# NE ENGEDJ A ZSAROLÁSNAK!

Hogyan lehet védekezni a

# ZSAROLÓVÍRUS TÁMADÁS

ellen?

## MI A ZSAROLÓVÍRUS?


Zsarolóvírus (ransomware) alatt olyan kártékony szoftvert értünk, amelynek célja valamilyen módon „túszul ejteni” a felhasználók informatikai eszközein tárolt adatokat, amelyeket csak váltságdíj megfizetése esetén tesz újra elérhetővé.

## A FERTŐZÉS MÓDJAI

**e-mail üzenetek fertőzött csatolmánya**

**káros weboldalak**

**sérülékenység, hibás konfiguráció, felhasználói mulasztás kihasználása**

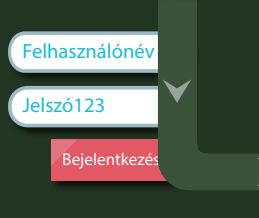

A támadók célja a káros kódok céleszközre történő eljuttatása.


A weboldal megnyitásával automatikusan letöltésre kerülnek a káros kódok (exploit kit).



Általában számláknak és egyéb hivatalos dokumentumoknak álcázott fájlok megnyitására próbálják rávenni az áldozatot.

szamla.exe szamla.pdf




A rendszer egy sérülékenységének, hibás konfigurációjának, vagy gyenge jelszóvédelmének kihasználásával akár admin hozzáférést is képesek szerezni a támadók.

Káros kódok telepítése és futtatása a fertőzött eszközön.

Az áldozatok merevlemezén található fájlok titkosításához, általában asszimetrikus titkosító algoritmusokat használnak.


A titkosítást követően, az áldozat képernyőjén megjelenik egy figyelmeztető üzenet (ransom note), amelyben ismertetik, hogy mi történt a fájlokkal és a felhasználó mekkora összegű váltságdíj ellenében kaphatja vissza az adatokat.

Miután eltávolításra került a káros kód a rendszerből, a legutóbbi biztonsági mentésből állítsuk helyre az adatokat.

Az áldozat nem fizeti ki a váltságdíjat.

Az áldozat kifizeti a váltságdíjat.

A támadó a fizetés ellenére sem biztosítja a visszafejtő kulcsokat, így a felhasználó továbbra sem fér hozzá a fájlokhoz.

A támadó a fizetést követően valóban átadja a dekriptáláshoz szükséges kulcsokat és a felhasználó visszakapja a fájljait.
*Megjegyzendő, hogy ennek bekövetkezése nem valószínű.*

A későbbi visszafejtés reményében érdemes a titkosított állományok megőrzése, ugyanis előfordulhat, hogy a kártevő készítői programozási hibát vétettek, vagy önként nyilvánosságra hozzák a dekriptáláshoz szükséges mester kulcsot.

## HOGYAN VÉDEKEZZÜNK?

### FELHASZNÁLÓ

- Mindig telepítsük a használt szoftverek biztonsági frissítéseit.
- Használjunk védelmi szoftvert és rendszeresen frissítsük annak vírusdefiníciós adatbázisát.
- Rendszeresen készítsünk biztonsági mentéseket, lehetőleg egy elkülönített, fizikailag is leválasztható meghajtóra (pl.: külső winchester), a biztonsági mentéseket érdemes a 3-2-1 elv alapján készíteni.
- Ne nyissuk meg ismeretlen feladótól érkezett e-mail üzenetek mellékleteit, különös tekintettel a tömörített, illetve dupla kiterjesztésű *(.doc.exe)* állományokra.
- Szabályozzuk a mappákhoz való hozzáféréseket.

### RENDSZERGAZDA

- Tervezetten és rendszeresen vizsgáljuk felül a nyitott portokat, a szükségteleneket tegyük elérhetetlenné, a szükségeseket pedig tartsuk fokozott felügyelet alatt, naplózzuk és módosítsuk az alapértelmezett portszámokat.
- Korlátozzuk a gyakori portok internet irányából történő elérését (megadott IP címekről, csak bizonyos felhasználók számára).
- Tiltsuk az üzemeltetéshez használt portok külső hálózatból történő elérését, ehelyett javasolt a VPN kapcsolatok alkalmazása.
- Rendszeresen frissítsük a határvédelmi rendszerek szoftvereit, illetve az eszközök feketelistáit.
- Időszakosan vizsgáljuk felül a felhasználók jogosultságait (szükségtelen felhasználók felfüggesztése, távoli hozzáféréssel rendelkező felhasználók számának minimalizálása.
- Alkalmazzunk szigorú jelszóházirendet, amennyiben lehetséges szorgalmazzuk a kétfaktoros autentikáció használatát.

## HA MÁR MEGTÖRTÉNT A BAJ...

- Mielőbb válasszuk le az adott eszközt a hálózatról.
- 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.

nki.gov.hu
csirt@nki.gov.hu (incidens bejelentés)

1996 NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERVÉDELMI INTÉZET