CTI Jelentés

A kriptovaluták veszélyei

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERVÉDELMI INTÉZET

RENDŐRSÉG POLICE

Tartalomjegyzék

Bevezetés

Manapság igen népszerűvé váltak a különböző kriptovaluták. Rengeteg történet kering róluk a médiában, az interneten, néhányan a gyors meggazdagodást látják benne, néhányan a jövő pénztechnológiájának gondolják, és persze ki ne hallott volna a férfiról, aki 2010-ben 2 darab pizzát rendelt 10 000 Bitcoinból, ami mai árfolyamon körülbelül 150 milliárd forintot érne.

Jelen kiadvány célja tájékoztatni a lakosságot a kriptovalutákkal való visszaélésekről, amit az NBSZ NKI-hoz bejelentett incidensek alapján kiemelten fontosnak tartunk. A **KiberPajzs együttműködés** keretében a tipikus csalási módok bemutatásában partnerünk volt az **Országos Rendőr-főkapitányság Bűnügyi Főigazgatóság Bűnügyi Főosztálya**.

A legjobb védekezés a tájékozódás, így ezt a CTI jelentést ajánljuk minden olvasónknak, aki kriptovalutákkal bármilyen módon tevékenykedni tervez vagy csak szeretne egy kicsit elmélyülni a témában.

Mi az a kriptovaluta?

A kriptovaluta egy gyűjtőfogalom, ami alatt olyan digitális eszközöket értünk, amelyek közös jellemzője, hogy decentralizált módon működnek, azaz felügyeletüket nem egy központi szervezet végzi - mint például egy bank vagy egy állam - hanem a valutát használók közössége.

Megalkotásukkor az egyik legfontosabb szempont az volt, hogy a működtetésük ne igényeljen előzetes bizalmat a tranzakció egyik résztvevőjétől sem. A blokklánc technológia önmagában, "számítástechnikailag" hivatott biztosítani az adatok hitelességét emberi felügyelet nélkül, és így a résztvevőknek nem szükséges egymásban bízniuk a működéshez.

Ezen tulajdonságán felül általánosan elmondható róluk, hogy pszeudo – anonim módon működnek, tehát egy felhasználó valódi identitása nem látszódik egyértelműen –, mivel a tranzakciókban címeket használnak nevek helyett - azonban bizonyos specifikus körülmények között lehetséges kinyomozni azt. Ez azt is jelenti, hogy a hagyományos pénzekhez képest sokkal nehezebben lekövethetők a tranzakciók mozgása.

Mindezt úgy érik el, hogy a valutát használók közösen egy számítógépes hálózatot alkotnak, és egymás között általuk kódban meghatározott szabályoknak engedelmeskednek.

Ezen a hálózaton hogyha valaki pénzt szeretne küldeni, akkor azt egy bányász *(a kriptovaluta bányászatról később bővebben is szót ejtünk)* először rögzíti, majd a tranzakció szabályosságát a hálózatot használó összes többi résztvevő ellenőrzi.

A hagyományos pénzek valamilyen módon a valósághoz vannak kötve olyan szabályokkal, mint például az aranystandard, ami az adott ország valutájának értékét az arany egy rögzített mennyiségével egyenlőként határozza meg.

Ez a kriptovaluták esetében a legtöbb esetben ez alapvetően nem így működik, az értéküket szimplán a kereslet-kínálat határozza meg. Ezáltal az értékük nagyon változó: annyit érnek, amennyiért valaki hajlandó megvásárolni őket. A legolcsóbb kriptovaluták centek töredékét érik, a legdrágábból pedig egy darab értéke egy középkategóriás autó értékével feleltethető meg.

A kriptovaluták sokáig a pénzügyi világ "vadnyugatának" számítottak. Az **Európai Unió kriptopiac-rendelete (MiCA)** azonban e téren változást hoz, megkísérli átláthatóbbá és fogyasztóbarátabbá tenni a kriptopiacot. Mindennek a hazai jogrendbe történő átültetés is folyamatban van, amennyiben az Országgyűlés elfogadja a **Nemzetgazdasági Minisztérium törvényjavaslatát,** ami lényeges változást hoz azzal, hogy a kriptovaluták - bizonyos megkötésekkel - pénzügyi szolgáltatásnak minősülnek majd, és így a Magyar Nemzeti Bank felügyelete alá fognak tartozni.

A kriptovaluta kifejezés a **kriptográfia** (azaz a titkosítás) – és **valuta** (azaz pénznem) szavak összetételéből származik.

Ez azért van így, mert a biztonságukat különféle kriptográfiai megoldások hivatottak megoldani, mint például a különböző **hashelő algoritmusok**, és az úgy nevezett **blockchain** technológia.

Ezek elsőre ijesztően hangozhatnak, de valójában csak annyit jelentenek, hogy olyan titkosítási módszereken alapulnak, amik egyirányúak, más szóval nem visszafejthetőek, és a tranzakciók listája egy nyilvánosan elérhető, utólag nem módosítható, azonban egyértelműen lekövethető módszerrel van nyilvántartva *(ez az ún. ledger)*.

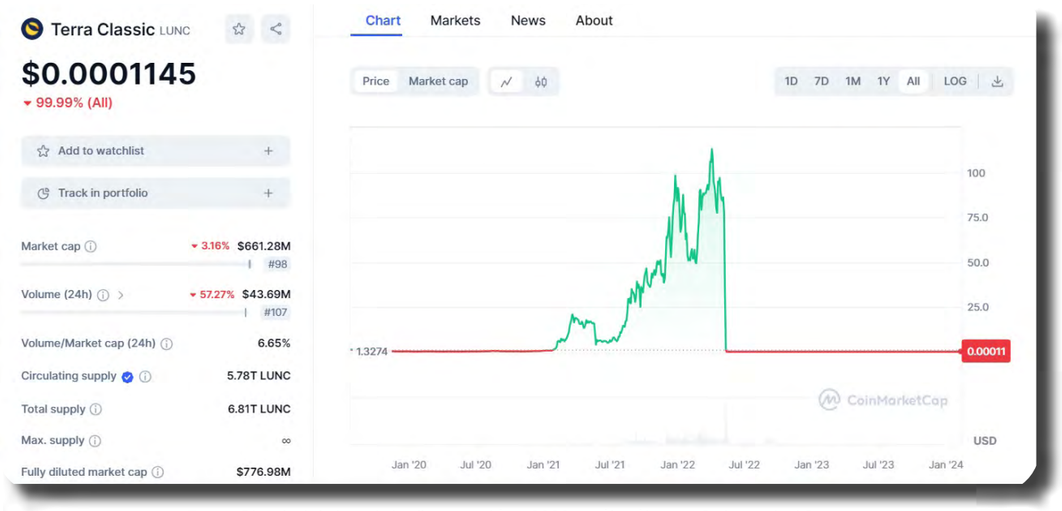
A legnépszerűbb kriptovaluták

A kriptovaluta, mint befektetés

Az emberek gyakran tévesen úgy gondolják, hogy a kriptovalutákkal való kereskedés, vagy az abba való fektetés gyors és könnyű út a vagyonhoz. A valóság azonban az, hogy ez a piac rendkívül ingatag és kiszámíthatatlan, tele van kockázatokkal és spekulációval.

Ahogyan azt az élet többi területén is tapasztalhatjuk:
„Ha valami túl szép ahhoz, hogy igaz legyen, akkor az valószínűleg nem igaz".

Sokan elvesztik megtakarításaikat a kriptovaluták körüli felhajtás és a nagymértékű spekuláció miatt, és ez a legtöbb esetben több kárt okoz, mint hasznot. Ezek a valuták a hagyományos pénzekhez képest értéküket tekintve sokkal nagyobb mozgást végeznek: némelyik értéke naponta 10 000%-ot növekszik, majd néhány nappal vagy órával később ezt el is veszíti.



A Terra Classic kriptovaluta összeomlása 2022. májusában - CoinMarketCap

Ez a tulajdonság azonban egy kétélű kard: hiszen amilyen könnyen nyereséget lehet vele elérni, ugyan olyan könnyű vele veszíteni is. Sőt, egy felmérés szerint (eToro) a kereskedők 90%-a hosszútávon veszít vele, mégpedig a pénzük mintegy 36.3%-át. Nem csoda hát, hogy a kriptovaluta kereskedők 75%-a 2 éven belül felhagy ezzel a tevékenységével.

Volatilitás

Ennek több oka is van. A legnyomósabb érv a már korábban is említett árképzési mechanizmus, vagyis hogy értéküket a kereslet – kínálat határozza meg, és a jelentés elkészültekor még semmilyen kötelező jellegű szabály/törvény nem befolyásolja azt. Ezen kívül fontos még a piac mérete, az adott valutába fektetett valós tőke mennyisége is. Ezekből több probléma is ered: könnyű piac manipuláció, whalek, spekulatív befektetők, pump and dump coinok.

A kriptovaluták óriásai, a bálnák (whale) azok a piaci résztvevők, akik hatalmas részt birtokolnak egy adott valutából, többnyire sok száz millió vagy több milliárd dolláros nagyságrendben. A név a piacra gyakorolt hatásukra utal.

A kilétük természetesen anonim, viszont a tárcájuk mindenkiével együtt nyilvános, a pénzmozgásukat követve olyan mintha pontosan belelátnánk egy milliárdos mikor, hova, mennyi pénzt küld. Egy-egy tranzakciójukkal hatalmas változást tudnak okozni bármelyik valuta értékében.

Gondoljuk csak végig, mi történik például ha egy bálna óriási mennyiségű kriptovalutát, pl. Dogecoint ad el. Az eladási megbízás kiadásakor a hatalmas mennyiségű tőke elárasztja a piacot, a fellelhető kínálat megnövekszik. Ezután kettő forgatókönyv játszódhat le. Az első az, hogy a kereslet nem követi le a megnövekedett kínálatot, konstans marad, a második pedig hogy nemhogy nem követi le, de éppen ellenkezőleg: lezuhan a piaci pánik miatt.

Akárhogy is, de végső soron egy egyenlőtlenség alakul ki a piacon a kereslet és a kínálat között, és a kiegyenlítéshez az árnak változnia kell. Ebben az esetben a Dogecoin értéke összességében csökkenni fog, hiszen az eladók kénytelenek lesznek olcsóbban adni a megnövekedett kínálat miatt. Ez a folyamat hasonlóképpen játszódik le ellenkező esetben is, tehát amikor egy bálna nagy mennyiséget vásárol, akkor megugrik a kripto egységnyi ára.

Ami tovább súlyosbítja a helyzetet, az az, hogy a bálnák tisztában vannak pozíciójukkal, és semmi sem akadályozza meg őket abban, hogy azzal visszaéljenek: sok esetben szánt szándékkal befolyásolják a piacot. Az egyik legalapvetőbb ilyen piaci **manipuláció** az, hogy egy nagy mértékű eladással az árat a fentebb közölt módon csökkenni kényszerítik, majd visszavásárolják az alacsonyabb áron, kvázi „ingyen pénzhez" jutva csupán a saját pénzük mozgatásával.

Természetesen a világon semmi sincs ingyen, így ezt az anyagi előnyt a kisebb befektetők kárára érik el. A stratégia neve whale dump, és buy back, és ez a módszer csak egy a sok eszköz közül, amivel a piacot manipulálni lehet. Ezek az eszközök nagyban hozzájárulnak a kriptovaluták árának kiszámíthatatlanságához.

Ezeken kívül az is közrejátszik a **volatilitáshoz**, hogy a pénzeszközök világában, ez a technológia még nagyon újnak számít, gyerekcipőben jár, és ezáltal kevés történelmi adat vizsgálható az ármozgásukról.

Sok kereskedő és befektető tevékenykedik az úgynevezett technikai elemzést alkalmazva, aminek a lényege az, hogy a múltban történt mozgásokat vizsgálva modelleket, szabályokat állítanak fel maguknak, amivel megpróbálják megjósolni, hogy az adott valuta árfolyama hogyan fog viselkedni. Ezek azonban a kevés adat miatt erősen spekulatív jellegűek, mondhatjuk, hogy még a legprofibbak sem tudják megjósolni mi fog történni pontosan.

Egy felmérés szerint a sikerességi arányuk a jóslásban körülbelül 55%, tehát alig jobb mintha valaki csak hasraütés-szerűen tippelne.

Összességében elmondható, hogy bár csábítóan hangozhat hogy valaki kriptovalutával kereskedjen, vagy abba fektessen, azonban tisztában kell lenni annak magas kockázatával. Bár az igaz, hogy a Bitcoin ára a keletkezése óta többször hatalmasat ugrott, aztán visszaesett, és összességében eddig növekvő tendenciát mutatott, semmi garancia nincsen rá, hogy ez a jövőben is így fog folytatódni.

Technológiai veszélyek

Nemcsak a volatilis piaci árak rejtegetnek veszélyeket, hanem maga a kripto technológia is. Ugyanúgy, ahogy az összes létező informatikai rendszer, ez sem hibátlan, rosszakarók kihasználhatnak bennük sérülékenységeket, és még ha a rossz szándékot ki is vesszük a képletből, magától is kialakulhatnak spontán hibák emberi közbeavatkozás nélkül.

Elfelejtett jelszó

Nézzük például a legegyszerűbb technológiai veszélyt: az elfelejtett jelszó esetét. Még egy hagyományos rendszerben ez annyit jelent, hogy valamelyik biztonsági rendszerrel, például biztonsági kérdéssel vagy e-mailre történő jelszóváltoztató link kérésével ismételt belépést nyerhetünk fiókunkba.

Ha az internetbankunkba nem tudunk belépni, legrosszabb esetben egy bankfiókban az ügyintézők segíteni tudnak új jelszót generálni, addig ez a kriptovaluták esetében teljességgel lehetetlen, ugyanis nem létezik semmilyen support vagy helpdesk.

Kivételes eset, ha elrugaszkodunk a decentralizáltságtól, és megbízunk egy céget a kriptovaluta pénztárcánk menedzselésével, ami a technológia elveivel szemben helyezkedik el, – hiszen így már valakiben meg kell bíznunk – például egy kriptovaluta tőzsdét, mint a Binance vagy egy wallet kezelőt, például a MetaMaskot.
Legyünk tudatában annak, hogy ebben az esetben ezek a cégek teljes hozzáféréssel rendelkeznek a pénztárcánk fölött.

Kriptovaluták esetében minden birtokos rendelkezik egy privát kulccsal (kvázi jelszóval) ami egy hosszú „véletlenszerű" karakterlánc, és például így néz ki:

(L4yGCJHksjbN62hC2bg4TgSiCcEqTPPDZUjGjuiQLymEY7sky9Df)

Ez a jelszó szükséges ahhoz, hogy a pénzünket el tudjuk költeni, nélküle teljességgel lehetetlen a hálózaton egy tranzakciót lebonyolítani. Ha ezt elfelejtettük, akkor az úgynevezett helyreállítási jelmondattal (recovery phrase) újragenerálhatjuk a jelszavunkat.

A helyreállítási jelmondat egy 12-24 szó által alkotott mester jelszóként lehet gondolni.
A szavak véletlenszerűek, és az, hogy mennyi szó szükséges az újrageneráláshoz, kriptovalutától függ.

TUDTAD?

Egy **recovery phrase** Bitcoin esetében például így nézhet ki:

„luck duck friends war rain pear opera desk line rock number open"

A védelmére rendkívüli figyelmet érdemes fordítani, ugyanis az ismeretében bárki teljeskörű hozzáférést tud szerezni a kriptovalutánkhoz. Abban az esetben, ha elfelejtjük vagy nem férünk hozzá ehhez a szólánchoz, a rendszer anonimitása és **a felügyelő szervek hiánya miatt örökre elveszítjük a pénzünket, visszaszerzésére nincs lehetőség**.

Ez történt például Stefan Thomassal, a programozóval, aki privát kulcsát egy biztonságos merevlemezen tárolja, amihez elfelejtette a mester jelszavát. Az adattárolón lévő privát kulcssal mintegy 240 millió dollárnyi Bitcoint mozgósíthatna, azonban Stefan nem tud hozzáférni, és már csak 2 belépési próbálkozása maradt, mielőtt az adat törlődik, és ezáltal a pénzét visszafordíthatatlanul elveszíti.

Rossz címre utalás

Egy másik valóságos veszély az, ha véletlenül rossz címre utaljuk kriptovalutánkat. Minden lehetséges kiosztható „bankszámlaszám" már létezik, csak a legtöbbnek nincsen tulajdonosa, amelyekhez senki nem fér hozzá, így ha oda küldjük pénzünket, azt sosem látjuk viszont.

De nem is feltétlenül szükséges, hogy mi hibázzunk! A clipboard hijack támadások lényege az, hogy egy hacker átveszi rendszerünk másoló-beillesztő funkciója felett az irányítást, és ezt többek között kriptovaluta csalásra is fel tudja használni. Az ilyen támadások során a bünözők valamilyen káros kóddal fertőzik meg az eszközünket, ami ezután tudtunkon kívül a háttérben fut, és várakozik. Amikor a rosszindulatú programok észreveszik, hogy a clipboardunkra egy kriptovaluta címet másoltunk, akkor azt kicserélik egy előre meghatározott másik címre, ami a támadóé, és így küldéskor mi magunk utaljuk át a kriptorabló „zsebébe" a pénzünket anélkül, hogy neki meg kellett volna szereznie privát kulcsunkat.

51 % támadás

Az anonimitás és a bizalom szükségességének elkerülése végett minden kriptovalutának központi eleme egy olyan mechanizmus, ami ellenőrzi azt, hogy egy utaláskor az adott illető „számláján" van-e elegendő mennyiségű pénz. Ha nincs, akkor a tranzakció nem megy végbe.

Banki utalás esetén ezt a bank rendszere intézi, kriptovaluta utaláskor azonban ezt az ellenőrzést az egész valutát használók közössége hitelesíti egy ún. konszenzus mechanizmus segítségével, aminek a működési elve részleteiben valutánként változnak, de néhány dologban mégis megegyeznek.

Egy tranzakció kezdetekor minden adott valutát használó tudomására jut, hogy egy címről egy másik címre valaki tranzakciót szeretne kezdeményezni. Ezt követően különböző, bonyolult matematikai műveletek segítségével ellenőrzésre kerül, hogy lehetséges-e egyáltalán a folyamatot végrehajtani. Ha a felhasználók legalább fele úgy gondolja, hogy igen, akkor kialakul a konszenzus, és a tranzakció megtörténik.

Ebből következik, hogy ha valaki rendelkezik a konszenzus mechanizmus több mint felével, akkor gyakorlatilag uralni képes a rendszert. Egy ilyen támadónak lehetősége nyílik a saját valutáját többször is elkölteni anélkül, hogy az az ő számlájáról elfogyna, (ezt hívjuk double spendingnek) illetve meggátolni egyébként hiteles tranzakciók sikeres lefutását. Nem nyílik azonban lehetősége pénz teremtésére és mások pénzének elköltésére.

Ehhez a támadáshoz irtózatos nagy befektetés szükséges a támadó részéről, ezért nagyobb, kiforrottabb hálózatokon, mint például a Bitcoin vagy az Ethereum az előfordulása valószínűtlen, de technikailag azonban nem lehetetlen. Sőt, kisebb hálózatokon a történelemben már többször is előfordult.

Okos szerződések veszélyei

Az okos szerződések olyan programok, amelyek segítségével két fél egy kriptovaluta hálózaton egymással megegyezhet, hogy bizonyos általuk meghatározott feltételek teljesülése esetén különböző tranzakciók menjenek végbe. Felhasználhatók például ingatlanügyekben, a bérleti szerződések egyszerűsítéséhez, ezzel csökkentve a közvetítők szükségességét, vagy szerzői jogok érvényesítéséhez.

Ezek a programok megmásíthatatlanok, és magán az adott kriptovaluta hálózaton futnak le. A céljuk az, hogy két fél megegyezése esetén ne legyen szükség az egymás iránti bizalomra, hiszen a kód maga hivatott teljesíteni a megegyezést. A számos előny mellett azonban ez a technológia is rejt magában veszélyeket.

Egyrészt könnyen lehet őket átverésekhez használni, hiszen egy átlagos felhasználó nem feltétlenül ért a kódoláshoz, a program pontos működését nem minden esetben érti hibátlanul, így egy csaló könnyű szerrel csempészhet bele rosszindulatú kódrészletet, amivel akár teljes irányítást is szerezhet áldozata kriptovaluta pénztárcája fölött.
Ezen kívül mint minden kódban, ezekben is lehetnek nem szándékos hibák, sérülékenységek. Ezt kihasználva az okos szerződések meghackelhetővé válhatnak.
A helyzetet tovább rontja, hogy ezek a kódok végérvényesen a blockchainbe íródva, „kőbe vésve” tárolódnak, utólagosan lehetetlen módosítani őket, így ha a beiktatásuk után veszünk észre hibát bennük, azon változtatni már nem fogunk tudni.

A kvantumszámítógépek jövőbeli veszélyei

A kvantumszámítógépek fejlődése nem csupán a kriptovalutákra gyakorol jelentős hatást, hanem az információbiztonság egész területére.
A jelenlegi biztonsági rendszereink megbízhatóságát a titkosítási technológiák feltöréséhez szükséges, elképesztő mennyiségű számítási teljesítmény biztosítja. Ez a teljesítmény olyan mértékű, hogy a titkosítás feltörése csak elképzelhetetlenül hosszú idő alatt lehetséges, azonban mindez megváltozhat a jövőben, a kvantumszámítógépek által. Mivel ezek az eszközök más elven működnek, mint a hagyományos számítógépek, bizonyos műveleteket hatványozottan gyorsabban végeznek el, így egy olyan titkosítás, ami egy hagyományos számítógépnek több millió évbe telne, egy kvantumszámítógépnek csupán másodpercekbe. Jelenleg még limitált az ilyen gépekhez való hozzáférés, és a működtetésük is kifejezetten nehézkes, de a Google, a NASA és több, egykor startupként indult cég (pl. D-Wave, Rigetti) is azon dolgozik, hogy ez gyökeresen megváltozzon néhány éven belül.

A kriptovalutákkal kapcsolatba hozható csalások, átverések

A legnagyobb veszélyforrás mindezek ellenére még mindig az emberek rosszindulata, a különféle csalások megléte. A kriptovaluták technológiai adottságaik miatt tökéletes fizetőeszköze a bűnözőknek.

Nehezen lenyomozhatóak, így a legtöbb esetben még a rendőrség sem tud segíteni, ha kripto csalás áldozatai lettünk, ezért különösen fontos tájékozódnunk, hogy még időben felismerjük az ilyen kísérleteket. Az alábbiakban bemutatunk néhány gyakori módszert, amivel a kiberbűnözők csalni próbálnak.

Webshop csalások

Az elmúlt években hatalmas népszerűségnek örvendenek a különféle online kereskedési platformok, mint például a wish.com és az alibaba.com. Ezek a külföldi weboldalak kevésbé szigorú szabályozások alapján üzemelnek, mint a hazai oldalaink, részben ezért is történhetnek meg rajtuk ezek a típusú csalások. Alapvetően már az is gyanús lehet, hogyha egy adott termék jelentősen olcsóbb, mint bárhol máshol, de hogyha a fizetési módok között kizárólag a kriptovalutás fizetés szerepel, akkor biztosak lehetünk benne, hogy a termék nem létezik, és csupán egy átveréssel van dolgunk.

Kriptobányászati csalások

A kriptobányászat önmagában nem egy csalás, hiszen szimplán annyit jelent, hogy az adott hálózat azon szereplői, akik a tranzakciókat elvégzik, a munkájukért cserébe jutalmat kapnak. Bárki lehet bányász, de ahhoz, hogy ez kifejezetten jövedelmező legyen, hatalmas számítási kapacitásra, vagyis sok számítógépre van szükség. A sok számítógép rengeteg pénzbe kerül, és ezt sokan nem szeretnék kifizetni, inkább olyan csaló programokat készítenek, amik az áldozatok számítógépére települnek, és a háttérben nekik bányásznak az áldozat számítási kapacitását felhasználva.

Ha a program jól van megírva, az áldozat gyakorlatilag semmit nem vesz észre az egészből, mert amikor szükség van a számítógép erőforrásaira, akkor minimalizálja magát, a háttérben csupán akkor bányászik, amikor az nem feltűnő.

Intő jele lehet, hogy ilyen típusú támadás áldozatai lettünk:

- ha a számítógép bekapcsolt állapotban van, de használaton kívül is hangosan hűti magát
- ha a villanyszámlánk indokolatlanul megnövekszik, vagy ha a számítógép teljesítményében jelentős lassulást veszünk észre

Hamis Initial Coin Offeringek

Az ilyen típusú átverések rendszerint egy új kriptovaluta meghirdetésével kezdődnek. A valós kriptók esetében is gyakori finanszírozási forma az elsődleges coin kibocsátás (Initial Coin Offering), aminek a lényege az, hogy a befektetők a valuta életciklusának egy korai fázisában vásárolhatnak belőle, ezzel támogathatják a fejlesztőit, mindezt a jövőbeli magas hozam reményében.

Hamis esetben viszont a csalók nem létező, vagy létező, de téves információkkal ellátva hirdetik meg a projektjüket, ezzel csábítva befektetőket magukhoz. Hogyha pedig elérték az általuk összecsalni kívánt pénzösszeget, akkor nyom nélkül eltűnnek a befektetők pénzével. Ez történt például a Modern Tech esetében is, akik a Pincoin nevű kriptovalutájukkal nagyjából 660 millió dollárt loptak el 32 000 befektetőjüktől.

Mindenképpen érdemes tehát befektetéskor alaposabban utánajárni az adott kriptovalutának.

Intő jel lehet:

- ha irreális hozamot ígér a projekt
- ha nem megfelelően van dokumentálva
- ha ködösítenek
- ha nem tiszta ki vagy kik állnak a projekt fejlesztése mögött

Kihagyhatatlan üzleti lehetőségek

Ez a csalás típus talán a leggyakoribb, ebből fakadóan rengeteg formája létezik, de általában úgy kezdődik, hogy egy hamis kriptoguru felkeres egy üzleti lehetőséggel. Egy különleges, és kihagyhatatlan pénzkeresési módszert javasol, ami nem megterhelő, és kifejezetten jól lehet vele keresni.

A módszernek rengeteg féle verziója van, a csalók néha csak azt szeretnék, különböző Instagram oldalakat kövessünk be, majd fényképpel igazoljuk, hogy ezt megtettük. Előfordul, hogy egyszerűen azt állítják, a nekik elküldött kriptónkat pár nap alatt megtöbbszörözik. Van, hogy valós munkát végeztetnek velünk, azonban azt állítják, hogy ahhoz hogy ki tudjanak fizetni minket, előbb egy kisebb befizetésre van szükség a mi oldalunkról. A legsúlyosabb esetben a megtévesztésünk érdekében kezdetnek valóban vissza is küldenek nekünk kisebb nyereségeket, annak a reményében, hogy a kezdeti sikereken felbátorodva nagyobb összegeket is rájuk bízzunk, de mindezt csupán azért teszik, hogy előbb-utóbb eltűnhessenek a nekik adott pénzünkkel.

Nem is feltétlenül kell, hogy üzleti ajánlatot tegyenek, esetenként ugyanis social média hírességeket, vagy jól ismert nagyvállalatok vezérigazgatóit megszemélyesítve, deepfake technikákkal scam giveaway-eket, azaz ajándékozásokat (scam giveaway) hirdetnek. Ezekben az esetekben a leggyakrabban egy **adathalász oldalra irányítják tovább az áldozatokat**, ahol ellopják a személyes adataikat. (A deepfake-ről tájékozódni vágyóknak ajánljuk, az erről szóló jelentésünket, ami ITT érhető el a honlapunkon.)

Ponzi-sémák

Ezek a módszerek nagy múltra mutatnak vissza a pénzügyi csalások történelmében, a kihagyhatatlan üzleti ajánlat egyik specifikus típusai. Hagyományosan nem a kriptovalutákhoz köthetőek, de mivel azok anonimitásuk miatt megkönnyítik a csalók dolgát, és a **technikai komplexitásuk búvóhelyként szolgál a csalóknak**, ezért a mai világban leginkább már csak kriptovalutákkal alkalmazzák őket.

A lényege az, hogy a befektetőiknek **irreálisan magas hozamot ígérnek**, ezzel becsábítva őket a rendszerbe. Általában nagy kultuszt, hatalmas médiakampányokat szerveznek maguk köré, miközben ideális befektetési lehetőségnek mutatják magukat. A régi befektetőket az elején valóban kifizetik, mégpedig az új befektetők által befizetett összegekből, akik mivel valóban gyarapodtak anyagilag, „hiteles" forrásként tovább hirdetik a projektet, és a legtöbb esetben maguk sem tudják hogy az átverés részei. A probléma akkor következik be, amikor a rendszer már nem tud új befektetőket szerezni, és így nem tudják kifizetni a régi befektetőket, ezért az egyszerűen összeomlik. Ilyenkor rendszerint a tulajdonosok **az összes jelenleg bent lévő pénzzel nyomtalanul eltűnnek**, temérdek megkárosított befektetőt hagyva maguk mögött.

Romantikus csalások

Rendszerint a csaló ilyen esetekben megpróbál hozzánk érzelmileg közel kerülni, és az érzelmeinkre hatva, mondva csinált indokokkal pénzt kicsalni tőlünk. Gyakori, hogy a pénzt kriptovalutában kérik a lenyomozhatatlanságuk megőrzése érdekében. Az erről szóló CTI jelentésünk ITT érhető el.

AI csalások

Vitathatatlan, hogy a mesterséges intelligencia-alapú technológiák (pl. ChatGPT) 2023 egyik legfőbb témája volt. A technológia körüli felhajtás miatt rengeteg ember valamiféle varázstechnológiának gondolja, ami csodákra képes. A „meggazdagító" AI-kat hirdető csalók pont ezt a hiszékenységet használják ki. Rendszerint azt állítják, hogy az általuk kínált mesterséges intelligencia az emberi tévedések/érzelmi érintettség hiánya miatt automatikusan sokkal nagyobb sikerrel kereskedik helyettünk. Nekünk mindössze annyi a dolgunk, hogy várakozunk, amíg megfelelő hozamot nem ér el a befektetett pénzünk után. **Ezek azonban minden esetben átverések, és valójában a pénzünk vagy adataink ellopása céljából készültek.** Gondoljuk csak végig, ha létezne ilyen mesterséges intelligencia, azt mégis miért árulná bárki? Azzal csupán annyit érne el az illető, hogy gazdasági versenytársakat generálna magának, ezzel a saját bevételét csökkentve.

Hazai trendek

KiberPajzs partnerünk, az Országos Rendőr Főkapitányság tájékoztatása szerint 2022. évtől kezdődően Magyarországon kiemelkedő tendenciaként jelentek meg azon bűncselekmények, amelyek az áldozatok kriptovalutáit célozták. Ezen bűncselekmények a 2023-as évben megtöbbszöröződtek.

Elkövetési módszerek

Az alábbi két tipikus módszer figyelhető meg:

1. Kisebb számú esetekben a sértett tárcájának privát kulcsához **ismeretlen személy, ismeretlen módon hozzáférve átutalásokat hajtott végre**.

2. Az elkövetők egy **kriptovaluta befektető cég nevében követik el bűncselekményeiket**. A megtévesztés hatékony végrehajtása érdekében alkalmaként valódi céget alapítanak a tevékenységük leplezése érdekében, amelyhez gyakran hoznak létre egy megnyerő, megbízhatóságot sugalló weboldalt is. Cégalapítás tekintetében kedvelt helyszín az elkövetők által kedvelt helyszín a karib-térségi Saint-Vincent és a Grenadine-szigetek fővárosában található székhelyszolgáltató tekintettel arra, hogy ezen országban semmilyen kriptovaluta pénzügyi felügyeleti szervnek nincsen hatásköre.

A csalók elsődleges kapcsolatfelvételi platformja a csalóknak a Facebook Messenger, azonban előszeretettel fizetnek Facebook hirdetésekért tevékenységeik optimalizálásáért. Robotokkal érik el, hogy a csaló oldalak a Google keresési találatok között minél előbb szerepeljenek, ezáltal azt érik el, hogy a sértettek hogy a sértettek „maguk találjanak rá" a kedvező befektetést hirdető cég weboldalára.

Célpontok

Az eddigi tapasztalatok tekintetében a sértetti körökben korosztálytól függetlenül mindenki megtalálható, azonban legnagyobb számban az idősebb korosztály esik áldozatul. A fiatalabbak körében jellemzően előfordulnak olyan esetek is, amikor népszerű társkereső oldalakon hamis felhasználói fiókok mögé rejtőzött csalók javasolják a befektetést a társkeresőknek.

A folyamat

A használt technikákban, történetekben és kisebb részletekben előfordulnak eltérések az egyes esetek között, de általánosan elmondható, hogy a következő főbb pontok az ilyen jellegű csalások nagy százalékában megtalálhatók.

1. A sértettnek regisztrálni kell az elkövető weboldalán, ahol meg kell adnia a nevét és a telefonszámát.

2. Az elkövetők telefonon felveszik a kapcsolatot a sértettel, amelyet presszionálás és ösztönzés követ a befektetések végrehajtása érdekében.

3. Az elkövetők többnyire hagyományos fiat valutákkal történő kisebb befizetéseket kérnek egy befektetési számla megnyitásához. Ez a befizetés átutalással vagy bankkártyával történő vásárlással egy külsős oldalon megy végbe. Egy valódi cég látszatát keltve egy pénzintézettel is szerződést kötnek azért (például: Spencer and Stanley), hogy az elkövetéshez használt weboldalon közvetlenül lehessen bankkártyával fizetni.

4. Az első összeg befizetése után az elkövetők további befektetésre veszik rá a sértettet, illetve ha a sértett ki kívánja venni az általa befizetett összeget, akkor különböző legendák mellett további összegeket kérnek befizetésre.

5. Az elkövetők a téves tudat további erősítéséhez és további fizetésekre történő rábírás érdekében az általuk üzemeltetett weboldalon a sértettek részére saját személyes fiókot hoznak létre, ahol láthatják, hogy a befektetésük már mekkora – jellemzően nagy mértékű – hozamot hozott. Arra vonatkozóan nincs bizonyíték, hogy az elkövetők által üzemeltetett oldalon valódi, pénzügyi tevékenységből származó adatok láthatók, de feltételezhető, hogy azt ők maguk szerkesztik megtévesztés céljából.

6. A kezdőösszeg befizetését követően ráveszik a sértettet egy **exchange** (kereskedő) számla nyitására valamelyik népszerű kripto kereskedő oldalon (pl Binance, Coinbase), ahol a sértettnek a pénzéből kriptovalutát (jellemzően Bitcoint vagy Ethereumot) kell vásárolnia és átutalnia az elkövető anomim hot tárcájába.

7. A csalók az informatika terén nem jártas sértettek részére segítséget is nyújtanak oly módon, hogy ráveszik, hogy töltsék le az installálást nem igénylő, **Anydesk nevű asztali megosztó program**ot, amin keresztül rácsatlakoznak a sértettek számítógépére, és az elkövetők végeznek el minden regisztrációt és tranzakciót. Ebben az esetben a sértettnek csak el kell küldenie az elkövető részére a személyes adatait és személyigazolványának fényképét az exchange számla megnyitásához, illetve átutalásnál/vásárlásnál csak engedélyezni kell azokat a bankjánál.

8. Az anonim tárcából további anonim tárcákba hajtanak végre utalásokat, jellemzően a sértettől származó kripto összeget más – feltehetően bűncselekményből származó– összegekkel összemosva. A felderítés nehezítése érdekében több tucat, akár több száz anonim tárcába is történhet utalás, mielőtt valódi fizetőeszközökre megtörténne a kriptovaluták átváltaása.

A nyomozás

Egyes bűncsoportok a Spencer and Stanley hamis kriptobefektető cég esetén is több tucat anonim tárcát használnak. Egy nem megnevezett elkövetői csoport egyik exchange tárcája az Egyesült Arab Emírségekben található bybitnél van vezetve, amelyen 2024.01.31. napig bezárólag közel 1 milliárd Ft-nak megfelelő – feltehetően bűncselekményből származó – összegű Bitcoin kriptovaluta fordult meg.

A kereskedő tárcák regisztrálásához ügyféladatokra, KYC dokumentumokra van szükség, azonban jellemzően ezen fiókokat strómanok nevére nyitják.

A fentiek miatt ezen bűncselekményekben érintett pénzösszegek visszaszerzése nem garantálható egyértelműen, mivel azok más, feltehetően bűncselekményből származó jelentős méretű pénzösszegekkel összemosásra kerülnek, így kétséget kizáróan nem állapítható meg, hogy a sértettől származó összeg pontosan melyik tárcába került átutalásra és mikor ki által került felvételre.

Anonim hot vagy cold tárcából történő lefoglalás legnagyobb sikerrel csak akkor kivitelezhető, ha annak birtokosa más módon már azonosításra került, és realizálás, illetve kutatás során megtalálásra kerül a tárca privát kulcsa, amelyet felhasználva az összeg átvezethető a hatóság által létrehozott exchange számlára.

A nyomozást nehezíti az is, hogy a csalók jellemzően az amerikai Cloudfare fordított proxyszolgáltatót használják a valódi IP címük elrejtése érdekében, illetve a weboldalaikhoz tartozó domain neveket anonimitást biztosító amerikai cégeken (pl. NameCheap, Porkbun) keresztül regisztrálják.

Külföldi domain nevek felderítése tekintetében rövidtávon azonban várható előrelépés a nemzetközi IP címek kiosztásáért felelős ICANN szervezet kezdeményezése miatt, amely keretében létrehoztak egy online adatkérési felületet, amelyre magyar hatóság tagja is regisztrálhat önállóan.

A nyomozásokat ezen csalások tekintetében tovább nehezíti az is, hogy az elkövetők rendszerint külföldön tartózkodnak ismeretlen helyen és digitális lábnyomaikat álcázzák virtuális magánhálózati szolgáltatók segítségével.

Elkövetési módszer vonatkozásában előfordul a külföldi bűncsoportok esetében, hogy olyan személyeket is beszerveznek, akik anyanyelvi szinten beszélnek magyarul, így még hitelesebbek tudnak maradni a tevékenységeik során.

Egyes esetekben előfordul az is, hogy a „befektetések" mellett piramis játékhoz hasonlóan az elkövetők a sértettek részére különböző szinteket hoznak létre, amely alapján minél magasabb szintre kerül, annál magasabb „hozamot" vehet ki. A szintek közötti lépéshez további – kriptovalutában történő – befizetés szükséges.

Összefoglaló

- Ingyen pénz nem létezik. Senki sem fog ingyen kriptovalutát ajánlani, és varázslatos mesterséges intelligencia sem létezik, ami egy éjszaka alatt megtöbbszörözi a vagyonunkat. Ha valaki ilyennel kecsegtet, szinte biztosak lehetünk benne, hogy átverés részesei vagyunk. **Legyünk szkeptikusak!**

- Befektetéskor több forrásból tájékozódjunk, és mindig tartsuk észben, hogy bármilyen befektetés - de különösen a kripto - nem játék, és legrosszabb esetben pár kattintással az egész vagyonunkat elveszíthetjük. Kerüljük a hypeot, vegyük észre, hogyha egy projekt körül túlzottan nagy a felhajtás!

- Soha, semmilyen körülmények között **ne adjuk meg másnak a kriptovaluta pénztárcánk belépési adatait**! Ha valaki elkéri tőlünk, akkor egy csalóval van dolgunk!

- Mindig végezzünk alapos kutatást! A kriptovaluta piac és technológia óriási sebességgel fejlődik, változik, ezért fontos hogy napra készek legyünk! Tájékozódj a témát érintő törvényekről is!

- Csak megbízható és jól ismert kriptovaluta-tárcákat, és tőzsdéket használjunk! Pénz küldésekor ellenőrizzük pontról pontra, hogy a tranzakció részletei pontosak-e, mielőtt megerősítjük őket!

- Ha mindenképpen nagyobb mennyiségű kriptovalutát szeretnénk tárolni, akkor használjuk az internetre nem csatlakoztatott cold walleteket!

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2024