**WannaCry Ransomware Attack**

WannaCry is a ransomware attack that struck in May 2017, impacting over 200,000 computers across 150 countries. The attack exploited a vulnerability in Microsoft Windows, known as **EternalBlue**, which allowed it to spread rapidly across networks without user intervention.

**Key Points**

* **How It Worked**: WannaCry encrypted users' files, rendering them inaccessible, and demanded a ransom payment in Bitcoin to unlock them. The attack exploited a vulnerability in the SMB protocol, which Microsoft had patched in March 2017. However, many systems remained unpatched, leaving them vulnerable.
* **Global Impact**: The attack caused widespread disruption, particularly in sectors like healthcare, where the UK's National Health Service (NHS) saw significant operational issues, leading to the cancellation of appointments and surgeries. Other affected organizations included major corporations like FedEx and Renault.
* **Response**: A cybersecurity researcher inadvertently discovered a "kill switch" that slowed the spread of WannaCry by registering a domain embedded in the malware's code. Microsoft urged users to apply the security patch and issued updates even for unsupported versions of Windows.
* **Lessons Learned**: WannaCry highlighted the critical importance of timely software updates and the need for strong cybersecurity practices. The attack also underscored the global nature of cybersecurity threats, prompting many organizations to reassess their security strategies.