NotPetya – Maersk (2017)

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. 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 (robado a la NSA) 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:

1. Falla Técnica (El Vector de Cadena de Suministro)

Compromiso de M.E.Doc: Los atacantes (identificados por agencias de inteligencia como el grupo Sandworm, vinculado al GRU ruso) comprometieron los servidores de actualización de Linkos Group (desarrolladores de M.E.Doc). Insertaron el malware en una actualización legítima. Cuando Maersk instaló la actualización en sus oficinas de Ucrania, el malware entró con privilegios de administrador.

Capacidad de Propagación: A diferencia de un ransomware tradicional, NotPetya utilizó EternalBlue (exploit de SMB) y MimiKatz (para extraer credenciales de la memoria) para saltar de una computadora infectada a toda la red global sin intervención humana.

2. Falla Humana / Operativa

Privilegios Excesivos: Muchos usuarios y procesos tenían privilegios de administrador local innecesarios. Esto permitió que herramientas como MimiKatz recolectaran credenciales de administradores de red que habían iniciado sesión en máquinas locales, facilitando el compromiso total del dominio de Active Directory.

3. Falla Política / Estratégica

Subestimación del Riesgo Geopolítico: Al operar en una zona de conflicto (Ucrania), la empresa no aisló lógicamente sus operaciones en ese país del resto de su red global. Se priorizó la conectividad y eficiencia operativa sobre la resiliencia y seguridad, permitiendo que un problema en una pequeña oficina de Odessa "apagara" los puertos en Los Ángeles y Róterdam.

Dato Clave de Resiliencia: Durante el incidente, Maersk descubrió que casi todos sus controladores de dominio (DC) estaban cifrados. Se salvaron solo porque una oficina en Ghana sufrió un corte de energía en el momento exacto del ataque, manteniendo un controlador de dominio desconectado y permitiendo la reconstrucción manual de la red global.

Tabla Técnica del Ataque: NotPetya / Maersk

Elemento	Descripción
Tipo de ataque	**Wiper Malware / Supply Chain Attack.** (Disfrazado de Ransomware, pero diseñado para destrucción masiva de datos sin posibilidad de recuperación).
Actor o grupo atacante	**Sandworm (APT44 / Voodoo Bear).** Atribuido por múltiples agencias de inteligencia al **GRU (Servicio de Inteligencia Ruso).**
Vector de entrada	**Ataque a la cadena de suministro (Supply Chain).** Compromiso del servidor de actualizaciones del software contable **M.E.Doc.**
Vulnerabilidad explotada	**CVE-2017-010 (EternalBlue):** Exploit de SMBv1. Además, uso de **MimiKatz** para extracción de credenciales de texto plano en memoria (LSASS).
Etapas del ataque (MITRE ATT&CK)	**1. Initial Access:** Supply Chain Compromise (T1195.002). **2. Execution:** Software Deployment Tools (T1072). **3. Persistence:** No relevante (el objetivo era destrucción inmediata). **4. Lateral Movement:** SMB/Windows Admin Shares (T1021.002) y Explotación de vulnerabilidades (T1210). **5. Impact:** Data Destruction (T1485) y Disk Structure Adversary (T1488).
Sistemas o servicios comprometidos	**Active Directory (AD) global**, Servidores de archivos, Bases de datos, ERP, Sistemas de gestión de terminales portuarias y 45,000 estaciones de trabajo Windows.

Duración del incidente	**Intrusión inicial:** 27 de junio de 2017. **Cifrado total:** Pocas horas. **Restauración total:** Aproximadamente **10 días** para recuperar servicios básicos y **semanas** para la normalización operativa completa.
Mecanismos de detección y respuesta	**Detección tardía:** Basada en síntomas (pantalla de cifrado). **Respuesta:** Desconexión física manual de redes, intervención de **Microsoft** y **KPMG**, y reconstrucción del Active Directory usando un controlador de dominio "sobreviviente" en Ghana.

Evaluación del Impacto (Modelo CIA)

Principio	Descripción del impacto	Evidencia del caso
Confidencialidad	**Impacto Bajo / No documentado.** El objetivo de NotPetya no era la exfiltración de datos, sino el sabotaje. Aunque el malware tenía acceso total, no hay evidencia de que se robara propiedad intelectual o datos de clientes.	Informes de **CrowdStrike** y **Wired** confirmaron que el código del malware no contenía funciones de comando y control (C2) para la extracción masiva de archivos; su diseño era de "un solo sentido".
Integridad	**Impacto Crítico.** El malware alteró el sector de arranque de los discos (**MBR - Master Boot Record**) y cifró la tabla de archivos maestros (MFT), volviendo los datos ilegibles y los sistemas inarrancables.	Los servidores de **Active Directory** de Maersk fueron corrompidos. El malware "enmascaraba" el cifrado destructivo como un proceso de chkdsk (reparación de disco) falso para engañar al usuario mientras destruía la integridad del sistema operativo.
Disponibilidad	**Impacto Total / Catastrófico.** Los servicios de logística global de Maersk quedaron completamente paralizados. La incapacidad de acceder a los sistemas de inventario y rutas detuvo la operación física en puertos.	**76 terminales portuarias** quedaron fuera de servicio. Durante días, Maersk tuvo que gestionar el movimiento de miles de contenedores de forma **manual (papel y lápiz)**. El acceso al correo corporativo y sistemas internos estuvo caído por más de una semana.

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**

Relación con Marcos Normativos

Marco Normativo	Control / Dominio Relacionado	Explicación de la Mitigación / Prevención
ISO/IEC 27001:2013	**A.12.6.1: Gestión de vulnerabilidades técnicas**	El control exige obtener información sobre vulnerabilidades y tomar medidas. NotPetya explotó el puerto 445 (SMB) mediante *EternalBlue*. Un control efectivo de parches (**MS17-010**) habría detenido la propagación inicial.
ISO/IEC 27001:2013	**A.13.1.1: Controles de red (Segmentación)**	Maersk tenía una red plana. Este control exige separar los servicios de red. Si las oficinas de Ucrania hubieran estado en una

		red segmentada (VLAN aislada), el malware no habría saltado al resto de los 800 centros de datos globales.
NIST CSF (v1.1)	**PR.AC-4: Gestión de acceso (Mínimo privilegio)**	NotPetya usó *MimiKatz* para robar credenciales en memoria. Si Maersk hubiera aplicado el principio de menor privilegio y protegido los procesos de LSASS, el malware no habría obtenido credenciales de administrador de dominio para moverse lateralmente.
NIST CSF (v1.1)	**ID.SC-1: Gestión de riesgos de la cadena de suministro**	El vector fue una actualización de software de un tercero (M.E.Doc). NIST exige evaluar la seguridad de los proveedores. Una política de "Sandboxing" para actualizaciones de terceros habría detectado el comportamiento inusual antes de la instalación.
GDPR (Reglamento General de Protección de Datos)	**Art. 32: Seguridad del tratamiento (Disponibilidad y Resiliencia)**	Aunque el enfoque principal es la privacidad, GDPR obliga a las empresas a garantizar la **disponibilidad** de los datos. La incapacidad de recuperar sistemas por falta de backups offline funcionales habría resultado en multas de hasta el 4% de la facturación global bajo el régimen actual.

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.

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