

Oszustwa z kryptowalutami i serwisami randkowymi w tle

3 października 2024

Eksperci alarmują, że cyberprzestępcy coraz częściej stosują nowe metody w celu dokonywania oszustw związanych z inwestowaniem w kryptowaluty. Jednocześnie korzystają ze starych i znanych już sposobów na rynku. I co gorsza, cały czas znajdują kolejne ofiary. Do tego bezprawnie sięgają po wizerunki znanych osób i tworzą fałszywe giełdy cyfrowych walut, żeby wzbudzać zaufanie. Uważać szczególnie muszą użytkownicy popularnych serwisów randkowych, gdzie może ich czekać tzw. świniobicie. Obietnice szybkiego zysku bez ryzyka powinny zawsze wzbudzać nieufność. Natomiast w celu ochrony środków finansowych trzeba dokładnie sprawdzać oferty inwestycyjne i stojące za nimi podmioty.



W przestrzeni publicznej coraz częściej mówi się o oszustwach związanych z inwestowaniem w kryptowaluty. Oszuści tworzą m.in. fałszywe projekty kryptowalutowe lub fundusze inwestycyjne, które są rzekomo promowane przez znane osoby. Jak podkreśla Anna Kwaśnik, ekspertka NASK ds. budowania świadomości cyberbezpieczeństwa, dzięki technologii deepfake,

powstają spreparowane materiały reklamowe np. z politykami, celebrytami czy ze sportowcami. W nich obiecywany jest szybki i duży zysk, najczęściej bez ryzyka. Inną metodą działania cyberprzestępców są fałszywe giełdy kryptowalut. One do złudzenia przypominają prawdziwe tego typu podmioty, mają podobne oprawy wizualne oraz nazwy domen.

„W branży kryptowalutowej coraz częściej dochodzi do oszustw, w których przestępcy podszywają się pod znane osoby w reklamach umieszczanych w social mediach, zachęcając do inwestycji na fałszywych platformach. Po założeniu konta i podaniu numeru telefonu ofiara spotyka się z agresywnymi telefonami od osoby podającej się za konsultanta. Za pomocą manipulacji i technik socjotechnicznych przekonuje ona inwestora do zainstalowania oprogramowania zdalnego dostępu, takiego jak Anydesk czy Teamviewer. W ten sposób oszust uzyskuje dostęp do konta i kradnie środki” – komentuje Janusz Zieliński, ekspert rynku kryptowalutowego z platformy ARI10.

Z kolei Anna Kwaśnik zaznacza, że przestępcy działają również za pośrednictwem popularnych serwisów randkowych. Ta metoda określana jest jako tzw. świnioobicie (z ang. pig butchering). Oszuści najpierw nawiązują z poszkodowaną osobą relację przyjacielską lub romantyczną (etap tzw. tuczenia świni), a następnie zachęcają ją do zainwestowania na rynku kryptowalut. Kiedy zasoby finansowe inwestora zostały wyczerpane lub gdy zaczyna coś podejrzewać, przestępca nagle znika (tzw. etap zarzynania). Ekspertka z NASK wspomina też o schemacie Ponziego. Zarówno w przypadku kryptowalut, jak i innych inwestycji jest to nielegalne działanie. Wkłady nowych inwestorów służą do wypłacania obiecanych zysków starym inwestorom. Tym samym ci na końcu listy mogą nigdy nie otrzymać zwrotu. Jednym z przykładów takiego przedsięwzięcia jest platforma Bitconnect. W tym przypadku obiecywano zwroty z inwestycji w bitcoinie sięgające nawet 40% miesięcznie.

„Z sygnałów, które do nas dochodzą, w tym od osób poszkodowanych, wynika, że popularnym sposobem działania

oszustów jest metoda polegająca na wyłudzeniu środków poprzez instalowanie oprogramowania umożliwiającego zdalne monitorowanie komputera. Służy to przejęciu kontroli nad komputerem ofiary i pozyskaniu danych do konta bankowego. W grę wchodzi także nakłanianie ofiar do dokonywania przelewów w celu rzekomego odblokowania większych kwot, które mają do nich należeć” – mówi Michał Żuławiński ze Stowarzyszenia Inwestorów Indywidualnych (SII).

Jak zaznacza Jakub Martenka z ARI10, część osób otrzymuje informacje, że mają do odebrania kryptowaluty o wartości kilku tysięcy euro. Ekspert chciałby wierzyć, że ta metoda oszustów nie jest już skuteczna, ale statystyki pokazują, że wciąż znajdują się kolejne ofiary. Jeśli więc ktoś dostanie podobną wiadomość, powinien zachować szczególną ostrożność. Należy unikać udostępniania jakichkolwiek danych osobowych czy finansowych. Trzeba też zgłosić podejrzaną sytuację odpowiednim służbom lub bezpośrednio do platformy, pod którą rzekomi przedstawiciele się podszywają.

„Są też oszustwa typu »rug pull«. Najprościej ujmując, polegają na tym, że twórcy projektu związanego z kryptowalutami nagle wycofują wszystkie pieniądze z inwestycji, zostawiając inwestorów z bezwartościowymi tokenami. Takie sytuacje zdarzają się w projektach opartych na technologii blockchain, na przykład na Ethereum, gdzie transakcje są zarządzane przez programy komputerowe zwane inteligentnymi kontraktami” – dodaje ekspertka z NASK-u.

Inwestowanie pieniędzy zawsze wiąże się z ryzykiem. Według Anny Kwaśnik, dlatego niezwykle ważne jest, aby przed przekazaniem jakichkolwiek środków finansowych dokonać dokładnej weryfikacji. W Polsce można to zrobić na stronie Komisji Nadzoru Finansowego, która prowadzi rejestr legalnie działających podmiotów. W przypadku chęci zainwestowania w kryptowaluty warto zapoznać się z rankingiem polecanych giełd i wybrać taką, która cieszy się największym zaufaniem. Jednak nadal nie gwarantuje to oczywiście pełnego bezpieczeństwa.

„Należy dokładnie przeanalizować ofertę inwestycyjną i być czujnym na obietnice szybkich i dużych zysków przy minimalnym ryzyku. Trzeba sprawdzić autentyczność mediów społecznościowych i materiałów wideo. Warto się upewnić, że są prawdziwe, a nie generowane przez sztuczną inteligencję lub nie są skopiowane z innych profili bądź łądząco nie przypominają oryginalnego profilu firmy. Do tego dochodzi weryfikacja rejestracji firmy w odpowiednich rejestrach oraz numerów identyfikacyjnych. Należy też zwrócić uwagę na komunikację. Odpowiedzi powinny pochodzić od rzeczywistych osób, a nie od botów. Lokalne firmy powinny zapewniać polskojęzyczną stronę i nie mieć istotnych błędów stylistycznych” – podpowiada Izabela Mazur, ekspertka rynku kryptowalutowego z ARI10.

Z kolei Michał Żuławiński wymienia przykładowe sytuacje, w których powinna zapalać się czerwona lampka w głowie każdej potencjalnej ofiary przestępstw finansowych. To m.in. obietnice zysku bez ryzyka, natarczywe namawianie do inwestycji, nękanie telefonami, wyłudzenie danych do bankowości elektronicznej lub kart kredytowych czy żądanie zainstalowania jakiejkolwiek aplikacji na komputerze. Jak przekonuje ekspert z SII, w razie wątpliwości zawsze lepiej zrezygnować z rzekomo wyjątkowej oferty. W myśl zasady, że lepiej stracić okazję niż pieniądze. Ponadto o sprawie warto także powiadomić policję. Im więcej sygnałów dotrze do niej, tym większa jest szansa na złapanie przestępców.

„Rynek kryptowalut jest międzynarodowy i na oszustów może natknąć się każdy, kto inwestuje w cyfrową walutę. Wśród poszkodowanych są też Polacy. Mówią o tym komunikaty podawane przez Komendę Główną Policji, Centralne Biuro Zwalczania Cyberprzestępczości i inne instytucje, które walczą z oszustwami inwestycyjnymi. Za pomocą manipulacji i podstępnych metod, zmyślonych scenariuszy i obietnic wielkiego zysku, oszuści wyciągają od potencjalnych inwestorów pieniądze” – przestrzega ekspertka z NASK-u.

Ofiara może na początku inwestowania zobaczyć na swoim koncie domniemany zysk, co podkreśla Adam Radomski, ekspert rynku kryptowalutowego. Ma to na celu zachęcenie do dalszych inwestycji. Jak dodaje ekspert, w momencie próby wypłaty swoich środków pojawiają się pierwsze trudności. Oszuści przerzucają odpowiedzialność na problemy techniczne. Ewentualnie oznajmniają, że w celu odblokowania zysków wymagana jest dodatkowa opłata. Ofiary często zaciągają różnego rodzaju zobowiązania w postaci kredytów lub wykorzystują swoje oszczędności, aby móc odblokować „zarobione” środki. W rzeczywistości wypłata jednak nie następuje, oszuści milkną i znikają z pieniędzmi.

„W Europie Wschodniej, Azji i Afryce hurtowo tworzy się call center w celu oszukiwania ludzi. Z rynkowych obserwacji i sygnałów wynika, że najmocniej jesteśmy narażeni wtedy, kiedy dzwoni do nas osoba ze wschodnim akcentem i mówi po polsku, że proponuje inwestycje. Sam otrzymywałem takie telefony i zawsze były to próby wyłudzenia pieniędzy” – podsumowuje Jakub Martenka.

Źródło tekstu i ilustracji: [MondayNews.pl](https://mondaynews.pl)