Od jakiegoś czasu gram w Watch Dogs. Nie jest to nic szczególnego. Gra ta miała już swoje pięć minut kilka lat temu, a mimo to postanowiłem do niej wrócić, a nawet natchnęła mnie do pewnych przemyśleń.

Watch Dogs to surrealistyczna wizja świata, w której wcielamy się w żądnego zemsty hakera chcącego pomścić swoją siostrzenicę. Czemu pomścić? Bo została zabita w zamachu na życie głównego bohatera – Aidena. Czemu próbowano go zabić? Tutaj oszczędzę spojlerowania osobom, które jeszcze nie grały, a być może kiedyś zamierzają. Pozostałych zapraszam do obejrzenia tego jak gram w tą grę w charakterystyczny dla siebie sposób komentując.

Czy polecam ją jako grę do wartkiej i emocjonującej rozgrywki? Jest to średniej jakości kopia GTA ze średniej jakości mechaniką sterowania pojazdów (identyczną jak w GTA) oraz dobrą fabułą, co zdecydowanie czyni ją dobrym przerywnikiem pomiędzy kolejnymi strzelankami nie mającymi większej głębi poza zastrzeleniem przeciwnika i szukaniem kolejnego.

Jednakże wracając do tego dlaczego nawiązuję właśnie do tej gry i czemu piszę, iż Watch

Dogs to surrealistyczna wizja świata. W wizji tej pojawia się ctOS czyli Centralny System Operacyjny (Central Operating System), który kontroluje niemal każdy element technologii w mieście oraz zawiera informacje o wszystkich mieszkańcach metropolii, które można wykorzystać do różnych celów. W jednym ze zwiastunów twórcy gry całkiem dokładnie opowiedzieli czym jest ctOS, do czego służy i jakie dane przetwarza.

Obecnie w naszym kraju wdrażane są tzw. „mDokumenty„. Projekt ten jest realizowany przez Ministerstwo Cyfryzacji. Prócz tego projektu istnieje też inny taki jak „ProfilZaufany”. Jest to krok w stronę skomputeryzowania kolejnego etapu naszego życia jakim jest komunikacja z urzędami czy też identyfikacja własnej tożsamości. Być może dążymy do stworzenia własnego realnego ctOS'u, który będzie zarządzał naszym życiem. Na szczęście nie jest to aż tak bliskie jak niektórzy by mogli się spodziewać.

Jak pisałem wcześniej gra skłoniła mnie do pewnych releksji. Główna fala tych przemyśleń dopadła mnie jakiś czas temu, gdy wracałem metrem do domu. Stojąc na uboczu wagonu w pewnym momencie z przerażeniem zauważyłem fakt, iż praktycznie nie ma osoby która nie byłaby bezmyślnie wpatrzona w swój smartfon tak jakby był on całym światem. Niektórzy przeglądali Facebooka – co wydaje się całkiem normalne, inni szukali informacji na studia – i to nie dziwi, inni zaś oglądali firmy przyrodnicze na serwisie o nazwie zaczynającej się na „porn”, a kończącej się na „hub.com” – no dobrze, nie inni. Taki delikwent był tylko jeden. Sam byłem nie lepszy prowadząc zawiłą i skomplikowaną komunikację poprzez Facebooka na temat ósmej już edycji Security BSides Warsaw, która odbędzie się w 2018 roku w Warszawie.

Skąd o tym wiem? Czyżbym dokonał jakiegoś wybitnego shakowania smartfonów w metrze? Nie. W dzisiejszych czasach smartfony mają tak dobre ekrany, że spokojnie można czytać z nich z kilku metrów oraz pod każdym kątem. Kilka dni temu po zakupie telefonu odkryłem w domu to, iż jestem w stanie odczytać to co jest na ekranie leżąc ponad metr od telefonu i patrząc na niego pod kątem około dwudziestu stopni. Oznacza to, że osoba siedząca obok czy stojąca nade mną w metrze, w autobusie czy w innym miejscu publicznym także doskonale widzi wyświetlacz mojego telefonu. Czytając recenzje mojego telefonu znajduje między innymi takie opinie „Kąty widzenia są w XA1 bez zarzutu – można patrzeć

na wyświetlacz z każdej strony.” i zdecydowanie potwierdzam. Niestety to co wydaje się dla wielu zaletą jest też zaletą dla osób chcących poznać naszą tożsamość lub po prostu osób wścibskich zaglądających nam w telefon na przykład w metrze czy autobusie. W większości przypadków po krótkiej obserwacji konkretnej osoby udaje sie ustalić podstawowe dane takie jak na przykład tożsamość. A wszystko to poprzez profil na Facebooku/Twiterze/innym portalu, zainteresowania czy też aktualne problemy, które możemy wyczytać z rozmów na ekranie. Podobnie jest z rozmów telefonicznych, które ludzie często prowadzą tak ochoczo podczas przebywania w miejscach publicznych czy też swobodnego przemieszczania się po mieście. Moimi ulubionymi są długie rozmowy prowadzone w autobusie w taki sposób, iż dokładnie słychać nie tylko rozmówcę, który stoi obok nas, ale również i osobę po drugiej stronie. Niestety wiele telefonów domyślnie jest bardzo głośnych jeśli chodzi o rozmowy telefoniczne. Tutaj alternatywą zdecydowanie są słuchawki.

Co to oznacza dla obserwującego? Oznacza to przede wszystkim pełen pakiet informacji mogących służyć do przygotowania potencjalnego ataku. Oczywiście, można tutaj przytoczyć argument, że kto by chciał mnie atakować. Każdy z nas ma konto bankowe, a większość posiadaczy kont bankowych ma zainstalowane aplikacje na swoich telefonach. Przez nasze komputery i urządzenia mobilne przepływają miliardy bajtów miesięcznie, co bardziej aktywny użytkownicy są w stanie skonsumować około 80 GB miesięcznie transferu (dane pochodzą z mojego domowego firewalla, w czasach gdy moi współlokatorzy byli bardziej aktywni internetowo). Te dane w każdej chwili mogą stać się obiektem ataku. Czasem jest tak, że celem ataku nie stają się nasze pieniądze jak pisałem wcześniej czy też nasze tajemnice a my sami. Kradzież tożsamości jest najbardziej dotkliwą rzeczą jaka może spotkać człowieka w dzisiejszych czasach. Skończyć może się to kredytem czy innymi przykrymi konsekwencjami związanymi z tym, że ktoś się za nas poda. A wszystko to przez nas smartfon.

O ile wizja zaprezentowana w Watch Dogs pokazuje, iż całość hakowania miałaby się odbywać w sposób na pozór bardzo magiczny to w realnym świecie byłoby to bardziej związane z zagadnieniami socjotechnicznymi czy też po prostu z wykonaniem sprawnego i prawidłowego reserchu na temat osoby, którą obieramy sobie na cel.

Jak? To proste. Załóżmy teoretycznie, że nasza bohaterka „Kasia” właśnie jedzie metrem, a ja stoję obok niej. Z racji tego, że „Kasia” siedzi widzę doskonale jej telefon. Być może gdyby miała filtr prywatyzujący nie widziałbym teraz ekranu jej nowego iPhonaX oraz zdjęć,

które właśnie wysyła swojemu chłopakowi „Tomkowi”. Znając ludzką naturę myślę, iż nie chciała bym widział te zdjęcia oraz wiedział, że są one podziękowaniem za kupiony wczoraj telefon. Po wysłaniu zdjęć bohaterka naszej historii blokuje swój telefon i chowa do kieszeni. Dobra praktyka. Nawet jak go zgubi będzie miała pewność, iż telefon jest zablokowany, a znalazca nie dostanie się do niego, czy też nie daj Boże zobaczy zdjęcia, ale co z tego skoro ja już i tak je widziałem. Kilkanaście sekund po tym jak schowała telefon przychodzi powiadomienie. Szybko sięga do kieszeni i odblokowuje telefon. Ma ustawiona blokadę, nie wystarczy tylko swipnać w górę. Okazuję się, że nie użyła również wzoru do odblokowania telefonu. Być może słyszała, że na ekranie smartfona zostaje ślad po palcu i jesli cześciej odblokowujemy telefon niż go przecieramy można odczytać wzór odblokowania. „Kasia” użyła blokady na hasło. Dokładnie użyła kombinacji liter, cyfr i znaków. Wow, można powiedzieć bardzo świadomy użytkownik z tej naszej „Kasi”. Problem pojawia się w logice z jaką „Kasia” tworzyła hasło. Jako, że nasza bohaterka jest bardzo rezolutną osobą, konwersuje nie tylko z „Tomkiem” oraz korzysta z takich portali jak Tinder czy Badoo. Ponieważ uważa iż „Tomek” mógłby się obrazić o to, postanowiła użyć hasła, którego nigdy nie zgadnie, nawet jak mu powie jakie jest. Użyła swojej daty urodzin oraz imienia w formacie: Imię+DD-MM-YYYY. Czyż nie genialnie? „Tomek” i tak zawsze zapomina o jej urodzinach, musi mu przypominać więc daty na pewno nie odgadnie przy próbie zalogowania, a do tego jeszcze ten plus i myślniki… Nasza bohaterka po odblokowaniu odpisała swojej koleżance „Monice” oraz zaczęła przeglądać swój wall na Facebooku. Po kilku chwilach mam w pamięci imiona, nazwiska i avatary jej znajomych. To pomoże mi potem poprzez jej znajomych znalezienie jej samej. Wystarczy tylko przejrzeć znajomych pod kątem powtarzających się osób. Jako iż „Kasia” uznała, że jej hasło jest bardzo bezpieczne, bo tak twierdzi internetowa sprawdzarka haseł, którą pokazano jej w liceum na lekcjach informatyki postanowiła użyć go nie tylko do telefonu ale i do między innymi Facebooka oraz maila. Niestety „Kasia” nie pamiętała już tego, co mówiono na lekcjach informatyki zaraz po pokazaniu sprawdzarki haseł. Każde kolejne użycie hasła w innym miejscu powoduje, że hasło traci swoją siłę i staje się bezużyteczne. Potem, jest już tylko z górki. W ciągu dwudziestu czterech godzin sprzedaję tożsamość „Kasi” gdzieś na jednej z tych złych stron w owianym złą sławą „darknecie”.

Oczywiście jest to scenariusz stworzony specjalnie na potrzeby tej publikacji i nigdy nie miał miejsca, przynajmniej z moim udziałem, zarówno jako atakującego, ale też i jako ofiary. Niestety scenariusz choć fikcyjny jest bardzo możliwy. Wysoce prawdopodobnym jest, że gdzieś na świecie już się wydarzył i wydarzy się jeszcze nie raz. Być może ktoś w ten sposób straci pieniądze z konta?

Tak jak pisałem, sposobów by ochronić swoją prywatność jest kilka, między innymi filtry

zaciemniające ekran. Ochronią one nas nie tylko przed wścibskim okiem osób, z którymi dzielimy przestrzeń ale również uniemożliwią odczyt naszego ekranu. Kolejnym sposobem na ochronę, jest po prostu rozważne korzystanie z naszych urządzeń mobilnych w miejscach publicznych.