Cyberdefence 24

aut. Andrzej Kozłowski 27.08.2020

BANKI I BANKOMATY CELEM HAKERÓW Z KOREI PÓŁNOCNEJ

Hakerzy z Korei Północnej włamują się do banków na całym świecie w celu dokonania nielegalnych przelewów pieniędzy oraz uszkodzenia bankomatów, tak aby "wypluwały pieniądze" - ostrzegł amerykański rząd.

Cztery amerykańskie agencji federalne (USCYBERCOM, FBI, Departament Skarbu i CISA z Departamentu Bezpieczeństwa Wewnętrznego) wystosowały komunikat, w którym ostrzegają przed ponownym wzrostem aktywności północnokoreańskich hakerów. Ich głównych celem są po raz kolejny instytucje finansowe z całego świata.

Od lutego 2020 roku północnokoreańscy hakerzy wznowili operacje ukierunkowane na ataki na banki w wielu państwach w celu przeprowadzenia nielegalnych transferów finansowych oraz uszkodzenia bankomatów w taki sposób, żeby "wypluwały" one pieniądze.

Amerykańskie organy ścigania zatytułowały te kampanię "Fast Cash" i oskarżyły o nią północokoreańską agencje szpiegowską Biuro ds. Ogólnego Rozpoznania (Reconnaissance General Bureau). "Fast Cash" rozpoczęła się w 2016 roku i trwa do dziś, a stopień zaawansowania oraz liczba ataków zdecydowanie wzrosła w ostatnim czasie.

W przeciągu ostatnich lat Korea Północna była obwiniana za ataki na sektor prywatny, w szczególności instytucje finansowe w Azji, Afryce i Ameryce Południowej, ale również w Europie, w tym w Polsce. Cyberprzestępcy koncentrowali się na kradzieży danych oraz generowaniu środków finansowych. W swoich operacjach wykorzystywali strukturę złośliwego oprogramowania, która została przez ekspertów nazwana MATA. Zawiera ona między innymi kilka modułów ładujących oraz zainfekowane wtyczki.

Czytaj też: Polska celem Korei Północnej. Hakerzy wykradali dane i środki finansowe

Bryan Ware z Departamentu Bezpieczeństwa Wewnętrznego USA napisał, że Korea Północna zademonstrowała niezwykłą elastyczność zmieniania swojej taktyki tak aby maksymalnie wykorzystać luki w sieciach i systemach sektora finansowego, ale również do atakowania firmy z innych sektorów gospodarki. Jego słowa potwierdza wykryty w ostatnim czasie nieznany rodzaj złośliwego oprogramowania wykorzystywanego przez hakerów Korei Północnej. Trojan zdalnego dostępu stanowił kluczową cyberbroń Pjongjangu podczas kampanii wymierzonej w sektor obronny USA, jaka miała miejsce w tym roku.

Czytaj też: Korea Północna powiększa arsenał „cyberbroni”