Synology®

Védje szervezetét a zsarolóprogramokkal szemben

A zsarolóvírus-támadások az előrejelzések szerint csak 2023-ban összesen billió dollár veszteséget fognak jelenteni a szervezeteknek.[1] A gyors helyreállítási lehetőségekkel rendelkező adatvédelmi tervek kulcsfontosságúak a zsarolóvírusok és a kiberbűnözés hatásainak mérséklésében.

Date 2023. okt. 13.

Biztonsági másolatok: az utolsó védelmi vonal katasztrófa esetén

Amikor rosszindulatú törlés vagy módosítás következtében elvesznek az adatok, a biztonsági másolatok lehetővé teszik a kulcsfontosságú adatok visszaállítását és a leállási idő csökkentését. Használja ki a Synology adatvédelmi megoldásait a teljes informatikai infrastruktúra biztonsági mentési stratégiájának kialakításához.

Teljes körű védelem

A végpontok, valamint az elsődleges biztonsági másolatok védelmével többszörös biztonsági hálót hozhat létre adatai számára.

Gyors helyreállítás

Az azonnali helyreállítási lehetőségekkel minimálisra csökkentheti az állásidőt katasztrófa esetén.

Megváltoztathatatlan tárolás

Akadályozza meg az adatok és pillanatfelvételek illetéktelen módosítását.

Licencet nem igénylő biztonsági mentések

Korlátozások és rejtett díjak nélkül annyi adatról készíthet biztonsági másolatot, amennyit a tárhelye lehetővé tesz.

Központi védelem a zsarolóvírusok ellen

Munkaállomások, szerverek, virtuális gépek és felhőalkalmazások flottájáról gyűjtheti össze a biztonsági másolatokat. Az adatdeduplikálás és a növekményes biztonsági mentés funkcióval optimalizálhatja a tárhelyhasználatot, és elkerülheti a sávszélesség szűk keresztmetszetéből adódó problémákat. https://www.synology.com/dsm/solution/infrastructure

Fizikai munkaterhelések

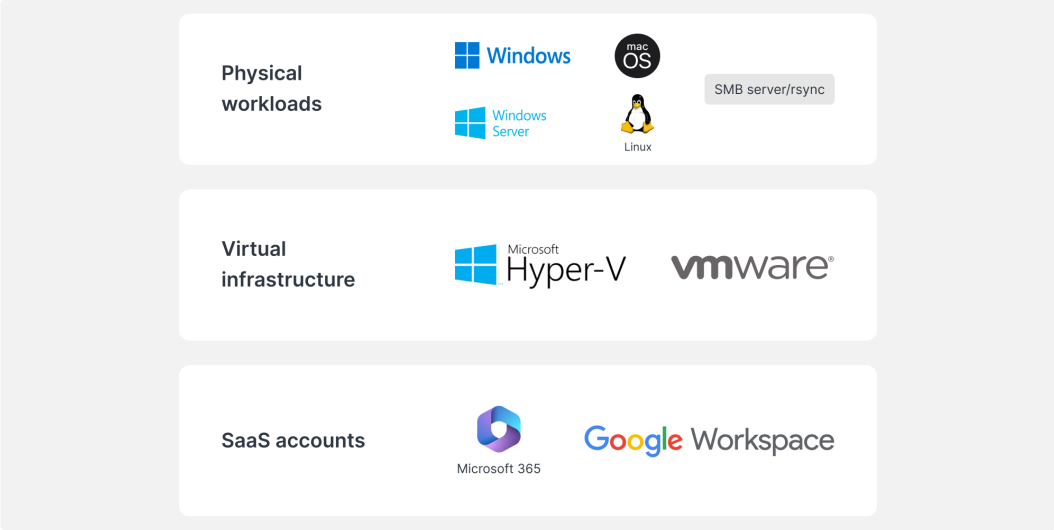
Rosszindulatú támadások esetén teljes biztonsági mentéssel és rugalmas, fájlszintű helyreállítással védheti a végpontokat.

Virtuális infrastruktúra

Hatékony adatcsökkentő technológiákkal biztonsági másolatot készíthet a VMware® vSphere™, Microsoft® Hyper-V® virtuális gépekről és LUN egységekről.

SaaS-fiókok

Az újonnan hozzáadott fiókok automatikus észlelésével folyamatos védelmet biztosíthat a felhőben tárolt adatok számára.



Hatékony helyreállítás

Csökkentse minimálisra a létfontosságú, éles környezeti rendszerek állásidejét a biztonsági másolatok helyi vagy külső Synology rendszerről való gyors visszaállításával.

Nullához közeli RTO

A munka mielőbbi folytatásához biztonsági másolati lemezképeket csatlakoztathat VMware®, Hyper-V® vagy Synology Virtual Machine Manager rendszeren. A szolgáltatáskimaradás elkerülése érdekében alternatív hipervizorra állíthatja vissza a virtuális gépeket.

Minimális RPO

Igény szerint beállíthatja a biztonsági mentés gyakoriságát, ezzel minimálisra csökkentheti a támadás során potenciálisan érintett adatok mennyiségét. A növekményes biztonsági mentésnek és a deduplikálásnak köszönhetően gyorsan megvédheti a rendszereket.

Intuitív működés

Lehetővé teheti az alkalmazottak számára, hogy kényelmes portálon tallózzák és megtekintsék a leveleket, névjegyeket és fájlokat a visszaállítás előtt, ezzel felhasználóbarátabb élményt nyújt, és csökkenti az informatikai munkacsoportok terheit.

Újabb biztonsági szint hozzáadása

A 3-2-1 biztonsági mentési stratégiát követheti egy harmadik adatkészlet külső helyszínen vagy a felhőben való tárolásával, így védve adatait tűz, természeti katasztrófa vagy lopás ellen.

Külső szerverekre

Tárolja a biztonsági mentéseket egy másodlagos helyen lévő Synology szerveren a fizikai katasztrófa elleni védelem érdekében, és replikálja a megváltoztathatatlan pillanatfelvételeket a zsarolóprogramok elleni védelem érdekében.

A felhőbe

Készítsen biztonsági másolatot nagyobb felhős társzolgáltatóra, így kliensoldali AES-256 titkosítással védi az adatokat a jogosulatlan hozzáféréstől. https://c2.synology.com/storage/nas

Megbízható a különböző iparágakban

„A Synology [...] lehetővé tette számunkra a szerverhez tartozó hardver kiadásainak csökkentését, [...] miközben az infrastruktúra és a munkaállomások biztonsági mentése, a rendszernaplózás és a fájlkezelés sokkal egyszerűbbé vált.”
https://www.synology.com/company/case_study/Investortools

„Az Active Backup for Business megoldásnak köszönhetően minden biztonsági mentésünk központosítva van és a nap 24 órájában folyamatosan elérhető, ami segít minimalizálni az állásidőt és betartani a FERPA előírásait.”
https://www.synology.com/company/case_study/University_of_Washington

„[...] Az Active Backup for Business lenyűgöző biztonsági mentési sebességre képes, és a duplikált adatok törlése terén is fantasztikus teljesítményt nyújt – a szerveren tárolt 58 TB adatból mindössze 28 TB-ról kellett mentést készíteni. [...]”
https://www.synology.com/company/case_study/SHISEIDO_Taiwan_ABB

„[...] Az Active Backup for Business [...] lehetővé teszi számunkra az összes biztonsági mentési feladat egyetlen központi konzolról való kezelését. A gyors és megbízható helyreállítás szintén az üzletmenet folytonosságát szolgálja.”
https://www.synology.com/company/case_study/UNESCO

Gyakori kérdések

Mi az a zsarolóvírus?

A zsarolóvírus a kártevő szoftver olyan típusa, amely titkosítja az áldozatok fájljait. A támadók ezután váltságdíjat követelnek az adatokhoz való hozzáférés visszaállításáért, és gyakran azzal fenyegetőznek, hogy nemfizetés esetén véglegesen megsemmisítik az adatokat. A zsarolóprogramos támadások rendkívül zavaróak lehetnek, és jelentős pénzügyi veszteségeket okozhatnak az egyének és a szervezetek számára. Fontos, hogy megvédje magát és eszközeit a zsarolóvírusok ellen, például a szoftverek naprakészen tartásával és a fájlok rendszeres biztonsági mentésével.

Milyen típusú zsarolóvírusok vannak?

A zsarolóvírusoknak számos típusa létezik, és folyamatosan új törzseket fejlesztenek ki. A zsarolóvírusok leggyakoribb típusai a következők:

- **Titkosító zsarolóvírus** – A zsarolóvírusok leggyakoribb típusa úgy titkosítja az áldozat fájljait, hogy azokhoz a visszafejtési kulcs nélkül nem lehet hozzáférni. A támadók ezután váltságdíjat követelnek a kulcsért cserébe
- **Kizáró zsarolóvírus** – Ez a típus kizárja az áldozatokat a számítógépükből a bejelentkezési adatok megváltoztatásával vagy egy olyan üzenet megjelenítésével, amely megakadályozza, hogy az áldozat hozzáférjen a rendszeréhez. A támadók ezután váltságdíjat követelnek a számítógép zárolásának feloldásáért
- **Szolgáltatott zsarolóvírus (RaaS)** – Olyan üzleti modell, amelyben a támadók zsarolóvírust kínálnak más személyeknek vagy csoportoknak, akik támadásokat szeretnének végrehajtani. Általában az előbbiek biztosítják a zsarolóvírust és kezelik a kifizetéseket, míg az utóbbiak a váltságdíj adott százalékát kapják
- **Scareware (hamis veszéllyel fenyegető vírus)** – Ennek célja, hogy a váltságdíj kifizetése érdekében ráijesszen az áldozatokra. Jellemzően hamis biztonsági figyelmeztetések vagy üzenetek megjelenítésével jár, amelyek azt állítják, hogy az áldozat számítógépe vírussal fertőzött. A támadó ezután váltságdíjat követel az állítólagos fertőzés eltávolításáért

Hogyan terjed a zsarolóvírus?

A zsarolóvírusok jellemzően adathalász e-mailek útján vagy a számítógépes rendszer sebezhetőségének kihasználásával terjednek. Adathalász támadásnál a támadó olyan e-mailt küld, amelynek forrása látszólag hiteles, például bank vagy ismert vállalat. Az e-mail gyakran tartalmaz egy hivatkozást vagy mellékletet, amelyre kattintva a zsarolóprogram települ az áldozat számítógépére. A rendszer sebezhetőségének kihasználása hasonló, azzal a különbséggel, hogy a támadó a rendszer biztonsági hiányosságait kihasználva az áldozat tudta nélkül telepíti a zsarolóprogramot. Mindkét esetben telepítése után a zsarolóprogram gyorsan átterjedhet az ugyanazon a hálózaton lévő többi számítógépre.

Mi a zsarolóprogramos támadás tipikus folyamata?

A zsarolóprogramos támadás folyamata jellemzően a következő lépéseket követi:

1. Adathalász e-mail küldésével vagy a rendszer biztonsági résének kihasználásával a támadó hozzáférést szerez az áldozat számítógépéhez
2. Amint a támadó hozzáfér az áldozat számítógépéhez, telepíti a zsarolóprogramot a rendszerre
3. A zsarolóprogram ezután titkosítja az áldozat fájljait, ezzel elérhetetlenné teszi azokat a felhasználó számára
4. A támadó ezután váltságdíjat követel az áldozattól, általában digitális valuta, például Bitcoin formájában, a titkosított fájlokat feloldó kulcsáért cserébe
5. Ha az áldozat kifizeti a váltságdíjat, a támadó megadja a visszafejtési kulcsot, és az áldozat hozzáférhet a fájljaihoz. Nincs azonban garancia arra, hogy a támadó valóban megadja a kulcsot, és még ha megadja is, az áldozat fájljai megsérülhetnek vagy megrongálódhatnak a titkosítási folyamat során

Fontos megjegyezni, hogy ennek a folyamatnak számos változata létezik, és nem minden zsarolóprogramos támadás követi pontosan a fenti lépéseket. Egyes támadásoknál például egyáltalán nem szerepel a fájlok titkosítása, míg mások a kényszerítés vagy a zsarolás más formáit tartalmazhatják.

Hogyan kaphatok zsarolóvírust?

A zsarolóvírust számos módon elkaphatja. Az egyik leggyakoribb mód adathalász e-mailben a rosszindulatú hivatkozásra vagy mellékletre való kattintás. Az ilyen típusú e-maileket úgy tervezték, hogy hivatalosnak tűnjenek, gyakran jól ismert vállalatot vagy szervezetet utánoznak. Ha rákattint a hivatkozásra vagy a mellékletre, ezzel telepíti a zsarolóprogramot a számítógépére. A zsarolóvírus elkapásának másik módja, hogy felkeres egy feltört webhelyet. Ezeket a webhelyeket támadók törték fel, és olyan kódot szúrtak be, amely automatikusan telepíti a zsarolóprogramot a számítógépére, ha felkeresi a webhelyet. A zsarolóvírust elkaphatja úgy is, hogy fertőzött fájlokat tölt le az internetről. Ez akkor fordulhat elő, ha gyanús webhelyről tölt le fájlt, vagy ha ismeretlen személy által megosztott fájlt tölt le. Röviden, fontos, hogy óvatos legyen az internetes böngészés során, és kerülje a hivatkozásokra való kattintást vagy az ismeretlen forrásból származó fájlok letöltését. Ez elősegítheti a zsarolóvírusokkal és más típusú kártevőkkel szembeni védelmet.

Kik a zsarolóvírusok célpontjai?

A zsarolóprogramos támadások bárkit megcélozhatnak, aki az internetre csatlakoztatott számítógépet vagy más eszközt használ. Egyes csoportok azonban másoknál nagyobb valószínűséggel válnak célponttá. A zsarolóprogramos támadások például gyakran a vállalkozásokat veszik célba, mivel ezek gyakran értékesebb adatokkal rendelkeznek, és inkább hajlandók váltságdíjat fizetni azok visszaszerzéséért. A kórházak, iskolák és más, kritikus szolgáltatásokat nyújtó intézmények szintén gyakori célpontok, mivel a zsarolóprogramos támadás megzavarhatja működésüket, és veszélybe sodorhatja emberek életét. Magánszemélyeket is érhet zsarolóprogramos támadás. Ezekben az esetekben a támadók megpróbálhatnak pénzt kicsikarni az áldozattól azzal fenyegetőzve, hogy törlik személyes fájljaikat, vagy nyilvánosságra hozzák bizalmas adataikat, ha nem fizetnek váltságdíjat. A zsarolóprogramos támadások célpontjait gyakran az adatok értéke és az alapján választják ki, hogy hajlandóak-e váltságdíjat fizetni azok visszaszerzéséért.

Milyen kockázatokkal jár a váltságdíj kifizetése?

A váltságdíj kifizetése a zsarolóvírusos támadónak a fájlok visszaszerzésének legegyszerűbb módjának tűnhet, de valójában nagyon kockázatos döntés lehet. A váltságdíj kifizetése számos kockázatot rejt magában, például a következőket:

- Nincs garancia arra, hogy a támadó valóban megadja a visszafejtési kulcsot. Számos esetben a váltságdíjat fizető áldozatok soha nem kapják meg a kulcsot, és továbbra sem férnek hozzá a fájljaikhoz
- A váltságdíj kifizetése arra bátoríthatja a támadókat, hogy folytassák a támadási kampányukat. Ha a támadók tudják, hogy az áldozatok hajlandóak kifizetni a váltságdíjat, a jövőben nagyobb valószínűséggel hajtanak végre további támadásokat
- A váltságdíj kifizetése jövőbeni támadások célpontjává teheti önt. Ha a támadó tudja, hogy hajlandó váltságdíjat fizetni, a jövőben nagyobb valószínűséggel lesz célpontja újabb támadásnak
- A váltságdíj kifizetése törvénytelen lehet. Bizonyos esetekben a váltságdíj kifizetése egy bűnszervezetnek a terrorizmus vagy más illegális tevékenységek finanszírozásának tekinthető

Bár a váltságdíj kifizetése a fájlok visszaszerzésének legegyszerűbb módjának tűnhet, valójában nagyon kockázatos döntés lehet. A döntés előtt fontos alaposan mérlegelni a kockázatokat.

Milyen költségekkel jár a zsarolóvírus?

A zsarolóprogramos támadás költsége jelentősen függ számos tényezőtől, ilyen például az alkalmazott zsarolóvírus típusa, a titkosított fájlok száma és a támadás hatékonysága. Egyes esetekben a zsarolóprogramos támadás költsége viszonylag alacsony lehet, a támadók néhány száz dolláros váltságdíjat követelnek. Más esetekben a költségek sokkal magasabbak lehetnek, a támadók több ezer dollárt vagy még többet követelnek az áldozat fájljaihoz való hozzáférés visszaállításáért. A váltságdíj kifizetésével járó közvetlen költségek mellett a zsarolóprogramos támadásoknak jelentős közvetett költségei is lehetnek. A zsarolóprogramos támadás például állásidőt és termeléskiesést okozhat, ami bevétel- és jövedelemkieséssel jár. Ez megrendítheti a vállalat hírnevét és az ügyfelek bizalmát, ami hosszú távon negatív hatással lehet az üzletmenetre. Ezek a közvetett költségek gyakran sokkal magasabbak magánál a váltságdíjnál.

Melyek a zsarolóvírus jelei?

A zsarolóprogramos támadás jelei a zsarolóvírus adott típusától függően változhatnak. Van azonban néhány általános közös jelei:

- A fájlok titkosítva vannak, és nem tud hozzáférni ezekhez
- Üzenetet kap a támadótól, amelyben váltságdíjat követel a visszafejtési kulcsért cserébe
- Ismeretlen programok vagy folyamatok futnak a számítógépén
- Számítógépe lassúvá válik vagy nem válaszol
- Számítógépe szokatlan hibaüzeneteket vagy felugró ablakokat jelenít meg

Ha azt gyanítja, hogy számítógépét zsarolóvírus fertőzte meg, fontos a gyors cselekvés. Válassza le számítógépét az internetről, hogy megakadályozza a zsarolóvírus terjedését.

Hogyan előzhetők meg a zsarolóprogramos támadások?

Számos lépés végrehajthat a zsarolóprogramos támadások megelőzéséhez, ilyenek a következők:

- Használjon elismert víruskereső vagy biztonsági szoftvert, és tartsa azt naprakészen. Ez segíthet megvédeni számítógépét a zsarolóprogramoktól és más típusú rosszindulatú programoktól
- Legyen óvatos az e-mail-üzenetek mellékleteinek vagy hivatkozásainak megnyitásakor. A zsarolóvírust gyakran adathalász e-maileken keresztül kézbesítik, ezért legyen körültekintő, hogy mire kattint
- Tartsa naprakészen operációs rendszerét és egyéb szoftvereit. A szoftverfrissítések gyakran biztonsági javításokat is tartalmaznak, amelyek segíthetnek megvédeni számítógépét a zsarolóvírusok és más fenyegetések ellen
- Rendszeresen készítsen biztonsági másolatot a fájlokról. Ez segíthet megvédeni az adatait, ha számítógépét zsarolóvírus fertőzte meg. Feltétlenül kövesse valamelyik javasolt biztonsági mentési stratégiát, ilyen például a 3-2-1 biztonsági mentési stratégia
- Legyen tisztában a zsarolóvírusok kockázataival, és tájékoztassa szervezetében a munkatársakat ezekről a fenyegetésekről. Ez segíthet megelőzni a zsarolóprogramos támadásokat, és megkönnyíti azok észlelését és az azokra való reagálást

A zsarolóprogramos támadások megelőzésének legjobb módja, ha éber marad, és lépéseket tesz számítógépének és adatainak védelme érdekében. Ez segíthet csökkenteni a zsarolóprogramos támadás kockázatát, és megkönnyítheti a helyreállítást, ha mégis bekövetkezik.

Hogyan védhet meg a Synology a zsarolóvírus ellen?

A megelőző intézkedések elengedhetetlenek annak elkerüléséhez, hogy zsarolóvírus áldozatává váljon. A választott víruskereső szoftver mellett használja a Synology megoldásait:

- **Hozzáférés megakadályozása** – Csökkentse a zsarolóvírusok terjedését fájl-, alkalmazás- és hozzáférési engedélyek beállításával, valamint biztonságos bejelentkezési hitelesítőadatok konfigurálásával a Secure SignIn és a C2 Password szolgáltatás segítségével
- **Eszközök védelme** – Az elavult rendszerek nagyobb veszélynek vannak kitéve. Frissítse az összes NAS eszközt egyszerre a Synology Central Management System (CMS) segítségével, és gondoskodjon a többi eszköz védelméről a Synology Directory Server és a C2 Identity csoportszabályzatának használatával
- **Gyanús fájlok elkerülése** – A gyanús fájlokat tartalmazó levélszemét és adathalász e-mailek gyakran használt módszerek a zsarolóvírusok terjesztésére. A Synology MailPlus hatékony védelmet nyújt a rosszindulatú programok és a levélszemét ellen
- **Biztonsági rések keresése** – A Synology biztonsági tanácsadó segítségével rendszeresen keresheti a rosszindulatú programokat, a biztonsági réseket és a rendellenes bejelentkezési tevékenységeket. A NAS eszközök biztonságának javítása érdekében célszerű megvalósítani a javasolt módosításokat.
  https://www.synology.com/dsm/overview/security

További módszerek adatai védelmére

A flotta kezelése

Használja ki azt a számos funkciót, amellyel központilag kezelheti az adathozzáférési engedélyeket, a szoftver és a rendszer állapotát, valamint sok mást.
https://www.synology.com/dsm/overview/administration

Az összes rendszer felügyelete

Az eszközök helyétől függetlenül azonosíthatja a gyanús bejelentkezési tevékenységeket, kezelheti a frissítéseket és felügyelheti az eszközök állapotát.
https://www.synology.com/dsm/feature/active-insight

Adatainak védelme

A 3-2-1 biztonsági mentési szabály követésével megvédheti adatait a véletlen és rosszindulatú módosítástól vagy törléstől.
https://www.synology.com/dsm/solution/data_backup

Védelem minden szögből

Töltse le kiberbiztonsági ellenőrző listánkat, és azonosítsa gyenge pontjait hackertámadás esetén.
https://global.download.synology.com/download/Document/Software/Brochure/Firmware/DSM/7.0/hun/S

Első lépések

Kapcsolat

További információkért forduljon a regionális értékesítőhöz
https://www.synology.com/form/inquiry/sales

Hol vásároljak?

Synology-partnerek keresése a régióban
https://www.synology.com/wheretobuy

Megjegyzés:

1. eSentire, 2022-es hivatalos kiberbűnözési jelentés
   https://www.esentire.com/resources/library/2022-official-cybercrime-report

Védje szervezetét a zsarolóprogramokkal szemben

https://www.synology.com/hu-hu/dsm/solution/ransomware

Synology weboldal

https://www.synology.com/

Kapcsolatfelvétel

https://www.synology.com/company/contact_us