**A large ransomware attack due to vulnerabilities found in Microsoft operating systems**

Over the past few years, technology has made many great advances but also suffered some spectacular failures.

There have been ransomware attacks and data leakages that have affected some of the biggest companies and millions of customers around the world. Let's take a look back at one of the worst software failures in recent history.

In May 2017, a large ransomware attack called WannaCry hit NHS England and various organisations in the UK and around the world.

Once your computer has been affected, it locks up the files and encrypts them in a way that you cannot access them anymore. It then demands payment in bitcoin in order to regain access.

Security experts warn there is no guarantee that access will be granted after payment. Some ransomware that encrypts files ups the stakes after a few days, demanding more money and threatening to delete files altogether.

The attack was due to vulnerabilities found in Microsoft operating systems installed in millions of computers around the world.

According to Microsoft, the Windows versions that were vulnerable to the attack were versions which were no longer supported by Microsoft such as Windows 8 and Windows XP, which the NHS trusts and affected companies seemed to be running.

An estimated 75,000 computers in 99 countries have been infected by what is being called the biggest attack of its kind in history.

Hospitals and doctors' surgeries in parts of England were forced to turn away patients and cancel appointments after they were infected with the ransomware, which scrambled data on computers and demanded payments of $300 to $600 to restore access. People in affected areas were being advised to seek medical care only in emergencies.

The attack exploited a Windows networking protocol to spread within networks, and while Microsoft released a patch nearly two months ago, it’s become painfully clear that patch didn’t reach all users.

What has Microsoft done to tackle it?

The company published an emergency XP patch over the weekend to protect against the ransomware, but it was too late for NHS and countless other victims.

How to stop it spreading

A cybersecurity researcher have discovered a "kill switch" that can prevent the spread of the WannaCry ransomware - for now. Registering a domain name used by the malware stops it from spreading."Essentially they relied on a domain not being registered and by registering it, we stopped their malware spreading,"