieży danych. Użytkownikowi nie przeszkadza to, jeśli oczekuje anonimowości, bo węzeł końcowy nie wie kto i skąd wysła dane. Ale jeśli w sesji Tor przesyłane są informacje wrażliwe (loginy, hasła, treść korespondencji) to krytyczną jest również ochrona poufności - i o to musi zadbać już sam użytkownik.

- [ja href="http://www.derangedsecurity.com/time-to-reveal"](http://www.derangedsecurity.com/time-to-reveal)
- [ja href="http://www.derangedsecurity.com/deranged-gives-you-100-passwords-to-governments-embassies/"](http://www.derangedsecurity.com/deranged-gives-you-100-passwords-to-governments-embassies/) DEranged gives you 100 passwords to Governments Embassies [ja href="http://www.derangedsecurity.com/deranged-gives-you-100-passwords-to-governments-embassies/"](#)