TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

# Cyber weather

February 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, February 2025

## Data breaches and leaks

- Continued frequent attempts to hack M365 accounts with Dropbox-themed messages. Breached accounts used for invoice fraud and new phishing messages.
- Organisations targeted by brute force attacks, including a few exceptionally massive ones.
- Facebook accounts hijacked by asking for phone numbers and verification codes in Messenger on the pretext of a competition.

## Scams and phishing

- People in Finland trust the police. Fraudsters have exploited this trust and sent scam messages in the name of the police, made phone calls posing as Europol officials and sent fake SMS in the name of judicial authorities.
- Scams in the name of the tax administration have attempted to steal online banking credentials.

## Malware and vulnerabilities

- Several reports about Magecart attacks against Finnish webshops.
- Reports about email messages with attached files including a QR code.

## Automation and IoT

- Top-selling IoT devices in Finland do not meet all the requirements set in the Radio Equipment Directive (RED)[4]. RED becomes applicable 8/2025.
- IoT devices are left in the field. Solutions: facility monitoring plans, documented life cycles of installed devices, processes for detecting superfluous devices.

## Network performance

- Four disruptions in public communications networks were detected in February.
- Slight decline in the number of reports about denial-of-service (DoS) attacks.
- DoS attacks did not cause significant disruptions in Finnish online services in February.

## Spying

- Russia-linked APT groups are exploiting a phishing method targeting Microsoft’s cloud email accounts. The victim is lured in to confirming the connection of the attacker’s device identifier with the victim’s account, giving the attacker access to the account.[5] Russian actors have also used linked devices in campaigns targeting Signal accounts.[6]

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

Risk management is key to software security – and gives a competitive edge. Secure software development is not only a technical requirement, it also ensures business continuity, software reliability and maintaining customer trust. Proactive risk management helps identify software development and procurement risks early, reducing repair costs and security threats.[7]

The NCSC-FI has received reports about Finnish webshops being targeted by Magecart attacks in which malicious plugins are added to the website or malicious scripts injected into its source code. If you operate a webshop, stay up to date on the website's security updates and safeguard your admin credentials. Check your site for malicious code or plugins.[8]

Companies should regularly check how visible their internal network devices and certificates are on the public internet. For example, the Censys service allows users to search for their devices. When examining the results, focus on how device certificates are signed, which services are detected and where the devices are located.

Report: Satellite broadband is an important alternative and additional resource for organisations in preparing for disruptions in telecommunications networks. The purpose of a recent report by the NCSC-FI and the National Emergency Supply Agency is to provide an overview of the use of satellite broadband technologies and services in the preparedness efforts of organisations vital for the security of supply. The report is also useful to other organisations that wish to utilise satellite broadband technologies and services.[9]

# Overview of cyber security in February

- February's cyber weather included rain and sleet caused by critical vulnerabilities in Ivanti Connect Secure and Policy Secure products, which enabled arbitrary code execution on affected devices.[10] A serious vulnerability in Palo Alto's PAN-OS system allowed attackers to bypass authentication and execute commands on the device.[11]

- CEO fraud emails have been circulating from addresses like *firstname.lastname.organisation/domain[at]outlook[.]com*. [12]

  - The Finnish used in these scams has been more accurate than before, and recipients are often addressed by their first name. The scam typically begins with a message requesting a favour and asking the recipient to respond via email due to an urgent situation. If the victim replies, the scammer asks them to purchase gift cards as corporate gifts for the organisation.

- Numerous phishing attempts impersonating authorities:[13]

  - In February, the NCSC-FI received several reports of scam emails and phone calls impersonating various authorities. The aim of these scams has been to trick victims into revealing sensitive personal information, such as banking details. Authorities will never ask for online banking credentials or payment card details over the phone.

  - To verify the authenticity of a call from an authority, you can contact the agency's customer service or switchboard. Contact details can be found on official websites. The websites of various authorities also provide updates on scams conducted in their name. You can also find information on current scams in the NCSC-FI's weekly reviews.

- M365

  - In M365 data breach cases reported to the NCSC-FI, there have been attempts to log in to user accounts within minutes after credentials were entered into a phishing page. In many cases, following the breach, attackers have sought billing-related information and attempted invoicing fraud by changing the recipient's account number to that of the criminal.[14]

  - Although most of these cases are financially motivated, it's important to remember that user accounts may also be targeted by other actors than mere opportunists. Cybersecurity companies such as Microsoft and Volexity have reported a recent campaign by a state-linked cyber threat actor targeting Microsoft 365 cloud service credentials. The campaign has been directed at sectors including central government, ICT and telecommunications providers, healthcare, defence, and energy.[15]

1 kk

# **Cyber security trends**
in the past 12 months

| | 2024 | | | | | | | | | | 2025 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Mar | Apr | May | Jun | Jul | Aug | Sep | Oct | Nov | Dec | Jan | Feb |
| **Data breaches and leaks** | 🌧 | 🌩 | 🌩 | 🌦 | 🌦 | ☀ | 🌦 | 🌧 | 🌧 | 🌧 | ⛈ | 🌧 |
| **Scams and phishing** | 🌧 | 🌩 | 🌩 | 🌧 | 🌧 | 🌧 | ☀ | 🌦 | 🌧 | 🌧 | 🌧 | 🌧 |
| **Malware and vulnerabilities** | 🌧 | 🌩 | 🌧 | 🌦 | 🌦 | 🌧 | 🌧 | 🌧 | 🌧 | ⛈ | 🌩 | 🌦 |
| **Automation and IoT** | ☀ | ⛈ | 🌧 | 🌧 | 🌦 | 🌧 | 🌧 | 🌧 | ☀ | 🌧 | 🌦 | 🌧 |
| **Network performance** | 🌦 | 🌧 | 🌧 | 🌧 | 🌦 | 🌧 | 🌧 | 🌧 | ☀ | 🌧 | 🌧 | 🌦 |
| **Spying** | 🌧 | 🌧 | 🌧 | 🌧 | 🌧 | 🌧 | 🌧 | 🌧 | 🌧 | 🌧 | 🌧 | 🌧 |