



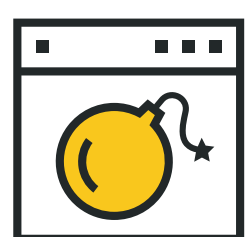
OPROGRAMOWANIE RANSOMWARE
W URZĄDZENIACH MOBILNYCH

POŻEGNAJ SIĘ ZE SWOIMI PLIKAMI

Ransomware odbiera ci dostęp do urządzenia mobilnego i plików, żądając w zamian okupu. Ten typ szkodliwego oprogramowania blokuje ekran urządzenia i uniemożliwia dostęp do niektórych plików oraz funkcji.



JAK SIĘ ROZPRZESTRZENIA?



Odwiedzanie niebezpiecznych witryn internetowych.

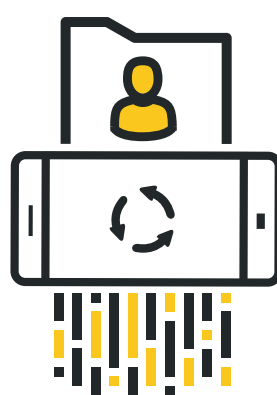


Pobieranie fałszywych wersji prawdziwych aplikacji.



Klikanie szkodliwych linków i załączników dołączonych do wiadomości e-mail wysłanych jako phishing.

JAKIE ISTNIEJĄ ZAGROŻENIA?



Może zaistnieć konieczność fabrycznego zresetowania urządzenia, które będzie prowadzić do utraty wszystkich danych.



Agresor będzie miał pełny dostęp do Twojego urządzenia, a w konsekwencji —możliwość udostępnienia danych stronom trzecim”.

CO MOGĘ ZROBIĆ?



Regularnie twórz kopie zapasowe danych i aktualizuj wszystkie aplikacje oraz system operacyjny.



Nie kupuj niczego w sklepach z aplikacjami stron trzecich.



Jeśli to możliwe, zainstaluj aplikację bezpieczeństwa do urządzeń mobilnych, która ostrzeże o naruszeniu bezpieczeństwa urządzenia.



Zwracaj uwagę na wiadomości e-mail oraz strony internetowe, które wydają się podejrzane lub niewiarygodne.



Nie przydzielaj nikomu uprawnień administratora.



Nie płać okupu. W ten sposób będziesz finansować przestępców i zachęcać ich do kontynuowania nielegalnej działalności.