Tryb porno to ściema?

10 sierpnia 2010

Tryb prywatny (zwany często ze względu na swe najczęstsze zastosowanie trybem porno) to funkcja dostępna obecnie we wszystkich popularnych przeglądarkach internetowych, która w założeniu ma pozwalać użytkownikom na przeglądanie Internetu bez pozostawiania jakichkolwiek śladów na lokalnym komputerze. Wokół tej funkcji narosło wiele mitów i nieporozumień. Wielu użytkowników nowoczesnych przeglądarek uważa, że włączenie porno trybu zapewnia ich internetowym poczynaniom stuprocentową anonimowość przynajmniej w obrębie własnego komputera oraz lokalnej/domowej sieci komputerowej. Czy tak rzeczywiście jest?

Pierwszą powszechnie ignorowaną przeszkodą na drodze do osiągnięcia w pełni anonimowego (z punktu widzenia lokalnego systemu komputerowego) surfowania jest fakt, że typowe przeglądanie stron internetowych pozostawia ślady nie tylko w samej przeglądarce, ale również w innych zakamarkach naszego systemu operacyjnego. Częściową historię przeglądania można odzyskać z pamięci podręcznej DNS (na jej wyczyszczenie pozwala polecenie ipconfig /flushdns).

Warto również zawsze pamiętać, że ruch sieciowy z naszego komputera, zanim trafi do Internetu, najczęściej przechodzi jeszcze przez jakieś urządzenia sieciowe (przełączniki, domowy lub firmowy router, itd.). Tego typu urządzenia bardzo często umożliwiają skuteczne śledzenie internetowych poczynań poszczególnych komputerów pracujących w sieci LAN, na co oczywiście stosowanie trybu prywatnego również nie ma jakiegokolwiek wpływu.

Wiemy już więc, że nawet jeśli przeglądarka nie zdradzi naszych tajemnic, to intruz może poznać nasze internetowe poczynania na podstawie śladów pozostawionych przez nasz system operacyjny lub też analizując ruch w sieci LAN. Czy

jednak chociaż sama funkcja trybu prywatnego zaimplementowana w popularnych przeglądarkach rzeczywiście działa na tyle skutecznie, by przynajmniej tędy nie wyciekały nasze sekrety?

Niestety już na pierwszy rzut oka można zauważyć, że niektóre działania wykonywane w popularnych przeglądarkach w trybie prywatnym pozostawiają trwałe ślady. Żeby się o tym przekonać, wystarczy tylko w dowolnej przeglądarce dodać jakąkolwiek stronę internetową do Ulubionych/Zakładek. Stan Ulubionych/Zakładek zostanie trwale zmieniony, nasze działanie pozostawi więc trwały ślad w przeglądarce internetowej. Można powiedzieć, że jest to uzasadnione, gdyż jest następstwem świadomego działania użytkownika, moim zdaniem nie jest to jednak oczywiste. Na tym jednak nie koniec, z popularnych przeglądarek pracujących w trybie prywatnym potencjalnie wycieka o wiele więcej informacji.

Warto zastanowić się w tym momencie przez chwilę nad tym, w jaki sposób możliwe jest szczegółowe zbadanie skuteczności trybu prywatnego danej przeglądarki. Otóż moim zdaniem warto rozważyć dwie metody. Pierwszą jest po prostu ręczna analiza kodu źródłowego (jeśli takowym dysponujemy) w poszukiwaniu wszelkich fragmentów odpowiedzialnych za zapis informacji na dysku twardym i dokładna analiza działania tychże funkcji w trybie prywatnym. Drugą metodą może być np. porównanie stanu dysku twardego (w szczególności katalogów wykorzystywanych przez daną przeglądarkę) przed oraz po surfowaniu w trybie prywatnym. Wszelkie różnice będą oznaczać, że przeglądarka jednak dokonuje pewnych permanentnych zapisów informacji będąc w trybie porno.

Jeśli skorzystamy z jednej z powyższych metod, to okaże się, że wszystkie cztery najpopularniejsze przeglądarki (Internet Explorer, Firefox, Chrome oraz Safari) niestety dokonują zapisów informacji mogących zdradzić nasze działania w trybie prywatnym. Z dokładnych badań prowadzonych w tym zakresie wynika, że przeglądarki m.in. powszechnie zachowują w trybie prywatnym kopie certyfikatów, klucze SSL oraz zależnie od

okoliczności oraz konfiguracji również inne informacje. Dane te po zakończeniu prywatnego surfowania nie są usuwane i pozwalają potencjalnemu intruzowi na skuteczne określenie (przynajmniej częściowej) historii przeglądania.

Poważnym zagrożeniem dla naszej prywatności są również rozmaite rozszerzenia, wtyczki i dodatki, tak powszechnie używane obecnie przez internautów. Praktycznie każdy z tego typu dodatków potencjalnie może w trybie prywatnym na własną rękę dokonywać zapisu informacji mogących się w przyszłości przyczynić do naruszenia naszej prywatności. O ile Internet Explorer oraz Chrome domyślnie wyłączają większość dodatków i rozszerzeń w trybie prywatnym, to już Firefox zezwala w takiej sytuacji na swobodną pracę wszystkich gadżetów…

Przyglądając się więc dokładniej spotykanym dziś w przeglądarkach trybom prywatnym, można dojść do wniosku, że funkcje te delikatnie mówiąc nie spełniają dobrze swego statutowego zadania. Dzieje się tak po części z winy twórców przeglądarek, a po części w wyniku występowania wielu różnych innych potencjalnych źródeł wycieku newralgicznych informacji. Nie bez znaczenia jest również niewiedza samych użytkowników, którzy często naiwnie wierzą w stuprocentową skuteczność trybu prywatnego i przeceniają jego możliwości. Na koniec zapraszam do wspólnego zastanowienia się nad potencjalnie najbardziej skutecznym sposobem na osiągnięcie najskuteczniejszego trybu prywatnego.

Autor: \m/ojtek
Źródło: Hard Core Security Lab