# **NotPetya / M.E.Doc Supply Chain Attack (2017)**

### **1. Core Issue**

The NotPetya attack was a **weaponized supply chain compromise**. Attackers infiltrated the update servers of **M.E.Doc**, a Ukrainian accounting software vendor, and delivered malicious updates containing the NotPetya malware. Although it masqueraded as ransomware, its true purpose was **destructive sabotage**, causing irrecoverable system damage. The core issue was the **exploitation of trusted financial software used by most Ukrainian businesses**.

### **2. Who Was Attacked**

The entry point was **M.E.Doc**, a widely used Ukrainian tax accounting application. Attackers compromised its update mechanism to deliver malware directly to thousands of businesses that relied on it for regulatory compliance.

### **3. Who Was Affected**

* **Primary victims**: Ukrainian businesses, banks, energy companies, airports, and government offices.
* **Collateral victims**: Global companies with Ukrainian operations, including **Maersk (shipping), Merck (pharmaceuticals), FedEx (logistics), and Rosneft (oil)**.
* The attack spiraled beyond Ukraine, creating worldwide disruption with damages estimated at **over $10 billion**, making it one of the most destructive cyberattacks in history.

### **4. Exploit Chain Details**

1. **M.E.Doc Breach** – Attackers compromised the vendor’s update servers.
2. **Malware Injection** – Trojanized updates containing the NotPetya wiper masquerading as ransomware were signed and distributed.
3. **Execution** – Once installed, the malware overwrote the Master Boot Record (MBR) and encrypted the Master File Table (MFT), rendering systems inoperable.
4. **Propagation** – Used **EternalBlue (SMBv1 exploit)** and **Mimikatz-like credential harvesting** to spread laterally.
5. **Destruction** – Files were not recoverable; even ransom payments could not restore systems.

### **5. Prevention / Protection Steps**

* **Vendor Vetting**: Closely evaluate critical financial/regulatory software vendors.
* **Patch Management**: Apply SMB-related patches promptly (EternalBlue had fixes prior to the attack).
* **Network Segmentation**: Isolate financial systems from production networks.
* **Incident Playbooks**: Maintain backups offline and rehearse ransomware response drills.

### **6. Fixes & Vendor Response**

* M.E.Doc was forced to **shut down its update servers** after the breach.
* Microsoft and security vendors issued detection and recovery guidance.
* Global governments condemned the attack, attributing it to Russian state-sponsored groups.

### **7. If No Fix Available**

* Isolate compromised networks immediately.
* Rebuild systems from clean images or backups.
* Rotate all credentials due to potential credential theft.
* Migrate away from compromised vendor tools until security assurance is provided.

### **8. Reference Material**

* Wired – “The Untold Story of NotPetya, the Most Devastating Cyberattack in History”:  
   https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
* Microsoft Security Response Center – Guidance on NotPetya Malware:  
   https://msrc.microsoft.com/blog/2017/06/guidance-for-responding-to-the-petya-ransomware-attack/
* US-CERT Alert (TA17-181A) – Petya Ransomware:  
   https://www.us-cert.gov/ncas/alerts/TA17-181A
* Kaspersky Securelist – ExPetr/NotPetya:  
   https://securelist.com/exploring-petya-notpetya/78902/
* Talos Intelligence – M.E.Doc compromise analysis:  
   https://blog.talosintelligence.com/2017/07/the-medoc-connection.html
* ENISA Threat Landscape – Supply Chain Attacks Report 2021:  
   https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

### **9. Further Reading**

* NCSC-UK – “NotPetya Cyber Attack Overview”:  
   https://www.ncsc.gov.uk/report/summary-of-notpetya
* MITRE ATT&CK – T1195: Supply Chain Compromise:  
   https://attack.mitre.org/techniques/T1195/
* SANS Institute Analysis – Lessons Learned from NotPetya:  
   https://www.sans.org/blog/lessons-learned-from-notpetya/
* CrowdStrike Global Threat Report – NotPetya Analysis:  
   https://www.crowdstrike.com/global-threat-report/
* FireEye – NotPetya Technical Details and Mitigations:  
   https://www.fireeye.com/blog/threat-research/2017/07/notpetya-technical-analysis.html

### **10. Tooling**

* Microsoft Defender for Endpoint – Ransomware detection and response:  
  <https://www.microsoft.com/en-us/security/business/threat-protection/microsoft-defender-endpoint>
* Sysmon (Microsoft Sysinternals) – Monitoring lateral movement and credential theft:  
   https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon
* Zeek – Detecting SMB lateral movement:  
   https://zeek.org/
* Snort / Suricata IDS rules for NotPetya indicators:  
   https://www.snort.org/downloads
* YARA rules for NotPetya samples:  
  <https://github.com/Yara-Rules/rules>
* VirusTotal – Detection and file analysis:  
   https://www.virustotal.com/