Researchers warn internet users, Pakistani hackers targeting your PCs, laptops and mobile: What to know

Cybersecurity researchers are issuing urgent warnings to internet users in India about a surge in hacking attempts originating from Pakistan, targeting personal computers, laptops, and mobile devices. This escalation in cyber activity appears to be linked to heightened geopolitical tensions between the two nations. According to a report by Economic Times, Pakistani hackers are sending malicious PDF files which are linked to phishing domains. The report also adds that the Indian officials have confirmed that they have thwarted multiple cyberattacks from Pakistan in the last few days.According to cybersecurity experts, this digital aggression follows a pattern of tit-for-tat cyberattacks between suspected pro-India and Pakistan-based hacking groups. Recent claims include an Indian hacktivist group, 'India Cyber Force,' reportedly breaching Pakistani government and private sector databases. In response, a Pakistan-based group, 'Team Insane PK,' allegedly targeted the Indian Army College of Nursing website with provocative messaging.

How Pakistani hackers are targeting your PCs, laptops and smartphones

As reported by Economic Times, the hackers are sending malicious PDF documents titled *Report & Update Regarding Pahalgam Terror* Attack. The document is said to mimic official Indian government website but it is linked to malicious phishing domains. Users who download and open this file risk their devices being compromised.

Experts highlight that these attacks are not isolated incidents but rather part of a broader cyber conflict. Vishal Salvi, CEO of cybersecurity solutions firm Quick Heal Technologies, stated there has been a "sharp escalation in Pakistan-backed cyber campaigns targeting Indian defence, government, and critical infrastructure sectors."

Quick Heal's analysis has identified the hacker group APT36 (Transparent Tribe) as actively deploying CrimsonRAT malware through sophisticated phishing attacks, often in conjunction with a remote monitoring and management (RMM) tool known as MeshAgent. These attacks are strategically timed to coincide with hacktivist-driven DDoS attacks and website defacements aimed at undermining public trust.

Furthermore, another sub-group of APT36, known as SideCopy, is reportedly broadening its targets to include sectors like railways and oil, utilizing new malware payloads such as CurlBack RAT. These groups are continuously adapting their tactics to evade detection by security software.

Experts emphasise that cyberattacks have evolved beyond mere disruptive acts and are now being employed as deliberate extensions of geopolitical strategy. "Cyberattacks are no longer fringe acts of disruption... They have become deliberate extensions of geopolitical strategy," Sundareshwar Krishnamurthy, partner and leader - cybersecurity at PwC India told Economic Times.

What users need to keep in mind to stay safe from cyberattacks

- Be extremely cautious of unsolicited emails and messages, especially those with attachments or links related to sensitive topics like security or current events.
- Verify the authenticity of any PDF files or documents before downloading or opening them, especially if they appear suspicious or are received from unknown sources.
- Double-check the URLs of websites before entering any sensitive information, ensuring they are legitimate and not mimicking official sites.
- Keep your operating systems, antivirus software, and other security applications up to date.
- Be wary of clicking on suspicious advertisements, particularly those with provocative or nationalistic imagery.
- Exercise caution while browsing online, especially on less reputable websites.