Bitdefender

Hakerzy wykorzystują ofiary do kopania kryptowalut

14.04.2023

Zdalne włamanie się do urządzenia lub oprogramowania wymaga sporej wiedzy technicznej. A gdyby hakerzy mogli przekonać ludzi do zhakowania swoich własnych urządzeń? Wymaga to znacznie mniej pracy i nie tak dużej wiedzy technicznej. Dlatego cyberprzestępcy znaleźli nowy sposób, aby nakłonić ludzi do pobrania i zainstalowania złośliwego oprogramowania, które będzie wykorzystywało procesory ofiar do kopania kryptowalut dla hakerów.

Według raportu TechRadar badacz bezpieczeństwa Rintaro Koike wykrył złośliwą kampanię, w której hakerzy wymyślili sposób na złamanie zabezpieczeń legalnych stron internetowych (głównie w Japonii, Korei Południowej i Hiszpanii) oraz wyświetlanie fałszywych powiadomień o aktualizacjach przeglądarki internetowej Chrome.

Nowa kampania phishingowa

Gdy cyberprzestępcy wysyłają wiadomość phishingową, najczęściej informują o tym, że należy natychmiastowo podjąć jakieś kroki, aby ustrzec się przed rzekomym niebezpieczeństwem. To sprawdzona metoda, ale w tym przypadku przestępcy wybrali inną drogę.

„Wystąpił błąd podczas automatycznej aktualizacji Chrome. Zainstaluj pakiet aktualizacji ręcznie później lub poczekaj na następną automatyczną aktualizację" – brzmi wyświetlona fałszywa wiadomość. Brak pilności może być jeszcze bardziej przekonujący dla niektórych użytkowników.

Badacz bezpieczeństwa odkrył również, że kod jest kompatybilny z ponad 100 językami, więc prawdopodobnie stanowi część większej kampanii gotowej do wdrożenia na całym świecie.

Hakerzy wykorzystują ofiary do kopania kryptowalut – jak się bronić?

Oczywiście plik pobierany przez ofiarę nie ma nic wspólnego z aktualizacją Chrome. W rzeczywistości jest to koparka kryptowalut Monero, która użyje procesora do wydobycia kryptowalut bez wiedzy użytkownika. Jak zauważają badacze – w tym przypadku nie każdy antywirus jest w stanie ochronić urządzenie przed zainfekowaniem.

„Najlepszą ochroną przed tą kampanią phishingową jest podstawowa wiedza informatyczna. Użytkownicy powinni wiedzieć, że Google Chrome posiada własne mechanizmy aktualizacji i nie ma potrzeby ręcznego aktualizowania przeglądarki. Warto pamiętać także o zabezpieczeniu swojego urządzenia za pomocą antywirusa wyposażonego w

odpowiedni moduł antyphishingowy, który zminimalizuje ryzyko wejścia w sfałszowany link prowadzący do niebezpiecznej strony internetowej” – radzi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło: https://bitdefender.pl/hakerzy-wykorzystuja-ofiary-do-kopania-kryptowalut/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 14.04.2023
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.