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 tájékoztató**t ad ki a **Flubot fertőzés miatt** megnövekedett számú, **kéretlen szöveges üzenetek útján terjedő,** látszólag csomagküldő szolgáltatóktól érkező**, káros hivatkozást tartalmazó SMS üzenetekkel kapcsolatban**.
Az NBSZ NKI további vizsgálatai alapján a fertőzésben érintett készülékek esetén a Flubot kártevő folyamatosan figyeli a készülékeken futtatott alkalmazásokat, és amennyibe pénzügyi vagy kriptovalutákhoz kapcsolódó alkalmazás indítását észleli, abban az esetben egy ún. overlay technikával az eredeti alkalmazás mellett egy a hozzá hasonló adathalász felületet nyit meg, amely a felhasználó által beírt felhasználónév és jelszó párost rögzíti és továbbítja egy külső vezérlőszerverre.
Fertőzés esetén az eddigi ismeretek szerint a vezérlőszerver az alábbi alkalmazásokat 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 statikus vizsgálata alapján azonban a fenti lista változhat, ugyanis a célzott alkalmazások listája nincs „hardkódolva” a kártevőben, azokat futásidőben kapja meg a vezérlőszervertől titkosított HTTP forgalomban.

Az NBSZ NKI-hoz érkezett megkeresések alapján az alkalmazások letöltését és telepítését követően a fertőzésekkel kapcsolatban az NBSZ NKI az alábbi lépések megtételét javasolja:

1. „**FluBot Malware Uninstall**”[1] alkalmazás **letöltése** a Google Play Áruházból.

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

2. A fertőzött készülék **Wi-Fi és mobil adatkapcsolatának leállítása**.
3. A képernyőn megjelenő lépések végrehajtása.
4. Rosszindulatú alkalmazás eltávolítása.
5. A képernyőn megjelenő lépések végrehajtásával vonja vissza az alapértelmezett indítóválasztást.
6. FluBot Malware Uninstall alkalmazás eltávolítása.
7. Amennyiben a „FluBot Malware Uninstall” alkalmazás segítségével a fertőzés nem szűntethető meg, abban az esetben:
   a. A készüléken tárolt adatokról (pl. fényképek, kapcsolati adatok, stb.) biztonsági mentés készítése.
   b. A készülék gyári beállításokra történő visszaállítása javasolt.

FluBot Malware Uninstall alkalmazás működését az NBSZ NKI munkatársai 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