TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Cyber weather

August 2025

Cyber weather, August 2025

Data breaches and leaks

- The number of data breaches more than tripled after the calm of July. Case numbers have typically increased in early autumn as employees return to workplaces.
- In several incidents, the breaches were still triggered by successful M365 phishing campaigns, where a malicious link arrived from a familiar sender.
- Teams calls also became more common as a root cause of breaches in August.

Scams and phishing

- SMS scams carried out in the name of child protection have generated significant criminal proceeds. In August, losses suffered by citizens and organisations reached hundreds of thousands of euros.
- In addition to email, SMS and phone calls, criminals are now also using Microsoft Teams calls for their scams. Fraudsters posing as IT support attempt to persuade victims to install remote management software on their devices.

Malware and vulnerabilities

- A critical vulnerability in Citrix NetScaler ADC and NetScaler Gateway products is being actively exploited.
- Both in Finland and internationally, malware disguised as a PDF editor has been detected. When downloading software, it is important to verify the reliability of both the programme and the website.
- Globally, the first case of AI-based ransomware has been reported. The malware can generate malicious code on an infected device using artificial intelligence, making it harder to identify and detect.

Automation and IoT

- In Poland, a poorly protected remote management system of a small hydroelectric dam was misused. In Ukraine, openly visible internet-connected cameras and unpatched IoT devices were likewise exposed to abuse.
- These cases serve as a reminder of the importance of basic security measures for IoT and automation systems.

Network performance

- Denial-of-service attacks did not cause significant impact on Finnish online services.
- Globally, however, record-breaking attacks continue to be reported.

Spying

- Authorities in several countries issued warnings about cyber espionage carried out by a China-linked APT group, targeting among others telecommunications operators and internet service providers.
- The group has been publicly referred to by names such as Salt Typhoon, Operator Panda and Ghost Emperor.
- The Finnish Security Intelligence Service (Supo) also took part in the publication.

NCSC-FI’s tips and recommendations for improving cyber security preparedness:

In August, an application round for funding support to implement the Finnish Cybersecurity Act was opened. The Finnish Transport and Communications Agency Traficom may grant funding to micro, small and medium-sized organisations within the scope of the Act, in order to meet the requirements set out in the Act and to raise the level of cyber security within the organisations. The application period is open until 16 October 2025 at 16.15.

Traficom, together with the Finnish Security Intelligence Service (Supo), published a statement on Finland’s cyber security threat level. The threat level rose with the outbreak of the war in Ukraine in 2022 and has remained elevated since. The number of serious cases investigated by the NCSC-FI has more than doubled compared to last year.

The EU’s cyber security requirements for radio equipment became applicable at the beginning of August. The regulatory framework covers devices that use radio frequencies, such as mobile phones, smartwatches and baby monitors. The new rules will enhance consumer security, as only radio equipment meeting the cyber security requirements may be placed on the EU market in future.

Overview of cyber security in August

August marked the end of the calm summer season. The return from summer holidays and back to workplaces was reflected in a clear rise in case numbers, as well as in the volume of reports received by the NCSC-FI.

- Key phenomena in August included vulnerabilities and data breaches, which also featured prominently in international cyber security reporting. The global SharePoint vulnerability that caused concern in July and August also raised worries in Finland, though the number of successful exploitation cases has remained relatively limited. Cyberattacks against dams in Norway and Poland highlight the importance of considering security aspects and protecting vulnerable systems — regardless of sector or target.

The total number of data breach reports received in August reached this year's peak. Owing to several successful breaches, a high number of phishing detections and attempted breaches can also be expected in September.

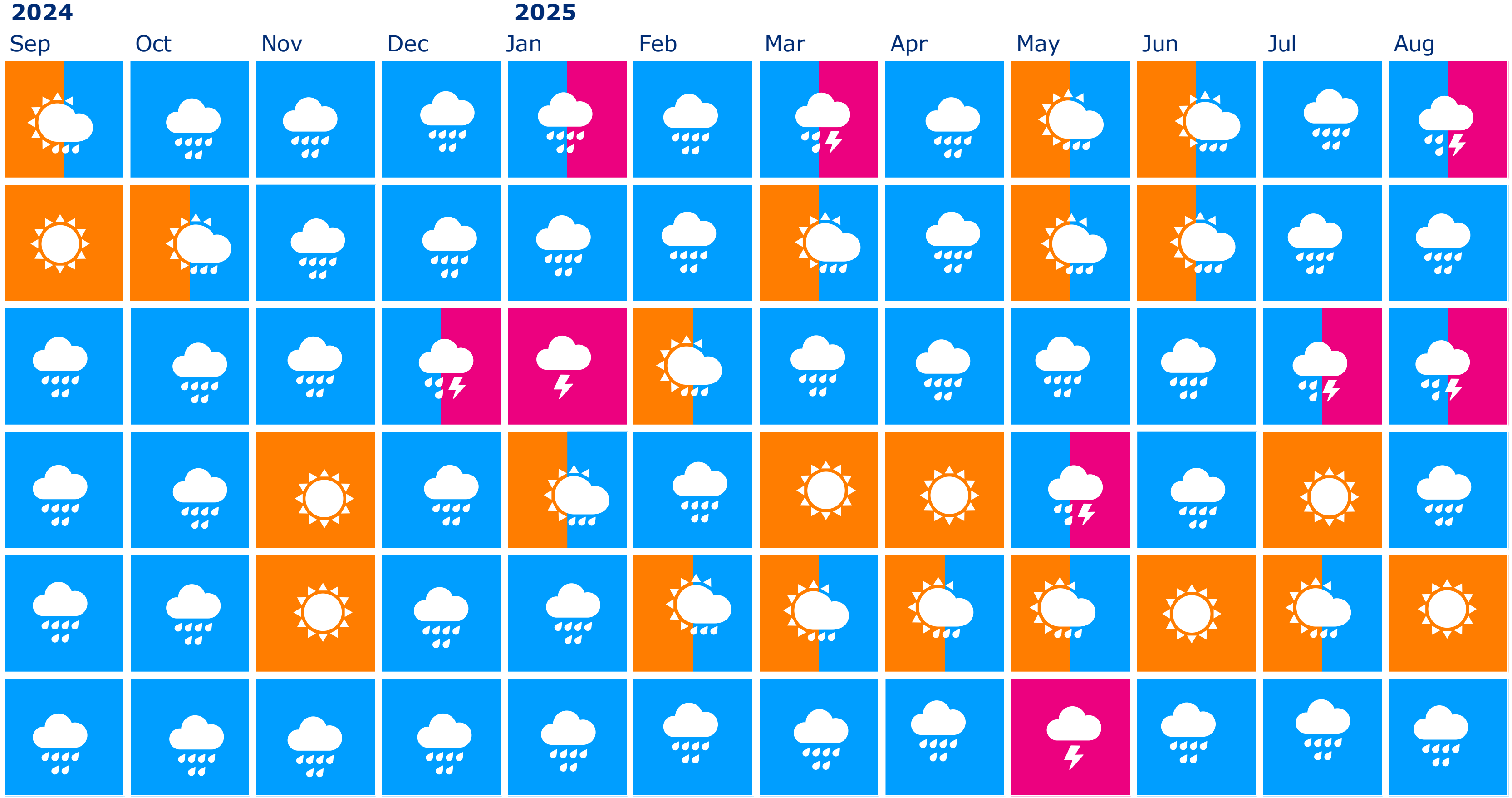
- In some of the data breach cases observed in Finland, an Adversary-in-the-Middle (AiTM) technique has been used to bypass multi-factor authentication. During account takeover, for example, the attacker may create a mail rule that moves incoming messages to the Deleted or Archive folder and marks them as read. By using redirect and forwarding rules, the criminal attempts to hide notifications and prompts about follow-up messages sent from the account.

Phishing has remained a significant threat throughout the summer season. August was no exception to this trend, with particular growth observed in phishing targeting Microsoft 365 credentials. However, the overall number of phishing reports appears to have levelled off from the steep upward trend seen earlier in the summer.

- The NCSC-FI received several reports of phishing cases where the message appeared to come from a familiar source. The subject line of the phishing email often refers to a shared file. The link in the message often points to a document shared from the organisation's Online SharePoint or OneDrive service. However, the actual phishing link is embedded within the shared document, redirecting the victim to a site designed to steal Microsoft 365 credentials.
- With the holiday season over, it is important to remind staff of the dangers of phishing. At the start of autumn, it is advisable to review common rules and different ways to identify potential phishing messages and scams. Checking links and web addresses, for example, is a simple but essential skill for avoiding many threats. The NCSC-FI has also published guidance on identifying AiTM phishing.

1 kk

Cyber security trends
in the past 12 months



	2024 Sep	Oct	Nov	Dec	2025 Jan	Feb	Mar	Apr	May	Jun	Jul	Aug
Data breaches and leaks	🌦	🌧	🌧	🌧	🌧	🌧	⛈	🌧	🌦	🌦	🌧	⛈
Scams and phishing	☀	🌦	🌧	🌧	🌧	🌧	🌦	🌧	🌦	🌦	🌧	🌧
Malware and vulnerabilities	🌧	🌧	🌧	⛈	🌩	🌦	🌧	🌧	🌧	🌧	⛈	⛈
Automation and IoT	🌧	🌧	☀	🌧	🌦	🌧	☀	☀	⛈	🌧	☀	🌧
Network performance	🌧	🌧	☀	🌧	🌧	🌦	🌦	🌦	🌦	☀	🌦	☀
Spying	🌧	🌧	🌧	🌧	🌧	🌧	🌧	🌧	🌩	🌧	🌧	🌧