WannaCry Attack to NHS 12May 2017

In this section you should look at the events that occurred when the NHS was infected with   
the WannaCry worm. This is where you establish what happened! Some questions that   
would be useful to ask yourself when looking at this section could be:  
• What is WannaCry?

The WannaCry cyber attack began on the morning of Friday 12 May 2017 and, within a day, was reported by Europol to have infected more than 230,000 computers in at least 150 countries26 27. This global attack quickly became a matter of public concern, with the UK’s national media paying particular attention to the impact and the response of the NHS in England. 2.2. The cybersecurity firm Avast identified WannaCry as one of the broadest and most damaging cyber attacks in history28. The majority of the attacks targeted Russia, Ukraine and Taiwan but Chinese universities, Spanish Telefonica, Russia’s Interior Ministry and global firms like FedEx also reported that they had been impacted alongside the NHS29 . Nissan Motor Manufacturing UK in Tyne and Wear halted production after the ransomware infected some of their systems and Renault stopped production at several sites in an attempt to stop the spread of the ransomware. 2.3. The WannaCry ransomware cryptoworm targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payment in the Bitcoin cryptocurrency. The initial infection was likely through an exposed vulnerable internet-facing Server Message Block (SMB) port30, rather than email phishing as initially assumed31 . 2.4. The work of a cybersecurity researcher, who activated a ‘kill-switch’32 on the evening of Friday 12 May, had the effect of stopping WannaCry infecting further devices. Without this intervention, it is likely that the impact that WannaCry had on services would have been even greater

On Friday 12th May 2017, the [NHS](https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/), was brought to a standstill for several days due to the WannaCry outbreak, affecting hospitals and GP surgeries across England and Scotland.  Although the NHS was not specifically targeted, the global cyber-attack highlighted security vulnerabilities and resulted in the cancellation of [thousands of appointments and operations](https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS-Summary.pdf), together with the frantic relocation of emergency patients from stricken emergency centres. Staff were also forced to revert to pen and paper and use their own mobiles after the attack affected key systems, including telephones.

The WannaCry ransomware exposed [a specific Microsoft Windows vulnerability](https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf), not an attack on unsupported software. Most of the NHS devices infected with the ransomware, were found to have been running the supported, but unpatched, Microsoft Windows 7 operating system, hence the extremities of the cyber-attack. [The ransomware also spread via the internet](https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf), including through the N3 network (the broadband network connecting all NHS sites in England), but fortunately, there were no instances of the ransomware spreading via NHSmail (the NHS email system).

[NHS England reported](https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS-Summary.pdf) at least 80 out of the 236 trusts were affected in addition to 603 primary care and other NHS organisations, including 595 GP practices.  The Department, NHS England and the National Crime Agency reported that no NHS organisation paid the ransom, but the Department does not know how much disruption to services cost the NHS [although estimates total £92m](https://www.digitalhealth.net/2018/10/dhsc-puts-cost-wannacry-nhs-92m/)

• What devices did the worm affect?  
• What was the impact the worm had on the NHS?  
• What was the aftermath of the infection?  
• What does the NHS incident demonstrate about the importance of Network and   
Cyber-Security?