CHIŃSCY HAKERZY KRUSZĄ CYBERMUR ROSYJSKICH SŁUŻB SPECJALNYCH

Hakerzy powiązani z Chinami wykorzystali złośliwe oprogramowanie podczas cyberataków na rosyjską służbę wywiadu FSB oraz inne podmioty rządowe federacji. Kreml oficjalnie ogłosił, że padł celem wrogiej operacji „cybernajemników", realizujących zadania obcego państwa. Kampania była nastawiona na kradzież poufnych danych i dokumentów.

Specjaliści Sentinel Labs przeanalizowali kampanię, podczas której hakerzy wykorzystali złośliwe oprogramowanie „Mail-O" w ramach działań wymierzonych w rosyjską służbę wywiadu FSB oraz inne podmioty rządowe tego kraju. Operacja miała miejsce w 2020 roku.

O wrogiej kampanii oficjalnie poinformowała strona rosyjska w specjalnym raporcie opublikowanym w maju br. Narodowe Centrum Koordynacji Incydentów FSB razem z Rostelecom wskazało, że kilka instytucji oraz organizacji państwowych padło ofiarą operacji grupy APT.

W dokumencie podkreślono, że Rosja stała się celem „cybernajemników działających na rzecz realizacji interesów obcego państwa", o czym świadczą użyte narzędzia, metody oraz szybkość i jakość podejmowanych czynności.

Jak tłumaczy Rostelecom, głównym celem hakerów było naruszenie bezpieczeństwa infrastruktury IT i kradzież poufnych danych, w tym dokumentów uznawanych za tajne oraz korespondencji władz federalnych. Do realizacji tych zadań wykorzystano rozwiązania krajowych dostawców technologii, w tym np. Mail.ru czy Yandex.

Aby skutecznie przeniknąć do państwowych sieci, hakerzy użyli 3 metod: phishingu, wykorzystania podatności i luk w aplikacjach oraz cyberataków na partnerów i kontrahentów rządowych.

Pierwsza myśl: Zachód

Początkowo w sieci pojawiały się spekulacje, że ze względu na charakter kampanii (m.in. jej poziom zaawansowania) została ona przeprowadzona przez Stany Zjednoczone, członków sojuszu Five Eyes lub inne państwo zachodnie. „Najprawdopodobniej tak nie było" – podkreśla Juan Andres Guerrero-Saade, ekspert Sentinel Labs.

Zdaniem specjalisty „Mail-O" jest wariantem dobrze znanego w środowisku wirusa o nazwie „PhantomNet" lub „SManager", który jest powszechnie używany przez grupę hakerską TA428. Analiza wrogich operacji z przeszłości wskazuje na jej chińskie pochodzenie. Hakerzy słyną z atakowania zarówno celów położonych w Azji, jak i samej Rosji.

W rozmowie z CyberScoop Juan Andres Guerrero-Saade podkreślił, że chińskie cyberszpiegostwo wymierzone w Rosję nie powinno nikogo szokować. „Stosunki chińsko-rosyjskie są złożone i dotyczą

wielu spornych kwestii, takich jak wspólna granica, interesy gospodarcze czy dyplomatyczne” – zaznaczył specjalista Sentinel Labs.

Dla wielu obserwatorów publiczne udostępnienie raportu na temat cyberataków na rządowe agencje, w tym FSB, jest zachowaniem „niecodziennym” w przypadku Kremla. Jednak jak tłumaczy na łamach CyberScoop rosyjski dziennikarz Andrei Soldatov, specjalizujący się w służbach specjalnych, przedstawienie szerszej społeczności faktów zawartych w dokumencie ma pokazać, że nawet FSB stoi w obliczu takich samych zagrożeń, jak inne organizacje w pozostałych krajach.

Czytaj też: Ukraiński rząd trafiony cyberatakiem rosyjskich służb specjalnych