Ataque de Ransomware NotPetya contra Maersk (2017)

Un análisis del ciberataque que paralizó al gigante del transporte marítimo

Consultoría de Ciberseguridad Sualba

Octubre 2025

Introducción al Incidente

27 de junio de 2017

¿Qué fue NotPetya?

Un **ransomware destructivo** (wiper) que se propagó globalmente, afectando a múltiples organizaciones, con Maersk como una de las víctimas más notables.

Origen del ataque

Ucrania, a través de una actualización comprometida del software de contabilidad **MeDoc**, ampliamente utilizado en el país.

Métodos de propagación

Explotación de la vulnerabilidad **EternalBlue** en el protocolo SMB de Windows y herramientas de robo de credenciales como **Mimikatz**.

Objetivo real

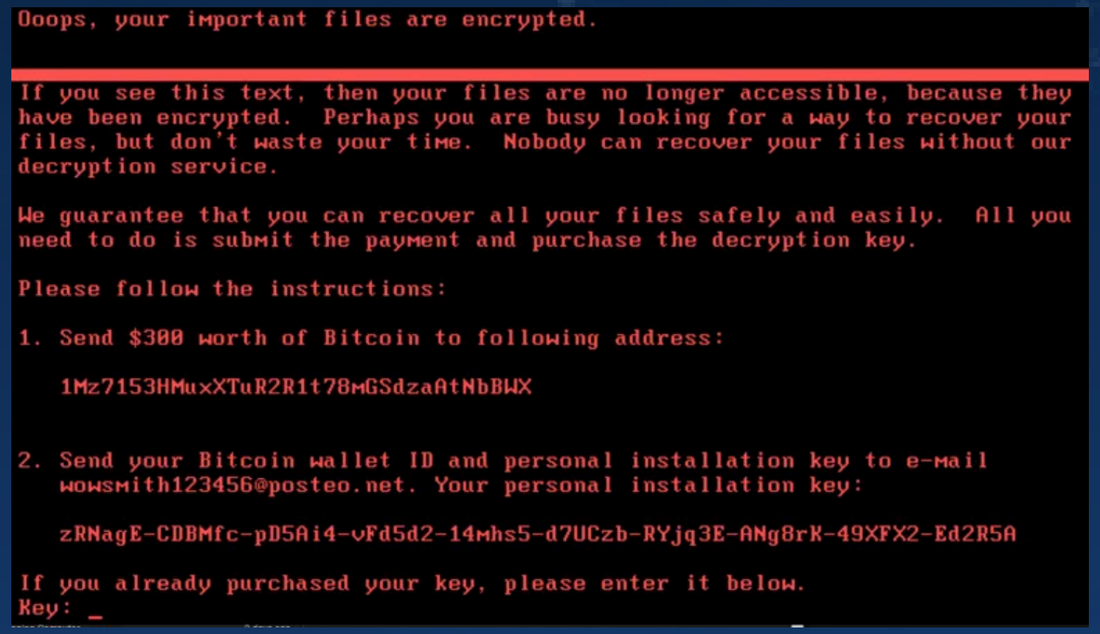
A diferencia de un ransomware tradicional, NotPetya fue diseñado para **destruir datos**, no para obtener rescates. Destruía la tabla maestra de archivos (MFT), haciendo imposible la recuperación.

Impacto en Maersk

- Paralización de puertos y terminales en varios continentes
- 45.000 estaciones de trabajo y 4.000 servidores afectados
- Pérdidas estimadas entre 250-300 millones de dólares

Anatomía del Ataque

Fases del ataque NotPetya



Impacto en la Triada CIA

- **Confidencialidad:** Riesgo de exposición de datos sensibles
- **Integridad:** Destrucción de la tabla maestra de archivos (MFT)
- **Disponibilidad:** Caída completa de sistemas críticos

1 Reconocimiento

Identificación de vulnerabilidades en software ampliamente utilizado (MeDoc en Ucrania).

2 Intrusión

Malware ingresó mediante una actualización de software legítima comprometida, distribuyéndose a través de los canales oficiales.

3 Escalada de Privilegios

Uso de herramientas como Mimikatz para robar credenciales administrativas y obtener acceso privilegiado.

4 Movimiento Lateral

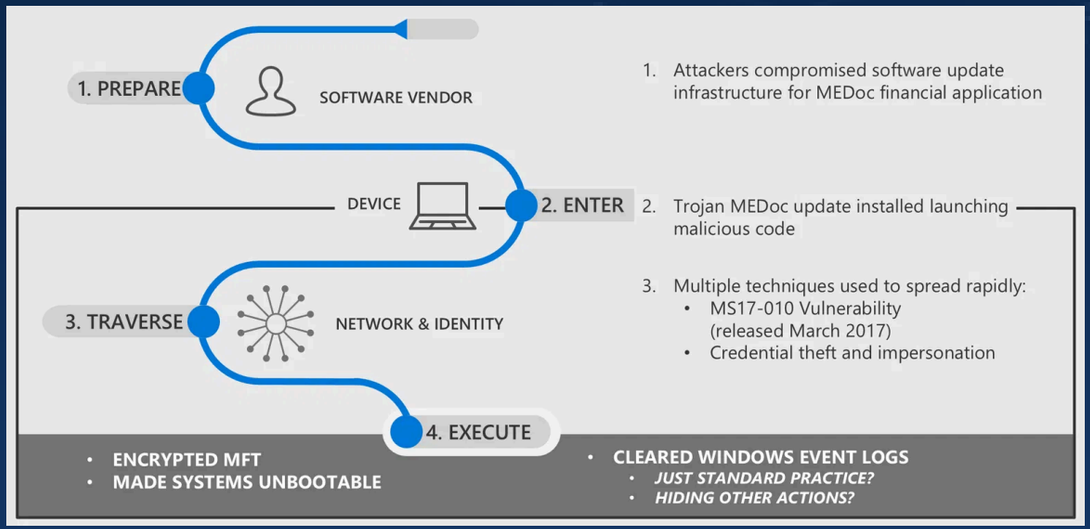
Explotación del protocolo SMB sin parches (vulnerabilidad EternalBlue) para propagarse de un sistema a otro.

5 Ejecución del Objetivo

Cifrado y destrucción de sistemas, inutilizando servidores y estaciones de trabajo de forma permanente.

Vulnerabilidades Explotadas

Fallos de seguridad aprovechados



Detección tardía

El ataque fue identificado cuando sus efectos ya eran masivos, lo que demuestra que los mecanismos de detección existentes eran reactivos y no preventivos.

Protocolos obsoletos (SMB v1)

Sistemas sin aplicar los parches de seguridad que Microsoft ya había publicado para la vulnerabilidad EternalBlue.

Gestión débil de credenciales

Credenciales administrativas almacenadas sin medidas de protección adecuadas, facilitando el uso de herramientas como Mimikatz.

Ausencia de segmentación de red

Permitió que el malware se moviera libremente entre áreas críticas de la organización, maximizando el impacto del ataque.

Defensas perimetrales insuficientes

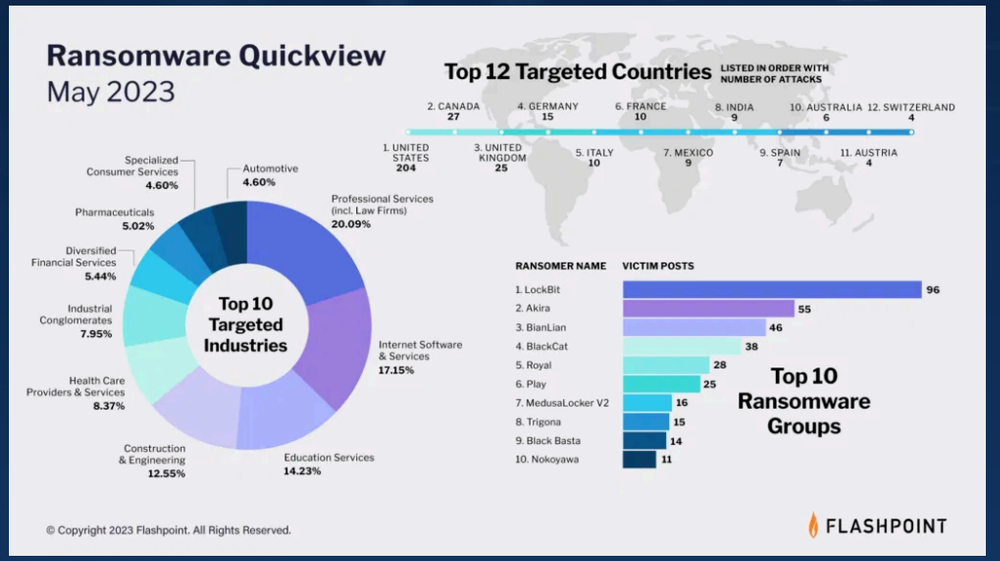
Firewalls no configurados para inspeccionar tráfico lateral ni detener movimientos internos maliciosos.

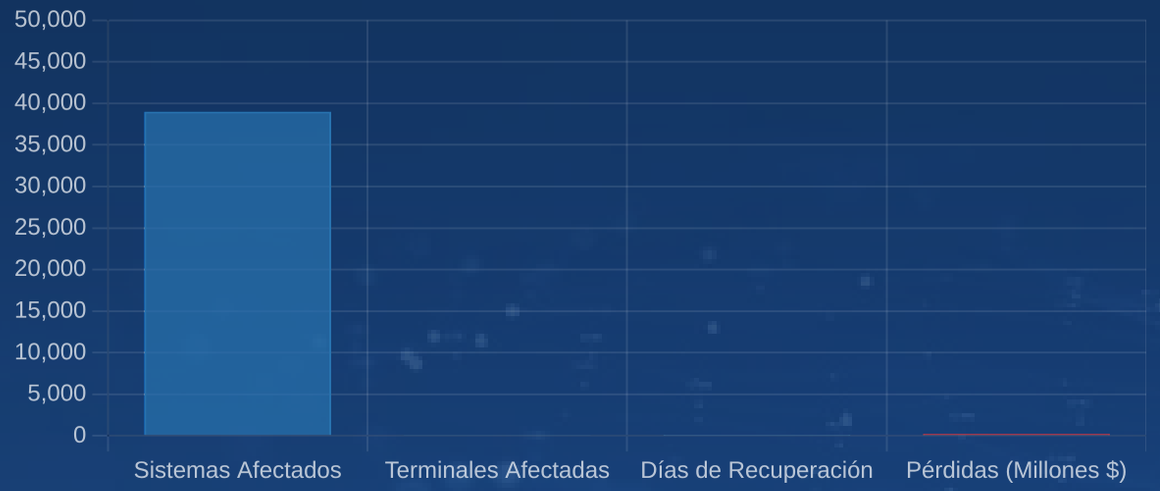
Carencia de detección proactiva

Falta de sistemas de prevención de intrusiones (IPS) y de políticas Zero Trust que hubieran limitado los accesos no autorizados.

Impacto del Ataque

Consecuencias en Maersk y la cadena global





Impacto Operativo

- 45.000 estaciones de trabajo y 4.000 servidores inutilizados
- Paralización de operaciones en 76 puertos y terminales globales
- Restablecimiento completo requirió 10 días

Impacto Económico

- Pérdidas directas estimadas entre 250-300 millones de dólares
- Costes de restauración de sistemas y penalizaciones por incumplimientos

Impacto en Infraestructuras Críticas

- Afectación al comercio mundial y cadenas de suministro globales
- Demostró la vulnerabilidad de sectores estratégicos ante ciberataques

Impacto Reputacional

- Daño a la imagen de Maersk como líder mundial en transporte marítimo
- Pérdida temporal de confianza de clientes, inversores y socios

Acciones de Contención

Respuesta inmediata al ataque

Desconexión inmediata de redes

Desconexión controlada de segmentos afectados e interrupción de conexiones entre centros de datos para romper la cadena de propagación.

Configuración de firewalls

Implementación de reglas en firewalls NGFW para bloquear el tráfico malicioso asociado al protocolo SMB.

Segmentación de red

Aislamiento de sistemas críticos en VLANs independientes e implementación de controles bajo el principio de Zero Trust.

Protocolo de Respuesta a Incidentes

Detección
Identificación de actividad maliciosa en la red

Activación de IRP
Activación de protocolos de gestión de incidentes

Coordinación global
Coordinación de equipos de TI y ciberseguridad

Colaboración externa
Contacto con CERTs y proveedores de seguridad

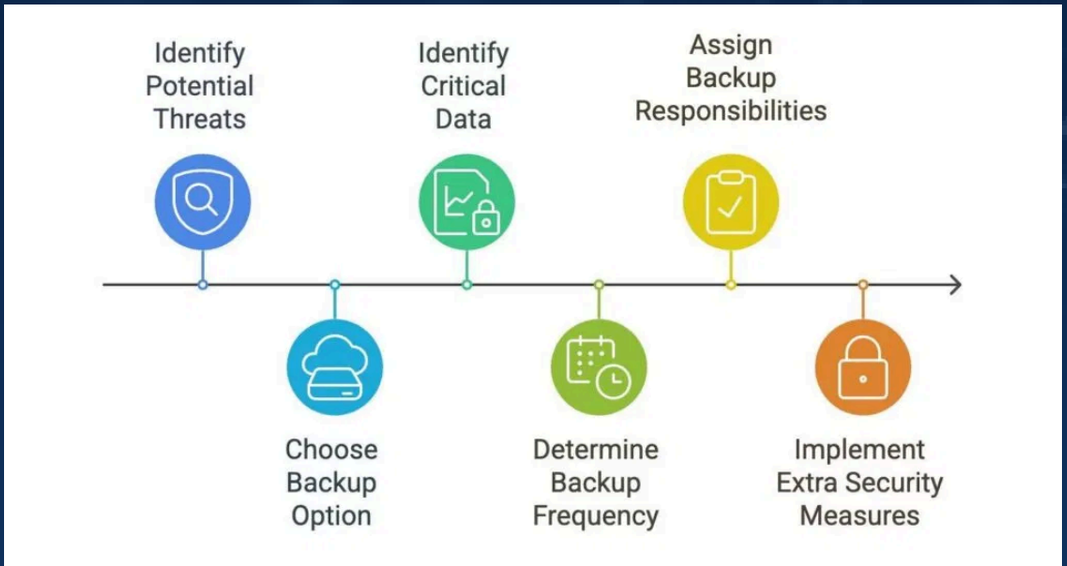
Monitorización reforzada
Despliegue de sensores IDS/IPS adicionales

Resultado de la contención

Las acciones permitieron estabilizar la situación en un plazo relativamente corto, evitando que toda la infraestructura quedara inutilizada.

Proceso de Recuperación

Caso de referencia internacional



Reconstrucción de infraestructura

Reinstalación completa de 4.000 servidores y 45.000 estaciones de trabajo. El malware había inutilizado la Master File Table (MFT), haciendo imposible la restauración directa.

10	1	76
Días para recuperación	Copia de seguridad viable	Puertos afectados

La copia de seguridad salvadora

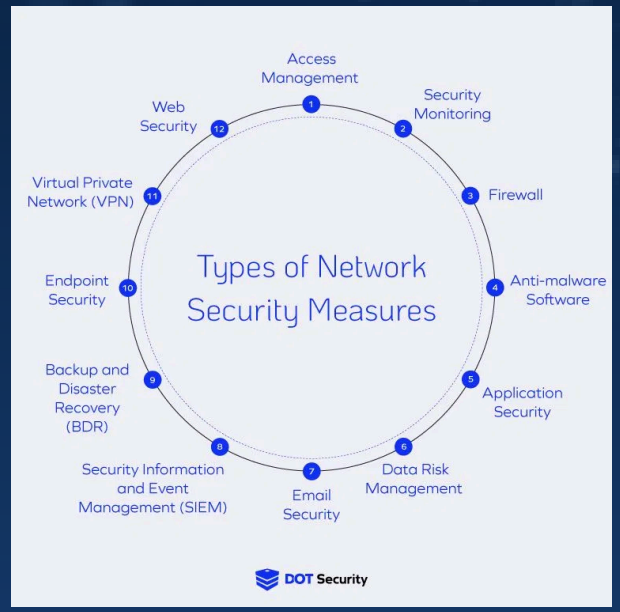
Tras descubrir que gran parte de las copias de seguridad internas estaban comprometidas, se localizó una copia íntegra y no comprometida en una oficina remota en África, lo que permitió iniciar la reconstrucción de toda la red corporativa global.

Cronología de la recuperación

- **Día 1-2: Contención y evaluación**
  Aislamiento de sistemas afectados y evaluación del alcance del daño.
- **Día 3-5: Reconstrucción de infraestructura crítica**
  Priorización de sistemas logísticos y de reservas esenciales.
- **Día 6-9: Restauración progresiva**
  Implementación de nueva arquitectura segmentada y resiliente.
- **Día 10: Operatividad restaurada**
  Restablecimiento de operaciones críticas a nivel global.

Medidas Preventivas

Protección contra ataques similares



Seguridad en Redes Básicas

- Gestión segura de routers y switches (contraseñas robustas)
- Implementación de VLANs para segmentar el tráfico
- Firewalls con listas de control de acceso estrictas

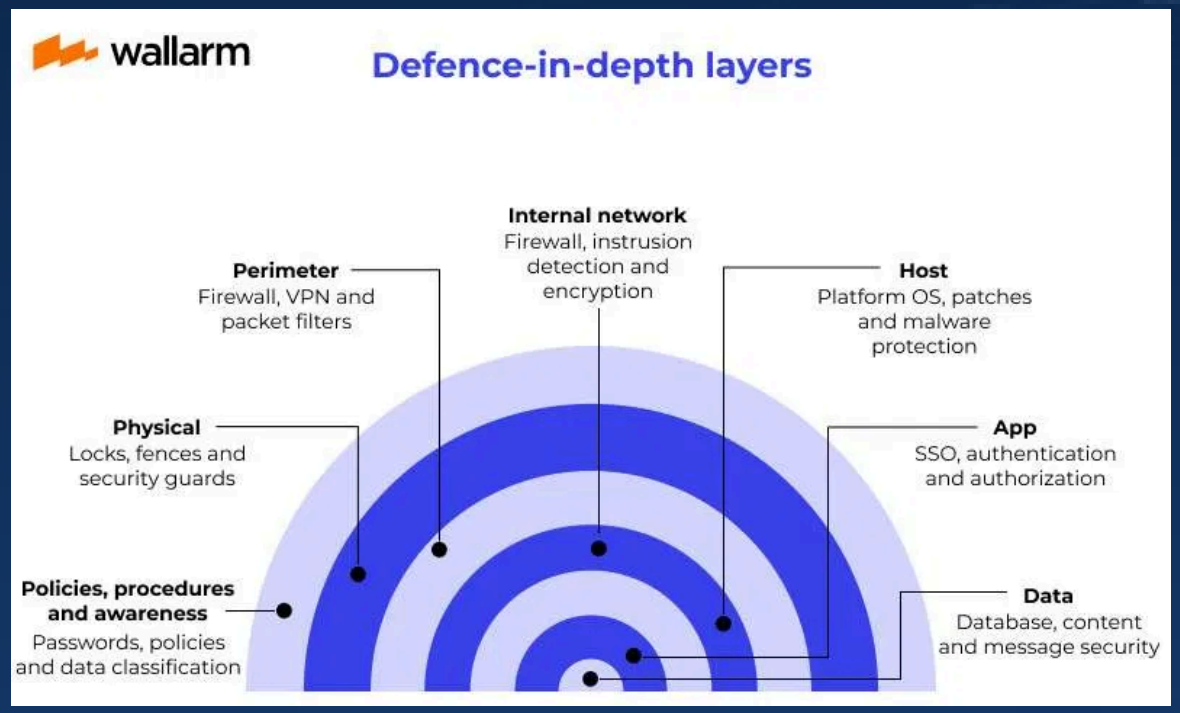
Protección Avanzada de Infraestructuras

- Segmentación de red avanzada entre entornos críticos
- Firewalls de Nueva Generación con inspección profunda
- Sistemas IDS/IPS para monitoreo proactivo

Respaldo y Continuidad

- Copias de seguridad offline e inmutables
- Planes de Recuperación ante Desastres (DRP)
- Estrategias de Continuidad de Negocio

Conclusiones



> *"El ataque NotPetya demostró que incluso las organizaciones más grandes y con mayores recursos pueden ser vulnerables si no implementan una estrategia de seguridad en profundidad y planes de continuidad de negocio adecuados."*

Punto de inflexión para la ciberseguridad global

El ataque NotPetya marcó un antes y un después en la percepción de las amenazas cibernéticas, revelando la vulnerabilidad de infraestructuras críticas y la necesidad de una defensa robusta a nivel global.

La defensa en profundidad es una necesidad

No es un principio teórico, sino una necesidad ineludible en el panorama actual de amenazas. La segmentación de red, actualizaciones de parches y monitorización proactiva son fundamentales.

Importancia de la resiliencia

La capacidad de Maersk para recuperarse en 10 días fue notable, pero el coste económico y reputacional fue inmenso. Los planes de recuperación ante desastres (DRP) y continuidad de negocio (BCP) deben ser sólidos y probados periódicamente.

Colaboración internacional

La colaboración entre organizaciones, CERTs nacionales y proveedores de seguridad es crucial para combatir ciberamenazas sofisticadas que trascienden fronteras y sectores.