TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Cyber Weather

December 2025

Changes to Cyber Weather reports in 2026

The layout and content of Cyber Weather reports will be updated starting with the January 2026 edition. The changes aim to make the publication more accessible, more consistent in quality, and at the same time more informative.

Customer feedback was taken into account during the development work, and we have retained the best elements of Cyber Weather. In addition, new content and a stronger focus on anticipation will be introduced.

Going forward, more extensive analysis slides, such as the Top 5 threats, will be published as part of the March and September reports.

Cyber Weather, December 2025

Data breaches and leaks

- December was calm in terms of data breaches and data leaks. Compared with November, nearly 30% fewer reports were received.
- Exploitation of vulnerabilities in Cisco products and in React Server Components was observed in the data breach cases.

Scams and phishing

- During the holiday season, extensive phishing targeted accommodation providers and their customers. Criminals seek to obtain access credentials to accommodation services and use them to harvest payment card details.
- Instant messaging accounts have been compromised more than before. Attackers employ repeated login attempts or try to create a new account using the victim's phone number. Verification messages should not be approved nor links in them opened. Personal accounts should be protected with multi-factor authentication.

Malware and vulnerabilities

- A critical vulnerability was identified in React Server Components (CVE-2025-55182).
- A vulnerability was discovered in the TOTOLINK X5000R home router, which under certain conditions allows the device to be taken over. No patch is available for the vulnerability (CVE-2025-13184).
- A critical vulnerability was also identified in Cisco Secure Email Gateway and Secure Email and Web Manager products (CVE-2025-20393).

Automation and IoT

- Based on our observations, remote management connections for OT systems have been implemented insecurely in Finland. This is due, among other things, to default configurations in edge devices used for remote access, which are unsuitable for OT environments as they allow unrestricted traffic to and from the internet.

Network performance

- During Christmas week, the pro-Russian NoName launched again denial-of-service attacks against Finnish targets. There were no significant impacts, but combating the attacks required additional work.
- The US Department of Justice has charged an individual linked to the NoName group. According to the indictment, NoName is reported to have received financial support from the Russian government.
- In late December, subsea cable damage in the Baltic Sea and Storm Hannes caused several service disruptions.

Spying

- According to the United States, Russia is behind the hacktivist groups Cyber Army of Russia Reborn (CARR) / Z-Pentest and NoName057(16), which have carried out cyberattacks and disruption activities in Western countries. Several other countries joined the public statement. CARR/Z-Pentest is linked to Russia's GRU.
- Denmark and Germany have also publicly accused Russia of cyberattacks. Denmark was targeted by denial-of-service attacks and an attack against a water utility. In Germany, attacks targeted air traffic control systems, and attempts were made to interfere with elections.

NCSC-FI's tips and recommendations for improving cybersecurity preparedness:

The Finnish Transport and Communications Agency Traficom has updated its regulation on critical parts of communications networks. The revised regulation extends the scope of the requirements, in certain respects, to also cover 5G base stations.

Managing administrator accounts is a key element of cloud service security. In the Information Security Now! article on best practices in the management of cloud service administrator accounts (available in Finnish), we review the three most common cloud services — Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP) — and explain how their administrator accounts should be secured and maintained.

After the festive season, many households may have new routers and other network devices whose settings should be reviewed to improve security. You can find guidance on router settings and secure connections in our guide *"Home network and router security."*

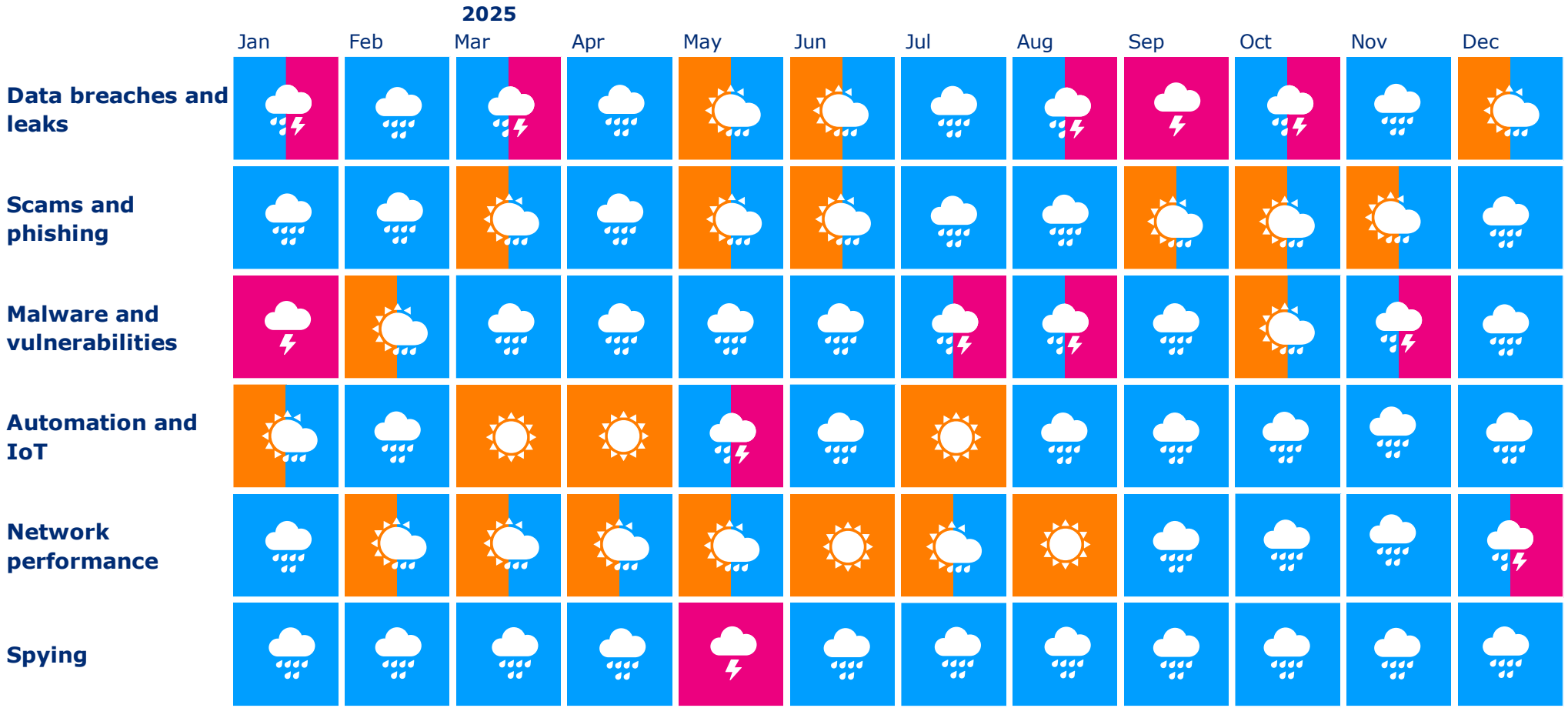
Overview of cybersecurity in December

December began relatively calmly from a cybersecurity perspective, although conditions deteriorated slightly towards the end of the month.

- At the beginning of the month, several reports were received concerning fake profiles created on the Topline.com website, in connection with suspected identity theft. A significant amount of data from LinkedIn user profiles had been copied to the site.
- A moderate number of critical vulnerabilities were reported. Among these, vulnerabilities affecting Cisco's email security products and the React Server Components vulnerability CVE-2025-55182 — known as React2Shell — stood out in the early part of the month. On New Year's Eve, another incident involving damage to a data transmission cable between Finland and Estonia was observed. As a result, a multi-authority operation was carried out targeting the vessel Fitburg, which is suspected of having damaged Elisa's cable with its anchor. However, the incident did not cause significant impacts on data transmission.
- Somewhat unexpectedly, one of the most notable events towards the end of the year was Storm Hannes, which caused power outages across the country. According to the Finnish Meteorological Institute, the storm was among the most severe in decades, leaving up to 180,000 customers without electricity simultaneously.
  - Severe natural phenomena, along with the outages and physical damage they caused, had significant indirect effects on data transmission.

Cybersecurity trends
in the past 12 months

1 kk



Long-term cyber weather: Cybersecurity of industrial automation

Industrial automation is closely associated with OT (Operational Technology) systems, which refer to devices, systems and software used for the real-time control and monitoring of physical production processes. Disruptions to these systems can, in the worst case, lead to serious and wide-ranging incidents that endanger the functioning of society. Based on recent observations, the three most serious cyber threats targeting OT systems are hacktivism, espionage and sabotage:

- The aim of hacktivists is to disrupt targets and to exploit collected data for information influence operations.
- Espionage may be conducted to gain a competitive advantage or to support political intelligence gathering.
- The motivation for sabotage may be financial gain or state-driven influence.

The operating environments of sectors using industrial automation are changing at an accelerating pace. Digitalisation, the use of artificial intelligence and IT/OT convergence are increasing, and automation systems, remote management, monitoring and the required data are becoming increasingly dispersed from traditional plant environments to a growing number of locations. There is a risk that industrial automation environments fail to keep pace with developments in cybersecurity and that resources remain insufficient compared with those available in the IT domain.

As the volume of data grows, along with the need for secure and resilient connections, the length and complexity of supply chains, the complexity of environments and the expansion of the attack surface, preparedness faces new kinds of challenges.

- At the same time, increasing emphasis is being placed on preparedness and the security of production environments. Regulation and requirements are expanding, new standards are being introduced, and cybersecurity aspects are considered in the standards from the outset.
- The EU's Cyber Resilience Act (CRA) requires manufacturers to produce a software bill of materials (SBOM) for their products, the use of which has been promoted internationally. This will, among other things, facilitate vulnerability management.

The NCSC-FI cooperates with stakeholders in the field of industrial automation through domestic and international networks, provides guidance and support in incident situations, and maps unsecured automation systems, login interfaces and management panels exposed to the internet.