

TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

August 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 August 2026

Cyber weather remains rainy

The cybersecurity situation in Finland in August was characterised particularly by phishing, breaches of online services and new obligations introduced by EU regulation. As expected, the number of Microsoft 365 account breaches also increased following the summer holiday season.

Phishing took many forms, including payroll scams, impersonation of cybersecurity experts and scams impersonating Signal support.

The exploitation of a vulnerability in the WordPress core software disclosed in July continued in August, with compromised sites being used to distribute malware to visitors. The vulnerability has been exploited to compromise a very large number of Finnish websites.

Stormy cyber weather abroad

- The public sector has been targeted by cyberattacks in several countries.
- Latvia's vehicle registration system suffered a data breach and leak in August. The attackers gained access to personal data on 1.2 million people spanning several years.
- In Germany, two ministries of the State of Berlin were targeted by a data-stealing ransomware attack, as a result of which the ministries had to be disconnected from the network.
- In France, the series of significant data breaches seen throughout the year continued with an attack on the tax administration disclosed in August, in which data relating to approximately 680,000 individuals or businesses was stolen.

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



Keep website content management systems, such as WordPress, and their plugins continuously up to date, and remove unnecessary plugins and user accounts. We updated our WordPress security guidance during the summer.



Authorities and organisations have jointly launched a campaign promoting safe internet use at the start of the new school year. Traficom and the police have created a website on everyday information security, which provides practical cybersecurity tips for guardians and children.



We also published guidance to help companies understand when users must be informed about the use of artificial intelligence or AI-generated content. In practice, this applies, for example, to chatbots added to websites. Users must always be informed that they are interacting with an AI chatbot. We recommend that companies make use of the guidance, Code of Practice and icons published by the European Commission when implementing these obligations.

Cyber weather phenomena

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



Cyber weather

August 2026



Data breaches and leaks

- A large number of data breaches were reported in August.
- In most of the breaches, attackers exploited vulnerabilities as an attack vector.
- Device code phishing was prominent in Microsoft 365 account breaches.



Malware

- During August, numerous websites were observed distributing malware using the ClickFix technique.
- During the reporting period, two ransomware incidents were reported to the NCSC-FI.



Vulnerabilities

- The upward trend in the number of vulnerabilities continued in August.
- Data leaks resulting from the exploitation of vulnerabilities were also observed in August.



Scams and phishing

- Criminals once again targeted employees returning from holiday with scams.
- Do not trust callers who claim to be from technical support or to be calling about cybersecurity.



Automation and IoT

- Traffic cameras procured by Slovakia were found to be insecure and manufactured in Russia, posing a risk of exploitation for military intelligence purposes.
- Several backdoors have been found in routers manufactured by the Chinese company ZBT.



Network performance

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



Cyber weather

August 2026 1/2



Data breaches and leaks

- Breaches of vulnerable WordPress sites accounted for a significant proportion of data breaches carried out by exploiting vulnerabilities.
- Of the Microsoft 365 account breaches reported in August, 51% were carried out using device code phishing and 44% using AiTM phishing. Criminals also used Microsoft Teams chats to approach finance directors and pressure them into making money transfers or paying invoices urgently.
- Further investigation revealed that a data breach that occurred in July was serious: the personal data of more than 10,000 people was leaked in the incident.



Malware

- In August, several websites in the Finnish cyberspace were observed distributing malware using the ClickFix technique. The large number of breaches affecting WordPress websites has also led to a significant increase in ClickFix incidents.
- Two ransomware incidents were reported to the NCSC-FI during August. In both cases, internationally known cybercriminal groups were behind the attacks, including the Qilin and Krybit groups.



Vulnerabilities

- A severe, actively exploited vulnerability in N-able N-Central servers (CVE-2026-18556, CVE-2026-18577).
- A vulnerability in Metabase software allows an unauthenticated attacker to carry out an SQL injection attack remotely (CVE-2026-72898).
- Critical vulnerabilities in Citrix NetScaler ADC and Gateway products (CVE-2026-19489, CVE-2026-19490).



Cyber weather

August 2026 2/2



Scams and phishing

- In August, cybercriminals focused their attention on employees returning from holiday. Among the flood of emails waiting for them were also “urgent” phishing messages designed to trick returning employees into opening fraudulent links.
- Do not trust scammers posing as security authorities. If someone calls claiming to be contacting you about cybersecurity or offering a mandatory application update or support, do not trust the caller. Never disclose passwords, recovery keys, passcodes, PINs or other verification codes over the phone.



Automation and IoT

- Hundreds of traffic surveillance cameras procured by the Slovak government were found to have been manufactured in Russia. Undocumented backdoors were discovered in the cameras, allowing them to be taken over completely. The cameras had been sold by a Cypriot shell company. Insecure traffic cameras have been exploited elsewhere in the world for espionage and military intelligence purposes, and this is also a concern in Slovakia.
- Several backdoors have been discovered in routers manufactured by the Chinese company ZBT, allowing attackers to take control of the devices. Devices manufactured by ZBT are also sold under many other brand names.

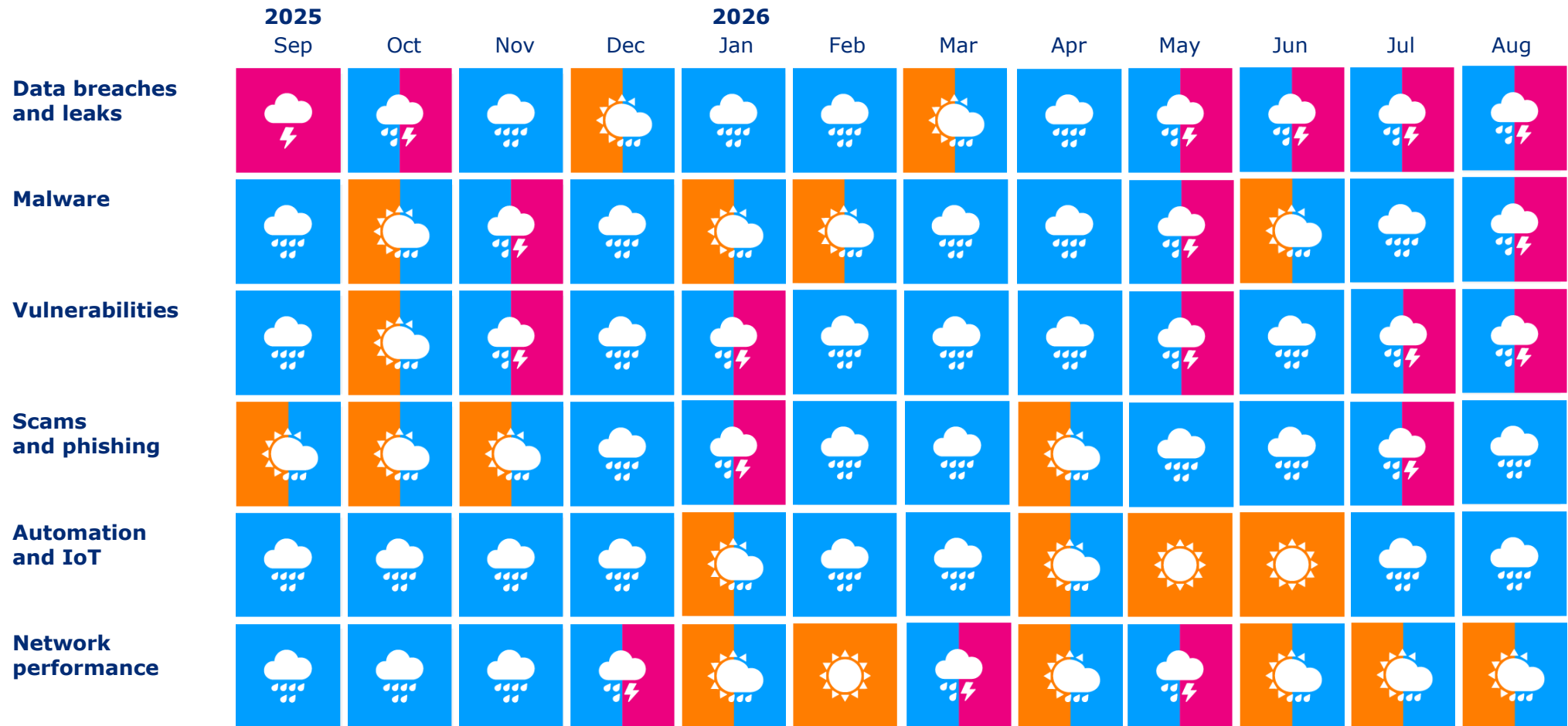


Network performance

- The number of super-botnets consisting of compromised IoT devices, servers and cloud infrastructure is growing, and the potential volume of attack traffic they can generate poses a significant risk to the availability of digital services.
- The pro-Russian hacktivist group Server Killers has claimed responsibility for several denial-of-service attacks in Europe, the most significant of which targeted Norway’s public administration.



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

No significant changes are expected in the cyber weather. The exploitation of vulnerabilities observed during the summer is likely to continue.

As in the previous year, the number of incidents is expected to increase as autumn approaches.

Organisational preparedness

- From a vulnerability management perspective, it is extremely important for organisations to regularly inventory their devices and systems. Reported incidents have included examples of outdated devices and software that organisations were not even aware were still in use.
- Faster update cycles require active monitoring.
- Device manufacturers often announce upcoming updates in advance, so organisations should monitor these notifications and plan their own actions accordingly.



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.