TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

July 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 July 2026

Summer showers reported in July's cyber weather

In midsummer, fewer information security incidents than in a typical month were reported to the NCSC-FI, but the number of reports has begun to rise again. This follows the familiar summer trend seen in previous years, as the holiday season affects reporting activity.

However, dark clouds gathered over the July cyber skies in the form of a handful of ransomware attacks in Finland. The first half of the year was relatively dry in terms of ransomware, but as the weather warmed up, cybercriminals became more active.

In line with this year's trends, several vulnerabilities were again disclosed in July. Four of these were highlighted in vulnerability advisories issued by the NCSC-FI. A key reason for the significant increase in the number of vulnerabilities is the use of AI-based methods to discover vulnerabilities.

Microsoft 365 (M365) account breaches have occurred in waves for several years. The situation has been calmer during the summer, but account breach campaigns are expected to become more active again as autumn approaches.

The evolving capabilities of AI systems and the potential threats associated with these systems and their use were also prominent topics in July. At the same time, it is worth remembering that generative AI also offers significant opportunities for defenders.

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

We issued a reminder about the risks posed by poorly secured network devices. A network device that is inadequately secured or monitored can provide a direct route into an organisation’s internal network and critical systems. It is important to allocate sufficient resources to securing network devices and to practise responding to incidents involving them.

Usernames were introduced in the WhatsApp instant messaging application, which may enable more convincing scams and increase their prevalence. Organisations should consider registering their official usernames as early as possible.

The number of malware incidents involving the ClickFix technique increased again in July. Organisations can use technical measures to prevent and limit the impact of ClickFix attacks, as described in our guidance published last year.

Cyber weather phenomena

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

Cyber weather
July 2026

1 mo.

Data breaches and leaks

Many WordPress breaches have been reported to the NCSC-FI. The number of ransomware reports has increased compared with the first half of the year.

The number of M365 account breaches decreased significantly during the holiday season.

Malware

More cases than usual of malware distribution were observed in July, especially involving the ClickFix technique. WordPress breaches have exposed websites to this type of malware distribution.

Vulnerabilities

Vulnerabilities continue to be discovered at an accelerating rate. In July, the number of CVE identifiers assigned in 2026 exceeded 40,000, compared with just over 45,000 in the whole of 2025.

Scams and phishing

In July, CEO fraud attempts targeted employees covering for colleagues during the holiday season.

Observations indicate increased use of AI tools to carry out scams.

Automation and IoT

The automation systems of several US water utilities have been attacked. The systems were poorly secured or had no security measures in place at all. System owners should improve security in cooperation with their system suppliers.

Network performance

A few denial-of-service attacks targeted Finnish organisations, but their impact on availability was limited.

Cyber weather
July 2026 1/2

1 mo.

Data breaches and leaks

- In July, a large number of WordPress sites were compromised and used to distribute malware using the ClickFix technique.
- The number of ransomware reports has increased compared with the first half of the year. In several cases, organisations' data has been leaked, or attackers have threatened to publish it.
- The number of M365 account breaches decreased significantly during the summer holiday season. The number of incidents is expected to increase significantly again once the holiday season ends.

Malware

- Reports of malware distributed using the ClickFix technique increased during July. Malware using the ClickFix technique is distributed particularly through compromised websites.
- The increased number of breaches affecting WordPress sites is also reflected in malware distribution, with compromised websites being used to distribute malicious code or software.
- Various malware detections were reported to the NCSC-FI during the month, but the observations did not indicate any larger-scale malware activity.

Vulnerabilities

- Vulnerabilities were disclosed in WordPress (wp2shell) that can be chained to enable unauthenticated remote code execution. Exploitation of the vulnerabilities has also been observed in Finland (CVE-2026-63030, CVE-2026-60137).
- A vulnerability was disclosed in Linux kernel versions 6.0–7.1 that allows a local user to escalate their privileges (CVE-2026-53362).
- A critical vulnerability was disclosed in NGINX products. The vulnerability allows an unauthenticated attacker to execute code remotely (CVE-2026-42533).

Cyber weather
July 2026 2/2

1 mo.

Scams and phishing

- Criminals have actively carried out scams impersonating executives of various organisations. In July, CEO fraud attempts targeted employees covering for colleagues during the holiday season.
- Observations indicate increased use of AI tools to carry out scams.
- AI tools have also been used to create fraudulent videos impersonating the police and targeting people of foreign background living in Finland. Instant messaging and video communication services such as WhatsApp and Google Meet have been used for these scam video calls.

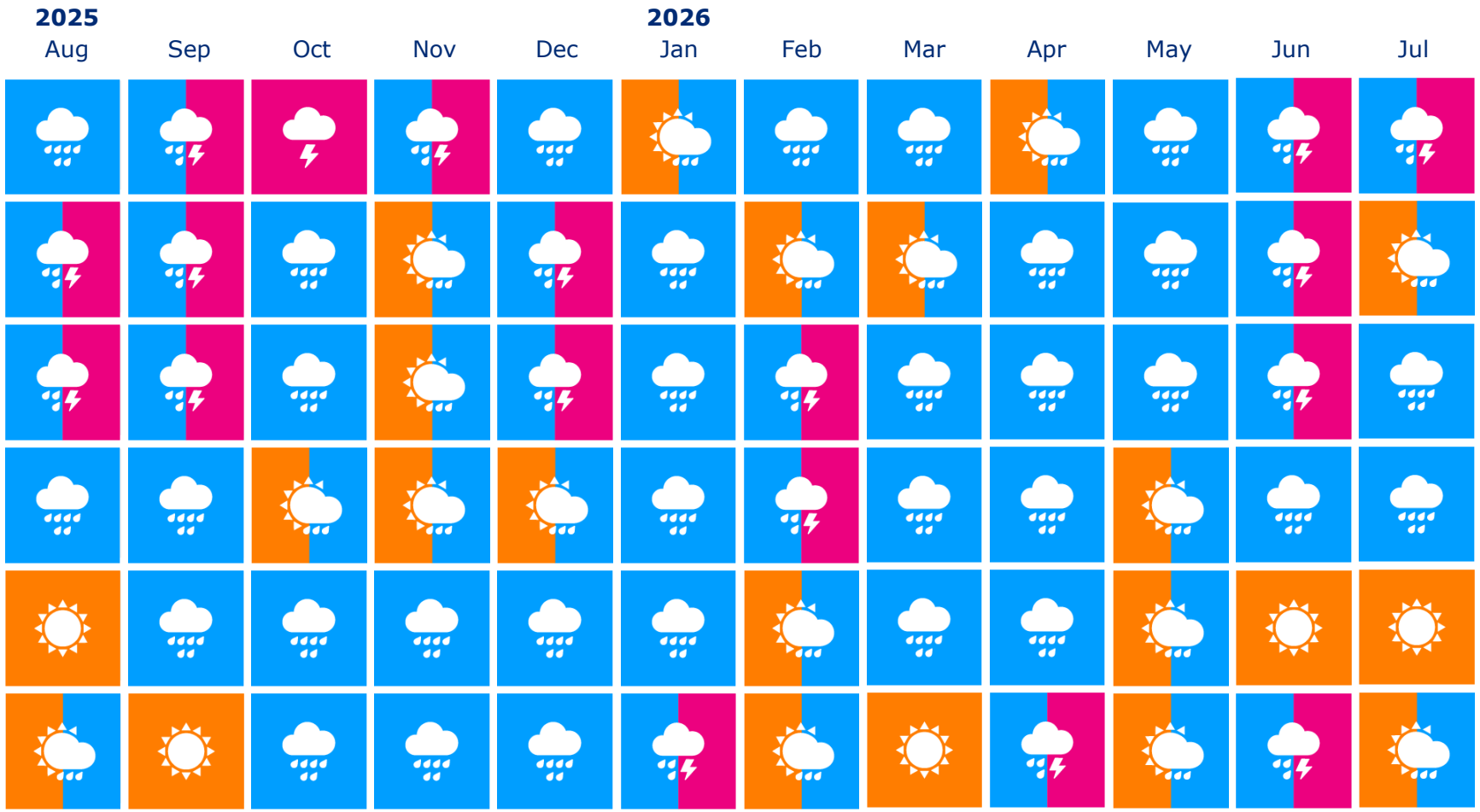
Automation and IoT

- The automation systems of several US water utilities have been attacked since late July. The attacks have caused moderately long service outages. In these cases, the systems were poorly secured or had no protection in place at all.
- Carrying out such attacks is technically straightforward. Whether an attack takes place depends primarily on the attacker's motivation.
- Many automation systems in Finland also remain inadequately protected.
- Owners of automation systems should improve security in cooperation with their system suppliers.

Network performance

- A report published in July identified a new type of denial-of-service attack against CDN services that exploits conversion between the HTTP/3 and HTTP/1.1 protocols to amplify traffic.
- Denial-of-service attacks may be used as a diversion as part of broader cyber operations.

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 number of M365 account breaches carried out using device code phishing is expected to increase sharply in late summer and early autumn. Organisations should prepare for this by blocking device code sign-in for users through a separate Device Code Flow Conditional Access policy and monitoring users who require the service.

Discussion of the cybersecurity implications of evolving AI systems is also expected to remain prominent throughout the autumn.

Organisational preparedness

- Due to the growing number of vulnerabilities and the rapid exploitation of zero-day vulnerabilities, organisations should actively monitor the vulnerability landscape. Particular attention should be paid to patching processes.
- Securing network edge devices is a key part of organisational cyber preparedness. Effective risk management requires proactive patch management, secure configurations, multi-factor authentication and effective monitoring for incidents.

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.