TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Cyber weather

April 2025

Cyber weather, April 2025

Data breaches and leaks

- The number of data breaches in April was lower than earlier in the year.
- Stolen user credentials for hotel and travel booking services, especially Booking.com credentials, were still used to phish for payment card details from customers who had used the services to make bookings.
- Breaches of M365 credentials continued, and Dropbox-themed AiTM phishing messages were particularly frequent.

Scams and phishing

- Active campaigns phishing for online banking credentials. SMS scams have impersonated Finnish Customs and the Tax Administration, luring victims into clicking on links taking them to phishing websites.
- Phishing scams have also threatened recipients with a parking fine.
- In a scam, mobile certificate users have been tricked into accepting unknown identification events.

Malware and vulnerabilities

- A critical vulnerability in a SAP NetWeaver software component (CVE-2025-31324) is being exploited and should be patched immediately.
- A critical vulnerability in Ivanti Connect Secure (CVE-2025-22457) is being exploited. Old versions should be updated without delay.

Automation and IoT

- In terms of automation and IoT systems, April brought lovely spring weather. No major observations were reported during the period under review.
- On 6 May, the US authorities issued the guideline "Primary Mitigations to Reduce Unsophisticated Cyber Threats to Operational Technology".

Network performance

- Six disturbances were detected in public communications networks in April, one of which had a high severity rating (A).
- During the week with county and municipal elections, a pro-Russia hacktivist group targeted denial-of-service (DoS) attacks against Finnish websites, including those of political parties. The attacks had no significant impact on the conduct of the elections.

Spying

- Apple has issued warnings to its users who have been spied on with commercial spyware.
- France connected several cyber attacks that it had investigated to the Russian group APT28.
- Poland and Romania discovered espionage against their central governments and public sectors. The espionage exploited a Microsoft vulnerability.

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

Traficom issued new guidelines on the assessment and approval process for information systems and information security in April. The guidelines are intended for authorities and companies that process nationally or internationally classified information in electronic form.

Obligations under the NIS 2 Directive and the Finnish Cybersecurity Act entered into force on 8 April 2025. The new Act creates a more structured framework for cyber security in Finland and requires entities critical to society to comply with obligations regarding cyber security incidents.

Numerous vulnerabilities have been discovered this spring, particularly in network edge devices. Vulnerability management is difficult if an organisation is not sufficiently familiar with its environment. Systems should be mapped and documented regularly.

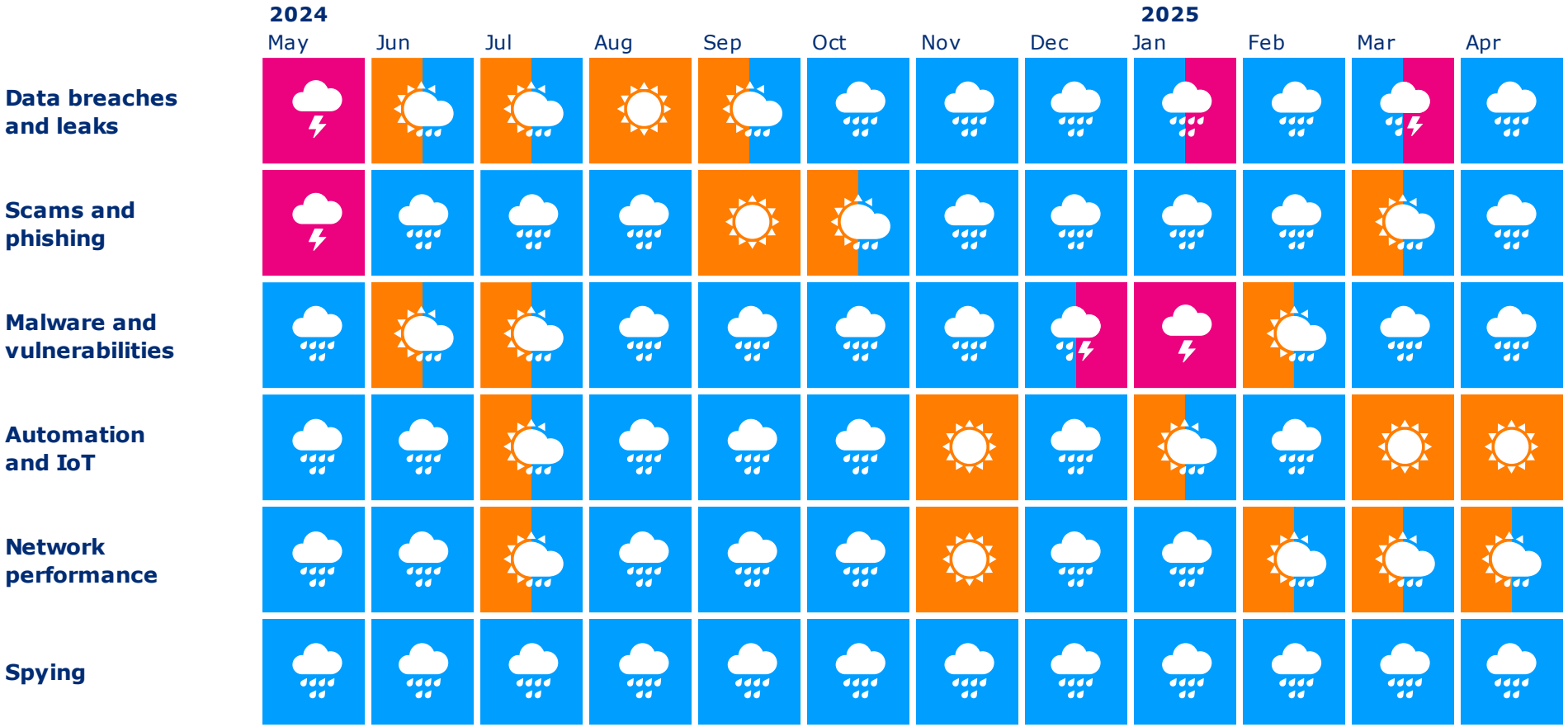
Overview of cyber security in April

April was relatively quiet in terms of cyber security issues:

- The county and municipal elections that took place early in the month woke up the pro-Russia hacktivist group NoName057(16) from hibernation, as six Finnish domains were included in the group's lists of targets after a break of a few months. DoS attacks targeted the websites of political parties, public transport operators, and public and private sector organisations, for example. Overall, the attacks had a limited impact and did not affect the conduct of the elections.
- Easter 2025 was very quiet in terms of cyber security observations. Organisations should nevertheless be aware that holidays or other significant events that deviate from the normal routine may increase attacker activity.

- Phishing was once again highlighted in April cyber weather with prominent phenomena including scams in the name of banks and accommodation booking services. Phishing messages and websites were usually of a rather high quality, and some phishing attempts were targeted against the mobile certificate, a service used for electronic identification.
  - Attackers often contact potential victims via SMS or WhatsApp. The sender's name is often edited to appear like an actual organisation.
  - Scam campaign themes vary from month to month, and the approaching summer holiday season will most likely cause an increase in campaigns associated with hotel and booking services, in particular. Some scam attempts involving booking services have indicated data breaches against the service in question, as attackers have been able to send messages through the booking system.
- Network edge devices continue to be targeted by attacks:
  - The number of attacks against edge devices used by organisations has increased. The importance of quickly updating devices cannot be emphasised enough, because attackers are actively looking for vulnerabilities in earlier versions in the contents of published updates, for example.
- Uncertainty about funding for the CVE database caused concern in April. The CVE project ultimately secured funding for the next 11 months. All current vulnerability management tools use CVE identifiers.
  - A beta version of the European Vulnerability Database (EUVD), maintained by the EU Agency for Cybersecurity (ENISA), was launched in mid-April. This new database will issue its own identifiers for vulnerabilities and therefore does not depend on CVE identifiers, though it will continue to make use of them as well. Other international operators have also quickly developed solutions to adapt to the situation.

Cyber security trends
in the past 12 months



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.

Symbols

New

Updated

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.

Growing emphasis on protecting telecommunications infrastructure

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.