HAKERZY ATAKUJĄ ROUTERY. CELEM BUDOWA BOTNETU Z IOT

Grupa hakerska atakuje routery działające w oparciu o oprogramowanie Tomato - ostrzegają eksperci cytowani przez serwis Ars Technica. Ich zdaniem hakerzy przejmując kontrolę nad sprzętem pracują obecnie nad budową rozległego botnetu z urządzeń Internetu Rzeczy.

Złośliwe oprogramowanie, z którego korzysta grupa hakerska stojąca za serią ataków, to samorozprzestrzeniający się wirus poszukujący urządzeń zabezpieczonych z użyciem domyślnych danych (login i hasło).

Z Tomato korzystają routery zarówno używane przez firmy w celu usprawnienia działania VPN, jak i użytkownicy indywidualni.

Botnet, do którego dołączane są zhakowane urządzenia nazywa się Muhstik i został wykryty przez specjalistów z branży cyberbezpieczeństwa dwa lata temu, kiedy z jego użyciem atakowano serwery działające w oparciu o system operacyjny Linux i urządzenia Internetu Rzeczy. Botnet ten atakował też podatności w aplikacjach takich jak Webdav, WebLogic, Webuzo czy popularny system WordPress.

Badacze z firmy Palo Alto Networks poinformowali, że w ataku na routery pracujące na oprogramowaniu Tomato Muhstik korzysta z już zainfekowanych urządzeń, które skanują sieć w poszukiwaniu sprzętów zabezpieczonych domyślnymi hasłami. Routery te są następnie przejmowane i zarządzane przez hakerów zdalnie z serwera IRc po to, by również one skanowały sieć w poszukiwaniu innych podatnych na infekcje urządzeń. Wirusy, które cyberprzestępcy instalują na przejętych sprzętach to m.in. kryptominery służące do nielegalnego pozyskiwania kryptowalut, a także oprogramowanie służące do przeprowadzania ataków zmasowanej odmowy dostępu do usług (DDoS).

Firma zaleca internautom korzystającym z urządzeń internetu rzeczy, by byli ostrożni przy pobieraniu nowego oprogramowania dla routerów z sieci, zwłaszcza w przypadku programów open source. Przy instalacji oprogramowania sprzętowego doradzane jest natomiast przestrzeganie wszystkich procedur bezpieczeństwa określonych przez jego producenta - czytamy w treści rekomendacji Palo Alto Networks.