Tabnabbing - co to takiego?

Internet jest dla wielu z nas narzędziem pracy, źródłem wiedzy, rozrywki i inspiracji. Niestety, jest to również miejsce, w którym czyha wiele niebezpieczeństw. Jednym z największych problemów w sieci jest kradzież danych. Zdobyć je można na wiele sposobów, a o większości z nich w ogóle nie mamy pojęcia. Czy wiecie czym jest tabnabbing i jak się przed nim chronić?

Tabnabbing - co to jest?

Tabnabbing polega na podmianie zawartości strony internetowej. Nazwę temu rodzajowi oszustwa nadali internauci - “tab” oznacza po angielsku kartę w przeglądarce, natomiast “nabbing” odnosi się do porwania, zagarnięcia. Tabnabbing jest rodzajem phishingu, czyli ataku mającego na celu wyłudzenie danych, poprzez udawanie innej osoby czy instytucji, np. wykorzystując fikcyjny serwis, podszywający się pod znaną stronę internetową.

Tabnabbing jest rodzajem ataku mającego na celu wyłudzenie danych [...]

Celem tabnabbingu jest kradzież naszych danych. Oszustwo to wykorzystuje powszechny nawyk otwierania wielu kart w przeglądarce. Kiedy haker wykryje brak ruchu na stronie (oznacza to, że przeglądamy inny serwis), podmienia jej zawartość, ikonę i nagłówek karty oraz próbuje zmusić nas do podania danych, np. symulując wylogowanie ze skrzynki e-mail.

Tabnabbing - przebieg ataku

Zauważenie ataku przez nasze oko jest niemalże niemożliwe - musielibyśmy patrzeć na pasek kart dokładnie w tym samym momencie, w którym następuje podmiana lub przyłapać hakera na gorącym uczynku. Możecie to przetestować sami - patrząc na ten tekst, spróbujcie przeczytać nazwę chociaż jednej z otwartych kart. Prawdopodobnie będzie to niemożliwe, gdyż zobaczycie jedynie rozmazany obraz. Ten rodzaj ataku wykorzystuje naszą nieuwagę, a także nieświadomość - próby przechwycenia danych spodziewalibyśmy się raczej przy wejściu na stronę, a nie wtedy, kiedy już się na niej znajdujemy.

Poniżej przedstawiamy jak dokładnie przebiega atak tabnabbingowy, na przykładzie skrzynki pocztowej Gmail:

- użytkownik wchodzi na prawidłową stron Gmail,
- haker namierza moment, w którym użytkownik nie jest aktywny na stronie,
- atakujący podmienia ikonę i tytuł otwartej karty oraz wygląd strony (np. nazwę karty na “Gmail”, a na stronie będzie znajdowało się okienko logowania do poczty, przypominające wygląd oryginalnej strony),
- użytkownik powraca do karty i stwierdza, że prawdopodobnie wystąpił błąd i został wylogowany, sam się wylogował lub zapomniał zamknąć kartę,
- użytkownik loguje się ponownie w fikcyjnym oknie, a dane dostępowe są przesyłane do hakera,
- haker przekierowuje użytkownika do prawidłowej strony Gmail, w której użytkownik i tak był już zalogowany,
- użytkownik nic nie zauważa i jest przekonany, że prawidłowo się zalogował, a haker uzyskuje dostęp do danych.

Powyższy przykład odnosi się do tzw. targetowania ataków - oznacza to, że oszust najpierw śledzi jakie strony przeglądamy, a następnie, w zależności od tego jakie dane chce uzyskać, podmienia jedną z nich. Jeśli nie ma nas aktualnie na stronie, zmienia jej zawartość - aby zwiększyć wiarygodność, w treści może wpisać np. "Wystąpił błąd. Zaloguj się ponownie" i zamieścić okienko logowania.

Warto także wiedzieć, że hakerzy często wykorzystują nie tylko nieuwagę internautów, ale i strach. Dla przykładu - złodziej przekierowuje nas na fałszywą stronę, która pokazuje komunikat, że poprzedni (prawdziwy) serwis nie był stroną oryginalną i jeśli byłeś na niej zalogowany, musisz natychmiast zalogować się ponownie i zresetować swoje hasło, inaczej konto zostanie usunięte. Pod wpływem strachu zazwyczaj nie działamy rozważnie i wpisujemy nasze dane bez zastanowienia.

Zwracajmy także uwagę na wygląd strony, jej szyfrowanie [...]

Tabnabbing - jak się przed nim uchronić

Jak się chronić przed tego rodzaju atakami? Jak zwykle, najlepszym sposobem jest uwaga i ostrożność. Jeśli zostaniemy wylogowani ze strony, najlepiej zamknąć kartę, otworzyć nową i ponownie wpisać adres lub otworzyć ją z zakładek. Zwracajmy także uwagę na wygląd strony, jej szyfrowanie (każdy serwis, w którym podajemy swoje dane, powinien mieć certyfikat SSL!), a także adres - fałszywe strony nigdy nie będą miały takiego samego adresu jak oryginalne, ale zazwyczaj różnią się niemalże niezauważalnie (np. "paly" zamiast "play").

Dodatkową ochroną jest także działanie, które powinno być standardem, a mianowicie stosowanie różnych loginów i haseł na każdej ze stron. Oczywiście znacznie utrudnia to ich zapamiętanie, ale w ten sposób najlepiej zabezpieczymy swoje dane. Warto również wyrobić sobie nawyk sprawdzania strony, jej adresu i wyglądu przy każdorazowym wejściu, przed zalogowaniem.

Tabnabbing jest kolejnym dowodem na to, że hakerzy nie działają bezmyślnie - zazwyczaj podczas ataków wykorzystują psychologiczne i socjologiczne mechanizmy, dzięki którym sami podajemy im nasze dane jak na tacy. Jak z tym walczyć? Myśleć, sprawdzać, być ostrożnym. Większość hakerów szuka wyłącznie łatwych łupów - jeśli my nie ułatwimy im zadania, to najprawdopodobniej sami odpuszczą.