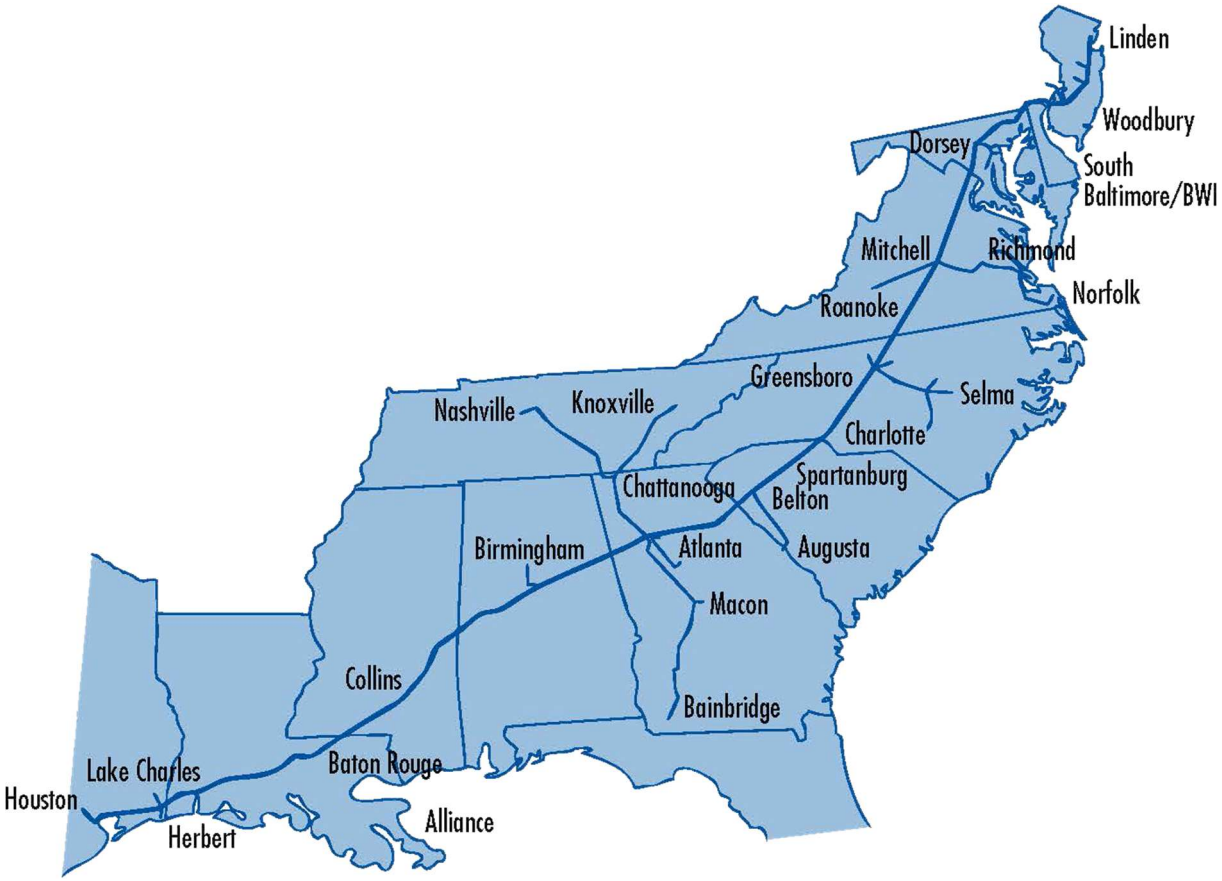
Mit üzen a Colonial Pipeline elleni hacker támadás?

Ahogy pénteken a hazai sajtóban is megjelent kibertámadás miatt ideiglenesen leállították az Egyesült Államok legnagyobb, finomított kőolajszármazékokat szállító vezetékhálózatának egyes részeit, mivel kibertámadás érte az azt üzemeltető Colonial Pipelinet. A támadást a - valószínűleg orosz hátterű -, DarkSide nevű csoport követte el, amely az elmúlt hónapokban több hasonló esetért is felelős. A csoport, miután bejutott egy szervezethez, először lemásol minden használható adatot, majd titkosítja az összes elérhető számítógépet és csak egy nagyobb összeg (a Colonial Pipeline esetén 2 millió dollár) fejében hajlandó feloldani a zárat, miközben azzal fenyegeti az áldozatot, hogy az adatokat nyilvánosságra hozza.

A szóban forgó kőolajvezeték, Texastól egészen New Jersey államig húzódik és a keleti parti szállítások közel 40%-ért felel (ez a teljes amerikai piac 15-20%-a). A vállalat néhány nagy reptér (így a világon második legnagyobb utasforgalmat lebonyolító atlantai és tizenyolcadik charlottei), ipari komplexumok és katonai létesítmények legnagyobb kőolajszármazék szállítója, így a támadás érthető módon fájdalmasan érintette az amerikai üzleti világot.

A zsarolóvírusok és kibertámadások világában nincs olyan, hogy túl nagy célpont.



Digitális vadnyugat

A média és a közbeszéd az ilyen és ehhez hasonló kibertámadások kapcsán hajlamos az érthető elemekre koncentrálni: bűnözők zárolták a szervezet adatait és pénzt követelnek a visszaállításukért. Ez egy klasszikus, könnyen érthető minta: hasonló egy vonatrabláshoz, banki túszejtéshez vagy egy

repülőgép eltérítéséhez. Az üzem leállása természetesen fájdalmas és a kár, a Colonial esetén, naponta valószínűleg millió dolláros nagyságrendű.

Sokkal nehezebben értelmezhető az ilyen támadások másik eleme, az adatlopás. Végső soron nem tűnik el semmi, minden adat visszaállítható néhány órás, legrosszabb esetben napos biztonsági mentésekből. A sajtóban manapság naponta közül különböző adatlopásos eseteket, holott a többségük nyilvánosságra sem kerül, a világ mégis megy tovább. Hol itt a gond?

A gond, mint rendesen, a következményekkel van. A digitális világban, ami egyszer kikerült egy szervezet birtokából, az semmilyen módon nem szerezhető vissza és egyfajta multiplikátor hatás révén a jövőben növeli mind a támadások kockázatát, mind azok hatását és lehetséges kiterjedtségét is. Ha úgy tetszik a ma kibertámadásai jelentős részben a múlt hibáiból táplálkoznak. Egy kibertámadás a jövőben más szervezetek vagy magánszemélyek százait teheti védtelenné, vagy kényszerítheti őket ellenlépésekre (pl. a jelszavaik vagy igazolványaik lecserélése, biztosítások vagy szoftverek beszerzése).

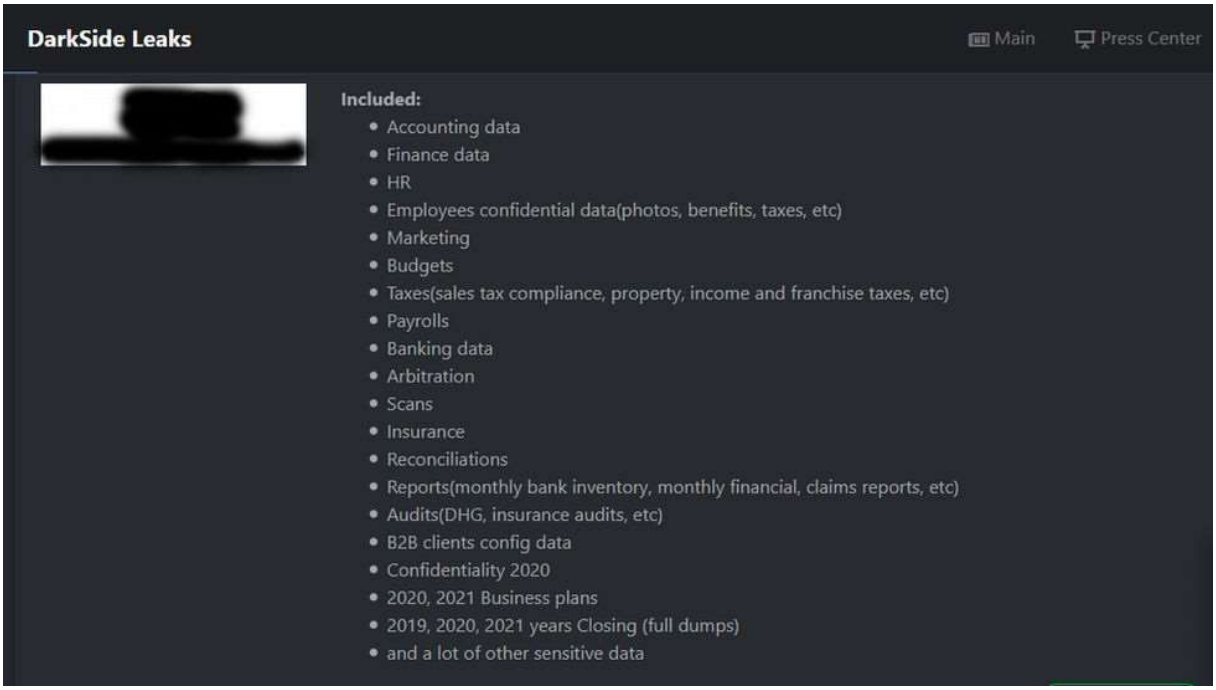
A zsákmány

A Colonial Pipeline kapcsán a világsajtó a zsarolóvírustámadásra koncentrált, holott legalább annyira zavarba ejtő az adatlopás, amelyet a nyomozásban résztvevők is megerősítettek és amelyről a hackercsoport is közleményt adott ki. A DarkSide-hoz hasonló csoportok módszere, hogy miután bejutottak egy rendszerbe lemásolnak mindent, ami akár csak kicsit is értékesnek tűnik: valamennyi kompromittált számítógép összes elérhető jelszavát (így a böngészőben tároltakat is) és szervezetenként eltérő adattömeget (üzleti állományokat, levelezéseket, adatbázisokat, fotókat, gyakorlatilag bármit, amit találnak). Ezt követően az adatok az esetleges megrendelőhöz kerülnek (ha van), majd előbb-utóbb a feketepiacra: a belépési azonosítók a százmilliós jelszóadatbázisokat gazdagítják, amelyeket néhány száz dollárért bárki megvásárolhat és amelyek közül néhányról utóbb tudomást szerez a közvélemény.

A DarkSide közleményben hozta nyilvánosságra milyen típusú adatok kerültek hozzájuk. Gondoljunk csak bele milyen érték kerülhet most a támadás esetleg megrendelőihez vagy az állományok későbbi megvásárlóihoz!

- A vállalat szállításainak teljes listája, köztük a hadászati célúak is, amelyből következtetni lehet csapatmozgásokra, az egyes állomáshelyek technikai felszereltségére és egy sor más dologra
- Pénzügyi és béradatok, amelyek nyilvánosságra kerülve bérfeszültséget okozhatnak vagy kiszolgáltathatnak munkavállalókat
- Karbantartási adatok, melyekből következtetni lehet a rosszul karbantartott vagy sérülékeny vezetékrészekre. A Colonial Pipelinenak, - saját bevallásuk szerint is kihívást jelent a több tízéves vezetékrendszer karbantartása - tavaly nyáron öt napjába telt, hogy elhárítsa az Egyesült Államok legnagyobb ilyen jellegű szárazföldi katasztrófáját, melynek során 4,5 millió liter kőolajszármazék ömlött Huntersville mellett a természetbe
- A munkatársak személyes adatai, amelyek később felhasználhatóak személyiséglopáshoz, zsaroláshoz (pl. betegségeken vagy személyes tragédiákon keresztül), reputációromboláshoz

A kikerült adattömeg visszaszerzése nem lehetséges. Ha a vállalat nem fizet, akkor a hackerek elvben kiszivárogtatják majd az adatokat, a gyakorlatban azonban ez nagyon ritkán valósul meg, sok esetben amiatt, mert a cégek inkább kifizetik a kért összeget. Az ellopott adatok azonban már kikerültek és ezen nem lehetséges változtatni. A hackerek az ellopott adatokból annyi alkalommal igyekeznek majd hasznot húzni, ahányszor lehetséges. Az adatok többszörözhetőek, és kizárólag az idő vagy más körülmény általi relevanciavesztésük teheti őket értéktelenné és így többé-kevésbé veszélytelenné.



A következmények

Hétfőn, amikor ez a cikk megjelenik, a Colonial Pipeline működése még nem állt helyre. A Biden adminisztráció vasárnap vészhelyzeti rendelkezést adott ki, amely engedélyezi, hogy a kőolajszármazék szállításban résztvevő sofőrök, az érintett államokban többet dolgozzanak az egyébként megengedettnél az szállítás zavartalanságának biztosítása érdekében. Az Brent olaj és egy sor más termék ára megugrott ahogy az érintettek igyekeznek más forrásból pótolni a kiesést. Iparági szakértők arra figyelmeztetnek, hogy amennyiben rövid időn belül nem áll helyre a szállítás, komoly fennakadások lehetnek a keleti államok energiaellátásában.

Mit tehet egy a szervezet a saját biztonságáért?

Az információbiztonságban az optimális megoldás szinte minden esetben a megelőzés. A robosztus rendszerek, megfelelően konfigurált hálózati védelmi eszközök, jól informált és veszélyekre figyelő munkatársak egy szervezet immunrendszerét jelentik a digitális világban; egy betegséget sokkal könnyebb egyáltalán nem elkapni, mint megpróbálni meggyógyulni belőle és javítani a károkat, amelyeket okozott.

1. A **megfelelően telepített és konfigurált hálózati- és hálózati védelmi eszközök** a kibertámadások elleni védekezés talán legfontosabb eszközei, amelyek nélkül egy modern, felelősségteljes vállalat nem képzelhető el.

2. A **szoftverfrissítések telepítése** a már ismert sérülékenységek befoltozásának legjobb módja. A kibertámadások jelentős része ismert és régóta fennálló sérülékenységeket használ ki a kezdeti lépésekhez.
3. Az **adathordozók titkosítása és a kulcsok biztonságos tárolása** az adatlopás elleni védekezés talán legolcsóbb eszköze.
4. Egy **naprakész üzletmenetfolytonossági terv** segíthet csökkenteni a kibertámadások okozta károkat és gyorsan visszaállítani a vállalat normál működését.
5. A **munkavállók képzése**, a virtuális tér veszélyeivel szembeni felkészültségük növelése a szervezetek digitális immunrendszerének fontos eleme. Az emberi hiba lehetősége a legjobban finanszírozott és működtetett információbiztonsági rendszer technológiáját is képes lehet kiszolgáltatni.

Nagy Demeter Viktor

Szenior tanácsadó

ABT Hungária Tanácsadó Kft.