**Fałszywe mody do Minecrafta kradną dane. Ponad 1500 graczy ofiarą ataku hakerskiego!**

**Minecraft, kultowa gra z ponad 300 milionami sprzedanych kopii i 200 milionami aktywnych graczy miesięcznie, właśnie stała się celem wyrafinowanej kampanii cyberataków. Eksperci z Check Point Research ujawnili, że złośliwe modyfikacje do gry, udostępniane na GitHubie, infekowały komputery niczego niepodejrzewających użytkowników – głównie nastolatków. Atak, który dotknął co najmniej 1500 graczy przypisywany jest rosyjskojęzycznemu cyberprzestępcy.**

Złośliwe mody podszywały się pod popularne narzędzia używane przez graczy, takie jak Oringo czy Taunahi, znane jako "cheaty". Po ich zainstalowaniu uruchamiany był downloader w Javie, który pobierał kolejne elementy złośliwego oprogramowania. Drugi etap kradł loginy, hasła i dane z przeglądarek, a trzeci – zaawansowany spyware – wyciągał informacje z aplikacji takich jak Steam, Discord czy Telegram, a nawet przechwytywał zrzuty ekranu. Dane były następnie przesyłane przez... Discorda, co pozwalało na ukrywanie ataku w normalnym ruchu sieciowym.

Choć tożsamość autora kampanii nadal pozostaje nieznana, ślady pozostawione w kodzie oraz analiza aktywności wskazują na rosyjskojęzycznego cyberprzestępcę. Złośliwe pliki zawierały komentarze pisane po rosyjsku, a momenty publikacji i aktywności powiązane są ze strefą czasową UTC+3 (obejmującą m.in. Moskwę). Eksperci Check Point Research sugerują, że za atakiem może stać osoba lub grupa działająca w ramach podziemnego modelu „malware-as-a-service” (MaaS), wykorzystująca GitHub jako narzędzie do masowej dystrybucji złośliwego kodu.

**Dlaczego Minecraft?**

Około 65% społeczności graczy Minecrafta to osoby poniżej 21. roku życia – młode, aktywne i często nieświadome zagrożeń. Dzięki ogromnej popularności modów i otwartości na eksperymentowanie z nieoficjalnymi dodatkami, środowisko Minecrafta staje się łatwym celem.

Według wstępnej analizy infrastruktury atakujących, zainfekowanych mogło zostać ponad 1500 komputerów. Specjaliści Check Pointa uważają jednak, że skala może okazać się znacznie większa. Repozytoria GitHub, przez które rozpowszechniano złośliwe pliki, były dostępne publicznie i trudne do odróżnienia od legalnych modów.

**To nie pierwszy raz, gdy komputerowe od lat są łakomym kąskiem dla cyberprzestępców.** W 2021 roku popularność zdobyła kampania wykorzystująca malware RedLine Stealer, który ukrywał się w fałszywych crackach do gier udostępnianych przez YouTube i Discord, infekując tysiące urządzeń na całym świecie. W 2022 roku głośno było o przypadku złośliwego launchera „Among Us” rozpowszechnianego wśród graczy na Twitchu i Reddit, który podszywał się pod aktualizacje gry, a w rzeczywistości instalował spyware kradnący dane z przeglądarek i portfeli kryptowalutowych. Z kolei w zeszłym roku gracze platformy Steam stali się ofiarami kampanii phishingowej „SteamDrop”, która wykorzystywała wiadomości od znajomych oferujące rzadkie skiny do CS:GO. Kliknięcie w fałszywy link kończyło się utratą konta i dóbr cyfrowych.

**Jak się chronić?**

l Pobieraj mody tylko z oficjalnych i sprawdzonych źródeł.

l Unikaj „cheatów” i narzędzi automatyzujących grę – to ulubione przynęty hakerów.

l Używaj aktualnego oprogramowania antywirusowego i włączonego firewalla.

l Zainstaluj rozwiązania typu Threat Emulation, które analizują zachowanie aplikacji jeszcze przed uruchomieniem.

Z pozoru niewinna gra może stać się furtką do utraty prywatności, oszczędności, a nawet tożsamości cyfrowej.

Źródło: Check Point Research, czerwiec 2025.

Szczegóły techniczne: [pełny raport CPR](https://research.checkpoint.com/2025/minecraft-mod-malware-stargazers/)