ATHENIAN TECH

NEWSLETTER

April 2025

THREAT INTELLIGENCE BY ATHENA

From the Editor's Desk

In today's interconnected world, real-world events increasingly echo through the digital realm. The incident that hogged the limelight in India, and whose repercussions can still be felt in cyberspace, is the happenings in Pahalgam, a hill station in the Anantnag district of Jammu and Kashmir Region. The Pahalgam attack stands as one of the most gruesome acts of terrorism in modern Indian history.

IN THIS NEWSLETTER

Issue #02

On the fateful day of 22 April, militants gunned down 26 innocent tourists in one of the most idyllic hill stations in the country. The heinous act by terrorists led to relations between India and Pakistan reaching a new low. India, which was at the receiving end of such an act of terror, took a slew of measures, important among them being keeping the Indus Water Treaty in abeyance and asking Pakistani nationals to leave India within a specified date, in this case, 27 April. The acts of terror on the ground not only led to world leaders extending their support to India but also showed the world that India was the aggrieved party. While India increased pressure on Pakistan in the real world, hacktivist groups linked to Pakistan rallied together to not only spread the anti-India narrative but also, through their acts, tried to spread a fear psychosis among the Indian public.

While these hacktivist groups did attempt to penetrate the defence establishment or institutions associated with them, they even tried to destabilize the democratic fabric of India by intruding into the database of the High Court of Andhra Pradesh. It must be remembered that most of the actions by these groups after the incident in Pahalgam were primarily symbolic, rather than genuine attempts to cause widespread fear and disruptions in India.

Such incidents, such as the one in Pahalgam, reinforce that while protecting our borders, it is equally important to keep our cyberspace safe by maintaining proper cyber hygiene. This is very important in the present day. According to our analysts, the intrusions in cyberspace by hacktivist groups linked to Pakistan represented a coordinated model of hybrid warfare (against India), where digital breaches deliver not only data but also psychological payloads aimed at undermining institutional trust and national morale.

Compounding India's cybersecurity woes is the simultaneous transformation of the leak economy. Since the takedown of *RaidForums* in April 2022, dark web actors have been rebuilding. But in April 2025, fragmentation deepened. Two major hubs—BreachForums.st and LeakBase.io—vanished or were abandoned, disrupting the coordination of cybercriminals and hacktivists.

BreachForums.st, long regarded as the successor to *RaidForums,* went offline on 15 April after its moderators admitted to a critical backend vulnerability. While they denied a breach, scepticism grew after someone attempted to sell the forum's source code on *DarkForums.* Many interpreted this as a premeditated exit.

As forums collapsed or were revealed as potential honeypots, cybercriminals scattered to encrypted messaging platforms such as TOX and Matrix or retreated into invitation-only communities. With no central hub left, coordination has become opaque, decentralized, and more complicated to monitor.

This fragmentation offers challenges and rare insights for law enforcement and intelligence analysts. Similar infrastructure reused across successor forums provides a trail of breadcrumbs, hinting at shared actors or repeated mistakes. However, the takeaway is sobering for CISOs and national cyber defenders: the threat has not disappeared—it has simply mutated into something more fragmented, paranoid, and difficult to trace.

The post-Pahalgam cyber offensive and the dark web's crumbling leak economy illustrate a changing landscape. The former uses breaches to seed disinformation and panic, while the latter reveals a threat actor ecosystem increasingly defined not by dominance but by evasion and distrust.

India must now prepare to defend its networks and neutralize the narratives these breaches enable. In this age of digital hybrid warfare, perception is as potent as penetration, and psychological disruption may outlast the breach itself.
Welcome to the second issue. We look forward to walking on this road with you. We will be more than happy to incorporate your views in this newsletter if you have any. So feel free to share your questions and opinions at pankaj.toppo@atheniantech.com. Till we meet again, happy reading.

Pankaj Anup Toppo

Cyber Escalation Post Pahalgam: India Confronts a New Age of Narrative Warfare

The 22 April the terrorist attack in Pahalgam, which claimed 26 civilian lives, sent immediate tremors through India's security establishment. What is however, worth noting that the reverberations, of this macabre incident have not been confined to the physical domain. Post the incident in Pahalgam, a digitally distributed campaign followed, against India, less a string of isolated attacks, more a cohesive escalation of cyber operations designed to erode public trust and exhaust institutional resilience, in India.

In the days following the terrorist attack at Pahalgam, India has found itself at the receiving end of an asymmetric cyber offensive orchestrated by a constellation of threat actors with ideological, geopolitical, and psychological motives. Athenian Tech's analysts suggest that this wasn't merely retributive hacktivism but an emergent model of coordinated digital warfare, defined not only by breaches but also by the narratives they seeded through their actions, in cyber space.

Judicial Breach: An Institutional Symbol Targeted

On April 29, Pakistan-linked hacktivist group Team Insane PK announced it had breached the Andhra Pradesh High Court's database. A 2.5GB data dump containing SQL logs, personnel records, and internal case scripts was released. For observers, the implications were twofold: technical access to sensitive systems and a calculated strike against the machinery of Indian democracy.

Unverified claims of additional defacements on Rajasthan government subdomains have circulated, suggesting the group's objective extended beyond disruption to include high-visibility psychological impact.

Police and Academic Data: An Institutional Symbol Targeted

Elsewhere, Delhi Police records surfaced on a dark web forum known for hosting threat actor discussions. Screenshots shared by a user identifying as *@h4ck3r* on DarkForums pointed towards an unauthorized access to crime databases through phpMyAdmin—possibly via credential reuse or SQL injection. The leak's packaging was more troubling than the leak itself: it came accompanied by false-flag claims around the Pahalgam attack, aiming to obscure attribution and sow public confusion.

Meanwhile, on 28 April, a group identifying itself as *V for Vendetta Cyber Team* released a leak archive titled **OPINDIAN.zip,** comprising data harvested from institutions such as IIT Delhi, IIT Mandi, and the National Academy of Agricultural Sciences (NAAS), New Delhi. Collected through outdated CMS exploits and password reuse, the cache included student rosters, financial records, and internal research archives—underscoring the vulnerability of India's intellectual capital in the cyber domain.

Meanwhile another hacktivist group *The Anonymous* 71 defaced NAAS's official website in a related follow-on. Experts believe that the attackers utilized credentials or code fragments exposed in the OPINDIAN leak—demonstrating how breaches now function as handoffs between loosely coordinated actor groups.

Misinformation as Modality: TRF's Disinformation Drive

Adding another dimension, The Resistance Front (TRF), a known separatist-affiliated group, circulated documents purporting to be internal communications from Indian intelligence agencies. Though forensic analysis remains unclear on the authenticity of the documents, the objective was clear: undermine public faith in counter-terror operations by implying internal complicity in the Pahalgam incident.

Such efforts underscore a shift in tactic: from penetrating networks to manipulating public perception.

Strategic Targets and Psychological Payloads

Cyber operations have also targeted India's defence and financial sectors. A claim from the Pakistan *Cyber Force alleges* a breach at **Hindustan Aeronautics Limited (HAL),** with purported access to documents linked to the LCA Tejas fighter programme. Although unverified, the authentic leak would represent a significant compromise of intellectual property.

In a separate incident, the *Central Bank of India* was at the receiving end of a distributed denial-of-service (DDoS) threat, again from DarkForum's *@h4ck3r*, who claimed access to the bank's confidential customer data. No breach has yet been confirmed, but the tactic reflects a broader trend: leveraging the threat of compromise to project systemic vulnerability.

Further, **TEAMPK,** another Pakistan-aligned group, published personal details of Indian Army veterans online, including their home addresses and their contact details. The targeting of ex-servicemen appears to be a psychological tactic aimed not at gaining a battlefield advantage but to cause emotional demoralization.

A Landscape in Flux: Key Takeaways

What's unfolding is not cybercrime in the traditional sense. It's strategic, distributed, and increasingly psychological in its execution. Several patterns now define the post-Pahalgam threat landscape:

- **Cross-group Exploits:** The NAAS breach exemplified how one leak can fuel subsequent attacks. What begins as infiltration quickly becomes shared infrastructure for follow-on strikes—fostering informal cyber coalitions across ideological geographies.

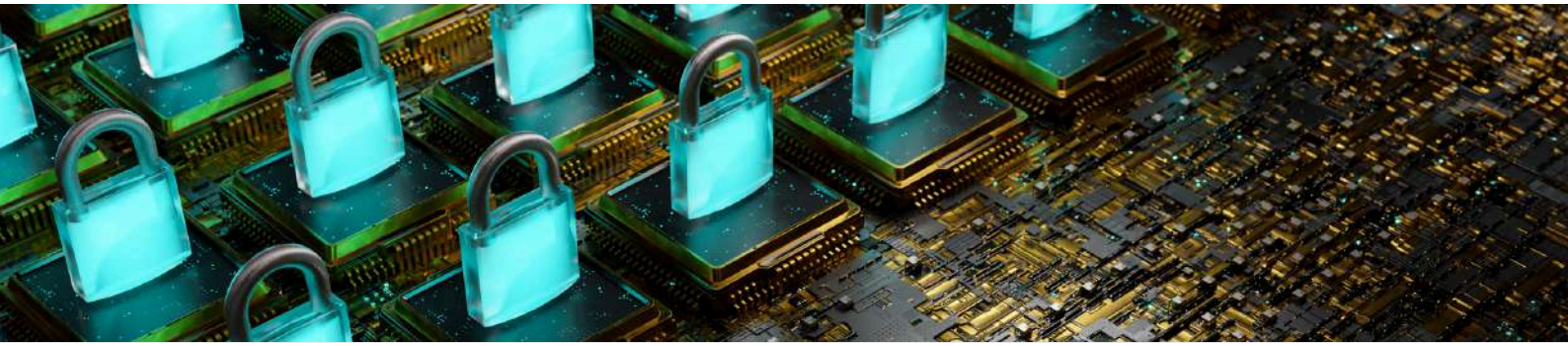
- **Narrative as Payload:** Leaks today arrive not only with data but with context—often false, often misleading. These are operations designed to question state credibility more than to dismantle systems.

- **Emergent Actor Ecosystem:** Groups operating under banners such as *Akatsuki Cyber Team,* Team Insane Pakistan, and *V for Vendetta Cyber Team* reflect an evolving federation of digital adversaries—sharing tools, targets, and narratives.

- **Broadening of Targets:** Institutions once considered peripheral to statecraft, such as universities, courts, and coaching portals, are now primary attack surfaces. It reflects a strategy aimed at simulating a state under siege.

The post-Pahalgam cyber offensive is no longer about persistence. It's about projection. Every leaked database, tampered record, and defaced website feeds into a larger narrative architecture engineered to portray India as vulnerable and reactive.

India must defend its networks and the narrative these attacks seek to fuel and cause further panic as that is more damaging that the actual act itself.



April's Reckoning: The Unravelling Trustscape of the Dark Web

In the shadow of RaidForums' takedown on 12 April, 2022, the dark web's leak economy had been steadily reassembling itself: quietly, cautiously, and consistently with the hum of paranoia. But in April 2025, that uneasy constellation splintered. What emerged was not absence, but something more volatile: suspicion, fragmentation, and an infrastructure in freefall.

By the end of the month, two of the most frequented forums, on the dark web, among cybercriminals—**BreachForums.st** and **LeakBase.io**—had either shut down or had disappeared entirely. What followed was a scramble of revival attempts, each greeted less with enthusiasm and more with scrutiny. Analysts familiar with the cyclical nature of forum takedowns are now in consensus: *April did not mark the death of the leak economy, but the fraying of its social fabric.*

BreachForums.st: A Controlled Retreat or a Camouflaged Exit?

The first rupture came on 15 April. **BreachForums.s**t, the de facto successor to RaidForums, went dark. In a domain where splashy seizure banners often herald takedowns, this one was subdued. The administrators issued a PGP-signed note admitting to a critical zero-day vulnerability in their MyBB backend. The moderators acknowledged no data breach, and users were advised to steer clear of potential clones—some of which, they warned, could be law enforcement traps.

But in spaces built on mistrust, such reassurances rarely suffice. A listing briefly surfaced on **DarkForums,** purporting to sell the source code of BreachForums. For many, that was enough to suspect the exit wasn't defensive but planned and transactional.

Breached.fi: A Resurrected Shell, a Withering Centre

Within days, a new forum emerged: **Breached.fi.** It bore the aesthetics of continuity and was marketed as a safer, community-focused rebirth of its predecessor. The administrator, alias **"Anastasia,"** a former moderator, stated that they were seeking to restore the forum's legacy—sans its operational laxities.

The forum drew initial interest. Then came the unravelling.

A user attempting to verify Anastasia's Telegram channel encountered a law enforcement seizure banner. If compromised, Anastasia's PGP keys could also cast doubt on the forum's very foundation.

Technical breadcrumbs further deepened suspicions. Security researchers identified an unusual open **port 19191** on the server's IP—linked to known threat vectors, including the Bluefire Trojan and OPSEC surveillance tools, according to Virus Total. Though ports can be repurposed, the pattern raised flags.

Soon, a leak from within the platform surfaced, including email addresses and hashed credentials. Confidence eroded swiftly. By Day 5, **Breached.fi was offline.** Many now regard it as a honeypot—perhaps an intentional sting, perhaps a platform that was compromised before it ever took off.

BreachForums.sx: A Fork in Familiar Soil

Then came **BreachForums.sx,** launched around 30 April by a former moderator known as **"Momondo."** He distanced himself from the prior teams, citing inadequate OPSEC and poor crisis response. His platform promised a clean start—ethically and technically.

But by now, the trust had curdled into suspicion.

A user named Krekti flagged several overlaps between BreachForums.sx and Breached.fi. These weren't cosmetic. Both forums reportedly resolved to the same **.onion backend.** Outgoing emails bore **identical SMTP headers**. More alarmingly, depending on the domain used to access the site, visitors encountered either a login prompt—or a spoofed law enforcement seizure notice.

In earlier eras, such inconsistencies might have been blamed on incompetence. In today's hardened dark web culture, however, they are taken as signs of entrapment.

LeakBase.io: The Quiet Disappearance

While the BreachForums ecosystem was publicly convulsing, **LeakBase.io** vanished with barely a whimper. Known for credential stuffing and lookup tools, the platform had quietly enabled a large cohort of mid-tier actors. There was no farewell post, no redirect, and DNS records simply stopped resolving.

Speculation has filled the vacuum: law enforcement action, internal sabotage, or burnout. Whatever the cause, the void has scattered users into smaller, closed venues—some encrypted, most invitation-only, all wary.

What Remains: A Culture of Suspicion

Across this newly scattered terrain, what stands out is not an absence but a recalibration of trust. With few reliable figures left—*Loki* and *Tanaka* among the missing, either by choice or compulsion—users have turned inwards.

Today's dark web is not built to scale but to survive.

New forums are rarely public. Users inspect onion service hashes, trace TLS certificate reuse, and dissect email headers before engaging. Forums aren't seeking popularity. They're seeking insulation from law enforcement agencies, rivals, and the ghosts of the forums past.

To threat intelligence observers, the overlaps between **Breached.fi, BreachForums.sx,** and the original BreachForums offer rare attribution breadcrumbs. Reused infrastructure, backend code similarities, and even identical SMTP patterns can illuminate actor behaviour across takedown events.

For **law enforcement agencies,** the discourse is an opportunity. However, fragmentation is also a setback: the shift toward **TOX, Matrix,** and custom peer-to-peer channels reduces visibility.

For **CISOs,** the forum closures bring no comfort. Data from older breaches will continue to surface, often through even less traceable channels. The threat is not gone; it has simply become less legible.

April 2025 will certainly not be remembered as the end of the dark web's leak economy. It will be remembered as the moment it mutated into something opaquer, less trust-based, and infinitely more complex to index.
The architecture has not crumbled but merely retreated into the shadows.

ISMG Cyber Security Summit, Mumbai 2025: Cyber Resilience Moves from Policy to Practice

As cyber threats grow more frequent and fragmented, the conversation around digital resilience is shifting from regulatory alignment to operational readiness. At the **ISMG Cybersecurity Summit** held in Mumbai on 22 April 2025, this shift became visible in panel discussions and how crisis response was simulated, tested, and dissected.

A highlight of the summit was a live **cyber breach simulation,** in which Athenian Tech's CEO and Founder, Kanishk Gaur, assumed the role of CEO, along with other executives from various companies assuming the roles of DPO, CISO, and the legal counsel responding to a real-time data breach. The focus was not on novelty but on practical sequencing: who activates first, how communications are cascaded, and when regulatory engagement begins.

What stood out was the **coordination model:**

- A centralized command structure was formed within minutes of breach detection.
- Business Continuity Planning (BCP) was invoked immediately to protect downstream operations.
- A pre-drafted Crisis Communication Plan was deployed to ensure consistency across internal and external channels.

The lesson was clear: resilience isn't only about having tools but about how decisions flow through a system when the stakes are high.

These exercises became even more relevant when framed against India's **Digital Personal Data Protection (DPDP) Act, 2025.** Regulatory compliance is now dynamic, not just legal, and response architecture must reflect that shift.

Beyond crisis handling, the summit explored broader **emerging trends**. Sessions led by industry veterans like **Sameer Ratolikar (HDFC Bank)** and **Vishal Salvi (Quick Heal Technologies)** moved the discussion towards **AI-assisted detection, zero-trust access**, and **identity-first frameworks.** These are no longer conceptual—they're becoming operational defaults.

A particularly relevant takeaway was that **identity fabrics** are emerging as connective tissue across cloud and on-prem environments. Rather than defending the perimeter, enterprises are refactoring around who (or what) requests access, from where, and under what context.

We include these developments not for spectacle, but for signal. The shift from policy to practice is underway. In a post-breach world, success won't be measured by whether a breach occurred but by how intelligently and coherently institutions respond.

IBM Bets on Quantum Resilience: From Algorithm to Architecture

While the cybersecurity industry remains focused on known threats like ransomware variants, supply-chain breaches, and zero-day exploits, IBM is preparing for a different disruption. In April 2025, the company announced a sweeping **$150 billion investment in U.S. technology infrastructure**, with **$30 billion allocated explicitly to quantum computing and mainframe modernization.**

The rationale behind this move is urgent and forward-looking. As quantum computers edge closer to practical viability, their eventual ability to break classical public-key encryption algorithms is no longer theoretical. The threat landscape may not yet be quantum-active, but it is increasingly quantum-aware.

IBM's strategy is centred around **quantum-safe cryptography,** a class of algorithms resistant to decryption by quantum computers. On 23 April 2025, the **U.S. National Institute of Standards and Technology (NIST)** formally recognized IBM's cryptographic designs as part of the first global post-quantum standards. This milestone will guide global encryption upgrades in the years to come.

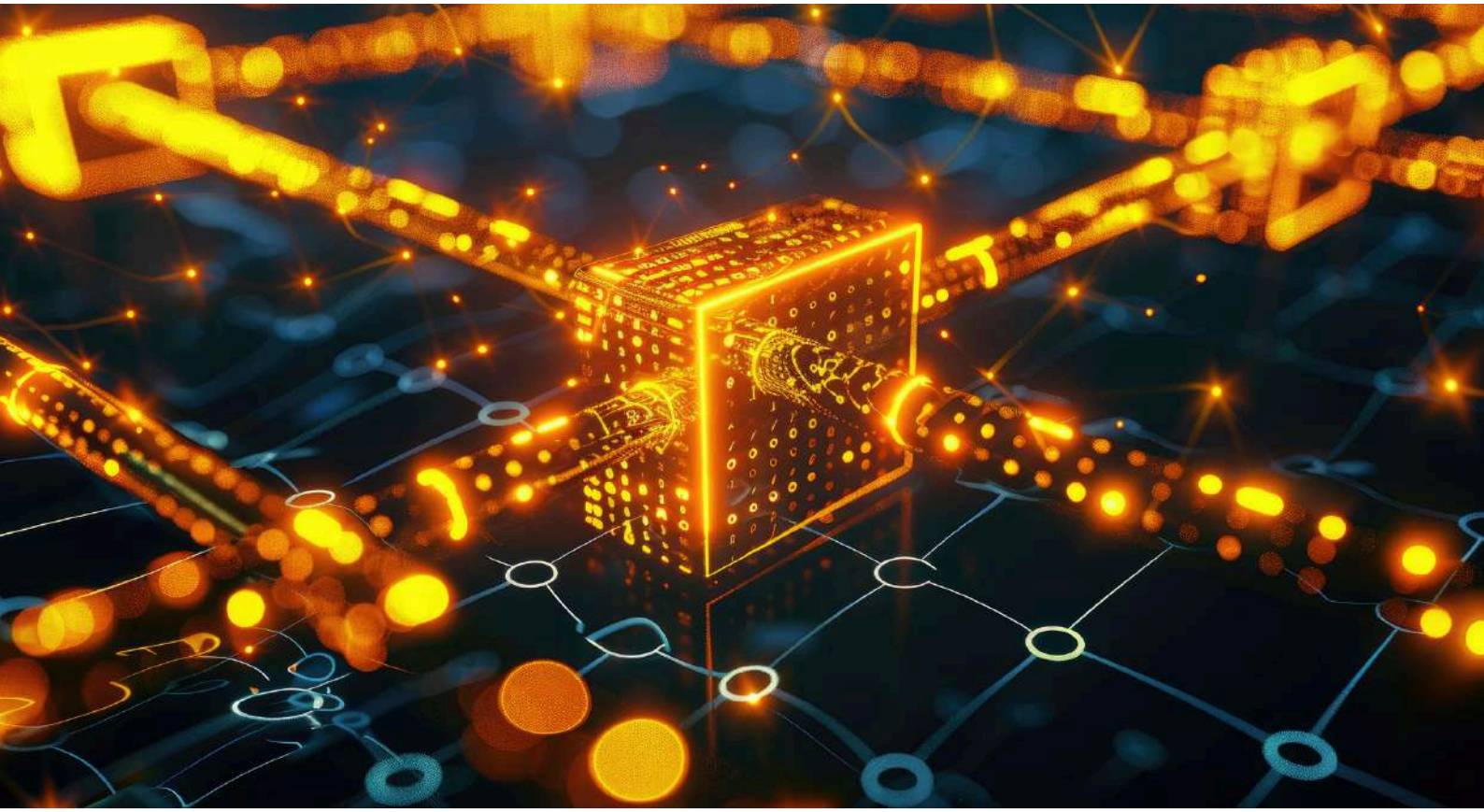
To accelerate adoption, IBM has partnered with fintech platform **BillGo,** integrating lattice and hash-based cryptographic methods into payment workflows and data handling layers. These algorithms are engineered to withstand Shor's algorithm and other quantum decryption techniques, securing sensitive transactions before the threat fully materializes.

However, IBM's quantum initiative is not limited to cryptographic tools. The company is also advancing an **identity-first security model**, where digital identity becomes the foundational control point across hybrid and AI-integrated environments. Central to this vision is the concept of **identity fabrics:** modular, standards-based systems that enable secure, policy-driven access across cloud, on-premises, and quantum-influenced infrastructure.

This approach acknowledges a structural shift already underway: in a world where data moves fluidly and users span human and machine identities, **resilience must come from integration, not perimeter controls.** Identity fabrics allow access governance to be contextual and cryptographically enforced—ensuring that the shift to post-quantum encryption is not bolted on, but embedded at the core.

We highlight IBM's direction not as an endorsement but as an indication. The threat of quantum decryption may not be immediate, but the timeline for mitigation is. Organizations planning for long-term data security, especially in finance, defence, and healthcare sectors, cannot afford to delay.

The future of encryption is not only mathematical. It is architectural.



From Signals to Decisions: AI Redefines the Security Stack at RSAC 2025

As cybersecurity threats grow in velocity, complexity, and volume, traditional perimeter-based defence models are being rethought, not in theory but in deployment. At this year's **RSA Conference 2025** in San Francisco, the emphasis shifted from static controls to adaptive, AI-anchored decision architectures, revealing not just where the field is headed but what security must now *become*.

Among the most closely followed developments was the rise of **agentic AI**—a class of autonomous systems capable of reasoning, triaging, and initiating responses with minimal human input. Where artificial intelligence has historically served as a detection aid, these systems are being positioned as autonomous decision-makers, particularly within threat response loops. From LLM prompt injections to AI model manipulation, sessions underscored that the tools designed to protect are now part of the attack surface.

This transformation was reflected in several product launches. **Google** unveiled its Gemini-augmented threat telemetry platform, focused on real-time decisions at the edge. **Cisco,** meanwhile, introduced model-hardened firewalls built to detect adversarial interactions within enterprise AI environments. A common theme emerged: *intelligent systems require intelligent controls, closer to the point of interaction, and awareness of the actors they serve.*

Equally telling was the focus on **identity-first architectures.** With distributed users, APIs, and machine agents operating across fragmented infrastructures, identity is increasingly seen as the single point of policy enforcement. Discussions around identity fabrics and **context-aware access controls** reinforced this trajectory, particularly for enterprises navigating sovereign data regimes and global compliance.

In this environment, we at **Athenian Tech Limited** made a timely debut. Backed by the UK's Department for International Trade and Plexal, we presented our privacy-first solutions, ranging from executive identity protection *(Thunderbolt)* to real-time ransomware prediction through its AI engine. We showed how our tools are designed for detection and interpretation, offering CISOs geopolitical overlays and operational clarity in moments of crisis.

We highlight these developments not for hype, but for their real-world directionality. The shift underway is structural. In a world of machine-speed threats, resilience will come not from more alerts—but from faster, context-driven decisions made closer to the source of risk. As this convergence accelerates, the question is whether AI will shape cyber defence or whether your architecture is prepared to meet it.

How to Stay Safe in a Hyper Connected World?

As our coverage this month reveals, from the fragmentation of dark web ecosystems to geopolitically driven disinformation campaigns, **cyber threats have entered a new operational phase.** They are no longer defined by singular breaches but by **slow compromises**, made possible not through systems alone but **by human habits.**

In a world redefined by agentic AI, rapid payments, and synthetic identities, the frontline of cybersecurity is increasingly behavioral. Voice calls, messages, deepfakes, and cloned interfaces now target the individual directly: at speed and scale. The breach doesn't always arrive with a payload. Sometimes, it walks in cloaked in routine.

Below are key steps you should follow, not in theory, but in practice:

Fraudulent Authority Calls

It often begins with a phone call, seemingly from a law enforcement official or a regulatory agency. The voice is calm, scripted, and precise. You're told that your name has surfaced in a case involving financial irregularities. There's a sense of urgency, but also clarity. All they need is verification. In that moment, the instinct to cooperate overrides the impulse to confirm. No official investigation operates like this, but in that pause, the damage is often already done.

Romance-Based Fraud

Some attacks don't rely on panic, they rely on patience. A message, a friend request, a slowly built connection. Fraudsters invest weeks, sometimes months, in cultivating rapport. The eventual ask: money, personal details, or intimate material doesn't come as a red flag. It arrives as a continuation of trust that has already been earned, in due course. When exploitation is disguised as affection, the breach leaves more than just technical scars.

Messaging-Based Banking Scams

On platforms like WhatsApp or SMS, attackers mimic institutional language with surprising accuracy. You're informed that your bank account is at risk, your PAN card is flagged, or your KYC is incomplete. A link is provided to update the same. The whole game seems and looks very plausible. But these messages don't aim to inform, they aim to rush you. Banks never use such channels for sensitive requests with their customers. But the interface is close enough. And when trust is compressed into seconds, mistakes become measurable.

Payment Requests via QR or UPI

The same speed that enables frictionless payments also enables real-time deception. Fraudsters send altered QR codes, unexpected refund requests, or UPI push prompts disguised as customer support. The transaction feels routine, until it isn't. In systems designed for immediacy, fraud doesn't need time. It just needs silence.

Job Offers Demanding Fees

A high-paying remote role. A legitimate-looking offer letter. A small fee for onboarding. The details are convincing but the channels are informal, and the verification almost always breaks down under scrutiny. The goal isn't employment. It's exposure. In a job market flooded with urgency and optimism, exploitation often dresses itself as opportunity.

Phishing and Support Impersonation

Scammers now pose as helpdesk agents from e-commerce platforms, banks, and subscription services. They call or message first, anticipating problems that don't exist. When you respond, they offer to fix it but require remote access or verification codes. Official support teams never initiate contact this way. But when a problem is pre-empted before it's even felt, suspicion can feel misplaced.

Unsecured Public Wi-Fi

Free Wi-Fi in cafes, hotels, or airports offers easy connectivity, and subtle vulnerability. On open networks, attackers can intercept traffic without needing direct access. Sensitive logins, transaction credentials, and session cookies can be captured in transit. A VPN helps—but awareness helps more. Not all threats are visible on screen.

Password Reuse and Weak Credentials

Even strong passwords become vulnerable when reused across services. If one site is compromised, attackers often test the same credentials elsewhere—a tactic known as credential stuffing. Password managers help break that chain. They ensure that a breach in one place doesn't become a breach everywhere.

Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) has moved from it being recommended to it being essential. Yet many still rely solely on SMS verification—susceptible to SIM swaps and interception. App-based authenticators, though slightly more effortful, provide stronger control. In systems where credentials are shared or federated, the second layer is often the one that holds.

Delayed Updates and Unpatched Systems

Security patches often arrive before public awareness of the vulnerability they address. But update prompts are delayed, ignored, or postponed for convenience. Attackers depend on this lag. Systems left even a few weeks behind can become targets. The habit of updating—automatically or proactively—remains one of the most quietly powerful defences.

Unlocked Devices and Poor Endpoint Hygiene

Unlocked laptops. Phones without biometrics. Browsers that remember too much. Physical access remains one of the easiest paths to compromise. Encryption, locking, and local authentication aren't high-friction measures—they're continuity enablers. Devices, like doors, should close behind you.

Manipulated Media and Deepfake Voice Cloning

With tools now able to recreate faces and voices convincingly, attackers no longer need passwords to impersonate. A voice note from a manager. A video call from a known contact. The impersonation may not be perfect, but it only needs to be believable long enough to trigger action. Verification must now extend beyond familiarity. Second-channel confirmation is no longer excessive. It's expected.

Athenian Tech

Contact Us

www.atheniantech.com

https://www.linkedin.com/company/athenian-tech/