aut. Szymon Palczewski 18.02.2021

USA: HAKERZY WYWIADU KOREI PÓŁNOCNEJ Z AKTEM OSKARŻENIA ZA MASOWE CYBERATAKI

Trzech hakerów północnokoreańskiego wywiadu zostało oskarżonych przez amerykański wymiar sprawiedliwości o szereg „destrukcyjnych" cyberataków, których głównym celem była kradzież środków finansowych, w tym kryptowalut, na rzecz rządu w Pjongjangu. Mężczyźni przez lata przeprowadzali liczne cyberoperacje w różnych częściach świata, generując łącznie straty w wysokości prawie 1,3 mld USD. W działania zaangażowany był również Kanadyjczyk, który został oskarżony o pranie pieniędzy pochodzących z cyberataków prowadzonych przez agentów Korei Północnej.

Według aktu oskarżenia trzech północnokoreańskich hakerów powiązanych z wojskiem brało udział w szeroko zakrojonych cyberoperacjach, aby przeprowadzić „serię destrukcyjnych cyberataków", w celu kradzieży i wyłudzenia ponad 1,3 mld USD – wskazuje Departament Sprawiedliwości Stanów Zjednoczonych.

Ich głównymi ofiarami były instytucje finansowe oraz firmy, a działalność koncentrowała się na opracowaniu wielu „złośliwych aplikacji kryptowalutowych" oraz stworzeniu i nielegalnym sprzedawaniu „platformy blockchain".

Paul Abbate, zastępca dyrektora FBI, podkreślił, że akt oskarżenia wiąże się z zarzutami Biura z 2018 roku dotyczącymi „bezprecedensowych cyberataków przeprowadzonych przez reżim Korei Północnej". Jak wskazał, działalność Pjongjangu w sieci dotknęła podmioty na całym świecie i tylko współpraca międzynarodowa z organami ścigania innych państw może pozwolić na skuteczną walkę z tym zagrożeniem. Przedstawiciel amerykańskich służb zaznaczył, że identyfikacja hakerów, przejęcie funduszy oraz postawienie aktu oskarżenia jest przejawem tego, że FBI podejmuje realne wysiłki na rzecz pociągnięcia Korei Północnej do odpowiedzialności za prowadzenie wrogich operacji w cyberprzestrzeni.

Według amerykańskich służb sprawa północokoreańskich hakerów jest „uderzającym przykładem" rosnącej współpracy między przedstawicielami rządów niektórych państw a wysoce zaawansowanymi cyberprzestępcami. Michael R. D'Ambrosio, zastępca dyrektora amerykańskich tajnych służb, wskazał, że osoby wymienione w akcie oskarżenia dopuściły się licznych bezprecedensowych naruszeń prawa: od ataków ransomware i kampanii phishingowych po napady na banki oraz zaawansowane operacje prania brudnych pieniędzy.

> *Agenci Korei Północnej, którzy używają klawiatur zamiast broni, kradnąc cyfrowe portfele kryptowaluty zamiast worków z gotówką, są największymi na świecie rabusiami banków.*

> John C. Demers, zastępca prokuratora generalnego USA

Zgodnie z aktem oskarżenia Jon Chang Hyok (31 lat); Kim Il (27) i Park Jin Hyok (36) byli członkami jednostek Reconnaissance General Bureau (RGB), wojskowej agencji wywiadowczej Koreańskiej Republiki Ludowo-Demokratycznej (KRLD), która zajmowała się działalnością hakerską. W środowisku jest znana jako Lazarus Group lub APT38.

„Dorobek" agentów Pjongjangu

Departament Sprawiedliwości USA wyróżnił katalog wrogich działań podejmowanych przez północnokoreańskich hakerów w celu „osiągnięcia korzyści finansowych". Wśród tych, które zostały wyróżnione w akcie oskarżenia należy wskazać na:

- cyberataki na branżę rozrywkową – operacja hakerska wymierzona w m.in. Sony Pictures Entertainment (listopad 2014r.) czy Mammoth Screen (2015r.) zajmujące się produkcją serialu fabularnego z udziałem brytyjskiego naukowca skupionego na energii jądrowej, który trafił do niewoli w Korei Północnej;
- cyberoperacje wymierzone w banki – w tym np. próby kradzieży ponad 1,2 mld USD z banków w Wietnamie, Bangladeszu, Tajwanie, Meksyku, Malcie i Afryce w latach 2015-2019 poprzez zhakowanie sieci komputerowych tych instytucji;
- kradzieże środków finansowych z bankomatów – pozyskanie gotówki za pośrednictwem systemów wypłaty pieniędzy określane przez rząd USA jako „FASTCash", w tym kradzież 6,1 mln USD z BankIslami Pakistan Limited (październik 2018 r.);
- kampanie ransomware – stworzenie „destrukcyjnego" oprogramowania szyfrującego WannaCry 2.0 (maj 2017r.) oraz liczne wymuszenia na firmach w latach 2017-2020, obejmujące kradzież wrażliwych danych i wdrażanie ransomware;
- tworzenie i zarządzanie złośliwymi aplikacjami kryptowalutowymi – rozwijanie wielu apek od marca 2018r. do co najmniej września 2020r., w tym takich jak Celas Trade Pro, WorldBit-Bot, iCryptoFx, Union Crypto Trader, Kupay Wallet, CoinGo Trade, Dorusio, CryptoNeuro Trader i Ants2Whale (zapewniały hakerom dostęp do urządzeń ofiar);
- cyberataki na podmioty odpowiedzialne za kryptowaluty – kradzież wirtualnych walut wartych dziesiątki milionów dolarów, w tym 75 mln USD od słoweńskiej firmy kryptowalutowej (grudzień 2017r.); 24,9 mln USD od indonezyjskiej firmy kryptowalutowej (wrzesień 2018r.); oraz 11,8 mln USD od firmy świadczącej usługi finansowe w Nowym Jorku (sierpień 2020r.), w której hakerzy wykorzystali złośliwą aplikację CryptoNeuro Trader jako backdoor;
- operacje typu spear-phishing – liczne kampanie prowadzone od marca 2016r. do lutego 2020, wymierzone w pracowników lub urzędników w Stanach Zjednoczonych, którzy współpracowali z kontrahentami dla wojska, podmiotami sektora energetycznego, firmami branży lotniczej, koncernami technologicznymi, a także samych przedstawicieli Departamentu Stanu i Departamentu Obrony USA.
- stworzenie „Marine Chain Token" i „Initial Coin Offering" – *opracowanie* i wprowadzenie do obrotu w 2017 i 2018 roku Marine Chain Token w celu umożliwienia inwestorom zakupu udziałów w statkach morskich, wspieranych przez blockchain, co pozwoliłoby Korei Północnej na potajemne pozyskiwanie środków od inwestorów, kontrolowanie interesów w zakresie żeglugi morskiej i unikanie sankcji Stanów Zjednoczonych.

> *Zakres wrogich działań północnokoreańskich hakerów był rozległy i*

> *długotrwały, a katalog popełnionych przez nich przestępstw jest oszałamiający. Postępowanie wyszczególnione w akcie oskarżenia to czyny zbrodniczego państwa narodowego, które nie powstrzymało się przed niczym, by dokonać zemsty i zdobyć pieniądze na wsparcie swojego reżimu.*
>
> Tracy L. Wilkison, pełniąca obowiązki prokuratora USA

Kanadyjczyk częścią „układanki”

Prokuratorzy federalni poinformowali również o oskarżeniu Ghaleba Alaumary’a z Mississauga w Ontario w Kanadzie, który miał brać udział w praniu brudnych pieniędzy na rzecz Korei Północnej. 37-latek przyznał się do winy i wskazał, że współpracował z hakerami odpowiedzialnymi za kradzież środków finansowych z bankomatów, cyberataki na banki czy innymi oszustwami internetowymi.

Jak wskazuje Departament Sprawiedliwości USA, mężczyzna zorganizował zespoły partnerów w Stanach Zjednoczonych i Kanadzie w celu wyprania milionów dolarów pochodzących z przestępstw. Alaumary współpracował również z Ramonem Olorunwą Abbasem (znanym jako „Ray Hushpuppi”) i innymi osobami, aby „prać fundusze z cybernapadu dokonanego przez Koreę Północną w maltańskim banku w lutym 2019r.”.

Prokuratura oraz FBI otrzymały nakaz upoważniający do przejęcia kryptowalut skradzionych przez hakerów Pjongjangu.

Czytaj też: ONZ: rozwój broni nuklearnej Korei Północnej możliwy dzięki hakerom