Zsarolóvírus

Mi is az a zsarolóvírus?

A zsarolóvírus egy olyan típusú rosszindulatú szoftver (malware), amelyet fájlok vagy számítógépek túszul ejtésére terveztek, hogy segítségével váltságdíjat követeljenek az áldozattól a hozzáférés visszaszolgáltatása érdekében. A zsarolóvírus támadások nagyon gyakorivá váltak, mivel ezek rendkívül jövedelmezők a bűnözők számára.

A legtöbb rosszindulatú programhoz hasonlóan a zsarolóvírus is a számítógép megfertőzésével kezdi meg működését, leggyakrabban egy fertőzött melléklet megnyitásával, vagy egy adathalász e-mailben lévő rosszindulatú hivatkozásra való kattintással. Miután a zsarolóvírus megfertőzte a számítógépét, titkosítja a merevlemezen lévő fájlokat – akár a teljes merevlemezt is – vagy bármilyen más eszközt, ami a számítógéphez kapcsolódik, így fájljaihoz Ön már nem férhet hozzá. Ezután tájékoztatja Önt, hogy a fájlok helyreállításának egyetlen módja az, hogy kifizeti a váltságdíjat a zsarolóknak (innen ered a zsarolóvírus elnevezés). Időnként a bűnözők azzal is fenyegetőznek, hogy nyilvánosságra hozzák fájljait, ha nem fizeti meg a váltságdíjat. A bűnözők nyomon követhetetlen digitális valutában, például Bitcoin formájában kérhetik a kifizetést. Ha kifizeti a váltságdíjat, a bűnözők esetleg biztosítják a fájljaihoz való hozzáférést, azonban erre nincs semmilyen garancia. Néha előfordul, hogy a pénz megszerzése után is titkosítva hagyják számítógépét, vagy folyamatosan további váltságdíjat kérnek.

A fertőzés elleni védelem

A számítógépét ugyanúgy védheti meg a zsarolóvírus fertőzéstől, mint a többi rosszindulatú programtól. Itt van három kulcsfontosságú lépés:

- **Frissítse rendszereit és szoftvereit**: A számítógépes bűnözők gyakran a szoftverekben lévő hibákat (úgynevezett sérülékenységeket) használják ki arra, hogy megfertőzzék számítógépét vagy egyéb eszközeit. Minél naprakészebb egy szoftver, annál kevesebb ismert sérülékenység található benne, és annál nehezebb a számítógépes bűnözők számára, hogy megfertőzzék. Ezért győződjön meg arról, hogy számítógépe operációs rendszere, alkalmazásai és egyéb eszközei számára engedélyezett az automatikus frissítés.

- **Víruskereső engedélyezése**: Használjon megbízható gyártótól származó, naprakész víruskereső szoftvert. Ezeket az eszközöket a rosszindulatú programok észlelésére és megállítására tervezték. A vírusirtó azonban nem képes blokkolni vagy eltávolítani az összes rosszindulatú programot, és általában nem tudja helyreállítani a fájlokat egy zsarolóvírus fertőzés után. A

számítógépes bűnözők folyamatosan innoválnak, új és kifinomultabb fertőzési taktikákat fejlesztenek ki, amelyek elkerülhetik az észlelést. Ugyanakkor a vírusirtók fejlesztői is folyamatosan frissítik termékeiket a rosszindulatú programok felismerése érdekében. Ez mára sok szempontból egy fegyverkezési versennyé vált, ahol mindkét fél megpróbál túljárni a másik eszén.

- **Legyen éber**: A számítógépes bűnözők gyakran adathalász e-mail támadások révén csapják be az embereket a zsarolóvírusok és egyéb rosszindulatú szoftverek telepítése érdekében. Például egy számítógépes bűnöző olyan e-mailt küldhet Önnek, amely valódinak tűnik és egy csatolmányt vagy hivatkozást tartalmaz. Akár tűnhet úgy is, hogy az e-mail a bankjától vagy egy barátjától származik. Azonban, ha megnyitja a csatolt fájlt vagy rákattint a hivatkozásra, aktiválhatja a számítógépet megfertőző rosszindulatú kódot. Ha egy üzenet a sürgetés érzetét kelti, vagy túl jónak tűnik, hogy igaz legyen, könnyen lehet, hogy az egy támadás. Legyen éber – a kiberbűnözők az érzelmeire is hatni próbálnak. – A józan ész gyakran a legjobb védelem.

Készítsen biztonsági másolatot adatairól, mielőtt azok megfertőződnének.

Mivel nem valószínű, hogy mindig képes lesz megakadályozni a fertőzést, a zsarolóvírusok elleni legjobb védelem a biztonsági mentések készítése. Ha van biztonsági másolata a fontos dokumentumokról és fájlokról, akkor a váltságdíj kifizetése helyett lehetősége van a biztonsági másolatból történő helyreállításra. Fontos, hogy valamilyen automatikus biztonsági mentést használjon, amely rendszeresen készít biztonsági másolatot az összes fájljáról. Tesztelje a visszaállítási eljárásokat, hogy megbizonyosodjon arról, hogy szükség esetén valóban helyre tudja állítani azokat. Számos egyszerű felhőalapú és helyi biztonsági mentési megoldás telepíthető a számítógépére, amely biztonságosan és rendszeresen másolatot készít az Ön fájljairól.

A szerzőről

Lenny Zeltser informatikai vezető az Axoniusnál, egy kiberbiztonsági eszközkezelő társaságnál. Emellett malware-ek elleni védekezést oktat, valamint publikál a SANS Intézetnél. Lenny a Twitteren is aktív: @lennyzeltser és egy biztonsági blog szerzője a zeltser.com-on.

Források

Biztonsági mentések?: https://www.sans.org/security-awareness-training/resources/got-backups
Állítsuk meg az adathalászatot: https://www.sans.org/security-awareness-training/resources/stop-phish
A frissítés ereje: https://www.sans.org/security-awareness-training/resources/power-updating
SANS FOR610 kurzus - Káros kódok visszafejtése: https://sans.org/for610

A fordítást készítette: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI)