KDDI Europe

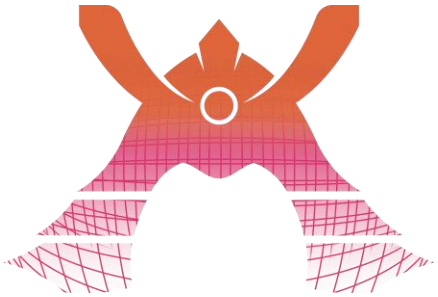
Threat Report

Volume 2

June 2025

Table Of Contents

Introduction



Welcome to the Threat Report. The purpose of this document is to provide an overview of the latest cybersecurity threats and trends 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

EU launches European vulnerability database[1]

The European Vulnerability Database (EUVD) is a database that contains publicly available information on vulnerabilities impacting IT products and services. The site which is currently running in its beta phase is fully operational and for each record, contains an “Alternative ID” which is the CVE ID to make cross referencing easier. The EUVD was established under the NIS2 Directive to enhance Europe’s cybersecurity autonomy.

Harrods hit by cyber attack[2]

Harrods is the latest target of a series of cyber attacks which appears to be aimed at retailers. The luxury department store says it restricted internet access at their sites as a response to mitigate the attack. It’s physical store as well as its online store continue to remain open to the public. They claim their IT security team took proactive steps to keep systems safe, and not much else has been revealed at this stage.

Insights

Threat Actors vs Retailers

In the past few months M&S, Co-op, Harrods, Arla Foods and even DIOR have witnessed cyber attacks against their systems. This begs the questions; What is going on? Why are retailers suddenly being attacked by threat actors?

According to a blog post last year (2024) titled “Rising Cyber Threats Pose Serious Concerns for Financial Stability” from the International Monetary Fund (IMF), the number of cyberattacks have more than doubled since the pandemic and losses since 2017 are estimated to have quadrupled to $2.5 billion in 2024, in the financial sector alone.

Therefore, threat actors are not showing a decline in their activities and retailers may have just been within their sights for the last couple of months. We cannot know why they have chosen now, and we cannot know when they will act again, however we do know how to protect ourselves against these known tactics and techniques.

Security should be considered a forethought; it is not something to be placed at the back of shelf and only brought forward when there is an issue. Most large retail shops have men stationed at the door, CCTV cameras, security tags on products and cash registers that are designed with security features to prevent unauthorized access. Clearly, they are concerned about their physical security and the same level of urgency should be placed on cyber security.

As stated previously, unless it is a zero-day attack, the tactics and techniques used by adversaries are known. The tools to combat them are also available, therefore we MUST be prepared and know what to expect.

Suggestions

Protection, Prevention and Takeaways

1. While the EUVD is tailored to enhance cybersecurity within the EU regulatory framework, the CVE system serves as a global standard for identifying and naming vulnerabilities. Both initiatives share common goals of improving vulnerability management and fostering collaboration, but they differ in their regulatory context, target audience, and specific focus areas. Organizations can benefit from understanding both frameworks to enhance their cybersecurity strategies effectively.

2. “What is important to my business?” is a good question to ask when thinking about security. Looking at the parts of the business that are crucial, and then formulating a plan to protect them from threat actors is an oversimplification of the actual process. However, this captures the essence of what it means to be proactive. In security, a proactive approach is always the best option. Acting after the damage has already occurred will be a bitter lesson that businesses should not have to learn.

3. Frequent security awareness training is important. Staff are less likely for fall for phishing emails or other deceptive tactics used by adversaries if they can recognize them. Since people are generally bound to forget the information they do not use regularly, there is a need to keep refreshing their memories so that identification of threat actors and their tactics becomes easier.

Common Vulnerabilities and Exposures (CVE)

Every month a CVE is selected at the discretion of the reports author discussed. This month it is a vulnerability affecting one of the most popular web browsers in the world.

CVE-2025-32705

Vendor : Microsoft

Product : Outlook

Published : 13 May 2025

Platform : Windows

Description

Out-of-bounds read in Microsoft Office Outlook allows an unauthorised attacker to execute code locally.

What does this mean for you ?

It means if a user opens a specifically crafted file with an affected version of the Microsoft Outlook software, an attacker can exploit this vulnerability.

What should you do about it ?

Be sure to install the Microsoft May 2025 Security Updates which include the necessary fixes for this vulnerability.

Links & References

1. https://digital-strategy.ec.europa.eu/en/news/eu-launches-european-vulnerability-database-boost-its-digital-security
2. https://www.bbc.co.uk/news/articles/c62x4zxe418o
3. https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability
4. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32705

Contact Us

KDDI Europe is a growing ICT solution provider based in London and a subsidiary of KDDI Corporation. It is the regional headquarters of EMEA and CIS regions offering a host of ICT services as a 'One-Stop' solution, including cloud computing, data centre, IT consulting, IT outsourcing, network, security, system integration and voice services.

The excellent reputation and trust enjoyed by our Telehouse data centres positioned around the world have kept us at the forefront of service and quality

Contact Information

Telephone Number	+44 20 7507 0001
Email Address	info@uk.kddi.eu
LinkedIn	https://linkedin.com/company/kddi-europe-limited

Website

LinkedIn