TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Cyber Weather

July 2025

#cyberweather

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

Cyber Weather, July 2025

Data breaches and leaks

- The number of data breaches declined slightly during the review period, but attempts increased.
- 70–80 per cent of reported incidents were linked to a SharePoint vulnerability. This highlights the importance of regular maintenance and timely updates of systems.
- In successful breaches, the volume of leaked data increased.
- In many attempted cases, however, security measures successfully prevented intrusions.

Scams and phishing

- Fraudulent messages were sent in the name of Traficom and the National Bureau of Investigation, threatening fines and child pornography charges. The scams were designed to harvest online banking credentials.
- A particularly aggressive email fraud demanded payment in bitcoin and threatened to expose sensitive images of the victim. All claims were fraudulent, and the blackmailer sent the same threat to thousands of recipients. The alleged images do not exist.

Malware and vulnerabilities

- A vulnerability in Microsoft SharePoint (CVE-2025-53770) has been widely exploited globally.
- Exploitation of vulnerabilities in Citrix NetScaler products (CVE-2025-5777 and CVE-2025-5349) is still being observed worldwide.
- The Android.BadBox2 malware continues to be detected in Finnish network traffic. The malware affects Android-based smart devices and links them to a botnet.

Automation and IoT

- The cyber security-related Regulation issued under the Radio Equipment Directive (RED) entered into force in February 2022 and became applicable on 1 August 2025.
- The Regulation introduces the first mandatory cyber security requirements for internet-connected wireless devices in the EU. Non-compliant products may be withdrawn from the market.
- In Finland, Traficom is responsible for market surveillance under the Regulation.

Network performance

- An international police operation was carried out against the pro-Russian hacktivist group NoName057(16). The operation resulted in arrest warrants, searches and seizures, as well as the shutdown of criminal IT infrastructure.
- Despite the successful operation, NoName057(16) continued its activities during July.

Spying

- SharePoint vulnerabilities have also been exploited in Finland in data breaches and attempted breaches.
- According to Microsoft, both APT actors and criminals have taken advantage of the vulnerability.
- The United Kingdom has imposed sanctions on entities linked to Russian military intelligence. The EU and NATO have likewise condemned Russia’s actions.

NCSC-FI's tips and recommendations for improving cyber security preparedness:

The OSCE Helsinki +50 anniversary conference was held at Finlandia Hall on 31 July. The NCSC-FI monitored the cyber security situation throughout the event. Both the conference day and the preceding week remained calm, with no significant incidents observed.

In late July, several cases of an aggressive extortion campaign were observed in Finland. Porn-themed extortion messages were sent to individuals and organisations, demanding payment in bitcoin. The subject line was often "cooperation offer", and the sender's address was spoofed to appear as the recipient's own email. This is a scam — the attacker has no access to the device.

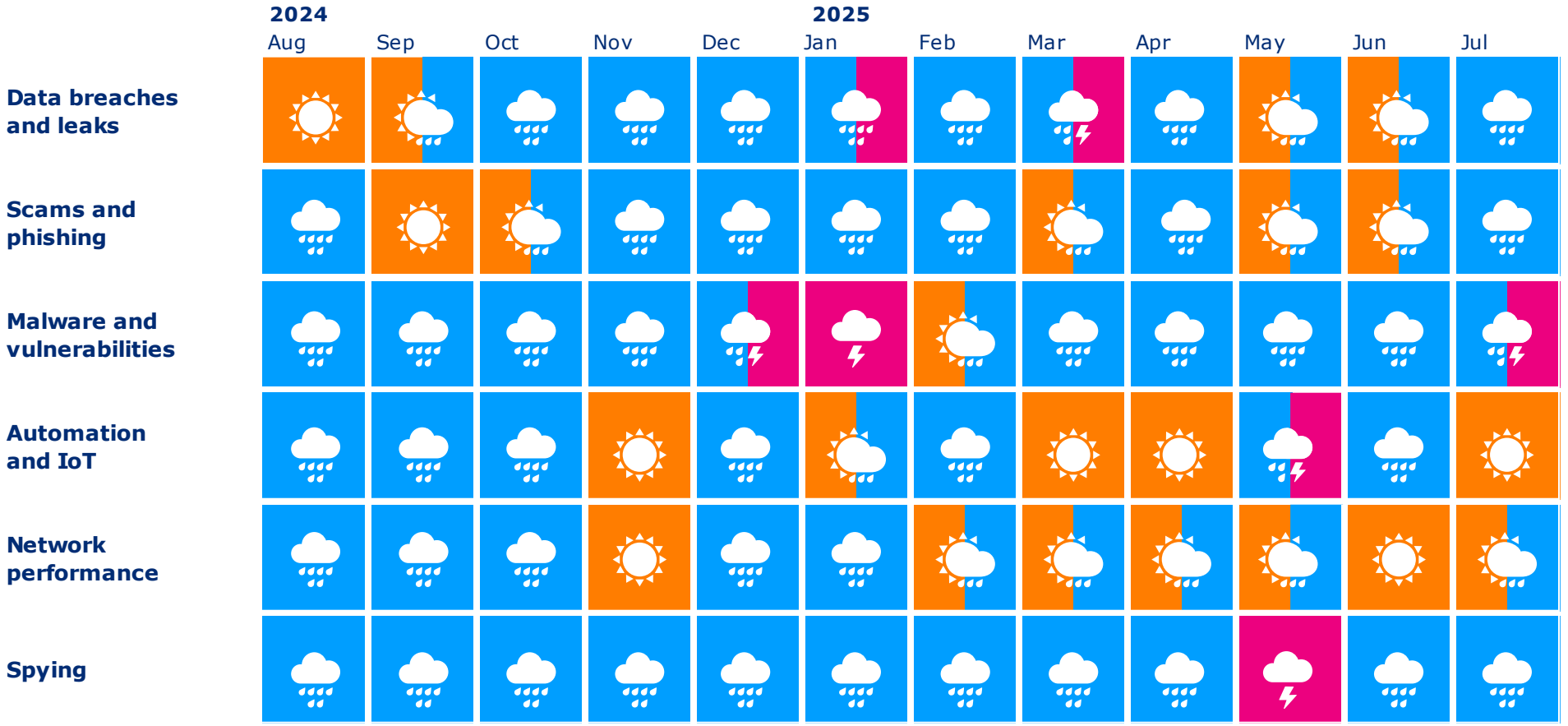
A critical vulnerability has been identified in the Microsoft SharePoint service, affecting on-premises SharePoint Server products. The vulnerability has been exploited worldwide.

Overview of cyber security in July

July began calmly in terms of cyber security, with conditions deteriorating towards the end of the month:

- During the month, data breaches were observed that weakened the overall picture of cyber security compared to earlier summer months.
  - In Finland, breaches targeted several companies in different sectors. In these cases, data including personal information was stolen. In most instances, however, the data did not include the most sensitive details, such as personal identity numbers.
- Serious global vulnerabilities have facilitated various cyberattacks.
  - In July, a critical vulnerability was identified in Microsoft's SharePoint service, which has been exploited worldwide. The vulnerability affects on-premises SharePoint Server products and does not impact the cloud-based version.
  - The vulnerability has been used in significant data breaches across the globe. Exploitation of this vulnerability is also evident in around 70–80 per cent of national data breaches reported in July.
- Attackers are exploiting the Direct Send feature in Microsoft 365 to send messages that appear to originate from within an organisation. This method enables them to bypass spam filters and email rules. It is recommended to review the settings of the Reject Direct Send function, and to apply strict SPF/DMARC configurations as well as multi-factor authentication.
- Malware-related detections levelled off slightly compared to June.
  - Detections of the BadBox 2.0 malware stabilised after June. However, the threat posed by the malware has not disappeared, as Google reports it has infected up to 10 million devices worldwide.

Cyber security trends
in the past 12 months



TOP 5 cyber threats in the near future (6–24 months)

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 information security and continuity of supply and service chains are increasingly critical.

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

3.

Organisations should prepare for AI-related challenges.

Organisations should try to identify challenges that artificial intelligence may cause and prepare for them by training their staff, for example.

Symbols

New

Updated

4.

Ransomware - Significant threat to organisations

Over the past year, several organisations in Finland have fallen victim to ransomware, and their number is also growing globally.

5.

Growing emphasis on protecting telecommunications infrastructure

It is important to protect telecommunications and information system infrastructure both abroad and at home, both because of accidents and natural phenomena and because of deliberate disturbances caused by outsiders.