TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

April 2026

Cyber weather

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

Overview of cyber weather in April 2026

April brought no major changes in cyber weather

The warming spring conditions were cooled in particular by Microsoft 365 account breaches, which were reported to the NCSC-FI in higher numbers than during the previous month. Rain showers also arrived during the month in the form of vulnerabilities disclosed in several different products.

The use of AI-based solutions for vulnerability discovery and exploitation became a major topic of discussion during the month.

The use of artificial intelligence in fraud has also been observed to be increasing.

- So far, the NCSC-FI is aware of only isolated cases in which AI-generated audio and video have been used, for example in CEO fraud and investment scams.

Traficom published cybersecurity scenarios for 2035 – four alternative futures

From a cybersecurity perspective, artificial intelligence, supply chains, the reliability of the information environment and the interconnectedness of critical infrastructure emerge as decisive issues in all scenarios.

The scenarios support preparedness, decision-making and strategic discussion in a context where the security of the future digital society is built on increasingly complex interdependencies.

Traficom's website was redesigned

We have redesigned the NCSC-FI website as part of Traficom's website platform upgrade. The change improves the functionality of the websites and enables further development in the future. Some isolated issues may still occur on the sites, such as broken links. We are continuously working to fix them. We apologise for any temporary disruptions caused by the renewal.

Hail shower of the month
AI-based vulnerability scanning is changing the landscape

AI-based vulnerability scanning became a major topic of discussion in April due to the capabilities it offers.

Advanced AI solutions are expected to enhance malicious vulnerability discovery and increase the number of exploitable vulnerabilities. Artificial intelligence can be used to identify previously unknown vulnerabilities, and AI is also capable of exploiting them autonomously.

AI solutions also significantly improve attack path analysis. By using AI-based tools, attackers can identify and chain together various factors that enable the exploitation of vulnerabilities, such as authentication, configuration and logic flaws within the targeted network environment.

This challenges traditional scanning methods, which may not fully recognise the overall risk posed by identified vulnerabilities.

However, advanced AI solutions are not expected to completely replace traditional signature-based vulnerability scanning. Instead, they are changing the nature of vulnerability assessment towards more autonomous, faster and more comprehensive capabilities that better account for threats and risk factors.

At the same time, AI-based applications also present opportunities for improving organisations' risk management and cybersecurity. According to some forecasts, AI applications could account for as much as half of current cyber defence and mitigation measures by 2028.

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

Register for an information session on the entry into force of the EU Cyber Resilience Act (CRA) on 3 June. The event is organised by Traficom, the Ministry of Transport and Communications, and the Finnish Information Security Cluster (FISC). At the event, representatives from the European Commission, national authorities and companies will present perspectives on the content of the regulation, its obligations and its national implementation.

Organisations are encouraged to transition to phishing-resistant authentication methods, such as FIDO2/WebAuthn or certificate-based authentication. Traditional multi-factor authentication (MFA) can increasingly be bypassed through Adversary-in-the-Middle (AiTM) attacks, OAuth abuse and session token theft.

The FINMISP service has been launched! FINMISP is a national cyber threat information sharing service provided by the NCSC-FI and based on the Malware Information Sharing Platform (MISP). The service enhances the sharing of technical threat intelligence related to nationally and internationally observed information security incidents. The NCSC-FI acts as the central node of the network and distributes information to service users.

Cyber weather phenomena

In this section,
we review developments and trends
in key cybersecurity phenomena.

Cyber weather
April 2026

1 mo.

Data breaches and leaks

Fourteen per cent more data breaches were reported than in March. However, fewer data leaks were reported in April. Several of the reported data leaks were caused by misconfigurations.

Malware

The month was active in terms of malware observations. The NCSC-FI received reports of, among other things, malware distributed using the ClickFix technique, as well as individual Magecart and infostealer malware cases.

Vulnerabilities

The number of disclosed vulnerabilities also remained high in April. Rapid patching of internet-facing devices and services continues to be essential in reducing opportunities for vulnerability exploitation.

Scams and phishing

In April, official messages from public authorities were fully migrated to the Suomi.fi service. Scammers are exploiting the situation by sending links to fraudulent services.

Scams related to hotel and travel booking services are increasing as the summer holiday season approaches.

Automation and IoT

US authorities published guidance on applying zero trust principles to OT systems.

IoT devices and consumer-grade network devices are attractive targets also for state actors.

Network performance

When providing AI services externally, organisations should consider the possibility of service overload and abuse.

The growing number of software vulnerabilities associated with the increasing use of artificial intelligence may also contribute to the expansion of botnets used in denial-of-service attacks.

Cyber weather
April 2026 1/2

1 mo.

Data breaches and leaks

- In April, significantly more compromised M365 accounts were reported than in March. Most credentials were phished using AiTM techniques, meaning that MFA alone is no longer sufficient to prevent account breaches.
- Thousands of phishing messages were sent from compromised accounts, which is expected to further increase the number of breaches in May.
- Several WordPress sites were compromised through vulnerabilities in plugins. Regular updates of WordPress and its plugins are essential. Verify also whether responsibility for updates lies with the web hosting provider or the website administrator.

Malware

- Magecart malware was detected in individual online stores. The malware is used to steal personal and banking details entered into e-commerce sites.
- The NCSC-FI also received reports of malware distributed using the ClickFix technique.
- Phishing and vulnerabilities have also been used to distribute malicious software and infostealer malware.
- The supply chain attacks targeting open-source libraries that occurred in March continue to appear as an attack vector.

Vulnerabilities

- CVE-2026-31431: The “Copy Fail” vulnerability in the Linux kernel allows a regular user to gain root privileges.
- CVE-2026-41940: A vulnerability in cPanel and WHM products allows an unauthenticated attacker to gain administrator-level access to the management panel. Exploitation has been observed and immediate patching is recommended.
- CVE-2026-35616: A vulnerability in FortiClient EMS that allows an attacker to compromise a device. The vulnerability is being actively exploited.

Cyber weather
April 2026 2/2

1 mo.

Scams and phishing

- In April, official messages from public authorities were fully migrated to the Suomi.fi service. Scammers are exploiting the situation by sending links to fraudulent services. Recognising online scams becomes easier when people are informed about scams in advance. Awareness gives people the opportunity to pause and assess whether an SMS, email or phone call is genuine or a scam. Do not follow links in SMS directing you to strong authentication services.
- Hotel and travel booking scams are increasing as the summer holiday season approaches. Think twice and verify with the service provider before paying unexpected extra charges.

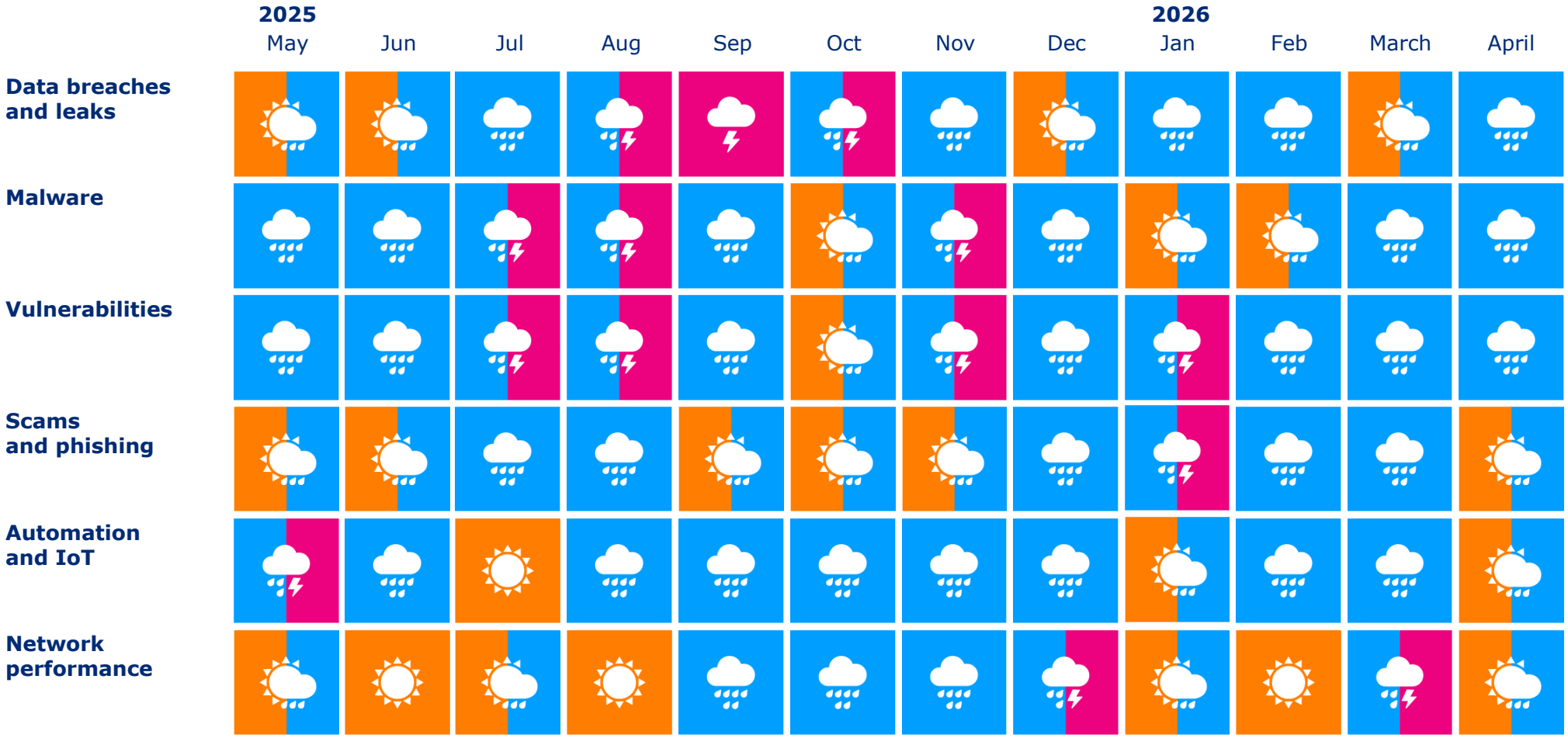
Automation and IoT

- A US interagency task force published guidance on applying zero trust principles to OT systems and environments.
- Poorly secured internet-connected cameras can also serve as valuable sources of information for intelligence services. For example, information on the movements of Iran's supreme leader Ayatollah Khamenei has reportedly been obtained from traffic camera footage.
- The US Cybersecurity and Infrastructure Security Agency (CISA) warned that Chinese cyber threat actors are building proxy networks from compromised IoT devices.

Network performance

- No serious disruptions were observed in public communications networks in April.
- AI-generated content can also be used to overload AI-based services provided externally by organisations. For example, when deploying a customer-facing chatbot on a website, organisations should take into account the limitations of the resources it uses.
- In addition to service congestion, massive volumes of input may also generate additional costs for organisations.

Cyber weather
in the past 12 months



Cyber weather forecast

The cyber weather forecast
provides a summary based on previous observations
and an indicative assessment of cyber threats
and their likely developments in the coming months.

Cyber weather forecast
Cyber threats remain at a typical level

1 mo.

The continued increase in Microsoft 365 account breaches, together with follow-on phishing messages sent from compromised accounts, is likely to lead to further account breaches in May.

AI technologies and their applications are evolving rapidly, which may cause sudden changes in attackers' methods and tactics. Continuous monitoring of the operating environment and adaptation to changes remain important for organisational security.

Organisational preparedness

- In vulnerability management, the rapid patching of internet-facing devices and services continues to be essential in reducing the exploitation of vulnerabilities.
- Know your network environment, the systems you use and their dependencies, and replace systems approaching end of life in a timely manner.
- Awareness-raising and multi-factor authentication (MFA) alone are not sufficient to protect employees against advanced account takeover attempts, such as phishing campaigns using the AiTM technique.

Worrying

The volume and severity of cyber threats are at a typical level.

However, the threat landscape can change rapidly — including in a negative direction.

The cyber weather forecast provides a summary based on previous observations and an indicative assessment of the cyber threat situation. It should not be used as the sole basis for preparedness – organisation-specific information and analysis must also be considered.