TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

June 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 June 2026

Dark clouds appeared in the June Cyber Weather, but a storm has so far been avoided

The impact of the global FortiBleed attack campaign was also felt in Finland, where approximately 20 devices were compromised. Although the campaign brought dark clouds to the horizon, no significant impacts have emerged so far.

The month brought with it the scams that are typical of the summer holiday season, and newly hired summer employees in particular should remain vigilant against them. In contrast, reports of Microsoft 365 account compromises declined toward the end of June, as expected.

In addition, the renewal of Microsoft Secure Boot certificates became a timely issue in June, as the expiration of existing certificates required organizations to take action to ensure the secure boot process of their devices.

The National Cyber Security Centre assessed the situation during the first half of 2026

The cyber security situation in Finland remained stable during the first half of 2026. Although there have been no significant sudden changes in the threat landscape, cyber threats have continued to evolve alongside advances in technology and changes in attackers' tactics. In particular, the use of artificial intelligence in cyber attacks, the rise in Microsoft 365 account compromises, and risks targeting supply chains have emerged as key areas of concern.

Hail shower of the month

The summer holiday season and temporary staffing arrangements provide fertile ground for CEO fraud

During the summer season, organizations typically employ more temporary staff and new employees who may not yet be familiar with established procedures or verification processes. This makes the period particularly attractive to criminals.

Typically, these scams involve someone impersonating a member of the company's executive management and requesting urgent actions, such as making wire transfers, purchasing gift cards, or paying invoices. The pretext may be, for example, an urgent corporate acquisition or another exceptional situation.

Criminals actively exploit phone calls, text messages, emails, instant messaging platforms, and social media. Therefore, simply claiming that a communication originates from a trusted source—such as a bank, a government authority, or a well-known company—does not guarantee its authenticity.

To mitigate these risks, organizations are encouraged to:

- ensure that payment approval and verification procedures are understood at all levels of the organization
- verify any unusual or exceptional requests through a separate communication channel
- avoid making financial decisions under pressure or in haste
- confirm the identity of the requester face to face whenever necessary.

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

The National Cyber Security Centre Finland at Traficom has compiled a checklist to help holidaymakers maintain good cyber security practices during the vacation season.

Protect network edge devices: Ensure that the management interfaces and other user interfaces of network edge devices are not accessible from the internet. Keep devices up to date at all times and continuously monitor their operation. Enable multi-factor authentication for VPN logins whenever possible.

The summer holiday season is peak season for scammers. Read our tips on how to avoid falling victim to scams.

Cyber weather phenomena

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

Cyber weather
June 2026

1 mo.

Data breaches and leaks

Network edge devices were targeted in a number of security breaches that exploited both software vulnerabilities and leaked user credentials. Despite the high number of incidents, serious consequences were avoided.

Malware

During the month, malware was distributed through email attachments as well as via malicious websites using the ClickFix technique. In terms of volume, malware detections remained at a moderate level.

Vulnerabilities

During June, the trend of newly discovered vulnerabilities continued to increase. The use of artificial intelligence to identify vulnerabilities has sparked extensive discussion worldwide.

Scams and phishing

Scam messages sent under the guise of child welfare services were used to harvest online banking credentials. Companies were targeted with scams related to domain name renewal. In scam phone calls purporting to be from Klarna, attackers attempted to persuade victims to install the UltraViewer remote access software on their computers.

Automation and IoT

On 3 June, the National Cyber Security Centre Finland hosted an information session on the Cyber Resilience Act. Answers to the questions raised during the event, as well as a recording of the session, are available on the event website.

Network performance

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

Cyber weather
June 2026 1/2

1 mo.

Data breaches and leaks

- Vulnerabilities are increasingly being exploited as the initial access vector in data breaches. In June, several Palo Alto GlobalProtect VPN devices were compromised through the exploitation of vulnerability CVE-2026-0257.
- As part of the FortiBleed attack campaign, more than 70,000 Fortinet FortiGate firewall and SSL VPN devices worldwide were compromised. Similar incidents were also observed in Finland, where the campaign led to a number of security breaches, and data from approximately 20 devices was leaked.
- Reports of Microsoft 365 account compromises declined towards the end of the month, in line with trends seen in previous years. In line with this trend, the next wave of account compromises can be expected after the holiday season, in early autumn.

Malware

- The National Cyber Security Centre Finland received reports of individual targeted email messages containing malware concealed within their attachments. These messages were intended to take control of the victim's computer or compromise accounts and credentials associated with it, such as Microsoft 365 accounts.
- Malware distribution campaigns using the ClickFix technique became more prevalent during the month. The ClickFix technique is used to distribute malware through suspicious or compromised websites. However, the malware was often detected early enough to prevent any damage from occurring.

Vulnerabilities

- The trend in vulnerabilities continued to accelerate, and current projections indicate that the number of newly discovered vulnerabilities will exceed 50,000 in 2026.
- At the beginning of June, the National Cyber Security Centre Finland issued a vulnerability advisory concerning a Check Point VPN vulnerability (CVE-2026-50751) that was being actively exploited.
- There has been considerable discussion worldwide about the potential of using artificial intelligence to discover new vulnerabilities.

Cyber weather
June 2026 2/2

1 mo.

Scams and phishing

- Numerous scam attempts carried out under the guise of child welfare services were reported. Messages were sent via both text message and email using various child welfare–related themes, including messages designed to mimic secure email communications. Phishing websites have also been observed using .fi domain names. The scam was designed to obtain victims' online banking credentials.
- Scam messages were sent to companies in the name of "DMS Finland". The messages requested that recipients renew their domain name registration.
- Scam phone calls were made in Klarna's name, during which the attacker attempted to persuade the victim to install the UltraViewer remote access software on their computer.

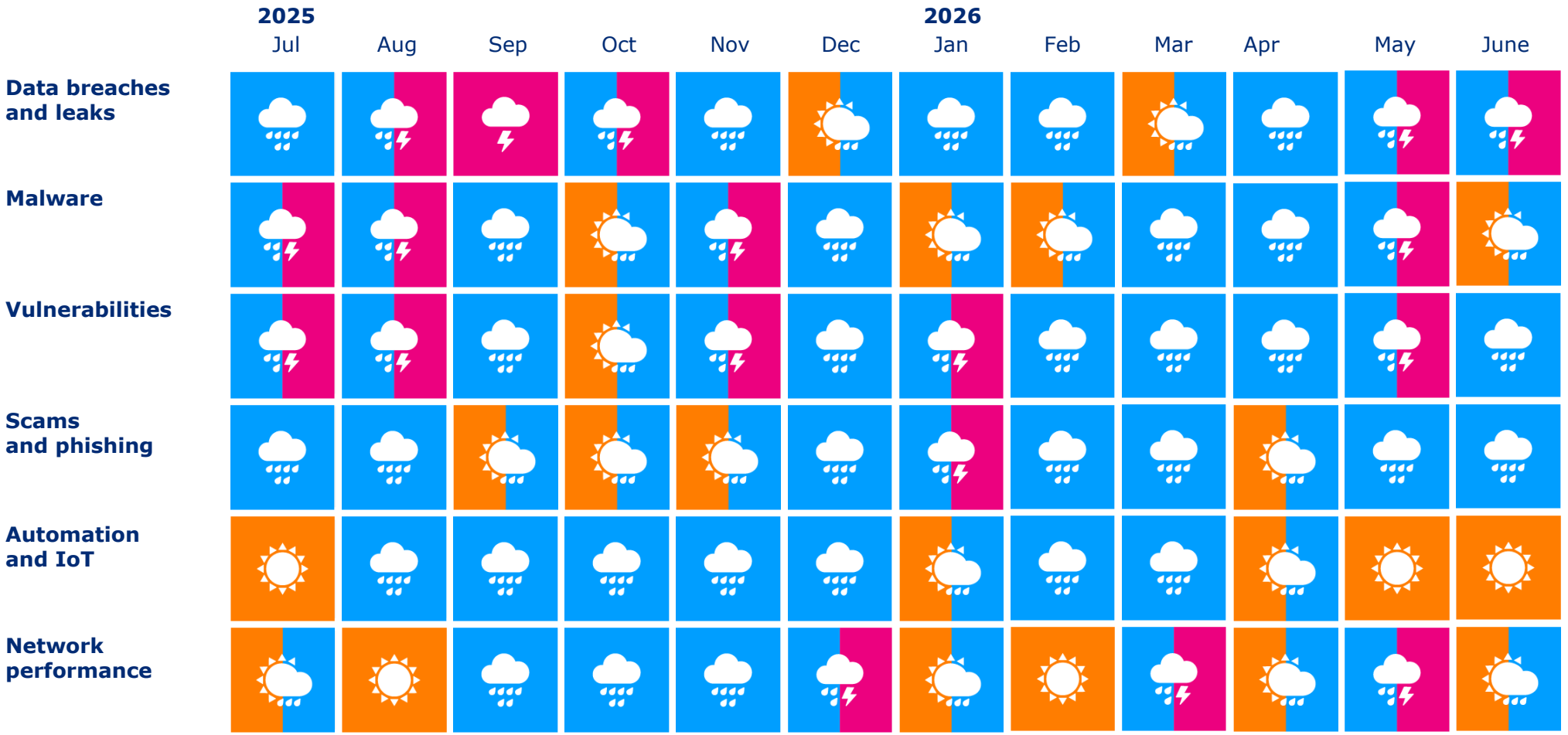
Automation and IoT

- On 3 June, the National Cyber Security Centre Finland hosted an information session on the Cyber Resilience Act. Answers to the questions raised during the event, as well as a recording of the session, are available on the event website.

Network performance

- In June, three minor and one more serious service disruption were observed in Finland's public communications networks, resulting in a partial interruption of voice services for subscriptions using standalone 5G networks.
- The impact of the denial-of-service attacks detected in Finland was limited to temporary disruptions.
- Although denial-of-service attacks have become increasingly commonplace in recent years, they can still have disruptive effects and organizations should take measures to protect themselves against them.

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.

1 mo.

Cyber weather forecast
Cyber threats remain at a typical level

The impact of the FortiBleed attack campaign, which became active in June, is expected to remain limited in Finland. The National Cyber Security Centre Finland is actively monitoring the situation.

The effects of the summer holiday season are expected to continue through July and August in the form of various scams.

Reports submitted to the National Cyber Security Centre Finland typically decrease during the summer season, but numbers begin to rise again in early autumn as organizations return from the holiday period.

Organizational preparedness

- Protecting network edge devices is a key component of an organization's cyber preparedness. Risk management requires proactive patch management, secure configurations, multi-factor authentication, and efficient monitoring of anomalies.
- An increase in Microsoft 365 account compromises can be expected after the holiday season ends. Organizations should implement protective measures to defend against account compromises.

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.