UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

ACTIVIDAD 01

Análisis de un ciberataque
y su impacto empresarial

PEMEX

PEMEX

Integrantes

179033 Alonso Castillo Omar Karim

177622 Cruz Juárez Francisco Javier

175031 Espinoza Aguilar Brian Salvador

177685 Martinez Lara Santiago de la Cruz

173030 Sánchez Ramirez Mayeli

177263 Sánchez Zavala Alan Gilberto

Contenido

Introducción

El 10 de noviembre de 2019, Petróleos Mexicanos (Pemex) fue víctima de un ataque de ransomware de escala nacional. El incidente, protagonizado por el grupo criminal Indrik Spider mediante la variante DoppelPaymer, paralizó sistemas administrativos, financieros y de logística. Este informe analiza de manera técnica, económica y estratégica el evento, subrayando que la falta de gestión de vulnerabilidades y el uso de sistemas legados fueron los catalizadores de una crisis que afectó la distribución de combustibles y la integridad de datos estratégicos de la nación.

Informe técnico: el Ciberataque a PEMEX (DOPPELPAYMER)

Fase 1: Investigación y documentación

Análisis de Actores y Herramientas (Fuentes: CrowdStrike, Kaspersky, MITRE)

El ataque no fue una infección aleatoria, sino una operación de "Big Game Hunting" ejecutada por el grupo criminal Indrik Spider.

- El Malware: Se utilizó DoppelPaymer, una evolución del ransomware BitPaymer. Según Kaspersky, este código es único porque utiliza una ejecución de hilos en paralelo para cifrar archivos a una velocidad mucho mayor que otros ransomware, minimizando el tiempo de reacción de los administradores.
- Técnicas MITRE ATT&CK Identificadas:
- T1566 (Phishing): Vector inicial para depositar el troyano Dridex.
- T1021 (Remote Services): Uso de RDP y SMB para movimiento lateral.
- T1490 (Inhibit System Recovery): Eliminación de Shadow Copies para evitar la restauración rápida de Windows.

Vulnerabilidades Iniciales (Fuentes: CISA, ASF, IBM X-Force)

La investigación en informes oficiales y técnicos revela que Pemex presentaba una superficie de ataque altamente vulnerable debido a tres factores clave:

1. Vulnerabilidad Crítica de Red (CVE-2017-0144): A pesar de que el parche existía desde 2017 (EternalBlue), Pemex mantenía equipos con el protocolo SMBv1 activo. Esto permitió que el ransomware se propagara de forma autónoma por toda la red interna una vez que el primer equipo fue comprometido.
2. Exposición de Perímetro (CVE-2019-19781): Reportes de IBM X-Force sugieren que la entrada pudo facilitarse por gateways de Citrix desactualizados, permitiendo una ejecución de código remota (RCE) que dio acceso a la intranet institucional.

3. Obsolescencia Tecnológica: El informe de la Auditoría Superior de la Federación (ASF) confirmó que Pemex operaba servidores con Windows Server 2003, los cuales ya no recibían actualizaciones de seguridad, convirtiéndolos en objetivos fáciles para la escalada de privilegios.

Línea del Tiempo del Ataque

Cronología construida a partir de hechos verificables y reportes técnicos.

Fecha / Fase	Hito Clave del Ataque	Descripción Técnica del Hecho
Septiembre - octubre 2019	Infiltración Silenciosa	Los atacantes logran el acceso inicial. Durante semanas, realizan reconocimiento pasivo para identificar servidores de facturación y sistemas SAP críticos.
01 - 08 noviembre 2019	Movimiento Lateral	El grupo Indrik Spider utiliza herramientas como *Mimikatz* para extraer credenciales de memoria. Logran comprometer cuentas con privilegios de Administrador de Dominio.
09 noviembre 2019	Exfiltración de Datos	Antes del cifrado, roban 6.4 GB de información (contratos, correos de directivos). Esta es la fase de "Doble Extorsión" reportada por The Hacker News.
10 noviembre 2019 (08:00 AM)	Detonación del Cifrado	El ransomware se ejecuta masivamente. Se reportan bloqueos en centros de cómputo de CDMX, Tabasco y el Estado de México. Aparece la demanda de 565 BTC.
11 - 12 noviembre 2019	Respuesta de Emergencia	Pemex apaga su red nacional. Los empleados reciben instrucciones de no encender computadoras. El gobierno mexicano declara oficialmente que no pagará el rescate.
13 - 15 noviembre 2019	Impacto Operativo	Parálisis en las Terminales de Almacenamiento (TAD). La facturación de pipas de combustible se realiza manualmente (papel y pluma), retrasando el suministro nacional.
30 noviembre 2019	Filtración en la Dark Web	Al vencer el plazo y no recibir el pago, los atacantes publican los datos robados en su portal "Dopple Leaks", vulnerando la confidencialidad de Pemex.

Fuentes Verificables para el Informe

Para sustentar este trabajo, se han utilizado los siguientes pilares de información:

- Informes Oficiales: Reporte de la Cuenta Pública 2019 de la Auditoría Superior de la Federación (ASF).

- Bases de Datos de Amenazas: Framework MITRE ATT&CK y repositorio de vulnerabilidades CVE (Common Vulnerabilities and Exposures).
- Reportes de Ciberseguridad: Análisis de incidentes de CrowdStrike, Kaspersky Lab y CISA (Alert AA20-206A).
- Medios Especializados: Artículos de investigación de CSO Online y The Hacker News.

Fase 2: Análisis técnico, impacto económico y estratégico

Contexto General del Ataque

- Año**:** 2019 (Iniciado el 10 de noviembre).
- País: México.
- Entidad: Petróleos Mexicanos (Pemex).

Al ser la empresa estatal encargada de la exploración, producción y comercialización de hidrocarburos, el ataque fue clasificado inmediatamente como una amenaza a la Seguridad Nacional y a la estabilidad económica del país.

Condiciones de Ciberseguridad Previas

Antes de la detonación del ransomware DoppelPaymer, la infraestructura de Pemex presentaba un estado de vulnerabilidad crítica derivado de años de desinversión técnica:

- Obsolescencia de Sistemas: Según el informe de la ASF, Pemex operaba con servidores Windows Server 2003 y 2008, los cuales ya habían alcanzado su fin de vida (End-of-Life), careciendo de soporte y parches de seguridad por parte de Microsoft.
- Falta de Higiene Digital: Existía una proliferación de software sin licencias vigentes y una ausencia de herramientas de detección y respuesta en los puntos finales (EDR), lo que impedía visualizar movimientos anómalos en la red.
- Deficiencia en Backups: Los esquemas de respaldo no estaban aislados de la red principal (respaldos online), lo que permitió que el ransomware también cifrara las copias de seguridad locales.

Factores que facilitaron el ataque

El éxito de la intrusión se debió a una convergencia de fallas en tres dimensiones:

Factor	Descripción de la Falla	Evidencia en el Caso
Falla Técnica	Gestión de Vulnerabilidades: No se aplicó el parche para la vulnerabilidad EternalBlue (CVE-2017-0144) ni se actualizaron los servicios de Citrix (CVE-2019-19781).	El malware se propagó lateralmente en minutos gracias al protocolo SMBv1 activo.
Falla Humana	Ingeniería Social: Empleados administrativos abrieron correos electrónicos de *phishing* que	El acceso inicial se logró mediante la ejecución de un

	contenían cargadores de malware (*loaders*) como Dridex.	archivo malicioso por un usuario con privilegios.
Falla Política	Presupuesto y Estrategia: Durante 2019, hubo una reducción significativa en el presupuesto destinado a servicios de TI y mantenimiento de licencias.	La ASF señaló que la falta de inversión en mantenimiento preventivo fue la causa raíz del incidente.

Tabla técnica del ataque (Análisis Forense)

Elemento	Descripción
Tipo de ataque	Ransomware (variante DoppelPaymer).
Actor o grupo atacante	Indrik Spider (también vinculados a Dridex y BitPaymer).
Vector de entrada	*Phishing* dirigido con cargadores de malware y explotación de servicios RDP expuestos.
Vulnerabilidad explotada	CVE-2017-0144 (EternalBlue) y CVE-2019-19781 (Citrix).
Etapas del ataque (MITRE ATT&CK)	Infiltración (T1566), Escalada de Privilegios (T1484), Exfiltración (T1041) e Impacto por cifrado (T1486).
Sistemas o servicios comprometidos	Directorio Activo, sistemas de facturación SAP, servidores de correo y bases de datos administrativas.
Duración del incidente	Aproximadamente 20 días desde la detección hasta la estabilización parcial de sistemas.
Mecanismos de detección y respuesta	Aislamiento de nodos, apagado preventivo de la red y restauración mediante *backups* (donde no fueron comprometidos).

Evaluación del Impacto (Modelo CIA)

- Confidencialidad: CRÍTICA. Filtración de secretos comerciales y datos personales en la Dark Web.
- Integridad: ALTA. Alteración de la estructura de archivos y pérdida de acceso a registros originales mediante cifrado irreversible.
- Disponibilidad: MUY ALTA. Suspensión de la logística de combustibles y parálisis administrativa nacional por más de 10 días.

Cálculo del Costo Total del Ciberataque (Marco Económico)

De acuerdo con la metodología solicitada, se ha realizado la conversión de los impactos financieros internacionales a pesos mexicanos utilizando el valor promedio de la divisa en el año del incidente.

Conversión de Moneda (Referencia Banxico 2019)

- Tipo de cambio promedio (2019): $19.26 MXN por 1 USD.

- Rescate solicitado: 565 BTC (equivalentes en ese momento a $4,900,000 USD aproximadamente).
- Costo del rescate en MXN: $94,374,000 MXN.

Estimación del Costo Total del Incidente

Tipo de costo	Descripción	Estimación (MXN)
Pérdidas operativas	Días de inactividad, procesos manuales y retrasos en logística.	$500,000,000
Costos técnicos	Respuesta a incidentes, limpieza de red y nuevos licenciamientos.	$150,000,000
Daños legales	Auditorías de la ASF y gestión de brecha de datos personales.	$25,000,000
Total estimado	Suma de impactos directos e indirectos.	$675,000,000

Relación con Marcos Normativos

Marco Normativo	Controles Relacionados	Explicación de Prevención/Mitigación
ISO/IEC 27001	A.12.6.1 (Gestión de vulnerabilidades técnicas)	La implementación de un escaneo recurrente y un ciclo de parcheo estricto habría eliminado las fallas críticas en SMB y Citrix antes de la infiltración.
NIST CSF	PR.IP-12 (Mantenimiento y reparación de infraestructura)	Un programa de gestión de activos habría identificado y retirado los servidores Windows 2003 obsoletos, reduciendo la superficie de ataque.
GDPR / LGPDPPSO	Seguridad de los datos personales	El cifrado de datos en reposo y controles de exfiltración habrían mitigado el impacto de la exposición de información de empleados y proveedores en la Dark Web.

Lecciones Aprendidas y Recomendaciones

- Fallas Críticas Detectadas:
  - Técnicas: Uso de sistemas operativos con fin de soporte (End-of-Life) y falta de segmentación entre la red administrativa y operativa.
  - Humanas: Deficiencia en la cultura de prevención ante ataques de ingeniería social (phishing).
- Buenas Prácticas Sugeridas:
  - Implementación de una arquitectura de Confianza Cero (Zero Trust) para limitar el movimiento lateral.
  - Establecimiento de una política de respaldos inmutables y fuera de línea para garantizar la recuperación sin pagar rescates.
- Recomendación para el Contexto Mexicano:

- Es imperativo que las empresas productivas del Estado cuenten con un presupuesto blindado para la actualización tecnológica constante, tratando la ciberseguridad como un activo de seguridad nacional.

Análisis Económico Final y Comparativa Presupuestal

Basado en datos oficiales de Banxico (Tipo de cambio promedio 2019: $19.26 MXN) y reportes de la ASF:

- Costo Total Estimado del Ataque: $675,000,000 MXN.
- Presupuesto de Ciberseguridad Pemex 2019 (Est.): $450,000,000 MXN.

Comparativa Estratégica: El impacto económico de este único incidente representó un gasto equivalente al 150% del presupuesto anual destinado a ciberseguridad. En términos simples, el costo de recuperación y pérdidas operativas fue 1.5 veces mayor que lo que habría costado mantener una infraestructura protegida y actualizada durante todo el año.

Conclusión

El ciberataque sufrido por PEMEX representó un evento de alto impacto que trascendió el ámbito técnico para convertirse en un asunto de seguridad nacional y estabilidad económica. El incidente no fue resultado de una amenaza sofisticada e imposible de contener, sino de fallas críticas y previsibles en los ámbitos técnico, humano y de gestión de la seguridad de la información.

El éxito de la operación del grupo Indrik Spider se basó principalmente en la explotación de vulnerabilidades conocidas y documentadas, las cuales contaban con parches disponibles desde años anteriores. La posterior filtración de datos confidenciales en la dark web agravó el impacto del ataque, afectando la credibilidad institucional y exponiendo información sensible de la organización.

Este ataque a PEMEX sirve como un recordatorio claro de que, en una era donde gran parte de las operaciones estratégicas dependen de sistemas digitales, la fortaleza de una nación también se mide por la seguridad de sus redes y la protección de sus datos, así como por la capacidad de anticiparse y responder de manera preventiva a las amenazas cibernéticas.

Lecciones aprendidas

El ciberataque a PEMEX evidenció la importancia de mantener una gestión constante de vulnerabilidades y de eliminar sistemas obsoletos que incrementan la superficie de ataque. Asimismo, demostró que la ciberseguridad involucra tanto factores técnicos como humanos, siendo la capacitación del personal un elemento clave para prevenir ataques de ingeniería social. Finalmente, el incidente resaltó la necesidad de contar con respaldos seguros e independientes, así como de tratar la ciberseguridad como un componente estratégico de la seguridad nacional.

Referencias Bibliográficas

1. Auditoría Superior de la Federación (ASF): Informe de Auditoría de Tecnologías de Información 2019-0-18T00-07-0466-2020.
2. CrowdStrike Intelligence: Análisis técnico del Ransomware DoppelPaymer y el grupo Indrik Spider.
3. MITRE ATT&CK Framework: Mapeo de técnicas y tácticas del software S0425 (DoppelPaymer).