The PDF files were encrypted with the ransomware called WannaCry. This ransomware encrypts files on a computer and demands payment in bitcoin to decrypt them. This attack has impacted more than 200,000 victims in over 150 countries.

WannaCry is a type of malware called ransomware that prevents or limits users from accessing their computer files until a ransom is paid to unlock them; it infects computers by sending out spam emails that contain malicious attachments or links. The WannaCry ransomware encrypts files on infected computers and then spreads itself using a vulnerability in the Server Message Block (SMB) protocol. The SMB protocol is used by Windows computers to share files, printers and serial ports and is commonly found in Windows operating systems. Microsoft released a patch for this vulnerability (MS17-010) in March 2017, but the attackers spread it using an exploit before most users had time to apply the patch.

WannaCry Ransomware has impacted more than 200,000 victims in over 150 countries around the world so far. The most severely affected countries are Russia, Ukraine, India, Taiwan, Japan, Indonesia. The WannaCry attack has been called the worst ever in terms of damage. It has disrupted hospitals, schools, banks, even the UK's National Health Service.

On 16 May 2017, Microsoft publicly announced that its security team had contained the attack after it affected systems in over 150 countries.

A "WannaCrypt" ransom note arrived with an email claiming to contain a locked file. The letter said it came from "Shadow #1" and demanded $300 in Bitcoin, or $300 in U.S. dollars paid to an address in South America or $600 worth of Bitcoin (worth approximately $1700 currently) paid privately (to avoid alerting law enforcement). The note also said the only way the owner of the encrypted files could regain access to them was to pay the ransom. To quickly spread, an email attachment bearing a Microsoft Word document whose macro had been altered to exploit the SMB vulnerability was sent primarily by spammers. The threat arrived through email spam sent primarily in Russia, Ukraine, France, Italy, China, India and Taiwan. It spread primarily to organizations in Europe. Associated spam emails included coupon offers for retail chains such as Tvitera Ltd., which sells computers and other technology products based in Russia; FedEx Freight Corporation based in Memphis; and Autonet which operates an online car sales platform for China-based car dealerships. The Microsoft Malware Protection Center initially identified the worm as ransomware, and noted that it was not a new variant of Petya but "a new ransomware that has not been seen before," and identified a related attempt in February 2017. It advised users who had enabled Windows Error Reporting to check for a description of the WannaCry attack in their reports, which would identify attacks from mid-April 2017. The attack was quickly associated with the NSA's EternalBlue exploit, leaked by the Shadow Brokers group on 14 April 2017 during their series of leaks.

658eeb4e9f3285