Przestępcy przejęli kontrolę nad 100 000 ruterów

2 października 2018

Cyberprzestępcy wprowadzili zmiany w serwerze DNS w ponad 100 000 ruterów na całym świecie. Dzięki temu są w stanie przekierować cały ruch przechodzący przez takie rutery. Pozwala im to np. na przeprowadzanie ataków phishingowych, podczas których zdobędą dane użytkowników czy uzyskają dostęp do ich kont bankowych.

Atak na serwery DNS ruterów nie jest niczym nowym. Jednak ten, do którego doszło 20 września wyróżniał się olbrzymią skalą.

Do ataku dochodziło, gdy ofiara odwiedziła witrynę, na której znajdował się odpowiedni skrypt. Był on wykonywany na komputerze ofiary i sprawdzał, czy w sieci wewnętrznej otwarte są konkretne porty. Następnie dochodziło do próby logowania się na ruter na prawach administratora. Używano przy tym metody brute force. Jako, że wielu użytkowników nie zmienia fabrycznych haseł i loginów, metoda ta w wielu przypadkach zadziałała. Po zalogowaniu na ruter przestępcy mogli zmieniać dane zapisane w serwerze DNS.

Wiadomo, że atak działa przeciwko ponad 70 modelom ruterów. Są

wśród nich produkty takich firm jak 3COM, D-LINK, Huawei, TP-LINK, Intelbras, MikroTiK czy TRIZ. Ofiarą cyberprzestępców padło ponad 100 000 ruterów, w większości znajdujących się w Brazylii. Wiadomo, że ich użytkownicy są przekierowywani na fałszywe witryny banków, firm hostingowych czy Netfliksa.

Autorstwo: Mariusz Błoński
Ilustracja: TheDigitalArtist (CC0)
Na podstawie: Myce.com
Źródło: KopalniaWiedzy.pl