OUCH! Październik 2024

OUCH!

Biuletyn Bezpieczeństwa Komputerowego

SANS SECURITY AWARENESS

Szkodliwe oprogramowanie

Krótka opowieść ku przestrodze

Sara pewnego dnia przeglądając media społecznościowe, natknęła się na reklamę nowej aplikacji do edycji zdjęć „PiksPerfect". Zaintrygowana jej oszałamiającymi możliwościami, pobrała ją bez wahania. Początkowo aplikacja działała świetnie, ale wkrótce jej telefon stał się powolny i zaczął wyświetlać losowe reklamy. Kilka dni później do Sary zadzwonił pracownik banku, w której poinformował ją o podejrzanych transakcji. Sprawdziła swoją aplikację bankową i odkryła, że jej oszczędności zostały niemal całkowicie wyczyszczone. Po zgłoszeniu oszustwa i zablokowaniu konta była zdezorientowana i zdenerwowana.

Postanowiła przeanalizować całą sytuację. Uświadomiła sobie, że pobrana aplikacja do edycji zdjęć była fałszywa. Sarah po tym zajściu stała się ostrożniejsza i zaczęła dogłębnie sprawdzać aplikacje mobilne przed ich zainstalowaniem. Teraz dzieli się swoją historią, aby ostrzec innych, rozumiejąc że chwila nieuwagi może mieć daleko idące konsekwencje.

Jak sprawdzić, które aplikacje są bezpieczne?

Aplikacje mobilne są niesamowicie wygodne. Umożliwiają robienie wielu rzeczy za naciśnięciem jednego przycisku. Cyberprzestępcy zaczęli się tym zainteresowali i rozpoczęli tworzenie fałszywych aplikacji mobilnych. Celem oszustów jest przejęcie kontroli nad urządzeniem, pozyskanie poufnych danych lub monitorowanie wszystkiego co robisz. Dlatego bardzo ważne jest upewnienie się, że instalujesz aplikacje z oficjalnej dystrybucji.

Po pierwsze i najważniejsze, pobieraj aplikacje mobilne tylko z oficjalnych sklepów tj. Apple App Store lub Google Play Store. Pomaga to zmniejszyć ryzyko pobrania podejrzanej aplikacji. Wystrzegaj się zewnętrznych sklepów z aplikacjami, które mogą być zarządzane przez cyberprzestępców. Jednakże zdarzają się wyjątki. Historia pokazała, że nawet aplikacji w oficjalnych sklepach mogą być fałszywe. Przedstawiamy kilka prostych kroków, które możesz podjąć, aby upewnić się, że pobierasz legalne i bezpieczne aplikacje mobilne.

1. **Sprawdź nazwę twórcy**: Szukając konkretnej aplikacji mobilnej stworzonej przez określoną firmę, upewnij się, że aplikacja, którą pobierasz, została stworzona przez tę firmę. Powszechną sztuczką oszustów jest tworzenie aplikacji mobilnych, które wyglądają bardzo podobnie do znanych aplikacji. Sprawdź nazwę dewelopera - czy jest to ta sama firma lub znany twórca, czy też aplikacja została stworzona przez kogoś, o kim nigdy nie słyszałeś? Inną opcją jest odwiedzenie oficjalnej strony internetowej aplikacji lub dewelopera, aby znaleźć bezpośrednie linki do aplikacji mobilnej w sklepie z aplikacjami. Tylko to zagwarantuje Ci, że pobierasz legalną aplikacje.

2. **Przeczytaj recenzje i oceny**: Sprawdź komentarze i oceny użytkowników. Oficjalna aplikacja z reguły będzie miała znaczną liczbę pozytywnych recenzji i wysokie oceny. Omijaj szerokim łukiem aplikacje z niewielką liczbą recenzji, wieloma negatywnymi recenzjami lub zbyt pozytywnymi recenzjami, które brzmią podejrzanie.

3. **Sprawdź liczbę pobrań**. Legalne aplikacje mają zazwyczaj dużą liczbę pobrań. Niech Ci się zapali czerwona lampa, jeśli zauważysz aplikację z niską liczbą pobrań.

4. **Sprawdź uprawnienia**: Przed pobraniem aplikacji przejrzyj jakich uprawnień wymaga aplikacja. Legalne aplikacje będą żądać uprawnień tylko niezbędnych do ich działania. Uważaj na aplikacje żądające nadmiernych lub nieistotnych uprawnień. Zastanów się czy dana aplikacja naprawdę musi znać lokalizację lub mieć dostęp do kontaktów czy mikrofonu?

5. **Regularnie aktualizuj oprogramowanie**: Legalne aplikacje są regularnie aktualizowane w celu naprawienia błędów i poprawy wydajności. Sprawdź historię aktualizacji aplikacji. Fałszywe aplikacje zazwyczaj nie są w ogóle aktualizowane.

6. **Bądź ostrożny w stosunku do nowych aplikacji**: Nowe aplikacje bez ocen i komentarzy powinny być traktowane z należytą ostrożnością. Jeśli aplikacja jest legalna, prawdopodobnie z czasem zyska pozytywne recenzje i oceny.

Jak już zdecydujesz się na pobranie aplikacji, upewnij się że są włączone automatyczne aktualizacje. W kodzie i konfiguracjach aplikacji mobilnych stale znajdowane są nowe błędy i luki. Dlatego miej pewność, że korzystasz z najnowszej wersji swoich aplikacji. Jeśli natomiast już nie korzystasz danej aplikacji, po prostu usuń ją z telefonu.

Redaktor gościnny

Danielle Strimbu jest managerem w Travel Minds Digital Agency. Posiada doświadczenie w technologii i zarządzaniu operacjami. Jako przewodnicząca wydarzeń w WiCyS Colorado Affiliate, stara się organizować angażujące wydarzenia, aby pomóc kobietom w cyberbezpieczeństwie. Posiada tytuł magistra w dziedzinie bezpieczeństwa systemów informatycznych oraz dyplom ukończenia studiów w zakresie zarządzania cyberbezpieczeństwem.

Źródła

Trzy najczęstsze sposoby ataków: https://www.sans.org/newsletters/ouch/top-ways-attackers-target-you/
Działania na emocjach - o tym jak cyberprzestępcy oszukują: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/
All You Need to Know About Background Data: https://www.avast.com/c-what-is-background-data#

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz