



Riasztás az interneten terjedő, zsaroló hangvételi levelekkel kapcsolatban

(2020.12.16.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) ismételt riasztást ad ki **az interneten terjedő, magyar nyelvű, zsaroló hangvételi levelekkel** kapcsolatban, amelyek állami és önkormányzati szerveket, közintézményeket és magánszemélyeket céloznak meg.

A zsaroló levelek szövegezése egyforma, jó magyarsággal írt, tartalmuk szerint a címzett **felölt tartalmú oldalakat látogatott**, amelyről a zsarolók kompromittáló videófelvétellel rendelkeznek, amit **eljuttatnak a címzett ismerőseinek, valamint a közösségi médiában is közzétesznek**, amennyiben az áldozat nem fizeti ki a kért váltságdíjat. További fenyegetésük, hogy az áldozat levelezési fiókjának hozzáférési adatait, valamint az ahhoz kapcsolódó összes e-mailjét is közzéteszik.

A zsaroló leveleket a SPAM szűrők sokszor nem szűrik ki megfelelően, mivel azok nem tartalmazzak olyan hivatkozást, ami alapján a szűrő felismerné őket. A mostani esetben a levelek tárgya „**Eszközét hackerek támadták meg. Ismerje meg a részleteket ASAP!**”, valamint a levelekben szereplő Bitcoin számla száma „**14MqefrM5WMe526Dpe1frodSRjD2Kn9hTH**” is azonos.

Az NBSZ NKI javasolja ezen levelek figyelmen kívül hagyását, továbbá a fenti indikátorok beállítását a SPAM szűrőben.

Példa a szóban forgó zsarolólevélre

Szia

Profi programozó vagyok, aki csak feltörte készüléke operációs rendszerét.

Több hónapja vagy a felügyeletem alatt.

A helyzet az, hogy készülékét egy felnőtt webhelyen keresztül fertőzte meg egy nemrégiben felkeresett webhely.

Hadd magyarázzak el mindent részletesen, ha nem sokat tudsz erről.

A trójai vírus teljes hozzáférést és ellenőrzést biztosít az eszköz felett.

Ugyanígy látok mindent, ami a képernyőn megjelenik, aktiválhatom a kamerát és a mikrofont az Ön tudta nélkül.

Ezen felül hozzáférhetek a teljes közösségi média névjegyzékéhez és a teljes könyvtárhoz is.

Megkérdezheti, hogy a víruskereso miért nem tudta felismerni a rosszindulatú programomat?



TLP: WHITE

Szabadon terjeszthető!

- A rosszindulatú programom illesztőprogramot használ, és az aláírása 4 óránként frissül, így a víruskeresője csendes.

Készítettem egy videót, amely megmutatja, mennyire elégedett vagy a képernyő bal oldalán, és a jobb oldalon láthatod az akkor nézett videót.

Egy kattintás elegendő ahhoz, hogy ezt a videót elküldjem a teljes levelezési és közösségi névjegyzékre.

Továbbmehetek, és közzétehetem az összes e-mail és üzenetküldő hozzáférési adatait is.

Ha ezt el akarja kerülni, akkor:

Intézzék az 1XXX dollár (USA dollár) átutalását a bitcoin pénztárcámba (ha nem tudja, hogyan kell ezt csinálni, akkor keresse fel a Google-t: „Vásároljon bitcoinot”).

Saját Bitcoin pénztárcám (BTC pénztárca): 14MqefrM5WMe526Dpe1frodSRjD2Kn9hTH

A fizetés kézhezvétele után azonnal törölöm a videót, és biztosíthatom Önöket, hogy soha többé nem hallanak tolem.

50 órája van (2 nap +) a fizetés megszervezésére.

A levél elolvasása után automatikusan értesítést kapok, ezért az időzítő attól a pillanattól indul, amikor elolvasta ezt a levelet.

Nem kell megpróbálni válaszolni nekem, mert értelmetlen (a feladó címe automatikusan generálódik).

Semmi értelme panaszt benyújtani, mivel ez az e-mail nem osztható fel, mint a bitcoin címem.

Soha nem követek el hibákat.

Ha megtudom, hogy megpróbálta megosztani ezt az e-mailt bárki mással, akkor privát videója azonnal mindenki számára elérhető lesz.

Tisztelettel.

Zsarolólevelekkel kapcsolatban további információkat találhat az NBSZ NKI honlapján, az alábbi hivatkozásokon:

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

Nemzetbiztonsági Szakszolgálat

Nemzeti Kibervédelmi Intézet

Telefon: +36-1-336-4833

Fax: +36-1-336-4886

Incidensbejelentés: csirt@nki.gov.hu

TLP: WHITE