Bitdefender

Usługa ułatwień dostępu na Android – pomoc dla osób niepełnosprawnych, czy cyberniebezpieczeństwo?

09.10.2023

Usługa ułatwień dostępu w Androidzie to potężne narzędzie, które pozwala osobom niepełnosprawnym łatwiej korzystać z urządzeń mobilnych. Jest także ulubionym narzędziem przestępców chcących przejąć kontrolę nad urządzeniem. Zespół Bitdefender postanowił przyjrzeć się Usłudze ułatwień dostępu na Androidzie. Dlatego w tym artykule przeanalizujemy, w jaki sposób może nam zagrażać dawanie aplikacjom niepotrzebnych dostępów oraz jak możemy się zabezpieczyć przed działaniami hakerów na Android.

Usługa ułatwień dostępu na Android – jak korzystają z niego hakerzy?

Usługa ułatwień dostępu to uprawnienie rzadko przywoływane przez aplikacje, które nie mają nic wspólnego z zapewnianiem osobom niepełnosprawnym przydatnych funkcji. Jej możliwości są dobrze znane

i bardzo niewiele oficjalnych aplikacji będzie je niepotrzebnie wykorzystywało w obawie, że ściągnie na siebie gniew Google.

Z drugiej strony producenci złośliwych aplikacji nie mają takich samych skrupułów, gdy wywołują uprawnienia ułatwień dostępu.
Wiele rodzajów złośliwego oprogramowania będzie próbowało uzyskać dostęp do tej opcji w celu przejęcia kontroli i monitorowania urządzeń.

Jeśli chodzi o pobieranie lub instalowanie aplikacji innych firm na urządzeniach, nie ma wątpliwości, że Android jest liderem w tej kategorii. Jednak ta sytuacja otwiera również możliwość zainstalowania złośliwego oprogramowania, które będzie próbowało uzyskać dostęp do urządzeń i wywołać uprawnienia dostępu.

Dlaczego warto zwrócić uwagę na usługi ułatwień dostępu?

Z usługi ułatwień dostępu można korzystać na niezliczone sposoby, aby pomagać ludziom, a oficjalne stanowisko Google jest takie, że z tej funkcji powinny korzystać tylko odpowiednie aplikacje przeznaczone dla osób niepełnosprawnych. Niestety wielu producentów aplikacji na Android swego czasu implementowało w swoich programach praktycznie wszystkie możliwe dostępy do urządzeń użytkowników, w tym usług ułatwień dostępu.

W nowoczesnych urządzeniach z Androidem już tak nie jest. Teraz tylko wtedy, gdy aplikacja potrzebuje określonego uprawnienia, użytkownik udzieli go jawnie. W rzeczywistości aplikacja musi określić, dlaczego potrzebuje tego konkretnego pozwolenia. Na przykład, po co zapewniać

aplikacji pogodowej dostęp do SMS-ów i połączeń telefonicznych?

Właściciele smartfonów i tabletów z Androidem muszą pamiętać, że usługi ułatwień dostępu mają ogromną moc. Powinniśmy natychmiast wzbudzić podejrzenia, gdy aplikacja poprosi o uprawnienia w tym obszarze.

Oto lista tego, co atakujący mogą zrobić, korzystając z ułatwień dostępu

- Usługa ułatwień dostępu może zobaczyć wszystko, co jest wyświetlane na ekranie i wprowadzić dane zgodnie z poleceniami użytkownika.

- Zezwolenie na uprawnienia dostępu może narazić właściciela urządzenia na ryzyko finansowe i osobiste. Atakujący mogą kraść poufne informacje, takie jak dane bankowe i inne dane osobowe (wiadomości z czatów, kod PIN, hasła do różnych kont, kontakty i wiele innych).

- Złośliwe oprogramowanie, takie jak trojany bankowe, może wykorzystywać tę usługę do wyświetlania przezroczystych nakładek, które oszukują użytkowników i kradną ich dane uwierzytelniające przy użyciu fałszywej aplikacji lub strony banku.

- Trojany można umieścić na aplikacjach bankowych i prawie na wszystkich innych aplikacjach w tym także na Ustawieniach. Dzięki

ułatwieniom dostępu trojany bankowe mogą odczytywać dane uwierzytelniające, podczas gdy użytkownicy wpisują je w rzeczywistej aplikacji bankowej. W rzeczywistości może to posunąć się tak daleko, jak symulowanie klikania przycisków i wykonywania przelewów pieniężnych.

- Wraz z uprawnieniami administratora urządzenia złośliwe oprogramowanie może robić wszystko na urządzeniu (tj. wysyłać SMS-y, przekierowywać połączenia etc.).

- Aby zapewnić trwałość, złośliwe oprogramowanie może uniemożliwić użytkownikowi jego odinstalowanie.

W jaki sposób zabezpieczyć smartfon z Androidem?

Użytkownicy Androida mogą zachować bezpieczeństwo, instalując rozwiązania zabezpieczające, takie jak systemy antywirusowe, które mogą stanowić proaktywny środek przeciwko zagrożeniom, które jawnie nadużywają możliwości ułatwień dostępu. Pamiętajmy także o tym, aby nie otwierać załączników do wiadomości e-mail od nieznanych nadawców, nie klikać łączy w podejrzanych wiadomościach, a także być zawsze podejrzliwym w stosunku do każdej aplikacji proszącej o uprawnienia dostępu – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefenter.

Źródło: https://bitdefender.pl/usluga-ulatwien-dostepu/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.

Data udostępnienia: 09.10.2023

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.