

Advisory on Heightened Cyber Threat Landscape Amid Geopolitical Tensions

In light of the recent escalation in geopolitical tensions between India and Pakistan, we are witnessing a corresponding rise in cyber activity that may pose risks to organizations across critical infrastructure, enterprise systems, and public-facing assets. Geopolitical conflicts often spill over into the cyber domain, and such periods typically see an increase in state-sponsored campaigns, hacktivist movements, and opportunistic attacks aimed at disrupting business continuity, stealing data, or spreading misinformation.

This advisory aims to provide a timely overview of the emerging threat landscape, outline specific indicators of malicious activity observed, and recommend actionable steps to fortify your cybersecurity posture during this sensitive period.

Executive Report: Cyber warfare post Operation Sindoor

Executive Summary

Operation Sindoor marked a decisive military response by the Indian Armed Forces, targeting nine terrorist camps in Pakistan and Pakistan-occupied Kashmir (PoK). This operation was launched in direct retaliation for the tragic Pahalgam terror attack, which claimed the lives of 26 civilians.

Following the Pahalgam incident, a surge in cyber activities was observed, spanning across various threat vectors along with huge misinformation campaigns:



- Spear-phishing campaigns by APT groups aimed at critical infrastructure
- Various Remote Access Trojans deployed for persistent access
- DDoS (Distributed Denial of Service) attacks disrupting online services
- Defacement operations targeting government and organizational websites

Parallel to this, retaliatory cyber activities were also noted from smaller hacktivist groups originating from regions like Pakistan, Algeria, Bangladesh and others. These groups primarily targeted Indian government entities, aiming to disrupt operations and assert symbolic victories in the digital domain.

Pakistan-linked SideCopy APT has expanded its scope of targeting beyond Indian government, defence, maritime sectors, and university students to now include entities under railway, oil & gas, and external affairs ministries. It has evolved its tactics such as multi-platform intrusions, repurposing open-source tools. Additionally, new payloads have been identified along with newer infrastructure.

This report encapsulates the key incidents and provides detailed briefings on their nature, impact, and underlying motivations.

BSE India has released a cybersecurity advisory amid rising Pakistan-linked threats to Indian BFSI Sector.



NOTICES

Notice No.	20250507-45	Notice Date	07 May 2025
Category	Compliance	Segment	General
Subject	Advisory from Indian Computer Emergency Response Team (CERT-In)		

Content

An advisory has been received from Indian Computer Emergency Response Team (CERT-In) highlighting on cyber threat campaign specifically targeting Indian organizations operating within the Banking, Financial Services, and Insurance (BFSI) sector. Market participants are particularly advised to take precautionary measures on potential cyber risks including high-impact cyber-attacks such as ransomware, supply chain intrusions, DDoS attacks, website defacement and malware.

We request all members to take steps to:

- Check if necessary security controls are in place as per SEBI CSCRF dated 20-Aug-2024.
- Conduct risk assessment and mitigate any findings.
- Beef up security monitoring of the systems with appropriate incident response plans.
- Utilise threat intelligence from CERT-In & NCIIPC and take necessary action on alerts/advisories released.
- Increase Threat Hunting activities.
- Report incidents to exchanges & regulators as per defined timelines.

All Members and market participants are advised to take note of the above and take appropriate steps to ensure safe marketplace.

For and on behalf of BSE Ltd

Devendra Kulkarni
Additional General Manager
Member Oversight

Bipin Veliyam
Additional General Manager
Member Oversight

Site optimized for IE8 & above, resolution 1024 X 768 & above. | Disclaimer | Sitemap

Copyright© 2015. All Rights Reserved. BSE Ltd. (22)

Timeline of Events

Recent escalating geopolitical tensions between India and Pakistan have sparked a surge in cyber activities, including data breaches, Advanced Persistent Threat (APT) campaigns, DDoS attacks and website defacements. This outlines the critical need for heightened vigilance and serious response due to the significant implications of these ongoing threats. Here is the summary of coordinated cyber-attacks that have transpired in the past few days:

DDoS

07 May 2025

- **Anonsec** attacked multiple civilian portals Government e-Marketplace (GeM), National Judicial Data Grid (NJDG), National Commission for Women (NCW), Election Commission of India (ECI), Public Enterprises Selection Board (PESB)
- **Islamic Hacker Army** executed coordinated attacks against Ministry of Defence (MoD), Ministry of Information & Broadcasting
- **Mr. Hamza**-led group launched rapid strikes on Indian Army, Indian Air Force, Indian Navy, Ministry of Defence (again)
- **Keymous+** launched staggered attacks targeting: BSNL, eProcurement (MoD), BSF (Border Security Force), National School of Drama (NSD)
- **SYLHET GANG-SG** targeted Ministry of Defence, Punjab National Bank (PNB)
- **Nation of Saviors** executed two waves: Drug Control Office (NCB), National Portal of Government of India, Open Government Data Platform India (OGD), Press Information Bureau (PIB), Uttar Pradesh Police (UP Police), Interpol India, Central Bureau of Investigation (CBI)

On May 8, 2025, while a large-scale missile attack by Pakistan targeting key Indian military and civilian areas in the north and west was successfully intercepted by India, cyber activities including website defacements and data breaches continued unabated in the digital realm.

- **Electronic Army Special Forces** targeted government websites: Prime Minister of India, President of India, Press Information Bureau, India Post.
- **Vulture** targeted the website of Ministry of Education, Government of India.

Date Leaks

07 May 2025

- **Team Azrael Angel Of Death:** Puneet, Joint Secretary (MoD) , Mail Server of Allahabad High Court, Indian Army personnel records
- **Team insane Pakistan** claims to have hacked Sardar Patel Institute of Economic and Social Research
- **DieNet** has targeted Rupashree Prakalpa Scheme

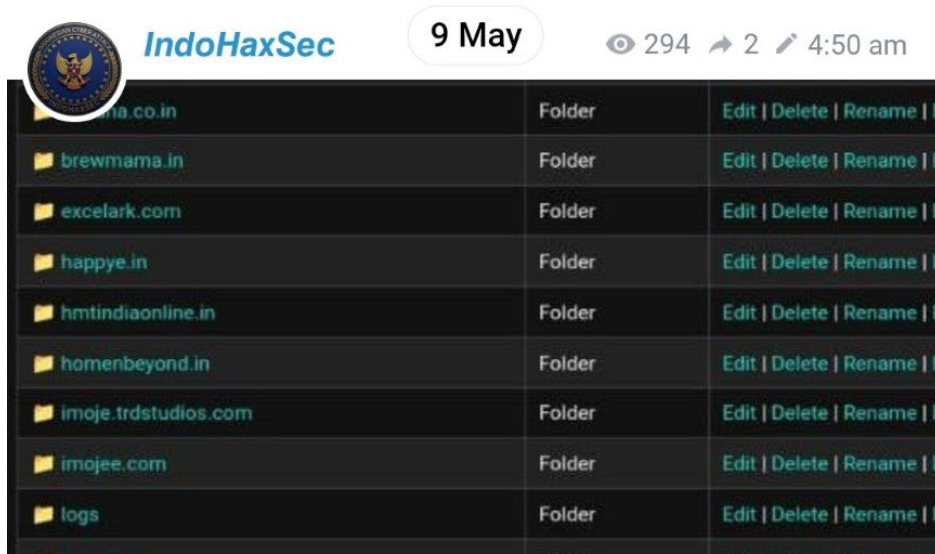
08 May 2025

- **GARUDA ERROR SYSTEM** claimed responsibility for leaking data from Yenepoya Ayurveda Medical College and Hospital.
- **INDOHAXSEC** claimed to have leaked database of Election Commission of India.

Further attacks planned

09 May 2025

DieNet has claimed to have breached National Informatics Centre (NIC) and exfiltrated 247GB of sensitive data. Hacktivist IndoHaxSec announces collaboration with Team Azrael – Angel of Death to initiate cyber-attacks targeting Indian Cyber Space. At 10:45 am, yet another post was made by IndoHaxSec group stating that another attack is scheduled for today.

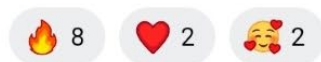


We say to India "Enjoy our attacks"

We will serve you a delicious meal for your cyberspace India!

*What we are doing is just an opening...
Because we have prepared for data leaks from
your country's government and bank sites..*

#IndoHaxSec
#Team_Azrael_Angel_Of_Death
#OpsIN
#JoinPkCyberWar



IndoHaxSec

87 10:45 am

The next attack is scheduled for today...
Enjoy India and PM modhi Bastard!

#INDOHAXSEC
#OpsIN
#JoinPkCyberWar



Misinformation

Amid the ongoing India-Pakistan conflict following "Operation Sindoor," a wave of misinformation has spread across social media platforms like X and Telegram. False claims suggesting that Pakistan's Air Force shot down Indian jets and targeted IAF bases have circulated widely, despite no official confirmation. These narratives, likely part of a coordinated disinformation campaign, have caused confusion and alarm. Fake reports, including impersonations of credible news outlets and edited content alleging Rafale crashes, have further fueled the chaos. Old incidents, such as a 2021 MiG-21 crash and a 2024 Sukhoi accident, are being misused to misrepresent current events, complicating the public's ability to discern truth during a sensitive military escalation.

False claims—like the "Dance of the Hillary" phone virus and fake news of INS Vikrant attacking Karachi—have spread panic, while recycled footage from unrelated conflicts is being misused online. Meanwhile, Pakistan faces criticism for internet censorship and deploying Chinese PL-15 missiles along the border, as its media pushes propaganda fueling regional instability.

APT and phishing campaigns

Multiple campaigns related to Pakistan-linked APT groups targeting the Indian Government entities has been identified. After our recent [advisory](#) on **APT36** using Pahalgam attack themed decoys, we have discovered "*Blackout Rehearsal Plan*" themed attack used by **SideCopy** APT group to deploy [recently](#) uncovered CurlBackRAT through MSI stagers.

Whilst more phishing documents of APT36 themed "*Advisory Notice Movement of Troops*", have popped up where lures related to Jammu & Kashmir, deployment of army were observed since starting of February 2025.

Name	First Seen
Advisory Notice Movement of Troops.ppam	2025-05-02
MoM & Action Points Regarding Pahalgam Terror Attack .pdf	2025-04-29
Report & Update Regarding Pahalgam Terror Attack.ppam	2025-04-24
PAHLGAM SIDE FIGURED NUMBERS.xlam	2025-04-23
J&K Police Letter Dated 17 April 2025.pdf	2025-04-17
List of Deployment Location.xlam	2025-02-25
Final List of OGWs.xlam	2025-02-26
List of Deployment.xlam	2025-02-05

The groups are also targeting both Linux and Windows platforms parallely with files named as:

- MILITARYSTRATEGY_00425.desktop
- Send_Letters_for_Joinings_and_Quarters.pdf
- SITREP_PahalgamSector.zip
- CrossBorderActivity_LogisticsRoutes_SuspectedInfil_Apr2025.kml.Ink

- Intercepts_Communications_AnantnagSector_Week16.wav.Ink
- JointOps_ResponsePlan_SouthKashmir_ScenarioAlpha.docx.Ink
- Pahalgam_Incident_Timeline_and_TacticalBreakdown.pptx.Ink
- ThreatMatrix_TRF_KashmirValley_Apr2025.xlsx.Ink
- WELFAREINITIATIVESJULY2025.pdf.Ink

Additionally, [Hunt.io](https://www.hunt.io) researchers observed APT36 employing ClickFix-style campaign spoofing Indian Ministry of Defence.

Hacktivist groups targeting India

We are actively tracking activities of more than 30 hacktivist groups in various channels such as Telegram, Twitter (X), and below listed are some of the most active ones primarily from Pakistan, Bangladesh, Indonesia, Egypt and others:

<ul style="list-style-type: none"> • AnonPioneers • Anonsec • Dark Engine • DieNet Group • Electronic Army Special Forces • Garuda Error System • IndoHaxSec • Islamic Hacker Army • Jakarta Cyber White • Kal Egy 319 	<ul style="list-style-type: none"> • Keymous+ • Mr. Hamza • Nation of Saviors • Pakistan Cyber Force • SHADOW • Sylhet Gang-SG • Team Azrael Angel of Death • Team Insane Pakistan • Team Kuwaiti Shadow Force • Vulture
--	--

Indicators of Compromise

MD5

```
cd6ad8ee1f0096fe33948b2b29a55512
905134a46153e071d453e086dc37c47a
609308aa7da464c40cb2927ebf01793a
e2babc163a149bc6ff79a3d43aeb54e7
e496c6fd5076f999f0bac84ee70743fa
51d9ad02e97ea0d2ef7715aefba867cf
706aa76efc46e5bf99d5794431dd99cd
746d43d040fa899f046cc830a9a0d24c
853553554d2600d877ee7b93f6af1f9e
```


ca3427edc13c3f568b510c07cf3429ee
c5325fbb5a40c12ecae8107b3af235a6
75ac4bd5f625ca6b714982ae28eb2553
0a1ea0e7119e125141792f24eceb62d2
95dfea2c3e7f5bfa8fc18258a6c40cd5
b62833e49f55d11f0b958dc8803621db
68c7c14b9ac69491b23b3c3ad88f3a1e
b6ef8bb7e47ddc55131990e21d2519a7
6af1776a02536f72f810ca0fa21f38ff
01e23e452f2621e747b6355bfa1c097b
15013ddcf8498efe6828e9f0c42b833c
a3d8e4f55c50bc916f6410f31a811e2d

Domains

nationaldefencebackup[.]xyz
nationaldefensecollege[.]com
mod[.]gov[.]in[.]indiandefence[.]services
sync[.]amsisupport[.]com
zohidsindia[.]com
raf74[.]duckdns[.]org

IP

167.86.97[.]58:17854
96.47.234[.]145
96.47.232[.]202
66.29.146[.]99
104.129.27[.]14

URLs

hxxps://nationaldefensecollege[.]com/content/WELFAREINITIATIVESJULY2025.rar
hxxps://nationaldefensecollege[.]com/content/kk.vbs
hxxps://nationaldefensecollege[.]com/welfare/gov_auth.php
hxxps://nationaldefencebackup[.]xyz/doc/Adjustable.lpk
hxxps://nationaldefencebackup[.]xyz/doc/Brawlers.sea
hxxps://nationaldefencebackup[.]xyz/doc/WELFAREINITIATIVESJULY2025.pdf
hxxps://nationaldefencebackup[.]xyz/doc/YbfbYauWli174.bin
hxxps://nationaldefencebackup[.]xyz/doc/gNLwUw23.bin
hxxp://167.86.97[.]58:17854/uploads/root_345044036645/letter
hxxps://zohidsindia[.]com/ac/cds.vbs
hxxps://zohidsindia[.]com/ac/Send_Letters_for_Joinings_and_Quarters.pdf

Potential Impact

- **Critical Infrastructure at Risk:** Spear-phishing and RATs threaten government and defence systems.
- **Service Disruption:** DDoS attacks affect government portals and online services.
- **Public PsyOps:** Misinformation, deepfake and defacement campaigns aim to spread panic and erode trust.
- **Transnational Hacktivism:** Involvement from groups in Pakistan, Algeria, Bangladesh increases cyber complexity.
- **Smart devices like CCTVs and voice assistants can be hijacked for surveillance, data theft, and psychological warfare, making them key vulnerabilities during wartime cyber operations.**
- **Enemy actors may use deepfakes to discredit leaders or incite communal tensions, deploy ransomware to extort or destroy data, and hack public service platforms to spread falsehoods or disrupt access.**

Recommendations and Mitigations

- **Enhance Defenses:** Implement Zero Trust architecture, conduct frequent security audits, and organize cyber drills to proactively test and strengthen defenses against evolving cyber threats.
- **Boost Threat Intel Sharing:** Enable real-time sharing of Indicators of Compromise (IOCs) and threat alerts across government and private sectors to accelerate detection and response.
- **Public Awareness:** Launch nationwide campaigns to educate citizens on identifying phishing attempts, spotting fake news, and practicing safe digital habits to reduce vulnerability.
- **Crisis Response:** Expand and train dedicated incident response teams, and regularly simulate cyberattacks to ensure rapid containment, recovery, and coordination during real-world incidents.
- **Monitor Social Platforms:** Deploy tools and partnerships to detect fake accounts, bots, and coordinated disinformation campaigns aimed at destabilizing public trust and spreading panic.
- **Global Coordination:** Collaborate with international allies for intelligence sharing, joint cyber exercises, and coordinated attribution of attacks to strengthen global cyber deterrence.
- **Resilience Building:** Encourage adoption of cyber insurance, promote backup systems, and provide civil defense training to enhance public and institutional preparedness for cyber incidents.
- **Safe Online Practices:** Avoid unverified links and attachments, use endpoint protection, regularly update software and OS, and ensure strong passwords for sensitive documents and devices.

- **IOC Blocking in SIEM and SOAR:** Block the IOC on SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation, and Response) systems for rapid detection and containment. This allows for timely blocking of malicious IPs, domains, and file hashes, reducing attack impact and accelerating response times.

Conclusion

The recent surge in cyber incidents underline the growing threat landscape targeting not just Indian government institutions but also everyday citizens. These actions aim to incite panic, erode public trust, and destabilize societal order. With Pakistani-affiliated threat actors signaling further attacks such as DDoS, website defacement, data leaks and campaigns, continuous monitoring and rapid response are essential. Seqrite Labs, India's largest malware analysis center- remains committed to vigilance, providing detailed technical insights and IOCs to support proactive defense and maintain national cybersecurity readiness.