Incident Response Report: WannaCry Ransomware Attack (2017)

---

1. Incident Classification

- **Incident Type:** Ransomware outbreak / Malware attack
- **Severity:** Critical — global impact affecting over 230,000 systems in 150 countries
- **Attack Vector:** Exploitation of Microsoft Windows SMB vulnerability via EternalBlue (CVE-2017-0144)
- **Impact:** System encryption, operational disruption, financial loss, and data inaccessibility
- **Targets:** Outdated and unpatched Windows systems, including organizations such as the UK National Health Service (NHS) and FedEx

---

2. Incident Detection

- Initial indicators included unusual network scanning on SMB port 445 and detection of anomalous SMB traffic patterns.
- Security systems generated alerts for multiple attempts to exploit SMB vulnerabilities and presence of ransomware-related files (e.g., ransom notes named `@WanaDecryptor@.exe`).
- End-users reported being unable to access files, with ransom demands displayed on affected machines.

---

3. Incident Response Steps Taken

Step 1: Identification and Containment

- Immediate isolation of infected endpoints to prevent lateral spread.
- Network segmentation implemented to restrict vulnerable subnet communications.
- Disabled SMB version 1 protocol to block the EternalBlue exploit vector.
- Blocked TCP port 445 on firewalls to reduce SMB traffic exposure.

Step 2: Eradication

- Deployed anti-malware tools to remove ransomware binaries from infected systems.
- Applied Microsoft security patch MS17-010 addressing the SMB vulnerability.
- Conducted network-wide scanning to identify and remediate additional infections.

Step 3: Recovery

- Restored affected systems and data from verified, clean backups to avoid ransom payment.
- Verified system integrity before reintegrating hosts into the production network.
- Maintained increased monitoring for residual threats post-restoration.

Step 4: Post-Incident Analysis

- Performed root cause analysis to determine infection vectors and propagation methods.
- Reviewed and improved patch management and vulnerability mitigation processes.
- Updated incident response plans based on lessons learned from the event.

---

4. Lessons Learned

- Timely patch management is essential to prevent exploitation of known vulnerabilities.
- Disabling or restricting legacy protocols such as SMB v1 significantly reduces attack surface.
- Network segmentation effectively limits the spread of malware infections.
- Robust, tested backup strategies enable recovery without paying ransom demands.
- Proactive network monitoring and alerting facilitate early detection and response.
- User education improves awareness and reduces accidental infections.

---

5. Evidence of Functionality

- SIEM detection rules were implemented to monitor for SMB exploit attempts and ransomware indicators, triggering high-severity alerts.
- Alert prioritization workflows ensured rapid escalation and activation of incident response procedures.
- Incident response steps and decisions were documented in a centralized case management system.
- Logs from security monitoring tools showed detection of EternalBlue scanning activity and ransomware artifacts.
- Network controls, including disabling SMB v1 and firewall rules blocking port 445, were applied as containment measures.