Luki w bezpieczeństwie przeglądarek Internet Explorer i Safari znów stanowią zagrożenie wśród internautów. Dziury pozostawały nieusunięte nawet pomimo faktu, że czołowi producenci byli świadomi ich istnienia przez miesiące, jeśli nie lata.

Przeglądarki ponownie podatne na ataki

Niespełna dwa miesiące temu głośno było o cyberprzestępcach, którzy w celu wyłudzania danych wykorzystują tzw. tabnabbing, czyli zmianę wyglądu kart w przeglądarkach internetowych. Okazuje się jednak, że przeglądarki mają znacznie więcej słabości. Internet Explorer, Firefox, Chrome i Safari – wszystkie one podatne są na ataki webmasterów, potajemnie zbierających prywatne hasła i loginy internautów, którzy odwiedzają ich strony. Mowa o takich danych jak: imiona i nazwiska, adresy email, lokacja, jak i zachowane w przeglądarkach hasła. Z całej czwórki najbardziej podatne na atak są Internet Explorer i Safari.

Wiadomość ujawnił Jeremiah Grossman, CTO firmy White Hat Security. Grossman zamierza rozwinąć ten wątek na zbliżającej się konferencji „Black Hat Security" w Las Vegas. Jak sam mówi, jest to sprawa dużej wagi, jako że dotyczy czterech najczęściej używanych w świecie przeglądarek. Wady pozostawały nieusunięte nawet pomimo faktu, że czołowi producenci byli świadomi ich istnienia przez miesiące, jeśli nie lata.

„Ujawnienie przez Grossmana luki w przeglądarkach przypomina sytuację, jaka miała miejsce w połowie czerwca 2010 roku, kiedy pracownik Google, Tavis Ormandy, ujawnił lukę w systemie Windows – mówi Łukasz Nowatkowski z G Data Software, producenta programów antywirusowych. W obu wypadkach powiadomiono odpowiednie firmy, lecz nie podjęły one niezbędnych działań zaradczych. Zarówno Tavis, jak i Grossman postanowili sami nagłośnić sprawę w nadziei na zmianę stanowiska firm. Z jednej strony jest to działanie kontrowersyjne, gdyż daje cyberprzestępcom wiedzę potrzebną im do przeprowadzania ataków, przynajmniej do czasu załatania dziur przez producentów oprogramowania. Z drugiej strony można ich zrozumieć, ponieważ tylko tak mogą sprawić, by duże firmy w końcu podniosły bezpieczeństwo swoich produktów."

Atak następuje bez wiedzy internauty

Aby doszło do ataku, Internauta musi odwiedzić witrynę, która wykorzystuje lukę przeglądarek. Kiedy to nastąpi, użytkownik prawdopodobnie w ogóle nie zauważy, że dzieje się coś nieprawidłowego. Atak wykorzystuje funkcję przeglądarek odpowiedzialną za automatyczne uzupełnianie pól formularza, gdzie zwykle wpisujemy dane do logowania.
Specjalnie zaprojektowany skrypt Java wyprowadza nasze dane z przeglądarki, po czym sam zamiast użytkownika automatycznie wpisuje je do obecnego na stronie formularza na logowanie: imię, nazwisko, adres e-mail, itp. Poza samym wejściem na witrynę, ze strony internauty nie jest wymagana żadna inna interakcja. Co więcej, poprzez zmianę ustawień strony, jej administrator może sprawić, że formularz oraz wpisywane do niego informacje stają się niewidzialne dla oka użytkownika, co czyni atak jeszcze trudniejszym do wykrycia.

Grossman bije na alarm, Apple milczy

Grossman powiadomił Apple o swoim odkryciu już 17 czerwca. Jak dotąd nie doczekał się żadnej odpowiedzi. „Jeśli Apple podjęłoby działania w celu usunięcia zagrożenia, to nie musiałbym mówić dzisiaj o tej sprawie publicznie" – komentuje Jeremiah Grossman.

Someday Interactive