MANOHAR PARRIKAR
idsa
MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

CYBER *Digest*

October 2025

- **Cyberattacks Target Automotive Industry**
- **European Airports Face Disruptions Following Cyberattack**
- **Cyberattack hits Russian Election Systems**
- **Cyberattack Halts Production at Japan's Asahi Group**
- **Panama's Ministry of Economy and Finance Discloses Security Breach**
- **Nursery Chain Hack Exposes Personal Details**
- **Las Vegas Teen Arrested for 2023 Casino Hacks**
- **India File**

Cyberattack Targets Automotive Industry

Tata Motors-owned Jaguar Land Rover (JLR) has extended its production shutdowns following a cyberattack that crippled global operations, halted manufacturing, and disrupted its supply chain. The company has taken its IT systems offline in response, while industry sources warn the impact could persist into November.[1] The cyberattack is expected to cost JLR hundreds of millions of pounds and has thrown its extensive supply chain into disarray. A Telegram group calling itself "Scattered Lapsus$ Hunters", combining the names of the notorious Scattered Spider, Lapsus$, and ShinyHunters collectives, has claimed responsibility for the breach by posting a screenshot allegedly showing JLR's internal systems, according to threat researchers. JLR, however, has not disclosed details of its investigation and is currently working with external experts.

Estimates suggest that JLR, a subsidiary of Tata Motors, may have incurred revenue losses of $50–70 million per week, with the total financial impact of the incident projected to range between $1.7 billion and $2.4 billion.[2] In a separate incident, automotive giant Stellantis confirmed that attackers had accessed data belonging to some of its North American customers through a breach of a third-party service provider's platform.[3] Following the attack, the company urged customers to remain vigilant against potential phishing attempts and to avoid clicking on suspicious links or sharing personal information in unsolicited emails, texts, or calls.

Tire manufacturing giant Bridgestone has also confirmed that it is investigating a cyberattack affecting operations at several of its North American manufacturing facilities.[4] The company stated that its swift response helped contain the incident in its early stages, preventing any theft of customer data or deeper network intrusion.

European Airports Face Disruptions Following Cyberattack

Several European airports faced continued disruption after a cyberattack hit Collins Aerospace, a company providing check-in technology.[5] The attack affected major hubs including London Heathrow, Berlin, and Brussels airports. Brussels Airport also requested airlines to cancel departing flights as its check-in systems remained down. Reports indicated that the disruption was confined to electronic check-in and baggage drop systems and could be managed through manual check-in procedures.

Cyberattack hits Russian Election Systems

Ukraine's military intelligence agency (HUR) claimed responsibility for hacking Russia's Central Election Commission (CEC) and other government services in response to elections held in "occupied" Ukrainian territories.[6] The operation coincided with Russia's "unified voting day," when regional and local elections take place simultaneously across the country, including in Crimea and other areas, which Kyiv and its allies deem illegal. HUR said its distributed denial-of-service (DDoS) attack targeted the CEC servers, Russia's electronic voting system. Russia confirmed that its election-related websites faced sustained attacks. Officials acknowledged that the CEC website

experienced intermittent outages but emphasized that the voting process itself was not affected.

Cyberattack Halts Production at Japan's Asahi Group

According to reports, Japanese beverage and beer giant Asahi Group Holdings remains unable to resume production at its domestic factories a day after a cyberattack, with no clear timeline for recovery.[7] The company operates 30 plants in Japan producing beer, beverages, and food products, but it is still assessing whether all facilities have halted operations. The producer of Asahi Super Dry Beer, Nikka Whisky, and Mitsuya Cider stated that its group companies in Japan suspended operations, including order processing, shipping, and call center services, following a system outage caused by a cyberattack, although no personal data breaches have been reported.

Panama's Ministry of Economy and Finance Discloses Security Breach

Panama's Ministry of Economy and Finance (MEF) reported that one of its computers may have been compromised by threat actors. The Ministry promptly activated security protocols to contain the threat, emphasizing that critical systems essential to operations remain secure.[8] According to MEF, potential malware was detected on a workstation, and swift action was taken to isolate the threat and safeguard the broader network. Reports indicate that over 1.5 TB of data from MEF, including emails, budget information, and financial files, may have been compromised by the INC Ransom group, which also released internal documents as proof of the breach.[9] MEF has not yet confirmed these claims. The ransomware group INC Ransom, active since 2023, threatened to release additional sensitive data if ministry officials failed to make contact, after initially publishing a small portion of the stolen information to pressure the victims.[10]

Nursery Chain Hack Exposes Personal Details

Hackers say they have stolen the pictures, names and addresses of around 8,000 children from the Kido nursery chain.[11] The gang of cyber criminals is using the highly sensitive information to demand a ransom from the company, which has 18 sites in and around London, with more in the US and India. The criminals say they also have information about the children's parents and carers as well as safeguarding notes. They claim to have contacted some parents by phone as part of their extortion tactics. The company has not released any public statements about the hack but parents and nurseries have been notified.

Las Vegas Teen Arrested for 2023 Casino Hacks

A teenage boy suspected of involvement in the cyberattacks targeting several Las Vegas casinos in late 2023 was arrested after turning himself in, according to the Las Vegas Metropolitan Police Department.[12] He was booked on multiple charges, including extortion, conspiracy to commit extortion, unlawful computer activity, and three counts of using personally identifiable information to harm or impersonate others. While authorities did not detail his specific role, they confirmed his connection to the high-profile casino breaches attributed to the Scattered Spider group, which carried out major attacks on

MGM Resorts International and Caesars Entertainment between August and October 2023.

India File

- Standardisation Testing and Quality Certification (STQC) is now mandatory for CCTV cameras in India to ensure compliance with cybersecurity, quality, and safety standards.[13] The certification aims to prevent data leaks, including attempts to extract footage through software modifications. Licenses will be granted only after authorities verify that there are no loopholes allowing surveillance data from India to be transmitted to foreign servers.
- In a major move to curb the misuse of telecom resources in cybercrimes and financial fraud, the Department of Telecommunications (DoT) and the Financial Intelligence Unit–India (FIU-IND) have signed a comprehensive Memorandum of Understanding (MoU) to strengthen information sharing and coordination.[14] The enhanced data-sharing framework will leverage advanced technology platforms, including the DoT's Digital Intelligence Platform (DIP) and FIU-IND's Finnex 2.0 portal. These system-based exchange portals will enable secure, real-time transmission of information between the two agencies.
- Amid rising cyber thefts, the government has made cybersecurity audits mandatory for all cryptocurrency exchanges and custodians. Platforms must engage a security auditor registered with the Indian Computer Emergency Response Team (CERT-In), the national agency handling cybersecurity incidents.[15] Additionally, registration with India's anti-money laundering authority, the Financial Intelligence Unit (FIU), now requires all virtual digital asset (VDA) service providers to comply with this rule. According to reports, FIU-designated directors, principal officers, and chief compliance officers of these firms are expected to implement the measures immediately.
- A recent report points out that India's education and research sector remains one of the most targeted for cyberattacks, facing an average of 7,095 weekly attacks per organisation, higher than government and consumer goods sectors and second globally only to healthcare.[16] The rise in attacks is driven by unique set of factors such as expanded digital footprint through hybrid learning, connected campuses, and widespread device use, combined with limited cybersecurity budgets, outdated infrastructure, and small IT teams, leaving institutions highly vulnerable.

[1] Industrial Cyber, Jaguar Land Rover cyberattack deepens, with prolonged production outage, supply chain fallout, 17 September 2025, https://industrialcyber.co/manufacturing/jaguar-land-rover-cyberattack-deepens-with-prolonged-production-outage-supply-chain-fallout/

[2] Dark Reading, Jaguar Land Rover Shows Cyberattacks Mean (Bad) Business, 3 October 2025, https://www.darkreading.com/cyberattacks-data-breaches/jaguar-land-rover-cyberattacks-bad-business

[3] Bleeping Computer, Automaker giant Stellantis confirms data breach after Salesforce hack, 22 September 2025, https://www.bleepingcomputer.com/news/security/automaker-giant-stellantis-confirms-data-breach-after-salesforce-hack/

[4] Bleeping Computer, Tire giant Bridgestone confirms cyberattack impacts manufacturing, 4 September 2025, https://www.bleepingcomputer.com/news/security/tire-giant-bridgestone-confirms-cyberattack-impacts-manufacturing/

[5] CNBC, What we know about the cyberattack that hit major European airports, 7 October 2025, https://www.cnbc.com/2025/09/21/what-we-know-about-the-cyberattack-that-hit-major-european-airports.html,

[6] The Record, Ukraine claims cyberattacks on Russian election systems; Moscow confirms disruptions, 16 September 2025, https://therecord.media/ukraine-claims-ddos-attack-russian-election-system

[7] Reuters, Japan's beer giant Asahi Group cannot resume production after cyberattack, 30 September 2025, https://www.reuters.com/technology/japans-beer-giant-asahi-group-cannot-resume-production-after-cyberattack-2025-09-30/

[8] Security Affairs, INC ransom group claimed the breach of Panama's Ministry of Economy and Finance, 15 September 2025, https://securityaffairs.com/182203/data-breach/panamas-ministry-of-economy-and-finance-data-breach.html

[9] SC Media, Data security incident admitted by Panama Ministry of Economy and Finance, 12 September 2025, https://www.scworld.com/brief/data-security-incident-admitted-by-panama-ministry-of-economy-and-finance

[10] Ibid.

[11] BBC, Children's names, pictures and addresses stolen in nursery chain hack, 25 September 2025, https://www.bbc.com/news/articles/c62ldyvpwv9o

[12] Cyberscoop, Las Vegas police arrest minor accused of high-profile 2023 casino attacks, 22 September 2025, https://cyberscoop.com/las-vegas-teenager-arrested-casino-attacks-scattered-spider/

[13] Matrabhumi, New cybersecurity measures: STQC certification now required for CCTV cameras in India, 14 September 2025, https://english.mathrubhumi.com/news/india/new-cybersecurity-measures-stqc-certification-now-required-for-cctv-cameras-in-india-qpdfsy7n

[14] Press Information Bureau (PIB), DoT and Financial Intelligence Unit- India Sign Landmark MoU to Combat Cyber Crimes and Financial Frauds, 25 September 2025, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2171135

[15] Business Standard, Cybersecurity audits mandatory for crypto exchanges amid rising thefts, 17 September 2025, https://www.business-standard.com/markets/cryptocurrency/government-mandates-cybersecurity-audits-for-crypto-exchanges-fiu-cert-in-125091700273_1.html

[16] The Economic Times, India's education sector remains prime cyberattack target: Report, 24 September 2025, https://economictimes.indiatimes.com/tech/technology/indias-education-sector-remains-prime-cyberattack-target-report/articleshow/124088526.cms