aut. Andrzej Kozłowski 04.03.2020

ROSYJSKA GRUPA CYBERPRZESTĘPCÓW SZTURMUJE SEKTOR FINANSOWY KOREI POŁUDNIOWEJ

Grupa cyberprzestępców, która od dawna zajmuje się atakowaniem instytucji finansowych na całym świecie skupiła się w 2019 roku na przedsiębiorstwach z sektora finansowego w Korei Południowej. W swoich działaniach wykorzystywała złośliwe oprogramowanie umieszczone w załącznikach wysyłanych za pomocą poczty elektroniczej oraz ransomware.

Badacze z Instytutu Bezpieczeństwa Finansowego w Korei Południowej przyznali, że grupa hakerska przez większość 2019 roku próbowała dokonać ataków phisingowych na sektor finansowy, ale również obiekty przemysłowe, szpitale i placówki medyczne w Korei Południowej.

Cyberprzestępcy znani pod kryptonimem TA505 są aktywni od 2014 roku i według analityków blisko współpracują z rosyjską grupą FIN7, współdzieląc narzędzia, techniki i procedury. FIN7 odpowiada za cyberataki, które doprowadziły do strat rzędu miliardów dolarów. Wcześniej, eksperci często mylili obie grupy ze względu na podobne narzędzia oraz zachowanie.

Najbardziej znanym narzędziem używanym przez TA505 jest trojan bankowy Dridex wykorzystywany do kradzieży danych logowania oraz ransomware Locky za pomocą którego atakowali swoje ofiary od 2016 roku. TA505 to rosyjskojęzyczna grupa odpowiadająca za wysyłanie tysięcy zainfekowanych e-maili do pracowników banków w Stanach Zjednoczonych, Singapurze oraz Zjednoczonych Emiratach Arabskich.

Instytut Bezpieczeństwa Finansowego poinformował, że TA505 próbowało dokonać phisingu w Korei Południowej za pomocą zainfekowanych plików Microsoft Excel wykorzystując złośliwe oprogramowanie FlawedAmmyy. Jest to trojan zdalnego dostępu, co oznacza, że umożliwia przejęcie kontroli nad zainfekowaną maszyną bez wiedzy ofiary. Haker może monitorować aktywność użytkownika oraz zbierać informacje o danych logowania.

Analiza ponad 600 tys. phishingowych e-maili wysłanych między lutym i grudniem roku pokazała, że większość z nich (80 proc) została wysłana w trakcie dni roboczych, większość z nich w środki i czwartki. Zdaniem analityków badających zdarzenie pokazuje to, że grupa wiedziała kiedy uderzyć, aby mieć największe szanse na sukces. Znaleziono również fałszywą, postawioną przez hakerów stronę, która wyglądem przypominała portal Apple i służyła do kradzieży danych koreańskich pracowników zatrudnionych w amerykańskich koncernach.