CSC429
Comprehensive Analysis of WannaCry Ransomware Attack

Prepared by:
Abdulrahman Alateeq
Mohammed Aljalajil
Abdulrahman Almayman

Summary of the Incident

What Happened?
The WannaCry ransomware attack exploited a vulnerability in Microsoft Windows systems using the **EternalBlue exploit**. It encrypted files on infected computers, locking them until a ransom in **Bitcoin** was paid.

How Did It Spread?
WannaCry combined **ransomware tactics** with **worm-like capabilities**, allowing it to spread rapidly across networks without requiring user interaction.

Major Impact:

- The **UK's National Health Service (NHS)** was severely disrupted, with 80 trusts affected. This led to canceled surgeries, delayed care, and diverted emergency patients.
- Global corporations like **FedEx**, **Telefónica**, and **Deutsche Bahn** also faced major operational setbacks.

Real-World View of WannaCry's Effects

Timeline

Mar. 2017	Apr. 2017	12 May 2017	13 May 2017	14 May 2017
Microsoft discovered a vulnerability in the SMB protocol and released the critical update MS17-010.	A hacker group, The Shadow Brokers, leaked EternalBlue, a tool designed to exploit the SMB flaw.	WannaCry ransomware began spreading worldwide, locking systems and demanding payment in Bitcoin.	Microsoft released emergency patches for unsupported systems (Windows XP, 8, and Server 2003).	CISA issued an alert urging organizations to patch systems and disable SMBv1.

Incident Analysis (Attack Methods)

Exploited the **MS17-010 vulnerability** in the SMB protocol of Microsoft Windows.

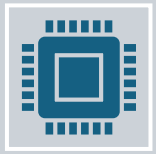
Used the **EternalBlue exploit**, a leaked NSA tool, to gain unauthorized access to systems.

Leveraged **DoublePulsar** backdoor to install ransomware undetected.

Spread like a worm, infecting networks without user interaction.

Incident Analysis (Root Causes)

Unpatched Systems: Many organizations failed to apply Microsoft's critical security update (MS17-010).



Outdated Software: Older systems like Windows XP were particularly vulnerable due to lack of updates.

Lack of Network Segmentation: Allowed the ransomware to spread rapidly across entire networks.

Incident Analysis (Impacts)

Financial: Estimated global losses of up to $4 billion.

Operational: NHS faced canceled surgeries, delayed care, and ambulance diversions. Companies like FedEx and Renault experienced production halts.

Reputational: Organizations lost trust for failing to secure sensitive data.

Legal: Some entities faced legal actions for non-compliance with data protection laws.

Comparative Insights

Similar Attack: NotPetya (2017):

Also leveraged EternalBlue and focused on spreading across networks.

Unlike WannaCry, NotPetya aimed to destroy data rather than collect ransom.

Patterns Identified:

Both exploited vulnerabilities in unpatched systems.

Relied on NSA-leaked hacking tools.

Highlighted the dangers of relying on outdated or unprotected software.

Mitigation Strategies

1

Keep Software Updated:

- Apply security patches promptly, such as Microsoft's **MS17-010**, to prevent known exploits.

2

Implement Reliable Backups:

- Regularly back up critical data and store it offline or in separate systems to avoid ransomware impact.

3

Network Segmentation:

- Divide networks into smaller sections with limited communication to minimize the spread of attacks.

4

Educate Employees:

- Conduct regular training on recognizing phishing emails and safe internet practices to reduce human error.

5

Develop Incident Response Plans:

- Create and test step-by-step guides to respond to attacks quickly and minimize damage.

6

Collaborate with Cybersecurity Experts:

- Partner with organizations like CISA for threat intelligence and best practices.

Thank You