Cyberdefence 24

aut. Szymon Palczewski 14.08.2020

PENTAGON ZAGROŻONY ROSYJSKIM CYBERATAKIEM. GRU OPRACOWAŁO NARZĘDZIE DO ZAAWANSOWANYCH KAMPANII

Hakerzy rosyjskiego wywiadu GRU posługują się nowym, nieznanym wcześniej złośliwym oprogramowaniem do prowadzenia zaawansowanych kampanii cyberszpiegowskim. Wirus jest przeznaczony do infekowania urządzeń bazujących na systemie Linux. Szczególnie narażone na operację hakerską są instytucje amerykańskiego sektora obronnego, w tym Departament Obrony USA.

Amerykańska NSA oraz FBI poinformowały, że hakerzy rosyjskiego wywiadu GRU, znani w środowisku jako Fancy Bear lub APT28, wykorzystują nowe, nieznane do tej pory złośliwe oprogramowanie o nazwie Drovorub, przeznaczone dla systemu Linux. Wirus stanowi podstawę działań cyberszpiegowskich – czytamy w komunikacie na oficjalnej stronie FBI.

W specjalnym poradniku „Russian GRU 85th GTsSS Deploys Previously Undisclosed Drovorub Malware", opracowanym przez FBI i NSA, stwierdzono, że Drovorub to narzędzie hakerskie przeznaczone do przesyłania plików, a także przekierowania danych na zewnętrzne nośniki oraz serwery. „Po wdrożeniu na zaatakowanym urządzeniu Drovorub zapewnia możliwość bezpośredniej komunikacji z infrastrukturą kontrolowaną przez zewnętrznego aktora, a także pobierania i wysyłania plików, wykonywania zdalnych poleceń oraz przekierowania ruchu sieciowego do innych hostów w sieci" – czytamy w poradniku.

Oprogramowanie wykorzystywane przez hakerów rosyjskiego wywiadu jest trudne do wykrycia, ponieważ skutecznie ukrywa ślady działania. Aby wzmocnić odporność sieci i systemów przed Drovorub, administratorzy powinni zaktualizować system Linux do wersji 3.7 lub nowszej. „Ponadto (…) zaleca się skonfigurowanie systemów tak, aby ładowały tylko moduły z ważnym podpisem cyfrowym, co utrudni aktorowi wprowadzenie złośliwego oprogramowania do systemu" – radzi NSA i FBI.

Wirus jest szczególnym zagrożeniem dla Stanów Zjednoczonych, ponieważ Linux jest wykorzystywany w systemach bezpieczeństwa narodowego, w tym wśród takich podmiotów jak Departament Obrony USA czy Defense Industrial Base.

„Drovorub to >szwajcarski scyzoryk< o możliwościach, które pozwalają napastnikowi wykonywać wiele różnych funkcji, takich jak kradzież plików i zdalne sterowanie komputerem ofiary" – stwierdził w rozmowie z agencją Reutera Steve Grobman, ekspert McAfee.

W tym miejscu warto podkreślić, że wydany poradnik jest przejawem strategii NSA i FBI, której jednym z elementów jest wspieranie sektora prywatnego w budowie świadomości w obszarze cyberbezpieczeństwa.

„Dla FBI jednym priorytetów w cyberprzestrzeni jest (…) wzmocnienie pozycji sektora prywatnego, rządowego i międzynarodowych partnerów poprzez proaktywną wymianę informacji" – podkreślił zastępca dyrektora FBI Matt Gorham na oficjalnej stronie Biura. Jak dodał, wydany poradnik jest znakomitym przykładem tego typu działań, które mogą dotrzeć do wszystkich zainteresowanych. „Nieustannie dzielimy się informacjami, które pomagają firmom i społeczeństwu chronić się przed złośliwymi hakerami" – zaznaczył przedstawiciel FBI.

Hakerzy rosyjskiego wywiadu GRU stanowią poważne zagrożenie dla bezpieczeństwa Stanów Zjednoczonych. Wynika to z faktu, że nieustannie prowadzą operacje wymierzone w amerykańskie sieci i systemy. Sytuacja nabiera jeszcze większego znaczenia w związku ze zbliżającymi się wyborami prezydenckimi w USA. Waszyngton za wszelką ceną chce uniknąć podobnych incydentów, jakie miały miejsce podczas ostatniej kampanii w 2016 roku, w którą silnie ingerowała Rosja.

Czytaj też: Rosyjski wywiad poluje na szczepionkę przeciwko Covid-19