Cyberdefence 24

**aut. Andrzej Kozłowski** 15.02.2021

# KTO KUPIŁ KODY ŹRÓDŁOWE WIEDŹMINA? KRAJOBRAZ PO ATAKU NA CD PROJEKT

Wykradzione w zeszłym tygodniu dane z CD Projektu miały zostać sprzedane za 7 milionów dolarów. Czy jednak na pewno? Pojawią się wątpliwości odnośnie tego czy aukcja się w ogóle odbyła. W międzyczasie pracownicy wymieniają dowody osobiste obawiając się skutków ataku.

Mija tydzień od ataku na CD Projekt. Producent takich hitów jak seria Wiedźmin  i Cyberpunk 2077 padł ofiarą ukierunkowanego cyberataku w wyniku którego hakerom udało się dostać do niektórych wewnętrznych systemów firmy. Atak został prawdopodobnie przeprowadzony przez grupę Hello Kitty, na co wskazuje zastosowane oprogramowanie ransomware oraz technika ataku. Hakerzy wcześniej stali za atakami na brytyjską służbę zdrowia w styczniu 2021 roku oraz byli odpowiedzialni za co najmniej dwa ataki w trakcie świąt Bożego Narodzenia. Jedną z ich ofiar był wtedy brazylijski dystrybutor energii elektrycznej, któremu przywrócenie pełnej sprawności działania systemów zajęło 4 dni. Część ekspertów wskazuje, że wcześniej Hello Kitty działał wcześniej pod nazwą DeathRansom widząc podobieństwa w używanym oprogramowaniu ransomware.

Hakerom udało się ukraść z firmy kody źródłowe gier Gwint, Wiedźmin 3 i Cyberpunk 2077. Początkowo hakerzy ujawnili w Internecie dane Gwinta, co jest standardową procedurą pokazującą po pierwsze, że hakerzy "nie żartują" i jest to ostatni sygnał dla firm, aby zaangażowała się w negocjacje. Po drugie służy uwiarygodnieniu posiadanych informacji, tak aby potencjalny nabywca wiedział co kupuje. Reszta kodów źródłowych została wystawiona na aukcji w darknecie z ceną początkową miliona dolarów. Aukcja została zakończona po tym, jak sprzedający otrzymali  otrzymali ofertę na sumę 7 milionów dolarów spoza forum. Sprzedaż miała być jednak ograniczona warunkiem braku jakiekolwiek dalszej dystrybucji czy dalszej sprzedaży plików. Ponadto wszystkie kody źródłowe miały zostać sprzedać w ramach jednego pakietu. Biorąc pod uwagę, że takie transakcje są najczęściej anonimowe, nie wiemy kto dokonał wpłaty i bardzo mało prawdopodobne, że kiedykolwiek się tego dowiemy.

Szybko pojawiły się spekulacje, że to sam CD Projekt chce w ten sposób odzyskać swoje pliki, inni wskazywali na konkurencję. Prawda jest taka, że same kody źródłowe trudno jest wykorzystać w praktyczny sposób. Konkurencja nie może po prostu ich użyć do produkcji własnych gier, ponieważ ryzykuje gigantycznymi karami oraz ostracyzmem w branży. Teoretycznie w przypadku Gwinta i Cyberpunka 2077 kody źródłowe mogłby zostać wykorzystywane do atakowania graczy w trybie gry wieloosobowej. Tylko, że w przypadku Cyberpunka 2077, tryb ten dopiero powstaje i z pewnością po wycieku danych zostanie sprawdzonych wielokrotnie tak aby nie powtórzyły się wpadki, które oglądaliśmy podczas premiery gry.  Autentyczność wylicytowanych danych miała potwierdzić izraelska firma KELA zajmująca się cyberbezpieczeństwem i monitorowaniem transakcji w darknecie.

Pojawiły się jednak informacje pochodzące od badaczy ds. cyberbezpieczeństwa, a dokładnie od Bretta Callowa z firmy Emsisoft, że do żadnej aukcji nie doszło. Jego zdaniem hakerzy jedynie udają, że udało im się sprzedać dane skradzione z serwerów polskiej firmy. Jego podejrzliwość wzbudza

zawrotna ceną za którą sprzedano kody źródłowe, podczas gdy średni koszt plików firmy wacha się od 20 tys. do 40 tys. Kod źródłowy gier, który raczej trudno jest wykorzystać w praktyczny sposób nie jest warty takiej zawrotne sumy – twierdzi analityk. Jego zdaniem cała sprawa z aukcją może być jedynie przykrywką niepowodzenia hakerów. Polska spółka odmówiła zapłacenia oczekiwanego przez przestępców okupu.  Która z tych wersji jest prawdziwa? Dowiemy się w najbliższym czasie.

Nie wiadomo również czy w ramach aukcji oferowano również inne pliki poza kodami źródłowymi. Hakerzy chwalili się przejęciem dokumentów firmy z działu finansowego, prawnego, zasobów ludzkich oraz informacji na temat planowanych inwestycji. W ich opinii dokumenty te miały doprowadzić firmę do ruiny. Na razie nie wiadomo jaki jest los tych danych.

CD Projekt początkowo zaprzeczył w oświadczeniu, że jakiekolwiek dane osobowe pracowników lub graczy są zagrożone, zalecał jednak ostrożność. Internet jednak huczy od plotek, że część osób zatrudnionych u giganta polskiego gamingu prewencyjnie wymienia dowody osobiste i weryfikuje się w Biurze Informacji Kredytowej. Do jednego z pracowników miał już zresztą dzwonić bank z informacją, że ktoś próbował na jego dane wziąć kredyt. CD Projekt poinformował o włamaniu Prezesa Urzędu Ochrony Danych Osobowych, a sprawą ataku zajmuje się Prokuratura Rejonowa Warszawa-Praga Północ. Jednocześnie biorąc pod uwagę obroty spółki, potencjalna kara od PUODO byłaby dość duża. Mało prawdopodobne wydaje się również złapanie sprawców - czego z pewnością świadomi są twórcy CD-Projektu.

Wciąż nie wiadomo w jaki sposób udało się hakerom przeniknąć do systemów firmy. Biorąc jednak pod uwagę pracę zdalną większości zespołu, ciągły pośpiech i praktycznie 100% skupienie się na poprawianiu Cyberpunka 2077 łatwo sobie wyobrazić, że zmęczenie pracowników mogło mieć tutaj kluczowe znaczenie w kontekście zachowania cyberbezpieczeństwa.

**Wzorcowa komunikacja**

Żadna firma nie może być chwalona, za to że jej zabezpieczenia zostały przełamane, szczególnie jak jest to kolejny raz z rzędu. Wcześniej CD Projekt padł ofiarą ataków w 2017 roku i można byłoby powiedzieć, że nie nauczono się na błędach. Biorąc jednak pod uwagę, że cyberataki uderzają praktycznie we wszystkich - poczynając od gigantów internetowych jak Facebook po instytucje rządowe - warto zdawać sobie sprawę, że coraz trudniej jest ich po prostu uniknąć. Dlatego tak ważna jest sprawna komunikacja po incydencie. W tym wypadku CD Projekt warto pochwalić. W przeciwieństwie do części firm, które ukrywają informacje o incydencie i potajemnie negocjują z hakerami wybrali oni pełną przejrzystość i transparentność, jednoznacznie odmawiając jakichkolwiek negocjacji z cyberprzestępcami. Opublikowali też notkę od hakerów, co dodatkowo było punktowane przez ekspertów z branży. Właściwa reakcja na incydent pozwoliła również na uniknięcie dużych strat na giełdzie. Cena akcji od momentu publikacji informacji o incydencie we wtorek 9 lutego do dzisiaj zmniejszyła się o 20 złotych.

Po tygodniu od incydentu, wciąż jest w sprawie więcej domysłów niż potwierdzonych informacji. Z pewnością była to kolejna rysa na wizerunku firmy. Po ciągle trwających problemach z premierą Cyberpunka 2077 teraz doszła jeszcze kwestia ataku hakerskiego. Jego negatywne skutki udało się jednak zminimalizować poprzez właściwą komunikację po incydencie bezpieczeństwa.