Cyberdefence 24

aut. Szymon Palczewski 11.05.2021

POLSKA NA MAPIE CELÓW GLOBALNEJ KAMPANII RANSOMWARE

Podmioty z Polski są celem trwającej kampanii ransomware, mającej charakter globalny. Wirus oferowany jest w dark webie i umożliwia hakerom m.in. przechwytywanie danych kart płatniczych oraz kopiowanie lub usuwanie plików. Phishing i spam stanowią główną metodę rozpowszechniania złośliwego oprogramowania.

Australijskie Centrum Cyberbezpieczeństwa (ang. Australian Cyber Security Centre – ACSC) ostrzega przed trwającą kampanią ransomware, wykorzystującą złośliwe oprogramowanie o nazwie „Avaddon". W alercie wskazano, że wrogie działania są wymierzone w podmioty z różnych stron świata.

Specjaliści tłumaczą, że Avaddon to wariant ransomware, który został po raz pierwszy wykryty w lutym 2019 roku. Z reguły był używany do prowadzenia operacji o charakterze cyberprzestępczym. Oprogramowanie jest oferowane w dark webie jako usługa typu ransomware-as-a-service (RaaS) i pozwala hakerom na m.in. przechwytywanie danych kart płatniczych, kopiowanie lub usuwanie plików, szyfrowanie systemów zmienianie ustawień.

> *Australijskie Centrum Cyberbezpieczeństwa jest pewne, że w kilku przypadkach oprogramowanie ransomware Avaddon miało bezpośredni wpływ na podmioty będące celem, w szczególności w Australii.*
>
> Australijskie Centrum Cyberbezpieczeństwa

Jak alarmują specjaliści ACSC, cyberataki z wykorzystaniem Avaddona, prowadzone w ramach trwającej kampanii hakerskiej, miały miejsce w różnych częściach świata. Wśród celów znajdowały się podmioty z Polski, a także: Australii, Brazylii, Chin, Czech, Niemiec, Indonezji, Jordanii, Hiszpanii, Wielkiej Brytanii, Belgii, Kanady, Kostaryki, Francji, Indii, Włoch, Peru, Portugalii, Zjednoczonych Emiratów Arabskich oraz Stanów Zjednoczonych.

Hakerzy używający tej odmiany ransomware swoje działania ukierunkowują na takie branże jak: edukacja, budownictwo, transport i logistyka, opieka zdrowotna, IT, przemysł, handel, wirtualna rozrywka, lotnictwo, energetyka, finanse, administracja państwowa, turystyka, marketing i farmacja.

W ramach kampanii wrogie działania prowadzone są najczęściej za pomocą phishingu i spamu w celu rozpowszechniania złośliwych plików JavaScript. W treści wiadomości znajdują się rzekomo zdjęcia oraz materiały, które mają być kompromitujące dla ofiary, a przez to skłonić ją do ich otwarcia.

Australijskie Centrum Cyberbezpieczeństwa wskazuje, że hakerzy posługujący się wirusem zazwyczaj żądają okupu w bitcoinach, w zamian oferując narzędzie deszyfrujące „Avaddon General Decryptor”. W tym celu stosują strategię „podwójnego wymuszania”. Polega ona na wywarciu presji na ofiarę, aby spełniła stawiane warunki, poprzez groźbę opublikowania pozyskanych danych oraz przeprowadzenie ataku typu DDoS.

Czytaj też: Atak ransomware wstrzymał dostawy paliwa w USA