TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

February 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 cyber security.

Cyber weather can be:

 calm

 worrying

 serious

Overview of cyber weather in February 2026

February remained rainy

Icy drizzle came from several directions: based on reports received by the NCSC-FI, criminals employed multi-channel tactics, including extortion messages, scam calls impersonating banks and authorities, robocalls, high-quality phishing emails, as well as investment and cryptocurrency scams.

Microsoft 365 account breaches continued, and the ability of AiTM attacks to bypass multi-factor authentication highlighted the need for stronger protective measures.

During February, several critical vulnerabilities were reported in widely used software and services. Although these vulnerabilities are technically significant and could, in the worst case, allow systems to be compromised or data to be misused, their national impact has so far remained limited.

Nevertheless, the situation is being closely monitored, as exploitation attempts have been observed in various environments.

Many of the identified vulnerabilities have received high CVSS scores, underlining the importance of timely patching and up-to-date security measures.

Key considerations regarding vulnerabilities

- Organisations are advised to ensure that critical systems are updated, and that logging and monitoring mechanisms are in place to detect potential exploitation attempts.
- It is also important to note that vulnerabilities are often exploited soon after disclosure, making rapid response essential for effective risk management.

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

The NCSC-FI has published guidance pages addressing the threat posed by the development of quantum computers to current encryption methods. The quantum threat particularly concerns data that must remain confidential far into the future, such as personal data, health data, trade secrets and non-disclosable government information.

Browser extensions can enhance functionality, but they also pose significant security risks, as they often have extensive access to browser content. Risks can be reduced by keeping the number of extensions low, removing unnecessary ones and installing new extensions only from official sources, while assessing the trustworthiness of the developer and the permissions requested.

The Digital and Population Data Services Agency has published new guidance on ensuring the impact of exercises and embedding development measures in practice. The guidance emphasises that exercises only deliver value if lessons learned and areas for improvement are documented, analysed and embedded into organisational practices. Organisations should therefore establish a clear process in which feedback, documentation and the follow-up of development measures support continuous improvement in preparedness and cybersecurity.

Icy shower of the month
Cyber dimension in the US–Israel attack on Iran

The United States and Israel launched an attack on Iran on 28 February 2026. In the early days of the operation, cyber activities were observed alongside kinetic strikes.

- Iranian online services and applications were disrupted, while several hacktivist groups launched retaliatory denial-of-service and website disruption campaigns.
- Particular attention was drawn to the hijacking of an Iranian prayer application, where the content was altered to oppose the Iranian government.
- Iran’s national internet connectivity dropped to around four percent of normal levels after the country widely restricted network access.
- Several countries have published assessments of the cybersecurity implications of the situation in Iran.
- According to these assessments, Iran and Iran-linked actors are still considered capable of conducting cyber operations, increasing the risk of indirect cyber threats, particularly for organisations with operations or supply chains in the Middle East.
- No significant cybersecurity impacts related to the situation in Finland.

Cyber weather phenomena

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

Cyber weather
February 2026

1 mo.

Data breaches and leaks

February was significantly more active than January. One significant data breach was observed, involving the exploitation of a zero-day vulnerability.

Reports of Microsoft 365 data breaches were 67% higher than in January.

Malware

In Finland, February remained calm in terms of malware. However, a few cases of malware distribution using the ClickFix technique were reported to the NCSC-FI.

Vulnerabilities

A large number of vulnerabilities were reported during the month. With a few exceptions, their impact in Finland remained largely limited.

Scams and phishing

Scam calls were made in the name of banks and authorities.

Fraudulent invoices were distributed via email.

Automation and IoT

Threat activity targeting automation systems became more serious in 2025.

AI-assisted findings improved the security of a robot vacuum system.

Network performance

Denial-of-service attacks did not cause significant disruptions in Finland.

Botnets used for denial-of-service attacks are also exploited for other types of criminal activity.

Cyber weather
February 2026 1/2

1 mo.

Data breaches and leaks

- A serious data breach targeted Government ICT Centre Valtori's mobile device management system, exploiting a previously unknown zero-day vulnerability in the software.
- Websites were compromised through the exploitation of various vulnerabilities and weak passwords.
- In one case, a company network was breached via a VPN service in a ransomware attack.
- A BEC fraud attempt linked to a Microsoft 365 account breach was detected in time and successfully prevented.

Malware

- The NCSC-FI received reports of a few websites distributing malware using the ClickFix technique.
- Malware has also been observed being spread through phishing emails themed around DocuSign, where users are prompted to click a link that results in malware being installed on their device.

Vulnerabilities

- Critical vulnerabilities were identified in Cisco Catalyst SD-WAN products. Organisations using these products should identify vulnerable devices in their environments, collect sufficient data and snapshots from affected devices, update them to the latest version, and conduct threat hunting for signs of exploitation (CVE-2026-20127 and CVE-2026-20129).
- Exploitation and attempted exploitation of Ivanti EPMM vulnerabilities (CVE-2026-1281 and CVE-2026-1340) were also actively observed in February.

Cyber weather
February 2026 2/2

Scams and phishing

- Callers in scam phone calls have impersonated representatives of banks and authorities.
- Accounts have been created on instant messaging services such as Telegram and WhatsApp using the phone numbers of subscription holders. In several cases, it is suspected that voicemail services associated with the subscription were exploited during registration.
- Fraudulent invoices have been sent by email, with the recipient's bank account number replaced by one controlled by the scammer.

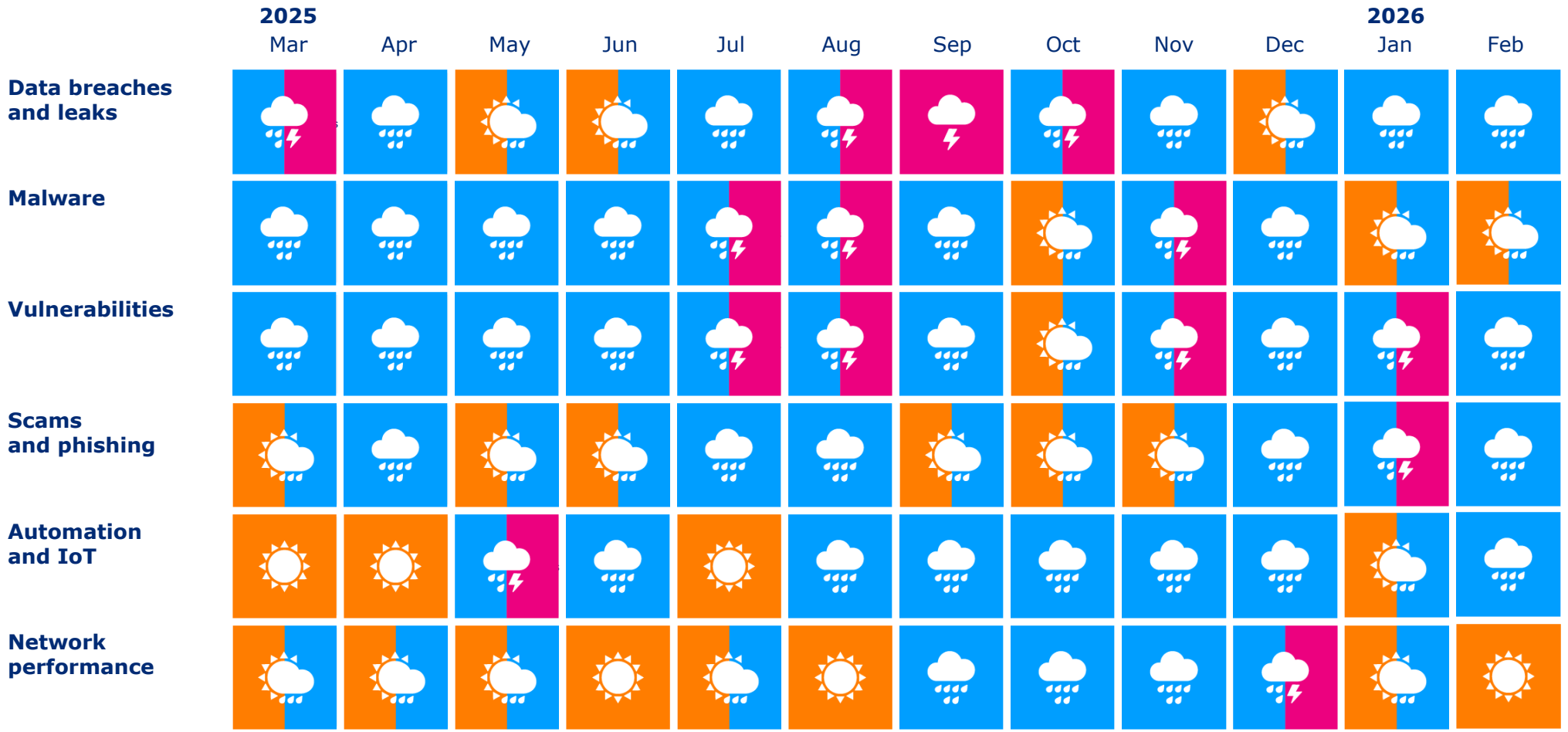
Automation and IoT

- The industrial OT cybersecurity company Dragos published its annual review. Key findings included a shift by some threat actors from gaining initial access to carrying out active disruption, as well as ongoing challenges for system operators in detecting malicious activity.
- Security weaknesses were discovered in a robot vacuum cleaner system, allowing access to 7,000 devices across 24 countries. The case demonstrates how AI tools can be used to identify vulnerabilities. It also highlights the importance of independent security audits, effective vulnerability disclosure channels, and baseline protections required under the Cyber Resilience Act (CRA).

Network performance

- The impact of denial-of-service attacks observed in Finland remained limited to temporary disruptions.
- Malware used to enrol network devices into botnets is also leveraged for other cybercriminal activities, such as advertising fraud and data collection.
- No serious disruptions were observed in public communications networks in February.

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

The previous forecast's assessment of secondary effects from the exploitation of vulnerabilities and account breaches materialised in February. The same trend is expected to continue: the increase in M365 and other account breaches is likely to lead to incidents such as invoice fraud, including CEO fraud schemes. Compromised accounts are also used to send follow-on phishing messages.

The rapidly evolving situation in the Middle East may 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.