

KRADZIEŻ 250 MILIONÓW DOLARÓW W KRYPTOWALUTACH. AMERYKANIE ZNALEŻLI WINNYCH

Ponad 250 milionów dolarów w kryptowalutach mieli ukraść hakerzy z Korei Północnej - tak twierdzi amerykański Departament Sprawiedliwości. Cyberprzestępcy odpowiadają również za „pranie brudnych pieniędzy” pochodzących z cyberataków.

Zdaniem Departamentu Sprawiedliwości USA (DoJ) północnokoreańscy hakerzy wykradli 250 milionów dolarów w kryptowalutach za pomocą cyberataków wymierzonych w sektor finansowy, w tym giełdy bitcoinów. Pozyskane środki cyberprzestępcy „wyprali” dzięki współpracy z chińskimi pośrednikami.

„Dzisiejsze oświadczenie ujawnia powiązania między programem cyberataków Korei Północnej a chińską siecią zajmującą się praniem brudnych pieniędzy” – wskazał zastępca prokuratora generalnego Brian C. Rabbitt z Wydziału Karnego Departamentu Sprawiedliwości, którego wypowiedź znalazła się na oficjalnej stronie DoJ. Jak dodał, obecna sprawa podkreśla ciągle zaangażowanie departamentu w przeciwdziałanie zagrożeniu stwarzanemu przez północnokoreańskich hakerów poprzez ujawnianie ich sieci przestępczych oraz śledzenie i przejmowanie nielegalnie pozyskanych środków.

„Dzisiaj prokuratorzy i śledczy po raz kolejny pokazali zaangażowanie w identyfikacji cyberzagrożeń, nakładaniu sankcji i zapewnianiu pomocy ofiarom złośliwych działań” – podkreślił zastępca prokuratora generalnego John C. Demers z Wydział Bezpieczeństwa Narodowego Departamentu Sprawiedliwości. Zazaczył, że mało prawdopodobne jest, aby Korea Północna zaprzestała prób ingerencji w systemy i sieci sektora finansowego, ponieważ w ten sposób generuje środki dla realizacji swoich celów militarnych, politycznych i innych.

W oświadczeniu Departamentu Sprawiedliwości podkreślono skuteczność amerykańskich służb „w śledzeniu i przejmowaniu wirtualnej waluty, co przestępcy wcześniej uznawali za niemożliwe”.

Emmerson Buie Jr., specjalny pełnomocnik FBI, zazaczył, że północnokoreańscy hakerzy nie mogą ukrywać swoich działań w anonimowej sieci. „Międzynarodowe programy prania kryptowalut podważają integralność naszych systemów finansowych na poziomie globalnym, a my użyjemy każdego narzędzia, jakie jest w naszym arsenale do zbadania i neutralizacji tych przestępstw” – podkreślił przedstawiciel FBI. Jak dodał, służby nadal będą podejmować swoje działania, aby zakłócić działanie aktorom, którzy starają się podważyć interesy USA.

Departament Sprawiedliwości wskazał na dwa kluczowe incydenty, które stały się przedmiotem sprawy. Po pierwsze, w lipcu 2019 roku hakerzy powiązani z Koreą Północną przeprowadzili cyberatak na sektor kryptowalut. Na skutek incydentu skradziono bitcoiny i tokeny o wartości ponad 272 000 dolarów (w tym tokeny PlayGame i IHT Real Estate Protocol).

W kolejnych miesiącach środki były „prane” za pomocą kilku pośredników. „W wielu przypadkach aktor konwertował kryptowalutę na BTC, Tether lub inne formy kryptowaluty - proces znany jako >przeskok łańcuchowy< - w celu zaciemnienia ścieżki transakcji” - czytamy na oficjalnej stronie DoJ. Organom ścigania udało się jednak wyśledzić skradzione fundusze, pomimo wyrafinowanych technik „prania pieniędzy”.

W drugim przypadku we wrześniu 2019 roku jedna z amerykańskich firm padła ofiarą cyberataku, w wyniku którego północnokoreańscy hakerzy uzyskali dostęp do wirtualnych zasobów przedsiębiorstwa, funduszy przechowywanych przez firmę na innych platformach oraz środków posiadanych przez partnerów firmy. „Cyberprzestępcy ukradli prawie 2,5 miliona dolarów i wyprali je za pośrednictwem ponad 100 kont na innej giełdzie wirtualnych walut” - stwierdził w oświadczeniu Departament Sprawiedliwości USA.

Wszystkie pozyskane fundusze zostały prawdopodobnie „wyprane” we współpracy z chińskimi pośrednikami. „Infrastruktura i rachunki komunikacyjne wykorzystywane do dalszych włamań i transferów funduszy były również powiązane z Koreą Północną” - czytamy w oświadczeniu.

Czytaj też: [Spektakularny rozwój cyberwojsk Korei Północnej. Hakerzy rozmieszczeni poza granicami kraju](#)