aut. Szymon Palczewski 05.12.2018

ROSYJSKIE GRUPY CYBERPRZESTĘPCZE W CZECHACH

Jak podaje czeska Służba Bezpieczeństwa (BIS) dwie rosyjskie grupy cyberprzestępcze włamały się do Ministerstwa Spraw Zagranicznych oraz Ministerstwa Obrony, a także uzyskały dostęp do skrzynek pocztowych członków armii. Sprawę ujawniono w rocznym raporcie opracowanym przez agencję czeskiego wywiadu.

Czeska Służba Bezpieczeństwa (BIS) zarzuca dwóm grupom cyberprzestępczym, znanym jako Turla i APT28, przeprowadzenie ataków na Ministerstwo Spraw Zagranicznych (MSZ), Ministerstwo Obrony oraz Armię Republiki Czeskiej. Incydenty były przeprowadzane w różnych kampaniach w 2016 i 2017 roku.

Przedstawiciele BIS stwierdzili, że system komunikacji elektronicznej MSZ został naruszony pierwszy raz w 2016 roku, kiedy to hakerzy uzyskali dostęp do ponad 150 skrzynek pocztowych personelu. Cyberprzestępcy skopiowali wówczas treści wiadomości e-mail wraz ze wszystkimi załącznikami. Eksperci badający incydent podkreślili, że „napastnicy skupili się głównie na skrzynkach pocztowych najważniejszych przedstawicieli ministerstwa, do których uzyskali dostęp".

Hakerzy włamali się również do innych rządowych sieci. Odnosząc się do sprawy BIS stwierdziło, że cyberprzestępcy posiadali listę określonych celów we wszystkich ważnych instytucjach państwowych. Przypadek skrzynek pocztowych w wielu kluczowych aspektach odpowiada podobnym incydentom, jakie miały miejsce w innych państwach europejskich w tamtym okresie.

Jak wskazują przedstawiciele BIS, w grudniu 2016 roku przeprowadzono kolejny atak na MSZ. Różnił się on od pierwszego tym, że hakerzy usiłowali zdobyć szczegóły logowania do skrzynek pocztowych za pomocą bardziej bezpośrednich sposobów działania (tzw. *brute force attaca*). Czeski wywiad nie przypisał ataków tylko do jednej grupy, lecz do dwóch.

Turla jest jedną z najstarszych i najbardziej wyrafinowanych rosyjskich grup hakerskich sponsorowanych przez państwo. Z kolei APT28 jest przede wszystkim znana z włamania do serwera Demokratycznego Komitetu Narodowego w 2016 roku, przed wyborami prezydenckimi w USA.

BIS powiedział, że oprócz ataków na Ministerstwo Spraw Zagranicznych, grupa APT28 jest również odpowiedzialna za inne ataki wymierzone w Czechy. Eksperci wykryli kilka ataków na cele wojskowe. Głównym narzędziem działania cyberprzestępców były tutaj wiadomości e-mail kierowane przede wszystkim do osób z dyplomacji wojskowej. Najpoważniejsze naruszenie związane było z kompromitacją kilku prywatnych kont poczty użytkowników związanych z Ministerstwem Obrony oraz armią.

W wyniku incydentu hakerom nie udało się wykraść żadnych informacji niejawnych. Wyciekły natomiast dane osobowe oraz inne dane wrażliwe, które mogą być wykorzystywane przez

cyberprzestępców do przeprowadzenia dalszych ataków cybernetycznych.