Bitdefender

# Czy Twój komputer jest zainfekowany koparką kryptowalut?

13.06.2024

Cryptojacking to czynność polegająca na przejęciu zasobów sprzętowych danej osoby poprzez włamanie do komputera PC za pomocą zmodyfikowanej koparki kryptowalut. Zasadniczo przestępcy instalują aplikację do wydobywania kryptowalut, która wykorzystuje sprzęt ofiary na jej korzyść. Na szczęście sporo charakterystycznych znaków może zdradzić obecność górnika kryptowalut w systemie. Dlatego w tym artykule przedstawimy metody na sprawdzenie, czy Twój komputer jest zainfekowany koparką kryptowalut.

**Wydobywanie kryptowalut**

Wydobywanie kryptowalut jest legalną działalnością i wiele osób wybiera tę metodę do wzbogacenia się. Niestety próg wejścia jest bardzo wysoki, ponieważ trzeba zainwestować w drogi sprzęt. Dlatego przestępcy doszli do wniosku, że mogą wykorzystać sprzęt innych osób do wydobywania

kryptowalut, aby uniknąć związanych z tym kosztów.

Chociaż wydobywanie kryptowalut może generować zyski, dzieje się tak poprzez drastyczne zwiększenie rachunków za energię elektryczną, nie wspominając o tym, że zwiększy to zużycie sprzętu. Wszystko to ma swoją cenę, która łatwo przekłada się na objawy, które każdy może zaobserwować.

Jeśli korzystasz z rozwiązania antywirusowego, to nie będziesz musiał się martwić o koparki kryptowalut w swoim systemie, chyba że je zainstalujesz. Jeśli Twój sprzęt nie jest zabezpieczony, to możesz sprawdzić, czy jest zainfekowany w inny sposób. Poniżej zamieszczamy kilka symptomów, które możesz zaobserwować, gdy Twój komputer jest wykorzystywany do kopania kryptowalut.

**Wysokie użycie procesora lub karty graficznej**

Jedną z oznak, że system może być zagrożony, jest to, że procesor lub karta graficzna działa nawet wtedy, gdy nie ma bieżącego zadania. Wielu internautów zaczyna podejrzewać, że coś może być nie tak, gdy na przykład ich ulubiona gra zaczyna gorzej działać, nawet jeśli w przeszłości nie zauważali tego problemu. Zwykle można wykryć winowajcę w Menedżerze zadań systemu Windows, ponieważ pochłania on dużo zasobów.

**Zwiększony hałas wentylatora i przegrzanie**

Gdy procesor lub karta graficzna otrzymuje intensywne zadania,

nagrzewa się, co powoduje, że wentylatory pracują głośniej. Jeśli nie robisz niczego, co wymagałoby od wentylatorów pracy na pełnych obrotach, odpowiedzialny może być inny proces. W rzeczywistości sytuacja może stać się na tyle tragiczna, że system chłodzący nie będzie w stanie nadążyć, a system okresowo się przegrzeje.

**Spadek wydajności**

Koparki kryptowalut mają wpływ nie tylko na gry. Niektóre z tych aplikacji są tak agresywne, że wpływają nawet na proste czynności, takie jak przeglądanie Internetu lub oglądanie filmu. Gdy proces eksploracji zużywa znaczne zasoby systemowe, do zwykłych zadań dostępnych jest mniej zasobów na inne czynności.

**Niewyjaśniona aktywność sieciowa**

Kopacze kryptowalut komunikują się z serwerami zewnętrznymi w celu koordynowania procesu wydobycia i aktualizacji transakcji blockchain, dlatego czasami użytkownicy mogą odkryć nietypową aktywność sieciową.

**Częste awarie**

Wykorzystywanie sprzętu do granic możliwości i ciągłe przegrzewanie systemu może obciążać system operacyjny i prowadzić do częstych awarii.

**Krótka żywotność baterii**

Intensywne wykorzystanie procesora lub karty graficznej przez oprogramowanie do kopania kryptowalut powoduje znacznie szybsze zużycie baterii niż zwykle na urządzeniach mobilnych lub laptopach. Ten typ złośliwej aktywności jest łatwiejszy do wykrycia na urządzeniach zasilanych bateriami.

**Nieznane procesy w Menedżerze zadań**

Jeśli nie możesz rozpoznać niektórych procesów uruchomionych w Menedżerze zadań systemu Windows i zużywają one duży procent zasobów systemowych, możesz sprawdzić w Internecie, czy nie są to kopacze kryptowalut udający zwykłe aplikacje.

**Zablokowany dostęp do narzędzi monitorowania systemu**

Jednym ze sposobów, w jaki złośliwe oprogramowanie stara się jak najdłużej pozostać poza zasięgiem radaru, jest wyłączenie dostępu do menedżera zadań lub innych narzędzi monitorowania systemu, aby utrudnić wykrycie.

„Wydobywanie kryptowalut jest legalne tylko wtedy, gdy znajduje się pod ścisłą kontrolą właścicieli urządzeń. Przestępcy używający złośliwego oprogramowania do kontrolowania sprzętu innych użytkowników sieci w celach zarobkowych nigdy nie znikną. Dlatego warto pamiętać o tym, aby zawsze korzystać ze skutecznego systemu antywirusowego, a także zachowywać czujność w przypadkach, gdy nasz system bez wyraźnego powodu zaczyna zwalniać lub pracować w niecodzienny sposób” – mówi

Arkadiusz Kraszewski z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło:https://bitdefender.pl/czy-twoj-komputer-jest-zainfekowany-koparka-kryptowalut/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 13.06.2024
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.