BLACK CELL
Protecting critical infrastructures

A zsarolóvírus támadások jellemzői, trendjei, valamint azok esetén alkalmazandó eljárások és előremutató gyakorlatok

Tartalom

Bevezetés

A zsarolóvírus (ransomware) támadások gyakorisága évről évre egyre nagyobb mértékben emelkedik. Az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) minden év októberében hozza nyilvánosságra a *Threat Landscape* (2021, 2022) című kiadványát, melyben az aktuális év fenyegetettségeit, trendjeinek alakulását veszi górcső alá. Ebben a dokumentumban, valamint más forrásokban megjelenő megállapítások egyre romló képet mutatnak a zsarolóvírusok megjelenésével, elterjedésével és változásaival kapcsolatban.

Nézzünk meg pár ijesztő, illetve a helyzetképet jobban megvilágító számadatot, mely a ransomware támadások veszélyeit és tendenciáit egyaránt jól mutathatja.

- Míg 2019-ben minden 14. másodpercben egy új vállalatot érintett a zsarolóvírus támadás. Ez a szám 2021-re minden 11. másodpercre csökkent;
- 2020-2021 éveket nézve megduplázódott a követelt váltságdíj összege (úgy a kis-, mint a nagyösszegű követelések esetén megfigyelhető;
- A hat legnagyobb zsarolóvírust terjesztő szereplő csak 2021-ben 40,6 millió dollárt tett zsebre a támadásokkal. Ebből majdnem 25 millió dollárt csupán az első két aktor;
- A támadások száma 28%-kal emelkedett meg 2022 harmadik negyedévében 2021 azonos időszakához képest;
- Az egészségügyi szektorban elkövetett támadások száma 60%-kal nőtt a tavalyi adatokhoz képest;
- A vállalkozásokat ért támadások száma Európában 22%-kal, míg Észak-Amerikában 47%-kal növekedtek meg egy év leforgása alatt;
- A zsarolóvírus támadás áldozatául esett szereplők 32%-a fizeti ki a váltságdíjat, azonban ezen szereplők csupán 65%-a kapja vissza az adatait;
- Az IDC *2021 Ransomware Study* című tanulmánya szerint a globális szervezetek mintegy 37%-a vallotta azt, hogy 2021-ben valamilyen zsarolóvírus támadás áldozata volt;
- A zsarolóvírus támadások áldozatául esett vállalkozások csupán 57%-a tudja visszaállítani az adatait korábbi mentésekből;
- A legmagasabb követelt összeg 2020-ban 50 millió, míg 2021-ben 70 millió dollár volt (arról nincs tudomásunk, hogy ez kifizetésre került-e);
- 2021 után 2022-ben továbbra is a zsarolóvírusok a leggyakoribb rosszindulatú programok;
- Az ilyen jellegű elkövetések közel akkora haszonnal kecsegtetnek, mint a hagyományos szervezetbűnözési formák, például a kábítószer-, fegyver-, vagy emberkereskedelem, azonban a lebukás esélye töredéke ezeknek, így nem meglepő, hogy folyamatosan nő az elkövetések és az elkövetők száma.

A zsarolóvírusokról

A zsarolóvírusok (ransomware) olyan kártékony kódok, amelyek során a támadók titkosítják az áldozat (szervezet) adatait, ezzel önmagában megzavarva az üzletmenet-folytonosságot, és számos esetben váltságdíjat is követelnek a titkosított fájlok feloldásáért vagy a feloldásukhoz szükséges kulcsért. Bizonyos esetekben a támadók nemcsak titkosítják a szervezet adatait, de emellett el is lophatják azokat, mely esetben pénzt (kriptovalutát) követelnek cserébe azért, hogy ne publikálják, vagy adják ki azokat a hatóságoknak, a versenytársaknak. Az utóbbi elkövetési magatartás merőben új, az elmúlt egy-két év eredménye, reagálva arra, hogy a szervezetek egyre nagyobb része megfelelő mentési technikákat alkalmazva már nem fizetett az elkövetőknek – mivel az adataikat vissza tudták állítani –, így kellett egy más módszer, mellyel bármilyen mentési technológia alkalmazása ellenére is fizetésre kényszeríthetik a megtámadott szervezeteket.

Az ilyen típusú károkozók néhány közös jellemzője, hogy:

- titkosítják az adatállományokat;
- zsarolóüzenet jelenítenek meg;
- határidőt szabnak a váltságdíj kifizetésére;
- törlik az állományok egy részét;
- az idő múlásával egyre több állományt tesznek végleg visszaállíthatatlanná.

A zsarolóvírusok általában aszimmetrikus titkosító algoritmusokat alkalmaznak, amelyek nehezen törhetőek, ezért általában csak abban az esetben van mód az állományok visszafejtésére, amennyiben:

- fizetnek a kiberbűnözőknek,
- a vírus készítői programozási hibát vétettek, vagy
- önként nyilvánosságra hozzák a titkosítás feloldásához szükséges kulcsot.

Míg korábban minden felhasználó, az egyszeri „kisembertől" a legnagyobb vállalatig áldozatul eshetett ezen támadásoknak, mára gyakoribb a kis-, közepes- és nagyvállalatok célzott támadása, mely egyúttal nagyobb előnnyel is kecsegtet. Azonban ez nem jelenti azt, hogy a kisebb szereplők – beleértve akár a magánszemélyeket is – ne eshetnének áldozatul ilyen támadásoknak.

Az első ransomware támadás 1989-ben történt, az ún. AIDS-trójai nevű, egészségügyi intézményeket támadó titkosító programmal. A CryptoLocker nevű program első változata 2013 év végén jelent meg, mely a könyvtárak és a fájlok teljes titkosítását végezte. Az első mindenki által jól ismert és számos szervezetet érintő zsarolóvírus támadás a 2016-os Petya volt, majd ezt követte a 2017-es NotPetya/WannaCry, bár ez utóbbit nem is nevezhetjük valódi zsarolóvírusnak, mert bár történt teljes lemeztitkosítás, valamint volt követelés, a kártékony kód úgy lett megírva, hogy azt nem lehetett visszafejteni.

Fizetni, vagy nem fizetni

Az algoritmusok által letitkosított fájlok titkosításának feloldásáért a kiberbűnözők általában komoly – egyre növekvő mértékű – váltságdíjat követelnek, melynek megfizetését a vállalatok igyekeznek elkerülni, azonban a reputációs és egyéb veszteségek ezt sokszor lehetetlenné teszik. Itt jön elő számtalan szervezet életében a kérdés; fizetni, vagy nem fizetni. A helyzet, ahogy sok más helyzet az életünkben és az üzleti világban nem fekete vagy fehér. Számtalan olyan tényező befolyásolhatja, melyre a feleken túl másnak nincsen rálátása. Így nem adható minden helyzetre alkalmazható tökéletes válasz a fenti kérdésre.

A Colonial Pipeline 2021-es fertőzése az egész Észak-amerikai kontinens üzemanyagellátását veszélyeztette, ezért a vezetőség – az FBI tanácsa ellenére – a 4,4 millió dolláros váltságdíjat fizetett ki a zsarolóknak. Az egyes tanulmányok pontos százalékos adatai ugyan eltérnek, de a nagyságrendek jól láthatóak belőlük; a zsarolóvírus támadás áldozatául esett szervezetek kisebb része (~30%) fizet a zsarolóknak a feloldókulcsokért, azonban ezen szervezetek közül csupán alig több, mint a felük (~65%) kapja vissza az adatait a váltságdíj megfizetése ellenére. Ugyan az amerikai kormányzat mellett működő OFAC (Office of Foreign Assets Control) (polgárjogi felelősségre vonás mellett) szankcionálhatónak minősítette a váltságdíjak kifizetését, rengeteg – főleg nagyobb – vállalat inkább fizet, csak a szolgáltatásukba vetett bizalom meg ne rendüljön, vagy az adataik ki ne szivárogjanak. Az ausztrál kormányzat egyenesen odáig ment, hogy a zsarolók által követelt összegek kifizetését illegális cselekménnyé, és komolyan büntethetővé kívánja tenni. Természetesen nem elhanyagolható tény, hogy a váltságdíjak – a nehezen követhető kripto-ügyleteknek köszönhetően – sok esetben terrorcsoportoknál, vagy elnyomó rezsimek kormányzatainál landolnak. Hazánkban ilyen tiltó jogszabály nem létezik.

Azon szervezetek közül, amelyek fizetnek a kiberbűnözőknek, közel 80% nem sokkal az első támadást követően ismét ransomware támadás áldozatául esik. Jól lehet addigra megteszik a megfelelő megelőző lépéseket, a támadások ekkor is komoly károkat – akár csak pár órás leállás esetén is – okozhatnak. A támadók tisztában vannak vele, hogy azon szervezetek, akik egyszer már fizettek, vélhetően újra megteszik ezt.

Két olyan módszer létezik, mellyel a fizetendő összeg csökkenthető, vagy akár le is nullázható; az egyik a zsarolókkal való alkudozás, melynek keretében a követelt összeg csökkentését kérheti a szervezet, s tárgyalások útján ezt a zsarolókkal elintézheti. A másik – hazánkban nem létező – módszer a kiberbiztosítás, mely a szervezeteket egy bármilyen más biztosítási konstrukcióhoz hasonló módon védi az ilyen jellegű közvetlen károktól azzal, hogy egy biztosítási összegig helytáll.

A világ minden bűnüldöző szerve és kiberbiztonsággal foglalkozó hatósága óva inti a szervezeteket a váltságdíj megfizetésétől, ezért – egyetértésben velük – zsarolás esetén azt tanácsoljuk, hogy ne fizessenek a kiberbűnözőknek.

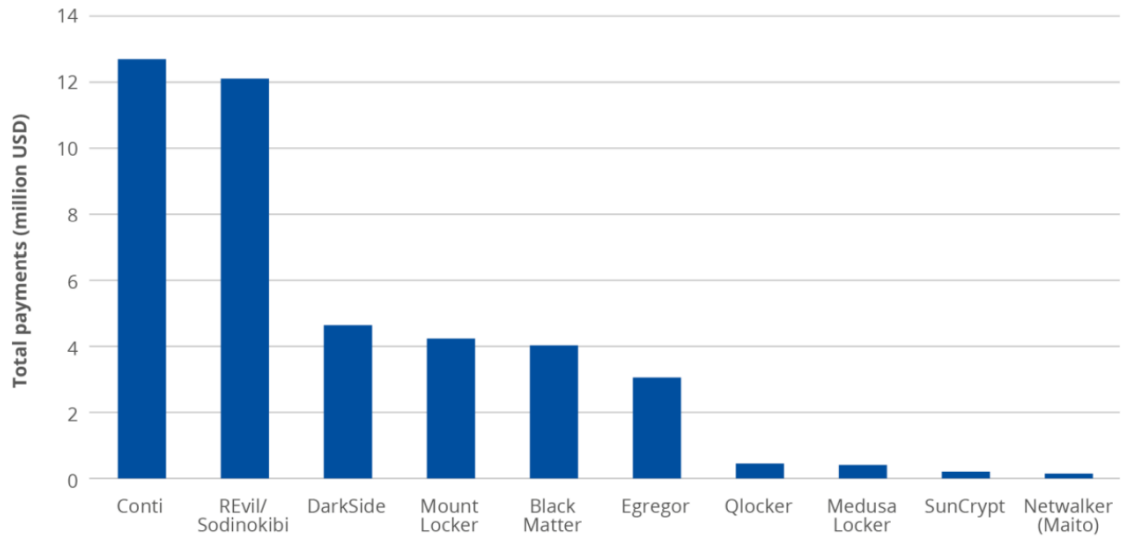
Az elkövetőkről

Érdemes pár szót ejteni az elkövetői körről, valamint annak felépítéséről. A világ figyelme a 2016-os Petya nevű zsarolóvírus támadás után irányult a még viszonylag ismeretlen típusú támadásokra. Figyelemmel arra, hogy ez idő tájt futott fel a kriptovaluták és az online kripto tárcák világa, mely teljes anonimitást tudott biztosítani az elkövetőknek, az első zsarolóvírusok óta ilyen módon követelnek váltságdíjat az áldozatoktól. Mozgás legfeljebb a követelt „pénznemben" történik, a legújabb trendek azt mutatják, hogy a kiberbűnözők már nem Bitcoinban, inkább Moneroban követelik a váltságdíjat.

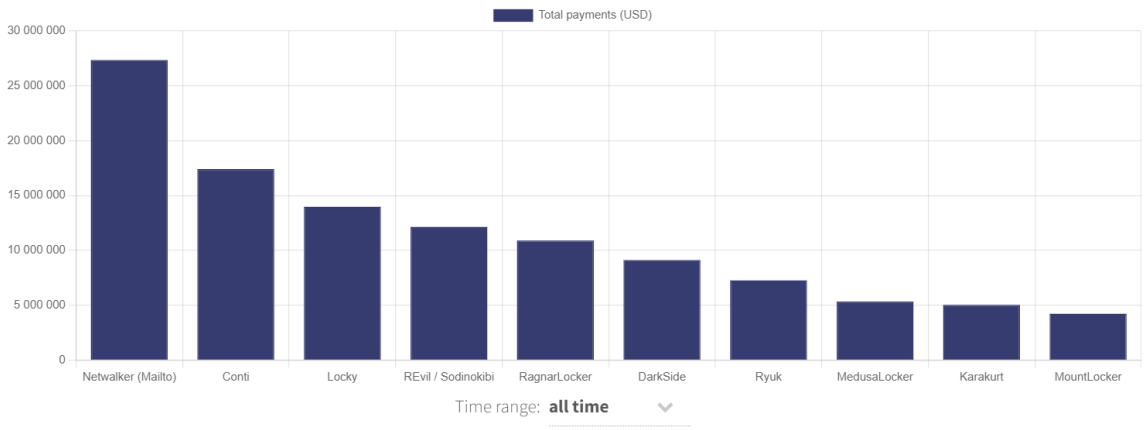
Az elkövetői kör három nagyobb csoportra osztható, mely a motivációjukat is meghatározza.

- Egyrészt beszélhetünk hagyományos értelemben vett, profitorientált (szervezett) bűnözői csoportokról, akiknek egyetlen motivációja a pénz, tehát ekként is választják ki az áldozataikat. A pénzügyi motiváció vezérli minden cselekedetüket, tehát az áldozatok nagy ipari vállalatok, komoly pénzügyi háttérrel és nagy reputációval.
- Félig állami, szabadúszó hekkercsoportok, melyek motivációja szintén pénzügyi. A profitorientált elkövetés feltételezi, hogy amennyiben nem a fenti cselekmények elkövetése áll a fókuszban, úgy őket egyes államok „felbérelhetik", így az általuk támadott – sokszor állami vállalatok, állami infrastruktúrák – entitások nem egy másik állammal, hanem egy hekkercsoporttal állnak szemben. Hívhatjuk őket államilag szponzorált elkövetőknek is.
- Állami elkövetők, melyek esetében egyes államok titkosszolgálatai, katonai csoportjai az elkövetők maguk. Ez a típusú elkövetés roppant ritka, hiszen ez a NATO alapokmányának 2016-os varsói módosítása szerint a kibertér immár a föld a víz és a levegő mellett ugyanolyan hadszíntérnek minősül, mint a korábban felsoroltak. Ilyen típusú elkövetés nyílt konfrontációhoz vezethetne az egyes államok között, mely extrém esetben akár konvencionális katonai válaszcsapást is eredményezhetne.

Természetesen a feni felosztás nem silószerű, így lehetnek átfedések az egyes csoportok, vagy azokon belül felépülő kisebb csoportok között. A legnagyobb elkövetői csoportok bevételei hatalmassá duzzadtak az elmúlt években.

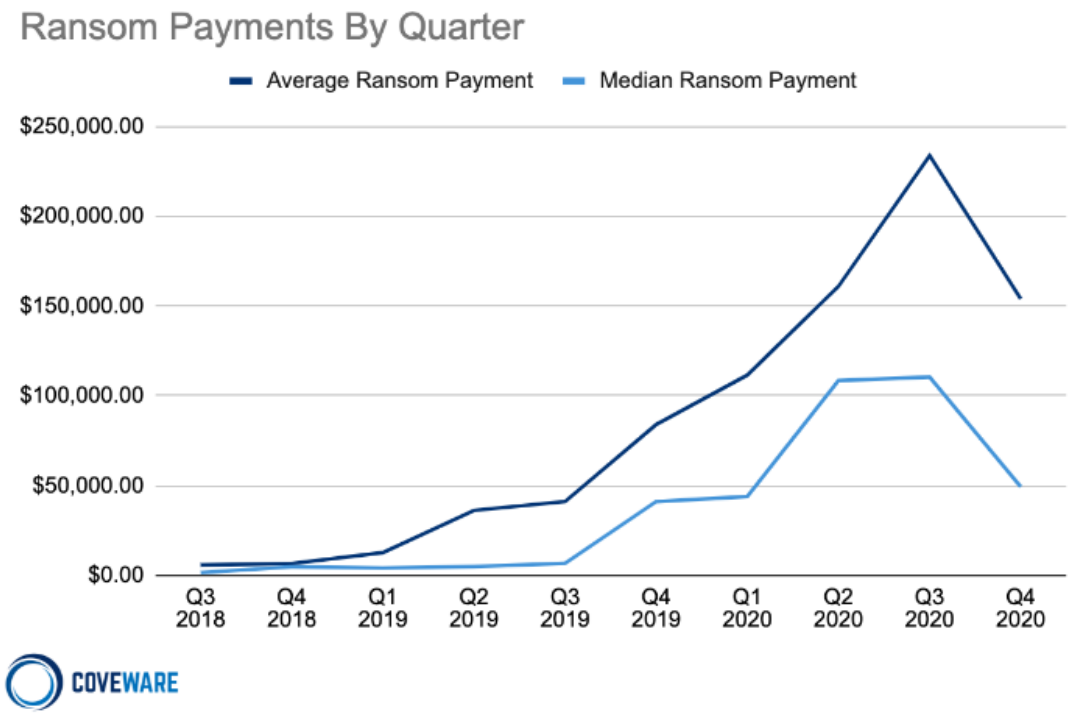


A kiberbűnözői csoportok bevételei (2021)



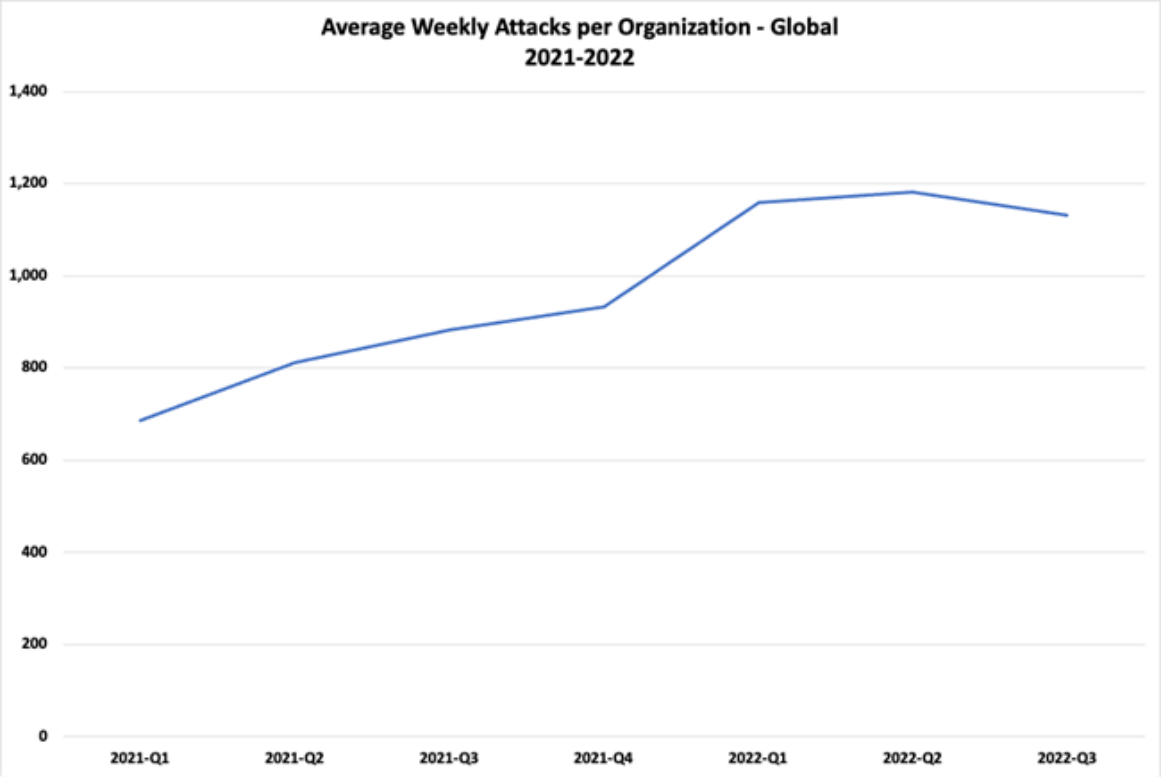
A kiberbűnözői csoportok bevételei (2022)

A fenti felosztásból láthattuk, hogy egyes elkövetők kvázi állami megbízásból dolgozó szereplők nem, vagy csak ritkán kerülhetnek rendőrkézre olyan államokban, ahol őket időről időre „alkalmazzák”.



A zsarolások átlagos és medián összegének alakulása 2018 Q3 – 2020 Q4

A támadások elkövetői általában nem „egyszemélyes elkövetők", hanem képzett, szervezett csoportok, akik megélhetésükként tekintenek a zsarolóvírus támadások elkövetésére. A legnagyobb ransomware családok és operátorok dollármilliókkal károsítják meg a gyanútlan szereplőket.



Általános heti szintű zsarolóvírus támadások alakulása (globálisan) 2021 Q1 – 2022 Q3

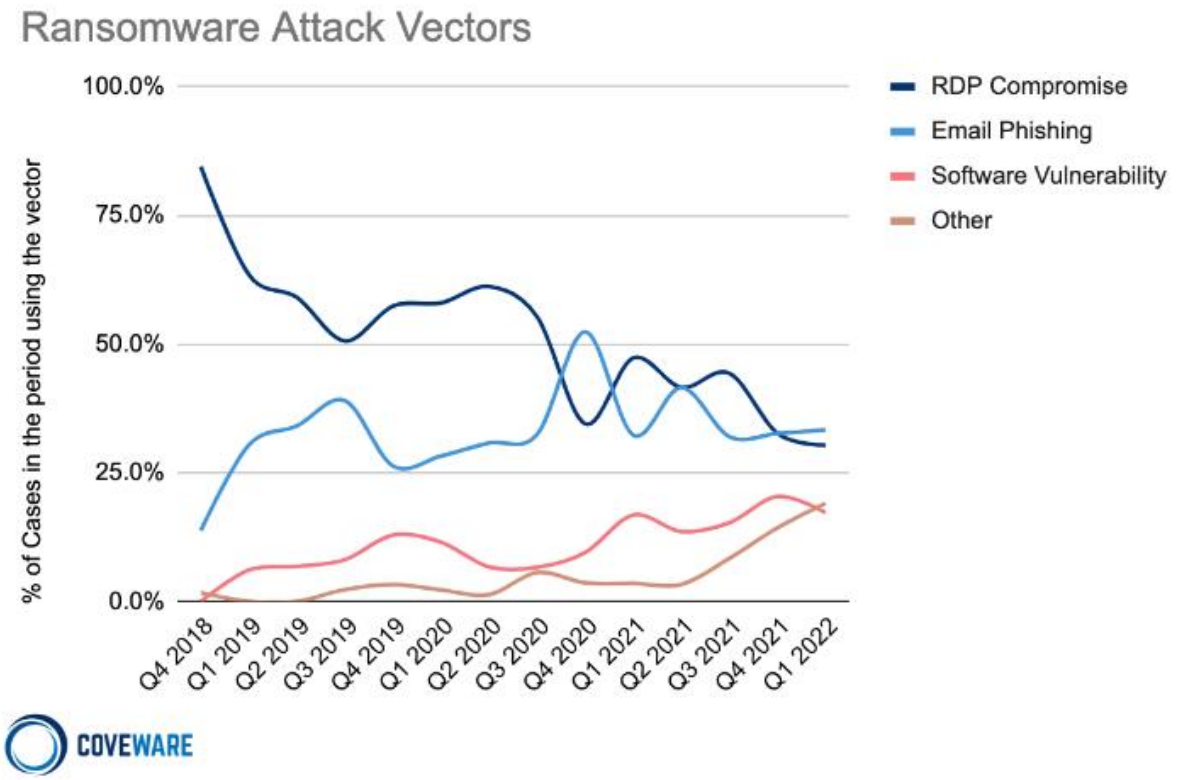
A támadásokról

A támadások az alábbi lépések szerint kerülnek végrehajtásra:

1. **Fertőzés**: A zsarolóprogramnak elég egyetlen végpontra vagy hálózati eszközre telepítenie magát ahhoz, hogy hozzáférést szerezzen az egész hálózat felett. Terjedhet adathalász e-mailben vagy akár fizikai adathordozón (pl. pendrive) is, de egyéb sérülékenységek kihasználása útján is beférkőzhet a rendszerbe.
2. **Kulcscsere**: A telepítést követően a zsarolóprogram jelet küld az elkövetőnek, hogy generálja le a rendszert zároló kriptográfiai kulcsokat.
3. **Titkosítás**: A zárolást követően a szoftver elkezd titkosítani minden fájlt, amit talál, mind a helyi gépen, mind a hálózaton.
4. **Zsarolás**: Most, hogy hozzáférést szerzett, majd letitkosította a fájlokat, a zsarolóprogram megjeleníti az áldozat által végrehajtandó lépéseket, a kulcscsere részleteit, a váltságdíj összegét és a fizetés elmaradásának következményeit.
5. **Feloldás vagy helyreállítás**: Ezen a ponton az áldozat vagy megpróbálhatja eltávolítani a fertőzött fájlokat és rendszereket, és tiszta biztonsági másolatból visszaállítani, vagy kifizetheti a váltságdíjat. Ha fizetésre kényszerül, a tárgyalás mindig egy lehetőség, mellyel csökkenthető lehet a kért összeg nagysága.

A támadások, illetve a kártékony kódok szervezet rendszereibe történő bejutásának két leggyakoribb módja töretlenül az email (phishing), valamint a Remote Desktop Protocol (RDP) szolgáltatások esetén a brute force megoldások alkalmazása, kiváltképpen, ha nincs többtényezős hitelesítés.

A támadások alapvetően biztonsági résekre, sok esetben nulladiknapi (zero-day) sérülékenységekre alapulnak. Ezek egy része nem ismert, melyek ellen olyan jól szervezett és technikailag jól kivitelezett védelmi modellek tervezése és bevezetése nélkül kisebb eséllyel tud védekezni bármely vállalat. Azonban ezeknek egy másik része már nyilvános, melyet a gyártók általában különösen gyorsan szoktak befoltozni. Ez ellen már könnyebben védekezhet bármely szervezet, amennyiben az eszközeit és szoftvereit rendszeresen frissíti. Ez sajnos gyakran elmarad, különösen olyan rendszerek esetén, melyek leállítása pénzveszteséggel járna a vállalatok számára.



A támadási vektorok alakulása 2018 Q4 – 2022 Q1 között

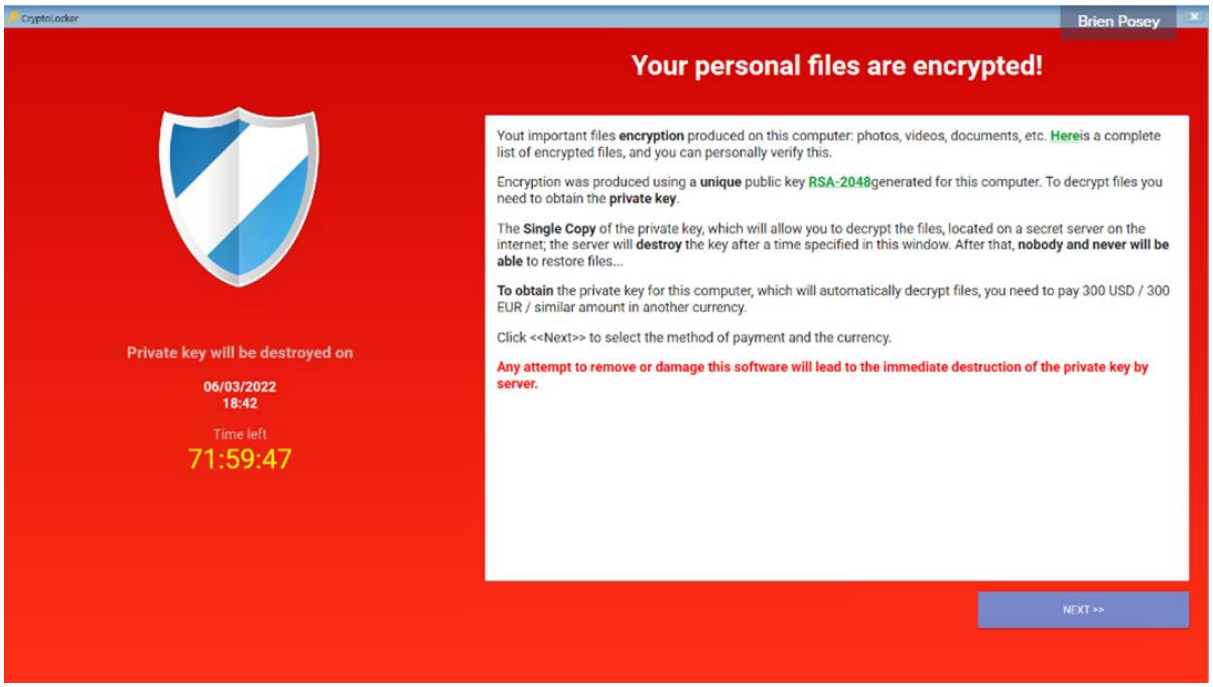
A zsarolóvírusok első széleskörű elterjedése után az elkövetők nyíltan, a megtámadott szervezetek nevével ellátott posztokat tettek közzé, mely biztosította őket a „hekkerkörökben" elérhető szakmai megbecsülésről. Ekkor a cél ugyan a követelt váltságdíj kikényszerítése volt, azonban a kártékony kódok csak az adattárolókat titkosították. Ezt követően a trendek fordultak, már a lemezek titkosításával egy időben az elkövetők a vállalatok adatait is ellopták, majd azokat – a váltságdíj fizetésének elmaradása esetén – a DarkWeben tették közzé. A trendben újabb csavar következett be, mikor az elkövetők már az ellopott adatok nyílt internetre publikálása mellett a versenytársaknak való eljuttatással is fenyegették a vállalatokat. Ez esetben a támadás áldozatául esett vállalatok a saját adataikat „vásárolhatták vissza", illetve a „hallgatás jogát" vették meg a zsaroló által meghatározott összeg megfizetésével.

Érdemes még pár szót ejtenünk egy viszonylag új trendről is, mely a Ransomware as a Service (RaaS) nevet viseli. A felhőszolgáltatások (IaaS, PaaS, SaaS) rövidített elnevezéseihez hasonló névképzés nem véletlen, a kiberbűnözők az általuk írt (low code) zsarolóvírusokat teszik közzé viszonylag alacsony áron, akár már 50 dollárért elérhetőek a DarkWeben. Az ilyen ún. kit-ek önmagukban, vagy a cselekmény elkövetéséből eredő százalékos „osztalék" formájában kerülhetnek kifizetésre a rosszindulatú aktoroknak. A RaaS szolgáltatás a felhőszolgáltatások attribútumaival rendelkezik: paraméterezhető, sőt bizonyos esetekben az infrastruktúrát és a szolgáltatás egészét adja a „szolgáltató", kizárólag a célpontot kell megadnia a szolgáltatást igénybe vevőnek.

Az ilyen RaaS szolgáltatások körébe tartozhatnak az alábbiak:

- Maga a zsarolóvírus és/vagy annak forráskódja;
- Egyéb testreszabási lehetőséget kínáló eszközök - például a célpont operációs rendszerének kiválasztásához, egyéni váltságdíj-felhívás írásához stb.;
- Egyéb rosszindulatú eszközök, például olyan programok, amelyek a titkosítás előtt adatokat lopnak el;
- A zsarolóvírus kezelésére szolgáló infrastruktúra;
- Vezérlőpanel;
- Technikai támogatás;
- Privát fórum az információcseréhez;
- Utasítások (user manual).

Fontos még megemlíteni, hogy a zsarolóvírus üzeneteket is hamisíthatják! Ekkor egy – a valódi zsarolóüzenetre megtévesztésig hasonló – üzenet ugrik fel a felhasználónál, mely a fizetési felszólítás mellett a rendszerben tárolt fájlok titkosításáról tájékoztat. Érdemes megnézni, hogy valóban megtörtént a fertőzés. Ezért az üzenet felugrásakor minden esetben nyissuk meg a feladatkezelőt és ellenőrizzük a futó folyamatokat, melyek között találhatunk olyan ismeretlen feladatot, mely az üzenetet generálhatta. Az üzeneten nincs bezáráshoz használt gomb, így az Alt+Crtl+Del vagy az F11 gomb megnyomásával ki tudunk lépni. Ezzel megerősíthető az üzenet valódisága.



Példa egy hamis zsarolóvírus üzenetre

A következményekről

Már láthattuk, hogy milyen károkat okozhatnak egyes zsarolóvírusok, azonban jelen fejezet rendszerezve tartalmazza azokat a számszerűsíthető és kevésbé mérhető következményeket és hátrányokat, melyekkel minden ransomware támadás áldozatául eső szervezetnek szembe kell néznie. Nézzük előbb a könnyen azonosítható következményeket:

- **Bíráságok, büntetések**

  Ezek lehetnek hatósági bírságok (pl. NAIH, NKI, vagy bármely más hatóság által kiszabott bírság), de lehet bíróság által megállapított kártérítés egy későbbi peres eljárás következményeképpen is.

- **Helyreállítás közvetlen költségei**

  Ezek általában technikai eszközök, valamint szakértői tanácsadás és rendszerintegráció díja (pl. adattárolók vásárlása, hadrendbe állítása, hideg/langyos/meleg tartalék beüzemelése, átköltözés DR site-ra, kommunikációs költségek, túlóra költségek, esetlegesen időlegesen felveendő munkaerő, etc.).

- **A helyreállítás közvetett költségei**

  Ezek általában a helyreállítást követő remediációs cselekményekből adódó költségek, mint például szabályzatok (BCP, DRP, mentési eljárásrend, etc.) megalkotása és frissítése, megfelelő logikai védelmi intézkedések (pl. megfelelő adatmentési beállítások, adattárolók beszerzése, adatkapcsolatok felállítása és szabályozása, többtényezős hitelesítés bevezetése, tudatosító képzések megszervezése és lebonyolítása, etc.). Ezek a további biztonságos működés költségeiként is értelmehetők, melyek korábban történt bevezetése esetén a támadás valószínűleg meg sem történt volna.

- **Leállás idején kieső bevételek**

  Ezek egyértelműen a gyártást, termelést vagy szolgáltatást végző vállalat állásideje alatt kiesett bevételek.

- **Reputációs veszteségek**

  Ezek lehetnek az elpártoló ügyfelek miatt kieső bevételek, de lehetnek a befektetők elmaradozásából eredő bevételkiesések is.

Mindent egybevetve a támadást követő helyreállítás költségei évről évre növekednek. A RaaS, mint modell megjelenése, valamint az adatok ellopása és közzététele, mint új fenyegetési faktor megjelenése a már jól kiépített infrastruktúrával rendelkező vállalatokat is komoly költségek bírására kényszeríthetik, hiszen ilyen esetben a tökéletesen megalkotott mentési eljárásrend, valamint az annak mentén tökéletesen működő mentések mind hiábavalók; ugyan az adatok visszaállíthatók, de az ellopott adatok fizetés hiányában végül az internetre vagy a versenytárshoz kerülhetnek. Mint láthattuk, a támadások jó része még mindig email-en (phishing), valamint RDP-n keresztül történik. Ezért egy jól felépített külső védelmi rendszer (határvédelmi megoldások, megfelelően konfigurált tűzfalak,

hálózatmonitorozás, valamint jól konfigurált SIEM/SOAR megoldások) is mit sem ér, ha a felhasználói tudatosság hiánya miatt bármely dolgozó fertőzött csatolmányt nyit meg, vagy fertőzött linkre kattint.

Mindent egybevetve a vállalatoknak meg kell fontolniuk, hogy a támadások megelőzése érdekében nagyobb összegeket invesztáljanak a kiberbiztonságuk kialakításába és fenntartásába. Ez általában ritkán találkozik a profitorientált felsővezetői elvárásokkal, mivel nehéz kialakítani a biztonságtudatos hozzáállást úgy, hogy a kiberbiztonsággal foglalkozó szervezeti egységnek úgy kell nagyobb összegeket kérnie a feladatai ellátására, hogy annak nincs „látható eredménye”, hiszen a be nem következett esemény nehezen értelmezhető nagyobb összegek másik oldalaként.

A védekezésről

A kezelésnél mindig jobb megoldás a megelőzés, így javasoljuk erre helyezni a hangsúlyt, még ha első ránézésre rengeteg idő-, energia- és anyagi ráfordítással is járhat. Fent már láthattuk, hogy milyen veszélyeket és milyen következményeket hordozhat magában egy ilyen zsarolóvírus támadás. Jelen fejezetben a vállalatoknak olyan megelőző védelmi intézkedési javaslatokat fogalmazunk meg, melyek ugyan általános jelleggel, de leírják azon teendőket, melyek bevezetése esetén a sikeres támadások esélye a minimumra csökkenthető. A lenti ajánlások mind adminisztratív, mind logikai és fizikai kontrollokként értelmezendők, tehát a szervezetnek nem elég egyes szervezési szabályok kialakítása, azok kikényszerítése is szükséges.

- Az üzleti folyamatok felmérése (Business Impact Analysis - BIA), valamint erre épülően egy üzletmenet-folytonossági tervezés (Business Continuity Plan - BCP) kialakítása;
- A fentiekhez kapcsolódóan egy katasztrófahelyreállítási terv (Disaster Recovery Plan – DRP) kialakítása;
- A fenti terveket megfelelő időközönként élesben is tesztelni szükséges;
- Megfelelő jogosultságmenedzsment keretrendszer kialakítása és fenntartása, mely magában foglalja a szerepkörök és felelősségek szétválasztását (Segregation of Duties – SoD), valamint a legkisebb jogosultság elve (Least Privilage) mentén kiosztott jogosultságok alkalmazását;
- A jogosultságok feladatok mentén történő szétválasztását, így a privilegizált fiókok mellett felhasználói fiókok megléte az üzemeltetést végzők esetén. A privilegizált fiók kizárólag az informatikai üzemeltetési feladatok ellátásának idejéig használható.
- Jogosultságok folyamatos felülvizsgálata, a szükségtelen jogosultságok azonnali visszavonása;
- A lehető legcsekélyebb mennyiségű és mértékű írási jogosultsággal rendelkező szereplőt engedélyezzünk ott, ahol ez nem szükséges;
- A privilegizált felhasználók számát és jogosultságait minimalizálni szükséges;
- Fejlesztési és tesztelési környezet szétválasztása az éles környezettől;
- Rendszeres, dokumentált és példákkal, gyakorlatokkal kiegészített tudatosítási tevékenység, mely magában foglalja nemcsak a felhasználói, de a rendszergardai, valamint a szervezet vezetői munkakörében foglalkoztatott személyeket is;
- Az internet felől nyitott portok szükségességét rendszeresen, tervezetten vizsgáljuk felül, a szükségtelen portokat tegyük elérhetetlenné, a szükségeseket pedig vessük fokozott felügyelet alá, naplózzuk és változtassuk meg az alapértelmezett portszámokat;
- Tiltsuk az üzemeltetéshez használt portok (SSH, RDP, Telnet, LDAP, NTP, SMB, stb.) külső hálózatból történő elérését, az üzemeltetési feladatok ellátásához javasolt a rendszerek VPN kapcsolaton keresztül történő távoli elérése;

- Korlátozzuk a gyakori portok elérését az internet irányából (megadott IP címekről, csak bizonyos felhasználók számára);
- Az ismert zsarolóvírus források (weboldalak, IOC-k) letiltása tűzfal szinten;
- Többtényezős hitelesítési megoldás alkalmazása minden rendszerfunkció esetén (felhasználó és privilegizált felhasználó esetén is);
- Incidensbejelentő platform (ticketing rendszer, vagy más megoldás) fenntartása, valamint a felhasználók bejelentési kedvének növelése;
- Kommunikációs és válságkommunikációs tervek elkészítése és tesztelése azon esetekre, amennyiben mégis megtörténne a támadás;
- Megfelelő mentési eljárásrend kialakítása, tesztelése és szeparált, BCP-ben meghatározott RPO és RTO értékekhez igazodó mentési struktúra felállítása;
- Folyamatos és központi kezelésű frissítések telepítése;
- Folyamatosan frissülő adatbázison alapuló, aktív vírusvédelmi megoldások alkalmazása;
- Email szűrési beállítások alkalmazása.

A korábbiakban ismertetésre került, hogy a sikeres támadások legnagyobb része még mindig emailben (phishing) kerül be a rendszerekbe, mely feltételezi, hogy legalább egy felhasználó a kártékony kódot tartalmazó fájlra, vagy linkre kattintott. Ezért a tudatosítás fontosságát hangsúlyozandó jelen fejezetben külön kitérünk ezen feladatok részletezésére.

A kiberbiztonsági tudatosítást az alábbiak szerint kell azt felépíteni:

- Megfelelően tervezett, éves képzési terv mentén kerüljön kialakításra;
- Mérhető legyen (be- és kimeneti értékek);
- Kellően gyakori kell, hogy legyen (belépéskor minden felhasználónak, valamint legalább évente egy alkalommal);
- Gyakorlatias felépítésű, példákkal, élethelyzetekkel, melyekkel a munkavállalók, privilegizált felhasználók és vezetők is azonosulni tudnak;
- Ismertesse a szabályozáson túl azok megszegésének következményeit;
- Ismertesse a fenyegetettségek működésének alapvető jellegzetességeit, valamint azok következményeit.

A kiberbiztonsági tudatosításnak (jelen esetben) az alábbiakra kell kiterjednie:

- Ne kattintson rosszindulatú linkekre;
- Ne töltsön le nem megbízható, rosszindulatú csatolmányt;
- Ne telepítsen ismeretlen forrásból származó programokat;
- Soha ne csatlakoztassanak ismeretlen USB-t a számítógépükhöz;
- Használjon VPN-t ha nem megbízható vagy nyilvános Wi-Fi-n keresztül csatlakozik;

- Folyamatosan frissítsen (operációs rendszer és szoftver/firmware szinten);
- Csatolmányok sandbox ellenőrzése;

A támadás esetén alkalmazandó eljárásokról

Fent láthattuk, hogy hogyan készüljünk fel a támadásokra, most nézzük m a teendő, ha a legnagyobb igyekezetünk ellenére mégis megtörtént a baj, és zsarolóvírus támadás áldozatai lettünk.

1. **A fertőzés izolálása**: A fertőzés terjedésének megakadályozása érdekében minél előbb különítsük el fertőzött végpontot a hálózat többi részétől és a megosztott tárolóhelyektől.

   Az első lépés, még akkor is, ha csak gyanítjuk, hogy egy számítógép fertőzött lehet, szigeteljük el azt a hálózat többi végpontjától és tárolóeszközétől. Kapcsoljuk ki a Wi-Fi-t, tiltsuk le a Bluetooth-t, és húzzuk ki a gépet minden olyan LAN-ról és tárolóeszközről, amelyhez csatlakoztatva van. Ez nem csak a terjedést fékezi meg, hanem a zsarolóprogramot is megakadályozza abban, hogy kommunikáljon a támadókkal. A hálózati mentéseket azonnal tiltsuk le, amennyiben a mentések egymást felülíró mentések, így nem készülhet olyan biztonsági mentés, mely már tartalmazza a kártékony kódot.

2. **A fertőzés azonosítása**: A rosszindulatú szoftvereknek számos különböző törzse létezik, és mindegyik más-más válaszlépést igényel. Vizsgáljuk át a számítógépen lévő üzeneteket és fájlokat, vagy futtassunk azonosító eszközöket, hogy pontosabb képet kapjunk arról, mivel állunk szemben.

   Ahogyan vannak rosszfiúk, akik a zsarolóvírusokat terjesztik, úgy vannak jófiúk is, akik segítenek harcolni ellenük. Az olyan oldalak, mint az ID Ransomware és a No More Ransom! Project segít a Crypto Sheriffnek azonosítani, hogy melyik törzzsel van dolgunk. Ha pedig tudjuk, hogy milyen típusú zsarolóvírussal fertőződött meg a munkaállomás, vagy a hálózat, az segít megérteni, hogyan terjed, milyen típusú fájlokat céloz meg jellemzően, és milyen lehetőségeink vannak az eltávolításra és fertőtlenítésre, ha vannak egyáltalán.

3. **Az esemény bejelentése**: Függetlenül attól, hogy törvényileg kötelesek vagyunk-e, nem rossz ötlet jelenteni a támadást a hatóságoknak. Ők segíthetnek az intézkedések támogatásában és koordinálásában.

   Természetesen sok esetben a vállalatok inkább „csendben” szeretnék intézni az ilyen „kellemetlen” helyzeteket, hiszen hatalmas reputációs veszteséggel járhat egy-egy ilyen támadás. A kifizetések alapvetően nagyon csekély százalékban járnak az adatok visszanyerésével, ezért nem is ajánljuk a fizetést. A támadás bejelentésével egyébként többeket megóvhatunk attól, hogy áldozattá váljanak. Minden egyes bejelentett támadással a hatóságok tisztább képet kapnak arról, hogy kik állnak a támadások mögött, hogyan férnek hozzá a rendszeréhez, és mit lehet tenni a támadások megállítása érdekében.

Itt szükséges megemlíteni még a bizonyítékok összegyűjtésének fontosságát, akár hatósági, akár más eljárás esetére. A bizonyítékokat csak akkor gyűjtsük be, ha képesek vagyunk biztosítani a tovább-fertőződés lehetőségének kizárását. Minden esetben kellő szaktudással rendelkező személy jegyzőkönyv felvétele mellett gyűjtse be ezeket.

4. **Határozzuk meg a lehetőségeinket**: A fertőzés kezelésének számos módja van. Határozzuk meg, hogy melyik megközelítés a legjobb a számunkra.

   A jó hír az, hogy vannak lehetőségeink. A rossz hír az, hogy a legkézenfekvőbb lehetőség a fizetés. Azonban ahogy már említettük, ez a lehető legrosszabb ötlet. Egyesek számára vonzónak tűnhet, ha egyszerűen engednek a hackerek követeléseinek, különösen, ha a váltságdíj kifizetése kevésbé költséges, mint a termelékenység esetleges elvesztése. A váltságdíj kifizetése azonban csak arra ösztönzi a támadókat, hogy más, hasonló vállalkozásokra vagy magánszemélyekre is lecsapjanak. A váltságdíj kifizetése csak a bűnös környezetet erősíti és lehet, hogy még az adatainkat sem kapjuk vissza.

5. **Helyreállítás és frissítés**: Használjunk biztonságos biztonsági mentéseket, valamint program- és szoftverforrásokat (korábbi konfigurációs mentéseket) a számítógép visszaállításához vagy egy új platform felszereléséhez.

   Számos webhely és szoftvercsomag létezik, amelyek potenciálisan eltávolíthatják a zsarolóvírust a rendszerből, köztük a legismertebb a No More Ransom! Project, de vannak más lehetőségek is.

   Teljes törlés

   A legbiztosabb módja a rosszindulatú vagy zsarolóprogramok eltávolításának a rendszerből az, ha az összes tárolóeszköz teljes törlését elvégezzük, és mindent újra telepítünk a nulláról. A rendszer merevlemezeinek formázása biztosítja, hogy a rosszindulatú szoftverek maradványai ne maradjanak meg. Ha megfelelő biztonsági mentési stratégiát követtünk, akkor a fertőzés időpontjáig minden dokumentumról, médiáról és fontos fájlról rendelkeznünk kell másolattal. Itt fontos pontosan meghatározni a fertőzés időpontját, mivel a frissen telepített rendszerek újra fertőződéséhez vezethet, ha olyan biztonsági mentést töltünk vissza, mely már tartalmazta a fertőzést, ami addig nem volt aktív.

   Rendszervisszaállítás

   Bár csábító lehet egy egyszerű rendszervisszaállítás, azonban a kártékony kódok a rendszerben bárhol megbújhatnak, így egy visszatöltés esetén azok újra a rendszerbe kerülhetnek.

   Biztonsági mentések érintettsége

   További probléma, hogy a zsarolóvírusok titkosíthatják a helyi biztonsági mentéseket. Ha olyan számítógéphez csatlakozik, amely zsarolóprogrammal fertőzött, akkor jó eséllyel a helyi biztonsági mentés adatai is titkosítva lesznek minden mással együtt. Ezért érdemes felhőbe, vagy külső, szeparált helyre menteni.

6. **Tervezzük meg hogyan tudnánk megelőzni az ismételt bekövetkezést** (tanuljunk a történtekből): Végezzünk felmérést arról, hogyan következett be a fertőzés, és milyen intézkedéseket tudunk végrehajtani annak érdekében, hogy ez ne fordulhasson elő újra.

   Az ilyen jellegű támadások tökéletes „éles tesztjei" a BCP-nknek, illetve egyéb más adminisztratív és szervezési szabályozónknak. Amennyiben a BCP-ben és a mentési eljárásrendben, valamint az incidenskezelési eljárásrendben foglaltak helyesen kerültek implementálására, úgy egy ilyen támadás esetén a szervezet által tett intézkedések maximálisan segítik a szervezetet a támadás felszámolásában. Azonban ezek a szabályozók – korábbi tapasztalások hiányában – ritkán sikerülnek „elsőre tökéletesre". Így egy-egy ilyen támadásból rengeteget tanulhatunk, például, hogy milyen hiányosságok tapasztalhatók a mentési eljárásrendünkben, amennyiben a nem sikerült, vagy csak nagyon régi mentést sikerült visszatöltenünk, vagy a BCP-nk, amennyiben a helyettesítő eljárásaink nem voltak alkalmasak az adott üzleti folyamataink kiváltására. Végül a gyökérokok feltárása során amennyiben arra jutunk, hogy emberi tényező okozta a fertőzés rendszerekbe jutását, úgy a tudatosítási tevékenység megismétlését, eltérő fókuszokkal.

2023. január 21.

dr. Faragó Tamás

IT Security Auditor

Black Cell Magyarország Kft.