# „Pénzt vagy életet!” – Zsarolóvírusok az egészségügyi informatikai rendszerekben

**Palicz Tamás dr.[1] ▪ Sas Tibor[1] ▪ Tisóczki József[2, 3]**
**Bencsik Balázs dr.[4] ▪ Joó Tamás[1, 5]**

[1]Semmelweis Egyetem, Egészségügyi Közszolgálati Kar, Egészségügyi Menedzserképző Központ, Budapest
[2]Pest Megyei Flór Ferenc Kórház, Kistarcsa
[3]Óbudai Egyetem, Biztonságtudományi Doktori Iskola, Budapest
[4]Nemzeti Kibervédelmi Intézet, Budapest
[5]Magyar Egészségügyi Menedzsment Társaság, Budapest

Az elmúlt években az egészségügyi adatok értékessége és az egészségügyi folyamatok sajátosságai miatt az adatokkal történő visszaélés egyre nagyobb jelentőséggel rendelkezik. Az Európai Unió általános adatvédelmi szabályozása mellett az általános információbiztonsági, köztük a technológiai és humán szempontok is újraértékelődtek. Cikkünkben bemutatjuk, hogy milyen jelentősége van a zsarolóvírus-támadásoknak az egészségügyi szektorban. A nemzetközi, elsősorban USA-beli adatok alapján az intézményi támadások egyik legfontosabb módszere az elkövetkező években a zsarolóvírus-támadás lesz, és ennek – különösen az egészségügyben, ahol szenzitív és értékes adatok mellett az idő tényleg életet jelent – a jelentősége várhatóan nőni fog. A zsarolóvírusok az adatok titkosítása és az alaptevékenységek blokkolása miatt jelentős hatással lehetnek a gyógyítófolyamatok eredményességére is. A jelenlegi nemzetközi helyzet bemutatása mellett a cikkben kitérünk a legfontosabb lehetséges teendőkre is, amelyeket a mindennapi gyógyítófolyamatokban részt vevők is alkalmazni tudnak a betegellátás folyamatossága érdekében.
Orv Hetil. 2020; 161(36): 1498–1505.

**Kulcsszavak:** kiberbiztonság, adatvédelem, zsarolóvírus, ransomware, kórház, egészségbiztonság

## “Your money or your life!” – Ransomwares in healthcare information systems

In recent years, due to the value of health data and the specificities of health processes, data breaches have become increasingly important. In addition to the general data protection rules of the European Union, aspects of general information security, including technology and human behaviour, have been reassessed. In this article, we present the importance of blackmail (ransomware) virus attacks in the health sector. According to international data, especially in the US, one of the most important methods of institutional attacks will be the extortion attack in the coming years, and this is expected to increase in importance, especially in health care where sensitive and valuable data are truly life-giving. Because of the encryption of data and the blocking of core processes, blackmail viruses can also have a significant impact on the effectiveness of therapy and healthcare. In addition to presenting the current international situation, the article also outlines the most important steps that can be taken by those involved in daily patient’s care to ensure continuity of patient care.

**Keywords:** cybersecurity, data protection, ransomware, hospital, health security

Palicz T, Sas T, Tisóczki J, Bencsik B, Joó T. [“Your money or your life!” – Ransomwares in healthcare information systems]. Orv Hetil. 2020; 161(36): 1498–1505.

(Beérkezett: 2020. március 11.; elfogadva: 2020. május 14.)

**Rövidítések**

EESZT = Elektronikus Egészségügyi Szolgáltatási Tér; FBI = (Federal Bureau of Investigation) Szövetségi Nyomozó Iroda; GDPR = (general data protection regulation) az Európai Unió általános adatvédelmi rendelete; HIS = (health/hospital information system) egészségügyi/kórházi informatikai rendszer; IT = (information technology) információs technológia; NKI = Nemzeti Kibervédelmi Intézet; RDP = (Remote Desktop Protocol) Távoli Asztal Hozzáférési Protokoll; ROI = (return on investment) befektetésarányos megtérülés

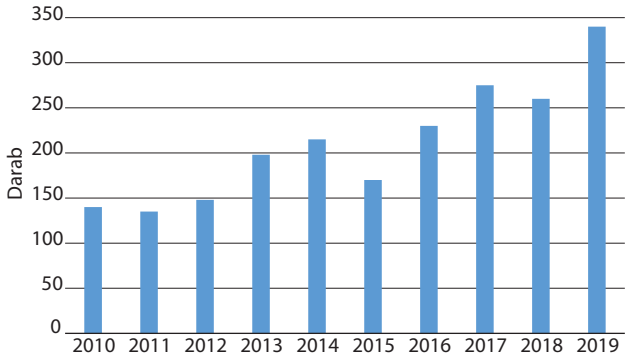
Képzeljük el, hogy egy beteget beutalnak egy megyei kórház sürgősségi osztályára, ahol dolgozunk. A beteg érkezésekor azonban kiderül, hogy nem tudunk alapvető diagnosztikai vizsgálatokat (például laboratórium, képalkotó) végezni, és emiatt a beteget sem tudjuk fogadni: a sürgősségi osztály működésképtelenné vált az informatikai rendszer hibája miatt. A monitorokon egy zsarolóvírus üzenete jelenik meg: „A fájlok elérhetetlenné váltak. Amennyiben hozzájuk akarsz férni, fizess!"

A filmbe illő jelenet a valóságban is megtörtént: 2019 szeptemberében az USA egyik középső részén levő egészségügyi központban (Campbell County Health, WY), ahol 20 kórház volt érintett egy, a fentiekhez hasonló incidensben. A kórház 8 órán keresztül kénytelen volt a betegeket a kb. 100 km-re levő másik egészségügyi intézménybe irányítani. Számos diagnosztikai modalitás – elsősorban laboratórium – nem működött, és 17 napot vett igénybe, amíg teljesen helyreállították a kórházi működéshez szükséges adatokat. A működésképtelenség hátterében zsarolóvírus-támadás állt [1].

Kórházainkban különösen szenzitív adatokat kezelnek az informatikai rendszerek. Az adatok és információk védelme kiváltképp fontos ezekben az intézményekben, hiszen a páciensek teljes élettörténete, kórképe nyomon követhető a medikai vagy kórházi informatikai rendszerekben (a továbbiakban: HIS) megtalálható adatbázisokban [2, 15]. A magánszemélyek adatainak védelmét 2018. május 25-től Magyarországon is az új európai uniós adatvédelmi rendelet (GDPR) szabályozza. Ennek elsődleges célja a személyes adatok egységes szintű adatvédelmének biztosítása. Személyes adatnak bármely olyan adatot tekinthetünk, amely alapján egy személy közvetlenül vagy közvetve beazonosítható (például név, lakhely, e-mail-cím stb. alapján), idetartozik a személyre vonatkozó vélemény vagy értékelés is. Ugyanakkor minden természetes személy egészségügyi adata (például zárójelentések, anamnézis, gyógyszerelés, de a káros szenvedélyekre vonatkozó információk) mellett a biometrikus adatok (például a faji, etnikai származásra, szexuális irányultságra vonatkozó adatok) is mind a különleges személyes adatok körébe tartoznak. Jellemzően ezen különleges személyes adatokat az egészségügyi ellátórendszerekben lokálisan és tömegesen kezelik, ami információbiztonsági szempontból fontos adottság. Kiemelendő, hogy a GDPR mellett hazánkban az egészségügyben keletkező adatok kezeléséről és védelméről az 1997. évi XLVII. törvény is rendelkezik. Magyarország egészségügyi adatvagyona óriási, ennek jelentős részét papíralapon tárolják. Az elmúlt években azonban fontos fejlesztések történtek ezen adatok elektronikus tárolása és feldolgozása érdekében. Itt kell megemlítenünk az Elektronikus Egészségügyi Szolgáltatási Tér (EESZT) kifejlesztését, 2017 őszén annak bevezetését, mely a jövőbe mutatóan képes megvalósítani a betegadatok online, valós idejű továbbítását, tárolását, a hozzáférési jogosultságoknak megfelelő elérését.

Ebben a folyamatban az egészségügyi dolgozók fontos felelősséggel rendelkeznek, és az információbiztonság szempontjából az egyes munkaköröknek és munkaköri csoportoknak a feladata és felelőssége eltérő [3]. A kórházi és egészségügyi rendszerekben tárolt adatok egy része ráadásul annyira specifikus és egyénre jellemző (például genetikai vagy biometrikus adatok), hogy azok megismerésével egy adott személy jól azonosíthatóvá válik, illetve az adatok elemzésével prognosztikus, prediktív értékek és tulajdonságok (esetleg várható megbetegedések) is jósolhatók. Emellett az egészségügyi szolgáltatók működésére jellemző, hogy a nagy rendszerek nyújtotta stabilitás miatt mind szervezetileg, mind egyénileg szívesen használják a kereskedelmi céllal létrejött levelezőrendszereket (például gmail), ami tovább növeli az adatvisszaélések lehetőségét. Olyan is előfordul, hogy a fenti rendszerek rugalmassága, felhasználóbarát sajátosságai miatt a szolgáltatókat felügyelő hivatalok, intézmények kommunikációja is átterelődik ezekre a csatornákra, ami további kockázatokat rejt magában.

Az információbiztonsági fenyegetések nem korlátozódnak csak egy bizonyos típusú és méretű intézményre, hanem minden intézmény ki van téve ennek a fenyegetésnek. Az orvosi csoportoknak és egészségügyi dolgozóknak pedig minden szinten erőfeszítéseket kell tenniük a biztonsági intézkedések megerősítése, a korszerűsített IT-infrastruktúra fenntartása, valamint a biztonsági és „hackelési" eseményekből szerzett ismeretek megosztása érdekében [4]. A kórházi adatvédelmet így nem lehet a pusztán az ott levő HIS-rendszerek védelmére szűkíteni, hanem az egyéb támogatófolyamatok (például kommunikáció, gazdálkodás stb.) esetében is teljes körű és magas szinten biztonságos folyamatokat és infrastruktúrát kell biztosítani a felhasználók valamennyi csoportja számára. Ez azonban többszörösen is nehéz folyamat. Könnyen előfordulnak az intézmények elleni külső támadások, melyek száma az utóbbi pár évben jelentős emelkedést mutatott az egészségügyi rendszerek és intézmények esetében. Az USA évek óta rendszeresen gyűjti az egészségügyi rendszerhez kapcsolódó adatvisszaéléseket, amelyek alapján mind az érintett intézmények, mind az érintett betegek/ügyfelek száma folyamatosan növekedett az elmúlt években. Az Amerikai Egyesült Államok egészségügyi ellátásért felelős minisztériuma (US Department for Health and Human Services, Office for Civil Rights) által 2010 óta gyűjtött adatok egyértelműen mutatják a fenti változást (adat-




**1. ábra** Az információbiztonsági incidenst elszenvedő egészségügyi szolgáltatók számának alakulása 2010 és 2019 között az USA-ban [1]

szolgáltatásukban csak azok az események szerepelnek, amelyek legalább 500 ügyfelet/beteget érintettek) *(1. ábra)*.

## Releváns fogalmak

A zsarolóvírusok működésének pontos megértéséhez minimális informatikai ismeret szükséges. A fogalmak bemutatásakor a magyar és az angol kifejezést egyaránt használjuk: az utóbbit elsősorban azért, mert az informatikában ezek a mindennapokban egyenértékű kifejezésekként vannak jelen. Ezek közül a legfontosabbak [5]:

- *Rosszindulatú program (malware):* Gyűjtőfogalom, amely valamennyi, kártékony számítógépes programot magában foglal. Ezek közül a legismertebbek a vírusok, férgek, kémprogramok, zsarolóvírusok, trójai programok vagy reklámprogramok. Speciális típusát jelentik az ún. rootkitek, amelyek a támadó számára magas szintű rendszerhozzáférést biztosítanak, vagy az ún. backdoor programok, amelyek a rendszeren egy „hátsó ajtót” kinyitva teszik lehetővé a behatolást.
- *Számítógépes vírus:* Futtatható kód, amely elhelyezi magát egy végrehajtható programban vagy dokumentumban. Az ezek elleni védelem a kórházak többségében megoldott a végpontokon és szervereken: számos olyan, kereskedelmi forgalomban kapható vagy ingyenesen hozzáférhető program található, amely jó hatásfokkal tudja ellenőrizni ezeket a vírusokat.
  Fontos megjegyezni, hogy az elmúlt évek tendenciái alapján olyan mértékű a rosszindulatú kódok számának növekedése, hogy ezzel a legjobban felkészült cégek sem tudnak naprakészen versenyezni.
- *Trójai program:* A trójai programok céljai közé tartozik a rosszindulatú kódok terjesztése a hálózaton (dropper), kémkedés a felhasználó után, erőforrás-kihasználás, valamint adatlopás. Hasznos, sokszor ajándéknak álcázott programról van szó, mely a felhasználó számára nem mutat károkozást, de a háttérben adatot lop, vagy jellemzően kapukat (portokat) nyit ki. Fejlettebb változataik a kémkedés mellett valóban képesek az ígért funkciók elvégzésére is – így csökkentve a lebukás veszélyét.
- *Zsarolóvírus (ransomware)-programok:* Zsarolóprogramok, melyek a felhasználó gépébe bejutva az ott található adatokhoz történő hozzáférést akadályozzák meg. Alapvetően két típusuk lehetséges ezeknek a vírusoknak: az egyik típus (’crypto’ vírusok) jellemzően az adatokat, főként a dokumentumfájlokat kódolja, titkosítja, és hagy egy üzenetet, melyből kiderül, hogy mennyi pénzért hajlandó a dekódolókulcsot odaadni a felhasználónak, aki így visszaállíthatja adatait. A másik típus esetén a hozzáférést gátolja meg a vírus (’locker’ vírusok), így teszik elérhetetlenné a felhasználó számára a működés szempontjából kritikusan fontos fájlokat [6]. Ebben az esetben is a díj megfizetését követően kapja meg a felhasználó a megfelelő kulcsot a fájlokhoz történő hozzáféréshez.
  Az elmúlt években a leggyakoribb zsarolóvírusok az alábbiak voltak: Locky, WannaCry, Bad Rabbit, Ryuk, Troldesh, Jigsaw, Cryptoloker, GoldenEye, Grandcab, Petya. 2019 decemberében hívták fel a figyelmet egy új zsarolóvírusra, amely kifejezetten az egészségügyben jelent meg: a Zeppelin orosz vagy szovjet utódállami eredetű, általában .exe vagy .dll fájlokon keresztül terjed, és nagyon hatásos a hálózatokban történő károkozásban, mert a biztonságimásolat-fájlok (backup files) törlésére is alkalmas. Szintén újgenerációs zsarolóvírus a Maze ransomware, amelynek az a sajátossága, hogy a zsarolási szándékot adatlopás előzi meg. Így az adat felhasználóját vagy tulajdonosát nemcsak a saját rendszerben levő fájlok visszaállítása kapcsán bírhatják fizetésre, hanem az ellopott adatok megsemmisítéséért is kérhetnek pénzt. 2019 novemberében fordult elő, hogy az ellopott betegadatok alapján a betegeket is elérte a zsarolás: pénzt kértek azért, hogy a személyes, egészségügyi vagy éppen genetikai adatokat ne hozzák nyilvánosságra. Erről azért is fontos tudni, mert az utóbbi időben a betegek tájékozódásában az online információszerzés forrásai egyre nagyobb számban vannak jelen [7]. Így a betegek digitális írástudásának elterjedése és az ismeretek szerzésének és az orvos-beteg kommunikáció új formáinak (internetes tájékozódás, e-mail, fórumok, közösségi [social] média stb.) a térnyerése fokozza a zsarolóvírusok megjelenésének lehetőségét a betegek körében is.
- *Titkosítás:* Olyan számítógép-művelet (algoritmus) alkalmazása, mely lehetővé teszi, hogy csak bizonyos felhasználók használhassanak meghatározott adatokat, illetve a titkosítással egy üzenetet is megváltoztathatunk úgy, hogy abból az eredeti üzenet csak valamilyen, kizárólag a küldő és a címzett által ismert eljárás segítségével fejthető vissza.
- *Kriptovaluta:* Olyan digitális fizetőeszköz, amely csak online használható és juttatható el egyik felhasználótól közvetlenül a másik felhasználóig. Ennek legis-

mertebb formája a bitcoin, amely „decentralizált digitális valuta”: ez azt jelenti, hogy amíg a legtöbb valutát bank, pénzintézet vagy elszámolóház kezeli, addig a bitcoinok közvetlenül az egyik embertől a másikhoz kerülnek, harmadik személy bevonása nélkül.

## A zsarolóvírus-fertőzés folyamata – „kórélettan”

Az USA Szövetségi Nyomozó Irodájának (FBI) ezzel a területtel foglalkozó anyaga három tipikus „fertőzési” lehetőséget ír le [8]:

1. E-mail-adathalász (phishing)-kampányok vagy célzott adathalászat (spear phishing): a kiberbűnöző valamilyen fertőzött csatolmányt vagy arra mutató linket küld a kiszemelt szervezet kiszemelt felhasználójának. Míg korábban az általános „támadások” voltak jellemzőek, manapság sokkal célzottabban és jobb hatásfokkal használják ezt az eszközt. Ennek a támadási fajtának a kivédésére az egyik leghatékonyabb forma, ha a felhasználókat folyamatos képezzük, és naprakész információval biztosítjuk tájékozottságukat.

2. A Távoli Asztal Hozzáférési Protokoll (Remote Desktop Protocol – RDP) sérülékenységei: Az RDP olyan informatikai hálózati protokoll, eljárás, amely lehetővé teszi a felhasználó számára, hogy az interneten keresztül ellenőrizze a számítógép erőforrásait és adatait. A számítógépes bűnözők különböző módszerekkel (például nyerserő- [brute-force] támadással vagy a ’sötét internet’ [dark web] piacterein vásárolt hitelesítő adatokkal) bejutnak az áldozatok rendszerébe, és jogosulatlan RDP-hozzáférést kapnak. Az RDP-hozzáféréssel a bűnözők számos rosszindulatú szoftvert – ideértve a zsarolóvírusokat is – telepíthetnek az áldozatul esett felhasználó rendszereibe.

3. Szoftversérülékenységek: A számítógépes bűnözők kihasználhatják a gyakran használt szoftverek biztonsági gyengeségeit, hogy megszerezzék az áldozatok rendszereinek ellenőrzését, és telepíthessék a zsarolóvírust. A különböző típusú sérülékenységekről a Nemzeti Kibervédelmi Intézet (NKI) napi szinten tájékoztatja a felhasználókat, érdemes azokat rendszeresen követni [9].

Az alábbiakban a zsarolóvírus-fertőzés egy tipikus esetét írjuk le:

1. A levelezőszerverre e-mail érkezik, amely egy csatolmányt is tartalmaz. Ez jellemzően olyan dokumentum, mely az átlagos felhasználóban nem kelt gyanút. Nagyon gyakran valamilyen számla, megrendelés vagy éppen valaminek a leírása található a csatolmányban: a kifinomultabb módszerek még azt is figyelembe tudják venni, hogy mi a szervezet alapfolyamata, és valami ahhoz kapcsolódó tevékenységet szimulálnak. Például gyakran található ’order, shipment, payment, invoice’ stb. a fájlok elnevezésében. (Például INVOICE_050975_titkarsag.zip – amelynél a titkarsag elnevezés arra utal, mintha a szolgáltatást onnan rendelték volna meg. Ebben az esetben a titkarsag@ e-mail-címen keresztül támadnak).

2. A kiválasztott felhasználó belép a rendszerbe, majd a szokásos munkamenetnek megfelelően áttekinti az előző nap végi és a korai reggeli e-maileket, majd megnyitja a káros fájlt tartalmazó e-mailt és az annak mellékleteként érkezett csatolmányt is.

3. Ezután a folyamatok elindulnak: a fertőzés, kódolás folyamata az adott felhasználó által elérhető összes mappára kiterjed.

4. A csatolt (például tömörített .zip) fájlban egy trójai (dropper) is van, amely egy Javascript-en keresztül (például http://berrysred.in/image/flags/…/404.php?f=404) letölti az összetevőket. Így megindul a titkosítás és az állományok átkódolása.

5. Ezt követően a dokumentumokat tartalmazó könyvtárakba lépve egy ’text’ üzenetben megtaláljuk a címet, ahonnan letölthető a visszaállító kód. A letöltés előtt azonban a szintén itt megadott számlaszámra kriptovalutában utalni kell egy meghatározott összeget.

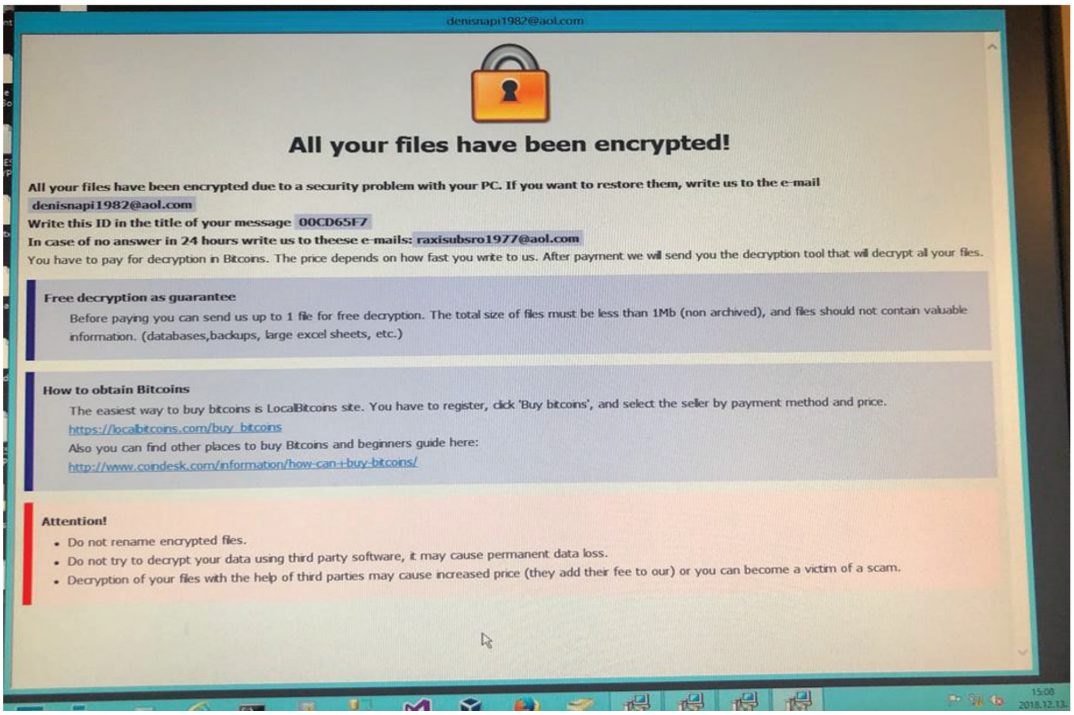
6. A zsaroló külön figyelmeztetést is küldhet annak érdekében, hogy legyen időnk átgondolni a fizetés-nem fizetés lehetőségét. A 2018 decemberében, egy magyar kórházban lezajlott támadás képernyőképén jól kivehetők az alábbiak: a vírus tájékoztatást ad, hogy mi történt (titkosítás), majd iránymutatást kap a felhasználó, hogy hogyan kell a díjat fizetnie. Ebben az esetben a képernyőn nincs olyan információ, amely arra utalna, hogy az áldozat számára mennyi idő áll rendelkezésre *(2. ábra)*.

7. Amennyiben a korábban bemutatott, újabb fejlesztésű vírusokkal találkozunk, akkor arra is egyértelmű iránymutatást kapunk, hogy mennyit és hogyan kell fizetni az ellopott adatok megsemmisítéséért, illetve hogy mennyiben érinti az ügyfeleket (például betegeket) a zsarolás.

## Zsarolóvírusok az egészségügyben

Az elmúlt években a kiberbűnözés egyik leghatékonyabb formája az ún. zsarolóvírusokon (ransomware) keresztül valósult meg. Ennek a formának a terjedése azért lett népszerű, mert viszonylag egyszerű eszközökkel, valamint gyors és magas pénzügyi megtérüléssel lehet elkövetni ezt a bűncselekményt.

Manapság a weben is elérhetők olyan fejlesztőeszközök, amelyekkel előállíthatók a zsarolóvírusok különböző változatai. Természetesen vannak és folyamatosan jelennek meg újonnan fejlesztett változatok is, amelyeket jól felkészült kiberbűnözők fejlesztettek ki. Itt több esetben is olyan jelentős felkészültséggel és erőforrásokkal rendelkező szereplők állnak, amelyek esetében feltételezhető valamilyen nemzeti támogatás is. A 2016–2017-ben a világon végigsöprő, az egészségügyi szektort is érintő [10] WannaCry zsarolóvírus hátterében az északkoreai Lazarus-csoportot sejtik, de ennek igazolása természetesen nehéz és körülményes, és inkább indirekt jeleken keresztül lehet erre következtetni.




**2. ábra** | Egy magyar kórházban lezajlott zsarolóvírus-támadás során lefényképezett képernyőkép [forrás: a szerzők saját ábrája]

A zsarolóvírusok terjedésének másik fontos szempontja, hogy az adatvisszaéléssel szemben – amikor az egészségügyi rendszerből érzékeny, de rendkívül értékes adatokat szereznek meg, és később azokat valamilyen módon értékesítik a dark weben – a zsarolóvírusok esetében rövid idő alatt (néhány óra vagy nap alatt) eldől, hogy a kiszemelt áldozat fizet vagy nem fizet. A fizetés kriptovalutában történik, így azok nem követhetők nyomon, és gyakorlatilag azonnal hozzáférhetők a világ bármely pontján. Szakértői anyagok szerint a zsarolóvírusok esetén a befektetésarányos megtérülés (return on investment – ROI) 1425% is lehet, amely extrém magas. Ez természetesen összefügg azzal is, hogy nagyon alacsony a belépési korlát, vagyis kis befektetéssel (eszközök, tudás stb.) be lehet lépni erre a „piacra".

Szintén szerepet játszik a terjedésben – és ez különösen az egészségügyre jellemző világszerte –, hogy az informatikai infrastruktúra és az információbiztonsági tudatosság sokkal fejletlenebb, mint például a pénzügyi szektorban. Az egészségügyi szervezetek esetében a rendelkezésre álló pénzügyi források allokációja kapcsán elsődleges szempont, hogy – a szervezeti missziót teljesítendő – minél több pénzügyi forrást a betegek gyógyításának közvetlen és közvetett költségeire lehessen fordítani: magasan képzett egészségügyi dolgozók alkalmazása vagy a legkorszerűbb eszközök és fogyóanyagok beszerzése történjen meg. Az informatika mint támogatófolyamat nem tartozott az egészségügyi szervezetek, kórházak kulcsfolyamatai közé: operálni úgy is lehet, hogy nincs semmilyen informatikai támogatás. Emellett az egészségügyön belül a gyógyítófolyamatokra nem volt jellemző az ipari kémkedés: amíg a betegadatok papíralapon gyűltek, nehéz volt nagy tömegben és könnyen feldolgozhatóan előállítani azokat az adatokat, amelyek a kutatás-fejlesztés-innovációs tevékenységhez megfelelő alapot jelentettek.

Az elmúlt években bekövetkezett változások, elsősorban a diagnosztika (például laboratórium, képalkotás) területén végbement fejlődés miatt azonban az egészségügyi szervezetek informatikai és információbiztonsági szempontból kiszolgáltatottabbá, sérülékenyebbé váltak. A betegek gyógyítására használt technológiáknak a fejlődését, az azokat támogató informatikai eszközigénynek a növekedését nem kísérte az információbiztonságra fordított erőforrások növekedése és ahhoz kapcsolódóan a humántényező fejlesztése. A 2016-os „zsarolóvírus-pandémiát" megelőzően világszerte jellemző volt, hogy a nagy kórházi rendszerekben is a biztonsági frissítést nem követő operációs rendszereket (gyakran még WinXP operációs rendszereket) futtató informatikai eszközöket használtak. A felhasználók pedig gyakorlatilag semmilyen ismerettel nem rendelkeztek a zsarolóvírusok természetéről [10].

## A zsarolóvírusok számának alakulása – „epidemiológia"

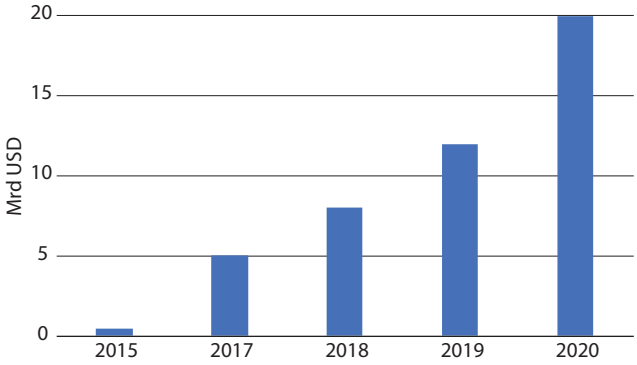
A zsarolóvírusok számának alakulásáról nincsenek megbízható adatok. A különböző biztonsági és biztonsági tanácsadással foglalkozó cégek évente adnak ki jelentéseket a legfontosabb tendenciákról és számokról. 2019. év végén jelent meg az EMSISOFT nevű cég kimutatása, amely az USA számait publikálta [11]. Éves jelentésük

előkészítése során a konkrét számokat és a tendenciákat olyan jelentősnek találták, hogy már 2019. december közepén közzétették a jelentést, majd év végén aktualizálták. A jelentés szerint 2019-ben a zsarolóvírus-támadásokkal leginkább érintett szektor az egészségügy volt: 764 egészségügyi szolgáltatót ért ilyen támadás, miközben 113 állami vagy helyi önkormányzati szervet és hivatalt, és 89 oktatási intézményt (egyetem, főiskola, tankerület) támadtak. A ransomware-vírusok által okozott károk költségét 7,5 Mrd USD-re becsülte a tanácsadó cég (ez valamennyi szektorra vonatkozó becslés). Egy másik elemzés 2019-re globálisan 11,5 Mrd USD-re becsülte a zsarolóvírusok által okozott károk költségét. Ugyanezen becslés 2021-re 20 Mrd USD-re teszi az okozott károkat [12]. Ez azt is jelenti, hogy a becslés szerint 2021 végére minden 11. másodpercben történik majd egy zsarolóvírus-támadás. Ha ezt összevetjük az EMSISOFT 2019-es tényadataival, amelyek a szektorokat hasonlítják össze, egyértelműen megállapítható, hogy az egészségügy lesz az a szektor, amely a zsarolóvírus-támadásoknak a leginkább ki lesz téve. A *3. ábra* jól mutatja, hogy a kezdeti „lineáris" növekedést 2020–2021 fordulóján exponenciális ugrás váltja. Ennek okai között a korábban már felsorolt tényezők játszanak szerepet: alacsony belépési korlát, magas ROI, kriptovaluták miatti láthatatlanság.

Ezzel összhangban van a Malwarebytes 2019. negyedik negyedévben kiadott jelentése, amely az egészségügyre jellemző előző évi adatokat és tendenciákat foglalja össze a kiberbűnözés szempontjából [13]. A rendelkezésükre álló USA-beli adatok alapján 2018 végéhez képest 45%-kal nőtt a végpontokon észlelt incidensek száma (14 000-ről 20 000-re). Kiemelkedően nőttek a trójai malware-ekkel történt visszaélések (82%-os növekedés). Ezek közül az Emotet és a Trickbot nevű trójai fertőzés fordult elő számottevően. Ez a jelentés is megerősíti, hogy – figyelembe véve a trójai fertőzések dinamikáját és az azt követő hatásokat – 2020-ban várhatóan növekedni fog a zsarolóvírussal kapcsolatos incidensek száma is.

Érdemes megemlíteni az FBI által 2019. október 2-án kiadott jelentést, amelynek adatai mintha nem esnének teljesen egybe a biztonsági cégek jelentéseivel. Az FBI szerint a zsarolóvírus-támadások száma 2018-hoz képest érdemben nem változott (ez valamennyi szektor adatait tartalmazta), azonban sokkal szofisztikáltabbak, specifikusabbak és költségesebbek lettek a zsarolóvírus-támadások által okozott károk és azok közép- és hosszú távú következményei [8].

A jelenlegi magyar jogszabályi környezetben a Nemzetbiztonsági Szakszolgálat szervezeti keretei között működő NKI gyűjti azokat a rosszindulatú információbiztonsági eseményeket, amelyek az egészségügyi intézményeket érik. Ehhez azonban az események jelentése szükséges, amely esetleges, és sok esetben jóval az incidenst követően kerül rá sor. Az események korai jelzése nemcsak a helyreállítást segíti, hanem segíthet a károkozó eredetének és szándékának kiderítésében, valamint a főbb sérülékenységek feltárása hozzájárul az egészségügyi intézmény információbiztonságának növeléséhez is. A fentiek miatt az NKI adatai nem tekinthetők reprezentatívnak, azonban 2020. első negyedévi adatok alapján elmondható, hogy a magyar egészségügyi intézményekben a zsarolóvírusok okozta támadások a harmadik leggyakoribb típusú támadást jelentik.




**3. ábra** A zsarolóvírusok által okozott károk költségeinek becslése 2020–2021 fordulójáig [1]

A tendenciákkal kapcsolatban összességében az alábbiak fogalmazhatók meg:

1. A jelenleg rendelkezésre álló adatok elsősorban az információbiztonsággal foglalkozó cégektől származnak, kevés megbízható állami adatbázis áll rendelkezésre.

2. Ezen adatok reprezentativitása (terület, szervezet típusok, szektorok szempontjából) nem mondható meg egyértelműen, így nehéz a teljes sokaságra vonatkozó következtetést levonni, az azonban mégis elmondható, hogy az egészségügy a zsarolóvírus-támadások egyik fontos területe.

3. A zsarolóvírusok működése alapján feltételezhető, hogy a trójai malware-ek számának növekedése együtt fog járni a zsarolóvírusok számának növekedésével, ami az elkövetkező években fog kicsúcsosodni.

## Egészségügyi hatások

A zsarolóvírusok általános hatásain (egészségügyi ellátási vagy más, üzleti támogatófolyamatok megszakadása, bizonytalan időre történő felfüggesztődése, a folyamatok helyreállítási szükségessége, reputációcsökkenés, közvetlen pénzügyi hatások a zsarolási és a helyreállítási díj miatt) kívül vannak az egészségügyre jellemző hatások is. Ezek elsősorban az egészségügyi szolgáltatás sajátosságaiból erednek. A zsarolóvírusok által okozott legfontosabb egészségügyi funkciózavarokat az eddig bekövetkezett zsarolóvírus-támadások tapasztalatai alapján a következőkben határozták meg [9]:

1. Sürgősségi szolgáltatást kell felfüggeszteni, és emiatt a sürgősségi ellátást igénylő betegeket más ellátóba kell irányítani. Az ellátórendszer szervezése alapján előfordulhat, hogy ez akár 100 km-es távolságot is jelent-

het. Ezekben az esetekben az ellátásszervezésnek és a központi koordinációnak kiemelt jelentősége van.

2. A betegek egészségügyi rekordjai átmenetileg vagy tartósan nem érhetők el. Előfordulhat végleges adatvesztés is, ami az orvosi döntést (diagnózis megállapítása, terápiás döntések) és ezáltal a betegek sorsát jelentősen befolyásolja.

3. Szolgáltatások felfüggesztésére, elhalasztására van szükség: elsősorban tervezett műtéteket, vizsgálatokat kell elhalasztani, illetve emiatt a kórházi felvételeket kell szüneteltetni a nem sürgős ellátások esetében is.

4. A fenti diszfunkciók következtében egy támadás jelentős pénzügyi hatással is jár: egy 2019-es retrospektív elemzés adatai alapján az Angliában 600 egészségügyi szervezetre kiterjedő 2017-es WannaCry-támadás kb. 35 millió font kárt okozott.

## A zsarolóvírus-támadások megelőzése – „prevenció”

Az NKI a honlapján részletes iránymutatást ad a teendőkkel kapcsolatban. Ezek nem egészségügy-specifikusak, hiszen a rosszindulatú támadás sem szektorspecifikus általában [14].

1. A legfontosabb védelmi intézkedés, amelyet tehetünk, hogy adatainkról elkülönített és fizikailag is leválasztható meghajtóra rendszeresen mentéseket készítünk a 3-2-1 elv alapján, azaz a biztonsági mentésből őrizzünk meg legalább 3 példányt, 2-féle adathordozón, amelyekből 1-et tároljunk teljesen leválasztva a hálózatról (offline).

2. Az operációs rendszer, illetve az alkalmazások (Adobe Flash, Java) hibajavításainak rendszeres, naprakész telepítése.

3. Mindenképp javasolt valamilyen vírusvédelmi megoldás használata, illetve naprakészen tartása (termékverzió, felismerési adatállományok frissítése stb.). Egyes vírusvédelmi megoldások képesek gyanús viselkedésminták alapján azonosítani és blokkolni a zsaroló kártevőket, ezáltal megelőzni a fertőzést.

4. Fontos a biztonságtudatos internethasználat: ismeretlen feladótól érkezett e-maileknek ne nyissuk meg a mellékletét – főképp ha ez tömörített vagy dupla kiterjesztésű (.doc.exe) állomány –, sem az e-mailekben szereplő hivatkozásokat.

5. Korlátozzuk a saját, illetve a szervezeten belüli mappákhoz való hozzáférést, az azokhoz tartozó jogokat, illetve tartsuk karban a felhasználói fiókokat.

## Teendők zsarolóvírus-támadás esetén – „terápia”

Támadás észlelése esetén a legfontosabb teendők az alábbiakban foglalhatók össze [14]:

1. Az FBI-hoz hasonlóan az NKI sem ajánlja a fizetést a zsarolóvírus-támadás esetén. Nincs garancia arra, hogy kapunk kódot a visszaállításra, és hogy az működőképes is lesz. Sok esetben szándékosan – vagy programozói hibából kifolyólag – eleve lehetetlenné teszik a visszafejtést.

2. A későbbi visszafejtés reményében célszerű a titkosított állományok megőrzése. A visszafejtésre lehetőséget biztosítanak nyilvános kódállományok, amelyek az interneten is megtalálhatók.

3. Ha már megtörtént a baj, és az intézménybe bekerült a zsarolóvírus, akkor az alábbi teendőink vannak:
- Az érintett eszköz lehető legsürgősebb leválasztása a hálózatról (a hálózati kábel kihúzása, a wifi kikapcsolása, a helyi hálózat lekapcsolása stb.).
- Az intézményi hálózaton meg kell szüntetni a kifele nyitott szolgáltatásokat és valamennyi fájlmegosztást.
- A fertőzött munkaállomás esetében a meghajtó teljes formázása szükséges. A teljes operációs rendszer újratelepítését és az aktív vírusvédelem bekapcsolását követően lehet az adatokat az archív mentésekből helyreállítani.
- Semmilyen hordozható adattárolót (pendrive, külső merevlemez) ne csatlakoztassunk a rendszerhez, hiszen ezzel a fertőzést tovább lehet vinni egy másik számítógépre.
- Az incidens felderítése után további intézkedések szükségesek, amelyek közül az egyik legfontosabb az incidens bejelentése és a kapcsolat felvétele az NKI-val.

A fentiek mellett számos olyan technikai sajátosság is van, amelyet kifejezetten az informatikai területnek, illetve az üzemeltetést végzőknek kell szem előtt tartaniuk, illetve megelőző beavatkozásként megtenniük (például portok kezelése, RDP használata, felhasználói fiókok karbantartása stb.).

## Következtetés

Az egészségügyi szolgáltatók információbiztonsági helyzete nagyon vegyes képet mutat, ami az itt tárolt adatok miatt, illetve az egészségügyi intézmények mint létfontosságú infrastruktúrák miatt különleges jelentőségű. Az információbiztonság szintjének megfelelő „eltalálása” sokszor nagy kihívást jelent: a rendszerek túlzott védelme (például a fizikai, adminisztratív és logikai eszközök túlzott használata) a szervezeti alapfunkciótól von el forrásokat, illetve akár akadályozhatja is az alaptevékenységet végző egészségügyi személyzet betegellátó tevékenységét. Ezzel szemben áll az, amikor a „túlzott rugalmasság” a biztonság rovására megy, így idéz elő információbiztonsági incidenst, illetve szélsőséges esetben (például zsarolóvírus-támadás esetén) így vezethet egy teljes informatikai rendszer használhatatlanságához, szélsőséges esetben az egészségügyi folyamatok teljes (például az egész kórház szintjén) leállásához. A jelenlegi tendenciák alapján az elkövetkező években az egészségügy számára információbiztonsági szempontból az egyik legnagyobb

kihívás a zsarolóvírus-támadások megelőzése, illetve az általuk okozott károk (anyagi és működésbeli) minimalizálása lesz.

*Anyagi támogatás:* A cikk megírása anyagi támogatásban nem részesült.

*Szerzői munkamegosztás:* P. T.: A cikk koncepciójának kidolgozása, szövegezési feladatok, az általános részek összeállítása. S. T., T. J.: A gyakorlati szempontok kiemelése, szövegezés. B. B.: Minőségbiztosítás, teendők, gyakorlati szempontok megfogalmazása. J. T.: Minőségbiztosítás, a teljes szöveg terjedelmének és szövegezésének véglegesítése. Minden szerző részt vett a cikk teljes szövegének nyelvi és szakmai szempontú javításában. A cikk végleges változatát valamennyi szerző elolvasta és jóváhagyta.

*Érdekeltégek:* A szerzőknek nincsenek érdekeltségeik.

## Irodalom

[1] PBS NewsHour. Ransomware and data breaches linked to uptick in fatal heart attacks. Available from: https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks [accessed: March 10, 2020].
[2] Ködmön J, Csajbók ZE. Information security in health care. [Információbiztonság az egészségügyben.] Orv Hetil. 2015; 156: 1075–1080. [Hungarian]
[3] Kim L. Cybercrime, ransomware, and the role of the informatics nurse. Nursing 2020; 50: 63–65.
[4] Russell Ritenour E. Hacking and ransomware: challenges for institutions both large and small. Am J Roentgenol. 2020; 214: 736–737.
[5] National Initiative for Cybersecurity Careers and Studies (Official website of of the Department of Homeland Security). Explore terms: a glossary of common cybersecurity terminology. Available from: https://niccs.us-cert.gov/about-niccs/glossary [accessed: March 10, 2020].
[6] Kaspersky. What are the different types of ransomware? Available from: https://www.kaspersky.com/resource-center/threats/ransomware-examples [accessed: March 10, 2020].
[7] Varga Zs, Horváth T. Patients' preferences for health-related use of Internet. [Betegpreferenciák az egészségügyi célú internethasználatban.] Orv Hetil. 2018; 159: 2175–2182. [Hungarian]
[8] FBI. Public Service Announcement. High-impact ransomware attacks threaten U.S. businesses and organizations. Available from: https://www.ic3.gov/media/2019/191002.aspx [accessed: March 10, 2020].
[9] Ghafur S, Kristensen S, Honeyford K, et al. A retrospective impact analysis of the WannaCry cyberattack on the NHS. NPJ Digit Med. 2019; 2: 98.
[10] Ehrenfeld JM. WannaCry, cybersecurity and health information technology: a time to act. J Med Syst. 2017; 41: 104.
[11] Emsisoft. The state of ransomware in the US: report and statistics 2019. Available from: https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/ [accessed: March 10, 2020].
[12] Adaptus. Global ransomware damage costs predicted to reach $20 billion (USD) by 2021. Available from: https://adaptus.com/6836-2/ [accessed: March 10, 2020].
[13] Malwarebytes. Cybercrime tactics and techniques: the 2019 state of healthcare. Available from: https://resources.malwarebytes.com/files/2019/11/191028-MWB-CTNT_2019_Healthcare_FINAL.pdf [accessed: March 10, 2020].
[14] National Cyber Security Center. [Nemzeti Kibervédelmi Intézet.] Available from: https://nki.gov.hu/ [accessed: March 10, 2020]. [Hungarian]
[15] Szócska M, Joó T. Health security issues. In: Finszter G, Sabjanics I. (eds.) Security challenges in the 21st century. Dialóg Campus Kiadó, Budapest, 2018; pp. 335–346.

(Palicz Tamás dr.,
*Budapest,* Üllői út 26., 1085
e-mail: palicz@emk.sote.hu)

*„Knowledge is power."* (Sir Francis Bacon, 1561–1626)
(A tudás hatalom.)