ATHENIAN TECH

NEWSLETTER

May 2026

THREAT INTELLIGENCE BY

ATHENA

Issue #02

In this Newsletter

From the Editor's Desk

One of the most defining moments that shook the globe in 2026 was the conflict in the middle-east involving Iran on one side and Israel and the United States of America on the other side. While India was in no way directly involved in the war, but the perception that India was getting too close to Israel and the United States of America, meant that India too got lacerated by the embers of this conflict. As a result, hacktivists owing allegiance to the pro-Palestine cause chose to target digital assets of Indian institutions.

These attacks largely spanned across sectors like government and education. While the intensity and severity of the attacks, motivated by the Palestine cause, reached its zenith in March and April, things have somewhat started to taper off in the first half of May. This is much like the present day situation on the ground in the middle-east, where the fragile ceasefire continues to hold, even though recent escalations, in the region continue to test its limits.

Moving to a more pressing concern i.e. the growing frequency and sophistication of ransomware attacks, large-scale data breaches, financially motivated cyber frauds and infrastructure-focused intrusions which have shown that cyber threats/attacks, these day directly have a bearing on economic stability, public trust, business continuity, and national resilience. This trend is only expected to gain strength going forward. A common feature of the cyberattacks these days is that cyber criminals are increasingly targeting industries that typically hold high-value intellectual property, critical infrastructure assets, and sensitive personal data.

Even though the government is taking the necessary measures to embolden the cybersecurity posture of country, attacks continue to batter Indian organisations. The recent claim by the DragonForce ransomware group of compromise of Kopran Pharma illustrates the growing sophistication and strategic nature of modern ransomware operations. Another sector that has been attracting attention of cyber criminals lately is the country’s agricultural biotechnology ecosystem. Mahyco Private Ltd, one of India’s prominent agricultural biotech and seed companies, was reportedly targeted by the ransomware group, TheGentlemen.

Major data breaches continue to expose systemic weaknesses across India’s rapidly digitising economy. The exposure of more than 514,000 records associated with Talentely, a career platform under Veranda Learning Solutions,

represents a particularly significant warning for India’s expanding education technology sector.

Beyond enterprise intrusions, India is also witnessing the rapid industrialisation of financially motivated cybercrime networks. Recent operations by law enforcement agencies have brought to light the scale, organisation, and sophistication of these criminal ecosystems.

One such operation that brought to light such facts in glaring details is the Operation CyHawk 4.0, led by the Delhi Police, which resulted in 1,429 arrests across more than 20 states. This operation also traced over ₹519 crore in fraudulent financial flows. Another operation, Operation Octopus 2.0, conducted by Hyderabad Police, too showed extent to which cybercrime has infiltrated legitimate financial systems.

It will not be wrong to say that even though cyber resilience has improved over the years, it is an irony that cyber scams, even to this day, continue to rely primarily on psychological manipulation rather than technical sophistication.

One of the primary reasons why this modus operandi is successful, but there is a lack of awareness about such scams. Coming to the scam that made headlines recently, a 73-year-old retired engineer reportedly lost ₹10.3 crore through a prolonged “digital arrest” scam. Such incidents prove that AI-generated deception is significantly enhancing the effectiveness of impersonation-based fraud. Such incidents also highlight the importance of increasing awareness about such scams, so that unsuspecting individual stay at arm’s length from such ingenious methods of deception.

Well, reading about the scams and attacks may give the impression that we are fighting a lost cause, but there is light at the end of the tunnel. India’s regulatory environment is evolving in response to these escalating threats. It is, in its own way, empowering the nation to catch the bull by its horns. The enactment of the Digital Personal Data Protection Act, 2023 and the notification of the Digital Personal Data Protection (DPDP) Rules, 2025 are a step in that direction.

These legislations lay the foundation for the major shift in how organisations must approach data governance, breach management, and cybersecurity accountability. At the architectural level, Zero Trust principles are rapidly becoming operational necessities rather than aspirational frameworks.

From the Editor's Desk

The Reserve Bank of India (RBI), the banking regulator, mandates that banks and NBFCs, combined with lessons from recent breaches, have reinforced the limitations of perimeter-centric security models.

Lastly, these days accessing the Internet through wi-fi at home is a common thing. Getting the wi-fi installed in a house, is one of the essential things that one gets done, when one moves into a new house. In this digitised world it is no longer a luxury but its surely a necessity. In this DIY section, we tell you what you should not be doing on your wi-fi.

Do sift through the pages of this endeavour and please do write to us at pankaj.toppo@atheniantech.com . We eagerly look forward to your suggestions so that we can mould this offering, to suit our tastes. If you however, like what you see and read, do spread the word around so that the word around is emboldened enough to tackle the challenges thrown at us with a certain degree of elan. Till we meet again,
Happy reading.

Pankaj Anup Toppo

Iran-Israel-US Conflict Triggers Cyber Attacks Targeting India

On 28 February 2026, the United States of America-Israel coalition launched air strikes against Iran, triggering a conflict that was designed to be short, decisive, and geographically contained. It was none of those things. What followed was six weeks of full-scale war, a closed Strait of Hormuz, fuel queues across Indian cities, and a government scrambling to ration cooking gas. But the embers of that conflict did not stop at the waterline. They drifted eastwards, and the Indian cyberspace caught fire. Athenian Tech analysts tracked the digital fallout of that conflict on Indian organisations, and what they found was a methodical, coordinated attack against the Indian digital space.

India Was Never Going to Be a Bystander

The reason India ended up in the crosshairs was neither accidental nor incidental. It was, in the assessment of Athenian Tech Research, entirely predictable.

India's deepening strategic alignment with both Israel and the United States of America had, over the years, created a perception problem among pro-Palestine hacktivist groups, and the Iran-Israel-US conflict converted that perception into an operational intent. The memory of 1999 remains vivid in these circles. When Pakistan's armed aggression in Kargil threatened to destabilise India's northern frontier, it was Israel that stepped in, to help India, with urgent military hardware, which included supplying India with laser-guided bombs, Heron and Searcher surveillance drones, and 155mm ammunition.

That partnership, forged under fire a quarter century ago, has not been forgotten by those who now found themselves on the opposite side of a different conflict. In the eyes of the hacktivist collectives that mobilised in March 2026, India's digital infrastructure was in no way a neutral ground. It was an extension of an alliance they were actively fighting against.

The First Wave: Defacement and Disruption

The opening phase of what Athenian Tech Research characterises as a two-wave campaign was dominated by web defacement and distributed denial-of-service (DDoS) operations. Between 03 and 27 March, eleven or more distinct hacktivist groups and dark-forum actors took aim at portals of the Government of India, educational institutions, and political websites, with 31 confirmed or claimed compromises recorded during the study period.

Four collectives, as mentioned below, drove the bulk of this activity:

Bangladesh Cyber Troops, operating a Telegram channel with over 59,200 subscribers, launched a coordinated DDoS campaign designated "Box-5" between 10 and 12 March. Their targets included the Jammu and Kashmir government port at jammu.nic.in and state portals in Jharkhand, Tamil Nadu, and Karnataka. The impact was independently verified through check-host.net, which returned 502 Bad Gateway responses from over twenty global nodes.

Team Azrael, a Pakistan-based collective whose full name, **Angel of Death**, signalled its intent rather plainly. They claimed defacement of multiple Indian websites on 03 March under the hashtags #OpIndia and #OpIsrael. The sites compromised by **Team Azarel** carried a consistent signature: a video background of the Pakistani army, the caption "Pakistan Zindabad," and anti-India, anti-Israel messaging.

The group used #Iran and #GeoNews tags to associate itself with the broader geopolitical conflict, despite its actual targets being exclusively Indian. Athenian Tech analysts assessed this as a deliberate attempt to ride the wave of geopolitical attention while pursuing, at its core, a long-standing nationalist anti-India agenda.

Team Insane Pakistan, allied with **Team Azrael**, they claimed responsibility on 8 March for defacing the Assam Higher Education portal at heis-rusa.assam.gov.in . The defaced page, hosted at /pak.html on the compromised government domain, carried the slogan "Pakistani Leets OWNED You Again." The group maintains redundant Telegram backup channels, a design choice that reflects operational awareness of takedown risk and a deliberate effort to sustain psychological pressure beyond any single disruption.

The Anonymous BD and its associated **NECROSWORD** persona operated in different ways. On 18 March, a NECROSWORD member defaced missionmodi.org, a supporter portal for Prime Minister Narendra Modi and the Bharatiya Janata Party (BJP). The attack vector, logged in defacement archives, was not a software vulnerability. It was an admin-interface misconfiguration.

Perhaps the most operationally disciplined of the defacement actors was **OpsShadowStrike**, a Malaysia-origin collective that ran a sustained three-week campaign from 2 to 22 April against 22 Indian websites. Their signature was a consistent defacement path, deployed across education portals, telecom providers, civil-society organisations, religious services, and media outlets. The consistency of that path across independent targets points to a shared toolkit or coordinated playbook, with links to the broader Pakistan-origin actor ecosystem active during the same window.

The Second Wave: When Hacktivists Became Data Brokers

What Athenian Tech analysts identified as the more strategically consequential development began quietly around 22 March and accelerated through most of April. The character of the threat shifted. The political defacements of Wave 1 gave way to something quieter, more mercenary, more sinister and with a far longer tail.

Dark-forum actors, eighteen distinct groups operating across DarkForums, Breached.st, BreachForums, and PwnForums, began listing databases of Indian organisations for sale. Athenian Tech analysts catalogued eighteen distinct listings between 22 March and 22 April. The range of targets was a provocation in itself.

The viskohr.com listing on 22 March, carrying 113,000 records, was followed two days later by a dataset of 500,000 Indian pharmacy managers and owners. By 4 April, a listing for Kotak Securities had appeared, claiming to contain 1.5 million records with names, mobile numbers, email addresses, and IP data.

On 9 April, a thread appeared on DarkForums offering what was described as data of the Election Commission of India (an autonomous, permanent constitutional body responsible for organising and overseeing the electoral processes in India) posted under a handle crediting the Pakistani hacktivist collective **Evil Markhors**. By 21 April, a single day had produced listings for the University of Yeniboya in Mangalore, a claimed 1TB Lenskart database, the Indian Union Academy's 103GB dataset, and what a threat actor named **MDGhost** described as a breach of Reliance Jio Infocomm's internal servers. The following day brought an Adda.io education database listing.

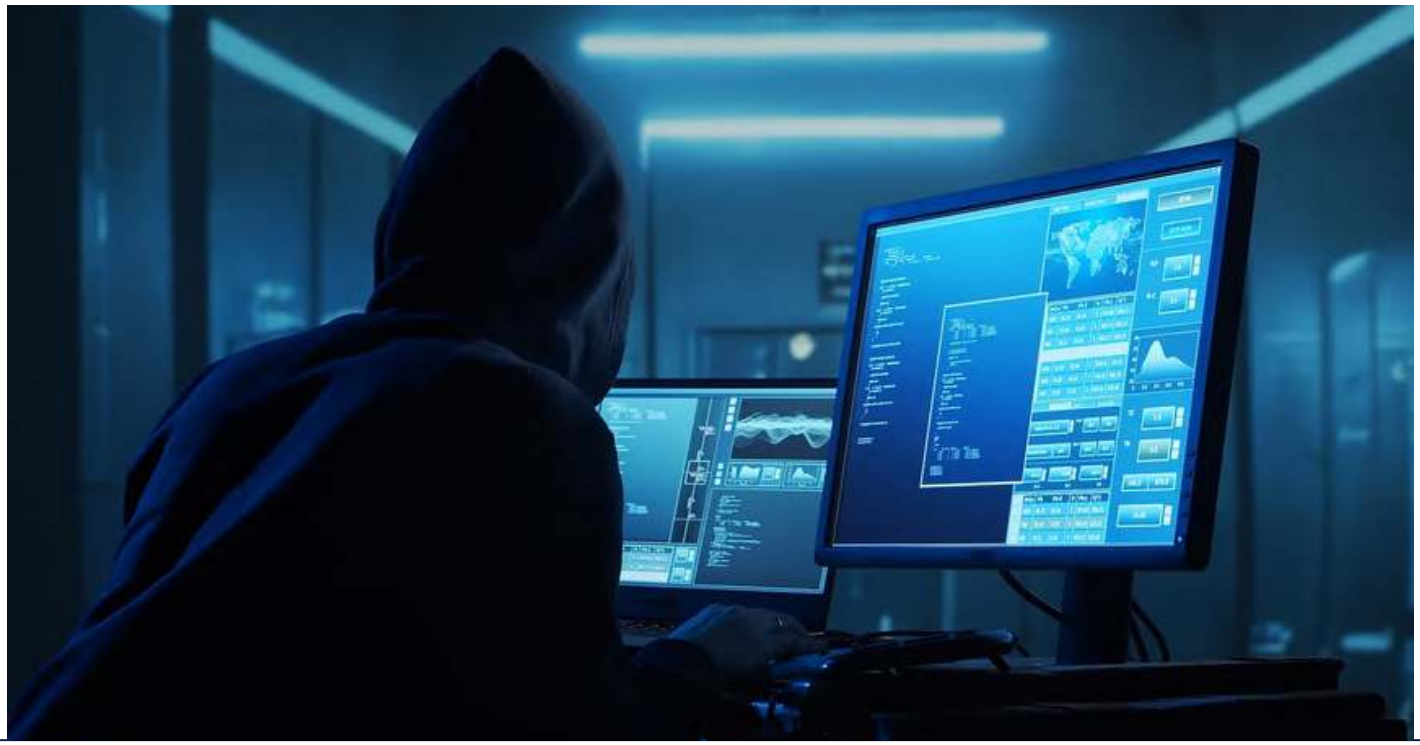
Athenian Tech is deliberate in noting that the data-broker wave cannot be directly attributed to the geopolitical conflict with certainty. The brokers operated behind pseudonymous handles with no explicit ideological framing. But the timing, coinciding precisely with the period of peak hacktivist activity against Indian targets, is structurally significant. Whether the motivation was geopolitical or opportunistic, the effect on Indian organisations is the same. Their data which is in circulation, will be resold, repackaged, and weaponised long after the Strait of Hormuz reopens.

The Technical Anatomy of the Campaign

Athenian Tech's analysis of the attack vectors observed across both waves paints towards a picture that should concern every Indian. The methods were not sophisticated. They did not need to be.

The most common initial access route was exploitation of public-facing applications, specifically CMS vulnerabilities in Apache, Nginx, and PHP installations running on Linux servers. Where software is held, misconfigurations open the door. The missionmodi.org compromise, attributed to an admin-interface misconfiguration, is the clearest example: no zero-day, no advanced persistent threat, just an unlocked gate. Credential-stuffing and brute-force attacks were observed against admin interfaces across multiple targets. For the DDoS campaigns, BCT and affiliated groups deployed tools that lowered the technical barrier enough for volunteer participants with minimal skills to join coordinated attack waves.

What stands out in the Athenian Tech MITRE ATT&CK mapping of the campaign is the Amplification stage, the sixth and final step of the kill chain observed. After defacement, the groups archived their work on Zone-H, DefacerID, and Haxor.id, then broadcast those links via Telegram and X. The attack itself was not the endpoint. The documentation and amplification of the attack was the strategic objective.



What Should the Indian Industry Do Now?

Athenian Tech Research's recommendations stem from the 51 days of direct observation of how these actors operated, what they targeted, and how they amplified their impact. They are structured around three pillars.

The first is preventive preparedness. This means auditing dark-web marketplaces for leaked credentials, enforcing zero-trust architecture with conditional MFA across all external access paths, implementing 24 to 48-hour patching cycles for Internet-facing appliances, and training employees on social-engineering attacks themed around the current conflict. WhatsApp APK delivery and deepfake-enabled phishing are expected to increase as tensions persist.

The second is active defence. Athenian Tech recommends real-time alignment with CERT-In and NCIIPC advisories; threat hunting focused on VPN logs and edge devices for web shells, Cobalt Strike beacons, and anomalous DNS patterns; and AI-augmented SOC capabilities. Signature-based detection fails against the polymorphic malware and living-off-the-land techniques observed in this campaign. Geographic traffic monitoring, scrutiny of Middle Eastern IP ranges, and active surveillance of hacktivist Telegram channels for #OpIndia activity are necessary at this threat level.

The third pillar is resilience and recovery. Air-gapped, immutable backups are essential for ICS/OT systems, core banking platforms, and healthcare infrastructure. Organisations must develop crisis-specific incident response playbooks covering DDoS attacks, ransomware with data exfiltration, supply-chain compromises, and disinformation campaigns. Cyber-insurance policy exclusions require urgent review, given that the kinetic-cyber hybrid nature of this conflict sits uncomfortably close to standard acts-of-war clauses.

DragonForce Ransomware Strikes Kopran Pharma with Double Extortion

On 4 April 2026, **DragonForce** listed data from Kopran Limited and Kopran Research Laboratories Limited on its dark web leak site. This marked one of India's most significant pharmaceutical-sector breaches in recent months. Kopran is a well-established Indian pharmaceutical company with over six decades of industry experience. The pharma giant was targeted by one of the most active ransomware-as-a-service groups in the cybercriminal ecosystem. Threat intelligence platforms confirmed the listing, and the group claimed to have exfiltrated nearly 284 GB of data. At the time of reporting, the company had not issued a comprehensive public disclosure.

The attack follows DragonForce's established double-extortion playbook: encrypting victim systems while threatening to publish stolen data unless a ransom is paid. Since emerging in late 2023, the group has listed dta from hundreds of organisations on its dark web leak site. It also continues to show cross-platform deployment capability across Windows, Linux, and NAS environments. Its targeting of Kopran reflects a broader strategic shift among ransomware groups. They have moved beyond manufacturing and IT services to target pharmaceutical and life sciences organisations. Their proprietary research data, regulatory submissions, and batch manufacturing records carry exceptional intelligence value.

Latest Cyber Breaches

What distinguishes the Kopran attack in India's pharmaceutical sector is the nature of the potential compromise. A pharmaceutical company's data is not merely commercially sensitive. It may include clinical trial records, drug formulation data, supply chain contracts, and regulatory correspondence with the Central Drugs Standard Control Organisation. In the wrong hands, such data can be weaponised for commercial espionage, competitor intelligence, or dark web monetisation. For an industry navigating tougher global regulation, the reputational and operational consequences can far outlast the immediate ransom demand.

In 2026, DragonForce remains one of the most significant ransomware groups threatening to the Indian industry. Its cartel-like model is based on actively recruiting affiliates on dark web forums and sharing profits from successful attacks. This has helped it maintain a high volume of victims across financial services, pharmaceuticals and manufacturing. Indian organisations in regulated industries need to view DragonForce as a structural, rather than episodic, risk. This requires continuous posture assessment, rather than just periodic patching.

Mahyco Private Limited Targeted by TheGentlemen Ransomware

On 08 April, 2026, threat intelligence trackers reported that **TheGentlemen** had breached Mahyco Private Limited. Mahyco is one of the leading agricultural biotech companies in India and is a pioneer in hybrid seed development since 1964. TheGentlemen is a Ransomware-as-a-Service group that was founded in mid-2025.

Its dark web listing confirmed data exfiltration, of Mahyco Private Limited, though the volume and nature of the compromised data has not been publicly verified. The incident placed a foundational Indian agri-biotech institution within a cybercriminal target set. That set has traditionally focused on consumer goods, manufacturing, and professional services organisations.

Mahyco's significance to the Indian agricultural ecosystem cannot be overstated. It develops and distributes hybrid seeds across multiple crop varieties. Its intellectual property portfolio includes proprietary germplasm data, breeding research, field trial documentation, and distribution network intelligence. The compromise of such data is not only a commercial risk to the organisation. It can also create strategic risks for the broader agricultural supply chain. Seed development is an inherently long-cycle industry, where one proprietary hybrid can represent years of research investment. Premature exposure of that work could fundamentally alter the commercial landscape.

TheGentlemen is assessed by threat intelligence researchers as a relatively sophisticated RaaS operative. It primarily targets consumer goods, manufacturing, materials, and professional services organisations across the United States of America, Brazil, Thailand, France, and Spain. The targeting of Mahyco represents an expansion into India's agricultural technology sector.

This sector has historically received less cybersecurity investment than financial services or IT. For India's agri-biotech companies, the Mahyco case is a structural warning. Sectors that were not primary ransomware targets can quickly become high-value opportunities. Threat actors are refining their understanding of which data types command the highest extortion or resale value.

Talentely Breach Exposes 500K+ Records, Warnings for the Education Sector

On 28 April 2026, India's Data Breach Intelligence Hub documented a critical-severity data breach involving Talentely, a career-focused platform under Veranda Learning Solutions that bridges students and employment opportunities. A threat actor published what is alleged to be a database of 514,412 records.

Classified at the highest severity level, the exposure is among the most significant breaches affecting the Indian education-linked technology in early 2026. The compromised records are believed to contain personally identifiable information. However, a full forensic accounting of the dataset had not been confirmed at the time of reporting.

Talentely's role as a platform aggregating student and graduate profiles gives this breach a particularly acute dimension. Such platforms typically hold academic credentials, employment aspirations, contact details, and sometimes financial information linked to course enrolments. For young professionals, digital footprints are often concentrated on these types of platforms.

Exposure to threat actors creates persistent risks of identity fraud, targeted phishing, and synthetic identity creation. Financial breaches can often be mitigated by freezing accounts or replacing cards. By contrast, exposed career and academic profiles create vulnerabilities that are far harder to reverse.

The Talentely breach reflects a broader and deeply concerning pattern in India's edtech and higher education technology sector. Cybercriminals are increasingly attracted to this sector because it combines three valuable characteristics. These are large aggregated databases, weaker security postures than finance or healthcare, and limited enforcement of data protection standards.

Latest Cyber Scams

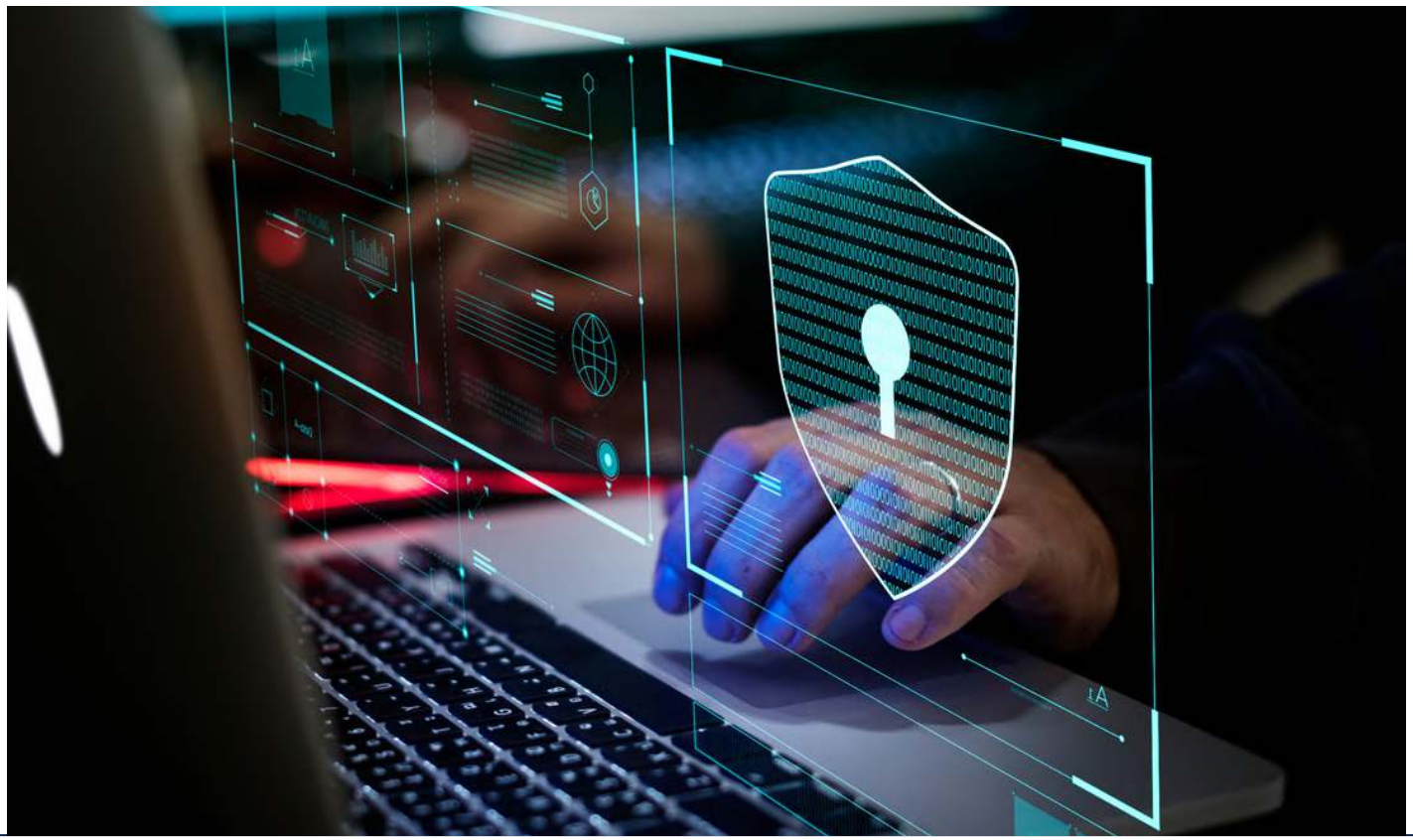
The cyber breaches of April 2026 were marked by technical precision and the quiet work of ransomware operators. In contrast, the cyber scams that swept across India were more intimate and disturbing. April 2026 saw some of India's most consequential law enforcement actions against cybercrimes. Coordinated operations spanned more than twenty states and resulted in thousands of arrests. Yet behind each enforcement headline lay thousands of victims. They were ordinary citizens, retired professionals, and small business owners manipulated through trust, fear, and human psychology. The incidents documented below are united less by technical architecture than by the sustained cruelty of their method.

Operation CyHawk 4.0 Traces ₹519 Crore Fraud Across 20 States

In the early hours of 6 April 2026, more than six hundred police teams, led by the Delhi Police, fanned out across India. They operated simultaneously across more than twenty states and Union Territories. Armed with intelligence profiles, transaction maps, and forensic warrants, the team from Delhi Police's cybercrime units moved against multiple targets. These included mule account operators, illegal call centres, SIM-card syndicates, and cash-withdrawal agents. The action became one of the most consequential digital law enforcement operations in India's history and was coined Operation CyHawk 4.0. Conducted on 6 and 7 April 2026, the 48-hour blitz followed a month-long intelligence exercise. It was carried out with India's Cyber Crime Coordination Centre under the Ministry of Home Affairs.

The results were staggering. Operation CyHawk 4.0 produced 1,429 arrests and apprehensions, alongside the registration of 499 new FIRs. Investigators traced over ₹ 519 crore in fraud proceeds moving through layered mule account networks. More than 8,371 suspects were questioned across participating states. Forensic examination of seized devices is ongoing. The operation targeted the full operational ecosystem of India's cybercrime syndicates. It covered mule account holders, SIM-card suppliers, call centre operators, and cash-out agents. Together, these actors convert digital balances into physical currency before investigative systems could trace them.

The operational architecture revealed by CyHawk 4.0 illustrates how modern Indian cybercrime syndicates operate. These are not opportunistic, disorganised groups of individual fraudsters. They operate with the structural discipline of a corporate enterprise. Their systems include tiered roles, commission-based pay, standardised scripts, and geographic separation of tasks. This separation is designed to prevent any single individual from seeing the full operation. Their financial layering methods are sophisticated enough to frustrate rapid asset freezing. Earlier in 2026, the Supreme Court of India directed the Central Bureau of Investigation (CBI) to prioritise digital arrest scam investigations. CyHawk 4.0 prosecutions will test India's ability to convert enforcement scale into durable legal accountability.



Hyderabad Police Expose Bank Insiders Behind India's Cyber Fraud Ring

While CyHawk 4.0 targeted front-line cybercrime operators, Hyderabad Police's Operation Octopus 2.0 went after something more structurally alarming. Announced in late April 2026, the operation targeted the financial infrastructure that makes stolen money usable. Special investigative teams were deployed across nine states in connection with 101 registered cases.

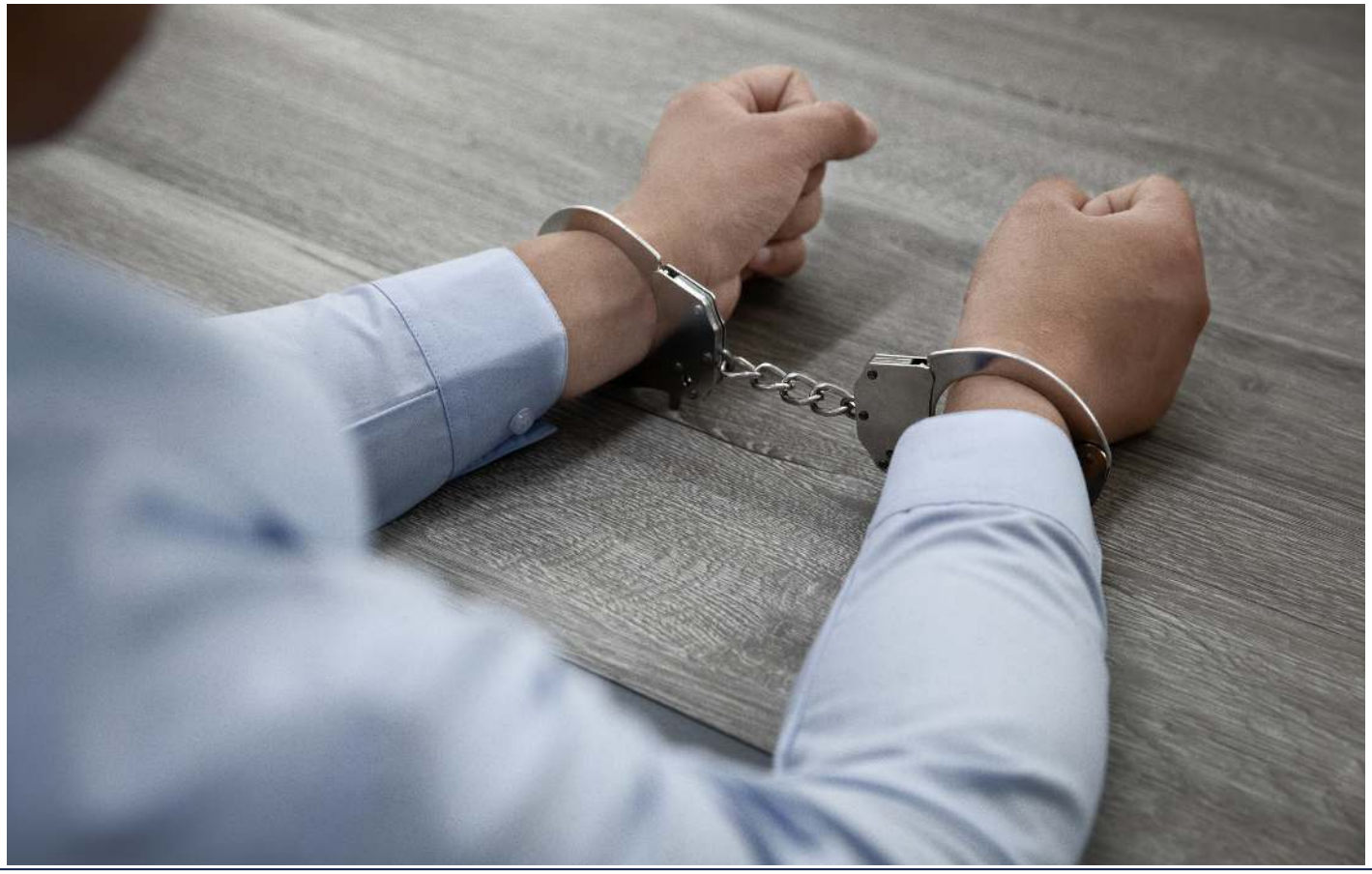
Hyderabad's Cyber Crime Police arrested 52 individuals whose roles exposed a troubling vulnerability in India's banking system. The striking part is that of those 52 arrests, 32 were bank officials. They included branch employees, KYC approvers, relationship managers, and field officers. These officials had allegedly been selling mule account services to criminal networks for direct financial compensation.

The mechanics of what these officials allegedly provided were simple, yet deeply damaging to India's financial system. When a cyber fraud victim transfers money, the same cannot remain in one account without triggering monitoring systems. Criminal networks, therefore, need freshly opened, apparently legitimate bank accounts. These accounts allow funds to be deposited and dispersed across layers before a freeze order is executed.

The 32 bank officials arrested in Octopus 2.0 are alleged to have supplied this infrastructure. They allegedly opened accounts on demand for people they knew were linked to criminal networks. They also delivered ATM cards, debit cards, and cheque books to order. In return, they received payment for each account supplied.

The Banking Insider: India's Most Overlooked Cyber Fraud Enabler

The bank insider dimension of India’s cyber fraud ecosystem is not new to investigators. However, 32 banking official arrests in one operation marks a significant escalation in enforcement capability. The case also shows how deeply criminal infrastructure has penetrated legitimate financial institutions. During April 2026, Hyderabad’s Cyber Crime Police registered individuals in cases spanning multiple fraud categories. These included investment fraud, trading fraud, digital arrest, social media fraud, matrimonial fraud, credit card fraud, FedEx scams, dating scams, and lucky draw fraud. The operation refunded approximately ₹ 69.9 lakh to identified victims by its conclusion. This was meaningful, but necessarily partial, restitution given the scale of the underlying fraud.



Retired Engineer Loses ₹10.3 Crore in Fake Courier Digital Arrest Scam

On 30 April 2026, the CBI took over a major digital arrest investigation. The case involved a 73-year-old retired engineer from New Delhi who was defrauded of approximately ₹ 10.3 crore after a months-long ordeal by his tormentors. It all began with a single phone call in October 2024. The case represents one of the largest individual losses attributed to a digital arrest scam in recent times.

It also shows the psychological architecture that makes this category of fraud so reliably effective. The victim was first contacted by people claiming to be employees of a multinational courier company. They told the unsuspecting victim that a parcel coming from Taiwan, in his name, had been intercepted at the Mumbai Airport, and stated that the package contained banned narcotics.

What followed was a textbook execution of the digital arrest methodology. The fraudsters instructed the victim to download a video-calling application and maintained unbroken contact, with him, for nearly eight hours. During the call, he was introduced to people posing as senior crime branch officials. They presented fabricated case files, alleged criminal charges, and threats of imminent family harm.

Those threats specifically targeted his children living abroad. The pressure was sustained, layered, and calibrated to stop him from consulting his family or contacting anyone, even legitimate authorities. Under this coercion, he transferred approximately ₹ 10.3 crore across multiple bank accounts. The fraud came to light after his family intervened and approached the police.

Preliminary investigations found that the defrauded amount had been routed through several bank accounts in layered transactions. Investigators identified indications that the masterminds operated from abroad, while domestic associates handled victim profiling and fund movement. Agencies have so far frozen approximately ₹ 60 lakh linked to the fraud, merely a fraction of the total loss suffered by the victim. This highlights how quickly criminal networks disperse proceeds across jurisdictions before recovery action begins. The CBI's involvement shows how seriously the government is treating high-value digital arrest cases. It also recognises that such investigations require intelligence reach well beyond state police boundaries.

FedEx Impersonation and Social Media Profile Takeover Scams Rise Sharply

Among the fraud categories driving enforcement action in April 2026, two stand out for their broad demographic reach. These are FedEx and courier impersonation scams, and social media impersonation fraud. Both exploit the victim's assumption that they are dealing with legitimate institutions or a known individual. However, they operate through different channels and affect the victim psychology. FedEx scams, a variation of digital arrest fraud, remain effective despite extensive public awareness campaigns. The initial call is designed to trigger panic before the victim can access counter-information. Claims about contraband, drugs, or illegal currency in a parcel create an immediate fear response, in unsuspecting victims, that overrides rational evaluation.

Social media impersonation fraud operates through a slower and more intimate mechanism. Fraudsters create near-identical copies of profiles belonging to trusted contacts, family members, or senior colleagues at work. They use these fabricated profiles to approach victims with urgent requests for money, investment participation, or sensitive information. The approach has become more effective as generative AI tools have improved.

These tools can produce convincing profile photographs, credible biographical details, and contextually appropriate conversational histories. In several April 2026 cases, victims received video messages that appeared to come from known individuals. Deepfake technology was used to generate convincing moving likenesses.

The convergence of FedEx-style fear induction and AI-powered impersonation marks a deeply unsettling frontier in India's cyber fraud landscape. What was once a challenge of social engineering is becoming a challenge of synthetic reality. Distinguishing genuine from fraudulent communication now requires verification tools that most ordinary users lack. The IT Amendment Rules 2026 mandate three-hour deepfake takedown timelines for platforms. They also require intermediaries to deploy automated detection tools, which represents a meaningful policy response to the threat. However, regulation moves on institutional timelines. Deepfake-enabled fraud moves at the speed of a single message or a thirty-second video call.

DPDP Act, 2023 Compliance Reshapes India's Data Governance Landscape

Through the first quarter of 2026, India's Digital Personal Data Protection (DPDP) Act, 2023 began moving from law to compliance reality. CERT-In mandates six-hour incident reporting, while SEBI requires listed companies to disclose major cyber incidents within twenty-four hours. The DPDP Act, 2023 framework also imposes dual reporting obligations for personal data breaches.

Together, these frameworks have created a regulatory landscape that demands dedicated governance infrastructure. Ad hoc incident response is no longer enough. Most Indian mid-market organisations still lack dedicated data protection officers and formal data processing inventories. For them, this convergence represents a significant operational challenge.

The DPDP Act, 2023 defines personal data breach in deliberately broad terms. It includes unauthorised processing, accidental disclosure, acquisition, sharing, use, alteration, destruction, or loss of access to personal data. These incidents qualify when they compromise confidentiality, integrity, or availability. Crucially, the Act prescribes reporting for all types of personal data breaches.

This applies regardless of the breach's sensitivity or its impact on affected individuals. Organisations therefore cannot rely on materiality thresholds they may have used historically. Every breach is, in principle, a reportable breach. The penalties for non-compliance are structured to encourage over-reporting rather than under-reporting.

The practical consequence for India's cybersecurity market is a decisive shift in enterprise investment priorities. Identity and Access Management, Infrastructure Security, and Managed Security Services have become leading segments of cybersecurity spend in 2026. This shift is driven by DPDP Act, 2023 and advisories by CERT-In, and sector-specific regulators such as the Reserve Bank of India (RBI) and Insurance Regulatory Development Authority of India (IRDAI). Organisations that treat DPDP Act, 2023 compliance as a checkbox exercise will remain exposed. Adding documentation to an unchanged security infrastructure is not enough. They risk regulatory penalties and the structural vulnerability that often accompanies non-compliance. India's most resilient enterprises are treating DPDP Act, 2023 as a data governance framework, and not merely as a legal obligation.

India's Enterprises Adopt Zero Trust as Mandatory Security Architecture

For several years, Zero Trust architecture occupied an aspirational position in Indian enterprise security conversations. It was widely acknowledged as a best practice and was frequently referenced in security strategy documents. Yet it was often deferred in favour of shorter-term tactical priorities. April 2026 marks the point when deferral ceased to be viable for many security analysts. The Reserve Bank of India's Fintech Regulation and Ethics in AI committee has mandated zero-trust architecture for banks and NBFCs. This requirement sits alongside AI-enabled monitoring and compulsory high-value fraud reporting. India's broader regulatory trajectory now expects organisations to have the visibility and access controls that zero trust provides.

The case for zero trust in India is reinforced by threat patterns from the first quarter of 2026. Most significant breaches during this period did not result from novel zero-day vulnerabilities or technically exotic attack chains. They resulted from compromised credentials used to authenticate into trusting systems. Those systems accepted the credentials without questioning the context of the access request. As security researchers often note, today's most dangerous attackers are logging in rather than hacking in. They use stolen credentials, legitimate remote access tools, and trusted vendor relationships. These methods let them move through environments that perimeter defences cannot see. Zero trust is the architectural response to this reality, enforcing continuous verification of every access request.

The operational transition to zero trust in India's enterprise landscape is being driven by three concurrent forces. The first is regulatory pressure from financial sector regulators. The second is growing recognition that hybrid work and cloud adoption have dissolved the legacy perimeter. The third is evidence that breach costs can exceed implementation costs by a substantial margin. Security system complexity remains a significant barrier. Many Indian organisations operate dozens of disconnected security tools. These tools can create blind spots and analyst fatigue instead of genuine visibility. The market response is a shift towards security platformisation, consolidating telemetry, analytics, and response into unified ecosystems. This shift is now visible across India's enterprise security spending patterns.

India's Enterprises Must Start Post-Quantum Cryptography Migration Now

Agentic AI and deepfake regulation have dominated India's cybersecurity attention through early 2026. Yet a slower-moving and ultimately more consequential threat is advancing beneath the daily incident landscape. That threat is the approach of cryptographically relevant quantum computing. The National Institute of Standards and Technology finalised its first post-quantum cryptographic standards in 2024. The global security community broadly agrees that organisations must begin migration planning. Those who delay will face a narrow window before the threat becomes operationally real. For Indian enterprises in financial services, healthcare, defence supply chains, and government-adjacent countries, this timeline is in no way theoretical.

The specific risk that quantum computing poses to current cryptographic infrastructure is well understood. Several algorithms underpin the encryption of sensitive data in transit and at rest. These include RSA, elliptic-curve cryptography, and the Diffie-Hellman key exchange. All are mathematically vulnerable to attacks by sufficiently powerful quantum computers. The timeline for such machines remains contested, with estimates ranging from five to fifteen years. However, the principle of "harvest now, decrypt later" changes the risk calculation. Nation-state adversaries may already be collecting encrypted data today for later decryption. For data with long-term sensitivity, this is an immediate strategic risk. Such data may include classified government communications, pharmaceutical research, or financial transaction records.

India's cybersecurity market response to the quantum threat is nascent but accelerating. Post-quantum security readiness has been identified as a strategic priority in the World Economic Forum's Global Cybersecurity Outlook 2026. Indian enterprises with global operations are beginning to receive guidance from international partners and regulators on migration timelines. For most Indian organisations, the practical first steps are inventory and assessment. From there, they can begin a phased migration roadmap that is aligned to NIST post-quantum standards. Organisations that begin this planning now will be in a stronger position than those waiting for regulatory mandates. By the time mandates arrive, the window for orderly migration may have already closed.

DIY Guide: Staying Safe on Your Home Wi-Fi

Most people set up a home Wi-Fi network once and never think about it again. The router sits in a corner, the password gets shared with guests, devices connected to the route, pile up over the years, and the whole arrangement quietly becomes one of the most exposed parts of a household's digital life. The problem is not the technology. It is the habits that form around it.

A home network is not just an Internet connection. It is the shared infrastructure through which phones, laptops, smart televisions, security cameras, and sometimes work devices all communicate. What happens on that network, and who can see it, depends almost entirely on how it has been configured and maintained.

How Do Home Networks Get Compromised?

The most common entry point is a router that still uses its factory-default username and password. These defaults are publicly documented and are widely known. Anyone who can reach the router's admin panel, whether physically or through a vulnerability, can change the settings, monitor traffic, or redirect connections without the owner ever getting wind of it.

A close second is an outdated router firmware. Manufacturers release firmware updates to patch security vulnerabilities, but most home routers never receive them because the process is manual, and most users do not know it exists. A router running two-year-old firmware may be carrying known, unpatched weaknesses that require no sophistication to exploit.

Shared passwords are another quiet risk. When a Wi-Fi password is given to every visitor, every repairperson, and every neighbour who asked for, the network's exposure grows with each new device that gets connected to it. Devices brought in by others are outside the owner's control, and any one of them could introduce a problem onto the network.

Safe Habits for Your Home Network

The first and most immediate step is to change the default admin credentials on your router. This is done through the router's settings panel, usually accessible by typing a local address like 192.168.1.1 into a browser. The username and password protecting that panel should be unique and not reused from anywhere else.

Check whether your router supports automatic firmware updates and enable that setting if it already does not. If you however, do not want to go via that route then, make it a habit of logging in every few months to check whether an update, in the firmware, is available. It takes ten minutes and removes a category of risks that most households carry without knowing it.

Create a separate guest network for visitors and for smart home devices. Most modern routers support this. It keeps outside devices off the same network segment as your primary laptop or phone, which limits what any compromised device can reach or observe.

Use WPA3 encryption if your router supports it. If not, WPA2 is acceptable. WEP is outdated and should not be used. This setting is found in the wireless security section of the router's admin panel.

A Few Rules to Follow

- Do not leave your router on factory default credentials.
- Do not share your primary Wi-Fi password with guests or temporary visitors.
- Do not connect work devices and personal devices on the same unsecured network without a firewall or separation in place.
- Do not ignore firmware update notifications from your router's manufacturer.
- Do not assume that because a network is password-protected, everything on it is private from other connected devices.
- Do not keep routers running indefinitely without a periodic restart, as memory-based vulnerabilities can persist across long uptimes.

The goal is not to turn a home network into a fortress, but to close the gaps that could make it an easy target. Most home network compromises do not involve advanced techniques. They involve default passwords that were never changed, updates that were never applied, and access that was shared a little too freely. Addressing those three things puts a home network in a considerably better shape.

Athenian Tech

Contact Us

www.atheniantech.com