



| Flash |

Rise of Hacktivism Incidents amid India-Pakistan Hostilities

F-2025-05-16a

Classification: TLP:CLEAR

Criticality: MEDIUM

Intelligence Requirements: Hacktivism, Distributed-Denial-of-Service

May 16, 2025

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 7:00 AM (EDT) on May 16, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Rise of Hacktivism Incidents amid India–Pakistan Hostilities

| Key Findings

- ZeroFox has observed an increase in hacktivist incidents targeting entities on both sides of the border during the recent escalation in hostilities between India and Pakistan.
- According to announcements from malicious collectives, leveraged tactics, techniques, and procedures (TTPs) include distributed-denial-of-service (DDoS), website defacement, and data breaches.
- Hacktivist groups often conduct attacks and select targets opportunistically, and notable geopolitical events—such as a rise in state tensions or the outbreak of conventional conflict—often provide the justification necessary to target entities perceived as socially, politically, or ideologically misaligned.
- As regional tensions continue to reduce, there is a very likely chance that hacktivism activities emanating from pro-India and pro-Pakistan collectives will reduce in intensity and tempo.

Details

ZeroFox has observed an increase in hacktivist incidents targeting entities on both sides of the border during the recent escalation in hostilities between India and Pakistan.

- On April 22, 2025, Pakistan-based militants killed approximately 26 people in the long-disputed region of Kashmir.¹ The incident led to a series of military actions by both Indian and Pakistani military forces.
- India responded on May 7, 2025, by launching air strikes targeting alleged terrorist infrastructure in Pakistan-administered Kashmir and Pakistan's Punjab region.²
- On May 10, 2025, India and Pakistan announced a ceasefire, though cross-border strikes continued for a short time immediately following its implementation.³
- As of the writing of this report, the situation remains tense, although the current ceasefire appears to have significantly reduced the risk of further military escalation.

Since the onset of these hostilities, various pro-Pakistan hacktivist collectives have claimed to have conducted over 100 cyberattacks targeting India-based entities; there has been an emphasis on government, education, and critical infrastructure sectors.⁴ Leveraged attack methods include DDoS attacks, website defacement, and data breaches.

- While hacktivism can result from perceived domestic injustices, it is very often tied to geopolitical incidents and rising state tensions, as previously observed following the onset of the 2022 Russia-Ukraine hostilities.
- ZeroFox has observed a higher number of hacktivist attacks targeting India-based entities than Pakistan-based ones, though the likely validity of the various collectives' claims varies significantly.

On May 16, 2025, prominent pro-Palestine hacktivist collective "Dark Storm Team" posted on its Telegram channel, claiming to have carried out a series of DDoS attacks targeting

¹ [hXXps://edition.cnn\[.\]com/2025/04/26/asia/india-family-friends-shattered-tourist-massacre-kashmir-intl-hnk](https://edition.cnn.com/2025/04/26/asia/india-family-friends-shattered-tourist-massacre-kashmir-intl-hnk)

² [hXXps://www.reuters\[.\]com/world/asia-pacific/pakistan-says-clashes-with-neighbour-india-killed-more-than-50-2025-05-13/](https://www.reuters.com/world/asia-pacific/pakistan-says-clashes-with-neighbour-india-killed-more-than-50-2025-05-13/)

³ [hXXps://www.reuters\[.\]com/world/india/pakistan-says-three-air-bases-targeted-by-indian-missiles-2025-05-10](https://www.reuters.com/world/india/pakistan-says-three-air-bases-targeted-by-indian-missiles-2025-05-10)

⁴ [hXXps://www.infosecurity-magazine\[.\]com/news/hacktivist-attacks-india/](https://www.infosecurity-magazine.com/news/hacktivist-attacks-india/)

various Indian government institutions and financial organizations. Some of the websites allegedly targeted include those of the following entities:

- Ministry of Commerce and Industry
- Ministry of External Affairs
- Ministry of Defence
- Department of Telecommunications
- Reserve Bank of India
- Punjab National Bank

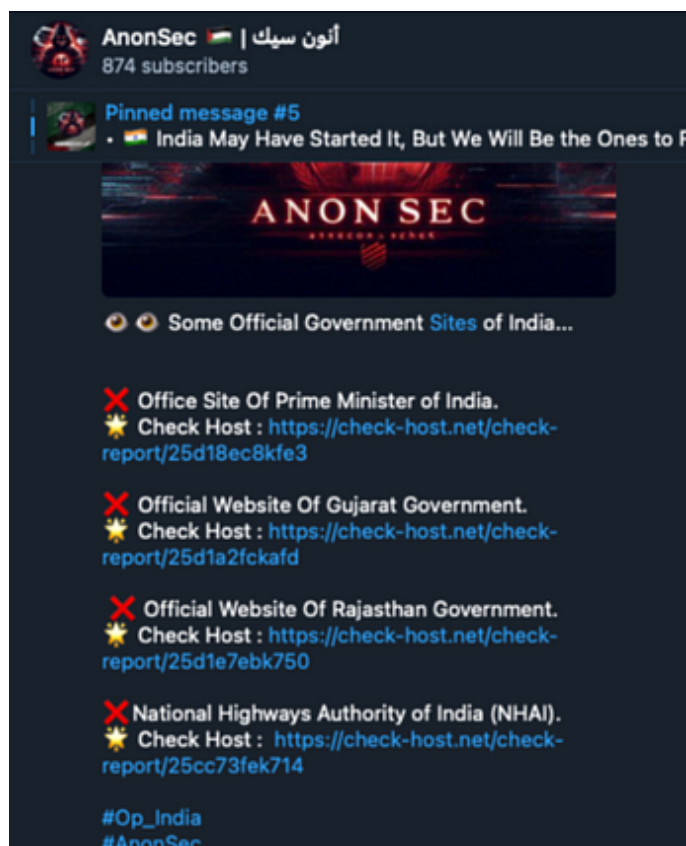
There is a likely chance that these attacks took place, given the provision of checkhost links by Dark Storm Team and the collective's other recent activity. Any impact upon the targeted organizations is unlikely to be sustained or significant, however.



Dark Storm Telegram post

Source: Telegram

On May 8, 2025, pro-Pakistan hacktivist collective “AnonSec” claimed on its Telegram channel to have successfully conducted DDoS attacks against multiple Indian government websites and institutions and provided checkhost links to verify its claims.



AnonSec Telegram post

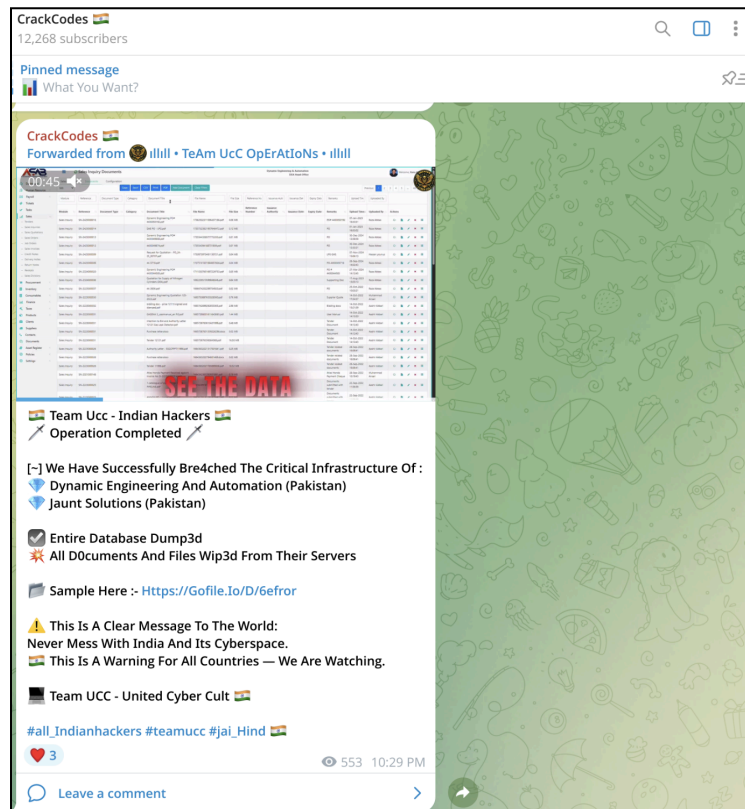
Source: Telegram

Hacktivist groups often conduct attacks and select targets opportunistically, and notable geopolitical events—such as a rise in state tensions or the outbreak of conventional conflict—often provide the justification necessary to target entities perceived as socially, politically, or ideologically misaligned. However, hacktivist collectives often falsely claim responsibility for attacks against prominent targets. Similarly, the complexity or impact of attacks are often exaggerated in a bid to garner publicity and accumulate media attention.

On May 12, 2025, ZeroFox observed a Telegram post by pro-India hacking collective “Team Ucc” claiming responsibility for the alleged breach of digital infrastructure

associated with two Pakistan-based victims: Dynamic Engineering and Automation (an engineering company) and Jaunt Solutions (a provider of business solutions software).

- Team Ucc claimed to have leaked the organizations' "entire database", but the link provided to access the data sample appears to be broken. This suggests there is a likely chance such claims are exaggerated or fabricated.



Team Ucc Telegram post

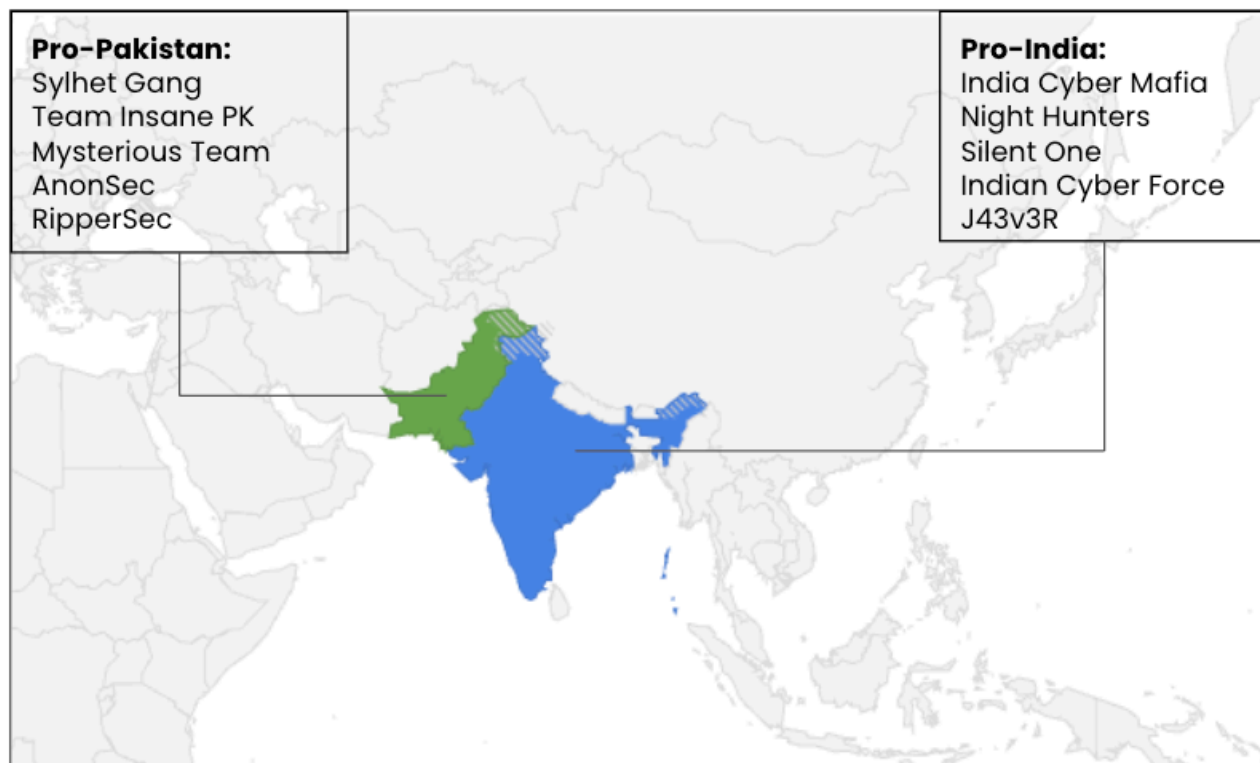
Source: Telegram

Pro-Palestinian hacktivist groups have reportedly announced collaboration with pro-Pakistani hacktivists in the targeting of India-based infrastructure.⁵

- Hacktivist collectives such as "Vulture" (an Iran-based collective), "RipperSec" (likely a Malaysia-based collective), and "Mysterious Team" (a Bangladesh-based collective) have all announced their intent to support Pakistan on their respective messaging platforms.

⁵ <https://www.darkreading.com/cyberattacks-data-breaches/pahalgam-attack-hacktivists-unite-opindia>

Collaboration between hacktivist groups is commonly observed and is usually announced via social media platforms such as X (formerly Twitter) or messaging channels such as Telegram. Allegiances are often shaped by perceived shared injustices underpinned by ideological, religious, political, or national beliefs. Hacktivist collectives are very likely collaborating in support of Pakistan due in part to the perceived pro-Israel and pro-Western stature exerted by India on the global stage.



Allegiances of active hacktivist collectives as of May 14, 2025

Source: ZeroFox Intelligence

It is likely that the current ceasefire agreement between India and Pakistan will sustain, though continued tensions in the Kashmir region will almost certainly continue to hamper India-Pakistan state relations. As tensions continue to reduce, there is a very likely chance that hacktivism activities emanating from pro-India and pro-Pakistan collectives will reduce in intensity and tempo. Collectives that have historically displayed targeting patterns that are not immediately pertinent to the India-Pakistan region—particularly those with pro-Russian and anti-Israel agendas—will very likely resume attacks against traditional targets.

Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are updated with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege, and implement network segmentation to separate resources by sensitivity and/or function.
- Implement phishing-resistant multi factor authentication (MFA), secure and complex password policies, and ensure the use of unique and non-repeated credentials.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud-based servers at least once per year—and ideally more frequently.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in deep and dark web (DDW) forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated TTPs.

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%