Cyberdefence 24

aut. Szymon Palczewski 10.04.2019

NAJPIERW BANKI, TERAZ KRYPTOWALUTY. TAK PJONGJANG FINANSUJE ROZWÓJ BRONI NUKLEARNEJ

Wyspecjalizowana grupa północnokoreańskich hakerów APT38 zmieniła obiekt zainteresowania. Po kradzieży ponad miliarda dolarów z instytucji finansowych na całym świecie, cyberprzestępcy skupili swoją uwagę na kryptowalucie. Większość uzyskanych środków przeznaczana jest na zwiększanie potencjału wojska, w tym rozwój nuklearnego potencjału - informuje Wired.

Marine Chain wyglądał jak każdy inny ambitny biznes. Strona internetowa firmy, która pierwszy raz pojawiła się w globalnej sieci w 2018 roku, była dobrze zaprojektowana, posiadała modną nazwę domeny „.io", czym zachęcała użytkowników do jej odwiedzania. Za pomocą atrakcyjnej witryny spółka Marine Chain obiecywała potencjalnym inwestorom czysty zysk, wskazując drogę do „lukratywnego międzynarodowego przemysłu żeglugowego" - pisze na łamach Wired Matt Burges.

Zainteresowani ofertą mogli dokonywać transferu środków do Vessel Token Offering (przyp. red. alternatywnej kryptowaluty opartej na blockchainie Ethereum), aby w ten sposób wejść w posiadanie określonych statków i następnie móc handlować z innymi nabywcami. Sporządzony przez firmę biznesplan został tak opracowany, że pobudzał wyobraźnię potencjalnych klientów, tym samym wzbudzając ich zaufanie. Według przedstawionych danych w 2022 roku Marine Chain przewidywała, iż 5% globalnych transakcji związanych z handlem statkami miałoby odbywać się w ramach platformy firmy.

Niestety, spółka Marine Chain okazała się być zwykłym oszustwem, za którym stoją północnokoreańscy hakerzy. Ich cel stanowili zamożni inwestorzy i ich majątki. Atrakcyjna strona internetowa firmy była jedynie prostą kopią konkurencyjnej spółki „Shipowner.io".

Pomysł z utworzeniem Marine Chain oznacza zmianę orientacji działań cyberprzestępców, których celem stały się kryptowaluty. Reżim Kim Dzong Una w ten sposób chce obejść liczne sankcje gospodarcze wymierzone w Pjongjang (m.in. zakaz importu węgla, drewna oraz innych materiałów). Rygorystyczna polityka wobec Korei Północnej ma zmusić rząd do porzucenia programu rozwoju broni atomowej.

Odpowiedzią Pjongjangu stały się cyberataki, których celem było szpiegostwo oraz kradzież środków finansowych. Państwowi hakerzy zostali przez ekspertów powiązani z szeregiem incydentów na giełdach kryptowalut oraz w tradycyjnych bankach. W wyniku działalności cyberprzestępców skradziono ponad miliard dolarów.

W okresie od stycznia 2017 roku do września 2018 północnokoreańscy hakerzy wykradli 571 milionów dolarów w kryptowalutach z pięciu czołowych giełd Azji. Jak wskazuje z jeden badaczy ONZ – „Cyberprzestrzeń jest wykorzystywana przez Pjongjang jako asymetryczny środek do

przeprowadzania nielegalnych i tajnych operacji w dziedzinie cyberprzestępczości oraz uchylania się od nałożonych sankcji".

Jedną z elitarnych grup hakerskich, znajdujących się w Korei Północnej, jest APT38. Według różnych szacunków liczy ona około 20 osób. W jej skład wchodzą wyspecjalizowani eksperci, a cała grupa jest dobrze wyposażona dzięki wsparciu rządu. Cyberprzestępcy APT 38 dzięki swojej działalności dostarczyli państwu około miliard dolarów w samym 2018 roku. Uzyskane środki zostały skradzione z banków oraz giełd kryptowalutowych.

„Jeden zespół, składający się z garstki osób znanych jako APT 38, jest odpowiedzialny za większość ataków" – stwierdził jeden z europejskich specjalistów. – „APT 38 jest kontrolowany przez główną organizację wywiadowczą Korei Północnej, Reconnaissance General Bureau".

APT38 odpowiada między innymi za „masowe cyberataki" w Bangladeszu, Indiach, Meksyku, Pakistanie, Filipinach, Korei Południowej, Tajwanie, Turcji i dwukrotnie w Chile i Wietnamie. Zachodni eksperci podejrzewają również, że członkowie grupy podjęli próbę uderzenia w banki Europy Zachodniej, ale wyższy poziom zabezpieczeń w tych państwach uniemożliwił hakerom skuteczne działanie.

Skradzione w wyniku cyberataku środki trafiają przede wszystkim do sektora militarnego. Głównym beneficjentem działalności hakerów jest północnokoreańskie wojsko. „Analitycy bezpieczeństwa jednomyślnie oceniają, że fundusze skradzione przez APT 38 - znaczny procent PKB Korei Północnej - są kierowane do programów rozwoju rakiet i broni nuklearnej Pjongjangu" – wskazuje ekspert, który pragnie pozostać anonimowym.

Wraz z ogólnym wzrostem liczby ataków na giełdy kryptowalut, stało się jasne, że Korea Północna używa bitcoinów jako sposobu wspierania swojej gospodarki. „Cyberbezpieczeństwo to już nie tylko zatrzymywanie przestępców czy ochrona technologii. Chodzi o uniemożliwienie reżimom, takim jak Korea Północna, zdobycia środków na wojnę nuklearną" – podkreśla specjalista. – „Musimy zadać sobie pytanie - kiedy Korea Północna przetestuje swoją kolejną rakietę i czy to naprawdę w porządku, że zapłacili za nią bitcoinem?".

Według ekspertów FireEye grupa APT 38 jest aktywna od co najmniej 2014 roku. Niemal od samego początku ogromna większość ataków grupy była skierowana przeciwko tradycyjnym bankom i instytucjom finansowym w celu przeprowadzenia nielegalnych transakcji, których końcowym odbiorcą jest Pjongjang. Jak informuje FireEye, APT38 należy wiązać z „Lab 110, organizacją podporządkowaną Reconnaissance General Bureau (RGB)".

„Myślę, że jest to prawdopodobnie najbardziej zaawansowana grupa z Korei Północnej" – podkreśla Ben Read, specjalista FireEye. – „Udało im się skompromitować wiele banków i przenieść wielkie środków poza granice państwa".

Jak podaje witryna Pyongyang Papers, siedziba APT38 znajduje się w północno-zachodnim mieście Sinuiju - graniczącym z najważniejszym partnerem handlowym kraju, Chinami. Główną metodą działania hakerów jest spearphishing, który wymaga specjalistycznej wiedzy na temat komunikacji wewnętrznej w danej firmie czy instytucji. Skuteczność tego typu incydentów sugeruje, że członkowie grupy biegle władają wieloma językami.

APT38 posiada ogromne środki finansowe na prowadzenie operacji oraz dostęp do najszybszych łączy internetowych, które mają zagwarantować skuteczność podjętych działań. Według FireEye hakerzy spędzają „około 155 dni w sieciach komputerowych swoich ofiar przed zakończeniem operacji". W jednym z przypadków, cyberprzestępcy penetrowali systemy nieprzerwanie przez dwa lata, zanim

przeprowadzili uderzenie.

Obecnie północnokoreańscy hakerzy skupili swoje zainteresowanie na kryptowalutach. „Korea Północna zwyczajnie potrzebuje pieniędzy” – wskazuje Priscilla Moriuchi, dyrektor w Recorded Future. Firma jako pierwsza zidentyfikowała fikcyjną działalność Marine Chain i powiązała ją z Pjongjangiem. Z kolei według ONZ skupienie Korei Północnej na kryptowalutach to próba uniknięcia sankcji, ponieważ są one „trudniejsze do śledzenia, mogą być prane wielokrotnie i są niezależne od regulacji rządowych”.

Źródło: Wired