fundacja instytut
CYBERBEZPIECZEŃSTWA

Przestępstwa związane z kryptowalutami

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

W ciągu ostatniej dekady byliśmy świadkami szybkiego rozwoju kryptowalut, które zyskały na popularności i wywarły duży wpływ na globalny sektor finansowy. Jednak wraz ze wzrostem ich znaczenia pojawiły się także coraz bardziej wyrafinowane oszustwa. Ich sprawcy szukają łatwego zysku kosztem innych. Przez lata znaleźli oni różne sposoby na wykorzystanie tej technologii w swoich nieuczciwych planach.

Czym jest kryptowaluta?

Kryptowaluty to zdecentralizowane pieniądze cyfrowe, które nie istnieją w świecie fizycznym i są jedynie cyfrowym zapisem opartym na specjalnie opracowanym algorytmie. Pierwsza kryptowaluta, czyli bitcoin, została wprowadzona przez osobę lub grupę osób o pseudonimie Satoshi Nakamoto w 2009 r. W kolejnych latach powstały także inne kryptowaluty, m.in. etherum, cardano, solana, litecoin[1]. Jedną z ich zalet jest to, że umożliwiają przesyłanie wartości przez Internet bez pośrednika, takiego jak bank lub podmiot przetwarzający płatności. Ze względu na ich znaczący wzrost popularności zaczęły być kupowane także w celach inwestycyjnych.

Każda kryptowaluta powiązana jest z blockchainem, czyli technologią służącą do przechowywania oraz przesyłania informacji o transakcjach zawieranych w Internecie, które zostają ułożone w postaci następujących po sobie bloków danych. Każdy z nich zawiera informacje o określonej liczbie transakcji, a szereg bloków składa się na pewien rodzaj łańcucha[2]. Transakcje, które zostają zapisane w łańcuchu, są nieodwracalne. Aby powstała kolejna jednostka danej kryptowaluty, konieczne jest rozwiązanie skomplikowanych działań matematycznych w celu zatwierdzenia nowego bloku i przyłączenia go do łańcucha. Proces ten nazywany jest kopaniem kryptowalut. Do wykonywania tych działań wykorzystywane są zaawansowane i drogie komputery o ogromnej mocy obliczeniowej, które pobierają duże ilości energii elektrycznej[3]. Blockchain charakteryzuje się dużym poziomem bezpieczeństwa i odpornością na podrobienia oraz manipulacje.

1 D. Ashmore, F. Powell, Bitcoin Price History 2009 to 2022, Forbes, 14.06.2023 r., https://www.forbes.com/advisor/in/investing/cryptocurrency/bitcoin-price-history-chart/ (dostęp: 26.07.2023).

2 What is blockchain?, McKinsey, 5.12.2022 r., https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-blockchain (dostęp: 26.07.2023).

3 S. Machniewski, Na czym polega kopanie kryptowalut?, Money.pl, 7.05.2022 r., https://www.money.pl/gospodarka/na-czym-polega-kopanie-kryptowalut-6763429848849216a.html (dostęp: 26.07.2023).

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

Cryptojacking

Kopanie kryptowalut wymaga odpowiedniego sprzętu, który zużywa duże ilości energii. Zazwyczaj używane są do tego zaawansowane komputery, ponieważ wykorzystanie zwykłego urządzenia tego rodzaju daje słabe efekty. Mając jednak do dyspozycji wiele zwykłych komputerów, można z kopania kryptowalut czerpać duże korzyści. Cryptojacking polega na zainfekowaniu cudzych urządzeń złośliwym oprogramowaniem i wykorzystaniu ich do kopania kryptowalut. Hacker korzysta zatem z mocy obliczeniowej sprzętu bez wiedzy i zgody jego właścicieli i czerpie z tego korzyści w postaci wydobytych kryptowalut[4]. Metodą często wykorzystywaną do zainfekowania komputera złośliwym oprogramowaniem do kopania kryptowalut jest phishing[5].

Cryptojacking jest niebezpieczny dla osoby, której komputer został zainfekowany, ponieważ złośliwe wydobycie kryptowalut zużywa moc obliczeniową urządzenia, generując spore koszty związane ze wzrostem rachunków za energię elektryczną, spadkiem wydajności sprzętu czy szybszym zużyciem podzespołów i częstszą koniecznością ich naprawy lub wymiany[6]. Oprogramowanie do wydobywania kryptowalut działa w tle i często pozostaje niezauważone przez użytkownika danego komputera. Istnieje jednak kilka symptomów, które mogą świadczyć o tym, że nasz sprzęt jest wykorzystywany do wydobywania kryptowalut. Nasze podejrzenia powinny pojawić się wówczas, gdy nasz komputer zaczyna wolniej pracować, częściej się przegrzewać i zużywać szybciej poszczególne podzespoły. Może być to bowiem efektem wykonywania skomplikowanych obliczeń potrzebnych do wydobywania kryptowalut. Cryptojacking może wiązać się ze sporymi stratami, dlatego warto się odpowiednio zabezpieczać, aby nie paść jego ofiarą. Poniższa grafika przedstawia kilka wskazówek, jak uchronić swój komputer przed cryptojackingiem.

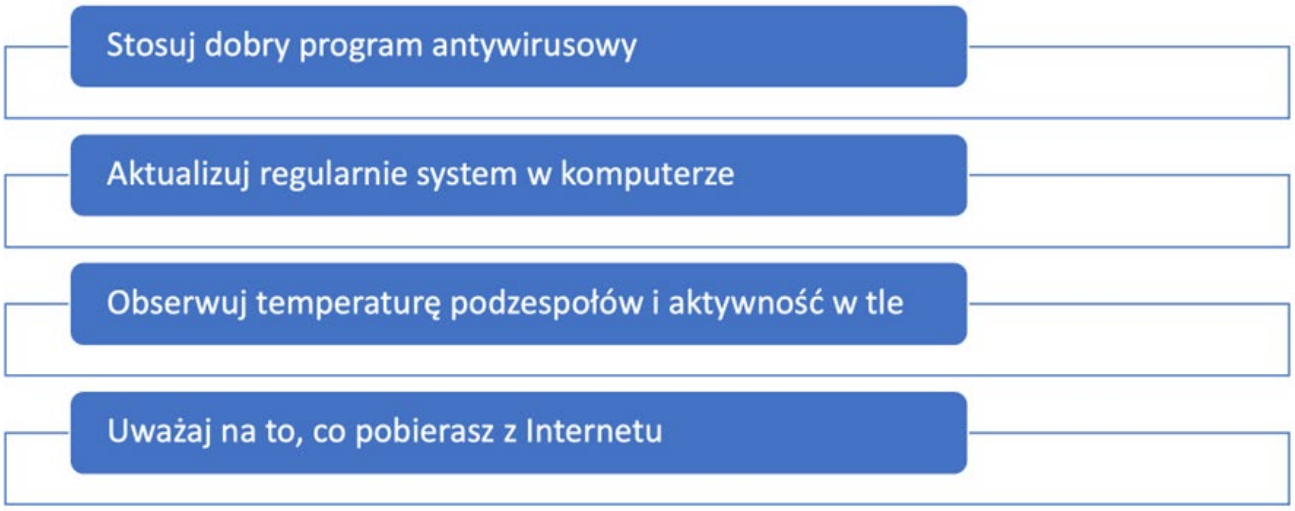
Podstawą jest dobry program antywirusowy, który nie pozwoli na zainfekowanie komputera złośliwym oprogramowaniem. W celu zadbania o bezpieczeństwo należy także regularnie przeprowadzać aktualizacje systemu, ponieważ często mają one na celu zlikwidowanie luk w bezpieczeństwie.

4 **Cryptojacking, Malwarebytes,** https://pl.malwarebytes.com/cryptojacking/ **(dostęp: 26.07.2023).**

5 **H. Tur, Cryptojacking – czym jest, jak go unikać i jak się go pozbyć?, PCWorld, 3.08.2019 r.,** https://www.pcworld.pl/porada/Cryptojacking-czym-jest-jak-go-unikac-i-jak-sie-go-pozbyc,414660.html **(dostęp: 26.07.2023).**

6 **L. Klusaitė, Co to jest cryptojacking i jak się przed nim bronić?, NordVPN, 29.03.2023 r.,** https://nordvpn.com/pl/blog/co-to-jest-cryptojacking/ **(dostęp: 26.07.2023).**

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości



Warto również na bieżąco obserwować, jak zachowuje się nasz komputer i czy nie daje podejrzanych sygnałów, które mogą świadczyć o tym, że został zainfekowany. Jeśli tak, należy jak najszybciej usunąć z niego złośliwe oprogramowanie. Ponadto zawsze warto zachować ostrożność w Internecie i nie wchodzić na podejrzane strony internetowe, nie pobierać podejrzanych plików ani nie klikać w niesprawdzone linki.

Wyłudzanie pieniędzy

Wzrost popularności kryptowalut oraz ich wartości na przestrzeni ostatnich lat sprawił, że stały się one atrakcyjne również z inwestycyjnego punktu widzenia. Wykorzystują to oszuści, którzy m.in. wyłudzają pieniądze poprzez podszywanie się pod platformy inwestycyjne oferujące inwestycje w kryptowaluty lub na rynku forex i gwarantują szybkie zyski. Zakładają oni fałszywe strony internetowe i z użyciem socjotechniki reklamują się w mediach społecznościowych. Namawiając ofiarę na inwestycje w kryptowaluty, są w stanie uzyskać od niej istotne dane osobowe czy też dane logowania do kont bankowych, co może doprowadzić do utraty przez tę osobę wszystkich pieniędzy na koncie.

Jedną z platform, która okazała się oszustwem inwestycyjnym, była Global Maxis. Jak podaje policja, osoby skuszone przez

tę platformę wizją szybkiego zarobku rejestrowały się na stronie internetowej, a następnie kontaktował się z nimi konsultant, który prosił o zainstalowanie na komputerach oprogramowania umożliwiającego obsługę pulpitu zdalnego. Za jego pomocą oszuści przejmowali kontrolę nad urządzeniami klientów, uzyskując także dostęp do kont bankowych pokrzywdzonych osób[7]. Następnie przelewali pieniądze z konta bankowego na inne konta, tak że ostatecznie trafiały one poza granice Polski i Europejskiego Obszaru Gospodarczego.

Podczas rejestracji na stronie internetowej Global Maxis konieczne było także podanie swoich danych osobowych, w tym przesłanie skanu dowodu osobistego. W ten sposób przestępcy pozyskali wiele danych osobowych, które następnie zostały wykorzystane do zaciągania kredytów i pożyczek na swoje ofiary[8]. Osoby rejestrujące się w Global Maxis zatem nie tylko straciły środki ze swojego konta bankowego, lecz także muszą spłacić dług.

Podsumowanie

Cryptojacking i podszywanie się pod platformy inwestycyjne w celu wyłudzenia pieniędzy to jedne z najpopularniejszych oszustw związanych z kryptowalutami. Pierwsze polega na wykorzystaniu cudzego sprzętu do wydobywania kryptowalut, a drugie na wprowadzeniu osoby w błąd celem wyłudzenia od niej pieniędzy. Rozwój nowych technologii sprawia, że w przyszłości mogą pojawiać się także inne oszustwa, które będą bazować na kryptowalutach. Kluczowe zatem jest bezpieczne i rozważne korzystanie z Internetu oraz stosowanie odpowiednich zabezpieczeń swojego komputera. Należy pamiętać, że uzyskiwanie wysokich i szybkich zysków jest mało prawdopodobne, a wobec podmiotów, które je oferują, należy zachować ostrożność.

7 Ostrzegamy przed oszustami podającymi się za brokerów finansowych, Policja Małopolska, https://malopolska.policja.gov.pl/krk/aktualnosci/12479,Ostrzegamy-przed-oszustami-podajacymi-sie-za-brokerow-finansowych-Material-wideo.html (dostęp: 26.07.2023).

8 Global Maxis – oszustwo (opinie). Jak wygląda? Jak odzyskać pieniądze?, Eurolege, 17.05.2022 r., https://www.eurolege.pl/global-maxis-oszustwo/ (dostęp: 26.07.2023).

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

Bibliografia

1. Ashmore D., Powell F., *Bitcoin Price History 2009 to 2022*, Forbes, 14.06.2023 r., https://www.forbes.com/advisor/in/investing/cryptocurrency/bitcoin-price-history-chart/ (dostęp: 26.07.2023).
2. *Cryptojacking*, Malwarebytes, https://pl.malwarebytes.com/cryptojacking/ (dostęp: 26.07.2023).
3. *Global Maxis – oszustwo (opinie). Jak wygląda? Jak odzyskać pieniądze?*, Eurolege, 17.05.2022 r., https://www.eurolege.pl/global-maxis-oszustwo/ (dostęp: 26.07.2023).
4. Klusaitė L., *Co to jest cryptojacking i jak się przed nim bronić?*, NordVPN, 29.03.2023 r., https://nordvpn.com/pl/blog/co-to-jest-cryptojacking/ (dostęp: 26.07.2023).
5. Machniewski S., *Na czym polega kopanie kryptowalut?*, Money.pl, 7.05.2022 r., https://www.money.pl/gospodarka/na-czym-polega-kopanie-kryptowalut-6763429848849216a.html (dostęp: 26.07.2023).
6. *Ostrzegamy przed oszustami podającymi się za brokerów finansowych*, Policja Małopolska, https://malopolska.policja.gov.pl/krk/aktualnosci/12479,Ostrzegamy-przed-oszustami-podajacymi-sie-za-brokerow-finansowych-Material-wideo.html (dostęp: 26.07.2023).
7. Tur H., *Cryptojacking – czym jest, jak go unikać i jak się go pozbyć?*, PCWorld, 3.08.2019 r., https://www.pcworld.pl/porada/Cryptojacking-czym-jest-jak-go-unikac-i-jak-sie-go-pozbyc,414660.html (dostęp: 26.07.2023).
8. *What is blockchain?*, McKinsey, 5.12.2022 r., https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-blockchain (dostęp: 26.07.2023).

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

www.instytutcyber.pl

fundacja instytut
CYBERBEZPIECZEŃSTWA

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości