Anàlisi d'un incident de ciberseguretat industrial

Colonial Pipeline

Firma digital: HAMZA EL HADDAD SABRI - DNI 39957159H

Digitally signed by HAMZA EL HADDAD SABRI - DNI 39957159H
Date: 2024.11.10 17:48:05 +01'00'

Alumne: Hamza El Haddad Sabri

Data: 10/10/24 - 10/11/24

---

1. Índex

2. Resum Executiu

Aquest treball analitza l'atac de ransomware que va afectar a Colonial Pipeline el maig de 2021, una empresa clau en el subministrament de combustible als Estats Units. L'atac va ser realitzat per un grup de hackers anomenat DarkSide, que va aconseguir accedir als sistemes de l'empresa i mitjançant un ransomware els va bloquejar, demanant així un rescat. Com a conseqüència, es va haver de tancar la principal xarxa de distribució de combustible, cosa que va provocar escassetat i pujada de preus en algunes zones del país.

En aquest treball, s'explica com va passar l'atac, quines debilitats va aprofitar el grup DarkSide i quins errors de seguretat hi havia en els sistemes de l'empresa. També es descriu com va reaccionar l'empresa, incloent-hi el pagament del rescat, i les accions que el govern va prendre després per millorar la protecció d'infraestructures crítiques.

3. Paraules Clau

Ransomware, Colonial Pipeline, Ciberseguretat, DarkSide, Atac informàtic, Resposta a incidents, Pagament de rescat, Vulnerabilitats, Ciberatac, Seguretat informàtica, Malware, Cibercriminalitat, Criptografia, Política de seguretat, Conseqüències econòmiques, Subministrament energètic, Protecció d'infraestructures, Enginyeria social, Protocol de seguretat.

4. Objectiu del Treball

L'objectiu d'aquest treball és analitzar l'atac de ransomware que va afectar Colonial Pipeline el 2021, tenint en compte els factors que van permetre l'incident, les seves conseqüències i les respostes adoptades per l'empresa i el govern. Aquest treball pretén identificar les vulnerabilitats de seguretat que van ser explotades, descriure les conseqüències de l'atac en termes econòmics i socials, i destacar les lliçons apreses que ens poden ajudar a millorar la ciberseguretat en infraestructures essencials.

5. Introducció i Posada en Context

Colonial Pipeline és una de les empreses més importants en el subministrament de combustibles com la gasolina, dièsel, querosè entre altres per als Estats Units. Aquesta infraestructura és considerada crítica, ja que proveeix gairebé el 45% del subministrament de combustible del país. A causa de la seva rellevància per al funcionament econòmic i social de la regió, la seguretat de Colonial Pipeline és una prioritat tant per a l'empresa com per a les autoritats.

El maig de 2021, Colonial Pipeline va patir un atac de ransomware per part del grup de cibercriminals conegut com a DarkSide. Aquest grup va aconseguir accedir als sistemes informàtics de l'empresa i va encriptar dades importants, impedint el funcionament normal de la xarxa de distribució de combustibles. Com a resposta, l'empresa va decidir tancar temporalment les seves operacions per prevenir la propagació del malware, fet que va generar una crisi de subministrament de combustibles que va impactar diversos estats dels Estats Units. La situació va portar a una pujada en els preus dels combustibles, provocant que el govern hagues de intervenir per gestionar la crisi.

6. Descripció tècnica de l'Incident

L'atac de ransomware a Colonial Pipeline es va caracteritzar per l'ús d'un malware de xifratge o també anomenat ransomware, creat pel grup DarkSide. Aquest programari maliciós es va infiltrar a la xarxa de l'empresa a través de punts vulnerables en els sistemes d'accés remot.

Una vegada dins la xarxa, el ransomware es va propagar ràpidament gràcies a una manca de segmentació en la infraestructura de Colonial Pipeline. Aquesta deficiència en la divisió de xarxes va permetre que el malware afectés diferents àrees crítiques. Per evitar més danys, l'empresa va decidir aturar temporalment les operacions.

Els responsables de l'atac, el grup DarkSide, van aplicar tècniques d'enginyeria social i van aprofitar vulnerabilitats conegudes en els sistemes de seguretat per obtenir accés inicial als sistemes.

6.1-Actius afectats

L'atac de ransomware a Colonial Pipeline va comprometre diversos actius crítics, la majoria dels quals eren essencials per a les operacions diàries.

Primerament, es van veure afectats pel ransomware els **sistemes operatius de gestió**. Aquests sistemes són responsables de monitorar i controlar el flux de combustible a través de la xarxa de canonades de l'empresa i quan el ransomware va encriptar els fitxers en aquests sistemes, es va perdre la capacitat de supervisió en temps real de les operacions, això va ser un dels principals factors que va forçar a Colonial Pipeline a interrompre el flux de combustible per evitar riscos majors, ja que no era possible garantir la seguretat de les operacions sense aquest monitoratge constant.

Els **sistemes de facturació i administració** també van ser compromesos durant l'atac. Aquests sistemes gestionen les transaccions financeres de l'empresa, incloent-hi la facturació als clients i altres processos administratius essencials. La interrupció d'aquests sistemes va impedir el processament correcte de les transaccions, creant problemes en la cadena de pagaments i afectant la capacitat de l'empresa per gestionar les operacions comercials. Això va augmentar la pressió sobre l'empresa per resoldre l'incident el més ràpidament possible.

A més, la **xarxa interna de comunicació** de l'empresa va ser seriosament compromesa. La propagació del ransomware dins de la xarxa interna va limitar l'accés als recursos compartits i va dificultar les comunicacions entre diferents departaments. Aquesta limitació en les comunicacions va complicar la resposta coordinada a l'incident, fent que l'empresa trigués més a reaccionar i a posar en marxa un pla efectiu per contenir l'amenaça.

6.2-Tipus d’Atac i Mètode

L'atac a Colonial Pipeline va ser un cas emblemàtic de ransomware, dut a terme pel grup de cibercriminals conegut com **DarkSide**. Aquest grup utilitza ransomware, infiltrant-se en les xarxes d'empreses per encriptar fitxers crítics i bloquejar l'accés a sistemes essencials fins que es compleixi un rescat. Segons la *Cybersecurity and Infrastructure Security Agency (CISA)*, el ransomware és una de les amenaces més greus per a infraestructures crítiques, com es va demostrar en aquest atac.

L'infiltració inicial a la xarxa de Colonial Pipeline es va dur a terme aprofitant una vulnerabilitat en els sistemes d'accés remot de l'empresa, un problema que, segons *IBM Security*, pot minimitzar-se amb el model de seguretat de confiança zero, que no es va aplicar correctament en aquest cas. Un cop dins de la xarxa, DarkSide va aprofitar la manca de segmentació de la xarxa per propagar el ransomware ràpidament, cosa que va afectar una àmplia gamma de sistemes, incloent-hi operacions, finances, i comunicacions internes.

L'estratègia del grup DarkSide va incloure l’ús d’enginyeria social per obtenir accés als sistemes, i un ransomware sofisticat capaç d'expandir-se automàticament per diverses parts de la xarxa, segons un informe de *MIT Technology Review* (2021). A més, la *Congressional Research Service (CRS)* destaca que el ransomware utilitzat en aquest atac estava dissenyat no només per encriptar dades, sinó també per extreure informació sensible, augmentant la pressió per al pagament del rescat a causa de la potencial publicació de dades.

Aquest tipus d'atac representa un model emergent de ransomware dissenyat per atacar infraestructures crítiques, creant crisis de subministrament a gran escala i pressions econòmiques immediates. Colonial Pipeline, després de veure interrompudes les seves operacions i d'enfrontar-se a una crisi de subministrament, va optar per pagar part del rescat per recuperar l'accés als sistemes i restablir les operacions, segons el *Department of Energy* (2021).

6.3-Vulnerabilitats explotades

L'atac a Colonial Pipeline va ser possible gràcies a diverses vulnerabilitats que el grup DarkSide va aprofitar per accedir als sistemes de l'empresa i executar el ransomware. Aquestes debilitats com ja s'ha explicat abans, es trobaven principalment en els sistemes d'accés remot i en la segmentació de xarxa, factors que van facilitar tant la infiltració inicial com la propagació del ransomware dins de l'organització.

En primer lloc, els sistemes d'**accés remot** de Colonial Pipeline presentaven vulnerabilitats importants. Segons el *Congressional Research Service* (CRS), es creu que DarkSide va aprofitar aquests accessos sense les proteccions necessàries, com ara l'autenticació multifactor, que podria haver bloquejat els intents d'accés no autoritzats. Aquest tipus de vulnerabilitat és comú en moltes empreses i sovint representa una porta d'entrada fàcil per a atacants externs, especialment quan es combina amb contrasenyes febles o reutilitzades.

Una altra vulnerabilitat clau va ser la **manca de segmentació de xarxa** dins de la infraestructura de Colonial Pipeline. La segmentació de xarxa és una pràctica de seguretat essencial per limitar la propagació d'un atac, ja que permet aïllar els sistemes compromesos i reduir l'abast del malware. En aquest cas, la xarxa de Colonial Pipeline no estava adequadament segmentada, cosa que va permetre al ransomware estendre's ràpidament per tota l'organització, afectant sistemes operatius, financers i administratius. Segons la *Cybersecurity and Infrastructure Security Agency (CISA)*, aquesta falta de segmentació va ser un dels factors clau que va amplificar l'impacte de l'atac.

A més, DarkSide va utilitzar tècniques d'**enginyeria social** per obtenir informació confidencial que va facilitar l'accés als sistemes interns de Colonial Pipeline. Aquestes tècniques poden incloure correus electrònics de phishing dissenyats per enganyar empleats a revelar informació crítica, com credencials d'accés.

6.4-Impacte

L'atac de ransomware a Colonial Pipeline va tenir un impacte significatiu, no només per a l'empresa sinó també per a la infraestructura crítica de subministrament de combustible dels Estats Units. L'impacte es va manifestar en diversos nivells:

1. **Interrupció de les Operacions**: Colonial Pipeline va optar per aturar les seves operacions completament com a mesura de precaució per evitar que el ransomware es propagés encara més. Aquesta decisió va provocar la interrupció temporal del subministrament de combustible a través de la seva xarxa, que abasta prop del 45% del subministrament de combustible de la costa est dels Estats Units. L'aturada va afectar l'enviament de gasolina, dièsel i altres combustibles essencials, creant una escassetat temporal en diversos estats i fent que molts ciutadans acaparessin combustible per por d'una crisi prolongada.
2. **Impacte Econòmic**: A nivell econòmic, l'atac va provocar una pujada dels preus del combustible en diverses regions afectades. Segons el *Department of Energy* (2021), els preus de la gasolina van experimentar un augment considerable a causa de l'escassetat i la demanda creixent. Aquesta situació va tenir un efecte dominó en altres sectors econòmics que depenen del subministrament regular de combustibles, com el transport i la logística, generant pèrdues econòmiques addicionals.
3. **Resposta Gubernamental**: L'atac va portar el govern dels Estats Units a intervenir per ajudar a gestionar la crisi i assegurar el subministrament de combustible. El Departament d'Energia va emetre permisos temporals per augmentar el transport de combustible per carretera i altres mitjans, tractant de minimitzar l'impacte de l'aturada de Colonial Pipeline. Aquest incident va forçar també una revisió de les polítiques de ciberseguretat per a infraestructures crítiques, amb noves mesures per reforçar la protecció contra ciberatacs d'alt risc, tal com recull la *Cybersecurity and Infrastructure Security Agency (CISA)* en el seu informe de 2023.

4. **Danys Reputacionals**: Colonial Pipeline també va patir un dany reputacional important a causa de l'atac. La decisió de pagar el rescat va ser controvertida i va ser àmpliament discutida en els mitjans de comunicació i entre els experts en ciberseguretat. Aquesta situació va exposar l'empresa a crítiques per no disposar de mesures de seguretat més robustes, i va posar de manifest la vulnerabilitat d'empreses que gestionen infraestructures crítiques.

6.5-Resolució del problema

La resolució de l'atac a Colonial Pipeline va requerir una combinació de mesures per recuperar l'accés als sistemes i restablir les operacions. En primer lloc, l'empresa va prendre la decisió controvertida de pagar part del rescat al grup de cibercriminals DarkSide. Segons fonts com el *Congressional Research Service* (2021), Colonial Pipeline va pagar prop de 4,4 milions de dòlars en Bitcoin als atacants per obtenir la clau de desxifrat necessària per recuperar l'accés als seus sistemes. Tot i així, el procés de desxifrat va ser més lent del que s'esperava, i l'empresa va haver de recórrer a altres mètodes per restablir les operacions.

Per minimitzar l'impacte de l'incident, el govern dels Estats Units va intervenir ràpidament amb mesures per facilitar el subministrament de combustible. El Departament d'Energia va emetre permisos temporals que permetien un augment del transport de combustible per altres mitjans, com camions i vaixells, per tal de mitigar l'efecte de l'aturada de la xarxa de canonades. Aquesta resposta va ajudar a reduir la crisi de subministrament en algunes regions afectades.

Després de l'incident, Colonial Pipeline va implementar una sèrie de millores en la seva infraestructura de seguretat per prevenir futurs atacs. Aquestes millores van incloure l'**adopció de l'autenticació multifactor** per a tots els sistemes d'accés remot, una mesura recomanada per la *Cybersecurity and Infrastructure Security Agency (CISA)* per evitar que atacs similars puguin tenir èxit en el futur. A més, l'empresa va treballar per millorar la **segmentació de la seva xarxa**, de manera que, en cas d'un altre atac, el malware no pogués propagar-se fàcilment per tota la infraestructura.

Finalment, Colonial Pipeline va augmentar la **formació en ciberseguretat** per als seus empleats, enfocant-se especialment en les tècniques d'enginyeria social que DarkSide va utilitzar per obtenir accés als sistemes. Aquestes mesures de formació tenen com a objectiu reduir la vulnerabilitat de l'empresa davant de futures amenaces i millorar la capacitat de resposta interna en cas d'incident.

Aquestes accions no només van permetre a Colonial Pipeline restablir les seves operacions i recuperar-se de l'atac, sinó que també van servir per enfortir la seva postura de seguretat davant de ciberamenaces, protegint millor els sistemes i dades crítiques que suporten el subministrament de combustible als Estats Units.

6.6-Reproductivitat de l’incident

L’atac a Colonial Pipeline ha servit d’exemple per comprendre com els atacs de ransomware poden impactar infraestructures crítiques, i ha posat de manifest la possibilitat que incidents similars es repeteixin en altres sectors essencials. La reproductivitat d'aquest incident és alta, ja que els ciberdelinqüents continuen perfeccionant les seves tècniques i adaptant les estratègies per afectar diverses indústries.

Casos similars d’atacs de ransomware a infraestructures crítiques s’han observat en altres empreses i sectors. Per exemple, el mateix any, l’empresa de processament de carn JBS va patir un atac de ransomware que va interrompre la producció en diverses plantes a tot el món, causant problemes de subministrament en el sector alimentari. De manera similar, l’empresa noruega Norsk Hydro va patir un atac de ransomware el 2019 que va afectar les seves operacions d’alumini a nivell global, generant grans pèrdues econòmiques. Aquests casos demostren que el ransomware és una amenaça recurrent per a infraestructures essencials.

La possibilitat de repetibilitat es, en part, per culpa de la disponibilitat del ransomware com a servei, que permet que grups de cibercriminals lloguin aquest tipus de programari a altres atacants amb poca experiència. Aixo augmenta el risc d'atacs a infraestructures crítiques, ja que facilita l'accés a tècniques avançades de ransomware a un ampli ventall d'actors malintencionats.

Tanmateix, des de l’incident de Colonial Pipeline, el govern dels Estats Units ha implementat mesures per reduir la probabilitat que es produeixin atacs semblants en el futur. Entre aquestes mesures, destaquen les recomanacions per adoptar una segmentació de xarxa més estricta, l’ús de l’autenticació multifactor, i una major col·laboració entre agències governamentals i empreses privades per compartir informació sobre ciberamenaces. Segons la *Cybersecurity and Infrastructure Security*

Agency (CISA), aquests protocols tenen com a objectiu millorar la resiliència de les infraestructures crítiques davant d'amenaces de ransomware.

Tot i els esforços per mitigar el risc, la complexitat creixent dels atacs de ransomware i la persistència dels ciberdelinqüents fan que la possibilitat de nous incidents sigui alta. L'incident de Colonial Pipeline ha deixat clar que, sense una implementació efectiva de les mesures de seguretat recomanades, el risc d'un atac similar continua existint. Per tant, és crucial que empreses d'infraestructures crítiques segueixin les millors pràctiques de seguretat per minimitzar la probabilitat i l'impacte de futurs incidents.

7. Conclusions

L'atac de ransomware a Colonial Pipeline ha posat de manifest la vulnerabilitat de les infraestructures crítiques davant les ciberamenaces i les greus conseqüències que aquests incidents poden tenir tant per a l'empresa afectada com per a la societat en general. Aquest incident va provocar una crisi de subministrament de combustible a la costa est dels Estats Units, afectant milions de persones i destacant la dependència de les infraestructures energètiques. A més, va evidenciar com un únic atac pot generar impactes econòmics i socials de gran abast, incloent-hi la pujada de preus i problemes logístics.

Un dels principals aprenentatges que es pot extreure d'aquest cas és la necessitat de mesures de seguretat més robustes, especialment en sectors clau com el subministrament energètic. La falta de segmentació de la xarxa i l'absència de protocols d'autenticació multifactor van facilitar l'accés dels atacants i van agreujar l'impacte de l'atac. En resposta, Colonial Pipeline i altres empreses d'infraestructures crítiques han començat a implementar aquestes millores, com recomana la *Cybersecurity and Infrastructure Security Agency (CISA)*, per reduir la probabilitat de futurs incidents.

A més, l'incident ha demostrat la importància de la col·laboració entre el sector públic i privat. La ràpida resposta del govern dels Estats Units va ser crucial per minimitzar l'impacte de l'atac, amb mesures que van permetre garantir el subministrament de combustible mitjançant altres vies. Aquesta col·laboració i el compromís del govern per reforçar la ciberseguretat d'infraestructures crítiques han estat essencials per establir noves normes de protecció i crear protocols de resposta a incidents en temps real.

Finalment, l'atac de Colonial Pipeline ha subratllat la urgència de formar els empleats en pràctiques de ciberseguretat i en la detecció de tècniques d'enginyeria social, que són cada vegada més utilitzades pels cibercriminals. La formació dels treballadors i la

conscienciació sobre les amenaces actuals són factors clau per prevenir futurs incidents.

En conclusió, l'incident de Colonial Pipeline és un recordatori poderós de la importància de la ciberseguretat en infraestructures crítiques. Amb les mesures adequades i una col·laboració estreta entre empreses i governs, es pot reduir el risc d'atacs similars en el futur. Aquest cas ens ensenya que la protecció d'aquests sistemes no és només una responsabilitat empresarial, sinó també un pilar per a la seguretat nacional i el benestar públic.

8. Bibliografia i annexos

Cybersecurity and Infrastructure Security Agency (CISA). (2021). *Ransomware guidance for organizations*. CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-131a

U.S. Department of Energy. (2021). *Colonial Pipeline Cyber Incident*. U.S. Department of Energy. https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

Grealish, G. (2021, August 3). *Colonial Pipeline hack and zero-trust security*. IBM Security. https://community.ibm.com/community/user/security/blogs/gerry-grealish1/2021/08/03/colonial-pipeline-hack-and-zero-trust-security

Congressional Research Service (CRS). (2021). *Colonial Pipeline: Ransomware and critical infrastructure*. CRS. https://crsreports.congress.gov/product/pdf/IN/IN11667

Cybersecurity and Infrastructure Security Agency (CISA). (2023). *The attack on Colonial Pipeline: What we've learned and what we've done over the past two years*. CISA. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

Dark Reading. (2021). *Colonial Pipeline cyberattack: What security pros need to know*. Dark Reading. https://www.darkreading.com/cybersecurity-operations/colonial-pipeline-cyberattack-what-security-pros-need-to-know

MIT Technology Review. (2021, May 24). *How the Colonial Pipeline hackers did it*. MIT Technology Review. https://www.technologyreview.com/2021/05/24/1025195/colonial-pipeline-ransomware-bitdefender/

Business Insider. (2022). *Business lessons learned from the Colonial Pipeline attack*. Business Insider. https://www.businessinsider.in/tech/enterprise/news/business-lessons-learned-for-the-colonial-pipeline-attack/articleshow/92821504.cms

Cyber Readiness Institute. (2021). *Analysis of the Colonial Pipeline ransomware attack*. Cyber Readiness Institute. https://cyberreadinessinstitute.org/es/el-cyber-readiness-institute-analiza-el-ataque-de-ransomware-a-colonial-pipeline/

Georgetown Environmental Law Review. (2021). *Cybersecurity policy responses to the Colonial Pipeline ransomware attack*. Georgetown Environmental Law Review. https://www.law.georgetown.edu/environmental-law-review/blog/cybersecurity-policy-responses-to-the-colonial-pipeline-ransomware-attack/