India, Pakistan hackers trade codes & command in digital firefight

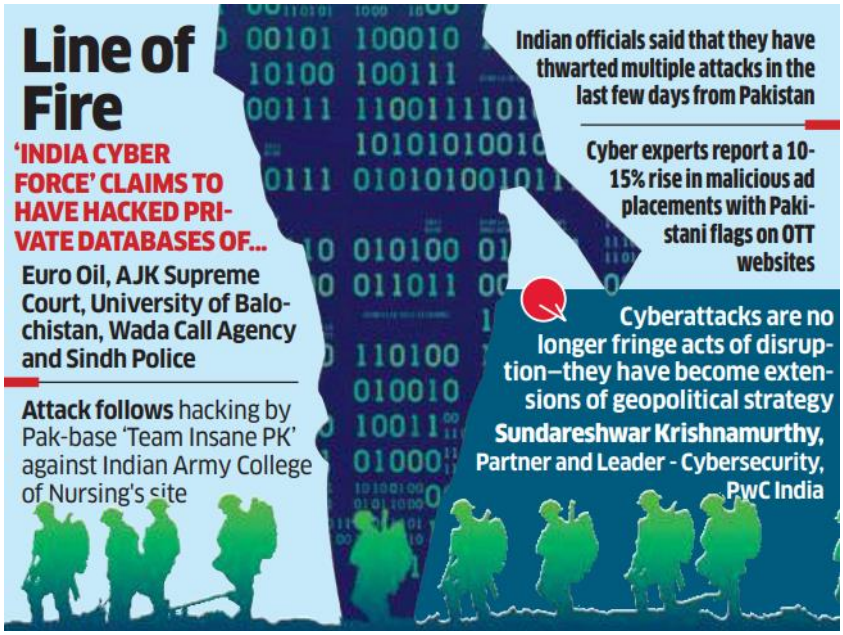
Rising tensions between India and Pakistan since last week's Pahalgam terror attack have spilled over into cyberspace, with multiple groups on either side engaging in hacking and cyberattacks. Indian officials said they have thwarted multiple attacks from Pakistan over the last few days.

Increasing tensions between India and Pakistan since the **Pahalgam terror attack** have extended into cyberspace with groups engaging in hacking and cyberattacks.

Experts expect further spike in these activities as cyberattacks have become "extensions of geopolitical strategy."

Last week, pro-India hacktivist group '**India Cyber Force**' claimed to have hacked Pakistani government and private sector databases of Euro Oil, AJK Supreme Court, University of Balochistan, Wada Call Agency and Sindh Police.

Earlier, Pakistan-based group '**Team Insane PK**' had hacked the Indian Army College of Nursing website and left a provocative message emphasising religious differences and the two-nation theory, echoing recent remarks by Pakistani army chief Asim Munir.



Meanwhile, cybersecurity experts in India have flagged a malicious PDF file titled 'Report & Update Regarding Pahalgam Terror Attack.pdf' circulating online. The document is linked to phishing domains, including indiadefencedepartment[.]link, which mimics official Indian government websites.

Indian officials said they have thwarted multiple attacks from Pakistan over the last few days.

"There has been a sharp escalation in Pakistan-backed cyber campaigns targeting Indian defence, government, and critical infrastructure sectors," said Vishal Salvi, CEO of cybersecurity solutions firm **Quick Heal Technologies**.

Quick Heal's team has identified hacker group APT36 (Transparent Tribe) deploying CrimsonRAT malware through sophisticated phishing attacks along with an RMM tool known as MeshAgent, he said.

"These attacks coincide with hacktivist-driven DDoS surges and website defacements aimed at destabilising public trust," Salvi said.

"We have also observed SideCopy, a sub-group of APT36, broadening its focus to sectors like railways and oil, using novel payloads like CurlBack RAT... They are continuously evolving their tactics to evade detection."

Cyber experts have also reported 10%-15% growth in malicious ad placements with Pakistani flags on OTT websites.

"Cyberattacks are no longer fringe acts of disruption... They have become deliberate extensions of geopolitical strategy," said Sundareshwar Krishnamurthy, partner and leader - cybersecurity at PwC India.

"Every major flashpoint now triggers coordinated digital offensives aimed at undermining a country's

critical infrastructure," he said. Such intrusions weaponise cyberspace to erode public trust when the stakes are highest, Krishnamurthy said.