TLP:WHITE
Szabadon terjeszthető!

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 **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**.

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

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:

> **„Hackerek hozzáférést szereztek a készülékéhez. Ellenőrízze 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 mutatkozzam be. Hivatásos programozó vagyok, aki a szabadidejében hackelésekre specializálódik.

Ezúttal sajnos te váltál a következő áldozatommá, 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 felnőtt 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 készülékeden és a közösségi oldalaidon.

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

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

Összeállítottam egy videót, amelyben te szerepelsz, ahogy éppen magaddal játszadozol 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.

Meg fogsz 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 átutalnod 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, törlöm az összes pajzán videódat, 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 rájönnék, hogy megpróbáltad ezt az e-mail továbbítani bárkinek is, azonnal nyilvánosságra hozom a piszkos videódat.

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.

Üdvözletem és sok szerencsét!

Zsarolólevelekkel kapcsolatban további információk találhatóak a 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