CTI Jelentés

Ransomware as a Service (RaaS)

Zsarolóvírus-szolgáltatás

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERVÉDELMI INTÉZET

Bevezetés

A zsarolóvírus vagy zsarolóprogram olyan szoftver, amely valamilyen módszer alapján zárol egy számítógépet vagy titkosítás útján elérhetetlenné tesz egyes fájlokat a tulajdonosa számára. A bűnözők ígéretei alapján ezeket csak a megadott váltságdíj kifizetése után teszik újra elérhetővé.

Az elmúlt évek tendenciái azt mutatják, hogy egyre sűrűbben támadnak nagyobb vállalatokat az egyes csoportok a nagyobb haszonszerzés reményében. Az egyéni felhasználók sincsenek biztonságban az ilyen fenyegetéssel szemben, azonban fontos tudni, hogy sokkal kecsegtetőbb célpontot nyújt egy olyan vállalat, amely (fiat-valutától függetlenül) több milliós vagy milliárdos bevétellel rendelkezik és olyan adatokat, információkat kezelnek és tárolnak, amelyek nyilvánosságra hozatala vagy elérhetetlenné tétele óriási anyagi és PR károkat okozna a vállalat számára.

Jelen dokumentum célja, hogy bemutassa azt az üzleti modellt, amely során a zsarolóvírus készítői tovább értékesítik szoftverjeiket vagy szolgáltatásukat olyan személyek, bűnbandák vagy államilag támogatott szervezetek számára, akik célzott vagy tömeges támadásokat indítanak magánszemélyek, cégek vagy kormányzati szervek ellen.

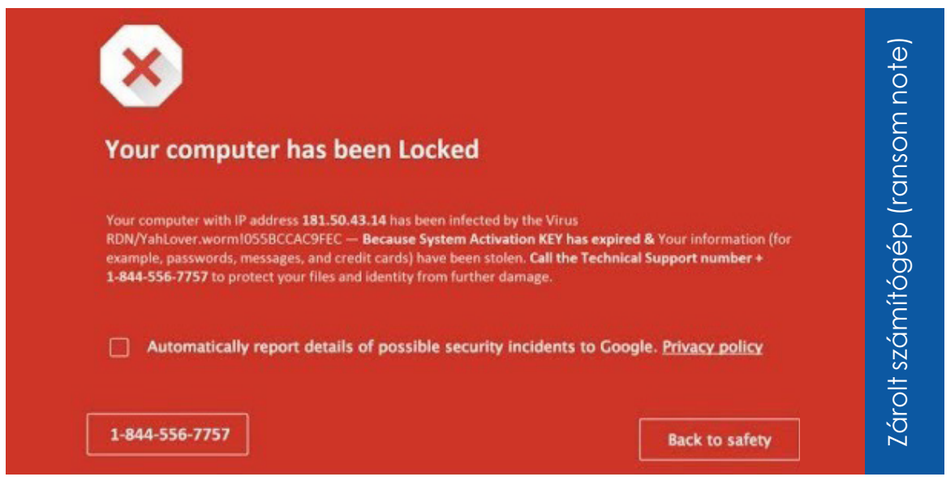
Tartalomjegyzék

A ransomware típusai

Összefoglalóan minden ilyen jellegű kártékony programról elmondható, hogy a számítógépet teljesen vagy részlegesen használhatatlanná teszi, és valamilyen váltságdíjat (ransom) követel annak helyreállításáért. A zsarolóvírusoknak alapvetően 4 típusa van:

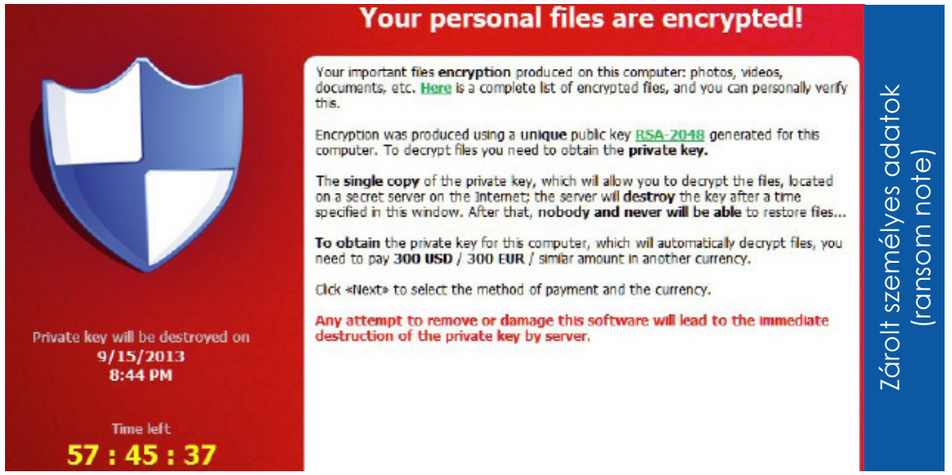
Locker ransomware

Ez a módszer teljesen blokkolja a számítógépes rendszerekhez való hozzáférést. Rendszerint social engineering technikákat és kompromittált hitelesítő adatokat használ a rendszerekbe való behatoláshoz. Miután bejutottak, a fenyegető szereplők blokkolják a felhasználók hozzáférését a rendszerhez amíg a váltságdíj ki nem lesz fizetve. Ezután áldozat képernyőjén egy olyan üzenet jelenik meg ami tájékoztat a fertőzés tényéről és a további teendőkről.



Crypto ransomware

Ezzel a módszerrel a számítógépen lévő összes vagy bizonyos fájlokat titkosítja, és váltságdíjat követel az áldozattól a visszafejtő kulcsért cserébe. Az újabb változatok már hálózati és felhőalapú meghajtókat is megfertőzhetnek. Leggyakrabban rosszindulatú e-mailek csatolmányaiban, weboldalak és letöltések útján terjednek.



Kettős zsarolóvírus

Ennél a módszernél a program nem csak titkosítja a fájlokat, hanem exportálja is azokat. Ilyenkor a támadók azzal is fenyegetőznek, hogy az ellopott adatokat közzéteszik és az eredeti fájlok használhatatlanok maradnak, ha a követeléseiket nem teljesítik. A váltságdíj kifizetése vagy a sikeres helyreállítás sem garantálja az adatok védelmét, ugyanis a fájlok a támadó birtokában maradnak ezután is.

RaaS

A RaaS (Ransomware as a Service – Zsarolóvírus mint szolgáltatás vagy szolgáltatott zsarolóvírus) kifejezés második része (as a service) utal az olyan szolgáltatásként nyújtott szoftverekre, amelyeket rendszerint a készítő elad vagy bérbe ad a vásárlónak vagy előfizetőnek. Az üzlet mindkét fél számára előnyös lehet: egyrészt a készítő többször is értékesítheti és állandó bevételt szerezhet az általa nyújtott szolgáltatásból, másrészt a vásárlónak nem kell foglalkoznia az adott termék fejlesztésével, így időt és akár pénzt is megtakaríthat.

A RaaS esetén ugyanez a helyzet: a kód készítője tömegesen értékesítheti (sőt, akár egyedi igényekre is szabhatja) programját, miközben sokkal kisebb kockázatot vállal az illegális tevékenység véghezvitele során, valamint a vásárló akár technikai tudás nélkül is hozzáférhet és elindíthat egy ilyen jellegű támadást. Ezeket a szoftvereket a darkweben tárolják és itt teszik elérhetővé az előfizetők részére. A szolgáltatás díja a program összetettségétől és funkcióitól függ, de általában kétféle fizetési konstrukció létezik. Az egyszeri díjazás esetén az ügyfél a program megvásárlása során egy összegben fizeti meg annak díját, míg a sikerdíjazás esetén egy kisebb összeget fizet meg előre az ügyfél, majd a sikeres támadás után a kapott váltságdíj egy részét megosztja a zsarolóvírus készítőjével.

A RaaS evolúciója

Az első zsarolóvírus az 1989-es AIDS trójai volt, amely titkosította az adatokat és váltságdíjat követelt a visszaállításért. A kártevőt kezdetben flopi lemezen terjesztették és csak a fájlok neveit titkosította, valamint szimmetrikus titkosítást használt, vagyis a visszafejtéshez szükséges információ elérhető volt az áldozat számítógépén.

A 90-es évek közepétől kezdték kombinálni a szimmetrikus és az aszimmetrikus titkosítást, így létrehozva egy sokkal hatékonyabb és komoly károkozásra képes módszert.

A 2010-es évek elejéig jellemzően sok zsarolóprogram rosszul volt implementálva és viszonylag egyszerűen helyrehozhatók voltak a titkosított állományok.

A bitcoin 2009-es megjelenése új teret nyitott a zsarolóvírusok előtt a részleges anonimitás miatt. Ezt megelőzően nehezen tudtak hozzájutni a bűnözők a kifizetett váltságdíjakhoz, ugyanis könnyen lenyomozhatók voltak az általuk használt e-pénztárcák. A bitcoin váltságdíjfizetés és az erős titkosítás kombináció eredményeképpen a CryptoLockerrel 2013 szeptemberétől 27 millió dollárt tudtak kicsalni az áldozatokból. A „spray and pray" módszert alkalmazták, vagyis a céljuk az volt, hogy minél több áldozatot szedjenek, de mindössze néhány 100 dolláros váltságdíjat követeltek jellemzően magánszemélyektől vagy kisebb cégektől, így egy sikeres fertőzés után „megfizethető" volt a helyreállítás. Magasabb váltságdíj követelése esetén valószínűleg sokkal kevesebb áldozat fizetett volna, így optimalizálhatták a bevételeiket.

A kiberbűnözők elkezdték felismerni a zsarolóvírusok értékét a vállalatok üzleti tevékenységének megzavarásában. Az előre definiált összegek helyett később már megbecsülték, hogy mekkora lehet a vesztesége az áldozatul esett vállalatnak, majd ennek függvényében határozták meg a váltságdíj összegét. Ennek az összegnek is még megfizethetőnek kellett lennie, azonban ez további optimalizálást jelentett a bevételek maximalizálása érdekében.

A modern zsarolóvírusok kialakulásához az erős titkosítás, gyors, anonim fizetési lehetőség és az üzleti tevékenység megzavarása mind hozzájárult.

2014-ben a zsarolóvírusok készítői és üzemeltetői elkezdték értékesíteni szoftverjeiket bizonyos online fórumokon (Ransomware as a Service – RaaS). Az első ilyen program a CTB-Locker volt, ahol már nem a készítők terjesztették a zsarolóvírust, hanem az ügyfeleik. A szerzett bevétel egy része így az üzemeltetőkhöz folyt be, jóval kisebb kockázat vállalás mellett. A korábbiakban csak a hozzáértő bűnözők tevékenykedtek ezen a területen, így viszonylag kevés áldozat esett csapdába világviszonylatban. A RaaS elterjedésének következménye lett az áldozatok számának növekedése, mivel olyan személyek is végrehajthatnak támadásokat, akiknek nincs meg az ehhez szükséges szaktudása, továbbá részben elszigetelődtek a bűnüldözéstől. Amikor nyomás helyezkedik rájuk vagy sikerül az illetékes hatóságoknak közelebb kerülniük a gyártókhoz, akkor feloszlanak és valamennyi idő elteltével új név alatt újrakezdik a tevékenységüket, ezzel teremtve egy „macska egér játékot".

A modern RaaS üzletág egy további jellemzője a fenntartott ügyfélszolgálat, ahol az áldozatok kérdéseket tehetnek fel és útmutatást kérhetnek, például a bitcoin vásárláshoz. Különböző váltságdíjkövetelők még azt is felajánlják a díjak megfizetése után, hogy részletes útmutatást adnak arról, hogy hogyan hajtották végre a fertőzést. Ezek a jellemzők azt mutatják, hogy üzleti érdeke a csoportoknak, hogy az áldozatok fizessenek. A legtöbb banda elsődleges célja a haszonszerzés, így az üzlet csak akkor lesz kifizetődő, ha az áldozatot sikerül meggyőzni, hogy a titkosított adatokat visszakapja. Természetesen ez sosem lesz garancia, mert mégis csak illegális tevékenységet folytató emberekkel tárgyal az áldozat.

A fertőzések további velejárója lehet, hogy a támadók kriptobányász programokat telepítenek az áldozatok eszközeire, így a feloldást követően kihasználhatják a számítógép erőforrásait. Más zsarolóprogramok hálózati szolgáltatás-megtagadás típusú támadást indíthatnak az ügyfeleikkel való kommunikáció megnehezítésére.

2018-tól kezdve még nagyobb nyomás helyeződött azokra a vállalatokra, akik ellen sikeres támadást hajtottak végre, azzal kezdték fenyegetni őket a zsarolóvírus üzemeltetői, hogy nyilvánosságra hozzák az ellopott adatokat, vagy viszonteladásra kínálják őket. Nyilvánvalóan minden esetben titkos üzleti információkról van szó, így az eddigi legrosszabb eshetőségnél (hogy elérhetetlenné válnak az adatok) még rosszabb eset következhet be.

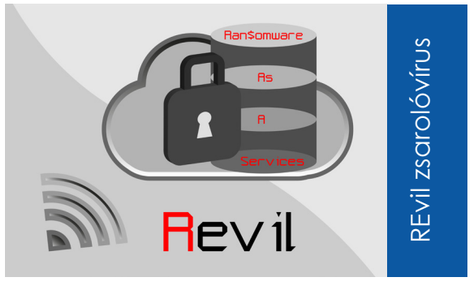
RaaS csoportok

DarkSide

A DarkSide üzemeltetői hagyományosan a Windows gépekre összpontosítottak, de nemrégiben Linux rendszerekre is kiterjesztették tevékenységüket, és a nem javított VMware ESXi hypervisorokat futtató vállalati környezeteket célozták meg. 2021. május 10-én az FBI közzétette, hogy a Colonial Pipeline incidens a DarkSide zsarolószoftverrel kapcsolatos. Később jelentették, hogy a Colonial Pipeline hálózatáról körülbelül 100 GB adatot loptak el és a szervezet állítólag közel 5 millió USD-t fizetett egy DarkSide leányvállalatnak.

REvil (Sodinokibi)

A Pinchy Spider nevű bűnszervezet értékesíti és jellemzően a nyereség 40%-át kéri el. Vélhetően a GandCrab volt a REvil elődje. 2019 áprilisában szűnt meg a GandCrab és ekkor kezdte meg működését a REvil. A Pinchy Spider rendszerint figyelmezteti az áldozatokat a tervezett adatszivárgásra és bizonyítékként minta adatokat is megosztanak. A támadást követően egy visszaszámláló indul el. A megadott idő letelte után az adatok egy részének vagy egészének közzétételét eredményezi.



Dharma

A Dharma 2016 óta elérhető a darkweben, és főként a távoli asztalelérést biztosító protokoll (RDP) biztonsági hibáit kihasználva jut be az áldozatok informatikai rendszerébe. A fertőzés során a gyakori kiterjesztéssel rendelkező fájlokat (dokumentum, táblázat, képek) titkosítja, és megakadályozza a hozzáférést, amíg az áldozat a meghatározott összegű Bitcoin váltságdíjat a zsaroló által megadott Bitcoin tárcába el nem küldi. A támadók általában 1-5 Bitcoint követelnek a célpontoktól a legkülönbözőbb iparágakban. A Dharma nem központilag irányított, ellentétben a REvil és más RaaS csoportokkal.

LockBit

A LockBit-et használó támadások eredetileg 2019 szeptemberében kezdődtek, amikor ".abcd vírusnak" nevezték el, amely a titkosított fájlok kiterjesztésére utalt. Leginkább kormányzati és vállalati célpontjaik voltak az USA-ban, Kínában, Angliában, Németországban, Franciaországban és Ukrajnában. A váltságdíj követelése során bizonyítékot is szolgáltatnak az áldozat dokumentumairól. A határidő lejárta után a társvállalat közismerten közzétesz egy mega[.]nz linket az ellopott adatok letöltéséhez.

Conti

A Conti az egyik legaktívabb zsarolóvírus csoport, amelynek profiljában főképp ipari rendszerek állnak, és már legalább 63 vállalat ipari vezérlőrendszere (ICS) elleni támadás köthető a nevükhöz.

NetWalker

A NetWalker (más néven Mailto vagy Koko) zsarolóvírust a biztonsági kutatók elsőként 2019 augusztusában azonosították. A NetWalkert a támadók elsősorban kormányzati szervek, egészségügyi intézmények és egyéb vállalatok elleni támadások során alkalmazzák, azonban otthoni felhasználók is célpontba kerülhetnek. A vírus eddigi legismertebb áldozatai az ausztrál Toll Group, az Illinois állambeli közegészségügyi szolgálat, valamint az ausztriai Weiz városi rendszerei. A NetWalker működése során megkísérli a teljes hálózat kompromittálását, illetve valamennyi csatlakoztatott adattároló eszköz titkosítását.

Az NBSZ NKI javaslatai

- Vizsgáljuk felül a nyitott portokat, zárjuk be a szükségtelen portokat, és biztosítsunk fokozott felügyeletete a szükséges portoknak és naplózásuknak!
- Korlátozzuk a gyakori portok internet irányából történő elérését (megadott IP címekről, bizonyos felhasználók számára)!
- 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 elérése.
- Tartsuk naprakészen a határvédelmi rendszerek szoftvereit!
- Csökkentsük a támadások kockázatát azáltal, hogy frissítjük a határvédelmi eszközök feketelistáját! (Több gyártó rendelkezik nyilvánosan elérhető listákkal pl.: Cisco.)!
- Függesszük fel a szükségtelen felhasználói fiókokat, mérsékeljük a távoli eléréssel rendelkező felhasználókat, és időszakosan vizsgáljuk felül a felhasználók jogosultságait!
- Alkalmazzunk szigorú jelszóházirendet és tegyük kötelezővé a jelszavak periódikus cseréjét!
- Készítsünk rendszeres időközönként online és offline (szalagos egység, külső merevlemez) biztonsági mentést és archiválást!

Biztonsági incidens bekövetkezése esetén az NBSZ NKI a következőket javasolja:

- Mielőbb válasszuk le az érintett eszközt a hálózatról!
- Az érintett adathordozók helyreállítása előtt készítsünk egy bitazonos másolatot!
- Ne fizessünk váltságdíjat, mert semmilyen garancia nincs arra, hogy a fájlok visszaállíthatók lesznek a fizetést követően!
- Jelentsük be az incidenst az NBSZ NKI részére a cert@govcert.hu e-mail címen!

További hasznos információkat olvashat az NBSZ-NKI által készített "Mit tegyünk, ha zsarolóvírustámadás ért bennünket?" című CTI jelentésében, amely összefoglalja a legfőbb tudnivalókat a zsarolóvírusokról, javaslatokat ad az ilyen jellegű támadások elkerülésére, valamint segítséget nyújt abban az esetben, ha

NEMZETI KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás! podcast

2022