

ELEVEN MÁRK

A VIRTUÁLIS VALUTÁK FELHASZNÁLÁSI LEHETŐSÉGEI EGYES BŰNÖZŐI KÖRÖK SZEMPONTJÁBÓL

(KÉZIRAT)

ABSZTRAKT

A köznyelvben csak „kriptovalutaként” emlegetett fizetőeszközök a közelmúltban igencsak nagy népszerűségnek örvendtek és mindmáig létező unkonvencionális fizetési eszközök. Viszont, mindamellett, hogy a fejlesztők a jövő mesés ígéretével és a bankoktól, az államtól való teljes függetlenséggel és a teljes egyenlőséggel kecsegtetnek, történetük során nyilvánvalóvá vált, hogy ezek sokkal inkább alkalmasak a bűnözők gyors, nemzetközi, lenyomozhatatlan fizetési eszközeinek, mint maguknak a fő célcsoportként kijelölt magánembereknek. E tanulmányban különböző bűnözői körök szempontjából kerül ismertetésre néhány már eddig feltárt, vagy lehetséges, az állam szempontjából hátrányos felhasználási mód.

BEVEZETÉS

A virtuális valuták kétségkívül az elmúlt évek egyik világszerte robbanásszerűen növekvő népszerűségű új típusú digitális fizetőeszközei. Azonban annak ellenére, hogy milliók használják, még mindig nem tudjuk őket teljesen megérteni,¹ állandóan változó kétes természetük miatt, még csak egységes jogi szabályozás se létezik, sem mindegyik országon, sem pedig nemzetközi szinten. Márpedig hasonlóra mindenképpen szükség lenne, mivel számos kiváló lehetőségét biztosítanak például a bűnözők és terroristák illicit pénzzel kapcsolatos tevékenységeihez, emiatt pedig egyértelműen több szempontból is találkoznak a nemzetbiztonság kérdéskörével, súlyosan veszélyeztetve azt. A továbbiakban némileg interdiszciplináris vizsgálat alá kerül a virtuális valuták néhány felhasználási formája az egyéni-, szervezett és kiberbűnözők részéről.

A VIRTUÁLIS VALUTÁK, MINT PÉNZMOSÁSI ESZKÖZÖK

¹<https://hackernoon.com/ten-years-in-nobody-has-come-up-with-a-use-case-for-blockchain-ee98c180100>
(Utolsó letöltés: 2018.04.25.)

A virtuális valuták egyelőre kétségtelenül kiváló eszközként funkcionálhatnak a pénzmosás területén, hiszen az utóbbi években a kereskedelmük rendkívüli módon felfutott, széles és folyamatosan változó a választék (mind a mennyiséget, mind a specifikációkat illetően), a nemzetközi térben könnyű őket gyorsan mozgatni, anonimitást biztosítanak, a hatóságok nincsenek felkészülve technikailag kellően rájuk (eddig inkább csak a Bitcoin-ra fókuszáltak), bűncselekmény észlelése esetén nem tudnak kihez fordulni információkérés és a vagyon zárolása érdekében, több országban kell engedélyeztetni a nyomozást és nincsenek egységes szabályozások se a valutákat illetően, nem sikerült még kellően definiálni őket.

A pénzmosás, mint klasszikus bűncselekmény, maga általánosan egy olyan folyamat, amelynek során a bűnözők, bűnözői körök az illegális forrásból – jellemzően bűncselekményből - származó jövedelmek azonosíthatóságát megkísérik ellehetetleníteni és a folyamat végén a jövedelmet legális forrásból származónak feltüntetni. A folyamat szoros összefüggésben van a gazdasági szférával, hiszen a folyamat végén jövedelem képződik nem törvényes úton ezzel pedig a tisztességes piaci tevékenységet folytató gazdasági szereplők közé indokolatlan piaci hátrányt keletkeztet. Az IMF egy nem is olyan korábbi becslése szerint a pénzmosás volumene a Föld összes országa egyesített GDP-nek 2-5%-át teszi ki.

A pénzmosási-folyamatot a legjobban az Egyesült Államokból eredeztethető háromfázisú modellel szokás leírni. E szerint sorban megkülönböztethető: elhelyezési-szakasz, rétegzési-szakasz és végül integrálási-szakasz.

Az elhelyezés szakaszában a készpénz elválik az alapbűncselekménytől és a pénzügyi szervezethez kerül. Ez a legrövidebb szakasz, valamint itt lehet a legnagyobb eséllyel felfedezni a cselekményt. A legtöbb virtuális valuta esetében azonban nincs könnyű dolga a hatóságoknak, hiszen akár a Bitcoin, akár más valuták már nagyon egyszerűen konvertálható a valuta hagyományos pénzből virtuális pénzzé és ez visszafelé is igaz. Az ilyen műveletekre „hivatalosan” körülbelül 12-13 ezer hely áll rendelkezésre egyelőre világszerte, de ezek száma rohamosan növekszik, nem beszélve a nem hivatalos váltásokról, amelyek száma ezeknek a több száz, vagy ezerszerese is lehet. Ráadásul az egyes értékhatárokat kijátszandó, gyakran alkalmazott, bevett módszer az úgynevezett struktúrálás is, amely tovább rontja az esélyeket a felderítésre, de ezt is el lehet kerülni, ha olyan személyek kerülnek a rendszerbe, akik nem is jelentik a gyanús eseteket. Mivel sok országban, köztük a már említett Romániában is sok a digitális valutaváltó, ugyanakkor ott rendkívül magas a korrupció a hatóságok körében is könnyen ki lehet ezeket az előnyöket használni.

A második, rétegzés (vagy bújtatás) szakaszban az illegális jövedelem elválik a forrástól. A bevételeket úgy rejtik el, hogy a jövedelem megszerzője, valamint a

bűncselekményből származó összeg felderíthetetlen legyen, a pénz útja követhetlenné válik, belépnek az Off-shore szereplők, pénzintézetek. Ezt virtuális valutáknál elősegíti, hogy a tranzakciók P2P-k, anonimak (valutánként változó mértékben), nem mennek át központilag szabályozott közegen, ahol felfigyelnének rájuk, a hozzáértés különösebb ismerete nélkül képesek követhetetlen tranzakciók egyszerű és gyors lebonyolítására.

A harmadik integrációs szakasz a legalizálás részmozzanata, amelynek segítségével a pénzmosó igazolni tudja a keletkezett vagyon legalitását. Ebben a szakaszban kerül vissza a bűncselekményből származó vagyon a tisztességes gazdaságba. Az azonosítás ebben a szakaszban már szinte lehetetlen. A virtuális valuta itt már maradhat virtuális formában, tovább vándorolhat a virtuális közegben a valós, vagy nem valós felhasználók között, vagy ismételten hagyományos formát ölthet a váltók révén, de központi felügyelet híján nem fog senki számára gyanút kelteni a pénzösszeg nagysága. További fontos tulajdonsága a virtuális valutáknak, amelyet ebben a szakaszban érdemes vizsgálni, hogy vannak olyan valuták, amelyek helyettesíthetők (Monero) és vannak olyanok, amik nem (Bitcoin). Vagyis abban az esetben, ha a nyomozóhatóság hozzáfér a főkönyvhöz, visszafejti azt, láthatóvá válik a „piszkos” pénz útja, tehát hogy melyik valuta kitől származik és így a konkrét személyhez való konkrét összeg kötése jobban hozzájárul az illegális pénzforgalom kiszűréséhez. Ami apró bizakodásra adhat okot, hogy a NAV egy munkatársa megerősítette, hogy 6 szoftver már a nyomozóhatóság látókörébe került és ebből 3 eredményesen tudja felderíteni a pénz útját a hálózaton, de ez csak a Bitcoin-ra érvényes, a többi 1500+ valutára nem. Ilyen forenzikus szoftverek és megoldásokat kínál egyéként az Elliptic és a Chainalysis is. A nyomozás és visszakövetés tehát legfőképpen a Bitcoinnál lehetséges, így ez az eljárás erősen korlátolt. Az így tisztára mosott pénzösszegeket pedig további pénzmosási eljárásoknak is alá lehet vetni, hogy be legyen biztosítva a siker (példul: elkönyvelik egy cég bevételeinek növekedéseként, szerencsejátékokba fektetnek, majd kiveszik nyereseményként az összegeket, ékszereket vásárolnak stb.)

A Bitcoin (és egyébként virtuális valuta) alapú pénzmosás minden kétséget kizárólag nemcsak elméleti szinten működik. 2016. januárjában már a holland hatóságok letartóztattak 10 személyt ezzel összefüggően egy összehangolt nemzetközi nyomozás keretében.² A csoport, bár Ausztráliában, Egyesült Államokban, Litvániában, és Marokkóban is tartott fent Bitcoin és hagyományos számlákat végül olyan amatőr módon bukott meg, hogy egyes bankoknak gyanút keltett az, hogy nagy összegű pénzek jelentek meg a csalók számláin, amiket szinte azonnal készpénzben ki is vettek. Mindazonáltal, attól függetlenül, hogy a holland hatóságok sikeresek

² <https://uk.reuters.com/article/us-netherlands-crime-bitcoin/dutch-arrest-10-men-suspected-of-using-bitcoin-to-launder-money-idUKKCN0UY0V8> (Utolsó letöltés: 2018.04.25.)

voltak, nem jelenti azt, hogy minden virtuális valuta csalás így fog véget érni, sőt azt is mondhatjuk, hogy az igazi küzdelem még csak most kezdődik, ugyanis mára nemcsak a hagyományos pénzmosási módszerekre kell figyelni, hanem számtalan új is megjelent a kriptovalutákkal összefüggésben.

Kiváló pénzmosási rendszernek mutatkozik a BitPay, Coinbase, Braintree és a Circle is. Kezdetben a Bitcoin egyik nagy hiányossága volt, hogy kevés helyen lehetett vele fizetni. Ezt felismerve ez a négy cég lehetővé teszi, hogy egyrészt Bitcoin fedezettel lehessen fizetni hagyományos pénzformákban meghatározott árukért, másrészt, hogy hitelkártyáért cserébe lehessen Bitcoin-t vásárolni. Ez már önmagában aggályos, hiszen itt már látható, hogy kiváló lehetőség nyílik a pénzmosásra, de az a bevezetendő koncepció, amely szerint a cégek hamarosan olyan hitelkártyákat is elfogadnak Bitcoin vásárlása céljából, amelyeket készpénzzel előre kifizettek csak tovább súlyosbítja ezen rendszerek illegális felhasználási lehetőségeit, tekintve, hogy egy személy akár több ilyen kártyát is birtokolhat, több identitással rendelkezhet.

A virtuális pénzváltók kérdése is elég aggályos a virtuális valutákra alapozó pénzmosási folyamatok nyomonkövetősége szempontjából. Olyan oldalakon keresztül, mint a Kraken, vagy a BTC-E kiváló lehetőség nyílik a virtuális valuták közötti akadálytalan átváltásokra és ezzel a bűnözői körök csak jobban bebiztosítják magukat. A BTC-E működését az amerikai hatóságok egyébként már a múlt évben felfüggesztették ezen a pénzmosási okokból kifolyólag, de WEX néven újra elérhető.

Pénzmosási lehetőséget kínálnak a Coloured Coin-ok is a Virtuális tőkepiacon. Ez egy olyan virtuális valuta típus, amely valódi vagyontárgyak képviseltére és kezelésére szolgál a Bitcoin blokkláncon. Ennek a koncepciónak az alapja, hogy a Bitcoin blokklánc nem csak tranzakciós adatokat képes tárolni, hanem valamekkora mennyiségben META-adatok tárolását is lehetővé teszik, ennek segítségével pedig ugyanúgy átruházhatók értékpapírok, részvények, tulajdonjogok stb., mintha valuta tranzakciók lennének. Erre az elvre és a Coloured Coin-ok népszerűsítésére már külön szolgáltatások is indultak, ilyenek a Chromaway és a Colu, illetve a Hedgy, amely a Bitcoin közösséget érintő áringadozásokat hivatott mérsékelni. Lehetséges a hordozókötvények kereskedelme is és mivel ezeket a kötvénytípusokat, amelyeket általában egy vállalat, vagy kormány bocsát ki, nem szokás nyilvántartásba venni ezért csak azok a tulajdonosai, akiknek a birtokukban. Ez pedig már önmagában nagyfokú anonimitást biztosít, nemhogy akkor, amikor bekerül egy ugyancsak anonimitást biztosító virtuális valutarendszerbe. Így ez biztosan nyomonkövethetelen pénzmosási módszer a bűnözők számára.

Egy másik kérdés a nemesfémalapú virtuális valutakereskedelem. Ilyen szolgáltatók a BitGold és a Goldmoney is. A nemesfémek a kereslet, a likviditás és a könnyű átruházhatóság miatt amúgy is kedvelt eszközei a pénzmosási műveleteknek és azok után, hogy gazdát cseréltek, beolvasztásra kerültek stb. gyorsan eltűntetik maguk után az árulkodó jeleket.

Megint csak egy másik aggasztó kérdés az MMORPG-en (Massively Multiplayer Online Role-Playing Games – Tömeges többjátékos online szereplőjátékok) keresztül történő pénzmosás. Ezekben a népszerű, több millió felhasználóval világszerte bíró játékokban, mint a Second Life és a World of Warcraft gyakoriak a fizetős tartalmak, valamint, hogy a játékosok egymással kereskednek. Éppen ezért kiemelkedő és kézenfekvő lehetőség nyílik a virtuális valuták egymás közötti, gyanútlan és zavartalan kereskedelmére, ráadásul a folyamat nagyon egyszerű és hatásos, hiszen a játékokban is vannak saját pénznemek, amikért virtuális valutákkal fizetnek, valamint a bűnözők a platformok között gyorsan tudnak mozogni. Éppen emiatt az FBI már korábban, 2011-ben nyomozásokat rendelt el és szakcionálta a World of Warcraft gyártóját, a Blizzardot is.³A lehetőség persze még mindig adott és nem csak ez a két online játék bír óriási online felhasználótáborral napjainkban.

Összefoglalva tehát a sok kínálkozó pénzmosási lehetőségéből látható, hogy hiába az a kevéske hatósági intézkedés és siker is, mivel a virtuális valuták és a pénzmosás kapcsolata csak egyre szorosabb és mélyebb lesz, az ezt feltérképezni és szabályozó szándékozó szervek pedig gyakorlatilag olyan helyzetben vannak, mint a Danaosz király lányai, akik a görög mitológia szerint az alvilágban arra kárhoztattak, hogy egy állandóan lyukas hordót próbálnak vízzel megtölteni az örökkévalóságig.

A VIRTUÁLIS VALUTÁK, MINT A CSALÁS ESZKÖZEI

A virtuális valutákkal kapcsolatos csalásoknak eddig még meg nem ismert számtalan módja létezhet, így ebben a részben a két leggyakoribbat, a ICO-kat és a váltási csalást fogjuk nagyon röviden bemutatni.

A csalás elkövetésének egyik a virtuális valutákhoz köthető lehetséges egyik új megoldás a ICO (Initial Coin Offering), vagyis a crowdfunding és a tőzsdei kibocsátás egy speciális keveréke. A crowdfunding közösségi tőkeági finanszírozást jelent, vagyis azok az oldalak, ahol a felhasználók pénzt adományozhatnak egy-egy ígéretesnek tűnő ötletre és ha ez beindul akkor mindenki jól jár, a támogatók és a támogató is. Ezzel ellentétben az ICO már

³ <https://www.computerworld.com/article/2471127/endpoint-security/intelligence-agencies-hunting-for-terrorists-in-world-of-warcraft.html> (Utolsó letöltés: 2018.04.25.)

nagyon kockázatos, mivel itt gyakorlatilag arról van szó, hogy egy virtuális valuta létrehozója gyűjt tőkét a valutakibocsátáshoz, cégépítéshez. A virtuális valuták spekulatív jellegéből és nagy kínálatából adódóan viszont nagyon kicsi annak az esélye, hogy ezek a projektek megvalósulnak, a befektetők pedig csak nagyon nehezen és hosszú idő után profitálhatnak ebből, feltéve ha profitálnak. Ugyanis nincs bebiztosítva, hogy a projekt kivitelezője időközben lelép a befektetett összegekkel, ahogyan azt tette a népszerű crowdfunding oldalon, a kickstarteren egy magyar „okos kerékpár csengő” a Shoka Bell fejlesztője 2018. januárjában 50 millió forinttal.⁴ Az egyik legismertebb ICO egyébként a SWARM.

Végezetül a csalás egy másik lehetséges módja lehet, és amelyre ugyancsak akadt már magyar példa is, hogy egy adott személy fix árfolyamon kínálja fel váltásra a virtuális valutát, majd mikor a gyanútlan személy átutalja az összeget a készpénz, vagy más valuta váltása előtt a csaló bármilyen kifizetés nélkül eltűnik a megszerzett összeggel. A nyomozást itt is nehezítheti a már említett probléma, mégpedig, hogy a virtuális valutának nincs felügyeleti szerve, nem vonható vissza a tranzakció és nem zárolható a virtuális valutából származó jövedelem, így, ha az összeget tovább utalják nehézkes annak felderítése.

A VIRTUÁLIS VALUTÁK LEHETŐSÉGEI A KIBERBŰNÖZŐK SZEMSZÖGÉBŐL

A legtöbb transznacionális kérdéshez hasonlóan, a kibertérben zajló konfliktus nem teljesen új, bár az elmúlt húsz több átalakuláson ment keresztül és ez a tendencia manapság is rohamosan zajlik,⁵ nemzetbiztonsági kihívások számtalan változatát felvonultatva a szakemberek és a hatósági szervek irányába.

Vitathatatlan tény, hogy a virtuális valutákkal kapcsolatos összes művelet (, bányászat, tranzakciók, tárolás stb.) ezen fizetőeszközök sajátos jellegéből adódóan a bárki számára elérhető kibertérben, a „vadonban”, valamint számítógépeken és okoskészülékeken megy végbe, meggátolhatatlan, hogy bármelyik szakaszban legyen a kiberbűnözők számára. Ami pedig rendkívül aggasztó, hogy a kiberbűnözői körök pedig nemcsak saját maguk számára kovácsolhatnak az egyes támadásokból előnyöket, hanem bedolgozhatnak például terrorista szervezeteknek, titkosszolgálatoknak, kormányoknak, vagy más hagyományos bűnözői köröknek is, a támadások pedig nemcsak pénzszerzésre irányulhatnak. Segítségükkel további más információk gigantikus mennyiségét lehet megszerezni, hátsó kapukat lehet nyitni

⁴ <https://qubit.hu/2018/01/29/tombolnak-a-befektetok-a-kickstarteren-hiaba-dobtak-ossze-200-000-dollar-se-hire-se-hamva-a-forradalmi-magyar-okoscseengonek-a-shoka-bellnek> (Utolsó letöltés: 2018.05.01)

⁵ MARK M. LOWENTHAL: *Hírszerzés – A titoktól a politikai döntésig*. Antall József Tudásközpont, Budapest, 2017. p. 416.

nemcsak a felhasználók gépein is, hanem akár kritikus infrastruktúrákon is, valamint igénybe lehet venni ezen eszközök erőforrásait, a felhasználók tudta nélkül. Ezek miatt, a magas (gyakorlatilag meghatározhatatlan) számú és kimenetelű kockázatai lehetőségek miatt, valamint az egyre leleményesebb kiberbűnözők és az exponenciálisan növekvő virtuális kiemelten fontos tanulmányozni a virtuális valuták ezen oldalát.

A továbbiakban bemutatásra kerülő veszélyforrások tükrében talán azt is elmondhatjuk, hogy az új típusú alternatív digitális fizetőeszközök nemzetbiztonsági kockázatait vizsgálva ez az egyik legfontosabb részfejezet lesz, bár a munka terjedelmi korlátai miatt csak a teljesség igénye nélkül, némi ízelítő formájában lehetséges bemutatni ezt. A legcélszerűbb vizsgálódási mód esetünkben, ha a virtuális valutázás folyamatát részekre bontjuk és ezeket vizsgáljuk meg a kiberbiztonsági sebzhetőségek tükrében. A részfolyamtokat két csoportra bonthatjuk, mivel vannak olyan felhasználók, akik bányászat útján is szerezhettek virtuális valutát és vannak olyanok, akik vásárlás esetén jutnak hozzá ehhez.

A FŐBB SEBEZHETŐSÉGI PONTOK A VIRTUÁLIS VALUTÁK KAPCSÁN

1. HARDVER (BÁNYÁSZAT ESETÉN)

A bányászati tevékenységhez az ehhez megfelelő eszközök széles skálája áll rendelkezésre a felhasználók számára. Három dolog az ami igazán lényeges, ha valaki ilyen tevékenységre vállalkozik: Ezek lehetnek hagyományos asztali számítógépek, hagyományos számítógépalkatrészekből házilag összeállított úgynevezett „rig”-ek, célhardverek, amelyeket speciálisan bányászatra terveztek, okostelefonok, szerverszámítógépek stb. Viszont minden egyes hardvernek, azok használatának megvannak a sajátos kockázatai.

Az asztali számítógéppel történő bányászat, amely a kezdetekkor még szélesebb körben volt elterjedt, legnagyobb kockázati tényezője, hogy a gyakran bárki számára nyílt forráskódú bányászati szoftvereken és a bányászati tevékenységgel összefüggően meglátogatott kétes oldalakon keresztül a kiberbűnözők hozzáférhetnek hozzá a számítógépen tárolt kényes személyes adatokhoz, felhasználónevekhez, jelszavakhoz stb. Természetesen ezt bányászat nélkül is meg lehet valósítani és a mindennapokban számtalan hasonló eset történik, de a bányászat tovább növeli ennek amúgy is magas esélyeit. Ez különösen magas nemzetbiztonsági kockázatot hordoz magában, főleg akkor, ha az adott személy kormányzati intézmény, vagy kritikus infrastruktúra fenntartásáért felelős szervezet alkalmazottja és rendszeresen „hazaviszi a munkáját”, mindemellett pedig a civil életben elkötelezett híve a virtuális valutázásnak.

A házilag, hagyományos számítógépalkatrészekből összeállított rig-ek szokás GPU alapú bányászként is emlegetni. Ennél a bányászati formánál a lényeg, hogy minél nagyobb bányászati sebességet érjenek el a lehető legkevesebb teljesítményre törekedve. A teljesítménycentrikus ház bányász számítógép felépítése merőben eltér a hagyományos számítógépektől. A lényeges elemek a tápegység, az alaplap és annyi nagyteljesítményű grafikus kártya, amelyet még az alaplap képes vezérelni, valamint a megfelelő hűtés. Persze ebben is helyet kap a RAM vagy a Processzor, de ezek kevésbé fontosak, mint az első három alkatrész.

Ezeknél a számítógépeknél kényes információ híján csak az okozhat igazán problémát, ha a támadó valamilyen úton-módon ezeken keresztül „felszivárog” egy olyan hálózaton található számítógépig, ami valóban tartalmaz kényes információkat. Amiatt viszont a hackernek könnyű dolga van, hogy itt nincsenek sem Antivirus programok, sem pedig olyan fejlett tűzfalak, mint a személyi számítógépeken. A számítógépek csak a már korábban említett nonce-ok keresésével vannak elfoglalva. Emellett ezek a rig-hálózatok, más dedikált hálózatokhoz hasonlóan, ugyanúgy funkcionálhatnak még kisebb-nagyobb botnet részeként, illetve adott esetben célzott DoS vagy DDoS támadáshoz is felhasználhatóak erőforrásként. A botnethez még annyit hozzáfűzhetünk, hogy már léteznek olyan eredményesen működő botnetek is, amik implementálnak bányászati képességeket is.⁶ Az egyik legismertebb ilyen botnet például az amúgy is rendkívül sokoldalú és emiatt ugyancsak rendkívül veszélyes Mirai botnet, amely nemcsak a számítógépekre és okos eszközökre jelent veszélyt, hanem a dolgok internetében elhelyezkedő ártalmatlannak tűnő eszközökre is.⁷ Ez további kellemetlenség lehet a felhasználók számára, hiszen a saját rig-eket (és bármelyik más eszközt) mások használják bányászatra, márpedig az utóbbi év végén már, botnet-től független általános jelenség a számtalan formában „testet öltő” cryptojacking, több millió más számítógépet is érintett.⁸ Ebben még egyelőre a témával foglalkozók inkább csak a felhasználói oldal sérelmeit tanulmányozzák, viszont azt nem szabad elfelejteni, sőt sokkal inkább kell szem előtt tartani, hogy ezzel a módszerrel a terrorista szervezetek és más bűnözői körök is óriási összegekhez juthatnak (vagy jutnak akár már most). Ugyanezek a hátrányok hozhatók fel a célhardveres bányászatnál is, mivel a számítógépek itt is csak az algoritmusokat fejtik és nem tárolnak

⁶https://index.hu/tech/2017/12/27/magyar_illegalis_mozis_oldal_bukott_le_azzal_hogy_a_nezok_gepeivel_kriptopenzt_banyasztat/ (Utolsó letöltés: 2018.04.25.)

⁷<https://securityintelligence.com/mirai-iot-botnet-mining-for-bitcoins/> (Utolsó letöltés: 2018.04.25.)

⁸<https://www.investopedia.com/news/hackers-target-computer-rigs-illegally-mine-cryptocurrencies/> (Utolsó letöltés: 2018.04.25.)

semmilyen lényeges információt. Ezeknél a számítógéptípusoknál a felhasználók vannak nagyobb veszélynek kitéve.

A szerverszámítógépes bányászatnál már egészen más a helyzet, főleg, ha a már személyi számítógép szakasznál látott kormányzati intézménynél, kritikus infrastruktúráért felelős szervezetnél dolgozó alkalmazottnál, esetleg rendszergazdánál jelentkezik az igény, hogy esetleg állami erőforrásokat igénybe véve gyarapítsa a virtuális vagyonát. Miért is alkalmasak a szerverszámítógépek, függetlenül attól, hogy kormányzati, vagy magánkézből vannak? A virtuális valutabányászat egy időigényes folyamat és a nagy teljesítmény és az üzembiztonság mellett, így a huzamos ideig történő rendelkezésre állás is szükséges a sikerhez. Ezek a tulajdonságok pedig a sokoldalú szervergépekben teljes mértékben megtalálhatóak. Egyedül talán az ár lehet az, ami a célhardverekkel szemben hátrányt jelent.

A bányászat efféle kivitelezésére konkrét példával is tudunk szolgálni a közelmúltból, amely igencsak extrém és nemzetbiztonsági relevanciával bír: 2018. februárjában egy orosz nukleáris kutatóintézetben az FSZB letartóztatott több kutatót is, mert az intézmény szuperszámítógépes infrastruktúráját használták fel Bitcoin-bányászatához. Abba még belegondolni is igen szörnyű, hogy milyen titkok szivároghattak ki esetleg ezáltal, illetve, hogy milyen „ajándécsomagok” érkeztek be az intézet hálózatába, főként annak tükrében, hogy például 2013-ban a Stuxnet-vírus milyen konkrét fizikai károkat okozott egy Iráni atomerőműben és mennyire döbbsentette meg ezzel a világ más országait is, akik eddig ilyen lehetőségekre nem is gondoltak.

Az orosz esetből két következtetést vonhatunk le: az egyik az, hogy az emberi mohóság a kötelességek ellenében nagymértékben befolyásolja a viselkedést, veszélyes cselekedetekre veszi rá, nemcsak az esetleg tapasztalan/tanulatlan személyeket, hanem még azokat a magasan képzett embereket is akiknek maximális tisztában kellene lenniük a munkájukból adódóan a felelősségi és kockázati tényezőkkel. A másik pedig az, hogy az eset kapcsán érdemes fokozottan odafigyelni és megelőzni a hasonló incidenseket a lehető legrövidebb időn belül, ugyanis ezekkel nem csak minősített, kritikus információk kerülnek veszélybe, hanem egyfajta közvetett üzenet is kinyilatkoztatásra kerül, mégpedig, hogy ezeken a hálózatokon esetleg más támadási módszerekkel is érdemes próbálkozni. Így ennek egy bizonyos időn belül újra ismételt súlyos következményei lehetnek.

Az okoskészülékekkel kivitelezett bányászat ugyancsak hasonló biztonsági kockázatokat vet fel, mint a személyi számítógépekkel és szervergépekkel kivitelezett bányászat. Az okostelefonok, tabletek manapság az iparágon belüli eszeveszett versenynek köszönhetően már megközelítik, sőt egyes csúcskategóriás készülékek esetében túl is

szárnyalhatják egy-egy alacsonyabb, vagy középkategóriás hagyományosabb számítógép kapacitásait, ezért sokszor már nem is telefonokról, hanem „kézi mobil” számítógépekről beszélhetnénk. Az Android és IOS platformokon is egyaránt rendelkezésre állnak már virtuális valuta bányász alkalmazások, amelyek az okoskészülékek kapacitásait erre a tevékenységre képesek összpontosítani (Android-on például a Bitcoin miner és a Crypto miner Pro, IOS-en a Crypto Coin Miner).

A probléma itt ismételt az, hogy nagyon sok az ismeretlen alkalmazás és a virtuális bányászatért rajongó felhasználók nem tekinthetők tudatosnak, nem néznek utána az egyes alkalmazások fejlesztőinek, illetve, hogy megint egy olyan készüléket használunk bányászatra, amelyen érzékeny információk nagy mennyiségét tároljuk. A gondok egyébként már itt is elkezdtek jelentkezni. 2018. februárjában már jelentek meg cikkek, hogy arról, hogy a Google Play Store-ban található alkalmazásokból legalább 19 titokban használja a készülékeket, főként a Monero rejtett bányászatára.⁹ Még ugyanebben a hónapban arról is napvilágra kerültek információk, hogy a Google az összes Chrome böngészőhöz készült kiterjesztést kitiltja a Chrome Store-ból, mert ezek sem teljes egészében a felhasználóknak bányásszák a virtuális valutákat, vagyis már itt is megjelent a Cryptojacking.¹⁰ De nem csak ilyen nyilvánvaló formái vannak az okoskészülékeken, a Trend Micro szakértői által felfedezett ANDROIDOS rejtett Monero bányász például nem igényel felhasználó általi hagyományos telepítést, magától is fertőz és szélsőséges esetben akár a meg is béníthatja az adott készüléket.¹¹ Itt tehát ismételt szembesültünk azzal, hogy nemcsak maguk a készülékek, azok egyes erőforrásai vannak veszélyben, hanem a felhasználók érzékeny adatai is.

Összefoglalva tehát megállapítható az, hogy a legnagyobb veszélyforrás a bányászati hardver megválasztásánál az, hogy az mennyire illeszkedik a mindennapi használatba, mennyire tartalmaz jelszavakat, felhasználóneveket, minősített adatokat stb. Viszont a kockázat mértékét maga a felhasználó is megnövelheti, főleg, ha minősített adatok kezelésével is foglalkozó kormányzati szervnél, kritikus infrastruktúráért felelős szervezetnél alkalmazott. Ekkor már igencsak fennáll a súlyos nemzetbiztonsági kockázat veszélye. Viszont ezek mellett a tényezők mellett nem szabad megfeledkeznünk arról sem, hogy bányásztól és kriptovalutáktól függetlenül minden ember alkotta szoftvernek, rendszernek, készüléknek

⁹ <http://www.alphr.com/security/1008522/google-play-store-apps-mine-cryptocurrency>
(Utolsó letöltés: 2018.04.25.)

¹⁰ <https://www.wired.com/story/google-bans-all-cryptomining-extensions-from-the-chrome-store/>
(Utolsó letöltés: 2018.04.25.)

¹¹ <https://securityaffairs.co/wordpress/70968/malware/hiddenminer-android-miner.html>
(Utolsó letöltés: 2018.04.25.)

alapvetően és elkerülhetetlenül számos más biztonsági sebezhetősége is van (nulladik napi sebezhetőség, hátsó kapuk stb.), ezek pedig csak utólag derülnek ki, jobb esetben a fejlesztők által kiadott javítások, rosszabb esetben pedig óriási károkat okozó támadások révén. A bányászattal kizárólag csak fokozni lehet ezeket a veszélyeket.

2. PÉNZTÁRCA (BÁNYÁSZAT ÉS VÁSÁRLÁS ESETÉN)

A pénztárca elengedhetetlen eszköz a virtuális valuták birtoklásához, hiszen ide érkeznek a vásárlás, vagy bányászat útján megszerzett valuták, valamint innen indulhatnak ki és érkezhetnek be a tranzakciók, itt zajlik tehát maga a tárolás. A virtuális valutázás szempontjából ez a legkritikusabb állomás, hiszen az ezt birtokló személy rendelkezik az ebben tárolt összegekkel és ha e felett valaki jogellenesen átveszi az irányítást nincs kihez segítségért fordulni a központi igazgatás hiánya miatt.

A jellegük szerint többféle pénztárcát különböztethetünk meg. Például ha a pénztárca csatlakozik az internethez akkor beszélünk „Hot Wallet”-ről, ha pedig nem akkor „Cold Wallet”-ről. Mindemellett beszélhetünk mobilkészülék esetén beszélhetünk „Mobile Wallet”-ről, számítógép esetén „Online Wallet-ről” és virtuális valutaörműletnek köszönhetően az elmúlt pár évben megjelentek a Ledger és a Trezor cég által forgalmazott eszközök a „Hardware wallet”-ek is. Ezek első látásra sokkal inkább tűnnek egy pendrive és egy MP3 lejátszó „házasságon kívüli szerelemgyermekének”, mintsem igazán korszakalkotó jelentőséggel bíró technológiai eszközöknek (annak ellenére, hogy egyik tulajdonságait sem örökölték) és ezt at tényt már az is igazolta, hogy egy Ledger Nano-t még egy 15 éves gyerek is képes volt feltörni 2018. márciusában, bár ezt utólag maga a cég ténylegesen csak nagy huza-vona után ismerte el.¹² További tipológiát alkothatunk még, ha pénztárcák „úgymond” nyitottságát vizsgáljuk. E szerint, persze nem hivatalosan, de megkülönböztethetünk „pseudo-anonim pénztárcákat” (például: BitcoinWallet, Electrum, Mycelium stb.) és „anonim pénztárcákat” (például: DarkWallet). A előbbi a széleskörben elterjedt pénztárcák, míg az utóbbi felhasználója maga is kihangsúlyozza, hogy a felhasználónak kétségkívül valamilyen rejtegetni valója van.

A virtuális valuták tehát az egész tevékenység legkritikusabb pontjai. Forenzikus megközelítésből, vagy másként a nyomozóhatóságok, nemzetbiztonsági szolgálatok szemszögéből ez a legkedvezőbb és információkban legjobban bővelkedő felület, ezekből érdemes feltérképezni a kapcsolati hálót, információt gyűjteni az elkövetőkről, terroristákról,

¹² <https://krebsonsecurity.com/2018/03/15-year-old-finds-flaw-in-ledger-crypto-wallet/>
(Utolsó letöltés: 2018.04.25.)

az azok közötti pénzmozgásokról. Viszont ez ugyancsak igaz a másik, bűnözői oldal képviselői felől is. Mivel a pénztárcák online felületen és alkalmazás formájában is elérhetőek, ebből kifolyólag pedig többségében szorosan kapcsolódnak a személyes eszközeinkhez, valamint gyakran nyílt forráskódúak mindenféle malware hordozójaként megfelelően funkcionálhatnak. Így a felhasználó ismételten óriási veszélynek teszi ki magát, személyes adatait sőt azokat is akikkel tranzakciókat folytat.

Persze a pénztárcák esetében nemcsak adatokat, hanem magától értetődően nagyméretű összegeket is el lehet tulajdonítani, ráadásul napjainkban már nem csak önálló esetekről beszélhetünk, hiszen az APT, vagy kevésbé népszerűbb hackercsoportok automatizált támadások keretében adott esetben több ezer felhasználó pénztárcája felett vehetnék át az irányítást, vagy ha nem is veszik át forgalomeltérítéssel, csomaghamisításokkal, valós idejű QR-kód és tranzakciós címcserékkel csak a saját számlákra irányítják át a tetszőleges áldozatok pénztárain tárolt összegeket. Ehhez pedig nem feltétlenül szükséges megszerezni a privát kulcsokat sem. Ezt pedig ugyanúgy végrehajthatják más bűnözői körök, terroristák, vagy akár konkrét kormányok megrendelésére is, nem csak saját célokra. Az elmúlt években számtalan példa volt arra, hogy több százezer dollárt, vagy milliókat loptak el, akár mérgezett Google hirdetésekén át,¹³ vagy nyilvános wi-fi hálózatokon¹⁴ keresztül a gyanútlan felhasználóktól, bár általánosságban azért hozzá kell tenni, sokkal inkább a tőzsdék, ahol óriási összegek összpontosulnak egy helyen. A legutóbbi ilyen támadás a tanulmány lezárása előtt Indiában a Coinsecure nevű tőzsdén ment végbe 2018. április 13.-án. Ennek során 438 BTC-t sikerült ellopnia, ami megközelítőleg 3 millió amerikai dollárnak felel meg,¹⁵ de egy 2018. januári eset figyelemreméltóbb és talán intőbb példaként szolgál, amely során a Coincheck nevű Japán tőzsdéről 530 millió (!) dollár értékben loptak el virtuális valutát. Ez volt a magát a Bitcoin-t is megrengető, híres 2014-es Mt. Gox tőzsdéről eltűnt 400 millió dollár értékű Bitcoin lopás óta valaha volt legnagyobb ilyen akció.¹⁶

Így tehát összefoglalóan azt mondhatjuk a pénztárcákról, hogy ezek a felületek kiválóan (vagy talán a legjobban) alkalmasak a kiberbűnözők által pénz, információ és identitás szerzésre is bármilyen, a szakasz elején részletezett kategóriába tartozzanak azok. A felhasználás módja

¹³ <http://fortune.com/2018/02/14/bitcoin-cryptocurrency-blockchain-wallet-hack/>
(Utolsó letöltés: 2018.04.25.)

¹⁴ <http://www.news.com.au/technology/online/hacking/restaurantgoer-has-bitcoins-stolen-over-unsecured-public-wireless-network/news-story/a82d75eb85763ee3d38678b430df3bf0>
(Utolsó letöltés: 2018.04.25.)

¹⁵ <https://bitcoinchaser.com/news/indian-exchange-coinsecure-hacked> (Utolsó letöltés: 2018.04.25.)

¹⁶ <http://money.cnn.com/2018/01/29/technology/coincheck-cryptocurrency-exchange-hack-japan/index.html>
(Utolsó letöltés: 2018.04.25.)

és célja tekintetében nincsen felső határ, attól függetlenül, hogy a tanulmány terjedelmére való tekintettel csak ennyit lehetett megemlíteni.

3. SZOFTVER (BÁNYÁSZAT ESETÉN)

A bányászati tevékenységből származó virtuális valutákhoz visszaugorva még meg kell egy fontos mozzanatot. Már beszéltünk a hardver megválasztásának kockázatairól, viszont a hardver önmagában még nem kezd el bányászni. Szükség van ehhez egy szoftverre is, amely a hardver munkáját közvetíti egyrészt a hálózat felé, másrészt a tulajdonos pénztárcája felé, valamint statisztikákat gyárt a felhasználó számára, aki ez alapján tervezi meg a különböző lépéseket. A legnépszerűbb szoftverek a Bitcoin bányászatához a Bitcoin Miner, BTC Miner, CGMiner, BFGMiner, MultiMiner, de ezeken kívül persze számtalan másik valuta-specifikus bányász szoftver is létezik.

A szoftverekkel kapcsolatos problémákkal már szembesültünk a pénztárcával kapcsolatos részben is: egyrészt problémát jelent, hogy sok szoftver nyílt forráskódú, bárki hozzáférhet, adhat hozzá cryptojacking,¹⁷ backdoor, rootkit, spy tool stb. kiegészítő funkciókat. Másrészt ezeket az egyénileg módosított szoftverváltozatokat a kiberbűnözők közzé is teheti saját készítésű, hivatalos webhelynek tűnő honeypot-okon, ahol még az adathalászatra is széleskörű lehetőség nyílik, valamint konkrét támadásokra ugyancsak lehetőség nyílik, kiváltképp abban az esetben ha a program telepítőjének vagy frissítésének álcáz malware-eket, amiket azután az internetet körületekintés nélkül felhasználó gyanútlanul letölt és feltelepít. A lehetőségek ebben az esetben sincsenek korlátozva.

4. TRANZAKCIÓ (BÁNYÁSZAT ÉS VÁSÁRLÁS ESETÉN)

Az utolsó vizsgálandó népszerű mozzanat tranzakció maga, amely általános művelet a bányászok és a valuta vásárlók körében egyaránt. A tranzakciók ugyebár két személy/csomópont között, P2P zajlanak. A P2P hálózat decentralizált jellegéből adódóan

¹⁷ A cryptojacking-jelenség egyre jobban növekvő problémájára jól rávilágít, hogy már az oldalakon megjelenő, egyszerűnek tűnő reklámokon keresztül is lehetséges a virtuális valuták bányászata a felhasználók tudta nélkül. A legnépszerűbb videómegosztó a YouTube már konkrét intézkedéseket is tett az ügyben: <https://www.telegraph.co.uk/technology/2018/01/29/youtube-shuts-hidden-crypto-jacking-adverts/> (Utolsó letöltés: 2018.04.25.)

Persze a jelenségre akadnak magyar példák is 2017-ből. Magyarországon nagyon népszerűek például az illegális mozi oldalak, ahol a felhasználók nem tudják megkerülni a reklámokat, hiszen, ha blokkolókat használnak nem tudják megnézni a filmeket. Ezt a kényszerhelyzetet egy népszerű online filmes oldal, a movie.cc rögtön ki is használta: https://index.hu/tech/2017/12/27/magyar_illegalis_mozis_oldal_bukott_le_azzal_hogy_a_nezok_gepeivel_kripto_penzet_banyasztat/ (Utolsó letöltés: 2018.04.25.)

kikerüli azokat a biztonsági mechanizmusokat (például: csomagszűrő tűzfalak), amiket adott esetben normál hálózati struktúrákban egy felhasználó nem tud. Ezzel egyrészt jobban bebiztosítja az anonimitást, másrészt viszont veszélyeknek teszi ki magát. Ez általánosan igaz a P2P hálózatokra, viszont a virtuális valutatranszakciók esetében, lévén hogy azok nem ilyen szokványos hálózatok, a felhasználó legnagyobb veszélyforrásának az tekinthető nem tud megbizonyosodni, hogy a kapcsolat végén valóban az a személy van, akire a felhasználó számít. Ezen kívül gondot okozhat még a korábban már említett tranzakció eltérítés, de ez csak a pénztárca szakaszban valósítható meg. Ha már bekerültek az adatok a blokkláncba óriási energiákat emésztene fel azok követése, a hash-ek azonosítása, visszafejtése, a blokkok átírása stb. és a szűkös időlimitek miatt ezek kivitelezhetetlen feladatok lennének még a szuperszámítógépekkel is.

Így tehát a tranzakciós folyamat esetében egyetlen veszélyfaktor van, mégpedig az, hogy a P2P kommunikáció végén az a felhasználó található-e, akinek az összeget valóban címeztük.

Összegezve tehát virtuális valutákat, azok egyes szakaszainak kiberbiztonsági kockázatait, ezek azok a legfőbb veszélyek, amelyek főként a felhasználókat fenyegetik, viszont a nemzetbiztonság szempontjából igencsak képes növelni a veszélyeket, ha a felhasználók közül az államigazgatási szférából is kerülnek ki személyek, illetve, ha azok egyéni haszonszerzés céljából, az ellenőrzési részeket kihasználva kormányzati informatikai erőforrásokat használnak fel. Természetesen azt fent kell tartani, hogy egyrészt tökéletes védelem az informatikában nem létezik, vagyis még számtalan ismert és eddig ismeretlen lehetőség nyílik a virtuális valutákon kívül is a támadásra, adathalászatra, másrészt, hogy a fenti bemutatás a teljesség igénye nélkül ment végbe, erre külön ennek címzett tanulmányban lehetne csak igazán sort keríteni.

A virtuális valutákkal és a kiberbiztonsággal kapcsolatban a továbbiakban még röviden bemutatunk egy figyelemre méltó, új jelenséget ugyanis az utóbbi időben számos eset akadt és a jövőben komoly komplikációk származhatnak belőle akár a közeljövőben is.

A DARK WEB ÉS KIBERBŰNÖZÉS VIRTUÁLIS VALUTÁKKAL ÖSSZEFÜGGŐ ÚJABB TENDENCIÁI, NEMCSAK PROFIKNAK – A RANSOMWARE-AS-A-SERVICE (RAAS) PLATFORMOK ÉS A CONSTRUCTION KIT-EK

A virtuális valuták szoros összefüggésben állnak a Web egy aprócska, ám annál sötétebb, hatóságilag szabályozhatatlan részterületével, a Dark Web – el, vagy Criminal Web-

el.¹⁸ Sokan a dark web-nek és az abban központi helyet foglaló, a hatóságok által már többször bezárt SilkRoad 1.0 és 2.0 online kereskedelmi felülethez kötik például a Bitcoin felvirágzását is,¹⁹ amely részben valóban igaz, hiszen a virtuális valuták gyors, korlátlan és anonim tranzakciós természete kiválóan illeszkedik a Dark Web, amúgy is anonim többlépcsős visszajelzési rendszeréhez,²⁰ amelyeket a vásárlások során alkalmaznak a résztvevők.

Általában, ha maga a Dark Web általában szóba kerül egy beszélgetésben a következő gondolat rögtön az lesz valamelyik résztvevő részéről az, hogy ez egy olyan hely az interneten, ahonnan kábítószert, bérgyilkosokat és fegyvereket lehet rendelni. Nem tévednek nagyot, hiszen valóban ilyen szolgáltatások milliói állnak rendelkezésre (eltekintve, most attól, hogy ezeknek jó része feltehetően csak átverés) kiegészítve hamisított iratokkal, kémtechnológiákkal és más illegális szolgáltatások százezreivel. A téma szempontjából a szolgáltatások apró részterülete, a cybercrime-as-a-service típusú szolgáltatásokon²¹ belül megrendelhető egyes ransomware-ek,²² valamint ezek az ezek tulajdonságainak a felhasználó általi tetszőleges variációját elősegítő úgynevezett „construction kit”-ek (építőkészletek) a lényegesek, ugyanis ezeknek a virtuális valuták felvirágzásával egyidőben, azzal párhuzamosan, az utóbbi időben elkezdett felfutni, úgyszólván szárnyalni a kereskedelme.

2017. májusában a világ már igazán megismerkedhetett a ransomware-kifejezéssel, amikor a feltehetően Észak-Korea által intézett támadás több, mint száz országában több százezer számítógép milliárdjait bénította meg a WannaCry nevű zsarolóvírus, amely a támadás után Bitcoin-ban követelt átutalást a felhasználóktól az adatokért cserébe. A vírus egyébként nemcsak abban az évben, hanem 2018. márciusában ismét felbukkant felfordulást okozva ezzel a repülőgépgyártó óriás, a Boeing Charlston-i üzemében.²³ Bár a köznyelvben ezt a vírust ismerik a legtöbben és ennek Észak-Koreából kiindulva kifejezetten gazdasági és politikai megfontolásai is voltak léteznek más ilyen típusú zsarolóvírusok is, például a Locky, ami 2017-

¹⁸ A Web, és azon belül a Dark Web részletesebb felépítését és hírszerzési megközelítéséért lásd: ALFRED ROLINGTON: *Hírszerzés a 21. Században – A Mozaik Módszer*. Antall József Tudásközpont, Budapest, 2015. pp. 100-108.

¹⁹ <http://fortune.com/2017/10/02/bitcoin-sale-silk-road/> (Utolsó letöltés: 2018.04.05)

²⁰ A Dark Web többlépcsős biztonsági rendszere röviden az adminisztrátorok közvetítő szerepére és a (vissza)jelzésekre épül. A vásárló ezeknek küldi el az áru, szolgáltatás összegét letétbe, ezek után pedig a kereskedő elküldi a címzettnek az árut, szolgáltatást. A vevőnek ezek után vissza kell jeleznie és az adminisztrátor tovább küldi a letétbe helyezett összeget a kereskedőnek. Ez egyfelől garanciaként szolgál a fizetésre, másfelől a közvetett kapcsolat miatt csökkenti annak kockázatát, hogy a vevő és a kereskedő egyszerre bukjon le.

²¹ <https://www.csoonline.com/article/3205253/data-breach/the-rise-and-rise-of-cybercrime-as-a-service.html> (Utolsó letöltés: 2018.04.25.)

²² <https://www.forbes.com/sites/forbestechcouncil/2017/03/17/ransomware-as-a-service-the-next-great-cyber-threat/#7cfd03dc4123> (Utolsó letöltés: 2018.04.25.)

²³ <https://www.seattletimes.com/business/boeing-aerospace/boeing-hit-by-wannacry-virus-fears-it-could-cripple-some-jet-production/> (Utolsó letöltés: 2018.04.25.)

ben fertőzött, a közösségi médiában, vagy a 2018. áprilisában detektált RansSIRIA, amely például a Szíriai menekültek helyzetére próbálja felhívni a figyelmet.²⁴

Ami nemzetbiztonsági problémát jelent, hogy az efféle a zsarolóvírusok és úgy általában a vírusok nem tesznek különbséget a kormányzati és nem kormányzati, valamint a kritikus infrastruktúrák számítógépek között. Az első WannaCry támadás során például áldozatul estek a német Deutsche Bahn vasúttársaság,²⁵ a brit National Health Service²⁶ és a magyar Telenor távközlési szolgáltató²⁷ számítógépei egyaránt, de hogy aktuálisak legyünk és konkrét összegekben is lássuk mire képesek az efféle támadások, talán megfelelő esetben bizonyul egy ugyancsak 2018. áprilisi ransomware támadássorozat után, amely kifejezetten kormányzati informatikai rendszereket célozott meg Atlantában ezzel pedig 2.7 millió dolláros kára keletkezett a városnak.²⁸

Éppen ezért jelent problémát az utóbbi időben megnövekedett kereslet a Dark Web-en²⁹ az olyan szolgáltatások iránt, ahol vagy konkrét zsarolóprogramokat lehet venni, vagy pedig ezeket a construction kit-ek-nek nevezett eszközöket, amelyekkel akár pár lépésben is össze lehet bármilyen malware-eket állítani, köztük a már említett zsarolóvírusokat is.³⁰ Ezt pedig a relatíve könnyű hozzájutás miatt, már szinte bárki megteheti és nem kell széleskörű informatikai tudás se ahhoz, hogy valaki innentől például zsarolóvírusokat programozzon.

Valószínűleg a jelenlegi virtuális valuta örület a közeljövőben egyre több személyt ösztönöz majd arra, hogy a másik illegális és alattomos módszer cryptojacking mellett ezen kiegészítő módszer segítségével szerezzen virtuális valutát, mint a közösségeken belül legálisnak számító nagyobb idő- és energiaigényesebb bányászat útján. Mondhatnánk persze, hogy a virtuális valuták még nem ennyire elterjedtek és az egyszerű felhasználók közül a legtöbb csak maximum hallott a létezésükről, de egyáltalán nem ért azokhoz, de ha kényszerhelyzetbe kerül a zsarolóvírusok miatt és gyorsan szükség van az elzárt információkra adott esetben kénytelenek lesznek megtanulni a működésüket. Ez pedig igaz az állami

²⁴ <https://securityaffairs.co/wordpress/71626/malware/ranssiria-ransomware.html>

(Utolsó letöltés: 2018.04.25.)

²⁵ <http://www.spiegel.de/netzwelt/web/wannacry-450-bahn-computer-von-cyber-attaque-betroffen-a-1147921.html> (Utolsó letöltés: 2018.04.25.)

²⁶ <https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/> (Utolsó letöltés: 2018.04.25.)

²⁷ <http://www.origo.hu/itthon/20170513-riasztast-adott-ki-a-wannacry-zsarolovirus-miatt-a-kormanyzati-esemenykezo-kozpont.html> (Utolsó letöltés: 2018.04.25.)

²⁸ <https://www.technoblog.net/a-ransomware-cost-the-city-of-atlanta-more-than-2-7-million/> (Utolsó letöltés: 2018.04.25.)

²⁹ <https://24.hu/tech/2017/12/30/par-ev-es-a-drognal-is-nagyobb-uzlet-lehet-a-zsarolovirus/> (Utolsó letöltés: 2018.04.25.)

³⁰ <https://securityaffairs.co/wordpress/37180/cyber-crime/tox-ransomware-builder.html> (Utolsó letöltés: 2018.04.25.)

szereplőkre is, hiszen, ha az újtípusú ransomware-ek olyan kritikus infrastruktúrák gépeit zárják majd le, amelyek folyamatos monitoring-ot igényelnek és gyors reagálás hiányában óriási problémákat képesek okozni (például: atomerőművek), nem lesz idő arra, hogy kivárják, míg valaki kitalálja, hogy hogyan lehet ezeket a vírusokat fizetés nélkül semlegesíteni.

Bár a Dark Web és a virtuális valuták összefonódását ebben a szakaszban csak kismértékben, inkább csak a megrendelhető kiberbűnözési szolgáltatások egy részén keresztül tanulmányoztuk, azt mindenképpen hozzá kell tennünk, hogy az internet ezen részének fennállásából még számtalan probléma fog származni a jövőben és az már most látszik, hogy a hatóságok, bár a SilkRoad esetében is érték el csekély eredményeket, ezek az eredmények igazából semmit sem érnek, hiszen egy kereskedelmi oldal bezárásával csak egy másik forgalmát növelik meg.³¹ mindazonáltal, azzal mindenképpen sikerülni óriási csapást mérni magára az egész Dark Web-re, ha valahogyan ki lehetne vonni a virtuális valutákat világszerte a forgalomból,³² hiszen akkor kénytelenek lennének nagyobb mértékben hagyományos pénzeszközöket használni, amiket már jobban nyomon lehetne követni. Ez lehetne az első fontos lépés tehát a felszámolásban, de az, hogy ezt hogyan is kéne megvalósítani egyelőre lehetetlen átlátni és kivitelezni, így ez egyelőre csak a jövő nagy kérdése marad.

ÖSSZEGZÉS

Bár a tanulmányban valamilyen szinten azért látható vált, hogy bűnözi oldalról mennyi fenyegetést hordozhatnak magukban a virtuális valuták, az igazi fenyegetések, csak akkor láthatók igazán, ha sokkal jobban kiszélesítésre kerül a vizsgált tárgy és belekerülnek például, a terroristák, az ellenérdekelt titkosszolgálatok, vagy a szeparatista mozgalmak. Sőt az is tartogathat némi érdekességet, ha virtuális valutákat egészen más, a gazdaság, vagy a környezet dimenziójában, mint más klasszikus Buzan-féle szektorokban vizsgáljuk. Ami biztosan látszik, hogy a Bitcoin óta eltelt 10 évben már több, mint 1500 virtuális valutáról beszélünk és még mindig nem mutatkozik egységes szabályozási, vagy hatósági fellépés a nemzetközi közösség részéről és igazából maguk a „legális” felhasználók se tudják igazán mire is használhatók jól ezek a fizetőeszközök. Azt tehát majd csak a jövő fogja számunkra igazán megmondani, mik is valójában ezek az alternatív fizetési eszközök.

³¹ Bár ezek más hasonló esetek, de jól mintázzák a konkurencia hasznát:

<https://index.hu/tech/2017/08/02/illegalis-aruhazakra-csaptak-le-a-sotet-weben-a-konkurencia-koszoni-szepe-n/> (Utolsó letöltés: 2018.04.25.)

³² Arra, hogy az államok hogyan tudnák megállítani a virtuális valutákat már több koncepció is létezik:

<https://steemit.com/cryptocurrencies/@thehutchreport/10-ways-governments-could-stop-cryptocurrencies> (Utolsó letöltés: 2018.04.25.)

FORRÁSOK

Szakirodalom:

MARK M. LOWENTHAL: *Hírszerzés – A titoktól a politikai döntésig*. Antall József Tudásközpont, Budapest, 2017.

ALFRED ROLINGTON: *Hírszerzés a 21. Században – A Mozaik Módszer*. Antall József Tudásközpont, Budapest, 2015.

Internetes források:

<https://hackernoon.com/ten-years-in-nobody-has-come-up-with-a-use-case-for-blockchain-ee98c180100>

(Utolsó letöltés: 2018.04.25.)

<https://uk.reuters.com/article/us-netherlands-crime-bitcoin/dutch-arrest-10-men-suspected-of-using-bitcoin-to-launders-money-idUKKCN0UY0V8>

(Utolsó letöltés: 2018.04.25.)

<https://www.computerworld.com/article/2471127/endpoint-security/intelligence-agencies-hunting-for-terrorists-in-world-of-warcraft.html>

(Utolsó letöltés: 2018.04.25.)

<https://qubit.hu/2018/01/29/tombolnak-a-befektetok-a-kickstarteren-hiaba-dobtak-ossze-200-000-dollart-se-hire-se-hamva-a-forradalmi-magyar-okoscsengonek-a-shoka-bellnek>

(Utolsó letöltés: 2018.05.01)

https://index.hu/tech/2017/12/27/magyar_illegalis_mozis_oldal_bukott_le_azzal_hogy_a_nezok_gepeivel_kripto_penzet_banyasztat/

(Utolsó letöltés: 2018.04.25.)

<https://securityintelligence.com/mirai-iot-botnet-mining-for-bitcoins/>

(Utolsó letöltés: 2018.04.25.)

<https://www.investopedia.com/news/hackers-target-computer-rigs-illegally-mine-cryptocurrencies/>

(Utolsó letöltés: 2018.04.25.)

<http://www.alphr.com/security/1008522/google-play-store-apps-mine-cryptocurrency>

(Utolsó letöltés: 2018.04.25.)

<https://www.wired.com/story/google-bans-all-cryptomining-extensions-from-the-chrome-store/>

(Utolsó letöltés: 2018.04.25.)

<https://securityaffairs.co/wordpress/70968/malware/hiddenminer-android-miner.html>

(Utolsó letöltés: 2018.04.25.)

<https://krebsonsecurity.com/2018/03/15-year-old-finds-flaw-in-ledger-crypto-wallet/>

(Utolsó letöltés: 2018.04.25.)

<http://fortune.com/2018/02/14/bitcoin-cryptocurrency-blockchain-wallet-hack/>

(Utolsó letöltés: 2018.04.25.)

<http://www.news.com.au/technology/online/hacking/restaurantgoer-has-bitcoins-stolen-over-unsecured-public-wireless-network/news-story/a82d75eb85763ee3d38678b430df3bf0>

(Utolsó letöltés: 2018.04.25.)

<https://bitcoinchaser.com/news/indian-exchange-coinsecure-hacked>

(Utolsó letöltés: 2018.04.25.)

<http://money.cnn.com/2018/01/29/technology/coincheck-cryptocurrency-exchange-hack-japan/index.html>

(Utolsó letöltés: 2018.04.25.)

<https://www.telegraph.co.uk/technology/2018/01/29/youtube-shuts-hidden-crypto-jacking-adverts/>

(Utolsó letöltés: 2018.04.25.)

https://index.hu/tech/2017/12/27/magyar_illegalis_mozis_oldal_bukott_le_azzal_hogy_a_nezok_gepeivel_kripto_penzet_banyasztat/

(Utolsó letöltés: 2018.04.25.)

<http://fortune.com/2017/10/02/bitcoin-sale-silk-road/>

(Utolsó letöltés: 2018.04.05)

<https://www.csoonline.com/article/3205253/data-breach/the-rise-and-rise-of-cybercrime-as-a-service.html>

(Utolsó letöltés: 2018.04.25.)

<https://www.forbes.com/sites/forbestechcouncil/2017/03/17/ransomware-as-a-service-the-next-great-cyber-threat/#7cfd03dc4123>

(Utolsó letöltés: 2018.04.25.)

<https://www.seattletimes.com/business/boeing-aerospace/boeing-hit-by-wannacry-virus-fears-it-could-cripple-some-jet-production/>

<https://securityaffairs.co/wordpress/71626/malware/ranssiria-ransomware.html>

(Utolsó letöltés: 2018.04.25.)

<http://www.spiegel.de/netzwelt/web/wannacry-450-bahn-computer-von-cyber-attacke-betroffen-a-1147921.html>

(Utolsó letöltés: 2018.04.25.)

<https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/>

(Utolsó letöltés: 2018.04.25.)

<http://www.origo.hu/itthon/20170513-riasztast-adott-ki-a-wannacry-zsarolovirus-miatt-a-kormanyzati-esemenykezo-kozpont.html>

(Utolsó letöltés: 2018.04.25.)

<https://www.technoblogy.net/a-ransomware-cost-the-city-of-atlanta-more-than-2-7-million/>

(Utolsó letöltés: 2018.04.25.)

<https://24.hu/tech/2017/12/30/par-ev-es-a-drognal-is-nagyobb-uzlet-lehet-a-zsarolovirus/>

(Utolsó letöltés: 2018.04.25.)

<https://securityaffairs.co/wordpress/37180/cyber-crime/tox-ransomware-builder.html>

(Utolsó letöltés: 2018.04.25.)

<https://steemit.com/cryptocurrencies/@thehutchreport/10-ways-governments-could-stop-cryptocurrencies>

(Utolsó letöltés: 2018.04.25.)

https://index.hu/tech/2017/08/02/illegalis_aruhazakra_csaptak_le_a_sotet_weben_a_konkurencia_koszoni_szepe_n/

(Utolsó letöltés: 2018.04.25.)