Global Threat Intelligence Report

Featuring Regulatory Insights

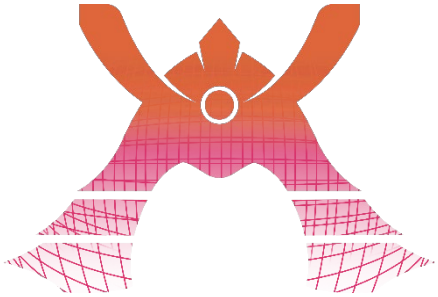
Volume 10 - February 2026

KDDI Europe

Cover Image: © Stuart Robertson (Senior Applications & Infrastructure Engineer, KDDI Europe). Photograph used with permission.

Table Of Contents

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.

News

The Latest Cybersecurity news

Europol makes arrests against "Black Axe" group [1]

On the 9th of January 2026, Europol published on its website that it had made 34 arrests during an action it was taking against the criminal organisation. The arrests were across 3 cities in Spain where €66,403 in cash was also found and seized by the security enforcement team. The organisation is believed to engage in criminal activities that are not limited to cybercrime alone and is reported to generate billions of euros yearly from its many operations.

CrowdStrike to acquire Seraphic [2]

On January 13th 2026, CrowdStrike announced it has signed an agreement to acquire Seraphic Security. The later provides a security solution for web browsers by using technology that turns any browser into a secure enterprise ready environment and delivering real-time protection against phishing, data risks and advanced threats. CrowdStrike intends to deliver a unified Next-Gen Identity strategy by integrating Seraphic's browser protection into it's Falcon platform.

Threat Insights

Supply Chain Attacks and CI/CD Pipelines.

CI/CD stands for Continuous Integration and Continuous Delivery/Deployment. It is a software development practice that automates how code is built, tested, and delivered. This automation enables faster deployment, higher-quality software, reduced human error, and better team collaboration, among many other benefits.

Because CI/CD systems are powerful and deeply integrated into the software delivery process, they are highly attractive targets for threat actors seeking to carry out supply chain attacks. From my perspective, these are some of the most common ways CI/CD pipelines are compromised'.

1. **Theft of credentials stored in CI/CD**: Information such as API keys, tokens and cloud credentials are frequently used by CI/CD systems. Since CI/CD systems often run with elevated privileges, these credentials can give attackers full access to production environments where they can inject malicious code leading to future iterations of software being compromised. A Palo Alto Networks red team exercise found that hard-coded IAM keys stored in a GitLab repository allowed testers to gain administrator-level access.
2. **Compromising package dependencies**: This could also be referred to as malicious code injection. The expectation here is that CI/CD systems will automatically pull and execute these packages which are basically bundles of code required by the application under development to work properly. By compromising the dependency packages, threat actors can infect the final application rolled out to users. A real-world example of this is the Shai-Hulud 2.0 supply chain attack.
3. **Exploiting Misconfigurations in CI/CD Infrastructure**: Threat actors exploit weak access controls and misconfigurations such as

overly broad repo permissions, exposed cloud resources leaking secrets, and unmonitored AWS accounts to steal credentials, manipulate code, and abuse CI/CD pipelines to execute malicious actions across the environment. Ultimately, these gaps create an easy pathway for attackers to infiltrate development workflows and compromise the integrity of the entire software supply chain

CI/CD pipeline exploitation gives attackers:

- Persistent access to cloud workloads
- Trusted distribution into production systems
- Ability to modify source code and artifacts
- Access to secrets and infrastructure credentials
- A way to infect thousands of downstream customers

This is why CI/CD pipeline security is a top priority in the software supply chain threat landscape.

Regulatory Insights

Surviving Regulatory Fines: Avoiding Financial Collapse Under UK and EU Cyber Laws

Regulators are no longer content with warnings. Fines under the UK CS&R Bill, GDPR, NIS2 and sectoral regimes are large, enforcement is active, and the financial and reputational fallout from outages or cybercrime can push firms toward insolvency. This article recaps the maximum penalties, explains the common triggers, and gives practical steps companies can take to reduce both financial exposure and reputational damage. Cyber insurance helps — but it is not a get-out-of-jail-free card.

What the maximum fines look like now

Under the UK GDPR, the Information Commission can impose maximum penalties of £17.5 million or 4% of an organisation's global turnover, whichever is higher, for the most serious infringements. Typical triggers are failures under Article 32 (security of processing), inadequate technical controls, delayed or incomplete breach reporting, poor supplier oversight, and failure to require multi-factor authentication. A high-profile example saw a data processor fined for not mandating MFA after attackers accessed systems used by NHS services, causing data theft and major disruption [3].

The NIS Regulations currently carry fines up to £17 million for the most serious operational failures. The incoming CS&R Bill will align NIS penalties with GDPR-style turnover-based caps — £17 million or 4% of worldwide turnover — dramatically increasing potential exposure for Operators of Essential Services and Digital Service Providers.

Sectoral regulators FCA and PRA can impose uncapped fines for operational resilience and governance failures; Ofcom and Ofgem can levy penalties tied to turnover for telecoms and energy firms. These sectoral regimes make resilience a board-level business risk, not just an IT problem.

In the EU, the “Cybersecurity Regulatory Triad” - NIS2, CRA, DORA - shifts enforcement from privacy to operational resilience [4]. NIS2 exposes essential entities to €10 million or 2% of global turnover for failing to implement proportionate security measures or for late reporting of significant incidents. The Cyber Resilience Act targets manufacturers of connected products and also imposes obligations across the supply-chain of digital products: fines of €15 million or 2.5% of turnover can follow if products are placed on the market with known vulnerabilities or without required updates. DORA focuses on financial services and their critical ICT providers and introduces the prospect of personal fines for executives — up to €1 million — where gross negligence or intentional misconduct is found.

Why fines can bankrupt a company

Regulatory penalties are only part of the cost. Legal defence, forensic investigation, remediation, customer notification, class-action settlements, and prolonged business interruption can be well above the fine itself. Reputational damage can dry up revenue and capital lines. For many firms, the combination of regulatory fines and consequential losses is the tipping point to insolvency.

Can cyber insurance save you?

Short answer: not for administrative fines in most cases. Regulated firms in the UK face explicit prohibitions on indemnification for regulatory penalties under rules such as the FCA Handbook. Even where there are no statutory bans, courts and insurers often treat fines for reckless or negligent conduct as uninsurable on public policy grounds. Norway and Finland are rare exceptions where limited coverage for administrative fines has been recognised, but insurers increasingly carve out gross negligence.

That said, cyber insurance remains critically important for preventing bankruptcy because it typically covers:

- Response costs: legal defence, forensic investigations, and PR.
- Civil liability: settlements and judgments from third-party claims.
- Business interruption: lost revenue during downtime.

But insurers have tightened terms. Two exclusions to watch: state-sponsored or "act of war" clauses that deny cover where attribution points to nation-state actors, and warranty-based underwriting that voids cover if pre-contractual statements (for example, about MFA or patching) prove false.

Important note: If your organisation has cyber insurance in place, ensure that the insurer is included in your Incident Response Plan among the parties that must be notified promptly upon becoming aware of a security incident. Virtually all cyber insurers require timely notification, and failure to notify within the required timeframe can jeopardise coverage—particularly where the policy makes prompt notice a condition precedent and where delay prejudices the insurer's ability to respond.

Practical steps to reduce financial and reputational risk

Insurance is a recovery tool, not a substitute for compliance. To reduce the chance of fines and to maximise recoveries after an incident, companies should prioritise the following:

- Gap analysis and framework adoption. Align controls with ISO/IEC 27001 or NIST CSF 2.0. Regulators look for evidence of recognised standards when assessing whether measures were "appropriate and proportionate."
- Incident reporting protocols. Automate detection and reporting workflows. Include insurer in the parties to be notified. Many penalties stem from late disclosure rather than the breach itself.
- Third-party risk management. Conduct legal and technical audits of suppliers. Under NIS2 and DORA, you are accountable for vendor security.
- Board-level oversight. Make cybersecurity a standing board agenda item. Documented approvals of risk assessments and remediation plans are a primary defence against personal liability.
- Insurance hygiene. Review policy wording with legal counsel and insurers before renewal. Avoid misstatements in applications and negotiate clarity on exclusions and conditionality.

- Tabletop exercises and crisis comms. Rehearse incident response with legal, management, technical, and PR teams to reduce response time and reputational harm.

Bottom line

You cannot buy your way out of regulatory responsibility. Fines are designed to punish and deter; insurers will not reliably step in to pay the price of regulatory failure. The pragmatic route is prevention: adopt recognised security frameworks, tighten supplier oversight, embed reporting discipline, and ensure board-level accountability. Use cyber insurance to cover the economic fallout — legal defence, remediation and business interruption — but treat it as part of a broader resilience strategy, not a replacement for compliance.

`

Column: Security Forefront

Were the 2025 Threat Forecasts Right?

In this column, we share our perspective on the latest cybersecurity trends, drawing on a wide range of sources. For this edition, through LAC's report 'LAC Security Insight', we would like to review the actual accident trends in 2025 while referring to the forecasts released by LAC for the first quarter of 2025 and gain insights.

Reference: LAC Co., Ltd. (2025) LAC Security Insight Vol.11 (Winter 2025), translated by Hiroki Morishita, KDDI Europe Limited.

Available at: https://www.lac.co.jp/lacwatch/pdf/20250313_lsi_vol11.pdf?utm_source=KEU&utm_medium=pdf&utm_campaign=threatreportKEUvol10pdf (Accessed: 30 January 2026).

Why Reviewing Last Year's Trends Matters

By looking back at the period from January to December 2025, we can understand how attackers actually operated. Their methods became faster, more automated, and increasingly focused on identity abuse. While LAC's report focuses on Japan, it helps in understanding patterns of major incidents that are common worldwide, and at the same time highlights what to pay attention to in the European context.

Introduction of LAC

LAC Co., Ltd., a subsidiary of KDDI, is one of Japan's most trusted cybersecurity companies. Through its SOC (Security Operation Centre), LAC provides advanced threat intelligence and incident response services. Their quarterly 'LAC Security Insight' report is widely recognized for analysing real-world attacks targeting Japanese organizations.

URL: https://www.lac.co.jp/?utm_source=KEU&utm_medium=organic&utm_campaign=threatreportKEUvol10hp

What LAC forecasted for 2025 in Japan (at the first quarter of 2025)

Increase and persistence of DDoS: This is driven by easily accessible DDoS for hire and residual vulnerable IoT devices that continue to be exploited for amplification and as part of botnets. Inventory management and vulnerability management of IoT devices are extremely important.

Human-targeting escalates: Phishing and social engineering (including investment scams and romance scams) continue to have high impact, extending beyond purely IT vulnerabilities to psychological methods.

Ransomware will continue to have a major impact in 2025: The primary method of initial access is through VPN/RDP or email to infect with RAT, and if MFA is weak or absent, abuse of Remote Monitoring and Management (RMM) tools (e.g., TeamViewer, AnyDesk, etc.) is also observed. At LAC, emphasis is placed on MFA, VPN strengthening, RMM governance, and training.

What happened actually in Europe 2025

DDoS: overwhelming in volume, strategic in impact

ENISA's dataset (Jul 2024–Jun 2025) shows DDoS accounted for ~77% of cyber incidents in the EU, mostly hacktivist-driven and low in individual impact but extremely frequent [5]. Throughout 2025, EU reporting continued to highlight waves of politically motivated DDoS against government and transport services [6]. DDoS has become an environmental threat—constant, noisy, and resource-draining.

Human-targeting escalates:

Phishing accounted for ~60% of initial EU intrusions [5]. Strictly speaking, the following data reflects the actual results for 2024, not 2025. This is because there is currently no data that fully covers 2025. However, using this data can still provide an understanding of the situation around 2025 [7].

- EU payment fraud patterns escalated: Social-manipulation scams up 156%, phishing up 77%.

- UK saw £1.1B+ yearly fraud losses.

Attackers now focus more on people than on systems.

Ransomware: remained the most damaging threat

The eCrime actor landscape continues to evolve, with ransomware remaining the most damaging threat. LockBit's infrastructure was disrupted in early 2024, but the group returned in 2025 with LockBit 5.0, targeting Europe again [8]. Industry analysis shows 2025 likely became Europe's worst ransomware year, hitting manufacturing, technology, and healthcare [9]. Ransomware is now a business continuity risk, not just a cyber risk.

Insight

The trends in Europe in 2025 largely confirm LAC's forecasts, showing that sustained DDoS activity, escalating persona-based attacks, ransomware pressure, and the abuse of remote access tools are not unique concerns in Japan, but rather consistent threat patterns globally.

Europe's experience highlights how regional contexts reinforce or reshape the same core risks. In the EU, politically and geopolitically motivated DDoS campaigns surged, zero-day exploits of VPN created urgent perimeter risks, and multinational financial ecosystems amplified the scale of fraud.

These distinctions demonstrate that LAC accurately predicted what would be important in 2025, while Europe illustrates how these threats manifest differently under geopolitical, regulatory, and economic conditions.

Recommendation

Readers can treat LAC's predictions as a reliable strategic benchmark.

However, it is essential to combine them with regional threat intelligence.

Focus on strengthening perimeter and identity management, managing remote access tools, improving ransomware recovery preparedness, and enhancing financial fraud defences, and tailor each measure to the specific threat situation in Europe.

Suggestions

Protection, Prevention and Takeaways

1. Threat actors follow the news, and so should you. A phishing email that appears to be based on real-world events can appear extremely legitimate. Staying informed through official press releases and legitimate communication channels will help you avoid being misled or scammed.
Take, for example, the case involving some users of the Manx email service [10]. After the provider announced that its ".net" service was being transferred to another provider, users began receiving phishing emails claiming they needed to provide their credentials and pay for a subscription, neither of which was true. Because the messages were tied to a legitimate announcement, many users were tricked into believing the requests were genuine.

2. Has your organisation developed or commissioned custom software? It is essential to maintain an up-to-date list of all components and third-party libraries used in any bespoke software or web applications. As part of regular security reviews, this list should be checked for newly discovered vulnerabilities that may have emerged after the application's release. Doing so helps ensure your business is not relying on "risky" software that could be exploited by threat actors.

3. AI-driven attacks are now mainstream and allow attackers to automate phishing at scale, generate malware variants faster than signature-based tools can react and exploit misconfigurations and exposed assets using AI-powered scanning. Users therefore need to more cautious of the information they interact with online.

Common Vulnerabilities and Exposures (CVEs)

Every month a CVE is selected at the discretion of the report's author to be discussed. This month it is a vulnerability affecting multiple versions of Microsoft Windows.

CVE-2026- 21265[11]

Vendor	Microsoft
Product	Windows 10/11, Windows Server 2012, 2016, 2019, 2022 Family
Publish Date	Jan 13, 2026
Platform	32-bit and 64-bit editions
CVSS (v3.1)	6.4

Description

The original certificates stored by Windows Secure Boot in the UEFI KEK and DB are approaching expiration. Devices containing affected certificate versions must update them to maintain Secure Boot functionality

What does this mean for you?

Certificate expiration breaks Secure Boot trust, weakens boot security and blocks future updates

What should you do about it?

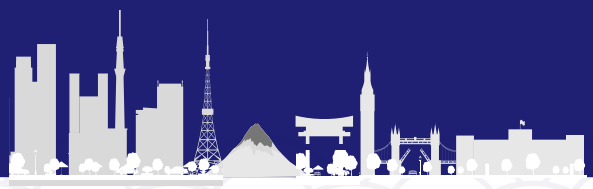
Install the security updates released by Microsoft on 13 January 2026 for relevant windows versions.

Links & References

1. Europol. (2019). 34 arrests in Spain during action against the 'Black Axe' criminal organisation – Criminal network engaged in a multitude of criminal activities and present in dozens of countries | Europol. [online] Available at: https://www.europol.europa.eu/media-press/newsroom/news/34-arrests-in-spain-during-action-against-black-axe-criminal-organisation [Accessed 15 Jan. 2026].
2. Crowdstrike.com. (2026). CrowdStrike to Acquire Seraphic, Turning Any Browser into a Secure Enterprise Browser. [online] Available at: https://www.crowdstrike.com/en-us/press-releases/crowdstrike-to-acquire-seraphic-security/ [Accessed 15 Jan. 2026].
3. Information Commissioner's Office (ICO) 2025, Software provider fined £3m following 2022 ransomware attack, ICO News and Blogs. [online] Available at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/03/software-provider-fined-3m-following-2022-ransomware-attack/ [30 January 2026].
4. Cloud Security Alliance (CSA) 2025, An update on European compliance: NIS2, CRA & DORA, CSA Blog. [online] Available at: https://cloudsecurityalliance.org/blog/2025/09/18/an-update-on-european-compliance-nis2-cra-dora [Accessed 30 January 2026].
5. ENISA. (2025). EU Consistently Targeted by Diverse Yet Convergent Threat Groups. [online] Available at: https://www.enisa.europa.eu/news/etl-2025-eu-consistently-targeted-by-diverse-yet-convergent-threat-groups [Accessed 30 Jan 2026].
6. ENISA / Industrial Cyber. (2025). ENISA highlights escalating hacktivist DDoS targeting EU. [online] Available at: https://industrialcyber.co/reports/enisa-2025-threat-landscape-report-highlights-eu-faces-escalating-hacktivist-attacks-and-state-aligned-cyber-threats/ [Accessed 30 Jan. 2026].
7. Tietoevry Banking. (2025). Payment Fraud Report 2025. [online] Available at: https://www.tietoevry.com/en/newsroom/all-news-and-releases/press-releases/2025/04/tietoevry-bankings-new-insight-report-reveals-an-increase-in-digital-payment-fraud-in-europe/ [Accessed 30 Jan. 2026].
8. Check Point Research. (2025). LockBit Returns — LockBit 5.0. [online] Available at: https://blog.checkpoint.com/research/lockbit-returns-and-it-already-has-victims/ [Accessed 30 Jan. 2026].
9. TicTac Cyber Security / PRWeb. (2025). Europe's Ransomware Attacks Set a 2025 Record. [online] Available at: https://www.prweb.com/releases/new-research-confirms-europes-ransomware-attacks-set-a-2025-record-302547621.html [Accessed 30 Jan. 2026].

10. brhade, R. (2026). Warning over scams targeting Manx.net email accounts. *BBC News*. [online] Available at: https://www.bbc.co.uk/news/articles/c70lwye131ro [Accessed 10 Jan 2026].
11. Microsoft.com. (2026). *Security Update Guide - Microsoft Security Response Center*. [online] Available at: https://msrc.microsoft.com/update-guide/vulnerability/ CVE-2026-21265 [Accessed 16 Jan. 2026].

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

Website

LinkedIn

Enquiry