Bitdefender

Fałszywe sieci Wi-Fi i hotspoty „Evil Twin”

21.02.2023

Chyba każdy użytkownik sieci korzystał kiedyś z ogólnodostępnej sieci Wi-Fi w miejscach publicznych. Niestety niewielu z nas zdaje sobie sprawę z tego, jakie może to nieść za sobą niebezpieczeństwo. Cyberprzestępcy coraz częściej tworzą fałszywe sieci Wi-Fi, aby za ich pomocą kraść cenne dane osobowe, hasła i loginy nieświadomych użytkowników.

Łączenie się z publicznymi sieciami Wi-Fi jest niebezpieczne samo w sobie z powodu ogromnej liczby zagrożeń związanych z kierowaniem ruchu przez otwarte, często nieuregulowane środowisko. Jednak fałszywe hotspoty Wi-Fi, znane również jako hotspoty Evil Twin, to inne narzędzie, stworzone przez hakerów do zachęcania niczego niepodejrzewające ofiary do łączenia się z niebezpiecznymi stronami i witrynami.

Czym są fałszywe sieci Wi-Fi?

Hakerzy coraz częściej tworzą fałszywe sieci w celu monitorowania ruchu,

kradzieży danych uwierzytelniających i przeprowadzania ataków typu man-in-the-middle (MITM).

W większości przypadków te fałszywe hotspoty wydają się niegroźne, ponieważ używają tej samej nazwy co sieć, którą naśladują. Zidentyfikowanie fałszywego hotspotu Wi-Fi na pierwszy rzut oka jest praktycznie niemożliwe, chyba że użytkownik specjalnie poszukuje takiej sieci.

Sieci publiczne często nie używają haseł lub stosują hasła proste do odgadnięcia, co czyni je bardzo podatnymi na ataki. Co gorsza niektóre miejsca publicznie wyświetlają hasło do swoich hotspotów Wi-Fi, dzięki czemu są jeszcze łatwiejszym celem do podszycia się pod nią. Ponieważ fałszywy bliźniaczy hotspot całkowicie kopiuje legalną sieć wraz z hasłem dostępu, często nie wzbudza podejrzeń użytkowników.

Dlaczego fałszywe hotspoty Wi-Fi są niebezpieczne?

Podobnie jak dostawcy usług internetowych operatorzy hotspotów Evil Twin przechwytują cały ruch po połączeniu się z ich fałszywą siecią. Bez odpowiedniego szyfrowania hakerzy widzą wszystko, co robisz online: jakie witryny odwiedzasz, ile czasu w nich spędzasz, a nawet mogą śledzić ruch generowany przez aplikacje internetowe na Twoim urządzeniu.

Wielu użytkowników twierdzi, że HTTPS wystarczy, aby odeprzeć próby przechwycenia prywatnych danych przez przestępców. Witryny HTTPS szyfrują Twój ruch w sieci, więc osoby atakujące nie powinny widzieć zbyt

wiele informacji poza witryną lub usługą, z którą się łączysz.

Jednak przy użyciu odpowiednich narzędzi hakerzy mogą przeprowadzać ataki polegające na usuwaniu SSL podczas przekierowywania Cię do wersji HTTP witryny, do której próbujesz uzyskać dostęp. W ten sposób ujawniają wszystkie dane z ruchu, które zostałyby zaszyfrowane przez SSL/TLS, w tym poświadczenia, dane osobowe (PII), szczegóły płatności, a nawet wiadomości na różnych platformach.

W jaki sposób bronić się przed fałszywymi sieciami Wi-FI?

Chociaż nie ma pewnego sposobu na wykrycie hotspotu Evil Twin, VPN może być najlepszą opcją bezpiecznego dostępu do publicznych sieci Wi-Fi.

Korzystanie z godnej zaufania sieci VPN i włączenie jej przed połączeniem z publicznymi hotspotami może zapobiec zbieraniu informacji o Tobie przez cyberprzestępców. Szyfrując ruch internetowy, sieci VPN uniemożliwiają hakerom przechwycenie Twojego ruchu sieciowego i kradzieży danych osobowych lub danych uwierzytelniających.

Zespół Bitdefender rekomenduje, aby przed połączeniem się z jakimkolwiek publicznym hotspotem Wi-Fi – zwłaszcza takim bez hasła – skorzystać z VPN. Wprawdzie nie zagwarantuje to ochrony we wszystkich przypadkach, jednak znacząco zwiększy szansę na to, że Twoje dane pozostaną prywatne i bezpieczne.

„Fałszywe sieci Wi-Fi to nadal bardzo poważny problem, który może być szczególnie dotkliwy w takich miejscach publicznych jak: szkoły, uniwersytety, centra handlowe i parki. Hakerzy często tworzą fałszywe hotspoty pozwalające im kraść dane niczego nieświadomych użytkowników, którzy połączyli się z ich siecią. Dlatego zalecamy korzystanie w takich miejscach z komórkowej transmisji danych, a jeśli to niemożliwe, łączyć się z siecią VPN" – radzi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora Bitdefender.

Źródło: https://bitdefender.pl/falszywe-sieci-wi-fi-i-hotspoty-evil-twin/

Data udostępnienia: 21.02.2023
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.