ATHENIAN TECH

NEWSLETTER

May 2025

THREAT INTELLIGENCE BY ATHENA

From the Editor's Desk

Tensions between India and Pakistan reached the tipping point, in May 2025, the aftereffects of which could be seen in cyberspace, thanks largely to the hyper-connected world that we live in, in the present day. Post the killings in Pahalgam on 22 April 2025, India took a number of measures, the most prominent being, to keep the Indus Water Treaty in abeyance.

IN THIS NEWSLETTER

Issue #03

These actions by India were largely aimed at sending a strong message across the globe that it will no longer take terrorist acts lightly. The Operation Sindoor, which was launched on 07 May 2025, further reaffirmed India's stand and also sent a strong message that it will also not shy away from hitting at perpetrators of such acts, wherever they are, and that too at will.

Tensions between India and Pakistan is nothing new, they have existed ever since both the countries were born, in 1947. It also needs to be remembered that at all times when tensions between the two countries have escalated and have led to a full scale war, Pakistan has always been the aggressor. Even this time, the killing of innocent tourists, by terrorists from across the border, in Pahalgam, forced India to take the necessary measures, and ultimately launch Operation Sindoor. However, this time around the tensions between the two countries took a very different face. Unlike traditional full-blown wars that were fought between the two countries, in the past, this time around India resorted to precision bombing of terrorists and terrorist hideouts inside Pakistan and Pakistan Occupied Kashmir.

At the very outset India made it very clear that its actions were not against the Pakistanis but was directed purely against the terrorists. The second and the most striking feature of the heightened tensions between the two nations, never seen in the past was the spilling over of the real life acrimony, onto the cyberspace. Post the killing of innocent tourists in Pahalgam, India was at the receiving end of meticulously planned cyberattacks by the hacktivist groups from across the border.

These attacks did slowdown post ceasefire, on 10 May 2025, but the increased number of attacks during such a short period (from the fourth week of April till mid-May 2025) does underscore the need to maintain proper cyber hygiene so that the cyber defences can be bolstered. This is important cause, the machinery/software in place, to strengthen cyber defences, never fails, it is the man, or simply put, humans like you and me, which is the weakest link in the entire cyber defence chain.

While institutions in India were at the receiving end, of cyberattacks, as a result of the recent tensions between India and Pakistan, elsewhere across the globe affiliates of the Coca-Company were impacted by cyberattacks. In the first instance the Everest Ransomware group struck Coca-Cola Al Ahlia (Dubai), using stolen RDP credentials and in the second instance a threat actor named

Gehenna breached Coca-Cola Europacific Partners (CCEP), stealing and auctioning over 63 GB of sensitive information. Both these incidents exposed the fragility of global supply chains, reinforcing calls for enhanced credential hygiene, endpoint detection, and third-party risk management.

In another incident Coinbase, one of the world's largest cryptocurrency exchanges was breached on 11 May. This attack, facilitated by bribed offshore support agents, allowed adversaries access to transaction histories and login metadata, though the core infrastructure remained secure. A $20 million ransom demand followed. This episode highlighted the increasing threat posed by insider compromise and the growing scrutiny on digital finance platforms.

These events reflect the broader trend in the cyber threat landscape. Threat actors can now leverage automated spear-phishing kits, adaptive ransomware, and AI-generated malware, effectively lowering the skill threshold needed to execute sophisticated attacks. In defence against such sophisticated attacks, the industry has responded with AI firewalls using federated learning, capable of threat detection without compromising user data privacy. These shifts suggest a fast-approaching arms race in AI-driven cybersecurity.

Meanwhile, GITEX Europe 2025, held from 21–23 May in Berlin, Germany showcased the convergence of AI and cybersecurity. Over 40,000 attendees and 1,400 exhibitors discussed how AI might add €1.4 trillion to the EU's GDP in the next decade. Cybersecurity stood out, with European investments projected to cross €84 billion by 2027. Innovative formats like "Pitchlimpics" connected startups with investors, further fuelling momentum in the tech and security domains.

Amid these macro-level shifts, experts stressed the need for individual cyber hygiene. Simple practices—such as using strong, unique passwords, enabling multi-factor authentication, encrypting data, and backing up critical files—can prevent personal and professional data loss. Given the increasing sophistication of threats, personal vigilance is now as critical as institutional security protocols.

Taken together, these events paint a vivid picture of a world where conflict, commerce, and cyber vulnerabilities intersect with increasing intensity. For India, the lessons from Operation Sindoor and the digital skirmishes that accompanied it are clear: the battleground has moved beyond borders and into the servers, clouds, and social networks of everyday life.

National security is now inseparable from cybersecurity. As states recalibrate their strategies, the coming decade will likely be defined as much by resilience in cyberspace as by might on the ground.

We look forward to walking this road with you. We will be more than happy to incorporate your views, in this newsletter, if any that you may have. So feel free to share your questions and views on the matter at pankaj.toppo@atheniantech.com . Till we meet again, happy reading.

Pankaj Anup Toppo

Operation Sindoor: The New Digital Frontline

Operation Sindoor, which India launched, on 07 May 2025 against terrorist hideouts and camps in Pakistan and Pakistan Occupied Kashmir, to avenge the death of the 26 civilians who were gunned down by terrorist linked to **The Resistance Front (TRF),** on 22 April 2025, witnessed action on the ground between the two countries. However, thanks to the hyper-connected world that we live in, in the present day, the hostilities, on the ground, spilled over to the cyberspace as well, in which hacktivist groups launched cyberattacks against institutions in India, the scale of which was not witnessed in recent times. As per various reports in the period between 07 May and 10 May, various groups supporting Pakistan launched approximately 1.5 million attacks against the Indian state. These attacks targeted a wide array of institutions across the nation's critical sectors.

Record-Breaking Surge in Attacks

Post the killings of 26 innocent civilians, by terrorists in Pahalgam, and even during **Operation Sindoor,** the nation’s cyber landscape saw a sharp escalation in hostile activity by hacktivist groups from across the border, according to reports by the **Indian Computer Emergency Response Team (CERT-In).**[1] Those hacktivist groups unleashed a volley of attacks on institutes of prominence, in India, primarily institutions of the Central and State Government.

1. Essential Measures for Industry for Safeguarding Business Operations against Cyber Security Threats https://www.cert-in.org.in/

Latest Cyber Breaches

One among the many groups that went up in arms against the Indian Union, in cyberspace, was Team Insane PK. The group launched a number of attacks against India, the most prominent being their intrusion into the server of the High Court of Andhra Pradesh. Post this intrusion, the group compromised and leaked 2.5 GB of data from the top court of the state of Andhra Pradesh.

Adding to this frenzy, in cyberspace, other hacktivist groups, especially those targeting institutions from the critical sector adopted a different approach. Rather than breaching and stealing data, **Keymous+ Team,** stuck to launching **Distributed Denial-of-Service (DDoS)** attacks, especially against the Ministry of Defence, Government of India. The primary objective of targeting their arsenal against the Ministry of Defence, was in all likelihood to bring one of the most critical sectors of the Indian Union, to a grinding halt, thereby leaving the country defenceless.

Another group that stuck to launching **DDoS** attacks on institutions of the Indian Union was the Islamic Hacker Army. The group directed all its energies against India's critical infrastructure and even launched **DDoS** attacks on private healthcare providers like Max Healthcare and Apollo Hospitals.

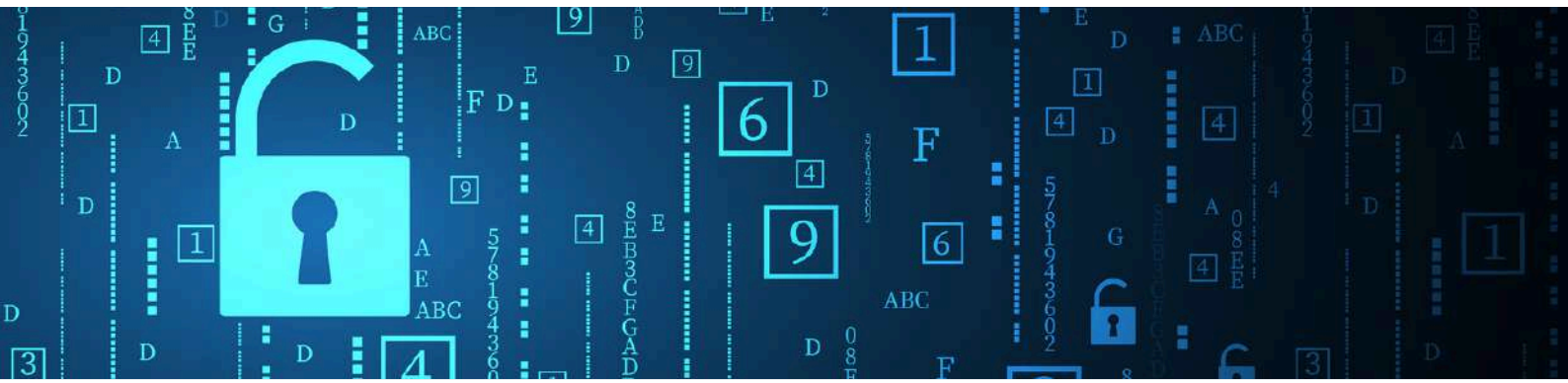
Cyber Strikes on Critical Sectors

The volley of strikes that the hacktivist groups launched at institutions, in India, were largely targeted at institutions that from the nation's critical infrastructure. Public sector institutions such as **Central Coalfields Limited (CCL)**, a subsidiary of **Coal India Ltd**., which is the world's largest government-owned coal producer, was attacked and their domain was compromised. The fact that the website had been compromised came to light when users browsing the **CCL** website (www.centralcoalfields.in) witnessed their screens light up with a message from "**Mr Habib 404 – Pakistani Cyber Force**," stating, "You thought you were safe, but we are here"—a clear and brazen taunt aimed at Indian cyber defences.

E-commerce platforms were also under attack, as the hacktivist group **Arabian Ghosts** targeted major platforms like Amazon India and Flipkart. They claimed responsibility for compromising these platforms. Their actions and messaging were part of the **#OpIndia** and **#GlobalFront** campaigns, promoting anti-India and pro-Palestinian narratives.

China's Moves Behind The Scenes

A concerning development at the time when hacktivist groups, form across the border, took the tensions between the two countries into cyberspace, was the outside help from China. Analysts have long drawn attention to China's quiet support in enhancing Pakistan's cyber capabilities, along with suspicions of them aiding threat groups like **APT36**, which are speculated to be benefit from the **China-Pakistan Economic Corridor (CPEC)**. **APT36**, emerged as one of the most sophisticated and malicious actor during the conflict, actively targeting individuals in India's defence and government sectors. They sent out phishing emails disguised as official briefings and honeytraps, and a much more advanced **CrimsonRAT** malware followed.



China's role was not limited to this, as its state media, such as **Xinhua** and **CGTN**, also played an active role in shaping global perception. They constantly echoed and amplified misinformation narratives during the conflict, like fake claims about vulnerabilities of India's defence. What was once the work of Twitter trolls and hacktivist groups was now being elevated by state-owned Chinese media, lending international visibility and false legitimacy to misinformation campaigns.

For Indian policymakers, this alignment between China and Pakistan has reignited concerns of a '**two-front**' confrontation, a threatening scenario that spans not only physical borders but also digital networks.

Disinformation Storm on Social Media

Adding another dimension to the rising hostilities both in the real world as well as in cyber space, a parallel assault was also being launched by a coalition of Pakistan-linked bot networks and hacktivists groups who sprung into action on social media.

These bot farms aimed on taking advantage of two things: AI's rapid advances in generating falsified images and deepfake videos, and the general unsuspecting public which was incapable to distinguish the real from the fake.

Bot networks on social media worked relentlessly to amplify hashtags such as **#FreeKashmir** and **#StopSindoorOps**, ensuring that these narratives trended across platforms like X (formerly Twitter), WhatsApp and Facebook. These hashtags were accompanied by false images which showed captured Indian Air Force (IAF) pilots and doctored videos of Indian leaders.

In one of the doctored videos even Nardenra Modi, Prime Minister of India was shown apologizing for having launched **Operation Sindoor.** As a result of this misinformation blitzkrieg the common man, who browsed the trending hashtags and posts following the conflict on social media, was instead bombarded by endless fabricated reports of casualties suffered by the Indian defence forces and even the common man. There was a also a footage of Indian Airforce jets being shot round in the recent round of hostilities. To counter, this misinformation blitzkrieg, the Government of India stepped to stem this tide. One of the actions, the Government, took in this regard was to send directives to

X (formerly Twitter) to block over 8,000 accounts from being shown to Indian users of the platform.

The ensuing disinformation campaign that followed post the killings in Pahalgam was not an isolated act of digital vandalism but was part of a broader, orchestrated campaign, the intent of which was beyond any iota of doubt to sow seeds of confusion, inflame public sentiment, and erode confidence, of the Indian public, in official channels of communication.

The Indian Response

In the aftermath of the Pahalgam terrorist attack and the **Operation Sindoor** that followed, India found itself at the receiving end of cyberattacks from across the border. While the objective of these attacks was to cripple the digital backbone of the country, what followed was not chaos; instead, an admirably swift response from India.

Leading the Indian response was the **Indian Computer Emergency Response Team (CERT-In)**, which issued the necessary advisories. These advisories by **CERT-In** acted as digital flares in a dark storm, guiding banks, organisations in the infrastructure sector and public institutions to reinforce their defences.

But it wasn't a lone effort. A broader alliance unfolded—one that brought together the **Defence Cyber Agency** the **National Critical Information Infrastructure Protection Centre (NCIIPC)** and top private cybersecurity firms. Working in close coordination these groups formed a kind of digital army, detecting, isolating, and neutralizing threats often within minutes of their emergence. The scale, and the utter failure, of the cyber assault came into sharp focus when **Maharashtra Cyber**, the dedicated cybersecurity and cybercrime investigation agency of the Government of Maharashtra released its analysis in a report to key law enforcement agencies, titled **"Road of Sindoor"**.

This study revealed that out of a staggering **1.5 million** attempted cyber intrusions from hacktivist groups, only **150** breaches were recorded. These numbers told a powerful story, not just of how intense the barrage had been, but how resilient India's cyber defences had become.

Behind the scenes, over **1,000** digital takedowns were carried out daily, targeting malicious websites, rogue applications, and disinformation networks that sought to distort public perception and sow seeds of confusion, among the public at large.

Now, that the dust has almost settled a clearer picture begins to emerge. Analysts see these events not just as another episode of digital conflict, but as a watershed moment. The cyberattacks did expose some vulnerabilities, but it also revealed the strength of India's growing cyber capabilities. The lessons are clear: to move forward, India must institutionalise real-time threat-sharing, invest heavily in homegrown cybersecurity tools, and most importantly, shape a cohesive national strategy that can adapt to the shifting terrain of modern digital warfare.

Twin Breaches Hit The Coca-Cola Company Affiliates

Everest Ransomware Strikes Again

On 22 May 2025, the **Coca-Cola Al Ahlia Beverages Company,** a bottler and distributor of The Coca-Cola Company, had been breached by the **Everest** Ransomware group. In the said breach, private employee records of the bottler and distributor were compromised. The leaked employee data appeared as password-protected files on the **Everest Data Leak Site (DLS)** hosted on the dark web, along with a countdown timer designed to pressurize the victims, along with an email contact for ransom negotiations.

The shadowy threat actor **Everest** Ransomware Group has been active since 2020. They are known for resorting to extortion after data breaches and have a history of ransomware attacks, data extortion, and selling unauthorised network access.

The approach of the threat actor in cracking the defences of the database of the **Coca-Cola Al Ahlia Beverages Company** was calculated and precise. According to our analysts, the Everest Ransomware Group most likely breached the security features of the database through initial access brokers, using compromised remote credentials, **Remote Desktop Protocol (RDP)** access, and other remote access tools.

Once inside, the group fell back to its old tactics, and prioritised stealing as much data as possible over everything else. At the end of their heist 959 employee records lay exposed, their personal histories and professional details were now available to the highest bidder on the dark web. Coming to the details of the heist, passport scans, some even belonging to minors of company executives were compromised. This just goes to show how an incident can turn from a professionally damaging cyber breach to a deeply horrifying violation of privacy, even of individuals. The attackers however, did not just stop at committing heinous privacy violations, they also seized internal and confidential business data.

Gehenna Breaches Coca-Cola Europacific Partners

But little did they know, the horror show for *The Coca-Cola Company's* affiliates was just starting. On 22 May 2025, the very same day as **Everest** breached through the defences of **Coca-Cola Al Ahlia Beverages** Company an independent threat actor Gehenna was also executed a breach targeting **Coca-Cola Europacific Partners (CCEP)**, the world's largest independent bottler for The Coca-Cola Company.

Gehenna has, in a short span of time, built a reputation being a sophisticated actor on the dark web, claiming responsibility for several high-profile breaches, including those that struck Samsung Germany and Royal Mail. According to our analysts, unlike many threat actors who rely on ransomware or extortion, **Gehenna** appears to specialise in orchestrating large-scale data breaches and then quietly selling the stolen information.

This was made clear because the breach at **CCEP** did not involve ransomware or extortion demands instead, it was a **targeted data exfiltration**, with the stolen information listed for sale via a dark web auction.

The stolen material was a treasure trove of data, with our analysts concluding that **Gehenna** made off with approximately **63 GB** of sensitive corporate data, including **7.5 million** Salesforce account records **(6 GB)**, **9.5 million** customer case files **(52 GB)**, **6 million** contact entries **(5 GB)**, and **400,000** product records **(300 MB)**.

Though neither **CCEP** nor the **Coca-Cola Al Ahlia Beverages Company** has officially acknowledged the breaches, these incidents have exposed a harsh reality about the digital age: data has become the weapon of choice, and the threat landscape is constantly shifting. Though ***The Coca-Cola Company*** itself remains unaffected, these attacks have surely stressed the importance of having in place strong cybersecurity governance across all regional subsidiaries of a big organisation.

The Coinbase Breach

On 11 May 2025, the digital vaults of **Coinbase,** one of the world's most trusted cryptocurrency exchanges, become the stage for a cyber drama unlike any before. In the shadows, an unknown adversary orchestrated a breach not through brute force or a single fatal flaw, but through a masterful blend of technical cunning and psychological manipulation. The attackers, who broke through the defences by preying on the **human element**. Overseas support agents, entrusted with privileged access to **Coinbase's** systems, unknowingly became accomplices after being bribed by the threat actors to get them past the security measures. With the doors to the castle now open, the intruders moved silently through Coinbase's inner sanctum, their every step calculated and unseen.

The shocking thing? No one even realized the breach until **Coinbase** received a $20 million (in bitcoin) extortion demand from the attackers in an email. The email threatened to publicly release stolen customer data, including names, addresses, phone numbers, partial Social Security numbers, masked bank account details, and images of official identification documents, unless the ransom was paid in full. Even though the data itself did not include any login credentials or access to private funds, this user information data is dangerous as it can be used to launch social engineering attacks on the victims. The attacker's aim was to put together a customer list that they could contact while masquerading as personnel from Coinbase.

The **Coinbase** CEO, Brian Armstrong, not one to be cowed down by ransom demands, hit them right back and refused to pay the ransom. He doubled down even more, offered a **$20 million** bounty right back, for information leading to the identification and prosecution of the attackers.

The Impact

The company's response was swift and admirably transparent, as unlike the other incidents, Coinbase immediately disclosed and acknowledged the breach in 72 hours. They pledged to reimburse any customer (s) targeted through social engineering attacks as a result of the leaks. Coinbase also initiated a comprehensive review of its global support operations, pledged to enforce zero-trust approach to access management.

While the immediate technical fallout seems to have been contained for now, the breach's implications ripple far beyond **Coinbase's** digital walls. It happened even though it’s a time of heightened regulatory scrutiny for crypto exchanges, amplifying worries about the sector's readiness to be regarded as a legitimate means of financial transactions.

This incident also underscored the most critical lesson for the digital asset industry: that the **human element,** whether through insider threats or social engineering, remains the most vulnerable in even the most technologically advanced systems. For the broader financial ecosystem, the **Coinbase** breach is a **red alert**, as the lines between traditional and digital finance blur, so too do the risks.

Attackers vs. Algorithms

Gone are the days when cyberattacks were the exclusive domain of lone wolves or small, specialised groups. Now more than ever, automated threats are increasingly becoming as much a danger as human cyber criminals. This fact was showcased in a report by **Fortinet** indicating that the pace of automated threats reached new heights in the month of May 2025.

Sending nervous shivers down the entire cyber world, **Fortinet** reported an unnerving **16.7 per cent** year-over-year surge in automated scanning activities—a clear indicator that algorithms are now coming to dominate the digital battlefield.

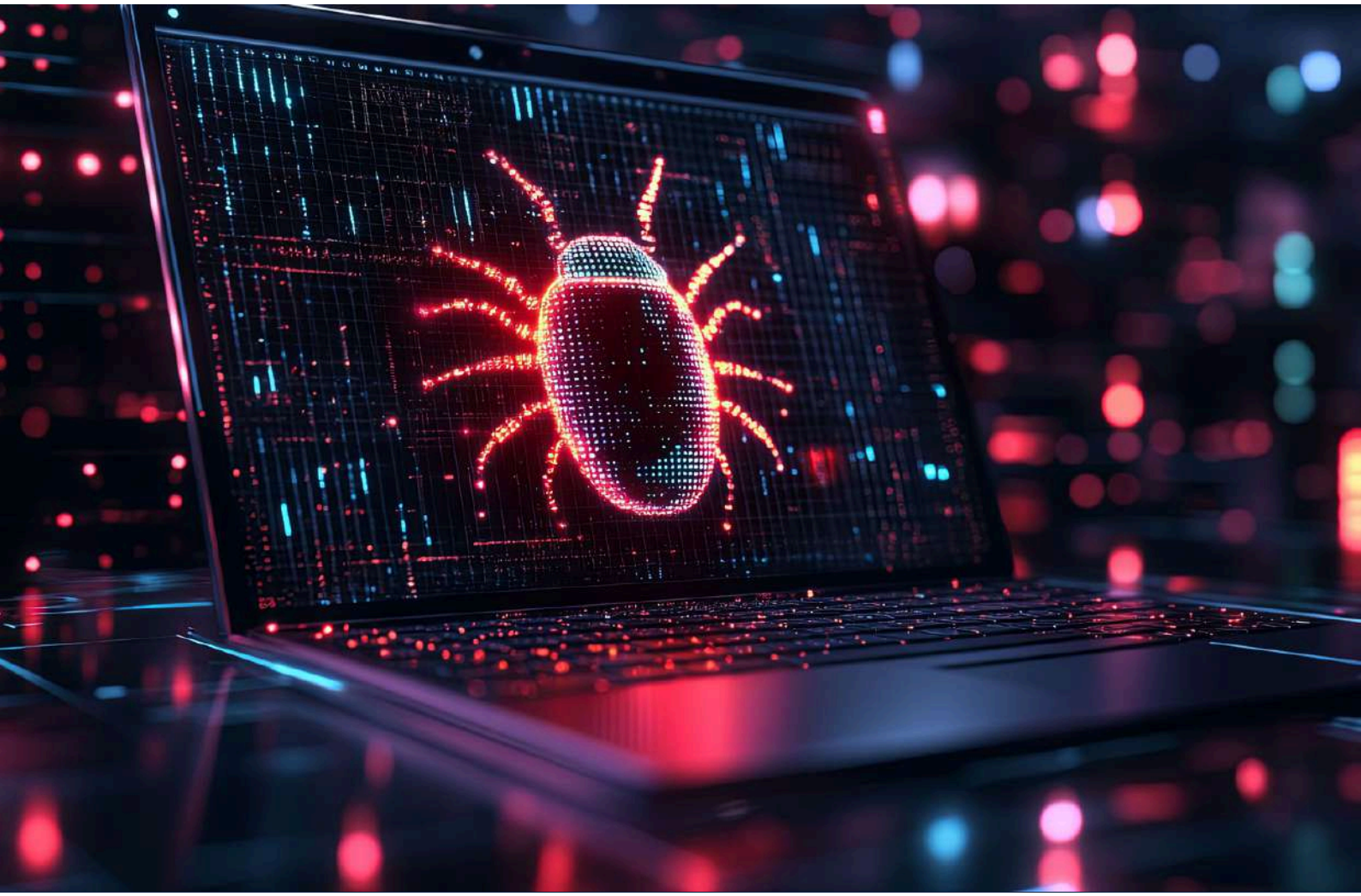
The existence of **Adaptive** Malware and Ransomware means that AI-powered malware is no longer static. It can autonomously adapt its behaviour and **mutate** on the go, to avoid getting caught by traditional antivirus and intrusion detection systems.

What is **even more troubling**, underground forums are seeing a spike in chatter about AI-generated **phishing kits** that are capable of crafting personalised spear-phishing emails in multiple languages, mimicking tone and formatting patterns with alarming accuracy.

This now means that whereas earlier you needed a certain amount of technical skill and creative acumen to craft phishing material, now any one can **craft endless amounts of personalized phishing emails**, in any language and slang they want. This is undoubtedly an inflection point, and AI will undoubtedly create many more legions of cybercriminals in the future.

On the defensive front, May 2025 saw the deployment of next-gen **AI firewalls** by several companies. These systems, built on federated learning models, can analyse attack patterns across networks in real time without compromising sensitive corporate data.

These next-level firewalls are continuously adapting, ensuring that organisations remain protected even as adversaries leverage artificial intelligence to develop increasingly sophisticated attack strategies. However, we must keep in mind that as we integrate AI into security systems, it's equally important to **secure AI itself**, ensuring it remains reliable, transparent, and trustworthy.



China's AI Supercomputer Rockets to Space

14 May 2025 may go down in history as the day computing truly left the bounds of this earth. On this day, China launched **twelve** satellites into the orbit from the **Jiuquan Satellite Launch Centre** in northwest China. Not as part of its routine space endeavour, but as the opening move in creating one of the most audacious technological feats ever attempted: a vast supercomputer network of **2,800** satellites circling the globe. China has embarked on an ambitious leap in space technology with the launch of its space-based AI supercomputer network.

Called the "**Three-Body Computing Constellation**", and flying high above earth's atmosphere, a new breed of supercomputer has come to life. Its name is inspired by the age-old mystery of the **three-body problem**, a puzzle first explored by Isaac Newton to understand the chaotic movements of three celestial bodies locked in a gravitational pull.

Orbiting silently, each of these AI-powered satellites carries an **eight-billion-parameter** model, that is capable of digesting and interpreting raw data in real time. Together, they form a vast, intelligent network with the potential to execute one **quintillion operations per second**, on par with the powerful supercomputers on Earth.

With this initial launch, China has taken a clear lead in the space-based AI computing race. However, the outcome of this new technological rivalry with the United States of America and other nations remains to be seen.

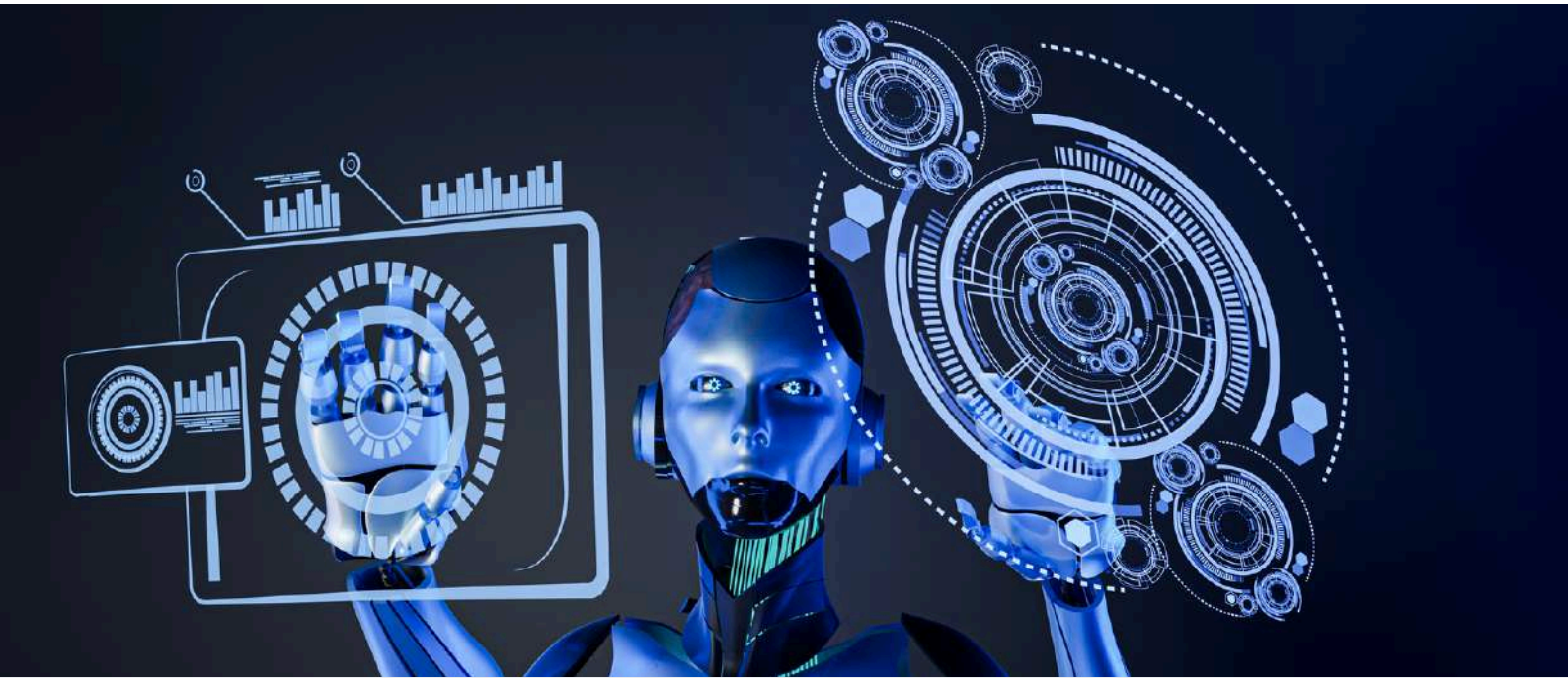
GITEX Europe: AI Takes Centre Stage

GITEX Europe 2025 was held between 21 to 23 May 2025 in **Berlin**, **Germany** transforming the city into the heart of the world's tech revolution. In its debut, the event drew an impressive crowd of over **40,000** visionaries, innovators and leaders. Under one sprawling roof, more than **1,400** exhibitors and over **750** startups from **100+** countries came together, turning the event into a buzzing crossroads of global innovation. AI naturally took centre stage, wowing crowds with demos that felt like glimpses into the future.

AI wasn't all that was dazzling crowds however, quantum computing made a bold entrance with some jaw-dropping breakthroughs, while the startup scene crackled with raw energy.

Artificial Intelligence at the Core

Without an iota of doubt, AI stole the spotlight at GITEX Europe 2025. Panelists, speakers, and exhibitors, all were in unison, and spoke in one single voice about the vast and game-changing potential that AI has. The buzz wasn't just hype, conversations circled around numbers too, like AI's projected €1.4 trillion boost to the EU's GDP over the next ten years. The biggest draw was undoubtedly AI agents, which are best understood as smart, self-driven systems making decisions and getting things done without needing a human in the loop.



Quantum Computing and Cybersecurity

IBM pulled quite the crowd with its interactive quantum showcase, at the event. Attendees got the rare chance to look inside the **IBM Quantum System Two** supercomputer, and got to check its complex inner workings and get a close feel of how quantum-powered computing actually functions.

Cybersecurity, meanwhile, stayed at the forefront and at the centre in the conversations, at the event. With Europe's cyber defence spending expected to hit **€84 billion** by 2027, GITEX Europe became a key gathering point for CISOs, CIOs, and policymakers. Serious discussions also unfolded on everything from AI-driven cyberattacks to the growing threat of state-backed hacking and the increasing headaches in the industry around cloud security. Big players like Crowdstrike and Fortinet showcased their latest tools, showing just how fast the cybersecurity world is moving to keep up with next-gen threats.

Startup and Investment Ecosystem

Meanwhile, the energy surrounding the startup ecosystem was in full swing at North Star Europe, a lively event that buzzed with fresh ideas. More than 400 investors and VCs mixed with up-and-coming founders, creating a space where big dreams met serious funding potential. The vibe was electric, especially during creative events like "Pitch in the Bus" and the "Pitchlimpics," where pitching a startup felt more like a show than a boring business pitch.

It is apparent from the incidents covered this month, cyber threats have become a daily reality thanks largely to the sophisticated threat groups targeting major corporations and opportunistic hackers exploiting personal devices. Protecting your data is not just about safeguarding information; it is about preserving your privacy, reputation, and peace of mind in a hyper-connected world.

What is your digital data? Your digital data is any of your information that's stored or processed on computers, phones, or the Internet. It includes everything from your photos and texts to big databases used by companies. Most of what we do online, shopping, transactions, streaming, chatting, relies on digital data being shared and stored. Because so much personal info is involved, practicing proper cyber hygiene is extremely important, to ensure that the data remains safe and it does not land in the wrong hands and then gives you sleepless nights.

Here we chart the path that you and your loved ones should take so that you and your near ones remain safe in this hyper-connected world, to be more precise keep their data safe in this digital world.

Set Strong, Unique Passwords

Think of your password like the key to your digital home, it might seem small, but it’s your first line of defence. Now imagine a bunch of cybercriminals roaming the Internet like digital pickpockets, trying out weak or reused passwords until something clicks. If you use the same password everywhere, one lucky guess could open up your entire online world, to strangers and possibly nefarious elements. That is why its is important to have strong password which are unique and so is difficult to guess and thus crack.

Adopt Multi-Factor Authentication (2FA, MFA)

But even the sturdiest lock can be broken open. That’s where multi-factor authentication (MFA) steps in, like a second lock at your door. With MFA, you need more than just a password, a code on your phone or an authenticator app becomes your second proof of identity. This extra step makes it exponentially tougher for intruders to get through, even if they’ve stolen your password.

Make Use of Encryption

Think of encryption as your data's invisibility cloak. Whether your files are chilling on your laptop or zipping through the Internet, encryption scrambles everything into nonsense for anyone who doesn't have the secret key. Most modern devices and cloud services offer built-in encryption, be sure to enable it.

Take Regular Backups

No fortress is complete without an escape plan. Regularly backing up your critical files, both on the cloud and on the physical hard drive, ensures that even if disaster strikes, your digital life can be restored and that too quickly. This habit protects you from hardware failures, ransomware attacks, or accidental deletions.

Know Your Privacy Settings

When you're exploring new applications or social media, it's easy to skip over privacy settings in the associated excitement. But these settings are your personal shield against oversharing. Take a few minutes to check them out, on your phone, on your social accounts and on your cloud storage. Share only what's essential, disable location tracking when possible, and be cautious about granting application's access to your contacts, camera, or microphone.

Train Yourself

Cybercriminals are basically professional storytellers, spinning believable stories through emails, fake websites, and sneaky attachments. Stay sharp by learning to identify the warning signs: unusual requests for private information, suspicious links, and messages that try to rush you into acting quickly or adding and urgency to act fast.

Regularly Update the Software

If you imagine your software as the walls of your fortress, over time, cracks will definitely appear, vulnerabilities that attackers can exploit. Regular updates are the repairs that keep your virtual walls strong. Make it a habit to update your operating system, applications, browsers, and plugins promptly and enable automatic updates where possible.

In this digital era, cybersecurity isn't just for experts, it's a daily practice for everyone. By incorporating these habits into your routine, you build resilience and confidence, enabling you to navigate the online world's twists and turns.

Athenian Tech

Contact Us

www.atheniantech.com

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