Cyberdefence 24

aut. Szymon Palczewski 05.03.2021

ARMIA USA OSTRZEGA PRZED OSZUSTWAMI Z UŻYCIEM KODÓW QR

Kody QR są coraz częściej wykorzystywane przez cyberprzestępców, co jest szczególnie widoczne w czasach pandemii, gdzie dystans społeczny, higiena oraz zdalne rozwiązania stają się kluczowe w walce z COVID-19. Oszuści za pomocą fikcyjnych kodów infekują urządzenia ofiar, przejmują nad nimi kontrolę lub pozbawiają oszczędności, przelewając środki na zewnętrzne rachunki.

Kody szybkiej odpowiedzi, znane powszechnie jako QR, zostały po raz pierwszy opracowane w połowie lat 90. XX wieku z myślą o produkcji i kontroli zapasów – przypomina U.S. Army Criminal Investigation Command. Nie należy ich mylić z uniwersalnym kodem produktu, czyli tzw. kodem kreskowym, znajdującym się na większości rzeczach oferowanych do sprzedaży.

W czasie pandemii koronawirusa kody QR są wykorzystywane coraz częściej ze względu na swój charakter, w tym możliwość bezdotykowej obsługi przy użyciu smartfona. Przykładem mogą być restauracje, w których kody zastępują tradycyjne, papierowe menu. Dzięki tego typu rozwiązaniu klient może zeskanować kod za pomocą swojego urządzenia, wybrać danie oraz za nie zapłacić dzięki bankowości elektronicznej. To wygodny i szybki sposób, zwłaszcza w czasie pandemii, gdzie kluczowa jest higiena i dystans społeczny.

Jednak jak większość rozwiązań, kody QR niosą ze sobą ryzyko, zwłaszcza gdy są wykorzystywane przez cyberprzestępców. W jaki sposób? U.S. Army Criminal Investigation Command wskazuje, że oszuści za pomocą fałszywych kodów mogą przejąć kontrolę nad urządzeniem ofiary i np.: modyfikować listę kontaktów, podłączyć do złośliwej sieci, rozsyłać zainfekowane wiadomości do osób z książki adresowej, wykonywać połączenia w celu naliczania dodatkowych opłat oraz dokonywać przelewu środków na określone konto dzięki mobilnej bankowości.

> *Oszustwa związane z kodami QR i kradzieże, choć nie są powszechne, stają się coraz popularniejsze i rozwijają się na wiele sposobów.*
>
> U.S. Army Criminal Investigation Command

Najczęściej do oszustw dochodzi poprzez drukowanie fałszywych kodów QR na etykietach i przyklejając je do różnych publicznie dostępnych powierzchni. Zaciekawiona ofiara skanuje go i jest najczęściej przekierowywana na złośliwe witryny. W ten niewymagający wysiłku sposób urządzenia są infekowane złośliwym oprogramowaniem.

Popularne jest również wykorzystywanie fałszywych kodów do wykonywania przelewów z urządzeń

użytkowników – wystarczy, że zeskanują kod i cała procedura transferu środków zostaje rozpoczęta. Przez nieuwagę ofiara może stracić wszystkie swoje oszczędności.

O oszustwach wykorzystujących kody QR ostrzegały w przeszłości m.in. holenderskie służby. Apelowano do obywateli o zachowanie szczególnej ostrożności podczas zakupów online, gdzie sprzedawca wysyłał kod po przekazaniu mu danych konta. „To nie jest normalna sytuacja, ponieważ Twoje imię i nazwisko oraz numer konta wystarczą, aby otrzymać płatność. W tym przypadku kod nie odnosi się w rzeczywistości do potwierdzenia płatności, ale do witryny logowania do bankowości. Oszuści, w połączeniu z przekazanym numerem konta bankowego, będą mogli uzyskać bezpośredni dostęp do rachunków bieżących i oszczędnościowych" – podkreślił komisarz Olivier Bogaert z Federalnej Jednostki ds. Przestępczości Komputerowej.

Ofiarami tego typu oszustw byli m.in. holenderscy klienci banku ING. Cyberprzestępcy za pomocą fikcyjnych kodów QR, których skanowanie aktywowało aplikację bankowości mobilnej przelewali na swoje rachunki środki z kont ofiar, pozbawiając je oszczędności.

Jak nie dać się cyberprzestępcom? Amerykańskie dowództwo radzi, aby przede wszystkim podchodzić z ostrożnością do znalezionych kodów QR i nie skanować ich bez chwili zastanowienia. „Czerwona lampka" powinna zapalić się nam za każdym razem, gdy po sczytaniu kodu zostaniemy poproszeni o podanie danych logowania do określonej usługi.

Co więcej, nie należy skanować kodów QR otrzymanych w wiadomościach e-mail, chyba że jesteśmy pewni, że pochodzą one z wiarygodnego źródła. Za każdym razem, gdy znajdujemy się w restauracji, sklepie lub innym obiekcie, gdzie znajdują się pracownicy, możemy zapytać o zweryfikowanie kodu udostępnionego dla klientów w celu upewnienia się, że wszystko jest w porządku i nie padniemy ofiarą oszustów. „Kto pyta, nie błądzi".

Czytaj też: Dostałeś SMS od FedEx? Uważaj na oszustów!