KDDI Europe

Global Threat Intelligence Report

Volume 6

October 2025

Table Of Contents

A Message to Readers

By Shintaro Takeda, Director, Strategy Development, KDDI Europe
October 1st, 2025

Greeting.

I would like to begin by expressing my sincere thanks to the team behind this report.
Henry Finnah – Thank you for keeping us engaged by selecting and sharing the most relevant news and vulnerabilities, giving us insights into ever-evolving cyber threats and occasional video appearance on our LinkedIn.
Konoka Kawakami – Thank you for designing the graphics, proofreading the content and distributing this valuable information through the monthly newsletters.

This edition marks the 6th volume of the Threat Report, which we at KDDI Europe launched in May to provide busy readers with what we felt was most relevant to be aware of and to improve the security of the organisations.

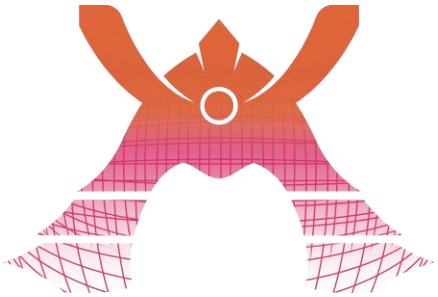
From this volume, I would like to introduce and welcome **Monica Galiano**, who will share her expertise in **Regulatory Insights**. As most of you are familiar with, threats to the business are not just cyberattacks but also changes to legislations. A lack of awareness can set you back compared to competitors or you may be penalised. We aim to provide you intelligence in an easy-to-read and concise manner.

It is our team's shared goal to support you and your business.

If you have any requests or questions regarding the report, please don't hesitate to reach out.

Sincerely,
Shintaro Takeda

Introduction



Welcome to the Threat Report. The purpose of this document is to provide an overview of the latest cybersecurity threats, trends and regulations that could impact organisations worldwide. By analysing recent incidents and emerging threats, we aim to equip our team and customers with the knowledge and insights necessary to proactively defend against potential attacks.

At KDDI Europe, our dedication to protecting our clients and their systems is unwavering. We are continuously investing in security technologies and training our staff to enhance defences and respond swiftly to any threats. We are deeply committed to ensuring that our customers are protected in accordance with the highest standards of cybersecurity.

It is our belief that our success is linked to the success of our customers' businesses. By safeguarding your operations, we aim to provide a secure environment where your business can thrive and grow. Thank you for taking the time to review this report.

Disclaimer

This content is provided for general informational purposes only and does not constitute legal advice. Readers should seek guidance from qualified legal professionals regarding the application of any law or regulation to their specific circumstances.

NEWS

The Latest Cybersecurity News

Jaguar Land Rover Suffer Cyber Attack. [1]

Vehicle production has been halted by the UK based automaker after falling victim to a cyber-attack at the beginning of September 2025. The organisation stated that while it did not believe any data had been stolen earlier, “some data” may have been affected. Production was scheduled to resume on the 24th of September 2025 but has since been pushed back as at the writing of this report. A group known as “Lapsus$ Hunters” has claimed responsibility for the attack and have been observed bragging about their attack on Telegram.

Cyber-attack causes flight delays across Europe.[2]

Passengers travelling from several European airports including Brussels, Berlin and Heathrow in London, had their flights cancelled or delayed due to a cyber-attack which has now been revealed to be a ransomware attack. Passengers had to be boarded manually because the automatic check-in and boarding software had been disrupted. Collins Aerospace, the company that provided the software that was used by the affected airports, is one of the largest aviation and defence companies in the world and is currently working to restore all systems.

Threat Insights

In light of the recent surge in cyber-attacks targeting organisations, it is worth asking whether attackers are employing techniques that outpace defensive measures or whether more effort is invested in compromising systems than securing them. A recent supply chain attack shows that such breaches are not inevitable; there are safeguards that can prevent them.

Mandiant, a cybersecurity firm owned by Google that specialises in cyber defence threat intelligence and incident response, investigated the Salesloft Drift breach [5] and revealed that the attack began when threat actors gained access to the Salesloft GitHub account. With this initial access, threat actors were then able to conduct reconnaissance then plan out their attack further. The method used by the threat actors to compromise the GitHub account was not stated in the report, however, we can explore 3 methods of preventing unauthorised access to accounts such as this.

1. MFA may not be perfect but should be enabled where possible. It is a fundamental security measure which can help reduce the risk of unauthorised access to user accounts. Despite its effectiveness, it remains surprisingly underutilised by some users today.
2. If Single Sign-On (SSO) is available on the platform, it should be enabled. SSO allows user accounts and access permissions to be managed centrally through an Identity Provider (IdP), such as Entra ID or Okta. This approach also supports the enforcement of security policies that govern access conditions during sign-in.
3. The use of an Identity Threat Detection & Response (ITDR) solution. ITDR solutions are designed to use behavioural analysis, anomaly detection and threat hunting to detect and respond to unauthorised attempts to sign into user accounts. For example, if a threat actor attempts to sign into an account from an unexpected location for the first time, the sign-in attempt can be blocked and or the appropriate team will receive a notification of this attempt.

If the system does not have mechanisms for enabling MFA or SSO, or ITDR is not viable, then consider a new provider/vendor, one with a greater commitment to security because security is a shared responsibility.

Regulatory Insights

The UK Data (Use and Access) Act 2025: what could it mean for You?

The UK Data (Use and Access) Act (DUA Act) is a recent UK Law that amends the Data Protection Act 2018, the UK GDPR, and the Privacy and Electronic Communications Regulations 2003 to promote innovation and facilitate data access and sharing.

Some provisions took effect immediately after Royal Assent on 19 June 2025, while most measures will be introduced through secondary legislation between summer 2025 and spring 2026. For general or expert overviews, see the ICO's published summaries [6][7].

Since many rules await further legislation and ICO guidance, below we highlight only a few amendments that are already applicable and enforceable today, along with our view on how they may impact You.

Digital Verification Service (DVS) Trust Framework

The DUA Act gives legal status to Digital Verification Services — accredited systems that allow individuals to prove information about themselves online (like their age, identity, or qualifications). This is not a compulsory digital ID, but a framework for secure, optional verification.

- DVS providers must ensure to meet defined security and compliance Standards and be ready to undergo external audits.
- DVS Consumers (organisations using DVS) should only engage accredited providers and contractually require compliance.

Recognised Legitimate Interest

The DUA Act introduces a new lawful basis for processing personal data without a balancing test (i.e. weighing the business interests against the individual's rights), provided it serves predefined socially beneficial purposes such as crime or fraud prevention, network and information system security, child protection, and emergency or public health response.

The addition of the Recognised Legitimate Interest:

- Provides clarity for processing data in security operations (e.g., intrusion detection, log analysis, threat intelligence).
- Enables faster incident response without a legitimate interest assessment.

Note that the new basis must be used strictly within listed purposes; misuse risks non-compliance.

Transparency obligations remain and privacy notices must be updated if this basis is used.

Automated Decision-Making (ADM)

Previously limited to consent, contract, or legal authorisation, ADM can now rely on any lawful basis except the new Recognised Legitimate Interest. Safeguards remain, such as informing individuals, allowing contestation, and enabling human review. Special category data is still restricted to consent or substantial public interest.

Watch out for new use cases that leverage ADM in your organisation. Your organisation remains responsible for ensuring ADM systems are secure, auditable, explainable, and supported by strong access controls and logging.

Scientific Research Clarifications

The Act now legally defines “scientific research”, “historical research” , and “statistical work” , expanding the scope of projects that qualify under this purpose.

- More data may be processed under scientific research purposes, increasing responsibilities for classification, pseudonymisation, and protection.
- Wider sharing of research data requires strict least-privilege access, monitoring, and review.

Applicability Across Jurisdictions

Organisations subject to both UK and EU GDPR must follow the stricter regime, since the DUA Act’s new permissions apply only in the UK. To manage this, businesses should map their data flows and, where possible, separate UK-only datasets from those under EU rules, using technical and organisational measures such as access controls or data residency solutions. Where separation is not feasible, applying the higher standard by default reduces risk. Clear records of processing, updated privacy notices, and appropriate transfer mechanisms for cross-border data remain essential to demonstrate accountability and ensure compliance across both regimes.

Conclusions

The DUA Act marks a turning point in UK data regulation. It introduces flexibility in data processing but also heightens security, ethical, and governance requirements. By cross-functional collaboration, organisation must ensure auditability, compliance, security and privacy by design, and protection of all new data flows.

As further provisions come into force, KDDI Europe will continue to provide insights on their impact on Your processes and operations.

Suggestions

Protection, Prevention and Takeaways

1. Security should never be reactionary; it should be proactive. Attacks should be anticipated, waiting for an attack to happen before formulating a solution is an approach that is bound to result in incurring cost and suffering from a disruption in service. An experienced IT professional can often identify the most vulnerable areas in their environment and where stronger security measures are needed. Are there any areas in your organisation you know fall short in terms of adequate security? Do you have a plan for resolving these deficiencies? Consider the answers to the questions as food for thought.

2. The ISO 22301 certification is an internationally recognised standard for Business Continuity Management System and is applicable to any organisation regardless of its size. It is beneficial to all, but maybe more relevant to high-risk sectors i.e. Oil and gas, utilities etc. In a nutshell it asks, “how prepared are you?” Following its guidelines is a good way to improve resilience, even if your organisation does not intend on getting this certification it is still worthwhile to go through documentation and processes involved as a self-evaluation to better understand how your organisation would fare in the face of cyberattacks, natural disasters or system failures.

3. How are you signing into portals provided by third parties and vendors? Who manages these accounts and how are they managed? Is there a documented process in place? Different SaaS applications and platforms are used across an organisation, but visibility should be maintained into each platform and administrators should ensure there is a protective mechanism in place and access is audited regularly to prevent unauthorised access.

Common Vulnerabilities and Exposures (CVE)

Every month a CVE is selected at the discretion of the report's author to be discussed. This report will also include the EUVD ID as well. This month it is a vulnerability affecting access points.

CVE-2025-10159 | EUVD-2025-27492 [8]

Vendor	Sophos
Product	AP6 Series Wireless Aps
Published	09 Sept 2025
Platform	N/A
CVSS	9.8

Description

An authentication bypass vulnerability allows remote attackers to gain administrative privileges on Sophos AP6 Series Wireless Access Points older than firmware version 1.7.2563 (MR7).

What does this mean for you?

Attackers can reach the access points management IP address to gain administrator level privileges on the device.

What should you do about it?

Immediately upgrade to the latest version of the application, so any version above 1.7.2563

Links & References

1. Sead Fadilpašić (2025). Jaguar Land Rover cyber attack outage continues - systems unlikely to be online for another week. [online] TechRadar. Available at: https://www.techradar.com/pro/security/jaguar-land-rover-cyber-attack-outage-continues-systems-unlikely-to-be-online-for-another-week [Accessed 22 Sep. 2025].
2. Wilson, T. (2025). European airport disruption continues after weekend cyber-attack. BBC News. [online] 22 Sep. Available at: https://www.bbc.co.uk/news/articles/cqjeej85452o.
3. We’re All in this Together. (n.d.). Available at: https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Year_in_Review_of_ZeroDays.pdf.
4. Charrier, C., Sadowski, J., Lecigne, C. and Stolyarov, V. (2024). Service Not Allowed. [online] Google.com. Available at: https://cloud.google.com/blog/topics/threat-intelligence/2024-zero-day-trends.
5. Salesloft.com. (2025). Salesloft Trust Portal. [online] Available at: https://trust.salesloft.com/?uid=Update+on+Mandiant+Drift+and+Salesloft+Application+Investigations.
6. Information Commissioner’s Office (ICO). (2025). The Data Use and Access Act 2025 (DUAA) – what does it mean for organisations? [online]. Available at: https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/data-use-and-access-act-2025/the-data-use-and-access-act-2025-what-does-it-mean-for-organisations/ [Accessed 24 September 2025].
7. Information Commissioner’s Office (ICO). (2025). The Data Use and Access Act 2025 (DUAA) – summary of the changes to data protection law. [online]. Available at: https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/data-use-and-access-act-2025/the-data-use-and-access-act-2025-duaa-summary-of-the-changes/ [Accessed 24 September 2025].
8. SOPHOS. (2025). Cybersecurity as a Service Delivered | Sophos. [online] Available at: https://www.sophos.com/en-us/security-advisories/sophos-sa-20250909-ap6 [Accessed 22 Sep. 2025].

Let’s Secure the Future — Together

KDDI Europe is the European headquarters of the Fortune Global 500 KDDI Corporation, delivering cutting-edge ICT and cybersecurity solutions with the precision and reliability Japan is known for.

With over 70 years of global expertise, we empower businesses across industries — from finance and retail to manufacturing and education — with secure, scalable infrastructure and 24/7 protection. Whether you’re looking to strengthen your cybersecurity posture or scale your global operations, **we are your partner, your enabler, your platformer.**

Security of Tomorrow, Today.

Contact Information

Telephone Number	+44 20 7507 0001
Email Address	info@uk.kddi.eu

Scan the QR codes below to connect with us online.

Website

LinkedIn

Enquiry