TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Cyber weather

January 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, January 2025

Data breaches and leaks

- Network edge devices of several manufacturers have been used in data breaches. The root cause is often device users' poor information security practices that expose vulnerabilities to quick exploits.
- M365 accounts have been hacked as a result of a successful Dropbox phishing campaign.

Scams and phishing

- Tax-themed scams have become more common again since the turn of the year. Tax-themed SMS messages have been used to lure victims to give their online banking details to fraudsters.
- Phishing campaigns have also employed search engine advertisements purchased by scammers. Fraudulent ads have appeared in searches using terms such as Traficom and the names of banks.

Malware and vulnerabilities

- Critical vulnerability in Fortinet's FortiOS and FortiProxy products. According to Fortinet, the vulnerability is actively exploited.
- Scams have been running on the Tori.fi and Facebook Marketplace platforms, among others, where the seller of a product has been tricked into installing malware.

Automation and IoT

- European Commission adopted a standardisation request on the Cyber Resilience Act on 20 January 2025.
- The BlinkenCity study on the use of unencrypted radio signals in the energy sector in Central Europe highlighted risks and the need to introduce more secure wireless communication methods.

Network performance

- Seven performance disturbances observed in public communications networks in January.
- The number of DDoS attack reports is on the rise.
- A pro-Russia hacktivist group targeted DoS attacks against Finnish websites in response to the Government Defence Report issued in December. The effects of the attacks were minor.

Spying

- A vulnerability discovered in the Ivanti Connect Secure VPN has been exploited around the world on day zero at least since mid-December to infiltrate organisations.
- Suspicions of hacked devices have also been investigated in Finland.

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

Network edge devices being visible and open to the internet increases the attack surface for malicious operators. Our Information Security Now! article highlights the always timely need to secure network edge devices.

Malware installed on phones is currently spreading via online marketplaces, enabling criminals to take control of the entire phone. We issued a reminder about safe online shopping and the importance of installing applications only from official application stores.

The NCSC-FI increased its preparedness level because of the Baltic Sea NATO Allies Summit in Helsinki on 14 January. In terms of cyber security, everything went peacefully.

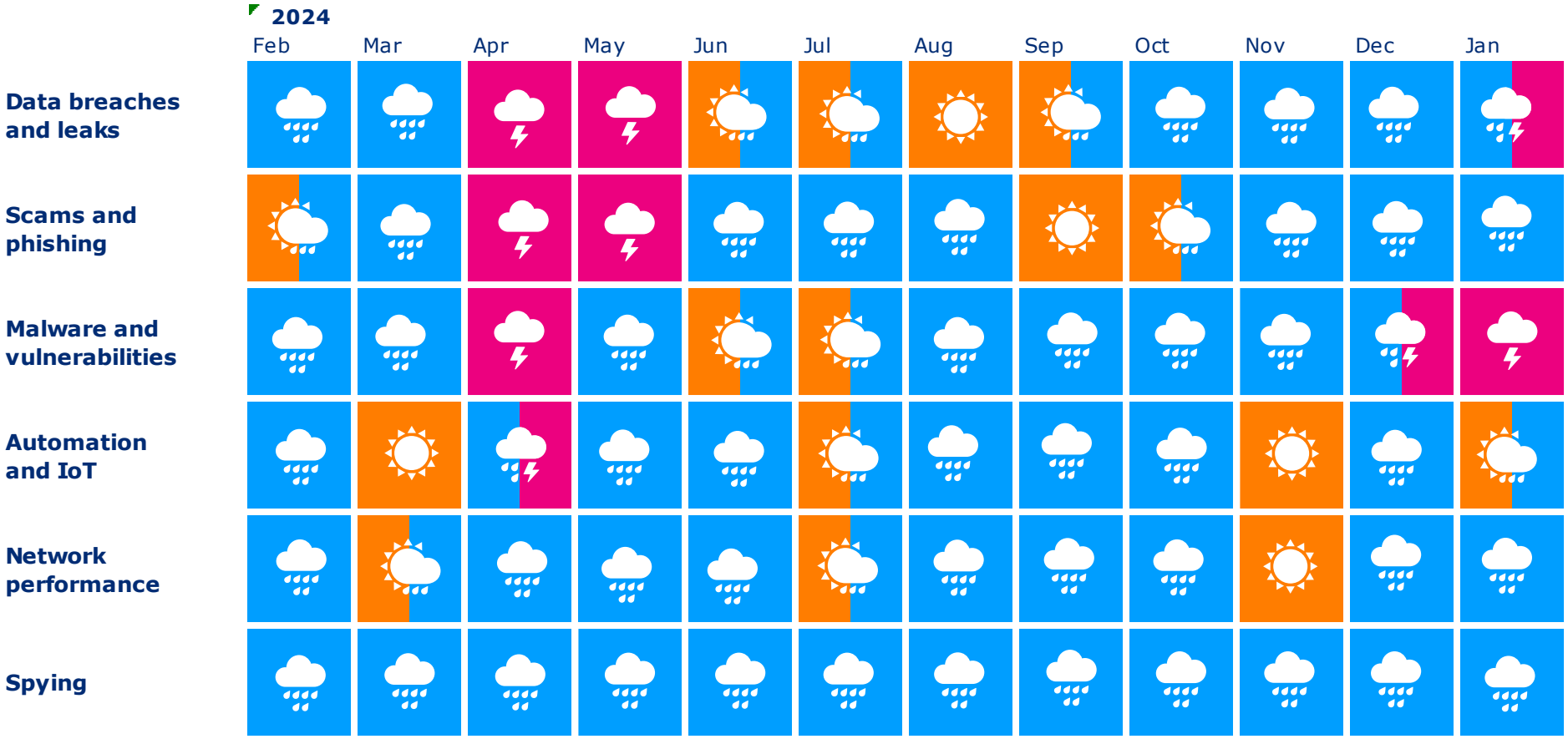
The InfoSec 2025 seminar is held on 12 March. This year's theme is protecting the digital society. The seminar is organised by Traficom and the Finnish National Emergency Supply Agency. The programme and registration form are available at tietoturvaseminaari.fi.

Overview of cyber security in January

- Rain clouds gathered in January skies because of vulnerabilities in Ivanti, Fortinet and SonicWall products. All vulnerabilities have been actively exploited. The NCSC-FI received reports about dozens of data breaches involving Ivanti and Fortinet devices.
  - Some of the vulnerabilities were used by attackers already before product owners were informed about them.
  - The exploitation of two of the vulnerabilities could be prevented completely by restricting the visibility of the management interface on public networks.
- A Microsoft 365 phishing campaign employing Dropbox became very active again in January. The campaign has resulted in numerous data breaches in different sectors, followed up by new phishing attempts.
  - In particular, criminals are exploiting PDF files shared from Dropbox to harvest email login credentials. The files have been shared under titles such as "LASKU_INV_PO300125.PDF". In cases reported to the NCSC-FI, attempts have been made to log in to a user account within minutes of the victim entering credentials on a phishing page.
  - In cases brought to the attention of the NCSC-FI, a message processing rule has been added to the hijacked email account, which moves all messages arriving with the word "dropbox" to the RSS Feed folder. The aim is to conceal suspicious activity in the account from the user.
  - The NCSC-FI's instructions on what to do in the event of a data breach give advice on preventive measures and explain the steps of ensuring the security of M365 accounts.

Cyber security trends
in the past 12 months

1 kk



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.

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.

3.

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.

New

Updated

Symbols

4.

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.

5.

Importance of protecting telecommunications infrastructure emphasised

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.