TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Cyber weather

May 2025

Cyber weather May 2025

Data breaches and leaks

- May remained calm in terms of data breach reports, following the trend seen in April.
- In cases of email account compromises, third-party email applications were used to access and exfiltrate messages from compromised M365 accounts — all without the user's awareness.

Scams and phishing

- The summer holiday season brings with it scams impersonating executives. Make sure to brief summer stand-ins on how to recognise fraud attempts — scammers do their homework and are always coming up with new tricks.
- The *Be vigilant on the web* campaign now also provides information security guidance in sign language.

Malware and vulnerabilities

- Scams and phishing campaigns employing various themes have involved the use of infostealer malware to extract information. As a result of successful scams and phishing attempts, these types of malware have been installed on targeted devices.

Automation and IoT

- The FBI has issued a warning about cybercriminals exploiting Internet of Things (IoT) devices connected to home networks for criminal activities, using the BADBOX 2.0 botnet.

Network performance

- In May, 7 disruptions were detected in public communications networks.
- Traditional denial-of-service attacks based on massive traffic volumes remain common and are becoming more powerful.
- Carpet bombing, application-layer attacks and the adaptation of attack traffic to bypass deployed protections are increasingly prevalent.

Spying

- Many Western countries have warned about the Russia-linked APT28 targeting the logistics and technology sectors for espionage purposes.
- The Netherlands and Microsoft reported on the likely Russia-linked actor Laundry Bear/Void Blizzard, which has spied on e.g. public authorities.
- The Czech Republic has linked espionage against its foreign ministry to the APT31 group and China.

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

The European Union Vulnerability Database (EUVD) was launched on 13 May 2025. The EUVD provides a long-awaited alternative to the US-based CVE database, whose funding continuity has recently been subject to uncertainty.

On 21 May, CISA published a report on cyber espionage and influence operations targeting technology and logistics companies in countries supporting Ukraine. The report sheds light on Russian influence activities that began in 2022, as well as the techniques, tactics and procedures used by units operating under the Russian military intelligence service GRU. These activities have been directed at companies operating in countries providing support to Ukraine.

The email applications used in M365 account compromises request extensive permissions to the compromised mailbox. Access rights granted to applications should be restricted so that only administrators are authorised to approve them.

The National Coordination Centre for Cyber Security Research, Development and Innovation (NCC-FI), operating within the NCSC-FI, has been granted co-funding from the European Union's Digital Europe Programme for a new four-year continuation period. The European Commission is funding the project with four million euros, and nearly the entire amount will be distributed as financial support to Finnish actors. The NCSC-FI will host a public webinar in June, presenting the latest insights into available national funding support and EU funding opportunities for the development of cyber security.

Overview of cyber security in May

- The start of the summer season has once again stirred up malicious activity, particularly visible in phishing and fraud-related observations. The past month brought with it some storm clouds also because several Western countries reported being targeted by attacks linked to state-sponsored cyber threat actors.
  - Toward the end of the month, a rising trend was noted in phishing attempts using adversary-in-the-middle (AiTM) techniques capable of bypassing multi-factor authentication. Observed themes included banking, postal services, taxation and vehicle-related scams.
- Vulnerabilities in various digital devices remain a key concern in the field of cyber security. When purchasing a device, it is important to consider not only its features and lifecycle, but also the manufacturer.
  - The transition to high-definition broadcasting on commercial TV channels from 1 July is prompting many households to purchase a smart TV. However, some devices on the market may pose a risk to household information security. Security shortcomings have been particularly noted in low-cost Android TV devices by unknown manufacturers sold online. When making a purchase decision, it is advisable to prioritise well-known and trusted brands over low price alone.
  - The threat posed by vulnerable network edge devices remains significant. Exploitation of vulnerabilities in devices such as firewalls and VPN appliances has been observed across Europe and globally — and Finnish organisations have not been spared. Network monitoring, rapid software updates and replacing end-of-life hardware with supported products are critical measures to avoid such threats.
- AI applications are becoming increasingly common among both organisations and private individuals. Cybercriminals have sought to exploit this growing popularity to conduct data breaches and spread malware.
  - Attackers are taking advantage of fake AI applications and websites, which contain hidden malware or malicious code. Malicious websites intended for malware delivery have been promoted via social media and search engine manipulation, among other tactics. When downloading applications, users should always assess their necessity and trustworthiness. In the case of free apps, it is advisable — where possible — to check the reliability of the publisher before proceeding.

Cyber security trends
in the past 12 months