Title:

WannaCry Ransomware Attack (2017)

Introduction:

In May 2017, the world experienced one of the most widespread and damaging ransomware attacks in cybersecurity history — the **WannaCry ransomware attack.

Within just a few hours, this attack infected more than 200,000 computers across 150+ countries, disrupted hospitals, transport systems, and global businesses, and highlighted severe vulnerabilities in unpatched Windows systems.

What made WannaCry so dangerous wasn't just the ransomware itself, but how quickly it spread using a leaked NSA exploit known as **EternalBlue**.

In this report, I'll break down how **WannaCry worked**, **why it succeeded**, and **what lessons we can learn** from it, even if you're not from a technical background.

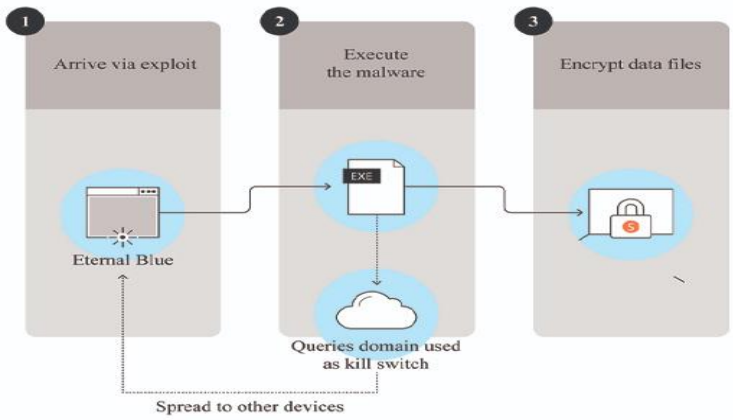
How the Attack Worked:

The attack exploited a critical vulnerability in the **SMBv1 (Server Message Block)** protocol, specifically **port 445**, which is used for file and printer sharing across Windows networks.

The vulnerability (known as **MS17-010**) allowed **remote code execution** using a leaked NSA exploit called **EternalBlue**. Here's how the chain of infection worked:

- **Scan the network** for vulnerable systems (port 445 open).
- **Exploit** the vulnerability using EternalBlue.
- **Drop and run the WannaCry ransomware payload**.
- **Encrypt files** on the victim's computer.
- **Spread to other machines** on the same network automatically.

Interestingly, the ransomware also attempted to connect to a **specific domain**. If this domain responded, the malware would stop (this was the built-in **kill switch**). When the attack was first launched, the domain didn't exist, so the malware spread freely until a security researcher registered the domain, stopping the attack.



After Infection: What WannaCry Did:

Once a system was infected, WannaCry did the following:

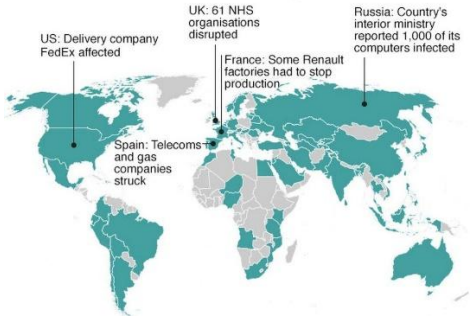
- Encrypted files using **AES-128 encryption**, then encrypted the AES key using **RSA**.
- Appended the file extension .WNCRY to encrypted files.
- Displayed a **ransom note** with a Bitcoin address, demanding $300–$600.
- Set a **72-hour timer** with a threat of file deletion if the ransom wasn't paid.
- Provided a fake "Decrypt" button (but decryption rarely worked even after payment).

Global Impact:

The attack affected **over 200,000 computers across 150+ countries** in a matter of hours. High-profile victims included:

- GB **UK's NHS (National Health Service)**: Emergency rooms shut down, appointments cancelled.
- US **FedEx**: Major delivery delays and system outages.
- ES **Telefonica**: Corporate network crippled.
- FR **Renault**: Factory production halted.

The total estimated damage ranged from **$4 billion to $8 billion USD**. The attack showed how vulnerable global systems were, especially those that hadn't installed security patches.



How It Was Stopped:

The attack was accidentally stopped by a 22-year-old British researcher **Marcus Hutchins**, who noticed the malware was trying to contact a strange domain name.

He registered the domain himself — and to his surprise, this act triggered the **kill switch**, instantly stopping WannaCry from spreading further.

However, systems already infected remained encrypted unless they were restored from backups or decrypted using tools developed later.

CIA Triad Analysis (Confidentiality, Integrity, Availability):

CIA Principle	Was It Affected?	How?
Confidentiality	Yes	Files were accessed and encrypted by attackers.
Integrity	No	Files were not modified, just locked.
Availability	Yes	Systems and files became unusable.

WannaCry clearly violated **Confidentiality and Availability** — core pillars of system security.

Lessons Learned:

The WannaCry attack highlighted critical cybersecurity weaknesses:

- **Unpatched systems are dangerous**: Microsoft released a patch (MS17-010) *before* the attack, but many systems didn't install it.
- **Network ports must be secured**: Leaving port 445 open was a big mistake.
- **Backup is essential**: Systems with offline backups recovered quickly.
- **Kill switches are powerful**: Malware can be stopped if we understand its logic.

Conclusion:

WannaCry changed how the world thinks about cybersecurity. It showed that:

- A single exploit can cause **global damage**.
- Tools created for espionage can become weapons.
- Basic practices like **patching, updating, and backing up** are crucial.

Understanding WannaCry is not just about analysing malware — it's about learning from a real event that impacted hospitals, factories, and people's daily lives.

References:

- Microsoft Security Bulletin MS17-010
- Europol Press Release on WannaCry
- MalwareTech Blog by Marcus Hutchins
- BBC News, CNN Reports on May 2017