KDDI Europe

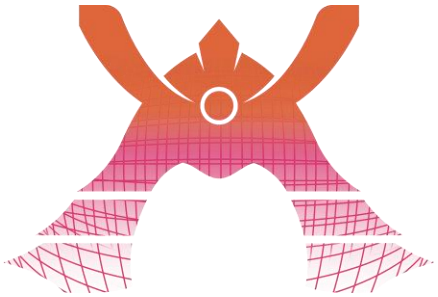
Threat Report

Volume 1

May 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

M&S Cyber Incident[1]

Marks & Spencer (M&S), a leading British retailer was affected by a cyber incident in the later part of April 2025 that impacted some of its services including their “Click and Collect” service. As part of the mitigation process, they stopped processing contactless payments. The incident also resulted in a pause from taking orders via their website and apps although their product range remained available to browse online.

WooCommerce Users Targeted by Phishing Attack [2]

A large-scale phishing campaign was launched by attackers to urge WooCommerce users to download a fake “critical patch”. This fake patch is actually a means to create a backdoor to the users' environment instead. This would allow the attackers to remote control the affected websites and use it for further malicious acts. The attackers made use of a typo-squatted URL similar to the WooCommerce address that had a "ė" in place of "e“ in an attempt to add legitimacy to the website that hosted the malicious file users were urged to download.

Insights

The Threat Of AI (Artificial Intelligence)

AI is everywhere, and most people have tried using it at some point. It is undoubtedly an effective tool that can reduce the effort and time spent performing tasks or searching for information. The field of cybersecurity is no exception to the adoption of Artificial Intelligence. Almost every major player in the Detection and Response business is attempting to or reportedly using AI to detect malicious or suspicious activity. Being able to notice patterns and make observations based on mountains of telemetry in a fraction of the time it would take an engineer to do the same is a welcome addition to the arsenal of protection tools.

Unfortunately, it is also being used by threat actors as a tool to exploit and deceive. AI allows threat actors to:

- Draft more convincing phishing emails.
- Generate fake images, videos, and voices meant to deceive.
- Assist them in writing harmful scripts and programs. For example, they could generate a fake but very convincing website to lure victims.

These are just a few possibilities. The ability to generate a voice that mimics someone in an influential position or even a video using the likeness of a CEO is truly frightful. The good news is that security professionals are aware of these tactics and are tirelessly working to produce solutions and improve existing ones. The unending tenacity of security vendors provides hope that threat actors will never go unchallenged.

Suggestions

Protection, Prevention and Takeaways

1. It is key to always remain vigilant. Smaller and medium sized businesses often believe they are too small of a target for threat actors, they believe they are not worth the effort, and no-one is going to bother attempting to compromise their systems. However, if larger organisations can be compromised then image the ease with which a smaller organisation lacking in the security would be attacked by threat actors. Security should never be an afterthought.

2. Artificial intelligence (AI) is here to stay whether or not we may not be entirely onboard. It has the potential to drastically improve productivity and ease some of the burden both employers and employees are under with respect to workload. Unfortunately threat actors also see the potential in how it can support their malicious activities and attacks. People should be aware of this, and it keep it at the back of their minds when interacting with content online. Take a second to question the credibility of new content you come across on the internet and apply a little bit of critical thinking before clicking links.

3. Updating and Patching systems may not be exciting, but they are one of the first steps that can be taken in securing IT infrastructure. Managing vulnerabilities will shut a door in the face in of threat actors who are constantly looking for ways to penetrate to compromise a system. Consider this analogy; you wouldn't keep using a lock if you know there was a screw that could be undone which would allow the lock to be opened without a key or passcode would you ?

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-2025-3070

Vendor : Google

Product : Chrome Browser

Published : 02 April 2025

Platform : Windows, Mac & Linux

Description

Insufficient validation of untrusted input in Extensions in Google Chrome prior to 135.0.7049.52 allowed a remote attacker to perform privilege escalation via a crafted HTML page.

What does this mean for you ?

It means if you downloaded an untrusted extension for your chrome browser which received some sort of input or data that was validated incorrectly, then this could allow privilege escalation.

What should you do about it ?

Upgrade to Chrome 135.0.7049.52 or higher for Linux and 135.0.7049.41/42 or higher for Windows and Mac.

Links & References

1. https://www.bbc.co.uk/news/articles/c9djvzwn858o.amp
2. https://thehackernews.com/2025/04/woocommerce-users-targeted-by-fake.html
3. Microsoft CVE - https://www.cvedetails.com/cve/CVE-2025-3070/

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