TLP: WHITE
Szabadon terjeszthető!

Rendkívüli tájékoztató

Csomagküldő szolgáltatók nevével visszaélő, malware terjesztéssel összefüggő SMS üzenetekkel kapcsolatban

FluBot blokkolása / eltávolítása

(2021. március 25.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) **rendkívüli tájékoztatót** ad ki a látszólag csomagküldő szolgáltatóktól érkező, kéretlen **SMS üzenetek** útján terjesztett **FluBot kártevővel kapcsolatban**.

Az NBSZ NKI további vizsgálatai alapján megállapította – a 2021.03.24-én közzétett riasztáshoz[1] kapcsolódóan –, hogy a fertőzésben érintett készülékek esetén a FluBot kártevő folyamatosan figyeli a készülékeken futtatott alkalmazásokat. Amennyiben a program pénzügyi vagy kriptovalutákhoz kapcsolódó alkalmazás indítását észleli, abban az esetben az eredeti alkalmazást „elfedi" (egy ún. overlay technikával), és az eredeti alkalmazás mellett, egy az eredetihez hasonló adathalász felületet nyit meg, amely képes a felhasználói (felhasználónév, jelszó) adatok kinyerésére és továbbítására.

Az eddigi ismeretek szerint a kártevő az alábbi alkalmazások felhasználóit célozza:

- MKB Mobilalkalmazás
- K&H mobilbank
- Budapest Bank Mobill App
- OTP SmartBank
- UniCredit Mobile Application
- George Magyarország
- Kripto tőzsdék, online Kriptotárcák:
- Blockchain Wallet
- Coinbase – Buy& Sell Bitcoin Crypto Wallet
- Binance - Buy& Sell Bitcoin Securely
- Blockchain Wallet

A malware vizsgálata alapján azonban a fenti lista változhat, ugyanis a célzott alkalmazások listája nincs előre rögzítve a kártevőben.

[1] https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-csomagkuldo-szolgaltatok-nevevel-visszaelo-malware-terjesztessel-osszefuggo-sms-uzenetekkel-kapcsolatban/

Az NBSZ NKI a FluBot fertőzésekkel kapcsolatban az alábbi sorrendben feltüntetett összes lépés megtételét javasolja:

1. „**FluBot Malware Uninstall**”[2] nevű alkalmazás **letöltése** a Google Play Áruházból, majd **telepítése**.
2. A fertőzött készülék **Wi-Fi és mobil adatkapcsolatának leállítása**.
3. A képernyőn megjelenő **utasítások követése**.
4. Az utasításokat követve, a **rosszindulatú alkalmazás eltávolítása**.
5. A képernyőn megjelenő lépések végrehajtásával az **alapértelmezett indítóválasztás visszavonása**.
6. „**FluBot Malware Uninstall”** nevű alkalmazás **eltávolítása**.

Amennyiben a „FluBot Malware Uninstall” nevű alkalmazás segítségével a fertőzés nem szűntethető meg, abban az esetben javasolt:

a. a készüléken tárolt adatokról (pl. fényképek, kontaktok, stb.) biztonsági mentés készítése, majd
b. a **készülék gyári beállításokra történő visszaállítása**.

Az NBSZ NKI munkatársai a „FluBot Malware Uninstall” nevű alkalmazás működését a következő verziókon tesztelték:

- Android 8.1;
- Android 9.0;
- Android 10.1;
- Android 11.0.

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

2 https://play.google.com/store/apps/details?id=space.linuxct.malninstall