

## **Nowa technologia wykrywania anomalii w aplikacjach od Bitdefender**

16.06.2023

Hakerzy nieustannie pracują nad opracowaniem nowych sposobów włamania się do telefonów i tabletów z Androidem za pośrednictwem oficjalnych sklepów, stron internetowych osób trzecich lub ręcznej instalacji. Powszechnie stosowaną metodą ataku jest oczywiście nakłanianie ludzi do pobierania i instalowania złośliwego oprogramowania z własnej woli. Dlatego firma Bitdefender postanowiła wprowadzić do rozwiązania Bitdefender Mobile Security for Android nową technologię App Anomaly Detection, dzięki której użytkownicy zyskają nową warstwę ochrony przed złośliwym oprogramowaniem.

### **Dlaczego Bitdefender wprowadza technologię wykrywania anomalii**

„System antywirusowy, który ma za zadanie zatrzymanie niebezpieczeństw na bramce wejścia, jest obecnie niewystarczające. Powody są dwa: po pierwsze użytkownicy, często nagminnie ignorują

niebezpieczeństwa w sieci, po drugie legalne i bezpieczne aplikacje potrafią po zainstalowaniu zmienić się po aktualizacji, nabierając cech złośliwego oprogramowania” – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Jednym z największych problemów bezpieczeństwa jest niefrasobliwy użytkownik urządzenia. Zespół Bitdefender od wielu lat dostrzega, że niektóre osoby ignorują powtarzające się ostrzeżenia, aby nie instalować złośliwej aplikacji, odrzucają wyniki skanowania, a nawet posuwają się do wyłączenia rozwiązania zabezpieczającego, aby móc faktycznie wdrażać niebezpieczne aplikacje wykorzystywane przez przestępców do ataków. Przy takich działaniach nawet najlepszy system antywirusowy nie jest w stanie uchronić urządzenia, zarządzanego przez takiego niefrasobliwego użytkownika.

Oficjalne sklepy z aplikacjami są zwykle bezpiecznymi źródłami aplikacji, ale badania przeprowadzone przez pracowników Bitdefender wykazały, że nie zawsze tak jest. Niektóre aplikacje prześlizgują się przez bramki i trafiają na urządzenia, nawet jeśli ich użytkownicy sądzą, że mają legalną aplikację. Czasami hakerzy są zainteresowani tylko wyświetlaniem irytujących reklam w innych aplikacjach, ale od czasu do czasu możliwe jest również uzyskanie programów implementujących złośliwe oprogramowanie. To jeden z powodów, dla których Google i inne firmy często usuwają aplikacje z oficjalnych sklepów.

Nie możemy również dyskutować zewnętrznych źródeł pobierania. Nowa technologia wykrywania anomalii w aplikacjach od **Bitdefender**  
Bitdefender

Jedną z mocnych stron Androida jest możliwość instalowania aplikacji bez korzystania z oficjalnych sklepów. Jest to również jedno z najważniejszych zagrożeń w zakresie bezpieczeństwa, ponieważ wiele zewnętrznych źródeł aplikacji na Androida roi się od złośliwego oprogramowania czekającego na dobrowolne zainstalowanie przez niefrasobliwych użytkowników.

### **Nowa technologia wykrywania anomalii**

Niestety zawsze istnieje możliwość, że nowe złośliwe oprogramowanie przedostanie się na urządzenie, czy to z oficjalnego sklepu, zewnętrznego źródła, czy też w wyniku złośliwej kampanii. Może przejść wstępną kontrolę systemu antywirusowego lub użytkownik może wymusić jego instalację. Jednak w każdym przypadku właściciel urządzenia musi pozostać chroniony nawet po zainstalowaniu tego podejrzanego oprogramowania. Zadanie rozwiązania zabezpieczającego nigdy się nie kończy.

Przykładem takiego złośliwego oprogramowania jest Xenomorph. To trojan bankowy, stale rozwijany, który ma dwa cele: omijanie skanów i dodawanie nowych funkcji. W tej chwili jest to prawdopodobnie jeden z najbardziej zaawansowanych aktywnych typów złośliwego oprogramowania.

Telefon komórkowy może zostać zainfekowany tym wirusem – nawet jeśli na urządzeniu działa już Bitdefender Mobile Security – jeżeli użytkownik „ręcznie” przyzna dostęp temu złośliwemu oprogramowaniu do wprowadzania zmian.

Nowa technologia wykrywania anomalii w aplikacjach od **Bitdefender**  
Bitdefender

Oczywiście niebezpieczna aplikacja może wyglądać na legalne i bezpieczne, ale jednym z jego działań jest wyświetlenie przezroczystego okna gotowego do przechwycenia danych wprowadzonych przez użytkownika. W tym właśnie momencie zadziała nowa funkcja wychwytywania anomalii Bitdefender, która zablokuje podejrzanę działalność i poinformuje o tym użytkownika. Więc jest to kolejna warstwa ochrony, która ostrzeże zagrożonego internautę – niezależnie od tego, czy podejrzana aplikacja jest nowa, czy działa na smartfonie już od wielu lat.

Oczywiście nie jest to jedyny scenariusz, w którym technologia zostanie aktywowana, ale przykład ten pokazuje, jak podstępne może być złośliwe oprogramowanie i jak działa Bitdefender, aby zapewnić ludziom bezpieczeństwo, bez względu na używaną platformę.

Nowe wykrywanie anomalii w aplikacji jest teraz dostępne dla wszystkich użytkowników Bitdefender Mobile Security dla systemu Android bez dodatkowych kosztów.

Źródło: <https://bitdefender.pl/nowa-technologia-wykrywania-anomalii-w-aplikacjach-od-bitdefender/>

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

Data udostępnienia: 16.06.2023

Z pozdrowieniami Piotr Rozmiarek

E-mail: [piotr.r@marken.com.pl](mailto:piotr.r@marken.com.pl) | Tel. bezpośredni: 570 400 019

Nowa technologia wykrywania anomalii w aplikacjach od **Bitdefender**  
Bitdefender

## 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.