Bitdefender

Jakie są zagrożenia związane z sideloadingiem aplikacji na smartfonie?

07.08.2023

Ekosystem Androida jest znany z narażenia na zagrożenia bezpieczeństwa z powodu aplikacji pobieranych z boku. Użytkownicy iOS mogą wkrótce znaleźć się w tej samej sytuacji, jeśli Apple zastosuje się do nowej unijnej ustawy o rynkach cyfrowych. Sideloading odnosi się do praktyki instalowania aplikacji ze źródeł innych niż oficjalne sklepy z aplikacjami, takie jak Google Play Store lub Apple App Store. Ładowanie boczne może oferować dostęp do szerszego zakresu programów i usług, ale wiąże się z wieloma zagrożeniami dla bezpieczeństwa.

Sideloading – najczęstsze zagrożenia

Siedeloading to praktyka, dzięki której możemy korzystać z wielu przydatnych aplikacji. Niestety niesie ona ze sobą także wiele cyberniebezpieczeństw. Poniżej zespół Bitdefender przygotował najpopularniejsze zagrożenia, z którymi możemy się spotkać podczas

korzystania z ładowania bocznego.

Złośliwe oprogramowanie

Największym problemem związanym z sideloadingiem jest nieświadome instalowanie złośliwego oprogramowania na naszym urządzeniu. Aplikacje pobierane z boku nie przechodzą tak samo rygorystycznych kontroli bezpieczeństwa, jak oprogramowanie dystrybuowane w oficjalnych sklepach z aplikacjami. Dlatego cyberprzestępcy mogą rozpowszechniać szkodliwe kody, które mogą wykonywać złośliwe działania.

W 2021 roku badacze Bitdefender odkryli partię złośliwych aplikacji na Androida dystrybuowanych za pośrednictwem stron trzecich, które podszywały się pod popularne marki. Zauważono, że cyberprzestępcy rozpowszechniali trojany bankowe TeaBot i Flubot w celu przeprowadzania ataków nakładkowych za pośrednictwem usług ułatwień dostępu Androida. Złośliwa kampania miała na celu przechwytywanie wiadomości, kradzież kodów Google Authentication, a także przejęcie pełnej kontroli nad urządzeniami z Androidem.

Gwarancja

Pobieranie aplikacji może czasami powodować problemy ze zgodnością z systemem operacyjnym urządzenia, prowadząc do awarii, problemów z wydajnością lub niestabilności systemu. Twój sprzedawca może uznać, że ten scenariusz jest podstawą do unieważnienia gwarancji Twojego smartfonu. Dlatego, jeśli jesteś zdecydowany na przeprowadzenie

ładowania bocznego, to skorzystaj ze starszego modelu smartfonu.

Prywatność

Aplikacje pobierane z sideloadingu mogą żądać nadmiernych uprawnień lub dostępu do poufnych danych na Twoim urządzeniu bez odpowiedniego nadzoru. Może to prowadzić do nieautoryzowanego dostępu do Twoich danych osobowych, w tym zdjęć, kontaktów i danych o lokalizacji.

Kontrola jakości

Oficjalne sklepy z aplikacjami nie tylko analizują aplikacje pod kątem zagrożeń dla bezpieczeństwa lub prywatności; dokładny proces sprawdzania zapewnia również to, że aplikacje działają zgodnie z reklamą przed umieszczeniem ich na liście. Sideloading pomija tę recenzję, zwiększając prawdopodobieństwo, że wdrożysz szkodliwą lub źle zaprojektowaną aplikację na swoim urządzeniu.

Piractwo

Pirackie wersje drogich aplikacji lub gier nie są niczym niezwykłym w świecie mobilnym, zwłaszcza w ekosystemie Androida. Piractwo komputerowe jest nie tylko nielegalne, ale może również narazić użytkownika na ryzyko związane z bezpieczeństwem lub prywatnością. Aplikacje pobrane z nieoficjalnych źródeł mogą zostać zmodyfikowane tak, aby zawierały złośliwy kod. Może to skutkować nieautoryzowanym dostępem, kradzieżą danych lub niechcianymi działaniami na Twoim

urządzeniu.

Luźne aktualizacje i wsparcie

Deweloperzy, którzy sprzedają swoje oprogramowanie poza oficjalnymi miejscami, mogą nie być tak skrupulatni w reagowaniu na luki związane z bezpieczeństwem lub prywatnością. Oznacza to, że aktualizacje zabezpieczeń mogą być dostarczane z opóźnieniem lub wcale. Ponadto w przypadku aplikacji pobieranych z boku czasami trzeba ręcznie sprawdzać dostępność aktualizacji, co nie powinno mieć miejsca w 2023 r.

Wniosek

Oczywiste jest to, że cyberprzestępcy przemycają złośliwe oprogramowanie do programów w oficjalnych sklepach z aplikacjami. Jednak szanse na stanie się ofiarą złośliwych kodów z tego źródła są znacznie mniejsze niż w przypadku pobierania aplikacji spoza oficjalnych sklepów. W systemie iOS cyberprzestępcy mają jeszcze mniejsze możliwości, ponieważ Apple ściśle kontroluje sposób, w jaki aplikacje są opracowywane i dystrybuowane do użytku na urządzeniach iDevices. W 2024 r. producent iPhone'a może zostać prawnie zmuszony do otwarcia systemu dla sideloadingu aplikacji, co oznacza, że użytkownicy iOS będą musieli stawić czoła podobnym zagrożeniom.

„Sideloading może brzmieć atrakcyjnie, jeśli pragniesz pewnych swobód lub nieuczciwych praktyk. Pamiętaj jednak, że ładowanie boczne jest głównym wektorem złośliwego oprogramowania przedostającego się na

nasze telefony. Jeśli mimo to pobierasz aplikacje, przynajmniej sprawdź, czy źródło jest zaufane i uważaj na aplikacje, które żądają nadmiernych uprawnień lub wydają się podejrzane w jakikolwiek sposób. Używaj także niezawodnej aplikacji antywirusowej do skanowania aplikacji pobranych z boku w celu wykrycia potencjalnych zagrożeń" – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło:https://bitdefender.pl/jakie-sa-zagrozenia-zwiazane-z-sideloadingiem-aplikacji-na-smartfonie/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 07.08.2023
Z pozdrowieniami Piotr Rozmiarek
E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender
Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.