



Riasztás az interneten terjedő, zsaroló hangvételű levelekkel kapcsolatban

(2021.05.04.)

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 azonos, 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 **felöltött 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**.

Az aktuális zsaroló levelek szövegezése a korábbiakhoz képest koherensebb, helyesírásiag jóval pontosabb, a hangnem pedig egységesen tegeződő.

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:

„Hackerek hozzáférést szereztek a készülékéhez. Ellenőrizze adatait AZONNAL!”, valamint a levelekben szereplő Bitcoin számla száma **„1GufcqD5AWADhXsjRjwQxB95Yex4Dc34b1”** is azonos.

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:

Helló!

Hadd mutakozzam be. Hivatásos programozó vagyok, aki a szabadidejében hackelésre specializálódik.

Ezúttal sajnós te váltál a következő áldozatomná, mivel feltörtem az operációs rendszeredet és a készülékedet.

Már hónapok óta figyelemmel kísérlek.

Egyszerűbben fogalmazva, megfertőztem a gépedet egy vírussal, miközben te éppen a kedvenc felöltött tartalmú weboldaladat böngészted.

Elmagyarázom részletesebben is, hogy mi történt, ha még nem lenne tapasztalatod ilyen fajta helyzetben.

Egy trójai vírus teljes hozzáférést és ellenőrzést ad számomra a készüléked felett.

Vagyis mindent látok és kezelhetek a képernyődön, bekapcsolhatom a kamerádat és a mikrofonodat, valamint egyéb dolgokat is, anélkül, hogy te erről bármit is tudnál.



TLP:WHITE

Szabadon terjeszthető!

Továbbá, hozzáférést szereztem még a teljes névjegyzékedhez a készülékeiden és a közösségi oldalaidon.

Joggal teheted fel a kérdést, miért nem értesített a víruskeresőd semmilyen kártevő programról?

- Nos, a kémprogramom egy speciális meghajtót használ, melynek a programkódját rendszeresen változtatja, és ezáltal a víruskeresőd nem lesz képes felismerni.

Összeállítottam egy videót, amelyben te szerepelsz, ahogy éppen magaddal játszadsz a képernyő baloldalán, miközben a jobboldal pedig azt a pornóvideót mutatja, amit éppen akkor néztél.

Mindössze néhány kattintás elegendő arra, hogy továbbítsam ezt a videót az összes barátodnak és ismerősödnek a közösségi oldalakon.

Megfogsz lepődni, de még egyéb nyilvánosan elérhető online felületen is közzé tudom tenni.

A jó hír az, hogy még megakadályozhatod, hogy mindez megtörténjen:

Nem kell mást tenned, mint átutálnod 1350 USD összegnek megfelelő bitcoint a BTC tárcámra,

(ha nem tudod, hogyan kell csinálni, keresgélj egy kicsit az interneten, - rengeteg cikk leírja lépésről lépés a teendőket).

A bitcoin tárcám a következő (BTC Wallet): 1GufcQD5AWADhXsjRjwQxB95Yex4Dc34b1

Amint megkapom az összeget, törölöm az összes pajzán videodat, és ígérem, hogy többet nem fogsz hallani felőlem.

Van rá 48 órád (pontosan 2 napod), hogy fizess.

Automatikus értesítést kapok arról, hogy mikor nyitottad meg ezt az e-mailt, és az időzítő pontosan ettől a pillanattól fogva kezd el ketyegni automatikusan.

Ne is próbálj meg válaszolni, mivel teljesen hiábavaló lenne (a küldő e-mail címe automatikusan generált és az internetről szereztem).

Ne próbálj meg panaszkodni vagy feljelenteni sem, mivel az összes személyes adatom és a bitcoin címem is titkosított, a blokklánc rendszer részeként.

Alapos munkát végeztem.

Ha rájönnek, hogy megpróbáltad ezt az e-mail továbbítani bárkinek is, azonnal nyilvánosságra hozom a piszkos videodat.

Légy következetes, és ne kövess el újabb buta hibákat. Tiszta és egyértelmű utasításokat adtam,

lépésről lépésre. Egyszerűen csak kövesd a lépéseket, és ezzel véget vethetsz ennek a kellemetlen szituációnak egyszer és mindenkorra.

Üdvözlétem és sok szerencsét!

Zsarolólevelekkel kapcsolatban további információk találhatóak a 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-terjedő-zsaroló-levelekről/>

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

TLP: WHITE

Legyen óvatos!

Már magyar nyelven is terjednek Sextortion zsarolólevelek, mutatjuk mire érdemes figyelni!

Feladó: Névtelen Hacker (sheri.787@h.nevtelenhacker.top)
Címzett: Te@email.hu
Tárgy: Ez az utolsó figyelmeztetésem

Árulkodó a feladó e-mail címe:
timothy.916@b.nevtelenhacker.top

Mindig nézzük meg a feladó címet, mert néhány esetben a küldő címéből is megállapítható a levél gyanús tartalma.

Sürgető hangnem, helyesírási hiba

Fontos, hogy ne essen pánikba! Olvassa át többször a levelet, hogy kiszűrje a gyanús elemeket.

UTOLSÓ FIGYELMEZTETÉS

Önnek lehetősége van arra, hogy megmentse a társadalmi életét - nem vagyok viccelő!

Az utolsó 72 órát adom meg a fizetés előtt, mielőtt elküldöm a videót maszturbációval az összes barátodnak és társának. Amikor utoljára látogattál egy fiatal tinédzserként egy Pornográf weboldalra, letöltötted és automatikusan telepítetted a létrehozott kémsoftvert. A program bekapcsolta a fényképezőgépet, és rögzítette a maszturbációját és a nézett videót maszturbálás közben. Szoftverem szintén letöltött e-mailek listáját és a Facebook-ismerőseinek listáját a készüléken. Mind a - Cert.mp4 - mind a maszturbációval és egy fájl a merevlemezemen található összes kapcsolattal.

Rejtett speciális karakterek, hogy a levél ne akadjon meg a spamszűrőn

Nagyon Derverz!

Ha azt szeretné, hogy mindkét fájl töröljem és titokban tartsam, akkor elküldned kell nekem a Bitcoin fizetést. Utolsó 72 órát adok át a pénzeszközök átutalására.

Furcsa nyelvezet, helyesírási hibák

Ha nem tudja, hogyan kell fizetni a Bitcoinnal, látogasson el a Google-ra és keressen - hogyan vásároljon bitcoint.

Közvetlenül küldjön 500.000 HUF (0.342384 BTC) erre a Bitcoin címre:

38tP8HBPeEqKuHEoH3uxWG3Nenz5rUxsRi
(másolja és illesse be)

1 BTC = 1.493.500 HUF most, így pontosan 0.342384 BTC küld a fenti címre.

Soha NE fizesse ki a kért összeget! Semmi nem garantálja, hogy a zsaroló tényleg rendelkezik Önről információkkal.

Ne próbálja meg csinálni!
Amint megnyitja ezt az e-mailt, tudom, hogy kinyitotta.

Folyamatosan váltogatják a közvetlen és közvetett (tegezés/magázás) megszólításokat.

Ez a Bitcoin cím csak Önhöz kapcsolódik, így tudni fogom, hogy elküldte a megfelelő összeget. Teljes fizetés esetén mindkét fájl eltávolítjuk, és kikapcsolom a szoftvert.

Ha nem küldi el a fizetést, elküldöm a maszturbációs videódat az összes ismerősének és társának, amelyet a letöltött kapcsolattartó listádról küld.

Íme a fizetési részletek:

Küldj 0.342384 BTC erre a Bitcoin címre:

38tP8HBPeEqKuHEoH3uxWG3Nenz5rUxsRi
(másolja és illesse be)

Amennyiben ilyen, vagy ehhez hasonló üzenetet kap egyszerűen törölje a levelet.

Ha mégis felmerül annak gyanúja, hogy a zsaroló valós információkkal rendelkezhet Önről, tegyen feljelentést az illetékes hatóságnál, illetve továbbítsa levelét mellékletként (fejléccel együtt) a cert@nki.gov.hu e-mail címre.

Meglátogathatja a rendőrséget, de senki sem segít.
Tudom, mit csinálók.
Nem élek az Ön országában, és tudom, hogy maradjon névtelen.

Ne próbáljon meg becsapni - azonnal tudni fogom - az én Spysoftom rögzíti az összes meglátogatott weboldalt és az összes nyomógombot.
Ha ezt teszed - elküldöm ezt a csúnya felvételt mindenkinek, akit ismersz, beleértve a családodat is!

Ne csalj meg! Ne felejtse el a szégyenet, és ha figyelmen kívül hagyod ezt az üzenetet, az életed tönkremegy.
Várom a Bitcoin fizetését.

Névtelen Hacker

Ui Ha több időre van szüksége a BTC vásárlásához és elküldéséhez, nyissa meg a jegyzetomböt, és írjon be - 48H ++ - és mentse el. Így kapcsolatba léphet velem.
Még 48 órát fogok adni, mielőtt elküldöm a videót a kapcsolattartóknak, de csak akkor, ha látom, hogy valóban meg akarod vásárolni bitcoint.

Névtelenek vagyunk.
Nem megbocsátunk. Nem felejtjük el.
Elvárják tőlünk.

A Sextortion zsarolólevelek egy másik - jellemzően külföldi - verziójában a felhasználók korábban kiszivárgott online bejelentkezési adatait is feltüntetik. A támadók ezzel próbálják meg állításukat - hamisan - hitelesebbé tenni.

Illyenkor sem szabad megijedni!

- Ellenőrizze e-mail címeinek és jelszavainak lehetséges kompromittálódását (haveibeenpwned.com).
- Rendszeresen változtassa meg jelszavait: javasolt a hosszú és összetett jelszavak használata, amely kis- nagybetűt, számot és speciális karaktert is tartalmaz.
- Eltérő szolgáltatásokhoz, eltérő jelszavakat alkalmazzon, amennyiben van rá lehetősége engedélyezze a kétfaktoros azonosítást.