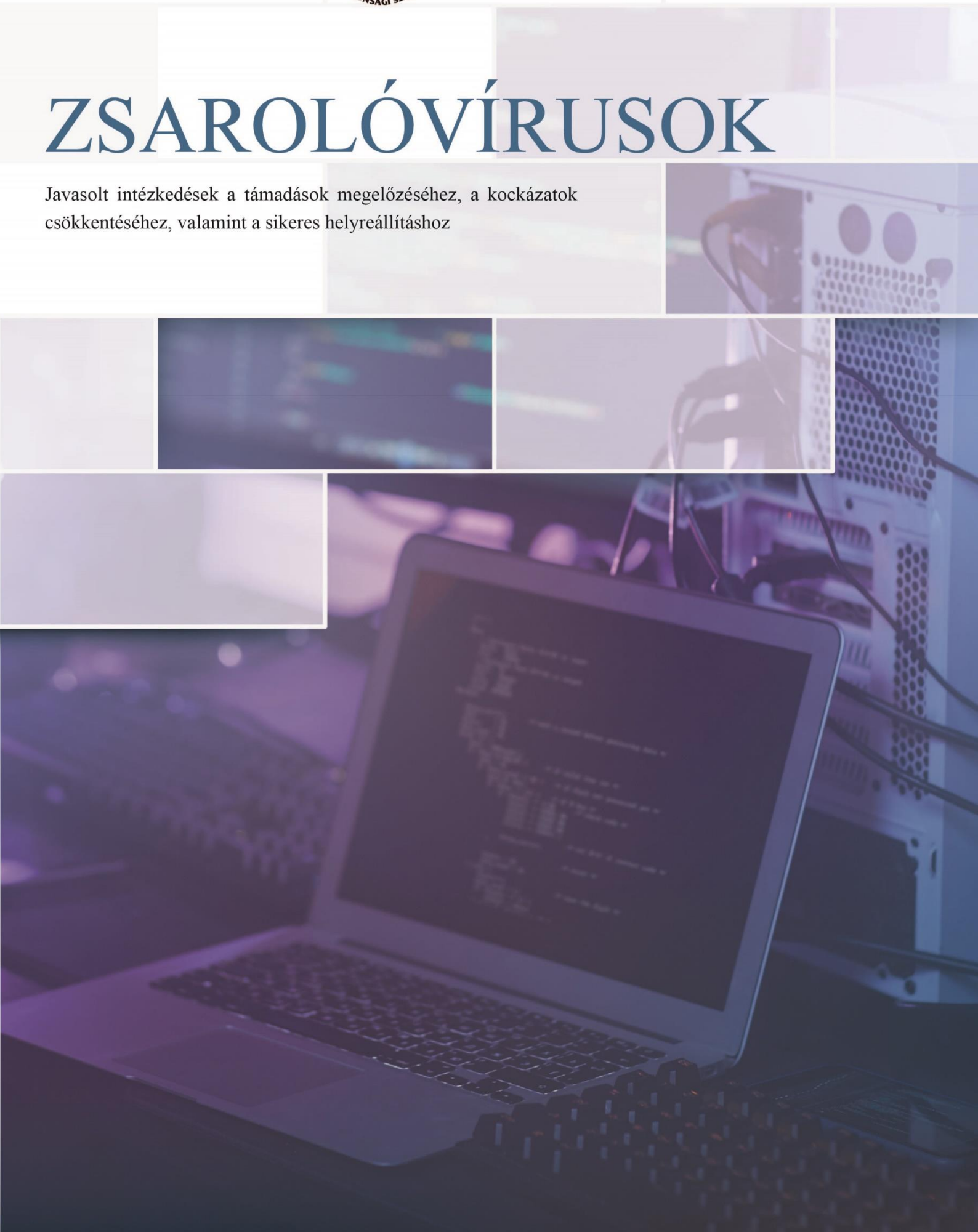
NEMZETI KIBERVÉDELMI INTÉZET

ZSAROLÓVÍRUSOK

Javasolt intézkedések a támadások megelőzéséhez, a kockázatok csökkentéséhez, valamint a sikeres helyreállításhoz



A zsarolóvírus támadások száma az elmúlt években világszerte nőtt, valamint egy új tendencia is kialakult: a támadók célzott támadásokat hajtanak végre olyan szervezetek ellen, amelyek egy magasabb váltságdíj kifizetését is megengedhetik maguknak. A támadások bármilyen szervezetet érinthetnek, amely nem teszi meg időben a szükséges intézkedéseket.

Ez a dokumentum összefoglalja a legfőbb tudnivalókat a zsarolóvírusokkal kapcsolatban, valamint javaslatokat fogalmaz meg a támadások elkerülésére, illetve bekövetkezett támadás esetén az adatok sikeres helyreállítására.

Háttér

A zsarolóvírus támadások bevételi modellje eredetileg a méretgazdaságosságra épült. A bűnözők a sérülékeny rendszereket nagy számban támadták és viszonylag alacsony váltságdíjat kértek az adatok visszaállításáért cserébe. Ezt a váltságdíjat az áldozatok gyakran ki is fizették.

Az elmúlt években azonban új módszer jelent meg: a rosszindulatú támadók több célzott támadást hajtanak végre olyan szervezetek ellen, amelyek képesek akár egy magasabb váltságdíj megfizetésére is. Miután hozzáférést szereznek az adott rendszerhez, hosszú időn keresztül elemzik annak működését, ennek eredményeként fel tudják mérni a szervezet „értékét” és egy olyan váltságdíjat állapítanak meg, amely arányban van ezzel.

Célcsoport

Informatikai vezetők, Információbiztonsági vezetők, valamint információbiztonsági szakemberek

Együttműködő partnerek

Szerzői jog

Szervezet	Szerzői jog
CERT-BE	Ez a kiadvány a CERT-BE publikációján alapul: Zsarolóvírus, hogyan védekezzünk és reagáljunk (Ransomware, how to protect and respond). A publikációból származó információk a CERT-BE előzetes hozzájárulásával kerültek felhasználásra.
NCSC-UK	Ez a kiadvány a NCSC-UK publikációján alapul: A malware és a Ransomware támadások megelőzése (Mitigating Malware and Ransomware attacks). A kiadványból származó információk a nyílt kormányzati licenc hatálya alá tartoznak.
NCSC-NL	Ez a kiadvány a NCSC-NL publikációján alapul: Zsarolóvírus, intézkedések a támadás megelőzéséhez, a kockázatok csökkentéséhez, valamint a sikeres helyreállításhoz (Ransomware Measures for preventing, limiting and recovering from a ransomware attack). A kiadványból származó információk a CC0 (Creative Commons Zero) licenc hatálya alá tartoznak.

Tények

1. A zsarolóvírus támadások hatása folyamatosan növekszik.
2. A zsarolóvírus támadás ellen tett intézkedések segítséget nyújtanak más rosszindulatú programok ellen is.
3. A zsarolóvírus támadások bevételi modellje megváltozott. A rosszindulatú támadók több célzott támadást hajtanak végre, olyan szervezetek ellen, amelyek képesek akár egy magasabb váltságdíj megfizetésére is.

Mi a zsarolóvírus?

A **zsarolóvírus**[i] olyan rosszindulatú program, amely a felhasználók adatait azzal a céllal titkosítja, hogy később csak a váltságdíj ellenében lehessen visszaállítani azokat.

Az ilyen típusú károkozó néhány főbb jellemzője, hogy:

- titkosítja az állományokat,
- zsaroló üzenetet jelenít meg,
- határidőt szab a váltságdíj kifizetésére,
- törli az állományok egy részét,
- az idő múlásával egyre több állományt tesz végleg visszaállíthatatlanná.

Szélsőséges esetekben a megfelelő működéshez nélkülözhetetlen rendszerfájlok titkosítása révén az informatikai rendszerhez való hozzáférést is blokkolja. Tekintettel a vírus pusztító jellegére, gyakran nehéz helyreállítani a naplófájlokat, és megtudni, hogy valójában mi történt. A hackerek szellemi tulajdon, valamint személyes adatok ellopása esetén is használhatnak zsarolóvírust, hogy valódi szándékaik rejtve maradjanak.

Kétféle zsarolóvírus létezik: Az egyik a számítógépet zárja le és megakadályozza az ahhoz való hozzáférést, a másik pedig a fertőzött rendszeren lévő állományokat titkosítja. A zsarolóvírusok fejlettebb változatai nem csak a helyi IT rendszereket képesek titkosítani, hanem a merevlemezeket, adatbázisokat, USB adathordozókat és a felhőben lévő adatokat is. Az áldozatnak mindkét típusú zsarolóvírus esetében váltságdíjat kell fizetnie, hogy ismét normálisan használhassa a számítógépét. A támadók ezt a váltságdíjat gyakran kriptovaluta formájában (például Bitcon) követelik.

A zsarolóvírus fertőzések alig különböznek a többi rosszindulatú program fertőzésétől. Ezen felül az intézkedések is, amelyeket egy szervezet megtehet a zsarolóvírusok ellen, nagyjából ugyanazok. A szervezet fejlettségétől függően a zsarolóvírus támadás hatása nagy skálán mozoghat az egyszerű bosszankodástól egészen a szervezet folyamatainak leállásáig.

Mekkora a váltságdíj?

Nagy különbség van az általános és a célzott támadás között. Általános támadás estén jelentős számú áldozatot fertőznek meg és néhány száz vagy ezer euro-t kérnek váltságdíjként. Az összeget szándékosan tartják alacsony szinten, annak biztosítása érdekében, hogy az áldozat számára az legyen a leggyorsabb és legolcsóbb helyreállítási mód.

Célzott, gondosan előkészített támadás esetén a váltságdíj az egymillió euro-t is elérheti. A rosszindulatú támadók ilyenkor a legnagyobb hatást akarják elérni. Egy ilyen támadásnak jelentős következményei lehetnek, például kritikus adatok és folyamatok válnak elérhetetlenné. A fenyegetés szólhat az adatok törléséről és nyilvánosságra hozataláról is, ezek a támadások egyre gyakoribbá válnak.

Azok a támadók, akik az érzékeny információk megszerzésére törekednek, gyakran használják a zsarolóvírust, hogy elfedjék valódi tevékenységüket. Ebben az esetben a zsarolóvírust, mint egy törlő eszközt használják, ami azt jelenti, hogy a

merevlemezen lévő adatok soha sem állíthatók vissza.

Az NBSZ-NKI nem javasolja a váltságdíj megfizetését. Nincs semmilyen garancia rá, hogy a kért váltságdíj megfizetése után megkapja a dekódoló kulcsot vagy jelszót. Ráadásul előfordul, hogy fizetés után az áldozat újból a támadók célpontjává válik.

Hogyan fertőzi meg a zsarolóvírus a rendszerét?

A támadók **sokféle módon fertőzhetik meg rendszerét**[ii] zsarolóvírussal, amely egyfajta káros program. Elég, ha megnyit egy e-mailben érkező káros mellékletet, vagy meglátogat egy rosszindulatú weboldalt. Sok áldozat telepíti a zsarolóvírust anélkül, hogy észrevenné azt.

A zsarolóvírus támadások a rendszer sérülékenységeit is kihasználják. Ilyenek például a sebezhető böngészők és a régi protokollok, mint például SMBv1, illetve az **RDP**[iii] hozzáférés. Más rosszindulatú programok, mint például a trójaiak is felhasználhatók a rendszerhez való hozzáférés érdekében.

Zsarolóvírus, mint szolgáltatás (Ransomware-as-a-Service)

A számítógépes bűnözést az egyre fokozódó profizmus és specializálódás jellemzi. A számítógépes bűnözők egyes csoportjai a hálózatokhoz való hozzáférés megszerzésére és eladására szakosodtak.

Más csoportok ezeket a hozzáféréseket használják ki, például zsarolóvírus segítségével. Különféle módszereket fejlesztenek ki, hogy azonosítsák a sérülékeny RDP portokat és visszaéljenek azokkal, például ellophatják a hitelesítő adatokat és más érzékeny információkat. Az RDP hozzáférés számos előnnyel jár: a meglévő hitelesítési adatok segítségével a támadók könnyebben leplezhetik tevékenységüket és az beleolvadhat a „normál” hálózati használatba. Mivel csak kevés vagy egyáltalán nem látható rosszindulatú hálózati forgalom van, a támadót nem feltétlenül veszi észre a rendszerfigyelés vagy egy éber rendszergazda.

A zsarolóvírus, mint szolgáltatás növekvő profizmusa ellenére az általános és a célzott támadás is speciális ismereteket igényel.

Megelőzés

1. Óvakodjon az adathalászattól!
2. Szervezze meg a sebezhetőség és frissítés kezelést, valamint a hálózati szegmentációt!
3. Korlátozza a kódfuttatás lehetőségét!
4. Szűrje a böngésző forgalmát!
5. Korlátozza az USB használatát!

A zsarolóvírusok ellen nincs csodaszer. A zsarolóvírus csupán a rosszindulatú programok sok változatának egyike. Ennek eredményeként a zsarolóvírus elleni intézkedések nagyrészt megfelelnek azoknak az intézkedéseknek, amelyek megvédik a rendszert más típusú rosszindulatú programokkal szemben.

A zsarolóvírusok célja gyakran a pénzügyi haszon. Ezért tanácsos a hálózatot mélyreható védelmi rendszerrel ellátni, így a támadóknak nagyobb erőfeszítéseket kell tenniük a sikeres támadás végrehajtása érdekében. A bűnözők felbecsülik a lehetséges nyereséget, és feladják, ha a támadás túl sok időt vesz igénybe a várható váltságdíjhoz képest.

1. Óvakodjon az adathalászattól

Az **adathalászat**[iv] a pszichológiai manipuláció egyik formája, amelyben az embereket arra veszik rá, hogy érzékeny adatokat adjanak át. A leggyakoribb adathalász módszer olyan hamis e-mailek küldése, amelyek úgy tűnnek, mintha megbízható feladótól érkeznének. Ezek az e-mailek gyakran tartalmaznak egy hamis

weboldalra mutató hivatkozást, amely személyes adatok megadását kéri, vagy meglátogatása fertőzött fájl letöltésével jár.

Az adathalászat elleni küzdelem mind technikai, mind emberorientált megközelítést igényel. Egyrészt képezheti alkalmazottait az adathalász üzenetek felismerésére, másrészt technikai megoldásokat is használhat.

Az NBSZ-NKI az alábbi alapvető intézkedések megtételét javasolja:

- javítsa az e-mail biztonságot az SPF, DKIM és DMARC használatával, valamint ellenőrizze a bejövő levelek forgalmát ezekkel a szabványokkal. Ez az intézkedés megakadályozza, hogy mások e-maileket küldjenek a szervezet nevében.

- Használjon spam szűrőket

- Rendszeresen végezzen adathalász-teszteket. Tanítsa meg munkatársainak a spam és adathalász e-mailek felismerését. A kellemetlenségek elkerülése érdekében ezeket a teszteket megfelelően koordinálja a szervezeten belül.

- Hozzon létre egy olyan folyamatot, amely lehetővé teszi a felhasználók számára az adathalász levelek jelentését és képezze ki alkalmazottait az ezzel összefüggő kapcsolattartásra. Gyakran küldik ki ugyanazt az adathalász levelet, csupán a bennük lévő hivatkozás változik.

- Növelje alkalmazottainak tudatosságát és alkalmazzon pozitív biztonsági kultúrát. Győződjön meg róla, hogy alkalmazottai tudják, hol kell bejelenteni az adathalászatot, és hogy megteszik-e azt még akkor is, ha már rákattintottak a rosszindulatú hivatkozásra.

- A levelező szoftverek gyakran tartalmaznak vizuális eszközöket, amelyek figyelmeztetik a felhasználókat a rosszindulatú e-mailekre. Ezek az eszközök lehetővé teszik a külső e-mailek címkézését is.

2. Szervezze meg a sebezhetőség és frissítés kezelést, valamint a hálózati szegmentációt.

A zsarolóvírusok egyes verziói kihasználják az operációs rendszerek, webböngészők, böngésző pluginek és alkalmazások sebezhetőségeit. Ezeknek a sebezhetőségeknek egy része nyilvánosan elérhető, és rendelkezésre állnak azok a javítások, amelyek csökkenthetik a fertőzés kockázatát.

Frissítések

A rendszerfrissítések végrehajtása jelentősen megnehezíti az újonnan felfedezett sérülékenységek kihasználását. A legtöbb szoftver automatikusan frissül. A frissítések javításokat is tartalmazhatnak, amelyekkel a szoftver jobb védelmet biztosít az új támadásokkal szemben.

Fontos a hálózaton lévő összes rendszer megfelelő időben történő javítása, nem csupán azoké, amelyek közvetlenül kapcsolódnak az internethez. A támadó oldalágon mozoghat a hálózatán, különösen egy célzott támadás esetén. Az összes rendszer időben történő frissítése megnehezíti a támadó számára a továbbjutást. Az **NBSZ-NKI** az alábbi intézkedések megtételét javasolja.

- Kövesse figyelemmel a használt szoftverek frissítéseit, valamint az azokat érintő sérülékenységeket.

- Frissítse operációs rendszerét a legújabb verzióra.

- Állítson be automatikus frissítést.

- Győződjön meg arról, hogy a víruskereső szoftver naprakész és minden releváns szolgáltatás engedélyezve van.

Hálózatfigyelés

A sikeres zsarolóvírus támadás alapja az időzítés: a támadók megpróbálnak minél tovább észrevétlenek maradni. Ezért a zsarolóvírus támadás megelőzése (a fertőződés esélyének csökkentése) érdekében fontos, hogy ezek a tevékenységek minél gyorsabban azonosításra kerüljenek. Az **NBSZ-NKI** az alábbi intézkedések megtételét javasolja:

- Vegye leltárba eszközeit és vezessen róluk naprakész nyilvántartást; egyértelműnek kell lennie, hogy mi található a hálózaton. Zsarolóvírus támadás esetén képesnek kell lennie nyomon követni, hogy kihez tartozik az érintett rendszer és hol helyezkedik el a hálózaton.

- Ismerje meg a hálózat alapvető működését, használjon segédprogramokat, hogy tudja milyen a normális működés a hálózatán.

- Állítson be észlelést a digitális támadások, illetve a rosszindulatú fenyegetések beazonosítása érdekében. Az észlelés nagy szereppel bír a támadás gyors azonosításában és megállításában.

- Kísérje figyelemmel, hogy a hitelesítő adatok nem sérültek-e.

- Ügyeljen rá, hogy a naplózás egy központi helyen történjen.

- A naplózás mellett a monitorozás is egy jó ötlet, határozza meg, mely naplóbejegyzések generáljanak riasztást és készítsen rá egy folyamatot.

- Fejleszteni kell a biztonsági események láthatóságát. Fedezze fel a biztonsági információs és eseménykezelő (SIEM) rendszerben lévő lehetőségeket.

- Fedezze fel az EDR rendszerekben rejlő lehetőségeket. Ez a szoftver lehetővé teszi a rendszerben lévő végpontok (többnyire PC-k) folyamatos monitorozását. Ezáltal képes lesz valós időben reagálni egy támadásra.

Hálózati szegmentáció

A hálózati szegmentálás további biztonsági réteget biztosít. Ez nagyon fontos a hálózaton történő oldalirányú mozgás megakadályozása érdekében. Az oldalirányú mozgás azt jelenti, hogy a támadó mélyebb és szélesebb körű hozzáférést nyer a hálózathoz. A hálózat funkcionális szegmensekre osztása megnehezíti a támadó munkáját. Végül is a hálózat azon részét, ahová a támadó belépett, teljes mértékben elzárhatjuk. Az **NBSZ-NKI** az alábbi intézkedések megtételét javasolja:

- Korlátozza a rendszerekhez való külső hozzáférést arra, ami feltétlenül szükséges.

- Gondoskodjon róla, hogy az alkalmazottak csak VPN-kapcsolaton keresztül férjenek hozzá a belső hálózathoz.

- Szegmentálja hálózatát. Azokat a rendszereket, amelyek nem igényelnek interakciót vagy kommunikációt, különféle szegmensekre kell felosztani. A felhasználók csak a szükséges szegmensekhez férjenek hozzá. Blokkolja a szegmensek közötti forgalmat. Ez az intézkedés magába foglalja a **zéró bizalom elvét**; azaz csak a kifejezetten megbízható forgalmat szabad engedélyezni.

- Korlátozza az adminisztrátori jogosultságokat és ezek megosztását.

- Győződjön meg arról, hogy a támadók nem tudnak kívülről bejelentkezni a rendszerbe. Használjon hosszú, összetett jelszavakat és vezesse be a fiók zárolási irányelvet a brute-force támadások ellen. használjon többfaktoros azonosítást (MFA) a felhasználók hitelesítésére.

Felügyeleti interfészek megerősítése

Az olyan felügyeleti interfész, mint a Remote Desktop Protocol (RDP) lehetővé teszi a rendszerek távoli elérését és működtetését. Ennek vannak funkcionális

előnyei; például egy alkalmazottnak nem kell fizikailag jelen lennie. Azonban ez az interneten keresztüli közvetlen hozzáférés a menedzsment interfészeket a támadók népszerű célpontjává is teszi. Többek között a *SamSam* zsarolóvírus is támadja ezeket, amely megpróbálja kihasználni az interneten hozzáférhető RDP szerverek gyenge jelszavait.

A hálózati hozzáférés korlátozását más néven rendszer megerősítésnek nevezik. Habár a víruskeresők és a tűzfalak segítik a biztonságot, a hozzáférés korlátozására is célszerű figyelmet fordítani. Nagyon fontos, hogy csak a nélkülözhetetlen hálózati interfészek legyenek elérhetőek, ami mellett meg kell szigorítani a termeléssel összefüggő adatok és környezet eléréséhez szükséges jogosultságokat.

- Ellenőrizze az RDP szükségességét. Amennyiben szükséges, úgy korlátozza annak elérését a megbízható gépekre (whitelist).

- Az RDP hozzáférést és az egyéb kapcsolatokat védje a brute-force támadások ellen. Bizonyosodjon meg róla, hogy a felhasználók csak VPN-en keresztül és többfaktoros azonosítás segítségével érhetik el a rendszert.

- Ellenőrizze, hogy a felhő alapú munkakörnyezetben a beállítások megfelelnek-e a legújabb ajánlásoknak. Az RDP portok hozzáférését szintén célszerű korlátozni.

- Védje megfelelően az RDP használatát.

Felhívjuk figyelmét, hogy az információbiztonság szempontjából kiemelten fontos, hogy az Ön szervezetének saját kockázatelemzését elvégezze. A fenti lista nem teljeskörű, és nem biztos azok közül minden intézkedés megfelel az összes szervezetnek.

3. Kódfuttatási lehetőségek korlátozása

Fontos a szervezet jogosulatlan kódfuttatással szembeni védelme. A jogosulatlan kódfuttatás általában valamilyen malware tevékenységgel függ össze. A makrók használata általános módszer támadások során, a támadók gyakran próbálják rávenni a felhasználót a makrók használatának engedélyezésére a káros kódot tartalmazó csatolmányok megnyitása esetén. Ha a szervezeten belül letiltásra kerülnek a makrók, ezzel ez a fajta támadás máris megelőzhetővé válik.

Biztonsági szempontból nem ajánlott a szoftvertelepítési jogosultság engedélyezése valamennyi felhasználó számára. Természetesen előfordulhat olyan helyzet, amikor erre szükség van. Célszerű létrehozni egy belső folyamatot, amelyen keresztül ez a lehetőség elérhetővé válik a felhasználók számára, így biztosítható, hogy nem kísérlik meg megkerülni a korlátozást. Az **NBSZ-NKI** az alábbi intézkedések megtételét javasolja.

- „Whitelist” készítése az engedélyezett programok futtatásához

- Makrók tiltása Office fájlokban

- ActiveX tiltása Office fájlokban

- Automatikus lejátszás tiltása

4. Internetes forgalom szűrése

A kifelé irányuló internetes forgalom lebonyolításához célszerű proxy-t használni. Ezzel szűrhetővé válnak a felkereshető webhelyek, pl.: blokkolhatók az ismert káros weboldalak.

5. USB eszközök korlátozása

Külső adathordozókon keresztül (pl.: USB flash memória) a rendszer könnyen malware fertőzés áldozatává válhat. Éppen ezért javasolt az USB portok lezárása, USB eszközök blokkolása. Az USB eszközök használatát korlátozottan lehet

engedélyezni egyes felhasználók számára, a szervezet igényei szerint.

Milyen hatása van a zsarolóvírus támadásnak?

A zsarolóvírus korlátozza az adatokhoz, illetve a rendszerhez való hozzáférést a titkosítás feloldásáig. Ez súlyos károkat okozhat, pl.: pénzügyi veszteség, jó hírnév elvesztése. A zsarolóvírus nem csak az adott szervezetet érinti, hanem annak teljes környezetét is. Még gondosan konfigurált biztonsági mentésekkel is időbe telik, mire a szervezet működése helyreáll. A leállás idejére szükségessé válhat a folytonossági folyamatok aktiválása.

Célzott támadás esetén az elkövetők hozzáférést szereznek a célpont informatikai rendszeréhez. Ez veszélyezteti az adatok integritását és bizalmasságát. Ebben az esetben az informatikai rendszer további malware-ekkel is megfertőződhet.

A sikeres zsarolóvírus támadás nemcsak a titkosított adatokat érinti, közvetett vagy végleges károk is keletkezhetnek.

A zsarolóvírus támadás következményeinek csökkentése

1. Az adatokhoz és filerendszerhez való hozzáférés korlátozása
2. Helyreállítási stratégia kidolgozása

1. Az adatokhoz és fájlrendszerhez való hozzáférés korlátozása:

A zsarolóvírus szabad terjedése megakadályozható, amennyiben korlátozzuk az egyes felhasználók adatokhoz és fájlrendszerhez való hozzáférését. Mindenki csak a számára feltétlenül szükséges eléréssel rendelkezzen. Ez a megoldás előnyös lehet a biztonsági mentések és a felhő alapú adattárolás szempontjából is.

Nagyon fontos egy jó hozzáférés menedzsment alkalmazása és a hozzáférési jogosultsági szabályok szigorú betartása. Ehhez elengedhetetlen a pontos adminisztráció. Folyamatosan nyomon kell követni a szervezeten belüli változásokat, pl.: felhasználó érkezése, áthelyezése vagy távozása a szervezettől. Minden ilyen változás együtt jár az adott felhasználói jogosultságok változtatásával is.

A hozzáférés ellenőrzés még fontosabb a rendszergazdai fiókok esetében, ugyanis ezek a fiókok kiterjesztett hozzáféréssel és jogosultsággal rendelkeznek. Rendszergazdai jogosultsággal rendelkező felhasználói fiókról nem célszerű internetezni, e-mailt küldeni, vagy bejelentkezni valamely munkahelyi rendszerre. Ez az intézkedés a rendszer bizonyos területeire korlátozhatja a zsarolóvírus támadást.

A zéró bizalom elve egyre népszerűbb. Ez az informatikai biztonsági keretrendszer útmutatásként szolgálhat a **BYOD**[v] (Bring Your Own Device) házirendet használó szervezetek számára. A kockázatok csökkentése érdekében ilyen esetben javasolt a mikro-szegmentálás vagy egy PAM (Privileged Access Management) megoldás használata. A mikro-szegmentálás a gyakorlatban a 'whitelisting' módszer alkalmazását jelenti. A felügyeleti rendszer alkalmazása kiterjedhet a hálózat egyes részeire, vagy egészére is. A PAM (privilegizált hozzáférés kezelés) magába foglalja az adminisztrátori, valamint a kiemelt felhasználói tevékenységek figyelését és naplózását. Az egyes engedélyek csak korlátozott ideig érvényesek, a felhasználó csak ebben az időtartamban jogosult az adott feladat elvégzésére. Ez a megoldás kiegészíthet egy, már meglévő IAM (Identity Access Management) rendszert.

2. Helyreállítási stratégia kidolgozása:

A biztonsági mentések nélkülözhetetlenek egy zsarolóvírus támadás utáni

helyreállításhoz. A működés szempontjából nélkülözhetetlen fájlokról és rendszerekről készített mentés korlátozza a zsarolóvírus hatását.

- Adatok csak az utolsó mentés idejéig állíthatók vissza.
- Az online mentések szintén fertőzöttek lehetnek (az online mentés azt jelenti, hogy a biztonsági mentés közvetlenül csatlakozik a hálózathoz, ellentétben az offline mentésekkel. Offline mentésre példa egy fizikailag leválasztott merevlemez, vagy mágneses kazetta).
- A biztonsági mentések nem lehetnek elérhetőek olyan helyről, amely megfertőződhet.
- A biztonsági mentések integritását és sérülésmentességét rendszeresen ellenőrizni kell.

Meg kell győződni róla, hogy a biztonsági mentéseken kívül egyéb védelmi intézkedések is rendelkezésre állnak, ugyanis elsősorban a megfelelő kiberbiztonsági szabályok alkalmazása védheti meg a szervezetet a támadástól.

Amennyiben a biztonsági mentés tartalmáról kell döntést hozni, szükséges a szervezet számára kritikus adatok felmérése, ideértve azon funkciókat is, amelyeknek a helyreállítás után minél hamarabb (órákon vagy napokon belül) működniük kell.

- Alkalmazza a 3-2-1 elvet, azaz minden adatról készüljön legalább három különböző mentés, legalább két külön adathordozóra. Ezek közül egy legyen fizikailag elkülönítve (offline mentés).
- Korlátozza a biztonsági mentéshez való hozzáférést.
- A biztonsági mentés részét kell képeznie a rendszer naplófájljainak is.

Fontos ellenőrizni, hogy mennyi ideig tart a biztonsági mentésből történő helyreállítás. Ez különösen fontos az üzleti folytonosság biztosításához, hiszen jelentős különbség adódik, ha egy helyreállítás napok helyett hetekig tart. Célszerű meghatározni egy helyreállítási időtartamot és ehhez igazítani a biztonsági mentés stratégiáját.

Kockázatos, ha a biztonsági mentés ugyanazon a platformon fut, mint a működő hálózat. Megfontolandó, hogy a biztonsági mentés saját környezetben fusson. Javasolt teljes más technológia használata, pl.: Windows rendszer esetén a biztonsági mentés Linux alapú környezetben való futtatása.

Mi a teendő, ha bekövetkezik a fertőzés?

A zsarolóvírus által titkosított adatok helyreállítására a legmegbízhatóbb megoldás a biztonsági mentésből történő visszaállítás.

Amennyiben erre nincs lehetőség, célszerű ellenőrizni, hogy létezik-e dekódoló a fertőzésre, pl.: **'No More Ransom' projekt**[vi], amely civil és rendőri erők közös kezdeményezésében működik.

Korlátozott fertőzés esetén:

- Távolítsa el a fertőzött rendszerelemeket a hálózatból.
- Távolítsa el a zsarolóvírust a rendszerből, amennyiben szükséges, telepítse újra az egész rendszert.
- Jelentse az esetet a rendőrség felé.
- Állítsa helyre a rendszert a biztonsági mentésekből.

Egész hálózatra kiterjedő fertőzés esetén:

- Léptesse életbe a vészhelyzetre vonatkozó tervet.
- Szigetelje el a teljes hálózatot a külvilágtól.

- Kérje kiberbiztonsági szakértő segítségét.
- Jelentse az esetet a rendőrség felé.
- Állítsa helyre a rendszert a biztonsági mentésekből.
- Ellenőrizze, hogy van-e bejelentési kötelezettsége a Nemzeti Kibervédelmi Intézet, valamely felügyelő hatóság, ügyfél, illetve más testület felé. ű
- Vegye figyelembe az alkalmazandó adatvédelmi szabályokat is.

Kommunikáció az alkalmazottakkal

Zsarolóvírus támadás esetén sok extra munkára lesz szükség. Sok részlet nem lesz világos, rengeteg kérdés merülhet fel, különösen a felderítés során (Pl.: Milyen mértékű a probléma?). Tanácsos megfontolni a kommunikációt a fertőzés bekövetkezését követően.

Fel kell térképezni az érintettek felé történő kommunikációs formákat, arra az esetre, ha a levelező rendszer is érintett. Egyes szervezetek a közösségi médiát és/vagy egyéb információs pontokat alkalmaznak. Javasolt ezen eljárások rögzítése, illetve rendszeres gyakorlása és értékelése.

Emellett meg kell határozni, hogy ilyen esetekben mely szervezetekkel való együttműködésre van szükség. A leállás alatt ellenőrizze a létfontosságú folyamatokat és dolgozza ki az üzleti folytonossági tervet. Vegye figyelembe, hogy egyes munkavállalókra igen jelentős teher hárulhat, amely akár hetekig is eltart. Fontos a megfelelő pihenőidő biztosítása, így a helyreállítás idejére biztosítható az optimális munkavégzés.

Kell-e fizetni?

A váltságdíj megfizetése nem ajánlott, mivel nem garantálja a probléma megoldását. Nagy a valószínűsége, hogy a dekriptálás során problémák merülnek fel, ugyanis a dekódoló eszköz sokszor kevésbé hatékony, mint a kódolást végző zsarolóvírus. Legrosszabb esetben a helyreállítás nem lesz lehetséges. Ráadásul a váltságdíj megfizetése arra ösztönzi a hackereket, hogy folytassák a tevékenységet, újabb és újabb támadási módokat keresve, ezzel még több kárt okozva a társadalom és a gazdaság számára.

Egyes esetekben előfordult, hogy a támadók újabb követeléssel álltak elő a váltságdíj megfizetése után, illetve ugyanaz a zsarolóvírus újra titkosította az áldozat adatait.

Incidens bejelentése

Bejelentését megteheti a területileg illetékes rendőrkapitányságon, valamint elektronikus formában a Rendőrség weboldalán.

Bejelentés esetén készüljön fel a következő kérdésekre:

- Mely rendszerek érintettek?
- Érintett infrastruktúra és hálózati címek meghatározása?
- Milyen védelmi eszközöket alkalmazott (vírusvédelmi eszközök, tűzfalak)?
- Volt-e tudomása előzetesen fenyegetésről?
- A kár becsült mértéke (gazdasági és reputációs szempontból is), személyes adatok érintettsége?
- Milyen helyreállítási intézkedések történtek?

Összegzés

Amíg a cégek nem fordítanak megfelelő figyelmet az IT biztonságra, addig a különböző malware programok létezni fognak. Az ilyen támadás azon az elven nyugszik, hogy az érintett nincs más lehetősége a fizetésen kívül. A megelőzéssel tehát nem csak a saját szervezetünkön segítünk, hanem

hozzájárulhatunk az ilyen típusú bűncselekmények számának csökkentéséhez is.

Fontos tudni, hogy nem minden zsarolóvírus támadás előzhető meg, ezért kérjük győződjön meg róla, hogy felkészült-e a következmények elhárítására.

Hivatkozások

[i] https://nki.gov.hu/it-biztonsag/tudastar/zsarolovirus-ransomware-v2/
[ii] https://nki.gov.hu/it-biztonsag/kiadvanyok/segedletek/informatikai-behatolasok-es-felismeresuk/
[iii] https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-nyitott-rdp-port-biztonsagi-kockazatai/
[iv] https://nki.gov.hu/it-biztonsag/tudastar/adathalasz-tartalom-phishing-2/
[v] https://nki.gov.hu/it-biztonsag/kiadvanyok/segedletek/mobil-eszkozok-hivatali-hasznalata/
[vi] https://www.nomoreransom.org/

További tájékoztatók

https://nki.gov.hu/it-biztonsag/kiadvanyok/segedletek/nki-tajekoztato-a-zsarolovirusokrol/
https://nki.gov.hu/it-biztonsag/kiadvanyok/segedletek/jelszo-vilagnap-2020/
https://nki.gov.hu/it-biztonsag/kiadvanyok/segedletek/kozigazgatasi-kibervedelmi-eszkoztar/
https://nki.gov.hu/it-biztonsag/kiadvanyok/segedletek/adathalaszat-legjobb-vedekezes-a-megelozes/
https://nki.gov.hu/wp-content/uploads/2019/03/21_Pszichologiai-befolyasolas-vedekezes-a-csalasok-ellen.pdf
https://nki.gov.hu/wp-content/uploads/2019/03/22_Adathalasz-tamadasok.pdf
https://nki.gov.hu/wp-content/uploads/2019/03/17_Biztonsagi-mentesek.pdf
https://nki.gov.hu/wp-content/uploads/2019/03/9_Ceges-es-maganadatok-biztonsaga.pdf

Média

https://nki.gov.hu/it-biztonsag/mediatar/ransomware-kisfilm/