Bitdefender

Hakerzy rozpowszechniają rozszerzenie Rogue ChatGPT Chrome w celu przejęcia kont na Facebooku

27.03.2023

Zespół Bitdefender niedawno zauważył cyberprzestępców kradnących konta na Facebooku przy użyciu złośliwej wersji legalnego rozszerzenia przeglądarki ChatGPT dostępnego w Chrome Web Store. Nieuczciwe rozszerzenie, nazwane „ChatGPT for Google”, zostało pobrane ponad 9 000 razy w dedykowanym sklepie internetowym przeglądarki.

Chociaż to fałszywe rozszerzenie reklamuje się jako narzędzie integrujące ChatGPT z wynikami wyszukiwania przeglądarki, to niestety może także służyć do kradzieży sesyjnych plików cookie Facebooka.

Hakerzy rozpowszechniają rozszerzenie Rogue ChatGPT Chrome

Hakerzy zaczęli reklamować fałszywe rozszerzenie do ChatGPT 14 marca (miesiąc po dacie jego publikacji) za pomocą reklam w wyszukiwarce Google. Podobno wyszukiwanie „Chat GPT 4”, „ChatGPT 4” lub podobnych odmian słów kluczowych powodowało wyświetlanie użytkownikom sponsorowanych wyników prowadzących do tego złośliwego narzędzia.

Kliknięcie w polecane linki przenosiło internautów do nieuczciwej strony docelowej reklamującej „ChatGPT dla Google”. Dalsze podążanie tą ścieżką prowadziło ich do „oficjalnej” strony rozszerzenia w sklepie internetowym Chrome.

Aby uniknąć dodatkowych podejrzeń, hakerzy załączyli złośliwy kod, dzięki któremu mogli kraść pliki cookie, używając prawidłowego kodu rozszerzenia. Innymi słowy internauci nadal mogli z niego korzystać, co odwracało ich uwagę od ukrytego celu narzędzia.

Po instalacji rozszerzenie wykorzystuje funkcję obsługi do zbierania plików cookie sesji Facebooka. Następnie szyfruje je kluczem AES i eksfiltruje dane na serwer atakującego za pomocą żądania GET.

Hakerzy przejmują konta na Facebooku

Po odszyfrowaniu skradzionych plików cookie cyberprzestępcy mogą ich użyć do zalogowania się na konta ofiar na Facebooku z pełnymi prawami własności. Jak donosi BleepingComputer, sprawcy wykorzystują przejęte

konta do prowadzenia złośliwych kampanii i rozpowszechniania zakazanych materiałów, takich jak propaganda ISIS.

Złośliwe rozszerzenie posiada również prymitywny mechanizm trwałości, aby uniemożliwić ofiarom odzyskanie kont. Po ich przejęciu narzędzie automatycznie zmienia dane do logowania i nazwy profili, następnie ustawia zdjęcie profilowe tak, aby pasowało do fałszywego użytkownika o nazwie „Lilly Collins".

Na szczęście rozszerzenie zostało usunięte z Chrome Web Store. Jednak eksperci ds. bezpieczeństwa uważają, że cyberprzestępcy mogą mieć plan tworzenia kopii zapasowych w postaci uśpionego, równie złośliwego rozszerzenia.

„Hakerzy często wykorzystują rozszerzenia do przeglądarek, żeby infekować urządzenia użytkowników Internetu. W tym celu podszywają się pod popularne aplikacje, takie jak ChatGPT, aby skłonić jak najwięcej internautów do pobrania niebezpiecznego pliku. Co ciekawe, bardzo często sfałszowane rozszerzenia faktycznie spełniają swoje funkcje, jednak jednocześnie pobierają i wysyłają hakerowi informacje dotyczące naszej aktywności w sieci. Dlatego zawsze pamiętajmy o tym, aby zabezpieczyć nasze urządzenia za pomocą skutecznego antywirusa wyposażonego w odpowiednie moduły antyphishingowe" – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło: https://bitdefender.pl/hakerzy-rozpowszechniaja-rozszerzenie-chatgpt/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.

Data udostępnienia: 27.03.2023

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.