TLP:WHITE
Szabadon terjeszthető!

Tájékoztatás

hamis vírusirtó alkalmazásokkal kapcsolatban

(2022. szeptember 08.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) **tájékoztató**t ad ki **hamis vírusirtó alkalmazásokkal kapcsolatban.**

A **Sharkbot** egy androidos készülékekre készített „újgenerációs" trójai program, amely elsősorban kompromittált eszközökről **pénzátutalások kezdeményezésére** szakosodott, azáltal, hogy **képes automatikusan kitölteni** a fertőzött eszközre telepített **legális banki alkalmazások mezőit**, illetve akár **teljes távoli hozzáférést** biztosíthat a fertőzött eszközön a támadó számára.

A káros kód számos káros funkcióval rendelkezik, képes például **billentyűnaplózásra**, **SMS üzenetek** elfogására, legutóbbi verziója pedig az internetes „sütikhez" is hozzáférhet. (Utóbbi azért veszélyes, mivel azok olyan szoftver- és helymeghatározási paramétereket tartalmazhatnak, amelyek segíthetnek megkerülni az ujjlenyomat-ellenőrzéseket, vagy bizonyos esetekben a felhasználói hitelesítéshez szükséges tokent is.)

Nemzetközi kiberbiztonsági csoportok jelzése alapján a Sharkbot új verzióját fedezték fel a **Google Play** áruházban elérhető alkalmazásokban. A káros kód egy mobil antivírus (**Kylhavy Mobile Security**), illetve egy eszköztisztító (**Mister Phone Cleaner**) alkalmazásnak **álcázva** került fel a Play áruházba.
Az alkalmazások azóta eltávolításra kerültek az alkalmazásboltból, azonban a felhasználóknak saját maguknak kell törölniük a készülékükről, amennyiben korábban telepítették azt.

Az appok önmagukban nem tartalmaztak rosszindulatú kódot, mivel a Sharkbot új változata két lépcsőben hajtja végre a támadást. A felhasználó letölti a jóindulatúnak tűnő szoftvert, később az egy frissítést kér – amellyel letöltésre kerül a vírus is. A felhasználó gyanúját esetleg az keltheti fel, hogy a frissítés nem a Google Play-en keresztül érkezik, hanem az alkalmazás futása közben maga az alkalmazás akar frissíteni.

TLP:WHITE
Szabadon terjeszthető!

A káros kódhoz kapcsolódó **indikátorok:**

C2 szerverek:

- n3bvakjjouxir0zkzmd[.]xyz (185.219.221[.]99)
- mjayoxbvakjjouxir0z[.]xyz (185.219.221[.]99)

Az NBSZ NKI javasolja a fenti alkalmazások haladéktalan eltávolítását, valamint az érintett eszköz gyári alapbeállításra történő visszaállítását követően a készüléken használt fiókokhoz tartozó jelszavak cseréjét.

Hivatkozások:

- https://www.cleafy.com/cleafy-labs/sharkbot-a-new-generation-of-android-trojan-is-targeting-banks-in-europe
- https://www.bleepingcomputer.com/news/security/sharkbot-malware-sneaks-back-on-google-play-to-steal-your-logins/
- https://thehackernews.com/2022/09/fake-antivirus-and-cleaner-apps-caught.html
- https://nki.gov.hu/it-biztonsag/hirek/ujabb-banki-kartevonek-sikerult-kijatszania-a-play-store-vedelmet/

Nemzetbiztonsági Szakszolgálat
Nemzeti Kibervédelmi Intézet
Telefon: +36-1-336-4833
Incidensbejelentés: csirt@nki.gov.hu