Nemzeti vészhelyzet lett Amerikában egy hekkertámadásból

A több mint tíz államot tüzelőolajjal és üzemanyaggal ellátó Colonial Pipeline múlt pénteken teljesen működésképtelenné vált egy zsarolóvírusos akciót követően.

A magánkézben lévő Colonial Pipeline az Egyesült Államok egyik leghosszabb és legfontosabb olajvezeték-hálózatát üzemelteti. A társaság infrastruktúrája a texasi olajmezőktől egészen New Jersey kikötőjéig szállítja a létfontosságú nyersanyagokat − napi 100 millió gallonnyi mennyiségben. Ennek fényében igencsak komoly aggodalmat keltett, hogy a vállalatot egy kibertámadás pénteken arra kényszerítette, hogy a teljes rendszerét leállítsa.

Befagyott az olaj

A Colonial Pipeline péntek óta többször frissített közleménye szerint május 7-én realizálták, hogy rendszerüket kompromittálták. A kezdetben meglehetősen szűkszavú és homályos tájékoztatást a hétvégén azzal pontosították, hogy megerősítették a zsarolóvírusos támadás tényét. Utóbbi miatt a cég maga állította le a működését biztonsági okokból, mivel vélhetően attól tartottak, hogy a hekkerek akár balesetet is okozó változtatásokat tehetnek a rendszerben.

A cég az illetékes hatóságok és kormányügynökségek értesítése mellett azonnal bevonta a FireEye biztonsági vállalat szakembereit is a nyomozásba, akik a cikk írásakor még javában dolgozhatnak az eset kivizsgálásán. A társaság természetesen hangsúlyozta, hogy mindent megtesz azért, hogy mihamarabb újraindulhasson a normális működés. Ez ottani idő szerint vasárnap estig ugyanakkor nem sok eredménnyel járt, mivel mindössze néhány mellékvezetéken indulhatott újra a szállítás. Arról pedig jelen pillanatban nincs pontos információ, hogy a főbb vonalakon mikor állhat helyre a rendes üzem.

A Colonial Pipeline nem kívánt reagálni azokra a kérdésekre, amelyek azt firtatták, hogy fizettek-e, vagy szándékoznak-e fizetni a zsarolóknak. Az akció mögött egyébként a Reuters a DarkSide elnevezésű csoportot sejti. A csapat bevett módszere, hogy a megfertőzött rendszerekben tárolt adatok titkosítása mellett az információkat magának is lementi, ami további nyomásgyakorlásra ad lehetőséget a „tusztárgyaláskor". A DarkSide emellett arról híres, hogy az illegálisan megszerzett pénz egy részét karitatív célokra fordítják, ezért is emlegetik őket egyfajta 21. századi Robin Hoodként.

A vezetékein fűtőolajat, gépkocsi-üzemanyagot és kerozint is szállító társaság leállása a jelek szerint egyelőre nem rengette meg az ország ellátását, köszönhetően a helyi tárolókban meglévő bőséges készleteknek. Amennyiben azonban hosszabb távra kiesne a rendszerből ez a lehetőség, az komolyabb problémákhoz, ellátási gondokhoz és abnormális ármozgáshoz vezethet. Az ügy súlyosságát jelzi, hogy *Joe Biden* elnököt a hétvégén részletesen tájékoztatták a támadásról, vala-

mint az is, hogy a közlekedés biztonságáért felelős kormányzati szerv vasárnap különleges vészhelyzeti engedélyt adott közel húsz államban veszélyes üzemanyagok közúti szállítására.

Divatba jött a zsarolás

A zsarolóprogramok az elmúlt néhány év alatt a digitális gazdaság egyik legnagyobb problémájává váltak. A statisztikák szerint a bűnözők egyre gyakrabban célozzák meg a helyi kormányzati rendszereket, iskolákat vagy egészségügyi intézményeket is, mert ezeken a helyeken nem feltétlenül működnek naprakész kiberbiztonsági protokollok, de a ransomware olyan arányú károkat okozhat nekik, hogy hajlamosabbak lesznek kifizetni a váltságdíjakat. Erre a trendre még jobban ráerősített a tömeges távmunka és az általános bizonytalanság.

Az amerikai igazságügyi minisztériumban nagyjából két héttel ezelőtt hoztak létre egy kifejezetten a zsarolóprogramokkal foglalkozó csoportot, de a központi bankok és a pénzügyi bűncselekményekkel foglalkozó hatóságok már világszerte vizsgálják a potenciális ellenlépések lehetőségeit. Egy 2021 elején létrejött munkacsoport, a Ransomware Task Force (RTF) agresszívabb fellépésre szólított fel a bitcoin és más kriptovaluták tranzakcióinak nyomon követésében, mivel ezek amellett, hogy egyre népszerűbbek a befektetők körében, meghatározó szerepet játszanak az üzleti célú ransomware-tevékenységek vérkeringésében is.

Forrás: https://bitport.hu/nemzeti-veszhelyzet-lett-amerikaban-egy-hekkertamadasbol

Válogatta: Fonyó Istvánné