TLP: WHITE
Szabadon terjeszthető!

Riasztás
megnövekedett Emotet aktivitás kapcsán

(2020. augusztus 31.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) **ismételt riasztást** ad ki a megnövekedett, Emotet malwarehez köthető káros tevékenység kapcsán.
A korábban kiadott riasztásunkat követően több magyarországi e-mail fiók kompromittálódott, azokról az Emotet malware oly módon került terjesztésre, hogy a megfertőzött e-mail fiók kapcsolati listájára SPAM levelek formájában az Emotet malware által generált üzenetek kerültek továbbküldésre, melyek jellemzően káros csatolmányt is tartalmaztak.
A rendelkezésünkre álló adatok alapján a mostani kampányban angol nyelvű levelek kerültek kiküldésre, amelyek jellemzően DOC kiterjesztésű csatolmányt tartalmaznak. Néhány elszórt esetben a csatolmány tömörített állományként (ZIP kiterjesztéssel) került kiküldésre.
Tekintettel arra, hogy a káros tevékenységhez köthető indikátorok dinamikusan változnak, az NBSZ NKI javasolja ezen változások nyomonkövetését, és a biztonsági rendszerekbe történő illesztését.

Fentiekre tekintettel az 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 beérkezett csatolmányokat a Virustotal oldalra feltöltve ellenőrizzék. Amennyiben a csatolmány vélhetően bizalmas, illetve személyes- vagy üzleti adatokat tartalmazhat, úgy ennek feltöltését Intézetünk nem javasolja! Ilyen esetekben javasolt más csatornán (pl.: telefon) felvenni a kapcsolatot az e-mail küldőjével és ellenőrizni a levél hitelességét.
- 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 kiterjesztésű fájlok, 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

Amennyiben gyanús e-mail érkezik az Önök felügyelete alatt álló e-mail fiókokba, kérjük, ellenőrzés céljából továbbítsák azt Intézetünk részére. Ebben segítséget nyújthat az alábbi linken elérhető új incidensbejelentő modul letöltése, illetve használata.

Jelen kampányhoz kötődő indikátorok:

SHA-256:

8bb634c8040c0dbdc8103c0bf90ca21e4ff6d65b9f63ed5a317b6e676ed0c7c5 (pack85389.doc)

f71f3f1581388613e005c5ec8d8fb3fad1a68cf6c59069f1fb1e9f80f040a8ed

(Complaint_Copy_140921134.zip)

Domain:

duhallow[.]com, alaksir[.]com, classic-recipes[.]com, duncanllc[.]com, dishnchips[.]com, huanuoav[.]com

IP:

179.60.229[.]168

132.148.215[.]84

A malwarehez köthető további indikátorok folyamatosan bővülő listája a https://paste.cryptolaemus.com/ oldalon található.

További hivatkozások:

- https://nki.gov.hu/figyelmeztetesek/karos-kod/emotet-malware-leiras/
- https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-megnovekedett-emotet-aktivitas-kapcsan/
- https://www.heise.de/security/artikel/Emotet-Trickbot-Ryuk-ein-explosiver-Malware-Cocktail-4573848.html

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