Border fire draws in digital war, tourists looking for quick bucks

Synopsis
Amid rising India-Pakistan tensions, foreign hacker groups—mainly novice “script kiddies”—are launching low-sophistication cyberattacks on Indian digital infrastructure. While many claims are fake or exaggerated, experts warn of real espionage threats from Pakistan-linked APT36. Attacks include phishing, DDoS, and defacements, often exploiting public emotion and misinformation.

The India-Pakistan conflict has become an opportunity for several ‘digital war tourists’ or foreign hacker groups to seek some quick bucks or drive religious agenda by launching cyberattacks on the national digital infrastructure.

Cyber researchers have identified an army of state/non-state actors like Moroccan Soldiers, Team R70 (Russia) Lulzsec Arabs (the Middle East), Islamic

Hacker Army (Iraq), Sylhet Gang SG (Bangladesh) and Team Azrael-Angel of Death (Palestine) claiming to deface websites and breach sensitive data from several Indian government and private organisations in the past week, cybersecurity experts told ET.

However, these are “script kiddies” or novice hackers who use pre-written scripts and tools to carry out cyberattacks, they said. Most commonly they use methods like phishing and exploiting vulnerabilities in web applications.

Security firm CloudSEK said it has identified more than 100 claims of data theft or credential loss which were exaggerated, recycled or fake.

These aren't sophisticated cybercrime syndicates. Instead, they ride the wave of geopolitical unrest to seek attention, drive nationalistic agenda and gain followers, or even financial rewards from buyers on the dark web, experts said.

“These attacks—mostly involving DDoS (distributed denial of service), website defacement and data breaches—focus on government, educational, media and ecommerce platforms. Most of these operations appear ideologically driven rather than financially motivated,” said Pagilla Manohar Reddy, a threat intelligence researcher at CloudSEK.

Such activities are not unprecedented and have been evident during the ongoing Russia-Ukraine war and Israel-Palestine conflict, he said “In the past week, hacktivist groups have made grandiose claims of cyber breach. For instance, Bangladesh’s SYLHET GANG-SG and DieNet claimed to have exfiltrated 247 GB of data from India’s National Informatics Centre. However, an analysis of a 1.5 GB sample by CloudSEK showed only publicly available marketing materials.

Similarly, Team Azrael-Angel Of Death claimed 1 million citizen records from the Election Commission, but was debunked as recycled data from a 2023 leak, not a fresh compromise, CloudSEK said.

“Cyberattacks often spike around major geopolitical incidents, posing not just financial but also reputational risks—including to public infrastructure,” said Sundareshwar Krishnamurthy, partner and leader, Cybersecurity at PwC India.

Organisations should adopt vulnerability scans, real-time threat monitoring, strict network segmentation and regular phishing simulations in such volatile scenarios, he said, adding: “Even if data is breached, backups enable continuity and limit ransomware impact.”

However, there is one real threat – the APT36, a Pakistan-linked espionage group also known as Transparent Tribe. ET reported last week about Quick Heal Technologies detecting three hacking attempts by this group and its parent entity, SideCopy, on India’s government and defence IT systems. “The group has used malware payloads, including the AllaKore and Crimson RATs, granting the attackers extensive remote control and unfettered access to infected systems,” said Sanjay Katkar, joint managing director at Quick Heal Technologies.

Cybercriminals are also using AI-generated images and videos to carry out phishing social media and messaging apps.

“We've seen fake official-looking letters with made-up numbers, or videos that pretend to show new attacks on India but actually use old war pictures to trick people,” CloudSEK’s Reddy said.

"We’ve seen a spike in low-sophistication cyber activities—website defacements and emotionally manipulative phishing campaigns—often riding on the heightened tensions," said Malcolm Gomes, chief operating officer at identity verification platform IDfy.

"These typically spread via WhatsApp, Telegram and social media, preying on national sentiment to steal personal data or financial details, as the lowest hanging targets," he said.