TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Cyber weather

March 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, March 2025

Data breaches and leaks

- The number of Akira cases has increased during the first quarter of the year. The access vectors exploit edge devices and lacking MFA.
- Compromised M365 accounts have been used for invoicing fraud. The messages were made to appear more credible by registering a domain that resembles the one used by the victim (typosquatting).

Scams and phishing

- The NCSC-FI's new instructions help to avoid scammers online and on the phone.
- A high number of tax-themed phishing messages circulated in March, attempting to harvest online banking credentials.
- Social media accounts are being hijacked again by sending the victim an instant message asking for the victim's phone number and a "lottery code".

Malware and vulnerabilities

- Ransomware infections were detected in March, and Akira was particularly prominent in the reports. Attacks have exploited vulnerable network edge devices.
- Updates to edge devices should always be installed without delay.

Automation and IoT

- Japan has introduced its own cyber security label for IoT devices.
- European standardisation organisations have accepted the EU Commission's standardisation request concerning the Cyber Resilience Act (CRA) and begun their work.

Network performance

- No network performance disruptions were observed in public communications networks in March.
- DDos-as-a-service has become more common as a form of denial-of-service attacks. The Mirai-based GorillaBot network has been used in attacks against Finnish targets.

Spying

- Chinese APT groups exploit IT supply chains as well as remote access and management tools — and their vulnerabilities — to break into organisations.
- Cyber attacks against Ukraine and its supply chains continued active. Targets included logistics and defence sectors and central government.

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

The NCSC-FI published on 27 March a crisis communication guide aimed at organisations, providing information on different types of cyberattacks as well as the methods and tactics used by cyber criminals. The guide offers tips on how to prepare communication strategies in advance and how to communicate effectively during and after a cyberattack.

Microsoft continuously releases new updates to its cloud services. Subscription settings should preferably be checked every six months in the Entra ID (former Azure Active Directory) settings of the Microsoft 365 subscription, if the organisation's M365 subscription settings are not otherwise continuously monitored. The NCSC-FI has issued instructions on Entra ID directory and user management settings.

The NCSC-FI has updated its advice on the introduction of a password manager.

Overview of cyber security in March

- In March, we received reports about the exploitation of vulnerabilities in edge devices. These vulnerabilities are an important access vector, which is why it is crucial to keep edge devices up to date.
  - Multiple international information security authorities have issued warnings about vulnerabilities in, for example, Fortinet's widely used firewall products. For example, the US cyber security agency CISA added the Fortinet vulnerability CVE-2025-24472, published earlier this year, to its known exploited vulnerabilities (KEV) catalogue. Vulnerabilities have been exploited, for example, to spread ransomware. Attacks are specifically targeting the management interfaces of firewall devices.
  - Fortinet's network devices have also been a major issue in reports received by the NCSC-FI. We recommend that users of these devices immediately check and disable the visibility of the device management interfaces in public networks and ensure that the devices are up to date.
- Various scams have continued active.
  - The NCSC-FI has received reports about scam calls in the name of the NCSC-FI, a phishing campaign harvesting banking details in the name of the Tax Administration, scam messages impersonating S-Bank, a Neste-themed scam and a phishing campaign in the name of the postal operator Posti.
  - Facebook credential theft also continues with scammers sending messages via Messenger trying to hijack accounts with the help of a phone number and a verification code.
  - How to recognise authentic websites and authorities – avoid online scam (in Finnish). https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-yksityishenkiloille/nain-tunnistat-aidot
- Several M365 data breaches using the AiTM technique have been reported in various sectors. In many cases, attackers have attempted to send further messages from hijacked accounts.
  - The NCSC-FI's AiTM guidance is available here: https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/instructions-and-guides/increasing-number-m365-data-breaches-utilise-aitm-phishing

Cyber security trends
in the past 12 months

1 kk