DOI: 10.38146/BSZ.2022.9.9

Zsarolóvírusok és a No More Ransom projekt

Ransomwares and the No More Ransom project

Halász Viktor
rendőr százados
Készenléti Rendőrség,
Nemzeti Nyomozó Iroda

Absztrakt
Cél: Az írás célja a zsarolóvírusok kategóriáinak, főbb működési elveinek, valamint a zsarolóvírusokkal szembeni fellépés érdekében az Europol által létrehozott No More Ransom projektnek a bemutatása.
Módszertan: A zsarolóvírusokkal kapcsolatos adatokat egyrészt a témában készült tanulmányok és felmérések feldolgozásával, másrészt pedig az ilyen bűncselekmények nyomozása és a nemzetközi bűnügyi együttműködés során szerzett személyes tapasztalatok útján gyűjtöttem.
Megállapítások: Az utóbbi években a zsarolóvírus fertőzések száma folyamatosan nőtt, a bűnözők által alkalmazott módszerek fejlődtek, az ilyen támadásokkal okozott kár pedig minden korábbinál magasabb, ezért egyre nagyobb szükség van a No More Ransom-hoz hasonló projektekre.
Érték: A tanulmány segít jobban megérteni a zsarolóvírusok működését a hazai bűnüldöző szervek nyomozói számára, és betekintést nyújt a titkosított fájlok visszaszerzésének egy lehetséges módszerébe.

Kulcsszavak: zsarolóvírus, kártékony kód, kiberbűnözés, No More Ransom

Abstract
Aim: The purpose of this article is to present the categories of ransomwares, the main operational principles of these malwares and Europol's No More Ransom project to combat ransomware.
Methodology: I collected data regarding ransomwares by processing studies and surveys on the subject, also by personal experience gained during the investigation of such crimes and international criminal cooperation.

Findings: In recent years the number of ransomware infections has steadily increased, the methods used by criminals have improved and the damage caused by such attacks is higher than ever which is why there is an increasing need for projects like No More Ransom.
Value: The study helps domestic law enforcement investigators better understand how ransomware works and provides insight into a possible method for recovering encrypted files.

Keywords: ransomware, malware, cybercrime, No More Ransom

Bevezetés

2021 májusában az USA keleti partvidékének lakói hiába próbálták megtankolni az autóikat. Több üzemanyagtöltő állomáson már napok óta nem lehetett benzinhez jutni, és egyre több kutat kerítettek körbe sárga szalagokkal az egyre súlyosbodó üzemanyaghiány miatt. Mások a tervezett repülő útjaikat voltak kénytelenek újratervezni, ugyanis a repülőtereken szintén nem állt rendelkezésre elég üzemanyag egyes járatok elindításához. A kialakult helyzetben a lakosok pánikvásárlásba kezdtek, tovább rontva a helyzeten, ami odáig vezetett, hogy Joe Biden amerikai elnök országos veszélyhelyzetet hirdetett.

Az események 2021 májusának elejére nyúltak vissza, amikor is ismeretlen hackerek megszerezték a keleti partvidék legnagyobb olajvezetékét üzemeltető Colonial Pipeline egyik dolgozójának VPN jelszavát, amellyel belépve először mintegy 100 GB-nyi adatot loptak el, majd pedig egy zsarolóvírust telepítettek a rendszerbe. Bár a vírus csak a számlázó alrendszert blokkolta, az attól való – jogos – félelem miatt, hogy később az üzemeltetésért felelős, sokkal fontosabb alrendszereket is megfertőzheti, a Colonial Pipeline vezetői a teljes vezeték leállítása mellett döntöttek. Az elkövetők 75 bitcoin – akkori árfolyamon több mint négymillió dollár összegű – váltságdíjat követeltek a feloldókulcs megadásáért, amelyet a Colonial Pipeline vezetői az FBI felügyelete mellett egy napon belül kifizettek (URL1).

A vezeték teljes működésének helyreállítása még ezzel együtt is hat napig tartott, és az általános üzemanyaghiány mellett az évtized legmagasabb üzemanyagárait is eredményezte az USA-ban. A támadás idején a Colonial Pipeline a majdnem 9000 km hosszan elterülő vezetékével Texastól New Jersey-ig az egész keleti partvidék olajszügségletének mintegy felét biztosította nap mint nap, a vírusfertőzés pedig az addigi legnagyobb kritikus infrastruktúra elleni támadásnak bizonyult az USA történelmében.

A fenti példa azonban csupán a csúcspontja (legalábbis mostanáig) egy mintegy másfél évtizede tartó folyamatnak, amely során a zsarolóvírusok a kezdeti, bosszantó kellemetlenséggel járó programokból az egyik legelterjedtebb és legnagyobb kárt okozó számítógépes vírusfajtává nőtték ki magukat, hatalmas veszteségeket okozva magánszemélyeknek és nagyvállalatoknak egyaránt.

A zsarolóvírusok fejlődésének főbb állomásai

A zsarolóvírus az angol ransomware kifejezés magyarosított változata, ami a ransom (váltságdíj) és malware (kártékony kód) szavak összevonásából született (Humayun, Jhanjhi, Alsayat, & Ponnusamy, 2021). Bár az eredeti kifejezés is találó, a magyar átírás talán ebben az esetben még inkább kifejezi ezeknek a programoknak a lényegét: olyan kártékony kódokról van szó ugyanis, amelyek titkosítják vagy zárolják az áldozat adatait vagy akár az egész számítógépes rendszerét, és a feloldáshoz szükséges eszközt egy bizonyos összeg megfizetésétől teszik függővé. Ilyen módon leegyszerűsítve pedig valóban olyan vírusokról beszélünk, melyeknek lényegi funkciója az áldozatok zsarolása.

Bár a zsarolóvírusok utóbbi évekbeli fejlődése okán a fenti fogalom határai kezdenek egyre halványulni, és a bűnözők minduntalan újabb taktikákat vetnek be a célpontok által egyre szélesebb körben használt védekezési módszerek kijátszása érdekében, ezen kártékony kódoknak továbbra is a zsarolás a meghatározó lényegi motívuma.

Mint minden más vírusfajta esetén, a zsarolóvírusok kapcsán is az internet előtti időkben, az otthoni számítógépek elterjedésének hajnalán kell keresnünk a legkorábbi ilyen károkozó megjelenését. Az első, széles körben ismertté vált ransomware-t 1989-ben küldték szét postai úton, floppy lemezeken egy konferencia résztvevőinek, és egyszerű, szimmetrikus kulcsú titkosítással tette olvashatatlanná a C:\ meghajtón tárolt fájlokat. Ezt követően az 1990-es évek közepén egyetemi kutatók egy gondolatkísérlet keretében lefektették a kriptográfia támadó módon történő alkalmazásának elméleti alapjait, kitérve már az aszimmetrikus kulcsú kriptográfia előnyeire is (Young & Yung, 1996) azonban mindennek ellenére a 2000-es évek közepéig a zsarolóvírusok főként csupán koncepcióként léteztek és nem valós fenyegetésként voltak jelen a kibertérben.

A 2000-es évek közepére azonban az internet elterjedtsége, az online tér kommunikációra való használata és a személyi számítógépeken tárolt személyes adatok mennyisége elérte azt a szintet, amely már kedvező környezetet teremtett az első, valódi, szélesebb tömegeket érintő zsarolóvírusok megszületésének. Ebben az időszakban a legelső variánsok jellemzően e-mailek útján terjedtek

és viszonylag könnyen feltörhető, szimmetrikus titkosítást használtak, azonban már előre jelezték a zsarolóvírusok egyre szélesebb körű terjedésének várható irányát. Nem sokkal később már az aszimmetrikus kulcsú titkosító vírusok is megjelentek, amelyek már sokkal komolyabb veszélyt jelentettek az internethasználókra nézve, illetve szintén a zsarolóvírus-fajták egy újabb elágazásaként az első lezáró típusú vírusvariánsok is terjedni kezdtek.

A zsarolóvírusok szempontjából azonban a mai napig a legfontosabb technológiai újítás 2009-ben született meg a bitcoin képében, ami alapvető hatást gyakorolt a ransomware-ek jövőjére. A kriptovaluták megszületéséig ugyanis a zsarolóvírusok gyenge pontját a váltságdíj behajtásának módjai jelentették: bár több különböző módszer is létezett a váltságdíjak begyűjtésére (az ajándékkártyáktól kezdve az emelt díjas SMS-eken át a PayPal szerű internetes fizetési szolgáltatások igénybevételéig), minden módszer szükségszerűen valamilyen harmadik szolgáltatóhoz kötődött, akin keresztül a nyomozó hatóságnak mindenképpen lehetősége nyílt a pénz útjának nyomon követésére és a megszerzett összegek zárolására. A bitcoin megszületésével azonban létrejött az első olyan decentralizált, senkitől sem függő – és emellett ráadásul nagy részben anonim – fizetési rendszer, mely az utolsó építőkövet jelentette a viszonylag kockázatmentes és hatékony zsarolóvírus-támadások alapjának lefektetéséhez.

Természetesen ez nem jelentette azt, hogy a bitcoin megalkotásával egyidejűleg a zsarolóvírusok száma is hirtelen és nagymértékben azonnal megemelkedett volna, hiszen ekkor még a kriptovaluták jóindulattal is csak játékpénznek voltak tekinthetők, és egyáltalán nem volt biztos, hogy bármiféle értékkel fognak rendelkezni a jövőben. Ezekben az években – bár érezhetően egyre gyorsuló –még mindig viszonylag mérsékelt ütemben növekedett a ransomware-ek mennyisége, azonban amikortól már nyilvánvalóvá vált, hogy a kriptovaluták nem csupán egy átmeneti technológiai érdekességként fognak szerepelni a történelemkönyvekben, hanem a gazdaság integráns részévé válnak, a zsarolóvírusok száma is drasztikus emelkedésnek indult. Ez az időszak a 2010-es évek közepére tehető, és ezt tekinthetjük a zsarolóvírusok – máig tartó – aranykora kezdetének is. Innentől kezdve gyakorlatilag minden létező zsarolóvírus-variáns bitcoinban követelte a váltságdíj összegét, és ez volt az az időszak is, amikor az ismert ransomware-ek, de főképp a fertőzések száma évről évre folyamatosan a többszörösére emelkedett (URL2).

Bár a ransomware támadásoknak a – következő fejezetben részletesen tárgyalt – sémája ekkorra már nagyjából kikristályosodott, a számadatok növekedése mellett folyamatos technológiai fejlődésnek is tanúi lehettünk. Példaként: a vírusok által használt titkosítási algoritmusok folyamatosan újabbakra cserélődtek (elliptikus görbe kriptográfia, hibrid titkosítás); általánossá vált a TOR-on

keresztül elérhető felületek használata az áldozattal való kommunikáció csatornájaként; megjelentek az első zsarolóvírusok Androidra, Linuxra és Apple eszközökre; szélesedett a támadási vektorok száma (az e-mailek és a weboldalak mellett megjelentek az appok, illetve egyre inkább kihasználásra került a közösségi média, a hirdetési bannerek útján történő átirányítás és a legtöbb zero-day sérülékenység); valamint jellemzővé vált a statikus C & C szerverek helyett a véletlenszerű tartomány generálási metódusok (DGA) használata a vírussal való kommunikáció céljából (Oz, Aris, Levi & Uluagac, 2021).

Az igazán jelentős változásokat azonban nem a pusztán technológiai jellegű előrelépések okozták, hanem a bűnözők által használt módszereknek, illetve magának a ransomware ökoszisztémának az átalakulása. Ez utóbbinak a legfontosabb állomása az úgynevezett RaaS (Ransomware as a Service – zsarolóvírus szolgáltatások) elterjedése. Míg korábban a ransomware támadások kivitelezéséért magukat a vírusokat megalkotó, magas technikai képzettséggel rendelkező kiberbűnözők voltak a felelősek, addig a 2010-es évek közepétől kezdődően egyre jellemzőbb RaaS ökoszisztéma lehetővé tette, hogy a vírusokat létrehozó személyektől egyre inkább elkülönüljenek az azokat ténylegesen használó bűnözők. Minimális technikai tudással is képes volt bárki ettől fogva ransomware-t vásárolni a dark neten (akár a hozzá tartozó know how-al), és saját elhatározása szerint kiválasztani a célpontokat, a fertőzés módját és a követelt összeg nagyságát. A fejlesztők mindezért vagy egyszeri összeget kaptak a ransomware eladásakor, vagy egyfajta affiliate rendszerben a beérkező váltságdíjak bizonyos hányadát (a bevezetőben említett Colonial Pipeline megtámadása mögött álló DarkSide csoport éppen ilyen affiliate rendszert működtetett). A potenciális zsarolóvírus-támadók számának növekedésével pedig természetszerűen a támadások száma is növekedett (Oosthoek, Cable & Smaragdakis, 2022).

Mindez organikus módon oda is vezetett, hogy a támadások általános jellege is lassan de biztosan átalakult. Az évtized elejére jellemző, az internetfelhasználók tömegeit válogatás nélkül célzó, kis összegű váltságdíjat követelő támadások mellett egyre nagyobb számban megjelentek a fókuszált, egy-egy konkrét célpontra koncentráló, a sikeres fertőzés esetén jelentős váltságdíjat követelő akciók is. Értelemszerűen ez utóbbi célpontok már nem a magánszemélyek köréből kerültek ki, hanem az adataik elvesztésére különösen érzékeny, fizetőképes és ezért fizetési hajlandósággal is rendelkező vállalkozások voltak. Az ő esetükben továbbá nem csupán az adatok titkosítása, hanem akár azok nyilvánosságra hozatala is hatékony zsarolási lehetőséget jelentett, amivel szemben ráadásul védekezni sem lehet – az ekkorra már egyre általánosabbá váló – biztonsági mentésekkel. Ez az időszak tekinthető a hatalmas multinacionális cégeket és kritikus infrastruktúra üzemeltetőket érintő, millió dolláros

váltságdíjak kifizetésével járó, világsajtót megmozgató támadások – jelenleg is tartó – korszakának.

A pandémia 2020-as kitörése pedig ezt követően csak még tovább súlyosbította a helyzetet azáltal, hogy az irodai dolgozók tömegeit kényszerítette otthoni – rendszergazdák által nem felügyelt eszközökön és szoftverekkel történő – munkavégzésre, a többszörösére növelve ezzel a lehetséges támadási vektorok számát.

A zsarolóvírusokban rejlő lehetőségek már jelenleg is rendkívül profitábilis, igen mérsékelt kockázatokkal járó támadási formát biztosítanak a bűnözőknek, azonban nem lehet sok kétségünk afelől, hogy a ransomware-ek mögött álló technológia és bűnözési ökoszisztéma fejlődése ettől még nem fejeződött be. Az jelenleg még ugyan kétséges, hogy mi lesz a ransomware-ek fejlődésének következő jelentős állomása, az viszont nem, hogy mindez a bűnüldöző szerveknek újból különösen nagy kihívásokat jelent majd.

A zsarolóvírusok működése és típusai

Egy zsarolóvírus-támadás jellemzően a következő szakaszokból épül fel: fertőzés, telepítés, kommunikáció, végrehajtás, zsarolás és együttműködés (Aldauiji, Batarfi, & Bayousif, 2022).

A *fertőzés* fázisa akkor kezdődik, amikor a kártékony kód – bármilyen módon – a megtámadott rendszerbe jut. Az elkövetők számos támadási vektort alkalmaznak a vírus célpontba juttatására, a legegyszerűbbtől az egészen összetettig. Viszonylag primitív, ám hatékony – és épp ezért gyakori – módszer a vírusnak különböző e-mail csatolmányok útján történő terjesztése, ahol magát a telepítendő vírusfájlt csatolják a levélhez valamilyen megtévesztő néven (például önéletrajzként) álcázva, és bízva abban, hogy a figyelmetlen címzett egyszerűen telepíti azt. Ennél kissé kifinomultabb módszer, amikor egyébként valóban ártalmatlannak tűnő fájlokban (a leggyakrabban Word vagy Excel dokumentumokban) elrejtett makrók segítenek a vírus számítógépre juttatásában. Az e-mailek útján történő terjesztés történhet továbbá egyszerű linkek beágyazásával is, amelyekre kattintva az áldozat maga keresi fel a kártékony kódot letöltő webszervert (természetesen a tudta nélkül). Maguknak a káros kódot tartalmazó weboldalaknak az üzemeltetése egyébként önmagában is a fertőzési módszerek másik nagy csoportját képezi, és ha nem e-mailek útján irányítják ide az áldozatokat, akkor vagy hirdetések feladásával teszik ezt (ez esetben a hirdetés maga megjelenhet teljesen megbízható weboldalakon is, tovább csökkentve az áldozatok gyanakvását) vagy egyszerűen önmagukban is

tömegeket vonzó oldalak létrehozásával (általában ilyenek a kalóz- vagy pornóoldalak, illetve újabban az „ingyenes” sorozatnéző website-ok). Az e-mailek és weboldalak útján történő terjesztés mellett kisebb arányban előfordulnak szofisztikáltabb módszerek is, úgymint a vírusos applikációk fejlesztése és app-áruházakban való közzététele, illetve az sms-ben vagy instant üzenetküldő szolgáltatások útján megosztott linkek alkalmazása (amivel főleg mobileszközöket vesznek célba), vagy éppen magában az operációs rendszerben rejlő, frissen felfedezett sérülékenységek kihasználása. Bár filmekben gyakran visszatérő motívum a fertőzött pendrive használata is, a valóságban ez nem különösebben jellemző fertőzési mód. Még ha kétségtelenül működőképes módszerről is beszélünk (hiszen egészen biztosak lehetünk benne, hogy egy „ott felejtett” pendrive-ot előbb utóbb valaki csatlakoztat egy számítógéphez), a kibertér nyújtotta biztonságos közeget nincs értelme elhagynia a bűnözőknek, ha egyébként a többi módszer is kellőképpen hatásos, illetve emellett tömegesen is alkalmazható (Kapoor et al., 2021).

Értelemszerűen a fertőzés a sikeres támadások szükségszerű szakasza, épp ezért akár jó hírnek is tekinthető, hogy gyakorlatilag az összes fertőzési módszernél szükség van az áldozat valamilyen fokú figyelmetlenségére és közbenjárására (hiszen ez azt jelenti, hogy már egyszerű tudatosítással is nagymértékben csökkenthető lehet egy sikeres támadás kockázata).

A *telepítés* fázisában a sikeresen bejutott kártékony kód ténylegesen is telepíti magát a megfertőzött rendszeren, és észrevétlenül átveszi az irányítást azon rendszerelemek felett, amelyekre a végrehajtás későbbi fázisában szükség lesz. Hogy melyek ezek, az főleg a zsarolóvírus kategóriájától, illetve a megtámadott rendszer típusától függ. Ez utóbbiak leggyakrabban még ma is a személyi számítógépek, azonban egyre inkább terjednek az okostelefonokat célzó zsarolóvírusok (azon belül is az Android operációs rendszert futtató eszközök), illetőleg megjelentek már az első jelei az IoT (Internet of Things) eszközöket célzó vírusvariánsoknak is.

A *kommunikációs fázis* során a zsarolóvírus általában kiépíti a kapcsolatot az úgynevezett C & C (Command & Control – irányító és ellenőrző) szerverrel. A szerver gyakorlatilag az elkövetők eszköze arra, hogy a települt vírust irányítani tudják, illetve a vírus által küldött (legtöbbször ellopott) adatokat fogadják. Léteznek olyan esetek is, amikor a vírus előre adott utasítások alapján, irányító szerver nélkül, automatizáltan működik, azonban mégis az irányító szerverek alkalmazása az általánosan elterjedt módszer. Ilyen módon az elkövetők meghatározhatják, hogy mikor aktivizálódjon a vírus, kiválaszthatják a titkosítandó fájlokat, illetve szert tehetnek akár olyan adatokra is, amelyek puszta megszerzése is további zsarolási potenciált jelent. A rendszer feletti irányítás megszerzése

okán továbbá képesek lehetnek arra, hogy a vírussal további alrendszereket, vagy a közös hálózaton lévő további rendszereket is megfertőzzenek.

A C & C szerver eléréséhez szükséges IP cím vagy domain sokszor közvetlenül megtalálható a kártékony kódban, ez azonban értékes nyomot jelent a bűnüldöző hatóságok számára, illetve megkönnyíti a vírussal szembeni védekezést is. Ebben az esetben ugyanis a fix szerver irányába tartó kommunikáció letiltásával a vírus megbénítható más rendszereken már azelőtt, hogy a kapcsolatot egyáltalán ki tudta volna építeni. A fejlettebb vírusvariánsok ezért már úgynevezett DGA (domain generation algorithm – tartomány generálási algoritmus) technológiát alkalmaznak, mely során a vírus nagyobb számú domaint generál a kommunikációhoz, amelyek közül nem tudható, hogy az elkövetők melyiket veszik majd ténylegesen igénybe (jelentősen megnehezítve ezzel a jövőbeli szűrést is).

A *végrehajtási fázis* során a kártevő ténylegesen is elindítja azt a folyamatot, ami később a zsarolás alapját fogja képezni. Az ebben a fázisban végrehajtott tevékenység alapján különíthetjük el a legmarkánsabban a különböző zsarolóvírus-fajtákat, melyek két fő családra oszlanak: a titkosító és a zároló vírusokra, illetve ezeket harmadik kategóriaként kiegészíthetik az adatlopó ransomware-ek is.

A zsarolóvírusok legnépesebb, a legtöbb támadásért felelős családját a titkosító (encrypting) vírusok jelentik. Az ilyen ransomware-ek célja, hogy az áldozat számítógépén lévő adatfájlokat titkosítsák, amelyhez több fajta módszert is alkalmaznak. Az egyszerűbb, szimmetrikus kulcsú titkosítás esetén a malware ugyanazt a kulcsot használja a titkosításhoz, amelyet a dekódoláshoz is. Ennek előnye, hogy kevesebb erőforrást igényel, így a titkosítási folyamat gyorsabb lesz és több fájlt érinthet, hátránya viszont, hogy a kulcsot vagy magában a kártékony kódban kell rögzíteni, vagy az áldozat számítógépén kell generálni, majd onnan visszajuttatni a C & C szerverhez (mindkét módszer magában foglalja a kulcs megismerésének elvi lehetőségét, és valóban sok korai zsarolóvírus-variánst sikerült ilyen módon dekódolni). A bonyolultabb, aszimmetrikus kulcsú titkosítás már egy kulcspárral dolgozik, amelynek egyik tagja (a publikus kulcs) a titkosításhoz szükséges, míg a másik (privát kulcs) a dekódoláshoz kell. Mivel a privát kulcsot az elkövetőknek sehol nem kell megosztaniuk, ezért a titkosítás gyakorlatilag feltörhetetlen, másrészről pedig akár minden célpont részére külön kulcspár is generálható. Cserébe ez a módszer sokkal erőforrás igényesebb és csak lassabb titkosítást tesz lehetővé. Mindkét módszer előnyeit ötvözi azonban a hibrid megoldás, mely során a titkosítás szimmetrikus módon történik, és csak a keletkezett szimmetrikus kulcsot titkosítja újra a malware aszimmetrikus módon. Ez a fajta módszer így gyors titkosítást tesz lehetővé nehéz feltörhetőség mellett.

Ha valakit titkosító zsarolóvírus-támadás ért, akkor a következő belépésnél a korábbi adatai helyén ugyanolyan elnevezésű, azonban más (az adott vírusvariánsra jellemző) kiterjesztésű fájlok fogadják, amelyeket semmilyen alkalmazással nem tud megnyitni. A fájlok mellett általában található egy újonnan generált szöveges dokumentum is, ami a végrehajtandó instrukciókat közli az áldozattal (ezt nevezzük zsaroló üzenetnek). A zsaroló üzenetben általában felhívják az áldozatot arra, hogy vásároljon bizonyos összegű bitcoint, majd azt küldje meg az üzenetben megadott címre, cserébe – szintén az üzenetben megadott módon, általában e-mailben vagy webes felületen keresztül – megkapja a dekódoláshoz szükséges kulcsot vagy a teljes dekódoló eszközt. Ritkább esetekben előfordul, hogy a megadott felületen élő (chates) kommunikációt is lehet folytatni az elkövetőkkel, általában az instrukciók gyorsabb megadása vagy éppen a váltságdíj összegén történő alkudozás lehetőségének megteremtése céljából.

A végrehajtási módszer szerinti másik nagy kategóriát a lezáró (locker) típusú ransomware-ek alkotják, amelyek konkrét adatokat ugyan nem titkosítanak az eszközön, azonban valamilyen módon megakadályozzák az ahhoz való hozzáférést. A lezáró zsarolóvírusok száma kisebb a titkosító ransomware-ekhez képest, és főleg a 2010-es évek elején voltak inkább jellemzők, azonban még manapság is találkozhatunk ilyen esetekkel. A kisebb „népszerűség” oka abban keresendő, hogy az ilyen fajta fertőzéssel szemben könnyebb védekezni, ugyanis egy egyszerű rendszer-újratelepítés, hardware-csere, vagy bizonyos esetekben akár újraindítás is megoldhatja a problémát. Vannak azonban olyan eszközök, ahol éppen az ilyen vírusok jelentik a nagyobb veszélyt; ezek jellemzően az okostelefonok (tekintettel arra, hogy esetükben a rendszer-újratelepítés sokszor az adatok elvesztésével is jár, a hardware-elemek cseréje pedig sokszor nem oldható meg a gyakorlatban).

A lezáró zsarolóvírusok is többfajta módszert alkalmazhatnak, melyek közül a leggyakoribbnak a képernyőt zároló ransomware-ek tekinthetők. Ezek – akár alternatív képernyő létrehozásával, akár más módon – „érzéketlenné” teszik a képernyőt bármiféle utasításra, és a feloldást szintén váltságdíj megfizetéséhez kötik. Találkozhatunk továbbá csak a böngésző ablakát zároló vírusokkal is, amelyek általában egy javascript kód segítségével akadályozzák meg a felhasználót, hogy bármiféle utasítást adjon a böngészőnek. Tekintve, hogy az ilyen vírusok hatásainak semlegesítése viszonylag egyszerű, ezért a zárolt képernyőn vagy a böngészőben megjelenő zsaroló üzenetet gyakran ijesztő elemekkel is kombinálják a nagyobb eredményesség érdekében (általában megpróbálják elhitetni az áldozattal, hogy a hatóság zárolta az eszközt valamilyen illegális tevékenység miatt, de előfordultak olyan esetek is, amikor a vírus pornográf felvételeket jelenített meg a képernyőn kikapcsolhatatlanul, ezzel helyezve nyomást

az áldozatra). A lezáró ransomware-ek utolsó, egyben legveszélyesebb fajtáját az úgynevezett MRB (master boot record) vírusok jelentik, amelyek magához a rendszerindításhoz szükséges adatokat módosítják oly módon, hogy már az operációs rendszer alapvető betöltését is megakadályozzák, lehetetlenné téve a legtöbb semlegesítési módszer (például helyreállító eszköz letöltése, böngésző újratelepítése stb.) alkalmazását.

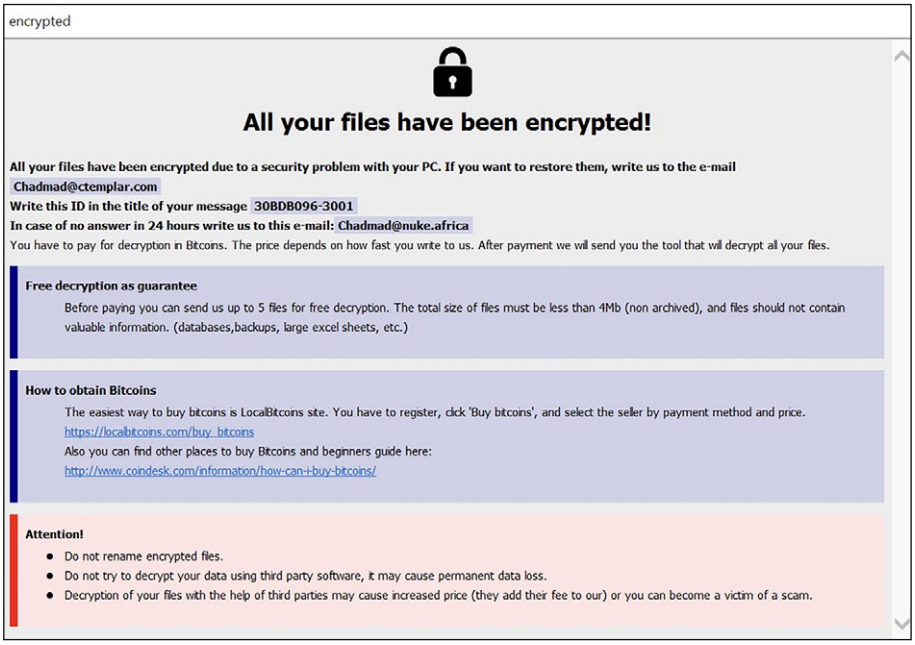
Utolsó végrehajtási módszerként mindenképpen szükséges említést tenni az adatlopó zsarolóvírusokról is, amelyek a bűnözők által alkalmazott legújabb taktikát testesítik meg arra való reakcióként, hogy a potenciális célpontok egyre nagyobb része készít rendszeres biztonsági másolatokat az adatairól, így ezek titkosítása nem jelentene a számára nagy hátrányt. Az adatlopó vírusokkal az elkövetők nem titkosítják az adatokat, hanem egyszerűen ellopják őket a fertőzés után, és azok közzétételével fenyegetik meg az áldozatot (előfordulhat természetesen olyan eset is, amikor a lopástól függetlenül még a titkosítást is elvégzi a vírus, dupla zsaroló potenciált adva az elkövető kezébe). A sikeres adatlopást követően az áldozat kezében védekezési módszer gyakorlatilag nem marad, és teljesen kiszolgáltatottá válik a zsarolóknak: csak arról hozhat döntést, hogy fizet-e, vállalva annak kockázatát, hogy még további összegeket követelnek tőle; vagy nem fizet, vállalva annak kockázatát, hogy az adatokat közzéteszik. Bár a közzététel közvetlen anyagi kárt nem okoz, azonban nagyobb vállalatok esetében hatalmas reputációvesztéssel járhat, illetve különböző hatósági büntetéseket is vonhat maga után (ilyen módon pedig akár súlyosabb is lehet, mint az adatok egyszerű elvesztése a titkosítás miatt). Mindenképpen lényeges különbség azonban az adatlopó, valamint a titkosító és lezáró malwarek között, hogy nemfizetés esetén az előbbinél a zsarolók részéről egy további aktív műveletre van szükség a fenyegetés beváltásához, míg a másik két esetben elég ugyebár, ha nem tesznek semmit. Tekintve, hogy ettől az aktív művelettől az elkövetőknek közvetlenül haszna már nem származik, így azt sokszor a fizetés elmaradásának ellenére sem teszik meg (természetesen az erre való fogadás mindig kockázattal jár), ha pedig mégis, úgy leggyakrabban dark net oldalakon publikálják az adatokat, melyek látogatottsága az átlag állampolgárok körében elhanyagolható (mindazonáltal tény, hogy innentől fogva elvileg bárki bármikor visszaélhet az adatokkal). Ezen körülmények ezért az adatlopó ransomware-ek esetén éppen ellentétes hatással vannak a fizetési hajlandóságra, valamelyest kiegyenlítve az utólagos védekezés lehetetlenségét.

Szükséges végül megjegyezni, hogy az úgynevezett zsaroló e-mailek nem tartoznak a zsarolóvírusok csoportjába (holott sokszor egy lapon említik őket, akár szinonimaként is használva a két kifejezést), hanem teljesen külön kibertámadási kategóriában foglalnak helyet. Zsaroló e-mailek esetén ugyanis a zsarolási

potenciál egyedül az e-mailben előadott történet ijesztő voltában keresendő (legtöbbször erotikus oldalak látogatásával gyanúsítják meg a címzettet, akitől bitcoint követelnek azért, hogy a webkamerával róla készített képeket ne osszák meg az ismerőseivel), azonban az esetek túlnyomó többségében az ilyen üzenetek mögött nincs valós vírusfertőzés, az elkövetők pedig egyszerűen csak a célpontok hiszékenységére építenek. Éppen ezért az ilyen fajta elkövetési módszer során a fentebb említett hat elkövetési fázis közül egyedül a zsarolást találjuk meg, és mindezen okból az ilyen cselekmények külön kezelendők a zsarolóvírus-támadásoktól.

A *zsarolás* szakaszában az elkövetők már túl vannak a titkosításon, és egyértelműen a célpont tudomására hozzák, hogy mi történt vele és milyen módon szabadulhat a fertőzés következményei alól. Mint említésre került, a titkosító vírusok esetén egy hátrahagyott szöveges fájlban, míg a lezáró ransomware-eknél a képernyőn jelenik meg a zsaroló üzenet az instrukciókkal.

1. számú ábra: *A Phobos ransomware zsaroló üzenete*



Forrás: URL3.

A zsaroló üzenetek tartalma és összetettsége erősen változó, azonban legalább egy fizetésre szolgáló bitcoin címet a követelt összeg megjelölésével minden üzenet tartalmaz, emellett pedig általában valamilyen egyedi azonosításra

alkalmas azonosítót az áldozat számára, egy kommunikációs csatornát, ahol fel lehet venni a kapcsolatot az elkövetőkkel (legtöbbször e-mail cím vagy dark netes chat felület útján), a nemfizetés esetén a következményekre való felhívást, esetlegesen pedig instrukciókat a bitcoin vásárlás menetére, és leírást arra vonatkozóan, hogy mit is csinál pontosan a vírus a számítógéppel. Számos alkalommal a fizetési hajlandóság serkentését célzó trükkök is szerepelnek az üzenetben, úgy mint engedmény, ha az áldozat meghatározott időn belül fizet, valamilyen végső határidő, fenyegetés az adatok nyilvánossá tételére vonatkozóan, vagy akár egy felajánlás, hogy néhány kiválasztott fájlt az elkövetők ingyen is dekódolnak (a bizalom építésének jegyében). Amennyiben az elkövetők megjelölnek valamilyen kommunikációs csatornát, úgy akár alkudozás is kezdődhet az áldozatok és a zsarolók között, mely a legtöbbször valóban a váltságdíj összegének csökkentéséhez vezet. A kifizetett váltságdíjak összege azonban így is évről évre nő, és nemcsak abszolút értékben, hanem az egyes kifizetett váltságdíjak átlagos értéke tekintetében is többszörös növekedésről beszélhetünk. A 2010-es évek elején jellemző néhány száz dollárról ez a szám mostanra a több tízezer dolláros tartományban mozog, köszönhetően egyrészt a nagyvállalatok által kifizetett, nem ritkán milliós összegű váltságdíjaknak is (Oosthoek, Cable & Smaragdakis, 2022).

A zsarolóvírusok kapcsán az egyik leggyakrabban felmerülő kérdés, hogy fizessünk-e a zsarolóknak vagy sem. Természetesen amennyiben van alternatív mód az adatok visszaszerzésére (mint például egy biztonsági mentés, vagy a következő fejezetben bemutatásra kerülő No More Ransom projekt), úgy a válasz egyértelmű. Legtöbbször azonban – főleg egy friss vírusvariáns esetén – az adatok gyors visszaszerzésére nincs más reális lehetőség. A bűnüldöző szervek ajánlása ekkor is az, hogy a zsarolóknak semmiképpen se fizessünk, hiszen ez egyrészről további forrásokkal látja el a bűnözőket, másrészről egy következő zsarolás esetén potenciális célpontként tekintenek majd ránk (miután egyszer már fizetési hajlandóságról tettünk bizonyságot), harmadrészt pedig semmi garancia nincs arra, hogy a fizetés hatására a zsarolók valóban betartják az ígéretüket. A már említett Colonial Pipeline elleni támadás során például a biztosított dekódolási eszköz olyan lassúnak bizonyult, hogy a rendszer helyreállításához végül egyáltalán nem vették igénybe, azonban egyes kutatások szerint is átlagosan a kifizetett váltságdíjjal zárult esetek negyedében az elkövetők végül nem szolgáltatnak semmilyen adatot a dekódoláshoz (Conolly & Borrison, 2022). Ugyanakkor – bár még egyszer szükséges kiemelni, a fizetés bűnüldözési szempontból semmilyen módon nem támogatható – sajnos a realitás az, hogy bizonyos helyzetekben a célpontnak a fizetés az egyetlen valós esélye a károk minimalizálására. Nagyobb vállalatok esetén a titkosított adatok

elvesztése a működés olyan fokú zavarát okozhatja, a nyilvánosságra kerülése pedig olyan bizalomvesztést okozhat, ami a váltságdíjként követelt összeg többszörösét kitevő kárhoz, vagy akár a cég megszűnéséhez is vezethet. Mindezzel tisztában vannak a zsarolók is, és részben ez az oka annak, hogy az utóbbi években a támadások hangsúlya a tömegesen célba vett internetfelhasználókról a gondosan kiválasztott, nagy fizetési képességgel és várható hajlandósággal rendelkező cégek felé irányult. Bár a kifizetések számát a vélhetően magas látencia miatt csak megtippelni lehet, bizonyos felmérések a fizetési hajlandóság arányát akár 50% fölé is teszik (Conolly & Borrison, 2022).

Az *együttműködés* fázisa – az előbb kifejtettek alapján – értelemszerűen csak esetleges; amennyiben az áldozat nem fizet, úgy nem is beszélhetünk semmilyen együttműködésről. Fizetési hajlandóság esetén azonban megtörténik az áldozat részéről a bitcoin átutalás (nagyjából a 2010-es évek közepétől fogva a bitcoin véglegesen felváltott minden korábban jellemző fizetési módot), az áldozat pedig szerencsés esetben megkapja az adatok dekódolásához vagy a lezárás feloldásához szükséges eszközt (vagy egy ígéretet arra vonatkozóan, hogy az ellopott adatait nem teszik közé). Az együttműködés fázisa részben a nyomozás irányát is befolyásolja, ugyanis sikeres együttműködés esetén legalábbis lehetőség nyílik a kifizetett váltságdíj nyomon követésére a blokkláncon (az általános tapasztalatok szerint az elkövetők a bitcoin megszerzését követően azt rövid időn belül különböző mixer- vagy egyéb kriptovaluta-szolgáltatókon mozgatják át), vagy éppen a dekódolási eszköz megküldése során használt kommunikációs csatornára (például egy addig ismeretlen e-mail fiókra) vonatkozó adatok is megismerhetővé válnak.

A sikeres együttműködés továbbá a vagyonvisszaszerzés előtt is megnyitja az utat, ugyanis onnantól a nyomozás céljai között kell szerepeljen az elküldött bitcoin visszaszerzése is. Bár ez utóbbi nehéz vállalkozásnak tűnik, időről időre sikerrel végződik (mint ahogy az a Colonial Pipeline esetén is történt, ahol az elküldött 75 bitcoinból az FBI nyomozói egy hónapon belül képesek voltak visszaszerezni mintegy 63 bitcoint), és akár olyan abszurd helyzetekhez is vezethet, amikor az áldozat – az időközbeni árfolyam-növekedés eredményeképpen – éppenséggel hasznot realizál a ransomware támadás miatt (URL4).

A No More Ransom projekt

Mivel a 2010-es évek közepére nyilvánvalóvá vált, hogy a zsarolóvírusok fogják jelenteni a kibertérben a következő évek egyik legnagyobb fenyegetését, ezért a jelenségre a bűnüldöző szerveknek is valamilyen választ kellett adniuk. A lakosság tudatosítására és az áldozattá válás elkerüléséhez szükséges

javaslatok minél szélesebb körben való terjesztésére a nyomozók már ekkor is nagy hangsúlyt fektettek, azonban ez nem volt elég a fertőzések számának visszafordítására, vagy akár csak érzékelhető lassítására. Mindenképpen szükség volt tehát egy olyan eszközre is, amely a már bekövetkezett fertőzés esetén is segítséget nyújthat az áldozatoknak, és egyben megakadályozza, hogy a bűnözők pénzhez jussanak.

Ez utóbbi elgondolás alapján született meg az Europol koordinálása alatt a No More Ransom projekt, mely abból indult ki, hogy ha a titkosított fájlok dekódolását utólag elvégezzük, akkor ezzel a fertőzés káros hatásait gyakorlatilag teljes egészében semlegesítjük: az áldozatok visszakapják az értékes adataikat, a bűnözők pedig nem jutnak bevételhez. Bár az eszköz magához a bűnelkövetőkhöz nem viszi közelebb a nyomozókat, az áldozatok és a bűnmegelőzés szempontjából a legfontosabb célokat teljesíti.

A No More Ransom projekt lényege, hogy a kiberbűnözés ellen küzdő bűnüldöző szervek, IT-biztonsági cégek és egyetemi intézmények közösen együtt dolgoznak egy olyan adatbázis folyamatos építésén, ami tartalmazza a már ismert zsarolóvírus-variánsokat semlegesítő dekodolási eszközöket, és ezeket rendszerezve, széles körben, a használathoz szükséges minden lényeges információt megosztva hozzáférhetővé teszi az áldozatok számára. A No More Ransom projekt tehát alapvetően nem más, mint egy nyilvánosan elérhető webportál, amely az adataink visszanyeréséhez biztosítja a lehető legtöbb eszközt és információt.

A weboldal 2016. július 25-én indult, a kezdeti projektben pedig a holland rendőrség, az Europol Kiberbűnözés Elleni Európai Központja (EC3), a Kaspersky Lab és az Intel Security (jelenlegi nevén McAfee) dolgozott együtt. Az együttműködők listája gyorsan bővült; az indulást követő három hónapban újabb 13 ország bűnüldöző hatóságai csatlakoztak a kezdeményezéshez, köztük Magyarország képviseletében a Készenléti Rendőrség Nemzeti Nyomozó Iroda is. Év végéig a lista pedig még tovább gyarapodott az Európai Bizottsággal és az Eurojusttal, illetve további privát cégekkel is. A weboldal ekkor még csak angolul volt elérhető, és összesen csupán négy zsarolóvírus-variánshoz tartalmazott dekódolási eszközt.

Az Europol ezt követően minden évben sajtóközleményt adott ki az oldal indításának évfordulóján az addig elért eredményekről, illetve a köztes időben is nagy hangsúlyt fektetett további partnerek bevonására. Mindennek meg is lett az eredménye; a legutóbbi, hatodik évforduló során immár 188 partnerről volt lehetőség beszámolni, akik között most már minden kontinens rendőri egységei képviseltetik magukat, éppúgy, mint a legfontosabb vírusírtó és egyéb IT-biztonsági cégek, pénzintézetek, telekommunikációs szolgáltatók, európai uniós szervezetek és az akadémiai világ tagjai is. A számos együttműködő partnernek

természetesen meg is lett az eredménye; az oldalon immáron mintegy 136 dekódolási eszköz található, amelyekkel 165 zsarolóvírus-variáns titkosítási algoritmusa fejthető vissza (URL5).

Időközben maga az oldal is több ráncfelvarráson esett át, és most már 37 nyelven érhető el a dekódolási felület, illetve a zsarolóvírusokra vonatkozó általános tudástár a legfontosabb megelőzési tanácsokkal. A nyelvek között természetesen a magyar is megtalálható.

A platform sikerét jól szemléltetik az eredmények is; az oldalon lévő dekódolási eszközök a mai napig mintegy másfél millió áldozatnak segítettek az adataik visszaszerzésében anélkül, hogy ezért a zsarolóknak fizetniük kellett volna. Már önmagában a megsegített személyek száma is magáért beszél, azonban nem elhanyagolható az a körülmény sem, hogy mindez – a legóvatosabb becslések szerint is – több száz millió dollárnyi forrástól fosztotta meg a vírusok mögött álló bűnszervezeteket.

Kérdésként felmerülhet, hogy honnan is származnak ezek a dekódolási eszközök? Nos, több oka is lehet annak, hogy egy ransomware által alkalmazott titkosítási metódus visszafordíthatóvá válik.

Mivel gyakran a zsarolóvírusok készítői is követnek el hibákat, így magában a vírus programkódjában is lehet olyan hiányosság, ami miatt a vírus által alkalmazott titkosítási algoritmus visszafejthető lesz, amint a hibára valaki rábukkan. Pontosan ez történt például a Petya esetén, aminek kapcsán az egyik áldozat családtagja tette közzé GitHub-on a programkódból levezethető, általa felfedezett módszert (URL6).

Más esetekben maguk az elkövetők osztják meg a dekódoláshoz szükséges adatokat, mint ahogy azt a TeslaCrypt készítői is tették, akik egy sikeres víruskampány után a dark weben hirtelen közzétették – egy szűkszavú bocsánatkérés mellett – a dekódolási eszközök elkészítéséhez alapvetően szükséges mesterkulcsot (URL7). A bűnbánat mellett természetesen más oka is lehet egy ilyen cselekedetnek; a legprózaibb talán az, hogy az elkövetők már elég bevételre tettek szert és úgy gondolhatják, hogy a dekódoláshoz szükséges adatok megosztásának hatására a bűnüldöző szervek figyelme talán más irányba terelődik inkább.

Végül előfordulhat egyszerűen az is, hogy a bűnözőkre a nyomozók bukkannak rá, és a lefoglalt szervereken megtalálják a visszafejtéshez szükséges adatokat. Pontosan ez történt a CoinVault és a holland rendőrség esetében is, akiknek a Kaspersky Lab sietett a segítségére a dekódolási eszköz elkészítésében (URL8).

Bárhogyan is, az együttműködő partnerek jellemzően olyan szervezetek, amelyek a zsarolóvírusokkal így vagy úgy, de kapcsolatba kerülnek, és az erre vonatkozó adatokat (vagy egyes IT-biztonsági vállalkozások esetén már magát a kész dekódolási eszközt) rendszeresen megosztják az Europollal. A szervezet

ezt követően az információkat gyűjti, elemzi, értékeli, a még hiányzó eszközök fejlesztéséhez felhasználja és a végeredményt a portálon közzéteszi. A magyar rendőrség esetében például az Europol által üzemeltetett és a tagországok rendőri egységei által közösen használt malware elemző rendszeren (Europol Malware Analysis Solution – EMAS) keresztül történik a hazai nyomozások során lefoglalt zsarolóvírus-fájlok megosztása, melynek végpontja a KR NNI Kiberbűnözés Elleni Főosztályán található.

A projekt annak a szem előtt tartásával lett kidolgozva, hogy az áldozatoknak a megfelelő eszköz azonosításához és a dekódoláshoz semmilyen különösebb informatikai tudással ne kelljen rendelkezniük. Természetesen nem várható el egy átlagos számítógép-felhasználótól, hogy a titkosított fájlok karakterisztikái alapján kutatást folytasson az interneten és az alapján azonosítsa, hogy egyáltalán milyen vírus áldozata lett (amennyiben erre semmi nem utal a zsaroló üzenetben). A No More Ransom portálon épp ezért a Crypto Sheriff nevű eszköz siet az áldozatok segítségére a vírus azonosításában.

A Crypto Sheriff fül alatt egy egyszerű űrlap felületen találja magát a látogató, amelyen mindössze két dolgot kell megtennie: fel kell töltenie kettő titkosított fájlt a fertőzött számítógépről, valamint be kell másolnia a zsaroló üzenet szövegét a megjelenő ablakba (de akár ez utóbbi is feltölthető .txt vagy .html formátumban).

2. számú ábra: *A Crypto Sheriff felülete magyar nyelven*

Forrás: URL9.

Amennyiben a zsarolóvírus már szerepel az adatbázisban, úgy a Crypto Sheriffől megtudjuk, hogy mely dekódolási eszközt kell letöltenünk a portálról, az eszközök mellett pedig részletes, lépésről-lépésre vezető útmutatókat is találunk azok használatához. A legtöbb esetben azonban nem lesz különösebb nehéz dolgunk: csupán ki kell jelölnünk a titkosított fájlokat a letöltött eszközzel, ami ezt követően elvégzi a dekódolást és újból létrehozza az új, immár titkosítatlan fájlokat is a számítógépen. Természetesen a dekódolás önmagában csak az adatainkat adja vissza, a fertőzést nem szünteti meg, így a vírust ettől függetlenül kell eltávolítanunk a számítógépről (antivírus szoftver segítségével, rendszer visszaállítással vagy akár manuálisan).

Természetesen – és egyben sajnos – azonban nem minden zsarolóvírushoz található dekódolási eszköz az adatbázisban, és ennek oka, hogy sok zsarolóvírushoz egyszerűen még nem is létezik ilyen eszköz (az újabb vírusok esetén pedig értelemszerűen időnek kell eltelnie ahhoz, hogy egyáltalán lehetőség adódjon a dekódolásra). Tekintettel azonban arra, hogy a No More Ransom projekt jelenleg a legszélesebb körű ilyen célú együttműködés, így legnagyobb eséllyel és leggyorsabban ezen a felületen fogják az áldozatok a még nem visszafejthető zsarolóvírusokhoz is a megfelelő eszközt megtalálni a jövőben. Ezekben az esetekben is ajánlott ezért a titkosított fájlokat elmenteni, és időről-időre újra ellenőrizni őket a Crypto Sheriffel.

A No More Ransom projekt jelenleg a rendelkezésre álló leghatékonyabb eszköz az áldozatok számára az adataik visszaszerzéséhez, azonban épp ilyen hasznos a nyomozók számára is a büntetőeljárások során a zsarolóvírusok gyors azonosítására és annak ellenőrzésére, hogy a sértett adatai visszaállíthatók-e (ugyanis a feljelentők többsége még mindig nem ismeri a No More Ransom biztosította lehetőségeket, főleg, ha korábban soha nem került kapcsolatba zsarolóvírusokkal).

Összegzés

A zsarolóvírusok az utóbbi másfél évtizedben a számos vírusvariáns egyikéből rövid idő alatt az egyik leghatékonyabb, legjövedelmezőbb és legkisebb kockázattal járó fegyverré nőtték ki magukat a kiberbűnözők kezében. A kriptovaluták elterjedésével párhuzamosan a ransomware támadások számának rohamos emelkedésének lehettünk tanúi, és emellett a támadások mögött álló technológiák is megállás nélkül fejlődtek. Mindez oda vezetett, hogy ma már minden internetfelhasználónak és vállalkozásnak figyelemmel kell lennie a ransomware támadások kockázataira, a bűnüldöző hatóságok tagjainak pedig tisztában kell lenniük ezeknek

a kártevőknek a jellemzőivel, a működésük főbb elveivel és a bűnözők által használt módszerekkel, hogy hatékonyan tudjanak reagálni ezekre a támadásokra.

Épp ilyen hatékony fellépés igényével és széles körű nemzetközi rendőri összefogás eredményeként született a No More Ransom projekt is, amely zsarolóvírus áldozatok millióinak nyújt segítséget a titkosított adataik visszaszerzésében szerte a világon anélkül, hogy a bűnözők részére váltságdíjat kellene ezért fizetniük. Bármilyen módon fejlődik is tovább a zsarolóvírusok ökoszisztémája, a kiterjedt nemzetközi együttműködésnek a jövőben is központi szerepet kell betöltenie a kiberbűnözők elleni harcban.

Felhasznált irodalom

Aldauiji, F., Batarfi, O. & Bayousif, M. (2022). Utilizing Cyber Threat Hunting Techniques to Find Ransomware Attacks: A Survey of the State of the Art. *IEEE Access*. https://doi.org/10.1109/ACCESS.2022.3181278

Conolly, A. Y. & Borrison, H. (2022). Reducing Ransomware Crime: Analysis of Victims' Payment Decisions. *IEEE*, *119*. https://doi.org/10.1016/j.cose.2022.102760

Humayun, M., Jhanjhi, N. Z., Alsayat, A. & Ponnusamy, V. (2021). Internet of things and ransomware: Evolution, mitigation and prevention. *Egyptian Informatics Journal*, *22*(1), 105–117. https://doi.org/10.1016/j.eij.2020.05.003

Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G. & Davidson, I. E. (2021). Ransomware detection, avoidance, and mitigation scheme: a review and future directions. *Sustainability*, *14*(1), 8. https://doi.org/10.3390/su14010008

Oosthoek, K., Cable, J. & Smaragdakis, G. (2022). A Tale of Two Markets: Investigating the Ransomware Payments Economy. *arXiv preprint arXiv:2205.05028*. https://doi.org/10.48550/arXiv.2205.05028

Oz, H., Aris, A., Levi, A. & Uluagac, A. S. (2021). A survey on ransomware: Evolution, taxonomy, and defense solutions. *ACM Computing Surveys, 1*(1), 1–40. https://doi.org/10.48550/arXiv.2102.06249

Young, A. L. & Yung, M. (1996). Cryptovirology: Extortion-Based Security Threats and Countermeasure. *Proceedings 1996 IEEE Symposium on Security and Privacy*, 129–140. https://doi.org/10.1109/SECPRI.1996.502676

A cikkben található online hivatkozások

URL1: *Wilkie, C.: Colonial Pipeline paid $5 million ransom one day after cyberattack, CEO tells Senate.* https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html

URL2: *As Ransomware Payments Continue to Grow, So Too Does Ransomware's Role in Geopolitical Conflict.* https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-ransomware/
URL3: *Ransomware in the CIS.* https://securelist.com/cis-ransomware/104452/
URL4: *Dutch university wins big after Bitcoin ransom returned.* https://www.dw.com/en/dutch-university-wins-big-after-bitcoin-ransom-returned/a-62337229
URL5: *Hit by ransomware? No More Ransom now offers 136 free tools to rescue your files.* https://www.europol.europa.eu/media-press/newsroom/news/hit-ransomware-no-more-ransom-now-offers-136-free-tools-to-rescue-your-files
URL6: *Petya ransomware dekodolási metódusát leíró GitHub bejegyzés.* https://github.com/leo-stone/hack-petya
URL7: *TeslaCrypt shuts down and Releases Master Decryption Key.* https://www.bleepingcomputer.com/news/security/teslacrypt-shuts-down-and-releases-master-decryption-key/
URL8: *CoinVault: Caught red-handed.* https://www.kaspersky.com/blog/coinvault-in-court/23123/
URL9: *A Crypto Sheriff felülete a No More Ransom portálon.* https://www.nomoreransom.org/crypto-sheriff.php?lang=en

A cikk APA szabály szerinti hivatkozása

Halász V. (2022). Zsarolóvírusok és a No More Ransom projekt. *Belügyi Szemle*, *70*(9), 1887–1905. https://doi.org/10.38146/BSZ.2022.9.9