Minden, amit a zsarolóvírusokról tudni kell

Elfoglalt. Fáradt. Egyszerűen csak játszani akar a Pokémon Góval vagy hozzá akar férni a céges belső hálózathoz. Akármilyen okból az „Emlékeztessen később” gombra kattint egy szoftverfrissítéskor, sebezhetővé teszi eszközét a zsarolóvírusokkal szemben.

Ez csupán egyike annak a számtalan módszernek, amellyel a zsarolóvírusok beférkőzhetnek a rendszerekbe. A hirdetésekbe rejtett malware, az adathalász e-mailek és az USB-meghajtókon keresztüli kifinomult támadások mind gyakran használt módszerek a célpont rendszereinek feltörésére. Vizsgáljuk meg közelebbről az egyik gyakori forgatókönyvet.

„Emlékeztessen később”

Nem létezik tökéletes szoftver. A fejlesztők rendszeresen felfedeznek hibákat a programokban, emiatt hibajavításokat tesznek közé. Amikor elhalasztjuk a bővítmények vagy alkalmazások frissítését, a támadók könnyedén kihasználhatják az ismert sebezhetőségeket. Az egyik népszerű exploit kit (a kliensoldali sebezhetőségek észlelésére szolgáló szoftver) azt derítette ki, hogy a sikeres támadások 80 százalékáért a Flash felelős. Legyen az a Flash, Silverlight vagy éppen Google Chrome, frissítse rendszeresen és telepítse a javítócsomagokat.

Megfertőződött

A fertőzött eszköz segítségével a zsarolóvírus átveszi az irányítás a célba vett rendszerek felett. Ezt követően aszimmetrikus kulcscsere használatával titkosítja a fájlokat. Lényegében az történik, hogy a vírus a felhasználó beleegyezése nélkül képes elérhetetlenné tenni annak adatai – és kizárólag a vírus fejlesztője rendelkezik a feloldáshoz szükséges kulccsal. A zsarolóvírusok egyes fajtái a hálózaton keresztül is terjednek. A biztonsági szakértők előrejelzése szerint az ilyesfajta önterjedés idővel egyre általánosabbá válik majd.

Zsarolóüzenet jelenik meg

A fertőzés megtörténte után egy üzenet jelenik meg a képernyőn, amelyben a zsarolók követelik, hogy bitcoinokban fizessen váltságdíjat az adatokért. A váltságdíj összege jellemzően 200 és 10 000 dollár közé esik, de egyes intézmények ennél sokkal magasabb árat kénytelenek fizetni. Egy kaliforniai kórház 17 000 dollárt volt kénytelen kicsengetni az adataiért cserébe. Ugyanis minden egyes nap, ameddig nem fértek hozzá az adataikhoz, 100 000 dollárjukba került.

A biztonsági szakértők azt javasolják, hogy ne fizessen váltságdíjat. A zsarolóvírusok egyes típusai vagy nem tudják feloldani a fájljai titkosítását, vagy automatikusan megsemmisítik azokat. A Talos fenyegetéseket vizsgáló kutatói arra jutottak, hogy ezek a rosszindulatú, mindent megsemmisítő zsarolóvírusok egyre elterjedtebbé válnak. A 2016 Midyear Security Report című biztonsági jelentésünkben a kutatók arra hívták fel a figyelmet, hogy a zsarolóvírusok tekintetében egyre inkább aggodalomra ad okot az adatintegritás kérdése. A támadók megbízhatatlanok abban a tekintetben, hogy megőrzik az általuk titkosított adatok integritását, és például a meghamisított orvosi vagy mérnöki adatok hatalmas károkat okozhatnak.

Ráadásul a váltságdíj megfizetésével bűnügyi szervezetet támogatunk. Ameddig ezek a bűnszervezetek pénzt keresnek az ilyen támadásokkal, addig a zsarolóvírusok újabb és újabb változataival fognak előállni.

Hogyan állítsa meg a zsarolóvírusokat?

A zsarolóvírusok támadására a legjobban réteges biztonsági megközelítés alkalmazásával lehet felkészülni.

Támadás előtt

Többféle egyszerű módszerrel erősítheti a védelmet. A biztonság kedvéért érdemes megfontolni egy katasztrófa-elhárítási partner igénybe vételét, hogy az üzletmenet folytonossága a legrosszabb bekövetkezése esetén is fennmaradjon. Azonban ennél egyszerűbb intézkedések is léteznek. Fontos adatainak védelme érdekében rendszeresen készítsen biztonsági mentést a fájljairól. Telepítsen reklámblokkoló alkalmazásokat, és amikor a szoftverek jelzik, mindig frissítse azokat.

A reklámblokkolók önmagukban nem képesek az összes rosszindulatú hirdetést észlelni és blokkolni, illetve a kártékony linkeket azonosítani. Fontolja meg a kevesebb mint 5 perc alatt telepíthető Cisco® Umbrella használatát. Az alkalmazás észleli a rosszindulatú oldalakat, és hoszt-szinten blokkolja a kéréseket.

Támadás alatt

Az Umbrella használatával a zsarolóvírus-fájlok döntő többsége a DNS-rétegnél megállítható, mielőtt azok elérnék a végfelhasználói eszközöket. A legkiválóbb óvintézkedések megtétele mellett sem létezik olyan módszer, amely teljes körű védelmet nyújt a zsarolóvírusok ellen.

Látni kell, hogy mi történik a hálózaton, és a támadásokat azok bekövetkezésekor kell tudni azonosítani. A Cisco Stealthwatch™ fenyegetésészlelő a hálózati forgalmat figyeli és látja, ha valami rendellenes – például egy zsarolóvírus okozta támadás – történik, és riasztást ad ki a rendszert érő támadásról.

Minden, amit a zsarolóvírusokról tudni kell

Amikor a fájl megpróbálja futtatni önmagát, a Cisco hatékony eszközökkel állítja meg:

- Az Umbrella azáltal védi a rendszert, hogy blokkolja a vírusos fájl titkosítási kulcsot tartalmazó infrastruktúrának küldött kéréseit. Ez azt jelenti, hogy a zsarolóvírus nem képes kommunikálni, és nem kapja meg az adatok titkosításához szükséges információt.
- Amikor az Umbrella blokkolja a kérést, a Cisco következő generációs tűzfala a kapcsolat blokkolásával biztosítja az extravédelmet.
- Ha egy fájl túljut a DNS-rétegen és a tűzfalon is, a Cisco Advanced Malware Protection (AMP) for Endpoints megoldása blokkolja a fájl futtatását, majd egy lépéssel még tovább megy. Folyamatosan elemzi a rendszeren belüli összes fájlaktivitást, így lehetőséget ad az összes rosszindulatú fájl felkutatására és eltávolítására.

Támadás után

Ha a zsarolóvírus már megfertőzte a rendszert, fel kell mérni a kárt és meg kell akadályozni a továbbterjedést. Az AMP megakadályozza az ismert rosszindulatú fájlok futtatását, és eltávolítja azokat a végpontokról.

Azt megakadályozandó, hogy a zsarolóvírusok elterjedjenek a vállalati hálózaton, a Cisco TrustSec® technológiával végrehajtott dinamikus szegmentáció segítségével beazonosítható, hogy a hálózat mely részeit érte el az adott zsarolóvírus, és megállítható a terjedése.

Szeretne bővebb információkhoz jutni? Látogasson el a cisco.com/go/ransomware oldalra.

(1110R) C11-737870-00 09/16