

## 24 MLN USD SKRADZIONE W 7 MINUT. PLATFORMA KRYPTOWALUT „ZAPŁACIŁA ZA BŁĄD”

---

Sumę 24 milionów dolarów udało się ukraść hakerowi odpowiedzialnemu za cyberatak na platformę zajmującą się inwestowaniem na rynku kryptowalut. Cyberprzestępca wykorzystał istniejące luki w zabezpieczeniach. „To nasza wina” – mówią przedstawiciele firmy.

Harvest Finance to wirtualna platforma, która umożliwia użytkownikom inwestowanie w kryptowaluty w celu generowania zysku pochodzącego z wahań cen na rynkach. W związku z tym, że firma funkcjonuje w oparciu o cyfrowe rozwiązania jest „atrakcyjnym” podmiotem z punktu widzenia cyberprzestępców.

Odzwierciedleniem takiego stanu rzeczy jest najnowszy incydent, w ramach którego napastnikowi udało się wykraść aktywa o wartości około 24 milionów dolarów. „26 października br. haker dokonał kradzieży środków z zasobów Harvest Finance” – czytamy w oficjalnym komunikacie firmy. Pozyskane przez cyberprzestępcę środki pochodziły z zdecentralizowanej usługi finansowej (ang. decentralized finance service – DeFi).

Władze Harvest Finance postanowiły natychmiast zareagować na cyberatak. Wiadomości potwierdzające incydent oraz opisujące podejmowane przez firmę działania od razu zostały zamieszczone w sieci za pomocą mediów społecznościowych, w tym na Twitterze.

Like other flashloan attacks, the attacker did not give time to respond, performing the attack in 7 minutes end to end.

Wallet of the attacker exiting through renBTC<https://t.co/O6hqnmTXC>

Source: [@devops199fan](#)

— Harvest Finance (@harvest\_finance) [October 26, 2020](#)

Zgodnie z udostępnionymi informacjami haker wykorzystał exploit kryptograficzny, aby wyprowadzić fundusze z Harvest Finance na własne rachunki. Zgodnie ze wstępnymi szacunkami udało mu się ukraść 13 milionów dolarów z puli „USD Coin” (USDC) oraz 11 milionów z puli „USD Tether” (USDT). Co ciekawe, cyberprzestępca dwie minuty po cyberataku, z niewiadomych przyczyn, zwrócił firmie 2,5 miliona dolarów.

Na skutek incydentu firma podjęła decyzję o skierowaniu funduszy z pul płynności do skarbcza. „Środki są obecnie zabezpieczone i nie mogą być przedmiotem dalszych rynkowych manipulacji” – czytamy w

oświadczeniu Harvest Finance. Dla platformy oznacza to spadek akcji i utratę wartości o około 33,8 miliona dolarów.

Jak wskazują władze firmy, haker pozostawił za sobą sporą ilość danych umożliwiających jego identyfikację. Według Harvest Finance jest to osoba dobrze znana w branży kryptowalut.

In addition to the BTC addresses which hold the funds, there is now a significant amount of personally identifiable information on the attacker, who is well-known in the crypto community.

We are putting out a 100k bounty for the first person or team to reach out to the attacker

— Harvest Finance (@harvest\_finance) [October 26, 2020](#)

### **„Otwarte drzwi” dla hakera**

W wiadomościach opublikowanych na Twitterze firma podkreśliła, że cyberatak był możliwy w wyniku jej własnego błędu, co pozostawiło „otwarte drzwi” dla hakera. „Popełniliśmy błąd, przyznajemy się do tego” – czytamy na profilu Harvest Finance. Dodatkowo firma zadeklarowała, że zrobi wszystko, aby ograniczyć tego typu incydenty w przyszłości.

- We take responsibility for this engineering error and are ensuring such incidents are mitigated in the future
- Formulating a remediation plan for affected users is the top priority
- We humbly request that the funds are returned to the deployer so that it can returned to users

— Harvest Finance (@harvest\_finance) [October 26, 2020](#)

Równocześnie władze platformy zwróciły się do cyberprzestępcy „z prośbą” o zwrócenie skradzionych środków. „Udowodniłeś, że masz rację. Jeśli możesz zwrócić środki użytkownikom, społeczność będzie Ci bardzo wdzięczna. Głównym celem jest zwrócenie funduszy tym, których to dotyczy” – czytamy w oświadczeniu firmy. Wydaje się, że scenariusz, w którym haker dobrowolnie oddaje pozyskane 24 mln dolarów jest mało prawdopodobny.

Ponadto Harvest Finance zaoferowała nagrodę w wysokości 400 000 dolarów każdemu, kto znajdzie sposób na zwrot skradzionych środków. „Zdecydowanie zalecamy skupienie wszystkich wysiłków na zapewnieniu pomyślnego zwrotu środków użytkownikom” – podkreśliły władze firmy.

**Czytaj też:** [Amerykanie zlikwidowali „pralnię bitcoinów”. Darknet stracił ważne ogniwo](#)