TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Cyber weather

November 2025

Cyber weather, November 2025

Data breaches and leaks

- The alert concerning Microsoft 365 account breaches was withdrawn on 27 November 2025. Despite this, the threat of account compromise has remained high. Multi-factor authentication alone is not sufficient to mitigate the risk.
- Data breaches were carried out by exploiting vulnerabilities:
  - Microsoft WSUS Remote Code Execution CVE-2025-59287
  - Adobe Commerce and Magento Open Source CVE-2025-54236
  - ASUS AiCloud - CVE-2025-2492

Scams and phishing

- Fake online shops are after consumers' money in the wake of year-end promotions. Christmas season discount campaigns are particularly popular with fraudsters.
- Scam call blocking solution developed by Traficom and Finnish telecommunications operators won the European Crime Prevention Award. Earlier in the autumn, the solution had also won the Finnish crime prevention award.

Malware and vulnerabilities

- Critical and exploited vulnerability in the Fortinet FortiWeb product (CVE-2025-64446).
- A second wave of the Shai-Hulud malware has widely infected npm packages, harvesting credentials and sensitive information from systems using them. Organisations should review their development infrastructure for signs of compromise.
- Magecart malware concealed in compromised online shops is stealing customers' payment card details.

Automation and IoT

- The CRA Implementing Regulation (EU) 2025/2392 on the technical description of the categories of important and critical products has been published on EUR-Lex.
- Multi-purpose botnets such as Aisuru provide attackers with a wide range of capabilities. Even if botnets are successfully disrupted, the devices often remain vulnerable and can be used to form new botnets.

Network performance

- The largest botnets used for denial-of-service (DoS) attacks continue to grow, and ever larger attacks are being reported. The increasing number of unsecured IoT devices is fuelling this trend, which is expected to continue in the future.
- Microsoft reported successfully mitigating a record-breaking Aisuru botnet DoS attack exceeding 15 Tbps, with the attack traffic originating from more than 500,000 source addresses. Aisuru is composed of compromised home routers and IoT devices, such as surveillance cameras.

Spying

- Cyber threat actors continue to exploit both known and newly discovered vulnerabilities in network devices to carry out data breaches. In November, targets included, among others, Cisco devices.
- A data leak linked to an Iranian cyber actor revealed details about the group's operations.
- Reporting related to Iran also highlighted interest in the defence industry and the aviation sector.

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

OWASP, which maps security threats affecting web applications, is in the process of updating its Top 10 list. In the new edition, both the headings and the ranking of threats are set to change to some extent. Supply chain–related threats are also emerging as a new category in the list.

The risk of digital skimming increases ahead of major sales events and holidays. In digital skimming attacks, criminals inject malicious code into online shops to steal payment details entered during the checkout process. Although Black Friday has already passed, the risk should also be kept in mind when shopping for Christmas gifts. Read more in our Information Security Now! article "The invisible thief in your online shop – Digital skimming can have significant financial impacts" (in Finnish).

At the beginning of December, we published an Information Security Now! article focusing on administrator accounts in cloud services. You can find tips on securing administrator accounts in the article "Managing cloud service administrator accounts – best practices" (in Finnish).

Overview of cybersecurity in November

Overall, November's cyber weather was rainy, but at the same time fairly calm. During the month, a few noteworthy phenomena were observed in Finland and globally.

In reports received by the NCSC-FI, newer observations included attacks using the ClickFix technique and the Shai-Hulud 2.0 malware. The BadBox 2.0 malware, which became familiar during the summer season, continues to be detected.

- In ClickFix attacks, internet users are tricked into executing malware on their own devices. The attack method imitates small, familiar tasks such as "Confirm you are human" prompts and CAPTCHA-style checks that users are accustomed to encountering during everyday web browsing.
- Shai-Hulud 2.0 is a computer worm that spreads in development environments. Its propagation has been extremely rapid, infecting several popular npm packages, including numerous packages published by Zapier, ENS Domains, PostHog and Postman. New packages containing malicious code continue to be identified. In Finland, a small number of reports related to the malware have been received.

The growth in data breaches targeting Microsoft 365 accounts slowed in November, and at the end of the month we withdrew the severe alert that had been in force since September. The number of M365 breach reports has so far returned to August levels, but the underlying threat has not disappeared.

An international disruption affected Cloudflare's services on 18 November, impacting the availability of several popular services. The incident was fairly visible to everyday internet users, temporarily preventing access to services such as X and ChatGPT.

Cybersecurity trends
in the past 12 months