

PÓŁNOCNOKOREAŃSCY CYBERPRZESTĘPCY ZAINTERESOWANI BITCOINEM

Powiązana z władzami Korei Północnej grupa cyberprzestępcza Lazarus prowadzi działania zmierzające do kradzieży danych specjalistów od kryptowalut takich jak bitcoin - podała w piątek agencja Reutera, powołując się na raport Secureworks.

Zajmująca się zabezpieczeniami i oceną zagrożeń komputerowych firma Secureworks odnotowała 25 listopada e-mailową kampanię phishingową wymierzoną w ludzi z branży kryptowalut, którym oferowano stanowisko dyrektora ds. finansowych jednej z londyńskich giełd wirtualnych walut. Osoby, które kliknęły załączony do wiadomości link, instalowały na swoim komputerze złośliwe oprogramowanie zapewniające cyberprzestępcom zdalny dostęp do urządzenia.

Na podstawie analizy kodu zastosowanego w ataku specjaliści z Secureworks podejrzewają, że stoi za nim wiązana z Koreą Północną grupa Lazarus. Pracownicy frankfurckiego oddziału firmy przypisują Lazarusowi również przeprowadzenie ataku na hollywoodzkie studio Sony w 2014 roku oraz wyprowadzenie 81 mln dolarów z centralnego banku Bangladeszu.

Bitcoin cieszy się dużą popularnością w Korei Południowej, odpowiadającej za około 20 proc. wszystkich światowych transakcji w tej kryptowalucie. Na tamtejsze giełdy wirtualnych walut przypuszczono w ostatnim czasie serię ataków; odpowiedzialnością za nie obarczono Koreę Północną, która ma wykazywać zainteresowanie bitcoinem od 2013 roku. Pozbawiona centralnego nadzoru kryptowaluta pozwalałaby na obejście sankcji, jakimi obłożone jest to państwo.

Obecne działania przypisywane przez analityków grupie Lazarus mają wynikać z gwałtownego wzrostu wartości bitcoina, która osiągnęła w piątek rekordową wysokość 17,8 tys. dolarów (w porównaniu z niespełną tysiącem dolarów na początku bieżącego roku).

Zdaniem analityków listopadowy atak jest tylko częścią wciąż trwającej kampanii zapoczątkowanej jeszcze w 2016 roku.

