CTI jelentés

Mit tegyünk, ha zsarolóvírus támadás ér bennünket?

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT 1996

NEMZETI KIBERVÉDELMI INTÉZET

Bevezetés

A zsarolóvírus támadások száma az elmúlt években világszerte növekedett, hétről hétre egyre újabb és hihetőbb, "sikeresebb" **zsarolóvírusokkal összefüggő technikákkal** állnak elő a támadók.

Jelen dokumentum összefoglalja a legfőbb tudnivalókat a zsarolóvírusokkal kapcsolatban, **hogyan lehet elkerülni** a zsarolóvírus okozta **következményeket**, illetve hogy, **mit tegyünk** ha már bekövetkezett.

Tartalomjegyzék

Mit a zsarolóvírus (ransomware)?

A zsarolóvírus olyan **rosszindulatú program**, amely a **felhasználók adatait** azzal a céllal **titkosítja**, hogy később csak a **váltságdíj ellenében** lehessen **visszaállítani** azokat.

Az ilyen típusú károkozó néhány főbb jellemzője, hogy:

- titkosítja az állományokat,
- zsaroló üzenetet jelenít meg,
- határidőt szab a váltságdíj kifizetésére,
- törli az állományok egy részét,
- az idő múlásával egyre több állományt tesz végleg visszaállíthatatlanná.

Szélsőséges esetekben a megfelelő működéshez nélkülözhetetlen rendszerfájlok titkosítása révén az informatikai **rendszerhez való hozzáférést is blokkolja**. Tekintettel a vírus **pusztító jellegére**, gyakran nehéz helyreállítani a naplófájlokat, és megtudni, hogy valójában mi történt. A hackerek szellemi tulajdon, valamint személyes adatok ellopása esetén is használhatnak zsarolóvírust, hogy valódi szándékaik rejtve maradjanak.

Kétféle zsarolóvírus létezik: Az egyik a **számítógépet zárolja** és **megakadályozza az ahhoz való hozzáférést**, a másik pedig a fertőzött rendszeren lévő **állományokat titkosítja**. A zsarolóvírusok fejlettebb változatai nem csak a helyi IT rendszereket képesek titkosítani, hanem a merevlemezeket, adatbázisokat, USB adathordozókat és a felhőben lévő adatokat is. Az áldozatnak mindkét típusú zsarolóvírus esetében váltságdíjat kell fizetnie, hogy ismét normálisan használhassa a számítógépét. A támadók ezt a **váltságdíjat gyakran kriptovaluta formájában** (például Bitcoin) követelik. A zsarolóvírus fertőzések alig különböznek a többi rosszindulatú program fertőzésétől. Ezen felül az intézkedések is, amelyeket egy szervezet megtehet a zsarolóvírusok ellen, nagyjából ugyanazok. A szervezet fejlettségétől függően a zsarolóvírus támadás hatása nagy skálán mozoghat, az egyszerű bosszankodástól egészen a szervezet folyamatainak leállásáig.

Hogyan kerülhet zsarolóvírus az eszközeinkre?

Eszközeink több féle módon is megfertőződhetnek, itt a leggyakoribb technikákat olvashatjuk. Az, hogy az adott zsarolóvírus épp melyik technikát/technikákat használja, a vírus készítőjén múlik.

E-mail üzenetben érkezik csatolmányként, gyakran valamilyen közmű szolgáltató, bank, stb... design elemeivel együtt. Ebben az esetben a támadók arra törekednek, hogy minél valósághűbben, hihetőbben legyen elkészítve az adott elektronikus levél.

Hirdetésekre, **idegen linkekre kattintva** is kerülhet zsarolóvírus a gépünkre. Itt általánosan elmondható, hogy a készítők valamilyen figyelemfelkeltő, szinte hihetetlennek tűnő téma köré "csomagolják" az adott linket, céljuk, hogy minél többen kattintsanak rá.

Fertőzött weboldalról települ eszközünkre a vírus. A fertőzött weboldalak összefüggésben lehetnek a fentebb említett hirdetések és idegen linkekkel kapcsolatban. Előfordulhat, hogy ezekre kattintás után fertőzött weboldalra jutunk. Szintén elmondató, hogy ezek a weboldalak figyelemfelkeltő céllal lettek létrehozva. Csak megbízható oldalakat látogassunk meg, ha kell keressünk rá fórumokon, hogy az adott oldal megbízható-e vagy sem.

Nem eredeti, megbízható forrásból telepítünk programokat az eszközre. Érdemes figyelni a különböző szoftvergyűjtő oldalakra, illetve hasonlóan az e-mail esetében, a támadók akár valamilyen népszerűbb szoftver weboldalát is lemásolhatják, így jutattva a kártékony programot gépünkre. Mindig győződjünk meg a szoftverek telepítésekor, hogy az eredeti és hiteles weblapot használjuk.

Gyengén védett távoli asztali kapcsolaton keresztül (RDP) is lehetőségük van a bűnözőknek kártékony programokat telepíteni, a legtöbbször tudtunk nékül. RDP kapcsolatoknál mindig erős jelszót használjunk, ez még inkább kritikus az adminisztrációs jogokkal rendelkező felhasználói fiókok esetében.

A számítógépünkön található **sérülékenység kihasználása**. Előfordulhat, hogy a legális és jó forrásból letölött szoftverünkben egy ún. hátsó kapu (backdoor) található. Ilyen esetben a hátsó kapu létezése az adott szoftver fejlesztőjének a felelőssége, mindennapi felhasználóként alacsony eséllyel vessük észre. Érdemes figyelemmel kísérni a napi IT biztonsági cikekket, ezekből még akár a baj bekövetkezése előtt értesülhetünk a hibáról és intézkedhetünk.

A zsarolóvírusok esetében elmondható, hogy általánosságban az emberi gyengeséget, **hiszékenységet** vagy **jóindulatot használja ki**. Minden esetben **győződjünk meg** az adott **e-mail vagy weboldal valódiságáról**, tájékozódjunk egy számunkra ismeretlen szoftver telepítése előtt a többi felhasználó tapasztalatából!

Az alábbi képeken néhány hírhedtebb zsarolóvírus "felületét" szeretnénk bemutatni. Ilyen és hasonló zárolási ablakokkal találkozhat a felhasználó, amennyiben eszköze megfertőződik az említett kártevővel.

1. ábra: a Wannacry és Notpetya zsarolóvírusok ransom note-jai.

Mit tehetünk, ha már bekövetkezett a legrosszabb?

Ha minden igyekezetünk ellenére a titkosított állományaink vagy a jellegzetes zsarolóvírusoknál előforduló zárolási ablak fogad minket, a következő tanácsok segíthetnek minket a helyzet megfelelő és szakszerű kezelésében.

Mielőbb **válasszuk le az adott eszközt a hálózatról**, a legtöbb zsarolóvírus képes hálózaton belül terjedni, így érdemes minél hamarabb megszünteni ennek lehetőségét a hálózaton megtalálható többi eszköz épségének megőrzése érdekében.

A hálózaton **állítsuk le a kifelé nyitott szolgáltatásokat** és a belső fájlmegosztást is!

A fertőzött munkaállomás(ok)on a **meghajtó teljes formázása javasolt**. Csak a teljes operációs rendszer újratelepítése, valamint az aktív vírusvédelem bekapcsolása után lehet az adatokat az archív mentésekből helyreállítani.

Hordozható adattárolót (pendrive, külső merevlemez) **sem ajánlott csatlakoztatni**, hiszen ezzel a fertőzést tovább lehet vinni egy másik számítógépre.

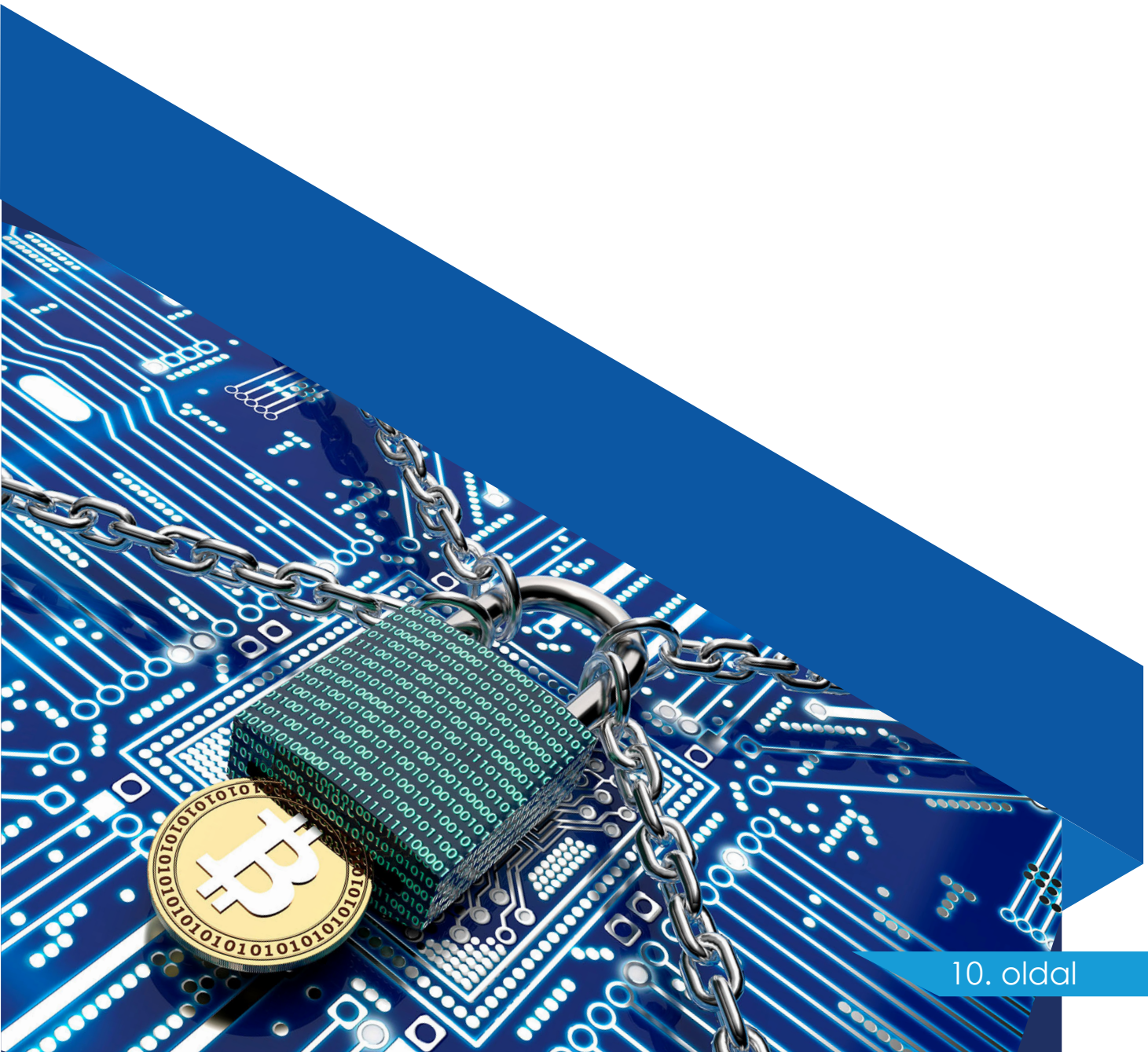
Az incidens felderítése után gondoskodjunk a **megfelelő (ellen)intézkedésekről**, illetve próbáljuk meg kideríteni, hogy milyen szoftver, weblap vagy szolgáltatás okozhatta a kellemetlenségeket. Ez nagy segítség lehet a kibertámadások visszaszorításában, illetve a jövőbeni ilyen jellegű bosszúságok elkerülésében.

Ne fizessünk váltságdíjat! Nincs rá garancia, hogy kapunk kódot a visszaállításhoz, és hogy az működőképes is lesz. Sok esetben szándékosan – vagy programozói hibából kifolyólag – eleve lehetetlenné teszik a visszafejtést.

A későbbi visszafejtés reményében célszerű a **titkosított állományok megőrzése**. Ebben nyújthat hatékony segítséget a **CryptoSearch** nevű, Michael Gillespie biztonsági kutató által Windows platformra készített **ingyenes program**, amely egy folyamatosan frissülő online adatbázist használva (ID Ransomware) jelenleg kb. 240 variáns felismerésével képes automatikusan detektálni a titkosított fájlokat és róluk egy, a felhasználó által választott meghajtóra – az eredeti könyvtárszerkezet megtartásával – mentést készíteni.

Mindenképp tüzetesen **ellenőrizzük a titkosított állományok állapotát**, akár külső szakértő segítségével. A zsarolóvírus programok egy részénél előfordulhat, hogy csak a fertőzött eszköz felhasználójára szeretne ráijeszteni, illetve pénzt szerezni, azonban a fájlokban érdemi kár nem keletkezik.

Telefonok, mobileszközök esetében **kikapcsolás után távolítsuk el a SIM-kártyákat**, **memóriakártyákat**, illetve **egyéb csatlakoztatható adattároló** eszközöket!



Hogyan lehet megelőzni egy zsarolóvírus támadást?

Az operációs rendszer, illetve az alkalmazások (Adobe Flash, Java) hibajavításainak rendszeres telepítésén túl mindenképp javasolt valamilyen vírusvédelmi megoldás használata, illetve naprakészen tartása (termékverzió, felismerési adatállományok).

A legfontosabb védelmi intézkedés, amit tehetünk, hogy adatainkról egy elkülönített, és fizikailag is leválasztható meghajtóra **rendszeresen mentéseket készítünk**. (Lásd: 3-2-1 elv alapján, azaz a biztonsági mentésből őrizzünk meg legalább 3 példányt, 2 féle adathordozón, amelyből 1-et tároljunk teljesen offline.)

Fontos a **biztonságtudatos internet használat**: ismeretlen feladótól érkezett e-maileknek **ne nyissuk meg** a mellékletét — főképp ha ez egy tömörített, vagy dupla kiterjesztésű (.doc.exe) állomány — sem az e-mailekben szereplő hivatkozásokat.

Korlátozzuk a mappákhoz való **hozzáférést**!

Egyes **vírusvédelmi megoldások** képesek gyanús viselkedésminták alapján azonosítani és blokkolni a zsaroló kártevőket, ezáltal megelőzni a fertőzést.

- Ismeretlen pendrive-ot, egyéb külső adattároló eszközt ne csatlakoztassunk a számítógéphez.

- Windows operációs rendszer esetében engedélyezzük a Windows Update szolgáltatásban az automatikus frissítés letöltést, illetve telepítést.

- Egyéb szoftverek esetében a beállítások között keressük meg a frissítések automatikus telepítése menüpontot, amennyiben megtalálható ilyen szolgáltatás az adott szoftvernél. Ezzel gondoskodhatunk arról, hogy a gyártó által kiadott legfrissebb hibajavítások és frissítések, a lehető leghamarabb települnek számítógépünkre vagy egyéb eszközünkre.

- Ne használjunk elavult, frissítésekkel már nem rendelkező operációs rendszereket és más egyéb telepíthető szoftvereket.

Érdemes tehát a fentebb említett tanácsokra időt, illetve amennyiben szükséges pénzt fordítani. A megelőzésre fordított pénzösszeg még mindig csak a töredékét fogja kitennni, a zsarolók által követelt kriptovalutának, nem is említve a felesleges bosszúságot és a helyreállítási műveletekre igénybe vett időt.

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36(1)325 7672

Nemzeti Kibervédelmi Intézet

@nki.gov.hu

Kibertámadás!
podcast

2022