Nemzeti Kibervédelmi Intézet
Kormányzati Eseménykezelő Központ

Ikt. sz.: 404/A-49/9/2016.

TLP:WHITE
Szabadon terjeszthető!

Tájékoztatás ransomware fertőzés terjedése miatt

(2016.04.14)

Tisztelt Ügyfelünk, a Kormányzati Eseménykezelő Központ tájékoztatást ad ki az elmúlt időszakban tapasztalt **ransomware (zsarolóvírus) terjedése** miatt.

A káros kód **elektronikus levél segítségével vagy kártékony kódot tartalmazó web oldal** útján terjed. A kéretlen levél tartalmaz egy mellékletet, egy **tömörített állományt.** Amennyiben a zip/rar fájl megnyitásra kerül, és a káros kód sikeresen lefut, a **ransomware titkosítja a dokumentumokat a helyi és hálózati mappákban**. A titkosítás megszüntetéséhez szükséges kulcsot a támadó ellentételezés átadását követően (pl. bitcoin) ígéri, egyes kártevők esetében ismert alternatív módszer (pl. Petya).

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: **reference number #(véletlenszerű nyolc jegyű szám), last payment notice, innvoice, fax, account, notice**
- Az e-mail mellékletének neve lehet: **copy_invoice_(véletlenszerű nyolc jegyű szám)**

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

- erősítse a **felhasználói tudatosságot** – Fontolja meg, mielőtt megnyit egy állományt!
- korlátozza felhasználói **jogosultságokat** – Felhasználó ne legyen rendszergazda!
- **készítsen rendszeres biztonsági mentést**
- **tárolja** a biztonsági mentéseket **elkülönítve** – Ne tárolja 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 információ: http://tech.cert-hungary.hu/tech-blog/150511/zsarolo-kartevok-eltavolitasa

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