



Jak się bronić przed oszustwem typu "tabnapping"

Ludwik Krakowiak, IDG News Service

27 maja 2010 10:03

Najnowsze wersje przeglądarek internetowych wyposażone są w filtry blokujące próby oszustwa (phishing) - ich zadaniem jest ostrzeżenie przed zagrożeniem w momencie, gdy przeglądarka próbuje otworzyć potencjalnie groźną witrynę. "Tabnapping" wymyka się takim zabezpieczeniom.

W Internet Explorerze mechanizm zabezpieczeń przed oszustwami nosi nazwę **SmartScreen**, Firefox i Chrome oferują **ochronę przed phishingiem i złośliwym oprogramowaniem** (stosowne opcje dostępne są w menu ustawień aplikacji), a Opera dysponuje systemem **Fraud Protection**. Podobne rozwiązanie znaleźć można również w Safari.

Zadaniem wspomnianych wyżej technologii filtrujących jest przede wszystkim ostrzeżenie o zagrożeniu w momencie, gdy przeglądarka próbuje otworzyć potencjalnie groźną witrynę. Tymczasem nowa metoda oszustwa, "[tabnapping](#)", omija tę pierwszą linię obrony, ponieważ istotą takiego ataku jest działanie z opóźnieniem. Przypomnijmy - napastnik mógłby podmienić stronę otwartą na jednej z wielu zakładek w przeglądarce bez wiedzy użytkownika.

Jak się bronić przed "tabnappingiem"

Sprawdź URL-e w pasku adresu przeglądarki przed wypełnieniem jakiegokolwiek formularza czy podaniem prywatnych informacji. Przeglądarki Microsoftu i Google'a pomagają w identyfikacji prawdziwej domeny dzięki funkcji **zakreślania domen** (domena jest prezentowana w czarnym kolorze, reszta adresu - na szaro).

Sonda: Czy uważasz "tabnapping" za realne zagrożenie bezpieczeństwa?

Tak		50,00% - 46
Nie		34,78% - 32
Trudno powiedzieć		15,22% - 14

Jeśli nie przypominasz sobie, byś otwierał daną witrynę wymagającą autoryzacji, nie loguj się na niej. Jeśli na karcie widzisz stronę z formularzem logowania, zamknij ją i otwórz ponownie w nowym oknie lub na nowej karcie przeglądarki.

Korzystaj z rozszerzeń do przeglądarek, pełniących funkcje menedżerów haseł, np. [RoboForm](#).

Dodatki te powiązują ID i hasło logowania z konkretnym adresem internetowym, nie ma więc możliwości zalogowania się z użyciem zapisanych danych w witrynie podszywającej się pod oryginalną stronę.

Wskazówki pozornie mogą się wydawać trywialne. Przypomnijmy sobie jednak, jak często w pośpiechu przełączamy się pomiędzy poszczególnymi kartami w oknie przeglądarki nie zwracając uwagi na takie "szczegóły" jak adres URL.

Komentuje Mateusz Sell, prezes firmy MKS



Mateusz Sell PC World: Czy jest skuteczna metoda, by się chronić przed "tabnappingiem"?

Mateusz Sell: Opisana sytuacja jest typowym atakiem polegającym na podszywaniu się pod witrynę. Przede wszystkim należy mieć świadomość, że takie zagrożenie może się pojawić.

Najlepszym zabezpieczeniem jest zasada ograniczonego zaufania. Pamiętajmy o tym, że w wielu przypadkach fałszywe zakładki nie wyglądają w 100% jak strony www, które próbują imitować.

Nie należy otwierać linków z nieznanymi źródłami, a przed zalogowaniem się na konkretną witrynę warto sprawdzić, czy w oknie przeglądarki widnieje ikona "kłódki". Jej brak może oznaczać, że strona, na której się znaleźliśmy została spreparowana.

Podczas korzystania z usług bankowości elektronicznej rekomendujemy zwracanie szczególnej uwagi na to, czy wszystkie aktywne okna były przez nas otwierane. W przeciwnym wypadku nie należy wpisywać naszych loginów i haseł.

Czy producenci przeglądarek internetowych mogliby współpracować z twórcami oprogramowania antywirusowego, by zmniejszyć ryzyko skutecznego oszustwa opartego o metodę "tabnapping"?

Współpraca pomiędzy twórcami programów antywirusowych oraz przeglądarek wcale nie musi być potrzebna. Tabnapping jest tak naprawdę bardziej zabiegiem socjotechnicznym, niż wyszukaniem luk w samym oprogramowaniu.

Ponadto obecnie producenci przeglądarek internetowych udostępniają szerokie spektrum możliwości dla twórców antywirusów, umożliwiające stworzenie odpowiedniego pluginu, który zabezpieczy użytkowników przed tego typu atakami. Jako producent oprogramowania antywirusowego również rozważamy uwzględnienie ochrony przed tą metodą ataku we wtyczce, nad którą obecnie pracujemy.