Jeśli korzystasz z zakładek w Internet Eksplorerze, Firefoksie lub innych przeglądarkach, możesz być poważnie zagrożony "tabnabbingiem". O nowym cyberprzestępczym i superskutecznym pomyśle na kradzież danych internautów poinformował właśnie na swoim blogu Aza Raskin, członek zespołu Mozilla Firefox.

Do ataku dochodzi przy zmianie zakładki w internetowej przeglądarce. Strona zawierająca złośliwy kod wykorzystuje moment, gdy Internauta skupia swoją uwagę na innej witrynie, by w tym czasie całkowicie zmienić swój wygląd. Po szybkiej transformacji cyberprzestępcza witryna wygląda jak popularne strony logowania, np. do poczty Gmail. Ponieważ zmianie ulega nie tylko sam wygląd witryny, lecz również ikona zakładki, bardzo trudno zorientować się, że jest to próba kradzieży tożsamości.

Phishing, tyle że jeszcze bardziej podstępny
"Mamy do czynienia z całkowicie nową i wyjątkowo wyrafinowaną wersją phishingu" - mówi Tomasz Zamarlik z G Data Software, producenta wysokiej klasy oprogramowania antywirusowego. "Tabnabbing na pionierskim przykładzie Gmail to jedynie wierzchołek góry lodowej. Zagrożeni są nie tylko użytkownicy kont pocztowych lecz przede wszystkim posiadacze internetowych kont bankowych czy użytkownicy portali społecznościowych. Straty wynikłe z zastosowania tej metody ataku na większą skalę mogą być trudne do przewidzenia".

Według Azy Raskina "nowe narzędzie daje cyberprzestępcom możliwość sprawdzenia na jakie strony loguje się użytkownik (np. Facebook, Citibank, Twitter). A zatem podmiana wyglądu strony i ikony w zakładce przeglądarki może być dopasowana indywidualnie. Co więcej: atak może stać się jeszcze bardziej niebezpieczny, gdy zamiast fałszywej kopii strony startowej użyty zostanie ekran informujący o wygaśnięciu sesji i automatycznym wylogowaniu. Byłoby to szczególnie skuteczne w przypadku bankowości internetowej."

Apel o ostrożność
Najbardziej narażeni na tabnabbing są użytkownicy Firefoxa i Internet Explorera. Safari oraz Chrome okazały się częściowo odporne na atak (np. w Safari ikona zakładki pozostaje niezmieniona). Z niewiadomych przyczyn, serwer na którym znajdował się blog Raskina dzień po ogłoszeniu tej wiadomości przestał działać. „Bezpieczną” demonstrację ataku można zobaczyć pod tym adresem: http://avivraff.com/research/phish/article.php?1250748237. Aby zadziałała, należy przejść do innej zakładki i odczekać kilkadziesiąt sekund, a później wrócić.

Nowa metoda **phishingu** nie ma jeszcze nawet własnej nazwy (tabnabbing to propozycja internautów), gdy Raskin podkreśla, że jej powstanie rzuca nowe światło na funkcjonalność przeglądarki i konieczność wpisywania loginów i haseł na stronach www. Tymczasem "zalecane jest sprawdzanie każdego detalu, w tym zwłaszcza sprawdzanie zawartości pola adresu www strony, na której ma nastąpić logowanie. Aby oszczędzić sobie tej pracy i zminimalizować ryzyko wystąpienia ataku, można też sprawdzić czy włączona jest opcja antyphishingowego skanowania http w programie antywirusowym. W przypadku posiadania oprogramowania G Daty, powinna ona być włączona automatycznie, w większości przypadków trzeba będzie ją uruchomić samodzielnie".

Źródło: **Someday Interactive**