TRUST IN GERMAN SICHERHEIT

A titkosító vírusok működéséről

A fájlokat titkosító és a számítógépeket a felhasználók előtt lezáró kártevők a legveszélyesebbek közé tartoznak, mivel a kódolás feltörésére a legtöbbször nincs mód, és így adatainkat örökre elveszíthetjük.

Egy zsaroló vírus (angolul ransomware) ugyanazt teszi elektronikus formában, mint egy hagyományos bűnöző: elvesz tőlünk valamit, majd pénzt kér azért, hogy visszaadja. Ezek a kártevők két fő típusba sorolhatóak: az első a titkosító trójaiak, a második pedig a képernyőzárak.

A titkosító trójaiak módszeresen végigsöpörnek a merevlemezen, és úgy módosítják a dokumentumokat és a fotókat, hogy azok a titkosítás feloldásához szükséges kulcs nélkül soha többet nem lesznek megnyithatóak. A kulcsot a bűnözőktől vehetjük meg, jellemzően 150 ezer forint körüli összegért, de fizetni igen kockázatos, mivel jó eséllyel a pénzünk elveszik, de a kulcshoz nem jutunk hozzá. Más megoldás viszont nincs igazán: a feltörésre még egy szuperszámítógép birtokában sincs esélyünk.

A képernyőzárak jellemzően a teljes operációs rendszert zárolják, egészen addig, amíg a váltságdíjat ki nem fizetjük. Többségük valamilyen „hatósági figyelmeztetést” jelenít meg, amely arról tájékoztat, hogy a gépen „inkriminált” állományok találhatóak, és a „hatóság” eljárást kezdeményez, hacsak a felhasználó nem fizeti be a rá kiszabott „büntetést”.

Zsaroló kártevőkből több száz különböző változat létezik, a legismertebb titkosítók a Cryptolocker, a Cryptowall, a VaultCrypt és a CTB-Locker, a legelterjedtebb képernyőzár pedig az FBI Trójai, vagy más néven Reveton.

Miért terjednek olyan jól?

A zsaroló kártevők terjesztésére rendszerint az emberek megtévesztésének (social engineering) segítségével kerül sor. Az embereknek hajlamuk van arra, hogy segítsenek egymásnak, és motiváltak arra is, hogy elkerüljék a problémákat. A bűnözők pedig kihasználják ezeket a tulajdonságokat.
Egy tipikus példa a hamis megrendelési visszaigazolás. Ezekhez az e-mailekhez rendszerint csatolva van egy fájl, melyet az áldozatnak meg kell nyitnia. Ha valaki kap egy e-mailt, amely tájékoztatja arról, hogy a „rendelése megérkezett”, de nem emlékszik arra, hogy rendelt volna valamit, akkor hajlamos megnyitni a csatolmányt, hogy „megtudja a részleteket”.

Egy másik, tipikus módja a megfertőződésnek az, ha fertőzött weboldalra tévedünk. Ilyenkor nincs szükség semmilyen letöltésre, és arra sem, hogy valamire rákattintsunk, egyszerűen böngészés közben fertőződik meg a számítógépünk.

A vírusok működését segítik a külső alkalmazások sérülékenységei. A Word, az Adobe Acrobat, a Java vagy magának az operációs rendszernek a biztonsági rései kihasználhatóak a terjesztésükre.
A zsaroló kártevők működése ráadásul rendkívül gyors. A csatolmány megnyitása után néhány ezredmásodperccel már zárolásra kerülhet a gép, de a titkosító kártevők is hasonlóan gyorsak. Mialatt a titkosító komponens telepítésre kerül, a kártevő kapcsolatba lép a bűnözők szerverével, és letölti a titkosításra használt egyedi kulcsot. Amikor a zsaroló üzenet megjelenik a képernyőn, rendszerint már késő van mindenhez: a dokumentumok titkosításra kerültek.

Miért nem mindig segít a vírusirtó?

A vírusirtó szoftverek gyártói évek óta koncentrálnak arra, hogy blokkolják a titkosító kártevők működését. A védelem alapját még mindig a rendszeresen frissített vírusleírások (szignatúrák) képezik, de ezek rendszeres frissítése már messze nem elegendő a védelemhez. A proaktív, magatartás alapú védelem célja, hogy szignatúrák nélkül is felismerje a kártevőket, pusztán az alapján, ahogyan azok viselkednek a számítógépen.
Felmerülhet a kérdés, hogy miért nem létezik önálló védelmi program a zsaroló kártevők ellen. Technikailag lehetséges lenne elkészíteni egy olyan szoftvert, mely védelmet nyújt a legtöbb zsaroló kártevő ellen. A problémát az jelenti, hogy ez a szoftver annyira leterhelné – és így le is lassítaná – a számítógépeket, hogy a felhasználók nem szívesen telepítenék a gépükre. A feladat tehát a vírusirtó szoftverek készítői számára az, hogy úgy nyújtsanak maximális védelmet, hogy közben minimalizálják a szoftvereik erőforrásigényét.

Mit tehetünk a fertőzés megelőzésére?

Mivel a zsaroló kártevők által titkosított adatokat nem lehet visszanyerni, a legfontosabb mind az otthoni, mind a vállalati felhasználók számára, hogy folyamatosan biztonsági másolatokat készítsenek adataikról. Ideális esetben naponta készül ilyen másolat, melyet azután a számítógéptől teljesen külön tárolunk, ami azt jelenti, hogy a külső adathordozó sem vezeték nélküli, sem vezetékes hálózaton nincs összekapcsolva a számítógéppel. A feladat elvégzését megkönnyíti, hogy egyes vírusirtó szoftverekben (például G Data) beépített mentési modult találunk.

A G Data emellett azt tanácsolja, hogy folyamatosan telepítsük a külső alkalmazások és az operációs rendszer frissítéseit. A harmadik fél szoftvereibe került sérülékenységek ellen a vírusirtók

sérülékenységvédelme (exploit protection) ugyan védelmet tud nyújtani, de ennek megvannak a maga korlátai. A legjobb, ha minden alkalmazás biztonsági frissítéseit telepítjük.

A harmadik fontos teendőnk a magatartás alapú és a felhő alapú védelem aktiválása. A heurisztikus, proaktív, valamint a reputáció alapú védelmi technológiák kiegészítik a hagyományos vírusvédelmet, és további biztonsági rétegeket képeznek a számítógépen. Ezek segítségével a vírusirtó képes kiszűrni például azokat a még nem ismert kódokat, programokat, melyek hátsó kapukat nyitnak a gépen, és külső szerverekről próbálnak meg adatokat letölteni.

Fontos tudni, hogy ugyan nem létezik 100 százalékos biztonságot nyújtó védelmi program, de a folyamatosan frissített vírusirtó szoftver használata rendkívül fontos. A különböző védelmi technológiák kombinálásával a minőségi szoftverek megbízható védelmet nyújtanak, a kockázatot pedig nulla közeli szintre csökkenti a rendszeres mentés.

Ugyanakkor van néhány magatartási szabály, amit fontos betartanunk. Így például megnyitás nélkül érdemes törölnünk azokat az e-maileket, amelyek az alábbi három kritériumból legalább kettőnek megfelelnek:

- ismeretlen feladótól érkeznek,
- sürgető hangnemben vannak megírva, és negatív következményeket helyeznek kilátásba,
- és valamilyen cselekvésre hívnak fel (ellenőrizze a mellékletet).

Mivel a kártevők jellemzően annak a felhasználónak a nevében futnak a gépen, aki be van jelentkezve, így érdemes nem rendszergazdai, hanem általános felhasználói jogosultsággal használni a gépet.

Vállalati környezetben a különböző szoftverek futását korlátozhatjuk házirendkezelővel is, a G Data Policy Manager segítségével például kijelölhetjük, hogy milyen gyártóktól származó programokat lehessen elindítani. Emellett lehetőség van arra, hogy a csoportházirendek szerkesztésével korlátozzuk, hogy milyen mappából legyen futtathatóak a különböző programok. Mivel a legtöbb kártevő ideiglenes mappákból vagy a lomtárból indítja el magát, ez is növeli a biztonságot. (Erről részletesebben a G Data angol nyelvű letölthető whitepaperében olvashat.)

Mit tegyünk, ha megfertőződött a számítógépünk?

Először is ne essünk pánikba, mert az egészen biztosan csak ront a helyzeten. Az első és legfontosabb, hogy a fertőzött számítógépet húzzuk le a hálózatról, hogy a fertőzés ne tudjon átterjedni más gépekre. Adott esetben a gépet kapcsoljuk ki, majd a merevlemezt tisztítsuk meg úgy a kártevőktől, hogy a vírusirtó indítólemezét használjuk, így nem az alapértelmezett operációs rendszert indítjuk el, hanem a vírusirtó szoftver kezelőfelületét.

A váltságdíjat ne fizessük ki! Egyáltalán nem garantált, hogy visszakapjuk az adatainkat, de ha fizetünk, azzal hozzájárulunk a szervezett bűnözés sikeréhez. Az adatainkat állítsuk helyre a külső mentésből, és ha erre szükség van, akkor egy adattörlő szoftver segítségével fertőtlenítsük a merevlemezt, majd telepítsük újra a számítógépet.

G Datáról

A G Data már 30 éve megbízható partner a vírusvédelemben. 1985-ben a cég alapítója, Kai Figge mutatta be a világ első vírusirtó koncepcióját, majd két évvel később ő és társa, Frank Kühn készítették el a legelső antivírust Atari ST rendszerre. A G Data az első gyártók között készített vírusirtót MS DOS és Windows rendszerre is. A Ruhr-vidékről induló vállalkozás szoftverei

hamarosan több millió német számítógépen futottak, és a cég azóta is őrzi pozícióját az anyaországban.

A G Data ma több mint 300 saját munkatárssal rendelkezik, és 9 európai országban önálló képviseletet tart fent. A céget emellett elkötelezett disztribútorok több ezer minősített szakértő munkatársa képviseli az Egyesült Államoktól Ausztráliáig, több mint 90 országban. A magyarországi disztribúciót a V-Detect Antivírus Kft. látja el. Ügyfelei között a számos 10-20 fős kisvállalat mellett megtalálhatóak a tízezres kliensszámmal rendelkező nagyvállalatok és az olyan szervezetek is, mint a 359 várost és önkormányzatot magába foglaló Észak-Rajna-Vesztfália tartomány.

Az európai gyártók közül a G Data rendelkezik a legtöbb elismeréssel. A nemzetközi PC World magazin 2012-ben a G Data InternetSecurity szoftvert a világ legjobb védelmi szoftverének választotta.

A G Data minden fontos vírusirtóteszten részt vesz, így a termékek teljesítménye folyamatosan ellenőrizhető. A cég licencpolitikája lehetővé teszi, hogy ügyfelei a szoftverekből mindig a legfrissebb változatot használják. A magyarországi terméktámogatást 24/7-es nemzetközi terméktámogatás egészíti ki.