TLP: WHITE
Szabadon terjeszthető!

Riasztás
megnövekedett Emotet aktivitás kapcsán

(2020. augusztus 19.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet riasztást ad ki a megnövekedett, Emotet malware-hez köthető káros tevékenység kapcsán. Az Emotet-hez köthető támadások jellemzően emailben terjesztett SPAM levelekkel kezdődnek. Az elmúlt időszakban több alkalommal jelentek meg sajtóhírek arra vonatkozóan, hogy az Emotet-hez köthető C2 és botnet hálózat felszámolása folyamatban van, ennek ellenére a hálózat továbbra is aktív, külföldi partnereink részéről is több jelzés érkezett a malware által okozott támadások kapcsán. Javasolt a kapcsolódó hálózathoz köthető indikátorok változásainak folyamatos nyomonkövetése.

Fentiekre tekintettel a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) javasolja legalább az alábbi alapvető intézkedések megtételét.

- A felhasználók tudatosságának növelése, különös tekintettel az adathalász célú levelekkel kapcsolatban. Amennyiben a felhasználók valamelyike az elmúlt időszakban nyitott meg gyanús hivatkozást, levél csatolmányt, azt haladéktalanul jelezze az üzemeltetésnek, illetve az informatikai biztonsági felelősnek.
- A felhasználók figyelmének felhívása arra, hogy egyes levelek csatolmányként tartalmazhatnak olyan futtatható állományokat, amelyek egyéb dokumentumnak vannak álcázva (pl. „dokumentum.pdf.exe”, „tajekoztato.txt.exe”).
- Amennyiben lehetséges az aktív tartalmak és makrók központi kezelésének beállítása, tiltása, különösen a .doc és .docx és más MS Office dokumentumok esetében.
- A távoli hozzáférési lehetőségek és a nyitott portok felülvizsgálata, a szükségtelen portok bezárása, a szükséges portok fokozott felügyelete.
- Rendszeres offline biztonsági mentés (szalagos egység, külső merevlemez) készítése.
- Határvédelmi szoftverek frissítése és a hivatkozásokban szereplő indikátorok védelmi eszközökön történő beállítása

A malware-hez köthető indikátorok folyamatosan bővülő listája a https://paste.cryptolaemus.com/ oldalon található.

További hivatkozások:

- https://nki.gov.hu/figyelmeztetesek/karos-kod/emotet-malware-leiras/
- https://www.heise.de/security/artikel/Emotet-Trickbot-Ryuk-ein-explosiver-Malware-Cocktail-4573848.html
- https://paste.cryptolaemus.com/emotet/2020/08/17/emotet-malware-IoCs_08-17-20.html

Nemzetbiztonsági Szakszolgálat
Nemzeti Kibervédelmi Intézet
Telefon: +36-1-336-4833
Fax: +36-1-336-4886
Incidensbejelentés: csirt@nki.gov.hu