ATHENIAN TECH

NEWSLETTER

September 2025

THREAT INTELLIGENCE BY ATHENA

Issue #07

In this Newsletter

From the Editor's Desk

As we are gradually approaching the tail of this calendar year, a peculiar trend is coming to the fore that is the shifting nature of cyberattacks. From the attacks that have been listed in this journal, it is apparent that the nefarious elements in the growing and promising but equally dangerous digital domain are now shifting their focus from targeting the business sector. As you sift through the pages of this newsletter you will see that attackers have now enveloped within their attack surface, even investment banks. In this newsletter we have attempted to list down some of the major attacks that made headlines in the cyber security space. While cyber attackers have gradually shifted their focus, one trend that has been a constant in today's day and age is the scams that happen with a heady dose of technology. Such scams continue to happen with gay abandon but and their nature is also strikingly, as will be evident, as you turn the pages of this newsletter. Through this newsletter we have tried to bring important developments that have happened in the realm of cybersecurity in the month of August and September.

It will not be wrong to say that that the second half of 2025 was a marked departure of the happenings, in cyberspace, especially during the run up to Operation Sindoor, during the operation and its aftermath. That was a period which witnessed unrelenting attacks on primarily institutions from the critical sector. The months of August and September were comparatively tepid and even the attacks that happened during that period, largely happened in the private sector, even globally.

Among the major incidents that grabbed headlines during this period was the cyberattack on Jaguar Land Rover (JLR), the UK-based automotive subsidiary of India's Tata Motors. The attack, which was attributed to hacker groups Scattered Spider and *ShinyHunters* paralysed production and IT systems across the UK, Slovakia, India, and China which resulted functions like manufacturing, registration, logistics, and retail operations. Initially, the automative major denied any data theft but later confirmed the compromise of certain customer and operational data. The attack grabbed headlines and its severity can be gauged by the fact that independent estimates had placed weekly losses, as result of this attack, to the tune of £50 million. Total damages as a result of this attack will most likely be more and the aftereffects could well be felt in the months to come.

From the Editor's Desk

While attackers for most part directed their attention towards the private sector, APT36 aka Transparent Tribe maintained its unidirectional focus towards institutions of the Government of India. The threat actor group, between 22-26 August 2025 launched a phishing campaign against institutions of the Government of India. Some of the major institutions that the group targeted included names like Department of Defence Production, the Indian Air Force and the Ministry of External Affairs. Their modus operandi was to send emails which contained malicious files which covertly got in touch with attacker-controlled servers to download the malware. This phishing campaign attacked systems running on Microsoft Windows as well as BOSS Linux, India's indigenous operating system. Through this phishing attack the APT group got access to sensitive documents within the government machinery.

The other major cyberattack which made headlines in the previous two months was the incident at Salesloft–Drift, which came to light on 20 August 2025. The said attack exposed the weaknesses in the SaaS ecosystem. In this attack the attackers infiltrated Salesloft's private GitHub repositories and inserted software to gain access. Post getting access the attackers among other things got access to sensitive CRM data. The breach impacted over 700 companies and included names like Zscaler, Cloudflare, Palo Alto Networks, Google, and PagerDuty.

The other major attack to have made headlines in September was the breach at Insight Partners a global software investor partnering with high-growth technology, software, and Internet startup and ScaleUp companies. The breach led to compromise of sensitive information like fund records, tax filings, and banking documents. It is believed that that attack was largely successful because of employment of stolen credentials, by the attackers, which was acquired through social engineering. Among other things this breach shows the gradual shift of attackers who are now finding financial institutions and investment firms as attractive targets purely because of the quality and nature of information that they store.

While organisations continued to face the wrath of cyberattacks, the cyber scams continued to torment individuals. Some of the major scams to have made it big are mentioned below. Those are mentioned in greater detail at the in the pages that follow.

- In Kolkata, a businessman lost nearly ₹4 crore in a honeytrap and was duped into investing in a dubious crypto-trading scheme after being lured by a woman who he had met on Facebook.
- Investigations uncovered a fake stock-trading apps that defrauded Indian investors to the tune of ₹25 crore using cloned brokerage platforms.
- A Hyderabad based businessman lost ₹1.19 crore in an app-based investment fraud.
- Federal prosecutors charged 28 individuals in a USD 65 million global scam targeting senior citizens via India-based tech-support call centres.

At the Black Hat USA 2025, experts demonstrated how nefarious elements are weaponising AI. Sessions showcased how generative AI models create deepfake voices, craft personalised spear-phishing emails, and generate polymorphic malware that is capable of rewriting itself in the middle of the attack, which helps it to evade detection. At the summit, researchers also brough to light zero-day vulnerabilities in VPN gateways and enterprise collaboration tools, underscoring the shrinking window between vulnerability discovery and exploitation.

As technology permeates into every possible space of our lively, it is not surprising that we are slowly but gradually being surrounded by the smart devices. These devices in turn make our lives smart. To ensure that these devices bring the necessary advantages for which they were designed need to be safe and most importantly the umbrella under which they will be housed—your house—which by the virtue of housing such appliances becomes a smart home, needs to be protected. In this issue we list down the tips that you can follow to secure your smart home.

We hope you like this issue as much as liked putting it together. We look forward to your suggestions as they help us strive to excel in our endeavour. If you have any suggestions on how we can improve this honest effort of ours please do write in to us at pankaj.toppo@atheniantech.com . Till we meet again, next month. Happy reading.

Pankaj Anup Toppo

Cyberattack Hits Jaguar Land Rover

On 02 September 2025, Jaguar Land Rover (JLR), the UK-based automotive arm of Tata Motors, suffered a major ransomware attack that severely disrupted its global production and IT infrastructure. The cyberattack, reportedly orchestrated by hacker groups *Scattered Spider and ShinyHunters*, affected core manufacturing, registration, logistics, and retail systems of the automative major. Although JLR stated there was “no evidence” of customer personal data being stolen, the company later acknowledged that “some data” had indeed been comprised in the attack.

As a result, JLR was forced to shut down multiple production lines in its key facilities across the United Kingdom, Slovakia, India, and China. The incident affected both domestic operations and international logistics, resulting in stalled deliveries, suspended registrations, and strained customer service infrastructure. Independent estimates suggest that as a result of this attack, JLR incurred weekly losses amounting to at least £50 million, with the total cost likely to run into hundreds of millions of pounds, as disruptions extended well into late September, with further delays anticipated in October.

Founded in 1868, the Tata Group is one of India’s oldest and most respected business conglomerates. The group has interests in areas spanning steel, automotive, IT services, energy, telecommunications, and consumer goods. The legacy of the group, especially business legacy, is such that it represents a benchmark for industrial capability and corporate integrity. Tata Motors, which acquired JLR in 2008, had successfully transformed the British auto major into a premium brand globally, with a strong market presence in Europe, the US, and China.

Latest Cyber Breaches

The latest breach in September 2025 is the second major cyberattack on am entity of the Tata Group this year. In March this year, Tata Technologies, the IT major from the group, suffered a ransomware attack involving *Hunters International*, which resulted in the leak of over 1.4 terabytes of sensitive data, including engineering blueprints and personal information of its employees.

The JLR attack directly affected India's industrial and employment ecosystem. Several Indian plants temporarily laid off workers. Smaller suppliers reported suspended orders, endangering cash flows and supply chain stability. Although the breach occurred in Europe, its aftershocks echoed across India's automotive sector, showing how digital infrastructure vulnerabilities in one region can destabilise economic activity in a different corner of the globe.

What It Means for India?

This incident is more than a corporate setback; it's a cautionary tale. If the Tata Group, with its formidable resources and technical expertise, can suffer back-to-back ransomware attacks, the cyber readiness especially of smaller Indian firms comes under the radar.

Experts argue that the concept of industrial strength in the 21st century must now include cyber resilience. As manufacturing becomes increasingly digitised, attackers can paralyse entire value chains not by sabotaging machinery, but by compromising the software that runs them. This incident, involving a flagship global brand, signals a new era where reputation, revenue, and national economic interests are all vulnerable to digital sabotage. The cyberattack on JLR is not just a disruption; it is a strategic wake-up call. It underscores the urgent need for robust cybersecurity frameworks, particularly for firms operating globally or those that are part of the critical supply chains.

Government of India Under Attack from Transparent Tribe

Between 22 and 26 August 2025, various institutions of the Government of India like Department of Defence Production, Indian Air Force, and the Ministry of External Affairs, received ZIP attachments which looked like routine meeting documents, on their official mailboxes. These attachments, which seemed harmless at first glance, concealed a well-planned malware campaign. Inside the ZIP files were .desktop shortcut files, deceptively named and designed to resemble PDFs. When clicked, the files launched a legitimate-looking decoy document while simultaneously contacting attacker-controlled infrastructure to download malicious payloads. Some of these payloads were hosted on widely trusted platforms such as Google Drive, enabling the malware to bypass common security filters and network defences.

The campaign was attributed to *Transparent Tribe (APT36)*, an APT group linked to Pakistan with a known history of targeting institutions of the Government of India and critical infrastructure assets. While the group has been active for years, what made this attack particularly significant was its cross-platform reach, a first for this adversary. The malicious files were tailored not only for Microsoft Windows but also for India's indigenous BOSS Linux, which is widely used across government offices. This marked the first known instance of Transparent Tribe adapting its malware toolkit to target BOSS Linux, signalling an evolution in its technical capabilities and intent.

The attack chain relied heavily on social engineering tactics designed to exploit daily work habits. Victims were sent emails that mirrored legitimate meeting requests. The fake documents, once opened, communicated with attacker infrastructure via temporary WebSocket servers like seemysitelive[.]store, used to fetch and execute secondary payloads. These temporary servers were deliberately chosen to reduce traceability and ensure operational agility. Once the payload was downloaded, persistent implants were deployed on the victim's system, granting the attackers long-term access to sensitive government emails, files, and internal communications.

By the end of August, multiple cybersecurity vendors had begun tracking the campaign. Although the exact number of compromised systems has not been publicly disclosed, internal threat assessments suggest that dozens of machines were likely breached before any detection or response could be initiated. Systems tied to government departments and defence infrastructure were reportedly among those affected. The risk extended beyond immediate data theft, raising concerns about long-term espionage, credential theft, and lateral movement across secured networks.

Experts believe that this incident marks a strategic escalation by Transparent Tribe. Not only did they demonstrate the ability to build platform-specific malware, but they also adapted their tactics to bypass widely deployed security mechanisms by utilising legitimate cloud services, such as Google Drive. The decision to target both Windows and BOSS Linux suggests a growing emphasis on persistent, targeted intrusions that can adapt to the unique technology landscape of entities of the Government of India.

In conclusion, the August 2025 campaign by Transparent Tribe represents more than just another phishing attack. It reflects the growing sophistication and determination of adversarial groups like APT36 to undermine national security through digital espionage. As attackers evolve, so too must India's cyber defences—across all platforms, operating systems, and user behaviours.

Salesloft–Drift Supply-Chain Attacks Hits the SaaS World

On 20 August 2025, Salesforce and Salesloft jointly confirmed a supply chain cyberattack linked to the Salesloft–Drift chatbot connector. The campaign had begun months earlier, in March 2025, when attackers breached Salesloft's private GitHub repositories. They inserted malicious GitHub Actions in workflows, giving themselves a persistent foothold. By July 2025, the attackers had infiltrated Drift's AWS infrastructure, where they escalated their privileges and began forging fraudulent OAuth tokens which is an authentication key used by SaaS applications to access user data without requiring passwords.

These forged tokens allowed adversaries to interact with Salesforce APIs undetected, using legitimate-seeming requests to siphon off large volumes of data. Between 14-20 August, defenders noticed anomalously high Salesforce API traffic originating from Drift. Sensitive data objects—such as Users, Cases, and support histories—were being downloaded in bulk. Salesforce responded on 20 August by revoking all OAuth tokens associated with Drift and removing the connector from its AppExchange. By then, however, data exfiltration was already complete.

Global Impact

By early September, the scale of the breach had become fully apparent. Over 700 companies had been compromised, including Zscaler, Palo Alto Networks, Cloudflare, PagerDuty, SpyCloud, and Google. Analysts confirmed that attackers had accessed not only CRM data but also high-value embedded credentials, including AWS keys, Snowflake tokens, and access keys potentially tied to production environments. These credentials could be exploited for future intrusions, data manipulation, or infrastructure compromise.

The OAuth tokens, in particular, gave attackers persistent, trusted access across cloud services, bypassing passwords, MFA, and anomaly-based detections. Investigations suggest that the attackers enjoyed months of undetected access, quietly refining their methods and expanding their reach.

Lessons for the SaaS-Driven World

With tens of millions of records compromised and financial damages expected to exceed hundreds of millions of dollars, this breach represents one of the most significant SaaS supply chain incidents to date. But the real lesson lies beyond numbers. The attack illustrates a critical vulnerability in today's software ecosystems: trust is often delegated to APIs and third-party connectors, making the security of one vendor a potential weak point for hundreds of others.

As SaaS adoption deepens, security hygiene must evolve beyond internal endpoints. It must include build pipelines, token policies, and third-party connectors. This breach proves that one poisoned workflow is enough to take down hundreds of companies, often before a single alarm is triggered.

The GE Edge and Mesa 500 GB Data Leak

On 15 September 2025, the cybersecurity world was jolted by the release of the GFW Report, which revealed what experts are calling the most extensive leak ever linked to China's digital censorship management. More than 500 gigabytes of sensitive data, including source code, configuration files, internal documentation, and developer notes from Chinese contractors GE Edge and Mesa, were posted online. These two firms are believed to be deeply embedded in the architecture of the Great Firewall of China, that are responsible for the surveillance and filtering of internet traffic on a national scale. Unlike typical ransomware leaks that aim for financial extortion, this disclosure appeared intentional, offering a rare and detailed look into how censorship and surveillance are deployed at scale.

The leaked archive contained far more than just programming code. Cybersecurity analysts found detailed operational playbooks, SSL/TLS fingerprinting algorithms for tracking encrypted connections, and deep packet inspection modules capable of intercepting and analysing online activity in real time. It also included internal communications showing that engineers were actively patching flaws, responding to incidents, and updating filtering mechanisms. These files laid bare the technical sophistication of the Great Firewall, while also exposing its vulnerabilities.

Beyond Borders: Global Reach of Censorship Tools

While the primary focus of the Great Firewall is to maintain control over China's domestic internet space, the leak revealed that the technologies built by GE Edge and Mesa have found their way into telecommunication systems beyond China. Investigators traced elements of the leaked infrastructure being marketed and implemented in countries across Asia and Africa, often under the pretext of "network management" or "lawful interception" solutions. These deployments, however, carry the same core censorship functionalities, raising concerns that China's surveillance model is being exported and replicated under more subtle branding.

252 Million Identity Records Leaked

On 5 September 2025, cybersecurity researchers disclosed a massive exposure of 252 million identity records caused not by hackers or zero-day exploits but by simple misconfigured cloud servers. This was a breach born out of negligence rather than intrusion. No malware was deployed, no perimeter was breached, and the data was simply left unprotected. It was basically accessible to anyone who stumbled upon the correct endpoint. The revelation highlighted how basic lapses in configuration can eclipse even the most sophisticated cyberattacks in scale and impact.

The Breadth of the Exposure

The leaked datasets spanned at least seven countries— Turkey, Egypt, Saudi Arabia, the United Arab Emirates, Mexico, South Africa and Canada. The compromised information included fields like full names, phone numbers, residential addresses, and, critically, government-issued identity numbers. For millions of citizens, this wasn't just a privacy violation but a ready-made toolkit for fraud. Criminals could exploit this data and use it for identity theft, get fraudulent loans, launch SIM-swap attacks, and large-scale phishing campaigns. Entire populations, rather than isolated victims, are now suddenly vulnerable to systemic exploitation, as a result of this breach.

Why the Numbers Matter?

At 252 million records, the dataset dwarfs many of the world's most notorious breaches. Analysts warned that the frauds enabled by such a cache could lead to billions of dollars in global losses, as identity data forms the backbone of banking, insurance, and verification systems. The incident underscores a harsh reality of the cloud era: one overlooked configuration error can compromise the security of millions instantly. With cloud platforms designed for global scalability, a single misstep is magnified across borders and populations.

The Global Aftermath

Governments in all seven affected countries scrambled to respond. Regulators demanded accountability from hosting providers and cloud service operators, pressing for explanations of how such a basic safeguard had failed. Yet by the time servers were secured, researchers reported that large portions of the dataset had already been copied and distributed across dark web forums. Once public, containment was impossible. The episode revealed a dangerous blind spot in global cybersecurity priorities. While governments often focus their regulations on malware, hostile actors, and cyberattacks, negligence, human error, and poor configuration practices can be equally catastrophic. Without rigorous monitoring, auditing, and enforced compliance, misconfigured cloud systems will continue to offer adversaries open doors, requiring no lockpicks.

Breach at Insight Partners

On 12 January 2025, cybersecurity investigators announced that Insight Partners, one of the world's most prominent venture capital firms, had been targeted in a cyberattack. At that time, the breach drew limited media coverage, largely eclipsed by larger incidents in the telecom and technology sectors. However, the incident resurfaced with renewed urgency on 02 September 2025, when Insight Partners formally confirmed that attackers had accessed and exfiltrated confidential fund records, tax filings, and banking documents. Notification letters were sent to employees, former staff, and limited partners, confirming the scope of the damage. The breach served as a reminder that in today's evolving threat landscape, even investment firms are not immune from cyber attacks.

The Breach Unfolds

The attack did not rely on sophisticated malware or zero-day exploits. Instead, forensic investigators traced it back to a targeted social engineering campaign. Multiple insiders had unknowingly surrendered login credentials, granting attackers silent access to systems containing highly sensitive operational and financial data. Over time, adversaries exfiltrated thousands of such files, including wire transfer instructions, partnership agreements, banking statements, and tax documentation. The operation appeared to be designed for stealth: no ransomware was deployed, no demands were made. The intent was to remain undetected until all valuable data had been harvested and, potentially, brokered on the dark web or to competitors.

The Ripple Effect on Startups

With over USD 80 billion in assets, Insight Partners is connected to hundreds of startups across various sectors, including SaaS, fintech, cybersecurity, and emerging technologies. The breach doesn't just affect Insight; it potentially exposes sensitive information from many of these companies. Leaked files may include fundraising decks, valuation data, investor communications, and strategic plans.

Security analysts warn that attackers could use this information in business email compromise (BEC) scams, posing as investors or executives to trick startups into sending money or signing fake documents. This puts founders, CFOs, and legal teams at risk. In the venture capital world, where trust and reputation are everything, this kind of exposure can do serious, lasting damage.

The breach reveals a growing trend—that of attackers targeting VC firms, not just the startups they invest in. With more deals happening online and sensitive data being stored in the cloud, venture firms have become high-value targets in the threat landscape.

To put it simply cyber scams are nothing but a result of insidious use of technology by rogue elements in the society to satiate their evil desires. In short a cyber scam is a form of gratification, especially for those with evil intentions but in this entire process of self gratification a common or an innocent individual gets conned and suffers monetary losses. News of the common individuals falling for the evil designs of nefarious elements makes it to the new section publications with amazing regularity, in today's times. This trend on one hand does mean that the men and women hatching these evil designs are getting smarter by the day, sadly through ingenious use of technology. At the other end of the spectrum the growing severity and intensity of scams, also exposes the underbelly of the digital world, a world which co-exists with the highly technically sound and intelligent people but is truly unaware of how to spot the dangers which dark side of technology exposes them to.

This section is an attempt to spread awareness especially among such individuals so that they are in know of the ingenious methods employed by the nefarious elements to con them. Below mentioned are some of the notable scams that made its way to the publications.

Kolkata Businessman Scammed in Honeytrap

In July 2025, a 44-year-old businessman from Salt Lake, Kolkata, struck a friendship with a woman he met on Facebook. The friendship soon turned into a lure. The woman persuaded the businessman to invest through a so-called crypto-trading platform, which promised quick profits. Totally floored by his new friend the businessman, acting on her advice, between 17 July and early September, made multiple transfers through RTGS amounting to nearly ₹3.8–4 crore to the platform.

The businessman who was totally in a vice like grip of the woman totally believed in whatever she asked him to do. Even the dashboard showcasing his investments appeared convincing; it displayed a wallet balance of more than USD 2 million (around ₹178 crore), suggesting his investments had multiplied many times over.

The fact that the business was conned only came to light when he attempted to withdraw his investment on 8 September 2025. The platform demanded a 15 per cent “upfront tax” before releasing any money. When he refused, his account was blocked. Realising he had been conned the businessman reported the matter through the National Cyber Crime Reporting Portal and filed a case with the Bidhannagar Cyber Crime Police Station.

Scamsters Dupe Investors of ₹25 Cr

In September 2025, an investigation by a leading business daily *Business Standard* uncovered a series of coordinated scams in which investors lost nearly ₹25 crore to fake trading apps and fraudulent stock market schemes. The victims were lured through large WhatsApp groups, where scammers posed as financial mentors offering trading tips, fake research reports, and links to mobile apps or web dashboards that mimicked legitimate broker platforms.

Once inside these dashboards, users saw their “investments” grow quickly, money doubling or even tripling within days. The rapid returns encouraged them to deposit larger amounts. However, when they attempted to withdraw their own funds, they were asked to pay 10–15 per cent of their portfolio value as “tax” or “compliance fees.” Those who refused were locked out, and those who complied found their withdrawals still blocked.

ED Flags Growing Threat of App-Based Investment Scams

The Enforcement Directorate (ED) has flagged this as a rising threat, noting that single-victim, multi-crore losses are becoming increasingly common. Investigators found that many of the apps used in these scams were clones of real trading platforms, hosted on foreign servers, and promoted through targeted online ads and peer endorsements in WhatsApp groups.

Victims included professionals, entrepreneurs, and retirees, many from upper-middle-class, who were misled by the appearance of legitimacy and the peer pressure of group participation. Authorities warn that such scams are growing in sophistication, combining social engineering with technology to exploit investor trust. An investigation is ongoing to trace the origins of these apps and the criminal infrastructure supporting them.

Hyderabad Trader Loses ₹1.19 Cr in App Scam

On 4 September 2025, a 44-year-old businessman from Shamshergunj, Hyderabad, fell victim to a fake stock-trading scam after being added to a WhatsApp group that claimed to offer exclusive investment tips. Members of the group, impersonating as representatives of a reputed brokerage firm, convinced him to download a professional-looking trading app. Over the next several weeks, he made 15 bank transfers, totalling ₹1.19 crore, believing that his portfolio was growing steadily.

The app displayed a fake portfolio value of ₹4.93 crore, showing massive returns that encouraged continued investment, form the businessman. But the fraud followed a now-familiar pattern. When the businessman attempted to withdraw his funds, the platform demanded an “upfront tax” of 15 per cent on the displayed balance. When he refused to pay, his account was blocked completely, cutting off his access to both the app and his supposed investments.

Police Launch Investigation

The victim reported this fraud to the Hyderabad Cybercrime Police, who registered a case under the Information Technology (IT) Act, 2000 and the Bharatiya Nyaya Sanhita (BNS), India's updated criminal law framework. Investigators traced the stolen funds to at least eight different bank accounts, suspected to be part of a broader fraud network.

Authorities have urged the public to report such scams immediately. Officials emphasise that early reporting can sometimes allow authorities to block the stolen funds before they are moved offshore, providing victims with a small but vital window for recovery.

YouTubers Expose $65M Scam Involving Senior Citizens

On 18 September 2025, U.S. federal prosecutors unsealed charges against 28 individuals linked to a transnational organised crime network that defrauded elderly victims worldwide of nearly USD 65 million (approximately ₹540 crore). The operation, led by Chinese nationals, heavily relied on India-based scam call centres pretending to be tech support or refund departments. The primary targets, in this scam, were senior citizens, who were fooled into wiring large sums of money under the guise of fixing computer problems or receiving refunds.

The scam network operated between 2019 and 2024, with their activity traced across New York, California, Florida, and Texas. Funds were funnelled through layers of money mules, who received payments and helped launder the proceeds. In one case, a mule was linked to at least USD 1.8 million in funds obtained through fraud. During raids conducted across multiple states, federal agents seized luxury vehicles, electronics, and cash, and froze bank accounts linked to the syndicate. So far, USD 4.2 million has been recovered for the victims.

YouTubers Turn Whistleblowers

What makes this case unique is the unusual involvement of two American YouTubers, Pierogi from Scammer Payback and the team at Trilogy Media. Both have spent years infiltrating scam call centres, recording conversations, exposing mule networks, and tracking fraudulent fund transfers. Their sting operations provided crucial evidence to U.S. authorities, which helped establish the foundation of the current case.

This case illustrates how public-private collaboration, including independent digital investigations, can play a vital role in disrupting global cybercrime networks. With India-based operations once again at the centre of a large scam, the incident also raises concerns over cross-border accountability and the use of call centre infrastructure in widespread financial fraud.

Black Hat USA 2025

Held from 3–7 August 2025 in Las Vegas, Black Hat USA 2025 once again proved why it remains the world's most influential cybersecurity conference. Unlike DEF CON, known for hacker showmanship, Black Hat brings together corporate defenders, security researchers, and policymakers for some serious dialogue on emerging cyber threats. The 2025 edition delivered a strong message: the threat landscape is evolving fast, and defenders are struggling to keep up.

Artificial Intelligence (AI) dominated this year's presentations, not only as a defensive tool but also as an increasingly powerful asset in the attacker's arsenal. Researchers demonstrated how generative AI models can be weaponised to launch tailored spear-phishing attacks, create deepfake voices, and generate polymorphic malware, code that can rewrite itself mid-attack to evade detection.

One of the most discussed sessions included a live demo of AI-generated audio convincingly bypassing voice-based enterprise authentication systems. The rise of AI-enabled social engineering is no longer theoretical; it is an operational reality.

Emerging Technology Trends

As always, the “Zero-Day Arsenal” was a major highlight. Experts disclosed new, unpatched vulnerabilities affecting widely used systems, including VPN gateways and enterprise collaboration platforms. The trend points to a growing emphasis on silent infiltration rather than loud, disruptive attacks. The time between vulnerability discovery and exploitation is shrinking, leaving defenders with little margin to respond.

Another central theme was supply chain compromise, particularly via SaaS integrations and third-party APIs. Presentations demonstrated how attackers are now utilising these indirect routes to gain access to enterprise networks, often bypassing traditional security layers. A detailed case study mirrored earlier breaches involving Google and Cisco, underscoring how CRM platforms and cloud services are becoming the new frontline.

As one keynote speaker noted, “*Cybersecurity in 2025 is no longer about locking your own doors, it’s about knowing every window your neighbour leaves open.*” The event made it clear that protecting modern enterprises requires a blend of AI-driven analytics, human expertise, and vigilant oversight of third-party vendors. The future of cyber defence will depend as much on external awareness as internal controls.

Neuromorphic Computing: The Next Leap in AI Efficiency

Neuromorphic computing, once a topic only discussed by scientists, is now starting to appear in real-world tests. These are new computer chips that are designed to function more like the human brain. Instead of running nonstop like normal processors, they only fire up when something changes, just like how our brain reacts to any new information. This makes them much faster and more energy-efficient, especially for tasks such as recognising images, making decisions, or analysing data in real-time.

Earlier this year, a European research team tested neuromorphic chips in autonomous drones. The drones were able to process video footage and make flight decisions in real-time, all without connecting to any external server. That kind of speed and independence is game-changing for military and emergency applications, where delays can be costly. Similar chips are also being tested in wearable medical devices to monitor patients continuously without draining battery life.

As companies and governments begin to incorporate neuromorphic chips into robots, self-driving cars, and healthcare tools, the pressure is on to ensure that they're built safely from the outset. These chips have amazing potential, but without strong rules and good design, they could become tools for the wrong side.

Neuromorphic computing isn't just a concept anymore; it's real and coming fast. And as machines begin to "think" more like humans, cybersecurity teams will need to act just as smart to keep up.

DIY Guide to Securing Your Smart Home Devices

Technology has permeated into every nook and cranny of our lives, so it was but natural that technology started playing a key role into the biggest investment that an individual makes in his or his life. Not so long ago, say 20 years back anyone living in the hot sweltering months of May-June in Delhi, after a hard day's work would have to first reach home and then switch on the air conditioning and wait to the room to cool down before carrying on with his/her daily chores. Cut to 2025, now you can switch on the air conditioner of your house as your leave your office. This way your room/house will be at an ambient temperature as your reach home. To put it simply what makes a normal home smart, is the availability of smart devices. This includes home appliances that you use on a daily basis like your washing machine, refrigerator and even the lock to safeguard your house. Considering that the homes are increasingly becoming smart and the availability of smart home appliances are only adding to the trend, it is imperative that you keep this most expensive and important investment of your life safe from the prying eyes of nefarious elements. While the mode of entering into a smart home would be a bit different compared to entering into a traditional home, the impact of pilferage in smart home can also be far more detrimental than in a traditional home. Remember, if miscreants have access to your sensitive information, it is way too easy for them to make inroads into your smart home and walk away with goods and information about you, the effects of which will be far more detrimental that physical pilferage of your goods, a common feature in traditional heists. Remember the entry into a smart home is technically easier than in a traditional home, cause a smart lock can be easily opened by miscreants if they have the necessary information, which is the key. Thus it is in your interest to protect the home which you so laboriously built with love and lifelong hardwork to truly call it your own.

Secure Your Your Wi-Fi

The Wi-Fi network, at your home, is essentially the “front door” of your smart home. To put it simply the entry point to your smart home. Every smart device, in the home, from a baby monitor to a doorbell camera, can be operated through it remotely. The smart devices, at homes, ride on the back of the connectivity provided by the Wi-Fi. Thus to ensure that the no one hacks into those devices, it is imperative to secure your Wi-Fi. To secure the Wi-Fi, for starters, you should use a strong and unique password and enable modern encryption standards such as WPA3, or at least WPA2. It is equally important to change the default SSID (the Wi-Fi network's name), as default identifiers make it easier for hackers to guess device models and launch targeted attacks. Equally important, is to update the router firmware regularly so that any security vulnerabilities are patched on time.

Change Default Device Credentials

It has been observed that majority breaches of smart devices do not happen because of advanced hacking skills, but because of simplest of issues like sticking to the default/factory settings like usernames and passwords. Cybercriminals often compile large databases of common login details for popular devices, and once they identify your model, they can easily access your device, especially if your have not changed the factory/default settings. Thus it is important that post unpacking, the new smart gadget that you a new gadget should be to replace the default username and password with a strong, unique combination. Under no circumstances should the same password be reused on different devices.

Keep Firmware Updated

Smart devices, like laptops and smartphones, receive regular software updates to fix discovered vulnerabilities. Sadly, many users either disable updates or forget to check for them, leaving their devices vulnerable. Where possible, automatic updates should be enabled. If not available, establishing a regular schedule, such as once a month, to manually check and update each device is a prudent practice.

Put Your Smart Devices on Their Own Wi-Fi

Think of your smart devices (like your smart TV, doorbell, or light bulbs) as different rooms in your house, and imagine an attacker as an uninvited guest at a party. Just because they slip into one room doesn't mean they should get access to other rooms in your house. This is exactly the reason why it's smart to keep your smart devices on a separate Wi-Fi network.

Most routers allow you to set up a "guest" network. If you connect only your smart devices to this guest network, you create a safety barrier between them and your laptop, phone, or work computer. So even if one device is hacked, the hacker can't easily sneak into the rest of your digital life.

Don't Give Devices More Access Than They Need

Now, some smart devices behave like nosy neighbours. A smart bulb, for instance, doesn't really need to know your location or listen through your microphone, yet some apps still request for those permissions.

Before saying "yes" to everything, take a minute to check what each device or app is asking for. Turn off any access that doesn't make sense. The less personal information your gadgets hold, the harder it is for anyone to misuse it later.
Remember that some apps might not function perfectly if you refuse certain permissions. For instance, a voice-controlled device could have difficulty if microphone access is turned off. Therefore, it's about finding the right balance: only grant the device what it genuinely needs to carry out tasks which it is meant to, and nothing more.

Monitor and Audit Regularly

Securing your smart home is an ongoing effort, not a one-time task. Routers often log connected devices, so check these logs regularly. If you find an unfamiliar device on your network, treat it as a warning sign and investigate promptly. Disconnect it if needed and change your passwords to keep control in your hands.

In conclusion, smart homes should make life easier, not increase vulnerability. By following these simple yet effective measures, you build a digital defence around your household. Technology is designed to serve you, not to put you at risk, and with regular attention to security practices, the convenience of smart living can coexist with peace of mind.

Athenian Tech

Contact Us

www.atheniantech.com

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