ATHENIAN TECH

NEWSLETTER

July 2025

THREAT INTELLIGENCE BY ATHENA

Issue #05

Table of Contents

In this Newsletter

From the Editor's Desk

Deepfakes have come to haunt us again. With deepfakes it has generally been seen that they misuse the video of a famous personality to drive in their message with the intention to con the common man. In this case the scammers, to lend legitimacy to their evil designs bit more than they could chew and misused the videos of Mr Narendara Modi, Prime Minister of India and that of Ms Nirmala Sitharaman, Union Finance Minister of India. Both the deepfakes of these political heavy weights was used to market an investment scheme which looked too good to be true. The investment scheme, as was apparent in the spiel, in both the deepfakes, spoke of a onetime investment that guaranteed returns, which were astronomical and that too with a government guarantee. It all looked too good to be true but in both the cases there were glaring gaps which raised a doubt of suspicion that such an investment scheme, in times of low interest rates, could not to be true. In case of the more gullible ones, who bit the bullet, they were taken to a page, in which they were expected to furnish their details, post which the scammer masquerading as a financial consultant would make one more attempt to cajole them to fall for what he was selling. To lend legitimacy the scammers not only misused the videos of political bigwigs no less than the Prime Minister and the Union Finance Minister of the country, but they sold the investment dream through misuse of videos of senior journalists. Given the manner in which deepfakes are used to con common people, going forward, it will be in our interest to believe in something or buy into something only after one is 200 per cent sure on the matter. After all coming to the deepfakes that came to light recently, there can't be more legitimacy that is being sold by no less than the faces of the Prime Minister and the Union Finance Minister of the country, and their message is conveyed on the back of deepfakes of senior journalists. This is ammunition enough for even naysayers to bite the bullet. So, going forward, stay aware and always believe in anything with a pinch of salt.

In the world of data breaches Quantas, Australia's flagship airline was breached. The breach, which came to light on 30 June, exposed personal data of 5.7 million of its customers which included details like names, addresses, phone numbers and their date of birth. The breach, which is one of the largest, in Australia, since Optus and Medibank in 2022 highlights the risks of outsourcing to third-party vendors without stringent security protocols. The other incident, in July 2025, which exposed how dangerous vulnerabilities at end of third parties could put a company at risk, was the breach of Louis Vuitton.

The luxury brand, on 4 July 2025, confirmed of a breach which happened in South Korea. The said breach happened through compromised third-party systems. In the breach details like customer names and their contact details were leaked. It needs to be mentioned no financial data was exposed in the breach.

Staying in the domain of data leaks another sensitive breach came to light which exposed details of approximately 19,000 Afghan nationals and 100 British intelligence and Special Forces personnel. This disclosure was traced to a mail, which was mistakenly sent by an employee of the UK's Ministry of Defence, which contained a spreadsheet containing relocation applicants' details under the Afghan Relocations and Assistance Policy (ARAP).

This disclosure endangered Afghan allies, who feared Taliban reprisals, and compromised British operatives. This case underscores how even minor errors can escalate into national security crises, stressing on the importance of rigorous data-handling protocols.

Sticking to the domain of data breaches in July 2025, Rezayat Group, a business conglomerate from Saudi Arabia, was hit by a ransomware attack that was linked to the Everest group. Attackers claimed theft of 10GB of corporate data, including client contracts. Though the authenticity of the dataset remains unclear, reputational fallout could jeopardize existing and future partnerships. Everest, tied to Russian-linked networks, has a history of targeting multinationals like Coca-Cola, Mediclinic, and AT&T.

It is now becoming more than apparent that AI will play a greater role than ever, going forward, which will not only change but even alter the manner in which businesses and governments function. The Global Summit on AI, Emerging Tech Law, and Governance (GSAIET2025), held on 24 July 2025, in New Delhi, brought together policymakers, technologists, and legal experts to address regulatory gaps. At the conference Dr Pavan Duggal, noted cyber lawyer emphasized on the fragmented nature of global AI governance, while Dr Rajiv Mani, Additional Secretary, Ministry of Law & Justice, Government of India and Alfredo M. Ronchi, General Secretary of the European Commission's MEDICI Framework, among others called for stronger oversight. Kanishk Gaur who was part of a panel—AI Accountability & Liability—at the conference warned of AI's unchecked expansion, comparing it to a "tsunami."

He highlighted the absence of accountability in data collection and warned against uploading sensitive IDs (such as Aadhaar or voter cards) to AI platforms. His call to action urged faster development of ethical and legal safeguards.

Staying within the domain of AI, a new class of AI, Agentic AI, is emerging beyond generative models. Unlike prompt-driven systems, Agentic AI demonstrates autonomous, goal-oriented decision-making by gathering real-time data, analyzing context, and executing tasks through APIs.

In our effort to make this world cyber safe, this is our fifth attempt at reaching out to you. Do let us know about what you feel about our attempts at reaching out to you. We will be more than happy to incorporate your views. 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

Deepfakes Make Headlines Once Again

Deepfakes, the scourge of modern times, have once again rocked the nation, and this time around, important personalities from different fields have been scathed by this menace, not only that scamsters are piggy banking on these important and influential personalities, in an attempt to con the common man.

In a recent case a sophisticated online financial scam has been detected, which is actively being circulated on Facebook. The said video leveraged a manipulated or AI-generated deepfake video of Prime Minister Narendra Modi to lend credibility to a fake investment platform called "Paytastic Prism." The scam uses emotionally persuasive language, fraudulent endorsements by Indian leaders and technocrats, and AI-driven claims of “guaranteed earnings.” The campaign is hosted through a redirector link that collects personal data and solicits a minimum investment of ₹21,000 under the pretext of high daily returns via a secure network allegedly tied to the State Bank of India.

In another development, a deepfake of Ms Nirmala Sitharaman, the Union Finance Minister, was circulated on Facebook, as late as in end of June 2025, in which she was shown promoting an investment scheme, which seemed too good to be true, but in reality, was fake. In the said fake video, the present day Union Finance Minister was shown promoting an AI-driven solution that promised guaranteed returns of ₹1.9 lakh per month on a one-time minimum investment of ₹21,000.

Why is This Investment Scheme Fake?

What is being sold in the video through the deepfake of Ms Sitharaman seems too good to be true, and coming from the Union Finance Minister, most would certainly believe every word that is spoken. However, there are certain things, about the investment scheme which not only raise suspicion but also forces us to believe that it is fake. The spiel in the video is silent about the investment period (how long one needs to remain invested) for the returns to start flowing. Worse the spiel does not say a word about how long the returns from the investment would flowand it does not answer how a one-time investment will generate monthly returns of ₹ 1.9 lakh per month.

Additionally, the branding in this clip is inconsistent and misleading. Senior journalist Rajdeep Sardesai is presently associated with the India Today Group, but the video featuring Sardesai with Mrs Sitharaman bears the logo of Times Now. Even in the case of the video featuring the interview done by Ms Palki Sharma Upadhyay of Ms Sitharaman, while the former is associated with News18, the video bears the logo of the India Today Group.

Not The First Time

This is not the first time that scammers have misused the identity of influential personalities, including that of the Union Finance Minister Ms Sitharaman. A similar incident occurred in 2024, where a video was spread online in which she was shown as promoting an investment platform that guaranteed ₹15 lakh returns within 30 days on a investment of ₹21,000. Like in the recent case of Ms Sitharaman, even this case, the video had no mention of the investment period and that of how long the returns would flow from the said investment, Most importantly even in this case the spiel did not say a word on howSimilarly, this incident also had certain things not clear, like the period of return and didn't mention the investment period for how long a person has to invest.

Further on 19 February 2025, another deepfake clip was shared which featured Ms Sitharaman endorsing an automated platform called “Quantum A.I.” which promised daily earnings of up to ₹80,000 from an investment of ₹21,000.

That’s not all, in another incident on 23 May 2025, another deepfake video was discovered where Ms Sitharaman and senior journalist Palki Sharma Upadhyay were discussing an investment scheme. Experts detected unnatural jaw movements and, distorted background.

Many other high-profile personalities, including Narendra Modi, Prime Minister of India, Mukesh D. Ambani, Chairman and Managing Director, Reliance Industries and Virat Kohli, former captain of the Indian Cricket team were targeted by scammers to make deepfakes.

What is a Deepfake?

A Deepfake is a form of synthetic media that is created by using AI) and deep learning techniques, where existing images, videos, or audio recordings are manipulated to make it appear as if someone did or said something they never actually did.

In the instances mentioned above the scammers by using the deepfake of influential personalities (politicians and senior journalists), in a move to make their evil designs look genuine so that they are able to gain the trust of the public with ease. In the instances mentioned above scammers have used deepfakes of important personalities (Mr Modi and Mr Sitharaman) and senior journalists (Mr Sardesai and Ms Upadhyay). In the instances mentioned above not only have scammers used important politicians to convey their message but have used senior journalists to convey their message, in an attempt to gain credibility to their evil designs.

The Most Recent Attack Chain

In the case of the most recent incident featuring Ms Sitharaman, occurred when a fake Facebook account “Times.India” posted the said video. The video, that was posted, included a link, when people clicked on the link mentioned in the post or video/video, they were directed to cloned website that resembled the website of The Times of India. Clicking anywhere on the website takes the individual to a registration form.

The details asked in the form include things like name, email, and phone number, for further interaction. Once the user submits the form (with the necessary details), a scammer posing as a financial consultant contacts him/her, to sell the spiel about the investment scheme which was used as a bait in the deepfake.

Impact

In all the instances mentioned above a deepfake is used to lure unsuspecting individuals into a bogus investment scheme. By submitting personal information, victims can be forced to bite the bullet after future interactions with the scammer. Apart from financial losses data collected by the scammer through registration forms can be sold on the dark web or can be reused for future scams.

The emotional impact on victims could be severe. Victims may face stress and loss of confidence when they realise, that they have been conned. Moreover those who bit the bullet after having buying into the spiel, sold through Mr Modi and Ms Sitharaman, could even loose trust in the government.

This scam would certainly have caused reputational damage to important personalities who had been scathed by this scam. This includes personalities like the Murthy’s and the media houses.

Data Breach at Qantas

Australia's flagship carrier Qantas became the latest victim of a data breach. On 30 June 2025, personal details of about 5.7 million of its customers were leaked. While no financial information or passwords were compromised, in the said breach, the incident has raised concerns due to the sheer volume of personal data that got exposed which included details like names, email addresses, phone numbers, home addresses and date of birth of its customers.

This breach happened because a cybercriminal group, gained accessunauthorised access to a third-party customer service platform that was being used by Qantas.. The said third party at whose end the breach happened helps businesses manage and improve their customer support operations. The TTP of the attack is believed to involve advanced social engineering techniques that include AI-generated voice cloning which was used to infiltrate systems. Qantas confirmed that its core operational systems, flights, and bookings were not impacted, by the said breach, and that customer accounts remained secure.

Till now, no group has officially claimed responsibility for this incident. However, reports suggest that a hacking group known as "Scattered Spider" (also known by aliases such UNC3944, Octo Tempest and Star Fraud) may be behind the breach. This group is known for executing high-level intrusions through a mix of technical skill and psychological manipulation.

Response by Qantas

On 09 July 2025, Quantas notified the Australian Federal Police the Australian Cyber Security Centre and the Office of the Australian Information Commissioner about the breach. The airline is working with forensic cybersecurity investigators and external security experts to assess and contain the impact, of the breach.

It needs to be noted that to boost customer trust and support, Qantas improved its customer support by introducing a 24/7 helpline for resolving customer queries. Post this breach, they informed every passenger who was impacted, offering transparency around the nature of the compromised information and also enabled self-check visibility in Frequent Flyer accounts. Further the airline has been cooperating with the national authorities in the investigation of this incident.

A Wake-Up Call for the Aviation and Cybersecurity Sectors

The breach at Qantas is a reminder that cybersecurity threats are no longer limited to internal systems of a company. The growing dependence of an organisation on the external service providers, especially those operating across borders, has given birth to risks that demand high-level security checks, real-time monitoring, and legally enforceable compliance frameworks.

This breach, at Quatas, is one of the largest breaches of Australia since the high-profile attacks on Optus and Medibank, in 2022. Law firm Maurice Blackburn has already filed a formal complaint against the airline, alleging that it failed to adequately safeguard customer data in line with privacy laws.

Data Breach Exposes Details of UK's Secret Services

A data breach first recorded in 2022 has now come to light, and has exposed the identities of UK intelligence officers, Special Forces members, and thousands of Afghan nationals who had collaborated with the British. UK Government had banned the media from reporting on this incident by a strict court order. But due to rising legal pressure as law firms started demanding justice for the people exposed in the breach, those restrictions have been lifted, allowing the press to report on the full extent of the breach.

In 2022, an employee of the UK Ministry of Defence (MoD) accidentally sent an email containing a spreadsheet to a group of Afghans who had applied for relocation under the Afghan Relocations and Assistance Policy (ARAP).The file contained sensitive details of nearly 19,000 Afghan citizens, as well as 100 British officials, including MI6 agents and Special Forces personnel. This accidental disclosure placed both Afghan allies and UK operatives at serious risk.

In response, the UK Government launched a secret relocation operation named Operation Rubific in August 2023 to move thousands of Afghans to safety. However, the data breach revealed details like the names, job details, and contacts of people working secretly with the UK. This created a national security emergency and instilled fear among many Afghans, who feared reprisal from the Taliban. . The exposure of UK spies and Special Forces is a serious national security threat. The seriousness of the breach can be gauged from the fact that the John Healey, Defence Secretary, offered his sincere apology for the breach. Law firms are now demanding legal action for the people who are affected, by the said breach.

This breach is a reminder that even a simple mistake can be lethal, especially when sensitive data is involved. The breach underlines the the need of for data protection policies reform, as failure to do so can risk many lives.

Saudi Industrial Services Group Breached

In July 2025, Saudi Arabia's Rezayat Group—a major industrial services conglomerate operating across engineering, manufacturing, logistics, and more—was hit by a ransomware attack that is attributed to the Everest gang, a notorious cybercriminal collective with ties to past high-profile breaches. The Rezayat Group comprises of 25 companies operating across sectors like engineering, manufacturing, logistics and others.

The hackers posted data on their dark web leak site, claiming to have stolen several gigabytes of data. The researchers have investigated the sample data that the attackers shared in their post. Some of the samples contain the contract information of the company with their clients, which can affect the company's reputation, and thereby have an impact not only on existing project but also have the possible inflow of project, in future. The Saudi-headquartered Rezayat Group operates in over 13 Countries across the globe.

The attackers claimed to have breached approximately 10GB of the company's records. However, researchers find it hard to attest this claim primarily because of the paucity of enough proof shared by the hackers to support their claim.

The Everest ransomware group is no stranger to global cybercrime. Believed to have ties with the Russian-linked BlackByte cartel, the group has a history of attacking major enterprises. In recent months, the group has claimed responsibility for several high-profiled attacks. On 22 May 2025, the group targeted multinational soft drinks producer Coca-Cola. On 25 May 2025, the group targeted Mediclinic, a $5 billion organisation in the health sector and threatened to leak the stolen internal data and employee records, unless its ransom demands were met. The Group was also behind the cyberattack on AT&T in October 2022.

Luxury Brand Louis Vuitton Reports Data Breach

Following instances of data breaches at luxury brands like Dior, Tiffany & Co., and Must It, in South Korea, Louis Vuitton too, faced a similar fate, which was discovered on 4 July 2025. Post the luxury brand taking note of the data breach, it published a notice on its website which stated that a third-party temporarily accessed the company's systems on 08 June and exposed sensitive customer information. The company assured its customers that no financial information was compromised in the breach.

South Korea is not the only jurisdiction in which Louis Vuitton faced threats like the afore-mentioned breach as similar incidents were reported across the brand's international branches, in the same month. The company's Turkey division disclosed that approximately 143,000 customers were affected by a similar breach. Around the same time, Louis Vuitton UK also confirmed a customer data leak. The common thread which links all the three incidents was the involvement of third-party entities that gained unauthorised access to sensitive information. This growing wave of intrusions raises concerns about a decline in brand value and erosion of customer trust.

The rise in cyberattacks on luxury brands highlights the growing threat posed by vulnerabilities with third-parties. To counter such threats, companies need to strengthen their cybersecurity frameworks. Post this breach, customers were advised to monitor their communications closely, avoid clicking on suspicious links, and report any unusual activity to the relevant customer support channels.

AI Accountability Takes Centre Stage at GSAIET2025

The leading lights of the AI domain came under one roof on 24 July 2025. On the said day, a dazzling assortment of global thought leaders, experienced lawyers and intelligentsia descended on the stage of the Global Summit on AI, Emerging Tech Law, and Governance (GSAIET2025). The speakers included esteemed personalities like Dr Rajiv Mani, Additional Secretary, Ministry of Law & Justice, Government of India and Alfredo M. Ronchi, General Secretary of the European Commission's MEDICI Framework, among others. The summit—the brainchild of Dr Pavan Duggal, a senior advocate at the Supreme Court of India and a global authority in Cyberlaw and Cybersecurity.

In his opening remarks Dr Pavan Duggal, shed light on the current landscape of AI regulations. He then highlighted how different global jurisdictions are developing frameworks to govern the use and reduce the impact of AI technologies. Dr Duggal, after giving recommendations for Indian policymakers to enable them to come to grips with the rapidly changing landscape, concluded his speech to an applauding audience.

Kanishk Gaur, CEO of Athenian Tech, was part of a panel at the summit—AI Accountability & Liability. Speaking at the panel, he highlighted his concerns regarding AI and the lack of safeguards to protect Private Personal Information (PPI) on AI platforms. He compared the rapid growth of AI to a tsunami and stressed that legal and ethical frameworks in the field of AI are still lagging behind. He also shed light on the ambiguity in data collection by AI firms and their lack of responsibility in case of data leaks.

Further, Mr Gaur warned the rapt audience about the risks of uploading documents like Aadhaar cards, Voter IDs on AI platforms. He concluded his speech by making a passionate call to action for professionals in the audience to come together in making clear AI regulations to protect institutions and consumers.

Agentic AI

Agentic AI is growing rapidly in the field of AI and is becoming the transformative force, moving beyond the capabilities of standard and even Generative AI to make fully autonomous and goal-oriented systems.

Agentic AI refers to a class of artificial intelligence systems that are fully capable of making Autonomous Decision-Making a step ahead of classical AI or generative AI, which depends on reacting to prompts or being set to follow predefined rules. Agentic AI can take its own decisions independently on how to complete a task that has been assigned to it. One of its features is Goal-Oriented Behaviour, which makes it very efficient as it doesn't waste time on unnecessary work, as it is designed to work on specific tasks only. It works on the principle of divide and conquer, which is to break down the big task into smaller parts and solve them. It has the capabilities to integrate with Api to concrete actions in the real world or digital world.

For working on an AI model, data plays a very important role; it is one of the fundamental things of AI. Its working also starts with gathering the data from multiple sources like APIs, databases, user interactions, etc, to understand the current state. Then it further moves to the reasoning part. The collected data is then being used for collecting insights, interpreting queries and detecting patterns to understand the context. The decision-making part will give efficiency, accuracy, and predict outcomes. After that, the Learning and Adaptation part will take place, and then our agent will be ready to make decisions on its own.

Emerging Use Cases and Examples

Nowadays, Agentic AI has spread to almost every field, whether it's tech or non-tech. For an e-commerce website, Agentic AI is handling the flash sales, dynamically adjusting pricing, and triggering notifications based on real-time data. This whole task is handled by Agentic AI. When we talk about the tech sector, almost everything can be done by using this, like code generation and refinement, CI/CD Automation.

It works in HR operations by automating resume screening, answering HR queries, and performing various tasks such as updating job statuts and streamlining onboarding processes. Agentic AI can not only help by automating the tasks, but it can also fundamentally redesign how the work is done.

The rapid pace at which technology is evolving, is a double-edged sword. While on the one hand advancements in technology does have its share of benefits but it also exposes all us to a new kind of threats/dangers. And in this context we are speaking about cyber threats. The fact remains that despite the imminent dangers, in his hyper-connected world, we willingly leave our digital footprints which are later on devoured by nefarious elements, especially on social media platforms. For anyone who has not yet bit the bullet of social media, must truly be living under a rock. Finding such people in this hyper-connected world would be nothing less than a miracle. On the other hand one cannot deny the popularity of social media platforms. While it is nice to be connected with the world via social media, it is equally important to stay safe when traversing these platforms. Some precautions that one should ideally be taking when navigating the web of social media, whether to seek pleasure or to gain insights are mentioned below.

Strengthen Password & Access Management

One of the most important steps in ensuring data safety is to set a strong password and implement access management. This involves creating strong, unique passwords, preferably a mix of upper and lowercase letters, numbers, special characters and symbols. Try to avoid the reuse of one password across multiple platforms. You should regularly update your passwords, especially after any breach or if you come across/notice any suspicious activity. To simplify secure management, consider using a reputable password manager.

Enable Two-Factor Authentication (MFA)

Enabling Multi-Factor Authentication (MFA) provides an extra layer of security to your account. Instead of relying only on a password, which can be guessed, leaked, or stolen, MFA works by combining two or more different types of verification. It uses your phone or a security key, and something you are, like your fingerprint or face. You should use MFA to stay safer online.

Use Secure Networks

Use of a secure network is a crucial step in safeguarding your personal and sensitive data. The Wi-Fi networks that are found in cafés, restaurants, airports and other public places are generally exploited by hackers as they are easy to hack. You should avoid using Internet services from these sources, and if it is an emergency, connect it through a trusted Virtual Private Network (VPN) as it encrypts your Internet traffic and masks your IP address, which makes it difficult for hackers to track or steal your data. Your personal Wi-Fi should be protected by a strong password and use WPA2 or WPA3 encryption standards.

Avoid Accepting Friend Requests from Strangers

You should avoid accepting friend or follow requests from an unknown persons. Scammers and cybercriminals often create fake profiles to trick people. Also, try to avoid follow requests from people who have a very few followers or suspicious profile pictures. Accepting unknown people can expose you to identity theft, phishing scams and even cyberstalking.

Think Before You Click

Nowadays, cybercriminals often send suspicious links through email, messages, social media, or pop-up ads to trick users. When clicked these links will take you to a phishing website or lead you to downloading malware onto your system that can corrupt your system or worse case, corrupt your system. You should avoid clicking on such links. Always check the sender, look for spelling errors or strange URLs, and avoid clicking on anything that seems unexpected or too good to be true.

Athenian Tech

Contact Us

www.atheniantech.com

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