**Igrzyska Gier Wideo w niebezpieczeństwie? Esport na celowniku hakerów!**

**Wraz z szybkim wzrostem popularności esportu, cyberzagrożenia zaczynają przybierać na sile, stawiając pod znakiem zapytania przyszłość tej dynamicznie rozwijającej się branży. Czy igrzyska olimpijskie gier wideo, które zyskały aprobatę Międzynarodowego Komitetu Olimpijskiego i mają oficjalnie zadebiutować w 2025 roku, są zagrożone przez cyberprzestępców?**

E-sport, który przyciąga miliony fanów z całego świata i generuje miliardowe przychody, stał się atrakcyjnym celem dla cyberprzestępców. Ataki cybernetyczne mogą mieć katastrofalne skutki dla przebiegu turniejów, reputacji organizatorów, a nawet dla postrzegania esportu jako poważnej dyscypliny sportowej – piszą analitycy Check Point Software Technologies w swoim najnowszym raporcie. Kiedy w grę wchodzą tak ogromne pieniądze, cyberprzestępcy z pewnością nie będą próżnować.

Ostatnie lata były świadkami wielu spektakularnych ataków na firmy z branży gier wideo. Capcom, twórca takich hitów jak Street Fighter czy Resident Evil, padł ofiarą groźnych ataków ransomware. Polski CD PROJEKT RED, twórca Wiedźmina i Cyberpunka 2077, również poniósł ogromne straty w wyniku cyberataków. Nawet wyczekiwany przez fanów hit GTA VI nie uchronił się przed atakiem, za którym stał zaledwie 17-letni haker, który wcześniej na swoim koncie miał włamania do systemów Ubera!

Z szacunków ekspertów Check Pointa wynika, że koszty związane z tymi atakami są ogromne – sięgają milionów dolarów w formie okupów, a także niosą ze sobą trudne do naprawienia szkody wizerunkowe.

**Czy esportowe igrzyska są w niebezpieczeństwie?**

Popularność esportu wzrosła do tego stopnia, że Międzynarodowy Komitet Olimpijski postanowił włączyć go do swoich igrzysk. Jednak sukces tej inicjatywy może być zagrożony przez rosnącą liczbę cyberataków. Czy widmo cyberprzestępczości zagraża debiutowi e-sportu na olimpiadzie?

W miarę jak e-sport zyskuje coraz większe uznanie, staje się również celem dla ataków DDoS, kradzieży kont graczy oraz oszustw w turniejach. Przykładem może być [tegoroczny atak na zespół T1](https://consent.yahoo.com/v2/collectConsent?sessionId=3_cc-session_0c6de0e9-cc49-4e8f-bb28-987e0484aae1) oraz turniej League of Legends Korea (LCK), który musiał zostać zawieszony, a mecze przeniesione do zamkniętych pomieszczeń. Skutki takich działań są ogromne – sponsorzy i widzowie oczekują płynnego przebiegu wydarzeń, a wszelkie zakłócenia mogą prowadzić do ogromnych strat finansowych i reputacyjnych.

Hakerzy nie zawsze działają w pojedynkę. Często wykorzystują dostępne na darknecie narzędzia, takie jak botnety, które można wynająć za zaledwie kilkaset dolarów. Ataki mogą być również wynikiem rywalizacji między zespołami esportowymi, próbującymi zdyskredytować swoich konkurentów, zdobyć przewagę lub wyeliminować ich z rywalizacji. W jednym z turniejów popularnej gry [Apex Legends haker "Destroyer2009" zhakował dwóch streamerów](https://protect.checkpoint.com/v2/___https:/ca.movies.yahoo.com/movies/apex-legends-hacker-says-game-130021810.html___.YzJlOmNwYWxsOmM6bzoyN2VmYjA0NDk5ZWY1NDQ1NjkxMzVmNDM5OWVjMjhlNzo2OmY4ODU6NGQ3NTI0ZjE1ZTkxNzMyOTAyOGIwMTRjYWM3ZTAzM2U0YjViOWY4NGJjNWUyM2Y5OTQyYzViNmJjYzI5ZTQ5YzpwOlQ6Tg), oskarżając ich o oszukiwanie, co spowodowało zamieszanie i chaos w trakcie rywalizacji.

Jednak to nie wszystko, eksperci Check Point Research podkreślają, że hakerzy atakują również konta profesjonalnych graczy, aby uzyskać dostęp do poufnych informacji. Atakujący często naśladują oficjalne wiadomości i strony internetowe znanych organizacji, prawdopodobnie oferując różne nagrody i wiadomości. Jednak niektóre oszustwa phishingowe bywają znacznie bardziej wyrafinowane. Przykładowo cyberprzestępcy byli w stanie włamać się bezpośrednio do działu wsparcia amerykańskiego wydawcy gier 2K, dzięki czemu fałszywe e-maile zostały wysłane oficjalnymi kanałami. Nawet czescy gracze wiedzą o ryzyku utraty swoich kont i przedmiotów w grze. Martin „zur1s” Sláma na przykład stracił swoje konto w grze podczas turnieju CS:GO na żywo. Nie tylko nie mógł kontynuować turnieju, ale również skradziono mu przedmioty w grze o wartości 300 tys. koron czeskich. Cyberataki są zatem wymierzone nie tylko w same turnieje, ale także w poszczególnych graczy.

**Przyszłość esportu w rękach cyberochrony**

Zbliżające się olimpijskie wydarzenie e-sportowe z pewnością przyciągnie uwagę nie tylko milionów fanów, ale także cyberprzestępców. Jeśli branża nie zainwestuje w odpowiednie środki ochrony, debiut igrzysk esportowych może zostać zagrożony. Jedno jest pewne – cyberbezpieczeństwo stanie się kluczowym czynnikiem determinującym przyszłość tej nowoczesnej dyscypliny.