Sophos, firma specjalizująca się w technologiach ochrony informacji, ostrzega przed hakerami wykorzystującymi problem z oprogramowaniem antywirusowym firmy McAfee, który doprowadził setki tysięcy komputerów na całym świecie do stanu nieużywalności, zmuszając je wielokrotnie do ponownego uruchomienia.

McAfee wydało wczoraj aktualizację, która błędnie wykrywa nieszkodliwy plik Windows, svchost.exe, jako "W32/Wecorl.a", co spowodowało krytyczne problemy na komputerach, na których zainstalowano łatę.

Hakerzy postanowili wykorzystać wpadkę producenta oprogramowania. Wykorzystując niedozwolone techniki optymalizacji wyników wyszukiwania (SEO), utworzyli strony internetowe pełne treści, która na pierwszy rzut oka wydaje się być związana z problemem fałszywych alarmów McAfee, ale naprawdę są przeznaczone do infekowania komputerów odwiedzających.

Sophos zidentyfikował szkodliwe witryny, które znajdują się na pierwszej stronie wyników wyszukiwania Google dla fraz związanych z alarmami false positive McAfee.

"Wystarczającym problemem są już komputery w twojej firmie, które odmówiły współpracy z powodu wadliwej aktualizacji oprogramowania antywirusowego. Jeszcze gorzej, gdy zainfekujesz swoją sieć, szukając rozwiązania problemu za pomocą Google", wyjaśnia Graham Cluley, starszy konsultant ds. technologii w Sophos. "Te zainfekowane witryny znajdują się na pierwszej stronie wyników wyszukiwania Google. To bardzo prawdopodobne, że wiele osób kliknie na nie. Jeśli odwiedzisz odnośniki, mogą pojawić się ostrzeżenia pop-up z informacją na temat kwestii bezpieczeństwa. Ostrzeżenia te są fałszywe i mają na celu skłonienie użytkownika do pobrania niebezpiecznego oprogramowania, które może doprowadzić do uzyskania przez hakerów kontroli nad firmowymi komputerami lub kradzieży danych karty kredytowej."

W przeszłości, hakerzy wykorzystali te same techniki do infekowania użytkowników, polujących na informacje o problemach małżeńskich Sandry Bullock oraz śmierci gwiazd takich jak Michael Jackson czy Johnny Depp.

"Manipulowanie wynikami wyszukiwania (SEO) jest dziś jednym z najszybciej rozwijających się obszarów cyberprzestępczości" wyjaśnił Cluley. "Hakerzy wiedzą, że ludzie korzystają z wyszukiwarek, chcąc znaleźć najnowsze informacje, i tylko czyhają aby zainfekować ich komputery."

Sophos zaleca przedsiębiorstwom, aby te chroniły użytkowników, stosując oprogramowanie, które skanuje wszystkie odwiedzane strony w poszukiwaniu złośliwego oprogramowania i działalności przestępczej.

Więcej informacji na temat ataku można znaleźć na blogu Grahama Cluleya pod adresem
http://www.sophos.com/blogs/gc/g/2010/04/22/hackers-exploit-mcafee

Sophos