Cyberdefence 24

aut. Szymon Palczewski 29.05.2020

OPERACJA GRU W AMERYKAŃSKICH SIECIACH. NSA OSTRZEGA PRZED ROSYJSKIMI HAKERAMI

Państwowi hakerzy działający na zlecenie Kremla odpowiadają za złośliwą kampanię wymierzoną w użytkowników oprogramowania przeznaczonego do wymiany korespondencji online. Amerykańska National Security Agency (NSA) wrogie działania przypisała rosyjskim służbom wywiadu oraz specjalistycznym komórkom wojskowym.

Rosyjscy hakerzy wykorzystywali lukę w oprogramowaniu Exim Mail Transfer Agent od co najmniej sierpnia ubiegłego roku. Złośliwą operację prowadziło Głównego Centrum Technologii Specjalnych (GTsST) GRU, znane lepiej pod nazwą Sandworm – czytamy w oficjalnym komunikacie amerykańskiej NSA. Exim jest serwerem poczty elektronicznej dla systemów uniksowych.

Występująca w Exim luka – CVE-2019-10149 – umożliwiała hakerom rozsyłanie specjalnie spreparowanych wiadomość e-mail w celu realizacji dalszych złośliwych operacji. Eksperci NSA podkreślają, że grupa Sandworm wykorzystując lukę mogła zdalnie wykonać następujące czynności na zaatakowanym urządzeniu: dodać nowych „uprzywilejowanych użytkowników”; wyłączyć ustawienia bezpieczeństwa sieci; zaktualizować konfiguracje SSH, aby umożliwić dodatkowy zdalny dostęp; czy ingerować w inne procesy w ramach urządzenia w celu prowadzenia bardziej zaawansowanych działań.

Mówiąc prościej, rosyjscy hakerzy mogli wysyłać specjalnie spreparowane wiadomości e-mail w celu wykonywania poleceń z uprawnieniami administratora, które pozwalały m.in. na instalowanie programów, modyfikowanie danych oraz tworzenie nowych kont.

„Hakerzy prowadzili działania za pomocą oprogramowania Exim (…) wysyłając do ofiar złośliwe wiadomości” – precyzuje NSA w oświadczeniu. Po wykryciu luki twórcy oprogramowania wydali komunikat, w którym wówczas stwierdzili, tu cytat – „Obecnie nie ma dowód na aktywne wykorzystanie tej podatności”. Jednak w obliczu możliwego zagrożenia wydano aktualizację dla Exim, która jest obecnie rekomendowana przez NSA dla wszystkich użytkowników ze względów bezpieczeństwa.

W ostatnim czasie również niemieckie służby bezpieczeństwa poinformowały o penetracji krajowych sieci i systemów przez rosyjskich hakerów powiązanych z FSB. Jak informowaliśmy wcześniej, głównym celem Moskwy byli operatorzy infrastruktury krytycznej.

Niemieccy eksperci publicznie podkreślili, że na początku bieżącego roku odkryli dowody „długotrwałych kampanii hakerskich” wymierzonych w krajowe systemy o kluczowym znaczeniu dla bezpieczeństwa państwa. Głównym zadaniem rosyjskich hakerów było wykorzystanie publicznie dostępnego, ale także specjalnie opracowanego złośliwego oprogramowania, aby trwale „zakotwiczyć się” w sieci IT oraz ukraść informacje, a nawet uzyskać dostęp do konkretnych systemów niemieckich operatorów infrastruktury krytycznej.

Czytaj też: Wieloletnia penetracja niemieckich sieci przez Rosjan. Przygotowania do cyberuderzenia?