Bitdefender

Funkcja Create2 w Ethereum wykorzystana w napadzie na kryptowaluty o wartości 60 milionów dolarów

16.11.2023

Badacze bezpieczeństwa odkryli wyrafinowany schemat, w którym przestępcy wykorzystali funkcję Create2 Ethereum, co doprowadziło do znacznej kradzieży kryptowalut. Ta złośliwa operacja, ujawniona przez specjalistów ds. zwalczania oszustw Scam Sniffer Web3, spowodowała szkodę dla 100 000 ofiar na łączną kwotę około 60 milionów dolarów w okresie sześciu miesięcy.

Zrozumienie Create2 i jego luk w zabezpieczeniach

Aktualizacja „Constantynople” sieci Ethereum wprowadziła funkcję „Create2”, następcę oryginalnej funkcji Create.

Ta funkcja umożliwia bardziej zaawansowaną interakcję z inteligentnymi kontraktami, w tym wstępne obliczanie adresów kontraktów. Wprowadził jednak również luki w zabezpieczeniach.

Raport Scam Sniffer wskazuje, że Create2 można zmanipulować w celu wygenerowania nowych adresów kontraktowych bez historii transakcji, co umożliwi im ominięcie alertów bezpieczeństwa portfela.

Jak doszło do kradzieży z wykorzystaniem Create2?

Sprawcy ostatniej kradzieży Ethernum wykorzystali czyste adresy do fałszywych transakcji. Niczego niepodejrzewający użytkownicy podpisywaliby te transakcje, nieświadomie przenosząc swoje aktywa na adresy kontrolowane przez atakującego.

W odmianie tego exploita napastnicy utworzyli adresy podobne do legalnych, oszukując użytkowników, aby wysyłali zasoby na fałszywe adresy.

Zatrucie adresowe: nowa warstwa oszustwa

Strategia, znana jako „zatruwanie adresów”, polega na tworzeniu partii adresów i wybieraniu tych, które najlepiej odpowiadają potrzebom oszustwa. Jedna ofiara straciła oszałamiającą kwotę 1,6 miliona dolarów w jednej transakcji dokonanej pod tak zatrutym adresem.

Oszustwo nie ogranicza się wyłącznie do tej metody; we wcześniejszych wersjach napastnicy wysyłali niewielkie ilości kryptowalut do

potencjalnych ofiar, zdobywając ich zaufanie przed dokonaniem kradzieży.

Zalecenia zespołu Bitdefender dotyczące ochrony Twojej kryptowaluty

Jeśli chcesz chronić się przed tymi i innymi oszustwami związanymi z kryptowalutami, to zespół Bitdefender stworzył dla Ciebie kilka podstawowych zasad cyberbezpieczeństwa związanego z tą branżą.

- Używaj specjalistycznego oprogramowania antywirusowego, aby odeprzeć próby phishingu i inne zagrożenia cyfrowe.
- Zawsze weryfikuj adresy transakcji, szczególnie w przypadku znacznych kwot.
- Rozważ użycie portfeli sprzętowych w celu zwiększenia bezpieczeństwa.
- Regularnie aktualizuj i twórz kopie zapasowe oprogramowania portfela.

„Warto także zawsze szukać dodatkowych wskazówek dotyczących zachowania bezpieczeństwa w świecie kryptowalut w zasobach eksperckich i obszernych przewodnikach na temat unikania oszustw związanych z tą branżą. Zachowanie czujności i ciągłe pozyskiwanie nowych informacji ma kluczowe znaczenie dla ochrony zasobów cyfrowych w coraz bardziej złożonym i ewoluującym krajobrazie cyberbezpieczeństwa” – mówi Krzysztof Budziński z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło:https://bitdefender.pl/funkcja-create2-w-ethereum-wykorzystana-w-napadzie-na-kryptowaluty/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 16.11.2023
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.