TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

March 2026

Cyber weather

Cyber weather gives you an update on the key information security incidents and phenomena of the month.

The product is primarily targeted at those who work with information security issues at different levels of organisations. Cyber weather gives readers a quick overview of recent and upcoming events in the field of cybersecurity.

Cyber weather can be:

 calm

 worrying

 serious

Overview of cyber weather in March 2026

Cyber weather remained rainy

Rain clouds gathered over the spring cyber landscape due to several supply chain attacks carried out through software components. The threat actor TeamPCP conducted these attacks via open-source software, including Trivy, Kicks and the Python package LibLLM.

The wave of Microsoft 365 account breaches appears to have eased compared to the previous month.

In March, we published three vulnerability bulletins on critical vulnerabilities.

Unusually few ransomware cases have been reported to the NCSC-FI so far this year. However, ransomware activity continues to increase internationally, meaning the situation in Finland may also change rapidly.

Glimmers of light amid the rain came from the participation of the NCSC-FI and the Finnish Security and Intelligence Service in an international operation countering cyber espionage conducted by Russia's military intelligence service (GRU). The operation disrupted the use of a global cyber espionage network formed from compromised TP-Link routers.

The GRU had used vulnerable routers, among other things, to spy on users by altering the devices' DNS settings. This enabled adversary-in-the-middle attacks (AiTM) and the decryption of encrypted network traffic.

NCSC-FI’s tips and recommendations for improving cybersecurity preparedness

The NCSC-FI published situation cards to help organisations communicate about cyber incidents. The cards provide an overview of different types of incidents and practical support for related communications.

We invite organisations to participate in the free Vartijatonttu pilot project, which assesses the ability of Finnish companies to detect and respond to current cybersecurity threats. Participants receive benchmarking data on their cyber maturity, an analysis on real threat scenarios and concrete recommendations for improvement.

The NCSC-FI’s new guide, *Managing software security – roles and competence needs* (available in Finnish only), supports the systematic management of software security throughout the software lifecycle. This helps ensure the continuity and resilience of organisations and society as a whole in the digital environment.

A webinar series titled Critical code, aimed particularly at software developers, will begin on 17 April. Organised by the NCSC-FI, the series addresses software security from a practical perspective, focusing on how to develop better and more secure code. The webinars will be held in Finnish.

Hail shower of the month
Instant messaging accounts targeted by takeover attempts

During the early part of the year, the NCSC-FI has received numerous reports of incidents involving instant messaging accounts. Targets have included Telegram, WhatsApp and Signal accounts.

A wide range of incidents has been reported. In some cases, accounts have been created using phone numbers belonging to another person or numbers that are no longer in use. Account takeovers and unauthorised use have been carried out, for example, using account linking features that allow the same account to be used on another device. Attackers attempt to obtain the linking code through phishing.

Instant messaging accounts can be protected by enabling multi-factor authentication and ensuring that no unknown devices are connected to the account. Default PIN codes for voicemail services should also be changed. Organisations should provide guidance to employees on the use of instant messaging applications in a work context.

Internationally reported campaigns demonstrate that account takeovers in instant messaging services can lead to serious incidents.

International observations on instant messaging incidents

- In Germany, authorities warned of phishing attacks conducted via instant messaging applications, particularly Signal, likely carried out by a state actor. The targets included high-ranking politicians, government officials, members of the armed forces and journalists.
- Authorities in the Netherlands published information about a global campaign in which cyber threat actors linked to the Russian state sought to compromise the Signal and WhatsApp accounts of high-profile individuals.
- In Italy, a Signal-based campaign has attempted to obtain individuals' personal data through social engineering techniques.

Cyber weather phenomena

In this section,
we review developments and trends
in key cybersecurity phenomena.

Cyber weather
March 2026

1 mo.

Data breaches and leaks

March was relatively steady in terms of data breaches. However, some more significant breaches and data leaks occurred during the month. The attacks were mainly carried out by exploiting vulnerabilities.

Malware

In March, supply chain attacks targeting open-source software by a threat actor had widespread impact both nationally and internationally.

Vulnerabilities

A high number of vulnerabilities continued to be reported during the month. Their impact in Finland remained fairly limited.

Scams and phishing

In March, a large number of tax-themed scam messages were observed, related to tax refunds, tax decisions and back taxes.

Information is being gathered from companies via WhatsApp group chats for use in invoice fraud schemes.

Automation and IoT

The United States banned the import of consumer routers manufactured abroad, citing national security concerns.

Network performance

Slightly more denial-of-service attacks were reported in March compared to earlier months of the year, but no significant impacts were observed.

Alongside technical denial-of-service attacks, disruption targeting human interfaces may also be emerging as a growing trend.

Cyber weather
March 2026 1/2

1 mo.

Data breaches and leaks

- In a joint operation by authorities, cyber espionage conducted by Russia's military intelligence service was disrupted. The espionage campaign exploited a vulnerability in TP-Link routers (CVE-2023-50224) to compromise devices. Attackers used compromised, particularly unpatched routers for espionage, for example by redirecting network traffic through their own infrastructure.
- A data breach targeted the systems of Digitalist Experience Oy, involving customer data from Viking Line.
- Reports of Microsoft 365 account breaches submitted to the NCSC-FI were nearly half the number recorded in February.

Malware

- The threat actor TeamPCP successfully carried out a supply chain attack targeting open-source software, including the Trivy security scanner, LiteLLM and Checkmarx. The attacker introduced a backdoor into the software, and malicious versions were widely distributed publicly. The attack led to data breaches around the world.
- More malware incidents than usual were reported to the NCSC-FI during March.

Vulnerabilities

- A critical vulnerability was disclosed in Citrix NetScaler ADC and NetScaler Gateway products (CVE-2026-3055), allowing data in memory to be exposed from affected systems. Immediate patching is recommended.
- A critical vulnerability was also disclosed in the F5 BIG-IP APM access management system (CVE-2025-53521). Organisations are advised to update to a patched version and check their environments for signs of exploitation.
- A critical vulnerability was also identified in the Axios JavaScript package distributed via npm.

Cyber weather
March 2026 2/2

1 mo.

Scams and phishing

- In March, tax-themed scam messages were sent under the pretext of tax refunds, tax decisions or back taxes.
- Payment card details were harvested in scams impersonating rental housing services.
- Internal company information has been collected for invoice fraud schemes via WhatsApp group chats. In one method, a scammer impersonated a company executive by email, asking an employee to create a group chat and share the invitation link in a reply message. This method has not previously been reported to the NCSC-FI.

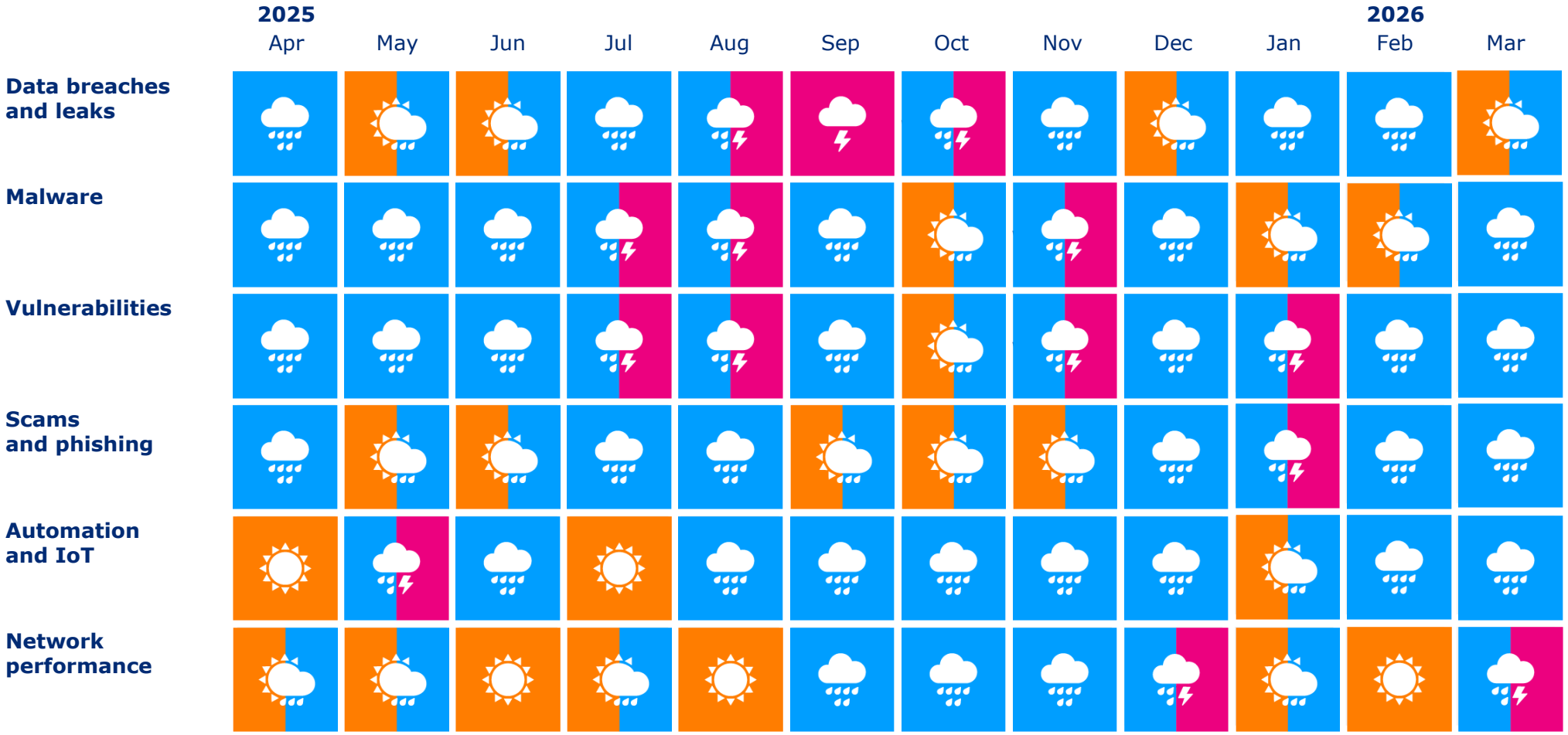
Automation and IoT

- In the United States, foreign-manufactured routers have been assessed as posing risks to households and information networks, including enabling espionage and intellectual property theft.
- The US Federal Communications Commission (FCC) has banned the import, marketing and sale of consumer routers not manufactured in the United States.
- To obtain approval for sale, routers must undergo regulatory assessment, and manufacturers are required to present plans to relocate production to the United States.
- Consumers may continue to use their existing devices.

Network performance

- In March, there was reporting on district courts and administrative courts becoming burdened by material generated using artificial intelligence.
- Generative AI also enables the overloading of various other services, such as customer service functions and official registries.
- The NCSC-FI has received reports of cases where customer service has been congested, for example through mass submission of fabricated oversight or monitoring requests.

Cyber weather
in the past 12 months



Cyber weather forecast

The cyber weather forecast
provides a summary based on previous observations
and an indicative assessment of cyber threats
and their likely developments in the coming months.

Cyber weather forecast
Cyber threats remain at a typical level

Cyber risks related to software dependencies will continue to require attention. The supply chain attack campaigns observed in March are unlikely to be the last, and they highlight the seriousness of the phenomenon.

The rapidly evolving situation in the Middle East may also continue to have unexpected secondary effects on Finland, for example through complex supply chains.

Organisational preparedness

- Awareness-raising and multi-factor authentication (MFA) alone are not sufficient to protect employees against advanced account takeover attempts, such as phishing campaigns using the AiTM technique.
- Organisations should implement advanced security features, including conditional access policies, risk-based authentication and continuous access evaluation.

Worrying

The volume and severity of cyber threats are at a typical level.

However, the threat landscape can change rapidly — including in a negative direction.

The cyber weather forecast provides a summary based on previous observations and an indicative assessment of the cyber threat situation. It should not be used as the sole basis for preparedness – organisation-specific information and analysis must also be considered.

TOP 5 cyber threats in the near future

6–24 mo.

1 Serious vulnerabilities are being exploited faster

In addition to installing an update that fixes the vulnerability, it is often necessary to investigate whether the vulnerability has already been exploited before the patch.

2 The increasing use of AI requires risk management

Organisational preparedness and active risk management measures are essential as the use of artificial intelligence increases rapidly.

3 Information security and continuity of supply and service chains

To ensure cybersecurity, organisations need to understand their own supply chains. Most organisations are more or less dependent on outsourced digital services.

4 Protecting critical infrastructure is essential

The rapidly evolving cyber landscape affects the protection of critical infrastructure.

5 Ransomware is a significant threat to organisations

The number of ransomware incidents continues to increase globally.

● = new threat on the Top 5 list