Nemzeti Kibervédelmi Intézet
Kormányzati Eseménykezelő Központ

Ikt. sz.: 30700/0/25680-4/2016

TLP:WHITE
Szabadon terjeszthető!

Tájékoztató hírlevél zsaroló kártevő kampányról
(2016.08.19)

Tisztelt Ügyfelünk!

A Kormányzati Eseménykezelő Központ tájékoztatást ad ki az elmúlt időszakban tapasztalt **új Locky ransomware (zsaroló kártevő) variáns hazai terjedése** miatt.

A káros kód **elektronikus levél segítségével** terjed, amely **mellékletként** tartalmaz egy **tömörített állományt** (*zip/rar)* vagy egy *.docm* kiterjesztésű makrókat is tartalmazó dokumentumot. Amennyiben ez megnyitásra kerül és a káros kód sikeresen lefut, egy távoli szerverről letöltődő tényleges ransomware kód **titkosítja a dokumentumokat és más fájlokat a helyi és hálózati mappákban**.

Az e-mailekkel kapcsolatban jelenleg az alábbi információk állnak rendelkezésre:

- Feladó: az áldozatot **megtévesztendő** rendszerint **valós személy** vagy **intézmény** nevével visszaélve, akár a címzett lehetséges ügyfélkörének megfelelően.
- Az e-mail tárgya lehet pl.: *"Documents Requested", "New Doc XX-XX", "Emailing-XXXX", "Message from"CUKPRXXXXXXX"* (ahol az X számot jelöl).
- A levél törzsszövegében vélhetően nem tartalmaz megszólítást.
- Az e-mail mellékletének neve lehet pl.: *„YYYYmmddHHMM.zip”* (ahol a betűk az aktuális évet, hónapot, napot, órát és percet jelölik).

Az ilyen és ehhez hasonló **e-mailek** és azok mellékleteinek megnyitása mindig **veszélyeket hordozhat magában**, ezért a fertőzések megelőzése érdekében javasoljuk:

- Erősítse a **felhasználói tudatosságot** – Fontolja meg, mielőtt megnyit egy állományt.
- A **felhasználók** - vagy a felhasználók tevékenysége - számára **csak a számukra kijelölt feladatok végrehajtásához szükséges hozzáféréseket engedélyezze**.
- Szigorítsa **a makró futtatási lehetőségeket** az e-mail kliens biztonsági beállításaiban (pl.: Outlook\Beállítások\Adatvédelmi központ beállításai\Makróbeállítások).
- **Készítsen rendszeres biztonsági mentést**.
- **Tárolja** a biztonsági mentéseket **elkülönítve** – Ne csak a hálózati meghajtón.

Javasoljuk, hogy a fenti paramétereknek megfelelő **e-mailt, illetve fájlt semmiképp se nyissák meg**, ha ilyen vagy **ehhez hasonló** e-maillel vagy fájllal találkoznak, haladéktalanul értesítsék a Kormányzati Eseménykezelő Központot. További információt az alábbi hivatkozásokon találhat:

- http://tech.cert-hungary.hu/tech-blog/150511/zsarolo-kartevok-eltavolitasa
- https://www.fireeye.com/blog/threat-research/2016/08/locky_ransomwaredis.html

Kérjük, továbbítsa a tájékoztatót a háttérintézményei felé.

Kormányzati Eseménykezelő Központ
GovCERT-Hungary
Telefon: +36-1-336-4833
Fax: +36-1-336-4886
Incidensbejelentés: cert@govcert.hu