Bitdefender

Grupa Lazarus używa nowego miksera do prania skradzionych Bitcoinów

16.02.2023

Lazarus Group, czyli północnokoreański gang, który notorycznie popełnia cyberprzestępstwa, został niedawno przyuważony podczas próby obejścia amerykańskich ograniczeń związanych z mikserami kryptowalut. Hakerów przyłapano na korzystaniu z nowej usługi do prania skradzionych aktywów kryptograficznych.

Zgodnie z raportem firmy Elliptic zajmującej się analizą blockchain północnokoreańska grupa cyberprzestępców Lazarus zaciemniła transfery o wartości około 100 milionów dolarów w Bitcoinach, które skradli od października ubiegłego roku.

Czym są miksery kryptowalut?

Miksery kryptowalut, zwane również tumblerami, to usługa, która łączy aktywa kryptograficzne wielu użytkowników, próbując zaciemnić kod właścicieli i pochodzenie funduszy.

W zeszłym roku Biuro Kontroli Aktywów Zagranicznych (OFAC)

Departamentu Skarbu USA nałożyło szereg sankcji na usługi miksowania kryptowalut, takie jak Tornado Cash i Blender. Ograniczenia zostały nałożone z powodu włamania do mostu międzyłańcuchowego Axie Infinity o wartości 600 milionów dolarów, które przypisano grupie Lazarus.

Po wejściu ograniczeń w życie operator Blendera podobno odzyskał z usługi prawie 22 miliony dolarów w Bitcoinach i przerwał dalszą pracę. Jednak nowa analiza Elliptic sugeruje, że nieistniejący Blender mógł zostać ponownie uruchomiony, tym razem pod pseudonimem Sindbad. Odnowiona usługa jest prawdopodobnie obsługiwana przez tego samego operatora.

Czy Sindbad to rzeczywiście nowy mikser do prania skradzionych Bitcoinów?

„Dziesiątki milionów dolarów z Horizon i innych hacków powiązanych z Koreą Północną przeszły przez Sindbada" – czytamy w oświadczeniu Elliptic. – „Podobnie jak Blender, Sindbad jest mikserem zabezpieczającym, co oznacza, że jego operator ma pełną kontrolę nad zdeponowanymi w nim kryptoaktywami. Analiza eliptyczna wskazuje, że Sindbad jest w rzeczywistości wysoce prawdopodobnym rebrandingiem Blendera, za który odpowiada ta sama osoba lub grupa."

Do powyższego przekonania skłoniły firmę zajmującą się analizą blockchain m.in. poniższe argumenty:

- Usługi mają podobną infrastrukturę, konwencje nazewnictwa i język.

- Niektóre tryby działania są identyczne, w tym opóźnienia transakcji, długość kodów miksera i listów gwarancyjnych.
- Podobne wzorce zachowań w łańcuchu, takie jak charakterystyka transakcji i zaciemnianie transakcji za pośrednictwem usług stron trzecich.
- Wczesne transakcje przychodzące do Sindbada o wartości prawie 22 milionów dolarów pochodziły z portfela podejrzanego operatora Blendera.
- Wiele transakcji na aktywach związanych z Sindbadem, w tym transakcje testowe i płatności za promocję usług, pochodziło z portfela podejrzanego operatora Blendera.

„W ostatnich latach zauważyliśmy wyraźny wzrost zainteresowania kryptowalutami wśród wielu użytkowników sieci. Miksery kryptowalut z zasady są usługami, które mogą zwiększyć poziom bezpieczeństwa naszych aktywów. Jednak musimy pamiętać, że mogą być wykorzystywane przez cyberprzestępców do zacierania śladów pochodzenia (np. kradzieży). Dlatego, jeśli zdecydujemy się na korzystanie z tych narzędzi, powinniśmy dokładnie zweryfikować, czy operator danej usługi jest rzetelny i uczciwy. Musimy także pamiętać o tym, że jeśli postanowimy przechowywać swoje kryptowaluty na dysku twardym, zawsze powinniśmy zabezpieczyć nasze urządzenie za pomocą skutecznego oprogramowania antywirusowego” – mówi Mariusz Politowicz z firmy Marken, polskiego dystrybutora oprogramowania Bitdefender.

Źródło:https://bitdefender.pl/grupa-lazarus-uzywa-nowego-miksera-do-prania-skradzionych-bitcoinow/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.

Data udostępnienia: 16.02.2023

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.