Riasztás Emotet malware-rel kapcsolatban

(2021. február 12.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) **riasztás**t ad ki **Emotet malware[1] fertőzéssel kapcsolatban** folytatott vizsgálata és nemzetközi partnerektől érkezett jelzések alapján, melynek során **különböző szolgáltatásokhoz kapcsolódó felhasználói fiókok belépési adataink kompromittálódása merült fel**. Az NBSZ NKI eddigi ismeretei szerint a kompromittálódás a kliens oldalon történt fertőződés eredménye, nem az online szolgáltatást nyújtó kiszolgáló infrastruktúrából kerülhettek ki a bejelentkezési adatok.

Az Emotet egy fejlett, moduláris banki trójai, amely elsősorban banki szektort célzó kártevők terjesztőjeként vált ismertté. Károkozás tekintetében az Emotet malware továbbra is napjaink egyik legköltségesebb és legpusztítóbb kártevői közé tartozik, amely a pénzügyi szektoron túl immár kormányzati- és magánszektort egyaránt céloz. Alapképességeit tekintve elsősorban banki adatok lopására szakosodott, ugyanakkor az újabb változatai – a különböző letölthető modulok révén – szinte bármilyen más káros tevékenységre alkalmasak (pl. személyes adatok ellopása vagy zsarolóvírus telepítése).

Az Emotet malware kapcsán az NBSZ NKI folyamatosan figyelemmel kíséri a nemzetközi szakmai sajtóban és fórumokon megjelenő, valamint partnerszolgálatoktól származó információkat, melyek elemzését követően több alkalommal is közzétett a fertőzéshez kapcsolódó riasztást és káros kód leírást honlapján.

Az esetleges Emotet fertőzés kiszűrésére az NBSZ NKI javasolja az Emocheck alkalmazás használatát, amely elérhető a https://github.com/JPCERTCC/EmoCheck/releases oldalon letöltve. Fontos, hogy a fenti alkalmazás csak az Emotet fertőzés felismerésére alkalmas, a további letöltött káros kódokat nem ismeri fel!

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,

[1] •https://nki.gov.hu/figyelmeztetesek/karos-kod/emotet-malware-leiras/

- az érintett e-mail fiókok esetében az érintett fiók felfüggesztése, valamint a jelszó soron kívüli megváltoztatása, továbbá a fiókhoz kapcsolódó tevékenységnapló vizsgálata.

Általános, kockázatcsökkentő javaslatok:

- **A felhasználók rendszeres képzése és tudatosítása, kiemelve, hogy milyen intézkedési kötelezettségük van, amennyiben gyanúsnak ítélt e-mail üzenettel találkoznak.**
- **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 a több faktoros (MFA/2FA) bejelentkezés engedélyezése a levelezőrendszerben.
- Hosszú és összetett jelszavak használata, amelyek tartalmaznak kis- és nagybetűt, számot, speciális karaktert.
- Jelszavak rendszeres időközönkénti ciklikus 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 a 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.**

Kapcsolódó hivatkozások

- https://nki.gov.hu/wp-content/uploads/2020/04/Riasztas_nyitott_RDP_port_v3.pdf
- https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-megnovekedett-emotet-aktivitas-kapcsan/
- https://nki.gov.hu/figyelmeztetesek/riasztas/ismetelt-riasztas-megnovekedett-emotet-aktivitas-kapcsan/

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