UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

ACTIVIDAD 01 - Análisis de un ciberataque real y su impacto empresarial.

Edwin Admael Castillo Gómez *181700*

Diego Osvaldo Hernández Fernández *182217*

Carlos René Castillo Olvera *182033*

CNO V: *Seguridad Informática*

30/01/2026

Docente: *Servando Contreras*

Índice

Contenido

Introducción

El ciberataque de NotPetya de 2017 es uno de los incidentes de ciberseguridad mas destructivos de la historia moderna, no solo por su alcance global, sino por su verdadera naturaleza: un gran sabotaje disfrazado de ransomware. A diferencia de otros ataques, NotPetya fue únicamente diseñado para causar interrupción operativa masiva, afectando infraestructuras criticas y cadenas de suministro internacionales en tan solo unas horas.

En el presente trabajo analizamos el impacto del malware NotPetya en la empresa Maersk, el mayor operador marítimo de transporte marítimo de contenedores a nivel mundial, cuya operación global fue paralizada casi por completo. A través de una línea del tiempo, una evaluación técnica del ataque, el análisis del impacto bajo el modelo CIA, el cálculo de pérdidas económicas, entre otros criterios, se busca comprender como diversas fallas técnicas, operativas y estratégicas permitió que el incidente NotPetya localizado en Ucrania escalara tanto hasta casi destruir a Maersk.

Para comenzar, cabe recalcar que el caso NotPetya – Maersk permite comprender las implicaciones reales de lo que es la falta de resiliencia digital en organizaciones altamente interconectadas y dependientes de las tecnologías de la información.

NotPetya – Maersk (2017)

Línea del Tiempo NotPetya - Maersk (2017)

https://prezi.com/view/m0VILbIscfj2ph5YluT4/?referral_token=m92o20lnB3FN

1. Contexto General del Ataque: NotPetya (2017)

Año, país y entidad afectada

Año del incidente: Junio de 2017 (el brote principal comenzó el 27 de junio, víspera del Día de la Constitución en Ucrania).

País de origen/Impacto inicial: Ucrania fue el epicentro (objetivo estratégico). El ataque se propagó globalmente en cuestión de horas.

Origen del brote (Paciente Cero): La empresa tecnológica Linkos Group, desarrolladora del software contable M.E.Doc. La cual los atacantes comprometieron sus servidores de actualización para distribuir el malware NotPetya. Dado que M.E.Doc es el software estándar y obligatorio para el pago de impuestos en Ucrania, la infección se expandió de forma inmediata a todas las empresas que operaban en dicho país.

Empresa afectada: A.P. Møller-Mærsk (Maersk), la empresa de logística y transporte de contenedores más grande del mundo, con sede en Dinamarca.

- **Alcance del daño en Maersk:** El ataque paralizó 76 terminales portuarias en todo el mundo y afectó a 800 centros de datos, 1,200 aplicaciones y aproximadamente 45,000 laptops y 4,000 servidores.
- **Otras empresas afectadas (Víctimas globales):** Además de Maersk, el ataque impactó a corporaciones como FedEx (a través de TNT Express),

la farmacéutica Merck, la constructora francesa Saint-Gobain, la alimentaria Mondelez y el fabricante de bienes de consumo Reckitt Benckiser.

Condiciones de ciberseguridad previas

El ataque no fue un evento aislado, sino la culminación de una campaña de sabotaje del grupo Sandworm (Unidad 74455 del GRU ruso). Este grupo, identificado por dejar referencias a la novela Dune en su código, utilizó a Ucrania como laboratorio tras ejecutar los primeros apagones cibernéticos de la historia en 2015 y 2016.

Bajo este acecho, Maersk operaba con debilidades críticas:

Centralización de la Identidad (Active Directory): Maersk utilizaba un único "bosque" de AD global sin segmentación efectiva. Al caer una oficina (Odessa), el atacante obtuvo automáticamente las "llaves maestras" de toda la red mundial, permitiendo que un problema local se volviera una parálisis global en minutos.

Gestión de Parches y Legado de EternalBlue: Pese a existir el parche MS17-010 desde marzo de 2017, la inmensa infraestructura de Maersk dificultó una actualización total. Esto dejó la puerta abierta para que el exploit EternalBlue propagara el malware de forma automatizada.

Dependencia Legal (El Caballo de Troya): Maersk estaba obligada por ley a usar M.E.Doc para operar en Ucrania. Sandworm aprovechó esta confianza para comprometer la cadena de suministro, insertando el malware en una actualización legítima que evadió los perímetros de seguridad de la compañía.

Factores que facilitaron el ataque

El éxito de NotPetya en Maersk no fue un solo error, sino una combinación de fallas en tres niveles:

- **Falla Técnica (Cadena de Suministro):** El grupo **Sandworm (GRU)** comprometió las actualizaciones del software **M.E.Doc**. Maersk instaló inadvertidamente el malware con privilegios de administrador. NotPetya utilizó **EternalBlue** y **MimiKatz** para propagarse de forma automatizada por toda la red global en minutos.
- **Falla Humana / Operativa:** Existía una gestión deficiente de **privilegios**. El exceso de permisos de administrador local permitió que el malware robara credenciales de red de la memoria de las estaciones de trabajo, facilitando el control total del Active Directory.
- **Falla Política / Estratégica:** Se priorizó la **eficiencia operativa sobre la resiliencia**. Al no segmentar lógicamente la red de Ucrania (zona de alto riesgo geopolítico) del resto del mundo, un incidente en una oficina regional en Odessa paralizó terminales portuarias globales en Los Ángeles y Róterdam.

2. Tabla Técnica del Ataque: NotPetya

Elemento	Descripción
Tipo de ataque	**Wiper Malware / Supply Chain Attack.** Sabotaje destructivo bajo apariencia de ransomware.
Actor atacante	**Sandworm (APT44 / GRU).** Unidad de inteligencia militar rusa.
Vector de entrada	**Compromiso de cadena de suministro.** Servidor de actualizaciones del software **M.E.Doc.**

Vulnerabilidad	**CVE-2017-010 (EternalBlue):** Exploit de SMBv1 y **MimiKatz** para robo de credenciales.
Etapas (MITRE ATT&CK)	**Acceso:** T1195.002 (Supply Chain) **Ejecución:** T1072 (Deployment Tools) **Movimiento Lateral:** T1021.002 (Admin Shares) **Impacto:** T1485 (Data Destruction).
Sistemas Afectados	**Active Directory Global**, ERP, Gestión de Terminales y 49,000 equipos (Servidores/PCs).
Duración	**Cifrado:** < 1 hora. **Restauración básica:** 10 días. **Normalización:** Semanas.
Detección y Respuesta	**Detección:** Basada en síntomas (destrucción). **Respuesta:** Aislamiento físico de red y reconstrucción manual de AD (vía respaldo en Ghana).

3. Evaluación del Impacto (Modelo CIA)

Principio	Impacto	Evidencia Clave
Confidencialidad	**Bajo**	El malware no fue diseñado para exfiltrar datos (sin funciones de comando y control C2). El objetivo fue el sabotaje, no el espionaje.
Integridad	**Crítico**	Alteración irreversible del **MBR** y la **MFT**. El malware engañaba al usuario simulando una reparación de disco (chkdsk) mientras destruía el sistema operativo.

Disponibilidad	**Catastrófico**	Parálisis de **76 terminales portuarias**. Maersk operó manualmente con "papel y lápiz" durante días ante la caída total de sistemas de inventario y logística.

4. Cálculo del Costo Total del Ciberataque (Marco Económico)

Tipo de costo	Descripción	Estimación (MXN)
Pérdidas operativas	Caída en ingresos por parálisis de 76 terminales portuarias, interrupción de pedidos durante semanas y logística manual.	**$4,356,000,000** ($240M USD)
Daños reputacionales	Aunque Maersk recuperó clientes, el valor de la acción sufrió volatilidad inmediata y se perdió confianza en la cadena de suministro.	**$544,500,000** ($30M USD)
Costos técnicos	Reinstalación de 4,000 servidores, 45,000 PCs, consultoría de emergencia (KPMG/Microsoft) y reconstrucción de Active Directory.	**$544,500,000** ($30M USD)
Costos legales / regulatorios	En 2017, GDPR aún no estaba en pleno vigor sancionador como hoy, pero hubo costos de cumplimiento y auditorías extraordinarias.	**$0** (No hubo multas públicas significativas reportadas)
Pago de rescate o extorsión	**NotPetya era un Wiper.** Aunque pedía $300 USD en BTC por máquina, Maersk no pagó ya que no había forma técnica de recuperar los datos.	**$0**

TOTAL ESTIMADO	**Pérdida total declarada por el grupo Maersk en su informe anual.**	**$5,445,000,000 MXN**

5. Relación con Marcos Normativos

Marco Normativo	Control / Dominio	Impacto en la Mitigación
ISO 27001	**A.12.6.1: Gestión de Vulnerabilidades**	La aplicación oportuna del parche **MS17-010** habría bloqueado el exploit *EternalBlue* y la propagación inicial.
ISO 27001	**A.13.1.1: Segmentación de Red**	Aislar lógicamente las oficinas de Ucrania habría evitado que el brote local infectara los **800 centros de datos** globales.
NIST CSF	**PR.AC-4: Mínimo Privilegio**	Restringir permisos administrativos y proteger procesos de memoria (LSASS) habría neutralizado el robo de credenciales vía **MimiKatz**.
NIST CSF	**ID.SC-1: Riesgo de Cadena de Suministro**	Evaluar la seguridad de **M.E.Doc** y aplicar "Sandboxing" a sus actualizaciones habría detectado el malware antes de su ejecución.
GDPR	**Art. 32: Disponibilidad y Resiliencia**	Exige la capacidad de restaurar datos tras un incidente. La falta de **backups offline** funcionales habría supuesto multas de hasta el 4% de la facturación.

Explicación de Mitigación Estratégica

Si Maersk hubiera tenido estos controles maduros, el impacto se habría reducido de la siguiente manera:

Prevención (Vulnerabilidades): El uso de herramientas de escaneo constante (NIST PR.IP-12) habría identificado los sistemas sin el parche de Microsoft mucho antes de junio de 2017.

Contención (Segmentación): La implementación de una arquitectura de "Zero Trust" o segmentación robusta (ISO A.13.1.1) habría servido como un "muro de fuego", confinando el ataque solo a los servidores que usaban M.E.Doc en Ucrania, salvando las terminales portuarias globales.

Recuperación (Resiliencia): El incidente de Ghana demostró que Maersk no tenía Backups Offline (fuera de línea) actualizados para sus controladores de dominio. El control de ISO A.17.1.2 (Continuidad de TI) exige redundancia que no dependa de la misma red infectada.

6. Lecciones aprendidas y recomendaciones

El caso de NotPetya demostró que las mayores fallas no fueron solo técnicas, sino también de gestión. Maersk tenía sistemas obsoletos, parches sin aplicar y, sobre todo, una red global sin segmentación, lo que permitió que el malware se propagara en minutos entre países. Además, sus respaldos no estaban preparados para un escenario extremo donde todos los controladores de dominio fueran destruidos al mismo tiempo. A nivel organizacional, la ciberseguridad no era una prioridad estratégica: los planes de mejora existían, pero no se ejecutaron porque no impactaban en los indicadores de desempeño

de los directivos. También se evidenció el riesgo de confiar en proveedores sin controles sólidos, como ocurrió con el software ucraniano comprometido.

Este ataque dejó claro que prácticas como la segmentación de redes, la actualización constante de sistemas, la aplicación rigurosa de parches, los respaldos aislados y los planes de recuperación probados pueden reducir drásticamente el impacto de un incidente. La seguridad debe integrarse en la estrategia empresarial, con apoyo ejecutivo, monitoreo continuo y controles como autenticación multifactor y modelos de acceso restringido.

Para México y Latinoamérica, las lecciones son aún más relevantes, ya que muchas organizaciones operan con infraestructura antigua, menor inversión en seguridad y alta dependencia de proveedores externos. Es fundamental modernizar sistemas, separar redes críticas, mantener copias de seguridad fuera de línea, capacitar al personal y exigir estándares de seguridad a terceros. La continuidad del negocio debe planearse considerando que un ataque puede paralizar operaciones completas. NotPetya mostró que la ciberseguridad no es solo un tema técnico, sino un factor clave para la estabilidad operativa, económica y hasta nacional.

Conclusiones

El presente análisis del ataque NotPetya a la empresa demuestra que la magnitud del impacto no fue solo consecuencia de una única vulnerabilidad, sino de un efecto acumulativo de deficiencias técnicas, operativas y de gobierno en seguridad de la información. Por ejemplo la ausencia de una segmentación adecuada, la falta de aplicación oportuna de parches de seguridad y la dependencia de un solo proveedor comprometido crearon un escenario perfecto para la propagación global de malware en un corto periodo de tiempo.

La perspectiva tomada en el modelo CIA nos muestra como el ataque tuvo un impacto critico en la integridad y bastante catastrófico en la disponibilidad de los sistemas, por otro lado la confidencialidad no fue el objetivo principal de los atacantes. Las pérdidas económicas, operativas y reputacionales posteriores al incidente nos enseñan como la indisponibilidad de los sistemas pueden generar consecuencias enormes que podrían terminar completamente con una empresa.

Para finalizar, el caso NotPetya refuerza la necesidad de que la ciberseguridad sea tomada como un elemento estratégico del gobierno y no únicamente como algo técnico, especialmente en entidades organizacionales gigantes, complejas y altamente interconectadas.

Referencias y Bibliografía

- **CISA (Cybersecurity & Infrastructure Security Agency).** (2017, 1 de julio). *Petya Ransomware (Alert TA17-181A)*. https://www.cisa.gov/news-events/alerts/2017/07/01/petya-ransomware
- **ENISA (European Union Agency for Cybersecurity).** (2017). *Analysis of the NotPetya/ExPetr cyber-attack: Lessons for the EU*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017
- **MITRE ATT&CK.** (2023). *NotPetya (S0368) - Software Profile*. https://attack.mitre.org/software/S0368/
- **CrowdStrike.** (2017, 29 de junio). *NotPetya technical analysis: A triple threat*. https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/
- **Kaspersky Lab.** (2017, 27 de junio). Schrödinger's Pet(ya). Securelist - Kaspersky. https://securelist.com/schrodingers-petya/78870/

- **A.P. Møller - Mærsk.** (2018). *Annual Report 2017*. https://investor.maersk.com/static-files/d533735a-5df7-423c-8611-d4a2c3bf31b0
- **Greenberg, A.** (2018, 22 de agosto). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. Wired. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
- **The Hacker News.** (2017, 27 de junio). *NotPetya: Everything you need to know about the global attack*. https://thehackernews.com/2017/06/petya-ransomware-attack.html
- **O'Donnell, A.** (2024, 18 de junio). *The breach cost how much? How CISOs can talk effectively about the toll of a cyber incident*. CSO Online. https://www.csoonline.com/article/3844334/the-breach-cost-how-much-how-cisos-can-talk-effectively-about-the-toll-of-a-cyber-incident.html
- **Executive Summary.** (s/f). A Columbia university case study. Columbia.edu. Recuperado el 31 de enero de 2026. https://www.sipa.columbia.edu/sites/default/files/2022-11/NotPetya%20Final.pdf#:~:text=El%20ataque%20tambi%C3%A9n%20desactiv%C3%B3%20las%20herramientas%20de,por%20WhatsApp%20y%20sus%20cuentas%20de%20Gmail