Kétségtelen, hogy korábban már sok szó esett a WannaCryptor kártevőről (más néven WannaCry vagy WCrypt), azonban sokan azóta is lebecsülik az ezzel kapcsolatos veszélyeket, és nem tettek meg mindent a hatékony megelőzés érdekeben. Az ESET szakemberei összeszedtek néhány érdekességet, amely segíthet a WannaCryptor típusú fenyegetések kivédésében.

Az SMB sebezhetősége

A korábbi beszámolókkal ellentétben a WannaCryptor aktiválásához nem szükséges rosszindulatú linkre vagy csatolmányra kattintani, mert a kártevő az EternalBlue néven ismeretes szoftveres sebezhetőséget kihasználva támad. Az eszközt állítólag az Egyesült Államok Nemzeti Biztonsági Ügynöksége (NSA) fejlesztette ki, de később a Shadow Brokers hackercsapat ellopta és az elsősorban vállalati hálózatokban fájl- és nyomtatómegosztásra használt Microsoft Server Message Block (SMB) program elavult verzióiban található kritikus hibák támadására használták fel.

Az interneten a 445-ös (általában SMB-vel társított) nyitott portok után kutatva, a támadók kihasználták az SMB hibáit, és telepítették a DoublePulsar nevű támadó eszközt, amelyről szintén azt feltételezik, hogy azt az NSA-tól lopták. Ez a hátsó ajtó megnyitotta az utat a fő kártevőnek, amely a feltelepülés és a futtatás után titkosította a fájlokat.

Azt is fontos megjegyezni, hogy a Microsoft már a kártevő globális elterjedése előtt 59 nappal kiadott egy kritikus biztonsági frissítést , illetve jóval a támadás előtt a szoftvergyártó figyelmeztette is a felhasználókat, hogy az SMB első, három évtizede kint levő verziójának (SMBv1) használata sebezhető lehet, emiatt annak használata a továbbiakban nem javasolt. A WannaCryptor rombolása még a hibajavító frissítések telepítése nélkül is elkerülhető lett volna, ha a felhasználók még idejében végrehajtanak néhány alapvető biztonsági beállítást.

Régimódi funkciók, modern tartalom

A WannaCryptor féregszerű funkcionalitása néhány régebbi technológiára emlékeztetett. A biztonsági szakemberek arra számítottak, hogy a zsarolóvírus önterjesztő funkcióval is rendelkezik majd, azonban hasonlóan a régi férgekhez - a Code Red 2001-ben, az SQL Slammer
2003-ban, a Sasser 2004-ben és a

Conficker
2008-ban - a WannaCryptor is a javítatlan, kiszolgáltatott céges hálózatok révén terjedt, olyan sebezhetőségeket kihasználva, amelyekre már régóta rendelkezésre állt a javítás. Azonban a régi típusú kártevőkkel ellentétben most egy olyan zsarolóvírus csapott le a vállalatokra, amely teljesen megbénította a fertőzött gépeket, és a helyi hálózatra vagy az internetre csatlakozó gépekre átterjedve, az SMB hibákat kihasználva követelt váltságdíjat az elkódolt, titkosított adatokért cserébe.

Pénzügyi kudarc

Az ESET egyik szakembere nemrégiben mutatott rá arra, hogy a kártevő üzemeltetői nem tartották be a titkosított fájlok feloldására tett ígéreteket, pedig az áldozatok kifizették a váltságdíjat. A támadók nem is rendelkeztek olyan megoldással, amelynek révén megállapíthatták volna, hogy ki fizetett vagy ki nem, így a titkosítás feloldásához szükséges kódokat sem adhatták oda a megzsarolt felhasználóknak, tehát ezt hamisan ígérték meg.

Elmondható, hogy az akció valójában pénzügyileg kudarc volt a támadók számára, tekintettel a kampány terjedelmére és az okozott kár mértékére. A támadás mintegy 300 000 gépet veszélyeztetett, amelyek mindegyikének elvileg 300 dollárt (három nap után 600 dollárt) kellett volna fizetnie a titkosítást feloldó kulcsért. A WannaCryptorhoz társított három Bitcoin fiók tulajdonosai - eddig ismeretlen módon - július végén és augusztus elején kiürítették a számlájukat, amelyen körülbelül 52 bitcoin (140 000 dollár) volt. Más zsarolóvírussal elkövetett támadások sokkal kevesebb áldozat megfertőzésével is dollármilliókat hoztak a kiberbűnözőknek.

A fenti tények és más furcsaságok ismeretében, a biztonsági szakemberek úgy vélik, hogy a támadást nem a pénzszerzés motiválta, hanem az adatok megsemmisítése, de az is lehet, hogy egy kisebb akció irányítása csúszott ki a bűnözők kezéből.

A 10 dolláros megoldás

A WannaCryptor rombolását Marcus Hutchins, más néven MalwareTech, egy 22 éves angol kártevőelemző felfedezése állította meg. A kutató a kódmintákat vizsgálva észrevett egy sajátosságot: a kártevők megpróbáltak összekapcsolódni egy fura elnevezésű, regisztrálatlan domain címmel.

A szakember elkezdte vizsgálni a domaint, majd 10 dollárért regisztrálta is azt, amely a kutató tudta nélkül a zsarolóvírus végét jelentette: ugyanis amikor a WannaCryptor csatlakozott a már

élő, működő domainhez, akkor a kártevők ahelyett, hogy megkezdték volna a terjedést és a lemezek titkosítását, egyszerűen leálltak, vagyis igazából ez egy titkos leállítási lehetőség volt. Ez kulcsfontosságú volt a WannaCryptor terjedésének lelassításában.

Azonban az ügy még egy fordulatot tartogatott: Hutchinst letartóztatták, és megvádolták a Kronos elnevezésű banki trójai program fejlesztésével és terjesztésével. Később számos gyanús online személlyel való együttműködéssel vádolták meg a szakembert, aki jelenleg is őrizetben várja a tárgyalást, ahol ha a vád bebizonyosodik, akár 40 éves börtönbüntetéssel is sújthatják.