

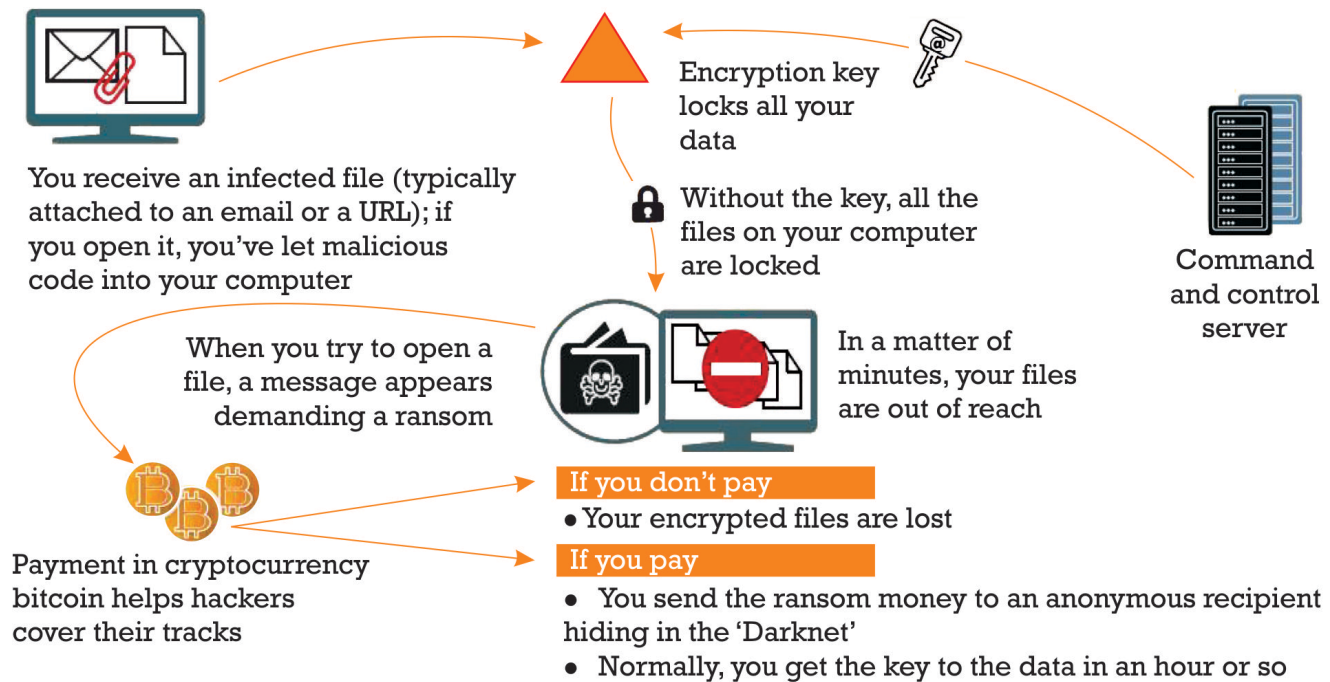


Ransomware - WannaCry



HOW RANSOMWARE WORKS

Malicious code blocks access to the data in your computer



WHAT IS RANSOMWARE	HOW THE HACKERS STRUCK		GOVT AGENCIES/COMPANIES AFFECTED GLOBALLY
<ul style="list-style-type: none"> ❖ 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 	<ul style="list-style-type: none"> ❖ 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 	<ul style="list-style-type: none"> ❖ The hackers' group later made the tools freely available in April, saying it was a "protest" against US President Donald Trump ❖ Microsoft had by then already released a software upgrade fixing the issue ❖ But not all users were prompt in installing the upgrades 	<ul style="list-style-type: none"> ❖ 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
HOW DOES IT WORK	How They FELL FOR IT		GLOBAL IMPACT
<ul style="list-style-type: none"> ❖ 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 	<ul style="list-style-type: none"> ❖ 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 		<ul style="list-style-type: none"> ❖ 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

