Maersk NotPetya Cyberattack (2017)

Jeshiah Babumba | CYSE 200T | April 23 2026.

BLUF

The 2017 NotPetya attack on Maersk caused massive global disruption by exploiting unpatched systems, leading to billions in damages and highlighting the importance of patch management, network segmentation, and cyber resilience.

What Happened?

A destructive malware attack (NotPetya) spread globally and crippled Maersk's shipping operations.

June 27, 2017
Attack begins

Hours Later...
Systems fail worldwide

24 hours...
Operations shut down

Days later...
Ports unusable

Weeks...
Recovery begins

Impact of the Breach

45,000 PCs destroyed **4,000 servers wiped** **130+ countries affected**

Global shipping shutdown Supply chain disruption

$300 MILLION LOSS

One of the most disruptive cyberattacks in history

How Did It Happen?

Attack Vector

- Compromised software update (MeDoc)

Attack Methods

- EternalBlue exploit
- Rapid network spread

Weaknesses

- Unpatched systems
- No network segmentation
- Over-trusted internal access

Mitigation strategies

Security Fixes

- Patch systems regularly
- Use endpoint detection (EDR)
- Maintain offline backups

Defense Strategy

- Network segmentation
- Zero Trust model
- Secure supply chain
- Incident response planning

Conclusion

The Maersk NotPetya attack proved that a single vulnerability can disrupt global infrastructure. Strong cyber hygiene, system updates, and layered defenses are critical to preventing future large-scale cyberattacks.