Ransomware - WannaCry

HOW RANSOMWARE WORKS

Malicious code blocks access to the data in your computer

You receive an infected file (typically attached to an email or a URL); if you open it, you've let malicious code into your computer

Encryption key locks all your data

Without the key, all the files on your computer are locked

Command and control server

In a matter of minutes, your files are out of reach

When you try to open a file, a message appears demanding a ransom

Payment in cryptocurrency bitcoin helps hackers cover their tracks

If you don't pay

- Your encrypted files are lost

If you pay

- You send the ransom money to an anonymous recipient hiding in the 'Darknet'
- Normally, you get the key to the data in an hour or so

WHAT IS RANSOMWARE

- The malware shutting down computers worldwide is **known as WannaCry** and variants of that name
- This type of malware is **called ransomware as it first scrambles a victim's files and then demands a payment** to unscramble them

HOW DOES IT WORK

- WannaCry seems to be deployed via a worm — a programme that spread by itself between computers
- Once malware is inside an organisation, it will find vulnerable machines and infect them too
- Infections reported in 150 countries, including Russia and China. In UK, hospital systems badly hit

HOW THE HACKERS STRUCK

- The ransomware exploits a weakness in Microsoft Windows systems that was identified by the US National Security Agency and given the name 'EternalBlue'
- But NSA's code was among a cache stolen by a hackers' group known as The Shadow Brokers, who then attempted to sell it in an online auction
- The hackers' group later made the tools freely available in April, saying it was a "protest" against US President Donald Tump
- Microsoft had by then already released a software upgrade fixing the issue
- But not all users were prompt in installing the upgrades

How They FELL FOR IT

- Cyber extortionists tricked victims into opening malicious attachments to spam emails that appeared to contain legitimate files
- The ransomware encrypted data on the computers, demanding payments of $300 to $600 via the digital currency bitcoin to restore access

GOVT AGENCIES/COMPANIES AFFECTED GLOBALLY

- Britain's National Health Service (NHS)
- Russian interior ministry (about 1,000 computers)
- Spain's communications giant Telefonica
- Spain's power firm Iberdrola
- FedEx in the US
- Japanese carmaker Nissan's plant in England
- German rail operator Deutsche Bahn
- French automaker Renault halted production at several sites in Europe

GLOBAL IMPACT

- A cyber security firm said it had seen 2,00,000 cases of the Wanna Cry attack
- Asian nations also hit hard by the ransomware