aut. Małgorzata Fraser 02.08.2021

PRZEGLĄDARKA BRAVE I REKLAMY GOOGLE WYKORZYSTANE DO ROZPOWSZECHNIANIA ZŁOŚLIWEGO OPROGRAMOWANIA

Marka przeglądarki Brave, popularnej wśród osób zainteresowanych ochroną swojej prywatności posłużyła cyberprzestępcom do rozpowszechniania złośliwego oprogramowania – podał serwis Ars Technica. Z wykorzystaniem reklam Google promowano link do fałszywej domeny, zbliżonej nazwą do oficjalnej strony przeglądarki, na której znajdowało się złośliwe oprogramowanie pozwalające wykradać wrażliwe dane użytkowników internetu.

Jak działał atak?

Atak opiera się na wykorzystaniu domeny bravė[.]com, z nazwą łudząco podobną do prawdziwego adresu domeny strony internetowej przeglądarki Brave. Jedyne, czym różnią się oba adresy, to znak diakrytyczny nad „e" oraz to, że kliknięcie „Pobierz Brave" na fałszywej stronie internetowej instaluje na komputerze użytkownika złośliwego oprogramowania znanego jako ArechClient i SectopRat.

Ruch do fałszywej strony cyberprzestępcy kierowali z wykorzystaniem reklam Google w wyszukiwarce internetowej, które zostały ustawione tak, aby wyświetlały się internautom poszukującym treści powiązanych z przeglądarką. Reklamy wyglądały przy tym bardzo wiarygodnie i kierowały ruch do złośliwej witryny nawigując go przedtem przez szereg przekierowań.

Co chcieli osiągnąć cyberprzestępcy?

W analizie z 2019 r. firma zajmująca się cyberbezpieczeństwem G Data opisała instalowane przez złośliwą witrynę oprogramowanie jako trojana umożliwiającego zdalny dostęp do atakowanego komputera, pozwalającego również na strumieniowanie widoku ekranu użytkownika.

G Data opublikowało również aktualizację swojego opracowania na temat tego narzędzia, w którym eksperci stwierdzili, iż zostało ono rozbudowane o kolejne funkcjonalności, pozwalające na wykradanie wrażliwych danych ofiary, profilowanie jej systemu, a także zdalną łączność z serwerem atakujących.

Według specjalistów z innej firmy – Silent Push – ta sama metoda została wykorzystana do ataku w oparciu o marki innych popularnych programów, takich jak np. komunikator Telegram, czy przeglądarka TOR.

Jak zadziałały firmy, które wykorzystano w ataku?

Google po otrzymaniu od firmy Brave informacji o złośliwej kampanii usunęło reklamy pomagające w jej realizacji, a firma NameCheap, którą wykorzystano do rejestracji fałszywej domeny, usunęła jej

adres z sieci.

To, co zwraca uwagę, to fakt, że fałszywa strona Brave była bardzo trudna do odróżnienia od prawdziwej – miała ważny certyfikat TLS i według Ars Techniki wykrycie oszustwa mogło być wyzwaniem nawet dla osób uważnie korzystających z internetu.

Chcemy być także bliżej Państwa – czytelników. Dlatego, jeśli są sprawy, które Was nurtują; pytania, na które nie znacie odpowiedzi; tematy, o których trzeba napisać – zapraszamy do kontaktu. Piszcie do nas na: redakcja@cyberdefence24.pl. Przyszłość przynosi zmiany. Wprowadzamy je pod hasłem #CyberIsFuture.