aut. Sylwia Gliwa 28.10.2020

PÓŁNOCNOKOREAŃSCY HAKERZY Z GLOBALNĄ MISJĄ WYWIADOWCZĄ. GRUPA KIMSUKY ROZPRACOWANA

Działania północnokoreańskich hakerów, odpowiedzialnych za prowadzenie globalnej misji wywiadowczej zostały odkryte. Jak informuje amerykańska CISA wraz FBI grupa zbierała informacje odnośnie polityki zagranicznej, polityki nuklearnej i sankcji nałożonych na Pjongjang.

Agencja ds. Cyberbezpieczeństwa i Infrastruktury (CISA), Federalne Biuro Śledcze (FBI) oraz U.S. Cyber Command Cyber National Mission Force informują za pośrednictwem strony CISA o ogłoszeniu kolejnego alertu bezpieczeństwa dla cyberprzestrzeni. W ramach opublikowanego raportu, instytucje opisują działalność Kimsuky – północnokoreańskiej grupy powiązanej ze strukturami rządowymi.

Działania grupy wymierzone są w ogólnoświatowe cele i skupione są, jak informują amerykańskie agendy, na pozyskiwaniu informacji na potrzeby rządu Korei Północnej. Co więcej hakerzy w ramach tego zespołu działają prawdopodobnie przynajmniej od 2012 roku.

Jak czytamy w raporcie, przewidywania wskazują, że Kimsuky otrzymał od rządu w Pjongjangu zlecenie przeprowadzenia globalnej misji wywiadowczej. Z danych przekazanych w alercie, Kimsuky prowadzi działania w zakresie gromadzenia danych wywiadowczych przeciwko osobom i organizacjom w Korei Południowej, Japonii i Stanach Zjednoczonych. Działania wywiadowcze skupione są głównie na polityce zagranicznej i kwestiach bezpieczeństwa narodowego związanych z Półwyspem Koreańskim, polityką nuklearną i sankcjami.

W ramach działań grupa skupia się przede wszystkim na taktyce inżynierii społecznej, phishingu profilowanego czy za pomocą metody tzw. wodopoju (watering hole attacks). W ramach swoich aktywności, grupa pisała maile do swoich ofiar, które miały pozyskiwać ich zaufanie np. poprzez podszywanie się pod dziennikarzy i kierowanie próśb o udzielenie wywiadu. Po tym jak ofiara zgodziła się na udzielenie wywiadu, hakerzy wysyłali kolejną wiadomość z zainfekowanym załącznikiem. Temat rozmowy był dobierany pod ofiarę i był zgodny z tematami „na topie”.

Grupa, jak wskazują wyniki analizy, po zdobyciu dostępu do urządzenia ofiary, do prowadzenia kolejnych działań m.in. malware określany przez ekspertów jako BabyShark. To samo oprogramowanie było wykorzystywane przez inną grupę północnokoreańskich hakerów grupy Thallium, znanej również jako APT37.

Działalność Kimsuky była już wcześniej opisywana przez media, które wskazywały na wykrytą aktywność przeciwko emerytowanym ambasadorom, generałom, oraz członkom Ministerstwa Spraw Zagranicznych oraz resortu zjednoczenia Korei Południowej. Podczas omawianej przez serwis ZDNet pod koniec sierpnia kampanii, hakerzy wykorzystali metodę spear-phishingu. Przedstawiciele grupy rozsyłali e-maile przekierowujące ofiary na fałszywe strony zawierające witrynę do logowania. Podczas

gdy użytkownik wpisywał dane, cyberprzestępcy je rejestrowali.

Jak informujemy na bieżąco na naszych łamach, Korea Północna regularnie rozwija swoje cyberzdolności. Na przestrzeni lat Pjongjang rozbudował cyberwojsko oraz opracował nowe narzędzia hakerskie. Cyberprzestrzeń stanowi wymiar, w którym obchodzone są międzynarodowe sankcję oraz pozyskiwane fundusze na finansowanie armii a także programu nuklearnego.

Czytaj też: „Sztuka (cyber)wojny" według Korei Północnej. Nikt nie jest bezpieczny w sieci?

Tylko w zeszłym roku, według szacunków ONZ, poprzez wykorzystanie cyberataków których celem była kradzież środków z systemów bankowych oraz giełd kryptowalutowych Pyongyang wygenerowała około 2 miliardy dolarów zysków. Jak wskazywało organizacja, zdobyte w ten sposób fundusze zostały przeznaczone na rozwój programu broni masowego rażenia (BMR).