TLP:WHITE
Szabadon terjeszthető!

Tájékoztatás

az interneten terjedő, zsaroló hangvételű levelekkel kapcsolatban

(2022.06.20.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet tájékoztatót 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, amelyekkel állami és önkormányzati szerveket, közintézményeket és magánszemélyeket céloznak.

A levelek szövegezése alapvetően azonos, a korábbi hasonló zsarolólevelekhez képest koherensebbek, helyesírás szempontjából jóval pontosabbak, a hangnemük pedig egységesen tegeződő.

Az üzenetek tartalma szerint a címzett készülékét megfertőzték egy trójai vírussal, amelynek segítségével az áldozat informatikai eszközéhez 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 **felnőtt 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 pénzösszeg változó lehet, jellemzően: 1250 EURO.

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

„Fizetési felszólítás. Tartozásrendezési kérelem.”

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!

Sajnos, rossz hírem van számodra. Néhány hónappal ezelőtt sikerült teljes hozzáférést szereznem az összes eszközödhöz, melyekkel az internetet szoktad böngészni. Ezt követően folyamatosan figyelemmel kísértem minden internetes tevékenységedet. Az alábbiakban összefoglalva áttekintheted az események sorrendjét:

Korábban vásároltam hackerektől egy speciális hozzáférést különböző e-mail fiókokhoz (manapság ez egy igen egyszerű, online elvégezhető művelet). Így már nyilvánvaló, hogy a te e-mail fiókodba is könnyedén be tudtam jelentkezni. Egy héttel később feltelepítettem egy trójai vírust az összes eszközöd operációs rendszerébe, melyekkel az e-mail-fiókodba szoktál bejelentkezni. Ami azt illeti, ez egy meglehetősen egyszerű feladat volt (mivel te magad nyitottad meg az adott hivatkozásokat a beérkező leveleidben). Egyszerűen zseniális!

TLP:WHITE
Szabadon terjeszthető!

Ennek a szoftvernek a segítségével hozzáférhetek az összes vezérlőhöz az eszközeiden (például a videokamerádhoz, a mikrofonodhoz, a billentyűzetedhez stb.). Könnyűszerrel le tudom tölteni a szervereimre az összes adatodat, fényképedet, böngészési előzményeidet és egyéb információidat. Hozzáférhetek a közösségi hálózatokon lévő összes fiókodhoz, üzenetküldéseidhez, az e-mailjeidhez, beleértve a csevegési előzményeidet és a névjegylistádat is. A vírusom rendszeresen frissíti a fájlazonosítóit (mivel egy illesztőprogram vezérli), és ennek köszönhetően a vírusirtó szoftvered számára észrevétlen tud maradni. Eddigre már gondolom számodra is világos, hogy miért nem volt sejtelmed sem rólam mindezidáig, amíg el nem küldtem neked ezt a üzenetet...

A veled kapcsolatos információk összegyűjtése során arra is rájöttem, hogy igazi rajongója és gyakori látogatója vagy a felnőtteknek szóló weboldalaknak. Rendkívül imádod a pornóoldalak böngészését, miközben izgató videókat nézhetsz, és hihetetlen élvezeteketben lehet részed. Őszintén megmondom, hogy nem tudtam megállni, hogy ne készítsek nehány felvételt a perverz szóló akcióidról, amiket aztán összeállítottam egy pár külön videóba, megmutatva, hogyan szoktál önkielégíteni és a végén elélvezni. Ha még mindezután is kételkednél bennem, mindössze néhány egérkattintásra van szükségem ahhoz, hogy megosszam ezeket a videókat a kollégáiddal, a barátaiddal, sőt még a rokonaiddal is. Vagy akár az internetre feltöltve teljesen nyilvánosságra is hozhatom őket. Őszintén hiszem és remélem, hogy te egyáltalán nem szeretnéd, hogy ilyen dolgok megtörténjenek, szem előtt tartva mindazokat a bizarr dologokat, melyeket azokban a videókban szoktál nézegetni, (pontosan tudod, hogy mit is értek ezalatt), ez teljes katasztrófát jelentene számodra. Természetesen, még megoldhatjuk a dolgot a következő módon:

Átutalsz nekem egy 1250€ értéknek megfelelő bitcoin összeget (az átutalás időpontjában érvényes átváltási árfolyam szerint), így miután megkaptam az átutalást, habozás nélkül azonnal eltávolítom az összes nyavalyás videót. Utána pedig úgy teszünk, mintha ez az egész soha meg sem történt volna. Továbbá biztosíthatlak afelől, hogy az összes kártevő szoftvert deaktiválom és eltávolítom az összes eszközödről. Ne aggódj, tartani fogom a szavam. Szerintem ez egy igen méltányos ajánlat, főleg ilyen alacsony áron, figyelembe véve azt is, hogy milyen hosszú időn keresztül kísértem figyelemmel a profilodat és a forgalmadat. Ha még nem ismernéd a bitcoin vásárlásának és átutalásának a menetét, akkor csak annyit kell tenned, hogy megkeresed a szükséges információkat az interneten.

A bitcoin tárcám címe a következő: 1DMSacAjQdgyobXtsJ88pMpkmYNffEyQAz

Mindössze 48 órád (vagyis 2 nap) áll rendelkezésre, és a visszaszámlálás közvetlenül az e-mail megnyitása után kezdődik.

Ne felejtsd el továbbá észben tartani és nem elkövetni a következőket:

> Ne próbálj meg válaszolni az e-mailemre (ezt az e-mailt a beérkező leveleid közt generáltam a visszaküldési címmel együtt).

> Ne próbáld meg hívni a rendőrséget vagy egyéb biztonsági szerveket. Sőt, eszedbe se jusson megosztani mindezt a barátaiddal.

Ha értesülök róla (és felkészültségemnek hála, ez rögtön be is következhet, hiszen az összes rendszered az irányításom alatt áll és folyamatosan figyelem) -

a piszkos videóid késedelem nélkül nyilvánosságra kerülnek.

> Ne próbálj meg engem felkutatni – ez teljességgel hiábavaló kísérlet lenne, mivel a kriptovaluta tranzakciók mindig névtelenek maradnak.

> Ne próbáld meg újratelepíteni vagy eltávolítani az eszközeid operációs rendszerét sem. Ez is értelmetlen lenne,

hiszen az összes privát videódat már rég lementettem külső szerverekre.

Továbbá, nem kell amiatt aggódnod:

> Hogy nem kapom meg az általad végrehajtott pénzátutalást.

Nyugi, az átutalást, mihelyst elküldted, azonnal nyomon tudom követni, elvégre szüntelenül figyelemmel kísérem az összes tevékenységedet

(a trójai vírusom pedig képes távolról irányítani minden folyamatot, hasonlóan a TeamViewer-hez).

TLP:WHITE
Szabadon terjeszthető!

> Hogy továbbra is terjeszteni fogom a videóidat, miután elküldted nekem a pénzt.

Hidd el, teljesen értelmetlen lenne számomra ezután is tovább zavarnom téged. Ha valóban ez lenne a szándékom, már rég megtehettem volna!

Korrekt és tisztes feltételek között rendezhetjük el az ügyet.

Végül fogadj meg tőlem egy jótanácsot... Ezentúl sokkal jobban ügyelj arra, hogy ne keveredhess még egyszer ilyen fajta kínos szituációkba!

Javaslatom – fordíts nagyobb figyelmet arra, hogy jelszavaidat mindig kellő rendszerességgel megváltoztasd!

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

- https://nki.gov.hu/it-biztonsag/kiadvanyok/segedletek/tudnivalok-a-sextortion-zsarololevelekrol
- https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztatas-keretlen-level-utjan-terjedo-zsarolo-levelekrol/

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