

Riasztás az interneten terjedő, zsaroló hangvételű levelekkel kapcsolatban

(2022.01.05.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet ismételten riasztást ad ki **az interneten terjedő, magyar nyelvű, zsaroló hangvételű levelekkel** kapcsolatban, azok számossága, valamint az érintett szervezetek és címzetti köre miatt.

Az elmúlt napokban **ismételten megnövekedett** az olyan zsaroló hangvételű levelek száma, amelyek állami és önkormányzati szerveket, közintézményeket és magánszemélyeket céloznak.

A levelek szövegezése alapvetően azonos, a korábbi hasonló zsarolólevelekhez képest koherensebb, helyesírásiilag jóval pontosabb, a hangnem pedig egységesen tegeződő.

Az üzenetek tartalma szerint a címzett készülékét megfertőzték egy trójai vírussal, amelynek segítségével az áldozat informatikai eszközehez hozzáférést szereztek. A támadó azt is állítja az e-mailben, hogy készített egy kompromittáló videó felvételt, amelyet a felhasználó kamerájával rögzített és a felvételen az áldozat **felöltt tartalmú oldalak látogatása közben végzett tevékenysége látható**.

A zsaroló felhívja a levél címzettjének figyelmét arra, hogy amennyiben a kért összegű váltságdíj nem kerül kifizetésre, abban az esetben a kompromittáló felvételt **eljuttatja a címzett ismerőseinek, illetve a közösségi médiában is közzéteszi azt**. A váltságdíjként kért pénzüsszeg változó, jellemzően: 1350 EURO.

A zsaroló leveleket a SPAM szűrők sok esetben nem szűrik ki megfelelően, mivel azok nem tartalmazznak olyan hivatkozást, ami alapján a szűrő felismerné őket. A mostani esetben a levelek tárgya:

„Fizetési felszólítás.”

Az NBSZ NKI javasolja az **ilyen és ehhez hasonló levelek figyelmen kívül hagyását**, továbbá a fenti indikátorok beállítását a SPAM szűrőben.

Példa a szóban forgó zsarolólevélre:

Szia!

Sajnálom, de van egy kis rossz hírem számodra.

Néhány hónappal ezelőtt hozzáférést szereztem azon készülékeidhez, melyekkel az internetet szoktad böngészni.

Azóta folyamatosan nyomon követem az internetes tevékenységeidet.

Az események az alábbi sorrendben történtek:

Korábban számos e-mail fiókhhoz vásároltam hozzáférést hackerektől (manapság ez egy nagyon egyszerű, online elvégezhető feladat).

Ennek köszönhetően, akadály nélkül be tudtam jelentkezni az e-mail fiókodba.

Egy héttel ezután pedig sikerült telepítenem egy trójai vírust az összes olyan készüléked operációs rendszerére, melyeket ezzel az e-mail címmel regisztráltál.

Ami azt illeti, ez roppant egyszerűen ment végbe (mivel te magad kattintottál a beérkező levelekben található linkekre).

TLP:WHITE

Szabadon terjeszthető!

Az okos dolgok valójában nagyon egyszerűek. (^)

A szoftverem lehetővé teszi, hogy hozzáférjek az összes vezérlőhöz az eszközeidben, például a videokamerához, a mikrofonhoz és a billentyűzethez.

Sikerült letöltenem az összes személyes adatodat, valamint a böngészési előzményeidet és a fényképeidet a szervereimre.

Hozzáférésem van az összes üzenetedhez, továbbá az e-mailjeidhez, a közösségi oldalaidhoz, a névjegyzékedhez és még a chat-előzményeidhez is.

A vírusom szüntelenül frissíti az aláírásait (mivel illesztőprogram-alapú), és ezáltal láthatatlan marad a víruskeresőd számára.

Így most már te is értheted, hogy miért maradtam észrevétlen egészen mostanáig ...

Miközben információkat gyűjtöttem rólad, észrevettem, hogy milyen nagy rajongója is vagy a felnőtteknek szóló weboldaloknak.

Nagy élvezettel szoktál pornóoldalakat böngészni és pajzán videók nézegetni, és mindeközben kéjesen szórakoztatod magad.

Rögzítettem néhány bizarr jelenetet rólad, majd összeállítottam belőlük egy videót, ahogy szenvedélyesen orgazmusing maszturbálsz magad.

Ha még ezután is kételkednél szándékom komolyságában, akkor jobb, ha tudod, hogy mindössze néhány egérvégképp képes vagyok megosztani a videót barátainkkal, rokonainkkal és még kollégáinkkal is.

Illetve, az sem jelentene nagy kunsztot, hogy akár teljes nyilvánosságra hozzam azokat a videókat is, amelyekre élvezkedni szoktál.

Őszintén hiszem, hogy nem szeretnéd, hogy mindez megtörténjen, mivel magad is tisztában vagy az általad nézegetett videók különösen perverz mivoltával,

ami valódi katasztrófát jelentene számodra, ha kitudódna.

Javaslom, oldjuk meg inkább így:

Mindössze annyit kell tenned, hogy átutalsz 1350€ megfelelő bitcoin összeget a számlámra (az éppen aktuális átváltási árfolyam alapján),

és mihelyst a tranzakció sikeres megtörtént, haladéktalanul törölöm az összes kompromittáló jelenetet rólad.

Utána akár úgy is tehetünk, mintha még sohasem találkoztunk volna.

Megnyugtathatlak, hogy az összes káros szoftver is törölni fog mindegyik készülékedről. Illetve, biztosíthatlak afelől, hogy betartom az ígéreteimet.

Szerintem ez egy meglehetősen korrekt ajánlat ilyen alacsony ár mellett, szem előtt tartva azt, hogy milyen sok erőfeszítésbe tellett nekem,

hogy ilyen hosszú ideig figyelemmel kísérjem a profilodat és a tevékenységeidet.

Ha esetleg nem tudnád hogyan kell bitcoint vásárolni és küldeni – könnyedén felvilágosíthatod magadat, ha rákeresel az erre vonatkozó információkra.

Bitcoin tárcám a következő: 126jWBzaLXqEv9zHG5rNTXaVH4KZZxpio

Az e-mail megnyitása után legfeljebb 48 órád (pontosabban két napod) van a tranzakció végrehajtására.

Az alábbiakban pedig nézzük át, hogy mik azok, amiket nem szabad tenned:

**Ne kísérelj meg válaszolni az e-mailjeimre (a beérkező levelek közt található e-mailt én hoztam létre a visszaküldési címmel együtt).*

**Ne próbáld hívni a rendőrséget vagy más biztonsági szolgálatot. Sőt, még csak ne is gondold arra, hogy ezt megoszd a barátainkkal.*

Amint rájönnek erre - (és kétséged se legyen afelől, hogy erre képes vagyok, mivel teljes kontrollom van az összes rendszered felett) -

a videó abban a pillanatban elérhető lesz a nagy nyilvánosság számára.

**Ne kísérelj meg engem keresni - ennek semmi értelme. Minden kriptovaluta tranzakció teljesen névtelenül történik.*

**Ne kísérelj meg újratelepíteni az operációs rendszereket az eszközeiden, vagy megszabadulni tőlük. Ez szintén értelmetlen lenne, mivel az összes videó elérhető távoli szervereken is.*

Most pedig vegyük át azokat a dolgokat, melyek miatt nem kell aggódnod:

**Hogy nem kapom meg az átutalt pénzt.*

TLP: WHITE



TLP:WHITE

Szabadon terjeszhető!

- Emiatt ne aggódj. A tranzakciót a sikeres végrehajtása után is nyomon tudom követni, mivel továbbra is figyelemmel kísérem minden tevékenységedet

(a trójai vírusom távvezérlési funkcióval is rendelkezik, hasonlóan a TeamViewer-hez).

*Hogy annak ellenére is nyilvánosságra fogom hozni a videódat, hogy a pénzáttalásod már megtörtént.

- Hidd el nekem, számomra teljesen értelmetlen lenne tovább bonyolítani az életedet. Ha valóban ezt akarnám, már rég megtettem volna!

Minden a méltányosság jegyében fog történni!

Ja, és mielőtt elfelejteném ... a jövőben próbálj meg többé nem belekeveredni ilyen helyzetekbe!

Fogadd meg a tanácsom – változtasd meg rendszeresen a fiókjaid jelszavait.

Zsarolólevelekkel kapcsolatban további információkat találhat a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet honlapján:

- <https://nki.gov.hu/it-biztonsag/kiadvanyok/segedletek/tudnivalok-a-sextortion-zsarololevelekről>
- <https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztatas-keretlen-level-utjan-terjedo-zsarolo-levelekről/>



NEMZETI

KIBERVÉDELMI INTÉZET

Nemzetbiztonsági Szakszolgálat
Nemzeti Kibervédelmi Intézet
Telefon: +36-1-336-4833
Incidensbejelentés: csirt@nki.gov.hu

TLP: WHITE