TLP:WHITE
Szabadon terjeszthető!

Tájékoztatás
Emotet malware ismételt felbukkanásával összefüggésben

(2021. november 22.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) **tájékoztató**t ad ki az **Emotet malware új variánsával kapcsolatban.**

A jelenleg rendelkezésre álló információk alapján a terjesztés ezúttal is **Word/Excel**, illetve **jelszóvédett Word** állományok útján történik.

Ahol felmerül a fertőzés gyanúja, ott az NBSZ NKI az alábbi intézkedések megtételét javasolja:

- a különböző online szolgáltatásokhoz tartozó, a számítógépre mentett belépési adatok azonnali megváltoztatása (jelszó csere, többfaktoros azonosítás engedélyezése).
- a fertőzött munkaállomások izolálása, szükség esetén javasolt az érintett infrastruktúra teljes ellenőrzése,
- az érintett e-mail fiókok esetében a fiókok felfüggesztése, valamint a jelszavak soron kívüli megváltoztatása, továbbá a kapcsolódó tevékenységnaplók vizsgálata.

Általános, kockázatcsökkentő javaslatok:

- **A felhasználók rendszeres képzése és tudatosítása, kiemelve, hogy milyen intézkedési kötelezettségük van, amennyiben gyanúsnak ítélt üzenettel találkoznak.**
- **A felhasználók figyelmének felhívása arra, hogy egyes levelek csatolmányként tartalmazhatnak olyan futtatható állományokat, amelyek más dokumentumnak vannak álcázva (pl. „dokumentum.pdf.exe”, „tajekoztato.txt.exe”).**
- Amennyiben lehetséges, a többfaktoros (MFA/2FA) bejelentkezés engedélyezése az alkalmazott levelezőrendszeren.
- Hosszú és összetett jelszavak használata, amelyek tartalmaznak kis- és nagybetűt, számot, speciális karaktert.
- Jelszavak rendszeres időközönkénti cseréje, továbbá eltérő szolgáltatásokhoz javasolt eltérő jelszavak alkalmazása.
- 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 nyitott portok felülvizsgálata, a szükségtelen portok bezárása, a szükséges portok fokozott felügyelete, szűrése.
- Rendszeres offline biztonsági mentés (szalagos egység, külső merevlemez) készítése.
- **Bármely, az Önök intézményét érintő informatikai biztonsági incidens vonatkozásában – figyelemmel az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 13§ (3) pontjára – az NBSZ NKI haladéktalan tájékoztatása.**

Hivatkozások:

- https://isc.sans.edu/forums/diary/Emotet+Returns/28044/
- https://urlhaus.abuse.ch/browse/tag/emotet/
- https://www.bleepingcomputer.com/news/security/emotet-malware-is-back-and-rebuilding-its-botnet-via-trickbot/
- https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-megnovekedett-emotet-aktivitas-kapcsan/
- https://nki.gov.hu/figyelmeztetesek/riasztas/ismetelt-riasztas-megnovekedett-emotet-aktivitas-kapcsan/
- https://nki.gov.hu/figyelmeztetesek/karos-kod/emotet-malware-leiras/

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