Global Threat Intelligence Report

Featuring Regulatory Insights

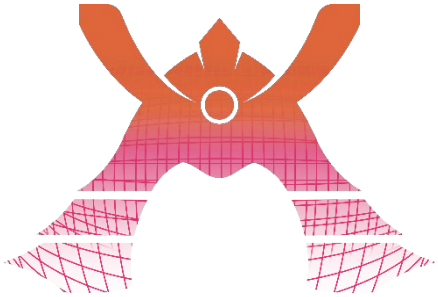
Volume 11 - March 2026

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

Odido suffers cyber-attack [1]

Odido the largest telecommunications provider in the Netherlands has been the victim of a cyber-attack, a data breach to be specific. The criminals were able to access the customer data including personal data of 6.2 million people. Odido reported that the incident occurred on the weekend of February 7th 2026 and that no passwords, call logs or billing information were affected. However, identification data such as passports and driver's license details may be included in the data exfiltrated.

French National Bank Account Registry Breach [2]

On February 18th 2026, an official press release from the French government disclosed another cyber incident amid the ongoing wave of attacks targeting French institutions. The statement confirmed that, beginning in late January 2026, one of the country's most critical financial surveillance systems had sensitive data stolen. According to the release, stolen credentials were used to access data on 1.2 million accounts, including personal information and, in some cases, tax-related details. The government reported that work is underway to restore the service under the best possible conditions and that users concerned will be contacted and informed that access to their data has occurred.

Threat Insights

Anatomy of a Breach

How does a data breach occur?

In films, we often see a hacker typing furiously on a keyboard while staring at a screen filled with incomprehensible symbols. After a dramatic pause, they hit the enter key and utter the iconic Hollywood line: “I’m in.” With that simple montage, the criminal or anti-hero instantly gains full access to a protected system and all the data within it.

In reality, data breaches are rarely so cinematic. In fact, they are often disappointingly mundane. A breach can begin with something as simple as a phone call to an office, where an attacker pretends to be from the IT department and politely asks for login credentials. Social engineering, not flashy hacking, is frequently the entry point.

Given the surge in recent data breaches, it is worth exploring some of the primary methods threat actors use to compromise systems:

1. Phishing and Social Engineering

Most breaches involve some form of phishing. Attackers trick individuals with legitimate access into revealing credentials or granting system access. A lack of multi-factor authentication (MFA) can make this even easier, but even when MFA is present, well-executed social engineering can bypass it. Once an attacker establishes trust, they can simply persuade the target to provide the one-time code or token. Interestingly, according to the latest M-Trends report from Mandiant, phishing may be declining as an initial access vector but still remains one of the most effective initial access vectors and cannot be underestimated.[3]

2. Exploiting Vulnerabilities and Misconfigurations

Unpatched vulnerabilities, weak configurations, and default credentials often provide adversaries with easy access to sensitive systems. Attackers

exploit these weaknesses to escalate privileges, execute malicious scripts, or exfiltrate data.

3. Credential Theft and the Purchase of Stolen Credentials

Threat actors may steal credentials using malware such as infostealers or purchase them on underground markets. With valid credentials in hand, attackers can often walk straight into systems without needing to exploit technical vulnerabilities. The latest report from Googles Mandiant shows Credential theft as an initial access method rose significantly, from 10% to 16% between 2023 and 2024.[3]

4. Third-Party and Supply Chain Attacks

Attackers may breach a vendor, partner, or service provider to gain indirect access to a target organisation. This method is often more technical and resource-intensive than phishing or credential theft, but its effectiveness continues to grow as organisations become more interconnected.

5. Insider Threats

Although less frequent than external attacks, insider threats whether through malicious intent or unintentional negligence can be highly damaging. Because insiders already have legitimate access, their actions may go unnoticed until it is too late. Insider threats accounted for around 5% of initial access cases but remain disproportionately impactful.[3]

Conclusion

AI has been used by attackers to reinforce their efforts, but it does not appear to take centre stage in recent data breaches. The methods above may be refined or aided with AI but ultimately these tactics have been around for a long time and have remained effective.

The methods used by threat actors to cause data breaches are not always sophisticated. Social engineering, negligence, and weak security practices often provide easier paths than technical exploits. Ultimately, a system is only as secure as the people who use and manage it. Attackers understand this and they will continue leveraging human error as one of their most reliable tools.

Regulatory Insights

The Post-Quantum Shift: Aligning Regulatory Compliance with Next-Gen Infrastructure

The era of theoretical quantum threats has officially ended. In early 2026, the global cybersecurity landscape shifted from "wait-and-see" to active transition. With the formal rollout of the NIST Post-Quantum Cryptography (PQC) standards [4] and the introduction of the EU's 2026 Cybersecurity Package [5], organisations are no longer just fighting hackers; they are contending with the obsolescence of the classical mathematical foundations that have secured our digital world for decades. This article examines the immediate regulatory pressures in the EU and UK, the "Harvest Now, Decrypt Later" (HNDL) phenomenon, and how some major infrastructure vendors are currently offering quantum-resistant solutions. Finally, we provide a strategic roadmap for CISOs to transition from legacy RSA/ECC architectures to a quantum-safe posture before the 2030 "Z-Day" deadline.

The Quantum Threat: Beyond the Hype

Encryption is widely recognised as the most effective way to keep data secret. CISA [6] identifies two vital encryption functions that are at the basis of all cryptographic operations: key establishment that enables securing communication, and digital signatures that provides authenticity, integrity and non-repudiation. These functions currently work on the assumption that some mathematical problems are unsolvable, but this will no longer be true when **Cryptographically Relevant Quantum Computing** (CRQC) [7] will become available. CRQC represents a stable, fault-tolerant quantum system capable of breaking the large integer factorisation and discrete logarithm problems that underpin modern public-key cryptography.

While a full-scale CRQC may still be a few years away, the threat is already active through **"Harvest Now, Decrypt Later" (HNDL)** attacks. State-sponsored actors and sophisticated cyber-syndicates are currently intercepting and storing encrypted communications with the intent to decrypt them once quantum advantage is achieved. If your data's "secrecy life" exceeds the time it takes to develop a quantum computer, that data is already vulnerable.

How to Quantify Risk: The Mosca's Theorem

To measure the level of risk, the ETSI guide [8], already in 2016, introduced the simple but chilling formula:

$$X + Y > Z$$

Where:

- **X**: is the number of years your data must remain secret (e.g., a patient's medical record or a 15-year trade secret).
- **Y**: is the time (in years) required to migrate your systems to PQC (industry average is currently 7–10 years).
- **Z:** The time (in years) until a CRQC is available.

If the time you need to protect data plus the time you need to migrate exceeds the threat timeline, your security has already failed. Most experts, including the G7 Cyber Expert Group (CEG) [9] warn that this "quantum advantage" could emerge within a decade.

If your data must be secret for 15 years (X) and your migration takes 10 years (Y), but a CRQC arrives in 12 years (Z), your data stolen today may be decrypted while it is still supposed to be a secret. The imperative? Protect your data flows with a Post-Quantum Cryptography algorithm.

What Industries are Most Affected?

Post-Quantum Cryptography is a universal necessity, but the urgency varies by the "shelf life" of the data handled. While Financial Institutions are the most heavily regulated in 2026, other sectors face equal or greater risk:

- **Healthcare and Pharmaceuticals:** Genomic data and drug R&D are "forever secrets." If stolen today, they can be exploited decades from now.
- **National Security:** Classified intelligence and diplomatic communications intercepted today could remain sensitive well into the 2050s.
- **Critical Infrastructure:** Systems with long lifecycles, such as energy grids or telecommunications backbones, often contain "cryptographic antipatterns" [10] - hard-coded legacy keys that cannot be easily updated.

Short-lived data, like one-time passwords, is at lower risk. The "Extreme Risk" category is reserved for **Long-lived Data**, such as legal contracts, trade secrets, and identity data.

The 2026 Regulatory Surge: EU and UK Perspectives

As of March 2026, PQC has transitioned from a best-practice recommendation to a looming regulatory obligation.

On January 20, 2026, the European Commission announced a comprehensive **Cybersecurity Strategy package**. This includes proposed amendments to the **NIS2 Directive** that would require Member States to adopt PQC migration policies as part of their national strategies.

While the **EU Quantum Act** is currently a proposal scheduled for formal adoption in mid-2026, it has already set clear milestones:

- **End of 2026:** Member States must have national PQC roadmaps in place.
- **By 2030:** Transition of high-risk use cases (finance, health, energy) to PQC.
- **By 2035:** Full system transition across the EU.

Regulators are already leveraging the **"state-of-the-art"** clauses in NIS2 and GDPR to argue that failing to plan for PQC constitutes a failure of risk management, especially for data with a 10-year+ secrecy life.

The UK is moving via individual sectoral mandates driven by the **National Cyber Security Centre (NCSC)**. In February 2026, the NCSC released updated guidance:

- **By 2028:** All organizations must complete a **Cryptographic Discovery** (inventory of all systems using RSA/ECC).
- **By 2031:** Critical National Infrastructure (CNI) must complete PQC upgrades.

The Vendor Response: Offering the Defence

The mid-January to mid-February window saw major vendors move from research to commercialisation of products that support NIST-standardised algorithms (ML-KEM, ML-DSA). Hereafter, we report examples from three leading networking technology vendors:

Palo Alto Networks: On January 30, 2026, Palo Alto launched its Quantum-Safe Security solution. Their most significant innovation is Cipher Translation. This allows their firewalls to act as a "quantum gateway," wrapping legacy applications in PQC-protected tunnels without requiring the internal code of those applications to be rewritten. They have also integrated a Cryptographic Bill of Materials (CBOM) tool to help enterprises find "hidden" vulnerable algorithms.

Fortinet: In early 2026, Fortinet standardised on **ML-KEM-768** (the NIST standard) for IPsec VPNs and TLS 1.3 connections in its latest FortiOS releases. They are championing a **"Hybrid Mode,"** which combines classical encryption with PQC. This ensures that even if a theoretical flaw is found in the new PQC mathematics, the legacy classical layer still provides a fallback.

Cisco: as of February 2026, Cisco has integrated **ML-KEM** into its high-end **IOS XE and XR** branches. In collaboration with major telecommunications providers, Cisco is enabling **Quantum-Secure WAN services**, targeting CNI clients who need to secure long-haul data transport against HNDL threats.

Strategic Recommendations for 2026

Organisations should not wait for formal enforcement to begin the risk management process. To align with the current regulatory surge:

- Conduct Cryptographic Discovery: Map every instance of RSA and ECC. You cannot protect what you cannot see.
- Enforce Data Minimisation: If you don't need the data, delete it. Minimisation is the only 100% quantum-proof defence.
- Adopt Hybridisation: Follow the Europol/NIST [10] recommendation to use hybrid encryption—combining the reliability of the old with the resilience of the new.
- Audit Supply Chains: Review guidance from groups like CMORG [11] and demand CBOMs from your tech vendors during 2026 renewals.

Conclusion

In early 2026 the regulators have spoken: quantum-readiness is a foundational requirement for any entity handling sensitive data. The vendors have updated their portfolios to provide the necessary tools, and the legislative proposals have provided the impetus. For the modern and risk aware enterprise, the question is no longer *if* you will migrate to PQC, but whether you will complete your migration before your legacy encryption becomes a vulnerability. In the race between quantum advancement and cryptographic defence, the time to start was yesterday; the second-best time is now.

Suggestions

Protection, Prevention and Takeaways

1. Human error remains the weakest Link. Whether it's handing over credentials, failing to patch systems, or mishandling sensitive documents, negligence enables many breaches, making people as critical to security as technology. Organisations need to invest in improving security knowledge for staff and not just the technological aspect.

2. Zero-Trust Architecture (ZTA) as a Default Strategy. Adopt a "never trust, always verify" model across the organisation. Zero-Trust ensures that every user, device, and connection is continuously authenticated, authorised, and validated. With credential theft, insider misuse, and lateral movement on the rise, Zero-Trust helps contain breaches before they spread.

3. Continuous Threat Exposure Management. Regular scans catch unpatched vulnerabilities and misconfigurations that attackers often exploit to escalate privileges or exfiltrate data. The key work here is "Continuous", the process should be repetitive and this cycle needs to run in perpetuity. The threat landscape is everchanging and static reactive security is no longer enough. Threat actors evolve quickly, especially with the growth of infostealers, supply-chain exploitation, and AI-enhanced attacks so organisation cannot afford to be oblivious and remain a step behind adversaries.

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-2026-21510 | EUVD-2026-7337 [11]

Vendor	Microsoft
Product	Windows 10/11, Windows Server 2012, 2016, 2019, 2022 Family
Publish Date	Feb 10, 2026
Platform	32-bit and 64-bit editions
CVSS (v3.1)	8.8

Description

Protection mechanism failure in Windows Shell allows an unauthorized attacker to bypass a security feature over a network.

What does this mean for you?

An attacker could bypass Windows SmartScreen and Windows Shell security prompts allowing attacker-controlled content to execute without user warning or consent.

What should you do about it?

Install the security updates released by Microsoft on 10 Feb 2026 for relevant windows versions.

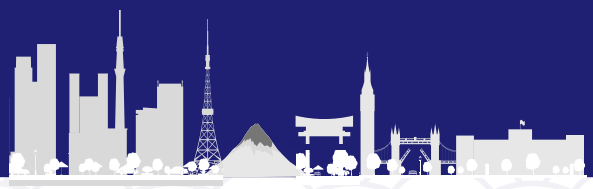
Links & References

1. Abrams, L. (2026). *Odido data breach exposes personal info of 6.2 million customers*. [online] BleepingComputer. Available at: https://www.bleepingcomputer.com/news/security/odido-data-breach-exposes-personal-info-of-62-million-customers/ [Accessed 24 Feb. 2026].
2. MACE, E. (2026). *COMMUNIQUÉ DE PRESSE Paris, le 18 février 2026 N°401 Accès illégitimes au...* [online] Presse - Ministère des Finances. Available at: https://presse.economie.gouv.fr/acces-illegitimes-au-fichier-national-des-comptes-bancaires-ficoba/ [Accessed 24 Feb. 2026].
3. Google Cloud (Mandiant) 2025, M-Trends 2025: Data, Insights, and Recommendations From the Frontlines, Google Cloud Blog, 23 April. Available at: https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2025/ [Accessed: 24 February 2026].
4. National Institute of Standards and Technology (2026) Post-Quantum Cryptography. Available at: https://csrc.nist.gov/projects/post-quantum-cryptography (Accessed: 2 March 2026).
5. European Commission (2026) Cybersecurity Package - Questions & Answers. Available at: https://digital-strategy.ec.europa.eu/en/faqs/cybersecurity-package-questions-answers (Accessed: 2 March 2026).
6. Cybersecurity and Infrastructure Security Agency (2026) Product Categories for Technologies That Use Post-Quantum Cryptography Standards. Available at: https://www.cisa.gov/resources-tools/resources/product-categories-technologies-use-post-quantum-cryptography-standards (Accessed: 2 March 2026).
7. Palo Alto Networks (2026) What is a Cryptographically Relevant Quantum Computer (CRQC)?. Available at: https://www.paloaltonetworks.com/cyberpedia/crqcs-cryptographically-relevant-quantum-computers (Accessed: 2 March 2026).
8. ETSI (2016) ETSI EG 203 310 V1.1.1 (2016-03): CYBER; Quantum-Safe Cryptography (QSC); Quantum Risk Assessment and Assessment of Readiness. Sophia Antipolis: European Telecommunications Standards Institute. Available at: https://www.etsi.org/deliver/etsi_eg/203300_203399/203310/01.01.01_60/eg_203310v010101p.pdf (Accessed: 2 March 2026).
9. G7 Cyber Expert Group (2026) G7 Cyber Expert Group statement on advancing a coordinated roadmap for the transition to post-quantum

cryptography in the financial sector. Available at: https://www.gov.uk/government/publications/advancing-a-coordinated-roadmap-for-the-transition-to-post-quantum-cryptography-in-the-financial-sector/g7-cyber-expert-group-statement-on-advancing-a-coordinated-roadmap-for-the-transition-to-post-quantum-cryptography-in-the-financial-sector-january-20 (Accessed: 2 March 2026).

10. Europol (2024) Prioritising Post-Quantum Cryptography Migration Activities in Financial Services. Available at: https://www.europol.europa.eu/publications-events/publications/prioritising-post-quantum-cryptography-migration-activities-in-financial-services (Accessed: 2 March 2026).
11. Cross Market Operational Resilience Group (2025) Guidance for Post-Quantum Cryptography. April 2025 edn. Available at: https://www.cmorg.org.uk/sites/default/files/2025-06/CMORG%20-%20Guidance%20for%20Post-Quantum%20Cryptography%20-%20April%202025%20-%20TLP%20CLEAR%20(1).pdf (Accessed: 2 March 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