

Wykrywanie anomalii aplikacji Bitdefender na Androida rzuca światło na nowe cyberzagrożenia

28.08.2023

Wykrywanie anomalii aplikacji to pierwsza w branży antywirusowej dodatkowa warstwa ochrony, która działa w czasie rzeczywistym i jest oparta na zachowaniu aplikacji. Wprowadzenie pierwszej w branży technologii zwykle daje ciekawe rezultaty i dokładnie to samo stało się z dodaniem Wykrywania Anomalii Aplikacji do Bitdefender Mobile Security dla Androida. Cyberprzestępcom będzie teraz znacznie trudniej wykorzystywać niebezpieczne oprogramowanie, ponieważ działania aplikacji same w sobie zdradzają jej złe intencje.

Wykrywanie anomalii aplikacji Bitdefender – w jaki sposób działa?

Nowa technologia działa na zasadzie analizy zachowania aplikacji po ich zainstalowaniu. Jest to ważne, ponieważ przestępcy dokładają wszelkich starań, aby ukryć swoje zamiary, co obejmuje zapewnienie, że aplikacje Wykrywanie anomalii aplikacji Bitdefender na Androida rzuca światło na nowe cyberzagrożenia

pozostaną w stanie uśpienia przez długi czas, zanim zaczną działać, przesyłanie aktualizacji, które zamieniają legalną aplikację w zagrożenie, a nawet wykorzystywanie luk dnia zerowego w celu naruszenia bezpieczeństwa urządzenia.

Wykrywanie anomalii – wstępne wnioski

Po kilku miesiącach od uruchomienia modułu wykrywania anomalii producent Bitdefender przeanalizował dane i przygotował wstępne wnioski. Pierwszym z nich jest to, że sposób, w jaki aplikacja zachowuje się w tle, może szybko ujawnić jej prawdziwe intencje, nawet jeśli na początku była pozornie legalną aplikacją. Zdaniem zespołu Bitdefender ludzie chętnie pobierają adware. Wielu użytkowników Androida szuka także pirackich aplikacji, pełnych gier, cracków i podobnego oprogramowania.

Rzeczywistość jest taka, że większość treści znajdujących się na pierwszej stronie wyników wyszukiwania w Internecie jest pełna złośliwych aplikacji. Jest to podstęp mający na celu nakłonienie ludzi do pobrania fałszywych aplikacji na Androida, które przynajmniej zainstalują trudny do usunięcia pełnoekranowy system reklam.

To nie tylko reklamy, to coś znacznie gorszego

Badanie zespołu Bitdefender wykazało, że wiele z tych fałszywych aplikacji to w rzeczywistości ukryte oprogramowanie reklamowe. Prawdopodobnie są tworzone w sposób zautomatyzowany, aby stworzyć iluzję różnych wersji!

Wykrywanie anomalii aplikacji Bitdefender na Androida
rzuca światło na nowe cyberzagrożenia

Bitdefender[®]

Samo oprogramowanie reklamowe jest agresywne, sprytnie ukrywa się przed użytkownikiem i jest trudne do usunięcia. Tak naprawdę, oprogramowanie reklamowe nie pojawi się nawet w ciągu pierwszych kilku tygodni, lecz pozostanie ukryte. Jeśli jednak spróbuje wykonać cokolwiek na urządzeniu użytkownika, np. wyświetlić reklamę na pełnym ekranie, technologia wykrywania anomalii aplikacji szybko poinformuje użytkowników o zagrożeniach.

„Niektóre aplikacje przechwytywane przez funkcję App Anomaly Detection zawierają trojany bankowe, które mogą kraść dane finansowe, rejestrować naciśnięcia klawiszy, robić zrzuty ekranu i nie tylko. Ponadto jedną szczególną tendencją, którą zaobserwowano, jest rozprzestrzenianie się oprogramowania stalkerware – niebezpiecznego typu aplikacji wykorzystywanej przez ludzi do szpiegowania dzieci lub współmałżonków. W większości przypadków użytkownicy uważają, że faktycznie instalują legalne aplikacje. W rzeczywistości oprogramowanie to ma tylko wspólną nazwę z oryginałami. Sklepy i strony internetowe stron trzecich są pełne fałszywych aplikacji, co czyni je jednym z głównych miejsc dystrybucji” – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło: <https://bitdefender.pl/wykrywanie-anomalii-aplikacji-bitdefender/>

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

Data udostępnienia: 28.08.2023

Wykrywanie anomalii aplikacji Bitdefender na Androida
rzuca światło na nowe cyberzagrożenia

Bitdefender[®]

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.