Bitdefender

Północnokoreańska grupa hakerska zaatakowała wiele organizacji w Korei Południowej

13.12.2023

Władze Korei Południowej oskarżyły północnokoreańskie ugrupowania hakerskie „Andariel” o kradzież informacji o technologiach obronnych wielu firm, a także kryptowalut o wartości około 400 000 dolarów. Hakerzy z Korei Północnej często pojawiają się w wiadomościach ze względu na ich zaangażowanie w przestrzeni kryptowalut oraz jako operatorzy oprogramowania ransomware. Jak wskazano w ostatnim raporcie badawczym, od 2017 r. prawdopodobnie ukradli kryptowaluty o wartości do 3 miliardów dolarów, a Korea Południowa była jednym z ich głównych celów.

Hakerzy z Korei Północnej znowu w akcji

Jak się okazuje, tym razem hakerzy powiązani z Koreą Północną nie zadowolili się jedynie kradzieżą kryptowalut, lecz zrobili o wiele więcej.

Najnowsze doniesienia wskazują na to, że obrali oni za cel wiele firm kluczowych dla obronności ich południowych sąsiadów.

„Północnokoreańska organizacja hakerska „Andariel" włamała się do krajowych firm z branży obronnej, ukradła ważne dane techniczne, m.in. dotyczące broni przeciwlotniczej, a także wyprała pieniądze z bitcoinów otrzymanych w zamian za oprogramowanie ransomware za pośrednictwem konta cudzoziemki" – podała Seoul Metropolitan Police Agency.

Niebezpieczny cyberincydent między Koreami

Z tego, co dotychczas ujawniły władze, ugrupowanie hakerskie wykorzystało krajową firmę wynajmującą serwery, aby uderzyć w organizacje w Korei Południowej. Policja przejęła pocztę elektroniczną krajową i zagraniczną (konta użytkowników serwerów). Ponadto wszczęto 40 dochodzeń, które wykazały, w jaki sposób hakerzy włamali się do instytutów badawczych, firm farmaceutycznych, a nawet organizacji hostującej ich serwery. Jedna z dotkniętych firm posiadała informacje dotyczące broni przeciwlotniczej używanej w Korei Południowej.

„Policja odkryła, że skradziono łącznie 1,2 TB plików, które prawdopodobnie zawierały ważne technologie i dane, oraz powiadomiła odpowiednie firmy, ale niektóre z nich nie były nawet świadome szkód, a inne zgłosiły obawy związane ze spadkiem zysków, które skłoniło ich do skontaktowania się z policją" – podały również władze.

Departament Wsparcia Dochodzeń w sprawie Bezpieczeństwa Agencji Policji Metropolitalnej w Seulu współpracuje obecnie z FBI w sprawie ataków za granicą, ofiar i osób zaangażowanych w tę kampanię.

„Grupy hakerskie powiązane z reżimami autorytarnymi są niezwykle niebezpieczne, ponieważ bardzo trudno zatrzymać ich działalność. Tacy hakerzy są opłacani i chronieni przez kraje, dla których pracują. Ponadto Korea Północna zrobiła sobie z procederu kradzieży kryptowalut dochodowy sposób na wzmacnianie gospodarki. Dlatego niezależnie od tego, gdzie się znajdujemy, powinniśmy dbać o bezpieczeństwo dóbr cyfrowych, szczególnie jeśli posiadamy kryptowaluty. Pamiętajmy o tym, aby zawsze korzystać z unikalnych i silnych haseł oraz zabezpieczyć swoje urządzenia za pomocą skutecznego systemu antywirusowego” – mówi Krzysztof Budziński z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło:https://bitdefender.pl/polnocnokoreanska-grupa-hakerska-zaatakowala-wiele-organizacji-w-korei-poludniowej/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 13.12.2023
Z pozdrowieniami Piotr Rozmiarek
E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender
Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony

użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.