TLP:WHITE
Szabadon terjeszthető!

Rendkívüli tájékoztató a Microsoft Defender által generált fals-pozitív riasztásokkal kapcsolatban

(2021. december 01.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) **rendkívüli tájékoztatót** ad ki a Microsoft Defender által generált **fals-pozitív** jelzésekkel kapcsolatban.

Nemzetközi szaksajtóban megjelent információk alapján a **Microsoft Defender 1.353.1874.0** verziója **minden** Office dokumentum megnyitása esetén *Emotet* fertőzés jelenlétét jelzi, és megakadályozza a fájl megnyitását. A jelzés *Win32/PowEmotet.SB* vagy *Win32/PowEmotet.SC* malware fertőzést mutat.

A Microsoft oldalán elérhető a javított vírusdefiníciós adatbázis.

A fenti vírusvédelmi rendszer által generált *Emotet* jelzések kapcsán az NBSZ NKI azt javasolja, hogy ellenőrizzék le a vírusdefiníciós adatbázis verziószámát, és amennyiben az nem a legfrissebb, úgy az kerüljön telepítésre.

Amennyiben a riasztás **ezt követően** is fennáll, javasoljuk az érintett munkaállomás leválasztását a helyi hálózatról, és alapos átvizsgálását.

Hivatkozások:

- https://www.bleepingcomputer.com/news/microsoft/microsoft-defender-scares-admins-with-emotet-false-positives/
- https://borncity.com/win/2021/12/01/microsoft-defender-version-1-353-1874-0-meldet-flschlich-trickbot-emotet/

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