Tárgy: figyelemfelhívó tájékoztatás és gyakorlati „túlélési” tippek zsarolóvírus fenyegetéssel kapcsolatban

Készítette: dr. Varga Balázs információbiztonsági megbízott, RITEK Zrt.

Utolsó frissítés: 2017. június 6.

2017. májusában világméretű fertőzést és súlyos károkat okozott az ún. zsarolóvírusok családjába tartozó „WannaCry” elnevezésű kártékony program. Sajnos nem zárható ki, hogy a jövőben más alkalommal is előforduljon ilyen méretű vírusfertőzés.

A RITEK Zrt. a felhasználók tudatosítása, illetve kármegelőzés céljából készítette el jelen gyakorlati tippeket is tartalmazó, figyelemfelhívó tájékoztatóját, amelyet most díjmentesen közread.

1) Miért érdemes elolvasnom ezt a tájékoztatót?

Egy fertőzött e-mail melléklet, vagy az e-mailben szereplő link megnyitásával az adott számítógépen lévő összes dokumentum titkosításra kerülhet. Ily módon **akár hónapok munkája is elveszhet! A titkosítás feloldásának váltságdíja a 100.000 Ft-ot is meghaladhatja** (és a megvásárolt dekódolókulcs nem is minden esetben működik) **!** Tehát **a kár súlyos adatvesztés, illetve jelentős anyagi veszteség is lehet.**

2) Mi az a zsarolóvírus?

Olyan kártékony alkalmazás, amely legtöbbször e-mailek mellékletében vagy e-mailben szereplő link megnyitásával terjed. A levélben szereplő fertőzött melléklet, illetve link megnyitásával a kártékony alkalmazás aktiválódik és titkosítja a felhasználó számítógépén (meghajtóin) lévő összes fájlt! A titkosított fájlok visszaállítását pedig „váltságdíj” megfizetéséhez köti.

3) Hogyan lehet védekezni a zsarolóvírusokkal szemben?

- **Legyünk fokozottan körültekintőek az e-mail csatolmányok megnyitásakor! Különösen, ha külföldi vagy ismeretlen feladótól kaptunk levelet.** Ha már a feladó nevéből, vagy a tárgyból egyértelműen látszik, hogy ez egy kéretlen levél/hamis levél, akkor helyezzük a levelező program SPAM mappájába, vagy töröljük ki elolvasás nélkül. **Ha véletlen rákattintottunk a kéretlen/hamis levélre akkor még nincs baj, de a levél mellékletét, vagy a levélben szereplő linket semmiképpen se nyissuk meg.**

- **Az e-mailek futtatható mellékletét** (*.exe, *.com, *.jar, stb.) **NE nyissuk meg.** Tömörített fájl melléklet (*.zip, stb.) megnyitásakor legyünk nagyon körültekintőek! (ha lehetséges inkább hívjuk fel a feladót, hogy valóban ő küldte-e a levelet)
- A Windows operációs rendszerünk naprakészen tartalmazzon minden biztonsági frissítést. Legyen telepítve a számítógépre naprakész vírusvédelmi rendszer. (ezen feladatok elvégzéséről általában az adott szervezet informatikus kollégái gondoskodnak)
- **Csak megbízható weboldalakat látogassunk.** (Például a legújabb mozifilmeket, sorozatokat ingyenesen megtekintésre kínáló, vagy az egyébként fizetős szoftverek ingyenes letöltését kínáló weboldalak sokszor nem megbízhatóak, kivéve azon oldalakat, amelyek ezeket a szolgáltatásokat jogszerűen, díjfizetés ellenében nyújtják.)
- Ne kattintsunk olyan online hirdetésekre, amelyek irreális dolgokat, „fűt-fát” ígérnek. A józan, mérlegelő gondolkodással sok pénzt és időt takaríthatunk meg magunknak.
- **Ha egy fájl makró futtatását kéri, azt NE engedélyezzük!** Jellemzően Word (*.doc, *docx), vagy Excel (*.xls, *.xlsx) fájlok megnyitásakor fordulhat elő ilyen kérés.
- **HÓNAPOK MUNKÁJA VESZHET EL, HA NEM KÉSZÍTÜNK BIZTONSÁGI MENTÉST!** Minden olyan dokumentumról készítsünk rendszeres biztonsági mentést, amelynek az elvesztése „érzékenyen” érintene minket, vagy munkáltatónkat. A biztonsági mentés készítésének módjáról, feltételeiről a szervezet informatikai biztonsági ~, illetve mentési szabályzatában találhatunk információt, vagy kérdezzük meg az illetékes informatikus kollégákat. **A leggyakoribb biztonsági mentési módok**: hálózati mappába, külső adathordozóra (külső merevlemez, pendrive), CD/DVD-re mentés. Amennyiben külső adathordozóra mentünk, ne felejtsük el a biztonsági mentés elkészítését követően először szabályosan leválasztani a meghajtót a megfelelő Windows ikon segítségével, majd fizikailag is kihúzni az adathordozó USB adatkábelét a számítógépből (ha a külső meghajtó folyamatosan csatlakoztatva van a számítógéphez, ugyanúgy lekódolja egy vírus a tartalmát, mint a belső meghajtókét).
- **Ha bizonytalanok vagyunk, hogy az adott levél kéretlen/hamis levél-e, inkább várjunk és kérdezzünk** meg egy informatikus kollégát, vagy hívjuk fel a feladót, ha ez lehetséges…

4) **Hogyan tudom eldönteni, hogy kéretlen/hamis az adott e-mail?**

Az alábbiak észlelése esetén legyünk fokozottan óvatosak!

- Az e-mail feladója külföldi, illetve az e-mailt idegen nyelven írták, de a munkáltatónk csak belföldi ügyfelekkel, partnerekkel van kapcsolatban.
- **Gyanús a feladó e-mail címe:** például: zshul@centrum.sk, conpjock@scglobal.net; lay-naleno@cprrq.net; jeffersckai.wadel@plusminus.bg, stb.
- **Az e-mail szövege fogalmazási, ragozási hibáktól hemzseg.**
- Az e-mail szövege akár hihetőnek tűnik, de a szöveg megfogalmazása, a grafikai, design elemek, stb. miatt **olyan érzésünk van, hogy valami nem „stimmel" ezzel a levéllel.**
- Ismerőseink számítógépe is megfertőződhet, így **adott esetben ismerőseink e-mail címéről is érkezhet postafiókunkba fertőzött e-mail!** Tehát: amennyiben ismerőseinktől kaptunk gyanús tartalmú e-mailt, inkább hívjuk fel őket, mielőtt megnyitnánk a levél mellékletét, vagy az abban szereplő linket.
- Az adott szolgáltatóval már egy ideje kapcsolatban állunk (bank, csomagküldő cég, webshop, bármilyen szolgáltató cég), **de az adott levél nagyon eltérő az eddig megszokottól** (pl.: fogalmazási hibák, nem szokványos tartalom, nem megszokott grafikai elemek).

5) **Milyen trükkökkel próbálják meg megtéveszteni a gyanútlan felhasználót? Konkrét példák.**

Legyünk nagyon körültekintőek, ha a következők közül bármelyiket tapasztaljuk. (a felsorolás nem teljeskörű) Olyan e-mailt kapunk, amelyben

- arra hívják fel a figyelmünket, hogy csomagunk érkezett (közismert szállítócég adatai, logója simán ott lehet a hamis levélben!), s a szállítási információk a csatolt mellékletben találhatóak,
- értesítenek, hogy valamilyen probléma (zárolás, tárhely túllépése, stb.) merült fel a Paypal, Gmail, stb. fiókunkkal kapcsolatosan és kattintsunk a levélben szereplő linkre, illetve nyissuk meg a levél mellékletét,
- egy telekommunikációs cég (de bármilyen más szolgáltató is lehet) értesít minket, hogy lejárt tartozásunk van, bővebb információért nyissuk meg a csatolt mellékletet.
- Bankunk számlakivonatot küldött e-mailben (de mi nem is kértünk ilyen szolgáltatást a banktól).
- Értesítést kapunk, hogy faxunk érkezett, amelyet a levél melléklete tartalmaz.

- Az adott szolgáltatótól számlát/levelet kapunk *.doc, *docx, stb. fájlban. A dokumentum megnyitása után csak értelmezhetetlen karakterek jelennek meg a szövegfájlban. Az e-mailben azonban tájékoztattak minket, hogy engedélyezzük a makrók futtatását a csatolt fájl megnyitásakor, s akkor majd helyesen megjelenik a tartalom. De ez is csak egy trükk, mert a makró engedélyezésével lefutna a vírus és titkosítaná az adatainkat!

Jogi nyilatkozat