# Petya Ransomware Attack

## Why in news?

\n\n

Petya ransomware hit operations at one of the three terminals at Jawaharlal Nehru Port Trust (JNPT)

\n\n

## What is Petya?

\n\n

\n
- Petya is a ransomware, similar to the Wannacry attack.
\n
- It is part of a new wave of cyberattacks that has hit computer servers all across Europe, locking up computer data and crippling enterprise services in the corporate sector.
\n

\n\n

## How exactly does Petya spread?

\n\n

\n
- The ransomware locks up a computer’s files and demands $300 Bitcoins as ransom to unlock the data.
\n
- All data on a computer, network gets encrypted.
\n
- Once the malware infects the computer, it will wait for an hour and then reboots the system.
\n
- After the rebooting, the files are encrypted and the user gets a ransom note on their PC asking them to pay up.
\n
- Users are also warned against switching off their PC during the rebooting process, because it could make them lose their files.

\n

\n\n

## Which are the most affected countries?

\n\n

\n

- The attack is believed to have started in Ukrainian software called **MeDoc.**
  \n
- It is used by many government organisations in the country.
  \n
- According to reports, this is also the reason why **Ukraine was the worst affected.**
  \n
- Over 60% of attacks took place in Ukraine.
  \n
- Russia is second on the list with 30%.
  \n

\n\n

## How can the ransomware attack be stopped?

\n\n

\n

- When it comes to decrypting files, currently there is no solution.
  \n

\n\n

\n

- For now, users who have lost their data can’t really recover it unless they have a backup.
  \n
- There’s no way of getting the decryption key from the hackers, since the email account has been shut down.
  \n
- However, according to a tweet from HackerFantastic, when the system goes in for a reboot, the user should power off the PC.
  \n
- There is no way of stopping the attack from the spreading, given it exploits vulnerabilities in the network.
  \n
- For users, it is best to keep a back up of all their data. Preferably this data

should not be online, and it should be encrypted.
\n
- Users should also not click on email links from suspicious ids or click on links asking for access to personal information.
\n
- Also keep your Windows PC updated with the latest software.
\n

\n\n

\n\n

**Source: LiveMint, Indian Express**

\n

