OUCH! Styczeń 2024

OUCH!

SANS SECURITY AWARENESS

Biuletyn Bezpieczeństwa Komputerowego

Kody QR

Wstęp

Zastanawiałeś się kiedyś, czym są kwadraty z kropkami i kreskami, które są nazywane „kodami QR” ? Najczęściej można je zauważyć na stronach internetowych, plakatach, są też używane jako bilety mobilne lub wykorzystywane podczas rezerwacji w restauracjach. Jak działają i czy istnieją zagrożenia związane z kodami QR, którymi należy się martwić? Spróbujmy się tego dowiedzieć.

Kod QR wskazujący stronę internetową SANS OUCH.

Jak działają kody QR?

Kod QR oznacza „Quick-Response code” i jest kodem składającym się z czarnych i białych kwadratów (mogą być również w innych kolorach i zawierać tło). Te kwadraty te można łatwo utworzyć za pomocą generatorów kodów QR i służą do szyfrowania informacji, takich jak adresy URL witryn, dane kontaktowe e-mail lub inne dane. Kody QR są jak kody kreskowe, tylko bardziej wszechstronne. Większość aparatów w telefonach rozpoznaje i dekoduje informacje zakodowane w kodzie QR. Innymi słowy, gdy spróbujesz zrobić zdjęcie kodu QR za pomocą aparatu w swoim urządzeniu, urządzenie rozszyfruje kod QR i zapyta, czy chcesz zastosować się do zawartych w nim informacji, np. otworzyć link do strony internetowej.

Jakie jest niebezpieczeństwo?

Kody QR mogą być trudne do zweryfikowania pod kątem bezpieczeństwa, co ułatwia cyberprzestępcom rozpowszechnianie szkodliwych i niebezpiecznych treści. Kod QR może skierować Cię do złośliwej witryny internetowej, która próbuje wyłudzić dane osobowe, takie jak dane logowania lub numery kart kredytowych, może nawet próbować zainstalować złośliwe oprogramowanie na urządzeniu. Ponadto kody QR mogą wykonywać dodatkowe czynności, takie jak dodanie kontaktu do listy lub utworzenie wiadomości e-mail w Twoim imieniu. Kod QR sam w sobie nie stanowi zagrożenia; jednakże może to być informacja lub działanie, które są wywoływane za ich pomocą, może być.

Załóżmy, że jesteś w mieście lub na lotnisku i na ścianie wisi plakat promujący produkt, który wydaje się być interesujący. Na plakacie znajduje się kod QR, za pomocą którego można szybko uzyskać więcej informacji. Możesz nie zauważyć, że na kodzie QR jest naklejka z innym kodem QR. Patrząc na plakat nie zdajemy sobie sprawy, że kod QR na plakacie został naklejony przez przestępcę. Po zeskanowaniu kodu QR, chcąc dowiedzieć się więcej o produkcie, zostaniesz przekierowany na stronę internetową kontrolowaną przez przestępców.

Co zrobić, żeby być bezpiecznym?

- Zachowaj ostrożność, zanim zeskanujesz kod QR. Najpierw zadaj sobie pytanie: Czy źródło jest godne zaufania? Czy plakat, restauracja lub strona internetowa nie wzbudza podejrzeń? Jeśli ktoś zostawił w samochodzie ulotkę z kodem QR, czy można uznać ją za bezpieczną?
- Po zeskanowaniu kodu QR urządzenie zapyta Cię, czy potwierdzasz działania, które próbuje wymusić kod. Na przykład, jeśli kod QR jest łączem do strony internetowej, urządzenie zapyta Cię, czy chcesz odwiedzić tę witrynę, zanim na nią przejdziesz. Warto poświęcić trochę czasu na zapoznanie się z do działania lub samym linkiem i upewnienie się, że odwiedzenie witryny nie stwarza niebezpieczeństwa.
- Upewnij się, że telefon komórkowy jest zawsze zaktualizowany i ma zainstalowaną najnowszą wersję systemu operacyjnego. Upewnij się, że telefon komórkowy jest zawsze zaktualizowany i ma zainstalowaną najnowszą wersję systemu operacyjnego. Najłatwiej to zrobić, włączając automatyczne aktualizacje na urządzeniu.
- Nie ma potrzeby instalowania specjalnych aplikacji mobilnych do dekodowania kodów QR, wystarczy, że będziesz mógł skorzystać z wbudowanego aparatu w swoim urządzeniu. Jeśli witryna wymaga pobrania specjalistycznej aplikacji do skanowania kodów QR, najprawdopodobniej aplikacja jest złośliwa.
- Zastanów się dwa razy, zanim podasz poufne dane na jakiejkolwiek witrynie internetowej, do której trafisz za pomocą publicznie dostępnego kodu QR.

Kody QR to wygodny sposób na dostęp do wszelkiego rodzaju informacji. Wykonanie kilku prostych kroków pomoże w pełni z nich korzystać.

Redaktor gościnny

Abdulmajeed AlAbdulhadi jest konsultantem ds. systemów IT/OT w Saudi Aramco z ponad 27-letnim doświadczeniem. Jest Certyfikowanym Audytorem Systemów Informatycznych (CISA) oraz Certyfikowanym Menedżerem Bezpieczeństwa Informacji (CISM) z patentem cyberbezpieczeństwa przyznanym przez amerykański urząd patentowy (10,693,906).

Źródła

Oszustwa bazujące na wiadomościach tekstowych: https://www.sans.org/newsletters/ouch/messaging-smishing-attacks/
Ataki i oszustwa telefoniczne: https://www.sans.org/newsletters/ouch/vishing/
Bezpieczeństwo urządzeń mobilnych:
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltf4e23f61005c39a7/60e8b43fb1bfa71471c7c3a0/ouch!_july_2021_securing_your_mobile_device_pl.pdf

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz