TLP: WHITE
szabadon terjeszthető!

Riasztás

egészségügyi intézményeket érintő Emotet terjesztési kampánnyal kapcsolatban

(2020. szeptember 23.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) riasztást ad ki Emotet malware fertőzéssel kapcsolatban folytatott vizsgálata alapján, melynek során több **egészségügyi intézmény** infrastruktúrájának érintettsége merült fel.

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.

Fentiekre tekintettel az NBSZ NKI az alábbi intézkedések megtételét javasolja:

- a határvédelmi rendszer szoftverének frissítése,
- a felhasználók tudatosságának növelése, különös tekintettel a **jelen kampányban használt levelekkel kapcsolatos tudnivalók**ra:
  - **az Állami Egészségügyi Ellátó Központ, illetve a Szabolcs-Szatmár-Bereg Megyei Kórházak és Egyetemi Oktatókórház nevében kerülnek kiküldésre az e-mailek,**
  - **a levelek tárgyában és a csatolmányokban jellemzően a COVID-19 járvánnyal kapcsolatos teendőkre hivatkoznak,**
  - **a levéltörzsben valódinak tűnő, korábbi levelezésre való hivatkozással próbálják meg elérni a csatolmány megnyitását,**
  - **több esetben előfordult, hogy az inkriminált e-mail több különböző formátumú csatolmányt is tartalmazott,**
  - **a levelek aláírásmezőjének tartalma szintén teljesen valósághű,**

- amennyiben a felhasználók valamelyike az elmúlt időszakban nyitott meg gyanús hivatkozást, levél csatolmányt, azt haladéktalanul jelezze az üzemeltetésnek, illetve az informatikai biztonsági felelősnek
- fertőzés gyanúja esetén izolálják a hálózattól a fertőzött munkaállomásokat, szükség esetén javasolt az érintett infrastruktúra teljes ellenőrzése,
- 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.**

Hivatkozások

- https://nki.gov.hu/figyelmeztetesek/karos-kod/emotet-malware-leiras/
- 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