Amit a zsaroló “vírusokról” tudni kell...

Vírus-e a zsarolóvírus?

A ma ismert zsarolóvírusok valójában nem is vírusok.

Ez azt jelenti, hogy képtelenek önállóan reprodukálni saját magukat és képtelenek arra is, hogy számítógépről számítógépre terjedjenek. Helyesebb emiatt a **zsaroló program** elnevezés.

Ez olyan, mint egy „üzleti vállalkozás”

A zsarolóvírusok célja nem az öncélú pusztítás, hanem a közvetlen haszonszerzés. Ennek megfelelően nem egyszerű csínytevésről van szó, hanem minden tekintetben megtervezett bűncselekményről.

A zsaroló programok készítői gondosan ügyelnek arra, hogy olyan programokat készítsenek, amelyeket a víruskeresők nem ismernek fel. Ennek érdekében az ismertebb víruskereső programokkal gondosan tesztelik is „termékeiket”, és ha szükséges módosítják, hogy a védelmen biztosan átjusson.

Nem egyszerűen szabadon engedik a „vírust”, mert önmagától nem tud terjedni. Hanem gondosan megtervezik, hogy hogyan és miként, milyen alkalmazásokba építik be, mikor és hogyan „dobják piacra”.

Újabb verziókat jellemzően nem naponta adnak ki, hanem jellemzően néhány hetente. Ekkor azonban gyakran 300-400 féle új változatot is kiadnak különféle csatornákon. Ezzel megnehezítik azt, hogy vírusvédelem gyártók csak lassabban tudjanak minden változatra reagálni.

Az üzleti modell része, hogy ismereteink szerint a zsarolók ügyelnek arra, hogy aki fizet, annak ténylegesen vissza is állítják az adatait. Ennek ellenére javasoljuk, hogy más megoldást keressenek adataik helyreállítására, mivel a fizetéssel csak a bűnözőket erősítik.

Akkor hogyan kerül a számítógépre?

A zsarolóvírusok a szó hagyományos értelmében vett megtévesztéssel kerülnek a számítógekre.

Egyszerűen megkérik a felhaszálót rá, hogy töltsék le, vagy ha elektronikus levélben érkezett, akkor indítsák el a mellékelt programot.

Sőt adott esetben arra is megkérik a felhasználót, hogy letöltés és telepítés előtt kapcsolják ki a számítógép vírusvédelmét, mert az akadályozhatja a telepítést.

Ön komolyan venné az alábbi kérést?

Kérem, hogy ha nyaralni megy, akkor az értékeit készítse ki a konyhaasztalra, hogy tűz esetén a tűzoltók könnyebben kimenthessék azokat.

Kérjük, hogy az ajtóra jól láthatóan írja ki, hogy mikor érkezik vissza és a riasztó készülék kódját se felejtse el megadni.

Hogyan védekezhetünk a zsarolóprogramok ellen?

A hatékony vírusvédelem, mint például az **AVG** (http://www.avg.hu/) nagyon fontos. Ugyan a zsarolóprogramok készítő mindent megtesznek annak érdekében, hogy a vírusvédelmek ne ismerjék fel ezeket a programokat, de még mindig az antivírus gyártók reagálnak leggyorsabban ezekre a támadásokra.

Soha ne telepítsen bizonytalan forrásból származó programot.

Legyen különösen elővigyázatos, ha egy weboldal vagy program a vírusvédelem kikapcsolását kéri öntől.

Legyen elővigyázatos! Ha a program látszólag ismerőstől érkezett is, de vajon az ígért feladat ellátása, adatok megtekintése érdekében logikus és szokásos-e például egy letöltéskezelő telepítése? Általában nem.

Életszerű-e, hogy például egy mindössze néhány számot tartalmazó Excel fájlt tömörítve küldjön valaki? Nem valószínű....

Hogyan csökkentse a károk kockázatát egy esetleges sikeres támadás esetén?

Lehetőleg normál munkavégzéshez ne használjon és ne adjon másnak se rendszergazdai jogosultságot.

A zsarolóprogramok általában nem próbálnak meg rendszergazdai jogosultságot szerezni, hanem a feltűnést kerülve csak azt titkosítják, amihez hozzáférnek. A kevesebb jogosultság kevesebb kockázatot is jelent.

Használjon verziózó rendszereket

Így ugyan kellemetlenséget és többletmunkát eredményez egy zsarolóprogram, de helyrehozhatatlan károkat vagy adatvesztés nem okoz.

A modern operációs rendszerek (pld. Windows 7,8,10) lehetővé teszik, hogy a módosított (így a titkosított) fájlok korábbi állapota helyreállítható legyen. Ha ezt a szolgáltatást számítógépen engedélyezték és úgy állították be, hogy a korábbi verziók törlésére a felhasználó nem jogosult, akkor a felhasználó jogosultságait használó zsaroló program sem lesz rá jogosult.

Ha az operációs rendszer nem is támogatja ezt a fajta megoldást, akkor szóba jöhetnek az ilyen funkciókkal ellátot hálózati tárolók (NAS-ok). De egyes felhőszolgáltatások is biztosítják ezt a funkciót.

A megfelelően beállított fájlszerverek, NAS-ok és felhő szolgáltatások verziózó rendszere akkor is biztonságos maradhat, ha egy adott gépen a feladat elvégzése érdekében helyi rendszergazdai jogosultsággal kell dolgozni.

A korábbi verziók mentése természetesen többlet tárhelyet igényel, ugyanakkor használata nagyon kényelmes, mivel automatikusan megtörténik a korábbi verziók mentése.
Ne felejdje! A verziózó rendszerek használata a rendszeres biztonsági mentést nem teszi feleslegessé!

Mindig legyen biztonsági mentése adatairól

A biztonsági mentésről akkor is helyreállíthatóak az adatok, ha semmi más nem segít.

A biztonsági mentést tartalmazó adathordozót mindig csak a mentés idejére csatlakoztassa a számítógéphez és annak befejeződését követően válassza le!
Ne mindig ugyanazt az eszközt használja!
A mentés sikerességét és az adatok olvashatóságát ellenőrizze!

A biztonsági mentés visszatöltése rendszerint már adatvesztés nélkül nem végezhető el, ugyanakkor csak a legutóbbi mentés óta keletkezett adatokat kell valamilyen módon újra előállítani.

Egy kis történelem és amit még hasznos tudni:

A zsaroló vírusok (ransomware) megjelenése Evgenij Mihailovics Bogacsev nevéhez fűződik. Jelenleg a ő a világ legkeresettebb kiberbűnözője. Az FBI 5.000.000$ nyomravezetői díjjal jutalmazza azt, aki az Bogacsevet segít kézrekeríteni.
Forrás: https://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev

Hogyan működik:

A zsaroló vírusok általában hibrid titkosító megoldásokat használnak, amelyben kombinálják az erős kulcsú nyilvános kulcsú megoldást, a szimmetrikus kulcsú megoldásokkal.

A nyilvános kulcsú megoldások előnye, hogy nagyon erős titkosítást lehet vele megvalósítani, ugyanakkor relatíve lassúak. Mivel a megfejtéshez nem ugyanaz a kulcs (jelszó) szükséges, mint a titkosításhoz, ezért gyakorlatilag feltörhetetlen az ilyen módon titkosított fájl, mivel a megfejtéshez szükséges jelszó nincs jelen a számítógépen, tehát megtalálni is lehetetlen. A titkosításhoz használt „jelszó„ ismerete pedig nem segít hozzá a megfejtéshez szükséges „jelszó” megtalálásához.

A hibrid megoldások az adatok titkosításához szimmetrikus eljárást használnak, ahol a titkosítás ugyanazzal a jelszóval történik, mint a megfejtés. Ez ugyanúgy nagyon erős védelmet biztosít, csak a kulcsvédelem gyengébb, mivel az jelen van. Előnye, hogy ez az eljárás sokkal gyorsabb, mint nyilvános kulcsú eljárás, így ugyanannyi idő alatt több adat titkosítható. Ezt követően pedig csak a szimmetrikus titkosításnál használt jelszót titkosítják nyilvános kulcsú eljárással. Így ötvözik a gyorsaságot a feltörhetetlenséggel.

Újabban megjelentek primitívebb, csak szimmetrikus eljárást használó változatok is, más bűnözői csoportoktól. Ezek esetében a jelszót valahogyan elrejtve általában magán a számítógépen tárolják. Így ezeknél kellően nagy erőfeszítéssel esély lehet a megfejtésre, mivel csak az elrejtett kulcsot kell megtalálni.