Bitdefender

A Bitdefender Mobile Security új oktatási réteget kap a hatékony átverés-riasztási (Scam Alert) funkcióhoz

Az egyik alapvető biztonsági réteg a tájékozott felhasználó. Az online fenyegetések megismerése ugyanolyan fontos, mint a biztonsági megoldás háttérben történő futtatása, és a Bitdefender Mobile Security for Androidban elérhető új oktatási réteg célja, hogy az emberek még tájékozottabbak legyenek.

A Bitdefender Mobile Security for Androidhoz hozzáadott legújabb funkció a Scam Alert nevet viseli. Ez egy olyan új képesség, amellyel a biztonsági megoldás az értesítésekben megjelenő SMS-üzeneteket és linkeket vizsgálja. A Scam Alert figyelmezteti a felhasználókat, ha rosszindulatú linket kapnak, és tájékoztatást nyújt számukra a teendőkről.

A Scam Alert funkció ereje különösen olyan globális kampányok során mutatkozik meg, mint például a Flubot nevű banki trójai, amely SMS-üzeneteken keresztül terjed egyik eszközről a másikra, és a hamis weboldalra mutató link is SMS-ben érkezik a felhasználók készülékére. Ezt követően, ha valaki megnyitja az SMS-ben kapott linket, akkor egy ál-weboldalra kerül, ahol egy validnak tűnő, ám de káros kóddal fertőzött program letöltésére próbálják rávenni a felhasználókat. Ha valaki letöltötte az appot, akkor a vírusnak ki-bejárása van a névjegyzékükbe, az SMS és MMS fiókjaiba stb.: persze teszi mindezt úgy a kártevő, hogy az áldozat ebből semmit sem érzékel. Mivel banki trójairól van szó, leginkább a pénzügyekhez kapcsolódó applikációkat veszi célba, úgy, hogy lemásolja, letükrözi azokat, és szépen létrehozza a saját maga kis káros applikációját, ami pontosan ugyanúgy fog kinézni, mint az eredeti app. És ha innentől kezdve az áldozat bármikor megnyitja azt a bizonyos – jellemzően pénzügyi - appot, akkor bizony már a csalók markában van, hiszen tálcán kínálta nekik minden szenzitív adatát.

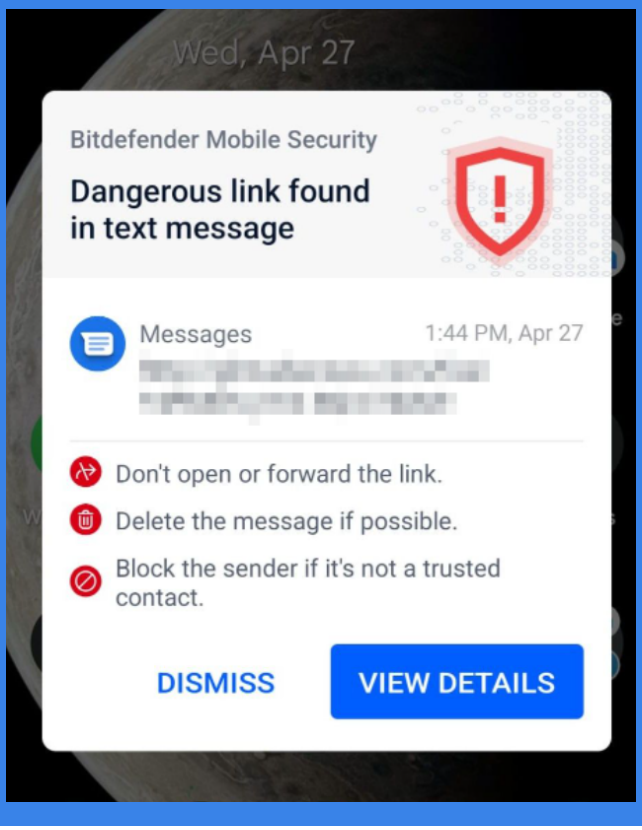
A tudás hatalom!

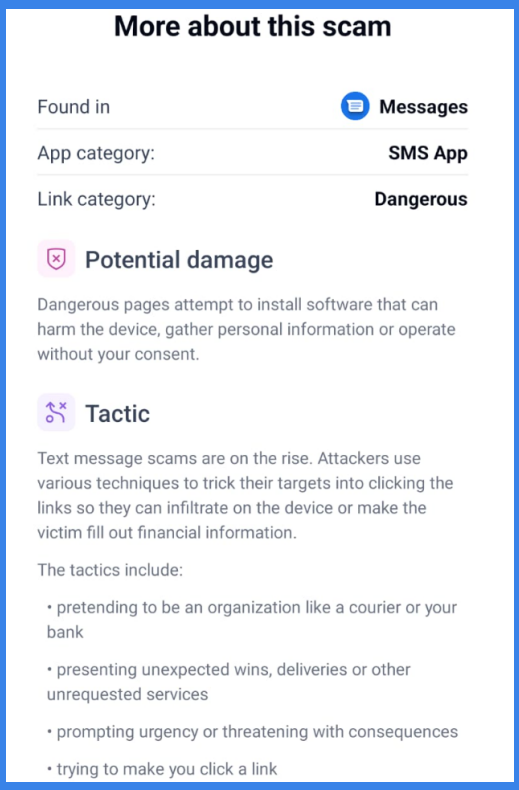
A támadók indítékai nem mindig egyértelműek. Előfordul, hogy egy link egy adathalász webhelyre küldi a potenciális áldozatot, de ez a legjobb esetben is csak a legideálisabb forgatókönyv. Egy rosszindulatú link bizonyos helyzetekben olyan weboldalra irányíthatja át a felhasználót, amely egy veszélyes alkalmazás letöltését indítja el. Lásd Flubot. És a Flubot a közelmúltban hazánkban is többször felütötte a fejét: 2021 tavaszán rengeteg ember készülékét fertőzte meg, ezt követően – bár kisebb volumenben – de 2022 januárjában is visszatért a kártevő. Üzemeltetői, használói az aktuális eseményeket felhasználva változtatják meg az üzeneteket, abból a célból, hogy jobban horogra csalják az áldozatokat. A FluBot malwaret felhasználó csalások jó példák arra, milyen is az, amikor a kiberbűnözők jól alkalmazkodnak az aktuális helyzethez és maga a csalási formula, miképp tud releváns maradni az idő előrehaladtával. Mindig van új a kibertér alatt. A csali SMS sok esetben más-más ürügyet használ: a tavaly tapasztalt „futárcéges-csomagja érkezett” indokot felváltotta egy csomaggal kapcsolatos nem létező problémának a megemlítése, majd új komponensként megjelent az az új változata is, ami egy korábbi Facebook Messengeren elterjedt csaláshoz hasonlít. Ebben a változatban a felhasználók SMS-t kapnak egy ismerősüktől, amiben a „Te vagy ebben a videóban / Úgy néz ki, mint Te?” kérdések, vagy ezek további variációja szerepel. És a kérdés után található egy link, aminek megnyitása után a már fent említett analógia az irányadó.

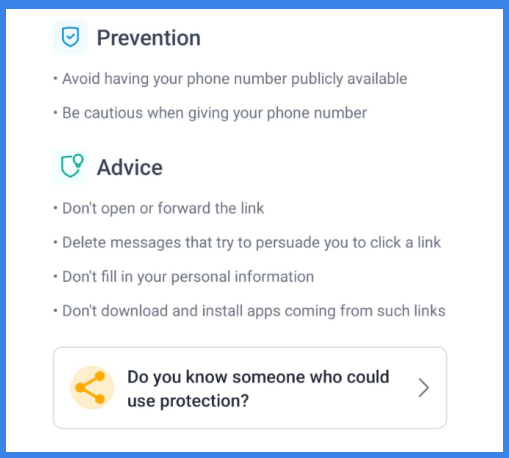
Az ilyen jellegű fenyegetések azért tudnak életben maradni, mert hullámokban érkeznek különböző üzenetekkel és különböző időzónákban. Míg maga a rosszindulatú program meglehetősen statikus marad, a hordozásához használt

üzenet, a droppereket befogadó tartományok (és minden más) folyamatosan változik. A Bitdefender Mobile Security & Antivirusban már alapértelmezetten elérhető Scam Alert funkció telemetriájának elemzésével 2021. december 1-e óta több mint 200.000 rosszindulatú SMS üzenetet fogtak el, amelyek a FluBot malware terjesztésére irányultak.

Ha a Bitdefender Mobile Security felhasználója ilyen üzenetet kap, az új Scam Alert tájékoztatja, hogy az egy rosszindulatú link, és semmiképpen ne nyissa meg. Az új oktatási réteg további információkat kínál: részletesen tájékoztatja a felhasználókat a kockázatokról és arról, hogy milyen károkat szenvedhettek volna el, ha rákattintanak a linkre, valamint tanácsokat ad, hogy a jövőben hogyan minimalizálhatják a kockázatot hasonló fenyegetések kapcsán.







A fenyegetések folyamatosan változnak

A Scam Alert szükségességét nem lehet vitatni, különösen most, hogy az ilyen típusú fenyegetések rendkívül elterjedtek. A bűnözők folyamatosan próbálják frissíteni a rosszindulatú szoftvereket és az alkalmazott taktikákat, azért, hogy új fenyegetéseket fejlesszenek ki. A lehető legjobb védelemhez tájékozott felhasználókra van szükség, és az oktatási réteg csak egy újabb lépés ezen cél felé.

A Scam Alert elérhető a Bitdefender Mobile Security for Android alkalmazásban minden új és jelenlegi felhasználó számára. Ez a biztonsági megoldás szerves részét képezi a védekezésnek, és még ha a felhasználó megpróbálja megnyitni a rosszindulatú linket, a Web Protection réteg blokkolja a link betöltését a böngészőben.

Fontos megemlíteni, hogy csak azért, mert egyes felhasználók iOS-t futtatnak, még nem jelenti azt, hogy biztonságban vannak. Az esetek többségében egy olyan rosszindulatú kampánynak, mint a Flubotnak, az a célja, hogy minél több androidos eszközt fertőzzön meg, és átirányítson egy másik fenyegetésre, például adathalászatra, ha a célpont iOS-eszközön nyitotta meg a linket. Ebben a helyzetben a Bitdefender Mobile Security for iOS-ben található Web Protection átveszi az irányítást, és blokkolja a linket.