CIA od 10 lat podsłuchuje rutery różnych producentów

17 czerwca 2017

Przez ostatnich 10 lat CIA infekowała i podsłuchiwała rutery wielu popularnych producentów. Z najnowszych dokumentów ujawnionych przez „WikiLeaks" w ramach zastawu „Vault 7" dowiadujemy się, że kod o nazwie CherryBlossom szczególnie efektywnie działa przeciwko modelom D-Link DIR-130 oraz Linksys WRT300N. Rutery te można bowiem zdalnie zainfekować nawet, jeśli ustawiono na nich silne hasła. Exploid o nazwie Tomato jest bowiem w stanie zdobyć to hasło jeśli tylko na ruterach uruchomione jest UPnP. Oczywiście jeszcze łatwiej zdobyć hasła do ruterów chronionych słabymi lub fabrycznymi hasłami. Z dokumentów dowiadujemy się, że wykorzystywany od 2007 roku zestaw CherryBlossom działa na 25 modelach ruterów, jednak możliwa jest jego modyfikacja tak, by działał na ponad 100 modelach.

WikiLeaks ujawniła 175-stronicowy przewodnik użytkownika CherryBlossom. Opisano w nim bazujący na Linuksie system operacyjny, który działa na wielu różnych urządzeniach. Po zainstalowaniu na docelowym ruterze CherryBlossom zamienia go w przekaźnik sygnałów z kontrolowanego prze CIA serwera o nazwie CherryTree. Serwer może przydzielać ruterowi różne zadania, pozwala na sprawdzanie statusu misji, zdobytych danych czy przeprowadzanie na ruterze działań administracyjnych. Wspomniane misje polegają np. na podsłuchiwaniu konkretnego użytkownika korzystającego z ruter. Użytkownicy mogą być identyfikowania po adresach IP, MAC, adresach e-mail, nickach z czatów czy numerze VoIP. Zadania misji to np. przechwytywanie całego ruchu, przechwytywanie jego wybranych elementów, kopiowanie adresów, przechwytywanie nazw użytkowników, przekierowanie przeglądarki na witrynę, na której zostanie przeprowadzony atak typu drive-by, stworzenie połączenia VPN, które daje CIA dostęp do sieci lokalnej czy

też przepuszczenie całego ruchu przez kontrolowany przez CIA serwer proxy.

Cała komunikacja odbywająca się pomiędzy zainfekowanym ruterem a serwerem CherryTree jest szyfrowana i uwierzytelniania. Dodatkowo zaszyfrowane dane udają ciasteczko HTTP GET proszące o przysłanie pliku graficznego. W odpowiedzi CherryTree rzeczywiści wysyła plik graficzny.

Warty podkreślenia jest przede wszystkim fakt, że powyższe narzędzia dają CIA bardzo duże możliwości i są wykorzystywane co najmniej od 2007 roku, a więc od czasu, gdy metody atakowania ruterów były znacznie słabiej rozwinięte niż obecnie.

Autorstwo: Mariusz Błoński
Na podstawie: ArsTechnica.com
Źródło: KopalniaWiedzy.pl