CTI Jelentés

US Colonial Pipeline elleni támadás következményei

1996
NEMZETBIZTONSÁGI SZAKSZOLGÁLAT
Fortes fortuna adiuvat

NEMZETI
KIBERVÉDELMI INTÉZET

Tartalomjegyzék

Bevezetés	3
US Colonial Pipeline és a kibertámadás	4
A támadás közvetlen hatásai	7
A támadás közvetett hatásai	10

Bevezetés

A technológia folyamatos fejlődésével az infokommunikációs eszközök integrálódása egyre elterjedtebb a kritikus infrastruktúrákban a könnyebb kezelhetőség, monitorozás és reakcióképesség növelése érdekében. Az átlag polgári élet függősége ezen infrastruktúrák folyamatos elérhetőségétől veszélyesen erős. Már több regény és mozifilm bemutatta mi történne, ha ezen szolgáltatásokban kiesés történne. Sajnos, sok esetben a valóság még ijesztőbb, mint a fikció. A társadalom tagjainak mindennapjait támogató kritikus infrastruktúrák folyamatosan célkeresztben vannak ellenséges kormányok vagy kiberbűnözői csoportok által.

US Colonial Pipeline és a kibertámadás

A Colonial Pipeline az Egysült Államok egyik legnagyobb üzemanyag elosztó vállalata, amit 1961-ben alapítottak. Naponta kb. 2.5 millió hordónyi üzemanyagot szállítanak le a Mexikói-öbölből a Keleti-part egész területére, amelynek üzemanyagszükségletének 45%-át kiszolgálja. A vezetékrendszer 13 államon, 8850 kilométeren keresztül húzódik. A Colonial csővezetékeire támaszkodik ezenkívül megannyi benzinkút, repülőtér és katonai bázis, amelyek mind az állami és mind a civil élet alapvető részét képezik.

2021. május 6-án a Colonial kibertámadásra lett figyelmes, amikor 100 GB-nyi adatellopását és rendszerfájlok titkosítását fedezték fel. A feloldásért az akkori árfolyamon 4,3 millió dollár körüli értékű bitcoin kriptovaluta váltságdíjat követeltek a támadók.

A Colonial Pipeline az Egysült Államok egyik legnagyobb üzemanyag elosztó vállalata, amit 1961-ben alapítottak. Naponta kb. 2.5 millió hordónyi üzemanyagot szállítanak le a Mexikói-öbölből a Keleti-part egész területére, amelynek üzemanyagszükségletének 45%-át kiszolgálja. A vezetékrendszer 13 államon, 8850 kilométeren keresztül húzódik. A Colonial csővezetékeire támaszkodik ezenkívül megannyi benzinkút, repülőtér és katonai bázis, amelyek mind az állami és mind a civil élet alapvető részét képezik.

2021. május 6-án a Colonial kibertámadásra lett figyelmes, amikor 100 GB-nyi adat ellopását és rendszerfájlok titkosítását fedezték fel. A feloldásért az akkori árfolyamon 4,3 millió dollár körüli értékű bitcoin kriptovaluta váltságdíjat követeltek a támadók. Ahhoz, hogy a további káreseteket megelőzzék a vállalat május 7-én publikusan bejelentette, hogy vezetékeiket lezárják és az üzemanyagszállítást kamion konvojokon folyatják, amíg nem tisztázódik az incidens és annak háttere. A támadás alapját egy szofisztikált távoli elérhetőségű ransomware (Remote Access Ransomware) adta, amit az erre szakosodott kiberbűnözői csoport a Darkside vitt végbe. A Colonial vállalat kifizette a követelt váltságdíjat egy kelet európai bitcoin tárca felé.

Az incidens TTP (tactics, techniques, and procedures) részleteiről a hatóságoktól hivatalos jelentés nem készült azonban egy kongresszusi meghallgatás során Charles Carmakal a FireEye Mandiant cég vezető alelnöke megerősítette, hogy egy kiszivárgott VPN jelszóval jutottak be a támadók a hálózatra. A jelszó egy már inaktív felhasználóhoz tartozott aki feltehetően megegyező autentikációs információkat használt más szolgáltatásokhoz is.

A vállalat - biztonsági protokollja szerint - gyors reagálás keretében értesítette a hivatalos szerveket, (FBI, NSA, CISA) és felkértek ezenkívül egy privát céget a FireEye-t, hogy segédkezzenek a kialakult helyzet megoldásában. A CISA (Cybersecurity and Infrastructure Security Agency) és az FBI (Federal Bureau of Investigation) kiadott egy figyelmeztetést a kritikus infrastruktúrák üzemeltetőinek a Darkside ransomware által fennálló veszélyhelyzet miatt, mivel a csoport RaaS (Ransomware as a Service) azaz zsarovírust, mint szolgáltatásnyújtást biztosít más kiberbűnözőknek.

Május 10-én offline, a 4-es vonal manuális visszaállítása sikeresen megtörtént, további vonalak azonban lezárva maradtak. Végül a Colonial május 12-én elkezdte az üzembehelyezési terv szerint visszaállítani az üzemanyag szállítást, csökkentett üzemmódban, viszont még így is körülbelül 2 hétbe telt, amíg a teljes vonalon megjelenik ennek a hatása.

Június 7-én a Szövetségi Igazságügyi Minisztérium bejelentette, hogy a váltságdíj nagy részét, 75-ből 63,7 bitcoint sikeresen visszanyertek. Az FBI a kezdetektől nyomon követte az összeg tranzakcióit, ami legalább 23 digitális címet foglalt magába. A végcím privát kulcsát az FBI megszerezte, aminek segítségével jogi úton engedélyezve feltörték a számlát és visszatulajdonították a váltságdíjból származó 63,7 bitcoint.

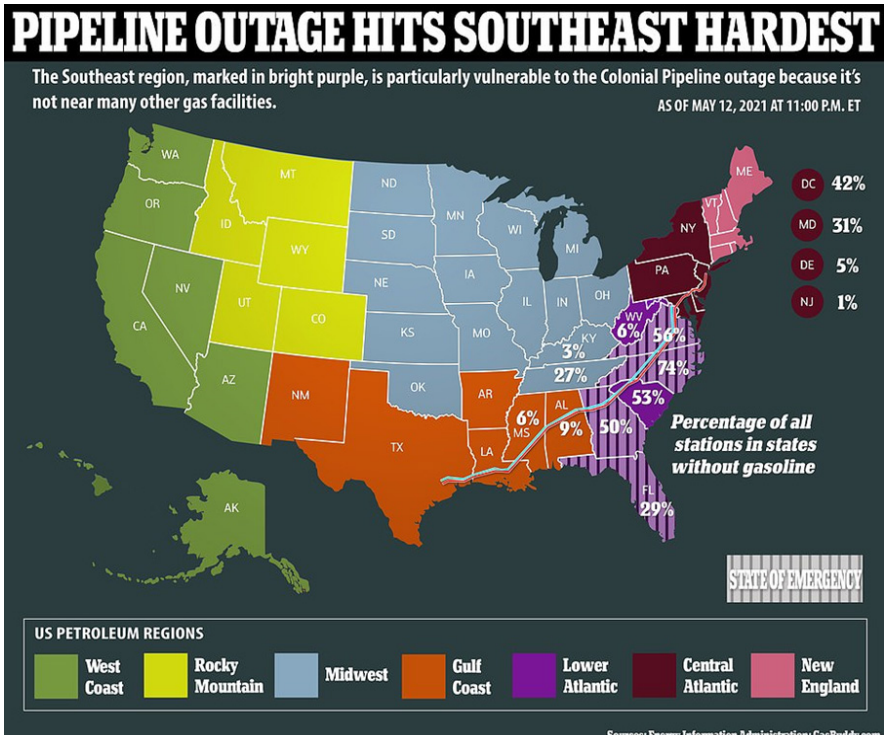
Mindez természetesen kihatással volt az üzemanyag piaci értékére, és további növekedést idézett elő az árakban is. A július 12-i hétre az üzemanyag elérte a 85 cent/liter körüli értéket, hiába állt vissza a termelés és a szállítás a Colonial hálózatán. Az érintett államok benzinkútjain az összeg növekedés még drasztikusabbá vált. Ezek sok esetben elérték az 1,84 dollár/liter-es pontot is.

A támadás közvetlen hatásai

Az előzőekben ismertetett incidens technikai szempontból nem nevezhető, se egy szolgáltatás-megtagadásos (DoS) támadásnak, sem egy káoszt keltő OT (Operational Technology) támadásnak, mivel nem a csővezetékek lezárása volt a támadók célja. A szolgáltatások leállítása és a csővezetékek lezárása a további kármegelőzéssel járó folyamat részét képezték a Colonial vállalat részéről. A Colonial azért is döntött ezen megoldás mellett, mivel az üzemanyag folyamatos leszállítását a Keleti-part felé folytatni tudták tanker teherszállító járművek segítségével. A lezárástól, a május 12-i részleges feloldásig kb. 1,3 millió hordó üzemanyagot sikerült leszállítani. Ugyan ez csak a hányada a napi szintű szállítás mennyiségének, viszont a normál felhasználást ki tudta volna szolgálni. Azonban a publikum felé tett sajtóbejelentések futótűzként terjedtek és hatalmas pánikot keltettek a társadalomban, amivel egy üzemanyag felvásárlási láncreakció jött létre.

Feltehetően a Covid-19 pandémiás helyzet hatásai miatt, 2020 novembere óta folyamatosan emelkedő amerikai üzemanyagárak május 10-én 80 cent/liter körüli átlagértéken tetőztek, amely egy alapvető frusztrációt váltott ki az emberekből. A Colonial által tett sajtóbejelentés után pánikszerű módon tömeges üzemanyagfelvásárlás indult meg. Több hírportál és közösségi média platformján megjelentek képek, ahol emberek petrolkémiai termékek tárolására nem alkalmas tárolókba szállították el az üzemanyagot, mint például esővízgyűjtő hordó, duplarétegű szemeteszsák és nyitott vödrök.

Ebből adódóan a keleti-parti államok sok benzinkútjáról készlethiányt jelentettek. Ez legfőképp Észak és Dél-Karolinára volt jellemző, ahol az üzemanyagkifogyás által sújtott benzinkutak száma a teljes államban elérte a 74%-ot is. Több helyről a vásárlók közötti inzultációkról és verekedésekről számoltak be a források.



A Colonial rendszerleállításból származó üzemanyaghiánytól szenvedő benzinkutak százalékos száma 2021. május 12-én az Egyesült Államok Keleti-partján. Forrás: Daily Mail

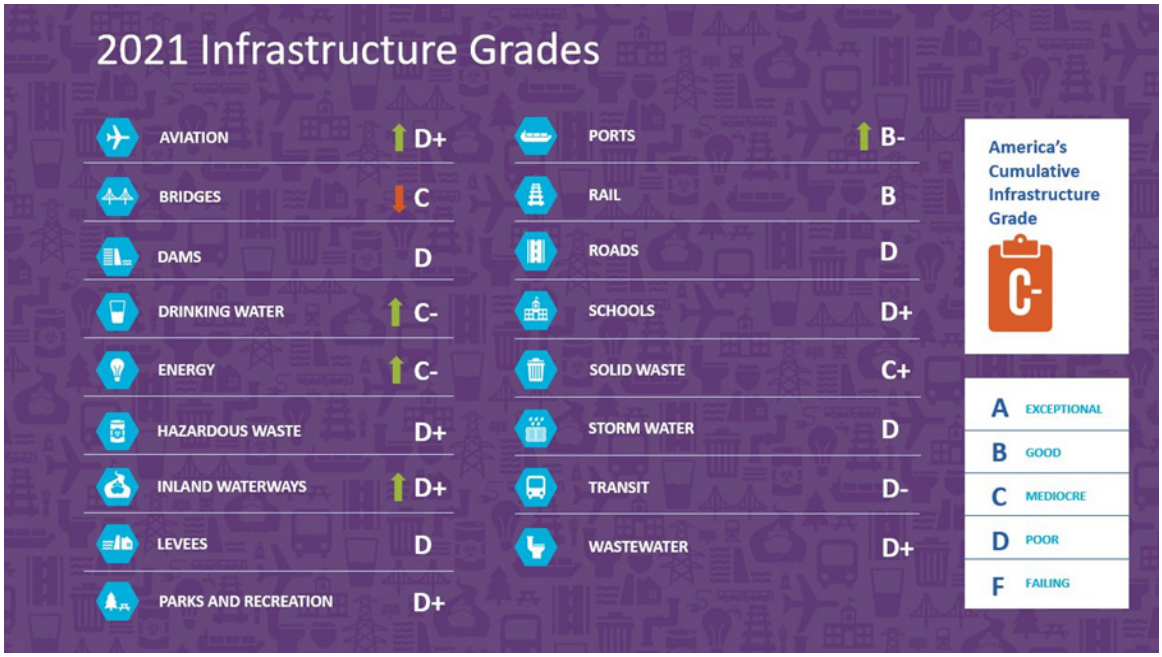
Mindez természetesen kihatással volt az üzemanyag piaci értékére is, és további növekedést idézett elő az árakban. A július 12-i hétre elérte a 85 cent/liter körüli értéket, hiába állt vissza a termelés és a szállítás a Colonial hálózatán. Az érintett államok benzinkútjain az összeg növekedés még drasztikusabbá vált. Ezek sok esetben elérték az 1,84 dollár/liter-es pontot.

Az Egyesült Államok összesített átlag üzemanyagár (dollár per liter) változása.


Pump operation: Follow instructions on screen
We are currently out of _____
Due to the Colonial Pipeline shutdown, *Circle K* is working with limited fuel supply in many areas. During this time, we are experiencing fuel outages in some stores.
Circle K is continually assessing the fuel situation and working hard to get our fuel supply to full capacity, to all our stores, as soon as possible. We apologize for the inconvenience.
Verifone
YES
NO
CANCEL
HELP
Insert chip card

A támadás közvetett hatásai

Az Egyesült Államokban alapvető probléma az infrastruktúrák modernizálása, és sok esetben a megfelelő módú funkcionálás is. Például, a ma használatban lévő elektromos szolgáltató telephelyek többsége, az 1960-as évek óta nem esett át komolyabb fejlesztésen, ezért az utóbbi években 3-szor több áramszolgáltatás kiesés tapasztalható, mint 1984-ben. Az „American Society of Civil Engineers" csoport 2021-es kiadványában „C-"-re értékelte összességében az amerikai infrastruktúrákat, ami ugyan javulás a 4 évvel korábbi „D+"-ról, viszont még mindig panasszal illetik a helyzetet.



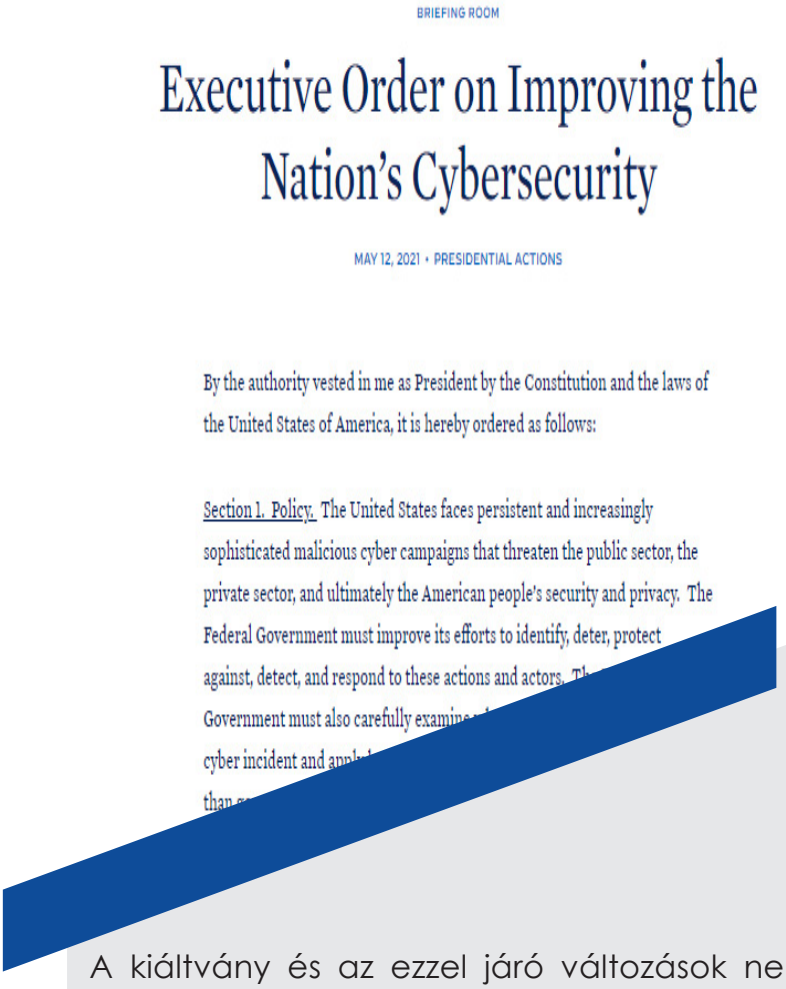
Az American Society of Civil Engineers által kiadott 2021-es értékelés infrastruktúra kategóriákra bontva. Forrás: ASCE's 2021 Infrastructure Report Card

Ezzel párhuzamosan a kiberbiztonság terén is tapasztalható egy fajta lemaradás az amerikai infrastruktúrában, miközben a biztonsági incidensek száma növekszik, és a fenti ransomware támadásból is jól láthatóan a támadók egyre kritikusabb célpontokat érnek el. A Colonial incidens mellett az utóbbi időkben történt még a floridai Oldsmar városi víztisztító üzemét érő hacker támadás, és a Texas államon végig söprő tartós áramszolgáltatás hiány az elavult eszközöket meghibásító erős természeti behatások miatt. Ezen események, és az infrastruktúra állapotának tükrében feltétlen szükséges az átfogó változás.

Május 12-én az Egyesült Államok elnöke Joe Biden kihirdette az Executive Order végrehajtási kiadványát „Executive Order on Improving the Nation's Cybersecurity" címen, részben reagálva a 6 nappal azelőtti Colonial incidensre.

A kiáltvány 5 fő témát céloz meg:

- A fenyegetettségi információk könnyebb megosztása.
- A Software Bills of Material és Zero Trust Architecture megközelítések felé átvezetni a szövetségi kiberbiztonsági infrastruktúrákat, ezzel modernizálva azokat.
- Létrehozni a publikus és privát szervezeteket megcélzó Cyber Safety Review Board-ot az incidensek kivizsgálására és az azutáni biztonsági javítás ajánlások készítésére.
- Sérülékenységek és incidensek észrevételének javítása szövetségi állami hálózatokon.
- A National Security Systems biztonsági követelményeinek további kibővítése .



BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. Th
Government must also carefully examin
cyber incident and appl
than

A kiáltvány és az ezzel járó változások nem csupán az állami informatikai rendszerek biztonságát reméli fejleszteni, de a magánszektorban elhelyezkedő szereplőkét is. Emellett, Joe Biden „American Job Plan" javaslata, – amely a Kongresszus előtt áll megszavazásra – ugyan csak nagy hangsúlyt fektetne a kritikus infrastruktúrák modernizációja és valószínűsíthetőleg összhangban lesz az előbb említett Executive Order-rel.

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2022