Bitdefender

Gracze na celowniku hakerów – oszustwa na Steam i Discord

14.11.2023

Hakerzy i przestępcy nigdy nie lekceważą wartości aktywów graczy, nawet jeśli sami gracze często nie zastanawiają się, jak ważne są ich konta i dane personalne. Właśnie dlatego platformy do gier, takie jak Steam, lub usługi przesyłania wiadomości, np. Discord, są wykorzystywane przez cyberprzestępców do bezpośredniego atakowania niczego niepodejrzewających graczy.

Oszustwa na Steam i Discord

To, co czyni graczy wyjątkowym celem, to splot okoliczności, których nie można spotkać nigdzie indziej. Po pierwsze, wielu graczy jest zawsze online, w takiej czy innej formie. Nawet jeśli nie grają w gry wieloosobowe, platformy do gier, z których korzystają, umożliwiają im kontakt z innymi ludźmi za pomocą aplikacji na urządzenia mobilne, co oznacza, że wielu graczy jest online praktycznie 24 godziny na dobę, 7

dni w tygodniu.

Drugi problem polega na tym, że konta do gier mogą być niedoceniane przez użytkowników, co oznacza również, że użytkownicy nie będą odpowiednio dbać o ich bezpieczeństwo. Nie zapominajmy o tym, że średnia wartość konta na Steam aktywnego użytkownika wynosi 1900 dolarów. Jest to suma, na którą chętnie skusi się cyberprzestępca.

Cele hakerów działających na Steam

Przejęcie konta Steam to jeden z najczęstszych rodzajów ataków na użytkowników tej platformy i biorąc pod uwagę średnią wartość konta Steam, nietrudno zrozumieć dlaczego. Użytkownik może utracić dostęp do konta na wiele sposobów, ale wyróżniają się dwa.

W niektórych przypadkach przestępcy skontaktują się z potencjalną ofiarą, podając się za pracownika Steam i informując ją o problemie. Mogą powiedzieć, że ktoś zgłosił Twoje konto lub że wkrótce zostaniesz zbanowany. Dyskusja będzie zmierzać w jednym kierunku, ponieważ użytkownik musi podać dane uwierzytelniające, a nawet kod uwierzytelniania wieloskładnikowego, jeśli jest skonfigurowane.

Gdy napastnicy znajdą się na koncie, zmienią dane uwierzytelniające i zatrzymają konto dla okupu. W zależności od wagi włamania lub wartości konta mogą zrezygnować z okupu i po prostu spróbować sprzedać go gdzie indziej.

Inną powszechną metodą są linki phishingowe z dowolnej platformy, w

tym samej Steam, Discord, SMS-ów, mediów społecznościowych, poczty e-mail i tak dalej. Korzystanie z uwierzytelniania wieloskładnikowego nie jest wymuszane na platformie Steam, co oznacza, że nie każdy będzie miał je włączone. O wiele łatwiej jest przejąć konto Steam, które nie jest chronione przez MFA

„Niestety, na tym nie kończą się kłopoty użytkowników Steama. Oszustwa handlowe są również dość powszechne, zwłaszcza że rynek Steam zajmuje się przedmiotami cyfrowymi, które są wymieniane z innymi użytkownikami za prawdziwą walutę. Gracze często otrzymują oferty dotyczące przedmiotów cyfrowych w celu wymiany na realne pieniądze. Rzecz w tym, że Steam nie obsługuje wypłat kredytów w Portfelu, PayPal, kart podarunkowych ani żadnej formy oferty wymiany gotówkowej" – mówi Arkadiusz Kraszewski z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Oszuści często oferują przedmioty niskiej jakości w zamian za dane osobowe, proponują klucze do gier na płycie CD, lub chcą korzystać z innych platform zakupowych. W niektórych sytuacjach oszuści mogą nawet chcieć wymienić zakupione przedmioty za pomocą fałszywych kart kredytowych.

Handel na Steamie jest znacznie bardziej niebezpieczny, niż mogłoby się wydawać. Użytkownicy muszą zwracać uwagę, gdy inwestorzy próbują przekształcić transakcję w sytuację awaryjną, i upewnić się, że poświęcą odpowiednio dużo czasu, aby dokładnie sprawdzić daną ofertę.

Wreszcie jedno z bardziej niebezpiecznych oszustw dotyczy kart

podarunkowych portfela Steam i jest znacznie bardziej złożone niż jakiekolwiek poprzednie wymienione w tym artykule. W tym wypadku przestępcy kontaktują się z użytkownikami Steama telefonicznie i nakłaniają ich do zakupu kart podarunkowych portfela Steam w celu pokrycia podatków, kaucji, długów lub dostarczenia pieniędzy wygranych w loteriach. Oszuści często podają się za agentów różnych agencji, w tym IRS.

Discord nie pozostaje daleko w tyle

Discord to jedna z ulubionych platform graczy, ponieważ umożliwia gromadzenie się miłośników danych tytułów na dedykowanych serwerach. Używanie go jako platformy do przesyłania wiadomości umożliwia wykonywanie połączeń audio i udostępnianie plików. Niestety, oszuści i hakerzy mogą również korzystać z tych samych funkcji, które czynią tę platformę świetną do przeprowadzania ataków phishingowych.

Podobnie jak w przypadku Steam, z użytkownikami mogą kontaktować się osoby podające się za administratorów Discorda wyłącznie, aby wyłudzić dane uwierzytelniające lub inne istotne informacje.

Niektórzy oszuści niespodziewanie kontaktują się z użytkownikami, a nawet podszywają się pod Twoich znajomych, próbując przekonać ich do pobrania niebezpiecznego pliku, który zawiera złośliwe oprogramowanie. Hakerzy mogą na przykład podawać się za niezależne studio deweloperskie i potrzebować pomocy przy testowaniu gry.

Cyberprzestępcy często także przejmują konta na Discordzie.

Bitdefender zaobserwował, że hakerzy próbują nakłonić ofiary do zaoferowania im tokenów sesji z Konsoli programisty, które następnie zostają wykorzystane do kradzieży konta.

Użytkownicy Discorda muszą także uważać na wszelkie wiadomości twierdzące, że są beneficjentami bezpłatnego dostępu do Nitro. Zazwyczaj Nitro to funkcja Discord, która zapewnia dostęp do specjalnych korzyści w zamian za uiszczenie odpowiedniej zapłaty. Aby wykorzystać rzekome środki Nitro, użytkownicy muszą zeskanować kod QR, który prawdopodobnie będzie prowadził do niebezpiecznego łącza lub pliku.

Gracze na celowniku hakerów – jak się bronić przed oszustwami na Steam?

Gaming to o wiele bardziej niebezpieczna przestrzeń, niż mogłoby się wydawać na pierwszy rzut oka. Różnorodność oszustw i rodzajów cyberataków dowodzi, że przestrzeń gier jest atrakcyjna dla przestępców i że ich ataki są skuteczne. Dlatego zachowanie cyberbezpieczeństwa na Steam i Discordzie powinno być priorytetem dla każdego gracza. Zespół Bitdefender przygotował kilka prostych zasad, dzięki którym będziesz mógł poprawić jakość swojej cyberochrony.

- Zawsze, gdy to możliwe, włączaj uwierzytelnianie wieloskładnikowe.
- Nigdy nie udostępniaj swoich danych uwierzytelniających ani tokenów sesji innym użytkownikom, niezależnie od tego, za kogo się podają.

- Uważaj na każdą wiadomość, która rzekomo jest pilna i wymaga Twojej natychmiastowej odpowiedzi.
- Uważaj na nieznanych użytkowników, którzy wysyłają Ci linki lub pliki.
- Poświęć trochę czasu na przejrzenie transakcji Steam.
- Korzystaj z rozwiązań antywirusowych na wszystkich swoich urządzeniach, także mobilnych. Wiele z tych oszustw zostanie natychmiast zatrzymanych przez rozwiązanie bezpieczeństwa.

Źródło: https://bitdefender.pl/gracze-na-celowniku-hakerow-oszustwa-na-steam-i-discord/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 14.11.2023
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.