Bitdefender

Gracze, uważajcie na linki GTA VI Beta Version do pobrania z reklam sponsorowanych na Facebooku

22.07.2024

Premiera GTA VI na PS5 i Xbox Series planowana jest na jesień 2025 r., a gracze na PC będą musieli poczekać trochę dłużej. Nie powstrzymało to jednak podmiotów zagrażających przed wykorzystaniem wyczekiwanej gry akcji-przygody od amerykańskiego wydawcy gier. Badacze z Bitdefender wykryli wysoce podejrzane reklamy na Facebooku, promujące fałszywe wersje beta GTA VI, które można pobrać bezpłatnie na komputery PC.

Oto co odkryli badacze Bitdefender

- Strona na Facebooku promowała darmowy dostęp do wersji beta GTA dla pierwszych 100 osób za pośrednictwem sponsorowanych

reklam na Facebooku w dniach 16–18 lipca.

- Na stronie wyświetlano trzy oddzielne reklamy, obie wykorzystujące ten sam przekaz i grafikę. Na dzień 19 lipca żadna ze złośliwych reklam nie była już aktywna.

- Potencjalny zasięg tych reklam to setki internautów, a zgodnie z polityką przejrzystości UE Meta, docelowa grupa odbiorców to osoby w wieku od 18 do 65 lat. Ponadto podział demograficzny pokazuje złośliwe reklamy skierowane do użytkowników w Europie, w tym we Francji, Polsce, Rumunii, Niemczech, Hiszpanii, na Węgrzech, we Włoszech, Grecji, Holandii i Szwecji.

Reklamy zachęcają graczy do dołączenia do wersji beta GTA VI i pobrania wersji na swoje urządzenie. Przycisk Pobierz powiązany z reklamami prowadzi użytkowników do złośliwej strony internetowej. Po kliknięciu przycisku „Pobierz teraz” znajdującego się nad fałszywym licznikiem pobrań, z Dropboxa pobierana jest złośliwa próbka.

Ta złośliwa domena najwyraźniej hostuje również oszustwo związane z Ethereum na swojej stronie indeksowej, która została utworzona 27 czerwca 2024 r.

Oto analiza złośliwej sprzedaży przeprowadzona przez badacza ds. bezpieczeństwa Andrieja Mogage'a:

Plik MSI pobrany za pośrednictwem reklamy na Facebooku podszywa

się pod legalnego instalatora GTA VI i naśladuje proces instalacji. Sam plik jest złośliwy, z wieloma podobieństwami do złośliwego oprogramowania FakeBat loader.

Wniosek ten wyciągnięto na podstawie sposobu działania: wykorzystano plik MSI podszywający się pod legalne oprogramowanie, aby wdrożyć złośliwe ładunki utworzone przez innych operatorów wraz ze skryptami programu PowerShell.

Oprogramowanie malware FakeBat loader jest szeroko rozpowszechniane za pośrednictwem fałszywych stron internetowych i reklam, aby ułatwić pobieranie złośliwego oprogramowania następnej generacji, takiego jak programy kradnące informacje i trojany RAT (Remote Access Trojans), które wykradają dane uwierzytelniające i informacje finansowe z naruszonych systemów, a nawet oprogramowania ransomware.

Badacze Bitdefender zauważyli, że trzy złośliwe próbki dostępne do pobrania z trzech reklam są „uszkodzone" i nie mogą dokończyć swojego działania, aby uruchomić dodatkowe ładunki na urządzeniach użytkowników lub zainicjować jakichkolwiek procesów eksfiltracji danych.

Biorąc pod uwagę te niepowodzenia, nie jest niczym niezwykłym, że osoby stojące za tą kampanią zaczynają modyfikować swoje złośliwe oprogramowanie i zarabiać na potencjalnych ofiarach.

Wskazówki i zalecenia dotyczące bezpieczeństwa

Gracze, uważajcie na linki GTA VI Beta Version do pobrania z reklam sponsorowanych na Facebooku

Ionut Baltariu z Bitdefender, który sam jest zapalonym graczem, apeluje do użytkowników o zachowanie ostrożności i unikanie postów, reklam i wiadomości promujących wcześniejszy dostęp do oczekiwanej części gry GTA.

Jak zadbać o swoje bezpieczeństwo?

Nigdy nie pobieraj plików wykonywalnych ani plików gier, zwłaszcza ekscytujących nadchodzących wydań, z reklam lub postów w mediach społecznościowych. Oszuści i cyberprzestępcy będą również wykorzystywać wiadomości i gorące tematy, aby oszukiwać użytkowników Internetu lub przeprowadzać ataki malware.

Zachowaj ostrożność w przypadku plików dostępnych do pobrania za pośrednictwem Dropbox, Discord, Trello, Google Drive i Microsoft OneDrive.

Sprawdź fakty przed zaangażowaniem się w jakiekolwiek reklamy lub wiadomości, które widzisz na platformach mediów społecznościowych. Dokładnie sprawdź informacje tylko na stronie internetowej twórcy gry.

Bądź na bieżąco z najnowszymi oszustwami i powiedz znajomym ze społeczności graczy, aby również dbali o swoje bezpieczeństwo

„Zadbaj o cyberbezpieczeństwo, korzystając z rozwiązania antywirusowego chroniącego przed niebezpieczeństwami w sieci, w tym trojanami bankowymi, złodziejami danych uwierzytelniających, oprogramowaniem wymuszającym okup, exploitami i innymi groźnymi

zagrożeniami elektronicznymi, w tym złośliwym oprogramowaniem FakeBat loader” – mówi Arkadiusz Kraszewski z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło:https://bitdefender.pl/gracze-uwazajcie-na-linki-gta-vi-beta-version-do-pobrania-z-reklam-sponsorowanych-na-facebooku/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 22.07.2024
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.